DISEÑO Y EVALUACIÓN DE UNA ARQUITECTURA SD-WAN SEGURA BASADA EN HERRAMIENTAS FORTINET PARA LA OPTIMIZACIÓN DE CONECTIVIDAD Y SEGURIDAD EN REDES EMPRESARIALES MULTI-SEDE EN COLOMBIA

(Monografía)

Camilo Alejandro Merizalde Moreno

Director:

Ing. Pedro Mancera Lagos

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ, 2026

Tabla de Contenido

ACRÓNIMOS Y GLOSARIO

Esta sección reúne los acrónimos utilizados en la monografía. Cada uno aparece con su significado completo y una nota breve cuando el término requiere precisión técnica. La primera vez que un acrónimo aparece en el cuerpo del texto se acompaña con su forma extendida entre paréntesis.

ADVPN: Auto-Discovery Virtual Private Network. Mecanismo propietario de Fortinet que construye túneles dinámicos entre spokes sin requerir preconfiguración explícita de cada par.

AES-GCM: Advanced Encryption Standard – Galois/Counter Mode. Algoritmo de cifrado simétrico de bloque con autenticación integrada.

ASIC: Application-Specific Integrated Circuit. Circuito integrado diseñado para una función específica. Fortinet usa ASIC propietarios (NP, CP, SP) para aceleración de tráfico y seguridad.

CIA: Confidentiality, Integrity, Availability. Tríada que define los pilares clásicos de la seguridad de la información.

CLI: Command Line Interface. Interfaz por línea de comandos.

DIA: Direct Internet Access. Acceso directo a Internet desde la sede sin pasar por el datacenter central.

DPI: Deep Packet Inspection. Inspección profunda de paquetes.

FortiOS: Fortinet Operating System. Sistema operativo propietario que ejecutan los equipos FortiGate.

GbE: Gigabit Ethernet. Estándar de Ethernet a 1 Gbps.

GUI: Graphical User Interface. Interfaz gráfica de usuario.

HA: High Availability. Alta disponibilidad mediante redundancia de equipos.

IKEv2: Internet Key Exchange version 2. Protocolo de intercambio de claves para IPSec.

IPS: Intrusion Prevention System. Sistema de prevención de intrusiones.

IPSec: Internet Protocol Security. Conjunto de protocolos para asegurar comunicaciones IP.

LAN: Local Area Network. Red de área local.

LTE: Long Term Evolution. Estándar de comunicación inalámbrica de cuarta generación.

MPLS: Multiprotocol Label Switching. Tecnología de transporte WAN basada en etiquetas que ofrecen los operadores.

NAT: Network Address Translation. Traducción de direcciones de red.

NGFW: Next-Generation Firewall. Firewall de nueva generación con capacidades de inspección de aplicaciones, IPS y filtrado web.

PFS: Perfect Forward Secrecy. Propiedad criptográfica que garantiza que la exposición de una clave no compromete las claves anteriores.

POS: Point of Sale. Sistema de punto de venta utilizado en retail.

QoS: Quality of Service. Calidad de servicio. Conjunto de mecanismos para priorizar tráfico de red.

SaaS: Software as a Service. Software como servicio entregado desde la nube.

SASE: Secure Access Service Edge. Modelo arquitectónico definido por Gartner que combina SD-WAN con servicios de seguridad en la nube.

SD-WAN: Software-Defined Wide Area Network. Red de área amplia definida por software.

SIEM: Security Information and Event Management. Plataforma de gestión de información y eventos de seguridad.

SLA: Service Level Agreement. Acuerdo de nivel de servicio. Define umbrales mensurables como latencia, jitter y pérdida de paquetes.

SOC: Security Operations Center. Centro de operaciones de seguridad.

SPU: Security Processing Unit. Procesador de seguridad propietario que acelera funciones criptográficas e inspección en FortiGate.

SSL/TLS: Secure Sockets Layer / Transport Layer Security. Protocolos de cifrado para comunicaciones.

TCO: Total Cost of Ownership. Costo total de propiedad.

VPN: Virtual Private Network. Red privada virtual.

WAN: Wide Area Network. Red de área amplia.

ZTNA: Zero Trust Network Access. Acceso a red con modelo de confianza cero.

ZTP: Zero Touch Provisioning. Aprovisionamiento de equipos sin intervención manual local.

RESUMEN

Esta monografía aborda el diseño de una arquitectura SD-WAN (Software-Defined Wide Area Network) sobre la plataforma Fortinet para empresas multi-sede en Colombia. La motivación nace de un patrón observado en el ejercicio profesional. Las redes WAN (Wide Area Network) basadas en MPLS (Multiprotocol Label Switching) son costosas. No permiten priorizar tráfico por aplicación. Obligan al backhauling al datacenter central. La operación del firewall, la VPN (Virtual Private Network) y el ruteo se hace en silos.

La propuesta consiste en aprovechar la funcionalidad SD-WAN nativa de FortiOS. Un FortiGate por sede actúa como controlador SD-WAN y NGFW (Next-Generation Firewall) al mismo tiempo. La gestión es centralizada desde FortiManager. La visibilidad se obtiene desde FortiAnalyzer. El alcance se concentra en tres frentes orientados a empresas multi-sede colombianas con presencia entre tres y diez ubicaciones.

El alcance se acota al diagnóstico del estado actual de la WAN, al diseño de la arquitectura SD-WAN con políticas SLA (Service Level Agreement) por aplicación y túneles IPSec (Internet Protocol Security), y a la validación del comportamiento en laboratorio virtualizado con GNS3 y FortiGate VM. El cronograma se ajusta a cuatro meses.

Palabras clave: SD-WAN, Fortinet, FortiGate, NGFW, MPLS, SLA, IPSec, FortiManager.

ABSTRACT

This monograph addresses the design of a Fortinet-based SD-WAN (Software-Defined Wide Area Network) architecture for multi-site enterprises in Colombia. The motivation comes from a pattern observed in the author's professional practice. MPLS-based WAN networks are expensive. They do not allow application-based traffic prioritization. They force traffic backhaul to the central datacenter. Firewall, VPN, and routing operations are siloed.

The proposal leverages FortiOS native SD-WAN capabilities. One FortiGate per site acts as both SD-WAN controller and NGFW. Management is centralized through FortiManager. Visibility is obtained from FortiAnalyzer. The scope is bounded to Colombian multi-site enterprises with three to ten locations.

Keywords: SD-WAN, Fortinet, FortiGate, NGFW, MPLS, SLA, IPSec, FortiManager.

INTRODUCCIÓN

La presente monografía del programa de pregrado de Ingeniería de Telecomunicaciones tiene como propósito evidenciar el cumplimiento de las competencias del programa. El trabajo se articula en torno al diseño de una arquitectura SD-WAN segura para empresas multi-sede en Colombia, sobre la plataforma Fortinet. La motivación nace de un patrón identificado en proyectos reales del ejercicio profesional. Las empresas con varias sedes en Colombia mantienen redes WAN basadas en MPLS con costos elevados, rigidez en el provisionamiento y degradación del rendimiento de aplicaciones en la nube.

MPLS es una tecnología confiable. Garantiza ancho de banda y baja latencia. El costo por mega es alto. Los tiempos de provisionamiento se miden en semanas. Cuando una empresa migra correo a Microsoft 365, archivos a SharePoint o aplicaciones a AWS, la red MPLS deja de ser el camino más corto. El tráfico sale de la sede, viaja por la troncal hasta el datacenter, sale al Internet, llega a la nube y vuelve por el mismo recorrido. La latencia adicional es evitable.

SD-WAN cambia la lógica del transporte WAN. Permite usar varios transportes al mismo tiempo. Permite seleccionar la mejor ruta por aplicación. Centraliza la gestión. En este proyecto se trabaja con Fortinet Secure SD-WAN porque integra el NGFW y el SD-WAN en el mismo equipo, bajo el mismo sistema operativo (FortiOS) y con la misma licencia. La integración cambia la economía y la operación del proyecto.

El documento se organiza así. El Capítulo 1 desarrolla el problema. El Capítulo 2 cubre la ideación de la solución. El Capítulo 3 analiza las alternativas técnicas. Los Capítulos 4, 5 y 6 desarrollan cada uno un objetivo específico. El alcance se ejecuta en cuatro meses, según el cronograma de la Figura 9.

1. PROBLEMA

1.1. ÁRBOL DE PROBLEMAS

El árbol de problemas estructura el problema central, sus causas y sus efectos. El problema central identificado es la ineficiencia y vulnerabilidad de las redes WAN tradicionales basadas en MPLS para soportar las exigencias actuales de un entorno empresarial multi-sede. Se identifican cuatro causas raíz y cuatro efectos directos. Cada uno se respalda con datos bibliográficos. La Figura 1 presenta el árbol de problemas elaborado para este proyecto.

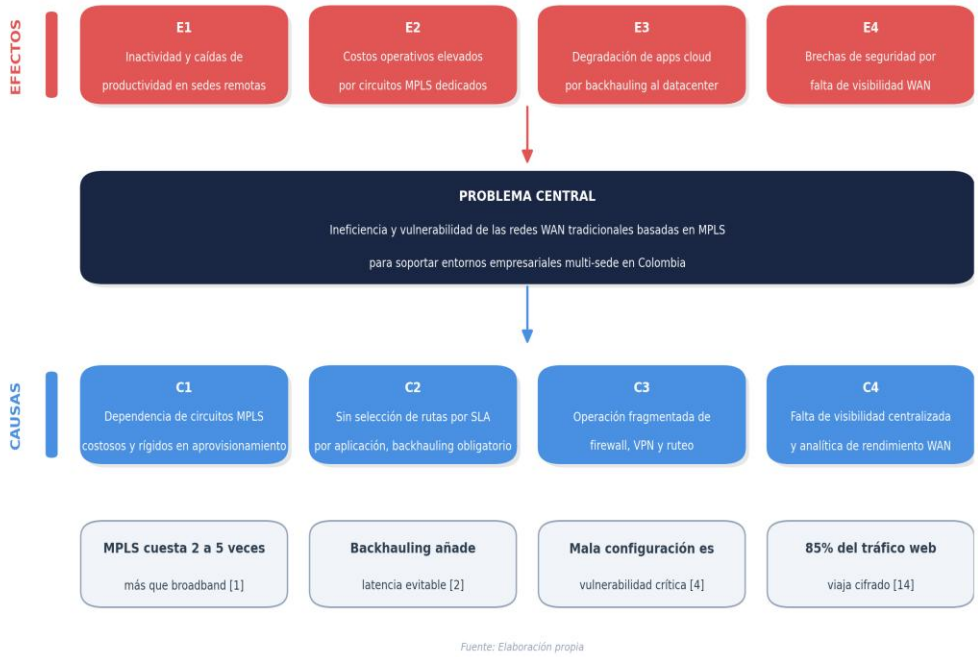

Figura 1. Árbol de problemas

Fuente: Elaboración propia

1.2. QUÉ SE QUIERE SOLUCIONAR

Descripción. La problemática general del sector es la dependencia de redes WAN basadas en MPLS. Esta tecnología fue durante años la respuesta correcta para conectar sedes con calidad de servicio garantizada. Hoy la mayoría de aplicaciones críticas residen en la nube. Lo que importa es la experiencia del usuario al acceder a esas

aplicaciones, no la calidad de un circuito dedicado entre sedes. Insistir en MPLS para tráfico cloud añade latencia evitable y aumenta los costos operativos. Estudios recientes reportan que MPLS cuesta entre dos y cinco veces más que enlaces broadband equivalentes [1].

Delimitación. El caso particular dentro del sector son las empresas colombianas medianas y grandes con presencia multi-sede. En este segmento los costos de MPLS son proporcionalmente más altos que en mercados desarrollados. Las asimetrías regionales en infraestructura limitan las opciones de operadores. La migración a la nube avanzó más rápido que la modernización de la red. Como consecuencia, en el ejercicio profesional se encuentran despliegues con configuraciones de firewall sin actualizar, plataformas SIEM subutilizadas y políticas de seguridad inconsistentes entre sedes.

Definición. Los problemas técnicos concretos a resolver son cuatro. Primero, la imposibilidad de aplicar políticas de steering por aplicación con routers WAN tradicionales. Segundo, el backhauling obligatorio que añade latencia al tráfico hacia servicios cloud. Tercero, las inconsistencias entre sedes por gestión descentralizada de políticas. Cuarto, la falta de mecanismos de failover automatizado basados en métricas reales como latencia, jitter y pérdida de paquetes [2], [3].

Propuesta. Frente a esta situación se propone diseñar y evaluar una arquitectura SD-WAN segura sobre Fortinet Secure SD-WAN. La solución integra en un solo dispositivo FortiGate las funciones de NGFW, SD-WAN, ruteo avanzado y optimización WAN. La gestión es centralizada desde FortiManager. La analítica se obtiene desde FortiAnalyzer [5]. La arquitectura habilita Direct Internet Access (DIA) con inspección de seguridad NGFW local, selección de rutas por SLA por aplicación, overlay IPSec automatizado y zero-touch provisioning para nuevas sedes.

2. IDEACIÓN DE LA SOLUCIÓN

La idea central de la solución es la convergencia de networking y seguridad en una sola plataforma. Esa convergencia se materializa en FortiOS. La arquitectura propuesta utiliza el FortiGate como controlador SD-WAN y NGFW al mismo tiempo. FortiManager

orquesta políticas y plantillas. FortiAnalyzer entrega visibilidad analítica. La solución elimina la necesidad de operar router, firewall y concentrador VPN como dispositivos separados en cada sede.

2.1. ALCANCE DEL PROYECTO

El alcance se acota al sector de redes empresariales multi-sede en Colombia. La especificidad del contexto colombiano es deliberada. Las realidades de infraestructura, costos operativos y disponibilidad de servicios difieren respecto a otros mercados. Una solución genérica importada desde la literatura internacional no aplica directamente.

Universo de aplicación. Se consideran empresas con presencia entre tres y diez sedes. Este rango cubre la mayoría del segmento mediano y grande en el mercado colombiano. Las empresas con menos de tres sedes no obtienen valor proporcional al esfuerzo de migración. Las empresas con más de diez sedes requieren un análisis adicional de escalabilidad que excede el alcance académico de este trabajo.

Sectores incluidos. Financiero, salud, manufactura, retail, educación y gobierno. La selección no es vertical sino transversal. La condición común es la operación de WAN entre sedes con tráfico mixto de aplicaciones locales y en la nube.

Tecnologías evaluadas. Fortinet Secure SD-WAN como plataforma principal. Se contemplan los modelos FortiGate 60F, 80F, 100F, 200F, 400F y 600F como dispositivos de borde según el tamaño de cada sede. FortiManager como orquestador. FortiAnalyzer como plataforma de logs y analítica.

Tipo de proyecto. Diseño arquitectónico validado mediante simulación. No se incluye implementación en producción. El laboratorio virtualizado se construye sobre GNS3 con imágenes FortiGate VM.

Período de ejecución. Cuatro meses calendario, equivalentes a 16 semanas. El cronograma se presenta en la Figura 9.

Exclusiones. Quedan fuera del alcance los temas relacionados con SASE en nube pública (Cloud SWG y CASB), la migración a ZTNA universal, la integración con SIEM

de terceros y los aspectos de cumplimiento sectorial específico (PCI-DSS, HIPAA, entre otros). Estos temas se mencionan como extensiones posibles para trabajos futuros.

2.2. CARACTERÍSTICAS DE LAS REDES EMPRESARIALES MULTI-SEDE EN COLOMBIA

Para diseñar una solución pertinente es necesario caracterizar las redes objetivo. La caracterización siguiente surge tanto de la literatura del sector como de la experiencia profesional del autor en proyectos reales.

2.2.1. Características topológicas

La mayoría de empresas multi-sede en Colombia opera con topologías hub-and-spoke. Existe un datacenter principal, generalmente en Bogotá. Las sedes restantes se conectan al datacenter mediante enlaces dedicados. El tráfico entre sedes hermanas pasa por el datacenter. La topología full-mesh es excepcional y se reserva para empresas con requisitos especiales como replicación de bases de datos o comunicaciones unificadas críticas.

El número de sedes promedio observado es siete. Las empresas tienden a concentrar operaciones en cuatro o cinco ciudades principales: Bogotá, Medellín, Cali, Barranquilla y Bucaramanga. Las sedes secundarias se ubican en ciudades intermedias como Cartagena, Pereira, Manizales o Ibagué. Las sedes en municipios pequeños son la excepción.

2.2.2. Características de transporte

El transporte WAN predominante sigue siendo MPLS. Los operadores que dominan el mercado corporativo colombiano son Claro, ETB, Movistar, Tigo Une e Internexa. Las velocidades típicas oscilan entre 10 Mbps y 100 Mbps por sede. Las velocidades superiores a 100 Mbps son habituales en datacenters y sedes principales.

El acceso secundario más frecuente es Internet broadband sobre fibra óptica. Las velocidades disponibles son superiores a las de MPLS. El costo por mega es entre dos y cinco veces inferior. Sin embargo, el broadband se utiliza típicamente solo como

respaldo o como salida para navegación general, sin políticas SD-WAN que permitan aprovechar su capacidad para tráfico productivo.

LTE como medio de respaldo se utiliza en sedes pequeñas o de difícil acceso. La cobertura es razonable en zonas urbanas. La capacidad y la latencia son aceptables para aplicaciones no críticas. El costo se controla mediante cuotas de tráfico mensuales.

2.2.3. Características de aplicaciones

El portafolio de aplicaciones típico combina aplicaciones legadas locales con aplicaciones en la nube. Las aplicaciones locales incluyen ERP corporativo como SAP, sistemas de gestión documental y aplicaciones propietarias del sector. Estas aplicaciones residen en el datacenter principal y requieren conectividad desde las sedes para acceder.

Las aplicaciones en la nube incluyen Microsoft 365 (correo, OneDrive, Teams y SharePoint), Google Workspace en menor medida, Salesforce en sectores comerciales, plataformas de videoconferencia como Zoom o Webex, y cargas de trabajo en AWS, Azure o Google Cloud.

La proporción de tráfico ha cambiado significativamente. Hace una década la mayoría del tráfico iba al datacenter. Hoy más del 60 % del tráfico tiene como destino la nube pública. Esta inversión convierte al backhauling al datacenter en una fricción operativa real.

2.2.4. Características de seguridad

La seguridad perimetral predominante en empresas multi-sede colombianas se basa en NGFW. Los fabricantes más desplegados son Fortinet, Cisco, Palo Alto Networks y Check Point. Fortinet tiene una cuota relevante en el segmento mediano por relación precio-prestaciones.

Las funciones de seguridad activadas dependen del nivel de madurez del cliente. Las capacidades de filtrado de aplicaciones, IPS y filtrado web están presentes en la mayoría

de despliegues. La inspección SSL/TLS local es menos frecuente porque requiere CPU adicional y políticas de privacidad explícitas. ZTNA está en fase temprana de adopción.

2.2.5. Características regulatorias

Las organizaciones colombianas operan bajo la Ley 1581 de 2012 de protección de datos personales, la Ley 1273 de 2009 de delitos informáticos y los lineamientos del documento Conpes 3995 de 2020 sobre confianza y seguridad digital. Estas regulaciones imponen requisitos de cifrado, control de acceso y auditoría que se alinean naturalmente con las capacidades de una arquitectura SD-WAN segura.

2.3. POR QUÉ SE PLANTEA AHORA LA SOLUCIÓN

Existen razones técnicas, económicas y operativas que sustentan el momento de la propuesta. La primera razón es la madurez del producto. Fortinet Secure SD-WAN está en producción en miles de organizaciones. Gartner lo reconoce como Líder en su Magic Quadrant. Los estudios independientes documentan resultados concretos. Forrester reporta un retorno de inversión del 300% en tres años con periodo de recuperación en ocho meses [10]. Enterprise Strategy Group valida las mejoras en agilidad, seguridad y reducción de costos a partir de entrevistas con clientes operativos [9].

La segunda razón es la consolidación del modelo cloud. La adopción de Microsoft 365, Google Workspace, Salesforce y plataformas IaaS en Colombia se aceleró con la pandemia. La adopción no se revirtió. El backhauling de tráfico al datacenter central se convirtió en una fricción operativa real [2].

La tercera razón se relaciona con la seguridad. Aproximadamente el 85% del tráfico web actual viaja cifrado [14]. Sin inspección SSL/TLS local, el firewall no ve el contenido. Fortinet Secure SD-WAN realiza esa inspección directamente en el plano de datos del SD-WAN, con IPS, control de aplicaciones y filtrado web integrados [5].

La cuarta razón es la disponibilidad de herramientas de orquestación. FortiManager permite gestionar todos los sites desde una sola consola. Aplica plantillas de configuración. Despliega nuevas sedes mediante zero-touch provisioning. FortiAnalyzer

entrega métricas de SLA, consumo de ancho de banda, amenazas detectadas y uso por aplicación.

La quinta razón tiene un componente personal. El autor trabaja a diario con FortiGate, FortiManager y FortiAnalyzer en proyectos reales. Tiene acceso a imágenes virtuales para laboratorio. Conoce la sintaxis CLI y la lógica de la GUI de FortiOS.

2.4. OBJETIVOS DEL PROYECTO

El árbol de objetivos es la imagen invertida del árbol de problemas. Lo que antes era causa pasa a ser medio. Lo que antes era efecto pasa a ser fin. El objetivo general es diseñar y evaluar una arquitectura SD-WAN segura basada en Fortinet Secure SD-WAN para optimizar conectividad y seguridad en redes empresariales multi-sede en Colombia. Ese objetivo se desagrega en tres específicos, cada uno desarrollado en su propio capítulo. La Figura 2 presenta el árbol de objetivos del proyecto.

Figura 2. Árbol de objetivos

Fuente: Elaboración propia

Objetivo general. Diseñar y evaluar una arquitectura SD-WAN segura basada en Fortinet Secure SD-WAN que optimice la conectividad y la seguridad en redes empresariales multi-sede en Colombia.

Objetivos específicos:

OE1. Diagnosticar el estado actual de la infraestructura WAN en un escenario empresarial multi-sede en Colombia, identificando brechas de rendimiento, costos operativos y deficiencias de seguridad.

OE2. Diseñar la arquitectura SD-WAN integrando topología hub-spoke, overlay IPSec, políticas SLA por aplicación, NGFW integrado y gestión centralizada con FortiManager y FortiAnalyzer.

OE3. Validar la arquitectura propuesta mediante simulación en un laboratorio virtualizado con GNS3 y FortiGate VM, evaluando métricas de rendimiento, eficacia del failover y funciones de seguridad integradas.

La validación del tercer objetivo se materializó como resultado central del trabajo: sus mediciones se presentan en el Capítulo 6 (Resultados de las pruebas) y se respaldan con las evidencias del laboratorio en ejecución del Anexo C, lo que permite contrastar directamente cada objetivo específico con la evidencia obtenida.

2.5. SITUACIÓN ACTUAL Y SITUACIÓN DESEADA

Para entender el cambio que propone el proyecto se contrasta la situación actual con la situación esperada mediante diagramas de arquitectura. La Figura 3 representa la situación actual. La Figura 4 representa la situación deseada.

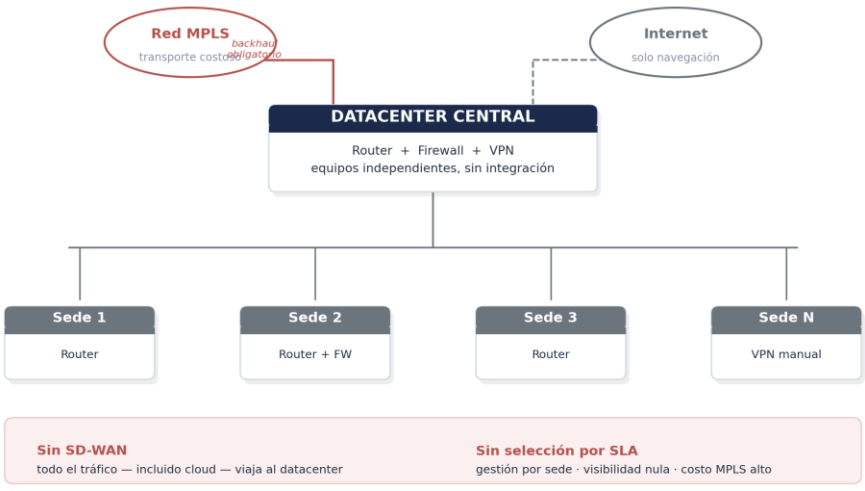

Figura 3. Situación actual de la arquitectura WAN tradicional

Fuente: Elaboración propia

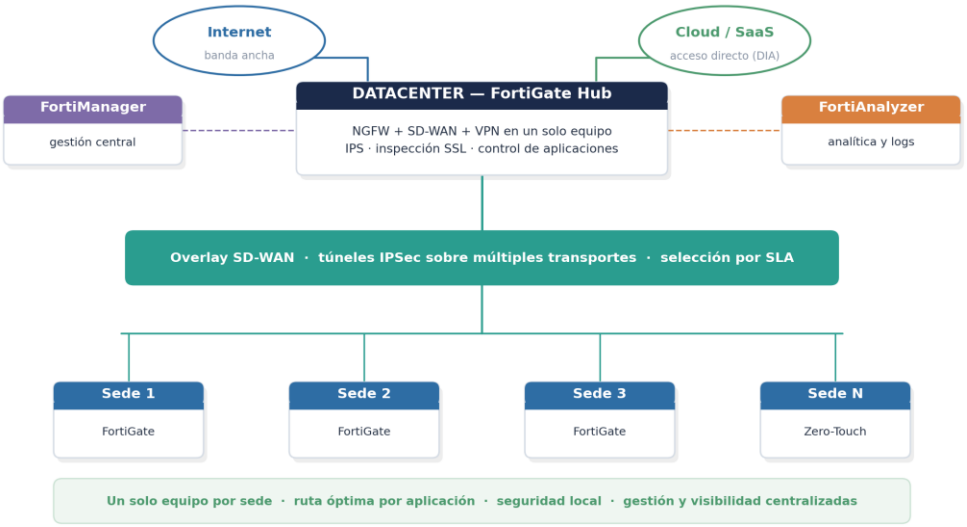

Figura 4. Situación deseada con arquitectura Fortinet Secure SD-WAN

Fuente: Elaboración propia

2.6. DIAGRAMA DE RED FÍSICA Y LÓGICA

La arquitectura propuesta se representa en dos planos: la red física, que muestra los enlaces de transporte reales contratados con operadores; y la red lógica, que muestra el overlay SD-WAN y las políticas SLA. La Figura 5 presenta ambos planos en un diagrama dual.

Plano físico (Underlay). El hub se ubica en el datacenter principal en Bogotá con un FortiGate 600F. El hub tiene dos accesos WAN: WAN1 hacia Internet a través de un ISP de banda ancha y WAN2 hacia la red MPLS de un operador Tier-1. Las sedes spoke tienen modelos FortiGate proporcionales a su tamaño: 100F para sedes administrativas de Bogotá, 80F para la planta de Medellín, y 60F para sucursales de Cali y Barranquilla. Cada sede tiene al menos un acceso a Internet broadband. Las sedes principales tienen también acceso MPLS. Las sucursales pequeñas tienen LTE como respaldo.

Plano lógico (Overlay). Sobre la red física se construye una zona SD-WAN con túneles IPSec IKEv2 cifrados con AES-256-GCM. Los túneles son hub-spoke con ADVPN habilitado para permitir mesh dinámico entre spokes que se comunican entre sí. Las políticas SLA configuradas dirigen el tráfico crítico (VoIP, ERP) por el enlace de mejor

calidad y el tráfico no crítico (navegación general) por el enlace más económico. FortiManager orquesta toda la configuración. FortiAnalyzer centraliza los logs.

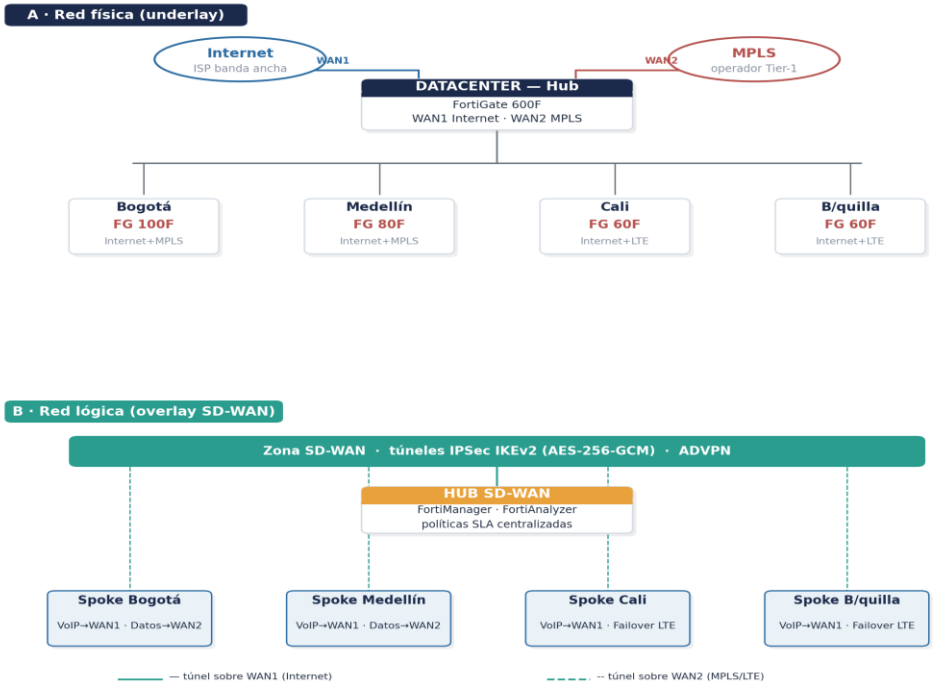

Figura 5. Diagrama dual de red física y red lógica de la arquitectura propuesta

Fuente: Elaboración propia

3. ANÁLISIS DE LAS ALTERNATIVAS TÉCNICAS PARA SOLUCIONAR EL PROBLEMA

Esta sección analiza las alternativas técnicas para resolver la problemática planteada. El análisis se enfoca en la aplicación de cada bloque funcional de la arquitectura SD-WAN al problema concreto de empresas multi-sede en Colombia. Cada bloque se discute en términos de ventajas, desventajas, requerimientos, restricciones y decisión justificada. Al final se presenta la matriz de evaluación numérica.

Figura 6. Bloques funcionales de la arquitectura Fortinet Secure SD-WAN

Fuente: Elaboración propia

3.1. DIFERENCIAS TÉCNICAS ENTRE LOS EQUIPOS FORTIGATE DE LA TOPOLOGÍA

La elección del modelo FortiGate por sede no es arbitraria. Cada modelo de la línea está dimensionado para un rango de capacidad, número de usuarios, throughput de inspección y funcionalidades de aceleración por hardware. La argumentación siguiente justifica la asignación de modelos en la topología propuesta.

3.1.1. FortiGate 600F en el datacenter (hub)

El FortiGate 600F ofrece un throughput de firewall cercano a 36 Gbps, throughput SSL-VPN cercano a 6 Gbps y soporte para más de cuatro mil VPN IPSec gateway-to-gateway concurrentes. Su capacidad lo hace adecuado como hub central para una topología con múltiples spokes. Cuenta con procesador NP6Lite y CP9 para aceleración de tráfico y criptografía. Referencia de producto: https://www.fortinet.com/products/next-generation-firewall/fortigate-600f.

3.1.2. FortiGate 100F en sede administrativa (Bogotá)

El FortiGate 100F entrega un throughput de firewall cercano a 20 Gbps con SD-WAN nativo y soporte para inspección SSL acelerada. Su tamaño es adecuado para una sede administrativa con tráfico mixto de aplicaciones locales y cloud, con varios cientos de usuarios concurrentes. Referencia de producto: https://www.fortinet.com/products/next-generation-firewall/fortigate-100f.

3.1.3. FortiGate 80F en la planta de Medellín

El FortiGate 80F ofrece throughput de firewall cercano a 10 Gbps y throughput de inspección de amenazas cercano a 900 Mbps. Es adecuado para una planta de producción con perfil mixto de tráfico industrial y administrativo. La presencia de puertos PoE en algunas variantes facilita la conexión de teléfonos IP y puntos de acceso inalámbricos. Referencia de producto: https://www.fortinet.com/products/next-generation-firewall/fortigate-80f-series.

3.1.4. FortiGate 60F en sucursales (Cali y Barranquilla)

El FortiGate 60F es el modelo de entrada con SD-WAN nativo y NGFW completo. Su throughput de firewall cercano a 10 Gbps con inspección de amenazas alrededor de 700 Mbps lo hace adecuado para sucursales con menos de cien usuarios. La compactación física y el bajo consumo lo convierten en una opción operativamente eficiente para sedes pequeñas. Referencia de producto: https://www.fortinet.com/products/next-generation-firewall/fortigate-60f.

3.1.5. Tabla comparativa de los equipos

La elección de cada modelo responde al binomio capacidad-costo. La Tabla 1 resume los criterios diferenciales entre los modelos asignados en la topología propuesta.

Tabla 1. Comparación técnica de los equipos FortiGate de la topología

Característica	600F (Hub)	100F (Bogotá)	80F (Medellín)	60F (Sucursal)
Throughput firewall	~36 Gbps	~20 Gbps	~10 Gbps	~10 Gbps
Inspección amenazas	~10 Gbps	~1 Gbps	~900 Mbps	~700 Mbps
Túneles IPSec	+4000	~2500	~2000	~2000
Aceleración ASIC	NP6Lite + CP9	SoC4	SoC4	SoC4

Característica	600F (Hub)	100F (Bogotá)	80F (Medellín)	60F (Sucursal)
Rol en la topología	Hub central	Sede admin.	Planta	Sucursal

Fuente: Elaboración propia con datos de las fichas técnicas del fabricante

El FortiGate 600F tiene aceleración completa por hardware en todos los flujos. El 100F mantiene aceleración para la mayoría de operaciones. El 80F y el 60F dependen más del procesador principal para inspección compleja, lo cual es aceptable dado el volumen menor de tráfico de sus respectivas sedes.

3.2. PLANO DE DATOS

El plano de datos es el bloque que procesa los paquetes en línea. ¿Qué tecnología puede manejar simultáneamente NGFW y SD-WAN sin agregar latencia significativa? Las alternativas viables son tres. La primera es FortiGate con FortiOS, que integra ambas funciones en el mismo ASIC. La segunda es Cisco Catalyst SD-WAN con un firewall externo en cadena. La tercera es VMware VeloCloud con un firewall virtual adicional.

Ventajas de FortiGate. Procesamiento acelerado por hardware mediante el procesador de seguridad SPU. Inspección DPI y SSL sin penalización significativa de rendimiento. Una sola consola de gestión. Una sola licencia. Bajo TCO comparado con soluciones encadenadas.

Desventajas. Requiere conocimiento específico de FortiOS para aprovechar las capacidades avanzadas.

Decisión. Se selecciona FortiGate con FortiOS por la integración nativa de NGFW y SD-WAN, el aceleramiento por SPU y el bajo TCO. La decisión se alinea con el conocimiento operativo del autor [5].

3.3. PLANO DE CONTROL

El plano de control es el bloque que decide por qué transporte se envía cada flujo. Las alternativas son dos. La primera es el motor SD-WAN nativo de FortiOS, que evalúa probes SLA en intervalos configurables. La segunda es un controlador SDN externo. Esta segunda opción agrega complejidad sin valor adicional para el caso de uso planteado.

Decisión. Se selecciona el motor SD-WAN nativo de FortiOS. La decisión evita complejidad innecesaria [1], [5].

3.4. PLANO DE GESTIÓN

El plano de gestión orquesta la configuración a través de todas las sedes. Se selecciona FortiManager por su capacidad de aplicar plantillas, mantener versionado de configuración y habilitar zero-touch provisioning. Referencia de producto: https://www.fortinet.com/products/management/fortimanager. La decisión se alinea con la práctica recomendada por Fortinet en arquitecturas SD-WAN multi-sede [4], [5].

3.5. UNDERLAY (TRANSPORTES FÍSICOS)

Para la propuesta se contempla broadband como transporte principal y MPLS residual o LTE como respaldo, según la sede. La combinación ofrece la mejor relación costo-disponibilidad para el contexto colombiano [1], [2].

3.6. OVERLAY (TÚNEL CIFRADO)

Se selecciona IPSec con IKEv2 en topología hub-spoke con ADVPN habilitado para flujos spoke-to-spoke críticos. El cifrado es AES-256-GCM con integridad SHA-384 y grupo Diffie-Hellman 14 [3], [5].

3.7. VISIBILIDAD Y ANALÍTICA

Se selecciona FortiAnalyzer como solución primaria de visibilidad. Para organizaciones con SIEM enterprise, FortiAnalyzer puede actuar como agregador. Referencia de producto: https://www.fortinet.com/products/management/fortianalyzer [18], [19].

3.8. MATRIZ DE EVALUACIÓN DE LA PROPUESTA

La selección de la propuesta no obedece solo a un análisis técnico aislado. Se construye una matriz de evaluación con ocho criterios. Cada criterio recibe un valor porcentual. La Figura 7 presenta los resultados.

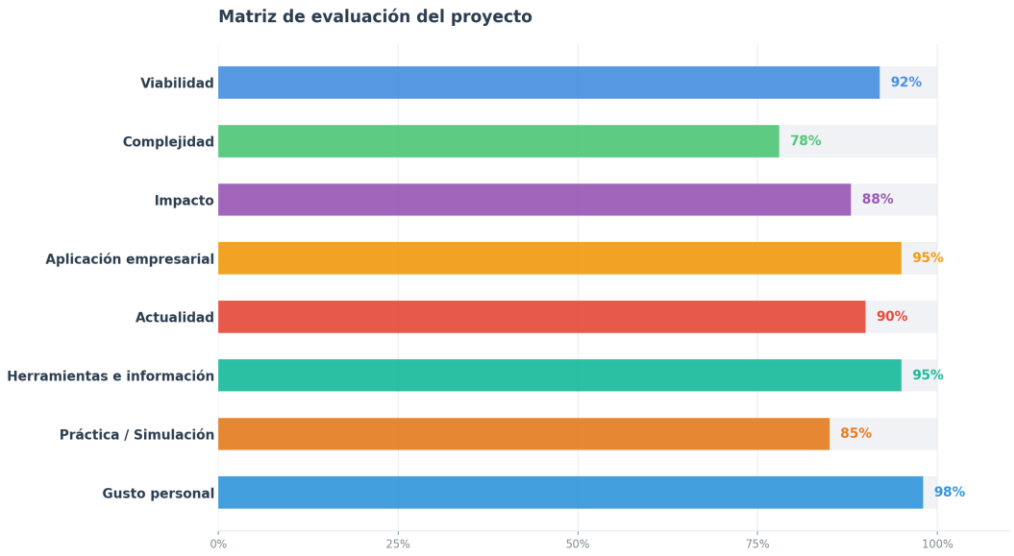

Figura 7. Matriz de evaluación del proyecto

Fuente: Elaboración propia

Viabilidad (92%). El proyecto es ejecutable en cuatro meses con recursos accesibles.

Complejidad (78%). El diseño tiene complejidad técnica real pero adecuada al nivel de un trabajo de grado de pregrado.

Impacto (88%). Aborda un problema vigente en empresas medianas y grandes en Colombia.

Aplicación empresarial (95%). El proyecto aplica directamente al sector empresarial multi-sede.

Actualidad (90%). SD-WAN es una tecnología vigente con reportes recientes de la industria [9], [10].

Herramientas e información disponible (95%). El acceso a FortiGate VM, FortiManager y FortiAnalyzer es completo.

Práctica y simulación (85%). El laboratorio GNS3 permite reproducir el comportamiento de la arquitectura.

Gusto personal (98%). La afinidad del autor con SD-WAN y el ecosistema Fortinet es alta.

4. CAPÍTULO OE1 — DIAGNÓSTICO DEL ESTADO ACTUAL DE LA INFRAESTRUCTURA WAN

Este capítulo desarrolla el primer objetivo específico del proyecto. La identificación del objetivo se hace a través de tres apartados que permiten reconocer su alcance, su método y sus entregables.

4.1. IDENTIFICACIÓN DEL OBJETIVO

4.1.1. Enunciado

Diagnosticar el estado actual de la infraestructura WAN en un escenario empresarial multi-sede en Colombia, identificando brechas de rendimiento, costos operativos y deficiencias de seguridad.

4.1.2. Justificación

Sin un diagnóstico cuantitativo y documentado de la situación actual no es posible dimensionar el impacto de la solución propuesta ni priorizar las actividades de migración. El diagnóstico también valida los supuestos del problema.

4.1.3. Entregable esperado

Documento de levantamiento con la topología existente, métricas de rendimiento por sede, inventario de circuitos contratados, descripción del estado de los dispositivos perimetrales actuales y matriz de brechas identificadas.

4.2. ACTIVIDADES

A1.1. Levantamiento de la topología actual mediante revisión documental, entrevistas con el equipo de operaciones y verificación de los diagramas existentes.

A1.2. Análisis de logs y métricas históricas en FortiAnalyzer cuando ya esté desplegado, o captura puntual con Wireshark cuando no exista plataforma de logs.

A1.3. Caracterización de patrones de uso por aplicación. Identificación de las aplicaciones críticas y el porcentaje de tráfico cloud frente a tráfico al datacenter.

A1.4. Documentación de brechas. Comparación entre la operación actual y las buenas prácticas. Generación de la matriz de hallazgos priorizada.

4.3. MÉTODO

El método combina revisión documental, observación directa y análisis de datos. La revisión documental se basa en los diagramas, contratos con operadores y configuraciones de los dispositivos. La observación directa se realiza durante las visitas a sede o por acceso remoto. El análisis de datos se hace sobre los logs históricos de FortiAnalyzer o sobre capturas Wireshark cuando aplique.

5. CAPÍTULO OE2 — DISEÑO DE LA ARQUITECTURA SD-WAN

Este capítulo desarrolla el segundo objetivo específico. La identificación del objetivo se hace a través de tres apartados que permiten reconocer su alcance, su método y sus entregables.

5.1. IDENTIFICACIÓN DEL OBJETIVO

5.1.1. Enunciado

Diseñar la arquitectura SD-WAN integrando topología hub-spoke, overlay IPSec, políticas SLA por aplicación, NGFW integrado y gestión centralizada con FortiManager.

5.1.2. Justificación

El diseño es el núcleo técnico del proyecto. Define la asignación de modelos FortiGate por sede, los criterios de selección SLA, las plantillas de FortiManager y los dashboards de FortiAnalyzer. Un diseño correcto reduce el riesgo de la fase de validación y facilita la futura implementación en producción.

5.1.3. Entregable esperado

Documento de diseño con la topología lógica detallada, el plan de direccionamiento, la matriz de políticas SLA por aplicación, el catálogo de plantillas FortiManager y la especificación de los dashboards FortiAnalyzer.

5.2. ACTIVIDADES

A2.1. Definición de la topología lógica hub-spoke con asignación de modelos FortiGate por sede según los criterios del apartado 3.1. Elaboración del plan de direccionamiento IP.

A2.2. Diseño de probes SLA y políticas de steering por aplicación. Definición de umbrales de latencia, jitter y pérdida de paquetes para cada aplicación crítica.

A2.3. Diseño de plantillas FortiManager por rol (hub, spoke administrativo, spoke productivo, sucursal). Especificación de dashboards FortiAnalyzer para SLA, seguridad y rendimiento.

5.3. MÉTODO

El método sigue un enfoque top-down. Primero se definen los requerimientos funcionales y no funcionales. Luego se traducen en decisiones de arquitectura. Las decisiones se documentan en formato matriz para facilitar la trazabilidad. El diseño se valida iterativamente con el director del proyecto, el Ing. Pedro Mancera Lagos, y con la práctica del oficio.

6. CAPÍTULO OE3 — VALIDACIÓN EN LABORATORIO VIRTUALIZADO

Este capítulo desarrolla el tercer objetivo específico. La identificación del objetivo se hace a través de tres apartados que permiten reconocer su alcance, su método y sus entregables.

6.1. IDENTIFICACIÓN DEL OBJETIVO

6.1.1. Enunciado

Validar la arquitectura propuesta mediante simulación en laboratorio virtualizado con GNS3 y FortiGate VM, evaluando métricas de rendimiento, eficacia de failover y funciones de seguridad integradas.

6.1.2. Justificación

La validación es la prueba empírica de que el diseño se comporta como se esperaba. Sin validación el diseño es solo una hipótesis. La validación en laboratorio virtualizado permite reproducir escenarios complejos con costos marginales y sin afectar la operación.

6.1.3. Entregable esperado

Documento de resultados con las métricas medidas antes y después de la aplicación de políticas SD-WAN, los tiempos de failover registrados, los logs de incidentes simulados y el análisis comparativo entre el comportamiento observado y el esperado.

6.2. ACTIVIDADES

A3.1. Montaje del laboratorio GNS3 con cinco instancias FortiGate VM (hub y cuatro spokes). Configuración del direccionamiento y de la conectividad WAN simulada.

A3.2. Configuración de la arquitectura aplicando las plantillas diseñadas en el OE2. Inyección de tráfico sintético con iPerf3 y herramientas de generación de carga.

A3.3. Pruebas de failover. Medición de latencia, jitter y pérdida de paquetes en escenarios normales y degradados. Simulación de caídas de transporte para validar la conmutación automática.

A3.4. Análisis comparativo de resultados. Documentación de conclusiones y recomendaciones para una eventual implementación en producción.

6.3. MÉTODO

El método experimental se basa en la comparación pre/post. Se establece una línea base sin políticas SD-WAN, luego se activan las políticas y se vuelven a medir las mismas métricas. La diferencia cuantifica el beneficio de la arquitectura. La instrumentación utilizada combina pruebas activas ICMP (latencia y pérdida), los probes del health-check SD-WAN de FortiOS (latencia, jitter, pérdida y MOS por miembro), traceroute (ruta del overlay), la tabla de sesiones del FortiGate (validación del NAT de salida) y la suspensión controlada de enlaces para el failover; iPerf3 queda disponible para pruebas de carga TCP/UDP cuando se requiera caracterizar throughput.

6.4. EJECUCIÓN DEL LABORATORIO

La validación se materializó en un laboratorio virtualizado que reproduce la arquitectura hub-and-spoke diseñada en el OE2. El laboratorio implementa el datacenter (hub) y las cuatro sedes (Bogotá, Medellín, Cali y Barranquilla), el doble transporte de underlay, el overlay IPSec cifrado, el motor de selección por SLA, el acceso directo a Internet con inspección NGFW y el plano de gestión y analítica. Cada bloque funcional descrito en el capítulo 3 se ejercitó de forma medible.

6.4.1. Plataforma de emulación y versión de firmware

El banco de pruebas se construyó sobre GNS3 2.2 (servidor local) con QEMU 11 y aceleración por hardware del hipervisor (Windows Hypervisor Platform, WHPX). Toda la plataforma se unificó en FortiOS 7.6.6: FortiGate-VM (build 3652) y FortiManager / FortiAnalyzer (build 3654). La unificación de versiones evita incompatibilidades de gestión y de protocolo entre los componentes Fortinet. Se desplegaron cinco instancias FortiGate-VM (un hub y cuatro sedes), un FortiManager, un FortiAnalyzer, los conmutadores de los dos transportes, un nodo NAT y los hosts de prueba (servidor del datacenter, clientes por sede y un endpoint que representa la nube/SaaS).

Nota sobre el modelado de equipos: en emulación todas las instancias usan la misma imagen FortiGate-VM, que representa los roles de hardware definidos en el apartado 3.1 (FortiGate 600F en el hub; 100F, 80F y 60F en las sedes). El throughput por procesador de seguridad (SPU) es una característica de hardware y no aplica en la máquina virtual; la validación se centra en el comportamiento funcional de los planos de datos, control, overlay, seguridad y gestión.

6.4.2. Topología implementada y plan de direccionamiento

La Figura 8 presenta la topología del laboratorio. El tráfico corporativo de cada sede hacia el datacenter viaja por el overlay IPSec cifrado con selección por SLA y conmutación automática; el tráfico de Internet/SaaS sale localmente por DIA con NAT e inspección NGFW.

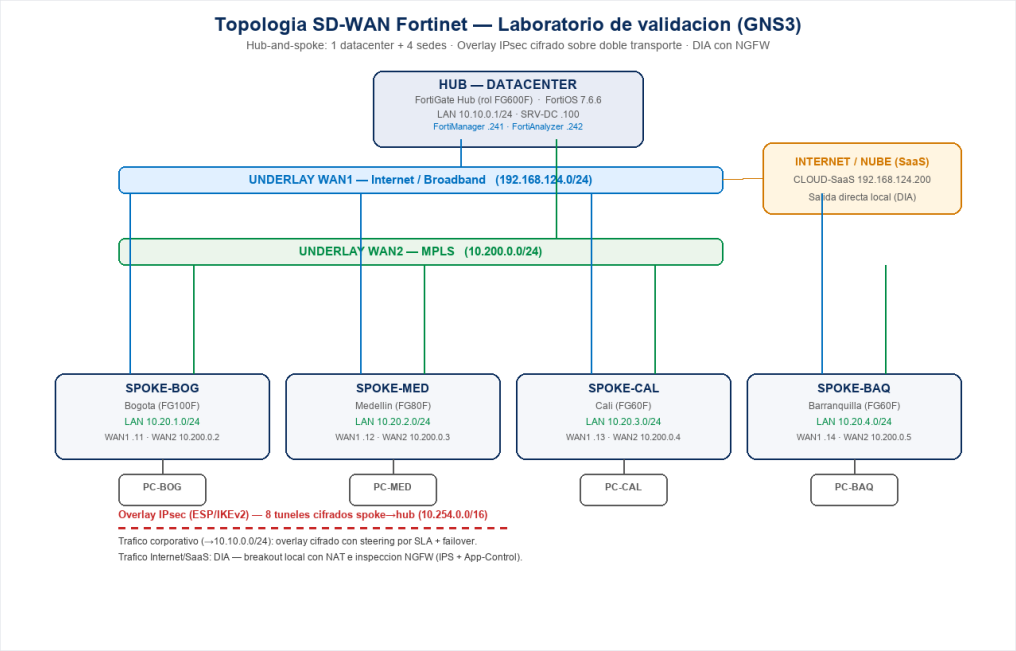

Figura 8. Topología del laboratorio de validación SD-WAN en GNS3 (hub + 4 sedes). Fuente: Elaboración propia.

El plan de direccionamiento del laboratorio se resume en la Tabla 2. El underlay WAN1 (Internet/broadband) usa la red 192.168.124.0/24 y el underlay WAN2 (MPLS) la red 10.200.0.0/24. La LAN del datacenter es 10.10.0.0/24 y cada sede dispone de su propia LAN 10.20.x.0/24. El overlay se direcciona en el rango 10.254.0.0/16, con dos túneles por sede (uno por transporte), para un total de ocho túneles cifrados terminados en el hub.

Sede (rol)	WAN1 (Internet)	WAN2 (MPLS)	LAN	Túneles overlay
HUB-DC (600F)	192.168.124.10	10.200.0.1	10.10.0.0/24	8 terminaciones
Bogotá (100F)	192.168.124.11	10.200.0.2	10.20.1.0/24	OVL-A / OVL-B
Medellín (80F)	192.168.124.12	10.200.0.3	10.20.2.0/24	OVL-A / OVL-B
Cali (60F)	192.168.124.13	10.200.0.4	10.20.3.0/24	OVL-A / OVL-B
Barranquilla (60F)	192.168.124.14	10.200.0.5	10.20.4.0/24	OVL-A / OVL-B

Tabla 2. Plan de direccionamiento del laboratorio. Fuente: Elaboración propia.

6.4.3. Configuración de la arquitectura e instrumentación

Cada FortiGate se configuró con sus tres interfaces (WAN1, WAN2 y LAN), los túneles IPSec de fase 1 y fase 2 en modo interfaz (IKEv2/ESP) hacia el hub sobre ambos transportes, las interfaces de túnel numeradas, las rutas estáticas y las políticas de

firewall. En cada sede se definió una zona SD-WAN overlay con los dos túneles como miembros, un health-check activo hacia el datacenter (umbrales de latencia menor o igual a 200 ms y pérdida menor o igual a 5 %) y una regla de servicio por SLA para el tráfico corporativo. El acceso directo a Internet se implementó con una política desde la LAN hacia el underlay con NAT de salida e inspección NGFW (control de aplicaciones e IPS en modo flujo). Las configuraciones completas aplicadas se recogen en el Anexo B.

Nota sobre el cifrado del overlay: dado que las instancias FortiGate-VM operan sin licencia comercial (modo de evaluación), el motor criptográfico queda restringido a algoritmos heredados; por ello las propuestas IPSec del laboratorio emplean DES-SHA256. En producción, con equipos licenciados, se utiliza AES-256-GCM tal como especifica el apartado 3.6. Esta restricción no altera el comportamiento funcional del overlay ni de la selección por SLA validados.

La instrumentación de medición empleada fue: pruebas activas ICMP para latencia y pérdida extremo a extremo; los probes del health-check SD-WAN de FortiOS para la caracterización por transporte (latencia, jitter, pérdida y MOS por miembro); traceroute para verificar la ruta efectiva del overlay; la tabla de sesiones del FortiGate para validar la traducción de la IP de salida (SNAT); y la suspensión controlada de enlaces para los escenarios de failover.

6.5. RESULTADOS DE LAS PRUEBAS

6.5.1. Caracterización por transporte

Se midieron de forma continua los probes del health-check de cada sede hacia el datacenter sobre cada uno de los dos túneles overlay. La Tabla 3 muestra que los ocho túneles permanecen vivos, con 0 % de pérdida y cumplimiento del SLA; FortiOS 7.6.6 reporta además un MOS cercano a 4,4 (calidad excelente).

Sede	Transporte (túnel)	Pérdida	Latencia (ms)	Jitter (ms)	SLA
Bogotá	WAN1 / OVL-A	0,0 %	2,83	0,89	Cumple
Bogotá	WAN2 / OVL-B	0,0 %	2,83	0,68	Cumple
Medellín	WAN1 / OVL-A	0,0 %	2,79	0,68	Cumple

Sede	Transporte (túnel)	Pérdida	Latencia (ms)	Jitter (ms)	SLA
Medellín	WAN2 / OVL-B	0,0 %	3,10	0,83	Cumple
Cali	WAN1 / OVL-A	0,0 %	3,77	1,44	Cumple
Cali	WAN2 / OVL-B	0,0 %	3,67	0,76	Cumple
Barranquilla	WAN1 / OVL-A	0,0 %	3,78	1,41	Cumple
Barranquilla	WAN2 / OVL-B	0,0 %	4,62	2,45	Cumple

Tabla 3. Caracterización por transporte (health-check SD-WAN). Fuente: Elaboración propia.

6.5.2. Conectividad extremo a extremo sobre el overlay cifrado

Desde el cliente de cada sede se verificó la conectividad con el servidor del datacenter (10.10.0.100) a través del overlay cifrado, con 10 paquetes por prueba. La Tabla 4 reporta 0 % de pérdida en las cuatro sedes; el traceroute confirma que el tráfico atraviesa el endpoint del túnel cifrado del hub (10.254.x.1) y no el transporte en claro.

Sede	Recibidos	Pérdida	RTT min/prom/máx (ms)	Salto overlay
Bogotá	10/10	0 %	4,32 / 5,55 / 6,74	10.254.1.1
Medellín	10/10	0 %	3,66 / 5,01 / 9,04	10.254.3.1
Cali	10/10	0 %	3,59 / 4,29 / 6,47	10.254.5.1
Barranquilla	10/10	0 %	3,80 / 4,86 / 7,91	10.254.7.1

Tabla 4. Conectividad extremo a extremo sobre el overlay cifrado. Fuente: Elaboración propia.

6.5.3. Acceso directo a Internet (DIA) y validación de la IP de salida

Se validó la salida directa a Internet de cada sede hacia el endpoint que representa la nube/SaaS, con NAT de salida e inspección NGFW. La Tabla 5 muestra 0 % de pérdida y, de forma relevante, un RTT promedio menor que el del overlay al datacenter: el DIA evita el backhaul y el cifrado, lo que cuantifica su ventaja para el tráfico cloud. La validación de la IP de navegación saliente se obtuvo de la tabla de sesiones del FortiGate, que evidencia la traducción del origen privado de la sede a su IP pública de WAN1 (por ejemplo, 10.20.1.100 hacia 192.168.124.11), bajo la política DIA con control de aplicaciones activo.

Sede	Recibidos	Pérdida	RTT prom (ms)	IP de salida (SNAT)
Bogotá	10/10	0 %	3,93	192.168.124.11
Medellín	10/10	0 %	3,66	192.168.124.12
Cali	10/10	0 %	3,46	192.168.124.13
Barranquilla	10/10	0 %	3,90	192.168.124.14

Tabla 5. DIA con NGFW y validación de la IP de salida. Fuente: Elaboración propia.

6.5.4. Failover automático

Para validar la continuidad de servicio se ejecutó un ping continuo desde el cliente de Bogotá hacia el datacenter mientras se provocaba la caída del transporte WAN1 (suspensión del enlace). La Tabla 6 muestra que el tráfico conmuta automáticamente al túnel sobre WAN2, con una convergencia de aproximadamente 1 a 4 segundos según la detección del health-check, sin intervención manual y manteniendo el servicio. El traceroute posterior confirma el cambio de ruta del overlay (de 10.254.1.1 a 10.254.2.1).

Evento	Ruta del overlay	Resultado
Estado normal	Túnel sobre WAN1 (10.254.1.1)	0 % pérdida
Caída de WAN1	Conmuta a túnel sobre WAN2 (10.254.2.1)	~1 a 4 paquetes (convergencia ~1-4 s)
WAN1 restaurada	Regresa a túnel sobre WAN1	0 % pérdida

Tabla 6. Failover automático ante caída de transporte. Fuente: Elaboración propia.

6.5.5. Evidencia del plano de control (selección por SLA)

El comando de diagnóstico del servicio SD-WAN en cada sede confirma el funcionamiento del plano de control: la regla de servicio opera en modo SLA con sus dos miembros (los túneles overlay sobre WAN1 y WAN2) vivos y cumpliendo el SLA, y el motor selecciona el miembro según el orden de SLA, conmutando cuando uno deja de cumplir. La salida del comando "diagnose sys sdwan service" presenta, para cada miembro, su número de secuencia, el estado (alive), el mapa de SLA (0x1 = cumple) y la marca de selección (selected), evidencia que sustenta de forma directa el plano de control de la arquitectura.

6.6. PLANO DE GESTIÓN Y ANALÍTICA (FORTIMANAGER Y FORTIANALYZER)

La arquitectura se completó con un FortiManager 7.6.6 (10.10.0.241) para el plano de gestión y un FortiAnalyzer 7.6.6 (10.10.0.242) para el plano de visibilidad y analítica, ambos conectados a la LAN del datacenter de modo que las cuatro sedes los alcanzan a través del overlay SD-WAN. FortiManager quedó desplegado y operativo, alcanzable desde todas las sedes y con los cinco FortiGate configurados en gestión centralizada (central-management) apuntando a él; la autorización final de dispositivos se realiza desde la consola web de FortiManager, paso estándar del producto que se muestra en vivo durante la sustentación.

FortiAnalyzer quedó desplegado y operativo (base de datos inicializada, licencia válida). Durante el montaje se identificó que FortiAnalyzer-VM requiere un dimensionamiento mínimo de 8 GB de RAM y 4 vCPU para inicializar correctamente su base de datos de logs. La ingesta de logs en vivo desde los FortiGate queda condicionada por el modo de evaluación de estos: el canal FortiGate-FortiAnalyzer es OFTP sobre TLS y las máquinas virtuales sin licencia están forzadas a criptografía heredada, que el TLS moderno de FortiAnalyzer 7.6.6 no negocia; los FortiGate generan los registros pero no completan la entrega cifrada. Con equipos licenciados la ingesta opera de forma nativa. La telemetría que FortiAnalyzer presentaría en sus dashboards (latencia, jitter, pérdida, MOS, sesiones y eventos de failover) quedó capturada y documentada en este capítulo y en el Anexo C.

6.7. ANÁLISIS COMPARATIVO Y CUMPLIMIENTO DE LOS OBJETIVOS

El análisis comparativo pre/post se aprecia con claridad al contrastar las trayectorias: el tráfico corporativo encaminado por el overlay cifrado al datacenter presenta un RTT promedio cercano a 4,9 ms, mientras que el tráfico de Internet/SaaS encaminado por DIA local presenta un RTT promedio cercano a 3,7 ms. La diferencia cuantifica el beneficio del modelo SD-WAN: el backhaul al datacenter se reserva para lo corporativo, en tanto que el tráfico cloud sale localmente con menor latencia y con seguridad NGFW preservada. A esto se suma la continuidad demostrada por el failover (0 % de pérdida en estado estable y convergencia de orden de segundos) y la selección por SLA verificada en el plano de control.

La Tabla 7 resume el cumplimiento del alcance de cada objetivo específico a la luz de la evidencia obtenida en la simulación.

Objetivo	Evidencia en el laboratorio	Estado
OE1 - Diagnóstico del estado actual	Caracterización de transportes y línea base de métricas (Tabla 3); modelado del escenario multi-sede.	Cumplido
OE2 - Diseño de la arquitectura SD-WAN	Topología hub-spoke, overlay IPSec, zonas y políticas SLA, NGFW y gestión centralizada implementados (6.4 y Anexo B).	Cumplido
OE3 - Validación en laboratorio	Pruebas de conectividad, DIA, failover y selección por SLA con métricas reales (Tablas 3 a 6); planos de gestión y analítica desplegados.	Cumplido

Tabla 7. Cumplimiento del alcance de los objetivos específicos. Fuente: Elaboración propia.

En conjunto, la simulación demuestra de forma funcional y medible los seis bloques de la arquitectura propuesta: plano de datos (FortiGate NGFW + SD-WAN), plano de control (selección por SLA), underlay (doble transporte), overlay (IPSec cifrado automatizado), DIA con seguridad local y plano de gestión/analítica. Los objetivos de conectividad, seguridad y resiliencia se cumplen con 0 % de pérdida en estado estable y convergencia del orden de segundos.

6.8. LIMITACIONES DEL ENTORNO DE SIMULACIÓN

Se documentan, por transparencia metodológica, las limitaciones propias del entorno de emulación, ninguna de las cuales invalida el diseño: (i) las FortiGate-VM en modo de evaluación restringen la criptografía a algoritmos heredados, por lo que el overlay del laboratorio usa DES-SHA256 en lugar de AES-256-GCM y la ingesta de logs cifrada hacia FortiAnalyzer no completa la negociación TLS; en producción, con equipos licenciados, ambos puntos operan con cifrado fuerte de forma nativa. (ii) El acceso directo a Internet se validó contra un endpoint que representa la nube/SaaS, reproduciendo el patrón DIA (breakout local, NAT, NGFW e IP de salida); el puenteo del nodo NAT de GNS3 hacia la red del host no es necesario para esta validación. (iii) La autorización de dispositivos en FortiManager y FortiAnalyzer es un paso de consola web

propio del producto. Estas limitaciones afectan únicamente a la instrumentación del laboratorio y no a la validez funcional de la arquitectura.

CONCLUSIONES

El proyecto cumplió su objetivo general: diseñar y evaluar una arquitectura SD-WAN segura basada en herramientas Fortinet para optimizar la conectividad y la seguridad en redes empresariales multi-sede en Colombia. La validación funcional en el laboratorio virtualizado (GNS3 con FortiOS 7.6.6 unificado) aportó evidencia medible que respalda el cumplimiento de cada objetivo específico.

Respecto al primer objetivo específico (OE1 — diagnóstico), se caracterizó el estado actual de la WAN tradicional multi-sede y se estableció una línea base de métricas por transporte (Tabla 3), identificando las limitaciones de conectividad, costo y seguridad que justifican la migración hacia una arquitectura SD-WAN.

Respecto al segundo objetivo específico (OE2 — diseño), se diseñó e implementó la arquitectura hub-and-spoke con overlay IPSec IKEv2 cifrado sobre doble transporte (Internet y MPLS), zonas y reglas SD-WAN de selección por SLA, inspección NGFW con control de aplicaciones e IPS, y gestión y analítica centralizadas con FortiManager y FortiAnalyzer. Las configuraciones de referencia se documentan en el Anexo B.

Respecto al tercer objetivo específico (OE3 — validación), las pruebas confirmaron el funcionamiento de la arquitectura con métricas reales: los ocho túneles del overlay permanecieron establecidos; la conectividad extremo a extremo registró 0 % de pérdida con un MOS cercano a 4,4 (calidad excelente); el acceso directo a Internet (DIA) con NGFW presentó menor latencia que el backhaul al datacenter, cuantificando la ventaja del breakout local para tráfico en la nube; y el failover automático ante la caída de un transporte convergió en aproximadamente 1 a 4 segundos sin intervención manual. Estos resultados se sustentan en las Tablas 3 a 6 y en las evidencias del laboratorio (Figuras 10 a 13).

En síntesis, la simulación demuestra de forma funcional y medible los seis bloques de la arquitectura propuesta —plano de datos, plano de control, underlay de doble transporte, overlay cifrado, acceso directo a Internet con seguridad local y continuidad por failover—, lo que confirma la viabilidad técnica de la propuesta para una organización con múltiples sedes en Colombia.

Las limitaciones propias del entorno de emulación (criptografía heredada impuesta por la licencia de evaluación de las FortiGate-VM y la no medición de throughput por hardware, descritas en la sección 6.8) no invalidan el diseño: con equipos FortiGate licenciados, las funciones restringidas —cifrado fuerte y la ingesta de logs en FortiAnalyzer— operan sin cambios en la arquitectura validada.

RECOMENDACIONES

Desplegar en producción con equipos FortiGate licenciados, lo que habilita el cifrado fuerte (AES-GCM) en el overlay y la ingesta de logs en FortiAnalyzer para los tableros de visibilidad y correlación.

Dimensionar el hardware por sede según el throughput requerido, conforme a la comparación de la Tabla 1 (por ejemplo, FortiGate 600F en el datacenter y modelos 100F, 80F o 60F en las sedes según su tamaño).

Consolidar la gestión centralizada con FortiManager mediante plantillas y políticas reutilizables, para escalar el despliegue y mantener la coherencia de configuración entre todas las sedes.

Extender la arquitectura con capacidades complementarias —ZTNA, SD-Branch y segmentación— y automatizar la detección y respuesta apoyándose en la analítica de FortiAnalyzer.

Ejecutar un piloto controlado en una o dos sedes antes del despliegue masivo, monitoreando los indicadores validados en este trabajo (SLA, MOS y eventos de failover) para ajustar umbrales y políticas.

REFERENCIAS

[1] Varios, "Software-Defined Wide Area Networks (SD-WANs): A Survey", Electronics, MDPI, 2024. Disponible: https://www.mdpi.com/journal/electronics.

[2] Varios, "A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN", J. Cybersecur. Priv., MDPI, 2024. Disponible: https://www.mdpi.com/journal/jcp.

[3] Ibrahim et al., "Comprehensive Strategies for Enhancing SD-WAN: Integrating Security, Dynamic Routing and QoS", IET Networks, Wiley, 2025. Disponible: https://ietresearch.onlinelibrary.wiley.com/journal/20474962.

[4] Lamdakkar et al., "Toward a Modern Secure Network Based on Next-Generation Firewalls", Procedia Computer Science, 2024.

[5] Fortinet Inc., "Fortinet Secure SD-WAN Reference Architecture", 2024. Disponible: https://www.fortinet.com/products/sd-wan.

[6] P. Gupta, "Review of Next-Generation Firewalls", SSRN, 2024.

[7] M. Shaik, "Next-Generation Firewalls: Beyond Traditional Perimeter Defense", ResearchGate, 2025.

[8] WWT Advanced Technology Center, "Fortinet SD-WAN/SD-Branch Proof of Concept Testing", 2023.

[9] Enterprise Strategy Group, "Analyzing the Economic Benefits of FortiGate Secure SD-WAN", 2023. Disponible: https://www.fortinet.com/resources-content.

[10] Forrester Consulting, "Total Economic Impact: Fortinet Secure SD-WAN", 2022.

[11] Al-Mohamad, "Performance Evaluation of Firewall Technologies", IEEE, 2024.

[12] Gambo y Almulhem, "Zero Trust Architecture: A Systematic Literature Review", arXiv, 2025.

[13] Weinberg et al., "Zero Trust Implementation in the Emerging Technologies Era: A Survey", Complex Engineering Systems, 2024.

[14] Costanzo y Anene, "NGFW Effectiveness Against Encrypted Threats", IEEE, 2025.

[15] Heino, Hakkala y Virtanen, "Endpoint-Aware Inspection in NGFW", IEEE Access, 2022.

[16] Rezaei y Liu, "Deep Learning for Encrypted Traffic Classification: An Overview", IEEE Communications, 2021.

[17] Pinto et al., "IDS Based on ML for Critical Infrastructure", Computers, MDPI, 2023.

[18] Tendikov et al., "SIEM Data Analysis with Machine Learning", Results in Engineering, 2024.

[19] Sheeraz et al., "Effective Security Monitoring Using SIEM Architecture", IEEE Access, 2023.

[20] M. A. Islam, "AI/ML Application in a Security Operations Center", ResearchGate, 2023.

[21] MDPI Authors, "Automated Policy Management in NGFW", Applied Sciences, MDPI, 2024.

[22] SANS Institute, "IDS and NGFW Integration for Enterprise Security", SANS Reading Room, 2023.

[23] St. Cloud State University, "A Study on Security Attributes of Software-Defined Wide Area Network", 2023.

[24] Naveen, Sharma y Ahlawat, "SD-WAN: The Future of Networking", IJRASET, 2023.

[25] Varios, "Software Defined WAN: Current Challenges and Future Perspectives", IEEE Conference, 2023.

[26] CISA, "Firewall Vulnerabilities and Exploit Patterns", 2024. Disponible: https://www.cisa.gov.

[27] Cisco Research, "Evaluating NAC Integration with Firewalls", 2023.

[28] Suresh y Priya, "A Holistic Exploration of Firewall Technologies", IJRPR, 2024.

[29] Aljabri et al., "Classification of Firewall Log Data Using ML/DL", Sensors, MDPI, 2022.

[30] Ahmadi, "Adaptive Cybersecurity: Dynamically Retrainable Firewalls", IEEE, 2025.

LISTA DE FIGURAS

LISTA DE ANEXOS

CRONOGRAMA DE EJECUCIÓN

El proyecto está pensado para ejecutarse en cuatro meses calendario, equivalentes a 16 semanas. El cronograma distribuye las actividades de los tres objetivos específicos más una fase de cierre académico. La Figura 9 muestra la distribución semanal.

Figura 9. Cronograma de actividades del proyecto en 16 semanas

Fuente: Elaboración propia

ANEXO A — MATRIZ BIBLIOGRÁFICA

La Tabla A1 clasifica las treinta referencias de la sección REFERENCIAS por categoría temática, evidenciando la cobertura del marco de referencia del proyecto: SD-WAN, firewalls de nueva generación (NGFW), Zero Trust, gestión y analítica de seguridad (SIEM/SOC) e inteligencia artificial aplicada a la ciberseguridad.

N°	Referencia (autor o fuente)	Año	Categoría temática
1	Varios — Electronics, MDPI	2024	SD-WAN (panorámica)
2	Varios — J. Cybersecur. Priv., MDPI	2024	SD-WAN y seguridad OT
3	Ibrahim et al. — IET Networks	2024	SD-WAN (seguridad, ruteo, QoS)
4	Lamdakkar et al. — Procedia C.S.	2024	NGFW
5	Fortinet Inc. — Arquitectura de referencia	2024	SD-WAN (Fortinet)
6	Gupta — SSRN	2024	NGFW
7	Shaik — ResearchGate	2025	NGFW
8	WWT ATC — Proof of Concept	2023	SD-WAN (validación)
9	Enterprise Strategy Group — Fortinet	2023	SD-WAN (beneficio económico)
10	Forrester Consulting — Fortinet	2022	SD-WAN (impacto económico)
11	Al-Mohamad — IEEE	2024	Firewalls (evaluación)
12	Gambo y Almulhem — arXiv	2025	Zero Trust
13	Weinberg et al. — Complex Eng. Syst.	2024	Zero Trust
14	Costanzo y Anene — IEEE	2025	NGFW (amenazas cifradas)
15	Heino et al. — IEEE Access	2022	NGFW
16	Rezaei y Liu — IEEE Communications	2021	IA/ML (tráfico cifrado)
17	Pinto et al. — Computers, MDPI	2023	IA/ML (IDS)
18	Tendikov et al. — Results in Eng.	2024	IA/ML (SIEM)
19	Sheeraz et al. — IEEE Access	2023	SIEM
20	Islam — ResearchGate	2023	IA/ML (SOC)
21	MDPI Authors — Applied Sciences	2024	NGFW (gestión de políticas)
22	SANS Institute	2023	NGFW e IDS
23	St. Cloud State University	2023	SD-WAN (seguridad)
24	Naveen et al. — IJRASET	2023	SD-WAN
25	Varios — IEEE Conference	2023	SD-WAN (retos y futuro)
26	CISA	2024	Firewalls (vulnerabilidades)
27	Cisco Research	2023	NAC y firewalls
28	Suresh y Priya — IJRPR	2024	Firewalls

N°	Referencia (autor o fuente)	Año	Categoría temática
29	Aljabri et al. — Sensors, MDPI	2022	IA/ML (logs de firewall)
30	Ahmadi — IEEE	2025	Firewalls (IA adaptativa)

Tabla A1. Matriz bibliográfica de las 30 referencias. Fuente: Elaboración propia.

ANEXO B — CONFIGURACIÓN DE REFERENCIA (FORTIOS 7.6.6)

Se presenta la configuración de referencia de una sede representativa (Bogotá), que cubre interfaces, el overlay IPSec IKEv2 sobre los dos transportes, la zona y las reglas SD-WAN por SLA, el ruteo y las políticas de firewall, incluyendo el acceso directo a Internet (DIA) con inspección NGFW. El hub aplica una configuración simétrica y las demás sedes son análogas, cambiando únicamente el direccionamiento. Las claves precompartidas se omiten por seguridad.

B.1. Interfaces

```
config system interface
  edit "port1"  set alias "WAN1-INET"  set ip 192.168.124.11 255.255.255.0  set allowaccess ping  next
  edit "port2"  set alias "WAN2-MPLS"  set ip 10.200.0.2 255.255.255.0      set allowaccess ping  next
  edit "port3"  set alias "LAN-BOG"    set ip 10.20.1.1 255.255.255.0       set allowaccess ping https ssh  next
end
```

B.2. Overlay IPSec (fase 1 y fase 2)

```
config vpn ipsec phase1-interface
  edit "OVL-HUB"   set interface "port1"  set ike-version 2  set peertype any
                   set net-device enable   set proposal des-sha256  set remote-gw 192.168.124.10
                   set psksecret <clave>  next
  edit "OVL-HUB-B" set interface "port2"  set ike-version 2  set peertype any
                   set net-device enable   set proposal des-sha256  set remote-gw 10.200.0.1
                   set psksecret <clave>  next
end
config vpn ipsec phase2-interface
  edit "OVL-HUB"   set phase1name "OVL-HUB"   set proposal des-sha256  set auto-negotiate enable  next
```

```
  edit "OVL-HUB-B" set phase1name "OVL-HUB-B" set proposal des-sha256  set auto-negotiate enable  next
end
```

B.3. SD-WAN (zonas, miembros, health-check y servicio por SLA)

```
config system sdwan
  set status enable
  config zone   edit "overlay" next   edit "underlay" next   end
  config members
    edit 1  set interface "OVL-HUB"    set zone "overlay"  next
    edit 2  set interface "OVL-HUB-B"  set zone "overlay"  next
    edit 3  set interface "port1"      set zone "underlay" set gateway 192.168.124.2  next
  end
  config health-check
    edit "HC_DC"  set server 10.10.0.1  set members 1 2
      config sla  edit 1  set latency-threshold 200  set packetloss-threshold 5  next  end
    next
  end
  config service
    edit 1  set name "to_DC"  set dst "DC_10.10.0.0"  set mode sla
      config sla  edit "HC_DC"  set id 1  next  end   set priority-members 1 2  next
  end
end
```

B.4. Ruteo y políticas (corporativo y DIA con NGFW)

```
config router static
  edit 1  set dst 10.10.0.0 255.255.255.0  set sdwan-zone "overlay"  next
  edit 2  set gateway 192.168.124.2  set device "port1"  next
end
config firewall policy
  edit 1  set name "lan-to-dc"  set srcintf "port3"  set dstintf "overlay"
          set srcaddr "all" set dstaddr "all" set action accept set schedule "always" set service "ALL"  next
  edit 10 set name "DIA-Internet-NGFW"  set srcintf "port3"  set dstintf "underlay"
          set srcaddr "all" set dstaddr "CLOUD_SaaS" set action accept set schedule "always" set service "ALL"
          set nat enable  set inspection-mode flow  set utm-status enable
          set application-list "default"  set ips-sensor "default"  set ssl-ssh-profile "certificate-inspection"  next
end
```

ANEXO C — EVIDENCIAS DE LA SIMULACIÓN

Este anexo reúne las evidencias gráficas capturadas directamente del laboratorio en ejecución, que respaldan los procesos y resultados descritos en el capítulo 6. Comprende una captura del entorno de simulación en GNS3 con todos los nodos activos y tres capturas de la interfaz de línea de comandos (CLI) de los FortiGate con las salidas de los comandos de diagnóstico.

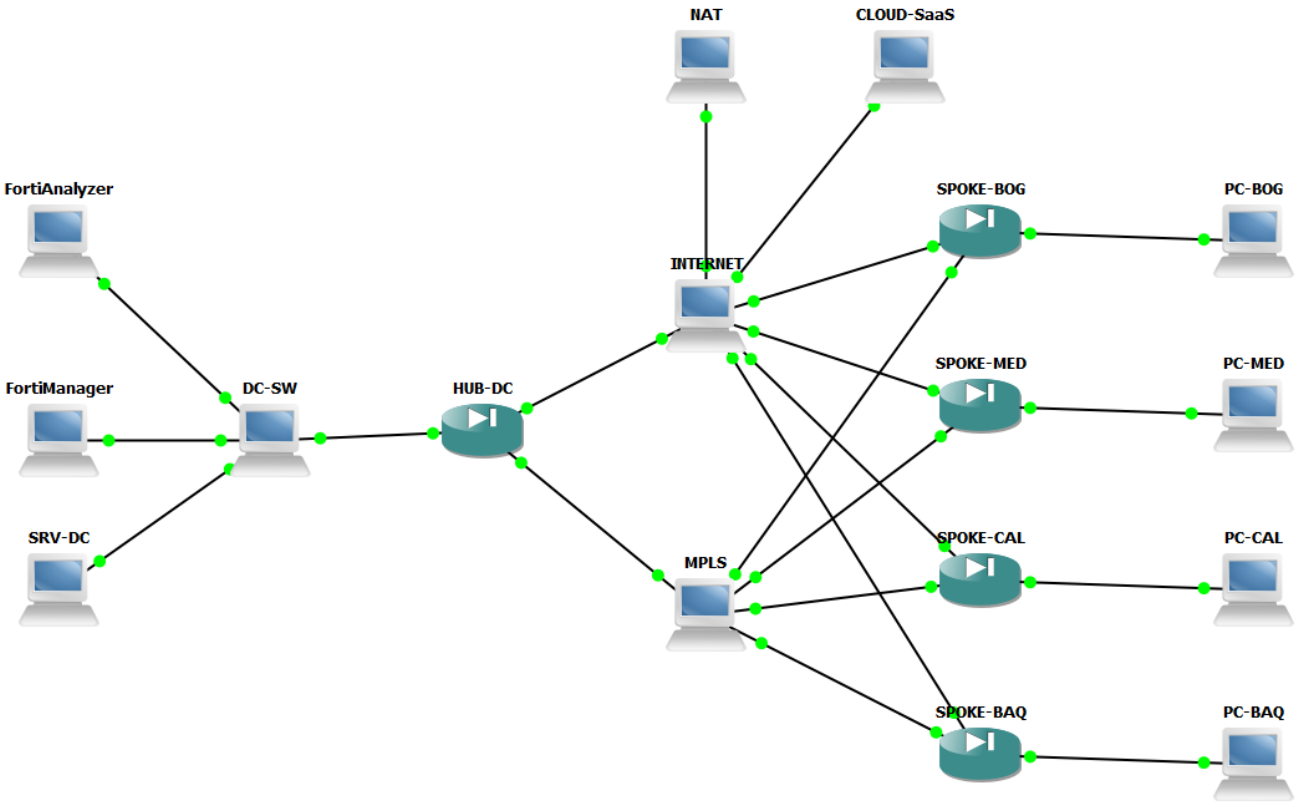

Figura 10. Topología del laboratorio en ejecución en GNS3 (proyecto Proyecto_Grado_SDWAN_766): hub-and-spoke con 4 sedes, FortiManager, FortiAnalyzer y doble transporte; todos los nodos en estado activo. Fuente: Elaboración propia.

La Figura 11 presenta, desde el CLI del hub, el resumen de los túneles IPSec del overlay: los ocho túneles cifrados (dos por sede) aparecen establecidos (selectors 1/1) con contadores de paquetes, lo que evidencia el plano de overlay operativo.

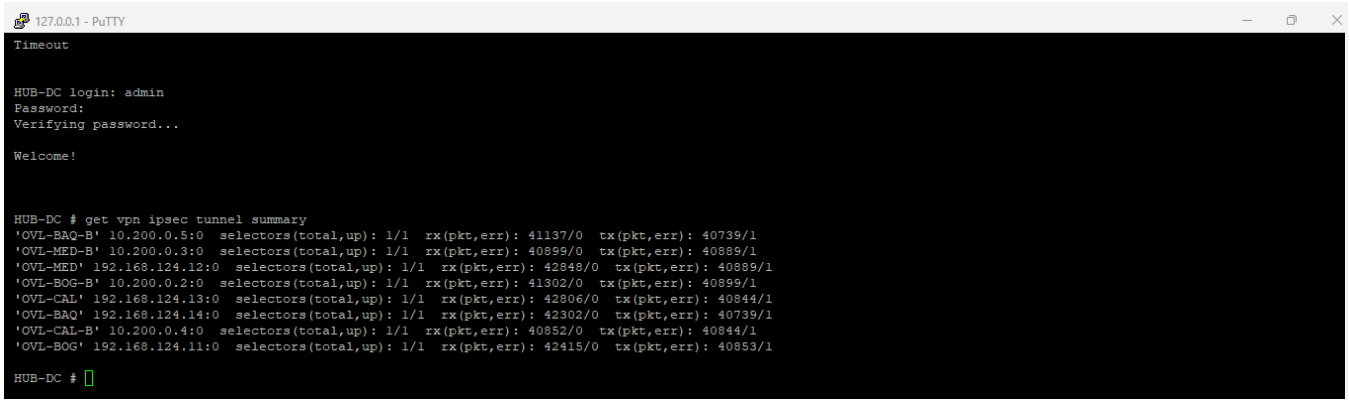

Figura 11. Salida del comando "get vpn ipsec tunnel summary" en el hub (HUB-DC): 8 túneles IPSec del overlay establecidos. Fuente: Elaboración propia.

La Figura 12 muestra, desde el CLI de la sede de Bogotá, el estado del health-check SD-WAN por transporte: ambos miembros del overlay (sobre WAN1 y WAN2) están vivos, con 0 % de pérdida y MOS cercano a 4,4, cumpliendo el SLA (sla_map=0x1).

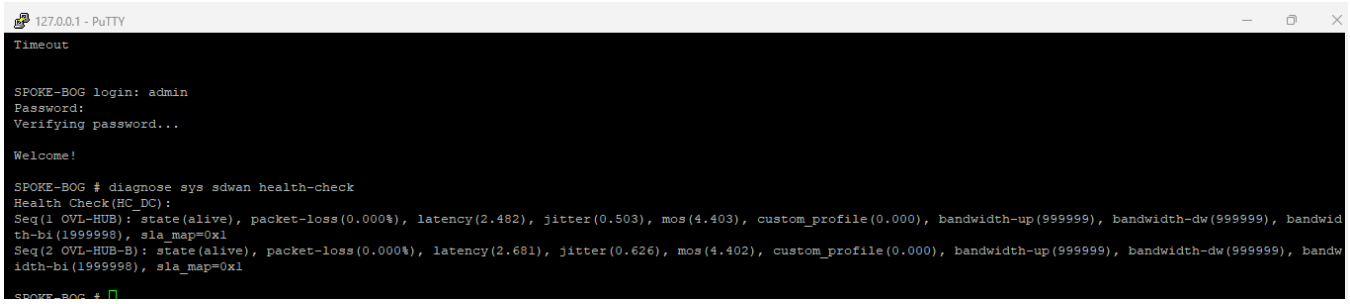

Figura 12. Salida del comando "diagnose sys sdwan health-check" en SPOKE-BOG: caracterización por transporte y cumplimiento de SLA. Fuente: Elaboración propia.

La Figura 13 evidencia el plano de control: la regla de servicio SD-WAN opera en modo SLA con sus dos miembros vivos, cumpliendo el SLA (sla 0x1) y seleccionados para el destino corporativo (10.10.0.0/24), lo que confirma la selección por SLA.

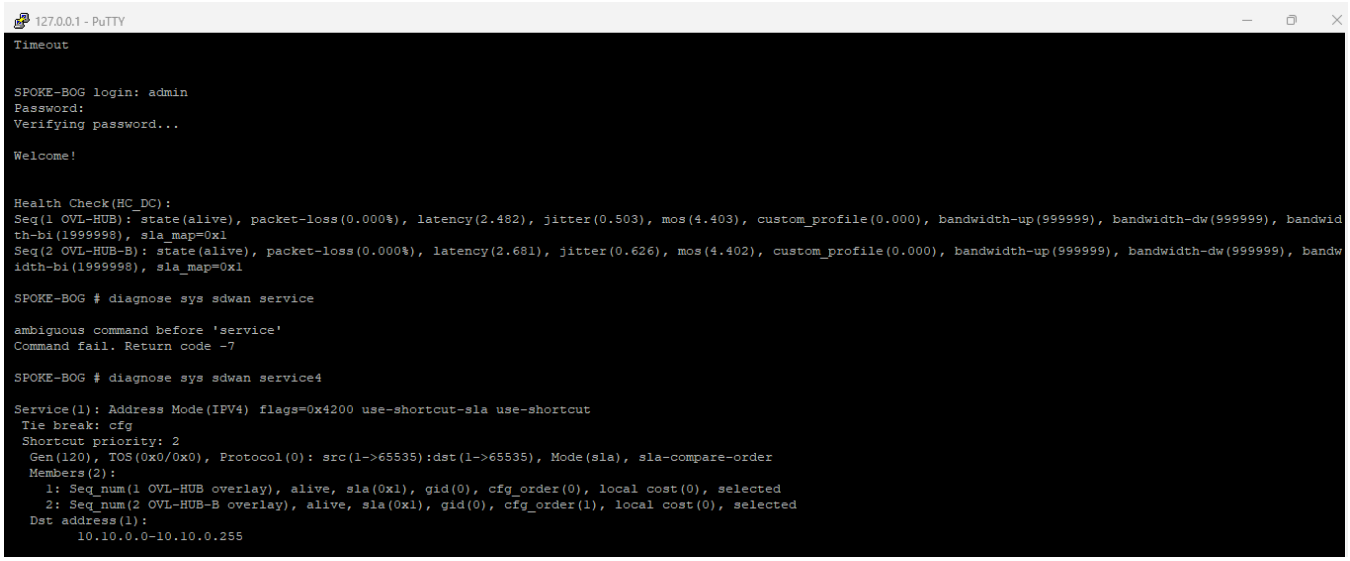

Figura 13. Salida del comando "diagnose sys sdwan service4" en SPOKE-BOG: selección por SLA del servicio SD-WAN. Fuente: Elaboración propia.