UNIVERSIDAD DEL AZUAY

Departamento de Posgrados

Implementación de SD-WAN en una agencia de la Cooperativa de Ahorro y Crédito Jardín Azuayo LTDA

Maestría en Telecomunicaciones

Autor:

Danny Marcelo Velásquez Ortega

Director:

César Andrés Cárdenas Neira

Cuenca, Ecuador 2023

DEDICATORIA

Con mucho amor a mi esposa Pame, por ser mi compañera y amiga durante este camino.

A mis amados hijos, Joaquín y Benja, mi inspiración en todo lo que realizo.

A mis queridos padres Marcelo y Eli, por el apoyo que siempre me brindan.

AGRADECIMENTO

A los docentes de la Maestría en Telecomunicaciones de la Universidad del Azuay, que compartieron sus conocimientos y experiencias mi profundo agradecimiento, de manera especial al Ing. Andrés Cárdenas Mgr, Ing. Daniel Iturralde Ph.D y al Ing. Jaime Burbano Mgr, por todo el apoyo brindado.

A la Cooperativa de Ahorro y Crédito Jardín Azuayo y sus autoridades, mi profundo agradecimiento por el apoyo económico brindado y las facilidades para poder implementar el proyecto planteado.

Implementación de SD-WAN en una Agencia de la Cooperativa de Ahorro y Crédito Jardín Azuayo LTDA

Resumen.

La Cooperativa Jardín Azuayo, se dedica a prestar servicios de ahorro y crédito a sus socios, a través de puntos de atención físicos y virtuales. Debido a su crecimiento, la arquitectura de red tradicional mediante la interconexión de enlaces MPLS, se ha vuelto compleja y costosa. El disponer de procesos manuales en la configuración, ha complicado la disponibilidad y convergencia de la red cuando se requiere aplicar despliegue de políticas. Adicional a esto, con la

arquitectura actual de enlaces en modo Activo – Pasivo en cada agencia, la convergencia de la red no se realiza de forma rápida. En el presente proyecto, se propone una guía detallada de los procedimientos realizados para la implementación de la tecnología SD-WAN, que mejora las técnicas de interconectar las WAN tradicionales, eliminando la necesidad de contratar enlaces MPLS costosos para la interconexión entre Data Centers y oficinas para establecer comunicación y redundancia de red de una agencia. Por lo tanto, adicional al ahorro mensual que obtendrá la Cooperativa, se simplificarán los procesos de enrutamiento manual por una administración centralizada para aplicación de políticas de forma dinámica, permitiendo monitorizar y administrar eficientemente la red.

Palabras Claves: SD-WAN, Cooperativa de Ahorro y Crédito Jardín Azuayo.

Implementation of SD-WAN in an Agency of the Jardín Azuayo LTDA Savings and Credit Cooperative

Abstract.

The "Cooperativa Jardin Azuayo" is dedicated to provide saving and credit services to its members in both physical and virtual places. Due to its growing the arquitechture of traditional network through the MPLS link interconnection it has become complex and expensive. Also, the utilization of manual processes in its configuration has complicated the availability and converge of the network when it is required to apply policy enforcement. Additionally, with the current architecture of active-passive mode links in each agency, the converge of the network is not done quickly. In the present project, a detailed guide of the procedures for the implementation of SD-WAN technology is proposed, which improves the technique to interconnect the traditional WAN by discarding the need to hire expensive MPLS links for the interconnection between the Data Center and the offices to establish communication and network redundancy of one agency. Thus, besides the monthly saving that the Cooperativa will obtain, the manual routing processes will be simplified by a centralized management to apply dynamical policies allowing to monitor and manage the network in an efficient way.

Keywords: SD-WAN, Cooperativa de Ahorro y Crédito Jardín Azuayo.

Translated by: Danny Marcelo Velásquez Ortega

Implementación de SD-WAN en una Agencia de la Cooperativa de Ahorro y Crédito Jardín Azuayo LTDA

Danny M. Velásquez O.
Maestría en Telecomunicaciones
Universidad del Azuay
Cuenca, Ecuador
dvelasquez@es.uazuay.edu.ec

***Abstract*—La Cooperativa Jardín Azuayo, se dedica a prestar servicios de ahorro y crédito a sus socios, a través de puntos de atención físicos y virtuales. Debido a su crecimiento, la arquitectura de red tradicional mediante la interconexión de enlaces MPLS, se ha vuelto compleja y costosa. El disponer de procesos manuales en la configuración, ha complicado la disponibilidad y convergencia de la red cuando se requiere aplicar despliegue de políticas. Adicional a esto, con la arquitectura actual de enlaces en modo Activo – Pasivo en cada agencia, la convergencia de la red no se realiza de forma rápida. En el presente proyecto, se propone una guía detallada de los procedimientos realizados para la implementación de la tecnología SD-WAN, que mejora las técnicas de interconectar las WAN tradicionales, eliminando la necesidad de contratar enlaces MPLS costosos para la interconexión entre Data Centers y oficinas para establecer comunicación y redundancia de red de una agencia. Por lo tanto, adicional al ahorro mensual que obtendrá la Cooperativa, se simplificarán los procesos de enrutamiento manual por una administración centralizada para aplicación de políticas de forma dinámica, permitiendo monitorizar y administrar eficientemente la red.**

***Index Terms*—SD-WAN, Cooperativa de Ahorro y Crédito Jardín Azuayo.**

I. INTRODUCCIÓN

Debido al gran desarrollo tecnológico que se ha dado en los últimos años, las empresas se han visto obligadas a implementar estrategias que permitan su transformación digital, con la incorporación de nuevas tecnologías que les permita mayores oportunidades de negocio en las diferentes áreas del mercado y reducir costes, con el objetivo de lograr mayor competitividad y una mejor experiencia a sus usuarios o clientes sobre los diferentes servicios, siendo esta la principal motivación para la implementación del presente proyecto en la Cooperativa de Ahorro y Crédito Jardín Azuayo LTDA.

El proyecto se enfoca en el cambio de generación que han tomado las diferentes arquitecturas de red que se implementan a nivel global, y en específico en las entidades financieras, Existen varios datos estadísticos de encuestas realizadas a nivel global que muestran la tendencia de la tecnología SD-WAN en ser implementada, dado que facilita diferentes soluciones como la digitalización para las empresas. De acuerdo con datos de "Statista", luego de una encuesta realizada en el año 2016 por Global Insights Pulse de KPMG, el sector de instituciones financieras y seguros, son las empresas que muestran mayor interés en la inversión en digitalización de sus procesos como se observa en la Fig. 1 [1].

Fig. 1. Sectores más orientados a la digitalización [1].

La topología de red tradicional no es capaz de satisfacer las necesidades que están basadas en otros servicios como: Multi-Cloud o SaaS (Software as a Service) que permiten una correcta implementación de la digitalización en las empresas. De acuerdo con "Gartner" en pocos años las Redes WAN Definidas por Software (SD-WAN) reemplazarán la estructura de WAN tradicional y pronostica que los gastos en servicios SD-WAN crecerán a una tasa anual del 84,7% [2]. Esto se puede observar en la Fig 2.

Las soluciones de Redes WAN Definidas por Software (SD-WAN), proporcionan un reemplazo para los enrutadores WAN con arquitectura de red tradicional y son independientes de las tecnologías de transporte WAN (MPLS, Internet, LTE, entre otras). Por lo tanto, proporciona una selección de rutas de aplicación dinámica y basada en políticas a través de múltiples conexiones WAN, logrando la optimización de enlaces, balanceo de carga, mayor disponibilidad de la red, entre otros beneficios.

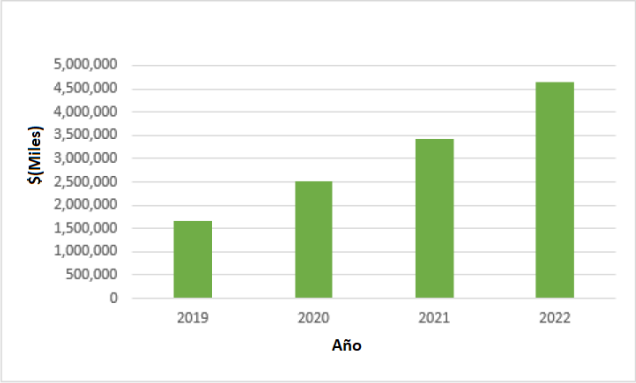

Fig. 2. Tendencias de crecimiento de SD-WAN [2].

Los siguientes datos obtenidos mediante una encuesta realizada por "Statistics", muestran las motivaciones principales de las organizaciones de todo el mundo para la implementación de SD-WAN, por ende con el 58%, la mayoría de los encuestados indican que los beneficios económicos son la motivación principal para la implementación de esta tecnología, seguido por la continuidad del negocio con un 50% y también otras características importantes como visibilidad de la red, mejor rendimiento de red, aplicaciones basadas en la nube y arquitectura centralizada, (Fig. 3) [3].

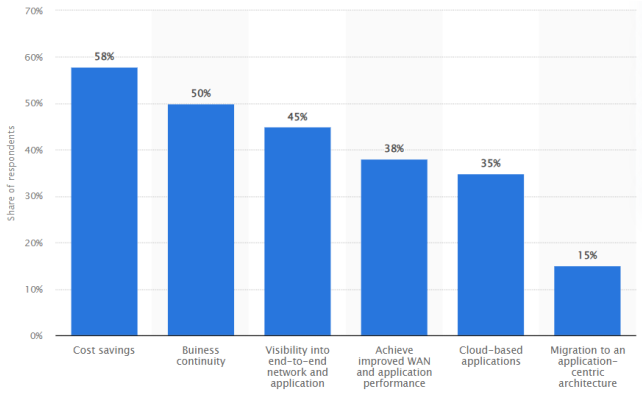

Fig. 3. Motivaciones para la implementación de SD-WAN [3].

La implementación de SD-WAN en la Cooperativa Jardín Azuayo, permitirá agilizar el camino hacia la transformación digital de la institución y fomentar el uso de canales virtuales en los diferentes puntos de atención, con una topología de red que permitirá mejorar la disponibilidad, estabilidad, gestión de la red y reducción de costes de los enlaces de transporte.

En [4] se analiza la arquitectura, funciones y beneficios de una red SD-WAN, se revisa la administración centralizada de redes WAN, y su relación con la nube y la importancia de la seguridad, para que finalmente los administradores puedan gestionar las redes de manera independiente del proveedor que les brinde conectividad desde los puntos remotos.

En [5] se revisa los avances de las redes SD-WAN en base a la antigua red tradicional, la arquitectura de la red SD- WAN y se analiza los avances representativos en cada capa de la red SD-WAN, finalmente se examina las oportunidades y los desafíos que presentan las nuevas técnicas y protocolos de red.

En [6] se realiza una descripción de SD-WAN y la importancia del balanceo de carga. Considerando que el balanceo de carga es una técnica de red tradicional que se usa comúnmente en los centros de datos, mientras que la WAN definida por software es una tecnología más nueva que puede utilizar las mismas capacidades de balanceo de carga para las conexiones WAN, pero de manera automatizada.

En [7] se realiza un estudio técnico económico de una implementación con arquitectura SD-WAN, mediante un caso de estudio para una empresa que dispone de Cajeros Automáticos (ATM) con un solo enlace de conexión del Tipo satelital, Very Small Aperture Terminal (VSAT). Por lo tanto, se examina el problema de la disponibilidad con un solo enlace y se propone la implementación de SD-WAN colocando un enlace de internet de banda ancha redundante con tecnología 4G/LTE, con lo cual el tráfico se direccionará automáticamente si una de las dos conexiones no funciona.

En [8] para considerar los beneficios del uso de una arquitectura de red SD-WAN, se realiza una comparativa entre la arquitectura de red tradicional con tecnología IP/MPLS, versus el uso del controlador SDN para administrar el tráfico en enlaces WAN, con el objetivo de utilizar en ambos escenarios la ruta óptima para una red específica.

En [9] considerando que en la red el aumento de tráfico multimedia sensible al ancho de banda cada vez es mayor, se establecen una serie de medidas de gestión de calidad para satisfacer las necesidades de transmisión y entrega eficientes en entornos limitados de red. Además, se introduce una técnica denominada la calidad de la experiencia QoE para lograr los objetivos de eficiencia en las aplicaciones y satisfacción del servicio desde la perspectiva del usuario final. Finalmente, el autor propone un marco que toma la retroalimentación de QoE en tiempo real y reenvía a los controladores SD-WAN para mejorar las rutas de transmisión.

En [10] se realiza la descripción detallada de una implementación de SD-WAN, utilizando diferentes proveedores de servicios de internet (ISP), se implementan configuraciones sobre una tecnología en particular y se evidencia los beneficios de esta tecnología aplicada, mediante la realización de pruebas de funcionamiento con distinto tipo de tráfico de video, voz y datos.

En [11] debido al gran crecimiento que ha tenido la aplicación de la tecnología SD-WAN en las empresas, se realiza un análisis de las amenazas y vulnerabilidades que se presentan en esta solución, cómo responder a estas y al final se verifica que la solución que ofrece la tecnología Fortinet (Fortigate), brinda mejores mecanismos de seguridad, sobre todo enfocados en la integridad, confidencialidad y seguridad.

II. MARCO TEÓRICO

Las redes de área amplia definidas por software (SD-WAN), parten del concepto de las redes definidas por software (SDN), que presentan un enfoque diferente a la forma tradicional de

administrar y operar una red, ya que a diferencia de éstas, separa los planos de datos y control, que permite simplificar y automatizar la administración de la red, como se observa en la Fig. 4 [9].

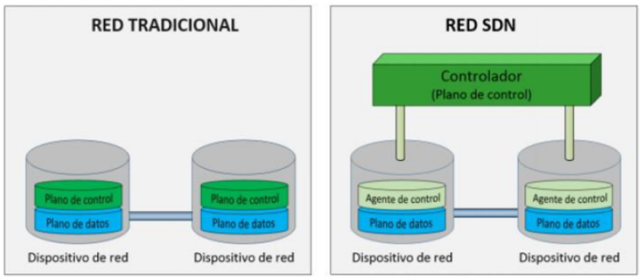

Fig. 4. Redes Tradicionales Vs Redes SDN [9].

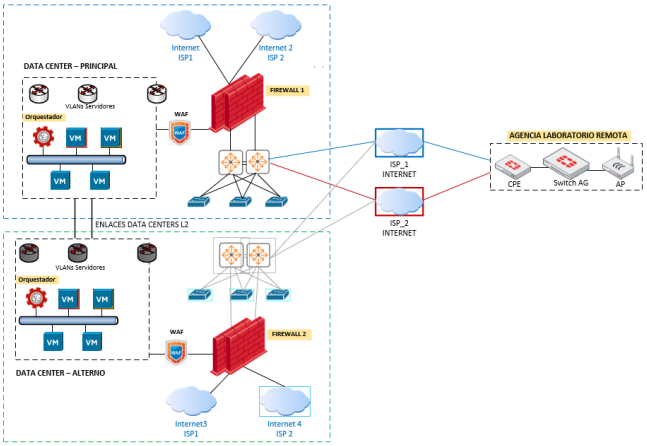

Fig. 5. Arquitectura SD-WAN para la Cooperativa Jardín Azuayo.

En la topología tradicional, cada dispositivo enrutador dispone de un plano de control independiente de su ubicación, es decir, cualquier función que ejecute solo intervendrá en ese dispositivo. A diferencia, en las redes definidas por software (SDN), se dispone de un agente de control que intervine en todos los dispositivos conectados, que definirá las reglas que deben ejecutar los dispositivos (enrutadores) conectados en la red, con esta estructura, se logra automatizar procesos manuales de configuración, que anteriormente no eran posibles en las redes tradicionales.

Las redes de área amplia definidas por software (SD-WAN), extienden los conceptos de las redes definidas por software (SDN) hacia la WAN (Wide Area Network), lo que permite al administrador, disponer del control y gestión centralizada de la red, por medio de la selección dinámica de rutas, por diversos medios de transporte (Internet, MPLS, LTE, entre otros), con lo que se logra centralizar y automatizar la administración de la red, mejorar su rendimiento, reducir el costo operativo y mejorar la escalabilidad.

La arquitectura SD-WAN propuesta para implementar en la Cooperativa de Ahorro y Crédito Jardín Azuayo (Fig. 5), está compuesta de los siguientes componentes, con su respectiva función:

a) El orquestador: cumple con la función de plataforma para la administración centralizada, gestión y control de la red WAN definida por software (SD-WAN), este componente de software se instaló en el centro de datos, en una máquina virtual, para poder gestionar desde aquí la red de manera sencilla e inteligente, mediante el despliegue de políticas para el control de tráfico de la red WAN, reduciendo considerablemente los tiempos de operación.

b) Firewall: este componente físico está ubicado en los centros de datos principal y alterno con capacidad de implementar SD-WAN dentro de su software, por lo tanto, cumplen con la función de ser los concentradores y generadores de los diferentes túneles VPN (Red Privada Virtual) IPSec (Seguridad del Protocolo de Internet) que se requirió para establecer la comunicación entre los centros de datos y los puntos remotos (Agencia Laboratorio), brindado las capacidades de seguridad y encriptación de los datos que viajan por los diferentes canales de transporte de los dos proveedores de Internet (ISP) que se contrataron para este proyecto.

c) Equipos remotos: son los equipos físicos, también con funciones de firewall que se instalaron en la agencia de laboratorio. Estos dispositivos se conectan con el firewall del centro de datos principal mediante túneles VPN (Red Privada Virtual) IPSec (Seguridad del Protocolo de Internet). En estos, también se puede aplicar políticas de seguridad que permite enrutar de manera segura el tráfico generado en la agencia, a través del medio de transporte (internet) que será instalado por dos proveedores de este servicio (ISP).

Con esta estructura, mediante el orquestador de la red SD-WAN (Red Amplia Definida por Software); se logró la configuración de políticas de enrutamiento, selección de rutas para los diferentes servicios, evaluando la calidad de los enlaces de transporte, balanceo de tráfico por dos los enlaces, aplicar políticas de calidad de servicio (QoS), mejorar la disponibilidad de la red y reducir los costos de operación de la red tradicional que actualmente funciona con enlaces MPLS costosos.

III. DESCRIPCIÓN DEL SISTEMA

Para la implementación de la arquitectura SD-WAN en la Cooperativa de Ahorro y Crédito Jardín Azuayo, se siguieron los siguientes lineamientos, hasta obtener los resultados esperados:

a) Definiciones iniciales.

Una vez definida la topología de red a implementar, se considera que la institución ya dispone de dos Firewall Fortinet (Fortigate) en los centros de datos, principal y alterno, y para su administración, se dispone también del software Fortimanager (orquestador), el cual se encuentra instalado en una máquina virtual en cada centro de datos, considerando que estos equipos ya vienen con el módulo para poder establecer SD-WAN en su software.

Con esa consideración, se planteó la adquisición de equipos de la misma tecnología (Fortigate, Fortiswitch, FortiAP) para

los puntos remotos, que permitan aplicar la topología SD-WAN para la Oficina Laboratorio. Por lo tanto, los Firewalls de los centros de datos permitieron habilitar las características SD-WAN y establecer la interconexión a la Oficina laboratorio remota, por medio de dos enlaces de internet corporativo, considerando la asignación a cada enlace de internet, las IPs públicas estáticas necesarias por parte de los proveedores (ISP) para la administración y posterior configuración.

Para lograr tal interconexión, se contratan también dos enlaces con proveedores diferentes de internet corporativo con IPs públicas asignadas en los dos Centros de Datos, los cuales funcionaron como concentradores de túneles VPN (Virtual Private Network) de esta solución. El direccionamiento que se definió tanto para la oficina y los Centros de Datos Principal y Alterno se puede observar en la Figura. 6.

DIRECCIONAMIENTO IP PROVEEDORES DE INTERNET				
ISP	RED	GATEWAY	IP ASIGNADA	
ISP 1 TELCO	157.100.X.X/30	157.100.X.X	157.100.X.X	OFICINA LABORATORIO
ISP 2 PUNTO	190.57.X.X/30	190.57.X.X	190.57.X.X	
ISP 1 TELCO	157.100.X.X/32	157.100.X.X	157.100.X.X	DATA CENTER PRINCIPAL
ISP 2 PUNTO	179.49.X.X/32	179.49.X.X	179.49.X.X	
ISP 1 TELCO	157.100.X.X/32	157.100.X.X	157.100.X.X	DATA CENTER ALTERNO
ISP 2 PUNTO	190.57.X.X	190.57.X.X	190.57.X.X	
LOOPBACK	10.250.X.X/16	...	....	

Fig. 6. Direccionamiento de Proveedores de Servicios de Internet ISP.

b) Definición de las subredes de la oficina laboratorio.

A continuación, se realiza la división de subredes, direccionamiento IP y la VLAN (Virtual Local Area Network) correspondiente a cada interfaz y servicio que se configuró en los equipos de red de la Oficina - Laboratorio (Fig. 7). Como se observa, la red principal está dividida en varios segmentos de red definidos, que posteriormente se configuró en cada dispositivo que opera en la oficina laboratorio, ya sea de red o usuario final.

DIRECCIONAMIENTO IP - OFICINA LABORATORIO						
SUBRED	AREA	DISPOSITIVO	DIRECCION IP	MASCARA	GATEWAY	VLAN
172.22.X.X/29	ADMINISTRACION	FORTIGATE	172.22.X.X	255.255.255.248		10
		FORTISWITCH DATOS 1	172.22.X.X	255.255.255.248	172.22.X.X	10
		GESTION REDES	172.22.X.X	255.255.255.248	172.22.X.X	10
172.22.X.X/29	FORTIAP	GATEWAY FORTIAP	172.22.X.X	255.255.255.248	172.22.X.X	15
		FORTIAP 1	172.22.X.X	255.255.255.248	172.22.X.X	15
172.22.X.X/29	GESTION WIFI	GATEWAY GESTION WIFI	172.22.X.X	255.255.255.248		19
		EQUIPO PORTATIL	172.22.X.X	255.255.255.248	172.22.X.X	19
172.22.X.X/29	GESTION BACKUP	GATEWAY GESTION WIFI	172.22.X.X	255.255.255.248	172.22.X.X	20
		EQUIPO PORTATIL	172.22.X.X	255.255.255.248	172.22.X.X	20
172.22.X.X/28	CAJAS	GATEWAY CAJAS	172.22.X.X	255.255.255.240		21
		CAJA 1	172.22.X.X	255.255.255.240	172.22.X.X	21
		CAJA 2	172.22.X.X	255.255.255.240	172.22.X.X	21
		CAJA 3	172.22.X.X	255.255.255.240	172.22.X.X	21
172.22.X.X/28	ASESORES Y COWORKING WIFI	GATEWAY ASESOR	172.22.X.X	255.255.255.240	172.22.X.X	22
		ASESOR 1	172.22.X.X	255.255.255.240	172.22.X.X	22
		ASESOR 2	172.22.X.X	255.255.255.240	172.22.X.X	22
		COWORKING 1	172.22.X.X	255.255.255.240	172.22.X.X	22
		COWORKING 2	172.22.X.X	255.255.255.240	172.22.X.X	22
172.22.X.X/28	ASESORES BACKUP	GATEWAY ASESOR	172.22.X.X	255.255.255.240		23
		ASESOR 1	172.22.X.X	255.255.255.240	172.22.X.X	23
		ASESOR 2	172.22.X.X	255.255.255.240	172.22.X.X	23
		COWORKING 1	172.22.X.X	255.255.255.240	172.22.X.X	23
		COWORKING 2	172.22.X.X	255.255.255.240	172.22.X.X	23
172.22.X.X/28	IMPRESORAS	GATEWAY IMPRESORA	172.22.X.X	255.255.255.240		24
		IMPRESORA 1	172.22.X.X	255.255.255.240	172.22.X.X	24
		IMPRESORA 2	172.22.X.X	255.255.255.240	172.22.X.X	24
		IMPRESORA 3	172.22.X.X	255.255.255.240	172.22.X.X	24

Fig. 7. Direccionamiento IP para Oficina - Laboratorio.

c) Configuración de equipos

El equipo de red (enrutador) que se instaló en la oficina laboratorio, es un equipo de la marca Fortinet, modelo FG-40F, este dispositivo además de cumplir con enrutamiento viene con funcionalidades de Firewall como parte de su software, el cual se activó mediante un licenciamiento denominado licencia BDL-950-36, que se adquirió como un producto adicional al dispositivo físico. Este licenciamiento permitió activar las capacidades de firewall de este dispositivo (Fig. 8). Para la conexión de los dispositivos de red de usuario final, se instaló un dispositivo switch de la misma marca, denominado como Fortiswitch que sirve para conectar los diferentes puntos de red de la oficina. Además, se consideró un dispositivo Punto de Acceso inalámbrico, denominado FortiAP, para los espacios físicos en donde se requiere este tipo de conexión inalámbrica, para darle un característica de movilidad a los equipos de cómputo de los usuarios de la oficina.

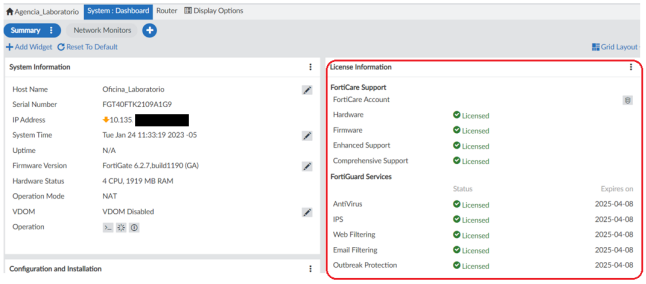

Fig. 8. Activación de Licenciamiento en equipo de red - Oficina Laboratorio.

Posterior a la activación de la licencia del dispositivo Fortigate, se procedió con la configuración del direccionamiento IP (Internet Protocol) de las dos interfaces físicas, etiquetadas como LAN 1 (Interfaz 1) y LAN 2 (Interfaz 2) que se utilizaron en la agencia, para dar salida directa a internet con cada una de las conexiones de los proveedores (Fig 9).

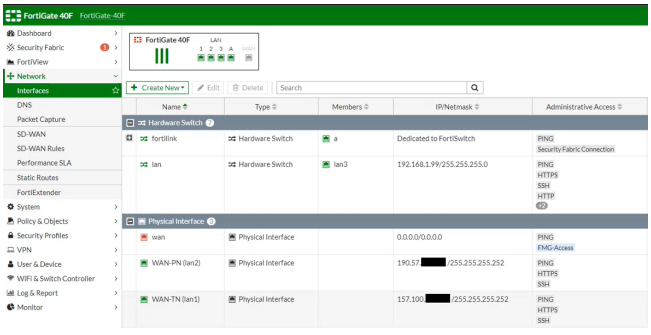

Fig. 9. Configuración de interfaces con cada proveedor de internet.

Es importante la configuración de una interfaz Loopback, se trata de una interfáz lógica interna del router, la cuál es de gran utilidad para administrar el dispositivo, ya que se garantiza siempre, que al menos una interface esté disponible para el acceso y administración remota. (Fig. 10).

Se procedió con la configuración de las VLAN (Virtual Local Area Network) que tiene la agencia laboratorio. De acuerdo con la Fig 7, se generó y se asignó el direccionamiento IP correspondiente. A continuación se observa la configuración realizada (Fig 11).

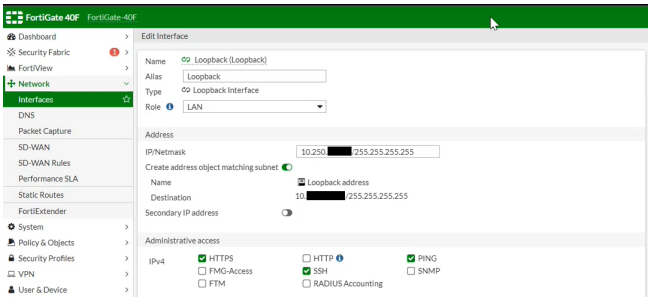

Fig. 10. Configuración de interfáz Loopback.

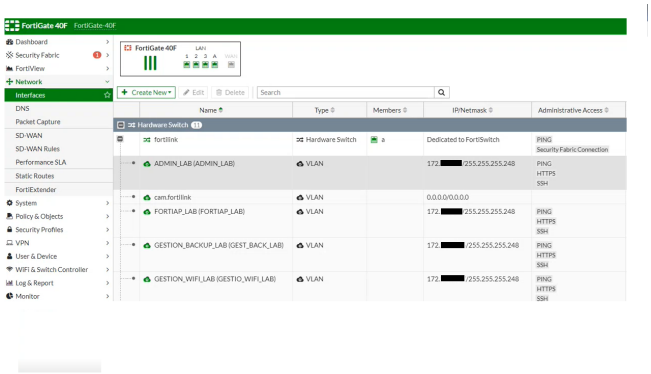

Fig. 11. Configuración de VLANs de la Oficina Laboratorio.

Se realizó la configuración de rutas estáticas en las interfaces del equipo Fortigate de la agencia laboratorio, enrutando hacia cada uno de los Centros de Datos, principal y contingente para posteriormente establecer la configuración de las VPNs que corresponda (Fig. 12).

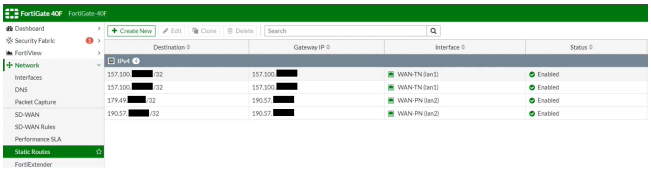

Fig. 12. Configuración de rutas estáticas.

Se realizó la configuración de las VPNs fase 1 y fase 2, y se estableció la tunelización IPSec (Internet Protocol Security) entre las interfaces LAN 1 y LAN 2 del equipo de la agencia, de acuerdo con el direccionamiento de la Fig. 13, hacia las interfaces de los Firewalls Fortigate que se encuentran en los Centros de Datos Principal y Alterno con el direccionamiento asignado. Así se cifró la comunicación de los datos que se transportan por estas conexiones virtuales (Fig. 14).

DIRECCIONAMIENTO IP PARA VPNs				
ISP	RED	GATEWAY	IP ASIGANADA	
ISP 1 TELCO	157.100.X.X/30	157.100.X.X	157.100.X.X	OFICINA LABORATORIO
ISP 2 PUNTO	190.57.X.X/30	190.57.X.X	190.57.X.X	
VPN TELCO	10.238.X.X/16	.....	10.238.X.X/16	DATA CENTER PRINCIPAL
VPN PUNTO	10.239.X.X/16	.....	10.239.X.X/16	
VPN TELCO	10.240.X.X/16	.....	10.240.X.X/16	DATA CENTER ALTERNO
VPN PUNTO	10.241.X.X/16	.....	10.241.X.X/16	

Fig. 13. Direccionamiento para las VPNs entre oficina y centros de datos.

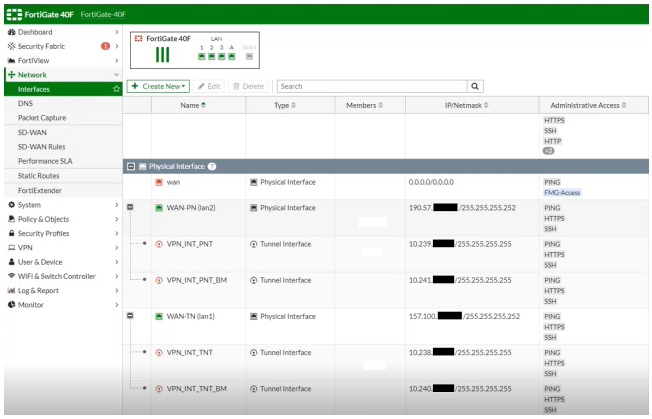

Fig. 14. Configuración de VPNs entre oficina y centros de datos.

Luego, se realizaron las configuraciones necesarias en el módulo de SD-WAN del equipo Fortigate de la agencia, se agregan como miembros las VPNs creadas anteriormente y las interfaces de salida LAN 1 y LAN 2 correspondiente (Fig. 15). Se puede observar que se ponen activas las cuatro VPNs y las interfaces asociadas, por lo que se ha generado la conectividad cifrada desde la agencia hacia los dos centros de datos. También se observa el consumo de datos que cursa por cada uno de los túneles VPNs.

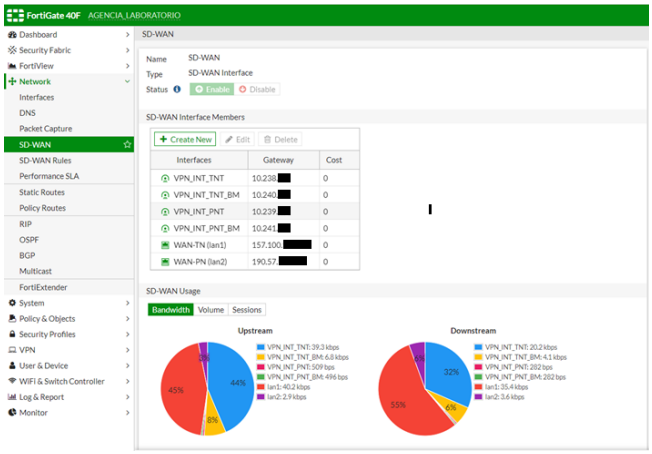

Fig. 15. Configuración de SD-WAN y agregación de VPNs e interfaces asociadas.

A continuación, se efectuó una combinación del Protocolo BGP (Border Gateway Protocol) para la publicación de rutas por los dos enlaces de internet y las interfaces correspondientes, para lograr la selección automática y dinámica de rutas mediante la característica de SD-WAN en el equipo FortiGate. Esto se realizó mediante la creación de scripts que permiten la combinación de estas características, a continuación se observa la primera configuración para la interconexión entre Data Center Principal y Alterno con la Oficina Laboratorio por los enlaces de Internet (Fig. 16).

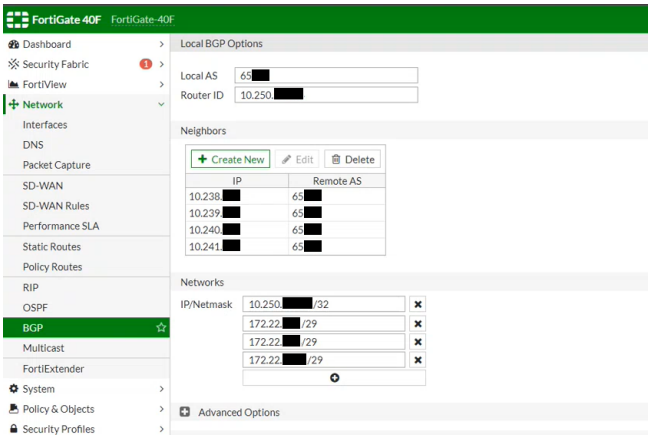

Fig. 16. Configuración de BGP desde oficina hacia centros de datos.

Establecidas las conexiones, partiendo de que en cada uno de los Firewall (Principal y Alterno), se dispuso de las configuraciones de los grupos de objetos o subredes que dieron salida a los diferentes servicios de la Agencia Laboratorio para realizar sus actividades financieras (servicios internos). Se realizó la configuración del grupo de objetos o subredes que se permitió el acceso desde la oficina laboratorio para los diferentes servicios (Fig. 17).

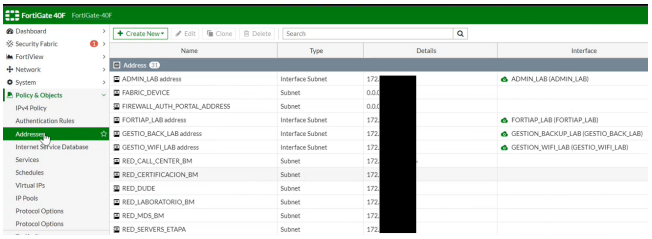

Fig. 17. Salida desde la oficina a servicios internos.

Posteriormente, se realizó la configuración del grupo de objetos que permitió dar salida a la oficina a servicios externos (correo, sistema transaccional, servidores) para los accesos a otros servicios que requiere la oficina (Fig. 18).

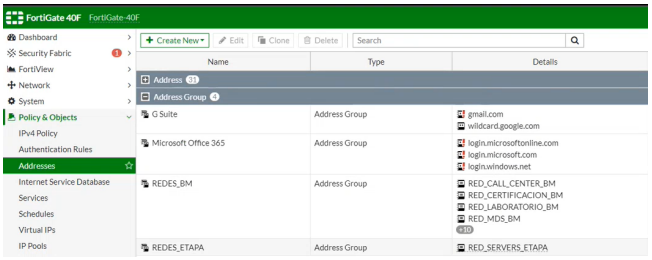

Fig. 18. Salida desde la oficina a servicios externos.

Se efectuó la configuración del SLA (Service Level Agreement) tanto para el Data Center Principal (ETAPA), como para el Alterno (Benigno Malo), aquí se definió los niveles de latencia, jitter y pérdida de paquetes que se consideraron aceptables en una conexión, caso contrario balancea el tráfico de datos por la conexión que se encuentre estable (Fig. 19). A continuación se puede observar el SLA para la salida hacia el Centro de Datos Principal.

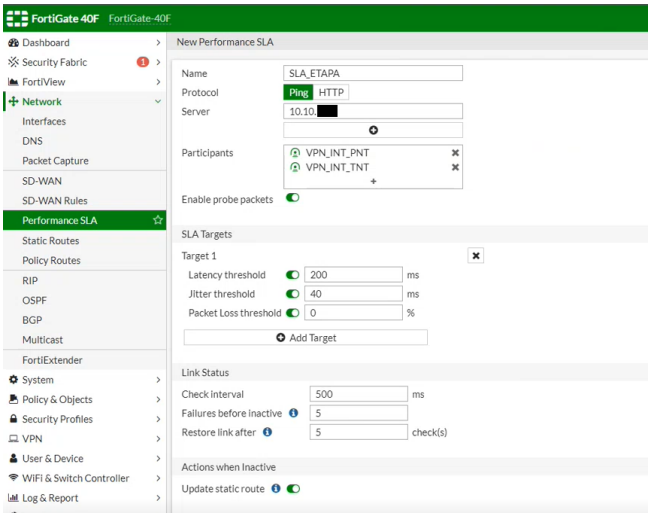

Fig. 19. SLA hacia Data Center Principal - ETAPA.

Se puede observar también el SLA (Service Level Agreement) configurado para la salida hacia el Centro de Datos Alterno, que tiene las mismas características que el implementado anteriormente para el Centro de Datos Principal, con los mismos valores considerados (Fig. 20).

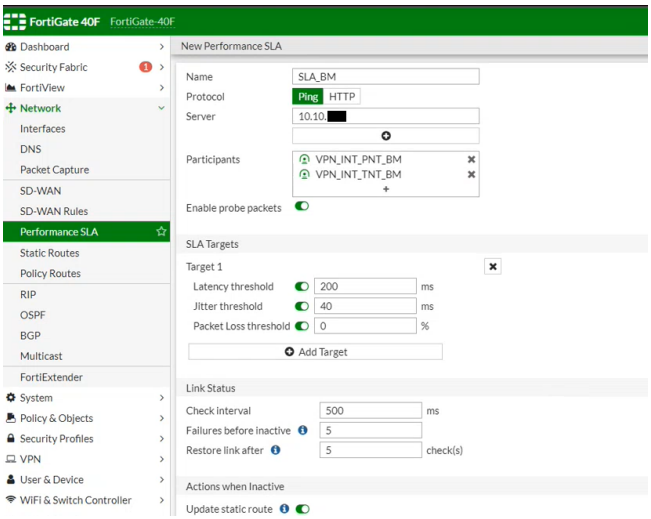

Fig. 20. SLA hacia Data Center Alterno - Benigno Malo.

Una configuración adicional se efectuó para el SLA (Service Level Agreement) de los servicios que se requiere que salgan directamente a internet desde la agencia, por ejemplo, el correo electrónico (Outlook) (Fig. 21).

En la Fig. 22 se observan los SLA (Service Level Agreement) generados en correcto funcionamiento. Cada uno realiza un análisis constante en tiempo real de todos los parámetros configurados, como latencia, jitter y pérdida de paquetes, que se estén generando en cada una de las conexiones. Además,

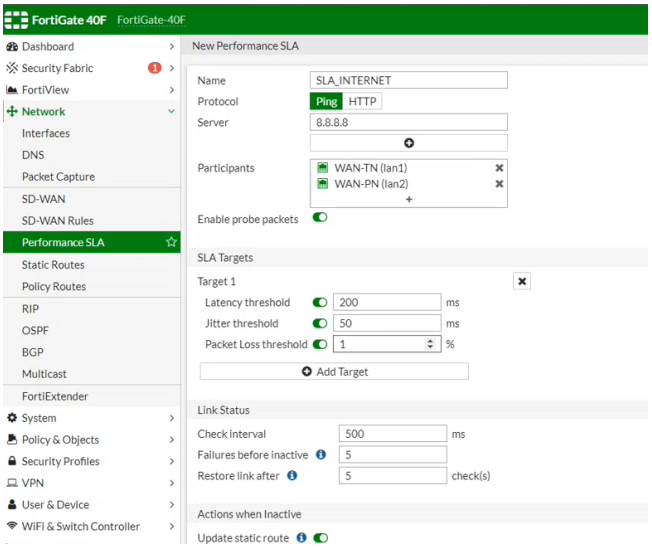

Fig. 21. SLA para salida a Internet de la Oficina Laboratorio.

se evalúan de manera constante y de forma automática, para determinar que el tráfico curse siempre por el mejor canal de comunicación, es decir el que tenga los valores configurados más bajos (Fig. 22).

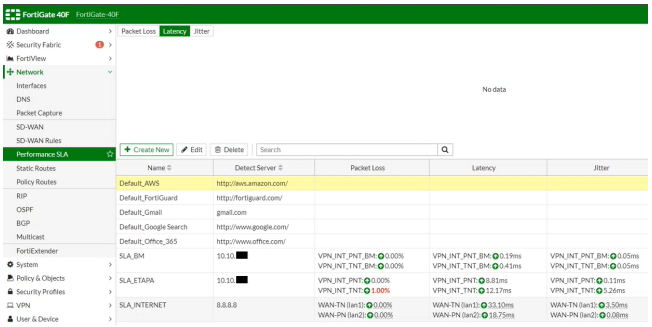

Fig. 22. SLAs en funcionamiento.

A continuación, se procedió a crear las reglas de SD-WAN en el equipo Fortigate de la Agencia-Laboratorio. En la figura se puede observar que se ha creado cada una de las opciones de salidas que va a tener el tráfico que transite entre Agencia y Centro de Datos. Además se tiene una tercera opción en caso de que algún tráfico no vaya a los centros de datos y tampoco a internet conocida como zona implícita (Fig. 23).

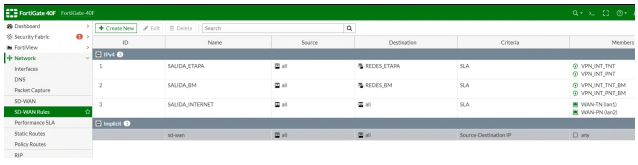

Fig. 23. Reglas SD-WAN para orientar el tráfico.

Dentro del módulo de interfaces, se procedió con la creación de una Zona Agencia, que permite disponer de un símil a una lista de acceso para posteriormente poder establecer los permisos de acceso a los diferentes servicios por medio de perfiles de navegación por VLAN, por ejemplo, el gerente de agencia tiene acceso a servicios diferentes que la VLAN de cajeros, por lo tanto, fue importante definir a qué servicio puede conectarse cada usuario, con la oficina en operación (Fig. 24).

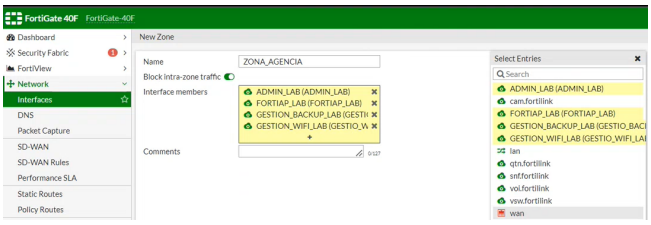

Fig. 24. Creación de una Zona Agencia.

Se realizó la configuración de las Políticas IPV4 en el equipo de la agencia para dirigir el tráfico desde y hacia los centros de datos e internet (Fig. 25).

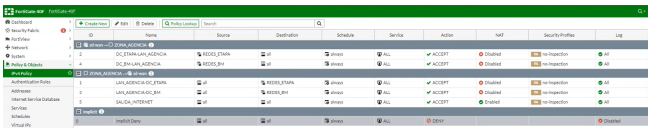

Fig. 25. Configuración de las Políticas IPV4.

Con las configuraciones realizadas, se logró conectar la agencia laboratorio hacia los centros de datos e internet, a continuación, se procedió a configurar la seguridad necesaria para la administración y acceso remoto (Fig. 26), esto dado que actualmente solamente se administra localmente y se debe tener especial cuidado con los tiempos de acceso remoto permitido, puertos, etc.

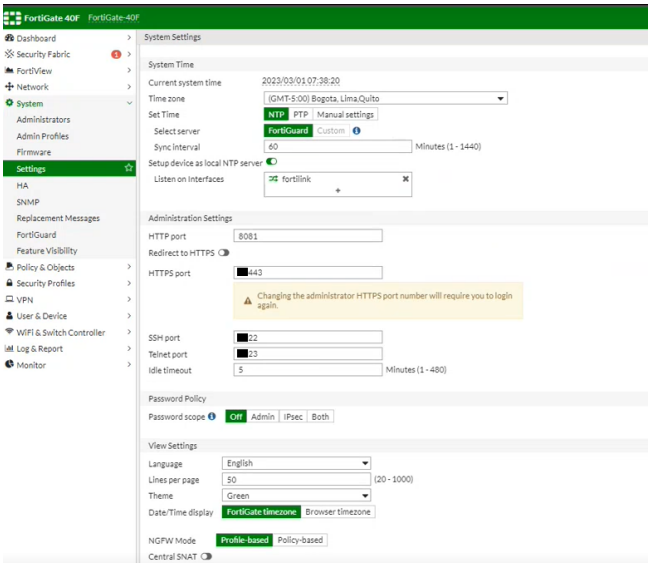

Fig. 26. Configuración de la seguridad de acceso al equipo.

Luego de establecer las políticas de SD-WAN, se realizó un enfoque en el orquestador (FortiManager), el cual se vinculó a la administración centralizada a la nueva Oficina-Laboratorio creada, desde donde se realiza el monitoreo, administración, y configuración de cualquier cambio que se requiera efectuar. (Fig. 27).

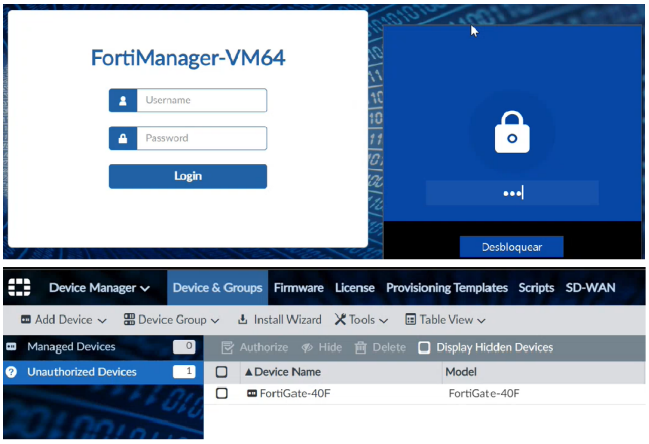

Fig. 27. Agregación de la nueva Oficina-Laboratorio al FortiManager.

Posteriormente, se configuraron los Templates necesarios en el Fortimanager, y se realizó la sincronización de los túneles configurados con anterioridad para que se pueda establecer la comunicación y sea posible administrar desde la consola del Fortimanager el dispositivo Fortigate en la agencia laboratorio, (Fig. 28).

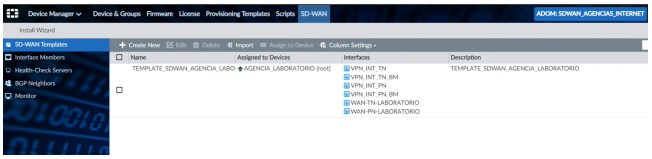

Fig. 28. Configuración de Templates en el Forti Manager.

A continuación, se realizó la configuración y vinculación del switch de datos Fortinet (Fig. 29), denominado Fortiswitch y del Punto de Acceso FortiAP a la consola Fortimanager, con estas configuraciones efectuadas en la Oficina Laboratorio, se puso en operación para posteriormente realizar las pruebas correspondientes.

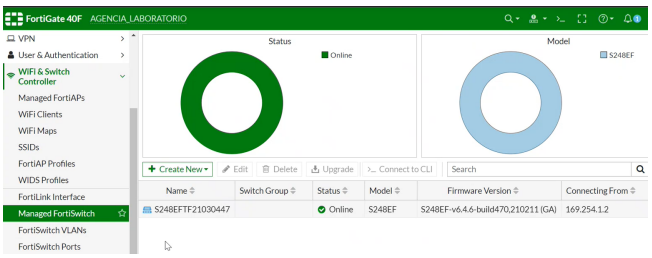

Fig. 29. Interconexión de Fortigate con Fotiswitch.

Luego de realizar la vinculación del Fortimanager con los dispositivos de red de la Oficina (FortiGate, FortiSwitch y FortiAP), los dispositivos se establecen en modo activo y se puede observar la topología funcionando correctamente (Fig. 30).

Fig. 30. Topología SD-WAN con equipos Fortinet.

En el orquestador Fortimanager, se configuró un perfil de pruebas para la configuración de las políticas de seguridad, aprovechando las características de seguridad que se logró anteriormente con la activación de licenciamiento FG-40F-BDL-950-36.

Con las políticas configuradas, se logró una visibilidad de la red mediante las características de Fortinet Security Fabric y prácticamente disponer de un Firewall de nueva generación en la Oficina Laboratorio, el cual permite realizar el filtrado web, anti spam, protección de DNS en el origen del tráfico (Agencia Laboratorio). A continuación, se observa parte de las configuraciones realizadas sobre el módulo del Fortigate, Web Filter (Fig 31).

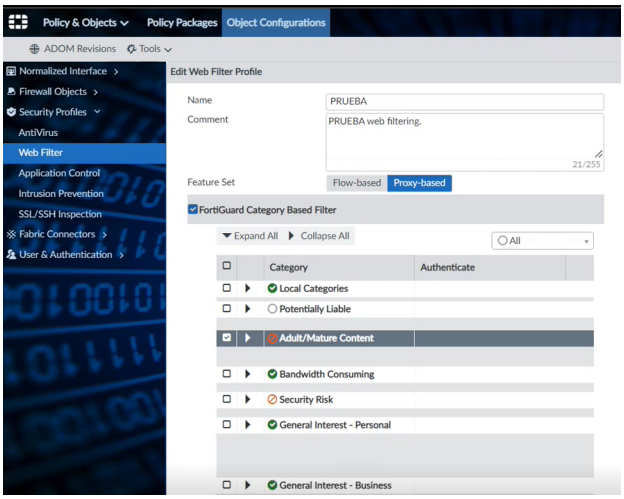

Fig. 31. Configuración de políticas de seguridad - Web Filter.

A continuación, se puede observar lsa configuraciones de seguridad realizadas en el Fortigate, mediante control de aplicaciones (Fig. 32).

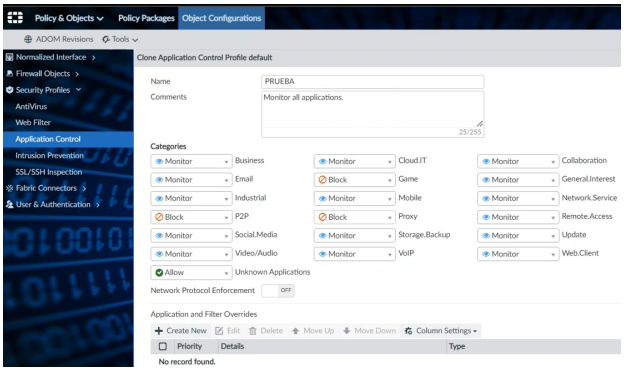

Fig. 32. Configuración de políticas de seguridad - Control de Aplicaciones.

IV. PRUEBAS DE FUNCIONAMIENTO Y RESULTADOS

Una vez culminada la implementación de SD-WAN en la Oficina Laboratorio de la Cooperativa de Ahorro y Crédito Jardín Azuayo, se procedió con las siguientes pruebas de funcionamiento:

En primera instancia, se realizó la conexión de una computadora portátil de manera física al Switch de datos (Fortiswitch), para que permita realizar las verificaciones de balanceo de carga y validación de las políticas de seguridad (Fig. 33).

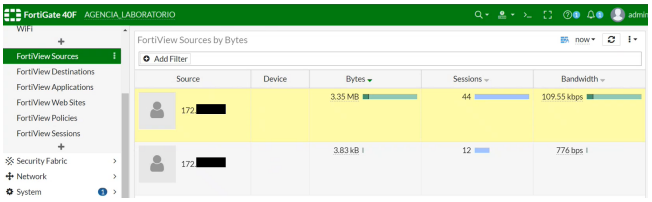

Fig. 33. Conexión de equipo portátil de pruebas a la red local.

Desde el equipo de pruebas se ejecutó el protocolo de mensajes de control de Internet (ICMP), mediante la herramienta ping sostenido al 8.8.8.8 de Google, con el propósito de evidenciar, que al momento que se desconecte una de las interfaces físicas LAN 1 o LAN 2 de cualquiera de los dos proveedores de internet, la respuesta del ping va siempre a mantenerse estable y con conectividad. En primera instancia para esta prueba, en la Fig. 34, se puede observar el ping con respuesta activa hacia cada una de las interfaces de salida de Internet del ISP 1 y ISP 2 (en el equipo Fortigate) y al dominio de Google.

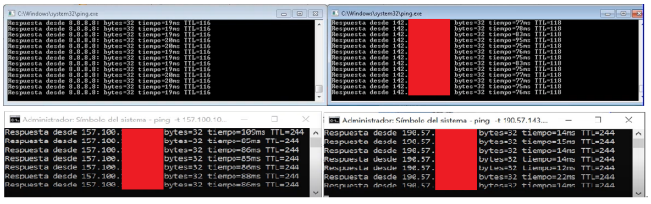

Fig. 34. Conectividad establecida del Fortigate a los dos enlaces de Internet.

A continuación, se desconectó la interface física LAN 2 correspondiente al ISP 2, y se observó que a pesar de que se pierde conexión con la dirección IPV4 de la interfaz, la conectividad hacia el DNS de Google, se mantiene sin pérdida de paquetes (Fig. 35).

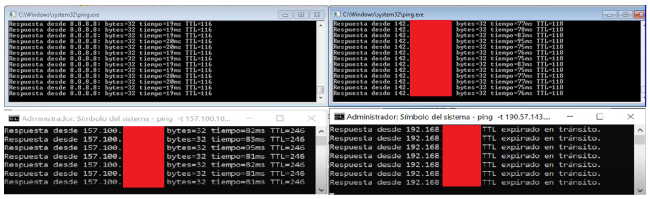

Fig. 35. Prueba de balanceo de carga desconectando al Proveedor ISP-2.

Se realizó el mismo proceso, pero desconectando la interfaz física del ISP 1, en donde se observó que no hay desconexión del ping sostenido hacia la dirección IPV4 correspondiente, ni tampoco pérdida de paquetes. Por lo tanto, también se comprobó el balanceo de carga entre interfaces (Fig. 36).

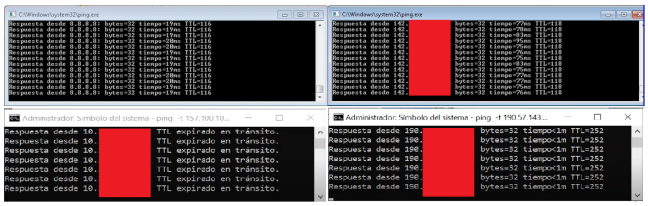

Fig. 36. Pruebas de balanceo de carga desconectando al Proveedor ISP-1.

Siguiendo el procedimiento, se comprobó el funcionamiento de los distintos filtros de seguridad configurados en el Firewall Fortigate de la Oficina Laboratorio, se intentó ingresar desde el computador de pruebas configurado previamente y que se conectó a la red LAN de la Agencia. Mediante éste se intenta ingresar a las redes sociales (Facebook, Instagram, Twitter, etc) sin tener éxito (Fig. 37), ya que está bloqueado el acceso a redes sociales en general en las VLANs de la Agencia.

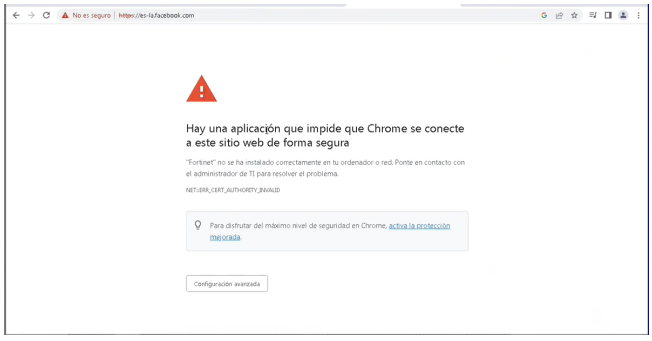

Fig. 37. Prueba con el bloqueo del acceso a redes sociales.

Se verificó también que se active siempre la visibilidad de los controles de seguridad aplicados, los cuales se encuentran implementados y en funcionamiento, por lo tanto, se pudo

constatar su correcta operación, estos perfiles se cargaron a las configuraciones del equipo Fortigate de la Oficina Laboratorio, otorgando seguridad a los datos que salen directamente a internet desde la agencia y sirven de base para las configuraciones que se realicen posteriormente de todas las oficinas de la Cooperativa Jardín Azuayo.

V. ANÁLISIS DE COSTOS

Una de las claves y factor determinante para que las empresas empiecen a migrar la topología de red tradicional a la nueva arquitectura SD-WAN, es el ahorro económico significativo que se logra con esta solución. Es decir, el poder utilizar para la interconexión de oficinas cualquier tipo de medio de transporte, ya sea internet, LTE, MPLS, etc, facilita la conectividad y disponibilidad de las conexiones, adicional a las características de balanceo de carga, seguridad, etc.

Por lo tanto, para este proyecto, se requirió enlaces de internet para interconectar los centros de datos con las oficinas, haciendo factible la migración de los enlaces MPLS antiguos y costosos a conexiones de internet de gran ancho de banda en cada sucursal, brindando una mayor velocidad de conexión a los servicios financieros, a un menor costo mensual.

Una consideración para la arquitectura SD-WAN con Fortinet, es que se requieren enlaces de internet con IPs públicas asignadas por los proveedores, para poder establecer los diferentes túneles VPN desde la agencia laboratorio hacia Centro de Datos Principal y Alterno.

A continuación, se observa el costo mensual y anual de los enlaces MPLS para una agencia en operación actual, con la arquitectura tradicional, considerando dos enlaces MPLS de 5 Mbps con cada proveedor (Fig. 38), se considera también el costo del equipo enrutador que se utiliza en la institución para establecer conectividad con esta topología (Fig 39).

ARQUITECTURA TRADICIONAL - COSTO CONEXIONES MPLS CON PROVEEDORES					
CONEXIÓN	PROVEEDOR	CANTIDAD	COSTO MENSUAL (USD)	COSTO ANUAL (USD)	COSTO TOTAL ANUAL CONEXIONES MPLS POR OFICINA
RED MPLS L3	ISP 1	5 MBPS	200	2400	$4.704,00
RED MPLS L3	ISP 2	5 MBPS	150	1800	
			SUBTOTAL	4200	
			TOTAL	4704	

Fig. 38. Costos de enlaces mensual-anual con enlaces MPLS por agencia.

ARQUITECTURA TRADICIONAL - COSTO DE EQUIPOS					
EQUIPO / LICENCIA	MARCA/MODELO	CANTIDAD	COSTO UNIT (USD)	COSTO TOTAL (USD)	COSTO TOTAL EQUIPOS POR OFICINA
ROUTER	MIKROTIK RB1100	1	950	950	$1064,00
LICENCIAS	...	...	...	...	
			SUBTOTAL	950	
			TOTAL	1064	

Fig. 39. Costo del equipo utilizado con la topología tradicional por agencia.

En la siguiente (Fig. 40), se observa el costo mensual y anual de dos enlaces de internet corporativo de 35 Mbps cada uno con IPs públicas asignadas por los proveedores ISP para la Oficina Laboratorio, se considera también el costo de equipos de la marca Fortinet y licencias que se utilizaron en la Oficina con topología SD-WAN (Fig. 41).

Para calcular el costo completo de la solución SD-WAN (equipos, enlaces) y establecer una comparativa con la arquitectura tradicional, se considera que la vida útil promedio de

ARQUITECTURA SD-WAN - COSTO CONEXIONES DE INTERNET CON PROVEEDORES					
CONEXIÓN	PROVEEDOR	CANTIDAD	COSTO MENSUAL (USD)	COSTO ANUAL (USD)	COSTO TOTAL ANUAL CONEXIONES INTERNET POR OFICINA
INTERNET CORPORATIVO	ISP 1	35 MBPS	80	960	$2150,4
INTERNET CORPORATIVO	ISP 2	35 MBPS	80	960	
			SUBTOTAL	1920	
			TOTAL	2150,4	

Fig. 40. Costos de enlaces mensual-anual con enlaces de Internet.

ARQUITECTURA SD-WAN - COSTO DE EQUIPOS Y LICENCIAS					
EQUIPO / LICENCIA	MARCA / MODELO	CANTIDAD	COSTO UNIT (USD)	COSTO TOTAL (USD)	COSTO TOTAL EQUIPOS POR OFICINA
ROUTER	FORTINET FG-40F	1	330	330	$ 1584,80
LICENCIA FORTIGATE	FG-40F-BDL-950-36	1	950	950	
LICENCIA FORTIMANAGER	FMG-VM-10-UG	1	135	135	
			SUBTOTAL	1415	
			TOTAL	1584,8	

Fig. 41. Costos de equipos y licencias para SD-WAN en Oficina Laboratorio.

equipos de red en una agencia es de cinco años, por ende, para este análisis se considera el valor total de equipos, licencias, y se divide para sesenta meses (5 años). Se contempla este promedio hasta que se realice un cambio de equipos por tiempo de uso.

El valor mensual calculado por equipos y licencias se adiciona al valor económico de los dos enlaces MPLS en el caso de la arquitectura tradicional, y de internet para SD-WAN (Fig. 42)

ANÁLISIS DE COSTOS - TOPOLOGIA TRADICIONAL VS SD-WAN			
COSTO MENSUAL (USD)		COSTO ANUAL (USD)	
TOPOLOGIA TRADICIONAL	TOPOLOGÍA SD-WAN	TOPOLOGIA TRADICIONAL	TOPOLOGÍA SD-WAN
409,73	205,61	4916,76	2467,32
AHORRO MENSUAL (USD)		AHORRO ANUAL (USD)	
204,12		2449,44	

Fig. 42. Costos de Topología Tradicional Vs SD-WAN.

Se puede observar a continuación, el costo total mensual y anual de las arquitecturas en análisis, considerando los equipos y enlaces de internet necesarios para el funcionamiento de una agencia (Oficina Laboratorio). En el caso de la arquitectura SD-WAN, se observa un ahorro mensual considerable, de $204,12 dólares y un ahorro total anual de $2449,44 dólares (Fig. 43). Es decir, la Cooperativa de Ahorro y Crédito Jardín Azuayo al implementar una Agencia con la topología de red SD-WAN, tendrá un ahorro mensual y anual en costos de enlaces de internet y equipos del 50.18%.

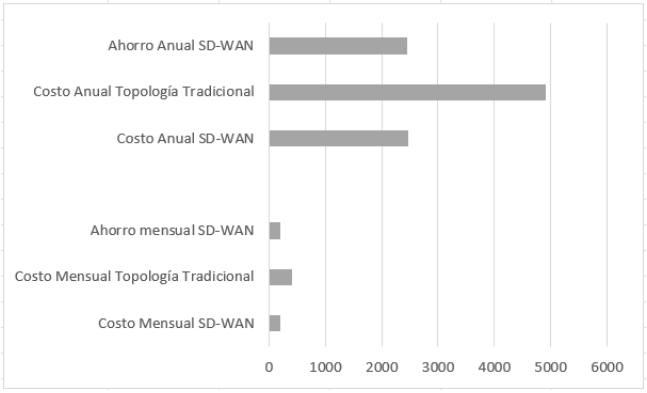

Fig. 43. Ahorro económico por agencia con SD-WAN.

VI. CONCLUSIONES

Se ha implementado la tecnología SD-WAN en la Cooperativa Jardín Azuayo, que permite una mejor velocidad de conexión de los diferentes servicios financieros que presta la institución en la agencia laboratorio, porque con la topología propuesta, todas las conexiones que se encuentran en la nube (Office 365, servicios externos) que anteriormente cursaban por enlaces MPLS desde la agencia hasta el centro de datos, para salir a Internet. Ahora con la salida directa a internet implementada en la agencia con dos proveedores (ISP), es evidente el mayor ancho de banda disponible, la fluidez y estabilidad en la conexión.

Uno de los mayores beneficios de la arquitectura SD-WAN, es el balanceo de carga entre enlaces de Internet, lo cual ha permitido mantener en uso constante los dos enlaces contratados para la agencia. Adicionando a esto la automatización en el uso del mejor enlace disponible. Con esta característica se aumenta la disponibilidad de la red por la convergencia automática entre enlaces y se han reducido varios procesos manuales de configuración para los administradores.

En base al análisis realizado, se ha verificado que existe ahorro económico considerable en los costos mensuales de las conexiones de Internet, ya que la cooperativa dispone de la interconexión mediante enlaces MPLS costosos, en cambio con esta nueva topología se mejora inclusive las perspectivas de negociación con los proveedores, que al momento de una migración masiva de todas las agencias de la institución, se logre acuerdos de mayor beneficio económico y mayor ancho de banda disponible por agencia.

El disponer de un orquestador, o "consola de mando", para la administración de los equipos SD-WAN con Fortinet, ha permitido tener el control, monitoreo y visibilidad de los equipos de red, en una sola pantalla, lo cual ha generado una percepción de tranquilidad al ser visible tanto la actividad de los equipos, amenazas, como la posibilidad del despliegue de configuraciones centralizado.

El Firewall que se ha levantado en la Agencia Laboratorio, brinda la tranquilidad a la institución ante cualquier amenaza, ya que prácticamente dispone de características similares a un Firewall de nueva generación, pudiendo establecer perfiles de navegación, de filtrado y bloqueo de conexiones posiblemente maliciosas por cada VLAN que se implemente, incluso por usuario, en caso de ser necesario.

Con las pruebas técnicas realizadas en la oficina laboratorio, se ha comprobado el funcionamiento de la solución SD-WAN durante todo el proceso de configuración, y se ha realizado los ajustes correspondientes, hasta disponer de una configuración definitiva, que permita un posterior despliegue masivo de la solución, en otras oficinas de la institución.

Se ha comprobado en la Oficina Laboratorio, que adicional a las mejoras en la conectividad, disponibilidad y balanceo de carga propias de SD-WAN. La capa de seguridad de los equipos Fortinet, permite disponer de un Firewall seguro en cada agencia que se implemente con esta tecnología.

El proyecto realizado, ha permitido elevar el nivel de conocimiento, para una administración eficiente de la solución planteada, que permita un despliegue adecuado en otras agencias y respuesta rápida a incidentes que se puedan presentar en el futuro.

REFERENCES

[1] Grenz, M. (15 de febrero de 2017). El sector financiero, el que más apuesta por la digitalización: https://es.statista.com/grafico/8085/el-sector-financiero-el-que-mas-apuesta-por-la-digitalizacion/

[2] Multapplied. (18 de noviembre de 2018) Why Managed SD-WAN Solutions are Game Changers for MSPs:https://www.multapplied.net/white-paper-why-managed-sd-wan-solutions-are-game-changers-for-msps/

[3] Mlitz, K. (23 de abril de 2021). Primary motivations of SD-WAN deployment for organizations worldwide in 2020, by category. https://www.statista.com/statistics/1208522/sdwan-deployment-motivation-global/

[4] P. Segeč, M. Moravčik, J. Uratmová, J. Papán and O. Yeremenko, "SD-WAN - architecture, functions and benefits," 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovenia, 2020, pp. 593-599.doi:10.1109/ICETA51985.2020.9379257: http://ieeexplore.ieee.org/stamp/stamp.jsptp=arnumber=9379257isnumber=9379148

[5] Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities," 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019, pp. 1-9: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=8847124isnumber=8846908

[6] S. Rajagopalan, "An Overview of SD-WAN Load Balancing for WAN Connections," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2020, pp. 1-4: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=9297574isnumber=9297368

[7] S. Andromeda and D. Gunawan, "Techno-economic Analysis from Implementing SD-WAN with 4G/LTE, A Case Study in XYZ Company," 2020 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, Indonesia, 2020, pp. 345-351: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=9163762isnumber=9163657

[8] I. Šeremet and S. Čaušević, "Advancing IP/IMPLS with Software Defined Network in Wide Area Network," 2019 International Workshop on Fiber Optics in Access Networks (FOAN), Sarajevo, Bosnia and Herzegovina, 2019, pp. 56-61: http://ieeexplore.ieee.org/stamp/stamp.jsptp=arnumber=8933726isnumber=8933657

[9] I. Ellawindy and S. S. Heydari, "QoE-Aware Real-Time Multimedia Streaming in SD-WANs," 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 2019, pp. 66-71. doi: 10.1109/NETSOFT.2019.8806622: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=8806622isnumber=8806619

[10] S. Velasco y J. Olivia, "Implementación de Redes SDN-WAN" Implementación de Redes SDN-WAN y evaluación de resultados sobre aplicaciones de uso recurrente en usuarios a través de distintos proveedores de servicios de internet (ISP´s)", 2020 Universidad de las Fuerzas Armadas, Sangolquí, Ecuador, 2020.

[11] Bustamante, J. R., Avila-Pesantez, D. (2021). Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results. Proceedings of the 2021 IEEE Engineering International Research Conference, EIRCON 2021. https://doi.org/10.1109/EIRCON52903.2021.9613418

[12] VMWARE. (13 de junio de 2021). Redes definidas por software. https://www.vmware.com/es/topics/glossary/content/software-defined-networking.html

[13] FORTINET. (13 de junio de 2021). ¿Qué es la SD-WAN? Definición y soluciones. https://www.fortinet.com/lat/products/sd-wan