ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

EMULACIÓN DE UNA RED SD-WAN (*SOFTWARE-DEFINED WIDE AREA NETWORK*) UTILIZANDO TECNOLOGÍA FORTINET Y EL SOFTWARE GNS3

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

JONATHAN JAVIER LÓPEZ ARÉVALO

DIRECTOR: MSc. PABLO WILIAN HIDALGO LASCANO

Quito, Septiembre 2020

AVAL

Certifico que el presente trabajo fue desarrollado por Jonathan Javier López Arévalo, bajo mi supervisión.

_____

MSc. Pablo Wilian Hidalgo Lascano
DIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Jonathan Javier López Arévalo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

Jonathan Javier López Arévalo

DEDICATORIA

A Dios porque su sabiduría me permitió llegar al último escalón,

Definitivamente a las dos personas que me dieron la vida
y que a partir de ese momento se encargaron de hacer de mí
una persona humilde, honesta y correcta,
por su incansable labor y apoyo,
a ustedes PADRES.

Sin lugar a duda, al principal motor
para conseguir todas mis aspiraciones y cumplir mis metas,
aquellas dos personas que llegaron a convertirse
en el mejor regalo que la vida me puede dar,
quienes me motivan a seguir adelante,
a ustedes Doménica y Julián.

Y como olvidarme de las dos personas que han cuidado de mí,
por ser el menor de la familia,
aquellas que de una u otra forma han estado ahí
para enseñarme que la vida no es solo responsabilidades,
sino que también está llena de alegrías y diversiones,
a ustedes Paola y JuanFer

Dedico esto a ustedes MI FAMILIA.

AGRADECIMIENTO

A Dios por nunca dejarme sólo y guiar mi vida por el camino correcto,

A mis padres por su apoyo incondicional desde

el primer día que empecé mi carrera,

A mi esposa y mi hijo que fueron las principales motivaciones

en momentos que desvanecía,

A mi hermano que siempre estuvo ahí para animarme

y distraerme en momentos de estrés,

A mi hermana que nunca me dejó caer y

me incentivó a tomar siempre buenas decisiones,

Al Ing. Pablo Hidalgo quien más que tutor, fue un gran amigo

por sus sabios consejos y confianza depositada en mí,

A mis amigos Dennis, Alexis, Álvaro, Freddy, Israel y Daniel

por ser parte de las personas que siempre me aportaron con buenos consejos,

A todas esas personas que de una u otra manera

ayudaron a mi formación profesional.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

GLOSARIO DE ACRÓNIMOS Y ABREVIATURAS

ACRÓNIMO	SIGNIFICADO
ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interfaces
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BRAS	Broadband Remote Access Server
CAPEX	Capital Expenditures
CLI	Command-Line Interface
CPE	Customer Premises Equipment
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSL	Digital Subscriber Line
DSLAM	Digital Serial Line Access Multiplexer
ESP	Encapsulation Security Payload
FEC	Forward Equivalence Class
GNS3	Graphical Network Simulator 3
GPON	Gigabit Passive Optical Networks
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infraestructure as a Service
ICMP	Internet Control Message Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISO	Imagen Sistema Operativo
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LER	Label Edge Router
LSP	Label Switched Path

LSR	Label Switched Router
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NFV	Network Function Virtualization
NGFW	Next Generation Firewall
ODL	OpenDayLight
OPEX	Operational Expenditures
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PaaS	Platform as a Service
PE	Provider Edge
POP	Post Office Protocol
QoS	Quality of Service
RSVP	Resource Reservation Protocol
SaaS	Software as a Service
SASE	Secure Access Service Edge
SD-DC	Software-Defined Data Center
SDN	Software-Defined Network
SD-WAN	Software-Defined Wide Area Network
SLA	Service-Level Agreement
SMTP	Simple Mail Transfer Protocol
SSD	Solid-State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
TCO	Total Cost Ownership
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VDOM	Virtual Domains
VLSM	Variable Length Subnet Mask
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAN	Wide Area Network
ZTP	Zero-Touch Provisioning

RESUMEN

El presente proyecto de titulación busca brindar un análisis de las Redes de Área Extendida Definidas por *Software* (SD-WAN), valiéndose para ello de la emulación de una SD-WAN Híbrida en el programa GNS3 y empleando los dispositivos de la tecnología FORTINET.

En el primer capítulo se describe el funcionamiento y los componentes de la tecnología *Multiprotocol Label Switching* (MPLS). Se aborda la teoría elemental de *Software-Defined Network* (SDN) para, posteriormente, dar paso al análisis de la SD-WAN, sus conceptos, arquitectura, beneficios, entre otros, y se explica el programa GNS3 y la tecnología FORTINET.

En el segundo capítulo se analiza el funcionamiento de la SD-WAN Híbrida. Se definen las políticas, Redes Privadas Virtuales, Ingeniería de Tráfico, seguridad, etc. Además, se detalla el control y análisis centralizado de la red a través de FortiManager y FortiAnalyzer y se finaliza el capítulo con las configuraciones en cada uno de los dispositivos.

En el tercer capítulo se comprueban los resultados de la emulación mediante pruebas operativas, de seguridad y monitoreo. De igual manera, se presentan argumentos que corroboran el comportamiento adecuado de las cualidades de la SD-WAN Híbrida.

En el cuarto capítulo se presentan las conclusiones obtenidas con el desarrollo de este proyecto de titulación, así como las recomendaciones para futuros trabajos de investigación.

Finalmente, se presentan los anexos que contienen el esquema completo de la SD-WAN Híbrida y los reportes generados por el equipo FortiAnalyzer, en los cuales se detallan las amenazas y riesgos que han intentado vulnerar la red.

PALABRAS CLAVE: SD-WAN, MPLS, GNS3, NGFW, IPsec, SSL, ZTP

ABSTRACT

This project aims to provide an analysis of Software-Defined Wide Area Networks (SD-WAN) through the emulation of a Hybrid SD-WAN in the GNS3 program, using FORTINET technology devices.

The first chapter of this study sets out the components and operation of the Multiprotocol Label Switching technology. The elementary theory of the Software-Defined Network, the concept, architecture and benefits of the SD-WAN are also addressed. The chapter closes with an overview of the GNS3 program and the FORTINET technology.

The second chapter reviews the operation of the Hybrid SD-WAN. The topology, IP address and functioning of the MPLS network and the SD-WAN are described. It is followed by a detailed description of the centralized control and analysis of the network through FortiManager and FortiAnalyzer. At the end of this chapter, the configurations of each one of the associated devices are listed.

The third chapter presents the results of the emulation through functional tests, security, monitoring, and so on. Equally important are the arguments developed here to verify the accurate performance of the qualities of the Hybrid SD-WAN.

The fourth chapter presents the main conclusions and recommendations that came out of this study to strengthen and implement further research projects.

Finally, the annexes of the hybrid SD-WAN scheme and the reports generated by the FortiAnalyzer device are set out. This way, it is possible to identify the threats and hazards that have attempted to breach the network.

KEYWORDS: SD-WAN, MPLS, GNS3, NGFW, IPsec, SSL, ZTP

1. INTRODUCCIÓN

En los últimos años, la comunicación y las redes tradicionales han ido evolucionando de manera acelerada, a tal punto que, las redes se encuentran en un ambiente de "Redes Definidas por Software". *Software-Defined Network* (SDN) se considera como una arquitectura emergente que es manejable, rentable y adaptable, lo que la hace ideal para la naturaleza dinámica de gran ancho de banda de las aplicaciones actuales. Esta arquitectura desacopla el control de red y las funciones de reenvío de datos, permitiendo que el control de la red se vuelva directamente programable y que la infraestructura subyacente se abstraiga para las aplicaciones y los servicios de red [1].

SD-WAN (*Software-Defined Wide Area Network)* conceptualmente se entiende como una combinación optimizada de las características y funciones de MPLS e IP, incluyendo las principales tecnologías *Network Function Virtualization*[1] (NFV) y *Software Defined Network* (SDN). Esto permite a la SD-WAN ser una red más inteligente al separar los planos de control y datos, contar con una administración centralizada y ahorrar costos de rendimiento y operación [2].

Durante los últimos años, en la Escuela Politécnica Nacional no se han desarrollado contenidos, herramientas o laboratorios referentes a SD-WAN, sino que se enfoca en las WAN tradicionales, con equipos y plataformas exclusivamente CISCO, de modo que a los estudiantes se les dificulta enfrentar los nuevos desafíos tecnológicos e ir más allá de la tecnología CISCO tradicional.

Por esta razón, se propone el estudio y emulación de una SD-WAN utilizando tecnología FORTINET y el *software* GNS3, con el fin de proporcionar a los estudiantes nuevos conocimientos acorde a la evolución de la tecnología y las redes actuales como es SD-WAN.

1.1 OBJETIVOS

El objetivo general de este Proyecto Técnico es emular una red SD-WAN (*Software-Defined Wide Area Network*) utilizando tecnología FORTINET y el *software* GNS3.

Los objetivos específicos del Proyecto Técnico son:

- Analizar las características y funcionalidades de la red MPLS y SD-WAN.

[1] **NFV:** *La virtualización de funciones de red (NFV) es una forma de virtualizar servicios de red, como enrutadores y firewalls que tradicionalmente se han ejecutado en hardware propietario.*

- Analizar la arquitectura de red a emular, incluyendo tecnología MPLS, basado en SD-WAN.
- Implementar el prototipo mediante tecnología FORTINET y el *software* GNS3.
- Analizar las pruebas y resultados obtenidos durante el desarrollo de la emulación.

1.2 ALCANCE

El presente Proyecto de Titulación se enfoca en el estudio y emulación de una red SD-WAN basado en la tecnología de FORTINET sobre el *software* GNS3. Con la finalidad de adquirir los conocimientos planteados se propone, en primer lugar, la instalación, manejo y familiarización del *software* de emulación GNS3. Se adjunta un manual (ANEXO A) que permite al estudiante instalar correctamente GNS3 junto con GNS3-VM, recomendación dada para sistemas operativos Windows o MAC OS, con el objetivo de aprovechar al máximo sus funcionalidades, desplegar topologías complejas (SD-WAN) y optimizar GNS3 en el uso de recursos como RAM o CPU [3].

Posteriormente, se describe la arquitectura de red que va a ser emulada en GNS3 con los equipos FortiGate, FortiManager y FortiAnalyzer, los cuales son importados directamente en el software de emulación. La ventaja de GNS3 es que el manejo y configuración de los equipos en el PC es similar a la realidad, ya que se necesitan las ISO (Imágenes del Sistema Operativo) de cada equipo, incluidas las de los dispositivos FORTINET. Los equipos FORTINET emulados tienen un periodo de prueba de 15 días por ser una versión de evaluación. Sin embargo, para el entorno de aprendizaje y emulación, se puede aprovechar aproximadamente el 90% de sus características y realizar respaldos o copias de seguridad, una vez finalice la versión de prueba.

Esto permitirá al estudiante adquirir y desarrollar conocimientos sobre nuevas tecnologías definidas por *software*, usando distintos fabricantes como CISCO, FORTINET, JUNIPER, RIVERBED, etc. El actual entorno académico requiere familiarizarse con equipos de otros fabricantes, aparte de los proporcionados exclusivamente por los equipos CISCO de la institución, que no disponen de las funcionalidades de SD-WAN.

En la Figura 1.1., se ha propuesto una SD-WAN Híbrida, conformada por una red MPLS y la WAN de acceso a Internet, considerando que determinadas empresas desearán mantener su infraestructura MPLS. Además, se tendrán LANs en cada sitio o sucursal, las cuales usarán las conexiones de banda ancha para tráfico de Internet que requiera menor latencia y túneles IPsec (*Internet Protocol Security*) o la red MPLS para tráfico que requiera mayor seguridad frente a ataques. De igual manera, se tendrá el controlador FortiManager

junto con FortiAnalyzer conectados en la LAN de una de las sedes principales y una nube de acceso remoto para visualizar el acceso a través del portal web de FORTINET.

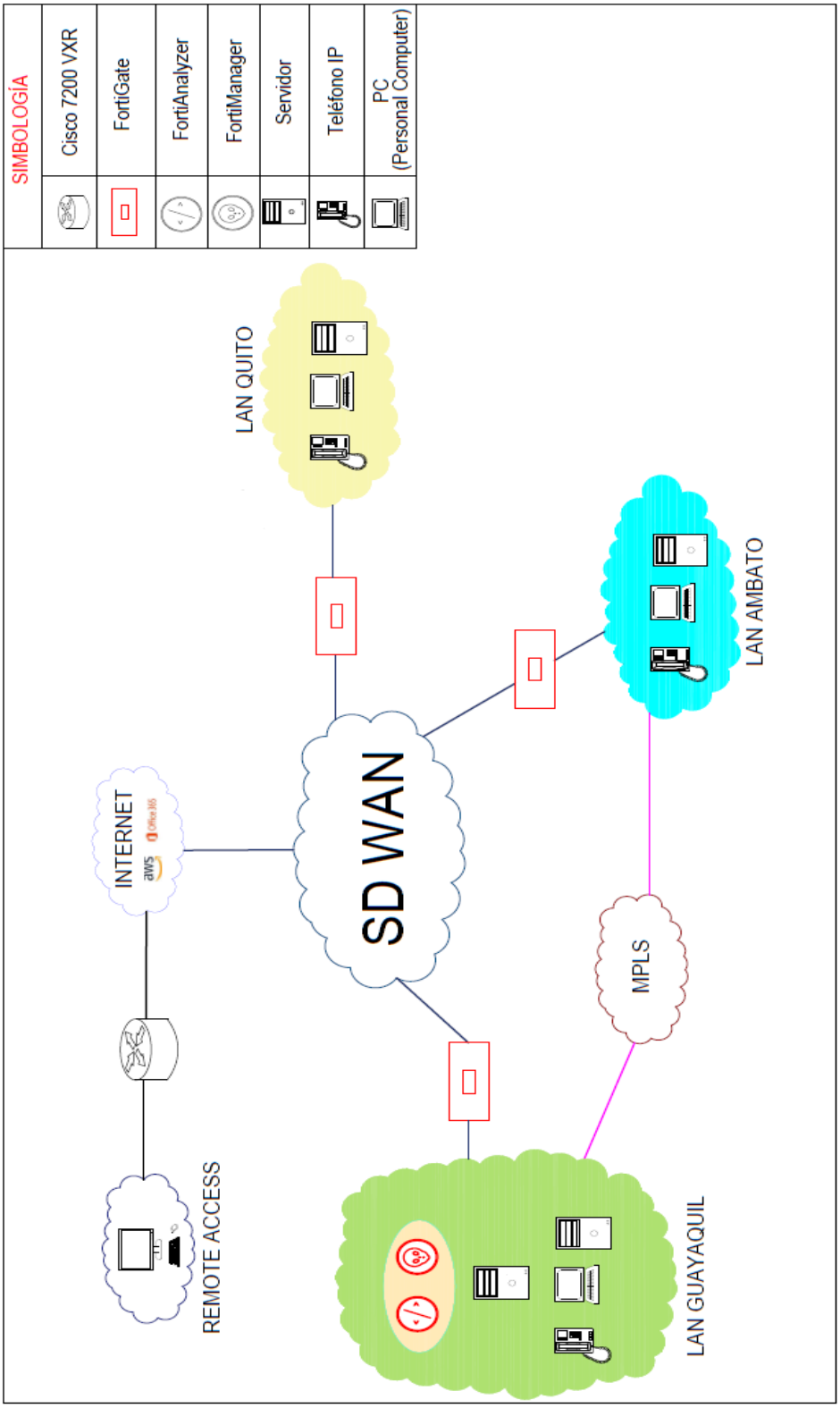


Figura 1.1. Diagrama de la SD-WAN a emular

Este portal web será a través de SSL-VPN (*Secure Sockets Layer-Virtual Private Network*) que proporciona un acceso remoto seguro y usa tecnología TLS (*Transport Layer Security*), la cual se encuentra en la mayoría de los navegadores modernos, facilitando el acceso para los empleados [4].

En la emulación se tomarán en cuenta los servicios de correo, transferencia de archivos y DNS. Se implementará la gestión basada en políticas y reglas de la SD-WAN, con el fin de demostrar que el enrutamiento de tráfico es automático y selectivo para garantizar que las aplicaciones críticas usen la mejor ruta en función de parámetros como latencia, *jitter,* etc., mientras que el otro tipo de tráfico de mayor seguridad hará uso del enlace MPLS mediante VPN´s.

Es importante recalcar que la seguridad es el mayor inconveniente en las SD-WAN. Por este motivo, se ha decidido utilizar la tecnología FORTINET. La SD-WAN tendrá un manejo centralizado en FortiManager que permitirá agregar o remover cualquier política, regla o perfiles de seguridad de manera óptima y sin necesidad de viajar al sitio. Todas estas funcionalidades, en conjunto, conforman una SD-WAN.

Cabe destacar que en la emulación se emplearán productos FORTINET sin licencia, es decir, versiones de prueba para fines de estudio. En consecuencia, ciertas características propias del fabricante no estarán disponibles, como: Filtros web y de correo, *Virtual Domains*[2] (VDOMs), Mapas de calor, entre otras; por ende, estas características no se podrán visualizar en la emulación.

El presente Trabajo de Titulación no tendrá un producto final demostrable porque será la emulación de una red SD-WAN utilizando tecnología FORTINET en el software GNS3.

1.3 MARCO TEÓRICO

1.3.1 REDES DE ÁREA EXTENDIDA TRADICIONALES

Las WAN (*Wide Area Network*) conectan varias Redes de Área Local (LAN) entre sí, a través de *routers* y *Virtual Private Network* (VPN), que permiten la comunicación de voz, datos y video a largas distancias entre múltiples sucursales y centros de datos de una misma empresa. Las WAN operan generalmente en las capas Física y Enlace del modelo OSI [5].

[2] **VDOM:** *son un método para dividir una unidad FortiGate en dos o más unidades virtuales que funcionan como múltiples unidades independientes.*

En las WAN tradicionales cada instancia del plano de datos contiene su propio plano de control. A continuación, se detallan todas y cada una de las desventajas que presentan las WAN tradicionales con base a su estructura que se muestra en la Figura 1.2.

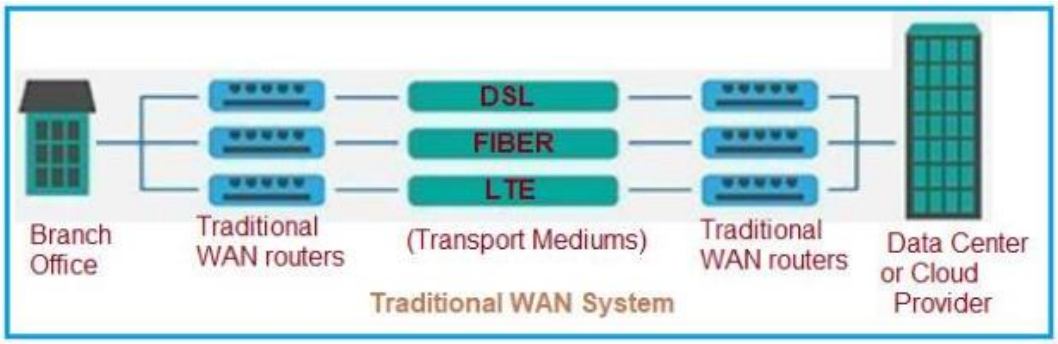


Figura 1.2. WAN Tradicional [6]

1.3.1.1 Funcionamiento WAN

Las WAN tradicionales funcionan a través de la compra e instalación de circuitos propietarios para enrutar servicios IP a sus clientes previstos. Esto se hace con capas de hardware subyacente para completar las redes en su totalidad. El alcance de este tipo de redes hace que la administración de los equipos de TI (Tecnologías de la Información) sea un trabajo engorroso y laborioso, debido a la cantidad de dispositivos de *hardware* instalados y procesos necesarios para administrar la actividad de la red [7].

La seguridad se maneja en forma de listas de bloqueo IP y de control de acceso para evitar que el tráfico malicioso se infiltre en la red.

La configuración de sucursales adicionales y ubicaciones remotas requeriría *hardware* adicional, lo que a su vez eleva los costos para las empresas.

La escalabilidad en las WAN tradicionales es más compleja en comparación con las SD-WAN, ya que se necesita una planificación exhaustiva, junto con la implementación del soporte logístico requerido para establecer la infraestructura necesaria para que las operaciones funcionen [7].

1.3.1.2 Desventajas WAN

- El *failover*[3] depende completamente del estado del enlace, es decir se requieren de varios segundos para su restauración, lo que provoca retardos importantes o una mala experiencia en los usuarios finales.

[3] ***Failover:*** *es un modo operativo de respaldo, es decir las funciones son asumidas por componentes secundarios.*

- La configuración está alojada localmente en cada enrutador, es decir es distribuida.
- Las nuevas políticas deben ser administradas por dispositivo, es decir el administrador debe manipular cada equipo individualmente para cambiar éstas.
- Se necesita de un buen intervalo de tiempo (meses) para la instalación de nuevos sitios. Esto conlleva establecer el circuito o enlace, aprovisionamiento de equipos y gestión de cambios [8].
- La arquitectura WAN tradicional es estática y privada, por lo que dificulta la migración a la nube.
- Ancho de banda limitado de los costosos circuitos privados, lo que inhibe el despliegue e impacta el rendimiento de las aplicaciones.
- Dependiente del centro de datos (topología *Hub and Spoke*[4]) ya que no tiene un acceso directo a los recursos de la nube desde las sucursales, provocando un retardo que minimiza el rendimiento [9].
- Infraestructura compleja debido a que la WAN tradicional incluye múltiples dispositivos de función única conectados a través de enlaces WAN que dificultan su gestión.
- Rendimiento imprevisible de aplicaciones ya que el tráfico de las aplicaciones en los enlaces de Internet carece de un Acuerdo de Nivel de Servicio (SLA[5]) que permita predecir su rendimiento [9].

Por otro lado, están las tecnologías WAN públicas que dependen de Internet. El Internet provee una red global para empresas, que permite conectar sus sucursales y compartir información a través de éste. Sin embargo, el problema de seguridad es la razón por la que las empresas empezaron a usar VPN, ya que cualquier persona podía ver la información que viaja a través de Internet. De esta manera, muchas empresas en las que el nivel de seguridad es alto, optaron por escoger las tecnologías WAN privadas que implicaban un mayor costo, mientras que, si se deseaba mayor flexibilidad y menor costo, Internet era la mejor opción.

En la Figura 1.3. se muestran las diferentes tecnologías que fueron diseñadas para comunicación WAN privada como: Frame Relay, ATM, Metro Ethernet, MPLS, etc., en las

[4] ***Hub and Spoke*****:** *todas las rutas o spoke se conectan con un punto central conocido como hub.*
[5] **SLA:** *Service Level Agreement es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.*

que se aplicaba el mismo criterio, si se necesitaba mayor ancho de banda funcionaba mejor una WAN dedicada, de lo contrario sería mejor una WAN conmutada [5].

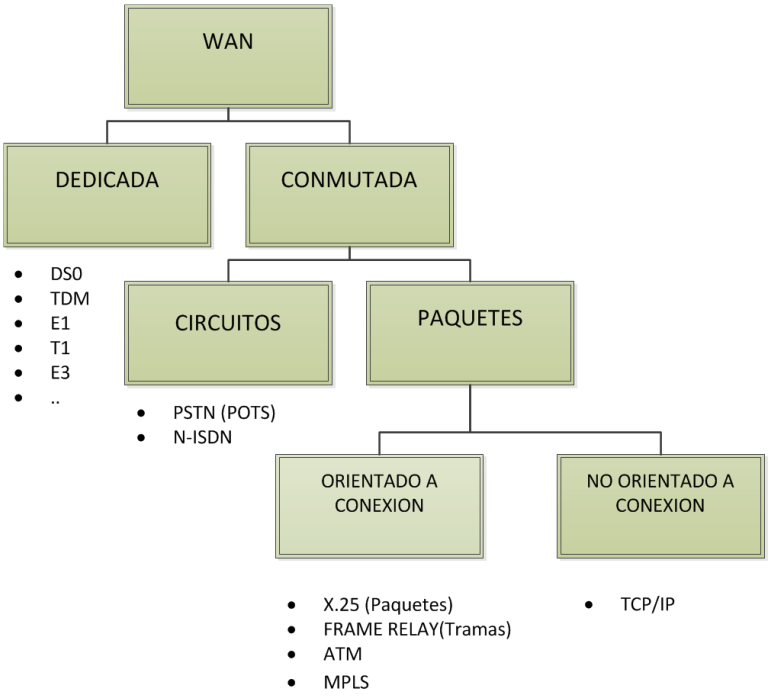


Figura 1.3. Opciones WAN [10]

Actualmente, varias de estas tecnologías son consideradas obsoletas por lo que se discute a detalle una tecnología en particular conocida como *Multiprotocol Label Switching* (MPLS), en vista de que, actualmente es la más utilizada en el mundo y será parte de la emulación a realizar.

1.3.2 MULTIPROTOCOL LABEL SWITCHING (MPLS)

Es una arquitectura que provee una eficiente designación, enrutamiento, envío y conmutación de flujos de tráfico a través de la red [10]. MPLS incrementa la velocidad de datos a través de la red y mejora su rendimiento, ya que la decisión de enrutamiento está basada en etiquetas asignadas y no en la cabecera IP, como se realiza tradicionalmente en redes IP.

1.3.2.1 Fundamentos de MPLS [10]

- MPLS permanece independiente de los protocolos de capa de enlace y capa red.
- Traduce las direcciones IP en etiquetas simples de longitud fija.
- Soporta distintos protocolos como los correspondientes a IP, ATM y Frame Relay.
- Provee nuevas capacidades significativas en: QoS, Ingeniería de Trafico, VPN y un soporte Multiprotocolo.

- Sólo los *routers* de borde se encargan de realizar procesamiento a nivel de capa 3.
- Los *routers* ubicados en el interior de la nube MPLS, por su parte, solo conmutan paquetes con base en la revisión y conmutación de etiquetas.

1.3.2.2 Componentes de MPLS

La arquitectura MPLS diferencia dos tipos de *routers:* LER *(Label Edge Router)* y LSR *(Label Switched Router),* como se muestra en la Figura 1.4.

- ✓ **LER o PE (*Provider Edge*):** *routers* que se encuentran en el borde de la red MPLS, encargados de conectar diversas redes como ATM, Frame Relay, etc. y de asignar y retirar las etiquetas en la entrada o salida de la red MPLS [10].
- ✓ **LSR o P (*Provider*):** *routers* que se encuentran en el núcleo de la red y que son parte del proveedor de servicios, encargados de la distribución de etiquetas para encaminar los paquetes [10].

FEC (*Forward Equivalence Class*): es una representación de un grupo de paquetes que comparten los mismos atributos para su transporte [10].

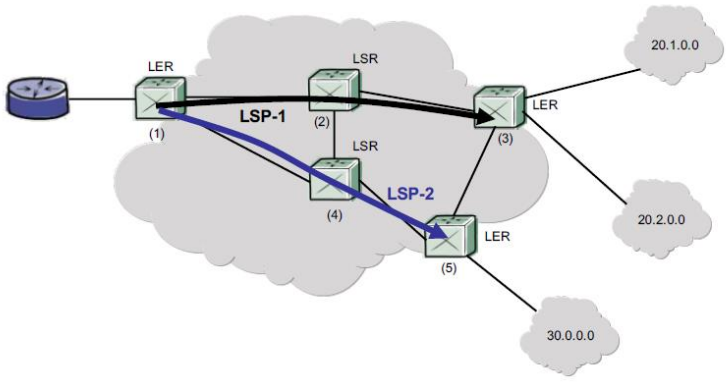


Figura 1.4. Componentes de una red MPLS [10]

Es importante mencionar, que los LSP (*Label Switched Path*) que se muestran en la Figura 1.4. son caminos específicos unidireccionales a través de la red MPLS, equivalentes a un circuito virtual de otras tecnologías WAN.

1.3.2.3 Funcionamiento de MPLS [10]

En la Figura 1.5. se visualiza el funcionamiento de MPLS, resumido en los siguientes cinco pasos:

1. Establecimiento de rutas y asignación de etiquetas, antes de transferir los paquetes.
2. Distribución de etiquetas y creación de tablas.

3. Recepción del paquete e inserción de etiqueta.
4. Conmutación de etiquetas y reenvío del paquete.
5. Extracción de etiqueta y entrega del paquete.

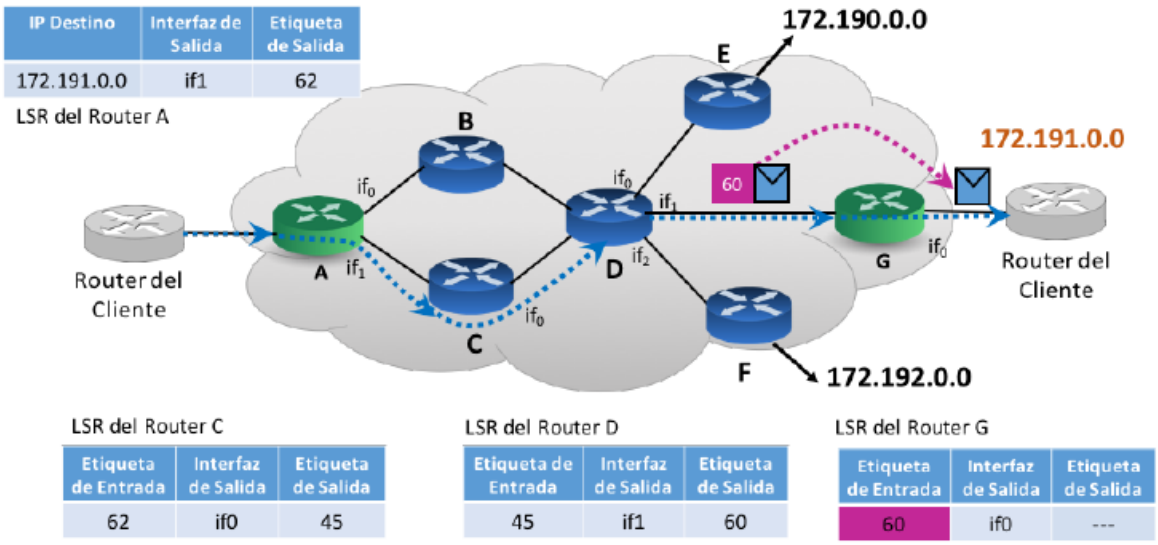


Figura 1.5. Funcionamiento de una red MPLS [10]

1.3.2.4 Desventajas de MPLS [5]

- Alto costo de MPLS en comparación con el costo normal de conectividad de Internet.
- Adaptación a nuevas tecnologías como aplicaciones en la nube. No es eficaz enviar aplicaciones SaaS[6] e IaaS[7] a un nodo central por el retardo que provoca.
- Requiere de un tiempo significativo para el despliegue de una nueva sucursal. Además, existen zonas donde no es fácil llevar MPLS, pero si pueden llegar *Asymmetric Digital Subscriber Line* (ADSL) o módems 4G.
- Requerimiento de un administrador de red en la sucursal para la configuración, lo que significa un aumento de costos de operación.
- Tener más de un proveedor resulta muy costoso.

[6] **SaaS:** *Software as a Service, se trata de cualquier servicio basado en la web. Algunos ejemplos son: Salesforce, Dropbox, Gmail, etc.*
[7] **IaaS:** *Infraestructure as a Service, consiste en proveer y gestionar recursos de computación a través de Internet; como servidores, almacenamiento, equipos de red y virtualización. Permite tener más control que PaaS (Platform as a Service). Ejemplos populares de IaaS son: Amazon Web Service, Google Cloud, Azure, etc.*

Por lo tanto, MPLS es una tecnología no fácil de implementar y costosa en relación con tecnologías tradicionales, por lo que se ha evolucionado a SD-WAN o SD-WAN Híbrida que compensan los problemas de MPLS.

1.3.3 SOFTWARE DEFINED NETWORK (SDN)

Una Red Definida por *Software* (SDN) tiene como objetivo principal separar el Plano de Control del Plano de Datos, a diferencia de las redes de datos tradicionales. El control de la red se lo realiza a través de la programación de reglas en un dispositivo denominado controlador SDN, por lo que la gestión de la red es altamente centralizada en este controlador, encargado de manejar toda la inteligencia de la red [11].

En lo referente a su implementación, se simplifica el diseño y control en comparación con redes tradicionales, en vista de que se obtiene independencia del fabricante del equipo y se reducen los dispositivos, ya que se pueden virtualizar funciones de red en un mismo *hardware* (NFV).

1.3.3.1 Arquitectura SDN

Según la Figura 1.6. la arquitectura SDN comprende tres capas: la capa de Aplicación, la capa de Control y la capa de Infraestructura o de Datos. Estas tres capas se comunican a través de las interfaces *southbound y northbound,* también conocidas como *Application Programming Interfaces* (API) que ofrecen un conjunto de protocolos para que dos aplicaciones se comuniquen entre sí [12].

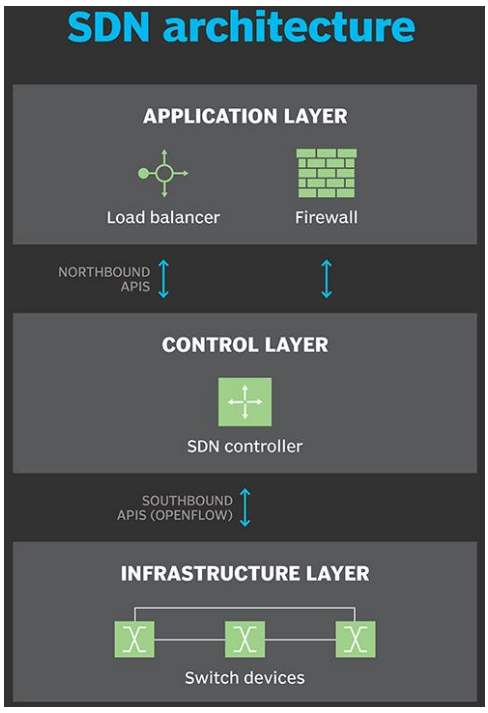


Figura 1.6. Arquitectura SDN [12]

La capa de Aplicación lógicamente contiene aplicaciones de red que usan las empresas, con el fin de introducir nuevas funciones como seguridad, balanceo de carga, capacidad de administración, etc. Esta capa puede recibir una vista abstracta y global de la red y usar esa información para proporcionar una guía adecuada a la capa de Control. La interfaz entre la capa de Aplicación y la capa de Control se conoce como la interfaz *northbound*, la cual actualmente no tiene una API estandarizada [13].

La capa de Control representa el *software* del controlador SDN que actúa como el cerebro de la red. Esta capa es responsable de la programación y gestión de la red, utilizando la información proporcionada por el plano de reenvío de datos para definir el funcionamiento y enrutamiento de la red. La capa de Control se comunica con la capa de Infraestructura a través de la interfaz conocida como *southbound* [12]. *OpenFlow*, es la interfaz *southbound* más utilizada, principalmente de conmutadores.

La capa de Infraestructura también llamada Plano de Datos, está compuesta por los conmutadores físicos de la red. Es responsable principalmente del reenvío de datos, así como de la recopilación de estadísticas [13].

1.3.3.2 Protocolo OpenFlow

Es el primer estándar que define la interfaz de comunicación entre el controlador y diferentes dispositivos de red de la arquitectura SDN, con el objetivo de ajustar el comportamiento del Plano de Datos. La arquitectura que propone este protocolo, como se muestra en la Figura 1.7. ha sido diseñada para que se apoye en tres componentes: Controlador, Tablas de Flujo y dispositivos (*switches*) [14].

1. Controlador, es la parte inteligente que dialoga con todos los *switches* y les transmite a éstos la información que necesitan.
2. Tablas de Flujos, instaladas en cada uno de los *switches* que indican a cada dispositivo la acción a realizar con el tráfico.
3. Dispositivos (*switches*), con soporte para OpenFlow.

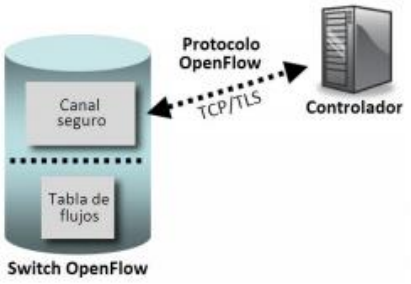


Figura 1.7. Arquitectura de OpenFlow [14]

En un *router* o *switch* tradicional, el paquete de mayor velocidad de reenvío y las decisiones de alto nivel ocurren en el mismo sitio. Por otro lado, un *switch OpenFlow* separa estas dos funciones; la parte de reenvío de paquetes reside en el *switch,* mientras que las decisiones de enrutamiento se trasladan al Controlador [11].

La ruta de los datos de un *switch OpenFlow* viene definida por la Tabla de Flujos, la cual contiene una serie de campos de las cabeceras de los paquetes y una acción. De esta manera, *OpenFlow* permite desplegar fácilmente una estrategia de reenvío e implementar protocolos de conmutación de red de forma centralizada y con una visión global [11].

En conclusión, el protocolo *OpenFlow* indica al tráfico como fluir basado en los parámetros y requerimientos específicos de las aplicaciones. Además, *OpenFlow* tiene la facilidad de ser desplegada en una red existente ya sea física o virtual.

1.3.3.3 Beneficios SDN [15]

Esta sección muestra las principales ventajas de las SDN, con el fin de compensar los desafíos que enfrentan las arquitecturas de red tradicionales.

- Simplifica el aprovisionamiento y la administración de la red.
- Flexibilidad de la red.
- Mejor uso de los recursos de red disponibles, para mejorar el rendimiento.
- Menor gasto de capital (CAPEX[8]).
- Menor gasto de operación (OPEX[9]).
- Ejecución de Ingeniería de Tráfico.
- Mayor visibilidad de toda la red gracias a la separación de planos de Control y Datos.
- Mejor seguridad gracias a la mayor visibilidad de la red.

1.3.3.4 Desafíos SDN [15]

A pesar de que SDN ofrece una potencial solución para los proveedores de red, su implementación y desarrollo implica algunos desafíos que se muestran en esta sección.

[8] **CAPEX:** *capital expenditures o gastos de capital, son fondos para adquirir, actualizar y mantener activos físicos como propiedades, equipos, etc.*
[9] **OPEX:** *operational expenditures, es el costo permanente para el funcionamiento del sistema.*

- Confiabilidad en las SDN: una de las soluciones es añadir redundancia en el controlador central de la arquitectura de red.
- Escalabilidad en las SDN: el rendimiento de la SDN depende del controlador y de los recursos del *switch,* de tal manera que, si el controlador enfrenta problemas de rendimiento se agregará un retardo en las actualizaciones. Por lo tanto, cuando una organización hereda grandes redes de producción pueden encontrarse con este problema.
- Amenazas de Seguridad SDN: mayor vulnerabilidad debido a que es una infraestructura recientemente desplegada y elimina el uso de enrutadores y conmutadores físicos. Su gestión es centralizada, por lo que, los riesgos de seguridad aumentan, más aún cuando el tráfico circula a través de Internet.

1.3.4 SOFTWARE-DEFINED WIDE AREA NETWORK (SD-WAN)

Actualmente, en el sector WAN existe la necesidad de incrementar el ancho de banda y disminuir la latencia debido a la migración masiva de aplicaciones a la nube. Con la evolución de la tecnología, las empresas gastan millones para actualizar su infraestructura del Centro de Datos, por lo que se vuelve inminente actualizar también la WAN a SD-WAN [5]. Con el objetivo de solventar estas necesidades y la alta inversión, aparece la SD-WAN por su capacidad de adaptación al mercado. Adicionalmente, es importante mencionar que todo comenzó con la llegada de la SDN.

La tendencia del crecimiento exponencial de los servicios en la nube, tomando en cuenta los servicios: *Software as a Service* (Saas), *Platform as a Service* (PaaS) e *Infraestructure as a Service* (IaaS), se muestra en la Figura 1.8. [5].

Figura 1.8. Evolución de los servicios en la nube [5]

Existen tres principales factores que impulsan la evolución de la WAN a la SD-WAN:

1. La nube está transformando la red.
2. Las comunicaciones unificadas están llegando a ser una parte critica de los negocios.
3. La informática tradicional está adoptando un enfoque centralizado en la red.

Es importante mencionar que la SD-WAN, proporciona enrutamiento de aplicaciones definidas por *software* a la WAN y conecta muchas ubicaciones de una organización, mientras que SDN, se enfoca internamente dentro de la LAN o la red central del proveedor de servicios.

1.3.4.1 Definición SD-WAN

SD-WAN, es una tecnología que tiene el potencial de revolucionar el sector de las redes de área extendida y viene dada como reemplazo de los servicios de optimización WAN, VPN-MPLS, automatización y administración de redes. Además, SD-WAN se puede entender como un enfoque único que permite a las organizaciones enrutar el tráfico a ubicaciones remotas, a través de medios de transporte más apropiados y proporcionar capacidades mejoradas para monitorear y administrar el tráfico de la red en tiempo real [5].

1.3.4.2 Arquitectura SD-WAN

Existen tres capas principales como se muestra en la Figura 1.9., que conforman la arquitectura de una SD-WAN: *Cloud Network,* Servicios Virtuales y Orquestación y Análisis.

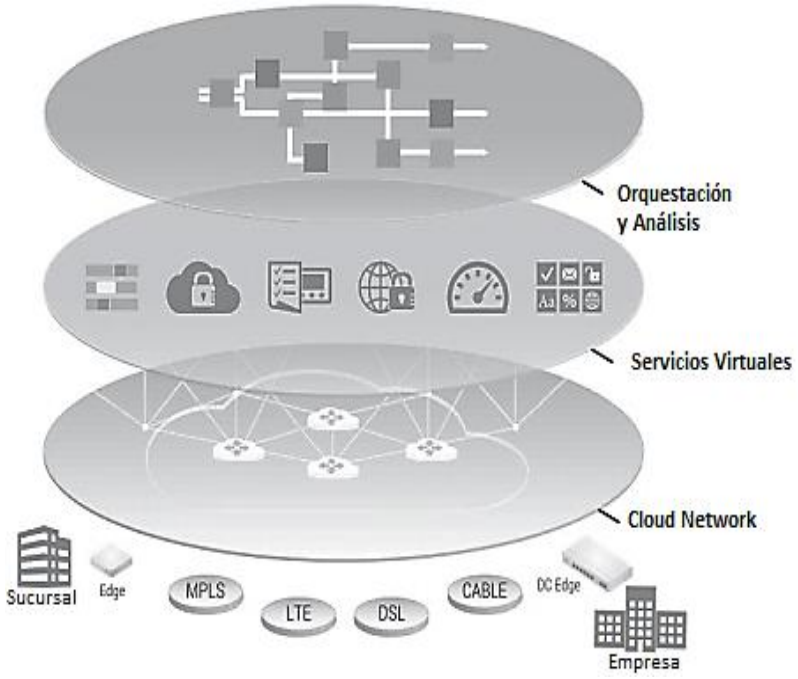


Figura 1.9. Arquitectura SD-WAN [5]

La capa *Cloud Network* da la facilidad de tener una red basada en superposición, que es capaz de establecer conexiones a través de infraestructuras IP públicas y privadas; ha sido diseñada con el fin de facilitar la comunicación entre oficinas remotas, aplicaciones y servicios en la nube [5]. Una parte importante de esta capa es su seguridad, dado que SD-WAN usa la infraestructura pública de Internet como red de transporte.

La capa Servicios Virtuales, por su parte, combina tres tipos de servicios: servicios en la sucursal (*firewall*), servicios en el centro de datos (optimización WAN, *firewall*) y servicios en la nube (*SaaS, PaaS, IaaS*). Además, se encarga de optimizar el flujo de comunicación hacia cada uno de los diferentes tipos de servicios [5].

La capa de Orquestación tiene tres componentes principales: el Plano de Gestión, el Plano de Control y la Estructura de Políticas. En primer lugar, el Plano de Gestión representa un resumen de alto nivel de políticas, configuraciones, monitoreo e informes. La consolidación de todas estas características crea una interfaz de administración, capaz de controlar fácilmente la implementación total de una red. El concepto detrás de esto es conocido como *Zero-Touch Provisioning* (ZTP), en la que cada dispositivo no requiere ser configurado individualmente, sino que el dispositivo descarga su configuración desde el Plano de Control. Desde este punto de vista, el Plano de Control se encarga de la automatización de la red, mientras que la Estructura de Políticas como su nombre lo indica se refiere a las políticas de garantía de servicio [5].

1.3.4.3 Funcionamiento de la SD-WAN

SD-WAN es una superposición a la red existente, es decir una red operando sobre otra red; utiliza soluciones de tunelización para diferenciar la red física de la red lógica, como se muestra en la Figura 1.10.

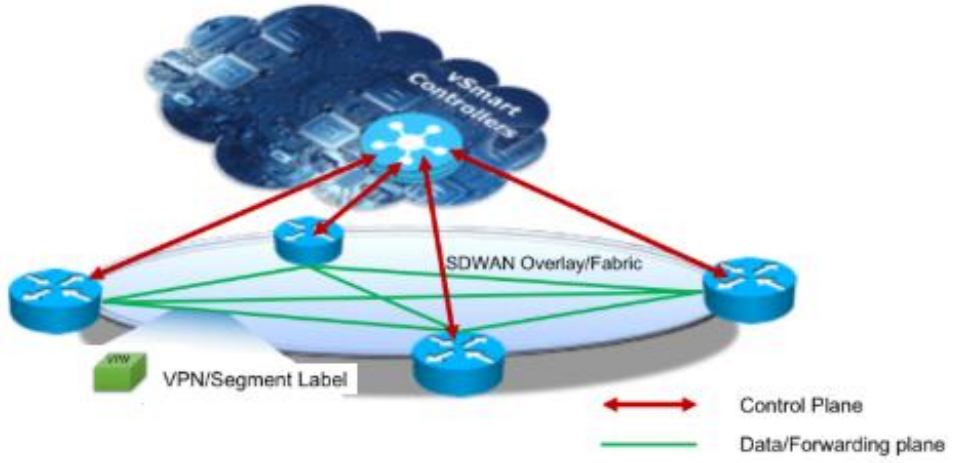


Figura 1.10. Funcionamiento SD-WAN [16]

SD-WAN implementa un controlador centralizado, que actúa como un único panel para administrar toda la red y establecer políticas. Las políticas permiten controlar las rutas de tráfico, SLA, *failover,* monitorización, etc. Una vez definidas las políticas, éstas se envían desde el controlador a cada nodo SD-WAN para que sean configuradas sin intervención alguna de un administrador de redes (ZTP) [8].

Posteriormente, con las políticas ya configuradas en cada uno de los nodos, la red SD-WAN monitorea de manera inteligente el rendimiento de los enlaces, y empieza a enviar el tráfico por la mejor ruta basado en el SLA especificado anteriormente. Llegado a este punto, desaparece cualquier interrupción del circuito al desviar el tráfico a un enlace de respaldo o redundante.

1.3.4.4 Opciones de despliegue de SD-WAN

En la Tabla 1.1., se muestran las opciones de despliegue de una SD-WAN: propia, administrada y como servicio.

Tabla 1.1. Ventajas de las opciones de despliegue de SD-WAN

SD-WAN PROPIA	SD-WAN ADMINISTRADA	SD-WAN COMO SERVICIO
Control Total	Funcionalidad	Facilidad de Despliegue
Independencia	Escalabilidad	Flexibilidad

Entre las ventajas de la primera opción se tiene: control total e independencia. El control total evita la intervención de terceros en cualquier proceso de la empresa, lo que es importante para las empresas que manejan información confidencial. La independencia, por su parte, es un factor crucial para la flexibilidad que permite a las empresas hacer cambios significativos en su infraestructura de TI[10] rápidamente, sin esperar por procesos complicados o que conllevan tiempo por parte de los ISPs (*Internet Service Provider*) [5]. Sin embargo, los requerimientos fundamentales son que la empresa debe contar con recursos significativos y tener experiencia en el campo para su correcta implementación.

Por otro lado, entre las ventajas de tener una SD-WAN administrada están: funcionalidad, escalabilidad y personal calificado. Al hablar de funcionalidad, se refiere al corto tiempo que toma en implementar una característica específica en la arquitectura SD-WAN, gracias a sus departamentos de TI especializados. La escalabilidad es asegurada, ya que los recursos de los ISPs pueden considerarse ilimitados y pueden crecer con base en la

[10] **TI o IT:** *Information Technology, es el uso de computadoras para almacenar, recuperar, transmitir y manipular datos o información.*

demanda del cliente. De esta manera, SD-WAN administrado elimina la necesidad de que las empresas tengan profesionales especializados en TI, provocando un ahorro de costos en el personal de las empresas [5]. Generalmente, esta solución resulta más apropiada para empresas pequeñas.

Finalmente, existe una tercera opción llamada SD-WAN como servicio que aprovecha la funcionalidad de la nube y proporciona importantes beneficios. Entre ellos se encuentra: la flexibilidad, despliegue rápido y costo menor que las SD-WAN anteriores.

1.3.4.5 Tipos de arquitectura SD-WAN

A medida que la tecnología sigue evolucionando, la solución SD-WAN se ha segmentado en tres distintas arquitecturas como: sitio a sitio, nube e híbrido [17].

En primer lugar, la solución SD-WAN sitio a sitio es el tipo más básico que incluye solo una conectividad de malla completa entre todas las sucursales de la empresa, sin conectarse a una puerta de enlace en la nube. Esta solución es apropiada para empresas que alojan todas sus aplicaciones internamente, es decir no utilizan aplicaciones en la nube. Su combinación apropiada con una red MPLS básica funcionaría adecuadamente; para aplicaciones en tiempo real se usaría MPLS y para todo lo demás la SD-WAN [17]. Por lo tanto, sus ventajas son:

- Costos mensuales de ancho de banda bajos o nulos en la nube SD-WAN.
- Modelado de tráfico en tiempo real, mejorando el rendimiento de todas las aplicaciones.
- Mejor recuperación ante desastres, al tener una buena conectividad de *backup.*

En segundo lugar, SD-WAN habilitada para la nube, destinada principalmente para empresas que desean optimizar el rendimiento y confiabilidad de sus aplicaciones en la nube, ya que la puerta de enlace de la nube se conecta directamente con los principales proveedores como *Office365, Salesforce,* etc. Los beneficios son similares a la arquitectura anterior, a diferencia de una conectividad de *backup* mejorada y el rendimiento de aplicaciones en la nube [17].

Finalmente, la solución SD-WAN híbrida que combina las arquitecturas mencionadas anteriormente. Es capaz de proporcionar una infraestructura WAN de malla completa confiable y conectividad a la nube de alto rendimiento. Este modelo híbrido permite mayor flexibilidad, sin embargo, en aspectos de configuración y seguridad se vuelve más complejo que las soluciones anteriores. [15]

1.3.4.6 Beneficios de la SD-WAN [9]

En esta sección se detallan los beneficios de la SD-WAN respecto a las WAN tradicionales y, posteriormente se hace una comparación con las tecnologías MPLS e IPsec VPN. Las principales ventajas de la solución WAN definida por *software* que carece la WAN tradicional son las siguientes:

- Reducción de costos de circuito al utilizar opciones de conectividad de menor costo y mayor velocidad.
- Rentabilidad y fuerte impacto en redes empresariales: los límites geográficos desaparecen y el modelo de pago es en función del crecimiento.
- Mejora la visibilidad, es decir, identifican de manera inteligente las aplicaciones desde el primer paquete de tráfico de datos, con el fin de tomar decisiones más inteligentes.
- Control de múltiples rutas ya que permite diferentes conexiones para que fluya el tráfico como MPLS, conexión de banda ancha, un túnel IPsec, etc.
- Reduce la complejidad, es decir, su administración y control es a través de un único panel, el cual tiene una interfaz gráfica amigable para el usuario.
- Adopción de servicios basados en la nube. El tráfico en las WAN tradicionales generalmente pasa por el centro de datos para permitir un filtrado constante; esto origina una mayor latencia para servicios alojados en la nube. Por lo tanto, con SD-WAN se elimina la necesidad del tráfico de *backhaul* [11] y mejora el rendimiento de aplicaciones en la nube.
- SD-WAN proporciona *QoS* ya que realiza un monitoreo de tráfico en tiempo real.
- Capacidad de admitir aplicaciones de gran ancho de banda de manera simultánea.
- Alto nivel de seguridad al contar con funciones como cifrado extremo a extremo y autenticación de los dispositivos.
- Tiempos de implementación más cortos ya que no necesita contar con una planificación anticipada, ni apoyo logístico para su implementación (ZTP). Por lo tanto, mejora la escalabilidad.

[11] ***Backhaul*****:** *en el ámbito de telecomunicaciones se refiere a una red de retorno hacia el centro de datos.*

1.3.4.6.1 SD-WAN vs MPLS vs IPsec VPN **[5]**

A continuación, se establece una comparación de la SD-WAN con MPLS, debido a que es la tecnología WAN más utilizada en los últimos años; y, posteriormente se la compara con IPsec. En la Tabla 1.2., se muestran las ventajas de cada tecnología.

Tabla 1.2. Ventajas de SD-WAN y MPLS

SD-WAN	MPLS	IPsec VPN
Costos más bajos	Confiabilidad o fiabilidad	Confidencialidad
Adaptación a la Nube	Alto nivel de QoS	Integridad
Seguridad Garantizada	Escalabilidad	Independencia de la Aplicación
Escalabilidad		
Elimina limitaciones de Ancho de Banda		
Administración más sencilla		

En primer lugar, se analizan las ventajas de SD-WAN. Respecto al costo, varían de acuerdo con el tipo de despliegue, por ejemplo, si no es una SD-WAN administrada reduce considerablemente los gastos de operación. De todas formas, cualquier tipo de despliegue SD-WAN resulta más conveniente, en comparación con MPLS.

La adaptación a la nube es una ventaja que simplemente MPLS no puede proporcionar y que es fundamental para empresas que necesitan acceso instantáneo a aplicaciones de negocios en la nube.

SD-WAN garantiza la seguridad, en vista de que proporciona cifrado completo de todas las conexiones basado principalmente en IPsec y SSL, a diferencia de MPLS que separa el tráfico mediante VPNs que lo protegen del Internet, pero no del ISP.

La escalabilidad se mejora en SD-WAN, ya que cada dispositivo de borde tiene la característica *plug-and-play*[12] que permite la incorporación rápida de sucursales a la WAN actual.

[12] ***Plug and play*****:** *dispositivos que funcionan con un sistema informático tan pronto como se conectan.*

SD-WAN usa conectividad a Internet, lo que permite a los clientes actualizar su suscripción a Internet con base en las necesidades y así eliminar los límites de ancho de banda rápidamente. En MPLS por su parte, el ancho de banda del canal de comunicaciones requiere tiempo y un alto costo.

La administración de red es mucho más sencilla, ya que SD-WAN proporciona un control sobre toda la red WAN a través de una interfaz gráfica simple.

Por otro lado, se encuentran las ventajas de MPLS. La más importante es su fiabilidad debido a que usa un mecanismo orientado a la conexión que proporciona un canal privado virtual para cada VPN del cliente. Lamentablemente, SD-WAN no puede proporcionar el mismo nivel de fiabilidad que MPLS, ya que usa la infraestructura pública de Internet como red de transporte. De esta manera, lo correcto sería usar MPLS y complementarlo con SD-WAN.

A pesar de que MPLS no proporciona mecanismos de QoS basados en aplicaciones como SD-WAN, aun se considera muy eficiente su mecanismo de conmutación de etiquetas que permite una manipulación del tráfico de manera eficiente. Además, MPLS es altamente escalable al igual que SD-WAN, sin embargo, lo que le llevaría más tiempo es la implementación del servicio de VPNs.

Finalmente, es importante mencionar que IPsec se considera como un producto complementario de otras soluciones WAN, especialmente de SD-WAN. Sus dos principales ventajas son la confidencialidad e integridad que hacen que IPsec tenga la máxima seguridad para comunicación por Internet. [5] Además, no existen problemas de compatibilidad de aplicaciones a través de la solución de VPNs.

1.3.4.7 Desventajas de la SD-WAN

Es importante conocer las desventajas que presenta la solución SD-WAN, con el fin de fortalecer las áreas donde presentan debilidades y así maximizar el rendimiento de la SD-WAN. A continuación, se detallan las desventajas:

1. Gestión e implementación, es decir, que es esencial contar con personal de TI que pueda planificar, diseñar y mantener esta solución [6].
2. El sistema no es completamente inmune al rendimiento lento, ya que existe la posibilidad de *jitter* y pérdida de paquetes al depender de la conectividad pública de Internet [6].

1.3.4.8 Análisis de seguridad en la SD-WAN

La solución SD-WAN es un reemplazo para la red existente basada en MPLS, la cual se considera confiable y segura durante los últimos años. Por otro lado, SD-WAN usa como transporte de datos la infraestructura pública de Internet que no es lo suficientemente segura. Esta solución utiliza las últimas tecnologías, tales como SDN y encapsulación que no son consideradas tan estables y seguras como MPLS en la industria [18]. SDN tiene muchas vulnerabilidades de ser atacada en comparación con las WAN tradicionales.

Uno de los problemas surge debido a que cuentan con un controlador centralizado, que puede ser un punto único vulnerable a ataques y fallas, afectando a toda la red. Otra vulnerabilidad es cuando los piratas informáticos pueden engañar a los ingenieros para instalar aplicaciones que comprometan la seguridad de la red [18].

Existen vulnerabilidades en el manejo del CPE (*Customer Premises Equipment*), ya que se configura automáticamente en el sitio del cliente, mientras que con MPLS son aprovisionados y desplegados por un administrador de red que viaja al sitio remoto [18].

Teniendo en cuenta todos estos factores, es necesario analizar la solución SD-WAN desde la perspectiva de seguridad, que permita identificar sus áreas vulnerables a ataques. Esto con el fin de proponer contramedidas para mitigar ataques en el futuro. Una de ellas, es usar la tecnología FORTINET que se destaca frente a otros proveedores por el aspecto de seguridad, gracias a su experiencia y trayectoria. Posteriormente, se explica a detalle cómo maneja FORTINET la seguridad en el despliegue de la SD-WAN.

1.3.5 REDES DE ACCESO

Conceptualmente, la red de acceso llamada también de última milla hace referencia al segmento de la red de telecomunicaciones que brinda conexión a los usuarios finales con la red del proveedor [35].

1.3.5.1 Arquitectura de la Red de Acceso

Para una mejor comprensión, en la Figura 1.11. se muestra la arquitectura de un tipo de red de acceso alámbrica. En este caso, es una red de acceso *Digital Subscriber Line* (DSL), que interconecta los usuarios finales con el proveedor de servicio; cuenta con un servidor de acceso remoto de banda ancha (BRAS[13]) y el multiplexor (DSLAM[14]) [36].

[13] **BRAS:** *Broadband Remote Access Server, enruta el tráfico hacia y desde dispositivos de acceso remoto de banda ancha (DSLAM) en un proveedor de servicios de Internet de la red (ISP).*
[14] **DSLAM:** *Digital Serial Line Access Multiplexer, encargado de multiplexar varias interfaces de clientes en un canal digital de comunicaciones.*

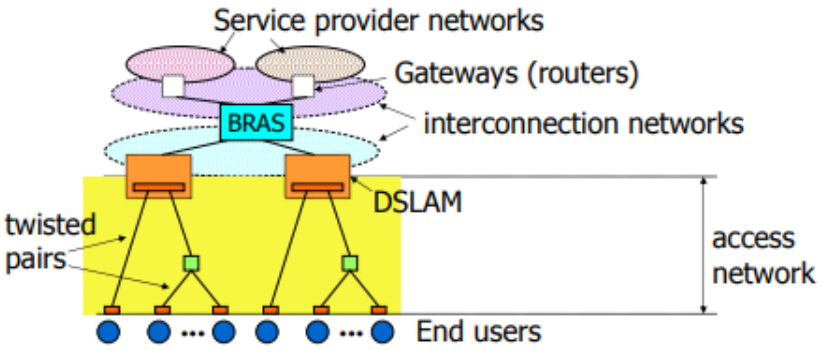


Figura 1.11. Arquitectura de una red de acceso DSL [36]

1.3.5.2 Tipos de Tecnologías de Acceso

En la Figura 1.12. se visualizan los distintos tipos de tecnologías de acceso, divididos en grupos: las redes de acceso cableadas y las inalámbricas.

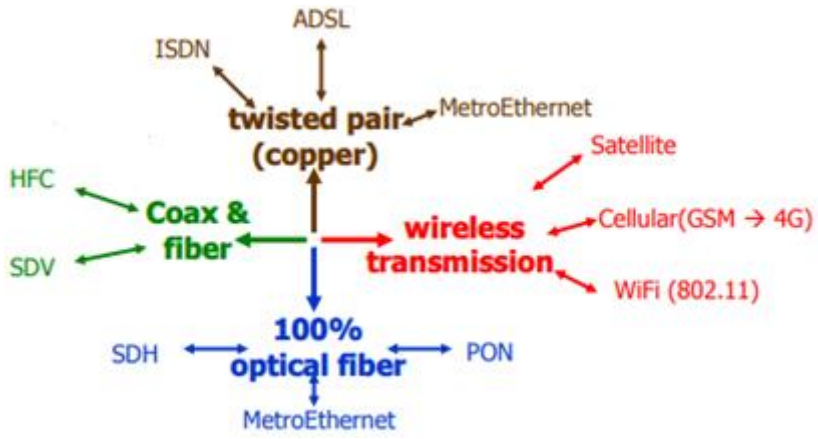


Figura 1.12. Tipos de red de acceso [36]

1.3.6 GRAPHICAL NETWORK SIMULATOR (GNS3)

Es una herramienta muy utilizada por ingenieros en redes y telecomunicaciones, con el fin de emular, configurar, probar y solucionar problemas de redes, tanto virtuales como reales. A pesar de que irónicamente las siglas de su nombre se refieren a este *software* como un simulador, GNS3 admite tanto dispositivos de red emulados como simulados. GNS3 originalmente solo emulaba dispositivos CISCO a través de un *software* llamado *Dynamips* [19]. Actualmente, ha evolucionado a tal punto que admite diferentes dispositivos de múltiples proveedores de red como FORTINET, JUNIPER y muchos otros más.

Es un programa *Open Source*[15], que se utiliza para emular varios sistemas operativos en un entorno virtual y está estrechamente vinculado con:

[15] ***Open Source:*** *software de código abierto, es decir diseñado de manera que sea accesible gratuitamente al público para que puedan verlo, modificarlo y distribuirlo.*

- *Dynamips:* es un emulador de dispositivos CISCO, es decir proporciona las ISO de estos equipos directamente en los enrutadores emulados en el programa [19].
- *Qemu:* es una plataforma de virtualización y emulación de hardware de código abierto [19].
- *Virtualbox* y *VMware:* programas de virtualización.
- *Wireshark:* es un analizador de protocolos de red.

1.3.6.1 Arquitectura de GNS3

El programa GNS3 consiste de dos principales componentes: *software* GNS3 y máquina virtual GNS3.

1.3.6.1.1 Software GNS3

Hace referencia a la interfaz gráfica de usuario (GUI) y la parte de *software* necesaria para la operación de GNS3. Este componente instala el *software "todo en uno"* en la PC local, ya sea sistema operativo de Windows, Mac o Linux; la instalación de este componente sin la máquina virtual es suficiente, siempre y cuando el usuario solo desee crear topologías básicas utilizando enrutadores CISCO. Por lo tanto, su configuración es limitada y no ofrece tantas opciones respecto a la topología y dispositivos admitidos [19].

1.3.6.1.2 Máquina virtual GNS3

Se puede ejecutar la máquina virtual de GNS3 en la misma PC o de forma remota en un servidor, con el fin de que los dispositivos creados en la GUI estén alojados y ejecutados por una máquina virtual o un servidor local. La opción más recomendada es a través de VMware Workstation o Virtualbox; el objetivo de su instalación en conjunto con el *software* GNS3 es para crear topologías más avanzadas o si se desea incluir diferentes dispositivos de red que requieran la plataforma QEMU, como los equipos FortiGate, FortiManager, FortiAnalyzer, entre otros [19].

1.3.6.2 Emulación y simulación en GNS3

GNS3 es un *software* que emula o imita el hardware de un dispositivo y ejecuta imágenes reales en el dispositivo virtual, sin tener el problema de comandos no reconocidos o no funcionales, como por ejemplo copiar la ISO de un dispositivo y ejecutarlo en un dispositivo emulado en GNS3 [19]. Sin embargo, GNS3 también simula las funciones de dispositivos, en los cuales no se ejecutan sistemas operativos reales como por ejemplo los *switches* y *hubs* que son simulados por el programa.

1.3.6.3 Requerimientos de GNS3

En la Tabla 1.3. se muestran los requisitos, que son los recomendados para un entorno avanzado de GNS3, con el objetivo de aprovechar al máximo sus características de virtualización y emulación.

Tabla 1.3. Requerimientos óptimos de GNS3 [19]

ITEM	REQUERIMIENTOS ÓPTIMOS
Sistema Operativo	Windows 10 (64 bit)
Procesador	i7 CPU, 8 o más núcleos lógicos – AMD-V / RVI Series o Intel VT-X
Virtualización	Se requieren extensiones de virtualización. Es posible que se deba habilitar esto, a través del BIOS de la computadora.
Memoria	16-32 GB RAM
Espacio en disco	Disco de Estado Sólido (SSD) con 80 GB de espacio disponible
Notas adicionales	La virtualización de dispositivos consume mucho procesador y memoria, por lo tanto, mientras más se aumente es mejor. Tener en cuenta si el dispositivo configurado supera la RAM y el procesador.

1.3.6.4 Ventajas y desventajas de GNS3

El *software* GNS3 ofrece ventajas significativas en comparación con otros simuladores de red, como el mismo *Cisco Packet Tracer.* Sin embargo, así como posee grandes virtudes presenta también ciertas particularidades que se detallan en la Tabla 1.4.

Tabla 1.4. Ventajas y Desventajas de GNS3

VENTAJAS	DESVENTAJAS
Compatibilidad con diferentes sistemas operativos.	Instalación con máquina virtual resulta un tanto compleja.
Es *Open Source.*	Consume gran cantidad de recursos en RAM
GUI amigable y fácil de entender.	ISO no vienen incluidas en el *software.*
Trabaja con ISO de dispositivos reales.	
Análisis de la red emulada en tiempo real.	
Conexión de la red emulada a un entorno real.	
Uso de Wireshark para captura de paquetes.	
Suficiente documentación y soporte directo en el sitio web de GNS3.	

1.3.7 FORTINET

Es una empresa multinacional de Estados Unidos que se dedica al desarrollo y comercialización de *software*, dispositivos y servicios de ciberseguridad, como *firewalls*, antivirus, sistema de prevención de intrusos, entre otros [20]. La arquitectura FORTINET Security Fabric aborda los desafíos de seguridad más críticos, ya sea entornos de red de aplicaciones, en la nube o móviles y ofrece una verdadera plataforma de ciberseguridad que proporciona:

- Amplia visibilidad de toda la superficie de ataque digital, para gestionar mejor los riesgos [20].
- Flujos de trabajo automatizados para aumentar la velocidad de las operaciones y las respuestas [20].

FORTINET ofrece muchos productos de *software* y *hardware* destinados a servicios de conexión, VoIP[16], autenticación, SD-WAN y otras aplicaciones. Entre los más destacados se encuentran los dispositivos FortiGate, FortiManager, y FortiAnalyzer que se explican a detalle, en conjunto con la funcionalidad de *Secure SD-WAN,* debido a que son temas relevantes por ser parte de la emulación.

1.3.7.1 SD-WAN Segura

La SD-WAN a más de ofrecer un adecuado manejo de aplicaciones, mejora el rendimiento para aplicaciones de *Software* como Servicio (SaaS) y servicios de comunicación unificada. Sin embargo, una de las principales deficiencias de las SD-WAN es la seguridad, por el hecho de acceder directamente al Internet.

Tomando en cuenta esta deficiencia, *Secure SD-WAN* de FORTINET incluye una de las mejores funcionalidades de seguridad como NGFW[17] y otras como SD-WAN, teniendo como resultado un despliegue unificado con estas dos características. Por lo tanto, la *Secure SD-WAN* tiene como fin reducir costos, simplificar las operaciones, mejorar el rendimiento, habilitar una postura de alta seguridad y proporcionar un mecanismo de control centralizado que pueda determinar y enrutar la trayectoria ideal para el tráfico [21].

A continuación, se describen las principales razones por las que *Secure* SD-WAN es una de las mejores opciones, tanto para microempresas como para macroempresas. Algunas de las empresas que cuentan con su servicio se muestran en la Figura 1.13.

[16] **VoIP:** *voz sobre el protocolo de Internet.*
[17] **NGFW:** *Next Generation Firewall, cuenta con capacidades adicionales como conocimiento y control de aplicaciones, inteligencia de amenazas entregada en la nube, etc.*

Figura 1.13. Empresas con el servicio SD-WAN de FORTINET [21]

- FORTINET ofrece capacidades de seguridad, enrutamiento avanzado, optimización WAN y redes SD-WAN en un único dispositivo. Respecto a la seguridad NGFW, ofrece mejoras en la detección y solución frente a ataques. Es importante mencionar que es el único vendedor de SD-WAN que ofrece inspección SSL [21].
- Mejora el rendimiento de aplicaciones en la nube, es decir, prioriza aplicaciones críticas de las empresas, a través de un balanceo WAN eficiente [21].
- Administración Centralizada, es decir, gestiona por completo a través de un único panel amigable para el usuario, mejorando la escalabilidad y garantizando que su organización pueda acceder rápida y fácilmente a las aplicaciones en la nube [21].
- Bajo TCO (*Total Cost Ownership*): mejora del TCO hasta en un 50% comparado con arquitecturas tradicionales [21].
- Implementación remota: Aprovisionamiento automático del dispositivo (ZTP).

En la Figura 1.14., se muestra el cuadrante mágico de Gartner respecto al despliegue de infraestructura WAN, en el cual se puede visualizar los mejores proveedores o líderes en el ambiente WAN actual, uno de ellos FORTINET.

Figura 1.14. Cuadrante Mágico de Gartner de infraestructura WAN [21]

1.3.7.2 FortiGate

Es un dispositivo o *software* que puede considerarse como "*todo en uno".* Permite la creación de redes basadas en la seguridad, que incluye un sistema de prevención de intrusos (IPS), filtrado web, inspección SSL, SD-WAN, entre otros. Estos dispositivos satisfacen las necesidades de rendimiento de arquitecturas de TI híbridas altamente escalables, lo que permite a las organizaciones reducir la complejidad y administrar los riesgos de seguridad [22]. Puede ser desplegado como *hardware* local o administrado, máquina virtual, o SaaS en la nube. Los dispositivos de *hardware* de nivel de entrada comienzan en alrededor de $500, y los precios empresariales de gama alta pueden alcanzar los $350,000 en el caso del 7060E-8 [23].

1.3.7.3 FortiManager

Los equipos FortiManager permiten la gestión, administración y configuración de manera centralizada de miles de dispositivos FORTINET, incluidos equipos FortiGate, FortiAnalyzer, FortiSwitch, que estén dentro del entorno de comunicaciones. FortiManager ofrece un TCO más bajo al minimizar tanto los costos iniciales de implementación, como los gastos operativos continuos. Es uno de los dispositivos más versátiles que proporciona una diversa gama de despliegues, flexibilidad de crecimiento, gestión de actualizaciones, monitorización, administración sencilla, rápido aprovisionamiento y configuración, integración con FortiAnalyzer, etc [22]. Al igual que FortiGate puede ser desplegado de manera física o virtual.

1.3.7.4 FortiAnalyzer

Este dispositivo provee de una potente herramienta de gestión y análisis de registros, generación periódica y automatizada de informes configurables por el administrador, ejecución de diferentes utilidades de diagnóstico, así como herramientas complementarias de análisis de vulnerabilidades o *scanning* de red. Además, permite reportar y almacenar eventos de seguridad, tráfico de red, contenido web y mensajes para medir el cumplimiento de políticas de una organización [22]. Se sincroniza completamente con FortiManager como punto central de control, es decir, que el manejo tanto de las funcionalidades de FortiAnalyzer como de FortiManager se lo realiza desde un único dispositivo y está disponible a través de *hardware* o de modo virtual.

La ventaja de estos tres dispositivos es que su interfaz gráfica es bastante amigable con el usuario, por lo que un administrador de redes puede entender fácilmente el despliegue de la red o encontrar de manera más eficiente problemas o fallas.

2. METODOLOGÍA

En este capítulo se presenta un análisis del funcionamiento de la red SD-WAN Híbrida, previo a la configuración de los equipos. En primer lugar, se definen las funciones de MPLS, así como políticas, reglas y otros, con el objetivo de comprender cómo va a trabajar la red antes de ser emulada. Posteriormente, se detalla la configuración de cada dispositivo.

2.1 SOFTWARE GNS3

Previo al análisis de la SD-WAN Híbrida, se describen los recursos utilizados para la instalación del *software* GNS3 con su máquina virtual. Además, se adjunta un manual de instalación y configuración en el ANEXO A, en el cual se detalla cada uno de los pasos para el funcionamiento óptimo de éste.

GNS3 es un emulador de redes que incluye un conjunto de funcionalidades e imágenes de dispositivos de diversos fabricantes que permiten a los ingenieros en redes y telecomunicaciones evitar posibles errores o compras innecesarias de dispositivos en una implementación real. La elección de GNS3 fue principalmente por 3 razones: es *Open Source,* es capaz de emular topologías complejas y está disponible para Windows o Linux.

Los recursos utilizados para la instalación y manejo avanzado de GNS3 son los siguientes: un computador con Windows 10, i7-2.6 GHz de procesador, 6 núcleos, 16 GB de RAM, puerto ethernet, acceso a Internet de buena velocidad y las ISO de los dispositivos. En caso de no disponer de estos recursos, en el ANEXO A se especifican los requerimientos mínimos necesarios para su instalación y se indica el proceso para agregar las imágenes de los dispositivos a GNS3.

2.2 ANÁLISIS DE LA ARQUITECTURA DE RED

En este apartado se analiza la topología de la red y se definen los parámetros de direccionamiento, políticas, tipo de seguridad, entre otros aspectos. El objetivo es analizar el funcionamiento de toda la red antes de la emulación, de tal manera que se entienda cómo trabaja una SD-WAN, antes de configurar cada uno de sus parámetros.

2.2.1 TOPOLOGÍA DE LA RED

En esta sección se detalla la topología de la red, componentes de las redes de área local, red de área extendida, SD-WAN y remota, con sus respectivas ubicaciones.

La arquitectura de red está formada por tres LANs (*Local Area Network*), las cuales se encuentran ubicadas en tres ciudades del Ecuador, cumpliendo cada una distintos papeles. En primer lugar, existe una LAN en la ciudad de Guayaquil que actúa como sede principal,

es decir cuenta con recursos a los cuales las otras LAN necesitan acceder y es el punto de control centralizado de toda la red, como se muestra en la Figura 2.1.

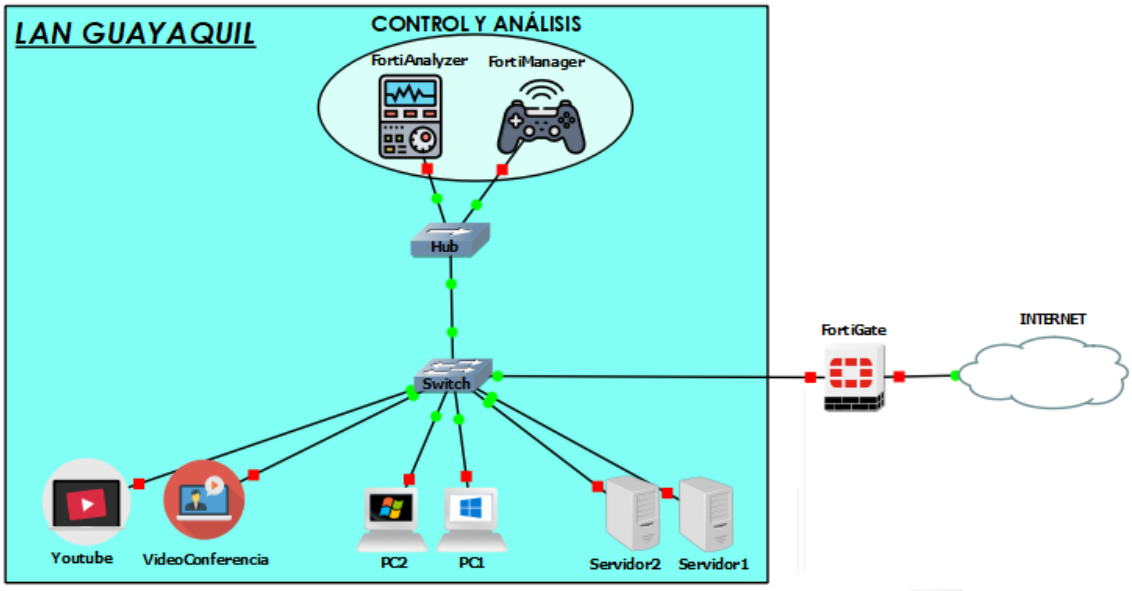


Figura 2.1. Topología LAN Guayaquil

En segundo lugar, existe una LAN en la ciudad de Quito que actúa como un Centro de Datos; al igual que la sede de Guayaquil cuenta con recursos a los cuales las otras LAN necesitan acceder, como se muestra en la Figura 2.2.

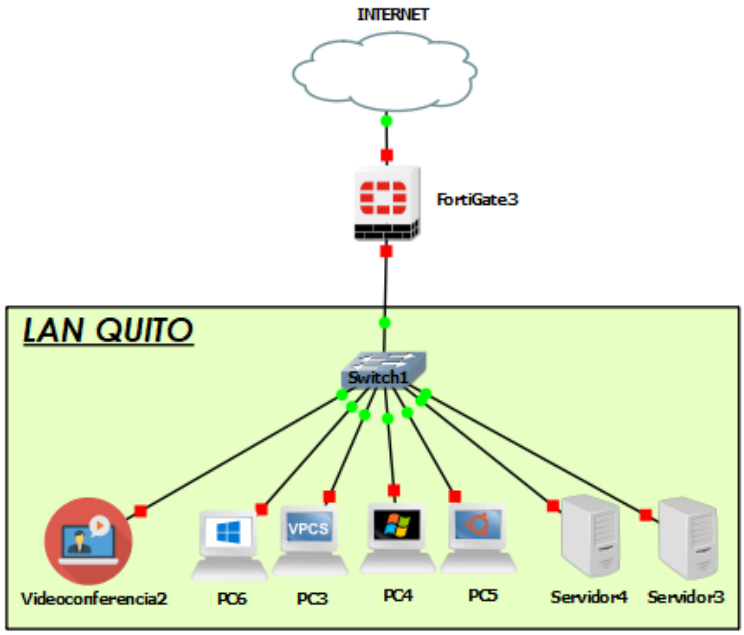


Figura 2.2. Topología LAN Quito

En la Figura 2.3., se visualiza una LAN ubicada en la ciudad de Ambato que actúa simplemente como una sucursal, es decir que necesita acceder a los recursos tanto de la

LAN de Quito como de Guayaquil, pero ésta no cuenta con recursos debido a que su rol es mucho más sencillo que el de un Centro de Datos o una sede principal.

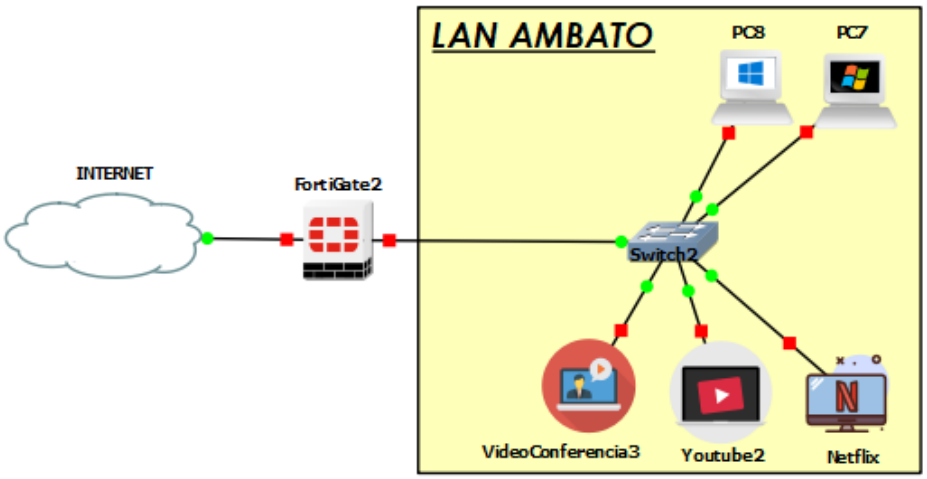


Figura 2.3. Topología LAN Ambato

Además, existe una red MPLS que representa la infraestructura de red tradicional de una empresa con el fin de evidenciar que se puede mantener la infraestructura MPLS para que funcione en conjunto con la SD-WAN. Es importante aclarar que la LAN de Ambato no está conectada a la red MPLS, a fin de comprobar su funcionamiento al utilizar como solución únicamente la SD-WAN. De este modo, se tienen los dos escenarios dentro de la emulación para un mejor entendimiento.

Posteriormente, se explica a detalle el funcionamiento de la red MPLS, de tal manera que en la Figura 2.4., se visualiza un esquema de su topología.

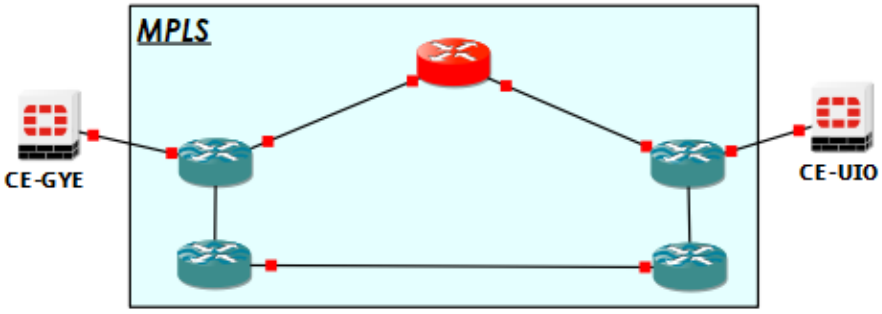


Figura 2.4. Topología de la red MPLS

Finalmente, en la Figura 2.5. se visualiza la topología completa de la red con los enlaces de acceso a Internet, la nube de acceso remoto y todas las áreas mencionadas anteriormente. Posteriormente, se define el direccionamiento IP y se explica a detalle el funcionamiento de cada una de las redes de área local y extendida, con sus dispositivos internos.

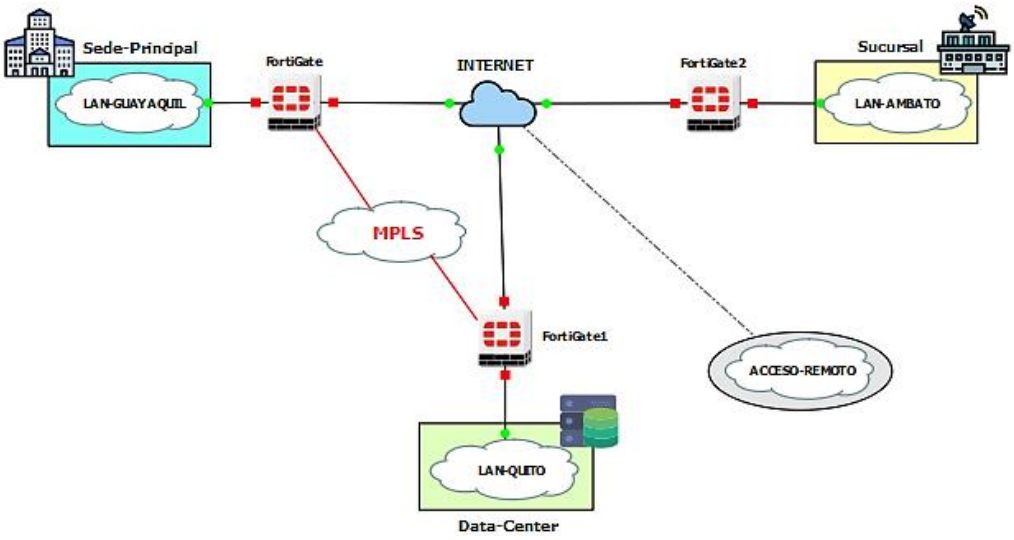


Figura 2.5. Topología completa de la red

2.2.2 DIRECCIONAMIENTO IP

En este apartado, se detalla el direccionamiento IP que consiste en la asignación de una dirección IP a cada uno de los equipos pertenecientes a la empresa, para que puedan hacer uso de los servicios que la red brinda. En este caso, por ser una emulación se han utilizado direcciones IP privadas para toda la red; en la realidad se haría uso de direcciones IP públicas ofrecidas por el ISP para el acceso a Internet.

En la Tabla 2.1. se muestran los rangos de direcciones IP privadas para las clases A, B y C, con el fin de tener una mejor comprensión sobre el direccionamiento. En general, la red cuenta con una sede, un Centro de Datos y una sucursal; por lo tanto, con el propósito de diferenciar las redes de área local o la red de área extendida, la red MPLS y la red de acceso remoto se usan direcciones de clase A, clase B y clase C, respectivamente.

Tabla 2.1. Clases de direcciones IP privadas

TIPO	RANGO DE DIRECCIONES	
	DESDE	HASTA
CLASE A	10.0.0.0	10.255.255.255
CLASE B	172.16.0.0	172.31.255.255
CLASE C	192.168.0.0	192.168.255.255

Tomando en cuenta que el enfoque no es el direccionamiento IP, no se ha utilizado VLSM[18] sino que se ha usado una simple distribución de direcciones IP de clase A para cada LAN

[18] **VLSM:** *Variable Length Subnet Mask.- Método para optimizar el uso de direcciones IP, se emplea cuando subredes dentro de una misma red requieren máscaras de diferente longitud.*

y conexiones de banda ancha de Guayaquil, Quito y Ambato; IP de clase B para la red MPLS e IP de clase C para la LAN de acceso remoto. Partiendo desde una IP privada de cada clase, en la Tabla 2.2. se muestra la organización de las direcciones IP de toda la red.

Tabla 2.2. Distribución de direcciones IP para la emulación

LAN/WAN	Red	IP Inicial	IP Final (Gateway)	IP de Broadcast
LAN-GYE	10.10.1.0/24	10.10.1.1	10.10.1.254	10.10.1.255
LAN-UIO	10.10.2.0/24	10.10.2.1	10.10.2.254	10.10.2.255
LAN-AMB	10.10.3.0/24	10.10.3.1	10.10.3.254	10.10.3.255
WAN-GYE	10.200.1.0/30	10.200.1.1	10.200.1.2	10.200.1.3
	10.200.2.0/30	10.200.2.1	10.200.2.2	10.200.2.3
	10.200.3.0/30	10.200.3.1	10.200.3.2	10.200.3.3
WAN-UIO	10.200.6.0/30	10.200.6.1	10.200.6.2	10.200.6.3
WAN-AMB	10.200.7.0/30	10.200.7.1	10.200.7.2	10.200.7.3
	10.200.8.0/30	10.200.8.1	10.200.8.2	10.200.8.3
WAN-MPLS	172.16.5.0/30	172.16.5.1	172.16.5.2	172.16.5.3
	172.16.5.4/30	172.16.5.5	172.16.5.6	172.16.5.7
	172.16.5.8/30	172.16.5.9	172.16.5.10	172.16.5.11
	172.16.5.12/30	172.16.5.13	172.16.5.14	172.16.5.15
	172.16.5.16/30	172.16.5.17	172.16.5.18	172.16.5.19
	172.16.5.20/30	172.16.5.21	172.16.5.22	172.16.5.23
	172.16.5.24/30	172.16.5.25	172.16.5.26	172.16.5.27
LAN-REMOTA	192.168.1.0/24	192.168.1.1	192.168.1.254	192.168.1.255
WAN-REMOTA	10.200.5.0/30	10.200.5.1	10.200.5.2	10.200.5.3

En la Figura 2.6, se visualiza la topología de la red junto con el direccionamiento, de manera que se pueda tener una mejor comprensión de la distribución de las direcciones IP, especialmente de los enlaces WAN. Basados en la Tabla 2.2. en la WAN-GYE se tienen tres enlaces con el fin de tener alta disponibilidad al ser considerada como sede principal; éstos pueden ser del mismo o de diferente ISP. En la WAN-UIO solo existe un enlace ya que al no ser considerada como sede principal, en caso de alguna caída o saturación puede utilizar la red MPLS. Finalmente, en la WAN-AMB como redundancia se consideran dos enlaces, ya que la sucursal de Ambato no tiene conexión con la red MPLS.

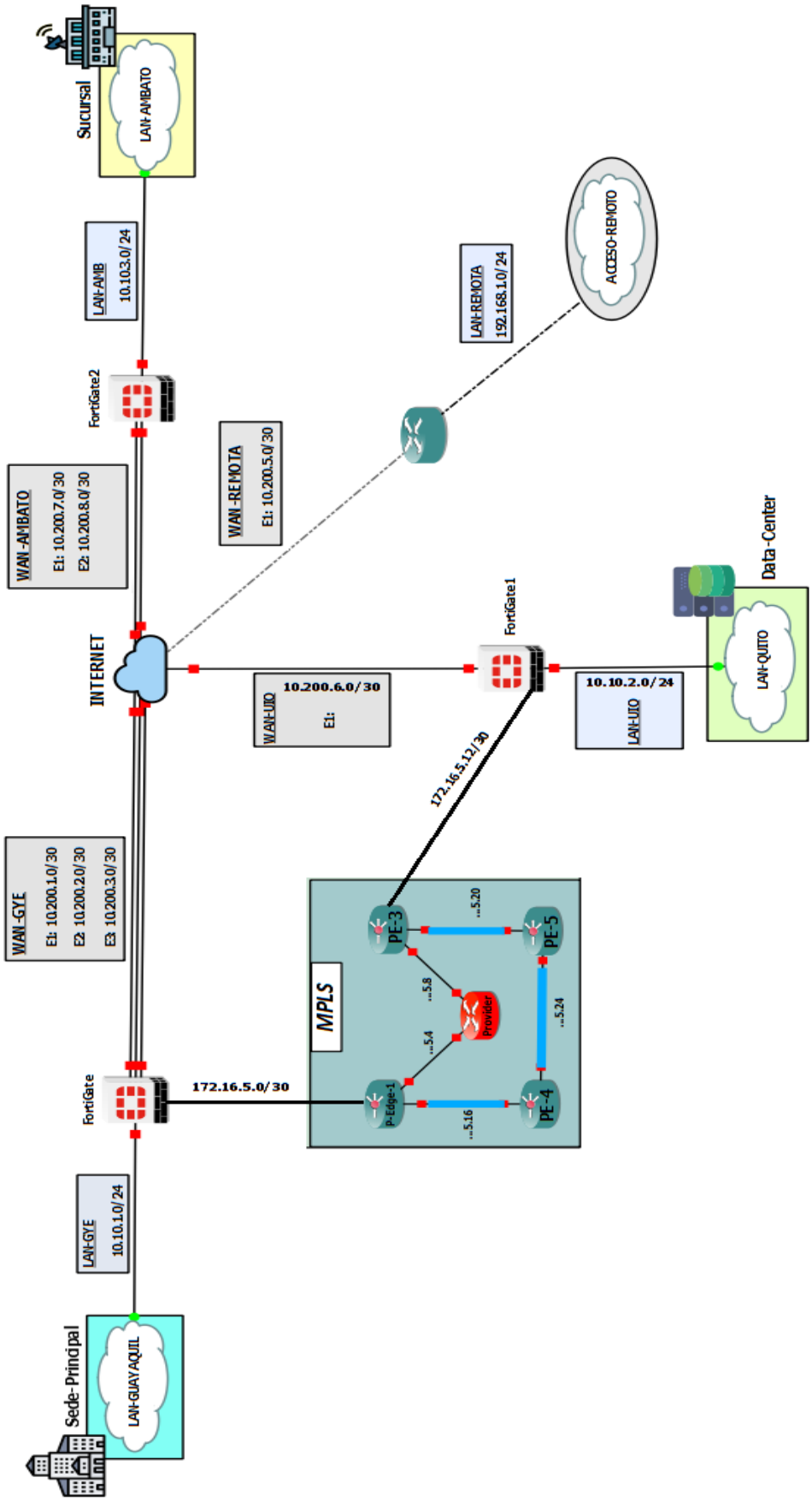


Figura 2.6. Direccionamiento IP y topología de la red emulada

2.2.3 FUNCIONAMIENTO DE LAS REDES DE ÁREA LOCAL

En esta sección, se describe el rol de cada LAN ubicada en Guayaquil, Quito y Ambato y de cada uno de los dispositivos que las conforman.

2.2.3.1 LAN Guayaquil

El rol que cumple la LAN Guayaquil es el de una sede central o principal, es decir donde se concentran la mayoría de las funciones importantes o desde donde se emiten las órdenes; se considera como el punto central de administración de sedes secundarias, de Centros de Datos y sucursales de una organización.

La red de área local ubicada en Guayaquil está dividida en 4 zonas: un área de servidores como recurso necesario para que las otras LAN accedan, un área de atención al cliente para que los empleados realicen actualizaciones o procesos simples de trabajo, un área de control para administrar todas las LAN desde un único punto (sede principal) y un área de teletrabajo para realizar videoconferencias.

Tomando en cuenta los recursos máximos de memoria RAM y procesador, se ha dispuesto usar un servidor DNS[19] y un servidor TFTP[20] en el área de servidores, 2 PCs en el área de atención al cliente, 2 PCs en el área de teletrabajo y 1 dispositivo en el área de control conocido como FortiManager con las funcionalidades de FortiAnalyzer que se explican a detalle posteriormente. En la Figura 2.1. de la sección de topología se puede visualizar cada uno de los dispositivos de la LAN Guayaquil.

La posibilidad de incrementar los dispositivos en cada área depende de los recursos de hardware de la PC utilizada en la emulación; en este caso se está ocupando el 100 % de los recursos disponibles, ya que el dispositivo de control y administración ocupa gran cantidad de memoria RAM (4096 *Megabytes*) y procesador.

2.2.3.2 LAN Quito

La red de área local de Quito actúa como un Centro de Datos, que está compuesto de servidores y computadores en red con el fin de procesar, almacenar y difundir grandes cantidades de datos. Por lo general, las empresas dependen de los servicios y datos contenidos en un Centro de Datos, lo que le convierte en un punto muy importante de la red, ya que contiene recursos necesarios a los cuales las otras redes necesitan acceder.

La LAN de Quito está dividida en 3 zonas, las cuales son idénticas a las de Guayaquil, a excepción del área de control que permite la administración de toda la organización. Esta

[19] **DNS:** *Domain Name System.- Sistema encargado de la traducción de nombres a direcciones IP.*
[20] **TFTP:** *Trivial File Transfer Protocol.- Permite transferir archivos de manera más fácil que FTP.*

área no se dispone en Quito ya que el control se lo hace desde un único punto central, en este caso la sede principal, ya que no tendría sentido tener más de un punto de control porque esto incrementaría el costo de adquisición de dispositivos de administración.

Los dispositivos instalados en Quito corresponden a un servidor de Correo y un servidor Syslog en el área de servidores, 3 PCs en el área de atención al cliente y 1 PC en el área de teletrabajo. En la Figura 2.2. de la sección de topología se puede visualizar cada uno de los dispositivos de la LAN ubicada en Quito.

2.2.3.3 LAN Ambato

Finalmente, la red de área local ubicada en Ambato actúa como una sucursal, ya que es una oficina más pequeña y remota con un menor número de funcionalidades y sin ningún recurso o servidor al cual las otras redes tengan que acceder. De esta manera, la LAN de Ambato está dividida solamente en 2 zonas: el área de atención al cliente y el área de teletrabajo. Por lo tanto, no cuenta con servidores ni con dispositivos de administración, ya que cumple el rol de una sucursal. En la Figura 2.3. de la sección de topología se puede visualizar cada uno de los dispositivos de la sucursal en Ambato.

2.2.4 FUNCIONAMIENTO DE SERVIDORES

En esta sección, se explica a detalle los servidores que van a ser utilizados en las redes de área local y cómo va a funcionar cada uno de ellos. Un servidor se desarrolla en un hardware típico que ejecuta un *software* específico con el fin de proporcionar servicios a otros dispositivos conocidos como clientes. Existen 4 servidores que se van a instalar: servidor DNS, servidor de Correo, servidor de Transferencia de Archivos y servidor Syslog.

2.2.4.1 Servidor DNS

En primer lugar, el *Domain Name System* (DNS) se lo puede describir como la agenda telefónica de Internet o un sistema compuesto por muchos servidores DNS organizados en una jerarquía. Los usuarios acceden a la información en línea a través de nombres de dominio amigables como "*google.com"* o "*gns3.com"* y el DNS es el responsable de la traducción de los nombres de dominio a direcciones IP para que los navegadores web puedan cargar recursos de Internet [24].

Un servidor DNS es el componente principal que implementa el protocolo DNS; tiene un índice de nombres de dominio y direcciones IP, de tal manera que cuando se lo solicite, puede indicar la dirección actual asociada con un nombre de dominio, o averiguarlo en otros servidores DNS raíz o maestros si no lo conoce [25]. Diseñado para ubicar y entregar fácilmente sitios web a usuarios finales a través de Internet o una red privada, eliminando así la necesidad de que los usuarios memoricen direcciones IPv4 o IPv6.

Existen varias soluciones que ofrecen servicios DNS, ya sea comerciales, así como de código abierto, entre ellas el DNS de Microsoft con la versión BIND y Dnsmasq en las distribuciones Linux [26]. En la emulación propuesta, la mayoría de los dispositivos y configuraciones están basados en el sistema operativo Linux, por lo tanto, se ha decidido utilizar Dnsmasq. El paquete Dnsmasq es muy liviano, compatible con IPv4 o IPv6, fácil de configurar y útil para redes pequeñas. Cuenta con un subsistema que proporciona un servidor DNS local, que se encarga de servir los nombres de dispositivos locales que no se encuentran en el DNS global.

Anteriormente se mencionó que el servidor DNS está ubicado en la sede principal en Guayaquil, con el fin de que todas las redes de área local puedan acceder a éste en cualquier momento que lo requieran. Se encuentra desarrollado sobre *Ubuntu Server,* el cual está instalado en una máquina virtual a través del programa de virtualización VMware e integrado en GNS3.

El funcionamiento de la base de datos del Servidor DNS será simple, es decir contará simplemente con los nombres de dominio de dispositivos locales y servidores de la red con sus respectivas direcciones IP, como por ejemplo "*sdwanmail.com"*, "*fortigateGYE.com"*, "*dnsserver.com"*, entre otros. Por lo tanto, cualquier usuario final podrá hacer *ping* o acceder a cualquier sitio web a través de nombres de dominio amigables, inclusive los que accedan remotamente a través del portal web. La instalación y configuración del servidor DNS, se explicará en el Capítulo 3.

2.2.4.2 Servidor de correo

Un servidor de correo es una aplicación que actúa como una oficina de correos virtual utilizando el modelo cliente-servidor. El servidor almacena y ordena el correo entrante para su distribución a los usuarios locales; es decir envía y recibe correos electrónicos. El *software* del servidor de correo permite al administrador del sistema crear y gestionar cuentas de correo electrónico para cualquier dominio alojado en el servidor; en este caso el nombre de dominio es "*sdwan.local",* que puede proporcionar cuentas de correo electrónico que terminen en "*@sdwan.local"* [27].

Los servidores de correo se dividen en dos categorías: los servidores de correo salientes conocidos como servidores SMTP[21] y los servidores de correo entrantes como IMAP[22] o POP3[23], como se muestra en la Figura 2.7. Disponen de varias opciones para su

[21] **SMTP:** *Simple Mail Transfer Protocol.- Encargado de transmitir correos.*
[22] **IMAP:** *Internet Message Access Protocol.- Almacenan los mensajes recibidos y enviados.*
[23] **POP3:** *Post Office Protocol.- Almacenan copias de los mensajes en los servidores.*

despliegue. De esta manera, se utiliza el *software* Postfix para el envío de correos y el *software* Dovecot para la recepción de correos.

Figura 2.7. Funcionamiento de servidores SMTP y POP [28]

El servidor de correo se desarrolla sobre una máquina virtual con *Ubuntu Server.* En esta máquina se instala y configura Postfix que corresponde a un agente de transferencia de correo gratuito, encargado de enrutar y entregar el correo electrónico; y Dovecot que corresponde a un servidor de correo electrónico de código abierto, encargado de recibir y almacenar los correos. Estas implementaciones son las más comunes, seguras y fáciles de manejar.

El servidor de correo está ubicado en la red de área local de Quito, que actúa como Centro de Datos, de tal manera que es el encargado de proporcionar cuentas de correo electrónico a los distintos usuarios que trabajen en todas las sedes y sucursales. La base de datos del servidor contará de tres cuentas de correo, con el fin de que cada una corresponda a un usuario por localidad; es decir 1 usuario en la sede principal, 1 usuario en el Centro de Datos y 1 usuario en la sucursal. El nombre de dominio para las cuentas corresponde a "*sdwan.local",* es importante mencionar que el nombre de dominio, el número de cuentas y el sitio web puede ser modificado por el administrador. El servidor está accesible desde cualquier sitio, e inclusive desde el acceso remoto a través del portal web.

Finalmente, el servidor de correo interactúa con el servidor DNS ya que para acceder al sitio web, no es necesaria la dirección IP del servidor, sino simplemente a través del sitio web *"www.sdwanmail.com".* La instalación y configuración se explica posteriormente en el Capítulo 3.

2.2.4.3 Servidor de transferencia de archivos

El servidor *Trivial File Transfer Protocol* (TFTP) se utiliza únicamente para transferir archivos pequeños entre dispositivos de una red, basado en el protocolo FTP. Las principales diferencias están en el protocolo de transporte y el mecanismo de autenticación;

TFTP usa UDP[24] sin autenticación, mientras que FTP usa TCP[25] y requiere autenticación, por lo tanto, FTP protege la información [29].

Para el despliegue de este servidor se usa un dispositivo disponible en GNS3, conocido como Toolbox*,* el cual ya tiene pre-instalado este servidor y solamente se necesita descargarlo de la página web de GNS3 e importarlo. El servidor está ubicado en la red de área local de Guayaquil, de tal manera que tanto el Centro de Datos como la sucursal puedan enviar archivos simples de configuración o actualizaciones de sus dispositivos a través de este servidor.

2.2.4.4 Servidor SYSLOG

El servidor Syslog se utiliza para consolidar registros de diagnóstico y monitoreo de múltiples dispositivos en una sola ubicación; es decir es una herramienta para facilitar la administración, supervisión y mantenimiento de redes. Los mensajes de Syslog se componen generalmente de información básica como: dirección IP, hora de registro y mensaje de registro [30].

De igual manera, se usará el mismo dispositivo del servidor TFTP conocido como Toolbox*,* ya que esta herramienta de GNS3 también cuenta con un servidor Syslog pre-instalado. Este servidor se encuentra en la red de área local de Quito, de tal forma que exista un registro de diagnóstico de la sede y de la sucursal en el Centro de Datos.

2.2.5 FUNCIONAMIENTO DE LAS REDES DE ÁREA EXTENDIDA

En esta sección, se explica a detalle cómo va a trabajar la red MPLS, es decir su protocolo de enrutamiento, Ingeniería de Tráfico, túneles, entre otros aspectos. Además, se detalla el funcionamiento de la WAN de acceso a Internet.

2.2.5.1 Multiprotocol Label Switching (MPLS)

La infraestructura de MPLS se ha desplegado en la red, considerando que actualmente muchas de las empresas usan esta tecnología para la comunicación con sus oficinas remotas. Tomando en cuenta este aspecto, la idea es mantener la infraestructura MPLS para trabajar junto con la SD-WAN. MPLS tiene como función principal interconectar la sede principal en Guayaquil con el Centro de Datos en Quito. Está conformada por 5 *routers* de los cuales 4 de ellos actúan como *Provider Edge Router* y 1 de ellos actúa como *Provider Router,* tal como se muestra en la Figura 2.8.

[24] **UDP:** *User Datagram Protocol.- Envío de datagramas sin establecer conexión previa.*
[25] **TCP:** *Transmission Control Protocol.- Protocolo de transporte confiable orientado a conexión.*

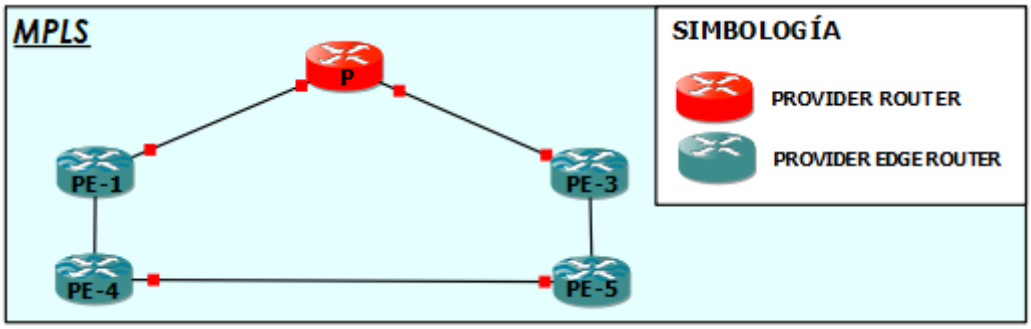


Figura 2.8. Red MPLS y sus componentes.

Adicionalmente al direccionamiento IP detallado en la sección 2.2.2, existe una configuración de direcciones IP para interfaces de *Loopback* con el fin de facilitar algunos aspectos de configuración tanto para los túneles, como para la Ingeniería de Tráfico. En la Tabla 2.3. se muestran las interfaces de *Loopback* utilizadas en cada *router.*

Tabla 2.3. Interfaces de Loopback

INTERFACES	DIRECCIÓN IP
Loopback 10	1.1.1.1/32
Loopback 20	2.2.2.2/32
Loopback 30	3.3.3.3/32
Loopback 40	4.4.4.4/32
Loopback 50	5.5.5.5/32

El protocolo de enrutamiento utilizado es *Open Shortest Path First* (OSPF), el cual es un protocolo de Estado de Enlace, que tiene bajo tiempo de convergencia y proporciona a todos los equipos una visión completa de toda la red; realiza actualizaciones únicamente al detectar cambios en red y emplea mejores métricas en comparación a los protocolos Vector-Distancia [31]. Además, OSPF no tiene limitación en cuenta de saltos y su base de datos se utiliza para construir un árbol con los enlaces de menor costo, y en el caso de existir más de una ruta con igual costo la política es distribuir el tráfico de manera balanceada.

Este protocolo está desplegado en los *routers* de la red MPLS y en las interfaces de los dispositivos FortiGate que interconectan la sede principal con el Centro de Datos. En la red MPLS los dispositivos FortiGate actúan como *Customer Edge Routers,* de tal manera que la conmutación multiprotocolo de etiquetas está habilitada solamente en las interfaces direccionadas a los PE o P *routers,* y no en las dirigidas a los equipos FortiGate. En este punto la red MPLS se encuentra habilitada.

Tomando en cuenta que BGP[26] es compañero de MPLS con el fin de proporcionar una gran escalabilidad para redes, adicionalmente en los PE se está ejecutando BGP con reflector de ruta entre PE-1 y PE-3 para que puedan comunicarse dinámicamente entre sí y conozcan las rutas sin introducir ningún bucle.

MPLS provee nuevas capacidades en áreas como Ingeniería de Tráfico que permite mejorar la utilización de la red mediante la distribución de tráfico de acuerdo con la disponibilidad de recursos, evitando así la congestión en cualquier camino. Por lo tanto, en la red MPLS se ha habilitado Ingeniería de Tráfico mediante el protocolo *Resource Reservation Protocol* (RSVP) basado en el parámetro ancho de banda. Las interfaces de los PE *routers,* tendrán una disponibilidad máxima de 1000 Kbps, mientras que las interfaces del P *router* una disponibilidad máxima de 500 Kbps, con el fin de visualizar el mecanismo de Ingeniería de Tráfico.

Otra capacidad importante de MPLS, es la creación de túneles gracias al *stack* de etiquetas. Por lo tanto, existirá un túnel basado en el ancho de banda entre PE-1, PE-4, PE-5 y PE-3, con un requerimiento de 800 Kbps como mínimo de ancho de banda. En la Figura 2.9. se visualiza el túnel formado entre ambos *routers*, de tal manera que la elección de la ruta se hace de forma automática de acuerdo con los parámetros de Ingeniería de Tráfico mencionados anteriormente.

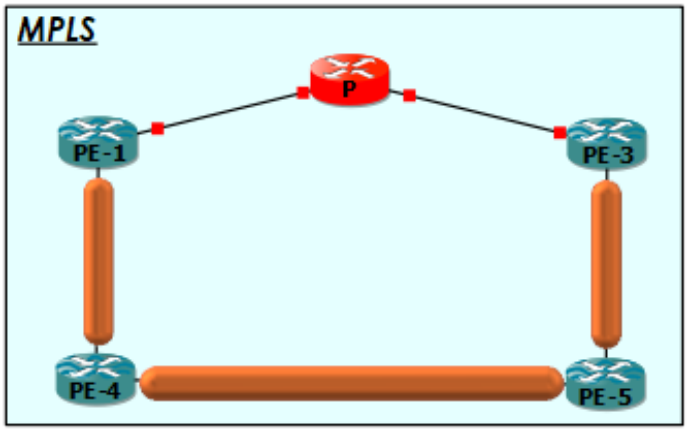


Figura 2.9. Tunelización MPLS entre PE-1, PE-4, PE-5 y PE-3

Finalmente, la red MPLS debe funcionar en conjunto con la SD-WAN, de tal manera que, de acuerdo con los requerimientos o necesidades, la red automáticamente escogerá la mejor ruta para enviar el tráfico hacia las distintas oficinas remotas. Es importante mencionar que la configuración de cualquier parámetro o aspecto interno de la red MPLS

[26] **BGP:** *Border Gateway Protocol.- Utilizado para transportar información de enrutamiento externo, ya sea de clientes o Internet.*

se lo deberá realizar específicamente en cada uno de los *routers* de la red, ya que es una infraestructura totalmente independiente a la SD-WAN.

2.2.5.2 WAN de acceso a Internet

La SD-WAN es inmensamente útil si ya se tiene una red MPLS, es decir estas dos tecnologías son totalmente compatibles. La SD-WAN permite agregar conexiones públicas de Internet a la red con facilidad, ya sea mediante DSL[27], cable, fibra o cualquier otro transporte IP para tráfico de prioridad más baja, a un costo mucho menor que MPLS. De esta manera, se puede entender que la WAN con acceso a Internet, es simplemente un enlace público de bajo costo de Internet conectado desde los dispositivos FortiGate ubicados en Guayaquil, Quito y Ambato.

En la sede principal de Guayaquil, existe más de una sola conexión a Internet, con el fin de aumentar el rendimiento y la velocidad, ya que una sola línea de banda ancha no proporcionaría el tiempo de actividad adecuado que exigen las aplicaciones críticas para la empresa y provocaría dificultades para tener túneles IP de alto rendimiento y confiables entre oficinas remotas. Por lo tanto, en la sede principal existen tres enlaces de banda ancha.

En el Centro de Datos existe una sola conexión a Internet, ya que, en caso de necesitar aumentar el rendimiento o velocidad, puede utilizar la red MPLS para acceder a Internet a través de la sede principal que dispone de mayor cantidad de conexiones de banda ancha, inclusive en el caso de que este enlace presente alta latencia o se caiga puede hacer uso de la red MPLS.

De igual manera, en la sucursal existe más de un enlace de banda ancha, en caso de que la red presente alta latencia, requiera un túnel IP confiable o si el enlace falla, con el fin de evitar perder la comunicación. Por lo tanto, la sucursal cuenta con dos enlaces de banda ancha. En el caso de existir más sucursales, no es necesario comprar circuitos privados MPLS entre sucursales, ya que SD-WAN permite construir una red segura y mallada utilizando el Internet público.

Finalmente, en la Figura 2.10. se visualizan todas las conexiones a Internet, desde cada uno de los sitios. Cabe recalcar que en la emulación no está especificado el tipo de transporte IP como fibra, cable, DSL u otros debido a que los clientes tienen la flexibilidad de soportar múltiples tipos, por lo tanto, depende por cuál transporte la empresa se incline. En la emulación se lo toma como líneas de banda ancha en general. Respecto a la nube

[27] **DSL:** *Digital Subscriber Line.- Servicios de comunicaciones a través de líneas telefónicas.*

de acceso remoto simplemente es a través de Internet en cualquier sitio del mundo que se encuentre.

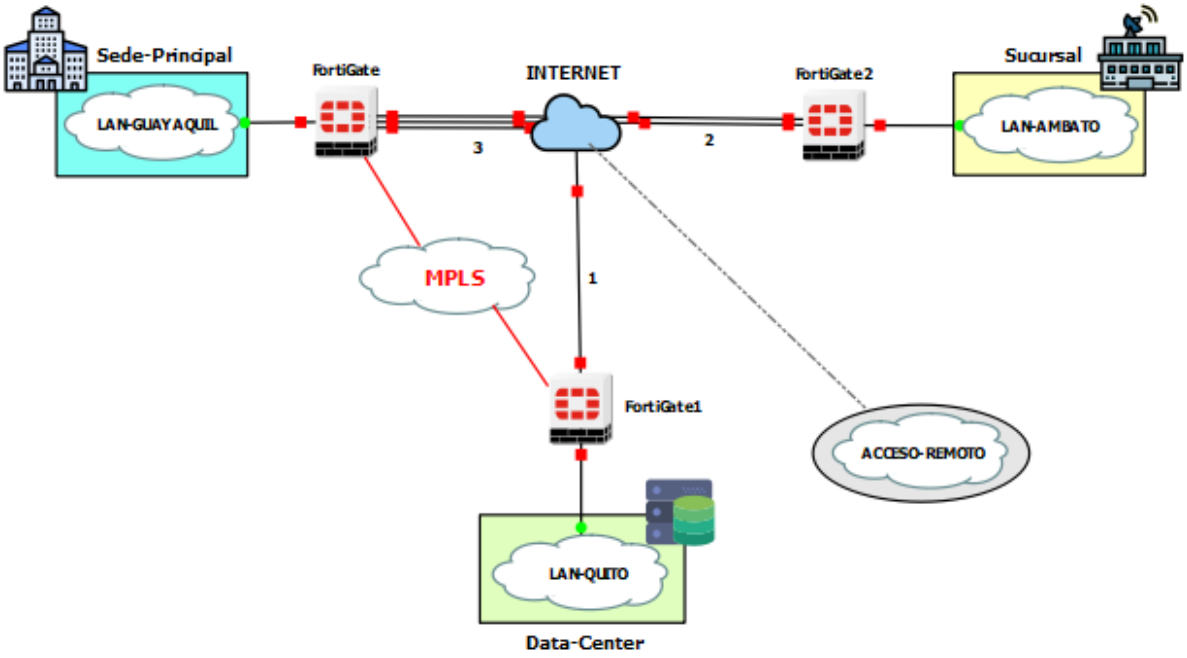


Figura 2.10. Enlaces de acceso a Internet de la red

2.2.6 FUNCIONAMIENTO DE LA SD-WAN

Esta sección juega un papel muy importante, ya que explica detalladamente cómo va a funcionar la SD-WAN, es decir sus reglas, políticas, tipo de seguridad, control, administración, entre otros aspectos, los cuales requieren un análisis más profundo en comparación con las otras secciones, debido a que SD-WAN es el tema fundamental de la emulación.

2.2.6.1 Enlaces de la SD-WAN

Los enlaces MPLS, enlaces de acceso a Internet y túneles o VPNs correspondientes a la sede principal, Centro de Datos y sucursal forman parte de la SD-WAN, a excepción únicamente de la red de acceso remoto que corresponde a la SSL-VPN. En la Figura 2.11. se visualiza un ejemplo de todas las redes que forman parte de la SD-WAN en el FortiGate de la sede principal; el objetivo es permitir que las redes ubicadas en Quito, Guayaquil y Ambato interactúen entre sí y se las pueda controlar y administrar desde un único punto, en este caso desde el FortiManager. Por lo tanto, se tendrá una red automatizada, centralizada e inteligente que mejorará el rendimiento de cada uno de los enlaces basado en reglas o políticas, las cuales se explican a detalle posteriormente. Es importante mencionar que los FortiGate del Centro de Datos y la sucursal tienen un esquema similar,

con la única diferencia de que asocian a la SD-WAN sus enlaces directamente conectados, como se muestra en las Figuras 2.12. y 2.13.

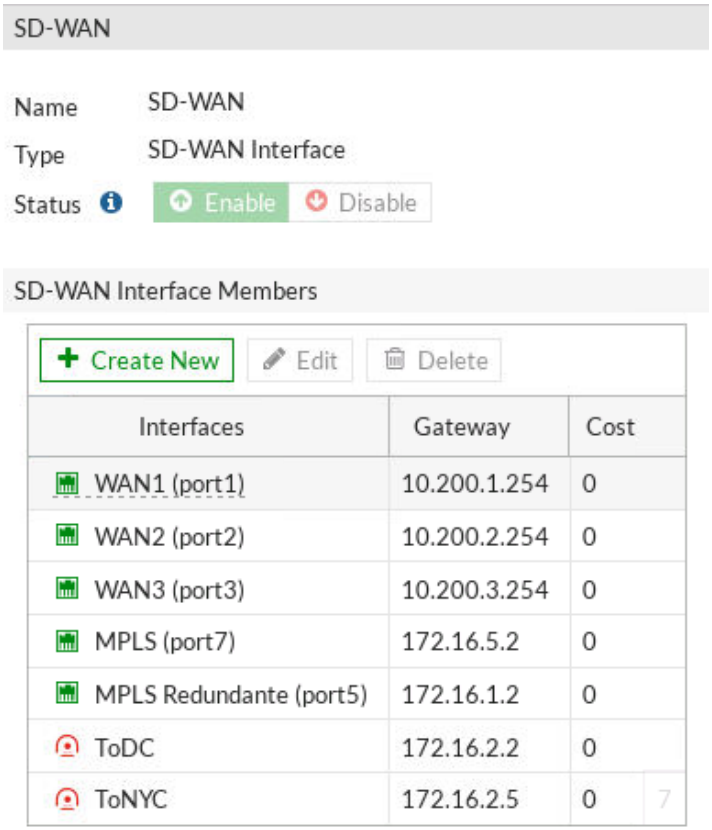


Figura 2.11. SD-WAN de la Sede Principal

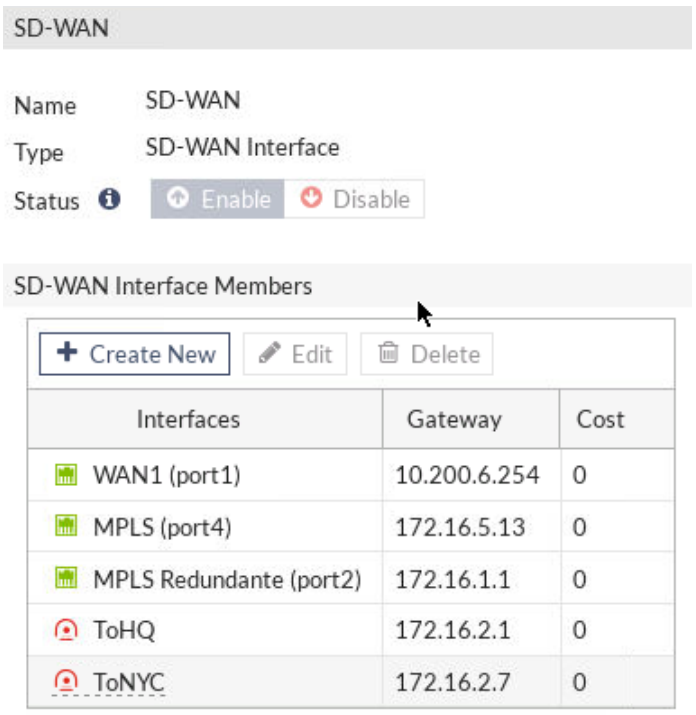


Figura 2.12. SD-WAN del Centro de Datos

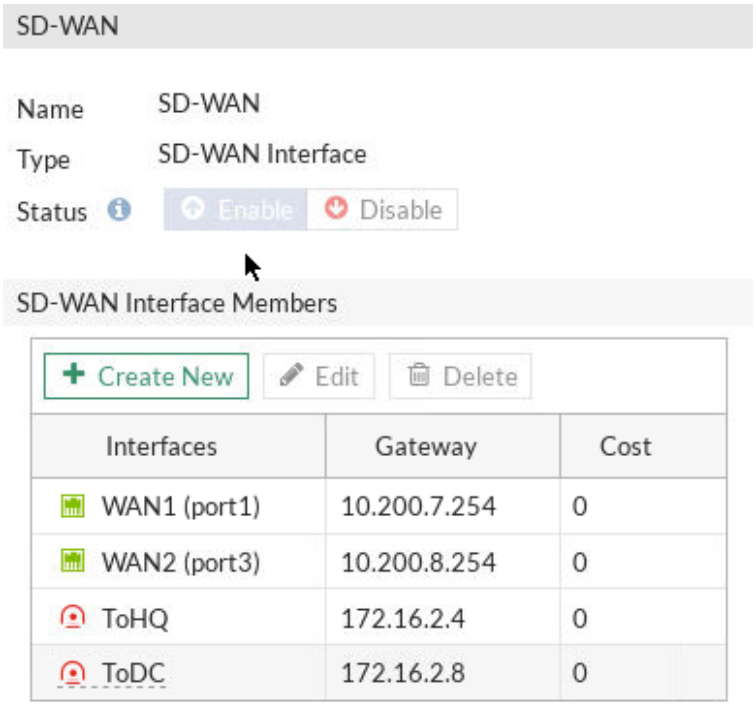


Figura 2.13. SD-WAN de la Sucursal

2.2.6.2 VPNs de la SD-WAN

Las redes privadas virtuales pueden tener túneles de dos tipos: *Internet Protocol Security* (IPSec) o *Secure Sockets Layer* (SSL). En este caso, se hizo uso de los túneles IPsec para las conexiones internas de la empresa, es decir entre la sede principal, Centro de Datos y la sucursal debido a que ofrece mayor seguridad; mientras que el SSL-VPN gracias a su compatibilidad con cualquier navegador sin requerir *software* adicional, está dedicado explícitamente para el acceso de usuarios a través de Internet, es decir usuarios que se encuentran fuera de cualquier oficina de la empresa.

2.2.6.2.1 IPsec-VPN

Los túneles IPsec de la empresa funcionan de la siguiente manera: en la sede principal existen dos VPNs, una dirigida hacia el Centro de Datos llamada *"ToDC"* y otra dirigida hacia la sucursal denominada *"ToNYC".* En el Centro de Datos de igual manera existen dos VPN, una dirigida a la sede principal llamada *"ToHQ"* y otra dirigida hacia la sucursal llamada también *"ToNYC".* Finalmente, en la sucursal de igual manera existen las dos VPN, una dirigida hacia la sede principal llamada *"ToHQ"* y la otra dirigida hacia el Centro de Datos llamada *"ToDC".*

En la Figura 2.14. se visualizan las VPNs correspondientes a cada sector.

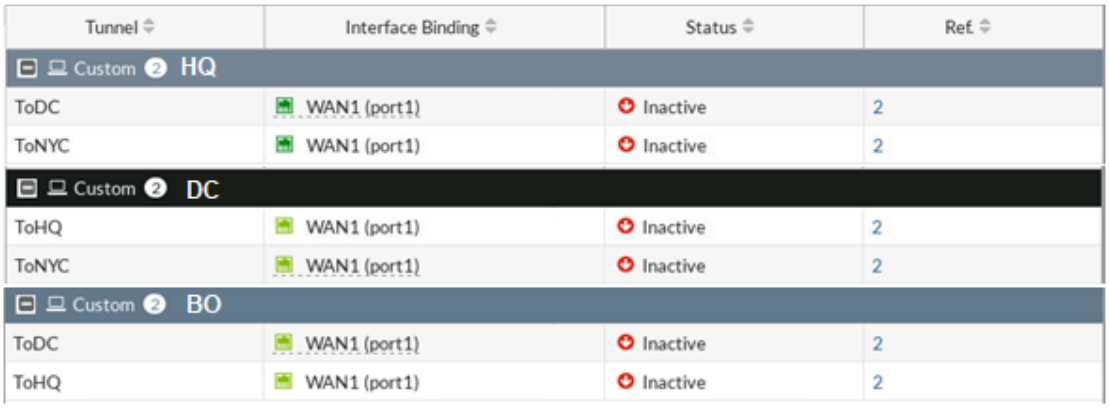


Figura 2.14. IPSec-VPNs de la red SD-WAN

2.2.6.2.2 SSL-VPN

Por otra parte, se encuentra la SSL-VPN para el acceso de usuarios a servicios de la empresa a través de Internet. La finalidad de escoger este tipo de VPN es por la facilidad de acceso para los clientes y empleados gracias a la compatibilidad con Google Chrome, Firefox, etc., ya que no requiere ningún programa adicional. Sin embargo, esta facilidad lo vuelve más vulnerable o inseguro; pero la decisión se basa también de acuerdo con los servicios a los cuales los usuarios van a acceder. En este caso, los usuarios de la VPN solo acceden a servicios como correo electrónico y almacenamiento de archivos, por lo tanto, es suficiente la SSL-VPN.

Existen dos SSL-VPN, uno en la sede principal que permite el acceso a los servidores TFTP y DNS, mientras que el otro en el Centro de Datos que permite el acceso al servidor de correo electrónico, desde cualquier sitio.

2.2.6.3 Políticas y objetos

Antes de continuar con las políticas, es importante mencionar que una vez agregados todos los enlaces a la SD-WAN en la sede principal, Centro de Datos y sucursal, en forma general se establece una sola ruta estática (0.0.0.0/0) para la SD-WAN, que le permita alcanzar a Internet; esto es necesario en cada FortiGate. Sin embargo, esto no significa que ya se puede navegar en Internet, aquí viene la importancia de las políticas que son las que definen los puertos por donde ingresa y sale el tráfico, y los objetos que definen las subredes de origen y destino del tráfico. Las políticas cumplen un papel importante en la seguridad, ya que en ellas se define el tipo de seguridad a usar; esto se explica a detalle en secciones posteriores.

2.2.6.3.1 Políticas de la sede principal

En la sede principal se definen 6 políticas, una de ellas es una política implícita o por defecto de todos los dispositivos FortiGate que se encarga de negar cualquier tipo de tráfico

hacia cualquier destino, conocida como "*Implicit Deny"* y otras 5 políticas creadas por el administrador de red.

La política llamada "*InternetAccess"* define como puerto de entrada al puerto 6 que corresponde al puerto conectado a la LAN de Guayaquil y como puertos de salida a los puertos de la SD-WAN. En esta política existe una particularidad que se refiere a la SD-WAN como puerto de entrada; su objetivo es permitir al Centro de Datos acceder a Internet utilizando sus enlaces de banda ancha a través de la red MPLS, en caso de existir saturación o pérdida de paquetes en su único enlace de banda ancha. Las subredes de origen en esta política corresponden a la "*HQ Subnet"* o LAN de la sede principal, "*DC Subnet"* o LAN del Centro de Datos y la "*MPLS Network"*, y el destino está definido como "*all"* que hace referencia a Internet. De esta manera, esta política permite que la sede principal pueda navegar en Internet.

La política *"To_DC"* define como puerto de entrada a la LAN y puerto de salida la SD-WAN. La subred de origen correspondiente a "*HQ_Subnet"* y las subredes de destino correspondientes a "*DC_Subnet"* y "*BO_Subnet"* o LAN de la sucursal. Esta política permite que la sede principal establezca conexión con el Centro de Datos y la sucursal de forma unidireccional, es decir el transporte de tráfico tomando como origen siempre a la sede. El tráfico en dirección contraria corresponde a la política llamada *"From_DC"* que define como puerto de entrada a la SD-WAN y puerto de salida a la LAN. Las subredes de origen corresponden a "*DC_Subnet", "BO_Subnet", "MPLS Network",* y *"VPN"*; y el destino corresponde a la subred *"HQ_Subnet".* De esta forma, se establece conexión con la sede principal desde el Centro de Datos y la sucursal; es importante mencionar que la *"VPN"* hace referencia a las redes privadas virtuales o túneles de la red, los cuales se explican posteriormente a detalle.

La política de *"InterOfficeTraffic_BO_DC"* define como puerto de entrada la SD-WAN y como puerto de salida también la SD-WAN. Las subredes de origen corresponden a *"BO_Subnet", "DC_Subnet", "MPLS Network", "MPLS Redundancy"* y *"VPN",* mientras que la subred de destino corresponde a *"DC_Subnet"* y *"BO_Subnet".* Esta política permite establecer la conexión entre la sucursal y el Centro de Datos o viceversa, a través de la sede principal, es decir el FortiGate de la sede principal actúa como un intermediario para el paso de tráfico. Por ejemplo, el tráfico entra por los enlaces de acceso a Internet de la sede principal y sale por los enlaces de la red MPLS, por lo tanto, los puertos de entrada y salida corresponden a la SD-WAN.

La política *"SSL-VPN"* define como puerto de entrada el túnel SSL-VPN y como puerto de salida el de la LAN. El tráfico viene desde la *"SSLVPN_TUNNEL_ADDR1"* y *"PortalWeb_Users"* con destino a la subred *"HQ_Subnet".* Esta política permite acceder a usuarios ubicados en otros sitios del mundo a los recursos de la sede principal, a través de Internet.

Finalmente, en la Figura 2.15. se pueden visualizar todas las políticas de la sede principal que permiten tener una mejor comprensión de lo explicado anteriormente.

ID	Name	From	To	Source	Destination
2	To_DC	LAN (port6)	SD-WAN	HQ_Subnet	DC_Subnet BO_Subnet
3	From_DC	SD-WAN	LAN (port6)	DC_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	HQ_Subnet
1	InternetAccess	LAN (port6) SD-WAN	SD-WAN	HQ_Subnet DC_Subnet MPLS Network MPLS Redundancy	all
5	InterOfficeTraffic_BO_DC	SD-WAN	SD-WAN	BO_Subnet VPN DC_Subnet MPLS Redundancy MPLS Network	DC_Subnet BO_Subnet
6	SSL-VPN	SSL-VPN tunnel	LAN (port6)	SSLVPN_TUNNEL_ADDR1 PortalWeb_Users	HQ_Subnet
0	Implicit Deny	any	any	all	all

Figura 2.15. Políticas de la Sede Principal

2.2.6.3.2 Políticas del Centro de Datos

En el Centro de Datos al igual que en la sede principal se dispone de 6 políticas, una "*Implicit Deny"* y otras 5 políticas creadas por el administrador de red. Las políticas tienen un funcionamiento similar al de la sede principal, de tal forma que se hará énfasis en los aspectos que han variado.

La política "*InternetAccess",* define como puerto de entrada el de la LAN y como puerto de salida la SD-WAN correspondientes al Centro de Datos; en este caso la única diferencia es que la subred de origen corresponde a *"DC_Subnet"*, y el destino igualmente "*all".* Esta política permite a todos los usuarios del Centro de Datos navegar en Internet.

La política *"To_HQ_BO"* al igual que en la sede principal define los mismos puertos de entrada y salida, pero correspondientes a la SD-WAN del Centro de Datos; en esta política

la subred de origen corresponde a la *"DC_Subnet"* y las subredes de destino son "*HQ_Subnet"* y *"BO_Subnet".* Esta política establece la conexión unidireccional desde el Centro de Datos hacia la sede principal y la sucursal. La política *"From_HQ_BO"* define los mismos puertos en la dirección contraria y tiene como subredes de origen "*HQ_Subnet", "MPLS Network", "BO_Subnet"* y *"VPN";* mientras que la subred de destino corresponde a *"DC_Subnet".* Esta política se encarga de establecer la conexión desde la sede principal y la sucursal hacia el Centro de Datos, a través de la VPN o la red MPLS.

La política *"InterOfficeTraffic_HQ_BO"* define como puerto de entrada y salida a la SD-WAN; las subredes de origen corresponden a *"BO_Subnet", "HQ_Subnet", "MPLS Network", "MPLS Redundancy"* y *"VPN",* mientras que las subredes de destino son la *"HQ_Subnet"* y *"BO_Subnet".* Esta política permite establecer una conexión desde la sucursal hacia la sede principal o viceversa, pero pasando por el Centro de Datos, es decir el FortiGate del Centro de Datos actúa como un intermediario. El tráfico ingresa por el enlace de acceso a Internet del Centro de Datos y sale por la red MPLS, por tal motivo ambos puertos de la política corresponden a SD-WAN.

La política *"SSL-VPN"* al igual que en la sede principal tiene el mismo mecanismo con los puertos correspondientes al Centro de Datos, la única diferencia es que la subred de destino corresponde a *"DC_Subnet".* De esta manera, los usuarios podrán acceder a los recursos del Centro de Datos desde cualquier sitio del mundo, a través de Internet. Finalmente, en la Figura 2.16. se puede visualizar todas las políticas del Centro de Datos.

ID	Name	From	To	Source	Destination
2	To_HQ_BO	LAN (port3)	SD-WAN	DC_Subnet	HQ_Subnet BO_Subnet
3	From_HQ	SD-WAN	LAN (port3)	HQ_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	DC_Subnet
1	InternetAccess	LAN (port3)	SD-WAN	DC_Subnet	all
4	InterOfficeTraffic_HQ_BO	SD-WAN	SD-WAN	BO_Subnet VPN HQ_Subnet MPLS Redundancy MPLS Network	HQ_Subnet BO_Subnet
5	SSL-VPN	SSL-VPN tunnel	LAN (port3)	SSLVPN_TUNNEL_ADDR1 DC_PortalWeb_Users	DC_Subnet
0	Implicit Deny	any	any	all	all

Figura 2.16. Políticas del Centro de Datos

2.2.6.3.3 Políticas de la sucursal

La sucursal difiere con respecto a la sede principal y al Centro de Datos ya que es una oficina remota más sencilla, en la que se han definido 3 políticas creadas por el administrador y la política *"Implicit Deny".*

La política *"InternetAccess",* define como puerto de entrada a la LAN y como puerto de salida a la SD-WAN correspondientes a la sucursal; la subred de origen es *"BO_Subnet"* y el destino es *"all".* Esta política permite a los usuarios de la sucursal acceder a Internet.

La política *"To_HQ_DC"* define los mismos puertos de la política anterior y la misma subred de origen, la única diferencia es la subred de destino correspondiente a *"HQ_DC_Supernet"*. Esta política establece la conexión desde la sucursal hacia el Centro de Datos y la sede principal de forma unidireccional. La política *"From_HQ"* define como puerto de entrada la SD-WAN y como puerto de salida el de la LAN; las subredes de origen corresponden a *"HQ_DC_Supernet", "MPLS Network", "MPLS Redundancy"* y *"VPN",* mientras que la subred de destino corresponde a *"BO_Subnet".* Esta política establece la conexión desde la sede principal y el Centro de Datos hacia la sucursal. Finalmente, en la Figura 2.17. se puede visualizar todas las políticas de la sucursal.

ID	Name	From	To	Source	Destination
3	To_HQ_DC	LAN (port2)	SD-WAN	BO_Subnet	HQ_DC_Supernet
1	InternetAccess	LAN (port2)	SD-WAN	BO_Subnet	all
2	From_HQ	SD-WAN	LAN (port2)	HQ_DC_Supernet VPN MPLS Redundancy MPLS Network	BO_Subnet
0	Implicit Deny	any	any	all	all

Figura 2.17. Políticas de la Sucursal

2.2.6.4 Reglas de la SD-WAN

En concordancia con las políticas de la red, se procede a definir las reglas que describen el comportamiento de la SD-WAN. Estas reglas permiten a la red ser más inteligente y tomar decisiones automáticamente para enrutar el tráfico con base en parámetros como latencia, ancho de banda, entre otros. A continuación, se describe el mecanismo de las reglas SD-WAN de la sede principal, del Centro de Datos y de la sucursal.

2.2.6.4.1 Reglas de la sede principal

En la sede principal existen 3 reglas, la primera llamada *"To-DC",* su objetivo es llevar el tráfico que viene desde la sede principal o la sucursal hacia el Centro de Datos. Tomando

en cuenta que los caminos disponibles son la *"MPLS"* y la VPN *"ToDC",* la SD-WAN elegirá la mejor ruta automáticamente con base en el parámetro de latencia; en caso de un aumento inesperado del retardo la SD-WAN se encarga de escoger el mejor camino.

La segunda regla llamada *"To-BO",* tiene como objetivo llevar el tráfico desde la sede principal o Centro de Datos hacia la sucursal por el mejor camino, basados en el mismo parámetro, esto es latencia. Es importante mencionar que el parámetro puede ser modificado a criterio del administrador o del cliente, por ejemplo, ancho de banda, pérdida de paquetes, SLA, etc.

A continuación, la regla de *"InternetAccess",* que se encarga de balancear el tráfico que permite a la sede principal o al Centro de Datos navegar por Internet; se incluye el Centro de Datos ya que, si su enlace de conexión a Internet presenta problemas, se define que haga uso de uno de los enlaces de la sede principal. La SD-WAN escoge la mejor de las 3 conexiones de banda ancha, en caso de existir varias sesiones simultáneas hará un balanceo de carga, de tal forma que el tráfico se distribuya por todas las conexiones basado en un SLA. Finalmente, en la Figura 2.18 se muestran todas las reglas de la sede principal.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
2	To-DC	HQ_Subnet BO_Subnet	DC_Subnet	Latency	MPLS Redundante (port5) ToDC MPLS (port7)
3	To-BO	HQ_Subnet DC_Subnet	BO_Subnet	Latency	ToNYC MPLS Redundante (port5) MPLS (port7)
1	InternetAccess	HQ_Subnet DC_Subnet	all	SLA	WAN1 (port1) WAN2 (port2) WAN3 (port3)
Implicit 1					
	sd-wan	all	all	Source IP	any

Figura 2.18. Reglas SD-WAN de la Sede Principal

2.2.6.4.2 Reglas del Centro de Datos

De la misma manera en el Centro de Datos se tienen 3 reglas SD-WAN, una de ellas es *"To-HQ",* que se encarga de escoger el mejor camino entre el Centro de Datos y la sede principal, basándose en la latencia.

A continuación, la regla *"To-BO"* que tiene como función escoger la mejor ruta disponible para llevar el tráfico desde el Centro de Datos o la sede principal hacia la sucursal. De la misma manera que las reglas anteriores, se basa en el parámetro latencia.

Luego, existe una regla llamada *"InternetAccess"* que se encarga de escoger la mejor ruta basada en la latencia para que los usuarios del Centro de Datos accedan a Internet. En este caso, tiene la posibilidad de escoger su única conexión de banda ancha o a su vez llegar a Internet usando como intermediario al FortiGate de la sede principal. Finalmente, en la Figura 2.19. se visualiza las reglas del Centro de Datos.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
2	To-HQ	DC_Subnet	HQ_Subnet	Latency	MPLS Redundante (port2) ToHQ MPLS (port4)
3	To-BO	DC_Subnet HQ_Subnet	BO_Subnet	Latency	ToNYC MPLS Redundante (port2) MPLS (port4)
1	InternetAccess	DC_Subnet	all	Latency	WAN1 (port1) MPLS Redundante (port2) MPLS (port4)
Implicit 1					

Figura 2.19. Reglas SD-WAN del Centro de Datos

2.2.6.4.3 Reglas de la sucursal

Para la sucursal, se definen 3 reglas SD-WAN, la primera llamada *"ToHQ"* que se encarga de escoger la mejor ruta para llevar el tráfico desde la sucursal hacia la sede principal. Tiene como opciones de ruta las VPN *"ToHQ"* y *"ToDC",* de tal manera que en base a la latencia escogerá el mejor camino.

La regla *"ToDC"* tiene el mismo mecanismo con un destino diferente, es decir se encarga de llevar el tráfico desde la sucursal hacia el Centro de Datos.

Finalmente, la regla *"InternetAccess"* que permite a los usuarios navegar por Internet utilizando el mejor camino. En este caso, se tiene solamente dos enlaces de banda ancha como se muestra en la Figura 2.20., por lo tanto, al existir demasiado tráfico se puede utilizar balanceo de carga al igual que en la sede principal.

ID	Name	Source	Destination	Criteria	Members
IPv4 3					
2	ToHQ	BO_Subnet	HQ_Subnet	Latency	ToHQ ToDC
3	ToDC	BO_Subnet	DC_Subnet	Latency	ToHQ ToDC
1	Internet	BO_Subnet	all	SLA	WAN1 (port1) WAN2 (port3)
Implicit 1					
	sd-wan	all	all	Source IP	any

Figura 2.20. Reglas SD-WAN de la Sucursal

2.2.6.5 Seguridad de la SD-WAN

En esta sección se explica el tipo de seguridad aplicado a la red de la empresa. Los perfiles de seguridad son los mismos para la sede principal, el Centro de Datos, y la sucursal. La licencia de FortiGuard permite tener el entorno completo de seguridad, en este caso se configuran solo los perfiles permitidos en la versión de prueba de FortiGate.

Es importante recordar que la SD-WAN de FORTINET es la única solución en el mercado con seguridad *Next-Generation Firewall* (NGFW) incorporada [21]. Es decir, en el mismo dispositivo FortiGate funcionan la SD-WAN y NGFW, que permiten el control de aplicaciones y protección contra ataques externos.

2.2.6.5.1 Modos NGFW

Existen dos modos de NGFW, el primero basado en perfiles y el segundo en políticas. En este caso, se utiliza el modo por defecto correspondiente a *NGFW Profile-Based,* debido a que éste funciona con cualquier modo de inspección del tráfico. Este modo NGFW permite crear perfiles de seguridad dentro del control de aplicaciones, el filtrado web, antivirus, entre otros, los cuales son asociados a alguna de las políticas.

2.2.6.5.2 Modos de inspección del tráfico

Existen dos modos de configuración para inspeccionar el tráfico, uno de ellos está basado en flujo y el otro está basado en proxy. En este caso, se puede usar cualquiera de acuerdo con el perfil de seguridad asociado a cada una de las políticas establecidas anteriormente.

Flow-Based es el modo por defecto y la inspección se realiza en directo, es decir a medida que los paquetes pasan por el FortiGate son inspeccionados en tiempo real, sin tener que enviarlos a un *buffer* para una inspección más profunda; las ventajas de este modo es que el usuario tiene un mayor *throughput,* tiempos de respuestas más cortos en la navegación y minimiza errores de *timeout* [32]. En la Figura 2.21. se visualiza su mecanismo de trabajo.

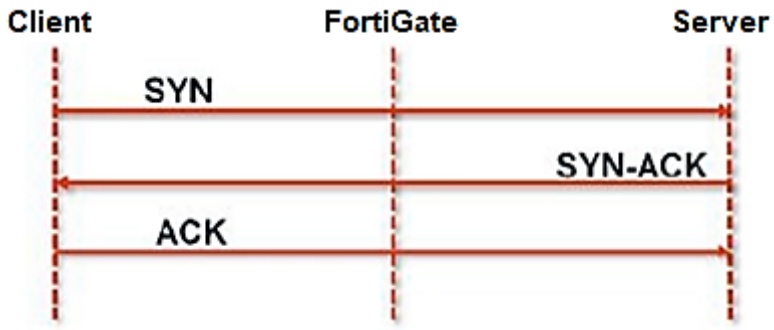


Figura 2.21. Mecanismo de *Flow-Based* [32]

En el segundo modo *Proxy-Based,* los paquetes se almacenan en un *buffer* temporal donde se realiza la inspección, su ventaja es que permite un análisis completo del tráfico y mayor protección contra amenazas; sin embargo, requiere más recursos y agrega latencia debido a su mecanismo que se visualiza en la Figura 2.22.

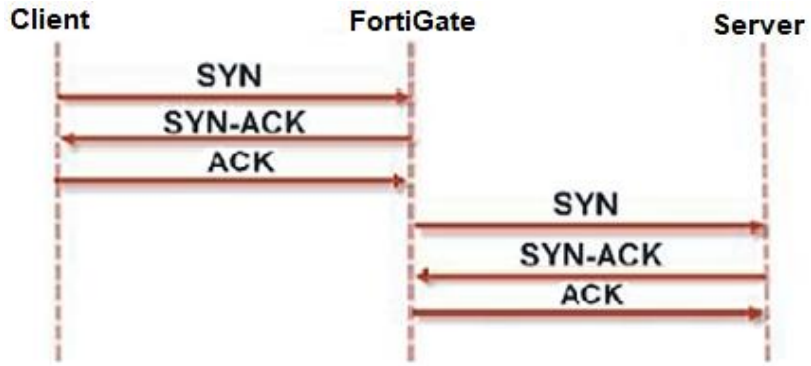


Figura 2.22. Mecanismo *Proxy-Based* [32]

2.2.6.5.3 Tipos de inspección SSL

La inspección SSL se puede realizar de dos maneras, una de ellas es *Certificate Inspection* que se encarga solamente de inspeccionar la información de las cabeceras de los paquetes, por lo tanto, no se puede inspeccionar los datos encriptados que pasan por el FortiGate. Por otro lado, *Deep Inspection* que permite desencriptar el contenido de las conexiones y así realizar una inspección total [32]. En el presente caso, se usa el modo *Deep Inspection* que funciona juntamente con el control de virus, aplicaciones e intrusos. Es importante mencionar que este tipo de inspecciones funcionan con certificados, de tal manera que se debe usar el certificado *"Fortinet_CA_SSL"* que viene por defecto en los equipos.

2.2.6.5.4 Antivirus

En este caso, se asocia el perfil por defecto de antivirus a las políticas establecidas en los dispositivos FortiGate, de tal forma que se tenga una capa extra de seguridad. Es importante mencionar, que este antivirus no reemplaza los antivirus instalados en las computadoras internas, sino que los complementa. La inspección definida para el análisis de los paquetes es *Flow-Based* combinada con *Deep Inspection.*

2.2.6.5.5 Control de aplicaciones

El control de aplicaciones detecta y actúa en base al tráfico generado por las aplicaciones. Se encarga de impedir, monitorear o permitir el acceso a aplicaciones establecidas por el administrador, ya sea de forma específica o por categorías. En este caso, se crea un perfil que define el control sobre la categoría de acceso remoto, encargado de bloquear el acceso a aplicaciones como TeamViewer, Anydesk, entre otras. Además, se bloquea el acceso a

Spotify y se establece un filtro de control que bloquee las aplicaciones de juegos en el navegador en base a la categoría, vendedor y nivel de riesgo.

2.2.6.5.6 Sistemas de Prevención de Intrusos (IPS)

Esta herramienta permite proteger activamente los equipos de ataques conocidos al acceder a Internet; la lista de ataques se actualiza constantemente con los servicios de paga de FortiGuard. En el presente caso, se crea un perfil encargado de proteger a los equipos de trabajo, el cual bloqueará todas las conexiones hacia sitios Botnet[28]. De la misma forma, se pueden establecer filtros de nivel de riesgo, sistema operativo y tipo de protocolo para permitir o bloquear el tráfico. Inclusive se pueden definir excepciones para equipos que obligatoriamente necesiten acceder a dicho sitio, utilizando su dirección IP.

Por otro lado, se encuentran los ataques de Denegación de Servicios (DoS) que consumen todos los recursos del equipo como RAM, CPU, números de puertos, etc. Generalmente, su objetivo es que la unidad deje de responder a peticiones legítimas cuando los ataques son grandes, como se muestra en la Figura 2.23. Por lo tanto, se crea una política DoS con los umbrales por defecto a excepción de los parámetros de inundación y escaneo de paquetes TCP y UDP que están configurados por el administrador.

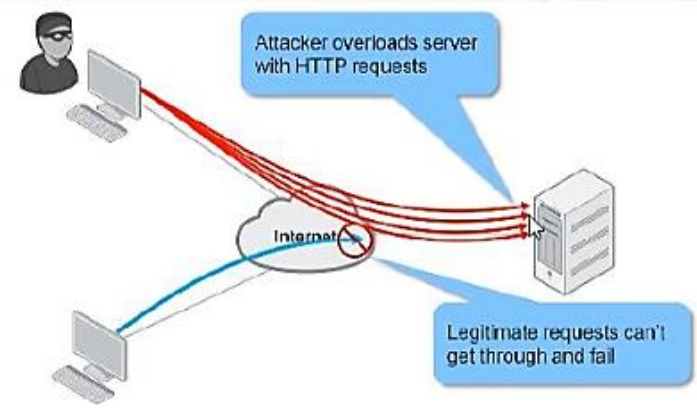


Figura 2.23. Ataque DoS [32]

2.2.6.5.7 Grupos de aplicación en políticas

Los grupos de aplicaciones funcionan con *Traffic Shapers;* esta herramienta permite limitar y controlar uso del ancho de banda. Por lo tanto, se puede dar mayor prioridad a ciertas aplicaciones de acuerdo con el ancho de banda que necesiten. Sin embargo, funcionan siempre y cuando el control de aplicaciones esté asociado a una de las políticas. En este caso, se asocia a la política de acceso a Internet que proporciona mayor prioridad a las aplicaciones de Teletrabajo en la sede principal, Centro de Datos y sucursal.

[28] **Botnet:** *red de equipos que han sido infectados por malwares.*

2.2.6.5.8 Firewall de aplicaciones web

Su función es proteger un servidor que ejecuta una aplicación web como el servidor de correo del Centro de Datos. El perfil predeterminado contiene las firmas y restricciones introducidas por FortiGuard, sin embargo, está disponible solamente si trabaja en modo de inspección basado en proxy y combinado con *Deep Inspection*. En la emulación no se configura este perfil ya que se necesita la licencia de FortiGuard.

2.2.6.5.9 Web filter, DNS filter, e-mail filter

El filtrado web, DNS, y de *e-mail* son otros tipos de seguridad que se pueden introducir en la red y su mecanismo es simple, como su nombre lo indica se encarga de filtrar paquetes; sin embargo, todos estos necesitan tener los servicios de paga de FortiGuard, por lo que no están presentes en la emulación.

2.2.6.6 Monitoreo de enlaces de la SD-WAN

Esta sección permite supervisar el rendimiento de los enlaces miembros de la SD-WAN, mediante señales de sondeo a un servidor. De esta manera, la medición de cada enlace se la puede hacer en función de la latencia, *jitter,* y pérdida de paquetes; está relacionado con la Calidad de Servicio *(QoS)*. Es indispensable la dirección IP de un servidor en el destino para que se realice correctamente el monitoreo de los enlaces.

En la Figura 2.24. se visualizan los enlaces a monitorear de la sede principal; en primer lugar, está el *"QoS",* que corresponde a las rutas dirigidas hacia la sucursal. A continuación, está el *"QoSInternet"* encargado de los enlaces de conexión a Internet. Finalmente, está el *"QoS_DC"* que monitorea los enlaces dirigidos hacia el Centro de Datos.

Name	Detect Server	Packet Loss	Latency	Jitter
QoS	10.10.3.254	MPLS Redundante (port5): MPLS (port7): ToNYC:	MPLS Redundante (port5): MPLS (port7): ToNYC:	MPLS Redundante (port5): MPLS (port7): ToNYC:
QoSInternet	8.8.8.8	WAN1 (port1): WAN2 (port2): WAN3 (port3):	WAN1 (port1): WAN2 (port2): WAN3 (port3):	WAN1 (port1): WAN2 (port2): WAN3 (port3):
QoSMPLS	10.10.2.100	MPLS Redundante (port5): MPLS (port7): ToDC:	MPLS Redundante (port5): MPLS (port7): ToDC:	MPLS Redundante (port5): MPLS (port7): ToDC:

Figura 2.24. Monitoreo de enlaces de la Sede Principal

Con respecto al Centro de Datos, se encarga de monitorear los enlaces dirigidos hacia Internet a través del *"QoS_Internet",* los enlaces dirigidos hacia la sede principal a través del *"QoS_MPLS"* y los enlaces dirigidos hacia la sucursal a través del *"QoS_To_BO",* como se muestra en la Figura 2.25.

Name	Detect Server	Packet Loss	Latency	Jitter
QoSInternet	8.8.8.8	WAN1 (port1): MPLS Redundante (port2): MPLS (port4):	WAN1 (port1): MPLS Redundante (port2): MPLS (port4):	WAN1 (port1): MPLS Redundante (port2): MPLS (port4):
QoSMPLS	10.10.1.100	MPLS Redundante (port2): MPLS (port4): ToHQ:	MPLS Redundante (port2): MPLS (port4): ToHQ:	MPLS Redundante (port2): MPLS (port4): ToHQ:
QoS_To_BO	10.10.3.254	MPLS Redundante (port2): MPLS (port4): ToNYC:	MPLS Redundante (port2): MPLS (port4): ToNYC:	MPLS Redundante (port2): MPLS (port4): ToNYC:

Figura 2.25. Monitoreo de enlaces del Centro de Datos

Finalmente, la sucursal cumple un mecanismo similar a la sede principal y Centro de Datos. Se encarga de monitorear los enlaces dirigidos el Centro de Datos a través del *"QoSDC",* a la sede principal a través del *"QoSHQ"* y a Internet a través del *"QoS_Internet".* En la Figura 2.26. se visualizan los enlaces monitoreados.

Name	Detect Server	Packet Loss	Latency	Jitter
QoSDC	http://10.10.2.100/	ToDC: ToHQ:	ToDC: ToHQ:	ToDC: ToHQ:
QoSHQ	10.10.1.100	ToDC: ToHQ:	ToDC: ToHQ:	ToDC: ToHQ:
QoSInternet	8.8.8.8	WAN1 (port1): WAN2 (port3):	WAN1 (port1): WAN2 (port3):	WAN1 (port1): WAN2 (port3):

Figura 2.26. Monitoreo de enlaces de la Sucursal

2.2.6.7 FortiManager en la SD-WAN

El dispositivo FortiManager, es el encargado de la administración y configuración de equipos de manera centralizada. Está ubicado en la sede principal de Guayaquil, de tal manera que se puede definir nuevas políticas, VPN, reglas, etc. a todos los equipos FortiGate a través de su GUI. El despliegue de nuevas oficinas remotas o ZTP se lo puede realizar desde FortiManager, sin que el administrador de red tenga que desplazarse al sitio. Su funcionamiento en la red es muy importante, ya que actúa como centro de control y análisis.

2.2.6.8 FortiAnalyzer en la SD-WAN

Las funciones de FortiAnalyzer están habilitadas en FortiManager, por lo tanto, se encuentra ubicado en la misma sede principal. Su función en la red es el análisis del tráfico, generación automática de informes, emisión de reportes de seguridad, entre otros aspectos

que permitan conocer el estado de la red. El objetivo de usar un único dispositivo para tareas de control y análisis es minimizar y optimizar recursos de la PC, ya que el dispositivo FortiAnalyzer consume 4 MB de RAM y 2 vCPU. El uso de dispositivos independientes es aconsejable en caso de necesitar mayor espacio para almacenamiento de informes y reportes.

2.3 EMULACIÓN DE LA RED

En este apartado se indica específicamente la configuración de cada equipo, para que cumpla con el funcionamiento analizado anteriormente. En caso de que el mecanismo de configuración sea similar en 2 o más dispositivos, se detalla solamente el de uno de ellos.

2.3.1 CONFIGURACIÓN DE LA RED MPLS

Los enrutadores de la red MPLS mantienen el mismo mecanismo de configuración, difiriendo únicamente en las interfaces, direcciones IP y el protocolo BGP; por lo tanto, se explicará el de un *Provider Edge Router,* el mismo que requiere más parámetros de configuración.

Tanto en el *router* PE como el *router* P, lo primero a configurar son las direcciones IP, las interfaces de *Loopback,* y el protocolo de enrutamiento mencionado OSPF. Posteriormente, se configura MPLS en cada uno de los enrutadores, como se visualiza en la Figura 2.27.

```
interface FastEthernet0/1
 ip address 172.16.5.5 255.255.255.252
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls ip
 ip rsvp bandwidth 1000
```

Figura 2.27. Configuración de MPLS en una interfaz del *router* PE

A continuación, se configura la Ingeniería de Tráfico junto con los túneles o VPNs, como se muestra en la Figura 2.28.

Por otro lado, en la Figura 2.29. se visualiza la configuración OSPF en el FortiGate, que se encarga de interconectar la sede principal y el Centro de Datos a través de la red MPLS. Los parámetros de OSPF en la GUI de FortiGate son los mismos que se configuran a través del CLI como área, redes directamente conectadas e interfaces.

```
router ospf 1
 mpls traffic-eng router-id Loopback10
 mpls traffic-eng area 0
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 172.16.5.0 0.0.0.3 area 0
 network 172.16.5.4 0.0.0.3 area 0
 network 172.16.5.16 0.0.0.3 area 0
interface Loopback10
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel0
 ip unnumbered Loopback10
 mpls ip
 tunnel destination 3.3.3.3
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth  800
 tunnel mpls traffic-eng path-option 1 dynamic
 no routing dynamic
```

Figura 2.28. Configuración de Ingeniería de Tráfico y Túnel en el *router* PE

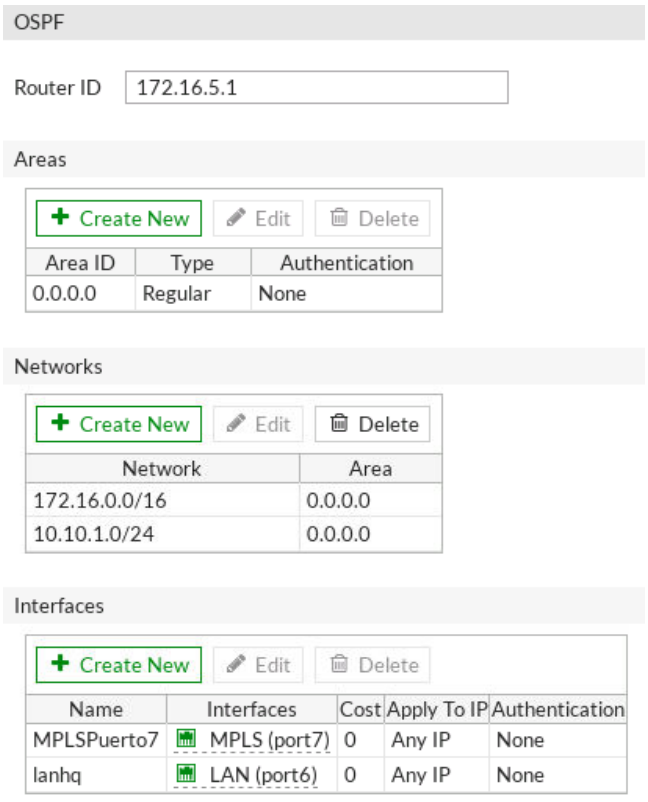


Figura 2.29. Configuración OSPF en FortiGate

2.3.2 CONFIGURACION DE LA RED DE ACCESO REMOTO

La configuración de la red dedicada a los usuarios que necesiten acceder fuera de las oficinas de la empresa es simple, es decir solamente se configura en un enrutador una red que tenga acceso a Internet. Con este propósito se habilita un protocolo de enrutamiento y

una lista de acceso que se encargue de permitir la navegación solo a los usuarios de esa red.

2.3.3 CONFIGURACIÓN DE PUERTOS

En esta sección se explican detalladamente los parámetros a configurar de un puerto, ya que los demás cumplen el mismo mecanismo. En el presente caso se toma como ejemplo a la sede principal.

En la configuración de interfaces se tiene la facilidad de asignarle un nombre e inclusive un rol. En este caso, se toma como ejemplo la configuración del puerto conectado a la red de área local de la sede principal llamado *"LAN"*, con la opción de añadirle una dirección IP de forma manual o DHCP; para la emulación se configura de forma manual. Los accesos administrativos permitidos son importantes, ya que de acuerdo con el rol que cumple cada puerto van variando; en el presente caso se necesita acceder a *"HTTPS", "HTTP", "PING", "SSH"* y *"FMG-Access".* Además, está la opción de servidor DHCP la cual será habilitada solamente en esta interfaz. En la Figura 2.30. se visualiza la configuración del puerto LAN.

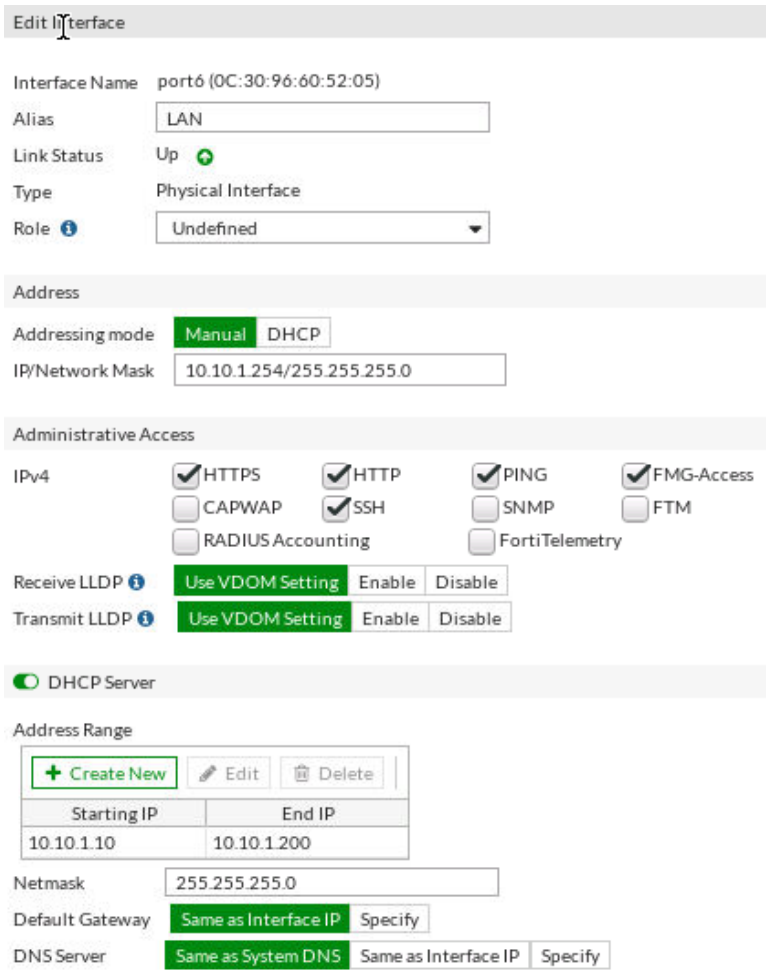
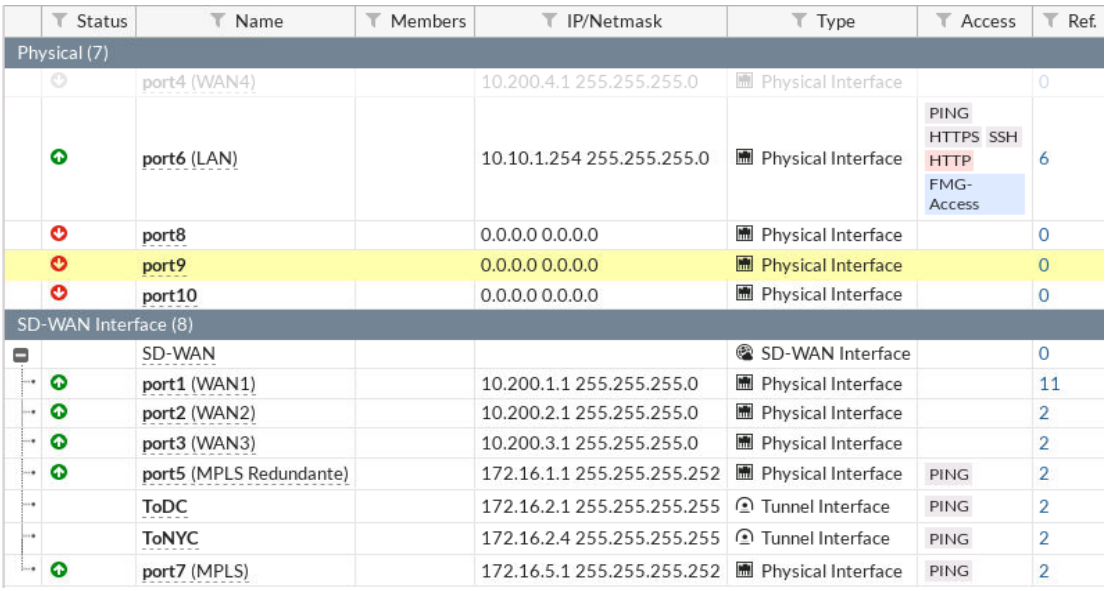


Figura 2.30. Configuración puerto LAN de la Sede Principal

En la Figura 2.31. se visualizan todas las interfaces configuradas en la sede principal, tomando en cuenta que algunas de ellas forman parte de la SD-WAN. Al igual que en la sede principal, el Centro de Datos y la sucursal muestran un esquema similar.



	Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (7)							
		port4 (WAN4)		10.200.4.1 255.255.255.0	Physical Interface		0
		port6 (LAN)		10.10.1.254 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	6
		port8		0.0.0.0 0.0.0.0	Physical Interface		0
		port9		0.0.0.0 0.0.0.0	Physical Interface		0
		port10		0.0.0.0 0.0.0.0	Physical Interface		0
SD-WAN Interface (8)							
		SD-WAN			SD-WAN Interface		0
		port1 (WAN1)		10.200.1.1 255.255.255.0	Physical Interface		11
		port2 (WAN2)		10.200.2.1 255.255.255.0	Physical Interface		2
		port3 (WAN3)		10.200.3.1 255.255.255.0	Physical Interface		2
		port5 (MPLS Redundante)		172.16.1.1 255.255.255.252	Physical Interface	PING	2
		ToDC		172.16.2.1 255.255.255.255	Tunnel Interface	PING	2
		ToNYC		172.16.2.4 255.255.255.255	Tunnel Interface	PING	2
		port7 (MPLS)		172.16.5.1 255.255.255.252	Physical Interface	PING	2

Figura 2.31. Interfaces de la Sede Principal

2.3.4 CONFIGURACIÓN DE VPN

En este caso se explica la configuración de una VPN, ya que todas las restantes cumplen el mismo mecanismo. La VPN llamada *"ToDC",* se encarga de dirigir el tráfico desde la sede principal hacia el Centro de Datos a través de un túnel. Los parámetros de configuración son el *Gateway* remoto o dirección IP de salida, método de autenticación y algoritmos de cifrado, como se muestra en la Figura 2.32.

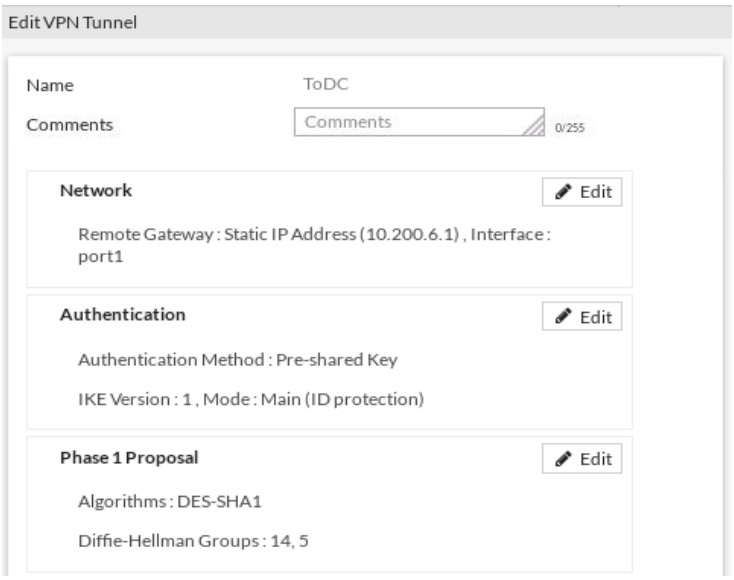


Figura 2.32. Configuración de VPN *"ToDC"*

Por otro lado, está la SSL-VPN que permite el acceso de manera segura a usuarios a través del portal web. Los parámetros de configuración son interfaz, puerto por donde van a ingresar los usuarios, restricción de acceso, certificado de servidor, rango de direcciones, servidor DNS y el tipo de acceso a grupos de usuarios autenticados. En la Figura 2.33. se muestra la configuración de una SSL-VPN en FortiGate.

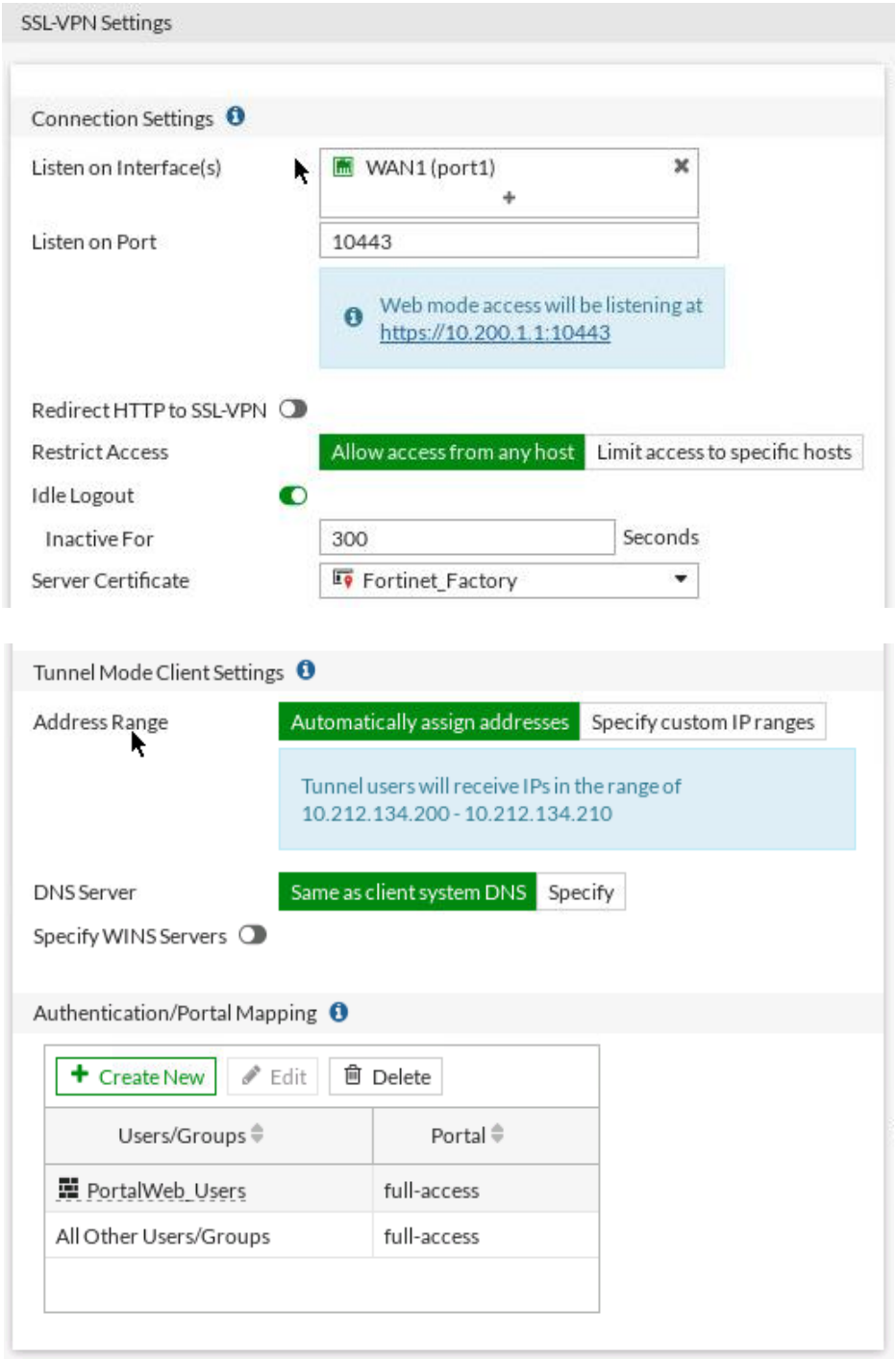


Figura 2.33. Configuración de una VPN

2.3.5 CONFIGURACIÓN DE POLÍTICAS Y OBJETOS

De igual manera, se explica la configuración de una sola política ya que las otras mantienen el mismo mecanismo, basados en su origen y destino.

El panel de configuración de las políticas muestra los siguientes parámetros: interfaces de entrada y de salida, origen y destino, horario de programación, servicios, acciones de aceptación o denegación de tráfico, modo de inspección, tipo de inspección SSL, perfiles de seguridad y opciones de identificación. En la Figura 2.34. se muestra el esquema de configuración.

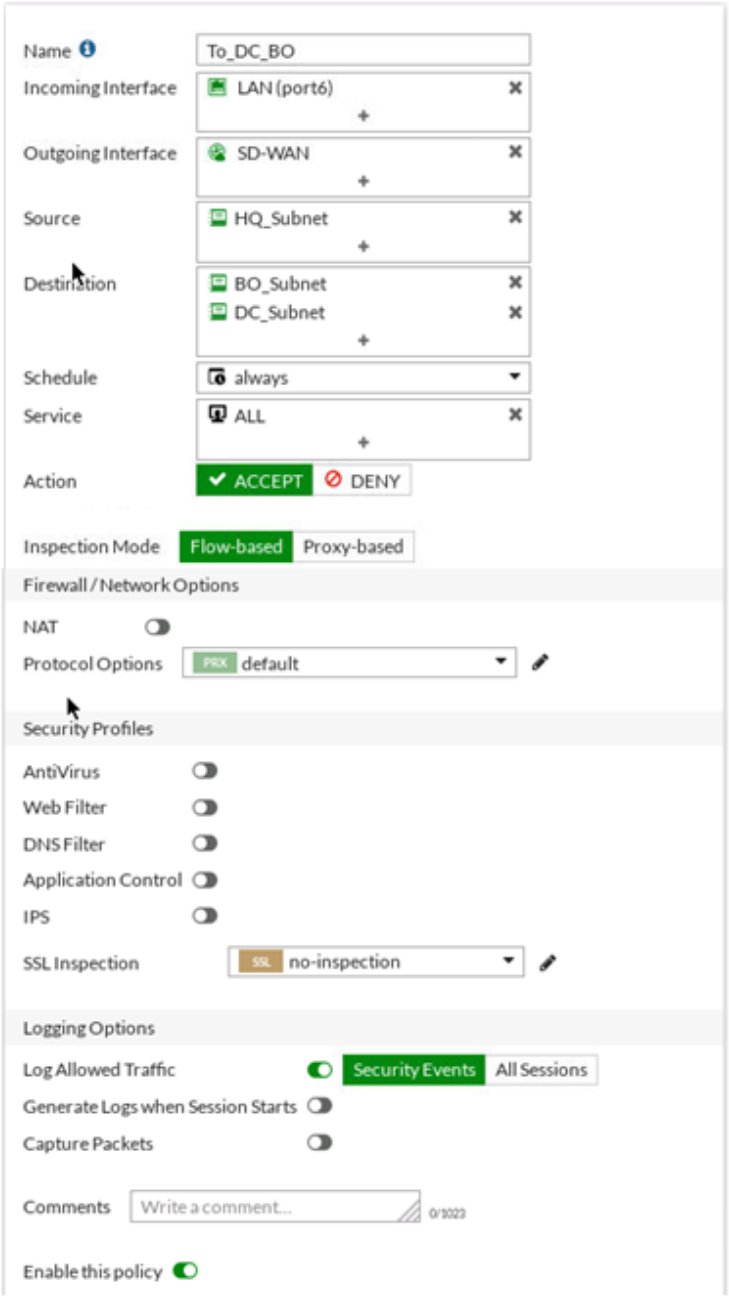
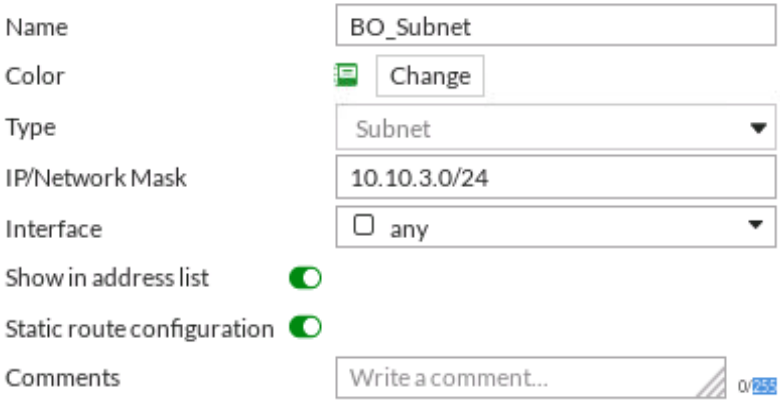


Figura 2.34. Configuración de seguridad asociada a la política "*To_DC_BO*"

El NAT es configurado o habilitado únicamente en las políticas de acceso a Internet como se muestra en la Figura 2.35. correspondiente a la política de la sede principal.

Figura 2.35. Configuración de NAT en política de acceso a Internet

En la Figura 2.36. se visualiza la configuración de objetos, encargada de asignar un nombre a una subred o dirección IP única para una mejor comprensión del funcionamiento de las políticas.



Name	Type	Details	Interface	Visibility	Ref.
Address 11					
BO_Subnet	Subnet	10.10.3.0/24		Visible	6
DC_Subnet	Subnet	10.10.2.0/24		Visible	8
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
HQ_Subnet	Subnet	10.10.1.0/24		Visible	11
MPLS Network	Subnet	172.16.5.0/24		Visible	2
MPLS Redundancy	Subnet	172.16.1.0/30		Visible	2
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel...	Visible	3
VPN	Subnet	172.16.2.0/24		Visible	2
Webterm1	Subnet	10.10.1.10/32		Visible	1
all	Subnet	0.0.0.0/0		Visible	8

Figura 2.36. Configuración y lista de objetos o direcciones

2.3.6 CONFIGURACIÓN DE REGLAS SD-WAN

En el panel de configuración de las reglas SD-WAN se establece las direcciones de origen y destino, el tipo de protocolo de transporte, la aplicación, la estrategia para la elección de la mejor ruta, las interfaces de salida, la medición del SLA o QoS y el criterio de calidad. Todas las reglas tienen el mismo mecanismo de configuración y difieren únicamente en las direcciones y criterios de calidad por parte del administrador; en este caso se establece como criterio la latencia. En la Figura 2.37. se visualiza el panel de configuración de las reglas SD-WAN.

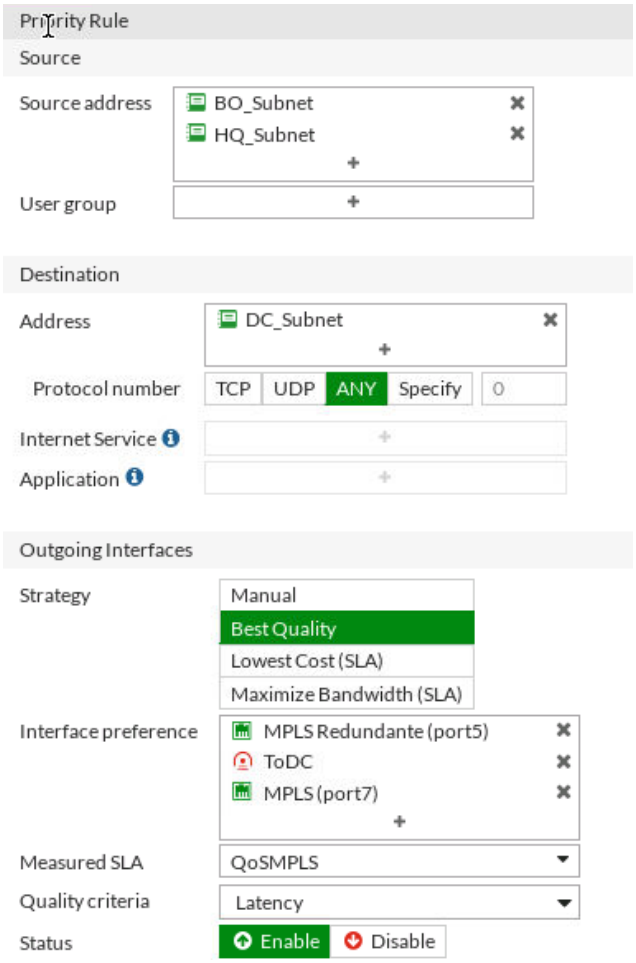


Figura 2.37. Parámetros de configuración de reglas SD-WAN

2.3.7 CONFIGURACIÓN DE PERFILES DE SEGURIDAD

En primer lugar, el perfil de seguridad de Antivirus presenta los siguientes parámetros de configuración: bloqueo o monitoreo de virus, protocolos inspeccionados, tratamiento de archivos ejecutables de Windows y protección de *malwares* de celulares. En este caso, se configura el perfil por defecto, pero se pueden crear otros perfiles siempre y cuando tenga la licencia de FortiGuard. En la Figura 2.38. se muestra la configuración.

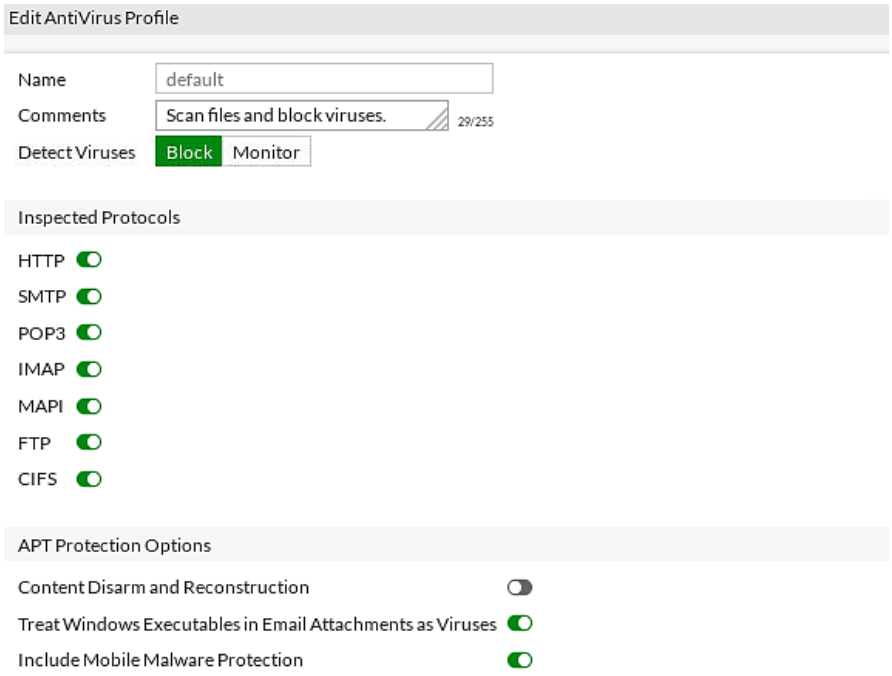


Figura 2.38. Configuración de perfil de Antivirus

En segundo lugar, los perfiles de control de aplicaciones. De igual manera, se configura el perfil por defecto debido a la necesidad de la licencia de FortiGuard. Los parámetros de configuración disponibles son: categorías de aplicaciones, aplicación del protocolo de red, filtros o aplicaciones anuladas, bloqueo del tráfico fuera de los puertos por defecto, identificación de tráfico DNS, entre otros. En la Figura 2.39. se muestra un ejemplo de configuración de control de aplicaciones.

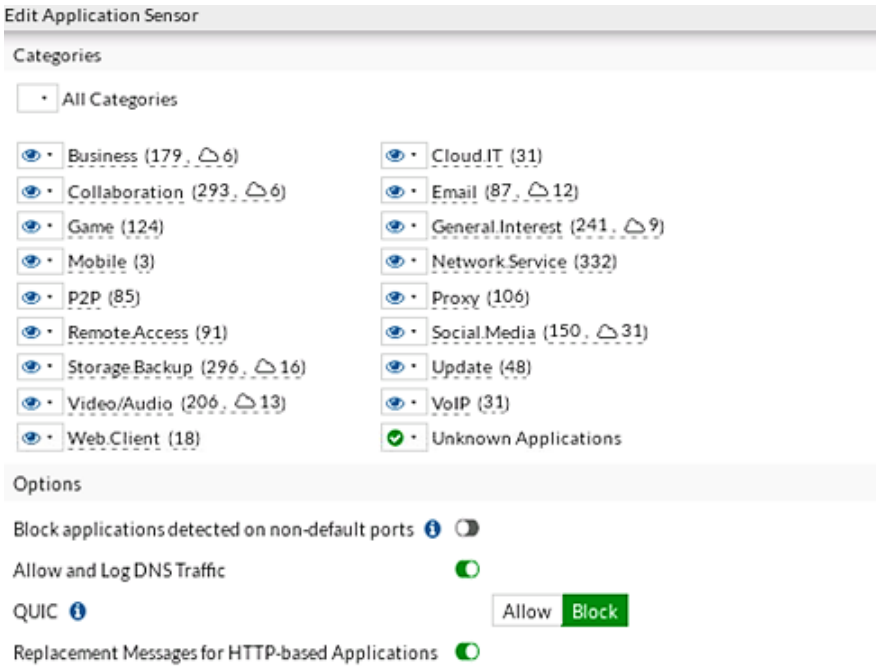


Figura 2.39. Panel de configuración de control de aplicaciones

En el sistema de prevención de intrusos se configura el bloqueo de URL maliciosos, filtros de IPS, monitoreo o bloqueo hacia sitios Botnet, entre otros. En la Figura 2.40. se muestran los parámetros de configuración más importantes.

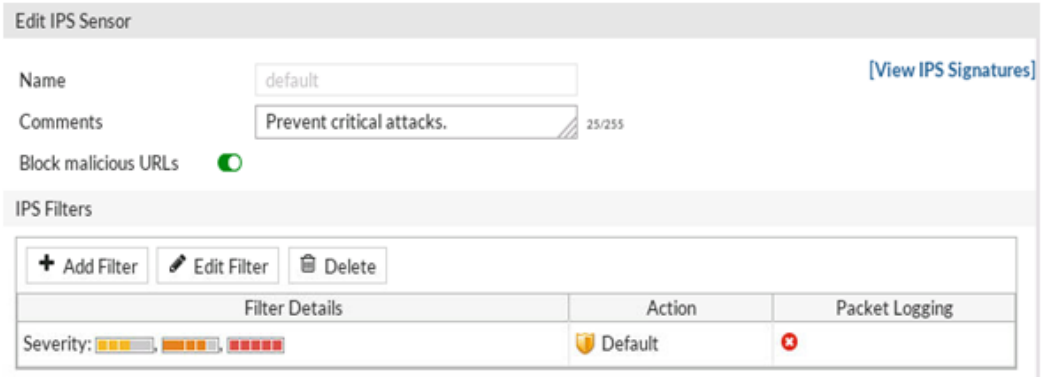


Figura 2.40. Configuración de IPS

Dentro del IPS, están las políticas de denegación de servicios (DoS) que permiten configurar la interfaz de entrada, direcciones de origen y destino, servicios y anomalías de capa 3 y capa 4. Las anomalías hacen referencia a la inundación de paquetes TCP, UDP, e ICMP; los umbrales son establecidos en base al criterio del administrador, de tal manera que, al sobrepasar ese umbral se identifica y bloquea todos los paquetes de ese tipo. En la Figura 2.41. se muestra su panel de configuración.

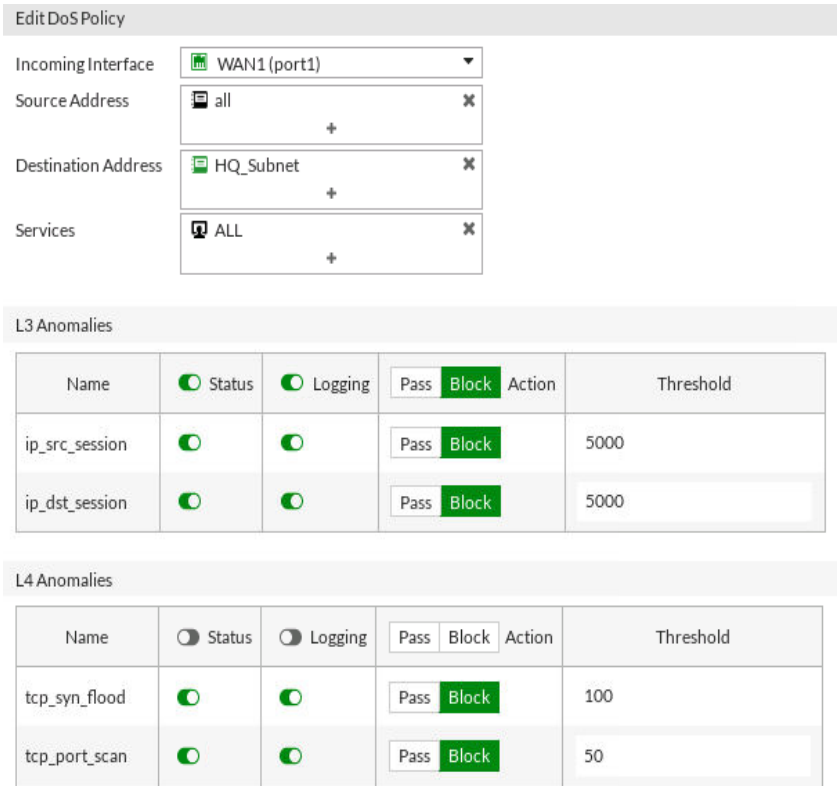


Figura 2.41. Configuración de políticas de DoS

Finalmente, se encuentra la configuración de los grupos de aplicación que funcionan a través de las políticas de *traffic shaping.* En este caso, se configura para el grupo de Teletrabajo que contiene aplicaciones como Skype, Telegram, Zoom y Webex. En la Figura 2.42. se visualizan los parámetros de configuración de las políticas como direcciones de origen y destino, tipo de servicio, grupo de aplicación (Teletrabajo), interfaz de salida, el tipo de compartición y la prioridad (alta).

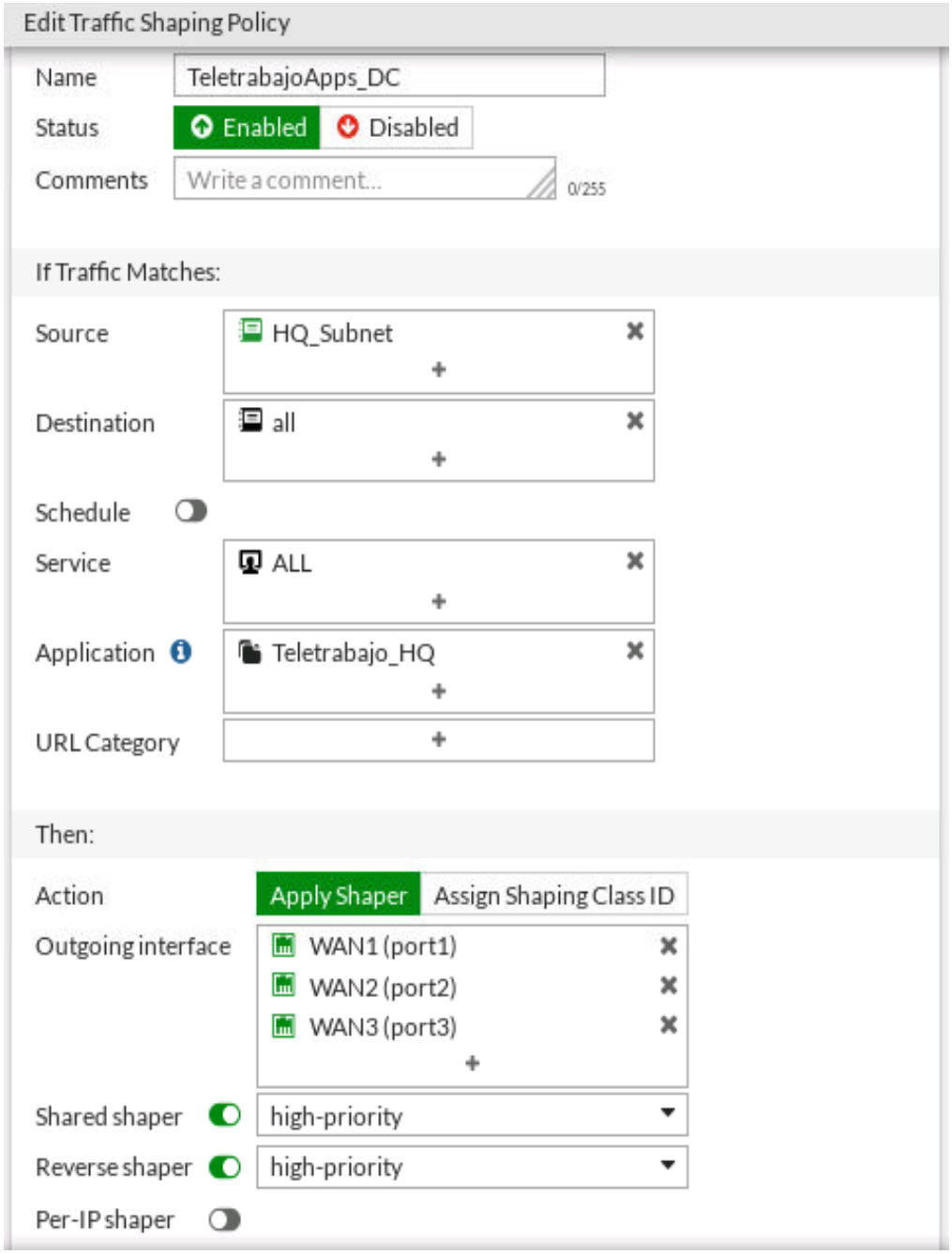


Figura 2.42. Configuración de políticas de *Traffic Shaping*

2.3.8 CONFIGURACIÓN DE LA CALIDAD DE SERVICIO EN LA SD-WAN

La configuración del monitoreo de enlaces define como parámetros principales los enlaces, el servidor remoto, estado de enlace, tiempos de revisión, tiempos de restauración y actualizaciones de rutas estáticas. Es necesario que en el destino exista un servidor para que funcione correctamente, en la Figura 2.43. se visualizan los parámetros.

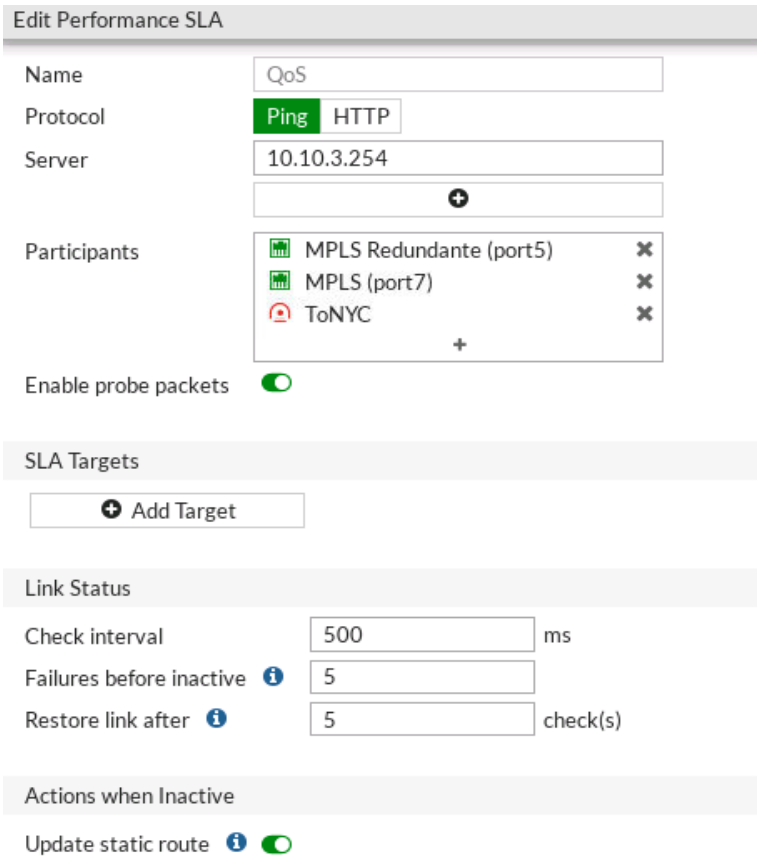


Figura 2.43. Configuración de QoS

2.3.9 CONFIGURACIÓN DE FORTIMANAGER CON FORTIANALYZER

Antes de agregar los dispositivos a FortiManager, es importante configurar dos parámetros a través del CLI; el algoritmo de cifrado y el protocolo SSL de FortiManager. Posteriormente, se procede a la configuración en la GUI de FortiManager, en la que se agregan los equipos FortiGate y se habilitan las características de FortiAnalyzer. El resto de las configuraciones como políticas, túneles, seguridad, SD-WAN, entre otros aspectos se los realiza de la misma manera que en los dispositivos FortiGate. Además, en FortiManager existe una base de datos independiente para configuraciones generales de cada FortiGate, mientras que una sola base datos general para las políticas, VPN, objetos, seguridad, etc. de todos los equipos. Esto ayuda a que el despliegue de nuevos equipos sea más rápido y eficiente, ya que la configuración se realiza una sola vez. En la Figura 2.44. se visualiza el panel de configuración para añadir dispositivos.

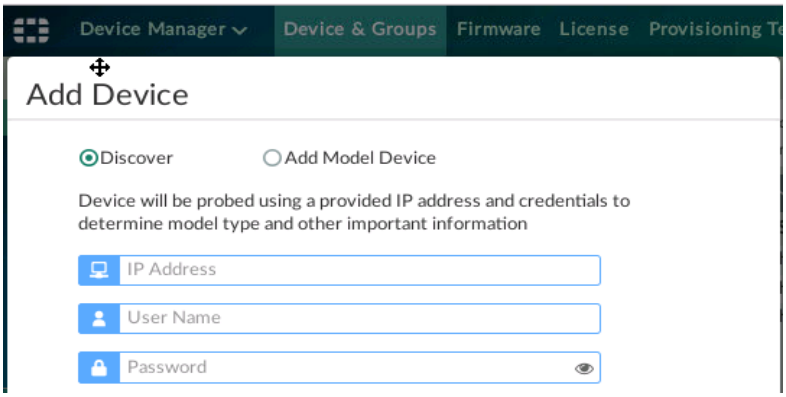


Figura 2.44. Configuración de dispositivos en FortiManager

2.3.10 CONFIGURACIÓN DE SERVIDORES

En esta sección se explica la configuración del servidor DNS y del servidor de correo, ya que los servidores de Syslog y TFTP vienen pre-instalados y configurados en un *appliance* disponible en la página web de GNS3.

La solución utilizada para el servidor DNS es Dnsmasq, adecuada para las distribuciones Linux. En la Figura 2.45. se visualizan los comandos ejecutados en *Ubuntu Server* para la correcta instalación del servidor.

```
sudo su
cd
apt-get update
apt-cache search dns
apt-cache search dnsmasq
apt-get install dnsmasq
```

Figura 2.45. Instalación del servidor DNS

Una vez instalado, se procede a editar el archivo de configuración de dnsmasq, en el que se habilitan las opciones de *"domain-needed"* y *"bogus-priv"*. Posteriormente, se procede a añadir las direcciones con sus respectivos nombres de dominio en el mismo archivo y se reinicia dnsmasq, como se muestra en la Figura 2.46.

```
nano /etc/dnsmasq.conf
#domain-needed          (Borrar #)
#bogus-priv             (Borrar #)
#local=/localnet/       (Cambio por local=/home.com/)

(añado las direcciones abajo de address=/double..)

address=/r1/10.1.1.1
address=/ubuntu-server/10.1.1.200
address=/docker2/10.1.1.102
systemctl restart dnsmasq
```

Figura 2.46. Configuración del servidor DNS

Por otro lado, el servidor de correo se instala usando el *software* Postfix y Dovecot. En la Figura 2.47. se muestran todos los paquetes necesarios y los comandos a ejecutar en *Ubuntu Server* para la instalación de este servidor; es importante mencionar que para algunos paquetes es necesario añadir los repositorios.

```
sudo su
apt-get update
apt-get upgrade
clear
apt install postfix
systemctl restart postfix
add-apt-repository ppa:ondrej/php
apt install php5.6
apt install apache2
apt install dovecot-imapd dovecot-pop3d
sytemctl start dovecot
sytemctl enable dovecot
```

Figura 2.47. Instalación de Servidor de Correo

Una vez instalado, se procede a la instalación de *Squirrelmail* que es una aplicación de correo justamente para servidores. Posteriormente, se configurarán 3 usuarios con el nombre de dominio *"sdwan.local"*, es decir las cuentas de correo electrónico tendrían la siguiente forma: *julian@sdwan.local, domenica@sdwan.local y javier@sdwan.local,* como se visualiza en la Figura 2.48. Finalmente, su acceso es a través del nombre de dominio www.sdwanmail.com que está configurado en el servidor DNS.

```
useradd javier
passwd javier
useradd domenica
passwd domenica
useradd julian
passwd julian

cd squirrelmail
mkdir javier
mkdir domenica
mkdir julian
usermod -m -d /var/www/html/squirrelmail/javier javier
usermod -m -d /var/www/html/squirrelmail/domenica domenica
usermod -m -d /var/www/html/squirrelmail/julian julian
ls -l
chown -R javier :javier javier
chown -R domenica: domenica domenica
chown -R julian:julian julian
ls -l
clear
```

Figura 2.48. Configuración de cuentas de correo electrónico

3. RESULTADOS Y DISCUSIÓN

En este capítulo se analizan los resultados obtenidos durante la emulación de la SD-WAN, así como las ventajas mencionadas acerca del uso del programa GNS3. De esta manera se comprobará el funcionamiento de la red y se validarán los conceptos y cualidades descritas anteriormente.

3.1 EMULACIÓN DE LA SD-WAN HÍBRIDA

En este apartado se comprobará que la SD-WAN funcione correctamente, desglosando cada uno de los parámetros que posibilitan el uso de ésta, por ejemplo, control centralizado, selección dinámica de ruta, aprovisionamiento de toque cero (ZTP), monitorización en tiempo real, entre otros. En primer lugar, la topología completa de la SD-WAN con todas las redes de área local y redes de área extendida, así como los emuladores de enlace se detallan en el ANEXO B.

3.1.1 TRANSPORTE MÚLTIPLE

En esta sección se comprueba que la SD-WAN pueda controlar múltiples rutas, es decir, la posibilidad de utilizar la red MPLS, túneles IPsec y la infraestructura pública de Internet como redes de transporte para enviar el tráfico hacia Internet u oficinas remotas. Para la verificación de su funcionamiento se envía un *ping* desde la sede principal hacia la sucursal, de tal manera que llegue a través de la red MPLS o el túnel IPsec que usa el enlace de banda ancha de Internet. El objetivo es poder visualizar que tanto la red MPLS, los túneles y las conexiones de Internet estén trabajando en conjunto para validar el transporte múltiple de SD-WAN. Tomando en cuenta que actualmente la mayoría de las empresas tienen infraestructura MPLS y deseen mantenerla, se la despliega en la emulación; ésta se combina con los diferentes transportes de la SD-WAN para tener una SD-WAN Híbrida.

En la Figura 3.1. se visualiza el *ping* desde la sede principal hacia la sucursal, utilizando como interfaz de salida la *"WAN1"* correspondiente a uno de los enlaces de Internet. Como se puede ver, se realiza un *traceroute* para determinar la ruta que toman los paquetes hacia su destino. En este caso, se utiliza un túnel IPsec por mayor seguridad, debido a que la información pasa a través de los enlaces directamente conectados a Internet. El túnel llamado *"ToNYC"* corresponde a la dirección 172.16.2.5. que se visualiza al realizar el *traceroute.*

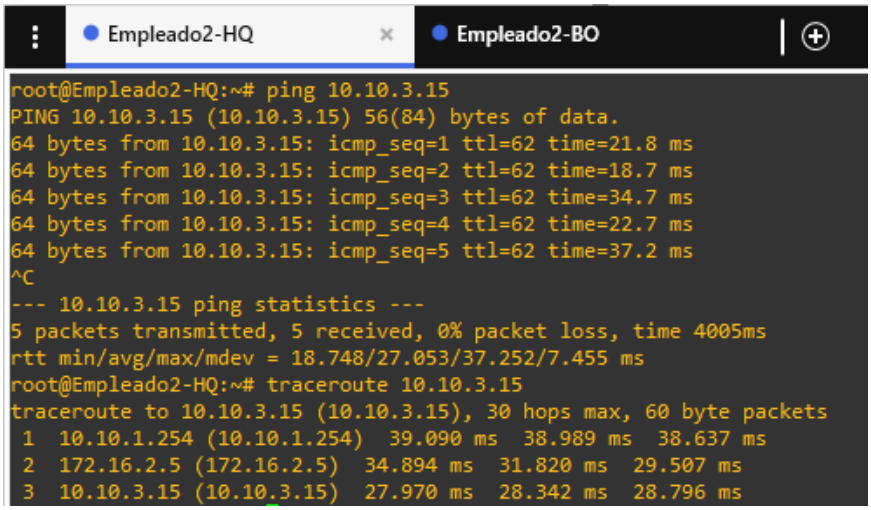


Figura 3.1. Ping HQ-BO a través del túnel IPsec

En el caso de que se desee usar otra red de transporte para enviar los mismos paquetes hacia la sucursal, la SD-WAN dispone de la ruta a través de la red MPLS. De la misma forma, se realiza un *traceroute* que permite visualizar en la Figura 3.2 cada uno de los saltos, los cuales corresponden a los *routers* de la red MPLS.

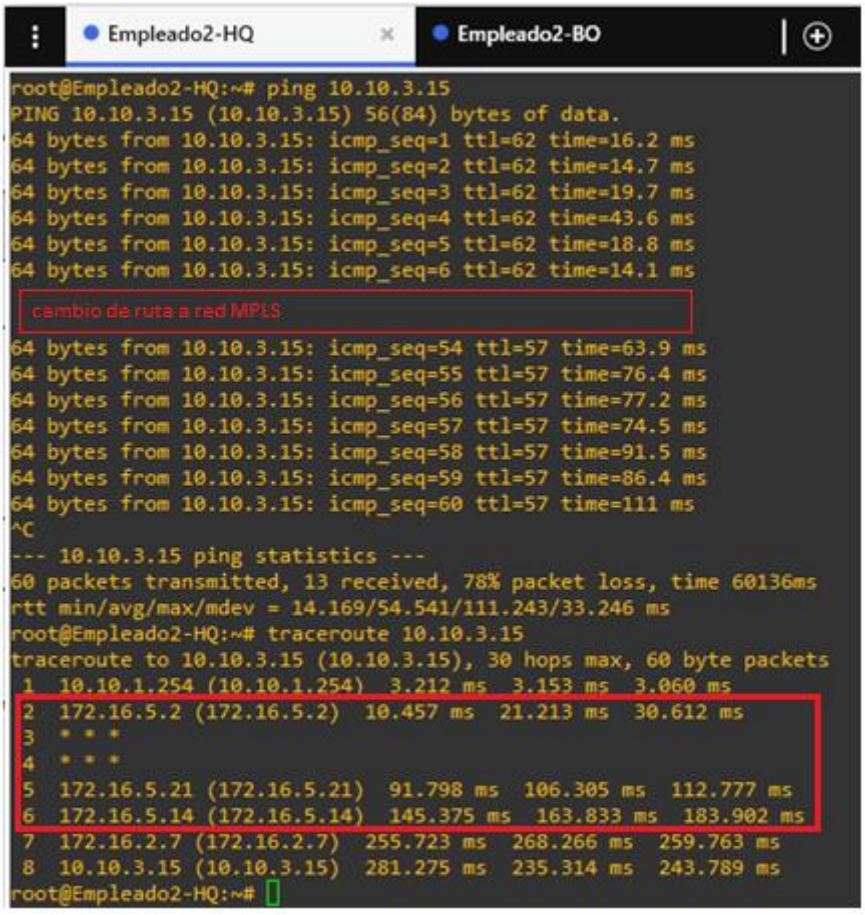


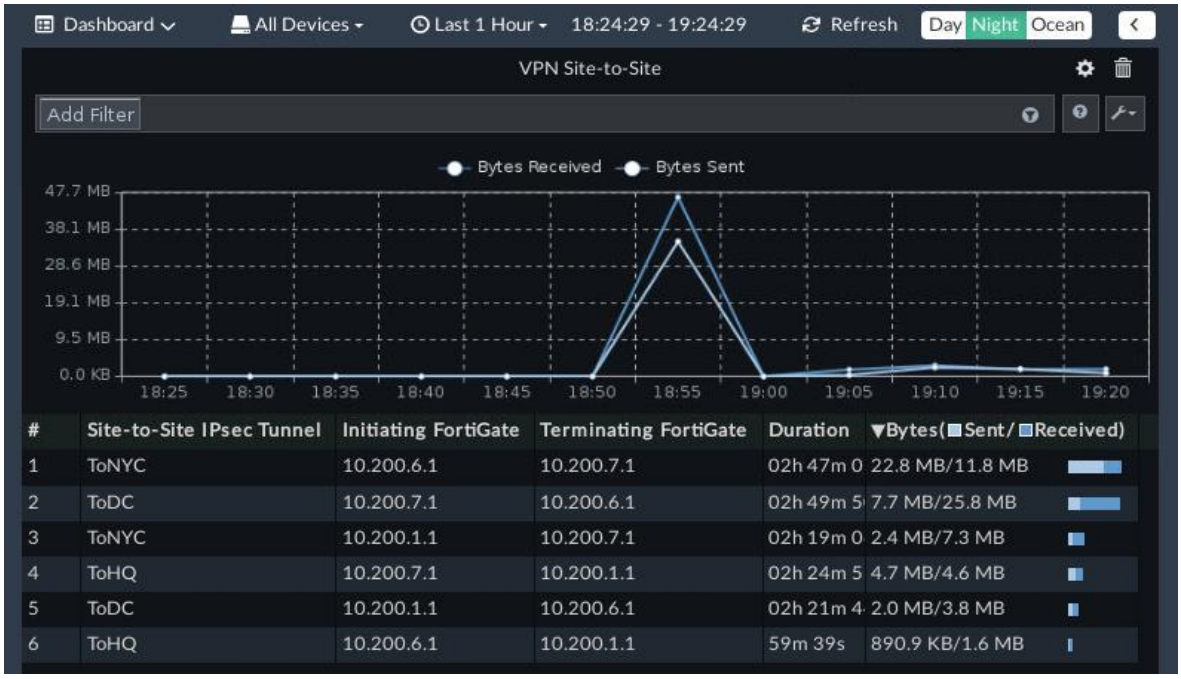
Figura 3.2. Ping HQ-BO a través de la red MPLS

Finalmente, se puede notar la interacción de la red MPLS con los túneles IPsec o Internet, es decir la SD-WAN Híbrida soporta y controla diferentes tipos de conexiones. En un ambiente real, se necesitarían las direcciones IP públicas que emiten los ISP en lugar de las direcciones privadas establecidas en la emulación denominadas WAN1, WAN2 y WAN3. El propósito es entender cómo la SD-WAN funciona como una red multi-transporte, ya que el intercambio de direcciones públicas por privadas es simple.

3.1.2 IPSEC-VPN

En esta sección se comprueba que la SD-WAN es una superposición a la red existente, a través de soluciones de tunelización que permiten diferenciar la red física de la red lógica. La SD-WAN usa túneles IPsec que ofrece un cifrado completo del tráfico para protegerlo del Internet y también del ISP.

En la Figura 3.3. se visualiza que los túneles IPsec de la sede principal, el Centro de Datos, y la sucursal están habilitados y operativos. A través de FortiAnalyzer, se verifica el estado de éstos y la cantidad de bytes de entrada y salida; por lo tanto, existen 6 túneles en total, distribuidos en cada sitio como se mencionó en la sección 2.2.6.2.



#	Site-to-Site IPsec Tunnel	Initiating FortiGate	Terminating FortiGate	Duration	▼Bytes(■Sent/■Received)
1	ToNYC	10.200.6.1	10.200.7.1	02h 47m 0	22.8 MB/11.8 MB
2	ToDC	10.200.7.1	10.200.6.1	02h 49m 5	7.7 MB/25.8 MB
3	ToNYC	10.200.1.1	10.200.7.1	02h 19m 0	2.4 MB/7.3 MB
4	ToHQ	10.200.7.1	10.200.1.1	02h 24m 5	4.7 MB/4.6 MB
5	ToDC	10.200.1.1	10.200.6.1	02h 21m 4	2.0 MB/3.8 MB
6	ToHQ	10.200.6.1	10.200.1.1	59m 39s	890.9 KB/1.6 MB

Figura 3.3. Túneles IPsec habilitados

Una vez que los túneles están habilitados se realizó una captura de paquetes a través de Wireshark que permite identificar el protocolo de seguridad de Internet que se encarga de cifrar los datos. En la Figura 3.4. se visualiza el protocolo *Encapsulation Security Payload* (ESP) que es el encargado de cifrar los datos por completo, de tal manera que se verifica

que la SD-WAN está utilizando túneles IPsec que ofrecen mayor seguridad que las VPNs de MPLS.

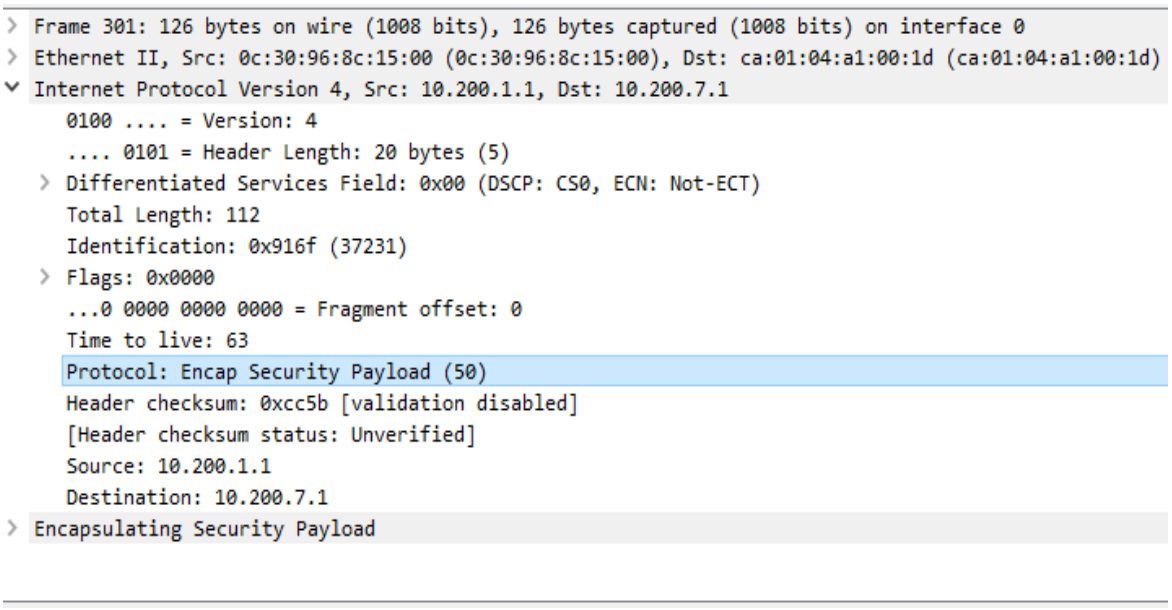


Figura 3.4. Verificación de cifrado de Túneles IPsec usando Wireshark

Finalmente, se puede comprobar que la SD-WAN garantiza mayor seguridad cifrando el tráfico que pasa a través de Internet, con túneles IPsec. A continuación, se analiza el uso de las SSL-VPN en el acceso remoto a través del portal web.

3.1.3 SSL-VPN DE ACCESO REMOTO

La SSL-VPN permite a los usuarios o empleados ubicados fuera de cualquier oficina, acceder remotamente a los recursos de la sede principal o del Centro de Datos de manera segura. Además, en esta sección se puede comprobar el funcionamiento del servidor de correo electrónico y del servidor DNS, ya que éstos son los servicios a los cuales van a acceder los empleados.

En este caso, en la Figura 3.5. se visualiza el acceso remoto de un empleado a la empresa, utilizando una conexión segura a través del portal web de FORTINET. El usuario solamente puede utilizar los servicios una vez *loggeado* en el portal. De lo contrario, no tendrá conexión a ninguno de los servidores, ni computadores de la red. Como se puede ver, la dirección IP del usuario remoto forma parte de la red 192.168.1.0/24, la cual es totalmente desconocida para la empresa.

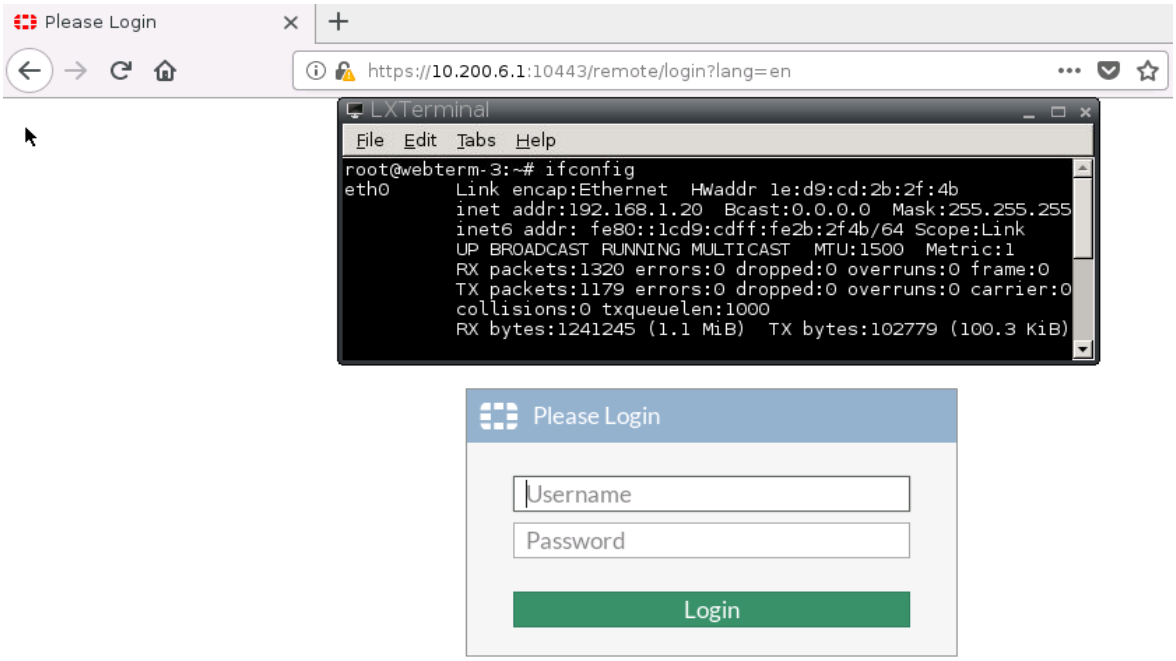


Figura 3.5. Ingreso al Portal Web Fortinet

La SD-WAN asigna un usuario y clave para acceder a los recursos internos de la empresa; una vez ingresadas las credenciales ya se tiene acceso a total a servicios de la red a través de una conexión SSL. En la Figura 3.6. se visualiza un panel de opciones que permite seleccionar el tipo de conexión que desea realizar el empleado, tal como HTTPS, SSH, VNC, entre otros.

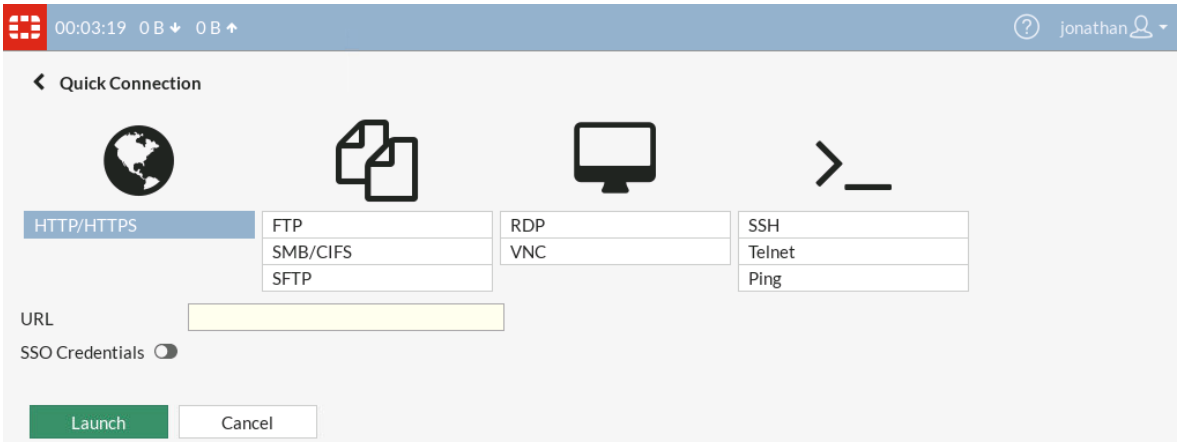


Figura 3.6. Tipos de conexión remota a través del Portal Web

Principalmente, el correo electrónico y el servidor DNS son los servicios a los cuales los empleados necesitan acceder. Por lo tanto, en la Figura 3.7. se comprueba cómo un usuario fuera de oficina puede acceder a la web de correo electrónico de la empresa. Utiliza una conexión HTTPS/HTTP y accede a través del URL www.sdwanmail.com. configurado

su dominio previamente en el servidor DNS. De esta manera, se verifica el funcionamiento de los servidores y la SSL-VPN

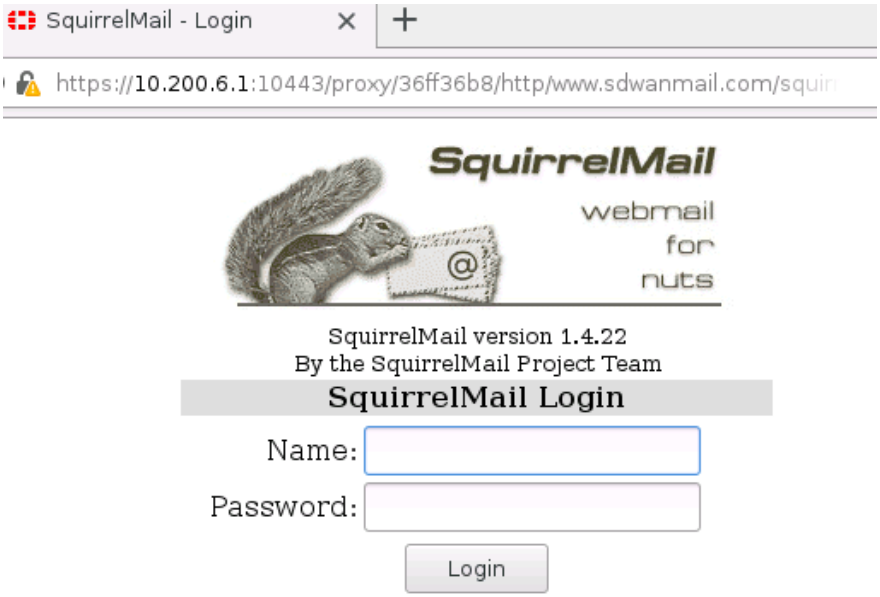


Figura 3.7. Acceso al correo electrónico usando una conexión SSL-VPN

A manera de comprobación, en la Figura 3.8. se intenta acceder al correo electrónico de la empresa desde la misma dirección IP y utilizando el mismo navegador, pero sin el portal web. En este caso, se visualiza que no existe conexión alguna con la página del correo ya que no es una conexión segura para la SD-WAN.

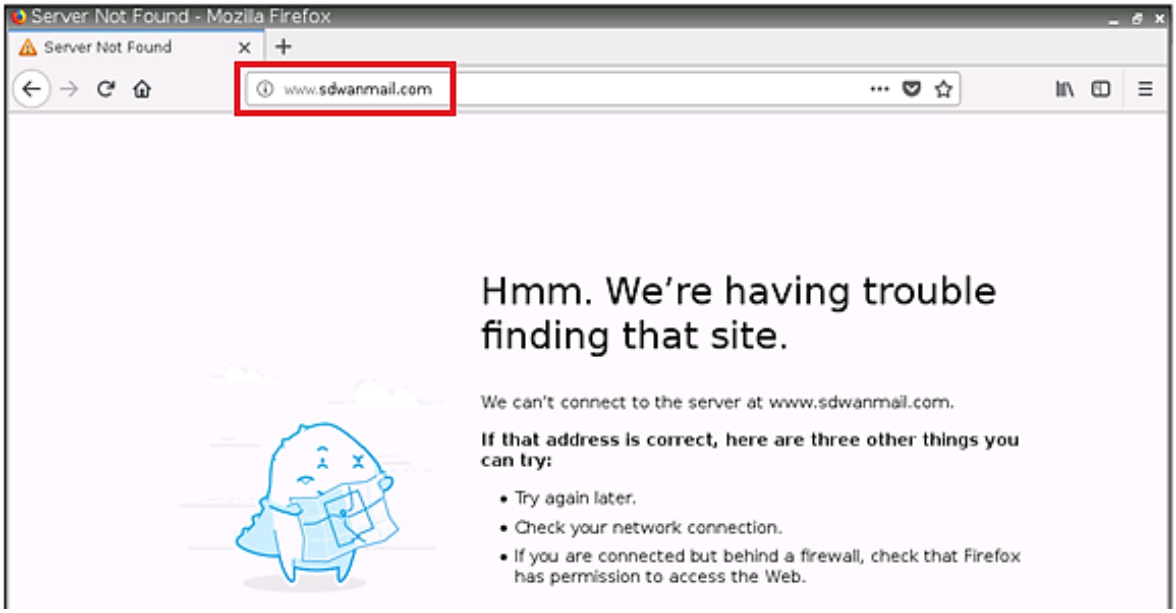
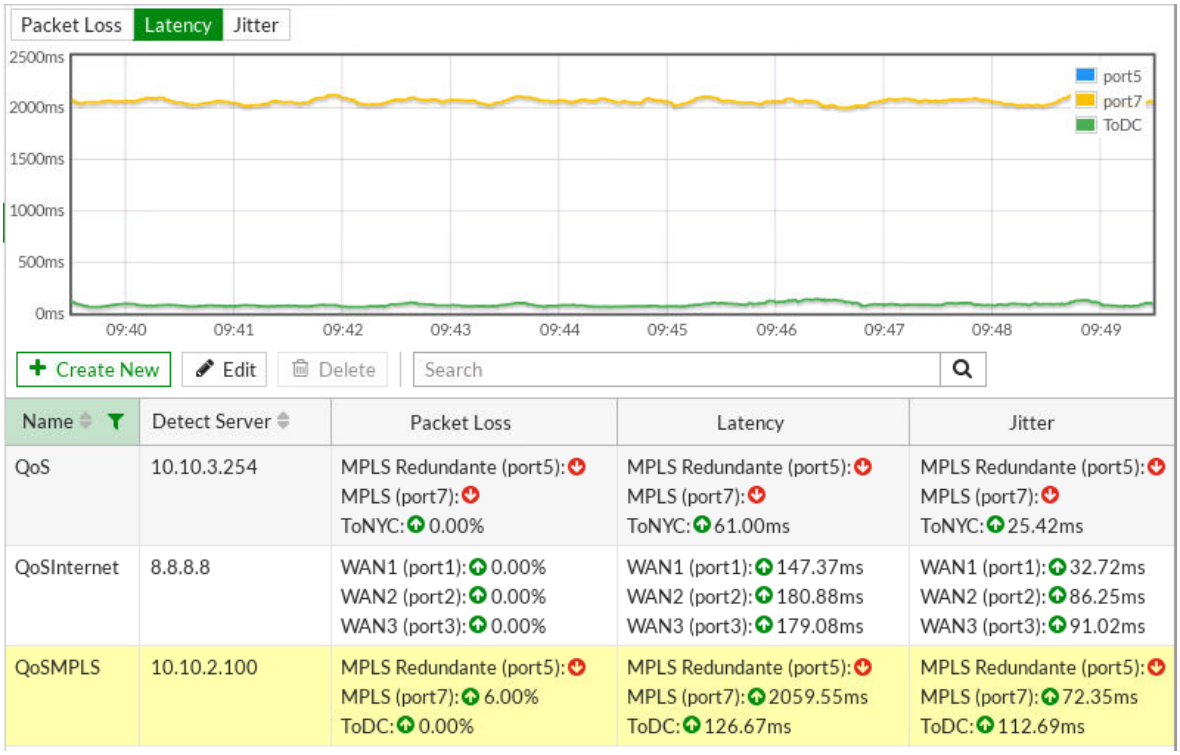


Figura 3.8. Acceso denegado al correo electrónico

3.1.4 MONITORIZACIÓN DE LA CALIDAD DE SERVICIO EN LOS ENLACES

En esta sección, se realiza en la SD-WAN un monitoreo inteligente de la Calidad de Servicio (QoS) a través del rendimiento de los enlaces en tiempo real, para lo cual se emplean tres parámetros principales como son: la pérdida de paquetes, la latencia y el *jitter;* inclusive puede basarse en un SLA. Esto permite que la SD-WAN tenga mayor conocimiento de sus enlaces para tomar decisiones sobre la selección del mejor camino.

En la Figura 3.9. se puede apreciar el monitoreo de los enlaces de la sede principal. Se observa que existen 3 destinos, correspondientes al Centro de Datos, sucursal e Internet; de tal manera que dentro de cada uno están los enlaces que utiliza la sede principal para alcanzarlos.



Name	Detect Server	Packet Loss	Latency	Jitter
QoS	10.10.3.254	MPLS Redundante (port5): MPLS (port7): ToNYC: 0.00%	MPLS Redundante (port5): MPLS (port7): ToNYC: 61.00ms	MPLS Redundante (port5): MPLS (port7): ToNYC: 25.42ms
QoSInternet	8.8.8.8	WAN1 (port1): 0.00% WAN2 (port2): 0.00% WAN3 (port3): 0.00%	WAN1 (port1): 147.37ms WAN2 (port2): 180.88ms WAN3 (port3): 179.08ms	WAN1 (port1): 32.72ms WAN2 (port2): 86.25ms WAN3 (port3): 91.02ms
QoSMPLS	10.10.2.100	MPLS Redundante (port5): MPLS (port7): 6.00% ToDC: 0.00%	MPLS Redundante (port5): MPLS (port7): 2059.55ms ToDC: 126.67ms	MPLS Redundante (port5): MPLS (port7): 72.35ms ToDC: 112.69ms

Figura 3.9. Monitorización de enlaces de la Sede Principal

Como se puede ver los enlaces *"MPLS"* y "*ToDC*" están habilitados; el camino redundante se habilita en caso de que los dos enlaces pierdan conexión, funcionando como un enlace de *backup.* La gráfica muestra cómo va variando la latencia en el tiempo, correspondiente a un promedio de *126.67 ms* del enlace *"ToDC"*.

Por otro lado, en la Figura 3.10. se visualiza un *ping* en el CLI hacia el Centro de Datos, a través del túnel *"ToDC"*, con el objetivo de comprobar que la monitorización de FORTINET se realice correctamente. Por lo tanto, el promedio de latencia de la figura anterior debe aproximarse al promedio del *ping* realizado desde una PC de la sede principal.

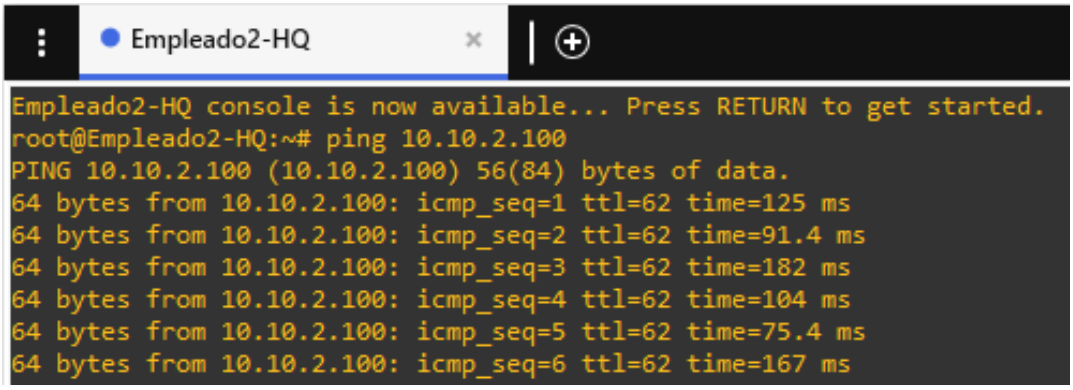


Figura 3.10. Latencia del Ping HQ-DC a través del túnel

El promedio de los tiempos de latencia corresponde a *124.13 ms* (744.8/6), valor aproximado a los *126.67 ms;* de esta manera se verifica que la monitorización está funcionando correctamente. La misma situación ocurre con los otros enlaces y hacia los otros destinos, utilizando como parámetro la latencia debido a que las reglas de la SD-WAN establecidas funcionan con éste. Sin embargo, se puede utilizar como parámetros la pérdida de paquetes, el *jitter*, o SLA, en caso de tenerlo como se muestra en la Figura 3.11.

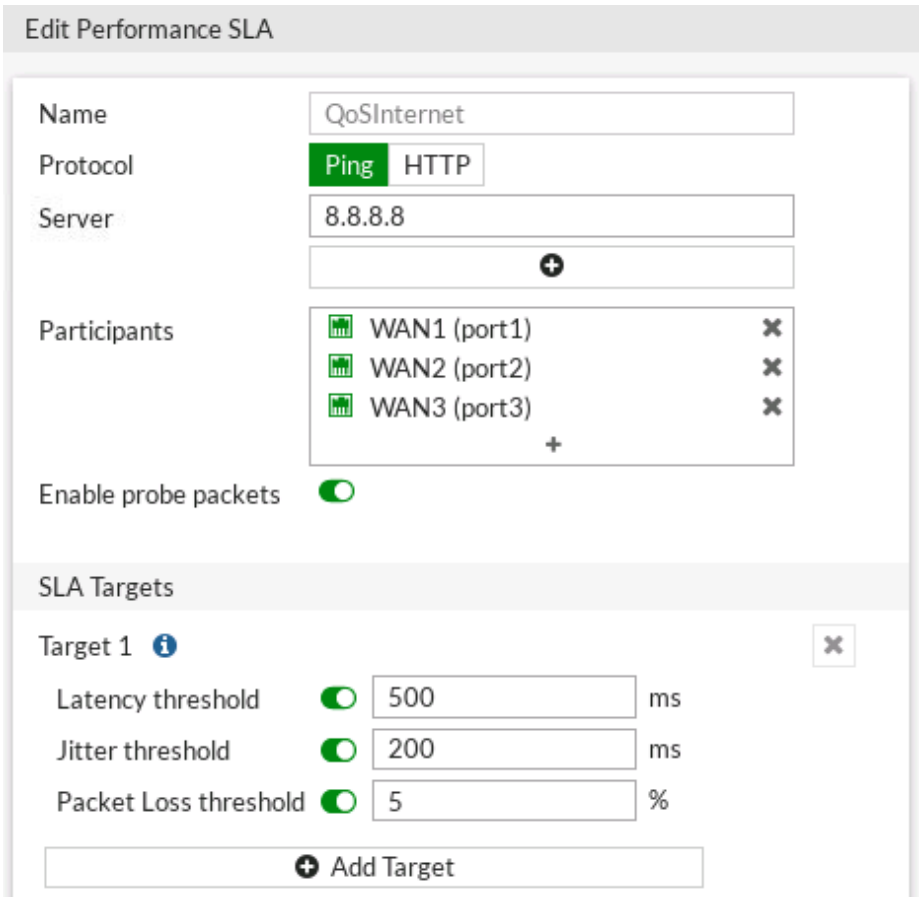


Figura 3.11. Monitoreo en base a un SLA

Finalmente, la SD-WAN ofrece un mecanismo de monitorización bastante eficaz que permite al administrador de la red conocer el estado de sus enlaces en cualquier momento e inclusive verificar si se cumple el SLA establecido entre el cliente y el ISP. En base con el estado de los enlaces, la SD-WAN toma decisiones de manera inteligente.

3.1.5 SELECCIÓN DINÁMICA DE RUTA

En esta sección se comprueba que la SD-WAN es una red automatizada, la misma que puede seleccionar las rutas de manera dinámica. La monitorización facilita a la red la posibilidad de escoger el mejor camino por el cual enviará el tráfico basado en algún parámetro o a su vez en el tipo de aplicación.

La comprobación se realiza mediante un *ping* desde la sede principal hacia el Centro de Datos, de tal manera que, en el primer escenario se hace uso del túnel *"ToDC";* en el segundo escenario la conexión a través del túnel se pierde y en el tercer escenario se emulará un aumento de latencia en el túnel a través de una herramienta llamada *NETem*. El objetivo es ver que el cambio o selección de la nueva ruta se realice de forma automática; en la Figura 3.12. se visualiza el primer escenario junto con su latencia promedio.

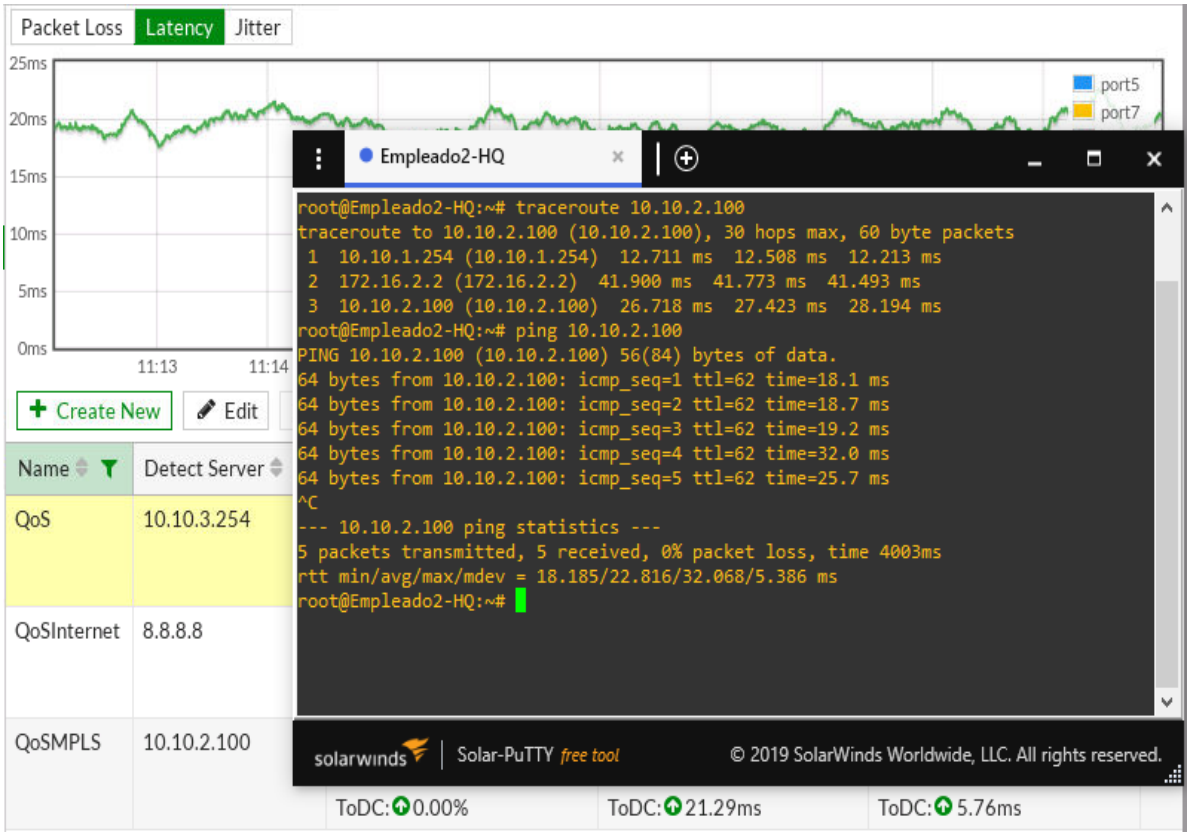


Figura 3.12. Ping HQ-DC utilizando el enlace de menor latencia (túnel)

En la Figura 3.13. se visualiza el segundo escenario. No existe ningún aumento de latencia, solamente una caída del túnel, de tal forma que automáticamente cambia al enlace MPLS ya que se perdió totalmente la conexión inicial, como se visualiza en la gráfica de monitorización del rendimiento. La respuesta frente a caídas de enlace es rápida gracias a la automatización de las operaciones de red. En el CLI se visualiza el aumento del tiempo de latencia en el cambio de enlace, y posteriormente cómo éste se va normalizando a *62.36 ms.*

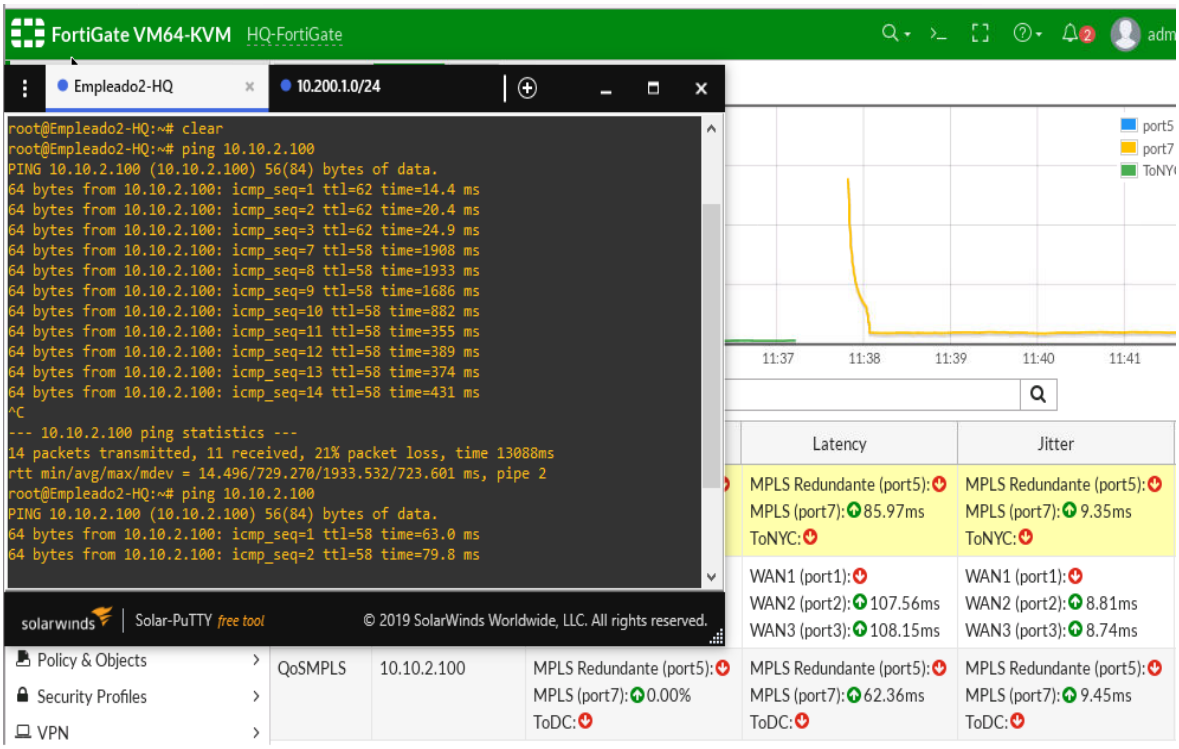


Figura 3.13. Selección dinámica de ruta por pérdida de conexión en el túnel

En la Figura 3.14. se visualiza el tercer escenario, que corresponde al aumento de latencia de *2000 ms* sobre el enlace del túnel. El objetivo en este caso es que la red automáticamente tome una decisión sobre cuál es el mejor camino, ya que ambos enlaces están disponibles. En este escenario, se decide por el enlace MPLS que es lo más lógico ya que éste presenta menor latencia.

La forma de comprobación es mediante la variación de los tiempos de latencia en el CLI y la herramienta de monitorización de enlaces de FORTINET. En la gráfica en mención se puede notar que desaparece el enlace del túnel (verde) debido al cambio de enlace y solamente se queda el enlace MPLS (amarillo), que presenta una latencia muy alta inicialmente. Sin embargo, en pocos segundos se va normalizando a un valor aproximado de *60.87 ms.*

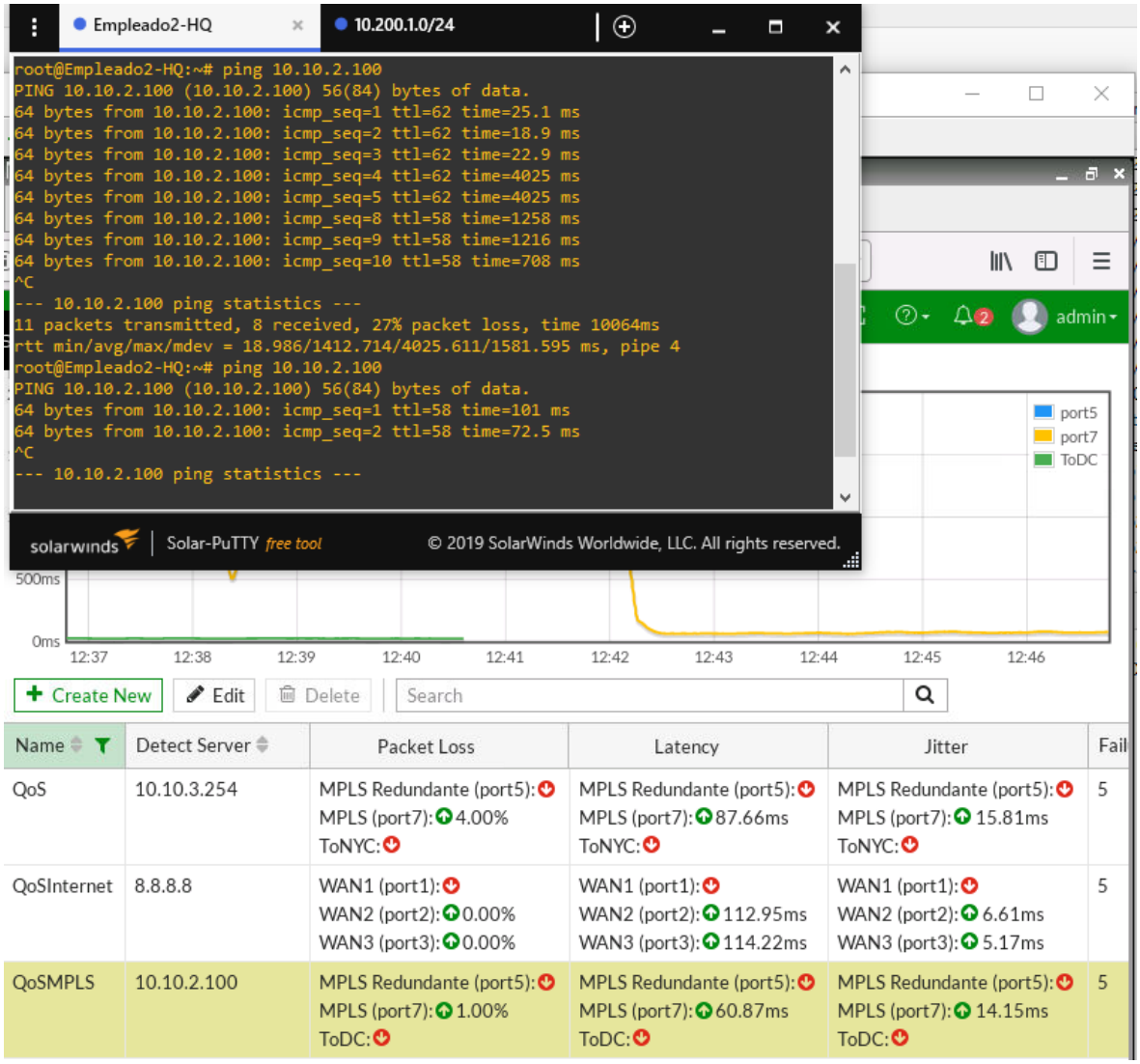


Figura 3.14. Selección automática de ruta por menor latencia

3.1.6 BALANCEO DE CARGA

En esta sección se verifica el balanceo de carga que realiza la SD-WAN cuando detecta que existen sesiones de varios usuarios hacia Internet. El balanceo de carga está habilitado solamente en las conexiones de banda ancha de la sede principal y la sucursal, con el fin de distribuir de manera equitativa el tráfico a Internet.

La sede principal cuenta con 3 enlaces de banda ancha, de tal manera que se realiza un *ping* a Internet y se navega en cualquier página web desde 3 usuarios distintos, con el fin de comprobar que el tráfico se distribuye por cada uno de los enlaces. En la Figura 3.15. se visualizan las sesiones de diferentes usuarios con su interfaz de salida, de tal manera que se verifica la utilización de los enlaces *"WAN1", "WAN2"* y *"WAN3"* simultáneamente para el acceso a Youtube, Wikipedia y Google.

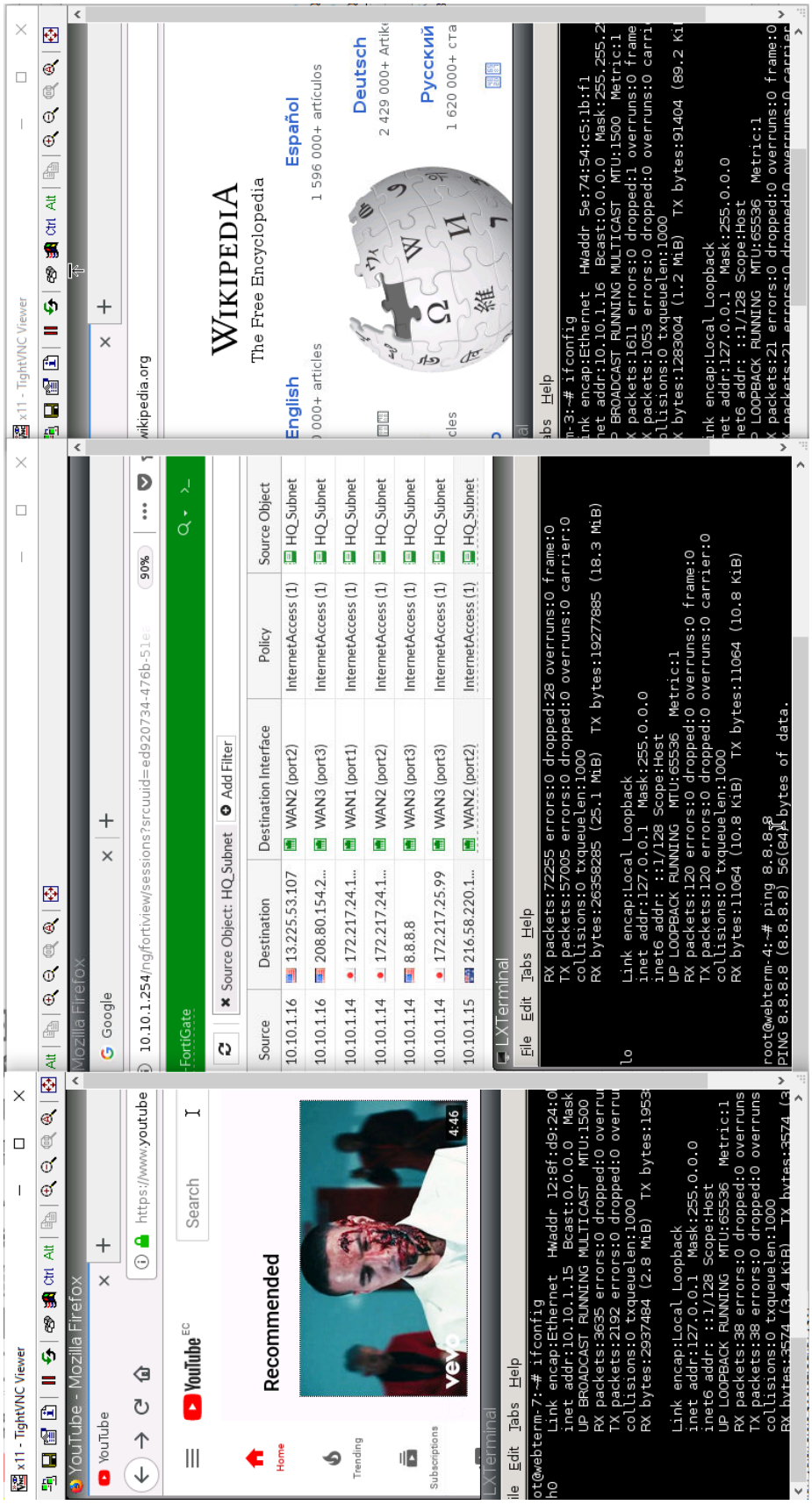


Figura 3.15. Balanceo de Carga en la Sede Principal

Al igual que en la sede principal, la sucursal también realiza balanceo de carga. En este caso, solo se usan dos enlaces para distribuir el tráfico, por lo tanto, se realiza un *ping* desde dos usuarios de la sucursal con direcciones IP diferentes. En la Figura 3.16. se visualiza el balanceo de carga por parte de dos usuarios de la sucursal.

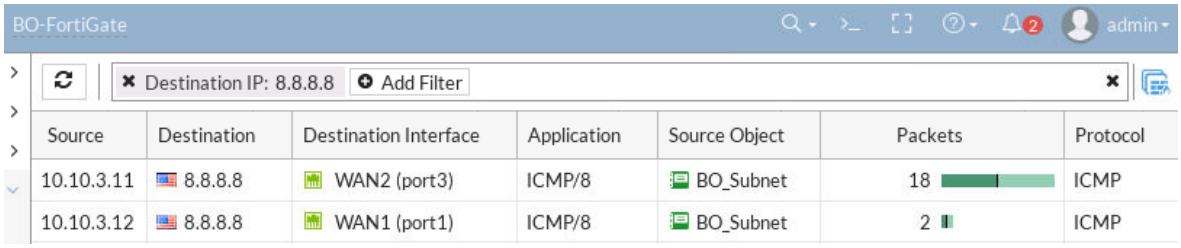


Figura 3.16. Balanceo de Carga en la sucursal

3.1.7 TRAFFIC SHAPING

El *Traffic Shaping* se encarga de controlar el uso del ancho de banda basado en las aplicaciones; es decir la SD-WAN tendrá mayor visibilidad o identificará de manera inteligente las aplicaciones y distribuirá el ancho de banda de acuerdo con las necesidades de la empresa.

En este caso se da mayor prioridad a un grupo de aplicaciones de teletrabajo que necesitan mayor ancho de banda. En el grupo llamado teletrabajo están aplicaciones como Zoom, Webex, Skype y Telegram, de tal manera que el momento que cualquier usuario necesite hacer una videoconferencia a través de estas aplicaciones tendrá prioridad en la distribución de ancho de banda. En la Figura 3.17. se visualiza la política de *Traffic Shaping.*

Figura 3.17. Política de *Traffic Shaping* para Teletrabajo

Para la comprobación, se verifica el ancho de banda de dos usuarios de la sede principal antes de aplicar la política. Se debe tomar en cuenta que en el entorno de emulación la velocidad es baja, ya que los dispositivos están corriendo dentro del programa GNS3 e inclusive la máquina virtual de GNS3 está a su vez dentro de VMware. Por lo tanto, el momento que ambos usuarios están viendo un video en Youtube y están usando un único enlace de acceso a Internet, el ancho de banda de cada uno es similar como se muestra en la Figura 3.18.

Source	Bytes	Sessions	Bandwidth	Packets
10.10.1.14	36.31 MB	38	1.49 Mbps	50,127
10.10.1.17	32.54 MB	72	1.32 Mbps	65,034

Figura 3.18. Ancho de Banda antes de aplicar la política

A continuación, se aplica la política de *Traffic Shaping* correspondiente al grupo de aplicaciones de teletrabajo. En este caso, uno de los usuarios empieza a usar la aplicación de Skype y el otro usuario se mantiene en un video en Youtube. En la Figura 3.19. se visualiza que el usuario de la IP 10.10.1.17 está en Skype. Por lo tanto, el uso de ancho de banda debe ser mayor para este usuario debido a que es una aplicación del grupo de teletrabajo, como se muestra en la Figura 3.20.

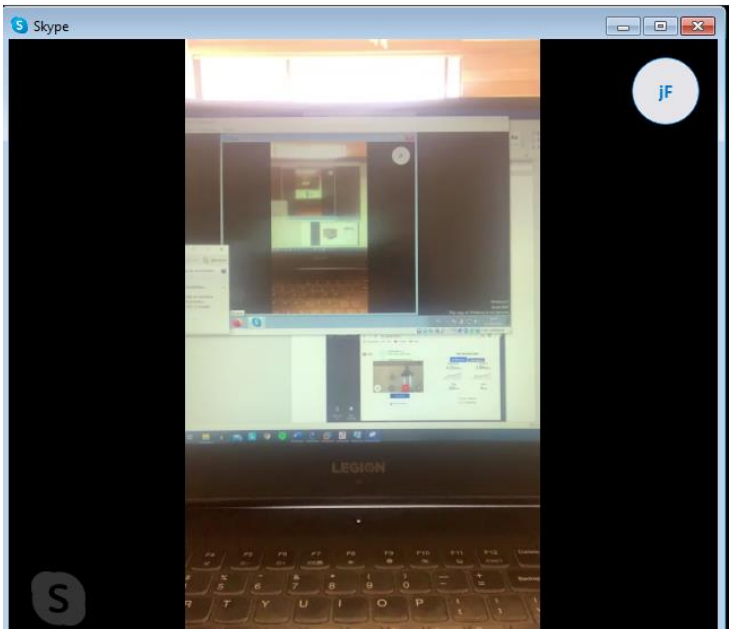


Figura 3.19. Usuario 10.10.1.17 en Skype

Source	Bytes	Sessions	Bandwidth	Packets
10.10.1.14	15.61 MB	88	2.28 kbps	21,237
10.10.1.17	10.19 MB	40	99.79 kbps	26,646

Figura 3.20. Ancho de Banda con la política *Traffic Shaping*

Además, se pueden aplicar políticas de *Traffic Shaping* basado en las direcciones IP de los usuarios y no en las aplicaciones. En este caso, como ejemplo se crea una política en la que el Gerente tendrá mayor ancho de banda y los empleados una cantidad menor; inclusive se pueden crear perfiles jerárquicos para gerentes, técnicos y empleados. En la Figura 3.21. se visualiza una prueba de velocidad antes de aplicar la política.

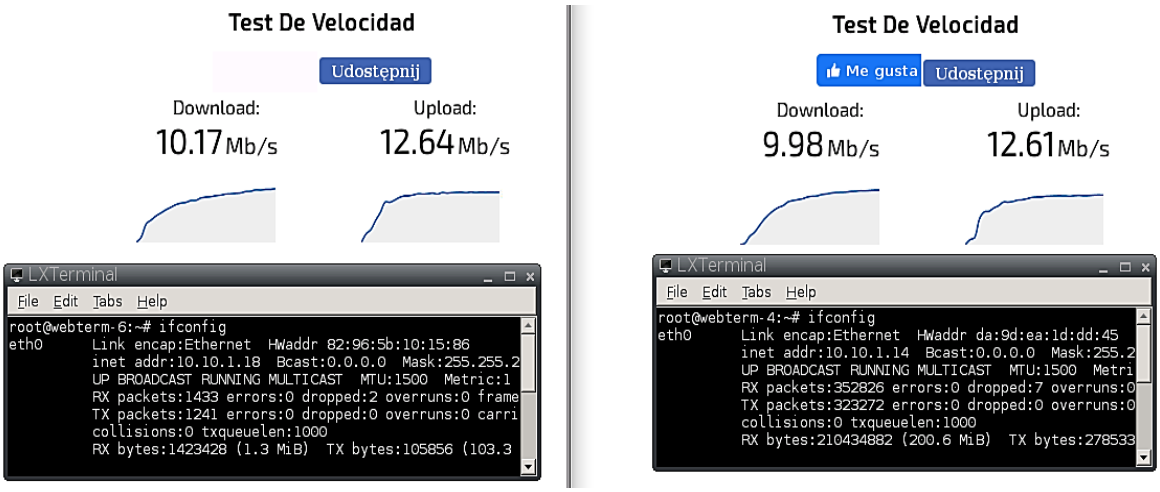


Figura 3.21. Velocidad del gerente y empleado sin la política

Una vez aplicada la política que define un ancho de banda máximo de 3 Mb/s a los empleados, se visualiza en la Figura 3.22. la velocidad de *download* del Gerente de 8.50 Mb/s y la del empleado de 1.85 Mb/s.

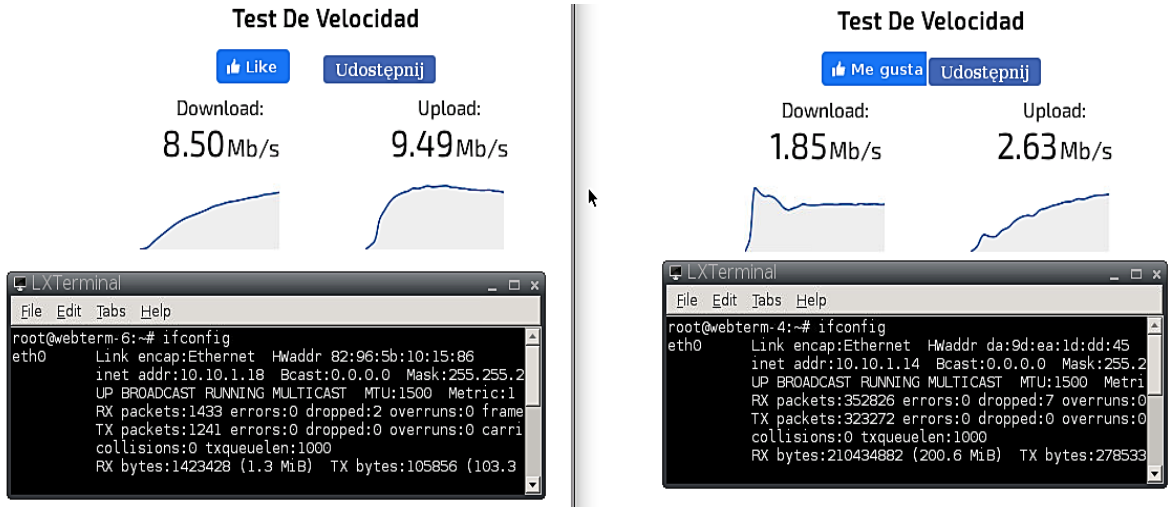


Figura 3.22. Velocidad del Gerente y empleado con la política

Finalmente, esta política de distribución de tráfico en base a la dirección IP fue explicada a manera de ejemplo, por lo tanto, es eliminada de la emulación.

3.1.8 SEGURIDAD NGFW E INSPECCIÓN SSL

En esta sección se comprueban todos los medios de seguridad que presenta la SD-WAN de FORTINET en un único dispositivo. Se verificará que la red cuente con NGFW e Inspección SSL y luego se detallará cada perfil de seguridad. Es importante mencionar que para una seguridad completa es necesario tener la licencia de FortiGuard.

En primer lugar, se comprueba que la SD-WAN tenga la funcionalidad de NGFW que permite realizar la inspección del tráfico y crear los perfiles de seguridad. En la Figura 3.23. se puede visualizar que la SD-WAN tiene activada esta función, la cual está basada en perfiles. Estos perfiles corresponden a antivirus, control de aplicaciones, IPS, etc. que se explican posteriormente.

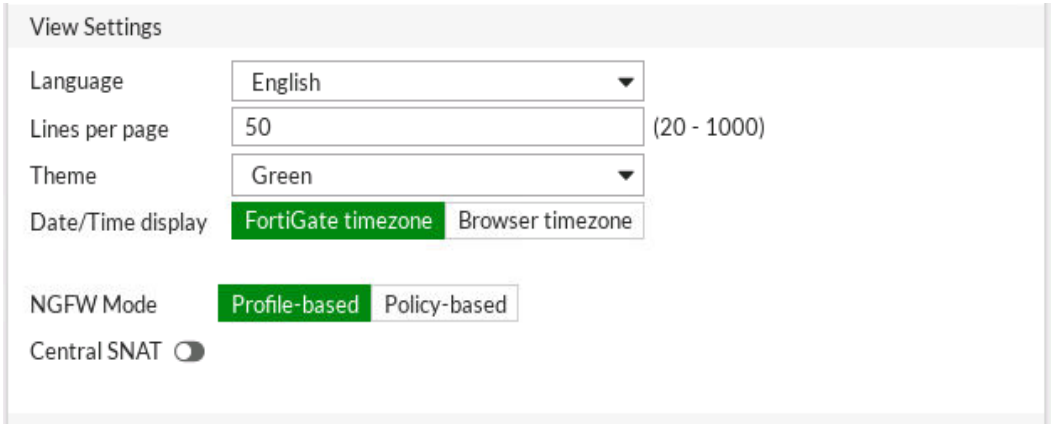


Figura 3.23. NGFW habilitado

En segundo lugar, se verifica que la SD-WAN tenga activada la funcionalidad de inspección SSL; en este caso debe ser el modo de inspección completo (*deep-inspection*) que permite agregar los perfiles de seguridad. En la Figura 3.24. se visualiza que todos los dispositivos tienen activada esta característica en la política de acceso a Internet.

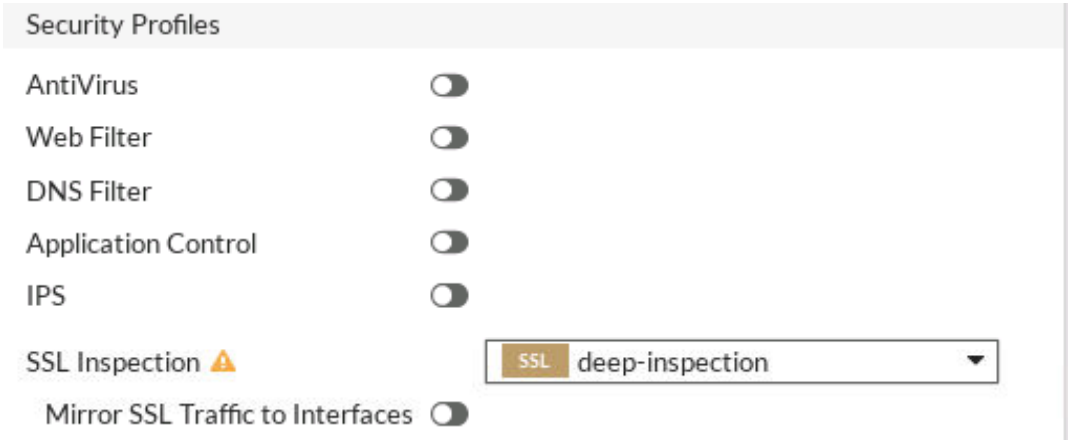


Figura 3.24. Inspección SSL profunda activada

3.1.8.1 Antivirus

La SD-WAN cuenta con un antivirus encargado de bloquear el acceso o descargas cuando detecta virus proveniente de Internet o páginas web; sin embargo, esto no quiere decir que las computadoras internas no necesitan un antivirus ya que pueden infectarse localmente a través de un periférico USB por ejemplo. Por lo tanto, el antivirus de SD-WAN se complementa con el antivirus local.

Para la comprobación de que el antivirus de la red esté funcionando correctamente, se accede a una página web que contiene archivos maliciosos o infectados con virus; por lo tanto, la SD-WAN debe bloquear la descarga de esos archivos y mostrar una advertencia. En este caso, se deshabilitó el antivirus del computador antes de acceder a la página web eicar.org. En la Figura 3.25. se visualiza la página web de eicar.

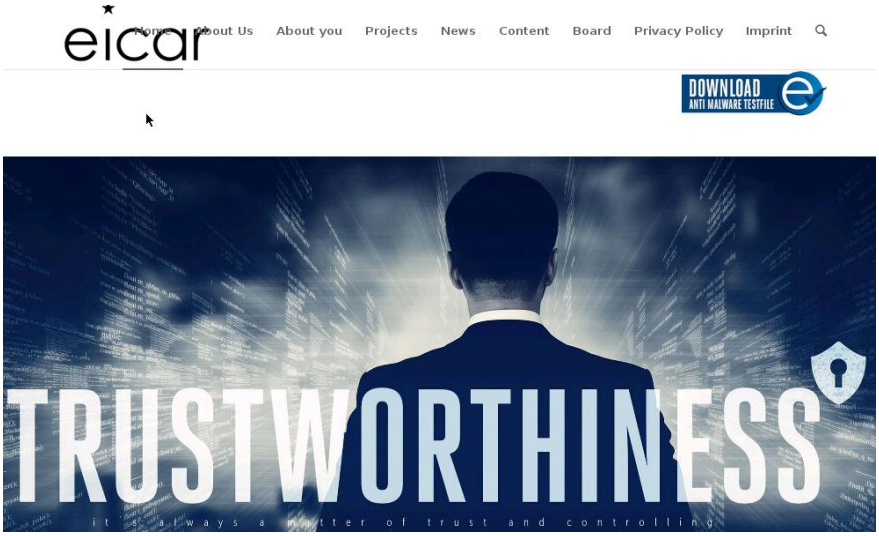


Figura 3.25. Prueba eicar de virus en Internet [33]

Antes de la descarga del archivo, en la Figura 3.26. se visualiza que la política de acceso a Internet está configurada con el perfil de antivirus por defecto.

#	Name	From	To	NAT	Source	Destination	Security Profiles
1	To_DC	LAN	sd-wan	Disabled	HQ_Subnet	DC_Subnet BO_Subnet	no-inspection
2	From_DC	sd-wan	LAN	Disabled	DC_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	HQ_Subnet	no-inspection
3	InternetAccess	LAN sd-wan	sd-wan	Enabled	HQ_Subnet DC_Subnet MPLS Network MPLS Redundancy	all	default Seguridad_Aplicaciones_ no-inspection default

Figura 3.26. Política de Internet con Antivirus habilitado

Finalmente, se procede a la descarga del archivo de eicar y se visualiza en la Figura 3.27. una advertencia indicando que el archivo está infectado con virus, de tal forma que la SD-WAN no permite que éste sea descargado.

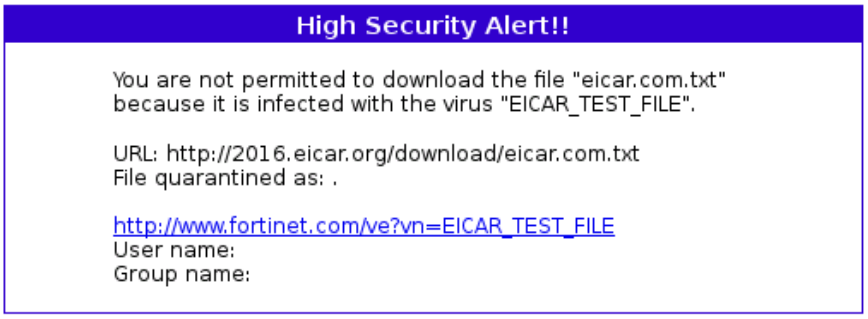


Figura 3.27. Advertencia y bloqueo de archivos infectados con virus

3.1.8.2 Control de aplicaciones

En esta sección se comprueba que el control de aplicaciones de la SD-WAN funcione correctamente basado en la sección 2.2.6. Se evalúan 2 escenarios, el primero respecto al control de aplicaciones por categoría y el segundo por aplicación específica. Además, existe un filtro para aplicaciones de juegos en el navegador.

En la Figura 3.28. se visualiza la política de acceso a Internet con el perfil de antivirus y el perfil de control de aplicaciones llamado *"Seguridad_Aplicaciones_HQ"*.

#	Name	From	To	NAT	Source	Destination	Security Profiles
1	To_DC	LAN	sd-wan	Disabled	HQ_Subnet	DC_Subnet BO_Subnet	no-inspection
2	From_DC	sd-wan	LAN	Disabled	DC_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	HQ_Subnet	no-inspection
3	InternetAccess	LAN sd-wan	sd-wan	Enabled	HQ_Subnet DC_Subnet MPLS Network MPLS Redundancy	all	default Seguridad_Aplicaciones_ no-inspection default

Figura 3.28. Política de Internet con control de aplicaciones

En el primer escenario se verifica que la SD-WAN no permita la conexión a ninguna aplicación de acceso remoto, en este caso se toma como ejemplo la aplicación TeamViewer. En la Figura 3.29. se visualiza una advertencia indicando que la aplicación TeamViewer no puede establecer conexión, a pesar de haber conexión a Internet (Youtube).

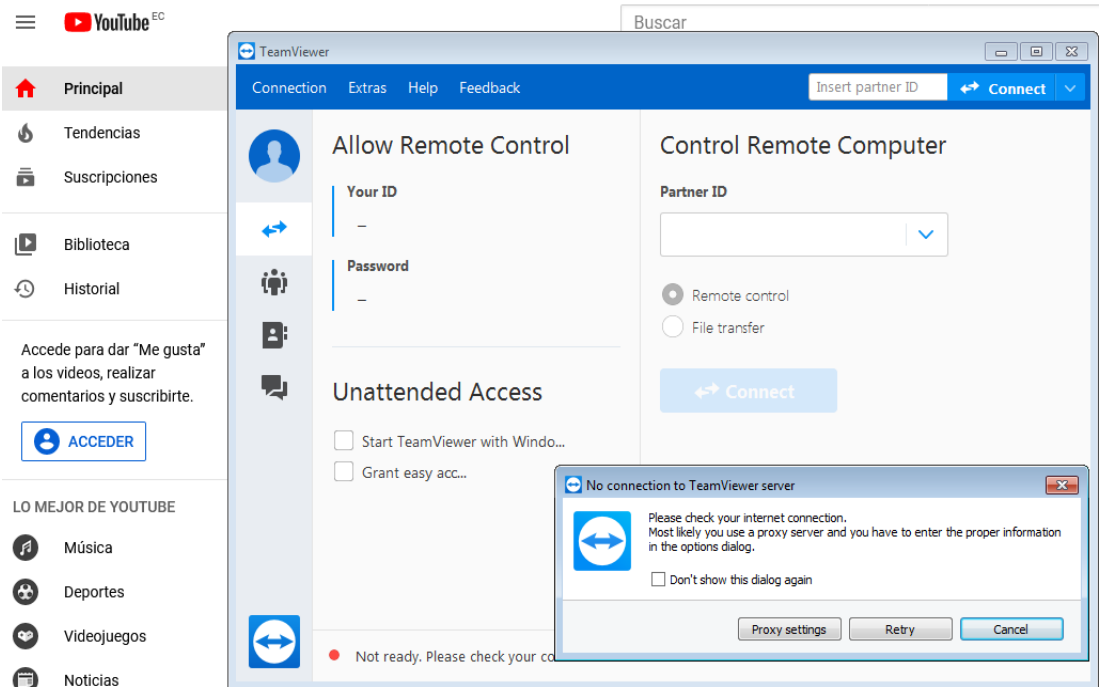


Figura 3.29. Control sobre aplicaciones de Acceso Remoto

En el segundo escenario se comprueba el control de aplicaciones no por categorías, sino para una aplicación en especial. En este caso se niega el acceso específicamente a la aplicación de Spotify. En la Figura 3.30. se visualiza que existe Internet a través de cualquier navegador, sin embargo, Spotify muestra un mensaje indicando que ha perdido la conexión a Internet.

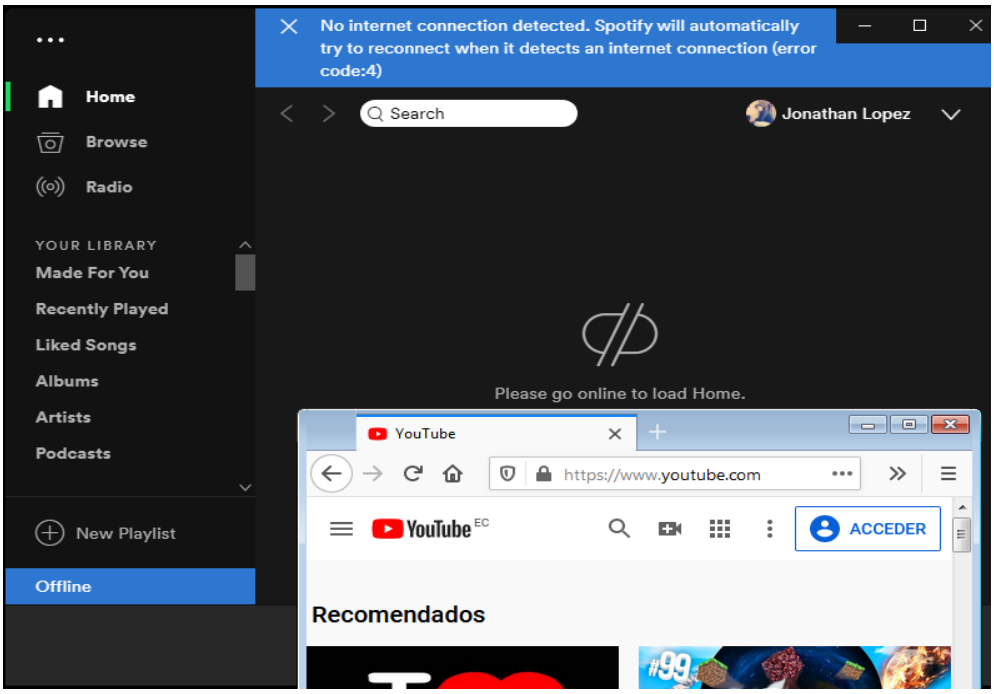


Figura 3.30. Acceso denegado a la aplicación Spotify

3.1.8.3 Sistema de Prevención de Intrusos (IPS)

El IPS está configurado para proteger a los usuarios de las conexiones hacia sitios Botnet y bloquear las URLs maliciosas. En este caso, no se puede comprobar debido a que no se conoce de un sitio en especial o a su vez una URL que exponga a la red. Sin embargo, posteriormente en la sección de análisis de seguridad se puede visualizar un mapa geográfico de los países donde prevalecen los sitios Botnet. Lo importante es conocer que la red tiene habilitado el perfil contra este tipo de ataques y en cualquier momento que uno de los usuarios intente acceder a estos sitios sin saberlo, inmediatamente bloqueará la conexión. En la Figura 3.31. se visualiza la política de Internet con el perfil de ISP llamado *"Protección Workstations".*

#	Name	From	To	NAT	Source	Destination	Security Profiles
1	To_DC	LAN	sd-wan	Disabled	HQ_Subnet	DC_Subnet BO_Subnet	no-inspection
2	From_DC	sd-wan	LAN	Disabled	DC_Subnet MPLS Redundancy VPN BO_Subnet MPLS Network	HQ_Subnet	no-inspection
3	InternetAccess	LAN sd-wan	sd-wan	Enabled	HQ_Subnet DC_Subnet MPLS Network MPLS Redundancy	all	default Seguridad_Aplicaciones_I Proteccion Workstations no-inspection default

Figura 3.31. Política de Internet con IPS

3.1.8.3.1 Política de Denegación de Servicios (DoS)

La política de *DoS* se encarga de proteger a la red de ataques que consumen todos los recursos de RAM, CPU, número de puertos, etc. Actualmente, existen muchos ataques por parte de los piratas informáticos para inundar la red de sesiones falsas, de tal manera que cuando exista una sesión legítima, el servidor o la red no tenga disponibilidad de recursos para aceptarla.

Para la comprobación, se espera una inundación de paquetes por un *hacker*, de tal forma que se saturen los recursos de la red. Es impredecible conocer el momento en que el ataque ocurrirá, de todas formas, es importante mencionar que la red tiene activado este tipo de seguridad en caso de que llegara a pasar. Los umbrales se establecen principalmente en los paquetes TCP, UDP e ICMP, con el fin de detectar las inundaciones más frecuentes desde un mismo usuario (*Hacker*) e inmediatamente bloquearlas. En la Figura 3.32. se visualiza la política de DoS.

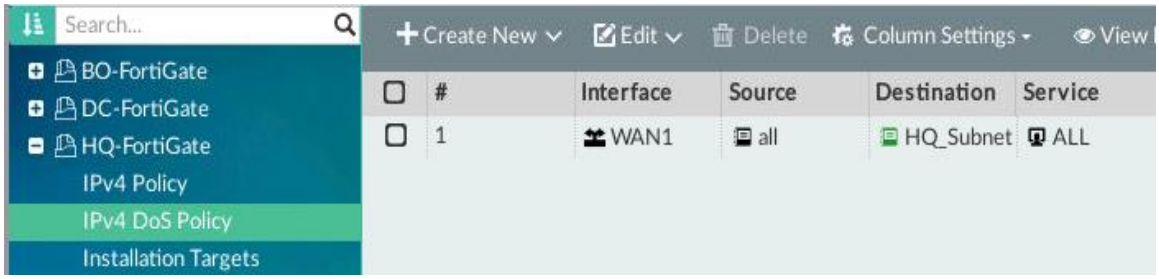


Figura 3.32. Política de DoS habilitada

Enhorabuena en la emulación ocurrió un ataque de DOS, es así como en la Figura 3.33. se puede visualizar la detección de una inundación de paquetes UDP desde la dirección IP 172.217.161.67 con una severidad de riesgo crítico, de tal forma que la SD-WAN inmediatamente se encarga de bloquear o aniquilar la sesión, basada en los umbrales de la política de DoS.

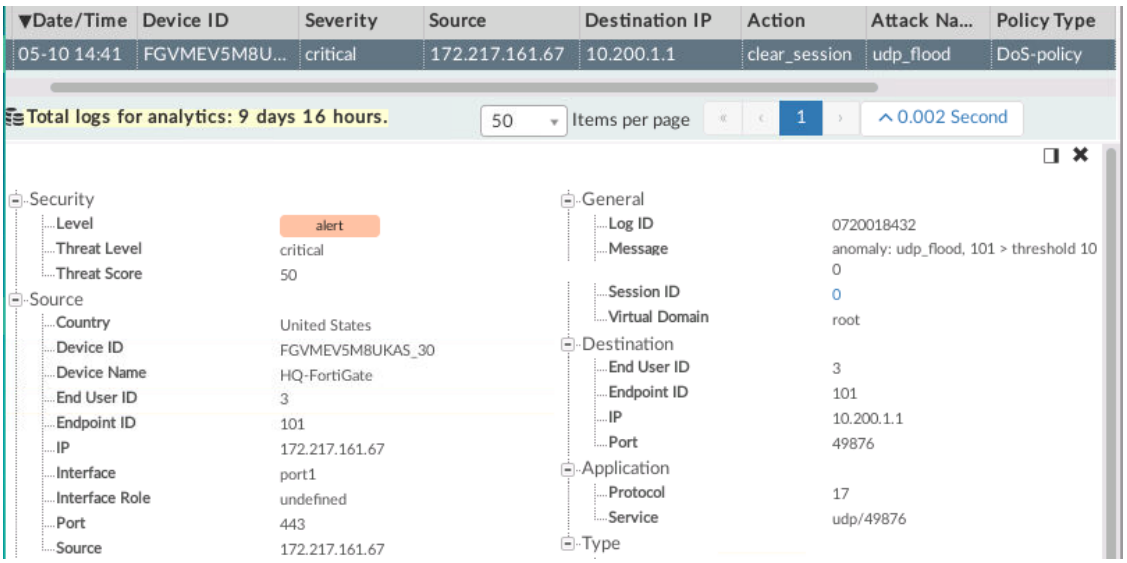


Figura 3.33. Detección y bloqueo de ataques de DoS

3.1.9 FORTIMANAGER: CONTROL CENTRALIZADO

En esta sección se muestra toda la red controlada desde un único panel y un ejemplo del aprovisionamiento de toque cero (ZTP). Con el fin de optimizar recursos de RAM y CPU, se verifica que solo este dispositivo sea el punto de control a través de las características de FortiManager y el centro de análisis a través de las características de FortiAnalyzer.

3.1.9.1 Punto de control de la red

En la Figura 3.34. se visualizan todos los dispositivos que están siendo administrados por FortiManager; de esta manera se pueden crear políticas, reglas, túneles, realizar cambios o actualizaciones, entre otros aspectos. Además, la pestaña de *"Logging Devices"* incluye

a los dispositivos sincronizados con FortiAnalyzer, de tal manera que para ambos casos se visualizan 3 dispositivos.

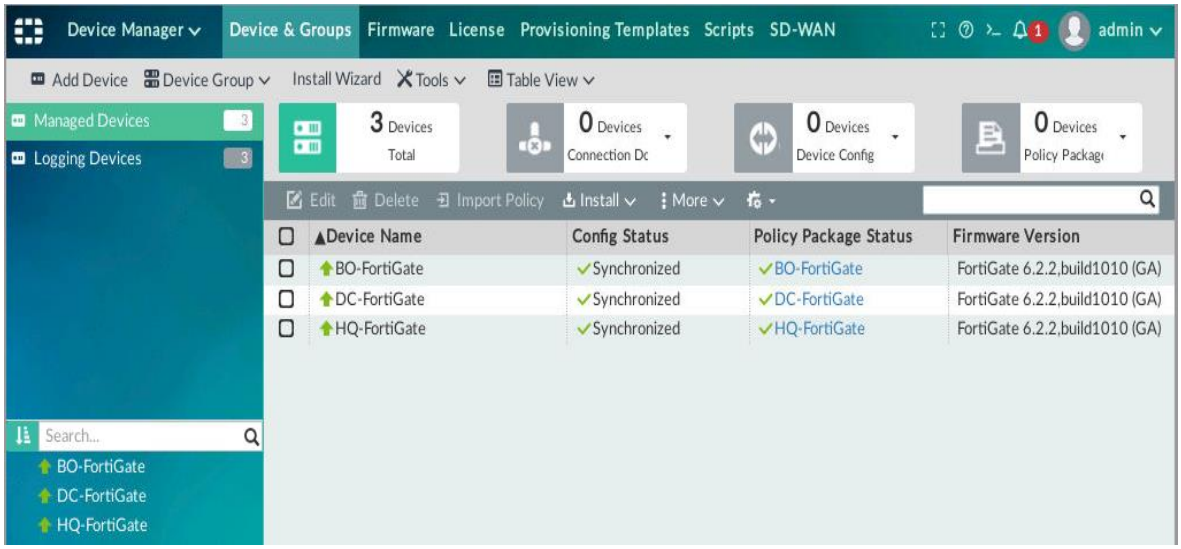


Figura 3.34. FortiManager como centro de control y administración

Es importante mencionar que en la SD-WAN está la red MPLS, sin embargo, no se pueden realizar cambios internamente en sus enrutadores a través del Centro de Control. De todas formas, la SD-WAN es una red inteligente que toma de decisiones basada en todos los miembros de la SD-WAN (incluyendo MPLS), como se visualiza en la Figura 3.35.

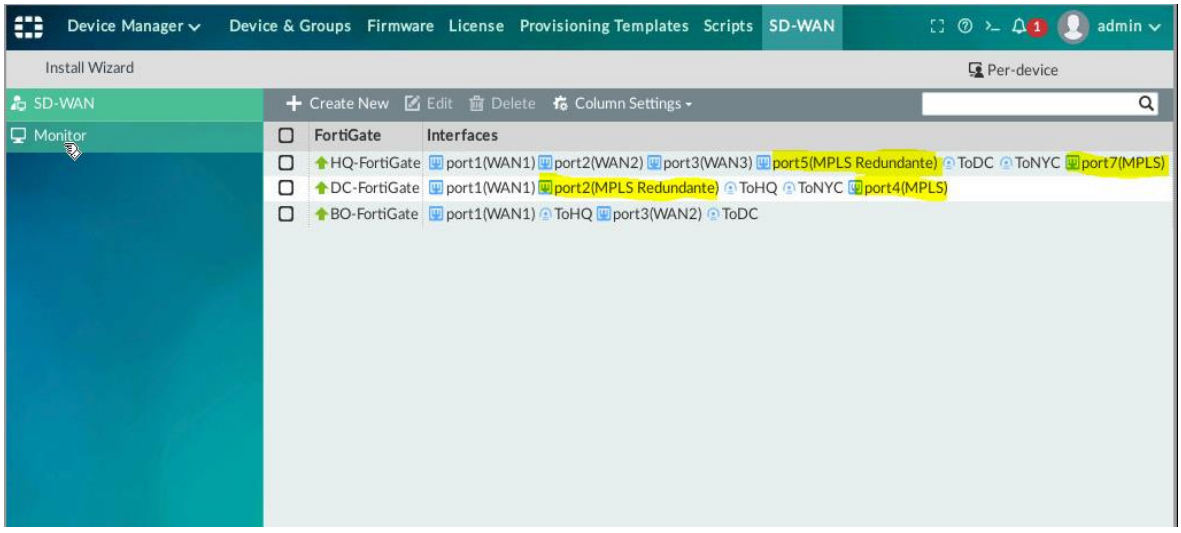


Figura 3.35. SD-WAN controlada por FortiManager

En la Figura 3.36. se visualiza el conjunto de políticas de la sede principal, de tal manera que desde FortiManager se puede crear, eliminar o actualizar cualquier política, al igual que las políticas del Centro de Datos y de la sucursal. El Centro de Control cuenta con una sola base de datos para las políticas, con el fin de que si son políticas o reglas similares se

despliegen una sola vez y no en cada dispositivo. Solamente la configuración de sistema se realiza por separado ya que cada dispositivo cuenta con una base de datos independiente para este aspecto.

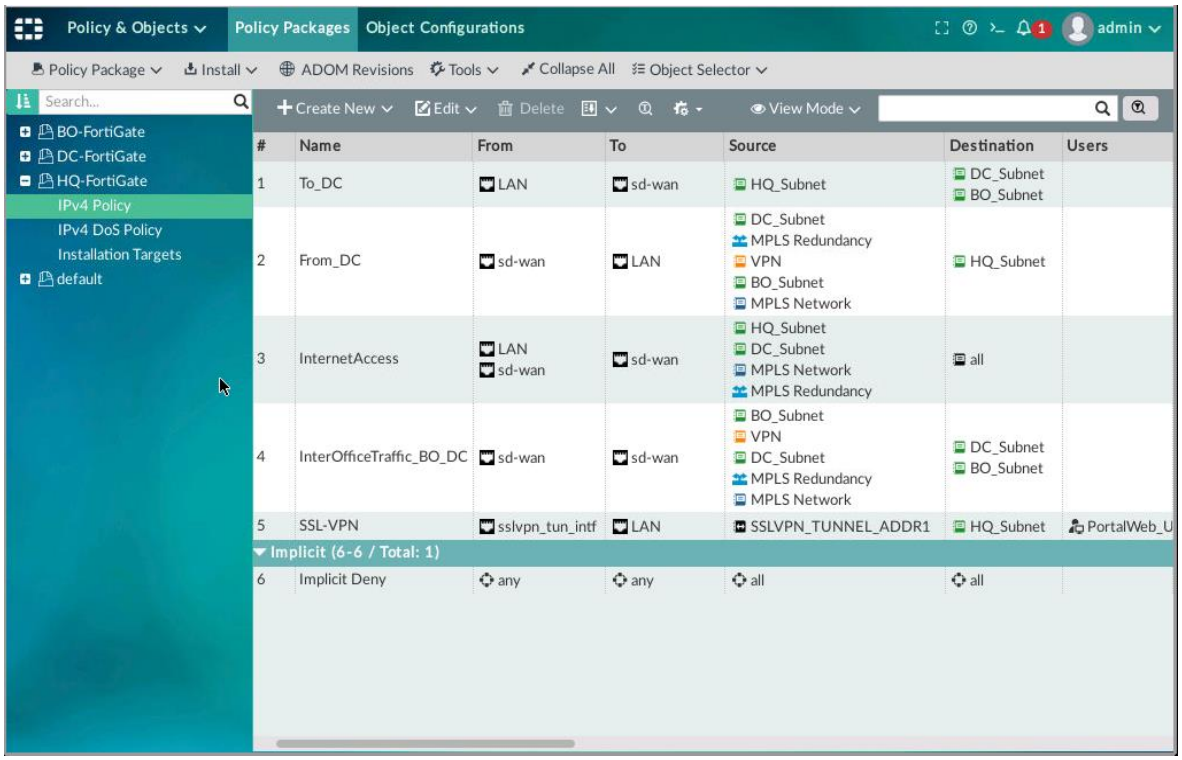


Figura 3.36. Políticas administradas desde el Centro de Control

3.1.9.2 Zero-Touch Provisioning (ZTP)

El aprovisionamiento de toque cero, conocido como ZTP se encarga de facilitar la implementación y configuración de dispositivos en nuevas oficinas remotas. Es importante mencionar dos características puntuales del ZTP; una de ellas es que no necesita de un administrador de red en el sitio; y, la segunda que no requiere que se configure individualmente cada dispositivo que se desea añadir, sino que puede descargarse o asociarse a la configuración de los dispositivos que ya están administrados por FortiManager. Por lo tanto, ZTP facilita la escalabilidad, reduce tiempos de implementación y minimiza costos.

Tomando en cuenta que los recursos de RAM como de CPU están funcionando en el máximo de sus capacidades, se despliega como ejemplo una nueva sucursal en Cuenca a través de FortiManager, en la cual se asocia la configuración de la política *"InternetAccess"*. En la Figura 3.37. se visualiza cómo el dispositivo está siendo agregado a FortiManager.

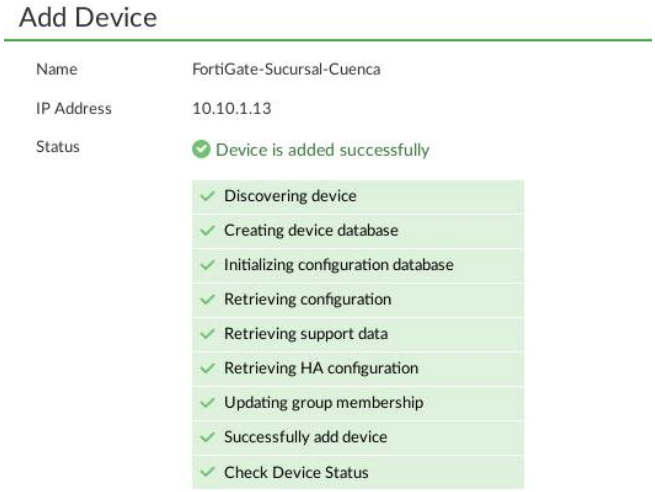


Figura 3.37. FortiGate-Cuenca añadido en FortiManager

En la Figura 3.38. se visualizan todos los dispositivos de la red, incluido el nuevo dispositivo de la sucursal en Cuenca, que ya está sincronizado para controlarlo desde FortiManager.

Figura 3.38. Dispositivos administrados por FortiManager

En la Figura 3.39. se visualizan todas las interfaces correspondientes al funcionamiento de la *"WAN1",* de tal forma que simplemente se agrega la interfaz del dispositivo de la sucursal en Cuenca para que se asocie a la configuración de los dispositivos existentes.

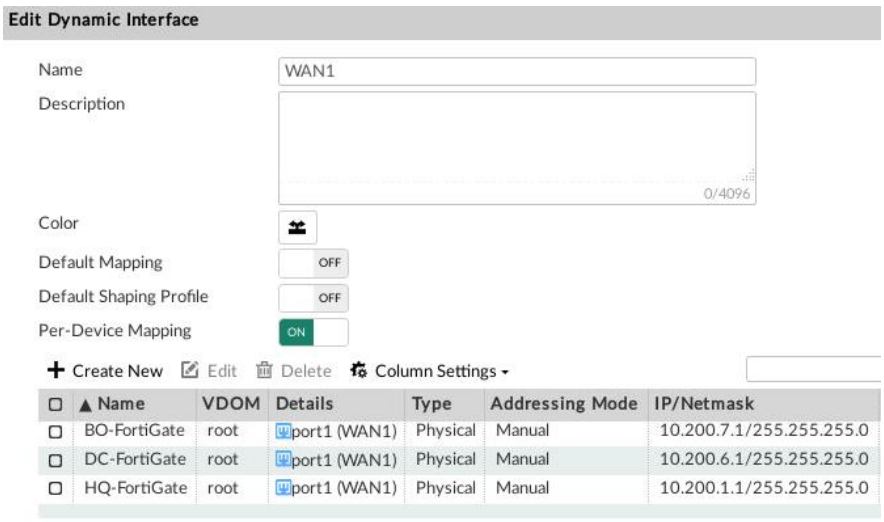


Figura 3.39. Configuración automática del nuevo dispositivo

En la Figura 3.40. se visualiza la política creada en la Sucursal correspondiente al acceso a Internet e idéntica a la de los dispositivos anteriores. Por lo tanto, el dispositivo debe ser enviado al sitio en Cuenca o a su vez descargado de la nube y simplemente conectarse a Internet. Finalmente, esta demostración del funcionamiento de ZTP debe ser eliminada de la emulación en vista de que ocasiona problemas en la PC, por el uso excesivo de RAM y CPU. En un ambiente de implementación física, el proceso a seguir será el mismo.

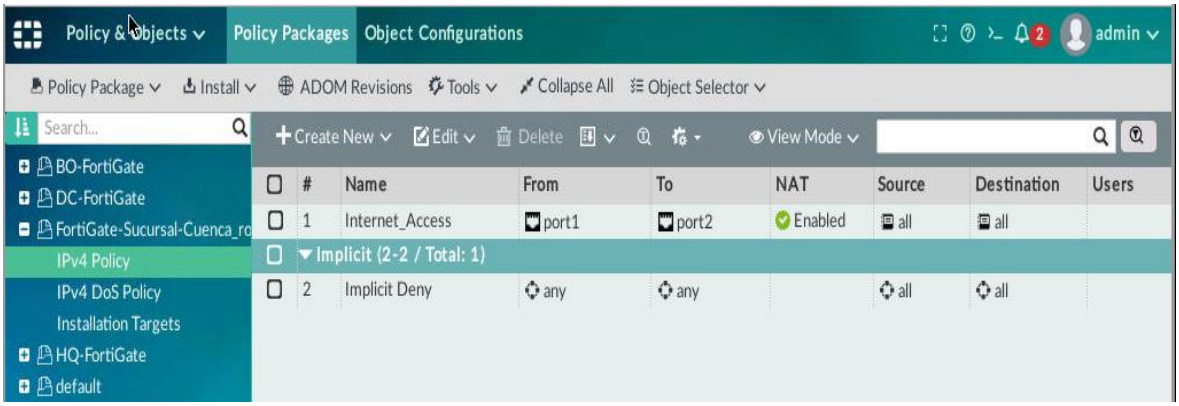


Figura 3.40. Política de Internet de la Sucursal en Cuenca

En la Figura 3.41. se comprueba únicamente que las características de FortiAnalyzer estén habilitadas en FortiManager como: reportes, incidentes, monitoreo y SOC. En la sección siguiente, se discute a detalle cada una de las funcionalidades de FortiAnalyzer.

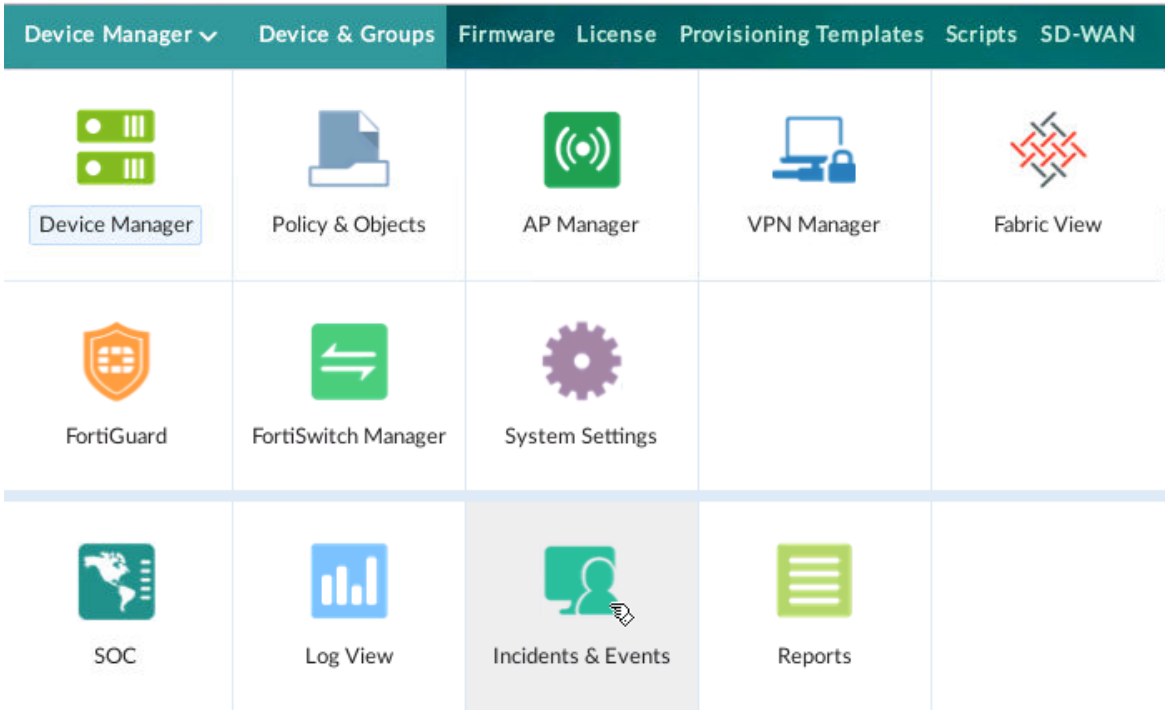


Figura 3.41. Características de FortiAnalyzer en FortiManager

3.1.10 FORTIANALYZER: ANÁLISIS Y REPORTES

En esta sección se verifican las funcionalidades de FortiAnalyzer dentro de FortiManager, principalmente el análisis de tráfico, seguridad y emisión de reportes. Esta herramienta es importante ya que permite al administrador conocer el estado de la red en tiempo real.

3.1.10.1 Análisis del tráfico

En la Figura 3.42. se visualiza el tráfico con el número de sesiones, interfaz, gráficas, entre otros datos, tomando en cuenta el origen de éste. Además, se puede ver que existen opciones para analizar el tráfico basado en el destino, país, políticas, DNS, etc.

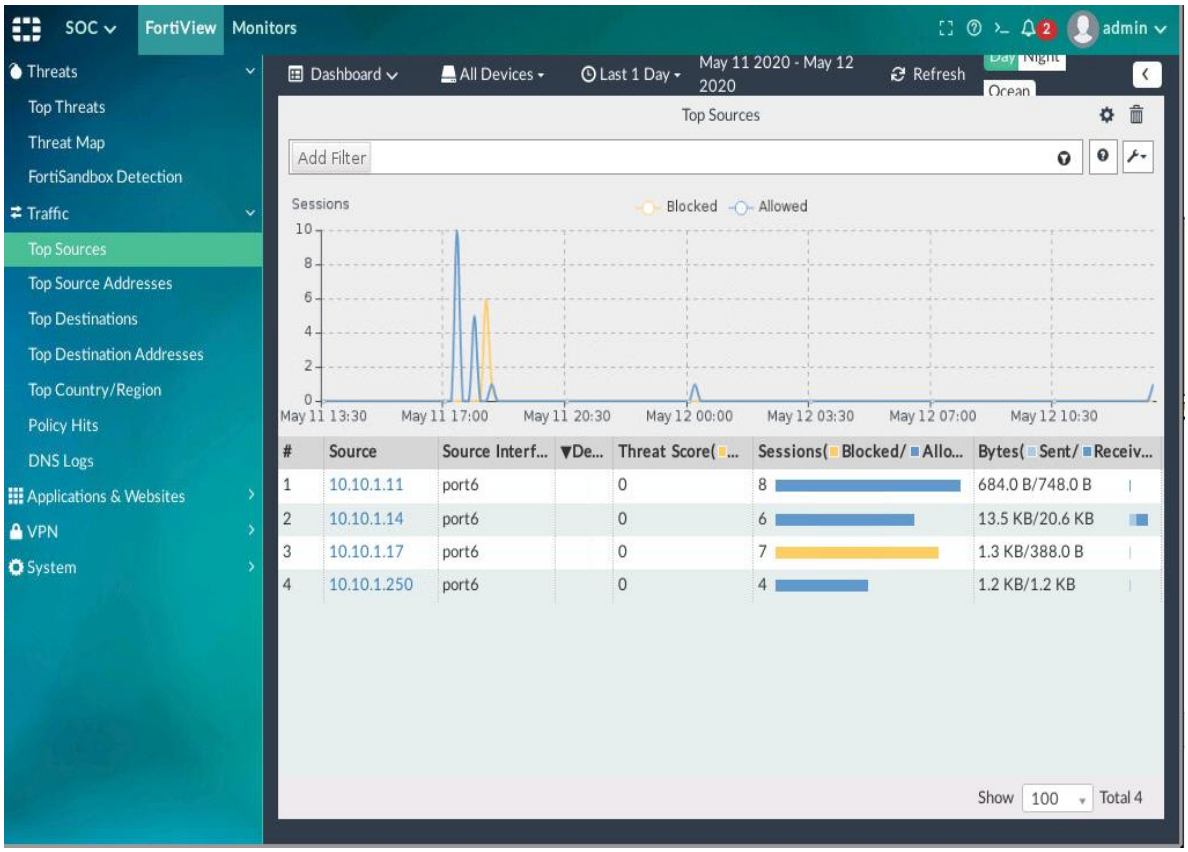


Figura 3.42. Análisis en base al tráfico

En la Figura 3.43. se muestra un análisis en base a las aplicaciones y a sitios web. De la misma manera están los datos con sus respectivas gráficas; en este caso se puede visualizar la aplicación Spotify con su categoría, nivel de riesgo, bytes etc. Esto permite al administrador conocer el número de clientes que desean acceder a una determinada aplicación y en función de estos datos bloquearlas o permitirlas bajo conocimiento del gerente de la empresa.

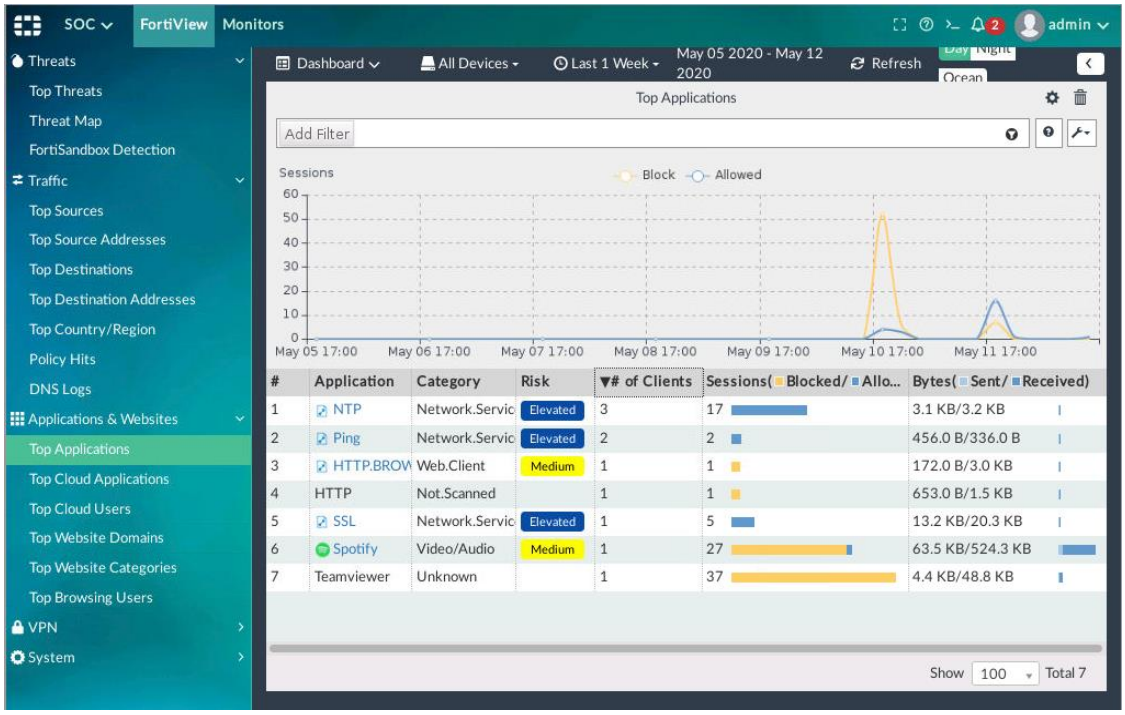


Figura 3.43. Análisis en base a aplicaciones

Además, se puede realizar un análisis más exhaustivo de cada una de las aplicaciones como se puede ver en la Figura 3.44., que despliega los datos y gráficas solo de esa aplicación y no de manera general como en la figura anterior.

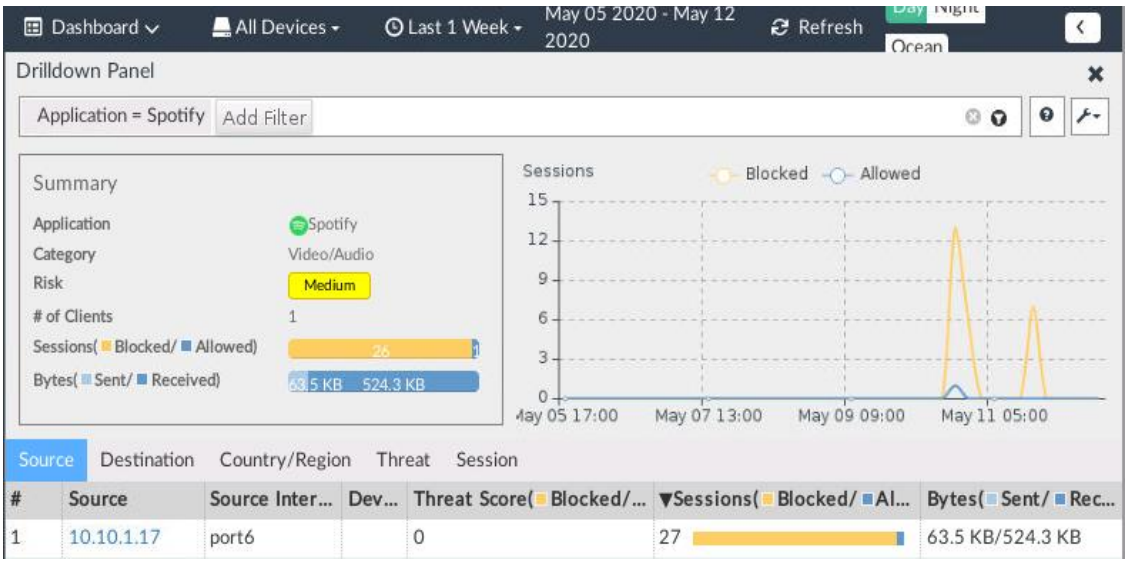


Figura 3.44. Análisis exhaustivo de una aplicación específica

En la Figura 3.45. se visualiza un análisis de las redes privadas virtuales ya sea de tipo IPsec o SSL. En este caso, se muestran todos los túneles IPsec y sus datos como: FortiGate de origen y destino, tiempo de duración del túnel y los bytes enviados y recibidos.

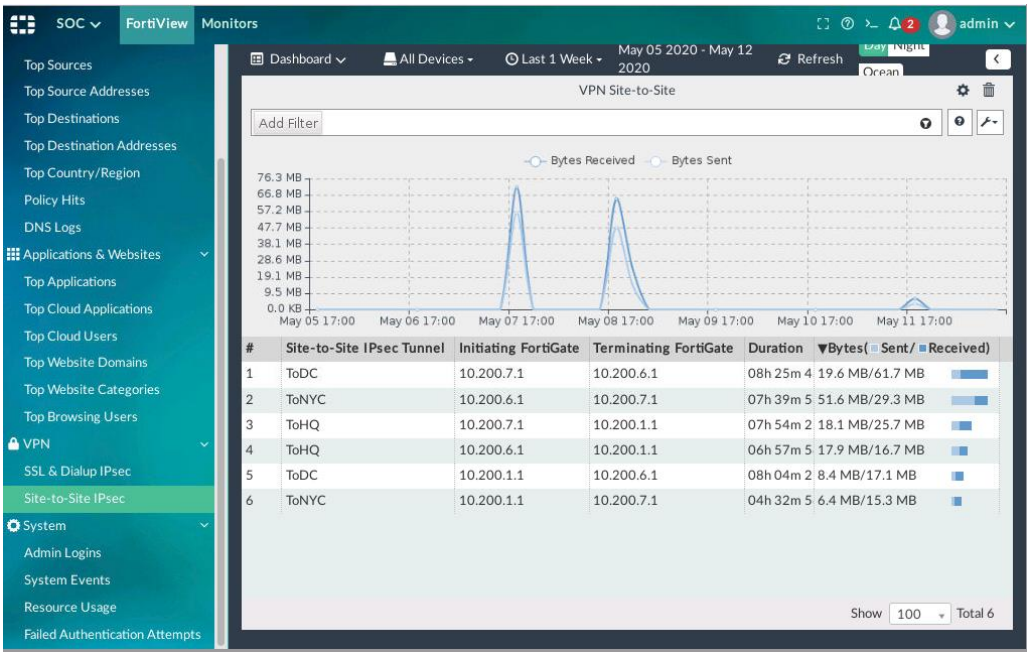


Figura 3.45. Análisis de túneles IPsec

En la Figura 3.46. se visualizan los datos correspondientes a la SSL-VPN creada para el acceso remoto. Se muestran datos como IP de origen, fecha de su última conexión, usuario, tipo de VPN y gráficas de los bytes enviados y recibidos.

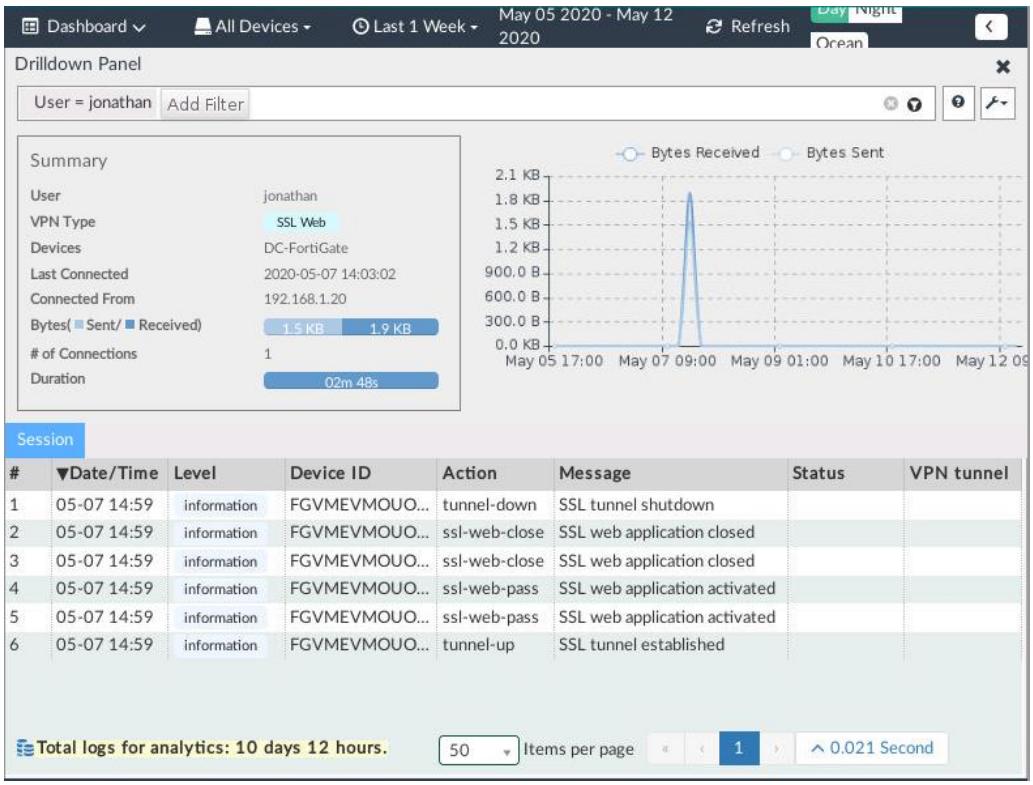
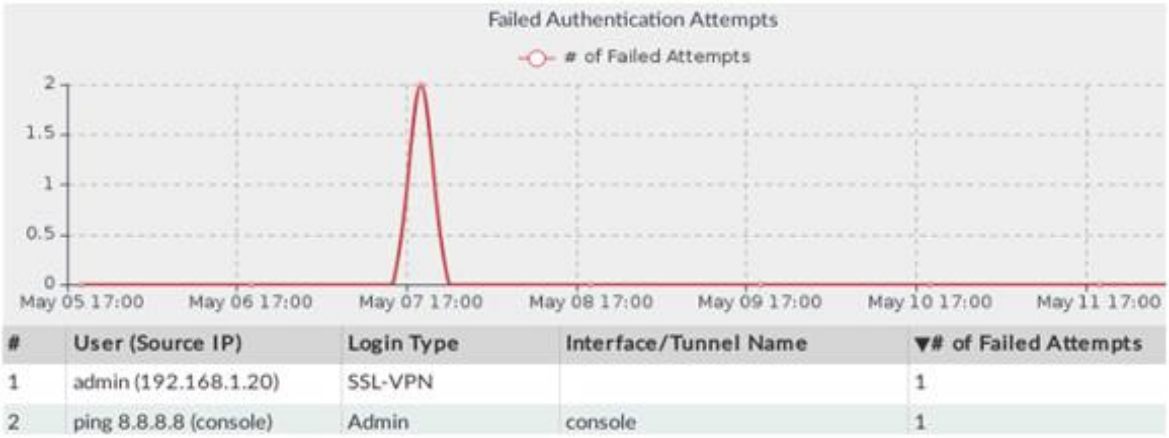


Figura 3.46. Análisis de la SSL-VPN

Posteriormente, está la sección de análisis del sistema que permite visualizar aspectos tales como: ingreso de administradores, eventos del sistema, uso de los recursos e intentos de autenticación fallidos. En este caso, para su comprobación se intentó ingresar al portal web y a la administración por consola de un FortiGate introduciendo un usuario incorrecto; su resultado se muestra en la Figura 3.47. Adicionalmente, en la Figura 3.48. se visualiza el uso de los recursos ya sea en datos o gráficas, específicamente de la memoria RAM.



#	User (Source IP)	Login Type	Interface/Tunnel Name	▼# of Failed Attempts
1	admin (192.168.1.20)	SSL-VPN		1
2	ping 8.8.8.8 (console)	Admin	console	1

Figura 3.47. Análisis de Autenticación fallida

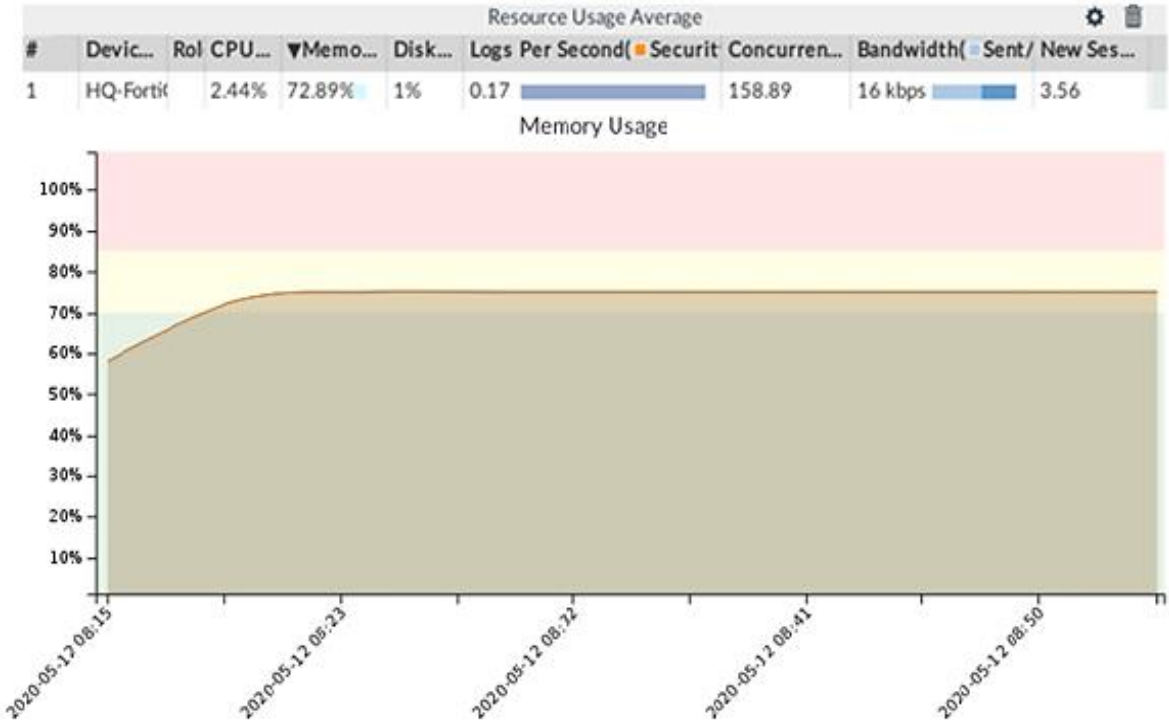


Figura 3.48. Análisis del uso de recursos

Finalmente, existe la opción de visualizar todos los aspectos mencionados con anterioridad a través de monitores, ya sea el tráfico, aplicaciones, rendimiento del sistema e inclusive el estado de los dispositivos.

3.1.10.2 Análisis de la seguridad

Al igual que el tráfico, la seguridad puede ser analizada a través de datos o mediante monitoreos y está dividida en antivirus, IPS, control de aplicaciones y DNS. En la Figura 3.49. se visualiza un esquema general de todas las amenazas de la red a través de monitoreos, inclusive un mapa en el cual se puede detectar geográficamente el origen de virus, intrusos, sitios botnet, etc.

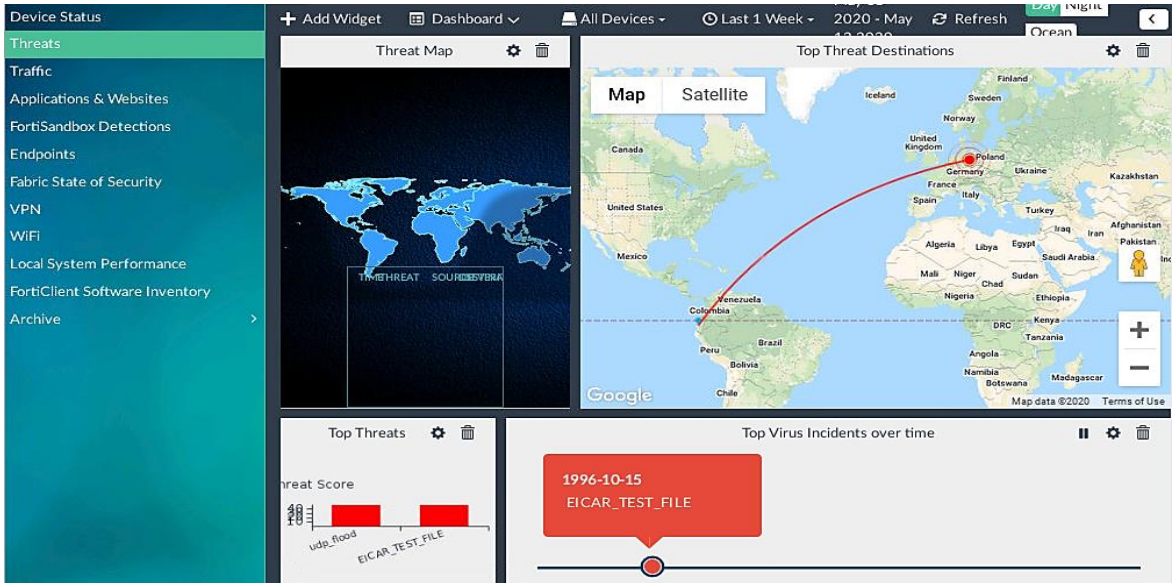


Figura 3.49. Análisis general de amenazas sobre la SD-WAN emulada

En la Figura 3.50. se visualiza el análisis de antivirus que muestra datos como: origen, tipo, riesgo, acción, etc. De igual manera ocurre con el IPS y el control de aplicaciones que se muestra en las Figuras 3.51 y 3.52.

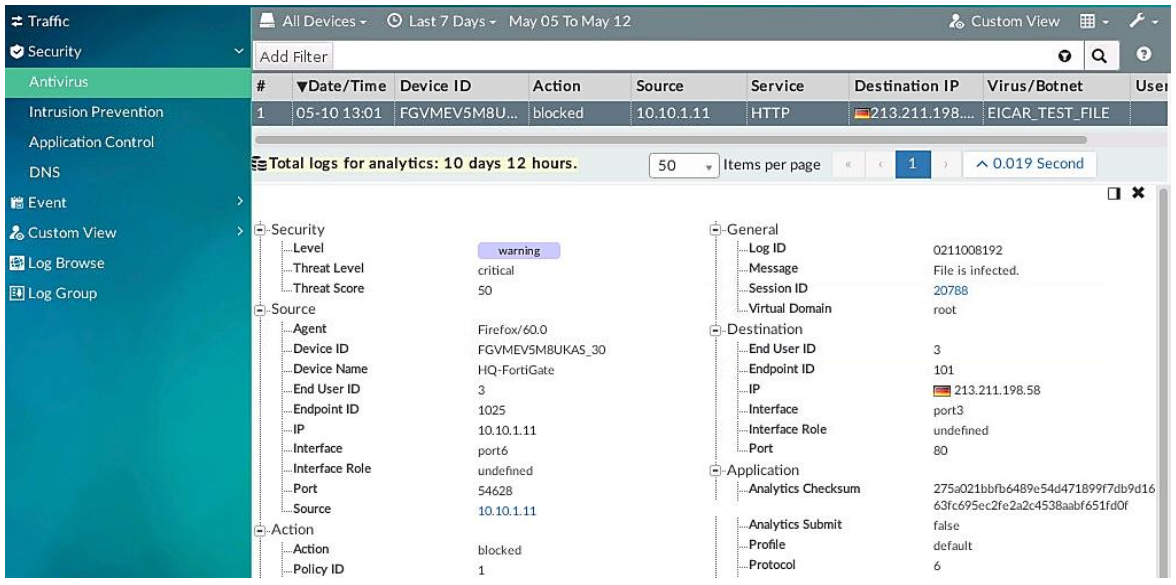


Figura 3.50. Análisis del perfil de antivirus

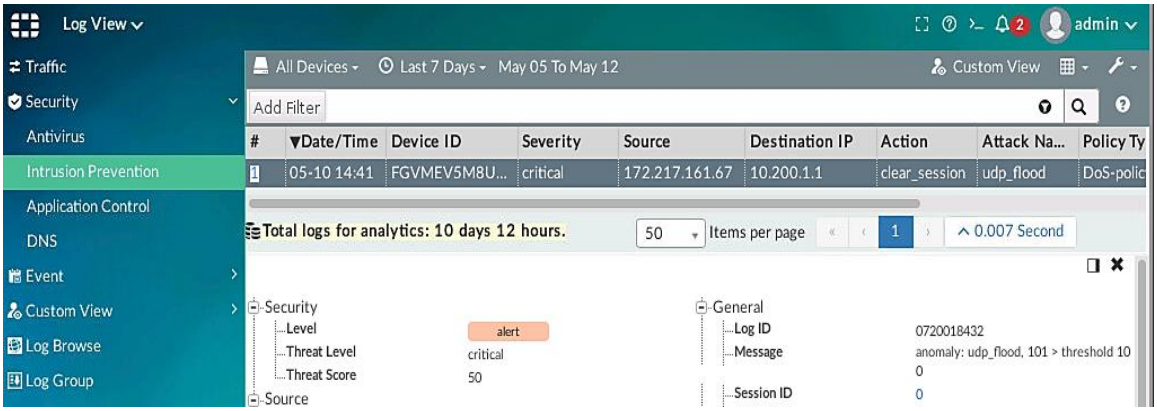


Figura 3.51. Análisis del IPS

Figura 3.52. Análisis del control de Aplicaciones

Es importante verificar un aspecto de la seguridad mencionado en la sección 3.1.7.3 correspondiente a un mapa geográfico de sitios Botnet, que permite identificar los países donde prevalecen estos, como se visualiza en la Figura 3.53.

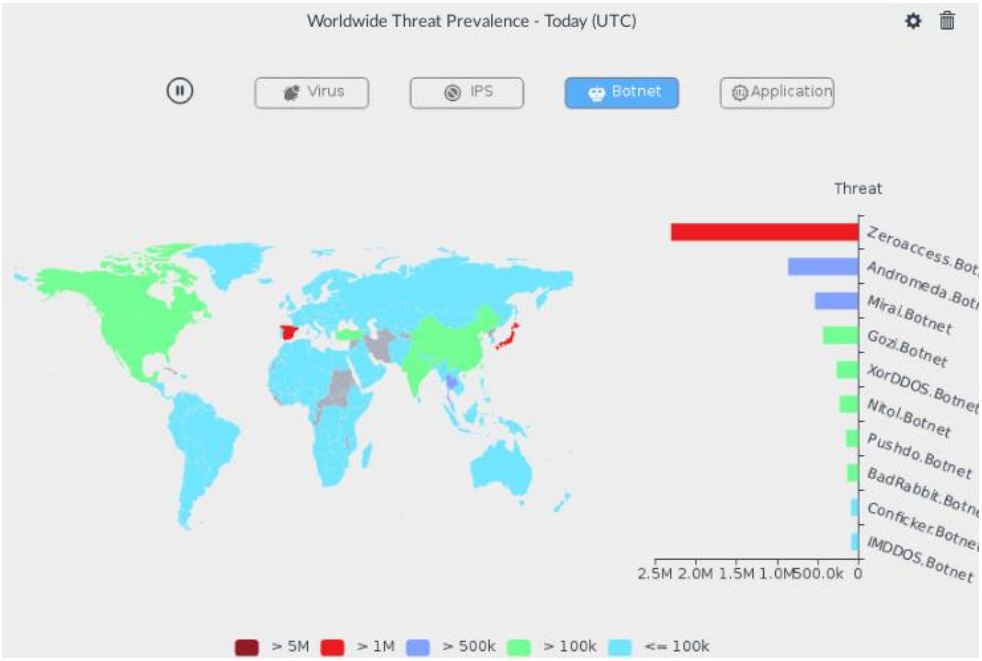


Figura 3.53. Mapa mundial de prevalencia de amenazas [34]

3.1.10.3 Reportes, incidencias y eventos

Esta sección es de mucha importancia, ya que describe la emisión de reportes acerca de la seguridad, VPN, amenazas, entre otros. De esta manera, la empresa o el departamento de TI puede conocer el funcionamiento de toda la red, así como las amenazas de las cuales pueden ser víctimas. En la Figura 3.54. se visualizan los reportes generados, los cuales pueden ser descargados en diferentes formatos e idiomas. El reporte de evaluación de amenazas se adjunta en el ANEXO C, en el cual se informa que se ha detectado un ataque IPS (udp_flood), un *malware/Botnet* (EICAR_TEST_FILE) y un acceso desde una aplicación remota (TeamViewer). El reporte de control de aplicaciones de riesgo, adjunto en el ANEXO D, detalla el nivel de riesgo, número de usuarios, sesiones y el ancho de banda que están consumiendo las aplicaciones spotify, chrome, *ping* y TeamViewer; inclusive estos parámetros se visualizan en las siguientes categorías: *Video/Audio*, *Remote Access, Network Service* y *Web Client.*

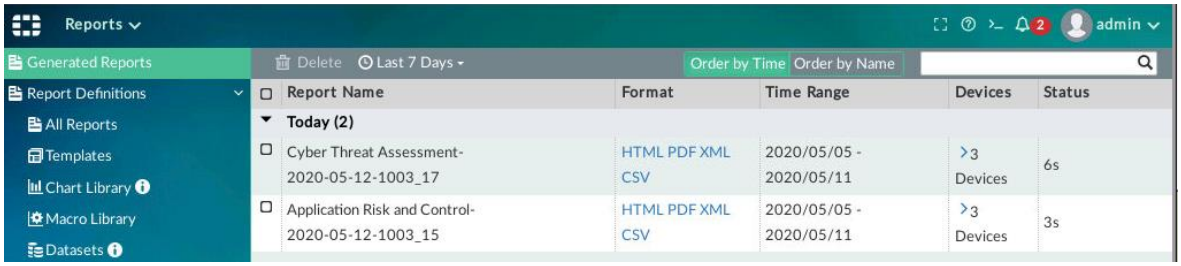


Figura 3.54. Reportes Generados en FortiAnalyzer

Finalmente, en la Figura 3.55. se muestran los eventos e incidentes que ocurren en cada uno de los dispositivos administrados por FortiAnalyzer; por ejemplo, "*Device offline*" indica que uno de los FortiGate se encuentra fuera de servicio, "*System Shutdown*" significa que un FortiGate estaba operativo y ha sido apagado, "*fgfm connection*" quiere decir que no hay conexión entre uno de los FortiGate con el FortiManager, entre otros. Algunos de estos eventos han sido provocados intencionalmente en la red, a fin de ser visualizados.

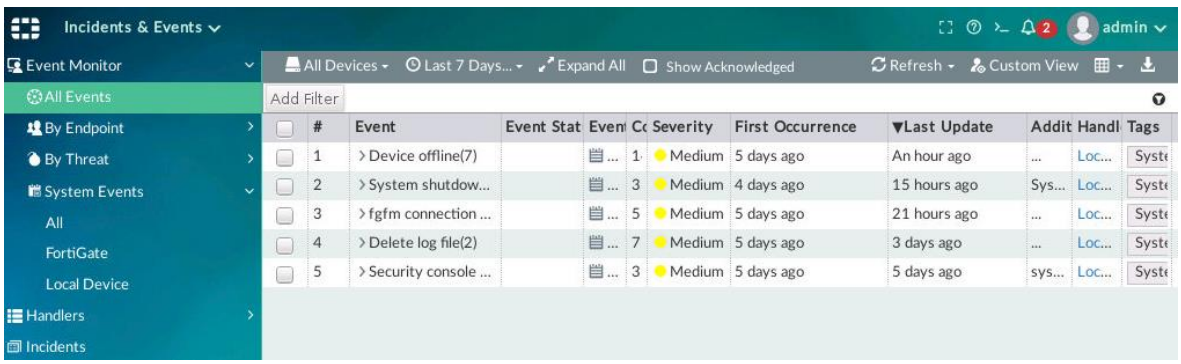


Figura 3.55. Incidentes y eventos de la SD-WAN emulada

Con base en los resultados de las secciones anteriores, especialmente el control a través de FortiManager y el análisis a través de FortiAnalyzer se comprueba que la administración de la SD-WAN es mucho más sencilla respecto a otras tecnologías, esto gracias a las FortiOS que ofrece FORTINET en sus dispositivos. Esto permite que el administrador de red tenga mayor flexibilidad para realizar actualizaciones e implementaciones basado en el estado y funcionamiento actual de la red, inclusive permite al dueño de la empresa entender cómo está operando su red gracias a la claridad de sus reportes.

3.1.11 ANCHO DE BANDA Y RENDIMIENTO DE APPS EN LA NUBE

En la Figura 2.10. se pudo notar que la SD-WAN Híbrida, tiene enlaces directamente conectados a Internet que eliminan el tráfico de *backhaul*. Por lo tanto, esto provoca un mayor rendimiento de aplicaciones en la nube, a diferencia de otras tecnologías en las que el tráfico pasa a través de un Centro de Datos.

Además, en la emulación de la SD-WAN Híbrida se comprueba que no depende del ancho de banda, ya que, en caso de necesitar un aumento de éste, solamente se debe actualizar la suscripción de Internet, es decir aumentar la velocidad contratada con el ISP, como se muestra en las Figuras 3.56. y 3.57. En otras tecnologías como MPLS, el aumento requiere un mayor análisis antes de su implementación.

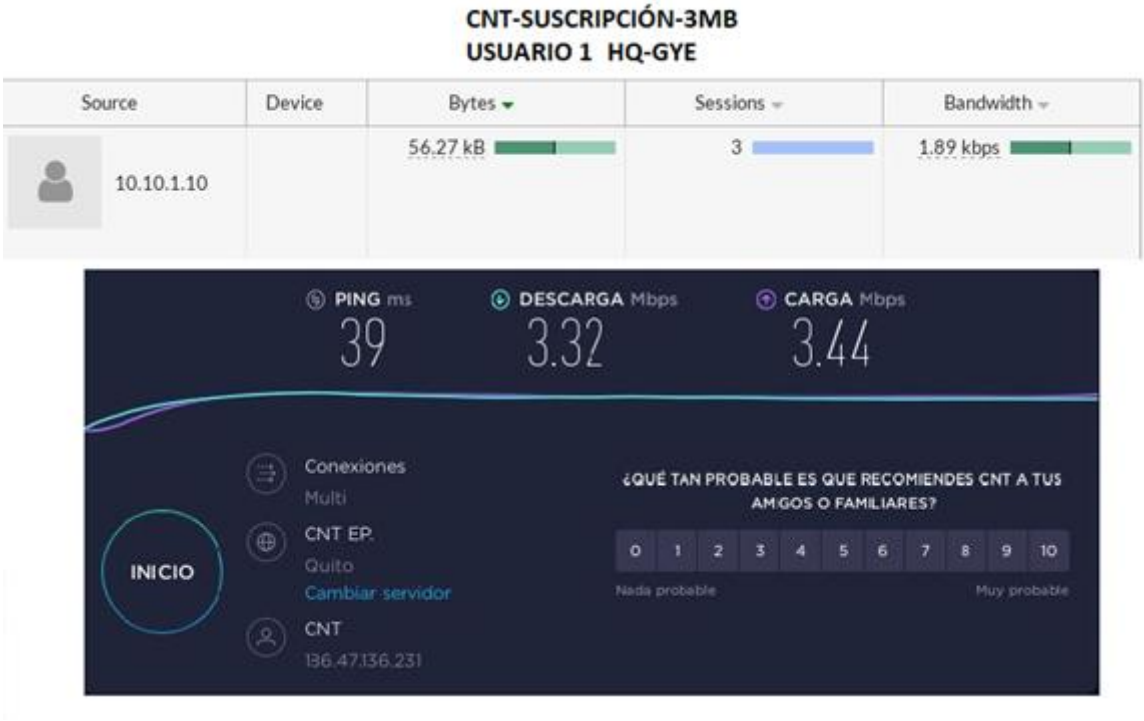


Figura 3.56. Suscripción inicial con CNT-3MB

Figura 3.57. Actualización de la suscripción con Netlife-10MB

Tomando en cuenta la función ZTP y la independencia del ancho de banda presentadas anteriormente, la SD-WAN emulada tiene escalabilidad mejorada. Es decir, se puede desplegar nuevas oficinas remotas y aumentar el ancho de banda con mayor facilidad y en menor tiempo.

3.2 USO DEL PROGRAMA GNS3

En este apartado se comprueban las funcionalidades de GNS3 las cuales permiten utilizarlo como reemplazo de otros programas, tales como Cisco Packet Tracer. Adicionalmente, se analiza el uso de dispositivos de distintos fabricantes, optimización de recursos a través de GNS3-VM y su capacidad de emulación.

3.2.1 DISPOSITIVOS DE DISTINTOS FABRICANTES

En la Figura 3.58. se puede visualizar como GNS3 permite utilizar dispositivos de diferentes fabricantes, tales como FORTINET, Cisco, Mikrotik e incluso máquinas virtuales de Windows y Ubuntu. Esta característica permitirá a estudiantes y administradores de red familiarizarse con dispositivos de distintos fabricantes y poder enfrentar nuevos desafíos que presenta la tecnología en el campo laboral.

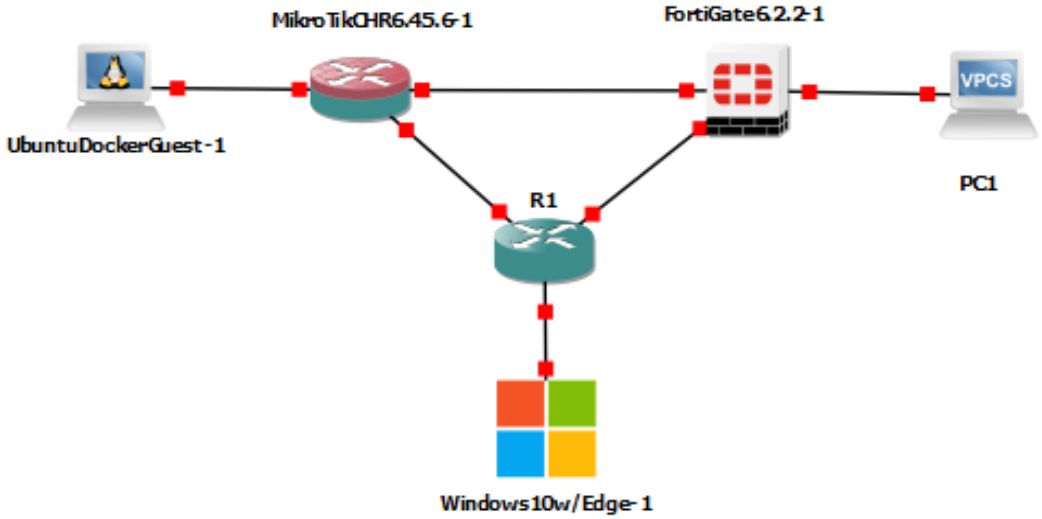


Figura 3.58. Interacción de GNS3 con dispositivos de diferentes fabricantes

3.2.2 OPTIMIZACIÓN DE RECURSOS CON GNS3-VM

Con base en la emulación de la SD-WAN, se pueden visualizar alrededor de 40 dispositivos tanto emulados como simulados, por lo que la cantidad de RAM y CPU consumida es bastante alta. En este caso, la GNS3-VM permite que todos los dispositivos se desplieguen sobre la máquina virtual y no directamente sobre la PC, de modo que en la máquina virtual se consuman todos los recursos virtuales, con el fin de que la CPU y la RAM de 16 GB puedan soportar la emulación de redes complejas. En la Figura 3.59. se visualiza en la GNS3-VM todos los dispositivos o recursos de la SD-WAN, a excepción de las máquinas virtuales que pertenecen a Virtualbox.

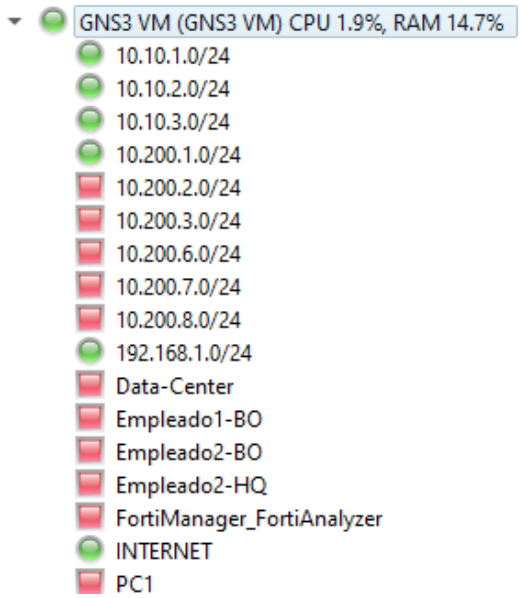


Figura 3.59. Dispositivos emulados sobre GNS3-VM

3.2.3 EMULACIÓN Y SIMULACIÓN

La emulación de dispositivos en GNS3 fue explicada anteriormente; de todas formas, en la Figura 3.60. se visualiza la ISO real del dispositivo FortiManager y en la Figura 3.61. los recursos de RAM y CPU que necesita para funcionar correctamente. Solamente los elementos de conmutación de GNS3 son simulados. En el caso de un despliegue real de una SD-WAN con tecnología FORTINET, las configuraciones, interfaz, CLI es similar a la de la emulación.

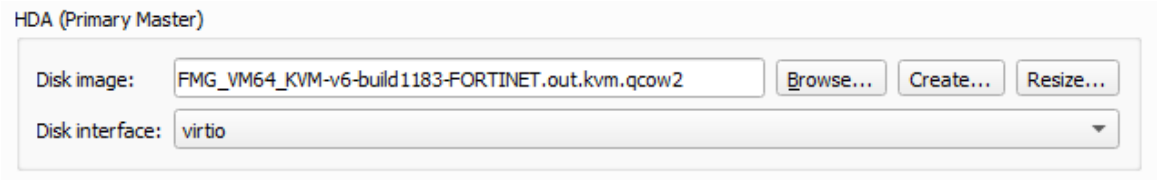


Figura 3.60. ISO de FortiManager descargada de FORTINET

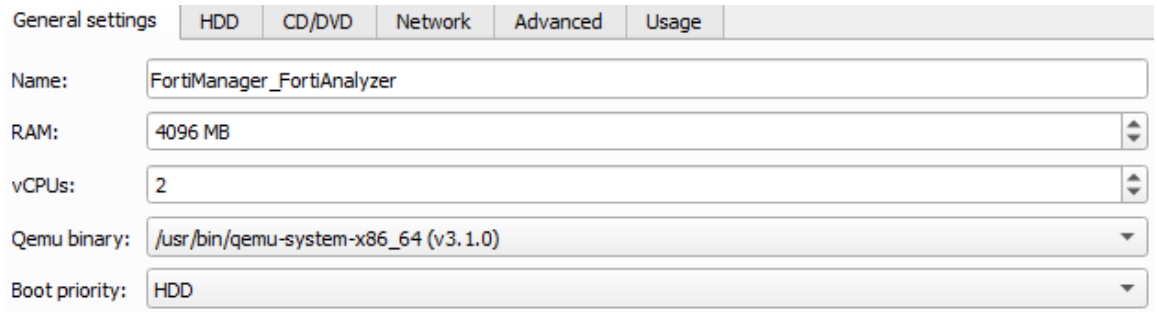


Figura 3.61. Recursos de RAM y CPU de FortiManager

4. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentan las conclusiones y recomendaciones del presente proyecto, basado en un análisis general de los resultados alcanzados, así como de la metodología utilizada.

4.1 CONCLUSIONES

Las definiciones, conceptos, arquitectura y funcionamiento descritos en el primer capítulo permitieron tener una mejor comprensión de la transición impulsada por *software* en el segmento WAN; este conocimiento previo contribuyó significativamente para el análisis y la emulación apropiada de la SD-WAN Híbrida utilizando tecnología FORTINET.

Durante la emulación de la SD-WAN se desarrollaron nuevas destrezas para el uso de un *software* distinto a Cisco Packet Tracer, conocido como GNS3. Esta herramienta permite utilizar dispositivos de diferentes fabricantes, de manera que los estudiantes puedan emular escenarios eligiendo distintos equipos con base en el rendimiento de funciones específicas. Es decir, se puede utilizar un equipo CISCO para enrutamiento, un equipo FORTINET como *firewall,* un equipo Aruba como punto de acceso, etc. De este modo, el proyecto facilita un manual de instalación y configuración para que los estudiantes, a más de emular, sean capaces de eliminar la restricción de trabajar con equipos de una marca específica.

El desarrollo de este Proyecto a través de la emulación de la red MPLS, permite también reforzar el conocimiento de los estudiantes de la Escuela Politécnica Nacional en cuanto a la práctica de MPLS, dado que su aprendizaje actualmente está enfocado principalmente en la teoría. Mediante la emulación se puede visualizar y entender el funcionamiento de la red MPLS, en particular, aspectos como: BGP con *route reflector,* Ingeniería de Tráfico utilizando RSVP, tunelización, entre otros; los cuales son altamente comprensibles en la práctica. Por esta razón, la red MPLS emulada permite tener una visión real de su despliegue, lo cual representa un valor añadido dentro del campo laboral.

Las arquitecturas de las SDN y de las SD-WAN cuentan con un controlador que se encarga de la toma de decisiones, como característica análoga. Considerando esta similitud, previo a emular la SD-WAN, es imprescindible comprender las SDN. Por esta razón, el estudio de la SD-WAN, permitió emular una SDN de manera implícita. Sin embargo, en la Figura 4.1. se muestra una SDN simulada con ODL como controlador que funciona como base inicial

para el desarrollo de la SD-WAN. Es importante mencionar que para su despliegue se utilizó la herramienta Mininet.

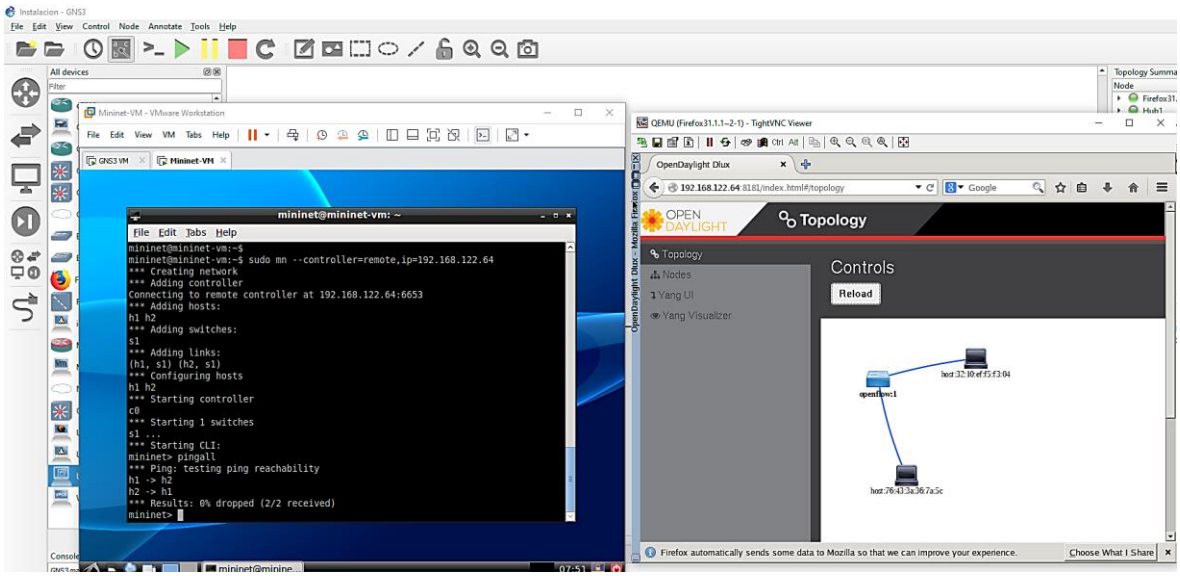


Figura 4.1. SDN con OpenDayLight utilizando Mininet

Los servicios o recursos disponibles en la sede principal y el Centro de Datos permiten conocer los parámetros de configuración de un servidor de correo electrónico y DNS. Durante la emulación de la SD-WAN, estos servidores se instalaron sobre máquinas virtuales y posibilitaron entender la virtualización de servidores de manera práctica, lo cual permite a los estudiantes integrar la virtualización y las SDN en un mismo despliegue, puesto que dichos aspectos son parte de las redes inteligentes.

Dado que la SD-WAN es una tecnología cuasi nueva, se presentaron dificultades para encontrar información de fuentes confiables y comprender su funcionamiento. Es así que, a través del análisis y emulación del presente proyecto se entiende que la SD-WAN usa la infraestructura pública de Internet para la transmisión de datos. Adicionalmente, la emulación de la SD-WAN en conjunto con la red MPLS ofrece mejores funcionalidades y optimiza el rendimiento de la red estableciendo políticas. Por ejemplo, una política es indicar que el tráfico de mayor confidencialidad se envíe a través de la red MPLS, mientras que el tráfico común de Internet a través de los enlaces de conexión de banda ancha. Esto con la finalidad de eliminar el tráfico de *backhaul* que ocasiona latencias en el tráfico de Internet. Por este motivo, la emulación de la SD-WAN Híbrida al ser multi-transporte, permite al estudiante familiarizarse con la optimización de las redes de transporte actuales y las que están por ser desplegadas en nuestro País.

Asimismo, el presente Trabajo de Titulación permite identificar la importancia que tiene la seguridad en las Redes Definidas por *Software,* y aún más en la SD-WAN debido al uso

de la infraestructura pública de Internet para la transmisión y recepción de datos. Mediante la emulación de la SD-WAN se describen y emulan parámetros de seguridad tales como: control de aplicaciones, sistemas de prevención de intrusos, antivirus, entre otros, indispensables en el despliegue de estas redes. En este sentido, este proyecto introduce conocimientos sobre seguridad, tanto teóricos como prácticos, y evidencia la necesidad de que se integre una asignatura de Seguridad dentro del pénsum académico de la carrera de Ingeniería en Electrónica y Telecomunicaciones.

Durante la emulación de la SD-WAN se utilizó tecnología FORTINET, la cual permite realizar el monitoreo y análisis exhaustivo de los enlaces de la red en tiempo real. Esto facilitó identificar la inteligencia con la que la SD-WAN realiza la selección dinámica de ruta. Esta selección se basa en parámetros como latencia, ancho de banda, pérdida de paquetes, aplicación e, inclusive, los SLA, los cuales se podrían utilizar para realizar balanceo de carga.

Con el desarrollo del presente proyecto se comprueba que la SD-WAN es una tecnología de red que permite tener control total desde un único sitio, en este caso, FortiManager en la sede principal. Con el objetivo de reducir tiempos de implementación, se comprobó la funcionalidad ZTP para desplegar nuevas oficinas remotas en cuestión de horas, eliminando la necesidad de un administrador en el sitio y la configuración individual de cada equipo.

Tomando en cuenta las vulnerabilidades de seguridad de otros proveedores por el acceso directamente a Internet, se determinó que FORTINET es, potencialmente, una de las mejores soluciones para el despliegue de una SD-WAN, gracias a las funcionalidades NGFW, inspección SSL y sus perfiles, mismas que maximizan la seguridad de la red. Además, se comprobó mediante *Wireshark* que la tunelización IPsec se encarga de cifrar por completo los datos que pasan a través de los enlaces de Internet, y la SSL-VPN, por su parte, crea una conexión segura de acceso remoto para sus empleados, mediante un portal web. Por lo tanto, la preocupación de las empresas por la seguridad de sus datos se reduce ampliamente.

La emulación de la SD-WAN permite a los estudiantes relacionarse con funcionalidades sustantivas de equipos, las mismas que simplifican procesos. Uno de ellos es FortiAnalyzer, una herramienta eficaz para el análisis del tráfico y seguridad en tiempo real. Se determinó que la misma es de gran apoyo, tanto para el administrador de red como para el gerente, ya que facilita conocer todo el funcionamiento, incidentes, ataques cibernéticos, etc., a través de la emisión automática de reportes inteligibles.

Se determinó que la SD-WAN de FORTINET representa un ahorro de costos en tres aspectos principales. En primer lugar, en cuanto a costos de operación (*OPEX*) a través de las funcionalidades ZTP y control centralizado; en segundo lugar, en los gastos de capital (CAPEX), al integrar las funcionalidades de SD-WAN, optimización WAN, *Firewall,* entre otras, en un único dispositivo (FortiGate); y, en tercer lugar, respecto al ancho de banda gracias a los enlaces directos a Internet, pues resulta más conveniente actualizar solamente la suscripción con el ISP.

Finalmente, este Proyecto incentiva al estudio y desarrollo de nuevas tecnologías sobre el mercado actual. El campo de Redes y Telecomunicaciones han tenido una evolución acelerada por la transformación digital y la contingencia actual por la que atraviesa el mundo debido a la pandemia. Estos aspectos han obligado a empresas públicas y privadas a virtualizar el trabajo, la educación, la medicina, entre otros. Por estos motivos, la SD-WAN Híbrida emulada encaja cabalmente como red de transporte, especialmente en Ecuador donde no se ha realizado aún un despliegue masivo de la SD-WAN.

4.2 RECOMENDACIONES

Se recomienda emular en la SD-WAN Híbrida un Centro de Datos definido por *software* (SD-DC) con la finalidad de que la red y el Centro de Datos sean administrados por el mismo controlador. Adicionalmente, es necesario investigar sobre los *Micro Data Centers* que tienen la capacidad de implementarse en tiempos reducidos y, de ser posible, reemplazar al Centro de Datos (Quito) de la SD-WAN Híbrida por la emulación de éste.

De igual manera, se puede emular una red definida por software hasta el usuario final. Es decir, investigar la SD-LAN y SD-WLAN e incorporar con la SD-WAN Híbrida. Adicionalmente, se recomienda averiguar sobre *Secure Access Service Edge* (SASE), el cual combina funciones de red y seguridad con capacidades WAN, esto es SASE converge con SD-WAN; esto último con el objetivo de mejorar la emulación de la SD-WAN Híbrida del presente proyecto.

Asimismo, emular una SD-WAN de otro fabricante, en este caso VMware que es la empresa líder según el cuadrante Mágico de Gartner y así realizar un cuadro comparativo para verificar cuáles son las ventajas o destrezas que presenta la *SD-WAN by VeloCloud* frente a la *Secure SD-WAN* de FORTINET.

La SD-WAN opera como red de transporte, por lo que se sugiere emular una red de acceso, ya sea MetroEthernet, MetroEthernet sobre MPLS o GPON y verificar su funcionamiento. En la Figura 4.2. se visualiza una sugerencia de la topología que puede desarrollarse en futuros proyectos.

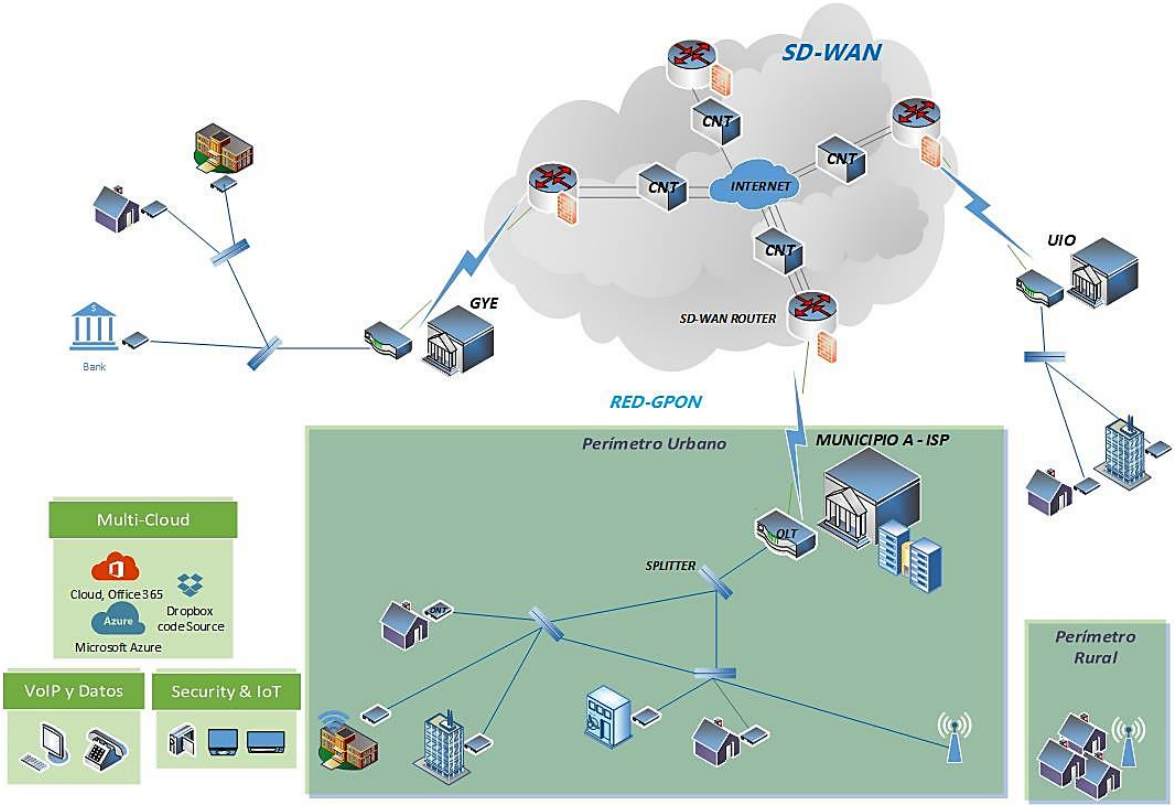


Figura 4.2. Esquema de SD-WAN con Red GPON

Además, se sugiere incorporar los dispositivos FortiSwitch y FortiAP, de tal modo que se visualicen las ventajas de utilizar el mismo proveedor para una LAN y WAN definidas por *software*. FortiSwitch permitiría tener una red inteligente, segura y automatizada a nivel local, mientras que FortiAP se encargaría de aprovisionar, monitorear y optimizar la red inalámbrica de manera continua. Estos dispositivos estarían controlados desde un único panel, como es FortiManager.

Por otro lado, se debe profundizar el tema de virtualización, tomando en cuenta que durante la emulación se configuran distintos servidores en un solo computador. Por ello, se recomienda introducir la asignatura de Virtualización en el pensum académico 2021 de la carrera de Ingeniería en Electrónica y Telecomunicaciones, la cual permitiría a los estudiantes prepararse para futuras certificaciones de VMware y despliegues de *Virtual Cloud Network.*

También es recomendable, adquirir una licencia de FortiGuard para poder emular todos los escenarios posibles de seguridad que ofrece la *Secure SD-WAN*, con el fin de visualizar las actualizaciones de la base de datos de FORTINET con las últimas amenazas y habilitar los perfiles de filtrado web, DNS y correo que maximizan la seguridad de la red e inclusive

aprovechar las características faltantes y eliminar las restricciones de la licencia de evaluación con respecto al número de políticas, VPN, VDOMS, etc.

Finalmente, con base en este Proyecto de Titulación se sugiere a la Universidad implementar un laboratorio de Telemática II, utilizando el programa GNS3 como complemento de *Cisco Packet Tracer,* y los equipos FORTINET que permitirían generar conocimientos sobre seguridad de redes y desplegar una SD-WAN. Esto implicaría prácticas de MPLS, SDN, SD-WAN, Seguridad, etc.

REFERENCIAS BIBLIOGRÁFICAS

[1] "Software-Defined Networking (SDN) Definition - Open Networking Foundation", Open Networking Foundation, 2020. [Online]. Disponible: https://www.opennetworking.org/sdn-definition/. [Último Acceso: 21- Mar- 2020].

[2] A. Steve, "How SD-WAN Facilitates WAN Security | SD Wan Experts", SD Wan Experts, 2020. [Online]. Disponible: https://www.sd-wan-experts.com/blog/sd-wans-make-wan-security-possible/. [Último acceso: 14- Feb- 2020].

[3] "Which emulator should I use? - GNS3", Docs.gns3.com, 2020. [Online]. Disponible:https://docs.gns3.com/1o4IX8nXISl5gb4BwoSFrUht3MeTjkzHM1TCeWAe669g/index.html [Último acceso: 14- Feb- 2020].

[4] "IPsec vs. SSL VPN: What's the Difference? | The Tech Portal", The Tech Portal, 2020. [Online]. Disponible: https://thetechportal.com/ipsec-vs-ssl-vpn-whats-the-difference/. [Último Acceso: 21- Mar- 2020].

[5] Projekter.aau.dk, 2020. [Online]. Disponible: https://projekter.aau.dk/projekter/files/281292955/Masters_thesis_Mario_Todorov.pdf. [Último Acceso: 21- Mar- 2020].

[6] "Difference between SD-WAN and Traditional WAN", Rfwireless-world.com, 2020. [Online]. Disponible: https://www.rfwireless-world.com/Terminology/Difference-between-SD-WAN-and-Traditional-WAN.html. [Último Acceso: 21- Mar- 2020].

[7] "SD-WAN vs. Traditional WAN | A Side-by-Side Comparison – ExterNetworks", SD-WAN, 2020. [Online]. Disponible: https://www.extnoc.com/sd-wan/sd-wan-vs-traditional-wan/. [Último Acceso: 21- Mar- 2020].

[8] "Traditional WAN vs. SD-WAN: Here’s What You Need to Know", Burwood Group, 2020. [Online]. Disponible: https://www.burwood.com/blog-archive/traditional-wan-vs-sd-wan-heres-what-you-need-to-know. [Último Acceso: 21- Mar- 2020].

[9] "Traditional WAN vs SD-WAN | VMware", VMware, 2020. [Online]. Disponible: https://www.vmware.com/latam/solutions/sd-wan-traditional-wan.html. [Último Acceso: 21- Mar- 2020].

[10] P. Hidalgo, "MULTIPROTOCOL LABEL SWITCHING (MPLS)", Quito, Ecuador, 2016.

[11] Bibdigital.epn.edu.ec, 2020. [Online]. Disponible: https://bibdigital.epn.edu.ec/bitstream/15000/6681/1/CD-5065.pdf. [Último Acceso: 21- Mar- 2020].

[12] "What is Software-Defined Networking (SDN)?", SearchNetworking, 2020. [Online]. Disponible: https://searchnetworking.techtarget.com/definition/software-defined-networking-SDN. [Último Acceso: 21- Mar- 2020].

[13] Repositorio.ug.edu.ec, 2020. [Online]. Disponible: http://repositorio.ug.edu.ec/bitstream/redug/45274/1/B-CINT-PTG-N.472%20Nazareno%20Arroyo%20Steven%20Edwing.pdf. [Último Acceso: 21- Mar- 2020].

[14] Oa.upm.es, 2020. [Online]. Disponible: http://oa.upm.es/42968/1/TFM_RAUL_ALVAREZ_PINILLA.pdf. [Último Acceso: 21- Mar- 2020].

[15] Scss.tcd.ie, 2020. [Online]. Disponible: https://www.scss.tcd.ie/publications/theses/diss/2016/TCD-SCSS-DISSERTATION-2016-042.pdf. [Último Acceso: 21- Mar- 2020].

[16] "Cisco SDWAN Design Series-Part-3- Control & Data Planes Logic – Net Design Areena", Netdesignarena.com, 2020. [Online]. Disponible: http://www.netdesignarena.com/index.php/2019/02/19/cisco-sdwan-design-series-part-3-control-data-planes-logic/. [Último Acceso: 24- Mar- 2020].

[17] M. Smith, "The 3 types of SD-WAN architecture", Network World, 2020. [Online]. Disponible: https://www.networkworld.com/article/3219653/the-3-types-of-sd-wan-architecture.html. [Último Acceso: 24- Mar- 2020].

[18] Diva-portal.org, 2020. [Online]. Disponible: http://www.diva-portal.org/smash/get/diva2:952048/FULLTEXT01.pdf. [Último Acceso: 24- Mar- 2020].

[19] "▷ GNS3 Guía Introductoria: Características y Requerimientos Mínimos", Telectrónika, 2020. [Online]. Disponible: https://telectronika.com/articulos/ti/que-es-gns3/. [Último Acceso: 24- Mar- 2020].

[20] "Learn more about Fortinet", Fortinet, 2020. [Online]. Disponible: https://www.fortinet.com/corporate/about-us/about-us.html. [Último Acceso: 24- Mar- 2020].

[21] "Soluciones de SD-WAN | Fortinet", Fortinet, 2020. [Online]. Disponible: https://www.fortinet.com/lat/products/sd-wan.html. [Último Acceso: 24- Mar- 2020].

[22] "Documentación de Fortinet en Español", Fortixpert.blogspot.com, 2020. [Online]. Disponible: https://fortixpert.blogspot.com/2015/06/documentacion-de-fortinet-en-espanol.html. [Último Acceso: 24- Mar- 2020].

[23] F. Analysis, D. Robb and P. Shread, "Fortinet FortiGate: Next-Gen Firewall Overview and Analysis", Esecurityplanet.com, 2020. [Online]. Disponible: https://www.esecurityplanet.com/products/fortinet-fortigate.html. [Último Acceso: 24- Mar- 2020].

[24] "What is a DNS Server", Cloudflare, 2020. [Online]. Disponible: https://www.cloudflare.com/learning/dns/what-is-a-dns-server/. [Último Acceso: 01- May- 2020].

[25] "What is a DNS server? | Internet.com", Internet.com, 2020. [Online]. Disponible: https://internet.com/domains/what-is-a-dns-server/. [Último Acceso: 15- May- 2020].

[26] "dnsmasq - Debian Wiki", Wiki.debian.org, 2020. [Online]. Disponible: https://wiki.debian.org/dnsmasq. [Último Acceso: 15- May- 2020].

[27] "Mail Server Definition", Techterms.com, 2020. [Online]. Disponible: https://techterms.com/definition/mail_server. [Último Acceso: 15- May- 2020].

[28] "What is a Mail Server and How Does it Work? (Article)", Samlogic.net, 2020. [Online]. Disponible: https://www.samlogic.net/articles/mail-server.htm. [Último Acceso: 15- May- 2020].

[29] "TFTP Server", Keil.com, 2020. [Online]. Disponible: https://www.keil.com/pack/doc/mw/Network/html/group__net_t_f_t_ps___func.html. [Último Acceso: 15- May- 2020].

[30] "Syslog: Servers, Messages & Security - Tutorial & Defintion [Free Tool!]", Network Management Software - Reviews & Network Monitoring Tools, 2020. [Online]. Disponible: https://www.networkmanagementsoftware.com/what-is-syslog/. [Último Acceso: 15- May- 2020].

[31] P. Hidalgo, "ENRUTAMIENTO EN REDES TCP/IP", Quito, Ecuador, 2018.

[32] "Administration Guide | FortiGate / FortiOS 6.4.0 | Fortinet Documentation Library", Docs.fortinet.com, 2020. [Online]. Disponible: https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/954635/getting-started. [Último Acceso: 15- May- 2020].

[33] "Eicar – EUROPEAN EXPERT GROUP FOR IT-SECURITY", *Eicar.org*, 2020. [Online]. Disponible: https://www.eicar.org/. [Último Acceso: 19- May- 2020].

[34] "FortiGuard", *FortiGuard*, 2020. [Online]. Disponible: https://fortiguard.com/threat-research/map. [Último Acceso: 20- May- 2020].

[35] O. Philco, "*Red de Acceso Caso: Red de Acceso de Operadores en Ecuador*", Quito, Ecuador, 2015.

[36] C. Courcoubetis, "*Access Network, Access Technologies, Broadband Services and Applications*", SPRING, 2007.

ANEXOS

ANEXO A. Manual de Instalación y Configuración de GNS3

ANEXO B. Esquema completo de la emulación de la SD-WAN Híbrida

ANEXO C. Reporte de Evaluación de Amenazas Cibernéticas

ANEXO D. Reporte del Control de Aplicaciones de Riesgo

ANEXO A

MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE GNS3

ANEXO B

ESQUEMA COMPLETO DE LA EMULACIÓN DE LA SD-WAN HÍBRIDA

ANEXO C

REPORTE DE EVALUACIÓN DE AMENAZAS CIBERNÉTICAS

ANEXO D

REPORTE DEL CONTROL DE APLICACIONES DE RIESGO

ORDEN DE EMPASTADO