ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DESARROLLO DE UN PROTOTIPO DE UNA RED SD-WAN (SOFTWARE-DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA FORTINET

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

DARWIN RAFAEL CADENA YANCHAPAXI

darwin.cadena@epn.edu.ec

DIRECTOR: M.Sc. PABLO WILIAN HIDALGO LASCANO

pablo.hidalgo@epn.edu.ec

DMQ, febrero 2022

CERTIFICACIONES

Yo, DARWIN RAFAEL CADENA YANCHAPAXI declaro que el trabajo de integración curricular 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.

Darwin Rafael Cadena Yanchapaxi

Certifico que el presente trabajo de integración curricular fue desarrollado por DARWIN RAFAEL CADENA YANCHAPAXI, bajo mi supervisión.

M.Sc. Pablo Wilian Hidalgo Lascano
DIRECTOR

DECLARACIÓN DE AUTORÍA

A través de la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el producto resultante del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

Darwin Rafael Cadena Yanchapaxi

M.Sc. Pablo Wilian Hidalgo Lascano

DEDICATORIA

El presente proyecto lo dedico de manera muy especial a mis padres José Rafael y María Ramona, por todo su esfuerzo, apoyo, sacrificio, siendo un ejemplo de lucha, de trabajo, de perseverancia y que han permitido que todo esto sea posible.

Para mis sobrinas, Heather, Caroline, Sophie, que han sido mi motor e inspiración en mi vida, para continuar creciendo en lo personal y profesional, para mi sobrino Danilo, un integrante recién llegado a la familia y una alegría más en nuestras vidas, espero ser un buen ejemplo a seguir como persona, para ustedes mis amores con mucho ***AMOR***.

Y sin olvidar a mis segundos padres, mis abuelitos, a José Luis por permitirme crecer como persona, alentarme siempre en los estudios y a ser mejor persona cada día, a María Hortencia, que en paz descanse y donde sea que estes, quiero que estés orgullosa de mí y esperando el día que volvamos a reencontrarnos.

Dedicado para ustedes mi Familia.

"Porque nunca es tarde,
y el tiempo sólo se acaba cuando se acaba la vida.
Y hasta ese momento, siempre existe una posibilidad para todo."

AGRADECIMIENTO

Muy agradecido con mis padres José Rafael y María Ramona, quienes me han apoyado incondicionalmente en todo momento a pesar de las adversidades, gracias a ellos he podido finalizar una etapa más de mi vida.

A mis hermanos Cristian, Diego, Alexis, a mi cuñada Ritina, gracias por siempre apoyarme y por su ejemplo brindado de seguir siempre para adelante.

A mi tutor M.Sc. Pablo Hidalgo, por su ayuda, orientación, dedicación, paciencia y sobre todo gracias por su confianza depositada en mi persona para poder culminar este proyecto.

A los Ingenieros Leonardo Quintero y Paulo Fernández por permitirme hacer uso de las instalaciones y equipos dentro de la empresa Puntonet S.A. para el desarrollo de este proyecto.

Y a todas las personas y amigos que me apoyaron de diferente manera, gracias a Johana y Gonzalo por su paciencia y colaboración brindada en esta última etapa; a mis amigos Christian, Gabriel, Gustavo, que me han acompañado siempre con sus palabras de aliento y motivación.

Siempre muy agradecido con todos.

ÍNDICE DE CONTENIDO

RESUMEN

En el presente Trabajo de Integración Curricular se desarrolla un prototipo de una red SD-WAN empleando equipos Fortinet, prototipo que puede ser utilizado como referencia y base en el aprendizaje de esta nueva tecnología.

En el primer capítulo, se describen los fundamentos teóricos, características y funcionalidades de las redes MPLS, del acceso a Internet, la SD-WAN y su importancia. Se revisa la virtualización de servidores en VMware, la teoría sobre el servidor multimedia Plex y las consideraciones sobre la tecnología y equipos del fabricante Fortinet.

En el segundo capítulo, se presenta el diseño e implementación de las redes propuestas para obtener una SD-WAN Híbrida; se incluyen sus topologías lógicas y físicas, componentes de hardware y software, direccionamiento, las políticas, reglas y seguridad que proporcionan los *firewalls* FortiGate; la administración centralizada con FortiManager y las configuraciones de cada uno de los equipos.

En el tercer capítulo se presentan los resultados de las pruebas de funcionamiento de la SD-WAN, verificando conectividad entre sitios, la administración del tráfico, seguridad y control de la red, así como el correcto funcionamiento de los servidores implementados. Adicionalmente, se presentan las conclusiones obtenidas con el desarrollo del proyecto, así como las recomendaciones para futuros trabajos.

Finalmente se presenta un conjunto de anexos correspondientes a los manuales y configuraciones detalladas de los equipos, configuraciones de los servidores, el detalle de las políticas, reglas y seguridad de la SD-WAN expuestas en el capítulo 2, así como un enlace en donde se encuentra un video que permite verificar el funcionamiento del producto final demostrable.

PALABRAS CLAVE: SD-WAN, MPLS, VMware, Plex, Fortinet, FortiGate, FortiManager.

ABSTRACT

In this Curriculum Integration Project, a prototype of an SD-WAN network is developed using equipment from the manufacturer FORTINET, which can be used as an input for learning this new technology.

The first chapter describes the theoretical fundaments, characteristics and functionalities of MPLS, Internet access, SD-WAN networks and its importance. It contains a review of server virtualization in VMware, the theory of the Plex media server and considerations of the technology and equipment from the manufacturer Fortinet.

The second chapter contains the design and implementation of the proposed networks to obtain a Hybrid SD-WAN; including their logical and physical topologies, hardware and software components, addressing, policies, rules, and security provided by FortiGate firewalls, centralized management with FortiManager, and configurations from each equipment.

The third chapter establishes the results and analysis of the SD-WAN performance tests, verifying connectivity between sites, traffic management, security and control network, as well as the correct performance of the implemented servers. Additionally, the conclusions obtained with the development of this project, as well as the recommendations for future projects.

Finally, this project contains annexes corresponding to the manuals and detailed configurations of the equipment, server configurations, the details of the policies, rules and security of the SD-WAN exposed in chapter 2, also contain a link where is including a video that allows to verify the operation of the demonstrable final product.

KEYWORDS: SD-WAN, MPLS, VMware, Plex, Fortinet, FortiGate, FortiManager.

1 INTRODUCCIÓN

Conceptualmente las SD-WAN (*Software-Defined Wide Area Network*), permiten gestionar y controlar de forma centralizada todos los componentes de hardware a través de software dentro de una infraestructura de red, de una manera más sencilla, aumentando el rendimiento, eficiencia, su estabilidad y automatizando la red ante diferentes escenarios o situaciones, reduciendo los costos de implementación [1].

En la carrera de Ingeniería en Tecnologías de la Información de la Escuela Politécnica Nacional, no se ha incorporado en su pensum, contenido, herramientas o laboratorios sobre las SD-WAN, lo cual dificulta a los estudiantes conocer sobre nuevas tecnologías. En el pensum se mantiene el estudio de WANs tradicionales, realizando laboratorios sobre equipos y plataformas Cisco cuyas versiones de software no permiten realizar prácticas sobre prototipos SD-WAN.

Por tal motivo se desarrolla un prototipo de red SD-WAN con tecnología Fortinet, con la finalidad de que los estudiantes puedan adquirir y aprovechar los conocimientos y beneficios que ofrece las SD-WAN, permitiendo que se preparen de mejor manera para el mundo laboral y los desafíos tecnológicos a los que se pueden enfrentar.

1.1 OBJETIVO GENERAL

Desarrollar un prototipo de una red SD-WAN (*Software-Defined Wide Area Network*) utilizando tecnología Fortinet.

1.2 OBJETIVOS ESPECÍFICOS

1. Analizar los fundamentos teóricos, características y funcionalidades de la red MPLS, red de acceso a Internet y SD-WAN.
2. Diseñar el prototipo de la red SD-WAN.
3. Implementar el prototipo de la red SD-WAN de acuerdo al diseño realizado.
4. Analizar los resultados en base a las pruebas de funcionalidad sobre el prototipo de red SD-WAN desarrollado.

1.3 ALCANCE

Se implementa un prototipo de una SD-WAN basada en la tecnología Fortinet. Para ello primero se diseña la SD-WAN, para luego pasar a emular las conexiones utilizando equipos FortiGate, y con el uso de la plataforma de FortiManager en la nube, se controla, configura o modifica de forma centralizada la SD-WAN.

Esto permitirá adquirir conocimientos sobre tecnologías que se han incorporado en el mercado, dado que en la carrera de Ingeniería en Tecnologías de la Información se estudia y se practica sólo con dispositivos Cisco, que no permiten desarrollar prototipos SD-WAN.

Dentro del diseño, se considera a una red IP/MPLS como una WAN principal, para el enrutamiento de etiquetas y paquetes, con configuración básica, ya que este proyecto no se basa en el estudio de este tipo de red. La IP/MPLS se la diseña asumiendo cierta capacidad de tráfico y usuarios; está conformada por un nodo de *Core* que tiene la funcionalidad de *router* P (enrutador del Proveedor) para el enrutamiento de etiquetas, y por tres nodos que cumplen la función de *routers* PEs (enrutador de Borde del Proveedor) para el acceso a la nube MPLS con ciertas características como Calidad de Servicio (QoS), Clase de Servicio (CoS) y Tablas de Enrutamiento Virtual (VRFs) [2].

Como WAN secundaria se estudia y diseña una WAN de acceso a Internet [3], para lo cual se emplea un *router* Cisco. En el PE de Puntonet está configurada la IP del *Gateway* con su máscara /29; a través de la última milla de fibra se conecta al *router* en modo *Switch* para entregar las IPs públicas y configurar los *firewalls* para salida a Internet.

Para emular los tres sitios que conforman la red, se colocan tres equipos *firewall* FortiGate, uno en cada sitio, los cuales conectan su LAN con la nube MPLS y con la red Internet; se proporciona seguridad a la red mediante túneles IPSec. Se crean políticas de Calidad de Servicio (QoS) priorizando el tráfico; se realiza enrutamiento dinámico, Acuerdos de Nivel de Servicio (SLA), entre otros.

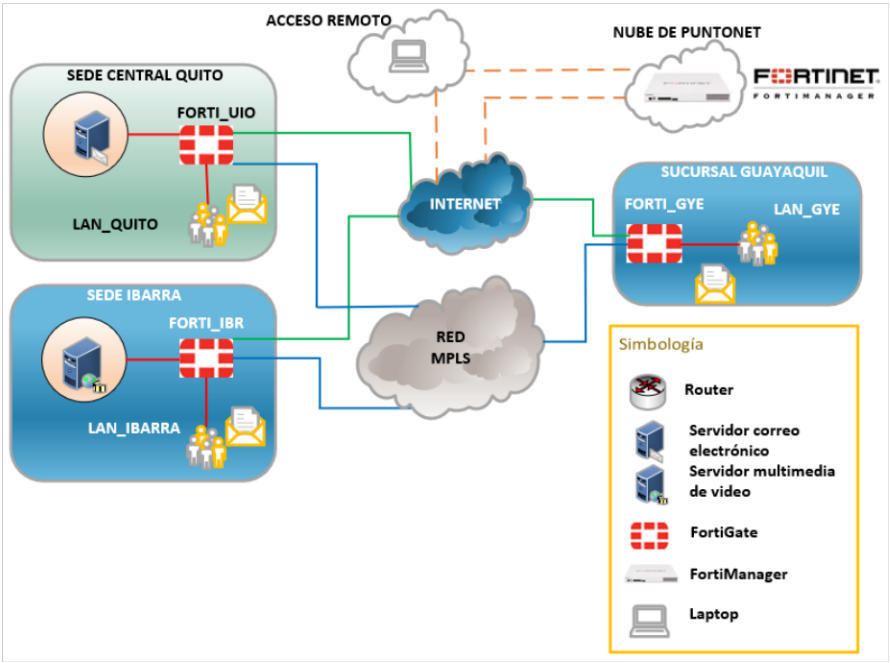


Figura 1.1. Diagrama del prototipo de Red Híbrida SD-WAN.

Para los servicios y el análisis del tráfico, se virtualiza los servidores de correo electrónico y DNS (*Servidor de Nombres de Dominio*) sobre una máquina virtual con VMware [4]. Para generar tráfico de datos y tráfico de video se utiliza el software Plex Media Server [5] que permite incorporar un servidor multimedia de video.

En la figura 1.1, se presenta el prototipo de la WAN híbrida propuesta, conformada por una WAN MPLS y una WAN de acceso a Internet. La Sede Central se tiene en la ciudad de Quito, donde se conecta el servidor de correo electrónico y el servidor DNS. Se emula desde el sitio de Ibarra la conexión al servidor multimedia de video, así como la emulación de una sucursal en la ciudad de Guayaquil. En cada sede tendrá su respectiva LAN.

Dentro de la red se toma en cuenta el tráfico de datos y video para el análisis, para lo cual se usan las funcionalidades que brinda SD-WAN con FortiGate, para demostrar que el enrutamiento es dinámico y selectivo, garantizando la mejor ruta para el tráfico en función de parámetros como latencia, *jitter*, pérdida de paquetes, seguridad, entre otros [6].

Para proporcionar una administración centralizada de la SD-WAN, se utilizan las funcionalidades de FortiManager [7] incorporada en la nube del proveedor Puntonet, en la cual se sincronizan los FortiGate mediante la IP pública o el *serial number*, pudiendo editar, modificar o eliminar políticas, reglas o parámetros directamente, sin tener que ir al sitio.

Concluida la implementación se realizan las respectivas pruebas para evidenciar el correcto funcionamiento de la red híbrida SD-WAN.

1.4 MARCO TEÓRICO

1.4.1 MPLS (MULTIPROTOCOL LABEL SWITCHING)

MPLS es una tecnología creada principalmente para el transporte de datos, su estándar IETF (*Internet Engineering Task Force*) corresponde al RFC 3031, mismo que permite un diseño con escalabilidad [8].

MPLS se basa en la conmutación de etiquetas; puede funcionar sobre diversos protocolos de capa Enlace, como Frame Relay, ATM, Ethernet, entre otros. Trabaja entre la capa de Enlace de datos y la capa de Red del modelo OSI (*Open System Interconnection*). MPLS fue creada para incrementar la velocidad de datos y mejorar el rendimiento mediante QoS (*Calidad de Servicio*), la cual se basa en la CoS (*Clase de Servicio*), debido a que el *router* observa la etiqueta del paquete para poderlo conmutar a través del *backbone* de la MPLS sin requerir hacer procesamiento de la cabecera de capa Red [9].

1.4.1.1 Cabecera MPLS

La cabecera MPLS que trabaja entre las capas 2 y 3 del modelo OSI (capa 2.5), se muestra en la figura 1.2.

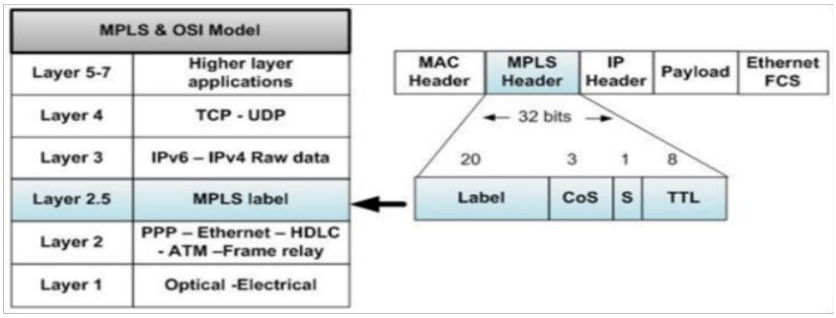


Figura 1.2. Cabecera MPLS [10].

1.4.1.2 Elementos de la red MPLS

- **LER (*Label Edge Router*):** *Routers* PE ubicados en el borde de la MPLS; colocan o retiran la etiqueta, dependiendo si el paquete ingresa o sale de la red [11].
- **LSR (*Label Switch Router*):** *Routers* P que reenvían los paquetes según el valor de la etiqueta; realizan la conmutación de etiquetas (*Label-Swapping Function*) [11].
- **LSP (*Label Switch Path*):** Conjunto de LSRs en secuencia que genera un camino para el paquete etiquetado a través de la MPLS, siendo unidireccional [11].
- **FEC (*Forwarding Equivalence Class*):** Hace referencia a un subconjunto de paquetes IP, que se encaminan bajo una etiqueta para ser tratados de la misma forma a través de los enrutadores LSR [11].
- **LDP (*Label Distribution Protocol*):** Protocolo utilizado dentro de la MPLS para la distribución de etiquetas, que permite levantar el camino LSP [11].

1.4.1.3 Arquitectura MPLS

Conformada por un Plano de Control y un Plano de Datos tal como muestra la figura 1.3.

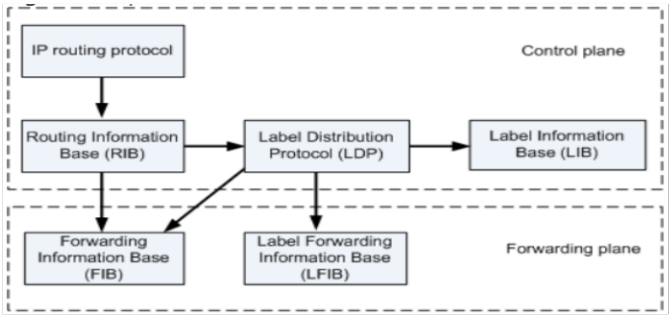


Figura 1.3. Arquitectura de la red MPLS [12].

1.4.1.4 Funcionamiento de la red MPLS

En la figura 1.4 se presenta el funcionamiento de la red MPLS, en la que se observa el camino LSP que va formando a través de los equipos LSR de la MPLS [13].

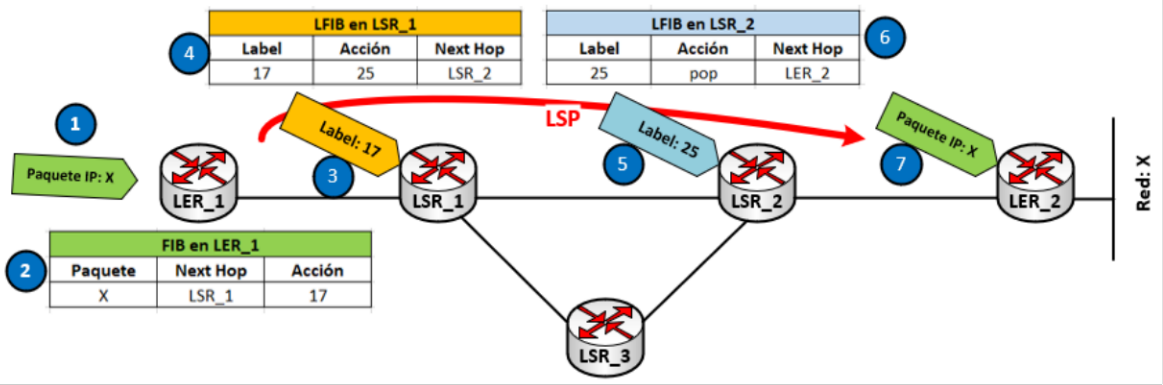


Figura 1.4. Funcionamiento de la red MPLS [13].

1.4.2 RED DE ACCESO A INTERNET

Representa al segmento de red que conecta al usuario final con el Proveedor de Servicio de Internet (ISP) a través de diferentes tecnologías (cableada o inalámbrica) [14].

1.4.2.1 Arquitectura de la red de Acceso

En la actualidad, las redes PON (*Red Óptica Pasiva*) son las más utilizadas como última milla. Disponen de una arquitectura punto a multipunto (P2MP), empleando *splitters* ópticos que dividen la señal descendente de un OLT (*Terminal de Línea Óptica*) en varias rutas hasta llegar a los usuarios. En sentido ascendente realizan la función contraria [15].

La figura 1.5, muestra una PON con los componentes que intervienen para llegar al usuario, a partir de los OLT ubicados del lado del proveedor de servicios. Los ONT (*Terminales Ópticos de Red*) ubicados en el usuario final, se conectan a las fibras de distribución, completando el tramo entre el proveedor y el usuario. La fibra óptica puede dividirse para 256 usuarios, llegando a un ONT que proporciona al usuario acceso a la red [15].

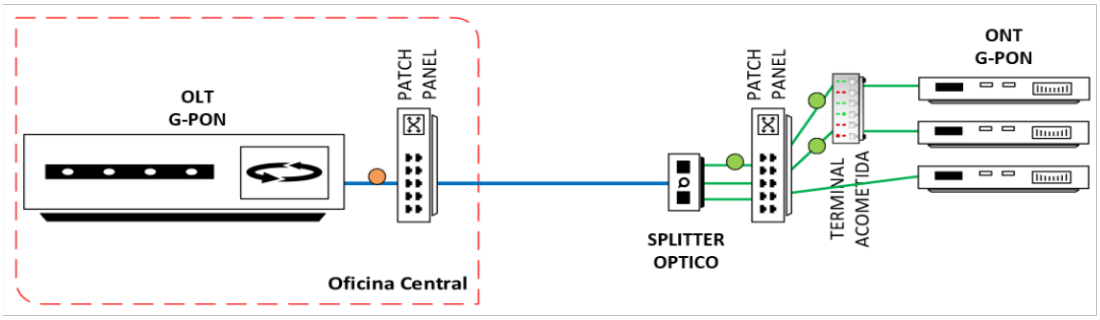


Figura 1.5. Arquitectura de una red de Acceso con Fibra Óptica.

1.4.2.2 Aplicaciones de las redes PON

Algunas de las aplicaciones son las redes de fibra (FTTx); se dividen en varias clases dependiendo del acercamiento al usuario final, los cuales son: FTTH (*Fiber to The Home*), FTTD (*Fiber to The Door*), FTTB (*Fiber to The Building*) y FTTC (*Fiber to The Cabinet*) [16].

1.4.2.3 Tipos de red de Acceso

Hace unos años, los operadores empleaban la infraestructura de acceso que había sido desplegada inicialmente para ofrecer servicios de telefonía y televisión, es decir, las redes de pares de cobre y de cable coaxial. Posteriormente, comenzaron a desplegarse nuevas tecnologías basadas en fibra óptica, más rápidas y seguras. En la figura 1.6 se presentan algunas tecnologías que sirven de acceso hacia la red de telecomunicaciones.

Figura 1.6. Tipos de red de acceso [17].

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

Actualmente los servicios de información demandan mayor ancho de banda, para lo cual SD-WAN ofrece mejor conectividad a cada aplicación, estando preparada para un entorno multi-nube sobre redes tradicionales MPLS y la red Internet; brinda soluciones con un enfoque definido por software, determinando la mejor ruta a nivel WAN para el tráfico [18].

1.4.3.1 Características SD-WAN

Según Gartner, SD-WAN proporciona las siguientes características que se destacan para dar soluciones y que dependerá del fabricante para su implementación [19] [20].

- Soporta varias conexiones WAN como MPLS, Internet, LTE (*Long Term Evolution*).
- Permite balancear el tráfico por diferentes WAN.
- Permite auto aprovisionamiento sin intervención de personal experto en redes o seguridad durante la instalación, denominado como *Zero-Touch Provisioning*.
- Permite una administración de la red centralizada, para poder realizar cambios de forma remota sobre políticas o el manejo de las distintas WANs.
- Soporta la creación de VPNs seguras.

1.4.3.2 Arquitectura SD-WAN

Provee una base de la red siendo mucho más fácil de gestionar en comparación con las WAN tradicionales; esta arquitectura puede mover la Capa de Control a la nube y en el transcurso, facilita y centraliza la administración de la red. Este nuevo esquema separa el software del hardware, permitiendo la virtualización de la red, haciéndola más flexible [21].

1.4.3.2.1 Tipos de Arquitectura

Existen varios tipos de arquitecturas, dependiendo del proveedor de la SD-WAN: Arquitectura local, Arquitectura basada en MPLS, Arquitectura basada en Internet y Arquitectura híbrida [21].

1.4.3.3 Componentes de la arquitectura SD-WAN

Se usa una descripción basada en el fabricante Cisco. Se debe considerar que los componentes varían según la solución de la SD-WAN y la que el proveedor brinde al cliente. En la figura 1.7 se presentan los planos y componentes que son parte de la arquitectura SD-WAN.

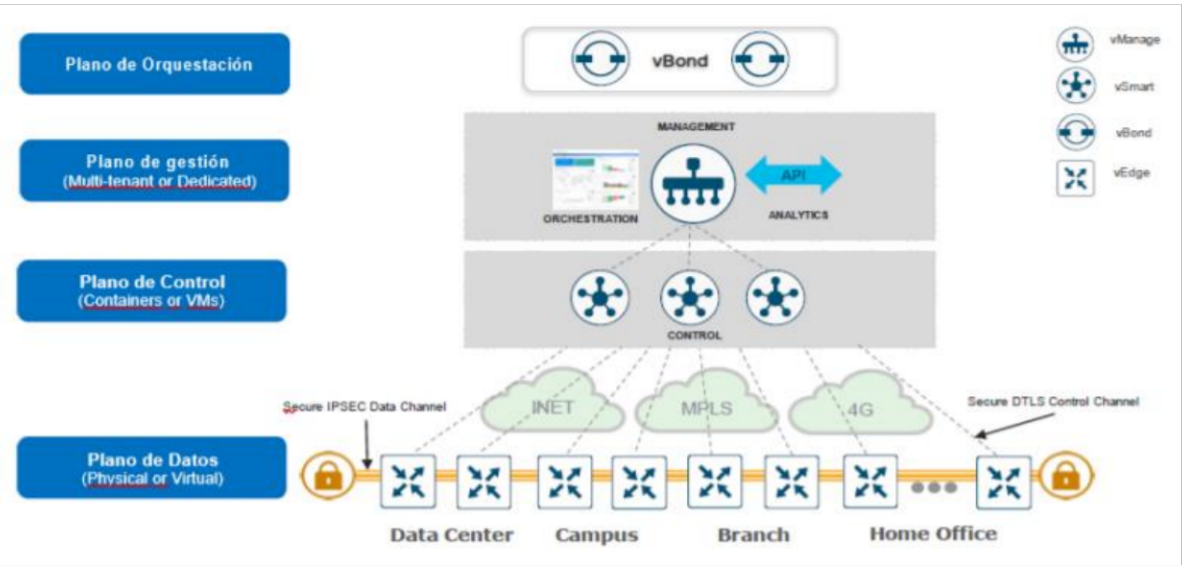


Figura 1.7. Componentes de la arquitectura SD-WAN basada en Cisco [22].

1.4.3.4 Funcionamiento de la SD-WAN

- Ofrece como una solución conectar a los usuarios desde donde se encuentre con cualquier tipo de aplicación ubicada en el Centro de Datos o la nube [23].
- SD-WAN se superpone a la red existente a través de túneles IPSec; consigue diferenciar la red física de la red lógica [23].

- SD-WAN otorga la separación del Plano de Control del Plano de Datos, generando una administración centralizada, lo que permite implementaciones rápidas *"sin intervención"*, con una administración unificada para las operaciones de red y seguridad, obteniendo una operación simplificada en el *border* de la WAN [23].
- SD-WAN a través del controlador centralizado puede establecer y conservar políticas que serán utilizadas para el control de rutas de tráfico, SLA, *failover*, monitoreo, etc [23].
- Una vez que se promueve la política, determina la ruta dinámica para que el tráfico fluya y de esa manera maximiza la funcionalidad; trabaja de tal manera que el tráfico se enrute automáticamente a través del mejor enlace disponible [23].

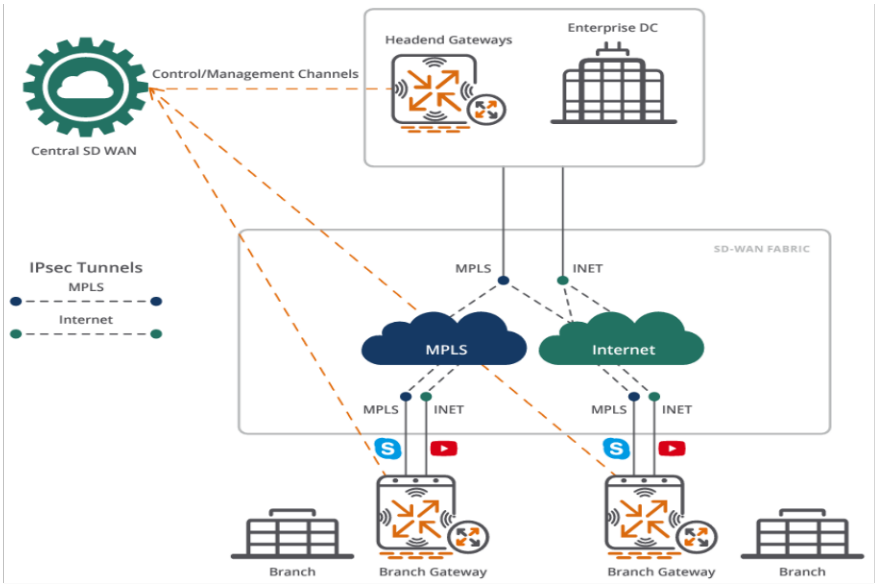


Figura 1.8. Funcionamiento de la SD-WAN [24].

1.4.3.5 Seguridad en la SD-WAN

La seguridad SD-WAN usa como componente la segmentación, permitiendo a las empresas aislar, priorizar y asignar tráfico dentro de la red de acuerdo a las necesidades y aplicaciones. El personal de TI puede colocar políticas de red para enrutar automáticamente el tráfico por el *firewall* si un usuario desconocido solicita el acceso a la red, también puede priorizar el tráfico para que viaje por un enlace específico; a esto se suma que SD-WAN proporciona seguridad a la red utilizando el protocolo IPSec para que el tráfico de la red sea autenticado [25].

1.4.3.5.1 IPSec (Internet Protocol Security)

IPSec se encuentra en el Plano de Datos de la SD-WAN; establece túneles dinámicamente entre los diferentes puntos de la red (ver Figura 1.9), proporcionando un medio seguro y

controlado de extremo a extremo a través de la VPN para el envío de datos, ocultando los saltos que da en la red, sin importar el tipo de transporte WAN que esté utilizando [26].

Las topologías lógicas que se configuran como una solución dentro de la SD-WAN, son diseñadas y anunciadas desde el Plano de Control hacia el Plano de Datos, que de forma centralizada define las políticas para la comunicación entre dispositivos; mediante las políticas establecidas se configurarán los túneles IPSec automáticamente [26].

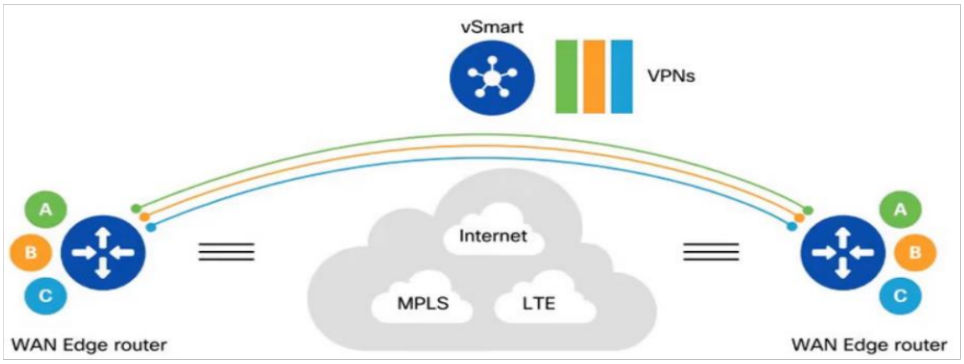


Figura 1.9. Túnel IPSec [27].

1.4.3.6 Políticas de la SD-WAN

En SD-WAN se configuran políticas centralizadas y localizadas para determinar automáticamente las rutas más eficientes para diversos tráficos entre sucursales y su Centro de Datos propio o la nube; de esta manera se busca mejorar el rendimiento a través del control de admisión, clasificación, marcado de tráfico, ancho de banda, priorización por aplicación, selección de rutas según los SLA e Ingeniería de Tráfico [22].

De acuerdo a la figura 1.10, las políticas se dividen en: políticas ***Centralizadas*** provistas a través del Plano de Control o *vSmart* y políticas ***Localizadas*** suministradas a través de los *routers* en el Plano de Datos o *vEdge*.

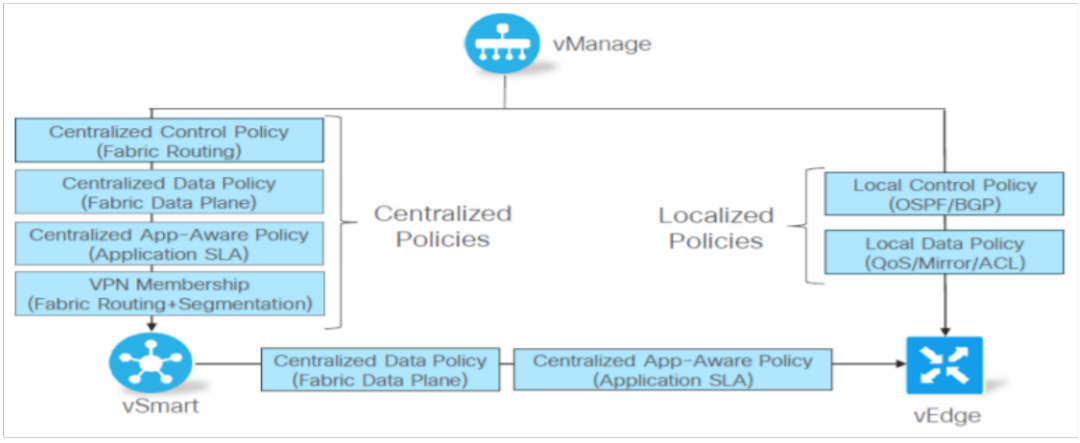


Figura 1.10. Diagrama de aplicación de políticas en SD-WAN [22].

1.4.4 VIRTUALIZACIÓN DE SERVIDORES

La virtualización viene siendo la utilización de un software que permite imitar las características de un hardware. Éstas se llaman Máquinas Virtuales VM (ver Figura 1.11), adquiriendo mayor flexibilidad, agilidad y escalabilidad, aumentando la disponibilidad y el rendimiento de los recursos; de esta manera se simplifica la administración de la infraestructura de red, reduciendo los costos de propiedad y operatividad [4].

Entre las propiedades de las Máquinas Virtuales, se tienen: Creación de particiones, Aislamiento, Encapsulamiento e Independencia con respecto al hardware [4].

Figura 1.11. Virtualización del Hardware, Máquina Virtual [28].

1.4.4.1 Servidor de correo electrónico Zimbra

Zimbra es una plataforma de mensajería y colaboración que sirve para enviar y recibir correo electrónico, agendar citas, reuniones, agregar contactos y todo lo que una plataforma de correo electrónico pueda realizar (ver Figura 1.12). Una de las ventajas de Zimbra es la implementación sobre código abierto, proporcionando mayor seguridad y sin costo de licencia. Zimbra puede trabajar desde un navegador web o ser configurado en alguna aplicación para correo [30]. En el capítulo 2 se indicará la instalación del servidor Zimbra virtualizado en VMware.

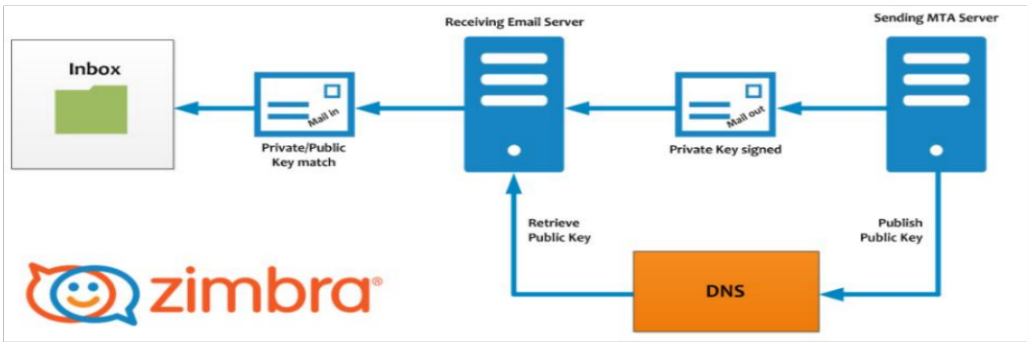


Figura 1.12. Esquema básico Servidor de Correo Zimbra [29].

1.4.4.2 Servidor DNS

Encargado de administrar nombres de dominio a través de un sistema jerárquico; dispone de una Base de Datos y un traductor, para que la búsqueda de un dominio sea más entendible y fácil de recordar, como por ejemplo *midominio.com*, en vez de la IP 172.0.0.1 [31] (ver Figura 1.13). En el capítulo 2 se indicará el procedimiento de su instalación.

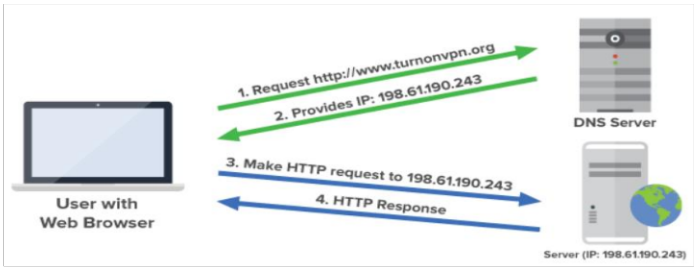


Figura 1.13. Diagrama de funcionamiento básico de un servidor DNS [32].

1.4.5 SOFTWARE PLEX MEDIA SERVER

Plex es un gestor de contenido multimedia casero, sirve para organizar contenido digital que se disponga en el computador como películas, fotos, música y cualquier archivo multimedia (ver Figura 1.14). Permite visualizar todo el contenido multimedia en cualquier dispositivo, manteniendo actualizada siempre la información y recordando el punto exacto en el tiempo en que se deja de ver o escuchar una película o canción respectivamente [33].

En base a esta aplicación, se puede crear un servidor parecido a Netflix, con contenido multimedia propio y acceso directo al archivo raíz del ordenador. También permite conectarse a otros canales como TED, *Comedy Central o SoundCloud* privados [34]. Plex es una aplicación cliente-servidor que está constituida de dos partes: Servidor Plex y Cliente Plex [33].

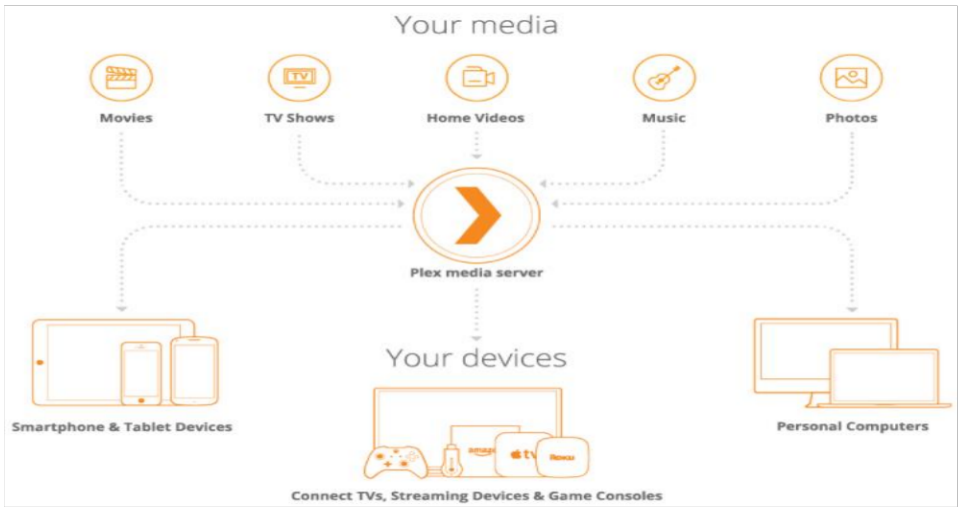


Figura 1.14. Conexión cliente–servidor de Plex [34].

1.4.6 FORTINET

Fortinet es una empresa líder mundial e innovadora en seguridad de redes, que brinda soluciones de alto rendimiento a través de sus productos de seguridad para un sinnúmero de empresas a nivel mundial. [35].

1.4.6.1 Secure SD-WAN

La innovación digital, las aplicaciones y herramientas en la nube, cada vez se vuelven más críticas para las empresas. Secure SD-WAN tiene como estrategia impulsar la seguridad que ofrece Fortinet con la infraestructura de red y la arquitectura de seguridad de una empresa, permitiendo flexibilidad y escalabilidad al incorporar nuevos sitios sin comprometer la seguridad. Fortinet combina un *firewall* de próxima generación con las funcionalidades avanzadas de SD-WAN [36].

1.4.6.2 FortiOS

FortiOS es un sistema operativo de seguridad multicapa que se ejecuta sobre dispositivos Fortinet empleando una versión modificada del núcleo Linux, es la base del Fortinet Security Fabric [37]. FortiOS ofrece una estrategia impulsada por la seguridad, logrando asegurar y acelerar la red, garantizando una buena experiencia al usuario mediante la innovación y mejoras que garantiza la optimización de aplicaciones en tiempo real, protección y prevención avanzada en los *firewalls* de próxima generación, también una integración y automatización efectiva en la nube [36].

1.4.6.3 FortiGate

Los FortiGate conocidos también como *firewall* de próxima generación *NGFW*, son dispositivos de seguridad, que permiten implementar redes seguras y una protección amplia, integrada y automatizada contra amenazas [38].

Los FortiGate son muy utilizados por su rendimiento y por su eficiencia en la seguridad. Cumplen con las características de *Secure* SD-WAN, tales como: Control de aplicaciones, Visibilidad completa, Protección contra amenazas, Filtrado de URL y Antivirus entre otras.

Los FortiGate a más de ser un *firewall*, también tienen la capacidad de SD-WAN, lo cual permite al cliente reducir la latencia y aumentar el rendimiento de las aplicaciones, ya que puede priorizar el tráfico crítico dependiendo de las necesidades de una empresa.

Algo muy importante que ofrece FortiGate, es la VPN IPSec, con lo cual asegura el rendimiento de las aplicaciones a través de la SD-WAN, brindando seguridad en la información [38].

1.4.6.4 FortiManager

Proporciona una gestión centralizada, automatizando los dispositivos Fortinet a través de una única consola, logrando una administración y visibilidad completa de sus dispositivos en toda la red [39]. Las características de FortiManager sobre los dispositivos FortiGate, permiten visualizar similitudes en cuanto a configuraciones y el aprovechamiento de sus funcionalidades (ver figura 1.15). Entre sus principales características se tienen: Gestión de consola única, Gestión centralizada de políticas y dispositivos, *Zero-Touch Provisioning*, Aprovisionamiento y monitoreo de Secure SD-WAN, Multitenencia y Dominios administrativos (ADOM) y Alta disponibilidad de Grado Empresarial [40]

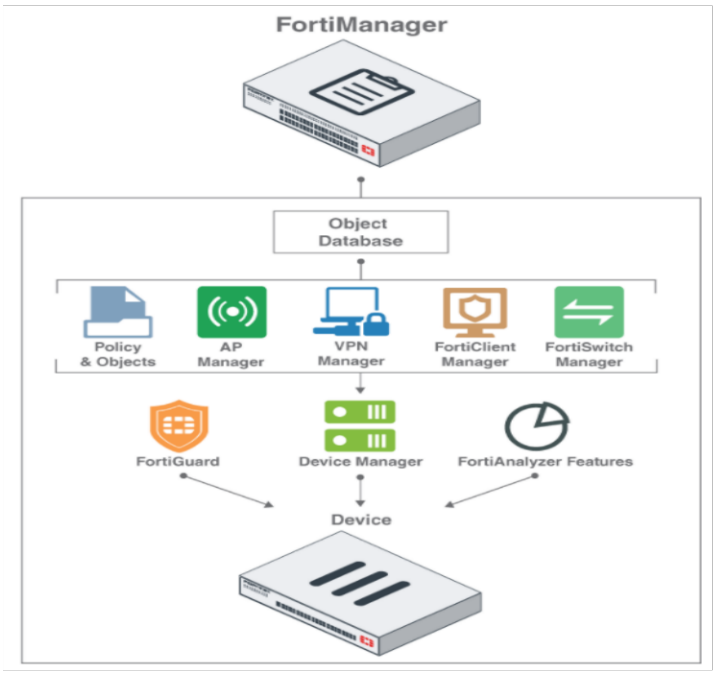


Figura 1.15. Funcionalidades de FortiManager [41].

2 METODOLOGÍA

En este capítulo se presenta el diseño e implementación del prototipo, para lo cual se especifican los requerimientos y características técnicas de los elementos a utilizar, para ser configurados en equipos físicos, en cada una de las redes propuestas.

2.1 REQUERIMIENTOS DEL PROTOTIPO

Se desarrolla una SD-WAN híbrida, con una WAN MPLS y una WAN de acceso a Internet, que interconecta tres sitios. En la Sede Central Quito se incorpora un servidor de correo electrónico y un servidor DNS; en la sede Ibarra se incorpora un servidor multimedia; y Guayaquil se incorpora solo como sucursal; cada sitio dispone una LAN de usuarios. Con la incorporación de la SD-WAN de Fortinet, se tiene conectividad entre LANs, acceso a los servicios por túneles IPSec a través de la WAN MPLS o de Internet; cada sitio tiene su propia salida a Internet, pudiendo también salir por la Sede Central, logrando redundancia, y mejor administración y direccionamiento del tráfico mediante políticas o reglas. También se incluyen políticas de seguridad que brindan los *firewalls* FortiGate. Se tendrá acceso remoto a los servicios a través de una VPN-SSL (*Virtual Private Network – Secure Sockets Layer*) configurada en la Sede Central Quito y lo más importante, se administrará la red de forma centralizada desde FortiManager.

Para la implementación de la WAN MPLS en hardware, se dispone de equipos Cisco ISR C2811. Para acceder al Internet se dispone de un equipo Cisco ISR C1111 que actúa como *switch* para obtener las IPs públicas desde el PE de borde de Puntonet, donde se encuentra la IP de *Gateway* de la subred /29; el software utilizado en ambas redes es Cisco IOS.

Para la funcionalidad de la SD-WAN se dispone de equipos hardware FortiGate 60F para la Sede Central en Quito; para las sedes de Ibarra y Guayaquil se dispone de FortiGate 40F; estos equipos harán la función directa como CEs en cada uno de los sitios. La versión del software FortiOS es v6.4.8, que permitirá implementar y configurar las funcionalidades SD-WAN. Para los dos modelos de equipos FortiGate, no existen diferencias en cuanto al software, la diferencia radica en el hardware, en el número de puertos WAN y LAN, que se incrementa en los FortiGate 60F.

Adicionalmente se implementan servicios de datos y video sobre 2 servidores, con memoria RAM de 4 GB, core i3 de 64 bits, con puerto Ethernet y sistema Operativo Windows 10. En el primero se instala VMware para virtualizar los servidores de correo y DNS; mientras que en el segundo se instala el software Plex Media Server para levantar el servidor multimedia.

Finalmente, para el control centralizado de la SD-WAN, se incorpora FortiManager, localizado en la nube del proveedor Puntonet; se creará un ADOM (*Administrative Domains*) personalizado para la administración de los equipos FortiGate.

2.2 DISEÑO DE LA RED MPLS

2.2.1 TOPOLOGÍA DE RED MPLS

La MPLS será la red principal, estará conformada por cuatro *routers* Cisco 2811, tres de ellos como *routers* PE para acceder a la nube MPLS interconectados a través de un *router* P de *Core* en una topología tipo estrella. Cada *router* PE se conectará a un *firewall* FortiGate en cada una de las tres sedes. En la figura 2.1, se describe la topología física y lógica de la red, la cual detalla los equipos, su distribución, conexiones e interfaces utilizados en cada *router*.

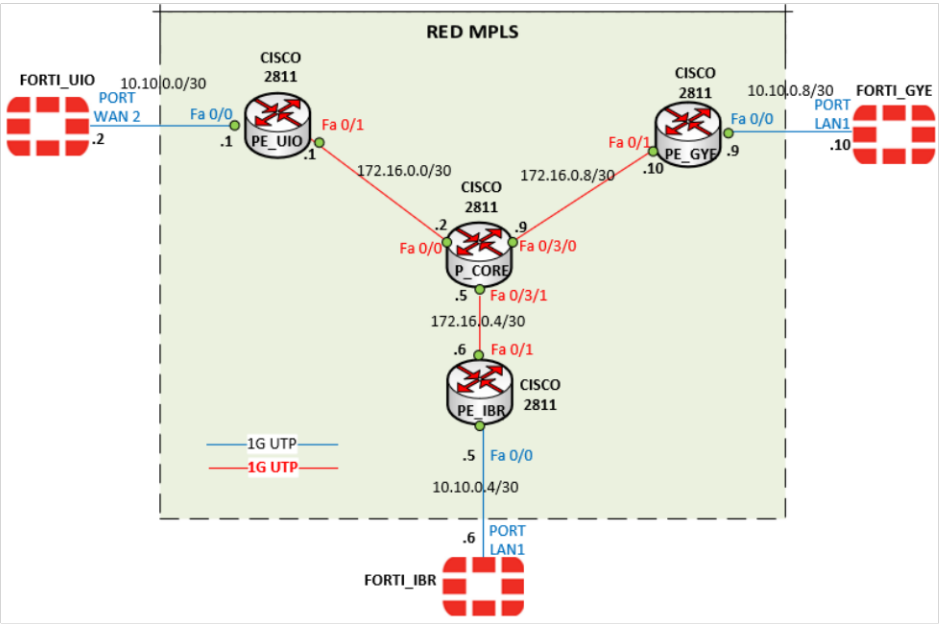


Figura 2.1. Topología física y lógica de la red MPLS.

2.2.2 DIRECCIONAMIENTO DE LA RED MPLS

Para el direccionamiento de la red se utiliza una subred privada de clase B (172.16.0.x), que permita establecer las conexiones punto a punto entre los *routers* de la nube MPLS; dicho direccionamiento se detalla en la Tabla 2.1.

Tabla 2.1. Direccionamiento IP de la red MPLS.

WAN	RED	IP_INICIAL	IP_FINAL	Máscara
PE_UIO – P_CORE	172.16.0.0/30	172.16.0.1	172.16.0.2	255.255.255.252
PE_IBR – P_CORE	172.16.0.4/30	172.16.0.6	172.16.0.5	255.255.255.252
PE_GYE – P_CORE	172.16.0.8/30	172.16.0.10	172.16.0.9	255.255.255.252

Adicionalmente, en cada *router* de la nube MPLS, se configura una interfaz lógica de *Loopback*, la misma que servirá como identificador para cada *router*, permitiendo asociar esta interfaz a los procesos OSPF (*Open Shortest Path First*) y BGP (*Border Gateway Protocol*), asegurando que no se pierdan las sesiones por algún inconveniente en las interfaces físicas. Para el direccionamiento *Loopback* se hace uso de direcciones privadas clase A, las mismas que se detallan en la tabla 2.2.

Tabla 2.2. Direccionamiento IP Interfaces *Loopback*.

HOSTNAME	INTERFACES	DIRECCIÓN IP	Máscara
PE_UIO	Loopback0	1.1.1.1/32	255.255.255.255
PE_IBR	Loopback0	2.2.2.2/32	255.255.255.255
PE_GYE	Loopback0	3.3.3.3/32	255.255.255.255
P_CORE	Loopback0	4.4.4.4/32	255.255.255.255

El intercambio de datos de los clientes en la nube MPLS se realiza en función de la conmutación de etiquetas soportando cualquier tipo de tráfico, generando un túnel unidireccional entre un par de *routers* PE o como se lo conoce como una ruta conmutada por etiquetas LSP (*Label Switched Path*) predeterminada. Las etiquetas LSP externas se conocen a través del protocolo LDP (*Label Distribution Protocol*) [42].

Para establecer la adyacencia BGP, los *routers* PE y P utilizan el protocolo de enrutamiento interior OSPF, determinando el camino más corto primero mediante un algoritmo de tipo estado de enlace e intercambiando la información sobre la topología de la red [42].

Si en un futuro se desea implementar más servicios en la nube MPLS, generando varias tablas de enrutamiento en lugar de utilizar una solo tabla de enrutamiento global en los routers PE, se utilizará VRF (*Virtual Routing and Forwarding*) que permitirá separar el tráfico; con esto cada cliente podrá utilizar una VRF diferente. Se utilizará MP-BGP (MultiProtocol - *Border Gateway Protocol*) para compartir la información de las VRF entre los *routers* PE; en el presente caso se utilizará la ***vrf datos*** [42].

MP-BGP es una extensión de BGP que admite familias de direcciones IPv4 e IPv6 y sus variantes de unidifusión y multidifusión; se utilizará para la distribución de prefijos de los clientes, separando el direccionamiento de cada cliente mediante la creación de rutas VPNv4 únicas dentro de la red MPLS [43].

A través de la combinación de VRF, MPLS y MP-BGP, se puede garantizar que el tráfico de una VPNv4 no se filtre a otra VPNv4, aprovechando de esta manera un mismo direccionamiento de IP privadas para cada sitio de VPNv4. Los *routers* PE traducen las IPs

a VPNv4, mantienen las rutas VPNv4, así solo necesitan conocer las rutas para las VPNv4 que tienen los sitios adjuntos en cada PE [43].

2.2.3 EQUIPO CISCO 2811

Para la implementación de la red MPLS se dispone de equipos Cisco 2811 de la Serie ISR, estos equipos permiten obtener la función de P y PE. En la tabla 2.3 se indican algunas características del equipo, el detalle completo se puede visualizar en el Anexo I.

Tabla 2.3. Especificaciones Router Cisco 2811.

ESPECIFICACIONES	
Algoritmos de cifrado	DES, Triple DES, SSL 3.0, 128-bit AES, 192-bit AES, 256-bit AES
Interfaces	USB: 2 x
	2 x 10Base-T/100Base-TX - RJ-45
	Management: 1 x console - RJ-45
	Serial: 1 x auxiliary - RJ-45
Slots de Expansión	4 (total) / 4 (free) x HWIC
	1 (total) / 1 (free) x NME
	2 (total) / 2 (free) x AIM
	2 (total) / 2 (free) x PVDM - SIMM 80-PIN
	2 memory
	1 (total) / 0 (free) x CompactFlash Card
Sistema Operativo	Cisco IOS IP Base
Estándares	IEEE 802.3af, IEEE 802.1x
Memorias DRAM, Flash	512 MB (instalada), 128 MB (instalada)
Características	Modular design, firewall protection, hardware encryption, VPN support, MPLS support, wall mountable, Quality of Service (QoS), PoE.
Protocolo Red/Transporte	IPSec

2.3 DISEÑO DE LA RED DE ACCESO A INTERNET

2.3.1 TOPOLOGÍA DE RED DE ACCESO A INTERNET

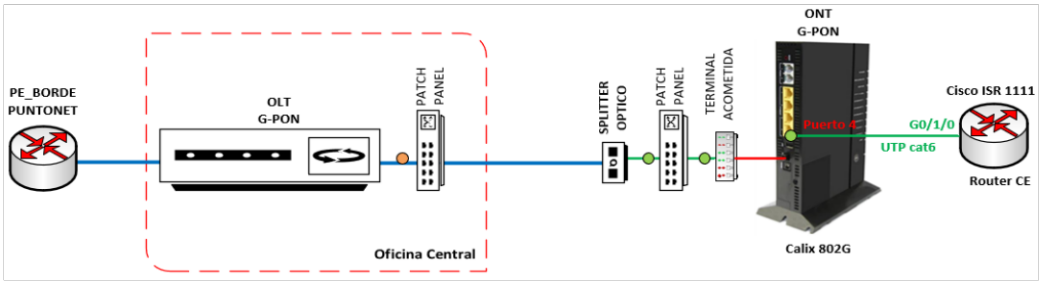


Figura 2.2. Red de acceso G-PON.

Para que cada sitio tenga acceso a Internet, en la práctica, se debe colocar su propia última milla con su *router* CE y conectar al FortiGate; en el presente proyecto, para acceder al PE de Puntonet, se utiliza una sola última milla de fibra G-PON interconectando el OLT a un

ONT de marca Calix 802G de cuatro puertos mostrado en la figura 2.2; desde el puerto cuatro se conecta con cable UTPcat6 a un *router* Cisco ISR C1111 como CE, que actuará en modo *switch* para la distribución de IPs públicas y se conectará a cada FortiGate en cada sitio.

En la figura 2.3 se muestra la configuración de la VLAN 281 que se aplica en el equipo Calix y es la misma que se configura en el PE de Puntonet, dicha configuración se explica más adelante en el apartado 2.7.2.

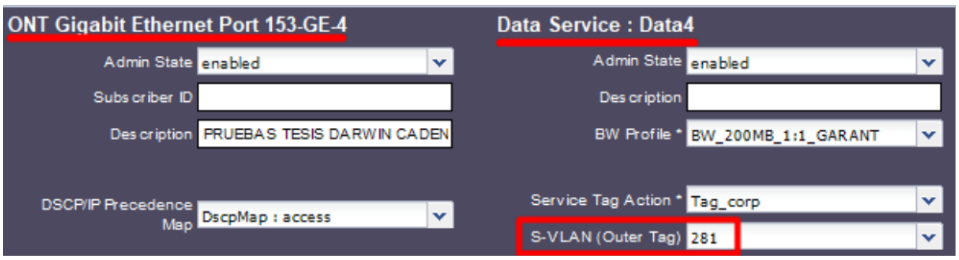


Figura 2.3. VLAN configurada en el ONT Calix.

La figura 2.4 muestra la topología física y lógica de la red de acceso a Internet, así como las conexiones de las interfaces entre el equipo CE y los *firewalls* FortiGate.

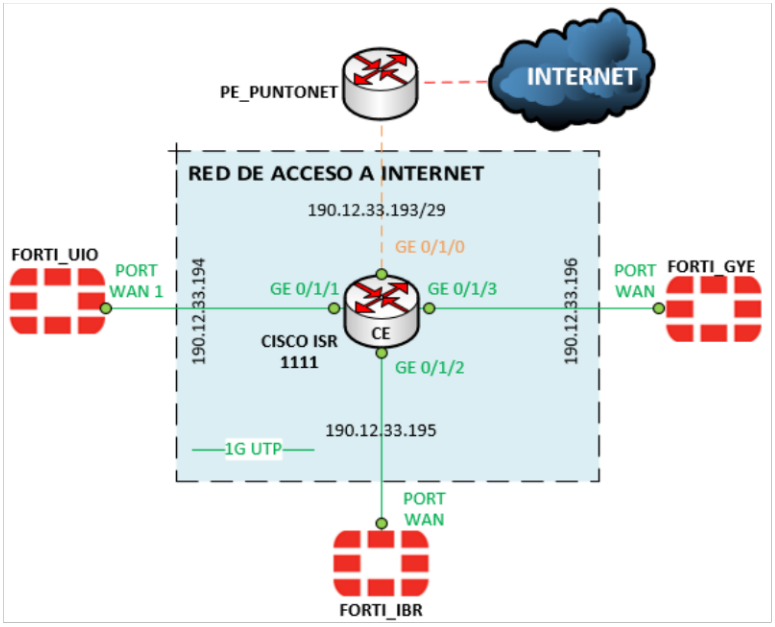


Figura 2.4. Topología física y lógica red de Acceso a Internet.

2.3.2 DIRECCIONAMIENTO DE LA RED DE ACCESO A INTERNET

El direccionamiento considera una subred pública clase B con máscara /29, que permite obtener 5 IPs públicas, de las cuales se utilizarán 3 IPs, una para cada sitio; la distribución de IPs se muestran en la tabla 2.4.

Tabla 2.4. Direccionamiento de IPs Públicas.

HOSTNAME	RED IP 190.12.33.192/29	MÁSCARA
GATEWAY PE_PUNTONET	190.12.33.193	255.255.255.248
FORTI_UIO	190.12.33.194	255.255.255.248
FORTI_IBR	190.12.33.195	255.255.255.248
FORTI_GYE	190.12.33.196	255.255.255.248

2.3.3 EQUIPO CISCO ISR 1111

Para la implementación de la red de Internet, se dispone de un equipo cisco ISR C1111 de 8 puertos, que es utilizado como *switch* para la distribución de IPs públicas. En la tabla 2.5 se indican algunas de sus especificaciones, su detalle se encuentra en el Anexo I.

Tabla 2.5. Especificaciones Router Cisco ISR C1111.

ESPECIFICACIONES	
10/100/1000 Gigabit Ethernet	Two GE ports allocated among RJ45 and SFP as: One combo port with 10/100/1000RJ-45 Ethernet port or SFP Ethernet port (labeled GE0/0/0). One dedicated 10/100/1000RJ-45 Ethernet port (labeled GE0/0/1)
Wireless VLANs	32 (encrypted and non-encrypted VLANs)
Default and maximum DRAM **Default and maximum flash**	4GB 4GB
LAN GE **PoE** **PoE+**	8 Port 4 Port 2 Port
Inline PoE	4 ports for -8P PIDs, 2 ports for -4P PIDs, 802.3af-compliant PoE or 802.3at-compliant PoE+

2.4 DISEÑO DE LA LAN

Dentro del diseño se consideran las LANs y el rol que cumplirán en cada uno de los 3 sitios, así como la distribución y segmentación de cada uno de los equipos y dispositivos internos.

2.4.1 TOPOLOGÍA DE LA LAN

Para las LAN, se consideran dos subredes tanto para Quito e Ibarra; una subred para los servidores y otra para los usuarios, de esta manera si un atacante, accede al servidor de correo, no lo hará a la LAN de usuarios y viceversa. Para la sucursal de Guayaquil se tiene solo una LAN para usuarios. Las pruebas harán uso de una PC para cada LAN de clientes, en cada una de las 3 sedes.

2.4.1.1 LAN Quito

Esta LAN cumplirá un rol como el de un Centro de Datos, en donde se procesa, almacena y difunde la información; será donde se concentra la mayor parte de las funciones y configuraciones, por lo que será considerado como un concentrador para la red MPLS.

En la LAN de Quito se configuran dos VLAN; por disponibilidad de equipos, se distribuye a través de un *router* Cisco ISR C1111 cumpliendo la función de *switch* de acceso (ver figura 2.5). En la LAN se tiene que: la VLAN 100 está relacionada al servidor de correo Zimbra, permitiendo el acceso al servicio desde cualquier LAN, dentro de la Sede Central o desde las sucursales; la VLAN 10 es para los usuarios, permite la comunicación con las demás sucursales y el acceso a los servidores: DNS, correo y multimedia, o salir al Internet.

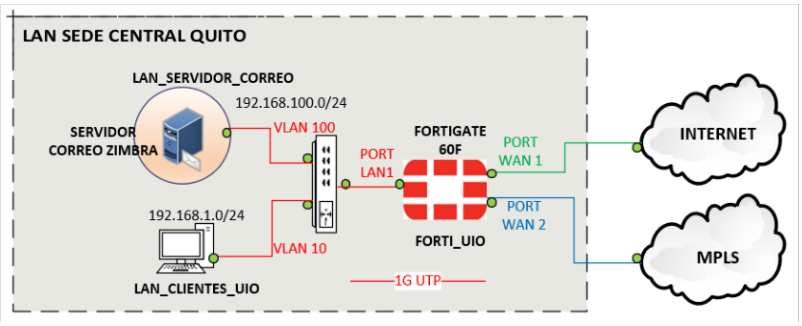


Figura 2.5. Topología LAN Quito.

2.4.1.2 LAN Ibarra

Esta LAN es muy similar a la de Quito. Para la distribución de VLANs se dispone de un *Router* Cisco ISR C1111 en modo *switch* de acceso (ver figura 2.6). En esta LAN se tiene que: la VLAN 200 es para la LAN del servidor multimedia, y a ella podrán acceder todas las LAN del proyecto; la VLAN 2 es para usuarios, para que accedan tanto a los servicios de correo y multimedia, tengan conectividad entre LANs y puedan navegar por el Internet.

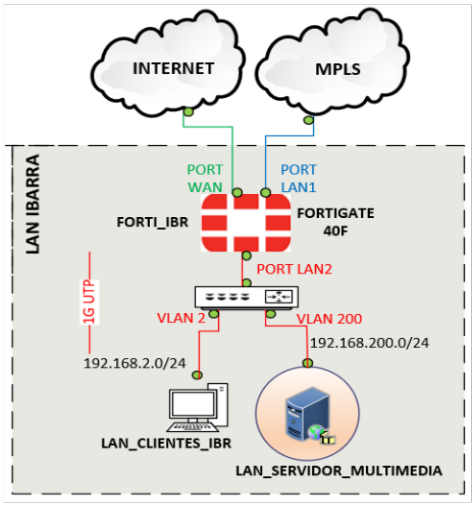


Figura 2.6. Topología LAN Ibarra.

2.4.1.3 LAN Guayaquil

En esta LAN, igualmente se dispone de un Cisco ISR C1111 como *switch* de acceso (ver Figura 2.7). Su rol será de una sucursal con funcionalidades mínimas y sin servidores; sólo

permitirá el acceso a los servicios de correo, multimedia, navegación por el Internet y comunicación entre LANs; para este punto se asigna la VLAN 30.

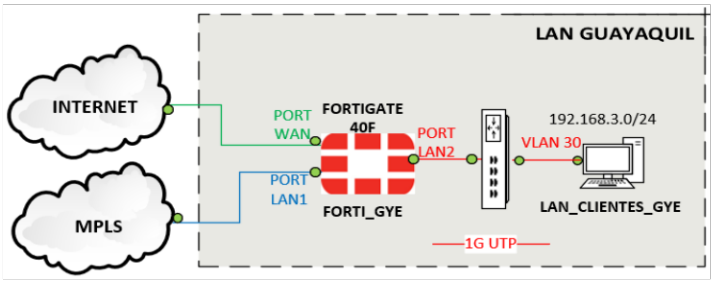


Figura 2.7. Topología LAN Guayaquil.

2.4.1.4 Direccionamiento LAN

Para el direccionamiento de cada sitio se utilizarán subredes privadas clase C (192.168.x.x), considerando escalabilidad a la red y que permita establecer la comunicación entre los servidores locales, entre LANs de los diferentes sitios a través de la red MPLS o la red Internet. El direccionamiento se detalla en la tabla 2.6.

Tabla 2.6. Direccionamiento IP de las redes LAN usuarios.

CIUDAD	LAN	VLAN	RED	IP_INICIAL (GATEWAY)	IP_FINAL
QUITO	LAN_CLIENTES	10	192.168.1.0/24	192.168.1.1	192.168.1.254
	LAN_ZIMBRA (SERVIDOR-ZIMBRA)	100	192.168.100.0/24	192.168.100.1	192.168.100.254
IBARRA	LAN_CLIENTES	2	192.168.2.0/24	192.168.2.1	192.168.2.254
	LAN_MULTIMEDIA (SERVIDOR-MULTIM)	200	192.168.200.0/24	192.168.200.1	192.168.200.254
GUAYAQUIL	LAN_CLIENTES	30	192.168.3.0/24	192.168.3.1	192.168.3.254

2.5 SERVIDORES

En esta sección se indica la funcionalidad de los servidores de la LAN de Quito y la LAN de Ibarra. Cada LAN de usuarios y usuarios remotos tendrá acceso a los servidores DNS, Correo electrónico y Multimedia. Los servidores serán implementados sobre un hardware y ejecutados a través de un software, obteniendo los servicios deseados.

2.5.1 SERVIDOR DNS

Se encuentra alojado en la VLAN 100 de la LAN en la Sede Central, implementado en el sistema operativo Ubuntu 16.04 LTS, el cual está instalado en una máquina virtual y virtualizado en VMware. Dentro de la distribución de Ubuntu, se utiliza el paquete *dnsmasq*, compatible con IPv4 o IPv6; se busca contar con una base de datos con los nombres de los dominios al utilizar un servidor DNS. Su función es facilitar el recordar un nombre o

dominio, en el presente caso ***sch.com***, en vez de una IP 192.168.100.100, IP asociada al servidor de correo y DNS. La instalación del servidor DNS se detalla en el Anexo II.

2.5.2 SERVIDOR DE CORREO ZIMBRA

Este servidor se instala en la misma máquina virtual donde está el servidor DNS en la LAN de Quito, de esta manera interactúan utilizando un modelo cliente-servidor, accediendo al buzón de correo mediante un navegador o una aplicación para *email*, digitando la IP 192.168.100.100 o mediante el dominio https://mail.sch.com (ver Figura 2.8). Se accederá a los servicios de correo en la Intranet para enviar/recibir correos, que permanecerán almacenados en la base de datos del servidor Zimbra. Para enviar los correos se utiliza el protocolo SMTP (*Simple Mail Transfer Protocol*) y para recibir o almacenarlos se utiliza los protocolos IMAP (*Internet Message Access Protocol*) o POP3 (*Post Office Protocol versión 3*). La implementación y acceso del servidor Zimbra se detalla en el Anexo II.

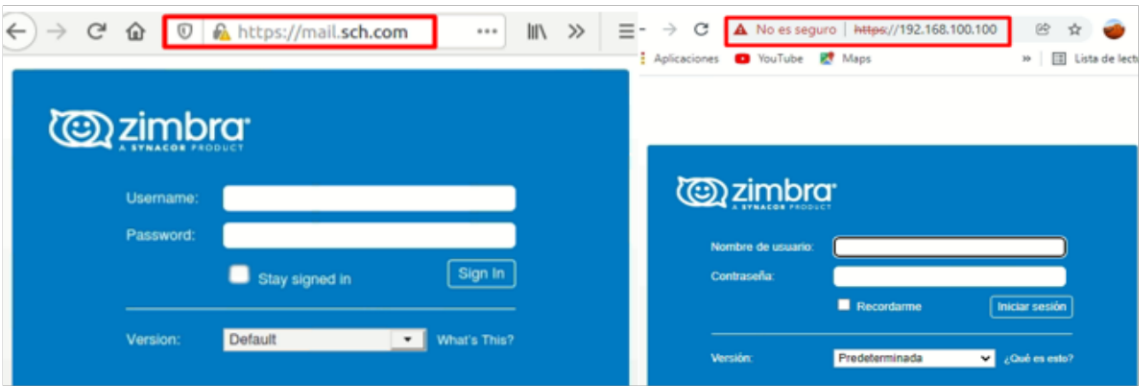


Figura 2.8. Interfaz Web Correo Zimbra.

2.5.3 PLEX MEDIA SERVER

Se encuentra alojando en la VLAN 200 de la LAN de Ibarra, en un hardware con sistema operativo Windows 10. Se instala el software en el ordenador para utilizarlo como servidor multimedia con contenido como video, audio o imágenes; la interfaz gráfica será por Web, utiliza un modelo Cliente-Servidor, se puede acceder al contenido por cualquier dispositivo siempre y cuando esté conectado a la Intranet; tanto el servidor como el cliente pueden ser descargados de la página oficial de Plex. La instalación y acceso se detalla en el Anexo II.

2.6 DISEÑO SD-WAN

2.6.1 TOPOLOGÍA SD-WAN

Una SD-WAN funciona con al menos dos WAN; en este proyecto se utiliza una MPLS y una red de acceso a Internet. Sus topologías fueron ya detalladas anteriormente; en la figura 2.9 se describe la topología de la SD-WAN, las interfaces en las que se conectan las

WAN a los *firewalls* FortiGate, las conexiones a nivel de la LAN en cada punto. Más adelante se explicará el funcionamiento de la SD-WAN, como sus reglas, políticas de la SD-WAN, perfiles de seguridad, túnel IPSec, VPN SSL, entre otros.; a modo de ejemplo en la topología se grafican los túneles IPSec creados en los FortiGate a nivel de la WAN de Internet y la MPLS entre Quito y Guayaquil, y la VPN SSL para acceso remoto.

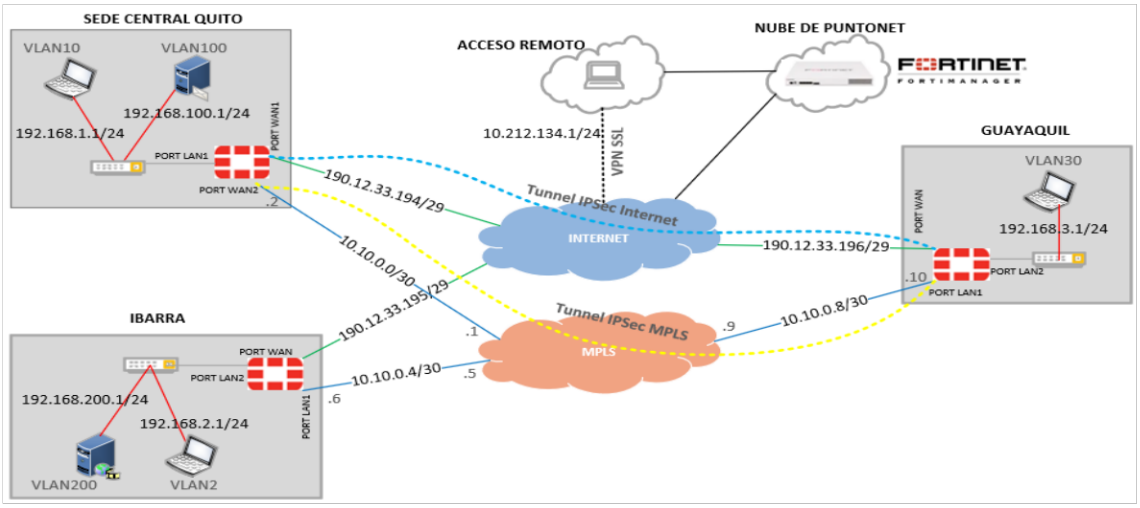


Figura 2.9. Topología de la SD-WAN Híbrida.

2.6.2 DIRECCIONAMIENTO SD-WAN

Para la configuración de la SD-WAN, en el presente caso, no se requiere de protocolos de enrutamiento entre la WAN y el FortiGate, solo se configura la IP asociada a la interfaz física y la IP de *Gateway*, así como las VLANs para cada subred LAN y los túneles IPSec. En la tabla 2.7 se detallan las IPs e interfaces asociadas a cada WAN y LAN. Adicionalmente en la tabla 2.8 se detalla el direccionamiento para los túneles IPSec.

Tabla 2.7. Direccionamiento SD-WAN.

CUIDAD	LAN/WAN	INTERFAZ FORTIGATE	RED	IP ASIGNADA	IP GATEWAY
QUITO	WAN_INTERNET	WAN1	190.12.33.192/29	190.12.33.194	190.12.33.193
	WAN_MPLS	WAN2	10.10.0.0/30	10.10.0.2	10.10.0.1
	LAN_ZIMBRA	LAN1	192.168.100.0/24	192.168.100.100	192.168.100.1
	LAN_CLIENTE	LAN1	192.168.1.0/24	192.168.1.200	192.168.1.1
IBARRA	WAN_INTERNET	WAN	190.12.33.192/29	190.12.33.195	190.12.33.193
	WAN_MPLS	LAN1	10.10.0.4/30	10.10.0.6	10.10.0.5
	LAN_MULTIMEDIA	LAN2	192.168.200.0/24	192.168.200.200	192.168.200.1
	LAN_CLIENTE	LAN2	192.168.2.0/24	192.168.2.200	192.168.2.1
GUAYAQUIL	WAN_INTERNET	WAN	190.12.33.192/29	190.12.33.196	190.12.33.193
	WAN_MPLS	LAN1	10.10.0.8/30	10.10.0.10	10.10.0.9
	LAN_CLIENTE	LAN2	192.168.3.0/24	192.168.3.200	192.168.3.1
VPN_SSL	LAN_REMOTA	--	10.212.134.0/24	10.212.134.200	10.212.134.1

Tabla 2.8. Direccionamiento Túneles IPSec.

TÚNEL IPSec	DIRECCIÓN IP INICIO	DIRECCIÓN IP FINAL
ToUIO_MPLS – ToIBR_MPLS	10.20.0.1/32	10.20.0.2/32
ToUIO_INTER – ToIBR_INTER	10.20.0.3/32	10.20.0.4/32
ToUIO_MPLS – ToGYE_MPLS	10.20.0.5/32	10.20.0.6/32
ToUIO_INTER – ToGYE_INTER	10.20.0.7/32	10.20.0.8/32
ToIBR_MPLS – ToGYE_MPLS	10.20.0.9/32	10.20.0.10/32
ToIBR_INTER – ToGYE_INTER	10.20.0.11/32	10.20.0.12/32

2.6.3 EQUIPOS FORTIGATE

Para la SD-WAN se dispone equipos *firewall* FortiGate de la serie 60F para la Sede Central Quito, en donde se realizan la mayoría de funciones de la SD-WAN, y equipos de la serie 40F para las sedes de Ibarra y Guayaquil. En la tabla 2.9 se detallan las especificaciones principales de los equipos, el detalle completo se encuentra en el Anexo I.

Tabla 2.9. Especificaciones FortiGate 60F y 40F.

ESPECIFICACIONES		
	FORTIGATE 60F	**FORTIGATE 40F**
GE RJ45 WAN / DMZ Ports	2 Port	1 Port
GE RJ45 Internal Ports	5 Port	3 Port
IPS Throughput	1,4 Gbps	1 Gbps
NGFW Throughput	1 Gbps	800 Mbps
Threat Protection Throughput	700 Mbps	600 Mbps
Firewall Throughput (1518 / 512 / 64-byte UDP packets)	10/10/6 Gbps	5/5/5 Gbps
Firewall Latency (64-byte UDP packets)	3,3 us	2,97 us
Firewall Throughput (Packets Per Second)	9 Mbps	7,5 Mbps
Concurrent Sessions (TCP)	700000	700000
Firewall Policies	5000	5000
IPsec VPN Throughput (512 byte)	6,5 Gbps	4,4 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200
SSL-VPN Throughput	900 Mbps	490 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	200
SSL Inspection Throughput (IPS, avg. HTTPS)	630 Mbps	310 Mbps
SSL Inspection Concurrent Session (IPS, avg. HTTPS)	55000	55000
Application Control Throughput (HTTP 64K)	1,8 Gbps	990 Mbps

2.6.4 FUNCIONAMIENTO DE LA SD-WAN

En esta sección se explica el funcionamiento de la SD-WAN, sus políticas y objetos, reglas de la SD-WAN, políticas de seguridad, SLA, túneles IPSec, VPN SSL, su administración, entre otros; esta sección es fundamental para el entendimiento de la SD-WAN.

2.6.4.1 Enlaces SD-WAN

Los enlaces de la MPLS y del Acceso a Internet son similares en todos los puntos del proyecto formando parte de la SD-WAN, al igual que los túneles IPSec creados a nivel MPLS y de Internet, excepto la VPN SSL que sirve para el acceso remoto a la Intranet. En la figura 2.10 se muestra los enlaces que pertenecen a la SD-WAN en la Sede Central Quito, con el objetivo de permitir que las redes de Quito, Ibarra y Guayaquil interactúen entre sí. El detalle de los enlaces de Ibarra y Guayaquil se encuentran en el Anexo III.

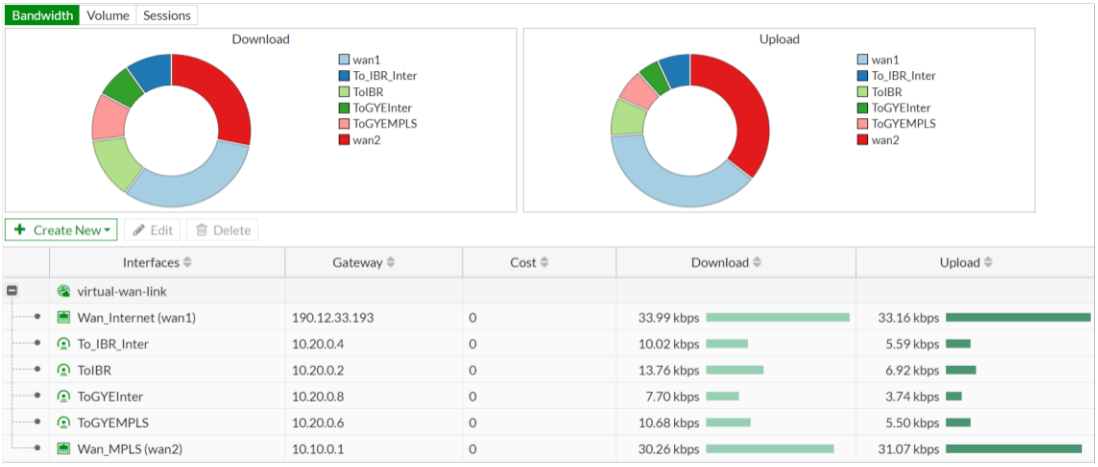


Figura 2.10. Enlaces SD-WAN Sede Central Quito.

2.6.4.2 Rutas Estáticas

Una vez agregados los enlaces SD-WAN se establece la ruta estática por defecto 0.0.0.0/0, que permite alcanzar la red Internet o la red MPLS; sin embargo, solo con esta ruta no se puede navegar por la red, por lo que también es importante definir políticas para determinar los puertos por donde ingresa y sale el tráfico, así como las subredes de origen y destino. Adicionalmente, se deben definir las rutas para alcanzar las IPs de las WAN y de los túneles IPSec destino, definiendo la Interfaz de salida y la IP *Gateway* de la WAN asociada; en la figura 2.11 se muestra el detalle de la Sede Central Quito. Los puntos de Ibarra y Guayaquil son similares y se especifican en el Anexo III.

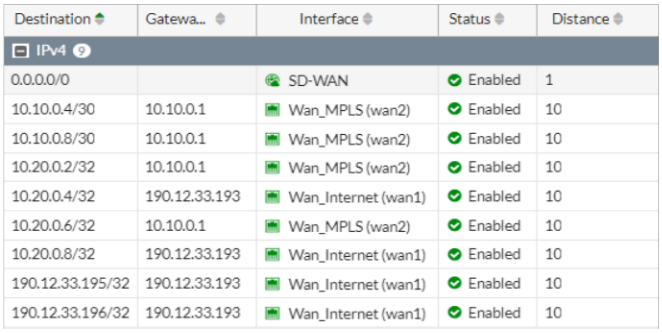


Figura 2.11. Rutas estáticas Sede Central Quito.

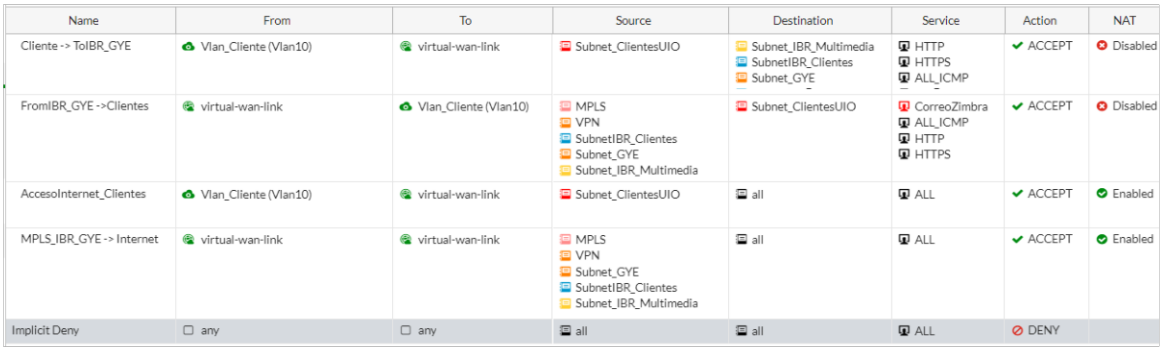
2.6.4.3 Políticas y Objetos

Para poder explicar las políticas y los objetos, se debe indicar que Fortinet llama ***objetos*** a las subredes IPs o rango de IP que intervienen en las políticas. Para poder dar salida o no al tráfico y su dirección, se definen políticas y objetos. Se toma como ejemplo la Sede Central Quito, aquí se definen 11 políticas; para que cada política sea considerada, se debe colocar en orden jerárquico de forma descendente, que irá cumpliendo primero con la política que tiene en la parte superior hasta llegar a la última en la parte inferior.

Como ejemplo se citarán cinco de las políticas para explicar su funcionamiento. La política ***Cliente -> ToIBR_GYE*** define como puerto de entrada la *Vlan_Cliente(VLAN10)* y como salida la *SD-WAN*, la subred de origen corresponde a la *Subnet_ClienteUIO* y las subredes de destino *Subnet_IBR_Multimedia, SubnetIBR_Clientes y Subnet_GYE*. Esta política permite que la Sede Principal Quito tenga conectividad con los puntos de Ibarra y Guayaquil de forma unidireccional. Para poder tener conectividad en el sentido contrario se establece la política ***FromIBR_GYE ->Clientes*** en donde el puerto de entrada es la *SD-WAN* y el puerto de salida la *Vlan_Cliente(VLAN10)*, las subredes de origen corresponden a *MPLS, VPN, SubnetIBR_Clientes, Subnet_GYE*, *Subnet_IBR_Multimedia* y la subred de destino sería *Subnet_ClientesUIO*. Con estas dos políticas se tiene conectividad en ambos sentidos entre las LAN de usuarios de la Sede Central Quito con Ibarra y Guayaquil.

Para tener acceso a Internet se toma como ejemplo la política ***AccesoInternet_Clientes***, se define el puerto de entrada la *Vlan_Cliente(VLAN10)* y como salida el puerto *SD-WAN*, la subred de origen es la *Subnet_ClienteUIO* y como destino *all*, haciendo referencia a Internet, de esta manera la política permite que la subred de los clientes naveguen por Internet. A esto se puede agregar que la política ***MPLS_IBR_GYE -> Internet***, tiene la misma función con la particularidad que la Sede Central también da salida a Internet a través de la MPLS a las subredes de Ibarra y Guayaquil, en el caso que las sucursales tengan inconvenientes con su WAN de Internet propia, dándoles redundancia en la navegación.

También existe una política por defecto la cual es negar cualquier tipo de tráfico hacia cualquier destino, la cual debe ser colocada al final de todas las políticas y para permitir que siga un orden jerárquico cumpliendo las primeras políticas, esta política es conocida como ***Implicit Deny***. En la figura 2.12 se muestran las políticas descritas anteriormente, cabe indicar que las Sedes de Quito e Ibarra son muy similares en cuanto a sus políticas y el rol que cumple cada una. El detalle de las demás políticas creadas tanto para la Sede Central Quito, Ibarra y Guayaquil se encuentran en el Anexo III.



Name	From	To	Source	Destination	Service	Action	NAT
Cliente -> ToIBR_GYE	Vlan_Cliente (Vlan10)	virtual-wan-link	Subnet_ClientesUIO	Subnet_IBR_Multimedia SubnetIBR_Clientes Subnet_GYE	HTTP HTTPS ALL_ICMP	ACCEPT	Disabled
FromIBR_GYE ->Clientes	virtual-wan-link	Vlan_Cliente (Vlan10)	MPLS VPN SubnetIBR_Clientes Subnet_GYE Subnet_IBR_Multimedia	Subnet_ClientesUIO	CorreoZimbra ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
AccesoInternet_Clientes	Vlan_Cliente (Vlan10)	virtual-wan-link	Subnet_ClientesUIO	all	ALL	ACCEPT	Enabled
MPLS_IBR_GYE -> Internet	virtual-wan-link	virtual-wan-link	MPLS VPN Subnet_GYE SubnetIBR_Clientes Subnet_IBR_Multimedia	all	ALL	ACCEPT	Enabled
Implicit Deny	any	any	all	all	ALL	DENY	

Figura 2.12. Políticas Sede Central Quito.

2.6.4.4 Reglas de la SD-WAN

Para que las políticas creadas anteriormente puedan ser consideradas, se definen reglas para determinar el comportamiento de la SD-WAN, permitiendo que la red sea inteligente y con libre autonomía para tomar decisiones a la hora de enrutar el tráfico, contemplando ciertos parámetros como latencia, *jitter* y pérdida de paquetes. Todas las reglas en cada uno de los puntos son similares. Al igual que en las políticas, se deben aplicar la reglas SD-WAN en orden descendente y dejando en la parte de abajo la regla **implícita *sd-wan*** que sirve para permitir cualquier tipo de tráfico a cualquier destino.

Como ejemplo se toman las reglas de la Sede Central Quito. La primera regla llamada ***ToMultimedia*** tiene como objetivo que las LAN de Quito alcancen el servidor Multimedia ubicado en Ibarra a través de un camino o por seguridad por el Túnel IPSec de nombre *To_IBR_Inter*, persuadiéndolo a seguir un camino determinado. Si el túnel de Internet, se llegara a caer por alguna causa, pasará a la segunda regla llamada ***ToMultimediaMPLS***, la cual cumple el mismo objetivo de la primera regla, pero por el túnel creado a través de la MPLS llamado *ToIBR*. La tercera regla llamada ***ToIBR***, permite la comunicación entre la LAN de Quito y la LAN de Ibarra; para este caso se tienen dos caminos, por el túnel de Internet *To_IBR_Inter* o por el túnel MPLS *ToIBR*; la SD-WAN tomará la mejor ruta automáticamente en base al parámetro de latencia, si llegara a aumentar la latencia buscará una ruta con menor retardo.

La cuarta regla ***ToGYE***, tiene el mismo objetivo que la tercera, con la diferencia que la comunicación la hará entre la LAN de Quito y la LAN de Guayaquil, es importante indicar que los parámetros pueden ser modificados de acuerdo a las necesidades para determinar la mejor ruta en base a la latencia, SLA, pérdidas de paquetes, ancho de banda, etc.

La quinta regla llamada ***Zoom***, define que las LAN de los usuarios de Quito, Ibarra y Guayaquil, para reuniones por al App Zoom, salgan siempre por la WAN de Internet de la Sede Central Quito y no por su WAN de Internet propia en el caso de Ibarra y Guayaquil.

La sexta regla llamada ***AccesoInternet***, tiene como objetivo dar navegación a todas las subredes que se tiene a nivel del proyecto, en caso de llegar a fallar su propia salida a Internet. En la figura 2.13 se muestran las reglas de la SD-WAN de la Sede Central; las reglas de las sedes Ibarra y Guayaquil se muestran en el Anexo III.

Name	Source	Destination	Criteria	Members
IPv4 6				
ToMultimedia	Subnet_Zimbra Subnet_ClientesUIO SSLVPN_TUNNEL_ADDR1	Multimedia	Latency	To_IBR_Inter
ToMultimediaMPLS	Subnet_Zimbra SSLVPN_TUNNEL_ADDR1 Subnet_ClientesUIO	Multimedia	Latency	ToIBR
ToIBR	Subnet_ClientesUIO Subnet_Zimbra	Subnet_IBR_Multimedia SubnetIBR_Clientes	Latency	ToIBR To_IBR_Inter
ToGYE	Subnet_Zimbra Subnet_ClientesUIO	Subnet_GYE	Latency	ToGYEInter ToGYEMPLS
Zoom	Subnet_ClientesUIO SubnetIBR_Clientes Subnet_GYE	Zoom.us-Zoom.Meeting Zoom	Latency	Wan_Internet (wan1)
AccesoInternet	Subnet_Zimbra Subnet_ClientesUIO Subnet_GYE Subnet_IBR_Multimedia +4	all	SLA	Wan_Internet (wan1)
Implicit 1				
sd-wan	all	all	Source-Desti...	any

Figura 2.13. Reglas SD-WAN Sede Central Quito.

2.6.4.5 VPN IPSec

Las redes privadas virtuales se integran en este proyecto para brindar mayor seguridad en la transmisión de datos, de manera que se utilizan túneles IPSec tanto a nivel de la red de Internet como de la red MPLS, logrando la comunicación interna a través de los túneles entre Quito, Ibarra y Guayaquil.

En este análisis en la figura 2.14 se muestran los túneles creados en la Sede Central Quito. En este punto se crean cuatro túneles IPSec, dos túneles a través de la MPLS para alcanzar la comunicación con Ibarra ***ToIBR*** y Guayaquil ***ToGYEMPLS***; de la misma manera un túnel creado por la red de Internet para alcanzar Ibarra ***To_IBR_Inter*** y un túnel para alcanzar Guayaquil ***ToGYEInter***. Los túneles IPSec son similares en los tres puntos del proyecto, los cuales se muestran en el Anexo III de Ibarra y Guayaquil.

Tunnel	Interface Binding	Status
Custom 4		
ToIBR	Wan_MPLS (wan2)	Up
ToGYEMPLS	Wan_MPLS (wan2)	Up
ToGYEInter	Wan_Internet (wan1)	Up
To_IBR_Inter	Wan_Internet (wan1)	Up

Figura 2.14. Túneles IPSec Sede Central Quito.

2.6.4.6 VPN SSL

La VPN SSL brinda seguridad, siendo su principal función el permitir acceso remoto a los servidores desde cualquier lugar del mundo. Existen dos formas de poder acceder, mediante un navegador o instalando la aplicación FortiClient en cualquier dispositivo. La VPN SSL sirve en la pandemia para realizar teletrabajo con solo tener acceso a Internet. La figura 2.15 muestra el acceso mediante la Aplicación FortiClient, se ingresa un *username* y un *password* que previamente se configura en el FortiGate de la Sede Central.

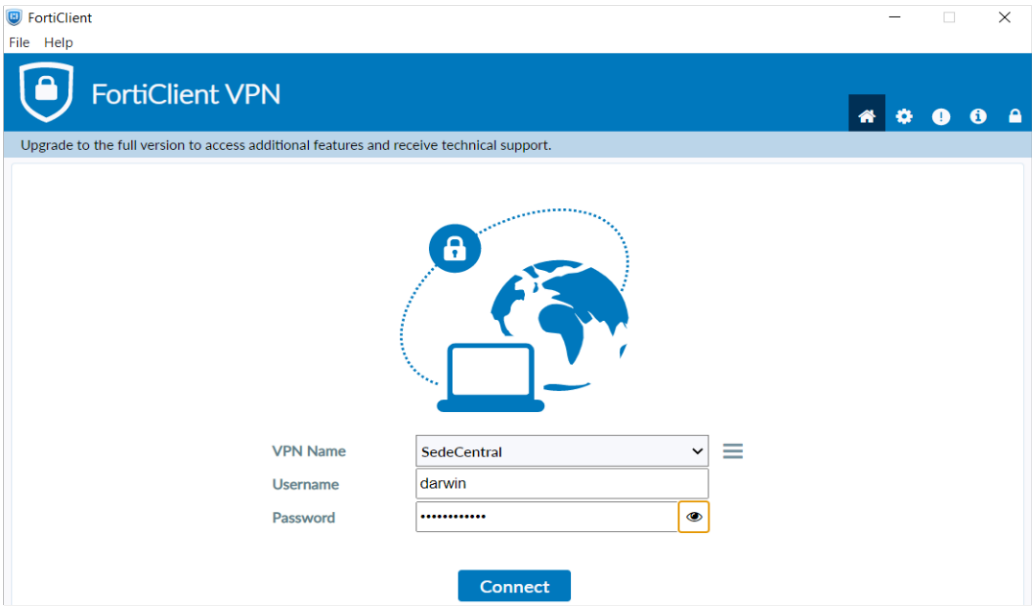


Figura 2.15. Aplicación FortiClient.

2.6.4.7 Políticas Traffic Shaping

Las políticas *Traffic Shaping* tiene como objetivo, optimizar los recursos disponibles, aprovechar de mejor manera y no subutilizar el ancho de banda que se tiene en cada enlace físico de la red MPLS o de la red de acceso a Internet; de esta manera se pueden reducir los costos adquiriendo un ancho de banda mínimo o promedio. Como toda política se debe cumplir un orden descendente. En la Sede Central Quito se dispone de cuatro políticas como se muestra en la figura 2.16.

Como ejemplo se explica únicamente la política ***ShapingZimbra***, la cual tiene como subredes de origen *MPLS*, *Subnet_ClienteUIO, Subnet_GYE, Subnet_IBR_Multimedia, SubnetIBR_Clientes, VPN* y *SSLVPN_TUNNEL_ADDR1* e IP de destino *Zimbra*; puerto de salida la Vlan_Zimbra (Vlan100). Se ingresa una velocidad de subida de 5 Mbps y una velocidad de descarga de 5 Mbps; se limita por servicio *ALL_ICMP, CorreoZimbra, HTTP* y *HTTPS*, y por aplicación *Zimbra* y *FortiClient*. Con esta política lo que se hace es limitar el ancho de banda que se dedica para el acceso al servidor Zimbra en la LAN,

compartiendo 5 Mbps de subida y de bajada con prioridad alta entre todas las subredes del proyecto, incluida para los usuarios remotos. El detalle de las demás políticas y las que se tiene en Ibarra y Guayaquil se especifican en el Anexo III.

Name	Source	Destination	To	Shared Shaper	Reverse Shaper	Service	Applications
IPv4 4							
ShapingZimbra	MPLS Subnet_ClientesUIO Subnet_GYE Subnet_IBR_Multimedia SubnetIBR_Clientes VPN SSLVPN_TUNNEL_ADDR1	Zimbra	Vlan_Zimbra (Vlan100)	5M	5M	ALL_ICMP CorreoZimbra HTTP HTTPS	Zimbra FortiClient
ToMultimedia	Subnet_ClientesUIO Subnet_Zimbra	Multimedia	To_IBR_Inter ToIBR	10M	10M	ALL_ICMP HTTP HTTPS Multimedia	Plex.TV Plex.VPN
Zoom	Subnet_ClientesUIO Subnet_Zimbra MPLS Subnet_GYE Subnet_IBR_Multimedia SubnetIBR_Clientes VPN	Zoom.us-Zoom.Meeting	Wan_Internet (wan1)	5M	10M	Internet Service	Zoom Zoom_File.Download Zoom_File.Upload Zoom_Login Zoom_Meeting Zoom_Meeting.Remote.Control
ToInternet	MPLS Subnet_GYE Subnet_IBR_Multimedia SubnetIBR_Clientes VPN Subnet_ClientesUIO Subnet_Zimbra	all	Wan_Internet (wan1)	10M_Media	20M_Media	ALL	

Figura 2.16 Traffic Shaping Sede Central Quito.

2.6.4.8 Seguridad de la SD-WAN

La seguridad que proporciona Fortinet con *Next-Generation Firewall* o NGFW como una solución, es única en el mercado y viene incorporada con la SD-WAN en los FortiGate; de esta manera permite tener el control de todo tipo de aplicaciones y proteger a la red contra ataques internos o externos. Se tiene una lista de perfiles de seguridad mostrados en la figura 2.17; los perfiles son los mismos y son aplicados en los puntos de Quito, Ibarra y Guayaquil. En el apartado 2.7.3.7 se detallará la configuración y el uso de los perfiles.

Figura 2.17. Perfiles de Seguridad *Firewall* FortiGate.

2.6.4.9 Calidad de Servicio en la SD-WAN

Esta sección se relaciona con la Calidad de Servicio (QoS), donde se puede levantar un monitoreo en tiempo real de los enlaces miembros de la SD-WAN. Se debe definir un sondeo a un servidor público como Google o un servidor local del proyecto en función de la latencia, *jitter*, pérdida de paquetes o SLA; la medición se lo realiza a un enlace o túnel que interviene en el sondeo para alcanzar dicha IP o servidor y definir la mejor ruta.

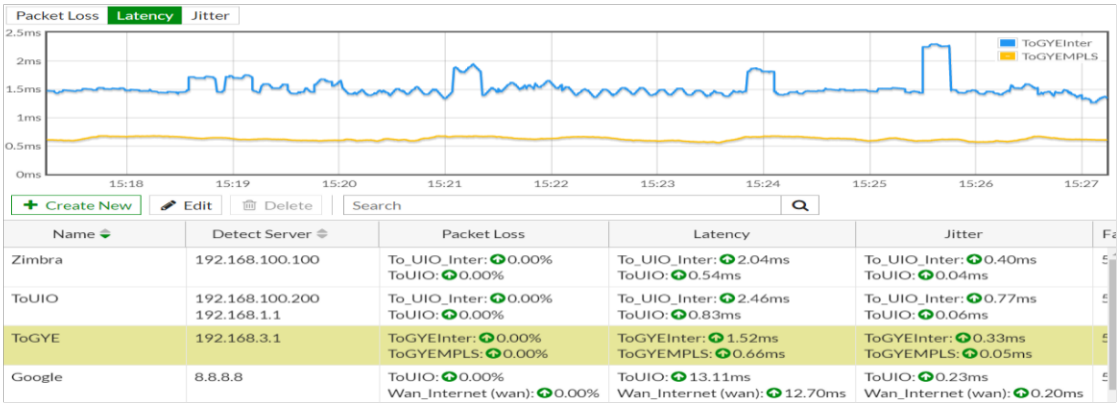


Figura 2.18. Calidad de Servicio Sede Ibarra.

En la figura 2.18 se visualiza el monitoreo a las IP o servidores públicos o locales en la Sede Ibarra, la primera QoS llamado ***Zimbra*** tiene como objetivo sondear las rutas dirigidas para alcanzar el Servidor de Correo por los túneles MPLS *ToUIO* o Internet *To_UIO_Inter*. La segunda QoS de nombre ***ToUIO*** corresponde a las rutas dirigidas para alcanzar las LAN de Quito por los túneles MPLS *ToUIO* o Internet *To_UIO_Inter*. La tercera QoS de nombre ***ToGYE*** corresponde a las rutas dirigidas para alcanzar la LAN de Guayaquil, sondeando los túneles de la MPLS *ToGYEMPLS* y de Internet *ToGYEInter*. La cuarta QoS de nombre ***Google***, corresponde a las rutas dirigidas para alcanzar el servidor Google o Internet, en este caso se puede salir por su propia WAN física o por el túnel MPLS *ToUIO* que va hacia Quito. La Calidad de Servicio de Quito y de Guayaquil se detallan en el Anexo III.

2.6.4.10 FortiManager

La incorporación de FortiManager para la administración centralizada, se hace a través de un ADOM implementado en la nube de Puntonet, que separa los dispositivos del proyecto con los clientes de Puntonet. En la figura 2.19 se observa el panel de control de FortiManager para agregar dispositivos FortiGate, así como crear objetos y políticas, crear VPNs. Desde aquí se agregan, quitan o modifican políticas SD-WAN, políticas de seguridad y reglas, actuando como un Centro de Control y monitoreo de la red.

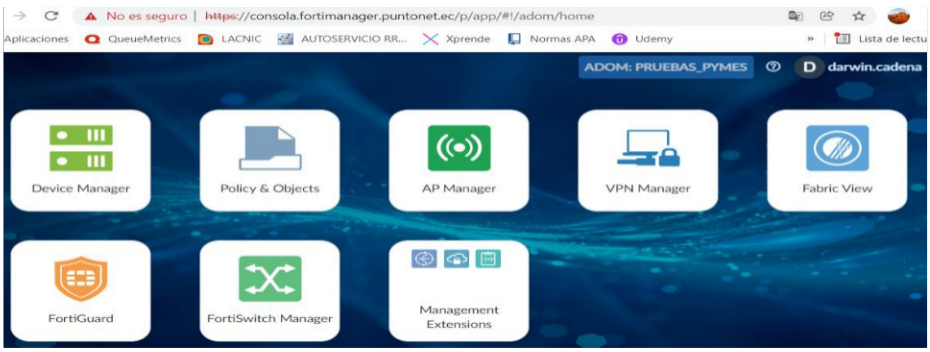


Figura 2.19. ADOM de FortiManager en la Nube de Puntonet.

2.7 IMPLEMENTACIÓN DEL PROTOTIPO

En esta sección se especifican las configuraciones de cada equipo perteneciente a cada sede. En la figura 2.20 se muestran los equipos físicos utilizados en la implementación del proyecto como *router* Cisco 2811 Serie ISR, Cisco ISR C1111, FortiGate 60F, FortiGate 40F, *laptops* utilizados como servidores. En la figura 2.21 se presenta un esquema para entender de mejor manera como están los equipos conectados y distribuidos en las Sedes Central Quito, Ibarra y Guayaquil.

Figura 2.20. Implementación de la red SD-WAN híbrida.

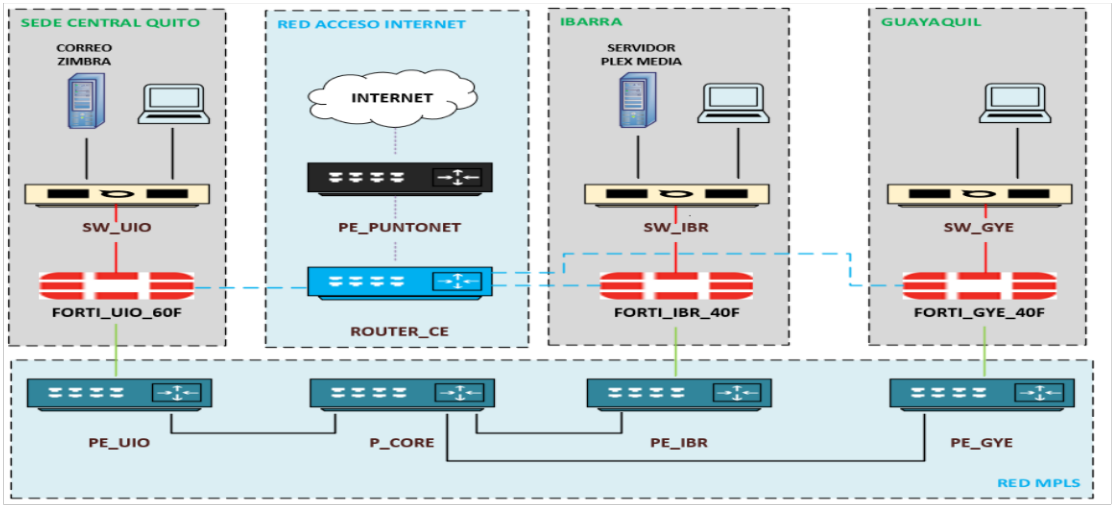


Figura 2.21. Diagrama de conexiones de los equipos del prototipo.

2.7.1 CONFIGURACIÓN RED MPLS

Tanto en los *routers* PE y P se configuran las direcciones IP y el protocolo OSPF con su ID en las interfaces físicas y lógicas o de *Loopback*; dentro del protocolo OSPF se asocia el protocolo MPLS para la conmutación de las etiquetas como se muestra en la figura 2.22.

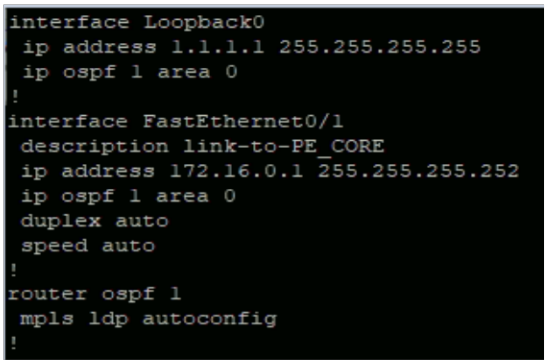


Figura 2.22. Configuración MPLS en router PE.

En la figura 2.23 se muestra el *router* PE_UIO con la configuración del protocolo MP-BGP con AS 100, sus vecinos asociados a través de la interfaz *Loopback* de los *routers* PE_IBR y PE_GYE, separando el tráfico y direccionamiento mediante la *vrf datos* y una VPNv4, se aplica en las interfaces Clase de Servicio y Calidad de Servicio mediante ACL; esto solo se configura en los router PE y no en el *router* P de *Core*.

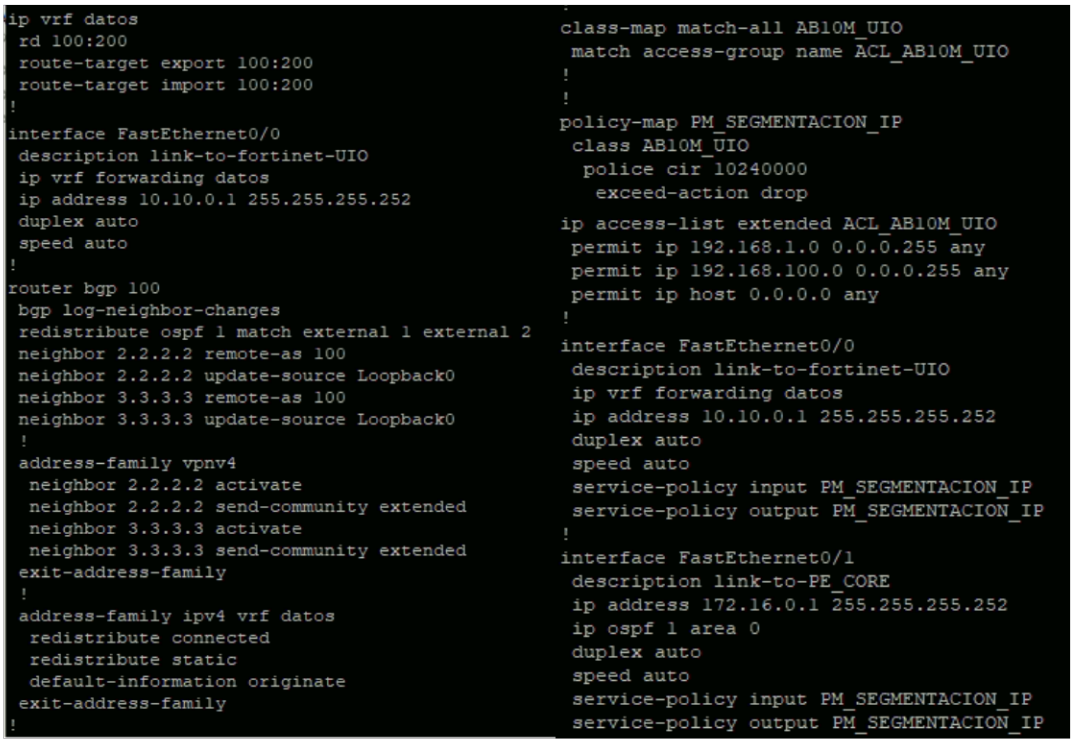


Figura 2.23. Configuración BGP y VRF en router PE_UIO.

Adicionalmente, como se muestra en la figura 2.24, se debe publicar en cada PE las subredes que están en la LAN detrás de cada *firewall*, con la particularidad de la ruta 0.0.0.0/0 para el PE_UIO, que permite dar salida a Internet a las sucursales por la WAN MPLS de la Sede Central Quito. Las configuraciones de los routers de la MPLS como PE y P se encuentran en el Anexo IV.

```
ip route vrf datos 0.0.0.0 0.0.0.0 10.10.0.2 name RutaDefault
ip route vrf datos 10.20.0.1 255.255.255.255 10.10.0.2 name RutaTunnelMPLS
ip route vrf datos 10.20.0.5 255.255.255.255 10.10.0.2 name RutaTunnelInternet
ip route vrf datos 192.168.1.0 255.255.255.0 10.10.0.2 name LANClienteUIO
ip route vrf datos 192.168.100.0 255.255.255.0 10.10.0.2 name LANZimbra
```

Figura 2.24. Publicación de subred en router PE.

2.7.2 CONFIGURACIÓN RED DE ACCESO A INTERNET

Anteriormente se explicó parte de la última milla y la configuración de la VLAN 281 en el ONT Calix en el apartado 2.3.1; adicionalmente para obtener las IP públicas, se configura también la VLAN 281 en el PE de Puntonet asociando la dirección IP de *Gateway* y la máscara para el proyecto como se muestra en la figura 2.25. En el lado de la red del prototipo se coloca un Cisco ISR1111 trabajando como *Switch* para entregar las IPs a cada *firewall*. En la red real se deberá instalar su propia última milla y colocar un *router* CE para cada sede. El detalle de la configuración del *router* CE se especifica en el Anexo IV.

```
RP/0/RP0/CPU0:PNETUIOMTZPE10#sh run interface TenGigE0/0/0/2.281
Tue Dec 28 16:12:58.718 ECT
interface TenGigE0/0/0/2.281
 description --- PRUEBAS TESIS DARWIN CADENA---
 vrf [redacted]
 ipv4 address 190.12.33.193 255.255.255.248
 encapsulation dot1q 281
```

Figura 2.25. IP Gateway en PE de Puntonet.

2.7.3 CONFIGURACIÓN DE LA SD-WAN

2.7.3.1 Configuración Interfaces

El proceso de configuración de las interfaces en todos los puntos es el mismo tanto para el puerto WAN como para los puertos LAN considerando VLANs; para los puntos de Quito e Ibarra se configuran dos VLAN y para Guayaquil una VLAN.

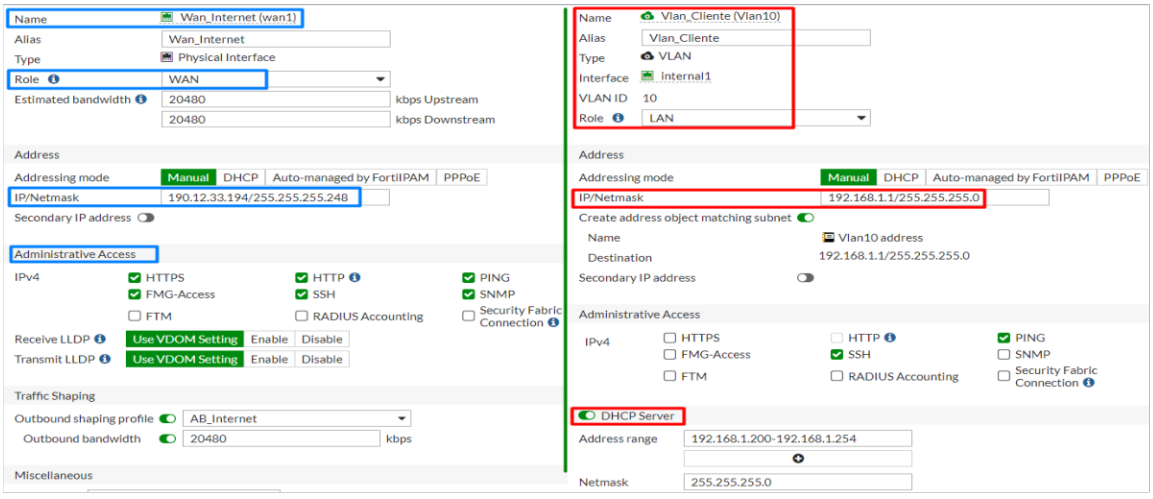


Figura 2.26. Configuración puerto WAN (izquierda) y puerto LAN (derecha).

Como se muestra en la figura 2.26, para la interfaz WAN se deben configurar los parámetros: nombre, rol como WAN, Ancho de Banda estimado, direccionamiento IP manual o por DHCP; para el presente caso se ingresa de forma manual la IP y su máscara; Los accesos administrativos permitidos son importantes de acuerdo al rol que cumple, en este caso se dan permisos *HTTPS, HTTP, PING, FMG-ACCESS, SSH* y *SNMP*.

Para el puerto LAN, se considera primero la configuración de las VLAN con los parámetros: nombre, tipo VLAN, la interfaz física a la que va asociada, el número de VLAN, su rol como LAN; también se debe configurar el direccionamiento IP de forma manual con la IP de Gateway y la máscara. Se define de acuerdo al rol los accesos administrativos, en este caso solo se habilita *PING* y *SSH*; adicionalmente se habilita *DHCP Server* para entregar automáticamente IPs a los usuarios de la LAN.

En la figura 2.27 se detallan las interfaces configuradas en las Sede Central Quito. El detalle de las interfaces configuradas en los puntos de Ibarra y Guayaquil son similares y se detallan en el Anexo III.

Name	Type	M..	IP/Netmask	Administrative ...	DHCP Ranges
802.3ad Aggregate 1					
Physical Interface 11					
Wan_Internet (wan1)	Physical Interface		190.12.33.194/255.255.255.248	PING HTTPS SSH SNMP +2	
To_IBR_Inter	Tunnel Interface		10.20.0.3/255.255.255.255	PING	
ToGYEInter	Tunnel Interface		10.20.0.7/255.255.255.255	PING	
Wan_MPLS (wan2)	Physical Interface		10.10.0.2/255.255.255.252	PING HTTPS SSH HTTP FMG-Access	
ToIBR	Tunnel Interface		10.20.0.1/255.255.255.255	PING	
ToGYEMPLS	Tunnel Interface		10.20.0.5/255.255.255.255	PING	
dmz	Physical Interface		10.10.10.1/255.255.255.0	PING HTTPS FMG-Access	
internal1	Physical Interface		0.0.0.0/0.0.0.0		
Vlan_Cliente (Vlan10)	VLAN		192.168.1.1/255.255.255.0	PING SSH	192.168.1.200-192.168.1.254
Vlan_Zimbra (Vlan100)	VLAN		192.168.100.1/255.255.255.0	PING	192.168.100.200-192.168.100.250

Figura 2.27. Interfaces Sede Central Quito.

2.7.3.2 Configuración Rutas Estáticas

La configuración de las rutas estáticas se muestra en la figura 2.28. Se escoge la opción Subnet para ingresar la IP remota con su respectiva máscara de red, se ingresa la IP *Gateway* de la interfaz física de la WAN Internet o MPLS local, automáticamente se asocia la interfaz física. De la misma manera se configuran las demás rutas estáticas, cambiando las IP e interfaz física según sea el caso, esto aplica para todos los puntos del proyecto.

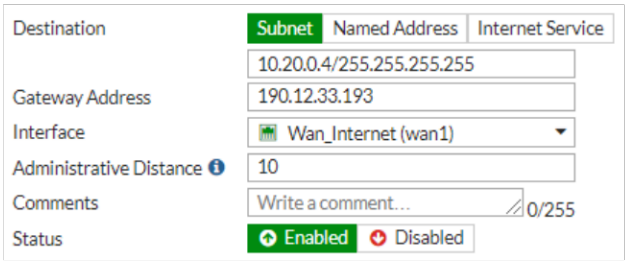


Figura 2.28. Configuración Ruta Estática.

2.7.3.3 Configuración de Políticas y Objetos

En este segmento, se explica solo una de las políticas configuradas, el mecanismo será el mismo para todas, interpretando cuáles son las interfaces de entrada y salida, los objetos o subredes que intervienen, así como los tipos de servicios.

Como ejemplo se detalla la política de la figura 2.29, ésta permite tener conectividad desde la LAN de Clientes Quito a las LAN de Ibarra y Guayaquil. En el panel se ingresan los parámetros: nombre de la política; interfaz de entrada y salida; objetos o subredes de origen y destino; horario programado o dejar en *always*; los servicios que se habilitan *ALL_ICMP, HTTP* y *HTTPS*; la acción puede ser Permitir o Negar lo antes especificado; el Modo de Inspección puede estar basado en flujo o actuar como servidor Proxy; el NAT se habilita cuando la LAN tiene como destino el Internet, cuando la conectividad es interna entre subredes no se habilita NAT; los perfiles de seguridad se agregan según la necesidad de brindar seguridad a la red; los tipo de inspección SSL dependen de la acción a tomar con los certificados SSL en los navegadores; y las opciones de *Logging* son para ver los eventos, sea de los perfiles de seguridad o de todas las sesiones relacionadas a la política.

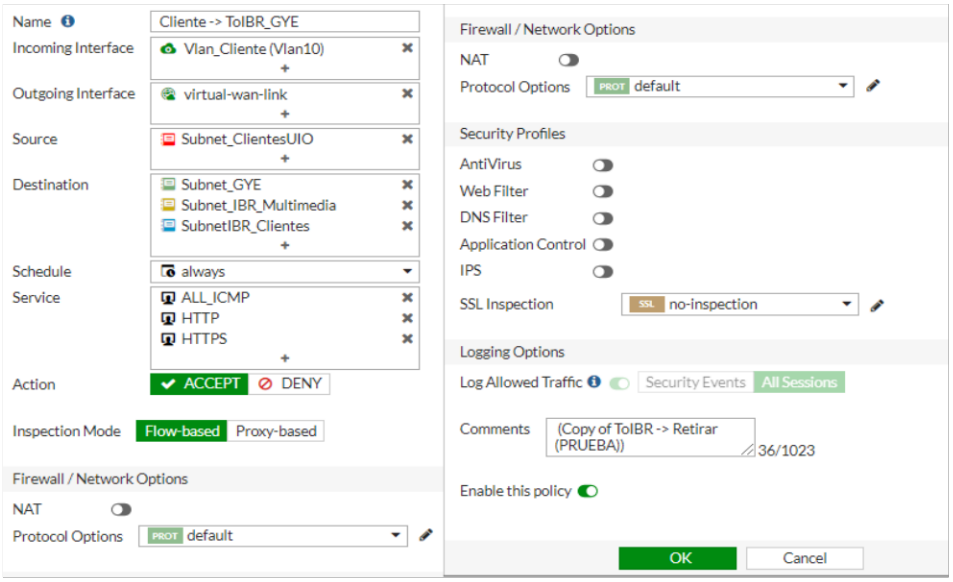


Figura 2.29. Configuración de Política en la Sede Central Quito.

En la figura 2.30 se muestra la configuración de los objetos, tienen la misma configuración en todos los puntos cambiando el direccionamiento IP. Los parámetros son: se establece un nombre; se ingresa la subred, dirección IP única con su máscara o rango de IPs; la interfaz se debe colocar como *any* para que no tenga restricción con ninguna interfaz. En la figura 2.31 se detallan los objetos configurados como subredes, IP única o rango de IPs en Sede Central. El detalle de los objetos de Ibarra y Guayaquil se indican en el Anexo III.

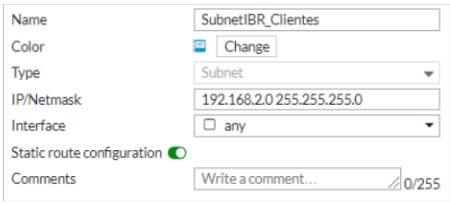


Figura 2.30. Configuración de Objetos.

Name	Details	Interface	Type	Ref.	Routable
IP Range/Subnet 15					
FABRIC_DEVICE	0.0.0.0/0		Address	0	Disable
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0	Disable
none	0.0.0.0/32		Address	0	Disable
UsuarioRemoto	192.168.1.50 - 192.168.1.70		Address	1	Disable
Zimbra	192.168.100.100/32		Address	2	Enable
Multimedia	192.168.200.200/32		Address	4	Enable
MPLS	10.10.0.0/24		Address	6	Enable
VPN	10.20.0.0/24		Address	6	Enable
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel ...	Address	8	Disable
Subnet_GYE	192.168.3.0/24		Address	9	Enable
SubnetIBR_Clientes	192.168.2.0/24		Address	9	Enable
Subnet_IBR_Multimedia	192.168.200.0/24		Address	10	Enable
all	0.0.0.0/0		Address	11	Disable
Subnet_ClientesUIO	192.168.1.0/24		Address	12	Enable
Subnet_Zimbra	192.168.100.0/24		Address	12	Enable

Figura 2.31. Lista de Objetos Sede Central Quito.

2.7.3.4 Configuración VPN IPSec

La configuración de los túneles IPSec son similares en todos los casos, lo único que cambia es la IP de la WAN remota y la interfaz de salida.

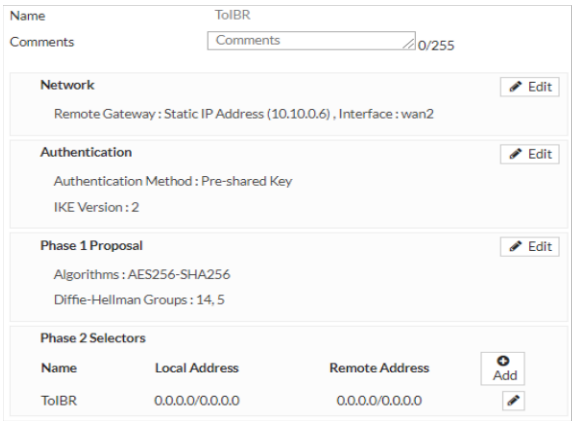


Figura 2.32. Configuración Túnel IPSec.

La figura 2.32 hace referencia al túnel MPLS entre Quito e Ibarra, donde se configuran los parámetros: nombre; IP de la WAN remota e interfaz WAN local; en Método de *Autenticación* se ingresa la clave escogida por cada administrador, debe ser la misma en ambos extremos; en la *Fase1* se especifican los algoritmos de cifrado AES256 y autenticación SHA256; en la *Fase2* se ingresa la subred local y remota, también cifrado AES256 y autenticación SHA256.

2.7.3.5 Configuración de la Calidad de Servicio

La configuración de un SLA o monitoreo son los mismos para todos los puntos, se muestra un ejemplo en la figura 2.33, el sondeo se debe realizar a un servidor local o público. Los parámetros a ingresar son: nombre; IP servidor remoto, ejemplo un *ping* al servidor multimedia 192.168.200.200; se especifican las interfaces o túneles participantes para alcanzar dicha IP; se pueden mantener los mismos parámetros o modificarlos en el Estado de enlace y se debe activar la actualización de las rutas estáticas.

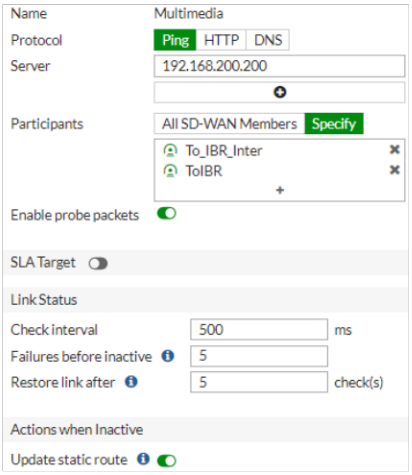


Figura 2.33. Configuración QoS.

2.7.3.6 Configuración Reglas SD-WAN

En la figura 2.34 se muestra como ejemplo la regla SD-WAN para alcanzar la LAN de Ibarra desde la Sede Central Quito, las configuraciones siguen el mismo proceso para cada una de las reglas SD-WAN de cada punto, donde se definen los parámetros: un nombre; subredes de origen; subredes destino; el número de protocolo de transporte UDP, TCP, *ANY* o alguno en específico; se agregan servicios o aplicaciones en caso de ser necesario; para las interfaces de salida se define estratégicamente, sea manual, por la mejor ruta, los que cumplen con los objetivos SLA o por Ancho de Banda; se agregan las interfaces de salida de preferencia, pueden ser interfaces físicas o túneles IPSec; se agrega la medición SLA creada y se da un criterio de calidad, *jitter*, *Latency*, ancho de banda, pérdida de paquetes, *upstream, downstream*, etc.

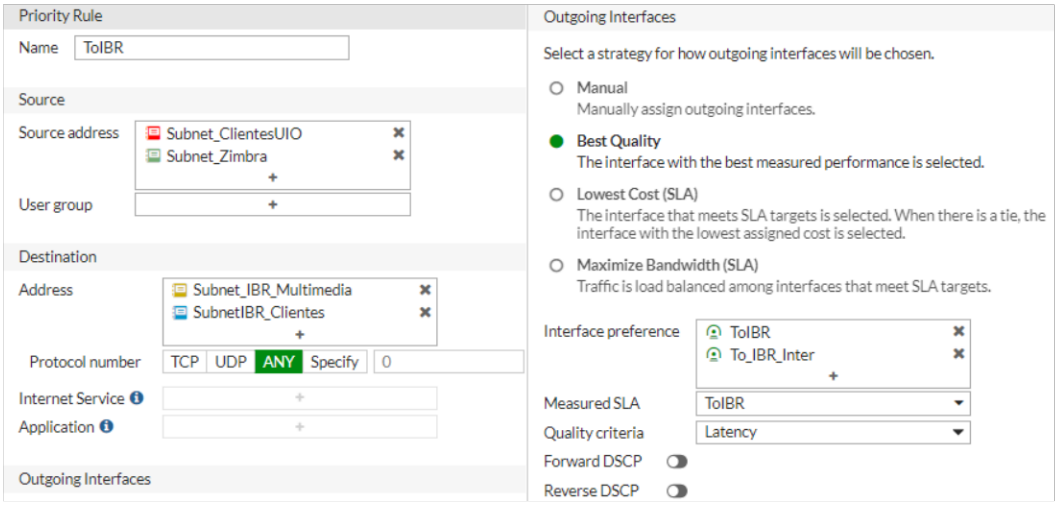


Figura 2.34. Configuración regla SD-WAN.

2.7.3.7 Configuración Perfiles de Seguridad

En esta sesión se toma como ejemplo el perfil de seguridad Antivirus de la figura 2.35.

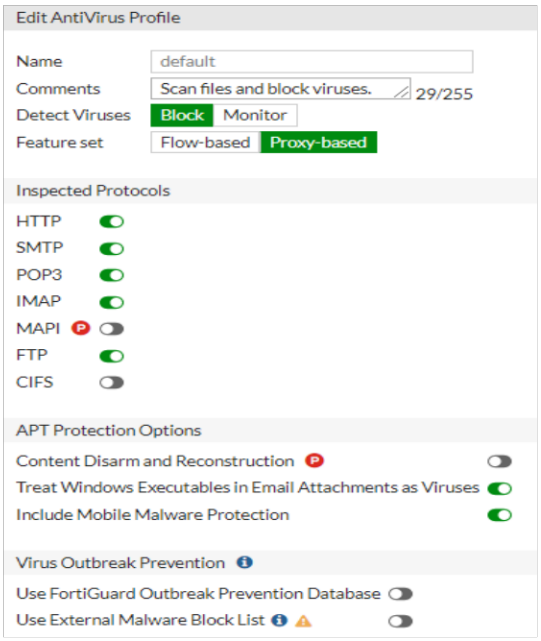


Figura 2.35. Perfil de seguridad Antivirus.

Este perfil viene configurado por *default* en el FortiGate, el cual no permite modificaciones. En el presente caso se utilizará este perfil. Se explican sus parámetros: al detectar un virus, puede bloquearlo o solo monitorear y dejar pasar los archivos sin ninguna acción; trabaja basado en flujo de datos o tipo servidor proxy; inspecciona los protocolos *HTTP*, *SMTP*, *POP3*, y otros que se indican en la figura; puede verificar si existe virus en archivos ejecutables en Windows enviados por *email* e incluye protección de *malware* Mobile para celulares. Se pueden crear perfiles Antivirus según la protección que se desee dar a la red,

siempre que se disponga de una licencia FortiGuard. Los demás perfiles de seguridad y sus configuraciones se detallan en el Anexo III.

2.7.3.8 Configuración Traffic Shaping

En la figura 2.36 se muestra la configuración de las políticas *Traffic Shaping.* Como ejemplo se toma la configuración para optimizar el ancho de banda para acceder al servidor Multimedia, los parámetros son las mismos en todas las políticas y son: nombre; subredes origen; la IP, subred o red destino; se especifican los servicios de la base *HTTP*, *HTTPS* o se crea un servicio propio como *Multimedia* (puerto Plex.TV); se definen aplicaciones *Plex.TV*, *Plex.VPN* en este caso; se ingresan las interfaces o túneles de salida; y se aplica un ancho de banda a compartir como prioridad.

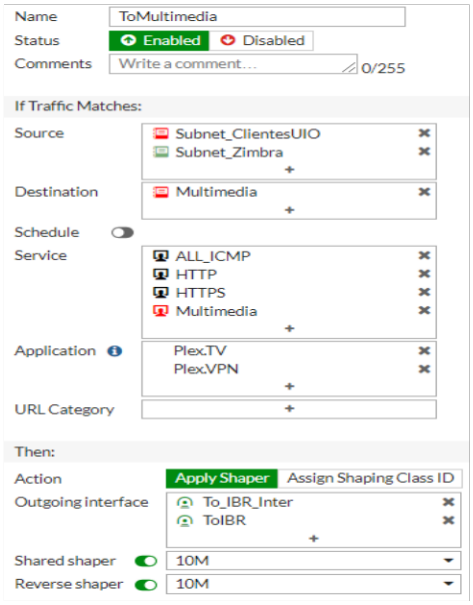


Figura 2.36. Configuración política Traffic Shaping.

2.7.3.9 Configuración VPN SSL

La VPN SSL se configura una sola vez en la Sede Central y se muestra en la figura 2.37.

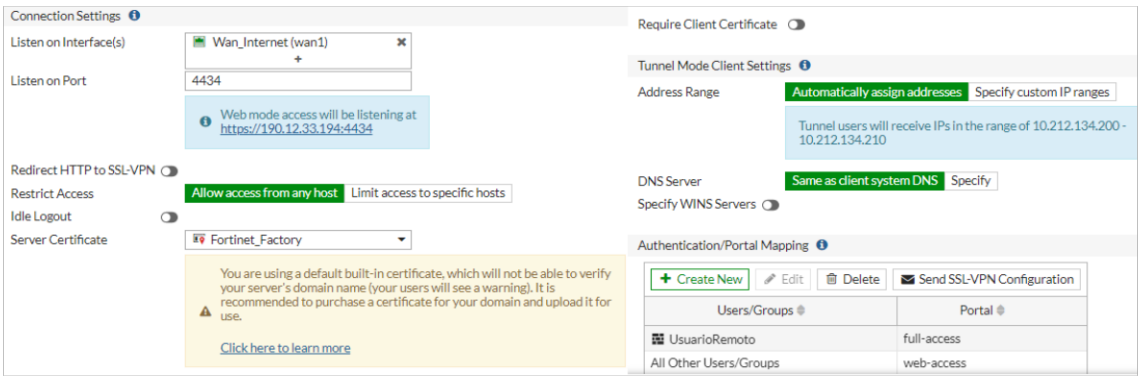


Figura 2.37. Configuración VPN SSL en FortiGate.

Se realizan pocos cambios de los que ya vienen por defecto, los mismos son: se coloca la interfaz WAN de Internet de escucha *Wan_Internet(wan1)*; puerto *4434* para el ingreso de usuarios; por *default* se da acceso a todos los usuarios o *host*; se utiliza el mismo rango de direcciones IP por *default*; en autenticación se agrega al grupo de usuarios agregados y autenticados; y se da acceso por web o la App FortiClient.

2.7.4 CONFIGURACIÓN FORTIMANAGER

La figura 2.38 muestra cómo agregar un equipo FortiGate mediante la GUI; hay varias maneras: ingresando la IP pública asociada al FortiGate, usuario y contraseña o con el *Serial Number*. La configuración desde FortiManager es similar respecto a configurar directamente desde el FortiGate. FortiManager dispone de una base de datos general para configurar políticas, reglas SD-WAN, VPN, objetos y perfiles de seguridad. Asocia una base de datos independiente para las configuraciones de cada FortiGate, permitiendo incorporar nuevos equipos desde cero, sin intervención de personal de TI en sitio. En la figura 2.39 se muestran los dispositivos agregados en el ADOM de FortiManager.

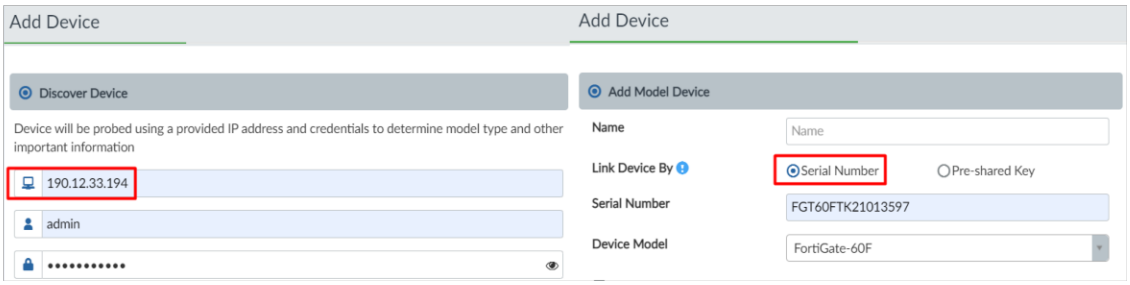


Figura 2.38. Agregar dispositivos en FortiManager.

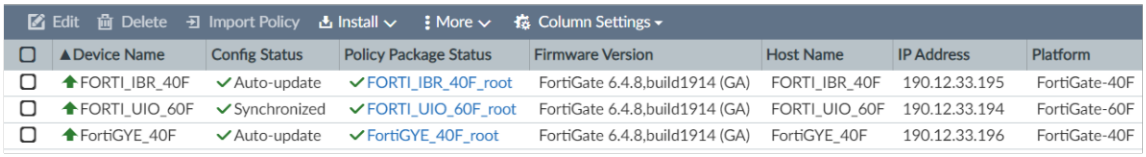


Figura 2.39. Dispositivos agregados en FortiManager.

2.7.4.1 Configuración de Scripts en FortiManager

En FortiManager, se crean *scripts* para la configuración de cualquier parámetro, interfaz o política. En la figura 2.40 se muestran dos plantillas; una para configurar un **Túnel IPSec**, en la *phase1-interface* se cambiarán los parámetros señalados, como el nombre del Túnel; la WAN asociada al túnel; la IP remota o *Gateway*; tener en cuenta que la clave secreta sea la misma en ambos extremos. Para la *phase2-interface* similarmente se coloca un nombre y el nombre del túnel de la *phase1*. El segundo *script* (derecha), se define para configurar una **interfaz WAN**, en *edit* se coloca la WAN dependiendo del número de

interfaces WAN o LAN del FortiGate, se coloca la IP WAN con su máscara, se definen los accesos administrativos a la IP como *ping*, *https*, *ssh*, un alias y se define su rol como *wan*. En la figura 2.41 se muestran los *scripts* creados y se pueden copiar e ir modificando, según las necesidades del administrador y la habilidad para configurar, editar, modificar o eliminar cualquier parámetro o políticas desde FortiManager para incorporar nuevos dispositivos.

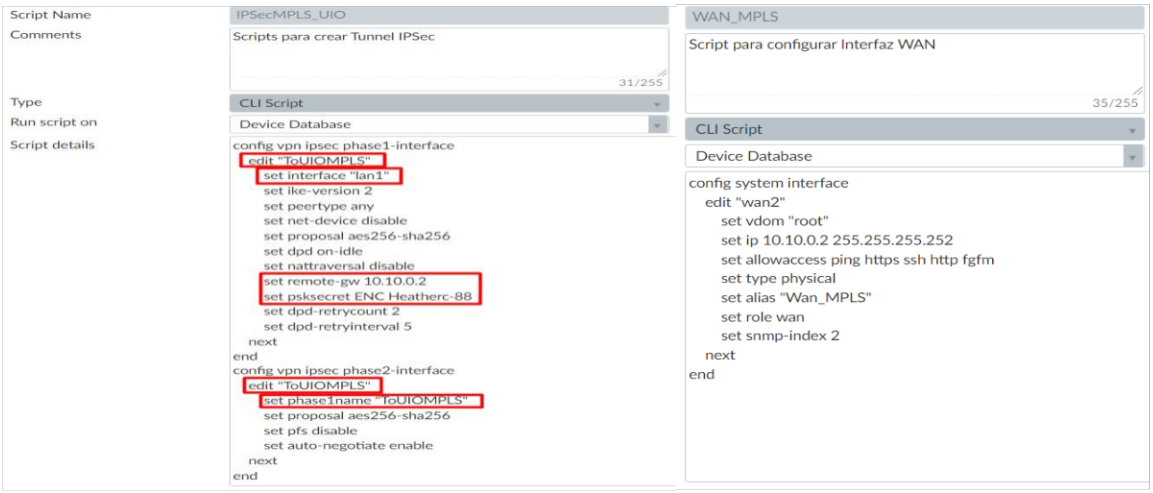


Figura 2.40. Scripts IPSec e Interfaz WAN en FortiManager.

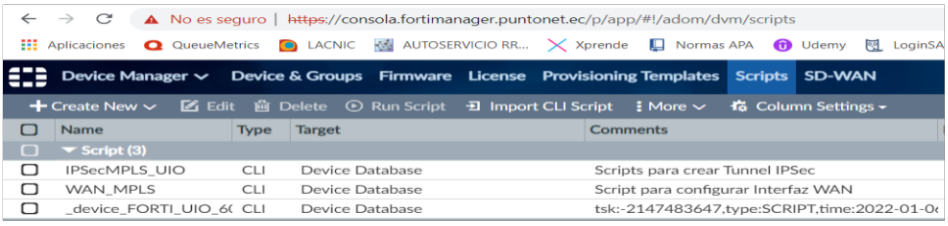


Figura 2.41. Scripts en FortiManager.

2.7.5 CONFIGURACIÓN DE SERVIDORES

La configuración de los servidores DNS y Zimbra ubicados en la LAN de la Sede Central, se realiza sobre Ubuntu 16.04 LTS de 64 bits, virtualizado mediante VMware Workstation 16 Pro, instalado en un servidor hardware con Windows 10. En Ubuntu se instala el paquete *dnsmasq* y se lo configura para levantar el servidor DNS local con el dominio ***sch.com***. Para el servidor de correo se instala *Zimbra Edition 8.8.15 GA Release* compatible con la distribución de Ubuntu 16.04 LTS desde su página oficial, se instalan todos los repositorios, se asocia al dominio *sch.com* y se configura para obtener un servidor Zimbra en la intranet.

La configuración del servidor de multimedia se hace directamente en un hardware de la LAN de Ibarra. Desde la página oficial de Plex, se descarga el software y se instala como servidor; de esta forma se accede al contenido previamente cargado en Plex Media Server. La configuración en detalle de los servidores se encuentra en el Anexo II.

3 RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

En este capítulo se describen los resultados obtenidos a partir del desarrollo de la red SD-WAN con equipos FortiGate y la administración centralizada con FortiManager; adicionalmente se incluyen las conclusiones y recomendaciones del trabajo realizado.

3.1 RESULTADOS

En esta sección se analizan los resultados obtenidos de la implementación de la SD-WAN con equipos físicos; se comprueba el correcto funcionamiento de la red, su conectividad, la selección dinámica de ruta, balanceo de carga, *traffic shaping*, failover, sus políticas de seguridad, control centralizado, aprovisionamiento de toque cero (ZTP), entre otras.

3.1.1 CONECTIVIDAD DE LA RED Y FUNCIONAMIENTO DE LOS SERVIDORES

3.1.1.1 Conectividad entre LANs

Para las pruebas se utilizan los comandos *ping* y *tracert*, propios del Sistema Windows. Desde una PC en la LAN de Guayaquil con IP **192.168.3.200** se realiza un *ping* para validar conectividad al servidor de correo, servidor multimedia, así como a cada PC de los usuarios de Quito e Ibarra, tal como se muestra en la figura 3.1. En la mayoría de casos se obtiene una latencia media de 2 a 3 ms para alcanzar los destinos; los tiempos de respuesta se reducen al ser enrutados por los túneles IPSec creados para seguridad de la información.

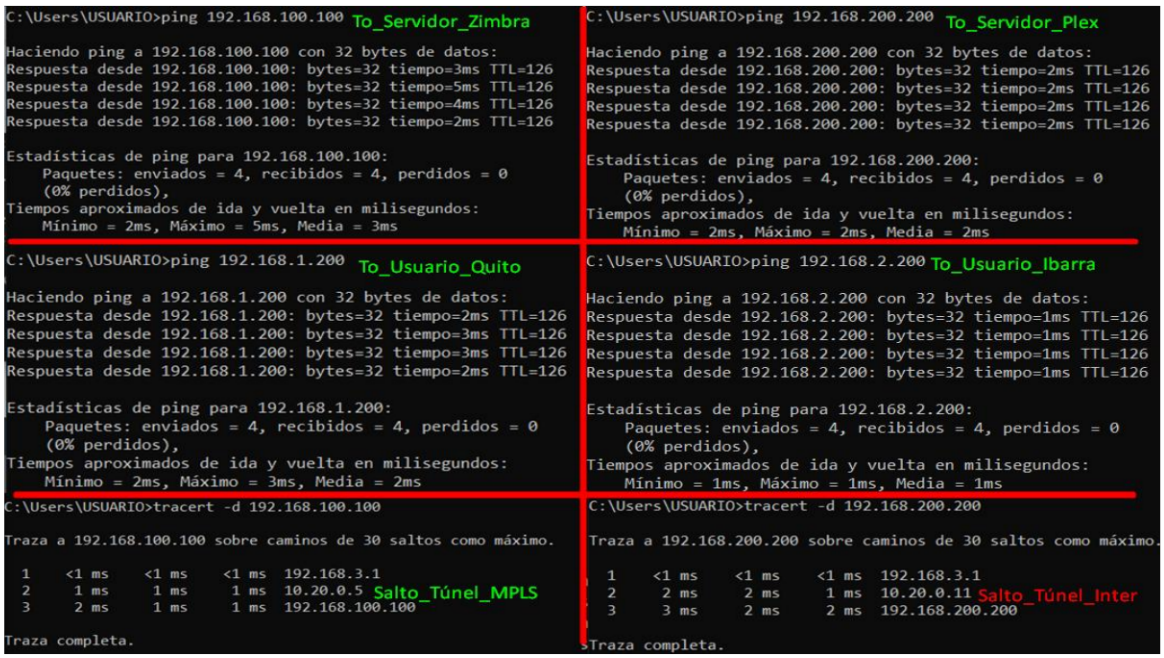


Figura 3.1. Conectividad entre redes LAN.

Adicionalmente se ejecuta el comando *tracert* a los servidores, para validar la trayectoria de los paquetes por los túneles IPSec hasta su destino; como prioridad, para alcanzar el servidor de correo o DNS, los usuarios acceden a través de los túneles de la MPLS y para acceder al servidor multimedia, los saltos son por el túnel de la red de acceso a Internet.

3.1.1.2 Funcionamiento de los Servidores

Los usuarios de la red interna, así como los usuarios remotos, tienen acceso a los servidores DNS, correo Zimbra o Plex Media Server. Se debe digitar en un navegador la URL https://192.168.100.100 o su dominio https://mail.sch.com para el servicio de correo; y para acceder al servidor multimedia Plex se digita la URL https://192.168.200.200:32400. Ambos servidores trabajan en modo cliente-servidor.

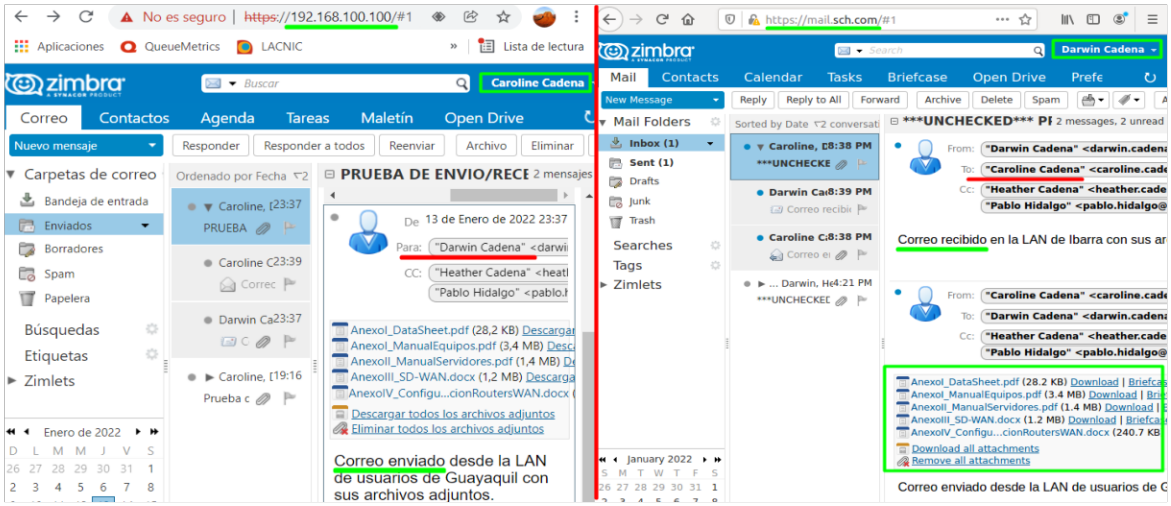


Figura 3.2. Envío (izquierda) /Recepción (derecha) de correos en Zimbra.

Para las pruebas, desde una PC en Guayaquil con IP 192.168.3.200, se ingresa a la cuenta caroline.cadena@sch.com como se muestra en la figura 3.2 (izquierda), se envía un correo con archivos adjuntos, cada buzón tiene una capacidad por defecto de 10 Mbps; siendo esta capacidad modificable en el servidor Zimbra. En la LAN de Ibarra, figura 3.2 (derecha), se accede a la cuenta darwin.cadena@sch.com donde se recibe el correo con sus archivos adjuntos, validando el envío/recepción de los correos correctamente.

El acceso al servidor multimedia cuya URL es https://192.168.200.200:32400; permite monitorear el número de usuarios que acceden o reproducen el contenido de video, audio o imágenes. Las características de Plex son muy similares a las de la plataforma Netflix, siendo fácil su implementación. Si se desea agregar o quitar contenido, se lo hace del lado del servidor; como cliente solo se puede acceder al contenido en modo lectura y descargarlo. La velocidad de acceso, al igual que la capacidad de almacenamiento del contenido, lo da el hardware donde se encuentra implementado el servidor (ver figura 3.3).

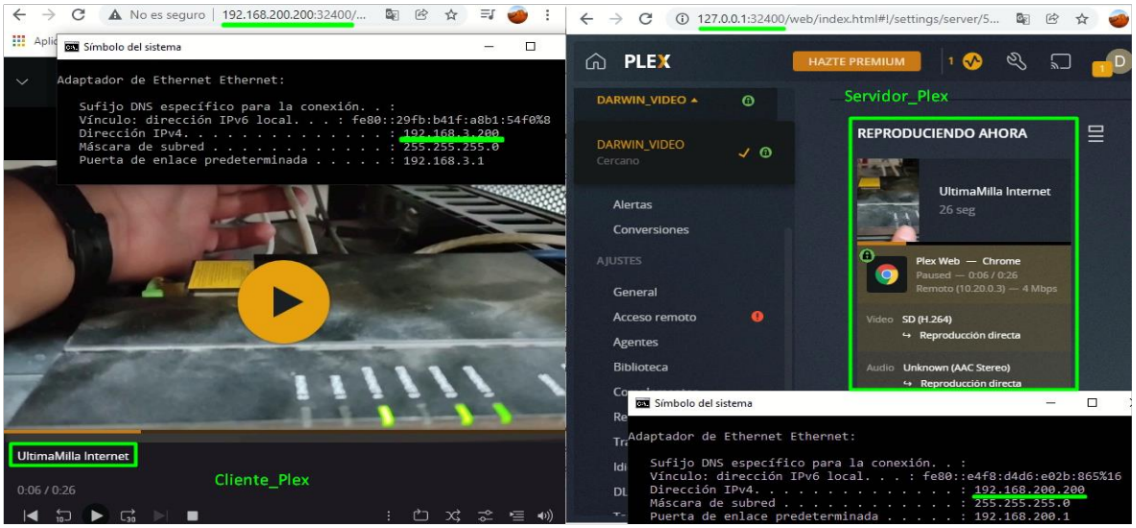


Figura 3.3. Plex Cliente – Servidor.

3.1.2 ADMINISTRACIÓN DEL TRÁFICO DE LA SD-WAN

3.1.2.1 Selección Dinámica de Ruta

En esta sección, se presenta la automatización de la SD-WAN, en la que se define la Calidad de Servicio (QoS), la selección dinámica de la mejor ruta utilizando parámetros como latencia, pérdida de paquetes, *jitter* o SLA.

La comprobación se realiza mediante un *ping* y *tracert* desde Guayaquil hacia Quito, a través de los túneles *ToUIOInter* y *ToUIOMPLS*. Para esto se tienen los siguientes escenarios. En la figura 3.4, se observa mediante el Performance SLA ***LanUIO***, en condiciones normales una latencia baja <= a 1ms y sin pérdida de paquetes por el túnel *ToUIOMPLS* de IP 10.20.0.5, considerado el mejor camino en condiciones normales.

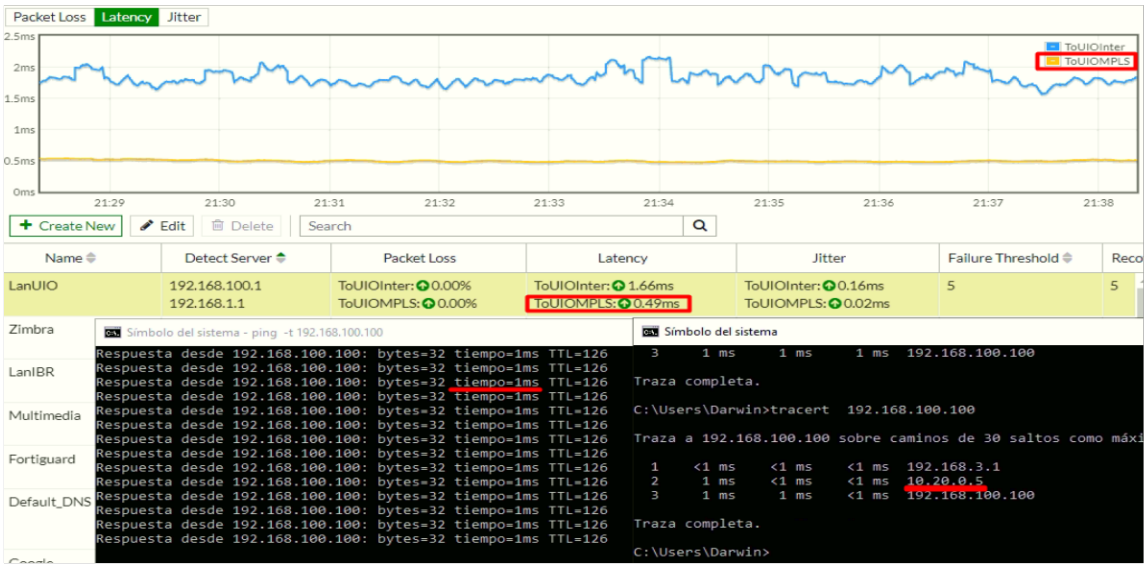


Figura 3.4. Selección dinámica de ruta en condiciones normales por túnel ToUIOMPLS.

Con la ayuda del programa ***TfGen***, se satura el túnel *ToUIOMPLS (línea naranja)*, volviéndolo inestable con pérdida de paquetes y retardos altos como se muestra en la figura 3.5. La SD-WAN al sondear las rutas, busca un mejor camino para alcanzar la IP destino o servidor; al tener una ruta alternativa por el túnel ToUIOInter (línea azul), automáticamente conmuta la salida y pone en *down* al túnel *ToUIOMPLS*. Mediante un *tracert* se pueden ver los saltos y la conmutación por el túnel *ToUIOInter* de IP 10.20.0.7.

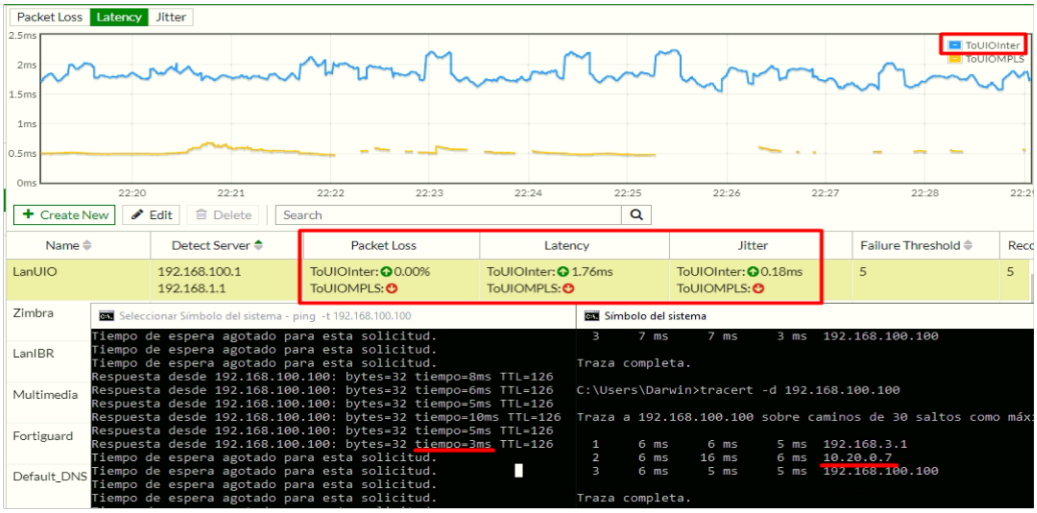


Figura 3.5. Selección dinámica de ruta al tener intermitencias por túnel ToUIOMPLS.

Al dejar de saturar el túnel *ToUIOMPLS,* se elimina la pérdida de paquetes y se normalizan los retardos, volviéndose el mejor camino en base a latencia y *jitter*; la SD-WAN vuelve a sondear y automáticamente cambia la salida por el túnel *ToUIOMPLS* (ver figura 3.6). La SD-WAN monitorea constantemente las rutas, válida y selecciona dinámicamente la mejor ruta para alcanzar el destino, brindando QoS y una conmutación automática del tráfico.

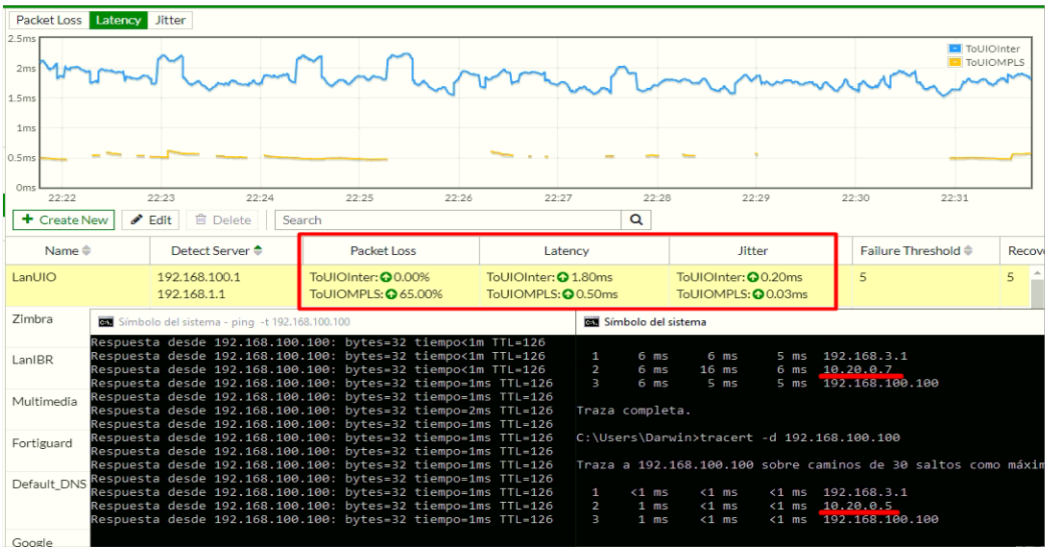


Figura 3.6. Selección dinámica de ruta al estabilizar el túnel ToUIOMPLS.

3.1.2.2 Balanceo con SD-WAN

En la siguiente sección, se valida el balanceo de carga que realiza SD-WAN cuando detecta a usuarios de la LAN de Guayaquil, con varias sesiones navegando en Internet, ya que se tienen dos rutas a Internet: por la WAN propia de Internet y por la Sede Central Quito a través de la MPLS. En la figura 3.7 se muestran varias sesiones abiertas en tiempo real. En el lado izquierdo, se reproducen videos en YouTube, validando que sale por la interfaz WAN propia de Internet ***WanInternet (wan)***; del lado derecho se levanta una reunión en Zoom, en la que para alcanzar dicha plataforma se observa que sale por la interfaz *ToUIOMPLS* hacia la Sede Quito. De esta manera la SD-WAN balancea el tráfico para no saturar un solo enlace, balanceando la carga cuando se accede a Internet o a aplicaciones que normalmente se utilizan para reuniones.

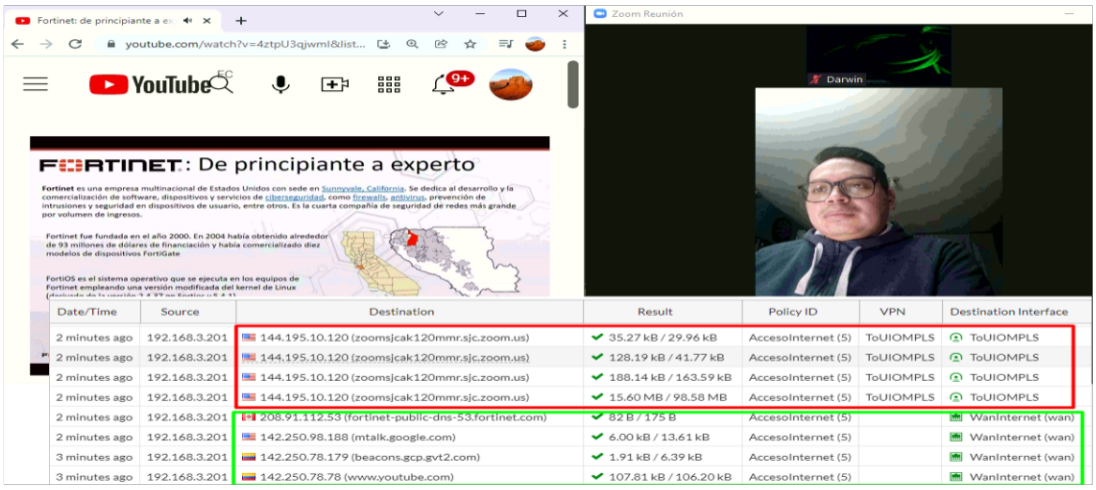


Figura 3.7. Balanceo de Carga.

3.1.2.3 Traffic Shaping

En la siguiente sección se limita y se distribuye de manera inteligente el Ancho de Banda tanto de subida como de bajada en las conexiones utilizando *Traffic Shaping*. Para las pruebas, como ejemplo, se configuran dos políticas como se muestra en la figura 3.8 para dos usuarios de la LAN Quito, luego de las pruebas se eliminan estas políticas.

Name	Source	Destination	To	Shared Shaper	Reverse Shaper	Service
IPv4 1/6						
Gerencia	Gerencia	all	Wan_Internet (wan1)	10M	10M	ALL
Ubuntu	Ubuntu	all	Wan_Internet (wan1)	5M	5M	ALL

Figura 3.8. Políticas Traffic Shaping.

En la figura 3.9, se realiza una prueba de velocidad para los dos usuarios conectados; no se tiene ninguna política aplicada aún, en ambos casos se tiene asignado 20 Mbps, siendo todo el ancho de banda contratado en la Sede Quito.

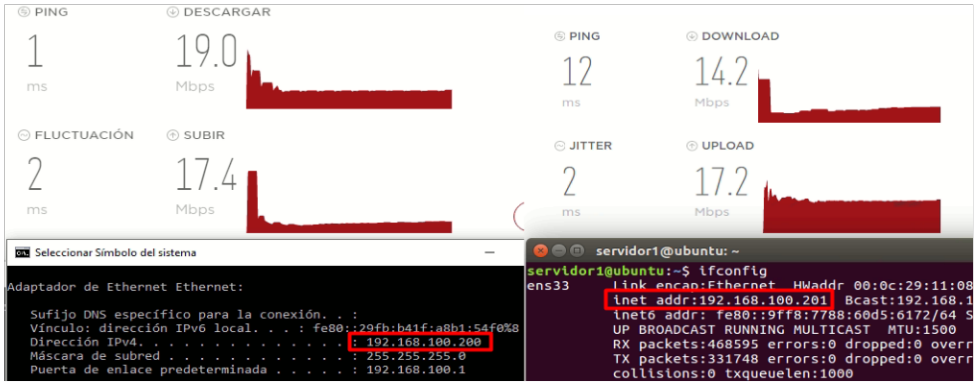


Figura 3.9. Ancho de Banda antes de aplicar la política.

En la figura 3.10 se muestran los dos usuarios, aplicando políticas donde se limita el ancho de banda por IP. En el caso del usuario con IP 192.168.100.200, se aplica la política ***Gerencia***, que asigna un ancho de banda de 10 Mbps simétrico con prioridad alta (izquierda); para el usuario con IP 192.168.100.201 se aplica la política ***Ubuntu*** que asigna 5 Mbps simétrico con prioridad media (derecha). En las pruebas de velocidad realizadas, se observa que existe cierta tolerancia con respecto al ancho de banda utilizado y al configurado en la política, pudiendo validar que la SD-WAN mediante políticas de *Traffic Shaping* puede limitar el ancho de banda de manera inteligente a través de la IP, por aplicaciones o distribuir el ancho de banda entre varios usuarios según la prioridad.

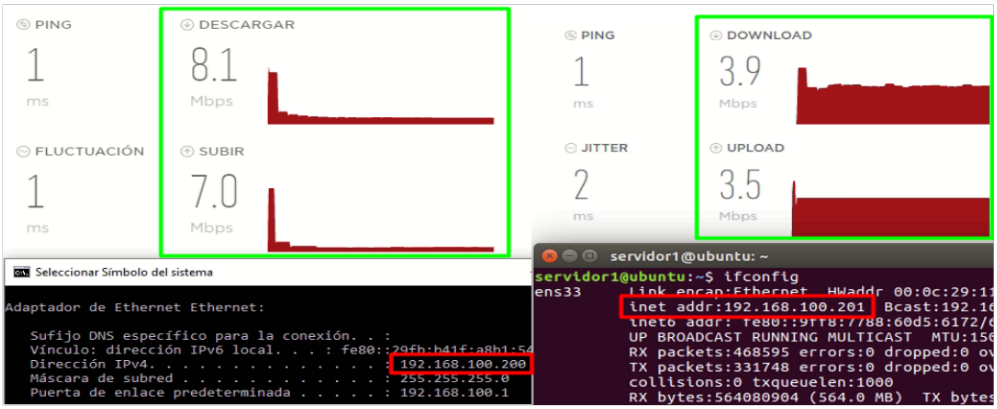


Figura 3.10. Ancho de Banda luego de aplicar la política.

3.1.2.4 Failover entre miembros de la SD-WAN

La conmutación en caso de errores o por *failover*, hoy en día es muy importante para aumentar la disponibilidad de los enlaces y el acceso a los servicios en una infraestructura de red, razón por la que en el proyecto también se aplica esta funcionalidad. En la configuración de la SD-WAN se estableció que, para acceder al servidor de correo, como enlace principal se lo hará por el túnel *ToUIOMPLS* (línea naranja), pero si por algún inconveniente se tiene una caída a nivel de la WAN MPLS, automáticamente se conmutará

por el enlace de respaldo que sería por el túnel ToUIOInter (línea azul). Mediante un *tracert* se valida la conmutación del túnel *ToUIOMPLS* con IP 10.20.0.5 al túnel ToUIOInter con IP 10.20.0.7, tal como se muestra en la figura 3.11.

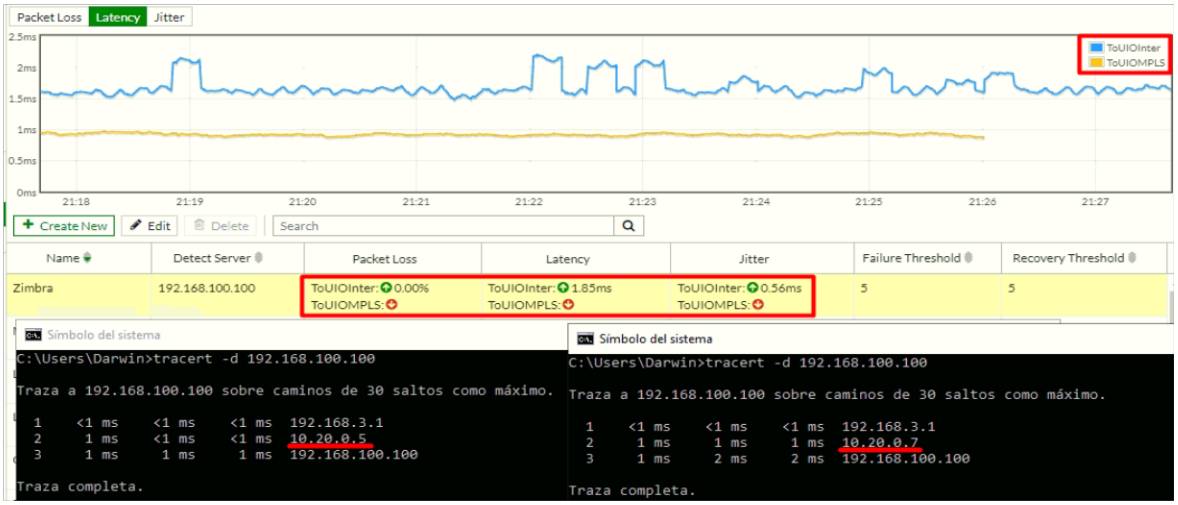


Figura 3.11. Failover al Servidor de Correo.

Lo mismo sucede cuando se quiere salir a Internet; mediante el monitoreo a la IP de *Google* 8.8.8.8 como se muestra en la figura 3.12, la salida lo hace por el enlace principal propio de la WAN de Internet. Si este enlace llega a fallar, se conmutará al enlace de respaldo, es decir en este caso saldrá por el túnel ToUIOMPLS de la red MPLS para acceder a Internet por la Sede Central en Quito. Esto se comprueba mediante un *tracert* donde los saltos al salir por la WAN de red de acceso, da el salto directamente a la IP del *Gateway* 190.12.33.193, pero si conmuta por el túnel de la MPLS, el siguiente salto es la IP del túnel MPLS 10.20.0.5 y luego da los saltos hacia Internet.

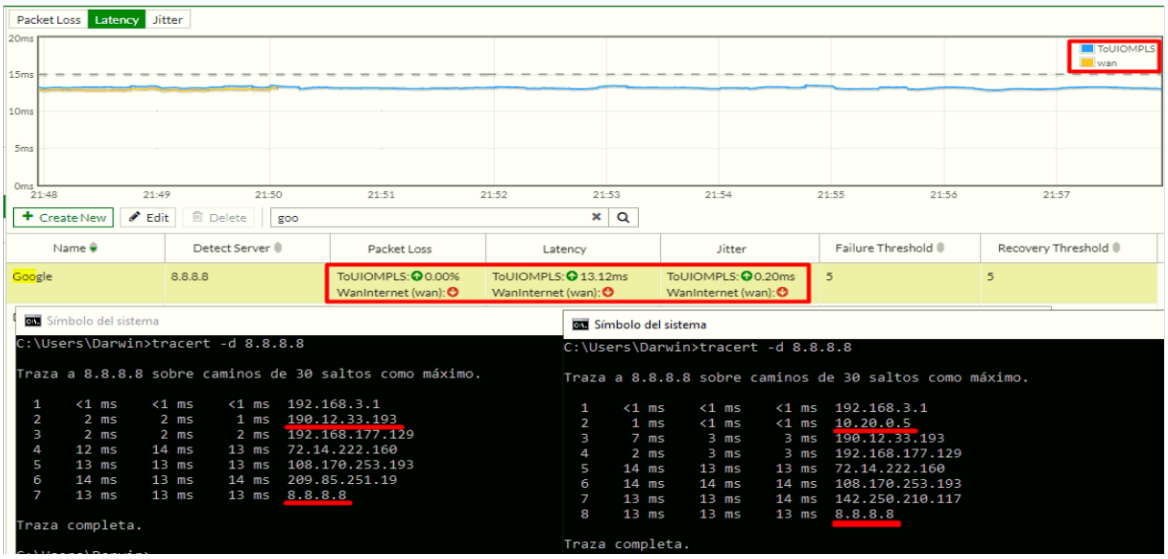


Figura 3.12. Failover hacia Internet.

Con esto se puede tener disponibilidad en los enlaces de un 99,9%, ya que existe un porcentaje de 3 a 4 paquetes perdidos al conmutar del enlace principal al de respaldo, validando la conmutación por error automática, siempre que los enlaces o túneles IPSec creados sean miembros de los enlaces de la SD-WAN.

3.1.3 POLÍTICAS DE SEGURIDAD NGFW E INSPECCIÓN SSL

Fortinet incorpora SD-WAN con seguridad en un mismo dispositivo denominado ***NGFW*** (*Firewall* de Próxima Generación). Para esto se activa la funcionalidad de NGFW en modo ***Profile-based*** que permite inspeccionar el tráfico y crear perfiles de seguridad. También se debe activar la Inspección SSL en modo ***deep-inspection*** (inspección completa) para que cada perfil de seguridad funcione adecuadamente como se muestra en la figura 3.13.

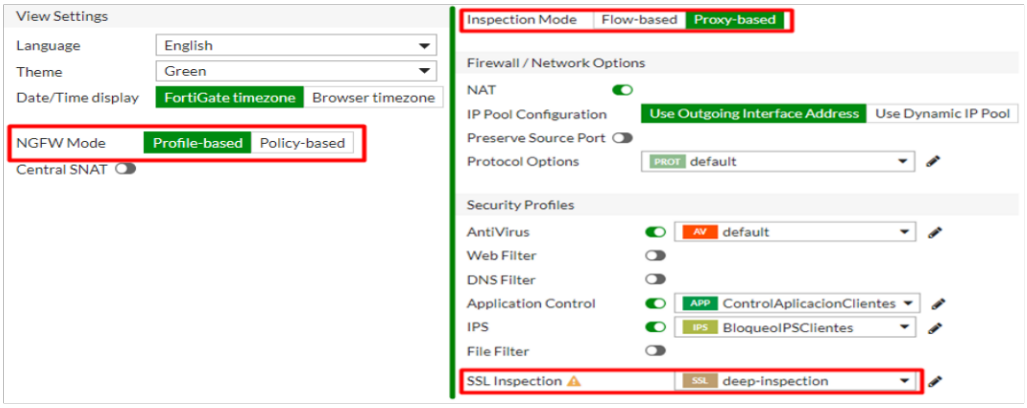


Figura 3.13. *NGFW* (izquierda), Inspección SSL (derecha).

Como dato importante, es necesario la instalación adecuada del certificado *Fortinet_CA_SSL* en los dispositivos de la LAN, para no tener el error de seguridad al acceder a cualquier página en un navegador como se muestra en la figura 3.14.

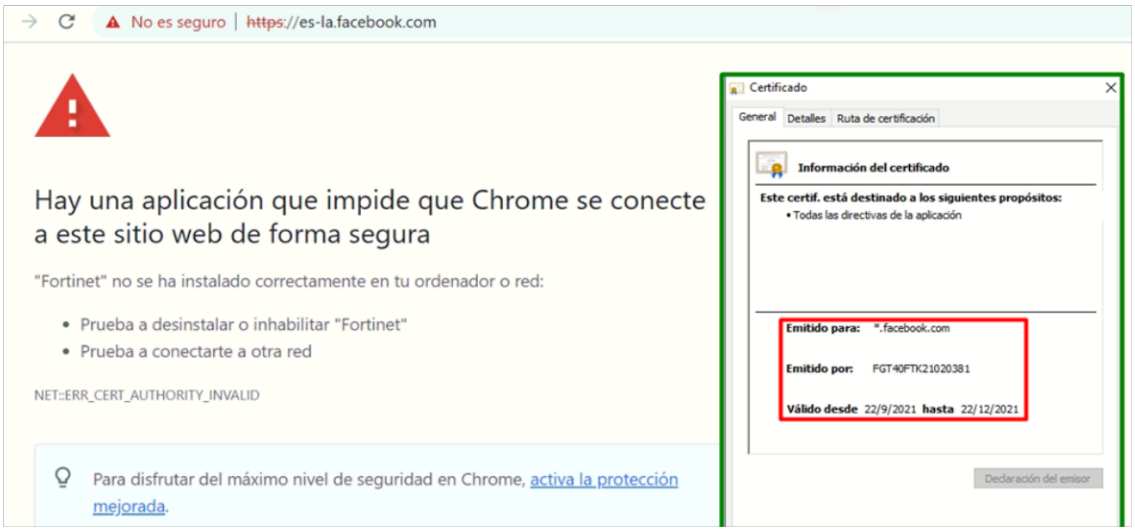


Figura 3.14. Certificado SSL de Fortinet.

3.1.3.1 Antivirus

Los FortiGate tienen la capacidad de bloquear virus o *malware* que provenga del Internet, pero es necesario complementar con un Antivirus en los dispositivos de la LAN para protección interna, ya que existen varias maneras de infectarse dentro de la red, como por ejemplo con memorias USB. Para las pruebas, se descarga en una PC archivos de prueba con virus inofensivo desde la página https://www.eicar.org/?page_id=3950 y con la App Anydesk se accede de forma remota a la PC del servidor multimedia; a continuación, se intenta transferir los archivos con virus observando que el *firewall* detecta los archivos infectados con virus y procede con el bloqueo, interrumpiendo su transferencia como se muestra en la figura 3.15.

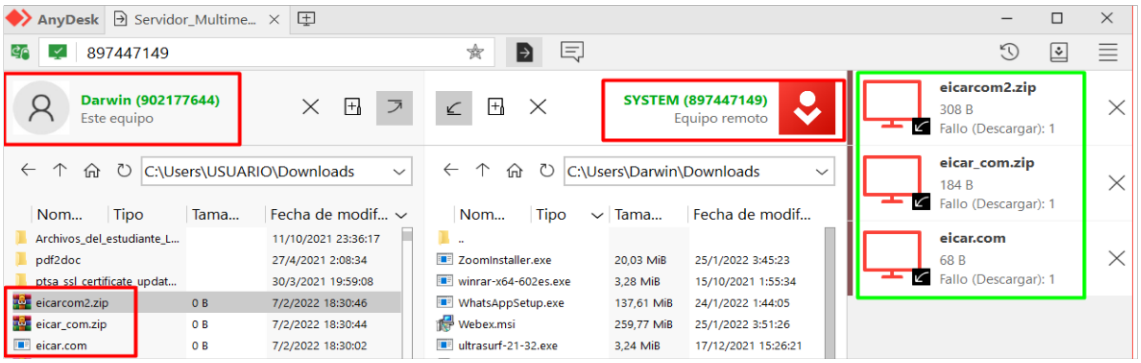


Figura 3.15. Bloqueo de archivos infectados con Virus.

De esta manera en un ambiente productivo, se pueden realizar las pruebas necesarias para validar que el perfil Antivirus esté funcionando y que la red interna permanece protegida ante virus o *malware* que provengan del Internet.

3.1.3.2 Web Filter

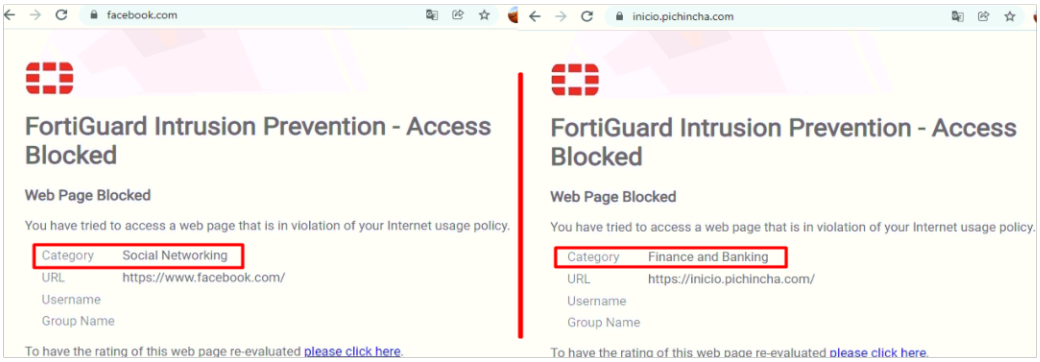


Figura 3.16. Filtro de Páginas Web.

En la siguiente sección se comprueba el control de acceso a las páginas web, para lo cual se pueden habilitar ciertas páginas que se consideran de utilidad a los usuarios y se bloquean páginas consideradas ofensivas o de contenido comprometedor para la red. Por

defecto las páginas vienen por categorías bloqueadas/habilitadas según la consideración de la base de datos de Fortinet. Para las pruebas, se procede con el bloqueo de páginas catalogadas por defecto en el *firewall* como páginas libres de acceso y sin censura. En la figura 3.16 se muestra el bloqueo a las páginas de Redes Sociales como https://www.facebook.com/, Banca y Finanzas como https://inicio.pichincha.com/.

3.1.3.3 Control de Aplicaciones

El siguiente perfil es muy similar al funcionamiento del perfil Web Filter, solo que se realiza el bloqueo/habilitación a nivel de aplicaciones por categoría especificado en el Anexo III apartado 2.3.3. Se parte del bloqueo general y se va habilitando categorías donde intervienen las aplicaciones que son parte del proyecto como ***Email***, ***Video/Audio*** para el cliente Plex; y ***Remote.Access***. En la figura 3.17 se valida que las aplicaciones como Office365 y Adobe permanecen bloqueadas por lo que es necesario habilitarlas.

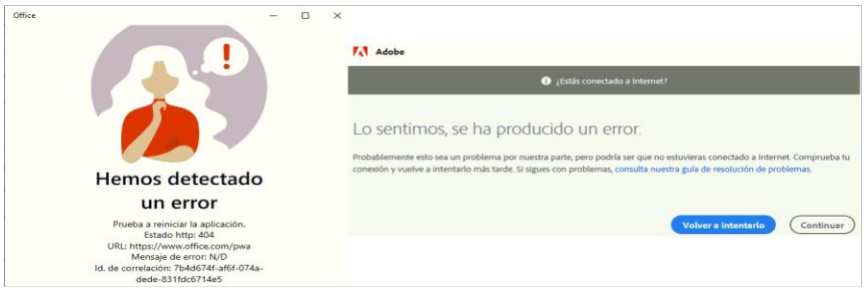


Figura 3.17. Bloqueo de Aplicaciones.

Dentro del perfil de Control de Aplicaciones, existe una categoría llamada ***Collaboration***, la misma que se habilita para tener acceso a las aplicaciones como Office365 y Adobe como se muestra en la figura 3.18. También se pueden crear filtros para habilitar solo ciertas aplicaciones y no toda la categoría; de esta manera se pueden controlar las aplicaciones a las que pueden tener acceso los usuarios.

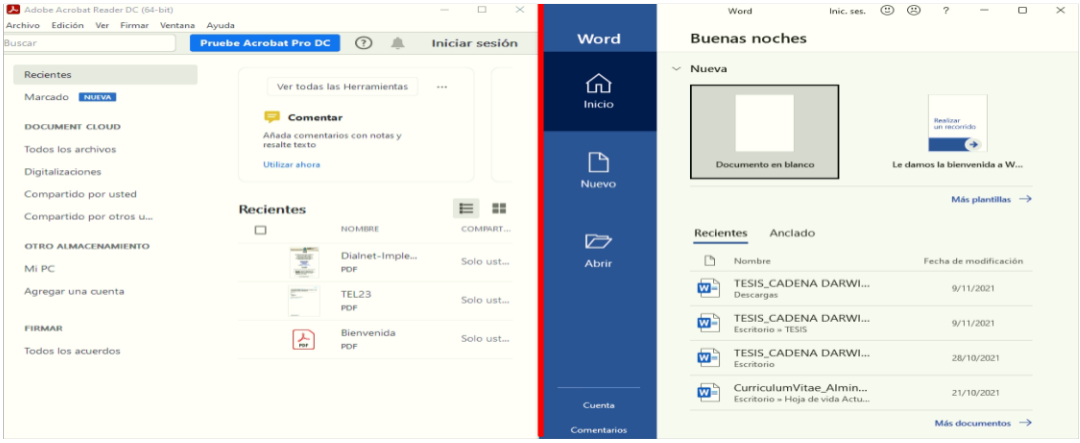


Figura 3.18. Acceso a Adobe y Office365.

3.1.3.4 Sistema de Prevención de Intrusos (IPS)

El IPS creado para este proyecto, brinda protección a los usuarios con sistema operativo Windows que intenten conectarse hacia sitios Botnet[1] y que puedan exponer a la red, bloqueando IPs y URL maliciosas con severidad media, alta y crítica.

Para las pruebas no se tiene conocimiento exacto de una IP o URL con Botnet, pero al tener habilitado el perfil de seguridad IPS, el *firewall* FortiGate bloqueará automáticamente la conexión a estos sitios cuando un usuario intente acceder. Para ello Fortinet dispone de una base de datos con aproximadamente 2349 IP que posiblemente contienen Botnet para ser bloqueados de manera inmediata. En la figura 3.19 se puede observar un mapa donde se encuentra distribuido geográficamente ***Mirai***, uno de los Botnet más grandes de todos los tiempos y responsable de los mayores ataques DDoS y que se propaga por fuerza bruta infectando en su mayoría a cámaras y dispositivos inteligentes conectados a Internet.

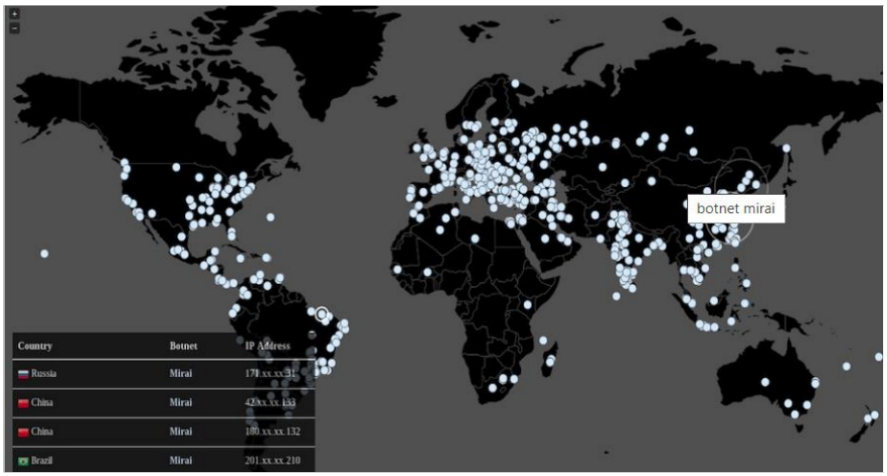


Figura 3.19. Distribución Geográfica de Botnet *Mirai* [44].

3.1.3.5 Denegación de Servicios (DoS)

Los perfiles DoS se encargan de proteger a la red ante ataques de cibercriminales o *hackers*, que ocasionan la indisponibilidad de los servicios y de la red. Para esto se habilita el perfil con la finalidad de detectar inundaciones principalmente de paquetes TCP, UDP e ICMP desde un mismo usuario o *hacker*; el *firewall* al detectar que se sobrepasa el umbral predeterminado de paquetes en la configuración, procederá con el bloqueo automático evitando que se consuman recursos de memoria RAM, ROM, puerto o periféricos de los servidores, PC de los usuarios o recursos de ancho de banda de la red.

[1] Botnet: Método utilizado por cibercriminales para lanzar ataques de DDoS, enviar correos no deseados como SPAM, detectar contraseñas o distribuir *rasonmware*.

Durante la implementación del proyecto, no se detectó ningún ataque externo que sature los recursos de la red para las pruebas, por lo que se deja habilitado la política de DoS, ya que es imprescindible proteger cuando un *hacker* realice un ataque y es mejor estar preparado. Existen empresas dedicadas a brindar soluciones de protección frente a ataques DoS; Fortinet con su *NGFW*, incorpora políticas para prevenir y mitigar este tipo de ataques sin necesidad de un dispositivo adicional.

3.1.3.6 Acceso Remoto VPN-SSL

En la siguiente sección se comprueba el acceso remoto a los servicios internos en la red utilizando una VPN de conexión segura habilitada en la Sede Central Quito. La conexión se realiza a través de la App FortiClient desde una red diferente; como se muestra en la figura 3.18, solo se tiene acceso a los servicios de correo con IP 192.168.100.100 y contenido multimedia de IP 192.168.200.200. Al realizar un *tracert*, se valida en ambos casos que el siguiente salto es la IP 190.12.33.194, IP pública asociada a Quito y posteriormente el salto a cada IP del servidor. El cliente remoto no tendrá acceso a otras IPs de la red interna; si desean navegar por Internet, lo harán por su propio proveedor de Internet, esto para no utilizar los recursos de ancho de banda de la Sede Central Quito.

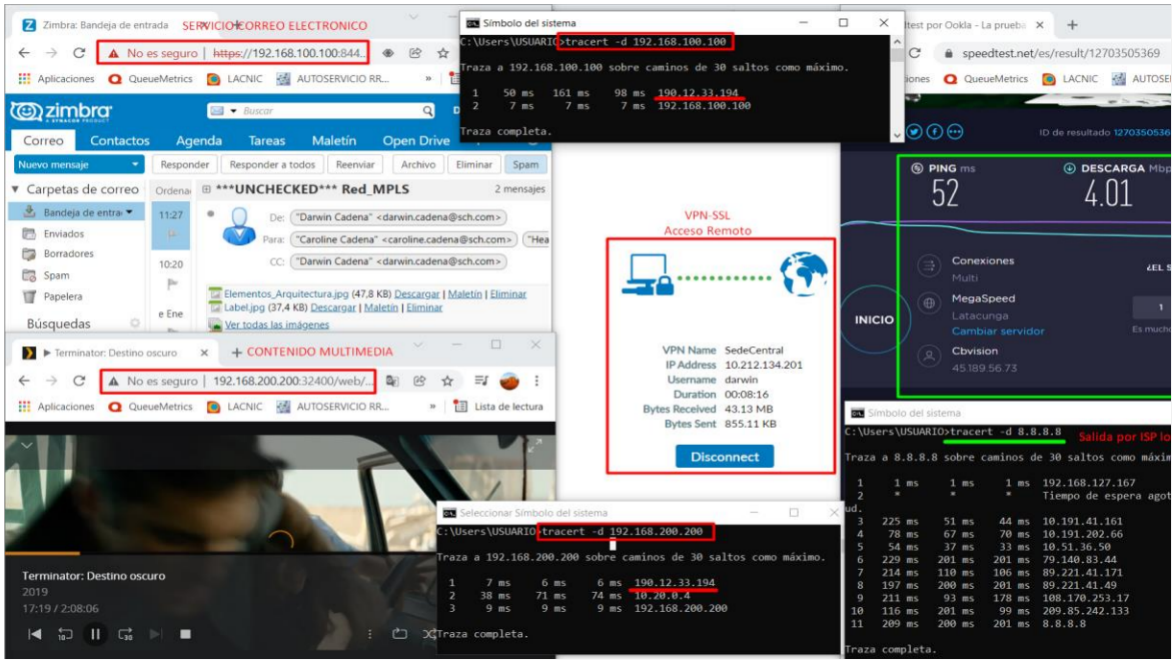


Figura 3.18. Acceso remoto VPN-SSL.

3.1.4 FORTIMANAGER PARA EL CONTROL DE LA SD-WAN

3.1.4.1 Control Centralizado de la Red

A través de FortiManager, se puede administrar, monitorear y controlar la red de forma centralizada desde un único panel. Desde el ADOM ***PRUEBAS_PYMES*** en FortiManager

de Puntonet, se accede digitando la URL https://consola.fortimanager.puntonet.ec como se muestra en la figura 3.19, a la administración de los 3 dispositivos FortiGate. Desde aquí se puede crear, modificar o eliminar políticas y reglas SD-WAN, túneles IPSec, políticas de Seguridad, crear *scripts*, actualizar *firmwares* y acceder a una de las funciones principales que es el aprovisionamiento de toque cero (ZTP) para incorporar nuevos dispositivos.

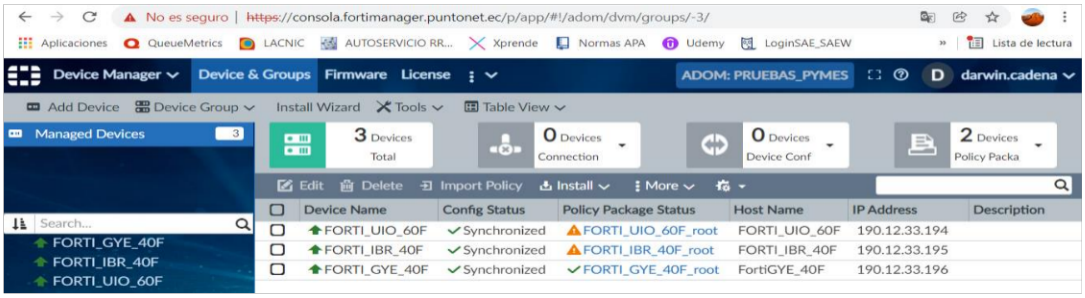


Figura 3.19. Panel de administración en FortiManager.

Desde el panel de Control de FortiManager se puede visualizar el conjunto de políticas configuradas para la Sede Central Quito como se muestra en la figura 3.20, así como también de la Sede Ibarra y Guayaquil, desde donde se puede agregar, actualizar o eliminar cualquier política. FortiManager guarda las políticas en una base de datos general, pero al querer configurar una política lo hará de forma independiente en cada FortiGate.

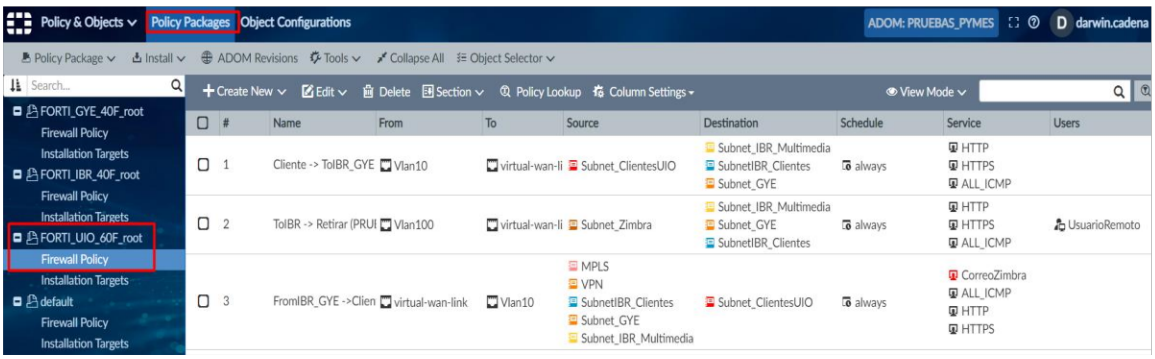


Figura 3.20. Políticas administradas desde FortiManager.

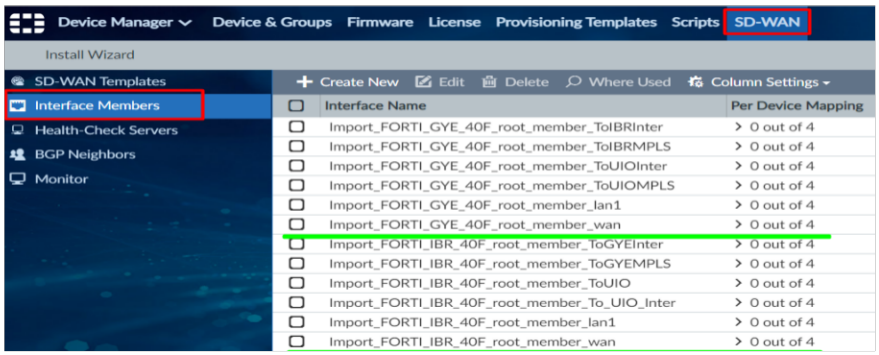


Figura 3.21. Miembros de la SD-WAN desde FortiManager.

De igual manera FortiManager tiene la funcionalidad SD-WAN, para incorporar las interfaces físicas o túneles IPSec que serán miembros de la SD-WAN para cada uno de los dispositivos, tal como se muestra en la figura 3.21.

FortiManager proporciona el monitoreo y validación del consumo de ancho de banda de las interfaces y túneles IPSec que son miembros de la SD-WAN, manteniendo la QoS en base a los SLA de cada FortiGate como se muestra en la figura 3.22.

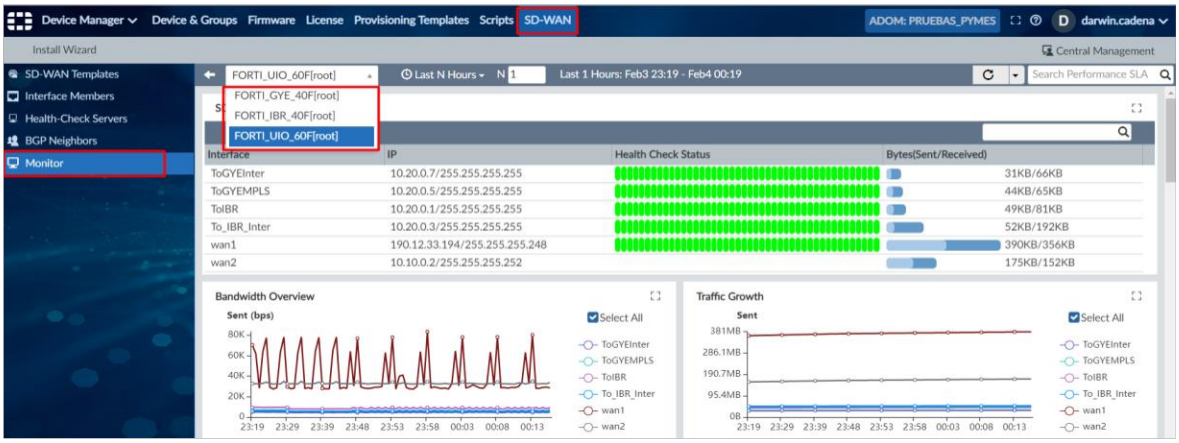


Figura 3.22. Monitoreo de la SD-WAN desde FortiManager.

FortiManager permite crear, eliminar o actualizar perfiles de Seguridad como Antivirus, *Web Filter, Application Control, Intrusion Prevention*, como se muestra en la figura 3.23. La configuración se realiza en cada perfil de forma general, para luego asociarla o instalar los cambios de forma independiente en cada FortiGate.

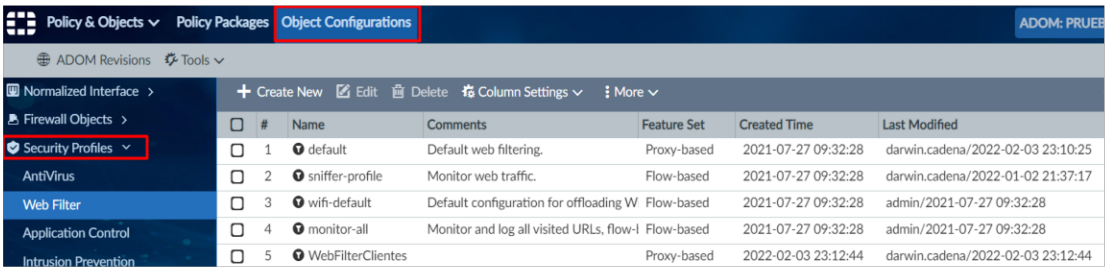


Figura 3.23. Perfiles de Seguridad desde FortiManager.

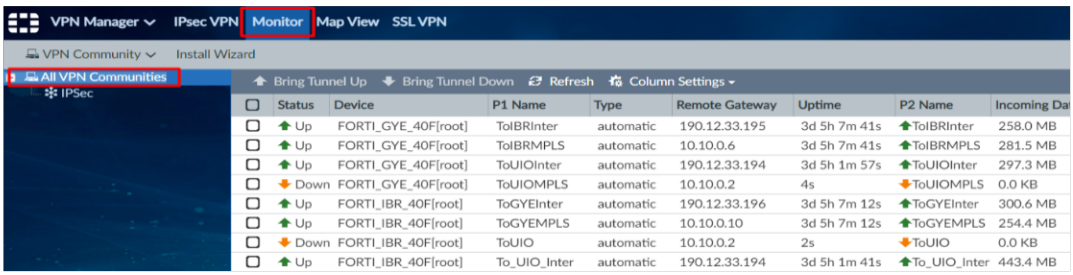


Figura 3.24. Túneles IPSec desde FortiManager.

El Centro de Control FortiManager también admite crear, eliminar o modificar túneles IPSec como se muestra en la figura 3.24, De igual manera permite monitorear cada uno de los túneles, el estado *up/down* en que se encuentran y su tiempo de actividad entre otros.

FortiManager configura de forma centralizada la VPN-SSL para el acceso remoto de los usuarios, permitiendo la creación de usuarios que tendrán acceso a la VPN. En la figura 3.25 se comprueba el acceso de los usuarios remotos mediante el monitoreo que FortiManager realiza a la VPN, dejando un histórico de las conexiones realizadas.

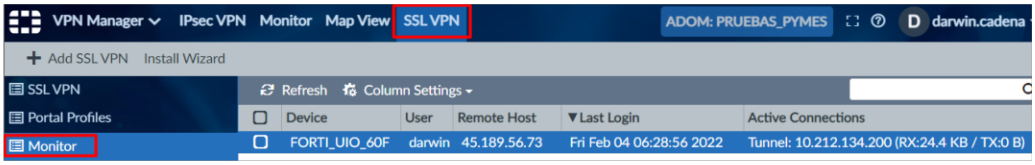


Figura 3.25. VPN-SSL desde FortiManager.

3.1.4.2 Zero-Touch Provisioning (ZTP)

Una de las funcionalidades importantes que Fortinet incorpora a través de FortiManager es la implementación y configuración de dispositivos desde cero, de manera remota, esto es sin necesidad de la presencia de un administrador en sitio. Adicionalmente, ZTP permite utilizar las configuraciones de dispositivos ya asociados para crear plantillas de aprovisionamiento y *scripts* para nuevos dispositivos, facilitando la escalabilidad de las empresas, reducción en tiempos de implementación y de costos. Como ejemplo, en la figura 3.26, se incorpora la Sucursal Riobamba, en la que se muestra la asociación del FortiGate en el FortiManager a través del *serial number*; con esto se pueden agregar dispositivos, configurarlos y enviarlos al sitio para su instalación e incorporación inmediata.

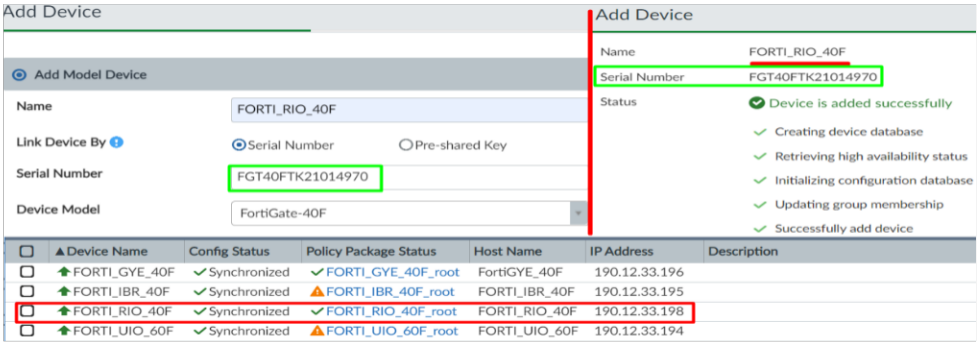


Figura 3.26. FortiGate-Riobamba agregado en FortiManager

3.1.4.2.1 Plantillas de Aprovisionamiento

Mediante las plantillas de aprovisionamiento se pueden configurar dispositivos desde cero, de forma masiva, validando el ZTP, siempre que tengan configuraciones comunes. Para la siguiente prueba se crea la plantilla para cambiar ciertos parámetros de la configuración

por defecto en el FortiGate de la Sucursal Riobamba con IP 190.12.33.198. En la figura 3.27 se detallan los parámetros comunes a ser cambiados y aplicados desde FortiManager como el puerto *https* de acceso del 443 al 4434, los DNS FortiGuard por defecto a los DNS de Google y el tema de color verde a un tema obscuro como se muestra en la figura 3.28.

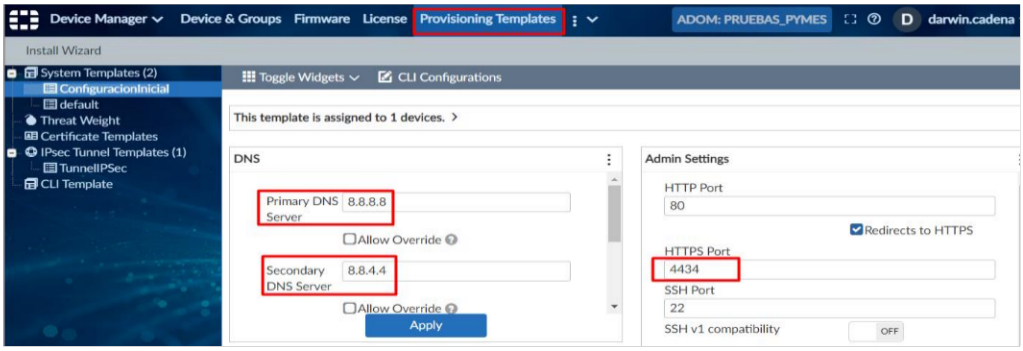


Figura 3.27. Plantillas de Aprovisionamiento desde FortiManager.

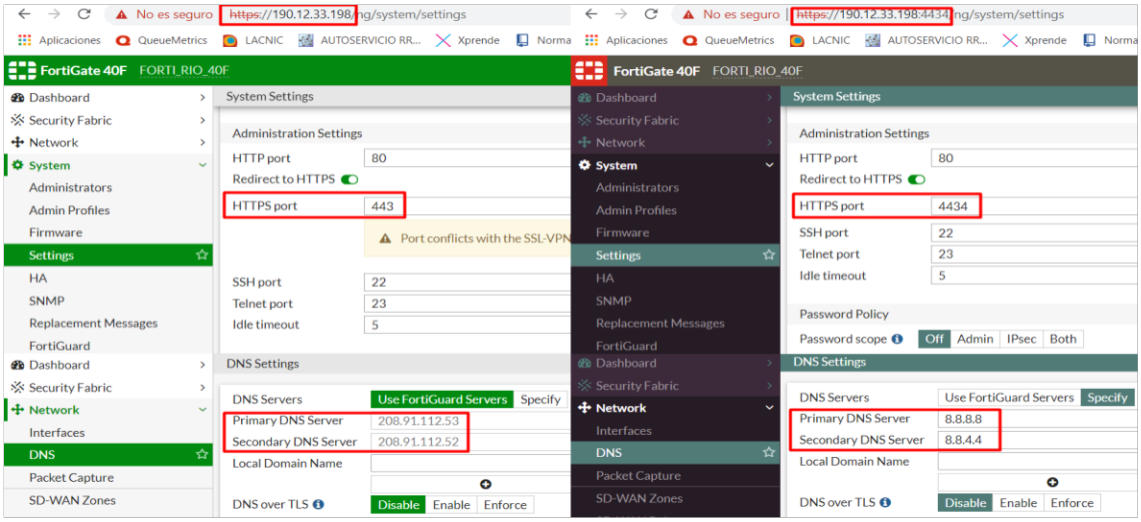


Figura 3.28. Cambio aplicado desde FortiManager.

Las configuraciones que no son comunes y que se deben hacer en cada FortiGate, puede realizarse configurando en la base de FortiManager de forma general para instalar en cada FortiGate de forma personalizada. De esta manera se facilita la administración de los dispositivos y de la red utilizando un único panel de control.

3.2 CONCLUSIONES

A partir de los resultados obtenidos en el desarrollo del prototipo de la SD-WAN se concluye que se ha cumplido plenamente el objetivo general y los objetivos específicos propuestos.

Muchas empresas conectan sus sitios a través de una MPLS a un concentrador para acceder a los servidores y permitir la navegación por un solo enlace a Internet; con la

incorporación de las SDN el esquema de la red cambia radicalmente, su implementación es fácil, de bajo costo, trabaja sobre WAN existentes y conserva su infraestructura actual.

Para el proyecto se implementó la red de acceso a Internet y la red MPLS, obteniendo una SD-WAN híbrida; mediante las pruebas y resultados, esta SD-WAN híbrida, ofrece mejores funcionalidades que la MPLS optimizando el rendimiento de la red; considerando que la red MPLS es una red privada que no atraviesa por el tráfico que se genera en Internet. Para mejorar este limitante, se incorporan túneles IPSec en ambos enlaces WAN, mejorando el rendimiento, la latencia y lo más importante, se brinda seguridad a través del cifrado de la información.

En el prototipo desarrollado, Fortinet ha permitido monitorear los túneles de la SD-WAN en tiempo real, al igual que ha permitido seleccionar dinámicamente la ruta y ver la funcionalidad del *failover,* lo que ha llevado a mejorar la disponibilidad a un valor del 99.9%.

En la red diseñada e implementada se ha verificado que el balanceo de carga, permite la distribución de carga de acuerdo al ancho de banda asignado por las políticas de Traffic Shaping, convirtiendo a la SD-WAN híbrida en una red inteligente y con autonomía propia.

A partir del prototipo SD-WAN desarrollado y de los resultados obtenidos, se ha observado la gran ventaja que tiene este tipo de redes, al permitir desde el panel central de FortiManager monitorear y establecer reglas o políticas de manera general, para luego ser aplicadas de forma individual en cada dispositivo de las sedes.

La funcionalidad de ZTP se puso en manifiesto al incorporar la nueva sede Riobamba, sin necesidad de un administrador en sitio, apoyándose con plantillas de aprovisionamiento, *scripts* y de las mismas configuraciones de los dispositivos asociados, permitiendo reducir el tiempo de implementación de la nueva sede.

Este trabajo de integración curricular ha permitido reforzar y adquirir conocimientos en una nueva tecnología WAN, así como desarrollar destrezas en configuración de equipos Cisco y Fortinet. Al mismo tiempo se considera que este trabajo podrá servir de guía a estudiantes de la FIEE que deseen trabajar con esta tecnología y con equipos de otros fabricantes.

3.3 RECOMENDACIONES

Se recomienda disponer del licenciamiento FortiGuard en los FortiGate para acceder a los perfiles de Seguridad y así relacionarse correctamente (*match*) con la base de datos de los servidores FortiGuard. Adicionalmente es importante asociar DNS FortiGuard con una latencia menor a los 90 ms, para que siempre se realice el *match* y las políticas de

seguridad funcionen adecuadamente de acuerdo a las configuraciones; caso contrario, al no alcanzar los DNS, se entrará en conflicto y se bloquearán las políticas de seguridad.

Cuando se aplican las políticas del *firewall*, reglas SD-WAN, políticas de *Traffic Shaping*, se recomienda seguir un orden descendente, en donde la política o regla que menos peso tiene, debe ser ubicada en la parte superior, para terminar con la política o regla de mayor peso en la parte inferior, que permita o niegue todo.

Cuando se configura la VPN-SSL para el acceso remoto, es recomendable solo dar acceso a los servicios de la red; si el usuario remoto desea navegar por Internet, los FortiGate tiene la opción para que navegue por su propio proveedor de Internet, de esta manera no se utilizarán los recursos de la Sede, no se satura el canal y no es necesario realizar un *upgrade* del ancho de banda de la red de acceso a Internet.

Los datos o información son muy importantes para una empresa, por lo que es recomendable virtualizar los servidores, esto provee seguridad y permite realizar respaldos periódicamente de la información sin interrumpir los servicios en la red.

Para asociar dispositivos en los FortiManager, es importante colocar la IP de la ubicación del FortiManager en el FortiGate, en el menú *Fabric Connectors*; luego se debe aprobar la asociación en el FortiManager; si no se realiza esta gestión, se tendrán errores al querer realizar cualquier modificación desde FortiManager.

Es recomendable instalar los certificados *Fortinet_CA_SSL* en los dispositivos de la LAN, para que funcione adecuadamente el acceso a páginas Web y solo a sitios seguros; si no se instala, bloqueará cualquier página al aplicar la Inspección SSL en el *firewall*.

Se recomienda la instalación de Antivirus en los dispositivos de la LAN; si bien los *firewalls* brindan protección hacia la red de Internet, también se pueden infectar dentro de la LAN mediante memorias USB, discos duros externos, transferencia de información, archivos adjuntos en los correos de la intranet, descarga de contenido multimedia, entre otros.

La implementación de una SD-WAN también se la puede emular mediante software, para el caso de la facultad en la que no se dispone de los equipos necesarios en el laboratorio, se recomienda incorporar computadoras con procesadores i7 y memoria RAM de 12 GB como mínimo. Estos equipos permitirán acceder e implementar redes SD-WAN sobre el software GNS3 u otro software similar, involucrando prácticas para desarrollar el conocimiento y las destrezas relacionadas con redes MPLS, red de acceso a Internet, SD-WAN, virtualización de servidores, seguridad; e incorporar otros fabricantes que existen en el mercado, preparando al estudiante de mejor manera para el mundo laboral y profesional.

4 REFERENCIAS BIBLIOGRÁFICAS

[1] Julio Saiz, B., 2021. Redes SD-WAN, características y beneficios. [online] Blog.alhambrait.com. Available at: <https://blog.alhambrait.com/redes-sd-wan-caracteristicas-y-beneficios> [Accessed 10 September 2021].

[2] Blog de noticias | Optical Networks. 2021. ¿Qué es la red MPLS y cómo funciona?. [online] Available at: <https://www.optical.pe/blog/que-es-una-red-mpls/> [Accessed 13 September 2021].

[3] Cloud Computing | Adaptix Networks | Cómputo en la Nube. 2021. Dirección IP Privada, Pública, Dinámica, Estática. [online] Available at: <https://www.adaptixnetworks.com/direccion-ip/> [Accessed 19 September 2021].

[4] VMware. 2021. Virtualization Technology & Virtual Machine Software: What is Virtualization?.[online] Available at: <https://www.vmware.com/latam/solutions/virtualization.html> [Accessed 14 August 2021].

[5] [6] Fernández, Y., 2021. Plex, qué es y cómo funciona. [online] Xataka.com. Available at: <https://www.xataka.com/basics/plex-que-es-y-como-funciona> [Accessed 18 September 2021].

[6] Fortinet. 2021. *¿Qué es la SD-WAN? Soluciones WAN definidas por software | Fortinet*. [online] Available at: <https://www.fortinet.com/lat/products/sd-wan> [Accessed 5 August 2021].

[7] Fortinet. 2021. *Administración de panel único basada en la automatización*. [online] Available at: <https://www.fortinet.com/lat/products/management/fortimanager> [Accessed 19 September 2021].

[8] Huidobro Moya, J. and Millán Tejedor, R., 2002. [online] Ramonmillan.com. Available at: <https://www.ramonmillan.com/documentos/mpls.pdf> [Accessed 8 October 2021].

[9] Tlm.unavarra.es. 2021. [online] Available at: <https://www.tlm.unavarra.es/~daniel/docencia/rba/rba06_07/trabajos/resumenes/gr14-MPLSEnLinux.pdf> [Accessed 9 October 2021].

[10] TechClub Tajamar. 2021. *Red MPLS - TechClub Tajamar*. [online] Available at: <https://techclub.tajamar.es/red-mpls/> [Accessed 17 October 2021].

[11] Grass, M., 2021. [online] Biblioteca.unlpam.edu.ar. Available at: <http://www.biblioteca.unlpam.edu.ar/rdata/tesis/i_grared578_c.pdf> [Accessed 3 November 2021].

[12] HdezF, G., 2019. *Conociendo la arquitectura básica de una red MPLS - Comunidad Huawei Enterprise*. [online] Comunidad Huawei Enterprise. Available at: <https://forum.huawei.com/enterprise/es/conociendo-la-arquitectura-b%C3%A1sica-de-una-red-mpls/thread/582304-100237> [Accessed 21 October 2021].

[13] Valenzuela, R., n.d. *Multi-Protocol Label Switching. Ing. Román Valenzuela - PDF Free Download*. [online] Docplayer.es. Available at: <https://docplayer.es/3157020-Multi-protocol-label-switching-ing-roman-valenzuela.html> [Accessed 15 November 2021].

[14] Veá Baró, A., 2002. *EVOLUCIÓN DE LA TECNOLOGÍA DE ACCESO A INTERNET*. [online] Tdx.cat. Available at: <https://www.tdx.cat/bitstream/handle/10803/9156/Tavb06de23.pdf?> [Accessed 3 November 2021].

[15] Viavisolutions.com. 2021. *Red óptica pasiva (PON) | VIAVI Solutions Inc.*. [online] Available at: <https://www.viavisolutions.com/es-es/red-optica-pasiva-pon> [Accessed 15 November 2021].

[16] Huidobro, J., 2014. Acceso de banda ancha a Internet. [online] Acta.es. Available at: <https://www.acta.es/medios/articulos/internet/026001.pdf> [Accessed 7 November 2021].

[17] eConectia. 2017. *Tipos de conexiones a Internet. ¿Cuál te conviene más?*. [online] Available at: <https://www.econectia.com/blog/tipos-de-conexiones-a-internet-cual-te-conviene-mas> [Accessed 16 November 2021].

[18] Miray Consulting. 2021. *SD-WAN - Definición, funcionamiento y ventajas de la red del futuro | Blog Miray*. [online] Available at: <https://www.mirayconsulting.com/sd-wan-definicion-funcionamiento-y-ventajas-de-la-red-del-futuro/> [Accessed 7 November 2021].

[19] axessnet. 2021. *SD-WAN: ¿Para qué sirve y cuáles son sus ventajas frente a la WAN?*. [online] Available at: <https://axessnet.com/sd-wan-para-que-sirve-y-cuales-son-sus-ventajas-frente-a-la-wan-tradicional/> [Accessed 7 November 2021].

[20] MTnet. 2018. *¿Qué es una Software Defined WAN y cuáles son las ventajas para tu infraestructura? - MTnet*. [online] Available at: <https://www.mtnet.com.mx/que-es-

una-software-defined-wan-y-cuales-son-las-ventajas-para-tu-infraestructura/> [Accessed 16 November 2021].

[21] TAIGA CONSULTING S.A. 2021. *TIPOS DE ARQUITECTURA SD-WAN*. [online] Available at: <https://www.taiga-consulting.com/blog/tecnologia-de-la-informacion-1/tipos-de-arquitectura-sd-wan-1> [Accessed 7 November 2021].

[22] CARRILLO, Á. and IVONNE RONCANCIO, I., 2020. *DISEÑO DE RED PARA LA INTEGRACIÓN DE SEDES TIPO MARKET DE UNA EMPRESA DE PRODUCCIÓN Y COMERCIALIZACIÓN DE ALIMENTOS BASADO EN CONECTIVIDAD SDWAN*. [online] Repositorio.unbosque.edu.co. Available at: <https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/4269/Carrillo_Hernandez_%C3%81lvaro_Javier_2020.pdf?sequence=1&isAllowed=y%3E> [Accessed 10 November 2021].

[23] Jennings, J., 2019. *Traditional WAN vs. SD-WAN: Here's What You Need to Know*. [online] Burwood Group. Available at: <https://www.burwood.com/blog-archive/traditional-wan-vs-sd-wan-heres-what-you-need-to-know> [Accessed 20 November 2021]

[24] Sanchez, D., 2020. *Aruba SD-WAN Dynamic Path Steering with SLA*. [online] Aruba. Available at: <https://www.arubanetworks.com/resource/aruba-sd-wan-dynamic-path-steering-with-sla/> [Accessed 22 November 2021].

[25] Irei, A., 2021. *¿Qué es WAN definida por software o SD-WAN? - Definición en WhatIs.com*. [online] ComputerWeekly.es. Available at: <https://www.computerweekly.com/es/definicion/WAN-definida-por-software-o-SD-WAN> [Accessed 21 November 2021].

[26] RO, C., 2021. *REDES BASADAS EN SOFTWARE COMO ESQUEMA DE CONECTIVIDAD Y ADMINISTRACION WAN EN ENTORNOS CORPORATIVOS*. [online] Repository.unad.edu.co. Available at: <https://repository.unad.edu.co/bitstream/handle/10596/40124/ce11luq354.pdf?sequence=3> [Accessed 7 November 2021].

[27] Craven, C., 2020. *What Is SD-WAN Security? Definition*. [online] sdxcentral. Available at: <https://www.sdxcentral.com/networking/sd-wan/definitions/what-is-sd-wan-security/> [Accessed 21 November 2021].

[28] Robles, M., n.d. VIRTUALIZACION DE SERVIDORES CON VMWARE. [online] Usmp.edu.pe. Available at: <https://www.usmp.edu.pe/vision2017/pdf/materiales/VIRTUALIZACION_DE_SERVIDORES_CON_VMWARE.pdf> [Accessed 21 November 2021].

[29] Olivencia, R., 2016. *Creando un sistema de correo profesional con Zimbra (2/2): Configuración*. [online] Blog Irontec. Available at: <https://blog.irontec.com/crear-sistema-de-correo-profesional-con-zimbra-ii/> [Accessed 21 November 2021].

[30] Zimbra-support.net. n.d. *Zimbra Support*. [online] Available at: <https://www.zimbra-support.net/index.php/es/> [Accessed 21 November 2021].

[31] Fernández, I., 2020. *Qué es el servidor DNS: todo lo que necesitas saber*. [online] El blog de Orange. Available at: <https://blog.orange.es/red/que-es-el-servidor-dns/> [Accessed 22 November 2021].

[32] Delteil, P., 2019. *Cómo montar un servidor DNS malicioso*. [online] Medium. Available at: <https://medium.com/hacking-info-sec/c%C3%B3mo-montar-un-servidor-dns-malicioso-29fc939bc741> [Accessed 22 November 2021].

[33] Aragón, D., 2016. *Plex: qué es y para qué sirve*. [online] Qloudea Blog Especialistas en servidores NAS. Available at: <https://qloudea.com/blog/que-es-plex-para-que-sirve-plex/> [Accessed 23 November 2021]. Plex Support. 2021. *What is Plex?* | *Plex Support*. [online] Available at: <https://support.plex.tv/articles/200288286-what-is-plex/> [Accessed 22 November 2021].

[34] Plex Support. 2021. *What is Plex?* | *Plex Support*. [online] Available at: <https://support.plex.tv/articles/200288286-what-is-plex/> [Accessed 22 November 2021].

[35] Web.archive.org. 2016. *Fortinet, Inc. - Annual Report*. [online] Available at: <https://web.archive.org/web/20170409021208/http://investor.fortinet.com/secfiling.cfm?filingID=1262039-17-8&CIK=1262039> [Accessed 10 November 2021].

[36] Fortinet.com. 2021. *Fortinet Secure SD-WAN*. [online] Available at: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet_secure_sdwan.pdf> [Accessed 14 November 2021].

[37] Fortinet. 2021. *FortiOS: el sistema operativo de Security Fabric para permitir la transformación digital*. [online] Available at: <https://www.fortinet.com/lat/products/fortigate/fortios> [Accessed 22 November 2021]

[38] Quanti Solutions. 2021. *FortiGate: Conociendo el Firewall*. [online] Available at: <https://quanti.com.mx/articulos/conociendo-el-firewall-fortigate/> [Accessed 16 November 2021].

[39] Docs.fortinet.com. 2021. *FortiManager | Fortinet Documentation Library*. [online] Available at: <https://docs.fortinet.com/product/fortimanager/7.0> [Accessed 19 November 2021].

[40] Fortinet. 2021. *Administración de panel único basada en la automatización*. [online] Available at: <https://www.fortinet.com/lat/products/management/fortimanager> [Accessed 19 November 2021].

[41] Help.fortinet.com. n.d. *FortiManager Architecture*. [online] Available at: <https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FortiManager_Admin_Guide/0300_FMG_architecture/0000_FMG_architecture.htm> [Accessed 23 November 2021].

[42] Noction. 2018. BGP / MPLS Layer3 VPNs | Noction. [online] Available at: <https://www.noction.com/blog/bgp-mpls-layer3-vpns> [Accessed 10 January 2022].

[43] Salcedo, O., Pedraza, L. and Espinosa, M., 2012. Evaluación de redes MPLS/VPN/BGP con rutas reflejadas. [online] Scielo.org.co. Available at: <http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2012000200010> [Accessed 10 January 2022].

[44] 1000 Tips Informáticos. 2021. *Mira el mapa que muestra los ataques en vivo de "Mirai"*. [online] Available at: <https://www.1000tipsinformaticos.com/2016/10/mira-el-mapa-que-muestra-los-ataques-en-vivo-de-mirai.html> [Accessed 1 February 2022].

5 ANEXOS

ANEXO I. DATASHEET DE EQUIPOS UTILIZADOS EN LA IMPLEMENTACIÓN DEL PROTOTIPO DE LA SD-WAN.

ANEXO II. MANUAL DE INSTALACIÓN SERVIDOR DNS, SERVIDOR DE CORREO ZIMBRA Y PLEX MEDIA SERVER.

ANEXO III. DETALLES DE LA CONFIGURACIÓN E IMPLEMENTACIÓN DE LA SD-WAN.

ANEXO IV. CONFIGURACIÓN DE LOS ROUTERS CISCO DE LA RED MPLS, RED DE ACCESO A INTERNET, RED LAN Y FIREWALL FORTIGATE.

ANEXO V. VIDEO DEL PRODUCTO FINAL DEMOSTRABLE.

ANEXO I

DATASHEET DE EQUIPOS UTILIZADOS EN LA IMPLEMENTACIÓN DEL PROTOTIPO DE LA SD-WAN

ÍNDICE DE CONTENIDO

CISCO2811 Datasheet

Get a Quote

Overview

The Cisco 2800 Series provides significant additional value compared to prior generations of Cisco routers at similar price points by offering up to a fivefold performance improvement, up to a tenfold increase in security and voice performance, new embedded service options, and dramatically increased slot performance and density while maintaining support for most of the more than 90 existing modules that are available today for the Cisco 1700, Cisco 2600, and Cisco 3700 Series.The Cisco 2800 Series features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1/xDSL connections. The routers offer embedded encryption acceleration and on the motherboard voice digital-signal-processor (DSP) slots; intrusion prevention system (IPS) and firewall functions; optional integrated call processing and voice mail support; high-density interfaces for a wide range of connectivity requirements; and sufficient performance and slot density for future network expansion requirements and advanced applications.

Cisco 2811 Router 2800 Series ISR	
Manufacturer	Cisco Systems, Inc
Manufacturer Part Number	CISCO2811
Product Type	Cisco 2811 Router
Form Factor	External - modular - 1U
Dimensions (WxDxH)	43.8 cm x 41.7 cm x 4.5 cm
Weight	6.4 kg
DRAM Memory	512 MB (installed) / 768 MB (max) - DDR SDRAM
Flash Memory	128 MB (installed) / 256 MB (max)
Data Link Protocol	Ethernet, Fast Ethernet
Network / Transport Protocol	IPSec
Remote Management Protocol	SNMP 3
Features	Cisco IOS IP Base , modular design, firewall protection, hardware encryption, VPN support, MPLS support, wall mountable, Quality of Service (QoS)
Compliant Standards	IEEE 802.3af, IEEE 802.1x
Power	AC 120/230 V (50/60 Hz)

Specification

CISCO2811 data sheet	
Manufacturer	Cisco Systems, Inc
Manufacturer Part Number	CISCO2811
Product Type	Router
Form Factor	Desktop - modular - 1U

Connectivity Technology	Wired
Data Link Protocol	Ethernet, Fast Ethernet
Network / Transport Protocol	IPSec
Remote Management Protocol	SNMP 3
Encryption Algorithm	DES, Triple DES, SSL 3.0, 128-bit AES, 192-bit AES, 256-bit AES
Authentication Method	Secure Shell v.2 (SSH2)
Features	Modular design, firewall protection, hardware encryption, VPN support, MPLS support, wall mountable, Quality of Service (QoS)
Compliant Standards	IEEE 802.3af, IEEE 802.1x
DRAM Memory	512 MB (installed) / 768 MB (max) - DDR SDRAM
Flash Memory	128 MB (installed) / 256 MB (max)
Status Indicators	Link activity, power
Connectivity Slots	
Interfaces	USB : 2 x 2 x 10Base-T/100Base-TX - RJ-45 Management : 1 x console - RJ-45 Serial : 1 x auxiliary - RJ-45
Expansion Slot(s)	4 (total) / 4 (free) x HWIC 1 (total) / 1 (free) x NME 2 (total) / 2 (free) x AIM 2 (total) / 2 (free) x PVDM - SIMM 80-PIN 2 memory 1 (total) / 0 (free) x CompactFlash Card
Power	
Power Device	Power supply - internal
Voltage Required	AC 120/230 V (50/60 Hz)
Dimensions / Weight / Miscellaneous	
Width	43.8 cm
Depth	41.7 cm
Height	4.5 cm
Weight	6.4 kg
Compliant Standards	CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, FCC Part 15, ICES-003 Class A, EN 61000-6-2, FIPS 140-2, EN300-386, EN 60950-1
System Software	
OS Provided	Cisco IOS IP Base

Download Resource

Transition Guide

Guide to Upgrade Your ISR G1 and ISR G2 Routers to ISR 4000

Want to Buy

Order Now | Get a Quote

Why Router-switch.com

As a leading network hardware supplier, Router-switch.com focuses on original new ICT equipment of Cisco, Huawei, HPE, Dell, Hikvision, Juniper, Fortinet, etc.

200+	18,000+	$20,000,000	50%-98%	100%
Countries we Sold	Customers Trusted	Inventory Available	Off Global List Price	Safe Online Shopping

Contact Us

- Tel: +1-626-239-8066 (USA) 852-30691898/ 852-30691868 (Hong Kong)
- Fax: 852-30691898 (Hong Kong)
- Email: sales@router-switch.com

C1111-8P Datasheet

Get a Quote

Router-Switch.com
Leading Network Hardware Supplier

Overview

Cisco 1100 Series Integrated Services Router (ISRs) delivers Cisco IOS® XE Software, providing WAN, comprehensive security, wired and wireless access in a single, high-performance platform. Cisco 1100 Series ISR is ideal for Small and Medium enterprise branch offices. The C1111-8P is the ISR 1100 8 Ports Dual GE WAN Ethernet Router, delivering 1 WAN port and 8GE LAN ports.

Quick Spec

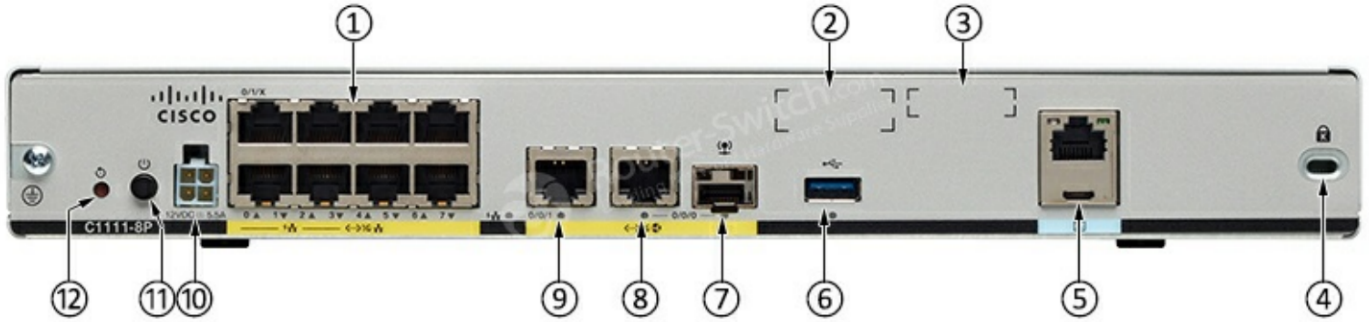
Figure 1 shows the appearance of C1111-8P.

Table 1 shows the quick spec.

Model	C1111-8P
GE	1
GE/SFP combo	1
ADSL2/VDSL2+	N/A
LTE Advanced (CAT6)	N/A
802.11ac	N/A
GE	8
PoE	4
PoE+	2
Integrated USB 3.0 AUX/console	Yes
Dimensions (H x W x D)	1.75 x 12.7 x 9.03 in. (42 x 323 x 230mm) (includes rubber feet)
Weight with AC PS (w/o modules)	5.5 Lbs. (2.5 kg) maximum

Product Details

Figure 2 shows the back ports of C1111-8P. It doesn't include the antennas.



Note:

(1)	LAN	(7)	GE 0/0/0 - SFP
(2)	CLEI Label	(8)	GE 0/0/0 - RJ45
(3)	Serial Number	(9)	GE 0/0/1
(4)	Kensington Lock Slot	(10)	4-pin Power Connector
(5)	RJ45 / Micro USB Console	(11)	Power Switch
(6)	USB3.0	(12)	Reset Button

Table 2 shows the business benefits.

Business need	**Features/description**
Lightweight, compact size with low power consumption	●Can be deployed in many different environments where space, heat dissipation, and low power consumption are critical factors.
High performance to run concurrent services	●High performance allows customers to take advantage of broadband network speeds while running secure, concurrent data, voice, video, and wireless services.
High availability and business continuity	● Redundant WAN connections for failover protection and load balancing. ● Dynamic failover protocols such as Virtual Router Redundancy Protocol (VRRP; RFC 2338), Hot Standby Router Protocol (HSRP), and Multigroup HSRP (MHSRP).
Consistent, high application performance levels	● The router can run multiple services simultaneously with minimal performance degradation.
Risk mitigation with multilevel security	● Network perimeter security with integrated application inspection firewall. ● Data privacy through high-speed IP Security (IPsec) Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) encryption. ● High-performance VPNs: DMVPN, FlexVPN, GET VPN, EzVPN ● Cisco Umbrella™ security architecture to provide content filtering via category-based URL classification and blocking, thus helping increase productivity and providing better use of company resources. ● Enforced security policy with OpenDNS. ● Security hardware acceleration. ● Trustworthy systems with Field-Programmable Gate Array (FPGA) and hardware anchor. ● Encrypted traffic analytics maintain integrity of encrypted flow
Unified control of wired and wireless networks from a common console for streamlined operations	● Simplifies and centralizes configuration and management of wireless and wireline devices. Supports WLAN services without requiring a wireless LAN controller. ● Supports Mobility Express for WLAN-enabled routers.
Remote configuration and management to keep local IT staff lean	● Supports separate console/auxiliary and USB ports. ● Can be configured to work with optional USB token. ● Supports TR-069.

Performance ● Throughput ● Service reliability	● Crypto performance up to 250 Mbps for 1100-8P and 150 Mbps for 1100-4P. ● A distributed multicore architecture with the industry's first internal services plane. ● Remote installation of application-aware services that run identically to their counterparts in dedicated appliances.
Lower WAN expenditures	● Cisco Software-Defined WAN (SD-WAN) (over the Cisco Application Policy Infrastructure Controller Enterprise Module [APIC-EM]) support for optimized WAN connection.
Pay as you grow: IPsec performance upgrade model	● Router IPsec capacity can be increased with a remote performance-on-demand license upgrade (no hardware upgrade) for exceptional savings andCapEx budget management.
IT consolidation, space savings, and improved Total Cost of Ownership (TCO)	● Single converged branch platform integrates routing, switching, security, and performance management capabilities.
Business continuity and increased resiliency	● The entire 1100 Series supports Power over Ethernet (PoE) and PoE+ power to endpoints.

Product Accessories
Licenses

Table 3 shows the licenses for C1111-8P.

Licenses	Description
C1-SL-1100-8P-APP	AppX Foundation License for Cisco ISR 1100 8P Series
SL-1100-8P-SEC	Security License for Cisco ISR 1100 8P Series
SL-1100-8P-SECNPE	NPE Security License for Cisco ISR 1100 8P Series
C1-SL-1100-8P-SEC	Security Foundation License for Cisco ISR 1100 8P Series
FL-VPERF-8P-200	IPSEC PLUS 200 Mbps License for Cisco ISR 1100 8P Series

Small Form-Factor Pluggable Supported

Table 4 shows the SFP for Cisco 1100 Series Routers.

Small Form-Factor Pluggable	ISR 1100 8P	ISR 1100 4P	Description
GLC-EX-SMD	Yes	Yes	1000BASE-EX SFP transceiver module, SMF, 1310nm, DOM.
GLC-LH-SMD	Yes	Yes	GE SFP, LC connector LX/LH transceiver; with DOM.
GLC-SX-MMD	Yes	Yes	GE SFP, LC connector SX transceiver; with DOM.
GLC-ZX-SMD	Yes	Yes	1000BASE-ZX SFP; with DOM.
GLC-FE-100ZX	Yes	Yes	100BASE-ZX SFP (80km).
GLC-GE-100FX	Yes	Yes	100FX SFP on GE ports.
GLC-BX-D	Yes	Yes	1000BASE-BX SFP, 1490NM.
GLC-BX-U	Yes	Yes	1000BASE-BX SFP, 1310NM.

Compare to Similar Item

Table 5 shows the comparison between C1111-4P and C1111-8P.

Model	C1111-8P	C1111-4P
WAN GE	1	1
WAN GE/SFP combo	1	1
ADSL2/VDSL2+	N/A	N/A
LTE Advanced (CAT6)	N/A	N/A
802.11ac	N/A	N/A

LAN GE	8	4
PoE	4	2
PoE+	2	1
Integrated USB 3.0 AUX/console	Yes	Yes

Get more information

Do you have any question about the **C1111-8P?**

Contact us now via **Live Chat** or **sales@router-switch.com**.

Specification

C1111-8P Specification	
Description	ISR 1100 8 Ports Dual GE WAN Ethernet Router
Physical Properties	
Dimensions (H x W x D)	Non-LTE models: H x W X D = 1.75 x 12.7 x 9.03 in. (42 x 323 x 230mm) (includes rubber feet)
Weight with AC PS (w/o modules)	5.5 Lbs. (2.5 kg) maximum
AC Input Power	
Input voltage	Universal 100 to 240 VAC
Frequency	50-60 Hz
Input current	PoE not enabled: 0.82A maximum PoE enabled: 1.55A Maximum
Surge current	90 A peak and less than 8 Arms per half cycle
Ports	
Micro USB Port	One RJ-45: Separate console port
USB port	USB 3.0 Type A host port USB devices supported: USB flash memory
Console port	One USB 5-pin micro Type B: Console management connectivity
10/100/1000 Gigabit Ethernet	Two GE ports allocated among RJ45 and SFP as: One combo port with 10/100/1000RJ-45 Ethernet port or SFP Ethernet port (labeled GE0/0/0) One dedicated 10/100/1000RJ-45 Ethernet port (labeled GE0/0/1)
Wireless VLANs	32 (encrypted and non-encrypted VLANs)
Wireless specifications	2x2 .11ac Wave 2
Default and maximum DRAM	4GB
Default and maximum flash	4GB
Inline PoE	4 ports for -8P PIDs, 2 ports for -4P PIDs 802.3af-compliant PoE or 802.3at-compliant PoE+
Acoustic for Cisco 1100 Series ISRs	Not Applicable - Fanless design

Approvals and compliance	Emission 47 CFR Part 15 CISPR 32 Edition 2 EN 300 386 V1.6.1 EN 55032:2012/ AC:2013 EN 55032:2015 EN61000-3-2 2014 EN61000-3-3: 2013 ICES-003 ISSUE 6:2016 KN 32: 2015 V-2/2015.04 V-3/2015.04 TCVN 7189: 2009 CNS13438: 2006 IEC 60950-1 EN 60950-1 UL 60950-1 CSA C22.2 No. 60950-1 Immunity CISPR24: 2010 + A1: 2015 EN 300 386 V1.6.1 EN55024: 2010 + A1: 2015 KN35: 2015 TCVN 7317: 2003
Environmental	
Operating humidity	5 to 85% relative humidity
Operating temperature	32 to 104°F (0 to 40°C) Sea Level; 32 to 77°F (0°C to 25°C) at 10,000 ft 1.5°C derating per 1000 ft
Altitude in China	0-6560 ft (0-2000 m)
Altitude in all other countries	0-10,000 ft (0-3050 m)
Transportation and Storage	
Nonoperating temperature	-40 to 158°F (-40 to 70°C)
Nonoperating humidity	5 to 95% relative humidity (noncondensing)
Nonoperating altitude	0 to 15,000 ft (0 to 4570m)

Download Resource

Support and Resources

Cisco Integrated Services Routers 1000 Series Datasheet

Transition Guide

Guide to Select New Cisco Routers

Guide to Upgrade Your ISR G1 and ISR G2 Routers to ISR 4000

Want to Buy

Order Now Get a Quote

Why Router-switch.com

As a leading network hardware supplier, Router-switch.com focuses on original new ICT equipment of Cisco, Huawei, HPE, Dell, Hikvision, Juniper, Fortinet, etc.

200+	18,000+	$20,000,000	50%-98%	100%
Countries we Sold	Customers Trusted	Inventory Available	Off Global List Price	Safe Online Shopping

Contact Us

- Tel: +1-626-239-8066 (USA) 852-30691898/ 852-30691868 (Hong Kong)
- Fax: 852-30691898 (Hong Kong)
- Email: sales@router-switch.com

DATA SHEET

FortiGate® FortiWiFi 60F Series

FG-60F, FG-61F, FWF-60F, and FWF-61F

Next Generation Firewall
Secure SD-WAN

The FortiGate/FortiWiFi 60F series provides a fast and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance
- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification
- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking
- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management
- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric
- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
10 Gbps	**1.4 Gbps**	**1 Gbps**	**700 Mbps**	Multiple GE RJ45 | Variants with internal storage | WiFi variants

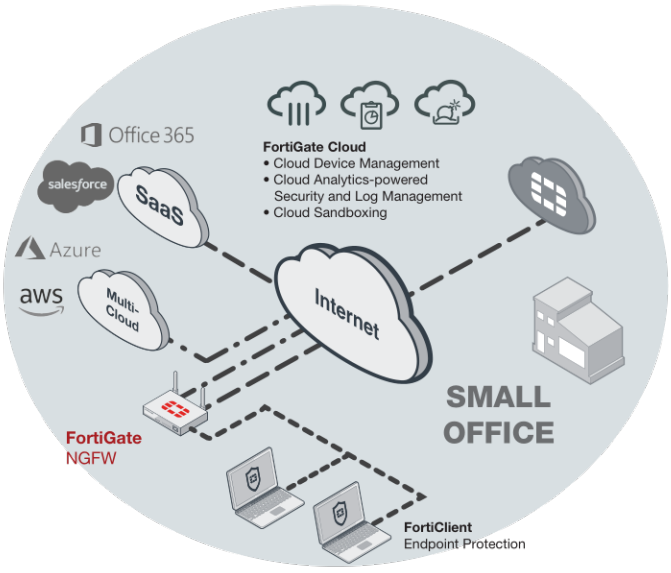
DEPLOYMENT

Next Generation Firewall (NGFW)

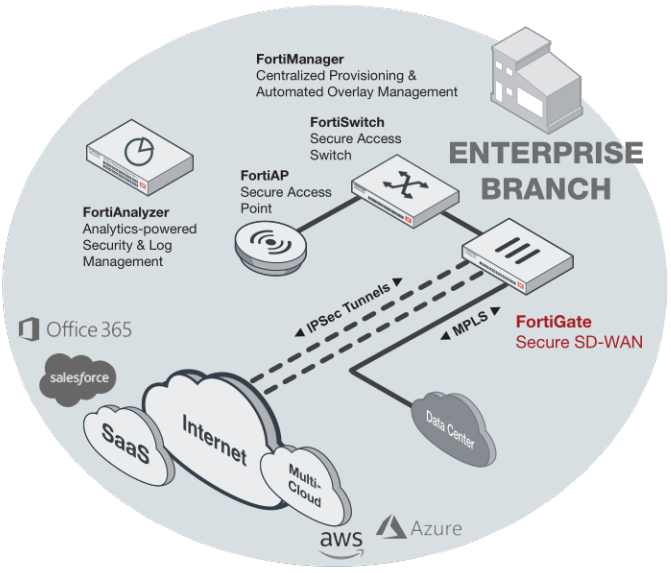
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplified and intuitive workflow with FortiManger for management and zero touch deployment
- Strong security posture with next generation firewall and real-time threat protection



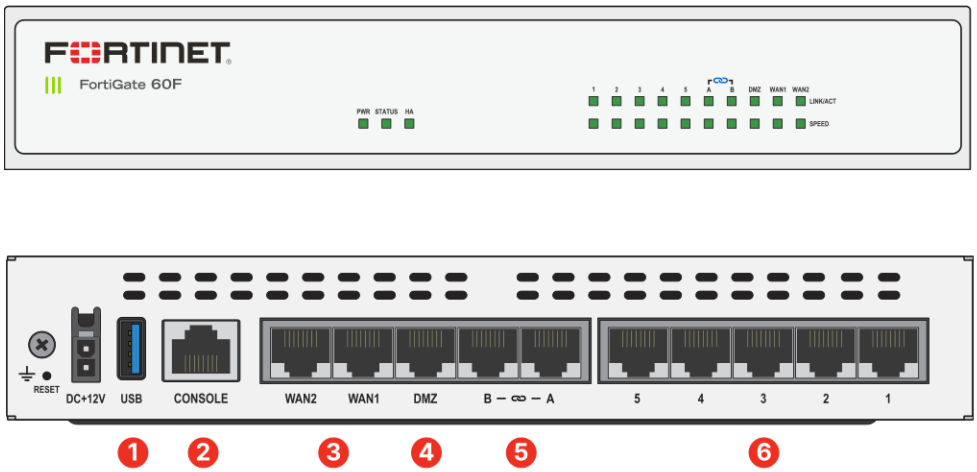
Small Office Deployment (NGFW)



Enterprise Branch Deployment (Secure SD-WAN)

HARDWARE

FortiGate / FortiWiFi 60F/61F



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

Hardware Features

Powered by Purpose-built Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

3G/4G WAN Connectivity

The FortiGate 60F Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Secure Access Layer

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

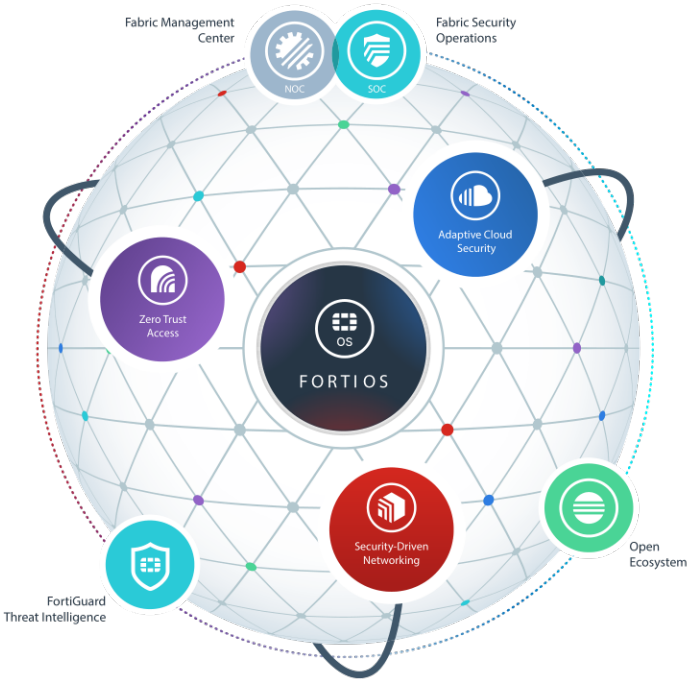
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated**: Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SPECIFICATIONS

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	–	–	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	–	1 × 128 GB SSD	–	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1.4 Gbps			
NGFW Throughput [2, 4]	1 Gbps			
Threat Protection Throughput [2, 5]	700 Mbps			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps			
Firewall Latency (64 byte UDP packets)	3.3 µs			
Firewall Throughput (Packets Per Second)	9 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	900 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	630 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	400			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps			
CAPWAP Throughput (HTTP 64K)	8 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	16			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3			
Height x Width x Length (mm)	38.5 × 216 × 160 mm			
Weight	2.23 lbs (1.01 kg)			
Form Factor	Desktop			
Radio Specifications				
Multiple User (MU) MIMO	–	–	3×3	
Maximum Wi-Fi Speeds	–	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	–	–	20 dBm	
Antenna Gain	–	–	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

SPECIFICATIONS

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Operating Environment and Certifications				
Power Rating	12Vdc, 3A			
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz			
Maximum Current	100Vac/1.0A, 240Vac/0.6A			
Power Consumption (Average / Maximum)	17.0 W / 18.5 W	17.2 W / 18.7 W	17.2 W / 18.7 W	17.5 W / 19.0 W
Heat Dissipation	63.1 BTU/hr	63.8 BTU/hr	63.8 BTU/hr	64.8 BTU/hr
Operating Temperature	32–104°F (0–40°C)			
Storage Temperature	-31–158°F (-35–70°C)			
Humidity	Humidity 10–90% non-condensing			
Noise Level	Fanless 0 dBA			
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN			

ORDERING INFORMATION

Product	SKU	Description
FortiGate 60F	FG-60F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port)
FortiGate 61F	FG-61F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage
FortiWiFi 60F	FWF-60F	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2)
FortiWiFi 61F	FWF-61F	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2), 128GB SSD onboard storage
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, and 80E/81E
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F and FG/FWF-80F series

BUNDLES

FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24×7	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video[1] Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•			
FortiGuard IoT Detection Service	•			
FortiGuard Industrial Service	•			
FortiConverter Service	•			
FortiGate Cloud Subscription		•		

1. Available when running FortiOS 7.0

FORTINET

www.fortinet.com

DATA SHEET

FortiGate® FortiWiFi 40F Series

FG-40F and FWF-40F

Next Generation Firewall
Secure SD-WAN

The FortiGate/FortiWiFi 40F series provides a fast and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security
- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance
- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification
- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking
- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management
- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric
- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

Firewall	IPS	NGFW	Threat Protection	Interfaces
5 Gbps	**1 Gbps**	**800 Mbps**	**600 Mbps**	Multiple GE RJ45 | WiFi variants

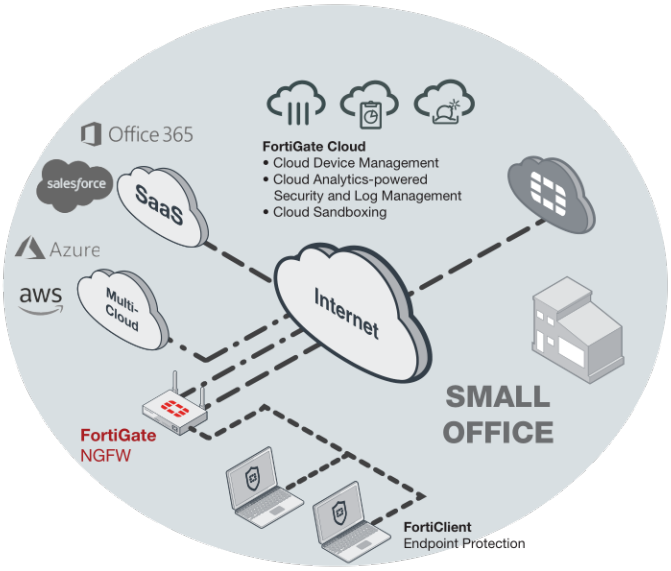
DEPLOYMENT

Next Generation Firewall (NGFW)

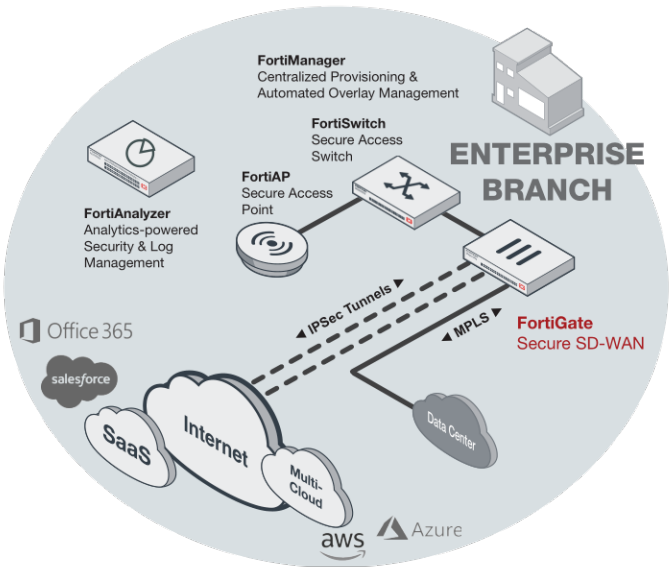
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, and applications across the entire attack surface, and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

Secure SD-WAN

- Consistent business application performance with accurate detection and dynamic WAN path steering on any best-performing WAN transport
- Accelerated Multi-cloud access for faster SaaS adoption with cloud-on-ramp
- Self-healing networks with WAN edge high availability, sub-second traffic switchover-based and real-time bandwidth compute-based traffic steering
- Automated Overlay tunnels provides encryption and abstracts physical hybrid WAN making it simple to manage
- Simplified and intuitive workflow with FortiManger for management and zero touch deployment
- Enhanced analytics both real-time and historical provides visibility into network performance and identify anomalies
- Strong security posture with next generation firewall and real- time threat protection



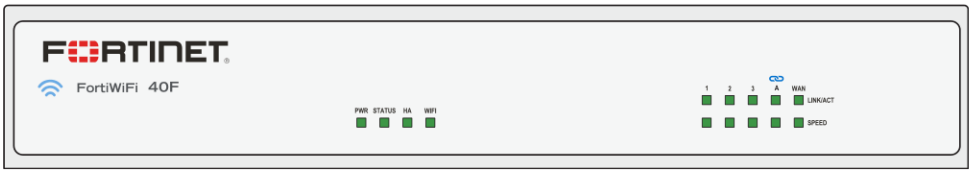
Small Office Deployment (NGFW)

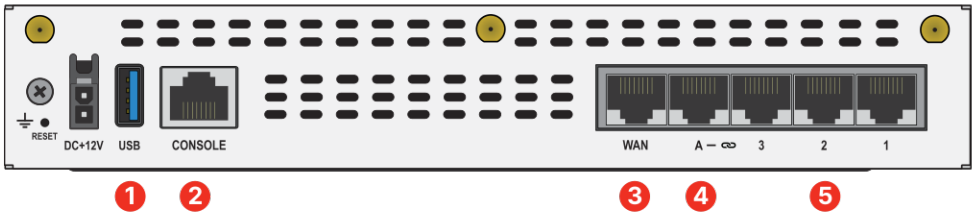


Enterprise Branch Deployment (Secure SD-WAN)

HARDWARE

FortiGate/FortiWiFi 40F Series





Interfaces

1. 1x USB Port
2. 1x Console Port
3. 1x GE RJ45 WAN Port
4. 1x GE RJ45 FortiLink Port
5. 3x GE RJ45 Ethernet Ports

Hardware Features

Powered by Purpose-built Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables the best of breed NGFW Security and Deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

3G/4G WAN Connectivity

The FortiGate 40F Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Secure Access Layer

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

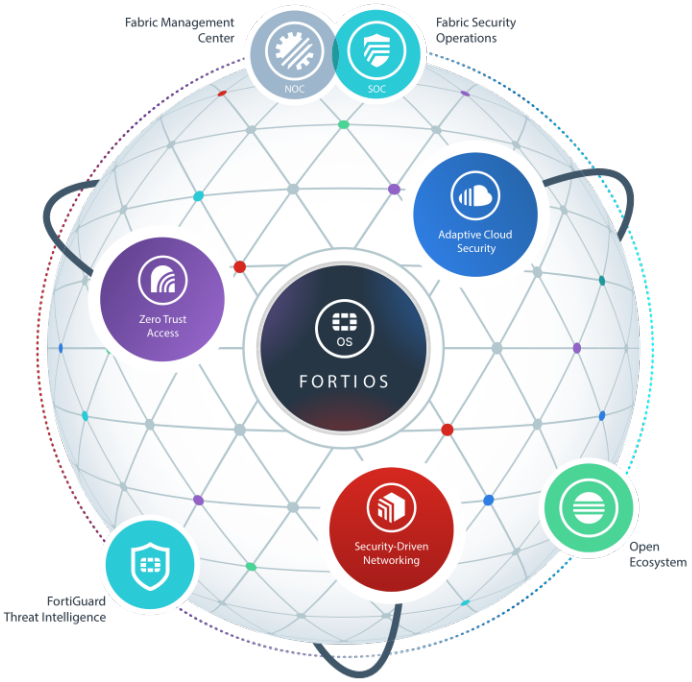
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad**: Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated**: Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated**: Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES

FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.

FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SPECIFICATIONS

	FORTIGATE 40F	FORTIWIFI 40F
Interfaces and Modules		
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	
Hardware Accelerated GE RJ45 Internal Ports	3	
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	
Hardware Accelerated GE RJ45 PoE/+ Ports	0	
Wireless Interface	0	Single Radio (2.4GHz/5GHz) 802.11 /a/b/g/n/ac-W2
USB Ports	1	
Console Port (RJ45)	1	
Onboard Storage	0	
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	1 Gbps	
NGFW Throughput [2, 4]	800 Mbps	
Threat Protection Throughput [2, 5]	600 Mbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps	
Firewall Latency (64 byte, UDP)	2.97 µs	
Firewall Throughput (Packet per Second)	7.5 Mpps	
Concurrent Sessions (TCP)	700 000	
New Sessions/Second (TCP)	35 000	
Firewall Policies	5000	
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	250	
SSL-VPN Throughput	490 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000	
Application Control Throughput (HTTP 64K) [2]	990 Mbps	
CAPWAP Throughput (HTTP 64K)	3.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	8	
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 40F	FORTIWIFI 40F
Dimensions and Power		
Height x Width x Length (inches)	1.5 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160	
Weight	2.2 lbs (1 kg)	
Form Factor (supports EIA/non-EIA standards)	Desktop	
Input Rating	12Vdc, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	13.4 W / 15.4 W	14.6 W / 16.6 W
Current (Maximum)	100V AC / 0.2A, 240V AC / 0.1A	
Heat Dissipation	52.55 BTU/h	56.64 BTU/h
Redundant Power Supplies		
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	
Radio Specifications		
Multiple (MU) MIMO	0	3 × 3
Maximum Wi-Fi Speeds	0	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	0	20 dBm
Antenna Gain	0	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

ORDERING INFORMATION

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports).
FortiWiFi 40F	FWF-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2).
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FG/FWF-40F, come with interchangeable power plugs. (XX=various countries code).
Wall Mount Kits	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.

BUNDLES

FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24×7	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video[1] Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•			
FortiGuard IoT Detection Service	•			
FortiGuard Industrial Service	•			
FortiConverter Service	•			
FortiGate Cloud Subscription		•		

1. Available when running FortiOS 7.0

ANEXO II

MANUAL DE INSTALACIÓN SERVIDOR DNS, SERVIDOR DE CORREO ZIMBRA Y PLEX MEDIA SERVER

Índice de Contenido

1 SERVIDOR DNS Y SERVIDOR ZIMBRA

Un servidor DNS nos sirve para poder darle un nombre a una IP, en vez de digitar la IP, se digita un nombre siendo así más fácil de recordar, de esta forma nos entregará mediante una interfaz gráfica la página a la que deseamos acceder vía web.

Zimbra es una plataforma de mensajería que sirve para enviar y recibir correos electrónicos, implementado sobre código abierto. Zimbra puede trabajar directamente sobre un navegador vía web o ser configurado en una aplicación para correos.

a. Software VMware Workstation Pro 16

VMware Workstation Pro es un software completo para poder ejecutar varios sistemas operativos como máquinas virtuales dentro de una PC física. Este tipo de software sirve para realizar pruebas, demostraciones o crear software en un entorno virtualizado, sin perder rendimiento y obteniendo una excelente experiencia como si se tratara de un entorno físico. En la figura A.1 se muestra el producto y la versión de VMware utilizado para la implementación de los servidores virtualizados [1].

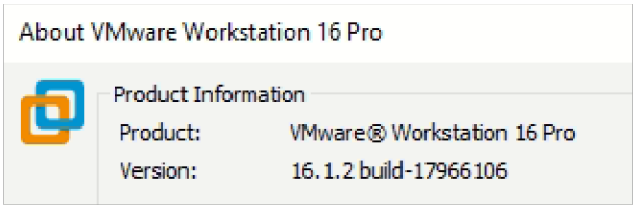


Figura A.1. VMware Workstation 16 Pro.

b. Requerimientos de Hardware para un entorno Virtualizado

Figura A.2. Características Laptop Toshiba.

Para la virtualización e implementación de los servidores DNS y Correo Zimbra, se hizo uso de una laptop Toshiba con las características especificadas en la Figura A.2, con Sistema Operativo Windows 10, en la laptop se instala el software VMware Workstation 16 Pro, se utiliza los requerimientos de hardware mínimos, los cuales se detallan en la tabla A.1.

Tabla A.1. Requerimientos de hardware mínimos para VMware.

	REQUERIMIENTOS MINIMOS
SISTEMA OPERATIVO ANFITRIÓN	Windows 10 Education
VIRTUALIZACIÓN	Habilitar la extensión en la BIOS del computador de ser requerido.
MEMORIA ROM	20 GB de Disco Duro, con espacio de 10 GB adicionales.
MEMORIA RAM	3 GB de RAM
NÚMERO DE PROCESADORES	i3 CPU, 2 o más núcleos lógicos.

c. Sistema Operativo Ubuntu y Versión de Zimbra

Para la instalación de los servidores virtualizados, se realizar sobre el Sistema Operativo Ubuntu 16.04 LTS de 64 bits mostrada en la figura A.3, esta distribución de Ubuntu soporta la instalación de la versión de Zimbra 8.8.15 GA Release, servidor utilizado en nuestro proyecto.

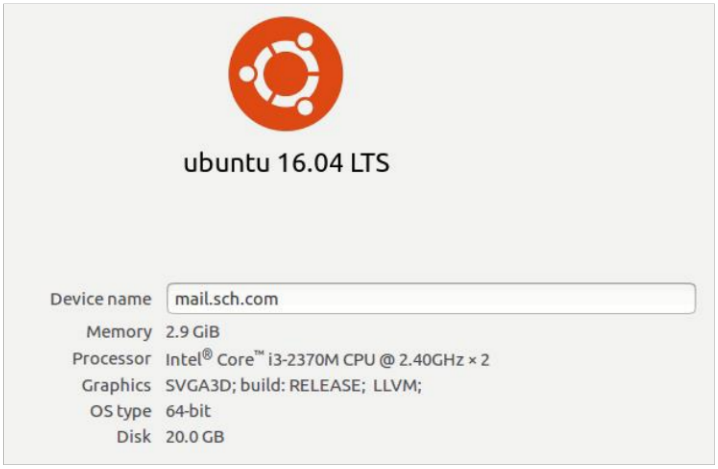


Figura A.3. Versión Sistema Operativo Ubuntu.

d. Preparación Servidor DNS y Servidor Zimbra

Para la instalación del dominio **sch.com**, se debe considerar que el dominio no será publicado en Internet, solo se utilizara a nivel de la Intranet del proyecto, por lo cual no es necesario adquirir o comprar el dominio en servicios de Hosting.

Para el servidor de correo Zimbra, se utiliza una distribución de Linux que cumple con los requisitos para una instalación adecuada.

e. Actualizar los repositorios de Ubuntu 16.04 LTS [2]

Para la actualización e instalación de los paquetes disponibles, así como la instalación de los servidores, es necesario el ingreso como *root* o superusuario, para lo cual se ingresa el siguiente comando, nos pedirá la clave que se tiene configurada para el ingreso a Ubuntu.

```
servidor1@ubuntu:~$ sudo su
[sudo] password for servidor1:
root@ubuntu:/home/servidor1#
```

Figura A.4. Modo *root*.

Para actualizar la lista de paquetes disponibles se ingresa el siguiente comando.

```
root@ubuntu:/home/servidor1# apt-get update
```

Figura A.5. Update del sistema.

Para instalar los paquetes disponibles se ingresa el siguiente comando.

```
root@ubuntu:/home/servidor1# apt-get upgrade
```

Figura A.6. Upgrade del sistema.

f. Configuración del Hostname del servidor [2]

En el siguiente fichero **hosts** se debe configurar el servidor, nombre del dominio y la IP privada que se da al servidor Zimbra, este paso será requerido más adelante al momento de instalar Zimbra.

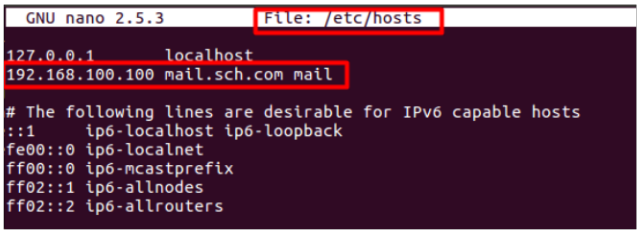


Figura A.7. Modificación fichero /etc/hosts.

También editamos el fichero ***hostname*** escribiendo el nombre del servidor más el dominio.

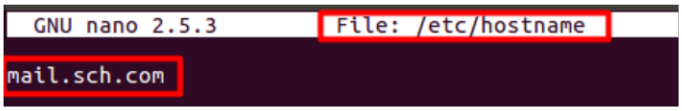


Figura A.8. Modificación fichero /etc/hostname.

Realizado los cambios, reiniciamos el sistema operativo con el comando ***Reboot***.

g. Instalación del servidor DNS [2]

Se procede a instalar DNS local mediante el siguiente comando, en caso de pedir confirmación, escribimos **Y** para que proceda con la instalación del paquete ***dnsmasq***.

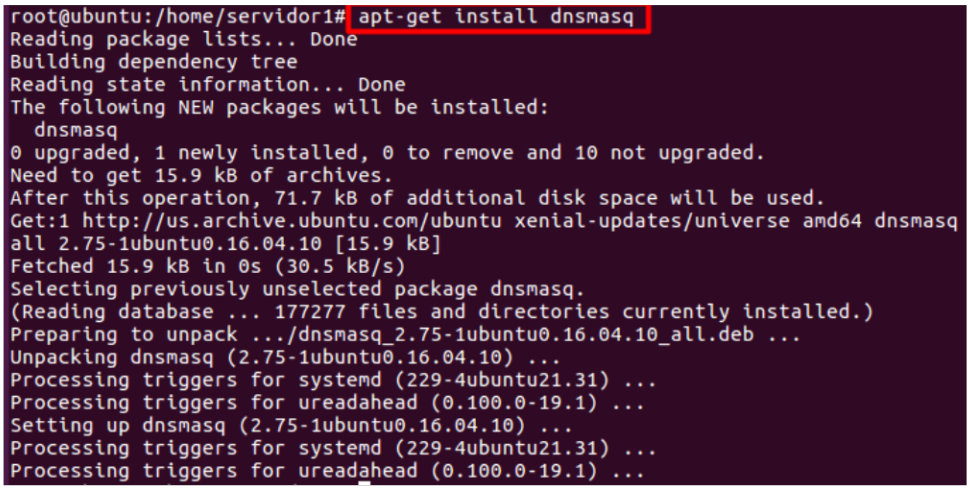


Figura A.9. Instalación paquete *dnsmasq*.

Editamos las configuraciones del fichero ***dnsmasq.conf*** agregando al final las siguientes líneas con los datos del dominio local, dirección IP local.

Figura A.10. Modificación fichero /etc/dnsmasq.conf

Guardamos el fichero, si todo está correcto, no debería salir ningún mensaje, procedemos con el reinicio del servicio.

```
root@ubuntu:/home/servidor1# service dnsmasq restart
```

Figura A.11. Reinicio servicio *dnsmasq*.

h. Zimbra Edition 8.8.15 GA Release [2]

Para instalar el servidor Zimbra, es necesario descargar los archivos desde la web oficial de Zimbra mediante el siguiente comando.

```
root@ubuntu:/home/servidor1# wget https://files.zimbra.com/downloads/8
.8.15_GA/zcs-8.8.15_GA_3869.UBUNTU16_64.20190918004220.tgz
```

Figura A.12. Descarga de Zimbra.

Debemos descomprimir el archivo descargado mediante el siguiente comando.

```
root@ubuntu:/home/servidor1# tar -xzvf zcs-8.8.15_GA_3869.UBUNTU16_64.
20190918004220.tgz
```

Figura A.13. Descompresión archivo Zimbra .tgz.

Mediante el siguiente comando, cambiamos de directorio.

```
root@ubuntu:/home/servidor1# cd zcs-8.8.15_GA_3869.UBUNTU16_64.2019091
8004220
```

Figura A.14. Cambio de directorio.

i. Instalación de Zimbra [2]

Mediante el siguiente comando, procedemos a instalar Zimbra, en el proceso nos solicitará si deseamos aceptar los términos y condiciones de la licencia, digitamos ***Yes***.

Figura A.15. instalación Zimbra y términos de licencia.

Nos preguntaran si deseamos instalar los repositorios de Zimbra, digitamos ***Y***.

Figura A.16. Instalación repositorios Zimbra.

Paso seguido, instalaremos solo los paquetes que son necesarios colocando **Y** para instalar, se excluyen ciertos paquetes poniendo ***No***, estos serían ***zimbra-dnscache*** que no necesitamos ya que se instaló *dnsmasq* como servidor DNS y ***zimbra-imapd (BETA – for evaluation only)***, paquete que está en modo prueba.

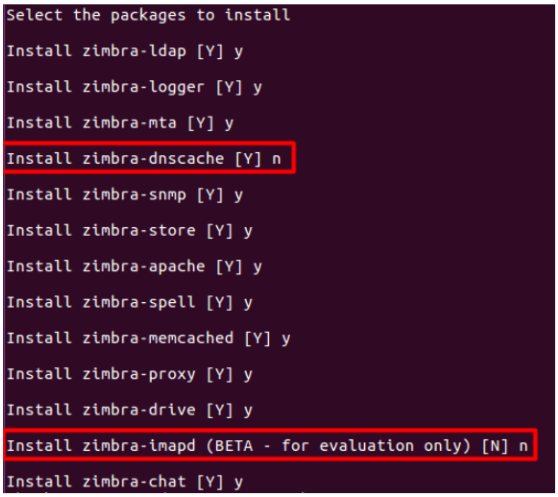


Figura A.17. Instalación paquetes Zimbra.

Presionamos ***Y*** para que se modifique el sistema.

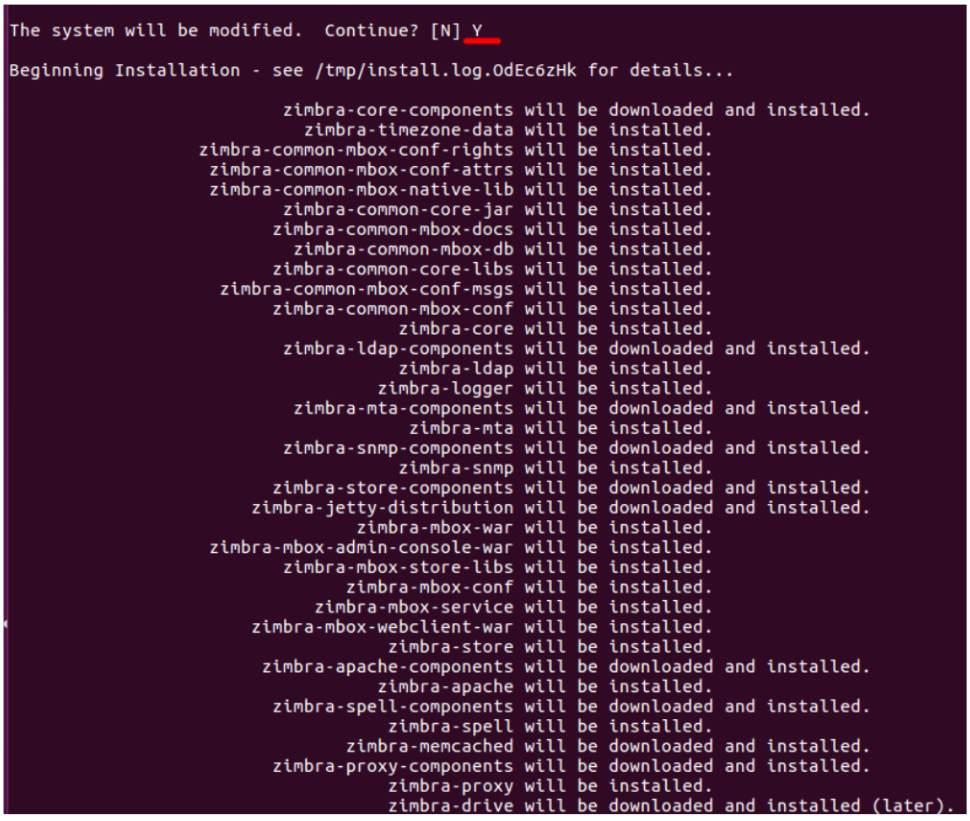


Figura A.18. Modificación del sistema.

El siguiente paso es modificar el dominio por defecto, se debe tener en cuenta el cambio y realizarlo bien, ya que este paso si no se modifica adecuadamente puede presentarse un fallo.

```
Running Post Installation Configuration:
Operations logged to /tmp/zmsetup.20211227-211508.log
Installing LDAP configuration database...done.
Setting defaults...

DNS ERROR resolving MX for mail.sch.com
It is suggested that the domain name have an MX record configured in DNS
Change domain name? [Yes] Y
Create domain: [mail.sch.com] sch.com
        MX: mail.sch.com (192.168.100.100)

        Interface: 192.168.100.100
        Interface: 127.0.0.1
        Interface: ::1
done.
Checking for port conflicts
```

Figura A.19. Modificación del dominio en Zimbra.

Se debe modificar la password del administrador de Zimbra ***admin***, para lo cual se debe ingresar en el menú principal digitando ***6***, luego en el submenú digitando ***4.***

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                          Enabled
   3) zimbra-logger:                        Enabled
   4) zimbra-mta:                           Enabled
   5) zimbra-snmp:                          Enabled
   6) zimbra-store:                         Enabled
        +Create Admin User:                 yes
        +Admin user to create:              admin@sch.com
******* +Admin Password                     UNSET
        +Anti-virus quarantine user:        virus-quarantine.j1il9tu7@sch.com
        +Enable automated spam training:    yes
        +Spam training user:                spam.aj3drs7i0@sch.com
        +Non-spam(Ham) training user:       ham.wj4s1hit@sch.com
        +SMTP host:                         mail.sch.com
        +Web server HTTP port:              8080
        +Web server HTTPS port:             8443
        +Web server mode:                   https
        +IMAP server port:                  7143
        +IMAP server SSL port:              7993
        +POP server port:                   7110
        +POP server SSL port:               7995
        +Use spell check server:            yes
        +Spell server URL:                  http://mail.sch.com:7780/aspell.php
        +Enable version update checks:      TRUE
        +Enable version update notifications:  TRUE
        +Version update notification email:    admin@sch.com
        +Version update source email:          admin@sch.com
        +Install mailstore (service webapp):   yes
        +Install UI (zimbra,zimbraAdmin webapps): yes

   7) zimbra-spell:                         Enabled
   8) zimbra-proxy:                         Enabled
   9) Default Class of Service Configuration:
   s) Save config to file
   x) Expand menu
   q) Quit

Address unconfigured (**) items  (? - help) 6
```

Figura A.20. Menú de configuración Zimbra.

```
Store configuration

   1) Status:                                  Enabled
   2) Create Admin User:                       yes
   3) Admin user to create:                    admin@sch.com
** 4) Admin Password                          UNSET
   5) Anti-virus quarantine user:              virus-quarantine.j1il9tu7@sch.com
   6) Enable automated spam training:          yes
   7) Spam training user:                      spam.aj3drs7i0@sch.com
   8) Non-spam(Ham) training user:             ham.wj4s1hit@sch.com
   9) SMTP host:                               mail.sch.com
  10) Web server HTTP port:                    8080
  11) Web server HTTPS port:                   8443
  12) Web server mode:                         https
  13) IMAP server port:                        7143
  14) IMAP server SSL port:                    7993
  15) POP server port:                         7110
  16) POP server SSL port:                     7995
  17) Use spell check server:                  yes
  18) Spell server URL:                        http://mail.sch.com:7780/aspell.php
  19) Enable version update checks:            TRUE
  20) Enable version update notifications:     TRUE
  21) Version update notification email:       admin@sch.com
  22) Version update source email:             admin@sch.com
  23) Install mailstore (service webapp):      yes
  24) Install UI (zimbra,zimbraAdmin webapps): yes

Select, or 'r' for previous menu [r] 4
```

Figura A.21. Submenú de configuración Zimbra.

En el siguiente paso, digitamos ***r*** para regresar al menú principal, luego digitamos ***a*** para aplicar los cambios de las configuraciones.

```
Select, or 'r' for previous menu [r] r

Main menu

   1) Common Configuration:
   2) zimbra-ldap:                             Enabled
   3) zimbra-logger:                           Enabled
   4) zimbra-mta:                              Enabled
   5) zimbra-snmp:                             Enabled
   6) zimbra-store:                            Enabled
   7) zimbra-spell:                            Enabled
   8) zimbra-proxy:                            Enabled
   9) Default Class of Service Configuration:
   s) Save config to file
   x) Expand menu
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
```

Figura A.22. Aplicando cambios en Zimbra.

Procedemos a digitar ***Yes*** para que los cambios sean guardados.

```
Save configuration data to a file? [Yes] Y
Save config in file: [/opt/zimbra/config.14122]
Saving config in /opt/zimbra/config.14122...done.
The system will be modified - continue? [No] Yes
```

Figura A.23. Guardar cambios en Zimbra.

La instalación se finalizará con un mensaje en donde nos solicita si deseamos enviar notificaciones a Zimbra, en este caso le decimos que ***No***.

```
You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Server.
The only information that will be transmitted is:
        The VERSION of zcs installed (8.8.15_GA_3869_UBUNTU16_64)
        The ADMIN EMAIL ADDRESS created (admin@sch.com)

Notify Zimbra of your installation? [Yes] No
```

Figura A.24. Notificación a Zimbra.

j. Panel de Administración Zimbra

Procedemos a digitar en un navegador la URL con el dominio configurado y el puerto, https://mail.sch.com:7071, se desplegará la interfaz gráfica para poder acceder a la consola de administración del servidor Zimbra vía Web, aquí podemos realizar la creación de los usuarios, cambio de claves, validación de envió/recepción de correos, etc.

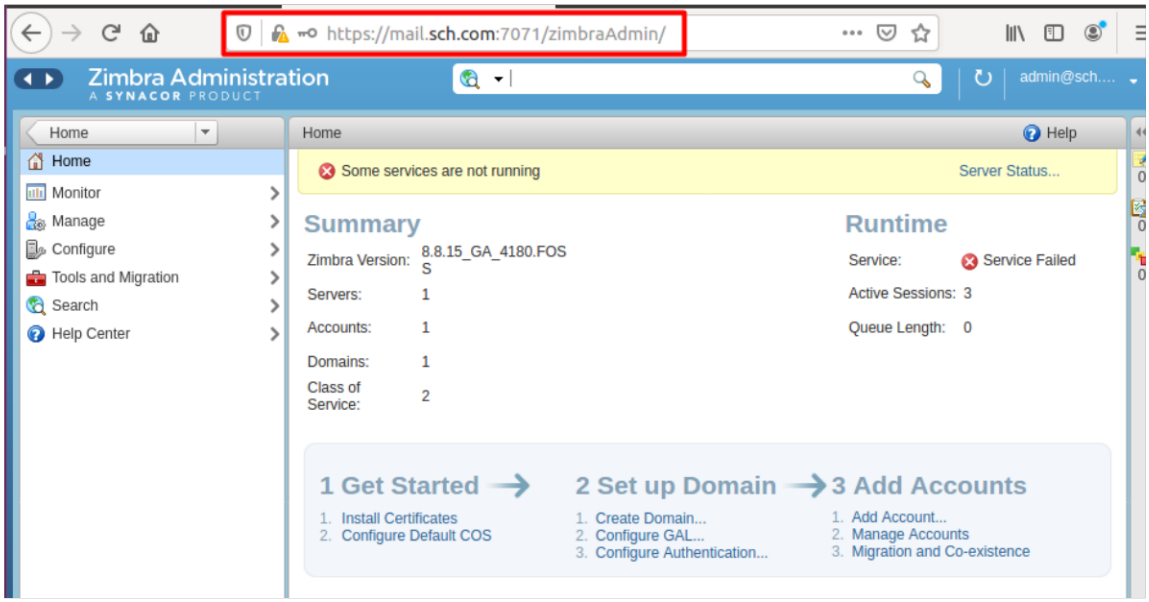


Figura A.25. Panel de administración Zimbra.

k. Creación Buzón de Correo

Dentro de la administración del panel de Zimbra, podemos crear los buzones de correo para cada usuario que deseemos, lo cual se puede crear de diferentes maneras la cuenta, esto dependerá de cómo administre el Ingeniero de TI, para este ejemplo se colocará de la siguiente manera nombre.apellido@sch.com, se puede llenar los demás campos, para el siguiente proyecto solo se considera la creación de la cuenta y un password para cada usuario.

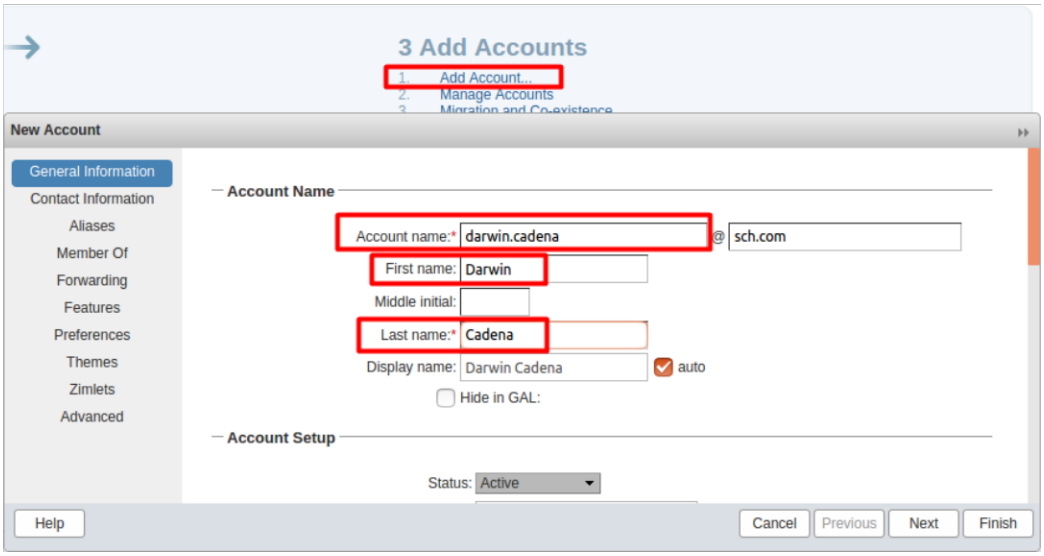


Figura A.26. Configuración Buzón de Correo.

Se coloca la password, se confirma y se procede con la finalización de la configuración.

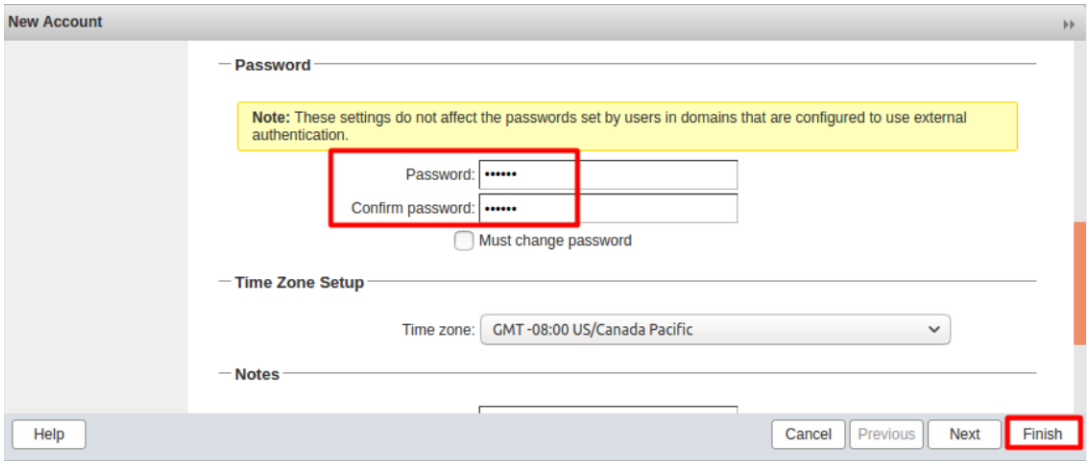


Figura A.27. Creación de Password para buzón de correo.

En el menú Home, luego en *Manage* y en *Account* podemos visualizar las cuentas de buzones de correo creadas y que están asociadas al dominio sch.com.

Figura A.28. Cuentas de correo.

Podemos visualizar el buzón nuevo creado y listo para poder ser utilizado para el envío y recepción de correos dentro de la red Intranet.

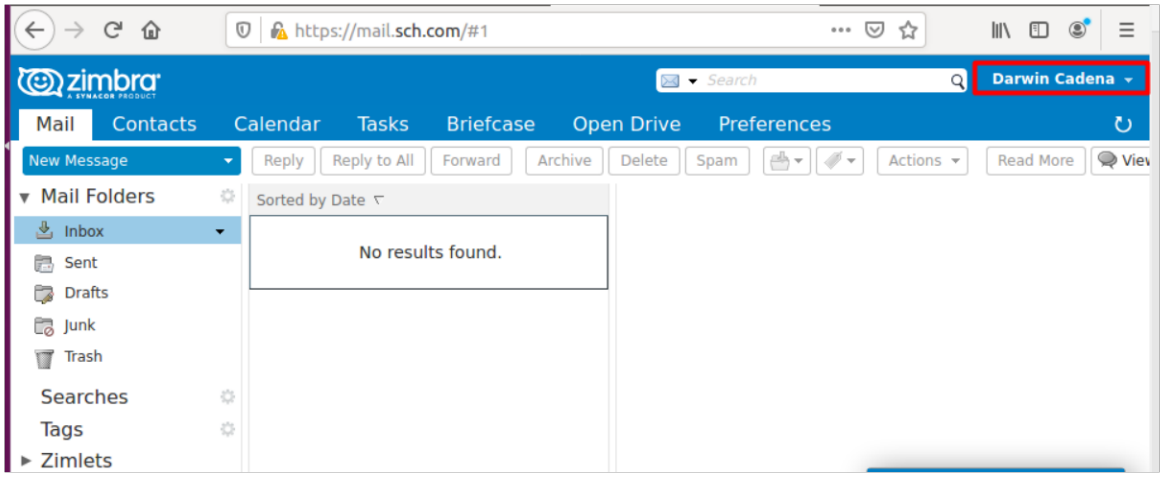


Figura A.29. Interfaz web buzón de correo Zimbra.

2 PLEX MEDIA SERVER

Plex es un gestor de contenido multimedia, el cual puede ser utilizado para reproducir contenido como películas, música, fotos que esté almacenado en nuestro ordenador de forma local o publicarlo en Internet como lo hace Netflix. Plex es compatible con todos los formatos de audio y video, organizándose por carpetas, cifrando la conexión al conectarse remotamente, además permite conectarse a otros canales como TED, *Comedy Central* entre otros.

I. Requerimientos de Hardware

Los requerimientos de hardware son de una laptop HP, en la cual se utilizará como servidor físico con las siguientes características.

Tabla A.2. Requerimientos de hardware mínimos para Plex.

	REQUERIMIENTOS MINIMOS
SISTEMA OPERATIVO	Windows 10 Education
PROCESADOR	Intel(R) Core (TM)2 Duo CPU T6500 @ 2.10GHz 2.10 GHz
MEMORIA ROM	85 GB de Disco Duro
MEMORIA RAM	4 GB de RAM
TIPO DE SISTEMA	Sistema operativo de 64 bits, procesador basado en x64

m. Instalación Plex Media Server [3]

Para la instalación de Plex media Server, debemos realizarlo directamente de la Página oficial https://www.plex.tv/media-server-downloads/, en donde podemos escoger para utilizarlo como servidor o como cliente, adicional se puede escoger para los diferentes Sistemas Operativos que hay en el mercado, para nuestro proyecto la descarga es para Windows.

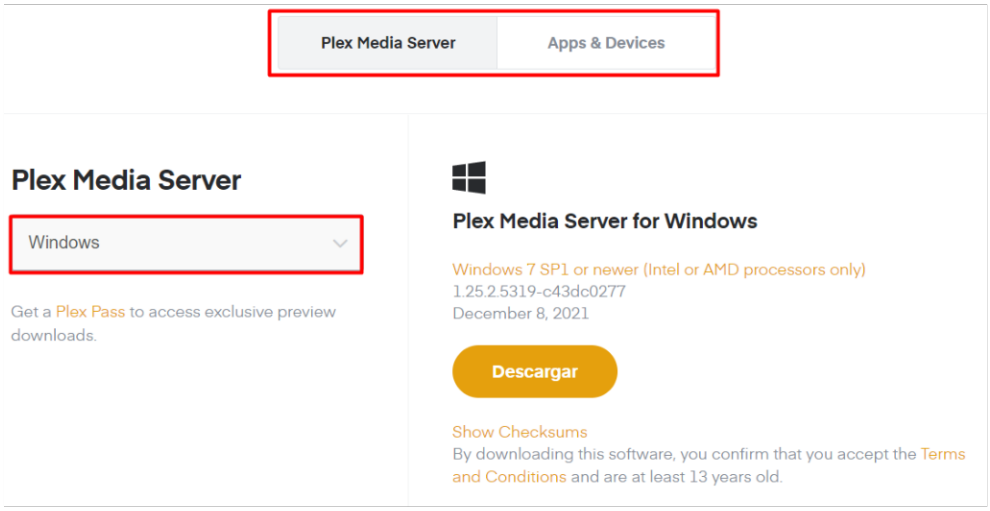


Figura A.30. Descarga de Plex cliente-servidor.

Al dar click en el botón Descargar, obtenemos un archivo .exe, lo ejecutamos y nos mostrará el asistente de instalación de Plex como servidor. El botón de ***Opciones*** es para elegir la ubicación en donde podemos instalar el servidor, el botón de ***Instalar*** es para comenzar el proceso de instalación automática

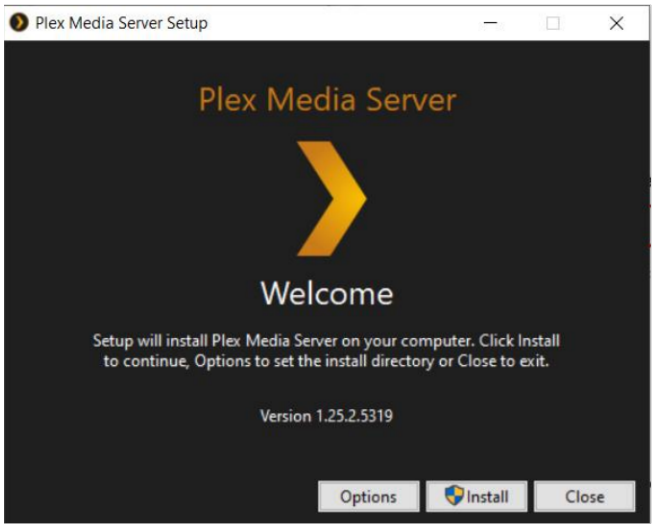


Figura A.31. Instalación Plex Media Server.

Cuando termina la instalación, se debe dar click sobre el botón Lanzar, para que el servidor se ejecute sobre el navegador que se tenga como predeterminado en el computador.

Aquí debemos registrarnos dentro de Plex, colocando nombre de usuario, un correo electrónico y una contraseña.

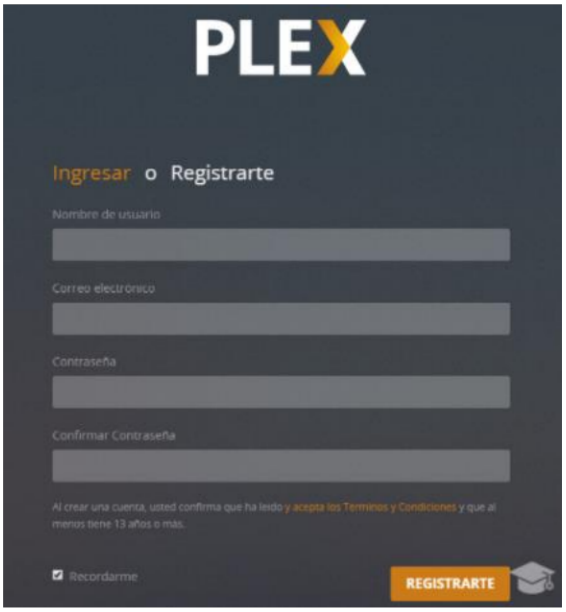


Figura A.32. Registro en Plex.

Luego en el panel de control principal, debemos colocarnos en la pestaña Nombre, para poder darle un nombre al servidor con el cual se identificará nuestra lista de multimedia, damos click en *Siguiente*.

Figura A.33. Configuración Servidor Plex.

El siguiente paso será la ***Biblioteca*** de medios, aquí se puede administrar y editar las bibliotecas creadas, por defecto se tiene dos, de fotos y música, se puede agregar o añadir más bibliotecas como por ejemplo de películas utilizado en el proyecto.

Figura A.34. Biblioteca de medios.

Al dar click en Añadir Biblioteca aparece la siguiente interfaz, aquí en el lado izquierdo, podemos seleccionar la o las carpetas en donde están las películas y así cargar de contenido al servidor.

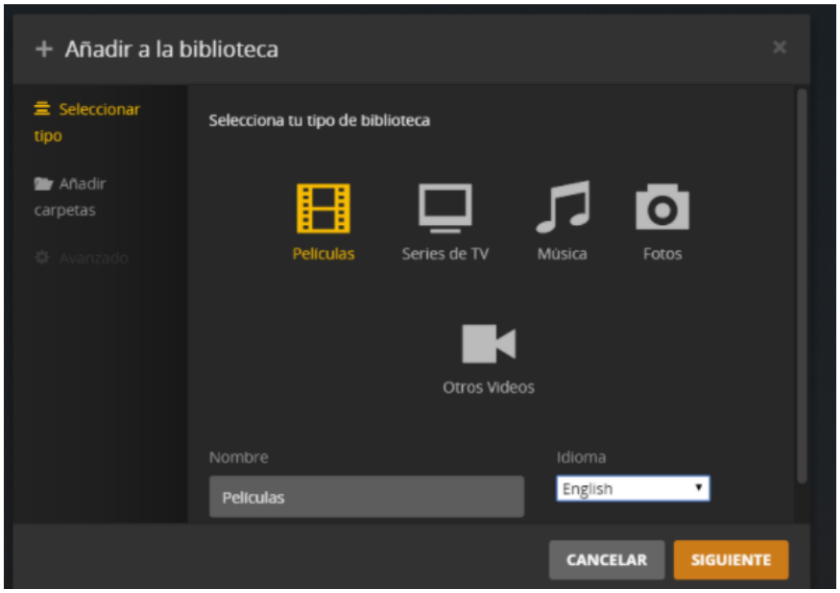


Figura A.35. Añadir bibliotecas de medios.

n. Web Plex Cliente

Mediante la interfaz Web como cliente, podemos visualizar nuestro contenido multimedia cargado, en este caso su nombre es ***DARWIN_VIDEO***, aquí tenemos dos bibliotecas, una de Películas y una de Música.

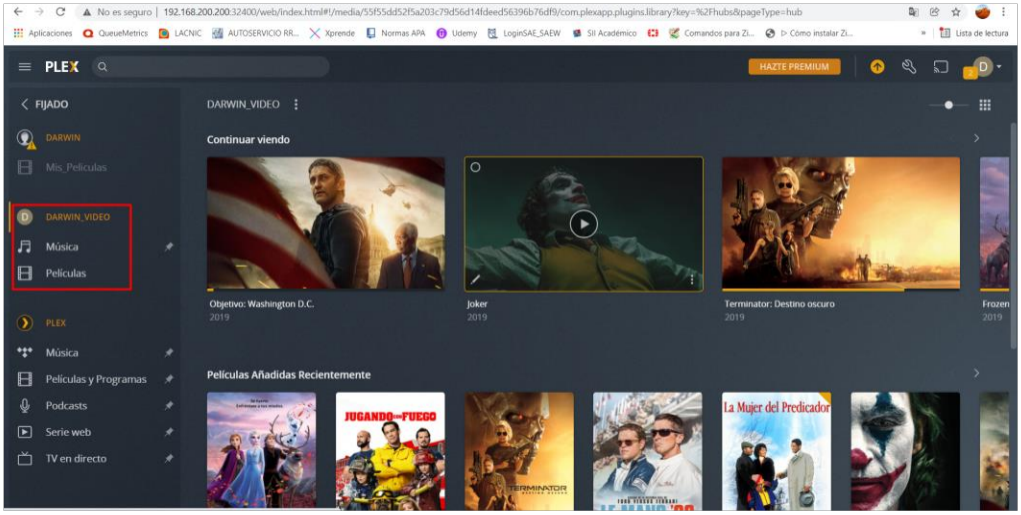


Figura A.36. Plex como Cliente vía Web.

o. App Plex Cliente

Como podemos observar, Plex se puede utilizar en diferentes dispositivos como cliente para reproducir el contenido que se tiene alojado en Plex como servidor, funcionando de esta manera como un cliente–servidor.

Figura A.37. Plex como cliente en App.

3 BIBLIOGRAFÍA

[1] Programasvirtualespc.net. 2021. *VMware Workstation Pro (2021) v16.2.0 Full + Serial [Mega]*. [online] Available at: <https://www.programasvirtualespc.net/utilidades/vmware-workstation-pro-12-5-1-4542065-full-seriales-windows/> [Accessed 26 December 2021].

[2] 4LiveHost. 2021. *Como Instalar Zimbra en Ubuntu Server 16.04*. [online] Available at: <https://4livehost.com/como-instalar-zimbra-en-ubuntu/> [Accessed 26 December 2021].

[3] Fernández, Y., 2020. *Plex, qué es y cómo funciona*. [online] Xataka.com. Available at: <https://www.xataka.com/basics/plex-que-es-y-como-funciona> [Accessed 28 December 2021].

ANEXO III

DETALLES DE LA CONFIGURACIÓN E IMPLEMENTACIÓN DE LA SD-WAN

Índice de Contenido

1 FUNCIONAMIENTO DE LA SD-WAN

1.1 ENLACES SD-WAN

1.1.1 ENLACES SD-WAN SEDE IBARRA

A continuación, se muestra en la figura 1.1 los enlaces WAN de la red MPLS y de Acceso a Internet, así como los túneles IPSec creados para brindar seguridad y permita conectarse con Quito y Guayaquil; formando parte de los enlaces SD-WAN.

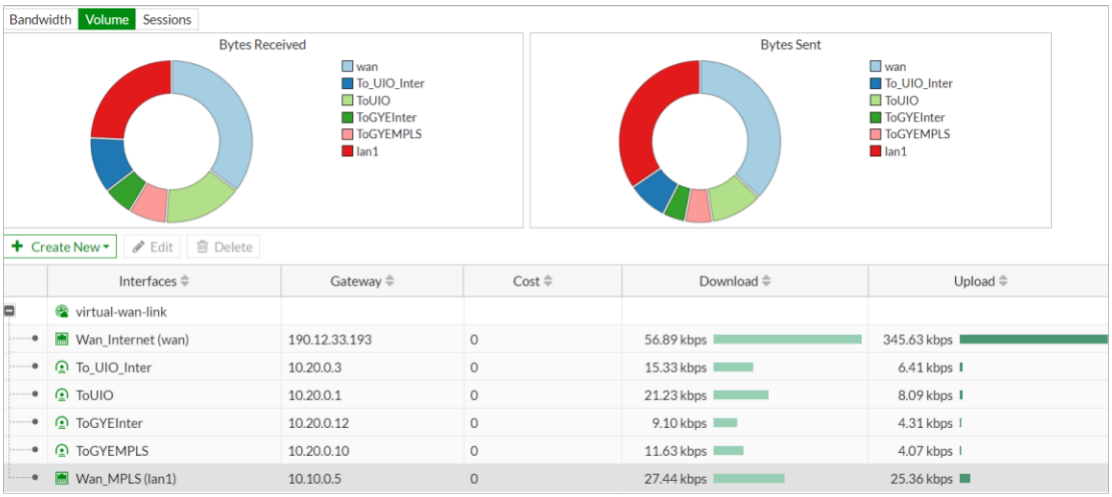


Figura 1.1. Enlaces SD-WAN Ibarra.

1.1.2 ENLACES SD-WAN SUCURSAL GUAYAQUIL

En la figura 1.2 se muestran los enlaces WAN y túneles IPSec creados en la Sucursal de Guayaquil y que de igual manera forman parte de la SD-WAN para la interacción con los sitios de Quito e Ibarra.

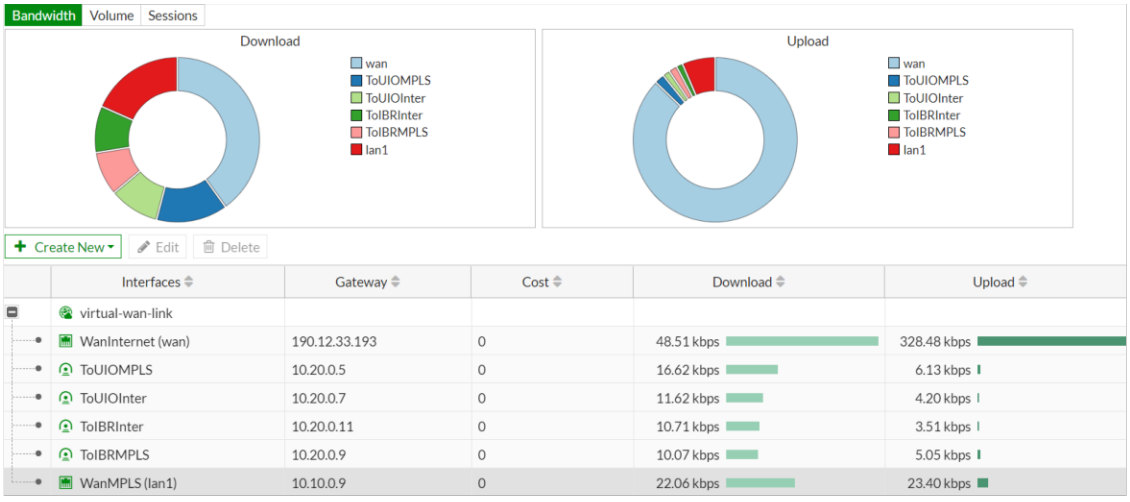


Figura 1.2. Enlaces SD-WAN Guayaquil.

1.2 RUTAS ESTÁTICA

1.2.1 RUTAS ESTÁTICAS SEDE IBARRA

Como se indica en la Sede Central Quito, se define una ruta estática por defecto 0.0.0.0/0, adicional a esta ruta se deben definir rutas que nos permitan alcanzar las IP destino de la WAN y los túneles en Quito y Guayaquil. En la figura 1.3 se muestran las rutas estáticas creadas en la Sede Ibarra y que nos permite alcanzar las IPs destino de la WAN MPLS y la red de Acceso a Internet como los túneles creados en cada una de las interfaces WAN.

Destination	Gatewa...	Interface	Status	Distance
IPv4 9				
0.0.0.0/0		SD-WAN	Enabled	1
190.12.33.194/32	190.12.33.193	Wan_Internet (wan)	Enabled	10
10.20.0.3/32	190.12.33.193	Wan_Internet (wan)	Enabled	10
190.12.33.196/32	190.12.33.193	Wan_Internet (wan)	Enabled	10
10.20.0.12/32	190.12.33.193	Wan_Internet (wan)	Enabled	10
10.10.0.0/30	10.10.0.5	Wan_MPLS (lan1)	Enabled	10
10.10.8.0/30	10.10.0.5	Wan_MPLS (lan1)	Enabled	10
10.20.0.1/32	10.10.0.5	Wan_MPLS (lan1)	Enabled	10
10.20.0.10/32	10.10.0.5	Wan_MPLS (lan1)	Enabled	10

Figura 1.3. Rutas estáticas Sede Ibarra.

1.2.2 RUTAS ESTÁTICAS SUCURSAL GUAYAQUIL

Al igual que en las otras sedes, se tiene la ruta por defecto 0.0.0.0/0 asociada a las SD-WAN, adicional se debe definir las rutas que nos permita alcanzar las IPs destino de las WAN y de los túneles en Quito e Ibarra. En la figura 1.4 se muestran las rutas estáticas de la Sucursal Guayaquil, que nos permite alcanzar las IPs destino de los túneles IPSec y las WAN de los sitios remotos.

Destination	Gateway...	Interface	Status	Distance
IPv4 9				
0.0.0.0/0		SD-WAN	Enabled	1
190.12.33.194/32	190.12.33.193	WanInternet (wan)	Enabled	10
190.12.33.195/32	190.12.33.193	WanInternet (wan)	Enabled	10
10.20.0.7/32	190.12.33.193	WanInternet (wan)	Enabled	10
10.20.0.11/32	190.12.33.193	WanInternet (wan)	Enabled	10
10.10.0.0/30	10.10.0.9	WanMPLS (lan1)	Enabled	10
10.10.0.4/30	10.10.0.9	WanMPLS (lan1)	Enabled	10
10.20.0.5/32	10.10.0.9	WanMPLS (lan1)	Enabled	10
10.20.0.9/32	10.10.0.9	WanMPLS (lan1)	Enabled	10

Figura 1.4. Rutas estáticas Sucursal Guayaquil.

1.3 POLÍTICAS Y OBJETOS

De igual forma se indica en este anexo que Fortinet llama ***objetos*** a las subredes, IPs o rango de IP que intervienen en las políticas. A continuación, se explican las políticas en cada una de las sedes para poder dar salida o no y sentido al tráfico.

1.3.1 POLÍTICAS SEDE CENTRAL QUITO

En la Sede Central Quito se definen 11 políticas mostrada en la figura 1.5, incluida su política por defecto que es negar todo tipo de tráfico, por lo que se coloca al final de todas las políticas, definiendo un orden jerárquico de forma descendente.

En orden jerárquico se ha definido como primera a la política ***Cliente -> ToIBR_GYE*** define como puerto de entrada la *Vlan_Cliente(VLAN10)* y como salida la *SD-WAN*, la subred de origen corresponde a la *Subnet_ClienteUIO* y las subredes de destino *Subnet_IBR_Multimedia, SubnetIBR_Clientes y Subnet_GYE*. Esta política permite que la Sede Principal Quito tenga conectividad con los puntos de Ibarra y Guayaquil de forma unidireccional.

La política ***ToIBR->Retirar(PRUEBA)*** se tiene el puerto de entrada la *Vlan_Zimbra(Vlan100)* y como puerto de salida la SD-WAN; las subredes de origen *UsuarioRemoto* y *Subnet_Zimbra*; y como subredes de destino las *Subnet_IBR_Multimedia*, *Subnet_GYE* y *SubnetIBR_Clientes*. Esta política se creó a modo de Prueba, para poder validar que tanto la LAN del servidor Zimbra y los usuarios remotos puedan acceder cada una de las LAN dentro del proyecto, esta política en la práctica debe ser eliminada, ya que no se requiere que los usuarios remotos o algún atacante que logre acceder a la LAN del servidor, tenga acceso a las redes de Ibarra o Guayaquil, con esta política se puede tener un hueco se seguridad.

Siguiendo la línea de la política *Cliente -> ToIBR_GYE*, para poder tener conectividad en el sentido contrario se establece la política ***FromIBR_GYE ->Clientes*** donde el puerto de entrada es la *SD-WAN* y el puerto de salida la *Vlan_Cliente(VLAN10)*, las subredes de origen corresponden a *MPLS, VPN, SubnetIBR_Clientes, Subnet_GYE*, *Subnet_IBR_Multimedia* y la subred de destino seria *Subnet_ClientesUIO*. Con estas dos políticas se tiene conectividad en ambos sentidos entre la Sede Central Quito con Ibarra y Guayaquil, de esta manera podemos acceder a los servidores DNS, correo electrónico desde cualquier LAN.

La política ***FromIBR_GYE ->Zimbra*** tiene como puerto de entrada la *SD-WAN* y el puerto de salida la Vlan_Cliente(Vlan100); las subredes de origen *MPLS, VPN, SubnetIBR_Clientes, Subnet_GYE*, *Subnet_IBR_Multimedia* y la subred de destino sería *Subnet_Zimbra*. Con esta política se da acceso para que las LAN de los usuarios de los sitios Ibarra y Guayaquil tengan acceso a los servidores DNS y correo Zimbra en Quito.

La política ***MPLS_IBR_GYE -> Internet***, tiene como puerto de entrada la SD-WAN y de la misma manera el puerto de salida la SD-WAN; las subredes de origen *MPLS, VPN, SubnetIBR_Clientes, Subnet_GYE*, *Subnet_IBR_Multimedia* y como subred de destino **all**. Esta política es muy importante para que la Sede Central también dé salida a Internet a través de la MPLS a las subredes de Ibarra y Guayaquil, en el caso que las sucursales tengan inconvenientes con su WAN de Internet propia, dándoles redundancia en la navegación.

La política ***Vlan10->Vlan100***, tiene como puerto de entrada la *Vlan_Cliente* y como puerto de salida la *Vlan_Zimbra(Vlan100)*; la subred de origen *Subnet_ClientesUIO* y la subred de destino la *Subnet_Zimbra*. Con esta política la LAN de usuarios de Quito pueden acceder a los servidores DNS y Correo Zimbra, por motivo de seguridad se tiene segmentado en dos VLAN. No se debe crear una política en el otro sentido, para no generar un hueco de seguridad en la red.

La política ***UsuarioRemotoZimbra***, tiene como puerto de entrada *SSL-VPN tunnel interface (ssl.root)* y como puerto de salida *Vlan_Zimbra(Vlan100)*; la subred de origen *UsuarioRemoto* y *SSLVPN_TUNNEL_ADDR1* y la subred de destino *Zimbra*. Con esta política se da acceso a los usuarios que están fuera de la intranet y necesitan acceso remoto, con la particularidad que solo puede acceder a la IP 192.168.100.100 que es la IP del servidor DNS y Zimbra, más no puede acceder a ninguna otra IP dentro de la LAN del servidor Zimbra.

La política ***AccesoRemotoMultimedia***, tiene como puerto de entrada *SSL-VPN tunnel interface (ssl.root)* y como puerto de salida *SD-WAN*; la subred de origen *UsuarioRemoto* y *SSLVPN_TUNNEL_ADDR1* y la subred de destino *Multimedia*. Con esta política se da acceso a los usuarios que están fuera de la intranet y necesitan acceso remoto al servidor multimedia que se encuentra en la Sede Ibarra, de igual forma solo puede acceder a la IP 192.168.200.200 que es la IP del servidor multimedia Plex y no podrá acceder a ninguna otra IP dentro de la LAN del servidor Multimedia.

La política ***AccesoInternetPrueba***, se define el puerto de entrada la *Vlan_Zimbra(Vlan100)* y como salida el puerto *SD-WAN*, la subred de origen es la *Subnet_Zimbra* y como destino ***all***, haciendo referencia a Internet. Esta política sirve para navegar por Internet a la LAN de los servidores DNS y Zimbra; a modo de prueba y para actualizaciones de los servidores, pero se debe tener desactivada, ya que puede ser un hueco de seguridad si la tenemos habilitada siempre.

La política ***AccesoInternet_Clientes***, se define el puerto de entrada la *Vlan_Cliente(Vlan10)* y como salida el puerto *SD-WAN*, la subred de origen es la *Subnet_ClienteUIO* y como destino ***all***, haciendo referencia a Internet. Con esta política se da acceso de navegación por Internet a la LAN de los usuarios en Quito.

También existe una política por defecto la cual es negar cualquier tipo de tráfico hacia cualquier destino, la cual debe ser colocada al final de todas las políticas y permita que siga un orden jerárquico cumpliendo las primeras políticas, esta política es conocida como ***Implicit Deny***.

Name	From	To	Source	Destination	Service	Action	NAT
Cliente -> TolBR_GYE	Vlan_Cliente (Vlan10)	virtual-wan-link	Subnet_ClientesUIO	Subnet_IBR_Multimedia SubnetIBR_Clientes Subnet_GYE	HTTP HTTPS ALL_ICMP	ACCEPT	Disabled
TolBR -> Retirar (PRUEBA)	Vlan_Zimbra (Vlan100)	virtual-wan-link	UsuarioRemoto Subnet_Zimbra	Subnet_IBR_Multimedia Subnet_GYE SubnetIBR_Clientes	HTTP HTTPS ALL_ICMP	ACCEPT	Disabled
FromIBR_GYE ->Clientes	virtual-wan-link	Vlan_Cliente (Vlan10)	MPLS VPN SubnetIBR_Clientes Subnet_GYE Subnet_IBR_Multimedia	Subnet_ClientesUIO	CorreoZimbra ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
FromIBR_GYE ->Zimbra	virtual-wan-link	Vlan_Zimbra (Vlan100)	MPLS VPN SubnetIBR_Clientes Subnet_IBR_Multimedia Subnet_GYE	Subnet_Zimbra	CorreoZimbra ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
MPLS_IBR_GYE -> Internet	virtual-wan-link	virtual-wan-link	MPLS VPN Subnet_GYE SubnetIBR_Clientes Subnet_IBR_Multimedia	all	ALL	ACCEPT	Enabled
Vlan10 -> Vlan100	Vlan_Cliente (Vlan10)	Vlan_Zimbra (Vlan100)	Subnet_ClientesUIO	Subnet_Zimbra	HTTP HTTPS ALL_ICMP CorreoZimbra	ACCEPT	Disabled
UsuarioRemotoZimbra	SSL-VPN tunnel interface (ssl.root)	Vlan_Zimbra (Vlan100)	UsuarioRemoto SSLVPN_TUNNEL_ADDR1	Zimbra	ALL_ICMP CorreoZimbra HTTP HTTPS	ACCEPT	Enabled
AccesoRemotoMultimedia	SSL-VPN tunnel interface (ssl.root)	virtual-wan-link	UsuarioRemoto SSLVPN_TUNNEL_ADDR1	Multimedia	ALL	ACCEPT	Enabled
AccesoInternetPrueba	Vlan_Zimbra (Vlan100)	virtual-wan-link	Subnet_Zimbra	all	ALL	ACCEPT	Enabled
AccesoInternet_Clientes	Vlan_Cliente (Vlan10)	virtual-wan-link	Subnet_ClientesUIO	all	ALL	ACCEPT	Enabled
Implicit Deny	any	any	all	all	ALL	DENY	

Figura 1.5. Políticas Sede Central Quito.

1.3.2 POLÍTICAS SEDE IBARRA

Para la sede Ibarra de igual se define 8 políticas definiendo un orden jerárquico de forma descendente como se muestra en la figura 1.6.

La política ***Multimedia_To_UIO_GYE(Prueba)***, tiene como puerto de entrada a *VlanMultimedia(Vlan200)* y como puerto de salida la *SD-WAN*; la subred de origen *Subnet_IBR_Multimedia* y las subredes de destino *Subnet_Zimbra*, *Subnet_GYE* y *SubnetClientesUIO*. Esta política es para pruebas, que nos permite tener conectividad con las LAN de Quito y Guayaquil, esta política debe ser retirada o inhabilitada, ya que puede ser un hueco de seguridad en la red.

La política ***Clientes -> ToUIO_GYE***, tiene como puerto de entrada la *VlanClientes(Vlan2)* y como puerto de salida la *SD-WAN*; la subred de origen *SubnetClienteIBR* y las subredes de destino *Subnet_Zimbra*, *SubnetClientesUIO* y la *Subnet_GYE*. Esta política permite a la LAN de usuarios de Ibarra tener conectividad unidireccional con las LAN de los usuarios en Quito y Guayaquil y también acceder al servidor DNS y correo Zimbra en Quito.

La política ***FromUIO_GYE -> Multimedia***, tiene como puerto la *SD-WAN* y como puerto de salida la *VlanMultimedia(Vlan200)*; tiene como subredes de origen *Subnet_Zimbra*, *MPLS*, *VPN*, *SubnetClientesUIO*, *Subnet_GYE* y *UsuarioRemoto* y como subred de destino la *Subnet_IBR_Multimedia*. Esta política permite que las LAN de los usuarios de Quito y Guayaquil y los usuarios remotos tengan acceso al servidor Multimedia.

La política ***FromUIO_GYE -> Clientes***, tiene como puerto la *SD-WAN* y como puerto de salida la *VlanClientes(Vlan2)*; tiene como subredes de origen *Subnet_Zimbra*, *MPLS*, *VPN*, *SubnetClientesUIO* y *Subnet_GYE* y como subred de destino la *SubnetClienteIBR.* Esta política en conjunto con la política ***Clientes -> ToUIO_GYE*** permiten tener conectividad en ambos sentidos con las LAN de los usuarios en Quito y Guayaquil y los servidores DNS y Zimbra.

La política ***Vlan2 ->Vlan200***, tiene como puerto de entrada la *VlanClientes (Vlan2)* y como puerto de salida la *VlanMultimedia(Vlan200)*; la subred de origen *SubnetClienteIBR* y la subred de destino la *Subnet_IBR_Multimedia*. Con esta política la LAN de usuarios de Ibarra pueden acceder al servidor multimedia Plex, por motivo de seguridad se tiene segmentado en dos VLAN. No se debe crear una política en el otro sentido, para evitar un hueco de seguridad en la red.

La politica ***ClientesToInternet***, tiene como puerto de entrada la *VlanClientes(Vlan2)* y como puerto de salida la *SD-WAN*; la subred de origen *SubnetClienteIBR* y la subred de destino ***all***. Con esta política se permite a la LAN de usuarios de Ibarra navegar por Internet.

La política ***MultimediaToInternet(Prueba)***, tiene como puerto de entrada la *VlanMultimedia(Vlan200)* y como puerto de salida la *SD-WAN*; la subred de origen *Subnet_IBR_Multimedia* y la subred de destino ***all***. Con esta política se permite a la LAN del servidor Multimedia Plex navegar por Internet, al igual que los servidores DNS y Zimbra, se tiene que tener inhabilitada esta política y solo utilizarla en momentos que se necesite para actualizaciones, ya que puede generarse un hueco de seguridad.

Por último, se tiene la política por defecto ***Implicit Deny***, la cual cumple la función de negar cualquier tipo de tráfico hacia cualquier destino, la cual debe ser colocada al final de todas las políticas y permita que siga un orden jerárquico cumpliendo las primeras políticas.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
Multimedia_To_UIO_GYE(Prueba)	VlanMultimedia (Vlan200)	virtual-wan-link	Subnet_IBR_Multimedia	Subnet_Zimbra Subnet_GYE SubnetClientesUIO	always	ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
Clientes -> ToUIO_GYE	VlanClientes (Vlan2)	virtual-wan-link	SubnetClienteIBR	Subnet_Zimbra SubnetClientesUIO Subnet_GYE	always	ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
FromUIO_GYE -> Multimedia	virtual-wan-link	VlanMultimedia (Vlan200)	Subnet_Zimbra MPLS VPN SubnetClientesUIO Subnet_GYE UsuarioRemoto	Subnet_IBR_Multimedia	always	ALL_ICMP HTTP HTTPS Multimedia	ACCEPT	Disabled
FromUIO_GYE -> Clientes	virtual-wan-link	VlanClientes (Vlan2)	Subnet_Zimbra MPLS VPN SubnetClientesUIO Subnet_GYE	SubnetClienteIBR	always	ALL_ICMP HTTP HTTPS Multimedia	ACCEPT	Disabled
Vlan2 -> Vlan200	VlanClientes (Vlan2)	VlanMultimedia (Vlan200)	SubnetClienteIBR	Subnet_IBR_Multimedia	always	ALL_ICMP HTTP HTTPS Multimedia	ACCEPT	Disabled
ClientesToInternet	VlanClientes (Vlan2)	virtual-wan-link	SubnetClienteIBR	all	always	ALL	ACCEPT	Enabled
MultimediaToInternet(Prueba)	VlanMultimedia (Vlan200)	virtual-wan-link	Subnet_IBR_Multimedia	all	always	ALL	ACCEPT	Enabled
Implicit Deny	any	any	all	all	always	ALL	DENY	

Figura 1.6. Políticas Sede Ibarra.

1.3.3 POLÍTICAS SUCURSAL GUAYAQUIL

Las políticas que se crean en Guayaquil son cuatro, al ser una sucursal tiene un rol más sencillo en comparación con la Sede Central Quito o la Sede Ibarra que son muy similares.

A continuación, en la figura 1.7 se muestran las políticas creadas para tener conectividad entre LAN de usuarios y acceder a los servicios de DNS, correo electrónico y multimedia.

La política ***ToIBR_UIO***, tiene como puerto de entrada la *Vlan30* y como puerto de salida la *SD-WAN*; la subred de origen *SubnetClientesGYE* y las subredes de destino *SubnetClientesIBR*, *SubnetClientesUIO*, *SubnetMultimedia* y la *SubnetZimbra*. Esta política nos permite tener conectividad unidireccional a la LAN de los usuarios y los servidores de DNS, Zimbra y multimedia Plex ubicados en Quito e Ibarra.

La política ***FromIBR_UIO***, tiene como puerto de entrada la *SD-WAN* y como puerto de salida la *Vlan30*; las subredes de origen *SubnetClientesIBR*, *SubnetClientesUIO*, *SubnetMultimedia*, *SubnetZimbra*, *MPLS* y *VPN*; y la subred de destino *SubnetClientesGYE*. Esta política con la política ToIBR_UIO nos permite tener conectividad en ambos sentidos a la LAN de los usuarios y los servidores DNS, Zimbra y multimedia Plex.

La política ***AccesoInternet***, tiene como puerto de entrada la *Vlan30* y como puerto de salida la *SD-WAN*; la subred de origen *SubnetClientesGYE* y la subred de destino ***all***. Esta política permite a la red de usuarios en la sucursal Guayaquil navegar por Internet.

Y finalmente se tiene la política por defecto ***Implicit Deny***, cumpliendo la función de negar todo tipo de tráfico a cualquier dirección, por lo que siempre o en la mayoría de casos se debe colocar al última para que siga la secuencia en orden jerárquico descendente y permita que las primeras políticas dejen pasar el tráfico de acuerdo a las necesidades de la red.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
ToIBR_UIO	Vlan30	virtual-wan-link	SubnetClientesGYE	SubnetClientesIBR SubnetClientesUIO SubnetMultimedia SubnetZimbra	always	ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
FromIBR_UIO	virtual-wan-link	Vlan30	SubnetClientesIBR SubnetClientesUIO SubnetMultimedia SubnetZimbra MPLS VPN	SubnetClientesGYE	always	ALL_ICMP HTTP HTTPS	ACCEPT	Disabled
AccesoInternet	Vlan30	virtual-wan-link	SubnetClientesGYE	all	always	ALL	ACCEPT	Enabled
Implicit Deny	any	any	all	all	always	ALL	DENY	

Figura 1.7. Políticas Sucursal Guayaquil.

1.4 REGLAS DE LA SD-WAN

Las reglas SD-WAN se configuran para determinar el comportamiento de la SD-WAN, permitiendo ser inteligente y con libre autonomía para tomar decisiones a la hora de enrutar el tráfico contemplando ciertos parámetros como latencia, jitter, perdida de paquetes. De igual manera que las políticas, se debe aplicar las reglas SD-WAN en orden descendente.

1.4.1 REGLAS SD-WAN SEDE IBARRA

En la figura 1.8 se muestra las reglas SD-WAN en la Sede Ibarra y que nos permite tener una red más inteligente, a continuación, se explica su mecanismo; la primera regla

ToZimbra tiene como objetivo alcanzar desde Ibarra los servidores DNS y Zimbra ubicados en Quito a través de un camino determinado que por seguridad se define al túnel IPSec creado por la MPLS llamado *ToUIO*. Si el túnel ToUIO no está disponible, pasará a la segunda regla ***ToZimbraInternet***, con el mismo objetivo de la primera regla alcanzar los servidores DNS y Zimbra, pero esta vez a través del túnel IPSec creado por la WAN de Internet llamado *To_UIO_Inter*.

La tercera regla se llama ***ToUIO***, desde Ibarra nos permite alcanzar cualquier IP de las subredes de Quito a través de cualquier túnel IPSec *ToUIO* o *To_UIO_Inter*, tomando la mejor ruta automáticamente en base al parámetro latencia, determinando una ruta con menor retardo.

La cuarta regla se llama ***ToGYE***, desde Ibarra nos permite alcanzar cualquier IP de la subred del usuario de Guayaquil a través de cualquier túnel IPSec *ToGYEInter* o *ToGYEMPLS*, de la misma forma tomará la mejor ruta automáticamente en base al parámetro latencia, determinando una ruta con menor retardo.

Name	Source	Destination	Crite...	Members
IPv4 7				
ToZimbra	Subnet_IBR_Multimedia SubnetClienteIBR	ToZimbra	Latency	ToUIO
ToZimbraInternet	Subnet_IBR_Multimedia SubnetClienteIBR	ToZimbra	Latency	To_UIO_Inter
ToUIO	SubnetClienteIBR Subnet_IBR_Multimedia	Subnet_Zimbra SubnetClientesUIO	Latency	ToUIO To_UIO_Inter
ToGYE	SubnetClienteIBR Subnet_IBR_Multimedia	Subnet_GYE	Latency	ToGYEInter ToGYEMPLS
Zoom	Subnet_IBR_Multimedia SubnetClienteIBR	Zoom.us-Zoom.Meeting Zoom Zoom_File.Download Zoom_File.Upload +3	Latency	ToUIO
AccesoInternet	Subnet_IBR_Multimedia SubnetClienteIBR	all	Latency	Wan_Internet (wan)
AccesoInternetTunnelUIO	Subnet_IBR_Multimedia SubnetClienteIBR	all	Latency	ToUIO
Implicit 1				
sd-wan	all	all	Volume	any

Figura 1.8. Reglas SD-WAN Sede Ibarra.

La quinta regla llamada ***Zoom***, define a las subredes de Ibarra que, si van a realizar una reunión por la App Zoom, tomen como salida el Internet que le proporciona la Sede Central Quito a través del túnel IPSec *ToUIO* creado por la MPLS.

La sexta regla ***AccesoInternet***, tiene como objetivo dar salida a Internet por su propia WAN de Internet a las subredes de la Sede Ibarra. La séptima regla ***AccesoInternetTunnelUIO***, tiene el mismo objetivo que la sexta regla, solo que la salida

a Internet será por la Sede Central Quito, a través del túnel IPSec *ToUIO* de forma predeterminada creado por la WAN MPLS.

Y la octava regla ***sd-wan***, es una regla por defecto para permitir todo tipo de tráfico a cualquier destino.

1.4.2 REGLAS SD-WAN SUCURSAL GUAYAQUIL

A continuación, en la figura 1.9 se muestran las reglas SD-WAN creadas en la Sucursal Guayaquil, que nos permite tener una red más inteligente para poder alcanzar los servicios del proyecto o servicios en la red de Internet.

La primera regla llamada ***ToZimbra***, tiene como objetivo que la LAN de Guayaquil pueda alcanzar el servidor DNS y Zimbra ubicados en la Sede Central Quito a través del túnel IPSec *ToUIOMPLS* de forma predeterminada creado por seguridad por la WAN MPLS.

La segunda regla ***ToMultimedia***, tiene como objetivo alcanzar el servidor multimedia Plex ubicado en la Sede Ibarra a través del túnel IPSec *ToIBRInter* de forma predeterminada creado por la WAN de Internet.

La tercera regla ***LanUIO***, permite a la LAN de usuarios de Guayaquil alcanzar cualquier IP o host de las subredes ubicadas en la Sede Central Quito, sea por el túnel IPSec de la WAN MPLS *ToUIOMPLS* o por el túnel IPSec *ToUIOInter* de la WAN de Internet, tomando la mejor ruta en base al parámetro de latencia determinando una ruta con menor retardo.

La cuarta regla ***LanIBR***, permite a la LAN de usuarios de Guayaquil alcanzar cualquier IP o host de las subredes ubicadas en la Sede Ibarra, sea por el túnel IPSec de la WAN MPLS *ToIBRMPLS* o por el túnel IPSec *ToIBRInter* de la WAN de Internet, tomando la mejor ruta en base al parámetro de latencia determinando una ruta con menor retardo.

La quinta regla ***Zoom***, define a la LAN de usuarios de Guayaquil que, si van a realizar una reunión por la App Zoom, tomen como salida el Internet que le proporciona la Sede Central Quito a través del túnel IPSec *ToUIOMPLS* creado por la MPLS.

La sexta regla ***Webex***, define a la LAN de usuarios de Guayaquil que, si van a realizar una reunión por la App Webex, tomen su propia salida a Internet o por la salida que le proporciona la Sede Central Quito a través del túnel IPSec *ToUIOMPLS*, todo dependerá que salida tome en función de un SLA, determinando la mejor ruta.

La séptima regla ***AccesoInternet***, tiene como objetivo dar navegación por el Internet a la red LAN de usuarios de la sucursal Guayaquil, a través de su propia WAN de Internet o

por el túnel IPSec *ToUIOMPLS* creado por la WAN MPLS para alcanzar la salida por la Sede Central Quito, dependiente que ruta tome de acuerdo a la latencia entre los dos enlaces de la SD-WAN.

Y la octava regla ***sd-wan***, es una regla por defecto para permitir todo tipo de tráfico a cualquier destino.

Name	Source	Destination	Crite...	Members
IPv4 7				
ToZimbra	SubnetClientesGYE	Zimbra	Latency	ToUIOMPLS
ToMultimedia	SubnetClientesGYE	Multimeda	Latency	ToIBRInter
LanUIO	SubnetClientesGYE	SubnetClientesUIO SubnetZimbra	Latency	ToUIOMPLS ToUIOInter
LanIBR	SubnetClientesGYE	SubnetClientesIBR SubnetMultimedia	Latency	ToIBRInter ToIBRMPLS
Zoom	SubnetClientesGYE	Zoom.us-Zoom.Meeting Zoom Zoom_File.Download Zoom_File.Upload +3	Latency	ToUIOMPLS
Webex	SubnetClientesGYE	Cisco-Webex Cisco-Webex.FedRAMP WebEx WebEx_Chat +7	SLA	ToUIOMPLS WanInternet (wan)
AcessoInternet	SubnetClientesGYE	all	Latency	WanInternet (wan) ToUIOMPLS
Implicit 1				
sd-wan	all	all	Source IP	any

Figura 1.9. Reglas SD-WAN Sucursal Guayaquil.

1.5 VPN IPSec

Las VPN se integran en el proyecto para brindar seguridad en la transmisión de los datos entre sedes, creando túneles tanto a nivel de la WAN MPLS como la WAN de Acceso a Internet, a continuación, se detalla de la Sede Ibarra y la sucursal Guayaquil.

1.5.1 VPN IPSec SEDE IBARRA

En la figura 1.10 se muestra los túneles creados en la Sede Ibarra, como en la Sede Central Quito, se crea de igual manera cuatro túneles; dos de ellos para alcanzar a Quito, uno por la WAN MPLS ***ToUIO*** y uno por la WAN de acceso a Internet ***To_UIO_Inter***; también se crea dos túneles para alcanzar la sucursal de Guayaquil, uno a través de la WAN MPLS ***ToGYEMPLS*** y uno a través de la WAN de acceso a Internet ***ToGYEInter***.

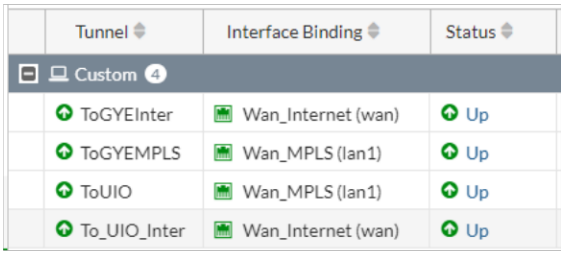


Figura 1.10. Túnel IPSec Sede Ibarra.

1.5.2 VPN IPSec SUCURSAL GUAYAQUIL

En la figura 1.11 se muestran los túneles creados en la Sucursal de Guayaquil, estos túneles sirven para poder conectarse con la Sede Central Quito y la Sede Ibarra, de igual manera se cuenta con cuatro túneles IPSec para brindar seguridad en la transmisión de los datos. Se tiene dos túneles creados a través de la red MPLS, el túnel ***ToIBRMPLS*** sirve para alcanzar Ibarra y el túnel ***ToUIOMPLS*** para alcanzar Quito; también se tiene dos túneles a través de la red de acceso a Internet, el túnel ***ToIBRInter*** para alcanzar Ibarra y el túnel ***ToUIOInter*** para alcanzar Quito.

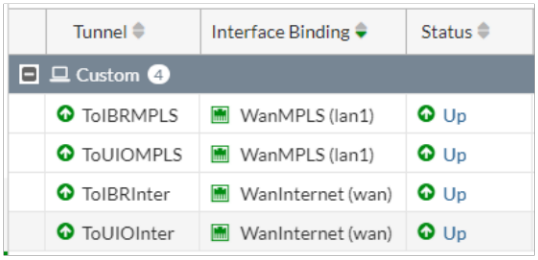


Figura 1.11. Túnel IPSec Sucursal Guayaquil.

1.6 POLÍTICAS TRAFFIC SHAPING

Las políticas Traffic Shaping tienen como objetivo optimizar y aprovechar de mejor manera el ancho de banda contratado, reduciendo justamente los costos en la adquisición del ancho de banda a un proveedor de servicios.

1.6.1 POLÍTICAS DE TRAFFIC SHAPING SEDE CENTRAL QUITO

En la Sede Central Quito se dispone de cuatro políticas como se muestra en la figura 1.12, la primera política ***ShapingZimbra*** tiene como subredes de origen *MPLS*, *Subnet_ClienteUIO, Subnet_GYE, Subnet_IBR_Multimedia, SubnetIBR_Clientes, VPN* y *SSLVPN_TUNNEL_ADDR1* y IP de destino *Zimbra*; puerto de salida la

Vlan_Zimbra(Vlan100); se ingresa una velocidad de subida de 5Mbps y una velocidad de descarga de 5*Mbps*; limitamos por servicio *ALL_ICMP, CorreoZimbra, HTTP* y *HTTPS*, y por aplicación *Zimbra* y *FortiClient*. Con esta política lo que hacemos es limitar el Ancho de banda que dedicamos para el acceso a nuestro servidor Zimbra en la red LAN, compartiendo *5Mbps* de subida y de bajada con prioridad alta entre todas las subredes de nuestro proyecto, incluida para los usuarios remotos.

La segunda política ***ToMultimedia***, tiene como subredes de origen *Subnet_ClienteUIO* y *Subnet_Zimbra* y la IP de destino *Multimedia*; puerto de salida los túneles IPSec *To_IBR_Inter* (interfaz WAN Internet) y *ToIBR* (interfaz WAN MPLS); se ingresa una velocidad de subida de *10Mbps* y una velocidad de descarga de 10*Mbps*; limitamos por servicio *ALL_ICMP, HTTP, HTTPS*, *Multimedia* y por aplicación *Plex.TV* y *Plex.VPN*. Con esta política lo que logra limitar el ancho de banda de *10Mbps* de subida y bajada con prioridad alta que se asigna a la LAN de Quito para que pueda acceder al servidor multimedia Plex situado en Ibarra a través de los túneles creados en las WAN MPLS y red de acceso a Internet.

La tercera política ***Zoom***, tiene como subredes de origen todas las LAN asociadas al proyecto y como destino *Zoom.us-Zoom.Meeting*; puerto de salida es la interfaz WAN de Internet *WAN1*; se ingresa una velocidad de subida de *5Mbps* y una velocidad de descarga de *10Mbps*; limitamos por servicio *Internet Service* y por aplicación todo lo que es relacionado a *Zoom*. Con esta política logramos limitar el ancho de banda con prioridad alta y que se utilizará para las reuniones por Zoom de todas las LAN del proyecto, ya que en las reglas SD-WAN se definió que el tráfico de Zoom salga por Quito y de esta forma no utilizar más ancho de banda que será utilizado para los servicios internos de la red.

Name	Source	Destination	To	Shared Shaper	Reverse Shaper	Service	Applications
IPv4 2							
ShapingZimbra	MPLS Subnet_ClientesUIO Subnet_GYE Subnet_IBR_Multimedia SubnetIBR_Clientes VPN SSLVPN_TUNNEL_ADDR1	Zimbra	Vlan_Zimbra (Vlan100)	5M	5M	ALL_ICMP CorreoZimbra HTTP HTTPS	Zimbra FortiClient
ToMultimedia	Subnet_ClientesUIO Subnet_Zimbra	Multimedia	To_IBR_Inter ToIBR	10M	10M	ALL_ICMP HTTP HTTPS Multimedia	Plex.TV Plex.VPN
Zoom	Subnet_ClientesUIO Subnet_Zimbra MPLS Subnet_GYE Subnet_IBR_Multimedia SubnetIBR_Clientes VPN	Zoom.us-Zoom.Meeting	Wan_Internet (wan1)	5M	10M	Internet Service	Zoom Zoom_File.Download Zoom_File.Upload Zoom_Login Zoom_Meeting Zoom_Meeting.Remote.Control
ToInternet	MPLS Subnet_GYE Subnet_IBR_Multimedia SubnetIBR_Clientes VPN Subnet_ClientesUIO Subnet_Zimbra	all	Wan_Internet (wan1)	10M_Media	20M_Media	ALL	

Figura 1.12 Traffic Shaping Sede Central Quito.

La cuarta política ***ToInternet***, tiene como subredes de origen todas las LAN asociadas al proyecto y como destino Internet ***all***; puerto de salida es la interfaz WAN de Internet *WAN1*; se ingresa una velocidad de subida de *10Mbps* y una velocidad de descarga de 20*Mbps*; no se agrega limitación de servicios ni de aplicaciones ya que tiene salida al Internet. Con esta política se limita el ancho de banda con prioridad media de subida a *10Mbps* y de descarga a *20Mbps* a todas las LAN o subredes que se encuentran en Quito, Ibarra y Guayaquil para la salida a Internet.

1.6.2 POLÍTICAS DE TRAFFIC SHAPING SEDE IBARRA

En la Sede de Ibarra se tiene de igual forma cuatro políticas como se muestra en la figura 1.13, para el aprovechamiento de mejor manera del ancho de banda en la sede.

La primera política de nombre ***ShapingMultimedia*** tiene como subredes de origen *MPLS*, *Subnet_GYE, Subnet_Zimbra, SubnetClienteIBR, SubnetClientesUIO, VPN* y la IP de destino *Multimedia*; puerto de salida la *VlanMultimedia(Vlan200)*; se ingresa una velocidad de subida de *10Mbps* y una velocidad de descarga de 10*Mbps*; limitamos por servicio *ALL_ICMP, HTTP, HTTPS* y *Multimedia*, y por aplicación *Plex.Tv* y *Plex.VPN*. Con esta política lo que hacemos es limitar el Ancho de banda que dedicamos para el acceso a nuestro servidor multimedia Plex en la red LAN de Ibarra, compartiendo los *10Mbps* de subida y de bajada con prioridad alta entre todas las subredes de nuestro proyecto interno y también para los usuarios que se conectan remotamente.

La segunda política ***ToZimbra***, tiene como subredes de origen *Subnet_IBR_Multimedia* y *SubnetClienteIBR* y la IP de destino *Zimbra*; puerto de salida los túneles IPSec *To_UIO_Inter* (interfaz WAN Internet) y *ToUIO* (interfaz WAN MPLS); se ingresa una velocidad de subida de 5Mbps y una velocidad de descarga de 5*Mbps*; limitamos por servicio *ALL_ICMP, HTTP, HTTPS* y por aplicación *Zimbra*. Con esta política se logra limitar el ancho de banda de *5Mbps* de subida y bajada con prioridad alta, que se asigna a la LAN de Ibarra para acceder al servidor DNS y Zimbra ubicado en Quito a través de los túneles creados en las WAN MPLS y red de acceso a Internet.

La tercera política ***Zoom***, tiene como subredes de origen *Subnet_IBR_Multimedia* y *SubnetClienteIBR* y como destino *Zoom.us-Zoom.Meeting*; puerto de salida es el túnel *ToUIO* creado por la WAN MPLS; se ingresa una velocidad de subida de 5Mbps y una velocidad de descarga de 10*Mbps*; limitamos por servicio *Internet Service* y por aplicación todo lo que es relacionado a *Zoom*. Con esta política logramos limitar el ancho de banda con prioridad alta para las reuniones de los usuarios por la App Zoom, para poder

conectarse, en el proyecto se define que debe salir por la WAN de Internet de la Sede Central Quito, por lo que el tráfico atraviesa la MPLS por el túnel creado para alcanzar dicha sede.

La cuarta política ***IBR_ToInternet***, tiene como subredes de origen *Subnet_IBR_Multimedia* y *SubnetClienteIBR* y como destino Internet ***all***; puertos de salida es la interfaz WAN de Internet *wan* y el túnel de la MPLS hacia Quito *ToUIO*; se ingresa una velocidad de subida de 10Mbps y una velocidad de descarga de 10*Mbps*; no se agrega limitación de servicios ni de aplicaciones ya que tiene salida al Internet. Con esta política se limita el ancho de banda con prioridad media de subida y de bajada a 10Mbps, teniendo redundancia al momento de salir a Internet, siendo por su propia WAN de Internet o por la Sede Central Quito.

Name	Source	Destination	To	Shared Shaper	Reverse Shaper	Service	Applications
IPv4 4							
ShapingMultimedia	MPLS Subnet_GYE Subnet_Zimbra SubnetClienteIBR SubnetClientesUIO VPN	Multimedia	VlanMultimedia (Vlan200)	10M	10M	ALL_ICMP HTTP HTTPS Multimedia	PlexTV PlexVPN
ToZimbra	Subnet_IBR_Multimedia SubnetClienteIBR	ToZimbra	To_UIO_Inter ToUIO	5M	5M	ALL_ICMP HTTP HTTPS	Zimbra
Zoom	Subnet_IBR_Multimedia SubnetClienteIBR	Zoom.us-Zoom.Meeting	ToUIO	5M	10M	Internet Service	Zoom Zoom_File.Download Zoom_File.Upload Zoom_Login Zoom_Meeting Zoom_Meeting.Remote.Control
IBR_ToInternet	Subnet_IBR_Multimedia SubnetClienteIBR	all	Wan_Internet (wan) ToUIO	10M_Media	10M_Media	ALL	

Figura 1.13 Traffic Shaping Sede Ibarra.

1.6.3 POLÍTICAS DE TRAFFIC SHAPING SUCURSAL GUAYAQUIL

A continuación, se describen las políticas de Traffic Shaping en la sucursal de Guayaquil mostradas en la figura 1.14 con sus particularidades.

La primera política ***ToZimbra***, tiene como subred de origen *SubnetClientesGYE* y la IP de destino *Zimbra*; puertos de salida los túneles IPSec *ToUIOInter* (interfaz WAN Internet) y *ToUIOMPLS* (interfaz WAN MPLS); se ingresa una velocidad de subida de *5Mbps* y una velocidad de descarga de 5*Mbps*; limitamos por servicio *ALL_ICMP, HTTP, HTTPS* y por aplicación *Zimbra*. Con esta política se logra limitar el ancho de banda de *5Mbsp* de subida y bajada con prioridad alta, que se asigna a la LAN de Guayaquil para acceder al servidor DNS y Zimbra ubicado en Quito a través de los túneles creados por seguridad en las WAN MPLS y red de acceso a Internet.

La segunda política ***ToMultimedia***, tiene como subred de origen *SubnetClientesGYE* y la IP de destino *Multimedia*; puerto de salida los túneles IPSec *ToIBRInter* (interfaz WAN Internet) y *ToIBRMPLS* (interfaz WAN MPLS); se ingresa una velocidad de subida de *5Mbps* y una velocidad de descarga de 10*Mbps*; limitamos por servicio *ALL_ICMP, HTTP, HTTPS* y por aplicación *Plex.TV* y *Plex.VPN*. Con esta política se logra limitar el ancho de banda de *5Mbps* de subida y *10Mbps* de bajada con prioridad alta, que se asigna a la LAN de Guayaquil para que pueda acceder al servidor multimedia Plex situado en Ibarra a través de los túneles creados en las WAN MPLS y red de acceso a Internet.

La tercera política ***Zoom***, tiene como subred de origen *SubnetClientesGYE* y como destino *Zoom.us-Zoom.Meeting*; puerto de salida es el túnel *ToUIOMPLS* creado por la WAN MPLS; se ingresa una velocidad de subida de *5Mbps* y una velocidad de descarga de 10*Mbps*; limitamos por servicio *Internet Service* y por aplicación todo lo que es relacionado a *Zoom*. Con esta política logramos limitar el ancho de banda con prioridad alta para las reuniones de los usuarios por la App Zoom, para poder conectarse, en el proyecto se define de igual manera que debe salir por la WAN de Internet de la Sede Central Quito, por lo que el tráfico atraviesa la MPLS por el túnel creado para alcanzar dicha sede.

Name	Source	Destination	To	Shared Shap...	Reverse Shaper	Service	Applications
IPv4 5							
ToZimbra	SubnetClientesGYE	Zimbra	ToUIOInter ToUIOMPLS	5M	5M	HTTP HTTPS ALL_ICMP	Zimbra
ToMultimedia	SubnetClientesGYE	Multimeda	ToIBRInter ToIBRMPLS	5M	10M	HTTP HTTPS ALL_ICMP	Plex.TV Plex.VPN
Zoom	SubnetClientesGYE	Zoom.us-Zoom.Meeting	ToUIOMPLS	5M	10M	Internet Service	Zoom Zoom_File.Download Zoom_File.Upload Zoom_Login Zoom_Meeting Zoom_Meeting.Remote.Control
Webex	SubnetClientesGYE	Cisco-Webex Cisco-Webex.FedRAMP	ToUIOMPLS WanInternet (wan)	5M	10M_Media	Internet Service	WebEx WebEx_Chat WebEx_Desktop.Sharing WebEx_File.Download WebEx_File.Sharing WebEx_File.Upload WebEx_Login WebEx_Remote.Control WebEx_WhiteBoard
ToInternet	SubnetClientesGYE	all	WanInternet (wan) ToUIOMPLS	10M_Media	10M_Media	ALL	

Figura 1.14 Traffic Shaping Sucursal Guayaquil.

La cuarta política ***Webex***, tiene como subred de origen *SubnetClientesGYE* y como destino *Cisco-Webex* y *Cisco-Webex.FedRAMP*; puertos de salida es el túnel *ToUIOMPLS* creado por la WAN MPLS y la interfaz WAN de Internet propia *wan*; se ingresa una velocidad de subida de 5Mbps y una velocidad de descarga de 10*Mbps*; limitamos por servicio *Internet Service* y por aplicación todo lo que es relacionado a Webex. Con esta política logramos limitar el ancho de banda con prioridad alta en

velocidad de subida, pero con prioridad media en descarga, para las reuniones de los usuarios por la App Webex, para este caso tiene redundancia de salida a la App sea por su propia WAN de Internet o por la WAN en la Sede Central Quito.

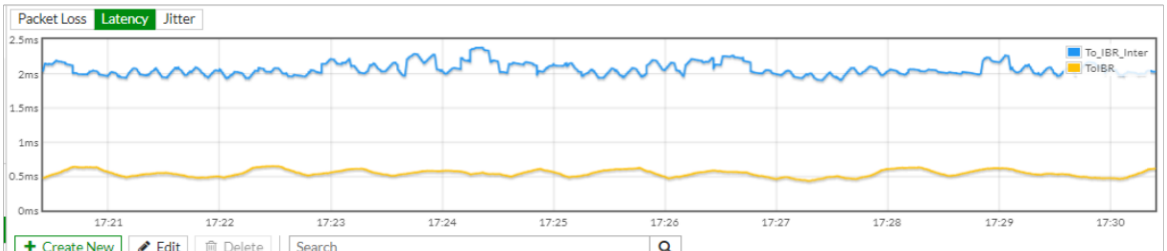
La quinta política ***ToInternet***, tiene como subred de origen *SubnetClientesGYE* y como destino Internet ***all***; puertos de salida es la interfaz WAN de Internet *wan* y el túnel de la MPLS hacia Quito *ToUIOMPLS*; se ingresa una velocidad de subida de 10Mbps y una velocidad de descarga de 10*Mbps*; no se agrega limitación de servicios ni de aplicaciones ya que tiene salida al Internet. Con esta política se limita el ancho de banda con prioridad media de subida y de bajada a 10Mbps, teniendo redundancia al momento de salir a Internet, siendo por su propia WAN de Internet o por la Sede Central Quito.

1.7 CALIDAD DE SERVICIO EN LA SD-WAN

A continuación, se muestra el detalle de la Calidad de Servicio de los enlaces y túneles que se monitorean de la Sede Central Quito y en la Sucursal Guayaquil, para determinar la mejor ruta en función de la latencia, jitter o perdida de paquetes.

1.7.1 CALIDAD DE SERVICIO SEDE CENTRAL QUITO

En la figura 1.15 se muestra la calidad de servicio en la Sede Central Quito que se lo realiza de la siguiente manera: la primer QoS de nombre ***ToIBR*** tiene como objetivo monitorear las rutas dirigidas para alcanzar las LAN que se encuentran en Ibarra, sea por el túnel MPLS *To_IBR* o por el túnel de Internet *To_IBR_Inter*. La segunda QoS de nombre ***ToGYE*** tiene como objetivo monitorear las rutas para alcanzar la LAN de Guayaquil, sea que alcancemos por el túnel de Internet *ToGYEInter* o de la MPLS *ToGYEMPLS*.



+ Create New | Edit | Delete | Search

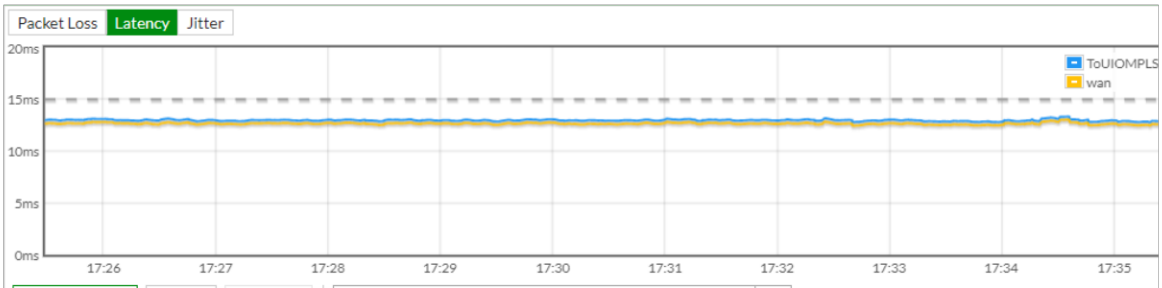
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Th
ToIBR	192.168.200.1 192.168.2.1	To_IBR_Inter: 0.00% ToIBR: 0.00%	To_IBR_Inter: 2.12ms ToIBR: 0.49ms	To_IBR_Inter: 0.39ms ToIBR: 0.05ms	5	5
ToGYE	192.168.3.1	ToGYEInter: 0.00% ToGYEMPLS: 0.00%	ToGYEInter: 2.21ms ToGYEMPLS: 0.59ms	ToGYEInter: 0.38ms ToGYEMPLS: 0.04ms	5	5
Multimedia	192.168.200.200	To_IBR_Inter: 0.00% ToIBR: 0.00%	To_IBR_Inter: 2.09ms ToIBR: 0.57ms	To_IBR_Inter: 0.55ms ToIBR: 0.05ms	5	5
Google	8.8.8.8	Wan_Internet (wan1): 0.00%	Wan_Internet (wan1): 12.58ms	Wan_Internet (wan1): 0.24ms	5	5

Figura 1.15 Calidad de Servicio Sede Central Quito.

La tercera Qos ***Multimedia***, tiene como objetivo sondear las rutas dirigidas para alcanzar el Servidor multimedia con IP 192.168.200.200 por el túnel MPLS *To_IBR* y por el túnel de Internet *To_IBR_Inter*. La cuarta QoS ***Google***, corresponde a las rutas dirigidas para alcanzar el servidor Google, para nuestro caso sólo disponemos de una sola WAN de internet física propia *wan1*.

1.7.2 CALIDAD DE SERVICIO SUCURSAL GUAYAQUIL

Como se muestra en la figura 1.16, la calidad de servicio en la Sucursal de Guayaquil se realiza de la siguiente manera: la primer QoS de nombre ***Zimbra*** tiene como objetivo monitorear las rutas para alcanzar el servidor Zimbra con IP 192.168.100.100 por el túnel de Internet *ToUIOInter* y por el túnel MPLS *ToUIOMPLS*. La segunda QoS de nombre ***Multimedia*** tiene como objetivo monitorear las rutas para alcanzar el servidor multimedia Plex con IP 192.168.200.200 por el túnel de Internet *ToIBRInter* y por el túnel MPLS *ToIBRMPLS*. La tercera QoS de nombre ***LanUIO*** corresponde a las rutas dirigidas para alcanzar las LAN de Quito, sondeando los túneles de la MPLS *ToUIOMPLS* y el túnel de Internet *ToUIOInter*. La cuarta QoS de nombre ***LanIBR*** corresponde a las rutas dirigidas para alcanzar las LAN de Ibarra, sondeando los túneles de la MPLS *ToIBRMPLS* y el túnel de Internet *ToIBRInter*. La quinta QoS de nombre ***Google***, corresponde a las rutas dirigidas para alcanzar el servidor Google o Internet, en este caso podemos salir por su propia WAN física o por el túnel MPLS *ToUIOMPLS* que va hacia Quito.



+ Create New | Edit | Delete | Search

Name	Detect Ser...	Packet Loss	Latency	Jitter	Failure Thresho...	Recov
Zimbra	192.168.100.100	ToUIOInter: 90.00% ToUIOMPLS: 90.00%	ToUIOInter: 15.05ms ToUIOMPLS: 13.42ms	ToUIOInter: 12.57ms ToUIOMPLS: 12.44ms	5	5
Multimedia	192.168.200.200	ToIBRInter: 0.00% ToIBRMPLS: 0.00%	ToIBRInter: 1.92ms ToIBRMPLS: 0.78ms	ToIBRInter: 0.20ms ToIBRMPLS: 0.04ms	5	5
LanUIO	192.168.100.1 192.168.1.1	ToUIOInter: 0.00% ToUIOMPLS: 0.00%	ToUIOInter: 2.16ms ToUIOMPLS: 0.65ms	ToUIOInter: 0.10ms ToUIOMPLS: 0.05ms	5	5
LanIBR	192.168.200.1 192.168.2.1	ToIBRInter: 0.00% ToIBRMPLS: 0.00%	ToIBRInter: 1.76ms ToIBRMPLS: 0.50ms	ToIBRInter: 0.15ms ToIBRMPLS: 0.04ms	5	5
Google	8.8.8.8	ToUIOMPLS: 0.00% WanInternet (wan): 0.00%	ToUIOMPLS: 12.90ms WanInternet (wan): 12.57ms	ToUIOMPLS: 0.13ms WanInternet (wan): 0.14ms	5	5

Figura 1.16 Calidad de Servicio Sucursal Guayaquil.

2 CONFIGURACIÓN DE LA SD-WAN

2.1 CONFIGURACIÓN INTERFACES

La configuración de los puertos WAN y LAN ya se especificó en el documento principal, aquí se muestran las interfaces configuradas para la Sede de Ibarra y de la Sucursal Guayaquil.

2.1.1 INTERFACES SEDE IBARRA

En la figura 2.1 se muestra las interfaces WAN configuradas en la Sede Ibarra y que pertenecen a la SD-WAN como las interfaces LAN y las VLAN para segmentar las redes.

Name	Type	Members	IP/Netmask	Administrat...	DHCP Ranges
Wan_MPLS (lan1)	Physical Interface		10.10.0.6/255.255.255.252	PING HTTPS SSH SNMP +2	
ToUIO	Tunnel Interface		10.20.0.2/255.255.255.255	PING FMG-Access	
ToGYEMPLS	Tunnel Interface		10.20.0.9/255.255.255.255	PING HTTPS HTTP FMG-Access	
Wan_Internet (wan)	Physical Interface		190.12.33.195/255.255.255.2...	PING HTTPS SSH SNMP +2	
ToGYEInter	Tunnel Interface		10.20.0.11/255.255.255.255	PING HTTPS HTTP FMG-Access	
To_UIO_Inter	Tunnel Interface		10.20.0.4/255.255.255.255	PING FMG-Access	
virtual-wan-link	SD-WAN Zone	Wan_Internet (wa... To_UIO_Inter ToUIO ToGYEInter +2	0.0.0.0/0.0.0.0		
LAN_IBR (lan2)	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS HTTP FMG-Access	
VlanMultimedia (Vlan200)	VLAN		192.168.200.1/255.255.255.0	PING HTTPS SSH SNMP +2	192.168.200.200-192.168.200.254
VlanClientes (Vlan2)	VLAN		192.168.2.1/255.255.255.0	PING SSH FMG-Access	192.168.2.200-192.168.2.254

Figura 2.1 Interfaces Sede Ibarra.

2.1.2 INTERFACES SUCURSAL GUAYAQUIL

En la figura 2.2 se muestra el detalle de las interfaces WAN y LAN que intervienen en la Sucursal de Guayaquil y que están asociadas a la SD-WAN como a las VLAN para segmentar la LAN de los clientes.

Name	Type	Members	IP/Netmask	Admini...	DHCP Ranges
WanMPLS (lan1)	Physical Interface		10.10.0.10/255.255.255.252	PING HTTPS SSH HTTP	
ToUIOMPLS	Tunnel Interface		10.20.0.6/255.255.255.255	PING FMG-Access	
ToIBRMPLS	Tunnel Interface		10.20.0.10/255.255.255.255	PING FMG-Access	
WanInternet (wan)	Physical Interface		190.12.33.196/255.255.255.248	PING HTTPS SSH HTTP FMG-Access	
ToUIOInter	Tunnel Interface		10.20.0.8/255.255.255.255	PING FMG-Access	
ToIBRInter	Tunnel Interface		10.20.0.12/255.255.255.255	PING FMG-Access	
virtual-wan-link	SD-WAN Zone	WanInternet (wan) ToUIOMPLS ToUIOInter ToIBRInter +2	0.0.0.0/0.0.0.0		
lan2	Physical Interface		0.0.0.0/0.0.0.0		
Vlan30	VLAN		192.168.3.1/255.255.255.0	PING HTTPS SSH HTTP FMG-Access	192.168.3.200-192.168.3.254

Figura 2.2 Interfaces Sucursal Guayaquil.

2.2 CONFIGURACIÓN OBJETOS

El detalle de las políticas se presentó en el apartado 1.3 de cada sede y la configuración de las políticas en el documento principal, por lo que en este apartado se muestra cada una de los objetos o subredes creadas y que intervienen en la Sede de Ibarra, figura 2.3 y la lista de objetos de la Sucursal de Guayaquil en la figura 2.4.

Name	Details	Interface	Type	Ref.	Routable
IP Range/Subnet 14					
all	0.0.0.0/0		Address	7	Disable
FABRIC_DEVICE	0.0.0.0/0		Address	0	Disable
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0	Disable
MPLS	10.10.0.0/24		Address	4	Enable
Multimedia	192.168.200.200/32		Address	2	Enable
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel inter...	Address	0	Disable
Subnet_GYE	192.168.3.0/24		Address	7	Enable
Subnet_IBR_Multimedia	192.168.200.0/24		Address	15	Enable
Subnet_Zimbra	192.168.100.0/24		Address	7	Enable
SubnetClienteIBR	192.168.2.0/24		Address	15	Enable
SubnetClientesUIO	192.168.1.0/24		Address	7	Enable
ToZimbra	192.168.100.100 - 192.168.100.100		Address	3	Disable
UsuarioRemoto	10.212.134.0/24		Address	2	Enable
VPN	10.20.0.0/24		Address	3	Enable

Figura 2.3 Lista de Objetos Sede Ibarra.

IP Range/Subnet 13					
FABRIC_DEVICE	0.0.0.0/0		Address	0	Disable
FIREWALL_AUTH_PORTAL_ADDRE...	0.0.0.0/0		Address	0	Disable
MPLS	10.10.0.0/24		Address	1	Enable
Multimeda	192.168.200.200/32		Address	2	Enable
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210	SSL-VPN tunne...	Address	0	Disable
SubnetClientesGYE	192.168.3.0/24		Address	16	Enable
SubnetClientesIBR	192.168.2.0/24		Address	3	Enable
SubnetClientesUIO	192.168.1.0/24		Address	3	Enable
SubnetMultimedia	192.168.200.0/24		Address	3	Enable
SubnetZimbra	192.168.100.0/24		Address	3	Enable
VPN	10.20.0.0/24		Address	1	Enable
Zimbra	192.168.100.100/32		Address	2	Enable
all	0.0.0.0/0		Address	6	Disable

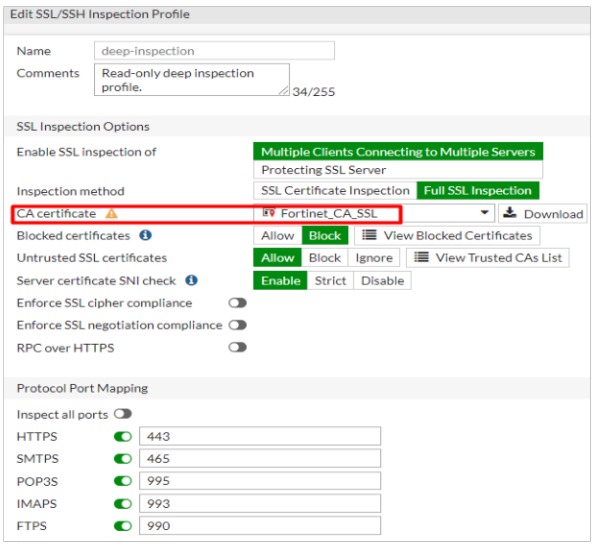
Figura 2.4 Lista de Objetos Sucursal Guayaquil.

2.3 CONFIGURACIÓN PERFILES DE SEGURIDAD

En la siguiente sección se detalla la continuación de las configuraciones de los perfiles de seguridad que se dispone en los FortiGate y de los cuales se utilizaran alguno de ellos.

2.3.1 INSPECCIÓN SSL/SSH

El escaneo de contenido de capa de socket seguro SSL, nos permite aplicar el escaneo a los perfiles de Antivirus, Control de Aplicación, prevención de Intrusos, etc., aplicando inspección SSL a las políticas del firewall. FortiOS dispone de tres perfiles de inspección SSL/SSH por defecto: *certificate-inspection*, *deep-inspection* y *no-inspection*.



c

Vamos a empezar por *no-inspection*, este modo no realiza ninguna acción de escaneo. El modo *certificate-inspection*, escanea solo la cabecera de los paquetes y no analiza los datos encriptados que pasan a través del firewall. Por otro lado, el modo *deep-inspection* descifra e inspecciona el contenido buscando amenazas y las bloquea, este modo no solo protege ataques que usan https, sino también bloquea otros protocolos cifrados con SSL como https, smtps, pop3s, imaps y ftps como se muestra en la figura 2.5.

Adicional, un dato importante, es necesario descargar el certificado desde el FortiGate *Fortinet_CA_SSL* e instalar en la PC, de esta forma el cliente puede acceder solo a sitios con certificados seguros SSL, los demás serán bloqueados y no se permitirá el acceso.

2.3.2 WEB FILTER

En el siguiente perfil de seguridad se especifica la configuración de los filtros para permitir, bloquear, monitoreo o poner en cuarentena las páginas Web que los usuarios puede o no acceder. Para esto se utiliza el perfil por defecto que nos proporciona los FortiGate, el perfil ya proporciona el bloqueo a páginas con contenido no apropiado; de igual forma permite el acceso a páginas que se utilizan normalmente y que no tienen contenido de peligro para el usuario. En base a esto, se puede bloquear/permitir páginas por categoría o sólo ciertas páginas, de esta manera se controla el acceso de los usuarios a la Web. Para las pruebas se bloquean las páginas para Redes Sociales como se muestra en la figura 2.6. La aplicación del perfil por defecto será el mismo en las tres sedes.

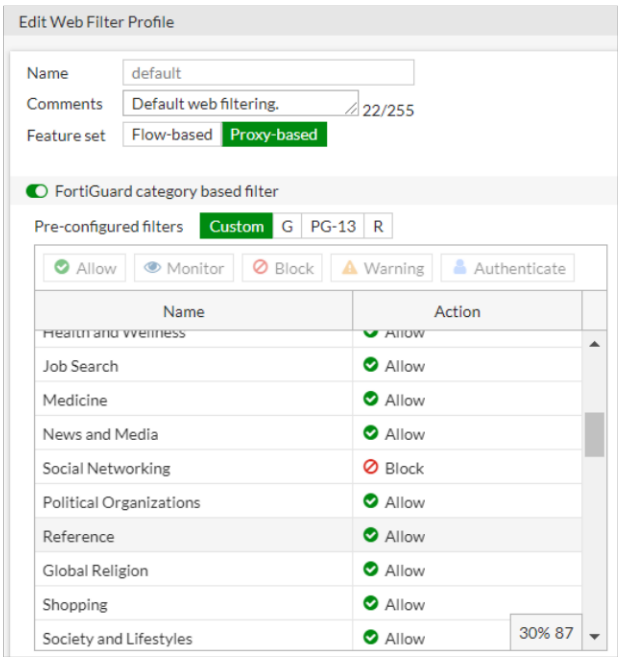


Figura 2.6 Perfil Control de Aplicaciones.

2.3.3 CONTROL DE APLICACIONES

Para el siguiente perfil, se basa en monitorear, permitir, bloquear o poner en cuarentena cualquier tipo de aplicación. En nuestro caso, como se muestra en la figura 2.7, se bloquean todas las categorías mostradas y solo se habilita las aplicaciones que necesitamos para tener acceso a nuestro proyecto como lo es la categoría ***Email*** para los correos electrónicos; y la categoría ***Video/Audio*** para acceder a Plex.TV. Adicional por cuestiones de manejo remoto, también se habilita la categoría ***Remote.Access*** para acceder a los servidores. También se puede bloquear aplicaciones por puertos que no estén por defecto o identificar el tráfico DNS.

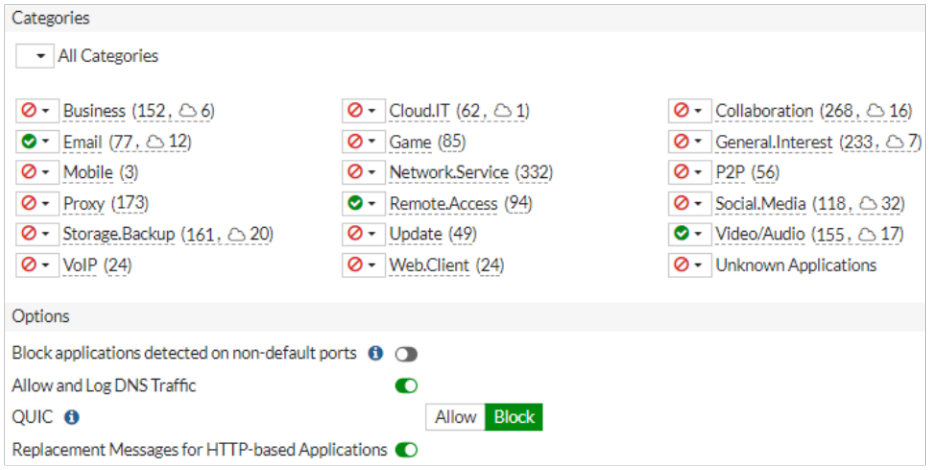


Figura 2.7 Perfil Control de Aplicaciones.

2.3.4 SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)

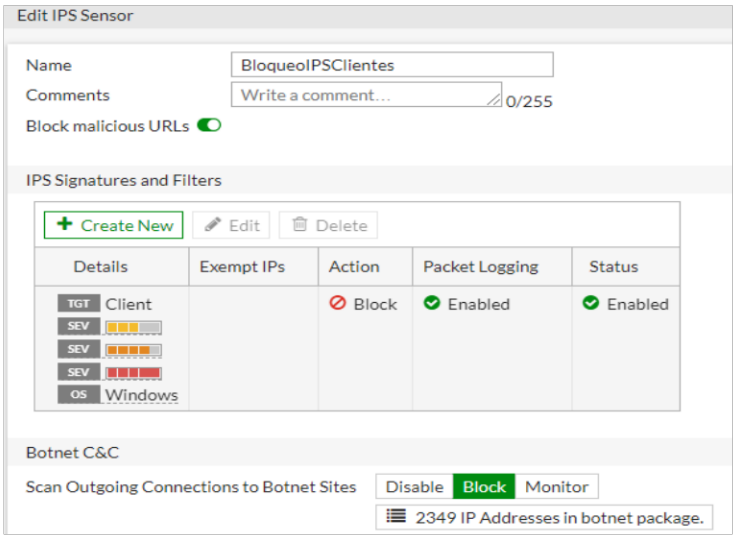


Figura 2.8 Perfil Prevención de Intrusos.

En la prevención de intrusos se crea un perfil como se muestra en la figura 2.8 de nombre ***BloqueoIPSClientes***, en principio se habilita el bloqueo general hacia URLs maliciosas, se crea un filtro de IPS bloqueando hacia sitios Botnet[1] con severidad media, alta y crítica para cliente o PC con sistema Operativo Windows. También se bloquea la salida a sitios botnet mediante una base de datos incorporada en FortiGate de aproximadamente 2349 direcciones IP.

2.3.5 DENEGACIÓN DE SERVICIO DoS

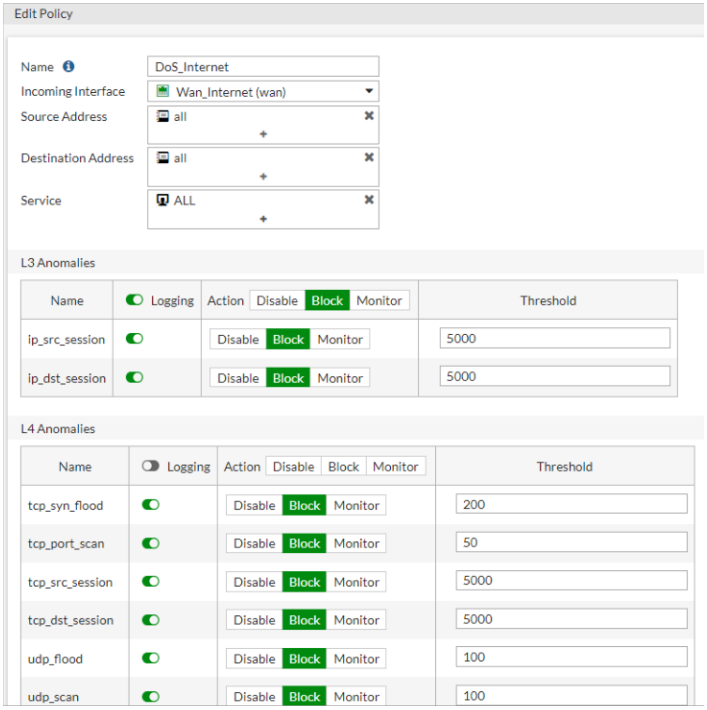


Figura 2.9 Perfil Denegación de Servicio.

Para poder bloquear ataques DoS, se debe crear políticas de protección, donde se ingresa la interfaz de entrada, las subredes de origen y la de destino, el tipo de servicio y habilitar las anomalías que se pueden presentar en capa 3 y capa 4 del modelo OSI. Las anomalías se pueden presentar como inundaciones de paquetes TCP, UDP, ICMP, para esto es necesario definir un número o un umbral que si sobrepasa se bloquee todos estos tipos de paquetes. En la figura 2.9 se muestra una política creada para el bloqueo que se puede generar desde cualquier origen que provenga de Internet, hacia cualquier destino de nuestra red interna, por

[1] Botnet: Método utilizado por cibercriminales para lanzar ataques de DDoS, enviar correos no deseados como SPAM, detectar contraseñas o distribuir rasonmware.

cualquier tipo de servicio; adicional se habilita las anomalías, se realiza ciertos cambios en los umbrales de capa 3 y capa 4, la mayoría de puede dejar por defecto.

ANEXO IV

CONFIGURACIÓN DE LOS ROUTERS CISCO DE LA RED MPLS, RED DE ACCESO A INTERNET, RED LAN Y FIREWALL FORTIGATE

ÍNDICE DE CONTENIDO

1 CONFIGURACIÓN DE LOS EQUIPOS DE LA RED MPLS

A continuación, se adjunta las configuraciones realizadas en los equipos de la red MPLS, tanto de los routers P y PE.

1.1 PE_UIO - ROUTER CISCO 2811 ISR

```
PE_UIO#sh run
Building configuration...

Current configuration : 2377 bytes
!
! Last configuration change at 01:41:14 UTC Sun Jan 2 2022 by tesis
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PE_UIO
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 C4OMOowMBpo5.b1ARuydzX4NGGjRT3V01VoyhoqGY/Q
!
no aaa new-model
!
dot11 syslog
ip source-route
!
!
ip cef
!
ip vrf datos
 rd 100:200
 route-target export 100:200
 route-target import 100:200
!
!
!
ip domain name tesis.ec
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
voice-card 0
!
```

```
crypto pki token default removal timeout 0
!
!
!
license udi pid CISCO2811 sn FTX1250A46K
username tesis privilege 15 secret 4
C4OMOowMBpo5.b1ARuydzX4NGGjRT3V01VoyhoqGY/Q

!
!
!
class-map match-all AB10M_UIOBR
 match access-group name ACL_AB10M_UIO
!
!
policy-map PM_SEGMENTACION_IP
 class AB10M_UIO
  police cir 10240000
   exceed-action drop
!
!
!
!

interface FastEthernet0/0
 description link-to-fortinet-UIO
 ip vrf forwarding datos
 ip address 10.10.0.1 255.255.255.252
 duplex auto
 speed auto
 service-policy input PM_SEGMENTACION_IP
 service-policy output PM_SEGMENTACION_IP
!
interface FastEthernet0/1
 description link-to-PE_CORE
 ip address 172.16.0.1 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
service-policy input PM_SEGMENTACION_IP
 service-policy output PM_SEGMENTACION_IP
!
router ospf 1
 mpls ldp autoconfig
!
router bgp 100
 bgp log-neighbor-changes
 redistribute ospf 1 match external 1 external 2
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family vpnv4
```

```
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 neighbor 3.3.3.3 activate
 neighbor 3.3.3.3 send-community extended
exit-address-family
!
address-family ipv4 vrf datos
 redistribute connected
 redistribute static
 default-information originate
exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route vrf datos 0.0.0.0 0.0.0.0 10.10.0.2 name RutaDefault
ip route vrf datos 10.20.0.1 255.255.255.255 10.10.0.2 name RutaTunnelIBR
ip route vrf datos 10.20.0.5 255.255.255.255 10.10.0.2 name RutaTunnelGYE
ip route vrf datos 192.168.1.0 255.255.255.0 10.10.0.2 name LANClienteUIO
ip route vrf datos 192.168.100.0 255.255.255.0 10.10.0.2 name LANZimbra
!
!

!
ip access-list extended ACL_AB10M_UIO
 permit ip 0.0.0.0 0.0.0.0 any
!

!
control-plane
!
!
!
mgcp profile default
!
!
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
end
```

1.2 PE_IBR - ROUTER CISCO 2811 ISR

```
PE_IBR#show running-config
Building configuration...

Current configuration : 2665 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PE_IBR
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 C4OMOowMBpo5.b1ARuydzX4NGGjRT3V01VoyhoqGY/Q
!
no aaa new-model
clock timezone UTC -5 0
!
dot11 syslog
ip source-route
!
!
ip cef
!
ip vrf datos
 rd 100:200
 route-target export 100:200
 route-target import 100:200
!
!
!
ip domain name tesis.ec
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
voice-card 0
!
crypto pki token default removal timeout 0
!
!
!
license udi pid CISCO2811 sn FTX1132F0M4
```

```
username tesis privilege 15 secret 4 C4OMOowMBpo5.b1ARuydzX4NGGjRT3V01VoyhoqGY/Q
!
!
!
class-map match-all AB5M_IBR
 match access-group name ACL_AB5M_IBR
!
!
policy-map PM_SEGMENTACION_IP
 class AB5M_IBR
  police cir 5120000
   exceed-action drop
!
!
!
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 description link-to-fortinet-IBR
 ip vrf forwarding datos
 ip address 10.10.0.5 255.255.255.252
 duplex auto
 speed auto
 service-policy input PM_SEGMENTACION_IP
 service-policy output PM_SEGMENTACION_IP
!
interface FastEthernet0/1
 description link-to-P_CORE
 ip address 172.16.0.6 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
 service-policy input PM_SEGMENTACION_IP
 service-policy output PM_SEGMENTACION_IP
!
router ospf 1
 mpls ldp autoconfig
!
router bgp 100
 bgp log-neighbor-changes
 redistribute ospf 1 match external 1 external 2
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 3.3.3.3 remote-as 100
 neighbor 3.3.3.3 update-source Loopback0
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
```

```
  neighbor 1.1.1.1 send-community extended
  neighbor 3.3.3.3 activate
  neighbor 3.3.3.3 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf datos
  redistribute connected
  redistribute static
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route vrf datos 10.20.0.2 255.255.255.255 10.10.0.6 name RutaTunnelUIO
ip route vrf datos 10.20.0.9 255.255.255.255 10.10.0.6 name RutaTunnelGYE
ip route vrf datos 192.168.2.0 255.255.255.0 10.10.0.6 name LANClienteIBR
ip route vrf datos 192.168.200.0 255.255.255.0 10.10.0.6 name LANMultimedia
!
ip access-list extended ACL_AB5M_IBR
 permit ip 192.168.200.0 0.0.0.255 any
 permit ip 192.168.2.0 0.0.0.255 any
 permit ip 10.20.0.0 0.0.0.255 any
 permit ip 10.10.0.0 0.0.0.255 any
!
logging trap errors
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
end
```

1.3 PE_GYE - ROUTER CISCO 2811 ISR

```
PE_GYE#show running-config
Building configuration...

Current configuration : 2580 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PE_GYE
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 C4OMOowMBpo5.b1ARuydzX4NGGjRT3V01VoyhoqGY/Q
!
no aaa new-model
clock timezone UTC -5 0
!
dot11 syslog
ip source-route
!
!
ip cef
!
ip vrf datos
 rd 100:200
 route-target export 100:200
 route-target import 100:200
!
!
!
ip domain name tesis.ec
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
voice-card 0
!
crypto pki token default removal timeout 0
!
!
!
```

```
!
license udi pid CISCO2811 sn FTX1010C1J9
username tesis privilege 15 secret 4 C4OMOowMBpo5.b1ARuydzX4NGGjRT3V01VoyhoqGY/Q
!
!
!
class-map match-all AB5M_GYE
 match access-group name ACL_AB5M_GYE
!
!
policy-map PM_SEGMENTACION_IP
 class AB5M_GYE
  police cir 51200000
   exceed-action drop
!
!
!
!
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 description link-to-fortinet-GYE
 ip vrf forwarding datos
 ip address 10.10.0.9 255.255.255.252
 duplex auto
 speed auto
 service-policy input PM_SEGMENTACION_IP
 service-policy output PM_SEGMENTACION_IP
!
interface FastEthernet0/1
 description link-to-PE_CORE
 ip address 172.16.0.10 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
 service-policy input PM_SEGMENTACION_IP
 service-policy output PM_SEGMENTACION_IP
!
router ospf 1
 mpls ldp autoconfig
!
router bgp 100
 bgp log-neighbor-changes
 redistribute ospf 1 match external 1 external 2
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 neighbor 2.2.2.2 remote-as 100
 neighbor 2.2.2.2 update-source Loopback0
 !
```

```
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
  neighbor 2.2.2.2 activate
  neighbor 2.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf datos
  redistribute connected
  redistribute static
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route vrf datos 10.20.0.6 255.255.255.255 10.10.0.10 name RutaTunnelMPLS
ip route vrf datos 10.20.0.10 255.255.255.255 10.10.0.10 name RutaTunnelInternet
ip route vrf datos 192.168.3.0 255.255.255.0 10.10.0.10 name LANClienteGYE
!
ip access-list extended ACL_AB5M_GYE
 permit ip 192.168.3.0 0.0.0.255 any
 permit ip 10.20.0.0 0.0.0.255 any
 permit ip 10.10.0.0 0.0.0.255 any
!
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
!
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
end
```

1.4 P_CORE - ROUTER CISCO 2811 ISR

```
P_CORE#sh run
Building configuration...

Current configuration : 1696 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname P_CORE
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$QdWI$sKY/nhbljhqXFS7Z2n5AG/
!
no aaa new-model
no network-clock-participate aim 0
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
ip domain name tesis.ec
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```

```
!
!
!
!
!
voice-card 0
!
!
!
!
!
username tesis privilege 15 secret 5 $1$m3eq$PLm5G85vjCgILOSxCwqV3/
archive
 log config
  hidekeys

!
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
 ip ospf 1 area 0
!
interface FastEthernet0/0
 description TO_PE_UIO
 ip address 172.16.0.2 255.255.255.252
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/3/0
```

```
 description TO_PE_GYE
 switchport access vlan 10
!
interface FastEthernet0/3/1
 description TO_PE_IBR
 switchport access vlan 5
!
interface FastEthernet0/3/2
!
interface FastEthernet0/3/3
!
interface Vlan1
 no ip address
!
interface Vlan5
 description TO_PE_IBR
 ip address 172.16.0.5 255.255.255.252
 ip ospf 1 area 0
!
interface Vlan10
 description TO_PE_GYE
 ip address 172.16.0.9 255.255.255.252
 ip ospf 1 area 0
!
router ospf 1
 mpls ldp autoconfig
 log-adjacency-changes
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
control-plane
```

```
!
!

!
!
!
!
line con 0
 login local
line aux 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
scheduler allocate 20000 1000
end
```

2 CONFIGURACIÓN DEL EQUIPO DE LA RED DE ACCESO A INTERNET

A continuación, se adjunta la configuración del router CE que actuará en modo Switch para la salida a Internet.

2.1 CE_INTERNET - ROUTER CISCO ISR C1111 MODO SWITCH

```
CE_INTERNET#sh run
Building configuration...

Current configuration : 6025 bytes
!
! Last configuration change at 17:44:48 UTC Sat Jan 8 2022
!
version 16.10
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname CE_INTERNET
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
```

```
 destination transport-method http
 no destination transport-method email
!
!
ip dhcp pool webuidhcp
!
!
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
multilink bundle-name authenticated
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-4028440538
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4028440538
 revocation-check none
 rsakeypair TP-self-signed-4028440538
!
!
license udi pid C1111-8P sn FCZ241680ZA
!
diagnostic bootup level minimal
!
```

```
spanning-tree extend system-id
!
!
!
redundancy
 mode none
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
 description LINK_TO_PE_PUNTONET
!
interface GigabitEthernet0/1/1
 description LINK_TO_FORTI_UIO
!
interface GigabitEthernet0/1/2
 description LINK_TO_FORTI_IBR
!
interface GigabitEthernet0/1/3
 description LINK_TO_FORTI_GYE
!
interface GigabitEthernet0/1/4
```

```
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
!
interface GigabitEthernet0/1/7
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login
!
!
!
!
!
!
end
```

3 CONFIGURACIÓN DE LOS EQUIPOS SWITCH PARA LA RED LAN

A continuación, se detalla los equipos router cisco que actuarán en modo Switch para la distribución de las VLAN en cada red LAN de cada sitio.

3.1 SW_UIO - ROUTER CISCO ISR C1111 MODO SWITCH

```
SW_UIO#sh run
Building configuration...

Current configuration : 1722 bytes
!
! Last configuration change at 12:46:01 UTC Thu Oct 5 2017
!
version 16.7
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname SW_UIO
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
```

```
!
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
!
crypto pki trustpoint TP-self-signed-3854141913
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3854141913
 revocation-check none
 rsakeypair TP-self-signed-3854141913
!
!
crypto pki certificate chain TP-self-signed-3854141913
!
!
license udi pid C1111-4P sn FGL223295U9
no license smart enable
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
!
redundancy
 mode none
!
!
vlan internal allocation policy ascending
!
!
```

```
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/0
 description LINK_TO_FORTI_UIO
 switchport trunk allowed vlan 1,10,100
 switchport mode trunk
!
interface GigabitEthernet0/1/1
 description LAN_SERVER_ZIMBRA
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/1/2
 description LAN_CLIENTES_UIO
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/1/3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip http server
```

```
ip http authentication local
ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
end
```

3.2 SW_IBR - ROUTER CISCO ISR C1111 MODO SWITCH

```
SW_IBR#sh run
Building configuration...

Current configuration : 6089 bytes
!
! Last configuration change at 16:52:14 UTC Sat Jan 8 2022
!
version 16.10
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname SW_IBR
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@ci
sco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
!
!
```

```
!
login on-success log
!
!
!
!
!
!
!
subscriber templating
multilink bundle-name authenticated
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-2869421436
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2869421436
 revocation-check none
 rsakeypair TP-self-signed-2869421436
!
!
license udi pid C1111-8P sn FGL2331137K
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
!
redundancy
 mode none
!
```

```
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
 description Link_To_FortiGate_IBR
 switchport mode trunk
!
interface GigabitEthernet0/1/1
 description LAN_Server_Multimedia
 switchport access vlan 200
 switchport mode access
!
interface GigabitEthernet0/1/2
 description LAN_CLIENTES_IBR
 switchport access vlan 2
 switchport mode access
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
```

```
interface GigabitEthernet0/1/6
!
interface GigabitEthernet0/1/7
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login
!
!
!
!
!
!
end
```

3.3 SW_GYE - ROUTER CISCO ISR C1111 MODO SWITCH

```
SW_GYE#sh run
Building configuration...

Current configuration : 6016 bytes
!
! Last configuration change at 17:56:52 UTC Sat Jan 8 2022
!
version 17.3
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform hardware throughput crypto 50000
!
hostname SW_GYE
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
login on-success log
!
```

```
!
!
!
!
!
!
subscriber templating
multilink bundle-name authenticated
no device-tracking logging theft
!
!
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-3155264845
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3155264845
 revocation-check none
 rsakeypair TP-self-signed-3155264845
!
!
!
license udi pid C1111-4P sn FGL2506LECW
memory free low-watermark processor 71830
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
```

```
vlan internal allocation policy ascending
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
 description LINK_TO_FORTI_GYE
 switchport trunk allowed vlan 1,30
 switchport mode trunk
!
interface GigabitEthernet0/1/1
 description LAN_CLIENTES_GYE
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface Vlan1
 no ip address
!
no ip http server
ip http secure-server
ip forward-protocol nd
!
```

```
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
!
!
!
!
!
!
end
```

4 CONFIGURACIÓN EQUIPOS FIREWALL FORTIGATE

A continuación, se adjunta un enlace, en donde se encuentra la configuración en código generado por línea de comandos CLI de cada uno de los FortiGate 60F y 40F de cada sede. No se agrega en este documento, por ser un código de gran extensión, por lo que se adjunta en archivos txt.

Enlace:

https://drive.google.com/drive/folders/1SUppPfFpkWNKpcfd8nCU32qN48TrJQ1-?usp=sharing

ANEXO V

VIDEO DEL PRODUCTO FINAL DEMOSTRABLE

A continuación, se adjunta un enlace del video del Trabajo de Integración Curricular como tema: DESARROLLO DE UN PROTOTIPO DE UNA RED SD-WAN (SOFTWARE-DEFINED WIDE AREA NETWORK) UTILIZANDO TECNOLOGÍA FORTINET; y los resultados obtenidos.

Enlace:

https://drive.google.com/drive/folders/10n3rFh0LcVn4_npoKS_WtyOwYg-Psz1P?usp=sharing