Pontificia Universidad Católica del Ecuador

FACULTAD DE INGENIERÍA
COORDINACIÓN DE POSGRADO

PUCE


**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**

**FACULTAD DE INGENIERÍA**

Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Gestión y Administración de TI

# SD-WAN: FACTIBILIDAD DE CONFIGURACIÓN COMO INFRAESTRUCTURA OVERLAY EMPRESARIAL

**Autor**: Jonathan Javier López Arévalo

**Director**: Dr. Gustavo David Salazar Chacón

Quito, enero 2023

**PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR**

## DECLARACIÓN Y AUTORIZACIÓN

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

A través de la presente declaración dejo constancia de que la Pontificia Universidad Católica del Ecuador podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

Jonathan Javier López Arévalo



Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647

## APROBACIÓN DEL TUTOR

En mi carácter de Director del Trabajo de Posgrado Titulado: "**SD-WAN: FACTIBILIDAD DE CONFIGURACIÓN COMO INFRAESTRUCTURA OVERLAY EMPRESARIAL**", presentado por el maestrante JONATHAN JAVIER LÓPEZ ARÉVALO, titular de la Cédula de Identidad Nº 1804307286 para optar al Grado de Magíster en Tecnologías de Información mención Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito, a los 3 días de enero de 2023

Firmado electrónicamente por:
GUSTAVO DAVID
SALAZAR CHACON

GUSTAVO DAVID SALAZAR CHACÓN C.I. 1716104797

GSALAZAR787@puce.edu.ec

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 2 % índice de similitud con otras fuentes.



Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647

# TURNITIN: HOJA DEL INFORME CON EL PORCENTAJE

Turnitin Informe de Originalidad

Procesado el: 03-ene.-2023 02:15 -05
Identificador: 1988144891
Número de palabras: 15291
Entregado: 1

Tesis Maestría - Jonathan López Por Jonathan Javier López Arévalo

| Índice de similitud | Similitud según fuente | |
|---|---|---|
| 2% | Internet Sources: | 2% |
| | Publicaciones: | 1% |
| | Trabajos del estudiante: | 2% |

1% match (trabajos de los estudiantes desde 09-sept.-2022)
Clase: Tesis Juan Carlos González Ortíz
Ejercicio: Tesis Juan Carlos González
Nº del trabajo: 1895713537

1% match (trabajos de los estudiantes desde 19-dic.-2022)
Submitted to Pontificia Universidad Catolica del Ecuador - PUCE on 2022-12-19

1% match (Internet desde 08-oct.-2022)
http://sedici.unlp.edu.ar/bitstream/handle/10915/129910/Documento_completo.pdf?isAllowed=y&sequence=1

FACULTAD DE INGENIERÍA COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR FACULTAD DE INGENIERÍA Trabajo de Titulación como requisito previo para la obtención del título de Magíster en Tecnologías de Información mención Gestión y Administración de TI SD-WAN: FACTIBILIDAD DE CONFIGURACIÓN COMO INFRAESTRUCTURA OVERLAY EMPRESARIAL Autor: Jonathan Javier López Arévalo Director: Dr. Gustavo David Salazar Chacón Quito, enero 2023 COORDINACIÓN DE POSGRADO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR DECLARACIÓN Y AUTORIZACIÓN Yo, Jonathan Javier López Arévalo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún posgrado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento. A través de la presente declaración dejo constancia de que la Pontificia Universidad Católica del Ecuador podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes. Jonathan Javier López Arévalo ii COORDINACIÓN DE POSGRADO APROBACIÓN DEL TUTOR En mi carácter de Director del Trabajo de Posgrado Titulado: "SD-WAN: FACTIBILIDAD DE CONFIGURACIÓN COMO INFRAESTRUCTURA OVERLAY EMPRESARIAL", presentado por el maestrante JONATHAN JAVIER LÓPEZ ARÉVALO, titular de la Cédula de Identidad Nº 1804307286 para optar al Grado de Magíster en Tecnologías de Información mención Gestión y Administración de TI, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería. En la ciudad de Quito, a los 3 días de enero de 2023 GUSTAVO DAVID SALAZAR CHACÓN C.I. 1716104797 GSALAZAR787@puce.edu.ec NOTA: Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: … % índice de similitud con otras fuentes. iii COORDINACIÓN DE POSGRADO TURNITIN: HOJA DEL INFORME CON EL PORCENTAJE iv COORDINACIÓN DE POSGRADO DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD v COORDINACIÓN DE POSGRADO ÍNDICE DE CONTENIDOS DECLARACIÓN Y AUTORIZACIÓN ..... 2 APROBACIÓN DEL TUTOR..... 3 ÍNDICE DE CONTENIDOS ..... 6 ÍNDICE DE TABLAS



Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647

# DEDICATORIA

A Dios porque su sabiduría me permitió alcanzar un nuevo objetivo académico,

Definitivamente a mis padres,
por su incansable labor y apoyo.

Sin lugar a duda, al principal motor
para conseguir todas mis aspiraciones y cumplir mis metas,
quienes me motivan a seguir adelante,
a ustedes Doménica y Julián.

A las dos personas que han cuidado de mí,
por ser su hermano menor,
aquellas que siempre están ahí
para enseñarme que la vida no es solo responsabilidades,
sino que también está inmersa de alegrías y diversiones,
a ustedes Paola y Juan Fernando.

A todos mis amigos y compañeros de trabajo que han formado parte de esta etapa importante de enriquecimiento profesional.

# ÍNDICE DE CONTENIDOS





Av. 12 de octubre 1076 y Ramón Roca
Apartado postal 17-01-2184
Telf.: (593) 2 2991647

# ÍNDICE DE TABLAS

CAPÍTULO II y IV



CAPÍTULO IV

# ÍNDICE DE GRÁFICOS

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN
Y ADMINISTRACIÓN DE TI

# SD-WAN: FACTIBILIDAD DE CONFIGURACIÓN COMO INFRAESTRUCTURA OVERLAY EMPRESARIAL

Autor: Jonathan López

Director -Tutor: Dr. Gustavo Salazar

Fecha: 3 de enero del 2023

## RESUMEN

El presente trabajo de titulación se enfoca en el análisis teórico y práctico de SD-WAN (Red de Área Extendida definida por Software) a través de las soluciones de dos fabricantes que abarcan un fuerte mercado en el Ecuador y que están ubicadas como líderes según el Cuadrante de Gartner respecto a Infraestructura WAN; estos son CISCO y FORTINET.

En el primer capítulo, se definen los objetivos generales y específicos, así como la justificación y alcance del proyecto de titulación con el fin de establecer un margen de conocimiento adecuado para impartir a la comunidad estudiantil y docente de la Pontificia Universidad Católica del Ecuador.

El segundo capítulo describe el surgimiento de la SD-WAN a partir de las SDN, así como un breve análisis de MPLS, para poder dar paso al análisis teórico fundamental de la SD-WAN y

de los componentes de cada una de las soluciones *Secure SD-WAN* de FORTINET y *SD-WAN Viptela* de CISCO.

En el tercer capítulo se describe el funcionamiento de la SD-WAN de cada uno de los fabricantes para así poder aclarar y entender mejor los conceptos teóricos a través de la práctica, es decir emulaciones, se abarcan temas funcionales como políticas, enrutamiento dinámico, seguridad, control y gestión, etc.

En el cuarto capitulo se discuten los resultados del presente proyecto que corroboran las ventajas que presenta la solución SD-WAN desde el punto de vista de dos importantes fabricantes, así como una comparativa entre estos y los escenarios adecuados de implementación.

En el quinto capítulo por su parte se determina la factibilidad de utilizar esta solución como infraestructura *overlay* dentro de las organizaciones y se presenta la propuesta de implementación de la SD-WAN dentro de la PUCE matriz con sus sedes acorde al escenario que se tiene en la actualidad.

Finalmente, se presentan las conclusiones que ha dejado el presente proyecto de titulación, así como las recomendaciones que sean de utilidad para futuros trabajos de investigación.

**Palabras clave:**
SD-WAN, WAN, SDN, MPLS, NGFW, ASIC, ZTP, IPSEC, EVE-NG, GNS3

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN TECNOLIGÍAS DE LA INFORMACIÓN MENCIÓN GESTIÓN
Y ADMINISTRACIÓN DE TI

# SD-WAN: FEASIBILITY OF CONFIGURATION AS AN ENTERPRISE OVERLAY INFRASTRUCTURE

Author: Jonathan López

Director: Dr. Gustavo Salazar

Date: January 3rd, 2023

## ABSTRACT

This degree project focuses on the theoretical and practical analysis of the SD-WAN (Software Defined Wide Area Network) through the solutions of two manufacturers that cover a strong market in Ecuador and that are located as leaders according to the Gartner Quadrant regarding WAN Infrastructure; these are CISCO and FORTINET.

In the first chapter, the general and specific objectives are defined, as well as the justification and scope of the degree project in order to establish an adequate margin of knowledge to impart to the student and teaching community of the Pontificia Universidad Católica del Ecuador.

The second chapter describes the emergence of SD-WAN from SDN, as well as a brief analysis of MPLS, in order to give way to the fundamental theoretical analysis of SD-WAN and the components of each of the solutions Secure SD-WAN of FORTINET and SD-WAN Viptela of CISCO.

The third chapter describes how each vendor's SD-WAN works in order to clarify and better understand the theoretical concepts through practice, i.e. emulations, functional topics such as policies, dynamic routing, security, control and management, etc. are covered.

The fourth chapter discusses the results of this project that corroborate the advantages of the SD-WAN solution from the point of view of two major vendors, as well as a comparison between these and the appropriate implementation scenarios.

The fifth chapter determines the feasibility of using this solution as an overlay infrastructure within the organizations and presents the proposal for the implementation of the SD-WAN within the PUCE matrix with its headquarters according to the current scenario.

Finally, the conclusions of this degree project are presented, as well as the recommendations that may be useful for future research works.

**Keywords:** SD-WAN, WAN, SDN, MPLS, NGFW, ASIC, ZTP, IPSEC, EVE-NG, GNS3

# INTRODUCCIÓN

Actualmente, la evolución de las redes en conjunto con los avances tecnológicos ha crecido de manera acelerada, más aún con la pandemia, forzando a un buen número de empresas que actualicen sus sistemas y migren hacia nuevos retos tecnológicos. Algunos de estos retos comprenden la virtualización, *machine learning*, inteligencia artificial, entre otros que van de la mano del uso cada vez mayor del Internet. Es así como varios países están siendo parte de esta transformación digital con objetivos de mejorar la tecnología y tener ciudades inteligentes con empresas que ofrezcan servicios más eficientes y así poder satisfacer las necesidades de crecimiento de la comunidad de un país.

Por este motivo, el mundo de las redes está migrando al escenario o soluciones de redes definidas por Software tanto a nivel LAN como WAN, con el objetivo de automatizar y tener redes inteligentes dentro de las empresas privadas y entidades gubernamentales que ofrecen servicios que demandan un mayor ancho de banda y una latencia mínima. Es aquí donde surge la factibilidad de reemplazar la infraestructura (WAN) actual de las empresas y entidades por una *Software-Defined Wide Area Network* (SD-WAN) que teóricamente es una red inteligente que combina las funciones de virtualización de red y las de SDN, a más de optimizar los servicios de MPLS en cuanto a latencia e Ingeniería de Trafico se refiere. Adicional mencionar la facilidad de gestión centralizada que ofrece y su significativo ahorro en costos de CAPEX y OPEX sin disminuir su rendimiento, lo cual es un gran punto a favor para el área financiera de cualquier organización.

Tomando en cuenta que en este último año la SD-WAN ha tenido una acogida bastante notoria a nivel mundial en diferentes países se vuelve inminente estudiarla, entenderla y más aún ver la factibilidad de implementarla en diferentes empresas del Ecuador. Es importante mencionar que algunas empresas ya hacen uso de la SD-WAN como Banco Guayaquil que ha obtenido resultados bastante positivos.

Por esta razón, se propone como tesis el estudio de esta solución desde el punto de vista de dos fabricantes que tienen un buen posicionamiento en el mercado respecto a esta tecnología SD-WAN; estos son CISCO y FORTINET con el fin de considerar la factibilidad de configuración dentro de las empresas como infraestructura *overlay*, a través del análisis de su funcionamiento, ventajas, desventajas y comparativas entre ellos. Cabe recalcar que no se pretende establecer que la una sea mejor que la otra ya que es un análisis bastante subjetivo, sin embargo, si se espera proponer los escenarios más adecuados para cada proveedor, acorde al modelo de negocio que maneja cada organización.

# 1 PLANTEAMIENTO DEL PROBLEMA

## 1.1 Formulación del Problema

Actualmente, el incremento del trabajo remoto y adopción de múltiples tecnologías *cloud* representan un impacto significativo en las topologías de red, esto conlleva a un aumento exponencial aplicaciones en la nube y del tráfico cifrado en las redes WAN corporativas (ITSitio, 2020).

Si bien es cierto, un gran porcentaje de empresas mantienen una infraestructura de red *Multiprotocol Label Switching* (MPLS) que garantiza seguridad, fiabilidad y calidad de servicio (QoS), sin embargo, su costo, mayor tiempo de implementación o actualización, malgasto de recursos de ancho de banda y mayor latencia respecto al tráfico remoto son desventajas que han dado lugar a tener un tipo de WAN de siguiente generación que compense estas falencias (Wang, 2019). Para ello, la SD-WAN (*Software-Defined Wide Area Network*) es una de estas alternativas.

Teóricamente, se puede considerar a la SD-WAN como una combinación optimizada de las características de MPLS e IP, adicionando tecnologías de *Network Function Virtualization* (NFV) y *Software Defined Network* (SDN), teniendo como característica fundamental la separación del plano de control y de datos. Esto permite a la SD-WAN ser una red más inteligente, dinámica, flexible con una administración centralizada que ahorre costos de rendimiento y operación (Steve, 2020).

En vista del ambiente evolutivo y considerando que la mayoría de las empresas mantienen una infraestructura MPLS se propone el estudio de la SD-WAN y su factibilidad de configuración como infraestructura overlay empresarial, tomando en cuenta la comparativa de dos soluciones SD-WAN de distintos proveedores que se mantienen como líderes según el cuadrante de Gartner.

La finalidad de este proyecto de titulación es proporcionar la información suficiente a los maestrantes respecto a la SD-WAN para que sea analizada la posibilidad de migración dentro de sus empresas, adicional permitir escoger el proveedor más adecuado de acuerdo con sus necesidades y requerimientos basado en la comparativa presentada.

## 1.2 Objetivos de la Investigación

### 1.2.1 Objetivo General

Establecer una comparativa entre SD-WAN (Software-Defined Wide Area Network) de CISCO y la SD-WAN de FORTINET para determinar la factibilidad y opción más adecuada como infraestructura overlay empresarial.

### 1.2.2 Objetivos Específicos

- Analizar las características de SD-WAN de CISCO y FORTINET.
- Analizar el funcionamiento de Viptela SD-WAN (CISCO) y Secure SD-WAN (FORTINET)
- Establecer y definir las ventajas/desventajas y desafíos entre las dos tecnologías de SD-WAN.
- Analizar la SD-WAN más factible acorde a los distintos modelos de negocio y sus requerimientos.

## 1.3 Justificación de la Investigación

El análisis de una red SD-WAN y su comparación entre dos tecnologías bien posicionadas en el mercado es necesaria debido a que en la actualidad las empresas demandan implementar o migrar a una red WAN más inteligente y centralizada que permita manejar de manera más efectiva y eficiente el tráfico remoto, el mismo que ha crecido exponencialmente como consecuencia del aumento de uso de la nube y transformación digital. Por ello, se vuelve indispensable el análisis de al menos dos tecnologías, en este caso CISCO y FORTINET que permitan definir la factibilidad de configurar una SD-WAN como una red *overlay* empresarial, eligiendo una de ellas de acuerdo con el escenario y requerimientos de implementación.

## 1.4 Alcance

El presente Proyecto de Titulación se enfoca en el estudio y análisis de una red SD-WAN basado en la tecnología de CISCO y FORTINET. Con la finalidad de adquirir los conocimientos planteados se propone, en primer lugar, la introducción general de las redes de área extendida tradicionales, así como Multiprotocol Label Switching (MPLS) ya que es actualmente una de las WAN más utilizadas.

Posteriormente, se propone definir todos los conceptos necesarios para entender el funcionamiento de una SD-WAN y sus temas derivados. Después de comprender la parte teórica, se plantea describir el funcionamiento de la SD-WAN de cada fabricante. Es importante recalcar que la seguridad es un inconveniente en las SD-WAN. El cual será analizados desde las dos tecnologías tanto CISCO como FORTINET.

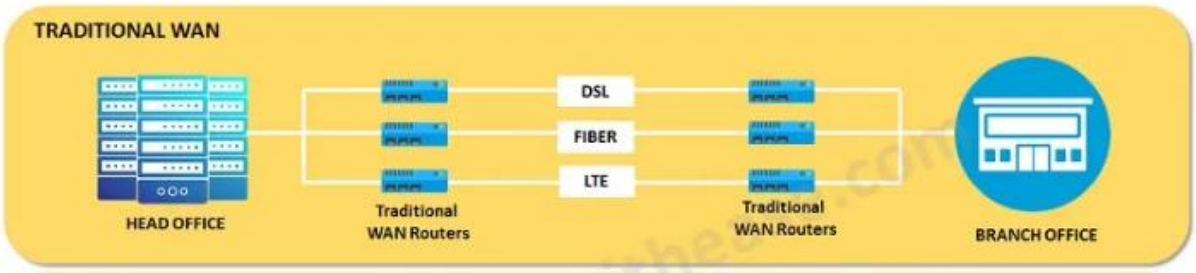
Se realizarán comparaciones de las dos tecnologías para esclarecer las ventajas de la una respecto a la otra y así poder emitir un criterio de la mejor opción acorde al escenario de implementación. Finalmente, basado en los resultados del análisis se corroborará la factibilidad de configurar una SD-WAN como infraestructura *overlay* empresarial, tomando en cuenta sus principales ventajas de ahorro de costos y efectividad.

# 2 FUNDAMENTACIÓN TEÓRICA

## 2.1 Redes de Área Extendida (WAN)

Basado en el enfoque de WAN tradicionales, estas funcionan a través de la compra e instalación de circuitos patentados a través de los cuales se enrutan los paquetes IP (servicios IP) a todos los clientes previstos. Este tipo de redes tradicionales hacía que la administración de los equipos de TI fuera bastante complejo y laborioso. Esto afectaba directamente a aspectos como la escalabilidad y control de las redes de área extendida para el proveedor de servicios (ExterNetworks, 2020).

**Figura 2.1.** WAN Tradicionales



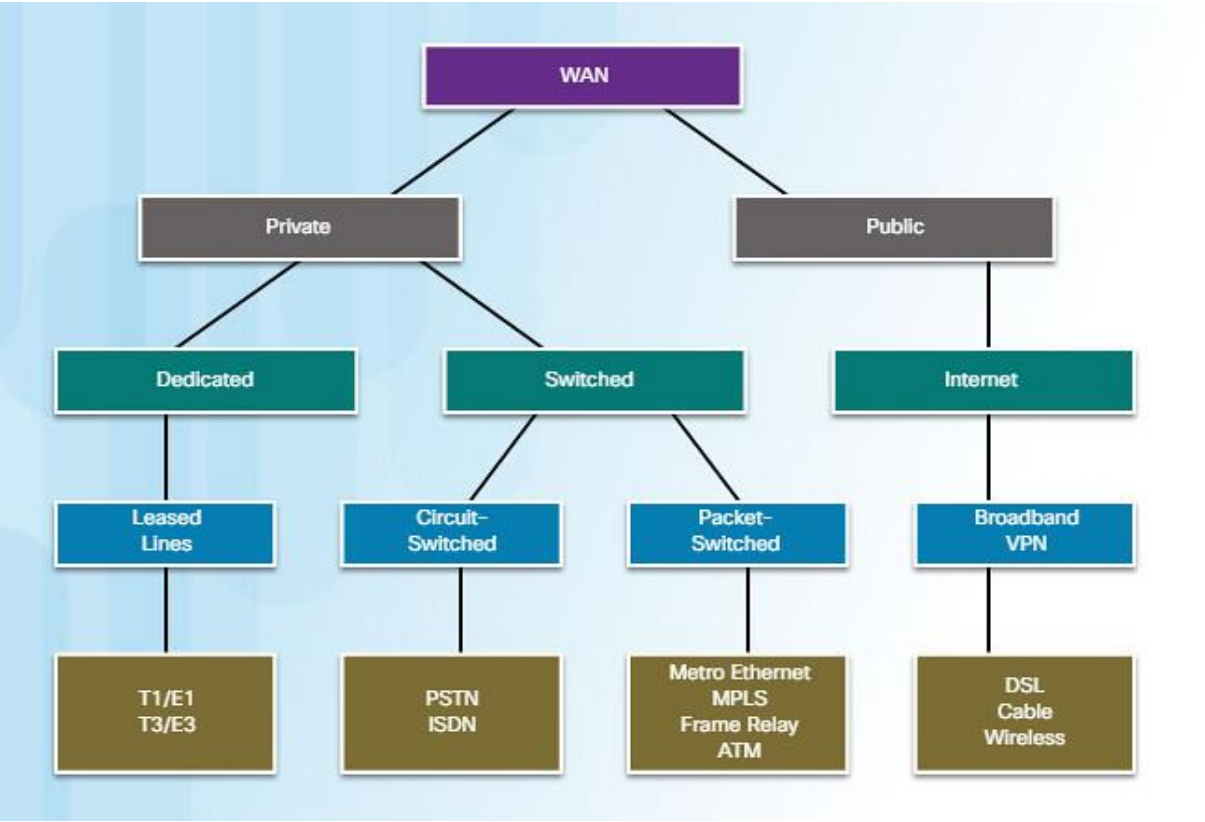

Fuente: (Bhardwaj, 2020)

### 2.1.1 Características – Desafíos WAN Tradicionales

- La configuración es local, es decir está distribuida en cada router.
- Su arquitectura tradicionalmente era privada y estática, impidiendo migraciones a la nube.
- Los altos costos de los circuitos o enlaces privados repercuten en un ancho de banda limitado.
- Altos tiempos de implementación (meses) para el despliegue de nuevos enlaces o sucursales.
- Las políticas son administradas independientemente en cada router, esto ocasiona un trabajo mayor para los administradores de red.
- En caso de falla del enlace se requieren de varios segundos para su restauración ya que el *failover*[1] depende completamente del estado del enlace, provocando retardos importantes que afectan la experiencia del usuario en cuestiones de funcionamiento de la red.
- Carecen de Acuerdos de Nivel de Servicio (SLA) a nivel de aplicaciones porque su rendimiento es imprevisible.
- Mantienen una topología *Hub & Spoke* que ocasiona la dependencia del centro de datos afectando así el rendimiento de la red, en términos de retardo.
- Infraestructura más compleja ya que los equipos tienen funciones únicas y específicas a diferencia de *Network Function Virtualization* (NFV).

[1] ***Failover:*** *modo de funcionamiento secundario de backup o respaldo en caso de falla.*

**Figura 2.2** Opciones de Conexión de Enlace WAN




Fuente: (Gómez, 2017)

En la Figura 2.2 se visualizan las diferentes tecnologías diseñadas para enlaces WAN como Frame Relay, ATM, Metro Ethernet, etc. Sin embargo, en la actualidad varias de estas tecnologías son consideradas obsoletas o muy antiguas a excepción de MPLS que es una de las más utilizadas, por esta razón, se describe con mayor detalle esta tecnología en el siguiente apartado.

## 2.2 Multiprotocol Label Switching (MPLS)

MPLS se diferencia de tecnologías tradicionales debido a que el enrutamiento está basado en etiquetas y no en la cabecera IP, es decir traduce las direcciones IP en etiquetas simples de longitud fija, con el objetivo de incrementar la velocidad de datos y mejorar el rendimiento de la red.

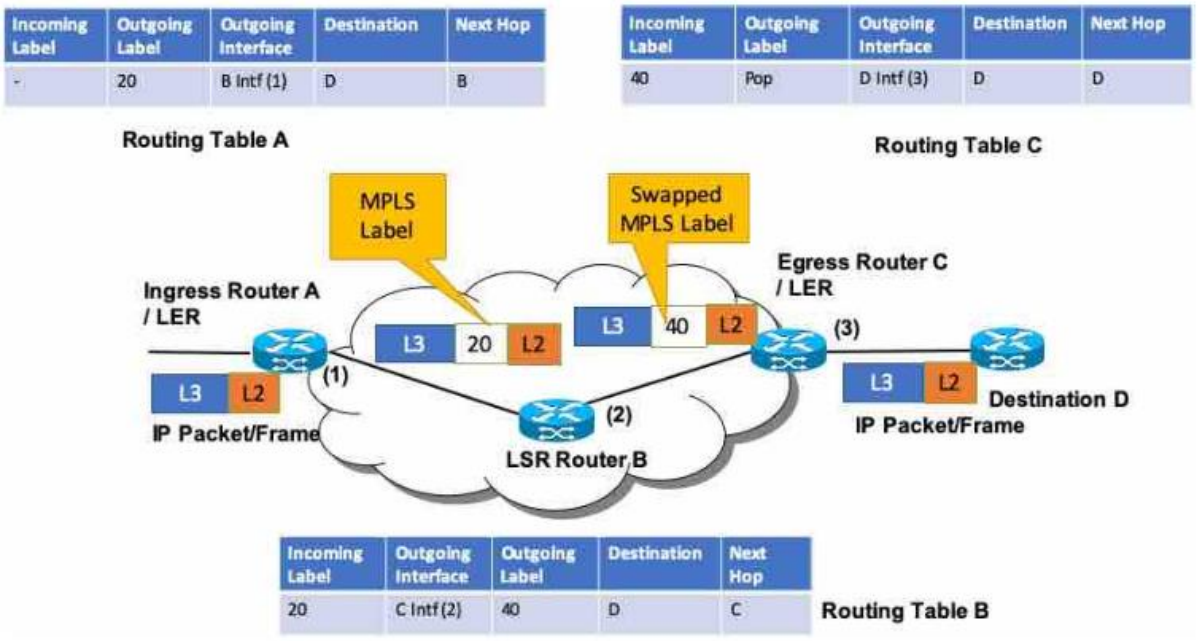
Es importante mencionar, que al utilizar etiquetas MPLS es independiente de los protocolos de capas 2 y capa 3 del modelo OSI. Algunas de las características por las cuales su uso es bastante común a nivel mundial es porque soporta distintos protocolos como IP, ATM, Frame Relay, etc. y provee funcionalidades como *Quality of Service* (QoS), *Traffic Enginnering*, y *Virtual Private Network.*

### 2.2.1 Funcionamiento de MPLS

En la Figura 2.3. se visualiza el funcionamiento de MPLS. En general, el proceso empieza por el establecimiento de rutas y asignación de etiquetas (antes de transferir los paquetes), distribución de etiquetas y creación de tablas, recepción del paquete e inserción de etiqueta, conmutación de etiquetas

y reenvío del paquete y finalmente la extracción de etiqueta y entrega del paquete (Hidalgo, 2020). Los componentes principales de MPLS son dos tipos de enrutadores: *Label Switched Router* (LSR) y *Label Edge Router (LER).*

**Figura 2.3.** Funcionamiento de MPLS




Fuente: (Pandya, 2020)

### 2.2.2 Inconvenientes de MPLS

- Tiempo significativo para la implementación de nuevas sucursales.
- Altos costos de nuevos enlaces MPLS en comparación de enlaces SD-WAN, por ejemplo.
- Adaptación más compleja a tecnologías de aplicación en nube como SaaS[2] e IaaS[3], tomando en cuenta que en MPLS los paquetes pasan por un nodo central que genera retardos.
- Requerimiento de Administradores de red en sitio para nuevos despliegues ya que no tienen funcionalidades de *Zero Touch Proviosioning* (ZTP) como SD-WAN.

## 2.3 Software Defined Network – Redes Definidas por Software (SDN)

La característica principal que diferencia una Red Definida por Software (SDN) de las redes de datos tradicionales es la separación del Plano de Control del Plano de Datos, de tal manera que la parte de

[2] **SaaS:** *Software as a Service, se trata de cualquier servicio basado en la web como Salesforce, Dropbox, Gmail, etc.*

[3] **IaaS:** *Infraestructure as a Service, hace referencia a servidores, almacenamiento, equipos de red y virtualización, por ejemplo: Amazon Web Service, Google Cloud, Azure, etc.*

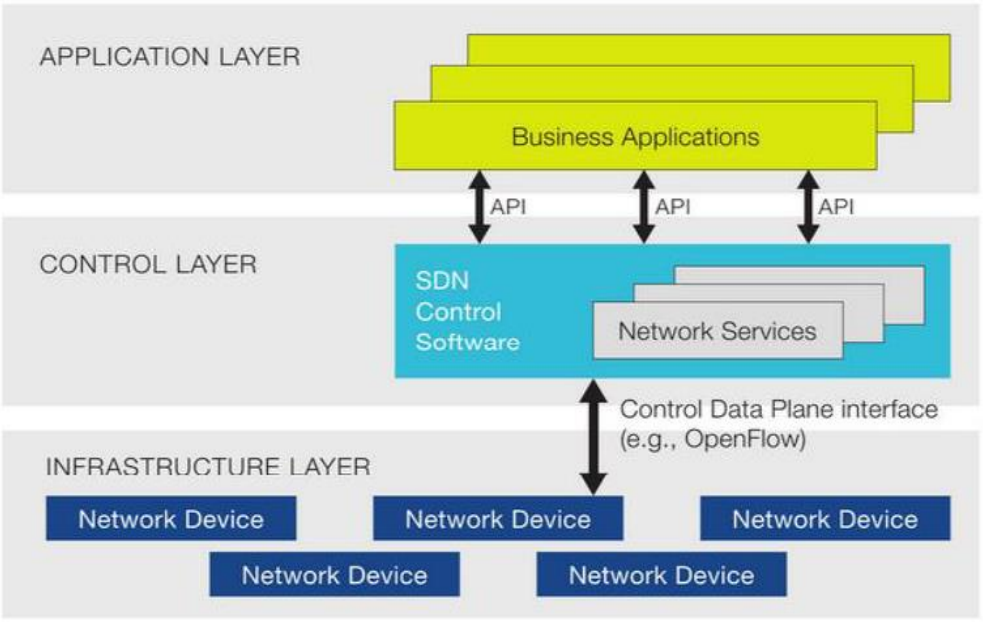
gestión y administración (políticas, reglas, configuraciones, etc.) se la realiza a través del llamado controlador SDN, es decir es el cerebro de la red. Por otro lado, el plano de datos encargado únicamente del reenvío de paquetes basado en las directrices emitidas por el plano de control.

Es importante tener en cuenta que su implementación es mucho más simple en comparación con redes de datos tradicionales ya que no depende de un único fabricante y además tiene la capacidad de virtualizar funciones de red (NFV) con el objetivo de utilizar menor cantidad de dispositivos.

### 2.3.1 Arquitectura SDN

En la Figura 2.4. se puede visualizar que la arquitectura de las SDN están divididas en tres capas: la capa de aplicación encargada de introducir funciones de seguridad, monitoreo y gestión a través de diferentes aplicaciones, la capa de control la arquitectura SDN comprende tres capas: la capa de Aplicación, la capa de control que representa la parte inteligente de la red, es decir el controlador SDN y la capa de infraestructura o plano de datos encargado únicamente del reenvío de los datos a través de los conmutadores físicos de la red (Rosencrance, 2022).

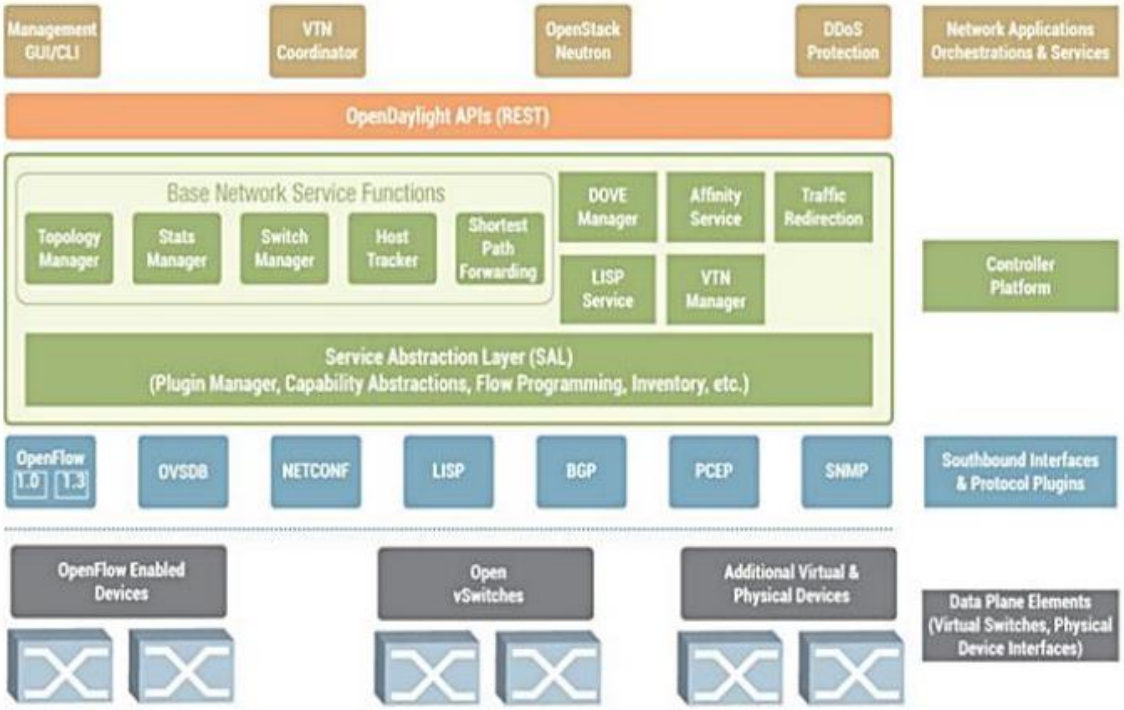
**Figura 2.4.** Arquitectura SDN




Fuente: (SDXcentral, 2018)

Estas tres capas se comunican a través de las interfaces *northbound y southbound también* conocidas como *Application Programming Interfaces* (API) que ofrecen un conjunto de protocolos para permitir la comunicación entre aplicaciones – controlador y controlador – conmutadores o equipos del plano de datos, respectivamente (Rosencrance, 2022). En la Figura 2.5. se pueden visualizar los protocolos *northbound y southbound.*

**Figura 2.5.** Protocolos Northbound y Southbound




Fuente: (SDXcentral, 2018)

Es importante aclarar que *OpenFlow* no es SDN, sino hace referencia a un protocolo *southbound* (el más utilizado) de SDN por su mayor desarrollo en cuanto a términos de estandarización e interoperabilidad se refiere. De manera general, *OpenFlow* no actualiza las tablas de enrutamiento de los dispositivos del plano de datos como los protocolos de enrutamiento tradicionales, este se encarga de modificar únicamente las *Flow tables*, las cuales tienen entradas a los distintos flujos de datos (Salazar, 2022).

### 2.3.2 Ventajas – Desventajas de SDN

A continuación, se muestra una tabla que resume los beneficios, así como los desafíos que implican las SDN:

**Tabla 2.1.** Ventajas y Desventajas de SDN

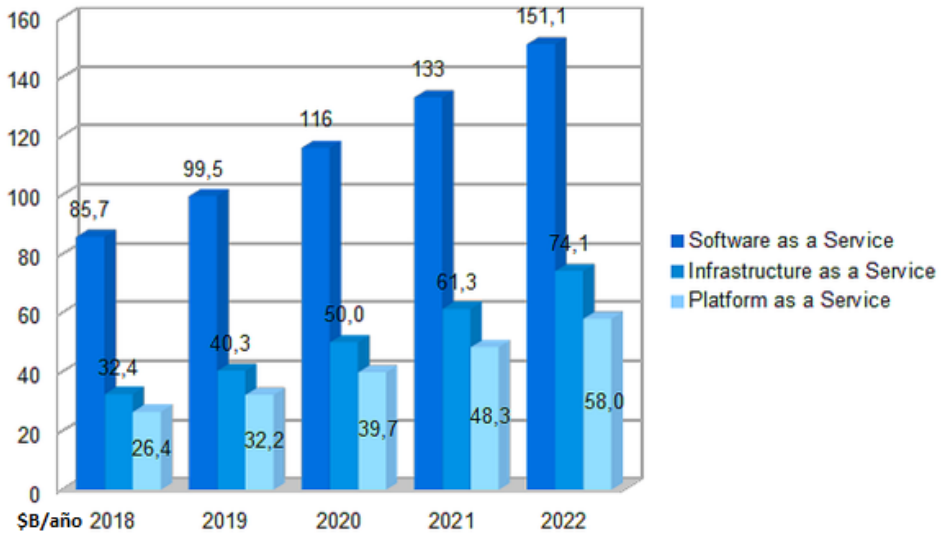
| **SOFTWARE DEFINED NETWORK (SDN)** | |
|---|---|
| **Ventajas** | **Desventajas** |
| • Disminución de CAPEX y OPEX (gastos por capital y operación)<br>• Ejecución más simple de *Traffic Enginnering*<br>• Mayor flexibilidad de la red<br>• Simplifica la gestión y administración de la red. | • Menor confiabilidad al disponer de un único punto central o controlador.<br>• Mayores vulnerabilidades de seguridad ya que es una infraestructura reciente y elimina el uso de equipos físicos como *routers* y switches. Además, de que el controlador es |

| | |
|---|---|
| • Reducción de tiempos de despliegue de configuraciones ya que el controlador es el cerebro de la red, y los conmutadores solo encargan del reenvío de datos. | un único punto de ataque que puede afectar a toda la red.<br>• La escalabilidad puede verse afectada si el controlador es de bajas prestaciones y con problemas de rendimiento. |

## 2.4 Software-Defined Wide Area Network (SD-WAN)

Existen ciertos aspectos que han hecho posible el surgimiento de las redes de área extendida de nueva generación, por ejemplo en la Figura 2.6 se visualiza la alta demanda de nubes públicas que existe actualmente, es decir el incremento de servicios como *Software as a Service* (Saas), *Platform as a Service* (PaaS) e *Infraestructure as a Service* (IaaS); adicionalmente, la actualización de la infraestructura de centros de datos por parte de las empresas gracias a la evolución acelerada de la tecnología, han obligado a las organizaciones a actualizar y mejorar la WAN. Es aquí donde aparece la SD-WAN gracias a su costo bastante menor en comparación de MPLS ofreciendo buenas prestaciones en términos de rendimiento, disminución de latencia, adaptabilidad, etc.

**Figura 2.6.** Evolución de SaaS, PaaS e IaaS




Fuente: (Gartner, 2019)

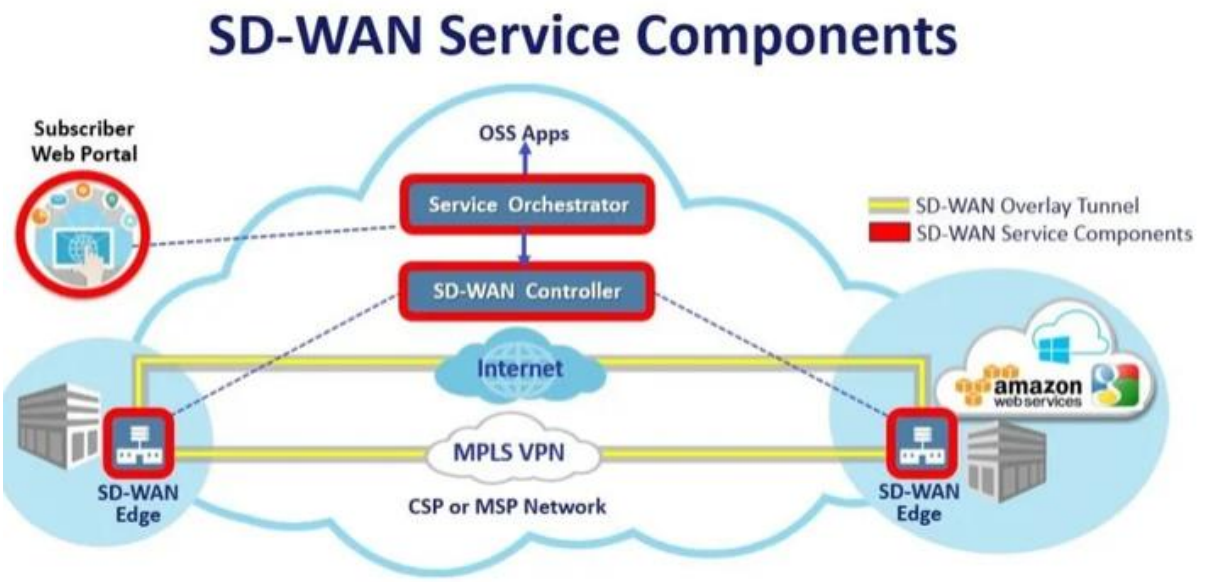
Antes de profundizar en el concepto, arquitectura y beneficios de la SD-WAN, cabe recalcar la diferencia con SDN, el primero a su vez proporciona enrutamiento a nivel WAN, mientras que el segundo es utilizado internamente dentro de la LAN o incluso en centros de datos.

SD-WAN, se define como una aplicación específica de SDN a tecnologías WAN (Salazar, 2022). Su finalidad es reemplazar los servicios de optimización WAN, VPN-MPLS, automatización, etc. Presenta características mejoradas de enrutamiento al ser multi-transporte y permite un mejor monitoreo y administración del tráfico de datos en tiempo real.

### 2.4.1 Componentes SD-WAN

La arquitectura abstracta de SD-WAN está dividida en dos partes: el plano de control y el plano de datos, con el objetivo de que esta sea administrada remotamente sin necesidad de un administrador de TI en sitio. Sin embargo, a pesar de su arquitectura de dos planos, en la Figura 2.7. se puede visualizar los tres componentes principales de una SD-WAN: el orquestador, el controlador y el *SD-WAN Edge.*

**Figura 2.7.** Componentes de SD-WAN




Fuente: (Lessing, 2021)

El *SD-WAN Edge* hace referencia al componente en donde se encuentran los puntos finales de la red, por tal motivo se conocen como los dispositivos SD-WAN de borde. Estos dispositivos pueden ser físicos, virtualizados e inclusive en la nube.

El controlador es el encargado de centralizar la administración de toda la red, con el objetivo de que los operadores e ingenieros de TI puedan ver y configurar políticas de la red a través de una interfaz única (*single pane of glass*).

El orquestador crea una interfaz de administración, capaz de supervisar el tráfico y controlar fácilmente la implementación total de una red a través de la aplicación de las políticas y protocolos establecidas en el controlador.

A partir de estos componentes (controlador-orquestador) aparece el término *Zero-Touch Provisioning* (ZTP), que permite a los dispositivos ser configurados de forma masiva descargándose únicamente las plantillas de configuración del plano de control, con el objetivo de automatizar la red y permitir el aprovisionamiento sin configuración o de toque zero, y así reducir los tiempos de implementación.

En la Figura 2.7. también se puede visualizar que SD-WAN es una superposición de la red existente, es decir una red virtual funcionando sobre otra red a través de túneles o Virtual Private Nertworks (VPN), en otras palabras, se puede decir que una característica importante de la arquitectura de SD-WAN es que permite establecer una red lógica sobre la red física.

### 2.4.2 Tipos de Arquitectura SD-WAN

En la Tabla 2.2, se muestran los tipos de arquitectura SD-WAN: local (*on-premise*), habilitada en nube (*cloud-enabled*) y SD-WAN troncales.

**Tabla 2.2. Tipos de arquitecturas de despliegue de SD-WAN**

| **TIPOS DE SD-WAN** | | |
|---|---|---|
| ***On-premise*** | ***Cloud-enabled*** | ***Cloud-enabled with backbone*** |
| - SD-WAN local ya que el hardware reside dentro de la organización.<br>- No utiliza la nube para ninguna conexión.<br>- Ideal para información confidencial que puede ser enviada por Internet. | - Conectadas a un Gateway virtual en la nube usando Internet.<br>- Mejor accesibilidad, integración y rendimiento en aplicaciones de nube. | - Se conecta a la red a través de la nube y adicional un punto de presencia (PoP) como dentro de un *data center.*<br>- Brinda mayor redundancia, ya que el tráfico puede cambiar de internet a una conexión privada.<br>- Agrega mayor consistencia. |

### 2.4.3 Beneficios - Desafíos de SD-WAN

Es importante mencionar las ventajas que SD-WAN presenta frente a otro tipo de tecnologías WAN tradicionales, sin embargo, también tiene desafíos que debe contrarrestar para que las organizaciones confíen plenamente en esta solución o a su vez adopten una SD-WAN híbrida que funcione en conjunto con la infraestructura actual que mantienen la mayoría de las empresas como es MPLS. A continuación, se detallan los principales atributos de SD-WAN:

- ✓ Mejor o mayor ancho de banda a menor costo, tomando en cuenta que se puede realizar ingeniería de tráfico basado en aplicaciones.
- ✓ Mejor rentabilidad tomando en cuenta que el pago es bajo demanda, es decir se adapta al crecimiento, adicional elimina los límites geográficos ya que utiliza la infraestructura pública de internet.
- ✓ Administración centralizada desde un único punto y a través de una amigable interfaz gráfica, lo que facilita la gestión para los ingenieros de TI.
- ✓ Ofrece una visibilidad holística de la red, lo que permite identificar de manera más inteligente el tipo de tráfico y así tomar mejores decisiones automatizadas de enrutamiento de paquetes.
- ✓ Mayor adaptabilidad y rendimiento a servicios basados en la nube, tomando en cuenta que puede reducir la latencia eliminando el tráfico de *backhaul* [4].
- ✓ Mejor rendimiento de la red al usar simultáneamente varias aplicaciones que requieren un gran

[4] ***Backhaul*****:** *hace referencia al tráfico que pasa por el centro de datos antes de ser enviado a otro extremo o sucursal, conocido como tráfico de retorno.*

ancho de banda.

- ✓ Reducción de tiempos de implementación gracias a su característica ZTP.
- ✓ Es multi-transporte, es decir permite diferentes conexiones o enlaces para el envío de datos.
- ✓ Mayor flexibilidad en la elección del tipo de conexión y del proveedor ya que la red puede utilizar conexiones públicas como privadas para enrutar el tráfico de paquetes.

#### 2.4.3.1 SD-WAN Híbrida (SD-WAN y MPLS)

Tomando en cuenta que MPLS es la tecnología WAN más utilizada es importante establecer una breve comparativa de esta con SD-WAN, de tal manera que se pueda asimilar todas las ventajas que puede presentar una SD-WAN Híbrida dentro de una organización o a su vez la factibilidad de uso de SD-WAN como infraestructura *overlay* manteniendo MPLS como *underlay*. A continuación, se muestra una tabla con la comparativa de estas dos tecnologías.

**Tabla 2.3.** Comparación de atributos de SD-WAN y MPLS

| SD-WAN | MPLS |
|---|---|
| Red con superposición virtualizada, abstracción del software del hardware. | Confiabilidad o fiabilidad |
| Gestión centralizada basada en políticas. | Alto nivel de QoS |
| Reducción de CAPEX | Seguridad Garantizada |
| Administración simplificada | |

#### 2.4.3.2 Desafíos de la SD-WAN

A pesar de que SD-WAN presenta varias ventajas que inclinan a las organizaciones a adoptar esta solución, es inminente también analizar un par de desafíos que esta implementación implica:

1. Se necesita de personal altamente calificado para su implementación y posteriormente para su administración y gestión, más aún si es una *SD-WAN on-premise.*
2. Controlar la seguridad y confidencialidad ya que utiliza la infraestructura pública de Internet, por lo que se vuelve más vulnerable a ataques de piratas informáticos. Sin embargo, a continuación, se analizarán dos soluciones de SD-WAN de diferentes proveedores bastante posesionados en el mercado que han contrarrestado el tema de seguridad de manera muy eficiente.
3. Al depender de la conectividad pública de internet el rendimiento lento, latencia o pérdida de paquetes depende del proveedor, por lo que es recomendable mantener enlaces de redundancia con diferentes proveedores.

Tomando en cuenta el cuadrante mágico de Gartner para la Infraestructura de borde a nivel WAN (*WAN Edge Infrastructure*) que se muestra en la Figura 2.8. se procederá a analizar las soluciones de dos

proveedores que están ubicados como líderes y que están bastante posicionados en el mercado ecuatoriano en cuanto a *routing, switching* y *firewalls* se refiere.

**Figura 2.8.** Cuadrante Mágico de Infraestructura WAN de borde


Fuente: (Gartner, 2021)

## 2.5 Cisco Viptela SD-WAN

En la sección anterior, se describió los planos que componen la arquitectura de una SD-WAN en forma general, sin embargo, en el caso de proveedores específicos como Cisco Viptela SD-WAN se compone de cuatro planos segregados: de administración, de orquestación, de control y de datos. Cada uno de estos planos están abstraídos uno del otro de tal manera que si se realiza algún cambio de equipo en el plano de datos no afecta a los planos superiores, manteniendo el mismo principio característico de abstracción de plano de datos y control de las SDN.

A continuación, se describen los principales atributos por las que Cisco Viptela SD-WAN es una de las mejores opciones según el cuadrante de Gartner:

- ✓ Interconexión rápida y segura desde cualquier ubicación y automatización a través de ZTP.
- ✓ Proporciona una WAN independiente del medio de transporte.
- ✓ Abstracción de la infraestructura WAN subyacente (red física) de los servicios y aplicaciones como: QoS, optimización WAN, IaaS, etc.
- ✓ Seguridad de cifrado extremo a extremo.
- ✓ Mayor visibilidad al proporcionar un único panel de administración, análisis y configuración de políticas *(Single Pane of Glass - SPOG)*
- ✓ Proporciona APIS tipo REST en el *southbound* que permiten a las organizaciones crear sus

propios servicios únicos.

- ✓ Ahorros en CAPEX y OPEX.
- ✓ Mayor Seguridad a través de diversas funcionalidades como IPS, inspección granular de paquetes, etc.

### 2.5.1 Componentes Cisco Viptela SD-WAN

Los componentes principales de esta solución son: Cisco vManage, Cisco vBond, Cisco vSmart y Cisco vEdge. A continuación, se detalla la funcionalidad de cada uno de estos.

**Cisco vManage**

Hace referencia al plano de administración o gestión de la SD-WAN, es decir la Interfaz Gráfica de Usuario (GUI) que permite la interacción directa con los administradores de la red. Este dispositivo se encarga de recopilar datos de telemetría de red, así como ejecución de análisis y notificaciones sobre cualquier evento inusual que ocurra en la SD-WAN. Además, permite la creación de *templates* para enviar configuraciones e ingeniería de tráfico con VPNs a los dispositivos en sucursales, esta funcionalidad es conocida también como ZTP. Para su implementación y despliegue puede ser en tres tipos: *on-premise,* nube pública o nube de cisco.

**Cisco vBond**

Hace referencia al plano de orquestación de la SD-WAN. Este dispositivo es encargado específicamente del proceso de incorporación y sincronización de nuevos dispositivos a la estructura SD-WAN a través de métodos de autenticación e integración de los vEdge en listas blancas.

**Cisco vSmart**

Hace referencia al plano de control de la SD-WAN, estos dispositivos son el cerebro la red *overlay* encargados del enrutamiento, políticas y seguridad. Los vEdge se conectan con los vSmart, de tal manera que cumplen un principio similar al de *Border Gateway Protocol (BGP) route reflector* o el de enrutadores *Dynamic Multipoint* VPN, sin embargo, es importante aclarar que no forman parte del plano de datos a pesar de que se emparejan con los vEdge.

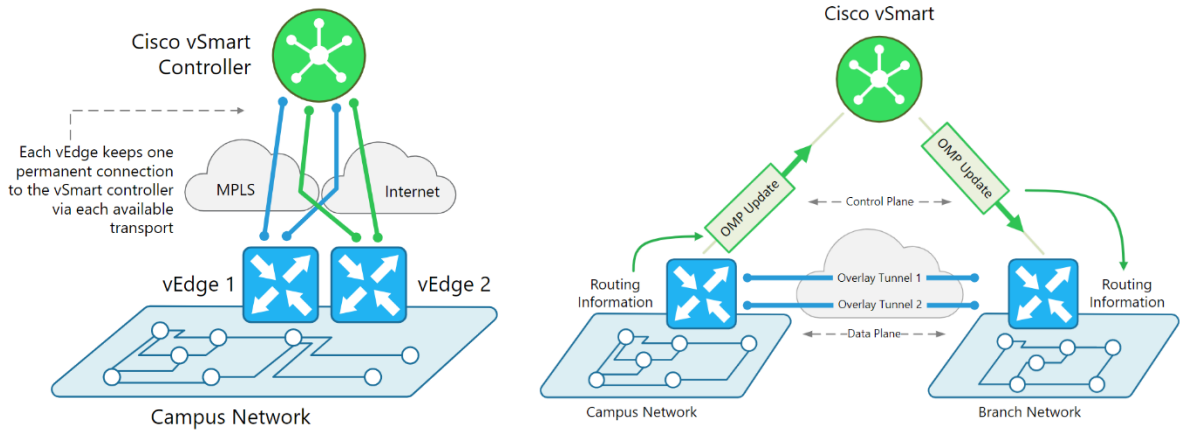
**Cisco vEdge**

Hace referencia al plano de datos de la SD-WAN, están situados en el borde de la WAN con el fin de establecer toda la estructura de red *underlay* y *overlay*. Es importante mencionar que los vEdge se comunican con los vSmart a través del protocolo *Overlay Management* (OMP), por lo que a continuación se revisa más a detalle este protocolo. Los vEdge pueden ser plataformas Viptela o dispositivos Cisco IOS-XE, ya sean físicos o virtuales.

### 2.5.2 Overlay Management Protocol (OMP)

Los Cisco vSmart utilizan el protocolo OMP para administrar le red *overlay*. Los enrutadores vEdge establecen conexiones seguras permanentes (*Datagram Transport Layer Security*) con los controladores vSmart a través de cada medio de transporte disponible (MPLS, Internet, LTE, etc.) para intercambiar información como prefijos, claves e información de políticas. Esto se puede visualizar en la Figura 2.9.

**Figura 2.9** Asociación OMP de los Cisco vEdges




Fuente: (NetworkAcademy.io, 2021)

OMP anuncia tres tipos de rutas:

1. **Rutas OMP (vRouter):** pueden ser rutas OSPF (*Open Shortest Path First*), BGP o cualquier otra información de enrutamiento redistribuida a través de OMP.
2. **Rutas TLOC (*Transport Locator*):** son los extremos de la VPN en los *routers* de borde WAN que se conectan a la red de transporte. Están formadas por dirección IP del sistema, color de enlace y tipo de encapsulación.
3. **Rutas de Servicio:** utilizadas para intercambiar servicios como *firewall*, IPS, optimización de aplicaciones y balanceadores de carga.

## 2.6 Fortinet SD-WAN

Otra solución de SD-WAN que tiende a ser una de las líderes según Gartner es la del proveedor FORTINET, por tal motivo a continuación se procede a realizar un análisis más detallado.

La *Secure SD-WAN* de FORTINET incluye funcionalidades de seguridad como NGFW (*Next Generation Firewall)* unificadas con otras como SD-WAN, esto hace que la solución de FORTINET corrobore las inconsistencias y dudas respecto a la seguridad de una SD-WAN en comparación con MPLS.

Al igual que la solución de CISCO, esta SD-WAN de FORTINET tiene como objetivo reducir el CAPEX y OPEX, simplificación de operaciones y aprovisionamiento y mejorar el rendimiento de la red sin dejar de lado la seguridad, sino al contrario ofrecer mejores mecanismos de seguridad gracias al posicionamiento que tienen en el mercado respecto a la línea de dispositivos de seguridad de red.

A continuación, se describen los principales atributos por las que *Secure* SD-WAN de FORTINET es una de las mejores opciones según el cuadrante de Gartner:

- ✓ Ofrece de manera unificada funcionalidades de seguridad NGFW con inspección SSL (*Secure Socket Layer*), enrutamiento avanzado, optimización WAN, SD-WAN en un único dispositivo.
- ✓ Aprovisionamiento de toque cero (ZTP).

- ✓ Disminución del Costo Total de Propiedad (TCO), es decir hace referencia a los precios de adquisición de un servicio, sus dispositivos, licencias y mantenimientos que necesite durante su tiempo de vida útil,
- ✓ Rendimiento mejorado de aplicaciones en la nube debido al eficiente balanceo WAN que realiza.
- ✓ Administración centralizada a través de un único equipo conocido como FortiManager en comparación con la solución CISCO que utiliza los dispositivos vManage y vSmart para la gestión y administración.

### 2.6.1 Componentes Fortinet Secure SD-WAN

Los componentes principales de esta solución son: FortiManager, FortiAnalyzer y FortiGate. Es importante destacar que su interfaz gráfica es bastante amigable respecto a otros *vendors.* A continuación, se detalla la funcionalidad de cada uno de estos.

**FortiManager**

Es el dispositivo encargado de la administración, gestión y configuración de distintos equipos de la marca FORTINET, en este caso específicamente se refiere a FortiGate y FortiAnalyzer. Desde este equipo se realiza las funciones de ZTP. Además, permite la integración con FortiAnalyzer en el mismo equipo siempre y cuando la WAN sea básica y no necesite una cantidad alta de recursos para manejar logs y reportería.

**FortiAnalyzer**

Como su nombre lo indica es el encargado del análisis y monitoreo de la SD-WAN, este permite desplegar los diferentes logs o registros, así como la generación automatizada de reportes e informes de eventos seguridad, VPNs y escaneo de la red. Puede ser desplegado de manera física, virtual y en la nube.

**FortiGate**

Este dispositivo integra funciones de red junto con funciones de seguridad y especialmente con la funcionalidad de SD-WAN, por este motivo es considerado como todo en uno. Es importante mencionar que este dispositivo es el de borde similar a vEdge en CISCO. Su nivel de seguridad es bastante llamativo ya que ofrece todas las funcionalidades de un Firewall NGFW. Puede ser desplegado en hardware, virtualizado o en nube como SaaS.

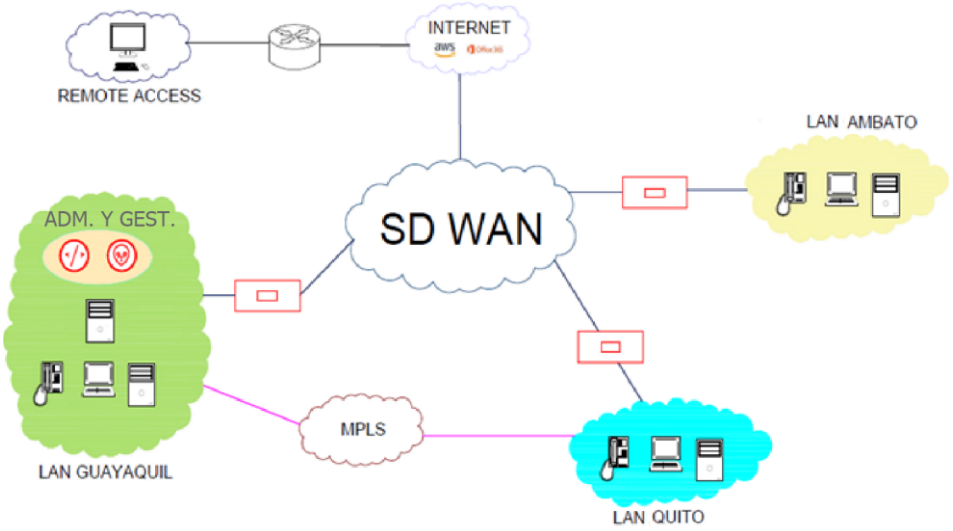
# 3 METODOLOGÍA

## 3.1 Arquitectura de la red de estudio: SD-WAN Híbrida

Independientemente del proveedor, existen dos escenarios respecto a la arquitectura de red, uno de ellos es una SD-WAN única para toda la red WAN empresarial, mientras que el otro es una SD-WAN Híbrida, que se refiere a la integración de SD-WAN con la infraestructura existente de las empresas, comúnmente siendo MPLS. En este caso, se toma en cuenta la arquitectura de red de una SD-WAN Híbrida para establecer la comparativa entre los dos fabricantes como FORTINET y CISCO, debido a que en Ecuador las empresas tienden a mantener su infraestructura por la inversión inicial realizada y por temas de seguridad tomando en cuenta que envían el tráfico crítico o confidencial por la red MPLS y porque esta arquitectura abarca un escenario más completo para el análisis.

En la Figura 3.1. se puede visualizar un bosquejo general de la arquitectura de la SD-WAN Híbrida a analizar. Con fines de estudio, se establece en la arquitectura una empresa con su oficina matriz en GYE, un centro de datos en Quito y una sucursal en Ambato. Es importante mencionar que la SD-WAN es el punto central de comunicación entre todas las oficinas de la empresa. Sin embargo, se aprecia una infraestructura existente entre UIO - GYE que hace referencia a la red MPLS que se mencionó anteriormente. Adicional, se visualiza una nube de acceso remoto con el objetivo de analizar también el funcionamiento de VPNs (*Virtual Private Network*) a través de la SD-WAN. Es importante mencionar que en la oficina matriz se encuentran los equipos de administración y gestión de la SD-WAN, mientras que en las otras oficinas únicamente los equipos de borde, por ejemplo, un vEdge o un FortiGate dependiendo del fabricante.

**Figura 3.1.** Arquitectura de la SD-WAN Híbrida.




Fuente: Autor

## 3.2 Conceptos Generales: Políticas, Objetos, Reglas y Seguridad de la SD-WAN

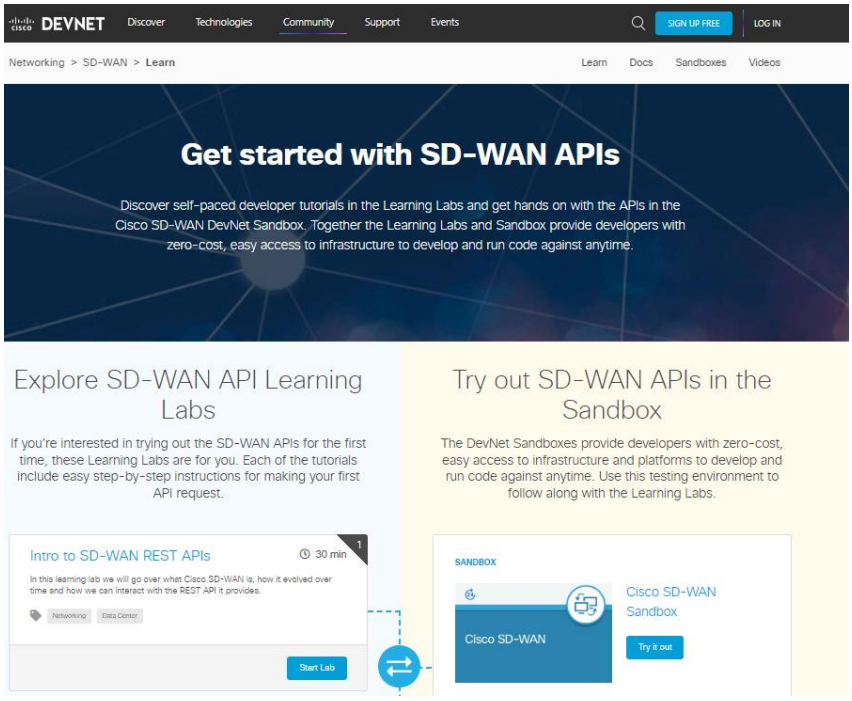
Es importante entender algunos conceptos que son primordiales dentro del funcionamiento de la SD-WAN previo al análisis de esta tecnología desde el punto de vista de los dos fabricantes a comparar.

- **Políticas:** sirven para definir o establecer los puertos por donde entra y sale el tráfico.
- **Objetos:** hace referencia a las subredes de origen y destino del tráfico, estas pueden ser IPs únicas o subredes declaradas con nombres.
- **Reglas:** en conjunto con las políticas son las encargadas de definir el comportamiento o funcionamiento de los enlaces que forman la SD-WAN.
- **Seguridad SD-WAN:** este término es un tanto variable dependiendo del fabricante ya que algunos proporcionan más funcionalidades que otros o a su vez funcionan dentro del mismo equipo o por separado.

## 3.3 Funcionamiento de la SD-WAN VIPTELA de CISCO

Para entender con mayor profundidad el funcionamiento de la SD-WAN VIPTELA de CISCO es importante relacionar los conceptos teóricos dentro de un ambiente práctico. Un aspecto importante para destacar sobre el fabricante es que en su plataforma ofrece laboratorios gratuitos de SD-WAN para la parte práctica; algunos de estos necesitan una reservación previa y la instalación de la VPN de CISCO para su desarrollo.

**Figura 3.2.** Laboratorios SD-WAN de CISCO




Fuente: (developer.cisco.com, 2022)

Sin embargo, en este caso, se tomará como ejemplo una SD-WAN ya desarrollada en el emulador EVE-NG, con el fin de entender su funcionamiento y establecer las diferencias y similitudes respecto al otro fabricante que se analizará con un emulador diferente.

### 3.3.1 Software de Emulación EVE-NG

En primer lugar, es un software de emulación de red que permite realizar pruebas de concepto (PoC) de diferentes proveedores. No tiene un cliente por lo que se accede a través de cualquier navegador reduciendo el consumo de recursos, sin embargo, para su correcto rendimiento en este escenario SD-WAN es recomendable una máquina con al menos 16 GB en RAM y 256 GB en disco de estado sólido. Su objetivo es brindar a los profesionales de redes la facilidad de emular ambientes de redes previo a su implementación para así poder minimizar errores y ahorrar recursos económicos y de *hardware/software* antes del despliegue en campo (Eve-ng.net, 2021).

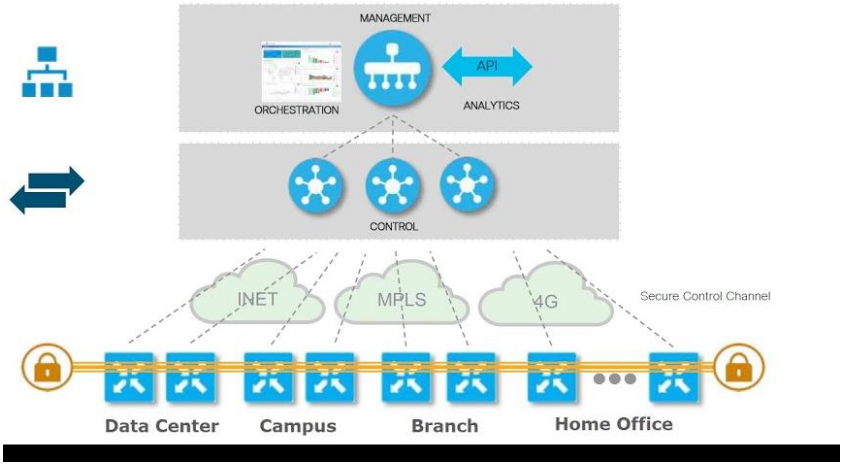
EVE-NG permite a los ingenieros de TI auto-entrenarse en marcas como CISCO, Juniper, Checkpoint, etc. a través de la construcción de redes acorde a los requerimientos y diseño que se planifique. Sus ventajas son la facilidad, rápido despliegue y mejoramiento de la arquitectura de red en un ambiente seguro de emulación sin afectar la red real existente (Eve-ng.net, 2021).

### 3.3.2 Enrutamiento de SD-WAN VIPTELA DE CISCO

En primer lugar, es importante establecer la diferencia entre la definición de paquetes de enrutamiento y paquetes enrutados. Los de enrutamiento hacen referencia a los mensajes que forman la *Routing Information Base* (RIB), mientras que los paquetes enrutados se definen como aquellos mensajes que deben ser enrutados por el equipo, es decir los mensajes de usuario.

Una vez entendido estos conceptos, de manera general el enrutamiento se realiza de la siguiente forma: los paquetes de enrutamiento son enviados desde los vEdges o equipos de borde hacia el plano de control, mientras que los paquetes enrutados se envían únicamente entre los vEdges, lo que permite tener una conectividad de extremo a extremos entre sedes o sede-matriz, toda esta comunicación a nivel WAN ya que la LAN está detrás de los equipos de borde (Salazar, 2021).

**Figura 3.3.** Enrutamiento de CISCO SD-WAN




Fuente: (I-MEDITA, 2020)

### 3.3.3 Selección del mejor camino usando OMP

Es importante mencionar como realiza la selección dinámica del mejor camino este fabricante ya que a diferencia de FORTINET y otros fabricantes lo realiza con OMP, protocolo que fue descrito anteriormente en la fase teórica.

OMP es el encargado de escoger el mejor camino a los diferentes destinos, sin embargo, las rutas OMP pasan a la tabla de enrutamiento de un vEdge siempre y cuando su TLOC o siguiente salto sea válido, es decir exista una comunicación bidireccional. Una vez que los vEdge anuncian todas las rutas OMP al plano de control o vSmarts, estos son los encargados de definir el mejor camino basado en diferentes políticas de enrutamiento (Latencia, Ancho de banda, Pérdida de paquetes, etc.) y enviar esta información al resto de vEdges (Salazar, 2021).

Existen diferentes parámetros o métricas para determinar la mejor ruta OMP, como, por ejemplo:

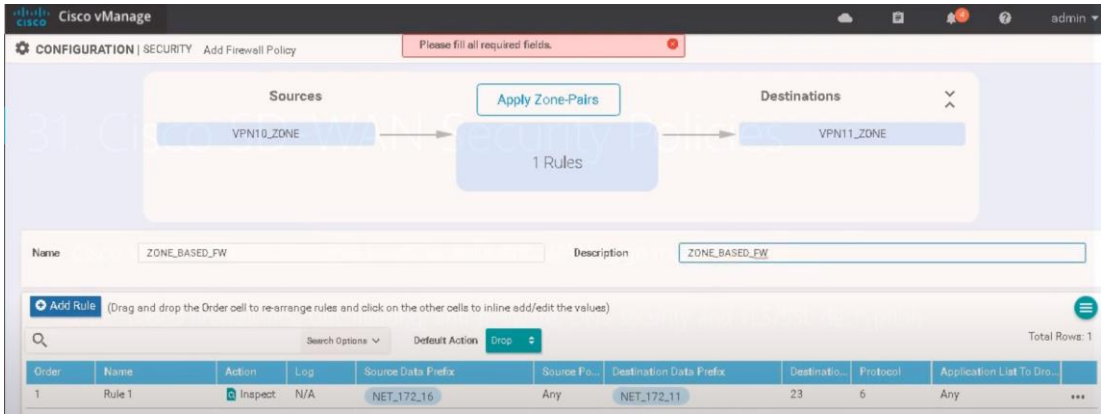
- Existencia de una ruta OMP válida, es decir si existe un TLOC válido.
- Ruta OMP originada locamente desde un vEdge que aprendida por el vSmart.
- Distancia Administrativa más baja.
- Preferir el origen de la rutade acuerdo con el siguiente orden: Directamente conectadas, estáticas, eBGP, EIGRP, OSPF. iBGP.

### 3.3.4 Seguridad de la SD-WAN

Independientemente del fabricante, es muy importante tener en cuenta la seguridad en la implementación de una SD-WAN ya que, al utilizar la infraestructura pública de internet como medio de transporte, existe mayor número de ataques de piratas cibernéticos, así como diferentes intentos de vulnerar la seguridad para fines mal intencionados. Por esta razón, Cisco como tal permite a través de vManage desplegar políticas de seguridad de diferentes tipos como:

- **Firewall**: permitir, bloquear o monitorea los paquetes basados en tipo de protocolo o puertos.

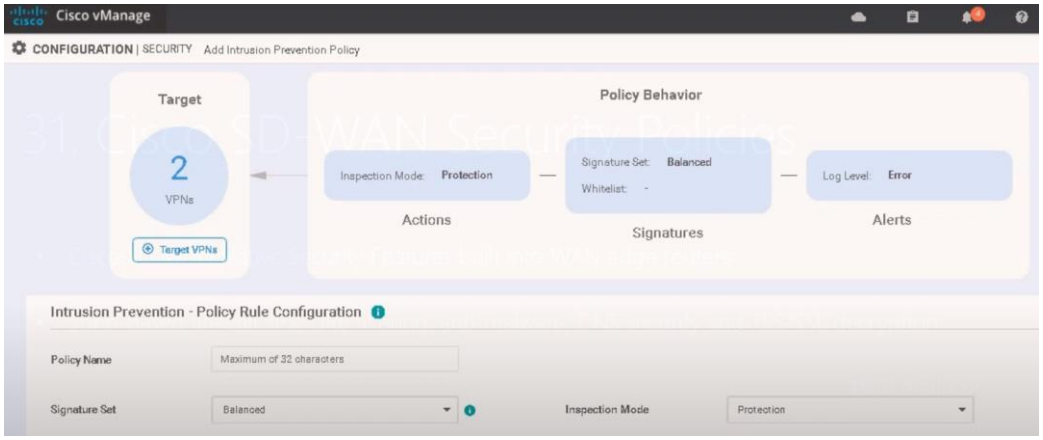
**Figura 3.4.** Política de Firewall




Fuente: (RAYKA, 2021)

- **Prevención de Intrusos (IP):** hace una inspección o detección previa al ingreso de paquetes, la detección conlleva mayor procesamiento ya que hace un análisis más profundo.

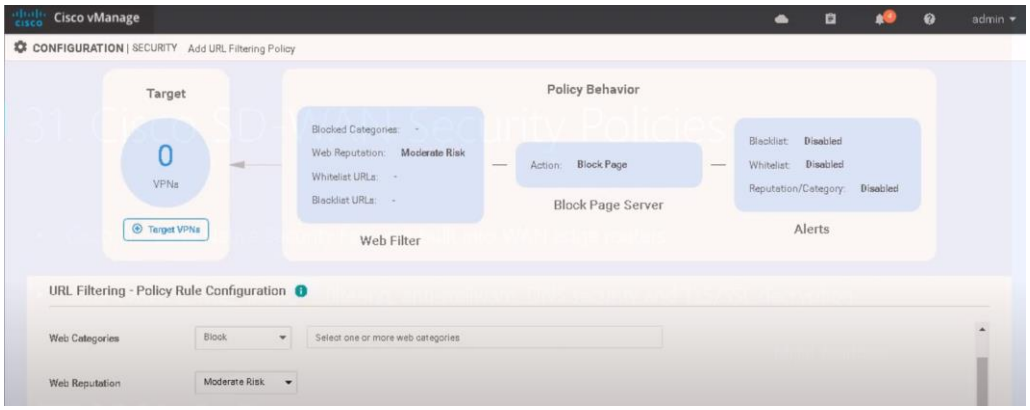
**Figura 3.5.** Política de Prevención de Intrusos.




Fuente: (RAYKA, 2021)

- **Filtrado de URL:** permite o bloquea páginas web por categorías o por su reputación del nivel de riesgo. Pueden también configurar páginas web especificas en listas negras o blancas.

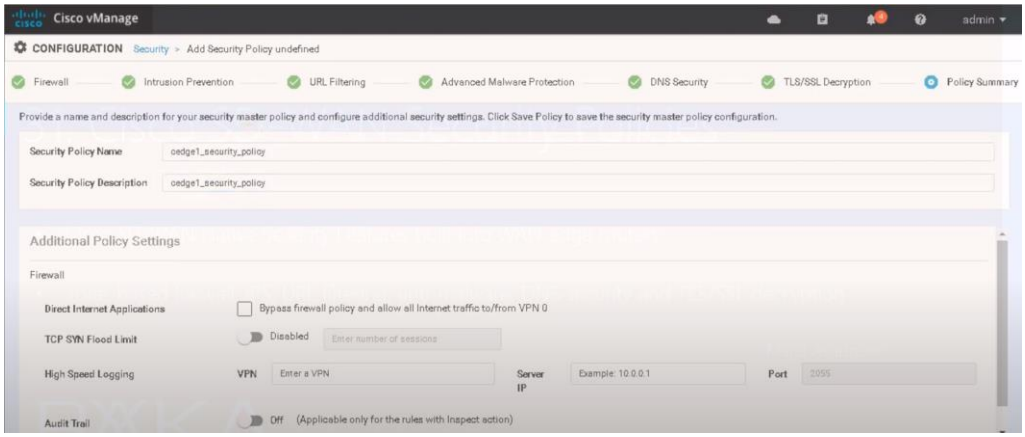
**Figura 3.6.** Política de Filtrado de URL




Fuente: (RAYKA, 2021)

- **Desencriptado TLS/SSL (*Transport Layer Security/Secure Socket Layer*):** para esto es necesario generar y activar los certificados propios de CISCO o externos en cada uno de los dispositivos que componen la SD-WAN Viptela de CISCO.

**Figura 3.7.** Política de Desencriptado TLS




Fuente: (RAYKA, 2021)

- **Protección avanzada de *malware*:** bloquea los *malware* comunes y más conocidos.
- **Seguridad DNS:** predecir dominios mal intencionados y neutralizar amenazas ocultas en túneles DNS.

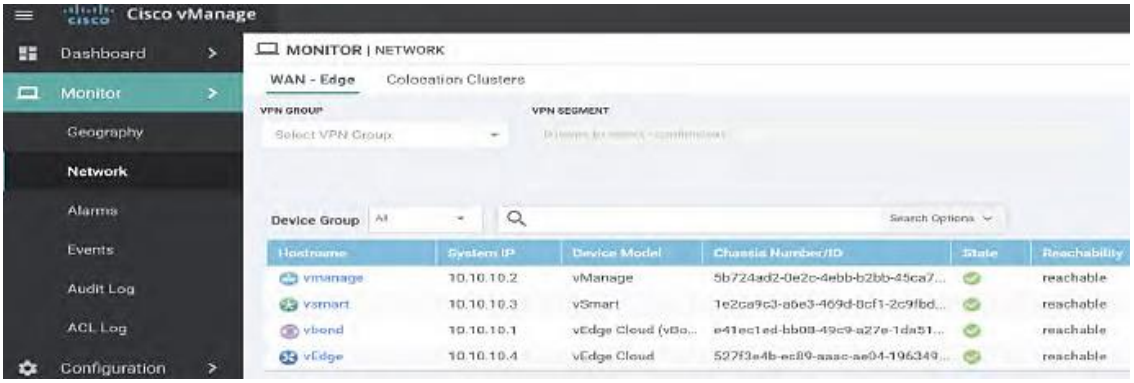
Cisco SD-WAN define como zonas a enlaces SD-WAN u otros VPNs site-to-site las cuales se puede ir personalizando o añadiendo políticas de seguridad de acuerdo con el tipo de tráfico que manejen dichas zonas.

Con la finalidad de mantener la encriptación, autenticación, y control de acceso extremo, Viptela adiciona a su seguridad la plataforma o solución Secure Extensible Network (SEN), basado en el uso de llaves públicas-privadas, las mismas que se encuentran en el plano de control. Además, es importante mencionar que los túneles de comunicación entre los dispositivos de borde o vEdges están protegidos por *Internet Protocol Security* (IPSec) al igual que los enlaces de la red de transporte (Salazar, 2021).

### 3.3.5 Monitoreo y Análisis

Otra funcionalidad o característica importante dentro del funcionamiento de la solución SDWAN Viptela es su capacidad de monitoreo y análisis de infraestructura. Por ejemplo, en la Figura 3.8. se puede visualizar la interfaz gráfica que presenta vManage para tener una visualización completa de toda la red y sus componentes (Salazar, 2021).

**Figura 3.8.** Monitoreo de la red y sus componentes.

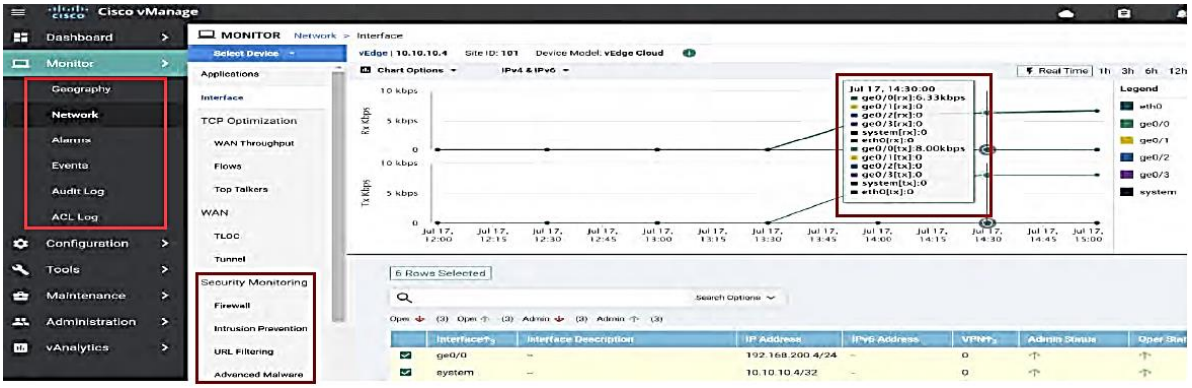



Fuente: (Salazar, 2021)

Adicionalmente, permite monitorear y tener un reporte o *dashboard* de diferentes tipos de eventos, alarmas, logs, y también un monitoreo de todos los eventos respecto a las políticas de seguridad mencionadas anteriormente. En la Figura 3.9. por ejemplo, se puede visualizar el tráfico generado por cada interfaz y además se visualiza las pestañas de monitoreo de seguridad de las políticas previamente aplicadas a ciertas zonas.

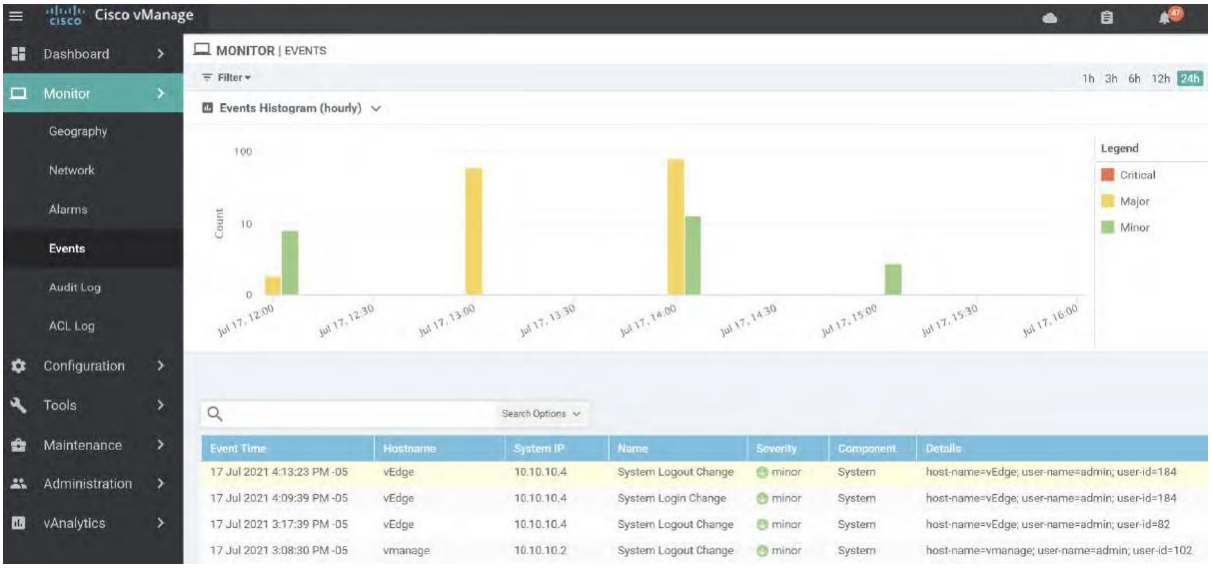
La funcionalidad de monitoreo presenta una interfaz bastante amigable, inclusive permite visualizar cada uno de los eventos que ocurren dentro de la red con toda la información detallada del *hostname*, IP y el usuario y motivo del evento. Para ello, en la Figura 3.10. se muestra un ejemplo de los eventos de *Login* y *Logout* de la sesión de los equipos vEdge y Vmanage con la información mencionada anteriormente.

**Figura 3.9.** Monitoreo de Tráfico y Seguridad




Fuente: (Salazar, 2021)

**Figura 3.10**. Monitoreo de Eventos y logs




Fuente: (Salazar, 2021)

### 3.3.6 Control y Administración de la SD-WAN

Respecto al control de la SDWAN Viptela es importante recalcar que el cerebro o plano del control es el vSmart encargado del enrutamiento inteligente y selección de los mejores caminos utilizando OMP. Sin embargo, la administración y manejo se realiza desde vManage ya que es la GUI que interactúa directamente con los administradores de red. Por lo tanto, desde vManage se monitorea y administra toda la red incluso se puede generar *templates* y desplegarlos a través de este, con el fin de cumplir la funcionalidad ZTP.

Además, vManage permite mejorar la experiencia de administración/telemetría a través de APIs tipo REST que establecen la interfaz entre la red SDWAN y el manejo de esta con la finalidad de lograr los empresariales planteados (Salazar, 2021).

#### 3.3.6.1 Conexión de vEdge a la solución Viptela o vManage

Existen diferentes maneras de agregar un vEdge a un vManage, una de ellas puede ser a través de certificados externos u otra a través de una *Smart Account* de Cisco. De este modo se adjunta el ANEXO

A (Moisa J. 2019), que es un manual de interconexión de los vEdge con la cuenta de CISCO en caso de que lo requiera. La segunda forma y la más recomendada es a través de EVE-NG, para esto de igual forma se adjunta el enlace de una Implementación completa de SDWAN CISCO, el cual contiene un video bastante claro de cómo realizar un laboratorio de emulación paso a paso, realizado por PyNet Labs en el 2021:

***https://www.youtube.com/watch?v=PDxK2qIL_rQ&t=3936s***

## 3.4 Funcionamiento de la Secure SD-WAN de FORTINET

Al igual que con el fabricante anterior para entender el funcionamiento de la SD-WAN de FORTINET es necesario combinar la teoría con un ambiente práctico. Para ello se analizará una emulación de SD-WAN de FORTINET ya desarrollada en el software de emulación GNS3.

### 3.4.1 Software de Emulación GNS3

GNS3 es un software que permite a los administradores de red emular, configurar, probar y solucionar problemas de redes ya sea virtuales o reales. Es importante mencionar que es un software gratuito de código abierto por lo que cuenta con una gran comunidad que apoya a su desarrollo y soporte. Hay que tomar en cuenta que la emulación de SD-WAN es un escenario de redes avanzado por lo que se utiliza la opción de VM GNS3, que se trata del uso de VMware Workstation para ejecutar localmente la máquina virtual de GNS3 en la PC, esta puede ser descargada directamente de su página web oficial. (gns3.com, 2021).

De la misma manera que con EVE-NG, es recomendable una máquina con al menos 16 Gb en RAM y 256 Gb en SSD ya que el programa se ejecuta acorde al rendimiento del hardware de la PC. Este software permite emular imágenes de diferentes fabricantes a través de sus diferentes herramientas como Dynamips, Qemu, entre otros. Para este caso, la emulación ya desarrollada hace uso de dispositivos de la marca FORTINET con sus ISO descargadas de la página oficial del fabricante.

El objetivo principal de este software es permitir a los Ingenieros de red emular entornos de red avanzados con el fin de minimizar errores y ahorrar recursos previos a una implementación. Inclusive, permite a los ingenieros prepararse para certificaciones a futuro de cualquier tipo ya que tiene compatibilidad con diversos fabricantes.

### 3.4.2 Objetos y Políticas en la SDWAN de FORTINET

En primera instancia, están los objetos que permiten identificar y diferenciar las distintas subredes, rango de IPs, VPNs, incluso ciertas PCs o direcciones web específicas. Es muy importante previamente configurar los objetos para facilitar la configuración y entendimiento al administrador de la red.

En la Figura 3.11. por ejemplo, se visualiza un conjunto de objetos configurados para una SD-WAN, estos son de tipo subred, IP específica y uno de rango de IPs de VPN, los mismos que se utilizan dentro de la configuración de las políticas.

**Figura 3.11.** Objetos de una SD-WAN de FORTINET

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

Fuente: (López, 2020)

Una vez que ya se tiene agregado los enlaces de la SD-WAN, que únicamente son configuraciones de direccionamiento y enrutamiento para salir a Internet, sin embargo, aún no se puede navegar en Internet ya que son las políticas de la SD-WAN las que van a definir desde y hacia donde sale el tráfico. Estas políticas cumplen un papel crucial dentro de la SD-WAN ya que adicional a lo mencionado, también aquí se agregan los diferentes tipos de seguridad que se detalla en la sección 3.4.4.

En la Figura 3.12. se muestra un ejemplo de políticas de una Sede Principal de la SD-WAN, basta explicar algunas de ellas para entender su funcionamiento. Por ejemplo, la política "*To_DC*" permite la salida de todo el tráfico desde la LAN de la sede principal (HQ) hacia el Data Center (DC) y la sucursal (BO) a través de las interfaces de LAN (port6) y SD-WAN (enlaces de internet). La política de "*Internet Access"* a su vez permite la salida del tráfico desde la Sede Principal (HQ), Data Center (DC), Red MPLS hacia cualquier destino (all), que de manera implícita es la salida a Internet. Una política también importante de ver su funcionamiento es la de "*SSL-VPN"* que corresponde a un túnel o VPN tipo *Secure Socket Layer*, que permite la salida del tráfico de todos los usuarios dentro del grupo PortalWeb_Users hacia la sede Principal. La política "*Implicit Deny*" es la que viene por defecto y niega todo el tráfico, por tal motivo las políticas mantienen un orden de prioridad de ejecución desde arriba hacia abajo, es decir que las políticas se ejecutan en el siguiente orden To_DC, From_DC, InternetAccess, etc. y al final la Implicit Deny.

Aquí termina el análisis del funcionamiento de las políticas, sin embargo, en esta configuración también se adiciona todos los tipos de seguridad que se quiera personalizar a cada política, si se analiza profundamente por ejemplo la política de "*InternetAccess"* debe tener configurado la mayor seguridad posible que se verá posteriormente.

**Figura 3.12.** Políticas de una SD-WAN (Sede Principal)

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

Fuente: (López, 2020)

### 3.4.3 Selección del mejor camino usando reglas de la SDWAN

A diferencia de la SD-WAN de Viptela, la selección dinámica de la mejor ruta en FORTINET se realiza a través del uso de reglas (no utiliza OMP) que permiten realizar la toma de decisiones de enrutamiento de manera automática basada en parámetros como latencia, ancho de banda, pérdida de paquetes, etc. Estas reglas son las que proporcionan inteligencia a la red, por lo que cumplen un papel importante en la SD-WAN al ser una característica fundamental del concepto de esta de solución (López, 2020).

En la Figura 3.13. se puede visualizar un ejemplo de las reglas definidas en una SD-WAN de FORTINET basada en la arquitectura mencionada anteriormente de una sede principal, centro de datos y una sucursal, para este caso se muestran las reglas de la sede principal.

**Figura 3.13.** Reglas de la Sede Principal de la SD-WAN

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

Fuente: (López, 2020)

Es importante explicar una de estas reglas para comprender claramente su funcionamiento, en primer lugar, al igual que en las políticas mantienen prioridad en el orden de ejecución de arriba hacia abajo.

Por ejemplo, la regla *"To-DC"* indica que el tráfico que sale de la sede principal y la sucursal hacia el centro de datos puede tomar cualquiera de las rutas disponibles ya sea el túnel *ToDC* o la de *MPLS*, esta elección la realiza la SD-WAN de manera automática basado en el parámetro configurado de *latencia*. La regla *"To-BO"* funciona de manera similar, sin embargo, la regla *"InternetAccess"* se diferencia por el parámetro SLA que hace referencia a un *Service-level Agreement* de tal manera que si este no se cumple en algún enlace ocupa cualquiera de los otros enlaces SD-WAN (WAN1, WAN2, WAN3) que mantenga un mejor SLA, adicional se puede configurar un balanceo de carga en caso de que exista una sobrecarga de tráfico sobre uno o dos enlaces. Es así como están funcionando las reglas de la SD-WAN que realizan los cambios en tiempo real de cada una de las rutas hacia la mejor basada en los parámetros mencionados, cabe recalcar que estos cambios no afectan o son imperceptibles para el usuario final, demostrando así la inteligencia de la SD-WAN.

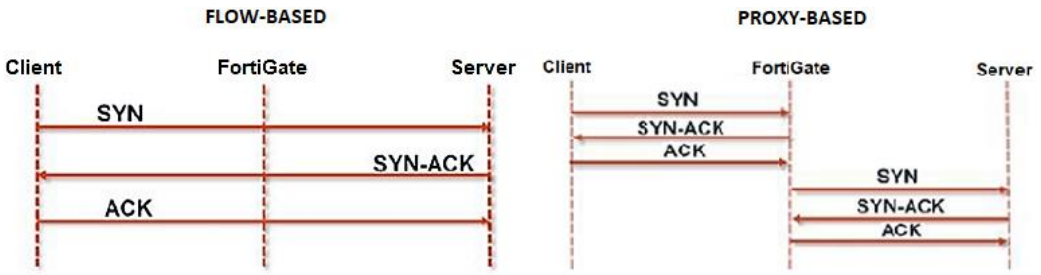
### 3.4.4 Seguridad de la SD-WAN

La seguridad en la SD-WAN como se mencionó anteriormente es de gran importancia. Por tal motivo, el fabricante FORTINET despliega un nivel bastante avanzado y profundo de seguridad, ya que es una empresa que ha logrado posicionarse como una de las mejores en temas de seguridad de redes y datos. Sin embargo, ahora también se está abriendo caminos al área de *networking*, un ejemplo de ello es la SD-WAN y los diferentes equipos a nivel LAN como FortiSwitch, APs, etc.

Secure SD-WAN de FORTINET es una solución que incorpora las funcionalidades de SD-WAN junto con la seguridad *Next Generation Firewall* (NGFW), por no decir la única (Fortinet, 2021). Permite desplegar diferentes perfiles o políticas de seguridad como se detalla a continuación, sin embargo, al igual que con Viptela para la mayoría de ellos es indispensable el uso de un certificado propio del fabricante (viene por defecto en el equipo) o alguno externo (Docs.fortinet.com, 2020).

- **Inspección de Tráfico:** ofrece dos tipos de inspección de tráfico, una basada en flujo y otra basada en proxy. La primera ofrece un mejor rendimiento y menores tiempos de respuesta ya que los paquetes son inspeccionados a medida que pasan por el FortiGate, mientras que el segundo tiene un análisis más profundo en un buffer temporal ofreciendo mayor seguridad y protección contra amenazas (Docs.fortinet.com, 2020). Por defecto es configurado basado en flujo, esto ya depende del modelo de negocio o del administrador de la red. En la Figura 3.14. se visualiza un esquema del funcionamiento de cada uno de estos flujos.

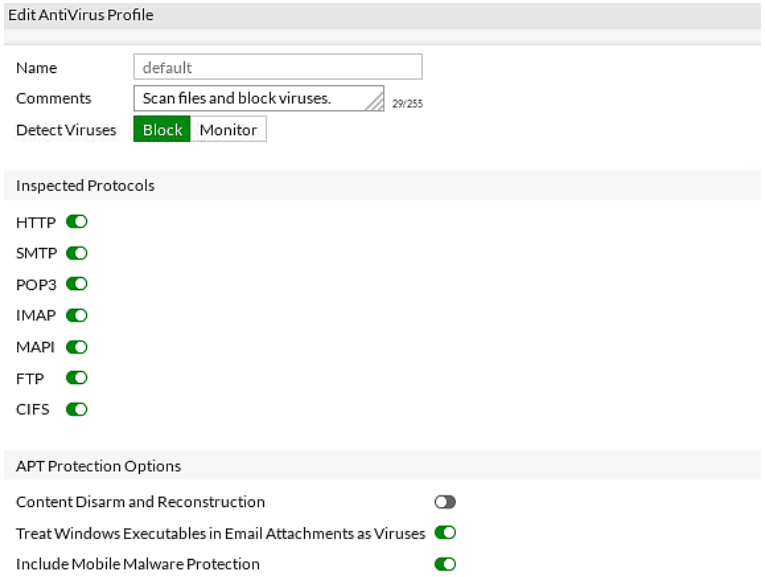
**Figura 3.14.** Tipos de Inspección de FortiGate.




Fuente: (Docs.fortinet.com, 2020)

- **Antivirus:** este perfil se encarga de bloquear o monitorear virus, protocolos sospechosos y malwares a nivel WAN, este tipo de seguridad no reemplaza el virus de computadoras de la LAN, sino que las complementa. En la Figura 3.15. se visualiza un ejemplo de una política de Antivirus, la cual se encarga de bloquear todo tipo de malware y virus e inspeccionar los protocolos como SMTP, POP3, FTP, etc.

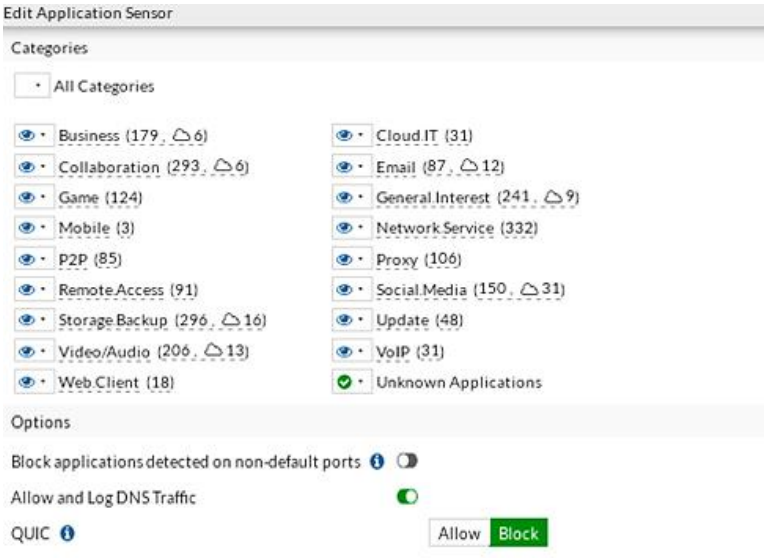
**Figura 3.15.** Política de seguridad de Antivirus




Fuente: (López, 2020)

- **Control de aplicaciones:** como su nombre lo indica se encarga de monitorear, bloquear o permitir el tráfico de aplicaciones definidas por el ingeniero de red. Puede definirse sobre aplicaciones puntuales o a su vez por categorías. En la Figura 3.16. se muestra un ejemplo de una política de control de aplicaciones, en la que se bloquea aplicaciones desconocidas y se monitorea todo el resto de las categorías como acceso remoto, redes sociales, VoIP, etc.

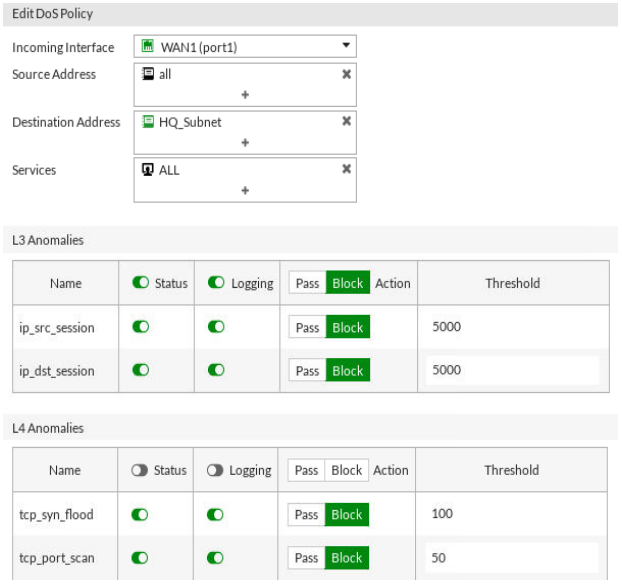
**Figura 3.16.** Política de Control de Aplicaciones




Fuente: (López, 2020)

- **Sistema de Prevención de Intrusos (IPS):** evita los ataques más comunes de Internet, así como las conexiones a sitios Botnet. También permite controlar los ataques de Denegación de Servicios (DoS) que saturan los recursos de los equipos con peticiones falsas. En la Figura 3.17. por ejemplo, se visualiza una política de DoS sobre todo el tráfico de entrada a la sede principal, de tal manera que se configura los umbrales máximos de sesiones a nivel de capa 3 y 4.

**Figura 3.17.** Política de DoS



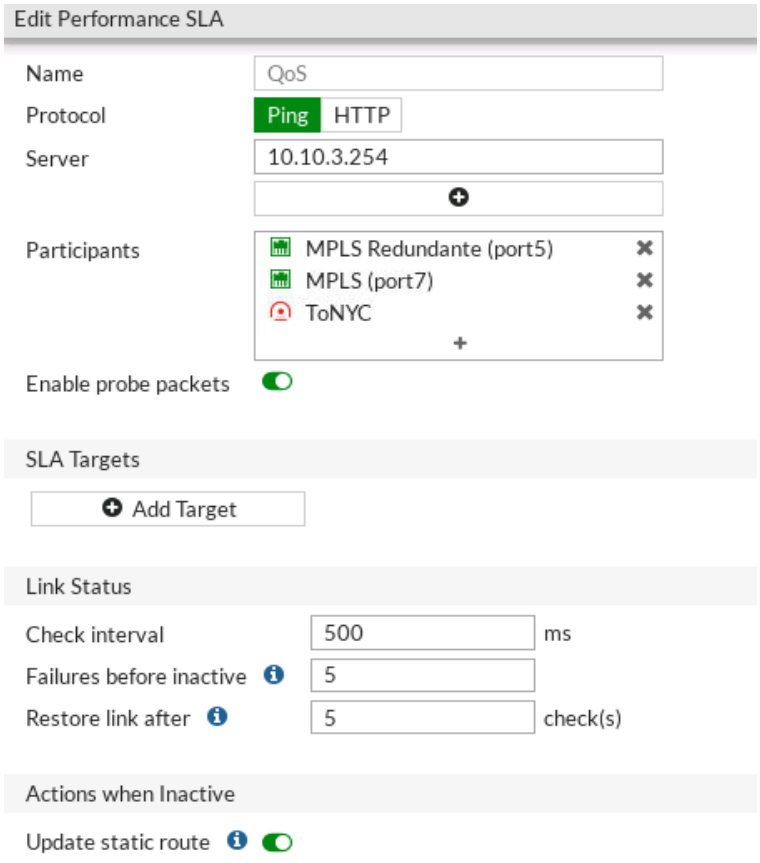

Fuente: (López, 2020)

- **Firewall de aplicaciones web:** esta política es la encargada de proteger a los servidores que ejecutan aplicaciones web como el servidor de correo, banner, biblioteca, etc. que generalmente se encuentran dentro del centro de datos.
- **Filtro web, DNS y de e-mail:** como su nombre lo indica se encarga del filtrado de paquetes a nivel de DNS, e-mail y web.
- **Grupos de aplicación:** es un tipo de control que permite limitar el uso del ancho de banda. Funciona para definir grupos VIP y establecer diferentes usos de ancho de banda.

### 3.4.5 Monitoreo y Análisis (FortiAnalyzer)

La GUI de monitoreo de este fabricante es bastante amigable con el usuario y está relacionado estrechamente con la Calidad de Servicio (QoS). Permite realizar la supervisión de los enlaces que forman la SD-WAN a través de señales de sondeo enviadas a un servidor en el destino. Para entender mejor su funcionamiento en la Figura 3.18. se visualiza que el protocolo para sondear los paquetes es a través de PING, es necesario configurar la IP de un servidor en el destino y a su vez los enlaces que se desea monitorear basado en los siguientes parámetros de QoS: intervalo de revisión, número de paquetes o sesiones fallidas antes de declarar los enlaces inhabilitados, número de paquetes o sesiones fallidas antes de declarar los enlaces habilitados. Una vez configurados en la Figura 3.19. se muestran todas las rutas a monitorear con diferentes destinos de tal manera que la flecha roja muestra que el tráfico no está pasando por ese enlace sino porque el que muestra una flecha verde hacia arriba.

**Figura 3.18.** Configuración de monitoreo de enlaces




Fuente: (López, 2020)

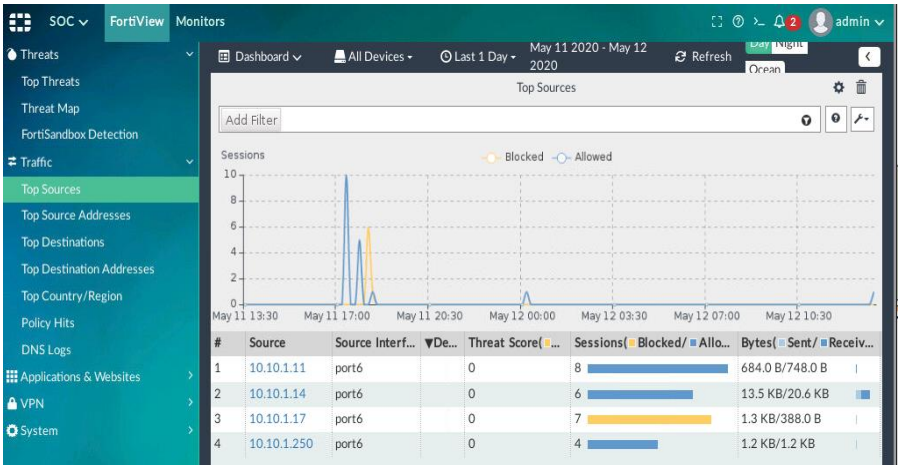
**Figura 3.19.** Enlaces monitoreados

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

Fuente: (López, 2020)

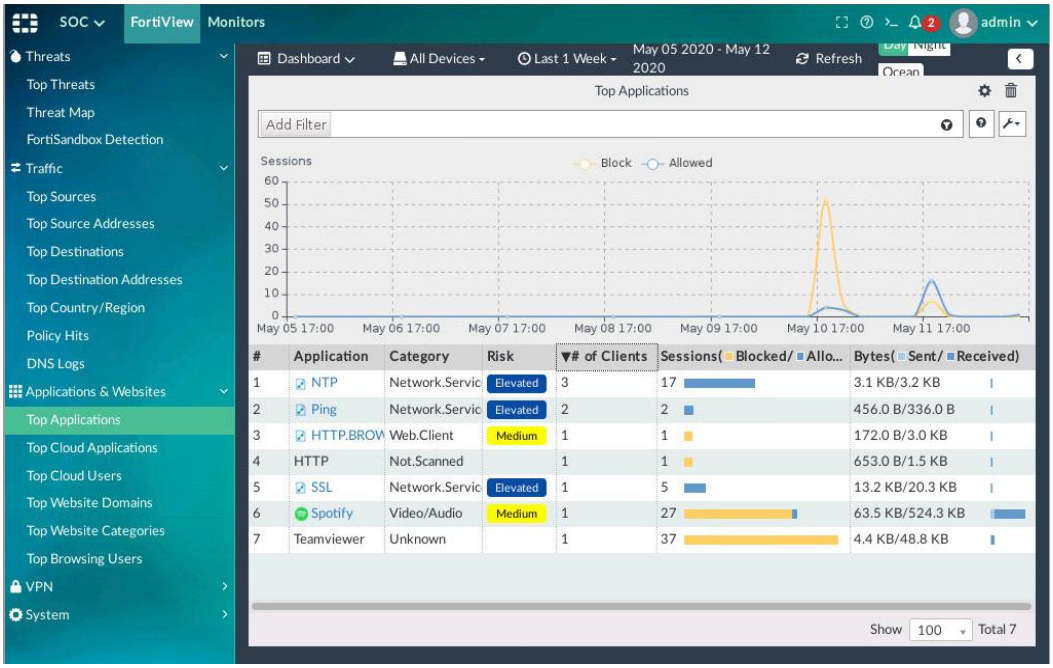
Es importante mencionar que adicional a este monitoreo están disponibles todas las funcionalidades de análisis más profundo que ofrece el equipo FortiAnalyzer, este puede funcionar de manera independiente o a su vez dentro del propio equipo de control y Administración FortiManager, en casos de que se necesite gran cantidad de recursos para análisis, reportería y generación de informes (automático) se recomienda utilizar los equipos independientes. En esta emulación ya desarrollada funciona dentro de FortiManager. Por ejemplo, en la Figura 3.20, 3.21 y 3.22 se muestra un ejemplo de la ejecución de los diferentes tipos de análisis como: tráfico, aplicaciones, logs de autenticación, etc., de los cuales se subdividen varios niveles y opciones de monitoreo de estas categorías.

**Figura 3.20.** Análisis del tráfico



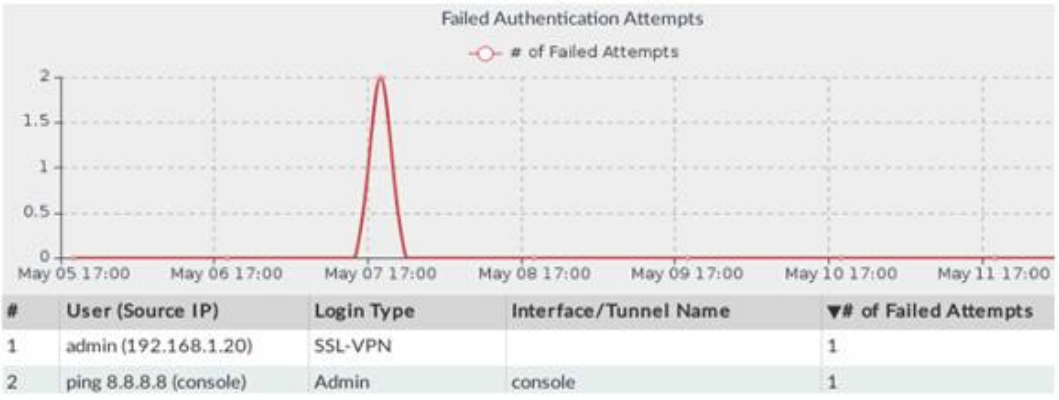

Fuente: (López, 2020)

**Figura 3.21.** Análisis de aplicaciones




Fuente: (López, 2020)

**Figura 3.22.** Análisis de Autenticación



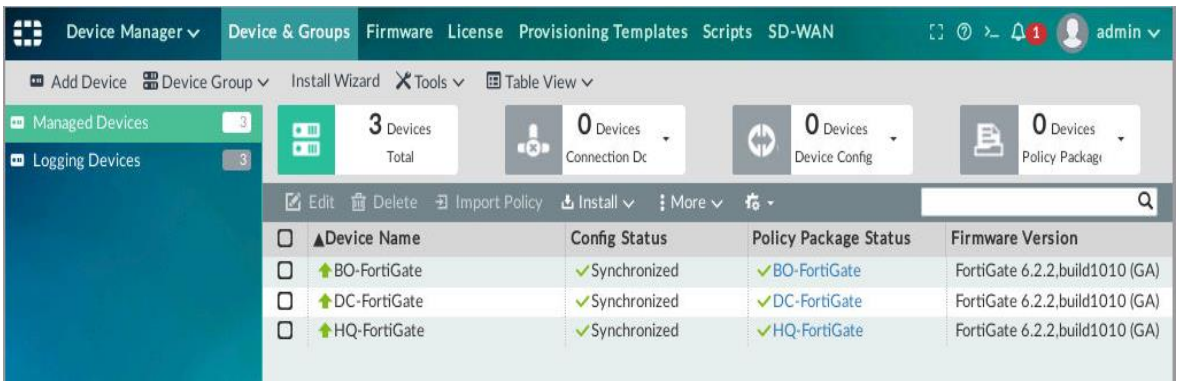

Fuente: (López, 2020)

### 3.4.6 Control y Administración de la SD-WAN (FortiManager)

En el caso de Secure SD-WAN de FORTINET el control y administración se realiza desde el equipo FortiManager, de tal manera que este es el encargado de desplegar políticas, reglas, VPNs de manera centralizada hacia cualquier sucursal u centro de datos ya que para la emulación que se está analizando este equipo de control se encuentra en la sede principal. Al igual que la SD-WAN de Cisco permite la creación de *templates* para configurar políticas e implementarlas en nuevas sucursales auotmaiticament4e a través de la funcionalidad ZTP. Se puede decir que es el cerebro de la SD-WAN en un único dispositivo (en Cisco es vSmart y vManage) tanto para el control e inclusive el análisis en caso de que se utilice FortiAnalyzer en el mismo equipo como se mencionó con anterioridad.

En la Figura 3.23. por ejemplo, se puede visualizar la GUI de administración de FortiManager una vez agregados los FortiGates de la sede principal (HQ), centro de datos (DC) y sucursal (BO), desde ese panel se tiene diferentes funcionalidades que se despliegan en los equipos específicos o en todos.

**Figura 3.23.** Centro de Control y Administración FortiManager

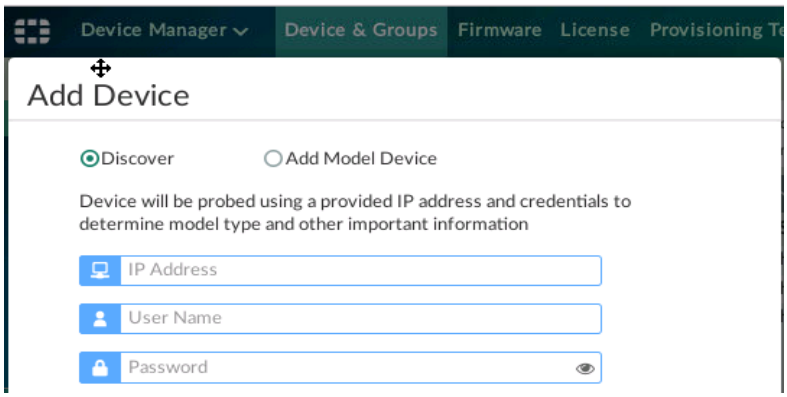



Fuente: (López, 2020)

#### 3.4.6.1 Conexión de FortiGates a FortiManager en la Secure SD-WAN

En este caso el proceso de agregación de los equipos de borde al controlador FortiManager es sencillo, ya que se lo realizar agregando el modelo y serial del dispositivo o a su vez el mismo FortiManager descubre los dispositivos de borde y los agrega a través de la IP, el usuario y contraseña como se muestra en la Figura 3.24.

**Figura 3.24.** Conexión de FortiManager con FortiGates




Fuente: (López, 2020)

# 4 ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Una vez analizado el concepto de SD-WAN, SD-WAN Híbrida y todos los subtemas que este conlleva de manera teórica, fue menester detallar su funcionamiento de manera práctica a través de emulaciones ya realizadas para entender y relacionar todas estas características de la SD-WAN, inclusive se utilizó dos fabricantes diferentes que tienen buenas referencias respecto a esta solución.

De esta manera, en este último capítulo se procede al debate de los resultados, ventajas, desafíos que cada uno de los fabricantes ofrece para así establecer una comparativa entre ellos, con el fin de visualizar la factibilidad de su configuración como infraestructura *overlay* en las empresas, tomando en cuenta que cada una puede ser mejor dependiendo del modelo de negocio.

A continuación, se establece una comparación de cada funcionalidad en común entre los fabricantes estudiados anteriormente y a su vez aquellas que no las tiene el uno u otro fabricante para saber cuál de estas soluciones genera menor impacto en caso de no tener una de estas.

## 4.1 Multi-Transporte

Una característica primordial de SD-WAN es la de controlar o permitir múltiples rutas de transporte a nivel WAN, en este caso ambos fabricantes tanto CISCO como FORTINET permiten utilizar ya sea los enlaces de la SD-WAN, túneles IPsec o a su vez la infraestructura MPLS existente en caso de ser una SD-WAN Híbrida. Esto se puede comprobar a través de un ping desde la sede a cualquier sucursal y simular una caída de cualquiera de los enlaces y visualizar que el tráfico utiliza otra red de transporte como MPLS, LTE. etc. Esta funcionalidad únicamente se difiere en la interfaz gráfica de usuario en cada fabricante, sin embargo, dentro del análisis de factibilidad de implementación de SD-WAN como configuración *overlay* en una organización.

## 4.2 Selección dinámica de ruta

Esta característica como se detalló anteriormente de igual forma se cumple en los dos fabricantes, sin embargo, aquí si difieren en su funcionamiento, por ejemplo, CISCO utiliza OMP para realizar este proceso mientras que FORTINET lo realiza a través de reglas que funcionan en conjunto con las políticas. Por este motivo, esta funcionalidad es un segundo detonante para optar por una SD-WAN, cabe mencionar que desde el punto de vista del autor de esta tesis la GUI de esta funcionalidad es más amigable la de FORTINET que la de CISCO.

## 4.3 Seguridad de la SD-WAN

Respecto a la seguridad si existe cierta diferencia entre el uno y otro fabricante, en este caso FORTINET toma la delantera por el hecho de que su potencial como empresa está radicado en seguridad de redes, es decir ya mantenían un mercado bastante estable en equipos como *firewalls.* Por este motivo, dispone de más perfiles de seguridad que CISCO como los mencionados en el capítulo anterior, sin embargo, CISCO también mantiene varias políticas indispensables de seguridad. Un plus importante de

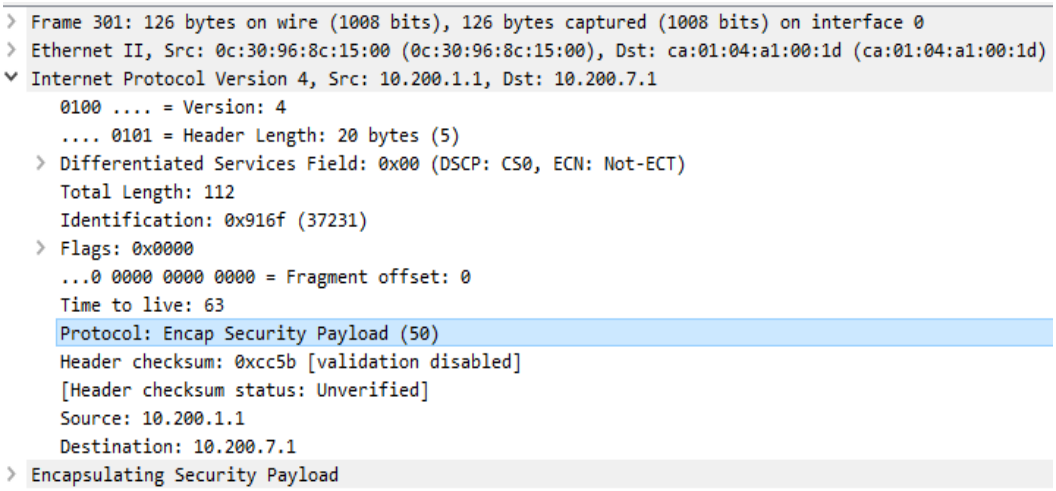
FORTINET en este aspecto es que mantenía tanto la seguridad NGFW como las funcionalidades de SD-WAN en un único dispositivo por lo que la administración y gestión se facilita.

## 4.4 Túneles IPsec

Respecto a los túneles IPsec de la red *overlay* es una funcionalidad que mantienen los dos fabricantes. En este punto no difieren, ya que es parte de la SD-WAN como tal garantizar encriptación y cifrado de los paquetes en la red superpuesta o tunelización para protegerlo de Internet, ya que como se mencionó una ventaja de esta solución es que usa la infraestructura pública de Internet que si bien es cierto abarata costos, aumenta disponibilidad, pero así mismo requiere un protocolo de encapsulación del tráfico al ser expuesto a mayor número de ataques.

Por ejemplo, en la Figura 3.25. se puede visualizar el protocolo de encapsulación de seguridad del tráfico (ESP) que corrobora la seguridad de IPsec, encargado de cifrar y proteger el tráfico. Esta es una captura de paquetes realizada a través de wireshark de una emulación SD-WAN con túneles IPsec.

**Figura 4.1.** Comprobación del protocolo IPsec a través de Wireshark




Fuente: (López, 2020)

Es importante mencionar que FORTINET para el acceso remoto ofrece también una VPN tipo *Secure Socket Layer* (SSL), que ofrece mayor facilidad al usuario final de acceso (configuración) a través de la VPN a los servicios de la sede principal a diferencia de la VPN IPsec que requiere un conocimiento mayor para que el usuario final pueda configurarlo.

## 4.5 Monitoreo y Análisis

Esta funcionalidad presenta bastante similitud entre los dos fabricantes, inclusive el monitoreo y análisis tanto en CISCO como FORTINET se lo puede realizar a través del dispositivo de administración, ya sea vManage o FortiManager respectivamente. Esta es una gran ventaja ya que permite monitorear la QoS de los enlaces para que en función de eso se realice la selección dinámica de ruta. Adicional, presentan una GUI bastante amigable para realizar el análisis exhaustivo de cada uno de los eventos, logs, amenazas, etc., lo que facilita la detección y prevención de varias amenazas. Se puede decir que la única diferencia es que en el caso de FORTINET debido a que presenta mayores seguridades por el

NGFW, se puede analizar más aspectos o perfiles de seguridad configurados en la SD-WAN.

## 4.6 Control Centralizado

El control centralizado, así como funciones ZTP, *templates*, etc. está presente en los dos fabricantes, pero si difiere en lo siguiente, por ejemplo, CISCO maneja dos dispositivos para el control y administración de la red, como vSmart que es el cerebro de la red y vManage que es el dispositivo que interactúa directamente con el usuario para la gestión centralizada, por su parte en FORTINET el cerebro y dispositivo de administración está en un único dispositivo llamado vManage. Es importante recalcar este aspecto ya que desde mi punto de vista tener todo en un único dispositivo facilita la comprensión del funcionamiento y administración de la red, por el contrario, CISCO necesita configuraciones adicionales y mayor investigación sobre el funcionamiento de vSmart para su implementación. Sin embargo, esta funcionalidad es primordial para dar el paso hacia la SD-WAN dentro de una organización por todos los aspectos mencionados anteriormente.

## 4.7 Reducción de Costos

El ahorro de costos es un punto bastante considerable que la SD-WAN tiene a su favor y que es de hecho muy decisivo para la mayoría de las organizaciones. En este caso, no se puede definir un valor exacto tanto del uno como del otro fabricante ya que el costo de los equipos va variando de acuerdo con los escenarios existentes, es decir mientras son organizaciones de mayor escala, mayor número de sucursales o mayor número de licencias, el valor se va incrementando. De este modo, se puede entender que CISCO y FORTINET son soluciones que no van a tener gran variación en el costo, sin embargo, lo realmente importante es el ahorro que representa esta solución respecto a otras soluciones WAN existentes que aproximadamente es de un 35% al utilizar la infraestructura pública de Internet, sin afectación a su rendimiento.

## 4.8 Comparativa de SD-WAN Viptela de CISCO vs SDWAN FORTINET

**Tabla 4.1.** Comparación de CISCO vs FORTINET (SD-WAN)

| | **CISCO VIPTELA** | **FORTINET** |
|---|---|---|
| **Multi-Transporte** | SI | SI |
| **Selección Dinámica de Ruta** | SI | SI |
| **Application Specific Integrated Circuit (ASIC)** | NO | SI |
| **NGFW** | SI | SI |
| **IPsec y SSL** | SI | SI |
| **Disponibilidad Multiplataforma** | SI | SI |
| **Administración y Gestión** | SI | SI |

| | | |
|---|---|---|
| **Centralizada** | | |
| **SD-Access/SD-Branch Segura** | SI | SI |
| **Self Healing (Auto-recuperación)** | SI | SI |
| **Costo (TCO por Mbps protegido)** | Desconocido | $4 |

Fuente: (Fortinet, 2021)

## 4.9 Escenarios de Implementación

Posteriormente a los resultados, se puede definir a las dos soluciones como válidas para su implementación en varias organizaciones, ya que ofrecen varios beneficios. Sin embargo, tanto la una como la otra va a ser la solución más adecuada dependiendo del escenario o modelo de negocio. Por esta razón, se menciona ciertos ejemplos de los escenarios para los cuales es más eficiente usar FORTINET y para cuales CISCO.

### 4.9.1 Escenario I

Es lógico que un escenario adecuado para usar ya sea FORTINET o CISCO va a depender mucho del fabricante ya existente en la organización, por ejemplo, si en la red tienen equipos como switches, Access Points, Firewall y otros equipos de red de la marca CISCO, obviamente es más adecuado optar por la solución de Viptela, ya que se puede aprovechar de mejor manera la compatibilidad y funcionalidad de todos los equipos en conjunto. Lo mismo ocurre si se tiene FortiSwitch, FortiAPs, FortiGates, etc., van a funcionar de manera más eficiente que al mezclar equipos de distintas marcas.

### 4.9.2 Escenario II

Este escenario es un tanto subjetivo ya que depende mucho del punto de vista de cada uno. Pero acorde a la tesis desarrollada en el caso de que la organización tenga un enfoque bastante avanzado en el área de *routing & switching* puede ser más adecuado utilizar la solución de Viptela tomando en cuenta que tienen mayor liderazgo en ese aspecto según el cuadrante de Gartner. Esto desde el punto de vista del autor.

### 4.9.3 Escenario III

De igual manera es subjetivo este escenario, pero en el caso de que la organización maneje una data bastante critica, confidencial o transaccional, es decir requiera un alto nivel de seguridad es recomendable o adecuado utilizar la solución Secure SD-WAN de FORTINET, tomando en cuenta que estos son líderes en el aspecto de seguridad de redes según el cuadrante de Gartner. Esto desde el punto de vista del autor.

# 5 PRESENTACIÓN DE LA PROPUESTA

## 5.1 Análisis de factibilidad

Basado en la teoría, funcionamiento y resultados se puede emitir con mayor certeza un criterio respecto a la factibilidad de configuración de la SD-WAN como infraestructura overlay de una organización. Por lo tanto, se deduce que es bastante recomendable la implementación de esta solución en diferentes organizaciones en el Ecuador por todas las ventajas que ofrece, además de reducir costos sin afectar el rendimiento de la red, al contrario, la vuelve más eficiente.

## 5.2 Propuesta de implementación

De esta manera, se presenta la propuesta de la implementación de la Secure SD-WAN de FORTINET en la PUCE y sus sedes, tomando en cuenta que se tienen los equipos FortiGate y FortiAnalyzer con las funcionalidades de SD-WAN (equipos actuales) en PUCE Matriz, con el objetivo de tener una red más inteligente y eficiente. Es importante mencionar que no es un escenario de los detallados anteriormente, ya que en este caso se cuenta con una de LAN y WLAN con equipos de marca CISCO en la PUCE Matriz, sin embargo, por temas de seguridad se tiene NGFW del fabricante FORTINET, es por esto que se tiene un nuevo escenario en el cual se aprovecha el potencial de cada uno de los fabricantes (*routing & switching de cisco y seguridad de fortinet*). Como desafío se espera corroborar la compatibilidad de funciones entre equipos de estos fabricantes, los cuales serán verificados a futuro con la implementación de esta solución y adquisición del equipo faltante FortiManager.

# CONCLUSIONES Y RECOMENDACIONES

Finalmente, se presentan las conclusiones y recomendaciones del trabajo de titulación acorde al análisis y discusión de los resultados obtenidos.

## Conclusiones

La parte conceptual o teórica descrita en el segundo capítulo del presente proyecto de titulación permite aclarar o comprender de mejor manera las nuevas tecnologías definidas por *software*, tanto a nivel LAN como WAN, de tal manera que este conocimiento previo aporta sustancialmente para el análisis del funcionamiento de la SD-WAN detallado en el capítulo tres a través de dos fabricantes líderes en el mercado respecto a esta solución.

El desarrollo teórico-práctico de la SD-WAN permite entender de manera implícita el concepto y funcionamiento de las SDN ya que estas son el punto inicial que dio lugar a la SD-WAN, es así como el presente trabajo permite identificar las características más representativas y análogas de estas soluciones como la separación del plano de control con el plano de datos y que las dos utilizan un controlador como cerebro de la red para la toma automática e inteligente de decisiones de enrutamiento, seguridad, monitoreo, etc. en la red.

Tomando en cuenta que se puede tener soluciones SD-WAN, así como SD-WAN Híbrida, el presente trabajo de titulación permite analizar la opción de mantener la infraestructura MPLS y combinarla con las funcionalidades de SD-WAN ya que se optimiza el rendimiento de la red, de acuerdo con el escenario al que se lo aplique. Por ejemplo, un escenario adecuado para combinar estas dos tecnologías es al tener políticas que manejen el tráfico de alta confidencialidad a través de la red MPLS, mientras que el tráfico común o de *streaming* a través de los enlaces SD-WAN, con el objetivo de eliminar las latencias ocasionadas por el tráfico de *backhaul* de MPLS, el cual en caso de *streaming*, actualizaciones, entre otros tipos de tráfico no es necesario. Una implementación de este tipo es la del banco de Guayaquil, ya que maneja su data crítica o confidencial utilizando MPLS y granula el tráfico restante a través de la SD-WAN. Por lo tanto, el presente proyecto de titulación aclara y corrobora la ventaja de ser multi-transporte por medio de los distintos conceptos teórico-prácticos y ejemplos revisados a lo largo del desarrollo de esta tesis, es importante recalcar que esta funcionalidad se cumple en ambos fabricantes.

El presente proyecto de titulación de manera implícita permite aprender conocimientos sobre seguridad de redes, tomando en cuenta que uno de los desafíos de la SD-WAN es garantizar la seguridad ya que

utiliza la infraestructura pública de Internet para la transmisión de datos. De este modo, es menester conocer los diferentes perfiles de seguridad que ofrece cada uno de los fabricantes como CISCO y FORTINET, lo cual se visualizó durante el desarrollo de este trabajo. Por ejemplo, IPS, control de aplicaciones, IPsec, DoS, etc. son algunas de las políticas que se definieron en capítulos anteriores de manera teórica y práctica, permitiendo así al maestrante a conocer a profundidad cada una de ellas y la importancia que este tema se merece actualmente.

Durante el análisis del funcionamiento de la SD-WAN tanto de CISCO como FORTINET, se identificaron y validaron cada una de las ventajas que incentivan hacia la configuración de la SD-WAN como infraestructura overlay, cabe mencionar algunas de ellas como: control centralizado, ZTP, multi-transporte, NGFW e IPsec, selección dinámica de ruta, gestión y administración desde un único panel, etc. Todas estas características se validaron en las soluciones de los dos fabricantes, de tal manera que se puede concluir que cualquiera de estas opciones es válida para su implementación, sin embargo cabe recalcar que existe escenarios más adecuados para cada una de ellas, como se mencionó a lo largo del desarrollo del trabajo.

El análisis de una característica importante como control centralizado y ZTP, permite concluir que la SD-WAN reduce considerablemente los tiempos de implementación en comparación a tecnologías WAN tradicionales, inclusive MPLS ya que se puede desplegar nuevas sucursales en cuestión de horas y sin la necesidad de un ingeniero de redes en el sitio, tomando en cuenta que la GUI de administración es bastante amigable y se la puede realizar desde el controlador ubicado en la sede principal. Adicionalmente, hay que mencionar que la SD-WAN permite la ejecución de plantillas o *templates* para que la configuración se vuelva más sencilla y rápida, esto desde ambos fabricantes.

Se concluye adicionalmente que las herramientas de análisis que ofrece la SD-WAN tanto de CISCO como FORTINET dentro del plano de control son bastante eficaces respecto al análisis de tráfico, eventos, y seguridad en contra de cualquier tipo de ataque, de tal manera que es un gran apoyo para el administrador de red, inclusive su GUI permite ser inteligible para usuarios que no tienen el mismo conocimiento que un ingeniero de redes (gerentes, directores, jefes), de tal manera que facilita el seguimiento de riesgos y auditorías de seguridad, en caso de que se llegue a términos legales por algún ataque de piratas informáticos.

La comparativa realizada entre estos dos fabricantes no presentan mayores diferencias, al contrario, se concluye que las dos opciones son factibles, sin embargo, la presente tesis permite identificar que en cuestión de seguridad únicamente FORTINET presenta ciertas ventajas por el mismo hecho de que su potencial está radicado en ese mercado, ya que las funcionalidades de SD-WAN y NGFW están combinadas en un mismo equipo. Por otra parte, CISCO presenta ciertas ventajas en cuestiones de

compatibilidad de *routing & switching* ya que su mercado es fuerte en cuestión de equipos como *routers, switches, APs*, por lo que presentaría mayor compatibilidad en caso de implementar una SD-LAN y SD-WAN dentro de una organización.

El desarrollo del presente trabajo de titulación permite determinar que la SD-WAN representa un ahorro económico en aspectos como: costos de operación (OPEX) ya que facilita el despliegue y control de nuevas sucursales a través de las funcionalidades mencionadas anteriormente (ZTP), costos de capital (CAPEX) ya que combina varias funcionalidades en un único dispositivo (esta funcionalidad especialmente en FORTINET) y costos respecto al ancho de banda ya que resulta más conveniente modificar los planes de suscripción con los ISP que implementar un nuevo enlace MPLS.

Finalmente, este proyecto permite concluir que es factible la configuración de SD-WAN como infraestructura *overlay* dentro de una organización ya sea manteniendo la infraestructura existente (MPLS) o a su vez implementando una SD-WAN por completo. Por lo tanto, la tesis permite determinar que es bastante viable la propuesta de implementación de la SD-WAN en la PUCE y sus sedes ya que permite obtener un ahorro de costos sin afectación del rendimiento de la red, más bien se tiene como resultado una red más inteligente y eficiente.

## Recomendaciones

Se recomienda investigar sobre las soluciones de *Software Defined Data Center* (SD-DC), SD-LAN y SD-WLAN para analizar la factibilidad de configuración dentro de la Sede Principal de la PUCE con el objetivo de implementar una solución integral definida por software y obtener una red más inteligente tanto a nivel LAN como WAN.

Se recomienda analizar el funcionamiento de la SD-WAN de VMware y compararla con las soluciones de los fabricantes detallados a lo largo de este proyecto de titulación por dos razones importantes: una de ellas es porque se encuentra también como líder en el cuadrante de Gartner y la segunda porque dentro del Centro de Datos se tiene equipos de la marca VMware (VxBlock System) de tal manera que puede ofrecer grandes ventajas su implementación combinada con una SD-DC del mismo fabricante.

Se recomienda emular estas soluciones desde el software GNS3 y EVE-NG para que sirva como material de apoyo para estudiantes de pregrado, ya que actualmente la SD-WAN es una tecnología cuasi nueva pero necesaria dentro del pensum académico de los futuros ingenieros que se dediquen al área de redes e infraestructura.

Finalmente, se recomienda investigar sobre nuevas soluciones que nacen a partir de las redes definidas por software como SASE o a su vez a partir de la virtualización, con el fin de proponer una migración completa de equipos físicos del centro de datos de la PUCE hacia la nube, de tal manera que en caso de alguna catástrofe física la información, equipos y funcionamiento no se vea afectado.

# REFERENCIAS


1. ITSitio. (2022). *Por qué vale la pena migrar de un modelo MPLS tradicional a SD-WAN.* Obtenido de: https://www.itsitio.com/ec/por-que-vale-la-pena-migrar-de-un-modelo-mpls-tradicional-a-sd-wan/#:~:text=SD%2DWAN%20est%C3%A1%20cambiando%20radicalmente,esenciales%20en%20su%20estrategia%20comercial.

2. Wang, D. (2019), *Software Defined-WAN for the Digital Age, 1st ed.* New York: CRC Press.

3. Steve, A. (2020). *"How SD-WAN Facilitates WAN Security | SD Wan Experts", SD Wan Experts*. Obtenido de: https://www.sd-wan-experts.com/blog/sd-wans-make-wan-security-possible/.

4. ExterNetworks. (2020). *"SD-WAN vs. Traditional WAN"*. Obtenido de: https://www.extnoc.com/sd-wan/sd-wan-vs-traditional-wan/.

5. Bhardwaj, R. (2022). *SD WAN vs TRADITIONAL WAN - IP*. Obtenido de: https://ipwithease.com/sd-wan-vs-traditional-wan/

6. Burwood Group. (2020). *Traditional WAN vs. SD-WAN: Here's What You Need to Know*. Obtenido de: https://www.burwood.com/blog-archive/traditional-wan-vs-sd-wan-heres-what-you-need-to-know.

7. VMware. (2020). *Traditional WAN vs SD-WAN*. Obtenido de: https://www.vmware.com/latam/solutions/sd-wan-traditional-wan.html.

8. TechClub Tajamar. (2022). *Conexión WAN - ISDN*. Obtenido de: https://techclub.tajamar.es/conexion-wan-isdn/https://techclub.tajamar.es/conexion-wan-isdn/

9. Hidalgo, P. (2016). *MULTIPROTOCOL LABEL SWITCHING (MPLS)*. Quito, Ecuador.

10. Pandya, A. (2020). *MULTIPROTOCOL LABEL SWITCHING (MPLS) QUICK REFERENCE GUIDE*. Obtenido de: https://theunprecedentedcult.in/articles/technology/multiprotocol-label-switching/

11. Projekter. (2020). *Analysis of Software-Defined Wide-Area Networking*. Obtenido de: https://projekter.aau.dk/projekter/files/281292955/Masters_thesis_Mario_Todorov.pdf.

12. Bibdigital. (2020). *Implementación de un prototipo de una SDN empleando una solución basada en Hardware.* Obtenido de: https://bibdigital.epn.edu.ec/bitstream/15000/6681/1/CD-5065.pdf.

13. SDXcentral. (2022). *SDN Architecture*. Obtenido de: https://www.sdxcentral.com/sdn/definitions/inside sdn architecture/

14. Salazar-Chacón, G. D., & Marrone, L. (2020, November). OpenSDN Southbound Traffic Characterization: Proof-of-Concept Virtualized SDN-Infrastructure. In *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0282-0287). IEEE.

15. SearchNetworking, (2020). *What is Software-Defined Networking (SDN)*. Obtenido de: https://searchnetworking.techtarget.com/definition/software-defined-networking-SDN.

16. Repositorio.ug.edu.ec. (2020). *Diseño e implementación de un prototipo SD-WAN basado en raspberry PI.* Obtenido de: https://repositorio.ug.edu.ec/bitstream/redug/45274/1/B-CINT-PTG-N.472%20Nazareno%20Arroyo%20Steven%20Edwing.pdf.

17. Salazar, G. (2020). Introducción a SDN. Quito, Ecuador, 2022.

18. Ch, G. D. S., Naranjo, E. F., & Marrone, L. (2018, November). SDN-Ready WAN networks: Segment Routing in MPLS-Based Environments. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 173-178). IEEE.

19. Scss.tcd.ie. (2020). *Software-Defined Networking: Current State, Adoption Factors and Future Impact on Network.* Obtenido de: https://www.scss.tcd.ie/publications/theses/diss/2016/TCD-SCSS-DISSERTATION-2016-042.pdf.

20. Gartner. (2018). *IaaS or PaaS: what to choose? Besides the SaaS.* Obtenido de: https://phonemantra.com/iaas-or-paas-what-to-choose-besides-the-saas/

21. SDXcentral. (2022). *SD-WAN Defined: What is SD-WAN (Software-Defined Wide Area Network)*. Obtenido de: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/

22. Rfwireless-world.com. (2020). *Difference between SD-WAN and Traditional WAN*. Obtenido de: https://www.rfwireless-world.com/Terminology/Difference-between-SD-WAN-and-Traditional-WAN.html.

23. Salazar-Chacón, G. D., & García, A. R. R. (2021, April). Segment-Routing Analysis: Proof-of-Concept Emulation in IPv4 and IPv6 Service Provider Infrastructures. In 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) (pp. 1-7). IEEE.

24. NetworkAcademy.io. (2021). *What is SD-WAN*. Obtenido de: https://www.networkacademy.io/ccie-enterprise/sdwan/what-is-sd-wan

25. Chacón, G. D. S., & Altamirano, G. X. C. (2015). Empleo de path-control tools en una red empresarial moderna mediante políticas de enrutamiento. 3c Tecnología: glosas de innovación aplicadas a la pyme, 4(1), 1-18.

26. Fortinet. (2021). *Soluciones de SD-WAN | Fortinet*. Obtenido de: https://www.fortinet.com/lat/products/sd-wan.html.

27. Fortixpert.blogspot.com. (2020). *Documentación de Fortinet en Español*. Obtenido de: https://fortixpert.blogspot.com/2015/06/documentacion-de-fortinet-en-espanol.html.

28. Eve-ng.net. (2021). *EVE – The Emulated Virtual Environment for network, security and DevOps Professionals* -. Obtenido de: https://www.eve-ng.net/

29. Salazar Chacón, G. D. (2021). Hybrid Networking SDN y SD-WAN: Interoperabilidad de arquitecturas de redes tradicionales y redes definidas por software en la era de la digitalización (Doctoral dissertation, Universidad Nacional de La Plata).

30. I-Medita.com. (2020). *Cisco-SD-WAN Training Course*. Obtenido de: https://www.youtube.com/watch?v=ZiJnWFoaJe8

31. Rayka-co.com. (2021). *Cisco-SD-WAN Security Policy*. Obtenido de: https://rayka-co.com/lesson/31-cisco-sd-wan-security-policy/

32. Moisa, J. (2019). *Fundamentos de Viptela en Interconexión de vEdge.* Obtenido de: https://community.cisco.com/t5/documentos-routing-y-switching/fundamentos-de-viptela-e-interconexion-de-vedge/ta-p/3898610

33. PyNetLabs. (2021). *Implementación de Cisco SD-WAN Lab: instale vManage, vBond y vSmart en SD-WAN Fabric a través de EVE-NG.* Obtenido de: https://www.youtube.com/watch?v=PDxK2qIL_rQ&t=3936s

34. GNS3.com. (2021). *Getting started with GNS3.* Obtenido de: https://docs.gns3.com/docs/

35. Docs.fortinet.com (2020). *Administration Guide | FortiGate / FortiOS 6.4.0 | Fortinet Documentation Library.* Obtenido de: https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/954635/getting-started

36. Fortinet.com. (2021). *Top 5 SD-WAN Vendoors Solutions and Comparisons.* Obtenido de: https://www.fortinet.com/lat/products/sd-wan-providers

37. Salazar, G. (2016). Fundamentos de QoS-Calidad de Servicio en Capa 2 y Capa 3. *Cisco.*

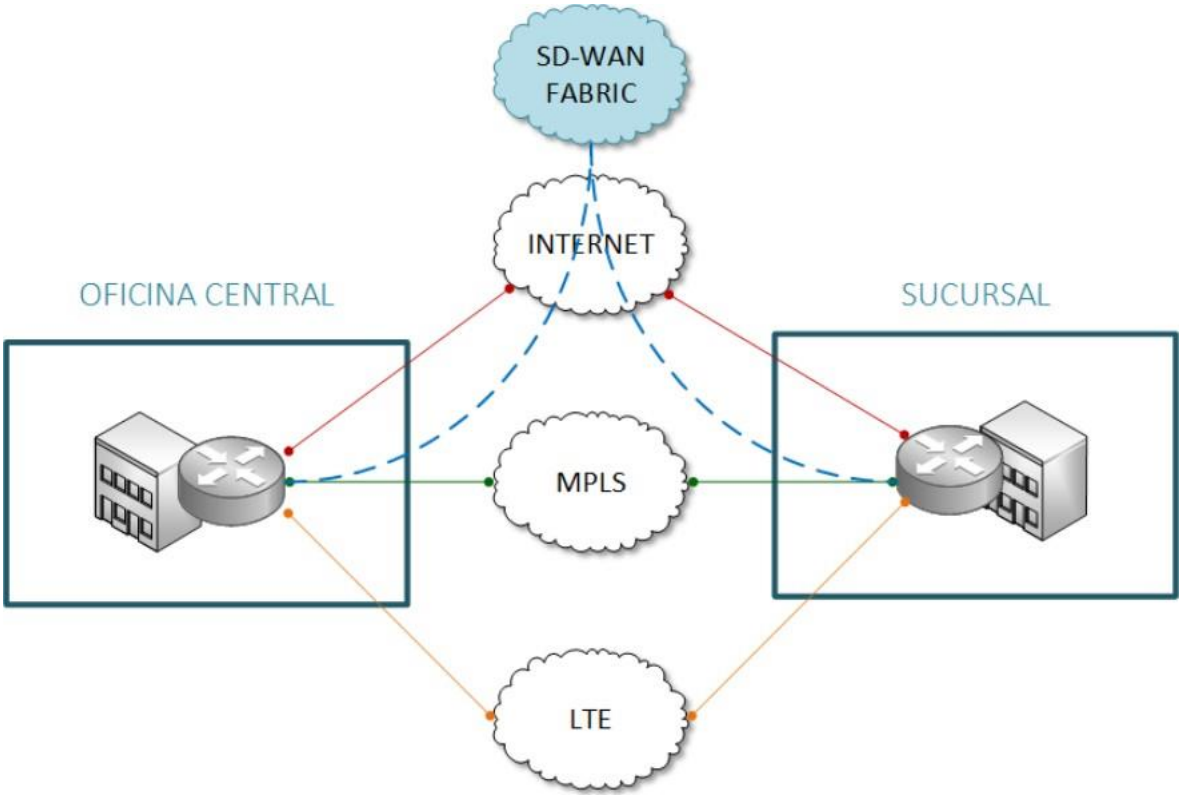
# ANEXOS

## ANEXO A

Realizado por : Julio E. Moisa

CISCO SDWAN VIPTELA – MANUAL INTERCONEXIÓN DE vEDGE

Fundamentos de Viptela e interconexión de vEdge




Hoy en día se habla mucho de la evolución de las redes de datos o de las tendencias en la tecnología, una de ellas es SDN (Redes definidas por software), desde de donde se extraen diferentes conceptos siempre con la esencia o fundamento de SON, que dan como resultado: SD Security, SD Access y SD-WAN.

La tecnología SDN se enfoca en la administración, programabilidad, automatización, entre otras funciones de/para los equipos de red, generando una mejor experiencia a los administradores de red, quienes de manera centralizada pueden controlar todos sus dispositivos que soportan dicha tecnología, mejora el funcionamiento de la red segmentando funciones de los dispositivos físicos.

En este artículo me enfocare en la solución de Cisco para SD-WAN: Viptela. Donde conoceremos los componentes de la arquitectura y los pasos necesarios para un aprovisionamiento de los controladores y la conexión de los vEdge.

Creado por Julio E. Moisa

El concepto de SD-WAN mantiene el objetivo de poder conectar las diferentes sucursales de una organización o incluso interconexión entre organizaciones, incluyendo una arquitectura que permite a las empresas u organizaciones la transformación digital, migraciones de servicios a la nube y gestionar múltiples enlaces de una manera segura y predecible sin mayor intervención de un administrador.

En la actualidad contamos con diversidad de medios para culminar ese objetivo:

- MPLS L3VPN
- MPLS L2VPN
- LTE/5G
- Internet
- Enlaces dedicados, etc.

¿Cuáles son algunas de ventajas que tiene SD-WAN Viptela sobre las redes tradicionales?

- Basado en SDN, permite ampliamente ser una solución escalable y adaptable al contexto.
- Viptela puede trabajar sobre cualquier de los medios más comunes de comunicación, con el fin de habilitar la comunicación entre sitios remotos de manera segura y predecible. Con el termino medios me refiero a ejemplo: MPLS, LTE, Fibra óptica, e incluso sobre Internet.
- Balanceo de carga por defecto.
- Brinda analítica para visibilidad y resolución de problemas.
- Los costos pueden disminuir entre un 40% a 50%, en muchos casos hasta más.
- Administración centralizada a través de la nube u on-premise.
- La segmentación de los planos de control, datos y administración, lo cual en los equipos tradicionales bien todo incluido, lo que en cierta manera puede retardos en el procesamiento de los datos, creación de colas de salida, etc.
- Levantamiento de instalaciones en cuestión de minutos. Levantar una red en una nueva ubicación puede llevar cierto tiempo, en lo que se planea, configura u optimiza una red; con Viptela únicamente hacemos la conexión entre los componentes a través de Internet o enlaces privados y desde el vManage podemos transferir un template con las configuraciones a los vEdge en los sitios remotos que deseemos configurar, y en cuestión de minutos el sitio quedara en funcionamiento.

La solución de Cisco SD-WAN Viptela ha sido desarrollada por poder resolver funciones complejas que las redes WAN tradicionales enfrentan, dicho esto, Viptela se basa en 3 áreas claves:

- Simplicidad
- Seguridad sobre múltiples capas
- Métodos de optimización para la entrega de los servicios.

A través de estas áreas, SD-WAN Viptela puede funcionar a través de cualquier medio de transporte y transferir cualquier tipo de servicio.

## Controladores Cisco SD-WAN Viptela

Aquí es donde la arquitectura se vuelve más interesante. Conoceremos cada uno de sus componentes,

recordemos que una de las características de SD-WAN es la segmentación de tareas y gracias a los controladores nosotros podemos contar una solución innovadora.

SD-WAN separa:

- Plano de control
- Plano de datos
- Plano de administración

Existe un 4to plano, conocido como plano de orquestación, este tipo de plano de se encarga de hacer todas las conexiones entre los vEdge y los controladores de la arquitectura de Viptela.

Ok, conozcamos los controladores que son componentes esenciales de Cisco Viptela:

| | |
|---|---|
|  | El vEdge es básicamente el dispositivo que colocamos en nuestro centro de datos para realizar la interconexión con el ISP y nuestra red. Veámoslo como el dispositivo de borde, en el básicamente no realizaremos mayor configuración y es el encargado del plano de datos. |
|  | vBond, es el orquestador inicial de la arquitectura, es el controlador encargado de establecer la conexión entre el vEdge y el vSmart. Es el encargado de los procesos iniciales de seguridad y Zero Touch (ZTP I PNP). Básicamente es el encargado de hacer la conexión con los vEdge a SD-WAN, aquí se intercambia información esencial para poder cumplir con la conexión. |
|  | vSmart, es considerado el cerebro de SD-WAN y es donde reside la tarea del plano del control. En redes tradicionales, los planos (control, datos y administración) residen en un mismo dispositivo, en SD-WAN esa idea no existe, los vEdge ya no cuentan con esa carga. VSmart es responsable de políticas, enrutamiento, etc. Trabaja junto con el protocolo OMP utilizado para la red overlay de SD-WAN y asi poder compartir la información del vManage con los vEdge. OMP trabaja muy similar a iBGP. |
|  | vManage, trabaja el plano de administración y es aquí donde pasaremos trabajando, vManage ofrece una interface para que podamos interactuar con la arquitectura de SD-WAN, aquí aplicaremos configuraciones, monitoreo, resolución de problemas, actualizaciones a los vEdge, etc. |

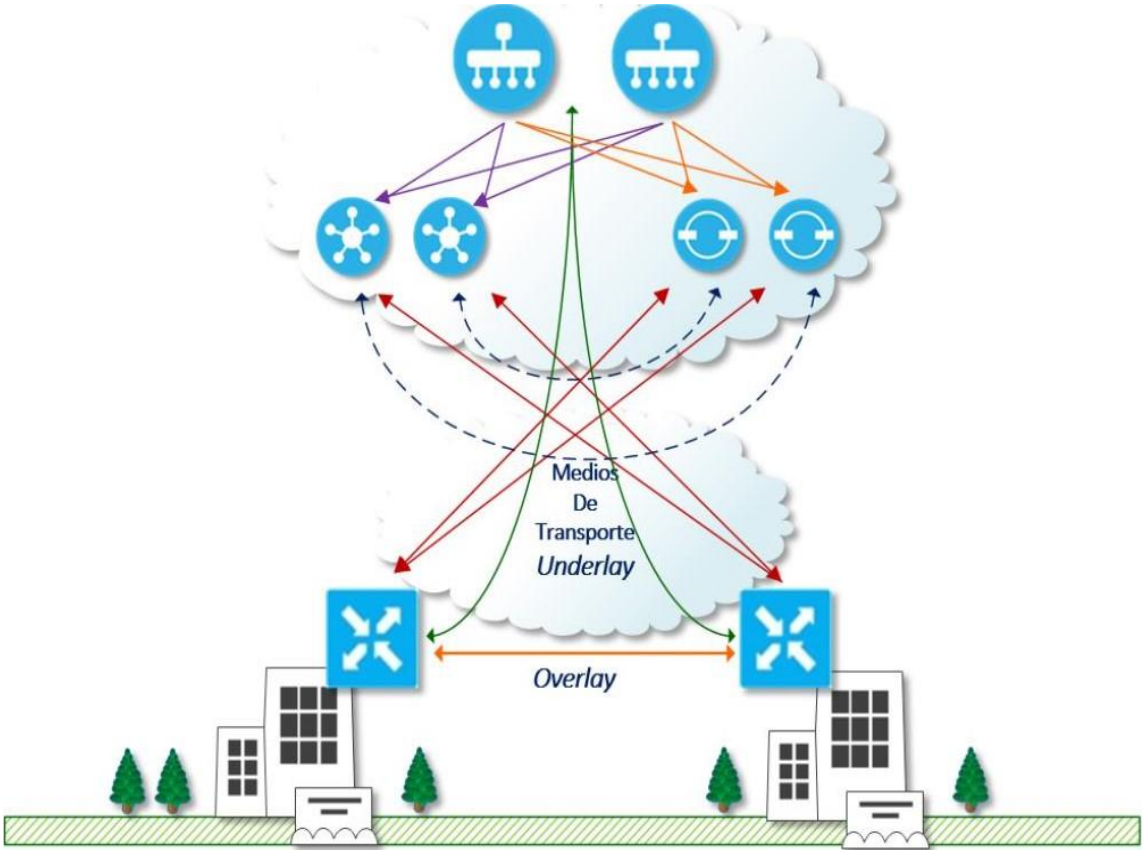
A través de las licencias (Essential, Advantage, Premier) de Viptela también conocidas como DNA, podemos obtener ciertas capacidades, incluyendo Analítica (Licencia Premier).

Independiente al tipo de deployment que deseemos realizar (nube u on-premise) los controladores ya vienen incluidos con la licencia de DNA, con la diferencia que:

- Deployment en la nube, Cisco realiza el aprovisionamiento de manera automática después de realizar solicitarlo al equipo de Cisco, para más información podemos abrir un caso con el Cisco TAC.

- Deployment on premise, para este tipo de aprovisionamiento el cliente debe crear sus servidores virtuales para la instalación de los controladores.

Por lo general los controladores son establecidos en parejas activo-activo a excepción del vManage que funciona en modo activo standby. Las organizaciones pueden tener más 2 controladores de cada tipo y lo menos para que funcione SD-WAN es 1 de cada uno.




La terminología Underlay se enfoca en los medios de transporte utilizados para establecer la comunicación entre los controladores y los vEdge. Básicamente indica las conexiones físicas.

Mientras que la terminología Overlay es utilizada para representar los túneles que se construyen de manera automática entre los vEdge y que sobre esto trabaja el protocolo OMP.

## ¿Cómo conectar un vEdge router a la arquitectura de Viptela?

Ahora, que hemos aprendido sobre los controladores, conoceremos los pasos para interconectar un vEdge router a la fabric/arquitectura de Viptela.

Paso I) Para iniciar debemos crear o solicitar la creación de una Smart Account, este tipo de cuenta es

utilizada para contar con un sistema centralizado de nuestras licencias o softwares. Básicamente es un repositorio centralizado.

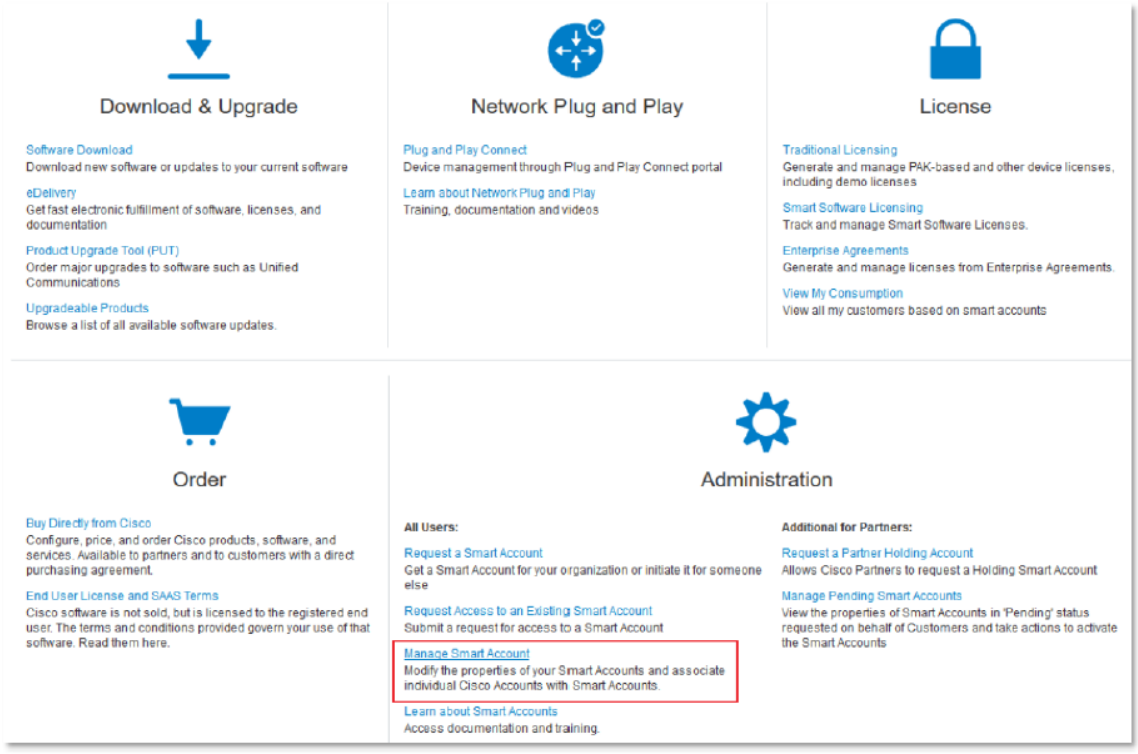
La cuenta la podemos crear a través del siguiente enlace:

https://www.cisco.com/c/en/us/products/software/smart-accounts.html#mstickvnav—l , donde una vez ingresada la información Cisco se pondrá en contacto con nosotros.

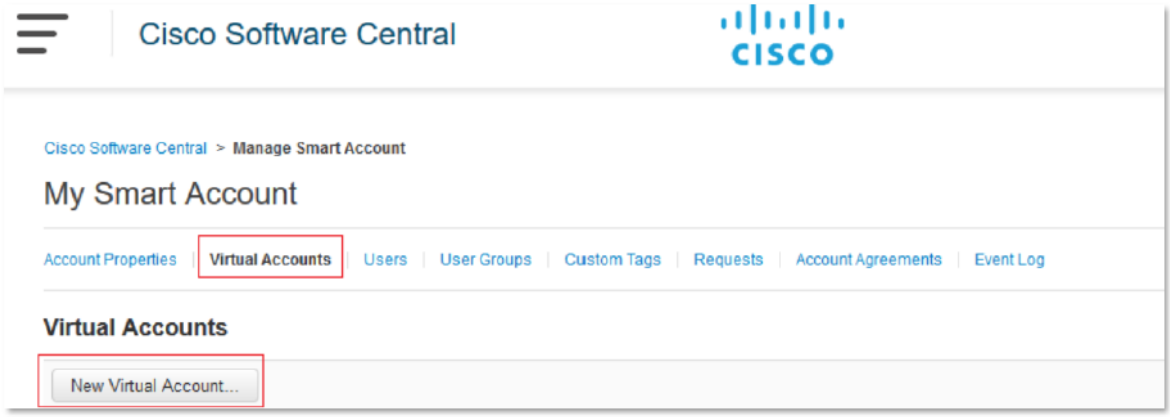
Otra forma de crear la Virtual Account, es solicitando apoyo a un Partner autorizado por Cisco.

Paso 2) Una vez creada y aprobada la Smart Account, debemos dentro de ella una Virtual Account, esta cuenta nos servirá para tener un control de nuestros controladores de Cisco Viptela, y nos servirá para hacer una sincronización con el vManage y de esta manera poder agregar nuestros vEdge de una manera fácil y rápida.

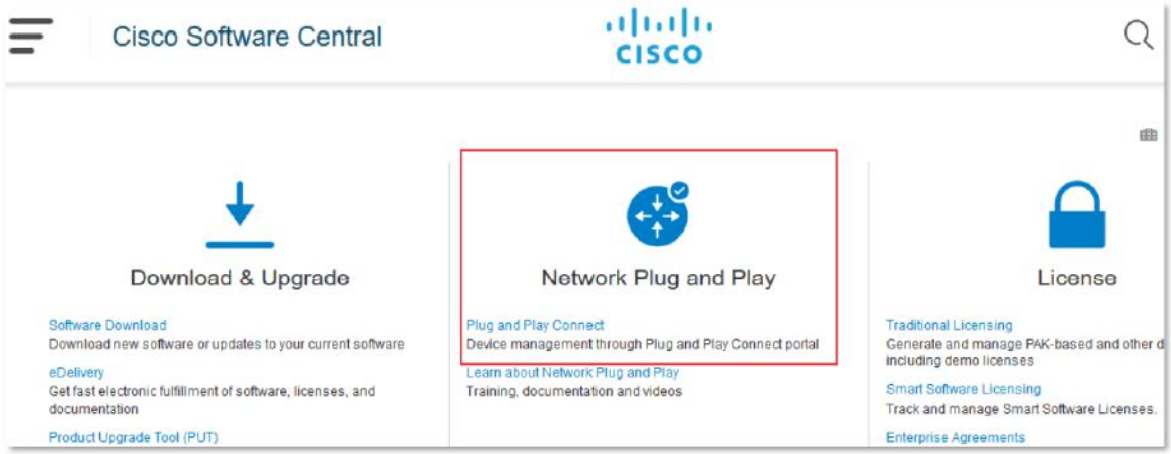
Para ingresar y administrar la Smart y Virtual Account, debemos ingresar al siguiente enlace: https://software.cisco.com/



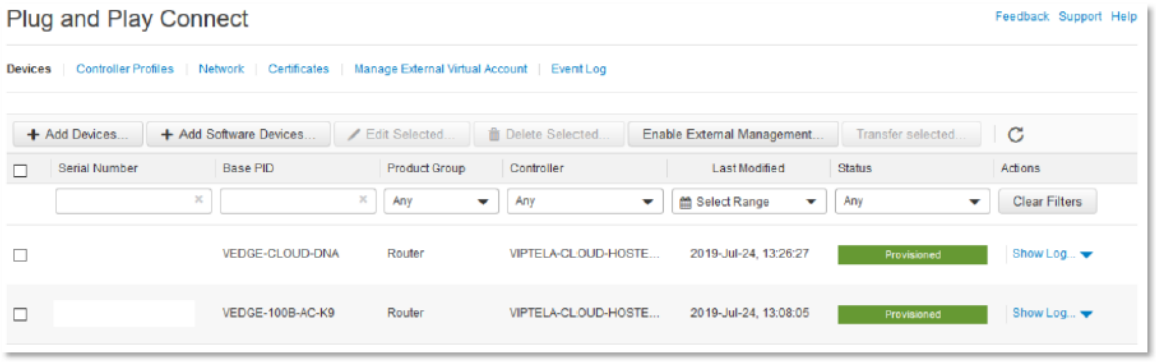
Dentro de la opción Manage Smart Account, seleccionamos Virtual Account y creamos una nueva, la cual puede seleccionarse como public.




Una vez creada la Virtual account, podemos abrir un caso con el Cisco TAC, para solicitar todo el soporte necesario y que nos apoyen con agregar los vEdge dentro de la opción de Plug and Play Connect y aprovisionar los controladores y la red.

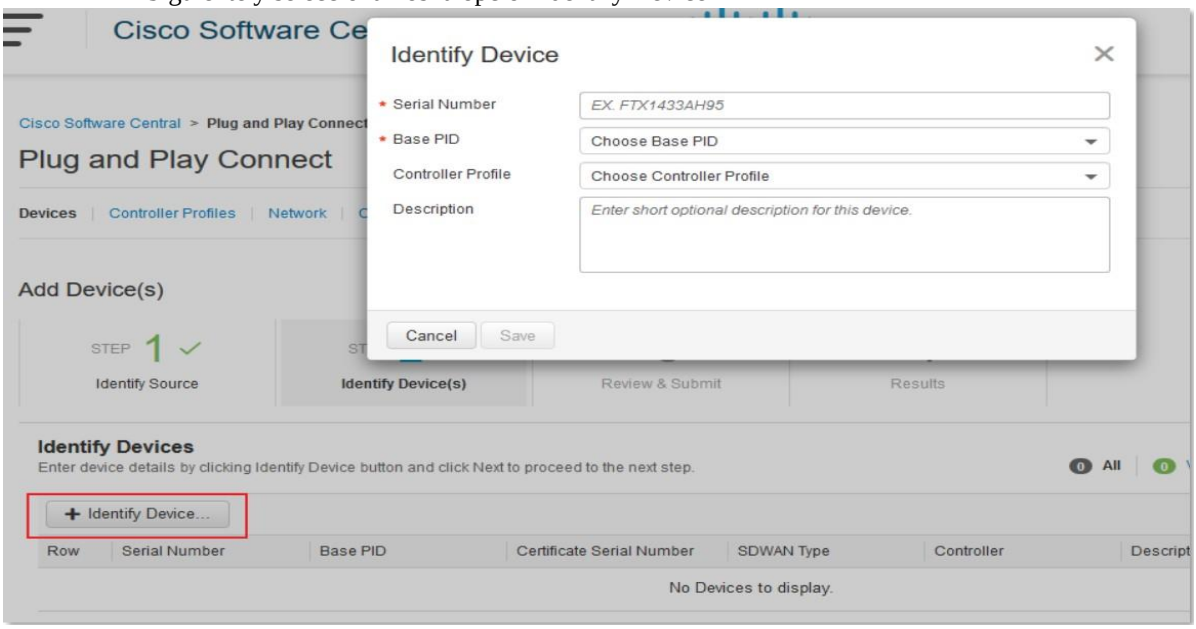



Dentro de esta opción podemos visualizar nuestros vEdge e información sobre los controladores y network, adicional a certificados.




Podemos agregar los vEdge incluyendo el número de serie que aparece en la caja de almacenaje o bajo el vEdge, y seleccionamos la opción Add Devices.

- Enter device info manually, podemos utilizar un archivo CSV si se desea.
- Siguiente y seleccionamos la opción Identify Device




- Colocar el número de serie del vEdge
- Base ID: Colocar el modelo del vEdge
- Controller Profile: Se coloca el controlador con el que se trabajara, este tuvo que haber sido aprovisionado por Cisco previamente.

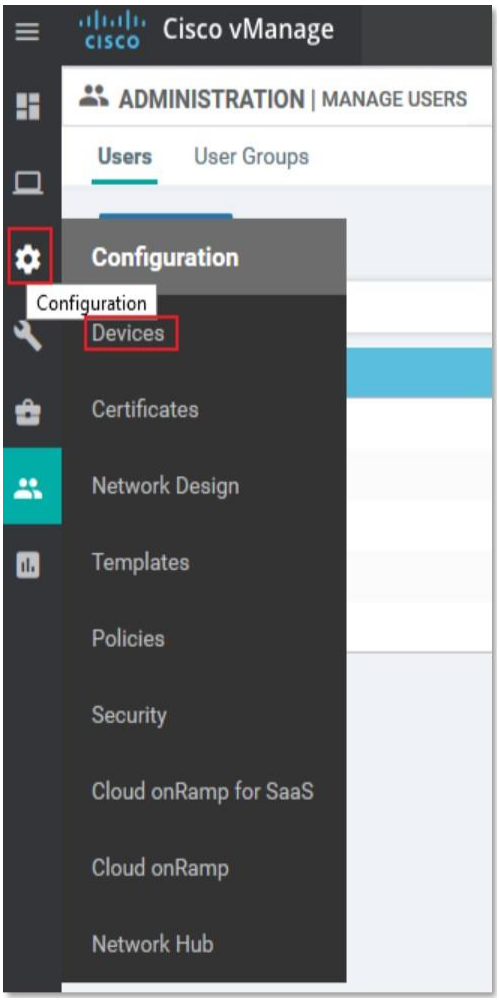
Una vez ingresada esta información, se hace clic en Next, se verifica la información y se finaliza el ingreso del vEdge.

Cisco debe proporcionar vía correo electrónico, la información sobre el acceso al vManage, e incluso haber solicitado un direccionamiento IP público, para permitir únicamente el ingreso a través de esa dirección IP, esto por motivos de seguridad.

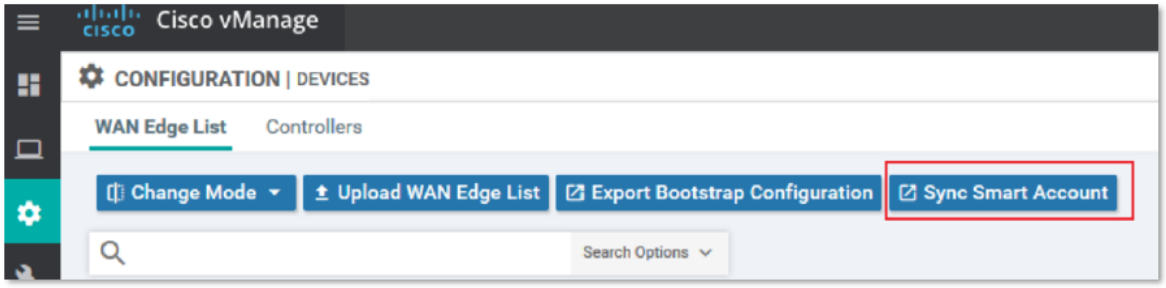
Creado por Julio E. Moisa

Ingresemos al vManage, colocando nuestras credenciales. Cisco brindara las credenciales por defecto y posteriormente el administrador puede crear cuentas de nivel: Administrador, Operador o básico. También se pueden modificar o crear niveles específicos.

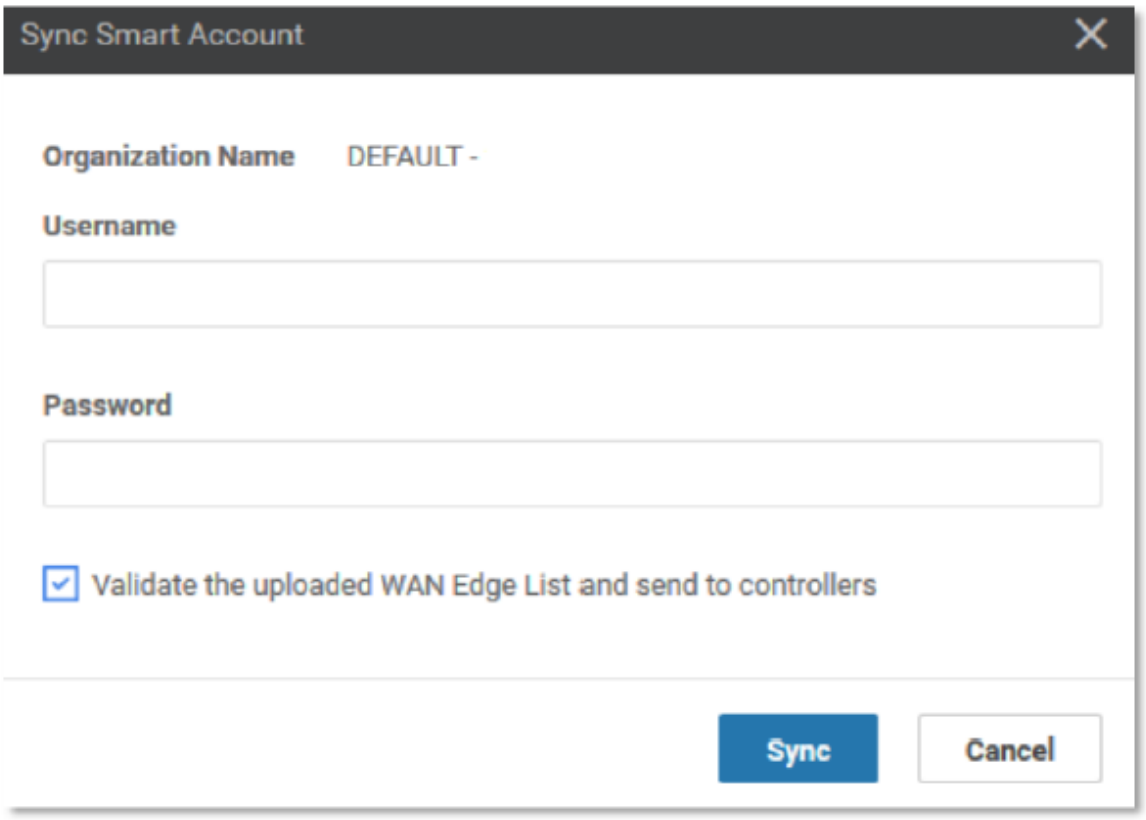

Una vez hemos ingresado al vManage, seleccionamos el icono de Configuration y luego Devices:



Luego seleccionamos la opción: **Sync Smart Account**



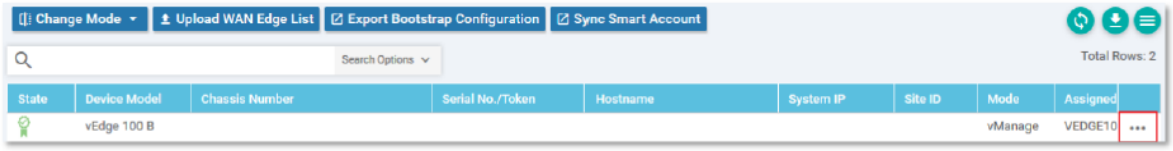

Seleccionando esa opción podremos sincronizar los vEdge dentro la opción Plug and Play Connect del Smart account y colocando nuestras credenciales los vEdge será agregados de manera automática a nuestro vManage. Fácil y rápido.

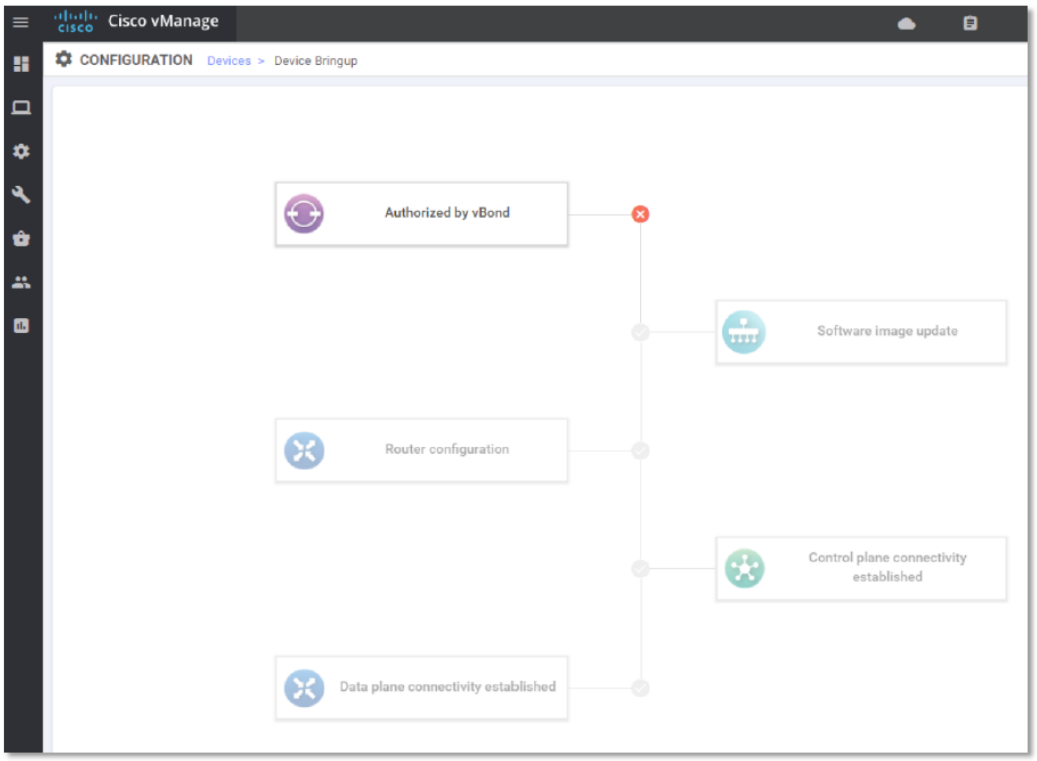



Una vez adherido el vEdge al vManage, necesitamos aplicar ciertos parámetros dentro del vEdge, por ejemplo, un Template, para iniciar puede ser un Template por defecto, el cual contendrá la información necesaria para realizar la sincronización de manera adecuada y así poder utilizar el dispositivo y aplicarle configuraciones, políticas, etc.

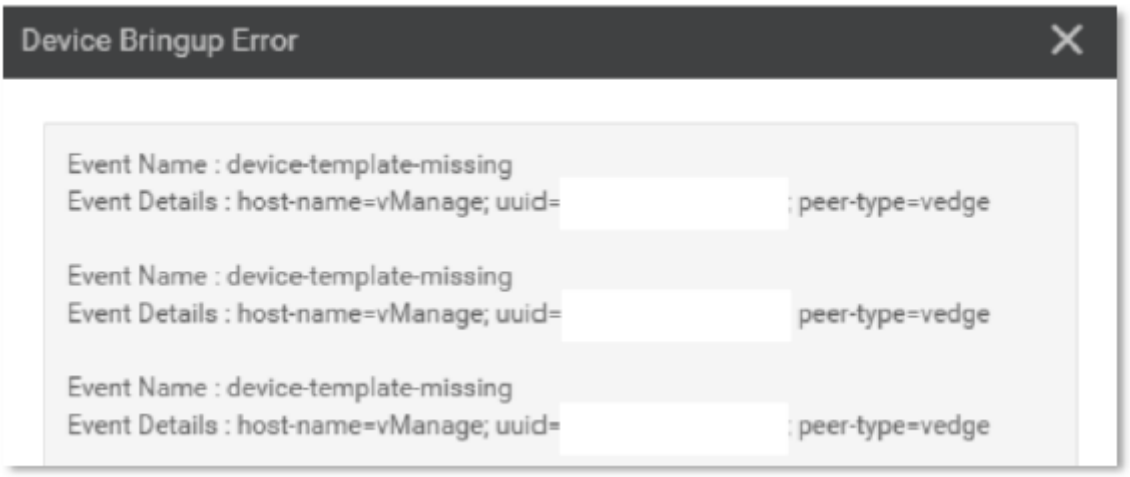
Creado por Julio E. Moisa

Si seleccionamos los 3 puntos que aparecen al final del dispositivo podremos y seleccionamos la opción Device Bring Up, podremos observar algún inconveniente si hace falta alguna información como el template, veamos las siguientes imágenes.



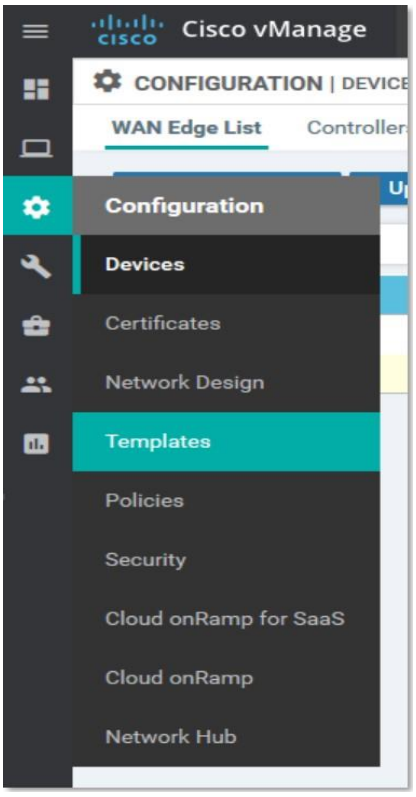
Hagamos clic sobre el cuadro: Authorized by vBond y observemos que muestra.




Nos indica que no existe un template, entonces debemos crearlo, para eso sigamos los siguientes pasos.

## Agregar un template a un vEdge

Paso I) Seleccionamos el icono de Configuración y luego seleccionamos Templates

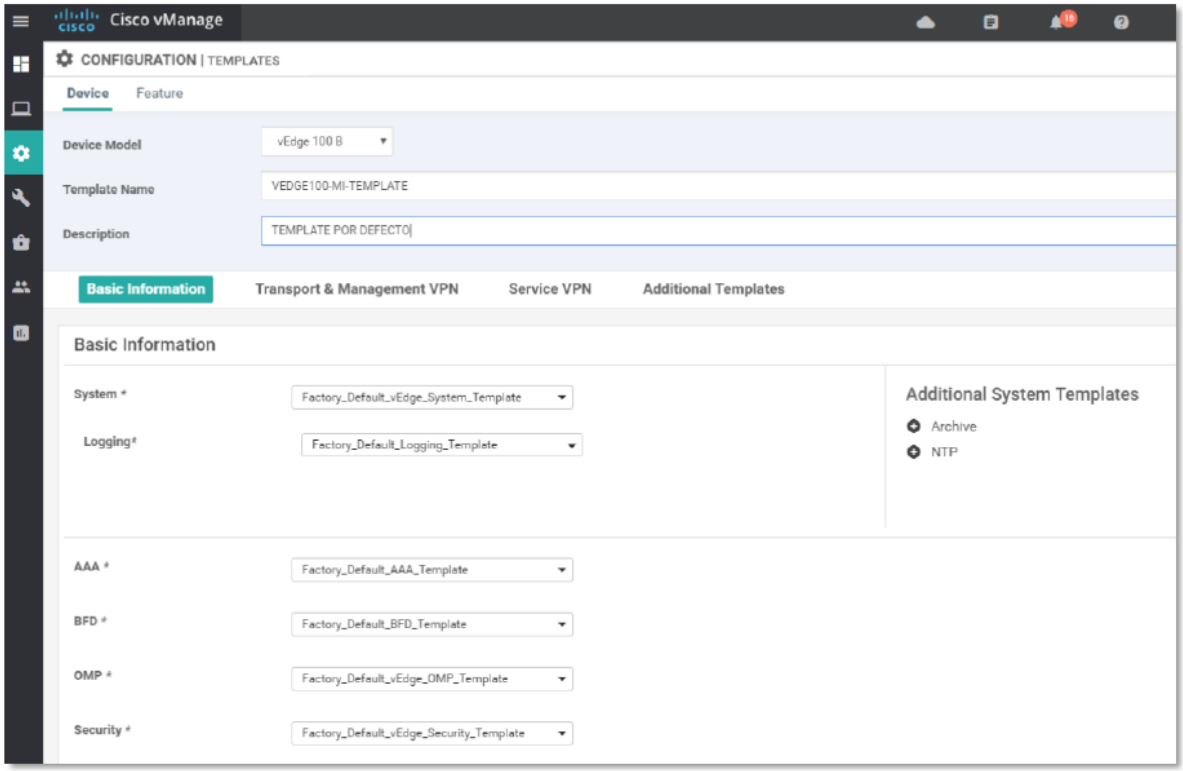


Paso 2) Seleccionar la opción Create Template

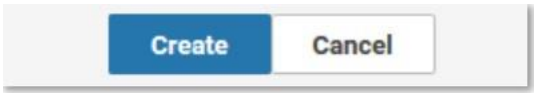
Paso 3) Seleccionamos:

- El modelo de nuestro vEdge
- Colocamos un nombre al Template
- Agregamos una descripción del Template

Para efectos de demostración dejaremos todos los valores por defecto.

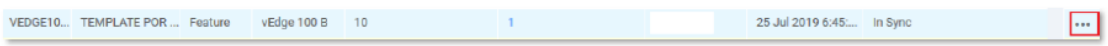



Luego presionamos el botón azul de Create, que se encuentra abajo.

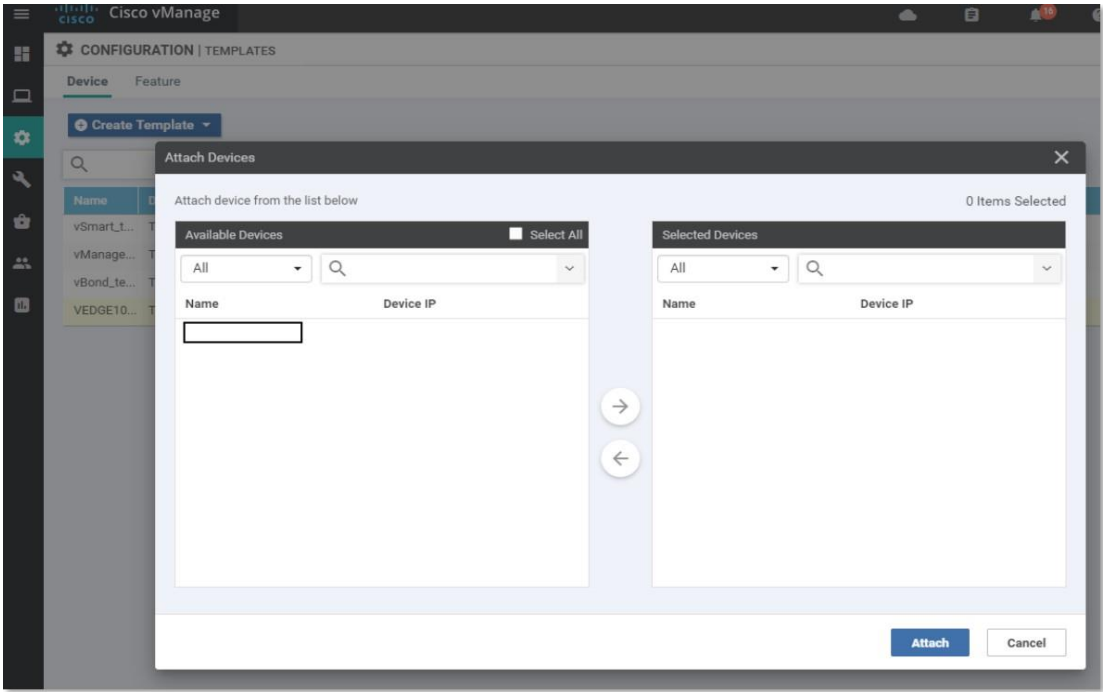



Paso 4) Asignamos el template a los dispositivos que deseamos tengan este template, esto es (útil cuando queremos hacer un aprovisionamiento en sitios remotos, donde solo enviamos la configuración inicial o final que los equipos deben de tener para poderlos administrar.

Hacemos clic en los 3 puntos.



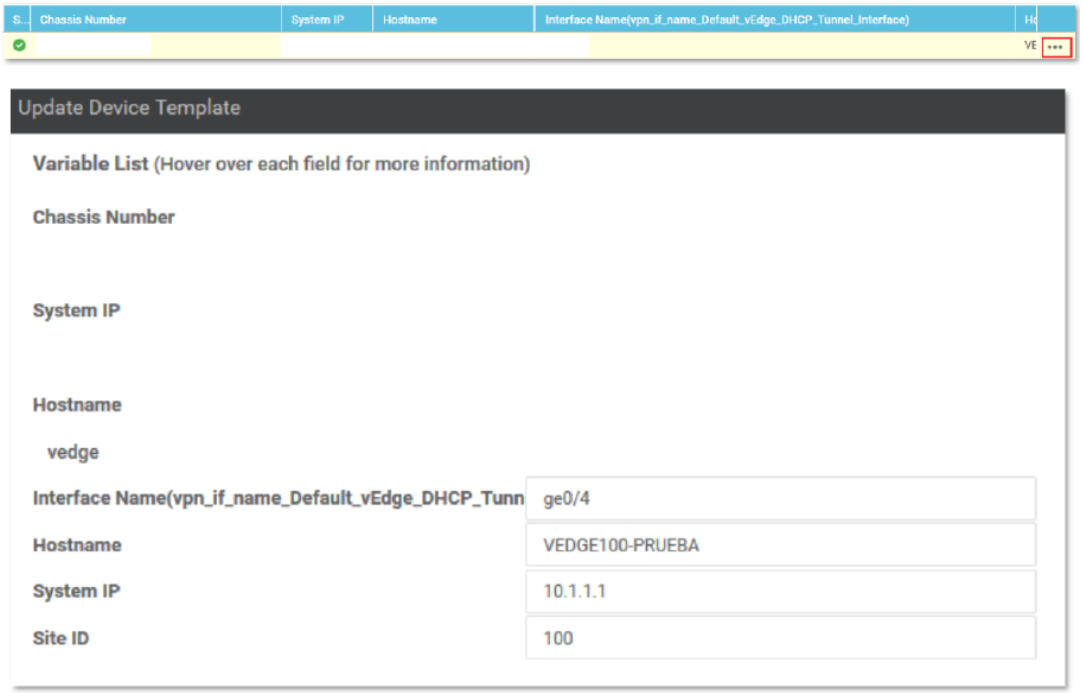

Paso 5) Transferimos el o los vEdge(s) que deseamos tengan el template, luego presionamos el botón Attach.



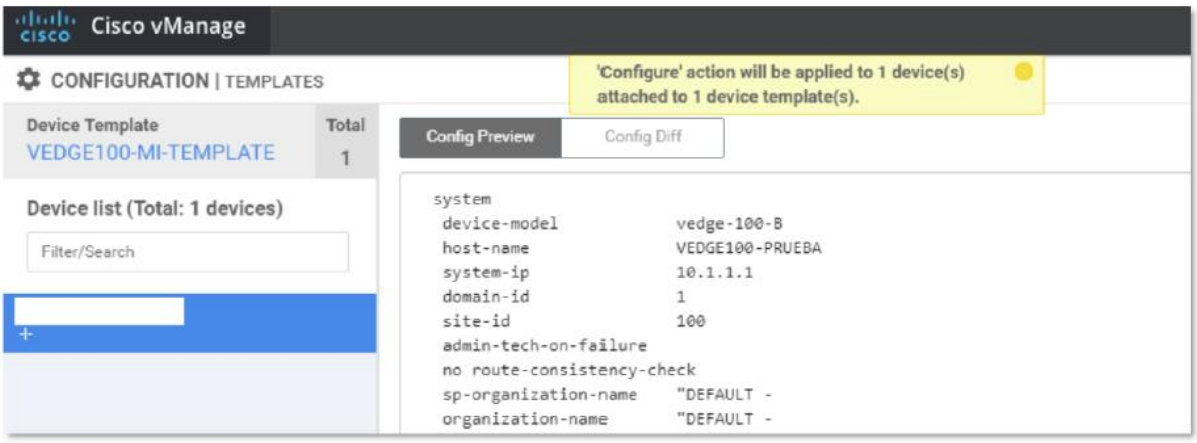

Paso 6) Verificamos que todo se encuentre bien y seleccionamos Next.

Paso 7) Configuramos el dispositivo. Esta sección es importante ya que indicamos que interface del vEdge será utilizada, site ID que es básicamente un identificador del sitio remoto donde se colocare el dispositivo, y por último el system IP, que básicamente funciona como el router-id de los protocolos de enrutamiento tradicionales o como una loopback.

Seleccionamos los 3 puntos y luego Edit Device Template

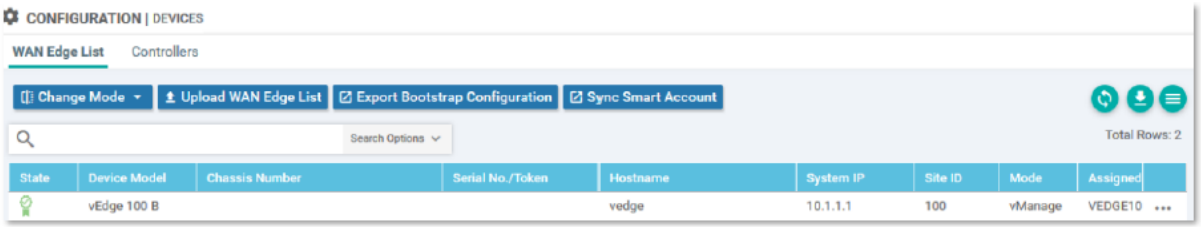


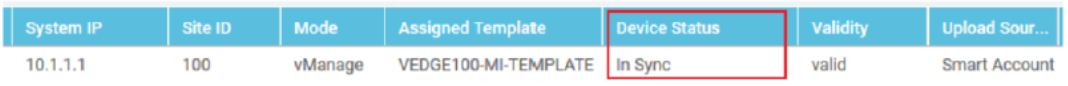

Paso 8) Configuramos el dispositivo



Una vez realizados los pasos anteriores podemos verificar si el vEdge ya se encuentra sincronizado y listo para funcionar, a través del botón de Configuration > Devices




Ya aparece como sincronizado, podemos concluir que nuestro vEdge esté listo para ser utilizado y aplicarle la configuración que nosotros deseemos. En algunas ocasiones se requiere actualizar la imagen del vEdge para que sea compatible con la versión del vManage.