UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERÍA DE SISTEMAS

Trabajo de titulación previo
a la obtención del título
de Ingeniero de Sistemas

PROYECTO TÉCNICO:

“MICRO-SEGMENTACIÓN EN CENTROS DE DATOS DEFINIDO POR SOFTWARE SOBRE LA PLATAFORMA VMWARE NSX”

AUTORES:

DARÍO XAVIER MOLINA ROBLES

BYRON FERNANDO TEJEDOR CABRERA

TUTOR:

ING. ROBERTO AGUSTÍN GARCÍA VÉLEZ, Ph.D.

CUENCA - ECUADOR

2021

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Darío Xavier Molina Robles con documento de identificación N° 0104510805 y Byron Fernando Tejedor Cabrera con documento de identificación N° 0105694384, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana, la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación: **"MICRO-SEGMENTACIÓN EN CENTROS DE DATOS DEFINIDO POR SOFTWARE SOBRE LA PLATAFORMA VMWARE NSX"**, mismo que ha sido desarrollado para optar por el título de: *Ingeniero de sistemas*, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores, nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Cuenca, marzo del 2021.

Darío Xavier Molina Robles

C.I. 0104510805

Byron Fernando Tejedor Cabrera

C.I. 0105694384

CERTIFICACIÓN

Yo, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: **"MICRO-SEGMENTACIÓN EN CENTROS DE DATOS DEFINIDO POR SOFTWARE SOBRE LA PLATAFORMA VMWARE NSX",** realizado por Darío Xavier Molina Robles y Byron Fernando Tejedor Cabrera, obteniendo el *Proyecto Técnico,* que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana.

Cuenca, marzo del 2021.

Ing. Roberto Agustín García Vélez, Ph.D.

C.I. 0103650891

DECLARATORIA DE RESPONSABILIDAD

Nosotros, Darío Xavier Molina Robles con documento de identificación N° 0104510805 y Byron Fernando Tejedor Cabrera con documento de identificación N° 0105694384, autores del trabajo de titulación: **"MICRO-SEGMENTACIÓN EN CENTROS DE DATOS DEFINIDO POR SOFTWARE SOBRE LA PLATAFORMA VMWARE NSX",** certificamos que el total contenido del *Proyecto Técnico*, es de nuestra exclusiva responsabilidad y autoría.

Cuenca, marzo del 2021.

Darío Xavier Molina Robles

C.I. 0104510805

Byron Fernando Tejedor Cabrera

C.I. 0105694384

Dedicatoria

El presente trabajo va dedicado a Dios y con todo mi cariño a mis queridos padres y hermano, quienes siempre me apoyaron incondicionalmente y fueron mi motivación para culminar la carrera.

De igual manera, a mis familiares y amigos quienes siempre creyeron en mí y estuvieron pendientes de mis avances en el estudio.

Agradecimientos

En primer lugar, quiero agradecer a Dios por mantenerme con salud y haberme dado la capacidad para poder estudiar y terminar este duro camino universitario.

Quiero agradecer también a mis padres por su esfuerzo y sacrificio, por haberme forjado para convertirme en la persona que soy, por haberme apoyado y a la vez por haberme permitido estudiar una carrera universitaria.

A mi hermano por su paciencia, por sus consejos y motivación para no rendirme en los momentos difíciles, por mostrarme que en la vida todo es posible y no hay impedimentos cuando se realiza una actividad con esfuerzo y dedicación.

A mi compañero de tesis por su amistad incondicional, por su constante apoyo y dedicación.
A mis mejores amigos Tadea y Bryan quienes han sabido ser un apoyo incondicional para mi vida.

A mis profesores y director de tesis por sus enseñanzas y por haberme preparado para convertirme en un profesional capaz de responder de manera eficaz al momento de ejercer mi profesión.

A mi familia y amigos por creer en mí. Por estar presentes en los momentos de necesidad y por brindarme apoyo de manera constante.

Finalmente quiero agradecerme a mí, por todas las malas noches soportadas en la universidad,[vii] por los trabajos hechos a último momento, por ese examen que no fui capaz de superar ya que esto me enseñó una lección más de la vida, por las materias aprobadas y que no tenían nada que ver con la carrera, , también por las materias reprobadas ya que me enseñaron en valor del tiempo y compromiso, por el reto que me puse al elegir esta carrera tan chevere, por las veces que no acepté ir de fiesta por cumplir mis obligaciones, por el certificado de paternidad que nunca llegó y sobre todo por mis deseos de seguir siempre adelante de triunfar en esta vida y no conformarme con lo que se supone debo conformarme. Por la humildad demostrada y por las pendejadas que hacen de mi vida una mejor.

Resumen

La administración de redes tradicionales son estáticas y requieren una gran cantidad de recursos para realizar cambios en su administración y gestión, lo cual representa un problema latente en cuanto se refiere a la adquisición y mantenimiento de equipos físicos, mismos que se encargan de solventar la necesidad de organizar la red dentro de un ámbito empresarial. Con el paso del tiempo el uso de los recursos de red crece a gran escala, esto ocasiona que las organizaciones requieran de grandes cantidades de capital para poder expandir el uso de la infraestructura para generar operaciones con mayor grado de eficiencia capaces de abarcar todas las necesidades generadas por la demanda de los recursos en el centro de datos.

Para solucionar este problema surge la alternativa de las redes definidas por software y sobre esto una tecnología disruptiva llamada Micro-segmentación, la cual nos habilita la posibilidad de administrar la red interna dentro del centro de datos. Esto permite crear nuevos conjuntos de subredes para conexiones de diferentes servicios de tal manera que puedan conectar, tráfico de este a oeste dentro de un centro de datos donde se permita un ingreso y salida transparente que a su vez es segura, desde una sola consola de administración.

Mediante el uso de Micro-segmentación se consigue administrar la red abriendo la posibilidad hacia un crecimiento de la red ágil y flexible con administración centralizada desde una consola de administración capaz de gestionar el uso de los recursos existentes dentro de las redes del centro de datos. Sumado a esto, la Micro-segmentación nos permite establecer políticas de seguridad con cargas de trabajo individual que actúan de acuerdo con la necesidad de cada servicio que se encuentra inmerso dentro del centro de datos, de esta manera se brinda un nivel de seguridad avanzado, con propuestas de solución enfocadas en una red convergente que se gestiona

bajo virtualización de tal manera que se permite evitar la adquisición de nuevos equipos de hardware para cada nueva implementación.

En este proyecto de titulación se plantea un escenario de centro de datos virtualizado en donde se podrá evidenciar el uso y administración de las redes definidas por software. Para ello se contará con la plataforma de virtualización VMware teniendo como hipervisor ESXi que a su vez es gestionado por VMware VCenter. Con el uso de estas soluciones se consigue generar el entorno de trabajo para el despliegue del componente NSX encargado de realizar la virtualización de red y gestionar los procesos de Micro-segmentación. Sumado a ello, se presentará el uso de Deep Security como software de seguridad adicional que trabaja junto a NSX para lograr consolidar un sistema de seguridad avanzado, en donde se aplica la Micro-segmentación, la cual tiene como propósito impedir que un ataque pueda propagarse de manera horizontal afectando a todos los servicios alojados en el centro de datos. Para validar nuestro escenario de pruebas se cuenta con una herramienta llamada KnowBe4, misma que ejecuta pruebas rigurosas que nos permiten identificar posibles fallas de seguridad en nuestro entorno virtualizado.

Abstract

The administration of traditional networks are static and require a large amount of resources to make changes in their administration and management which represents a latent problem in terms of the acquisition and maintenance of physical equipment, which are responsible for solving the need. to organize the network within a business environment. Over time the use of network resources grows on a large scale, this causes organizations to require large amounts of capital to be able to expand the use of the infrastructure to generate operations with a higher degree of efficiency capable of covering all needs generated by the demand for resources in the data center.

Solving this problem, the alternative of software defined networks arise and this is a disruptive technology called Micro-segmentation, which enables use to manage the internal network within the data center. This allows creating new sets of subnets for connections of different services in such a way that they can connect, traffic from east to west within a data center where a transparent entry and exit is allowed that in turn is secure, from a single console of management.

Through the use of Micro-segmentation, it is possible to manage the network, opening the possibility of agile and flexible network growth with centralized administration from an administration console capable of managing the use of existing resources within the data center networks. In addition to this, Micro-segmentation allows us to establish security policies with individual workloads that act according to the need of each service that is immersed within the data center, in this way an advanced level of security is provided, with solution proposals focused

on a converged network that is managed under virtualization in such a way that it is possible to avoid the acquisition of new hardware equipment for each new implementation.[xi]

In this degree project, a virtualized data center scenario is proposed where the use and administration of software-defined networks can be evidenced. For this, it will have the VMware virtualization platform having ESXi as a hypervisor, which in turn is managed by VMware VCenter. With the use of these solutions, it is possible to generate the work environment for the deployment of the NSX component in charge of performing the network virtualization and managing the Micro-segmentation processes. In addition to this, the use of Deep Security will be presented as additional security software that works together with NSX to consolidate an advanced security system, where Micro-segmentation is applied, which is intended to prevent an attack from spreading. horizontally affecting all services hosted in the data center. To validate our test scenario, we have a tool called KnowBe4, which runs rigorous tests that allow us to identify possible security flaws in our virtualized environment.

Tabla de contenido

Capítulo 1 ..... *1*

1.1 Introducción **1**

1.2 Justificación **5**

1.3 Antecedentes **7**

1.4 Problema de Estudio **9**

1.5 Importancia **11**

1.6 Objetivos **11**

1.6.1 Objetivo general 11

1.6.2 Objetivos específicos 11

Capítulo 2 ..... *12*

2.1 Estado del arte **12**

2.2 Virtualización **13**

2.2.1 Tipos de virtualización 14

2.2.2 Importancia de la virtualización 16

2.2.3 Definición de hipervisor 18

2.2.4 Tipos de hipervisor 18

2.3 Concepto de centro de datos definido por software **19**

2.4 Importancia de virtualizar el centro de datos **21**

2.5 Virtualización de la red **23**

2.5.1 Definición de Virtualización de la red 23

2.6 Tecnologías que comprenden la virtualización de Red **24**

2.6.1 Virtualización de Funciones de Red (Network Function Virtualization - NFV) 24

2.6.2 Redes Definidas Por Software – SDN 25

2.6.3 Desafíos de SDN 27

2.6.4 Características de las redes definidas por software 29

2.6.5 Diferencia entre una red física y una red definida por software 30

2.6.6 Importancia de las redes definidas por software 31

2.7 Servicio de Orquestación **32**

2.8 Integración SDN y NFV **33**

Capítulo 3 ..... *37*

3.1 Estudio de los riesgos de seguridad que afectan a los centros de datos **37**

3.2 Identificación de los riesgos que pueden surgir dentro del centro de datos **38**

3.2.1 Amenazas Físicas 38

3.2.2 Amenazas lógicas 39

3.2.3 Descripción de ataques comunes que afectan el funcionamiento del centro de datos 40

3.3 Herramientas utilizadas para el análisis de vulnerabilidades destinadas a centros de datos **43**

3.3.1 Nessus 43xiii
3.3.2 OpenVas 44
3.3.3 RanSim 44

3.4 Definición de Firewall 45
3.4.1 Tipos de Firewall 45
3.4.2 Ventajas de utilizar Firewall 46
3.4.3 Desventajas de utilizar Firewall 48
3.4.4 Diferencia entre un Firewall Físico y un Firewall Lógico 48

3.5 Trend Micro Deep Security 51
3.5.1 Ventajas de utilizar Trend Micro Deep Security 52
3.5.2 Desventajas de utilizar Trend micro deep security 54

Capítulo 4 56

4.1 Tecnología de VMware para la virtualización de centro de datos 56

4.2 Definición de ESXi como solución de VMware para ambientes empresariales 57
4.2.1 Ventajas de utilizar el hipervisor ESXi en un centro de datos 58
4.2.2 Desventajas de usar el hipervisor ESXi 59

4.3 Definición de VCenter Server, como orquestador de ambientes virtualizados 60
4.3.1 Gestor de virtualización de red Plug-ins 61

4.4 Definición de NSX Management 63
4.4.1 Importancia de implementar NSX en un centro de datos 64

Capítulo 5 67

5.1 ¿Que es la segmentación de red? 67

5.2 ¿Que es la Micro-segmentación? 68

5.3 En qué consiste la Micro-segmentación 70

5.4 La Micro-segmentación con su modelo cero confianza para la seguridad del centro de datos. ..71

5.5 Ventajas de la Micro-segmentación 73

5.6 NSX como solución de VMware para realizar Micro-segmentación 74

5.7 Arquitectura de NSX dentro de vSphere 76
5.7.1 Plano de Datos 77
5.7.2 Plano de Control 78
5.7.3 Plano de Administración 79

5.8 Componentes de NSX Management 80
5.8.1 Router DLR 80
5.8.2 Router ESG 83
5.8.3 vSwitch 84
5.8.4 Conmutadores Lógicos 85
5.8.5 Firewall 86
5.8.6 Controller Nodes 87
5.8.7 VXLan 88
5.8.8 Transport Zone 89

Capítulo 6.....*90*xiv

6.1 Despliegue del protocolo de pruebas **90**

6.2 Topología de red **91**

6.3 Direccionamiento IP **94**

6.4 Requisitos previos al despliegue de NSX sobre ESXi **96**

6.4.1 Network Time Protocol 96

6.4.2 Domain Name Server 97

6.5 Servicios alojados en el centro de datos **99**

6.5.1 Servicio de Active Directory como controlador de dominio 99

6.5.2 Apache como Servicio WEB.....100

6.5.3 Uso del protocolo SIP para VOIP 101

6.5 4 Postgresql como Base de Datos 102

6.6 Modelo Cero Confianza **102**

6.6.1 Firewall.....107

6.7 Protocolo de Pruebas **110**

6.7.1 Periodo de Prueba.....113

6.7.2 Prueba de vulnerabilidades en el centro de datos previo a aplicar Micro-segmentación.....113

6.7.3 Pruebas finales con la aplicación de Micro-segmentación 115

7 Resultados ***120***

Funcionamiento de la Micro-segmentación como método de aseguramiento de la red.....122

8 Conclusiones ***126***

9 Referencias.....*¡Error! Marcador no definido.*

Lista de Tablas

Tabla 1 Direccionamiento IP de cada host incluido dentro de la topología desarrollada 95
Tabla 2 Nombres de Dominio configurados en cada host 99

Lista de Figuras xvi

Ilustración 1 Comparativa entre centro de datos tradicional y centro de datos definido por software 21
Ilustración 2 Entendiendo NFV – SDN y sus componentes 34
Ilustración 3 Seguridad en un centro de datos (Trend Micro, 2018) 52
Ilustración 4 Interpretación de ESXi sobre un servidor físico (Vincentis, 2017) 58
Ilustración 5 Centro de datos virtual sobre ESXi desplegado de manera tradicional (Vincentis, 2017) 60
Ilustración 6: VCenter Server (Caballé, Cerda, Cinalli, Herrero, & de la cruz, 2019) 62
Ilustración 7 Arquitectura básica de una red virtual generada dentro de NSX (VMware, 2019). 66
Ilustración 8 Procesos entre plano de datos, plano de control y plano de administración 77
Ilustración 9 Topología de red 91
Ilustración 10 Redes Segmentadas por NSX 92
Ilustración 11 Vista de los equipos físicos presentes en nuestro proyecto de Micro-segmentación 93
Ilustración 12: Usuarios y Equipos pertenecientes al Directorio Activo 104
Ilustración 13 Manejo de políticas por grupo definidos según su categoría 105
Ilustración 14 Resumen de la creación de grupo de seguridad 106
Ilustración 15 Diferencia de la Seguridad con NSX DFW 108
Ilustración 16 Firewall ESG y DLR 109
Ilustración 17 Firewall General de la infraestructura 110
Ilustración 18 “Security Awareness Computer-Based Training Reviews and Ratings” ((Budge, O'Malley, Blankenship, Flug, & Nagel, 2020) 112
Ilustración 19 Knowbe4 en maquina sin configurar seguridad 115
Ilustración 20 Comunicación entre el agente y el administrador de deep security 116
Ilustración 21 Panel de alertas de las máquinas monitoreadas. 117
Ilustración 22 Prueba de contexto de la Micro-segmentación. 118
Ilustración 23 Reglas aplicadas como configuración de la microsegmentacón 119
Ilustración 24 Ambiente no seguro 123
Ilustración 25 Alerta del agente al usuario en detección de amenazas. 124
Ilustración 26 Aislamiento de red a la máquina infectada. 125

Capítulo 1

1.1 Introducción

En la actualidad los centros de datos se han convertido en el activo más preciado para las empresas, ya que en este se encuentra toda la información digital de valor incalculable para el funcionamiento, provisión de servicios y aplicaciones, por esta razón la industria de las comunicaciones, software y virtualización de los centros de datos han desarrollado nuevas y mejores características de rendimiento, administración y seguridad. Considerando que la parte tecnológica se mantiene actualizándose constantemente así pues las amenazas están evolucionando con ataques más sofisticados que comprometen el centro de datos de norte a sur y pueden llevar al colapso de los sistemas críticos de las empresas, aislando al centro de datos de los clientes.

Al mismo tiempo las redes tradicionales en los centros de datos pasan por un proceso de distribución lentas para el cambio y limitan los perímetros de seguridad desde y hacia el centro de datos, sin sistemas de monitoreo adecuados que nos ayuden a reaccionar en caso de existir una vulnerabilidad o varias de las amenazas que surgen con el transcurso de los días y los avances tecnológicos. Es por esta razón que emerge una alternativa favorable para la seguridad de un centro de datos y consiste en una solución que abarca la administración de la red desde una plataforma centralizada que nos permite la visualización completa de la red.

Por lo tanto, una red definida por software ofrece mayor flexibilidad al momento de ser configurada, al contar con un software subyacente que se encarga de virtualizar y gestionar los cambios generados por un operario de la red. Esta solución proporciona mecanismos de configuración que puede adecuar diferentes dispositivos virtuales que permiten acciones como el enrutamiento, distribución y a su vez la seguridad a nivel lógico tomando en cuenta que todo esto ocurre dentro de un centro de datos, sin necesidad de implicar equipos físicos. No obstante, las amenazas de los hackers son latentes, razón por la cual se aborda un tema esencial que implica la técnica basada en Redes Definidas Por Software (Software Defined Networking - SDN) dado que su configuración representa una necesidad para construir bloques de seguridad aplicando cargas de trabajo a cada máquina virtual.

De acuerdo con (Alcaráz, 2021), en la actualidad VMware es uno de los sistemas de virtualización más populares por su versatilidad, eficiencia y soporte a nivel mundial, esta plataforma de virtualización cuyo hipervisor[1] es (Elastic Sky X Integrated - ESXi) brinda la posibilidad de sostener una propuesta convergente con factores de configuración propios de las herramientas de VMware que nos permite gestionar acciones y generar políticas de control de acceso no solo a la red, si no a cada servicio alojado en el centro de

[1] hipervisor: “Es un software que crea y ejecuta máquinas virtuales (VM) y que, además, aísla el sistema operativo y los recursos del hipervisor de las máquinas virtuales y permite crearlas y gestionarlas”. (Red Hat, 2021)

datos definido por software, lo que hace posible una mayor capacidad de control y gestión de tareas.

La empresa VMware se encarga de crear software para brindar soluciones a los ambientes laborales ya sea virtuales o físicos, así pues, cubre las diferentes aristas de la infraestructura y considerando las soluciones para automatización de tareas y despliegues, sistemas de disponibilidad, optimización y gestión de procesos, proporcionando una visualización completa e integral desde un único sistema centralizada de administración. Así pues este entorno de virtualización presenta una suite de servicios distribuidos a nivel lógico, en donde se puede asignar recursos, mismos que son generados mediante políticas que permiten consolidar la utilidad de un centro de datos virtual, haciendo uso de la infraestructura que presenta VMware ya que ésta es capaz de agregar operaciones basadas en recursos asignados de manera subyacente, esto hace posible conectar varios sistemas dentro del centro de datos que forman el entorno virtual.

Basado en la infraestructura que presenta VMware a través de ESXi, que a su vez es administrada por el orquestador VCenter[2] es posible virtualizar una red completa sin necesidad de utilizar demasiados equipos de hardware. Esto permite a una empresa obtener muchas ventajas sobre una infraestructura de red tradicional. No obstante, según el autor (Vincentis, 2017) resulta primordial comprender el funcionamiento de la virtualización de

[2] vCenter: "Es un servicio que funciona sobre una máquina virtual y que nos permite gestionarlo todo de una forma totalmente centralizada" (Cinalli, 2019).

red planteada como solución de VMware Virtualización de Red y Plataforma Segura (Network Virtualization And Security Plataform - NSX), misma que es capaz de permitir la configuración de Switch Virtual Distribuido (Virtual Distributed Switch - VDS), Enrutador Lógico Distribuido (Logical Distributed Router -DLR), Puerta de Enlace de Servicio Edge (Port Edge Services - ESG), Red de Área Local Virtual Extensible (Virtual Extensible Local Area Network VXLan) y otros componentes de red.

Usando VMware NSX somos capaces de virtualizar la red además de ser posible configurar políticas específicas de firewall con cargas de trabajo a nivel individual, de acuerdo con los servicios alojados en cada host, de manera que todo el entorno subyacente tenga un nivel de seguridad avanzado. De este modo se puede controlar el funcionamiento de cada nodo y prevenir que un ataque se pueda propagar de forma horizontal en la red; Para lograr un nivel de seguridad avanzado, los autores (Gilman & Barth) recomiendan la implementación del entorno de red virtualizado con la aplicación de la metodología Cero Confianza[3], cuya funcionalidad cobra valor generando instancias con pruebas de autenticidad e integridad para posteriormente brindar autorización y limitar el acceso a los recursos de acuerdo con los privilegios asignados.

[3] Cero Confianza: es un modelo de seguridad de TI que requiere una verificación de identidad estricta para todas las personas y dispositivos que intentan acceder a los recursos en una red privada, independientemente de si se encuentran dentro o fuera del perímetro de la red (Cloudflare, 2021).

El uso de SDN representa un paradigma con respecto a las redes implementadas en ambientes físicos, sin embargo, no se tratan como tal por la razón de su capacidad para desplegar nuevos modelos de uso, otorgando flexibilidad y crecimiento dinámico a la red. Por tal motivo y tomando en cuenta la actualidad con los significativos avances que surgen tanto en las empresas y en la manera que se maneja el software, es imprescindible actualizar los sistemas de acuerdo con las necesidades de la organización tomando en cuenta los nuevos paradigmas de la virtualización, cuyo objetivo es claro si se toma en cuenta su uso y facilidad que presenta a la hora de desplegar un centro de datos, más aún si se trata de un punto tan crítico como la red de una empresa.

1.2 Justificación

En la actualidad existe un gran número de empresas y cada una de ellas está involucrada con la tecnología, no obstante, en muchas ocasiones se puede obviar el uso de alternativas que han surgido de acuerdo con el avance de la ciencia. Dicha tecnología implica modelos de implementación avanzados cuya necesidad es primordial cuando se trata del manejo de ambientes críticos dado que permiten administrar los centros de datos con tecnologías modernas que hacen posible aplicar modelos de seguridad alternos a los que se usa tradicionalmente.

El desarrollo de este proyecto resulta crucial dado que hace posible mejorar la administración de los centros de datos actuales, tomando en cuenta un componente sumamente importante que es la red, ya que esta permitirá la conexión entre nuestro centro de datos y el internet en general o bien una Red de Área Local (Local Area Network - Red

de Área Local-LAN) específica con la posibilidad de crear Zonas Desmilitarizadas (Demilitarized Zone Zonas Desmilitarizadas - DMZ) en cualquier parte de la red. En donde se tiene como cometido principal lograr una configuración de red definida por software cuyos atributos de implementación puedan contar con soluciones flexibles y ágiles capaces de responder a los requisitos cambiantes que se presentan día a día.

Mediante el estudio de Micro-segmentación en redes definidas por software se podrá analizar un nivel de seguridad evidentemente más avanzado que el usado de manera tradicional. Permitiendo tomar en cuenta aspectos de relevancia que permitan solventar limitaciones que se presentan actualmente en las redes de datos, del mismo modo se podrá evidenciar las ventajas que existen al momento de gestionar una arquitectura de red centralizada. Dado que el manejo de la red con SDN se usa mediante controladores cuya función se basa en la manera de administrar toda la red, es posible disminuir la cantidad de errores que pudieran ser cometidos durante la implementación de una topología de red.

Sumado a las ventajas mencionadas, se podrá analizar el comportamiento de las máquinas virtuales ubicadas dentro del centro de datos frente a un acontecimiento anormal provocado por algún tipo de ataque informático. De este modo se demuestra que la Micro-segmentación mediante la correcta configuración y aplicación de políticas con cargas de trabajo en cada nodo es capaz de mitigar la propagación de un virus a nivel lateral dentro de la red de datos.

1.3 Antecedentes

En (Chang Frank, 2018), se describe que, los centros de datos se asemejan a bóvedas virtuales, en donde se almacena la información y se busca conservar la integridad de los datos. Estos centros de datos están expuestos de manera incondicional a ataques cibernéticos, razón por la cual se aplica cimientos subyacentes que están conformados por equipos físicos, los cuales permiten combatir intrusiones dentro de un sistema crítico, mismos que son capaces de ofrecer una solución de seguridad mucho más eficiente; sin embargo, el costo que genera mantener cada uno de estos equipos son costosos, con el tiempo se llegan a devaluar y por motivos de hardware se vuelven propensos a perder compatibilidad con el software que se encuentra en constante actualización y se vuelven obsoletos.

En el libro del autor (Lawrence Miller, 2016) , se menciona que el aumento de tráfico que fluye dentro de un centro de datos y la aparición de la virtualización dentro de los servidores son inclinaciones que han colaborado a una falta de contexto y de visibilidad inmiscuidos en el centro de datos. Por lo general el tráfico que fluye entre servidores no pasan por un firewall, esto hace que no exista una inspección en cada nodo que se encuentra dentro de la red de datos. Al no existir supervisión, para los equipos de seguridad de red el tráfico que circula se vuelve invisible, no obstante, para evitar un tráfico no supervisado se

puede utilizar técnicas como hairpinning[4], cuya utilidad permitía circular el tráfico por un firewall centralizado, sin embargo, estas técnicas pueden generar un cuello de botella que dan como resultado rutas de comunicación ineficientes y complejas que de manera inevitable afectan el rendimiento de la red.

En los entornos de servidores virtuales es común configurar un host físico con varias tarjetas de red. Sin la existencia de VDS todo el tráfico se dirige hacia las máquinas virtuales, esto ocasiona complicaciones en los equipos de red que se encargan de solucionar ese tipo de problemas adheridos, que se convierten en una vulnerabilidad para los atacantes. Durante los últimos años se ha utilizado infraestructura de servidor implementando la filosofía que consiste en aplicar múltiples niveles, teniendo como resultado un tráfico mayor a las comunicaciones de cliente servidor o de internet. Gracias al avance de la tecnología hoy en día se puede gozar de soluciones factibles y aplicables dentro de un centro de datos, con ciertas ventajas sobre una configuración tradicional. De esta manera se logra ahorrar equipos físicos y se puede llevar a cabo soluciones flexibles que a su vez son eficientes dentro de una empresa, esto se logra gracias a la virtualización de red y su función de seguridad llamada por VMware "Micro-segmentación[5]".

---

[4] Hairpinning: "admite una inversión de paquetes describe la conexión entre dos hosts detrás del mismo dispositivo NAT, usándolos para mapear el punto final" (Akers, 2019).

[5] Micro-segmentación: "es una técnica de seguridad de red que permite a los arquitectos de seguridad dividir de forma lógica el centro de datos en diferentes segmentos de seguridad hasta el nivel de carga de trabajo individual y, posteriormente, definir los controles de seguridad e implementar servicios para cada segmento único" (VMware, 2021).

La virtualización de los servicios soporta el desarrollo de varias tecnologías, entre ellas la quinta generación de telefonía movil (5G). Así mismo, permite el desarrollo de varios modelos de negocio como los descritos en (Sacoto Cabrera, Guijarro, & Maillé, 2020) (Sacoto-Cabrera, Guijarro, Vidal, & Pla, 2020) (Sacoto Cabera , 2021) (Sacoto-Cabrera, Sanchis-Cano, Guijarro, Vidal, & Pla, 2018) (Sanchis-Cano, Romero, Sacoto-Cabrera, & Guijarro, 2017) para Operadores Móviles Virtuales (MVNOs) que se sustentan el conceptos de SDN, VNF, Cloud Computing, entre otros. En el mismo sentido, la virtualización de los servicios es la base para el desarrollo de sistemas de Internet de las Cosas (IoT), tal como se describe por los autores en (Vimos, 2018) (Sacoto-Cabrera, Rodriguez-Bustamante, Gallegos-Segovia, Arevalo-Quishpi, & León-Paredes, 2017) (Vimos, Sacoto, & Morales, 2016).

1.4 Problema de Estudio

Durante las últimas décadas se ha venido aplicando el uso de un modelo de red tradicional, cuya funcionalidad es manipulada por equipos encargados de gestionar el uso de la red y la conectividad con servicios alojados dentro de un centro de datos. Este modelo de configuración de red implica diversos factores que se tornan poco asequibles al momento de desplegar una arquitectura corporativa dado que puede presentar poca flexibilidad en comparación a una red definida por software.

El uso de equipos para manejar la red representan una manera de conectar y monitorear una estructura lógica manejada por enlaces de hardware, sin embargo no es la

manera más eficiente de despliegue para un centro de datos, ya que, al tomar en cuenta el avance de la ciencia se puede identificar maneras más ágiles de llevar a cabo estas operaciones, pudiendo generar varias ventajas significativas, entre ellas el ahorro de hardware, centralización de la data y aseguramiento de la red a través de las conocidas SDN. De esta manera se puede conseguir una implementación flexible y con manejo de reglas de seguridad aplicadas dentro del sistema conforme a medidas que permiten tener un control total o parcial de todo el tráfico que se está enviando a través de los diferentes protocolos de comunicación establecidos dentro del centro de datos.

En la actualidad existen nuevos ataques persistentes y sofisticados que afectan la integridad de los datos a través de malware, por esta razón es indispensable generar métodos de solución eficientes para abordar el problema de los intentos de intrusión dentro de los centros de datos. Como se menciona en (FSTJ Editorial Office & Ltd, 2008), centralizar la arquitectura y contar con las configuraciones pertinentes nos permite llegar a tener soluciones ágiles, capaces de mitigar cualquier intento de ataque siempre y cuando esta solución cumpla los criterios para detectar y generar procesos automatizados que permitan eliminar cualquier infiltración dentro de los centros de datos.

De la igual manera no se puede obviar la concurrencia de usuarios que se conectan al internet generando latencia, pérdida de datos e incluso pudiendo llegar a colapsar el sistema por consiguiente con la ayuda de los avances en la investigación y desarrollo de metodologías capaces de administrar de manera centralizada el uso de los recursos es realmente necesario implementar estas nuevas soluciones de despliegue y aseguramiento

que se han venido presentando para así afrontar nuevos retos para el aseguramiento de la información y servicios inmersos dentro de los centros de datos.

1.5 Importancia

Los administradores de los centros de datos y las empresas necesitan asegurar el tráfico que fluye internamente en el centro de datos debido a que el tráfico en los servidores contiene información sensible y es de carácter prioritario. A pesar de que existen varias alternativas que permiten asegurar el tráfico que fluye en el centro de datos, estas soluciones presentan una disminución en la optimización de las conexiones de datos internamente configuradas. Es por eso que este proyecto propone la aplicación de la Micro-segmentación como medida de seguridad a nivel de tráfico este – oeste aplicando cargas de trabajo con políticas que establecen seguridad a nivel individual en cada servicio alojado dentro del centro de datos.

1.6 Objetivos

1.6.1 Objetivo general

Desplegar una solución en redes definidas por software utilizando NSX para aplicar sobre esto Micro-segmentación dentro de una arquitectura de centro de datos, con la finalidad de generar políticas de seguridad que buscan evitar la propagación lateral de los ataques informáticos a una red definida por software.

1.6.2 Objetivos específicos

- Relevar, estudiar y caracterizar propuestas de aseguramiento de un entorno virtual utilizando Micro-segmentación.

- Desplegar una arquitectura centralizada con redes definidas por software utilizando VMware ESXi, VCenter y NSX.
- Desplegar un centro de datos virtualizado que permita asegurar los servicios alojados en el escenario planteado a través de técnicas de Micro-segmentación utilizando NSX.
- Consolidar un protocolo de pruebas que permitan identificar el nivel de seguridad de la red sobre la plataforma virtual.
- Analizar los Resultados obtenidos de acuerdo con la configuración establecida dentro del Centro de datos y generar conclusiones del proyecto especificado.

Capítulo 2

2.1 Estado del arte

En este capítulo se abordará conceptos que abarcan temas fundamentales sobre las redes tradicionales, los problemas ocasionados por ser estáticas, lentas para el cambio, heterogéneas, su falta de flexibilidad y administración distribuida. Adicionalmente se da a conocer conceptos necesarios para comprender nuestro proyecto y el tema central que es la virtualización de red en los centros de datos, considerando sus ventajas y desventajas y como esta tecnología disruptiva le brinda un nuevo enfoque y abre paso a nuevos retos en los centros de datos.

Los protocolos diseñados para lograr robustez en el Internet fueron diseñados en los años 60 y han funcionado bien hasta el día de hoy, sin embargo, en la actualidad el Internet de las cosas, las redes celulares y la creciente demanda de servicios en la nube requieren de cambios en tiempo real, de una administración centralizada y además de la independencia de un proveedor, es decir que se puedan programar interfaces abiertas y personalizadas de acuerdo a las necesidades de las empresas y no de los fabricantes de hardware, las redes tradicionales son altamente estáticas y solo cambian bajo un estricto control distribuido en la inteligencia de cada dispositivo como Routers y Switches. Adicional, las redes tradicionales no pueden atender la creciente necesidad del tráfico este-oeste en los mega centros de datos y los diversos patrones de tráfico con escala absoluta, dado que las tecnologías de red comunes son simplemente inadecuadas para escalar a los niveles requeridos. Se iniciará desde el nivel más básico por tal motivo es necesarios entender los componentes funcionales de un diseño basado en software hasta llegar a la virtualización de la red de en el centro de datos.

2.2 Virtualización

La virtualización consiste en el uso de una entidad de hardware conocida como anfitrión que permite crear un ambiente lógico capaz de simular recursos que pueden ser asignados de manera heterogénea a cada elemento inmerso en el centro de datos, por ejemplo, almacenamiento, máquinas virtuales, servidores, redes y aplicaciones. En consecuencia, se obtiene una forma para reducir gastos en cuanto al uso de recursos físicos que comprenden equipos de hardware los cuales consumen demasiada energía y a la vez

facilita el manejo de las Tecnologías de la información (Information Technology – TI) de forma eficaz, de manera que se produce mayor agilidad y eficiencia para las empresas (VMware, 2020).

Por lo tanto, (Gonzales Río, 2014) menciona en su libro que la virtualización consiste en abstraer recursos de manera centralizada sobre una infraestructura física permitiendo una combinación entre el hardware y software. Esta estrategia hace posible la integración y el uso de recursos compartidos. De esta manera se puede lograr que varias máquinas sean ejecutadas de forma simultánea sobre un mismo recurso físico encargado de proporcionar de manera lógica procesamiento y distribuciones de disco a cada máquina virtual agregada sobre la plataforma del hipervisor.

2.2.1 Tipos de virtualización

El autor (Márquez, 2011) en su documento de investigación considera a la virtualización como una capa de software que es insertada sobre el hardware permitiendo al anfitrión tener diferentes recursos asignados de manera dinámica y transparente haciendo de la infraestructura de red una solución con múltiples funcionalidades, de tal manera que sea posible adaptar la virtualización a cada necesidad, por tanto se definen diferentes tipos de virtualización sabiendo que cada uno cuenta con características propias que permiten tener un nivel óptimo en su implementación, entre ellos se encuentra la virtualización de servidores, virtualización de red y virtualización de escritorios remotos.

- Virtualización de Servidores

EL autor (Márquez, 2011) menciona que la virtualización de servidores consiste en alojar diferentes sistemas operativos sobre un mismo servidor físico mediante distintas máquinas virtuales que son capaces de otorgar un rendimiento elevado de manera que permita gestionar los recursos asignados a cada máquina de manera lógica a través de software especializado desarrollado por empresas dedicadas o por comunidades que trabajan sobre código open source.

Con el avance de la tecnología también creció la competitividad entre corporaciones de tal manera que el uso de la virtualización sobre hardware se vuelve una ventaja frente al manejo de soluciones comunes que no poseen virtualización permitiendo tener una mayor gestión de procesamiento y capacidad de respuesta optima en diferentes tareas como consultas o manejo de excepciones.

- Virtualización de Red

De acuerdo con los autores (Becci, Morandi, & Marrone, 2020) la virtualización de red al igual que en una red física permite desplegar componentes de interconexión, pero cuenta con mayores ventajas operativas dado que combina los recursos de software con los recursos de hardware tomando como centro una unidad administrativa. Con la virtualización de red también es posible crear routers, Switch, hubs, los mismos que pueden ser gestionados por el panel de administración de modo que admite asignar recursos

específicos a cada uno de los componentes y administrarlos de manera centralizada de tal manera que puedan ser monitoreados constante.

Las redes virtualizadas se pueden derivar en tres abstracciones básicas constituidas por el reenvío, estado distribuido y configuración. En cuanto a la abstracción de estado distribuido presenta una visualización global de la red que hace transparente al administrador de red la topología que comprende el conjunto de componentes que a su vez está constituido por muchas máquinas. Basado en la documentación de (ORACLE, 2014), la abstracción de reenvío permite al administrador precisar cómo se comportan las tramas de reenvío aun cuando existe un total desconocimiento en cuanto se refiere al hardware del proveedor y la abstracción de configuración o de especificación busca expresar los objetivos de red general simulando la forma en que se realiza en una red física.

- Virtualización de escritorios remoto

La virtualización de escritorio remoto consiste en crear máquinas virtuales para los usuarios de una empresa, estas máquinas virtuales son de gran capacidad y tienen como propósito brindar los recursos que de acuerdo con el sitio de (VMware, 2020) son accedidos mediante un software desde los llamados terminales tontos. Este servicio permite a las organizaciones brindar respuestas a las necesidades de manera más rápida, a su vez genera mejores oportunidades al poder adaptarse a entornos cambiantes.

2.2.2 Importancia de la virtualización

(VMware, 2020) en su sitio web afirma que la virtualización de un centro de datos permite asignar recursos heterogéneos con funciones compartidas entre los dispositivos virtuales, de tal manera que impulsa diferentes proyectos omitiendo la preocupación que se pueda generar referente a las limitaciones de hardware tomando en cuenta las utilidades de una arquitectura virtualizada cuyos recursos destinados a los hosts simulan máquinas físicas. Se puede quitar o agregar máquinas dinámicamente de un grupo y pueden ser administradas como un todo. En consecuencia, es posible automatizar tareas a través de una administración centralizada pudiendo obtener mayor flexibilidad operativa, así es posible adaptarse de manera rápida a los cambios del mercado.

El abastecimiento de las máquinas virtuales resulta mucho más fácil y ligero que de las máquinas físicas, esto gracias a la capacidad de crear una nueva máquina virtual en cuestión de segundos en la cual se puede instalar inmediatamente un sistema operativo con las respectivas aplicaciones, de esta manera se puede gestionar la carga de trabajo de manera individual. Es posible también inducir una máquina aprovisionada con el sistema operativo y aplicaciones preinstaladas mediante el proceso de importación.

Los recursos se distribuyen para las máquinas virtuales de acuerdo con las políticas establecidas por el administrador. De acuerdo con (Márquez) establecer políticas que distribuyan los recursos de manera eficiente puede garantizar el rendimiento de un host, de igual manera las políticas permiten establecer niveles de seguridad necesarios para la integridad del sistema.

La importancia de la virtualización se basa en los aspectos que brinda al centro de datos permitiendo al servidor estar compuesto por hardware dedicado en el cual va a ser instalado el hipervisor considerando su almacenamiento y recursos para la virtualización de manera que se permite optimizar el costo de la inversión o mayor aprovechamiento de los recursos actuales. Mediante la virtualización se consigue agrupar los recursos de infraestructura comunes y dejar atrás el modelo heredado de “una aplicación por servidor” gracias a la consolidación de servidores.

2.2.3 Definición de hipervisor

El autor (Márquez) menciona que el hipervisor es un software especializado que se instala sobre un equipo dedicado, entre sus funciones consta crear diferentes ambientes virtuales con diversos sistemas operativos, en consecuencia, es posible tener un control global de todos los sistemas virtualizados a la vez que permite aplicar varias técnicas para su administración. Al existir un software que se encargarse de los procesos de la virtualización es posible administrar los recursos y establecer parámetros de configuraciones para el manejo de los procesos incluso en caliente, esto se da gracias a que existe un hipervisor que se encarga de separar la capa física de la lógica y a la vez es capaz de asignar recursos heterogéneos a todas las maquinas que van a estar compartiendo los recursos de un host especifico.

2.2.4 Tipos de hipervisor

Los hipervisores pueden clasificarse en 2 tipos los cuales apuntan a diferentes estrategias y propósitos de implementación según los requerimientos establecidos por el administrador, a continuación, se detalla el concepto de cada uno de ellos:

- Bare-Metal

El hipervisor bare-metal es ejecutado directamente sobre el hardware y tiene como característica principal ser de carácter nativo, es decir, para su implementación no es necesario contar con un sistema operativo instalado previamente, así lo menciona (Ortiz, 2019).

- Hosted

El autor (Ortiz) refiere que el hipervisor de host tiene como característica principal que se ejecuta con la ayuda de una aplicación en un sistema operativo permitiendo emular otros sistemas. En este caso, además del hardware es necesario contar con características de virtualización en el equipo y las versiones de Sistema Operativo adecuadas.

2.3 Concepto de centro de datos definido por software

Los centros de datos de datos definidos por software tienen como fundamento ampliar los conceptos de virtualización de servidores como marco de referencia de sistemas centralizados en donde la abstracción de hardware y la segmentación de los recursos dentro del Centro de datos son el principio de la virtualización enfocada en el desarrollo de la optimización de los recursos físicos para administrarlos de manera eficiente con el uso del software. El uso de centros de datos definidos por software ofrece diferentes ventajas, entre

ellas la consolidación de sistemas hiper-convergentes[6], reducción de energía, menos costos de espacio, independencia de hardware, abstracción y pools de recursos, estos aspectos se convierten en soluciones eficientes para el manejo de un centro de datos centralizado dado que presentan elasticidad de acuerdo con los servicios implementados. Según (Hamburger, 2016) la virtualización de servidores ha permitido que el uso de hipervisores se convierta en un centro de fácil manejo de servicios, en base al traslado de la inteligencia x86 a la capa de virtualización. De esta manera la infraestructura física únicamente se encarga de su función como backplane[7] en donde se maneja el throughput[8] y ancho de banda necesarios, sumándose a la conectividad a nivel de hardware.

[6] Hiper-convergente: "Es una infraestructura definida por software que separa las operaciones de la infraestructura del hardware del sistema y las converge a nivel de hipervisor en un bloque único (y, por tanto, hiperconvergente)" (Hewlett Packard Enterprise, 2021) .

[7] Backplane: "Es una placa de circuito impreso que contiene conexiones (ranuras) para placas de expansión y permite la comunicación entre todas las placas conectadas" (EFRAM, 2015) .

[8] Throughput: "Es la cantidad de datos que se pueden transferir desde el origen al destino dentro de un período de tiempo determinado" (DNSstuff, 2019)

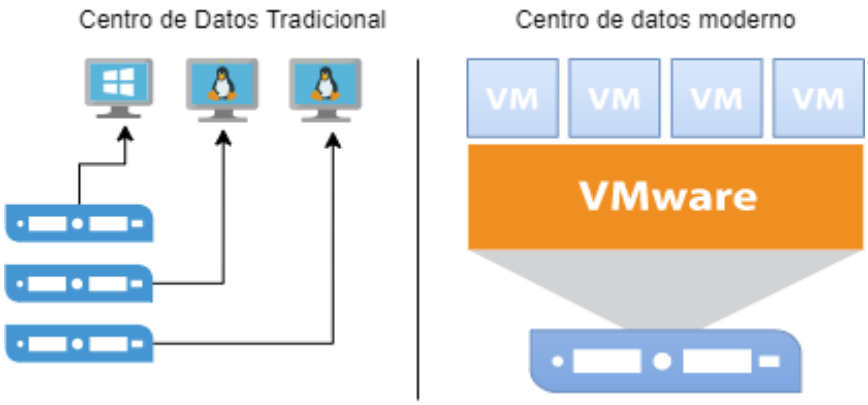

Ilustración 1 Comparativa entre centro de datos tradicional y centro de datos definido por software

2.4 Importancia de virtualizar el centro de datos

La virtualización de los centros de datos permite colocar aplicaciones, sistemas operativos, middleware en las distintas máquinas virtuales alojadas bajo la supervisión del hipervisor. Según (Lawrence Miller) la virtualización de centros de datos al final convierte las tareas en cargas de trabajo con opciones que resultan de gran utilidad al momento de manipular máquinas virtuales y llevar a cabo acciones de migración, creación o incluso clonación de cada máquina creada. Si bien es cierto, el hecho de virtualizar un centro de datos no implica que está libre de los ataques informáticos, sin embargo, al contener todos los recursos centralizados es posible gestionar de manera oportuna cualquier acción no autorizada que se pueda generar dentro del centro de datos.

Tal como da a conocer (Vincentis, 2017) en su libro, virtualizar un centro de datos permite establecer perímetros de seguridad adicionales ante posibles intentos de intrusiones informáticas dado que, al no existir un nivel de seguridad relativamente sofisticado, el atacante puede moverse a través del centro de datos sin complicaciones, logrando modificar o robar información. A pesar de que se aplica grandes cantidades de esfuerzo y recursos para evitar una infiltración, los hackers continúan aprovechándose de las vulnerabilidades presentes en los equipos físicos distribuidos que forman parte de un centro de datos, pudiendo instalar malware[9] y tomar el control o moverse lateralmente en todo el centro de datos. Entonces, es imprescindible contar con las garantías suficientes que permitan el aislamiento e integridad a nivel de físico y lógico aumentando de forma significativa la capacidad de confianza y la gestión de sistemas dentro de un entorno virtualizado.

Según (Chang, 2018) otro factor importante de la virtualización del centro de datos es la simplificación de la arquitectura basadas en el uso de servidores físicos dado que permite la optimización de los recursos y la gestión centralizada de los componentes que se encuentran en el centro de datos. A la vez, presenta la capacidad de escalamiento y alta disponibilidad con costos reducidos a diferencia de la implementación basada en equipos de hardware. Por tanto, el uso de la virtualización en los centros de datos resulta muy útil

[9] Malware: "hace referencia al software malicioso e incluye cualquier sistema de software que afecte los intereses del usuario" (Red Hat, 2021).

para las empresas ya que permite un crecimiento significativo de su sistema pudiendo gestionar de manera óptima los servicios que ofrece.

2.5 Virtualización de la red

Para la gran creciente cantidad de información y surgimiento de aplicaciones de internet existe una demanda de múltiples recursos por lo tanto (Faizul , y otros) mencionan que es necesario el uso de una plataforma con infraestructura subyacente eficiente capaz de soportar el despliegue de aplicaciones y servicios de red. Como se ha venido mencionando, las arquitecturas que comprenden los centros de datos en la actualidad carecen de beneficios que permitan contar con un soporte eficiente de calidad de servicio, la carencia de flexibilidad es otro de los factores que hacen del centro de datos con redes tradicionales menos utilizables a diferencia de un centro de datos con redes definidas por software. Teniendo en cuenta estas deficiencias que se suman a la poca capacidad de administración y defensa ante ataques informáticos se puede decir que la virtualización de la red en un centro de datos representa una solución efectiva para disuadir los problemas mencionados, además presenta otras ventajas que abarcan los temas de flexibilidad y escalabilidad en donde es posible tener una gestión centralizada y están previstas para proporcionar un mejor uso de los recursos evitado la exageración en el uso de la energía.

2.5.1 Definición de Virtualización de la red

Según (Lawrence Miller, 2016) la virtualización de la red es la integración entre los recursos de red de software y hardware en donde tienen como punto de gestión una única unidad administrativa centralizada. La virtualización de la red tiene un nuevo enfoque que permite una gestión y administración flexible y ágil debido a las grandes cargas de tráfico que se generan en la red de datos es necesario

2.6 Tecnologías que comprenden la virtualización de Red

2.6.1 Virtualización de Funciones de Red (Network Function Virtualization - NFV)

La NFV emerge de manera significativa en el mundo de las redes. Comprende un área de la tecnología que influye vigorosamente en el uso de la red, por lo tanto, permite un manejo eficiente de la infraestructura implementada en donde la red virtual puede ser diseñada, implementada y administrada con un enfoque que deja atrás el uso de dispositivos de hardware tradicionales. A la vez, el uso de NFV trae consigo ventajas que de acuerdo con (Zhang, 2018) implican el aprovisionamiento según la necesidad requerida por funciones de red adicionales, que incluyen eficiencia, escalabilidad a la vez que generan ahorro en el costo de implementación y operación.

La NFV está basada en el concepto de virtualización de servidores y contiene un concepto bastante apegado a la virtualización de centros de datos con una variante significativa que de acuerdo con (Zhu, Scott-Hayward, Jacquin, & Hill) permite incluir dispositivos de red, de igual manera brinda la capacidad para monitorear, aprovisionar y

administrar las entidades virtualizadas que sustituyen los dispositivos físicos. En efecto, el ecosistema de NFV comprende los dispositivos de red virtual junto con las herramientas de administración y la infraestructura que familiariza los componentes de software con el hardware subyacente de tal manera que puede ser implementada en cualquier disco duro genérico que brinda recursos de almacenamiento, trasmisión de datos y procesamiento.

2.6.2 Redes Definidas Por Software – SDN

La Unión Internacional de Telecomunicaciones (UIT) en su recomendación UIT-T Y.3300 de (Union Internacional de Telecomunicaciones, 2014) define a las SDN como : "un conjunto de técnicas que posibilitan programar directamente, orquestar, controlar y gestionar recursos de red. Lo cual facilita el diseño, la entrega y la operación de los servicios de red de una manera dinámica y escalable". De esta manera se puede decir que el uso de las redes definidas por software hace posible la implementación de entornos de red dinámicos mediante la aplicación de configuraciones basadas en interfaces abiertas que posibilitan tener una red escalable gracias a la abstracción del hardware cuya interconectividad de forma tradicional es totalmente estática.

En el mercado actual existe una gama de implementaciones de controles SDN ya sea de código abierto o comerciales. En cuanto se refiere a los controladores SDN de código abierto (Nadeau & Gray, 2013) presentan diversas maneras de implementación, a partir de

controladores basados en lenguaje C como NOX[10] o implementaciones basadas en el lenguaje JAVA, por ejemplo, Floodlight[11] o Beacon[12]. De esta manera se vive la experiencia de una amplia gama de posibilidades aplicadas con una combinación en donde no está ausente la heterogeneidad con los equipos ante un previo proceso que permite establecer confianza generalizada dentro de la arquitectura. Un controlador puede soportar más de una aplicación SDN a la vez que una arquitectura de control debe ser capaz de enfrentarse a posibles dificultades de seguridad, latencia, alta disponibilidad, incluso escalabilidad.

Sobre un controlador SDN se ejecutan aplicaciones que incluyen redes definidas por software capaces de interactuar por la parte norte con las instancias atribuidas a administrar el flujo programado en la red. Mediante la gestión del uso de las redes definidas por software se puede configurar los flujos que permiten realizar el enrutamiento de los paquetes buscando la mejor ruta, a la vez se puede equilibrar las cargas de tráfico mediante distintas rutas hasta llegar al conjunto de puntos finales. Mediante la administración dentro

---

[10] NOX: "Fue el primer controlador OpenFlow escrito en C ++ y también proporciona una API para Python. Ha sido la base de muchos proyectos de investigación y desarrollo en la exploración inicial del espacio OpenFlow y SDN" (Coker & Azodolmolky, 2021).

[11] Floodlight: "Es un SDN Controller desarrollado por una comunidad abierta de desarrolladores, muchos de los cuales de Big Switch Networks, que se utiliza con el protocolo OpenFlow para orquestar los flujos de tráfico en un entorno de redes definidas por software (SDN)" (SDxCentral Studios, 2014).

[12] Beacon: "Es un controlador OpenFlow rápido, multiplataforma, modular y basado en Java que admite operaciones tanto basadas en eventos como con subprocesos" (Erickson , 2013).

de las SDN permite revisar cambios en la topología de red y a la vez monitorizar si existen fallas en los enlaces o unión de nuevos dispositivos.

2.6.3 Desafíos de SDN

- Latencia

Según (Göransson & Black, 2014) en su libro señala que al existir el control de un sistema centralizado cuyos componentes se encuentran bajo una capa de virtualización es probable que se genere latencia en diferentes componentes alojados en el servidor, sin embargo uno de los objetivos de SDN en los centros de datos es llevar esta latencia que pueda existir a su nivel más bajo permitiendo así tener un control real de la red sin experimentar perdidas al momento de generar instrucciones de ida o vuelta. El retraso que puede tener en la red se podría generar por el servidor ya que este debería poder atender las solicitudes de manera oportuna y eficiente, si esto no ocurre puede generar una latencia tan insignificante a nivel de la red que puede llegar a ser despreciable, aun así, considerar la latencia en un ambiente definido por software es importante y representa un desafío crítico para las SDN.

- Escalamiento

El escalamiento y la capacidad de un mismo controlador para manejar todos los dispositivos a lo largo del servidor virtualizado es algo que en un principio se puede establecer como incierto teniendo en cuenta que aun cuando existe un solo panel de control se puede crear dispositivos a voluntad y requisitos para que la red funcione con rutas

optimas, sin embargo, de acuerdo con (Göransson & Black, 2014) es difícil saber qué tan bien un sistema centralizado puede manejar cientos, miles o decenas de miles de dispositivos de red y saber cuál es la solución cuando el número de dispositivos de red supera la capacidad del controlador para manejarlos.

- Alta disponibilidad (HA)

La alta disponibilidad es una de las principales características que se tiene en cuenta en los centros de datos ya sea por rutas alternas o centro de administración, estos no pueden ser un único punto de control ya que al momento de existir una falla en el sistema o en uno de los nodos puede llegar a colapsar la red en general, esto implica la necesidad de esquemas redundantes que (Göransson & Black, 2014) en su libro describe como rutas alternas y equipos de respaldos que permitan en caso de alguna falla conectar el servicio de manera automática. De esta manera se puede obtener implementaciones confiables capaces de mantener un sistema siempre disponible para los clientes que accedan a él. Seguridad

Al tener un servidor dedicado los ataques de seguridad pueden centrarse en ese único punto de falla y esto genera la posibilidad de que este tipo de solución sea más vulnerable a los ataques. Es por eso por lo que (Göransson & Black, 2014) menciona que es necesario definir acciones de protección planificadas de modo que se pueda establecer perímetros de seguridad capaces de mitigar los intentos de intrusiones en la red, haciendo posible la protección del centro de datos y sus componentes de tal manera que se pueda

generar confianza en el envío y recepción de datos tanto para el controlador centralizado como para la comunicación entre los dispositivos de red.

2.6.4 Características de las redes definidas por software

A medida que las redes definidas por software han venido evolucionando se puede identificar algunas de las características fundamentales, mismas que (Vincentis, 2017) las clasifica en automatización de redes y virtualización, control centralizado, apertura, separación de planos y dispositivo simplificado. De igual manera que en una máquina física, también las máquinas virtuales cuentan con su Tarjetas de Interfaz de Red Virtual (Virtual Network Interface Card - vNIC). Las aplicaciones y sistema operativo pueden establecer comunicación mediante un controlador de dispositivo estándar también conocido por VMware como controlador, de esta manera cada vNIC cuenta con su dirección de Control de Acceso al Medio (Medial Access Control- MAC) y dirección ip siendo capaz de responder al protocolo de Ethernet al igual que una Tarjeta de Interfaz de Red (Network Interface Card - NIC) física. Resulta importante mencionar que desde el exterior es imposible que el agente pueda identificar si se está comunicando con una máquina virtual o física.

Otra de las características de las redes definidas por software es que diferentes conmutadores virtuales pueden ser conectados a través de un adaptador de Ethernet físico, esta función permite dividir la carga de tráfico y conmutar en caso de existir alguna interrupción en la red. Con el uso de las redes virtualizadas en conjunto con las vNIC se

llega aabarcar en el concepto que maneja una Switch Virtual (Virtual Switch – vSwitch), el cual contiene diversos puertos virtuales que permiten la conexión a una misma red dentro del entorno virtual incluso si las máquinas virtuales se encuentran alojadas en diferentes servidores físicos. Este conjunto de puertos puede ser manipulados para poder gestionar el tráfico y aplicar políticas que permiten asegurar a mayor detalle el tráfico en la red basándose en el concepto de segmentación de red.

2.6.5 Diferencia entre una red física y una red definida por software

De acuerdo con la investigación llevada a cabo por (Mcnickle, 2014) en un dispositivo que soporta SDN las tablas de flujo son conformadas por el conjunto de esturas de datos, en esta tabla se pasa a examinar el paquete entrante para posterior tomar las acciones necesarias en función a las medidas proporcionadas dentro de la evaluación. Dichas acciones tratan al paquete y pueden dar la instrucción de reenvío hasta un puerto específico, propagar el paquete hacia todos los puertos o en su defecto descartar el paquete. Al ser un proceso genérico y programable mediante la lógica asociada a las tablas de flujo no presenta una gran diferencia entre las redes de hardware.

Al poner en marcha la implementación que comprende dispositivos de software existe un reducido conjunto de limitaciones en cuanto a los recursos se refiere, a que la potencia del procesador y la memoria necesaria no conforman un problema en implementaciones comunes. En una implementación de software existe mayor flexibilidad y permiten generar instrucciones más complejas a diferencia de una implementación

basada en dispositivos de hardware gracias a sus características que permiten la manipulación de conexiones desde un punto de control en donde se encuentra la red centralizada.

2.6.6 Importancia de las redes definidas por software

Los equipos que involucran puntos de red se han implementado durante varios años de forma correcta. Tanto enrutador, conmutadores, repetidores han sido usados en grandes proporciones dentro de varios entornos cumpliendo de manera satisfactoria su función de reenvío y filtrado de paquetes en cada destino final. No obstante, y tomando en cuenta el historial positivo de estas tecnologías tradicionales, la complejidad y tamaño de despliegue en la actualidad los dejan con mucho que desear. De acuerdo con (Nadeau & Gray, 2013) Entre las causas que buscan la migración de las redes tradicionales a las redes definidas por software se encuentra, los costos que genera operar equipos dentro de una red, la innovación necesaria en redes y sobre todo la gran cantidad de demanda para un centro de datos moderno. Durante este capítulo se menciona las tendencias y brinda rasgos sobre la razón por la cual los métodos de conexión de red tradicionales se están alejando del ámbito tecnológico dando paso al nuevo paradigma que comprende una orientación más amigable y escalable SDN.

Conforme ha pasado el tiempo, los dispositivos que forman parte de la red se han vuelto más complejos, esto es por causa de la creación de nuevos diseños y sofisticados sumados a la inteligencia integrada dentro de ellos. Así pues, los dispositivos de red han

venido generando nuevas funcionalidades que simplifican la administración de las condiciones de conectividad derivando en soluciones con alta eficacia, sin embargo, proporcionar este tipo de simplicidad puede complicar la dificultad de implementación. Es por esto por lo que el uso de SDN representa un reinicio para el diseño de dispositivos inmersos dentro de la red, esto lo afirman los autores (Nadeau & Gray, 2013) en su libro. En esencia, la simplificación de manejo de la red da paso al manejo de redes definidas por software en donde el punto más importante consiste en controlar los recursos informáticos a través de software de manera centralizada, teniendo como principal ventaja poder ver toda la red y de este modo tomar decisiones acertadas una vez que se tenga una comprensión avanzada de los eventos que suceden en cada situación. Pese a que el modelo SDN es similar en algunos aspectos al modelo distribuido, este segundo modelo cada vez se vuelve menos funcional debido a la creciente complejidad de las redes actuales aun cuando tienen un gran nivel de simplicidad, automatización y facilidad de uso.

2.7 Servicio de Orquestación

El manejo de la virtualización de funciones trae consigo un aspecto importante denominado Orquestación de Servicio el cual permite crear aplicaciones de red compuestas por recursos heterogéneos capaces de ejecutar implementaciones tecnológicas, no obstante, es necesario definir políticas de seguridad que reafirmen la seguridad de la red en un mundo

cambiante permitiendo incursionar hacia nuevos desafíos de seguridad enfocados en el control de acceso.

Como afirma (Márquez) el servicio de orquestación permite el desarrollo de nuevos servicios de red a través de la interconexión de funciones de red virtual, de esta forma se genera la gestión del ciclo de vida de una petición y se permite la reutilización de software. El servicio de orquestación trae consigo todo un proceso que se encarga de; recibir una solicitud de ejecución de una aplicación de red específica para seguidamente incluir y encadenar las VNF en la aplicación con el orden específico de acuerdo con la solicitud del servicio, luego crea las instancias de máquinas virtuales permitiendo la ejecución de las VNF requeridos sin olvidar optimizar el uso de los recursos utilizados. La siguiente instrucción consiste en interconectar las VNF con la implementación de conmutadores y enrutadores encargados de dirigir el tráfico, finalmente supervisa la petición de recursos para analizar si es necesario escalar los recursos hacia arriba o hacia abajo.

2.8 Integración SDN y NFV

Resulta muy importante controlar la forma en que interactúa cada una de las aplicaciones dentro del entorno de red para evitar el uso exagerado de recursos disponibles en entornos NFV/SDN, a la vez es necesario inspeccionar que los recursos sean asignados de manera adecuada de tal manera que exista la capacidad suficiente para interrumpir cualquier propagación ocasionada por aplicaciones de red maliciosas cuyo cometido es

provocar que se vea afectado el comportamiento de la red. La integración entre NVF y SDN hace posible la virtualización de la red dado que trabajan en conjunto para lograr el cometido que es crear dispositivos de red virtuales y controlarlos para el funcionamiento. Estos dos conceptos de virtualización de red tienen relación directa tal como se evidencia en la *ilustración 2*.

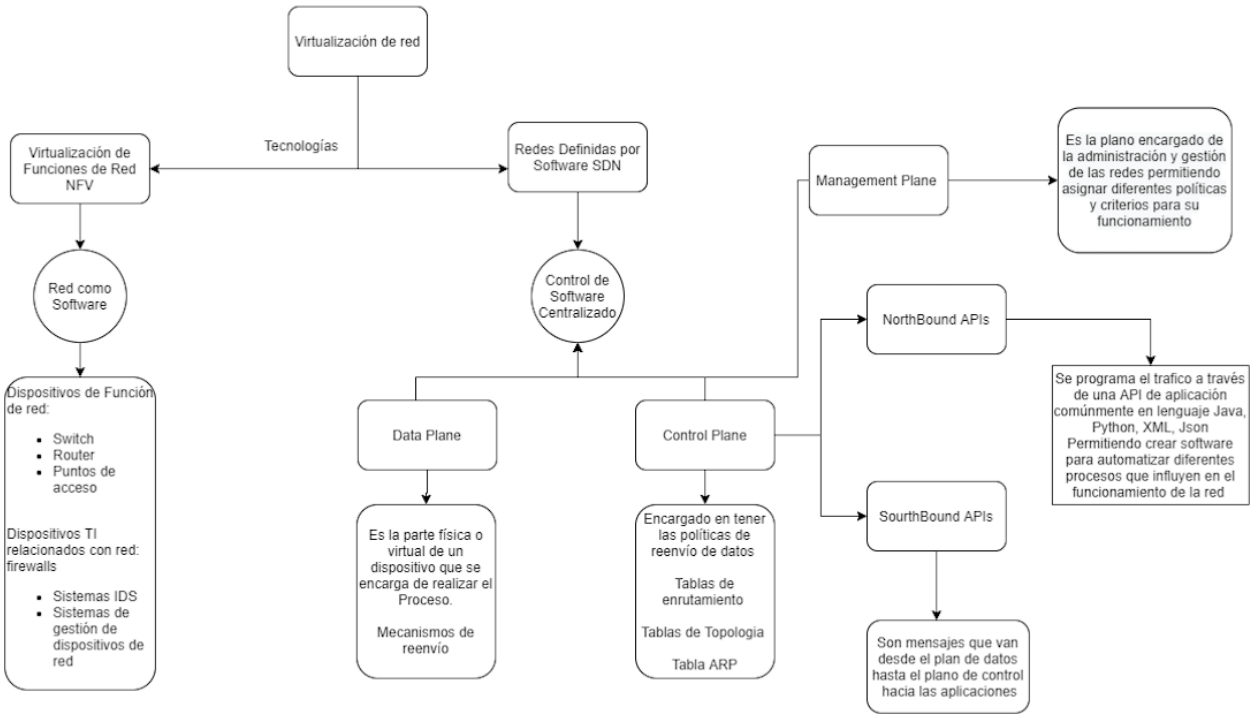

Ilustración 2 Entendiendo NFV – SDN y sus componentes

La industria implicada en la virtualización ha propuesto arquitecturas de referencia que permiten integrar SDN y NVF. La Fundación de Redes Abiertas (Open Networking Foundation - ONF) estandariza OpenFlow y pone en función el contexto que abarca el uso

de un controlador SDN junto a NVF como gestor de recursos de red a fin de que se genere una especial atención para fines de seguridad. Basado en estas arquitecturas el autor (Kerner, 2018) menciona que la implementación de la Virtualización de funciones de red y redes definidas por software optimizan las capacidades de red al ofrecer un control de funciones de red que hacen uso de software que reemplaza los middleboxes[13] gestionados mediante hardware. De esta manera es posible abarcar los crecientes requisitos de red diseñados en función a la programabilidad del software desarrollado para ofrecer despliegues de red flexibles capaces de otorgar acceso parcial cuya funcionalidad se encarga de evitar comportamientos maliciosos de los atacantes dentro de la infraestructura de gestión NVF y SDN.

Las NVF representan un nuevo paradigma dentro del entorno de telecomunicaciones ya que permite el uso de servidores genéricos para el alojo de máquinas virtuales, esto evita la adquisición de hardware dedicado que es sumamente costoso. Otro factor importante radica en que no es necesario comprar equipo adicional para desplegar nuevos servicios dentro del centro de datos pudiendo escalar y reducir nuevas implementaciones de servicios de red según la demanda, funcionando de manera similar a los servicios que actualmente prestan los proveedores de computación en la nube pública.

[13] Middleboxes “Se lo define como cualquier dispositivo intermediario que realiza funciones distintas de las funciones estándar normales de un enrutador IP en la ruta del datagrama entre un host de origen y un host de destino” (Carpenter, 2002).

El uso de SDN facilita la implementación y gestión de NFV gracias a su funcionalidad que dirige el tráfico de acuerdo con las funciones de cada segmento de trabajo en donde se permite modificar la cadena de servicio de manera simple al crear de forma adicional instancias de máquinas virtuales y hacer uso de SDN para reenviar instrucciones de control de tráfico.(Khondoker, 2018) Si se hace referencia a un enfoque de red tradicional, el administrador necesariamente debe incluir un proxy para la división de tráfico y reenvió de tráfico de acuerdo con las rutas asignadas. Con el uso de NFV junto a SDN únicamente es necesario agregar la llamada función de red virtual proxy y posteriormente actualizar las reglas de protección. De este modo la flexibilidad de la red aumenta de forma significativa al centralizar la gestión de la infraestructura de red.

Capítulo 3

3.1 Estudio de los riesgos de seguridad que afectan a los centros de datos

El centro de datos tiene diferentes riesgos potenciales por tal motivo en este capítulo se tratará sobre las amenazas fiscas y lógicas que pueden afectar a la correcta actividad de la empresa, de esta manera se podrá comprender el funcionamiento de los posibles ataques existentes a través de software. De igual manera se describirá la importancia de contar con medidas de contención ante los posibles riesgos físicos a los que está expuesto un centro de datos de una empresa.

Si bien es cierto, los centros de datos presentan vulnerabilidades lógicas que pueden desencadenar en una gran cantidad de problemas para la empresa pudiendo incluso provocar un bajo rendimiento del sistema o pérdida total de la información sensible, no obstante existe software especializado que facilita la identificación de estas vulnerabilidades lógicas que permiten adecuar nuestro centro de datos brindando la robustez necesaria para mantener el sistema en producción, por lo tanto, es necesario encontrar formas de protección que permitan tener los datos asegurados. Como primera línea de seguridad se considera al firewall el cual consiste en un sistema cuya finalidad es

mitigar los ataques destinados al centro de datos, de igual manera se presenta las ventajas y desventajas a considerar con el uso de este sistema de protección. Para concluir este capítulo se describe uno de los softwares de protección llamado Trend Micro Deep Security el cuál se dedica al aseguramiento de centros de datos que gracias a su orientación hacia ambientes virtuales tiene un enfoque primordial hacia el control de ataques informáticos dirigidos a servidores, máquinas virtuales e incluso actúa ante ataques basados en red permitiendo generar reportes recibidos por los agentes instalados en cada host sin tener incidencias directas que causen impacto sobre los recursos de red en uso.

3.2 Identificación de los riesgos que pueden surgir dentro del centro de datos

Un centro de datos debe ser protegido ante las amenazas de manera integral junto con los componentes que están sostenidos dentro de él ya que según comenta el autor (Gómez Vieites, 2014) no existe un único punto de ataque que puede ser aprovechado por intrusos para posteriormente generar conflictos que pueden resultar catastróficos para una empresa, estos ataques aprovechan vulnerabilidades que ponen en riesgo la integridad de la información ya que puede ser extraída de forma física directamente desde los servidores o a través de uno de los diversos ataques existentes en la actualidad. Dicho esto, se describe la clasificación de las amenazas en dos tipos: Amenazas Físicas y lógicas.

3.2.1 Amenazas Físicas

El autor (Gómez Vieites, 2014) menciona en su libro que las amenazas físicas son ajenas a intentos de intrusión generadas por hackers, sin embargo, pueden ser muy peligrosas y es necesario tomar las debidas normas de protección para mantener el funcionamiento de los sistemas sin conflictos. Entre los riesgos físicos se encuentran los cortes del suministro eléctrico, robos, destrucción de los equipos, condiciones atmosféricas o catástrofes ya sea de índole natural o artificial. De este modo se engloba los posibles casos de riesgo que también forman parte de la seguridad informática asumiendo que no son menos relevantes que las amenazas generadas por software. En consecuencia, también se puede realizar análisis de riesgos que determinan las acciones que deben ser tomadas de acuerdo con cada situación antes descritas para evitar daños generados por alguno de los riesgos ya mencionados.

3.2.2 Amenazas lógicas

Por otra parte (Gómez Vieites) menciona que las amenazas lógicas surgen en base a programas de software creados de manera intencionada con la finalidad de incrustarlos dentro de nuestro sistema pudiendo poner en riesgo la integridad de la información. Incluso las herramientas de seguridad pueden representar un arma de dos filos, la razón es simple: de igual manera que el administrador busca detectar los fallos en su red o sistema completo un intruso puede realizar la misma acción en busca de fallos para aprovechar y atacar a los equipos. Para realizar este tipo de barridos que ayudan a determinar la criticidad de un centro de datos se utilizan herramientas como NESSUS u OPENVASS. Por otro lado, están

los riesgos generados por puertas traseras o atajos que son insertadas por el programador durante el desarrollo de aplicaciones o sistemas operativos, aunque no son las únicas amenazas, también están presentes las llamadas bombas lógicas habituadas dentro de ciertos programas de software y a pesar de estar sin realizar ninguna actividad pueden ser activadas con la intención de perjudicar el funcionamiento del centro de datos.

Entre las amenazas lógicas también se cuenta con los canales de comunicación ocultos, estos permiten transferir información a canales locales o remotos a través de canales de comunicación que violan las políticas de seguridad aplicadas al sistema. En los centros de datos existen vulnerabilidades de los cuáles se aprovechan los ataques actuales debido a los pocos puntos de control de seguridad implicados en un perímetro del centro de datos.

3.2.3 Descripción de ataques comunes que afectan el funcionamiento del centro de datos

En la actualidad existe una gran cantidad de ataques que pueden ser aprovechados por los hackers para vulnerar un sistema informático, es por lo que resulta de vital importancia entender cuáles son y como afecta cada uno de ellos al funcionamiento del sistema integrado que conforma el centro de datos. A continuación, se menciona algunos de los ataques más conocidos en la actualidad, si bien se puede encontrar una gran cantidad

de información la siguiente sección se centrará en dar una breve definición de cada uno de ellos.

Gusano

Según (Fernandez, 2020) este tipo de ataque destaca por hacer uso de técnicas de propagación tanto activas como pasivas, se basa en un sistema operativo y luego se encarga de infectar a los nodos alojados a su alrededor. Cuenta con diversos vectores de transporte y es capaz de desencadenar un conjunto de instrucciones que son críticos para sistemas vulnerables. De esta manera el malware puede verse propagado en la red generando un caos dentro del centro de datos, tanto que si no existen acciones necesarias puede conllevar a la caída del sistema existente.

Virus

De acuerdo con lo mencionado por (Fernandez) en su artículo los virus son programas con contenido malicioso, cuyo objetivo es ejecutar instrucciones que buscan infectar a otros archivos que están inmersos dentro del sistema con la finalidad de modificar e incluso generar daños dentro del sistema informático que ha sido infectado.

Troyano

Según el artículo escrito por (Fernandez, 2020) el uso del troyano consiste en disfrazar archivos maliciosos en archivos o programas que se usan habitualmente para engañar a los usuarios. El objetivo de este malware es infectar el host y causar daño, de este modo es capaz de crear una puerta trasera que permite de dar acceso remoto desde el exterior de la red al equipo infectado.

Ransomware

Se lo conoce como un software específico que infecta el ordenador y concede a el hacker la capacidad de secuestrar la información del equipo de tal manera que el host se vuelva inaccesible para los usuarios. Por lo general, el objetivo del rasomware según (Fernandez, 2020) consiste en pedir recompensas a cambio de liberar el software secuestrado.

Denegación de Servicio (Denied of Services – DDoS)

Es uno de los ataques más conocidos y más propagado en la red según comenta el autor (Fernandez, 2020), debido a que es capaz de generar aglomeración de tráfico consumiendo toda la capacidad de procesamiento del servidor que puede derivar en una pérdida total del servicio. Sufrir un ataque DDoS causa interrupciones en los componentes del centro de datos en donde se tiene como consecuencia que el destino se vuelve inaccesible para los usuarios.

Arp Spoofing

En el libro escrito por el autor (Costas Santos, 2006) se menciona que el objetivo de este ataque consiste básicamente en suplantar la identidad de otra máquina ubicada en el segmento de red, de esta manera consigue acceso a los recursos de un sistema adherido que ha determinado alguna relación de confianza basada en la ip del equipo que fue suplantado.

Vlan Hopping

Este tipo de ataque consiste en la disponibilidad con la que cuenta el atacante para poder enviar el tráfico entre Redes de Area Local y Virtuales (Virtual LAN - vlan) que se encuentran distribuidas a lo largo de la red así lo establece (Ariganello, 2014) en su libro. Este tipo de ataque se puede lograr por diferentes métodos, entre ellos están: Método de etiquetas dobles y la suplantación de identidad del conmutador.

3.3 Herramientas utilizadas para el análisis de vulnerabilidades destinadas a centros de datos

Existen diferentes herramientas capaces de analizar vulnerabilidades en el centro de datos sin embargo se tendrá un enfoque de tres de ellas que basados en su comunidad brindan una gran gama de opciones a la hora de realizar tesis que permiten tener un informe detallado de todo lo relacionado a la seguridad en el centro de datos.

3.3.1 Nessus

En el libro enfocado en Nessus, escrito por el autor (Rogers, 2011) se encuentra que esta herramienta consiste en un software robusto multiplataforma de escaneo remoto de vulnerabilidades que se adapta fácilmente a las redes empresariales. Es un software de código abierto, razón por la cual es el programa adecuado en términos de presupuesto, además detrás existe una gran comunidad de desarrolladores actualizando de manera continua las bases de datos de este sistema de rastreo. De esta manera funciona mediante consola o de manera gráfica en donde muestra la información que va recopilando. Es

importante mencionar que también existe una versión pagada de Nessus que incluye complementos desplegados bajo un motor de escáner dedicado. A través de la consola Nessus es posible programar escaneos ligados a cron.

3.3.2 OpenVas

Los autores de (Möller & Haas, 2019) indican que OpenVas está conformado por un marco que incluye diferentes herramientas y servicios que presentan un modelo de solución integral de tal manera que se produce un escaneo de vulnerabilidades completo teniendo como principal propósito encontrar puertos abiertos dentro de un sistema. De este modo este escáner de vulnerabilidades cuenta con diferentes funciones enfocada en el centro de datos. Entre las funciones incluye pruebas no autenticadas, pruebas autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, ajuste de rendimiento para escaneos a gran escala y un potente lenguaje de programación interno para implementar cualquier tipo de prueba de vulnerabilidad.

3.3.3 RanSim

Herramienta de pago por excelencia que pertenece a la empresa KnowBe4, consiste en uno de los softwares más utilizados por las grandes empresas para el análisis de vulnerabilidades. Como lo indica el la empresa (Knowbe4) encargada del desarrollo de la

herramienta Ransim, este software realiza un análisis de puertos y a la vez simula la inyección de diferentes malware a la infraestructura que está siendo puesta a prueba para determinar la criticidad que existe en el entorno sistemático de la red, de esta manera es posible identificar vulnerabilidades presentes permitiendo a los administradores tener un enfoque importante para poder aplicar perímetros de seguridad según lo amerite la necesidad.

3.4 Definición de Firewall

Según (CISET, 2020) el Firewall consiste en un sistema sofisticado cuya funcionalidad radica en permitir o prohibir el acceso no autorizado dentro de una red, además son la primera línea de defensa de seguridad que se interpone ante las amenazas. Existen firewalls lógicos y físicos cada uno de ellos con características particulares que serán tratadas más adelante.

3.4.1 Tipos de Firewall

- Nivel de aplicación de pasarela: “Aplica solamente para aplicaciones específicas consideradas riesgosas, como servidores FTP o de intercambio libre de información entre usuarios (P2P). Suele ser muy eficaz, pero impone una merma en los recursos del sistema” (Raffino, 2020).
- Circuito a nivel de pasarela: “Vigila el establecimiento de conexiones TCP o UDP a través de sesiones de seguridad” (Raffino, 2020).

- Cortafuegos de capa de red: “Opera en base a la inspección de las direcciones IP y el intercambio de paquetes IP, empleando para ello datos alternos como la dirección MAC” (Raffino, 2020).
- Cortafuegos de capa de aplicación: “Opera ya en base a las aplicaciones, controlando su manera de alcanzar la Internet, por ejemplo, mediante Proxys” (Raffino, 2020).
- Cortafuegos personal: “Cortafuegos elegidos por el usuario e instalados en el sistema para atender a los requerimientos individuales de uso del sistema” (Raffino, 2020).

3.4.2 Ventajas de utilizar Firewall

Existe una gran cantidad de casos en los que piratas informáticos se aprovechan de las vulnerabilidades que presenta un centro de datos debido a la falta de implementación de un firewall, por lo tanto, la principal ventaja con la que cuenta el firewall es la capacidad de proteger un centro de datos de las amenazas externas. En base a lo mencionado en la página de (CISET, 2020) se puede decir que tener un firewall instalado permite que el administrador de red pueda tener control sobre la seguridad de la red ya que es el encargado de habilitar los puertos específicos que permiten la comunicación de datos entre los servicios alojados en el centro de datos. A continuación se detallan las características que hacen del firewall un sistema con ventajas significativas frente a las amenazas informáticas.

- Control del tráfico: El control de tráfico cumple la función de analizar los paquetes que atraviesan en la red, detectar cualquier amenaza y bloquear cualquier tipo de tráfico sospechoso.
- Seguridad anti-hackers: Los individuos dedicados al hacking se encuentran permanentemente buscando vulnerabilidades en el internet y un centro de datos no puede exponerse a estos peligros, el firewall se encarga de proteger la privacidad de la empresa ante los posibles intentos de piratería.
- Protección antimalware: Los malware se han convertido en una amenaza latente para la integridad de la información y no solo de las empresas, también de los usuarios que acceden al internet. Tener un firewall instalado puede evitar el alojamiento de archivos dañinos dentro del host a la vez que bloquea el ingreso de archivos sospechosos.
- Control de acceso: el firewall puede generar políticas de restricción o acceso a aplicaciones, de igual manera que puede restringir el tráfico que circula en la red, esto ayuda a la asignación de privilegios que permiten minimizar el riesgo ante infiltraciones no deseadas dado que bloquea la información de Servidor de Nombres de Dominio (Domain Name Server – DNS) para posibles sitios dañinos.
- Privacidad. A través de la red se puede suplantar identidades o acceder de manera imperceptible hasta la información de los usuarios, es por esto que la implementación de un firewall es crucial para prevenir la sustracción de datos propios de un cliente, el uso de la cámara, manipulación del equipo, etc.

3.4.3 Desventajas de utilizar Firewall

El firewall es capaz de bloquear el intento de intrusiones en la red de una empresa, sin embargo, existen formas en las que puede incrustarse algún tipo de malware siendo desapercibido por el cortafuegos. Se toma el ejemplo de (CISET, 2020) en donde menciona que, si un empleado abre un correo electrónico sospechoso sin tener en cuenta el riesgo que trae consigo, el virus puede propagarse sin inconveniente a pesar de tener el firewall activo. Esta representa una gran desventaja que es bien aprovechada por los hackers informáticos que son conscientes del poco conocimiento de los usuarios sobre estos riesgos potenciales.

Otro de los inconvenientes que trae consigo el uso de firewall es su implementación a gran escala y los esfuerzos que representa mantener un profesional que se encargue de mantener el sistema bajo control. El administrador debe estar al tanto de todo lo que ocurre en la red para poder asistir de manera rápida a eventos sospechosos que surjan dentro del entorno de red. Adicionalmente al costo de operación, el uso del firewall implica otros gastos que incluyen mantenimiento y licenciamiento así se afirma en la página de (CISET, 2020). Quizá estos dos aspectos representan uno de los factores más importantes a tomar en cuenta debido a su alto nivel de inversión económica.

3.4.4 Diferencia entre un Firewall Físico y un Firewall Lógico

Como sistema de protección ante intentos de intrusiones ocasionados por hackers dentro de un sistema informático se consigue considerar dos mecanismos de protección, los cuales son comprendidos por el firewall físico y el firewall lógico. Cada uno de ellos se comporta de manera diferente y cuenta con ciertas ventajas y desventajas, por lo tanto, al momento de elegir qué tipo de firewall a implementar se debe considerar cuál se adapta de mejor manera a las necesidades de la empresa, por consecuente el proceso de elección debe ser debidamente analizado de tal manera que el despliegue e implementación del firewall se pueda llevar a cabo de manera efectiva dentro del centro de datos.

Cuando se habla de un firewall físico se refiere a un dispositivo de hardware, este tipo de firewall representa una opción mucho más cara a comparación de un firewall lógico dado que consiste en un equipo especializado con componentes físicos, cuidadosamente seleccionados por sus fabricantes que hacen de este cortafuegos un equipo con la robustez suficiente que es capaz de administrar el filtrado de paquetes, pudiendo así controlar el tráfico que circula en el entorno del centro de datos (Satasiya & Rupal D., 2016). Al mismo tiempo, el uso de este equipo genera costos de operación y mantenimiento haciendo que la empresa deba asignar un presupuesto elevado para mantener en producción este tipo de firewall. Adicionalmente se debe tomar en cuenta un espacio físico adecuado para que pueda ser ubicado dentro del centro de datos, este espacio va a depender de las dimensiones del equipo. Tomando en consideración lo afirmado por (Vincentis, 2017) se puede mencionar que a diferencia de un firewall lógico, el firewall físico cuenta con un tiempo de vida reducido, esto hace que queden obsoletos en muy poco tiempo debido a la

incompatibilidad con nuevas actualizaciones y ausencia de mantenimiento por parte del fabricante. Esto se debe a que la tecnología cambia constantemente a tal punto que cada vez surgen nuevos equipos con nuevas actualizaciones y considerables mejoras en el rendimiento.

Por otra parte, se cuenta con el firewall lógico, el cual consiste en un programa informático basado en software que es capaz de emular el comportamiento de un firewall físico. Este tipo de firewall permite administrar de manera eficiente las reglas de filtrado con una gran capacidad para realizar cambios en cuestión de accesos dentro del centro de datos, por lo tanto, brinda mayor flexibilidad con respecto al firewall físico. De hecho, existe firewall lógico de código abierto que cuenta con toda una comunidad de desarrolladores que suben actualizaciones y brindan soporte de manera constante. Otra diferencia que menciona el autor (Jimenez, 2019) entre los dos tipos de firewall consiste en la conexión de la red, por lo que se refiere, un cortafuegos de hardware se sitúa entre el equipo e Internet mientras que el cortafuegos de software se sitúa entre el equipo y la red a la se realiza la conexión, sabiendo que existen diferencias en la usabilidad de tal manera que un firewall de software se instala en el dispositivo. En consecuencia, si se toma una portátil o móvil y se lo lleva a otro lugar, la protección va a seguir ahí. En cambio, un firewall de hardware es estático y el filtrado de paquetes se lleva a cabo en el router de borde.

3.5 Trend Micro Deep Security

Es una plataforma completa que se enfoca en asegurar la integridad de los datos dentro de los servidores, por consiguiente, es adaptable y muy eficiente cuando se trata de proteger las aplicaciones y los datos desplegados sobre plataformas virtuales o híbridas. Deep Security representa una opción importante para establecer perímetros de seguridad dentro del centro de datos, haciendo de la infraestructura desplegada, un sistema que cumple con las políticas de seguridad que han sido establecidas por la empresa. De esta manera, en el sitio web de (Trend Micro, 2018) se afirma que el uso de un software capaz de disminuir el nivel de vulnerabilidad del centro de datos puede garantizar un nivel de seguridad avanzado, esto gracias a su funcionalidad que hace posible asegurar perímetros de acuerdo con cada servicio.

Como se muestra en la documentación de Trend Micro, este software cumple con los estándares internacionales de la Organización Internacional de Estandarización (International Organization for Standardization - ISO) 27001, así pues, se rige a las normas establecidas para los sistemas de gestión de seguridad de los datos. Cuenta con acceso remoto a la infraestructura controlado de manera estricta y con monitoreo constante en donde el proceso de autenticación se basa en el uso de certificados y autenticación multifactor, como es el caso del Inicio de Sesión Único (Single Sign On – SSO) que utiliza el Active Directory integrado al complemento de Trend Micro.

Tal como menciona en la documentación oficial (Trend Micro, 2018) Deep Security permite monitorear los registros de seguridad a través de eventos generados por

los módulos de protección de manera que se recopila la información generada en cada nodo, según las cargas de trabajo desplegadas en la plataforma virtual. Los eventos que son generados son receptados por los módulos Anti-Malware, monitoreo, prevención de intrusiones, inspección de registros o firewall para ser analizados y generar alertas automáticas que operan durante las 24 horas durante los 7 días de cada semana. En caso de detectarse algún posible incidente el sistema prioriza las acciones de acuerdo con la amenaza para posteriormente tomar las acciones que corresponden de acuerdo con las configuraciones realizadas por el administrador.

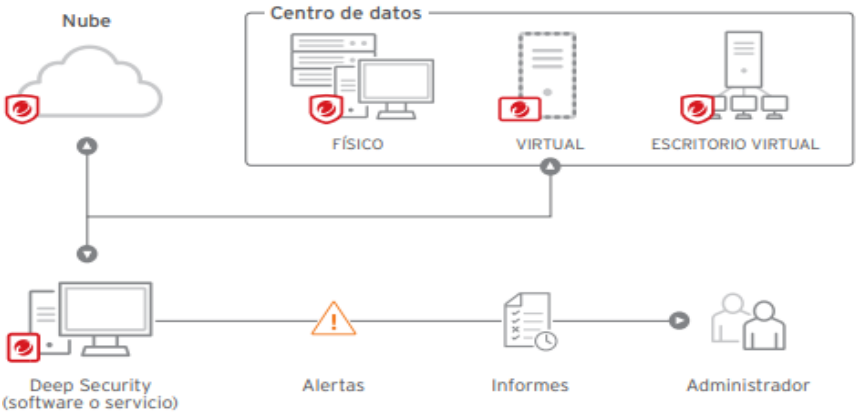

Ilustración 3 Seguridad en un centro de datos (Trend Micro, 2018)

3.5.1 Ventajas de utilizar Trend Micro Deep Security

Deep Security como software encargado de defender el centro de datos de los ataques de malware, de acuerdo con la documentación de (Trend Micro, 2018), esta

herramienta es capaz de llevar a cabo las revisiones de la información en busca de posibles archivos maliciosos sin colapsar el sistema a nivel de lectura/escritura en los discos, a la vez evitando el excesivo uso de la Memoria de Acceso Randómico (Random Access Memory - RAM). El tipo de solución que nos presenta este software de protección se puede apreciar con mayor relevancia en los entornos de virtualización que incorporan componentes sofisticados ya que hacen del uso de la red un entorno denso. Otra de las ventajas que ofrece este antivirus es la prestación de flexibilidad, análisis a nivel de hipervisor y es además es capaz de integrarse con las últimas versiones de la herramienta VMware VCenter encargada de orquestar los recursos del centro de datos desplegados sobre el hipervisor de VMware ESXi. Así mismo, aplica cargas de trabajo dirigidas a los nodos existentes dentro del centro de datos permitiendo el uso eficiente de los recursos en uso.

Este software no presenta una seguridad que se incorpora únicamente a nivel de hardware o software, es todo lo contrario, además de brindar protección de los centros de datos tradicionales se adapta a los sistemas virtualizados de tal manera que se aproxima como stateful firewall y a pesar de que no consigue llegar al nivel de los firewall de nueva generación ya representa una ventaja bastante acertada para minimizar la superficie de exposición al mundo de las redes sostenidos por los sistemas virtuales, así se menciona en la documentación (Trend Micro, 2018).

Muchos de los antivirus que circulan en la actualidad no consiguen parchar sistemas Linux y la razón es que muchas organizaciones ignoran el hecho de la necesidad que representa actualizar lo aplicativos que corren sobre los servidores de software libre. De igual manera, en la mayoría de los casos no existe soporte para sistemas obsoletos que actualmente siguen siendo utilizados en el mercado de la informática teniendo como resultado sistemas altamente vulnerables. Según la información tomada de la documentación (Trend Micro, 2018) Deep Security se encarga de la protección de sistemas como Windows 2000 o diferentes sistemas Linux dado que brinda una solución de parcheado virtual en donde se protege el entorno de forma dinámica de tal manera que no hace falta reiniciar los sistemas virtuales consolidando esta técnica de protección como muy eficiente a la vez que abarca un considerable decrecimiento en los costes.

Continuando con la información recopilada de la página (Trend Micro, 2018) se puede afirmar que Deep Security es altamente eficaz al momento de monitorizar la integridad de los sistemas, de tal manera que está incorporado al ámbito de servidores virtuales, servidores en la nube e incluso servidores físicos, además incluye una tendencia hacia las funcionalidades de protección de Almacenamiento conectado en red (Network Attached Storage - NAS). Esto hace de este software de protección una solución completa para cualquier sistema operativo o entorno virtual.

3.5.2 Desventajas de utilizar Trend micro deep security

Una vez analizadas las ventajas que brinda Deep Security, es necesario considerar los factores que resultan poco favorables al momento de adquirirlo. Como primera desventaja se puede considerar que Deep Security es un software propietario lo cual limita algunas funciones o número de usuarios basado en la licencia adquirida, otra de las desventajas surge al momento de la configuración ya que, configurar sus funciones resulta una tarea compleja y es necesario conocimiento detallado para logra un óptimo funcionamiento. Finalmente, se puede considerar como una desventaja, la implementación de plugins[14] que conectan con plataformas de virtualización. En el caso de VMware NSX pueden ocurrir fallas de conexión o inconvenientes al momento de integrar estas dos plataformas.

[14] Plugins: "es un fragmento o componente de código hecho para ampliar las funciones de un programa o de una herramienta" (NeoAttack, 2020).

Capítulo 4

4.1 Tecnología de VMware para la virtualización de centro de datos

El uso de la virtualización en los centros de datos en la actualidad está en auge, esto da paso al uso de tecnologías capaces de llevar a cabo operaciones automatizadas que dejan atrás las configuraciones tradicionales de una infraestructura empresarial de tal manera que resulta necesario utilizar software dedicado que permita incursionar en este mundo de la virtualización. Como solución a la propuesta de virtualización surge VMware, empresa que brinda toda una gama de soluciones de software, incluyendo la virtualización de servidores de tal manera que es posible gestionar y administrar de manera eficiente el uso del procesamiento, almacenamiento y red haciendo del centro de datos un entorno virtualizado con características que representan ventajas significativas en cuanto al manejo de la infraestructura existente dentro del centro de datos.

Durante este capítulo se define las herramientas que comprenden el ambiente virtual de VMware con la finalidad de entender el funcionamiento de los componentes y la

gestión de procesos que ocurren dentro de la infraestructura virtual desplegada en el centro de datos. De esta manera, se iniciará conceptualizando el hipervisor ESXi como estructura principal de implementación de un centro de datos, también se realizará el análisis de las ventajas y desventajas que ofrece este hipervisor desarrollo por VMware, seguidamente se explicará las funcionalidades del orquestador VCenter el cual permite administrar y gestionar los procesos que se llevan a cabo a través de la integración con NSX y sus funciones de red, de igual manera, en este tema se explicará conceptos y fundamentos de NSX junto a sus respectivas características dentro del ámbito de las redes definidas por software.

4.2 Definición de ESXi como solución de VMware para ambientes empresariales

En el libro desarrollado por (Hamburger, 2016) se postula a ESXi como un hipervisor Bare-metal desarrollado por VMware el cual cuenta con un nivel de virtualización de capa sólida probada de manera eficaz en producción, se ejecuta sobre un servidor físico y tiene como objetivo abstraer los recursos del procesador, almacenamiento, redes y memoria para posteriormente distribuirlos en diferentes máquinas virtuales. Cada uno de los servidores que forman parte de la infraestructura informática es tratado como un host independiente dentro del entorno virtual, sin embargo, se puede agrupar distintos servidores configurados de forma parecida teniendo en cuenta conexiones para la misma red tal como se muestra en la *ilustración 4*.

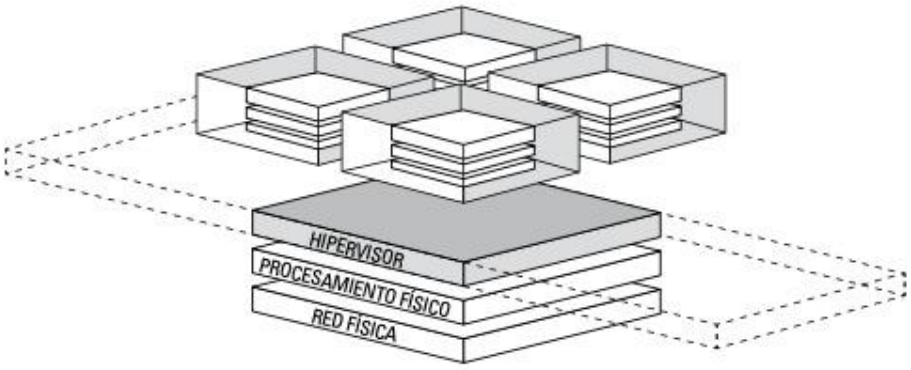

Ilustración 4 Interpretación de ESXi sobre un servidor físico (Vincentis, 2017)

4.2.1 Ventajas de utilizar el hipervisor ESXi en un centro de datos

Según el autor (Haletky, 2011), VMware ESXi es una plataforma de virtualización completa, por ende, ofrece diferentes ventajas significativas que trae consigo para la implementación en un centro de datos virtualizado. Al ser un hipervisor bare metal se encuentra instalado de manera directa sobre el hardware físico, esto permite repartir los recursos entre las máquinas virtuales instaladas de manera heterogénea a tal punto que es posible decidir cuanta memoria ram, almacenamiento, procesamiento o número de interfaces de red virtuales se va a utilizar, sin obviar un previo dimensionamiento que permita optimizar los recursos lógicos para evitar el uso exagerado de los recursos físicos.

ESXi tiene como núcleo una distribución Linux, por lo tanto, presenta un sistema ligero que ha sido modificado por la compañía para simplificar procesos y presentar al administrador del centro de datos una interfaz altamente trabajada para que el uso de la

plataforma sea completamente intuitivo, permitiendo a los usuarios nuevos la posibilidad de capacitarse en el uso de ESXi con el objetivo de formar una comunidad con amplio conocimiento sobre la virtualización tal como enfatiza (Mishchenko, 2010). Sumado a esto, el hecho de formar parte de los productos de VMware te da la alternativa de contar con soporte técnico contratado, de esta manera brinda todas las garantías que ofrece la empresa de VMware cuyo prestigio es muy conocido a nivel mundial.

4.2.2 Desventajas de usar el hipervisor ESXi

La implementación del hipervisor de VMware ESXi trae consigo muchos beneficios, no obstante, cuenta con desventajas que si no son bien analizadas pueden traer consecuencias poco favorables para la empresa, tal es el caso del aspecto económico en donde contratar una licencia con soporte para el uso de este hipervisor representa un alto costo, esto sin tomar en cuenta valores adicionales que se suman cuando se requiere hacer uso de funciones no incorporadas en la licencia original.

Otra de las desventajas de ESXi la menciona (Kuminsky, 2015) y consiste en la compatibilidad presente del software respecto al hardware ya que en la mayoría de los casos VMware desarrolla en conjunto con los fabricantes de servidores para poder optimizar y sacar versiones específicas para cada servidor tanto así que dependiendo la marca y versión puede existir problemas de drivers respecto a los componentes y su gestión desde el hipervisor similar a lo que se observa en la *Ilustración 5* en donde se evidencia el despliegue de una arquitectura tradicional.

Los productos de VMware a diferencia de otras empresas que se dedican a el área de virtualización no cuentan con documentación detallada en línea, lo cual representa un inconveniente al momento de desplegar las soluciones propuestas por VMware de manera que se debe tener un conocimiento previo de lo que se quiere hacer y como se lo debe hacer ya que caso contrario puede presentar varios inconvenientes al momento de desplegarla.

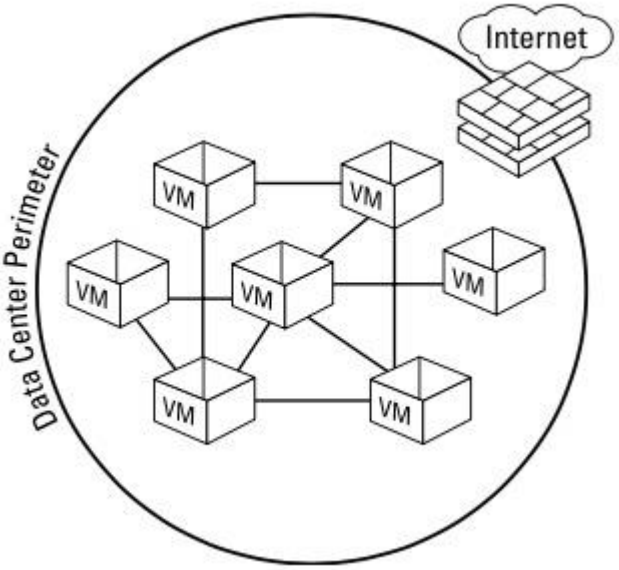

Ilustración 5 Centro de datos virtual sobre ESXi desplegado de manera tradicional (Vincentis, 2017)

4.3 Definición de VCenter Server, como orquestador de ambientes virtualizados

En (Kuminsky, 2015), se define VCenter como un software que se convierte en un punto de control dentro del centro de datos. Ofrece distintos servicios de gran importancia,

siendo estos; la configuración, control de acceso y monitoreo del rendimiento. Otra de sus utilidades consiste en su factibilidad para unificar recursos y posteriormente compartirlos entre diferentes máquinas virtuales. Lo consigue administrando la ejecución de máquinas virtuales en los servidores y la proyección de los recursos destinados a las máquinas virtuales dentro del centro de datos, tomando en cuenta las políticas que son regidas por el administrador del sistema. La *ilustración 6* nos permite visualizar de manera rápida y eficiente como VCenter Server es capaz de gestionar 2 servidores los cuales cuentan con su almacenamiento compartido donde van a ser desplegadas las máquinas virtuales.

4.3.1 Gestor de virtualización de red Plug-ins

VCenter como orquestador se basa en herramientas capaces de realizar el proceso de automatización basado en aplicaciones que son necesarias y se encargan de administrar varios elementos que se encuentran dentro del centro de datos. Por lo general utilizan la Interfaz de programación de aplicaciones ya sea mediante línea de comandos o el Protocolo Simple de Administración de Red conocido como (Simple Network Management Protocol - SNMP); al existir una gran cantidad de proveedores se necesita complementos específicos de adaptación mediante un conjunto de procedimientos y funciones API se logrará desplegar una solución de orquestación optima, la misma que puede tener ciertas políticas de nivel superior que a su vez se ejecutan en niveles inferiores por los complementos apropiados. Los complementos específicos del proveedor se utilizan para convertir las solicitudes de políticas de nivel superior en la solicitud SNMP o línea de comandos nativa

correspondiente específica para cada proveedor tal como se menciona en la conferencia (Wang, Hembroff, & Yedica, 2010).

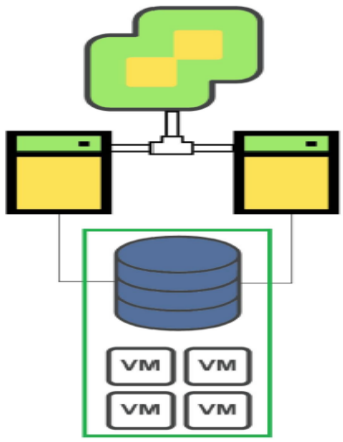

Ilustración 6: VCenter Server (Caballé, Cerda, Cinalli, Herrero, & de la cruz, 2019)

Si por alguna razón Virtual Center tiene algún problema y pierde conectividad el funcionamiento de los servidores informáticos y el entorno virtual seguirán funcionando de manera autónoma y no presentarán un fallo o inconveniente; ya que las máquinas virtuales ubicadas dentro del hipervisor seguirán ejecutándose en base a los recursos fijados con anterioridad a cada una de ellas. Solucionado el problema y se tenga en ejecución el sistema de Virtual Center Server se puede volver administrar el centro de datos nuevamente sin ningún inconveniente mediante la interfaz conveniente, en donde se tiene como opciones VMware Infrastructure Client, acceso web o a través de la terminal.

4.4 Definición de NSX Management

"NSX es una plataforma de virtualización de red que le permite implementar una amplia gama de servicios lógicos de red" tomado de (Caballé, Cerda, Cinalli, Herrero, & de la cruz, 2019). A la vez permite establecer funciones de firewall con inspección del estado de conexión en capa cuatro (stateful) para presentar segmentación a nivel de redes virtuales. Esta plataforma reparte los servicios al vSwitch permitiendo formar una cadena de procesamiento lógico. De esta manera llega a convertirse en un hipervisor de red en donde existe abstracción, control de recursos, flexibilidad y uso de pools de recursos. Es importante, no obviar que NSX se conecta y hace uso de una infraestructura de red que ya existe ofreciendo la ventaja de evitar la necesidad de adquirir más equipos físicos.

Cuando se habla de virtualización de red en base a NSX Management es importante recalcar que se trabaja bajo el concepto de una red lógica, por ende, cabe conceptualizar que no es más que un contenedor basado en software que permite manejar servicios de la red y conectar máquinas virtuales en redes específicas. Partiendo de idea que plasma el autor (Lawrence Miller, 2016) NSX representa una solución clave dentro de la arquitectura de red definida mediante el Centro de Datos Definido por Software (Software Define Data Center - SDDC), de igual manera que un ambiente virtualizado en donde se puede crear, eliminar o modificar máquinas virtuales, VMware NSX permite la virtualización de redes

en donde también es posible crear, modificar, actualizar y eliminar componentes de red lógicos. Como resultado se obtiene una visión del manejo de red en donde no solo es posible manejar un centro de datos con mayor facilidad y agilidad, dado que esta manera permite implementar dentro de la red subyacente un modelo de operación simplificado.

Al virtualizar la red con NSX cuya funcionalidad se asemeja a la de un hipervisor se puede aislar y proteger la integridad de la información de forma arbitraria, esto se debe a que es capaz de encapsular un conjunto de servicios que abarcan las capas dos hasta la siete del modelo OSI, de esta manera se encuentra presente la funcionalidad de enrutamiento, firewall, control de acceso, conmutación, equilibrio de carga. Todo este conjunto de funciones integradas a la virtualización de red mediante NSX brinda un mayor control del flujo de información dentro del el centro de datos.

4.4.1 Importancia de implementar NSX en un centro de datos

En la actualidad es posible encontrarse con diversas implementaciones de dispositivos SDN, tanto de código abierto como comerciales los cuales cuentan con conmutadores heredados y manejo de API que permiten la conexión para acceder a la red, en donde, la API hacia el norte representa una interfaz de bajo nivel que permite el paso a la red de dispositivos de manera consistente. Existen también casos en donde se proporcione una API de alto nivel cuya función implica abstraer la red de tal manera que el desarrollador de una aplicación no tenga preocupaciones por las conexiones virtualizadas, si no únicamente con la red a su alcance. La comunicación ocurre a través de

eventos y surgen desde el controlador hasta la solicitud del dispositivo. Estos eventos se pueden dar dentro de un paquete individual que fue procesado por el controlador o algún cambio de estado en la topología de red.

Distinto a otras arquitecturas heredadas, NSX permite que las redes virtuales puedan verse aprovisionadas, almacenadas, cambiadas e incluso se las puede programar o eliminar sin tener que pasar a revisar el nivel físico, así se obtiene una red desplegada y haciendo uso de todo el potencial otorgado por esta solución de software. Tomando la propuesta de solución que menciona el autor (Vincentis, 2017) la aplicación de NSX sobre un centro de datos virtualizado ha permitido llevar la administración de la red a otro nivel, en donde los cambios pueden realizarse de forma centralizada y programada dependiendo de los eventos que ocurran en el sistema, de modo que el administrador de red es capaz de identificar y mitigar fallos. Basado en esto VMware en la *ilustración 7* nos brinda una vista a una arquitectura básica la cual se logra gracias al uso de NSX con los diferentes componentes que son administradas dentro del entorno VMware.

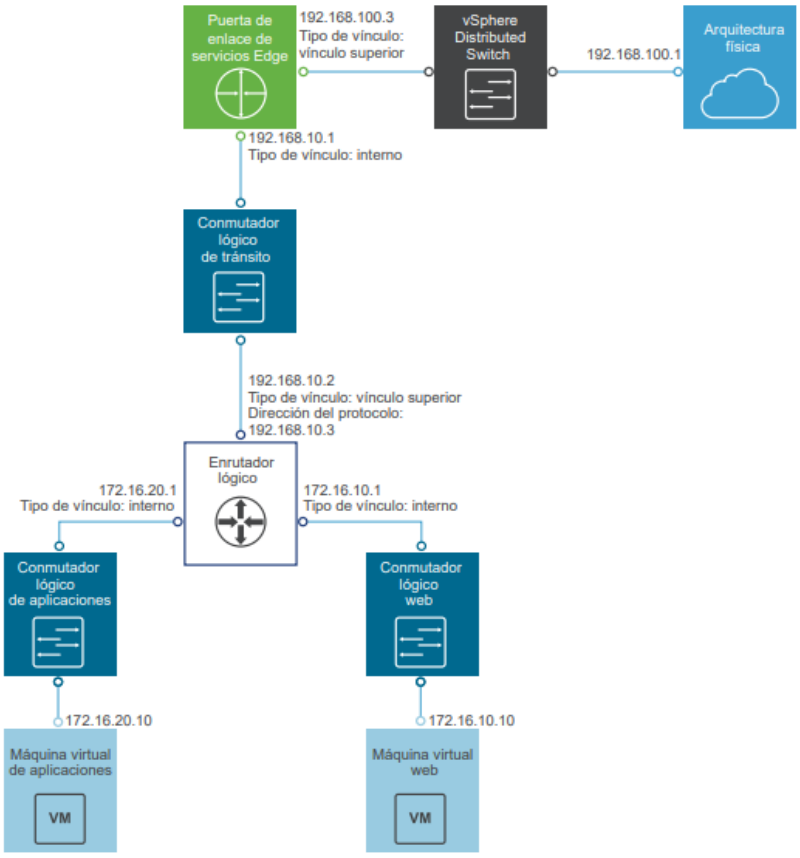

Ilustración 7 Arquitectura básica de una red virtual generada dentro de NSX (VMware, 2019)

Capítulo 5

5.1 ¿Que es la segmentación de red?

La segmentación de la red se ve relacionada al proceso que consiste en dividir o fragmentar una red en varias subredes diferentes de tal manera que es posible aumentar el rendimiento de la red y el número de equipos que están conectados a esa misma red tal como lo afirma (Lawrence Miller, 2016). Por lo tanto, segmentar la red permite crear diferentes segmentos lógicos partiendo de una red principal de tal manera que es posible crear subredes de diferente capacidad. De igual forma, la segmentación trae consigo la capacidad de gestionar una estación de administración de manera descentralizada que forma parte de la subred configurada por el administrador de tal manera que es posible realizar tareas de autogestión dentro de la infraestructura instalada, de este modo el tráfico que fluye entre segmentos divididos trabaja de forma independiente y la comunicación se lleva a cabo solo en caso de ser necesario.

La manera más común de segmentar la red según el blog (Winex, 2017) se da mediante el uso de vlans dado que permiten reducir el dominio y evita que posibles infiltrados vean todos los equipos |conectados a la red o salgan de su dominio asignado, de esta manera se produce una separación lógica a nivel de red de tal manera que se limita el tráfico a través de segmentos a tal punto que se cumple con los protocolos de seguridad que hacen de una red un entorno de trabajo fiable en donde se niegue el acceso a usuarios que no pertenezcan a la vlan correspondiente. Todo esto pasa a nivel de capa dos mediante

Switch y cuando se implementa medidas de seguridad como protección de la red virtualizada.

5.2 ¿Que es la Micro-segmentación?

En (Lawrence Miller, 2016), se manifiesta que la Micro-segmentación es una técnica de seguridad de red que permite a los arquitectos de seguridad dividir lógicamente el centro de datos en distintos segmentos de red de tal manera que al momento de gestionar la red esta pueda ser analizada individualmente su carga de trabajo y luego definir controles de seguridad permitiendo brindar servicios para cada segmento único. La Micro-segmentación permite al administrador de TI implementar políticas de seguridad flexibles en el interior de un centro de datos haciendo uso de tecnología de virtualización de red en lugar de instalar múltiples firewalls físicos. Además, la Micro-segmentación se puede usar para proteger cada máquina virtual (Virtual Machine - VM) en una red empresarial con controles de seguridad a nivel de aplicación y basados en políticas generadas por el administrador. De esta manera y debido a que las políticas de seguridad se aplican a cargas de trabajo separadas, el software de Micro-segmentación puede reforzar significativamente la resistencia de una empresa a los ataques.

Dentro de una red virtualizada, el hipervisor de red se encarga de administrar y supervisar el tráfico que fluye dentro del centro de datos, incluyendo las cargas de trabajo individuales de las máquinas virtuales así lo establece en su blog (Collado, 2016). No fuera posible este nivel de contexto y visibilidad sin la Micro-segmentación gracias a su capacidad de ayudar a establecer políticas de red de manera específica para cada carga de

trabajo pudiendo inclusive generar un registro del entorno virtualizado para poder tomar decisiones más inteligentes. Entre las características de la Micro-segmentación se menciona la importancia de afianzar el despliegue con el modelo cero confianza el cual permite aislar diferentes redes pudiendo limitar el acceso y otorgar el privilegio mínimo de acuerdo con las necesidades de cada usuario conectado a la red, de esta manera se consigue establecer controles de acceso estrictos y proteger los recursos de datos.

"Cualquier red virtual aislada puede estar conformada por cargas de trabajo distribuidas en cualquier parte del centro de datos, y las cargas de trabajo de la misma red virtual pueden residir en un mismo hipervisor o en hipervisores diferentes. Además, las cargas de trabajo en distintas redes virtuales aisladas pueden residir en un mismo hipervisor", así menciona (Vincentis, 2017).

Cabe mencionar que las redes virtuales se encuentran completamente aisladas de la infraestructura física subyacente, esto sucede gracias a la encapsulación del tráfico que existe dentro de los hipervisores dando como resultado una infraestructura de red íntegra y de acceso limitado únicamente al administrador cuyos privilegios de entrada al centro de datos le permitan visualizar los eventos que se van generando. De esta manera se cuenta con un nivel adicional de seguridad en donde las direcciones de la red lógica son totalmente distintas a las direcciones de red que pertenecen a los dispositivos físicos.

5.3 En qué consiste la Micro-segmentación

La Micro-segmentación, al formar parte del centro de datos y ser independiente del host que maneja el usuario final hace que sea posible realizar la configuración de políticas y privilegios que se asignan de acuerdo con la categoría de cada usuario o grupo que pertenezca. De tal manera que independientemente del equipo que se esté utilizando las políticas aplicadas siempre serán las mismas para cada host. En el libro escrito por (Lawrence Miller, 2016) se considera que los administradores tendrán el máximo privilegio que les permite crear, modificar, eliminar y activar o desactivar cada enlace de red, al tener estos privilegios significa que no todos los usuarios deben tener permisos de administrar la red, pues los privilegios deben ser controlados para usuarios y administradores de manera diferente, esto hace que se alcance un nivel de seguridad óptimo gracias a que se implementa un control de acceso a la red basado en credenciales que identifican a cada usuario y permite realizar actividades específicas dentro del centro de datos.

En efecto, la Micro-segmentación ayuda en la creación de redes al generar la DMZ para la seguridad dentro de un centro de datos sabiendo que un centro de datos tradicional está conformado por diferentes nodos que son gestionados mediante el orquestador. Al vincular las políticas de seguridad específicas con cargas de trabajo individuales, el software de Micro-segmentación limita la capacidad del atacante de moverse lateralmente a través de un centro de datos, incluso después de infiltrarse en las defensas perimetrales. Según (VMware, 2020) esto significa que puede eliminar las amenazas de servidor a servidor dentro del centro de datos, aislar de forma segura las redes entre sí y reducir la

superficie de ataque total de un incidente de seguridad de la red. El uso de la DMZ dentro de un centro de datos definido por software se gestiona con cargas de trabajo únicas independiente de su ubicación en la red, eliminando la manera tradicional de dividir el perímetro de seguridad y DMZ en un firewall físico.

5.4 La Micro-segmentación con su modelo cero confianza para la seguridad del centro de datos.

Es importante tomar en cuenta que en el mundo de la informática existen amenazas que constantemente buscan vulnerabilidades dentro de los centros de datos, esto implica implementar estrategias de seguridad sofisticadas y se logra con el uso de la Micro-segmentación, misma que aplica el modelo confianza cero. Según indica (Lawrence Miller, 2016) la combinación de la Micro-segmentación y el modelo permite un nivel de seguridad óptimo como estrategia de protección en diferentes áreas del centro de datos logrando generar un tipo de protección que en el libro (Gilman & Barth , 2017) conta como la técnica de “jamás confíes, siempre verifica” sabiendo que cada carga de trabajo será analizada a un nivel altamente detallado, de esta manera se llega a tener un modelo de control positivo el cual define de manera detallada que tráfico puede fluir en la red y así permite de manera segura rechazar todo el tráfico adicional que no esté definido. Existe la posibilidad de tener un modelo de control negativo el cual se enfoca en delimitar todo el tráfico que no está permitido en la red, no obstante, el tráfico adicional será aceptado.

Cuando se trata de la estrategia cero confianza se puede empezar por el tema del menor privilegio es imprescindible constatar que dé inicio no exista ningún tipo de confianza otorgada a las entidades dentro del centro de datos, esto incluye a los segmentos de red y a la vez las cargas de trabajo que influyen en las aplicaciones y servidor. En (Lawrence Miller, 2016), se postula que para establecer los niveles de confianza es necesario que la empresa sea quien establezca los límites de tal manera que cada segmento pueda ser accedido y controlado según el nivel al que fue asignado. Al mismo tiempo, esta estrategia de cero confianza implica un nivel detallado en donde es requerido el monitoreo e inspección constante del tráfico que fluye dentro del centro de datos a tal punto que es posible identificar actividad sospechosa y detectar amenazas para bloquear la actividad no autorizada. Cuando se habla de confianza cero es necesario revisar cada paquete e individuo que se encuentra en la red permitiendo identificar de manera rápida y segura anomalías en la red, de esta manera, una vez detectada la amenaza se procede a realizar la validación correspondiente la misma que en caso de no ser satisfactoria procederá a bloquear y aislar tanto al host como al tráfico que está emitiendo o recibiendo.

Como razón principal para implementar Micro-segmentación se enfoca en mantener un centro de datos con seguridad eficaz en donde el menor privilegio y confianza cero establecen límites con un nivel de granularidad sumamente preciso y aplicación de políticas adecuadas que verifican la información del tráfico que fluye de norte a sur y de este a oeste dentro del centro de datos. Por lo consiguiente, la aplicación de la Micro-segmentación permite a las empresas acogerse a un plan de seguridad en donde lo

primordial es proteger la información de cada segmento de la red con el uso de la estrategia de cero confianza de manera que la capacidad del atacante se vea extremadamente limitada impidiendo que se pueda mover de forma lateral dentro del centro de datos, así lo menciona (Lawrence Miller, 2016).

5.5 Ventajas de la Micro-segmentación

En un centro de datos definido por software se puede aprovechar la virtualización de redes para suministrar ventajas representativas que revolucionan las estrategias de seguridad de redes tradicionales, una red virtualizada permite tener un centro de datos optimizado en cuanto a la seguridad y rendimiento. A continuación, se presenta una lista que contiene algunas de las ventajas que nos ofrece la Micro-segmentación presentadas en (Lawrence Miller, 2016).

- Costos operacionales reducidos
- Se aprovecha la infraestructura existente
- Servicios de seguridad avanzada y direccionamiento de tráfico
- Flujos de tráfico simplificados
- Reducción de riesgos contra violaciones al centro de datos
- Combinación entre hardware y software pudiendo utilizar el recurso físico para ser usado como distintos recursos lógicos
- Políticas especializadas que permiten tener un mayor control del tráfico
- Capaz de brindar Autorización, Autentificación y Registro.

5.6 NSX como solución de VMware para realizar Micro-segmentación

Como señala (Wilmington, 2019), VMware se centró en revisar las estructuras de los modelos de seguridad comunes a nivel organizacional, como resultado obtuvo que los firewalls perimetrales por sí solos no son capaces de brindar seguridad en cuanto a la comunicación lateral (este - oeste) en donde el propósito sería desarrollar una función que permita segmentar la red de una manera que pueda ser adaptable a las necesidades de los clientes. Según plantea (Lawrence Miller, 2016), esta nueva metodología de protección con control de las rutas de comunicación este – oeste resultó sumamente importante para fortalecer la defensa del centro de datos y ayudar a mitigar los ataques cibernéticos. Si se toma en consideración el control de flujo en los distintos segmentos existentes a través de NSX se consigue realizar funciones de control de políticas de seguridad de manera centralizada, también es posible proporcionar aislamiento y otorgar cargas de trabajo en los hosts con un privilegio de red mínimo de acuerdo con su nivel dentro del sistema organizacional, así lo menciona (Wilmington, 2019).

La red es un factor fundamental en el despliegue de un centro de datos, por lo tanto, la seguridad de ésta no puede verse afectada por ningún motivo. Para ello se hace uso de herramientas que ayudan a gestionar de manera oportuna los eventos que suscitan dentro del entorno virtualizado. NSX como propuesta de solución de VMware permite realizar tareas de monitoreo e identificación de amenazas de manera autónoma y a la vez de forma

segura gracias a su alta gama de funciones que permiten micro-segmentar la red de modo que existe la manera de aislar los servicios en segmentos diferentes con reglas de firewall con parámetros que cumplen los requisitos de protección para cada servicio.

Dentro de NSX, el aislamiento se encuentra relacionado con la segmentación aplicada a múltiples niveles dentro de la red virtual. Cuando se maneja la segmentación de forma tradicional se habla de funciones que le competen a un enrutador físico o firewall diseñado para rechazar el tráfico no deseado entre segmento de red. Si se hace uso de NSX como plataforma de Micro-segmentación de redes se puede establecer funciones de firewall enfocados en la inspección que nos brinda la posibilidad de segmentar la red de forma virtual logrando de esta manera obtener aprovisionamiento automatizado, un rendimiento del firewall con ejecución sobre el kernel[15] y por otro lado se cuenta con un escalamiento horizontal con distribución hacia todos los nodos que incorpora la plataforma que comprende el centro de datos (Collado, 2016).

[15] Kernel: “es el elemento principal de los sistemas operativos, y es la interfaz fundamental entre el hardware de una computadora y sus procesos” (Red Hat, 2020).

5.7 Arquitectura de NSX dentro de vSphere

La solución de VMware NSX representa un conjunto de componentes que realizan funciones encaminadas a la red, así lo refiere (Lawrence Miller, 2016). Por ende. NSX tiene toda una estructura conformada por distintos componentes lógicos capaces de simular el funcionamiento de los dispositivos de hardware de tal manera que la plataforma virtualizada permite distribuir los servicios de red a través del vSwitch, mediante el cual es posible aplicar las políticas de aseguramiento generadas dentro de los componentes de la plataforma de Micro-segmentación, mismas que fueron definidas en las cargas de trabajo que se aplican a los hosts ubicados dentro del hipervisor agrega. A la vez, la plataforma de virtualización de red NSX cuenta con una arquitectura compuesta por distintos planos, entre ellos se mencionan los Plano de Datos, Plano de Control y Plano de Administración. Cada uno de los planos cumple una función específica y hace que sea posible abstraer la red a tal punto que puede ser segmentada y administrada de manera sencilla mediante el orquestador VCenter. En la *Ilustración 8* se puede visualizar como interactúa los diferentes planos.

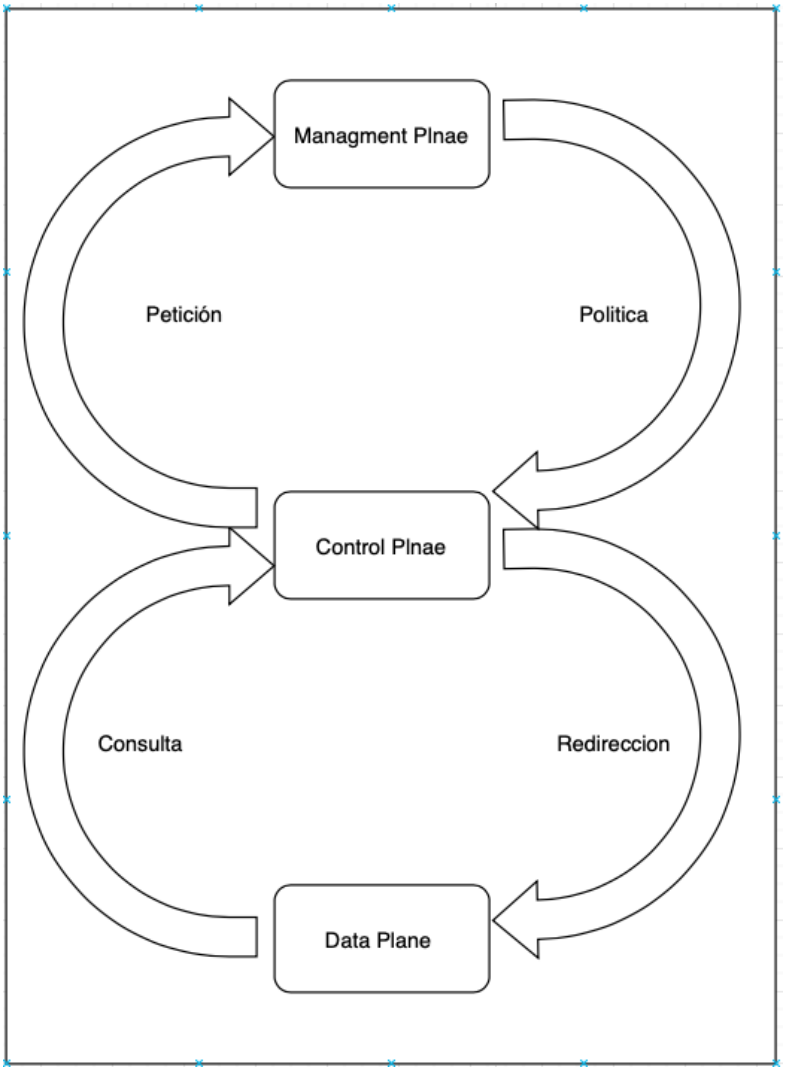

Ilustración 8 Procesos entre plano de datos, plano de control y plano de administración

5.7.1 Plano de Datos

NSX Virtual Switch basado en VSD junto a otros componentes permite habilitar servicios, mismos que conforman el plano de datos. Debido a la abstracción de la red física proporciona conmutación la cual es necesaria para tener una red virtualizada y al mismo tiempo aislada de las redes físicas compuestas por vlan. Según la documentación (VMware,

2019) el plano de datos facilita la implementación y escala el administración de la red a nivel de hipervisores logrando escalabilidad controlada, de la misma manera y no menos importante se puede llevar a cabo el control del estado de la red, calidad de servicio sumado a la facilidad de realizar copias de seguridad que a su vez puede ser restaurada. Adicional, este plano de datos incluye un conjunto de herramientas que presenta agilidad para resolver problemas de una red virtual, no obstante, también se puede supervisar y administrar el tráfico.

5.7.2 Plano de Control

Su ejecución se localiza dentro del clúster de NSX Controller mismo que a su vez representa un software de administración que proporciona funciones avanzadas dentro de un plano de control permitiendo realizar las funciones de conmutación y enrutamiento lógico como señala (VMware, 2019). De esta manera el plano llega a considerarse el centro de control central que abarca todos los conmutadores lógicos que se encuentran en la red al mismo tiempo que guarda la información de los hosts, VXLan y enrutadores lógicos distribuidos. Sobre el controlador se ejecutan las aplicaciones de red, lugar en donde se busca la manera óptima de controlar la administración, distribución dentro de la red, el envío de paquetes de acuerdo a las decisiones generadas anteriormente por el plano de control para las funciones de nivel superior que comprende el controlador y el segmento en donde se alojan las aplicaciones de red, como se menciona en la documentación

(VMware, 2019). Esta implementación incluye como parte determinante el costo que genera desarrollar las etapas de diseñar, construir, adquirir y operación de la red SDN.

Dentro del plano de control no pasa ningún tipo de tráfico de datos de modo que no afecta la conectividad en caso de ocurrir algún error en los nodos. De acuerdo con (VMware, 2019) la función principal del plano de control consiste en distribuir la información desde la red a los hosts y viceversa alcanzando un alto grado de resiliencia. NSX Controller permite escalar a nivel horizontal de manera que es posible agregar nuevos segmentos que a su vez pueden contener hosts y alojar servicios con cargas de trabajo independientes, de forma que se optimiza las rutas de envío de tráfico a la vez que ofrece alta disponibilidad a nivel de red, logrando consolidar un centro de datos eficiente.

5.7.3 Plano de Administración

Como expresa (VMware, 2019), este plano consiste en el punto de administración capaz de mantener la red de NSX centralizada. Se implementa semejante a un dispositivo virtual dentro del host ESXi creando instancias con relación 1 a 1 de manera que se facilita la creación de políticas y proporciona gestión de procesos a nivel de red. Para su total integración se busca tener un control de las políticas que rigen la red LAN las cuales se basan en protocolos que son requeridos para la comunicación y control de tráfico de acuerdo con las necesidades del administrador de red. Este plano interactúa directamente con el administrador y facilita la configuración de los aspectos que influyen en la red como

es el caso de NSX Manager, el cuál crea instancias que son aprovechadas por VCenter Server para la gestión de los componentes lógicos situados dentro de NSX.

Los equipos de red actuales, autónomos son capaces de establecer el plano de control de software, a su vez administrar y almacenar. Esto significa un costo mayor debido a la capacidad de procesamiento requerida y adquisición de software avanzado, a eso se le suma la capacidad de almacenamiento. Según (VMware, 2019) con la red que prevalece en la actualidad existe poca afluencia disponible y como resultado las funciones requeridas para los dispositivos deben ser implementadas por cada proveedor junto a los protocolos que también necesitan ser implementados aumentando de manera circunstancial los costos que se atribuyen al desarrollo de software.

5.8 Componentes de NSX Management

5.8.1 Router DLR

De acuerdo con el blog (Bertello, blog.bertello.org, 2015) el enrutador lógico distribuido es un componente de la plataforma NSX, el cual está optimizado para funcionar en ambientes virtuales realizando el proceso de reenvío de tráfico en la red que va dirigido hacia los grupos de puertos que contienen las máquinas virtuales, el envío se realiza de manera directa o a través de las vlans. Este enrutador dirige el tráfico hacia el enrutador externo permitiendo el proceso de hairpinning, de esta manera es posible administrar las rutas para que el tráfico fluya en torno a la capacidad de reenvío de cada vlan involucrada.

De esta manera se optimiza la fluidez del tráfico este – oeste dado que únicamente transita de extremo a extremo entre máquinas virtuales.

Este enrutador lógico permite añadir hasta ocho interfaces de vínculo superior capaz de emparejarse con un conmutador de capa 2, o un ESG. Del mismo modo, según (Bertello, blog.bertello.org, 2015) este router virtual permite crear hasta mil interfaces internas que se comunican con los VDS que a su vez permite la conexión con las máquinas virtuales instaladas en el software subyacente de ESXi. Es compatible con los protocolos de enrutamiento dinámico Abrir el Camino más Corto Primero (Open Shortest Path First - OSPF) y Protocolo de Puerta de Enlace de Frontera (Border Gateway Protocol – BGP) llegando a comunicarse con NSX Manager y NSX Controller.

Por consiguiente, el enrutador lógico distribuido proporciona aislamiento e independencia en las rutas de acceso a los datos de tal manera que los hosts radicados dentro del hipervisor y ubicados en subredes distintas puedan establecer comunicación entre sí sin tener que pasar a través de una nueva interfaz como sucede en el enrutamiento tradicional. De este modo las cargas de trabajo son capaces de proporcionar información de lo que sucede en la red de forma ágil y evitando atravesar un conjunto de puertos que ralentizarían el transporte del tráfico dentro de la infraestructura de red. Consta de dos componentes esenciales

Plano de control:

En la documentación (VMware, 2019). Se menciona que el plano de control consiste en el elemento proporcionado por la máquina virtual de control, misma que se

encuentra relacionada con los distintos protocolos de enrutamiento e intercambia tramas de datos con el dispositivo virtual de capa 3 como siguiente salto a la vez que establece comunicación con NSX Manager. En el caso de aplicar alta disponibilidad el dispositivo virtual del DLR se comunica con el clúster de NSX Controller a fin de que se proporcione Alta Disponibilidad (High Availability – HA) con la configuración de (activo – en espera) gracias a sus características de proporcionar máquinas virtuales dedicadas a este proceso.

Plano de datos:

Este componente consta de módulos de kernel ligados al DLR, los cuales se ven instalados dentro de los host ESXi siempre y cuando pertenezcan al dominio de NSX. Estos módulos de kernel comparten una similitud con las tarjetas de chasis modular que permiten el enrutamiento insertado mediante el clúster de control. Este componente del router DLR se encuentra equipado con las interfaces lógicas mientras que estas interfaces se conectan con los conmutadores lógicos al igual que con los puertos admitidos por las VLAN.

El Router DLR crea una instancia partiendo de la interfaz que según afirma el autor (Bertello, 2015) proviene desde el cliente de NSX Manager mediante el enrutamiento, de manera que NSX controller con el uso del plano de control dentro de los host ESXi es capaz de agregar las nuevas instrucciones del enrutador, incluyendo las MAC Virtual (Virtual MAC - vMAC), direcciónes ip e interfaces lógicas asociadas al mismo tiempo que la VM de control agrega los caminos IP conocidos por NSX gracias a la conexión que se establece con el uso de los protocolos de enrutamiento. Siendo así, la responsabilidad de distribuir las rutas conocidas de los hipervisores con las máquinas de control de DLR le

pertenece al clúster de controlador, de tal manera que cada nodo persistente dentro de la controladora se encarga de distribuir los datos de la instancia del router DLR con carga distribuida entre los distintos nodos supervisados por la controladora. Finalmente, para que el tráfico salga hacia la red externa los módulos de kernel con tramas de rutas se encargan de gestionar el tráfico para que se del siguiente salto mediante NSX Edge.

5.8.2 Router ESG

De acuerdo con la documentación (VMware, 2019) el ESG es un router lógico el cuál ofrece acceso a diferentes servicios procesados por NSX Edge para el despliegue de la infraestructura de red en donde el tráfico fluye de norte a sur de tal manera que brinda la posibilidad de gestionar: firewall, VPN, hacer NAT, utilizar servicios del protocolo de Configuración Dinámica del Host (Dynamic Host Configuration Protocol - DHCP), alta disponibilidad y equilibrio de carga. De esta manera se facilita el uso de componentes lógicos comprendidos por el entorno virtual para el control de tráfico aplicado a nivel del ESG como gestor de la interfaz de comunicación con la red exterior puesto que los servicios de NSX Edge y reglas de firewall son aplicables para el tráfico que fluye entre las distintas interfaces de red.

El router ESG contiene beneficios significativos, entre ellos destaca la posibilidad de asignación de varias interfaces pudiendo contener hasta diez interfaces usadas para la conectividad con la red interna y a su vez con el vínculo superior, sumado a esto, se puede instalar en el centro de datos diversos dispositivos virtuales cuyas interfaces de tráfico hacia

el sur se conectan con grupos de puertos protegidos y se comportan como Gateway para las máquinas virtuales ubicadas dentro del grupo de puertos a los que se encuentran asignadas. En cuanto a las interfaces de vinculo superior, estas se conectan directamente a los PortGroup de vínculo superior que cuentan con el acceso a la red externa y permiten la configuración de distintas direcciones IP de una red compartida por la empresa para poder realizar procesos que comprenden servicios de equilibrio de carga, Red Privada Virtual (Virtual Private Network - VPN) o Traducción de Direcciones de Red (Network Address Translation NAT).

5.8.3 vSwitch

Guiándonos en la documentación (VMware, 2019) el vSwitch consiste en un software especializado cuya función es crear una capa que permite abstraer el software que opera en los hipervisores permitiendo establecer comunicación entre la red física y los componentes existentes dentro de los servidores. La arquitectura de NSX vSwitch sostiene conmutadores distribuidos también conocidos como VDS de VMware VCenter, estos conmutadores suministran enlaces ascendentes locales que se encargan de gestionar la conectividad de cada uno de los hosts con los conmutadores físicos alojados fuera del entorno de VCenter.

Por consiguiente, el uso de los vSwitch representa la forma de conexión que permite el enlace entre la red física y lógica, sin embargo, el switch distribuido de VMware no tiene compatibilidad con soluciones alternas a VMware. Esto ocasiona que las cargas de trabajo

aplicadas a las máquinas virtuales necesariamente deben encontrarse conectadas al switch distribuido para poder acceder a las funciones y servicios que presenta NSX. Como ejemplo se puede analizar la documentación (VMware, 2019) donde se considera que un VDS pueden contener varios hosts ubicados en diferentes clústeres, no obstante, cada clúster al que pertenece un host en común debe conectarse a un mismo VDS, aunque comúnmente cada clúster se ascia con un único VDS permitiendo simplificar la implementación.

5.8.4 Conmutadores Lógicos

Tomando como referencia la documentación propia de VMwar (VMware, 2019) se menciona que la presencia de conmutadores lógicos dentro de un centro de datos con la plataforma NSX es posible manipular las redes virtuales de capa dos de manera que existe agilidad y flexibilidad de igual manera que ocurre con las máquinas virtuales. A la vez, permite crear nuevos conmutadores lógicos adicionales en caso de ser necesarios generando la capacidad de personalizar el uso de las redes según los requisitos de conectividad necesarios de tal manera que restringir las redes según las limitaciones estipuladas resulta totalmente fiable.

Las aplicaciones utilizadas por las empresas necesitan un aislamiento entre ellas por razones que involucran el aislamiento por errores y la seguridad de la información. Por esta razón resulta muy conveniente el uso de conmutadores lógicos que a su vez brindan la capacidad de establecer conectividad con los puntos finales a través de segmentos

virtualizados que son totalmente independientes a la red física de la red. De igual manera NSX permite crear diferentes conmutadores con dominios de difusión únicos que permiten mayor velocidad y flexibilidad a la hora de su implementación, incluso con características similares a los dominios de difusión que existen en una topología con red física.

5.8.5 Firewall

Brinda opciones de seguridad lógica avanzada para los centros de datos. A diferencia del firewall convencional, con el firewall lógico de NSX se tiene la capacidad de segmentar entidades de forma distribuida, aplicando reglas sobre cada máquina virtual de acuerdo con sus atributos, identidad de los usuarios, objetos u hosts. También permite la creación de la DMZ de acuerdo con las necesidades y aislamiento entre empresas con centros de datos virtuales. De esta manera se puede conseguir un centro de datos centralizado con protección sofisticada en donde según (Lawrence Miller, 2016) cada host cuenta con la ventaja de permitir únicamente el tráfico asignado a cada máquina virtual generando una opción de seguridad adicional a la que se presenta en un firewall de software tradicional. En este proceso de aseguramiento del centro de datos se tiene como principal objetivo definir reglas estructuradas, con supervisión de amenazas a través del tráfico horizontal y con atributos únicos que otorgan una reducción considerable de ataques dirigidos hacia los servidores ubicados en el clúster del hipervisor.

5.8.6 Controller Nodes

En la documentación presentada (Oracle, 2015) menciona que los controller nodes son componentes que forman parte esencial dentro del plano de control dado que contiene servicios encargados de la administración de módulos de encaminamiento de rutas distribuidas y conmutación de paquetes dentro de los hipervisores gracias a su capacidad de administración de sistemas convergentes. Al hacer uso de los nodos controladores NSX es capaz de adicionar funcionalidades, mismas que forman parte esencial de un sistema virtualizado como entorno de red dentro del centro de datos. Algunas de estas funciones se ven reflejadas en la existencia de un plano de control que es capaz de distribuir información del DLR así como de VXLan hacia otros hosts, sumado a esto permite agrupar los nodos de tal manera que existe alta disponibilidad y escalabilidad horizontal, adicionalmente el uso de los nodos otorga redundancia en los clústeres como razón de una división de la información de la red en cada uno de los nodos. De esta manera se consigue excluir la necesidad de contar con soporte de multidifusión en la red física y se obtiene un tráfico fluido y balanceado para cada uno de los hosts involucrados.

Cada nodo de controlador puede contener diferentes funciones encargadas de definir el tipo de tareas que el nodo va a implementar, entre ellas la distribución de cargas de trabajo entre los nodos mediante fragmentación. Para conseguir alta disponibilidad y escalabilidad adecuada el autor (VMware, 2015) menciona que es necesario implementar

un mínimo de tres controladores en cada cluster[16], esto agiliza el tiempo de inactividad que pueda generarse en caso de existir fallas físicas en el host siempre que exista una taza adecuada de escritura y óptimo almacenamiento en el disco de cada controlador.

5.8.7 VXLan

Este componente de NSX según la documentación (VMware, 2019) permite la creación de dominios con la capacidad de gestión de distintos inquilinos que pueden encontrarse aislados dentro de una estructura lógica del centro de datos de tal manera que el cliente pude crear redes lógicas y a su vez redes estáticas que comprenden los límites que existen en la red física. Una red VXLan es usada para el reenvío de paquetes entre los hosts a nivel de capa 2 con la capacidad de difusión de dominios subyacentes de capa 3. Cada clúster contiene su configuración de VXLan en donde cada uno de ellos es asignado a un conmutador lógico distribuido ocasionando que los hosts que pertenecen al clúster queden habilitados para ser reconocidos por los conmutadores lógicos.

El uso de transporte VXLan como se menciona en su documentación (VMware, 2019) proporciona enrutamiento y conmutación lógica, sin embargo, no es necesario la configuración de los parámetros de transporte cuando se trata de la implementación de un

[16] Cluster: “Conjuntos de computadoras unidas entre sí generalmente a través de una red de alta velocidad y que se comportan como si fuesen un único host” (Sities Google, 2015).

firewall distribuido. En el caso de requerir la configuración de VXLan es indispensable proporcionar un grupo de direcciones ip, tamaño de la Unidad Máxima de Transferencia (Máximum Transmisión Unity - MTU), identificador de vlan y un switch distribuido. De esta manera es posible obtener un conjunto de redes aisladas entre sí en donde cada una cuanta con un id de segmento por trama que permite diferenciar las redes lógicas sin tener la necesidad de establecer etiquetas vlan.

5.8.8 Transport Zone

Según la documentación (VMware, 2019), las zonas de transporte son las encargadas de controlar lo host a los que se puede comunicar con el conmutador lógico, sin restricciones de bloqueo entre clústeres dado que varios clústeres pueden pertenecer a una zona de transporte que es capaz de asignar el uso de una red en particular y qué máquinas virtuales pueden estar presentes. De acuerdo con los requerimientos del usuario el entorno NSX es capaz de contener distintas zonas de transporte, así como un clúster es posible que pertenezca a varias zonas de transporte sin embargo cada zona de transporte puede contener un único conmutador lógico.

Capítulo 6

6.1 Despliegue del protocolo de pruebas

Una vez revisado los capítulos planteados en esta tesis, pasando por el estado del arte y entendiendo las bases de la Micro-segmentación se realizó el despliegue de un laboratorio basado en la implementación de políticas de firewall dentro de un entorno virtualizado teniendo como objetivo dar un panorama amplio de lo que se puede lograr gracias al uso de las redes definidas por software y la Micro-segmentación en los centros de datos. En este capítulo se revisa el diseño establecido para desplegar el escenario que nos permite verificar la eficiencia del uso de virtualización de la red como perímetro de seguridad con cargas de trabajo a nivel individual de acuerdo con cada servicio configurado dentro de nuestro escenario de pruebas. EN primera instancia se presenta el diagrama establecido para el protocolo de pruebas de seguridad, junto a los componentes físicos y lógicos presentes en el desarrollo de este proyecto de titulación, seguidamente se procede a describir el direccionamiento ip de los hosts que se alojan dentro del servidor partiendo de nuestro escenario planteado. Una vez entendido la estructura es pasó a revisar los requisitos necesarios para desplegar el protocolo de pruebas y por ultimó se presenta los resultados de los procesos llevados a cabo durante el desarrollo de este proyecto que nos permitieron validar las funciones y características de NSX como plataforma de virtualización de red y Micro-segmentación.

6.2 Topología de red

La topología es una representación gráfica de los componentes físicos y lógicos de la red, generalmente está conformado por equipos como: routers, switch, hub, servidores, entre otros. Así pues, se presenta un panorama detallado en donde se incluyen todos los componentes de la red, incluso las conexiones físicas o lógicas. A continuación, en la *Ilustración 9* se presenta el diseño de la topología de red que va a ser desarrollada en el presente proyecto de titulación en la sección que abarca el protocolo de pruebas.

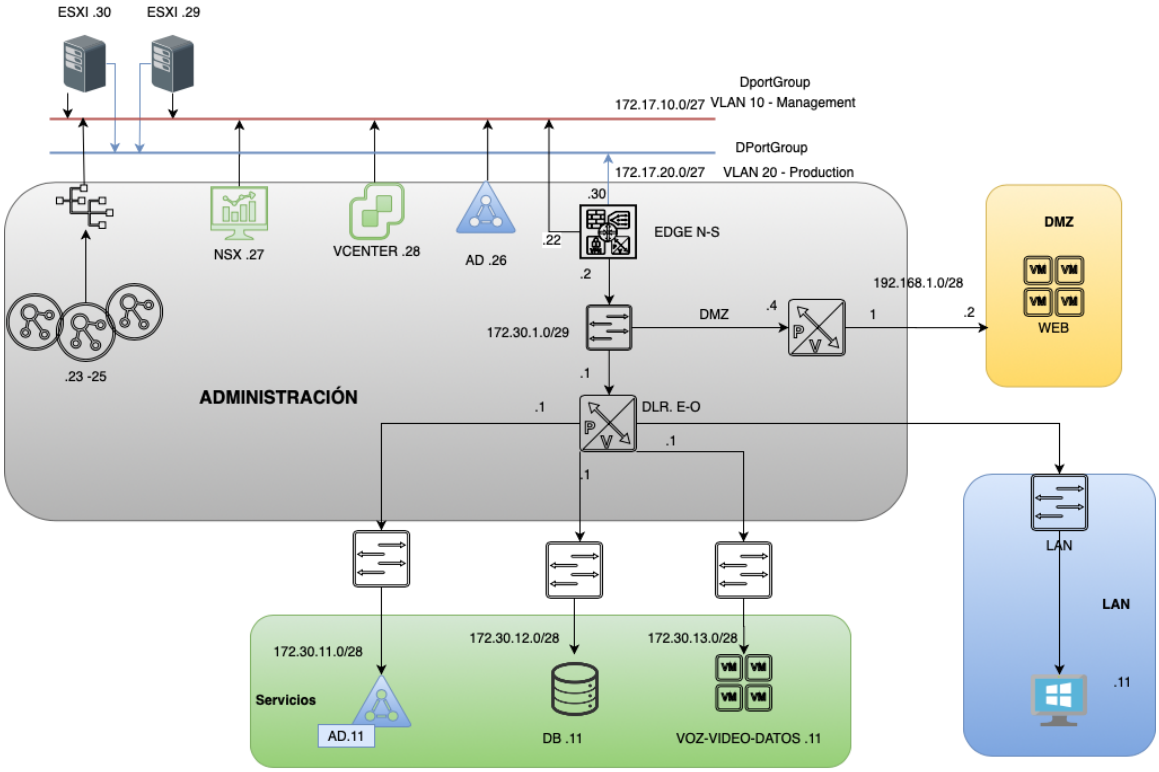

Ilustración 9 Topología de red

Respecto a nuestra topología de red, como se muestra en la *Ilustración 9* se cuenta con dos servidores HPE ProLiant DL160 Gen9 Server con un procesador Intel Xeon CPU E5-2609 v4 1.70GHz, cuenta con 8 procesadores lógicos y 2 NIC además de contar con 32Gb en ram con un almacenamiento de 2 TeraByte. Gracias a los recursos físicos de estos servidores nos es posible utilizar el hipervisor ESXi en cada uno de ellos, los cuáles se encuentran conectados con dos Routers Mikrotik Access Point RB941-2nD-TC, frecuencia de 2.4 GHz y rendimiento de CPU: 650Mhz, mismos que cuentan con las configuraciones de vlans 10 y 20 en los puertos correspondientes. Una vez estructurado la parte física se puede apreciar la segmentación realizado de las diferentes zonas (Administración – DMZ – LAN – Servicios) y gracias a NSX se crea las redes que hacen la intercomunicación permitiendo el tráfico Norte a Sur y Este a Oeste como se muestra en la ilustración 10.

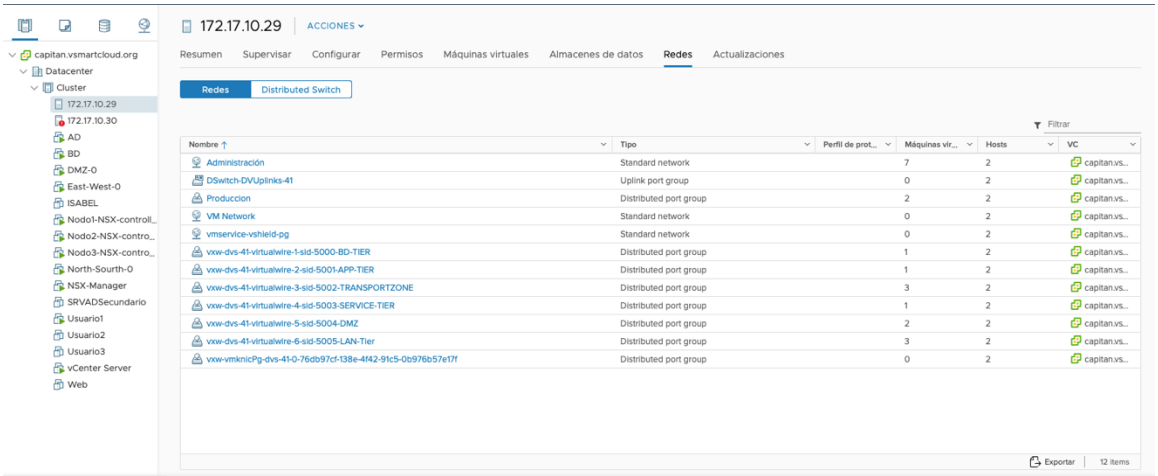

Ilustración 10 Redes Segmentadas por NSX

Conociendo los servicios y después de haber realizado el respectivo levantamiento de requerimientos para el despliegue de nuestra infraestructura de pruebas y haber realizado el dimensionamiento que se necesita para que se dé el correcto funcionamiento y evitar que no exista saturación de recursos durante el desarrollo de las actividades. Una vez analizados los requerimientos se da paso al despliegue de los servicios y configuraciones de red para posterior a ello aplicar Micro-segmentación. En la *Ilustración* 11 se muestra la topología física que está compuesta por 2 servidores físicos y los 2 Routers que están presentes en este proyecto de Micro-segmentación, cada uno de ellos con una configuración de vlan distinta para cada uno de sus puertos de conexión.

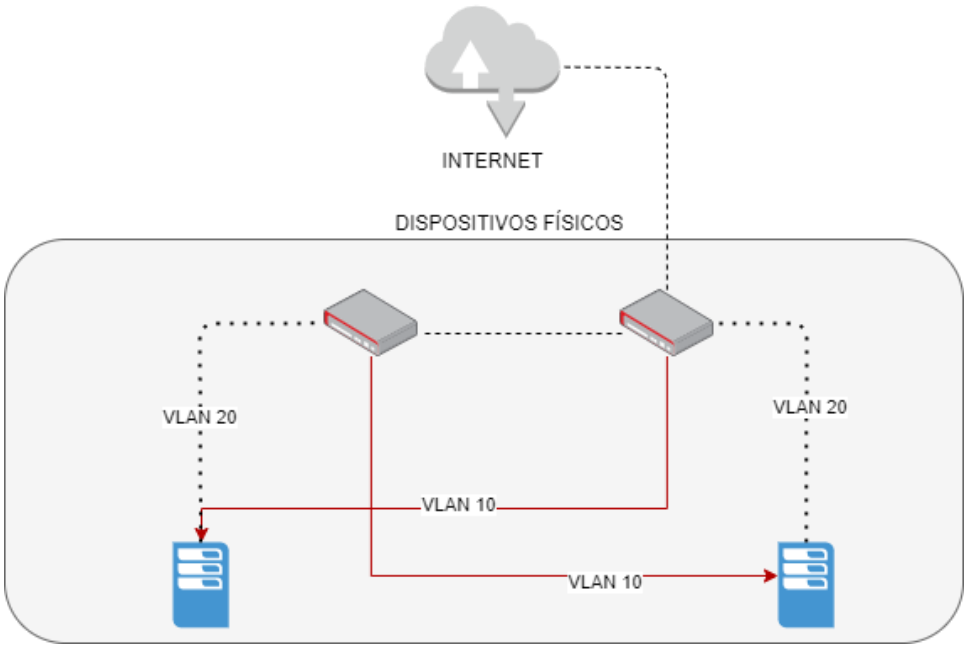

Ilustración 11 Vista de los equipos físicos presentes en nuestro proyecto de Micro-segmentación

6.3 Direccionamiento IP

Para realizar un direccionamiento ip dentro de la red se debe tomar en cuenta diferentes consideraciones que abarcan criterios fundamentales en razón que permitan tener un despliegue eficaz en cuanto al uso de identificadores ip. Cuando se realiza el direccionamiento ip es indispensable no obviar el dimensionamiento de la red ya que se debe tomar en cuenta la proyección hacia un futuro crecimiento o adición de nuevos hosts, de esta manera se obtiene una red escalable y fácil de administrar. Además se aplican las configuraciones de las vlans permitiendo tener una segmentación en nuestra red con un criterio de direccionamiento ip más pequeño por zona dado que ofrece beneficios de seguridad y aislamiento, esto gracias a su funcionalidad que permite separar el tráfico y evitar violaciones de información por parte de grupos no autorizados, otro de los beneficios que presenta el uso de vlans es la reducción de costos ya que permite un uso más eficiente del ancho de banda a la vez que ayuda a tener un control del tráfico en la red. Entonces, una vez realizado el análisis de los requerimientos necesarios para el despliegue de nuestra topología se representa en la *Tabla 1* las direcciones ip junto a los parámetros de configuración de acuerdo con cada host para su aplicación dentro de nuestro protocolo de pruebas y aplicación en redes definidas por software.

N# VLAN	RED	GATEWAY	BROADCAST	MASCARA DE RED	WILDCARD	IP	PREFIJO	HOST	SECCIÓN
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.30	/27	ESXi	ADMINISTRACIÓN
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.29	/27	ESXi	
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.28	/27	Vcenter	
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.27	/27	NSX	
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.26	/27	Active Directory	
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.25	/27	NSX Controller 1	
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.24	/27	NSX Controller 2	
VLAN 10	172.17.10.0	172.17.10.1	172.17.10.31	255.255.255.224	0.0.0.31	172.17.10.23	/27	NSX Controller 3	
VLAN 20	172.30.11.0	172.30.11.1	172.17.10.31	255.255.255.224	0.0.0.31	172.30.11.11	/27	DNS	SERVICIOS
VLAN 20	172.30.12.0	172.30.12.1	172.17.10.31	255.255.255.224	0.0.0.31	172.30.12.11	/27	Base de Datos	
VLAN 20	172.30.13.0	172.30.12.1	172.17.10.31	255.255.255.224	0.0.0.31	172.30.13.11	/27	VOIP	
VLAN 20	.1192.168.1.0	192.168.1.1	192.168.1.7	255.255.255.248	0.0.0.7	192.168.1.3	/29	Apache	DMZ
VLAN 20	192.168.100.0	192.168.100.1	192.168.100.255	255.255.255.0	0.0.0.255	192.168.100.11	/24	Cliente 1	LAN
VLAN 20	192.168.100.0	192.168.100.1	192.168.100.255	255.255.255.0	0.0.0.255	192.168.100.12	/24	Cliente 2	

Tabla 1 Direccionamiento IP de cada host incluido dentro de la topología desarrollada

6.4 Requisitos previos al despliegue de NSX sobre ESXi

Existen diferentes servicios que deben de estar correctamente configurados antes de desplegar completamente la topología. Se les conoce como requisitos previos ya que estos son indispensables para el funcionamiento total o parcial de los servicios, así se evitará tener problemas relacionados con la pérdida de datos o de incongruencias de información ya que estos servicios van a estar relacionados entre los siguientes servicios que se presentan a continuación:

6.4.1 Network Time Protocol

Configurar el servició de protocolo de tiempo de red (Network Time Protocol – NTP) es de gran utilidad dentro de un centro de datos porque nos ayuda a sincronizar la hora exacta dentro cada uno de nuestros hosts. Esto permite tener una correcta sincronía de configuración dado que en diferentes ocasiones cuando se instala un equipo la fecha y hora se registran basado en la zona horaria dando oportunidad a crear un problema con los servicios; sin embargo, al registrar el servicio de NTP en la maquina nueva o que estén en la red enviaran paquetes de verificación permitiendo sincronizar de manera automática todos los equipos, más aún cuando se trata de servicios críticos, en donde se necesita monitorizar, recibir alertas o para la gestión de logs en caso de presentar errores en el sistema. Cuando se sincroniza los relojes de los sistemas informáticos se tiene una latencia variable la cual es considerada despreciable y esta se rige por la zona horaria Tiempo universal coordinado (Universal Time Coordinated - UTC) que es ejecutado en segundo

plano y permite intercambiar la hora del sistema permitiendo el avanzar o retroceder de la hora asignada basado en una referencia de tiempo.

6.4.2 Domain Name Server

El sitio (AWS, 2020) define el DNS como “un sistema traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.vsmartcloud.org) a direcciones IP aptas para lectura por parte de máquinas (en este caso, 192.0.2.44)”. El sistema de nombre de dominio (Domain Name Server - DNS) es uno de los servicios esenciales que debe ser configurado; por lo que da la posibilidad de tener uno o varios dominios y en nuestro caso particular se realizó la implementación un dominio principal denominado “vsmartcloud.org” y un dominio secundario “micro.org”. Los cuales permiten acceder a los servicios por un nombre asignado en vez de utilizar la dirección ip. Contar con un servidor de DNS es indispensable por razones de seguridad y porque se presenta la dirección del sitio de una manera legible hacia los usuarios que acceden a los servicios, por ende, se puede realizar consultas web conociendo únicamente el dominio al cual se busca acceder y al servicio que se desea realizar la petición.

Cuando llegan a guardar la información de las zonas dadas por el espacio de nombres de dominio en la base de datos se denomina servidor DNS primarios, principal o maestro. Cada zona dispone de un sistema de nombre de dominio y debe contener al menos un servidor principal capaz de tener varios secundarios que permite tener un sistema redundante, seguro y disponible a manera de clúster. Si se modifica el servidor primario

los cambios van a replicarse en los secundarios sin embargo estos cambios pueden demorar en realizarse por lo cual consultar el principal siempre será más fiable que los secundarios.

Aquellos servidores secundarios que dependen de otros servidores primarios y no pueden resolver peticiones en su propia base son conocidos como esclavos, ya que siempre que no exista un registro en su base de datos solicitaran mediante un proceso jerárquico a otro servidor principal la resolución de la solicitud. Las diferentes solicitudes que no estén registrados en el servidor secundario se almacenan de manera temporal de forma local permitiendo tener un atajo en caso de peticiones futuras, esto genera un problema de seguridad ya que al tener datos temporales y exista un cambio en el archivo original no se verá actualizada la información hasta que se haga un vaciado de la cache del DNS. En la siguiente Tabla 2 se muestra la información con las direcciones ip y dominios asignados a cada host, de acuerdo con su localización dentro de la topología.

	HOST	IP	DNS	VLAN
ADMINISTRACIÓN	ESXi	172.17.10.30	nave.vsmartcloud.org	VLAN 10
	ESXi	172.17.10.29	killer.vsmartcloud.org	
	Vcenter Server	172.17.10.28	capitan.vsmartcloud.org	
	NSX Management	172.17.10.27	recluta.vsmartcloud.org	
	Active Directory	172.17.10.26	alien.vsmartcloud.org	
SERVICIOS	Active Directory	172.30.11.11	aire.micro.org	VLAN 20
	Ubuntu (DB)	172.30.12.11	agua.micro.org	
	Issabel	172.30.13.11	fuego.micro.org	
DMZ	Ubuntu (Apache)	192.168.1.3	www.micro.org	
LAN	Windows 7 (Cliente 1)	192.168.100.11	No Necesario	
	Windows 7 (Cliente 2)	192.168.100.12	No Necesario	

Tabla 2 Nombres de Dominio configurados en cada host

6.5 Servicios alojados en el centro de datos

6.5.1 Servicio de Active Directory como controlador de dominio

Entre los productos de Microsoft se encuentra el servicio de directorio activo el cuál es definido como “una estructura jerárquica que almacena información sobre objetos en la red. Un servicio de directorio proporciona los métodos para almacenar datos de directorio y ponerlos a disposición de los usuarios y administradores de la red. Por ejemplo, AD Servicios de Dominio (Domain Services - DS) almacena información sobre cuentas de usuario, como nombres, contraseñas, números de teléfono, etc., y permite que otros usuarios autorizados en la misma red accedan a esta información”, tomado de (Microsoft, 2017).

Un centro de datos ya sea físico o definido por software, necesita mantener un ente que se encargue de administrar cuentas de usuarios, restricciones de usuarios, etc. Por lo tanto, es importante hacer uso de un sistema jerárquico capaz de administrar las acciones que suceden en cada objeto de la red, permitiendo asignar roles y características propias a cada uno de los elementos y objetos que sean administrables. Esta función en nuestro protocolo de pruebas la cumple el servicio de directorio activo el cual permite registrar maquinas al dominio y brindar políticas a nivel de maquina o usuario con funciones de comunicación de red para su ingreso y establecimiento de políticas.

Cada usuario dentro de la red debe tener asignado sus roles y privilegios permitiendo tener un control especifico de diferentes tareas de tal manera que sea posible evitar fuga de información e identificación de cada usuario que está en nuestra organización. En caso de cambios o eliminación es posible identificar de manera clara y precisa quien fue la última persona en manipular la información. Adicionalmente el uso del controlador de dominio facilita los procesos de auditoria necesarios para tener un control respecto al consumo de recursos que genera los servicios de directorio activo.

6.5.2 Apache como Servicio WEB

En (Norfipc, 2020) los autores establecen que “un servidor web como su nombre lo indica, es un software instalado en el equipo con todas las condiciones necesarias para servir o entregar páginas web que le sean solicitadas por un navegador, asegurando que se

muestren y representen todos los elementos necesarios para su correcto funcionamiento y visualización. Existen varios tipos de servidores web, Apache es un software de código abierto, libre de uso y totalmente configurable, es en este momento el más utilizado en la red, ya sea en plataformas Linux o Windows.” El servidor web apache es uno de los servicios más utilizados gracias a su característica de código libre y multiplataforma además de poder ser accedido por diferentes clientes que cuenten con un navegador web. Los servicios web aceptan solicitudes de clientes y proceden a enviar la respuesta a dicha solicitud en donde se considera la integridad de la información y su estructura de manera que se permite establecer vistas estáticas o dinámicas de la información mediante la programación en Lenguaje de Marcas de Hipertexto (HyperText Markup Language - HMTL).

6.5.3 Uso del protocolo SIP para VOIP

Según (Sewan, 2019) la voz ip se define como “una tecnología que permite realizar llamadas telefónicas a través de Internet en lugar de a través de las redes de telefonía convencional, tradicional u analógica, con ventajas básicas y fundamentales”. Considerando eso se puede decir que voz sobre el protocolo ip o también conocido como Voip permite digitalizar la voz en paquetes de datos que posteriormente son enviados hasta el centro de datos mediante una red a diferencia de la telefonía convencional dado que en esos casos la información es enviada de manera analógica. El protocolo de iniciación de sección (Session Initiation Protocol - SIP) como refiere (3CX, 2021) es un protocolo de

señalización que permite establecer secciones entre usuarios y dar por concluidas las secciones, además se aplica el uso de este protocolo para iniciar las llamadas a manera de secciones para la transmisión de paquetes con el apoyo del protocolo de transporte en tiempo real (RTP – Real Time Transport Protocol).

6.5 4 Postgresql como Base de Datos

"Una base de datos es una colección organizada de información estructurada, que normalmente se almacena de forma electrónica en un sistema informático", así lo define el autor (Oto, 2020). Basado en esta definición se puede mencionar que Postgresql trabaja bajo sentencias SQL dado que forman parte del estándar utilizado en los sistemas de gestión destinados a las consultas dentro de las bases de datos relacionales. Las bases de datos conforman una herramienta cuya función es básicamente recopilar datos y almacenarlos de forma relacional para que el administrador pueda realizar consultas de manera rápida, efectiva e incluso cuando se trata de consultas complejas.

6.6 Modelo Cero Confianza

Según (Gilman & Barth , 2017) el modelo cero confianza se creó basado en afirmaciones respecto a la red como: "Siempre se considera a la red como un ambiente de constantes ataques que puede surgir de manera interno o externa" por eso se crea este modelo en 2010 por Forrester para establecer diferentes puntos de control que permite la

correcta aplicación de este modelo. Para ello es necesario definir 3 aspectos los cuales brindaran un entendimiento de lo que se busca alcanzar con esta implementación:

- Visibilidad: Es imposible proteger los recursos de los cuales no se tiene el conocimiento por lo tanto es de importancia identificar todos los dispositivos y servicios que van a ser monitoreados y protegidos. Así como la información sensible de la empresa y quien accede a ella debe ser evaluada y considera bajo premisa del menor privilegio.
- Políticas: Se debe tener en cuenta de todos los privilegios que existen en las organizaciones y usuarios para determinar controles de menor privilegio de acuerdo con cada usuario, es decir, cada política está diseñada para que el usuario tenga un ambiente especifico y controlado de acuerdo a sus funciones dentro de la organización de manera que se logre evitar la realización de acciones que no le corresponde o manipular información vital de la empresa.
- Automatización: La automatización nos permitirá tener planes de contingencia en caso de acciones no autorizadas dentro de la red, de tal forma que se busca asegurar el correcto uso de políticas y en caso de incumplimiento se pueda bloquear o aislar de manera rápida al usuario evitando así que se logre interactuar con usuarios que posean un mayor privilegio.

Una vez establecido y entendidos los 3 aspectos necesarios para la estrategia en estudio se puede empezar con el modelo cero confianza. El primer punto y lo más importante es definir los datos que son empleados en el sistema y los usuarios de la red, equipos y bienes que van hacer uso de esta información con la aplicación del servicio de directorio que brinda Windows Server donde se crea y define los usuarios, se registra equipos y se define políticas a nivel de unidad organizativa que incluye usuarios y equipos, además permite seleccionar parámetros como inicio de sección o registro de equipos en el inventario agregado como se muestra en la *Ilustración 12* en donde se observa algunos de los usuarios asignados con sus roles para el uso de los servicios. Todo este proceso de gestión de usuarios y equipos se o realiza mediante las Directiva de grupo (GPO - Group Policy Object).

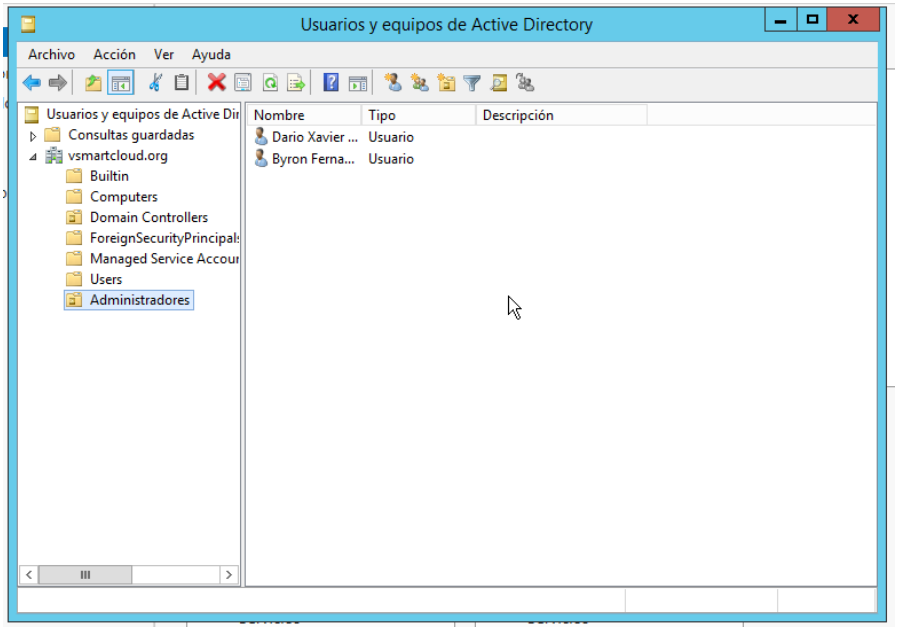

Ilustración 12: Usuarios y Equipos pertenecientes al Directorio Activo

La asignación de políticas se establece a nivel de objeto y NSX como software especializado en la virtualización de red es capaz de establecer reglas de seguridad a nivel de objeto de manera que se controla el comportamiento a través de grupos de equipos definidos según los parámetros de seguridad previamente analizados, mismos que cuentan con las mejores prácticas de seguridad tal como se muestra en la Ilustración 13. De esta manera se consigue establecer el principio de mínimo privilegio adicional al control de privilegios establecidos por NSX.

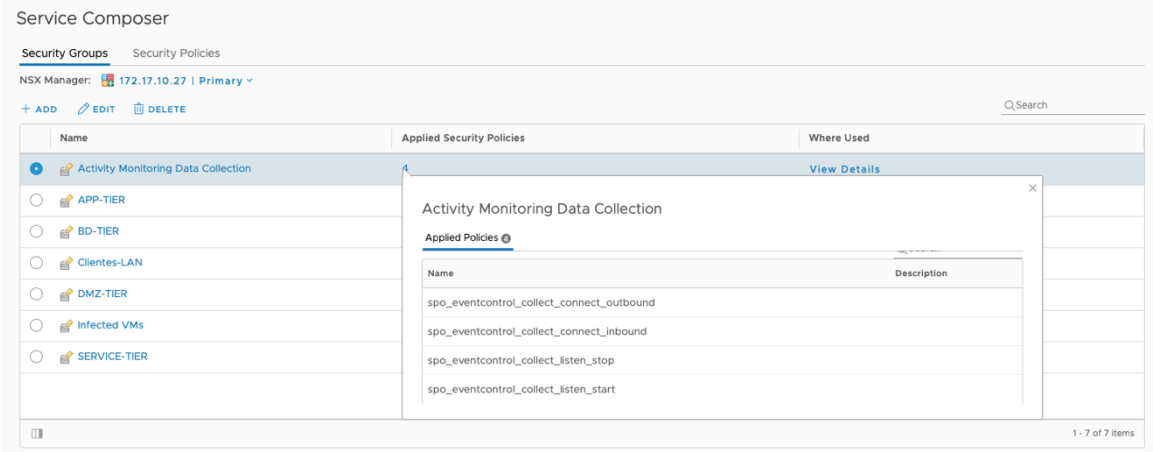

Ilustración 13 Manejo de políticas por grupo definidos según su categoría

Además de desplegar las políticas por usuario se hace uso de las políticas de NSX las cuales, basadas en el control de paquetes permiten analizar el tráfico en nuestra red y detectar posibles registros maliciosos para nuestro modelo de cero confianza con la administración de los grupos de seguridad en donde se aplican las políticas a los componentes de red tal como se muestra en la Ilustración 14. De esta manera se puede lograr que el sistema se vuelva más robusto.

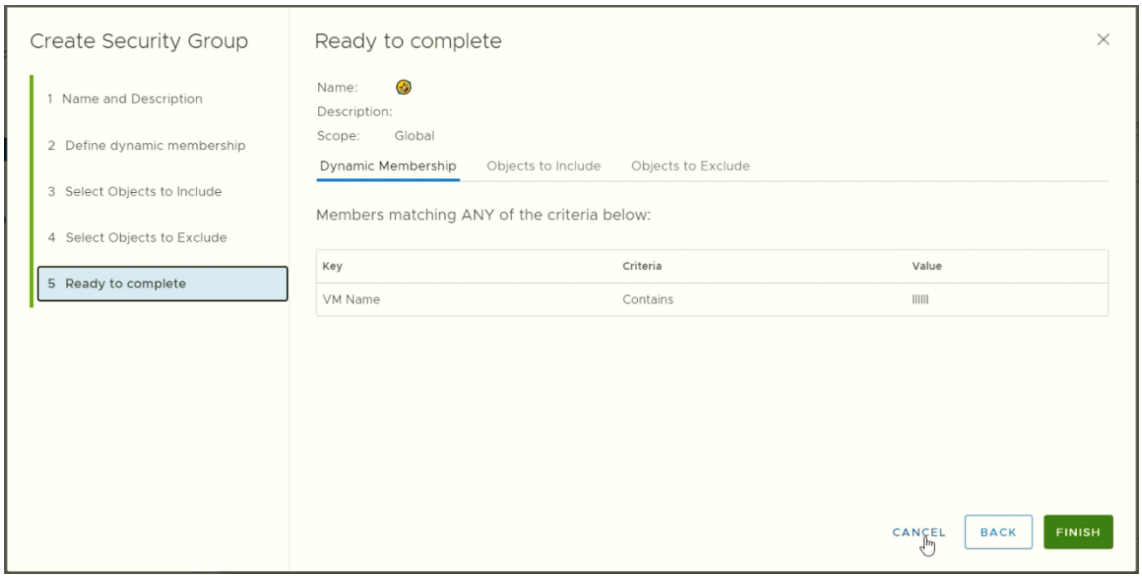

Ilustración 14 Resumen de la creación de grupo de seguridad

Adicional a las políticas que se mencionaron anteriormente existe la protección a través de reglas de firewall que son aplicadas a cada servicio alojado en la red, reglas que sirven para controlar y delimitar el tráfico entrante y saliente hacia los hosts que alojan los servicios dentro del entorno virtualizado. Para ello se generó políticas basadas en los servicios y usuarios que acceden a estos servicios entendiendo que el apartado de firewall se puede delimitar en diferentes ubicaciones de nuestra topología.

6.6.1 Firewall

Al implementar el firewall dentro de las SDN se consigue seguridad basada en el perímetro de red, esto significa que en los despliegues se logra eliminar la confianza por defecto que existe generalmente dentro de la infraestructura tradicional la cual genera capacidad de defensa ante ataques externos y no es capaz de defender el centro de datos cuando surgen ataques internos. Estas brechas de seguridad pueden ser mitigadas con la aplicación del modelo cero confianza el cual permite establecer reglas que consisten en delimitar y bloquear todo el tráfico con excepción de las reglas previamente asignadas que habilitan el ingreso a los servicios a través de puertos específicos asignados a cada aplicación.

Al aplicar el modelo cero confianza dentro de una arquitectura de red virtualizada con NSX el firewall físico resulta poco indispensable debido a que existe la capacidad de analizar el tráfico y bloquearlo a través del firewall lógico distribuido, mismo que permite el análisis de paquetes con cargas de trabajo a nivel individual con reglas aplicadas a cada servicio, un ejemplo claro de esta aplicación se demuestra en la ilustración 15.

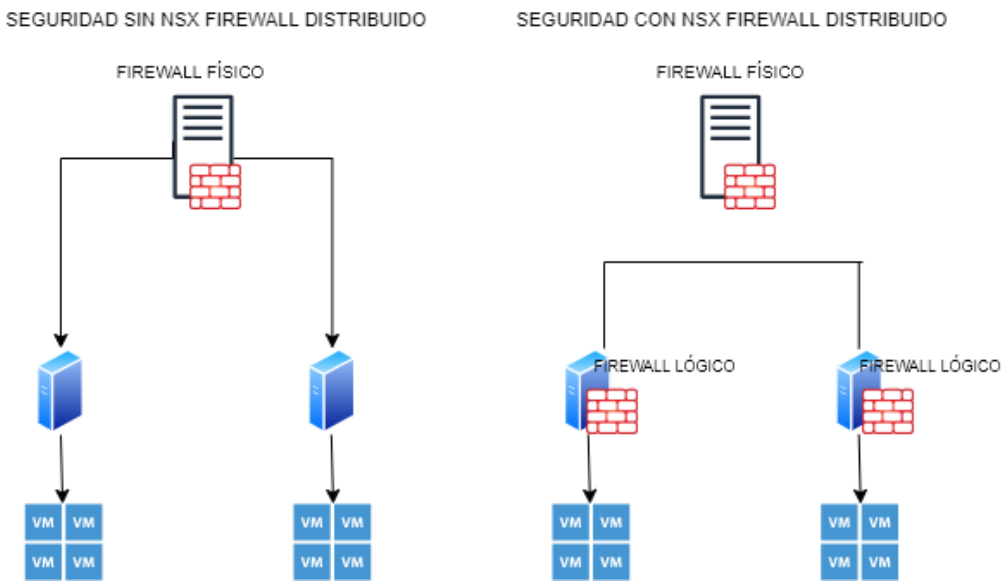

Ilustración 15 Diferencia de la Seguridad con NSX DFW

Dentro del firewall de NSX la última regla aplicada será la encargada de denegar todo el tráfico que no esté establecido o intente establecer conexión hacia los sitios protegidos, esta configuración está ubicada en los Routers ESG y DLR respectivamente los cuales se encargaran de los servicios que son solicitados en la red tal como se muestra en la ilustración 16.

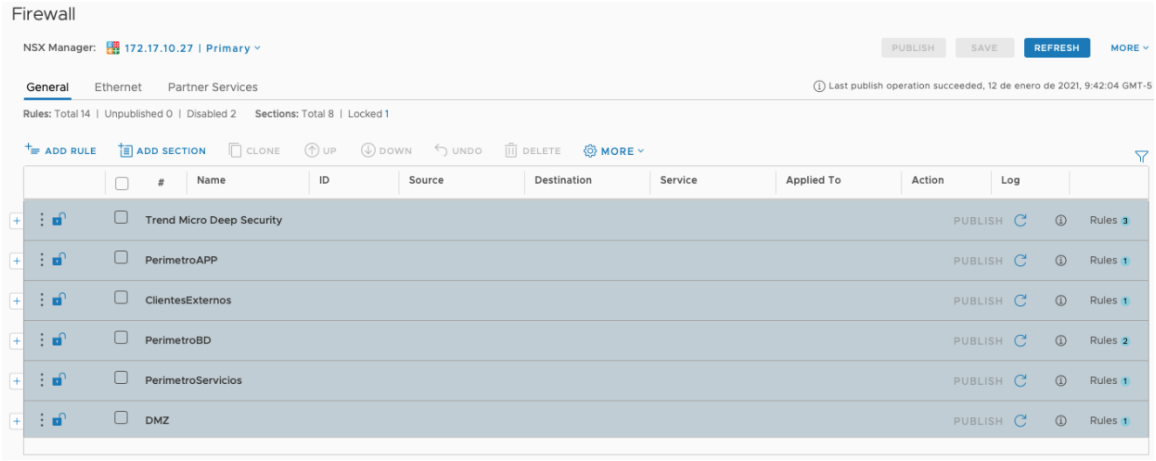

Ilustración 16 Firewall ESG y DLR

Siguiendo con el mecanismo de protección se establece las reglas para el firewall general de NSX el cual es el encargado del habilitar o deshabilitar las conexiones de la infraestructura, es decir, todo lo relacionado con el hipervisor y el orquestador son agregados para ser monitoreados con los módulos configurados en la red definida por software. Para asignar las reglas se procede a configurar en el menú configuraciones de firewall como se presenta en la ilustración 17.

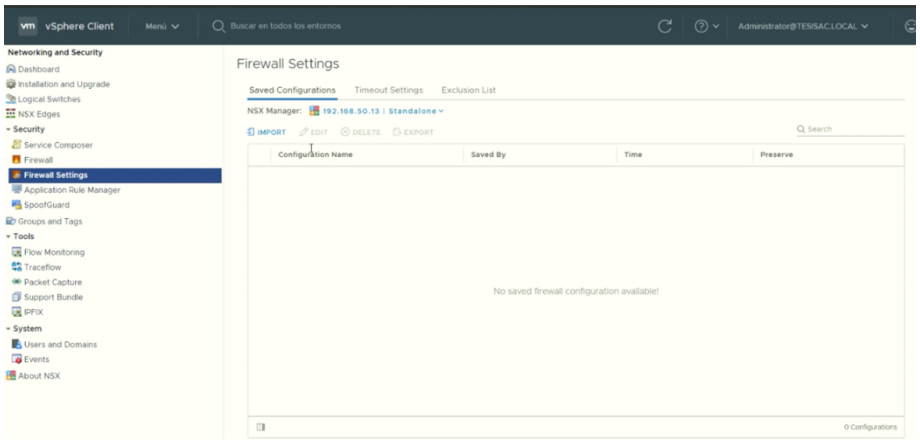

Ilustración 17 Firewall General de la infraestructura

6.7 Protocolo de Pruebas

Para realizar el escenario de prueba se accede al uso de un software de mucho prestigio, mismo que sería capaz de garantizar un conjunto de pruebas bastante complejas capaces de ofrecer un resultado que valide la aplicación de nuestro proyecto basado en Micro-segmentación con NSX. De esta manera se pudo evidenciar que nuestra propuesta de seguridad de centro de datos con NSX resulta una gran ventaja para las empresas cuya infraestructura sea considerablemente grande

Mediante los informes generados por la prestigiosa empresa Gartner[17] se puede evidenciar el cuadrante mágico de Gartner el cual se enfoca en definir el nivel de eficacia de las diferentes herramientas de validación de vulnerabilidades. Entre ellos se puede encontrar informes acerca de los hipervisores, software de protección, entre otros. Para realizar nuestras pruebas se tomó como base de referencia el cuadrante mágico que se puede ver en la *Ilustración 18*, en donde se evidencia la efectividad de las herramientas que brinda KnowBe4, empresa que se ubica en primer lugar a comparación de otras empresas que presentan software de igual aplicación, pudiendo demostrar la efectividad de este sistema en cuanto a la eficiencia en el análisis de vulnerabilidades dentro de un centro de datos, por tal motivo para realizar las pruebas de nuestro ambiente y la configuración realizada en el mismo, se hará uso de las herramientas disponibles por KnowBe4.

[17] Gartner: “es una firma de investigación y asesoría (analista) que ofrece investigación tecnológica a líderes empresariales, lo que les permite tomar decisiones sobre iniciativas clave” (SAGE, 2021).

Ilustración 18 "Security Awareness Computer-Based Training Reviews and Ratings" (

(Budge, O'Malley, Blankenship, Flug, & Nagel, 2020)

El período de prueba dedicado para el análisis del comportamiento de nuestro sistema de seguridad basado en redes definidas por software se encuentra establecido de manera que se pudo identificar que los sitios aprovisionados se encontraban protegidos ante los ataques informáticos más comunes que se pueden percibir en un centro de datos. De tal manera que fue posible constatar la eficiencia que presenta nuestra configuración de

Micro-segmentación con NSX pudiendo validar que es posible proteger el centro de datos con mecanismos que están a la vanguardia de la tecnología.

6.7.1 Periodo de Prueba

En este período de prueba se busca establecer un tiempo desde la configuración inicial hasta lograr un ambiente totalmente protegido para los servicios y equipos disponibles. Así pues, como primera instancia se pretende realizar una primera prueba con la herramienta que brinda KnowBe4 enfocada a diferentes hosts ubicados en la infraestructura interna. Una vez realizadas las pruebas y obtenida la información se procede a realizar la configuración de Micro-segmentación y modelo cero confianza aplicadas a los segmentos de la red para posteriormente volver a realizar las pruebas con la herramienta RanSim e identificar si las vulnerabilidades fueron mitigadas y el centro de datos se vuelve confiable.

6.7.2 Prueba de vulnerabilidades en el centro de datos previo a aplicar Micro-segmentación

En este caso se presenta un análisis de vulnerabilidades existentes en la infraestructura planteada sin configuraciones previas con NSX, de esta manera se evidencia si existe un ambiente seguro dentro del centro de datos en donde los servicios están expuestos a posibles ataques ya sea internos o externos. De igual manera se busca obtener una idea general de la gravedad que existe al no contar con un ambiente controlado que

permita establecer puntos de control para evadir los diferentes peligros a los cuales está expuestos los centros de datos de todas las empresas a nivel global.

Una vez completadas las pruebas de seguridad con la herramienta de análisis de vulnerabilidades RanSim se puede observar que los resultados obtenidos son poco favorables para la implementación en cuestión, dado que se puede observar fácilmente las fallas de seguridad que existen en una configuración convencional en donde no existe la aplicación del concepto de seguridad con redes definidas por software. De esta manera con los diferentes escenarios de prueba de seguridad que posee la herramienta antes mencionada como se muestra en la *Ilustración 19*, se puede afirmar que un ambiente que no cuenta con las configuraciones adecuadas que sirvan como perímetro de protección a los servicios alojados en los segmentos de red representa un alto riesgo ya que la integridad de los datos puede verse comprometida llegando a tener incidentes poco favorables para una empresa a nivel de sistemas.

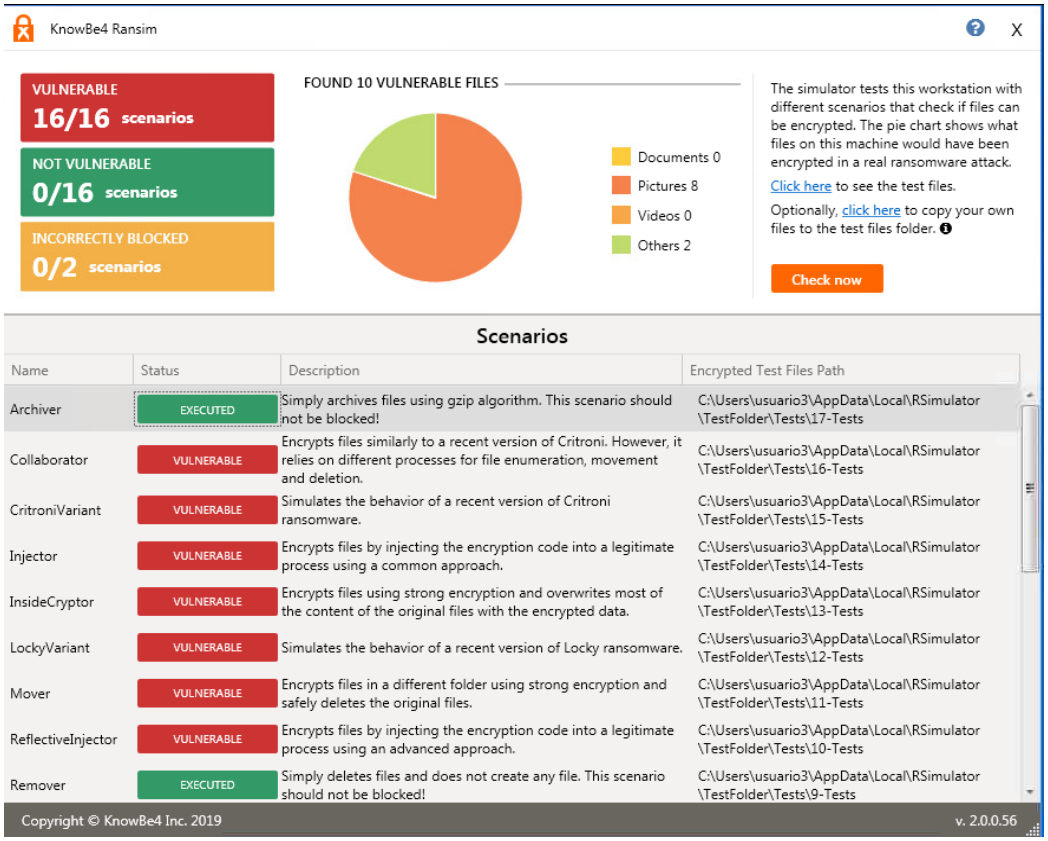

Ilustración 19 Knowbe4 en maquina sin configurar seguridad

6.7.3 Pruebas finales con la aplicación de Micro-segmentación

Las pruebas realizadas se pudieron aplicar tanto a equipos de manera individual como a nivel de grupos de equipos gracias a los agentes que despliega el software Trend Micro Deep Security capaces de monitorear constantemente los eventos de los hosts en los cuales se encuentran instalados y su principal función radica en comunicarse con el panel de administración en donde se analiza el evento enviado por el agente y se toman las

acciones de acuerdo a cada incidente permitiendo de esta manera admitir o bloquear las acciones del usuario. Adicional se configura políticas de firewall anti-Malware entre otros factores indispensables para realizar pruebas de contexto. En la *Ilustración 20* se muestra los parámetros que monitorea el agente y son receptados por el administrador de modo que es posible visualizar los eventos que se generan en los hosts que contienen el agente instalado.

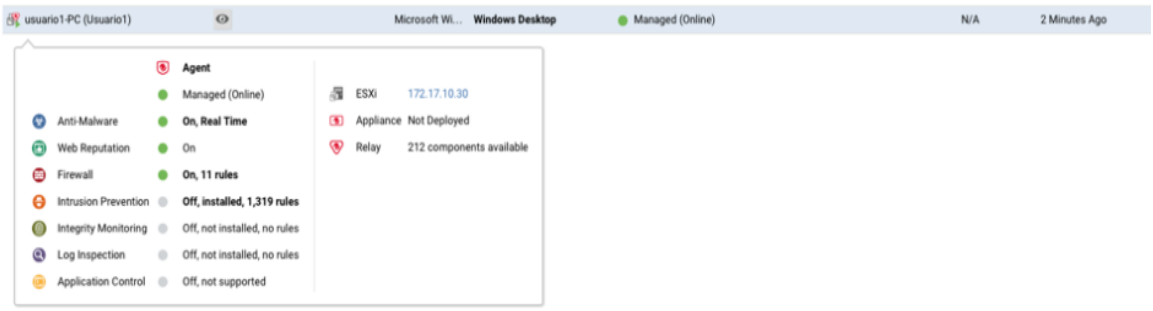

Ilustración 20 Comunicación entre el agente y el administrador de deep security

Una vez instalado el agente en los hosts y despegado el sistema de seguridad avanzada con Deep Security, el panel de administración empieza a recolectar información de los eventos que ocurren para ser analizados según la prioridad aplicada y posteriormente tomar las acciones de prevención y corrección respectiva. Como se presenta en la *Ilustración 21*, este software presenta de manera gráfica cada incidente ocurrido en los equipos de tal manera que el administrador de la red pueda tener una visibilidad de alto nivel y tomar las acciones respectivas de acuerdo con las políticas de la empresa apoyando de esta manera con seguridad adicional al aplicado con NSX.

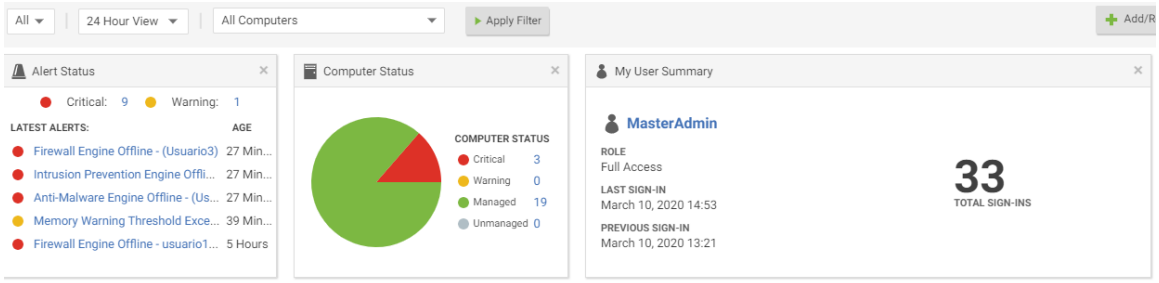

Ilustración 21 Panel de alertas de las máquinas monitoreadas.

Una vez establecidos los parámetros de configuración de aseguramiento de la red con el uso de NSX apoyado en el estrategia cero confianza y en el software Deep Security como complemento esencial de la Micro-segmentación se procede a ejecutar la herramienta de KnowBe4 denominada RanSim para la toma de una nueva muestra respecto al nivel de vulnerabilidad existente en los host para validar que las configuraciones realizadas sean altamente efectivas y permitan tener una infraestructura con protección robusta ante posibles intrusiones en hosts vulnerables dentro de la red.

Con esta muestra se consigue demostrar que la aplicación de Micro-segmentación mitiga cada uno de los ataques que fueron generados por la herramienta knowBe4 obteniendo como resultado un ambiente totalmente protegido y controlado gracias al constante monitoreo de amenazas que ejecuta el administrador de Deep Security. En la *Ilustración 22* se evidencia el nivel de seguridad que se llega a generar implementando políticas que nos permite NSX para controlar tanto el acceso como el control hacia los equipos y los servicios.

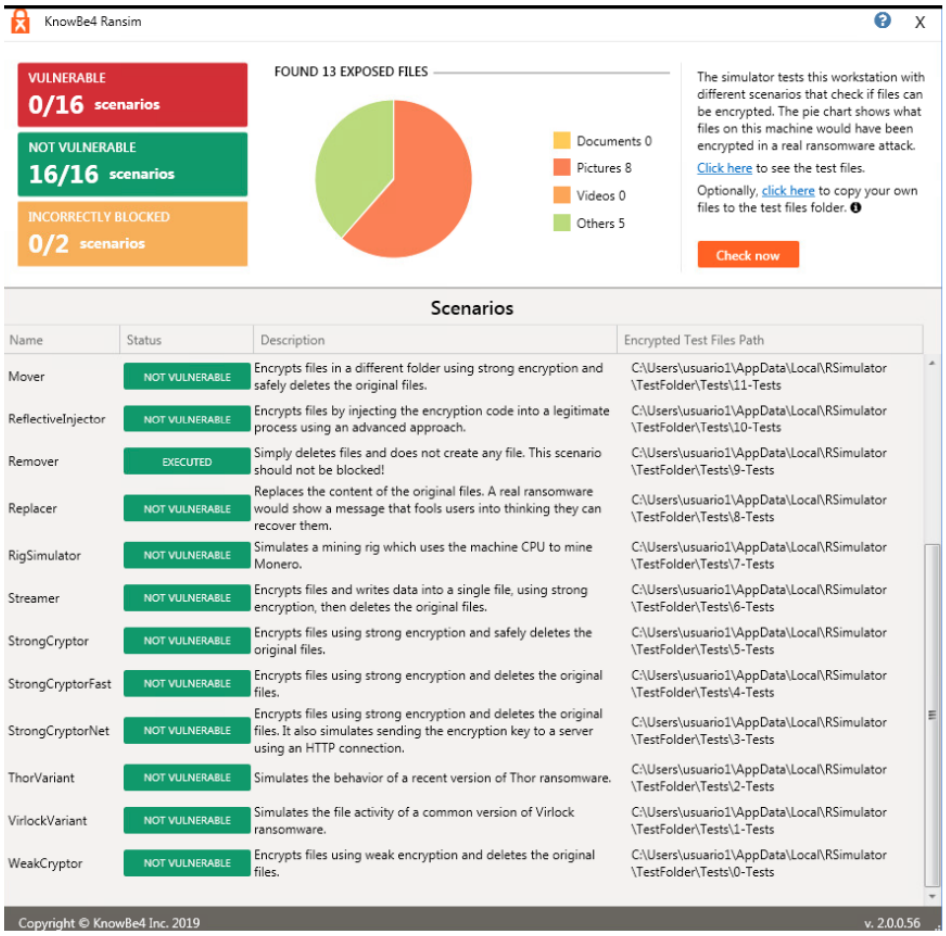

Ilustración 22 Prueba de contexto de la Micro-segmentación.

Adicional mediante TraceFlow como parte del protocolo de pruebas se analizar el tráfico de un adaptador origen y un destino en diferentes segmentos de red como se muestra en la *Ilustración23*, al momento de generar tráfico no permitido se puede evidenciar el correcto funcionamiento de las reglas de firewall y el rechazo de este tráfico. Es así como se logra establecer un ambiente seguro con protocolos de seguridad avanzada diseñadas para impedir que los hosts se vean infectados de forma lateral dentro del centro de datos.

Entonces, las reglas de firewall aplicadas bajo un previo diseño de red según la arquitectura de la organización permite contar con un ambiente confiable en donde se aplican conceptos mencionados en el presente proyecto, técnica cero confianza y uso de SDN.

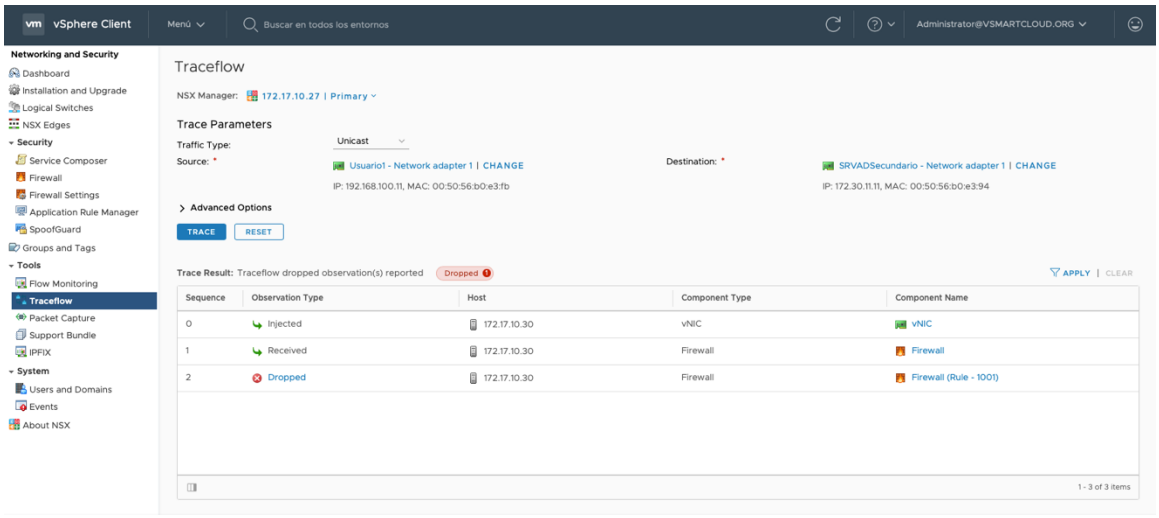

Ilustración 23 Reglas aplicadas como configuración de la microsegmentacón

7 Resultados

Gracias al proyecto de titulación realizado y a la investigación llevada a cabo se consiguió entender los conceptos y aplicaciones de la Micro-segmentación, de manera que fue posible identificar la aplicación de esta técnica de aseguramiento de diferentes perímetros de red de manera sofisticada. Con esto se logra desarrollar el conocimiento necesario para poder solventar los desafíos que representó desarrollar nuestra tesis considerando que el uso de la virtualización de red en nuestro medio es un tema novedoso dado que existe total atención ante estas tecnologías que poco a poco empiezan a ser comunes en el mercado ecuatoriano.

Se logró identificar la decadencia de la implementación de una red empresarial aplicando los modelos tradicionales que consisten en la protección de los servicios con un único perímetro de seguridad ubicado como primera y única línea de defensa ante ataques informáticos. Esta decadencia implica una evidente falta de seguridad hacia cada uno de los hosts existentes en el centro de datos por lo tanto es importante aplicar estas nuevas metodologías y tecnologías como el uso de la Micro-segmentación para poder cubrir las distintas brechas de seguridad que deja la implementación del modelo tradicional.

Mientras se llevó a cabo el desarrollo de este proyecto, se estudió con gran profundidad los temas relacionados con la virtualización de la red de manera que se llegó a la comprensión y diferencias que existe entre las redes definidas por software y Virtualización de funciones de red. Estos dos marcos de referencia hacen posible abstraer

los conceptos de red virtualizada a implementaciones de las arquitecturas de nueva generación en donde NVF comprende los elementos lógicos que pueden ser creados en ambientes virtualizados para interactuar conjuntamente con las SDN siendo que estas redes definidas por software representan el enfoque arquitectónico de red y comprenden la lógica del uso de los elementos creados bajo el enfoque que involucra las soluciones de administración de alto nivel de las redes operadas en los centros de datos de nueva generación.

Otro de los logros alcanzados está relacionado con el conocimiento obtenido sobre la administración de algunas de las soluciones ofrecidas por VMware. Gracias a las licencias demo obtenidas para el desarrollo de la tesis se pudo hacer un uso total de las funcionalidades de soluciones como VMware ESXi, VMware VCenter y VMware NSX pudiendo llegar a la comprensión de las funcionalidades y alcance que se puede obtener durante el despliegue de una infraestructura Virtualizada. Además de los aspectos positivos del uso de VMware se pudo revisar los aspectos negativos, de esta manera se identificó las ventajas y desventajas del uso de estas soluciones tomando en cuenta el costo beneficio de acuerdo con el tamaño de la empresa que vaya a usarlo.

Finalmente, con el uso de la solución NSX de VMware junto al software adicional Trend Micro y la estrategia zero trust se consiguió desplegar una infraestructura robusta, capaz de establecer perímetros de seguridad ya se a nivel de cada segmento o máquina virtual con el uso de reglas de firewall y análisis de amenazas a nivel individual. De esta manera, en caso de ser atacado el centro de datos, este se encuentra en las condiciones

necesarias para aislar el host amenazado del resto de la infraestructura para evitar que el ataque se expanda por la red de manera horizontal, alcanzando a cumplir el objetivo principal de la aplicación de NSX que consiste en evitar la expansión del malware logrando mitigar los ataques de manera eficiente.

Funcionamiento de la Micro-segmentación como método de aseguramiento de la red

Al realizar el despliegue de la arquitectura presentada en donde no se aplican las reglas de seguridad que se genera con NSX y no se cuenta con las políticas de firewall habilitadas se puede evidenciar las diferentes vulnerabilidades que pueden afectar a los terminales y su comunicación con el servidor poniendo la integridad del servidor en peligro al existir este riesgo potencial dentro de toda la organización. La fata de perímetros de seguridad dentro del centro de datos va a ocasionar que las amenazas encuentren vulnerabilidades y puedan expandirse a través de la red ocasionando consciencias graves según el tipo de ataque y los fines del mismo. El uso de la herramienta KnowBe4 nos permitió evidenciar las fallas de seguridad que existe dentro del centro de datos como se muestra en la *Ilustración* 24 una vez que el atacante logre sobrepasar el firewall de borde. Razón por la cual resulta de total importancia la aplicación de Micro-segmentación

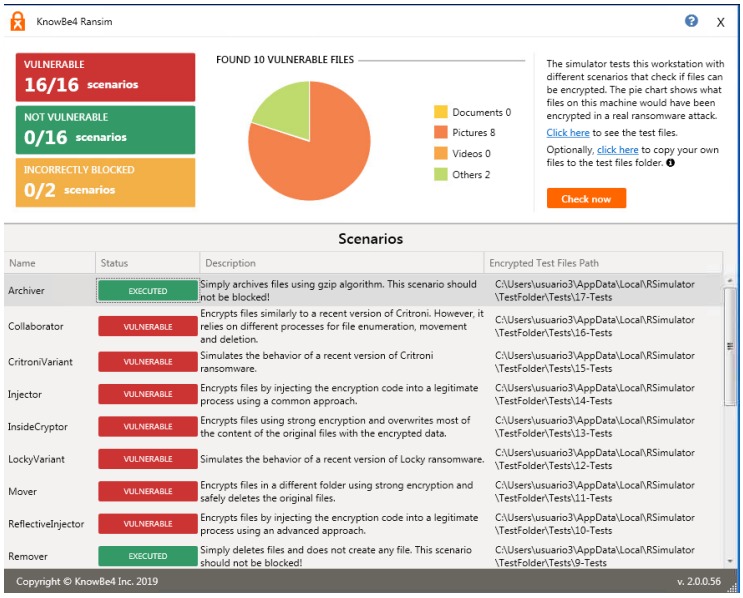

Ilustración 24 Ambiente no seguro

Por otro lado se logra contar con una infraestructura asegurada, en donde se aplica los conceptos de Micro-segmentación con NSX en donde se ha podido crear un ambiente que cumple con las características y seguridad de nueva generación para su correcto funcionamiento que consiste en detectar malware para posteriormente actuar de manera rápida y eficaz ante posibles amenazas o ataques que se pueden dar dentro del centro de datos, en nuestro proyecto de titulación se plantea la herramienta Knowbe4 que permite analizar 16 vulnerabilidades. Una vez realizadas las pruebas con este software en nuestra topología planteada, se consiguió llegar a evidenciar un nivel de vulnerabilidad nulo, esto gracias a la inspección realizada por NSX con cargas de trabajo a nivel individual en donde se consiguió bloquear los ataques que presenta la herramienta Knowbe4 en cada uno de los segmentos, no permitiendo la afectación de los servicios.

De acuerdo con lo mencionado en capítulos anteriores, si NSX que se encuentra apoyado por el antivirus Deep Security encuentra que una máquina de los usuarios o administradores se encuentra con posible riesgo o presentando comportamientos extraños automáticamente pasa a aislarle de los demás segmentos como se muestra la *Ilustración 25*, lo más importante es que el aislamiento de la máquina infectada puede ser aislada sin sufrir modificaciones físicas. Una vez que la amenaza haya sido mitigada y verificada por el antivirus Deep Security el host puede volver a su normal funcionamiento y continuar trabajando de manera continua.

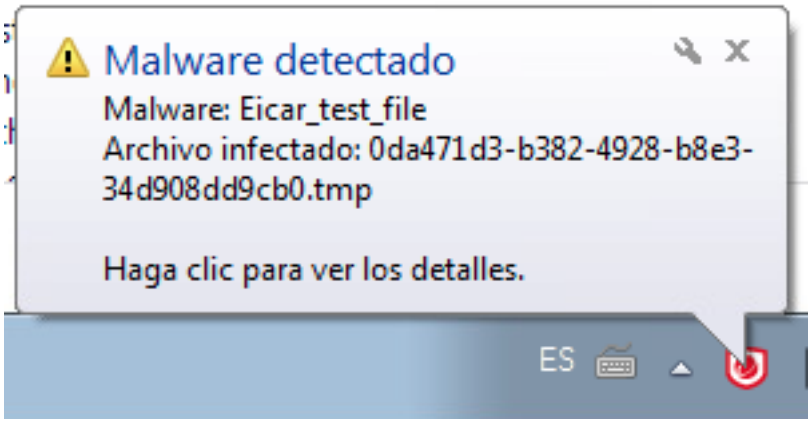

Ilustración 25 Alerta del agente al usuario en detección de amenazas.

Como se explicó anteriormente, el agente Deep Security es capaz de comunicarse con el administrador Deep security para informar constantemente la presencia de posibles amenazas en el host. Al estar cada equipo constantemente monitoreado reduce

constantemente la posibilidad de ser infectad a la red y en caso del agente detectar malware ocurre el aislamiento del host infectado. En la *Ilustración 26* se puede observar los eventos que ocurren una vez que se detectan amenazas, el antivirus identifica, verifica y pasa a tomar las acciones previamente configuradas

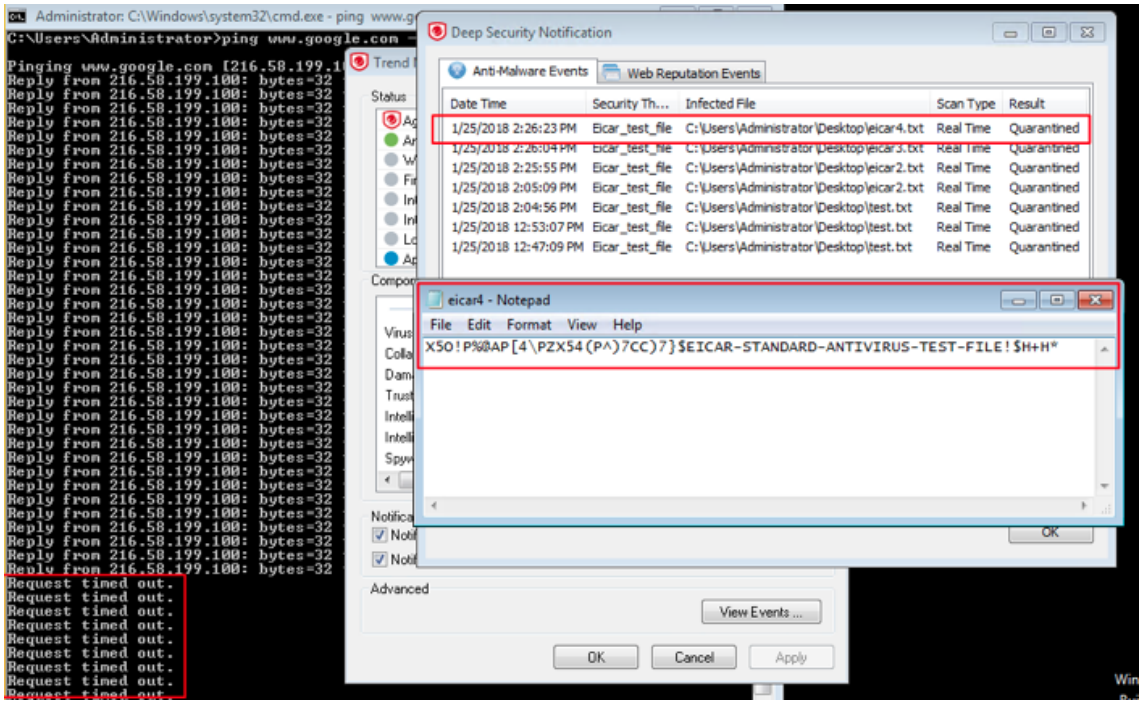

Ilustración 26 Aislamiento de red a la máquina infectada.

8 Conclusiones

Con el desarrollo de esta tesis se pudo concluir que resulta de vital importancia llevar a cabo un proceso de investigación de nuevas técnicas de aseguramiento de entornos virtualizados. De esta manera se puede llegar al análisis de tecnologías pioneras en el ámbito de la virtualización para poder establecer las mejores opciones de acuerdo con las necesidades empresariales tomando en cuenta las ventajas y desventajas que ofrecen las herramientas en cuestión.

Bajo el proceso de aprendizaje obtenido durante el desarrollo de este proyecto de titulación enfocado en las soluciones de VMware se pudo concluir la importancia de usar herramientas con varios años en el mercado por razones que incluyen experiencia y seguridad sobre todo si se trata de ambientes críticos en centros de datos virtualizados. El uso de estas herramientas de pago garantiza el correcto funcionamiento y la protección de los datos que representan el activo más importante de cualquier institución. De esta manera y con la aplicación de Micro-segmentación los problemas de seguridad informática se ven replegados de tal manera que se puede ofrecer ambientes con centros de datos seguros.

Elaborar un protocolo de pruebas resulta primordial ya que de esta manera se puede verificar que las implementaciones puedan ser probadas y posteriormente validadas. De esa manera se puede garantizar o declinar el funcionamiento de la aplicación de soluciones tecnológicas y el nivel de seguridad de la red, con mayor razón si se trata de la seguridad

y alta disponibilidad de los servicios alojados en los centros de datos en donde resulta sumamente importante proteger cada uno de los hosts existentes dentro del ambiente virtualizado.

Finalmente, se pudo concluir que NSX es la herramienta por excelencia para la aplicación de Micro-segmentación dado que hace posible hacer uso de la virtualización de red, un enfoque totalmente moderno y pensado para cubrir vulnerabilidades que existen, no obstante, es importante mencionar que se debe tener en cuenta el recurso económico para la implementación de esta solución de VMware ya que se considera que NSX es una herramienta enfocada en medianas y grandes empresas las cuales requieren una infraestructura robusta.

Bibliografía

Lawrence Miller, C. y. (2016). *Micro-Segmentacion para Dummies* . Hoboken, New Jersey: John Wiley & Sons, Inc.

Alcaráz, J. P. (8 de 01 de 2021). *Inforges*. Obtenido de Hiperconvergencia: Cuadrante mágico de Gartner 2020: https://www.inforges.es/post/hiperconvergencia-cuadrante-magico-de-gartner-2020

Vincentis, M. D. (2017). *Micro-segmentation For Dummies.* New Jersey: John Wiley & Sons, Inc.

Gilman, E., & Barth , D. (2017). *Zero Trust Networks.* California: O'Reilly Media, Inc.

Akers, S. (29 de 08 de 2019). *Lumen*. Obtenido de Hairping NAT: https://www.ctl.io/knowledge-base/network/lumen-cloud/hairpin-nats/

VMware. (03 de 03 de 2021). *VMware*. Obtenido de Microsegmentación: https://www.vmware.com/es/topics/glossary/content/micro-segmentation.html

Cinalli, F. (27 de 09 de 2019). *OpenWebinars*. Obtenido de Qué es vCenter Server: https://openwebinars.net/blog/que-es-vcenter-server/

VMware. (21 de 08 de 2020). *Virtualization*. Obtenido de What is Virtualization?: https://www.vmware.com/solutions/virtualization.html

Gonzales Río, M. D. (2014). *Tecnologías de Virtualización.* IT Campus Academy.

Cloudflare. (03 de 03 de 2021). *CLOUDFLARE*. Obtenido de Zero Trust Security | What's a Zero Trust Network?: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/

Márquez, A. (21 de 11 de 2011). *Virtualización de Servidores.* Obtenido de Universitat Politècnica de Catalunya: https://core.ac.uk/download/pdf/301205256.pdf

Becci, G., Morandi, M., & Marrone, L. (12 de 10 de 2020). *Seguridad en la virtualización de redes definidas por software.* Obtenido de V Taller del Grupo de Trabajo de Ingeniería de Internet / Argentina (IETF Day) - JAIIO 48 (Salta, 2019): http://sedici.unlp.edu.ar/handle/10915/88673

ORACLE. (21 de 09 de 2014). *Oracle.* Obtenido de Gestión de virtualización de red y recursos de red en Oracle® Solaris 11.2: https://docs.oracle.com/cd/E56339_01/pdf/E53790.pdf

Red Hat. (04 de 03 de 2021). *Red Hat*. Obtenido de ¿Qué es un hipervisor?: https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor

Ortiz, A. E. (10 de 09 de 2019). *HostDimeBlog*. Obtenido de ¿Qué Es Un Hipervisor? Tipos De Hipervisores 1 Y 2: https://www.hostdime.com.ar/blog/que-es-un-hipervisor-tipos-de-hipervisores-1-y-2/

Hewlett Packard Enterprise. (04 de 03 de 2021). *hpe.com*. Obtenido de ¿QUÉ ES LA HIPERCONVERGENCIA?: https://www.hpe.com/es/es/what-is/hyper-converged.html

EFRAM. (10 de 08 de 2015). *EFRAM BLOG*. Obtenido de What is the difference between a Backplane and a Motherboard?: https://m.blog.naver.com/PostView.nhn?blogId=framkang&logNo=220438385443&proxyReferer=https:%2F%2Fwww.google.com%2F

DNSstuff. (19 de 09 de 2019). *DNSstuff*. Obtenido de What Is Throughput in Networking? Bandwidth Explained: https://www.dnsstuff.com/network-throughput-bandwidth

Hamburger, V. (2016). *Building VMware Software-Defined Data Centers.* Birmingham: Packt Publishing Ltd.

Red Hat. (04 de 03 de 2021). *RedHat*. Obtenido de ¿Qué es el malware?: https://www.redhat.com/es/topics/security/what-is-malware

Chang, F. (2018). *Datacenter Connectivity Technologies: Principles and Practice.* The Netherlands: River Publishess.

Faizul , B., Boutaba, R., Esteves, R., Zambenedetti Granville, L., Podlesny, M., Rabbani, G., . . . Faten Zhani, M. (20 de 09 de 2012). *IEEE*. Obtenido de Data Center Network Virtualization: A Survey: https://ieeexplore.ieee.org/document/6308765/authors#authors

Zhang, Y. (2018). *Network Function Virtualization: Concepts and Applicability in 5G Networks.* New York: John Wiley & Sons, Inc.

Zhu, Y., Scott-Hayward, S., Jacquin, L., & Hill, R. (2017). *Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications.* Switzerland: Springer International Publishing.

Union Internacional de Telecomunicaciones. (06 de 06 de 2014). *Union Internacional de Telecomunicaciones*. Obtenido de Y.3300 : Marco de creación de redes definidas por software: https://www.itu.int/rec/T-REC-Y.3300-201406-I/es

Nadeau, T., & Gray, K. (2013). *DN: Software Defined Networks: An Authoritative Review of Network Programmability Technologies.* Tokyo: O'Reilly Media, Inc.

Göransson, P., & Black, C. (2014). *Software Defined Networks.* Waltham: Elsevier Inc.

Mcnickle, M. (19 de 06 de 2014). *SearchDataCenter *. Obtenido de Diez definiciones esenciales de virtualización de redes: https://searchdatacenter.techtarget.com/es/consejo/Diez-definiciones-esenciales-de-virtualizacion-de-redes

Coker, O., & Azodolmolky, S. (08 de 03 de 2021). *O'Reilly*. Obtenido de Redes definidas por software con OpenFlow - Segunda edición por Oswald Coker, Siamak Azodolmolky: https://www.oreilly.com/library/view/software-defined-networking-with/9781783984282/b0f4c4c4-dab7-4361-ad34-28e227ed8f15.xhtml

SDxCentral Studios. (15 de 09 de 2014). *sdxcentral*. Obtenido de What Is a Floodlight Controller?: https://www.sdxcentral.com/networking/sdn/definitions/what-is-floodlight-controller/

Erickson , D. (04 de 02 de 2013). *OpenFlow*. Obtenido de ¿Qué es Beacon?: https://openflow.stanford.edu/display/Beacon/Home.html

Kerner, S. M. (13 de 03 de 2018). *Enterprise Networking Planet*. Obtenido de ONF Announces Stratum Project to Redefine SDN: http://www.enterprisenetworkingplanet.com/netsp/openflow-is-the-past-as-onf-announcesstratum-project-to-redefine-sdn.html

Carpenter, B. (02 de 2002). *Internet Engineering Task Force*. Obtenido de Middleboxes: Taxonomy and Issues: https://tools.ietf.org/html/rfc3234

Gómez Vieites, Á. (2014). *Trend Micro Deep Security.* Madrid: RA-MA.

Fernandez, Y. (06 de 02 de 2020). *Xataka*. Obtenido de ¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, etcétera?: https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera

Costas Santos, J. (2006). *Seguridad y Alta Disponibilidad.* Madrid: RA-MA.

Ariganello, E. (2014). *Redes CISCO. Guía de estudio para la certificación CCNA Security.* Madrid: RA-MA.

Rogers, R. (2011). *Nessus Network Auditing.* Burlington: Elseiver.

Möller, D. P., & Haas, R. E. (2019). *Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications.* ZwitZerland: Springer.

Knowbe4. (05 de 02 de 2021). *Knowbe4*. Obtenido de Find out how vulnerable your network is against ransomware and cryptomining attacks.: https://www.knowbe4.com/ransomware-simulator

CISET. (04 de 11 de 2020). *Centro de Innovación y Soluciones Empresariales y Tecnológicas*. Obtenido de Firewall o cortafuegos: https://www.ciset.es/glosario/444-firewall

Raffino, M. E. (06 de 07 de 2020). *Concepto.de*. Obtenido de Firewall: https://concepto.de/firewall/

Satasiya, D., & Rupal D., R. (15 de 09 de 2016). *IEEE*. Obtenido de Analysis of Software Defined Network firewall (SDF): https://ieeexplore.ieee.org/document/7566125

Jimenez, J. (12 de 06 de 2019). *RedesZone*. Obtenido de Firewall de hardware vs software: diferencias y cuál debo usar para cada situación: https://www.redeszone.net/2019/06/12/diferencias-firewall-hardware-software/

Trend Micro. (02 de 02 de 2018). *Trend Micro.* Obtenido de Seguridad completa para entornos físicos, virtuales, híbridos y en la nube: https://www.trendmicro.es/media/ds/deep-security-datasheet-es.pdf

NeoAttack. (23 de 09 de 2020). *NeoAttack*. Obtenido de Plugin: https://neoattack.com/neowiki/plugin/

Haletky, E. L. (2011). *VMware ESX and ESXi in the Enterprise: Planning Deployment of Virtualization Servers.* Boston: Pearson Education.

Mishchenko, D. (2010). *VMware ESXi: Planning, Implementation, and Security.* Boston: Course Technology.

Kuminsky, K. (2015). *VMware vCenter Cookbook.* Birmingham: Packt Publishing Ltd,.

Wang, X., Hembroff, G., & Yedica, R. (10 de 2010). Using VMware VCenter lab manager in undergraduate education for system administration and network security. *Proceedings of the 2010 ACM conference on Information technology*

education (págs. 43 - 52). New York, NY, USA: Association for Computing Machinery. Obtenido de https://doi.org/10.1145/1867651.1867665

Caballé, X., Cerda, P., Cinalli, F., Herrero, H., & de la cruz, J. (2019). *VMware por vExperts.* España.

Winex. (05 de 03 de 2017). *Winex Academy Xperts*. Obtenido de Segmentación y Direccionamiento IP: http://www.winex.com.py/2017/03/05/segmentacion-y-direccionamiento-ip/

Collado, V. (18 de 05 de 2016). *Microsegmentación NSX | VMware | Adaptix Networks.* Obtenido de Cloud Computing | Adaptix Networks | Cómputo en la Nube: https://www.adaptixnetworks.com/microsegmentacion-nsx/?fbclid=IwAR2DugcTOKfWmAqu1GqRE0j6fUWT9pUq0KNsK3jJxVqcQ6utcsV-luH-uhU

VMware. (18 de 09 de 2020). *VMware*. Obtenido de What is Micro-Segmentation?: https://www.vmware.com/topics/glossary/content/micro-segmentation

Wilmington, G. (15 de 10 de 2019). *VMware*. Obtenido de Overcoming the Barriers to Micro-segmentation: https://blogs.vmware.com/networkvirtualization/2019/10/overcoming-barriers-to-micro-segmentation.html/?fbclid=IwAR2PaPAAGIKckFEQocewgUVfo2WxGonDqLro95XwBC4lop_7CPYfIjC90kg

Red Hat. (03 de 05 de 2020). *Red Hat*. Obtenido de ¿Qué es el kernel de Linux?: https://www.redhat.com/es/topics/linux/what-is-the-linux-kernel

VMware. (31 de 05 de 2019). *VMware*. Obtenido de Data Plane: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.install.doc/GUID-B715387F-983D-4458-B9FB-AD49FCE03E04.html

Bertello, G. (11 de 02 de 2015). *blog.bertello.org*. Obtenido de NSX for Newbies – Part 6: Distributed Logical Router (dLR): https://blog.bertello.org/2015/02/nsx-for-newbies-part-6-distributed-logical-router-dlr/

Bertello, G. (12 de 02 de 2015). *blog.bertello.org*. Obtenido de NSX for Newbies – Part 6: Distributed Logical Router (dLR): https://blog.bertello.org/2015/02/nsx-for-newbies-part-6-distributed-logical-router-dlr/

Oracle. (15 de 04 de 2015). *Oracle*. Obtenido de Installing and Configuring OpenStack in Oracle® Solaris 11.2: https://docs.oracle.com/cd/E36784_01/html/E54155/archover.html

Sities Google. (04 de 09 de 2015). *Sities Google*. Obtenido de Servidores T153 UTEQ: https://sites.google.com/site/servidores153uteq/clusters-de-servidores

VMware. (31 de 05 de 2019). *VMware*. Obtenido de VXLAN: https://docs.vmware.com/en/VMware-Validated-Design/5.0/com.vmware.vvd.sddc-design.doc/GUID-35A129F2-BC5C-49C7-8F6E-2886099ABFA4.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de Configurar VXLAN desde la instancia principal de NSX Manager: https://docs.vmware.com/es/VMware-NSX-Data-Center-for-vSphere/6.3/com.vmware.nsx.cross-vcenter-install.doc/GUID-49BAECC2-B800-4670-AD8C-A5292ED6BC19.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de NSX Installation Workflow and Sample Topology: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.3/com.vmware.nsx.install.doc/GUID-E651F026-B646-4F18-83C3-92CAD0D9533B.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de Agregar una zona de transporte: https://docs.vmware.com/es/VMware-NSX-Data-Center-for-vSphere/6.3/com.vmware.nsx.install.doc/GUID-0B3BD895-8037-48A8-831C-8A8986C3CA42.html

AWS. (01 de 08 de 2020). *AWS*. Obtenido de ¿Qué es DNS?: https://aws.amazon.com/es/route53/what-is-dns/

Microsoft. (31 de 05 de 2017). *Microsoft*. Obtenido de Introducción a Active Directory Domain Services: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Norfipc. (17 de 01 de 2020). *Norfipc*. Obtenido de Como instalar y configurar el servidor web Apache en Windows: https://norfipc.com/internet/instalar-servidor-apache.html

3CX. (13 de 01 de 2021). Obtenido de ¿Qué es SIP – Session Initiation Protocol?: https://www.3cx.es/voip-sip/sip/

Oto, J. (31 de 08 de 2020). *Javieroto*. Obtenido de SQLSERVER. ETL. ORACLE EN LA NUBE USANDO PASS, Y MAS EXPLICACIONES. WHERE.: https://javieroto.wordpress.com/2020/03/21/3-sqlserver-etl-oracle-en-la-nube-usando-pass-y-mas-explicaciones-where/

SAGE. (06 de 02 de 2021). *SAGE*. Obtenido de ¿Qué es Gartner?: https://www.sage.com/en-gb/blog/glossary/what-is-gartner/

Budge, J., O'Malley, C., Blankenship, J., Flug, M., & Nagel, B. (25 de 02 de 2020). *Forrester*. Obtenido de KnowBe4 Is A Leader Among Security Awareness And Training: https://www.knowbe4.com/press/knowbe4-named-a-leader-in-security-awareness-and-training-solutions-evaluation

VMware. (31 de 05 de 2015). *VMware*. Obtenido de Understanding the Controller Cluster Architecture: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.troubleshooting.doc/GUID-0C96F5D7-17BD-4AB1-8DAA-A858EB19FADC.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de Control Plane: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.install.doc/GUID-4E0FEE83-CF2C-45E0-B0E6-177161C3D67C.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de Management Plane: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.install.doc/GUID-69010816-CADD-4BEB-8915-8C8E2C044E0B.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de Control Plane: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.install.doc/GUID-4E0FEE83-CF2C-45E0-B0E6-177161C3D67C.html

VMware. (13 de 12 de 2019). *VMware*. Obtenido de NSX Edge: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.install.doc/GUID-2482B032-F420-432F-A6D0-6CD91506BFCC.html

VMware. (31 de 05 de 2019). *VMware*. Obtenido de NSX and vSphere Distributed Switches: https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.install.doc/GUID-9B22794A-AC90-418D-BAA7-199D9559CF29.html

Sacoto Cabrera, E., Guijarro, L., & Maillé, P. (2020). Game Theoretical Analysis of a Multi-MNO MVNO Business Model in 5G Networks. *Electronics*, 933.

Sacoto Cabera , E. (2021). *Análisis basado en teoría de juegos de modelos de negocio de operadores móviles virtuales en redes 4G y 5G.* Valencia: Universitat Politècnica de València.

Sacoto-Cabrera, E., Sanchis-Cano, A., Guijarro, L., Vidal, J., & Pla, V. (2018). Strategic interaction between operators in the context of spectrum sharing for 5g networks. *Wireless Communications and Mobile Computing*.

Sacoto-Cabrera, E. J., Guijarro, L., Vidal, J., & Pla, V. (2020). Economic feasibility of virtual operators in 5G via network slicing. *Future Generation Computer Systems, 109*, 172-187.

Vimos. (2018). Results of the implementation of a sensor network based on Arduino devices and multiplatform applications using the standard OPC UA. *IEEE Latin America Transactions*, 2496-2502.

Sanchis-Cano, A., Romero, J., Sacoto-Cabrera, E., & Guijarro, L. (2017). Economic feasibility of wireless sensor network-based service provision in a duopoly setting with a monopolist operator. Sensors. *Sensors*.

Sacoto-Cabrera, E., Rodriguez-Bustamante, J., Gallegos-Segovia, P., Arevalo-Quishpi, G., & León-Paredes, G. (2017). Internet of Things: Informatic system for metering with communications MQTT over GPRS for smart meters. 1-6.

Vimos, V., Sacoto, E., & Morales, D. (2016). Conceptual architecture definition: Implementation of a network sensor using Arduino devices and multiplatform applications through OPC UA. *IEEE International Conference on Automatica (ICA-ACCA)*, (págs. 1-5). Pucon.