UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERÍA
CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

DISEÑO DE UNA RED EMPRESARIAL DE TELECOMUNICACIONES PARA MANTENER LA OPERACIÓN Y COMUNICACIÓN DE LAS TECNOLOGÍAS DE VOZ Y DATOS EN LA EMPRESA TABACARCEN

Trabajo de Titulación para optar al título de INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

Autor:
Reyes Chiriboga Viviana Lizbeth

Tutor:
Mcs. José Luis Jinez Tapia

Riobamba, Ecuador.
Año 2022

DERECHOS DE AUTORÍA

Yo, **Viviana Lizbeth Reyes Chiriboga**, con cédula de ciudadanía 1723968697, autor (a) (s) del trabajo de investigación titulado: DISEÑO DE UNA RED EMPRESARIAL DE TELECOMUNICACIONES PARA MANTENER LA OPERACIÓN Y COMUNICACIÓN DE LAS TECNOLOGÍAS DE VOZ Y DATOS EN LA EMPRESA TABACARCEN, certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 14 de noviembre de 2022.

Viviana Lizbeth Reyes Chiriboga

C.I:1723968697

DICTAMEN FAVORABLE DEL TUTOR

Quienes suscribimos, catedráticos designados Tutor y Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **"DISEÑO DE UNA RED EMPRESARIAL DE TELECOMUNICACIONES PARA MANTENER LA OPERACIÓN Y COMUNICACIÓN DE LAS TECNOLOGÍAS DE VOZ Y DATOS EN LA EMPRESA TABACARCEN"**, presentado por **Mcs. José Luis Jinez Tapia**, con cédula de identidad número indique número de cédula, certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha asesorado durante el desarrollo, revisado y evaluado el trabajo de investigación escrito y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.
De conformidad a la normativa aplicable firmamos, en Riobamba a la fecha de su presentación.

Mcs. José Luis Jinez Tapia
Tutor

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNA

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **DISEÑO DE UNA RED EMPRESARIAL DE TELECOMUNICACIONES PARA MANTENER LA OPERACIÓN Y COMUNICACIÓN DE LAS TECNOLOGÍAS DE VOZ Y DATOS EN LA EMPRESA TABACARCEN**, presentado por **Viviana Lizbeth Reyes Chiriboga** con cédula de identidad número **1723968697,** bajo la tutoría de **Mcs. José Luis Jinez Tapia**; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar.
De conformidad a la normativa aplicable firmamos, en Riobamba a la fecha de su presentación.

Presidente del tribunal de grado
Ing. Luis Tello

Firma

Miembro del tribunal de grado
Ing. Carlos Peñafiel

Firma

Miembro del tribunal de grado
Dr. Klever Torres

Tutor
Mcs. José Luis Jinez Tapia

Firma

CERTIFICACIÓN

Que, **VIVIANA LIZBETH REYES CHIRIBOGA** con CC: **1723968697**, estudiante de la Carrera **ELECTRONICA Y TELECOMUNICACIONES. NO VIGENTE**, Facultad de **INGENIERÍA**; ha trabajado bajo mi tutoría el trabajo de investigación titulado " **DISEÑO DE UNA RED EMPRESARIAL DE TELECOMUNICACIONES PARA MANTENER LA OPERACIÓN Y COMUNICACIÓN DE LAS TECNOLOGIAS DE VOZ Y DATOS EN LA EMPRESA TABACARCEN**", cumple con el 0 %, de acuerdo al reporte del sistema Anti plagio **URKUND**, porcentaje aceptado de acuerdo a la reglamentación Institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 19 de agosto de 2022

Mgs. José Luis Jinez
TUTOR. TRABAJO DE INVESTIGACIÓN

DEDICATORIA

Este trabajado va dedicado al esfuerzo de mis padres Santiago Reyes y Pilar Chiriboga, a mi hermana Brishit Reyes por el apoyo incondicional que me ayudaron a no rendirme en este largo trayecto enfrentando las adversidades y enseñándome que cada esfuerzo tendrá su recompensa, así también a cada una de las personas que con palabras de apoyo, aliento y motivación ayudaron a culminar esta meta.

Viviana Reyes Ch.

AGRADECIMIENTOS

Primero quiero empezar agradeciendo a Dios el todo misericordioso por darme la dicha de poder seguir adelante cumpliendo mis sueños. Siendo mi mayor soporte en mi vida universitaria, como en mi vida personal.

Agradezco a mis padres Pilar Chiriboga, Santiago Reyes por ser mi motor, mi pilar fundamental en mi vida, ellos son mi ejemplo a seguir, con su dulzura, amor, severidad me enseñaron ha ser una mujer de bien, una mujer fuerte inteligente que puede retarse a la vida sin problema alguno, gracias por su apoyo, estoy tan agradecida que unas simples palabras quedan cortas, gracias por todo papitos.

A mi hermana Brillo Reyes sin duda ella es mi alegría, mi bebe, mi motivación para poder salir adelante, sin su alegría, carisma, locuras, enojos mi vida no tendría sentido.

A mi novio Hugo Delgado mi mayor apoyo, mi felicidad, mi fuerza, mi paz, la vida nos pone retos muy duros, pero no me cabe duda que el amor es más grande, el amor lo puede todo, Eres mi mayor bendición.

A mis amigos Docentes José Jínez y Leonardo Rentería, gracias por los momentos compartidos dentro y fuera de las aulas, no cabe duda que son los mejores docentes y personas que puedo conocer, gracias por sus enseñanzas, consejos, apoyo que me han brindado en mi vida universitaria, los voy a extrañar.

A mis amigos y familiares que siempre estuvieron a mi lado apoyándome en todo momento, por ser incondicionales conmigo, por no permitir que desmaye en el camino y ser más fuerte cada día.

Viviana L. Reyes Ch.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

En la actualidad las redes de datos han tomado gran importancia para una comunicación óptima debido al impacto de la tecnología en el desarrollo de las actividades diarias en las empresas, por lo tanto, se debe contar con un correcto diseño y despliegue de la infraestructura de red, tomando siempre como punto de partida el objetivo y giro del negocio, con la finalidad de adaptar los recursos tecnológicos para la mejora continua y desarrollo de la empresa. El objetivo principal de este trabajo es implementar una mejora en el diseño de la red LAN (Local Area Network) de datos, voz y video en la empresa TABACARCEN, para realizar un diseño adecuado y óptimo, se identificó el objetivo del negocio, políticas y lineamientos, para adaptar las mejoras tecnologías de la infraestructura de red a los servicios y requerimientos tecnológicos de la empresa. Durante el análisis para el diseño se evaluaron diferentes marcos de trabajos y de referencia, los cuales tienen como objetivo implementar las mejoras prácticas en torno a la gestión, control, diseño y despliegue de tecnología, en base a estándares y normativas. Con base en esto, se diseñó la red de datos para garantizar que la nueva red aporte al crecimiento y mejora continua de la empresa, apegándose a normativas y estándares. Además, para definir todas las mejoras posibles y alcanzables, se tomó como referencia el modelo OSI implementado por la ISO, con este modelo de referencia, se apreció entre la capa 1 hasta la capa 4 todos los estándares, protocolos y topologías que se pueden implementar, para asegurar que la red cumpla con un porcentaje alto de disponibilidad y confiabilidad, igualmente asegurar un mayor grado de madurez respecto al manejo y gestión de la seguridad de la información. Para la selección de los equipos, de igual manera, nos apegamos a fuentes confiables, grupos de investigación y consultoras de TI, como GARTNER Y FORRESTER, los cuales presentan a las diferentes marcas y fabricantes líderes en el mercado en diferentes áreas y sectores de la tecnología, en base a la respuesta de sus

equipos en situaciones críticas o de altos requerimientos, de esta manera aseguramos y corroboramos que la elección del equipamiento tecnología para la infraestructura de red sea la más adecuada.

Para verificar y evaluar el desempeño que tendrá la nueva red, se utilizaron herramientas de simulación que nos permiten conocer el comportamiento y funcionamiento de los equipos en la red, con esto podemos estimar el porcentaje de disponibilidad y confiabilidad de la red, además de contar con información actualizada y relevante que nos permitirán tener métricas para poder evaluar el desempeño y eventualmente realizar mejoras, para garantizar siempre la mejora continua del negocio.

Palabras claves: LACP**,** EVE-NG**,** FORTINET**,** NIC**,** SSH**,** VLAN.

ABSTRACT

Due to the impact of technology on the development of day-to-day work activities, the importance of data networks in all types of businesses has increased every day. As a consequence, it is crucial to rely on the proper design and implementation of the network infrastructure, taking the objective and line of the business into consideration as a preliminary step, with the intention of adjusting technology resources to the ongoing improvement and developmentof the business.The principal objective of this thesis is to upgrade the data, voice, and video LAN network design for TABACARCENbusiness; somepolicies, and guidelinesof the businesswere determined in order to conduct an acceptable and optimal design that would accommodate the technologicalnetworkofthe infrastructureupgrades with the services and technical demands of the organization. Various frameworks and references were assessed during the analysis stageof the design. The implementation of best practices for the management, control, design, and use oftechnology, based on standards and normative, was the major aim.Based on this the data network was designed to ensure the new network contributes to the growth and continuous improvement of the company, relying on normative and standards. Additionally, to achieve the best possible upgrades, the OSI model implemented by the ISO was taken as a reference. Following this model, all the applicable standards, protocols and topologies that can be implementedwere considered from layer 1 to layer 4. This was performed to ensure that the network performs with a high percentage of availability and reliability, at the same time guarantee a higher degree of confidence with respect to the management and operations of information security. For the equipment selection reliable sources, research groups and IT consulting firms like GARTNER Y FORRESTER were considered, which provided

different brands and manufacturers that are leaders in different technology markets and industries. The different equipment was proven under critical situations and high performance events. This way it was ensured and confirmed that the technological equipment for the network infrastructure was the most adequate.Simulation tools that help us comprehend the behavior and operation of the various pieces of equipment were used to estimate the percentage of availability and dependability of the network inorder to test and assess the performance of the new network. In addition to giving out current and pertinent data that will demonstrate measures to assess performance, upgrades should be made concurrently to guarantee the continuous improvement of the company.

Keywords: LACP**,** EVE-NG**,** FORTINET**,** NIC**,** SSH**,**VLAN.

Reviewed by:

Firmado electrónicamente por:
MISHELL GABRIELA SALAO ESPINOZA

Lic. Mishell Salao Espinoza

ENGLISH PROFESSOR

C.C. 0650151566

Introducción

La red empresarial es una colección de unidades de producción con el objetivo de compartir y desarrollar labores tales como ordenar y entrenar donde cada tarea realiza una función particular, pero busca el bien común. En la actualidad las redes empresariales constituyen el elemento central, y tienen gran importancia en los departamentos TI corporativos porque abren puertas a miles de personas para que puedan alcanzar un mayor desarrollo y por ende obtener más beneficios y oportunidades para progresar en cada uno de los negocios y emprendimientos.

Una forma de establecer estrategias de alianza es con Business Networks, programa que se ha convertido en una táctica exitosa en América Latina en la búsqueda de las MIPYMES que tengan expectativas reales en los mercados externos. [1]

Las redes empresariales (Red Corporativa, Campus LAN, Intranet, etc.) son de vital importancia para un crecimiento eficiente y sostenible; en un mundo de cambio constante basado en nuevas tecnologías de la información y la comunicación (TIC). Algunos de estos tienen un tamaño y complejidad que supera al de las redes de transporte. [2]

Al coexistir un gran incremento de los servicios de red y la posibilidad de aumentar el número de usuarios, se ve en la necesidad de llevar el crecimiento de tráfico de datos en la empresa, por lo que es necesario la propuesta del diseño de la infraestructura de telecomunicaciones con sus respectivas mejoras. [3]

Con respecto a la empresa Tabacarcen, en ésta se evidencia ciertas falencias significativas como: la falta de documentación principal sobre el diseño de la red que se maneja hoy en día, excesivas conexiones entre puntos, agujeros de seguridad en el firewall entre otros, para ello se propone una solución mediante el diseño apropiado de una nueva red empresarial de

telecomunicaciones ideal para obtener una óptima seguridad, flexibilidad, resistencia y un buen manejo de información y comunicación con el objeto de que el diseño de esta red esté preparado para el uso de tecnologías avanzadas.

Se diseñó una infraestructura de red de telecomunicaciones con la mejor tecnología en materia de medios transmisión, infraestructura y topología de red, según las necesidades, requerimientos y solicitudes a futuro. En el diseño de una red empresarial se da el uso de una ingeniería estructurada en la que existe 3 capas de forma jerárquica, núcleo (modularidad), distribución (resistencia) y acceso (flexibilidad).[4]

Para establecer una metodología se requiere una investigación experimental analizando el estado actual de la red de telecomunicaciones, tratando de investigar y comprobar la hipótesis previamente establecida directamente en la empresa que se va a aplicar el diseño de red. Adicionalmente se tomó en cuenta la metodología con el diseño de Bottom- up que toma decisiones comenzando con los detalles más pequeños, y los departamentos intentan resolver los problemas iniciales, creando juntos soluciones a otros inconvenientes más grandes en una empresa.

Entre los servicios de red analizados, se tiene la telefonía IP, internet, conexión de host, cámaras IP, red LAN y otros requerimientos para la empresa en el área de importaciones y exportaciones.[5]

La empresa Tabacarcen es un centro logístico en la ciudad de Quito, el cual maneja el 100% de la carga aérea internacional de importación que llega a la ciudad, teniendo clientes que consolidan el 70% de exportación que sale del país. Proporcionando servicios aeroportuarios y logísticos de carga, facilitando la conexión de los participantes del comercio exterior, con recursos humanos comprometidos, moderna infraestructura, basados en procesos seguros y eficientes, para soluciones integrales. [6]

Capítulo I

1.1. Planteamiento del problema

El correcto funcionamiento de la red de datos corporativos es sin duda un factor estratégicamente importante para el desarrollo de las actividades existentes dentro de la organización

En base a la entrevista que se realizó a la empresa Tabacarcen de forma no estructurada, puesto que se desarrolló a manera de conversación con el personal responsable del área de redes, de acuerdo a esa conversación se establece que se debe rediseñar la red debido a que existen falencias dentro de la red corporativa de telecomunicaciones actualmente, tales como las excesivas e innecesarias conexiones entre puntos de red, necesidad de transmisión de datos, voz, la utilización errónea de los diferentes tipos de cable (cable interior usado en exteriores), falta de documentación sobre el estado real de la red(topología), agujeros de seguridad en el firewall a nivel físico, diseño erróneo de la infraestructura de telecomunicaciones, falta de aplicación de protocolos de cableado estructurado y migración de direccionamiento IP inconclusa, además no se cuenta con métricas que permitan evaluar el desempeño de la red.

Llegando a determinar diferentes falencias que dependen del buen diseño de la red. Un dato estadístico realizado dentro de la empresa, en los edificios de exportaciones e importaciones, se comprobó que la conexión de usuarios dentro de la red es alrededor de 80 usuarios activos trabajando en las instalaciones, a su vez cuenta con 60 diferentes usuarios externos diarios que visitan sus instalaciones.

La empresa contiene puntos de red disponibles en diferentes áreas como son: 2 puntos de red en impresoras, 1 punto de red en contabilidad, en el área de transmisiones 6 puntos de red, y finalmente en el área de operaciones cuentan con 7 puntos de red. Existen 50 cámaras entre análogas e IP, mismas que no poseen documentación de la conexión y configuración.

Todo lo anteriormente mencionado nos lleva a plantearnos la siguiente pregunta de investigación ¿Cuál es el diseño apropiado para la infraestructura de red empresarial de la empresa Tabacarcen?

1.2. Objetivos

1.2.1. General

- Diseñar una red empresarial de telecomunicaciones alámbrica para la operación y la comunicación confiable para las tecnologías de voz, video vigilancia y datos mediante el estudio análisis y configuración de equipos de la empresa Tabacarcen.

1.2.2. Específicos

- Analizar las técnicas para el desarrollo e implementación de redes de datos empresariales de telecomunicaciones.
- Analizar la red voz, video y datos mediante el estudio de la infraestructura actual de telecomunicaciones.
- Proponer una nueva arquitectura empresarial de telecomunicaciones mediante la simulación y configuración de los equipos.
- Simular una red empresarial para los edificios de importaciones y exportaciones de la empresa Tabacarcen, mediante software de simulación de redes.

CAPÍTULO II

2. Marco teórico

2.1.Estado del arte

El diseño de la red para una empresa o una organización es más importante al momento de su implementación, hoy en día en la mayoría de las empresas optimizan recursos y tiempo. [1], [3], [5]

Existen varias opciones para asegurar estas redes, el más común es el uso de protocolos de encriptación de datos para los estándares Wifi como WEP y WPA [5] que encripta la información transmitida para proteger su confidencialidad proporcionada por los propios dispositivos. En el caso de VPN y el conjunto de estándares IEEE 802.1X, [7], [8][2] permiten la autenticación y autorización del usuario, existe a un protocolo de seguridad conocido como WPA2 (el estándar 802.11 b) que es una mejora sobre WPA, es la mejor seguridad de protocolo para Wifi actual ya que ayuda a crear redes informáticas inalámbricas. [7] [19] Cuando dos tarjetas inalámbricas están configuradas para usar el mismo protocolo en el mismo canal, estas tarjetas están listas para negociar la conexión en la capa de enlace [18] obteniendo que cada dispositivo 802.11a/b/g puede operar en uno de cuatro modos: modo maestro, modo de gestión (administrador), modo ad hoc y modo de monitor. [18] [7]

Se debe asegurar los principios del diseño de red para adherirse a las buenas prácticas del diseño obteniendo con las siguientes características:

Modularidad: El diseño de red de campo modular permite que él crezca y cambie mediante el uso de bloques de construcción, también conocidos como módulos, permitiendo que la red se expanda fácilmente en lugar de rediseñarse.

Elasticidad: Los diseños de red de campo deben contar con alta disponibilidad (HA) y su tiempo de actividad debe ser del 100 %. [2], [9]

Dentro del análisis de una red empresarial típica, está compuesta por una o más redes LAN interconectadas por uno o más enrutadores, donde el mayor volumen de tráfico sobre la red es basado en aplicaciones web. [10] De lo que cabe en topologías dentro de las redes empresariales se dividen en bloques modulares o jerárquicos con la siguiente retribución: Nivel de acceso, Nivel de distribución y Nivel principal Core.[11], [12]

En el diseño lógico de la red debemos partir del net dentro de la oficina, edificio o campus universitario. La topología en estrella o anillo, si su jerarquía es de dos o tres niveles, si esta conmutada o enrutada, etc. [2], [11], [13]El diseño de redes lógicas también incluye módulos de direccionamiento, nombres, selección de protocolos de enrutamiento, política de seguridad y administración de redes, entre otros. La elección del protocolo de enrutamiento, la seguridad de la red y la estrategia de gestión también es importante. [2], [11]

Con respecto al diseño físico de la Red de dispositivos a nivel 1, 2 y 3 estos deben seleccionarse para la red de área local (LAN) y su conexión a la WAN.

Habitualmente en redes corporativas se utiliza el protocolo OSPF por su eficacia en redes grandes, aunque en el caso de redes con equipos Cisco se utiliza mucho el protocolo EIGRP. [8], [13]Las partes fundamentales del diseño de redes de telecomunicaciones están compuestas por los medios de transmisión como fibra óptica con su estándar ITU-T-G.98X con características de línea óptica para redes de acceso y redes locales,[2], [13] sobre cobre están los cables de par trenzado sin blindaje (UTP) y sus diferentes tipos, para finalizar medios inalámbricos, encontramos un análisis de estándares para comunicaciones inalámbricas Wifi IEEE 802.11 y estándares IEE 802.15 para comunicaciones ópticas sin medios guiados.[11], [14]

Para determinar el tráfico generado por las solicitudes específicas analizadas utilizaremos los parámetros de la norma ETSI EG 202 para asegurar la calidad del servicio.[8]

Alguno de los usuarios prefiere el uso de la arquitectura FTTN (fibra hasta el nodo) tiene el propósito fundamental de abaratar costos para los usuarios y además utilizar la tecnología de cobre existente. [9]

Cuando la red es totalmente pasiva, óptica, y de gran ancho de banda, Tipo PON (Passive Optical Network), el haz de luz del emisor se distribuye hacia múltiples fibras siguiendo diferentes direcciones, o las confina en el sentido opuesto usando técnicas WDM y TDMA.[15]

La fibra óptica utilizada es G.652 C porque da alta capacidad de transmisión a un costo razonable siendo arquitectura más eficiente en el proceso de diseño que se lleva a cabo con FTTN, para llevar fibra a un Nodo con tecnología VDSL2.[16]

También tenemos la tecnología DWDM (Wavelength División Multiplexing) que aprovecha al máximo los recursos de la fibra óptica, pues en una sola fibra se puede enviar diferentes tipos de información usando diferentes longitudes de onda, que pertenecen al mismo hilo de fibra, esto es gracias a que DWDN multiplexa las señales en los extremos y usa como un medio único de transporte a ese hilo de fibra.[4], [17]

Adicional tenemos el servicio de Posicionamiento en una red UTMS prácticamente su funcionamiento se basa en el diseño de una red de telecomunicaciones en base a la frecuencia CDMA para su ubicación se trabajó en este caso vía satélite.[18]

Tenemos las redes de nueva generación NGN no es más que un modelo de arquitectura de red estándar que permite el desarrollo completo de los servicios proporcionados por el servicio IP multimedia, así como el desarrollo, la migración, sustituyendo los servicios de telecomunicaciones actuales.[19]

Este tipo de redes está basado en paquetes que permiten la prestación de servicios de telecomunicaciones y en las que se pueden utilizar varias tecnologías de transporte de banda ancha,

siendo compatible con QoS (Calidad de servicio), y donde las funciones relacionadas con el servicio son independientes de las tecnologías subyacentes involucradas en transporte. [19], [20]

2.1.1. Diseño de la red

Para el diseño de la red se planteó seguir un orden tomando como referencia el modelo OSI, Con esto logramos mantener un orden en base al flujo de información por las distintas capas que viajan los datos, evaluando todas las posibles mejoras en cada capa y evitando omitir cualquier detalle que podría ser de alto impacto para el desempeño de la red. Además, se evalúa el modelo típico de una red confiable, las cuales constan dentro de sus características que la red sea segura, confiable, disponible y que cuente con calidad de servicio para priorizar el ancho de banda o capacidad de canal para ciertas aplicaciones o servicios de alta demanda o críticos.

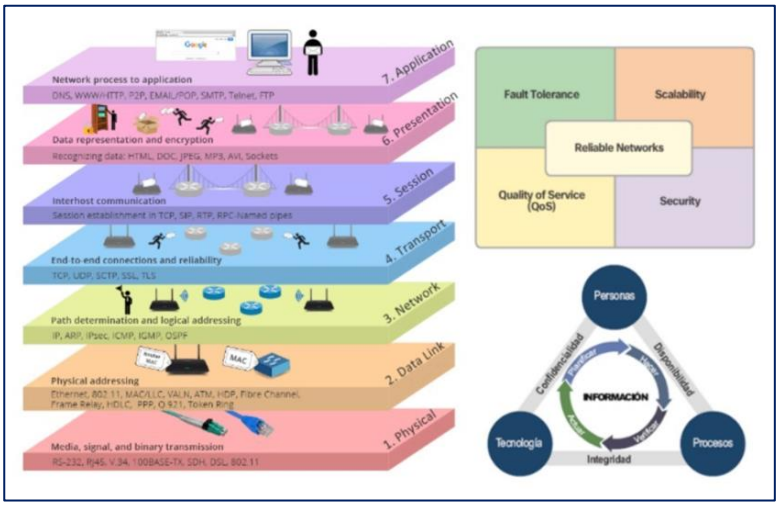


Fig. 1 Modelo OSI-Red Confiable
Fuente:[21]

2.1.2. EVE-NG

Para verificar y evaluar las configuraciones se planteó desarrollar un laboratorio de pruebas virtual en EVE-NG, el cual permite emular los diferentes equipos y realizar las mismas configuraciones que un equipo real, por lo tanto, con esto lograremos crear plantillas de configuración para poder efectuar las mejoras y cambios en caliente en producción, además de tener información de las configuraciones de los equipos para próximos trabajos o mantenimiento de esta.

Fig. 2 EVE- NG
Fuente: Elaboración Propia

2.1.3. Manejo de Tecnología y seguridad.

Algo importante de mencionar es la necesidad de crear una cultura institucional sobre el uso correcto de las tecnologías y el manejo de la información en las instituciones, por dicha razón, se planteó evaluar los diferentes marcos de referencia sobre el manejo de tecnología y la seguridad de la información, se tomó como referencia para el rediseño, COBIT 5, ITIL V4 e ISO 27001.

2.1.4. VLAN

La productividad del usuario y la adaptabilidad de la red son fundamentales para el crecimiento y el éxito empresarial. Las VLAN facilitan el diseño de redes que respaldan los objetivos de la organización. Las principales ventajas de usar VLAN son:

- Seguridad

Los grupos que contienen datos confidenciales están aislados del resto de la red, lo que reduce el riesgo de filtraciones de datos confidenciales.

- Costo reducido

Ahorro de costos debido a actualizaciones de red menos costosas y un uso más eficiente de los enlaces y el ancho de banda existentes.

- Mejor rendimiento

Dividir una red plana de capa 2 en varios grupos de trabajo lógicos (dominios de transmisión) reduce el tráfico de red innecesario y mejora el rendimiento.

- Eficacia de TI

Dividir la red en VLAN reduce la cantidad de dispositivos en el dominio de transmisión.

- Eficacia administrativa

Las VLAN facilitan la administración de la red para los usuarios con requisitos similares que comparten la misma VLAN.

Cada VLAN en la red conmutada corresponde a una red IP; Por lo tanto, al diseñar VLAN, se debe considerar la implementación de un esquema de direccionamiento de red jerárquico. El direccionamiento de red jerárquico significa que los números de red IP se aplican a segmentos de red o VLAN de manera ordenada, lo que permite que la red se vea como un todo. Los bloques contiguos de direcciones de red se reservan y configuran en dispositivos en un área específica de la red.

2.1.5. Modo de transmisión

2.1.5.1.Full dúplex

Ambos dispositivos pueden enviar y recibir datos a través del medio al mismo tiempo. La capa de enlace de datos asume que los medios están disponibles para que ambos nodos transmitan en

todo momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos [23]

2.1.5.2.Interfaz de red (NIC)

La NIC o una tarjeta de interfaz de red se puede interpretar como una tarjeta con puertos para establecer una conexión entre dispositivos. Estos son componentes de hardware que se pueden ubicar interna o externamente en dispositivos que necesitan acceso a Internet. Estos dispositivos pueden controlar la conectividad de la red en un modelo OSI con interfaces o capas. En general, una tarjeta de red puede controlar efectivamente el enlace físico y el enlace de datos entre dispositivos. Las NIC también se conocen con otros nombres, como controladores de interfaz de red, conmutadores LAN, tarjetas de conexión y tarjetas Ethernet. Estos dispositivos son capaces de realizar las funciones de DMA, interrupciones de E/S, partición y transferencia de datos.[24]

2.1.5.3.VPN (Red privada virtual)

La VPN opera dentro de la capa de red del modelo de comunicación de la capa TCP/IP. En particular, la VPN utiliza una infraestructura IPSec (arquitectura de seguridad IP) abierta. Describe la capacidad de crear una conexión protegida cuando se utiliza una red pública. Una VPN cifra su tráfico de Internet y oculta su identidad en directo. Por lo tanto, es muy difícil que terceros rastreen sus actividades en línea y roben datos. El cifrado se realiza en tiempo real.

2.1.6. Dirección lógica (IP)pública

Estos son visibles para cualquiera que navegue por Internet y se utilizan para identificar a los usuarios en redes grandes. Es para servidores que funcionan las 24 horas y puede alquilar varios servidores si es necesario. Es un número que identifica un dispositivo en la red y un punto de acceso a Internet.

2.1.7. Ataque de Capa 2 (Enlace de datos)

Los administradores de red implementan regularmente soluciones de seguridad para proteger los componentes en la Capa 3 y hasta la Capa 7. Usan VPN, firewalls y dispositivos IPS para proteger estos componentes. Si la capa 2 se ve comprometida, todas las capas superiores también se ven afectadas. Por ejemplo, si un atacante con acceso a la red interna captura tramas de Capa 2, toda la seguridad implementada en las capas anteriores se vuelve inútil. Un atacante puede causar mucho daño a una infraestructura LAN de Capa 2. Esta es considerada el enlace más débil. Esto se debe a que la LAN está tradicionalmente bajo el control administrativo de una sola organización. Los ataques contra una infraestructura LAN de capa 2 se describen en la tabla.[1]

Tabla 1 *Ataques de la capa 2*

Ataques tabla MAC	Abarca ataques de saturación de direcciones MAC.
Ataques de VLAN	Contiene ataques VLAN Hopping y VLAN Double-Tagging Esto también poseen ataques entre dispositivos en una misma VLAN.
Ataques de DHCP	Abarca ataques de agotamiento/starvation y suplantación/spoofing DHCP.
Ataques ARP	Incluye la suplantación/spoofing de ARP así como los ataques de envenenamiento/poisoning de ARP.
Ataques de Suplantación de Direcciones	contiene los ataques de suplantación/spoofing de direcciones MAC e IP.

Fuente: Elaboración Propia

2.1.8. PRTG

Una herramienta de monitoreo de red es esencial para mantener el sistema informático en funcionamiento y evitar problemas de red.

El monitoreo de la red también nos ayuda a mejorar la infraestructura de la red, ya que nos brinda información detallada sobre el uso de banda ancha y otros recursos de la red. Las principales ventajas de PRTG Network Monitor son:

- Se evitan pérdidas debidas a fallos de red no detectados.

- Reducir costes porque podemos comprar ancho de banda y hardware en función de las necesidades reales.
- Mejor rendimiento porque la monitorización de la red nos ayuda a evitar la saturación de la red.

2.1.8.1.Protocolo SMNP

El protocolo de árbol de escala múltiple (MSTP) puede asignar un grupo de VLAN a una sola instancia de un árbol de múltiples tramas (MSTI). Esto significa que el protocolo Spanning Tree se aplica específicamente a un grupo de VLAN en lugar de a toda la red.

El protocolo de árbol de expansión múltiple (MSTP) asigna varias VLAN a una instancia de un árbol de expansión, y cada instancia tiene una estructura de árbol de expansión independiente de las otras instancias de árbol de expansión. MSTP tiene las siguientes ventajas:

- El protocolo Múltiple Spinning Tree funciona con la mayoría de las VLAN.
- MSTP admite varias instancias en una única interfaz física. En los enrutadores MX y ACX, puede configurar las interfaces de las instancias RSTP, MSTP y VSTP como puertas de enlace perimetrales. [25]

CAPÍTULO III

3. METODOLOGÍA

3.1.Tipo de investigación

La investigación de la nueva red de la empresa TABACARCEN se desarrolló con base en a los parámetros de confiabilidad, disponibilidad y seguridad de la red, de acuerdo con estos parámetros se ha definido el estudio en base a la investigación de tipo aplicada tecnológica, ya que se realizó mediante la recopilación de conocimientos y el análisis de los parámetros.

De esta manera, se abordó dichos datos mediante una investigación cuantitativa para determinar el grado de confiabilidad de la red en función del tiempo a través del diseño y simulación de la red en un entorno de pruebas, y de manera cualitativa para determinar el nivel y grado de madurez entorno a la seguridad de la información a través de formularios y marcos de trabajos.

De esta manera se logró observar la situación actual de la red en la empresa y mejorarla de una manera eficaz con los métodos más adecuados, siguiendo normativas, estándares y buenas prácticas.

3.2.Diseño de investigación

Para abordar el problema y obtener resultados claros que se permite evaluar el desempeño de la red a través de métricas y porcentajes, se ha tomado como referencia una metodológica basada en un enfoque cuantitativo, desde el cual se obtuvo datos que determinan el porcentaje de disponibilidad y confiabilidad de la red, aplicando métodos probabilísticos y estadísticos a través de fórmulas matemáticas.

Para obtener estos datos usamos herramientas de monitoreo a través del protocolo SNMP, el cual nos entregó información sobre el tiempo de actividad que tuvo la red frente al tiempo inactivo o de

resiliencia, en base a esta información se extraerá los datos a través de la plataforma PRTG (Paessler Router Traffic Grapher) para determinar el porcentaje de disponibilidad de la red.

Sin embargo, para evaluar la madurez de la seguridad de la información, se implementó un método enfocado en un proceso cualitativo a través de herramientas y guías establecidas por marcos de trabajo o de referencia, los cuales evalúan ciertos requerimientos que debe cumplir la empresa para poder asegurar la integridad y seguridad de la información, como parte de las herramientas para evaluar este parámetro se tendrá tablas de Excel y listas de seguimiento o cumplimiento.

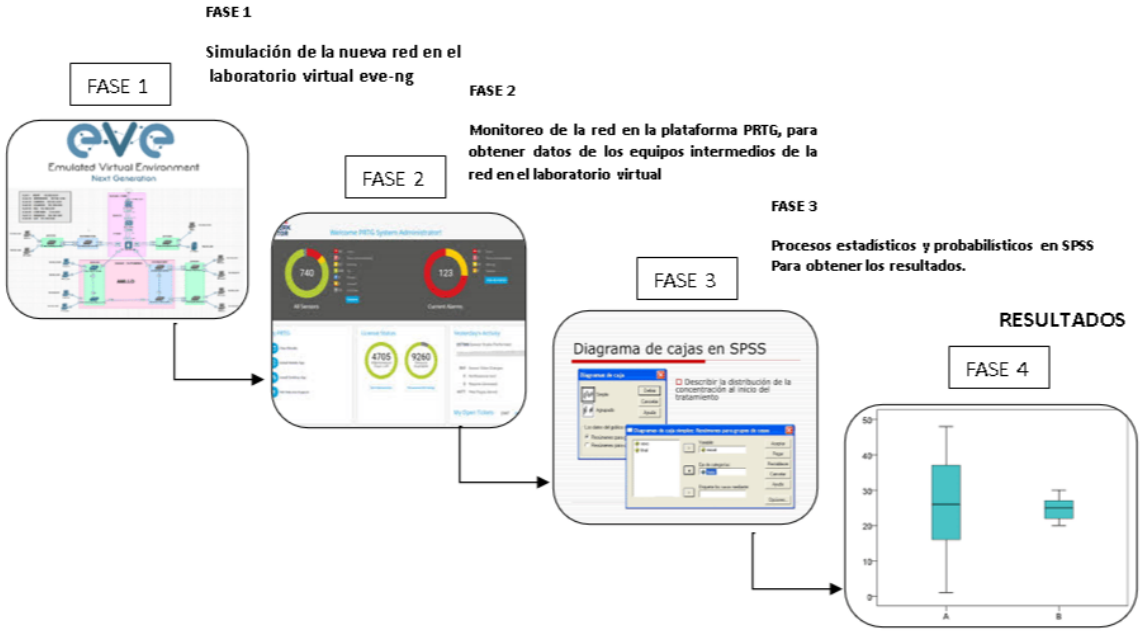


Fig. 1Proceso para el diseño de investigación- Autoría

3.3.Población y muestra

3.3.1. Población:

La población establecida para el estudio y análisis de la nueva red esta seleccionada en base a los parámetros o variables a estudiar, por lo tanto, para estudiar el grado de disponibilidad a partir

de una investigación cuantitativa, se tomó como población los equipos intermedios de la red, los cuales se encuentran ordenados en un modelo de capas en base a las acciones y características que desarrollarán dentro de la infraestructura de la red para evaluar la confiabilidad y disponibilidad.

Para estudiar los parámetros y variables relacionadas al estudio cualitativo, se toma como población todos los procesos, documentación e información sobre el manejo de la tecnología y la información de la empresa, con estos datos entonces se podrá determinar el grado y nivel de madurez evaluando la seguridad de esta.

3.3.2. Muestra:

La muestra se tomó del conjunto de datos mediante un proceso aleatorio y su tamaño dependió de la cantidad de datos previamente establecidos en la población, mediante las distintas configuraciones del tamaño muestral que fueron analizadas para un correcto desempeño según los requerimientos de la red de Telecomunicaciones.

Para las muestras de los parámetros y variables cualitativas se tomó como referencia toda la documentación e información brindada por la empresa TABACARCEN, con lo cual, se logró llenar el marco de trabajo para la seguridad de la información que se encuentra basado en la NIST.

3.4.Técnica:

Simulación: Esta técnica consiste en la simulación que ayuda a crear escenarios en condiciones reales, a través de una serie de procedimientos, análisis y configuraciones realizadas para lograr un resultado óptimo.

3.5.Fuentes de recopilación de información

Para el presente trabajo de investigación se realizó la recopilación de información investigativa y experimental acerca del diseño de una red empresarial así mismo sobre su infraestructura de redes.

Se llegó a realizar entrevistas no estructuradas o no dirigidas, para obtener un diagrama detallado sobre la red actual de la empresa y la configuración de los dispositivos que la componen.

Los repositorios como base de datos consultada contienen a ScienceDirect, y IEEE con una restricción de publicación que no exceda a 5 años.

3.6.Operacionalización de la variable

Tabla 2
Operacionalización de la Variable

Variable	Concepto	Indicadores	Técnicas e Instrumentación
Independiente Diseño de una red empresarial de telecomunicaciones para mantener la operación y comunicación de las tecnologías de voz y datos en la empresa TABACARCEN	La red empresarial de telecomunicaciones permite la conexión inalámbrica e inalámbrica entre los dispositivos y equipos de red mediante la aplicación de diferentes tipos de técnicas.	-Redireccionamiento de la red. -Configuración de los diferentes equipos para la comunicación. -Diseño de la red de comunicación (voz, datos, video) -Seguridad de la red de telecomunicaciones.	EVE- NG Fortinet VMware Workstatic Putty WinSCP PRTG
Dependiente Optimización de la red de Telecomunicaciones en la empresa TABACARCEN	El rendimiento de la red representa los parámetros que se van a evaluar para posteriormente dar un punto de vista sobre su estado.	-Pérdida de Paquetes -Calidad de servicio QoS -Confiabilidad -Disponibilidad	Aplicaciones para medir el tráfico de una red inalámbrica Software de análisis de tráfico en tiempo real.

Fuente: Elaboración Propia

3.7.Procedimiento y análisis

La empresa consta de 5 áreas de manera general, las cuales a su vez comparten servicios y recursos para operar de forma normal, sin embargo, es necesario priorizar ciertas áreas relacionadas a cada subred, con la finalidad de presentar mayor importancia a las operaciones y funciones de esta,

en base a esta idea principal, se tomó como referencia el modelo OSI para ir evaluando las características y funcionalidades que tuvo dicha arquitectura o modelo de red.

3.8.Situación actual de la red

Tabla 3
Oficinas- Edificio exportaciones

Segundo Piso				
Departamento	Usuarios de red	PC	Laptop	Impresora
Recepción principal	1	1	0	0
Desarrollo Humano	2	0	2	1
Business Inteling	1	0	1	0
Secretaria del gerente	1	1	0	0
Jefe financiero	1	0	1	0
Compras	1	0	1	0
Cobranzas y facturación	1	0	1	0
Sistemas	4	1	3	0
Asistente de control interno	1	0	1	0
Gerente de Operaciones	1	0	1	0
Asistencia Gerencia	1	0	1	0
Seguridad	1	0	1	0

Fuente: Elaboración Propia

3.8.1. Cuartos de comunicación del edifico de exportaciones Tabacarcen

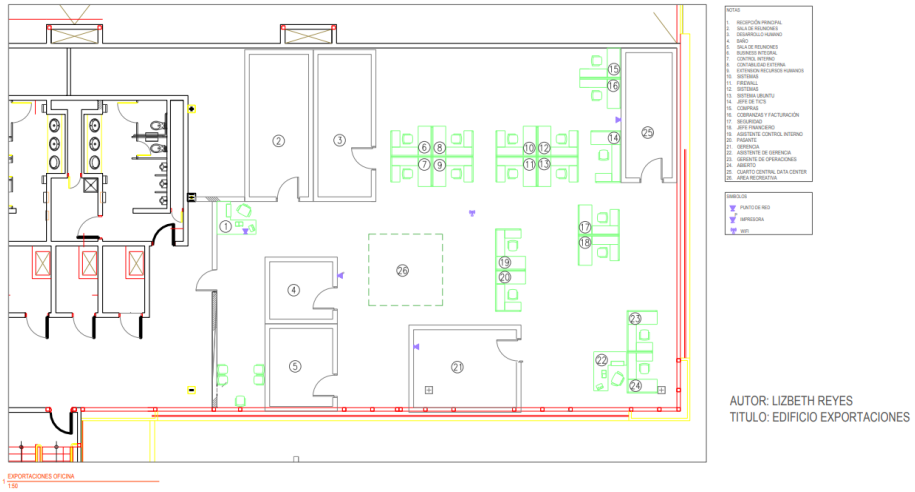


Fig. 4 Plano exportaciones-levantamiento - Autoría
Fuente: Elaboración Propia

Tabla 4

Descripción de equipos / comunicaciones-exportaciones

Cuarto 1 de comunicaciones							
Descripción	Marca	Modelo	Puertos	Características	Características puerto	Cantidad	Unidad de Rack
Switch	Aruba	1930 stwitch	24P	1G BASE-T Class 4 PoE/ 4T 10G SFP +	PUERTOS - 10GbE SFP+ port	1	1
Switch	Tp-link	tl-SG1024	24P	NS	NS	1	1
Router	Linksys	Linksys	5P	SE3005	NS	2	1
UPS	MARCA CDP	MODELO R-SMART1510		NS	NS	1	1

Fuente: Elaboración Propia

Fig. 5 Equipos-cuarto frio1

Fuente: Elaboración Propia

TABLA 5

Descripción de equipos / comunicaciones-exportaciones

Cuarto 2 de comunicaciones							
Descripción	Marca	Modelo	Puertos	Características	Características puerto	Cantidad	Unidad de Rack
Switch	tp-link	1930 stwitch	24P			1	1
Convertidor de medio WDM Fast Ethernet	tp-link	mc112cs	2P	Convierte el cable de fibra 100base-FX a a cable de cobre TX o viceversa		4	1
UPS	Forza	fx-1500 lcd				1	1

Fuente: Elaboración Propia

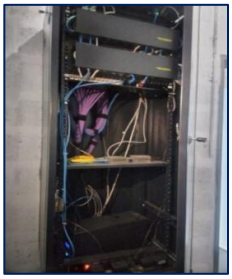


Fig. 6 Equipos-cuarto frio2
Fuente: Elaboración Propia

3.8.2. Cuarto frio celebrity

Tabla 6
Descripción de equipos / Cuarto frio celebrity

Descripción	Marca	Modelo	Puertos	Características	Cantidad
Switch	DC-LINK	00l75985(I-O)	24P	1G*coe smartswitch	1

Fuente: Elaboración Propia

3.8.3. Cuartos de comunicación del edifico de importaciones Tabacarcen

Business Center

Tabla 7 Descripción de equipos /Business Center - importaciones

Cuarto 1 – Para exteriores						
Descripción	Marca	Modelo	Puertos	Características	Características puerto Cantidad	Unidad de Rack
Switch	Aruba	1930 stwitch	24P	1G BASE-T Class 4 PoE/ 4T 10G SFP +	PUERTOS -10GbE SFP+ port 1	1

Fuente: Elaboración Propia

Fig. 7 Equipos- cuarto 1 business
Fuente: Elaboración Propia

Business Bar

Tabla 8
Descripción de equipos / Business Bar - importaciones

Red usuarios						
Descripción	Marca	Modelo	Puertos	Características	Cantidad	Unidad de Rack
Switch	Oruba	1930 stwitch	8P	administrable	1	1

Fuente: Elaboración Propia

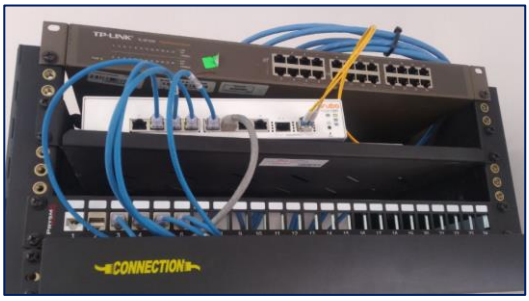


Fig. 8 Equipos- Business bar
Fuente: Elaboración Propia

3.8.4. Cuarto de comunicaciones Aduana

Tabla 9
Descripción de equipos/ Rack de Operaciones

Descripción	Marca	Modelo	Puertos	Características	Características puerto	Cantidad	Unidad de Rack
Switch	Oruba	1930 stwitch	18P	1G BASE-T Class 4 PoE/ 4T 10G SFP +	PUERTOS - 10GbE SFP+ port	1	1

Fuente: Elaboración Propia

Tabla 10
Descripción de equipos/ Cuarto de seguridad

Descripción	Marca	Modelo		
Switch	TP LINK	GMA	NO administrable	

Fuente: Elaboración Propia

Tabla 11
Descripción de equipos / Zona de distribución

Descripción	Marca	Modelo	Puertos	Características
Switch	Aruba	sn	sn	Con servicio a sistemas de combi. VLan50

Fuente: Elaboración Propia

3.9.Planos antiguos de la empresa

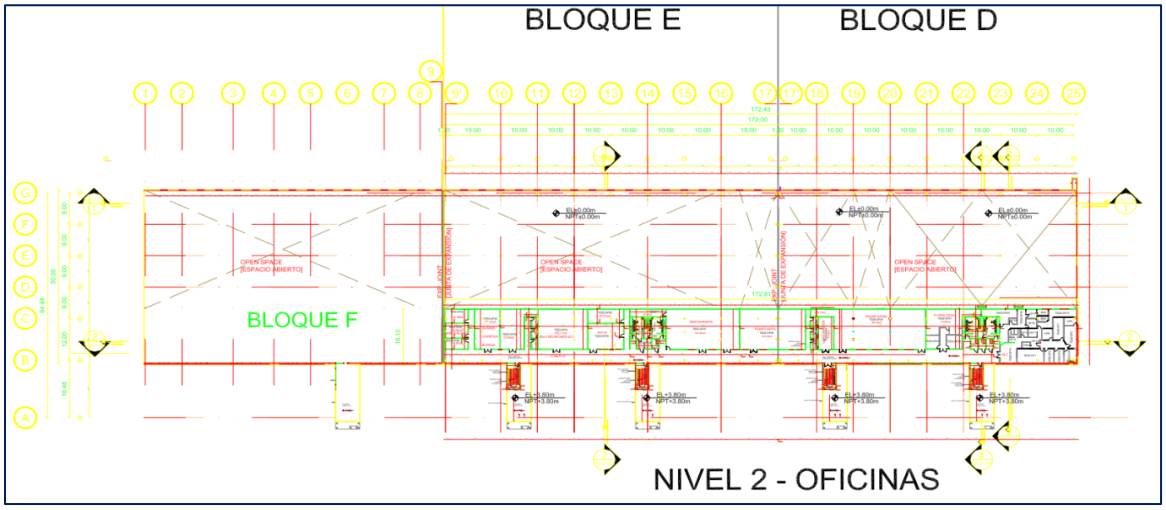


Fig. 9 Plano Edificio de exportaciones
Fuente: Tabacarcen

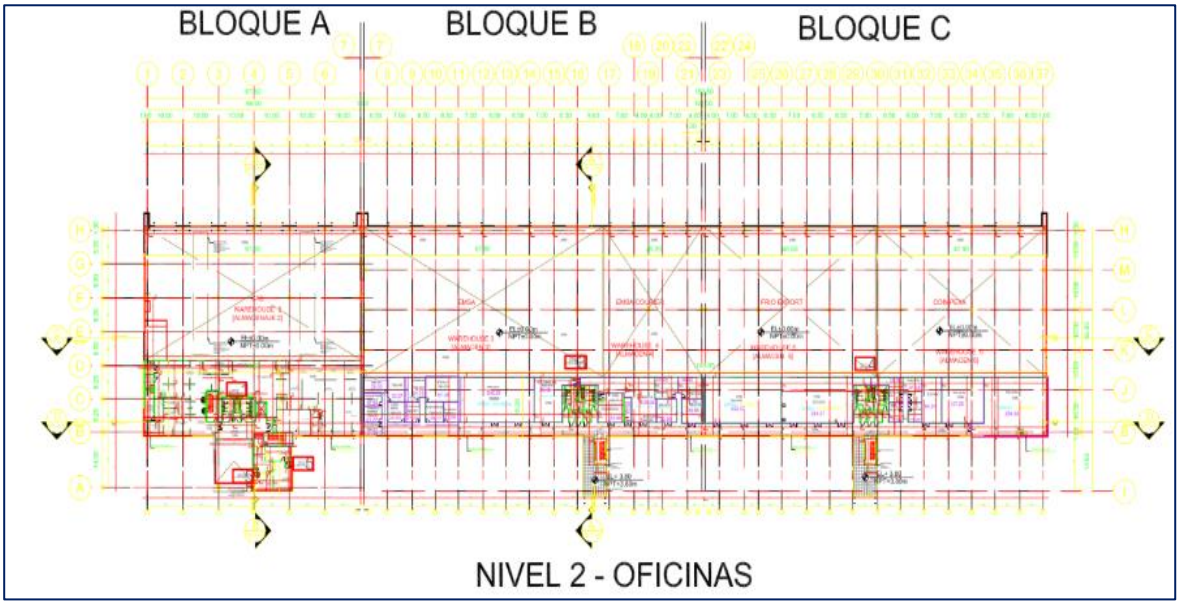


Fig. 20Plano edificio de importaciones

Fuente: Tabacarcen

3.10. Topología A

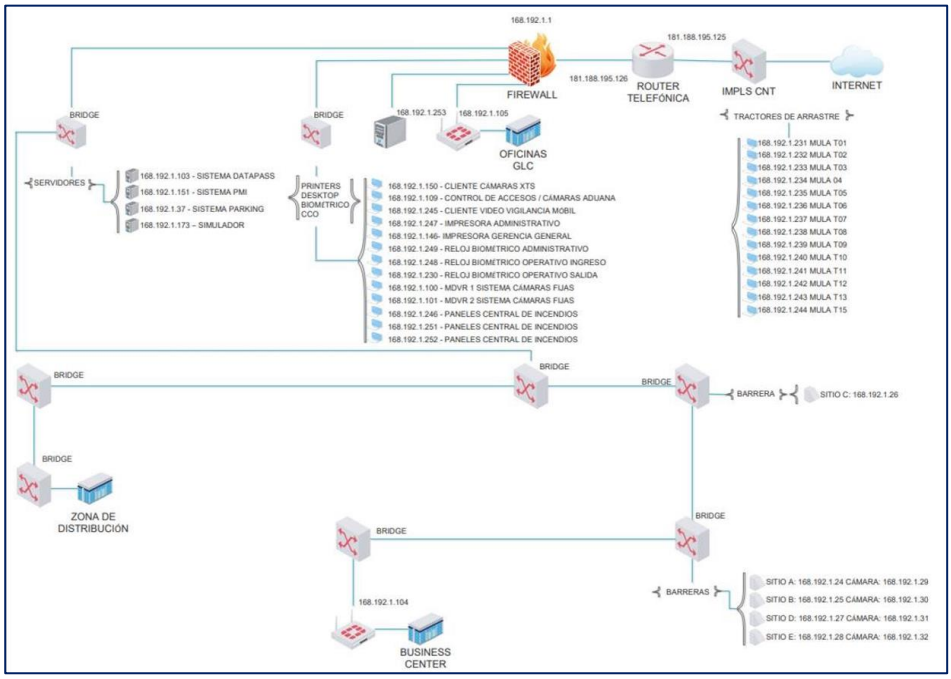


Fig. 11 Topología antigua de la red
Fuente: Elaboración Propia

3.11. Evaluación de requerimientos, técnicas y configuraciones en base a marcos de referencia.

Antes de iniciar con el estudio de los requerimientos y las configuraciones, es importante hacer un diagnóstico de las bases iniciales para un correcto diseño e implementación de una red empresarial de datos, no solamente consta de la parte de configuraciones e infraestructura de red como equipos intermedios y finales, esa área es el accionar o las herramientas que se encuentran implementas basadas en varias políticas y lineamientos establecidas previamente por un grupo interesado de la empresa.

Para cualquier parámetro o factor de tecnología que se agregue al negocio debe girar en torno al objetivo de este, es decir que debemos perseguir la misma idea de negocio y respetar las reglas de

este, por lo tanto, la infraestructura del diseño debe tiene como objetivo aportar al negocio y mejorar al mismo para su desarrollo.

Se debe considerar por lo tanto el tipo de negocio, el área o entorno donde se desarrolla, con este contexto claro, se podrá dar una solución a medida para adaptar la infraestructura tecnológica a las necesidades y requerimientos del negocio para dar soporte y mejora en base a los objetivos de este. Con esto claro se analizará algunos de los principales marcos de referencia para la gestión, gobierno, implementación y accionar de las tecnologías en los entornos empresariales.

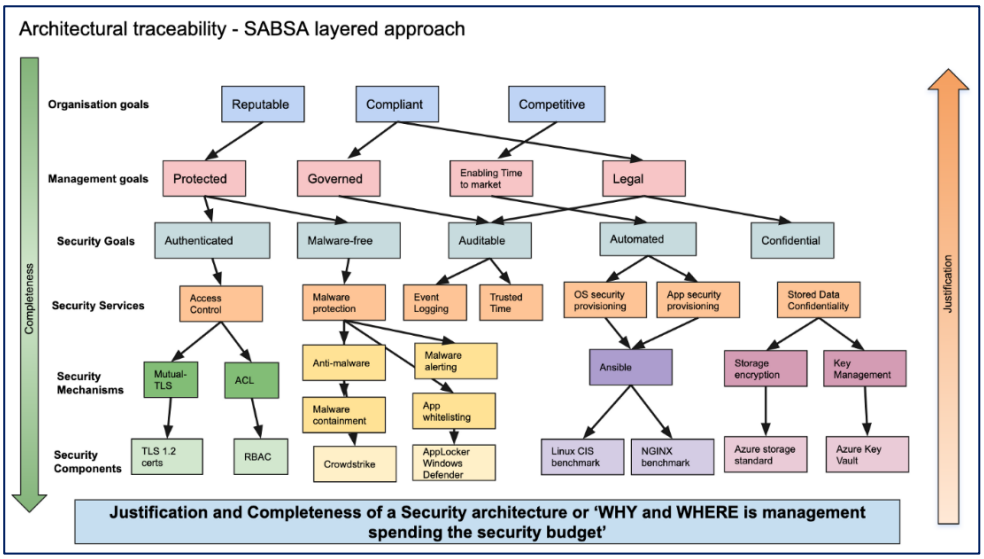


Fig. 12 Marco de referencia basado en SABSA
Fuente:[26]

La elección de equipos y las configuraciones deben ser seleccionadas para respetar y apegarse a políticas y lineamientos establecidos por los altos mandos con el objetivo de mantener el giro del negocio y mejorar el desempeño de este, por lo tanto, es de suma importancia establecer previamente las políticas y lineamientos basadas en los objetivos del negocio, esto se logra eventualmente creando grupos de trabajos los cuales siguen metodologías o buenas prácticas para sustentar ideas y acciones, tomando como partida algunos modelos o marcos de referencia.

Dentro de todos estos marcos de referencia siempre existe un ciclo que nos permite tener una retroalimentación continua para poder evaluar, como por ejemplo el ciclo de Deming o también conocido como PDCA, con la finalidad de poder medir el desempeño o rendimiento de un proceso o tarea, de esta manera se podrá tener presente la existencia de errores para poder tomar acciones sobre el mismo, logrando con ello mantener el ciclo de vida continuo del negocio, por lo tanto, es de suma importancia tener diferentes métricas para poder medir y evaluar cualquier proceso, función o tarea, con la finalidad de mantenerse siempre en la mejora continua.

Con dicho preámbulo, podemos tomar en cuenta, la necesidad de tener claros los principios, objetivos, lineamientos, políticas y procesos establecidos, con lo cual se logró apegar toda la infraestructura tecnología para el bienestar y la mejora continua de la empresa, para conseguir una correcta elección en base a la necesidades del negocio, es importante tomar como referencia y guía las diferentes normas y estándares internacionales, los cuales buscan el correcto funcionamiento de los equipos, medios y elementos tecnológicos que forman parte de toda una infraestructura, de igual manera, existen marcos de referencias creados por grupos y organizaciones internacionales que buscan generar buenas prácticas dentro de entornos empresariales, tomando como referencia normativas como CIS, CSC COBIT 5, ISA, ISO/IEC, NIST, etc. En base a las funciones y características que tiene de la red, es necesario seleccionar los equipos de manera adecuada, para esto podemos apegarnos a estadísticas u organizaciones que evalúan el desempeño de los mismo en situaciones críticas o de alto impacto, mediante lo antes mencionado se hace referencia el Cuadrante Mágico de Gartner, Forrester.

3.11.1 Equipos de red Firewall líderes en el mercado

Dentro de equipos líderes de red en el mercado se dispone el Firewall, posicionándose en categoría fuerte en parámetros y respondiendo frente a los diferentes ataques que han desarrollado, las resistencias, disponibilidad, vulnerabilidades, parches, etc.

Además, se considera importante entre ellos el cuadrante de Garther, siendo parte de ello Fortinet uno de los partícipes líderes de equipos corta fuego en el Firewall.

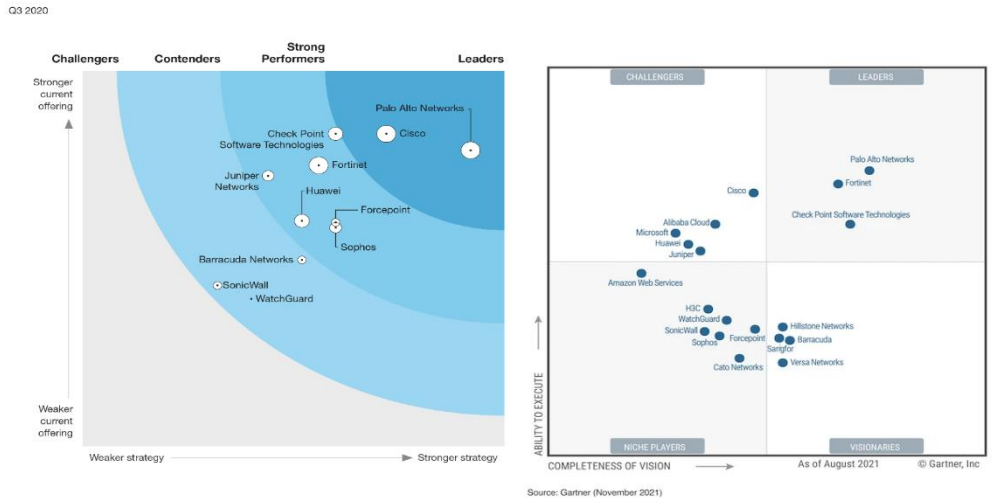


Fig.13 Equipos de red Firewall lideres en el mercado

Fuente: [27]

3.11.2 Equipos de red para LAN (Conmutación y Enrutamiento) líderes en el mercado.

Para equipos de Red LAN se basa en manera general tomando en cuenta la conmutación y enrutamiento. Siendo parte del mercado líder Cisco, Fortinet y Aruba dando énfasis en las soluciones inalámbricas de Forrester siendo Aruba una de sus primeras líderes.

Fig.14 Equipos de red para LAN (Conmutación y Enrutamiento líderes en el mercado

Fuente: [27]

Seguridad de dispositivos y plataformas finales de red líderes en el mercado.

En el mercado de seguridad de la información existen muchas plataformas para satisfacer las necesidades de las empresas. Existe la AV compartidas que permite hacer un análisis más profundo sobre los diferentes tipos de antivirus y su respuesta, teniendo como resultados falsos positivos o falsos negativos puedan existir.

Fig. 15 Seguridad de dispositivos y plataformas finales de red líderes en el mercado.

Fuente: [27]

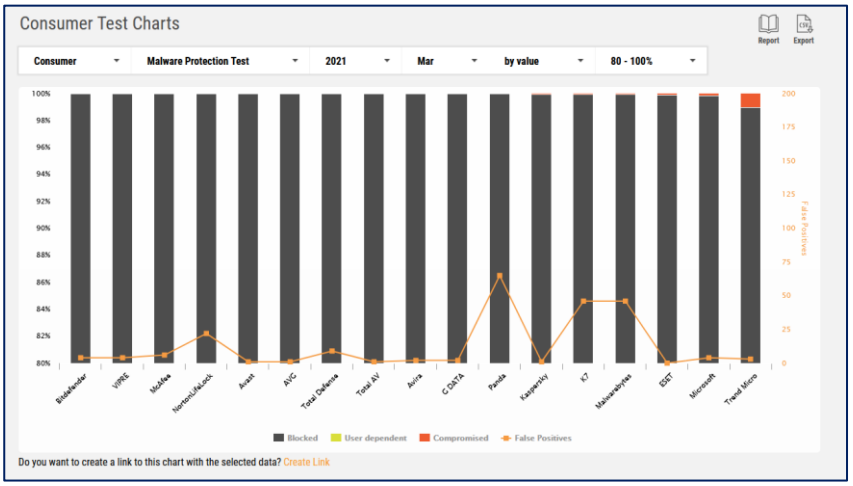


Fig. 16 AV comparativas
Fuente: [27]

Existe el ciclo de exageración para la seguridad de la red, en base de lo que es Garther y su evolución en la seguridad de la red con cada una de las recomendaciones, teniendo en cuenta IPS. Con estas referencias se definió que marca y modelo de equipos de red colocar dentro de la infraestructura, además se evaluó algunos otros puntos como las vulnerabilidades de los mismo y la atención de los fabricantes para reportar o parchar dichas brechas de seguridad en los equipos que pueden verse reflejados como un riesgo para el negocio, existe diferentes plataformas que nos permiten mantenernos informados respecto a esto, como es el caso de CVE.

CAPITULO IV

4. Resultados-discusión

4.1.Propuestas

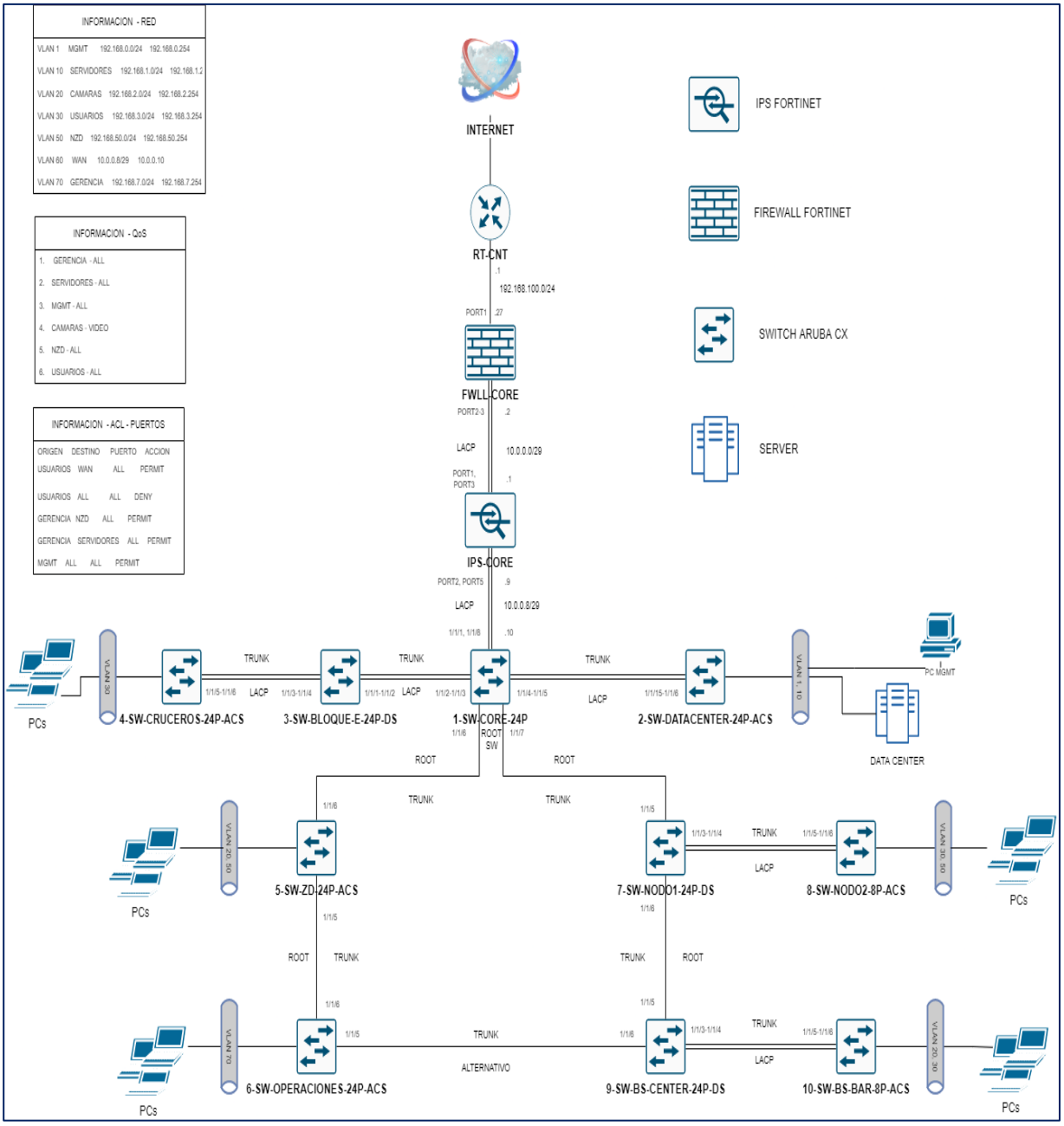


Fig. 17 Propuesta de red
Fuente: Elaboración Propia

4.1.1 Tabla de Direccionamiento

Tabla 12
Tabla de Direccionamiento

NOMBRE	VLAN	Dirección de red	Prefijo	Mascara	Rango Disponible	Broadcast
SERVIDORES	10	192.168.1.0	/24	255.255.255.0	192.168.1.1 - 192.168.1.254	192.168.1.255
CAMARAS	20	192.168.2.0	/24	255.255.255.0	192.168.2.1 - 192.168.2.254	192.168.2.255
USUARIOS	30	192.168.3.0	/24	255.255.255.0	192.168.3.1 - 192.168.3.254	192.168.3.255
N2D	50	192.168.5.0	/24	255.255.255.0	192.168.5.1 - 192.168.5.254	192.168.5.255
GERENCIA	70	192.168.7.0	/24	255.255.255.0	192.168.7.1 - 192.168.7.254	192.168.7.255
MGMT	1	192.168.0.0	/24	255.255.255.0	192.168.0.1 - 192.168.0.254	192.168.0.255
WAN	60	10.0.0.8	/29	255.255.248.0	10.0.0.9 - 10.0.0.12	10.0.0.13
FWLL-IPS	-	10.0.0.0	/29	255.255.248.0	10.0.0.1 - 10.0.0.4	10.0.0.5

DISPOSITIVO	INTERFAZ	DIRECCION IPV4	MASCARA DE SUBRED	PUERTA DE ENLANCE	CAPA
FWLL-CORE	PORT1	192.168.100.27	255.255.255.0	NO APLICA	CORE
	LACP (PORT2-3)	10.0.0.2	255.255.255.248	NO APLICA	CORE
IPS-CORE	LACP (PORT1,3)	10.0.0.1	255.255.255.248	NO APLICA	CORE
	LACP (PORT2,5)	10.0.0.9	255.255.255.248	NO APLICA	CORE
1-SW-CORE-24P	VLAN 1	192.168.0.254	255.255.255.0	10.0.0.9	CORE
	VLAN 10	192.168.1.254	255.255.255.0	10.0.0.9	CORE
	VLAN 20	192.168.2.254	255.255.255.0	10.0.0.9	CORE
	VLAN 30	192.168.3.254	255.255.255.0	10.0.0.9	CORE
	VLAN 50	192.168.5.254	255.255.255.0	10.0.0.9	CORE
	VLAN 60	10.0.0.10	255.255.255.248	10.0.0.9	CORE
	VLAN 70	192.168.7.254	255.255.255.0	10.0.0.9	CORE
2-SW-DATACENTER-24P-ACS	VLAN 1	192.168.0.2	255.255.255.0	192.168.0.254	ACCESO
3-SW-BLOQUE-E-24P-DS	VLAN 1	192.168.0.3	255.255.255.0	192.168.0.254	DISTRIBUCIÓN
4-SW-CRUCEROS-24P-ACS	VLAN 1	192.168.0.4	255.255.255.0	192.168.0.254	ACCESO
5-SW-ZD-24P-ACS	VLAN 1	192.168.0.5	255.255.255.0	192.168.0.254	ACCESO

6-SW-OPERACIONES-24P-ACS	VLAN 1	192.168.0.6	255.255.255.0	192.168.0.254	ACCESO
7-SW-NODO1-24P-DS	VLAN 1	192.168.0.7	255.255.255.0	192.168.0.254	DISTRIBUCIÓN
8-SW-NODO2-8P-ACS	VLAN 1	192.168.0.8	255.255.255.0	192.168.0.254	ACCESO
9-SW-BS-CENTER-24P-DS	VLAN 1	192.168.0.9	255.255.255.0	192.168.0.254	DISTRIBUCIÓN
10-SW-BS-BAR-8P-ACS	VLAN 1	192.168.0.10	255.255.255.0	192.168.0.254	ACCESO
PC MGMT	VLAN 1	192.168.0.253	255.255.255.0	192.168.0.254	ACCESO

Fuente: Elaboración Propia

4.2.Simulación

Antes de iniciar con las configuraciones a nivel de capas, fue necesario preparar el dispositivo de red con las configuraciones iniciales respecto al inicio de sesión al equipo y los métodos de acceso, igual manera configurar la fecha para analizar en caso de amenaza a través de los logs.

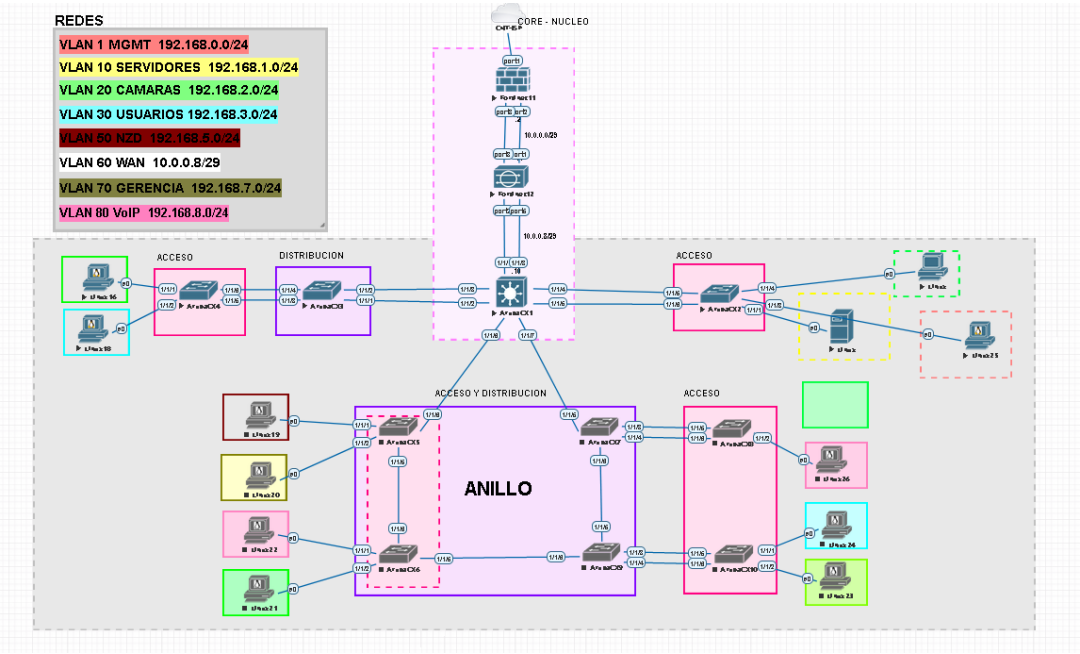
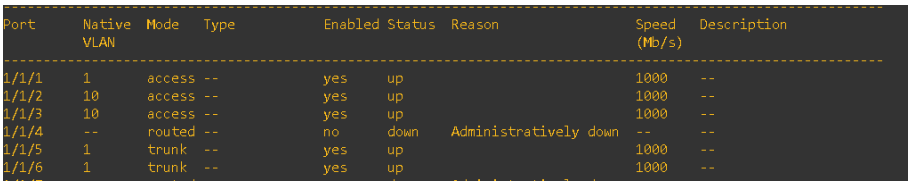


Fig. 18 Simulación de red en EVE-NG
Fuente: Elaboración Propia

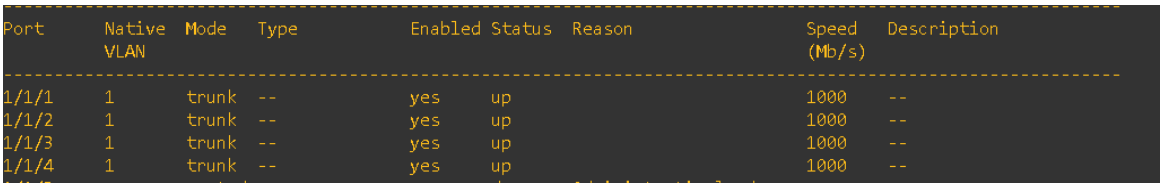
4.2.1 Ancho de banda

El ancho de banda hace referencia a la velocidad de red, expresa en velocidad bits por segundo bit/s, también conocida como capacidad de canal, donde la capa de acceso se conecta a los dispositivos de red, obteniendo las diferentes velocidades de interfaces que poseen los equipos.



Port	Native VLAN	Mode	Type	Enabled	Status	Reason	Speed (Mb/s)	Description
1/1/1	1	access	--	yes	up		1000	--
1/1/2	10	access	--	yes	up		1000	--
1/1/3	10	access	--	yes	up		1000	--
1/1/4	--	routed	--	no	down	Administratively down	--	--
1/1/5	1	trunk	--	yes	up		1000	--
1/1/6	1	trunk	--	yes	up		1000	--

Fig. 19Acceso- Velocidad de interface que tienen los equipos
Fuente: Elaboración Propia



Port	Native VLAN	Mode	Type	Enabled	Status	Reason	Speed (Mb/s)	Description
1/1/1	1	trunk	--	yes	up		1000	--
1/1/2	1	trunk	--	yes	up		1000	--
1/1/3	1	trunk	--	yes	up		1000	--
1/1/4	1	trunk	--	yes	up		1000	--

Fig. 20 Distribución- Velocidad de interface que tienen los equipos
Fuente: Elaboración Propia

4.2.2 Calidad de servicio QoS

Para mantener la calidad del servicio es necesario la velocidad y prioridad sobre el resto del tráfico. Para ello se asigna un ancho de banda diferente para cada red en traffic Shapers.

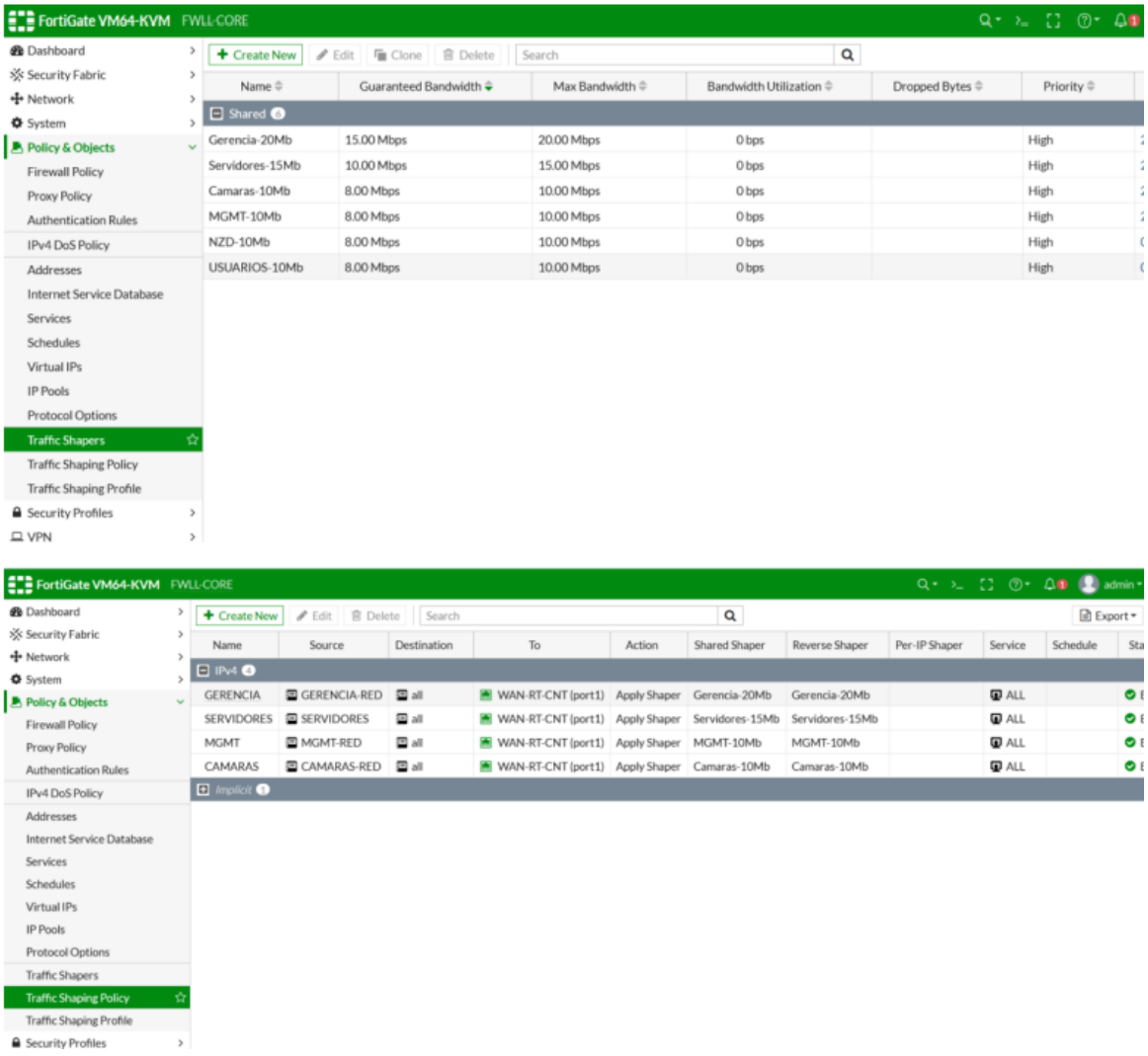


Fig. 21 Calidad de servicio QoS
Fuente: Elaboración Propia

4.3. Pruebas de hipótesis

4.3.1. Prueba de hipótesis 1 - Perdida de paquetes

- Hipótesis Nula

$$H_0: \mu_{RA} = \mu_{RN}$$

Los promedios de las pérdidas de paquetes de la red antigua y la red nueva, no son significativamente diferentes, siendo:

μ_{RA} = Perdida de paquetes de la nueva red

μ_{RN}= Perdida de paquetes de la antigua red

- Hipótesis alternativa

$$H_1: \mu_{RA} \neq \mu_{RN}$$

Los promedios de las pérdidas de paquetes de la red antigua y la red nueva, son significativamente diferentes.

- Media

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
paquetes	Se asumen varianzas iguales	91,002	,000	-6,440	97	,000	-22,89224	3,55454	-29,94701	-15,83748
	No se asumen varianzas iguales			-6,494	59,174	,000	-22,89224	3,52516	-29,94564	-15,83885

Fig. 22 Prueba T
Fuente: Elaboración Propia

Decisión: como $p - valor = 0.000 < 0.05$ se acepta la hipótesis alternativa, es decir los promedios de las pérdidas de paquetes de la red antigua y la red nueva, son significativamente diferentes.

Tabla 13
Estadísticas de Grupo

Estadísticas de grupo					
	Red	**N**	**Media**	**Desv. Desviación**	**Desv. Error promedio**
paquetes	RN	49	76,3878	7,60980	1,08711
	RA	50	99,2800	23,71174	3,35335

Fuente: Elaboración Propia

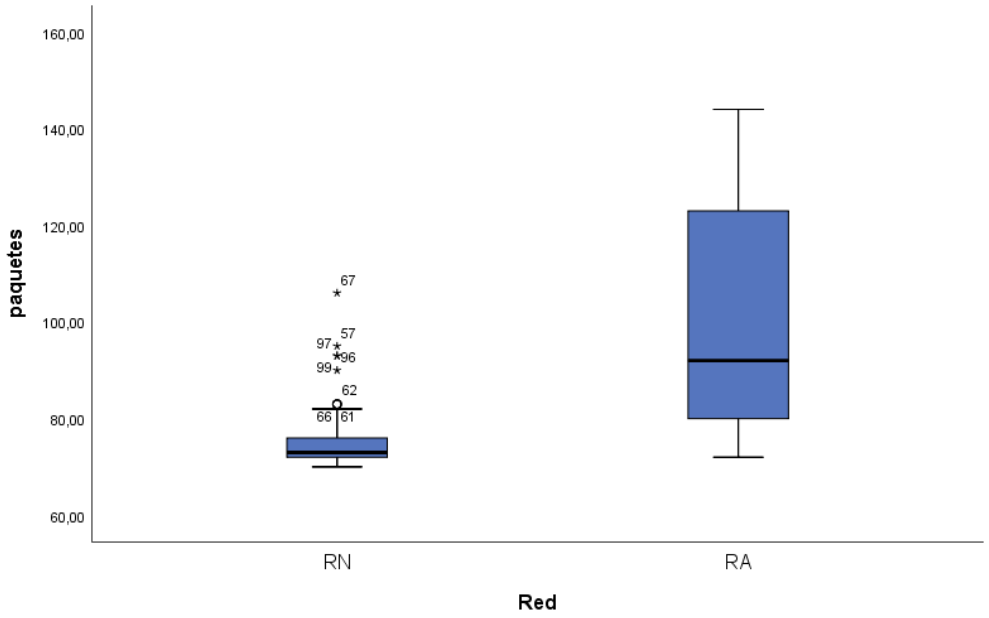


Fig. 23 Diagrama de caja
Fuente: Elaboración Propia

La pérdida de paquetes para la red nueva ha disminuido notoriamente en la comparación de cajas, adicional se ven datos atípicos debido a que se realizó pruebas en la web y existe posibles caídas de servidores o interferencias en el servicio de internet, por esa razón se tiene datos atípicos.

4.3.2. Prueba de hipótesis 2 – Tiempo de respuesta

- Hipótesis Nula

$$H_0: \mu_{RA} = \mu_{RN}$$

Los promedios de tiempo de respuesta de la red antigua y la red nueva, no son significativamente diferentes.

- Hipótesis alternativa

$$H_1: \mu_{RA} \neq \mu_{RN}$$

Los promedios de tiempo de respuesta de la red antigua y la red nueva, son significativamente diferentes.

- Media

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Tiempo	Se asumen varianzas iguales	8,296	,005	-1,517	97	,132	-5,29755	3,49185	-12,22791	1,63281
	No se asumen varianzas iguales			-1,524	82,064	,131	-5,29755	3,47603	-12,21240	1,61730

Fig. 24 Prueba T
Fuente: Elaboración Propia

Decisión: como $p - valor = 0.13 > 0.05$ no se acepta la hipótesis alternativa, es decir los promedios de tiempo de respuesta de la red antigua y la red nueva, no son significativamente diferentes. Debido a que ambas redes soportan los mismos servicios y aplicaciones por ende el tráfico es semejante.

Tabla 14
Estadísticas de Grupo

Estadísticas de grupo					
	Red	N	Media	Desv. Desviación	Desv. Error promedio
Tiempo	RN	49	78,1224	12,91097	1,84442
	RA	50	83,4200	20,83373	2,94633

Fuente: Elaboración Propia

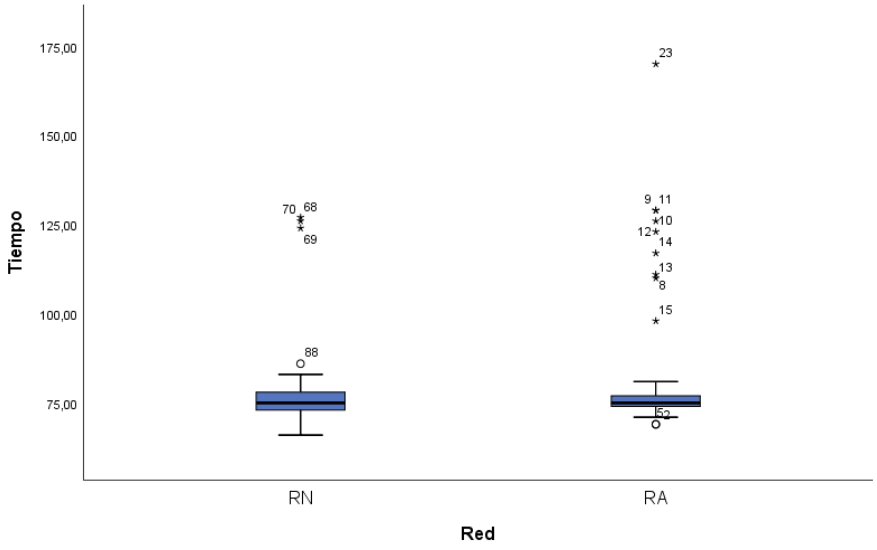


Fig. 25 Diagrama de caja
Fuente: Elaboración Propia

El tiempo de respuesta se lo toma como una analogía dentro de la calidad de servicio QoS donde menor tiempo de respuesta su calidad de servicio es mayor. Su comportamiento es similar debido que el servicio se lo determina en el grado de la satisfacción de los usuarios, en este caso las dos redes satisfacen las necesidades de la calidad de servicio.

4.3.3. Prueba de hipótesis 3 – Disponibilidad

- Hipótesis Nula

$$H_0: \mu_{RA} = \mu_{RN}$$

Los promedios de disponibilidad de la red antigua y la red nueva, no son significativamente diferentes.

- Hipótesis alternativa

$$H_1: \mu_{RA} \neq \mu_{RN}$$

Los promedios de disponibilidad de la red antigua y la red nueva, son significativamente diferentes.

- Media

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Disponibilidad	Se asumen varianzas iguales	,010	,922	4,557	97	,000	,03739	,00821	,02111	,05368
	No se asumen varianzas iguales			4,554	96,349	,000	,03739	,00821	,02109	,05369

Fig. 26 Prueba T
Fuente: Elaboración Propia

Decisión: como $p - valor = 0.000 < 0.05$ se acepta la hipótesis alternativa, es decir Los promedios de disponibilidad de la red antigua y la red nueva, son significativamente diferentes.

Tabla 15
Estadísticas de Grupo

Estadísticas de grupo					
	Red	N	Media	Desv. Desviación	Desv. Error promedio
Disponibilidad	RN	49	,9296	,04208	,00601
	RA	50	,8922	,03955	,00559

Fuente: Elaboración Propia

Tabla 16
Resumen de procesamiento de casos

Resumen de procesamiento de casos							
	Red	Casos					
		Válido		Perdidos		Total	
		N	Porcentaje	N	Porcentaje	N	Porcentaje
Disponibilidad	RN	49	100,0%	0	0,0%	49	100,0%
	RA	50	100,0%	0	0,0%	50	100,0%

Fuente: Elaboración Propia

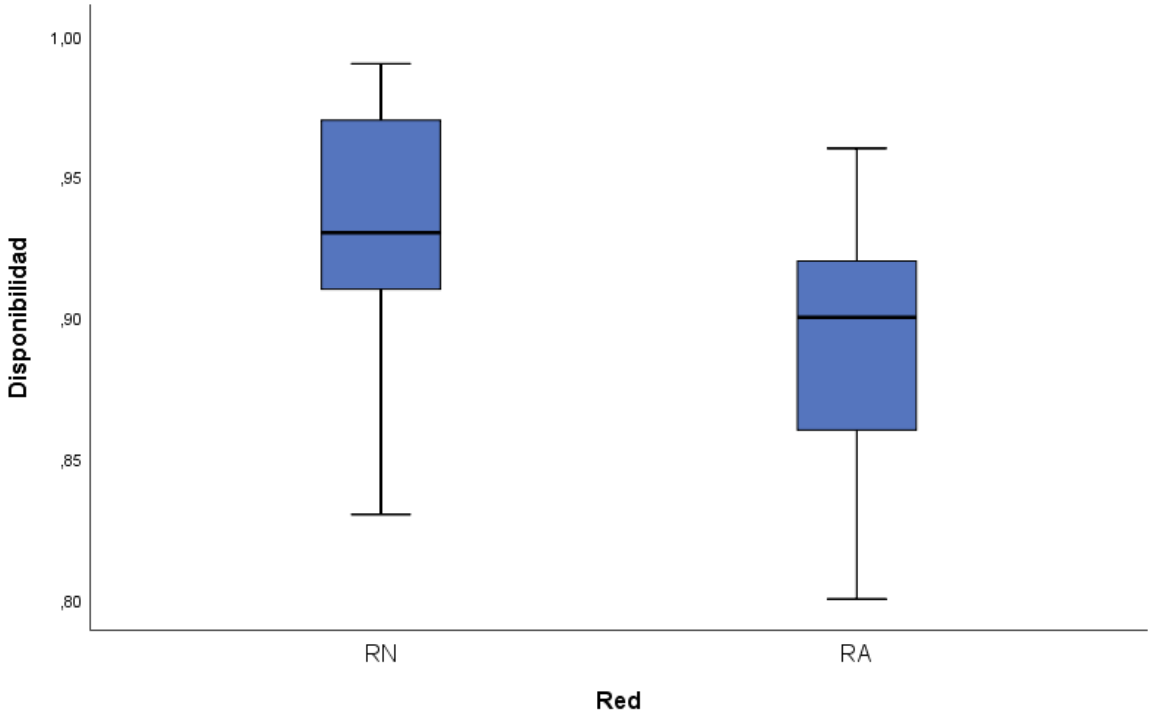


Fig. 27 Prueba T
Fuente: Elaboración Propia

La red nueva RN es factible dentro de la disponibilidad ya que está tomando en cuenta el tiempo de funcionamiento en cualquier periodo. Por lo tanto, la red nueva nos indica que en lo posible está disponible en un 99.9%.

4.3.4. Prueba de hipótesis 4 – Confiabilidad

- Hipótesis Nula

$$H_0: \mu_{RA} = \mu_{RN}$$

Los promedios de confiabilidad de la red antigua y la red nueva, no son significativamente diferentes.

- Hipótesis alternativa

$$H_1: \mu_{RA} \neq \mu_{RN}$$

Los promedios de confiabilidad de la red antigua y la red nueva, son significativamente diferentes.

- Media

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Confiabilidad	Se asumen varianzas iguales	11,678	,001	,979	97	,330	4,24959	4,33864	-4,36140	12,86059
	No se asumen varianzas iguales			,975	82,000	,332	4,24959	4,35679	-4,41744	12,91663

Fig. 28 Prueba T
Fuente: Elaboración Propia

Decisión: como $p - valor = 0.33 > 0.05$ no se acepta la hipótesis alternativa, es decir Los promedios de confiabilidad de la red antigua y la red nueva, no son significativamente diferentes, son iguales.

Tabla 17
Estadísticas de Grupo

Estadísticas de grupo					
	Red	N	Media	Desv. Desviación	Desv. Error promedio
Confiabilidad	RN	49	86,4796	25,67383	3,66769
	RA	50	82,2300	16,62774	2,35152

Fuente: Elaboración Propia

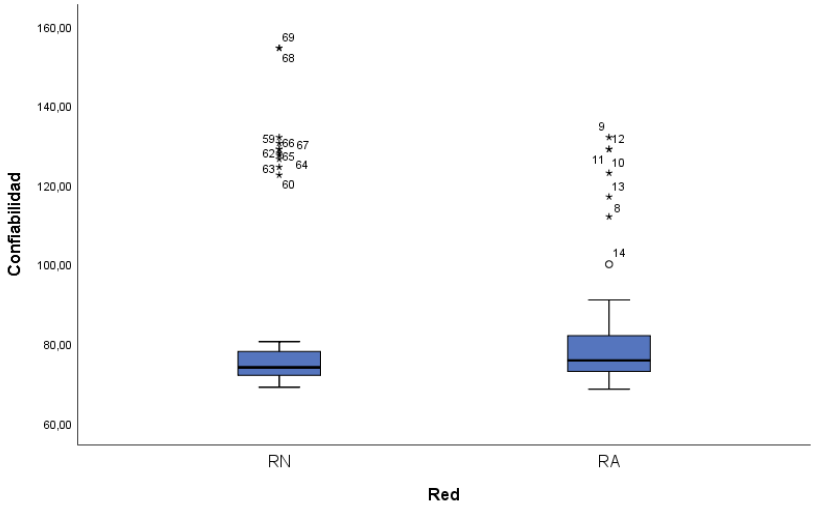


Fig. 29 Diagrama de cajas
Fuente: Elaboración Propia

Su comportamiento es similar debido a que ambas son semejantes porque se tiene una tecnología de red segura, permitiendo la conexión de una red LAN sobre la red pública.

4.4 Seguridad de la red

Proceso para obtener los resultados de la variable cualitativa entorno a la seguridad de la red:

- Tomando como guía y herramienta de evaluación el marco de trabajo de la seguridad de la información basado en la NIST, se desarrolló el proceso para evaluar la red actual y la red actual con las mejoras realizadas, debido a la falta de información, se desarrollaron las dos primeras etapas del marco de trabajo, con lo cual ya se puede tener un punto de partida para continuar con la mejora continua y gestión de la seguridad de la información en la red.

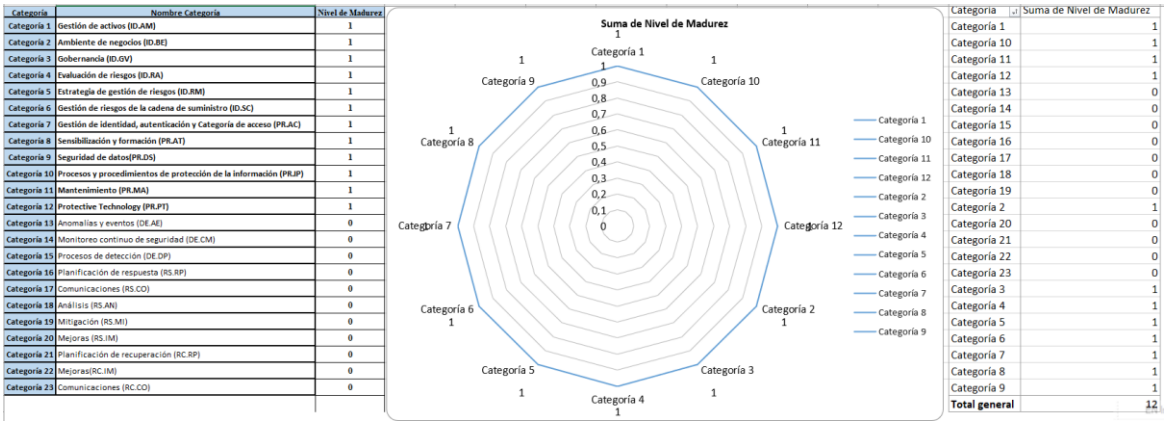
Los parámetros que se evalúa son los siguientes:

Madurez	
0. No existente	Categoría inexistente
1. Inicial	No Confiable- Ambiente impredecible donde las organizaciones no tienen actividades de Categoría y no
2. Repetible	Informal- Las actividades de Categoría existen pero no se ponen en practica. Los Categoríaes dependen
3. Definido	Estandarizado- Las actividades de Categoría existen y están diseñadas, han sido documentadas y
4. Gestionado	Monitoreado- Se utilizan herramientas en una forma limitada para soportar las actividades de Categoría
5. Optimizado	Es una estructura integrada de Categoría interno con un monitoreo en tiempo real por la gerencia, así como
6. No aplicable	Justificación aceptable inherente al negocio o a la estrategia de gestión

Atributo	Descripción	Peso de evaluación
Documentación	Registro actualizado de la información del Categoría que al menos incluye: Responsables,	15%
Operación	Facilidades del Categoría implementadas y en operación (Activo/Herramienta/Proceso)	30%
Normativa	Política documentada y aprobada por la organización que rige al Categoría y responde a las necesidades	20%
Seguimiento	Facilidades de monitoreo del Categoría implementadas y en operación, así como el mecanismo de	15%
Indicadores	Medición periódica de la efectividad del Categoría para cumplir su propósito de seguridad de información	10%
Mejora Continua	Plan en ejecución de mejoras a los Categoríaes, enfocada en una optimización de indicadores o de	10%

Fig. 30 Parámetros del NIST
Fuente: *[28]*

- Red Actual

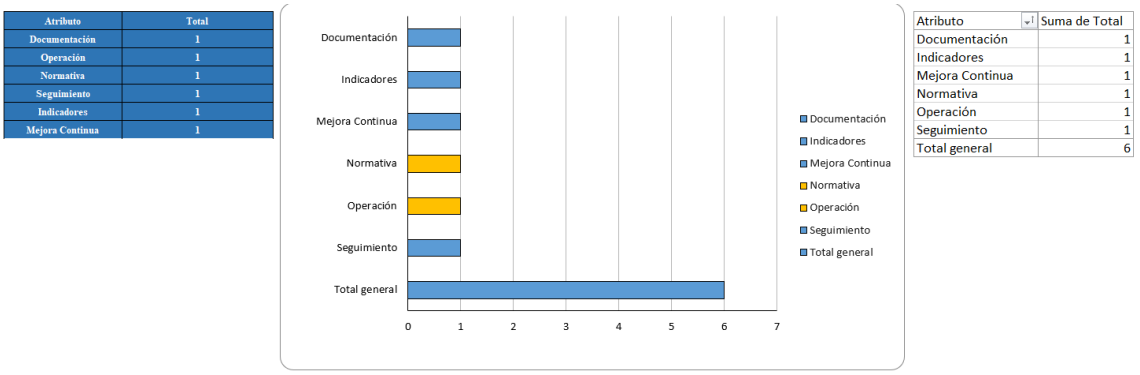


Categoría	Nombre Categoría	Nivel de Madurez
Categoría 1	Gestión de activos (ID.AM)	1
Categoría 2	Ambiente de negocios (ID.BE)	1
Categoría 3	Gobernancia (ID.GV)	1
Categoría 4	Evaluación de riesgos (ID.RA)	1
Categoría 5	Estrategia de gestión de riesgos (ID.RM)	1
Categoría 6	Gestión de riesgos de la cadena de suministro (ID.SC)	1
Categoría 7	Gestión de identidad, autenticación y Categoría de acceso (PR.AC)	1
Categoría 8	Sensibilización y formación (PR.AT)	1
Categoría 9	Seguridad de datos(PR.DS)	1
Categoría 10	Procesos y procedimientos de protección de la información (PR.IP)	1
Categoría 11	Mantenimiento (PR.MA)	1
Categoría 12	Protective Technology (PR.PT)	1
Categoría 13	Anomalías y eventos (DE.AE)	0
Categoría 14	Monitoreo continuo de seguridad (DE.CM)	0
Categoría 15	Procesos de detección (DE.DP)	0
Categoría 16	Planificación de respuesta (RS.RP)	0
Categoría 17	Comunicaciones (RS.CO)	0
Categoría 18	Análisis (RS.AN)	0
Categoría 19	Mitigación (RS.MI)	0
Categoría 20	Mejoras (RS.IM)	0
Categoría 21	Planificación de recuperación (RC.RP)	0
Categoría 22	Mejoras(RC.IM)	0
Categoría 23	Comunicaciones (RC.CO)	0

Categoría	Suma de Nivel de Madurez
Categoría 1	1
Categoría 10	1
Categoría 11	1
Categoría 12	1
Categoría 13	0
Categoría 14	0
Categoría 15	0
Categoría 16	0
Categoría 17	0
Categoría 18	0
Categoría 19	0
Categoría 2	1
Categoría 20	0
Categoría 21	0
Categoría 22	0
Categoría 23	0
Categoría 3	1
Categoría 4	1
Categoría 5	1
Categoría 6	1
Categoría 7	1
Categoría 8	1
Categoría 9	1
Total general	12

Fig. 31 Nivel de Madurez

Fuente: Elaboración Propia

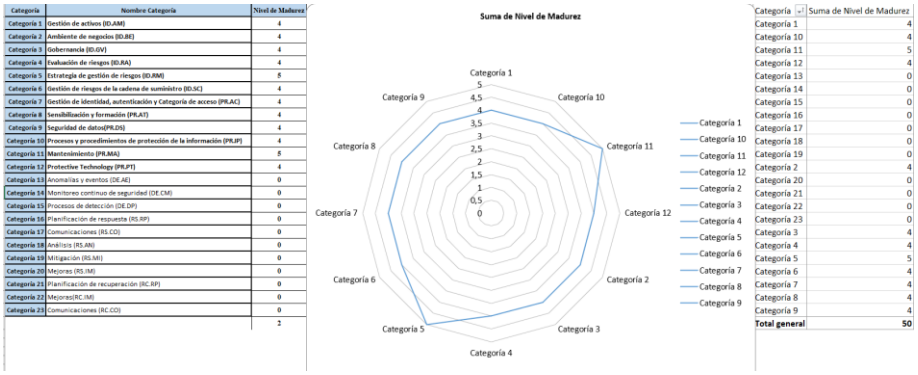


Atributo	Total
Documentación	1
Operación	1
Normativa	1
Seguimiento	1
Indicadores	1
Mejora Continua	1

Atributo	Suma de Total
Documentación	1
Indicadores	1
Mejora Continua	1
Normativa	1
Operación	1
Seguimiento	1
Total general	6

Fig. 32 Diagrama de barras- Nivel de Madurez
Fuente: Elaboración Propia

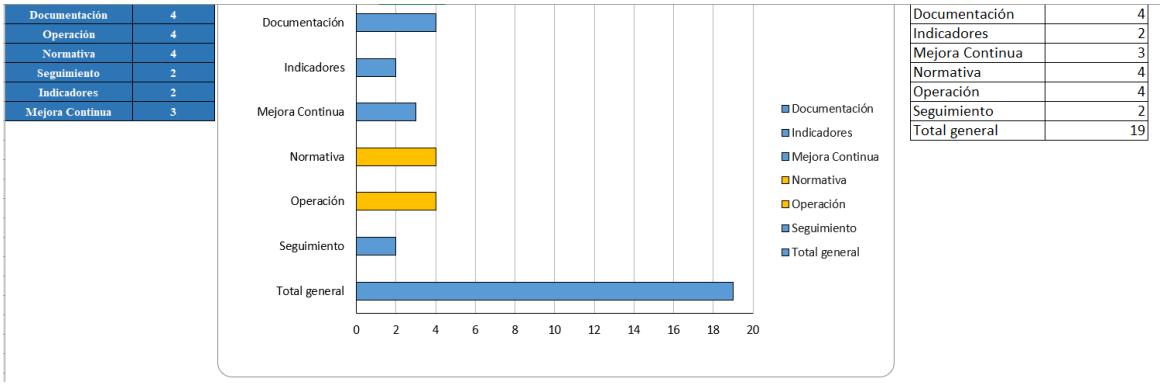
- Red Nueva



Categoría	Nombre Categoría	Nivel de Madurez
Categoría 1	Gestión de activos (ID.AM)	4
Categoría 2	Ambiente de negocios (ID.BE)	4
Categoría 3	Gobernancia (ID.GV)	4
Categoría 4	Evaluación de riesgos (ID.RA)	4
Categoría 5	Estrategia de gestión de riesgos (ID.RM)	5
Categoría 6	Gestión de riesgos de la cadena de suministro (ID.SC)	4
Categoría 7	Gestión de identidad, autenticación y Categoría de acceso (PR.AC)	4
Categoría 8	Sensibilización y formación (PR.AT)	4
Categoría 9	Seguridad de datos(PR.DS)	4
Categoría 10	Procesos y procedimientos de protección de la información (PR.IP)	4
Categoría 11	Mantenimiento (PR.MA)	5
Categoría 12	Protective Technology (PR.PT)	4
Categoría 13	Anomalías y eventos (DE.AE)	0
Categoría 14	Monitoreo continuo de seguridad (DE.CM)	0
Categoría 15	Procesos de detección (DE.DP)	0
Categoría 16	Planificación de respuesta (RS.RP)	0
Categoría 17	Comunicaciones (RS.CO)	0
Categoría 18	Análisis (RS.AN)	0
Categoría 19	Mitigación (RS.MI)	0
Categoría 20	Mejoras (RS.IM)	0
Categoría 21	Planificación de recuperación (RC.RP)	0
Categoría 22	Mejoras(RC.IM)	0
Categoría 23	Comunicaciones (RC.CO)	0
		2

Categoría	Suma de Nivel de Madurez
Categoría 1	4
Categoría 10	4
Categoría 11	5
Categoría 12	4
Categoría 13	0
Categoría 14	0
Categoría 15	0
Categoría 16	0
Categoría 17	0
Categoría 18	0
Categoría 19	0
Categoría 2	4
Categoría 20	0
Categoría 21	0
Categoría 22	0
Categoría 23	0
Categoría 3	4
Categoría 4	4
Categoría 5	5
Categoría 6	4
Categoría 7	4
Categoría 8	4
Categoría 9	4
Total general	50

Fig. 33 Nivel de Madurez
Fuente: Elaboración Propia



Documentación	4
Operación	4
Normativa	4
Seguimiento	2
Indicadores	2
Mejora Continua	3

Documentación	4
Indicadores	2
Mejora Continua	3
Normativa	4
Operación	4
Seguimiento	2
Total general	19

Fig. 34 Diagrama de barras- Nivel de Madurez
Fuente: Elaboración Propia

4.5 Planos actuales de la empresa / levantamiento de información

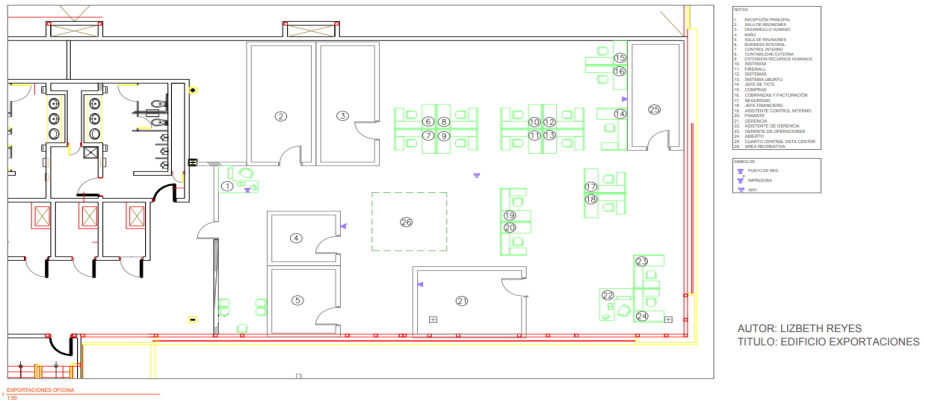


Fig. 35 Plano exportaciones-levantamiento - Autoría
Fuente: Elaboración Propia

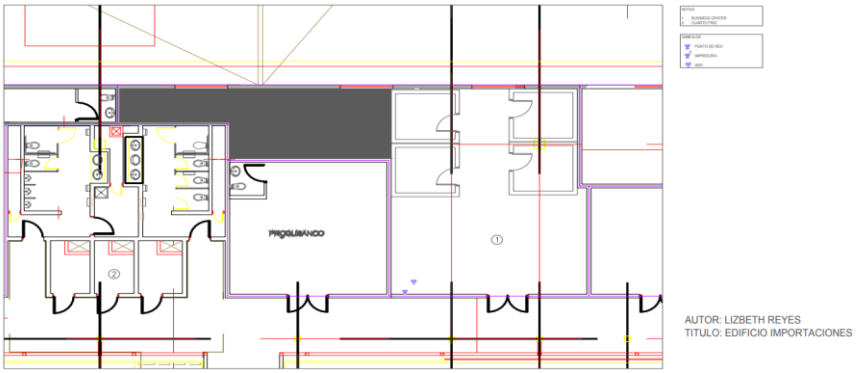


Fig. 36 Plano importaciones-levantamiento
Fuente: Elaboración Propia

CAPITULO V

5. Conclusiones y Recomendaciones

5.1. Conclusiones

- Después de todo el proceso de investigación, se realizó un profundo análisis para el desarrollo de la implementación de la red de datos empresarial de telecomunicaciones, todo esto en base a la documentación de la empresa TABACARCEN, con la ayuda de las herramientas de simulación y los datos obtenidos a partir de esta, se logró llegar a obtener herramientas y métricas que nos permitirán evaluar el desempeño de la red para las tecnologías de voz, video vigilancia y datos.
- Durante el análisis para seleccionar las diferentes tecnologías, protocolos y configuraciones, se optó por seleccionar en base a información confiable de grupos de investigación e instituciones que rigen en base a normativas y estándares mundiales para poder confiar en el desempeño de un equipo en base a diferentes tecnologías, todo esto mediante el estudio de la infraestructura antigua de la empresa y considerando las mejoras para la infraestructura de la nueva red, garantizando los parámetros como confiabilidad, disponibilidad y seguridad de la red.
- Finalmente, para probar y verificar todas las mejoras propuestas para la infraestructura de red de la empresa, se realizaron pruebas de simulación a través de EVE-NG, gracias a ello, se logró obtener resultados que pueden ser medibles y configuraciones que pueden ser replicadas en los equipos intermedios de la infraestructura red actual de la empresa para mejorar la misma y aportar con esto al crecimiento y mejora continua de la empresa.

5.2. RECOMENDACIONES

- Para garantizar un proceso óptimo de la red, es recomendable mantener los equipos intermedios de la red actualizados y parchados como especifica el fabricante, además de contar siempre con información actualizada de la misma, documentando cualquier cambio o modificando dentro de la topología la cual podrá ser utilizada para realizar mejoras para seguir siempre en la mejora continua aportando de esa manera al crecimiento de la empresa.
- Las herramientas para monitorear la red son claves para obtener datos relevantes que nos permitan evaluar y diagnosticar la red, sin una herramienta precisa, podríamos caer en el error de realizar cambios o tomar decisiones sin bases claras para efectuar estos, por esta razón, es recomendable que los datos tomados a través de herramientas de monitoreo sean implementadas de manera correcta para mantener en un estado de alerta a la red, evitando tener pérdidas de comunicación por fallos en los equipos.
- Los procesos de gestión sobre el manejo de la información y los equipos en la empresa, son importantes para poder evaluar la madurez de la red, por dicha razón, es recomendable mantener siempre los procesos y lineamientos apegados a normativas y estándares mundiales que se apeguen al giro del negocio, los cuales a través de estos aseguran un mayor grado de seguridad respecto a la seguridad de la red, evitando entonces tener problemas por brechas de seguridad.

Bibliografía

[1] S. Nesmachnow, H. Cancela, and E. Alba, “Técnicas evolutivas aplicadas al diseño de redes de comunicaciones confiables.”

[2] F. F. Alvarez Paliza Profesor Titular and D. Telecomunicaciones, “GUÍA PARA EL DISEÑO DE REDES EMPRESARIALES. (TRANSICIÓN IPv4-IPv6).”

[3] IMMY ANDRES RODRIGUEZ MUÑOZ, “DISEÑO DE UNA RED LAN PARA LA EMPRESA LA FLORIDA INVERSIONES CADENA HOTELERA ESTUDIANTE JIMMY ANDRES RODRIGUEZ MUÑOZ UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD DE INGENIERÍA PROGRAMA DE TECNOLOGÍA EN SISTEMAS,” 2020.

[4] G. Cecilia and V. Arias, “Organizaciones en red: Factores críticos de diseño,” Contaduría y administración, no. 225, pp. 9–38, 2018, Accessed: Jan. 08, 2022. [Online]. Available: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-10422008000200002&lng=es&nrm=iso&tlng=es

[5] W. Bedoya Garrido and H. L. Rincón Plazas, “Diseño de la red de comunicaciones de las instituciones de educación secundaria y educación superior de la comuna 1 de Neiva,” ADAIR, Rk, effects of weak high-frequency electromagnetic fields on biological systems, in radiofrequency radiation standards, Ed. Klauenberg, B.J., Grandolfo, M., and Erwin, D. N., Plenum Press, New York, 1995, 2020, [Online]. Available: https://repository.ucc.edu.co/handle/20.500.12494/16440

[6] “Tabacarcen S.A.” https://www.tabacarcen.com/ (accessed Jan. 08, 2022).

[7] Dennis Andrés Maigualema Quimbita and D. R. Ing. García, “UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE INGENIERÍA,” 2020.

[8] J. C. Santillán Lima, F. T. Molina Granja, M. F. Vásconez Barrera, W. G. Luna Encalada, and R. M. Lozada Yánez, “Requerimientos y diseño de infraestructura de redes para campus universitarios,” 2018, Accessed: Jan. 08, 2022. [Online]. Available: http://sedici.unlp.edu.ar/handle/10915/72078

[9] Santiago Perkins Parra Haro and Luis Fernando Inca Guaman, “UNIVERSIDAD NACIONAL DE CHIMBORAZO FACULTAD DE INGENIERÍA,” 2016.

[10] Chapper, “3 Diseño de Redes.”

[11] A. Gabriela and M. Bonilla, “"ESTUDIO Y DISEÑO DE UNARED DE PLANTA EXTERNA DE FIBRA ÓPTICA GPON PARA PROVEER SERVICIOS DE VOZ, VIDEO Y DATOS APLICADO A LA CIUDAD DE ALAUSÍ PARA LA CNT EMPRESA PÚBLICA RIOBAMBA,” 2016.

[12] L. M. O. V. R. M. Guilcapi Quisnancela, “Diseño y construcción de un prototipo de red inalámbrica para la gestión y facturación de comandas en tiempo real, aplicado en la implementación de bares-restaurantes inteligentes.,” Jan. 2020, Accessed: Jan. 09, 2022. [Online]. Available: http://dspace.espoch.edu.ec/handle/123456789/13763

[13] Edison Javier Suárez Bravo, “UNIVERSIDAD TECNOLÓGICA ISRAEL APROBACIÓN DEL TUTOR,” 2016.

[14] LIBARDO NIÑO CRUZ CAMILO ANDRÉS VENTO SERRATO, “DISEÑO DE UNA RED LAN PARA LA EMPRESA INTEL CORP LIBARDO NIÑO CRUZ CAMILO ANDRÉS VENTO SERRATO UNIVERSIDAD COOPERATIVA DE COLOMBIA FACULTAD DE INGENIERÍA PROGRAMA DE INGENIERÍA DE SISTEMAS SECCIONAL BOGOTA D.C. NOVIEMBRE 2016,” 2016.

[15] M. Pérez Gómez, “UNESUM-Ciencias: Revista Científica Multidisciplinaria DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA SOFTEL DIRECCIÓN PARA CORRESPONDENCIA: melisa@softel.cu,” Publicación cuatrimestral, vol. 5, no. 4, pp. 129–148.

[16] D. Lopez-Perez, A. Juttner, and J. Zhang, “Optimisation methods for dynamic frequency planning in OFDMA networks,” pp. 1–10, Nov. 2016, doi: 10.1109/NETWKS.2008.6231302.

[17] F. de Ciencias, E. Ingeniería, T. Iván, and B. Zavala, “PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ FACULTAD DE CIENCIAS E INGENIERÍA DISEÑO DE UNA RED LAN INALAMBRICA PARA UNA EMPRESA DE LIMA,” 2019.

[18] C. G. CARRANCO SOTO, “‘DISEÑO E IMPLEMENTACIÓN DE UNA RED DE FIBRA ÓPTICA CON TECNOLOGÍA OTN-DWDM PARA LA PROVISIÓN DE SERVICIOS DE DATOS, TELEVISIÓN POR CABLE Y TELEFONÍA A GRAN DISTANCIA,’” 2018.

[19] G. Echeverría and K. Gonzalo, “ESTUDIO Y DISEÑO DE UN ANILLO DE FIBRA ÓPTICA PARA INTERCONECTAR Y PROTEGER A VARIAS CENTRALES Y REPETIDORA DE LA CNT EP CHIMBORAZO, PARA BRINDAR SERVICIOS DE DATOS DE ALTA VELOCIDAD Y TRIPPLE PLAY,” 2017.

[20] J. P. P. A. L. A. C. Q. , J. C. Arango B., “Procedimiento para implementar QoS en la capa de acceso en redes de próxima generación enfocado en el servicio de voz”.

[21] “¿Qué es COBIT 5? Entendiendo el Gobierno de TI ó IT Governance.” https://geniusitt.com/blog/que-es-cobit-5/ (accessed Jun. 19, 2022).

[22] “Todo lo que usted necesita saber sobre ITIL V4 | Freshservice.” / (accessed Jun. 19, 2022).

[23] "4.4.2.4 Half duplex y full duplex." http://itroque.edu.mx/cisco/cisco1/course/module4/4.4.2.4/4.4.2.4.html (accessed Jun. 19, 2022).

[24] "Tipos y funciones de la tarjeta de interfaz de red (NIC) ⋆ Aprende a Programar Gratis." https://aprendiendoaprogramar.es/blog/tipos-y-funciones-de-la-tarjeta-de-interfaz-de-red-nic/ (accessed Jun. 19, 2022)

[25] "Juniper Networks- MSTP." https://www.juniper.net/documentation/mx/es/software/junos/stp-l2/topics/topic-map/spanning-tree-configuring-mstp.html (accessed Jun. 19, 2022).

[26] What is SABSA Enterprise Security Architecture and why should you care https://medium.com/@marioplatt/what-is-sabsa-enterprise-security-architecture-and-why-should-you-care-a649418b2742(accessed Aug 26,2019)

[27] New&Networks leader https://www.nomios.pl/en/news-blog/2021-gartner-magic-quadrant-enterprise-wired-wireless-lan-infrastructure/(accessed Dec 8, 2021)

[28] Parámetros de NIST https://www.hannainst.es/parametros/5427-certificado-de-calibracion-trazable-a-nist-para-fotometros-serie-hi96-1-parametro.html#/845-parametro-1_parametro(accessed Nov 14, 2021)

Srta. Viviana Lizbeth Reyes Chiriboga

ESTUDIANTE

C.I. 1723968697

Anexos

Anexo 1. Instalación y preparación del laboratorio virtual

- Requisitos

a. Windows 10

b. VWware Workstation 16

c. WinSCP

Anexo 2. Instalación Entorno de Pruebas Virtuales – Emulador EVE-NG

a. Ingresar al sitio web, ir hasta la pestaña de Descargas (DOWNLOAD)

b. Dar clic en el enlace marcado con azul (EVE-NG OVF)

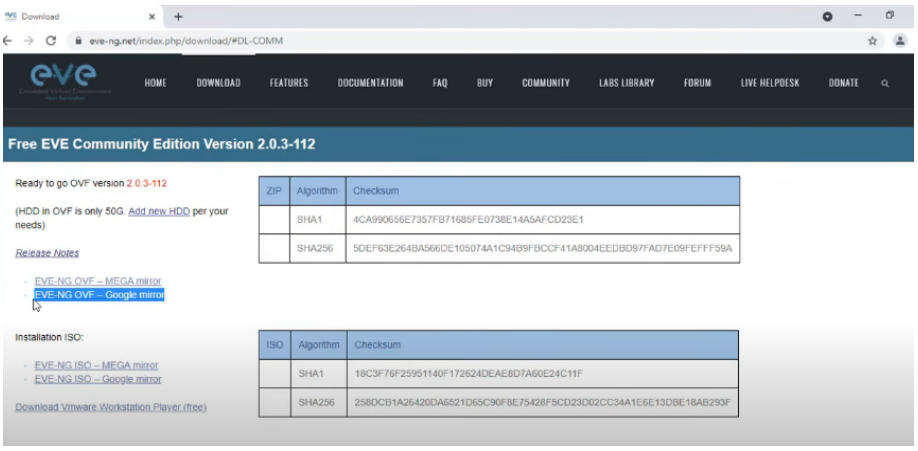


Fig. 37 Página oficial eve-ng

c. Ingresar a VMware Workstation 16, para crear el entorno de pruebas y seleccionamos el archivo descargado.

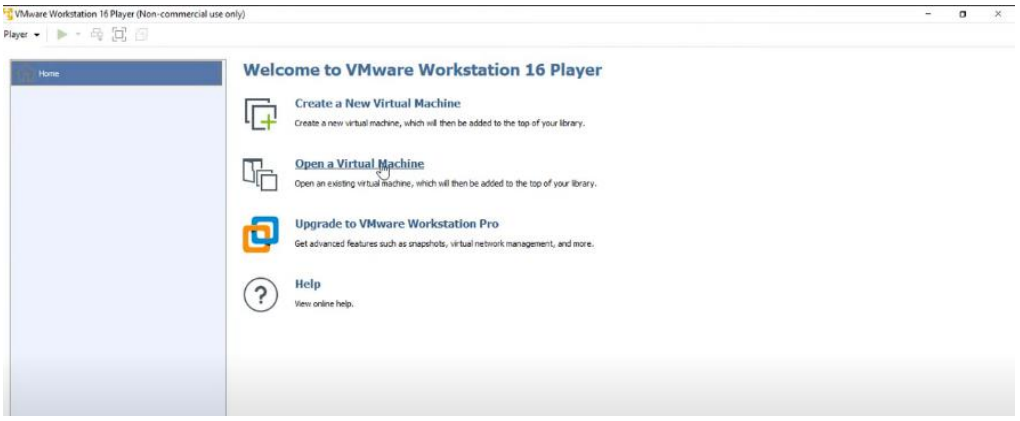


Fig. 38 Software VMware

d. Iniciamos la máquina virtual

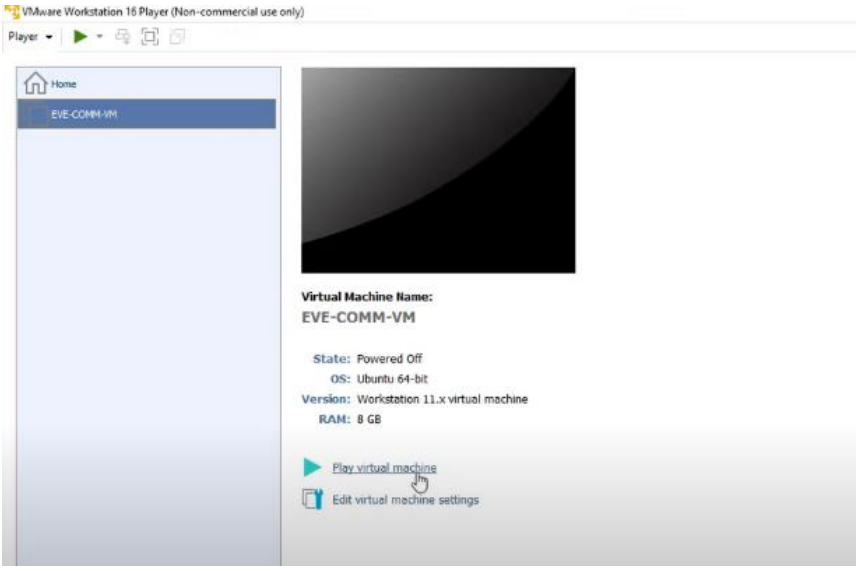


Fig. 39 Play virtual machine

e. Esperamos hasta que se instale, una vez terminado el proceso de instalación, ingresar las credenciales, para login: root y como password:eve

Fig. 40 VMware Workstation

f. Ingresará a configurar de parámetros para la conexión.

Una vez finalizado, ingresar con la dirección IP asignada a través de un navegador web.

Fig. 41 Dirección IP asignada

g. Entramos al laboratorio virtual eve-ng, para login: admin, password: eve

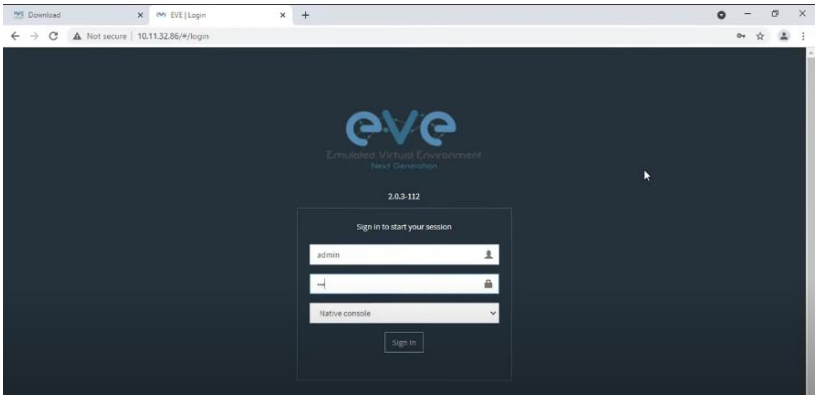


Fig. 42 Laboratorio virtual sign in

Anexo 3. Instalación de Sistemas Operativos para los equipos de red en EVE-NG

1. FORTINET

- Buscamos las versiones que soporta EVE-NG para FORTINET

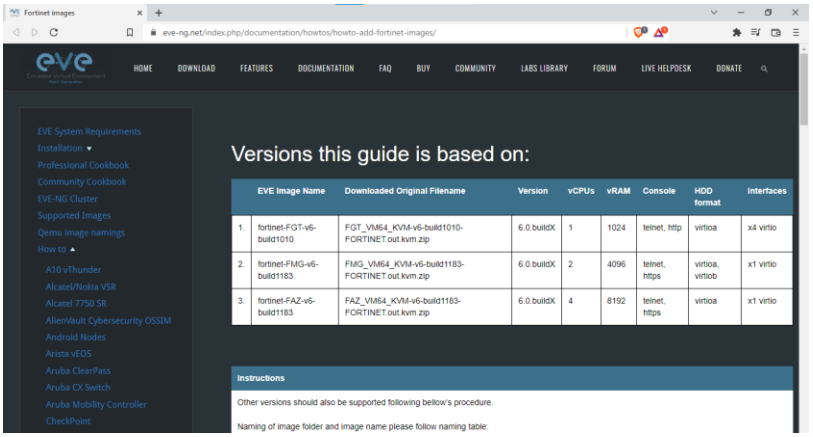


Fig. 7 Versiones que soporta EVE-NG

- Para descargar la imagen, ingresamos a la página oficial FortiCloud y Vamos hasta la pestaña de Support y seleccionamos VM Images.

Fig. 8 Versiones que soporta EVE-NG

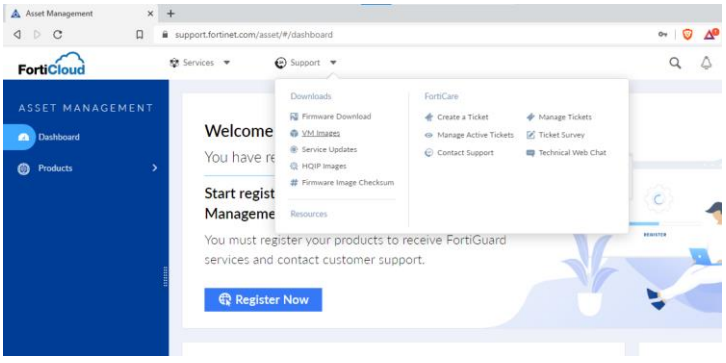


Fig. 44 Seleccionamos VM Images

- Seleccionamos el archivo terminado en .zip y descargamos.

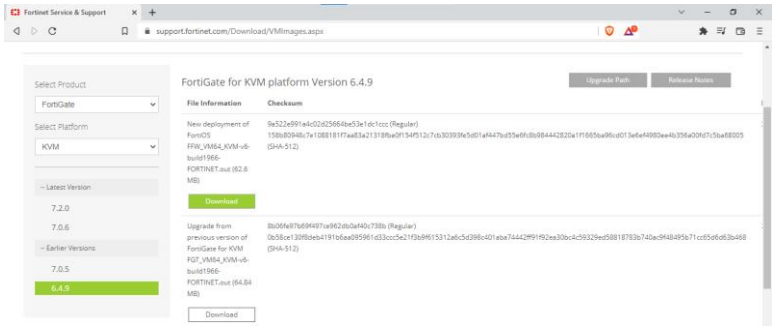


Fig. 45 Descargamos Fortis

- Ingresamos a WinSCP para poder transferir la imagen de Fortiget.

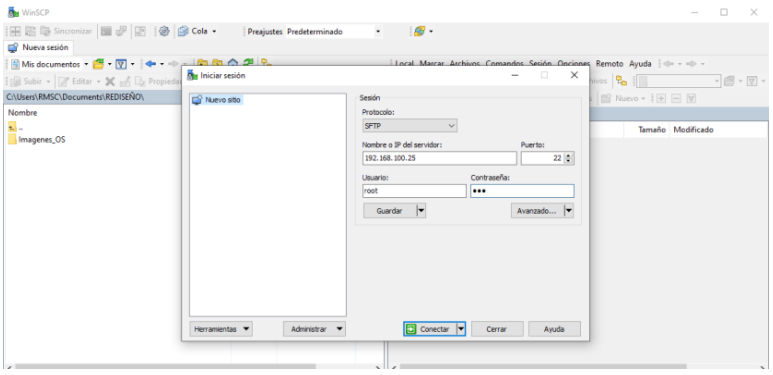


Fig. 46 Inicio de sesión WinSCP

- Creamos una carpeta en el directorio /opt/unetlab/addons/qemu, llamada Fortinet-FGT-v6-build1966.

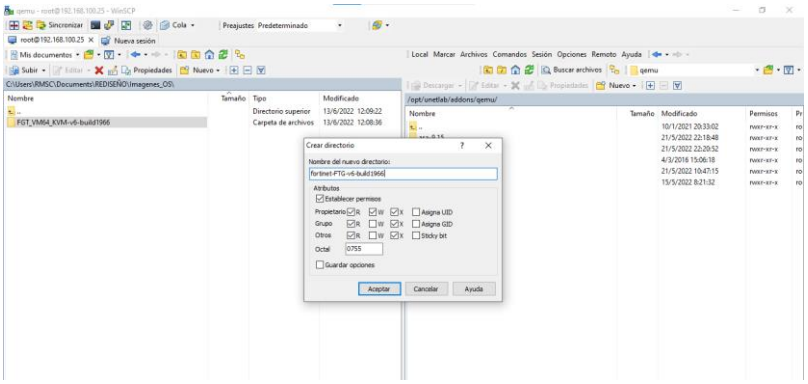


Fig. 47 Creación de directorio

- Finalmente transferimos el archivo.

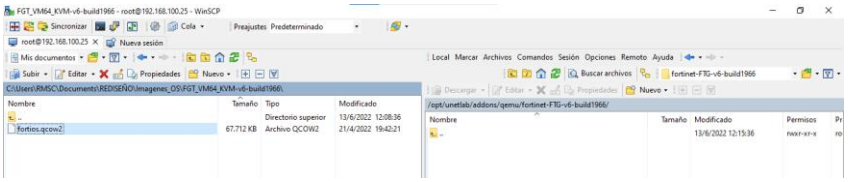


Fig. 48 Transferencia de archivo

- Renombramos el archivo fortios.qcow2 a virtioa.qcow2

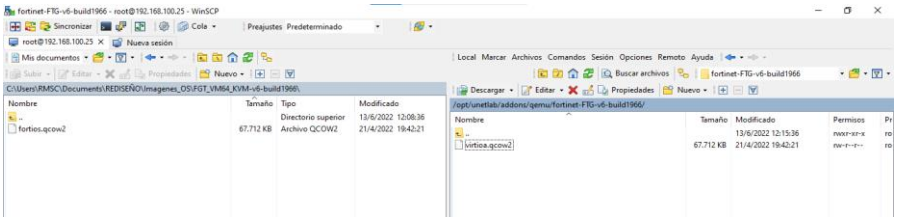


Fig. 10 Renombramos archivo fortios.qcow2

- Finalmente, para activar ingresamos el siguiente comando en el CLI de EVE-NG.

  /opt/unetlab/wrappers/unl_wrapper -a fixpermissions

Fig. 50 CLI de EVE-NG

- Ingresamos a EVE-NG para verificar

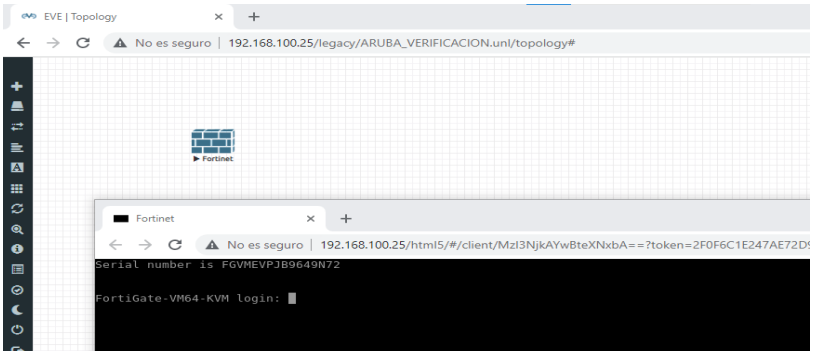


Fig. 51 Imagen habilitada

- **ARUBA**

La instalación para el OS de ARUBA es exactamente los mismos pasos, solamente debemos fijarnos que estamos seleccionando correctamente la imagen y la versión disponible en EVE-NG.

- Buscamos las versiones que soporta EVE-NG para ARUBA.

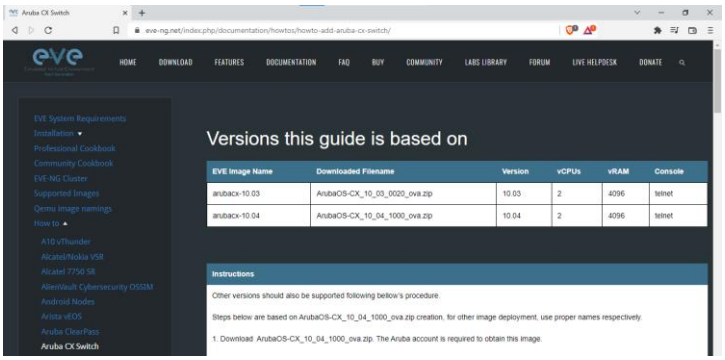


Fig. 52 Versiones de EVE-NG para ARUBA

- Para descargar la imagen, ingresamos a la página oficial.

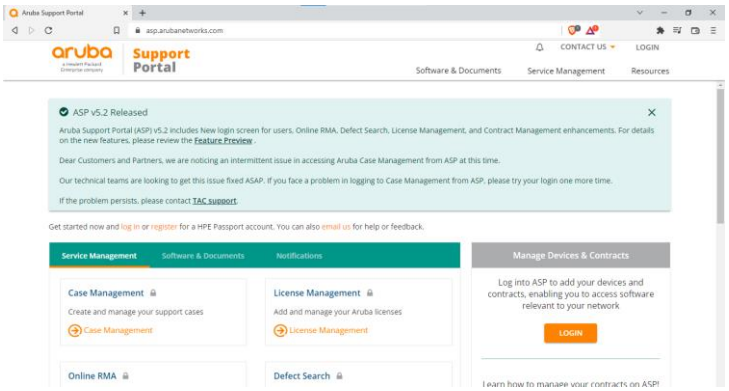


Fig. 53 Página oficial ARUBA

- Ingresamos a WinSCP para poder transferir la imagen de Fortiget

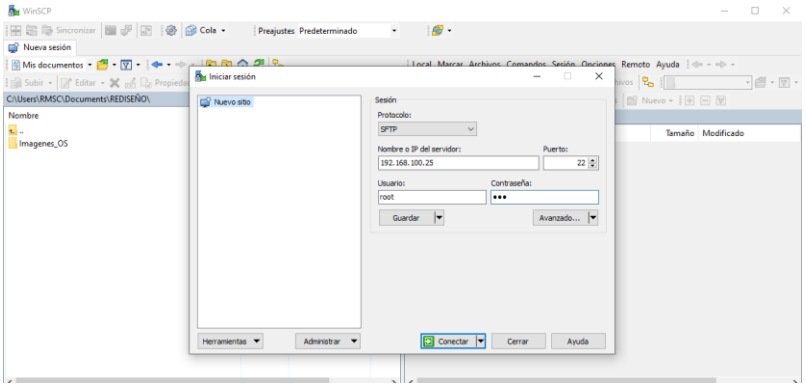


Fig. 54 WinSCP

- Creamos una carpeta llamada abc en el directorio principal, para poder extraer algunos ficheros con el comando. Ingresamos a través del Putty al eve-ng desde la plataforma virtual dirección ip tar xvf ArubaOS-CX_10_04_1000.ova.

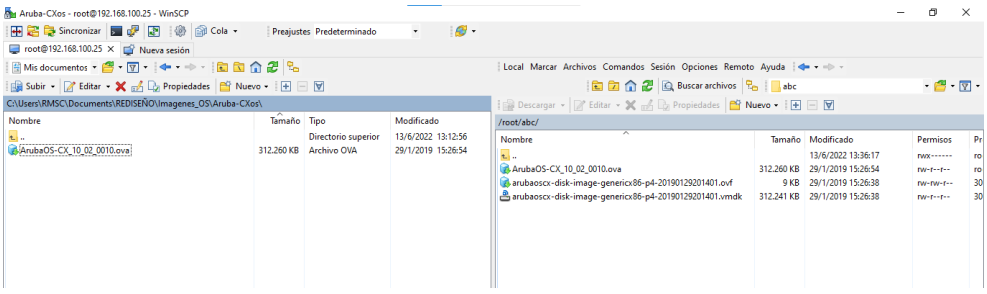


Fig. 55 Directorio principal

- Convertimos el archivo con el comando /opt/qemu/bin/qemu-img convert -f vmdk -O qcow2 arubaoscx-disk-image-genericx86-p4-20200311173823.vmdk virtioa.qcow2.

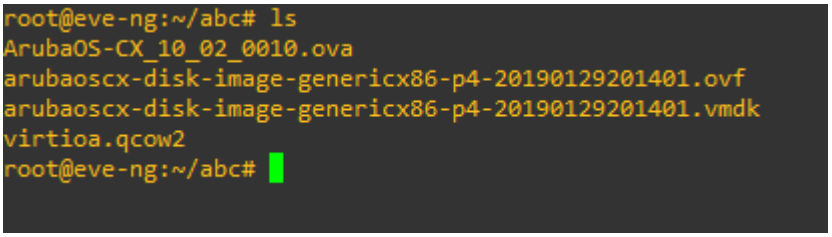


Fig. 56 Archivos de comando

- Creamos una carpeta en el directorio /opt/unetlab/addons/qemu, llamada arubacx-10.04

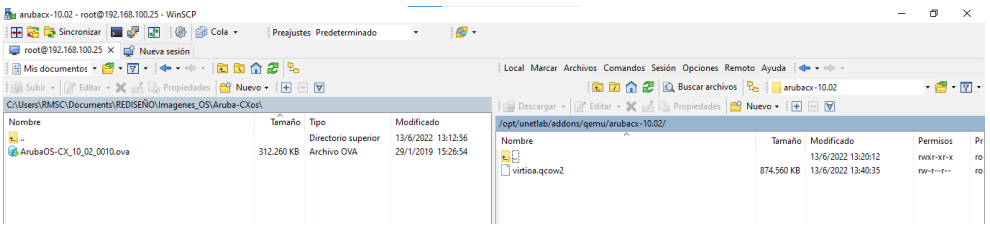


Fig. 57 Creación de carpeta

- Movemos hasta esa carpeta el archivo convertido. mv virtioa.qcow2 /opt/unetlab/addons/qemu/arubacx-10.04/

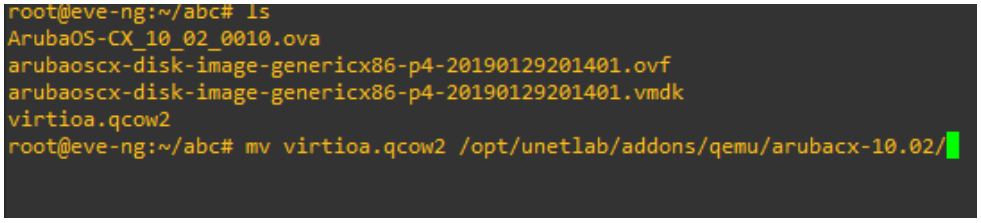


Fig. 58 CLI

- Finalmente, para activar ingresamos el siguiente comando en el CLI de EVE-NG /opt/unetlab/wrappers/unl_wrapper -a fixpermissions , config system interface, edit port1, set allowaccess https https ping ssh.

```
root@eve-ng:~# /opt/unetlab/wrappers/unl_wrapper -a fixpermissions
root@eve-ng:~# S_
```

Fig. 59 CLI EVE-NG

- Finalmente ingresamos a EVE-NG para verificar

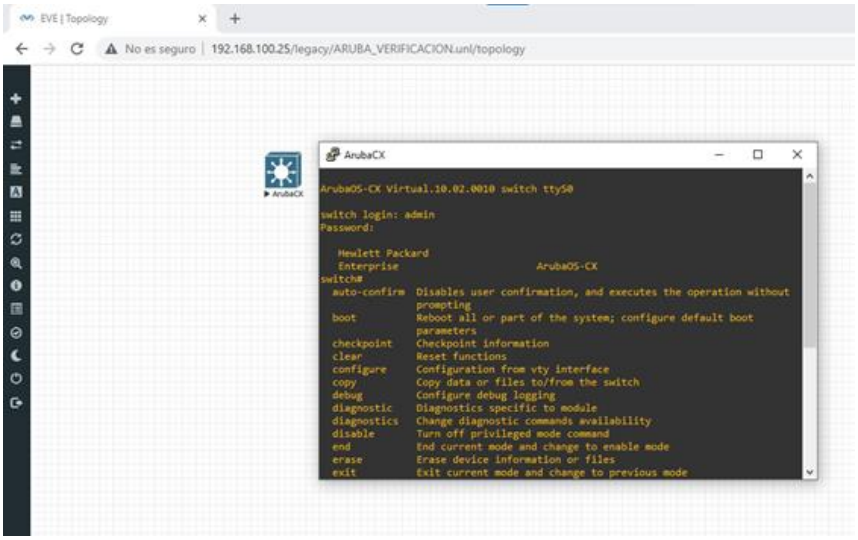
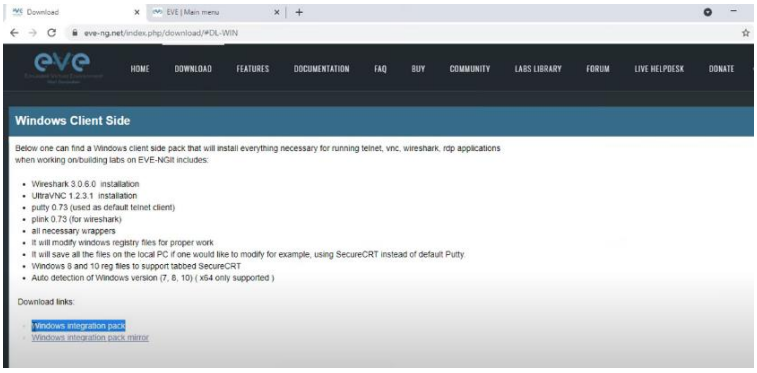


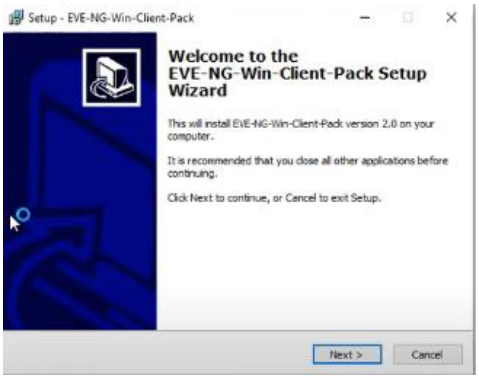
Fig. 60 Imagen Habilitada

Anexo 4. Instalación de las máquinas virtuales dentro de EVE-NG (Windows 7 y LINUX-TinyCore)

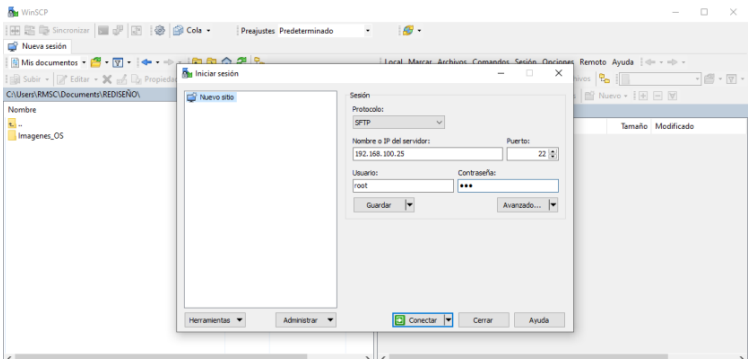
a. Windows 7

- Vamos hasta la página oficial de EVE-NG, para descargar las dependencias y software necesario para ejecutar Windows 7 en EVE-NG

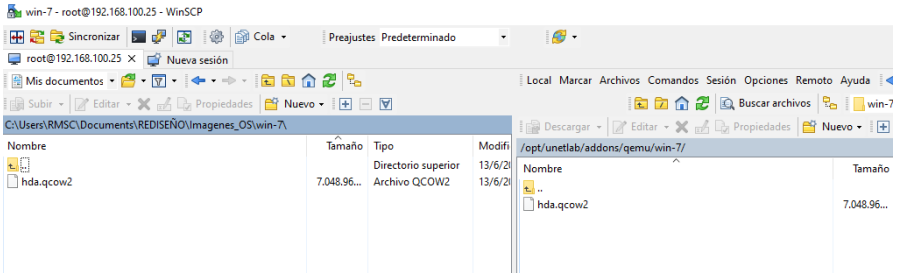




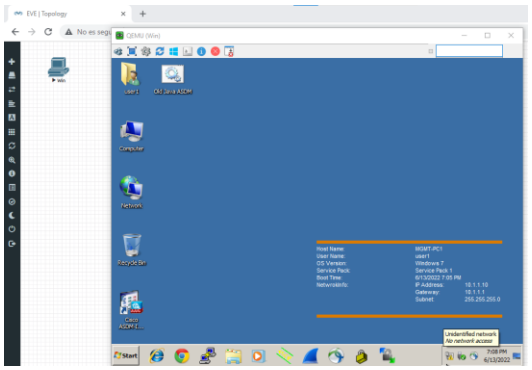
- Ingresamos a WinSCP para poder transferir la imagen de Windows 7



- Vamos hasta el directorio /opt/unetlab/addons/qemu y creamos una carpeta llamada win-7 y finalmente transferimos el archivo

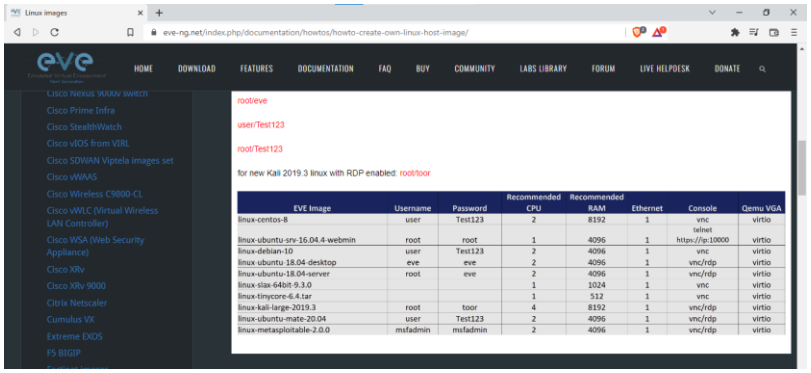


- Ingresamos a EVE-NG para verificar



b. LINUX-TinyCore

- Verificamos las versiones que soporta EVE-NG de LINUX



- A continuación, se muestra los pasos para poder instalar cualquier distribución , https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/

Download link for ready to use Linux Images Here

2. Download your desirable image

3. Using WinSCP or FileZilla SSH (TCP 22) to your EVE and upload downloaded image to the location: /opt/unetlab/addons/qemu/

4. Using Putty or other telnet client, CLI SSH (TCP 22) to your EVE and go to location:

```
cd /opt/unetlab/addons/qemu/
```

5. Unzip your uploaded image file, make sure you are using right name of uploaded image. Example for ubuntu desktop image below.

```
tar xzvf linux-ubuntu-desktop-16.04.4.tar.gz
```

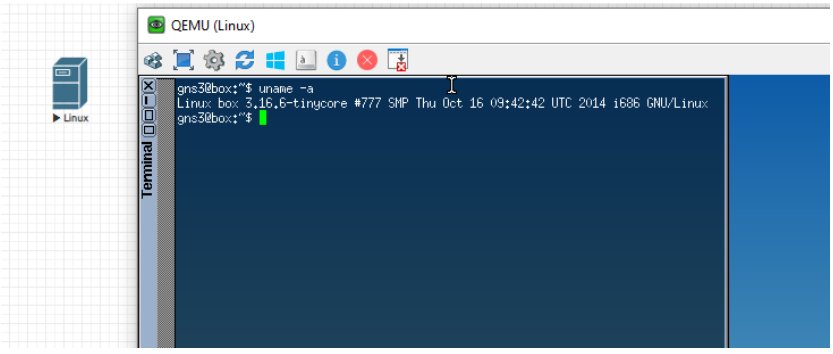
6. Remove raw zipped image file from EVE

```
rm -f linux-ubuntu-desktop-16.04.4.tar.gz
```

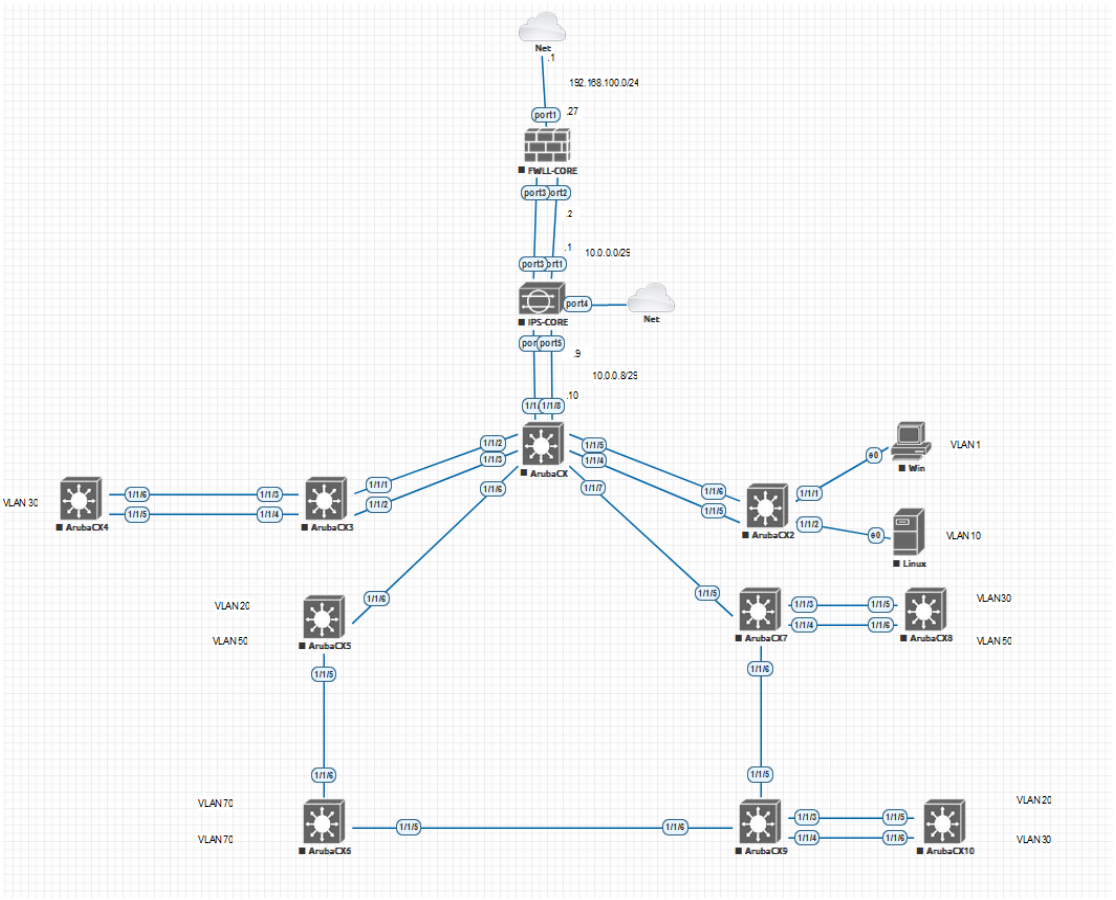
7. Fix permissions

```
/opt/unetlab/wrappers/unl_wrapper -a fixpermissions
```

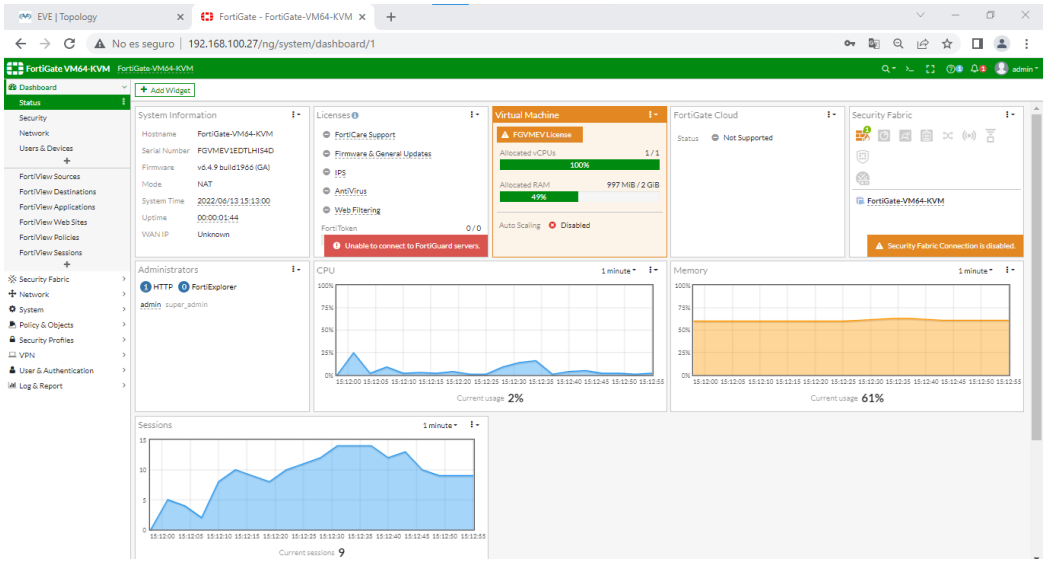
- Ingresamos a EVE-NG para verificar



4.15 simulación y configuración



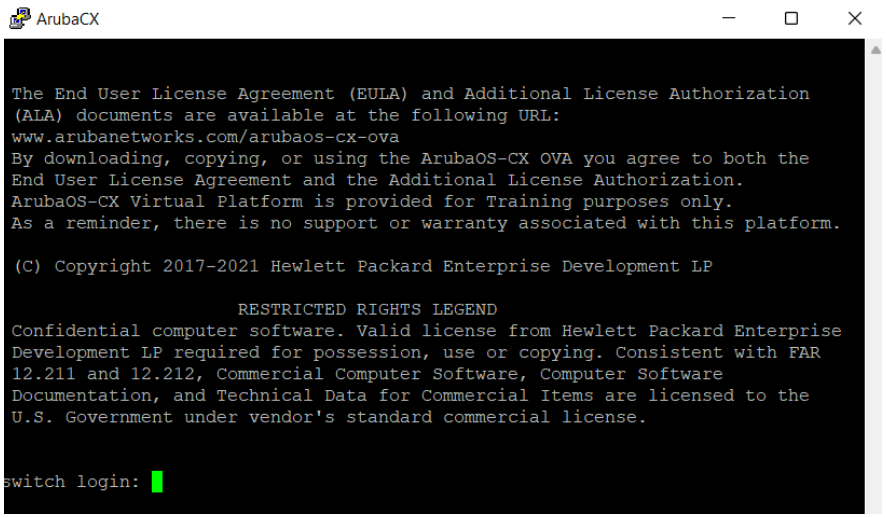
Simulación de red en EVE-NG



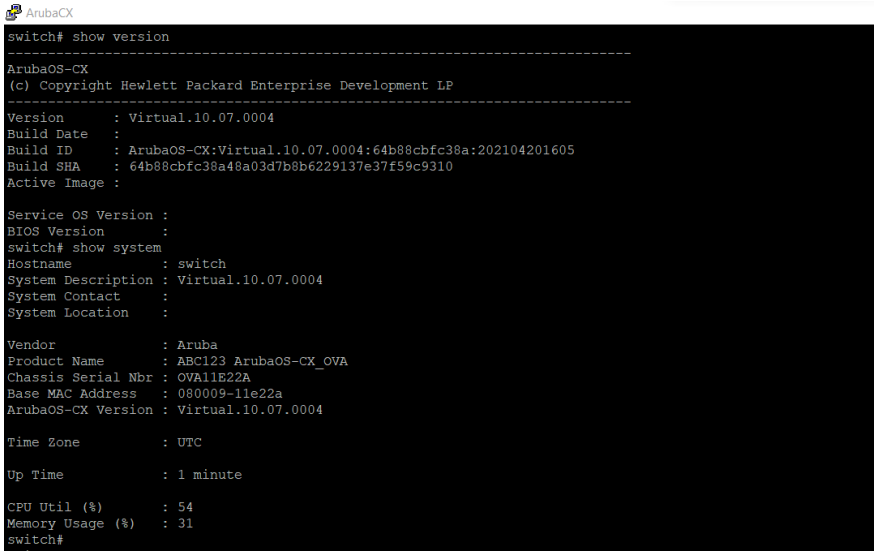
GUI WEB Fortinet - Fortigate

```
Fortinet
FortiGate-VM64-KVM # get system status
Version: FortiGate-VM64-KVM v6.4.9,build1966,220421 (GA)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Serial-Number: FGVMEVL0UU-SISDB
License Status: Valid
Evaluation License Expires: Fri Jul  8 16:05:05 2022
VM Resources: 1 CPU/1 allowed, 997 MB RAM/2048 MB allowed
Log hard disk: Not available
Hostname: FortiGate-VM64-KVM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 1
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1966
Release Version Information: GA
FortiOS x86-64: Yes
System time: Thu Jun 23 16:10:27 2022
```

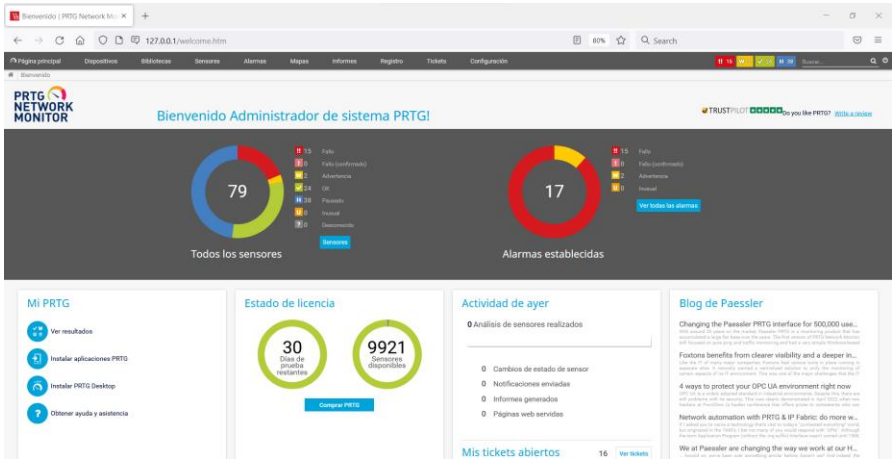
System Fortinet



System Aruba



System Aruba



NPM PRTG

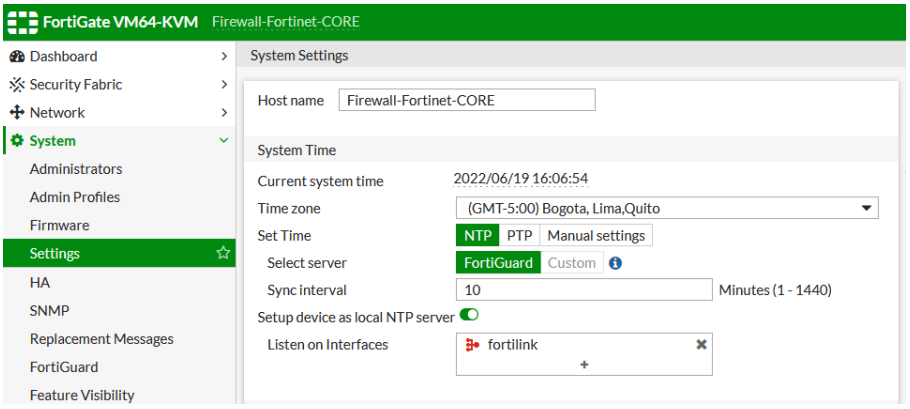
Antes de iniciar con las configuraciones a nivel de capas, es necesario preparar el equipo de red con las configuraciones iniciales respecto al inicio de sesión al equipo y los métodos de acceso, igual manera configurar la fecha para poder analizar en un caso de amenaza a través de los logs.

Anexo 5. Configuraciones Iniciales Fortinet Firewall - IPS

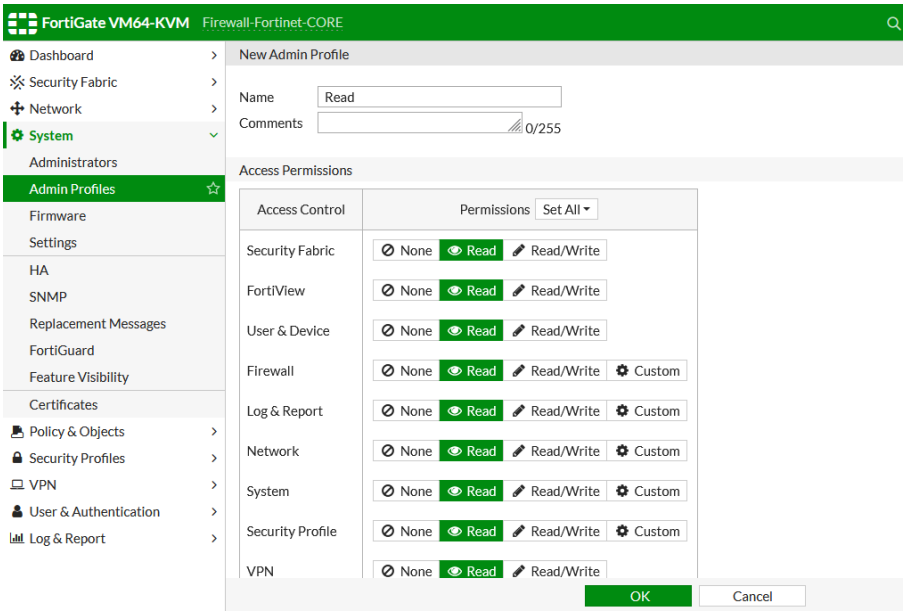
```
config system fips-cc
set entropy-token enable
end

config system global
set admin-concurrent disable
set admin-console-timeout 300
set admin-lockout-duration 300
set admin-lockout-threshold 3
set admin-login-max 1
set admintimeout 10
set allow-traffic-redirect disable
set anti-replay strict
set arp-max-entry 131072
set auth-keepalive disable
set av-failopen off
set av-failopen-session enable
set check-protocol-header strict
set check-reset-range strict
set fds-statistics enable
set fgd-alert-subscription advisory latest-threat
set fortiextender disable
set lldp-transmission disable
set login-timestamp enable
set post-login-banner enable
set pre-login-banner enable
set reset-sessionless-tcp disable
set special-file-23-support enable
end
```

```
config system interface
edit "<interfaz>"
set dhcp-relay-service disable
set fail-detect disable
set pptp-client disable
set arpforward disable
set broadcast-forward disable
set l2forward disable
set icmp-redirect disable
set vlanforward disable
set stpforward disable
set ident-accept enable
set ipmac disable
set netbios-forward disable
set security-mode <captive>
set device-identification disable
set lldp-transmision disable
next
```

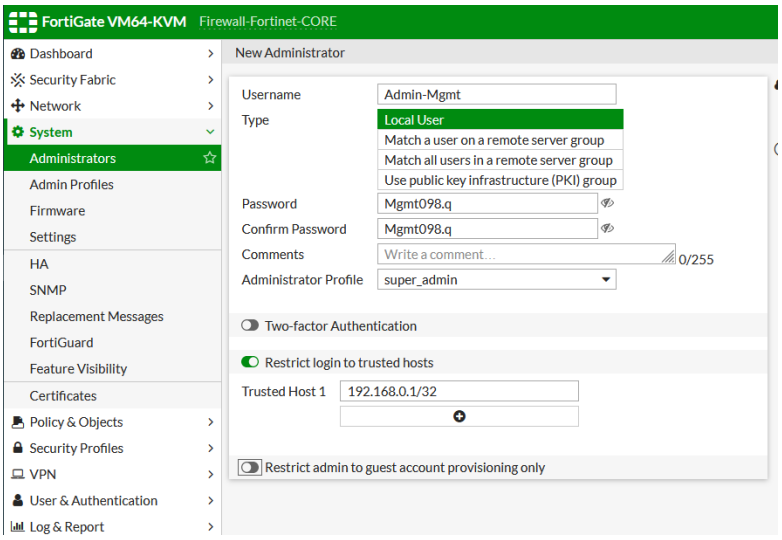
Configuraciones Iniciales para ingreso, seguridad y alteras



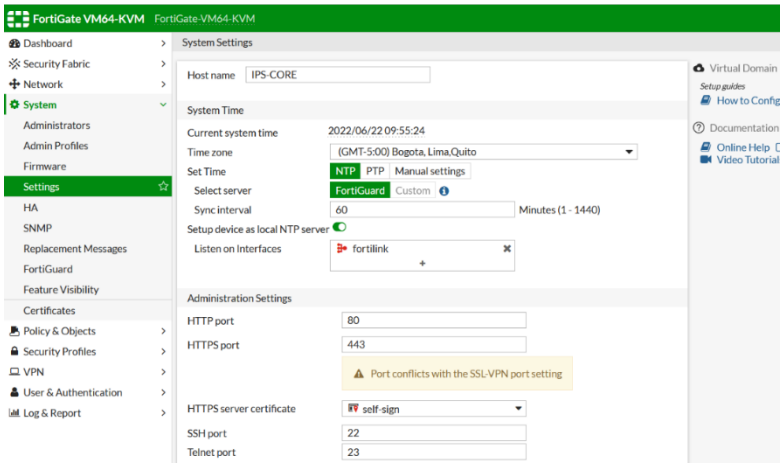
Configuración de Nombre, fecha y además lo configuramos como un servidor NTP para todos los dispositivos de la red



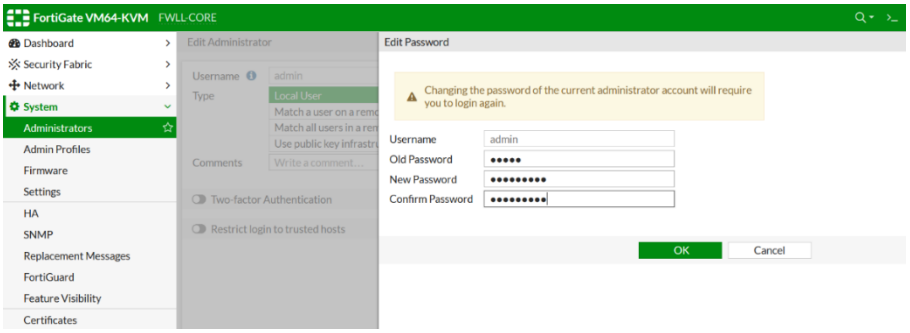
Configuración de un perfil de usuario para solo lectura



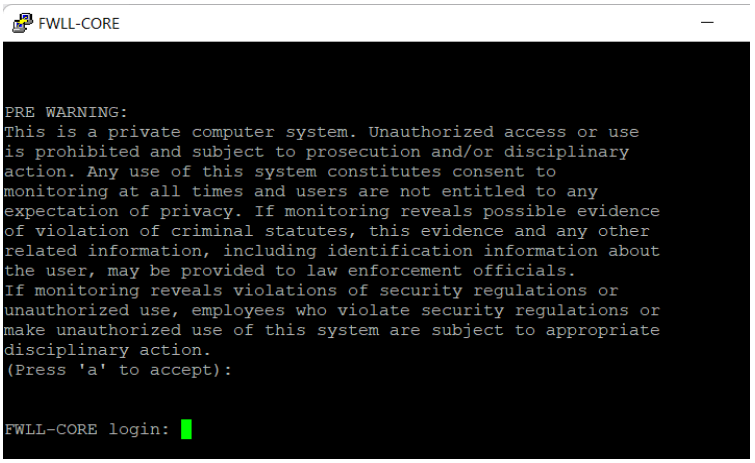
Creamos el usuario para administración del equipo



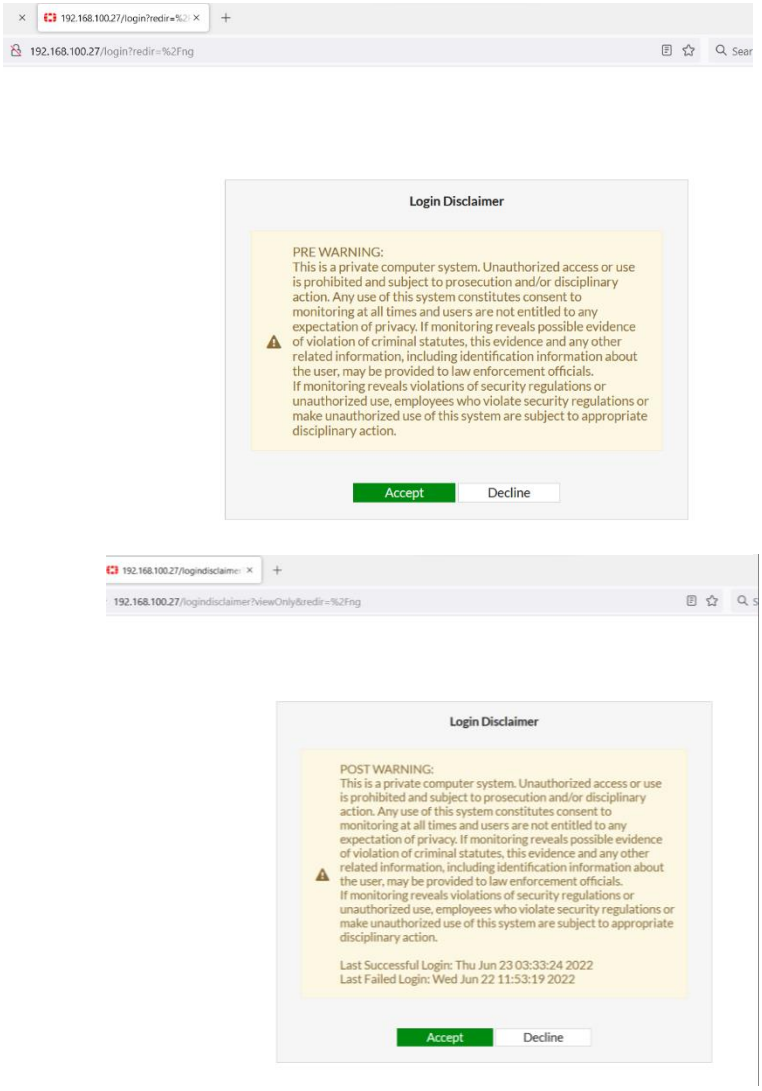
Configuración Inicial Fortinet



Cambio de Clave para admin



Verificación



Verificación

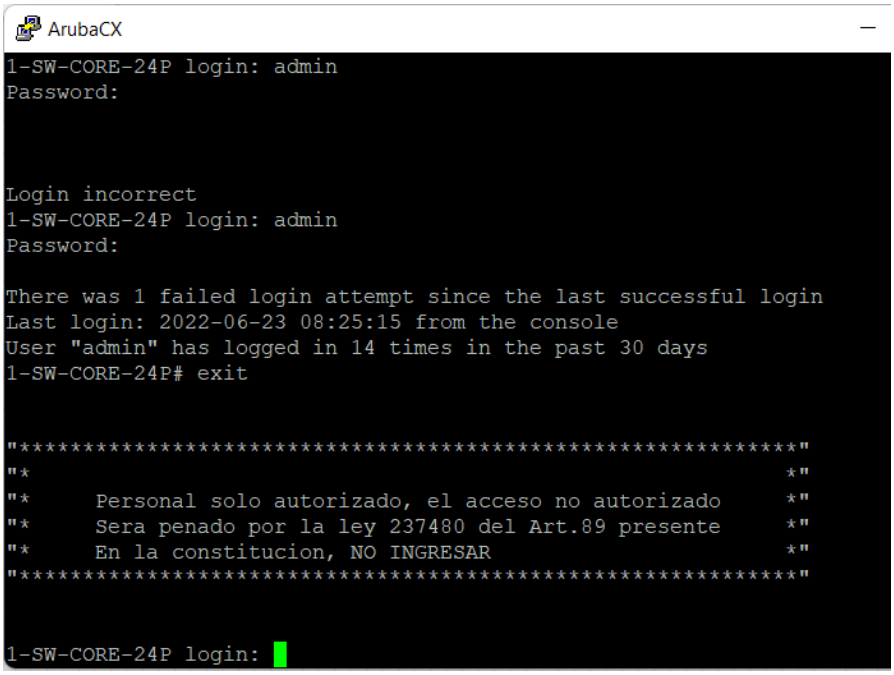
Anexo 6. Configuraciones Iniciales Aruba

```
configure terminal
system serviceos password-prompt
hostname "NOMBRE EQUIPO"
domain-name empresa.int
banner motd ^

"*****************************************************************"
"*                                                               *"
"*     Personal solo autorizado, el acceso no autorizado         *"
"*     Sera penado por la ley 237480 del Art.89 presente         *"
"*     En la constitucion, NO INGRESAR                           *"
"*****************************************************************"

^
password complexity
minimum-length 10
history-count 3
enable
exit
user admin password
Mgmt1SwCore.
ssh host-key rsa bits 2048
ssh maximum-auth-attempts 3
permit cli command ".*"
exit
ssh server vrf default
exit
configure terminal
cli-session
max-per-user 1
timeout 5
session-timeout 60
exit
```

Configuraciones Iniciales para ingreso, seguridad y alteras

```
interface vlan 1
description MGMT-SW-DATACENTER-24P
ip address 192.168.0.2/24
no shutdown
exit

ntp server 10.0.0.2
ntp enable
logging 10.0.0.2
exit

```

Configuraciones Iniciales para ingreso, seguridad y alteras



Verificación

Anexo 7. Configuraciones Capa 2 Aruba - Core

```
config
vlan 1
exit
vlan 10
name SERVIDORES
exit
vlan 20
name CAMARAS
exit
vlan 30
name USUARIOS
exit
vlan 50
name NZD
exit
vlan 60
name WAN
exit
vlan 70
name GERENCIA
exit
```

Creación de VLANs

```
int lag 1
no routing
vlan trunk allowed all
lacp mode active
no shutdown
exit

int lag 2
no routing
vlan trunk allowed all
lacp mode active
no shutdown
exit

int lag 3
no routing
vlan trunk allowed 1
vlan acces 60
lacp mode active
no shutdown
exit

interface 1/1/4-1/1/5
lag 1
no shutdown
exit

interface 1/1/2-1/1/3
lag 2
no shutdown
exit

interface 1/1/1
lag 3
no shutdown
exit
```

LACP

```
1-SW-CORE-24P# show vlan

-------------------------------------------------------------------------------------------------------------
VLAN  Name                             Status  Reason                Type      Interfaces
-------------------------------------------------------------------------------------------------------------
1     DEFAULT_VLAN_1                   up      ok                    default   1/1/6-1/1/7,1/1/9,lag1-lag2
10    SERVIDORES                       up      ok                    static    1/1/6-1/1/7,lag1-lag2
20    CAMARAS                          up      ok                    static    1/1/6-1/1/7,lag1-lag2
30    USUARIOS                         up      ok                    static    1/1/6-1/1/7,lag1-lag2
50    NZD                              up      ok                    static    1/1/6-1/1/7,lag1-lag2
60    WAN                              up      ok                    static    1/1/6-1/1/7,lag1-lag3
70    GERENCIA                         up      ok                    static    1/1/6-1/1/7,lag1-lag2
```

Verificacion VLANs

ArubaCX

```
1-SW-CORE-24P# show interface lag brief
-------------------------------------------------------------------------------------------------------------------
Port      Native  Mode   Type          Enabled Status  Reason                Speed   Description
          VLAN                                                               (Mb/s)
-------------------------------------------------------------------------------------------------------------------
lag1      1       trunk  --            yes     up      --                    2000    --
lag2      1       trunk  --            yes     up      --                    2000    --
lag3      60      access --            yes     up      --                    2000    --
```

Verificación LACP - CORE

```
1-SW-CORE-24P# show interface lag1

Aggregate lag1 is up
 Admin state is up
 Description :
 MAC Address                : 08:00:09:0f:b2:b0
 Aggregated-interfaces      : 1/1/4 1/1/5
 Aggregation-key            : 1
 Aggregate mode             : active
 Speed                      : 2000 Mb/s
 L3 Counters: Rx Disabled, Tx Disabled
 qos trust none
 VLAN Mode: native-untagged
 Native VLAN: 1
 Allowed VLAN List: all

 Statistic                        RX                  TX                Total
 ---------------- -------------------- -------------------- --------------------
 Packets                          1410                 2353                    0
   Unicast                           0                    0                    0
   Multicast                         0                    0                    0
   Broadcast                         0                    0                    0
 Bytes                           274789               621556                    0
 Jumbos                            0                    0                    0
 Dropped                           0                    0                    0
 Pause Frames                      0                    0                    0
 Errors                            0                    0                    0
   CRC/FCS                         0                  n/a                    0
   Collision                     n/a                    0                    0
   Runts                           0                  n/a                    0
   Giants                          0                  n/a                    0
```

Verificación LACP 1 - CORE

```
1-SW-CORE-24P# show interface lag2

Aggregate lag2 is up
 Admin state is up
 Description :
 MAC Address                : 08:00:09:0f:b2:b0
 Aggregated-interfaces      : 1/1/2 1/1/3
 Aggregation-key            : 2
 Aggregate mode             : active
 Speed                      : 2000 Mb/s
 L3 Counters: Rx Disabled, Tx Disabled
 qos trust none
 VLAN Mode: native-untagged
 Native VLAN: 1
 Allowed VLAN List: all

 Statistic                          RX                  TX                Total
 ---------------- -------------------- -------------------- --------------------
 Packets                           620                 2359                    0
   Unicast                           0                    0                    0
   Multicast                         0                    0                    0
   Broadcast                         0                    0                    0
 Bytes                          104937               622321                    0
 Jumbos                            0                    0                    0
 Dropped                           0                    0                    0
 Pause Frames                      0                    0                    0
 Errors                            0                    0                    0
   CRC/FCS                         0                  n/a                    0
   Collision                     n/a                    0                    0
   Runts                           0                  n/a                    0
   Giants                          0                  n/a                    0
```

Verificación LACP 2 - CORE

```
1-SW-CORE-24P# show interface lag3

Aggregate lag3 is up
 Admin state is up
 Description :
 MAC Address                : 08:00:09:0f:b2:b0
 Aggregated-interfaces      : 1/1/1 1/1/8
 Aggregation-key            : 3
 Aggregate mode             : active
 Speed                      : 2000 Mb/s
 L3 Counters: Rx Disabled, Tx Disabled
 qos trust none
 VLAN Mode: access
 Access VLAN: 60

 Statistic                          RX                  TX                Total
 ---------------- -------------------- -------------------- --------------------
 Packets                           889                 2612                    0
   Unicast                           0                    0                    0
   Multicast                         0                    0                    0
   Broadcast                         0                    0                    0
 Bytes                          490500               489126                    0
 Jumbos                            0                    0                    0
 Dropped                           0                    0                    0
 Pause Frames                      0                    0                    0
 Errors                            0                    0                    0
   CRC/FCS                         0                  n/a                    0
   Collision                     n/a                    0                    0
   Runts                           0                  n/a                    0
   Giants                          0                  n/a                    0
```

Verificación LACP 3 - CORE

Anexo 8. Configuraciones Capa 2 Aruba – Distribución

```
config
vlan 1
exit
vlan 10
name SERVIDORES
exit
vlan 20
name CAMARAS
exit
vlan 30
name USUARIOS
exit
vlan 50
name NZD
exit
vlan 60
name WAN
exit
vlan 70
name GERENCIA
exit
```

```
int lag 1
no routing
vlan trunk allowed all
lacp mode active
no shutdown
exit

int lag 2
no routing
vlan trunk allowed all
lacp mode passive
no shutdown
exit

interface 1/1/1-1/1/2
lag 2
no shutdown
exit

interface 1/1/3-1/1/4
lag 1
no shutdown
exit
```

```
interface vlan 1
description MGMT-SW-BLOQUE-E-24P
ip address 192.168.0.3/24
no shutdown
exit
```

ArubaCX3

```
3-SW-BLOQUE-E-24P# show interface lag brief
--------------------------------------------------------------------------------------------------------------------
Port      Native  Mode   Type          Enabled Status  Reason              Speed   Description
          VLAN                                                             (Mb/s)
--------------------------------------------------------------------------------------------------------------------
lag1      1       trunk  --            yes     up      --                  2000    --
lag2      1       trunk  --            yes     up      --                  2000    --
```

Verificación LACP

ArubaCX3

```
3-SW-BLOQUE-E-24P# show interface vlan 1

Interface vlan1 is up
 Admin state is up
 Description: MGMT-SW-BLOQUE-E-24P
 Hardware: Ethernet, MAC Address: 08:00:09:e2:2a:c2
 IPv4 address 192.168.0.3/24

 Statistic                        RX                  TX                Total
 ---------------- -------------------- -------------------- --------------------
 L3 Packets                          0                    0                    0
 L3 Bytes                            0                    0                    0
```

VLAN 1 MGMT

Anexo 9. Configuraciones Capa 2 Aruba – Acceso

```
config
vlan 1
exit
vlan 10
name SERVIDORES
exit
vlan 20
name CAMARAS
exit
vlan 30
name USUARIOS
exit
vlan 50
name NZD
exit
vlan 60
name WAN
exit
vlan 70
name GERENCIA
exit
```

```
int lag 1
no routing
vlan trunk allowed all
lacp mode passive
no shutdown
exit

interface 1/1/5-1/1/6
lag 1
no shutdown
exit

interface 1/1/2-1/1/3
no routing
vlan acces 10
no shutdown
exit

interface 1/1/1
no routing
vlan acces 1
no shutdown
exit
```

```
interface vlan 1
description MGMT-SW-BLOQUE-E-24P
ip address 192.168.0.3/24
no shutdown
exit
```

ArubaCX2

```
2-SW-DATACENTER-24P# show vlan

--------------------------------------------------------------------------------------------------------------------
VLAN  Name                            Status  Reason              Type      Interfaces
--------------------------------------------------------------------------------------------------------------------
1     DEFAULT_VLAN_1                  up      ok                  default   1/1/1,lag1
10    SERVIDORES                      up      ok                  static    1/1/2-1/1/3,lag1
20    CAMARAS                         up      ok                  static    lag1
30    USUARIOS                        up      ok                  static    lag1
50    NZD                             up      ok                  static    lag1
60    WAN                             up      ok                  static    lag1
70    GERENCIA                        up      ok                  static    lag1
```

Verificación

ArubaCX4

```
4-SW-CRUCEROS-24P# show interface brief
--------------------------------------------------------------------------------------------------------
Port      Native  Mode   Type          Enabled Status  Reason                Speed   Description
          VLAN                                                               (Mb/s)
--------------------------------------------------------------------------------------------------------
1/1/1     30      access --            yes     up                            1000    --
1/1/2     30      access --            yes     up                            1000    --
1/1/3     --      routed --            no      down    Administratively down --      --
1/1/4     --      routed --            no      down    Administratively down --      --
1/1/5     1       trunk  --            yes     up                            1000    --
1/1/6     1       trunk  --            yes     up                            1000    --
1/1/7     --      routed --            no      down    Administratively down --      --
1/1/8     --      routed --            no      down    Administratively down --      --
1/1/9     --      routed --            no      down    Administratively down --      --
1/1/10    --      routed --            no      down    Administratively down --      --
```

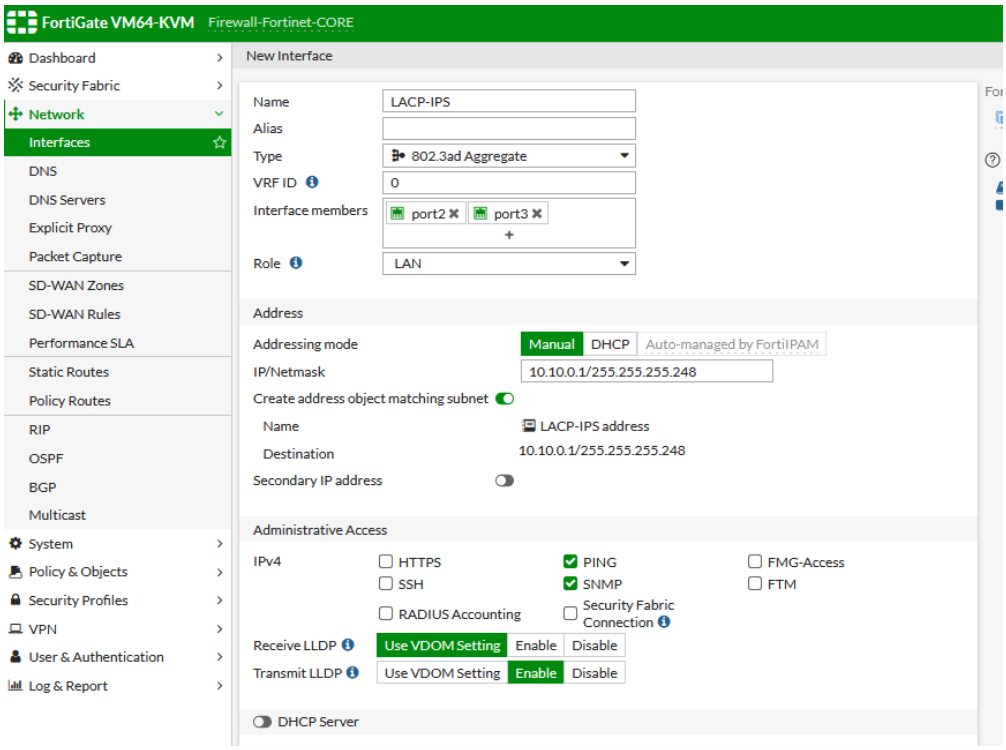
Verificación

ArubaCX2

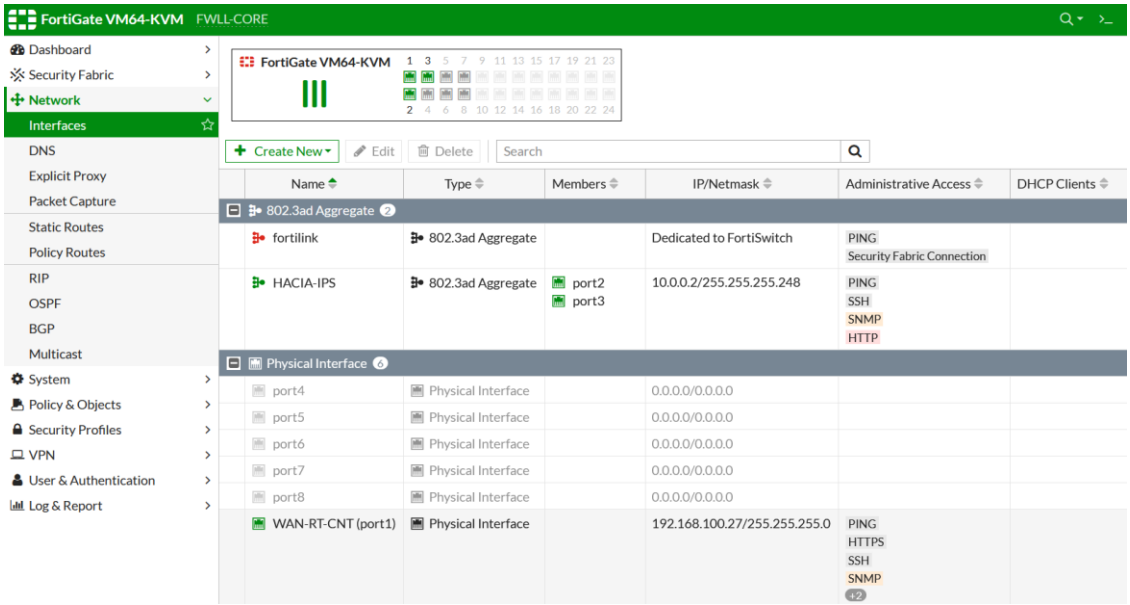
```
2-SW-DATACENTER-24P# show interface vlan 1

Interface vlan1 is up
 Admin state is up
 Description: MGMT-SW-DATACENTER-24P
 Hardware: Ethernet, MAC Address: 08:00:09:65:08:c9
 IPv4 address 192.168.0.2/24
    active-gateway ip 192.168.0.254

 Statistic                        RX                  TX                Total
 ---------------- -------------------- -------------------- --------------------
 L3 Packets                          0                    0                    0
 L3 Bytes                            0                    0                    0
```

Verificación

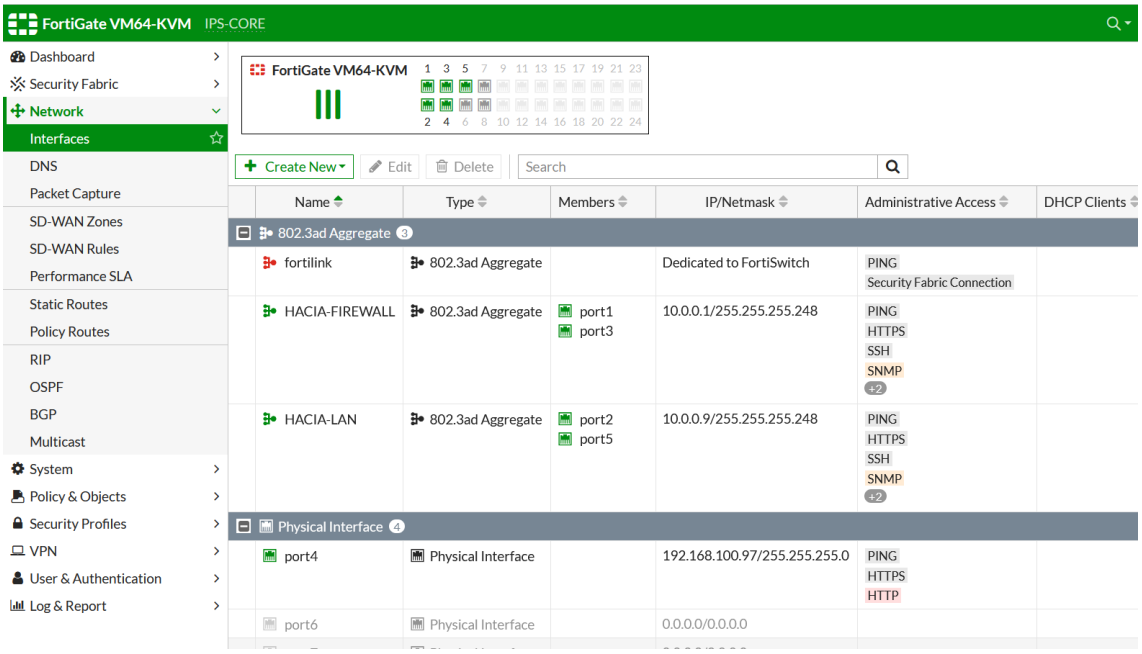
Anexo 10. Configuraciones Capa 2 Firewall-IPS



Configuración LACP en Fortinet



Verificación LACP - Firewall



Verificación LACP - IPS

Anexo 11. Configuraciones Capa 3 Aruba

```
interface vlan 1
description MGMT-GTWY
ip address 192.168.0.254/24
no shutdown
exit
interface vlan 10
description SERVIDORES-GTWY
ip address 192.168.1.254/24
no shutdown
exit
interface vlan 20
description CAMARAS-GTWY
ip address 192.168.2.254/24
no shutdown
exit
interface vlan 30
description USUARIOS-GTWY
ip address 192.168.3.254/24
no shutdown
exit
interface vlan 50
description NZD-GTWY
ip address 192.168.5.254/24
no shutdown
exit
interface vlan 60
description HACIA-WAN
ip address 10.0.0.10/29
no shutdown
exit
interface vlan 70
description GERENCIA-GTWY
ip address 192.168.7.254/24
no shutdown
exit
```

```
access-list ip ACL-LISTA
deny ip 192.168.3.0/24 192.168.0.0/24
deny ip 192.168.3.0/24 192.168.1.0/24
deny ip 192.168.3.0/24 192.168.2.0/24
deny ip 192.168.3.0/24 192.168.5.0/24
deny ip 192.168.3.0/24 192.168.7.0/24
deny ip 192.168.7.0/24 192.168.3.0/24
deny ip 192.168.1.0/24 192.168.3.0/24
deny ip 192.168.2.0/24 192.168.3.0/24
deny ip 192.168.5.0/24 192.168.3.0/24
permit ip any any
exit

interface lag 1
apply access-list ip ACL-LISTA in
exit

interface lag 2
apply access-list ip ACL-LISTA in
exit

interface 1/1/6
apply access-list ip ACL-LISTA in
exit

interface 1/1/7
apply access-list ip ACL-LISTA in
exit
```

```
vlan1           192.168.0.254/24        up/up

vlan10          192.168.1.254/24        up/up

vlan20          192.168.2.254/24        up/up

vlan30          192.168.3.254/24        up/up

vlan50          192.168.5.254/24        up/up

vlan60          10.0.0.10/29            up/up

vlan70          192.168.7.254/24        up/up


1-SW-CORE-24P#
```

Verificación

ArubaCX

```
1-SW-CORE-24P#  show ip route

Displaying ipv4 routes selected for forwarding

Origin Codes: C - connected, S - static, L - local
              R - RIP, B - BGP, O - OSPF
Type Codes:   E - External BGP, I - Internal BGP, V - VPN, EV - EVPN
              IA - OSPF internal area, E1 - OSPF external type 1
              E2 - OSPF external type 2

VRF: default

Prefix              Nexthop          Interface     VRF(egress)       Origin/   Distance/    Age
                                                                     Type      Metric
-------------------------------------------------------------------------------------------------
0.0.0.0/0           10.0.0.9         vlan60        -                 S         [1/0]        00h:42m:44s
10.0.0.8/29         -                vlan60        -                 C         [0/0]        -
10.0.0.10/32        -                vlan60        -                 L         [0/0]        -
192.168.0.0/24      -                vlan1         -                 C         [0/0]        -
192.168.0.254/32    -                vlan1         -                 L         [0/0]        -
192.168.1.0/24      -                vlan10        -                 C         [0/0]        -
192.168.1.254/32    -                vlan10        -                 L         [0/0]        -
192.168.2.0/24      -                vlan20        -                 C         [0/0]        -
192.168.2.254/32    -                vlan20        -                 L         [0/0]        -
192.168.3.0/24      -                vlan30        -                 C         [0/0]        -
192.168.3.254/32    -                vlan30        -                 L         [0/0]        -
192.168.5.0/24      -                vlan50        -                 C         [0/0]        -
192.168.5.254/32    -                vlan50        -                 L         [0/0]        -
192.168.7.0/24      -                vlan70        -                 C         [0/0]        -
192.168.7.254/32    -                vlan70        -                 L         [0/0]        -

Total Route Count : 15
```

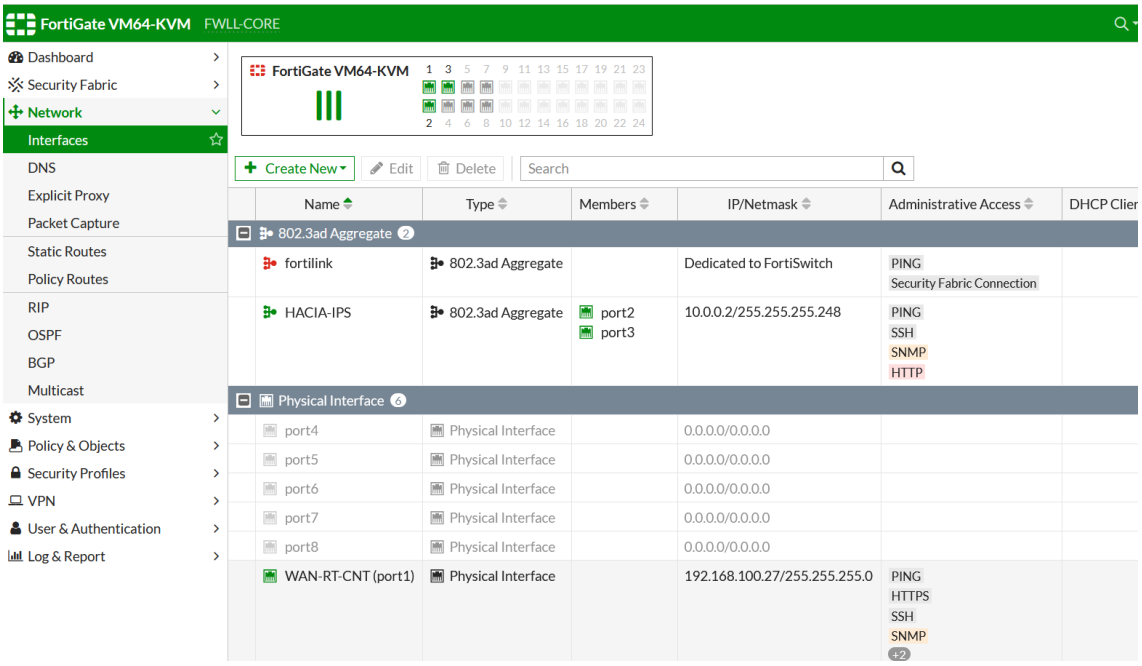
Verificación Tabla de enrutamiento

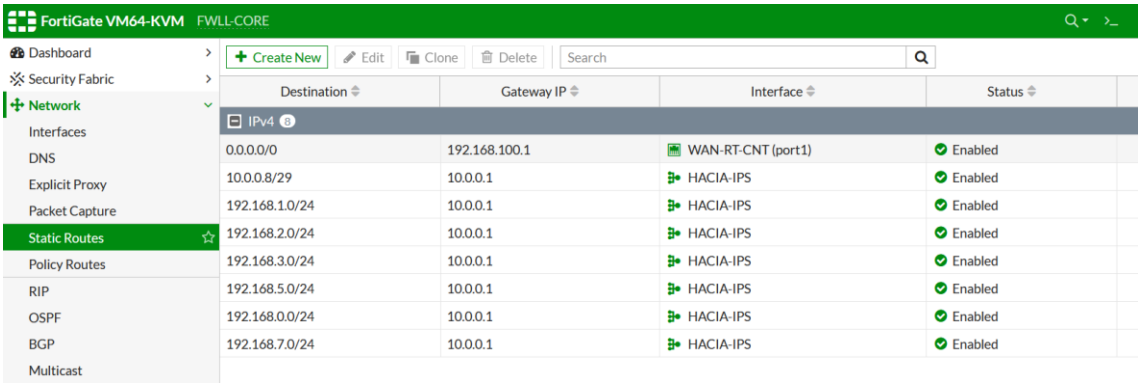
ArubaCX

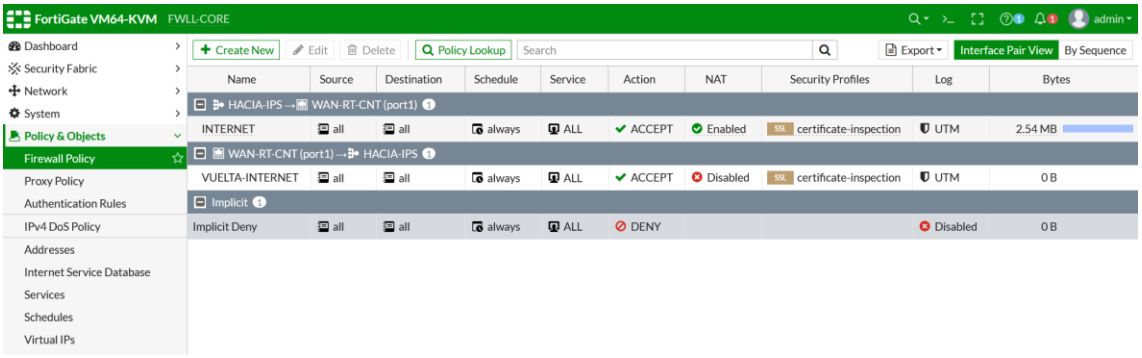
```
1-SW-CORE-24P# show access-list
Type       Name
  Sequence Comment
           Action                          L3 Protocol
           Source IP Address               Source L4 Port(s)
           Destination IP Address          Destination L4 Port(s)
           Additional Parameters
-------------------------------------------------------------------------------
IPv4       ACL-LISTA
        10
           deny                            any
           192.168.3.0/255.255.255.0
           192.168.0.0/255.255.255.0
        20
           deny                            any
           192.168.3.0/255.255.255.0
           192.168.1.0/255.255.255.0
        30
           deny                            any
           192.168.3.0/255.255.255.0
           192.168.2.0/255.255.255.0
        40
           deny                            any
           192.168.3.0/255.255.255.0
           192.168.5.0/255.255.255.0
        50
           deny                            any
           192.168.3.0/255.255.255.0
           192.168.7.0/255.255.255.0
        60
           deny                            any
           192.168.7.0/255.255.255.0
           192.168.3.0/255.255.255.0
        70
           deny                            any
           192.168.1.0/255.255.255.0
           192.168.3.0/255.255.255.0
        80
           deny                            any
           192.168.2.0/255.255.255.0
           192.168.3.0/255.255.255.0
        90
           deny                            any
           192.168.5.0/255.255.255.0
           192.168.3.0/255.255.255.0
       100
           permit                          any
           any
           any
```

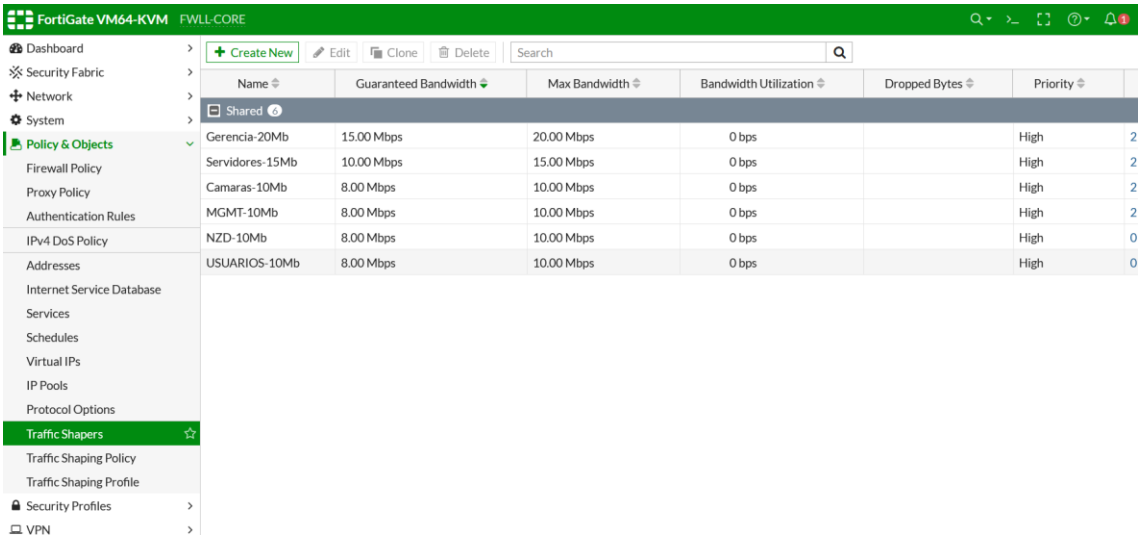
Verificación tabla de ACLs

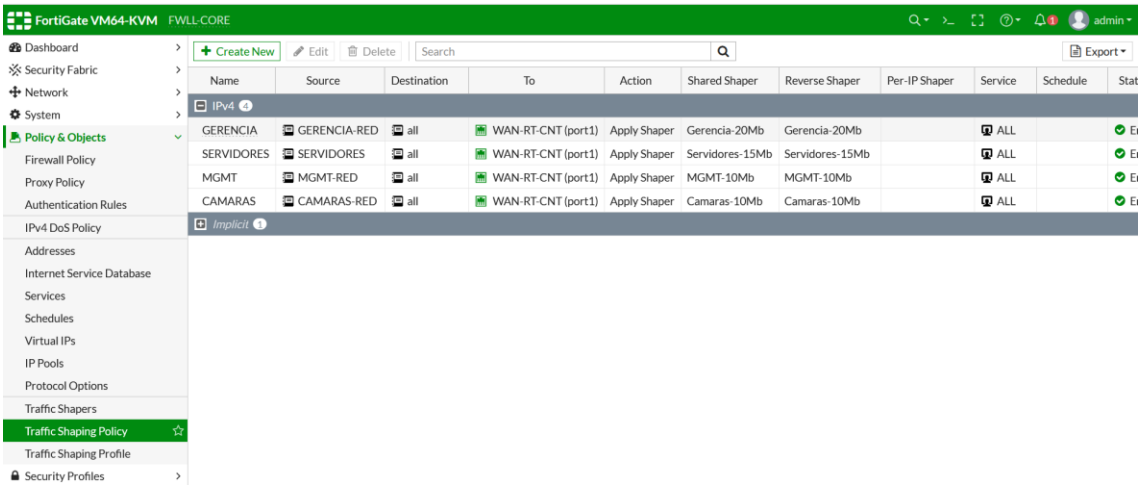
Anexo 12. Configuraciones Capa 3 Firewall – IPS

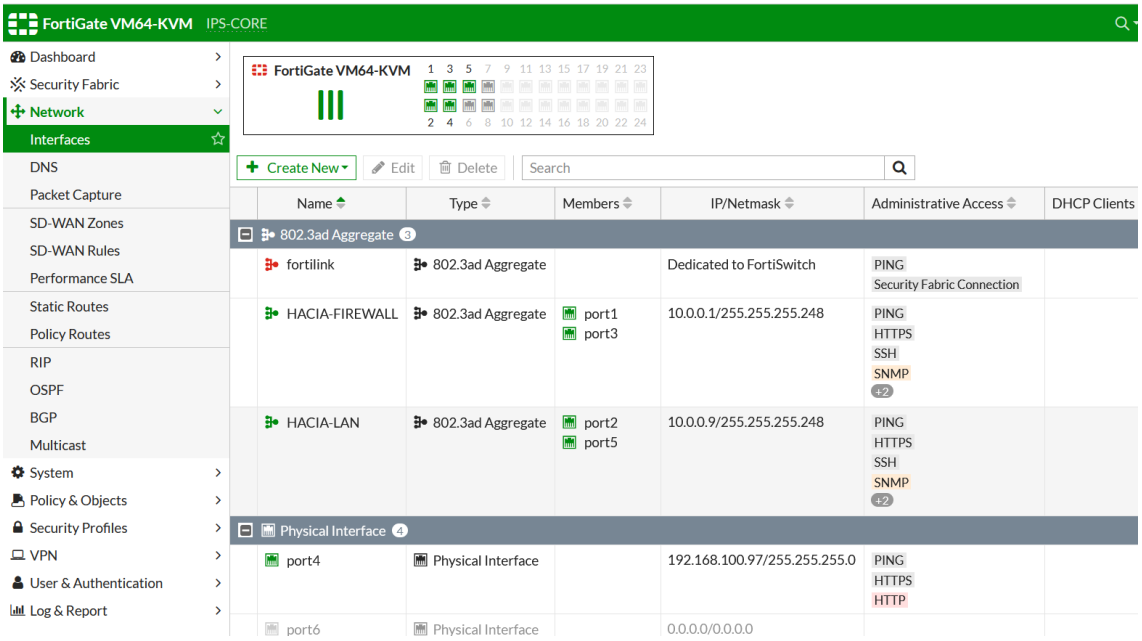


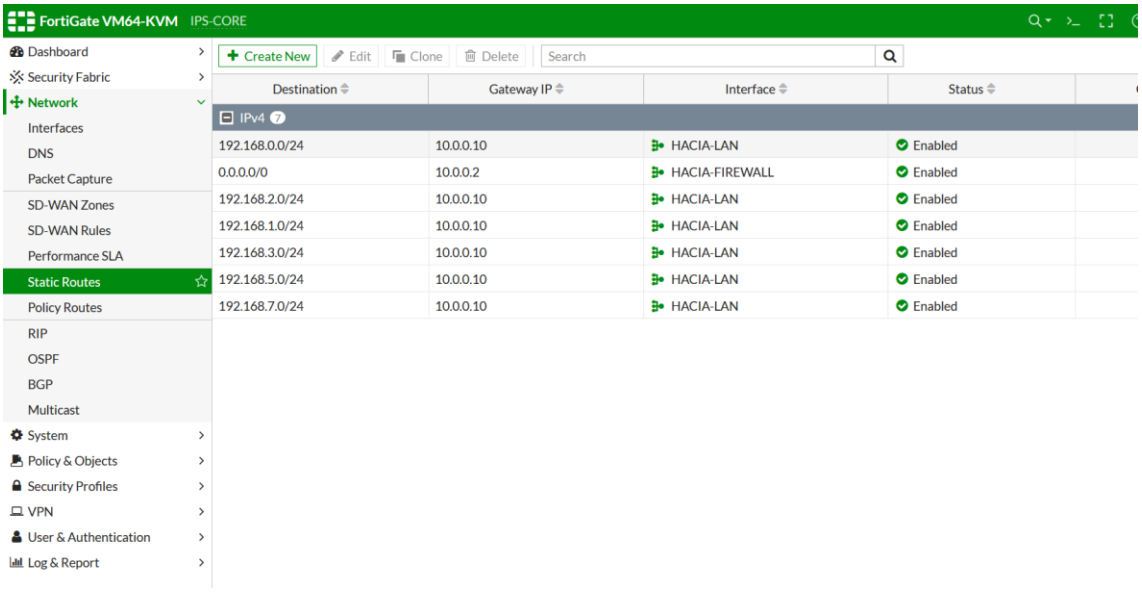


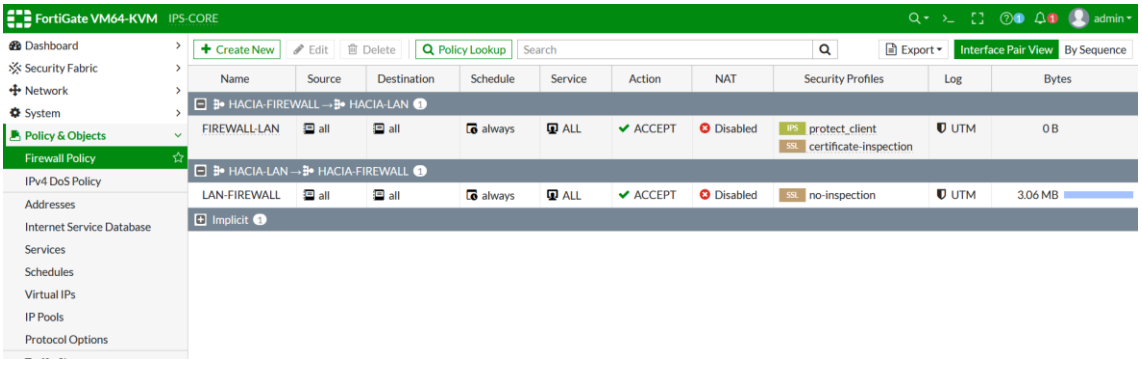

FortiGate VM64-KVM FWLL-CORE
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
Proxy Policy
Authentication Rules
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
Create New
Edit
Delete
Policy Lookup
Search
Export
Interface Pair View
By Sequence
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
HACIA-IPS → WAN-RT-CNT (port1)
INTERNET
all
all
always
ALL
ACCEPT
Enabled
certificate-inspection
UTM
2.54 MB
WAN-RT-CNT (port1) → HACIA-IPS
VUELTA-INTERNET
all
all
always
ALL
ACCEPT
Disabled
certificate-inspection
UTM
0 B
Implicit
Implicit Deny
all
all
always
ALL
DENY
Disabled
0 B


FortiGate VM64-KVM FWLL-CORE
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
Proxy Policy
Authentication Rules
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
Security Profiles
VPN
Create New
Edit
Clone
Delete
Search
Name
Guaranteed Bandwidth
Max Bandwidth
Bandwidth Utilization
Dropped Bytes
Priority
Shared
Gerencia-20Mb
15.00 Mbps
20.00 Mbps
0 bps
High
Servidores-15Mb
10.00 Mbps
15.00 Mbps
0 bps
High
Camaras-10Mb
8.00 Mbps
10.00 Mbps
0 bps
High
MGMT-10Mb
8.00 Mbps
10.00 Mbps
0 bps
High
NZD-10Mb
8.00 Mbps
10.00 Mbps
0 bps
High
USUARIOS-10Mb
8.00 Mbps
10.00 Mbps
0 bps
High


FortiGate VM64-KVM FWLL-CORE
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
Proxy Policy
Authentication Rules
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
Security Profiles
Create New
Edit
Delete
Search
Export
Name
Source
Destination
To
Action
Shared Shaper
Reverse Shaper
Per-IP Shaper
Service
Schedule
IPv4
GERENCIA
GERENCIA-RED
all
WAN-RT-CNT (port1)
Apply Shaper
Gerencia-20Mb
Gerencia-20Mb
ALL
SERVIDORES
SERVIDORES
all
WAN-RT-CNT (port1)
Apply Shaper
Servidores-15Mb
Servidores-15Mb
ALL
MGMT
MGMT-RED
all
WAN-RT-CNT (port1)
Apply Shaper
MGMT-10Mb
MGMT-10Mb
ALL
CAMARAS
CAMARAS-RED
all
WAN-RT-CNT (port1)
Apply Shaper
Camaras-10Mb
Camaras-10Mb
ALL
Implicit


FortiGate VM64-KVM IPS-CORE
Dashboard
Security Fabric
Network
Interfaces
DNS
Packet Capture
SD-WAN Zones
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Authentication
Log & Report
FortiGate VM64-KVM
Create New
Edit
Delete
Search
Name
Type
Members
IP/Netmask
Administrative Access
DHCP Clients
802.3ad Aggregate 3
fortilink
802.3ad Aggregate
Dedicated to FortiSwitch
PING
Security Fabric Connection
HACIA-FIREWALL
802.3ad Aggregate
port1
port3
10.0.0.1/255.255.255.248
PING
HTTPS
SSH
SNMP
+2
HACIA-LAN
802.3ad Aggregate
port2
port5
10.0.0.9/255.255.255.248
PING
HTTPS
SSH
SNMP
+2
Physical Interface 4
port4
Physical Interface
192.168.100.97/255.255.255.0
PING
HTTPS
HTTP
port6
Physical Interface
0.0.0.0/0.0.0.0

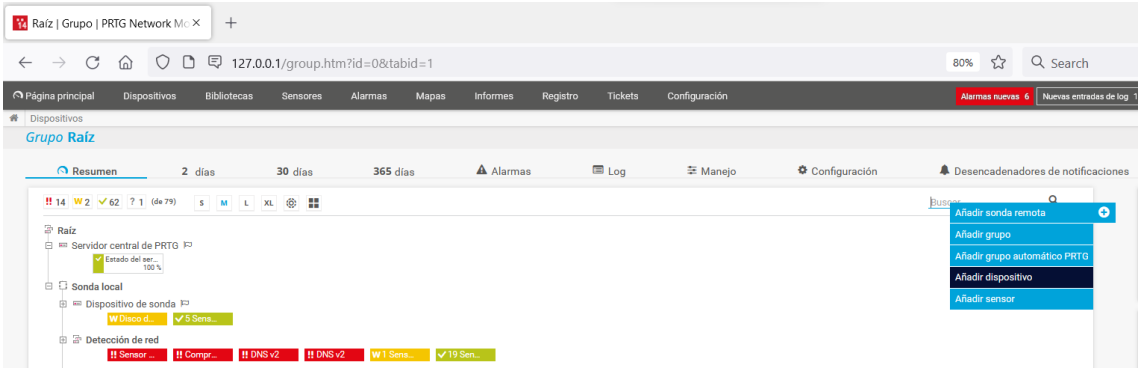

FortiGate VM64-KVM IPS-CORE
Dashboard
Security Fabric
Network
Interfaces
DNS
Packet Capture
SD-WAN Zones
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
Policy & Objects
Security Profiles
VPN
User & Authentication
Log & Report
Create New
Edit
Clone
Delete
Search
Destination
Gateway IP
Interface
Status
IPv4 7
192.168.0.0/24
10.0.0.10
HACIA-LAN
Enabled
0.0.0.0/0
10.0.0.2
HACIA-FIREWALL
Enabled
192.168.2.0/24
10.0.0.10
HACIA-LAN
Enabled
192.168.1.0/24
10.0.0.10
HACIA-LAN
Enabled
192.168.3.0/24
10.0.0.10
HACIA-LAN
Enabled
192.168.5.0/24
10.0.0.10
HACIA-LAN
Enabled
192.168.7.0/24
10.0.0.10
HACIA-LAN
Enabled


FortiGate VM64-KVM IPS-CORE
admin
Dashboard
Security Fabric
Network
System
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Create New
Edit
Delete
Policy Lookup
Search
Export
Interface Pair View
By Sequence
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
HACIA-FIREWALL → HACIA-LAN 1
FIREWALL-LAN
all
all
always
ALL
ACCEPT
Disabled
protect_client
certificate-inspection
UTM
0 B
HACIA-LAN → HACIA-FIREWALL 1
LAN-FIREWALL
all
all
always
ALL
ACCEPT
Disabled
no-inspection
UTM
3.06 MB
Implicit 1

Anexo 13. Configuraciones PRTG – MONITOREO DE LA RED (SNMP)

Aruba

```
151   snmp-server community Raiz
152   snmp-server host 192.168.100.7 trap version v2c community Raiz
```



Añadir grupo al grupo Sonda local ×

Añadir dispositivo nuevo

Defina un nombre y dirección IP de dispositivo, opciones para el descubrimiento automático y parámetros de credenciales para Windows, Linux, VMware/XenServer, SNMP y proveedores específicos de ser necesario.

Manual de PRTG: Añadir un dispositivo

Nombre y dirección del dispositivo

Nombre del dispositivo

SW-CORE-

Version de IP

- (•) IPv4
- ( ) IPv6

Dirección IPv4/nombre de DNS

10.0.0.10

Etiquetas

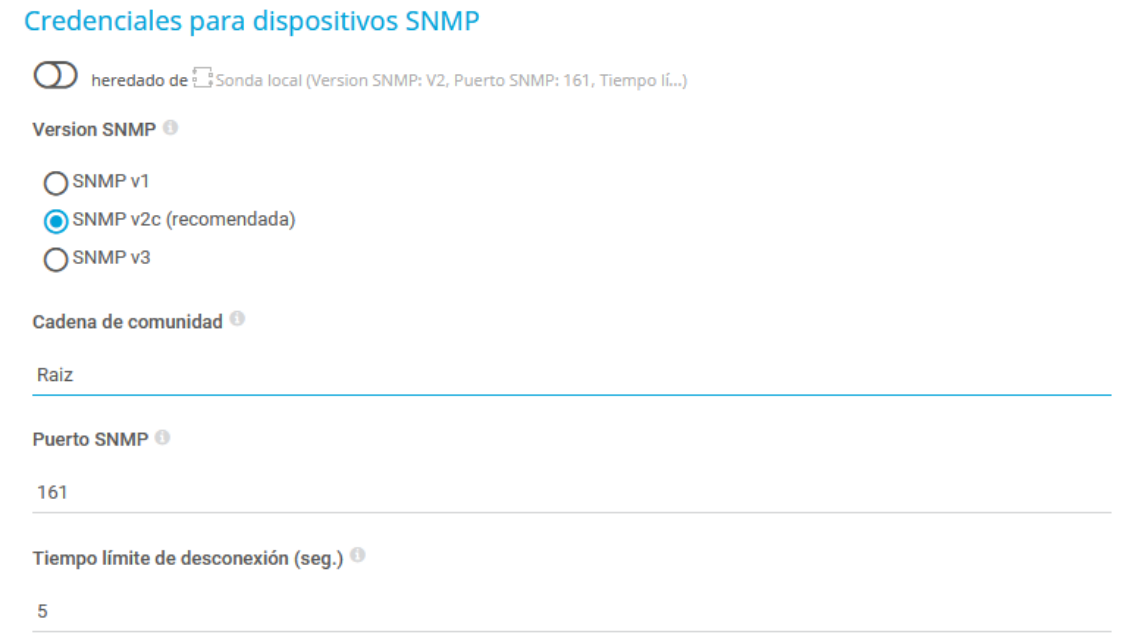
⊕

Icono de dispositivo

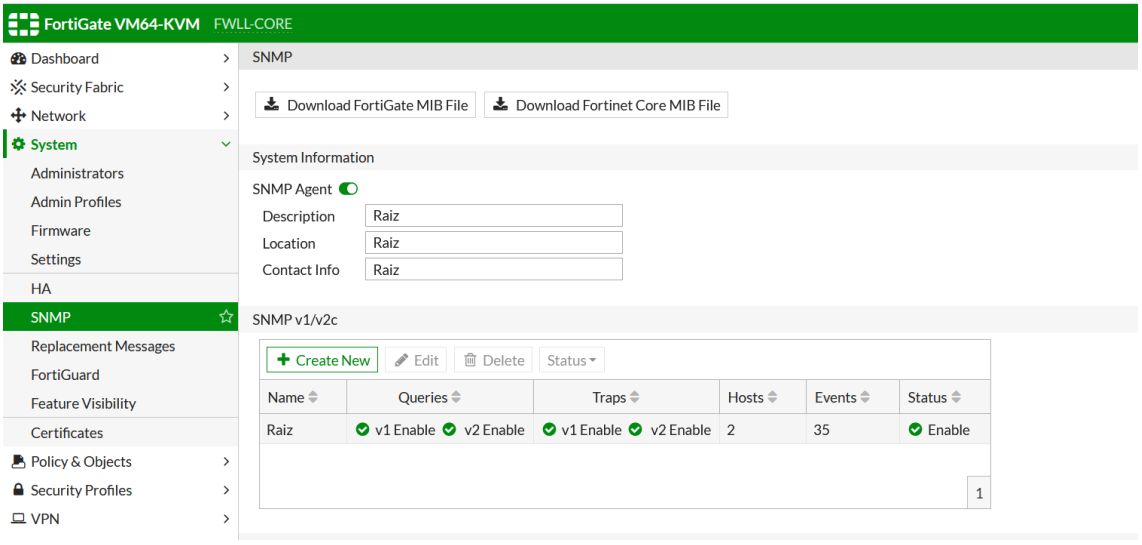
Identificación de dispositivo y descubrimiento automático

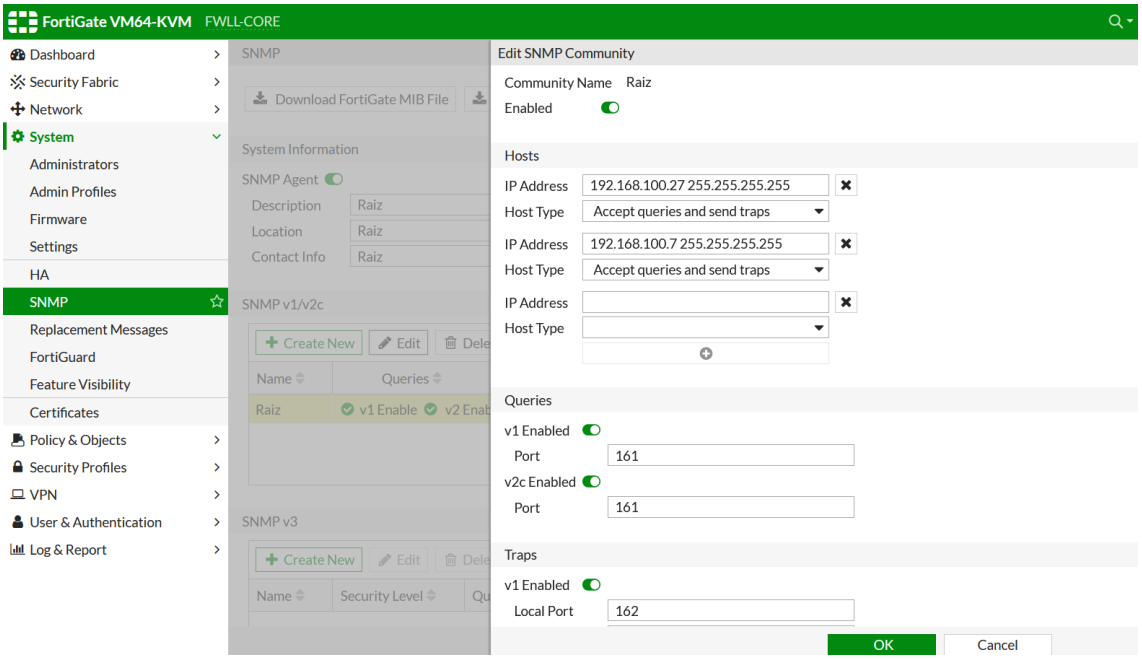
Nivel de descubrimiento automático

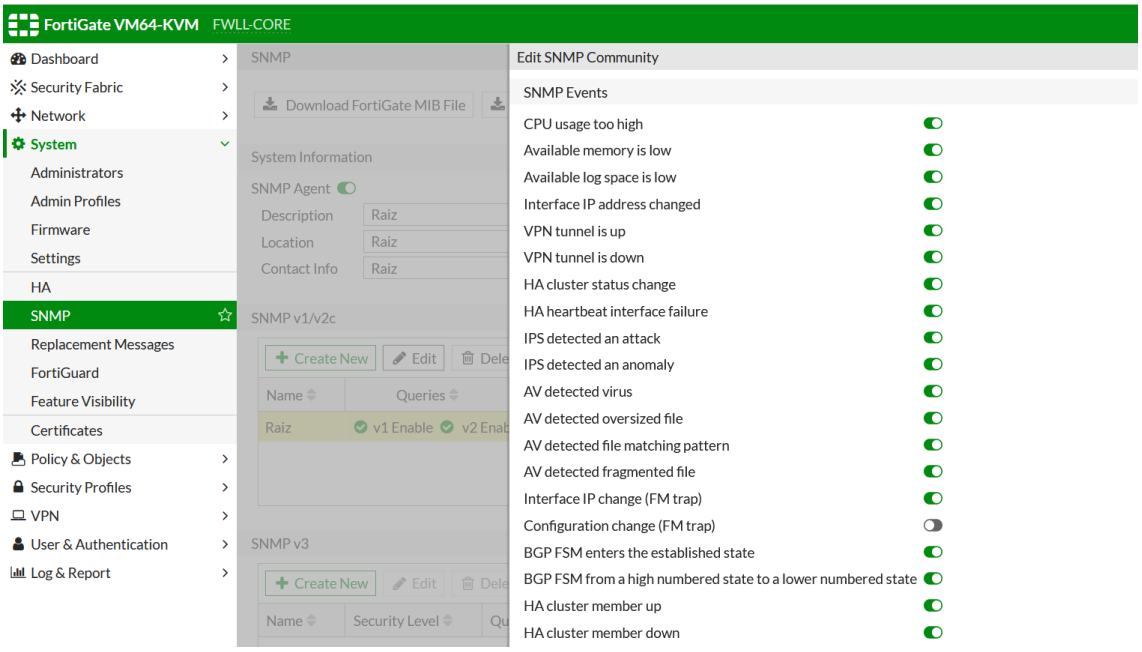
- ( ) Sin descubrimiento automático
- (•) Descubrimiento automático estándar (recomendado)
- ( ) Descubrimiento automático detallado
- ( ) Descubrimiento automático con plantillas de dispositivo específicas

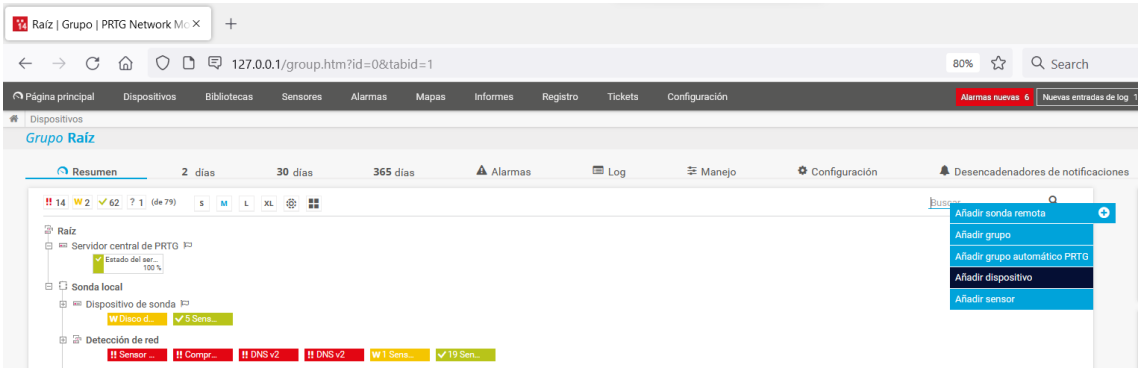

Credenciales para dispositivos SNMP
heredado de Sonda local (Version SNMP: V2, Puerto SNMP: 161, Tiempo lí...)
Version SNMP
SNMP v1
SNMP v2c (recomendada)
SNMP v3
Cadena de comunidad
Raiz
Puerto SNMP
161
Tiempo límite de desconexión (seg.)
5

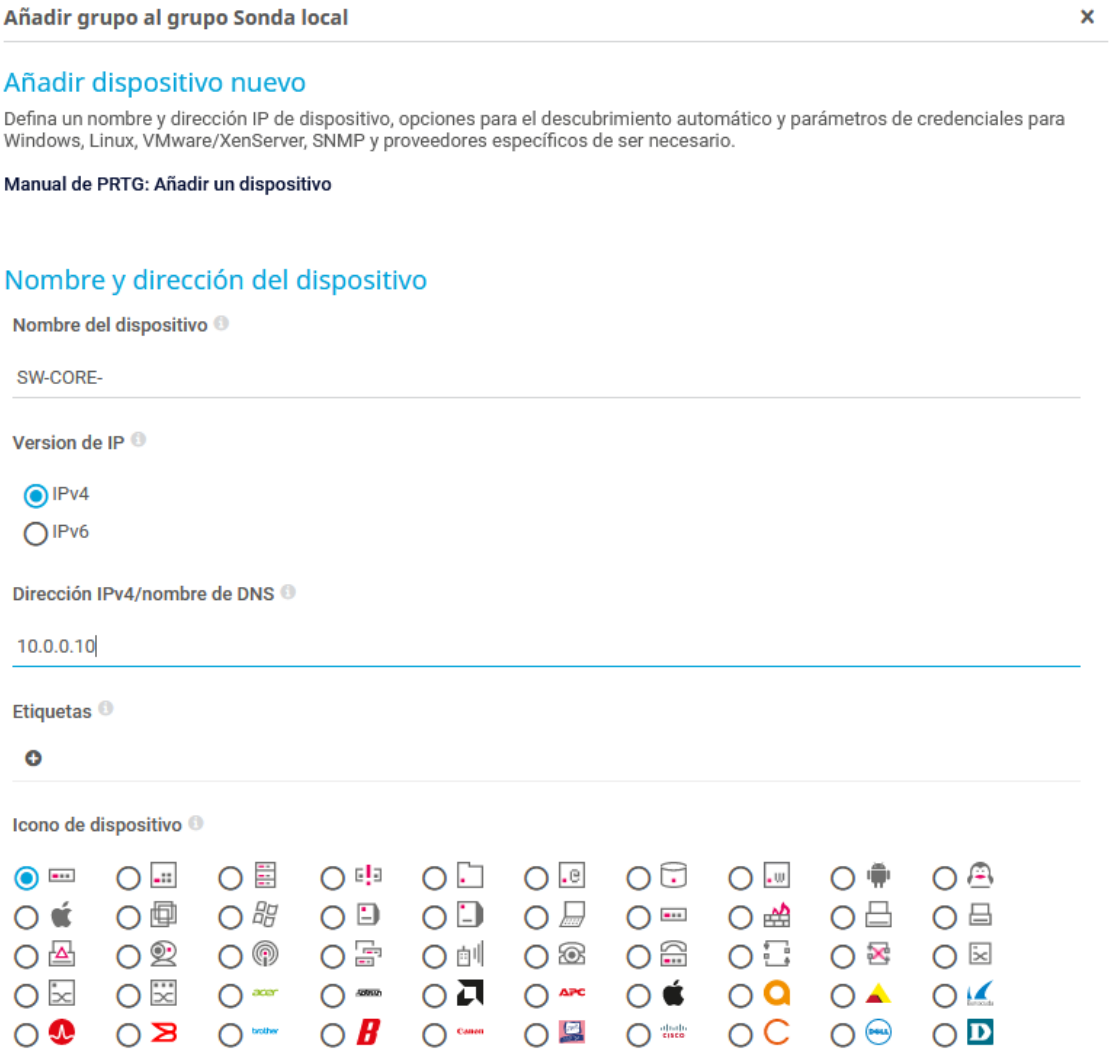
Fortinet


FortiGate VM64-KVM
FWLL-CORE
Dashboard
Security Fabric
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Policy & Objects
Security Profiles
VPN
SNMP
Download FortiGate MIB File
Download Fortinet Core MIB File
System Information
SNMP Agent
Description Raiz
Location Raiz
Contact Info Raiz
SNMP v1/v2c
Create New
Edit
Delete
Status
Name
Queries
Traps
Hosts
Events
Status
Raiz
v1 Enable v2 Enable
v1 Enable v2 Enable
2
35
Enable
1


FortiGate VM64-KVM FWLL-CORE
Dashboard
Security Fabric
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Policy & Objects
Security Profiles
VPN
User & Authentication
Log & Report
SNMP
Download FortiGate MIB File
System Information
SNMP Agent
Description Raiz
Location Raiz
Contact Info Raiz
SNMP v1/v2c
Create New
Edit
Name
Queries
Raiz
v1 Enable
SNMP v3
Security Level
Edit SNMP Community
Community Name Raiz
Enabled
Hosts
IP Address 192.168.100.27 255.255.255.255
Host Type Accept queries and send traps
IP Address 192.168.100.7 255.255.255.255
Host Type Accept queries and send traps
IP Address
Host Type
Queries
v1 Enabled
Port 161
v2c Enabled
Port 161
Traps
v1 Enabled
Local Port 162
OK
Cancel


FortiGate VM64-KVM FWLL-CORE
Dashboard
Security Fabric
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Policy & Objects
Security Profiles
VPN
User & Authentication
Log & Report
SNMP
Download FortiGate MIB File
System Information
SNMP Agent
Description Raiz
Location Raiz
Contact Info Raiz
SNMP v1/v2c
Create New
Edit
Name
Queries
Raiz
v1 Enable
SNMP v3
Security Level
Edit SNMP Community
SNMP Events
CPU usage too high
Available memory is low
Available log space is low
Interface IP address changed
VPN tunnel is up
VPN tunnel is down
HA cluster status change
HA heartbeat interface failure
IPS detected an attack
IPS detected an anomaly
AV detected virus
AV detected oversized file
AV detected file matching pattern
AV detected fragmented file
Interface IP change (FM trap)
Configuration change (FM trap)
BGP FSM enters the established state
BGP FSM from a high numbered state to a lower numbered state
HA cluster member up
HA cluster member down


Raíz | Grupo | PRTG Network Mc
127.0.0.1/group.htm?id=0&tabid=1
80%
Search
Página principal
Dispositivos
Bibliotecas
Sensores
Alarmas
Mapas
Informes
Registro
Tickets
Configuración
Alarmas nuevas 6
Nuevas entradas de log
Dispositivos
Grupo Raíz
Resumen
2 días
30 días
365 días
Alarmas
Log
Manejo
Configuración
Desencadenadores de notificaciones
Raíz
Servidor central de PRTG
Sonda local
Dispositivo de sonda
Detección de red
Añadir sonda remota
Añadir grupo
Añadir grupo automático PRTG
Añadir dispositivo
Añadir sensor


Añadir grupo al grupo Sonda local
Añadir dispositivo nuevo
Defina un nombre y dirección IP de dispositivo, opciones para el descubrimiento automático y parámetros de credenciales para Windows, Linux, VMware/XenServer, SNMP y proveedores específicos de ser necesario.
Manual de PRTG: Añadir un dispositivo
Nombre y dirección del dispositivo
Nombre del dispositivo
SW-CORE-
Version de IP
IPv4
IPv6
Dirección IPv4/nombre de DNS
10.0.0.10
Etiquetas
Icono de dispositivo

Identificación de dispositivo y descubrimiento automático

Nivel de descubrimiento automático

- ◯ Sin descubrimiento automático
- ◉ Descubrimiento automático estándar (recomendado)
- ◯ Descubrimiento automático detallado
- ◯ Descubrimiento automático con plantillas de dispositivo específicas

Credenciales para dispositivos SNMP

heredado de Sonda local (Version SNMP: V2, Puerto SNMP: 161, Tiempo lí...)

Version SNMP

- ◯ SNMP v1
- ◉ SNMP v2c (recomendada)
- ◯ SNMP v3

Cadena de comunidad

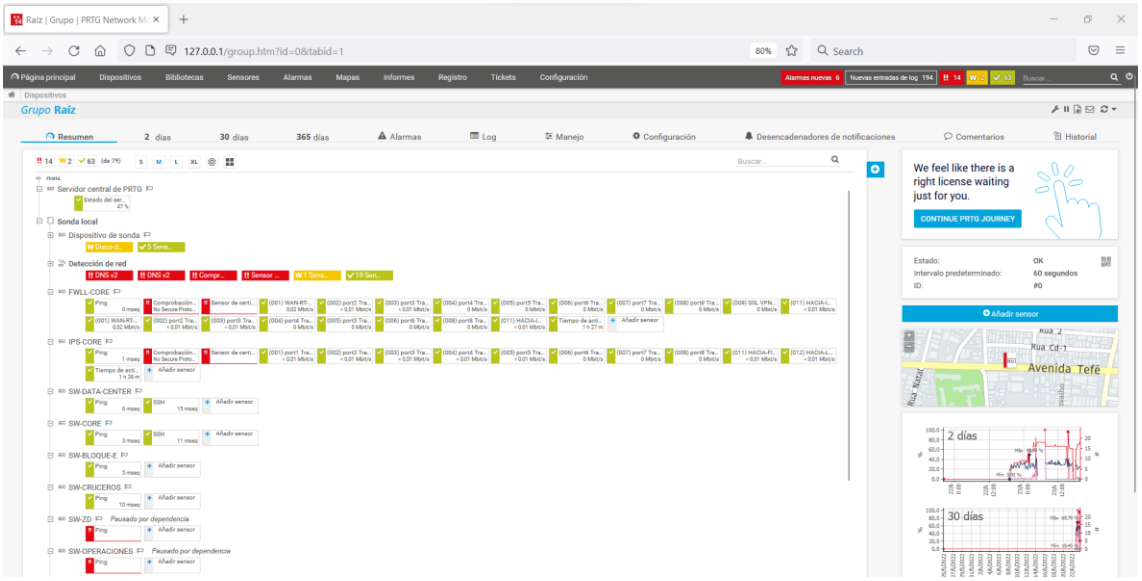
Raiz

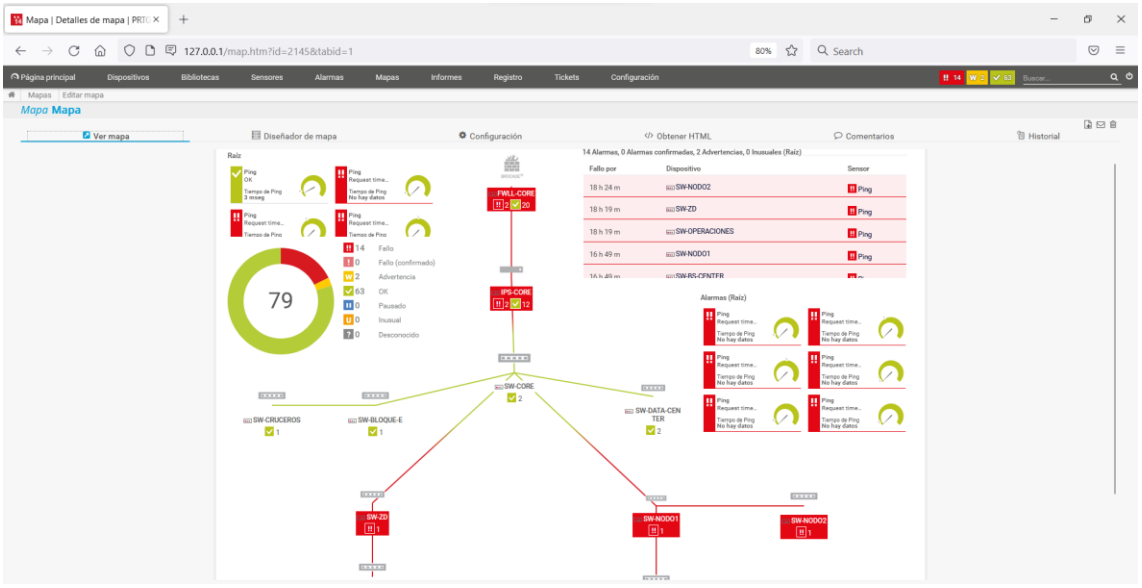
Puerto SNMP

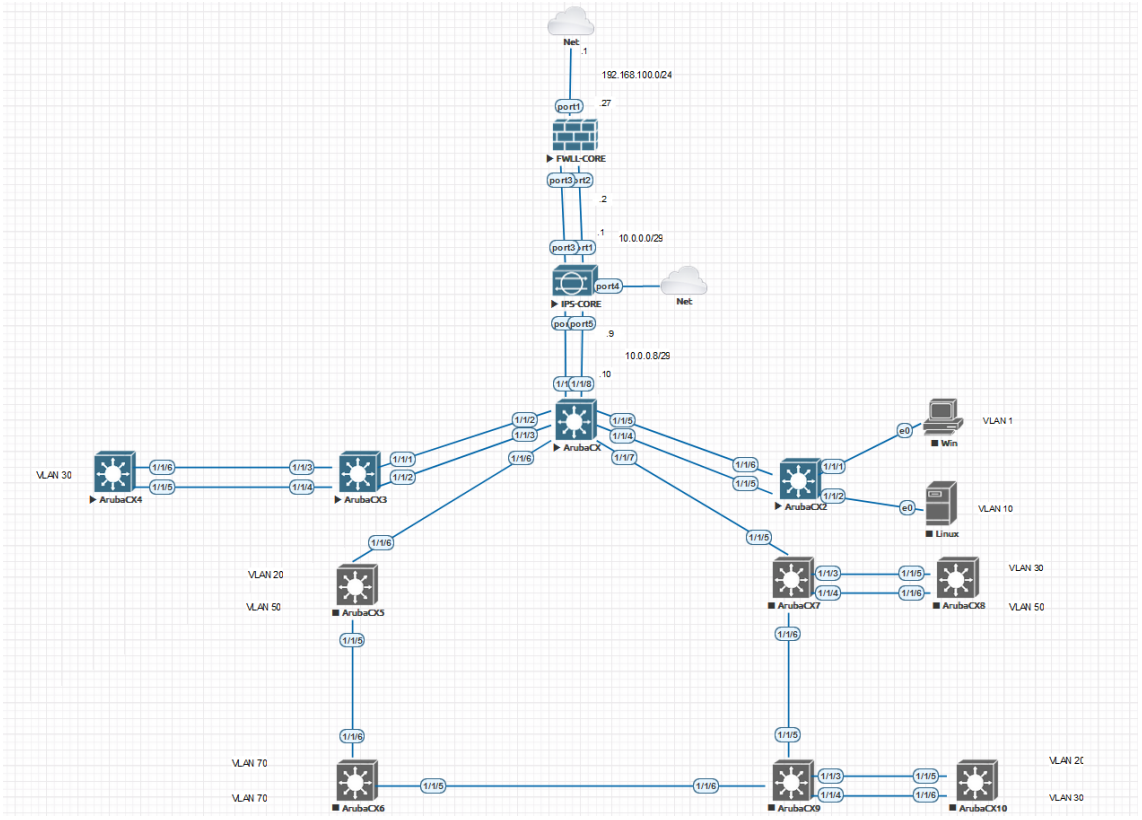
161

Tiempo límite de desconexión (seg.)

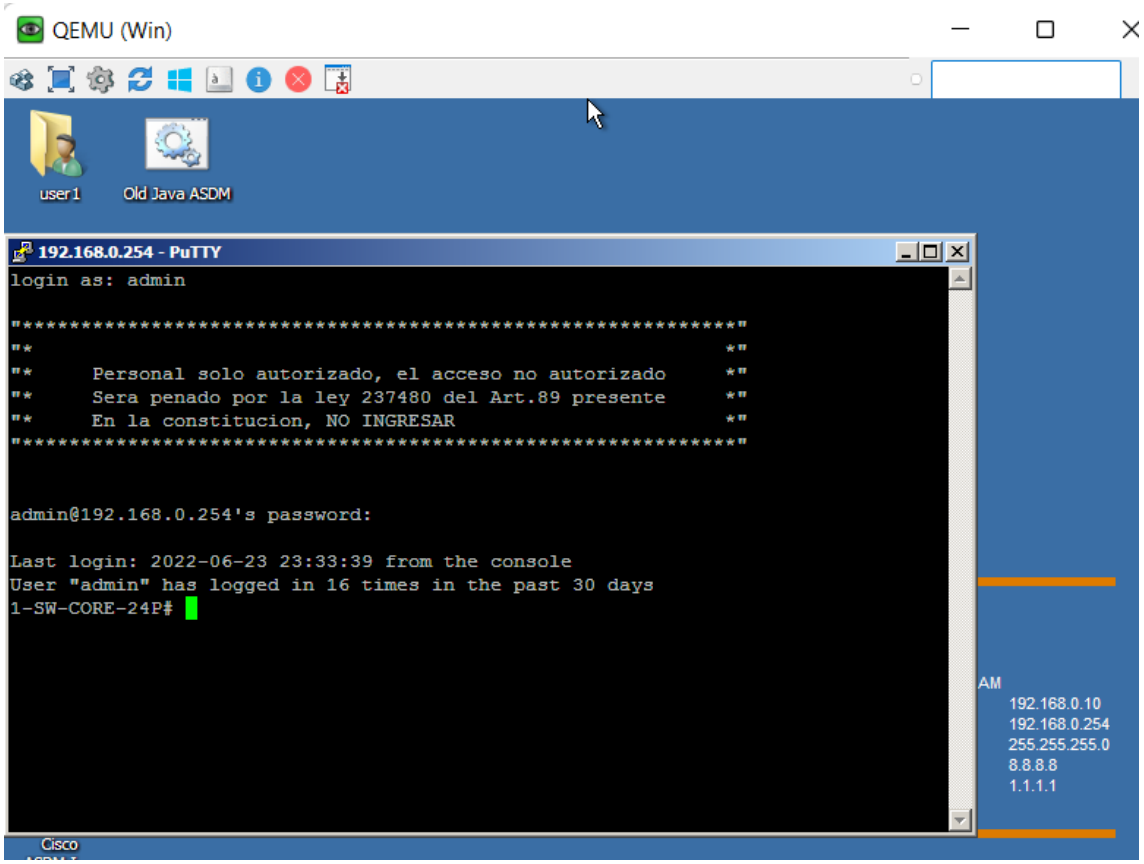
5

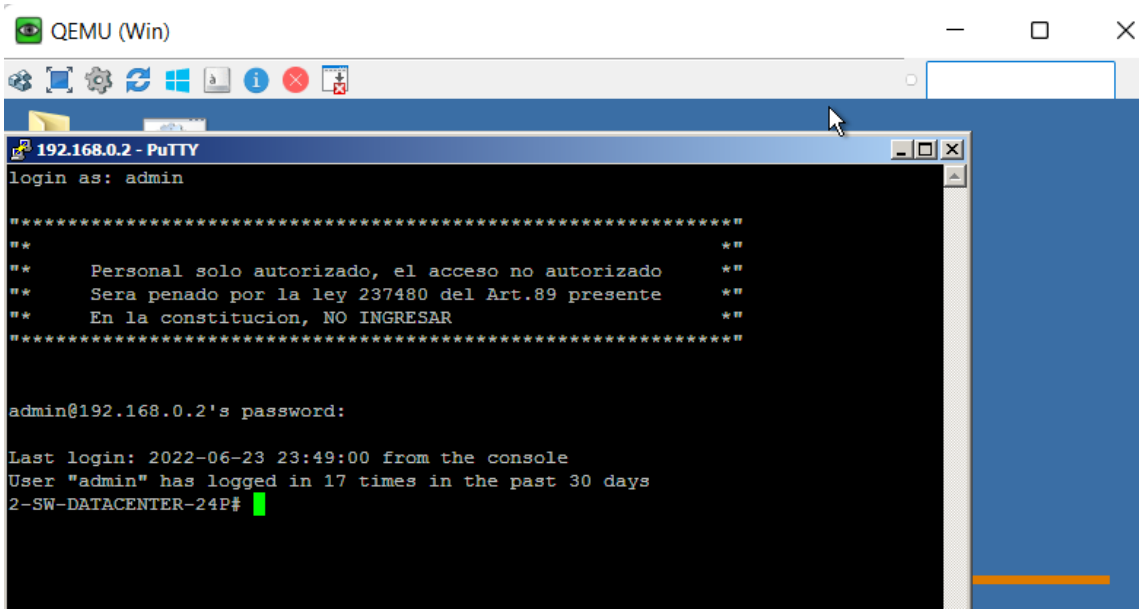


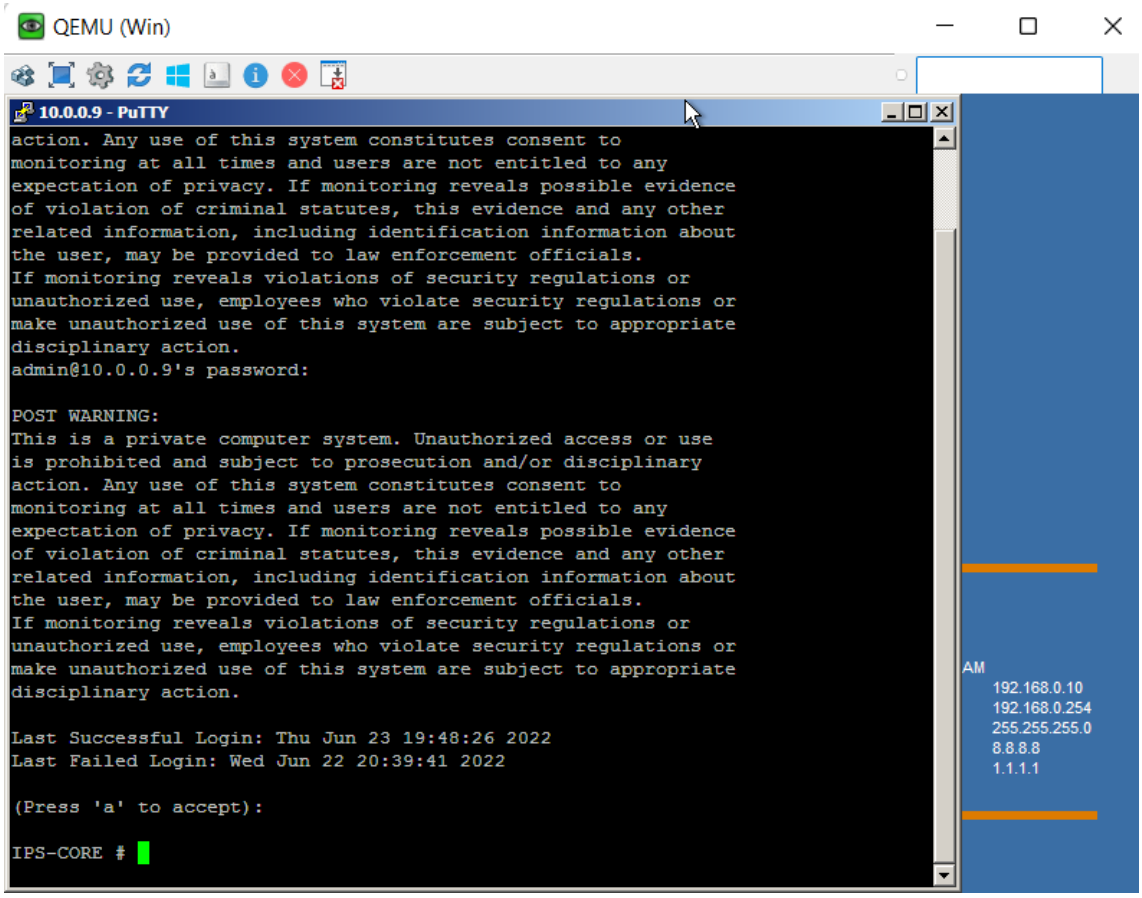

Mapa | Detalles de mapa | PRTG
127.0.0.1/map.htm?id=2145&tabid=1
Página principal
Dispositivos
Bibliotecas
Sensores
Alarmas
Mapas
Informes
Registro
Tickets
Configuración
Mapa Mapa
Ver mapa
Diseñador de mapa
Configuración
Obtener HTML
Comentarios
Historial
Raíz
79
FWLL-CORE
IPS-CORE
SW-CORE
SW-CRUCEROS
SW-BLOQUE-E
SW-DATA-CENTER
SW-25
SW-NODO1
SW-NODO2
Alarmas (Raíz)

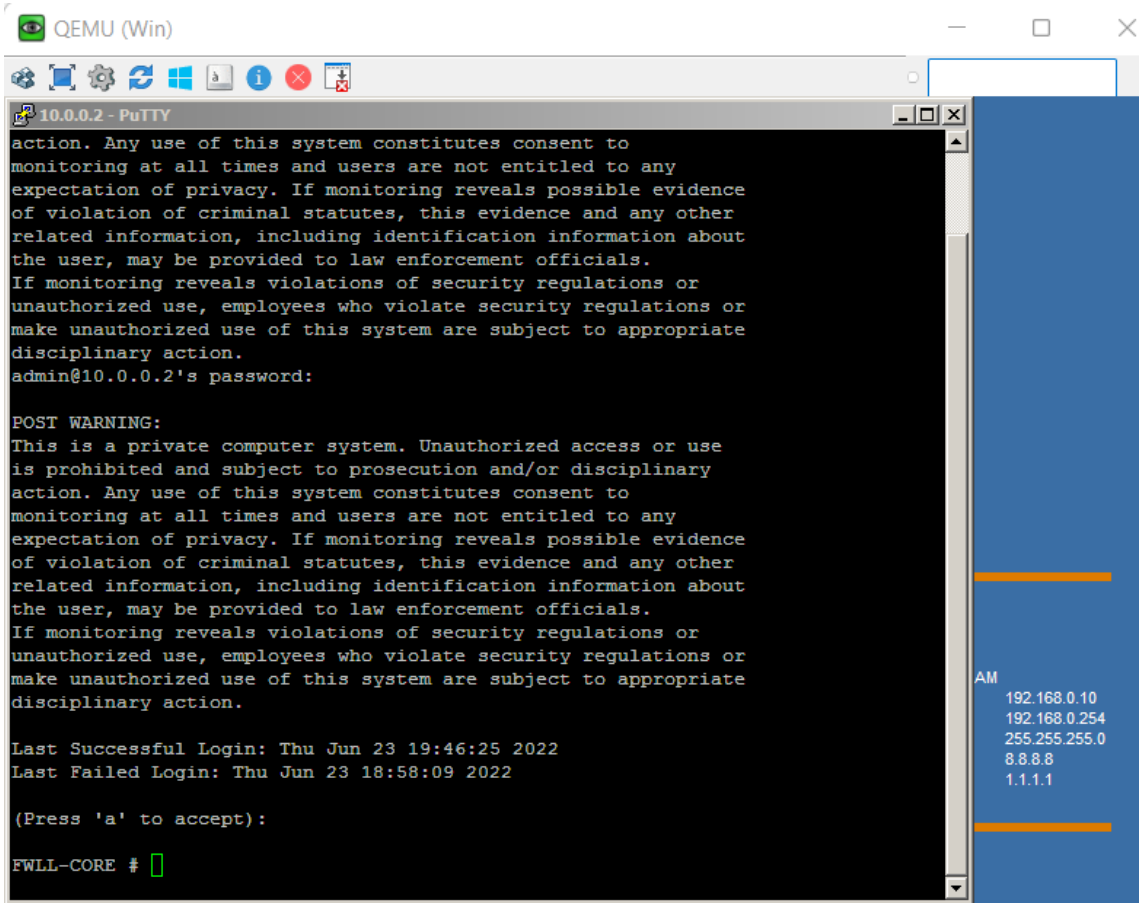

Net
192.168.100.0/24
port1
.27
FWLL-CORE
port3
port2
.2
.1
10.0.0.0/29
port3
port1
IPS-CORE
port4
Net
port5
.9
10.0.0.8/29
.10
1/1/8
ArubaCX
VLAN 30
ArubaCX4
ArubaCX3
VLAN 1
Win
ArubaCX2
VLAN 10
Linux
VLAN 20
VLAN 50
ArubaCX5
ArubaCX7
ArubaCX8
VLAN 30
VLAN 50
VLAN 70
VLAN 70
ArubaCX6
ArubaCX9
ArubaCX10
VLAN 30

Anexo 14. Gestión remota de los dispositivos de red por SSH

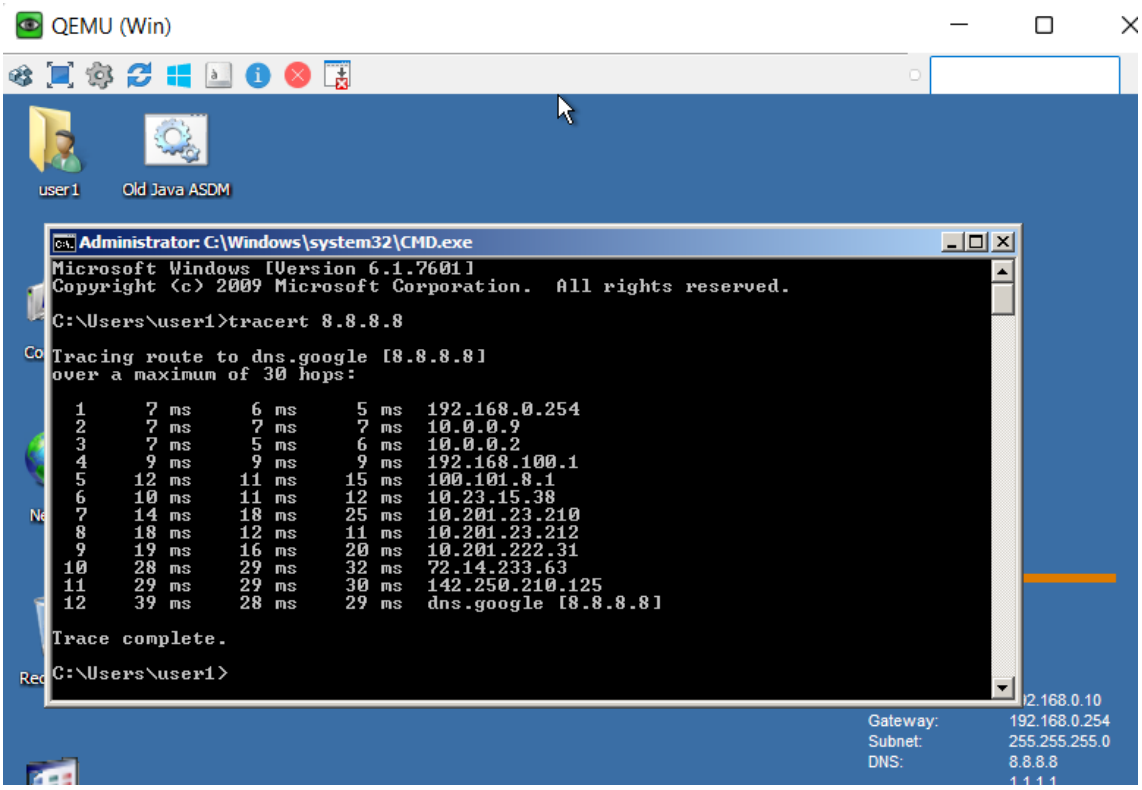





QEMU (Win)
10.0.0.9 - PuTTY
action. Any use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
admin@10.0.0.9's password:
POST WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. Any use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
Last Successful Login: Thu Jun 23 19:48:26 2022
Last Failed Login: Wed Jun 22 20:39:41 2022
(Press 'a' to accept):
IPS-CORE #
AM
192.168.0.10
192.168.0.254
255.255.255.0
8.8.8.8
1.1.1.1


QEMU (Win)
10.0.0.2 - PuTTY
action. Any use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
admin@10.0.0.2's password:
POST WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. Any use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
Last Successful Login: Thu Jun 23 19:46:25 2022
Last Failed Login: Thu Jun 23 18:58:09 2022
(Press 'a' to accept):
FWLL-CORE #
AM
192.168.0.10
192.168.0.254
255.255.255.0
8.8.8.8
1.1.1.1

Anexo 15. Acceso a Internet



Anexo 16. Pruebas de vulnerabilidad en simulación

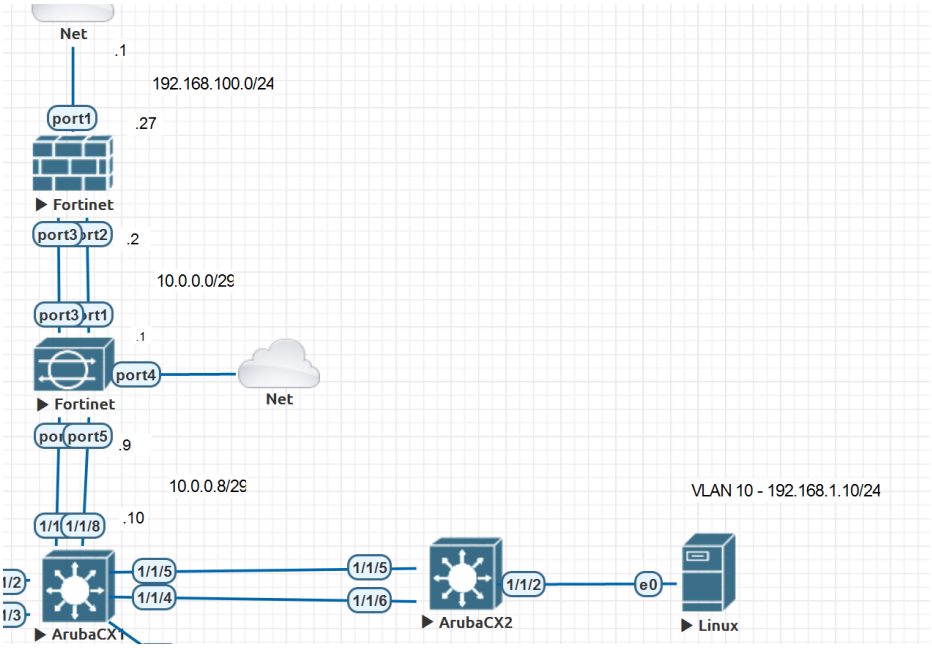


Figura 82 Topología para pruebas de Vulnerabilidad

Anexo 17. LLDP - CDP

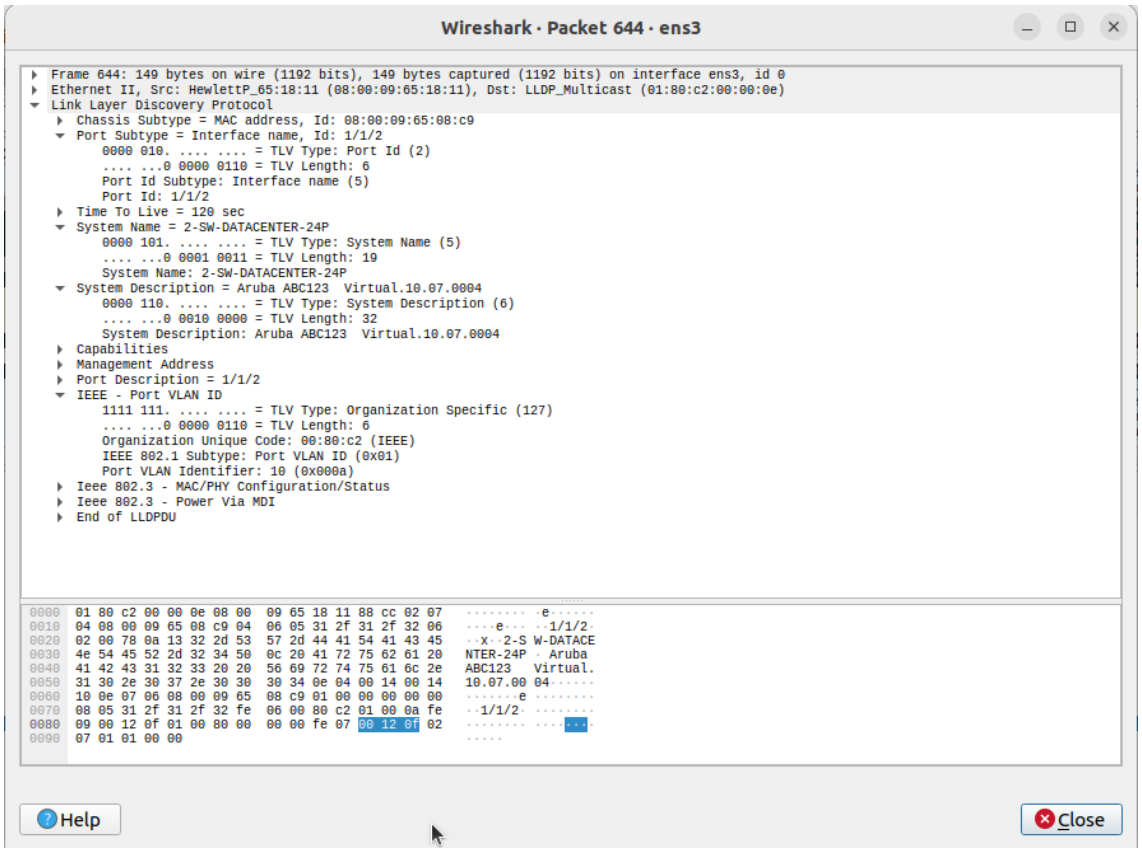


Figura 83 Información capturado por el sniffer Wireshark

Es importante desactivar él envió de paquetes de LLDP en los puertos de acceso del switch ya que puede comprometer la información del equipo de red de acceso como se muestra en la figura

```
2-SW-DATACENTER-24P# configure terminal
2-SW-DATACENTER-24P(config)# interface 1/1/2
2-SW-DATACENTER-24P(config-if)# no lldp transmit
2-SW-DATACENTER-24P(config-if)# exit
2-SW-DATACENTER-24P(config)# do write memorty
```

Anexo 18. MAC Flooding Attack

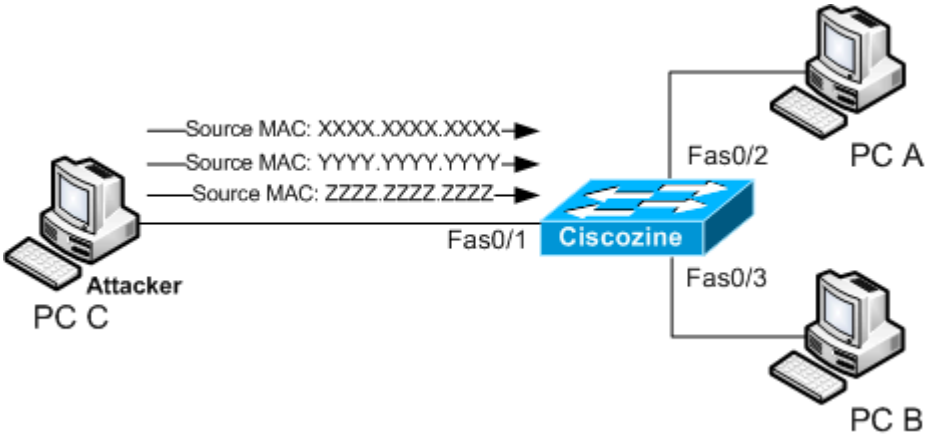


Figura 84 MAC Flooding Attack