UNIVERSIDAD NACIONAL DE INGENIERÍA

Área de conocimiento de Tecnología de la información y Comunicación

Diseño de la Infraestructura de Red de Datos y Seguridad Perimetral Para una Institución Del Estado de Nicaragua

Trabajo Monográfico para optar al título de Ingeniero en Telecomunicaciones

Elaborado por:	**Tutor:**
Br. Josue Adolfo Cruz Hernández	*Msc. Oscar Napoleón Martínez Zapata.*
Carnet: 2015-0036I	

17 de julio de 2024
Managua, Nicaragua

INDICE

Contenido **Pag**

Índice de Figuras

Dedicatoria

A Dios, fuente de sabiduría y fortaleza, por guiarme en cada paso de este camino académico y en cada aspecto de mi vida. Sin su amor y bendiciones, este logro no hubiera sido posible.

A mis padres Bayardo y Luz Marina, cuyo amor incondicional y sacrificio han sido la base sobre la cual he construido mis sueños. Gracias por enseñarme el valor del esfuerzo y la perseverancia, y por ser mi mayor apoyo en cada momento de mi vida.

Y, sobre todo, a mi hija Alessandra, mi mayor inspiración y motivo de superación. Cada sonrisa y abrazo tuyo me han dado la fuerza necesaria para seguir adelante. Este logro es tanto mío como tuyo, porque sin tu amor y alegría, este camino habría sido mucho más difícil de recorrer. Dedico este esfuerzo y dedicación a ti, con la esperanza de que siempre persigas tus sueños y alcances tus propias metas.

Agradecimiento

Primero y, ante todo, agradezco a Dios, cuya guía y fortaleza me han acompañado a lo largo de este arduo pero gratificante camino académico. Sin Su bendición y amor incondicional, este logro no habría sido posible.

A mis maestros, por su paciencia, dedicación y sabiduría. Sus enseñanzas han sido fundamentales para mi desarrollo académico y personal. Gracias por compartir conmigo su conocimiento y experiencia.

A mis hermanos, María José, Hazel y Bayardo, fuente inagotable de apoyo. A mis padres, por su amor incondicional, sus sacrificios y su constante motivación. A mi hija Alessandra, por ser mi mayor fuente de inspiración y alegría. Gracias por creer en mí y por estar siempre a mi lado, brindándome el ánimo necesario para continuar.

A mis compañeros de trabajo, Luis Munguía, Darío García, Wilmer Funez y Arnulfo Rivera por su comprensión y apoyo durante este proceso. Gracias por su paciencia y por permitir que equilibrara mis responsabilidades laborales con mis compromisos académicos.

Finalmente, a mi tutor Msc. Oscar Napoleón Martínez Zapata, por su guía, consejo y apoyo constante. Sus valiosas observaciones y su dedicación han sido cruciales para la realización de esta tesis. Gracias por creer en mi potencial y por su inestimable ayuda en cada etapa de este proyecto.

A todos ustedes, mi más sincero agradecimiento. Este logro es tanto mío como de ustedes.

Resumen

La presente tesis se enfocó en Diseñar la infraestructura de red de datos y seguridad perimetral para una institución del Estado de Nicaragua, con el propósito de mejorar aspectos clave como la escalabilidad, velocidad, confiabilidad, redundancia y almacenamiento. Para lograr este objetivo general, se delinearon una serie de objetivos específicos que guiaron el desarrollo de la investigación.

En primer lugar, se realizó un análisis exhaustivo de las condiciones tecnológicas existentes en el campo de las redes de datos y seguridad perimetral de la institución. Este análisis proporcionó una comprensión profunda de los desafíos y oportunidades presentes en la infraestructura de red, sentando las bases para el diseño propuesto.

Posteriormente, se llevó a cabo un proceso de levantamiento de requerimientos a través de encuentros con el personal a cargo y entrevistas detalladas. Esta etapa fue crucial para identificar las necesidades específicas de la institución y establecer los criterios clave para el rediseño de la red de datos y la seguridad perimetral.

El rediseño de la topología de red existente fue otro paso fundamental en el proceso, con el objetivo de optimizar el flujo de datos y garantizar la redundancia, confiabilidad de red, velocidad, almacenamiento y escalabilidad requeridos. Se implementaron cambios significativos en la infraestructura para mejorar su eficiencia operativa y prepararla para futuros desafíos.

Asimismo, se definió una estrategia de seguridad perimetral integral que resguardara la infraestructura de red de amenazas tanto internas como externas, garantizando la integridad y confidencialidad de los datos de la institución. Esta estrategia incluyó la implementación de tecnologías avanzadas y la coordinación de políticas de seguridad coherentes en toda la infraestructura.

Finalmente, se llevó a cabo una validación exhaustiva del diseño propuesto mediante simulaciones utilizando la herramienta de software GNS3. Esta etapa permitió verificar el óptimo funcionamiento del diseño de la infraestructura de red de datos y seguridad perimetral, identificando posibles áreas de mejora y asegurando que el diseño cumpliera con los requisitos establecidos.

En conclusión, el diseño de la infraestructura de red de datos y seguridad perimetral para la institución del Estado de Nicaragua representó un proceso riguroso y colaborativo que culminó en una mejora significativa en la capacidad tecnológica y de seguridad de la organización. Se espera que los resultados de esta investigación contribuyan al logro de los objetivos estratégicos de la institución en materia de tecnología y seguridad de la información.

1. Introducción

Una institución debe entender la Seguridad Informática como un proceso y no como un producto que se pueda "comprar" o "instalar". Se trata, por lo tanto, de un ciclo persistente, en el que se incluyen actividades como la valoración de riesgos, prevención, detección y respuesta ante incidentes de seguridad. [1]

Actualmente, la forma de comunicarnos se basa en las facilidades que la tecnología nos ofrece. Se entiende como tecnología de las comunicaciones a los medios por los que el ser humano controla o modifica con el fin de hacer más fácil el intercambio de información. [2]

Hoy, que la comunicación se comporta como la gran herramienta del siglo, hay que manejarla con gran precaución ya que se puede utilizar con objetivos que pueden dañar a un individuo, sociedad o incluso al mundo entero. La evolución tecnológica lleva de la mano la evolución de los riesgos tecnológicos, por lo cual es necesario generar proyectos que mitiguen en gran medida estos riesgos, blindando a las instituciones de ataques externos que pongan en peligro su información y la de sus usuarios. [3]

Cuando se habla de seguridad perimetral, nos estamos refiriendo a la forma de poner una barrera o frontera lo más inexpugnable posible entre nuestra red interna e Internet. El objetivo es restringir y controlar qué datos entran a nuestra institución o salen de ella. La principal ventaja de este tipo de seguridad es que permite al administrador concentrarse en los puntos de entrada, sin olvidar la seguridad del resto de servidores internos de nuestra red, para protegerlos frente a una posible intrusión y asegurar la confidencialidad de los recursos. [4]

Este documento involucra conocer, diseñar e implementar adecuadamente conceptos, esquemas, herramientas, metodologías, estándares, tendencias y normativas de seguridad en el manejo y utilización de los recursos tecnológicos y la información, con el objetivo de garantizar la integridad, disponibilidad y confidencialidad de los recursos tecnológicos y de la información

2. Antecedentes

En nuestro país y a nivel internacional se han llevado a cabo tesis y monografías de Diseño de Infraestructura de Red de Datos y Seguridad Perimetral, las cuales han beneficiado universidades, instituciones privadas, instituciones públicas, etc. Se ve la necesidad de proteger los datos de cualquier infraestructura de red para beneficio de los usuarios como el de las mismas instituciones.

En los siguientes trabajos tomados de repositorios de Universidades de Nicaragua, Colombia y Perú, respectivamente, podemos observar cómo se ha trabajado previamente con infraestructuras de red y seguridad perimetral para dar confiabilidad a las instituciones o empresas.

Este trabajo monografico fue retomado del respositorio de la Universidad Tecnologica de Pereira, con el Titulo de (*Diseño de infraestructura de red y seguridad informatica* Sabogal Manuel y Rios Manuel.

El presente documento consta de 8 capítulos divididos de la siguiente manera En el capítulo 1 se describen los conceptos teóricos y algunos trabajos relacionados con el diseño de redes de telecomunicaciones que tiene un componente industrial y ubicaciones rurales, aspecto importante a tener en cuentan el diseño debido a la geografía del departamento del Quindío. En el capítulo 2 se detalla el análisis previo de las instalaciones de red y activos tecnológicos de la compañía Green SuperFood, con este se pretende consolidar un punto de partida y realizar un levantamiento de requerimientos en conjunto con los stakeholders del proyecto, en busca de un diseño que se ajuste al presupuesto y necesidades. En los capítulos 3, 4 y 5 se presenta el diseño del cableado estructurado de las diferentes sedes de la compañía, con ubicaciones de puntos de red, Access Point para conexión inalámbrica, diseños de radio enlaces, entre otros, acompañados por las memorias de diseño y presupuesto con APUs de cada actividad. El capítulo 6 da cuenta del análisis de seguridad realizado a partir del diseño, recomendaciones y diseño de

seguridad perimetral informática. Finalmente, en el capítulo 7 se presentan las conclusiones *de la compañía GREEN SUPER FOOD*), elaborado por loa ingenieros del desarrollo de este trabajo y se proponen posibles mejoras. [4]

En la Universidad Nacional de Ingeniería (UNI) se encontró un trabajo monográfico el cual precede al nuestro, se llama (*PROPUESTA DE SOLUCIÓN DE SEGURIDAD PERIMETRAL EN EL RECINTO PEDRO ARAUZ PALACIOS DE LA UNIVERSIDAD NACIONAL DE INGENIERÍA), elaborado por los ingenieros Noguera Danilo y Rocha Luis.*

En dicho trabajo monográfico se analizó una de las dificultades que presenta la oficina de la Dirección Network Information Center .NI en el Recinto Universitario Pedro Arauz Palacios de la Universidad Nacional de Ingeniería, en cuanto a la protección de sus servicios de red, los cuales se encuentran alojados en servidores locales. Se identificó y analizó vulnerabilidades presentes en los servidores de la oficina NIC.NI, haciendo uso de herramientas disponibles en Kali Linux y una metodología de Hacking ético de pre-ataque o reconocimiento. Este análisis permitió la construcción de una matriz de riesgo, la cual muestra qué servicios son más relevantes para el funcionamiento de las actividades académicas y administrativas del recinto, así como también, de los riesgos asociados a esos servicios. A partir de los resultados obtenidos de la identificación de vulnerabilidades, se realizó el diseño lógico, la topología lógica y física de la propuesta de implementación del sistema de seguridad perimetral. La cual consisten en una solución open-source de seguridad perimetral llamada Security Onion, basada en un sistema de monitoreo y detección de intrusiones que analiza el tráfico entrante y saliente del recinto, mostrando alertas en tiempo real, para luego ser analizadas por el personal de la oficina NIC.NI del recinto con el fin de tomar decisiones que mitiguen o prevengan esos incidentes. Finalmente se realizó demostraciones del funcionamiento de la solución en un ambiente controlado en varios escenarios de posibles amenazas. [5]

El tercer trabajo que tomamos como referencia a nivel internacional fue el elaborado por el ingeniero Rosillo Atulio, extraído de la Universidad Católica Los Ángeles de Chimbote,, con el titulo de (*Propuesta para la implementación de la infraestructura de red en la sede del gobierno regional de tumbes, 2019*).

En esta tesis descrita como “Propuesta para la implementación de la infraestructura de red en la sede del gobierno regional de TUMBES, 2019”, cuyo objetivo general, fue desarrollar una propuesta para la implementación de la infraestructura de red en la sede del Gobierno Regional de Tumbes, 2019, que mejore la calidad de sus servicios públicos, la línea de investigación utilizó un diseño no experimental y de corte transversal, porque está descrita en un momento determinado con una población definida en el marco provisional del tiempo. En relación a la población la constituyó todos los servidores públicos de la sede del Gobierno Regional, haciendo un total de 528 empleados, se aplicó un tipo de muestreo no probabilístico por conveniencia, teniendo como criterio de selección a 140 funcionarios con conocimientos en TIC en un nivel medio o alto. Los resultados nos permitieron definir la propuesta de mejora para la nueva infraestructura de red y de telecomunicaciones, ejemplo, de los datos recogidos muestran a un 60.24% considera un nivel de satisfacción en la dimensión uno, requiere la intervención para la mejora de los servicios, para él caso de la dimensión dos , responde en sus encuestas 65.92%, no está conforme con los servicios que brinda la red actual En conclusión la implementación de nuevas tecnologías con tendencias modernas y actualizadas, mejorara la calidad de los servicios públicos, pues la reposición de nuevos equipos, la dará escalabilidad e incrementara la vida útil de la nueva red. [6]

3. Justificación

En esta institución del estado de Nicaragua se almacenan datos personales y de alta confiabilidad de toda la población a nivel nacional, de igual manera se llevan a cabo procesos electorales por lo cual la hace un blanco bastante apetecible para ataques cibernéticos como los que se han dado en otras instituciones del país.

Por lo antes mencionado una buena infraestructura de red de datos y seguridad perimetral puede aportar una serie de beneficios significativos a esta institución. Estos beneficios incluyen; Conectividad confiable, comunicación efectiva, acceso remoto, seguridad de datos, gestión de tráfico, escalabilidad, recuperación ante desastres, protección de la reputación, etc.

Actualmente, la infraestructura de red de datos es un componente crítico en las instituciones, ya que permite la comunicación y el intercambio de información entre los distintos departamentos y áreas. Por lo tanto, es importante diseñar una infraestructura de red adecuada que garantice la disponibilidad, seguridad y escalabilidad de la red.

La seguridad perimetral es un aspecto fundamental en la protección de los sistemas informáticos y la información de las instituciones, ya que permite establecer barreras de protección frente a posibles ataques externos e internos. Por lo tanto, es necesario diseñar una infraestructura de red que contemple la seguridad perimetral, para garantizar la protección de los datos y la información.

Disponer de una infraestructura adecuada para mitigar los ataques informáticos requiere de cierta experiencia. Los diseños, implementaciones y adquisiciones de soluciones de seguridad informática puede ser un proceso complejo que requiere de personal experto en el área, sin embargo, si se cuenta con una línea base, una guía adaptable de lo que se debe tener en cuenta a la hora de definir criterios y necesidades para tener una solución integral de seguridad informática, hace que el proceso sea más sencillo y de fácil socialización.

En resumen, una infraestructura de red de datos y seguridad perimetral bien planificada puede mejorar significativamente la eficiencia, la seguridad, la operatividad, y garantizar la disponibilidad de los servicios que brinda la institución, lo que a su vez beneficiará a la institución y principalmente a los usuarios, así como un mejor cumplimiento de sus objetivos y responsabilidades.

4. Objetivos

4.1. General:

Diseñar una infraestructura de red de datos y seguridad perimetral para una institución del Estado de Nicaragua, considerando aspectos de escalabilidad, velocidad, confiabilidad, redundancia y almacenamiento.

4.2. Específicos:

- Identificar las condiciones tecnológicas existentes en el campo de redes de datos y seguridad perimetral de la institución.

- Realizar mediante encuentros con el encargado del área y entrevista el levantamiento de requerimientos para la red de datos y la seguridad perimetral de la institución.

- Rediseñar la topología de red existente con el fin de optimizar el flujo de datos y garantizar redundancia, confiabilidad de red, velocidad, almacenamiento y escalabilidad.

- Definir una estrategia de seguridad perimetral que resguarde la infraestructura de red de amenazas internas y externas, garantizando la integridad y la confidencialidad de los datos.

- Validar mediante simulaciones el óptimo funcionamiento del diseño de infraestructura de red de datos y seguridad perimetral, utilizando la herramienta de software GNS3.

5. Marco Teórico

5.1. Bases Teóricas

5.1.1.1. Escalabilidad

Se hace referencia a la escalabilidad de un sistema informático cuando puede recibir más usuarios, y procesar más datos y solicitudes, sin reducir la velocidad de respuesta. Es decir, cuando el sistema puede adaptarse y reaccionar sin bajar la calidad del servicio, además se puede distinguir en: [2]

Escalabilidad vertical: Significa implementar un hardware más potente. Por ejemplo, incrementar la cantidad de CPU del servidor de un sitio web o añadir un disco duro más veloz a un ordenador.

Escalabilidad horizontal: Implica añadir más nodos al sistema. Suele consistir en agregar más equipos que puedan atender las solicitudes de forma conjunta.

5.1.1.2. Almacenamiento

El almacenamiento conectado a la red (NAS) es un servidor de archivos centralizado que permite a varios usuarios almacenar y compartir archivos a través de una red TCP / IP a través de Wifi o un cable Ethernet. También se conoce comúnmente como caja NAS, unidad NAS, servidor NAS o cabezal NAS. Estos dispositivos dependen de algunos componentes para funcionar, como discos duros, protocolos de red y un sistema operativo (SO) ligero. [2]

5.1.1.3. Velocidad

El término de velocidad se refiere a la capacidad de rendimiento que tiene una conexión a internet para poder intercambiar datos entre el Internet y el dispositivo de una persona y está determinado por el ancho de banda o por la cantidad de datos que se transfiere en un tiempo determinado.

La velocidad de Internet generalmente se mide en megabits por segundo (Mbps), tanto para descarga como carga de datos. También se considera la latencia como un parámetro importante. [2]

5.1.1.4. Confiabilidad

La confiabilidad en un sistema de redes informáticas se refiere a la capacidad de dicho sistema para funcionar correctamente y de manera consistente, cumpliendo con los requisitos y expectativas establecidos, durante un período determinado. Es un atributo crucial para garantizar que una red sea estable, segura y capaz de brindar servicios de manera continua.

La confiabilidad es un objetivo fundamental en el diseño, implementación y mantenimiento de sistemas de redes informáticas, especialmente en entornos críticos como empresas, instituciones gubernamentales, servicios en línea y otros donde la interrupción del servicio puede tener consecuencias significativas. [2]

5.1.1.5. Redundancia

La redundancia de red es un proceso que añade dispositivos de red, equipos y líneas de comunicación adicionales para mantener la conectividad en caso de que la ruta principal o una de sus partes/enlaces falle. [2]

5.1.1.6. Tecnología de la Información (TI)

La tecnología de la información (TI) es un proceso que utiliza una combinación de medios y métodos de recopilación, procesamiento y transmisión de datos para obtener nueva información de calidad sobre el estado de un objeto, proceso o fenómeno. El propósito de la tecnología de la información es la producción de información para su análisis por las personas y la toma de decisiones sobre la base de la misma para realizar una acción. [2]

5.1.1.7. Seguridad Perimetral

La seguridad perimetral en una infraestructura de red de datos se refiere a las medidas y tecnologías implementadas para proteger el perímetro de la red contra amenazas externas e internas. Esencialmente, establece una barrera defensiva alrededor de la red para protegerla de accesos no autorizados, ataques cibernéticos y otros riesgos de seguridad. [2]

Aquí hay algunas tecnologías y prácticas comunes utilizadas en la seguridad perimetral:

Firewalls: Los firewalls actúan como la primera línea de defensa al monitorear y controlar el tráfico de red entrante y saliente. Pueden bloquear o permitir ciertos tipos de tráfico según las reglas de seguridad establecidas.

Filtrado de Contenido: Se utiliza para controlar y bloquear el acceso a sitios web maliciosos o inapropiados, así como para prevenir la descarga de archivos peligrosos.

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS): Estos sistemas monitorean el tráfico de red en busca de comportamientos sospechosos o ataques conocidos y responden automáticamente para detener o mitigar el impacto de los ataques.

VPN (Redes Privadas Virtuales): Las VPN permiten a los usuarios acceder a la red de manera segura desde ubicaciones remotas a través de una conexión encriptada, lo que protege la confidencialidad de los datos transmitidos.

Autenticación de Usuarios: Se utiliza para verificar la identidad de los usuarios y dispositivos que intentan acceder a la red, generalmente a través de contraseñas, certificados digitales u otros métodos de autenticación.

Cifrado de Datos: Se utiliza para proteger la confidencialidad de los datos transmitidos a través de la red mediante la encriptación de la información sensible.

Gestión de Vulnerabilidades: Consiste en identificar y corregir vulnerabilidades en la infraestructura de red para prevenir posibles ataques. Esto puede incluir parcheo de software, actualizaciones de seguridad y evaluaciones de seguridad regulares.

En resumen, la seguridad perimetral en una infraestructura de red de datos es fundamental para proteger la red contra amenazas externas e internas. Incluye una variedad de tecnologías y prácticas diseñadas para mantener la integridad, confidencialidad y disponibilidad de los datos y recursos de la red.

5.1.1.8. Objetivos de la Seguridad Perimetral

Entre los principales objetivos de la Seguridad Perimetral podríamos destacar los siguientes: [2]

- Minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad
- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos.

Para cumplir con estos objetivos una organización debe contemplar cuatro planos de actuación:

- **Técnico:** Tanto a nivel físico como a nivel lógico.
- **Legal:** Algunos países obligan por ley a que en determinados sectores se implanten una serie de medios de seguridad (sector de servicios financieros y sanitario en USA, protección de datos personales en todos los estados miembros de la UE, etc.).
- **Humano:** Sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal.
- **Organizativo:** Definición e implementación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación. [2]

5.1.1.9. Servicios de la Seguridad Perimetral

Para poder alcanzar los objetivos descritos en el apartado anterior, dentro del proceso de gestión de la seguridad informática es necesario contemplar una serie de servicios o funciones de seguridad de la información: [2]

- **Confidencialidad**

Mediante este servicio o función de seguridad se garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, éstas no podrán acceder al contenido del mensaje original. Por lo tanto, este servicio pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de backup y/o de los datos transmitidos a través de redes de comunicaciones.

- **Autenticación**

La autenticación garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje.

Asimismo, también podemos hablar de la autenticidad de un equipo que se conecta a una red o intenta acceder a un determinado servicio. En este caso, la autenticación puede ser unilateral, cuando sólo se garantiza la identidad del equipo (usuario o terminal que se intenta conectar a la red) o mutua, en el caso de que la red o el servidor también se autentica de cara al equipo, usuario o terminal que establece la conexión.

- **Integridad**

La función de integridad se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática. De este modo, es posible detectar si se ha añadido o eliminado algún dato en un mensaje o fichero almacenado, procesado o transmitido por un sistema o red informática.

- **No repudiación**

El objeto de este servicio de seguridad consiste en implementar un mecanismo probatorio que permita demostrar la autoría y envío de un determinado mensaje, de tal modo que el usuario que lo ha creado y enviado a través del sistema no pueda posteriormente negar esta circunstancia, situación que también se aplica al destinatario del envío. Éste es un aspecto de especial importancia en las transacciones comerciales y que permite proporcionar a los compradores y vendedores una seguridad jurídica que va a estar soportada por este servicio.

En un sistema informático, por lo tanto, se puede distinguir entre la no repudiación de origen y la no repudiación de destino.

- **Disponibilidad**

La disponibilidad del sistema informático también es una cuestión de especial importancia para garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar

permanentemente a disposición de los usuarios que deseen acceder a sus servicios.

Dentro de la disponibilidad también debemos considerar la recuperación del sistema frente a posibles incidentes de seguridad, así como frente a desastres naturales o intencionados (incendios, inundaciones, sabotajes...).

Debemos tener en cuenta que de nada sirven los demás servicios de seguridad si el sistema informático no se encuentra disponible para que pueda ser utilizado por sus legítimos usuarios y propietarios.

- **Autorización (control de acceso a equipos y servicios)**

Mediante el servicio de autorización se persigue controlar el acceso de los usuarios a los distintos equipos y servicios ofrecidos por el sistema informático, una vez superado el proceso de autenticación de cada usuario.

Para ello, se definen unas Listas de Control de Acceso (ACL) con la relación de usuarios y grupos de usuarios y sus distintos permisos de acceso a los recursos del sistema.

- **Auditabilidad**

El servicio de auditabilidad o trazabilidad permite registrar y monitorizar la utilización de los distintos recursos del sistema por parte de los usuarios que han sido previamente autenticados y autorizados. De este modo, es posible detectar situaciones o comportamientos anómalos por parte de los usuarios, además de llevar un control del rendimiento del sistema (tráfico cursado, información almacenada y volumen de transacciones realizadas, por citar algunas de las más importantes).

- **Reclamación de origen**

Mediante la reclamación de origen el sistema permite probar quién ha sido el creador de un determinado mensaje o documento.

- **Reclamación de propiedad**

Este servicio permite probar que un determinado documento o un contenido digital protegido por derechos de autor (canción, vídeo, libro...) pertenece a un determinado usuario u organización que ostenta la titularidad de los derechos de autor.

- **Anonimato en el uso de los servicios**

En la utilización de determinados servicios dentro de las redes y sistemas informáticos también podría resultar conveniente garantizar el anonimato de los usuarios que acceden a los recursos y consumen determinados tipos de servicios, preservando de este modo su privacidad.

Este servicio de seguridad, no obstante, podría entrar en conflicto con otros de los ya mencionados, como la autenticación o la auditoría del acceso a los recursos. Asimismo, la creciente preocupación de los gobiernos por el control e interceptación de todo tipo de comunicaciones (llamadas de teléfono, correos electrónicos.) ante el problema del terrorismo internacional está provocando la adopción de nuevas medidas para restringir el anonimato y la privacidad de los ciudadanos que utilizan estos servicios.

- **Protección a la réplica**

Mediante este servicio de seguridad se trata de impedir la realización de "ataques de repetición" (replay attacks) por parte de usuarios maliciosos, consistentes en la interceptación y posterior reenvío de mensajes para tratar de engañar al sistema y provocar operaciones no deseadas, como podría ser el caso de realizar varias veces una misma transacción bancaria

Para ello. en este servicio se suele recurrir a la utilización de un número de secuencia o sello temporal en todos los mensajes y documentos que necesiten ser protegidos dentro del sistema, de forma que se puedan detectar y eliminar posibles repeticiones de mensajes que ya hayan sido recibidos por el destinatario.

- **Confirmación de la prestación de un servicio o la realización de una transacción**

Este servicio de seguridad permite confirmar la realización de una operación o transacción, reflejando los usuarios o entidades que han intervenido en ésta.

- **Referencia temporal (certificación de fechas)**

Mediante este servicio de seguridad se consigue demostrar el instante concreto en que se ha enviado un mensaje o se ha realizado una determinada operación (utilizando generalmente una referencia UTC-Universal Time Clock-). Para ello, se suele recurrir al sellado temporal del mensaje o documento en cuestión.

5.1.1.10. Tipos de Amenazas

Básicamente, podemos agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y; Actos maliciosos o malintencionados; algunas de estas amenazas son: [2]

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

A continuación, se presenta la descripción de algunas de las principales amenazas:

Spywre (Programas espías): Código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador (tendencias de navegación), para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercadeo, o para robar información personal (p.ej. números de tarjetas de crédito). Hay iniciativas de utilizarlos para controlar el uso de software pirata.

Según algunas estadísticas, cerca del 91% de los computadores tienen spyware instalado, y de acuerdo a un reporte de la firma EarthLink", en una revisión de cerca de 1 millón de computadores en Internet, el promedio de programas "spyware" en cada uno era de 28.

Troyanos, virus y gusanos: Son programas de código malicioso, que de diferentes maneras se alojan en los computadores con el propósito de permitir el acceso no autorizado a un atacante, o permitir el control de forma remota de los sistemas. El virus, adicionalmente, tiene como objetivo principal ser destructivo, dañando la información de la máquina, o generando el consumo de recursos de manera incontrolada para bloquear o negar servicios.

El vector de propagación de estos códigos es, casi siempre, otro programa o archivo (un programa ejecutable, imagen, video, música, reproducciones flash, etc.); de otra parte, los virus, se replican ellos mismos una vez instalados en el sistema.

Las estadísticas indican que mensualmente se generan cientos de estos programas, cuyo principal objetivo es robo financiero, poniendo en riesgo la información confidencial y el dinero de las personas y de las organizaciones, más que la destrucción de archivos.

La última tendencia en clases de virus se denomina cripto-virus, el cual, una vez insta-lado, cifra la información contenida en el disco del equipo, o algunos archivos contenidos en éste, y posteriormente se solicita una cantidad de dinero para que sus autores entreguen las claves para recuperar el contenido de los archivos cifrados (secuestro express de la información).

Phishing: Es un ataque del tipo ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros, aprovechando la confianza que éste tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios en algunos casos con pobres medidas de seguridad.

Actualmente, los ataques de phishing son bastante sofisticados, utilizando mensajes de correo electrónico y falsos sitios Web, que suplantan perfectamente a los sitios originales.

Spam: Recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos. Se han presentado casos en los que los envíos se hacen a sistemas de telefonía celular - mensajes de texto. o a sistemas de faxes. Para el año 2006, se tenía calculado que entre el 60 y el 70% de los correos electrónicos eran. "spam", con contenidos comerciales o de material pornográfico. Según la compañía Symantec, el tipo de spam más común en el año 2006 fue el relacionado con servicios financieros, con cerca del 30% de todo el spam detectado.

Botnets (Redes de robots): Son máquinas infectadas y controladas remotamente, que se comportan como "zombis", quedando incorporadas a redes distribuidas de computadores llamados robot, los cuales envían de forma masiva mensajes de correo "spam" o código malicioso, con el objetivo de atacar otros sistemas; se han detectado redes de más de 200.000 nodos enlazados y más de 10.000 formas diferentes de patrones de "bots".

Las organizaciones deberían revisar los computadores de sus redes de datos para detectar síntomas de infecciones relacionadas con este patrón, para evitar ser la fuente de ataques hacia otras redes o sistemas. También se requiere de la colaboración y aporte permanente de los usuarios finales y de los proveedores de acceso a Internet y prestadores de servicios como los "café Internet".

5.1.2. Infraestructura de Red

5.1.2.1. Definición Infraestructura de Red

Una Infraestructura de Red de Datos se refiere a la estructura física y lógica que permite la comunicación de datos entre dispositivos y sistemas dentro de una organización o red. Consiste en todos los componentes necesarios para facilitar la transferencia de información, incluyendo hardware, software, cables, protocolos de comunicación y dispositivos de red. [4]

Aquí hay una descripción más detallada de los componentes típicos de una infraestructura de red de datos:

Dispositivos de Red: Incluyen Router, switches, firewalls, puntos de acceso inalámbrico, balanceadores de carga y otros dispositivos que permiten la conexión y el enrutamiento de datos en la red.

Medios de Transmisión: Tales como cables de red (cobre, fibra óptica) y tecnologías inalámbricas (Wi-Fi, Bluetooth) que facilitan la transferencia de datos entre dispositivos.

Protocolos de Comunicación: Establecen las reglas y estándares para la comunicación de datos entre dispositivos en la red. Ejemplos incluyen TCP/IP, Ethernet, SNMP, y otros.

Servidores: Proveen servicios y recursos de red, como almacenamiento de archivos, aplicaciones, servicios de directorio, correo electrónico, y otros servicios que requieren acceso a la red.

Segmentación de Red: División de la red en segmentos más pequeños para mejorar el rendimiento, la seguridad y la administración. Esto puede lograrse mediante VLANs (Virtual LANs), subredes, y otros métodos de segmentación.

Seguridad: Incluye firewalls, sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), cifrado de datos, autenticación y otras medidas para proteger la red contra amenazas y accesos no autorizados.

Administración de Red: Herramientas y software utilizados para monitorear, administrar y mantener la infraestructura de red, incluyendo la configuración de dispositivos, la supervisión del rendimiento y la solución de problemas.

En resumen, una infraestructura de red de datos es el conjunto de componentes físicos y lógicos que permiten la comunicación y transferencia de datos dentro de una organización o red. Es fundamental para el funcionamiento eficiente y seguro de cualquier sistema de tecnología de la información y comunicación.

5.1.2.2. Hardware de Red

En la actualidad hay dos tipos de tecnologías que definen un concepto de enlace los enlaces de difusión (broabcast) y los enlaces punto a punto: [5]

5.1.2.2.1. Enlaces Punto a Punto Unicasting

Permite la conexión de dos equipos de manera independiente, y los enlaces van desde el emisor y el receptor los paquetes pequeños de datos viajan de manera de red por mensajería punto a punto., este tipo de comunicación donde hay un origen y destino se le conoce por unicasting (enlace punto a punto). [5]

5.1.2.2.2. Broadcasting

Llamada también red de difusión, en este caso todas las computadoras comparten un mismo canal ce trasmisión, los datos que se emiten llegan a todos los equipos de la red la diferencia es que cada mensaje va acompañado de un campo que se llama dirección y en este campo especifica cual es la dirección a la cual debe llegar el paquete de datos, las computadoras reciben el mensaje y verifican la dirección si es el destino lo reciben y lo procesan, si no es para la computadora ignoran el mensaje.

Podemos poner de ejemplo una red WIFI, en este caso la difusión del mensaje es través de una zona de cobertura y obedece a una canal WIFI. En comparación con la tecnología unicasting, cuando los medios de trasmisión también suelen enviar paquetes de datos a todas las computadoras con dato especial que se llama código de direccionamiento, cuando se envía todas las computadoras lo reciben y los procesan a esto se le llama broadcasting. [5]

5.1.2.2.3. Redes de área personal. (PAN)

Por su desenvolvimiento se les denomina PAN, son limitadas, las comunicaciones los de persona a persona, si tomamos ce ejemplo podría ser una computadora que tenga comunicación inalámbrica y se conecta con sus periféricos (impresora, mouse, keyboard, pantalla), necesariamente necesitan un cable para poderse comunicar. El bluetooth es una señal inalámbrica que conecta a dos dispositivos, convirtiéndose en una herramienta de mucha utilidad para las personas.

Las redes bluetooth usan el prototipo maestro – esclavo, en este caso dispositivo maestro le comunica al dispositivo esclavo que debe realizar, esta tecnología se usa para trasferir archivos de imágenes, datos, audio, video, etc. [5]

5.1.2.2.4. Redes de área local (LAN)

Son sistemas interconectados de uso local que se desenvuelven en un área específica dentro de una estructura física como domicilio, oficina, o fabrica, se usan para interconectar equipos informáticos personales, como computadoras impresoras, el propósito es compartir información, a este tipo de equipamiento de comunicaciones se le llama también redes empresariales.

Son las más usadas en el mercado empresarial o de Gobierno, las redes LAN complican su instalación cuando la infraestructura en que se quiere instalar no es la adecuada, en estos casos se crean redes inalámbricas, que acceden a través de un modem o punto de acceso (AP), así la computadora a se conecta con el computador b, pero a través de un AP. [5]

5.1.2.2.5. Redes de área Amplia (WAN)

Son redes de computadoras en un espectro mucho más amplio, por ejemplo, una red de alcance continental, las redes de computadoras de estas características, se interconectan a través de un host, que se encarga de trasportan la información a través de señales eléctricas desde una subred a otra subred. Casi en la mayor parte de redes de computadoras WAN, utiliza dos dispositivos diferentes, la línea de trasmisión y elementos de conmutación, la primera trasporta un paquete de datos entre una y otra computadora. [5]

5.2. Protocolos de Red

5.2.1. MLAG (Multi-Chassis Link Aggregation):

MLAG es un protocolo de red que permite a múltiples switches trabajar juntos como un solo switch virtual, ofreciendo redundancia y aumentando el ancho de banda de la red. Permite la creación de un enlace de agregación de enlaces entre dispositivos de red físicamente separados, lo que proporciona tolerancia a fallos y mejora el rendimiento de la red. [7]

5.2.2. LACP (Link Aggregation Control Protocol):

LACP es un protocolo estándar de la industria que se utiliza para la agregación de enlaces, también conocida como trunking o bonding. Permite combinar múltiples enlaces físicos entre dos dispositivos de red en un solo enlace lógico, aumentando así el ancho de banda y proporcionando redundancia. LACP coordina la formación y el mantenimiento de los enlaces agregados, lo que garantiza una distribución equitativa del tráfico y una recuperación rápida en caso de fallo de un enlace. [7]

5.2.3. OSPF (Open Shortest Path First):

OSPF es un protocolo de enrutamiento de estado de enlace que se utiliza en redes IP para calcular la mejor ruta entre routers, basándose en el estado de los enlaces y otros parámetros de la red. OSPF utiliza algoritmos para calcular las rutas más cortas y converger rápidamente en caso de cambios en la topología de la red. Es un protocolo dinámico y escalable, adecuado para redes grandes y complejas. [7]

5.2.4. DHCP (Dynamic Host Configuration Protocol):

DHCP es un protocolo de red que se utiliza para asignar de manera dinámica direcciones IP y otros parámetros de configuración de red a dispositivos en una red IP. Esto simplifica la administración de direcciones IP al automatizar el proceso de asignación, eliminando la necesidad de configurar manualmente cada dispositivo con una dirección IP única. [7]

5.2.5. VRRP (Virtual Router Redundancy Protocol):

VRRP es un protocolo de redundancia de enrutadores que se utiliza para proporcionar alta disponibilidad en redes IP. Permite que varios routers trabajen juntos como un grupo, con uno de ellos actuando como el enrutador maestro y los demás enrutadores de respaldo. Si el enrutador maestro falla, uno de los enrutadores de respaldo se convierte automáticamente en el nuevo enrutador maestro, garantizando la continuidad del servicio sin interrupciones. [7]

5.2.6. VPN (Virtual Private Network o Red Privada Virtual):

VPN (Virtual Private Network o Red Privada Virtual) es una tecnología que permite crear una red privada segura sobre una red pública como Internet. Utiliza técnicas de cifrado y protocolos de seguridad para asegurar la confidencialidad, integridad y autenticación de los datos transmitidos entre dispositivos conectados a través de la red pública. [7]

En una VPN, los datos se encapsulan y se cifran antes de ser transmitidos a través de la red pública. Esto permite a los usuarios acceder de forma segura a recursos de la red privada, como archivos, aplicaciones y servicios, desde ubicaciones remotas o dispositivos móviles.

Hay varios tipos de VPN, incluyendo:

- VPN de Acceso Remoto: Permite a los usuarios individuales acceder a la red privada de forma segura desde ubicaciones remotas a través de Internet. Los empleados pueden conectarse a la red corporativa desde sus hogares o mientras viajan utilizando software cliente VPN.

- VPN de Sitio a Sitio: Conecta dos o más redes privadas geográficamente dispersas a través de Internet, creando una red virtual segura entre ellas. Es útil para conectar sucursales de una empresa o para establecer conexiones entre socios comerciales.

- VPN de Acceso por Capas (Layer 2 VPN y Layer 3 VPN): Proporciona conectividad de red a nivel de capa 2 o capa 3 entre diferentes ubicaciones o dispositivos. Puede utilizarse para interconectar redes LAN remotas o para ofrecer servicios de conectividad a proveedores de servicios.

- VPN SSL/TLS: Utiliza el protocolo SSL/TLS para establecer una conexión segura a través del navegador web. Es comúnmente utilizado para proporcionar acceso remoto seguro a aplicaciones web y servicios en la nube.

5.2.7. IPsec (Protocolo de Seguridad de la Capa de Internet)

IPsec (Protocolo de Seguridad de la Capa de Internet) es un conjunto de protocolos y estándares criptográficos utilizados para asegurar las comunicaciones a través de redes IP. IPsec proporciona servicios de seguridad a nivel de red, incluyendo autenticación, integridad de datos y confidencialidad. [7]

Los componentes principales de IPsec son los siguientes:

- Autenticación de Encabezado (AH, Authentication Header): Proporciona autenticación e integridad de los datos transmitidos. El encabezado AH calcula un hash de los datos del paquete y lo incluye en el encabezado para que el receptor pueda verificar la integridad de los datos.

- Protocolo de Carga Útil de Seguridad (ESP, Encapsulating Security Payload): Proporciona autenticación, integridad y confidencialidad de los datos transmitidos. ESP cifra el contenido del paquete y añade una cabecera de seguridad para autenticación e integridad.

- Asociación de Seguridad (SA, Security Association): Es un conjunto de parámetros que definen los atributos de seguridad para una conexión específica, como los algoritmos de cifrado y autenticación utilizados, las claves y la dirección IP del destinatario.

IPsec se utiliza comúnmente para establecer conexiones VPN (Redes Privadas Virtuales) seguras entre redes o dispositivos remotos a través de Internet. También se puede utilizar para proteger el tráfico entre dispositivos en la misma red local.

5.3. Software GNS3

Para poder implementar el ***Diseño de Infraestructura de Red de Datos y Seguridad Perimetral Para una Institución Del Estado de Nicaragua,*** se hará uso de la herramienta GNS3, que permite emular dispositivos de redes a partir de IOS Cisco y por ende topologías completas sin la implementación de hardware que suele ser complicado y/o costoso de obtener. De esta forma se logran resultados y pruebas similares a los que se obtendrían en una topología de red real. GNS3 es utilizado por cientos de miles de ingenieros de redes en todo el mundo para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de pocos dispositivos a topologías grandes con muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube.

5.3.1. Sobre El Programa GNS3

GNS3 es un software gratuito de código abierto que puede descargarse libremente. Ha existido por más de 10 años y se desarrolla activamente por una comunidad creciente de más de 800,000 miembros. Originalmente solo emulaba dispositivos Cisco, pero ahora ha evolucionado y admite muchos dispositivos de múltiples proveedores de redes. [8]

GNS3 admite dispositivos emulados y simulados, términos que no significan los mismo, como se explica a continuación:

- **Emulación:** GNS3 imita o emula el hardware de un dispositivo y ejecuta imágenes reales en el dispositivo virtual. Por ejemplo, puede copiar el Cisco IOS de un Router Cisco real y ejecutarlo en un Router Cisco virtual en GNS3.
- **Simulación:** GNS3 simula las características y funcionalidades de un dispositivo como un Switch Cisco. No ejecuta el sistema operativo real, sino un dispositivo que simula el funcionamiento de un Switch L2 o L3 real el cual viene incorporado en GNS3.

5.3.2. Características de GNS3

GNS3 consta de dos componentes de software:

GNS3 ALL IN ONE (TODO EN UNO). Es el software cliente de GNS3 que se instala en la PC. Es la interfaz gráfica de usuario (GUI) donde se crean y emulan/simulan las topologías de red. Es un programa que requiere de otros programas, pero estos ya vienen integrados en un paquete listos para ser instalados en una sola ocasión. [8]

MAQUINA VIRTUAL (VM) GNS3. Cuando se crean topologías en GNS3 los dispositivos creados deben estar alojados y ejecutados en un servidor. Las opciones para este servidor son:

- **Servidor GNS3 local:** Se ejecuta localmente en el mismo PC donde se instaló el software All-in-One GNS3.

- **Máquina Virtual GNS3 local:** Se ejecuta localmente en la PC mediante software de virtualización como VMware Workstation, VirtualBox o Hyper-V.

- **Máquina Virtual GNS3 remota:** Haciendo uso de un servidor mediante VMware ESXi o incluso en la nube.

6. Análisis y presentación de resultados

6.1. Identificación de las condiciones tecnológicas existentes en el área de redes de datos y seguridad perimetral de la institución.

El primer capítulo de esta tesis sienta las bases para la investigación, centrándose en la identificación de las condiciones tecnológicas existentes en el área de redes de datos y seguridad perimetral de esta institución estatal en Nicaragua.

Antes de realizar cualquier propuesta de mejora en una red es necesario determinar los equipos ya existentes, así como la topología de la red esto permitirá identificar áreas de mejora y oportunidades de fortalecimiento en su infraestructura tecnológica.

6.1.1. Recopilación de Información

Mediante visitas previamente planificadas se logró visitar el lugar y tener observaciones directas en el área de redes de dicha institución del estado, también se lograron coordinar encuentros puntuales con el encargado de la misma, conociendo los equipos ya utilizados y la distribución de la red en la institución.

6.1.2. Identificación de los equipos

De igual forma gracias a las visitas realizadas a la institución y con la ayuda de la información suministrada por el encargado del área de redes, pudimos obtener el dato específico sobre los equipos utilizados actualmente en el área de redes de dicha institución.

6.1.2.1. Router Cisco 2900 series

Los enrutadores de servicios integrados Cisco ® serie 2900 se basan en 25 años de innovación y liderazgo de productos de Cisco. Las nuevas plataformas están diseñadas para permitir la siguiente fase de evolución de las sucursales, brindando colaboración multimedia enriquecida y virtualización a la sucursal mientras maximizan el ahorro de costos operativos. Las plataformas de enrutadores de servicios integrados Generación 2 están habilitadas para el futuro con CPU multinúcleo, soporte para alta DSP (procesadores de señal digital) de capacidad para futuras capacidades de video mejoradas, módulos de servicio de alta potencia con disponibilidad mejorada, conmutación Gigabit Ethernet con POE mejorado y nuevas capacidades de control y monitoreo de energía al tiempo que se mejora el rendimiento general del sistema. Además, un nuevo Cisco IOS ®La imagen universal de software y el módulo Services Ready Engine le permiten desacoplar la implementación de hardware y software, proporcionando una base tecnológica flexible que puede adaptarse rápidamente a los requisitos de red en evolución. En general, la serie Cisco 2900 ofrece un ahorro incomparable en el costo total de propiedad y agilidad de la red a través de la integración inteligente de seguridad, comunicaciones unificadas, servicios inalámbricos y aplicaciones líderes en el mercado.

Cisco 2900 Series Integrated Services Routers (ISR) están diseñados para satisfacer las demandas de empresas de tamaño medio y adecuarse a novedosos servicios en la nube.

Incluye 32/ puertos Ehernet integrados 10/100/1000 (conectividad RJ-45), una ranura para módulo de servicio de aplicación, 4 para tarjetas interfaz WAN de alta velocidad mejorada EHWIC, 3 ranuras para DSP y otra como módulo de servicio interno para servicios de aplicaciones. Distribución de energía PoE.

Con Módulo DSP optimizado para voz y vídeo, servicios de navegador VoiceXML certificados y soporte para correo de voz Cisco Unity Express, Cisco Communications Manager Express y Survivable Remote Site Telephony.

6.1.2.2. Switch Cisco Catalyst 2960

Los conmutadores Cisco ® Catalyst ® series 2960-S y 2960 son los conmutadores de borde de capa 2 líderes y brindan excelencia operativa mejorada, operaciones comerciales altamente seguras, sostenibilidad mejorada y una experiencia de espacio de trabajo mejorada. Son conmutadores de acceso de configuración fija diseñados para redes empresariales, medianas y de sucursales de nivel básico.

Los conmutadores Cisco Catalyst serie 2960-S con software LAN Lite tienen las siguientes capacidades:

- 24 y 48 puertos de conectividad de escritorio Gigabit Ethernet (GbE) 10/100/1000
- Enlace ascendente conectable de factor de forma pequeño SFP de 1 GbE
- Interfaz de almacenamiento USB para copia de seguridad, distribución y operaciones simplificadas de archivos
- Solución de problemas mejorada para la resolución de problemas, incluida la conectividad de enlaces y el diagnóstico de cables.
- Gestión de dirección IP única para hasta 16 conmutadores
- Una amplia gama de características de software para brindar facilidad de operación, operaciones comerciales seguras, sustentabilidad y experiencia de networking sin fronteras.
- Garantía limitada de por vida para el hardware, que incluye reemplazo al siguiente día hábil con servicio y soporte por 90 días

6.1.2.3. Switch TL-SG1024

El Switch TL-SG1024 Gigabit Ethernet le ofrece una solución de alto rendimiento, bajo costo, fácil de usar, sin fisuras y estándar para mejorar su red antigua a una red a 1000Mbps. Todos los puertos soportan auto MDI / MDIX por lo que no hay necesidad de preocuparse por el tipo de cable, sólo tiene que enchufar y listo. Por otra parte, con la innovadora tecnología de eficiencia energética, el TL-SG1024 ahorra en el consumo energético siendo una solución ecológica para su red de negocios.

Este Switch Gigabit TL-SG1024 de nueva generación cuenta con las últimas e innovadoras tecnologías de eficiencia energética que pueden ampliar en gran medida su capacidad de red con mucho menos consumo. Éste ajusta automáticamente el consumo de energía de acuerdo con el estado del enlace para limitar la huella de carbono de su red. También cumple con la DE RoHS de la UE, que prohíbe el uso de ciertos materiales peligrosos. Además, la mayoría del material de embalaje puede ser reciclado.

Todos sus 24 puertos son Gigabit RJ-45 que proporcionan una gran transferencia de archivos y también son compatible con dispositivos Ethernet de 10Mbps y 100Mbps. Con su arquitectura de no bloqueo, el TL-SG1024 redirige y filtra paquetes a la máxima velocidad del cable para un rendimiento máximo. Con su paquete Jumbo 10KB, el rendimiento de grandes transferencias de archivos se mejora considerablemente. El control de flujo IEEE 802.3x para el modo Full Duplex y la contrapresión para el modo Half Duplex alivian la congestión del tráfico y hacen el trabajo del TL-SG1024 fiable. Es una opción perfecta para actualizar su red a Gigabit al tiempo que protege correctamente su inversión anterior.

6.1.2.4. Switch Cisco Catalyst 3560 Poe-8

El Cisco Catalyst® – La serie 3560 es una línea de conmutadores de clase empresarial de configuración fija que incluyen funcionalidad Power over Ethernet (PoE) preestándar de Cisco IEEE 802.3af y en configuraciones Fast Ethernet y Gigabit Ethernet. Cisco Catalyst 3560 es un conmutador de capa de acceso ideal para acceso LAN de pequeñas empresas o entornos de sucursales, que combina configuraciones 10/100/1000 y PoE para una máxima productividad y protección de la inversión, al tiempo que permite la implementación de nuevas aplicaciones como telefonía IP, conectividad inalámbrica acceso, videovigilancia, sistemas de gestión de edificios y quioscos de vídeo remotos. Los clientes pueden implementar servicios inteligentes en toda la red, como calidad de servicio (QoS) avanzada, limitación de velocidad, listas de control de acceso (ACL), gestión de multidifusión y enrutamiento IP de alto rendimiento, manteniendo al mismo tiempo la simplicidad de la conmutación LAN tradicional.

Características principales

- Memoria interna: 128 MB
- Dimensiones (Ancho x Profundidad x Altura): 270 x 230 x 44 mm
- Peso: 2.3 kg
- Certificación: CE, FCC Class A certified, UL, TUV GS, cUL, EN 60950, EN55022, NOM, VCCI Class A ITE, IEC 60950, EN55024, UL 60950 Third Edition, CB, AS/NZ 3548 Class A, FCC Part 15, CSA C22.2 No. 60950-00, MIC
- Software incluido: Cisco IOS IP Base

6.1.3. Diagrama de la Infraestructura de red

El siguiente diagrama fue proveído por el encargado del área de Redes de la institución, en el que se muestran los equipos activos en la infraestructura de red de la institución.

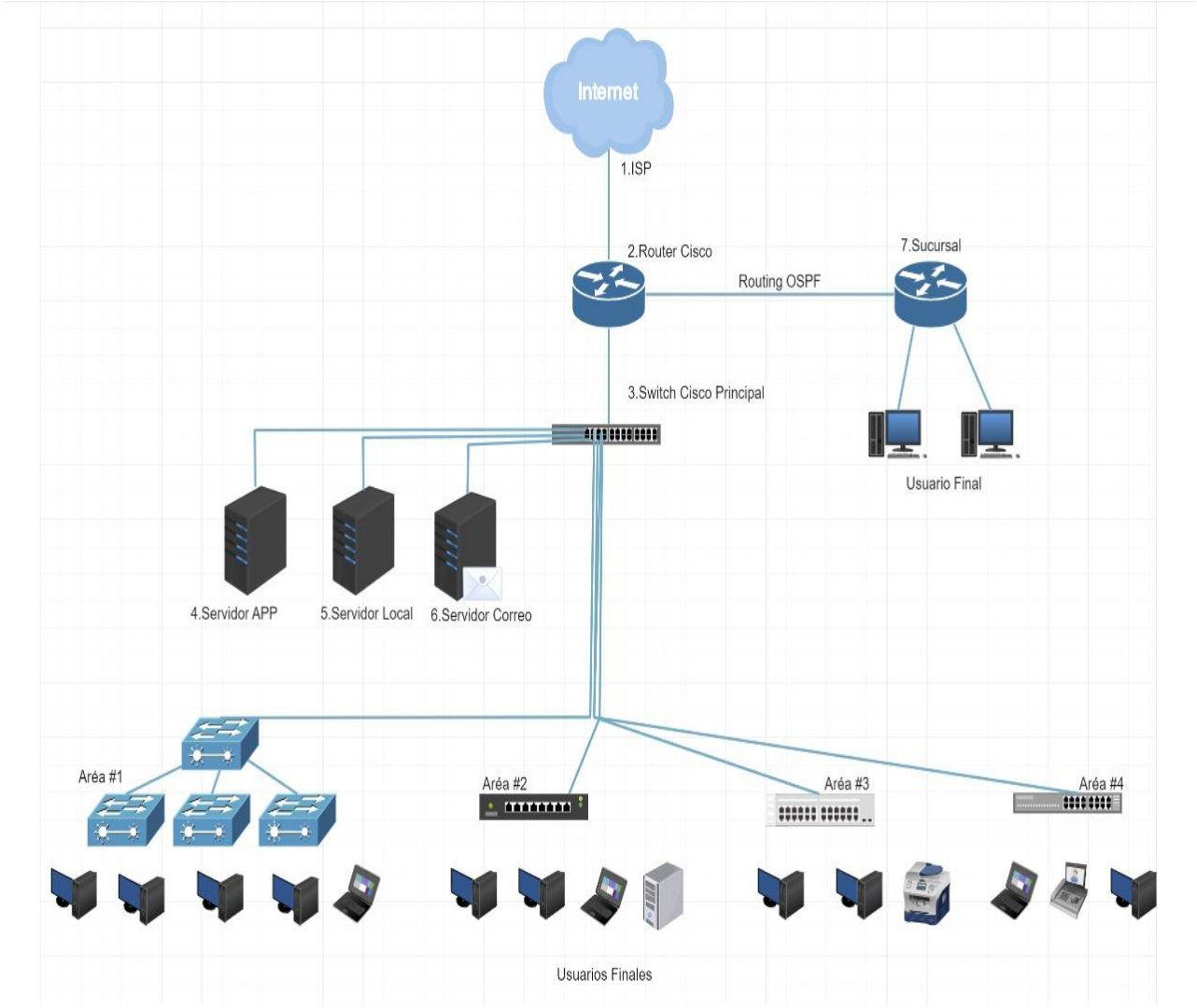


*Fig. 1 / **Topología Existente en la institución del estado de Nicaragua… (Fuente Propia)***

6.2. Levantamiento de los requerimientos para la red de datos y la seguridad perimetral de la institución.

El levantamiento de requerimientos es un proceso crucial en el diseño y la implementación de una red de datos y un sistema de seguridad perimetral efectivos. Este proceso implica identificar y documentar las necesidades y objetivos de la institución en términos de flujo de datos, redundancia, confiabilidad, velocidad, almacenamiento y escalabilidad de la red.

En el contexto de la institución en estudio, se han identificado problemas significativos relacionados con estos aspectos de la infraestructura de red. Por lo tanto, es fundamental realizar un levantamiento exhaustivo de requerimientos para abordar estos desafíos y garantizar que la nueva red y sistema de seguridad perimetral cumplan con las expectativas y necesidades de la organización.

Para ello, se empleará una entrevista detallada de levantamiento de requerimientos, cuyo objetivo es capturar de manera exhaustiva los aspectos críticos que guiarán el proceso de rediseño y fortalecimiento de la infraestructura de red y seguridad perimetral.

Dicha entrevista puede ser encontrada en Anexos entre las páginas 70 - 74

Resultados de la Encuesta de Levantamiento de Requerimientos

Tras analizar detenidamente los resultados de la encuesta de levantamiento de requerimientos para el rediseño de la infraestructura de red de datos y seguridad perimetral de nuestra institución del estado, se han identificado varias conclusiones importantes:

Requerimientos de Firewall: Los participantes muestran una preferencia por funcionalidades avanzadas como VPN, el control de acceso basado en políticas (PAC) y la detección y prevención de intrusiones (IDS/IPS). Además, se observa una diversidad en las preferencias de fabricantes y modelos de firewall, lo que sugiere la necesidad de una evaluación exhaustiva para seleccionar la mejor opción.

Requerimientos de Equipos: Se identifica la necesidad de diversos tipos de equipos adicionales, incluyendo switches de capa de acceso, switches de capa de distribución y Router de borde. Los participantes expresan interés en equipos de diferentes fabricantes, lo que destaca la importancia de la interoperabilidad y la compatibilidad en el proceso de selección de equipos.

Requerimientos de Protocolos: Los protocolos de enrutamiento como OSPF, MLAG, VRRP, son considerados esenciales para la nueva infraestructura de red, mientras que Ipsec, SSL/TLS y IKE son prioritarios para proteger la red perimetral. Estos resultados subrayan la importancia de implementar protocolos de enrutamiento robustos y medidas de seguridad sólidas para garantizar un funcionamiento seguro y eficiente de la red.

En resumen, los resultados de la encuesta proporcionan una visión detallada de los requerimientos específicos y las preferencias de los usuarios para el rediseño de la infraestructura de red de datos y seguridad perimetral de nuestra institución del estado. Estos hallazgos servirán como guía para el proceso de toma de decisiones y la planificación de la implementación, con el objetivo de mejorar la eficiencia, la seguridad y la confiabilidad de nuestra infraestructura de red.

6.3. Rediseño de la topología de red existente

En este capítulo, nos enfocaremos en el rediseño de la topología de red existente con el objetivo primordial de optimizar el flujo de datos y asegurar la redundancia, confiabilidad, velocidad, almacenamiento y escalabilidad de la red.

El rediseño de la topología de red existente se vuelve esencial a medida que las organizaciones enfrentan nuevas demandas y desafíos tecnológicos, como el aumento en el volumen de datos, la necesidad de mayor velocidad y confiabilidad, y la creciente demanda de almacenamiento y escalabilidad. Además, en un entorno en constante evolución, es imperativo que la infraestructura de red pueda adaptarse y crecer de manera flexible para satisfacer las necesidades cambiantes de la institución y sus usuarios.

6.3.1. Análisis de la Topología de Red Actual

El primer paso en el proceso de rediseño de la topología de red consiste en realizar un análisis exhaustivo de la topología de red actual. Para ello, se llevó a cabo una evaluación detallada de la infraestructura de red existente, centrándose en los siguientes aspectos:

- **Evaluación del Rendimiento:** Se examinaron los patrones de tráfico de red, la latencia y el tiempo de respuesta para identificar posibles cuellos de botella y áreas de congestión.

- **Análisis de Redundancia:** Se evaluaron las rutas de comunicación existentes y la presencia de mecanismos de redundancia para determinar la capacidad de recuperación de la red frente a fallos de hardware o enlaces.

- **Disponibilidad y Fiabilidad:** Se revisaron los tiempos de actividad históricos y los registros de incidencias para evaluar la fiabilidad y la disponibilidad de la red en su estado actual.

- **Velocidad y Almacenamiento:** Se analizó la velocidad de transferencia de datos en diferentes segmentos de la red y la capacidad de almacenamiento disponible en los dispositivos de almacenamiento conectados a la red.

6.3.2. Objetivos del Rediseño

Basándonos en los hallazgos del análisis de la topología de red actual, se establecieron los siguientes objetivos para el rediseño de la topología de red:

- **Optimización del Rendimiento:** Mejorar la eficiencia del flujo de datos mediante la eliminación de cuellos de botella y la optimización de las rutas de comunicación.

- **Aumento de la Redundancia:** Incrementar la resiliencia de la red mediante la implementación de mecanismos de redundancia y failover para garantizar la disponibilidad continua de servicios.

- **Mejora de la Disponibilidad y Fiabilidad:** Aumentar el tiempo de actividad y la fiabilidad de la red mediante la implementación de prácticas de alta disponibilidad y la mejora de los procesos de mantenimiento y gestión.

- **Incremento de la Velocidad y el Almacenamiento:** Mejorar la velocidad de transferencia de datos y la capacidad de almacenamiento para satisfacer las demandas de tráfico de datos en constante crecimiento.

- **Aseguramiento de la Escalabilidad:** Diseñar una topología de red que pueda escalar fácilmente para adaptarse al crecimiento futuro de la organización y las necesidades de la red.

6.3.3. Diseño de la Nueva Topología de Red

Con base en los objetivos establecidos, se propuso un diseño de topología de red renovado que cumpla con los requisitos de optimización del flujo de datos y garantice redundancia, confiabilidad, velocidad, almacenamiento y escalabilidad. El diseño incluye los siguientes elementos clave:

- **Selección de Modelo de Topología:** Se optó por una topología de red en estrella modificada que combine los beneficios de la centralización y la distribución, facilitando la gestión y la escalabilidad.

- **Implementación de Dispositivos de Red**: Se planificó la disposición y conexión de dispositivos de red, incluidos enrutadores, conmutadores, firewalls y servidores, para optimizar el rendimiento y la redundancia.

- **Configuración de Rutas y Protocolos:** Se definió la configuración de rutas y protocolos de enrutamiento para asegurar una comunicación eficiente y confiable entre los dispositivos de red.

- **Integración de Mecanismos de Redundancia**: Se implementaron tecnologías de redundancia, como enlaces troncales redundantes, protocolos de enrutamiento dinámico y clústeres de alta disponibilidad, para garantizar la resiliencia de la red

De esta manera quedaría la nueva topología de Red de esta institución del estado

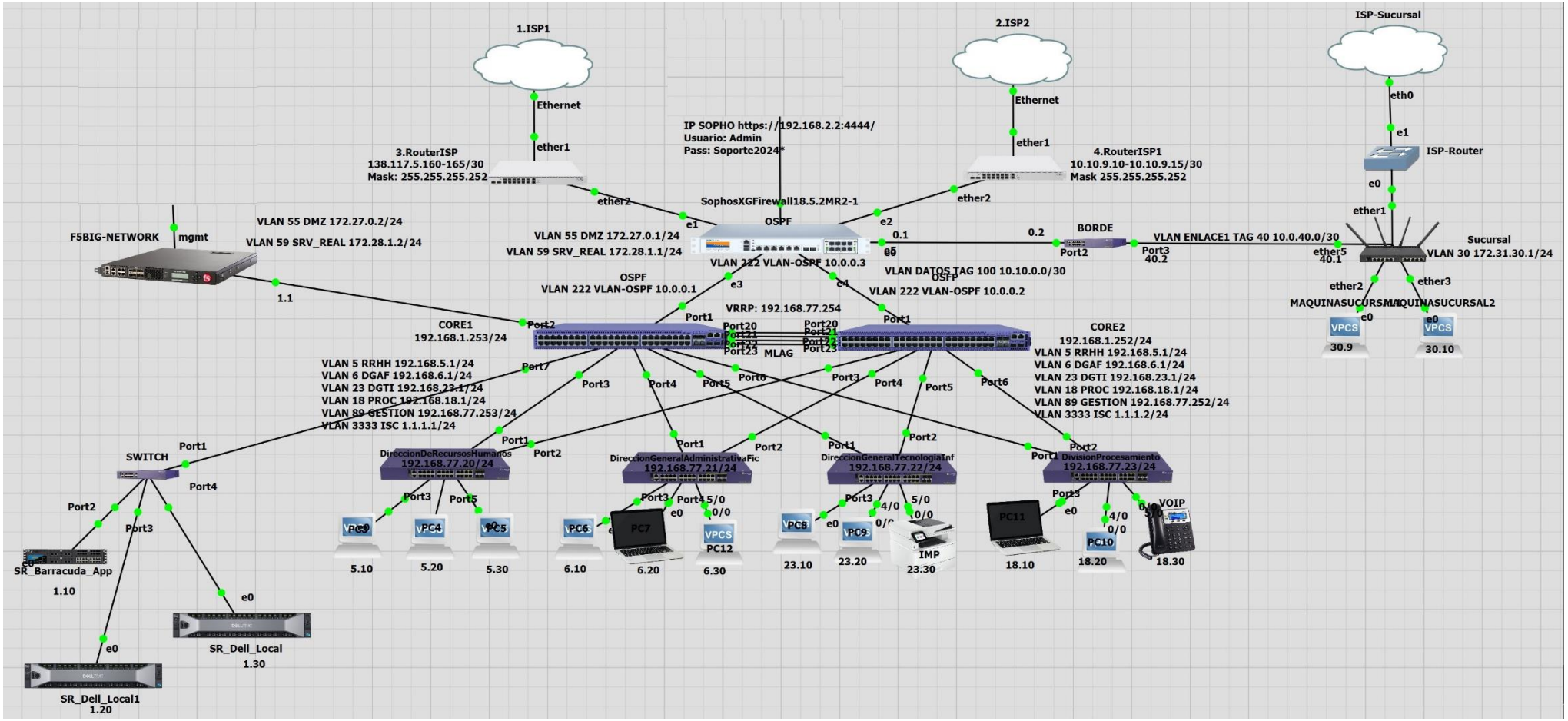


*Fig. 2 / **Nueva Topología de Red para la institución del estado de Nicaragua… (Fuente Propia)***

6.3.4. Equipos a Utilizar

En esta nueva topología de red dado los requerimientos solicitados por la institución, se determinó utilizar los siguientes equipos:

6.3.4.1. Mikrotik CRS326-24G-2S+RM

El MikroTik CRS326-24G-2S+RM es un switch de capa 3 compacto y de alto rendimiento fabricado por MikroTik, una empresa conocida por sus soluciones de red asequibles y versátiles. Aquí tienes información sobre las características clave de este equipo:

Puertos y conectividad: El CRS326-24G-2S+RM cuenta con 24 puertos Gigabit Ethernet (10/100/1000 Mbps) que proporcionan conectividad de red para dispositivos cableados, como computadoras, impresoras, teléfonos IP y otros dispositivos de red. Además, dispone de 2 puertos SFP+ (10 Gigabit) para conexiones de fibra óptica de alta velocidad, que permiten la conexión a otros switches, dispositivos de almacenamiento o redes de área amplia (WAN).

Capacidades de conmutación: Este switch ofrece capacidades de conmutación de capa 2 y capa 3, lo que le permite enrutar el tráfico entre diferentes redes VLAN y subredes IP. Esto es útil para segmentar y gestionar el tráfico en redes empresariales o en entornos de proveedores de servicios de Internet (ISP).

Gestión avanzada: El CRS326-24G-2S+RM es administrable a través de la interfaz de usuario gráfica (GUI) del software RouterOS de MikroTik. Esto proporciona acceso a una amplia gama de funciones de configuración y monitoreo, incluyendo la configuración de VLAN, enrutamiento estático y dinámico (OSPF, RIP, BGP), listas de control de acceso (ACL), calidad de servicio (QoS), y mucho más.

Compatibilidad con PoE: Aunque este modelo específico no ofrece soporte para PoE (Power over Ethernet), MikroTik ofrece otras variantes de switches de

la serie CRS que incluyen puertos PoE para alimentar dispositivos compatibles, como cámaras IP, puntos de acceso inalámbricos y teléfonos IP.

Montaje en rack: El CRS326-24G-2S+RM está diseñado para montarse en rack estándar de 19 pulgadas, lo que lo hace ideal para su implementación en centros de datos, armarios de red y entornos empresariales donde se requiere un espacio limitado.

En resumen, el MikroTik CRS326-24G-2S+RM es un switch versátil y potente que ofrece una combinación de puertos Gigabit Ethernet y 10 Gigabit SFP+, capacidades de conmutación avanzadas, gestión remota a través de RouterOS y un diseño compacto y montable en rack. Es una excelente opción para redes empresariales, proveedores de servicios de Internet y aplicaciones de centro de datos que requieren un rendimiento confiable y una buena relación calidad-precio.

Dentro del diseño de la Topología de Red, este equipo **MikroTik CRS326-24G-2S+RM** es el encargado de recibir mediante Fibra Óptica el enlace de datos e internet y es proporcionado y configurado por los ISP, donde ellos nos brindan una IP publica /30 y una IP WAN donde recibimos los enlaces de Datos.

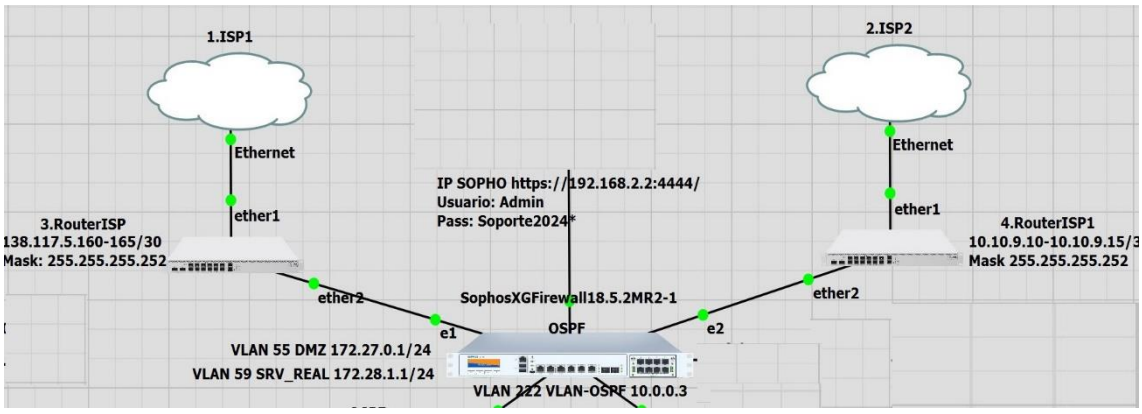


*Fig. 3 / **ISP o Proveedores… (Fuente Propia)***

6.3.4.2. Extreme Networks X690-48X-2Q-4C

El Extreme Networks X690-48X-2Q-4C es un switch de alto rendimiento diseñado para entornos de red empresariales y de centro de datos que requieren capacidades avanzadas de conmutación y enrutamiento. Aquí información sobre sus características principales:

Puertos y conectividad: El X690-48X-2Q-4C cuenta con 48 puertos 10GBASE-T (RJ45) para conexiones de red de alta velocidad a dispositivos compatibles con Ethernet de 10 Gigabits. Además, incluye 2 puertos QSFP28 para conectividad de 40/100 Gigabit y 4 puertos SFP28 para opciones de conectividad de alta velocidad a través de fibra óptica.

Rendimiento y escalabilidad: Este switch ofrece un rendimiento excepcional y una escalabilidad flexible para satisfacer las demandas de redes de alto rendimiento. Con una capacidad de conmutación de hasta varios terabits por segundo y tasas de reenvío de paquetes de varios millones de paquetes por segundo, el X690-48X-2Q-4C es capaz de manejar grandes volúmenes de tráfico de red de manera eficiente.

Capacidades de enrutamiento: El X690-48X-2Q-4C es un switch de capa 3, lo que significa que puede realizar funciones de enrutamiento avanzadas. Esto incluye la capacidad de enrutar tráfico entre diferentes subredes y segmentos VLAN, lo que proporciona una mayor flexibilidad y control sobre la distribución del tráfico en la red.

Características de seguridad: Este switch cuenta con funciones de seguridad avanzadas para proteger la red y los datos sensibles. Esto puede incluir listas de control de acceso (ACL), autenticación de puerto IEEE 8021X, inspección de paquetes y otras funciones de seguridad para proteger contra amenazas internas y externas.

Gestión y monitoreo: El X690-48X-2Q-4C ofrece opciones de gestión y monitoreo para administrar eficientemente la red. Esto puede incluir interfaces de usuario basadas en web, línea de comandos (CLI) y capacidades de gestión centralizada a través de protocolos como SNMP (Simple Network Management Protocol).

Calidad de servicio (QoS): Este switch admite QoS para priorizar el tráfico de red en función de la importancia y los requisitos de rendimiento de las aplicaciones. Esto garantiza una experiencia de red óptima para aplicaciones críticas como voz sobre IP (VoIP) y videoconferencia.

En resumen, el Extreme Networks X690-48X-2Q-4C es un switch de alto rendimiento y alta densidad que ofrece capacidades avanzadas de conmutación, enrutamiento y seguridad, así como opciones de conectividad flexible y escalabilidad para satisfacer las necesidades de redes empresariales y de centro de datos más exigentes.

Dentro del diseño de la Topología de Red, este equipo **Extreme Networks X690-48X-2Q-4C** son nuestros dispositivos Core y desempeñan un papel fundamental en una topología de red al proporcionar enrutamiento, conmutación y capacidades de interconexión para facilitar el flujo de datos dentro de la red. Son la columna vertebral de la infraestructura de red y garantizan un rendimiento, escalabilidad y disponibilidad óptimos de la red. En estos equipos es donde aplicamos la mayoría de protocolos como (OSPF, MLAG, VRRP, LACP, ETC).

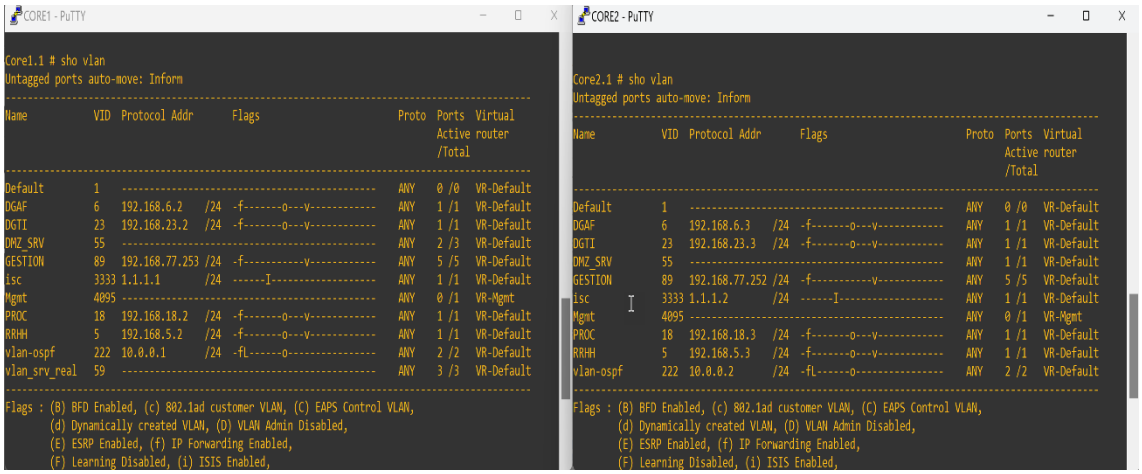


*Fig. 4 / **Creación VLAN... (Fuente Propia)***

En la Imagen 4 se muestran las VLAN creadas en ambos CORE, estas VLAN llevan asignados protocolos como IP forwarding, OSPF, VRRP y la asignación de sus respectivos IP.

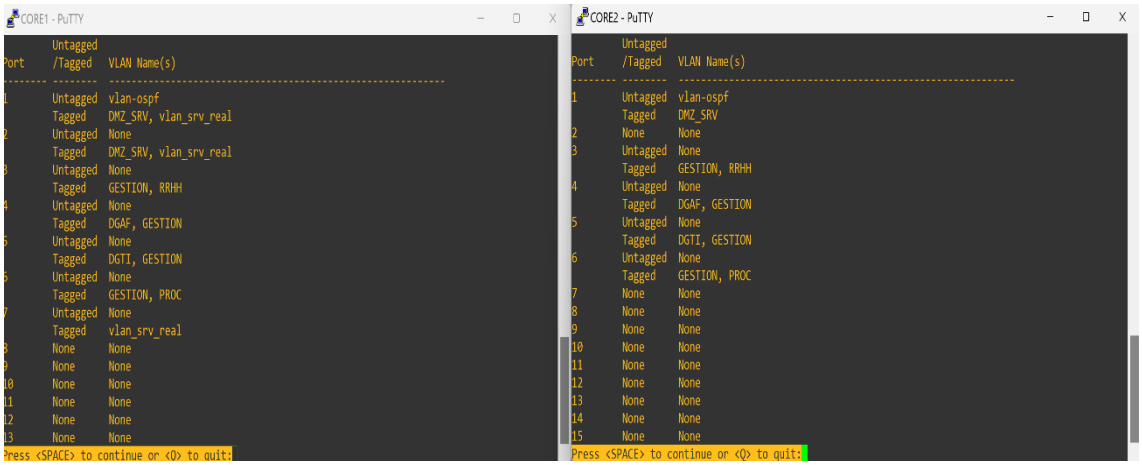


*Fig. 5 / **Asignación VLAN a puertos… (Fuente Propia)***

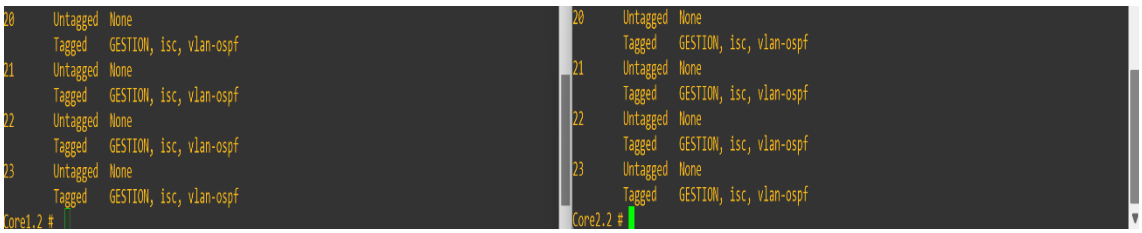


*Fig. 6 / **VLAN modo Tagged o Untagged… (Fuente Propia)***

Figura 5 y 6 asignación de VLAN a los puertos, ya sea modo Trunk o Acceso.

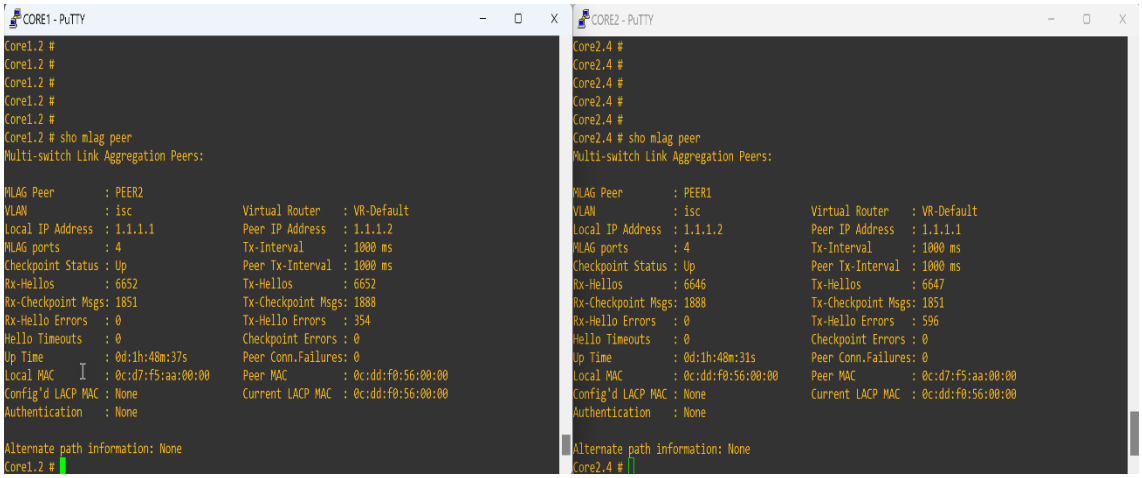


*Fig. 7 / **Configuración MLAG… (Fuente Propia)***

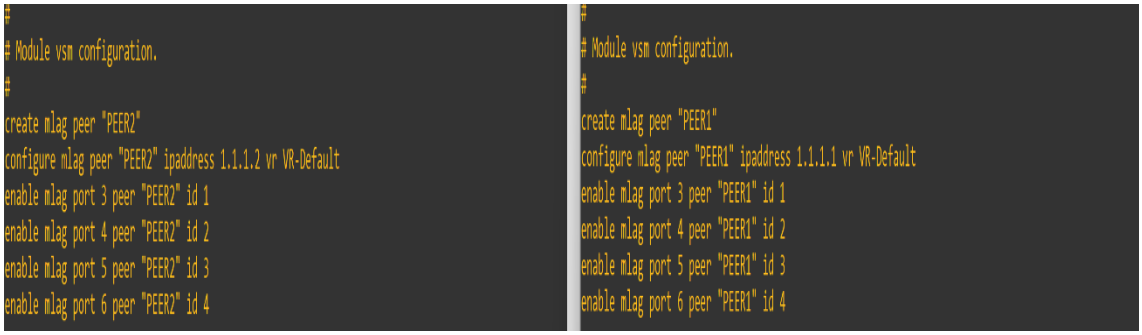


*Fig. 8 / Configuración MLAG **ID… (Fuente Propia)***

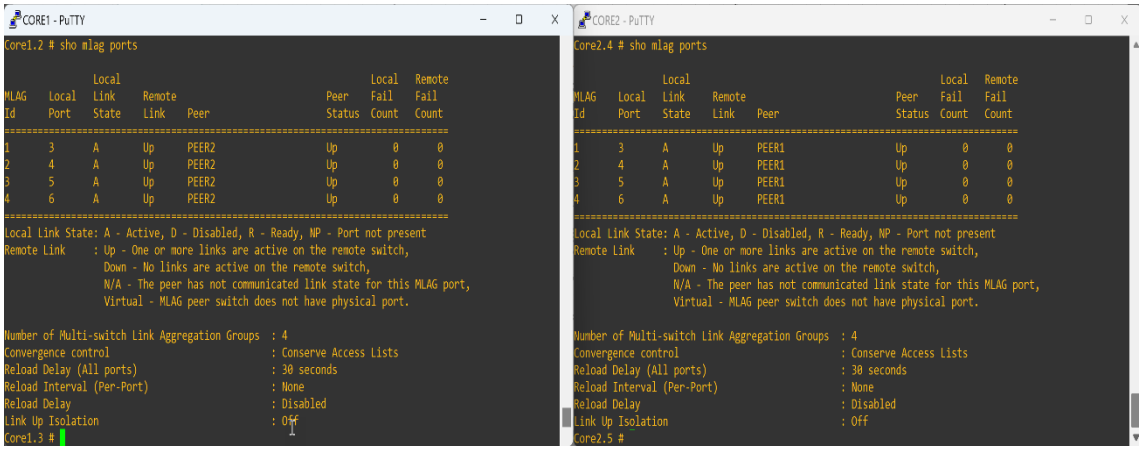


*Fig. 9 / Configuración **Puertos MLAG… (Fuente Propia)***

En la figura 7, 8 y 9 se muestra un grupo de puertos MLAG especificando el puerto del conmutador local, el conmutador del mismo nivel MLAG y un "mlag-id" que se utiliza para hacer referencia al puerto correspondiente en el conmutador del mismo nivel MLAG.

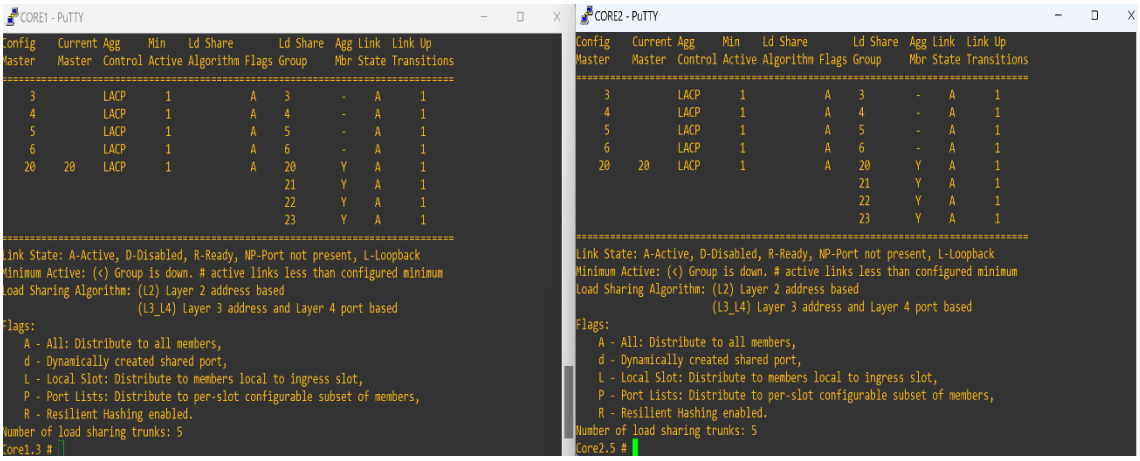


*Fig. 10 / **Configuración LACP… (Fuente Propia)***

Imagen 10, configuración de LACP (sharing), este nos permite agrupar varios puertos físicos para formar un único canal lógico.

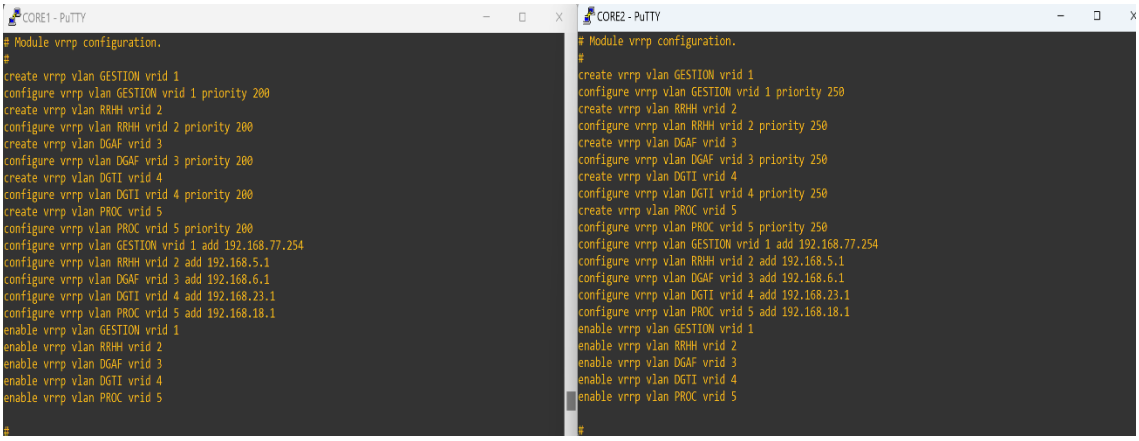


*Fig. 11 / **Configuración VRRP… (Fuente Propia)***

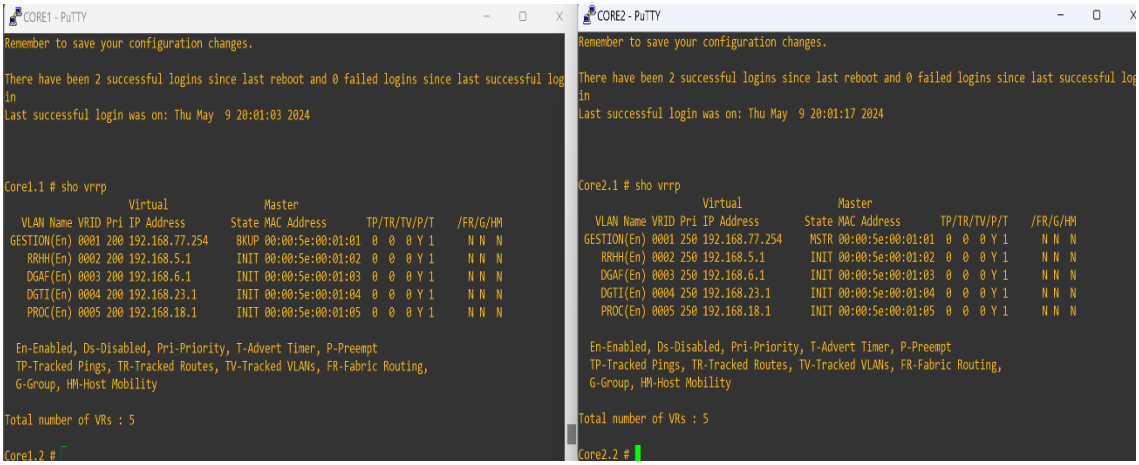


*Fig. 11 / **Configuración VRRP… (Fuente Propia)***

En las Figuras 11 y 12 se muestra el protocolo VRRP creado en ambos CORE, para garantizar la redundancia en nuestra topología.

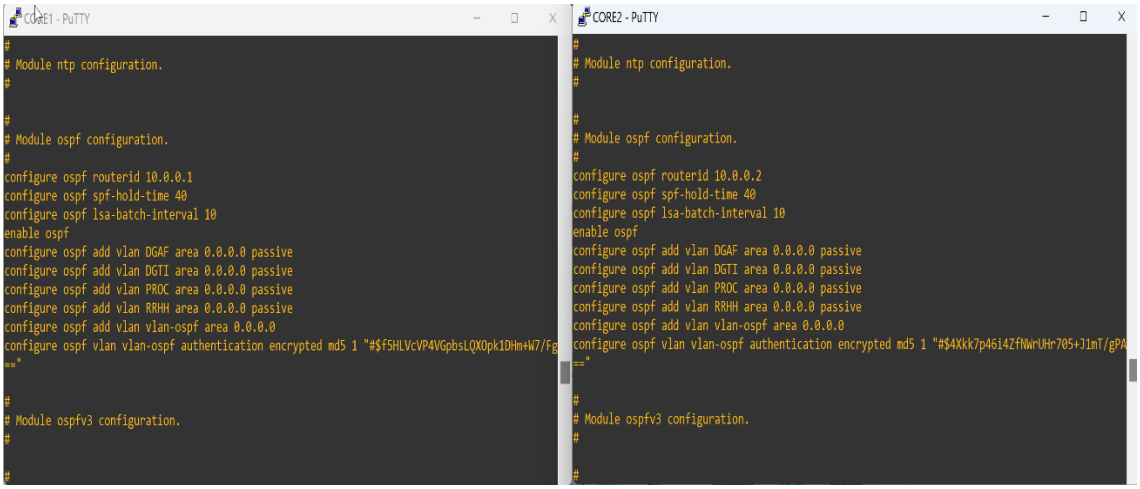


*Fig. 12 / **Configuración OSPF… (Fuente Propia)***

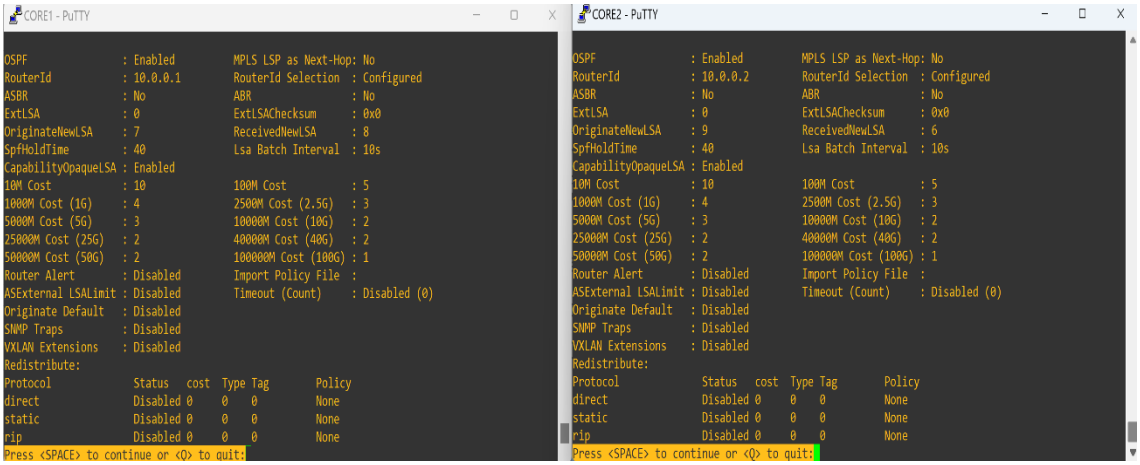


*Fig. 13 / **Configuración OSPF… (Fuente Propia)***

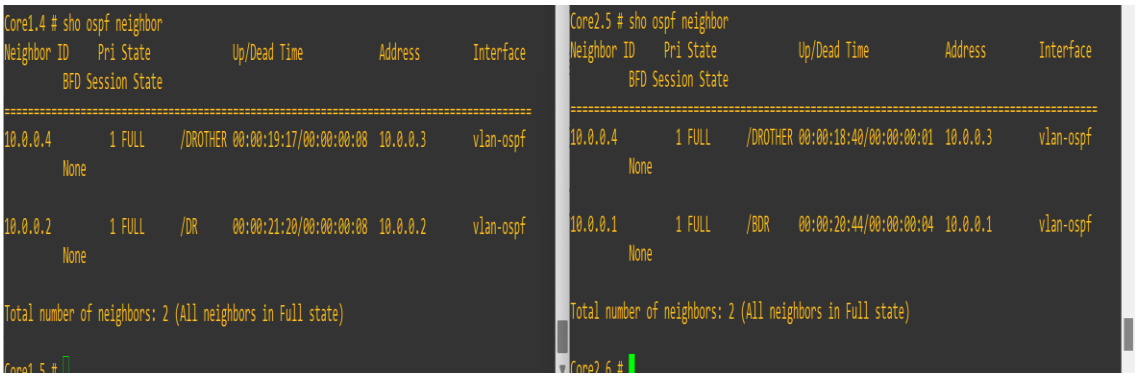


*Fig. 14 / **Configuración OSPF… (Fuente Propia)***

En las Figuras 13, 14, y 15 se muestra la configuración del protocolo OSPF en los CORE.

6.3.4.3. Extreme Networks X450

El Extreme Networks X450 es un switch de capa 3 que ofrece capacidades de enrutamiento avanzadas y funcionalidades de conmutación para redes empresariales. Aquí tienes algunos detalles sobre este equipo

Rendimiento y escalabilidad: El Extreme Networks X450 está diseñado para proporcionar un rendimiento sólido y escalabilidad para redes de tamaño mediano a grande. Ofrece una combinación de puertos de cobre y fibra óptica, lo que permite una conectividad versátil y flexible para diversos entornos de red.

Capacidades de enrutamiento: El X450 ofrece capacidades de enrutamiento avanzadas, lo que significa que puede realizar funciones de enrutamiento de capa 3. Esto le permite enrutar tráfico entre diferentes redes y segmentos VLAN, lo que resulta útil para dividir y gestionar eficientemente el tráfico en una red empresarial.

Características de seguridad: El switch X450 incluye características de seguridad robustas para proteger la red y los datos sensibles. Esto puede incluir listas de control de acceso (ACL), autenticación de puerto IEEE 802.1X, VLAN de invitado y otras funciones de seguridad avanzadas para proteger contra amenazas internas y externas.

Gestión y monitoreo: Extreme Networks X450 ofrece opciones de gestión y monitoreo para administrar eficientemente la red. Esto puede incluir interfaces de usuario basadas en web, línea de comandos (CLI) y capacidades de gestión centralizada a través de protocolos como SNMP (Simple Network Management Protocol).

Calidad de servicio (QoS): El switch X450 soporta QoS para priorizar el tráfico de red en función de la importancia y los requisitos de rendimiento de las aplicaciones. Esto garantiza una experiencia de red óptima para aplicaciones críticas como voz sobre IP (VoIP) y videoconferencia.

Alimentación redundante: Algunos modelos del Extreme Networks X450 pueden ofrecer opciones de alimentación redundante para garantizar la continuidad del servicio en caso de fallo de una fuente de alimentación.

En resumen, el Extreme Networks X450 es un switch de capa 3 robusto y versátil que ofrece capacidades de enrutamiento avanzadas, seguridad sólida, gestión eficiente y opciones de escalabilidad para satisfacer las necesidades de redes empresariales de tamaño mediano a grande.

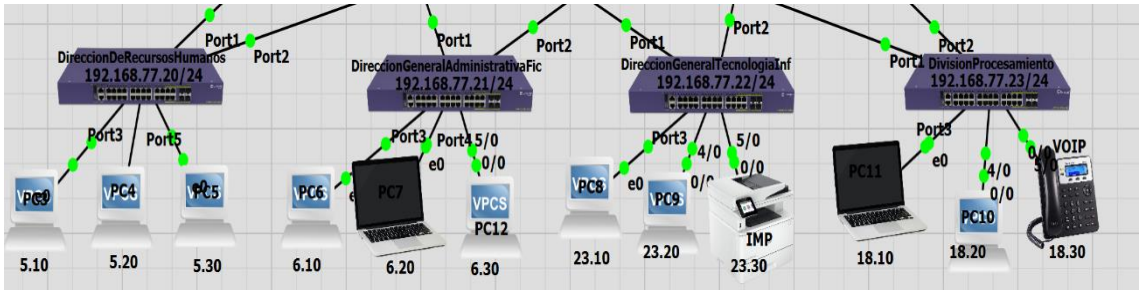


*Fig. 15 / **Capa de Acceso en la infraestructura de red de datos… (Fuente Propia)***

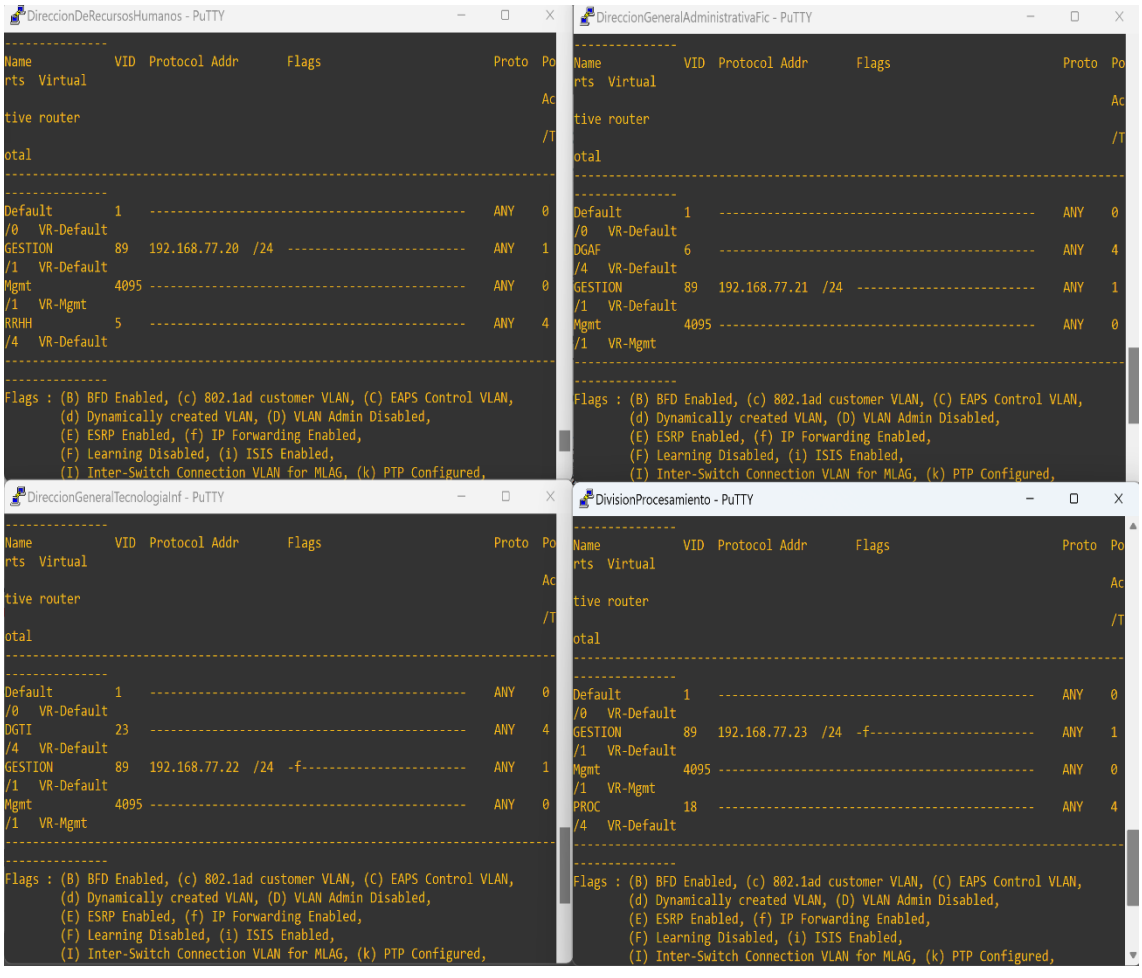


*Fig. 16 / **Creación VLAN en la capa de Acceso… (Fuente Propia)***

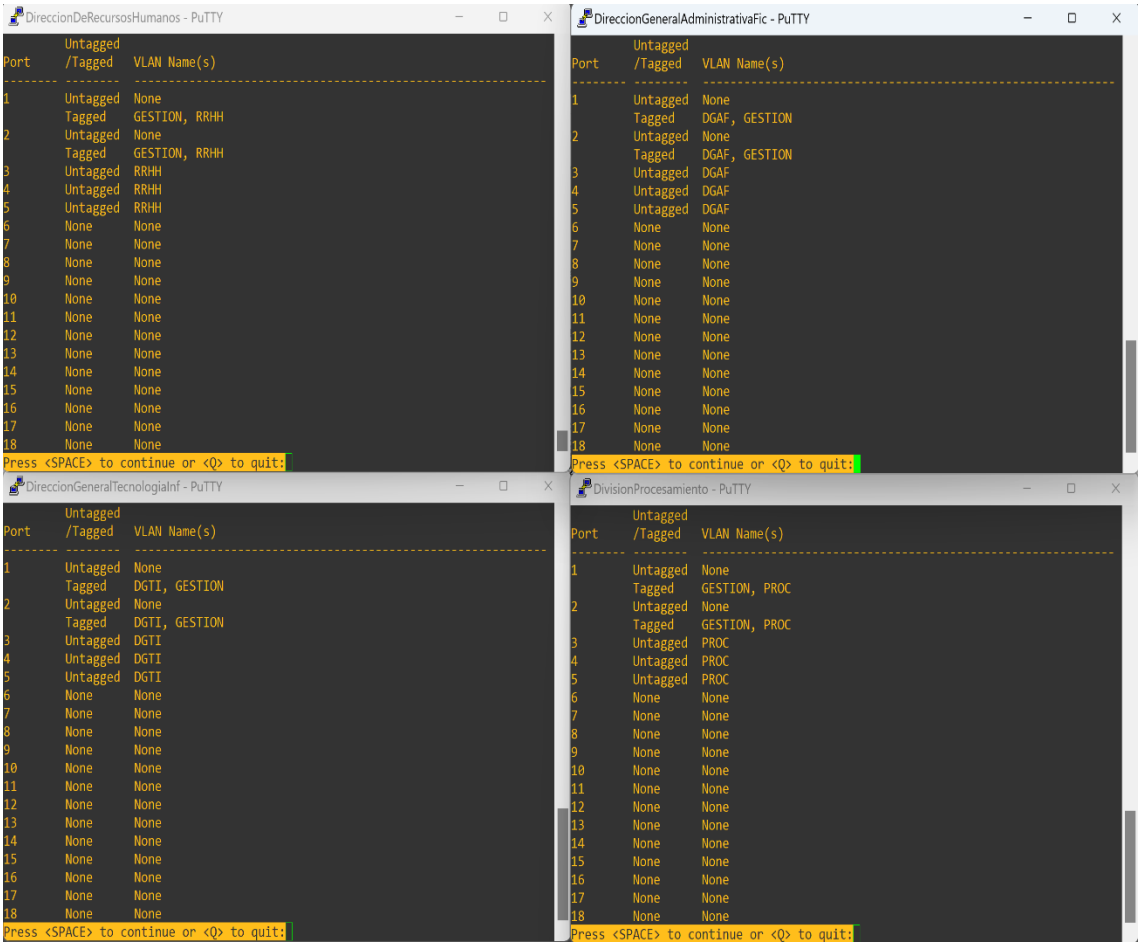


*Fig. 17 / **Asignación VLAN a Puertos en capa de Acceso… (Fuente Propia)***

En la figura 16 se muestra la capa de acceso y en las figuras 17 y 18 se observa la creación de VLANs y asignación a sus respectivos puertos.

6.3.4.4. Extreme Networks Summit X620

El Extreme Networks Summit X620 es un switch de la serie X de Extreme Networks, diseñado para ofrecer alto rendimiento, escalabilidad y fiabilidad en entornos empresariales.

Rendimiento y Capacidad: El Summit X620 ofrece un rendimiento excepcional y una alta capacidad de conmutación para manejar cargas de trabajo intensivas en datos en redes empresariales. Está equipado con procesadores potentes y una arquitectura diseñada para minimizar la latencia y maximizar el rendimiento de la red.

Escalabilidad: Este switch es escalable y puede adaptarse a las necesidades de crecimiento de la red empresarial. Ofrece opciones de expansión que permiten agregar más puertos o capacidades según sea necesario para satisfacer las demandas cambiantes de la red.

Diversidad de Puertos: El Summit X620 ofrece una variedad de opciones de conectividad, incluidos puertos Ethernet de cobre y fibra óptica. Esto permite la integración con una amplia gama de dispositivos de red y la creación de redes flexibles y versátiles.

Alta Disponibilidad: Extreme Networks se destaca por su enfoque en la alta disponibilidad de la red. El Summit X620 incluye características como fuentes de alimentación redundantes y capacidades de conmutación en caliente, que ayudan a minimizar el tiempo de inactividad no planificado y garantizan la continuidad del negocio.

Gestión Avanzada: El switch X620 viene con una amplia gama de herramientas de gestión que simplifican la administración y monitorización de la red. Esto incluye interfaces de usuario intuitivas, capacidades de gestión remota y opciones de automatización para optimizar el rendimiento y la eficiencia de la red.

Seguridad Integrada: Extreme Networks prioriza la seguridad de la red, y el Summit X620 incluye características de seguridad integradas para proteger la red empresarial contra amenazas y ataques cibernéticos. Esto puede incluir funciones como la detección de intrusiones, control de acceso y cifrado de datos.

A continuación, en las imágenes 19, 20, y 21 se muestra la configuración de este equipo como es la creación de Vlan, asignación de puertos (trunk y Acces) y enrutamiento.

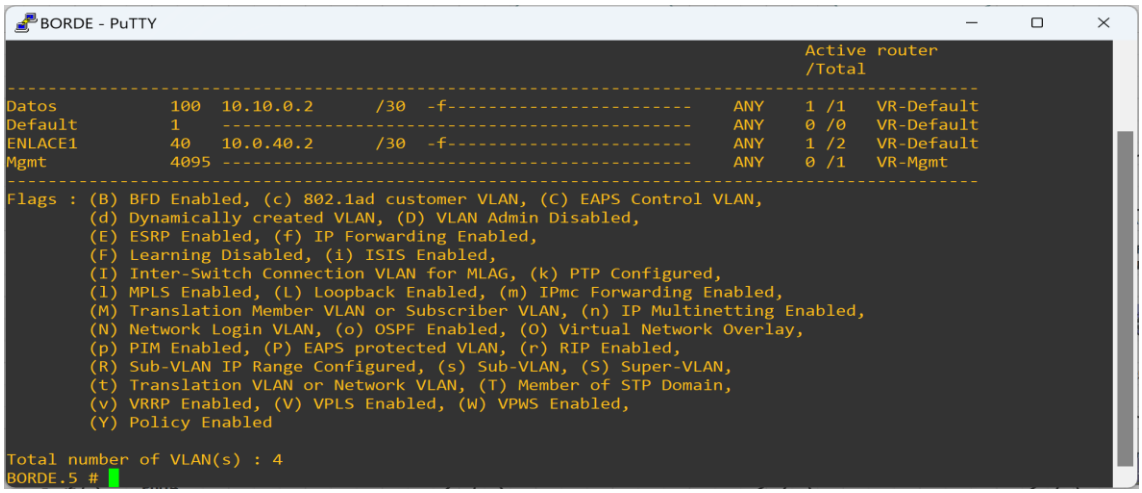


*Fig. 20 / **Creación VLAN Borde… (Fuente Propia)***

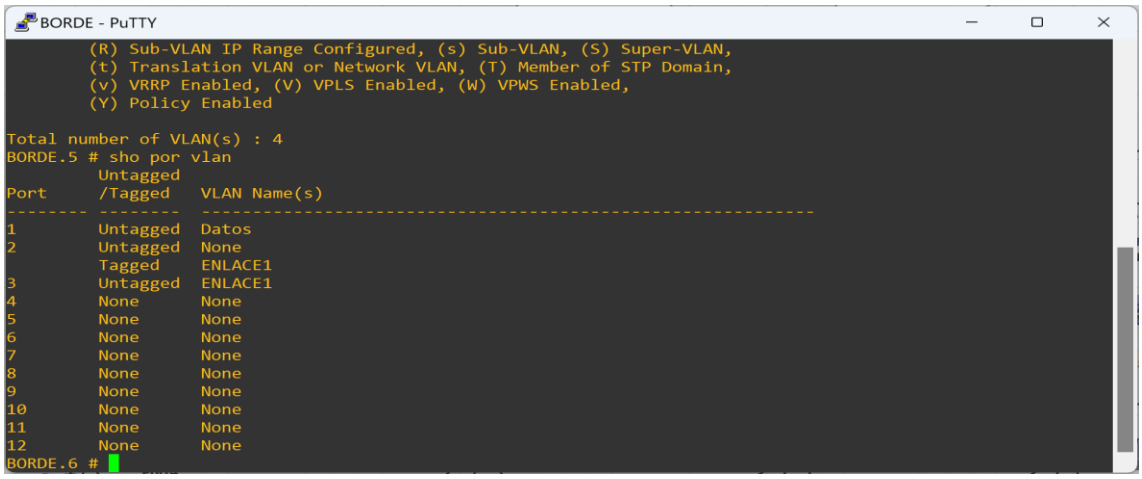


*Fig. 19 / **Asignación Vlan puertos Borde… (Fuente Propia)***

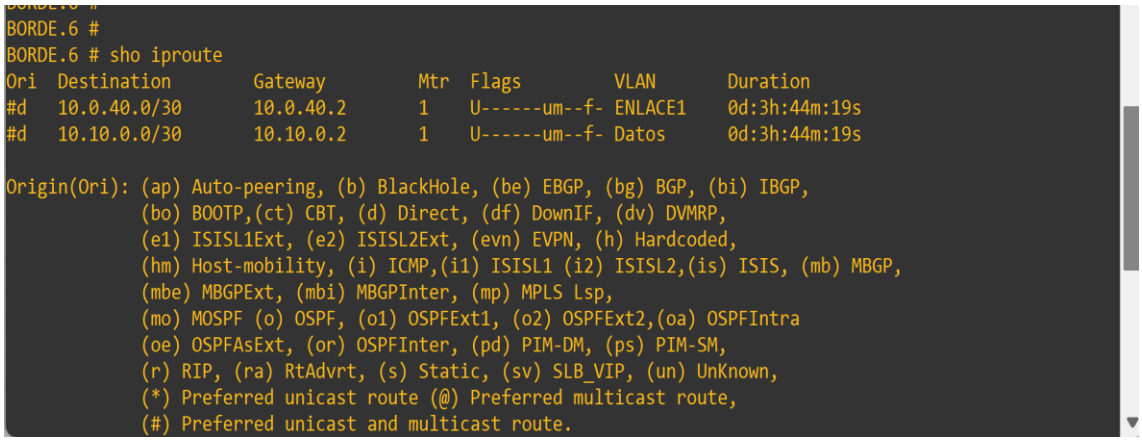


*Fig. 18 / **Enrutamiento Dinámico Borde… (Fuente Propia)***

6.3.4.5. Mikrotik RB4011iGS+5HacQ2HnD

El MikroTik RB4011iGS+5HacQ2HnD es un enrutador (router) de alto rendimiento y versátil fabricado por MikroTik, una empresa reconocida por sus soluciones de red robustas y económicas. Aquí tienes información sobre las características clave de este dispositivo:

Rendimiento potente: El RB4011iGS+5HacQ2HnD está equipado con un potente procesador de cuatro núcleos ARM de 1.4 GHz y 1 GB de RAM, lo que le proporciona un rendimiento excepcional para manejar cargas de trabajo intensivas en red y aplicaciones exigentes.

Conectividad versátil: Este enrutador cuenta con una variedad de interfaces de red para una conectividad versátil. Incluye cinco puertos Gigabit Ethernet (10/100/1000 Mbps), uno de los cuales puede funcionar como puerto PoE-in para alimentar el dispositivo a través de Ethernet. Además, dispone de dos puertos 10G SFP+ para conectividad de alta velocidad a través de fibra óptica.

Wi-Fi de alta velocidad: El RB4011iGS+5HacQ2HnD integra un punto de acceso inalámbrico de doble banda simultánea (2.4 GHz y 5 GHz) con soporte para los estándares Wi-Fi 802.11a/b/g/n/ac. Esto proporciona velocidades inalámbricas de hasta 1733 Mbps en la banda de 5 GHz y 300 Mbps en la banda de 2.4 GHz, lo que permite una conectividad inalámbrica rápida y confiable.

Funcionalidades avanzadas de enrutamiento y seguridad: Este enrutador es compatible con una amplia gama de protocolos de enrutamiento, incluyendo enrutamiento estático, RIP, OSPF y BGP. También ofrece características avanzadas de seguridad, como cortafuegos, listas de control de acceso (ACL), VPN (Virtual Private Network) y autenticación de usuario, que permiten proteger y gestionar el tráfico de red de manera eficaz.

Gestión flexible: El RB4011iGS+5HacQ2HnD es administrable a través de una interfaz de usuario intuitiva basada en web, así como a través de la línea de comandos (CLI) o la aplicación móvil de MikroTik (WinBox). Esto proporciona a los usuarios una variedad de opciones para configurar y gestionar el dispositivo de acuerdo a sus necesidades específicas.

Diseño compacto y robusto: El enrutador está diseñado en un factor de forma compacto y duradero, lo que lo hace ideal para su implementación en entornos empresariales, de oficina o domésticos donde se requiere un dispositivo confiable y de alto rendimiento.

En resumen, el MikroTik RB4011iGS+5HacQ2HnD es un enrutador potente y versátil que ofrece una combinación de conectividad por cable e inalámbrica de alta velocidad, funcionalidades avanzadas de enrutamiento y seguridad, y opciones de gestión flexibles. Es una excelente opción para redes empresariales, proveedores de servicios de Internet y aplicaciones de alta exigencia donde se requiere un rendimiento confiable y una amplia gama de características.

En la imagen 23, se muestra la interfaz de del equipo ubicado en nuestra sucursal, en el cual se configura Ip Address, creación de Bridge, reglas de firewall (Src.Address y Dst.Address), Nat, DHCP server, enrutamiento dinámico y creación de Ipsec Tunnel.

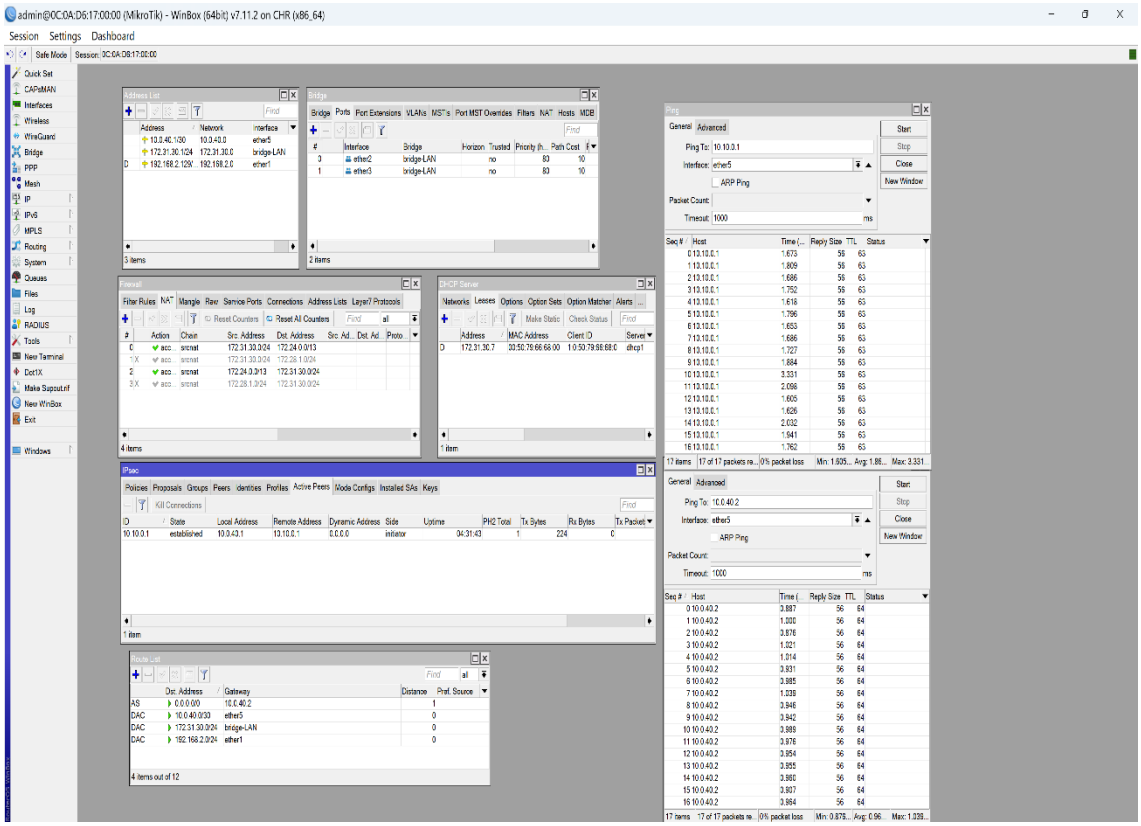


*Fig. 21 / **Configuración MikroTik Sucursal… (Fuente propia)***

6.3.4.6. Servidor Barracuda 1090

El Servidor Barracuda 1090 es parte de la línea de productos Barracuda Backup, diseñado específicamente para ofrecer soluciones de copia de seguridad y recuperación ante desastres para empresas de mediano a gran tamaño. Aquí hay información específica sobre este servidor:

Capacidad de Almacenamiento: El servidor Barracuda 1090 ofrece una capacidad de almacenamiento significativa, que puede adaptarse a las necesidades de datos de una empresa en crecimiento. Puede variar dependiendo de la configuración específica y de los discos duros utilizados, pero típicamente proporciona múltiples terabytes de capacidad de almacenamiento.

Rendimiento: Está diseñado para proporcionar un rendimiento rápido y confiable en las operaciones de copia de seguridad y restauración. Esto incluye velocidades de respaldo y restauración que pueden cumplir con los requisitos de empresas con grandes volúmenes de datos.

Escalabilidad: El servidor Barracuda 1090 está diseñado para ser escalable, lo que significa que puede crecer junto con las necesidades de almacenamiento de una empresa. Esto se logra a través de la capacidad de agregar almacenamiento adicional cuando sea necesario para manejar un mayor volumen de datos.

Funciones de Seguridad: Barracuda es conocido por su enfoque en la seguridad de los datos, y el servidor Barracuda 1090 no es una excepción. Ofrece características como cifrado de datos, autenticación de usuarios y controles de acceso para garantizar la integridad y confidencialidad de los datos almacenados.

Facilidad de Uso: Barracuda se esfuerza por hacer que sus soluciones sean fáciles de implementar y administrar. El servidor Barracuda 1090 generalmente viene con una interfaz de usuario intuitiva y herramientas de gestión que simplifican las tareas de administración y monitoreo.

Integración en la Nube: Además del almacenamiento local, el servidor Barracuda 1090 a menudo ofrece capacidades de integración en la nube, lo que permite realizar copias de seguridad en la nube para una mayor protección de los datos y la recuperación ante desastres.

6.3.4.7. Servidor Dell EMC PowerEdge R550

El servidor Dell EMC PowerEdge R550 es una solución empresarial diseñada para ofrecer rendimiento, escalabilidad y confiabilidad. Aquí tenemos más detalles sobre este servidor:

Rendimiento potente: El PowerEdge R550 está equipado con procesadores Intel Xeon escalables de última generación, lo que proporciona un rendimiento robusto para una amplia gama de cargas de trabajo empresariales. Estos procesadores ofrecen un alto rendimiento de cómputo y capacidades de virtualización avanzadas.

Escalabilidad: El servidor R550 está diseñado para adaptarse a las necesidades cambiantes de tu negocio. Ofrece una arquitectura escalable que te permite agregar capacidad de procesamiento, memoria y almacenamiento según sea necesario para satisfacer las demandas de crecimiento de tu empresa.

Fiabilidad y disponibilidad: Dell EMC PowerEdge R550 está diseñado para ofrecer una alta disponibilidad y confiabilidad. Incluye características como fuentes de alimentación redundantes y ventiladores intercambiables en caliente, que ayudan a minimizar el tiempo de inactividad no planificado y garantizan la continuidad del negocio.

Gestión simplificada: Dell ofrece una amplia gama de herramientas de gestión que facilitan la administración y monitorización del servidor R550. Esto incluye el uso de la plataforma de gestión integrada iDRAC (Integrated Dell Remote Access Controller), que permite realizar tareas de gestión de forma remota desde cualquier ubicación.

Seguridad integrada: El servidor PowerEdge R550 incluye características de seguridad integradas para proteger los datos y las cargas de trabajo empresariales. Esto puede incluir funciones como la protección de firmware, la encriptación de datos y las capacidades de seguridad basadas en hardware.

6.4. Definición de la estrategia de seguridad perimetral propuesta que resguarde la infraestructura de red de amenazas internas y externas

En el contexto actual de la ciberseguridad, proteger la infraestructura de red de amenazas tanto internas como externas se ha convertido en una prioridad crítica para las instituciones. En este capítulo, se propone una estrategia integral de seguridad perimetral que utiliza equipos de F5 Networks I 5800 y Sophos XG Firewall 5500. Este enfoque se centra en el despliegue eficiente de tecnologías avanzadas para mitigar riesgos y garantizar la integridad y confidencialidad de los datos.

Antes de definir la estrategia de seguridad perimetral, fue crucial comprender las amenazas internas y externas que enfrenta la infraestructura de red. Las amenazas internas pueden surgir de usuarios malintencionados o descuidados, mientras que las amenazas externas incluyen ataques de malware, ataques de denegación de servicio distribuido (DDoS) y intrusiones de hackers.

6.4.1. Estrategia Propuesta

Implementación para la Protección de Aplicaciones: Los dispositivos de F5 Networks ofrecen una gama de soluciones para la protección de aplicaciones web y la mitigación de ataques. Utilizando tecnologías como Web Application Firewall (WAF), Advanced Firewall Manager (AFM) y Secure Web Gateway (SWG), se puede establecer una defensa robusta contra amenazas externas dirigidas a las aplicaciones críticas.

Despliegue de Sophos XG Firewall 5500 para la Defensa Perimetral: Sophos XG Firewall 5500 proporciona un conjunto completo de características de seguridad, incluyendo firewall de próxima generación, protección contra intrusiones, prevención de amenazas avanzadas y filtrado de contenido. Al desplegar este firewall en el perímetro de la red, se puede establecer una barrera efectiva contra intrusiones externas y garantizar la seguridad de todo el tráfico de red.

Integración y Coordinación de Políticas de Seguridad: Es esencial que los equipos de F5 Networks y Sophos XG Firewall 5500 trabajen en conjunto para garantizar una defensa coherente y coordinada. La integración de políticas de seguridad, como la identificación de usuarios y la aplicación de reglas de acceso basadas en roles, permite una respuesta rápida y efectiva a las amenazas en tiempo real.

Monitoreo Continuo y Análisis de Amenazas: Además de la implementación de medidas de seguridad, se establece un sistema de monitoreo continúo utilizando herramientas de análisis de seguridad. Esto permitirá la detección temprana de actividades sospechosas y la respuesta inmediata a posibles amenazas, minimizando el impacto de los ataques.

La estrategia propuesta de seguridad perimetral, basada en equipos de F5 Networks I 5800 y Sophos XG Firewall 5500, proporciona una sólida defensa contra amenazas internas y externas. Al aprovechar las capacidades avanzadas de estas tecnologías, la institución puede proteger su infraestructura de red y salvaguardar la integridad de sus datos críticos. Sin embargo, es importante recordar que la seguridad cibernética es un proceso continuo y en constante evolución, y se requiere una vigilancia constante y actualizaciones periódicas para hacer frente a las amenazas emergentes.

6.4.2. Equipos a Utilizar

6.4.2.1. F5 Networks I 5800

El F5 Networks I 5800 es un dispositivo de la serie BIG-IP de F5 Networks, diseñado para proporcionar soluciones de entrega de aplicaciones y seguridad en la red para entornos empresariales y de proveedores de servicios. Aquí tienes información sobre sus características principales:

Equilibrio de carga de aplicaciones: El F5 Networks I 5800 ofrece capacidades avanzadas de equilibrio de carga de aplicaciones (ADC), que distribuyen el tráfico de red de manera inteligente entre múltiples servidores de aplicaciones para optimizar el rendimiento y la disponibilidad de las aplicaciones.

Escalabilidad y rendimiento: Este dispositivo está diseñado para escalar horizontal y verticalmente para adaptarse a las demandas cambiantes de tráfico de red. Ofrece un alto rendimiento con tasas de transferencia de hasta varios gigabits por segundo (Gbps), lo que garantiza una entrega rápida y eficiente de aplicaciones incluso en entornos de red de alta demanda.

Seguridad de aplicaciones: El F5 Networks I 5800 proporciona funcionalidades avanzadas de seguridad de aplicaciones para proteger las aplicaciones contra una amplia gama de amenazas cibernéticas, como ataques de denegación de servicio (DDoS), inyección de SQL, ataques de cross-site scripting (XSS) y otros ataques de aplicación.

Optimización de WAN: Este dispositivo incluye características de optimización de la WAN (Wide Area Network) que mejoran el rendimiento de las aplicaciones y reducen el consumo de ancho de banda en redes WAN. Esto se logra mediante técnicas como la compresión de datos, el almacenamiento en caché y la deduplicación de datos.

Control de acceso y autenticación: El F5 Networks I 5800 ofrece capacidades de control de acceso y autenticación que permiten a los administradores de red implementar políticas de seguridad granulares y garantizar el acceso seguro a las aplicaciones y los datos sensibles.

Gestión centralizada: Este dispositivo es administrable a través de una interfaz de usuario intuitiva que proporciona a los administradores de red visibilidad y control completos sobre el tráfico de aplicaciones y la seguridad de la red. Además, es compatible con la gestión centralizada a través de la plataforma de gestión BIG-IQ de F5 Networks.

En resumen, el F5 Networks I 5800 es una solución robusta y escalable de entrega de aplicaciones y seguridad en la red que proporciona un rendimiento excepcional, características avanzadas de seguridad y opciones de gestión flexibles para satisfacer las necesidades de las empresas y los proveedores de servicios de telecomunicaciones.

6.4.2.2. Sophos XG Firewall 5500

El Sophos XG Firewall 5500 es un dispositivo de seguridad de red de próxima generación fabricado por Sophos, una empresa líder en ciberseguridad. Aquí tienes información sobre sus características principales:

Firewall de próxima generación: El Sophos XG Firewall 5500 utiliza tecnología de firewall de próxima generación para proteger las redes empresariales contra una amplia gama de amenazas cibernéticas, incluyendo malware, ransomware, ataques de día cero y amenazas avanzadas persistentes (APT).

Inspección profunda de paquetes: Este dispositivo realiza inspección profunda de paquetes (DPI) para analizar el tráfico de red en busca de amenazas ocultas y aplicar políticas de seguridad granulares basadas en el contenido de los paquetes. Esto permite una detección más precisa y una protección más efectiva contra ataques cibernéticos.

Control de aplicaciones y usuarios: El Sophos XG Firewall 5500 permite a los administradores de red controlar y gestionar el acceso a aplicaciones y recursos de red mediante políticas de control de aplicaciones y usuarios. Esto incluye la capacidad de bloquear o permitir el acceso a aplicaciones específicas, así como la implementación de políticas de filtrado web basadas en categorías de contenido.

Seguridad avanzada de correo electrónico y web: Este dispositivo incluye funcionalidades avanzadas de seguridad de correo electrónico y web para proteger contra amenazas como phishing, spam, malware y sitios web maliciosos. Esto se logra mediante la implementación de filtros de correo electrónico y web, así como la inspección de URL y el análisis de archivos adjuntos.

VPN (Virtual Private Network): El Sophos XG Firewall 5500 ofrece capacidades de VPN seguras para permitir a los usuarios remotos acceder a la red corporativa de forma segura a través de Internet. Esto incluye soporte para protocolos VPN estándar como IPsec, SSL/TLS y L2TP, así como opciones de autenticación multifactor (MFA) y cifrado fuerte.

Gestión centralizada y visibilidad: Este dispositivo es administrable a través de una interfaz de usuario intuitiva que proporciona a los administradores de red visibilidad y control completos sobre el tráfico de red y las políticas de seguridad. Además, es compatible con la gestión centralizada a través de la plataforma de gestión Sophos Central, lo que permite la implementación y la administración centralizadas de políticas de seguridad en múltiples dispositivos.

En resumen, el Sophos XG Firewall 5500 es una solución robusta y completa de seguridad de red que proporciona protección avanzada contra amenazas cibernéticas, control de acceso granular, funcionalidades de VPN seguras y opciones de gestión flexibles. Es una excelente opción para empresas de todos los tamaños que buscan proteger sus redes contra las crecientes amenazas de seguridad en línea.

6.5. Validación del óptimo funcionamiento del diseño de infraestructura de red de datos y seguridad perimetral, mediante simulaciones utilizando la herramienta de software GNS3.

En este apartado se procederá a la validación del óptimo funcionamiento del diseño de infraestructura de red de datos y seguridad perimetral. Para ello, se empleará la herramienta de simulación de redes GNS3, que permitirá recrear y evaluar el comportamiento del sistema en un entorno controlado y realista. A través de diversas simulaciones, se verificará la eficacia y eficiencia del diseño propuesto, asegurando que cumpla con los requisitos de rendimiento, estabilidad y seguridad necesarios. Esta validación es crucial para confirmar que la infraestructura diseñada puede manejar adecuadamente el tráfico de datos y proteger la red contra posibles amenazas, garantizando así su robustez y fiabilidad en un entorno de producción real.

7. Conclusiones

La presente investigación ha culminado en el diseño integral de la infraestructura de red de datos y seguridad perimetral para una institución del Estado de Nicaragua, en cumplimiento de los objetivos establecidos. A lo largo del proceso, se ha abordado cada objetivo específico de manera exhaustiva, logrando avances significativos en la mejora de la postura tecnológica y de seguridad de la institución.

En primer lugar, se llevó a cabo una evaluación detallada de las condiciones tecnológicas existentes en el campo de las redes de datos y seguridad perimetral de la institución. Este análisis proporcionó una base sólida para comprender los desafíos y las oportunidades presentes en la infraestructura de red, sentando las bases para un diseño efectivo.

Mediante encuentros con el personal a cargo y entrevistas para el levantamiento de requerimientos, se recopiló información valiosa que orientó el proceso de diseño. La colaboración estrecha con los responsables del área permitió identificar necesidades específicas y considerar los objetivos estratégicos de la institución en cada etapa del proyecto.

El rediseño de la topología de red existente fue un paso crucial para optimizar el flujo de datos y garantizar la redundancia, confiabilidad, velocidad, almacenamiento y escalabilidad requeridos. Se implementaron cambios significativos en la infraestructura para mejorar la eficiencia operativa y prepararla para enfrentar los desafíos futuros.

La definición de una estrategia de seguridad perimetral representó otro hito importante en el proceso de diseño. Se propuso una serie de medidas y tecnologías, incluyendo la implementación de equipos F5 Networks i5800 y Sophos XG Firewall 5500, para proteger la infraestructura de red de amenazas internas y externas, garantizando la integridad y confidencialidad de los datos.

Finalmente, se validó el óptimo funcionamiento del diseño de infraestructura de red y seguridad perimetral mediante simulaciones utilizando la herramienta de software GNS3. Este proceso de validación permitió identificar posibles áreas de mejora y asegurar que el diseño propuesto cumpla con los requisitos y expectativas establecidos.

En conclusión, el diseño de la infraestructura de red de datos y seguridad perimetral para la institución del Estado de Nicaragua ha sido un proceso riguroso y colaborativo que ha resultado en una mejora significativa en la capacidad tecnológica y de seguridad de la organización. Se espera que este trabajo sirva como un marco sólido para la implementación exitosa de las recomendaciones propuestas y contribuya al logro de los objetivos estratégicos de la institución en materia de tecnología y seguridad de la información.

8. Recomendaciones

1. Mejora Continua de la Infraestructura

Recomendación: Implementar un plan de mejora continua para la infraestructura de red y la seguridad perimetral.

- **Detalles:** Establecer un calendario de revisiones periódicas (anuales o semestrales) para evaluar y actualizar la infraestructura de red y las políticas de seguridad perimetral, incorporando las últimas tecnologías y mejores prácticas.
- **Ejemplo:** Cada seis meses, realizar una auditoría de la red y la seguridad para identificar áreas de mejora y actualizar hardware y software según las necesidades detectadas.

2. Capacitación Continua del Personal

Recomendación: Desarrollar un programa de capacitación continua para el personal de TI.

- **Detalles:** Asegurar que el personal esté siempre al día con las nuevas tecnologías, protocolos de seguridad y mejores prácticas en gestión de redes.
- **Ejemplo:** Organizar talleres trimestrales y proporcionar acceso a cursos en línea para el personal de TI, enfocados en nuevas amenazas de seguridad, nuevas tecnologías de red, y actualización de certificaciones relevantes.

3. **Monitoreo y Análisis en Tiempo Real**

Recomendación: Implementar sistemas avanzados de monitoreo y análisis en tiempo real.

- **Detalles:** Utilizar herramientas de monitoreo continuo que permitan la detección proactiva de problemas de rendimiento y amenazas de seguridad.
- **Ejemplo:** Implementar una solución de SIEM (Gestión de Información y Eventos de Seguridad) que centralice los logs y eventos de seguridad para un análisis en tiempo real y una respuesta rápida ante incidentes.

4. **Simulaciones y Pruebas Regulares**

Recomendación: Realizar simulaciones y pruebas de estrés de manera regular para validar la robustez de la infraestructura.

- **Detalles:** Programar simulaciones periódicas de diferentes escenarios de carga y ataques para asegurarse de que la infraestructura puede manejar picos de tráfico y amenazas sin comprometer el rendimiento o la seguridad.
- **Ejemplo:** Utilizar GNS3 y otras herramientas de simulación para probar diferentes configuraciones de red y estrategias de seguridad bajo condiciones simuladas de alta demanda y ciberataques.

5. **Evaluación y Actualización de Equipos**

Recomendación: Realizar una evaluación periódica del hardware y software de red para asegurar que estén actualizados y funcionen de manera óptima.

Ejemplo: Planificar la actualización de equipos de red obsoletos y sistemas operativos que ya no reciban soporte. Asegurar de que todos los componentes de la red cumplan con los estándares modernos de rendimiento y seguridad.

9. Bibliografía

[1] G. Westreicher, «Economipedia.com,» 15 Enero 2022. [En línea]. Available: https://economipedia.com/definiciones/escalabilidad.html. [Último acceso: 31 07 2023].

[2] G. Alvaro, Enciclopedia de la Seguridad Informatica, Segunda ed., Mexico D.F: ALFAOMEGA GRUPO EDITOR S.A, 2014.

[3] L. A. Chavez Cruz, «Interconexión WAN de 3 sucursales de una empresa con casa matriz aplicando MPLZ como tecnologia de transporte mediante un diseño de red en GNS3,» Universidad Nacional de Ingenieria, Managua, 2022.

[4] M. Sabogal y M. Rios, «Diseño de infraestructura de red y seguridad informatica de la compañia Green Super Food,» Universidad Tecnologica de Pereira, Pereira, 2019.

[5] D. H. Noguera Rivera y L. F. Rocha Jambrina, «PROPUESTA DE SOLUCIÓN DE SEGURIDAD PERIMETRAL EN EL RECINTO,» Universidad Nacional de Ingenieria, Managua, 2020.

[6] A. Rosillo Moran, «PROPUESTA PARA LA IMPLEMENTACION DE LA INFRAESTRUCTURA DE RED EN LA SEDE DEL GOBIERNO REGIONAL DE TUMBES, 2019,» Universidad Católica Los Ángeles de Chimbote, Tumbes, 2019.

[7] I. E. T. F. (IETF), «datatracker,» Marzo 2010. [En línea]. Available: https://datatracker.ietf.org/doc/html/rfc5798. [Último acceso: 15 05 2024].

[8] GNS3, «gns3,» 2024 SolarWinds en todo el mundo, [En línea]. Available: https://www.gns3.com/. [Último acceso: 07 03 2024].

[9] R. TecnologiaMix, «Tecnología Mix,» Tecnología Mix, 13 Marzo 2021. [En línea]. Available: https://www.tecnologiamix.com/que-es-una-infraestructura-de-red/. [Último acceso: 22 Febrero 2023].

[10] C. H. Tarazona, «Amenazas informáticas y seguridad de la información.,» *Derecho Penal y Criminología,* nº 28, pp. 137-146, 4 Agosto 2007.

[11] L. Garcia, «CCM,» 09 Marzo 2023. [En línea]. Available: https://es.ccm.net/aplicaciones-e-internet/museo-de-internet/enciclopedia/10706-que-significa-alta-disponibilidad-en-redes/. [Último acceso: 31 Agosto 2023].

[12] CISCO, «© 2023 Cisco Systems, Inc.,» © 2023 Cisco Systems, Inc., 8 Enero 2014. [En línea]. Available: https://www.cisco.com. [Último acceso: 12 Octubre 2023].

[13] Mikrotik, «Mikrotik,» Mikrotik, [En línea]. Available: https://mikrotik.com/product/CRS326-24G-2SplusRM#fndtn-specifications. [Último acceso: 3 Abril 2024].

[14] F5, «F5 Inc.,» F5, 2024. [En línea]. Available: https://www.f5.com/es_es/products/big-ip-services/iseries-appliance. [Último acceso: 4 Abril 2024].

[15] Sophos, «Sophos Ltd,» Sophos, 1997 - 2024. [En línea]. Available: https://www.sophos.com/es-es/products/next-gen-firewall/tech-specs. [Último acceso: 25 Abril 2024].

10. Anexos

Entrevista para el Levantamiento de Requerimientos del Diseño de Infraestructura de Red de Datos y Seguridad Perimetral para una institución del estado.

Estimado/a Participante

Gracias por participar en esta encuesta. Tu opinión es fundamental para el proceso de diseño de la infraestructura de red de datos y seguridad perimetral de nuestra institución. Por favor, tómate unos minutos para responder las siguientes preguntas:

1) ¿Cuál es tu rol en la institución?

- □ **Director General de Tecnología**
- □ **Administrador de Redes**
- □ **Responsable de Seguridad Informática**
- □ **Usuario Final**
- □ **Otro (especificar)**

2) ¿Cuál es la topología de su red actual?

- □ **Punto a punto**
- □ **En bus**
- □ **En estrella**
- □ **En anillo**
- □ **En malla**
- □ **En árbol o jerárquica**
- □ **Topología híbrida, combinada o mixta.**
- □ **Otra (Especifique)**

3) ¿Qué tipo de equipos de red están en uso actualmente?

- □ **Enrutadores**
- □ **Conmutadores**
- □ **Firewalls**
- □ **Otra (Especifique)**

4) ¿Cuál es el rendimiento actual de su red en términos de ancho de banda?

- □ **100 Mbps subida – 50 Mbps bajada**
- □ **80 Mbps subida – 40 Mbps bajada**
- □ **60 Mbps subida – 30 Mbps bajada**
- □ **Otra (Especifique)**

5) ¿Cuáles son los principales desafíos o problemas que enfrenta con la infraestructura de red actual?

- □ **Seguridad**
- □ **Rendimiento**
- □ **Escalabilidad**
- □ **Almacenamiento**
- □ **Incompatibilidad con nuevas tecnologías**
- □ **Complejidad de gestión**
- □ **Todas las anteriores**
- □ **Otra (Especifique)**

6) ¿Qué aplicaciones o servicios críticos dependen de la infraestructura de red?

- □ **Correo**
- □ **Aplicación de Datos**
- □ **Conexión de Datos con Sucursales**
- □ **Almacenamiento servidor local**
- □ **Todas las anteriores**
- □ **Otra (Especifique)**

7) ¿Qué medidas de seguridad perimetral están en su lugar actualmente?

- □ **Firewalls**
- □ **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)**
- □ **VPN (Red Privada Virtual)**
- □ **Filtrado de Contenido Web**
- □ **Antivirus y Antimalware**
- □ **Otra (Especifique)**

8) ¿Cuál es su principal preocupación en términos de seguridad de red?

- □ **Brechas de Datos y Fugas de Información**
- □ **Ataques de Malware y Ransomware**
- □ **Intrusiones y Acceso no Autorizado**
- □ **Ataques de Denegación de Servicio (DDoS)**
- □ **Todas las anteriores**
- □ **Otra (Especifique)**

9) ¿Qué tipo de flexibilidad necesita su organización en términos de configuración y gestión de la red?

- □ **Escalabilidad**
- □ **Personalización**
- □ **Gestión Centralizada**
- □ **Adaptabilidad**
- □ **Facilidad de Implementación y Mantenimiento**
- □ **Todas las anteriores**
- □ **Otra (Especifique)**

10) ¿Qué funcionalidades de gestión y monitoreo considera más importantes para su organización?

- □ **Monitoreo de Red en Tiempo Real**
- □ **Alertas y Notificaciones**
- □ **Gestión de Configuración**
- □ **Análisis de Rendimiento**
- □ **Todas las anteriores**
- □ **Otra (Especifique)**

11) ¿Qué servicios o aplicaciones son críticos para tu trabajo diario en la institución? (Selecciona todos los que correspondan)

- □ **Correo Electrónico**
- □ **Sistema de Gestión de Documentos**
- □ **Aplicaciones de Ofimática (Microsoft Office, Google Workspace, etc.)**
- □ **Aplicaciones de Gestión Institucional (ERP, CRM, etc.)**
- □ **Acceso Remoto a Servidores**
- □ **Otros (especificar)**

12) ¿Consideras que la velocidad de la red actual es adecuada para tus necesidades?

- □ **Sí**
- □ **No**

13) ¿Has experimentado problemas de seguridad en la red de la institución en el pasado?

- □ **Sí**
- □ **No**

14) ¿Qué medidas de seguridad consideras más importantes para proteger la red de la institución? (Selecciona todos los que correspondan)

- □ **Firewall**
- □ **Antivirus/Antimalware**
- □ **Control de Acceso**
- □ **VPN (Redes Privadas Virtuales)**
- □ **Monitoreo de Eventos de Seguridad**
- □ **Otros (especificar)**

15) ¿Qué funcionalidades consideras imprescindibles para el nuevo firewall? (Selecciona todas las que correspondan)

- □ **Filtrado de Paquetes**
- □ **Inspección Profunda de Paquetes (DPI)**
- □ **Control de Acceso basado en Políticas (PAC)**
- □ **VPN (Redes Privadas Virtuales)**
- □ **Detección y Prevención de Intrusiones (IDS/IPS)**
- □ **Administración Centralizada**
- □ **Otros (especificar)**

16) ¿Qué tipo de equipos adicionales consideras necesarios para mejorar la infraestructura de red? (Selecciona todas las que correspondan)

- □ **Switches de Capa de Acceso**
- □ **Switches de Capa de Distribución**
- □ **Router de Borde**
- □ **Balanceadores de Carga**
- □ **Servidores Proxy**
- □ **Otros (especificar)**

17) ¿Qué protocolos de enrutamiento consideras esenciales para la nueva infraestructura de red? (Selecciona todas las que correspondan)

- □ **OSPF (Open Shortest Path First)**
- □ **MLAG (Multi-Chassis Link Aggregation)**
- □ **LACP (Link aggregation Control Protocol)**
- □ **BGP (Border Gateway Protocol)**
- □ **EIGRP (Enhanced Interior Gateway Routing Protocol)**
- □ **DHCP (Dynamic Host Configuration Protocol)**
- □ **RIP (Routing Information Protocol)**
- □ **VRRP (Virtual Router Redundancy Protocol)**
- □ **Otros (especificar)**

18) ¿Qué protocolos de seguridad consideras prioritarios para proteger la red perimetral? (Selecciona todas las que correspondan)

- □ **IPsec (Protocolo de Seguridad de la Capa de Internet)**
- □ **SSL/TLS (Protocolo de Capa de Transporte Seguro)**
- □ **IKE (Internet Key Exchange)**
- □ **L2TP (Protocolo de Tunelización de Capa 2)**
- □ **GRE (Encapsulación de Protocolo de Ruta Genérica)**
- □ **Otros (especificar)**

¡Gracias por tu tiempo y colaboración en completar esta encuesta!

Tabla comparativa entre Sophos XG Firewall 5500, Palo Alto Networks PA-3260 Next-Gen Firewall y Fortinet FortiGate 51E Firewalls JDTS-2024.

Característica	Sophos XG Firewall 5500	Palo Alto Networks PA-3260	Fortinet FortiGate 51E JDTS-2024
Rendimiento de Firewall	160 Gbps	8.2 Gbps	2.5 Gbps
Rendimiento de IPS	25 Gbps	4.4 Gbps	1 Gbps
Rendimiento de VPN	23 Gbps	2 Gbps	200 Mbps
Rendimiento de NGFW	40 Gbps	3.8 Gbps	1.8 Gbps
Conexiones concurrentes	50 millones	1.2 millones	200,000
Nuevas conexiones por seg	500,000	50,000	12,000
Puertos	8x 10G SFP+, 8x 1G RJ45, 2x 10G RJ45	12x 1G RJ45, 4x 1G SFP, 8x 10G SFP+	5x 1G RJ45, 2x 1G SFP
Interfaces adicionales	Módulos de expansión	Módulos de expansión	No aplicable
Altamente escalable	Sí	Sí	No
Soporte de SD-WAN	Sí	Sí	Sí
Soporte de VPN	IPsec, SSL VPN	IPsec, SSL VPN	IPsec, SSL VPN
Gestión	Local y en la nube	Local y en la nube	Local y en la nube
Soporte de amenazas avanzadas	Sí	Sí	Sí
Certificaciones de seguridad	NSS Labs, ICSA Labs, AV-Comparatives	NSS Labs, ICSA Labs, Common Criteria	NSS Labs, ICSA Labs
Precio aproximado	Alto	Muy Alto	Bajo

A continuación, se muestra una tabla con los precios aproximados de los equipos utilizados en el diseño de infraestructura de red y seguridad perimetral. Los precios pueden variar según la ubicación, proveedor, configuración, opciones adicionales de hardware, licencias y especificaciones.

Equipo	**Precio (USD)**
Mikrotik CRS326-24G-2S+RM	$227.00
Mikrotik RB4011iGS+5HacQ2HnD	$199.00
Extreme Networks X690-48X-2Q-4C	$16,000.00
Extreme Networks X450	$3,000.00
Extreme Networks Summit X620	$5,000.00
Servidor Barracuda 1090	$1,500.00
Servidor Dell EMC PowerEdge R550	$2,500.00
F5 Networks I 5800	$30,000 a $70,000
Sophos XG Firewall 5500	$20,000 a $50,000

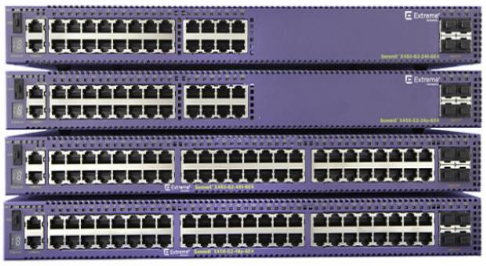
X450-G2 Series

Highlights

- Scalable edge switches with ExtremeXOS operating system
- 24-port or 48-port Gigabit Ethernet connectivity
- Copper and PoE+ models
- 4 x 10Gb SFP+ uplink ports on front faceplate
- Built-in 21 Gbps stacking ports on rear panel for all models (SummitStack-V84)
- Front-to-back airflow
- Modular PoE power supplies
- Hot-swappable fan tray and PoE power supplies
- All configurations non-blocking full duplex
- Role-based policy and Fabric Attach for secure, automated access to network applications or services

Smart Management Choices

- ExtremeCloud™ IQ for powerful, simple and secure public or private cloud management
- ExtremeCloud IQ – Site Engine for centralized, unified management capabilities



BUILT ON BROADCOM

Scalable edge switch with ExtremeXOS® modular operating system

The X450-G2 series is based on Extreme Networks ExtremeXOS, a highly resilient OS that provides continuous uptime, manageability, and operational efficiency. Each switch offers the same high-performance, non-blocking hardware technology, The X450-G2 series switches provide high-performance routing and switching, flexible stacking, PoE+support, and comprehensive security, while extending the benefits of ExtremeXOS to the campus edge.

The X450-G2 Series easy-to-use, yet powerful, management options include ExtremeCloud IQ and ExtremeCloud IQ - Site Engine for either cloud-based or on-premise oversight and configuration. The X450-G2 also supports role-based policies and Fabric Attach for secure, automated access to specific network resources and applications.

Intelligent Switching

The X450-G2 supports sophisticated and intelligent Layer 2 switching, as well as Layer 3 IPv4/ IPv6 routing. It also provides role-based policy capabilities, bidirectional Access Control Lists, and granular ingress/egress bandwidth limiting. Altogether, these enable fine-grained control over traffic, as well as secured access to network services and resources.

Performance and Scale

Switch Model	Maximum Active 1Gbe Ports	Maximum Active 10Gbe Ports	21 Gbps Stacking Ports	Aggregated Switch Bandwidth*	Frame Forwarding Rate*
X450-G2-24t-10GE4	24	4	2	212 Gbps	157.7 Mpps
X450-G2-48t-10GE4	48	4	2	260 Gbps	193.4 Mpps
X450-G2-24p-10GE4	24	4	2	212 Gbps	157.7 Mpps
X450-G2-48p-10GE4	48	4	2	260 Gbps	193.4 Mpps
X450-G2-24t-GE4	28	0	2	140 Gbps	104.2 Mpps
X450-G2-48t-GE4	52	0	2	188 Gbps	139.9 Mpps
X450-G2-24p-GE4	28	0	2	140 Gbps	104.2 Mpps
X450-G2-48p-GE4	52	0	2	188 Gbps	139.9 Mpps

* Includes stacking ports

- Less than 4 microsecond latency (64-byte)
- Layer 2/MAC Addresses: 68K
- IPv4 LPM Entries: 16K
- IPv6 LPM (64-bit) Entries: 8K
- IPv6 LPM (128-bit) Entries: 256
- 4096 VLAN/VMANs*
- 9216 Byte Max Packet Size (Jumbo Frame)
- 128 load sharing trunks, up to 32 members per trunk
- 1,024 ingress bandwidth meters
- Ingress and egress bandwidth policing/rate limiting per flow/ACL
- 8 QoS egress queues/port
- Egress bandwidth rate shaping per egress queue and per port
- Rate Limiting Granularity: 8 Kbps
- Rate Limiting: Per Class of Service
- All ports Full Duplex - half duplex operation is not supported

* 2 VLANs reserved for system use

Policy Capabilities

- Policy Profiles: 63
- Rules per Profile: Up to 1464
- Authenticated Policy Users per Switch: Up to 1024
- Authenticated Policy Users per Port: Up to 1024
- Unique Permit/Deny Rules per switch: 1464
- MAC Rules: 512
- IPv4 Rules: 512
- IPv6 Rules: 256
- L2 Rules: 184

Note: Policy and rule limits here reflect support available in EXOS 22.1.

X690 Series

Highlights

Family of 10Gb/100Gb Switches with Advanced Enterprise Capabilities

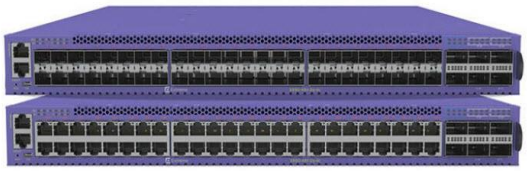
- Full featured ExtremeXOS® operating system with advanced features supporting switching, routing, SDN, and VXLAN
- Controlling aggregation switch for V300 and V400 edge devices with Extreme's Extended Edge Switching
- High-density 10Gb aggregation and leaf applications
- Non-blocking 1.76 Tbps switching capacity per system

Ease of Use — Flexible Management Options

- ExtremeCloud IQ - Site Engine application support
- Advanced command line interface
- Zero Touch Provisioning (ZTP+)
- Integrated web based management application

Flexible System Configurations

- Wide range of port speeds from 1Gb, 10Gb, 25Gb, 40Gb, 50Gb, and 100Gb
- Fiber SFP+ and copper 10GBASE-T models
- Hot-swappable modular power and fans
- AC and DC power supply options
- Front to Back and Back to Front airflow options
- Redundancy options for high availability



High-performance 48-port 10Gb aggregation and leaf switch

High-Density, 10Gb Enterprise LAN and Aggregation Switching

The X690 Series products are high-density, purpose-built 10Gb/100Gb switches designed for high-performance enterprise and aggregation applications. The X690 can support a range of interface speeds, including 1Gb, 10Gb, 25Gb, 40Gb, 50Gb, and 100Gb, all in a compact 1RU form factor. This enables the X690 to be flexibly deployed in either Enterprise LAN or high-density top of rack applications.

The X690 can also serve as the controlling aggregation switch within Extreme's Extended Edge Switching solution.

Two models of the X690 are available:

X690-48x-2q-4c

- 48 x 1Gb/10Gb SFP+ ports
- 2 x 10Gb/40Gb QSFP+ ports
- Up to 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports

X690-48t-2q-4c

- 48 x 100Mb/1Gb/10Gb 10GBASE-T ports
- 2 x 10Gb/40Gb QSFP+ ports
- Up to 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports

Product Specifications

Model	X690-48x-2q-4c	X690-48t-2q-4c
Ports	• 48 x 1Gb/10Gb SFP+ ports • 2 x 10Gb/40Gb QSFP+ ports • 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports • 1 x Serial console port RJ-45 • 1 x 10/100/1000BASE-T out-of-band management port • Micro-USB Type A storage port **QSFP Port Configurations Support** • 4 x 10Gb/40Gb QSFP+ ports and 2 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports **or** • 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports (two QSFP ports inactive)	• 48 x 100Mb/1Gb/10Gb 10GBASE-T ports • 2 x 10Gb/40Gb QSFP+ ports • 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports • 1 x Serial console port RJ-45 • 1 x 10/100/1000BASE-T out-of-band management port • Micro-USB Type A storage port **QSFP Port Configurations Support** • 4 x 10Gb/40Gb QSFP+ ports and 2 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports **or** • 4 x 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28 ports (two QSFP ports inactive)
Power Supplies	• Modular 770W AC power supply (up to two PSUs) • Modular 1100W DC power supply (up to two PSUs) • Front-Back and Back-Front airflow options	• Modular 770W AC power supply (up to two PSUs) • Modular 1100W DC power supply (up to two PSUs) • Front-Back and Back-Front airflow options
Fan Modules	6 fan modules Front-Back and Back-Front airflow options	6 fan modules Front-Back and Back-Front airflow options
Dimensions	17.4 in W / 19.2 in D / 1.7 in H (44.1 cm / 48.8 cm / 4.3 cm)	17.4 in W / 19.2 in D / 1.7 in H (44.1 cm / 48.8 cm / 4.3 cm)
Performance	• 1.76Tbps Switching Capacity • 759Mpps Forwarding Rate • Average Latency: 800 ns	• 1.76Tbps Switching Capacity • 759Mpps Forwarding Rate • Average Latency: 2.3 µsec
CPU Memory	• 2.4GHz Quad core CPU • 8GB DDR3 ECC memory • 32GB SSD memory	• 2.4GHz Quad core CPU • 8GB DDR3 ECC memory • 32GB SSD memory
Packet Buffers	12MB	12MB
Operating Conditions	• 0°C - 45°C operation • 10% to 95% relative humidity, non-condensing • 0 - 3000 meters altitude • Shock (half sine): 98 m/s2 (10 G), 11 ms, 9 shocks • Random vibration: 3 to 500 Hz at 1.5G rms	• 0°C - 45°C operation • 10% to 95% relative humidity, non-condensing • 0 - 3000 meters altitude • Shock (half sine): 98 m/s2 (10 G), 11 ms, 9 shocks • Random vibration: 3 to 500 Hz at 1.5G rms

X620 Series

Highlights

Family of 10Gb Edge Switches with Advanced Enterprise Capabilities

- Full featured ExtremeXOS® operating system
- SummitStack-V flexible stacking

Ease of Use - Flexible Management Options

- Integrated web-based management application
- Centralized management via ExtremeCloud™ IQ - Site Engine
- Advanced command line interface

Flexible System Configurations

- 10GBASE fiber connectivity
- Wide range of port speeds from 100Mb to 10Gb
- Hot swappable modular systems and compact small form versions
- Redundancy options for high availability
- All systems provide non-blocking, wire-speed performance

Advanced Modular 16 Ports 10Gb Ethernet Switches - 10GBASE-T and SFP+

- Hot-swappable modular power and fans
- AC and DC power supply options
- Front to Back or Back to Front airflow options

Compact 10 Port 10Gb Ethernet Switches - 10GBASE-T and SFP+

- Integrated power supplies and fans
- External redundant power supply (RPS) options

BUILT ON BROADCOM

10Gb Edge Ethernet Switch

The X620 product family are compact 10Gb Ethernet switches designed for high-speed edge applications in a small 1RU form factor. The X620 supports sophisticated, intelligent Layer 2 switching, as well as Layer 3 IPv4/IPv6 routing including policy-based switching/routing. The X620 simplifies network operation with the ExtremeXOS modular operating system, which is used among many networking products. The high availability ExtremeXOS operating system provides simplicity and ease of operation through the use of one OS everywhere in the network.

X620 Models

- X620-16x – 16 100Mb/1Gb/10Gb SFP+ ports using hot-swappable power supplies and fan modules
- X620-10x – 10 100Mb/1Gb/10Gb SFP+ ports with integrated power supply and fans

Product Specifications

X620 16 Port Models

	X620-16x	X620-10x
Ports	• 16 x 100Mb/1Gb/10GBASE-X SFP+ ports • 1 x Serial console port RJ-45 • 1 x 10/100/1000BASE-T out-of-band management port • USB 2.0 port	• 10 x 100Mb/1Gb/10GBASE-X SFP+ ports • 1 x Serial console port RJ-45 • 1 x 10/100/1000BASE-T out of-band management port • USB 2.0 port
Power Supplies	• Modular 300W power supply (up to two PSUs) • AC and DC power options • Mixed AC and DC configuration • Front-Back or Back-Front airflow options	• Integrated 100W AC PSU • RPS connector for external redundant PSU • Side to side airflow
Dimensions	17 in W / 17.4 in D / 1.7 in H (43.1 cm / 44.1 cm / 4.4 cm)	12 in W / 10.3 in D / 1.7 in H (30.48 cm / 26.2 cm / 4.3 cm)
Weight	11.1 lb / 5.0 kg (base system)	6.04 lb / 2.74 kg
Performance	Line rate 320Gbps/ 238Mpps Switching Capacity	Line rate 200Gbps/ 148.8Mpps Switching Capacity
CPU / Memory	1GHz CPU 1GB DDR3 ECC memory 4GB eMMC Flash memory	1GHz CPU 1GB DDR3 ECC memory 4GB eMMC Flash memory
Packet Buffers	2MB	2MB
Operating Conditions	0°C - 50°C operation 10% to 95% relative humidity, non-condensing 0-3000 meters altitude Shock (half sine): 30 m/s2 (3G), 11 ms, 6 shocks Random vibration: 3Hz to 500Hz at 1.5 G rms	

Scaling and Performance

MAC Addresses: 16K

IPv4 LPM Entries: 480

IPv4 Hosts:
- with min LPM IPv4 entries: 1500
- with max LPM IPv4 entries: 1500

IPv6 LPM (/64) Entries: 240

IPv6 Hosts: 1500

IP Multicast
- Groups: 256
- Max (S,G) entries: 1500

Latency:
- SFP+: average 900ns (64 byte packet)
- 10GBASE-T: average 2.4µsec (64 byte packet)

4092 user-created VLAN/VMANs

9216 Byte Max Packet Size (Jumbo Frame)

128 load sharing trunks, up to 8 members per trunk

ACLs 2048 ingress / 512 egress

Ingress and egress bandwidth policing/rate limiting per flow/ACL

1,024 ingress bandwidth meters, 256 egress meters

8 QoS egress queues/port

Egress bandwidth rate shaping per egress queue and per port

Rate Limiting Granularity: 8 Kbps

All ports only full duplex at all speeds

CRS326-24G-2S+RM

We are announcing a special version of the CSS326-24G-2S+RM switch, with added RouterOS as a second boot option, the new CRS326-24G-2S+RM.

This is a SwOS/RouterOS powered 24 port Gigabit Ethernet switch with two SFP+ ports, wire speed connectivity with several new switching features!

The "Dual boot" feature that allows you to choose which operating system you prefer to use, RouterOS or SwOS. If you prefer to have a simplified switch only OS with more switch specific features, use SwOS. If you are used to Winbox and would like the ability to use routing and other Layer 3 features on some ports in your CRS, boot and use RouterOS. You can select the desired operating system from RouterOS, from SwOS or from the RouterBOOT loader settings.

It gives you all the basic functionality for a managed switch, plus more: allows to manage port-to-port forwarding, apply MAC filter, configure VLANs, mirror traffic, apply bandwidth limitation and even adjust some MAC and IP header fields. SFP cage supports both 1.25 Gb SFP and 10 Gb SFP+ modules.

Specifications

Product code	CRS326-24G-2S+RM
CPU	98DX3236A1 800 MHz
RAM	512 MB
Storage type	Flash, 16 MB
Switch chip model	98DX3236A1
10/100/1000 Ethernet ports	24
SFP+ cages	2
Operating system	SwOS /RouterOS (Dual boot)
Supported input voltage	9 - 30 V (jack or passive PoE)
Dimensions	443 x 144 x 44 mm
Operating temperature	-40°C .. +60°C tested
Max power consumption	24 W
Serial port	RJ45

Features

- Non-blocking Layer 2 switching capacity
- 16K host table
- IEEE 802.1Q VLAN
- Supports up to 4K VLANs
- Port isolation
- Port security
- Broadcast storm control
- Port mirroring of ingress/egress traffic
- Rapid Spanning Tree Protocol
- Access Control List
- MikroTik neighbor discovery
- SNMP v1
- Web-based GUI

Included

24 V 1.2 A power adapter

Rack ears

THE 4011 SERIES

FUEL YOUR NETWORK

The RB4011 uses the amazingly powerful quad core Cortex A15 chip from Annapurna labs, an Amazon company, same as in our carrier grade RB1100AHx4 unit. The CPU supports IPsec hardware acceleration, there is 1GB of RAM, so this device will easily handle any task you have configured RouterOS to perform. All of this power, in a compact, fanless and professional looking solid metal enclosure in matte black.

Specifications

Product code	RB4011iGS+5HacQ2HnD-IN	
CPU	4 core AL21400 1.4 GHz	
Size of RAM	1 GB	
Storage	NAND 512 MB	
10/100/1000 Ethernet ports	10	
SFP+ port	1	
Switch chip model	RTL8367SB	
Wireless	2.4 GHz radio	5 GHz radio
Wireless regulations	Specific frequency range may be limited by country regulations	
Operating frequency	2412 - 2484 MHz	5150 - 5875 MHz
Wireless interface model	R11e-2HnD	QCA-9984
Supported protocol	802.11b/g/n	802.11a/n/ac
Chains	2	4
Antenna beam width	360°	
Antenna gain	3 dBi (2 antennas dual band, 2 antennas single 5 GHz band)	
Power Jack	1	
PoE in	Yes (port 1), passive, 18 - 57 V	
PoE out	Yes (port 10), passive, up to 57 V	
Max power consumption	23 W without PoE out, 44 W with PoE out	
Supported input voltage	12 V - 57 V (jack)	
Voltage Monitor	Yes	
PCB temperature monitor	Yes	
Operating temperature	-40 C .. +45 C	
Dimensions	228 x 120 x 30 mm	
Serial port	RJ45	
License level	5	
Operating System	RouterOS	

Wireless specifications

RATE (2.4 GHz)	Tx (dBm)	Rx (dBm)
1MBit/s	28	-100
11MBit/s	28	-94
6MBit/s	29	-96
54MBit/s	25	-80
MCS0	26	-96
MCS7	24	-79

RATE (5 GHz)	Tx (dBm)	Rx (dBm)
6MBit/s	33	-96
54MBit/s	29	-81
MCS0	33	-96
MCS7	28	-77
MCS9	26	-72

Ethernet test results

RB4011iGS+5HacQ2HnD-IN		Max possible throughput					
Mode	Configuration	1518 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	806.4	9,792.9	2,312.9	9,473.6	5,509.7	2,821.0
Bridging	25 bridge filter rules	806.4	9,792.9	1,037.4	4,249.2	1,153.2	590.4
Routing	none (fast path)	806.4	9,792.9	1,923.3	7,877.8	5092,3	2,607.3
Routing	25 simple queues	806.4	9,792.9	1,046.6	4,286.9	960.3	491.7
Routing	25 ip filter rules	593.7	7,209.9	625.2	2,560.8	564.6	289.1

IPsec test results

RB4011iGS+5HacQ2HnD-IN		RB4011iGS+5HacQ2HnD-IN IPsec throughput					
Mode	Configuration	1400 byte		512 byte		64 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Single tunnel	AES-128-CBC + SHA1	140.8	1577	141,2	578.4	139.9	71.6
256 tunnels	AES-128-CBC + SHA1	192.7	2158.2	200.5	821.2	203.4	104.1
256 tunnels	AES-128-CBC + SHA256	192.4	2154.9	200.5	821.2	203.4	104.1
256 tunnels	AES-256-CBC + SHA1	180.0	2016.0	188.2	770.9	190.3	97.4
256 tunnels	AES-256-CBC + SHA256	180.0	2016.0	188.2	770.9	190.3	97.4
256 tunnels	AES-128-GCM	192.7	2158.2	202.2	828.2	203.4	104.1

Barracuda Backup

Prevent data loss and minimize downtime

Barracuda Backup combines storage, software, and inline deduplication, to ensure your data is protected against loss no matter what happens. It's easy to deploy, usually in less than an hour. There are no per-application or per-agent licensing fees, and its single-pane-of-glass admin console makes management fast and easy.

Available as a hardware or virtual appliance, Barracuda Backup delivers near-continuous data protection and replication to an off-site appliance or to the cloud.

Defend against ransomware, disasters, and malicious destruction

Barracuda Backup lets you quickly recover files encrypted by ransomware. Simply eliminate the malware, delete the bad files, and restore them from a recent backup. Recovery can take as little as an hour—and the bad guys go home empty-handed.

Barracuda Backup's hardened Linux OS is less vulnerable to threats than Windows-based backup solutions. Data is protected in transit and at rest in the remote location by 256-bit AES encryption.

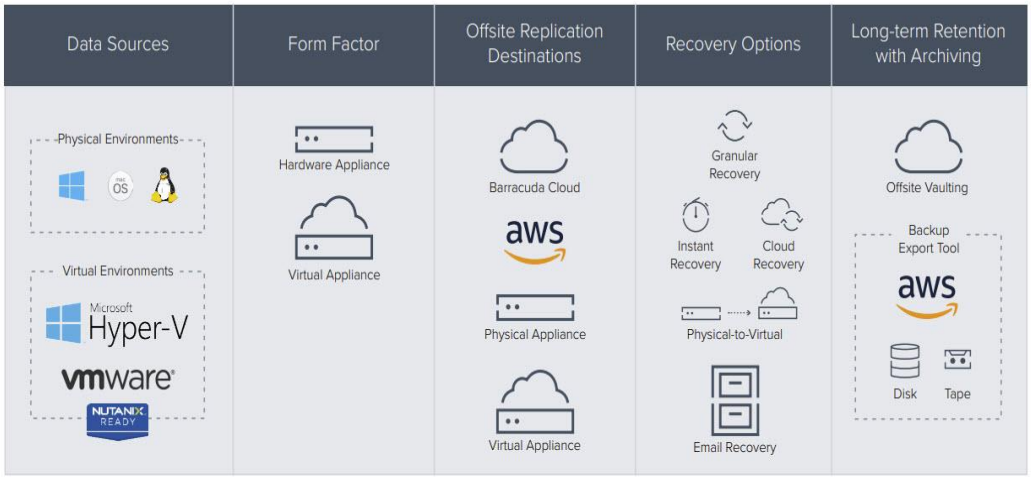
Rapid recovery from data loss

Barracuda Backup provides multiple recovery options to help you get back up and running quickly. With a Barracuda Cloud or Amazon Web Services (AWS) subscription, you can recover data from anywhere at any time, without the need for a local appliance.

Barracuda LiveBoot provides fast and easy recovery for on-premises VMware environments in cases where primary storage is lost or no longer available, while Cloud LiveBoot provides fast recovery for both VMware and Hyper-V virtual machines.

Flexible deployment and recovery

Barracuda Backup is available as a hardware or as a virtual appliance. Models range in capacity from 1 terabyte to 160 terabytes, to accommodate your specific backup needs. Barracuda Backup also has a wide range of offsite replication options for disaster recovery (Barracuda Cloud, hardware or virtual appliance, AWS).



Technical Specs

Backup

- Full local backup and restore
- Inline, block-level, source- and target-based deduplication
- Built-in WAN acceleration
- Cloud or site-to-site replication
- Real-time inline replication to offsite storage
- Export to Amazon Web Services (AWS), external disk, tape, autoloaders, or robotic libraries
- Near-continuous data protection
- VMware Changed Block Tracking (CBT)
- Encrypted client and server communication for additional security
- In case of disaster, Instant Replacement can deliver a new unit preloaded with data and configuration backed up to Barracuda Cloud Storage

Offsite Vaulting

- Vault historical revisions offsite to the Cloud
- Storage or a remote location
- Extend offsite-only retention up to 12 monthly and
- 7 yearly revisions

Long-term Retention

- Supports archiving to virtual tapes stored in AWS Simple Storage Service (S3) and Glacier using the AWS Storage Gateway-VTL

Ransomware Protection

- Immutable backup protection
- Hardened Linux platform
- Multi-factor authentication (MFA)
- Secure, air gapped cloud storage
- Role-based access control
- End-to-end encryption
- Ability to create IP/network restrictions

Recovery

- Physical-to-Virtual (P2V) restores
- Bare metal restore for Windows
- With a cloud subscription, download or recover data from anywhere at any time without the need for a local appliance
- Rapid VM recovery with LiveBoot for VMware, and Cloud LiveBoot for VMware and Microsoft Hyper-V environments
- Granular file recovery for VMware and Hyper-V
- File revision history
- Granular Microsoft Exchange message-level recovery
- Customers replicating to AWS have the option to restore backed-up virtualized systems directly to their own AWS environment EC2 compute environment for recovery

Replication

- 256-bit AES encryption of data in transit and at rest to remote locations
- Barracuda's replication technology gives you the flexibility to securely and efficiently send data to the Barracuda Cloud, a remote physical backup appliance, a remote virtual backup appliance, or AWS for offsite replication.
- Because Barracuda manages and optimizes our infrastructure in AWS, setup and configuration of AWS replication is simple—no advanced understanding of AWS required.

FEATURES	
Deployment Options	Physical Appliance, Virtual Appliance
Offsite Replication	Remote Physical Appliance, Remote Virtual Appliance, Barracuda Cloud Storage, Amazon Web Services (AWS)
Management Interface	Barracuda Cloud Control Centralized Administration
Backup Agents	Microsoft Windows (Windows Server, Hyper-V, Exchange, SQL), Linux, macOS
Network Backups	Network Attached Storage (NAS)
Host-Level Virtual Environments	VMware vSphere, Microsoft Hyper-V
Guest-Level Virtual Environments	Citrix XenServer, Kernel-based Virtual Machine (KVM), Oracle VM, Red Hat Virtualization
Deduplication	Global, Inline, Block-Level, Source- and Target-Based
Rapid Recovery	LiveBoot, Cloud LiveBoot, Physical-to-Virtual (P2V), LiveBrowse
Long-Term Retention	Offsite Vaulting to Barracuda Cloud, Export to Amazon Web Services (AWS), External Disk, Tape, Autoloader, Robotic Library

Physical Appliance

MODELS COMPARISON	190	295	290	390	490	690
CAPACITY						
Usable Storage	1 TB	2 TB	2 TB	4 TB	8 TB	12 TB
Recommended Environment	500 GB	1 TB	1 TB	2 TB	4 TB	6 TB
SPECIFICATIONS						
Form Factor	Desktop	Desktop	1U Micro	1U Mini	1U	1U
Dimensions (inches: W x H x D)	9.1 x 1.7 x 6.0	10.0 x 2.0 x 8.3	16.8 x 1.7 x 10.2	16.8 x 1.7 x 14.0	16.8 x 1.7 x 19.8	17.2 x 1.7 x 27.0
Weight (lbs)	4	6	9	12	26	26
Network Interface	1Gb RJ45	1Gb RJ45	1Gb RJ45	1Gb RJ45	1Gb RJ45	2 x 10Gb RJ45
10Gb Fiber SFP+ Transceiver Module (LC Multi-Mode)	-	-	-	-	-	-
Disk Arrangement	1 x 1 TB SSD	1 x 2 TB	1 x 2 TB	2 x 4 TB	4 x 4 TB	4 x 10 TB
Redundant Disk Array (Primary Array)	-	-	-	SW RAID 1	SW RAID 10	SW RAID 10
Dedicated Database and OS Disks	-	-	-	-	-	-
Redundant Disk Array (Database/OS Array)	-	-	-	-	-	-
Swappable Disks	-	-	-	-	Hot Swappable	Hot Swappable
Redundant Power Supplies	-	-	-	-		
Output Power (W)	60W	80W	250W	250W	400W	400W
AC Inputs (VAC)	100/240	100/240	100/240	100/240	100/240	100/240
Site-to-Site Replication	Sender	Sender	Sender	Sender	Sender/Receiver	Sender/Receiver

MODELS COMPARISON	790	890	895	991	995	1091	1191
CAPACITY							
Usable Storage	18 TB	24 TB	36 TB	48 TB	80 TB	128 TB	168 TB
Recommended Environment	9 TB	12 TB	18 TB	24 TB	40 TB	50 TB	60 TB
SPECIFICATIONS							
Form Factor	2U	2U	3U	3U	3U	4U	4U
Dimensions (inches: W x H x D)	17.4 x 3.5 x 25.8	17.4 x 3.5 x 25.8	17.4 x 5.3 x 23.8	17.4 x 5.3 x 23.8	17.4 x 7.0 x 27.9	17.4 x 7.0 x 27.9	17.4 x 7.0 x 27.9
Weight (lbs)	52	52	70	76	114	121	121
Network Interface	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45	2 x 10Gb RJ45
10Gb Fiber Interface SFP+ Transceiver Module (LC Multi-Mode)	OPTIONAL 2-port SFP+	OPTIONAL 2-port SFP+	OPTIONAL 2-port SFP+	STANDARD 2-port SFP+	STANDARD 2-port SFP+	STANDARD 2-port SFP+	STANDARD 2-port SFP+
Disk Arrangement	4 x 12 TB	6 x 12 TB	10 x 8 TB	12 x 10 TB	12 x 10 TB	18 x 10 TB	18 x 12 TB
Redundant Disk Array (Primary Array)	HW RAID 10	HW RAID 10	HW RAID 60	HW RAID 60	HW RAID 60	HW RAID 60	HW RAID 60
Dedicated Database and OS Disks	-	-	-	-	2 x 2 TB	4 x 2 TB	4 x 2 TB
Redundant Disk Array (Database/OS Array)	-	-	-	-	HW RAID 1	HW RAID 10	HW RAID 10
Swappable Disks	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable
Redundant Power Supplies	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable	Hot Swappable
Output Power (W)	800W	800W	1000W	1000W	1000W	1280W	1280W
AC Inputs (VAC)	100/240	100/240	100/240	100/240	100/240	100/240	100/240
Site-to-Site Replication	Sender/ Receiver	Sender/ Receiver	Sender/ Receiver	Sender/ Receiver	Sender/ Receiver	Sender/ Receiver	Sender/ Receiver

Barracuda
Your journey, secured.

PowerEdge R550

DELL Technologies

Hoja de especificaciones

2U, versátil, optimizado de valor y listo para la virtualización

Dell EMC PowerEdge R550, con procesadores escalables Intel® Xeon® de 3.ª generación ofrece flexibilidad agregada para organizaciones que buscan valor excepcional.

Innovación a escala con cargas de trabajo desafiantes y emergentes

El nuevo Dell EMC PowerEdge R550 es un servidor de 2U de doble conector que ofrece el mejor valor para las organizaciones que buscan las funcionalidades más recientes de procesamiento, I/O y almacenamiento. Le permite:

- Agregar núcleos y alimentación adicional: ofrece hasta dos procesadores escalables Intel Xeon de 3.ª generación con un máximo de 24 núcleos por conector
- Optar por memoria más rápida: admite hasta 16 DDR4 RDIMM a 2933 MT/s
- Mejorar el rendimiento y reducir la latencia: con hasta 3 ranuras PCIe Gen4 y 1 PCIe Gen3
- Incluir almacenamiento flexible: admite hasta 16 discos duros de 2,5"SAS/SATA o SSD o hasta 8 discos duros de 3,5" SAS/SATA o SSD
- Soporte para las cargas de trabajo de las pequeñas infraestructuras de TI y la virtualización de trabajos ligeros.

Aumente la eficiencia y acelere las operaciones con una infraestructura de computación autónoma

El portafolio de Dell EMC OpenManage Systems Management domina la complejidad de la administración y la protección de la infraestructura de TI. Con las herramientas intuitivas integrales de Dell Technologies, la TI puede brindar una experiencia segura e integrada al reducir los silos de información y procesos para concentrarse en hacer crecer el negocio. El portafolio de Dell EMC OpenManage es la clave para su motor de innovación, ya que desbloquea las herramientas y la automatización que lo ayudan a escalar, administrar y proteger su entorno tecnológico.

- El streaming de telemetría incorporado, la gestión térmica y la API RESTful con Redfish ofrecen visibilidad y control optimizados para una mejor administración del servidor
- La automatización inteligente le permite habilitar la cooperación entre las acciones humanas y las capacidades del sistema para alcanzar una mayor productividad
- Capacidades de administración de cambios integradas para la planificación de actualizaciones y la configuración e implementación sin problemas y sin intervención
- Integración de la administración de pila completa con Microsoft, VMware, ServiceNow, Ansible y muchas otras herramientas para entornos, incluidas en las instalaciones, la nube y el borde.

Protección incorporada a través de un portafolio completo de soluciones

Desde el silicio y la cadena de suministro hasta el retiro del activo, sepa que los servidores son seguros y cuentan con tecnologías innovadoras de Dell EMC e Intel. Le ofrecemos la confianza de la resiliencia cibernética con seguridad de clase empresarial que minimiza el riesgo para cualquier organización, desde pequeñas empresas hasta empresas de hiperescala.

- Comience de manera sólida con las funciones de seguridad de la plataforma, incluso antes de que se cree el servidor, incluida la verificación segura de componentes y la raíz de silicio de confianza.
- Manténgase sólido con innovaciones continuas que refuerzan la resiliencia cibernética, como el Administrador seguro de claves empresariales de OpenManage y la Inscripción automática de certificados
- Supere las amenazas con inteligencia, automatización y herramientas de recuperación que incluyen telemetría de iDRAC9, análisis en línea del BIOS y Recuperación rápida del SO

PowerEdge R550

Potencie la innovación con Dell EMC PowerEdge R550, el servidor 2U de 2 conectores diseñado para versatilidad y optimizado para valor excepcional.

- Infraestructura de TI pequeña
- VM ligera (densidad de máquina virtual)
- Específico para pequeñas empresas

Características	Especificaciones técnicas	
Procesador	Hasta dos procesadores escalables Intel Xeon de 3.ª generación, con hasta 24 núcleos por procesador	
Memoria	• 16 ranuras DDR4 DIMM, compatible con RDIMM de un máximo de 1 TB, acelera hasta 2933 MT/s • Solo soporta módulos DIMM DDR4 ECC registrados	
Controladoras de almacenamiento	• Controladoras internas: PERC H345, PERC H355, HBA355i, PERC H745, PERC H755, S150 • Inicio interno: módulo SD dual interno, USB, Boot Optimized Storage Subsystem (BOSS-S2): 2 SSD M.2 HWRAID • PERC externo (RAID): PERC H840 • HBA externo (no RAID): HBA355e	
Compartimientos para unidades	Bahías frontales: • Hasta 16 SAS/SATA/NVMe (HDD/SSD) de 2,5 pulgadas como máximo, 122,88 TB • Hasta 8 SAS/SATA (HDD/SSD) de 3,5 pulgadas como máximo, de 128 TB • Hasta 8 SAS/SATA (HDD/SSD) de 2,5 pulgadas, con un máximo de 61,44 TB	
Sistemas de alimentación	• Modo mixto Platinum de 600 W (100-240 V de CA o 240 V de CC) redundante de intercambio en caliente • Modo mixto Platinum de 800 W (100-240 V de CA o 240 V de CC) redundante de intercambio en caliente • Redundante de intercambio en caliente de 1100 W a 48 V de CC (Advertencia: Solo funciona con una entrada de alimentación de -48 V de CC a -60 V de CC)	
Opciones de enfriamiento:	Enfriamiento por aire	
Ventiladores	• Ventiladores estándar (STD) • Hasta cinco ventiladores cableados	
Dimensiones	• Altura: 86,8 mm (3,41 pulgadas) • Ancho:482 mm (18,97 pulgadas) • Profundidad: 721,69 mm (28,72 pulgadas), con bisel 685,78 mm (27 pulgadas) sin bisel	
Factor de forma	Servidor en rack de 2U	
Administración integrada	• iDRAC9 • iDRAC Direct • API RESTful de iDRAC con Redfish • Módulo de servicios de iDRAC • Módulo inalámbrico de Quick Sync 2	
Embellecedor	Bisel de LCD o bisel de seguridad opcional	
Software OpenManage	• OpenManage Enterprise • Complemento de OpenManage Power Manager • Complemento de OpenManage SupportAssist • Complemento de OpenManage Update Manager	
Movilidad	OpenManage Mobile	
Integraciones y conexiones	OpenManage Integrations • BMC Truesight • Microsoft System Center • Red Hat Ansible Modules • VMware vCenter y vRealize Operations Manager	Conexiones OpenManage • IBM Tivoli Netcool/OMNIbus • IBM Tivoli Network Manager IP Edition • Micro Focus Operations Manager • Nagios Core • Nagios XI
Seguridad	• Firmware firmado criptográficamente • Arranque seguro • Borrado seguro • Raíz de silicio de confianza • Bloqueo del sistema (requiere iDRAC9 Enterprise o Datacenter) • TPM 1.2/2.0 FIPS, certificado CC-TCG, TPM 2.0 China NationZ	
NIC integrada	LOM de 2 x 1 GbE	
Opciones de red	1 x OCP 3.0 (opcional)	
Opciones de GPU	No compatible	
Puertos	Puertos frontales • 1 puerto de iDRAC Direct dedicado (Micro-AB USB) • 1 puertos USB 2.0 • 1 x VGA	Puertos posteriores • 1 puertos USB 2.0 • 1 x serie (opcional) • 1 puerto Ethernet de iDRAC • 1 x USB 3.0 • 1 x VGA
	Puertos internos • 1 USB 3.0 (opcional)	
PCIe	3 ranuras PCIe de 4.ª generación + 1 ranura PCIe de 3.ª generación • 3 x16, de 4.° generación, de bajo perfil • 1 x8 de 3.° generación (4 canales) de bajo perfil	
Sistema operativo e hipervisores	• Canonical Ubuntu Server LTS • Hipervisor Citrix • Microsoft Windows Server con Hyper-V • Red Hat Enterprise Linux • SUSE Linux Enterprise Server • VMware ESXi	

Specifications	i5800	i5600
Intelligent Traffic Processing:	L7 requests per second: 1.8M L4 connections per second: 800K L4 HTTP requests per second: 12M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 Gbps L4/L7	L7 requests per second: 1.1M L4 connections per second: 500K L4 HTTP requests per second: 6M Maximum L4 concurrent connections: 40M Throughput: 60 Gbps/35 Gbps L4/L7
Hardware Offload SSL/TLS:	ECC†: 20K TPS (ECDSA P-256) RSA: 35K TPS (2K keys) 20 Gbps bulk encryption*	ECC†: 13K TPS (ECDSA P-256) RSA: 20K TPS (2K keys) 15 Gbps bulk encryption*
FIPS SSL:	N/A	N/A
Hardware Compression:	20 Gbps	N/A
Hardware DDoS Protection:	50M SYN cookies per second	25M SYN cookies per second
TurboFlex Performance Profiles:	Tier 3	N/A
Software Compression:	N/A	12 Gbps
Software Architecture:	64-bit TMOS	64-bit TMOS
On-Demand Upgradable:	N/A	Yes
Virtualization (Maximum Number of vCMP Guests):	8	N/A
Processor:	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processing cores)	One 4-Core Intel Xeon processor (total 8 hyperthreaded logical processor cores)
Memory:	48 GB DDR4	48 GB DDR4
Hard Drive:	1x 480 GB Enterprise Class SSD	1x 480 GB Enterprise Class SSD
Gigabit Ethernet CU Ports:	Optional SFP	Optional SFP
Gigabit Fiber Ports (SFP):	Optional SFP+ (SX or LX)	Optional SFP+ (SX or LX)
10 Gigabit Fiber Ports (SFP+):	8 SR or LR (sold separately); Optional 10G copper direct attach	8 SR or LR (sold separately); Optional 10G copper direct attach
40 Gigabit Fiber Ports (QSFP+):	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)	4 SR4/LR4 (sold separately) (QSFP+ optical breakout cable assemblies available to convert to 10G ports)
Power Supply:	1x 650W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)	1x 650W Platinum AC PSU (Additional PSU optional, 2x 650W DC PSU Option)
Typical Consumption:	265W (single power supply, 110V input)**	265W (single power supply, 110V input)**
Input Voltage:	100-240 VAC +/- 10% auto switching, 50/60hz	100-240 VAC +/- 10% auto switching, 50/60hz
Typical Heat Output:	905 BTU/hour (single power supply, 110V input)**	905 BTU/hour (single power supply, 110V input)**
Dimensions:	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis	1.72" (4.37 cm) H x 17.4" (44.2 cm) W x 30.6" (77.72 cm) D 1U industry standard rack-mount chassis
Weight:	26 lbs. (11.8 kg) (dual power supply)	26 lbs. (11.8 kg) (dual power supply)
Operating Temperature:	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operational Relative Humidity:	5% to 85% at 40° C	5% to 85% at 40° C
Safety Agency Approval:	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	ANSI/UL 60950-1-2014 CSA 60950-1-07, including A1:2011+A2:2014 IEC 60950-1:2005, A1:2009+A2:2013 EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
Certifications/ Susceptibility Standards:	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012 Class A; EN 61000-3-2:2014; EN 61000-3-3:2013; EN 55024:2010; FCC Class A (Part 15), IC Class A; VCCI Class A	ETSI EN 300 386 V1.6.1 (2012); EN 55032:2012 Class A EN 61000-3-2:2014; EN 61000-3-3:2013 EN 55024:2010 FCC Class A (Part 15); IC Class A; VCCI Class A

Notes: Performance-related numbers are based on local traffic management services only. Only optics provided by F5 are supported.
SFP+ ports in i10800, i10600, i7800, i7600, i5800, and i5600 are compatible with F5 SFP modules.

*Maximum throughput.

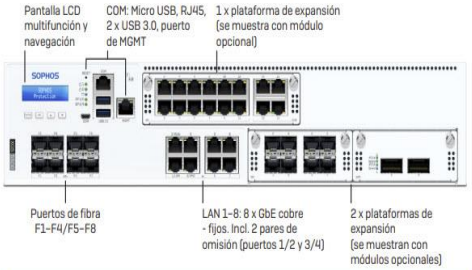
**Please refer to the Platform Guide: i5000/i7000/i10000/i11000 Series for the latest power ratings for your specific configurations (SSL, SSD, highline input voltage, DC, etc.).

†ECDHE-ECDSA-AES128-SHA256 cipher string tested.

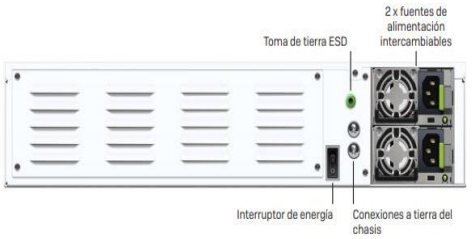
Serie 2U de Sophos XGS: perímetro empresarial
XGS 5500

Especificaciones técnicas

Vista frontal



Vista trasera



Especificaciones físicas	
Montaje	Raíles deslizantes 2U (incluidos)
Dimensiones Ancho x Altura x Profundidad	438 x 88 x 645 mm
Peso	17,8 kg / 39,24 lbs (fuera del paquete) 27 kg / 59,53 lbs (en el paquete)

Entorno	
Fuente de alimentación	2 x 100-240VAC, 50-60 Hz PSU de alcance automático internas e intercambiables
Consumo de energía	168,0 W / 573,81 BTU/h (inactivo) 478,01 W / 1117,43 BTU/h (máx.)
Temperatura en funcionamiento	0 a 40 °C (en funcionamiento) -20 a +70 °C (almacenamiento)
Humedad	10-90 %, sin condensación

Certificaciones de productos	
Certificaciones	CB, CE, UKCA, UL, FCC, ISED, VCCI, BSMI, RCM, NOM, Anatel, KC, CCC, SDPPI Prevista: TEC

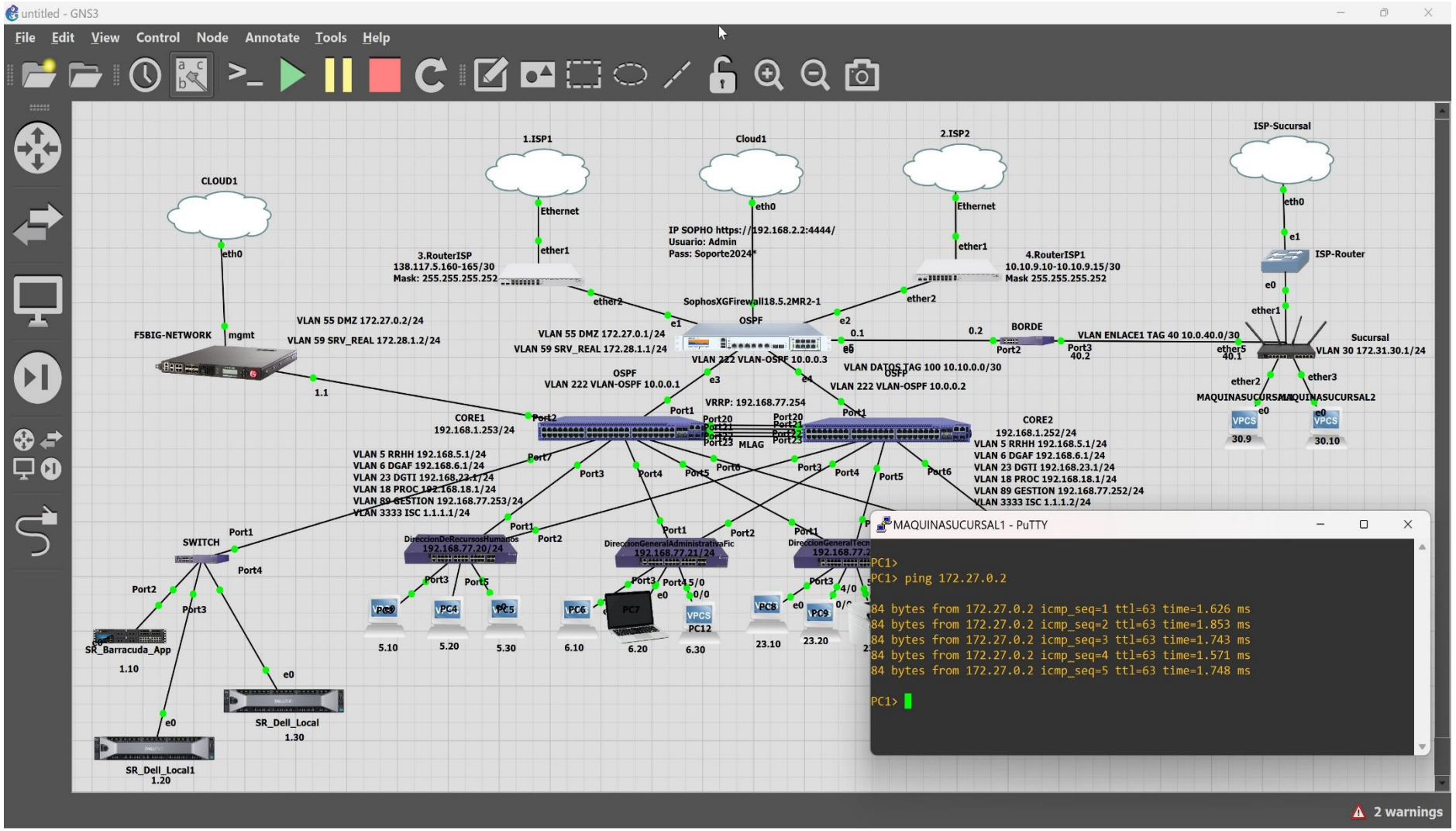
Rendimiento	*XGS 5500*
Rendimiento del firewall	100 000 Mbps
IMIX del firewall	52 000 Mbps
Latencia del firewall (UDP de 64 bytes)	5 µs
Rendimiento del IPS	40 000 Mbps
Rendimiento de la protección contra amenazas	14000 Mbps
NGFW	38 000 Mbps
Conexiones simultáneas	32400000
Conexiones nuevas/seg.	468000
Rendimiento de VPN IPsec	92500 Mbps
Túneles simultáneos VPN IPsec	10000
Túneles simultáneos VPN SSL	15000
Inspección SSL/ TLS de Xstream	13 500 Mbps
Conexiones simultáneas de SSL/TLS de Xstream	512000

Nota: Para obtener información sobre la metodología de evaluación del rendimiento, consulte la página 11.

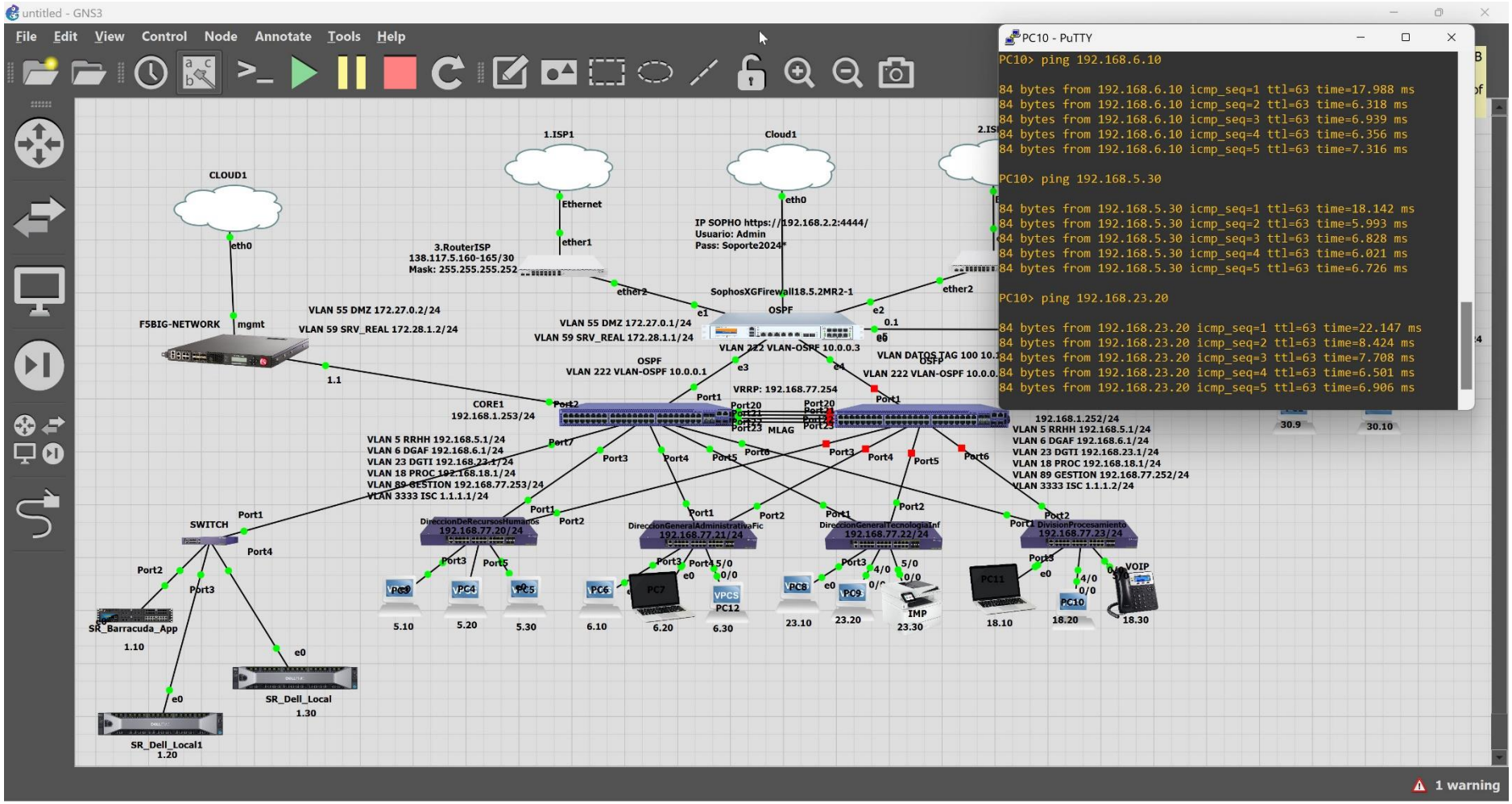
Interfaces físicas	
Almacenamiento (cuarentena local/registros)	2 x SSD SATA-III de 480 GB como mínimo HW RAID integrado en la CPU
Interfaces Ethernet (fijas)	8 x GbE cobre 8 x SFP+ 10 GbE de fibra*
Pares de puertos de omisión	2
Puertos de administración	1 x RJ45 MGMT 1 x COM RJ45 1 x Micro-USB (cable incl.)
Otros puertos de E/S	2 x USB 3.0 (delantero)
N.º de ranuras Flexi Port	2 + 1 para módulo de alta densidad
Módulos Flexi Port (opcional)	8 puertos GbE de cobre 8 puertos GbE SFP de fibra 4 puertos de 10 GbE SFP+ de fibra 4 puertos GbE de cobre de omisión (2 pares) 2 puertos de 40 GbE QSFP+ de fibra 8 puertos de 10 GbE SFP+ de fibra GbE de fibra de 2 puertos (LC) Omisión + GbE SFP de fibra de 4 puertos 10 GbE de fibra de 2 puertos (LC) Omisión + 10 GbE SFP+ de fibra de 4 puertos Módulo de alta densidad (NIC): 12 puertos GE de cobre + 4 puertos 2,5 GE de cobre
Densidad total máx. de puertos (incl. uso de módulos)	48
Conectividad complementaria opcional	Módulo DSL SFP (VDSL2) Transceptores SFP/SFP+
Pantalla	Módulo LCD multifunción

* Los transceptores (mini GBICs) se venden por separado

VPN Site-site



Redundancia Core_1



Redundancia Core_2