Pontificia Universidad Católica del Ecuador | SEDE ESMERALDAS

CARRERA:

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA DE INVESTIGACIÓN:

ANÁLISIS DE RENDIMIENTO DE PUERTAS DE ENLACE VPN MEDIANTE UNA ARQUITECTURA DE RED PARA LA COMUNICACIÓN SEGURA SITIO A SITIO ENTRE LAS PYMES.

LÍNEA DE INVESTIGACIÓN:

ESTUDIO, DISEÑO E IMPLEMENTACIÓN DE REDES DE COMUNICACIÓN DE DATOS

PREVIO A LA OBTENCIÓN DE TÍTULO DE:

INGENIERIO EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR:

BRAYAN GUILLERMO BORJA PIÑEIRO

ASESOR:

MGT. JUAN CASIERRA CAVADA

Esmeraldas – Ecuador
Agosto 2021

Agradecimiento

Ante todo, deseo expresar mi agradecimiento al asesor de la investigación de grado, Mgtr. Juan Casierra. Sin usted y sus virtudes como un gran profesional, este trabajo no lo hubiese logrado de forma natural, gracias por el apoyo brindado a la investigación.

Asimismo, agradezco a quienes fueron mis pilares en cada momento indecisión, mis faros en tiempo de desorientación, con sus sabias palabras, consejos alentadores y motivadores, creyeron en mi potencial y apostaron por mí ciegamente, para alcanzar unas de mis metas más anheladas (Isabel Tapia y Lilian Vera).

Aquellas divisiones como: el departamento de pastoral, departamento de financiero, departamento de TI y departamento de Bienestar, les doy las gracias por acogerme y abrirme sus puertas, por darme la oportunidad de ser parte de sus equipos de trabajo y aportar con mi granito de arena en cada una de estas áreas.

Mi más sincero agradecimiento a la persona que ha sido mi luz, mi guía, mi todo, por el apoyo incondicional, por su amor tranquilizante. Madre, no me cansaré de agradecerte todo lo que has hecho por mí.

Agradezco a mi padre, Marlon Borja Caicedo y a mis hermanos, dado que son mis resortes de vida, sin ustedes no tuvieras las fuerzas necesarias para salir a adelante.

De igual forma, le agradezco a Dios, mi familia y amigos. Todos los que han sido parte de este sendero de mi vida y contribuyeron de forma positiva en mi formación, mil gracias.

Estoy inmensamente agradecido con los maestros por compartir sus conocimientos y permitirme aprender de ellos.

Brayan Borja

Dedicatoria

Ketty Piñeiro de León, el eje de mi existencia a quien le atribuyo todo mi accionar, lo menos que puedo hacer por la mejor mamá del mundo, es dedicarle este trabajo terminado, por ser el soporte que necesité a lo largo de este camino de estudio, también a mi padre, mis hermanos que son mi razón de ser, amigos que confiaron y me supieron dar su apoyo a su manera. También me dedico la investigación por ser la prueba plasmante que todo esfuerzo tiene sus recompensas, por esta razón, les dedico este proyecto a todo los que me ven como un ejemplo a seguir en mis familiares y amigo, donde demuestro que si yo pude todos podemos.

Brayan Borja

Contenido

LISTA DE ILUSTRACIÒN

LISTAS DE TABLAS

RESUMEN

La tecnología de las redes privadas virtuales no es un tema nuevo hoy en día. Con el incremento considerable que se ha venido dando en los últimos años referente a la tendencia de trabajos remotos, conexiones con sucursales y trasmisión de información. Por estas y otras más peculiaridades, las empresas PYMES en vías de desarrollo optan por las arquitecturas de VPN para sus comunicaciones, por lo que deben asumir la responsabilidad que sus comunicaciones sean estables y segura. La presente investigación tiene como objetivo principal analizar tres modernas arquitecturas de VPN, Wireguard, OpenVPN e IPsec con la finalidad de nutrir a la comunidad de empresas PYMES de conceptos clave y actualizados para su implementación. La evaluación está asentada en el rendimiento de las puertas de enlace VPN de software. La etapa de análisis está basada en los efectos de la arquitectura de software y la etapa de implementación, donde se desarrollará un levantamiento puerta de enlace VPN para las arquitecturas de software seleccionadas con herramientas de Mikrotik. Esta investigación indica que, SSL-VPN, IPsec y Wireguard. Son protocolos que en la actualidad le garantizan a las PYMES confidencialidad, integridad, seguridad y velocidad, teniendo en cuenta que la información es cifrada y se envía por el túnel configurado, para el tráfico de paquetes por medios de arquitecturas de red. No obstante, se recomienda WireGuard en para entornos de producción, además esta arquitectura tiene el código de autenticación más seguro en la actualidad por su utilidad, velocidad extremadamente alta, baja sobrecarga por mensaje y agilidad de claves.

Palabras clave: Puertas de enlace, rendimiento, cifrado, autenticación, algoritmo, arquitectura.

ABSTRACT

Virtual private network technology is not a new topic today. With the considerable increase that has been taking place in recent years regarding the trend of remote work, connections with branch offices and transmission of information. Because of these and other peculiarities, PYMES in development opt for VPN architectures for their communications, so they must assume the responsibility that their communications are stable and secure. The main objective of this research is to analyze three modern VPN architectures, Wireguard, OpenVPN and IPsec, to provide the PYMES community with key and updated concepts for their implementation. The evaluation is based on the performance of software VPN gateways. The analysis stage is based on the effects of the software architecture and the implementation stage, where a VPN gateway survey will be developed for the selected software architectures with Mikrotik tools. This research indicates that SSL-VPN, IPsec and Wireguard. These are protocols that currently guarantee SMEs confidentiality, integrity, security, and speed, taking into account that the information is encrypted and sent through the configured tunnel, for packet traffic through network architectures. However, WireGuard is recommended for production environments, in addition this architecture has the most secure authentication code at present due to its usability, extremely high speed, low overhead per message and key agility.

Keywords: Gateways, performance, encryption, authentication, algorithm, architecture.

CAPÍTULO I: INTRODUCCIÓN

1.0 Presentación del Problema

La investigación presente de título “Análisis de rendimiento de puertas de enlace VPN Mediante una arquitectura de red para la comunicación segura punto a punto entre las PYMES” se basará en el análisis del rendimiento de las puertas de enlace o gateway de infraestructuras de red basándose en los diferentes protocolos de redes privadas virtuales más frecuentes en la actualidad para la medición del rendimiento es sus aplicaciones de punto a punto.

La peculiaridad de estas tecnologías de comunicación es asegurar un alta la fiabilidad, estabilidad, velocidad, disponibilidad y seguridad de la red.

La causa de la problemática surge, a razón de las implementaciones poco seguras e inadecuada de las empresas o instituciones respecto a las arquitecturas de red en función de las comunicaciones estables. Conforme a la investigación de análisis de impacto de los ataques de ransonware o secuestro de datos, concluye la presente investigación que en Colombia se registra 87 intentos de ataques por minuto, mencionando que el 19% de empresas fueron afectadas, sobre todo, el 83% de las organizaciones no cuentan con protocolos de respuesta a incidentes de seguridad. Testifica que, las partes vulnerable se encuentran en las políticas de seguridad, configuraciones inadecuadas y debilidad en la infraestructura tecnológica [1].

1.1. Planteamiento del problema

Las puertas de enlaces son dispositivos informáticos que permiten conectarse a redes heterogéneas, con diferentes protocolos que hacen posible la conexión. Su objetivo principal es la conversión de la información transmitida por medio del protocolo utilizado de la propia red, y luego realiza la misma conversión con la red de destino y su protocolo.

Se espera de las redes redundantes tener varias rutas que lleguen al mismo destino, es decir, las arquitecturas de este tipo tienen por definición establecer varios caminos con el objetivo de que si falla una vía se puede redireccionar por otro medio sin causar pérdida o retraso en el envío de paquetes, como, correo, mensajes, imágenes, videos de transmisión, entre otros.

Se puede decir que el tipo de red básica o simple está dividida en dos partes, las que se implementan en dos puntos de conexión en áreas separada.

Según la encuesta del Institute Ponemon el 67% de las empresas PYMES admitieron haber sido atacadas por ciberataque en 2018 [2]. Hoy en día las empresas en vías de desarrollo con proyectos de extensión de sucursales deben asumir la responsabilidad de sus comunicaciones de sitio a sitio, son las responsables de que sus comunicaciones sean segura.

Desde una realidad local e internacional, evidentemente, las empresas PYMES deben enfocarse en la seguridad y calidad de sus comunicaciones, por esta razón, existen muchos protocolos y programas que garantizan la estabilidad, solidez y confiabilidad de la red. Las redes privadas virtuales han sido adoptadas durante muchos años como método de solución a las comunicaciones por su diversidad de beneficios, cabe destacar que, las soluciones desiguales de red conllevan a una calidad de servicio diferente [3] . En cierto modo, la tendencia apunta que los trabajos serán desde el hogar y el uso de las VPN cada vez se hace más visible y necesaria, es por eso por lo que se tiene que conocer bien el uso y como proteger la información enviada, para ello, es de vital importancia el análisis de estas comunicaciones, ya que, se podrá deducir que tecnología es la más fructuosa para sus fines.

Las empresas medianas y pequeñas que disponen de oficinas distantes o trabajadores lejanos, dentro de sus arquitecturas de red, es muy común utilizar la tecnología de intranet. Sin

embargo, las distribuciones internas referente a un diseño de topología malla representa un gran obstáculo para las configuraciones de las VPN, estas barreras se presentan cuando existen conexiones heterogéneas, ya que demandan gran cantidad de información o hace uso de aplicaciones que generen un alto costo de ancho de banda [4][5].

Las interrogantes que se identifican para este estudio se desprenden de la siguiente observación:

Es probable que las empresas en vías de desarrollo no empleen canales seguros y tampoco evalúen sus rendimientos de calidad y enlaces de comunicación, por esta razón, se busca analizar un protocolo, canal seguro o túnel que atreviese las redes públicas. De tal forma, que represente estabilidad y confianza a la hora de transmitir datos confidenciales y clasificados, también se busca analizar el mecanismo de una red, para prevenir errores de retardo en caso falle alguna ruta de transporte.

Si bien es cierto, el internet es pieza clave para la implementación de las VPN y las conexiones de puertas de enlaces, las amenazas de robo de información crecen a razón que la tecnología avanza, sobre todo, los atacantes hábiles utilizan nuevas técnicas de robo de datos colocando en riesgo la integridad e información de los usuarios. Las redes privadas virtuales tratan de brindar un alto estándar de seguridad, relativo a la información enviada por el túnel o canal de conexión; dado que, como el remitente y receptor intercambian datos que están siendo encapsulados y cifrados de punto a punto por el protocolo de nivel superior.

1.2. Justificación

Es un hecho que la prioridad de las redes privadas virtuales es de brindar seguridad a las comunicaciones remotas de los usuarios dentro de una empresa, que necesita de la comunicación a las redes de área local en los ordenadores o dispositivos de sus trabajadores, a fin de que, los procesos existentes dentro de la red interna se puedan ejecutar remotamente, como ejemplo se citaron los siguientes eventos: acceso a la información, teletrabajo, administración de punto de ventas, acceso a sistemas sincronizados de forma segura, entre otros acontecimientos que hacen necesaria la implementación en las cadenas o sucursales de las PYMES [3].

Debido a la alta demanda de VPN existentes por las empresas, es necesario focalizar qué protocolo son los más actuales y los más perfeccionados. La presente investigación se enfocará en el análisis de rendimiento de puertas de enlace VPN mediante una arquitectura, para implementaciones de software en diferentes arquitecturas.

Por medio de este estudio se busca evaluar el rendimiento de las puertas de enlace VPN de software, análisis del efecto de la arquitectura de software, implementaciones rápidas de una puerta de enlace personalizada para todas las arquitecturas de software populares [3], comúnmente se logra establecer un mecanismo de seguridad en las comunicaciones con la implementación de un canal o túnel seguro, para prevenir la suplantación de identidad o phishing, intersección de las comunicaciones, en efecto el frecuente sabotaje informático.

También nutrirá a la comunidad de empresas PYMES de conceptos clave y actualizados al nivel de conocimiento a la hora de sus implementaciones, así mismo, busca orientar a las entidades sobre que arquitectura y protocolo de redes privadas virtuales es el más opcional para el beneficio de la empresa. Con un análisis de VPN bien detallado, las empresas podrán dotarse de conocimiento, prevenir fallos futuros en sus comunicaciones, si no se considera todos los parámetros de un buen estudio puede haber pérdidas de conexión u otro incidente perjudicial, por lo cual, sería una gran baja económica para las PYMES que realizan grandes cantidades de operaciones remotamente.

Este estudio propone entregar evaluaciones de caso comparativo referente al rendimiento de puertas de enlaces, basándose en arquitecturas de redes heterogéneas, empleando las tecnologías de protocolos VPN más comunes en la actualidad.

1.3. Objetivos:

1.3.1. General

Mostrar el protocolo de comunicación VPN de más impacto mediante una arquitectura de red para la comunicación segura sitio a sitio entre las PYMES.

1.3.2. Específicos

- Identificar los tipos de arquitectura de conexión de VPN más utilizados.
- Analizar el rendimiento de las diferentes tecnologías VPN (SSL-VPN, IPsec, WireGuard).
- Establecer la utilidad y el comportamiento del protocolo resultante, fundamentado en el rendimiento de la arquitectura de red seleccionada.

CAPÍTULO II: MARCO TEÓRICO

2.0. Antecedentes de la investigación

A continuación, se presentarán los análisis y las descripciones de investigaciones hechas en relación con el tema de estudio "Análisis de rendimiento de puertas de enlace VPN mediante una arquitectura de red redundante para la comunicación segura punto a punto entre las PYMES", que sirven de base de apoyo a nivel de conocimiento para realizar el análisis de las variables a estudiar, las cuales son: rendimiento de puertas de enlace VPN, arquitectura de red redundante y comunicación segura punto a punto.

La información de la presente investigación fue recopilada de fuentes bibliográficas digitales, tales como IEEE Explore, Scielo y Mendeley. Para la ejecución de la búsqueda se utilizó una metodología basada en un protocolo de búsqueda científica.

De esta manera se utilizó la cadena de búsqueda "(VPN) AND (PUERTA DE ENLACE) OR (ARQUITECTURAS DE RED)" que fue de gran ayuda para recuperar información relacionada con el tema de estudio. Es así como se han recuperado 6 estudios que abarcan relación directa con los protocolos analizar, en efecto, investigaciones de simulación de levantamiento de infraestructura de redes privadas virtuales, junto con la información del rendimiento que obtienen dichos servicios luego de ser implementados. Estos estudios han sido publicados entre el periodo 2016-2021 y serán detallados a continuación.

La investigación estudiada titula "Information and communication system technology with VPN site-to-site IPsec" la cual tuvo como objetivo principal resolver un problema de red en el proyecto de tecnología de la información y la comunicación (TIC) para conectar a través de dos capas conmutadas, pero usando una red diferente. La idea es monitorear los sistemas locales desde un centro operativo directamente desde la red local a través de internet. A manera de metodología se utilizó un estudio que consta de cuatro etapas, análisis del problema, diseño, implementación y pruebas. Como resultado, cabe destacar que, las simulaciones fueron realizadas en la aplicación GNS3 y utilizando dispositivos apropiado. En conclusión, se crearon sistemas de TIC para proporcionar conexión inalámbrica a internet para los visitantes de los

juegos asiáticos en el gimnasio Gelora Bung Karno, remplazando los puntos de acceso y CCTV por clientes de acceso VLAN [6].

Esta investigación se relaciona con el tema de estudio, considerando que proporciona información de las configuraciones y levantamiento de infraestructura mediante simulaciones en la herramienta GNS3, además proporciona datos sobre el enrutamiento que sirve para enviar dato por la capa tres, referentes al modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1).

El segundo artículo investigado lleva como título "A new approach for the securityof VPN". Esta investigación analizó las medidas de seguridad tradicionales de VPN y un enfoque completamente nuevo para la seguridad de VPN mediante el uso de una técnica de cifrado multifase, también presenta un nuevo concepto para aprovechar la gran conveniencia y disponibilidad de Internet de modo que pueda utilizarse como medio seguro para el enlace de las redes privadas virtuales. El procedimiento se llevó a cabo con un método de cifrado muy robusto, complejo, avanzado y seguro, es decir, un algoritmo de cifrado multifase. Se logró con este sistema, mejorar la seguridad e integridad de la carga útil incluso si el medio de comunicación está comprometido, como conclusión de la presente investigación, expone que, las tendencias y tecnologías emergentes modernas, como las redes sociales, las aplicaciones para compartir archivos y las aplicaciones de servicios públicos, rastrean los datos del usuario que se registran para mejorar la experiencia de la aplicación. Por lo tanto, se requiere un medio de comunicación más complejo y seguro para hacer un uso positivo de los servicios [7].

La investigación analizada comparte mucha relación en cuanto al tema que se está investigando, en especial referente a la seguridad de VPN. De igual manera, se hace referencia sobre las técnicas de cifrado multifase, debido a estos algoritmos es posible el encapsulamiento de paquetes de datos.

El tercer artículo analizado tiene como nombre "Performance Evaluation of VPN with Different Network Topologies", mismo que se centra en analizar el impacto del rendimiento con diferentes topologías de red VPN. La metodología se basó, en la evaluación, implementación de máquina de prueba y creación de pequeños entornos LAN para probar el rendimiento. Obteniendo como resultado el rendimiento de la VPN construida con la

herramienta multiprotocolo Softether, que es superior al del protocolo L2TP, en conclusión, se recomienda adoptar una topología en estrella o una topología de árbol, y que el número de capas de la topología de árbol no exceda las tres capas [4].

SoftEther VPN ("SoftEther" significa "Software Ethernet") es uno de los programas VPN multiprotocolo más potentes y fáciles de usar del mundo. Se ejecuta en Windows, Linux, Mac, FreeBSD y Solaris [8].

La tercera investigación es de gran utilidad con relación al tema de investigación propuesto. Según lo analizado, existe una gran variedad de conceptos acerca de lo que representa hoy en día el rendimiento de las VPN. Cabe recalcar que, a través de este documento se obtuvo una mejor visión o perspectiva con respecto a infraestructura, modelos, arquitecturas y topologías, dando así un mejor enfoque a la investigación.

Referente al cuarto artículo analizado de nombre “Análisis de rendimiento de puertas de enlace VPN” centrado en su indagación como objetivo primordial, las investigaciones de diferentes arquitecturas para implementaciones de software de puertas de enlace VPN y su efecto en el rendimiento. Para esta publicación se detalló el método de ejecución, a fin de que se implementara una aplicación de ejemplo de evaluación comparativa de VPN compatible con WireGuard con tres arquitecturas de software diferentes inspiradas en las soluciones de código abierto evaluadas, consiguiendo como resultado, la evaluación comparativa de efectos individuales y optimizaciones de forma aislada, por lo consiguiente, se descubre que WireGuard es la implementación de VPN de software más prometedora desde un punto de vista arquitectónico, por último se determina que, la arquitectura de canalización de WireGuard sobre DPDK logra 6,2 Mbps y 40 Gbit/s, la más rápida de todas las implementaciones de VPN evaluadas. Se descubrió que el principal cuello de botella para escalar las VPN de software son las estructuras de datos y la sincronización de múltiples núcleos, un problema que se puede abordar con una arquitectura basada en la canalización y el paso de mensajes [9].

Este estudio analizado es de vital importancia para asentar las bases de la investigación, tal es el caso, que se considera el más importante sin menospreciar a los de más artículo, pero este es fundamental, ya que, realiza un estudio de comparación de los protocolos OpenVPN, Linux IPsec y WireGuard que es prácticamente uno de los objetivos principal de la investigación.

El quinto articulo examinado tiene como título “Implementación de políticas de tráfico en una arquitectura de red para garantizar la seguridad de acceso y servicios en la PUCESE” en relación con el objetivo principal, la implementación de políticas de tráfico en una arquitectura de red que permita garantizar la seguridad de acceso y servicios de la Pontificia Universidad Católica del Ecuador Sede Esmeraldas (PUCESE). En su desarrollo se adoptó la metodología cualitativa, en la cual se empleó como técnica la entrevista que fue realizada al administrador de la red de la PUCESE, donde se emplearon preguntas de tipo dicotómicas para la obtención de los datos, y para la elaboración de las políticas de tráfico se utilizó el firewall Pfsense de código abierto (open-source). Por tal motivo, el resultado de esta investigación fue un análisis cualitativo donde se encontraron algunas vulnerabilidades que tiene la arquitectura de red de la PUCESE, tales como una mala segmentación de la red, no posee balanceador de carga para controlar el tráfico de manera equitativa y no posee una red privada virtual (VPN) que permita controlar de manera segura el acceso de los usuarios hacia los servicios que brinda la institución. En definitiva, este articulo consigue concluir que las reglas implementadas en el firewall Pfsense permitieron mejorar la seguridad de la arquitectura de red, debido a que su estructura tiene un grado alto de escalabilidad, es tolerante a fallos y posee una segmentación idónea minimizando las vulnerabilidades de los servicios que maneja la institución, además de poseer un control de acceso adecuado que también permitió controlar el tráfico entrante y saliente de la red de manera equitativa y segura [10].

Efectivamente este articulo aporta a la investigación información referente al tráfico de paquete por medio de las arquitecturas de red, por esta razón, es considerado como componente fundamental para lograr realizar las comparativas de rendimiento, además, sirve como hoja de ruta para identificar el cumplimiento de las infraestructuras a nivel de calidad y seguridad.

Terminando con los artículos examinados, el escrito tiene como nombre “Application Specific Tunneling Protocol Selection for Virtual Private Networks” este artículo se fundamenta en analizar diferentes protocolos de tunelización VPN como GRE, IPSec, PPTP y L2TP con IPSec para medir el rendimiento en términos de utilidad, RTT, Jitter y parámetros de seguridad. Según su metodología consiste en implementar los protocolos de túnel que se clasifican en acceso de sitio a sitio (SSL, GRE, IPSec) y VPN de acceso remoto (PPTP, L2TP, MPLS). A modo de los resultados, muestran que GRE es preferible para aplicaciones sensibles al retraso y al ancho de banda en el contexto de VPN de sitio a sitio y L2TP es más efectivo que PPTP

para VPN de acceso remoto. Como conclusión, las aplicaciones sensibles al ancho de banda y al tiempo, como la telefonía por Internet, las videoconferencias, la transmisión de audio / video, requieren propiedades de alto rendimiento y baja latencia, mientras que las aplicaciones como la transferencia de archivos, el correo electrónico y los documentos web no son sensibles al tiempo y tienen requisitos de rendimiento elástico [11].

Este trabajo es pertinente con la investigación, ya que aborda el análisis de diferentes protocolos de tunelización VPN como GRE, IPSec, PPTP y L2TP con IPSec para medir el rendimiento en términos de utilidad, RTT, Jitter y parámetros de seguridad, los cuales son adecuados para el acceso de sitio a sitio y el acceso remoto.

2.0.1 Bases teóricas científicas

En este apartado se detallan las bases teóricas-conceptuales explorada relacionada con la temática de estudio, definiciones según su autoría, conceptos que se describen de manera técnico-científico, se pretende a partir de las bases científica entender los conceptos para el análisis de conexiones de puertas de enlaces en medición de rendimiento.

Las VPN es una red que se constituye por utilizar conexiones públicas, es decir internet, a modo que conecta usuarios remotos u oficinas regionales a la intranet de una empresa en otras palabras a la red interna de la empresa. Su funcionalidad es utiliza estructura pública compartida mientras protege la privacidad a través de procedimientos de seguridad y protocolo de tunelización [12].

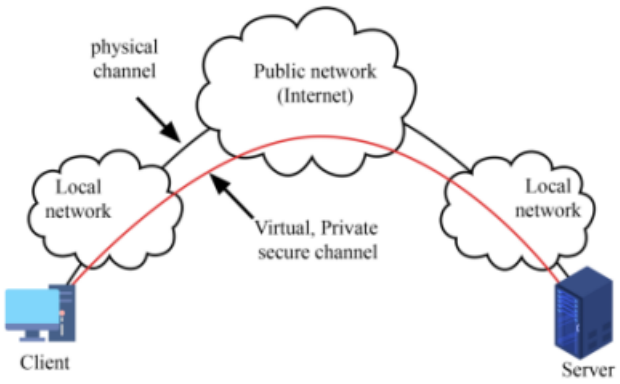


Ilustración 1. Arquitectura VPN [13]

2.1.0. Descripción general de arquitecturas de redes privadas virtuales

las redes privadas virtuales se configuran de diferentes maneras según su uso. Las más comunes entre ellas, de acceso remoto, sitio a sitio, basada en intranet y extranet [13] [14].

2.1.1. VPN de acceso remoto

Permite acceder de forma segura a una red cerrada y abrir todos los recursos o servicios disponible a distancia, beneficiando a quienes utilizan el hogar como puesto de trabajo, es decir, proporciona conexión segura y encriptada entre la red de la organización y la maquina remota [13] [15].

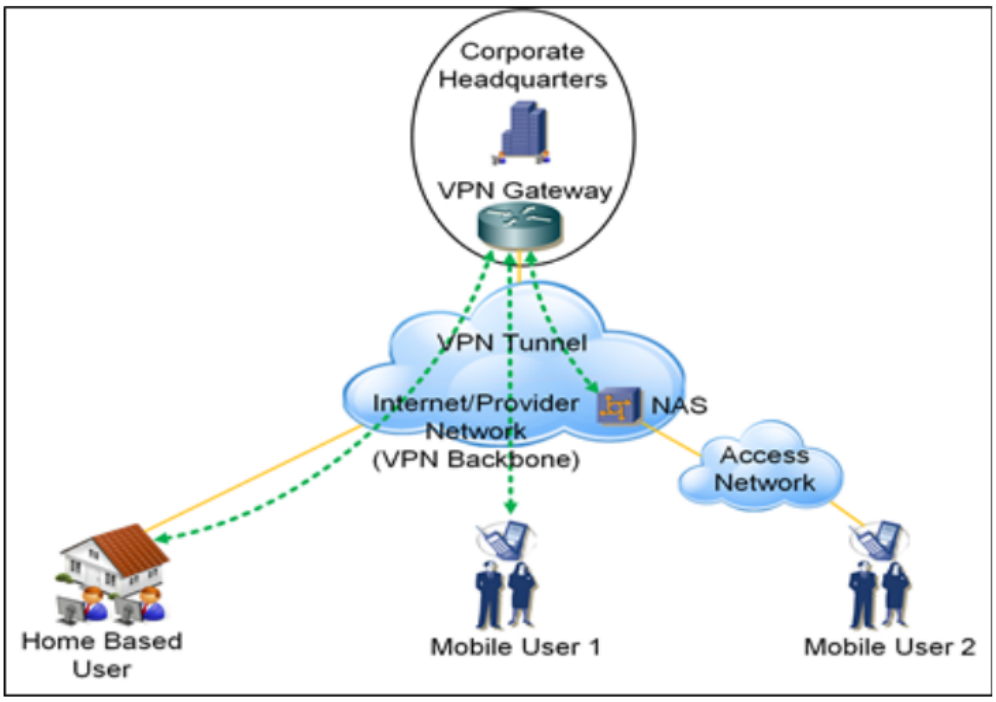


Ilustración 2. VPN de acceso remoto [2]

2.1.2. VPN de sitio a sitio

Permite la conectividad geográficamente en sitios dispersos de una organización, por ejemplo, una oficina central y sucursales, es utilizada para conectar redes de largas distancia a través de la red pública, de forma, que parezca estar situado en una red local [16][2]. Son conocida como VPN de enrutador a enrutador, además de ser aceptada por las grandes empresas [13].

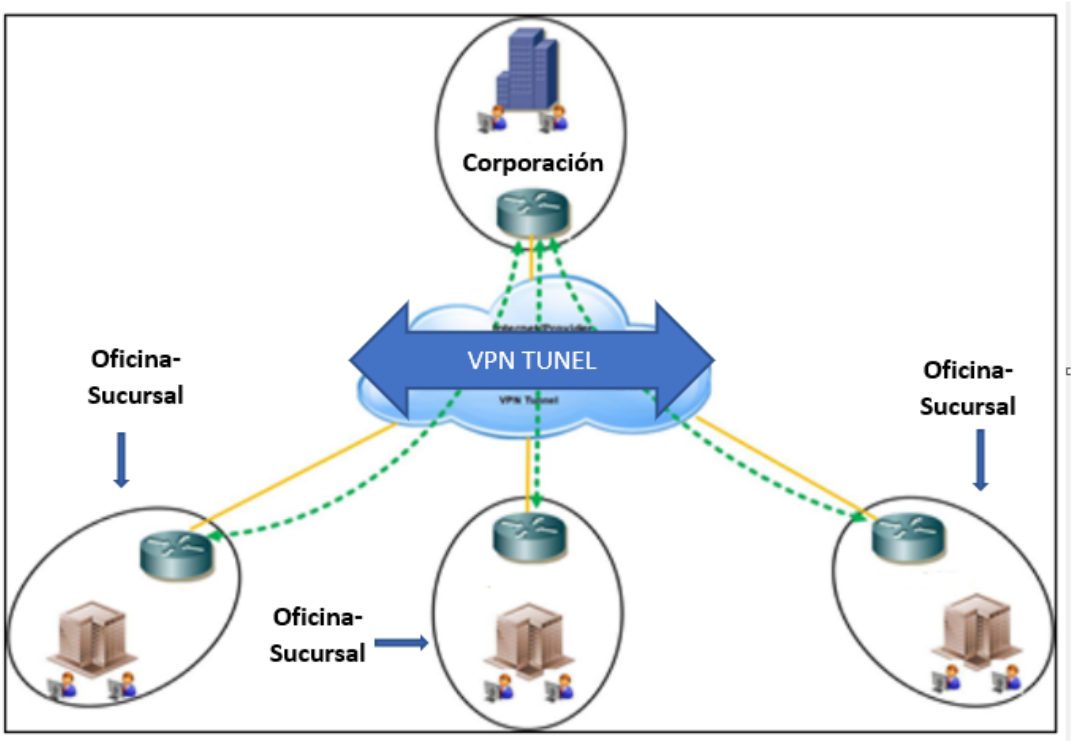


Ilustración 3. VPN sitio a sitio [2]

2.1.3. VPN basada en intranet

Crea una conectividad de la capa de red entre sitios de intranet remotos mediante la creación de una red superpuesta de IP sobre la red no privada, utilizando varios mecanismos de tunelización. Existen dos enfoques para crear dichos túneles, se hace popular cuando muchas oficinas de la misma empresa están conectadas usando el tipo de VPN sitio a sitio [17][13].

- **Enfoque basado en CPE o equipo local del cliente**
  Los túneles se establecen solo en dispositivos CPE
- **Enfoque basado en red**
  Los tuéneles se establecen entre los enrutadores de la red central no privada.

2.1.4. VPN basada en extranet

Este tipo de infraestructura hace referencia cuando las empresas utilizan las redes privadas virtuales sitio a sitio para tener una oficina adjunta a la adicional, sea que, conecta la red de una oficina central a las redes de sucursales remotas teniendo dos principales requisitos [13][17].

1. Compatibilidad con el trasporte de paquetes entre el tráfico de las redes sucursales y unidad central.
2. Soporte para la seguridad de datos.

Hoy en día hay dos tipos de infraestructura de VPN comunes de acceso remoto y de sitio a sitio.

Tabla 1: Comparativa de las infraestructuras sitio a sitio y acceso remoto [15]

Sitio a sitio	Acceso remoto
No requiere ningún cliente software	Requiere software de cliente
Se requiere un Router VPN en el lado del cliente	No se requiere un Router VPN
Todos los sistemas del lado del cliente pueden conectarse a la VPN	Sólo el sistema que está con el cliente remoto puede conectarse
,El cifrado lo realiza la VPN Router	El cifrado lo realiza el cliente de acceso remoto
El nombre de usuario y la contraseña no son para conectarse al servidor central servidor central	El nombre de usuario y la contraseña son necesarios
Requiere un proveedor de servicios dedicado para la comunicación VPN	Puede conectarse a través de cualquier proveedor de servicios
Los protocolos más utilizados son GRE, MPLS VPN, IPSec	Los protocolos comunes utilizados son PPTP, L2TP, IPsec y SSL VPN

2.2.0. Análisis de rendimientos de puertas de enlaces

Mediante el aplicativo GNS3 y Wireshark se pueden calcular varias métricas de rendimiento de VPN, analizando el comportamiento operativo de la arquitectura [18].

Las VPN se pueden implementar en dos escenarios diferentes: configuración cliente-servidor con múltiples clientes que se conectan a un servidor o en una configuración de sitio a sitio que conecta dos ubicaciones con un túnel seguro que maneja muchas conexiones independientes. Este último es más interesante desde el punto de vista del rendimiento, porque representa un cuello de botella potencial en la red y está sujeto a más tráfico que una configuración cliente-servidor. Las interconexiones seguras del centro de datos requieren un alto rendimiento y, a menudo, dependen de dispositivos VPN de hardware especializados. Su alto costo y su naturaleza de caja negra los hacen indeseables para algunos y crean un nicho para las soluciones VPN de software de código abierto que se ejecutan en hardware COTS. Este documento se centra en las configuraciones de sitio a sitio de alto rendimiento, realizadas con software VPN común [9].

MPLS VPN de capa 3

MPLS L3 VPN incorpora la técnica de enrutamiento y reenvío virtual y establece una conexión virtual entre la red de un proveedor de servicios (puede ser una red pública) y los sitios de la red final en lugar de una conectividad dedicada de extremo a extremo. El protocolo de puerta de enlace fronteriza juega un papel vital en el establecimiento de VPN de capa 3 en MPLS. VPN L3 en funciones MPLS en la capa de red. La red del proveedor de servicios debe conocer las direcciones IP de los dispositivos que envían tráfico a través de la VPN y las rutas deben transmitirse y filtrarse en toda la red del proveedor. La VPN de capa 3 requiere información sobre las rutas del cliente y también una configuración de política de enrutamiento y reenvío (VRF) de VPN más amplia que una VPN de capa 2 [18].

Latencia de la red: La latencia es la medida del retraso en la transmisión entre los saltos de origen y destino. En una red, la latencia puede deberse a varios problemas, como problemas de enrutamiento, errores en la interfaz, fragmentación de paquetes, colas de paquetes. Se puede medir de muchas maneras, como de ida y vuelta o de ida. Normalmente, la latencia se calcula como la mitad del tiempo de ida y vuelta. Suele medirse en milisegundos [18].

Rendimiento de la red: El rendimiento es la cantidad de carga de datos que se transmite o recibe en una red. Es la velocidad a la que los paquetes se distribuyen con éxito en una red de comunicaciones. El rendimiento también se conoce como tasa de flujo. El rendimiento se puede medir calculando la proporción del paquete o el tamaño de la ventana TCP por latencia [18].

Pérdida de paquetes: En una red, los paquetes de datos se envían/reciben entre el origen y el destino. Si alguno de los paquetes entre los procesos de comunicación no logra llegar al destino, se considera como pérdida de paquetes en la red. La pérdida de paquetes se calcula por la proporción de paquetes perdidos con respecto al número total de paquetes enviados [18].

Proporción de entrega de paquetes : La tasa de entrega de paquetes se define como el número de proporción de paquetes o datos que se reciben con éxito en el salto de destino en comparación con el número de paquetes enviados desde el salto de origen [18].

Tiempo de retraso de ida y vuelta: El tiempo de demora de ida y vuelta no es más que el tiempo que tarda una solicitud de red en viajar de un nodo a otro y viceversa. Suele medirse en milisegundos. La mitad del tiempo de ida y vuelta da la latencia de la red [18].

Tiempo de convergencia: El tiempo de convergencia es el grado de rapidez con el que los enrutadores alcanzan el estado de convergencia. Es uno de los principales indicadores clave de rendimiento en las redes modernas de alta velocidad. Un grupo de enrutadores que tienen datos de topología idénticos sobre la red en la que manipulan se denomina estado de convergencia. La propiedad de convergencia tiene un impacto principal en los protocolos de puerta de enlace interior, mientras que los protocolos de puerta de enlace exterior nunca dependen de la convergencia [18].

2.2.1. Protocolos que se utilizan en una VPN

Tabla 2: Rendimiento de los túneles VPN IP-sec , WireGuard, OpenVPN [13]*[2]*

Protocolos vpn	**IP-sec**	**WireGuard**	**OpenVPN**
Diseño	complejo	Se centra en la simplicidad y usabilidad	Complejo
Confidencialidad	Sí, el protocolo ESP ofrece confidencialidad	Si	Si
Costo	Alto costo	Bajo costo	Medio
Cifrado	Sí cifrado: modo de transporte y modo de túnel utilizados	Sí, ChaCha20-poly1305 para cifrado simétrico	TLS (AES/BF)
Integridad	Sí, el protocolo AH y ESP ofrece integridad	Si	Si
Velocidad	Se requiere mayor velocidad de procesamiento	alta velocidad en una amplia diversidad de dispositivos	Alta velocidad
Autenticación	Sí, el protocolo AH y ESP ofrece autenticación	Sí, Poly1305 para autenticación	TLS
Seguridad	Bueno	Más seguro que IP-Sec	Buena
Puerto	Puerto UDP 500 y TCP	Utiliza el puerto del protocolo de transmisión UDP 51820	UDP y el puerto 1194

2.3.0. Rendimiento del protocolo

La tabla 2. Muestra las características del resultado final y propiedades de los protocolos WireGuard, IP-sec y OpenVpn.

Tabla 3: Ventajas y desventajas IPsec [13]

	Ventajas	**Desventajas**
IP-SEC	Un gran nivel de implementación en la capa de red	Problemas de compatibilidad debido a diversos estándares
	Controla el tráfico entrante y saliente	Cifrado, descifrado y proceso complejo de tunelización
	Fácil mantenimiento.	El algoritmo de seguridad está en riesgo, el uso de IP Sec está dividido
		Se requiere mayor velocidad de procesamiento

Tabla 4: Ventajas y desventajas WireGuard *[13]*

	Ventajas	**Desventajas**
	WireGuard utiliza criptografía de alta gama para brindar una conexión en línea mucho más segura.	Problemas de seguridad con WireGuard ocurre porque la forma en que está automatizado haría que los proveedores de VPN registraran los datos del usuario
	El procedimiento Wire Guard VPN muestra una base de código menos pesada que OpenVPN e IP Sec, lo	Actualmente, WireGuard solo es efectivo en UDP). Eso significa que posiblemente puede ser

WireGuard	que facilita la verificación al encontrar vulnerabilidades.	bloqueado por un administrador de red. WireGuard es mejor con las distribuciones de Linux.
	El procedimiento Wire Guard muestra mejoras de rendimiento que pueden disminuir el uso de la batería y brindar un mejor mantenimiento de roaming en dispositivos móviles.	WireGuard es más nuevo, lo que significa que no se realizaron muchas pruebas
	Una disminución en la cantidad de código, mucho más seguro, mejor rendimiento y es fácil de usar.	
	WireGuard se creó para ofrecer altas velocidades y los puntos de referencia recientes demuestran que es más rápido que IP Sec y OpenVPN.	

***Tabla 5: Ventajas y desventajas OpenVPN** [8]*

	Ventajas	**Desventajas**
OPENVPN	Estabilidad	No es compatible con IPSec, el estándar actual para soluciones VPN.
	Multiplataforma, conocido por su portabilidad.	OpenVPN realiza una conjunción de soluciones a nivel de capa 2, capa 3 y capa

		7 las cuales no son un estándar de VPN.
	OpenVPN admite el transporte IPv6 (OpenVPN a través de la red IPv6)	Hay pocos fabricantes de hardware que lo integran en sus soluciones
	OpenVPN puede hacer uso de OpenSSL o PolarSSL	
	uso de SSL / TLS para la autenticación de sesión y el protocolo ESP de IPSec para el transporte seguro de túneles a través de UDP	

2.3.1. Tipos de arquitectura de red

Se logra generalmente en las arquitecturas elaborar un plan, para el desarrollo e implementación de una red con protocolos conectados entre sí. En este contexto, se refiere a las tecnologías de diferente infraestructura físicas que admiten a los servicios y protocolos programados que pueden trasladar los mensajes o paquetes de datos. Existe un término muy común en las arquitecturas de red, el cual es: segmentación de redes, en efecto, es la opción más segura de contar con dos redes diferentes físicamente separadas [19].

La separación de funciones, hace parte de las diversas características que tienen las arquitecturas de red, de igual forma, la conexión óptima entre cualquier cantidad de nodos, considerando los niveles de seguridad requeridos, recursos compartidos, administración de red, facilidad de uso, administración de datos, interfaces y aplicaciones [20].

Arquitectura de red básica

Una red básica empieza por un modelo de arquitectura de red separada por zonas, se recomienda fraccionar la red en el número de segmentos de red necesarios para lograr diferenciar y dotar de las medidas de seguridad y control de tráfico apropiados para cada uno de ellos. Esta separación es un concepto seguro y fundamental en la planificación de cualquier arquitectura de red e igualmente aplicable en Sistemas de Control Industrial [19].

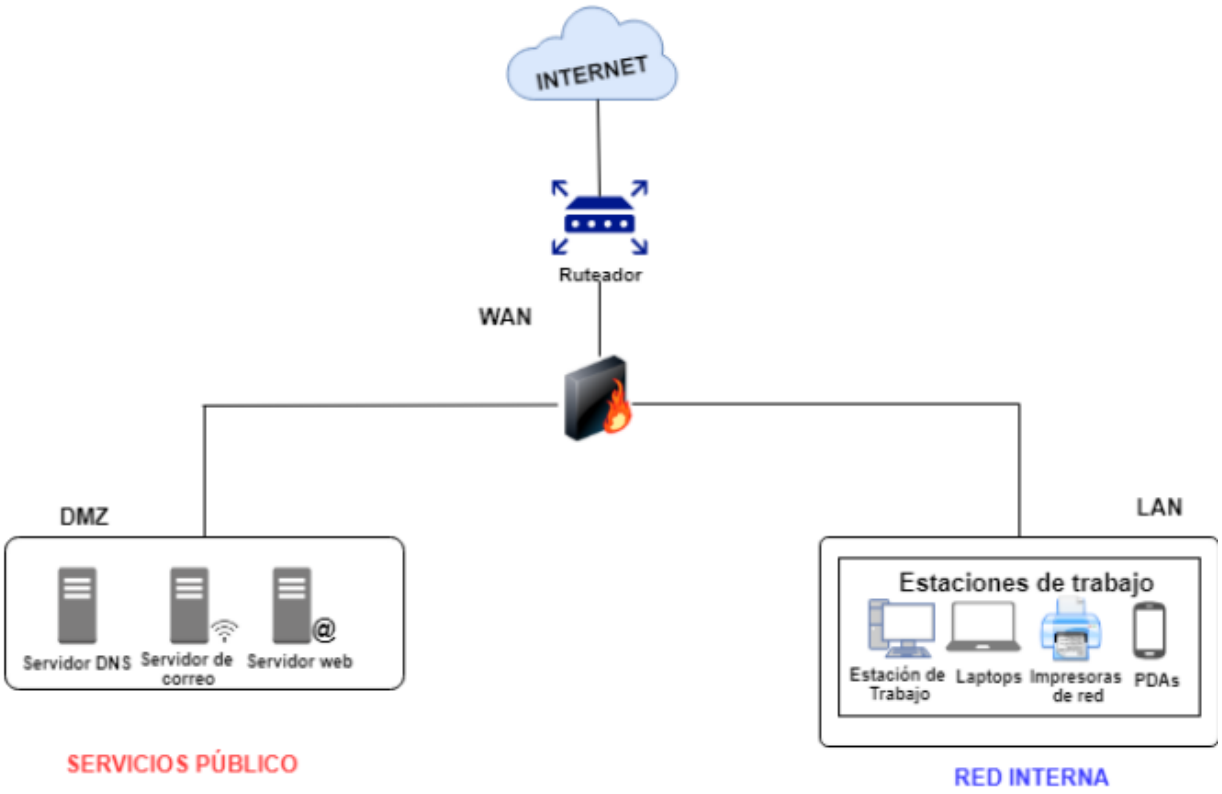


Ilustración 4 Modelo de una red Básica [19].

Arquitectura de red redundante

La segmentación de red es el principio fundamental de la arquitectura redundante, en la ilustración 5 podemos apreciar la conexión de una red redundante que está dividida en dos segmentos, el primer segmento de la parte derecha cuenta con un firewall y la red interna donde se encuentra las estaciones de trabajo (PC, Impresoras, etc.) y los servidores (Base de datos, Dominio, Aplicaciones entre otros) y en la parte izquierda tiene firewall de seguridad para bloquear conexiones no autorizadas a la red, tiene un DMZ (DNS, Correos, WEB) [19].

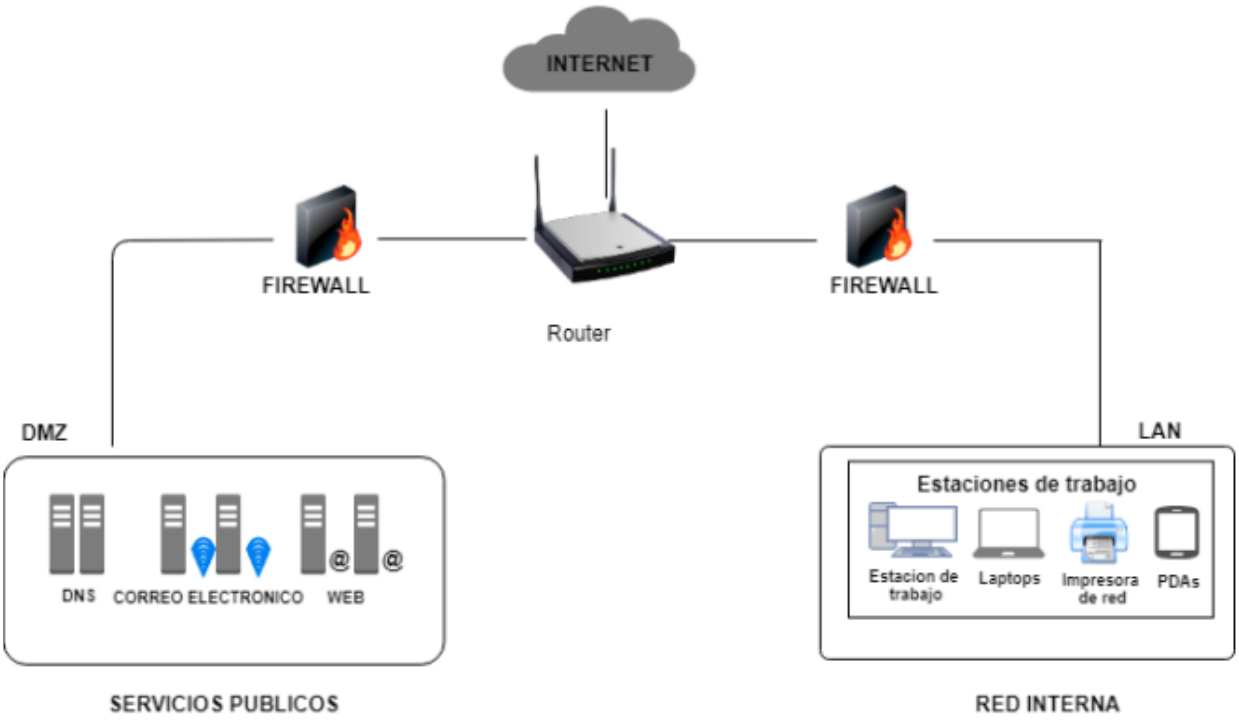


Ilustración 5Modelo de una red Redundante [19].

Arquitectura centralizada

En este tipo de arquitecturas, comienza con la idea de que toda, o gran fragmento de la capacidad de cómputo y almacenamiento de datos, debe estar concentrada en una única zona. En esta infraestructura, todos los usuarios o redes de usuarios acceden a una única red principal, la cual se conecta a un servidor o conjunto de servidores [21].

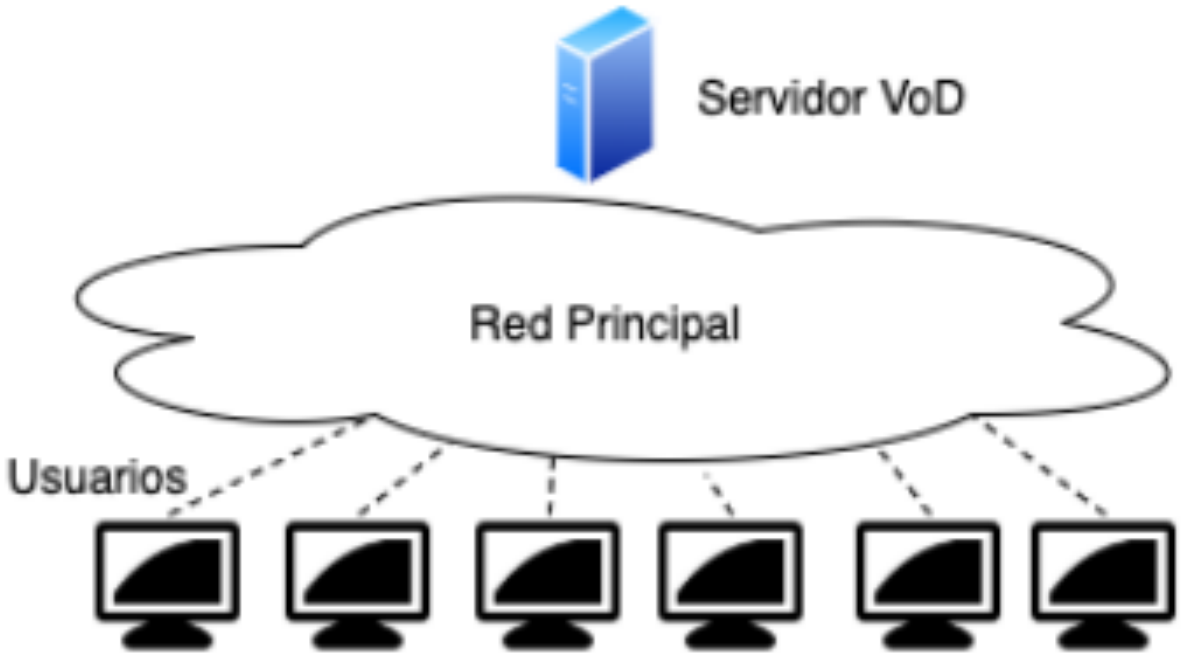


Ilustración 6 Arquitectura centralizada [21].

Arquitectura de servidores independiente

Es una forma de asegurar las posibilidades de escalamiento es implementar una arquitectura de servidores independientes donde los usuarios están separados en subredes locales, de forma que conservan un tráfico de red independiente. Este enfoque complica la administración, ya que requiere dirigir correctamente los servidores en múltiples ubicaciones, teniendo que requerir de personal técnico capacitado en esas locaciones, así como asegurar la seguridad física y lógica [21].

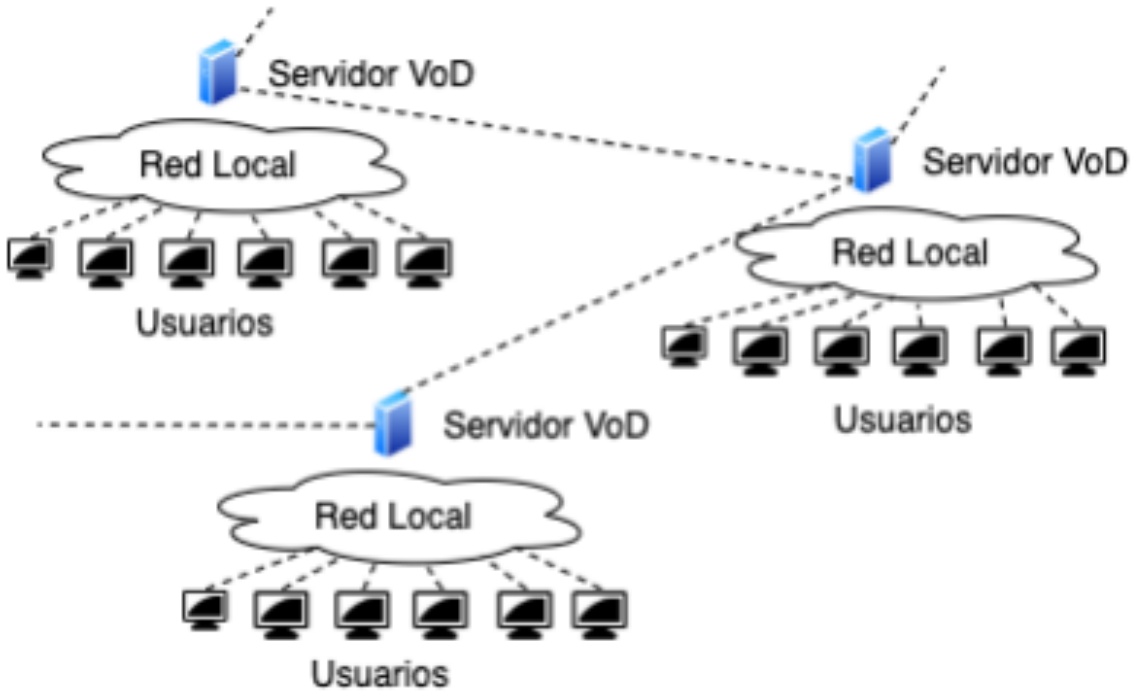


Ilustración 7. Arquitectura de Servidores Independientes[21].

Arquitecturas basadas en servidores proxys

Los servidores proxy de un nivel, son arquitecturas donde los servidores no están interconectados todos entre sí, diferenciándose de la arquitectura de servidores independientes, aquí cuando el usuario realiza una petición a través de la red local, si este se encuentra en el servidor proxy sé devuelve el contenido, mientras que si no lo tiene consulta al servidor central a través de la red principal [21].

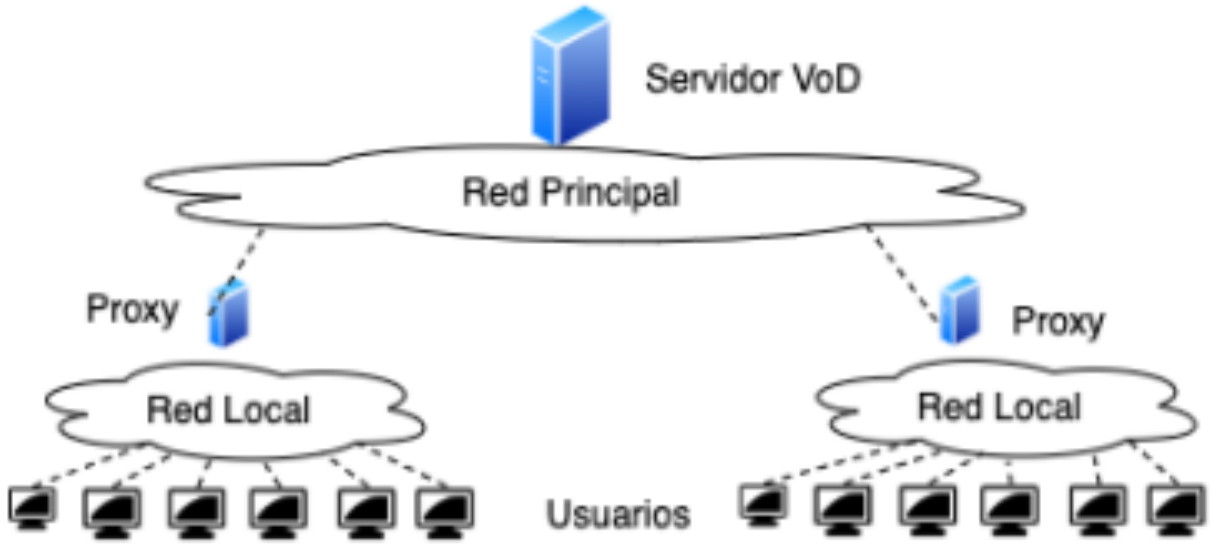


Ilustración 8 Arquitectura tipo Proxy [21].

2.3.2. Tipos de redes

Dentro de los tipos de redes existen términos similares WLAM, LAN Y MAN. Las tecnologías que hay detrás están relacionada con la red de área amplia, pero cada una designa su estructura diferente. Las redes LAN y MAN difieren de las WAN principalmente en su extensión [22].

LAN: acrónimo de *(Local Área Network*) red de área local. Trata de redes pequeñas (hogareñas o empresariales) en donde cada equipo está conectado al resto [20] [22] .

WLAN: (Wireless Local Área Network) red de área local inalámbrica. es en realidad una LAN, que no se realiza a través de conexiones por cable. En su lugar, emplea tecnología inalámbrica, a través de la que los ordenadores individuales se comunican entre sí o están conectados a otra red, como Internet [22].

MAN: del inglés Metropolitan Área Network o Red de Área Metropolitana. Este tipo de red puede definirse como la hermana mayor de la LAN y conecta ciudades y regiones metropolitanas a distancias de hasta 100 km, pero sigue siendo más pequeña que una red WAN [20] [22].

WAN: del inglés Wide Área Network o Red de Área Extensa, en este caso las redes se dan entre países enteros o inclusive pueden alcanzar una extensión continental, las WAN se usan para interconectar la LAN de la empresa a las LAN remotas en las sucursales y las ubicaciones de los empleados a distancia [20] [22].

2.3.3. Elementos de protocolos de VPN

Las VPN están basada en cuatro componentes que se refieren a las fases o etapas en su operación:

Autenticación: comprueba la identidad de los usuarios que emiten y reciben el tráfico antes de empezar la comunicación. **Túnel**: crea un medio de trasporte privado que pasa sobre la red pública, generalmente se encapsula en otro protocolo. **Cifrado**: hace legible la información mientras viaja por el túnel, usando algoritmo de cifrado o encriptación. **Control de flujo**: es la lógica de transferencia para el control de las operaciones entre los procesos de autenticación, el establecer el túnel y envió de los paquetes cifrados controlando el envío y recepción [23].

Autenticación OpenVPN

Dispone de pluralidad de métodos de autenticación al ser de código abierto, este permite la integración de muchos fabricantes y por esto se considera que es muy versátil en las formas como se auténtica OpenVPN, pero las principales son las siguientes: Local, PAM, RADIUS, Asimismo, se pueden usar otras fuentes como LDAP y cualquier plugin que se cree para este fin, cada fabricante debe comprometerse a desarrollar y vigilar las posibles vulnerabilidades de cada método implementado. Pues bien, cualquiera de estos métodos se encapsula en un proceso y viajan de cliente a servidor usando el protocolo llamado OpenSSL para enviar y recibir las credenciales, evitando sean legibles [23].

Autenticación WireGuard

No posee técnica de autenticación de usuarios como tal, sino más bien de dispositivo, aquí es donde el uso de clave pública y privadas son imprescindibles para la autenticación, cualquier cliente que tenga la clave pública del servidor y cuya dirección IP sea incluida en la lista blanca en la configuración del servidor, puede conectarse. A esto se le llama emparejamiento de dispositivos por intercambio de llaves [23].

Autenticación IPSec

Este procolo IPSec permite confirmar que las personas involucradas en la comunicación son en realidad quienes están invitadas. Además, tiene la tarea de afianzar la integridad de los datos, es decir, si alguien los cambia durante la transmisión entre dos partes, los cambios serán identificados y no se les permitirá hacer trampa [24].

2.3.4. Cifrado o encriptación

La fortaleza o debilidad de la mayoría algoritmos de cifrado depende directamente de la longitud de su llave. El número de combinaciones posibles aumenta exponencialmente con el tamaño de la clave y, por lo tanto, la dificultad para forzarlas. Es decir; mientras más bits se usen en la clave de cifrado (encriptado) más dificultoso será el descifrado por fuerza bruta y será obligatorio el uso de supercomputadores para realizar esta tarea [23].

Key Size	Possible combinations
1-bit	2
2-bit	4
8-bit	256
16-bit	65536
64-bit	4.2 x 10^9
128-bit	3.4 x 10^38
192-bit	6.2 x 10^57
256-bit	1.1 x 10^77

Ilustración 9 Longitud de la clave y posibles combinaciones [23].

A continuación, en la siguiente ilustración se mostrarán los años que se llevaría un computador para descifrar según su longitud:

		Types of Character Used				
		Only numbers	Lower-Case Alphabets	Upper & Lower-Case Alphabets	Alphanumeric (Upper & Lower Case)	Every Keyboard Symbol (inc. spacebar)
# of Characters		(Eg. 1234)	(Eg. Password)	(Eg. QwErTy)	(Eg. iAm1337)	(Eg. @$$h0|3l)
		10	26	52	62	95
Password Length	4	0.3 ms	15 ms	24 ms	490 ms	2.7 s
	5	3 ms	400 ms	13 s	31 s	4.3 min
	6	33 ms	10 s	11 min	32 min	6.8 h
	7	330 ms	4.5 min	9.5 h	33 h	27 days
	8	3.3 s	1.9 h	21 days	84 days	7 years
	9	33 s	2.1 days	2.9 years	14 years	670 years
	10	5.6 min	54 days	150 years	890 years	6.3×10^{4} years
	11	56 min	3.9 years	7.9×10^{3} years	5.5×10^{4} years	6×10^{6} years
	12	9.3 h	100 years	4.1×10^{5} years	3.4×10^{6} years	5.7×10^{8} years
	13	3.9 days	2.6×10^{3} years	2.1×10^{7} years	2.1×10^{8} years	5.4×10^{10} years
	14	39 days	6.8×10^{4} years	1.1×10^{9} years	1.3×10^{10} years	5.1×10^{12} years
	15	1.1 years	1.8×10^{6} years	5.8×10^{10} years	8.1×10^{11} years	4.9×10^{14} years
	16	11 years	4.6×10^{7} years	3×10^{12} years	5×10^{13} years	4.7×10^{16} years

Ilustración 10 Longitud de la clave y tiempo para descifrarlo[23].

2.3.5. Estudio previo para el análisis de rendimiento de puertas de enlaces

Conforme a los objetivos de la investigación y tema principal del estudio, se precisa analizar el rendimiento de las arquitecturas de redes privadas virtuales con los siguientes parámetros, seguridad, velocidad, estabilidad y compatibilidad.

Cabe considerar que, para una mayor riqueza de entendimiento sobre el rendimiento de puertas de enlaces, se ha considerado resaltar las conclusiones y resultado del estudio "Performance Analysis of VPN Gateways" mismo que evalúa las arquitecturas y protocolo proporcionado por la investigación.

Para este estudio previo se utilizó dispositivos no convencionales por las en cual consiste en una CPU dual Intel Xeon E5-2630 v4 (un total de 40 núcleos, incluido Hyper Threading) con 128 GiB de memoria y dos NIC Intel XL 710 de 40 Gbit/s [9].
Como se puede notar el hardware utilizado es muy superior a las herramientas que se utilizaron en la investigación, ya que consta de un servidor GNS3 cargado en un CPU de 16 de RAM y 8 núcleos para la simulación.

Según el artículo toda la carga de prueba se generó con scripts MoonGen personalizados que se ejecutan en un servidor separado.

El generador de carga personaliza las direcciones IP de los paquetes y los envía al dispositivo bajo prueba (DuT). El DuT está configurado para cifrar y reenviar todos los paquetes entrantes en el segundo puerto [9].

MoonGen es un generador de paquetes flexible de alta velocidad. Puede saturar enlaces de 10 GbE con paquetes de tamaño mínimo mientras usa solo un núcleo de CPU al ejecutarse sobre el marco de procesamiento de paquetes DPDK. El escalado multinúcleo lineal permite tasas aún más altas: se ha probado MoonGen con hasta 178,5 Mpps a 120 Gbit/s [25].

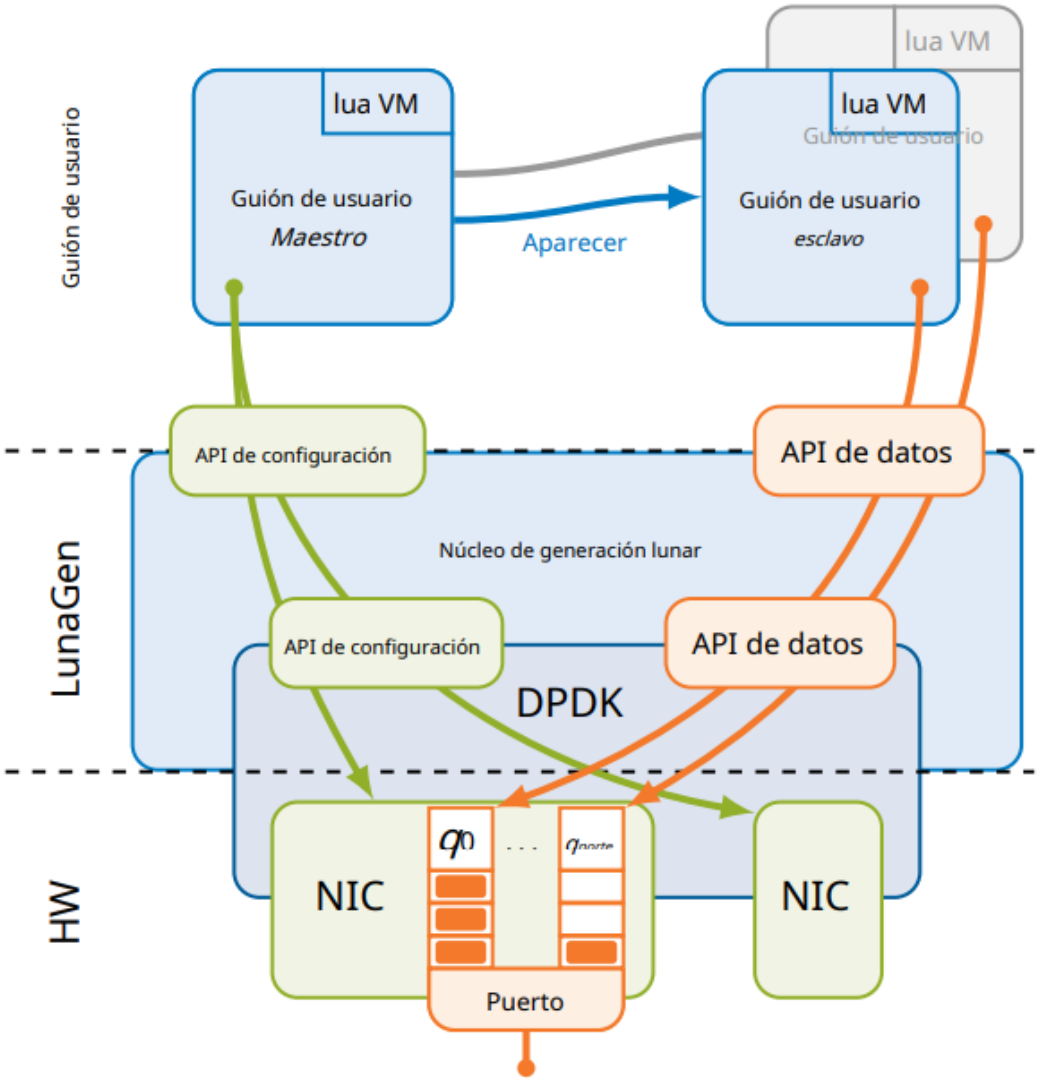


Ilustración 111 Arquitectura de MoonGen [25]

Este estudio en su marco investigativo se enfocó en tres parámetros: Número de flujos: Un flujo generalmente se clasifica por un 5- Tupla de dirección de origen y destino L3, protocolo L4 y puertos de origen y destino L4. Tasa de paquetes: La tasa de paquetes describe cuántos se procesan paquetes por segundo, a menudo dados en Mpps. En su configuración de referencia, se puede establecer una tasa de entrada determinada para el DuT y observar la tasa de salida de los paquetes procesados. Tamaño del paquete: El tamaño del paquete es un factor importante en mediciones, ya que la variación inteligente de los tamaños permite obtener información sobre el funcionamiento interno del dispositivo bajo prueba [9].

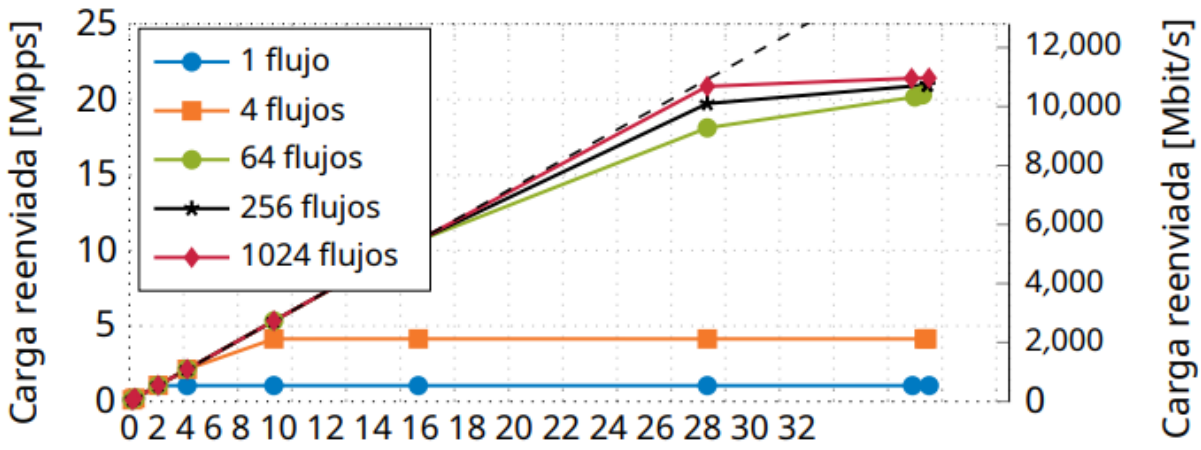


Ilustración 122 Carga de paquetes

En la ilustración 13 muestra las tasas medidas del enrutador Linux con tráfico de paquetes de tamaño fijo y una cantidad variable de flujos. El eje x muestra la carga aplicada al DuT, mientras que los ejes e izquierdo y derecho miden el tráfico que se recibió de vuelta en el generador de carga [9].

Se puede ver que el tipo de tráfico ya tiene un impacto medible en el nivel de enrutamiento: el tráfico que consta de uno o un pequeño número de flujos no se procesa tan fácilmente como el tráfico con muchos flujos. Para un solo flujo de 64 bytes, la tasa de reenvío es, en el mejor de los casos, 1 Mpps, mientras que con 1024 flujos aumenta constantemente hasta alrededor de 21,3 Mpps [9].

Como se ha presentado en este artículo, se midió el rendimiento de las tres implementaciones de VPN de software de código abierto IPsec, OpenVPN y WireGuard en configuraciones de sitio a sitio en hardware COTS que ejecuta Linux. Con los resultados se determinó que ninguno de ellos es lo suficientemente rápido para manejar la cantidad de paquetes en redes de 10 o 40 Gbit/s. Una cantidad considerable de gastos generales proviene de la pila de red subyacente de Linux, en la que se basan todas las versiones probadas. También menciona que Elegir los cifrados criptográficos correctos también puede ayudar. Los cifrados AEAD modernos, como AES-GCM o ChaCha20-poly1305, son mejores que los cifrados tradicionales de cifrado y luego mac [9].

Este artículo Performance Analysis of VPN Gateways, en su informe de 2011 Hoekstra. evaluó el rendimiento de OpenVPN en redes gigabit, centrándose en los cuellos de botella específicos del ancho de banda. Se centraron en las mediciones de rendimiento en términos de Mbit/s en lugar de millones de paquetes por segundo (Mpps) utilizando una MTU predeterminada de 1500 bytes. Para configuraciones seguras (AES-128-CBC con HMACSHA1) midieron un rendimiento máximo de alrededor de 270 Mbit/s. Una comparación más reciente (2017) de Lackovic. Mide el impacto de la compatibilidad con AES-NI en las velocidades de cifrado. En sus puntos de referencia, encuentran una aceleración significativa del 40 % y el 60 % para IPsec AES, y un aumento menor para OpenVPN del 10 % al 16 %. Sus hallazgos sobre AES-NI muestran la misma tendencia que otros resultados, pero siguen siendo un poco más bajos. Informan un aumento del 100 % al 320 % para IPsec en Linux, según el tamaño del paquete (0,48 Gbit/s a 0,94 Gbit/s para 64 bytes y 1,33 Gbit/s a 4,32 Gbit/s para 1462 bytes). Además, Lackovic evalúa las oportunidades de escalado de las VPN y concluye que IPsec es más escalable que OpenVPN [9].

CAPÍTULO III: METODOLOGÍA

3.1. Delimitación de la investigación

La delimitación espacial del proyecto propuesto está destinado a las medianas y pequeñas empresas, no obstante, no se apoyará en una específica.

Para la obtención de la información de impacto respecto a los protocolos a comparar del rendimiento SSL-VPN, Linux IPsec y WireGuard se recurrió a las fuentes bibliográfica IEEE, Scielo y Mendeley. Por medio de las herramientas GNS3 y VMware Workstation se simulará las redes privadas virtuales propuesta en el objetivo específico. Por otro lado, en vista que los protocolos evaluados cambian de versiones constantemente es necesario formular delimitación temporal, donde se manifiesta terminar la investigación (agosto 10 del 2022).

3.2. Tipos de investigación

Este proyecto investigativo es de tipo exploratorio dado que a consecuencia de la investigación se indagó para estructurar, planificar y determinar las diferentes herramientas de redes privadas virtuales para una comunicación segura mediante una infraestructura de red y sus puertas de enlaces.

Cabe resaltar que para este estudio se necesitó de un análisis descriptivo como tipo de investigación que ayude a focalizar las particularidades de cada artículo analizado para hacer las comparaciones con la información compilada en las diferentes herramientas de VPN y las puertas de enlaces.

La investigación también pertenece al tipo de estudio cuantitativo debido que el análisis de rendimiento se representa mediante números los cuales son determinante para realizar las comparaciones.
Dentro este marco se puede decir que esta investigación también es de tipo cualitativo porque permite seleccionar y rescatar explicaciones detallada de cada uno de los artículos basado en las observaciones de sus resultados, naturalmente refuerza el eje de estudio de esta investigación comparativa.

El enfoque mixto cualitativo y cuantitativo (QUAL/QUAN) precisó los comportamientos de los protocolos en las diferentes arquitecturas de redes, las cuales que por medio de políticas de tráfico se pretende encontrar vulnerabilidad de las arquitectura y rendimiento de las herramientas VPN que podrían ser aplicado por las PYMES [10].

Aunque para evaluar y modelar las canalizaciones y composiciones a nivel de hardware se podría utilizar el marco Consultivo, objetivo Bi-funcional y análisis de riesgos (COBRA). Ya que, esta metodología hace referencia al párrafo anterior en los aspecto cualitativo y cuantitativo de manera que agrega una orientación a la estrategia del análisis y evaluación, además en el diseño y la estimación de diversas arquitecturas [26]. No obstante, para esta investigación se utilizó la metodología SGSI basado en la norma ISO 27001 [27].

En efecto, la metodología Sistema de Gestión de Seguridad de la información en su diciplina asociada a las TIC mantiene un objetivo concluyente en los dispositivos que recolectan, procesan, intercambian, almacenan, acceden y transforman la información preservando la integridad, confidencialidad y la disponibilidad de los datos [27].

3.3. Métodos y técnicas

Existen muchos tipos de investigación, estas se diferencian por su finalidad. Por lo tanto, esta investigación está centrada en el método deductivo, ya que para tener un buen análisis que garantice la comunicación segura y el rendimiento se debe tener mucha información que parten de conceptos generales de diferentes bibliotecas digitales que luego son simplificado y concretado para el desarrollo de la investigación.

En el análisis de las puertas de enlaces y toda la información que se recuperó de las diferentes arquitecturas para determinar los efectos causados por cada una, se puede señalar que este estudio se aplicaron los métodos sintético y analítico para obtener el fundamento principal y sintetizar la arquitectura redundante como el centro de la investigación, ya que será la más apropiada para la implementación en las pequeñas y medianas empresas.

En efecto, la técnica de estudio de análisis documental aportó al trabajo la selección de información para el debido análisis de las variables de investigación.

3.4. Población y muestra

La presente investigación no aplicará población y muestras, debido al enfoque que tiene el estudio sobre la observación y la recolección de datos de fuentes bibliográficas de impactos. Por esta razón, el análisis de la red privada virtual para la comunicación segura será planteadas basándose en los resultados arrojados de los artículos evaluado respecto a herramientas de VPN y arquitecturas.

3.5. Descripción de instrumentos

Este trabajo investigativo tiene relación con el articulo "Análisis de rendimiento de puertas de enlace VPN " [9], mismo que consta de tres etapas: evaluación, análisis e implementación. Como instrumento para la recolección de información de la presente investigación se utilizó un laboratorio experimental en el aplicativo GNS3. También, se empleó una de las herramienta más utilizada en el análisis de paquete (Wireshark), esta herramienta va a detectar todo el tráfico encriptado que pasará por la red y de esta manera calcular el rendimiento [28].

Según el artículo "Application of SNORT and Wireshark in Network Traffic Analysis" manifiesta que expertos en seguridad, profesionales de red, educadores y desarrolladores, utilizan Wireshark por ser el analizador de protocolo más extendido y eficiente, generalmente esta herramienta se ejecuta en todas las plataformas UNIX, Linux, OS X y Windows [28].

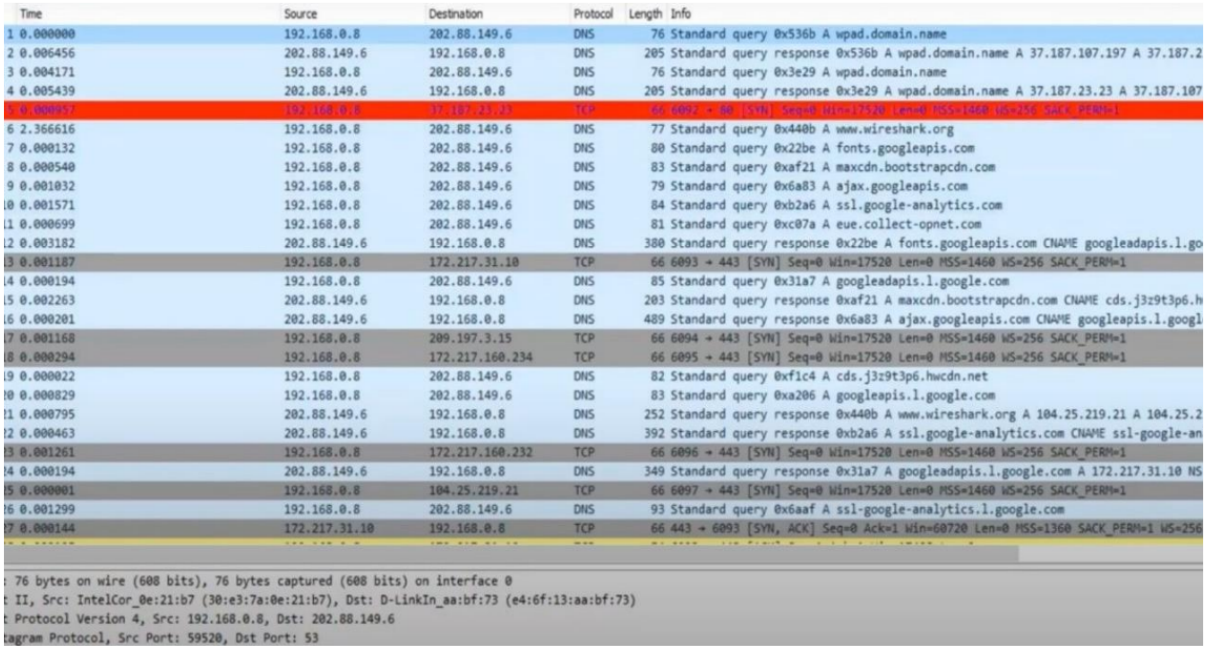


Ilustración 133 Análisis de paquetes de datos.

Dentro de este orden, la evaluación está asentada en el rendimiento de las puertas de enlace VPN de software, mientras la etapa de análisis está basada en los efectos de la arquitectura de software y finalmente la implementación, donde se desarrollará un levantamiento de una puerta de enlace VPN personalizada para todas las arquitecturas de software populares. Este instrumento brinda información sobre la evaluación de tres soluciones multiplataforma de VPN de software open-source más populares SSL-VPN, IPsec y WireGuard. Es fundamentado en una implementación propia de VPN que permite observar si se logra un mayor rendimiento, ya que consta de tres implementaciones de arquitecturas populares para poder compararla de forma separada [9].

3.6. Técnicas de procesamiento y análisis de datos

Para la extracción o procesamiento de datos, la técnica que se utilizó es la estadística descriptiva como el método de referencia que va a permitir analizar los datos del argumento práctico relacionado con el estudio " Implementación de políticas de tráfico en una arquitectura de red para garantizar la seguridad de acceso y servicios en la PUCESE", donde se emplearon preguntas de tipos dicotómica al administrador de red para la obtención de los datos, cabe resaltar que las preguntas están relacionada con el tipo de arquitecturas de red, no obstante,

para esta investigación se desarrolló un laboratorio experimental para la obtención de los datos [29] [30] [10].

En la investigación se establecen técnicas cuantitativas estadísticas con el fin de responder al objetivo de la investigación, por lo consiguiente, para el debido procesamiento de datos es necesario recurrir a organizadores visuales como: tablas o cuadros, listas, gráficos lineales, de barra o circular.

3.7. Normas éticas

De acuerdo con las normas éticas existentes, esta investigación está ligada a normativas y lineamientos inherentes de los parámetros legales actuales en el reglamento de grados de la PUCESE, además se fundamenta en la integridad, profesionalismo y autoría. Referente a los autores mencionados en la investigación, se mantiene una actitud de orden cognoscitivo, objetivo, reflexivo y moral, en el acopio de datos, en calidad de respeto, se mantiene fidelidad al trabajo de cada autor.

CAPÍTULO IV: RESULTADOS

4.1. Arquitecturas de VPN

En este proyecto se identificaron tres herramientas de arquitecturas para medir y evaluar el rendimiento de puertas de enlace VPN mediante una infraestructura de red simulada, para la comunicación segura sitio a sitio, se proporciona por medio de este documento, una revisión de los protocolos y arquitectura más reciente, actuales, de código abierto y segura para la implementación en las PYMES. En efecto, se pudo comprobar que las redes privadas virtuales más actuales son IPsec, OpenVPN y WireGuard conforme a la revisión bibliográfica de este estudio. No obstante, esta indagación instituye que estas arquitecturas analizadas pueden adaptarse las necesidades por sus diversas formas de configuración. Las configuraciones del laboratorio experimental estuvieron sujeta a las limitaciones de las herramientas del fabricante de Mikrotik.

En la presente investigación de forma experimental, se levanta un laboratorio en GNS3, simulando dos lugares diferentes, partiendo de una arquitectura de red sitio a sitio para el debido análisis, además, se utilizó software del del fabricante MikroTik.

Las configuraciones propuestas por el caso de laboratorio experimental están sujeta a las limitaciones del fabricante MikroTik.

4.2. Configuraciones arquitectura (SSL-VPN, IPsec, WireGuard)

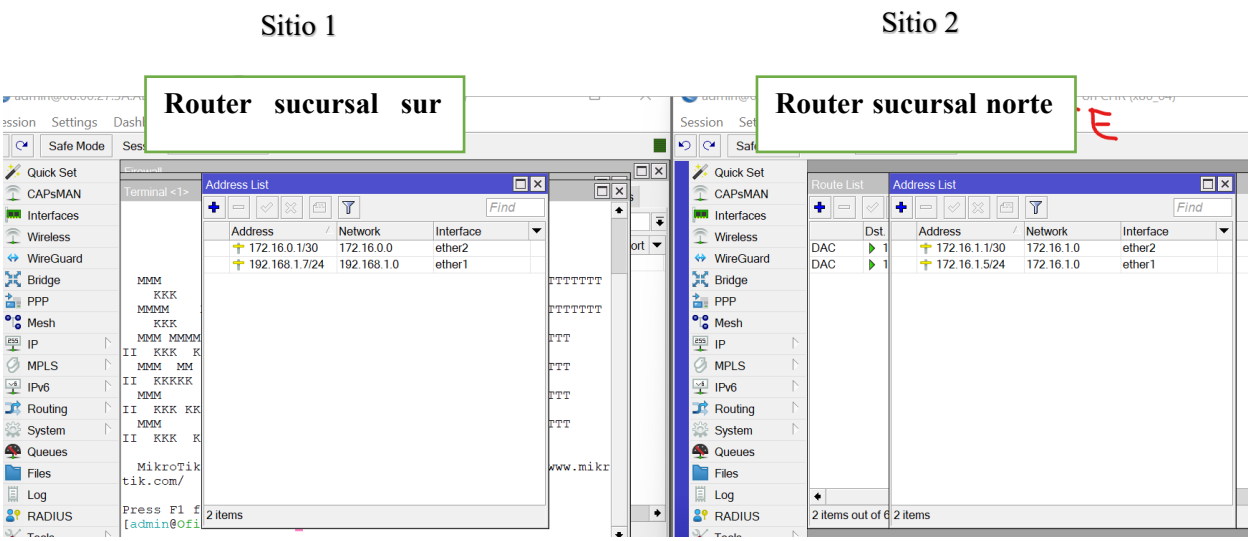


Ilustración 14 Configuración de Router sitio a sitio

En particular, es importante saber que, para el desarrollo del laboratorio, los Routers ya están configurados con los principios básicos y elementales tales como: direccionamiento de IP, habilitar los DNS, regla de Nat para la salida a internet y configuración de ruta.

Arquitectura VPN IPsec

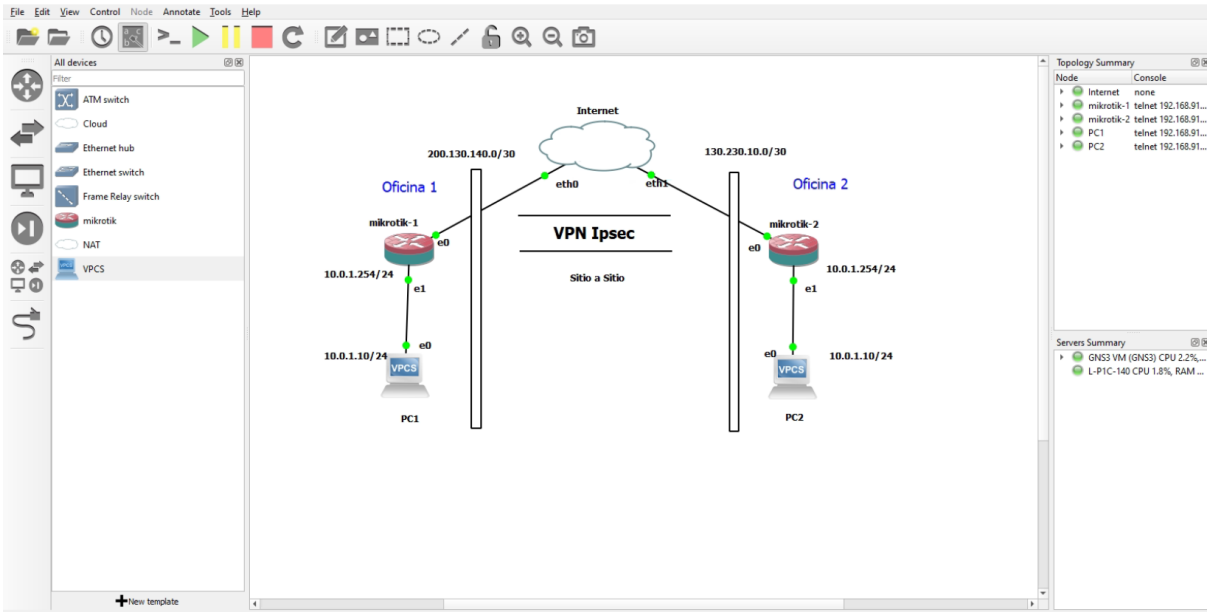


Ilustración 15 Arquitectura VPN IPsec

Tabla 5: Configuración del ambiente de prueba IPsec

Configuración	Oficina sur o sitio 1	Oficina norte o sitio 2
Configuración de Peer	x	x
Configuración de identidad (seleccionar el Peer creado)	X	X
Configuración de políticas de conexión sitio a sitio	X	X
Seleccionar el modo túnel	X	X
Regla de NAT	X	X

En la tabla 5, se muestran los pasos como se crea una VPN básica mediante el protocolo IPsec. Para el levantamiento de la arquitectura se utilizó los Routers de Mikrotik versión 7.4.1 estable, con la finalidad de obtener resultados ecuánimes con las demás infraestructuras.

Para el previo análisis de la arquitectura, como se ha mencionado ante, por medio del comando ping: instrumento que se utiliza comúnmente en el campo de las redes por sus diversos beneficios, se ha comprobado la velocidad de entrega y respuesta de paquetes.

Después de analizar la arquitectura, se puede concluir que a diferencia de WireGuard y OpenVPN, en esta arquitectura no se creó una interfaz para realizar la conexión sitio a sitio, requiere de mecanismos opcionales para dicha implementación, no obstante, todo el tráfico es soportado por la regla de NAT.

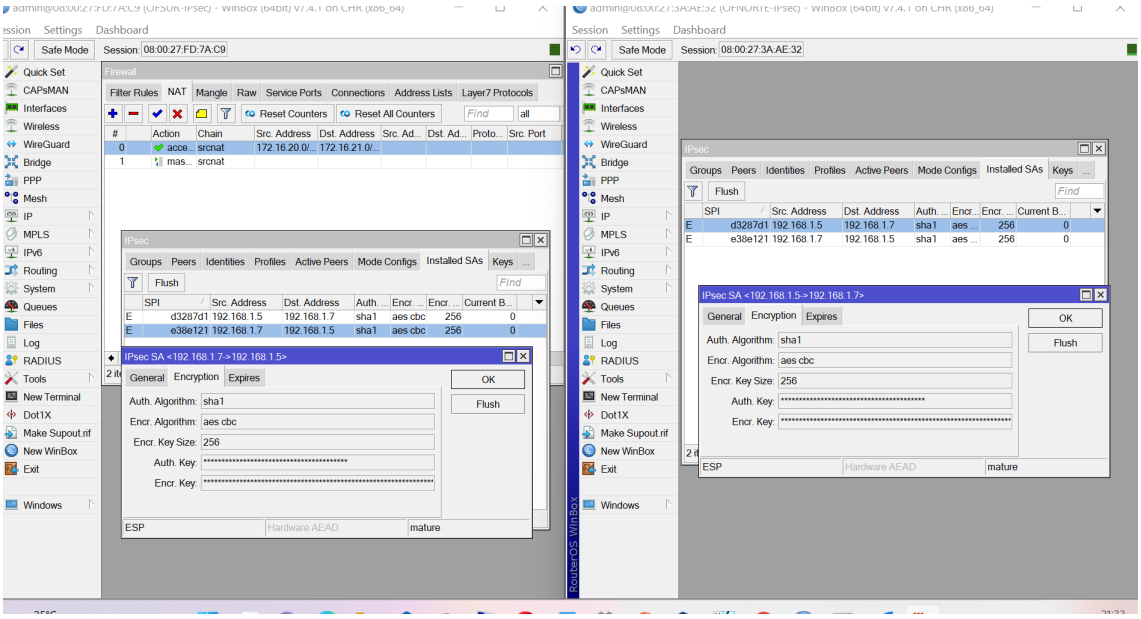


Ilustración 16 Encriptación y autenticación IPsec sitio a sitio

Como se puede visualizar en la ilustración 15, para el despliegue de esta arquitectura, se utilizó como algoritmo de encriptación SHA -1.

Según el artículo recopilado de la prestigiosa revista IEEE "Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA-2 and Modified SHA" indica que el algoritmo seleccionado para el desarrollo de la simulación es el más famoso y seguro, así mismo como SHA -2 [31].

SHA-1 fue publicado por el NIST en 1995. El SHA-1 mantiene una salida hash de 160 bits a través de 80 pasos de evaluación de la función de compresión. El SHA-1 se considera parte de las funciones de Merkle Damgard, donde el mensaje de entrada se divide en varios bloques y se procesa secuencialmente. El SHA-1 toma un mensaje de un tamaño predefinido y lo procesa usando la función de ronda SHA-1F [31].

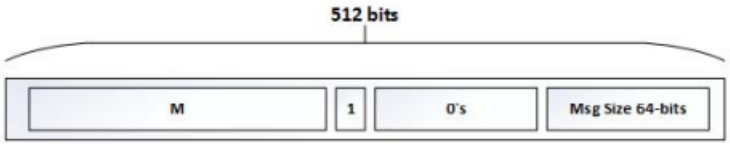


Ilustración 187 Relleno del mensaje antes del procesamiento [31]

En esta fase se incluye el preprocesamiento donde se rellena el mensaje para hacer su tamaño congruente con 512-bits. El relleno se realiza agregando "uno", el menor número de ceros y el tamaño del mensaje de 64-bits, como se muestra en la Ilustración 17 [31].

Después del relleno, el mensaje se divide en bloques de igual tamaño (Bi) cada uno de 512 bits. Cada bloque se divide en 16 palabras de 32 bits y se expande en 80 palabras de 32 bits utilizando la Ecuación (1), que produce 2560 bits. Estas 80 palabras están representadas por el Wt en el diagrama de bloques funcional del SHA-1, como se muestra en la ilustración 17. Las palabras de bloque se asignan a las primeras 16 palabras del Wt y el resto de las palabras expandidas se calculan utilizando estos valores y la ecuación de expansión del mensaje. La figura muestra que se utilizan cinco variables de estado de trabajo (A, B, C, D y E) para evaluar el valor hash intermedio después de cada paso. Estas variables se inicializan con valores hexadecimales fijos de 32 bits (H0=67452301, H1 =EFCDAB89, H2=98BADCFE, H3=10325476, y H4=C3D2E1F0) [31].

A pesar que, el algoritmo AES de AES-128 bits, tiene un tiempo de procesamiento relativamente más rápido en comparación con AES de 192 bits y AES de 256 bits conforme al artículo “Comparision of AES 128, 192 and 256 bits algorithm for encryption and description file” donde indica que, El uso de CPU utilizado para procesar el cifrado y descifrado de archivos basado en pruebas con algoritmos AES de 128 bits, 192 bits y 256 bits ha concluido que AES 192 tiene un porcentaje de uso de CPU que tiende a ser menor que AES de 128 bits o 256 bits, aunque en ciertos archivos tienen mayor porcentaje, también menciona en el resultado de la investigación que AES de 128 bits tiene el tiempo de procesamiento más rápido. Mientras que, en el momento del descifrado de archivos, AES de 128 bits tiene el tiempo de procesamiento más rápido en archivos con forma de archivo WinZip, archivos de Excel, imágenes, texto y video [32].

Para esta implementación se utilizó el algoritmo AES -256(Advanced Encyption Standard) como indica en la ilustración 16, con el fin de reforzar la seguridad e integridad de los paquetes.

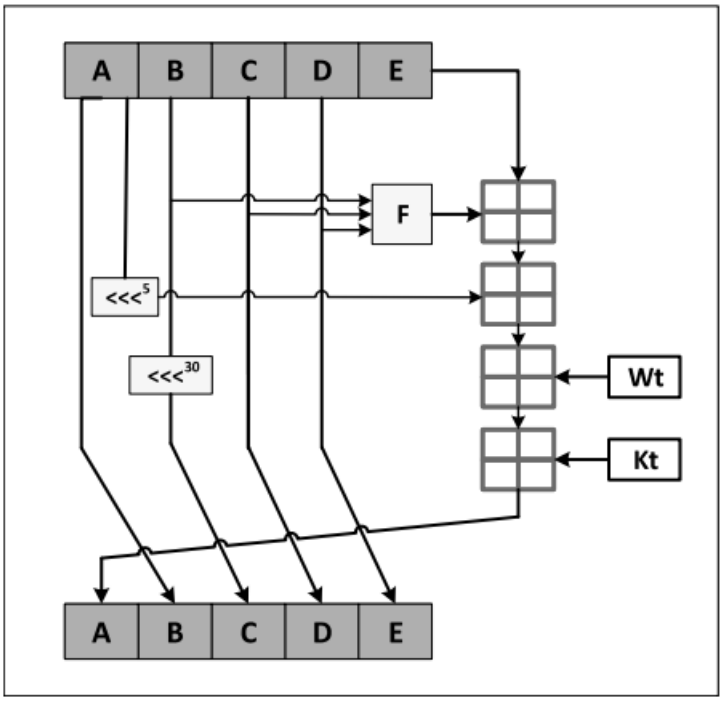


Ilustración 18 Bloque de funciones del SHA-1 [31]

A continuación, en la ilustración 19, se hace énfasis al análisis de tráfico por medio de la ruta o regla de NAT, ya que esta arquitectura no crea una interfaz para su conexión, donde se determinó que la velocidad de trasmisión de IPsec es superior a OpenVPN e inferior a WireGuard, dato que sorprendió en la investigación, dado que se esperaba que OpenVPN sea mayor en término de velocidad que IPsec, porque según IPsec necesita de otros medios para aumentar su rendimiento.

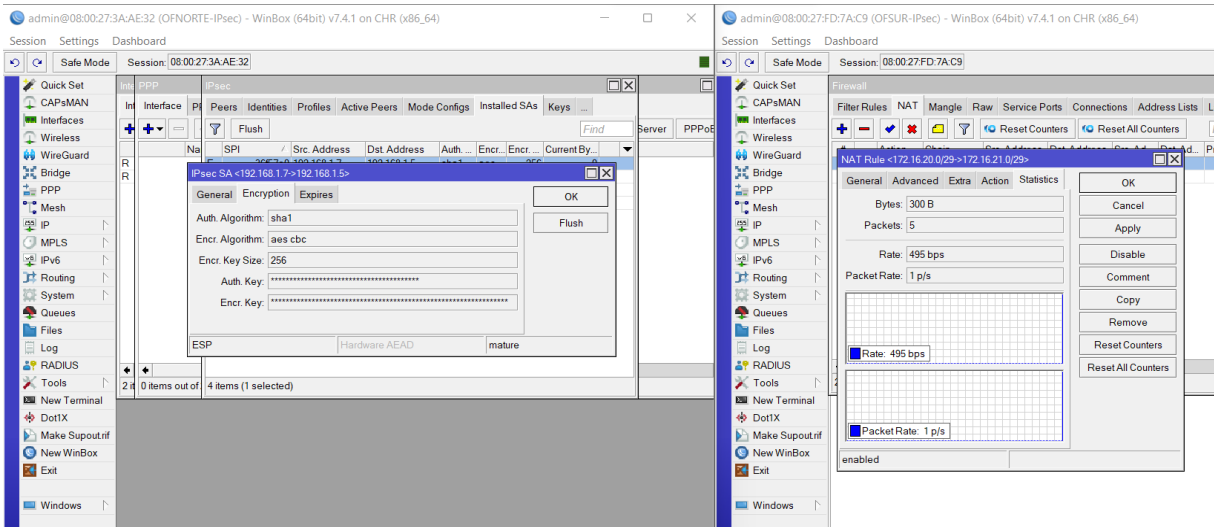


Ilustración 1919 Captura de tráfico VPN IPsec

Arquitectura OpenVPN

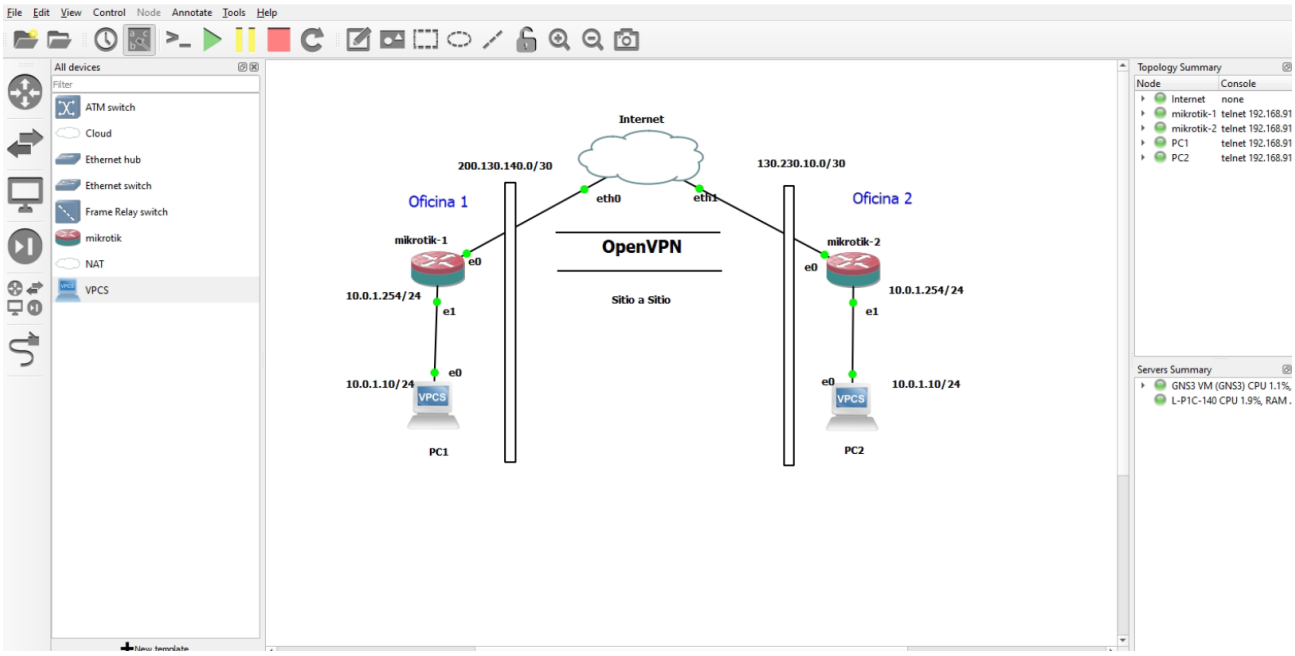


Ilustración 20 Arquitectura OpenVPN

Tabla 6: Configuración del ambiente de prueba OpenVPN

Configuración	Oficina sur o sitio 1	Oficina norte o sitio 2
Configuración de los certificados SSL (Exportar)	x	

Importar los certificados SSL (Importar)		x
Configuración perfil	x	
Configuración de Usuario	x	
Configuración de server 0	x	
Configuración de interfaz		x
Configuración de firewall (abrir puerto 1194)	x	
Regla Nat	x	
Configuración de rutas	x	x

En la tabla 6, se expone como se crea una VPN básica mediante el protocolo OpenVPN. Para el despliegue de la arquitectura se utilizó los Routers de Mikrotik versión 7.4.1 estable, considerando los dispositivos y recursos que se utilizaron en las demás simulaciones.

Cabe aclarar que, las configuraciones de encriptación y autenticación son similares al protocolo IPsec como se muestra en la siguiente ilustración.

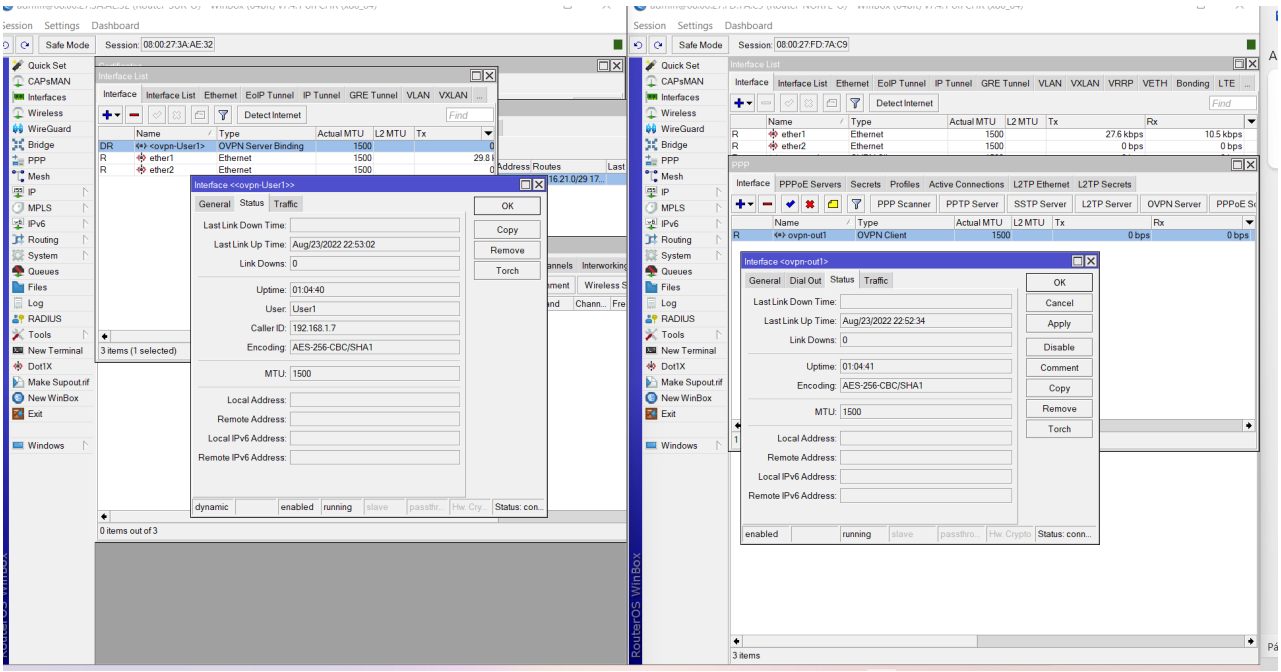


Ilustración 201: Configuración de encriptación y autenticación

Para comprobar el parámetro de la velocidad, por medio del comando ping: instrumento que se aplicó a los demás protocolos, se ha comprobado que la velocidad de entrega y respuesta de paquetes es inferior a Ipsec y WireGuard.

A continuación, el análisis del tráfico de la interfaz OpenVPN:

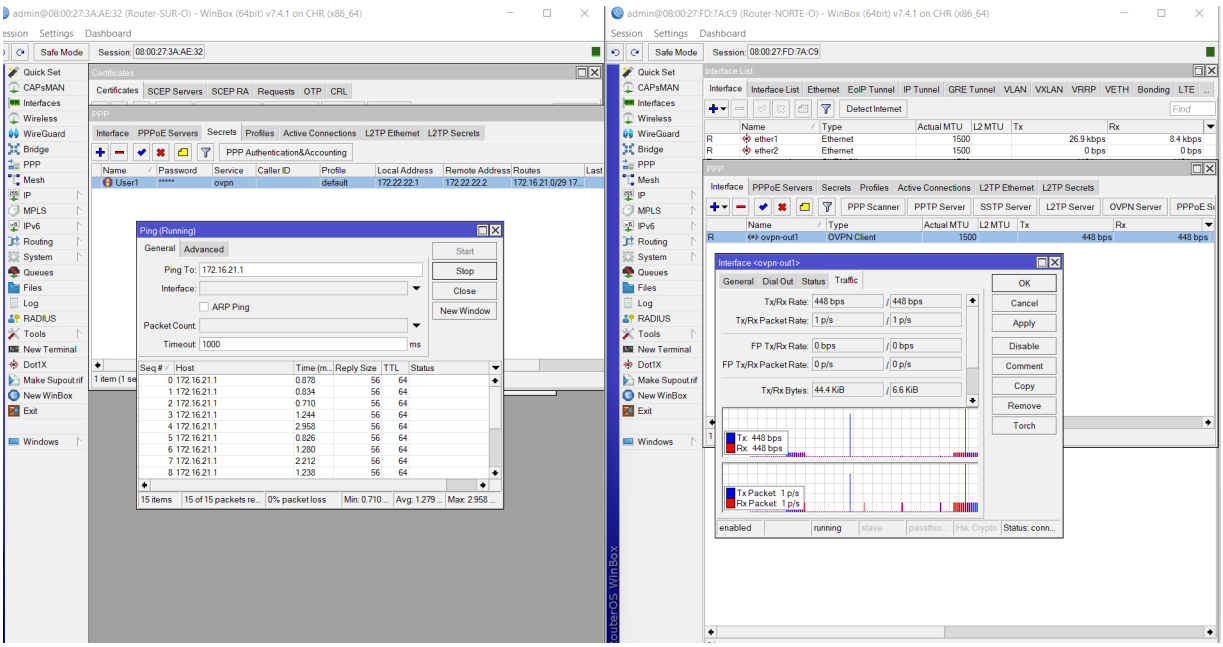


Ilustración 212 Trafico interfaz OpenVPN

Arquitectura WireGuard

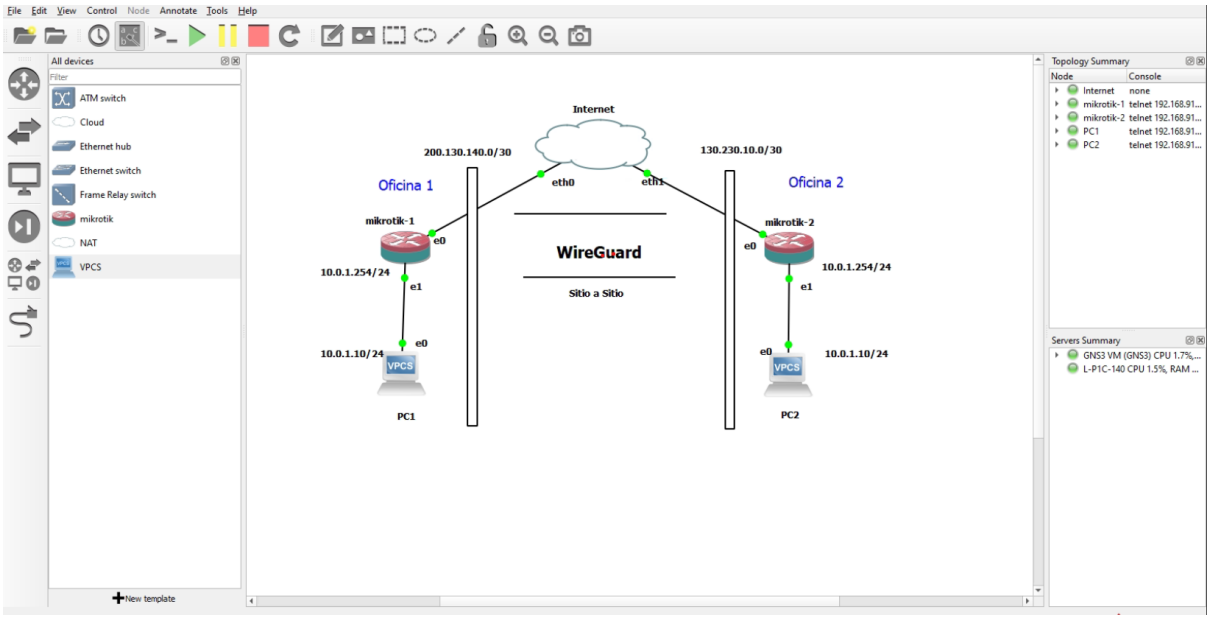


Ilustración 223 Arquitectura WireGuard

Tabla 6: Configuración del ambiente de prueba WireGuard

Configuración	Oficina sur o sitio 1	Oficina norte o sitio 2
Se crea la interfaz por el puerto 13231	x	x
Llaves privadas y públicas	x	x
Direcciónamelo, IP a la interfaz de WireGuard	x	x
Configuración de Peer sobre la interfaz ireGuard	x	x

Ruta para para la interfaz de WireGuard	x	x

En la tabla 5, se muestran los pasos como se crea una VPN rápida, confiable y segura. Para el levantamiento de la arquitectura se utilizó los Routers de Mikrotik versión 7.4.1 estable, ya que en versiones anteriores no se encuentra en protocolo WireGuard.

Para el previo análisis de la arquitectura, es preciso conocer cómo se realiza la encriptación de los paquetes, por medio del comando ping: instrumento que se utiliza comúnmente en el campo de las redes por sus diversos beneficios, se ha comprobado la velocidad de entrega y respuesta de paquetes.

WireGuard: trabaja con el cifrado simétrico ChaCha20, esta técnica de encriptación nace con el cambio de llaves privadas y públicas. Los sitios u oficinas de esta investigación generaron sus propias llaves privada y una pública, la llave pública es compartida por ambas localidades. Este cifrado inspeccionado cifró la información, carácter por carácter debido a su naturaleza de flujo y no por bloque. Mediante el código de autenticación Poly1305 que utiliza la construcción AEAD, según estudios y los artículos revisados, mencionan que es el mejor código de autenticación por su utilidad: velocidad extremadamente alta, baja sobrecarga por mensaje, agilidad de claves, entre otras.

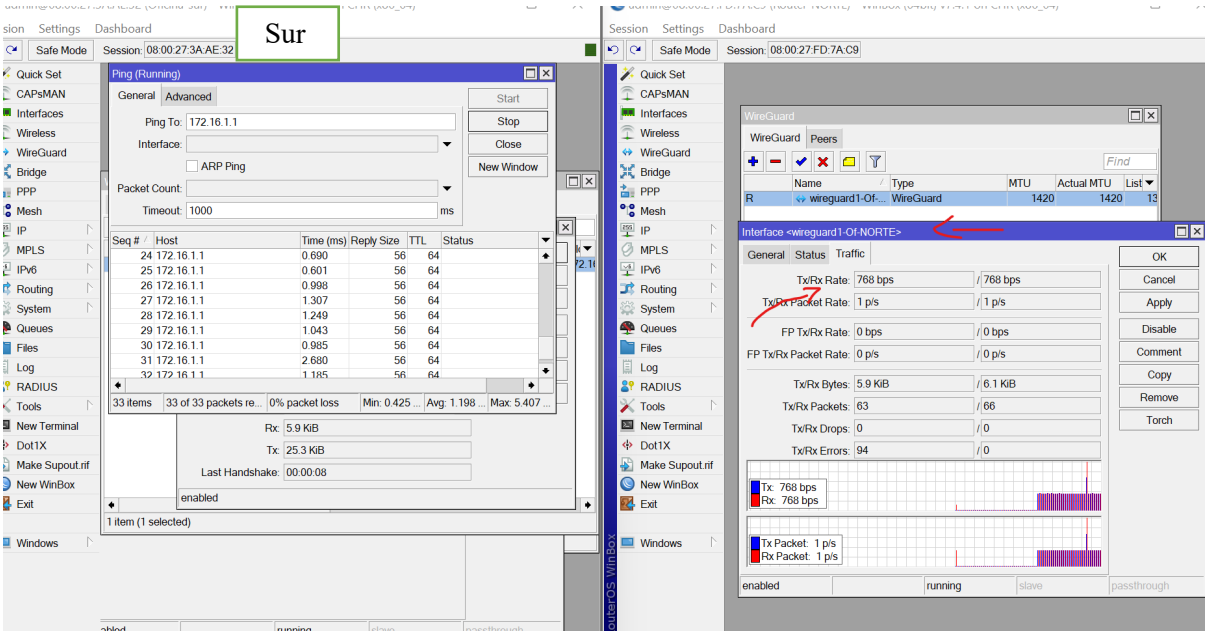


Ilustración 234 Análisis de tráfico, oficina norte

La ilustración 24, hace referencia al tráfico que está pasando por la interfaz de WireGuard en la oficina norte o sitio 2, partiendo de la simulación del laboratorio experimental.

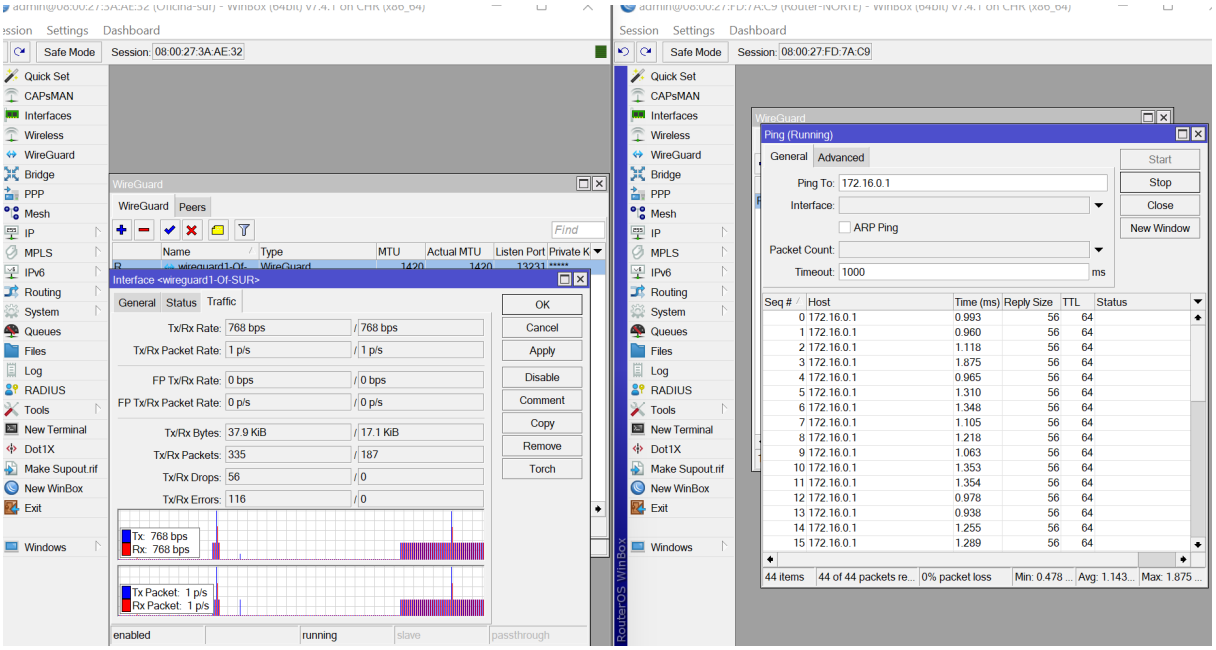


Ilustración 245 Análisis de tráfico, oficina sur

De igual forma, la ilustración 25 hace referencia al tráfico que está pasando por la interfaz de WireGuard en la oficina sur o sitio 1, partiendo de la simulación del laboratorio experimental.

4.3. Comparativa de rendimiento según el laboratorio experimental.

Para comparar las arquitecturas referentes a la velocidad, por medio de la herramienta de Mikrotik se analizó el tráfico correspondiente de cada túnel e interfaz, quedando como resultado el siguiente gráfico.

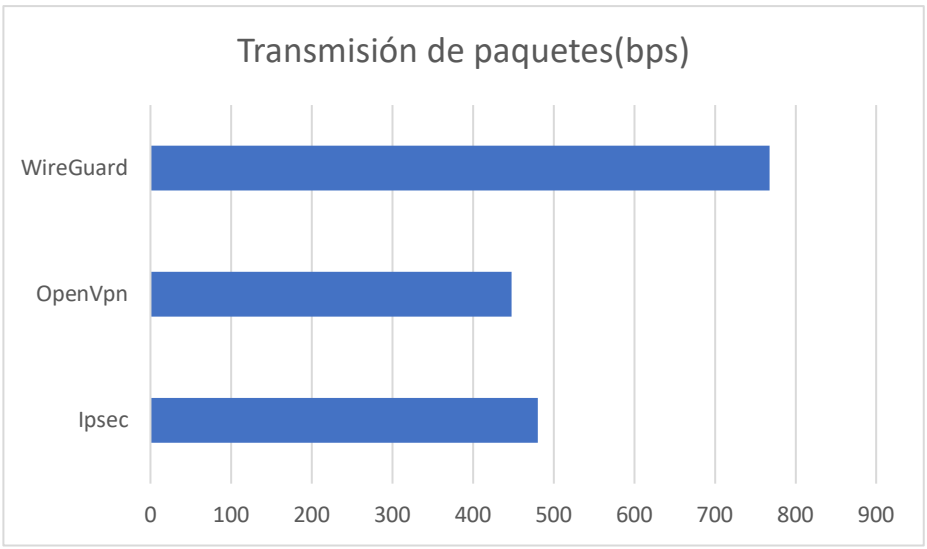


Ilustración 2625 Comparativa Trafico Mikrotik

Para comprobar la banda ancha de los túneles IPsec, WireGuard y OpenVPN, se envió el siguiente comando ping -n 100 -f (IP hacia al extremo de la puerta de enlace donde se quiere apuntar).

- **-n:** indica la cantidad de paquetes que se desea enviar por medio del comando ping.
- **-f:** ping de inundación, este parámetro no fragmenta los paquetes, podemos calcular el ancho de banda.

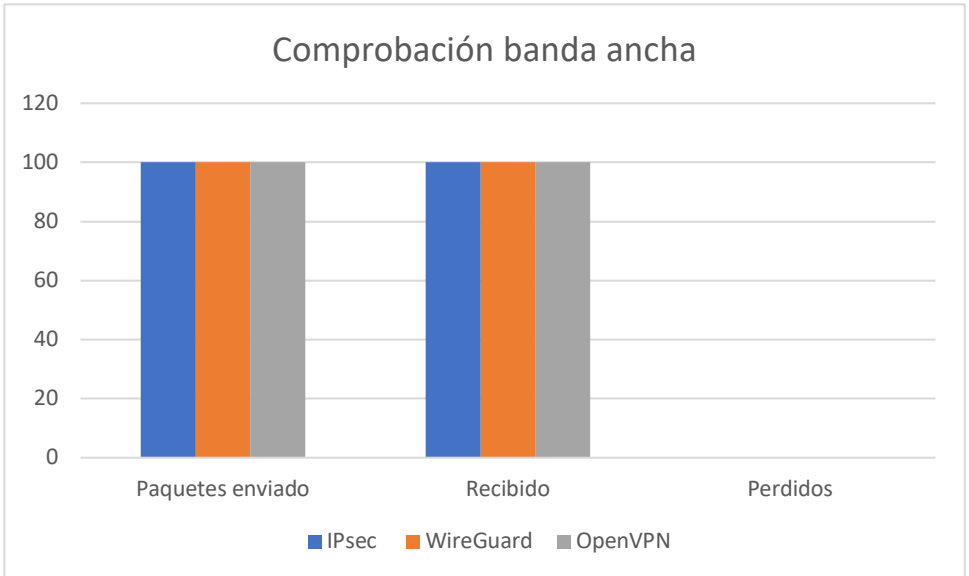


Ilustración 2726 Paquetes enviados

En el siguiente grafico se va a representar los tiempos aproximados de ida y vuelta de los 100 paquetes enviando en milisegundos.

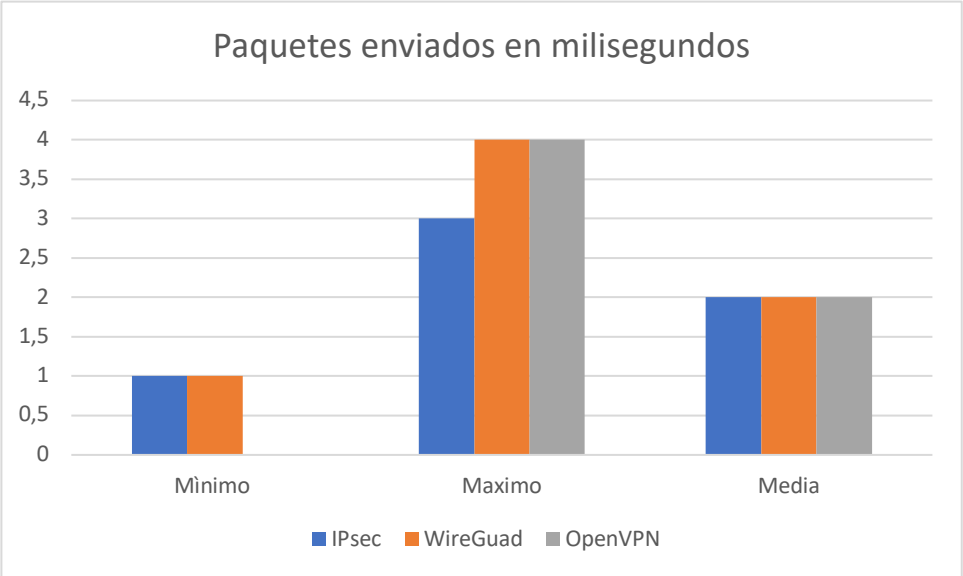


Ilustración 2827 Paquetes enviados en milisegundos

Esta investigación esta absuelta a preferencia o inclinación de infraestructuras, arquitecturas y protocolos. La información que se va a proporcionar en las siguientes tablas, es a raíz del análisis de rendimiento de puertas de enlace VPN mediante una arquitectura de red para la comunicación segura sitio a sitio entre las PYMES. El compendio de la investigación está compuesto a medida de las necesidades actuales referente a seguridad, integridad, velocidad entre otras métricas para el preciso análisis de transmisión de paquetes, seguida por la revisión bibliográfica. Además, los resultados están presentado de forma clara, precisa y fácil de entender, con la finalidad de adentrar a la parte interesada en las buenas prácticas de conocimiento de arquitectura e implementación de VPN.

4.4. Análisis de rendimiento (SSL-VPN, IPsec, WireGuard)

Tabla 6: *Resultado de la simulación según el análisis*

Parámetros	**IPsec**	**OpenVPN**	**WireGuard**
Seguridad	Medio	Medio	alto
Velocidad	Medio	Medio	Alto
Estabilidad	Medio	Medio	Medio

Compatibilidad	Alta	Medio	Baja

La tabla número 6, señala los resultados según los parámetros de rendimiento, seguridad, velocidad, estabilidad y compatibilidad, detallando con una escala de nivel, muy alto, alto, medio, bajo, muy bajo. De este modo, se determina la información transmitida en la tabla 6.

Tabla 7: *Análisis de la configuración y levantamiento de arquitectura*

Parámetros	**IPsec**	**OpenVPN**	**WireGuard**
Diseño	Complejo	Complejo	Simple
Puerto	UDP 500 y TCP	UDP y el puerto 1194	UDP 51820
Configuración	Complejo	Complejo	Simple
Conocimiento	Alto	Medio	Medio

De igual forma, en la tabla número 7, hace énfasis en el levantamiento y despliegue de una arquitectura de redes privadas virtuales. Es de importancia aclarar, que las configuraciones están dentro de un nivel de conocimiento medio, no obstante, en las métricas del diseño y configuración se manifiesta en término de complejidad y simplicidad, debido a los pasos y conocimiento que requiere la implementación de cada una.

Tabla 8: Resultado de los análisis del túnel Ipsec, OpenVPN y WireGuard.

Parámetros	**IPsec**	**OpenVPN**	**WireGuard**
Confidencialidad	Confiable	Confiable	Confiable
Costo	Alto costo	Medio	Bajo costo
Cifrado	modo de transporte y modo de túnel utilizados	OpenSSL	Sí, ChaCha20-poly1305 para cifrado simétrico
Autenticación	Cha1, md5	Cha1, md5	Poly1305
Integridad	ofrece integridad	ofrece integridad	ofrece integridad
Transporte	Políticas de Nat	Interfaz	Interfaz

En este apartado o tabla 8, se detallan los resultados del análisis de las puertas de enlaces, de tal forma que hace eco al mecanismo de tunelización de cada arquitectura.

4.5. Beneficio del protocolo resultante

WireGuard es una tecnología moderna, y pese a su reciente comienzo ha tenido gran acogida por su simplicidad y fácil de implementar, por ello es llamativo para algunas empresas y desconfiable para otras, no obstante, esta investigación se suma de lado de la sociedad que le da el visto bueno a esta arquitectura, a pesar de que está comprobado que al igual que IPsec y OpenVPN no son suficientemente rápido para manejar la cantidad de paquetes en redes de 10 o 40 Gbit/s, pero se recomienda WireGuard para entornos de producción, además esta arquitectura tiene el código de autenticación más seguro en la actualidad por su utilidad: velocidad extremadamente alta, baja sobrecarga por mensaje, agilidad de claves, entre otras. WireGuard demostró ser el protocolo más simple de configurar, transmite una sensación de seguridad y fue superior en velocidad concerniente a las arquitecturas analizadas.

CAPÍTULO V: DISCUSIÓN

Los resultados del trabajo se pudo apreciar las técnicas utilizadas en el proceso de encapsulación y encriptación de información como medida de seguridad, coincidiendo con el estudio "A new approach for the securityof VPN" donde manifiesta, que los datos del usuario se cifran utilizando un algoritmo de cifrado multifase y se encapsulan mediante el método de encapsulación tradicional, de esta forma concuerdan las investigaciones referentes a la seguridad e integridad de la información [7].

Como resultado del estudio "Análisis de rendimiento de puertas de enlace VPN" inspirado en el análisis de arquitecturas de redes privadas virtuales de código abierto, descubre que WireGuard es la implementación de VPN de software más prometedora desde un punto de vista arquitectónico, por ello, esta investigación coincide netamente con los resultados arrojados del trabajo propuesto, ya que, WireGuard es una tecnología que se diferencia de las demás por su arquitectura, simplicidad de configuración y su alta velocidad de transmisión de datos [9].

Sholihah, W. Rizaldi, T. y Novianty, I. [6], indica en su investigación realizada mediante simulación en la aplicación GNS3 que existe limitaciones en las virtualizaciones de las VLAM en el aplicativo mencionado, por esta razón, este trabajo concuerda con aquella afirmación, debido a que al momento de configurar y realizar el previo análisis de las arquitecturas seleccionadas en la misma herramienta, se pudo apreciar pequeñas inconformidades en la selección de controles de seguridad, cabe señalar que para las pruebas se utilizaron dispositivos de MikrotiK virtualizado.

D. Irawan1y Fatoni [16], menciona en su artículo "implementación de seguridad IP en la red VPN de sitio a sitio" que la VPN de sitio a sitio se usa para conectar redes que tienen largas distancias a través de la red pública para que parezca estar en una red local. En particular, en esta investigación se comprobó la conexión de dos redes LAN por medio de un túnel que

atraviesa la red WAN para conectar las sucursales a través de las redes privadas virtuales y de ese modo se asegura la trasmisión de datos.

Tomando como base el estudio de “Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol” [13], mismo que analiza las puertas de enlace IPsec y WireGuard en la parte de encriptación y autenticidad de los túneles VPN, indica que IPsec encripta la información a través de los algoritmos DES, 3DES, AES, sin embargo, en el despliegue de la arquitectura con dispositivos de MikrotiK realizado en esta investigación se pudo notar que los algoritmos de encriptación son AES-128, AES-256, para la autenticación MD5 y CHA-1. Respecto a WireGuard según el artículo trabaja con un cifrado simétrico ChaCha20 y para la autenticación Poly1305, utilizando la construcción AEAD de RFC7539, a diferencia, en Mikrotik se utilizan las llaves pública y privada generada por la herramienta, la información es encriptada con la llave pública y desencriptada con la llave privada y de esa forma operan los dos Routers.

CAPÍTULO VI: CONCLUSIONES

Se concluye que, SSL-VPN, IPsec y Wireguard. Son protocolos que en la actualidad le garantizan a las PYMES confidencialidad, integridad, seguridad y velocidad, teniendo en cuenta que la información es cifrada y se envía por el túnel configurado para el tráfico de paquetes por medios de arquitecturas de red.

Referente al análisis, se determina que las redes privadas virtuales, están basadas en cuatro componentes que se refieren a las fases o etapas en su operación: autenticación, túnel, cifrado y control de flujo. Por tanto, las arquitecturas como IPsec y OpenVPN desencripta la información por bloque, en cambio, WireGuard lo hace por flujo a través de las llaves privada y pública que son generadas para el intercambio de información, razón por la cual esta arquitectura tiene un rendimiento mayor a las tecnologías evaluadas.

En definitiva, el protocolo WireGuard es una tecnología en constante actualización, sus múltiples beneficios hacen de esta arquitectura de VPN una herramienta útil, confiable y segura, se diferencia de la demás tecnología por su velocidad extremadamente alta y baja sobrecarga, permitiendo un rendimiento considerable y productivo, constando con el mejor método de autenticación en la actualidad.

Para terminar , esta investigación presentó la identificación de los tipos de arquitectura de VPN más usuales en la hoy en día, en efecto, se sintetiza que las VPN de sitio a sitio y de acceso remoto son las más comunes e utilizada por las PYMES, a causa de, las comunicaciones de acceso remoto les permite acceder de forma segura a las redes privadas y abrir los servicios disponibles a distancia, de igual forma , la comunicación de sitio a sitio les permite acceder en sitios dispersos o sucursales que se utilizan para la comunicación entre sí.

CAPÍTULO VII: RECOMENDACIONES

Para utilizar el protocolo WireGuard en Mikrotik se recomienda trabajar con las versiones 7.1 en adelante, por motivo que en versiones anteriores no se cuenta con esta herramienta debido a que el protocolo WireGuard es una tecnología reciente.

También se recomienda elegir los cifrados criptográficos correctos y modernos, dado que puede ayudar a la estabilidad, seguridad e integridad de datos. Los cifrados AEAD, AES-GCM o ChaCha20-poly1305, son los mejores cifrados respecto a los tradicionales.

Es necesario tener en cuenta que se pueden realizar múltiples interfaces y es de buenas prácticas tener dos o más interfaces de túnel para la transmisión según la necesidad, y mucho mejor si se profundiza con conocimiento de puertas de enlaces, con el fin de utilizar las tres arquitecturas para procesos diferentes según el beneficio.

Es sumamente importante realizar los mantenimientos de puertas de enlaces en horario de poca concurrencia de tráfico, visto que estas modificaciones llevan al Router al 100% de operación y fácilmente se puede caer la red.

Es imprescindible tener un ambiente de prueba para realizar operaciones o configuraciones ante de realizar alguna modificación al Router que está en producción, con la finalidad de prevenir o ahorrar recursos, tiempo, dinero y esfuerzo.

REFERENCIAS BIBLIOGRÁFICAS

[1] 1234456487 and Sonny Eli Zaluchu, “Análisis del impacto de los ataques de ransomware en las Organizaciones colombianas como base de conocimiento para La determinación de nuevos mecanismos de rotección y Minimización de riesgos cibernéticos.,” vol. 3, no. March, p. 6, 2021.

[2] S. T. Aung and T. Thein, “Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks,” *2020 IEEE Conf. Comput. Appl. ICCA 2020*, pp. 3–7, 2020.

[3] M. H. M. Zaharuddin, R. A. Rahman, and M. Kassim, “Technical comparison analysis of encryption algorithm on site-to-site IPSec VPN,” *ICCAIE 2010 - 2010 Int. Conf. Comput. Appl. Ind. Electron.*, no. Iccaie, pp. 641–645, 2010.

[4] Z. Wu and M. Xiao, “Performance evaluation of VPN with different network topologies,” *2019 2nd Int. Conf. Electron. Technol. ICET 2019*, pp. 51–55, 2019.

[5] P. Polezhaev, A. Shukhman, and Y. Ushakov, “Implementation of dynamically autoconfigured multiservice multipoint VPN,” 2019.

[6] W. Sholihah, T. Rizaldi, and I. Novianty, “Information and communication system technology with VPN site-to-site IPsec,” *J. Phys. Conf. Ser.*, vol. 1193, no. 1, pp. 1–7, 2019.

[7] K. K. V. V. Singh and H. Gupta, “A new approach for the securityof VPN,” *ACM Int. Conf. Proceeding Ser.*, vol. 04-05-Marc, no. June, 2016.

[8] S. De la cruz Bernilla, “Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo,” *Univ. Nac. "Pedro Ruí Z Gall.*, 2019.

[9] M. Pudelko, P. Emmerich, S. Gallenmüller, and J. Carle, “Análisis de rendimiento de puertas de enlace VPN,” pp. 325–333, 2020.

[10] W. C. Rendón and W. Chango, “Implementación de políticas de tráfico en una arquitectura de red para garantizar la seguridad de acceso y servicios en la PUCESE . Implementation of traffic policies in a network architecture to ensure the security of access and services of the PUCESE .,” 2017.

[11] S. Jahan, M. S. Rahman, and S. Saha, “Application specific tunneling protocol selection for Virtual Private Networks,” *Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017*, pp. 39–44, 2017.

[12] R. Parthasarathy, S. S. Loong, P. Ayyappan, Z. A. Hamid, and A. S. Kumar, "Implementation of Site-To-Site IPSEC Virtual Private Network For Enterprise Network Design Using Cisco Packet Tracer Simulation Tool," *Int. J. Mech. Eng.*, vol. 7, no. 1, pp. 1293–1305, Jan. 2022.

[13] A. M. Abdulazeez, B. W. Salim, D. Q. Zeebaree, and D. Doghramachi, "Comparison of VPN Protocols at Network Layer Focusing on Wire Guard Protocol," *Int. J. Interact. Mob. Technol.*, vol. 14, no. 18, pp. 157–177, 2020.

[14] R. Bibraj, S. Chug, S. Nath, and S. Departamento, "Estudio técnico de VPN de acceso remoto y sus ventajas sobre sitio a sitio," vol. 1, no. enero, pp. 97–102, 2018.

[15] R. Bibraj, S. Chug, S. Nath, and S. L. Singh, "Technical study of remote access VPN and its advantages over site to site VPN to analyze the possibility of hybrid setups at radar stations with evolving mobile communication technology," *Mausam*, vol. 69, no. 1, pp. 97–102, 2018.

[16] D. Irawan1 and Fatoni, "Penerapan IP Security pada Jaringan VPN Site to Site di PT. Pertamina Ubeb Adera Pengabuan," *Univ. Bina Darma*, 2018.

[17] R. Cohen and G. Kaempfer, "On the cost of virtual private networks," *IEEE/ACM Trans. Netw.*, vol. 8, no. 6, pp. 775–784, 2000.

[18] N. Sai Prasad, M. Sri Kumaran, S. Prasad, and N. Sathish Kumar, "Implementation and Performance Analysis of Traffic Engineered Multiprotocol Label Switching Network for IPv6 Clients," *Proc. Int. Conf. Electron. Sustain. Commun. Syst. ICESC 2020*, no. Icesc, pp. 766–773, 2020.

[19] RI No. 43 20Permenkes19, *DISEÑO DE UN PROTOTIPO CON UNA ARQUITECTURA DE RED SEGURA EN LA PUCESE.*, no. 2. 2019.

[20] V. P. Tintín-Perdomo, J. R. Caiza-Caizabuano, and F. S. Caicedo-Altamirano, "Arquitectura de redes de información. Principios y conceptos," *Dominio las Ciencias*, vol. 4, no. 2, p. 103, 2018.

[21] H. Ordiales, "Comparativa de Arquitecturas para un servicio de Video bajo demanda de gran escala," no. July, pp. 1–5, 2020.

[22] B. A. Rodriguez Toala, E. J. Pincay Segovia, and K. Maldonado Zúñiga, "Las Redes Wan Y Su Importancia Para Los Ordenadores," *UNESUM-Ciencias. Rev. Científica Multidiscip. ISSN 2602-8166*, vol. 6, no. 1, pp. 1–14, 2022.

[23] T. Ing, A. Steven, A. Briones, and M. Sc, "ANÁLISIS DE VULNERABILIDADES SOBRE PROTOCOLOS VPN," 2021.

[24] V. V. Aparicio-Izurieta, "Seguridad con IP seguro en internet (IPSEC)," *Sapienza Int.*

J. Interdiscip. Stud., vol. 3, no. 1, pp. 978–987, 2022.

[25] P. Emmerich, S. Gallenmüller, D. Raumer, F. Wohlfart, and G. Carle, "MoonGen: A Scriptable High-Speed Packet Generator Paul," pp. 275–287, 2015.

[26] J. Zhao, A. Gonzalez, A. Amid, S. Karandikar, and K. Asanovic, "COBRA: A Framework for Evaluating Compositions of Hardware Branch Predictors," *Proc. - 2021 IEEE Int. Symp. Perform. Anal. Syst. Software, ISPASS 2021*, pp. 310–320, 2021.

[27] F. J. Valencia-Duque and M. Orozco-Alzate, "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000."

[28] G. Jain and Anubha, "Application of SNORT and Wireshark in Network Traffic Analysis," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1119, no. 1, p. 012007, Mar. 2021.

[29] S. R. Mejía Matute, L. G. Pinos Luzuriaga, W. B. Proaño Rivera, and E. B. García Galarza, "Capacidades Organizacionales en las Empresas de Manufacturas de Cuenca – Ecuador," *INNOVA Res. J.*, vol. 6, no. 2, 2021.

[30] J. L. Esparza-Aguilar, A. Soto-Maciel, M. I. De la Garza-Ramos, and J. M. San Martín-Reyna, "El desempeño financiero y la riqueza socioemocional en pequeñas y medianas empresas familiares y no familiares," *Tec Empres.*, vol. 15, no. 2, 2021.

[31] Z. Al-Odat, A. Abbas, and S. U. Khan, "Randomness analyses of the secure hash algorithms, SHA-1, SHA-2 and modified SHA," *Proc. - 2019 Int. Conf. Front. Inf. Technol. FIT 2019*, pp. 316–321, 2019.

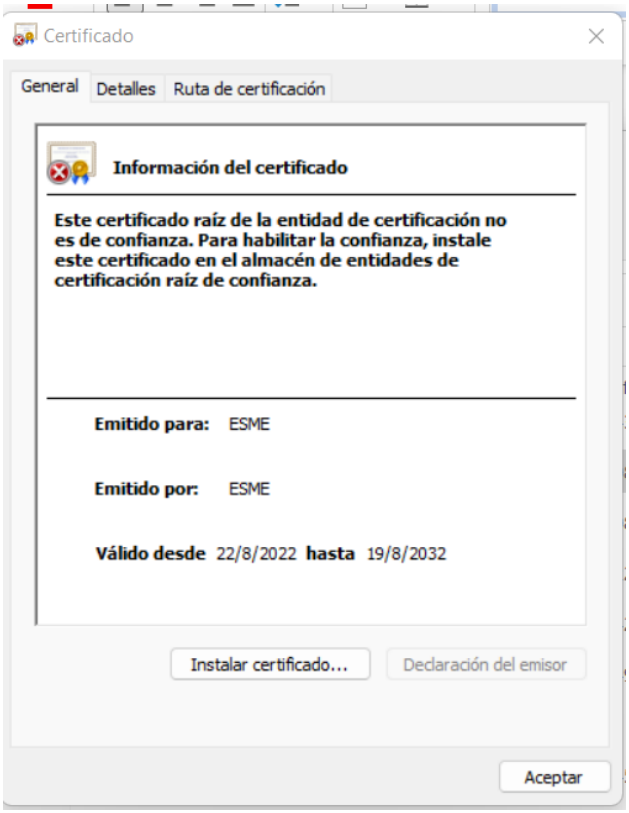
[32] R. Andriani, S. E. Wijayanti, and F. W. Wibowo, "Comparision of AES 128, 192 and 256 bit algorithm for encryption and description file," *Proc. - 2018 3rd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2018*, pp. 120–124, 2018.
10.1109/NSysS.2017.7885799.

[10] M. Iqbal, "Analysis of Security Virtual Private Network (VPN) Using

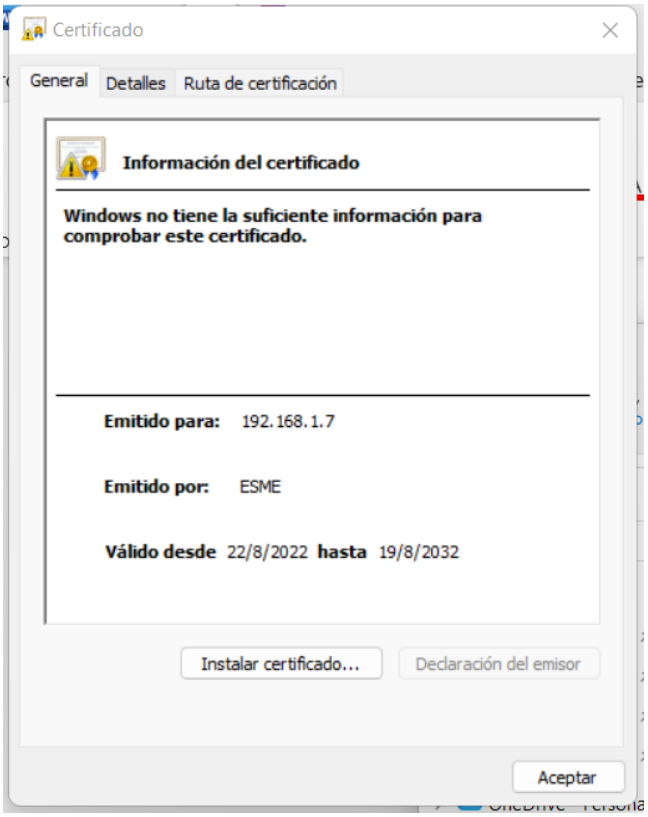
OpenVPN," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 1, pp. 58–65, 2019, doi: 10.17781/p002557.

ANEXOS

CERTIFICADO OpenVPN CLIENTE

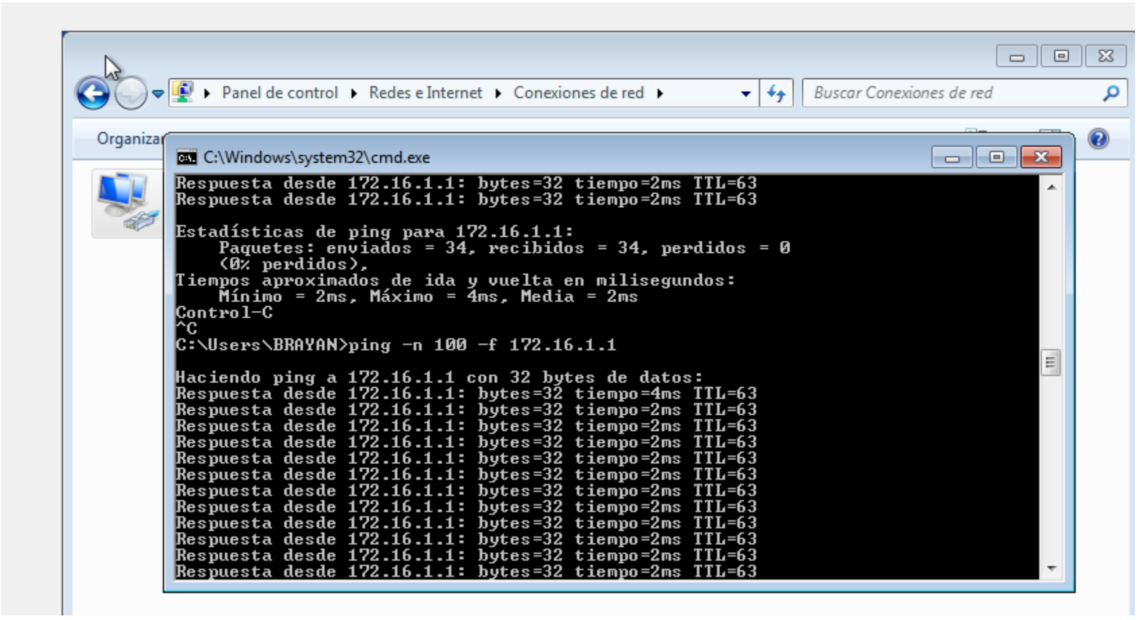


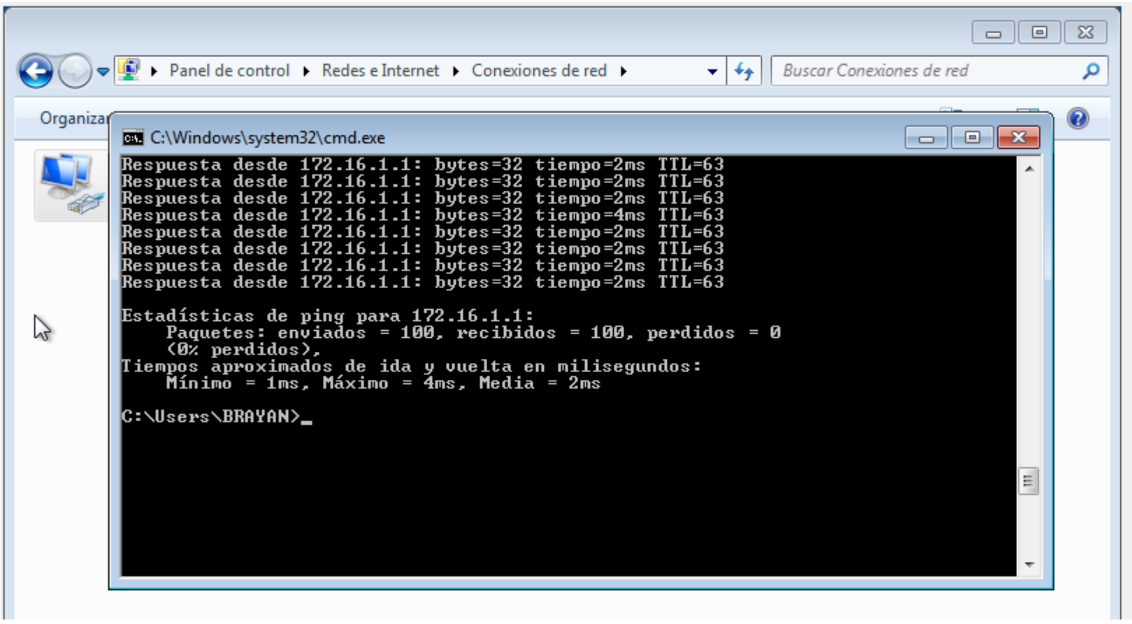
CERTIFICADO OpenVPN SERVER



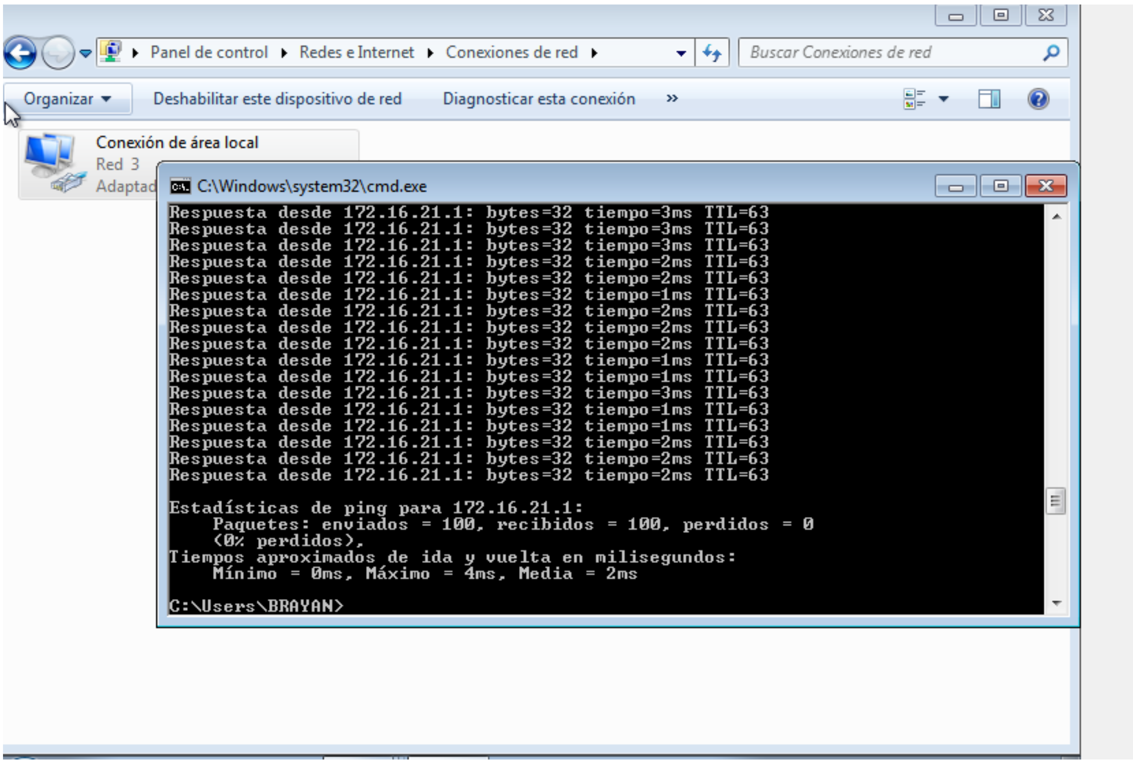
COMPROBACIÓN DE ANCHO BANDA

WireGuard





OpenVPN



IPsec