UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

MODELO DE INFRAESTRUCTURA DE RED VPN, PARA INTERCONEXIÓN SEGURA DE ORGANIZACIONES, USANDO IPSEC CON LINUX, BAJO UN ENTORNO VIRTUALIZADO DE CLIENTES Y SERVIDORES.

TESIS

PRESENTADA POR:

Bach. LORENA CHÁVEZ PAREDES

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2022

DEDICATORIA

Este trabajo está dedicado con mucho amor y entrega a mis padres Pedro y Naty, quienes con su esfuerzo y sacrificio siempre me apoyaron en mis estudios.

A mis hermanos, no solo por estar presentes aportando buenas cosas en mi vida, sino por los grandes lotes de felicidad y de diversas emociones que siempre me han causado, y que siempre fueron como un ejemplo de superación.

A mi hijo Sebastián por ser la motivación en mi vida, a mi esposo por su apoyo incondicional.

AGRADECIMIENTOS

- En primer lugar, a Dios por brindarnos salud, inteligencia, fortaleza, perseverancia para seguir adelante sin importar los obstáculos.

- En segundo lugar, agradecer a mis jurados, Mg. Carlos Boris Sosa Maydana, M.Sc. William Eusebio Arcaya, M.Sc. Magali Gianina Gonzales Paco y para mi director M.Sc. Edelfré Flores Velásquez por haber permitido hacer este proyecto realidad.

- A nuestros docentes de la Escuela Profesional de Ingeniería de sistemas por su enseñanza y dedicación.

ÍNDICE GENERAL

Pág.

CAPÍTULO II

REVISIÓN DE LA LITERATURA

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

Área : Telemática

Tema : Sistemas Distribuidos, Redes y Telemática

Fecha de sustentación: 04 de mayo del 2022

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE ACRÓNIMOS

DNS : Sistema de nombres de dominio.

HTTP : HyperText Transfer Protocol o Protocolo de Transferencia de Hiper Textos.

IP : Internet Protocol o protocolo de internet.

IPSEC : Internet Protocol Security, que significa Seguridad del protocolo de Internet.

LAN : Local Área Network o red de área local.

PYME : Pequeñas y medianas empresas.

TI : Tecnología de información.

VM : Máquina virtual.

VPN : Virtual Private Network, que significa Red Privada Virtual.

Wi-Fi : Wireless Fidelity es decir fidelidad inalámbrica.

WLAN : Wireless Local Área Network o red inalámbrica de área local.

WWW : World Wide Web o red informática mundial.

RESUMEN

Nuestra investigación denominada “MODELO DE INFRAESTRUCTURA DE RED VPN, PARA INTERCONEXIÓN SEGURA DE ORGANIZACIONES, USANDO IPSEC CON LINUX, BAJO UN ENTORNO VIRTUALIZADO DE CLIENTES Y SERVIDORES”. Con el propósito de mejorar la interconexión segura de datos, logrando consistencia y disponibilidad de los datos así mismo asegurando la confidencialidad de los mismos disminuyendo los riesgos informáticos a los que están expuestos. La investigación es de tipo experimental porque se procedió a realizar su respectiva comprobación para verificar el funcionamiento del modelo que se plantea, así mismo tendrá una naturaleza aplicada ya que se especificará de manera detallada el diseño del modelo. Para la obtención de información se indagó, preguntó y/o entrevistó con los jefes de TI, esto nos permitió obtener un diagnóstico claro de la situación real en la que se encuentran expuestas las organizaciones mencionadas. Utilizando las técnicas de recolección de datos en este caso se realizó una entrevista directa, lo que conllevo a realizar el diseño e implementación de un modelo de infraestructura de red VPN, utilizando el protocolo Ipsec, logrando una interconexión segura de datos, fiables y de baja inversión económica, para lo cual se utiliza software Libre con GNU-Linux CentOS y la solución Ipsec StrongSwan. En este caso el modelo de infraestructura será tomado como base o patrón a seguir, tanto en software y hardware, para la comunidad de nuestra Región y otras ciudades, para que puedan implementar esta solución segura y económica en sus organizaciones y puedan interconectar sus redes físicas locales entre sí, para compartir información y datos de manera segura, que es el día a día de las empresas. Concluyendo que la implementación del modelo de infraestructura de red VPN para la interconexión segura de organizaciones logra consistencia, confidencialidad, eficiencia y con un bajo costo de inversión.

Palabras clave: Modelo, Infraestructura de red, red VPN, Linux, Ipsec.

ABSTRACT

Our research called "VPN NETWORK INFRASTRUCTURE MODEL, FOR SECURE INTERCONNECTION OF ORGANIZATIONS, USING IPSEC WITH LINUX, UNDER A VIRTUALIZED ENVIRONMENT OF CLIENTS AND SERVERS". With the purpose of improving the secure interconnection of data, achieving consistency and availability of data, as well as ensuring their confidentiality, reducing the computer risks to which they are exposed. The investigation is of an experimental type because its respective verification was carried out to verify the operation of the proposed model, it will also have an applied nature since the design of the model will be specified in detail. To obtain information, the IT managers were inquired, questioned and/or interviewed, this allowed us to obtain a clear diagnosis of the real situation in which the aforementioned organizations were exposed. Using the data collection techniques in this case, a direct interview was carried out, which led to the design and implementation of a VPN network infrastructure model, using the Ipsec protocol, achieving a secure, reliable and low-cost interconnection of data. economic investment, for which Free software is used with GNU-Linux CentOS and the Ipsec StrongSwan solution. In this case, the infrastructure model will be taken as a basis or pattern to follow, both in software and hardware, for the community of our Region and other cities, so that they can implement this safe and economical solution in their organizations and can interconnect their physical networks. premises with each other, to share information and data in a secure way, which is the day-to-day of companies. Concluding that the implementation of the VPN network infrastructure model for the secure interconnection of organizations achieves consistency, confidentiality, efficiency and with a low investment cost.

Keywords: Ipsec, Linux, Model, Network infrastructure, VPN network.

CAPÍTULO I

INTRODUCCIÓN

El trabajo de investigación tiene por finalidad implementar un modelo de Infraestructura de Red VPN, para Interconexión Segura de Organizaciones, diseñando una metodología de procedimientos para lograr conexión de redes locales remotas, con el envío y recepción de los datos, de manera segura y fiable, en las organizaciones de la región Puno, utilizando redes privadas virtuales, para llegar a resultados y conclusiones que sirvan de referencia para otros trabajos sobre este tema y para empresas dedicadas a la prestación de estos servicios.

La interconexión segura de redes locales está siendo adoptada debido a que se alinea a las estrategias del área de TI de las organizaciones de nuestra región, quienes en su necesidad de contar con servicios que brinden confiabilidad, consistencia, y ahorro, utilizando tecnologías libres en sus aplicaciones de software, encuentran en las redes VPN utilizando Ipsec una solución que nos permitirá alcanzar los objetivos.

El presente proyecto tiene como objetivo general desarrollar un modelo de Infraestructura de Red VPN para mejorar la interconexión segura de datos entre las redes locales de las organizaciones, logrando consistencia y disponibilidad de los datos, asegurando la confidencialidad de los mismos, con bajo costo de inversión y utilizando software libre en su mayoría conjuntamente con el protocolo IPSEC y Linux, para evaluar los riesgos informáticos, brindando privacidad a las conexiones de sus redes locales y accesos remotos, mediante el cifrado de datos. El presente trabajo de investigación expone los siguientes capítulos.

En el Capítulo I, denominado planteamiento del problema, se da a conocer los objetivos e hipótesis de la investigación, así mismo en este capítulo se expone los motivos por el cual poder lograr la interconexión segura de datos mediante la implementación del trabajo de investigación.

En el Capítulo II, denominado marco conceptual, marco teórico en este capítulo se han identificado términos de referencia teóricos y técnicos que contribuyen a una mejor comprensión del problema objeto de estudio, cuya introducción ha sido estudiada por investigaciones previas

En el Capítulo III, denominado método de la investigación, donde se expone el tipo y diseño así mismo la técnica de recolección de datos que se utilizó para el trabajo de investigación.

En el Capítulo IV, denominado resultados y discusión, se describe la estructura y los procedimientos generales de la implementación del proyecto y los resultados de la investigación.

Y por último se exponen las conclusiones, recomendaciones, bibliografía y anexos.

1.1. PLANTEAMIENTO DEL PROBLEMA

1.1.1. Descripción del problema de la investigación

En la actualidad las organizaciones cuentan con una oficina principal, y sus sedes se encuentran en otras provincias, quedando aisladas de toda comunicación con la oficina principal, Cada uno de ellos tiene su propia red local, e incluso utiliza protocolos diferentes a los utilizados en otras sucursales, es decir, en todas partes hay una

configuración completamente local, no necesariamente compatible con alguna o todas las demás configuraciones de dominio dentro de la misma organización.

Hoy en día, la oficina principal y los usuarios remotos hacen transferencias de información por correo electrónico y/o un medio de almacenamiento externo, para consolidar dicha información, ya que ninguno de ellos está conectado a través de la red para llegar al servidor principal, este método no cuenta con la confidencialidad, privacidad y confidencialidad requerida para manejar la información, poniendo en riesgo la seguridad y manipulación por terceros ocasionando la perdida de la misma.

Dentro de este contexto se encontró organizaciones dentro de ellas Pymes, que no cuentan con una adecuada infraestructura de comunicación entre la oficina principal y sus sedes ya sea dentro de una misma ciudad u otra, ya que en un momento dado se convierte en una desventaja competitiva en la prestación de servicios adicionales que den un valor agregado a sus clientes.

Según la recopilación de información en algunas organizaciones se deduce que la mayoría no invierten en tecnología, debido al alto costo por parte de los proveedores de internet y el desconocimiento de nuevas tecnologías y sus aplicaciones. Y es que básicamente el propósito de este trabajo de investigación va enfocado en mejorar la infraestructura de sus redes a nivel tecnológico permitiéndoles que estén siempre conectadas optimizando la comunicación de los datos y evitar la exposición a los riesgos informáticos.

1.2. IDENTIFICACIÓN DEL PROBLEMA

1.2.1. Problema general

¿Cómo lograr que las organizaciones de Puno, conecten sus redes LAN físicas y accesos remotos, usando tecnologías de cifrado y de bajo costo para garantizar la confidencialidad, seguridad y protegiendo la privacidad de los mismos?

1.2.2. Problemas específicos

- ¿Qué niveles de funcionalidad, confiabilidad y seguridad deben existir en el diseño de una VPN para optimizar las comunicaciones de datos en las organizaciones de Puno?
- ¿Por qué las organizaciones de Puno no cuentan con la implementación de tecnologías adecuadas de cifrado de datos, para permitir las conexiones de sus redes LAN y sus dispositivos necesarios?
- ¿A qué riesgos informáticos están expuestas las organizaciones de Puno al no conectar sus redes locales y accesos remotos, con tecnologías de cifrado de datos?

1.2.3. Límites y restricciones

1.2.3.1. Limites

- Fecha esperada de entrega del proyecto
- Cantidad de recursos técnicos disponibles
- Requerimiento mínimos necesarios y esperados
- Establecer correctamente las políticas de seguridad y de acceso.

1.2.3.2. Restricciones

Las restricciones que se pudieron visualizar en el proyecto de investigación fueron los siguientes:

- Proyecto realizado por fases.
- Priorización de los requerimientos.
- No poder contar con los equipos necesarios para realizar las respectivas pruebas.

1.2.4. Justificación del problema

El desarrollo de este trabajo se da por las necesidades y el crecimiento que presentan las organizaciones de Puno, los avances son determinantes ya que requieren cambios drásticos que brinden seguridad, calidad y economía para mejorar el desempeño y las necesidades operativas que se presentan a diario en las organizaciones, en especial en nuestra ciudad de Puno. Hoy en día, el mayor éxito de las organizaciones es averiguar cómo aprovechar las oportunidades para ahorrar recursos y reducir costos, es por eso que al momento de implementar el modelo de infraestructura de red VPN, lograra un bajo costo de inversión. Uno de los inventos más exitosos y productivos, podemos reconocer que es el Internet, la red de Redes, la gran interconexión mundial de las redes existentes para compartir recursos entre los usuarios, sin limitarte a la diversidad de sistemas operativos y versiones que existen hoy en día. El modelo de infraestructura de red VPN en las organizaciones de Puno, dará seguridad en la interconexión de datos entre las redes locales, brindando funcionalidad, confiabilidad y protegiendo la privacidad de los mismos. Es por eso que al implementar el modelo de infraestructura de red VPN, en las organizaciones de Puno brindara eficiencia, confiabilidad y consistencia además de

optimizar los recursos de hardware y software garantizando la integridad la interconexión segura mediante el cifrado de sus datos

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general

Desarrollar un modelo de Infraestructura de Red VPN para mejorar la interconexión segura de datos entre las redes locales de las organizaciones de Puno.

1.3.2. Objetivos específicos

- Diseñar la red VPN segura, de alto nivel, logrando consistencia y disponibilidad de los datos, asegurando la confidencialidad de los mismos.
- Implementar la red VPN eficiente con bajo costo de inversión y utilizando software libre en su mayoría, utilizando el protocolo IPSEC y Linux.
- Evaluar los riesgos informáticos, brindando privacidad a las conexiones de sus redes locales y accesos remotos, mediante el cifrado de datos.

1.4. HIPÓTESIS

1.4.1. Hipótesis general

El diseño y la implementación del modelo de Infraestructura de Red VPN mejora la interconexión segura de datos entre las redes locales de las organizaciones de Puno.

1.4.2. Hipótesis especificas

- El diseño de la red VPN, logra consistencia y disponibilidad de los datos, asegurando la confidencialidad de los mismos.

- La implementación de la red VPN es eficiente y con bajo costo de inversión utilizando software libre en su mayoría.

- Los riesgos informáticos, disminuyen brindando privacidad a las conexiones de sus redes locales y accesos remotos, mediante el cifrado de datos.

1.5. OPERACIONALIZACIÓN DE VARIABLES

1.5.1. Variable dependiente

Modelo de Infraestructura de red VPN, para Interconexión Segura de Organizaciones.

1.5.2. Variable independiente

Usando Ipsec con Linux, bajo un entorno virtualizado se clientes y servidores.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES

2.1.1. Antecedentes internacionales

Quezada (2016), en su tesis. **"Diseño de una VPN para la entrada a las bases de datos científicas de la Universidad Nacional de Loja."** Su objetivo general es diseñar una red privada virtual que permita el acceso remoto a las bases de datos científicas disponibles en la Universidad Nacional de Loja. Generar un escenario de una VPN para entrar a las bases de datos científicas de la Universidad. Concluyendo que las redes privadas virtuales son la mejor elección para permitir que los alumnos accedan a las bases de datos científicas de la universidad gracias a su elevado nivel de confidencialidad, estabilidad, totalidad y veracidad (Quezada, 2016).

Peña (2016), **"Diseño e utilización de una red privada virtual (VPN- SSL) usando el procedimiento de autenticación LDAP en una organización privada"**, realizo el trabajo de averiguación con el objeto de conceptualizar una política de ingreso remoto a la red, equiparar el protocolo SSL. El uso de VPN-SSL está integrado a LDAP en la organización, lo que ayuda a garantizar la portabilidad, la integridad, seguridad y estabilidad de los datos, reducir los costos de uso y, especialmente, permitir que los usuarios y consultores externos se conecten desde cualquier ubicación geográfica de forma segura antes de que ocurra cualquier evento en el territorio. Con la utilización, se asegura la continuidad del comercio constantemente y una vez que el cliente posea acceso al internet sin la necesidad de estar físicamente en las instalaciones de la organización (Peña, 2016).

2.1.2. Antecedentes a nivel nacional

Atencio & Mamani (2017), **"Diseño e Utilización de un Primer ejemplar de Red Privada Virtual en Capa 3 usando Cisco IOS para la Universidad Nacional del Altiplano"**, el trabajo de indagación tuvo como fin primordial el hacer un diseño y siguiente la utilización de un primer modelo de Red Privada Virtual que posibilite garantizar y encriptar la información compartida en medio de las oficinas para operar y mantener el control del tráfico en LAN y WAN, originarios de la Universidad Nacional del Altiplano. Donde se hizo diseñar y llevar a cabo el primer modelo de una Red Privada Virtual en Capa 3 usando CISCO IOS que garantiza y encripta la información compartida entre la Oficina de Tecnología e Informática y las coordinaciones académicas de las 19 facultades de la Universidad Nacional del Altiplano. (Atencio, 2017).

Amenero (2012), en su trabajo de indagación nombrado **"Implementación de una Red Privada Virtual (VPN) Bajo Programa Independiente para Optimizar el Desempeño de Información entre los Locales de la Corporación Educativa Adeu, de La Metrópoli de Chiclayo"**. La finalidad general de esta indagación es llevar a cabo una VPN con el objetivo de optimizar la entrada a los datos entre los locales de la corporación Educativa ADEU. Según la indagación realizada y a los resultados logrados, se concluye que la herramienta OpenVPN posibilita entrar la información de forma óptima y eficaz, accediendo a diferentes recursos entre los locales de la organización de forma directa, y que, por medio de la utilización de una VPN bajo programa independiente, se optimiza la comunicación entre los locales en la corporación Educativa ADEU con un mejor ingreso a la información, (Amenero, 2012).

2.1.3. Antecedentes a nivel local

Melgarejo (2015), en su investigación denominada **"Red Privada Virtual Para La Prestación De Servicios Multimedia En El Campus Universitario De La Universidad Nacional El Altiplano-Puno".** Tuvo como objetivo implementar una VPN con servicios de alta demanda de tráfico autenticados por un portal cautivo en la plataforma Linux, garantizando conexiones a través de un servidor proxy. Concluyendo que la fibra óptica permite la implementación de una VPN oven LAN cifrada a través de un portal cautivo, evitando conflictos, mayor privilegio de navegación y la facilidad de interconectar a los usuarios, mejora considerablemente las tareas de autenticación, ruteo y direccionamiento IP, (Melgarejo, 2013).

2.2. MARCO TEÓRICO

2.2.1. Uso de las redes de computadoras

La mayor parte de las organizaciones poseen una porción notable de PCs. Al inicio, varias de estas PCs quizás hayan trabajado recluidas unas de otras, empero alguna vez, la gestión podría dictaminar que se necesita conectarlas para repartir la información en toda la compañía.

Se trata de compartir recursos, y el objetivo es hacer que todos los programas, dispositivos, especialmente los datos, estén disponibles para todos los usuarios de la red, independientemente del recurso o la ubicación física del usuario. Un ejemplo claro y popular es un grupo de oficinistas que comparten una impresora. Ninguno de los dos necesita realmente una impresora privada, mientras que un gran número de impresoras en red son más baratas, rápidas y fáciles de mantener que una gran colección de impresoras individuales.

Posiblemente compartir información sea todavía de mayor relevancia que compartir recursos físicos como impresoras y sistemas de respaldo en cinta magnética. La mayor parte tiene registros de consumidores, información de productos, inventarios, estados de cuenta, información fiscal y varios datos más online.

Una plataforma de producción de línea de montaje optimizada para PC no durará 5 segundos, incluso una pequeña agencia de viajes o un bufete de abogados de 3 personas depende en gran medida de una red de PC para dar a los empleados acceso instantáneo a la información. Noticias y documentos importantes.

En las organizaciones pequeñas, cada computadora puede estar en una oficina o puede estar en un edificio, pero en las organizaciones grandes, las computadoras y los empleados están distribuidos en docenas de oficinas y fábricas en muchos países. Las redes llamadas VPN (redes privadas virtuales) se pueden usar para unir redes privadas ubicadas en diferentes ubicaciones en una red grande. Es decir, no sería inconveniente que el cliente se encuentre a 15.000 kilómetros de sus datos para utilizar estos datos como si fueran locales.

En términos más simples, imagine un sistema de información empresarial como si estuviera construido a partir de una o más bases de datos que contienen información sobre la empresa y muchos empleados necesitan acceder a estos datos desde lejos. Por otro lado, los empleados que tienen en sus estaciones de trabajo máquinas más básicas se denominan consumidores; por ejemplo, pueden acceder a datos de forma remota para ingresarlos en las hojas de cálculo que desarrollan (a veces llamados clientes). bienes humanos del grupo de compras del cliente, aunque el entorno debe dejar claro si nos referimos al ordenador o a sus usuarios.

Las máquinas cliente y servidor se conectan mediante una red, como se muestra en la Figura 01 (Tanembaum, 2012).

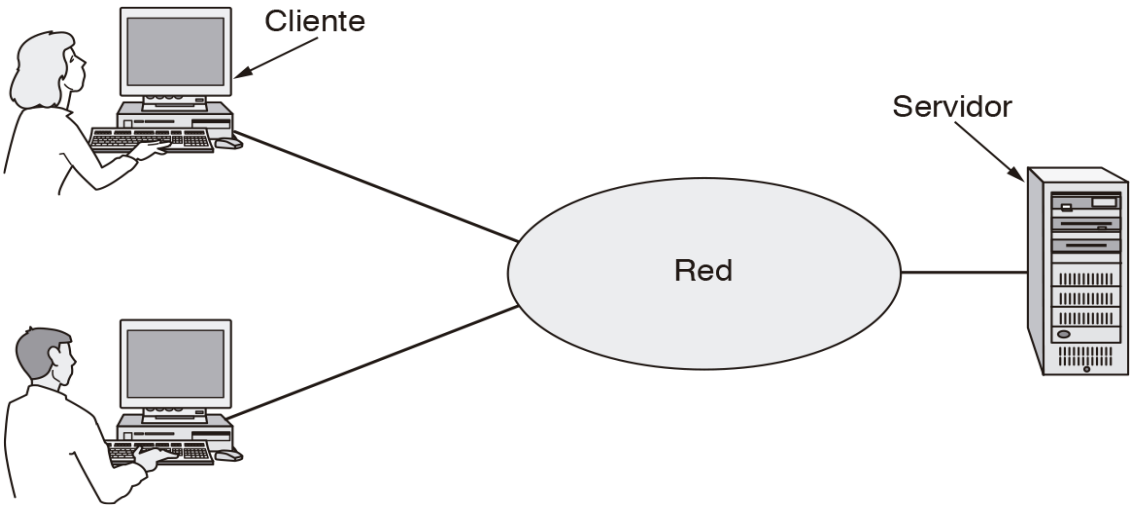


Figura 1: Una red con dos clientes y un servidor

Fuente: (Tanembaum, 2012).

La implementación más conocida es la aplicación web, donde el servidor crea páginas web a partir de su base de datos en respuesta a las solicitudes de los consumidores que pueden actualizarlas. El modelo cliente-servidor se aplica cuando el comprador y el servidor están en la misma propiedad (y pertenecen a la misma empresa), pero también cuando están bastante alejados. Por ejemplo, cuando alguien visita una página en la World Wide Web desde su casa, se utiliza el mismo modelo, donde el servidor web remoto representa el servidor y la computadora de la casa del cliente comprador.

La comunicación pasa una vez que el proceso comprador envía un mensaje por medio de la red al proceso servidor.

El proceso comprador espera un mensaje de contestación. Una vez que el proceso servidor recibe la solicitud, realiza la labor requerida o busca los datos solicitados y regresa una contestación. Estos mensajes se muestran en la Figura 02, (Tanembaum, 2012).

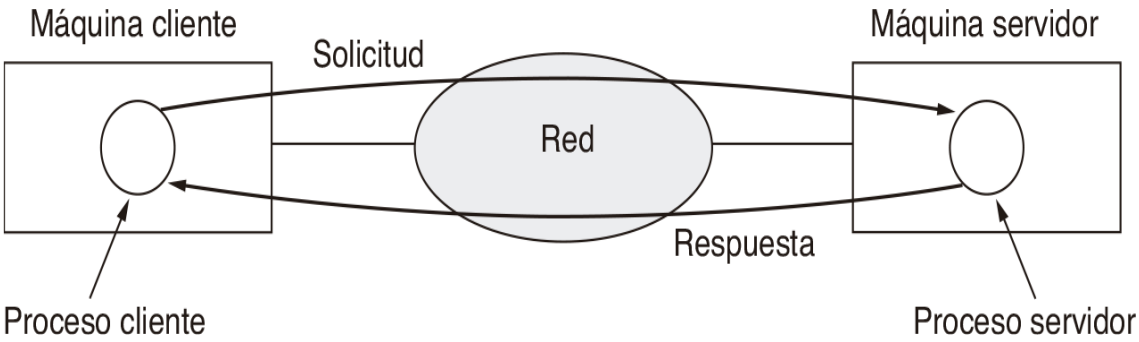


Figura 2: El modelo cliente/servidor implica solicitudes y respuestas

Fuente: (Tanembaum, 2012).

2.2.2. Clasificación de las redes de computadoras

Las redes de datos se dividen en dos grandes categorías: redes de área amplia (WAN) y redes de área local (LAN).

Sin embargo, el concepto de rango geográfico sigue siendo una clasificación didáctica eficaz y se ha conservado para dar cabida a otros estudios.

- **Red LAN**

Las LAN tienen una cobertura geográfica pequeña, como edificios o campus, y vienen en dos configuraciones comunes: LAN de telefonía, LAN alámbrica o alámbrica y LAN inalámbrica, LAN inalámbrica o WLAN. Los medios de transmisión más comunes para la comunicación en una LAN alámbrica son el par trenzado (protegido o no) y la fibra óptica. Entre los dispositivos activos comunes se encuentran un conmutador Ethernet para una LAN Ethernet cableada y un punto de acceso Wi-Fi (AP) para una LAN Wi-Fi inalámbrica. LAN es una organización, organización o personas que la usan para conectar sus propios grupos, (Rivera, 2016).

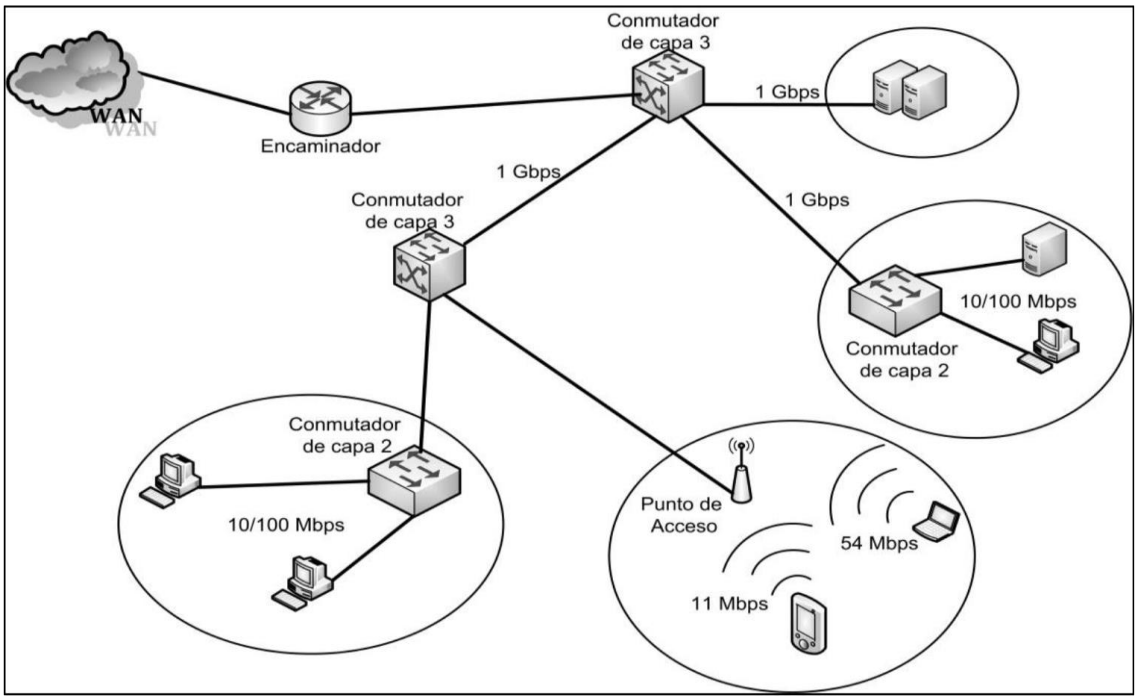


Figura 3: Ejemplo de red LAN

Fuente: (Rivera, 2016).

- **Red WAN**

Las redes WAN cubren un área geográfica más vasta y tienen la posibilidad de ser vistas como la adhesión de distintas redes LAN dispersas. Los medios de transmisión más frecuentes para interconectar las redes LAN cableadas son los medios cableados, aunque además se aplican vínculos inalámbricos.

Las redes WAN tienen la posibilidad de ser privadas, aunque lo más recurrente es utilizar redes públicas de proveedores para interconectar las redes LAN que las conforman, (Rivera, 2016).

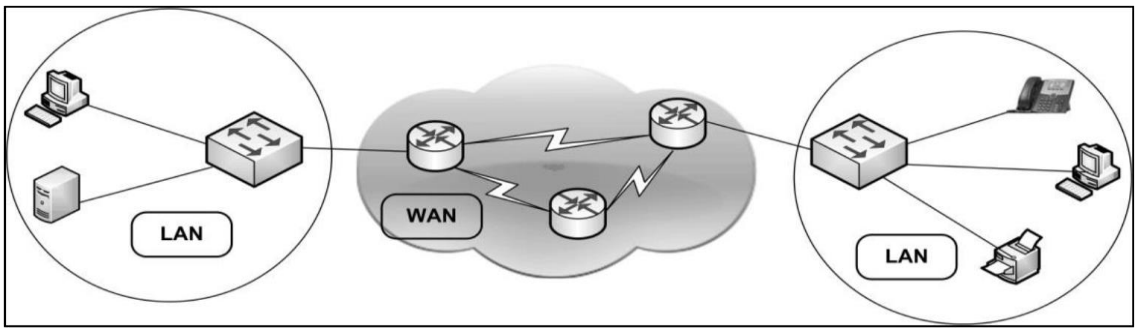


Figura 4: Ejemplo de red WAN

Fuente: (Rivera, 2016).

2.2.3. Redes privadas virtuales

Como su nombre lo indica, podemos concluir que es una red entre dos puntos tan cerca o tan lejos que podemos suponer que queremos que sean distintos o iguales en número. La información transmitida es privada. entre emisor y receptor. El término virtual se aplica a la privacidad y no al término red, ya que en la mayoría de los casos se trata de comunicación por un canal público y abierto, donde si tenemos una red privada, debería ser virtual a través de este canal público.

Una red privada virtual es una aplicación o sistema que permite la comunicación segura a través de un medio inseguro que es transparente para los usuarios o aplicaciones que establecen y reciben la conexión.

Esta definición se puede ampliar, con bastante precisión, y podemos decir que siempre que queramos asegurar una conexión entre dos puntos, podemos utilizar una VPN, independientemente de las capacidades de seguridad que ofrecen, la tenemos en nuestras comunicaciones, aunque la información debe salvarse del tercero. Además, en algunos casos, las VPN se denominan túneles porque transmiten información por un canal público, pero aíslan la información del resto, creando así muros virtuales que separan la

información entre nosotros y los demás. Estas paredes virtuales forman un túnel virtual que impide que la información viaje en ambas direcciones, de ahí el nombre del túnel.

La separación de la información se logra encriptándola y cuanto más seguro es el sistema, más seguridad nos brinda el sistema de encriptación, deseamos que cualquier avance importante en encriptación pueda transmitirse y transmitirse a nuestra VPN, (Fernandez, 2006).

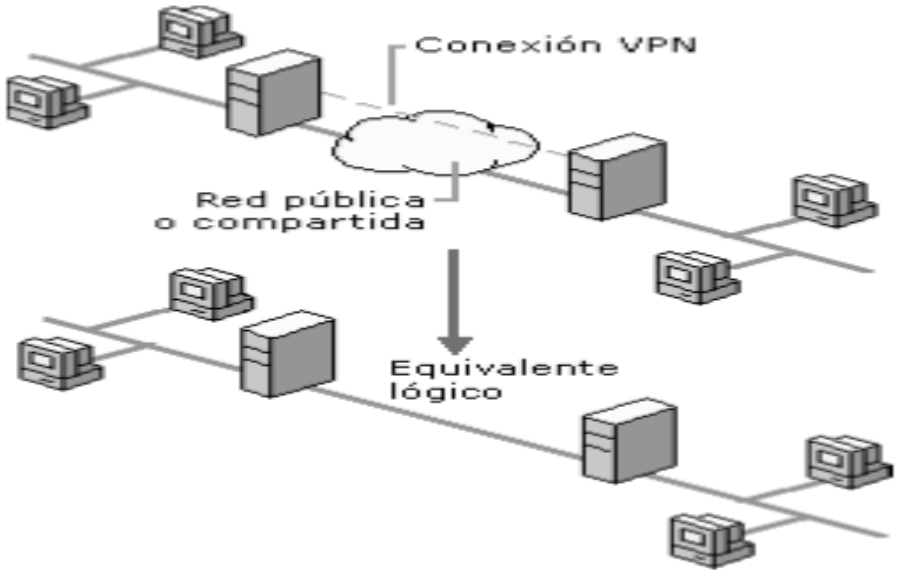


Figura 5: Red Privada Virtual

Fuente: (Fernández, 2006).

Las redes privadas virtuales son una tecnología cada vez más importante porque permiten transmitir información a largas distancias sin necesidad de construir una infraestructura de red compleja y costosa. Es por esto que es importante que cualquier ingeniero que busque avanzar en el campo de las redes de telecomunicaciones conozca esta tecnología, (Gonzalez, 2006).

2.2.4. VPN

VPN significa Red Privada Virtual, y es una tecnología de red que permite que una red de área local (LAN) segura se extienda a través de una red pública como Internet, mediante encapsulación y encriptación de los paquetes de datos en muchas máquinas remotas. Por medio del uso de la infraestructura de transporte público. logra que las computadoras en red envíen y reciban datos a través de una red compartida o pública como si fuera una red privada con funcionalidad, política de seguridad y administración completas. Esto se hace estableciendo una conexión según el tipo de VPN utilizando una conexión cifrada dedicada o una combinación de las dos, (Berners-Lee, 2000)

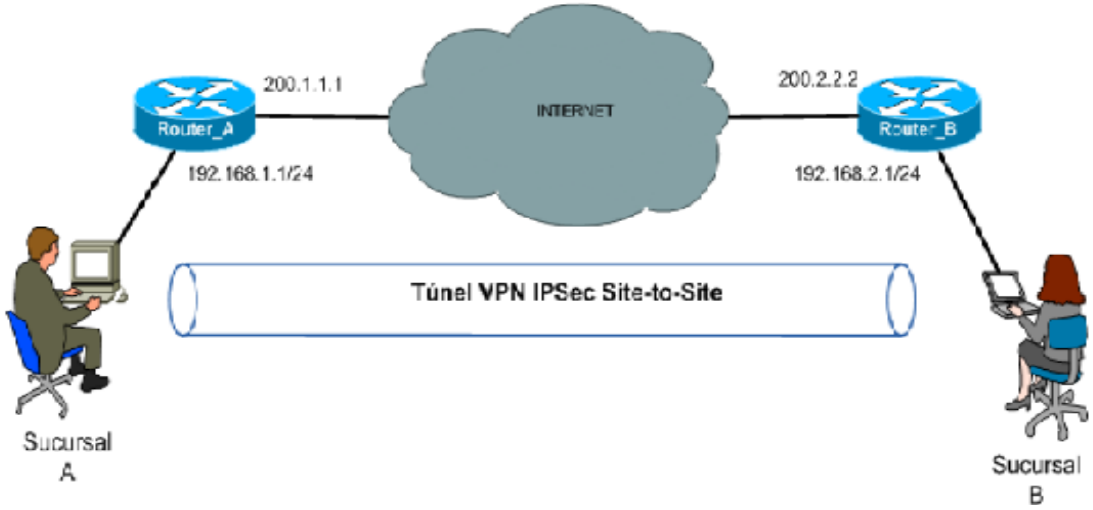


Figura 6: Virtual Prívate Network

Fuente: Red Privada virtual (figura), recuperado de https://www.locurainformaticadigital.com

Las VPN brindan una solución de bajo costo para implementar redes basadas en Internet a gran escala, además de proporcionar autenticación de usuario o dispositivo a través de encriptación, firma digital o acceso a contraseñas para una identificación clara; También proporciona integridad, garantiza que los datos transmitidos por el remitente sean correctos junto con los datos recibidos, y la confidencialidad y el cifrado garantizan

que nadie más que el remitente y el receptor sea interceptado o interpretado, (Alvarez, 2014).

2.2.5. Requerimientos básicos de un VPN

Las VPN deben tener algunos conceptos básicos antes de la implementación, como un conjunto de políticas de seguridad para encriptar datos, ya que no son visibles para clientes no autorizados en la red; Gestión de claves, para proporcionar cifrado entre el cliente y el servidor; compartir datos, aplicaciones y recursos; servidor de acceso y autenticación; Para que haya un control en la red sobre quién ingresa, verifica su identidad y tiene un registro estadístico de acceso; Gestión de direcciones, ya que la VPN debe generar direcciones para clientes en la red privada y debe asegurarse de que estas direcciones privadas sigan siendo las mismas; Finalmente, soporte multiprotocolo; Porque tiene que gestionar los protocolos comunes de Internet, como IP, por ejemplo (Alvarez, 2014).

2.2.6. Tipos de VPN

- **VPN de acceso remoto**

Los usuarios se conectan a una empresa desde ubicaciones remotas utilizando Internet como enlace de acceso. Una vez autenticados, tendrán el mismo nivel de acceso en la red local, (Alvarez, 2014).

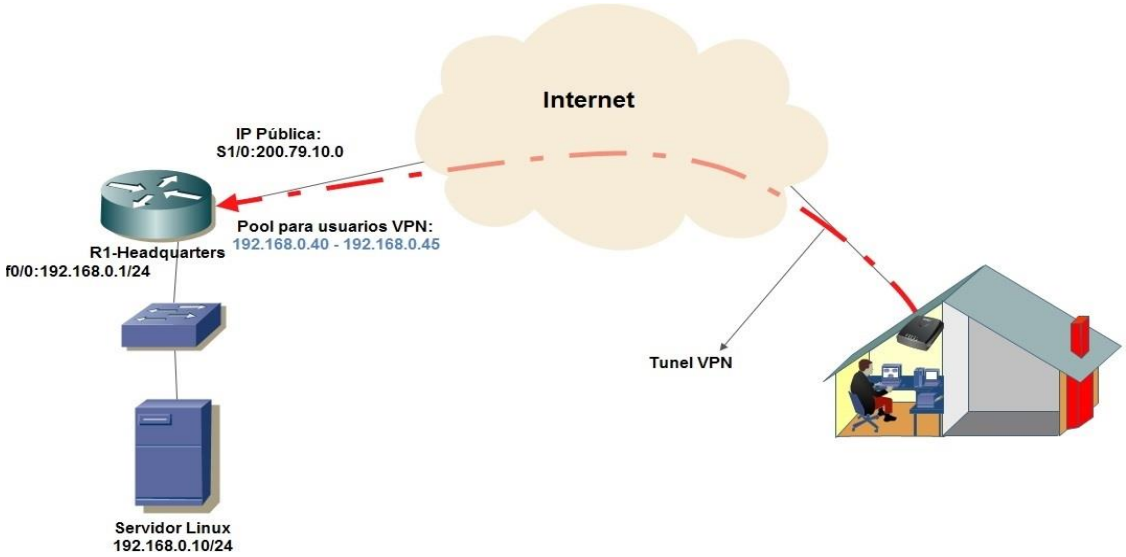


Figura 7: VPN de acceso remoto.

Fuente: Magagnotti (2013)

- **VPN punto a punto**

Es muy utilizado para conectar sucursales remotas a la oficina central de la organización, los servidores VPN o firewalls mantienen una conexión estable a internet y con esto se establece una conexión virtual tunelada con la sucursal. Las sucursales cuentan con conexión local a Internet. Las conexiones a Internet en la sede y las sucursales generalmente se consideran conexiones de banda ancha, lo que elimina el costo de los enlaces punto a punto dedicados, y más aún para las conexiones remotas, como las conexiones locales e internacionales., (Martel, 2019).

- **VPN interna (over LAN)**

Funciona como una VPN normal, excepto que se encuentra dentro de la misma LAN local y no a través de Internet. Se utiliza para aislar áreas y servicios de una misma red interna. También se utiliza para mejorar las características de seguridad de las redes Wi-Fi inalámbricas, (Alvarez, 2014).

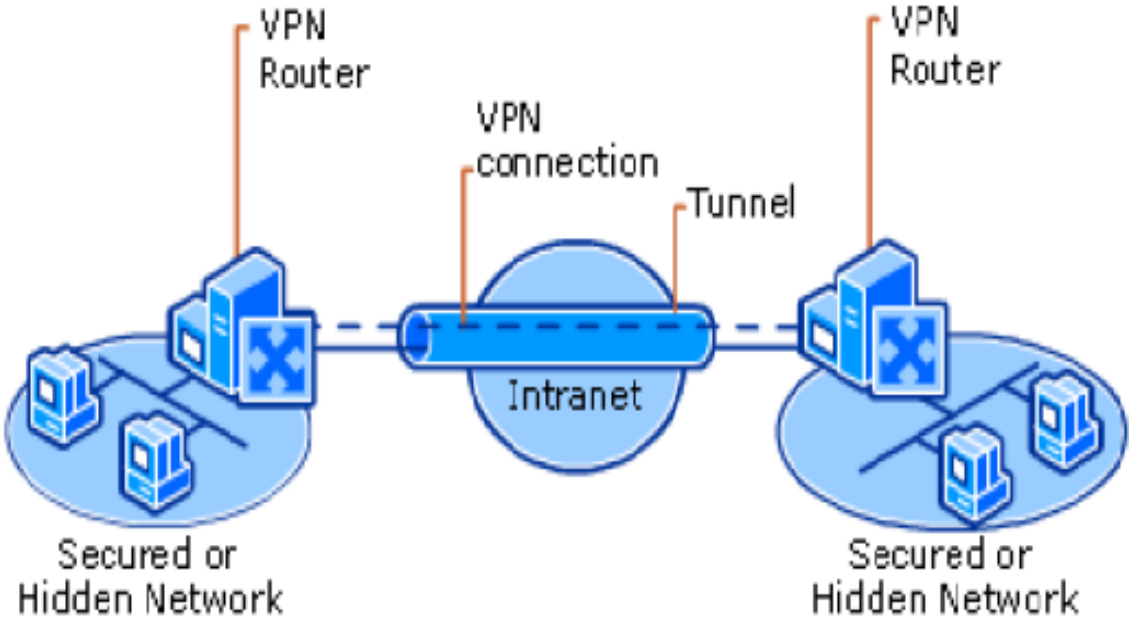


Figura 8: VPN over LAN.

Fuente: Melgarejo (2015).

2.2.7. Propiedades de la red VPN

- **Encapsulación**

Una VPN encapsula datos privados con un encabezado que les permite viajar a través de la red pública.

- **Autenticación**

Mediante esta propiedad, el servidor VPN autentica al cliente que quiere conectarse y comprueba que tiene los permisos correctos, ya que la autenticación entre ambos es mutua. La autenticación en una VPN incluye datos y autenticación de usuario. Es importante que así sea, se trata del nivel subjetivo de datos que se pueden obtener del sitio web.

- **Cifrado de datos**

Esta característica le permite convertir texto legible en texto ilegible, asegurando que solo el destinatario pueda convertirlo en texto legible.

Hay una serie de tecnologías de encriptación de datos que operan en diferentes niveles del modelo OSI y, por cierto, puede encontrar algoritmos de encriptación a nivel de enlace de datos y algoritmos de encriptación a nivel de red. Desde una perspectiva de seguridad, necesita saber qué tecnología de encriptación usa su organización, la fuerza de su encriptación y qué productos afectan directamente la seguridad de una VPN. (Ñacato, 2007).

2.2.8. Beneficios de una VPN

Los beneficios que ofrece una VPN en términos generales, se usan para describirlos al implementar la tecnología VPN, entre estos podemos destacar:

- **Seguridad**

En particular una VPN posee alta seguridad, el cual requiere la creación de un túnel a la red corporativa y cifra los datos de la computadora con el usuario y los servidores de la empresa. Utilizan protocolos de encriptación y autenticación estándar de la industria, lo que permite que los datos se oculten en un entorno web no seguro, pero que aún estén disponibles para los usuarios comerciales a través de una VPN.

En aquellas áreas donde se pueden realizar los beneficios potenciales, parece que todas las organizaciones deberían aplicar esta nueva tecnología de inmediato.

- **Transparencia**

En términos de transmisión, los usuarios de VPN tienen control total sobre la transmisión de información, una vez que se autentica el servidor VPN.

- **Flexibilidad**

Las VPN proporcionan más métodos de acceso que las WAN normales. Cada negocio tiene diferentes opciones de ancho de banda. Además, gracias al uso de túneles de protocolo y proxies de aplicación, es posible utilizar Internet en sistemas que no son totalmente compatibles con Internet.

- **Facilidad de instalación**

La configuración utiliza un software de cliente estándar, haciendo que el sistema sea fácil de usar para todos los usuarios de la red.

- **Cobertura**

Las redes de internet ya son muy comunes en la mayoría de los centros comerciales del mundo, su cobertura puede ser el beneficio más tangible de pasar de una red privada a una infraestructura basada en IP. A diferencia del teléfono fijo de una compañía telefónica, una conexión punto a punto a Internet es como una densa red de muchas redes, todas conectadas hasta el último rincón de la tierra.

- **Ahorro en los costos**

Las VPN ofrecen ahorros directos en comparación con otros métodos de comunicación, como líneas privadas y llamadas de larga distancia, y también brindan beneficios indirectos al reducir los costos de capacitación y equipos.

Las líneas privadas tradicionales ofrecen una ventaja a las empresas con altos requisitos de ancho de banda. Sin embargo, gran parte de este ancho de banda no es utilizado continuamente por las medianas empresas. En todos los casos existe la necesidad de pagar por la comunicación entre nodos remotos, principalmente porque son enlaces duros con recursos reservados.

Una conexión a Internet es más barata que una conexión de línea fija. generalmente las líneas arrendadas poseen un costo de conexión fijo y otro costo dependiente de la distancia, sin embargo, con este tipo de transporte, el costo aumenta significativamente a medida que aumenta el tamaño de la red. La idea de una VPN reducirá drásticamente los costos de conexión, (Ñacato, 2007).

2.2.9. Elementos de una VPN

Para el diseño de una Red VPN se necesita utilizar elementos, los mismos que se detallan a continuación:

- **Servidor VPN**

Esta es la computadora que recibe conexiones de clientes VPN mediante la red pública internet, actúa como enrutador.

- **Cliente VPN**

Es una computadora donde se inicia una conexión a un servidor VPN.

- **Conexión VPN**

Una conexión VPN es el enlace en donde los datos son encriptados para proporcionar acceso seguro a la red.

- **Túnel**

Forman las partes de la comunicación en las que se encapsulan los datos, los protocolos de tunelización utilizados para administrar los túneles y la encapsulación de datos privados.

- **Red Publica**

Es una red que proporciona servicios de comunicación que permiten transferir datos de un lugar a otro de una manera menos segura porque la información que viaja por la red puede ser interceptada por un tercero. Las redes públicas permiten la encapsulación de datos transmitidos a través de una conexión VPN.

- **Switch**

Es un dispositivo que conecta redes informáticas que operan en la capa 2 (capa de enlace de datos) del modelo OSI. Su función principal es conectar dos o más dispositivos, sirve como un puente que transmite datos de la red

- **Enrutador**

Dispositivo que ayuda a conectar computadoras que forman parte de una red. Es responsable de crear la ruta que se usará para cada paquete de datos, decidir qué método será el más económico para transferir información, enrutamiento entre dos o más redes, el objetivo es transferir información a través de la red desde un origen a un destino.

- **Firewall**

Es un sistema que puede proteger una computadora o una red informática, puede filtrar paquetes de datos que pasan por la red y se basa en instalar una barrera entre la computadora y los datos transmitidos. Por la red a través de software o hardware,

permitiendo autorizar o denegar según determinadas instrucciones allí configuradas. Es decir, se conecta al perímetro de la red de la organización para evitar el acceso de usuarios no autorizados.

- **Concentradores**

Son dispositivos que permiten la arquitectura de cableado de una red, incluyen anillos electrónicos, tarjetas y conectores que incluyen tecnología de conmutación de paquetes, y cuentan con herramientas de monitoreo y gestión para controlar el examen y diagnóstico de su actividad.

- **Conexión VPN de acceso remoto**

VPN es un servicio que permite el acceso remoto a la red interna de una organización, conexión VPN, el acceso remoto lo realizan clientes que cuentan con computadoras personales, conectados a una red privada en la cual un servidor VPN permite a los usuarios acceder a los recursos de la misma o a los recursos de toda la red, con autenticación mutua entre el servidor VPN y el cliente.

2.2.10. Arquitecturas VPN

- **VPN LAN TO LAN**

- Este esquema se utiliza para conectar oficinas remotas a la sede de la organización. Servidor VPN, con enlace a internet fijo. Acepte conexiones a Internet desde sitios web y configure túneles VPN. El servidor de la sucursal se conecta a Internet utilizando el servicio del ISP local. Por lo general, a través de conexiones de banda ancha. Esto elimina el costo de los enlaces punto a punto tradicionales, particularmente en las conexiones internacionales.

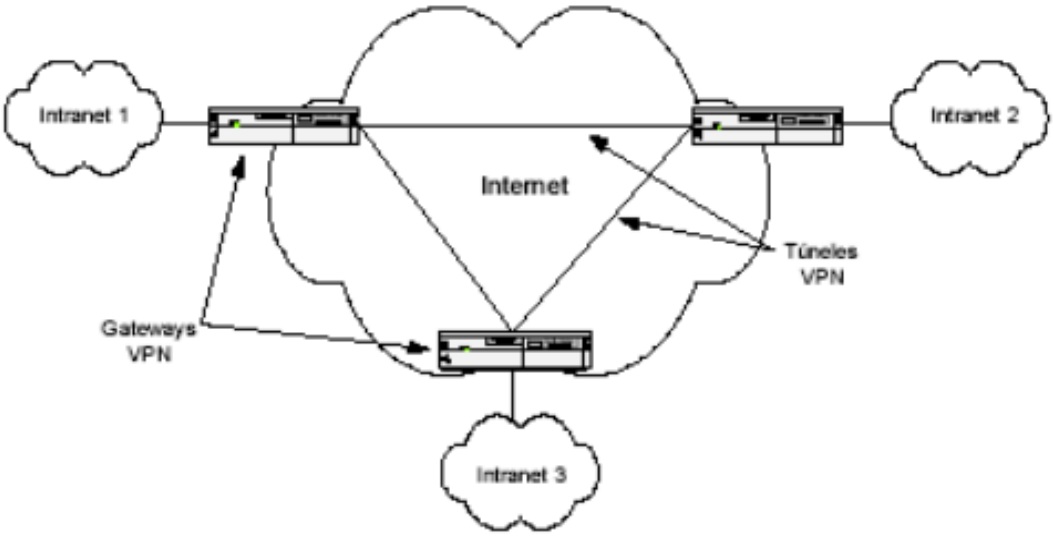


Figura 9: Solución VPN (LAN TO LAN)

Fuente: Gabriel (2008).

Tradicionalmente, para conectar dos o más oficinas remotas de una misma empresa, era necesario contratar enlaces de canales libres permanentes o circuitos virtuales. Las empresas adoptan diferentes topologías de WAN para conectar todos sus sitios remotos, incluidos: enlaces de red punto a punto, en estrella, parciales y completos, (Gabriel, 2008).

Esta configuración es de dos tipos:

- **Intranet**: Si una empresa tiene al menos una sucursal remota que se une a una red privada, puede hacerlo creando una VPN para conectar las dos redes, teniendo acceso únicamente los empleados.

- **Extranet**: Si una empresa tiene una relación cercana con otra empresa, (colaboradora, proveedora o cliente), puede desarrollar una red privada virtual, permitiendo un acceso compartido con usuarios externos.

Gracias a la arquitectura VPN externa, cada empresa debe controlar cuidadosamente el acceso a los recursos de la red de la empresa y los datos que se intercambiarán con los socios comerciales. Construir una topología VPN para redes externas implica complejidad en los sistemas de autenticación y control de acceso..

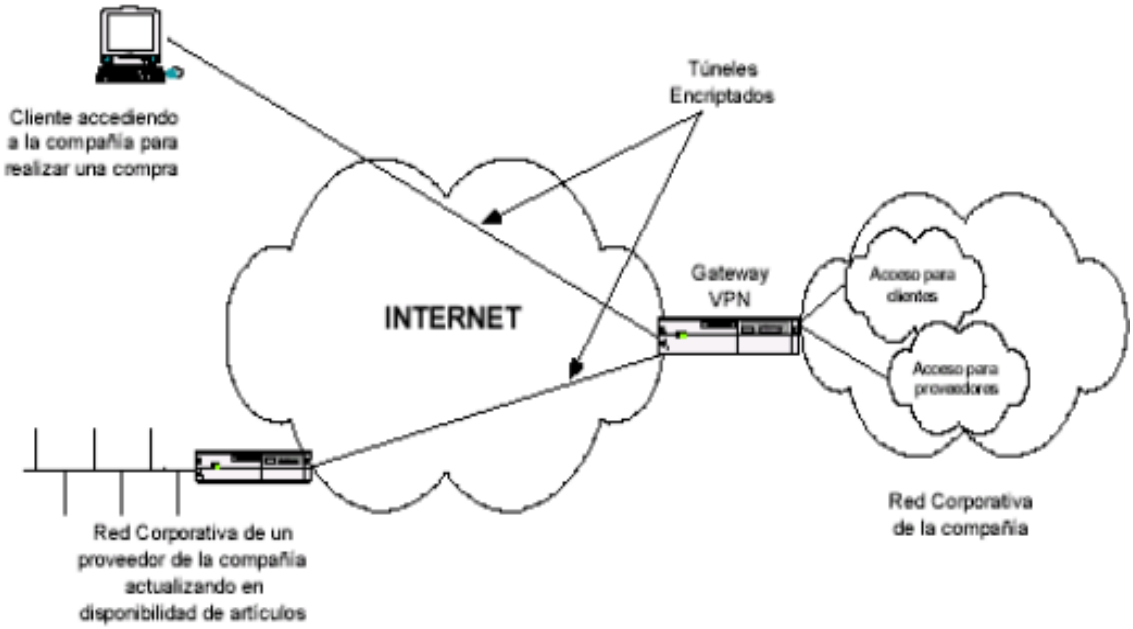


Figura 10: Diagrama de Extranet VPN.

Fuente: Gabriel (2008).

- **Acceso remoto VPN**

También conocido como VPNDN (telefonía de red privada virtual), este es probablemente el modelo más utilizado en la actualidad e incluye usuarios o proveedores de servicios que se conectan a una empresa desde ubicaciones remotas, oficina, hogar, hotel, avión, etc., utilizando internet.

Diferentes empresas reemplazaron su infraestructura de acceso con esta tecnología, incluso si conservan los módems antiguos por razones urgentes. Con el acceso VPN remoto, por ejemplo, un empleado se ha mudado a otro país y quiere acceder a la base de datos de la empresa, al correo electrónico interno o a cualquier otro recurso dentro

de la empresa, simplemente conéctese a Internet con una simple llamada loca al ISP de su ciudad y comience. su cliente de conexión VPN.

A partir del lanzamiento de Windows 98, Microsoft incluyó un cliente VPN de acceso telefónico que funciona con el protocolo de tunelización PPTP. Todas las puertas de enlace VPN vienen con software de cliente VPN para ser instalado en diferentes sistemas operativos en el mercado, (Gabriel, 2008).

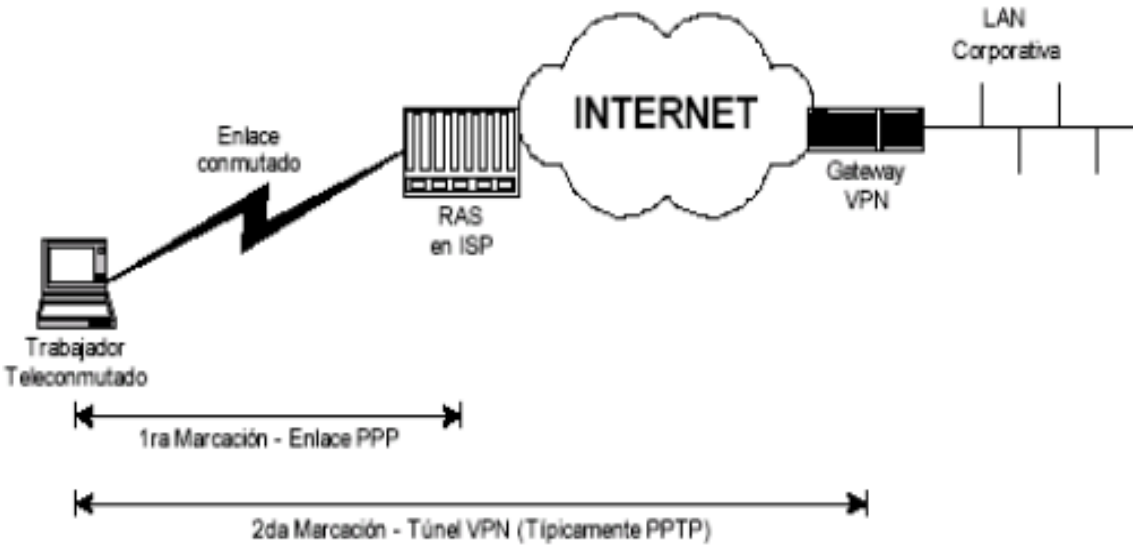


Figura 11: Diagrama de VPN por acceso remoto.

Fuente: Gabriel (2008).

- **Modelos de entunelamiento**

Muchos de los protocolos que se utilizan para transferir datos de un dispositivo a otro a través de una red, a falta de encriptación o medios seguros para evitar que nuestras comunicaciones sean interceptadas y rastreadas. HTTP, FTP, POP3 y muchos otros protocolos ampliamente utilizados utilizan conexiones de red explícitas. Este es un problema grave en cualquier situación en la que queramos transferir información sensible entre dispositivos, como cuentas de usuario (nombre de usuario y contraseña), y no tener un control absoluto sobre ellas. Para la creación de redes, para evitar que nadie intercepte

nuestra comunicación a través de la tecnología man-in-the-middle, como ocurre con las redes de red.

El problema del protocolo es que envía los datos en texto claro, es decir, sin cifrar, por lo que cualquier persona con acceso físico a la red a la que está conectada la máquina puede ver los datos. De esta forma, alguien que conecte su ordenador a una red y utilice un sniffer puede recibir y analizar todos los paquetes que circulan por esa red. Si alguno de estos paquetes envía una comunicación sin cifrar y pertenece a un protocolo que contiene información confidencial, esa información está en riesgo.

Por otro lado, si las conexiones están cifradas con un sistema que solo permite que dos hosts se entiendan entre sí, entonces no hay nada que puedan hacer los interceptores de paquetes de la tercera máquina, porque no podrán descifrar los mensajes.

Una forma de evitar este problema es utilizar una técnica llamada tunelización. Esta tecnología consiste básicamente en abrir conexiones entre dos dispositivos a través de un protocolo seguro, como SSH (Secure SHell). A través de los cuales se realizan transferencias no garantizadas, por lo tanto, son seguras, (Gabriel, 2008).

- **VPN interna**

Este esquema es el menos común, pero uno de los más poderosos para uso empresarial. Es un tipo de método diferente de acceso, en lugar de utilizar Internet como medio de comunicación, utiliza la propia red de área local (LAN) de la empresa. Se utiliza para aislar áreas y servicios de la red local interna. Esta capacidad es importante para mejorar las funciones de seguridad de una red inalámbrica.

La mayoría de los incidentes de seguridad involucran abusos en las redes corporativas, por lo que, aparte de los ataques externos, nadie debe prestar atención a los

ataques internos. Dependiendo del tipo de negocio o por razones legales, alguna información puede ser privada y confidencial a nivel del Ministerio.

Las VPN de varias secciones pueden ayudar a cumplir con estos requisitos de privacidad. El ejemplo clásico es un servidor que contiene información confidencial, como la nómina, ubicado detrás de un grupo de VPN y que proporciona autenticación adicional, así como encriptación adicional, lo que permite que solo el personal de recursos humanos autorizado acceda a la información, (Gabriel, 2008).

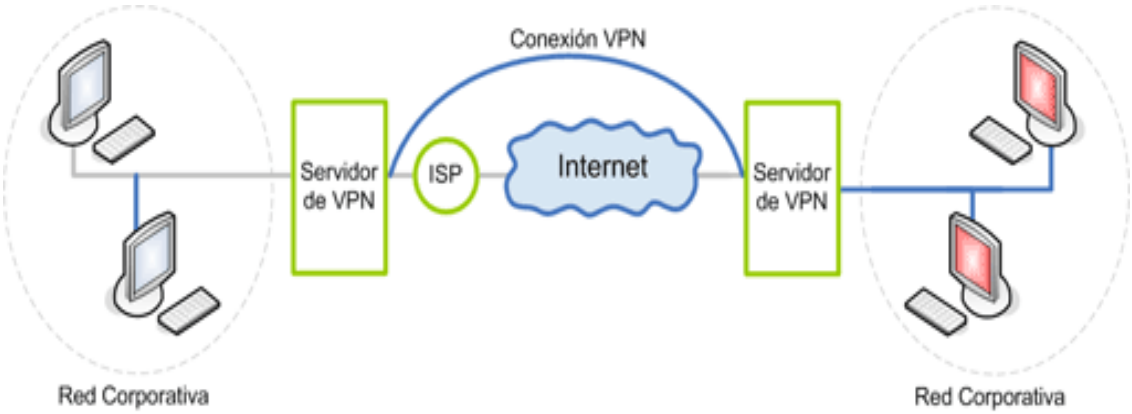


Figura 12: Arquitectura VPN interna.

Fuente: Gabriel (2008).

2.2.11. Tecnologías VPN

- **Confidencialidad de datos**

Es el servicio más importante que ofrecen las aplicaciones VPN. La privacidad es esencial porque los datos privados se envían a través de redes públicas y se pueden lograr por medio del cifrado de datos. Los datos enviados de una computadora a otra se codifican en un formato que solo otras computadoras pueden decodificar.

- **Integridad de los datos**

Si bien es importante cifrar los datos en una red pública, es igualmente importante verificar que los datos no hayan sido alterados en tránsito. Por ejemplo, IPsec tiene un mecanismo para garantizar que la parte cifrada de un paquete, o la parte completa del encabezado y los datos de un paquete, no haya sido alterada. Si se detecta una manipulación, el paquete se descarta. La integración de datos también puede incluir la autenticación de pares remotos.

- **Autenticación de origen de datos**

Verificar la identidad de la fuente de datos transmitida es importante, para protegerse de algunos ataques que utilizan la suplantación de identidad.

- **Confidencialidad o tunelizado de datos**

Es el proceso de encapsular un paquete completo dentro de otro y enviarlo a través de una red. La tunelización es útil en los casos en que se recomienda anonimizar el dispositivo que genera el tráfico. Por ejemplo, una máquina que usa IPsec encapsula el tráfico de varios servidores detrás de ella y agrega sus propios encabezados a los paquetes existentes. Al codificar el encabezado original del paquete y enrutarlo en función del encabezado de Capa 3 adicional agregado en la parte superior, el dispositivo de tunelización oculta efectivamente la fuente real del paquete. Es importante tener en cuenta que un túnel por sí solo no proporciona seguridad de datos. El paquete original solo se encapsula en otro protocolo y aún puede ser visto por el dispositivo de captura de paquetes si no está encriptado. Sin embargo, es por eso que es una parte integral de la forma en que funciona una VPN.

El tunelado consta de tres protocolos:

- **Protocolo de pasajero:** se transmiten los datos originales (IPX, NetBeui, IP).
- **Protocolo de encapsulación:** El protocolo (GRE, Ipsec, L2F, PPTP, L2TP) encapsula los datos originales.
- **Protocolo de transporte:** Es utilizado por la red por el cual se transmite la información.

El protocolo de pasajeros se encuentra en el protocolo de encapsulación, para ser colocado en el encabezado del protocolo del operador (generalmente IP) para su transmisión a través de la red pública. Para las VPN de sitio a sitio, el protocolo de encapsulación suele ser Ipsec o Encapsulación de enrutamiento genérico (GRE) incluyendo información sobre el tipo de paquete que encapsula y la información sobre la conexión entre el cliente y el servidor. Para las VPN de acceso telefónico, la tunelización generalmente se realiza mediante el Protocolo punto a punto, como parte de TCP/IP, es compatible con otros protocolos IP cuando se comunica a través de una red entre una computadora host y un sistema remoto. El túnel PPP utilizará uno de los métodos de transporte PPTP, L2TP o Cisco Layer 2 (L2F), (Cisco, 2008).

- **AAC Autenticación, autorización y cuenta**

Estos se utilizan para un acceso más seguro en un entorno VPN de acceso remoto. Cualquier computadora portátil o PC que use un software de cliente VPN correctamente configurado puede conectarse de manera segura a una red remota sin autenticación de usuario. Sin embargo, la autenticación de usuario también requiere que ingrese un nombre de usuario y una contraseña válidos antes de establecer una conexión. El nombre de usuario y la contraseña se pueden almacenar en el propio terminador VPN o en un servidor AAC externo que puede proporcionar autenticación a muchas otras bases de datos, como Windows NT y Novell LDAP. etc. Cuando la aplicación de acceso telefónico

envía una solicitud para crear un túnel, el dispositivo VPN solicita un nombre de usuario y una contraseña. Luego puede autenticar esto localmente o enviarlo a un servidor AAC externo para su verificación.

- Quién eres (autenticación)

- Qué se puede hacer (permisos)

- ¿Qué está haciendo realmente (contando)

La información de la cuenta es particularmente útil para rastrear el uso del cliente con fines de auditoría, facturación o informes de seguridad. (Cisco, 2008).

2.2.12. El protocolo IPSEC

2.2.12.1.Descripción del protocolo

Es básicamente un conjunto de estándares para integrar funciones de seguridad basadas en cifrado en IP. Brinda seguridad, integridad y confiabilidad de gráficos IP, combinando tecnología de clave pública, algoritmos de encriptación (DES, 3DES, IDEA, Blowfish), algoritmos hash (MD5, SHA) 1) y certificados digitales X509v3.

Debido a que el protocolo IPsec es modular, puede definir el conjunto de algoritmos que necesita sin afectar el resto de su implementación. Sin embargo, se definen algunos algoritmos estándar que todas las implementaciones deben admitir para garantizar la interoperabilidad en el mundo global de Internet. Estos algoritmos de referencia son DES y 3DES para cifrado y MD5 y SHA1 para funciones hash. Además, es perfectamente posible utilizar otros algoritmos que se consideren más seguros o más adecuados para un entorno concreto. Por ejemplo, se espera que los últimos algoritmos criptográficos IDEA Blowfish o Symmetric AES se utilicen ampliamente en un futuro próximo.

Figura 13: Tecnologías utilizadas en Ipsec.

Fuente: Algoritmos utilizados por Ipsec (Bautista, Cárdenas y Santos, 2008).

En Ipsec se distinguen los siguientes componentes:

- Dos protocoles de seguridad: el encabezado de autenticación IP (AH) y la carga útil de seguridad de encapsulación IP (ESP) proporcionan mecanismos de seguridad para proteger el tráfico IP.
- Protocolo de administración de claves de Internet Key Exchange (IKE) que permite que dos nodos negocien claves y todos los parámetros necesarios para establecer una conexión AH o ESP, (Perez, 2011).

2.2.12.2. Protocolo AH

El protocolo AH es un proceso que se puede usar en IPsec para garantizar la integridad y confiabilidad de los gráficos de IP. Es decir, proporciona al destinatario del paquete IP un medio para autenticar la fuente de los datos y asegurarse de que los datos

no hayan sido manipulados durante la transmisión. Sin embargo, no hay garantía de seguridad. En otras palabras, puede ver los datos enviados por un tercero.

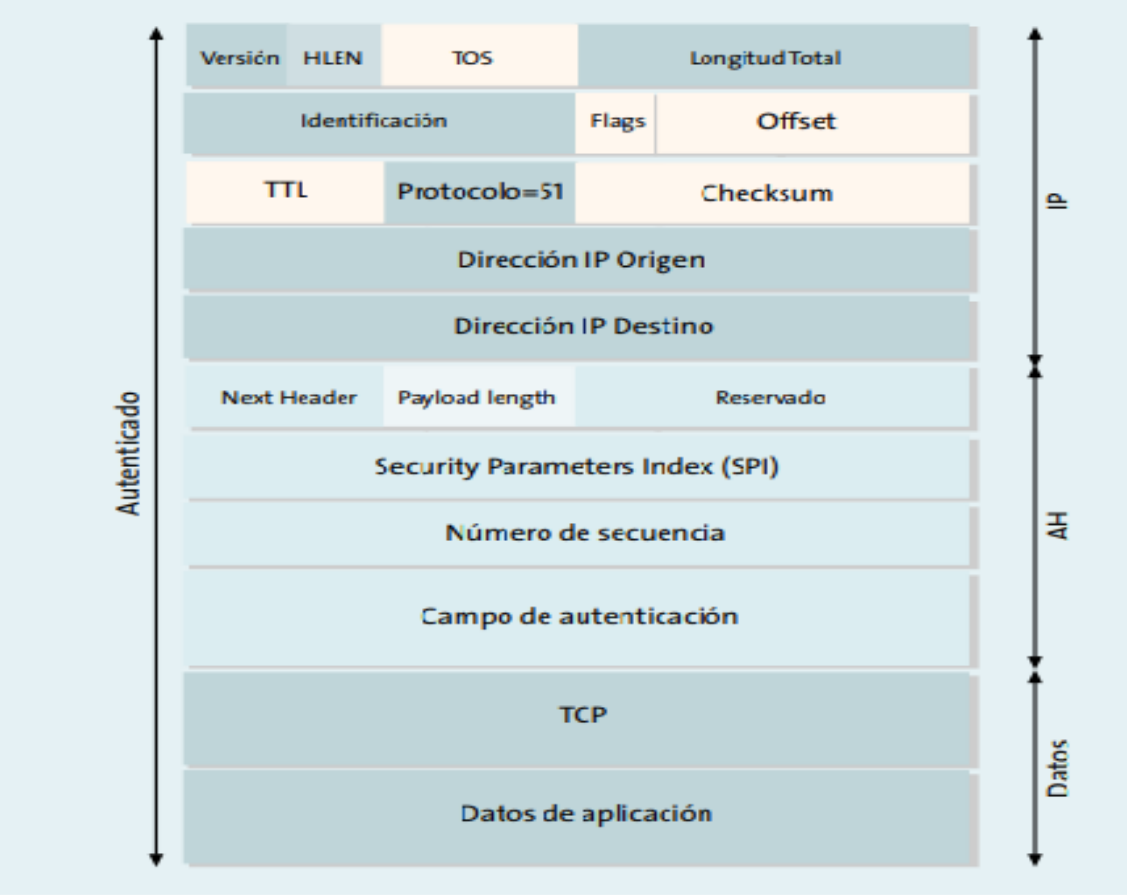


Figura 14: Estructura de un datagrama AH.

Fuente: Algoritmos utilizados por Ipsec (Bautista, Cárdenas y Santos, 2008).

Como su nombre lo indica, AH es el encabezado de autenticación entre el encabezado IP estándar (tanto IPv4 como IPv6) y los datos que se envían. Este es un mensaje TCP, UDP, ICMP o un esquema IP completo (consulte la Figura 14). Dado que AH es en realidad un nuevo protocolo IP, IANA le ha asignado un número decimal de 5,1. Esto significa que el campo de protocolo en el encabezado IP contiene el valor 51 en lugar del valor 6 o 17 asociado con TCP y UDP respectivamente.

El AH en el encabezado indica el tipo de datos en la capa superior. Es importante señalar que AH garantiza la integridad y confiabilidad de los datos transmitidos y los

encabezados de IP, a excepción de los campos variables (TOS, TTL, etiqueta, compensación, suma de verificación). La funcionalidad de AH se basa en el algoritmo HMAC. h Código de autenticación de mensaje. Este algoritmo consiste en aplicar una función hash al conjunto de datos de entrada y aplicar una clave cuya salida es una pequeña cadena llamada extract. Esto indica que el extractor tiene las mismas propiedades que la llave. Las huellas dactilares están asociadas con los datos y la persona que los creó. Esto se debe a que solo él conoce la clave.

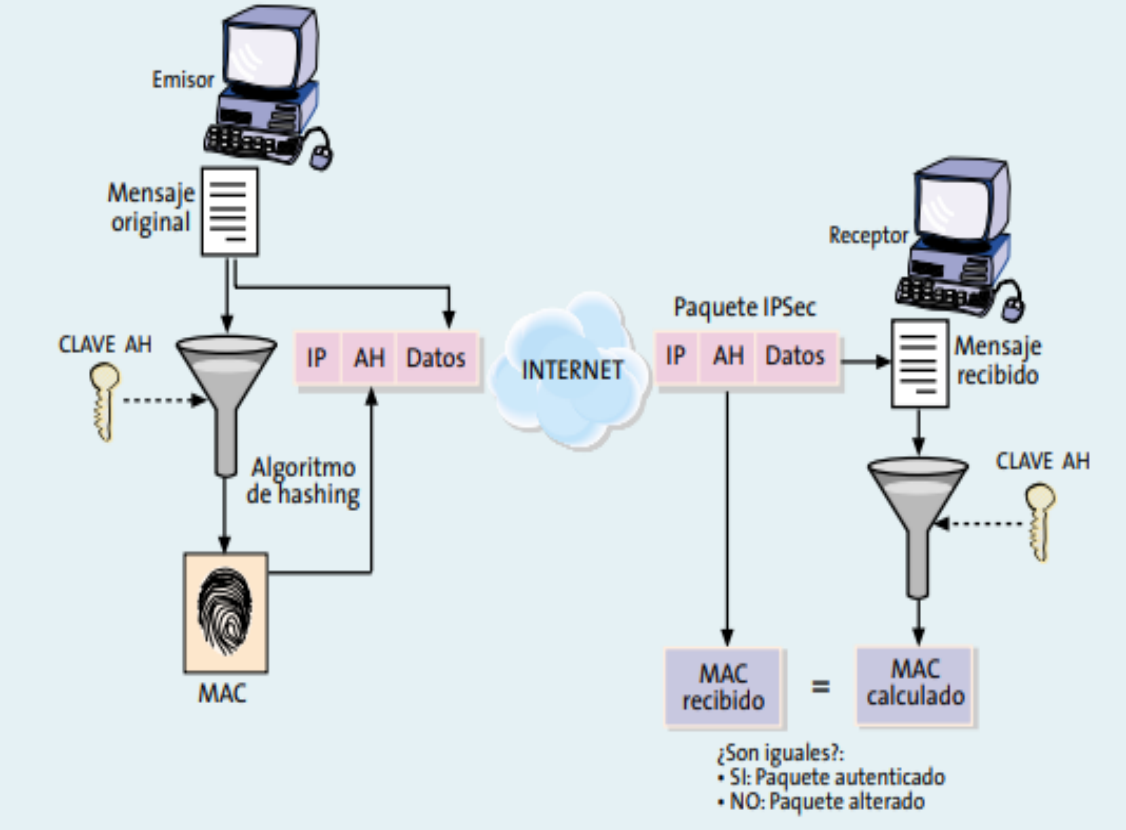


Figura 15: Funcionamiento del protocolo AH.

Fuente: Estrategias de aseguramiento de redes con IPSEC recuperado de XDOCS (Ávila, 2010).

(Fig. 15) muestra cómo funciona el protocolo AH, el remitente calcula un extracto del mensaje original, copiado en uno de los campos del encabezado AH. El paquete generado se transmite por la red, se itera al recibir el cálculo de extracción y comparación

con el paquete recibido en el paquete, si son idénticos, el receptor se asegura de que el paquete IP no haya cambiado durante la transmisión y desde el origen esperado. Si analizamos en detalle el protocolo AH, podemos concluir que su seguridad radica en que el cálculo de extracción (MAC) es imposible sin conocer la clave y que esta clave es conocida únicamente por el usuario, el emisor y el receptor, (Perez, 2011).

2.2.12.3. Protocolo ESP

El objetivo principal del protocolo de carga útil segura encapsulada (ESP) es garantizar la confidencialidad especificando cómo cifrar los datos transmitidos y cómo incorporar contenido cifrado en gráficos de IP.

Además, puede garantizar la integridad del origen de los datos y los servicios de autenticación al habilitar mecanismos similares a AH. Dado que ESP proporciona más funciones que AH, el formato del encabezado es más complejo; Este formato incluye un encabezado y un tráiler alrededor de los datos transmitidos. Estos datos pueden ser cualquier protocolo IP (como TCP, UDP, ICMP o un paquete IP completo). La Figura 16 muestra la estructura del diagrama ESP. Aquí puede ver cómo se envía el contenido cifrado o la carga útil.

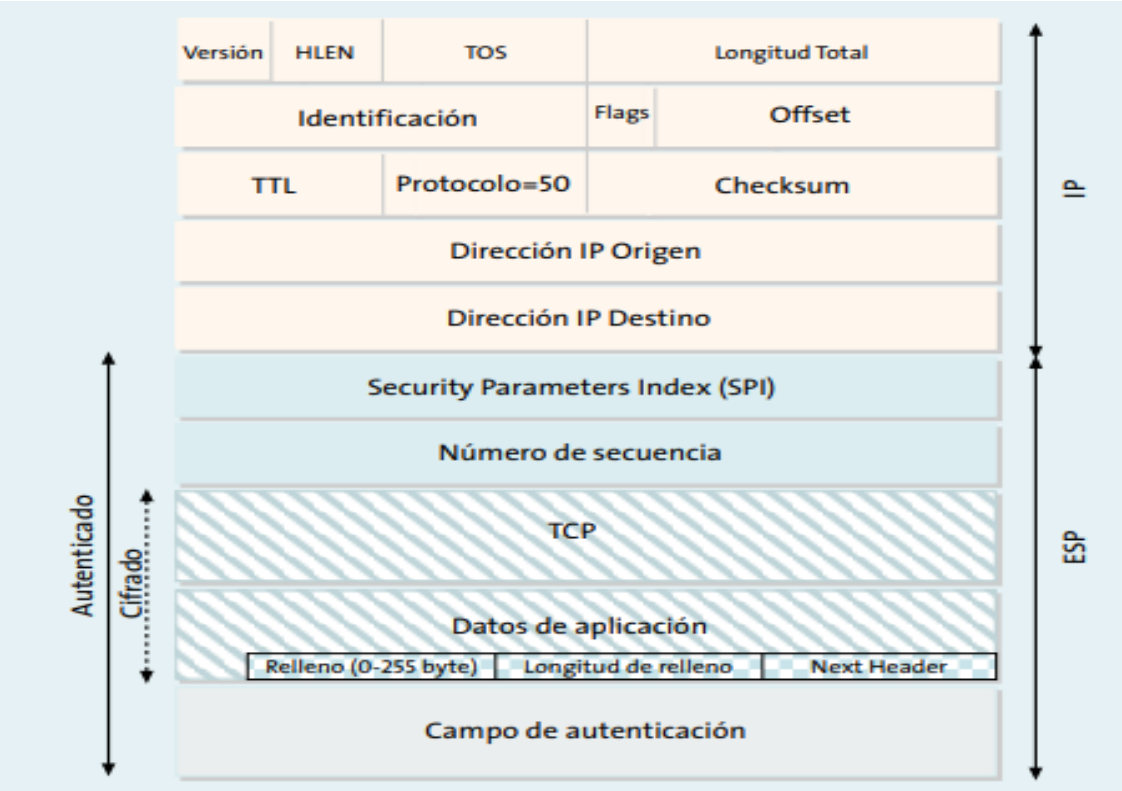


Figura 16: Estructura de un datagrama ESP.

Fuente: Estrategias de aseguramiento de redes con IPSEC recuperado de XDOCS (Ávila, 2010).

Debido a que los algoritmos de cifrado de bloques se usan comúnmente, la longitud de los datos cifrados debe ser un múltiplo del tamaño del bloque (o 16 bytes en la mayoría de los casos). Por lo tanto, la presencia de campos de relleno tiene una funcionalidad adicional, como se muestra en la Figura 17. Puede agregar caracteres de relleno al campo de datos para ocultar la longitud real, es decir, las características del campo de datos. Un atacante experimentado puede extraer información específica del análisis de parámetros de comunicación específicos, incluidos parámetros cifrados, como la demora entre paquetes y la longitud del mensaje. Las funciones de almacenamiento en caché están diseñadas para dificultar este tipo de ataques.

La figura 17 muestra cómo ESP envía datos en secreto. El remitente recibe el mensaje original, lo cifra, lo usa y usa una clave específica para colocarlo en el paquete

IP seguido del encabezado ESP. Si un paquete es interceptado por un tercero mientras se reenvía a su destino, el paquete solo obtiene un conjunto de bits mixto. En el destino, el destinatario utiliza la misma clave para volver a aplicar el algoritmo de cifrado y restaurar los datos originales. Claramente, la seguridad de este protocolo radica en la robustez del algoritmo de cifrado. Esto significa que el atacante no puede descifrar los datos sin conocer la clave, y la clave ESP solo la conocen los usuarios emisores y receptores. (Perez, 2011)

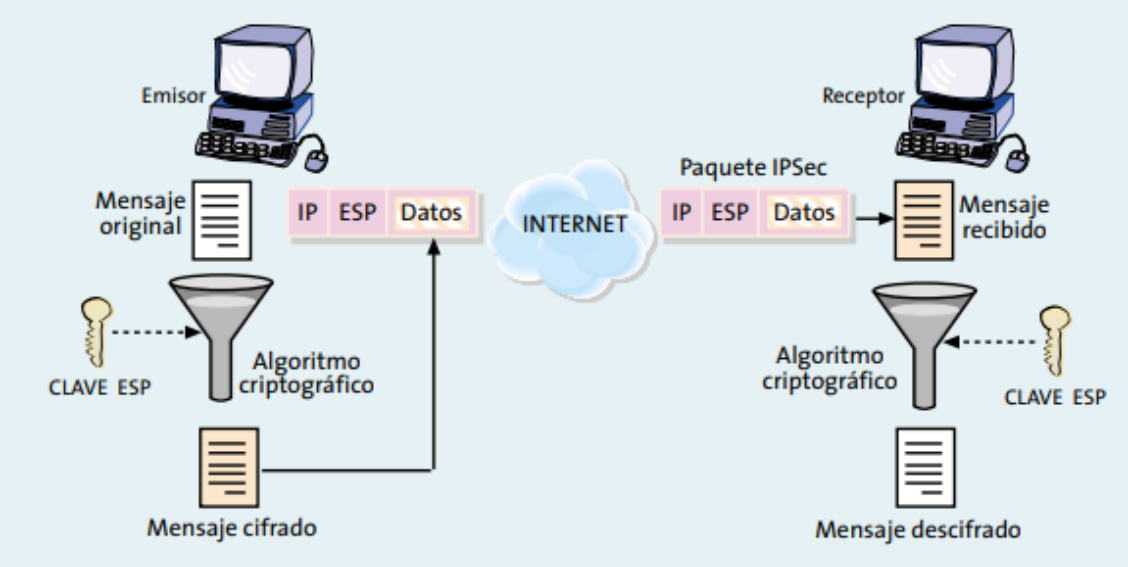


Figura 17: Funcionamiento del protocolo ESP.

Fuente: Estrategias de aseguramiento de redes con IPSEC recuperado de XDOCS (Ávila, 2010).

Por lo tanto, la distribución segura de claves es un requisito previo para el funcionamiento de ESP y también AH, como hemos visto antes. Asimismo, es fundamental que emisor y receptor estén de acuerdo tanto en el algoritmo de cifrado o hash como en el resto de parámetros comunes que utilizan, (Perez, 2011).

2.2.13. Los modos transporte y tunel.

2.2.13.1. El modo trasporte

En este modo, el contenido enviado por el sistema de datos AH o ESP son datos de la capa de transporte (como datos TCP o UDP), por lo que el encabezado IPSec se inserta inmediatamente después del encabezado IP y antes de los datos. El modo de transmisión tiene la ventaja de proporcionar una conexión de extremo a extremo, pero ambas partes deben comprender el protocolo IPSec.

2.2.13.2. El modo tunel

Si el contenido del esquema AH o ESP es un esquema IP completo. Dado que se incluye el encabezado IP original, se presenta el esquema IP con el primer encabezado AH o ESP agregado, luego se agrega el nuevo encabezado IP. Se utiliza para enrutar paquetes a través de la red. El modo túnel se usa comúnmente cuando el destino final de los datos no coincide con el dispositivo que realiza la función IPSec.

El modo de túnel se utiliza principalmente para determinar qué redes protege la puerta de enlace IPSec con la misma dirección IP. Esto centraliza el procesamiento del tráfico IPSec en su computadora. El modo túnel también es útil cuando se anonimizan los nodos conectados con ESP. Otra aplicación de demostración le permite crear una red privada virtual (VPN) en una red pública en modo túnel con ESP y AH. h Para una conexión segura a su red local, incluso si está utilizando una dirección privada o algo legítimo en Internet.

IPSec se puede implementar en servidores o dispositivos dedicados, como enrutadores y firewalls. Cuando se implementan estas características, se denominan

puertas de enlace IPSec. La Figura 18 muestra dos modos de operación para el protocolo IPSec:

- La parte A representa dos servidores que entienden IPSec y se comunican de forma segura. Dado que esta conexión está en modo de transmisión, solo el protocolo TCP o UDP y los datos de la aplicación son información protegida.
- La Parte B muestra dos redes que utilizan dos puertos IPSec para la comunicación. Por lo tanto, al usar la implementación del modo túnel, puede ver que la comunicación se lleva a cabo entre una computadora en la red local y otra computadora en la red pública de datos. Una computadora en una red local remota crea un túnel entre los puertos IPSec para proteger la comunicación entre las dos redes locales.

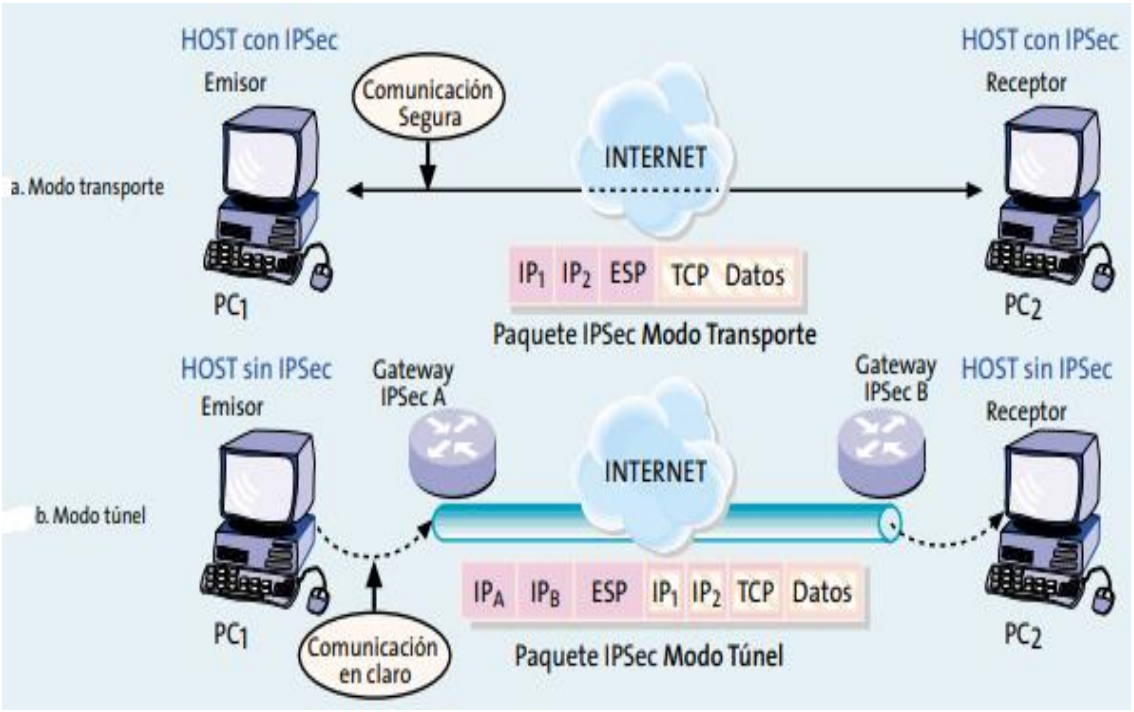


Figura 18: Modos de funcionamiento transporte y túnel en IPSec.

Fuente: Estrategias de aseguramiento de redes con IPSEC recuperado de XDOCS (Ávila, 2010).

Sin embargo, está claro que ambos dispositivos envían y reciben tráfico, como si estuvieran en la misma red local. Este esquema tiene la ventaja de que los nodos de una red fija pueden comunicarse de forma segura y transparente, al mismo tiempo que centraliza las funciones de seguridad en un punto, lo que facilita las actividades de gestión de la comunicación, (Perez, 2011).

2.2.14. IKE Internet key exchange

Este protocolo se utiliza para generar y administrar las claves necesarias para establecer una conexión de encabezado de autenticación (AH) y carga útil segura de encapsulación (ESP). Para establecer una conexión segura, dos o más participantes en una conexión IPsec deben ponerse de acuerdo sobre el tipo de cifrado y el algoritmo de autenticación. Esta configuración se puede realizar manualmente en ambos extremos del canal o a través de un protocolo que maneja la negociación automática de los participantes (protocolo IKE) (SA = Asociación de confidencialidad).

El protocolo IKE se encarga no solo de gestionar y gestionar claves, sino también de establecer conexiones entre cada participante. IKE no solo se puede usar con IPsec, sino que también se puede usar con varios algoritmos de enrutamiento como OSPF y RIP. IKE es un protocolo híbrido que integra dos protocolos complementarios, ISAKMP y Oakley. ISAKMP define colectivamente el protocolo de comunicación y la sintaxis de mensajes utilizados por IKE, y Oakley define la lógica para el intercambio seguro de claves entre dos partes previamente desconocidas.

El objetivo principal de IKE es crear una conexión cifrada y autenticada entre dos entidades. A través de esta conexión se negocian los parámetros necesarios para establecer una conexión IPSec segura. Estas negociaciones se desarrollaron en dos fases.

2.2.14.1. Primera fase IKE

Un escenario común para una aplicación donde ambos nodos crean un canal seguro y autenticado. Este canal seguro se logra utilizando encriptación simétrica y el algoritmo HMAC. La clave requerida se obtiene a partir de la clave primaria obtenida utilizando el algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad del contrato y requiere pasos adicionales para verificar la validez del contrato. Hay muchos métodos de autenticación, pero los más comunes se describen a continuación.

- El primer método de autenticación basado en el conocimiento de secretos compartidos. Un secreto compartido, es una cadena conocida solo por los dos que desean establecer una conexión IPSec. Mediante el uso de una función hash, cada parte se demuestra mutuamente que conoce el secreto sin revelar su valor y se autentica entre sí. Para evitar comprometer la seguridad de este mecanismo de autenticación, cada par de nodos debe tener un secreto diferente. Como resultado, la cantidad de secretos crece rápidamente con la cantidad de nodos, creando un entorno de IPsec múltiple. La gestión de claves de conexión de nodos es muy complicada. En este caso, le recomendamos que no utilice la autenticación de secreto compartido y, en su lugar, utilice la autenticación digital basada en certificados.

- El estándar IPSec prevé el uso de un método de autenticación basado en el uso de certificados digitales. El uso de un certificado le permite distribuir de forma segura la clave pública a cada nodo para que pueda probar su identidad al poseer la clave privada y alguna actividad criptográfica pública.

2.2.14.2. Segunda fase IKE

En esta fase se utiliza el canal de seguridad IKE para negociar parámetros de seguridad específicos relacionados con un protocolo específico (en este caso, IPSec). En esta fase se negocian las propiedades de la conexión ESP o AH y todos los parámetros requeridos. El equipo que inicia la conexión está configurado con una política de seguridad y ofrece todas las opciones posibles configuradas con prioridades configuradas. El primer sistema receptor aceptará aquel que cumpla con los parámetros de seguridad que haya establecido, y así mismo, ambos serán notificados del tráfico a intercambiar a través de dicha conexión.

Cómo funciona el protocolo IKE y cómo obtener la clave de sesión, la clave utilizada para proteger las conexiones ESP o AH, (De la luz, 2016).

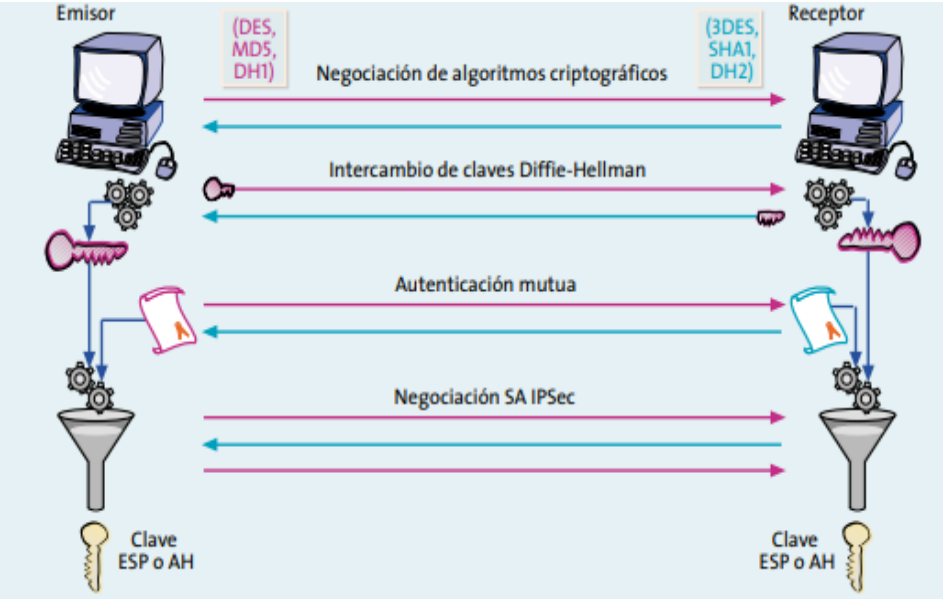


Figura 19: Funcionamiento del protocolo IKE

Fuente: Ipsec recuperado de Interworking (Barrera,2007).

2.2.15. Servicios de seguridad ofrecidos por IPSEC

- **Integridad y autenticación del origen de los datos**

AH es el protocolo más propicio si no hay necesidad de encriptación, la opción de autenticación del protocolo ESP brinda una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye un encabezado IP, esta opción tiene sentido. Muy importante para las aplicaciones que necesitan garantizar la estabilidad del contenido del paquete IP. IPsec tiene un mecanismo para garantizar que la parte cifrada del paquete, o el encabezado completo y la parte de datos del paquete, no se modifique. IPsec garantiza la integridad de los datos a través de la suma de verificación, una simple verificación de redundancia. Si se detecta manipulación, el paquete se cae.

- **Confidencialidad**

Los servicios de seguridad se obtienen a través de las funciones de cifrado incluidas en el protocolo ESP. En este caso, si no se garantiza la integridad de los datos, el cifrado no ayudará y deberá habilitar la opción de autenticación. Los datos enviados no pueden interpretarse como sin sentido, pero se aceptan como tráfico válido. Esto se puede lograr cifrando los datos antes de enviarlos a través de la red. Todos los datos enviados de una computadora a otra están encriptados para que solo otras computadoras puedan descifrarlos. Si la conexión está bloqueada, el hacker no podrá leer los datos. IPsec proporciona funciones de seguridad avanzadas, como algoritmos criptográficos sólidos.

- **Detección de repeticiones**

La autenticación protege contra la suplantación de IP, pero un atacante puede interceptar paquetes válidos y reenviarlos a su destino. Para evitar este ataque, tanto ESP como AH combinan acciones de detección de paquetes redundantes. Esta acción se indica

mediante el número de secuencia en el encabezado ESP o AH. El remitente aumenta este número para cada paquete enviado y el receptor lo verifica, por lo que se eliminan los paquetes redundantes.

El atacante no puede cambiar esta cadena porque está protegida por la opción de integridad de cualquier protocolo (AH o ESP) y cualquier cambio en este número hará que la verificación de integridad de la cadena no tenga éxito.

- **Control de acceso**

El uso de ESP y AH requiere el conocimiento de las claves, que son seguras a través de una sesión IKE para garantizar que ambos nodos se autentiquen entre sí y que solo los dispositivos necesarios compartan la conexión. Describe la autenticación y la autorización a las que se distribuirá. Tenga en cuenta que IPSec no significa acceso completo al recurso, ya que IPSec también proporciona la funcionalidad de autorización. Durante la negociación de IKE, el tráfico IP fluye a través de la conexión IPSec especificada. Esto es similar a un filtro de paquetes que tiene en cuenta el protocolo, las direcciones IP de las estaciones de origen y destino, los bytes y otros campos.

Por ejemplo, puede usar IPSec para permitir que las sucursales accedan a la red de área local del centro de negocios y evitar que el tráfico llegue a dispositivos especialmente seguros.

- **No repudio**

El no repudio es técnicamente posible en IPSec, si se utiliza IKE con autenticación mediante certificado digital, en este caso, la autenticación depende de la firma digital de un mensaje que contiene la identidad del participante junto con otros datos. La firma, gracias a la asociación entre la clave pública y la identidad asegurada por el certificado

digital, es una evidencia clara de que se ha establecido una conexión IPSec con una computadora específica, por lo que no puede ser pirateada. Rechazo. Sin embargo, en la práctica, esta prueba es más complicada, ya que requerirá almacenar mensajes de negociación IKE, además, no existe un procedimiento específico para procesar este evento en una fecha específica, (De la Luz, 2016).

2.2.15.1. Base de datos de seguridad

IPSec funciona con dos bases de datos de seguridad, una que contiene políticas de seguridad y otra que contiene asociaciones de seguridad, respectivamente SPD (Base de datos de políticas de seguridad) y SAD (Base de datos de asociaciones de seguridad). Policy Manager define un conjunto de servicios de seguridad para aplicar al tráfico IP entrante y saliente. Estas políticas se almacenan en SPD y las SA las utilizan cuando se crean. Todas las SA están registradas con SAD.

- **Bases de datos de asociaciones de seguridad (SAD)**

La base de datos SA almacena todos los parámetros relacionados con SA, y cada uno tiene una entrada en SAD donde se definen todos los parámetros necesarios para que IPSec procese los paquetes IP administrados por SA. Entre los parámetros que se encuentran en SAD están:

- Índice de normas de seguridad
- Protocolo utilizado por SA (ESP o AH)
- Cómo funciona el protocolo (tunelización o transferencia).
- Contador de números de serie
- Direcciones IP de origen y destino de SA.
- Utilizar el algoritmo de autenticación y la clave de autenticación.

- Algoritmo de cifrado y clave.

- Duración de las claves de autenticación y cifrado.

Los paquetes IP entrantes para ser procesados, se encuentra una SA adecuada en SAD que coincida con los tres valores siguientes: dirección IP de destino, tipo de protocolo IPsec y SPI. La dirección IP de destino y el tipo de protocolo IPsec se derivan del encabezado IP y el SPI se obtiene del encabezado AH o ESP. Si se encuentra la SA para el paquete IP entrante en cuestión, se manejará de acuerdo con los servicios de seguridad especificados. Entonces todas las reglas descritas en SPD para Government SA se aplican al paquete.

Para procesar los paquetes IP salientes, primeramente, se aplica el procesamiento relacionado con SPD. En caso de encontrar una política de paquetes salientes donde especifica que se requiere el procesamiento de IPSec, se busca un SAD para determinar si ya se ha creado una asociación de seguridad. Si se encuentra una entrada, el paquete se procesa de acuerdo con la SA; de lo contrario, si no se encuentra ninguna entrada para este paquete, se negocia una nueva SA y luego se almacena en la SAD. (Brollo, 2008).

2.2.16. Arquitectura cliente servidor

Desde un punto de vista funcional, la computación cliente/servidor se puede definir como una arquitectura distribuida que permite a los usuarios finales un acceso transparente a la información incluso en un entorno multiplataforma. Dado que la potencia de procesamiento se distribuye entre el cliente y el servidor, tiene una función de gestión de información centralizada.

Una red cliente/servidor es una red de comunicación en la que todos los clientes están conectados a un único servidor, centralizando los distintos recursos y aplicaciones

disponibles y poniéndolos a disposición según lo solicite el cliente. Esto significa que todas las acciones realizadas están centralizadas en el servidor, por lo que las solicitudes provienen de los clientes de protección, se definen los archivos compartidos y de uso, los archivos son de solo lectura y viceversa, se pueden modificar. Si se usa en una red mixta, este tipo de red se puede usar en conjunto (James, 2013).

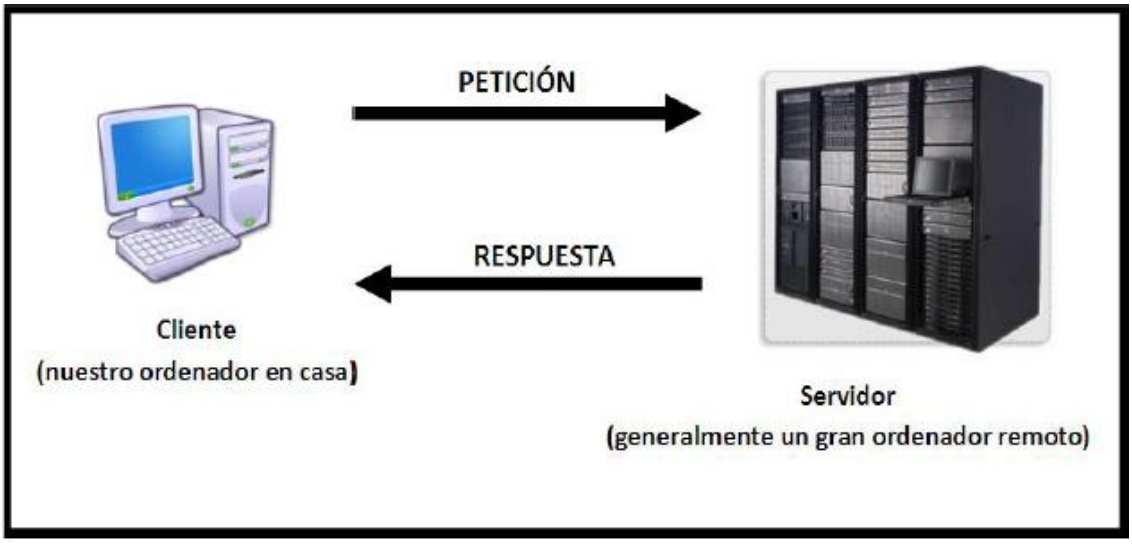


Figura 20: Esquema de la arquitectura cliente/servidor.

Fuente: (James,2013).

2.2.17. Centos LINUX

CentOS se deriva de las iniciales de Community Enterprise Operating System, una distribución de Linux para el mercado empresarial que busca una alternativa gratuita y compatible con Red Hat Enterprise Linux, y también es una distribución comercial basada en Gnu/Linux y es gratuita. contiene el siguiente conjunto: Servicios, soporte técnico y capacitación por los cuales se cobran suscripciones.

CentOS es un sistema de diseño muy estable. Es un excelente sistema para combinar cualquier plataforma para agregar seguridad, estabilidad, confiabilidad, seguridad y un rendimiento poderoso.

Es un servidor ideal no solo para la web sino también para virtualización como también para apoyar la infraestructura de nube muy familiar. CentOS soporta los métodos principales de virtualización como VMware, XEN, KVM, contenedores etc.

2.2.17.1. Ventajas y desventajas de CentOS LINUX

- **Estabilidad**

CentOS es uno de los sistemas Linux más estables del mercado y es ideal para servidores. Además, a diferencia de otros sistemas tradicionales, se basa en una de las mejores distribuciones de servidor, RHEL, y elige cuidadosamente los paquetes que se instalan por defecto. Para mayor estabilidad, solo las versiones estables de los paquetes están en el repositorio. Almacenamiento predeterminado.

- **Velocidad**

Al eliminar los paquetes innecesarios e instalar solo los paquetes necesarios, se obtiene un sistema más liviano donde se identifican el núcleo, los módulos que se usan con más frecuencia y los servicios.

- **Confiabilidad**

Es un sistema muy poderoso que usa menos paquetes, menos actualizaciones y simplifica la administración. El ciclo de vida es de aproximadamente 5 años con soporte completo y 10 años con renovaciones importantes. Este es un tiempo razonable a diferencia de otras distribuciones.

- **Software**

Otra gran ventaja de CentOS es la disponibilidad de software especializado, especialmente en el mundo del alojamiento, como ser compatible con cPanel, Plesk, CloudLinux y la mayoría del software de seguridad con licencia.

- **Respaldo y Soporte**

No brinda el mismo soporte que RHEL o Ubuntu, pero tiene una gran comunidad y una extensa documentación, y la mayor parte de la documentación de RHEL se basa en CentOS, por lo que es compatible con CentOS.

- **Requerimientos de hardware**

CentOS se puede instalar con o sin un entorno gráfico de Windows. Si su sistema está diseñado para estaciones de trabajo, tiene la opción de instalarlo en un entorno gráfico, pero para servidores, la opción de escritorio es para escritorio, no se requiere entorno. Instalar mejor el sistema sin entorno gráfico, (De leon, 2020).

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

2.3.1. Red VPN

Es una tecnología de red que permite la extensión segura de redes de área local (LAN) a través de redes públicas censuradas o no reguladas, Se permiten subredes o Internet, lo que permite que la computadora en red tenga todas las características, políticas de seguridad y administración de redes privadas. Puede enviar y recibir datos a través de una red compartida o pública. red como si fuera una red de área local, dependiendo del tipo de VPN, puede ser un sistema de seguridad dedicado, una conexión encriptada o una combinación de ambos métodos, esto se hace estableciendo una conexión a través de.

2.3.2. IPSEC

Es un marco de estándares abiertos para lograr comunicaciones privadas seguras sobre redes IP mediante el uso de servicios de seguridad encriptados. Se puede usar para cifrar el tráfico directamente entre dos computadoras (conocido como modo de transferencia) o para crear "túneles virtuales" entre dos subredes, que se pueden usar para la comunicación segura entre dos redes corporativas (conocido como modo de túnel).

2.3.3. Modelo

Un modelo informático es una representación de la realidad a través de abstracciones. El modelo se enfoca en algunas partes importantes del sistema (al menos aquellas que se relacionan con un tipo particular de modelo), reduciendo otras partes.

El modelo de información es una representación formal y abstracta del tipo de entidad que reside en su dominio. Estas entidades pueden ser objetos reales o representaciones de sistemas de software y objetos de procesos comerciales.

2.3.4. Infraestructura de red

- Por infraestructura de red entendemos todos los elementos básicos e imprescindibles de cualquier organismo u organismo público o privado (negocio, oficina o industria) que requiera total o parcialmente de los siguientes servicios de comunicación: teléfono, fax, ordenador, escáner, impresora, TPV, control , CCTV y control de accesos Los equipos de datos, climatización, extinción de incendios, etc. son las instalaciones, servicios e instalaciones técnicas necesarias para el desarrollo de una actividad o uso de un lugar.

- Los diversos componentes que componen una infraestructura de red son:

- sistema de cableado estructurado
- - equipo de comunicación eléctrica
- SAI: Sistema de alimentación ininterrumpida para ordenadores
- Sala de comunicaciones
- - Seguridad y control
- - red electrónica

2.3.5. LINUX

Es un sistema operativo como macOS, DOS o Windows. En otras palabras, Linux es el software que su computadora necesita para permitirle usar software como: editores de texto, juegos, navegadores de Internet, etc.

Linux se puede usar a través de una interfaz gráfica de usuario como Windows o macOS, pero también se puede usar a través de la línea de comandos como DOS. Linux se deriva de Unix. Este apareció en la década de 1960, desarrollado por los investigadores Dennis Ritchie y Ken Thompson de Bell Telephone Laboratories.

2.3.6. Servidor

Un servidor es un dispositivo que funciona para procesar solicitudes y entregar datos a otras computadoras que pueden conectarse a los clientes. Esto se puede hacer a través de su red local o de Internet. Los servidores generalmente consisten en potencia de procesamiento adicional, memoria y espacio en disco para manejar mejor la carga en el cliente de servicio. Podemos enumerar los tipos de servidores más comunes de la siguiente manera:

- Una base de datos de Internet.

- Un servidor proxy.

- Servidor FTP.

- Servidor de juegos en línea

Muchos sistemas en Internet utilizan un modelo de red cliente-servidor, como sitios web y servicios de correo electrónico. La alternativa cliente-servidor es un modelo peer-to-peer en el que cualquier dispositivo de la red puede actuar como servidor y cliente según sea necesario.

2.3.7. Virtualización

Es una tecnología de software que permite que muchos sistemas operativos diferentes actúen como invitados en un solo servidor físico. Estos se denominan máquinas virtuales (VM) que se ejecutan en hosts que simulan la virtualización. Por ejemplo, todo funciona como si los recursos de un servidor físico estuvieran divididos en múltiples servidores virtuales que pueden usarse para diferentes propósitos. Esta tecnología es una de las formas más efectivas de reducir el costo de su infraestructura de TI. De hecho, la virtualización se puede aplicar a servidores, redes, aplicaciones y centros de datos. Además, aporta eficiencia y flexibilidad a los negocios de sus clientes sin superar las inversiones presupuestarias tradicionales en TI. Es importante comprender que, con la virtualización de servidores, los procesos se distribuyen en menos computadoras, de modo que cada computadora pueda aprovechar mejor su capacidad total. Sin embargo, no tiene sentido tener servidores secundarios que utilicen solo una fracción de los recursos de hardware.

2.3.8. VMWARE

VMware es una de las herramientas más populares utilizadas en el proceso de virtualización. Para una mejor comprensión, la virtualización es un recurso para simular un sistema operativo mediante un motor de software. En este caso, este programa es VMware. Con VMware, el sistema operativo se convierte en un servidor físico. Puede ejecutarlo como si fuera instalado, pero no porque esos sistemas operativos se estén ejecutando en otro sistema llamado servidor de almacenamiento.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. POBLACIÓN Y MUESTRA DE INVESTIGACIÓN

3.1.1. Población

La población se refiere a todos los sectores o entidades (organizaciones, cooperativas, pymes, etc.) que participan en la investigación, es por ello que la población está conformada por 10 instituciones de la ciudad que cuentan con al menos dos redes locales, para conocer su realidad en sus comunicaciones y la seguridad de sus datos.

3.1.2. Muestra

Para la muestra se simulará una organización con 2 sitios y 02 redes locales, con un proveedor de servicios de acceso a Internet en cada red.

3.2. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN.

3.2.1. Tipo y diseño de investigación

La investigación de este proyecto es de tipo experimental porque es un tipo de investigación que utiliza la lógica y los principios que se encuentran en la ciencia y se llevará a cabo en el modelo de infraestructura VPN y la verificación. La investigación es de carácter aplicado, ya que tendrá muchos procesos detallados de desarrollo, y al mismo tiempo será un modelo a aplicar en empresas u organizaciones.

Se realizó un experimento para analizar si y por qué una o más variables independientes afectan a una o más variables dependientes. Los experimentos se pueden

hacer en el laboratorio o en la vida real. Aquí se involucran un número relativamente pequeño de personas o equipos (Sampieri, 2015).

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Para la recolección de la información se utilizaron diversas herramientas como: entrevistas, documentos, informes impresos y encuestas que se detallan en el siguiente cuadro.

Tabla 1: Técnicas e instrumentos para recolectar información.

TECNICA	PROCEDIMIENTO	INSTRUMENTO
Observación	Un examen realizado directamente en el contexto en el que ocurrió el evento o fenómeno observado, con el fin de examinar todos los aspectos inherentes a la conducta, el comportamiento y las características de ese entorno.	Guía de observación
Entrevista	Se realiza comunicación verbal con los responsables de campo TI para obtener el estado del entorno objeto de estudio.	Entrevista abierta
Encuesta	Las preguntas abiertas se envían a los usuarios en formato electrónico para recopilar información.	Cuestionario

Elaboración propia.

Para el trabajo de investigación se utilizaron entrevistas verbales, incluido el interrogatorio. Esto se aplicó a los responsables del sector TI en las organizaciones de la ciudad de Puno.

3.4. MATERIALES EMPLEADOS

3.4.1. Recursos computacionales usado para la implementación y funcionamiento del modelo de red VPN

Para el desarrollo, implementación y funcionamiento se utilizaron los siguientes recursos:

- **Caso planteado**

Se tiene una empresa, la cual tiene 02 locales físicos: una en Puno y otra en Juliaca, cada local tiene una red LAN con 100 equipos disponibles entre PCs, laptops, impresoras red, servidores locales con sistemas de gestión.

En el local de Puno, la empresa tiene almacenados sus bases de datos, sus sistemas de gestión, sistemas de seguridad, etc.

Cada local tiene un acceso a internet con un enlace dedicado ADSL por un proveedor de internet peruano (movistar, claro o bitel).

El problema radica que se desea que las 02 redes separadas geográficamente, pero de la misma empresa, ya que el local de Juliaca necesita utilizar los recursos informáticos del local de puno.

Hay soluciones comerciales de IP-VPN dedicados que alquilan los proveedores de internet, pero son altos los costos mensuales de estos servicios. por lo tanto, se propone instaurar una VPN LAN to LAN con el protocolo IPsec, utilizando software libre como strongswan, en CentOS 7.8.

3.4.2. Recursos de Hardware

Tabla 2: Recursos hardware utilizados.

El hardware con el que se desarrolló la aplicación es:	
01	LAPTOP LENOVO 8G, 16GB RAM, M2 512MB, 01 HD 1TB
01	ROUTER ADLS – CON ENLACE PROVEEDOR DE INTERNET (CABLE ESTACION)
01	CABLE UTP, PATH CORD
01	HD USB EXTERNO 1TB

Elaboración propia.

3.4.3. Recursos de Software

Tabla 3: Recursos de Software.

SOFTWARE USADO EN EL DESARROLLO DE LA INTERFAZ DE LA VPN
CENTOS 7.8 X86_64 (SISTEMA OPERATIVO) – INSTALADO EN LOS SERVIDORES VPN C/U EN 02 LOCALES
WIN 10 PRO 64BITS (SISTEMA OPERATIVO) – INSTALADO EN LOS PC-CLIENTE C/U EN 02 LOCALES
PUTTY (CLIENTE SSH WINDOWS)
SQUID (PROXY) - APLICACIÓN DE RED EN LINUX
FIREWALLD (FIREWALL PERIMETRAL) - APLICACIÓN DE RED EN LINUX
BIND (SERVIDOR DNS) - APLICACIÓN DE RED EN LINUX
STRONGSWAN (SERVIDOR VPN IPSEC) - APLICACIÓN DE RED EN LINUX

Elaboración propia.

3.4.4. Recursos y materiales para la investigación

Tabla 4: Recursos y materiales para la investigación.

Horas de internet (500 aprox.)
Textos de Redes VPN
Artículos de seguridad informática.
Otros textos referidos a la investigación.

Elaboración propia.

3.4.5. Presupuesto

La Tabla 05 muestra el precio unitario del equipo de prueba, así como el costo total de implementación del modelo VPN.

Tabla 5: Presupuesto para la realización de la investigación.

Descripción	Unidad de medida	Costo unitario (S/.)	Cantidad	Costo Total (S/.)
Laptop	Unidad	4000.00	01	4000.00
Computadora	Unidad	3500.00	01	3500.00
Compra AP /Switch	Unidad	80.00	01	80.00
Pacht Cord de Red 2 mts	Unidad	15.00	03	45.00
Honorarios profesionales (Búsqueda, diseño y pruebas de implementación, documentación)	Mensual	2000.00	03	6000.00
	Total			**13,625.00**

Elaboración propia.

3.5. METODOLOGÍA Y PROCEDIMIENTO

3.5.1. Fases de la metodología

La metodología por la cual se desarrolla el presente trabajo es de tipo experimental, de igual manera se describen detalladamente las siguientes etapas para la implementación del modelo y cuentan con todo lo necesario para su desarrollo.

- **Preparación**

Como una etapa pre de la investigación, se indagó en otros casos reales, realidades de infraestructura y seguridad en las comunicaciones de las redes en el departamento de

Puno y alrededores, conociendo casos de otras ciudades y países, analizando casos con soluciones propias cerradas y las de código abierto en muchas instituciones en el mundo.

Se preparó un laboratorio de redes, servidores, máquinas virtuales con Linux, Windows, router, etc.

- **Planeación**

En los procedimientos de toda la investigación se logró segmentar los pasos de los siguientes procesos:

1. Indagación, recopilación y búsqueda de información historia, actual y futura para solucionar problemas de seguridad de las comunicaciones en redes LAN de datos.
2. Iniciar el proceso de preparación de la documentación, proyecto de investigación, otras investigaciones, etc.
3. Selección de arquitectura, infraestructura, sistemas operativos, aplicaciones, versiones, protocolos, seguridad, proxys, firewall, dns, etc.
4. Implementación de laboratorio en un entorno controlado virtualizado con máquinas virtuales con servidores, estaciones, redes, etc.
5. Pruebas de rigor con el envío y recepción de datos entre dos rede LAN usando VPN con cifrado.
6. Documentación de pruebas y resultados.

- **Diseño**

En el diseño de la solución, para obtener los resultados de la investigación, y lograr poner en marcha el modelo de la infraestructura de la Red empresarial entre 02 locales remotos de una empresa organización del departamento de puno".

Se preparó dos redes locales, cada uno protegidas con un firewall perimetral en Linux, un proxy transparente y un servidor VPN con IPSec LAN to LAN.

Detrás del Firewall Perimetral y VPN. Se instaló un equipo Windows 10 Pro, para hacer las pruebas de comunicación de las 02 redes y el paso de paquetes de forma cifrada.

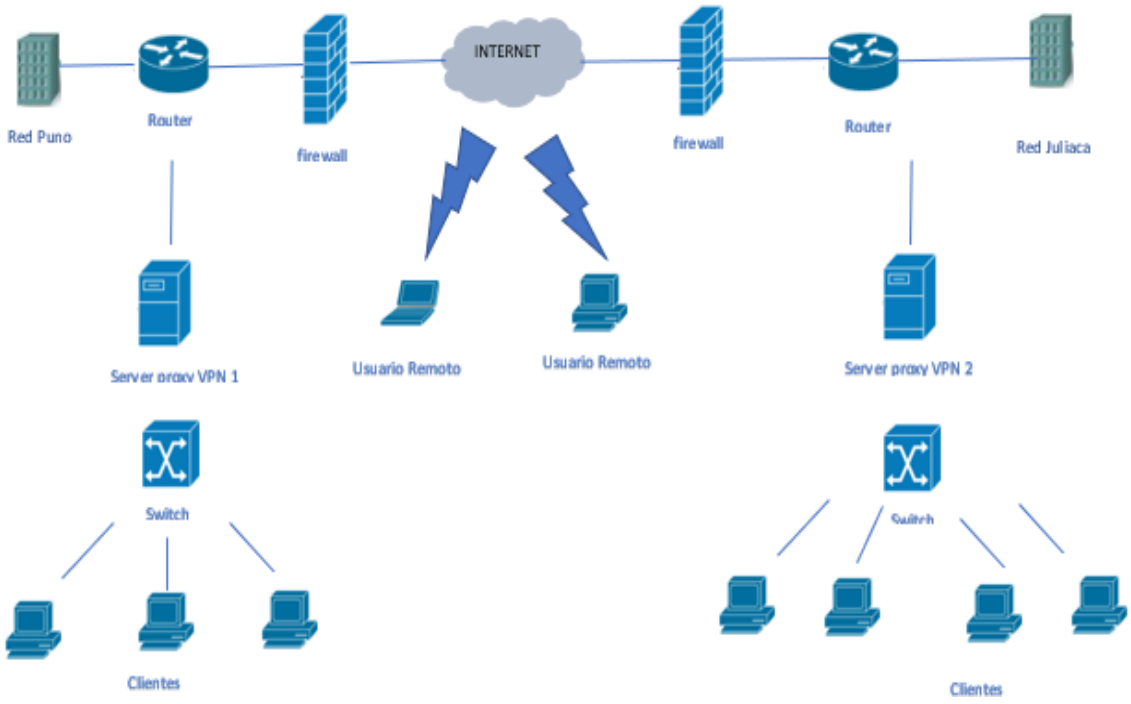


Figura 21: Esquema de la Red VPN.

Elaboración propia.

- **Implementación**

  Para implementar el modelo de infraestructura de red VPN, se plantea lo siguiente:

- proteger la infraestructura de red utilizando el sistema operativo Linux logrando comunicación a través de la creación del túnel.

- Realizar las configuraciones del servidor como de los clientes.

- Si se configura una VPN, se debe prestar atención a la seguridad y encriptación de la información y así evitar el acceso de terceros o intrusos.

- Supervisar los segmentos donde se transmite la información a través de la red, así como recopilar y analizar los paquetes de red.

- **Operación**

En los procesos de operación podemos lograr conexiones por la red compartiendo recursos como carpetas, archivos, impresoras, etc. podemos levantar algún servicio en una de las máquinas para lograr conexión desde la otra, en cada estación de trabajo con sistema operativo Windows y el servidor firewall VPN, estas estaciones tienen conexión transparente lógicamente entre sus redes, así están separadas remotamente.

- **Optimización**

Para optimizar el funcionamiento de la red VPN, se establecen restricciones de seguridad del usuario para que se equilibre la carga cuando se conectan a la red a través de Internet cuando se transmiten paquetes, se pueden habilitar algoritmos de compresión, hashing, etc., y encriptación. Para lograr el objetivo principal de transmisión segura y rápida de paquetes y datos confiables.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. PROCESO DE DESARROLLO DEL PROYECTO

4.1.1. Identificar los requerimientos del cliente

La organización empresarial en el departamento de Puno, tiene 02 locales físicos con redes LAN en cada lado, en las ciudades de Puno y Juliaca, en la sede central se encuentran los sistemas de información, bases de datos, servidores, DNS, proxy, etc. La necesidad empresarial radica en que los equipos del local secundario Juliaca, no pueden acceder a los recursos informáticos y seguridad del local principal.

Se optó por pedir información comercial a soluciones comerciales como IP VPN de Movistar, pero fue descartado por el alto costo. La organización necesita una conexión rápida, segura, ininterrumpida y de bajo costo, usando el Internet para el transporte de los datos entre las 02 redes.

4.1.2. Identificar las características de la red actual

Organización del departamento de Puno:

Local Central ciudad de Puno:

- Red Local de topología estrella de 100Mbps
- Enlace ADSL con fibra óptica Movistar de 100Mbps.
- Cableado estructura CAT6 con path panel, path cord, jacks, cable UTP, conectores, capuchas, rosetas, etc.

- 01 router ADSL de Movistar
- 01 Switch core HP de 16 ptos. 1000Mbps.
- 02 Switch de borda Mikrotik de 24 ptos. 100Mbps
- 50 pc´s
- 10 laptop´s
- 05 servidores

Local Secundario ciudad de Juliaca

- Red Local de topología estrella de 100Mbps
- Enlace ADSL de Claro de 20Mbps.
- Cableado estructura CAT5 con path panel, path Cord, jacks, cable UTP, conectores, capuchas, rosetas, etc.
- 01 Router ADSL Cisco de Claro
- 01 Switch core HP de 16 ptos. 1000Mbps.
- 20 Pc´s,
- 04 laptop´s.

4.1.3. Identificación de los requerimientos funcionales

Se crearán 04 máquinas virtuales utilizando VMware pro 15, 02 de ellos con CentOS 7.8 x86_64 (sistema operativo), los cuales serán:

- firewall perimetral

- firewall, proxy transparente
- squid, servidor DNS
- Bind
- servidor VPN
- IPsec
- Strongswan.

Las otras 02 máquinas virtuales se instalarán Windows 10 pro 64bits (sistema operativo) serán los PC-cliente en cada uno de los locales de la empresa u organización.

Con las siguientes características:

- **Máquina Virtual 01**

Tabla 6: Características SERVER CENTOS VPN 01

Nombre de la Maquina.	**CARACTERISTICAS**
SERVER CENTOS VPN 01 PUNO	- Memoria 2 GB - Procesador 1 - Hard disk 100 GB - Network adapter 1 - Network adapter 2 - Sistema operativo CentOS 7.8.

Elaboración propia.

- **Máquina virtual 02**

Tabla 7: Características SERVER CENTOS VPN 02

Nombre de la Maquina.	CARACTERISTICAS
SERVER CENTOS VPN 02 JULIACA	- Memoria 2 GB - Procesador 1 - Hard disk 100 GB - Network adapter 1 - Network adapter 2 - Sistema operativo CentOS 7.8.

Elaboración propia.

- **Máquina virtual 03**

Tabla 8: Características cliente Red-Puno

Nombre de la Maquina.	CARACTERISTICAS
CLIENTE RED PUNO	- Memoria 2 GB - Procesador 1 - Hard disk 100 GB - Network adapter 1 - Network adapter 2 - Sistema operativo Windows 10 - 64 bits

Elaboración propia.

- **Máquina virtual 04**

Tabla 9: Características cliente Red-Juliaca

Nombre de la Maquina.	CARACTERISTICAS
CLIENTE RED JULIACA	- Memoria 2 GB - Procesador 1 - Hard disk 100 GB - Network adapter 1 - Network adapter 2 - Sistema operativo Windows 10 - 64 bits

Elaboración propia.

4.2. PROCEDIMIENTOS GENERALES

En el proceso de creación del entorno virtual controlado para poner en marcha el modelo de infraestructura de redes VPN de una organización con 02 redes locales en diferentes sucursales de la empresa, se realizaron los siguientes procedimientos.

4.2.1. Instalación del Software de virtualización VMware 15

En esta fase, el software de virtualización se instala en los servidores físicos, las aplicaciones dentro de la máquina virtual acceden a la CPU, la RAM, el disco y sus interfaces, pero no directamente al hardware físico.

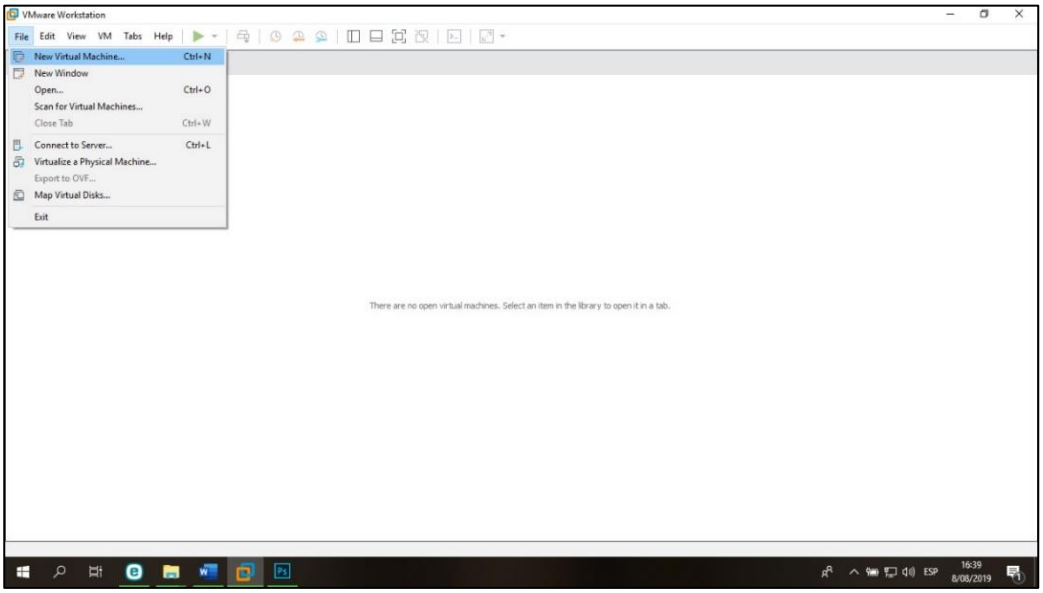
Figura 22: Software de virtualización VMware 15 pro.

Fuente: https://www.vmware.com/latam/products/workstation-pro/workstation-pro-evaluation.html.

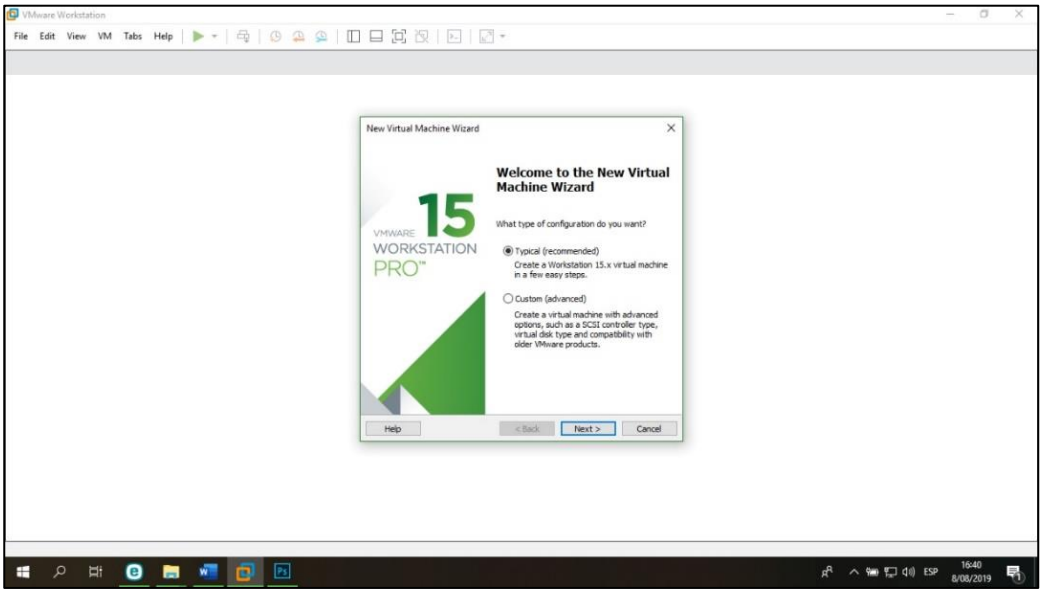
4.2.2. Creación de la Máquina virtual con VMware 15

En esta parte del desarrollo se procede a crear las máquinas virtuales con CentOS 7.8, donde se almacenará el servidor VPN -Puno.

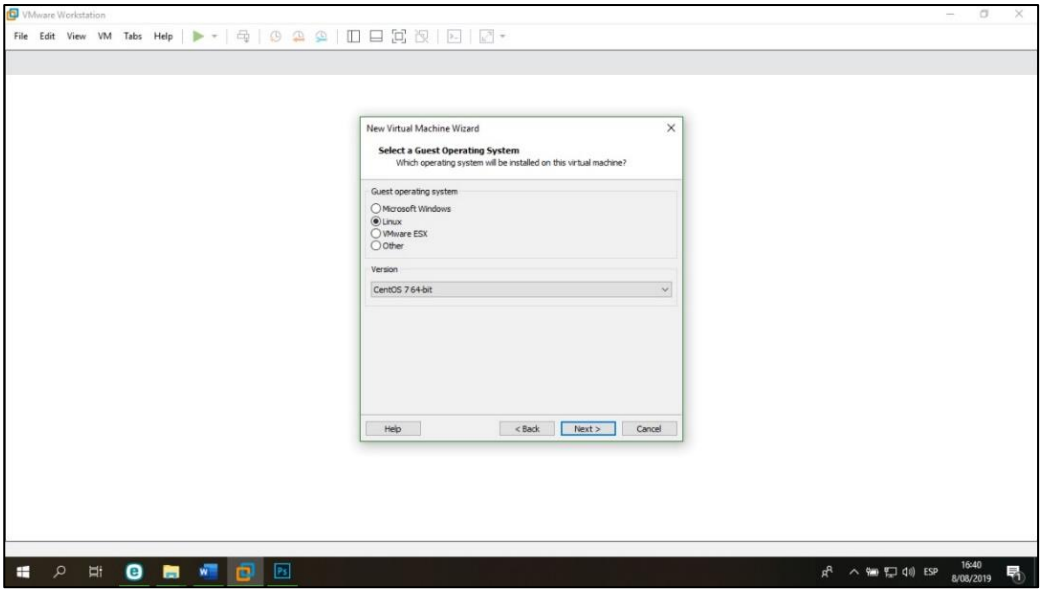
1. Ingresamos al menú: New Virtual Machine



2. Seleccionamos: Typical (recommended)

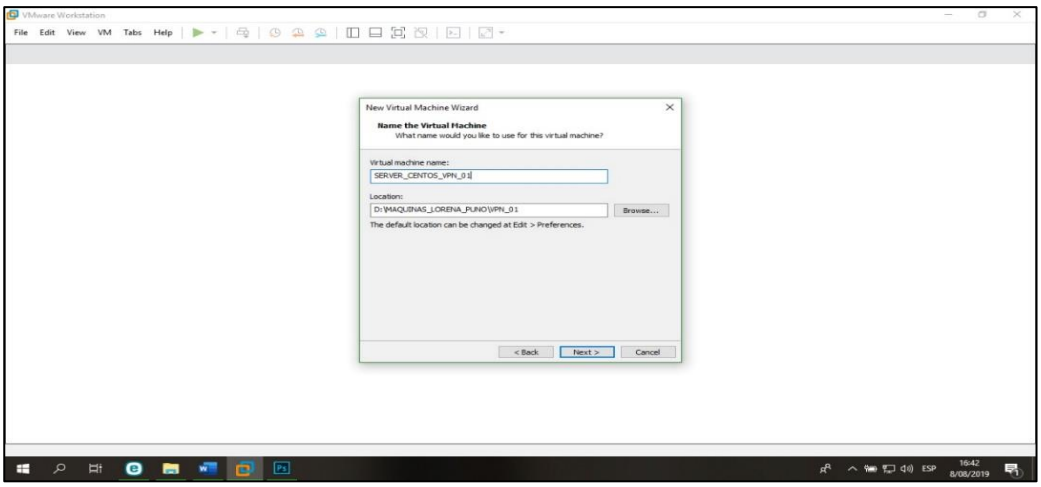


3. **Seleccionamos: Linux (sistema operativo invitado) y su versión (CENTOS 7.8 64bits)**

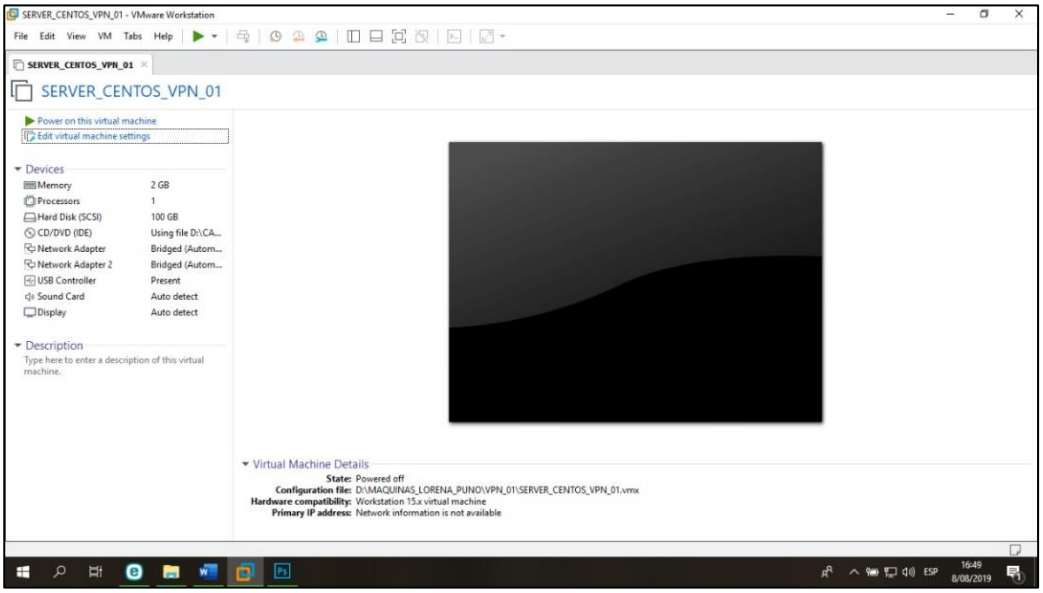


4. **Creación de las carpetas de almacenamiento de las máquinas virtuales de cada servidor.**

5. **Escribimos nombre de máquina virtual y seleccionamos carpeta de almacenamiento.**



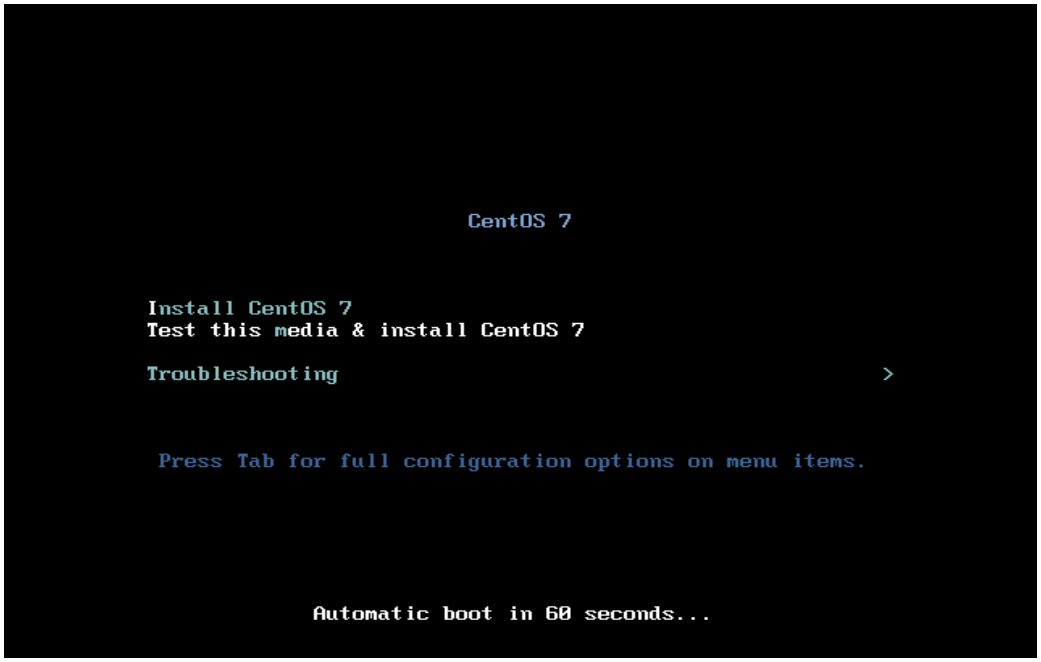
6. Resumen final de máquina Virtual



4.2.3. Inicio del proceso de instalación de CentOS 7.8

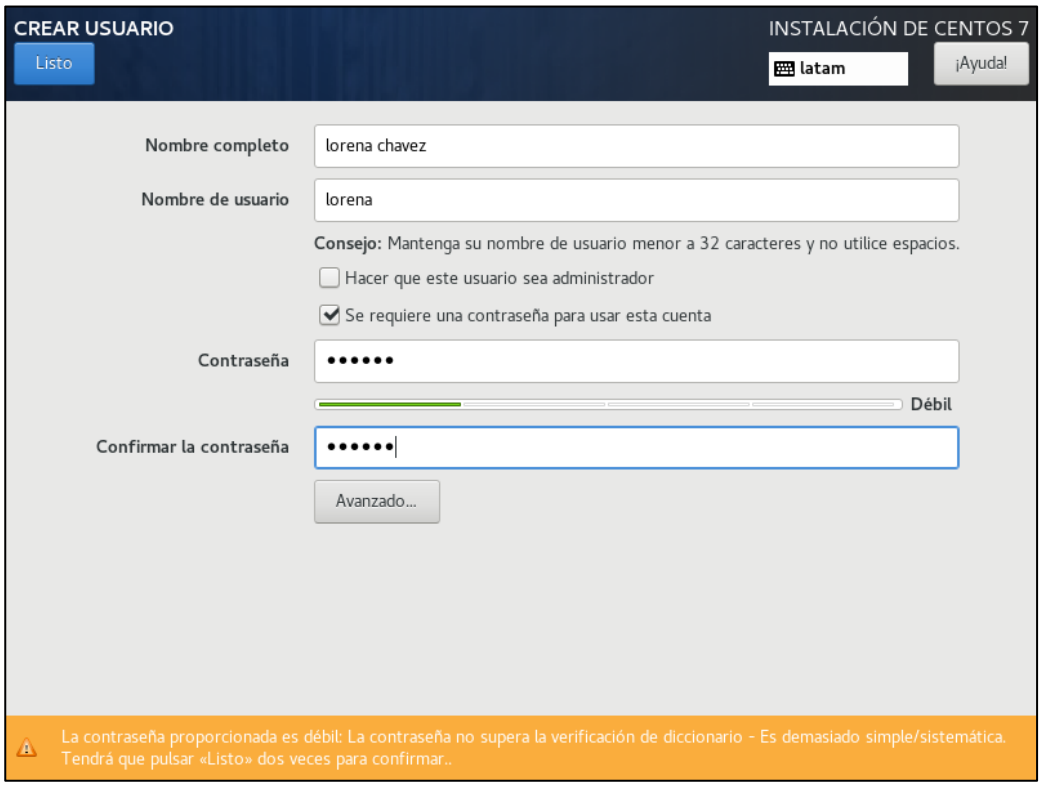
Es esta parte iniciamos la instalación de CentOS 7.8 en la máquina virtual creada con el software de virtualización VMware 15.

1. Ejecutamos power a la máquina virtual – primera pantalla del proceso de instalación CentOS 7.8



2. Resumen de la instalación – empezar instalación

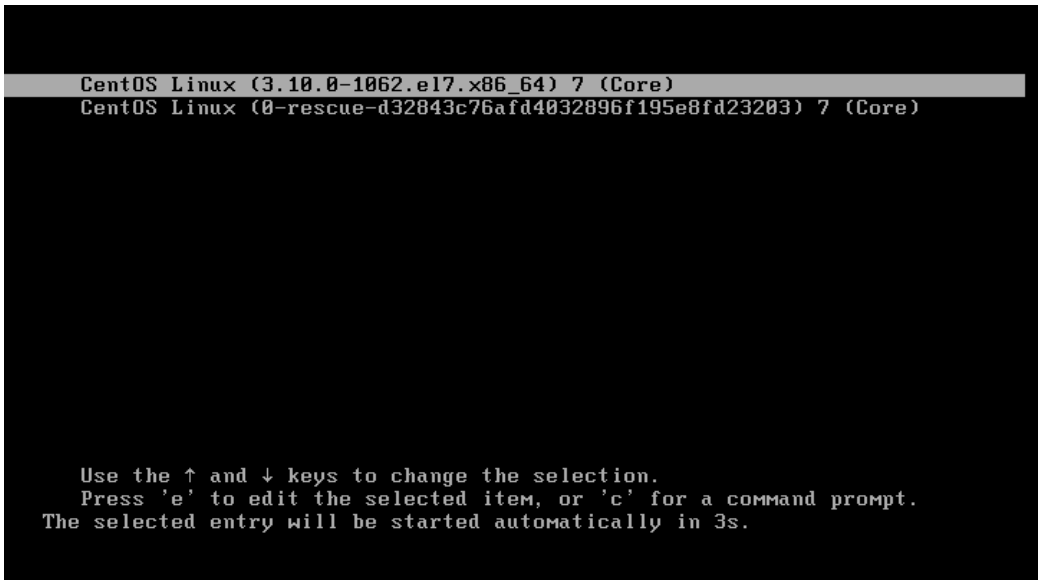
3. Creación del usuario y contraseña "lorena"



4. Término del proceso de instalación y reiniciamos

5. Carga de Linux CentOS 7.8

A continuación, se muestra el gestor de arranque de CentOS 7 del proceso de instalación.

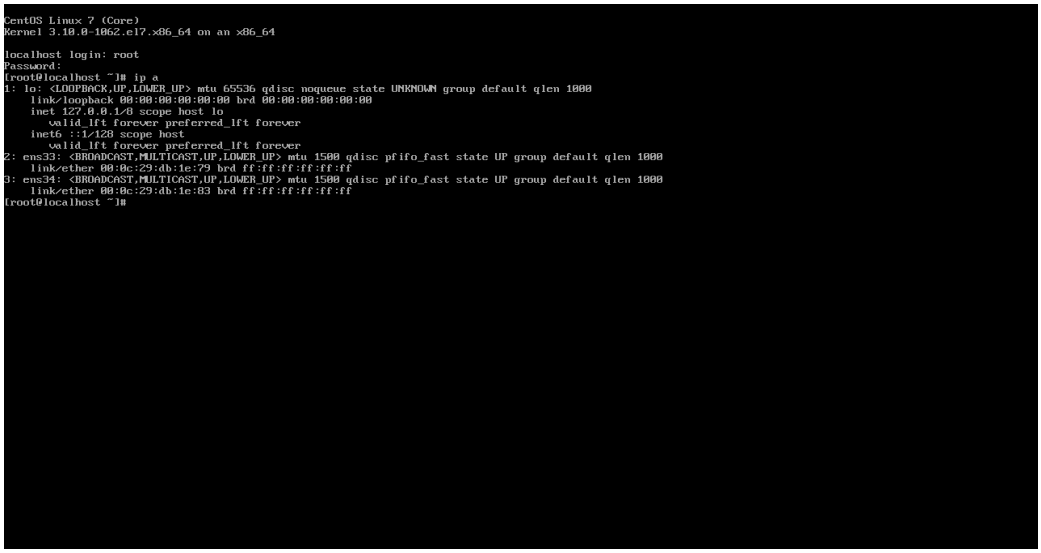


6. Login del usuario “root”

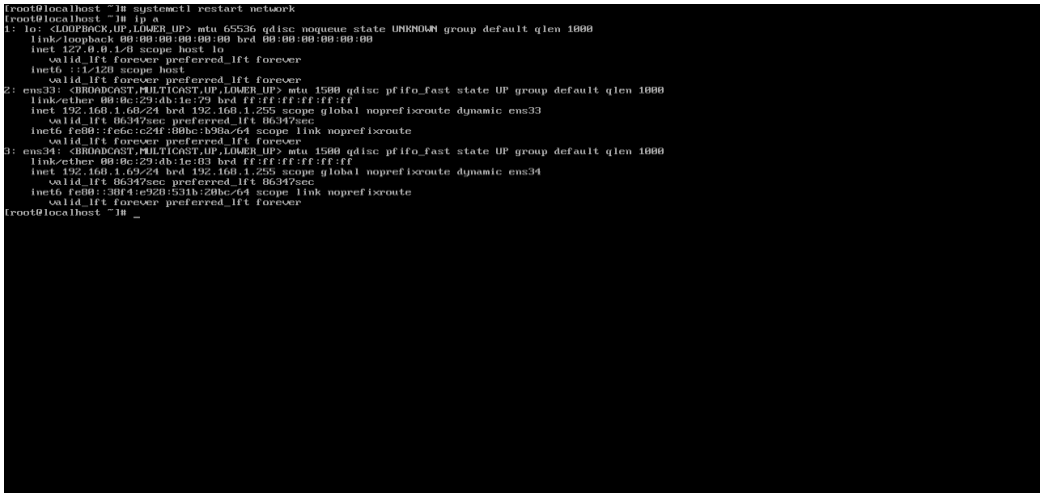
Root es el usuario administrador de nuestro marco de trabajo, el cual tiene amplios privilegios dentro del sistema, en este paso se muestra el inicio de sesión con el usuario root a nuestro servidor.

7. Verificamos la IP del sistema Linux CentOS 7.8

Para verificar las direcciones IP de nuestro servidor utilizamos el comando ip a, a continuación, podemos visualizar las direcciones IP asignadas a nuestro servidor.



8. Visualizamos las IP'S de las tarjetas de red

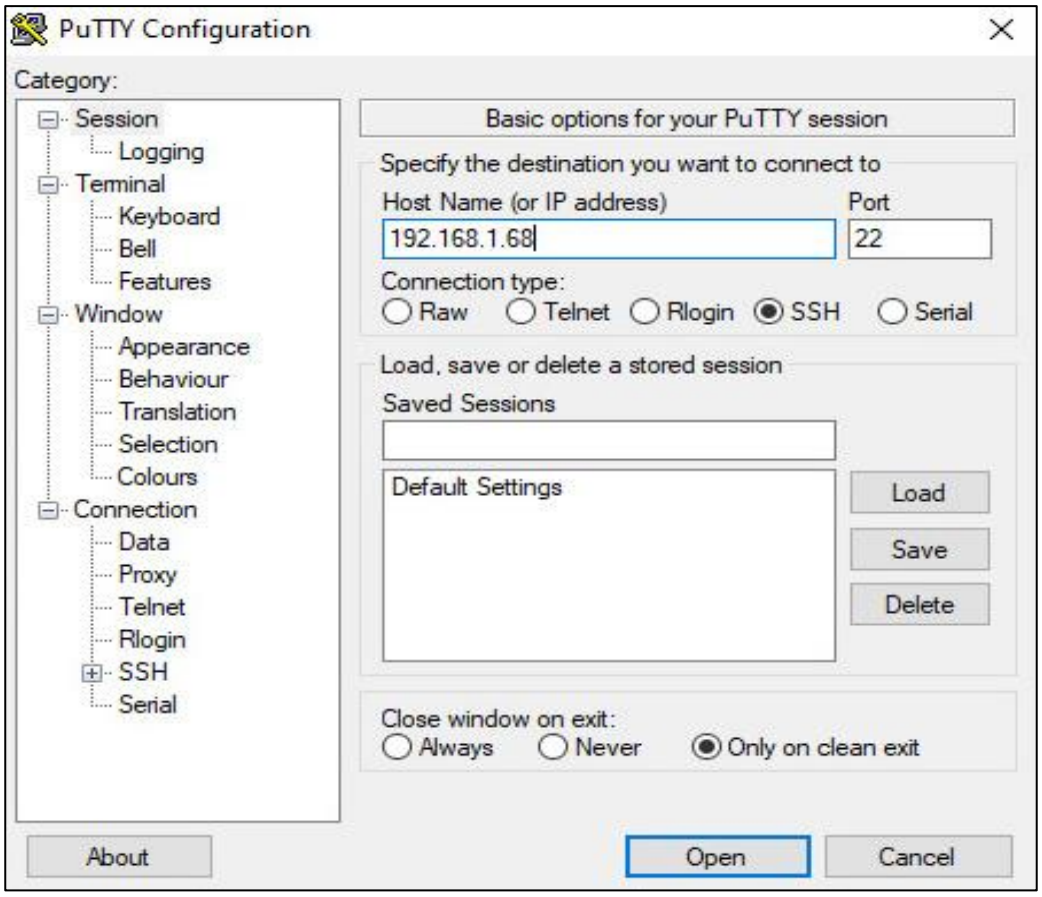


9. Acceso AL CentOS 7.8 por cliente SSH PUTTY, desde Windows.

Una vez configurado y abierto el respectivo puerto, que por defecto es el 22, podemos establecer una conexión remota desde Windows, utilizando PuTTY aplicación gratuita que no requiere instalación.

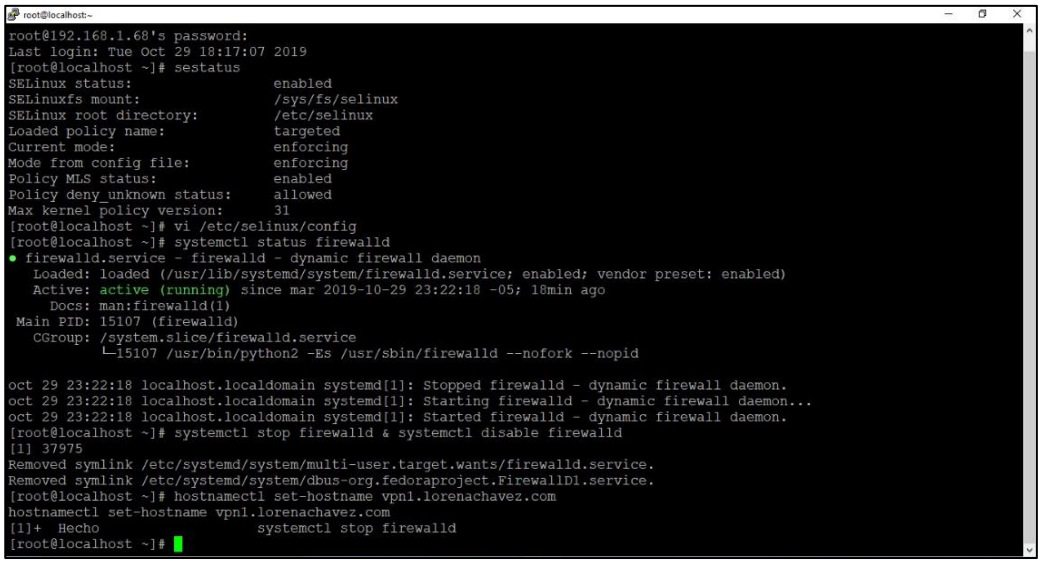
Para acceder introducimos los siguientes datos.

- Dirección IP del equipo con Linux CentOS.
- Nombre de la conexión.
- Puerto de conexión SSH.



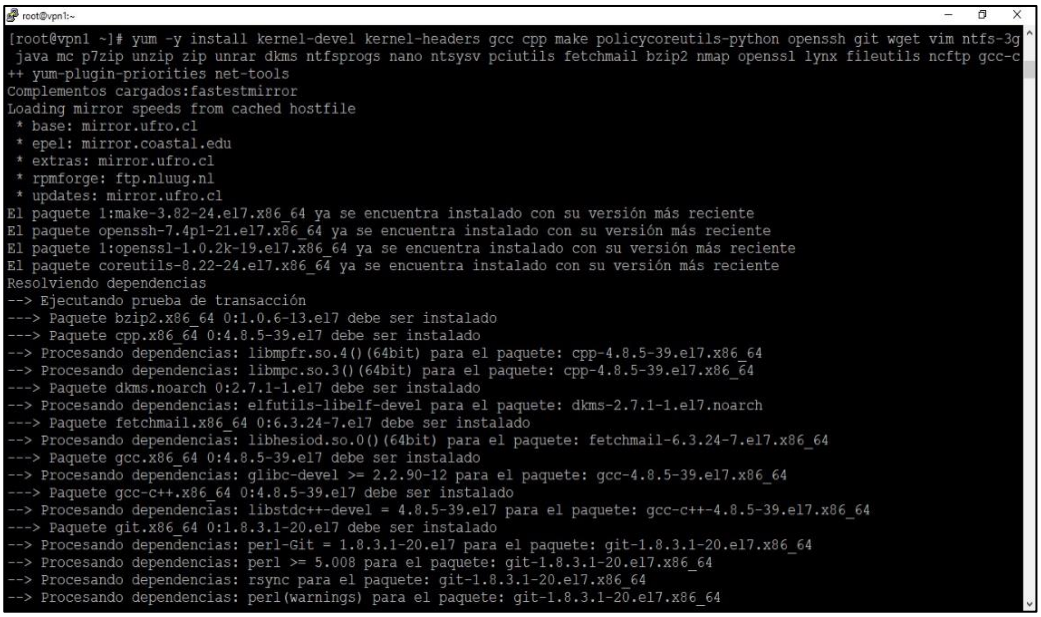
10. Cambio de hostname del server vpn1 (vpn1.lorenachavez.com)

En la siguiente imagen visualización el procedimiento de cambio de hostname, el cual es el nombre que le asignamos a la maquina server vnp1, para poder identificarla de forma sencilla en nuestra red VPN.



11. Instalamos paquetes extras, aplicativos del sistema

Hacemos uso de yum gestor de paquetes de software, desde la línea de comandos para gestionar el software, yum se encarga de instalar las dependencias necesarias de paquetes adicionales de forma automática para su correcto funcionamiento.



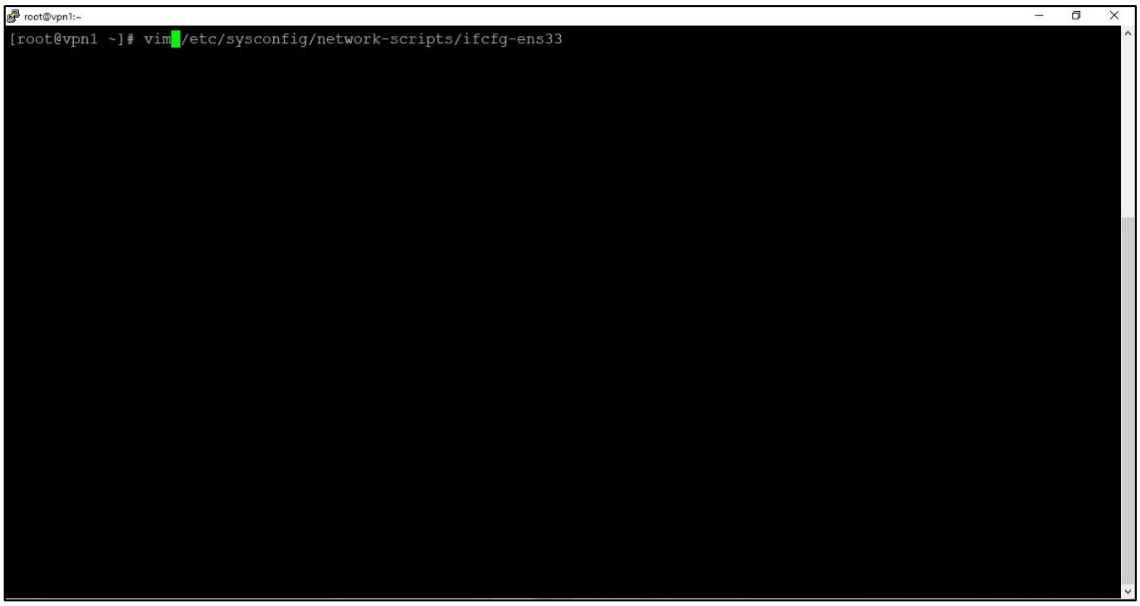
4.2.4. Implementación de redes Linux y Windows, conexiones y configuraciones

1. Agregamos IP estática a la tarjeta de red “ENS33”

CentOS 7 por defecto utiliza IP dinámica lo que quiere decir que cada vez que reinicie, la dirección IP será diferente, por lo que es necesario modificar y establecer una dirección IP estática.

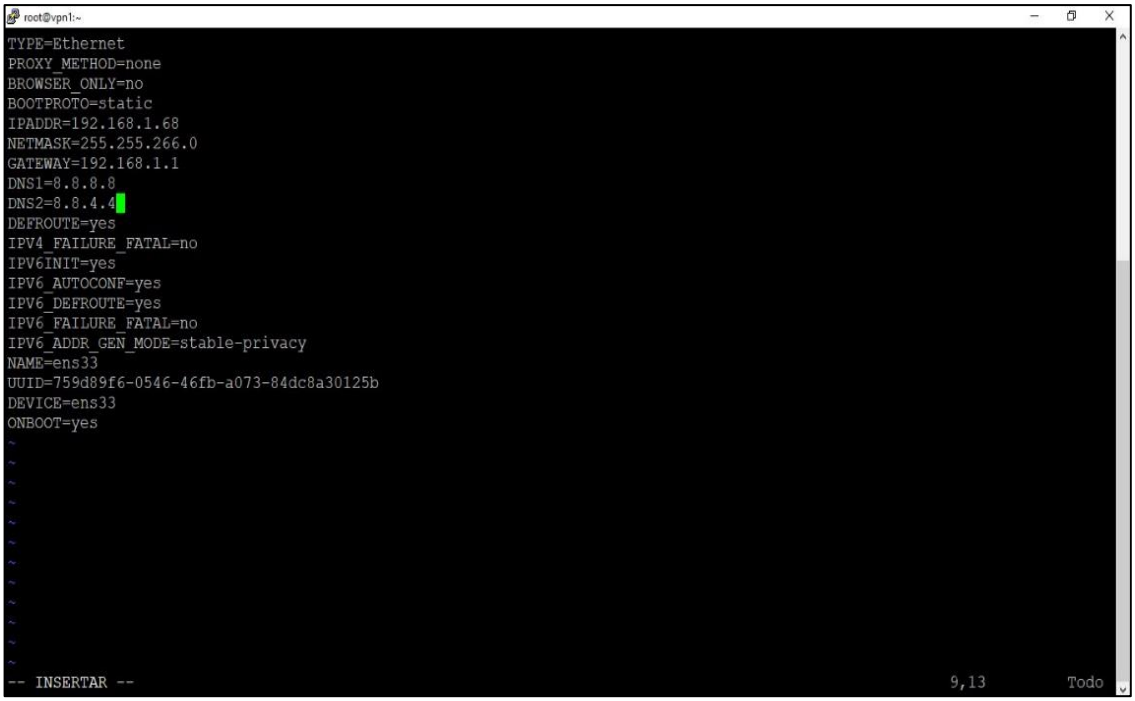
Para realizar el siguiente paso utilizamos el siguiente comando como se muestra en la imagen.

vim /etc/sysconfig/network-scripts/ifcfg-ens33



2. Agregar/cambiar variables IP estática -tarjeta de red “ens33”

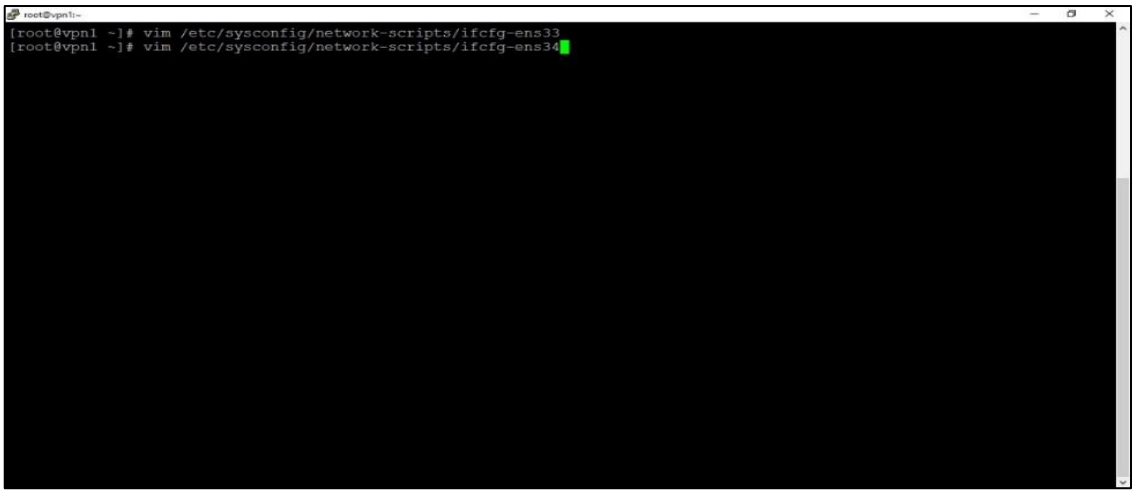
En la siguiente pantalla agregamos y modificamos la dirección IP estática, quedando de la siguiente manera y guardamos los cambios.



3. Agregamos IP estática a la tarjeta de red “ens34”

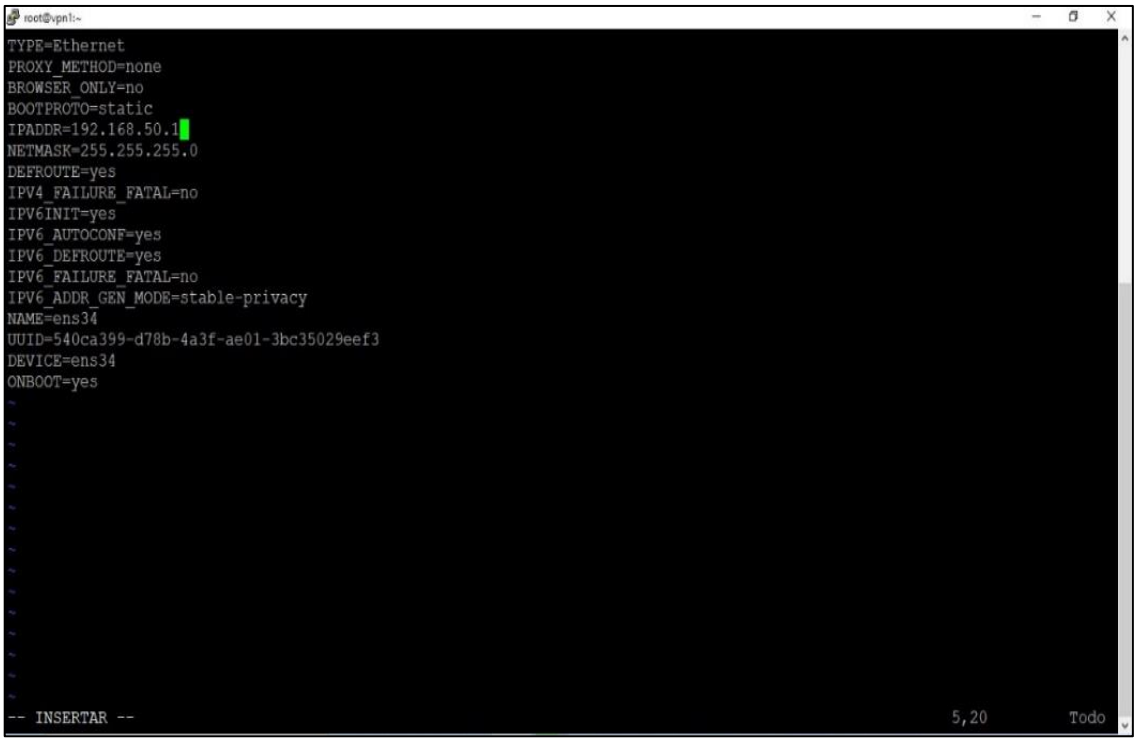
Para modificar la IP en la tarjeta de red ens34 utilizamos el siguiente comando:

vim /etc/sysconfig/network-scripts/ifcfg-ens34



4. Agregar/cambiar variables - IP estática -tarjeta de red “ens34”

Cambiamos y modificamos la dirección IP en la tarjeta de red como se aprecia en la pantalla, y guardamos los cambios.



5. Reiniciamos el servicio de RED "Network"

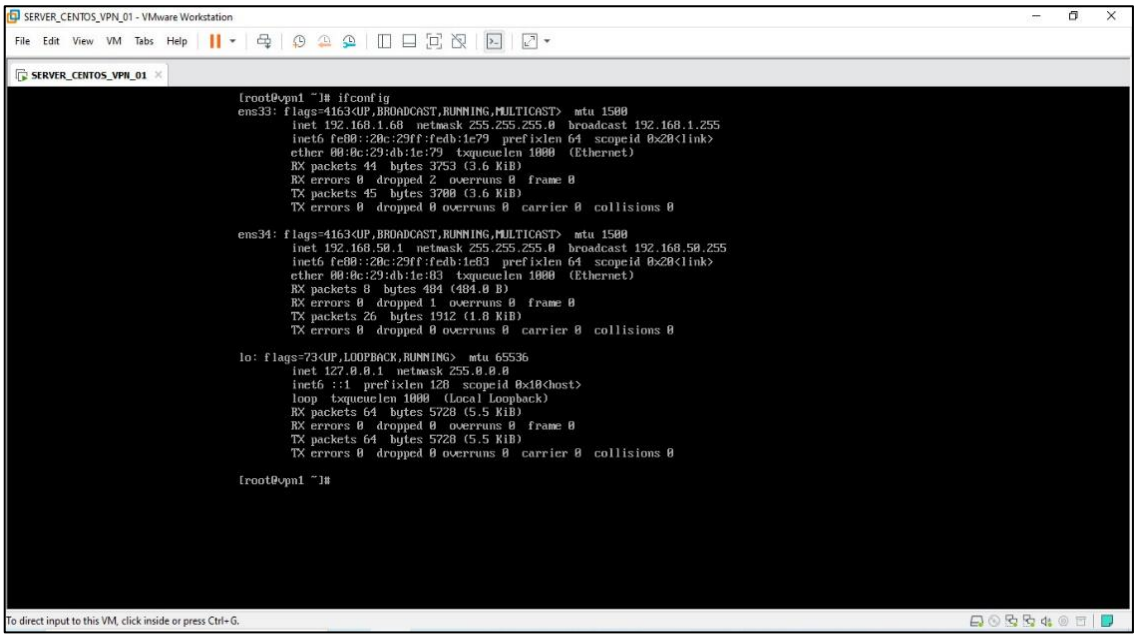
Reiniciamos el sistema utilizando el comando:

systemctl restart network

Para que surjan los cambios realizados. Como se muestra en la siguiente imagen.

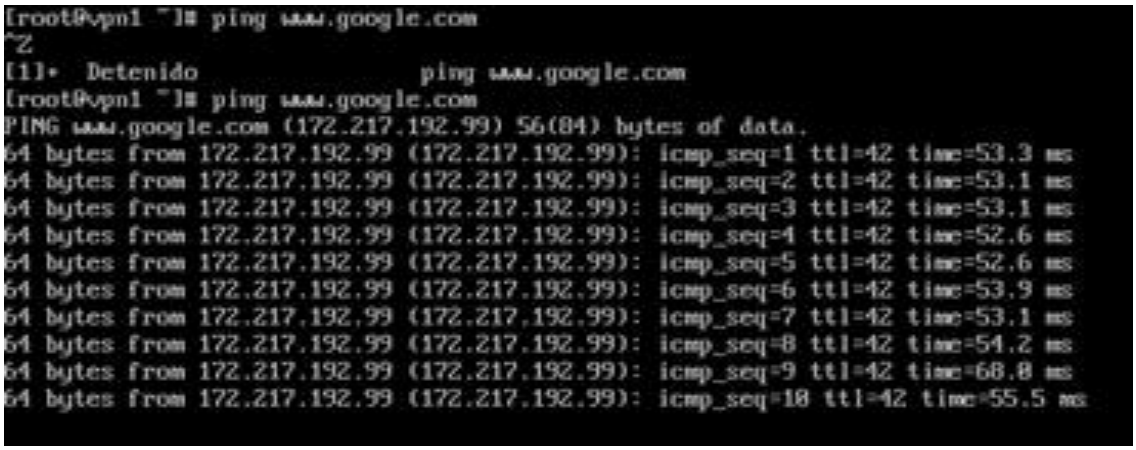
6. Verificamos las IPS del server vpn1 con CENTOS 7.8 (ifconfig)

Para verificar las direcciones IP estáticas de nuestra red utilizamos el comando **ifconfig** donde visualizamos que ya cuenta con IP estática.



7. Probamos conectividad

Probamos conectividad y el acceso a internet utilizando el comando ping.



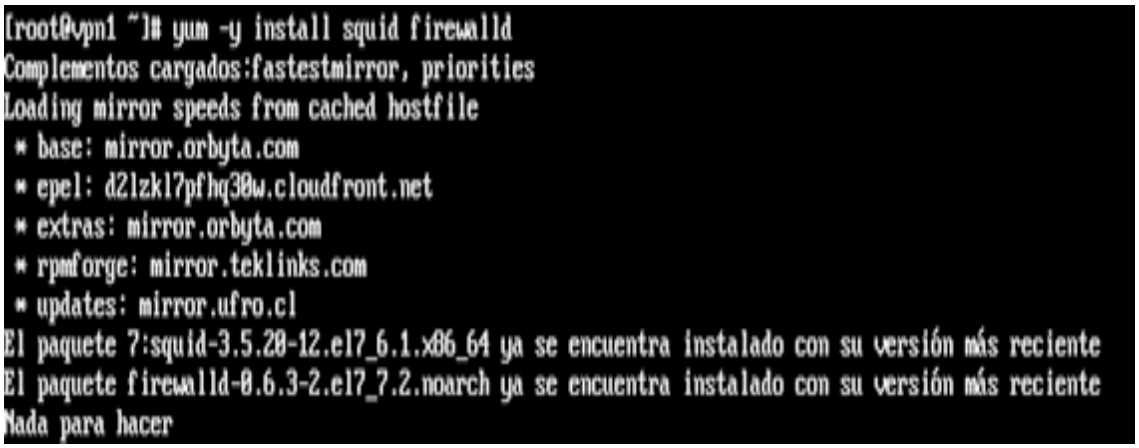
4.2.5. Instalación y configuración de SQUID & FIREWALLD

Instalamos y configuramos Squid para conectarse al servidor web, puede mejorar en gran medida el rendimiento del servidor al almacenar en caché, el firewalld actúa como una interfaz para el sistema de filtrado de paquetes a finde proteger todo el proceso de conexión a la red.

1. Instalamos los paquetes SQUID & FIREWALLD

Para la instalación de paquetes utilizamos el comando:

yum -y install squid firewalld



2. Configuramos SQUID

Para configurar proxy squid utilizamos el siguiente comando, el cual nos permite configurar el directorio donde almacenaremos y gestionaremos el acceso al cliente.

3. Archivo de configuración de SQUID (squid.conf)

Esta es la configuración básica, SQUID usa el archivo en etc/ink/ink.conf y puede trabajar en él usando el editor de texto sin formato ya que hay muchas opciones.

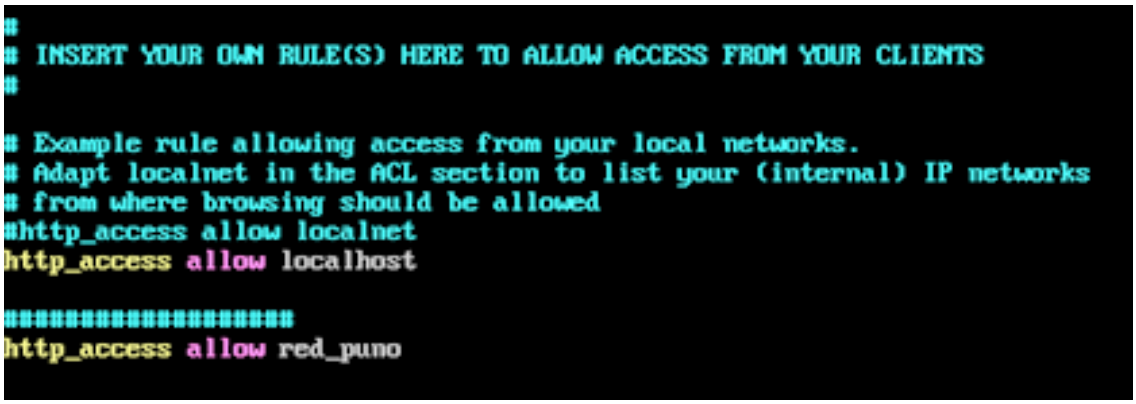
```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
"/etc/squid/squid.conf" 73L, 2315C                            1,1           Comienzo
```

4. Agregar lista de control

Agregamos listas de control de acceso a nuestro servidor, y cada una de ellas establecerá una regla de control de acceso que permitirá o denegará el acceso al squid, permitirá el acceso a la red local, es decir permite el acceso a lista red_puno =192.168.50.0/24

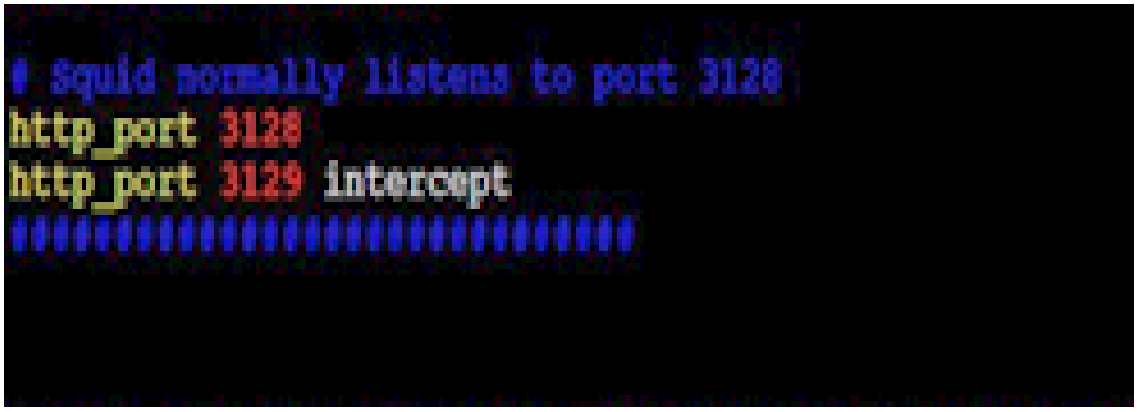
5. Declarando la regla ALLOW para la lista Red_Puno

Es una lista de control de acceso basada en la regla predeterminada, allow es declarada para permitir el acceso a los clientes que tengan el permiso para acceder a la red_puno.



6. Agregando puertos para SQUID: Normal y transparente

Agregamos un proxy normal **http_port 3128,** y un proxy transparente **http_port 3129 intercept,** Para ser más claro y útil, usar un proxy para hacer cumplir las políticas de uso de la red y proporcionar servicios de almacenamiento en caché y seguridad.



7. Agregando otras variables

Se agrega variables a SQUID para que funcione en todo su potencial en base a su cache tal como se muestra en la siguiente imagen.

```
##########################
cache_mem 500 MB
cache_dir aufs /var/spool/squid 10000 16 256
maximum_object_size 100 MB
cache_swap_low 90
cache_swap_high 95
cache_replacement_policy heap LFUDA
ftp_user lorenapuno@hotmail.com
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log
visible_hostname Server_Proxy_Puno_
```

8. Creación de directorios del caché

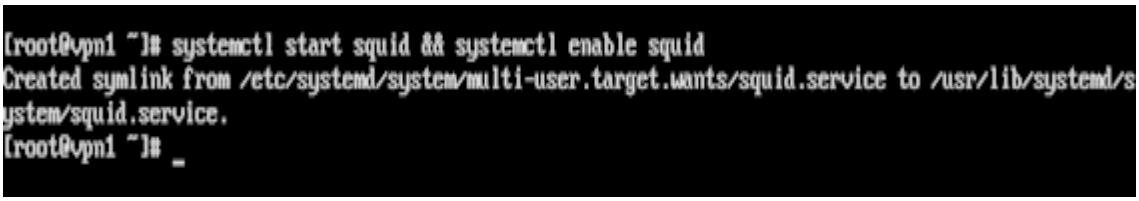
Antes de iniciar SQUID, y solo por primera vez, deberá ejecutar el siguiente comando para crear directorios de caché donde se guardarán las páginas. Utilizando el comando **squid -z.**

```
[root@vpn1 ~]# squid -z
[root@vpn1 ~]# 2020/01/31 00:34:10 kid1| Set Current Directory to /var/spool/squid
2020/01/31 00:34:10 kid1| Creating missing swap directories
2020/01/31 00:34:10 kid1| /var/spool/squid exists
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/00
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/01
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/02
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/03
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/04
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/05
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/06
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/07
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/08
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/09
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/0A
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/0B
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/0C
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/0D
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/0E
2020/01/31 00:34:10 kid1| Making directories in /var/spool/squid/0F

[root@vpn1 ~]# _
```

9. Iniciando el servicio SQUID en CENTOS

Iniciamos el servicio squid desde el arranque con los siguientes comandos

systemctl start squid && systemctl enable squid



10. Verificar SQUID con puertos abiertos

El comando **netstat -nlp | grep squid** es una herramienta para verificar los puertos abiertos en squid para que se ejecute un servicio, caso contrario el servicio no podrá ejecutarse.

4.2.6. Activación del firewall para proxy transparente

En esta fase para arrancar, habilitar y deshabilitar el servicio de firewall utilizamos el siguiente comando **systemctl start firewalld && systemctl enable firewalld.**

1. Asignando tarjetas ENS33, ENS34 para zonas external e internal, reiniciamos firewalld

Asignamos tarjetas de red ens 33 y ens34 para zona external e internal, para aceptar conexiones entrantes selectas y conexiones coexistentes en la misma red caso

contrario el resto son rechazadas, utilizando el comando **firewall -cmd --permanent --zone=external --add-interface=ens33,** luego reiniciamos el firewall.

```
[root@vpn1 ~]# firewall-cmd --permanent --zone=external --add-interface=ens33
success
[root@vpn1 ~]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.68  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:feda:8d09  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:da:8d:09  txqueuelen 1000  (Ethernet)
        RX packets 5243  bytes 5196439 (4.9 MiB)
        RX errors 0  dropped 74  overruns 0  frame 0
        TX packets 2202  bytes 156121 (152.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens34: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.1  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::20c:29ff:feda:8d13  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:da:8d:13  txqueuelen 1000  (Ethernet)
        RX packets 1119  bytes 98795 (96.4 KiB)
        RX errors 0  dropped 74  overruns 0  frame 0
        TX packets 12  bytes 876 (876.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 72  bytes 6560 (6.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72  bytes 6560 (6.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@vpn1 ~]# firewall-cmd --permanent --zone=internal --add-interface=ens34
success
[root@vpn1 ~]# firewall-cmd --reload
success
```

2. Agregando regla directa para proxy transparente

Activamos proxy transparente en firewalld, utilizando el archivo xml, abrimos, editamos y agregamos la regla utilizando la opción donde nos pide el nombre de la tarjeta ens34 el cual pertenece a la red internal de nuestro servidor, el proxy transparente estará conectado a la red internal.

```
[root@vpn1 ~]# vim /etc/firewalld/direct.xml
```

```
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <rule ipv="ipv4" table="nat" chain="PREROUTING" priority="0">-i ens34 -p tcp --dport 80 -j REDIRECT --to-ports 3129</rule>
</direct>
```

3. Agregando servicios y puertos al firewalld para que funcione el proxy transparente en zona internal

El firewalld por defecto cierra todo, con el siguiente comando:

Firewall-cmd –permanent –zone=internal –add-service=squid activamos el servicio dns para que consulten las máquinas de la red, las máquinas de la red salen por el proxy llamado squid, firewalld apertura el servicio squid para las maquinas internas.

```
[root@vpn1 ~]# firewall-cmd --permanent --zone=internal --add-service=squid
success
[root@vpn1 ~]# firewall-cmd --permanent --zone=internal --add-service=dns
success
[root@vpn1 ~]# firewall-cmd --permanent --zone=internal --add-port=3128/tcp
success
[root@vpn1 ~]# firewall-cmd --permanent --zone=internal --add-port=3129/tcp
success
[root@vpn1 ~]# firewall-cmd --reload
success
[root@vpn1 ~]#
```

4. Visualización de los LOGS del proxy

Se visualiza los reportes de los logs del proxy, para comprobar que las PC's que están atrás del servidor ya están navegando, lo cual indica que hay comunicación entre las máquinas.

```
1591549637.347     94 192.168.50.2 TCP_MISS/200 954 GET http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgU
rDgMCGgUABBTfqhLjKLEJQZPin0XCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72MkK8MCEAt%2BEJA8OEkP%2Bi9nmoehp7k%3D
- HIER_DIRECT/192.16.58.8 application/ocsp-response
1591549637.613     24 192.168.50.2 TCP_MISS/200 954 GET http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgU
rDgMCGgUABBSLIycRsoI3J6zPns4K1aQgAgaqHgQUZ50PIAkMzIo65YJGcmL88cyQ5UACEAnFLCUbza7DXF7cLpV1h2c%3D - HI
ER_DIRECT/192.16.58.8 application/ocsp-response
1591549638.742    136 192.168.50.2 TCP_MISS/200 456 GET http://ceement.rssx.hp.com/CeementWA/index.j
sp - HIER_DIRECT/15.72.228.57 text/plain
1591549644.967   3682 192.168.50.2 TCP_TUNNEL/200 3265 CONNECT apis.google.com:443 - HIER_DIRECT/172
.217.192.100 -
1591549644.968   3683 192.168.50.2 TCP_TUNNEL/200 3295 CONNECT www.gstatic.com:443 - HIER_DIRECT/64.
233.190.94 -
1591549644.968   2113 192.168.50.2 TCP_TUNNEL/200 4145 CONNECT content-autofill.googleapis.com:443 -
 HIER_DIRECT/172.217.192.95 -
1591549644.969    786 192.168.50.2 TCP_TUNNEL/200 5266 CONNECT adservice.google.com:443 - HIER_DIREC
T/64.233.190.156 -
1591549644.980   2288 192.168.50.2 TCP_TUNNEL/200 5197 CONNECT id.google.com:443 - HIER_DIRECT/64.23
3.190.94 -
1591549644.980   3701 192.168.50.2 TCP_TUNNEL/200 67422 CONNECT www.google.com:443 - HIER_DIRECT/64.
233.190.103 -
1591549651.557  12423 192.168.50.2 TCP_MISS/503 713 POST http://ceement.rssx.hp.com/CeementWA/ceemen
t_request.do - HIER_DIRECT/15.72.228.57 text/html


1591549695.855   6456 192.168.50.2 TCP_TUNNEL/200 4759 CONNECT accounts.google.com:443 - HIER_DIRECT
/172.217.192.84 -
1591549737.485 100718 192.168.50.2 TCP_TUNNEL/200 55736 CONNECT fe2cr.update.microsoft.com:443 - HIE
R_DIRECT/13.83.151.160 -
1591549797.274  66388 192.168.50.2 TCP_TUNNEL/200 6897 CONNECT self.events.data.microsoft.com:443 -
HIER_DIRECT/52.114.132.34 -
1591549871.352   4891 192.168.50.2 TCP_TUNNEL/200 5899 CONNECT fe3cr.delivery.mp.microsoft.com:443 -
 HIER_DIRECT/64.4.54.18 -
1591549933.313   1364 192.168.50.2 TCP_MISS/304 470 GET http://ctldl.windowsupdate.com/msdownload/up
date/v3/static/trustedr/en/authrootstl.cab? - HIER_DIRECT/190.216.160.254 -
1591549945.611   1147 192.168.50.2 TCP_TUNNEL/200 5574 CONNECT google.com:443 - HIER_DIRECT/172.217.
192.102 -
```

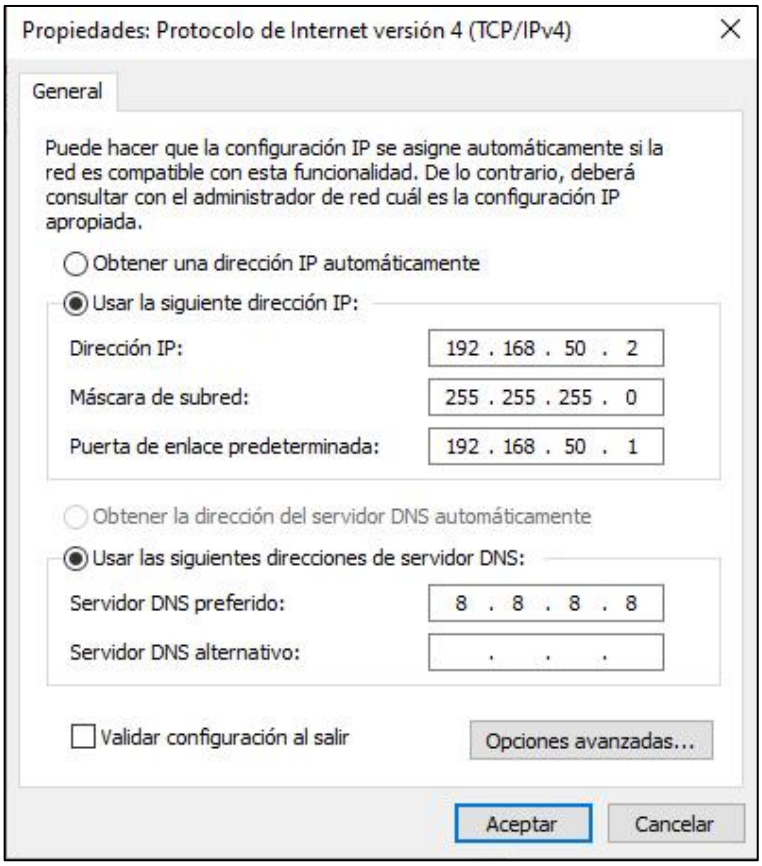
5. Visualización de los servicios y puertos abiertos en la zona internal desde el firewalld

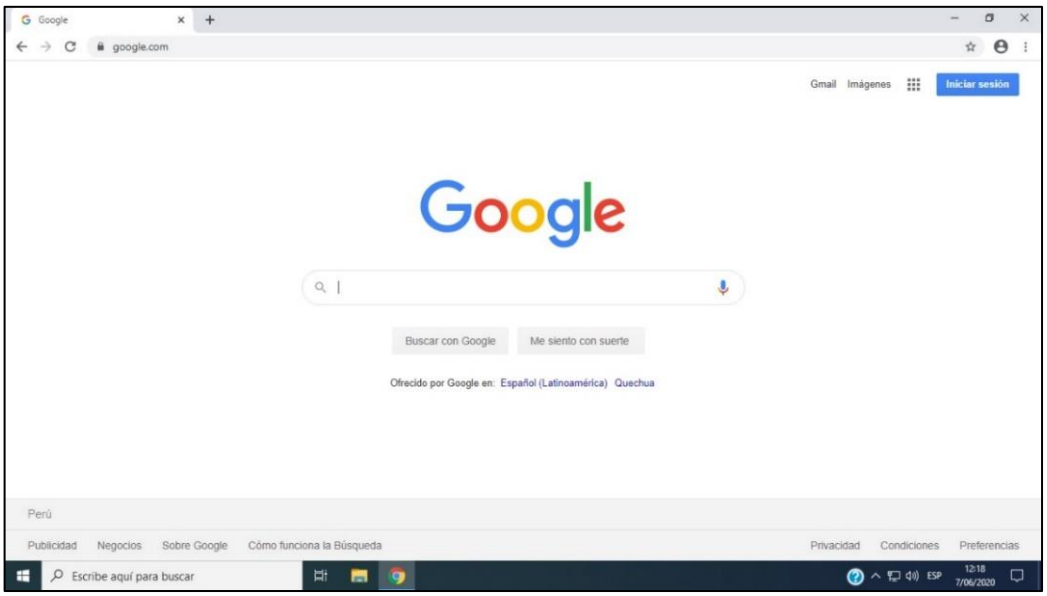
Es el comando del sistema firewalld para revisar que configuración tiene la zona internal y external, donde se visualiza que servicios y que puertos están abiertos.

```
[root@vpn1 ~]# firewall-cmd --zone=internal --list-all
internal (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens34
  sources:
  services: dhcpv6-client dns mdns samba-client squid ssh
  ports: 3128/tcp 3129/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

6. Probando desde un cliente WIN10 el funcionamiento del proxy transparente con el segmento 192.168.50.0/24

Probamos un cliente win10 donde se está probando que existe conexión a internet y que funciona el nivel del proxy.



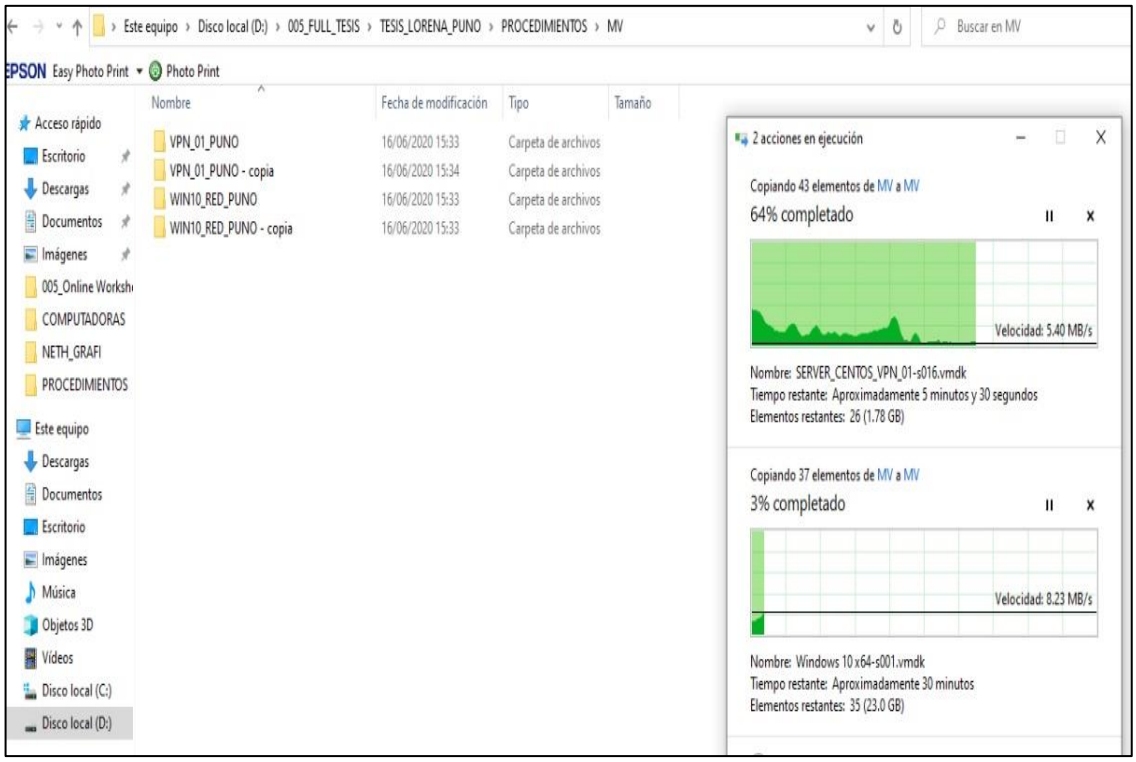


4.27. CREACIÓN DE LA MÁQUINA VIRTUAL PARA LA RED JULIACA

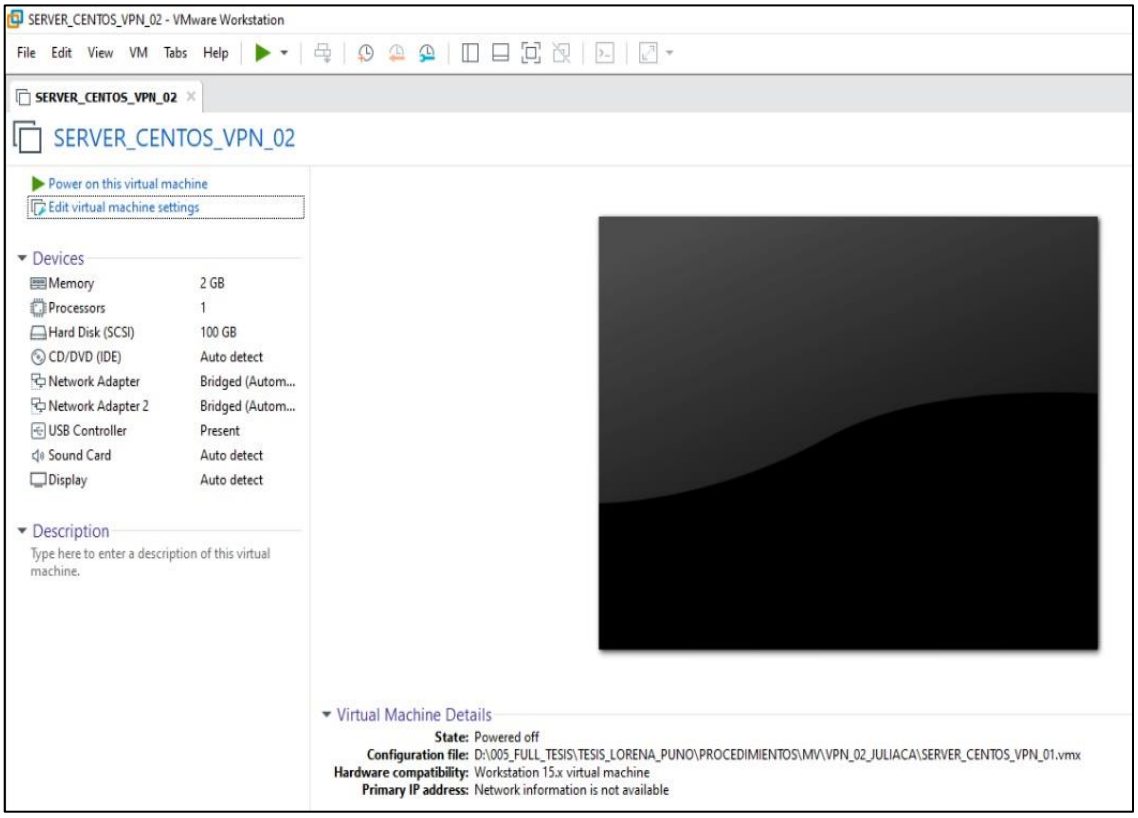
Para iniciar con instalación, configuración y puesta en marcha de la red Juliaca se repiten todos los procedimientos desde el punto 4.2.2 al 4.2.5.

Podemos optar por copiar los directorios de las 02 máquinas virtuales y configurarlas con los datos necesarios para la red Juliaca.

1. **Copiamos las carpetas de las máquinas virtuales: SERVER CENTOS CON VPN1_PUNO Y EL CLIENTE WIN10_RED_PUNO, HACIA VPN_02_JULIACA Y WIN10_RED_JULIACA**

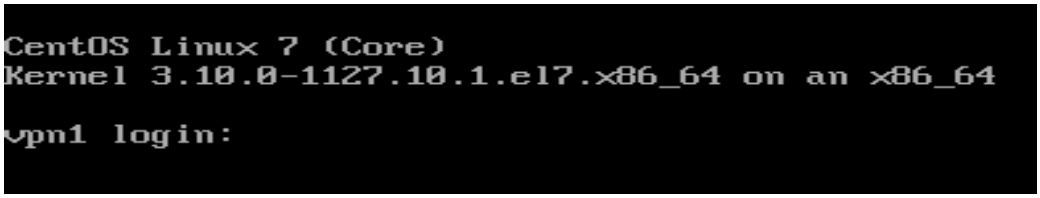


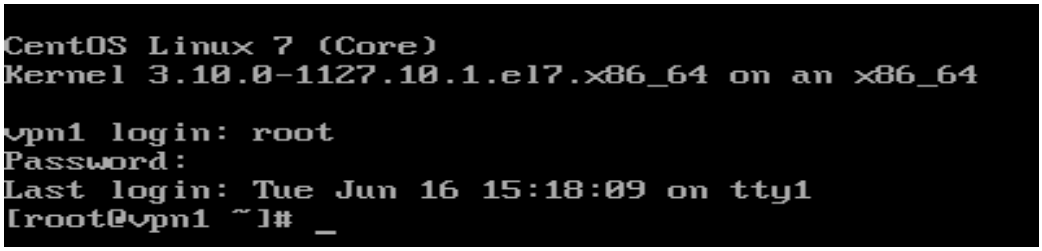
2. Cambiando el nombre de la máquina virtual “SERVER_CENTOS_VPN_02



3. Loguin en VM CON VPN2_JULIACA EN CENTOS 7.8

Logeamos al servidor 2, cambiamos el nombre y la IP.





4. Modificación del HOSTNAME DE VPN1 A VPN2

Modificamos el hostanme de nuestra red VPN2.

```
[root@vpn1 ~]# vim /etc/hostname _
```

```
vpn1.lorenachavez.com
```

```
vpn2.lorenachavez.com
```

5. Modificación de las IP de las tarjetas ENS33

Modificamos la IP a la primera tarjeta de la red external.

```
[root@vpn1 ~]# vim /etc/sysconfig/network-scripts/ifcfg-ens33_
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR=192.168.1.69_
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=8.8.8.8
DNS2=8.8.4.4
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens33
UUID=759d89f6-0546-46fb-a073-84dc8a30125b
DEVICE=ens33
ONBOOT=yes
ZONE=external
```

6. Modificación de las IP de las tarjetas ENS33

Modificamos la IP de la segunda tarjeta de red internal.

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR=192.168.80.1
NETMASK=255.255.255.0
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens34
UUID=540ca399-d78b-4a3f-ae01-3bc35029eef3
DEVICE=ens34
ONBOOT=yes
ZONE=internal
~
```

7. VERFICAMOS LAS NUEVAS IPS

Corroboramos que las nuevas IPs ya se están levantando.

```
[root@vpn2 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:d9:55:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.69/24 brd 192.168.1.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed9:551e/64 scope link
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:d9:55:28 brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.1/24 brd 192.168.80.255 scope global ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed9:5528/64 scope link
       valid_lft forever preferred_lft forever
[root@vpn2 ~]# _
```

8. Verificamos si SQUID está funcionando en CENTOS

Comprobamos que el squid está funcionando en el servidor de nuestra red de Juliaca, con el siguiente comando comprobamos que el squid está levantado y se está ejecutando, y verifica que el puerto squid está abierto.

```
[root@vpn2 ~]# netstat -nlp | grep squid
tcp6       0      0 :::3128                 :::*                    LISTEN      1187/(squid-1)
tcp6       0      0 :::3129                 :::*                    LISTEN      1187/(squid-1)
udp        0      0 0.0.0.0:54272           0.0.0.0:*                           1187/(squid-1)
udp6       0      0 :::48655                :::*                                1187/(squid-1)
[root@vpn2 ~]#
```

9. Verificamos si FIREWALLD está funcionando

Comprobamos que el firewalld está funcionando y ejecutándose.

```
[root@vpn2 ~]# systemctl firewalld status
Unknown operation 'firewalld'.
[root@vpn2 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since mar 2020-06-16 16:23:03 -05; 1min 35s ago
     Docs: man:firewalld(1)
 Main PID: 700 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─700 /usr/bin/python2 -Es /usr/sbin/firewalld --nofork --nopid

jun 16 16:23:01 vpn2.lorenachavez.com systemd[1]: Starting firewalld - dynamic firewall daemon...
jun 16 16:23:03 vpn2.lorenachavez.com systemd[1]: Started firewalld - dynamic firewall daemon.
jun 16 16:23:03 vpn2.lorenachavez.com firewalld[700]: WARNING: AllowZoneDrifting is enabled. Th...w.
Hint: Some lines were ellipsized, use -l to show in full.
[root@vpn2 ~]# _
```

10. Cambiamos la lista de control en SQUID del server VPN_02

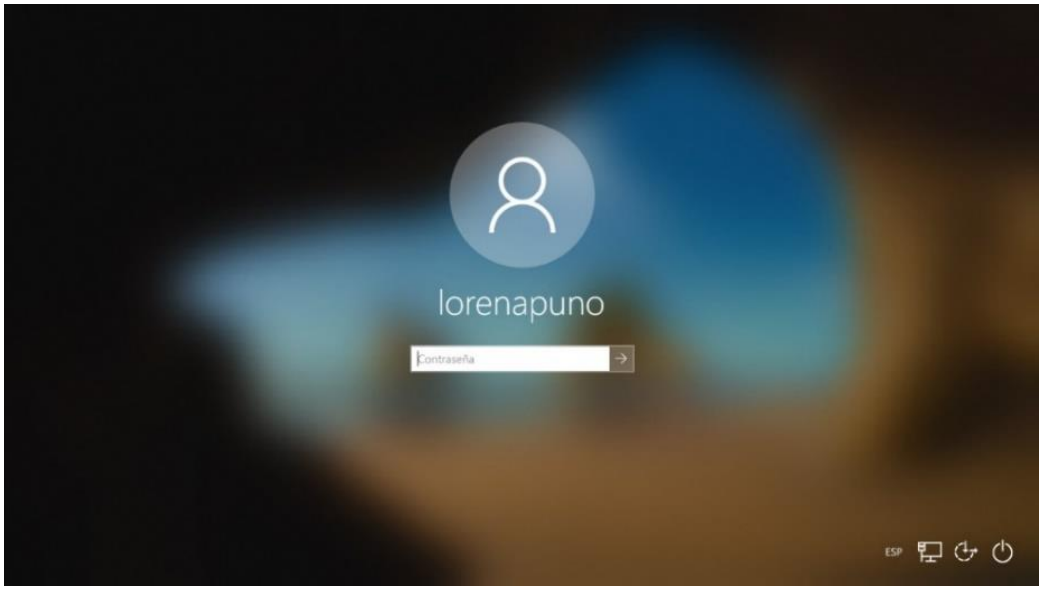
Ingresamos al archivo de configuración del squid que es el proxy, el cual va atender a la red 80, red de las PCs que están detrás del servidor de Juliaca.

```
acl red_puno src 192.168.80.0/24
############################
```

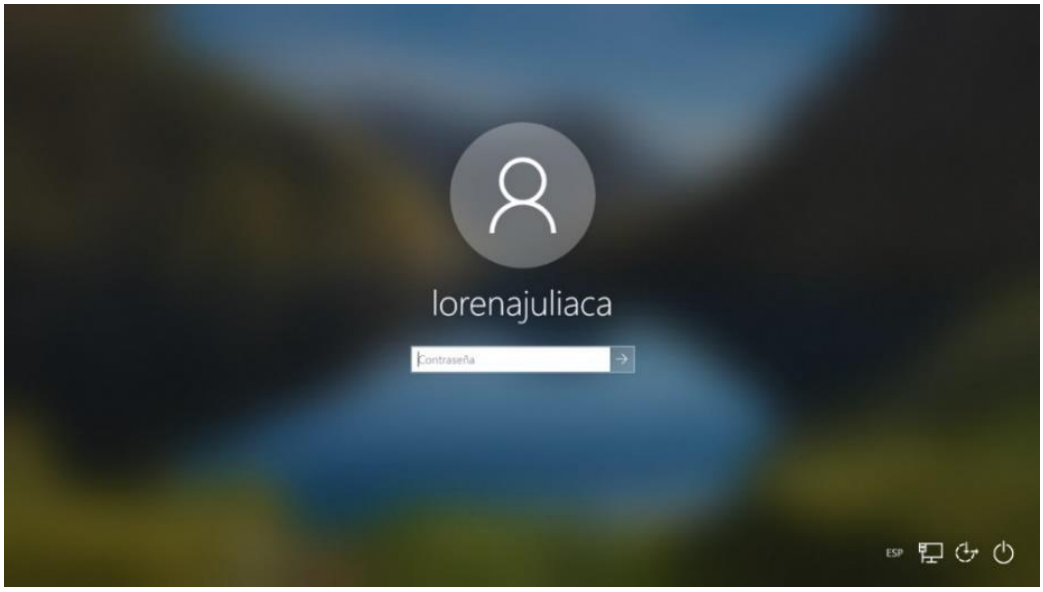
4.2.7. Configuración del cliente win 10 para la conexión de las redes

En los siguientes ítems, Ingresamos a la PC Windows que está detrás del servidor de Juliaca configuramos sus valores, sus tarjetas de red y poner la IP que corresponde al segmento 80.

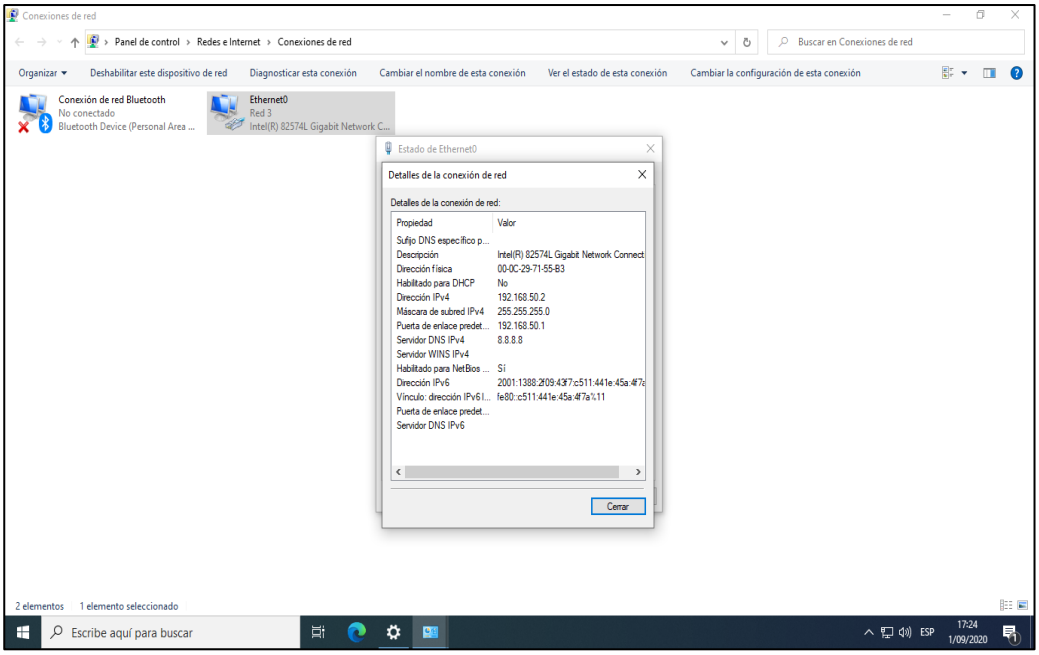
1. **Configuración de cliente WIN10, para probar la conexión de la Red Puno**



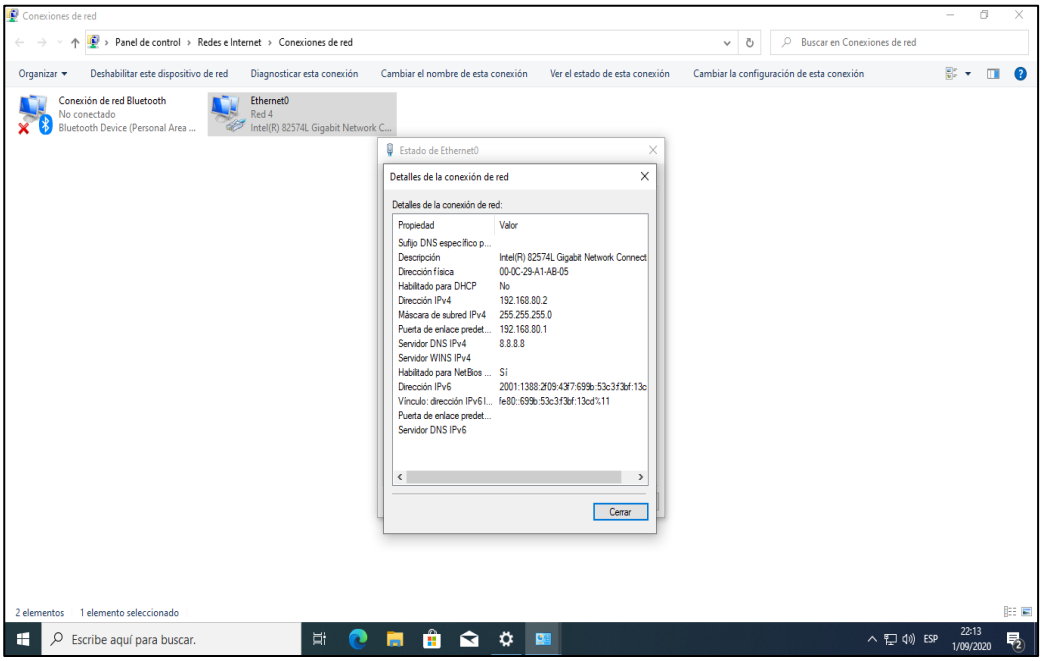
2. **Configuración de cliente WIN10, para probar la conexión de la Red Juliaca**



3. Configuración de interface de red de cliente WIN10 de Red Puno (IP / MÁSCARA DE SUBRED / PUERTA DE ENLACE/ DNS)



4. Configuración de interface de red de cliente WIN10 de Red Juliaca (IP / MÁSCARA DE SUBRED / PUERTA DE ENLACE/ DNS)



4.2.8. Resultados de las Pruebas de conexión

1. Prueba de conexión WEB por el PROXY en la Red Puno

Comprobamos que tenemos acceso a internet de la red Puno.

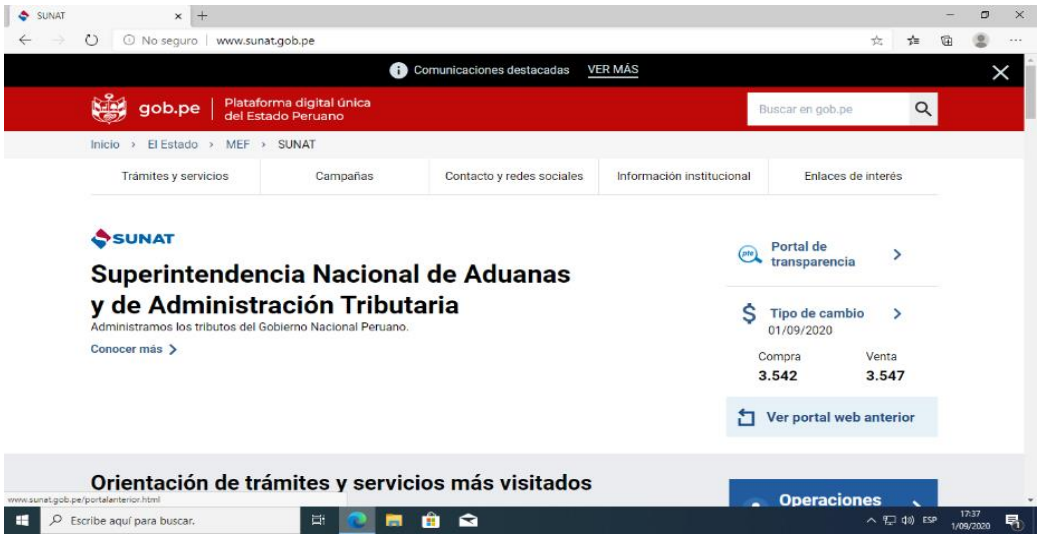
2. Prueba de LOGS en SQUID en el server Red Puno

Se realiza esta prueba para verificar los logs donde se muestran los registros de accesos, lo que permite ver si los servidores tienen acceso a internet y las maquinas que están detrás del servidor están navegando.

```
[root@vpn1 ~]# tail -f /var/log/squid/access.log
1598999922.345    158 192.168.50.2 TCP_MISS/200 10141 GET http://www.megagitel.com/sites/default/fil
es/banner/microtik.png - ORIGINAL_DST/162.214.101.17 image/png
1598999922.346    184 192.168.50.2 TCP_MISS/200 11729 GET http://www.megagitel.com/sites/default/fil
es/banner/dlink.png - ORIGINAL_DST/162.214.101.17 image/png
1598999922.585    840 192.168.50.2 TCP_MISS/200 315677 GET http://www.megagitel.com/sites/default/fi
les/styles/medium/public/services/servidores.png? - ORIGINAL_DST/162.214.101.17 image/png
1598999922.742    154 192.168.50.2 TCP_MISS/200 11356 GET http://www.megagitel.com/sites/default/fil
es/banner/ruckuss.png - ORIGINAL_DST/162.214.101.17 image/png
1598999922.799    180 192.168.50.2 TCP_MISS/200 24433 GET http://www.megagitel.com/sites/default/fil
es/styles/small/public/2020-03/reu-cajero-automatico-atm-640x400.jpg? - ORIGINAL_DST/162.214.101.17
image/jpeg
1598999922.808    210 192.168.50.2 TCP_MISS/200 9184 GET http://www.megagitel.com/sites/default/file
s/banner/ubique.png - ORIGINAL_DST/162.214.101.17 image/png
1598999922.872    210 192.168.50.2 TCP_MISS/200 42278 GET http://www.megagitel.com/sites/default/fil
es/gbb-uploads/bg-2.jpg - ORIGINAL_DST/162.214.101.17 image/jpeg
1598999924.469    171 192.168.50.2 TCP_MISS/200 2992 GET http://www.megagitel.com/modules/gavias_sli
derlayer/vendor/revolution/assets/loader.gif - ORIGINAL_DST/162.214.101.17 image/gif
1598999925.144    513 192.168.50.2 TCP_MISS/200 74957 GET http://www.megagitel.com/themes/gavias_eli
x/css/font-awesome/webfonts/fa-brands-400.woff2 - ORIGINAL_DST/162.214.101.17 font/woff2
1598999925.264    172 192.168.50.2 TCP_MISS/200 7983 GET http://www.megagitel.com/modules/gavias_sli
derlayer/vendor/revolution/fonts/revicons/revicons.woff? - ORIGINAL_DST/162.214.101.17 font/woff
1598999929.989    358 192.168.50.2 TCP_MISS/200 17337 GET http://www.megagitel.com/sites/default/fil
es/favicon.ico - ORIGINAL_DST/162.214.101.17 image/x-icon
_
```

3. Prueba de conexión WEB por el proxy en la Red Juliaca

Comprobamos que tenemos acceso a internet de la red Juliaca.



4. Prueba de LOGS en SQUID en el server Red Juliaca

Se realiza esta prueba para verificar los logs donde se muestran los registros de accesos de la red Juliaca, permite ver si los servidores tienen acceso a internet y las maquinas que están detrás del servidor están navegando.

```
[root@vpn2 ~]# tail -f /var/log/squid/access.log
1598999782.567     17 192.168.80.2 TCP_MISS/200 5253 GET http://www.sunat.gob.pe/img/escudo.7bb428f2
.png - ORIGINAL_DST/161.132.21.8 image/png
1598999782.808     17 192.168.80.2 TCP_MISS/200 567 GET http://www.sunat.gob.pe/a/txt/tipoCambio.txt
 - ORIGINAL_DST/161.132.21.8 text/plain
1598999782.825     22 192.168.80.2 TCP_MISS/200 617 GET http://www.sunat.gob.pe/a/txt/vencimientos.t
xt - ORIGINAL_DST/161.132.21.8 text/plain
1598999782.832     20 192.168.80.2 TCP_MISS/200 26034 GET http://www.sunat.gob.pe/img/campanas/2020/
c-CSvirual.png - ORIGINAL_DST/161.132.21.8 image/png
1598999782.839     35 192.168.80.2 TCP_MISS/200 2902 GET http://www.sunat.gob.pe/img/gob-pe.922f08f9
.png - ORIGINAL_DST/161.132.21.8 image/png
1598999782.854     18 192.168.80.2 TCP_MISS/200 3023 GET http://www.sunat.gob.pe/img/iconos/instagra
m.png - ORIGINAL_DST/161.132.21.8 image/png
1598999782.878     25 192.168.80.2 TCP_MISS/200 675 GET http://www.sunat.gob.pe/img/flecha-select.bc
1fd982.png - ORIGINAL_DST/161.132.21.8 image/png
1598999782.878     71 192.168.80.2 TCP_MISS/200 38546 GET http://www.sunat.gob.pe/img/campanas/2020/
c-raf.png - ORIGINAL_DST/161.132.21.8 image/png
1598999782.888     66 192.168.80.2 TCP_MISS/200 23553 GET http://www.sunat.gob.pe/img/campanas/2020/
c-sofia-web.jpg - ORIGINAL_DST/161.132.21.8 image/jpeg
1598999788.162    126 192.168.80.2 TCP_MISS/200 85149 GET http://www.sunat.gob.pe/img/favicon.7124d6
8e.ico - ORIGINAL_DST/161.132.21.8 image/x-icon
```

4.2.9. Implementación de STRONGWAN para el protocolo IPSEC.

En esta fase del proceso implementamos la configuración del STRONGWAN del protocolo Ipsec en CentOS 7.8, agregado variables a Linux, creación de rutas estáticas.

1. Edición del archivo SYSCTL.CONF para server VPN1

Para el servidor de la red Puno se activa el archivo SYSCTL.CONF, lo que nos permite ingresar variables a Linux, activamos la variable fortward el cual activa el paso de paquetes a través del proxy.

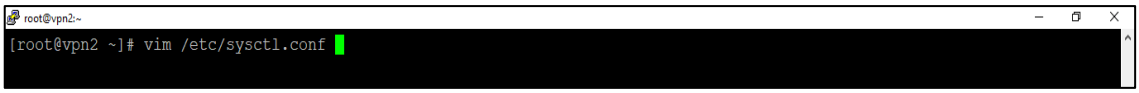
```
[root@vpn1 ~]# vim /etc/sysctl.conf
```

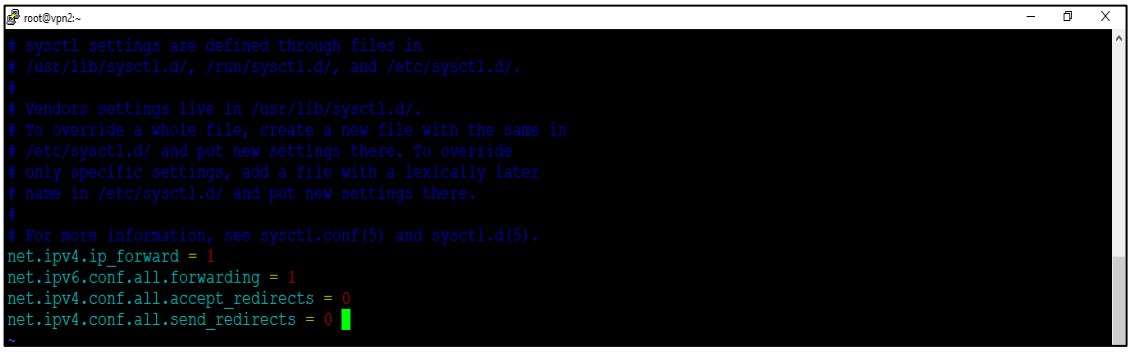
```
root@vpn1:~
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
```

```
root@vpn1:~
[root@vpn1 ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
[root@vpn1 ~]#
```

2. Edición del archivo SYSCTL.CONF para server VPN2

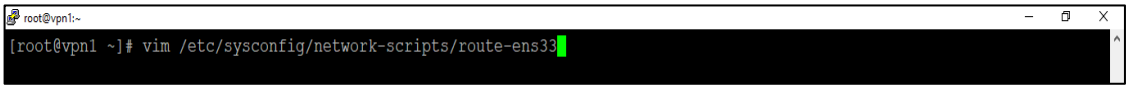
Para el servidor de la red Juliaca se activa el archivo SYSCTL.CONF, activamos la variable fortward el cual activa el paso de paquetes a través del proxy.





3. Creación de archivo route-ens33 RUTA ESTÁTICA SERVER (PUNO)

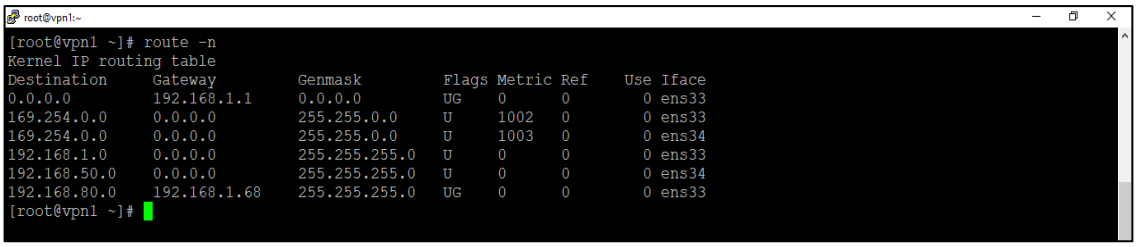
Se crean las rutas estáticas, las creamos en un archivo.



Una vez creada las rutas reiniciamos Linux con el comando **reboot,** para probar las rutas estáticas.

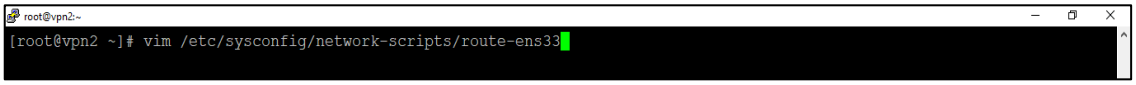
4. Probamos rutas estáticas en el Server Puno

Solo probamos la ruta estática haciendo pines. Para ver la conexión de la red Puno a la red Juliaca.



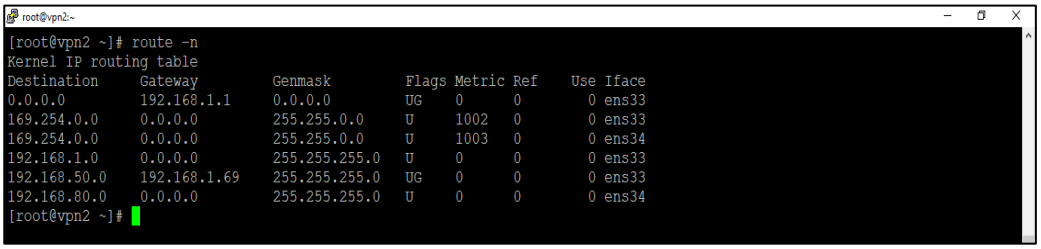
5. Creación de archivo route-ens33 RUTA ESTÁTICA SERVER (JULIACA)

Realizamos el mismo procedimiento en la red Juliaca.



6. Probamos rutas estáticas en SERVER JULIACA

Probamos la ruta estática haciendo pines. Para ver la conexión de la red Juliaca a la red Puno.



7. Instalamos STRONGSWAN (IPSEC) EN CENTOS 7.8 EN SERVER PUNO

Instalamos el programa strongwan en cada servidor, el cual habilitara el protocolo IPSEC para poder utilizar en Linux y levantar la red VPN, el cual se instala en cada servidor red Puno y red Juliaca.

```
root@vpn1:~
[root@vpn1 ~]# yum  -y install strongswan
Complementos cargados:fastestmirror, priorities
Loading mirror speeds from cached hostfile
 * base: mirror.orbyta.com
 * epel: mirrors.ukfast.co.uk
 * extras: mirror.orbyta.com
 * rpmforge: mirrors.ircam.fr
 * updates: mirror.orbyta.com
Resolviendo dependencias
--> Ejecutando prueba de transacción
---> Paquete strongswan.x86_64 0:5.7.2-1.el7 debe ser instalado
--> Resolución de dependencias finalizada

Dependencias resueltas

================================================================================================================================
 Package                    Arquitectura              Versión                       Repositorio              Tamaño
================================================================================================================================
Instalando:
 strongswan                 x86_64                    5.7.2-1.el7                   epel                     1.4 M

Resumen de la transacción
================================================================================================================================
Instalar  1 Paquete

Tamaño total de la descarga: 1.4 M
Tamaño instalado: 4.0 M
Downloading packages:
strongswan-5.7.2-1.el7.x86_64.rpm                                                  | 1.4 MB  00:00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

8. Verificamos versión de STRONGSWAN EN SERVER PUNO

```
root@vpn1:~
[root@vpn1 ~]# strongswan version
Linux strongSwan U5.7.2/K3.10.0-1127.19.1.el7.x86_64
University of Applied Sciences Rapperswil, Switzerland
See 'strongswan --copyright' for copyright information.
[root@vpn1 ~]#
```

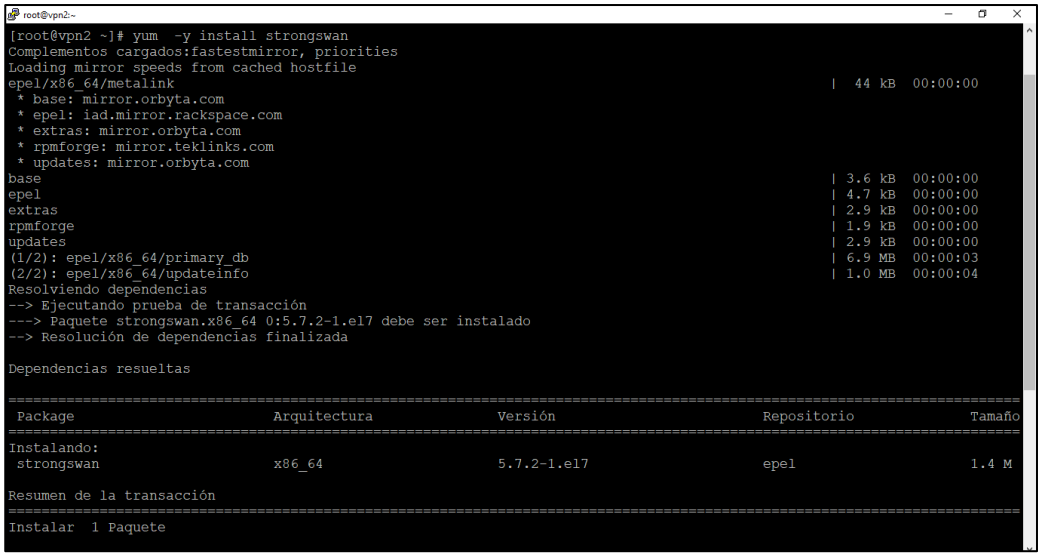
9. Iniciamos/agregamos AL ARRANQUE SERVICIO EN SERVER PUNO

```
root@vpn1:~
[root@vpn1 ~]# strongswan version
Linux strongSwan U5.7.2/K3.10.0-1127.19.1.el7.x86_64
University of Applied Sciences Rapperswil, Switzerland
See 'strongswan --copyright' for copyright information.
[root@vpn1 ~]# systemctl start strongswan && systemctl enable strongswan
Created symlink from /etc/systemd/system/multi-user.target.wants/strongswan.service to /usr/lib/systemd/system/strongswan.
service.
[root@vpn1 ~]#
```

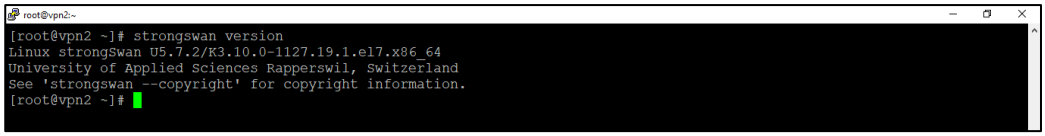
10. Verificamos el estado de STRONGSWAN EN SERVER PUNO

```
root@vpn1:~
[root@vpn1 ~]# systemctl status strongswan
● strongswan.service - strongSwan IPsec IKEv1/IKEv2 daemon using ipsec.conf
   Loaded: loaded (/usr/lib/systemd/system/strongswan.service; enabled; vendor preset: disabled)
   Active: active (running) since mié 2020-09-02 05:26:32 -05; 1min 35s ago
 Main PID: 3283 (starter)
   CGroup: /system.slice/strongswan.service
           ├─3283 /usr/libexec/strongswan/starter --daemon charon --nofork
           └─3312 /usr/libexec/strongswan/charon

sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[CFG] loading crls from '/etc/strongswan/ipsec.d/crls'
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[CFG] loading secrets from '/etc/strongswan/ipsec.secrets'
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[CFG] opening triplet file /etc/strongswan/ipsec.d/triplets.d...tory
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[CFG] loaded 0 RADIUS server configurations
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[CFG] HA config misses local/remote address
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[CFG] no script for ext-auth script defined, disabled
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[LIB] loaded plugins: charon pkcs11 tpm aesni aes des rc2 sha...e so
sep 02 05:26:32 vpn1.lorenachavez.com charon[3312]: 00[JOB] spawning 16 worker threads
sep 02 05:26:32 vpn1.lorenachavez.com ipsec_starter[3283]: charon (3312) started after 100 ms
sep 02 05:26:32 vpn1.lorenachavez.com strongswan[3283]: charon (3312) started after 100 ms
Hint: Some lines were ellipsized, use -l to show in full.
[root@vpn1 ~]#
```

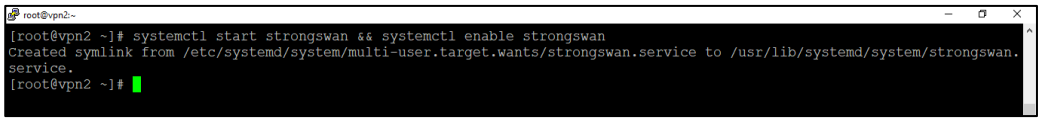
11. Instalamos STRONGSWAN (IPSEC) EN CENTOS 7.8 EN SERVER JULIACA



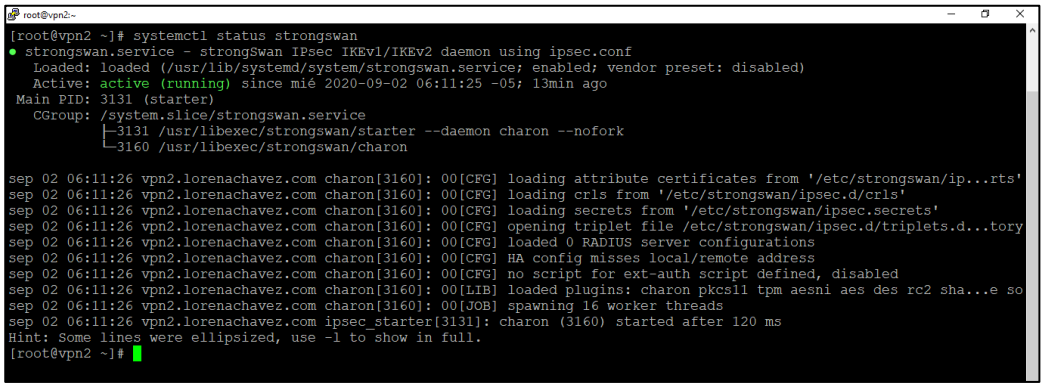
12. Verificamos versión de STRONGSWAN EN SERVER JULIACA



13. Iniciamos/agregamos al arranque servicio en SERVER JULIACA

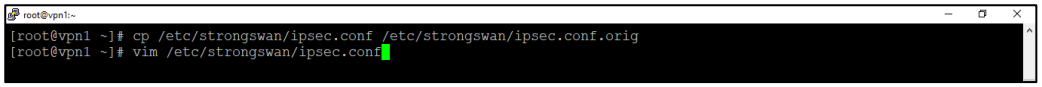


14. Verificamos el estado de STRONGSWAN EN SERVER JULIACA



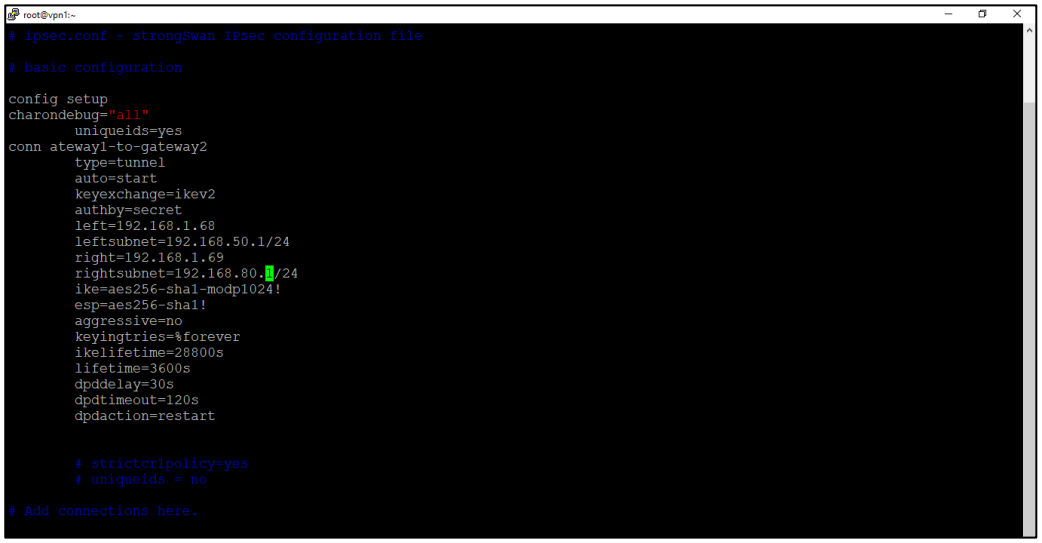
15. Verificamos contenido del directorio /etc/strongswan

16. Copiamos archivo ipsec.conf HACIA ipsec.conf. orig EN SERVER PUNO



17. Edición de archivo /etc/strongswan/ipsec.conf PARA SERVER (PUNO)

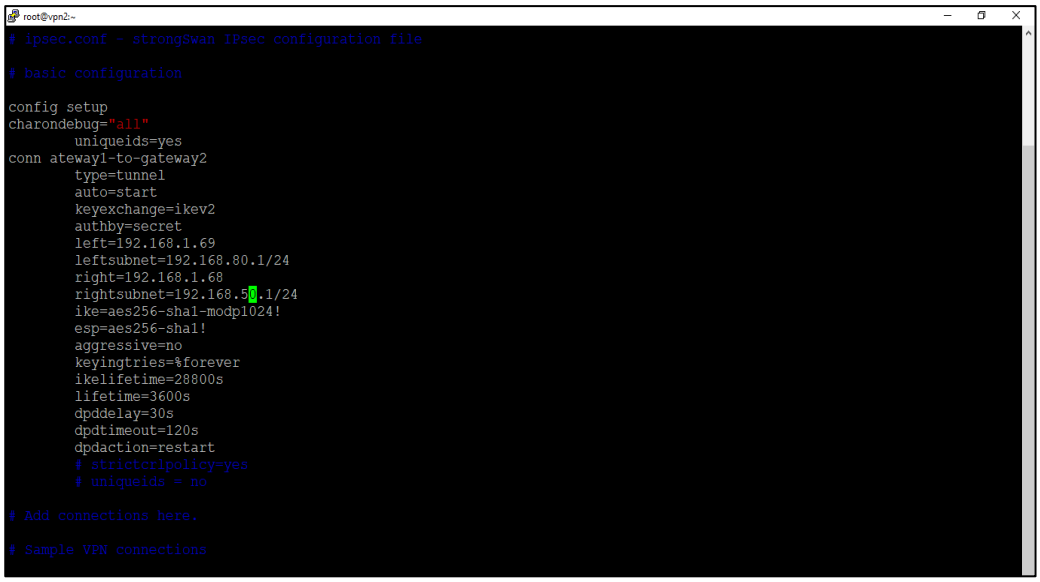
Debemos comentar la línea (charondebug =" all")



18. Copiamos archivo ipsec.conf HACIA ipsec.conf.orig EN SERVER JULIACA

19. Edición de archivo /etc/strongswan/ipsec.conf PARA SERVER (JULIACA).

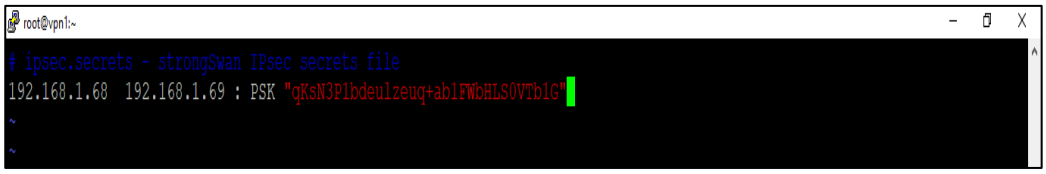
Debemos comentar la línea **(charondebug="all")**



20. Creación de clave PRE-COMPARTIDA FUERTE (PSK)

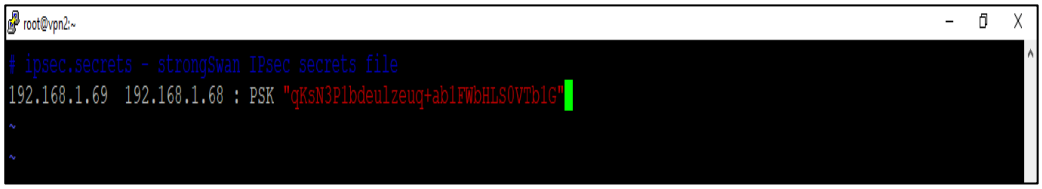
21. Edición archivo /etc/strongswan/ipsec.secrets – SERVER PUNO

22. Agregar datos en /etc/strongswan/ipsec.secrets – SERVER PUNO



23. Edición archivo /etc/strongswan/ipsec.secrets – SERVER JULIACA

24. Agregar datos en /etc/strongswan/ipsec.secrets – SERVER JULIACA



25. Reiniciamos el servicio STRONGSWAN EN SERVER PUNO

26. Reiniciamos el servicio STRONGSWAN EN SERVER JULIACA

4.3. RESULTADOS Y EVALUACIÓN DE LOS RIESGOS INFORMÁTICOS EN LA IMPLEMENTACIÓN DE LA RED VPN

Durante la implementación de una VPN, para lograr una conexión segura para las organizaciones, debemos realizar una evaluación de riesgos de TI, y es importante analizar los ataques detectados en la red por parte de terceros, lo que afecta la seguridad de la información de transmisión de datos a través de Redes físicas locales. Se establecen escalas de probabilidad para realizar la valoración de los riesgos al que están expuestas nuestras redes locales.

Tabla 10: Escalas de probabilidad de riegos informáticos.

PROBABILIDAD	NUMERO DE OCURRENCIA	VALOR
Muy bajo	Una vez al año	1
Bajo	Una vez por semestre	2
Medio	Una vez por trimestre	3
Alto	Una vez por mes	4
Muy alto	Una vez cada quince días	5

Elaboración propia.

La evaluación de impacto tiene en cuenta la asignación a nivel de seguridad de la información dentro de la organización.

Tabla 11: Valoración del impacto de los riesgos informáticos

Impacto	Porcentaje	Descripción del impacto	Valor
Muy bajo	Perdida de información entre 0.1 y 0.4%	- Esto no afecta la seguridad de la información dentro de la organización. - No afecta la imagen de la organización con clientes y terceros. - La información puede ser recuperada.	**1**
Bajo	Perdida de información entre el 0.5 y 0.9 %	- Esto no afecta la seguridad de la información de la organización. - Muestra un ligero efecto en la imagen de la organización con clientes y terceros. - La información se puede recuperar en una cantidad moderada de tiempo	**2**
Medio	Perdida de información entre el 1 y 10 %.	- Hay poco impacto en la seguridad de la información de la organización. - El impacto promedio en la imagen de la organización frente a los clientes. - La información se puede recuperar, pero no de la misma calidad.	**3**
Alto	Perdida de información entre el 11 y 20 %	- Tiene un impacto significativo en la seguridad de la información. - Fuerte influencia en la imagen de la organización. - Dificultad para recuperar información.	**4**
Muy alto	Perdida de información mayor al 20%	- Tiene un grave impacto en la seguridad de la información. - Impacto negativo en la imagen de la organización. - Dificultad para recuperar información.	**5**

Elaboración propia.

Con los resultados obtenidos en la implementación del modelo de Infraestructura de Red VPN para interconexión segura de datos entre las redes locales de las organizaciones de Puno, en el cuadro de valoración de los riesgos informáticos, se ubica en el nivel muy bajo del 0.1 y 0.4 % de perdida de información, brindando seguridad a las redes locales.

4.4. USO DE RESULTADOS Y CONTRIBUCION DEL PROYECTO

En el presente proyecto al obtener los resultados deseados, nos permite reconocer que el modelo de infraestructura de Red VPN podrá ser aplicado de manera óptima en diferentes organizaciones, pequeñas y medianas empresas e instituciones.

Contribuyendo a la comunidad de nuestra Región y otras ciudades, para que puedan implementar esta solución segura y económica en sus organizaciones y puedan interconectar sus redes físicas locales entre sí, con niveles muy altos de seguridad, logrando viaje de datos cifrados, oportunos e íntegros.

4.5. DISCUSIÓN

En nuestra investigación se determinó que el Diseño y la Implementación del modelo de infraestructura de Red VPN permitió mejorar la interconexión segura de datos entre las redes locales de las organizaciones de Puno, logrando consistencia, disponibilidad y confidencialidad de los mismos con un bajo costo de inversión.

Quezada (2016), con la realización de su trabajo de investigación obtuvieron como resultado el acceso a recursos internos desde una red externa a la institución, reduciendo la movilización constante a la biblioteca de cada una de las áreas de la universidad.

Pena (2016), con la implementación de la red VPN-SSL integrada con LDAP se coincide que el trabajo que desarrollo permitió ofrecer movilidad, garantiza la integridad, confidencialidad y seguridad en los datos y reducir los costos en la implementación.

Amenero (2012), de acuerdo a la investigación desarrollada hace constar que, mediante la implementación de una VPN bajo software libre, se optimiza la comunicación entre los locales de su cooperación educativa con un mejor acceso a la información.

Guerrero (2009), luego de analizar las soluciones VPN bajo software libre VPND, constituye una excelente opción para conectar una sede principal con varias oficinas por su gran estabilidad, por estar basada en un estándar como IPSEC. Y por poseer grandes bondades de seguridad.

Melgarejo (2013), con su trabajo realizado garantiza que la fibra óptica permite la implementación de una VPN cifrada a través de un portal cautivo, permitiendo el acceso y difusión de contenido multimedia de alto tráfico garantizando conexiones de alta velocidad y una cobertura total y la facilidad de interconectar a los usuarios que consigan una conexión fija o inalámbrica.

Atencio (2017), logra diseñar e implementar el prototipo de una Red Privada Virtual en Capa 3utilizando utilizando CISCO IOS que asegura y encripta la información compartida entre Oficina de Tecnología e Informática y las coordinaciones académicas brindando confidencialidad, integridad y autenticación a la red.

V. CONCLUSIONES

PRIMERA: Se diseñó e implemento el modelo de infraestructura de Red VPN que permite la interconexión de sus redes locales, logrando consistencia y disponibilidad de los datos, así mismo asegura la confidencialidad de la información que se transporta a través de la Red VPN.

SEGUNDA: Con la implementación de la Red VPN que se realizó satisfactoriamente se demuestra que es eficiente y tiene un bajo costo de inversión, ya que para su implementación se utilizó software libre en su mayoría, demostrando que el presupuesto definido es menor al costo que ofrecen los proveedores de Telefonía/Internet.

TERCERA: la implementación de la Red VPN ha demostrado que los riesgos informáticos, disminuyen en un 0.1 y .04 % de pérdida de información, brindando privacidad a las conexiones de redes locales, permitiendo accesos remotos y el cifrado de datos.

VI. RECOMENDACIONES

PRIMERA: El modelo de infraestructura de Red VPN utiliza el protocolo Ipsec y tiene beneficio altamente significativo, lo cual más adelante se puede mejorar con el uso de protocolos más sofisticados y poco conocidos, lo cual puede llegar a tener un alto nivel de seguridad al que ya se demostró en este trabajo de investigación.

SEGUNDA: Para la aplicación del modelo de infraestructura de Red ya sea en una organización, empresa u otra entidad, se debe tener en cuenta con que equipos se va a trabajar, de acuerdo a los requisitos mínimos tales como se detalla en la creación de las máquinas virtuales, tanto en hardware como en software.

TERCERA: capacitar al personal encargado del área de TI, para el brindar el soporte necesario y el buen funcionamiento de la Red VPN.

VI. REFERENCIAS BIBLIOGRAFICAS

Alvarez, J. S. (2014). *Redes de computadoras I - Redes privadas virtuales VPN*. Chile.

Amenero, V. (2012). *Implementacion de un red privada virtual VPN bajo software libre para optimizar el manejo de informacion entre los locales de la corporacion educativa ADEU de la ciudad de Chiclayo*. Chiclayo.

Atencio, A. M. (2017). *Diseño e implementacion de un prototipo de red privada virtual en capa 3 utilizando cisco IOS para la Universidad Nacional del Altiplano*. Puno.

Berners-Lee, T. (2000). *Tejiendo la red.* Madrid: Siglo XXI.

Brollo, G. (2008). *Redes privadas virtuales.*

Cisco. (13 de Octubre de 2008). *Como funcional las redes privadas virtuales.* Recuperado de: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

De la Luz, S. (13 de Setiembre de 2016). *RZ redes zone.* Recuperado de: https://www.redeszone.net/2011/09/13/ipsec-volumen-iv-ike-intercambio-de-claves-en-internet/

De Leon, A. (11 de Mayo de 2020). *Hosting DIARIO.* Recuperado de: https://hostingdiario.com/centos-linux/

Fernandez, A. (2006). *Redes privadas virtuales.* España.

Gabriel, G. (2008). *Redes privadas virtuales*. Recuperado de: http://exa.unne.edu.ar/informatica/SO/VPN_Gerardo_Brollo.pdf

Gonzalez, A. (2006). *Redes privada virtuales* (tesis de pregrado). Pachuca, hidalgo.

James, K. W. (2013). *Computer Networking-A Top- down* . (6ta edicion).

Martel, V. (03 de Abril de 2019). *Diseño de una red de comunicacion VPN sobre internet para un distribuidor autorizado de claro basado en RFC2764* (tesis de pregrado). Lima.

Melgarejo, R. (2013). *Red privada virtual para la prestacion de servicios multimedia en el campus universitario de la Universidad Nacional del Altiplano*. Puno.

Ñacato, M. (2007). *Diseño e implementacion de una Red Pri{l.o9yyy{´´ñvada Virtual (VPN) para la empresa Hato Telecomunicaciones* (tesis de pregrado). Quito.

Peña, D. (Octubre 2016). *Diseño e implementacion de una red privada virtual (VNP)*. Caracas.

Perez, S. (Noviembre de 2011). *Analisis del protocolo IPsec: el estandar de seguridad en IP*. Recuperado de: http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

Quezada, H. (2016). *Diseño de una VPN para el acceso a las bases de datos cientificas de la Universidad Nacional de Loja*. Loja, Ecuador.

Rivera, J. (2016). *Fundamento de redes informaticas.* IT Campus academy.

Sampieri, R. (2015). *Metodologia de la investigacion.* (7ma Edicion). Mexico: Interamericana Editores S.A.

Tanembaum, W. (2012). *Redes de computadoras.* Mexico: Pearson Eduacion.

ANEXOS

Anexo 1. Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES
PROBLEMA GENERAL	**OBJETIVOS GENERAL**	**HIPOTESIS GENERAL**	**DEPENDIENTE**
¿Cómo lograr que las organizaciones de Puno, conecten sus redes LAN físicas y accesos remotos, usando tecnologías de cifrado y de bajo costo para garantizar la confidencialidad, seguridad y protegiendo la privacidad de los mismos?	Desarrollar un modelo de Infraestructura de Red VPN para mejorar la interconexión segura de datos entre las redes locales de las organizaciones de Puno.	El diseño y la implementación del modelo de Infraestructura de Red VPN mejora la interconexión segura de datos entre las redes locales de las organizaciones de Puno.	Modelo de Infraestructura de Red VPN, para Interconexión Segura de Organizaciones.
PROBLEMAS ESPECIFICOS	**OBJETIVOS ESPECIFICOS**	**HIPOTESIS ESPECIFICAS**	**INDEPENDIENTE**
• ¿Qué niveles de funcionalidad, confiabilidad y seguridad deben existir en el diseño de una VPN para optimizar las comunicaciones de datos en las organizaciones de Puno? • ¿Por qué las organizaciones de puno no cuentan con la implementación de tecnologías adecuadas de cifrado de datos, para permitir las conexiones de sus redes LAN y sus dispositivos necesarios? • ¿A qué riesgos informáticos están expuestas las organizaciones de Puno, al no conectar sus redes locales y accesos remotos, con tecnologías de cifrado de datos?	• Diseñar la red VPN segura, de alto nivel, logrando consistencia y disponibilidad de los datos, asegurando la confidencialidad de los mismos. • Implementar la red VPN eficiente con bajo costo de inversión y utilizando software libre en su mayoría, utilizando el protocolo IPSEC y Linux. • Evaluar los riesgos informáticos, brindando privacidad a las conexiones de sus redes locales y accesos remotos, mediante el cifrado de datos.	• El diseño de la red VPN, logra consistencia y disponibilidad de los datos, asegurando la confidencialidad de los mismos. • La implementación de la red VPN es eficiente y con bajo costo de inversión utilizando software libre en su mayoría. • Los riesgos informáticos, disminuyen brindando privacidad a las conexiones de sus redes locales y accesos remotos, mediante el cifrado de datos.	Usando Ipsec con Linux, bajo un entorno virtualizado se clientes y servidores.

Anexo 2. Comandos utilizados

LISTA DE COMANDOS

Login del usuario	root
Verificar la IP del sistema	ip a
Verificar los nombres de la tarjeta de red	ls/sys/class/net/
Configuración de la tarjeta de Red	vi /etc/sysconfig/network-scripts/ifcfg-ens33 vi /etc/sysconfig/network-scripts/ifcfg-ens34
Reiniciar el servicio de RED	systemctl restart network
Actualización de todo el sistema	yum –y update
Verificación del estado de SELINUX	sestatus
Edición del archivo CONFIG de SELINUX	vi /etc/selinux/config
Verificación del estado de firewallad.	Systemctl status firewalld
Desactivar y detener el servicio firewalld	systemctl stop firewalld & systemctl disable firewalld.
Desactivar los servicios NetworkManager	systemctl stop NetworkManager & systemctl disable NetworkManager
Detener los servicios CUPS	systemctl stop cups & systemctl disable cups

Desactivar y detener los servicios	systemctl stop postfix & systemctl disable postfix
Postfix & ModemManager	systemctl stop ModemManager.service & systemctl disable ModemManager.service
Instalación de repo EPEL	yum –y install epel-release
Instalamos paquetes SQUID & FIREWALLD	yum –y install squid firewalld
Crear directorios de CACHE	squid –z
Iniciar el servicio SQUID en CentOS	systemctl start squid && systemctl enable squid