UNIVERSIDAD NACIONAL

"PEDRO RUÍZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

"Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo"

TESIS

Para optar el título profesional de ingeniero en computación e informática

ELABORADO POR:

Bach. De La Cruz Bernilla Segundo Magdaleno

Bach. Vera Cruz Jean Ronald Steven

ASESOR:

ING. Bravo Jaico Jessie Leila

LAMBAYEQUE - PERÚ

2019

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS
DECANATO
Ciudad Universitaria - Lambayeque

ACTA DE SUSTENTACIÓN Nº 072-2019-D/FACFyM

(Sustentación Autorizada por Resolución N° 1479-2019-D/FACFyM)

En la ciudad de Lambayeque, siendo las 12:00 del día 03 de Diciembre del 2019 se reunieron en la Videoteca del Laboratorio de Física-FACFyM los miembros del Jurado designados mediante Resolución Nº 994-2018-D/FACFyM, los docentes:

Dra. Ing. Giuliana Fiorella Lecca Orrego Presidente
Mg. Ing. Oscar Alex Serquén Yparraguirre Secretario
Mg. Ing. Denny John Fuentes Adrianzén Vocal

Para recibir la tesis titulada:

Implementación de una VPN con Open Source para la Gestión de Aplicaciones de Intranet en la Universidad Nacional Pedro Ruiz Gallo

desarrollada por los Bachilleres en Computación e Informática, **De la Cruz Bernilla Segundo Magdaleno y Vera Cruz Jean Ronald Steven**

Después de escuchar la exposición y las respuestas a las preguntas formuladas por los miembros del Jurado, se acordó APROBAR el trabajo por UNANIMIDAD con el calificativo de BUENO

En consecuencia, los Bachilleres en referencia quedan aptos para recibir el Título Profesional de **Ingeniero en Computación e Informática** de acuerdo a la Ley Universitaria, el Estatuto y Reglamento de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque.

Observaciones:

Para constancia del hecho firman.

Dra. Ing. Giuliana Fiorella Lecca Orrego
Presidente

Mg. Ing. Oscar Alex Serquén Yparraguirre
Secretario

Mg. Ing. Denny John Fuentes Adrianzén
Vocal

UNIVERSIDAD NACIONAL "PEDRO RUÍZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

"IMPLEMENTACIÓN DE UNA VPN CON OPEN SOURCE PARA LA GESTIÓN DE APLICACIONES DE INTRANET EN LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO"

Dra. Ing. Fiorella Lecca Orrego
Presidente

Mg. Ing. Oscar Alex Serquén Yparraguirre
Secretario

Mg. Ing. Denny John Fuentes Adrianzén
Vocal

UNIVERSIDAD NACIONAL "PEDRO RUÍZ GALLO"

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

ESCUELA PROFESIONAL DE INGENIERÍA EN COMPUTACIÓN E INFORMÁTICA

TESIS

"IMPLEMENTACIÓN DE UNA VPN CON OPEN SOURCE PARA LA GESTIÓN DE APLICACIONES DE INTRANET EN LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO"

M. Sc. Ing. Jessie Leila Bravo Jaico
Asesora

Bach. De La Cruz Bernilla Segundo Magdaleno
Tesista

Bach. Vera Cruz Jean Ronald Steven
Tesista

DEDICATORIA

Esta tesis está dedicada con mucho afecto y cariño:

A nuestros padres por su amor, trabajo y sacrificio en todos estos años, gracias a ellos hemos logrado llegar hasta aquí y convertirnos en lo que somos además de brindarnos su apoyo en todo momento a lo largo de esta etapa de nuestras vidas para llegar a ser unos profesionales.

A todas las personas que a pesar de tener poco tiempo y disponibilidad, nos brindaron apoyo en el transcurso del desarrollo de tesis.

Los Autores

AGRADECIMIENTO

Primeramente, agradecemos a Dios por darnos la vida, por ponernos en el lugar que estamos hoy día y mantenernos siempre en el camino correcto.

Gracias a nuestros padres: Ronald Vera y Melchora Cruz; Magdaleno De La Cruz y Mercedes Bernilla; por ser confiar y creer en nuestras expectativas, por los consejos, valores y virtudes que nos han inculcado a lo largo de nuestras vidas.

Agradecemos también a nuestra asesora de tesis la Ing. Jessie Leyla Bravo Jaico por habernos brindado la oportunidad de recurrir a su capacidad y conocimiento en la materia, así como también haber tenido paciencia para con nosotros y guiarnos durante todo el desarrollo de la tesis.

Y para finalizar agradecemos a todas aquellas que nos brindaron su tiempo para complementar nuestra información.

Los Autores

Índice General

Índice de Figuras

Índice de Tablas

RESUMEN

En la presente tesis se realizó un estudio cuyo propósito fue determinar que el uso de una VPN sería ideal para mejorar la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo, ya que al tratarse de una universidad nacional, siempre se ve envuelta en problemas administrativos, lo que ralentiza el tramite de documentos. Se aplicó un diseño cuasi experimental en la que se realizó un juicio de expertos a 2 ingenieros, quienes fueron reunidos para la votación unánime de nuestra metodología. Por lo tanto se concluyó que la metodología propuesta es válida y aplica, permitiendonos así trabajar en el diseño e implementación de la VPN con Open Source, que luego de investigar los softwares VPN de código abierto, nos decidimos por utilizar Softether VPN

ABSTRACT

In this thesis a study was conducted whose purpose was to determine the use of a VPN would be ideal to improve the management of intranet applications in our alam mater the National University Pedro Ruiz Gallo, since being a national university, it is always involved in administrative problems, which slows the processing of documents. A quasi-experimental design was applied in which an expert judgment was conducted to 2 engineers, who were gathered for the unanimous vote of our methodology. Therefore, it was concluded that the proposed methodology is valid and applied, allowing us to work on the design and implementation of open source VPN, which after investigating about open source VPN software, we decided to use Softether VPN

INTRODUCCIÓN

La UNPRG (Universidad Nacional Pedro Ruiz Gallo) con sede principal ubicada en Calle Juan XXIII, Lambayeque es la única universidad estatal de la región que viene brindando servicio de formación universitaria a estudiantes desde el 17 de marzo de 1970.

Nuestra *alma máter* tiene como misión formar capital humano líderes con base científica, humanística y tecnológica; comprometida con la excelencia académica y la responsabilidad social, a partir de la creatividad e innovación, investigación científica y eficiencia operativa, contribuyendo al desarrollo sostenible del país y la sociedad en un contexto globalizado, dinámico e interconectado.

Teniendo como visión al 2021 hacer de la Universidad Nacional Pedro Ruiz Gallo una institución académica con altos estándares de calidad y referente en el norte del país por su compromiso con la competitividad del capital humano, a partir de su labor formativa y producción de conocimiento de impacto.

Pues bien, actualmente en la UNPRG, algunos trabajadores administrativos de las oficinas más críticas (rectorado, vicerrectorado, asuntos académicos, red telemática, contabilidad general, etc…), tienen la necesidad de utilizar las aplicaciones de gestión administrativa para sus actividades funcionales, sin embargo no siempre el usuario trabajador de la universidad se encuentra en su oficina de trabajo, debido a que el personal se encuentra participando de comisiones de servicio, capacitaciones, o también por eventos extraordinarios como paros administrativos, tomas de universidad, licencias laborarles (eventuales), etc. Esto requiere de una alternativa de conectividad empresarial a estas aplicaciones críticas que retardan la productividad de cada dependencia. Estas aplicaciones críticas comprenden desde sistemas académicos (Actas virtuales en su gestión administrativa, GestAc, Presys, SIGA académico de enfermería – FE, SIBI),

administración de servidores(DNS, DHCP, FTP, telefonía IP, cámaras ip, entre otros), equipos cisco (Switchs, Routers, Access Points) Equipos de seguridad (Firewalls,WAF), sistemas de gestión administrativa-Financiera (SIGA, SIAF, SISGEDO, PDT, Planillas, Sistemas de mesa de partes, etc.) y finalmente de gestión de investigación (Sistema de Gestión de revistas científicas, Repositorios institucionales, Editorial, Inventario, Balance Score Card - tablero).

Asimismo, existen soluciones de acceso remoto, sin embargo, estas requieren un costo elevado por licencia, además demanda tiempo de gestión administrativa para adquirir dichas licencias.

Por otro lado, la seguridad de la información es indispensable en todo proyecto a gran escala. Por esto, basados en la ISO 27001, tendremos en cuenta los 3 pilares básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad).

De la misma manera, la introducción de Software Libre en el Perú ha sido favorecida gracias a la ley N°28612, que también es llamada de "Neutralidad Tecnológica" porque norma el uso, adquisición y adecuación de software por parte del Estado peruano. Esta ley prohíbe a cualquier entidad de la administración pública adquirir soportes físicos (hardware) que la obliguen a utilizar un solo tipo de software o que limiten de cualquier manera su autonomía informática.

Así pues, una de las condiciones básicas propuestas por la Superintendencia Nacional De Educación Superior Universitaria (SUNEDU) para el licenciamiento y acreditación de la Universidad Nacional Pedro Ruiz Gallo es contar con una infraestructura y equipamiento adecuado para que el personal administrativo y académico pueda cumplir sus labores, siendo este un motivo más para la realización de nuestra tesis.

En este sentido, la propuesta de tesis pretende cubrir una necesidad al respecto, proponiendo implementar una infraestructura de VPN con Open Source para la gestión remota de aplicaciones de Intranet en la Universidad Nacional Pedro Ruiz Gallo.

Una Red Privada Virtual (VPN) conecta los componentes de una red sobre otra red. La conexión de los usuarios de distintas redes a través de un túnel que se construye sobre Internet o sobre cualquier red pública, permitiendo a los usuarios trabajar en sus casas o empresas conectados de una forma segura con el servidor corporativo, usando la infraestructura provista por la red pública (Internet) ya que los datos aparecen como si fueran enviados a través de la misma red LAN, como si estuvieran en la empresa.

Entonces, esta investigación se fundamenta en el estándar ISO 27001 y el modelo empresarial CISCO, garantizando un túnel de autenticación segura para el acceso a intranet de forma confidencial e integra, permitiendo que la universidad agilice sus procesos y garantice el envío de datos de forma segura.

Finalmente, con el presente trabajo que tiene como objetivo general mejorar la gestión de aplicaciones de la Intranet con la implementación de una VPN Open Source en la Universidad Nacional Pedro Ruiz Gallo, nos permitirá acceder remotamente a las datos y aplicaciones internas, haciendo uso de software libre, ya que esto es muy pedido por los administrativos, entre ellos: vicerrectorado de investigación, DGA, asuntos académicos, red telemática, contabilidad general, etc. Ya que de estas oficinas depende realizar actividades que involucran la transmisión y aprobación de pagos, backups de diversos servicios, actualizaciones de notas y horarios, entre otras.

2019

CAPÍTULO I

DISEÑO TEÓRICO

1.1. ANTECEDENTES

1.1.1. Internacionales

1. Ing.Gloria E. Guerrero Mejias (2009) “DISEÑO Y ANÁLISIS DE SOLUCIONES SEGURAS VPN BASADAS EN SOFTWARE LIBRE” Presentado a la Universidad Central de Venezuela, para optar al título de Especialista en comunicaciones y redes de comunicaciones de datos.

   Llego a las siguientes conclusiones:

   - La implementación de la solución VPN LAN a LAN bajo software libre como StrongSwan es bastante sencilla. La complicación radica en las configuraciones adicionales que se realicen a fin de fortalecer la seguridad de la misma.
   - Si se quiere reforzar la seguridad de las soluciones VPN software libre a implementar con el uso de una Infraestructura de Clave Pública (PKI), se debe tener en cuenta que la gestión y el concepto pudieran resultar complejos si no se tienen políticas claras definidas al respecto.
   - Cabe reflexionar que una de las desventajas del software libre es la carencia en la realidad venezolana de empresas que den soporte y servicio especializado a estas soluciones, teniendo en muchos casos que ser asumido por la empresa que los implante.

2. Tomás Canovas, Juan (2008) “SERVICIO VPN DE ACCESO REMOTO BASADO EN SSL MEDIANTE OPENVPN”, Presentada a la Universidad Politécnica De Cartagena, para optar el título de Ingeniería Técnica de telecomunicación.

   Llego a las siguientes conclusiones:

   - Elegimos la tecnología para implementar VPNs basada en el protocolo SSL/TLS, para estudiar una estructura concreta capaz de construir redes privadas virtuales.

Entre las distintas implementaciones de esta tecnología, optamos por OpenVPN, por ser una herramienta completa y flexible.

- La tecnología SSL/TLS constituye sin duda alguna una opción flexible y robusta de asegurar las comunicaciones a través de la infraestructura de redes públicas. Esperamos que este documento permita comprender cómo funciona, y cómo se configura, sin demasiada dificultad, una conexión VPN SSL/TLS mediante OpenVPN.

1.1.2. Nacionales

1. Ricardo Armando Menendez Avila.(2012)"ESTUDIO DEL DESEMPEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN MPLS-VPN SOBRE MÚLTIPLES SISTEMAS AUTÓNOMOS." Presentado a la Pontifica Universidad Católica Del Perú, para optar el título de ingeniero de telecomunicaciones.

   Llegó a las siguientes conclusiones:

   - Se realizó un estudio detallado de la arquitectura MPLS y su uso principal en las implementaciones de redes privadas virtuales. Se planteó la necesidad de contar con un modelo que garantice el buen desempeño de una red VPN, y que pueda soportar incrementos futuros. Se logró identificar al modelo de implementación "MultiProtocolo BGP Multisalto entre Route Reflectors" como el más adecuado.
   - Se realizó la propuesta técnica en la cual se describe el escenario general al que se enfrenta un proveedor de servicio para brindar servicios VPN a grandes distancias. Se logró elaborar un plan de trabajo que permita lograr la conectividad de extremo a extremo y aprovechar los beneficios que este tipo de redes ofrece.
   - El costo del proyecto va acorde a las características del mercado, se ha tomando en cuenta los precios del mercado actual, ajustando la propuesta a la situación de nuestro país.

2. Ing. Patricia Lourdes Salas Chacón.(2014) “EL USO DE SOFTWARE LIBRE EN LA MINIMIZACIÓN DE COSTOS EN CENTROS DE TECNOLOGIA DE INFORMACIÓN EN UNA UNIVERSIDAD PERUANA” Presentado a la universidad Nacional de Ingeniería, para optar el grado académico de Maestro en Ciencias con mención en ingeniería de sistemas.

   Llego a las siguientes conclusiones:

   - Se ha demostrado que el proyecto propuesto es económicamente viable. Asimismo, promoverá la utilización de software libre en la Universidad Peruana de Ciencias e Informática, hecho que permitirá expandir la visión de los estudiantes respecto a la investigación en esta área de conocimiento.
   - La administración de un CTI basado en L TSP es más efectiva que la administración de un CTI convencional, el tiempo y costo asociado al trabajo del personal de soporte en efectuar tareas de reinstalación de equipos es O.
   - Existe incompatibilidad de con software propietario que solo corre sobre plataforma Windows, las empresas desarrolladoras de software CopyRight mantienen un monopolio del software que desarrollan, lo cual limita a la comunidad a ser simples usuarios finales.

1.1.3. Regionales:

1. Virgilio Amenero Vázquez. (2012) “IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN) BAJO SOFTWARE LIBRE PARA OPTIMIZAR EL MANEJO DE INFORMACIÓN ENTRE LOS LOCALES DE LA CORPORACIÓN EDUCATIVA ADEU, DE LA CIUDAD DE CHICLAYO.” Presentada a la universidad católica Santo Toribio De Mogrovejo, para optar por el título de Ingeniero de Sistemas y Computación.

   Llegó a la siguiente conclusión:

- La solución OpenVPN está segura de posibles ataques externos, encriptado la información para que no pueda ser visible ante personas ajenas a la institución y enfrascando las posibles vulnerabilidades ante la red pública, permitiendo la confidencialidad y seguridad en la transmisión de los datos.

2. Díaz Llatance Manuel Auner y Vieyra Dioses Gino Luis Alberto (2015) "DISEÑO DE UNA RED PRIVADA VIRTUAL PARA INTERCONECTAR LAS SUCURSALES DE LA EMPRESA TERRACARGO SAC." Presentada a la Universidad Nacional Pedro Ruiz Gallo, para optar el título profesional de ingeniero electrónico.

   Llego a las siguientes conclusiones:

   - Debido a las ventajas económicas que ofrecen las Redes Privadas Virtuales se puede concluir que se trata de una excelente tecnología para el acceso remoto, puesto que el uso de una VPN constituye un sustituto indispensable a los métodos tradicionales caros como es la transmisión de datos a través de fibra óptica punto a punto.
   - Una VPN podrá ser aplicada en todo tipo de entornos, desde las grandes empresas con sucursales en diversas partes del país o del mundo y varios trabajadores móviles hasta las pequeñas empresas que tengan dos o más sucursales en una sola ciudad.
   - Las VPN permiten brindar servicios a los clientes de la empresa en cualquier lugar del mundo, con lo que los clientes obtendrán la información que el necesita al instante, lo que generará una mayor productividad de la empresa.

1.2. Objetivos

1.2.2. Objetivo General

Mejorar la gestión de aplicaciones de la Intranet con la implementación de una VPN Open Source en la Universidad Nacional Pedro Ruiz Gallo.

1.2.3. Objetivos Específicos

- Realizar un estudio y descripción de la red actual en la UNPRG; para identificar y enfocar los usuarios críticos que requieran un acceso remoto a la intranet de la universidad.
- Determinar los requerimientos necesarios para la implementación de la VPN.
- Diseñar la topología física y lógica teniendo en cuenta criterios de seguridad y acceso rápido.
- Elaborar el presupuesto de los equipos que se requerirán y el plan de actividades conforme a la propuesta planteada.
- Realizar la evaluación de retorno de inversión del presupuesto haciendo uso del VAN, TIR y PR.
- Implementar una VPN para optimizar la gestión de Aplicaciones de la intranet de la UNPRG, para otorgar acceso remoto a las oficinas anteriormente identificadas.
- Demostrar con herramientas de testeo la seguridad e integridad de los datos que viajan por la VPN para garantizar la confidencialidad y disponibilidad de los mismos.

1.3. Base Teórica

1.3.2. VPN

Una VPN es una tecnología de red que permite una conexión segura a través de Internet conocida como túnel, mediante un proceso de encapsulación y encriptación de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Además, permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada. (González Valenzuela, 2014)

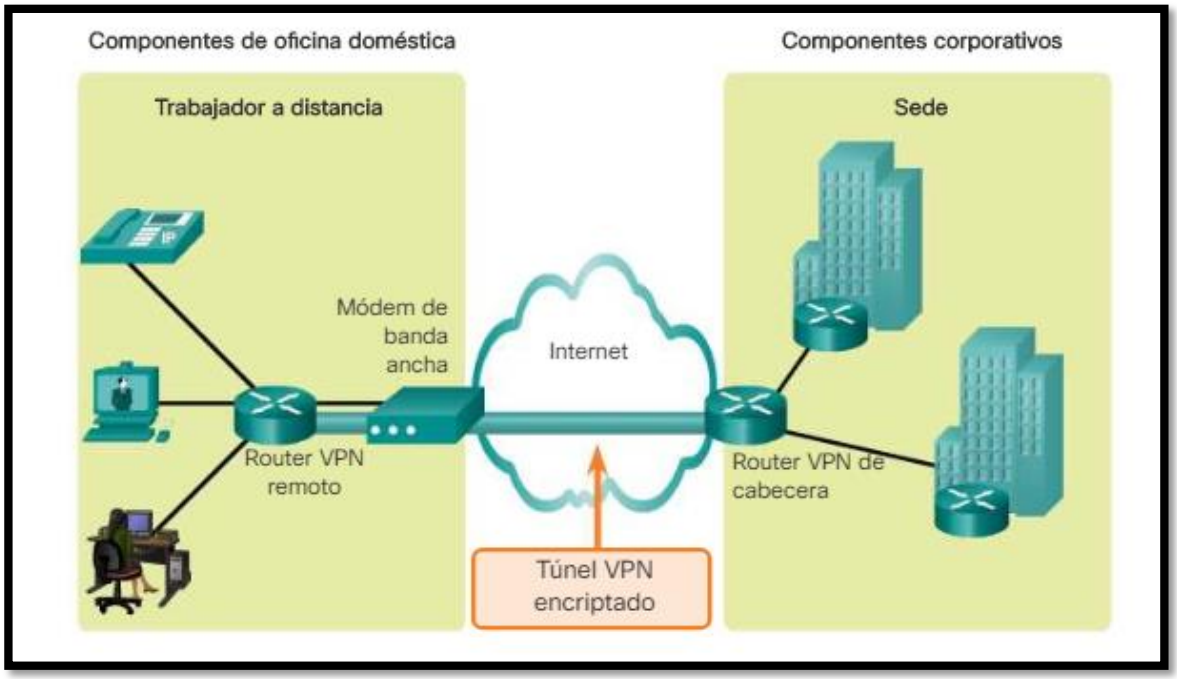


Figura 1: Trabajadores a distancia - VPN

Cisco (2018). Ilustración de Requisitos de conectividad de trabajadores a distancia [Figura]. Recuperado de https://ccnadesdecero.es/trabajo-a-distancia-beneficios-requisitos/

1.3.2.1. Requerimientos básicos de una VPN

Según Hernández (2009) expone que, al implementar una solución de red remota, una empresa necesita facilitar el acceso controlado a los recursos e información de la empresa. La solución debe permitir que los clientes itinerantes o remotos se conecten a los recursos

LAN, y la solución debe permitir que las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de enrutador a enrutador). Además, la solución debe garantizar la privacidad y la integridad de los datos a medida que atraviesan Internet. Las mismas preocupaciones se aplican en el caso de datos confidenciales que atraviesan una red interna corporativa.

Por lo tanto, una solución de VPN debe proporcionar al menos todo lo siguiente:

Confidencialidad. - Protege los datos de ser leídos por alguien no autorizado. Esto es posible gracias a mecanismos de cifrado de datos, que utilizan algoritmos criptográficos y claves secretas (valores conocidos solo por dos partes entre las que se establece la comunicación). Los datos solo pueden ser descifrados por alguien que conozca la clave secreta.

- **Integridad. -** Protege los datos de ser modificados durante la comunicación, por alguien no autorizado. Esto es posible gracias a mecanismos que generan un valor de autenticación de mensaje (MAC, Message Authentication Code). Si los datos son alterados por alguien no autorizado, el nuevo MAC calculado sobre el mensaje será distinto
- **Autenticación mutua.** Garantiza que la comunicación se desarrolla entre los auténticos participantes. Esto es posible porque cada extremo de la comunicación confirma la identidad del otro.
- **Protección frente a reenvíos**. - Garantiza que los datos no serán entregados más de una vez. De esta forma, un atacante no podrá interceptar y retirar alguno de los paquetes que componen el mensaje, e insertar otros paquetes malintencionados en la comunicación.
- **Protección frente al análisis de tráfico. -** Garantiza que no se podrá extraer información valiosa a través del análisis del tráfico de la comunicación (como

datos sobre emisor y receptor, frecuencia de la comunicación, cantidad de datos transmitidos, etc.). Esto es posible gracias a mecanismos de protección contra métodos de análisis de tráfico que pueda llevar a cabo un atacante.

- **Control de acceso. -**Garantiza que sólo los usuarios autorizados podrán a acceder a determinados recursos de la organización. Esto es posible gracias a mecanismos de filtrado, que permiten habilitar o bloquear ciertos tipos de tráfico de red, por ejemplo, permitiendo los accesos web, pero no la compartición de ficheros.
- **Dirección de direcciones**. - La solución debe asignar una dirección de cliente VPN en la intranet y garantizar que las direcciones privadas se mantengan privadas.
- **Cifrado de datos**. - Los datos transportados en la red pública deben ser ilegibles para clientes no autorizados en la red.
- **Administración de claves**. - La solución debe generar y actualizar claves de cifrado para el cliente y el servidor.
- **Soporte multiprotocolo**. - La solución debe manejar protocolos comunes utilizados en la red pública. Estos incluyen IP, Internetwork Packet Exchange (IPX), y así sucesivamente. (Roldan, 2017, pág. 8)

Una solución de Internet VPN basada en el protocolo de túnel punto a punto (PPTP) o el protocolo de túnel de capa dos (L2TP) cumple con todos estos requisitos básicos y aprovecha la amplia disponibilidad de Internet. Otras soluciones, incluida Internet Protocol Security (IPSec) se compone de un conjunto de normas que se utilizan para establecer una conexión VPN. (Microsoft, 2009)

Debido a que el mercado está inundado de soluciones VPN, debe tomarse precauciones adicionales para garantizar que se tome la mejor decisión posible al elegir una solución VPN para su empresa.

Las dos categorías principales de productos VPN para elegir son los dispositivos de hardware VPN dedicados y las VPN basadas en servidor, también denominadas VPN de hardware y software.

VPN de hardware: Una VPN de hardware ejecuta su red a través de un equipo dedicado que tiene su propio procesador y firewall. Este tipo de VPN es superior en dos áreas principales: seguridad y velocidad. El hecho de que la VPN de hardware solo maneja sus propias funciones, en lugar de ejecutarse sobre un dispositivo de propósito general, lo hace menos vulnerable a los ataques, mientras que su procesador dedicado evita que se consuman los ciclos de CPU de sus servidores. En el lado negativo, las VPN de hardware pueden ser costosas, y cuanto más necesite escalar, más se puede obtener con la propuesta.

Software VPN: Un software VPN es una aplicación que se ejecuta en un servidor. Las mayores ventajas de las VPN de software son la asequibilidad y la escalabilidad. Una VPN de software implicará una inversión inicial más baja que una VPN de hardware, y la ampliación es tan simple como actualizar los componentes del servidor de vez en cuando. En el lado negativo, su VPN será tan segura como el hardware en el que se está ejecutando, y la compartición del procesador / memoria probablemente hará que se atrase con respecto a las velocidades de VPN de hardware. (Morales, 2006, págs. 62-63)

1.3.2.2. Comparación VPN Hardware vs VPN Software

Tabla 1

Tabla 1: Cuadro Comparativo entre hardware y software VPN

	VPN HARDWARE	VPN SOFTWARE
Costo	Generalmente las VPN de hardware son más costosas.	Las VPN de software son baratas especialmente si es de software libre.
Escalabilidad	Depende del modelo y al costo asociado a la actualización de un modelo más grande. Limitada por la licencia.	La escalabilidad se basa en la actualización generalmente se traduce en reemplazar un procesador integrado o agregar memoria al sistema.
Seguridad	Son más seguras ya que la única función del hardware es la administración de conexiones VPN	Se ven obligadas a compartir un servidor con otras aplicaciones y sistemas operativos, lo que los hace más propensos a los ataques y menos seguros.
Mantenimiento	Están sujetos a contratos de soporte de mantenimiento que le dan derecho a actualizaciones y soporte de software.	Algunas VPN de software de código abierto, están disponibles de forma gratuita y no tienen costos de mantenimiento elevados
Rendimiento	Ofrecen mejor rendimiento, por lo que se dedica a una sola tarea, ofrecen equilibrio de carga.	Las soluciones VPN basadas en servidor a menudo están restringidas porque coexisten con otras aplicaciones, lo que restringe su rendimiento

Nota: Se tomó en cuenta las variables costo, escalabilidad, seguridad, mantenimiento y rendimiento.

1.3.2.3. Tipos de VPN

Existen básicamente dos tipos de VPN, estos son:

1.3.2.3.1. VPN de acceso remoto

Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la compañía siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, sin importar donde se encuentre. Estos dispositivos se conocen como puntos finales y pueden ser computadoras portátiles, tabletas o teléfonos inteligentes. Los avances en la tecnología de VPN han permitido que

se realicen comprobaciones de seguridad en los puntos finales para garantizar que cumplan una determinada postura antes de conectarse. (Cisco Systems, 2008)

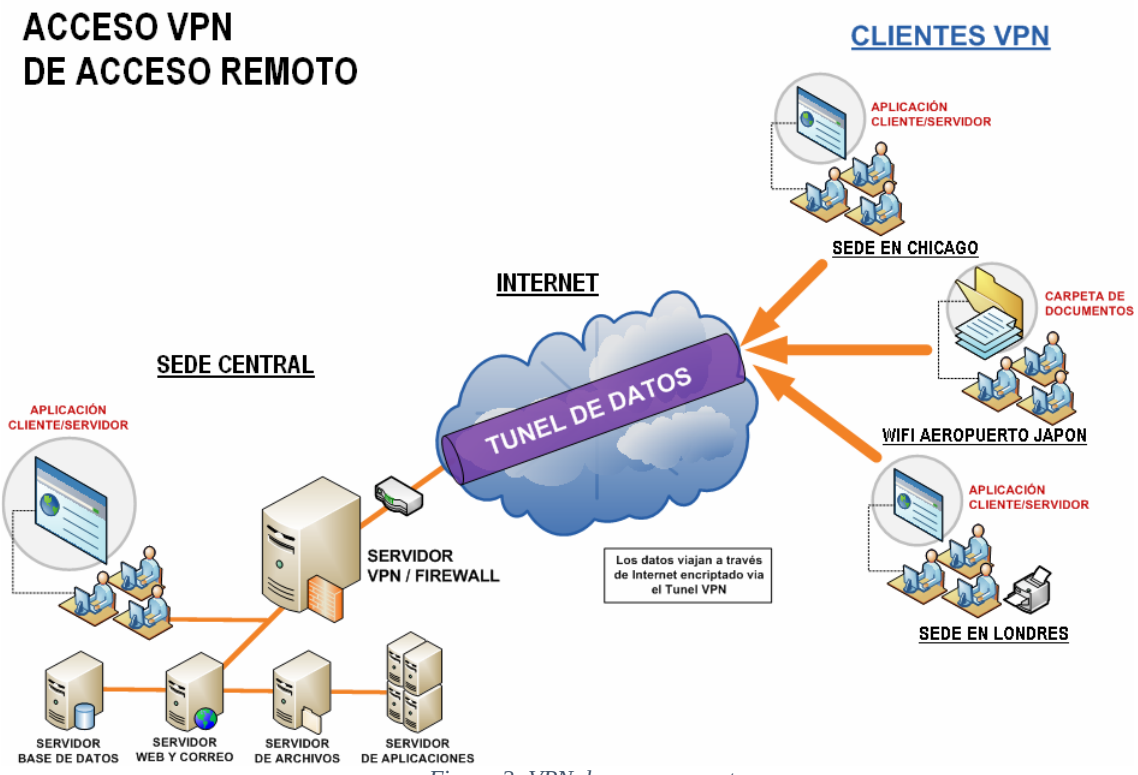


Figura 2: VPN de acceso remoto

Tomás C. (2008). Ilustración de VPN de acceso remoto [Figura]. Recuperado de https://core.ac.uk/download/pdf/60416203.pdf

1.3.2.3.2. VPN de Sitio a Sitio

Una VPN de sitio a sitio conecta la oficina corporativa a las sucursales a través de Internet. Las VPN de sitio a sitio se utilizan cuando la distancia hace que no sea práctico tener conexiones de red directas entre estas oficinas. El equipo dedicado se usa para establecer y mantener una conexión. Piense en el acceso de sitio a sitio como red a red. (Cisco Systems, 2008)

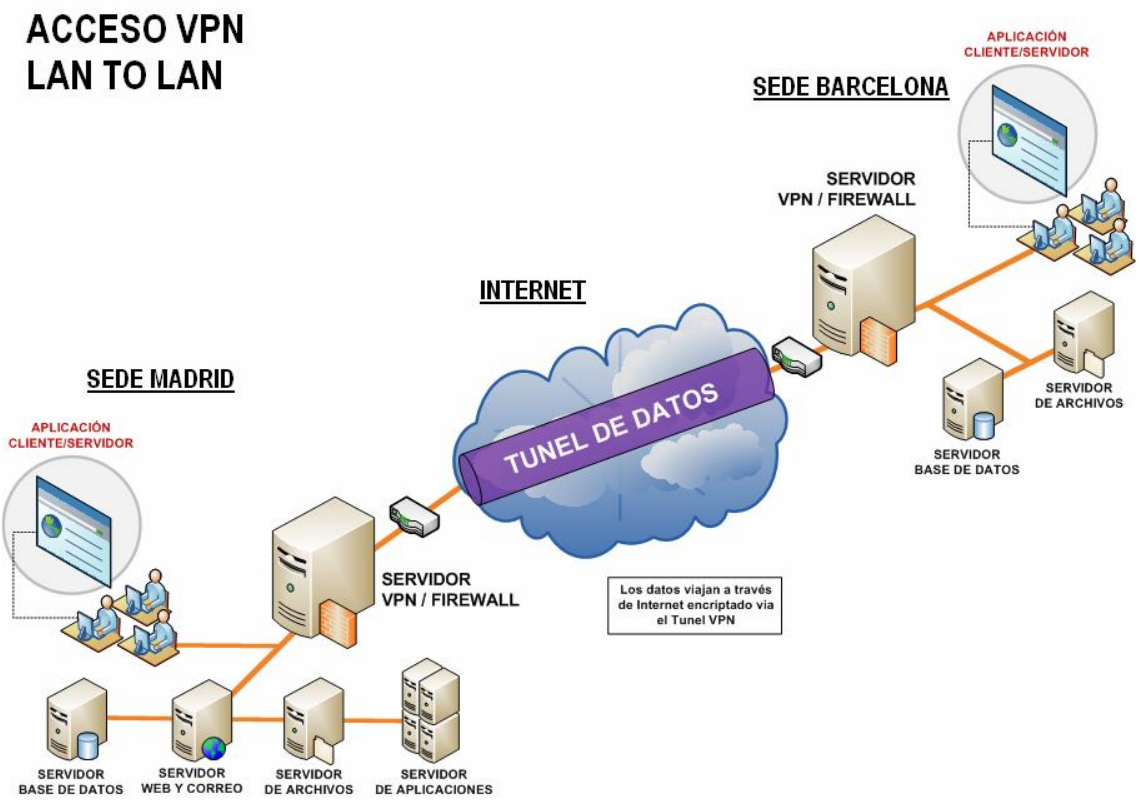


Figura 3: VPN de sitio a sitio

Tomás C. (2008). Ilustración de VPN LAN to LAN [Figura]. Recuperado de https://core.ac.uk/download/pdf/60416203.pdf

1.3.2.4. Protocolos Usados en VPN

- **Protocolo IPSec.**

  El protocolo de seguridad de protocolos en Internet (IPSec) proporciona las funciones de seguridad mejorada tales como algoritmos de encriptación más fuertes y más autenticación completa. El IPSec tiene dos modos de encriptación: túnel y transporte.

– Modo de transporte: IPSec cifra y autentica solo la carga útil real del paquete, y la información del encabezado permanece intacta.

– Modo de túnel: IPSec cifra y autentica todo el paquete. Después del cifrado, el paquete se encapsula para formar un nuevo paquete IP que tiene información de encabezado diferente.

También, todos los dispositivos deben utilizar una clave común o certificarla y deben tener configuración muy similar de las políticas de seguridad. (Cloud, s.f.)

IPSec es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados. (IBM®, 2010)

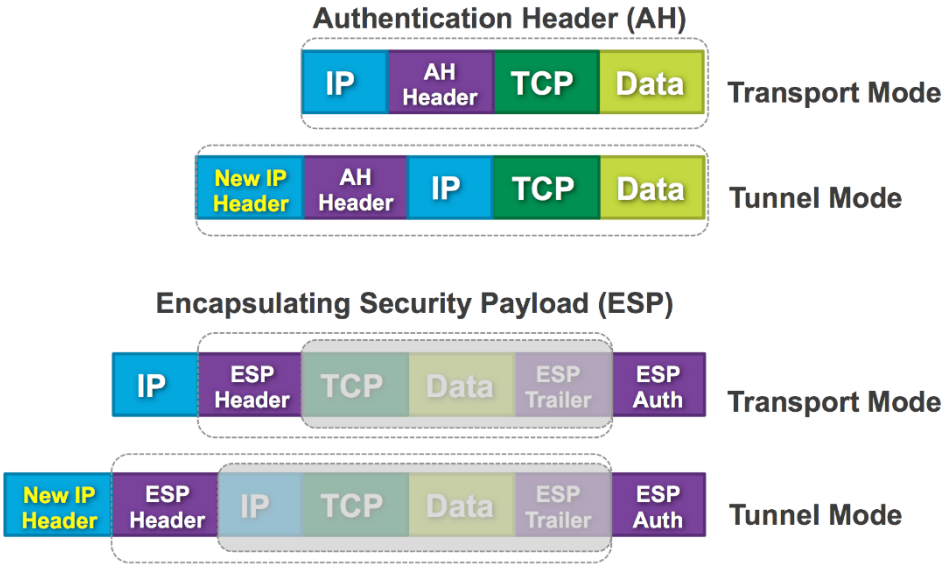


Figura 4: Modos de encriptación – IPSec

Marcin Latosiewicz (2017). Ilustración de Modo tunel y modo transporte [Figura]. Recuperado de https://community.cisco.com/t5/security-documents/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502

Protocolo PPTP/MPPE

El PPTP fue creado por el foro de PPTP, un consorcio que incluye US Robotics, Microsoft, 3COM, asciende, y ECI Telematics. El PPTP soporta el multi-protocol VPN, con 40-bit y el cifrado del 128-bit usando un protocolo llamado Microsoft Point-to-Point Encryption (MPPE). Es importante observar que el PPTP en sí mismo no proporciona la encripción de datos. (Cisco, 2006)

Protocolo L2TP

Es un protocolo de túnel utilizado para soportar la red virtual privada (VPN) o como parte de un servicio de entrega por ISPs. No provee ningún servicio de encriptación o confidencialidad por sí mismo. (VTNV Solutions Limited, s.f.)

El L2TP comúnmente llamado sobre el IPSec, esto proporciona la Seguridad del Protocolo IPSec sobre el Tunelización del protocolo Layer 2 Tunneling Protocol (L2TP). El L2TP es el producto de una sociedad entre los miembros del foro de PPTP, Cisco, y la Fuerza de tareas de ingeniería en Internet (IETF) (IETF). Utilizado sobre todo para los VPN de accesos remotos con los sistemas operativos del Windows 2000, puesto que el Windows 2000 proporciona a un cliente de IPSec y L2TP nativo. Los Proveedores de servicios de Internet pueden también proporcionar las conexiones L2TP para los usuarios de dial in, y después cifran ese tráfico con el IPSec entre su acceso-punta y el servidor de red de la oficina remota.

Protocolo SSL

SSL: (Secure Sockets Layer) traducido al español significa Capa de Conexiones Seguras. Es un protocolo que hace uso de certificados digitales para establecer comunicaciones seguras a través de Internet.

SSL es un protocolo diseñado para permitir que las aplicaciones puedan transmitir información de ida y de manera segura hacia atrás. Las aplicaciones que utilizan el protocolo Secure Sockets Layer sí sabe cómo dar y recibir claves de cifrado con otras aplicaciones, así como la manera de cifrar y descifrar los datos enviados entre los dos. (DigiCert® Inc, s.f.)

Protocolo TLS

TLS: es la siguiente generación del Certificado SSL; permite y garantiza el intercambio de datos en un entorno seguro y privado entre dos entes, el usuario y el servidor, mediante aplicaciones como HTTP, POP3, IMAP, SSH, SMTP o NNTP. Nos referimos al TLS como la evolución del SSL dado que está basado en éste último certificado y funciona de manera muy similar, básicamente: encripta la información compartida. (SW Hosting, 2014)

1.3.2.5. Cuadro comparativo de protocolos usados en una VPN

Para una implementación más segura de una VPN en la UNPRG antes debemos analizar los protocolos que existen, por ello a continuación presentamos un cuadro comparativo en donde exponemos las ventajas y desventajas de cada protocolo existente.

Tabla 2: Cuadro comparativo de protocolos usados en una VPN

	PTPP	**L2TP/IPSEC**	**SSTP**	**IKEV2**	**OPENVPN**
VENTAJAS	-Rápido en Data -Cliente estándar en casi todas las plataformas. -Fácil de preparar. - Soporta tunneling extremo a extremo y entre servidores	-Específicamente seguro. -Disponible en todos los dispositivos y sistemas operativos modernos. -Fácil de preparar. -No requiere software adicional. -Compatible con IP dedicada. -Buen Rendimiento. -Compatible con dispositivos NAT	-Tiene la capacidad de romper a través de la mayoría de los cortafuegos. -El nivel de seguridad depende de la contraseña secreta, pero generalmente es bastante seguro. -Totalmente integrado en el sistema operativo Windows. - Soporte por Microsoft	-Es Seguro: admite varias codificaciones como 3DES, AES, AES 256. -Equipado con soporte para dispositivos Blackberry. -Estable, especialmente cuando se reconectan después de perder conexiones o cambiar redes. -Fácil de preparar, al menos desde el lado del usuario final. Relativamente más rápido que L2TP, PPTP y SSTP.	-Muy fácil de instalar y usar -Ofrece un alto nivel de seguridad. -Altamente configurable y flexible. -Compatible con varios algoritmos de encriptación. -Gran apoyo comunitario
DESVENTAJAS	-En peligro debido a la NSA. -No es completamente seguro. -Protocolo desfasado.	-Más lento que otros OpenVPN. -Puede ser un problema si se utiliza en unos cortafuegos limitados. -No tiene puerto VPN aleatorio. -	-Debido a que los derechos de propiedad predeterminados son propiedad de Microsoft Corporation, no se puede considerar para la puerta trasera. -Solo funciona en plataformas puras de Windows.	-Soporte de plataforma limitado. -El puerto 500 UDP utilizado se bloquea fácilmente cuando se compara con soluciones basadas en SSL, como SSTP o OpenVPN. -No implementación de código abierto. -Complicado en la implementación de IKEv2 en el lado del servidor, puede causar varios problemas potenciales.	-Puede ser un poco complicado de preparar. -Requiere software de terceros. -El soporte para equipos de escritorio es excelente, pero en dispositivos móviles debe mejorarse.

Nota: Consideramos apropiado comparar los protocolos más usados en la última década.

1.3.2.6. Tipos de VPN software Basados en Open Source

1.3.2.6.1. SoftEther VPN

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

SoftEther VPN es de código abierto. Puede utilizar SoftEther para cualquier uso personal o comercial de forma gratuita.

Si tiene teléfonos inteligentes, tabletas o PC portátiles, la función del servidor L2TP / IPsec de SoftEther VPN le ayudará a establecer una VPN de acceso remoto desde su red local. El servidor L2TP VPN de SoftEther VPN es compatible con Windows, Mac, iOS y Android. (SoftEther , 2019)

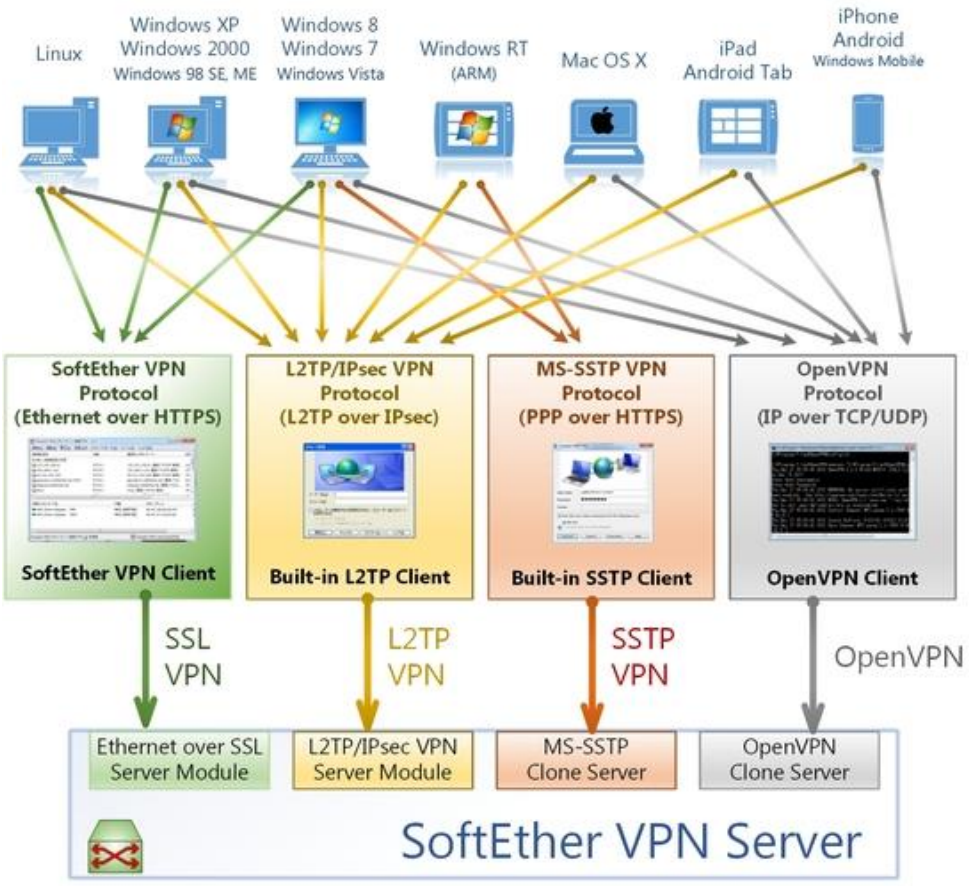


Figura 5: SoftEther VPN Server

Universidad de Tsukuba, Japón (2014). Ilustración de la arquitectura de Softether VPN [Figura]. Recuperado de https://www.softether.org/

Características de SoftEther VPN

- Software libre y de código abierto.
- Fácil de establecer VPN de acceso remoto y de sitio a sitio .
- SSL-VPN Tunneling en HTTPS para pasar a través de NAT y firewalls .
- Funciones revolucionarias de VPN sobre ICMP y VPN sobre DNS .
- Resistencia al firewall altamente restringido.
- Ethernet-bridging (L2) y enrutamiento IP (L3) a través de VPN.
- DNS dinámico y transversal NAT integrados para que no se requiera una dirección IP fija ni estática.
- AES de 256 bits y RSA de 4096 bits .
- Funciones de seguridad suficientes, como el registro y el túnel VPN interno del cortafuegos .
- Rendimiento de rendimiento de alta velocidad de clase 1 Gbps con poca memoria y uso de CPU.
- Windows, Linux, Mac, Android, iPhone, iPad y Windows Mobile son compatibles.
- SSL-VPN (HTTPS) y 6 protocolos principales de VPN (OpenVPN , IPsec , L2TP , MS-SSTP , L2TPv3 y EtherIP) son todos compatibles como protocolos de subsuelo de túneles VPN.
- La función de clonación OpenVPN admite clientes OpenVPN heredados.
- IPv4 / IPv6 de doble pila.
- Configure todos los ajustes en la GUI .
- Múltiples idiomas (inglés, japonés y chino simplificado).

- No hay pérdidas de memoria. Códigos estables de alta calidad, destinados a corridas a largo plazo. Siempre verificamos que no haya fugas de memoria o recursos antes de lanzar la compilación.
- Función de autenticación de usuario de dominio RADIUS / NT
- Función de autenticación de certificado RSA
- Inspección profunda de la función de registro de paquetes
- Función de lista de control de dirección IP de origen
- función de transferencia de syslog (SoftEther , 2019)

1.3.2.6.2. WireGuard

WireGuard es una VPN todavía rápido y moderno muy simple que utiliza el estado de la técnica de la criptografía. Está diseñado como una VPN de propósito general para ejecutarse en interfaces integradas y súper computadoras por igual, aptas para muchas circunstancias diferentes. Inicialmente lanzado para el kernel de Linux, ahora es multiplataforma y ampliamente implementable. Actualmente se encuentra en un gran desarrollo, pero ya puede considerarse como la solución VPN más segura, fácil de usar y más simple de la industria.

VENTAJAS

Sencillo y fácil de usar

WireGuard pretende ser tan fácil de configurar y desplegar como SSH. La conexión VPN se realiza simplemente mediante el intercambio de claves públicas muy simples, exactamente como el intercambio de claves SSH, y el resto es manejado de forma transparente por WireGuard.

Criptográficamente sonido

WireGuard utiliza criptografía de vanguardia, como el marco del protocolo de ruido , Curve25519 , ChaCha20 , Poly1305 , BLAKE2 , SipHash24 , HKDF y construcciones seguras de confianza.

Superficie de ataque mínima

WireGuard ha sido diseñado teniendo en cuenta la facilidad de implementación y la simplicidad. Está pensado para ser implementado fácilmente en muy pocas líneas de código y fácilmente auditable para vulnerabilidades de seguridad.

Alto rendimiento

Una combinación de primitivas criptográficas de velocidad extremadamente alta y el hecho de que WireGuard vive dentro del kernel de Linux significa que la red segura puede ser de muy alta velocidad. (wireguard, 2015)

DESVENTAJAS

- Las aplicaciones tienen bugs.
- Los desarrolladores avisan de que el código y el protocolo están en fase experimental.
- No hay soporte más allá de en Linux.
- No se ha lanzado ninguna versión que permita realizar un seguimiento CVE (vulnerabilidades y riesgos comunes) de ningún riesgo potencial para la seguridad.
- Muy pocos proveedores lo utilizan (debido a estos y otros motivos).

1.3.2.6.3. StrongSwan

StrongSwan es una implementación IPsec multiplataforma. El enfoque del proyecto se centra en los mecanismos de autenticación sólidos que utilizan certificados de claves

públicas X.509 y el almacenamiento seguro opcional de claves privadas y certificados en tarjetas inteligentes a través de una interfaz PKCS # 11 estandarizada y en TPM 2.0.

Características principales

- Se ejecuta en Linux 2.6, 3.xy 4.x kernels, Android, FreeBSD, OS X, iOS y Windows
- Implementa los protocolos de intercambio de claves IKEv1 e IKEv2 (RFC 7296)
- Soporte completamente probado de IPv6 IPsec túnel y conexiones de transporte
- Dirección IP dinámica y actualización de la interfaz con IKEv2 MOBIKE (RFC 4555)
- Inserción y eliminación automáticas de reglas de firewall basadas en políticas IPsec
- NAT-Trasversal a través de encapsulación UDP y puerto flotante (RFC 3947)
- IP virtuales estáticas y modos IKEv1 ModeConfig pull y push
- Grupo de direcciones IP virtuales gestionado por el daemon IKE o la base de datos SQL
- Autenticación de usuario IKEv2 EAP segura (EAP-SIM, EAP-AKA, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-MSCHAPv2, etc.)
- Retransmisión opcional de mensajes EAP al servidor AAA a través del complemento EAP-RADIUS
- Autenticación basada en certificados X.509 o claves previamente compartidas
- Uso de algoritmos de firma fuertes con *autenticación de firma en IKEv2*
- Gestión de CA (URI de OCSP y CRL, servidor LDAP predeterminado)
- Políticas potentes de IPsec basadas en comodines o CA intermedias

Desventajas

- StrongSwan en la configuración cliente/servidor no soportaba claves precompartidas y solo se soporta en las últimas versiones, lo cual obligaba al uso de certificados digitales X509.
- La instalación y configuración cliente/servidor como LAN a LAN de la solución es compleja.

1.3.2.6.4. OpenVPN

OpenVPN es una solución de VPN SSL de código abierto con todas las funciones que se adapta a una amplia gama de configuraciones, incluyendo acceso remoto, VPN de sitio a sitio, seguridad Wi-Fi y soluciones de acceso remoto a escala empresarial con equilibrio de carga, conmutación por error y multa. -granos controles de acceso.

OpenVPN implementa la extensión de red segura OSI layer 2 o 3 utilizando el protocolo SSL / TLS, admite métodos flexibles de autenticación de clientes basados en certificados, tarjetas inteligentes y / o autenticación de 2 factores, y permite políticas de control de acceso de usuarios o grupos específicos mediante el uso de reglas de firewall. aplicado a la interfaz virtual VPN. OpenVPN no es un proxy de aplicación web y no funciona a través de un navegador web.

VENTAJAS

- Las principales fortalezas de OpenVPN incluyen la portabilidad multiplataforma en la mayor parte del universo informático conocido, excelente estabilidad.
- OpenVPN admite el transporte IPv6 (OpenVPN a través de la red IPv6)
- OpenVPN puede hacer uso de OpenSSL o PolarSSL

- El modelo de seguridad de OpenVPN se basa en el uso de SSL / TLS para la autenticación de sesión y el protocolo ESP de IPSec para el transporte seguro de túneles a través de UDP.
- OpenVPN está construido para la portabilidad. En el momento de escribir este artículo, OpenVPN se ejecuta en Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X y Windows.
- OpenVPN es fácil de usar. En general, un túnel se puede crear y configurar con un solo comando (y sin los archivos de configuración necesarios)
- OpenVPN ha sido construido con un diseño fuertemente modular. Todo el cifrado es manejado por la biblioteca SSL, y toda la funcionalidad de tunelización IP se proporciona a través del controlador de red virtual TUN / TAP. (OpenVPN, 2015)

DESVENTAJAS

- No es compatible con IPSec, el estándar actual para soluciones VPN.
- OpenVPN realiza una conjunción de soluciones a nivel de capa 2, capa 3 y capa 7 las cuales no son un estándar de VPN.
- Hay pocos fabricantes de hardware que lo integran en sus soluciones, sin embargo al contarse con un sistema Linux, es implementable mediante software.

1.3.2.7. Cuadro Comparativo entre tipos de VPN Basados en Open Source

Tabla 3: Cuadro Comparativo entre tipos de VPN

	OpenVPN	StrongSwan	WireGuard	SoftEther
Protocolo	SSL-TLS	IPSec, IKEv2	SSH y Mosh	IPSec, OpenVPN, L2TPv3, SSL-VPN(https), MS-SSTP.
Autenticación	Autentifica los datos con certificados digitales y claves	Certificados y claves pre compartidas	Curve25519, ChaCha20 , Poly1305 , Claves pre compartidas	Encriptación con certificados digitales, IPSec/L2TP,Claves
Plataformas soportadas	Windows, Mac OSX, Linux, IOS, Android	Windows, Mac OSX, Linux, IOS, Android	Windows, Mac OSX, Linux	Windows, Mac OSX, Linux, IOS, Android
Idiomas	Inglés, Español, Francés, Ruso, Japonés	Ingles	Ingles	Inglés, Japonés y Chino
Actualización (Año)	2017	2018	2015	2019
Usuarios	2	1000+	--	10 000+
Puerto VPN alternativo	TCP 443 UDP 553	UDP 3947	UDP 7361	TCP 443,992,5555, 8888
Rendimiento	Depende de muchos factores, aunque, el uso de OpenVPN a través de UDP es generalmente más rápido que a través de TCP.	Fragmentación de mensajes (RFC 7383) para evitar problemas con la fragmentación IP	WireGuard vive en el interior del núcleo de Linux significa que las redes seguras puede ser muy alta velocidad	No hay pérdidas de memoria. Siempre se verifica que no hay memoria o de recursos fugas antes de la liberación de la construcción.

Nota: Hemos considerado los software VPN antes descritos para hacer esta comparación.

1.3.3. Metodologías para implementar proyectos de redes

1.3.3.1. Top-Down Network Design

Es una metodología que propone cuatro Fases, para el diseño de redes

I. Fase de Identificación de Necesidades y Objetivos de los Clientes

En esta fase se identificará los objetivos y restricciones del negocio, y los objetivos y restricciones técnicos del cliente.

- Análisis de los Objetivos Técnicos y sus Restricciones
- Caracterización de la Red Existente
- Caracterización del tráfico de la red

II. Fase de Diseño Lógico

En esta fase se diseñará la topología de red, el modelo de direccionamiento y nombramiento, y se seleccionará los protocolos de bridging, switching y routing para los dispositivos de interconexión. El diseño lógico también incluye la seguridad y administración de la red.

- Diseño de la Topología de red
- Selección de Protocolos de Switching y Routing
- Desarrollo de estrategias de seguridad de la red

III. Fase de Diseño Físico

Esta fase implica en seleccionar las tecnologías y dispositivos específicos que darán satisfacción a los requerimientos técnicos de acuerdo al diseño lógico propuesto (LAN / WAN)

1. Selección de Tecnologías y dispositivos para la red del Campus

- Diseño del Cableado Estructurado, Switch, Router, otros

2. Selección de Tecnologías y dispositivos para la red Empresarial

- Tecnología de acceso remoto (VPN, Línea dedicada, Acceso satelital, otros)

IV. Fase de Prueba, Optimización y Documentación

Cada sistema es diferente; la selección de métodos y herramientas de prueba correctos, requiere creatividad, ingeniosidad y un completo entendimiento del sistema a ser evaluado. Implementación de un Plan de Pruebas

- Prueba del Diseño de la red
- Optimización del Diseño de la red
- Documentación de la red

1.3.3.2. Metodología del desarrollo con Cisco

Cisco, el mayor fabricante de equipos de red, describe las múltiples fases por las que una red atraviesa utilizando el llamado ciclo de vida de redes PDIOO (Planificación –Diseño – Implementación –Operación –Optimización).

- Fase de planificación: los requerimientos detallados de red son identificados y la red existente es revisada.
- Fase de diseño: la red es diseñada de acuerdo a los requerimientos iniciales y datos adicionales recogidos durante el análisis de la red existente. El diseño es refinado con el cliente.
- Fase de implementación: la red es construida de acuerdo al diseño aprobado
- Fase de operación: la red es puesta en operación y es monitoreada. Esta fase es la prueba máxima del diseño.
- Fase de optimización: durante esta fase, los errores son detectados y corregidos, sea antes que los problemas surjan o, si no se encuentran problemas, después de que ocurra una falla. Si existen demasiados problemas, puede ser necesario rediseñar la red. (Cisco Services., 2006)

1.3.3.3. Metodología desarrollada por el Instituto Nacional De Estadística E Informática (INEI)

Para llevar adelante los Proyectos, el INEI ha adoptado un Marco Metodológico Único, esto nos permitirá el desarrollo del Diseño de una Red Informática.

El Marco Metodológico para un Proyecto constará de cuatro etapas siendo estas las siguientes:

ETAPAS

- Organización.
- Análisis.
- Desarrollo.
- Implementación.

A. ETAPA DE ORGANIZACIÓN

La Etapa de Organización es la primera Etapa del Marco Metodológico, en ésta se llevará adelante las siguientes actividades:

Modelamiento del Requerimiento

Se propone las Redes LAN/WAN ya que para la LAN abarca un Radio local y se sugiere la WAN ya las sucursales de las otras ciudades.

B. ETAPA DE ANALISIS

En esta etapa se analizará los recursos de la red y su estructura; Descripción de las estrategias para la integrar todas las áreas a la red.

C. ETAPA DE DESARROLLO

En esta etapa se tiene en cuenta los siguientes pasos.

- Diseño
- Diseño lógico

D. ETAPA DE IMPLEMENTACION

Comprende toda la instalación en la empresa.

- Cableado

1.3.3.4. Metodología elaborada por James Mccabe

- FASE I. ANÁLISIS DE LA SITUACIÓN ACTUAL.

Para llevar a cabo esta fase se debe realizar un reconocimiento de cada uno de los campos involucrados, permitiendo observar cuales eran las deficiencias y los problemas que presentaba la plataforma de comunicación proporcionada por la compañía de telecomunicaciones.

- FASE II. DETERMINACIÓN DE LOS REQUERIMIENTOS

Para dar comienzo a esta fase se debe estudiar tres tipos de interconexión de redes: fibra óptica, radio enlaces e interconexión satelital; realizar un estudio minucioso para observar cual se ajustaba más a los requerimientos exigidos por la empresa.

- FASE III. ANÁLISIS DE LAS NECESIDADES DEL SISTEMA

Para realizar el diseño de una red inalámbrica resulta indispensable llevar a cabo una serie de estudios de la ubicación de los equipos, ancho de banda, la frecuencia para el nuevo enlace y la potencia que deben poseer los equipos que se usaran.

Para este proyecto de tesis se utilizará una mezcla de todas las metodologías explicadas anteriormente, la cual nos ayudarán a completar de manera exitosa los objetivos específicos.

1.3.4. Juicio de expertos

El juicio de expertos es un método de validación útil para verificar la fiabilidad de una investigación que se define como "una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones" (Escobar-Pérez y Cuervo-Martínez, 2008:29).

Es aquí donde la tarea del experto se convierte en una labor fundamental para eliminar aspectos irrelevantes, incorporar los que son imprescindibles y/o modificar aquellos que lo requieran.

1.3.4.1. Criterios para la selección de expertos

En cuanto a los procedimientos de elección de los expertos, los autores indican una diversidad que incluye desde los que no implican ningún filtro de selección, como en los casos de afinidad o cercanía entre el experto y el investigador, hasta los que utilizan una serie de criterios estructurados como son:

- Biograma: Consiste en elaborar una biografía del experto en función de sus respuestas sobre aspectos de su trayectoria como, por ejemplo, años de experiencia y formación, investigaciones o acciones formativas, conocimiento del objeto de estudio, a partir de los cuales se infiere su adecuación y pertinencia para su actividad de experto.
- Coeficiente de Competencia experta: se inicia con las personas que inicialmente se han considerado expertos para que con su opinión y autovaloración indiquen su nivel sobre el conocimiento acerca del objeto de investigación, así como de las fuentes que les permiten argumentar y justificar dicho nivel.

1.3.5. Norma ISO 27001

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (isotools.org, s.f.)

Hoy en día, la seguridad de la información está constantemente en las noticias con el robo de identidad, las infracciones en las empresas los registros financieros y las amenazas de terrorismo cibernético. Un sistema de gestión de seguridad de la información (SGSI) es un enfoque sistemático para la gestión de la información confidencial de la empresa para que siga siendo seguro. Abarca las personas, procesos y sistemas de TI. (isaca.org, 2014)

Figura 6: ISO 27001

IndiaMART (2014). Ilustración de ISO 27001 Certification [Figura]. Recuperado de https://www.indiamart.com/proddetail/iso-27001-certification-20072601733.html

2019

CAPÍTULO II

MÉTODOS Y MATERIALES

2.1. Tipo y diseño de la investigación

2.1.2. Tipo de investigación: Investigación Aplicada

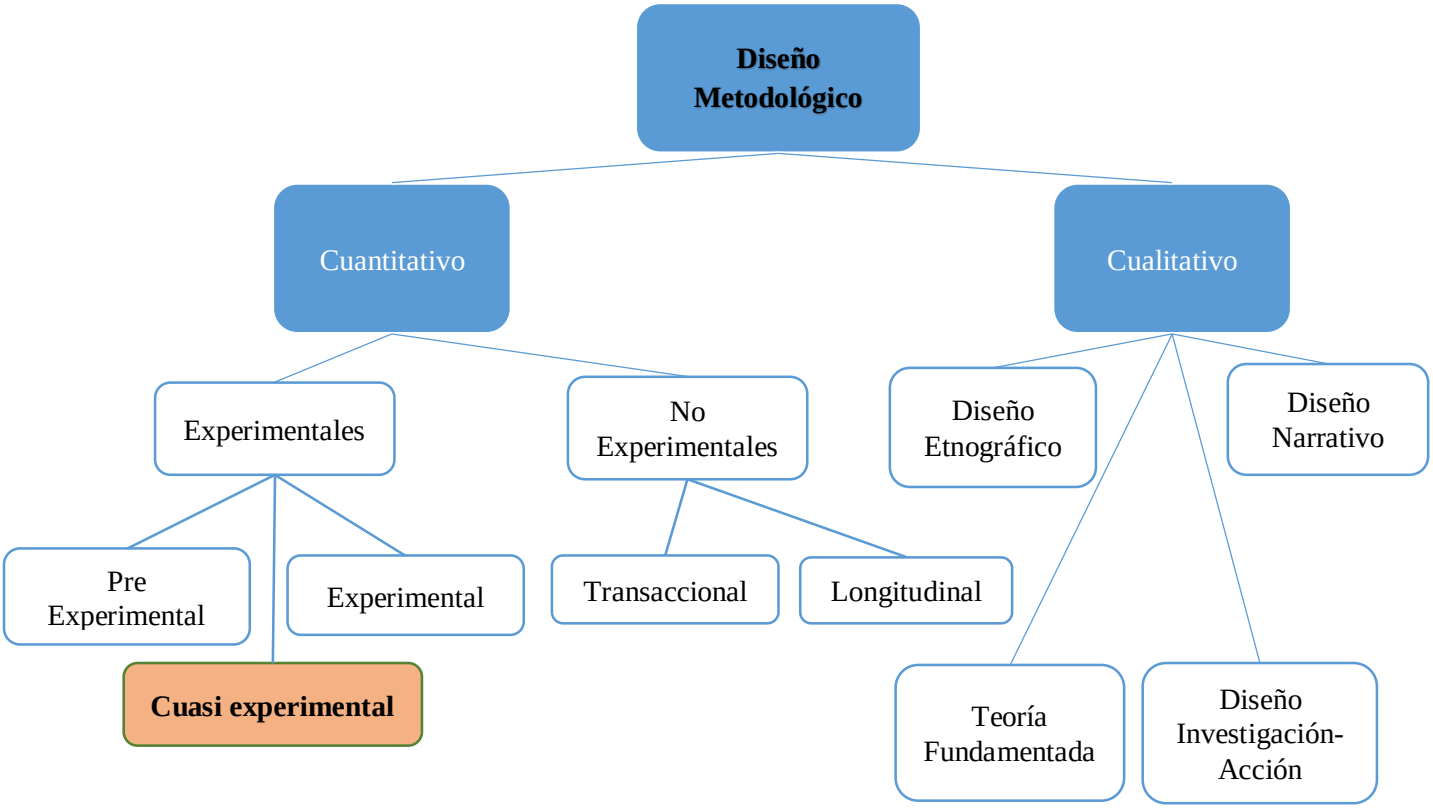
La investigación aplicada es un tipo de investigación en la que el investigador se centra en la resolución del problema en un contexto determinado para dar respuestas a preguntas específicas. Está basado en la resolución práctica del problema.

Para Murillo (2008), la investigación aplicada recibe el nombre de "investigación práctica o empírica", que se caracteriza porque busca la aplicación o utilización de los conocimientos adquiridos, a la vez que se adquieren otros, después de implementar y sistematizar la práctica basada en investigación. El uso del conocimiento y los resultados de investigación que da como resultado una forma rigurosa, organizada y sistemática de conocer la realidad.

2.1.3. Diseño de la Investigación: Cuasi experimental

El diseño de investigación es un conjunto de métodos y procedimientos utilizados al coleccionar y analizar medidas de las variables especificadas en la investigación del problema de investigación. Y esta se clasifica de la siguiente manera:

Tabla 4: Tipo de Diseño



El diseño de investigación con el que trabajaremos en el presente será el diseño cuasi experimental

El diseño es **cuasi experimental**, que estudia las relaciones causa – efecto, es decir, que se pretende estudiar el impacto de los tratamientos y los procesos de cambio, en situaciones donde los sujetos o unidades de observación no han sido asignados de acuerdo con un criterio aleatorio.

El método cuasi experimental es particularmente útil para estudiar problemas en los cuales no se puede tener control absoluto de las situaciones, pero se pretende tener el mayor control posible, aun cuando se estén usando grupos ya formados. Es decir, el cuasi experimento se utiliza cuando no es posible realizar la selección aleatoria de los sujetos participantes en dichos estudios. Por ello, una característica de los cuasi experimentos es el incluir "grupos intactos", es decir, grupos ya constituidos.

2.1.3.1. Tipos de diseños cuasi experimentales

- Experimentos naturales: Son los experimentos que se desarrollan en la población sin que medie ningún tipo de intervención intencionada. La intervención se da de forma natural o circunstancial y luego se evalúa la presencia de la enfermedad con el fin de evaluar el efecto de la intervención no intencionada.
- Estudios con controles históricos: Este estudio consiste en comparar que un grupo de pacientes que reciben una intervención o tratamiento con un grupo que había sido tratado con otro tipo de intervención en el pasado.
- Estudios post-intervención: Es una forma de evaluar una intervención y consiste en realizar observaciones posteriores a la utilización de una medida de intervención. Tiene la limitación de no tener información previa sobre el conocimiento del tema por parte de los participantes.
- Estudios antes/después: Este estudio establece una medición previa a la intervención y otra posterior. Además, puede incluir un grupo de comparación que no reciba la intervención y que se evalúa también antes y después con el fin de medir otras variables externas que cambien el efecto esperado por razones distintas a la intervención. (Cardona, 2003)

2.2. Diseño Metodológico

2.2.2. Diseño de Contrastación de Hipótesis

Teniendo como objetivo: Mejorar la gestión de aplicaciones de Intranet con la implementación de una VPN Open Source en la Universidad Nacional Pedro Ruiz Gallo, donde se medirá el impacto de la variable independiente: Implementación de una VPN con Open Source, sobre la variable dependiente: gestión de las aplicaciones de Intranet, midiendo y comparando los resultados obtenidos. Por ser este un diseño cuasi experimental, el diseño de contrastación de la hipótesis con pre prueba y pos prueba se formula de la siguiente manera:

$$Ge: O_1 \; X \; O_2$$

Dónde:

Ge: Grupo Experimental evalúa a los usuarios de las oficinas más críticas.

O_1: La observación 1 evalúa la Gestión actual a nivel administrativo de las aplicaciones de intranet.

X: Representa la implementación de una Red Privada Virtual con Open Source.

O_2: La observación 2 evalúa la gestión de las aplicaciones de intranet enfocando aspectos de eficiencia y corroborando la tesis con ayuda de software como t de student.

2.2.3. Definición y Operacionalizacion de Variables

Dónde:

- **Variable Independiente**

  X: Implementación de una VPN con Open Source.

- **Variable Dependiente**

  Y: Gestión de las aplicaciones de Intranet.

Tabla 5: Items a evaluar

	Dimensión	**Descripción**	**Indicadores**	**Tipo**
Y: Gestión de aplicaciones de intranet	Productividad	Se ampliará la gestión de labores académicas y administrativas, ya que los usuarios podrán acceder desde cualquier lugar y continuar con sus actividades	Tareas Realizadas	Cuantitativa
	Disponibilidad	Para que los empleados puedan acceder a archivos, aplicaciones empresariales y otros recursos en la red a través de un acceso remoto	Tiempo de respuesta	Cuantitativa
			Costo en viáticos	Cuantitativa
	Soporte	El software que se utilizará es libre y multiplataforma con una variedad de dispositivos	Dispositivos soportados	Cuantitativa
			Costo de implementación	Cuantitativa
	Seguridad	Se utilizará una encriptación, de modo que los datos no puedan ser capturados.	Encriptación de datos y nivel de seguridad	Cualitativa
			Numero de accesos no autorizados	Cuantitativa

Tabla 6: Formula para cada indicador

Indicadores	**Formula**
Tareas Realizadas(TR)	TR=Tareas asignadas – Tareas no realizadas.
Tiempo de Respuesta (TDR)	TDR=Tiempo de conexión VPN + Tiempo de ingreso a la aplicación de intranet
Costo en viáticos (CV)	CV=El costo depende de la ubicación de cada trabajador
Sistemas operativos soportados (SOS)	SOS=Cantidad de sistemas operativos soportados por softether
Costo de implementación (CI)	CI=Hardware + Software + Servicios
Números de accesos no autorizados (NAN)	NAN=Intentos de conexión – Números de accesos correctos.

Descripción:

- **Tares Realizadas**: Para encontrar las tareas realizadas antes de la implementación de la VPN se restarían las tareas no realizadas por algún motivo (Huelga, corte de luz, desastre natural, falta de tiempo, capacitación, etc) al total de tareas asignadas. Sin embargo, para encontrar las tareas realizadas después de haber implementado la VPN, tomaríamos el total de tareas asignadas, le restaríamos las tareas no realizadas en la oficina del trabajador y le sumaríamos las tareas realizadas con la ayuda de la VPN.

  Por ejemplo:

  A un trabajador del área de contabilidad se le ha asignado un total de 70 tareas en un mes de las cuales el trabajador no logró realizar 20 tareas. Mientras que con la VPN el trabajador cómodamente pudo haber echo 18 tareas, lo que representaría un 25.7% más que en un escenario sin VPN.

  En el siguiente cuadro nos proporciona el total de tareas realizadas antes de la implementación de la VPN y después de la implementación de la VPN.

Tabla 7: Tareas Realizadas en 1 mes

Antes de la VPN	Después de la VPN
TR = 70 - 20 = 50	TR = 70 - 20 + 18 = 68

Figura 7: Ejemplo de tareas realizadas

- **Tiempo de Respuesta**: Para encontrar el tiempo de respuesta antes de la implementación de la VPN se sumaría el tiempo que le toma al trabajador administrativo llegar desde su hogar u otra ubicación hasta la Universidad más el tiempo que le tomaría ingresar a su equipo y finalmente sumarle el tiempo que le tomaría acceder a la aplicación de intranet.

  En cambio, para encontrar el tiempo de respuesta después de haber implementado la VPN, sumaríamos el tiempo que le tomaría al trabajador conectarse a la VPN con el tiempo que le tomaría acceder a la aplicación de intranet.

  Por ejemplo:

  A un ingeniero encargado de la habilitación de módulos del programa SIGA que se encuentra en una capacitación en la ciudad de Lima le solicitan que habilite 5 módulos en el programa, por lo que sin contar los pasajes tendría que viajar desde Lima a Chiclayo (lo que le tomaría un pasaje rápido en avión unas 2 horas no por el viaje en si, sino por el tiempo en el aeropuerto), luego de Chiclayo a Lambayeque (30 minutos en combi) para llegar a la universidad e ingresar a su equipo e ingresar al programa SIGA. Mientras que con la VPN el ingeniero cómodamente pudo ingresar desde su laptop con una conexión a internet, conectarse a la VPN (2 minutos) e ingresar a la aplicación SIGA.

Tabla 8: Tiempo de respuesta en una capacitación

Antes de la VPN	Después de la VPN
TDR = 120 + 30 = 150	TDR = 2

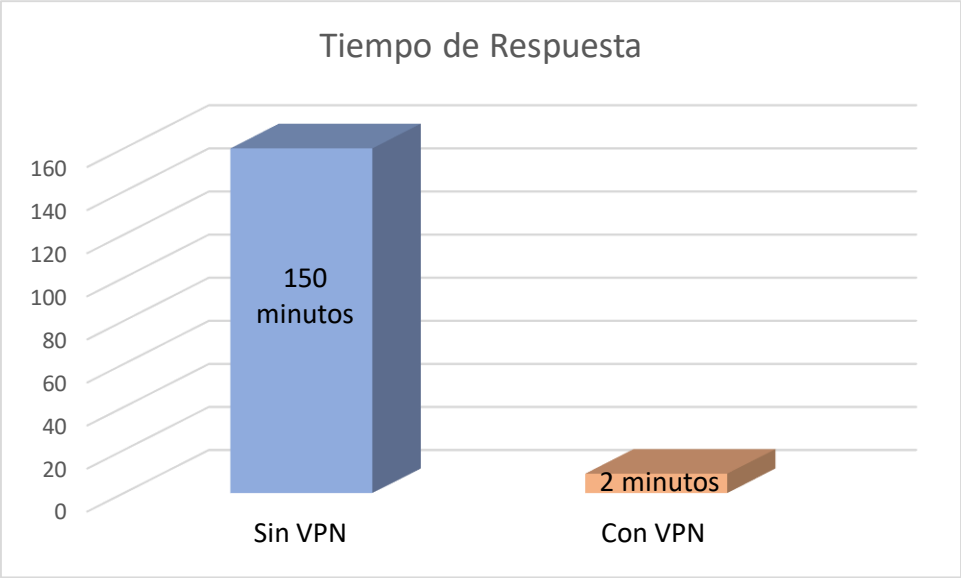


Figura 8: Ejemplo de tiempo de respuesta

- **Costo en viáticos**: Para encontrar el costo en viáticos antes de la implementación de la VPN se sumaría todo el dinero en pasajes que gastaría el trabajador administrativo (que dependiendo de la situación tendría que ser costeado por la Universidad) llegar desde su hogar u otra ubicación hacia la Universidad.

  En cambio, para encontrar el costo en viáticos después de haber implementado la VPN, no es necesario hacer ninguna sumatoria, puesto que su costo es 0.

  Por ejemplo:

  Tomando el ejemplo anterior, el costo de un pasaje en avión desde Lima a Chiclayo está cerca de 150 soles aproximadamente (dependiendo la fecha), luego de Chiclayo a Lambayeque 1.5 o 2 soles (dependiendo si es en combi o colectivo) para llegar a la universidad e ingresar a su equipo e ingresar al programa SIGA. Mientras que con la VPN no existiría ningún costo por pasajes, puesto que la VPN funciona desde cualquier lugar con conexión a internet.

- **Sistemas operativos soportados**: Este indicador no necesita mayor cálculo, puesto que en la actualidad los sistemas operativos que soporta la VPN son Windows, MacOS X, Android y iOS.
- **Costo de Implementación**: El costo de implementación antes de la tesis sería nulo, puesto que no existía una VPN, sino que se hacía uso de software sin licenciar el cual no era administrado por personal de informática de la universidad.

  Y para encontrar el costo de implementación de la VPN en la actualidad basta con sumar el costo de hardware, más el costo del software (costo 0) más el costo de los servicios a brindar.
- **Números de accesos no autorizados**: Para encontrar el número de accesos no autorizados hacia la VPN tendríamos que restar del número de intentos de conexión la cantidad de ingresos exitosos.

2.3. Técnicas y Materiales

2.3.2. Técnicas

Las técnicas usadas para el desarrollo del presente trabajo de titulación fueron las siguientes:

Observación

Se realizó en primer término una observación de campo participativa con un método natural, a fin de determinar a través de fuentes primarias la situación existente.

Entrevista

Para la entrevista que fue realizada en las diferentes oficinas de la universidad, antes fueron preparados con un bloque de preguntas que estas a su vez fueron analizadas y estudiadas previamente, y fueron enfocadas a investigar el origen del problema en la universidad, estas preguntas las podemos encontrar en el anexo N°2

2.3.3. Equipos a utilizar

2.3.3.1. Hardware a utilizar

Para llevar a cabo la tarea de implementación de la red privada virtual debemos tener en cuenta los equipos que se requerirán para que la VPN funcione sin problema alguno.

Estos equipos son:

Servidores

Actualmente está compuesta con 10 servidores físicos y los demás son servidores virtualizados, dos servidores configurados con Active Directory de Windows Server 2000 en donde se encuentran los usuarios de dominio y políticas de acceso de cada usuario que les permite acceder a los diferentes recursos de red disponibles en la universidad.

Servidor VPN

Para la implementación de la VPN se hará uso del servidor HP ProLiant DL360 Gen9 que actualmente posee el data center de la UNPRG, en el cual se encuentran servicios como Controlador de dominio,DHCP,DNS,FTP,Telefonia IP,entre otros, que estan distribuidos en particiones de disco duro para su correcto funcionamineto de los cuales algunos estan virtualizados con VMware ESXi para asi aprovechar los recursos del servidor fisico. Además de el servidor HP ProLiant DL580 Gen7 (donde se encuentra el controlador de dominio, el servidor DHCP, entre otros) el cual nos servirá como respaldo para la implementación de la VPN.

Servidor Firewall

En el data center actualmente dispone de dos firewall, uno para la parte WAN y otro para la parte LAN que protege contra los ataques y accesos no autorizados a la información de la universidad, así como también controla el trafico entrante y saliente hacia la internet.

Sin embargo, un firewall no protege por si mismo la red corporativa de las amenazas de ataque presente en internet, dado que información importante como nombres de usuarios, contraseñas, direcciones de servidores, pueden ser vulnerados, ya que la información no es del todo cifrada. Por lo que en una VPN se habilita un túnel privado, a través del uso de algoritmos de encriptamiento, lo que posibilita el uso de un medio público y compartido como internet para la transmisión de datos seguros.

Router

Para establecer conexión a internet en la universidad este contrata a un proveedor de servicios, el cual brinda un ancho de bnada de 1 Gbps aproximadamente, lo cual incorpora un Router Cisco, el cual es el enlace entre internet y la red LAN.

Adicionalmente la universidad dispone de un enlace con otra proveedora de servicios con una cantidad de ancho de banda reducida y se ha establecido la conexión interna, el servicio se usa en caso de emergencias para los servicios más críticos.

UPS

En la parte de suministro eléctrico, el data center cuenta con respaldo de UPS y Baterías de energía, así como también de un generador de energía, que entra en funcionamiento cuando se presentan interrupciones de energía. Cabe resaltar que los servidores deben estar siempre en funcionamiento para dar servicio a los demás.

Laptop, PC y Smartphone

Dispositivos finales de salida que serán usados para realizar pruebas de conexión con el servidor VPN, logrando así que podamos experimentar y resolver posibles errores en nuestra implementación.

2.3.3.2. Software a utilizar

SoftEther

Figura 9: SoftEther VPN

Universidad de Tsukuba, Japón (2014). Ilustración de logotipo de Softether VPN [Figura]. Recuperado de https://www.softether.org/

Como ya lo describimos en la página número 30, teniendo en cuenta las ventajas que ofrece esta aplicación, concluimos que es la más adecuada para implementar soluciones VPN, pues es un software gratuito de código abierto y que además se mantiene en constantes actualizaciones.

VirtualBox

Figura 10: VirtualBox

Oracle (2007). Ilustración de logotipo de VirtualBox [Figura]. Recuperado de https://www.virtualbox.org/

VirtualBox es un potente producto de virtualización x86 y AMD64 / Intel64 para empresas y para uso doméstico. Actualmente VirtualBox se ejecuta en hosts Windows. Linux, Macintosh y Solaris, además es la única solución profesional que está disponible gratuitamente como software de código abierto según los términos de la Licencia Pública General de GNU (GPL)

VMware vSphere 6.7

Figura 11: vmware vSphere

Vmware vSphere(2019). Ilustración de logotipo de vmware vSphere [Figura]. Recuperado de https://neuronet.cl/producto/licencia-vmware-vsphere-chile/

VMware Vsphere es la solución por excelencia para virtualizar centros de datos (Data Center) y aprovechando que la universidad cuenta con licencia para este software, el costo seguiría siendo 0.

Este software lo utilizaremos para virtualizar el sistema operativo (CentOS 7) en dónde se ejecutará el servidor de la red privada virtual.

WireShark

Figura 12: WireShark

Wireshark Foundation(1999). Ilustración de logotipo de Wireshark [Figura]. Recuperado de https://www.wireshark.org/

Wireshark es un analizador de protocolos open-source diseñado por Gerald Combs y que actualmente está disponible para plataformas Windows y Unix. Esta aplicación está dedicada para el análisis de tráfico y la resolución de problemas en red.

Este analizador de paquetes nos será útil para realizar pruebas y evidenciar que no se visualizan las claves y que estas están debidamente encriptadas.

CentOS 7

Figura 13: Centos 7

The CentOS Project(2018). Ilustración de logotipo de Centos 7 [Figura]. Recuperado de https://www.centos.org/

Centos 7 es un sistema operativo de software libre y código abierto basado en la distribución Linux Red Hat Enterprise Linux (RHEL). Lo que llama la atención es que esta versión es compatible con Microsoft Active Directory, lo cual nos permite trabajar con facilidad en entornos heterogéneos.

Windows 7 a +

Figura 14: Windows 10

Microsoft Corp.(2017). Ilustración de logotipo de Windows 10[Figura]. Recuperado de https://www.microsoft.com/

Un sistema operativo que todos conocemos, nos ayudará a instalar los programas en un entorno gráfico. Los programas son compatibles a partir de windows 7 en adelante.

PfSense

PfSense es una distribución personalizada adaptado para su uso como Firewall y Router. Se caracteriza por ser de código abierto, puede ser instalado en una gran variedad de ordenadores, y además cuenta con una interfaz web sencilla para su configuración.

Figura 15: PfSense

PfSense.org.(2017). Ilustración de logotipo de PfSense[Figura]. Recuperado de https://www.pfsense.org/

2.4. Corroboración de Hipótesis

Como ya explicamos en la base teórica el método para la corroboración de hipótesis que utilizaremos será el juicio de expertos. Método que a continuación describiremos y detallaremos los pasos a seguir para hacer un buen uso de esta.

2.4.2. Métodos para la obtención de juicio de expertos

Las formas de poner en acción la estrategia del juicio de experto son diversas, y podemos hacerlo desde propuestas muy poco estructuradas, hasta otras que impliquen un alto nivel de estructuración.

Algunas de estas propuestas son:

- Agregación individual de los expertos, que consiste en obtener la información de manera individual de cada uno de ellos, sin que estos se encuentren en contacto.
- Método Delphi, en el cual se recoge la opinión de los expertos de forma individual y anónima, devolviéndoles la propuesta de conjunto para su revisión y acuerdo, una leve dispersión llevará a afirmar que se ha llegado a un acuerdo.
- Técnica grupal nominal, los expertos aportan la información de manera individual, y después de forma grupal presencial se llega a un acuerdo.
- Método de consenso, donde de forma grupal y conjuntamente, los expertos seleccionados llegan a conseguir un acuerdo.

En la fase final del proceso de consulta a los expertos, se elaboran las conclusiones del juicio que serán utilizadas para la descripción en términos de validez y fiabilidad del instrumento de medición, sin desestimar la presencia de variables individuales como la personalidad o las habilidades sociales de los jueces que pueden generar sesgos a favor de uno o varios aspectos del mismo (Escobar Pérez, 2008).

2.4.3. Procedimiento para realizar el juicio de expertos

1. Definir el objetivo del juicio de expertos. En este apartado los investigadores deben tener clara la finalidad del juicio, ya que puede utilizarse con diferentes objetivos:

- Establecer la equivalencia semántica de una prueba que se encuentra validada en otro idioma
- Evaluar la adaptación cultural, es decir, el objetivo de los jueces es evaluar si los ítems de la prueba miden el mismo constructo en una cultura distinta; así por ejemplo, los ítems que midan agresividad en una prueba validada en el Tibet, pueden no estar midiendo lo mismo en Alemania
- Validar contenido en una prueba diseñada por un grupo de investigadores.

2. Selección de los jueces. Para ello han de tomarse en cuenta los criterios especificados anteriormente para la selección, considerando la formación académica de los expertos, su experiencia y reconocimiento en la comunidad. Se propone un mínimo de cinco jueces, dos de los cuales deben ser expertos en medición y evaluación, y para el caso de traducciones y adaptaciones de pruebas, se requiere por lo menos un experto en lingüística.

3. Explicitar tanto las dimensiones como los indicadores que está midiendo cada uno de los ítems de la prueba. Esto le permitirá al juez evaluar la relevancia, la suficiencia y la pertinencia del ítem. No hay que dar por sentado que el juez únicamente con la

descripción del constructo a medir pueda identificarlo claramente, ya que como se mencionó anteriormente, es posible que existan diferentes definiciones de un mismo constructo.

4. Especificar el objetivo de la prueba. El autor debe proporcionar a los jueces la información relacionada con el uso de la prueba, es decir, para que van a ser utilizados los puntajes obtenidos a partir de esta. Esto aumenta la contextualización del juez respecto a la prueba, incrementando a su vez el nivel de especificidad de la evaluación; ya que la validez de los ítems está directamente relacionada con su utilización, por ejemplo, para hacer un diagnóstico o un tamizaje, o evaluar desempeño, entre otros.

6. Diseño de planillas. La planilla se debe diseñar de acuerdo con los objetivos de la evaluación. En el anexo N°3 se colocará la planilla que utilizaremos para la elaboración del juicio de expertos en esta tesis.

7. Concordancia entre jueces. La información que proporcione cada experto les servirá para que puedan llegar a un consenso, y validar la propuesta.

8. Elaboración de las conclusiones del juicio. De acuerdo con lo acordado por los expertos se verá la manera de aplicar o modificar la propuesta planteada.

2019

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. Desarrollo de la metodología propuesta

Metodología Empleada para el Diseño e Implementación de la VPN

Dada las características y objetivos planteados en esta investigación, es necesario definir una metodología que indique las fases o pasos a seguir, en la búsqueda del alcance de dichos objetivos específicos. En tal sentido consideramos seleccionar según las metodologías descritas anteriormente, una metodología mixta con la finalidad de lograr los objetivos de la presente investigación.

A continuación, un cuadro resumen de la metodología propuesta por los autores:

Tabla 9: Desarrollo de la Metodología Propuesta

Fase	Descripción
1	Realizar un estudio y descripción de la red actual en la UNPRG
2	Determinar los requerimientos necesarios para la implementación de la VPN
3	Diseñar la topología física y lógica
4	Elaborar el presupuesto de los equipos que se requerirán
5	Implementar una VPN para optimizar la gestión de Aplicaciones de la intranet de la UNPRG
6	Demostrar con herramientas de testeo la seguridad e integridad de los datos que viajan por la VPN

3.1.2. Realizar un estudio y descripción de la red actual en la UNPRG

3.1.2.1. Técnicas usadas

En esta primera etapa de investigación, se realizó una observación a fondo de la situación actual de la universidad, se aplicaron entrevistas (como se muestra en el Anexo N°2) a los diferentes trabajadores administrativos que laboran en la universidad para identificar y enfocar a los usuarios más críticos que requieran acceso remoto a la intranet , así como también conocer la situación actual de la red, tales como los sistemas y aplicativos que son utilizados en las diferentes oficinas administrativas y los servicios que requieren para completar ciertas tareas (servicios de internet, correo, telefonía IP, entre otros).

3.1.2.2. Situación Actual

Pues bien, como sabemos actualmente en la UNPRG, algunos trabajadores administrativos (rectorado, vicerrectorado, asuntos académicos, red telemática,

contabilidad general, etc…), tienen la necesidad de utilizar las aplicaciones de gestión administrativa para sus actividades funcionales diarias, sin embargo no siempre el usuario trabajador de la universidad se encuentra en su oficina de trabajo, debido a que el personal se encuentra participando de comisiones de servicio, capacitaciones, o también por eventos extraordinarios como paros administrativos, tomas de universidad, licencias laborales (eventuales), etc. Esto requiere de una alternativa de conectividad empresarial a estas aplicaciones críticas que retardan la productividad de cada dependencia. Estas aplicaciones críticas comprenden desde sistemas académicos (Actas virtuales en su gestión administrativa, GestAc, Presys, SIGA académico de enfermería – FE, SIBI), administración de servidores(DNS, DHCP, FTP, telefonía IP, cámaras ip, entre otros), equipos cisco (Switchs, Routers, Access Points) Equipos de seguridad (Firewalls,WAF), sistemas de gestión administrativa-Financiera (SIGA, SIAF, SISGEDO, PDT, Planillas, Sistemas de mesa de partes, etc.) y de gestión de investigación (Sistema de Gestión de revistas científicas, Repositorios institucionales, Editorial, Inventario, Balance Score Card - tablero).

Si bien es cierto existen soluciones de acceso remoto que dan facilidades para la conexión, sin embargo, estas requieren un costo elevado por licencia, además demanda tiempo de gestión administrativa para adquirir dichas licencias. Por otro lado, la seguridad de la información es indispensable en todo proyecto a gran escala.

Por esto, basados en la ISO 27001 y teniendo en cuenta los 3 pilares básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad) proponemos implementar una infraestructura VPN con Open Source para la gestión remota de aplicaciones de Intranet en la Universidad Nacional Pedro Ruiz Gallo.

Ya que, la introducción de Software Libre en el Perú ha sido favorecida gracias a la ley N°28612, que también es llamada de “Neutralidad Tecnológica” porque norma el uso, adquisición y adecuación de software por parte del Estado peruano. Esta ley prohíbe a cualquier entidad de la administración pública adquirir soportes físicos (hardware) que la obliguen a utilizar un solo tipo de software o que limiten de cualquier manera su autonomía informática.

Finalmente, una de las condiciones básicas propuestas por la Superintendencia Nacional De Educación Superior Universitaria (SUNEDU) para el licenciamiento y

acreditación de la Universidad Nacional Pedro Ruiz Gallo es contar con una infraestructura y equipamiento adecuado para que el personal administrativo y académico pueda cumplir sus labores, siendo este un motivo más para la realización de nuestra tesis.

3.1.2.3. Personal objetivo

Luego de obtener la información de las oficinas administrativas y los trabajadores que laboran en dichas oficinas se determinó de acuerdo a las tareas que realizan y el impacto que genera hacia otras oficinas a las siguientes oficinas con sus respectivos trabajadores:

Tabla 10: Personal Objetivo

OFICINAS	NOMBRE	CARGO	SERVICIOS USADOS
Asuntos Académicos	Ing. Carlos Ruiz Oliva	Administrador y Programador de Notas académicas	GESTAC
Oficina de Abastecimiento	Ing. Marlon Alain Sandoval Paiva	Administrador de Sistema de Integración de Gestión Administrativa	SIGA
Red Telemática	Ing. Vladimir Sabino Gonzales Mechan	Administrador de Red Telemática	Administración de servidores
Contabilidad General	Ing. Cristian Paico Castillo	Administrador de SIAF	SIAF
Telemática - FACHSE	Ing. Percy Gonzales Ñique	Administrador de Sistema de pagos	SIAF
PostGrado - Informática	Ing. Luis Alberto Mija Camargo	Administrador de Sistema de pagos PostGrado	Acceso a servidores

3.1.3. Determinación de los requerimientos necesarios para la implementación de la VPN

El hardware y software a utilizar son puntos que ya fueron descritos en el capítulo 2 del presente trabajo de investigación, exactamente en la página 47.

3.1.4. Topologías

Las siguientes topologías fueron hechas en base a la implementación que se realizará en la red telemática de la Universidad Nacional Pedro Ruiz Gallo.

3.1.4.1. Topología Física

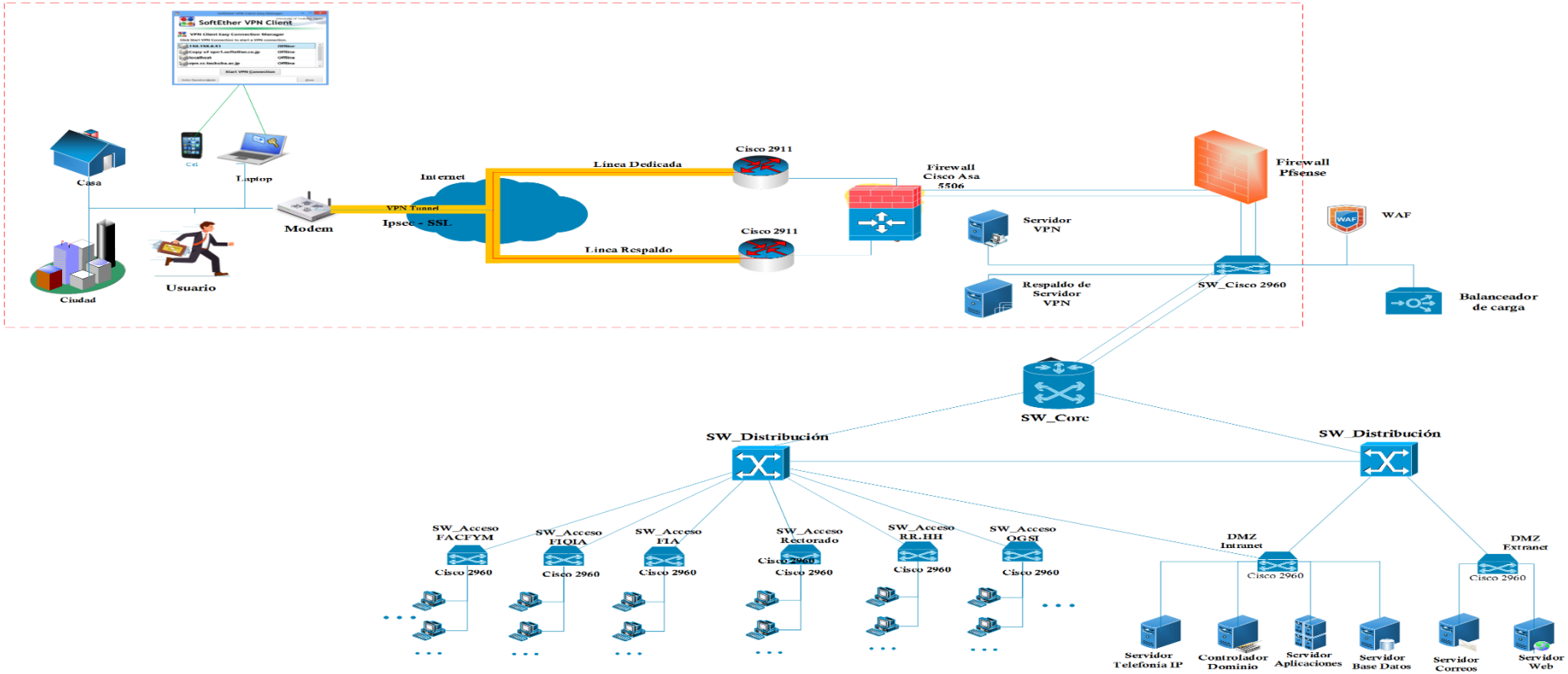


Figura 16: Topología física

3.1.4.2. Topología Lógica

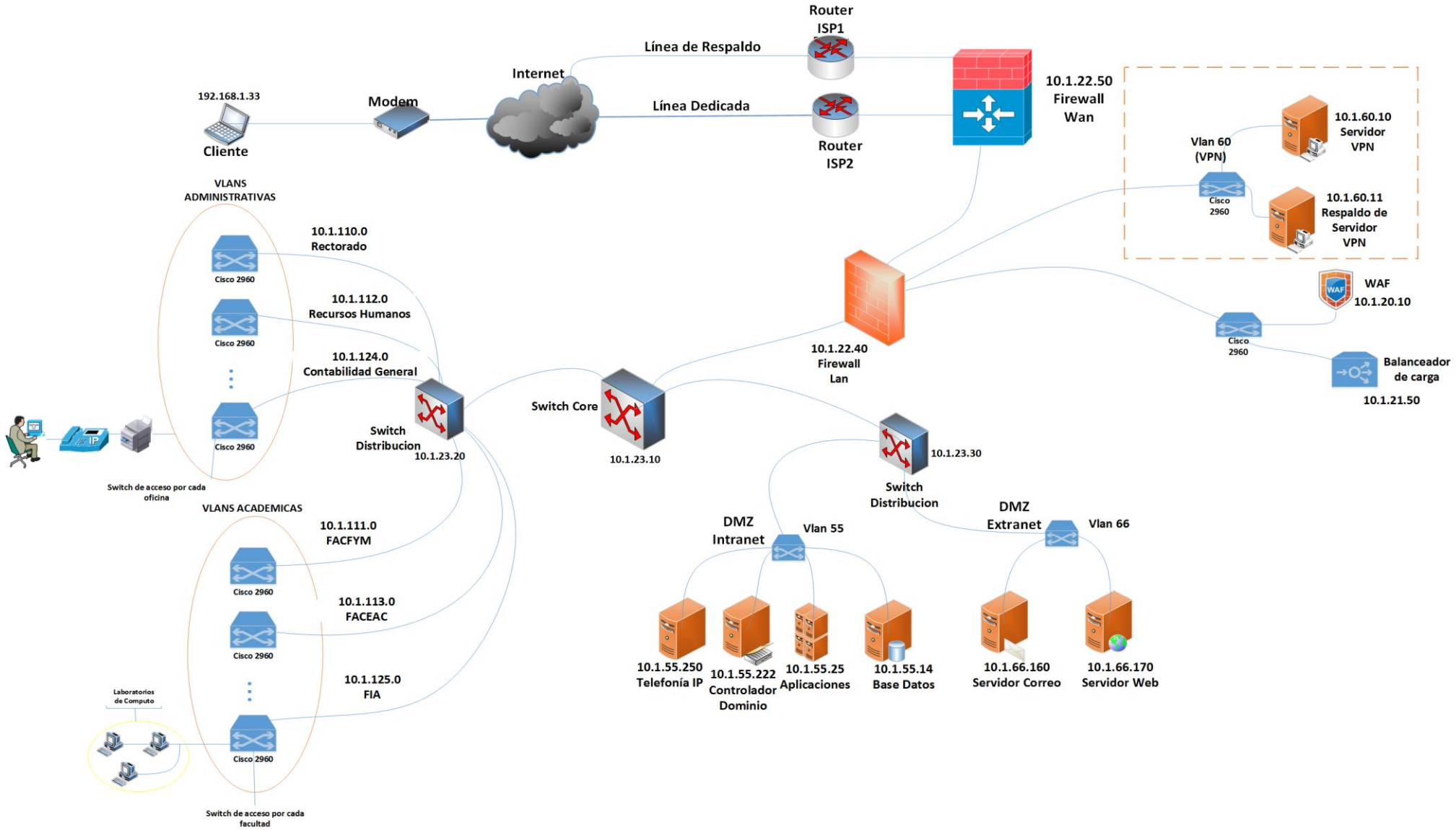


Figura 17: Topología Lógica

3.1.5. Presupuestos y Rentabilidad

3.1.5.1. Presupuestos

3.1.5.1.1. Presupuesto de hardware

Tabla 11: Presupuesto de Hardware

NOMBRE	CANTIDAD	PRECIO	SUBTOTAL
HP ProLiant DL580 Gen7	1	S/. 10 538.00	S/. 0.00
HP ProLiant DL360 Gen9	1	S/. 19 999.00	S/. 0.00
Cisco Catalyst 4506 (Sw Core)	1	S/. 8 624.44	S/. 0.00
Cisco Catalyst 3850 (Sw de Distribución)	2	S/. 15 301.40	S/. 0.00
Cisco ASA5506-K9 (Firewall)	1	S/. 3 482.50	S/. 0.00
Cisco Catalyst Compact 2960	1	S/. 3 536.72	S/. 3 536.72
HP 300GB 12G SAS 15K rpm SFF 2.5in Enterprise Hard Drive	1	S/. 1 153.04	S/. 1 153.04
16 GB DDR3 Memory upgrade for HP ProLiant DL580 G7	1	S/. 4 822.97	S/. 4 822.97
TOTAL			S/. 9 512.73

Todos los equipos cuyo subtotal es igual a S/. 0.00 son equipos de la universidad que serán reutilizados y repotenciados para este proyecto.

3.1.5.1.2. Presupuesto de software

Tabla 12: Presupuesto de Software

SOFTWARE	SUBTOTAL
PfSense v 2.4	S/. 0.00
SoftEther VPN 4.0	S/. 0.00
Vmware Vsphere 6.7	S/. 0.00
CentOS 7	S/. 0.00
TOTAL	S/. 0.00

Todo el software que utilizaremos está basado en software libre, por lo que no tendrá costo alguno.

3.1.5.1.3. Presupuesto de servicios

Los servicios que se detallan a continuación están basados en el trabajo de los dos tesistas:

Tabla 13: Presupuesto de Servicios

NOMBRE	VALOR TOTAL
Implementación y configuración	S/. 3 580.00
Soporte y mantenimiento	S/. 500.00
Capacitación	S/. 300.00
SUB TOTAL	S/. 4 380.00

3.1.5.1.4. Presupuesto Total

En la siguiente tabla presentamos el presupuesto total en base a 4 meses para 2 personas, en dónde incluimos los imprevistos.

Tabla 14: Presupuesto Total

PRESUPUESTO	SUB TOTAL
Hardware	S/. 9 512.73
Software	S/. 0.00
Servicios	S/. 4 380.00
TOTAL	S/. 13 892.73

3.1.5.2. Rentabilidad

En cuanto a la rentabilidad del proyecto calcularemos el VAN y el TIR, para posteriormente evaluar si el proyecto llega a ser rentable. Cabe resaltar que los flujos de cajas se tomarán de casos supuestos que se sucsiten en la universidad de no existir la VPN que planteamos implementar, ya que en su mayoría ésta produce beneficios intangibles, que describiremos posteriormente.

3.1.5.2.1. Cálculo del VAN, TIR y PR

3.1.5.2.1.1. Periodo de recuperación

El siguiente análisis de recuperación está basado en un periodo de 1 año y con una inversión inicial de S/ 13 892.73 (hardware + servicios). Considerando a la tasa de interés con un 10%

Tabla 15: Periodo de recuperación

	AÑO 0	AÑO 1
Inversión inicial	13 892.73	
Flujo Neto	-13 892.73	18 162.76

3.1.5.2.1.2. Valor Actual Neto

Es un valor actual de los flujos neto, que permiten conocer cuánto se va a ganar o perder con la inversión. Para calcularlo se utiliza la siguiente fórmula:

$$VAN = \sum_{t=1}^{n} \frac{FN_t}{(1+k)^t} - I_0$$

Dónde:

- FN_t = representa los flujos netos de cada periodo t
- I_0 = es el valor del desembolso inicial de la inversión
- n = es el número de periodos considerados
- k = es la tasa de interés

Entonces:

$$VAN = \frac{18\ 162.76}{(1+0.1)^1} - 13\ 892.73$$

$$VAN = 2\ 618.87$$

Como el resultado es mayor a 0 el proyecto es viable, ya que genera un beneficio

3.1.5.2.1.3. Tasa Interna de Retorno

Es la tasa de descuento o rentabilidad que ofrece una inversión. Es decir, es el porcentaje de beneficio o pérdida que tendrá una inversión para las cantidades que no se han retirado del proyecto. Para calcularlo se utiliza la siguiente fórmula:

$$0 = \sum_{t=0}^{n} \frac{FN_t}{(1+TIR)^t}$$

Dónde:

- FN_t = representa los flujos netos de cada periodo t
- n = es el número de periodos considerados

$$0 = -13\,892.73 + \frac{18\,162.76}{(1 + TIR)^1}$$

$$TIR = 0.31$$

El TIR es 1.21, es decir que el proyecto tiene una rentabilidad de 31% y es mayor al 10% (tasa de interés usado para el VAN), por lo tanto el proyecto es rentable.

3.1.5.3. Beneficios Intangibles

- Mejora de la imagen institucional de la Universidad.
- Mejora del nivel de satisfacción de los estudiantes y trabajadores administrativos gracias a la agilización en los procesos de sus trámites.
- Mejora el acceso rápido y oportuno a la información para mejor toma de decisiones.
- Apoya al crecimiento tecnológico de la Universidad.
- Mejora en la productividad de los trabajadores.
- Mayor seguridad en el acceso a carpetas compartidas (tuneleado).

3.1.6. Diseño e Implementación de la VPN

3.1.6.1. Diseño de la VPN

El presente diseño de la VPN a implementar, se basa en un estudio para mejorar el rendimiento de las aplicaciones de intranet, y llevar a que estos se puedan ejecutar desde cualquier ubicación con acceso a internet, siempre y cuando haya una autenticación de por medio, que garantice la confidencialidad, integridad y disponibilidad de los datos.

Este diseño tiene como objetivo considerar a las principales características que describiremos a continuación:

3.1.6.1.1. Características

- **Escalabilidad**: Nuestra VPN estará diseñada para que se adapte ante futuros cambios que pueda ocurrir en la universidad.

- **Manejabilidad**: Se diseñará una VPN que sea fácil de monitorear y gestionar. Es por eso que debemos definir políticas de seguridad estrictas para cada grupo.
- **Seguridad**: En este ámbito la VPN, permitirá el viaje seguro de los datos por medio del túnel virtual propiamente de la VPN (INTEGRIDAD); el ingreso de los usuarios a la red será gracias a la implementación de un servidor de certificados para la autenticación de usuarios (CONFIDENCIALIDAD) y estará accesible para el uso en cualquier horario, gracias a los servidores redundantes que se encuentran en la ciudad universitaria, los cuales se encuentran protegidos contra desastres naturales y corte eléctricos(DISPONIBILIDAD).

3.1.6.1.2. Actividades

Como en toda implementación de una VPN se deben realizar las siguientes actividades:

- **Actividad N°01: Análisis de equipos de red**
  Para la implementación de la VPN, primero debemos tener en cuenta los equipos que se utilizaran para el correcto funcionamiento sin interrupciones y a la vez faciliten el acceso a las aplicaciones de intranet.

- **Actividad N°02: Instalación de la VPN**
  Para la instalación del servidor VPN es necesario tener en cuenta la compatibilidad entre el sistema operativo en dónde se tiene pensado instalar y el software que se quiere utilizar.
  Luego de esto nos enfocamos en instalar el software VPN servidor en el sistema operativo. Debemos tener en cuenta que dependiendo del sistema operativo deberemos hacer que el servicio se inicie automáticamente.
  Se debe realizar las configuraciones iniciales propias de cada software de VPN.

- **Actividad N°03: Instalación de software de administración para la VPN**
  Al tratarse de una VPN, es normal querer administrarla desde un lugar remoto, para lo cual es necesario realizar la instalación de un software que sea capáz de permitirnos gestionarla y administrarla desde un entorno gráfico, ya que al ser software libre es muy probable que la instalación haya sido desde un terminal.

- **Actividad N°04: Habilitar los protocolos**
  Se debe tener en cuenta los protocolos que deseamos implementar para una conexión segura hacia el servidor, para esto, debemos investigar los protocolos que son compatibles con cada aplicativo VPN.
  A continuación, mostramos un cuadro en donde detallamos los protocolos y puertos que necesita cada software VPN de código abierto, cabe resaltar que un solo puerto es más que suficiente para su correcto funcionamiento.

Tabla 16: Protocolos y puertos para cada VPN con Open Source

	OpenVPN	StrongSwan	WireGuard	SoftEther
Protocolo	SSL-TLS	IPSec, IKEv2	SSH y Mosh	IPSec, OpenVPN, L2TPv3, SSL-VPN(https), MS-SSTP.
Puertos VPN alternativos	TCP 443 UDP 553	UDP 3947	UDP 7361	TCP 443,992,5555, 8888

– **Actividad N°05: Redireccionamiento IP**

Para esta actividad se debe tener definido 3 elementos fundamentales para el direccionamiento IP:

- Dirección IP privada en donde se instalará el servidor VPN
- Rango de direcciones IP que utilizaran los clientes para la conexión con el servidor, esto se configurará al momento de realizar el NAT y posteriormente en el apartado DHCP del mismo.
- Dirección IP pública a la cual se conectarán los clientes desde cualquier lugar con acceso a internet.

Distribución de IP por cada VLAN

- Para la distribución de IP en este caso se usaron datos distintos para proteger la información presente en la red de la universidad.
- En la distribución de IP en la VPN se consideró las VLANS existentes más importantes con sus respectivos números de red, así como se muestra en el siguiente cuadro:

Tabla 17: Distribución IP por VLAN

ID de VLAN	Descripción	Dirección de Red
55	Servidores Intranet	10.1.55.0/24
66	Servidores Extranet	10.1.66.0/24
110 (pares)	Oficinas Administrativas	10.1.110.0/24
125 (impares)	Oficinas Académicas	10.1.125.0/24
20 - 23	Otros Servicios	10.1.20.0/24
60	VPN	10.1.60.0/29

Tabla 18: Creación de Virtual Hub's

VIRTUAL HUB	RED
ACAD	**192.168.10.0**
ABAST	**192.168.20.0**
RTL	**192.168.30.0**
CONT	**192.168.40.0**
FACHSE	**192.168.50.0**
POSTG	**192.168.60.0**

- **Actividad N°06: Creación de grupos y usuarios**
  Aquí se realiza la creación de los grupos por cada oficina que tenga la empresa; es práctico también colocarle alguna descripción, para tener conocimiento de las funciones que los miembros realizan en el grupo.
  Según las buenas prácticas para la creación de nuevos usuarios, se recomienda siempre utilizar la letra inicial del primer nombre más el primer apellido y la letra inicial del segundo apellido.

- **Actividad N°07: Tipo de Autenticación**
  Existe una gran variedad de tipos de autenticación, las cuales nos proporcionan cierto grado de seguridad al momento de iniciar sesión con el usuario cliente, muchos de los cuales implican:
  - Tarjeta inteligente
  - Certificado
  - Nombre de usuario y contraseña
  - Contraseña de un solo uso
  - Tipo de credencial personalizada
  - RADIUS
  - Controlador de Dominio

  Algunos tipos de autenticación traen consigo la opción de agregarle un número de serie hexadecimal, este posteriormente se encriptará en un algoritmo para que sea más segura y difícil de descifrar.

- **Actividad N°08: Administración de políticas de seguridad**
  Las políticas de seguridad que se logren implementar en un grupo definirán los permisos y restricciones que los usuarios tendrán en el mismo.
  Para la prevención de ataques DoS es necesario implementar una medida de seguridad que permita bloquear dichos ataques, para que así la VPN sea mucho más segura. Además de los conocidos ataques DoS existen muchos más qe detallaremos a continuación:

Tabla 19: Tipos de Ataques

Tipo de ataque	Descripcion
Ataque DoS	En un ataque de denegación de servicio (DoS), un atacante sobrecarga el servidor con solicitudes, no puede procesarse dicha solicitud. Esto es una "denegación de servicio" ya que no se puede acceder al sitio.
Ping Flood	Ping flood se basa en enviar a la víctima una cantidad abrumadora de paquetes ping, usualmente usando el comando "ping" de UNIX como hosts el requisito principal es tener acceso a un ancho de banda mayor que la víctima.

Ping de la muerte	El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo.
Escaneo de puertos	Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles (es decir, qué servicio podría estar enumerando un puerto).
ARP Spoofing	ARP Poison Routing (APR), es una técnica utilizada para atacar una red cableada o inalámbrica de Ethernet. ARP Spoofing puede permitir que un atacante detecte frameworks de datos en una red de área local (LAN), modifique el tráfico o detenga el tráfico por completo.
ACK flood	Esta es una técnica para enviar un paquete TCP / ACK al objetivo a menudo con una dirección IP falsificada. Es muy similar a los ataques de inundación TCP / SYN
Ataque Man-In-The-Middle	Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc
OS Finger Printing	El término "huella digital del sistema operativo" / OS Finger Printing en Ethical Hacking se refiere a cualquier método utilizado para determinar qué sistema operativo se ejecuta en una computadora remota.
Ataques de Contraseña	Ataques de Contraseña Consiste en la prueba metódica de contraseñas para lograr el acceso a unsistema, siempre y cuando la cuenta no presente un control de intentos fallidosde logueo. Este tipo de ataques puede ser efectuado:o Por diccionario o por la fuerza bruta
Backdoors	También denominados “puertas traseras”, consisten en accesos noconvencionales a los sistemas, los cuales pueden permitir efectuar accionesque no son permitidas por vías normales

- **Actividad N°09: Pruebas (test)**

  Una vez finalizadas las actividades anteriores, se procede con un periodo de pruebas, en las que simulamos la creación de múltiples usuarios a los que les aplicamos políticas de seguridad diferentes por medio de sus grupos, probando así el permiso o denegación al momento de acceder al servidor por medio de la herramienta cliente.

También probamos la velocidad de respuesta de los clientes hacia el servidor.
Y por último la seguridad de encriptación en la que verificamos que la información que viaja por la VPN sea segura y así evitar que los datos puedan ser vulnerados con la ayuda de software de auditoria, de captura de paquetes, etc.

- **Actividad N°10: Monitoreo**
  Es importante que después de implementado el servicio, este tenga que estar constantemente monitoreado, en busca de posibles elementos con comportamientos inusuales en la VPN que ralenticen el acceso al servidor, para posteriormente sea informado al administrador para su pronta solución.
  Cabe resaltar que, ante posibles comportamientos inusuales, se han debido de establecer medidas de seguridad (en la actividad N°08) y enlaces redundantes entre los servidores para que el servicio de VPN no se vea afectado.

3.1.6.2. Implementación de la VPN

Ahora procedemos a realizar los pasos paralelamente a las actividades anteriormente detalladas en el apartado de diseño para que quede implementado el servidor, haciendo uso de la herramienta SoftEther VPN.

3.1.6.2.1. Paso N°01: Análisis de equipos de red

Los equipos utilizados en este proyecto se detallan a continuación:

Tabla 20: Analisis de equipos de red

Equipo	Características	Logo	Disponible
Firewall	-RAM:8 GB -Disco: 1 TB -NAT: Network Address Tranlation -Reportes y Monitoreo -Reglas de seguridad -2 interfaces de red	pfSense	SI
Firewall	- Cisco ASA 5500-X Next Generation, ASA 5506-X - 8 puertos GE, 1GE Mgmt - RAM: 4GB		SI

Switch (core)	-Catalyst 4506 -Diseño modular, la capa 4 de conmutación, conmutación Layer 3, conmutación Layer 2, soporte ARP. -Protocolos de enrutamiento. -Módulos de red (6) -Fuentes de alimentación(2)		SI
Switch (distribución)	-Switch Administrable capa L3 Cisco Catalyst 3850. - 48 puertos Gigabit 10/100/1000 - Fuente de poder redundante con 03 ventiladores - Soporta hasta stacking (apilamiento) de hasta 09 equipos con un total de 480 Gbps		SI
Switch (acceso)	- Switch Administrable Cisco Catalyst Compact 2960CG-8TC-L - 08 puertosGigabit 10/100/1000 - 02 puertos compartidos para fibra SFP - 128 MB RAM - 64 MB Memoria flash - Cisco IOS LAN Base Software.		NO
Servidor	-HP ProLiant DL580 G7 -Los procesadores de ocho núcleos. -RAM: (32 GB) PC3-10600R DIMM (DDR3) -DriveBackplane disco duro 8 -Interfaces De red 4 -Rack (4U = 7 pulgadas)		SI
Servidor	-HP Proliant DL360 G9 -Procesadores Intel® Xeon® E5-2600 v4 hasta 22 núcleos -Memoria DDR4 de 2400 MHz. -Conexión directa de hasta 16 unidades con controlador HPE Smart Array.		SI

	-Adaptador Ethernet 331i de 1 Gb, 4 puertos por controladora.		
HP 300 GB 15K SAS de disco duro	-Capacidad de almacenamiento 300 GB -Velocidad del eje (RPM) 15000. -Interfaz de la unidad SAS		NO
16GB DDR3 Memory Upgrade for HP ProLiant DL580 G7	-16GB PC3-12800 DDR3 1600MHz. -Factor de forma: DIMM de 240 pines -Velocidad: 1600 MHz DDR3 PC3-12800R		NO

3.1.6.2.2. Paso N°02: Instalación de la VPN

Este paso lo detallamos en el apartado de anexo N°1, en dónde lo explicamos con mayor profundidad.

3.1.6.2.3. Paso N°03: Instalación de Softether VPN Server Manager

A continuación descargaremos e instalaremos un software que nos permitirá la administración remota de la VPN desde un entorno gráfico y compatible con el sistema operativo Windows 7/8/8.1/10

Procedemos a descargar el programa “SoftEther VPN Server Manager” desde el sitio oficial de SoftEther alojado en la url:

https://www.softether.org/5-download

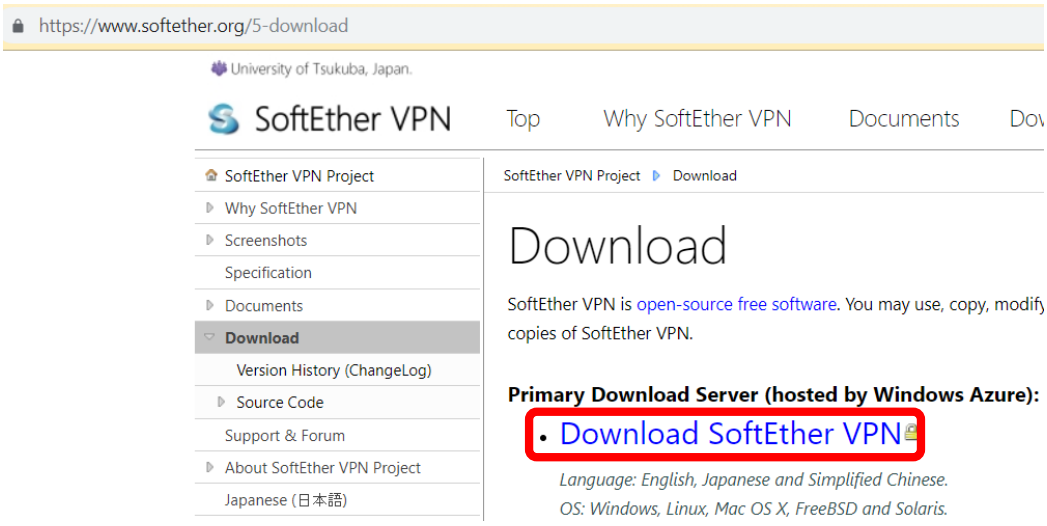


Figura 18: Link de descarga

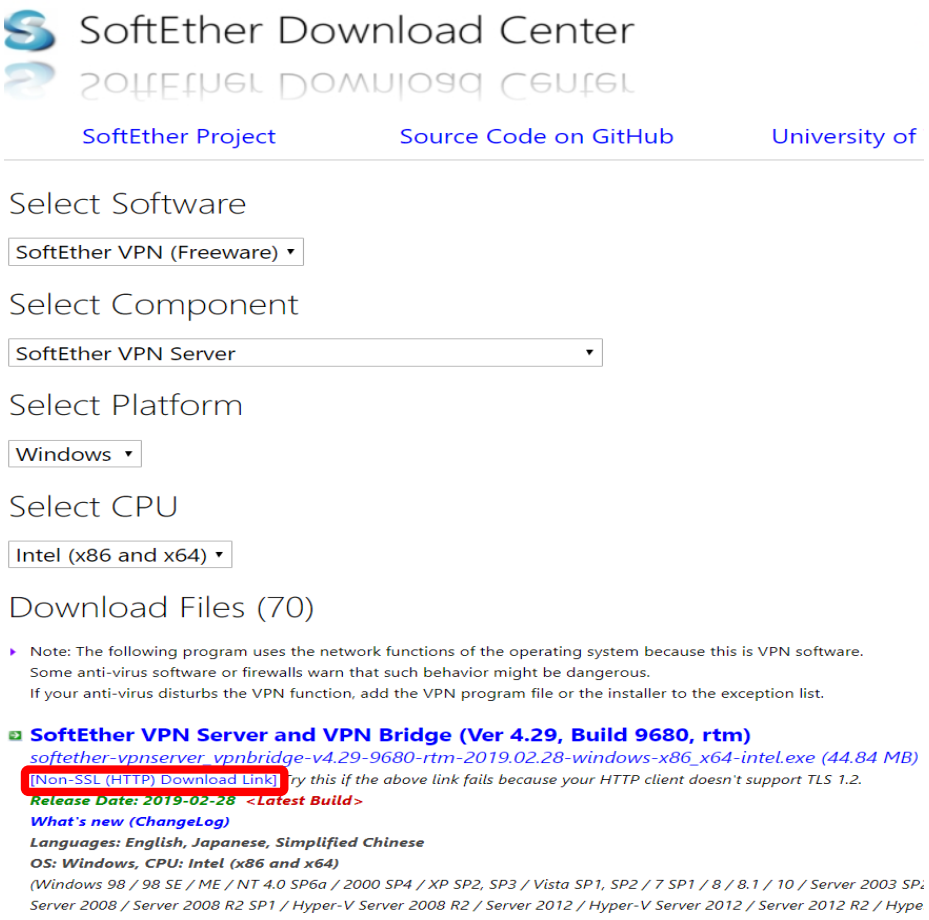


Figura 19: Descarga del software

Lo instalamos como administrador:

Figura 20: Ejecución como administraador

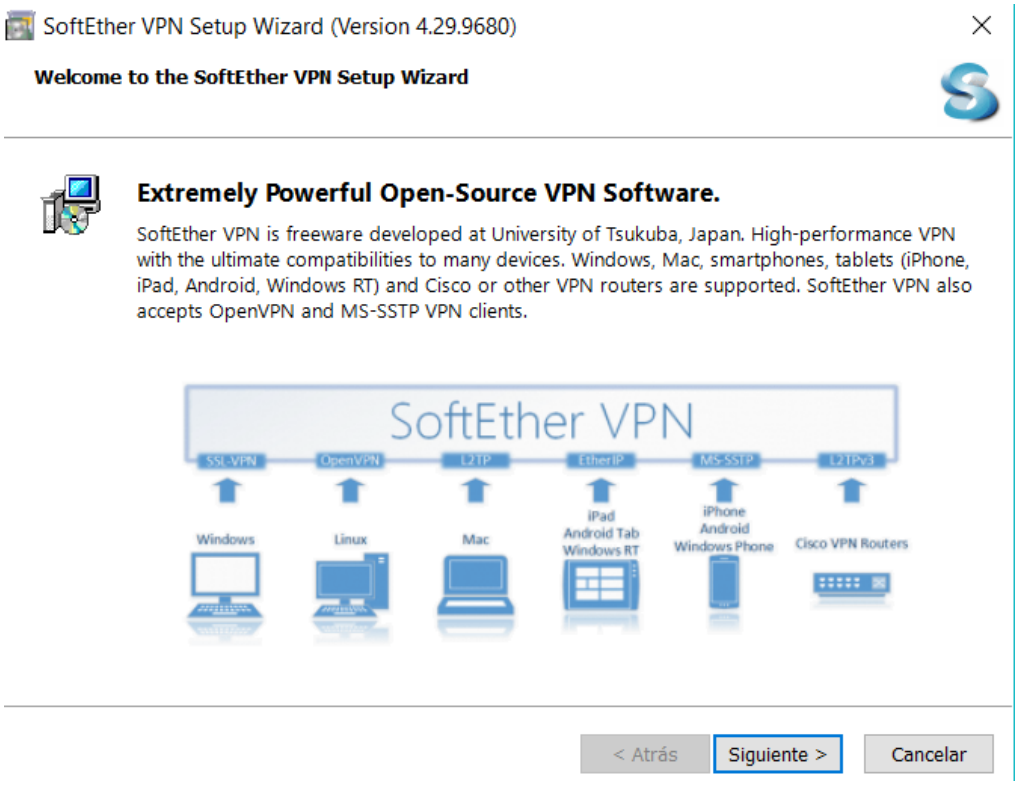


Figura 21: Instalación del Wizard

Escogemos el primer ítem y luego damos click en siguiente (y así sucesivamente hasta finalizar):

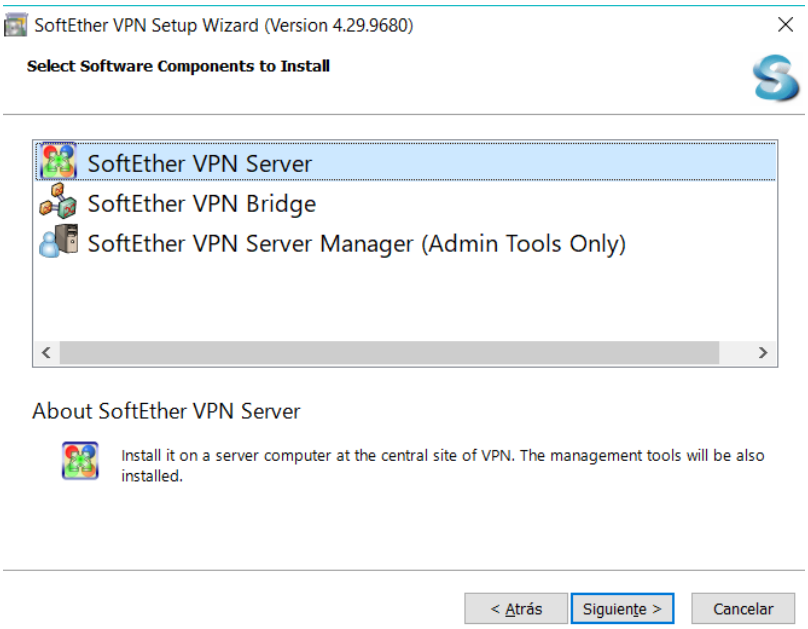


Figura 22: Selección del modo en que se utilizará

Abrimos el programa y agregamos una nueva conexión con el botón “New Setting”, colocamos un nombre y la dirección de red del servidor VPN levantado y damos click en OK

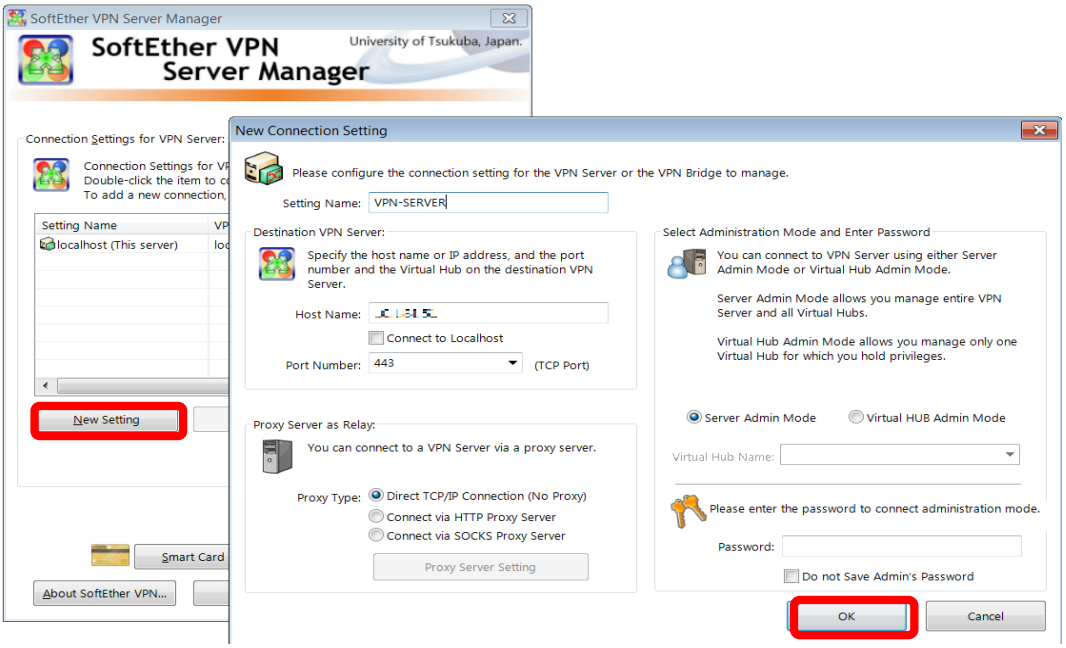


Figura 23: Accediendo al VPN Server

Seguidamente le damos click en **Connect** y creamos la contraseña:

Figura 24: Creación de contraseña

Se nos abrirá otra ventana en la que deberemos marcar el tipo de uso que le daremos a nuestra VPN, en este caso “Remote Access VPN Server”.

Al dar click en “Next” nos pedirá que ingresemos (creemos) el nombre de un hub virtual. Nosotros le llamaremos “VPN_VH_ADMIN”

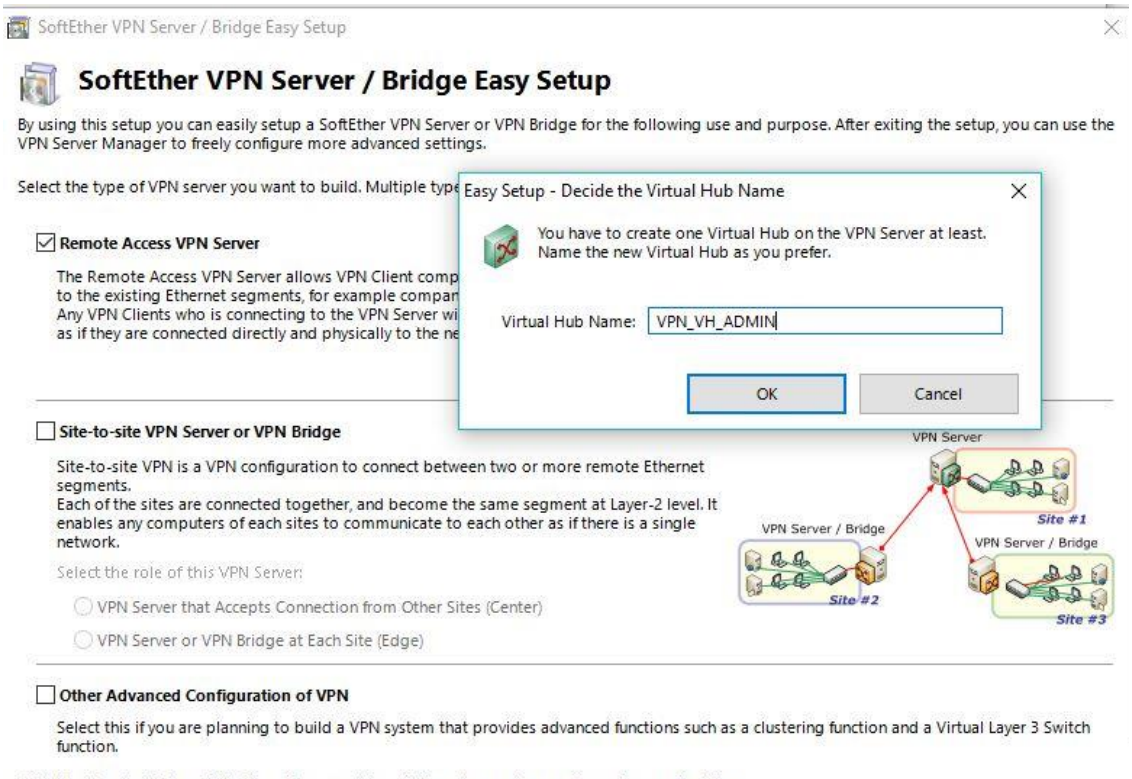


Figura 25: creación del Virtual Hub

Por motivos de seguridad no se muestra el nombre real del hub virtual.

Posteriormente se nos abrirá una ventana en la que nos pedirá ingresar un nombre DDNS, el cual nos permitirá acceder por medio de un enlace, ahorrándonos el trabajo de memorizarnos la dirección IP y ocultándola bajo este nombre.

Por motivos de seguridad, algunos datos en la siguiente figura han sido censurados:

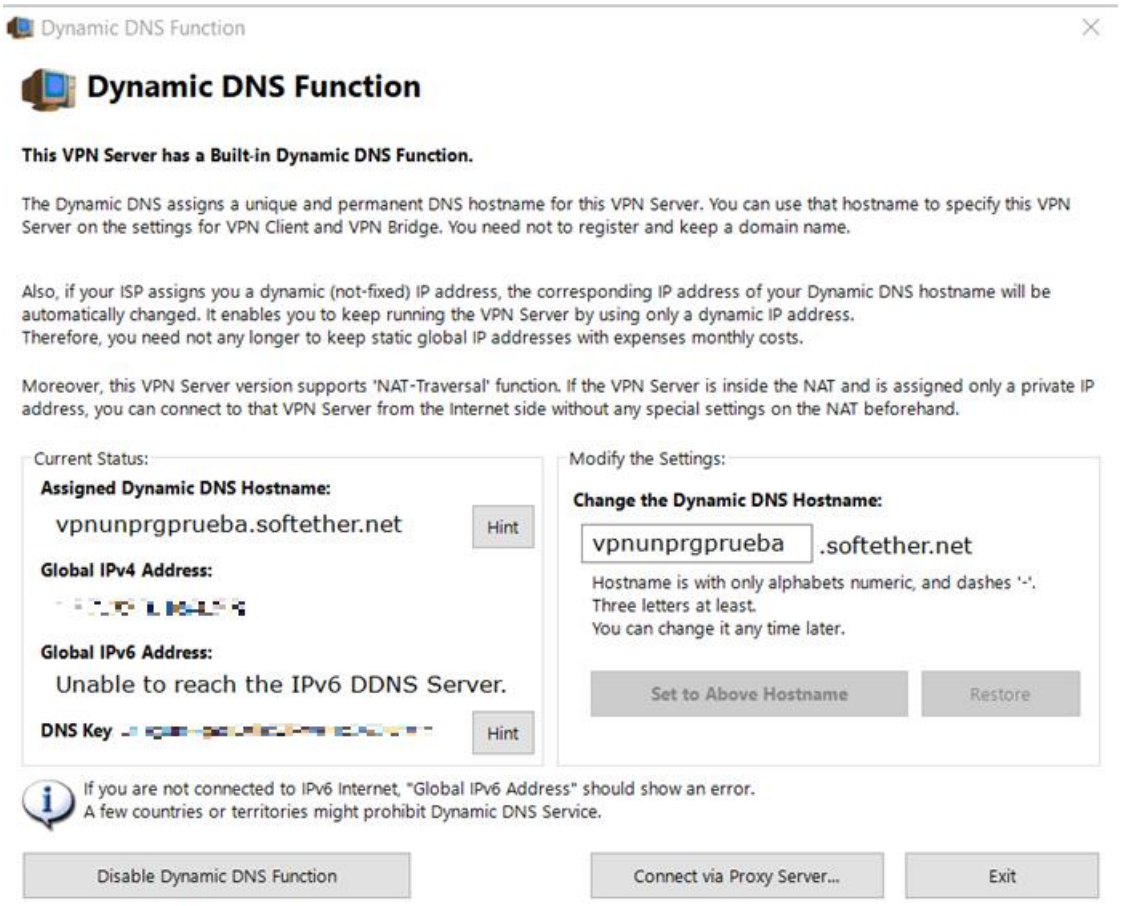


Figura 26: Nombre para el DNS dinámico

3.1.6.2.4. Paso N°04: Habilitar protocolos de la VPN

Como ya hemos descrito anteriormente SoftEther es multiprotocolo, sin embargo, en este proyecto nos enfocaremos en el protocolo L2TP/IPSec el cual

es utilizado para acceder remotamente desde cualquier entorno Windows, android, iOS y Mac OS.

Para habilitar el protocolo anteriormente mencionado, podemos usar tanto un entorno Windows, como desde el mismo CentOS 7.

Pues bien, luego de haber instalado por primera vez el software del paso anterior, se nos abrirá automáticamente una ventana, en la que se deberá marcar la opción “Enable L2TP Server Function (L2TP over IPsec)” para habilitar la función del servidor L2TP sobre IPsec

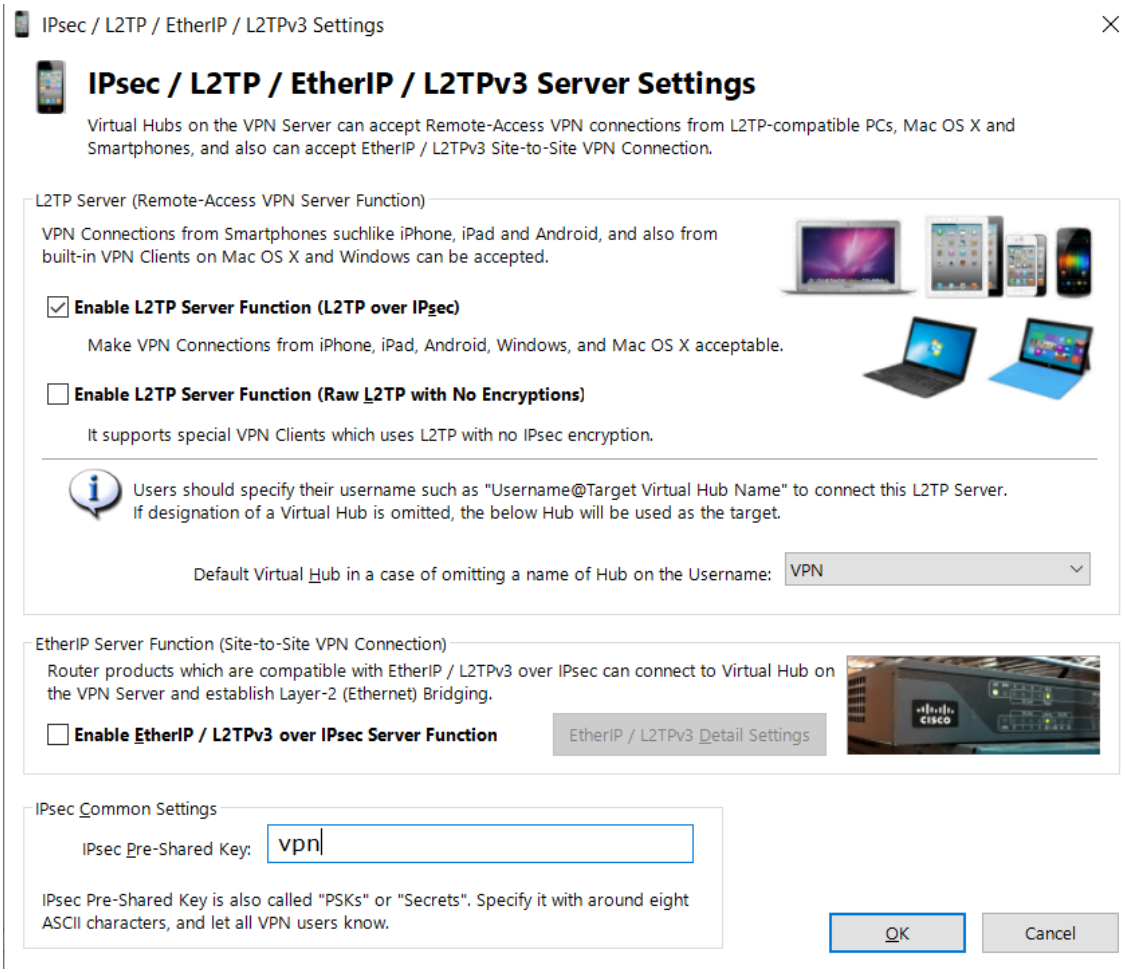


Figura 27: Habilitación de protocolo L2TP sobre IPsec

Si estamos en el menú principal del gestor nos dirigimos a la siguiente opción:

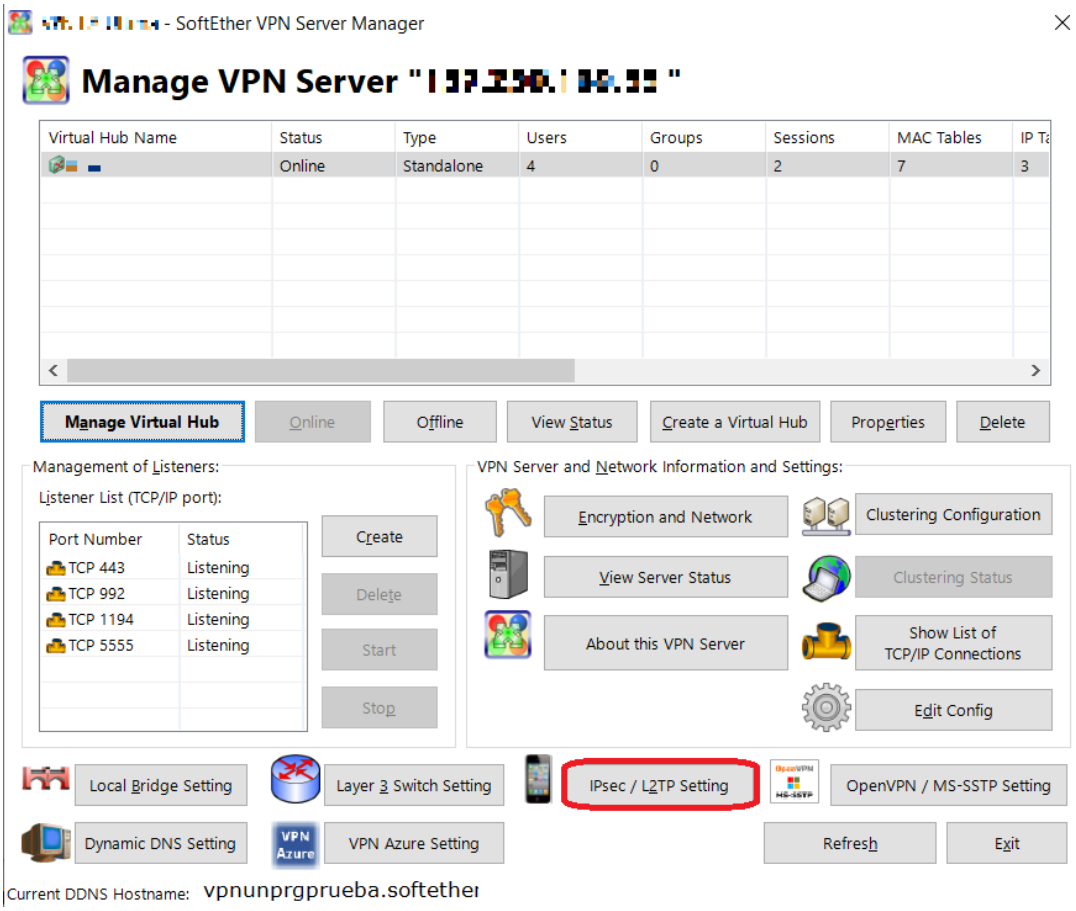


Figura 28: Ubicación del enlace a la ventana de configuración de protocolos

3.1.6.2.5. Paso N°05: Redireccionamiento IP

Para el redireccionamiento IP se necesitará de una herramienta proporcionada por el mismo software con el que venimos trabajando, su nombre SecureNAT.

3.1.6.2.5.1. SecureNAT

La función SecureNAT se divide en dos grandes partes: la función NAT virtual y la función de servidor DHCP virtual. El administrador del concentrador virtual puede permitir el uso a uno o ambos cuando SecureNAT está habilitado, sin embargo el DHCP virtual puede ser usado independientemente del estado de SecureNAT.

El NAT virtual será mejor explicado en el paso N°09

3.1.6.2.5.2. Como servidor DHCP

Esto permite a los clientes y administradores VPN recibir direcciones IP asignadas por el servidor DHCP virtual. A pesar de que el DHCP virtual no tiene numerosas opciones de configuración como lo posee Windows Server; se puede establecer fechas de vencimiento de direcciones IP, administrar tablas de arrendamiento y asignar varias opciones esenciales sin problemas.

- Configuración de DHCP

Ingresamos al gestionador del hub virtual

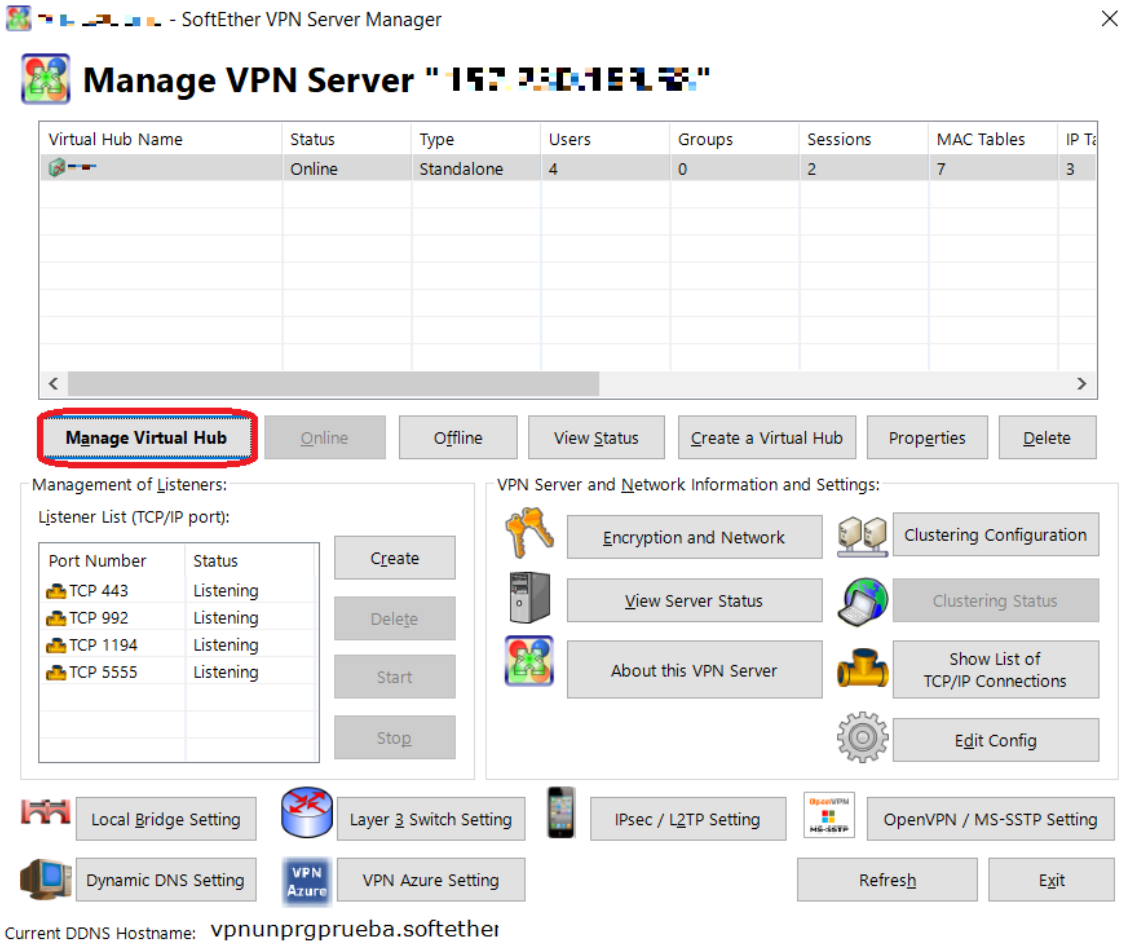


Figura 29: Ingreso a la ventana de gestión del Hub Virtual

Ingresamos al panel de configuración de SecureNAT

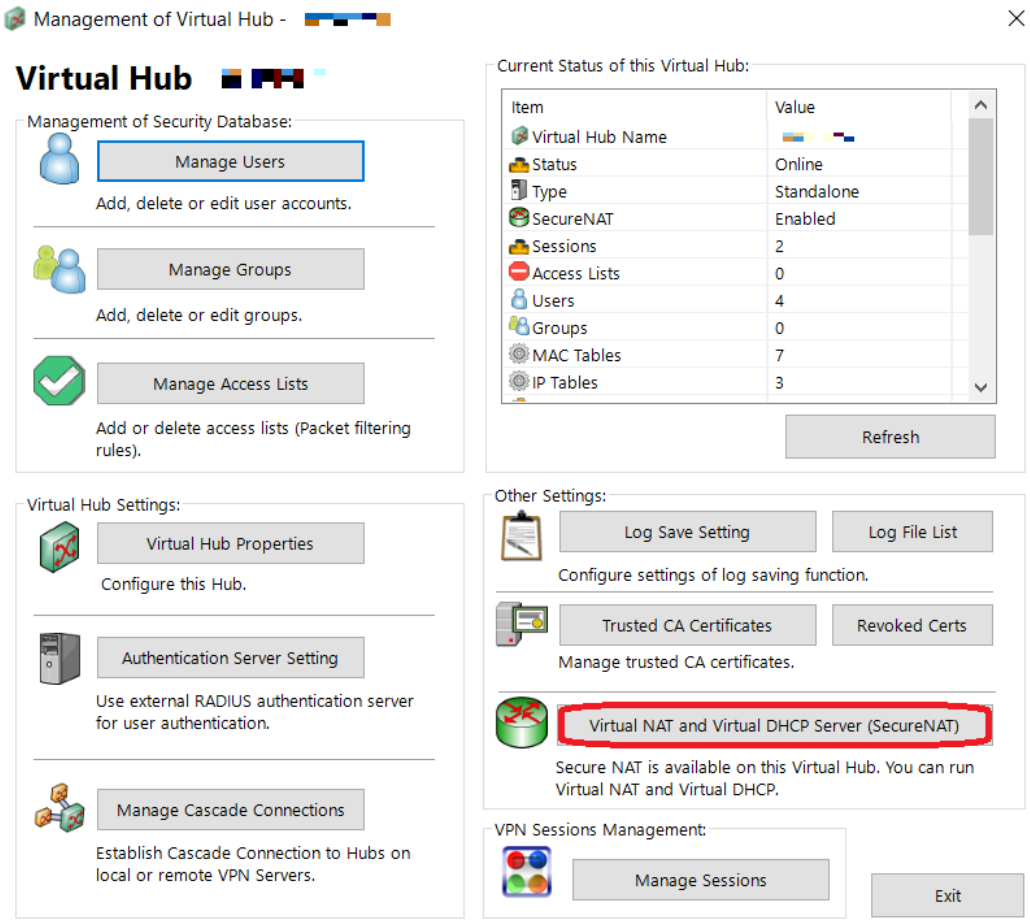


Figura 30: Ingreso al SecureNAT

Habilitamos la función SecureNAT, damos click en “Aceptar” en la nueva ventana que se nos abrirá y luego damos click en “SecureNAT Configuration”

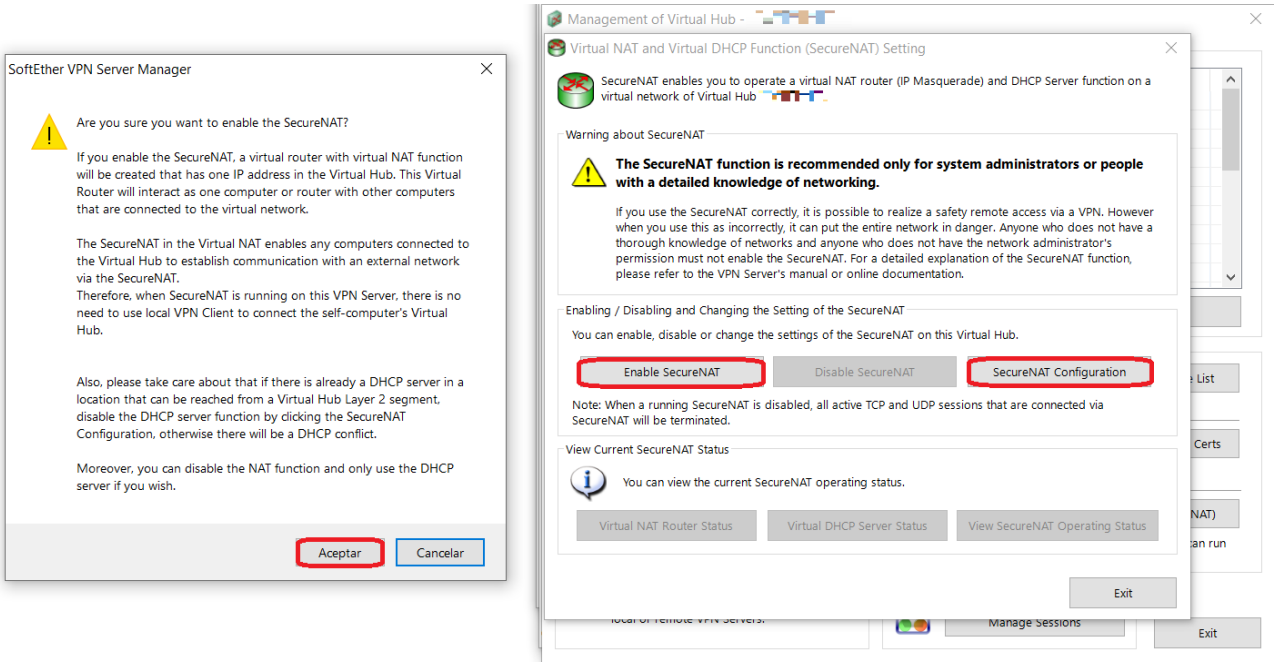


Figura 31: Habilitar SecureNAT y Acceso a la configuración

Configuración de DHCP virtual de acuerdo a la red definida para los clientes VPN en dicho virtual HUB. Aquí podemos ingresar un rango de direcciones IP para que los usuarios que se conecten no tengan problema alguno en recibir una dirección IP asignada por el DHCP virtual

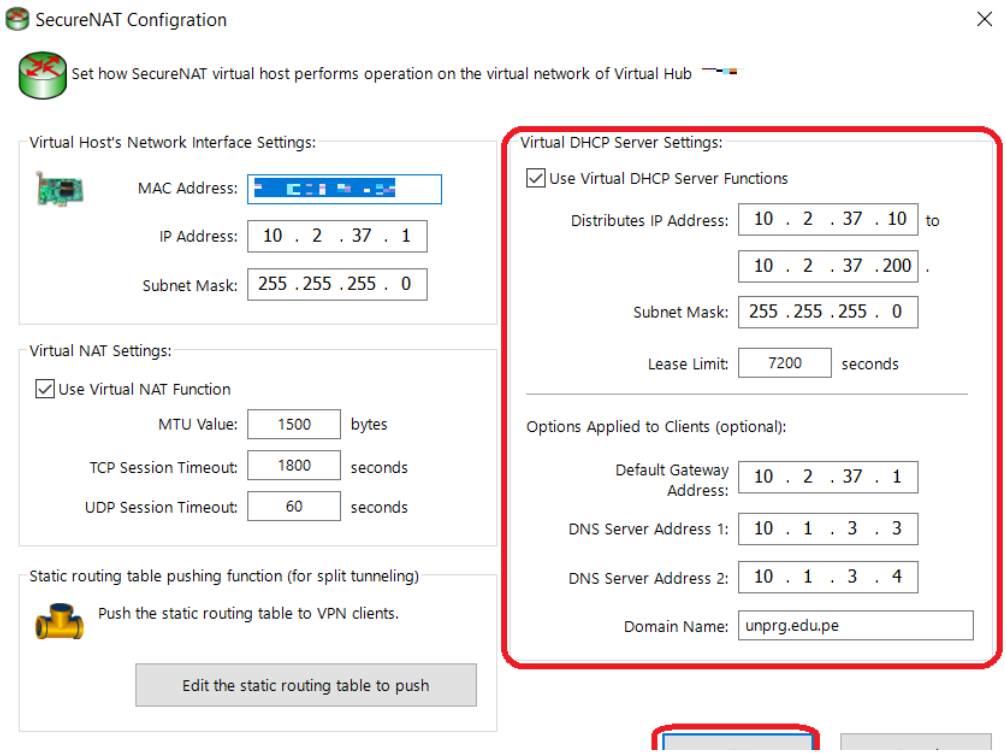


Figura 32: Configuración del DHCP virtual

Cuando el cliente se conecta al servidor con sus credenciales correctas el servidor DHCP le asignara una IP que fue definida para los usuarios.

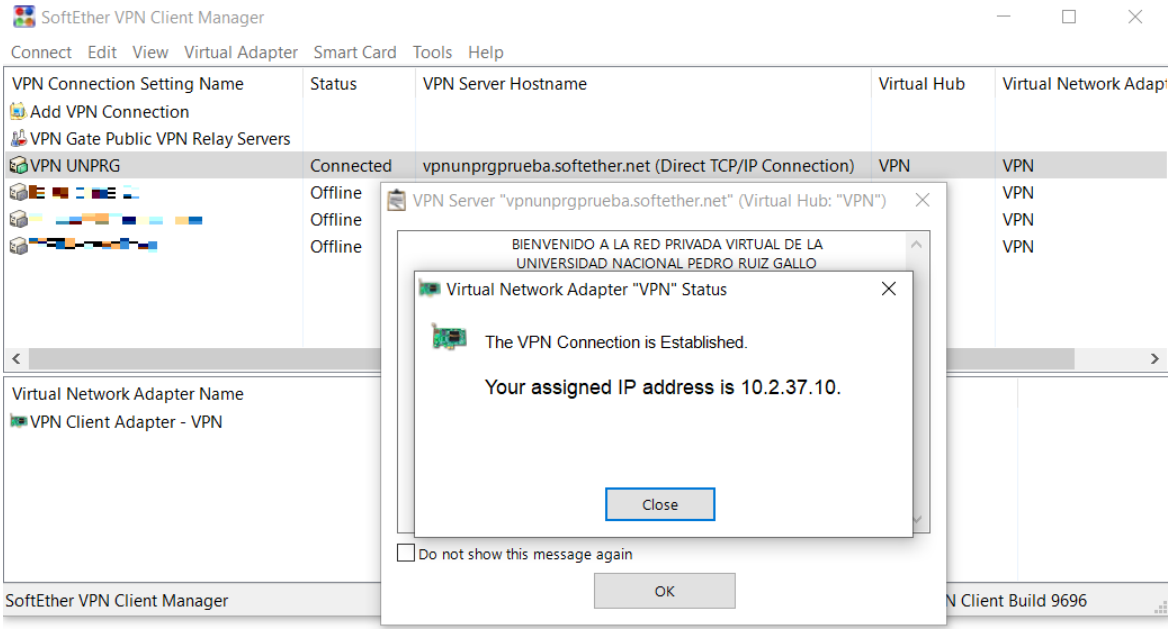


Figura 33: Asignación IP

3.1.6.2.6. Paso N°06: Creación de grupos y usuarios

CREACION DE USUARIOS

Los usuarios a crear ya fueron definidos anteriormente en la tabla N°7 lo cual facilita la creación y distribución de los diferentes usuarios.

Para la creación de usuarios se debe ingresar a la ventana de administración de HUB virtual en la cual nos permite administrar los usuarios.

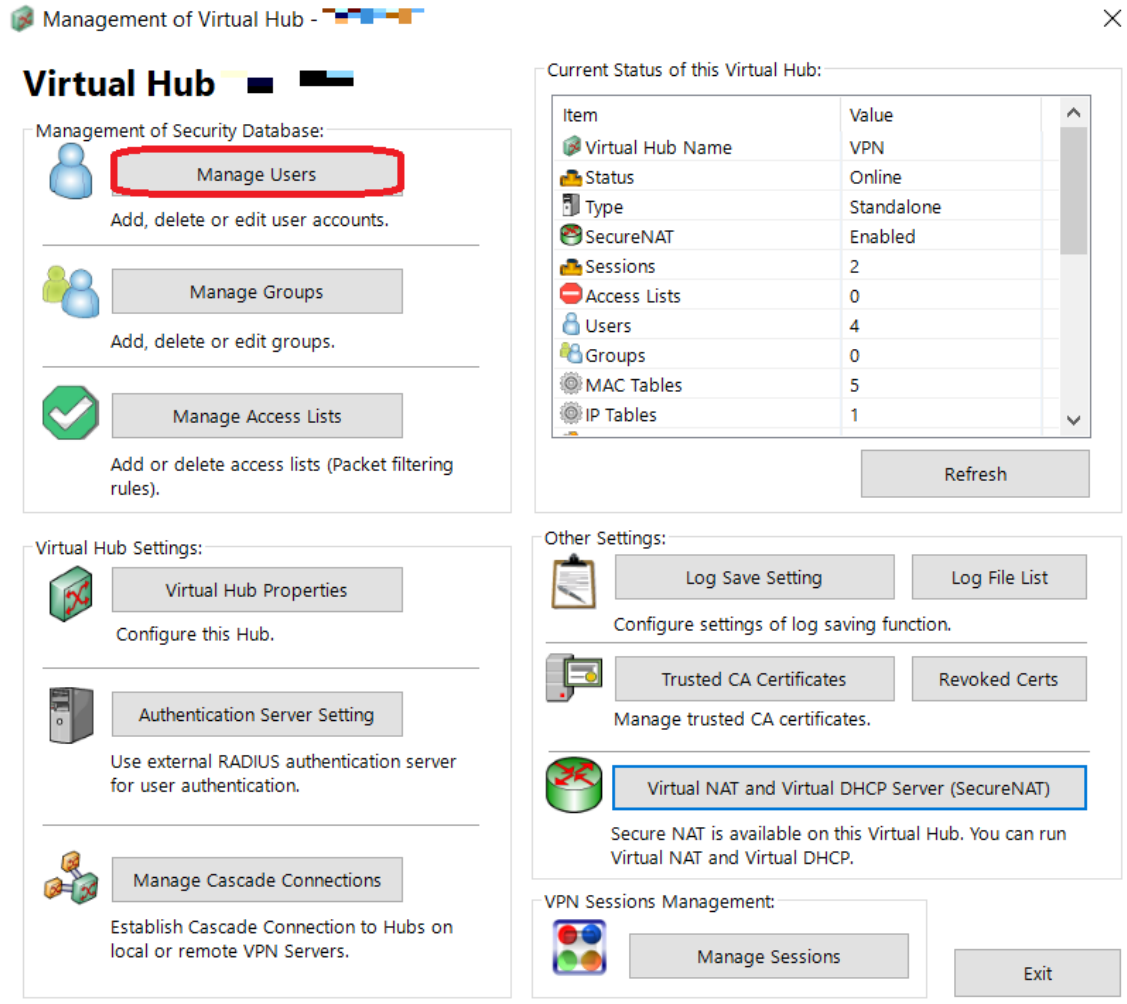


Figura 34: Administración de usuarios

En la ventana administración podemos crear, editar visualizar y eliminar a cada uno de los usuarios definidos. Así como se muestra en la figura N°30

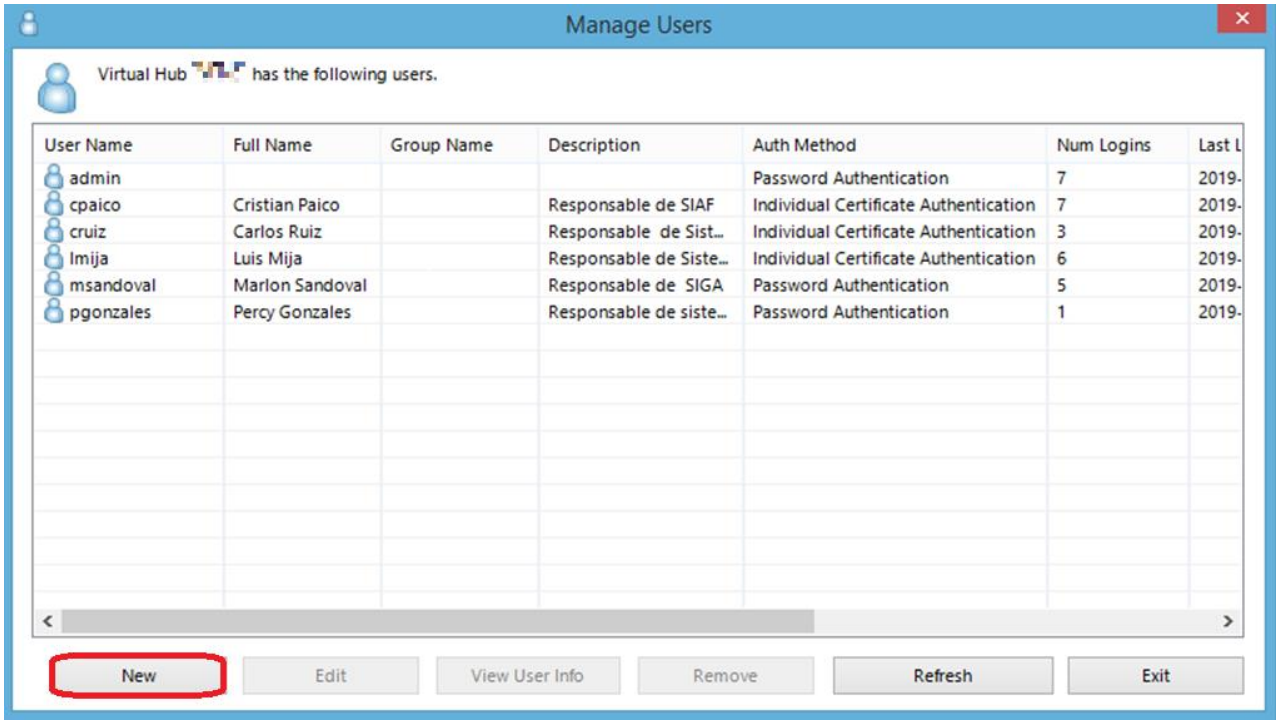


Figura 35: Usuarios actuales

Al crear el usuario se pueden adicionar información como una breve descripción y además se puede agregar a algún grupo para que los usuarios compartan las mismas políticas dentro de él. Ver figura N°31

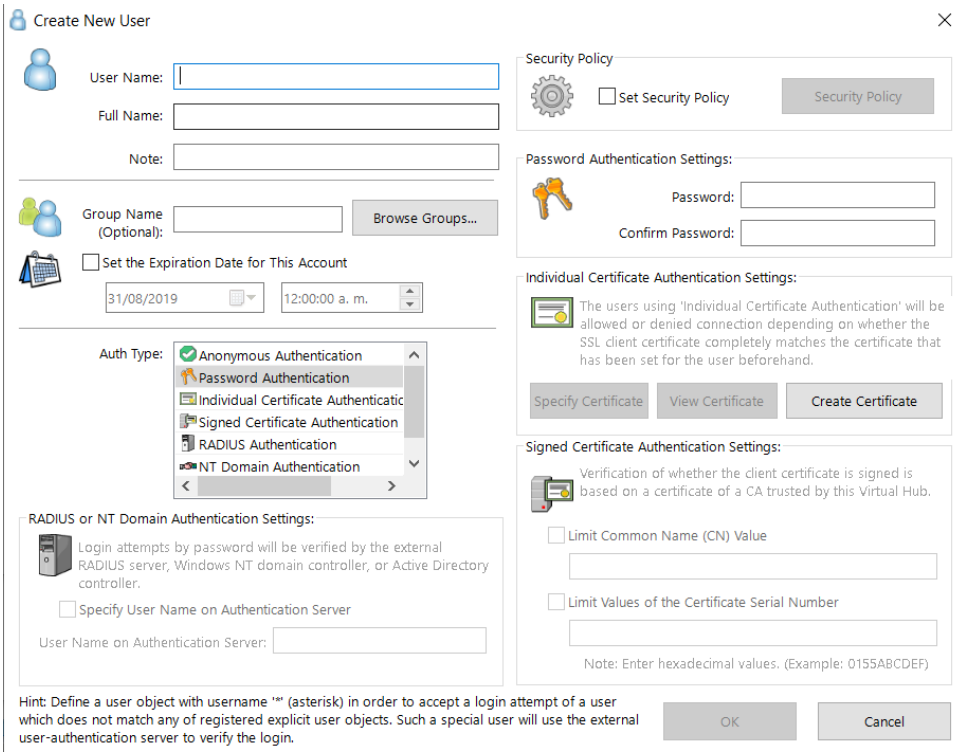


Figura 36: Creación de nuevo usuario

Luego de definir el tipo de autenticación en este caso por certificado digital, procedemos a crear el certificado, para lo cual nos pedirá que ingresemos ciertos datos que se muestran en la figura N°32

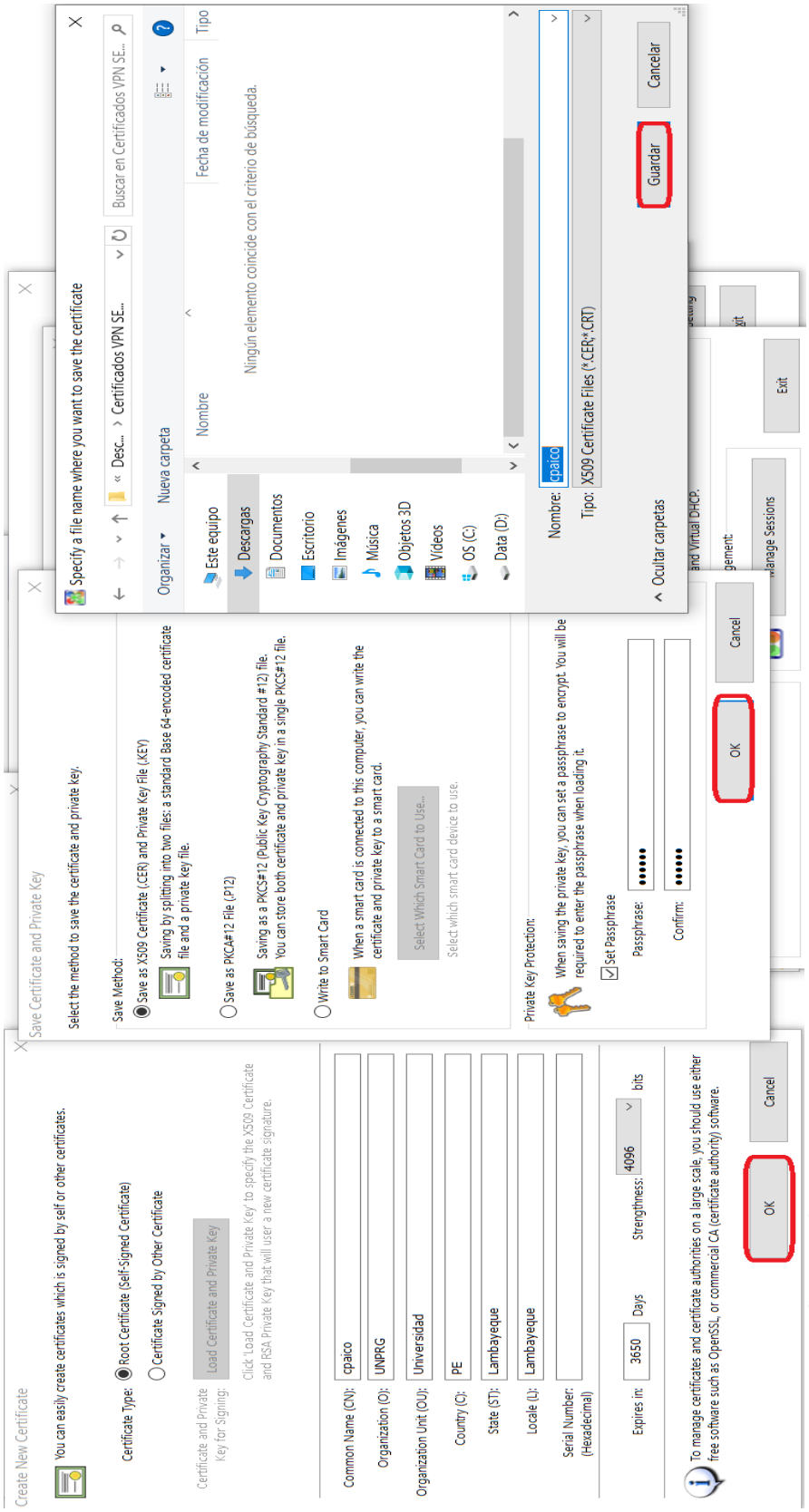


Figura 37: Creación de certificado digital

Como pudimos apreciar en la figura N°32 guardaremos el certificado (.CER) con su respectiva llave (.KEY) de dicho usuario creado, para posteriormente ser entregado a la persona que le corresponda. Cabe resaltar que dicho certificado puede ser protegido por una frase clave

CREACION DE GRUPOS

Para la distribución de grupos se consideró las oficinas a las cuales pertenecen los usuarios.

Para la creación de grupos se debe ingresar a la ventana de administración de HUB virtual en la cual nos permite administrar los grupos

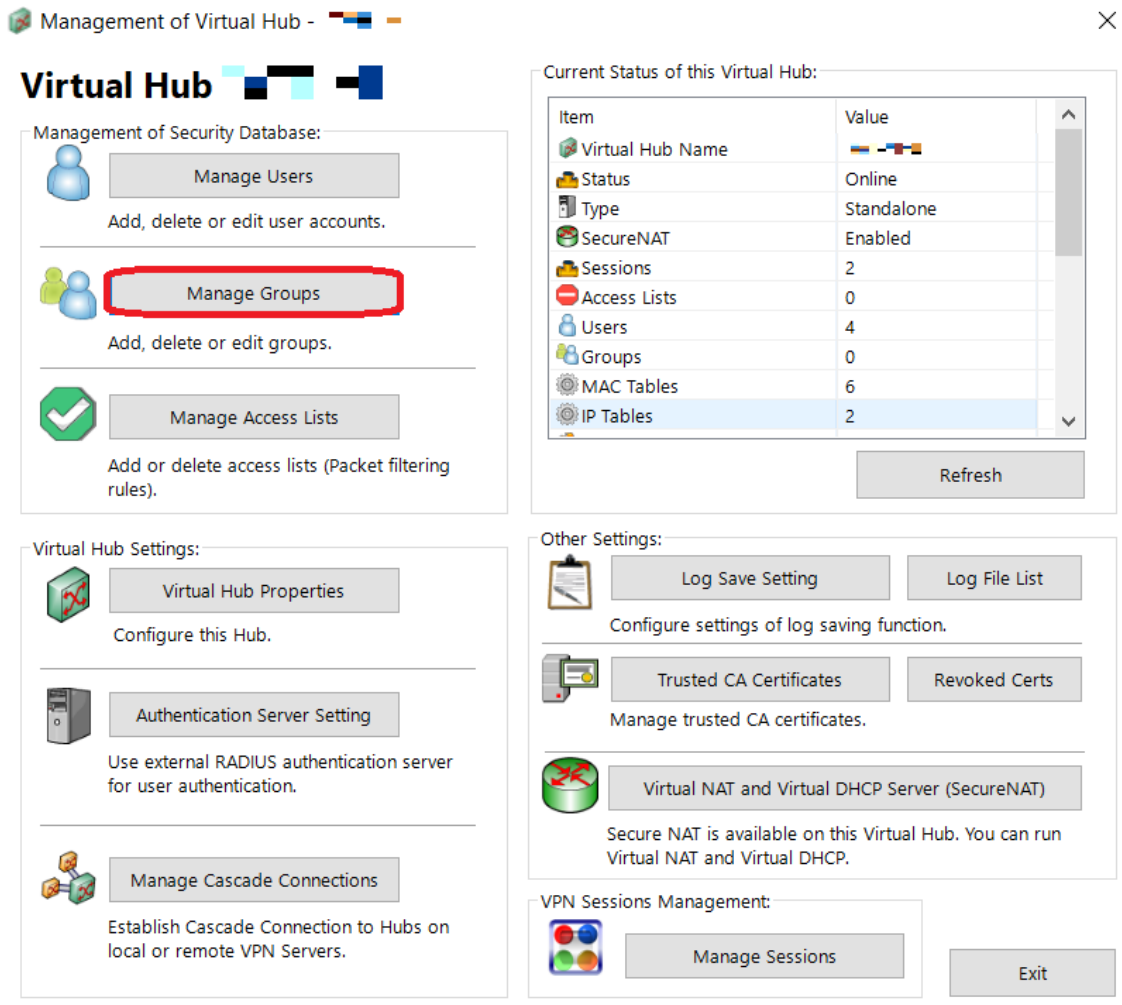


Figura 38: Administración de grupos

En la ventana de administración de grupos podemos crear, editar, eliminar y ver los miembros de usuarios que pertenecen a dicho grupo. Ver figura N°34

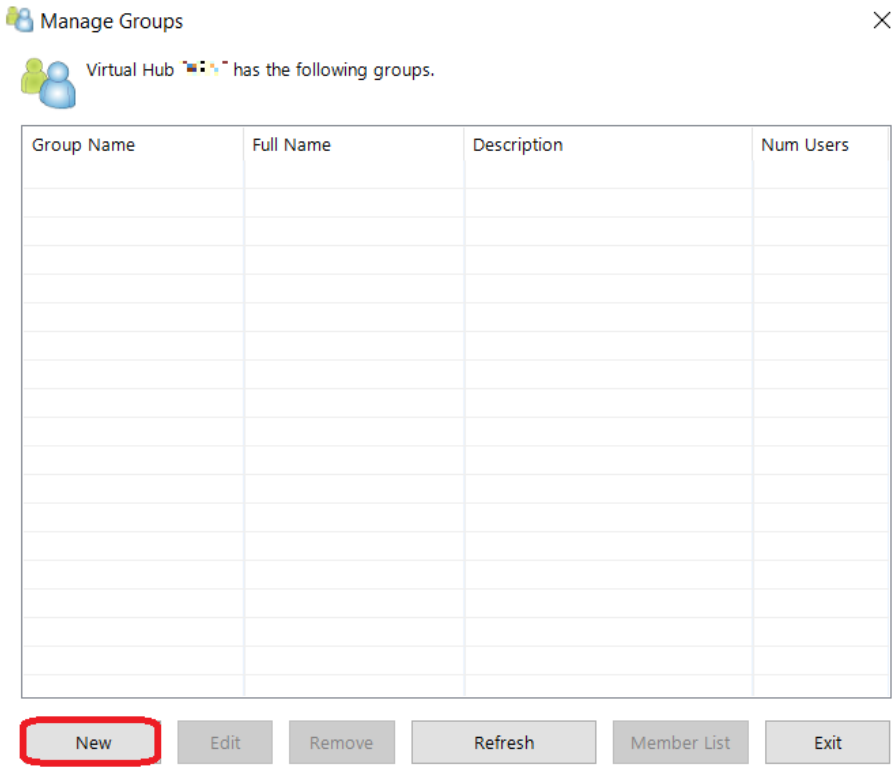


Figura 39: Grupos actuales

Se pueden agregar políticas de seguridad a un grupo determinado y configurar políticas de acuerdo al perfil de grupo seleccionado.

3.1.6.2.7. Paso N°07: Tipo de Autenticación

3.1.6.2.7.1. Autenticación

Con SoftEther VPN, la seguridad está garantizada mediante la realización de autenticación de usuario estricta cuando una nueva sesión de VPN intenta conectarse a un concentrador virtual para evitar una violación de seguridad mediante el cual un tercero no autorizado podría conectar a un concentrador virtual sin permiso.

3.1.6.2.7.2. Autenticación de certificado individual

Con la autenticación de certificado, cuando el equipo de origen conexión intenta conectarse al Hub virtual que presenta un nombre de usuario junto con un certificado electrónico X.509. El servidor comprueba SoftEther VPN si es correcto y el equipo de origen conexión sólo se permite para conectar si pasa.

3.1.6.2.7.3. Creación de Certificado para los Clientes

Para la creación de certificados digitales en los clientes se debe seleccionar el cliente y en propiedades nos mostrara las opciones para crear un certificado individual previamente antes se debe seleccionar el método de autenticación, así como se muestra en la siguiente figura

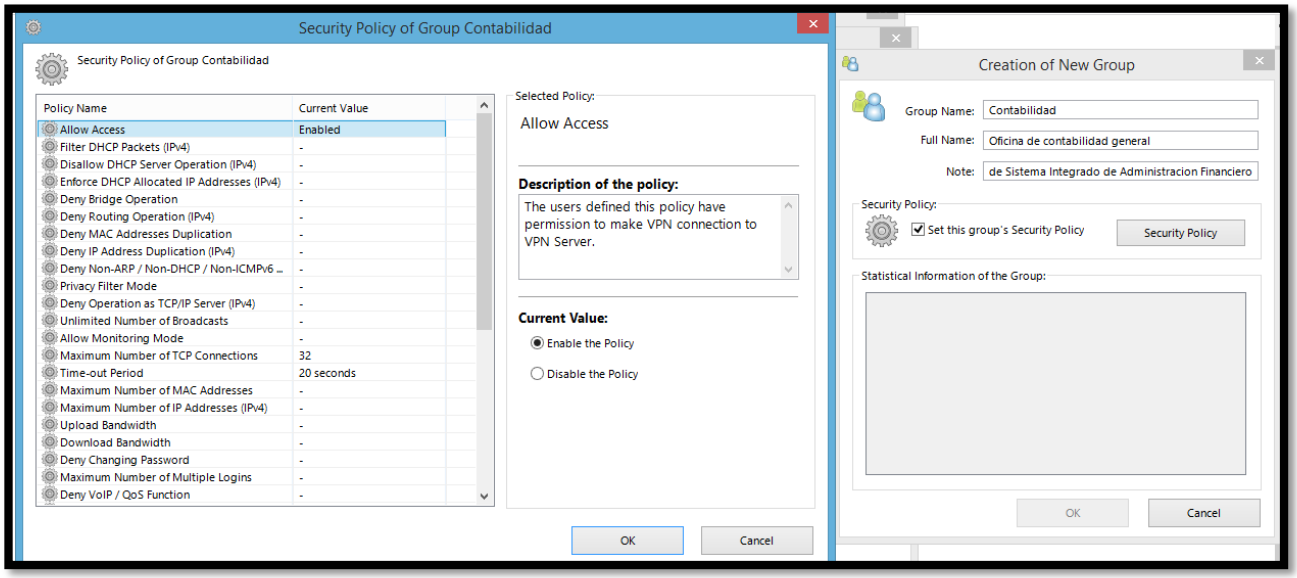


Figura 40: Aplicación de políticas de seguridad al grupo

Se agrega la información referida a cada usuario de acuerdo a los parámetros que son requeridos para la creación del certificado.

Se agrega el número serial en formato hexadecimal diferente para cada usuario y el tiempo de expiración en días, tal como se muestra en la figura N° 36

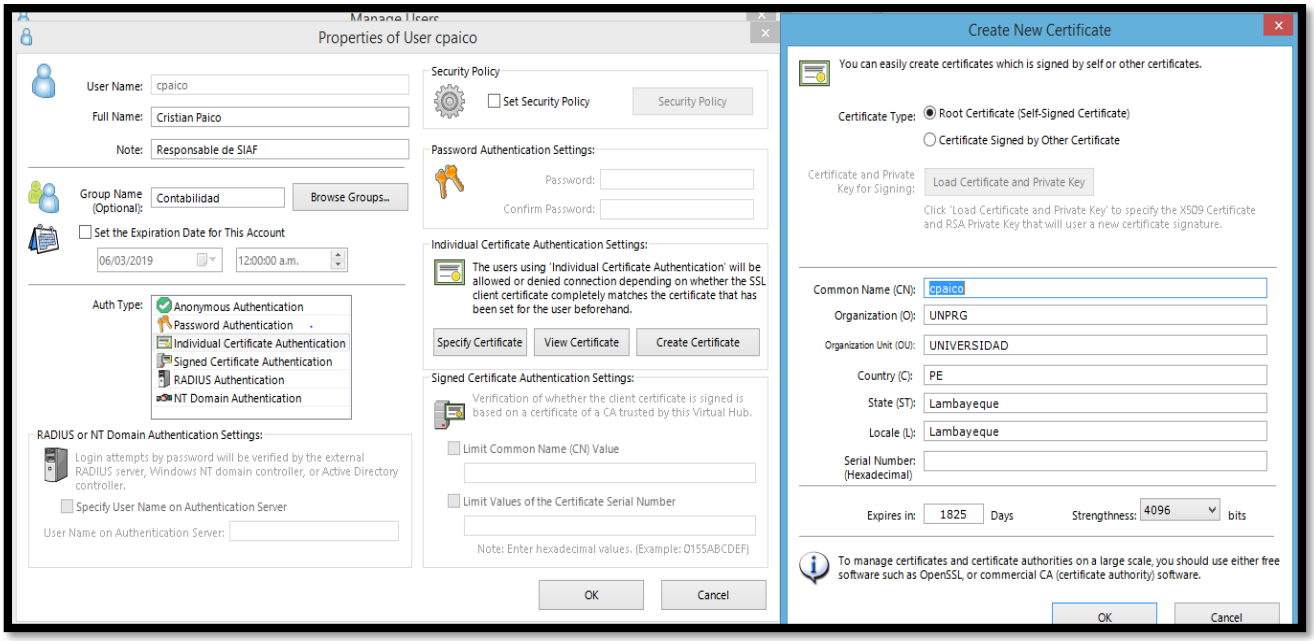


Figura 41: Creación de certificado digital para usuario

Luego se guardan el certificado en método de certificado X509 y PKF generando dos archivos para luego ser importados en los clientes y así poder conectarse al servidor VPN.

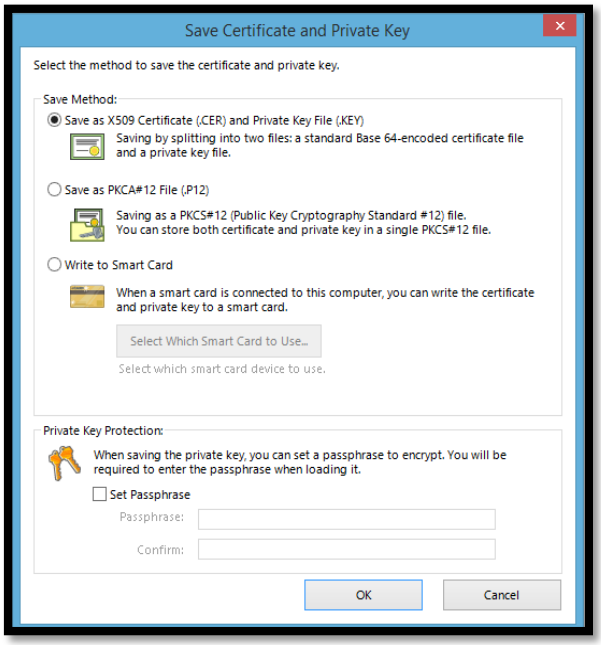


Figura 42: Método de guardado de certificado y llave

Luego de haber creado el certificado digital se puede visualizar y verificar los datos que fueron introducidos anteriormente, como se muestra en la siguiente figura.

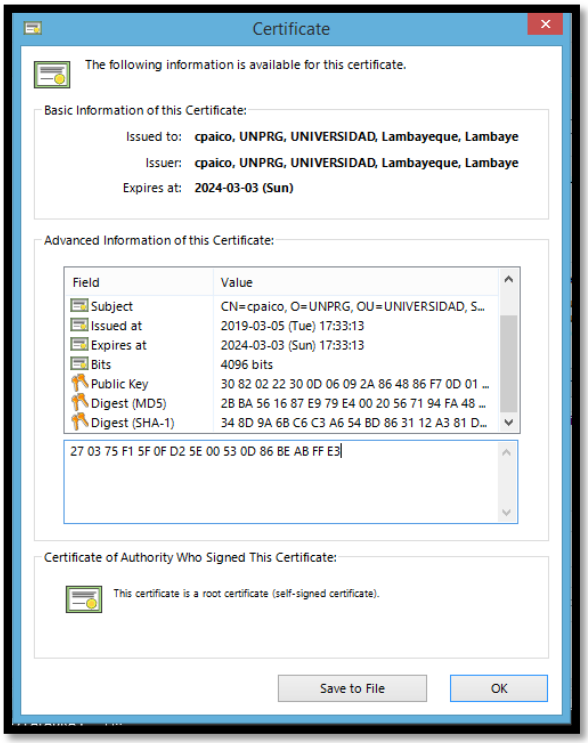


Figura 43: Información del certificado

3.1.6.2.8. Paso N°08: Administración de políticas de seguridad

3.1.6.2.8.1. Creacion de politicas de seguridad

La función de la política de seguridad es una de las funciones sofisticadas del Eje virtual SoftEther servidor VPN que permite que sólo los paquetes que han pasado la inspección y las políticas de contenido de los paquetes a pasar.

3.1.6.2.8.2. Políticas de Acceso Remoto

El área de red telemática es responsable de la creación y asignación de los accesos remotos.

El acceso de conexión remota (VPN), está permitido para los empleados de la organización y consultores externos.

Es de responsabilidad del usuario VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.

Cada nueva conexión (usuario) a la VPN puede efectuarse solo si dicho usuario dispone del acceso a internet y los programas de seguridad y autenticación.

El tráfico de la conexión VPN se encuentra limitado según el perfil de acceso del usuario VPN.

Los usuarios pueden establecer la conexión vía VPN de dos maneras: vía aplicación de cliente o vía aplicación en su celular.

Es el deber del usuario optimizar el uso de los recursos mientras se utilice el túnel VPN.

La máquina de los usuarios deben poseer un antivirus con las últimas huellas actualizadas.

Las estadísticas de la conexión de los usuarios VPN serán auditadas a través de un equipo recolector de Logs ().

3.1.6.2.8.3. El establecimiento de políticas de seguridad para los usuarios y grupos

- Establecer políticas de privacidad para los usuarios

Para el establecimiento de políticas de seguridad en un usuario en específico nos dirgimos a las propiedades del usuario y nos ubicamos en el apartado de “Security policy” como se muestra en la figura N° 39. Habilitamos la casilla y le damos click en el botón de a lado que se nos activará.

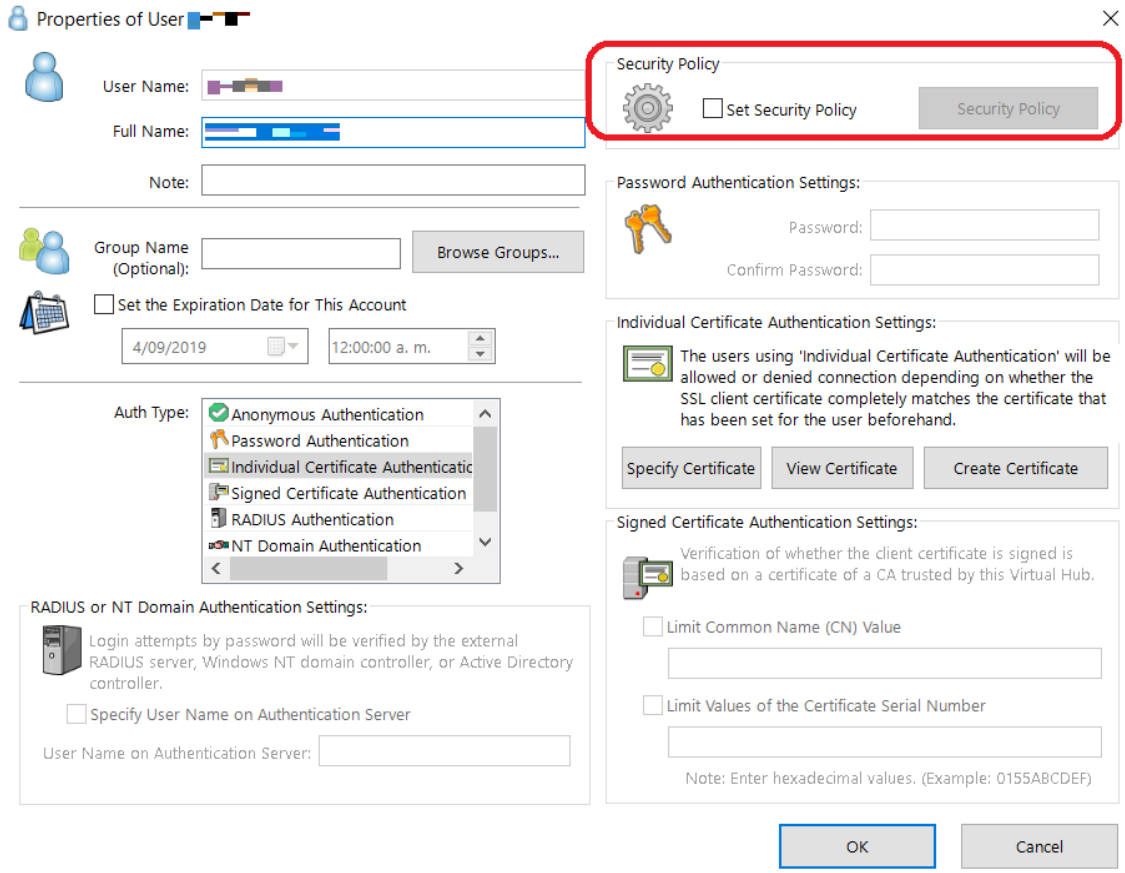


Figura 44: Casilla para ctivación de políticas de seguridad en usuario

A continuación se nos abrirá una nueva ventana (Ver figura N° 40) en la que podremos observar las 38 políticas que nos ofrece el software, las cuales mencionaremos posteriormente.

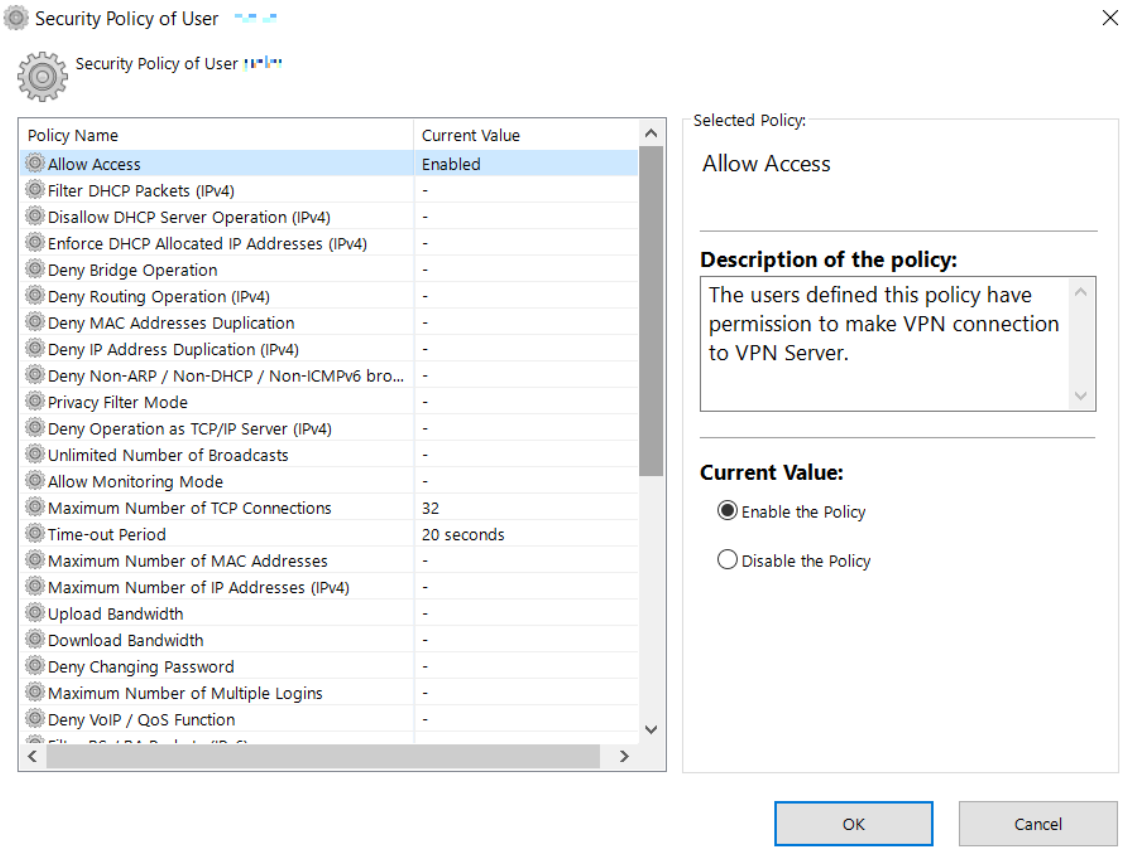


Figura 45: Políticas de Seguridad de usuario

– <u>Establecer políticas de privacidad para los usuarios</u>

Para el establecimiento de políticas de seguridad en un grupo en específico nos dirgimos a las propiedades del grupo y nos ubicamos en el apartado de “Security policy” como se muestra en la figura N° 41. Habilitamos la casilla y le damos click en el botón de a lado que se activará

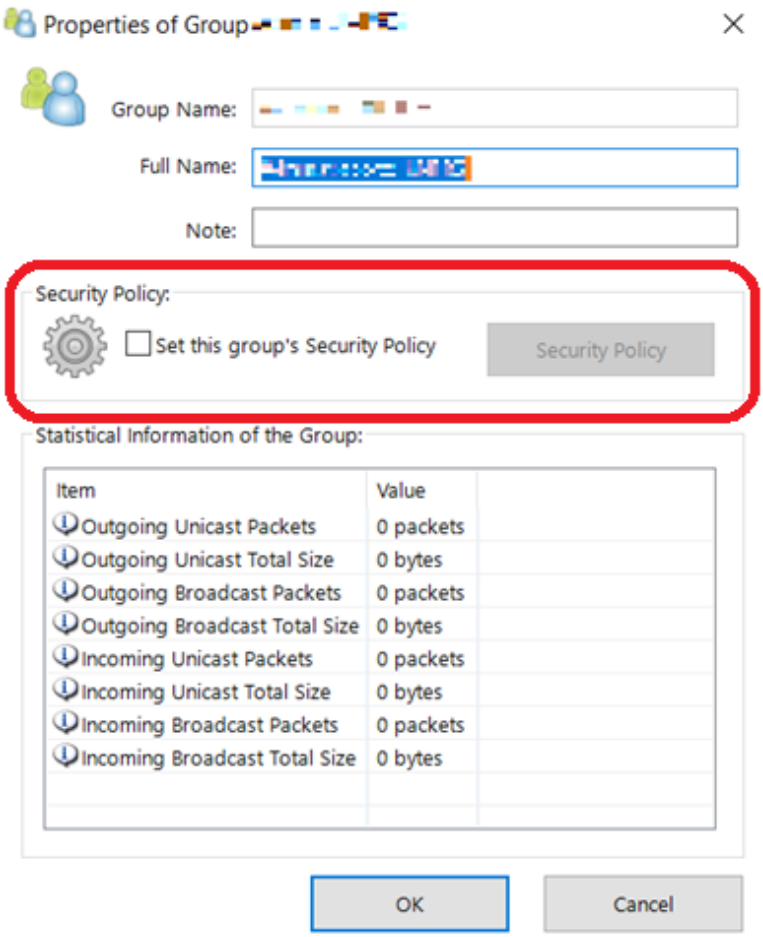


Figura 46: Casilla para ctivación de políticas de seguridad en grupo

Luego de esto se nos abrirá una ventana muy parecida al de la figura N° 40 en la que podremos modificar, habilitar o deshabilitar las políticas existentes, esta vez para todo un grupo de usuarios.

Actualmente existen 38 políticas en las que podemos interactuar y asignar al usuario o grupo en cuestión, estas son:

- Permitir política de acceso
- Filtrar paquetes DHCP (IPv4)
- Rechazar la política de operación del servidor DHCP (IPv4)
- Hacer cumplir las direcciones IP asignada por el DHCP (IPv4)
- Denegar la operación del puente
- Denegar la operación de enrutamiento (IPv4)
- Denegar duplicaión de direcciones MAC
- Denegar duplicación de direcciones IP (IPv4)

- Denegar transmiciones que no sean ARP, DHCP o ICMPv6
- Modo de filtro de privacidad
- Denegar la operación como servidor TCP / IP (IPv4)
- Número ilimitado de Broadcast
- Permitir modo de monitoreo
- Número máximo de conexiones TCP
- Periodo de tiempo de espera
- Número máximo de direcciones MAC
- Número máximo de direcciones IP (IPv4)
- Ancho de banda de subida
- Ancho de banda de descarga
- Denegar el cambio de contraseña
- Número máximo de inicios de sesión múltiples
- Denegar la función VoIP / QoS
- Filtro de RS(*) / Paquetes de RA(**) (IPv6)
- Filtrado de paquetes RA(**) (IPv6)
- Filtrar paquetes DHCP (IPv6)
- Rechazar la política de operación del servidor DHCP (IPv6)
- Denegar la operación de enrutamiento (IPv6)
- Denegar duplicación de direcciones IP (IPv4)
- Denegar la operación como servidor TCP / IP (IPv4)
- Número máximo de direcciones IP (IPv4)
- No permitir guardar contraseña en cliente VPN
- Desconexión automática del cliente VPN
- Filtrar todos los paquetes IPv4
- Filtrar todos los paquetes IPv6
- Filtrar todos los paquetes que no sean IP
- Sin enrutador predeterminado en IPv6 RA(**)
- Sin enrutador predeterminado en IPv6 RA(**) (IPv6 físico)
- VLAN ID (IEEE802.1Q)

(*) RS: Solicitud de router

(**) RA: Aviso de router

3.1.6.2.9. Paso N°09: Pruebas (test)

3.1.6.2.9.1. Levantamiento de reglas en el firewall

Cabe resaltar que para que exista una conexión con el exterior debemos establecer ciertas políticas de negociación con el firewall (en este caso pfsense), las cuales detallamos a continuación:

- Para el NAT

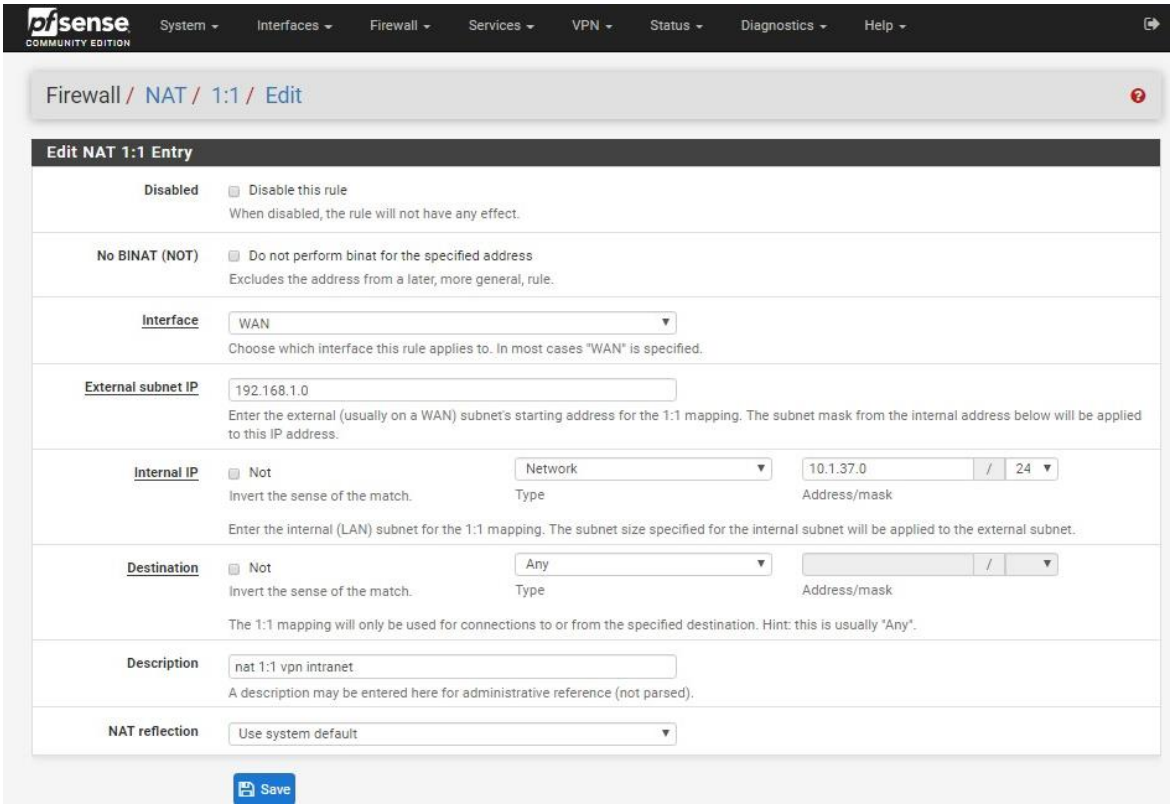


Figura 47: Configuración NAT

– Regla en el firewall

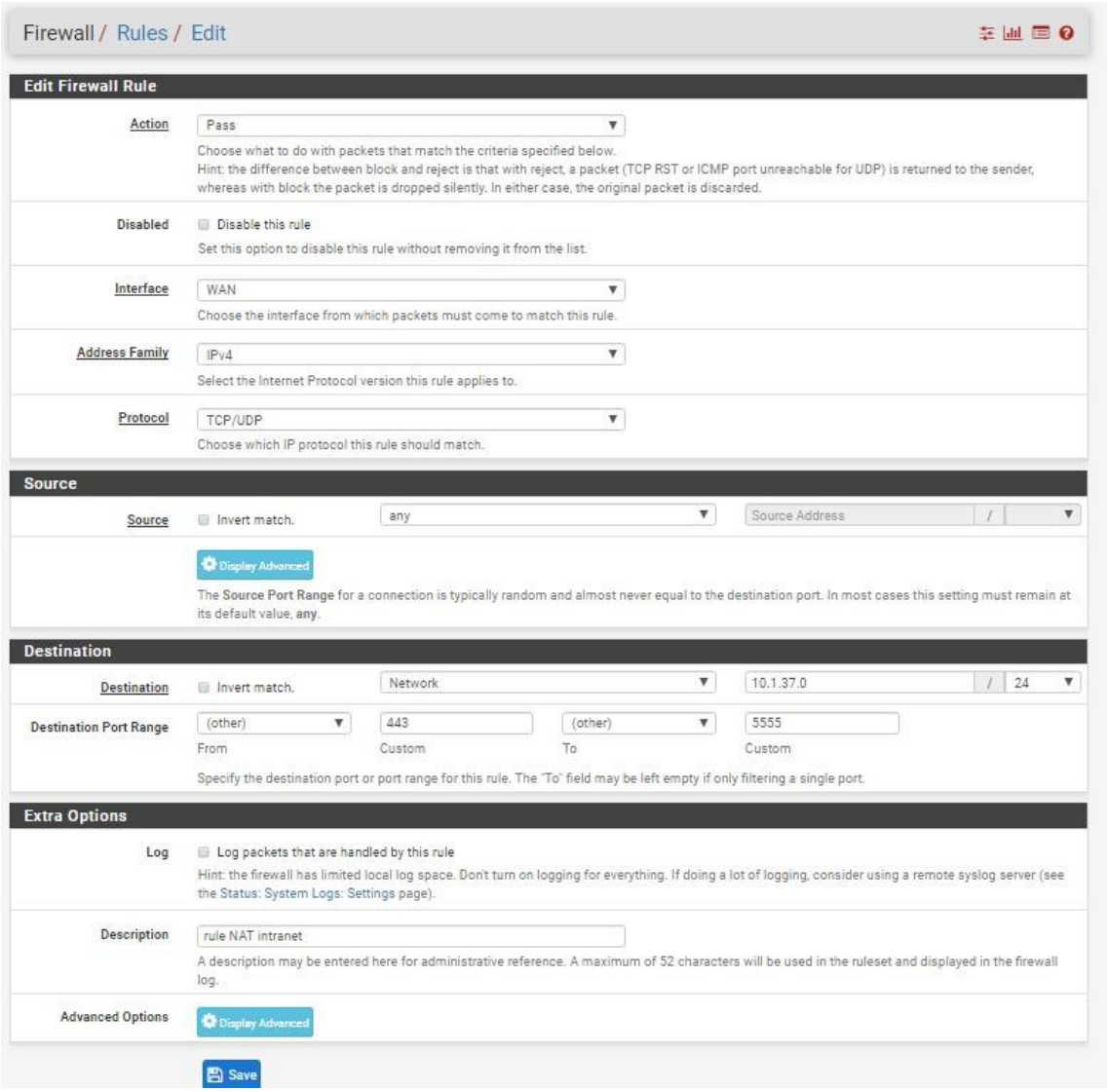


Figura 48: Regla en el firewall

3.1.6.2.9.2. Instalación e inicio de sesión de un usaurio

Siguiendo con el apartado de pruebas los usuarios que trabajarán con la VPN de la UNPRG deben seguir una serie de pasos para la correcta instalación, configuración y ejecución del software, los cuales se detallan a continuación:

1. Descargar el software desde este link:

http://www.softether-download.com/files/softether/v4.29-9680-rtm-2019.02.28-tree/Windows/SoftEther_VPN_Client/softether-vpnclient-v4.29-9680-rtm-2019.02.28-windows-x86_x64-intel.exe

2. Instalar el software como administrador:
    a. Click en siguiente

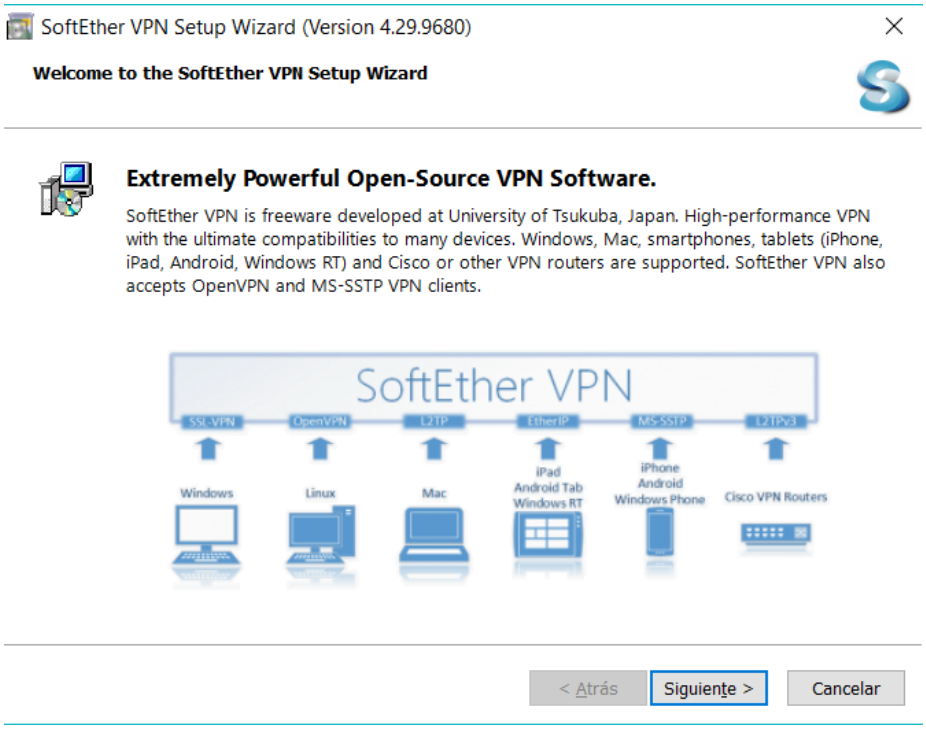


Figura 49: Bienvenida al wizard de Softether VPN

b. Click en SoftEther VPN Client, luego siguiente:

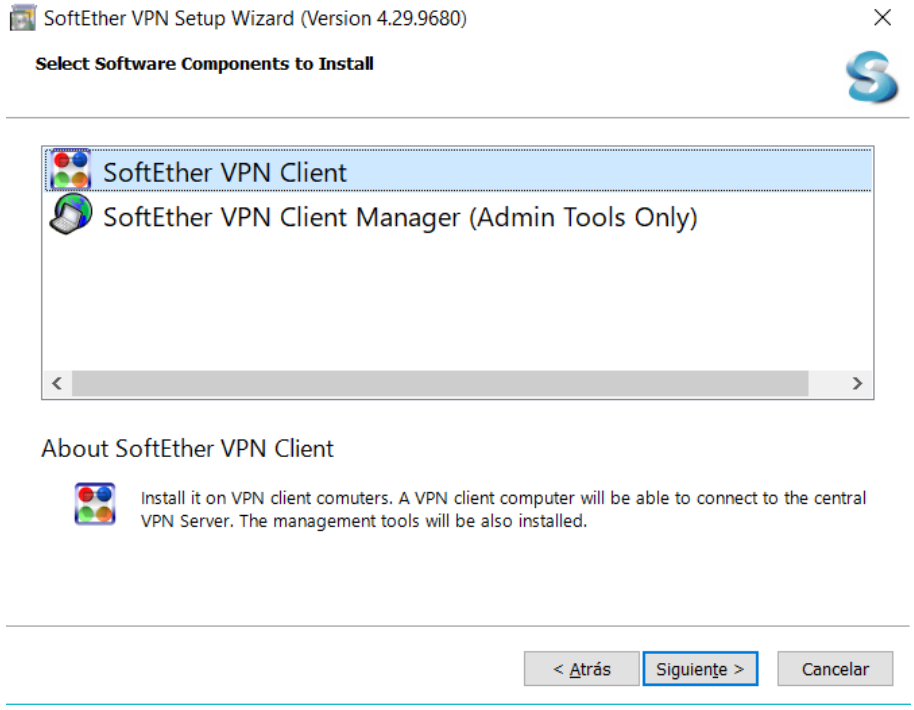


Figura 50: Selección del componente a instalar

c. Damos click en la palomilla para la licencia, luego siguiente:

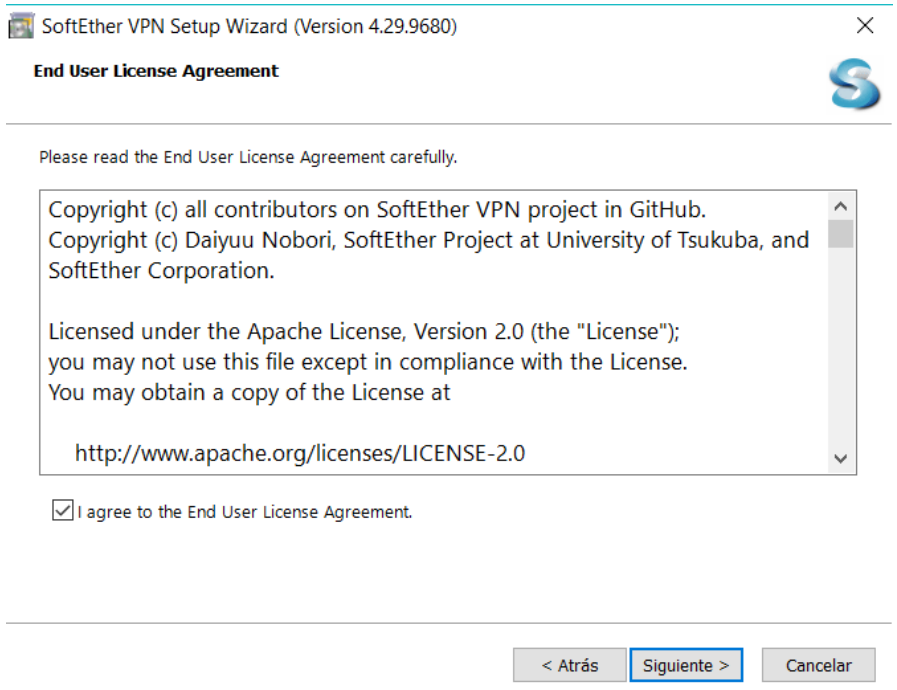


Figura 51: Aceptar los términos de la licencia

d. Siguiente otra vez:

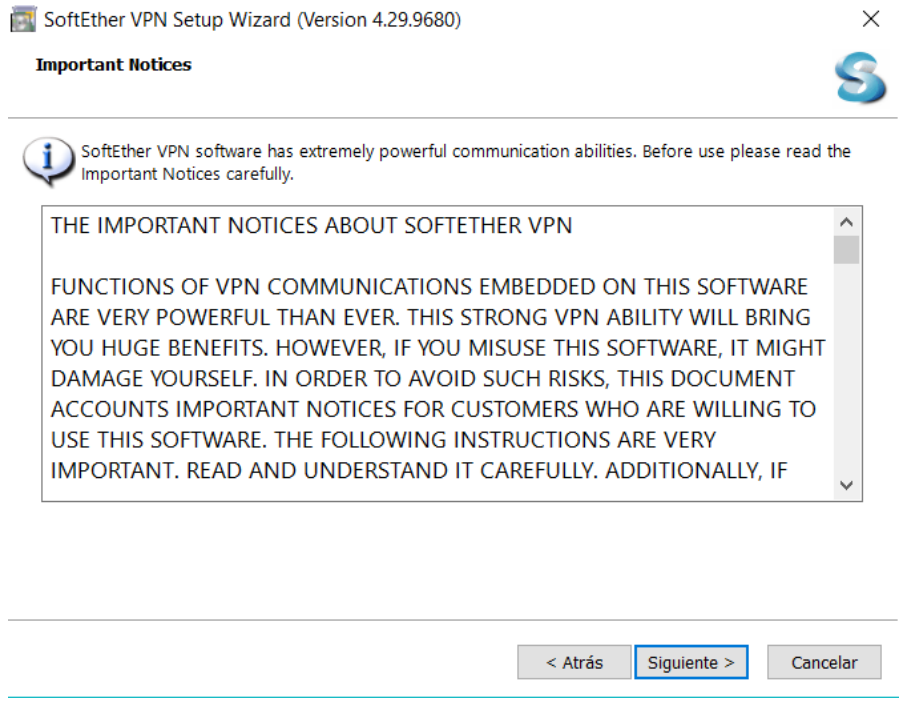


Figura 52: Información sobre el software a instalar

e. Dejamos en el directorio por defecto:

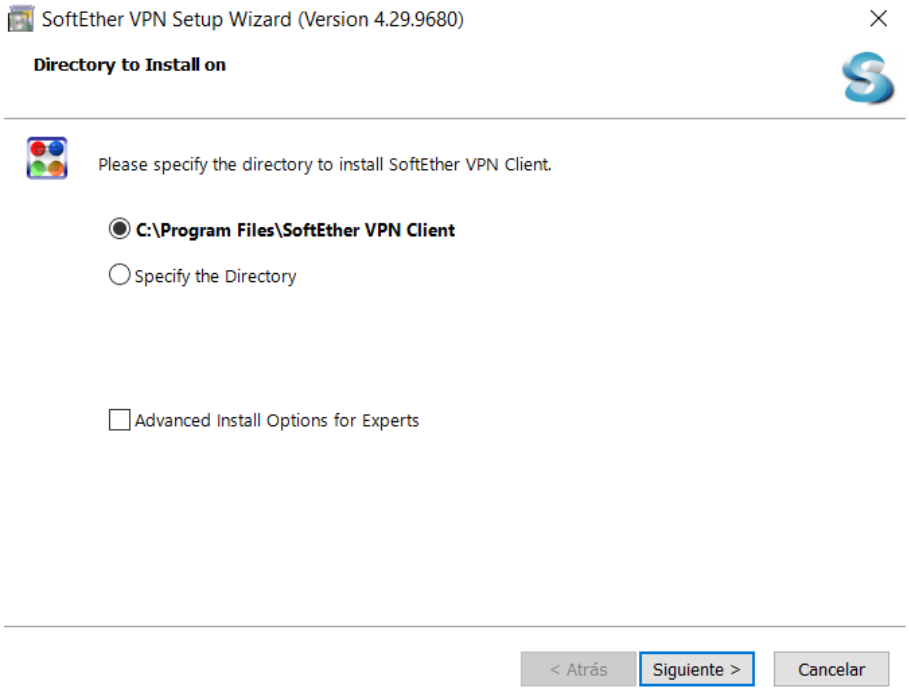


Figura 53: Directorio en el que se instalará el programa

f. Instalamos dando click en siguiente:

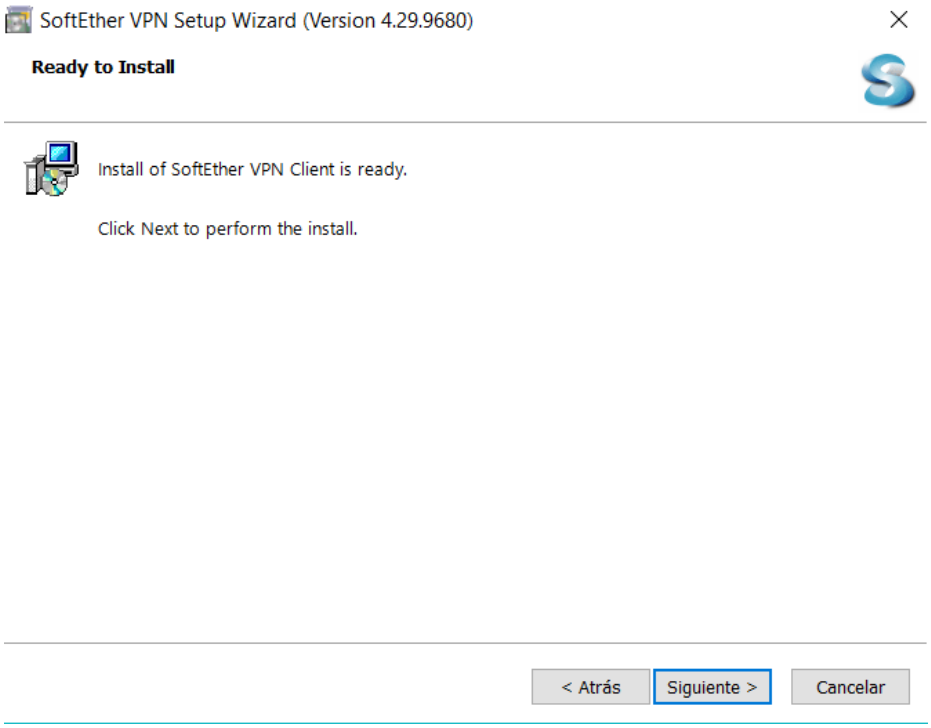


Figura 54: Confirmación final para el incio de la instalación

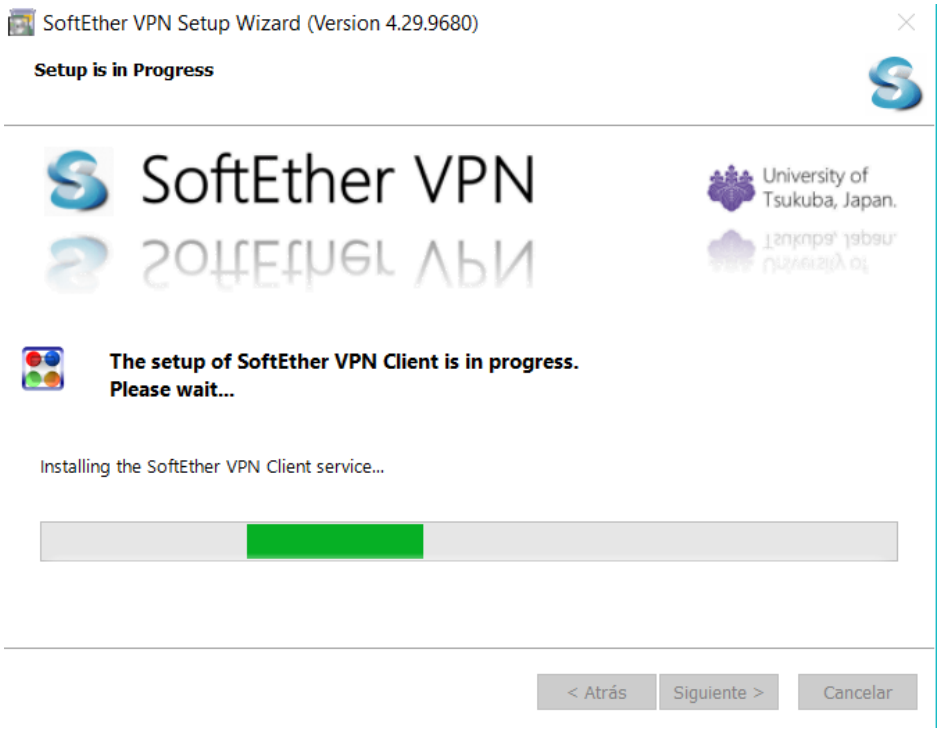


Figura 55: Progreso de la instalación

g. Para inciar el software dejamos activado el check y solo damos click en “Finalizar”:

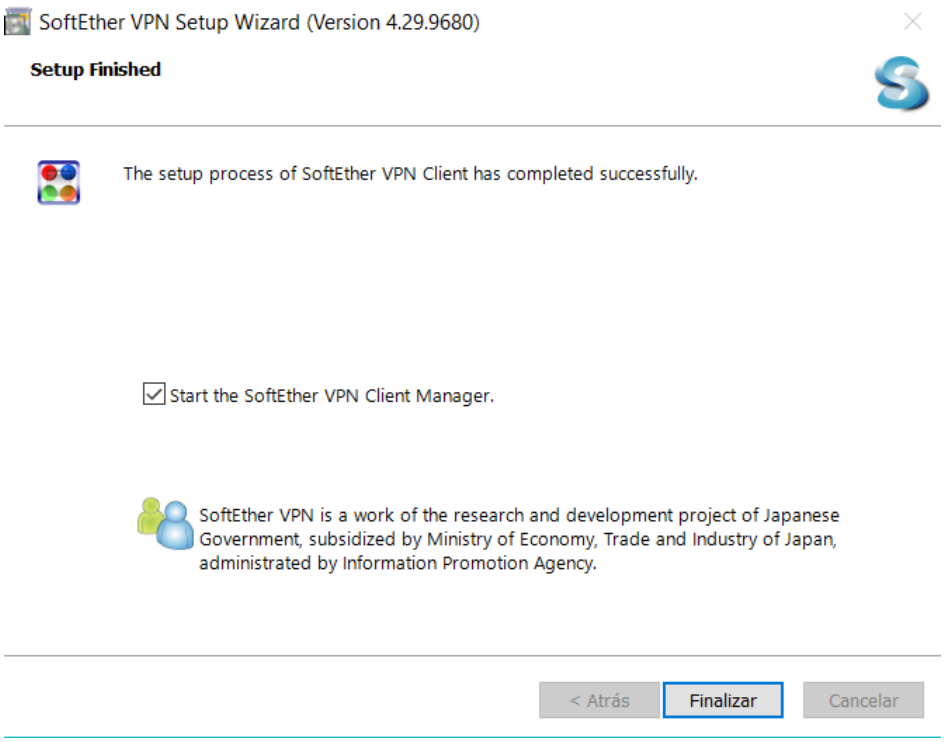


Figura 56: Finalización de la instalación del software

3. NOTA: Si ya está creado un adaptador virtual salte al paso 4

   Agregamos un adaptador virtual, dando doble click en “Add VPN Connection”.

   Luego damos click en Sí.

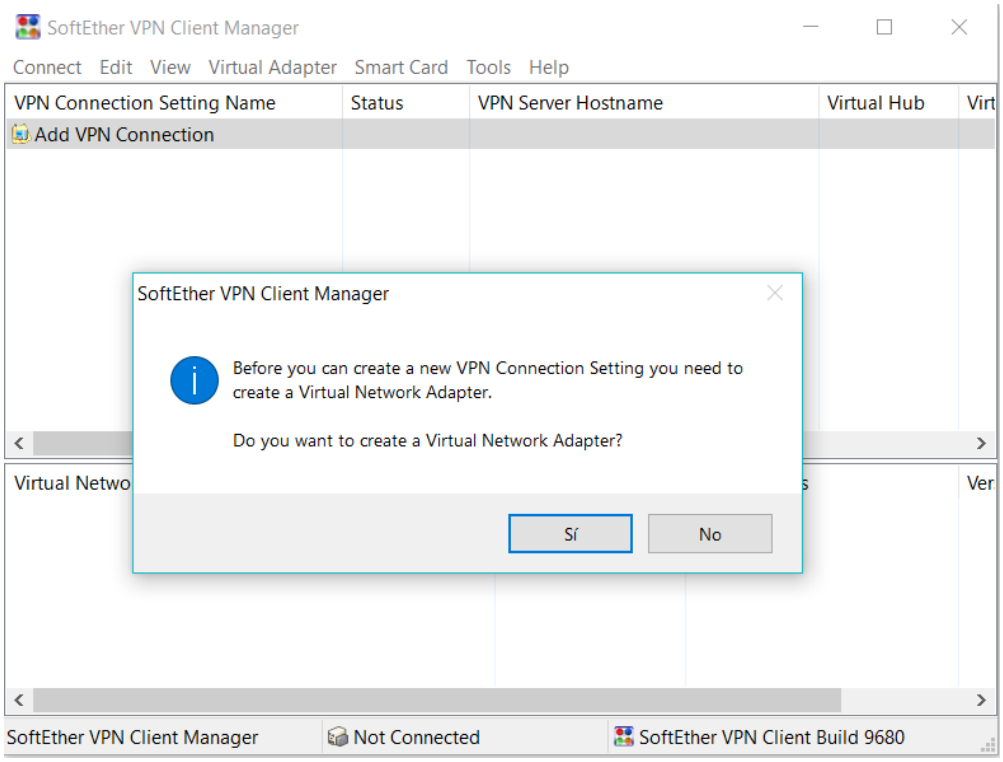


Figura 57: Inicio del programa Softether VPN Client Manager

Luego damos click en OK para agregar el adaptador virtual (No modifique el nombre del adaptador virtual)

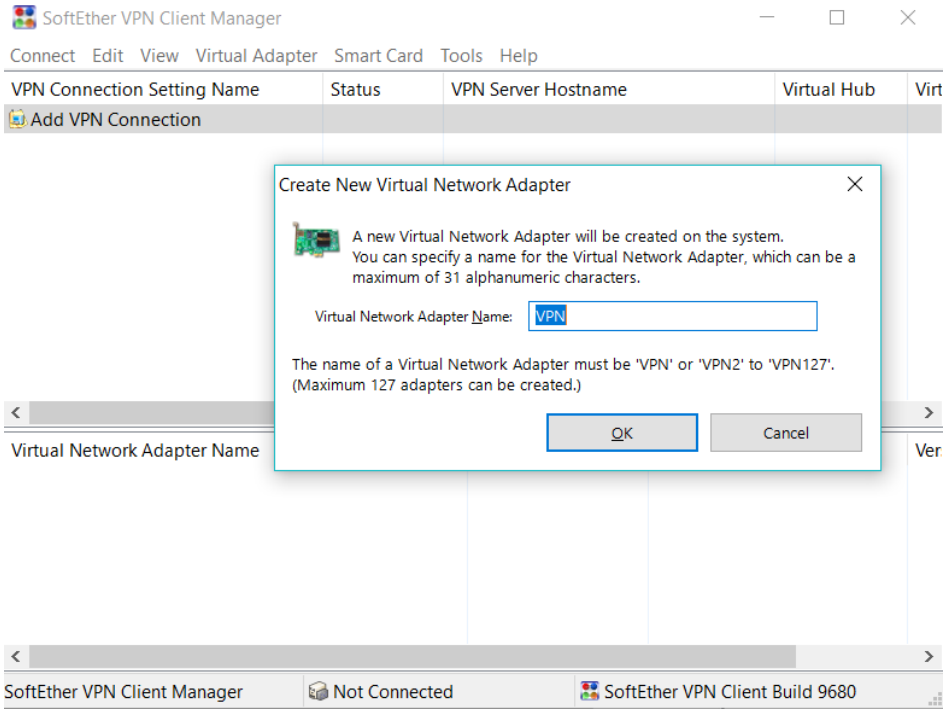


Figura 58: Creación del adapatador virtual

4. Hacemos doble click en “Add VPN Connection”. Aquí se mostrará esta ventana:

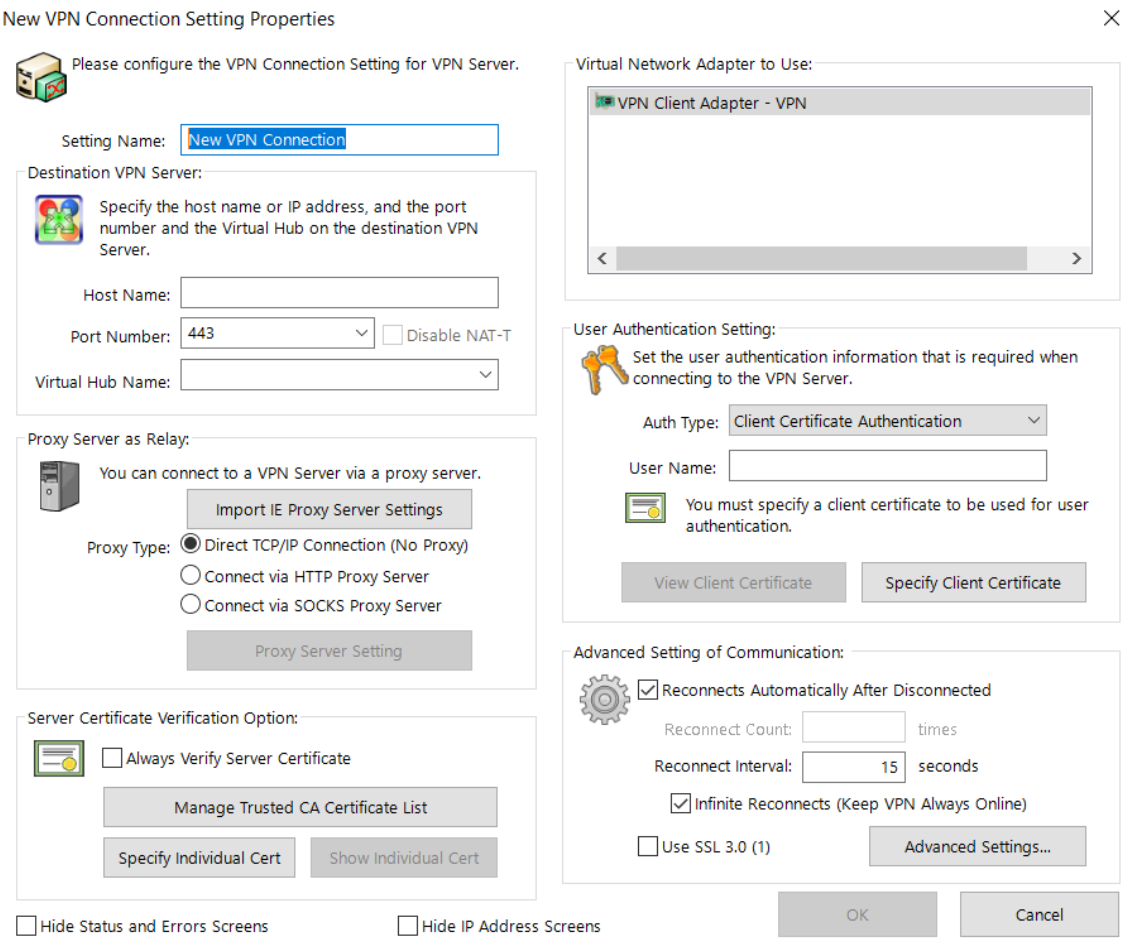


Figura 59: Propiedades y datos acerca de la nueva conexión

Lo rellenaremos con la siguiente información:

- Setting Name: Nombre de conexión, a su gusto
- Host Name: vpn.unprg.edu.pe
- Port Number: 443 (por defecto)
- Virtual Hub Name: Seleccionamos el virtual hub que le fue proporcionado por el administrador de TI. (Por favor no lo escriba manualmente.)

En el apartado de User Authentication Setting:

- Auth Type: Seleccione “Client Certificate Authentication”

– User Name: Digite el nombre de usuario proporcionado en su correo electrónico.

– Specify Client Certificate: Seleccione primero el certificado que se le envió a su correo (.CER) y luego la llave (.KEY)

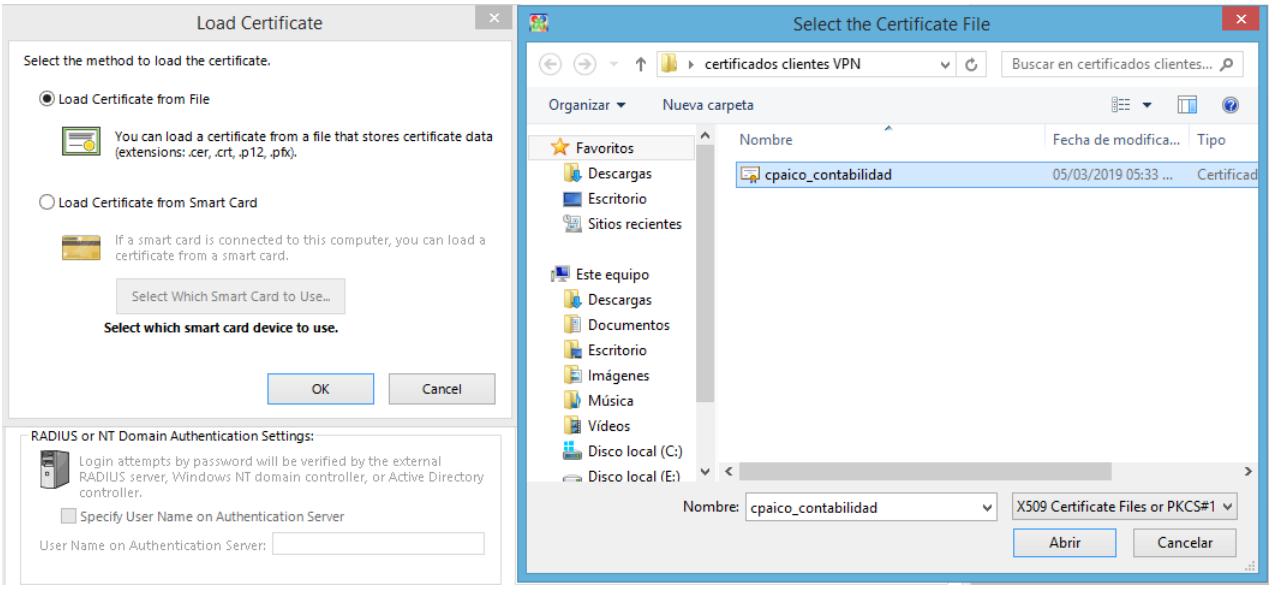


Figura 60: Ingreso de certificado y llave del usuario

Adicionalmente se le pedirá una frase "Passphrase" la cual es usada como protección a la llave antes proporcionada. Si no es añadido en su correo consulte con el administrador de TI.

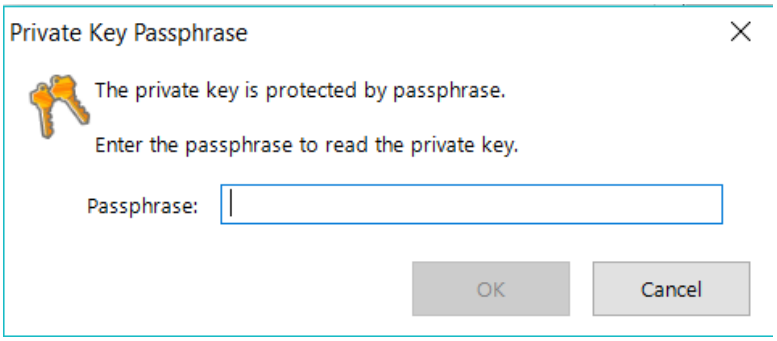


Figura 61: Igreso de la frase contraseña de la llave privada

Seguidamente hacemos click en OK para cerrar la ventana y guardar los cambios

5. Finalizado el paso anterior hacemos doble click en la nueva conexión para conectarse.

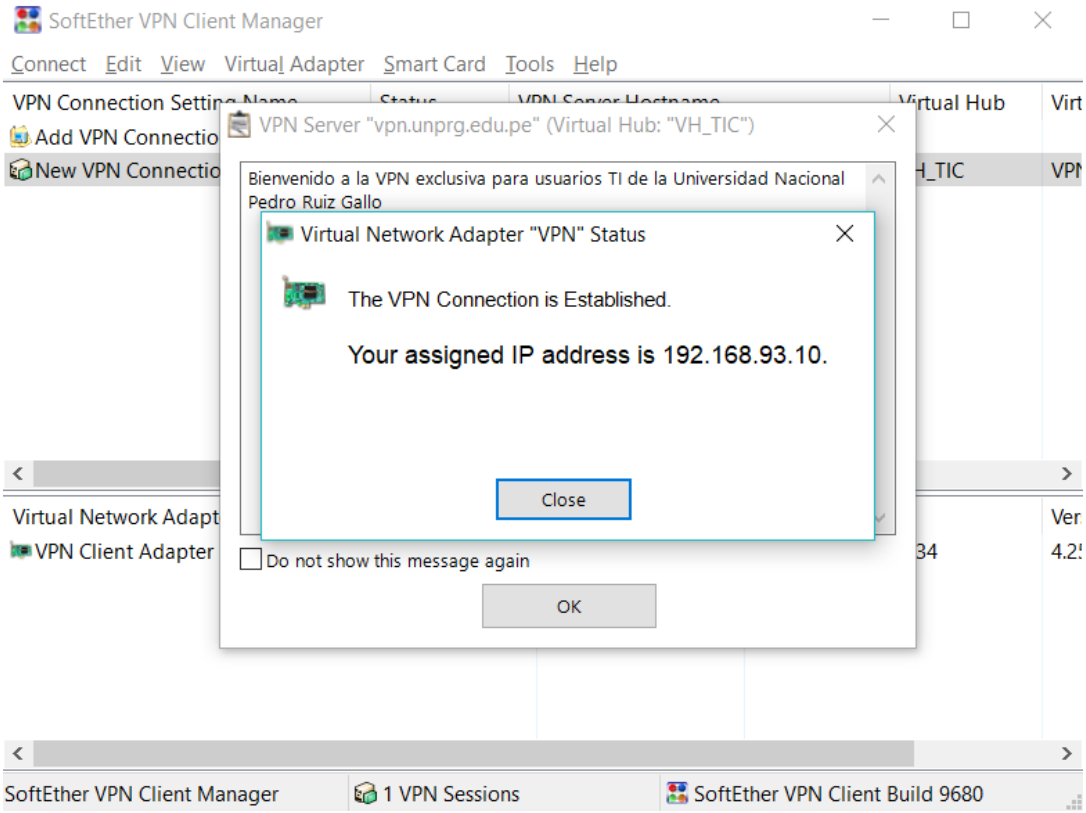


Figura 62: Ingreso y asignación de IP

3.1.6.2.10. Actividad N°10: Monitoreo

3.1.6.2.10.1. Análisis de resultados usando Wireshark

Para la validación de la seguridad en el esquema planteado en la presente tesis se ha necesitado la ayuda del software Wireshark y poder realizar la captura de los paquetes de la conexión de VPN entre el servidor y el cliente, para luego así visualizar las capturas de paquetes y analizar el trafico respectivo de los equipos de comunicación involucrados en el diseño.

Durante la prueba se establecieron las conexiones desde un cliente VPN hacia el servidor, previo a ello se verificaron la comunicación entre ambos dispositivos por medio de ping.

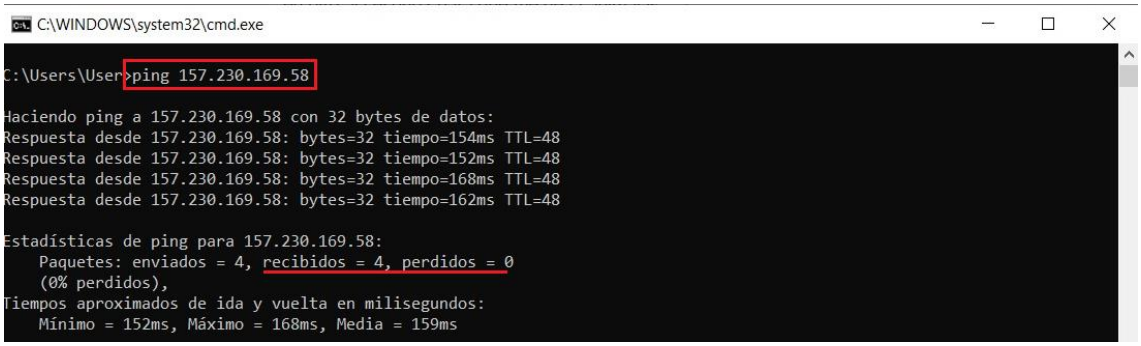


Figura 63: Ping al servidor donde está alojado la VPN

Se trabajó en 2 etapas: Captura de datos sin encriptación y captura de datos con encriptación.

- Captura de datos sin encriptación

Figura 64: Captura de datos sin encriptación

En la captura de datos sin encriptación se observa como los datos que viajan a través de la red no son seguras y pueden ser vulnerados por cualquier persona.

- Captura de datos con encriptación

Ahora, al implementar la VPN en los equipos, establecemos una nueva conexión entre el cliente y el servidor VPN y volvemos a realizar una captura con el programa wireshark, Esta vez habilitado el protocolo de Ipsec y certificado de seguridad.

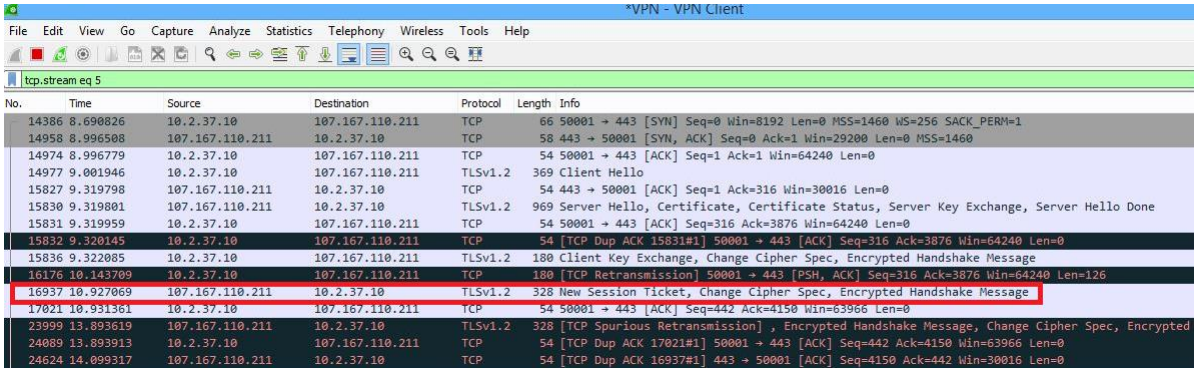


Figura 65: Registro de conexión capturado a través de wireshark

A partir de la captura se puede apreciar que la encriptación de los paquetes es funcional, la cual se procedió abrir el paquete para comprobar. Dando como resultado la siguiente imagen.

Figura 66: Captura de datos con encriptación

Como se puede apreciar la encriptación es exitosa y los datos que viajan por el túnel IPSec de nuestra VPN son protegidos durante la transmisión de los mismos.

Entonces con el análisis de los resultados arrojados por el software es que se comprueba que nuestra VPN logra una conexión optima además de encriptar todo el tráfico que fluya por ella.

2019

CAPÍTULO IV

CONCLUSIONES

Conclusiones

- Al analizar la situación actual de la universidad ,se logró recopilar información a través de entrevistas a las personas encargadas de las áreas más críticas en cuanto a función administrativa de la UNPRG, lo que nos llevó a proponer el uso de una VPN de bajo presupuesto
- Se lograron determinar los requerimientos de hardware y software para realizar una correcta implementación de la VPN haciendo uso de software libre que ofrecen seguridad y compatibilidad.
- Se diseñó la topología física y lógica teniendo en cuenta criterios de seguridad y acceso rápido.
- Se elaboró el presupuesto de los equipos que se requirieron y se plantearon los pasos a seguir para una implementación correcta.
- Se realizó la evaluación de retorno de inversión del presupuesto haciendo uso del VAN, TIR y PR concluyendo que el proyecto es viable para su implementación.
- Se demostró la implementación de la VPN a través de una simulación para la optimización de la gestión de aplicaciones de la intranet de la UNPRG, obteniéndose buenos resultados.
- Se demostró la seguridad e integridad de los datos por la VPN para garantizar la confidencialidad y disponibilidad de los mismos.

2019

CAPÍTULO V

RECOMENDACIONES

Recomendaciones

- Para reducir costos, recomendamos utilizar la función DDNS proporcionada por el mismo software, ya que aparte de brindar seguridad, el nombre es modificable siempre y cuando se mantenga la terminación ".softether.net"
- Por obvias razones de conocimiento informático, no está demás recomendar el uso del software administrador del server VPN por un experto en el campo de redes informáticas.
- Se recomienda usar el software "Softether VPN Server Manager" en un sistema operativo de entorno gráfico como windows 7 o superior, para mayor interactividad y evitar el uso de comandos, a no ser que el administrador conozca a fondo el programa.
- Para el uso de los clientes, se recomienda el uso de la herramienta "Softether VPN Client Manager", por ser una herramienta con entorno gráfico, de fácil acceso y con un poderoso sistema de encriptación
- Para una mejor administración de la VPN se recomienda crear un virtual hub para cada dependencia u oficina de la UNPRG
- Si el nateo se logra hacer por medio de un firewall externo, entonces recomendamos activar la función DHCP virtual sin el secureNAT
- Se recomienda a la UNPRG la adquisición de equipos de red con mayores características técnicas para un desempeño optimo de la red.
- Se exhorta a hacer uso del tipo de autenticación por certificados para las conexiones de los clientes hacia la VPN, ya que tienen mayor seguridad que un simple usuario y contraseña.

BIBLIOGRAFÍA

Implementación de una VPN con Open Source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo

BIBLIOGRAFÍA

Cardona, A. M. (2003). DISEÑOS CUASIEXPERIMENTALES.

cisco . (s.f.). *itesa.edu.mx*. Obtenido de http://www.itesa.edu.mx/netacad/networks/course/module6/6.1.2.2/6.1.2.2.html

Cisco. (Febrero de 2006). *¿Qué solución VPN es la adecuada para usted?* Obtenido de https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14147-which-vpn.html

Cisco. (Noviembre de 2013). *Cisco Community.* Obtenido de https://community.cisco.com/t5/security-documents/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502

Cisco Services. (2006). *El Mundo está Cambiando.¿Está su Red Lista?* Obtenido de https://www.cisco.com/c/dam/global/es_mx/assets/serviciospartners/otros_archivos/pdf/brochure lcsps_esp2006.pdf

Cisco Systems. (13 de Octubre de 2008). *Cisco Systems*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Cloud, O. (s.f.). *Oracle Cloud Infrastructure Documentation*. Obtenido de https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/overviewIPsec.htm

DigiCert® Inc. (s.f.). *Digicert*. Obtenido de https://www.digicert.com

González Valenzuela, A. (28 de Julio de 2014). *Universidad Técnica Federico Santa María.* Valparaiso: Universidad Técnica Federico Santa María.

Hernández H, H. (2009). *Diseño de una red privada virtual para el acceso remoto a la información de la empresa American Jeans de ambato desde la empresa super exitos de Guayauil*.

IBM®. (2010). *https://www.ibm.com*. Obtenido de https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.halz002/security_ipsec_vpn.htm

isaca.org. (2014). Obtenido de https://m.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2014%20-%20Exposición%202%20CIGRAS%20ISO%2027001%20-%20rbq.pdf

isotools.org. (s.f.). *Aspectos clave de su diseño e implantación*. Obtenido de https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Microsoft. (9 de Diciembre de 2009). *Microsoft Corporation.* EE.UU.: Microsoft Press. Obtenido de Microsoft Corporation Web site.

Morales, A. G. (2006). *Redes Privadas Virtuales.* Colombia.

Nacional, C. C. (julio de 2017). *Guía de Seguridad de las TIC.* Obtenido de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html

OpenVPN. (2015). Obtenido de OpenVPN community: https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn

Roldan, F. Z. (julio de 2017). *Guía de Seguridad de las TIC.* Obtenido de Guía de Seguridad de las TIC: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html

SoftEther . (enero de 2019). *SoftEther VPN Project*. Obtenido de https://www.softether.org

SW Hosting. (2 de Octubre de 2014). *SW Hosting*. Obtenido de https://www.swhosting.com

wireguard. (2015). *wireguard.com.* Obtenido de https://www.wireguard.com

ANEXOS

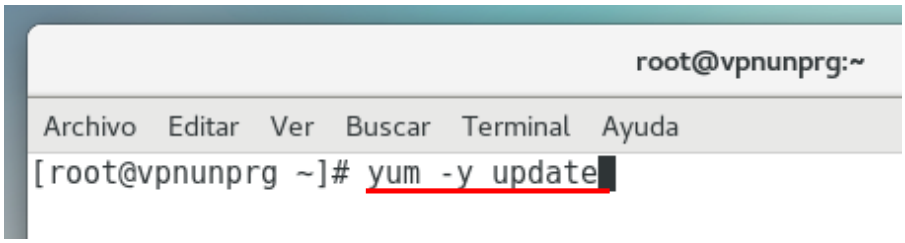
Implementación de una VPN con Open Source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo

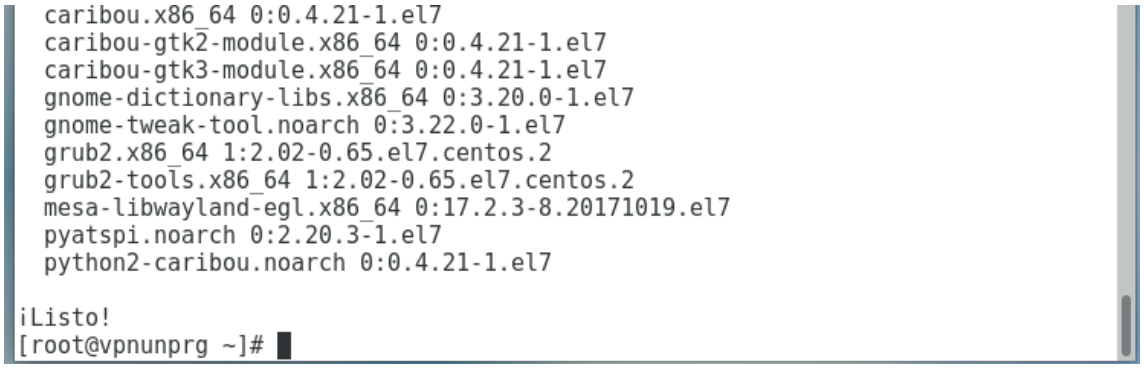
Anexos

Anexo N° 1

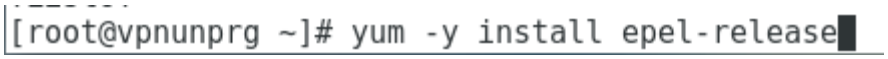
Instalación de SoftEther Server VPN en Centos 7

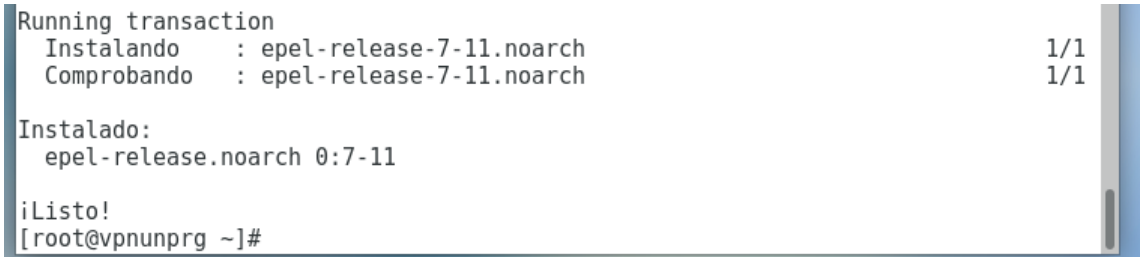
Primero, empezamos verificando si existen actualizaciones en Centos 7 y de ser así las instalamos con el siguiente comando:





Terminado de instalar todas las actualizaciones, ahora procedemos a instalar los paquetes adicionales para Linux Empresarial o EPEL hallados hasta la fecha con el siguiente comando:





Ahora instalamos un grupo de paquetes de herramientas de desarrollo o “Development Tools” en el cual se encuentra programas que son necesarios para compilar software o construir nuevos archivos, entre ellos está “make” el cual utilizaremos más adelante

```
[root@vpnunprg ~]# yum -y groupinstall "Development Tools"
```

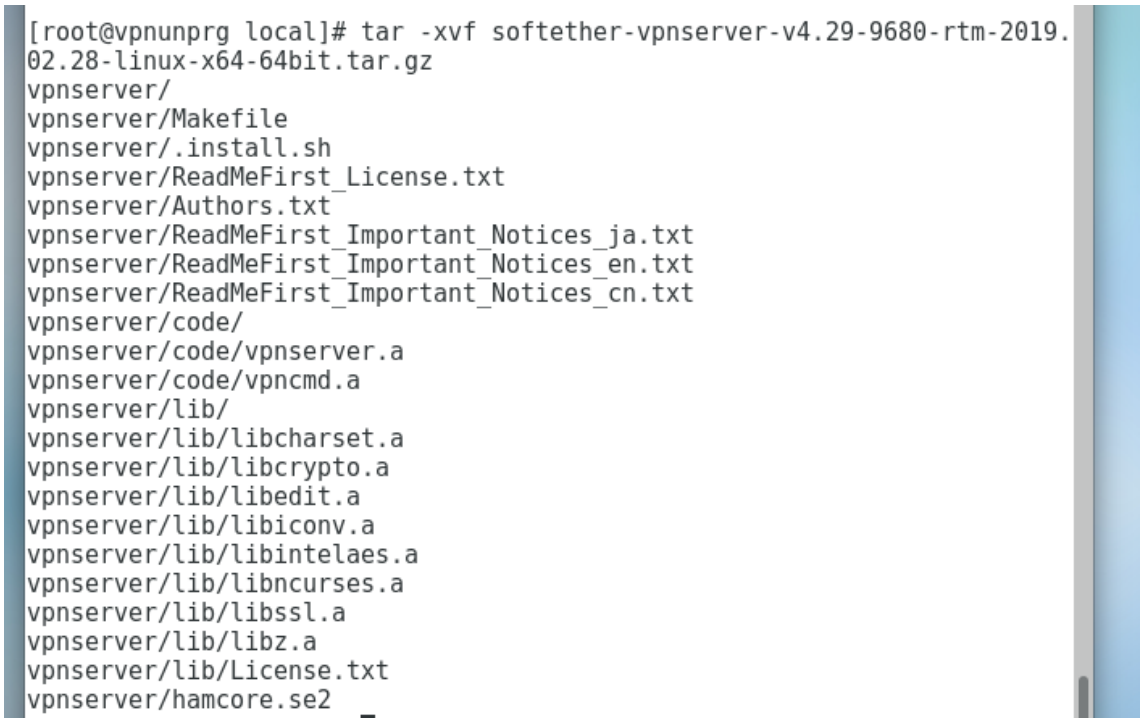
```
  perl-TermReadKey.x86_64 0:2.30-20.el7
  perl-Test-Harness.noarch 0:3.28-3.el7
  perl-Thread-Queue.noarch 0:3.02-2.el7
  perl-XML-Parser.x86_64 0:2.41-10.el7
  perl-srpm-macros.noarch 0:1-8.el7
  subversion-libs.x86_64 0:1.7.14-14.el7
  systemtap-client.x86_64 0:3.3-3.el7
  systemtap-devel.x86_64 0:3.3-3.el7

¡Listo!
[root@vpnunprg ~]#
```

Ahora nos ubicamos en el directorio “/usr/local” y seguidamente en esa ubicación descargamos el archivo de instalación de SoftEther VPN Server desde la página oficial haciendo uso del comando wget:

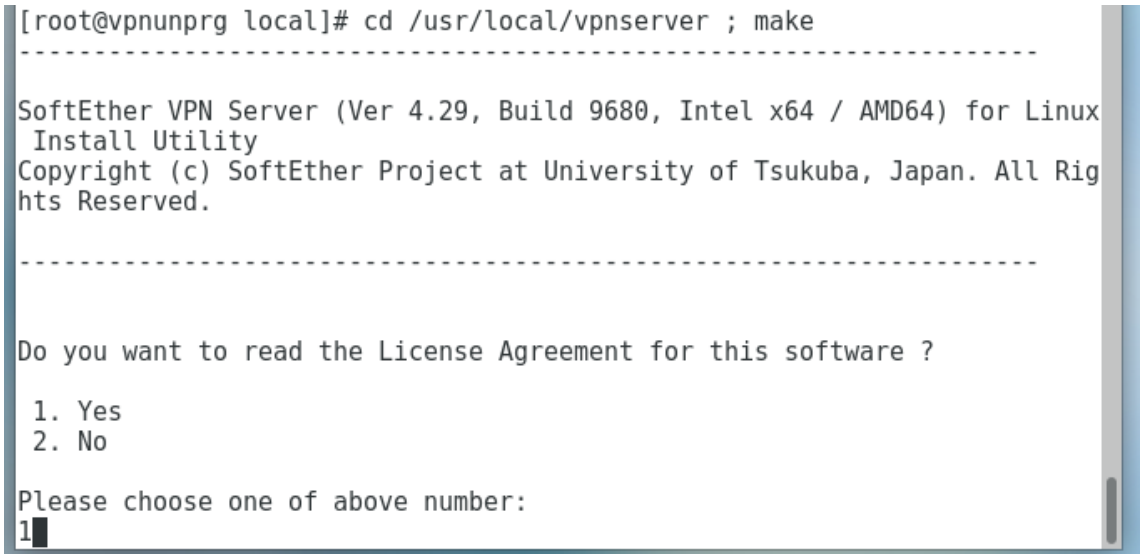
```
[root@vpnunprg ~]# cd /usr/local
[root@vpnunprg local]# wget -c http://www.softether-download.com/files/softether
/v4.29-9680-rtm-2019.02.28-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_
AMD64/softether-vpnserver-v4.29-9680-rtm-2019.02.28-linux-x64-64bit.tar.gz
```

```
Conectando con www.softether-download.com (www.softether-download.com)[130.158.7
5.49]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 6249245 (6,0M) [application/x-gzip]
Grabando a: “softether-vpnserver-v4.29-9680-rtm-2019.02.28-linux-x64-64bit.tar.g
z”

100%[======================================>] 6.249.245   1,14MB/s   en 5,2s

2019-03-01 12:03:05 (1,14 MB/s) - “softether-vpnserver-v4.29-9680-rtm-2019.02.28
-linux-x64-64bit.tar.gz” guardado [6249245/6249245]

[root@vpnunprg local]#
```

Luego de esto extraemos el archivo descargado en ese mismo directorio con la ayuda del comando “tar” de la siguiente manera:



Finalmente, para terminar de instalar SoftEther, una vez extraído el archivo lo tenemos que compilar, asi que nos dirigirnos al nuevo directorio creado y usamos el comando “make”, seguidamente aceptamos las licencias para el uso del software.



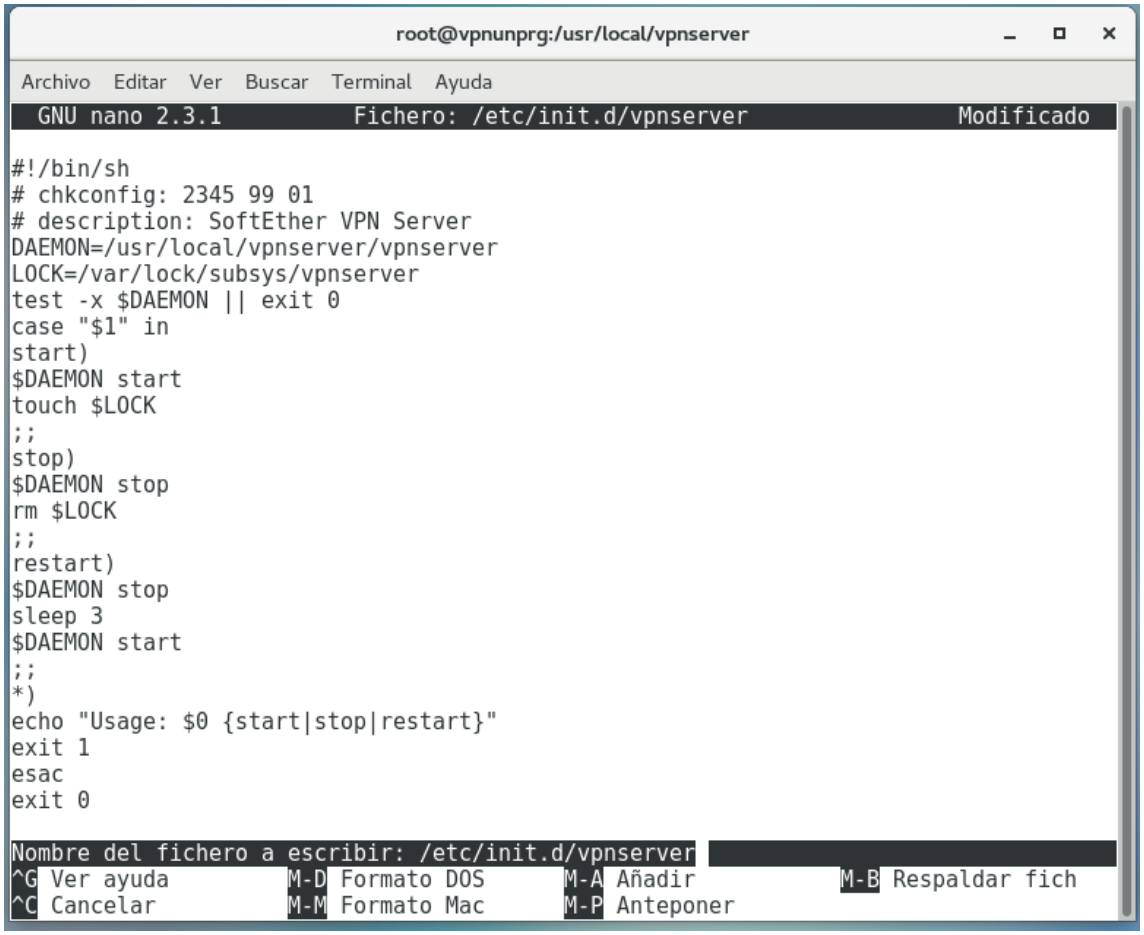
```
READ AND UNDERSTAND THE 'src/WARNING.TXT' FILE BEFORE USING THIS SOFTWAR
E. SOME SOFTWARE PROGRAMS FROM THIRD PARTIES ARE INCLUDED ON THIS SOFTWA
RE WITH LICENSE CONDITIONS WHICH ARE DESCRIBED ON THE 'src/THIRD_PARTY.T
XT' FILE.


Did you read and understand the License Agreement ?
(If you couldn't read above text, Please read 'ReadMeFirst_License.txt'
 file with any text editor.)

 1. Yes
 2. No

Please choose one of above number:
1
```

```
Did you agree the License Agreement ?

1. Agree
2. Do Not Agree

Please choose one of above number:
1
```

Una vez instalado haremos que se ejecute automáticamente en el inicio, para lograr esto, tendremos que crear un script en el directorio “etc/init.id/” de nombre “vpnserver”

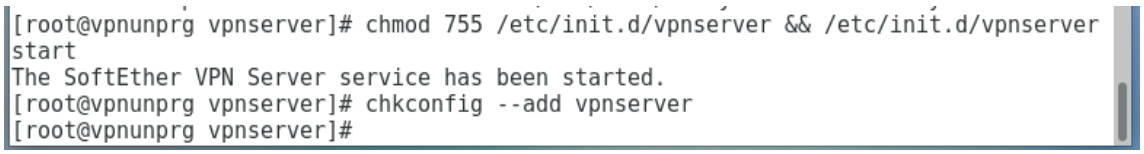
```
s versions. It helps you to completely and easily manage the VPN server services
running in remote hosts.

----------------------------------------------------------------------

make[1]: se sale del directorio `/usr/local/vpnserver'
[root@vpnunprg vpnserver]# nano /etc/init.d/vpnserver
```

En ese archivo pegaremos una serie de comandos que permitirá al sistema operativo hacer que el servicio VPN se ejecute desde el inicio. Estos comandos son los siguientes:



Le damos los permisos de lectura, escritura y ejecución para el propietario y solo de lectura y ejecución para los demás usuarios al archivo “vpnserver” ubicado en el siguiente directorio: “/etc/init.d/vpnserver”, seguidamente lo ejecutamos añadiendo un espacio y la palabra start.

En la siguiente línea usamos “chkconfig” con la opción --add para crear los enlaces simbólicos necesarios.

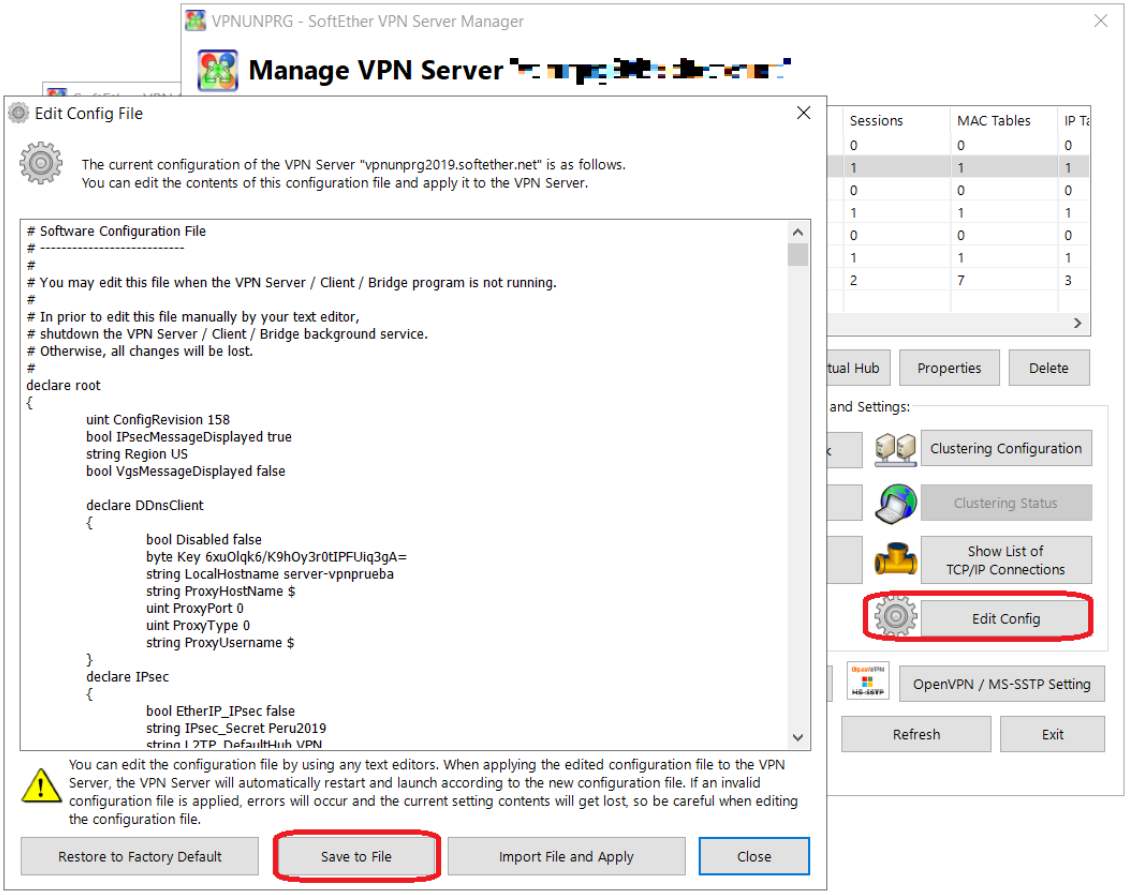


Anexo 2

Respaldo del Servidor VPN

Para realizar el respaldo de la VPN basta con dirigrinos al archivo de configuración “Edit Config” luego guardamos el archivo con la configuraciones realizadas en el servidor, incluyendo usuarios, grupos, entre otros.

Para restaurar esta configuración en otro servidor tenemos que importar el archivo dando click en el botón “Import File and Apply”



Anexo 3: Formato de Entrevista

Entrevista sobre red privada virtual(VPN)

OBJETIVO: La siguiente entrevista se realiza con la finalidad de conocer las necesidades actuales de la UNPRG, que a la vez nos ayudaran a complementar el desarrollo de nuestra tesis, titulada "Implementación de una VPN con Open Source para la gestión de aplicaciones de intranet en la Universidad Nacional Pedro Ruiz Gallo"

1. ¿Cuál es su rol principal en esta oficina?

2. ¿Para qué consideras usted necesario trabajar con vpn?

3. ¿Qué tan seguro considera usted el uso de aplicaciones de acceso remoto?

4. ¿Cree usted que mejoraría su productividad en la gestión de aplicaciones de intranet usando un software de acceso remoto?

5. ¿Cuándo fue la última vez que requirió conectarse a la intranet para la gestión de aplicaciones?

Anexo 4: Flujos para evaluar rentabilidad

Como lo explicamos en el capítulo 4 el retorno del dinero invertido en este tipo de proyectos tecnológicos genera una inversión menor a comparación de la propuesta echa por Virgilio Amenero Vásquez en su tesis "Implementación de una red privada virtual (VPN) bajo software libre para optimizar el manejo de información entre los locales de la corporación educativa adeu, de la ciudad de chiclayo". Tal como se muestra en los siguientes cuadros:

Velocidad	Precio
5 Mbps al 50%	S/.2,766.55

Inversión Final	Pagos por única vez	Pagos Mensuales
Speedy Business	S/. 0.00	S/. 2,766.55
Instalación y mantenimiento de OpenVPN	S/. 2,000.00	S/. 0.00
Costo de servidores	S/. 1,669.50	S/. 0.00
Sub Total S/.	S/. 3,669.50	S/. 2,766.55
Total S/. INC.IGV 18%	S/. 4,330.01	S/. 2,766.55

	PAGO EN MESES				
	I MES	II MES	III MES	IV MES	V MES
Propuesta	7,096.56	2,766.55	2,766.55	2,766.55	2,766.55

Lo que viene a ser un total de:

	Inversión total en los 5 meses
Propuesta	18162.76

Anexo 5: Plantilla Juicio de Expertos

Estimado experto, me es grato dirigirme a usted con la finalidad de solicitar su colaboración en la evaluación de la *"Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la universidad nacional Pedro Ruiz Gallo"*.

La evaluación de los ítems planteados contribuirá directamente a las conclusiones sobre la aplicabilidad y validez de la metodología; sin embargo la determinación de la validez de la metodología propiamente dicha, se determinará posteriormente a través de consenso entre revisores.

Nombres y apellidos del experto: _____

Formación académica: _____

Área de experiencia profesional: _____

Objetivo del Juicio de expertos: Validar el contenido y verificar si con la implementación de una VPN con open source en la universidad nacional Pedro Ruiz Gallo optimizaría la gestión de aplicaciones de intranet de la misma.

Objetivo de la validación: Usar los resultados obtenidos de la validación para la obtención de conclusiones con respecto a cada dimensión. Se usará valores promedio o representativos obtenidos a partir de la calificación de ambos revisores.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORIA	CALIFICACION	INDICADOR
SUFICIENCIA	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado Nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión complementaria.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD	1. No cumple con el criterio	El ítem no es claro
Los ítems se comprenden fácilmente, es decir su sintáctica y semántica son adecuadas	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado Nivel	Se requiere una modificación muy específica de algunos de los términos del ítem
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado Nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que se está midiendo.
RELEVANCIA	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
El ítem es esencial o importante, es decir debe ser incluido.	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado Nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Planilla de Validación

Dimensiones de la metodología	Ítems de la metodología a calificarse	Coherencia	Relevancia	Claridad	Suficiencia*	Observaciones
Productividad	Horas Trabajadas					
Disponibilidad	Tiempo de respuesta					
	Costo en viáticos					
Soporte	Dispositivos soportados					
	Costo de implementación					
Seguridad	Encriptación de datos y nivel de seguridad					
	Numero de accesos no autorizados					

¿Hay alguna dimensión que a su criterio falta evaluar? ¿Cual?

_____

_____

_____

*Para los casos de equivalencia semántica se deja una casilla por dimensión, ya que se evaluara si la traducción o el cambio en vocabulario son suficientes.

Constancia de validación

La constancia de validación es un formato que constituye la prueba de que el revisor ha realizado la validación de la metodología; asimismo da a conocer el resultado final de la validación.

Formato de Constancia de validación

Nombres y apellidos del Revisor: _____

Formación académica: _____

Áreas de experiencia profesional: _____

Nombres y apellidos del Revisor: _____

Formación académica: _____

Áreas de experiencia profesional: _____

Por medio de la presente hacemos constar que, a través del instrumento correspondiente, se revisó con fines de validación la *Metodología de verificación y validación de adquisición en la etapa de análisis de sistemas de información desarrollados a la medida en pequeños contextos,* habiéndose determinado por consenso que dicha metodología (es válida y aplica | no es válida y no aplica) como tal para su fin correspondiente.

Lambayeque, xx de Abril del 2019.

_____ _____

Firma Firma

Anexo 6: Juicio de Expertos Desarrollado

Juicio de Expertos

Estimado experto, me es grato dirigirme a usted con la finalidad de solicitar su colaboración en la evaluación de la *"Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la universidad nacional Pedro Ruiz Gallo"*.

La evaluación de los ítems planteados contribuirá directamente a las conclusiones sobre la aplicabilidad y validez de la tesis; sin embargo, la determinación de la validez de la tesis propiamente dicha, se determinará posteriormente a través de consenso entre revisores.

Nombres y apellidos del experto: Junior Eugenio Cachay Maco

Formación académica: Magister en Ingeniería de Sistemas

Área de experiencia profesional: Auditoría de Sistemas.

Objetivo del Juicio de expertos: Validar el contenido y verificar si con la implementación de una VPN con open source en la universidad nacional Pedro Ruiz Gallo optimizaría la gestión de aplicaciones de intranet de la misma.

Objetivo de la validación: Usar los resultados obtenidos de la validación para la obtención de conclusiones con respecto a cada dimensión. Se usará valores promedio o representativos obtenidos a partir de la calificación de ambos revisores.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORIA	CALIFICACION	INDICADOR
SUFICIENCIA	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado Nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión complementaria.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD	1. No cumple con el criterio	El ítem no es claro
Los ítems se comprenden fácilmente, es decir su sintáctica y semántica son adecuadas	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado Nivel	Se requiere una modificación muy específica de algunos de los términos del ítem
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado Nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que se está midiendo.
RELEVANCIA	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
El ítem es esencial o importante, es decir debe ser incluido.	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado Nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Planilla de Validación

Dimensiones de la metodología	Ítems de la metodología a calificarse	Coherencia	Relevancia	Claridad	Suficiencia*	Observaciones
Productividad	Horas Trabajadas	3	3	3	3	
Disponibilidad	Tiempo de respuesta	2	2	2	2	
	Costo en viáticos	2	1	1		
Soporte	Dispositivos soportados	2	3	2	3	
	Costo de implementación	3	3	3		
Seguridad	Encriptación de datos y nivel de seguridad	3	4	3	3	
	Numero de accesos no autorizados	3	4	3		

¿Hay alguna dimensión que a su criterio falta evaluar? ¿Cual?

Agilidad. | Burocracia, Tiempo de respuesta.

*Para los casos de equivalencia semántica se deja una casilla por dimensión, ya que se evaluara si la traducción o el cambio en vocabulario son suficientes.

Juicio de Expertos

Estimado experto, me es grato dirigirme a usted con la finalidad de solicitar su colaboración en la evaluación de la *"Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la universidad nacional Pedro Ruiz Gallo"*.

La evaluación de los ítems planteados contribuirá directamente a las conclusiones sobre la aplicabilidad y validez de la tesis; sin embargo, la determinación de la validez de la tesis propiamente dicha, se determinará posteriormente a través de consenso entre revisores.

Nombres y apellidos del experto: Carlos Antonio Rojas Ortiz

Formación académica: Mg. en Ing. de Sistemas

Área de experiencia profesional: Redes y Seguridad

Objetivo del Juicio de expertos: Validar el contenido y verificar si con la implementación de una VPN con open source en la universidad nacional Pedro Ruiz Gallo optimizaría la gestión de aplicaciones de intranet de la misma.

Objetivo de la validación: Usar los resultados obtenidos de la validación para la obtención de conclusiones con respecto a cada dimensión. Se usará valores promedio o representativos obtenidos a partir de la calificación de ambos revisores.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

CATEGORIA	CALIFICACION	INDICADOR
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado Nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión complementaria.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD Los ítems se comprenden fácilmente, es decir su sintáctica y semántica son adecuadas	1. No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado Nivel	Se requiere una modificación muy específica de algunos de los términos del ítem
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado Nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que se está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado Nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Planilla de Validación

Dimensiones de la metodología	Ítems de la metodología a calificarse	Coherencia	Relevancia	Claridad	Suficiencia*	Observaciones
Productividad	Horas Trabajadas	3	2	1	2	
Disponibilidad	Tiempo de respuesta	3	2	2	3	
	Costo en viáticos	2	3	3		
Soporte	Dispositivos soportados	3	3	4	3	
	Costo de implementación	3	4	3		
Seguridad	Encriptación de datos y nivel de seguridad	3	3	2	3	
	Numero de accesos no autorizados	2	4	2		

¿Hay alguna dimensión que a su criterio falta evaluar? ¿Cual?

Productividad → enfocarse a las horas dejadas de trabajar

Seguridad → especificar dentro del término muy amplio, a que aspecto específico se refiere

*Para los casos de equivalencia semántica se deja una casilla por dimensión, ya que se evaluara si la traducción o el cambio en vocabulario son suficientes.

Constancia de validación

La constancia de validación es un formato que constituye la prueba de que el revisor ha realizado la validación de la metodología; asimismo da a conocer el resultado final de la validación.

Formato de Constancia de validación

Nombres y apellidos del Revisor: Junior Eugenio Cachay Maco
Formación académica: Maestro en Ing. de Sistemas
Áreas de experiencia profesional: Auditora de Sistemas de Información

Nombres y apellidos del Revisor: Carlos Antonio Rojas Ortiz
Formación académica: Mag. Ingeniería de Sistemas
Áreas de experiencia profesional: Redes y Seguridad

Por medio de la presente hacemos constar que, a través del instrumento correspondiente, se revisó con fines de validación la *"Implementación de una VPN con open source para la gestión de aplicaciones de intranet en la universidad nacional Pedro Ruiz Gallo"*, habiéndose determinado por consenso que dicha tesis (es válida y aplica | no es válida y no aplica) como tal para su fin correspondiente.

Lambayeque, 15 de Julio del 2019.

Firma
Junior Eugenio Cachay Maco

Firma
Carlos Antonio Rojas Ortiz