UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

"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"

TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

VIRGILIO AMENERO VÁSQUEZ

Chiclayo, Junio 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"

POR:

VIRGILIO AMENERO VÁSQUEZ

Presentada a la Facultad de Ingeniería de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de
INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR EL JURADO INTEGRADO POR

Luis Augusto Zuñe Bispo
PRESIDENTE

Juan Torres Benavides
SECRETARIO

Gregorio Manuel León Tenorio
ASESOR

Dedicatoria

A mis padres y abuelos, por su comprensión y ayuda en los momentos buenos y malos, por haberme enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. Se la dedico por haberme dado ese cariño, calor humano y esa gran dosis de amor, pues gracias a ello soy quien soy hoy en día.

A todos ellos, muchas gracias de todo corazón.

Epígrafe

El verdadero progreso es el que pone la tecnología al alcance de todos.
(Henry Ford)

La imaginación es más importante que el conocimiento. El conocimiento es limitado, mientras que la imaginación no
(Albert Einstein)

Agradecimientos

- ✓ A Dios por estar siempre a mi lado, dándome las fuerzas necesarias para seguir luchando contra las adversidades que se me presentan y poder lograr mis metas y objetivos trazados

- ✓ A mi asesor Ing. Gregorio León Tenorio, por su acertada orientación y asesoría al compartir y apoyarme con sus conocimientos adquiridos y por su apoyo incondicional en la elaboración de la presente investigación.

- ✓ Al Ing. Fernando Ignacio Díaz Sánchez, por su apoyo y asesoría en la elaboración de la presente investigación.

ÍNDICE

ÍNDICE DE FIGURAS

RESUMEN

Ésta investigación estuvo centrada en la optimización del acceso a la información entre los locales de la Corporación Educativa ADEU, ubicada en la ciudad de Chiclayo; a través de la implementación de una VPN, la cual fue realizada en software libre, y como tal no incurre en gastos económicos excesivos y constituye un canal de comunicación seguro.

La investigación fue realizada en 3 etapas. Como parte de la primera etapa se realizó una entrevista al Jefe del Área de Sistemas, el cual manifestó que actualmente la información a la que accede el personal administrativo de los locales de dicha Corporación no cuenta con un medio de comunicación directo para compartir sus datos, por el contrario, están divididos, por lo cual el manejo y el acceso a la información es tedioso, ya que se requiere de otros medios tales como, dispositivos magnéticos y cuentas de correo públicas, que en la mayoría de los casos son canales de transferencia de información no seguros.

En la segunda etapa, teniendo en cuenta las necesidades planteadas por el Jefe del Área de Sistemas de la Corporación Educativa ADEU, se propuso un bosquejo de la VPN, la cual posteriormente fue modificada y validada por el Jefe del Área de Sistemas. Luego el modelo validado fue implementado en la herramienta de software denominada OpenVPN, realizándose las configuraciones apropiadas a los servidores y equipos necesarios para la realización de la implementación respectiva. Además se realizaron un conjunto de pruebas, a fin de que se asegure la conexión de la red y se descarten posibles vulnerabilidades de la red. Para el desarrollo de la VPN se hizo empleo de la "Metodología para la implementación de redes seguras", desarrollada por la empresa argentina CYBSEC.

Finalmente, la tercera etapa estuvo enfocada en la comparación de los resultados obtenidos en las etapas 1 y 2; y la demostración de las mejoras a la problemática de la corporación.

Mediante la implementación de la VPN se logró proporcionar un canal que permite transferir los datos de manera óptima y eficaz; permitiendo así, la confidencialidad y seguridad en su transmisión, sin tener que incurrir en gastos excesivos en la contratación de canales privados.

Palabras clave: optimización, herramienta de software, Metodología para la implementación de redes seguras.

ABSTRACT

This research focused on optimizing the management of information between local ADEU Educational Corporation, located in the city of Chiclayo, through the implementation of a VPN, which was conducted on free software, and as such incurring excessive economic costs and is a secure communication channel.

The research was conducted in 3 stages. As part of the first stage consisted of interviews with the Head of the Systems which stated that the information currently accessed by the local administrative staff of the Corporation has no direct means of communication to share their data, Instead, they are divided, so that the handling and management information is tedious, because it requires other means such as magnetic devices and public mail accounts, which in most cases are transfer channels information is not secure.

In the second stage, taking into account the needs expressed by the Head of the Educational Systems Corporation Adeu, proposed an outline of the VPN, which was subsequently modified and validated by the Head of the Systems. Then the validated model was implemented in the software tool called OpenVPN, performing the appropriate settings to servers and equipment needed to perform their respective implementation. We also carried out a set of tests, so as to ensure the network connection and discard any network vulnerabilities. For the development of the VPN was using the "Methodology for implementing secure networks," developed by the company CYBSEC Argentina.

Finally, the third stage was focused on comparing the results obtained in steps 1 and 2, and the demonstration of the improvements to the problems of the corporation.

Taking such results, by implementing the managed VPN provides a channel for transferring data optimally effective, allowing the confidentiality and security in transmission, without incurring excessive costs in hiring private channels.

Keywords: optimization, software tool, methodology for implementation of secure networks.

I. INTRODUCCIÓN

La Corporación ADEU (Asociación De Jóvenes Universitarios), tiene dos locales; uno de ellos es el colegio ADEU, ubicado en la Av.Grau#135, y la academia Preuniversitaria ADEU, ubicada en la Calle Juan Cuglievan#651. La Academia inició sus actividades en diciembre de 1983 en la ciudad de Chiclayo. Gracias a los logros obtenidos allí, hacia 1992 se inició la expansión de ADEU, en 1995 se creó el Instituto ADEU y en 1998, el primer colegio PRE Universitario. En 1999 aparece el nivel primario y en el año 2000 el nivel Kínder (ADEU Kids), a partir de allí se dio nacimiento a la Corporación Educativa ADEU.

Al contar con dos locales ubicados en distintos lugares, los sistemas de información comparten su información usando el correo electrónico, presentando el siguiente problema:

Deficiencia en el acceso a los Datos, causada porque la corporación educativa ADEU no cuenta con un canal privado para la transmisión de datos, además de no contar con capital para invertir en un servicio VPN arrendado. Esto trae como consecuencia que exista pérdida de tiempo en el acceso a la información, retrasando la transmisión de los reportes de notas, asistencias, pagos, reporte de alumnos y de profesores, reportes administrativos y de planillas. Además no tienen un medio que sirva como soporte para enlazar sus futuros sistemas a implementar. También se registraron algunos casos de pérdida de información al enviar datos por correo electrónico, causando inseguridad en el canal de comunicación, por su vulnerabilidad ante posibles ataques informáticos.

Del problema analizado en la Corporación Educativa ADEU se plantea la siguiente interrogante: ¿De qué manera se podría mejorar el acceso a los datos entre los locales de la corporación Educativa ADEU? Teniendo como hipótesis la siguiente afirmación: La implementación de una VPN bajo software libre OpenVPN, optimizará el acceso a los datos entre los locales de la corporación Educativa ADEU.

El objetivo general de esta investigación es implementar una VPN con la finalidad de optimizar el acceso a los datos entre los locales de la corporación Educativa ADEU. Como objetivos específicos de esta investigación es mejorar la seguridad en la transferencia de los datos, minimizar costos en la implantación de una tecnología VPN y configurar un servidor VPN que sirva como soporte para enlazar los futuros sistemas a implementar entre los locales.

La investigación realizada tiene justificación científica y tecnológica; ya que este tipo de tecnología permite utilizar métodos de encriptación y autentificación para garantizar el envío de información, ofreciendo un canal seguro a través del internet de forma confidencial e integra, permitiendo que las empresas agilicen procesos y garanticen el envío de datos de forma segura.

También tiene justificación Financiera y económica; ya que se encuentra en los planes de la Corporación Educativa, el cual es implementar una VPN para la integración de sus dos redes en un futuro. Por ello, están dispuestos a invertir en la implementación del diseño de red, además la herramienta tecnológica que se usó para la implementación de la VPN está basada en software libre, por lo tanto no se incurrió en gastos de licencias del producto.

II. MARCO TEÓRICO

2.1. Antecedentes de Investigación

2.1.1 Locales.

a) **Título:** Análisis y diseño de una red privada virtual para Essalud Lambayeque.
Autor: Collantes S, Molocho H., Ramírez F.
Universidad, año: Universidad Pedro Ruiz Gallo-Lambayeque-Perú, 2003.
Resumen: En el trabajo presentado por Collantes, Molocho y Ramírez (2003) se construyo una VPN basada en la tecnología de cortafuegos en EsSalud en la ciudad de Chiclayo; de este trabajo se aprecia el uso de las VPN y el tipo de seguridad que se debe brindar para conectar dicho local con las demás sucursales (Almanzor, Aguinaga Asenjo y Naylamp).
Correlación: La investigación presentada tiene relación con la tesis que se propone en estas páginas, puesto que, ambas dan a conocer los aspectos a tener en cuenta para la implementación de la seguridad en una VPN durante el traslado de la información. Además la tesis descrita ayudo para la implementación la seguridad de la VPN implementada.

b) **Título:** Diseño e implementación de un sistema de red para mejorar el sistema de comunicación en el proyecto especial de infraestructura de transporte nacional-provincial nacional-Zonal II Lambayeque
Autor: Cotrina R, Guevara F, Arlita.
Universidad, año: Universidad Santo Toribio de Mogrovejo Chiclayo, 2006.
Resumen: En el trabajo presentado por Cotrina y Guevara (2006) se diseñó e implementó un sistema de red para mejorar el sistema de comunicación en el proyecto especial de infraestructura de transporte nacional-provincial nacional-Zonal II Lambayeque, entre las cuales se implementó un servicio VPN desarrollada por la empresa Telefónica, la cual permitió una conexión permanente a otras redes de datos a través de Internet acelerando los procesos de envío de información.
Correlación: La investigación presentada tiene relación con la tesis que se propone ya que ambas analizan los pasos para la implementación de una VPN. Además la tesis presentada ayudo a dar una descripción de cómo es que se configura una VPN, siendo de ayuda para la investigación.

2.1.2 Nacionales:

a) **Título:** Desarrollo de una virtual private network (VPN) para la interconexión de una empresa con sus sucursales en provincias.
Autor: Percy Vivanco Muñoz
Universidad, año: Universidad Nacional Mayor de San Marcos, 2003.
Resumen: En el trabajo presentado por Percy Vivanco (2003) se desarrollo una VPN basado en la herramienta Open Source para el Grupo Santo Doming, utilizando un producto llamado CIPE (Crypto IP Encapsulation). El proceso de investigación y desarrollo planteados en el desarrollo de

esta tesis establece una plataforma para la creación de un nuevo servicio de valor agregado, basado en el concepto de VPN como modelo integral en las nuevas soluciones de redes usando tecnología Open Source.

Correlación: La importancia de esta tesis radica en el diseño de una VPN bajo software libre para cubrir la necesidad de establecer una conexión entre la sede central del Grupo Santo Doming y sus sucursales en Arequipa y Trujillo, de tal manera que se pueda utilizar las aplicaciones cliente - servidor entre dichas sucursales, evitando con ello un doble trabajo y el incurrir en sobrecostos que generen el mantener la información de la empresa de forma separada y descentralizada. Además se pudo constatar los beneficios de una VPN para nuestra investigación.

.

b) **Título:** Diseño de implementación de una VPN en una empresa comercializadora utilizando Ipsec.

Autor: Edgar Torres.

Universidad, año: Escuela politécnica nacional, 2006.

Resumen: En la investigación presentada por Edgar Torres (2006) se implementó una VPN para la empresa comercializadora CONFITECA utilizando la tecnología IPSec para interconectar sus locales en Ecuador, Perú y Colombia, para mejorar los procesos del manejo de información entre estas.

Correlación: La importancia de esta investigación radica en las ventajas y desventajas de la implementar de una VPN con la tecnología IPSec, esto ayudo a elegir la mejor tecnología para la implementación de la VPN.

2.1.3 Internacionales.

a) **Título:** Protocolos de Seguridad para Redes Privadas Virtuales (VPN)

Autor: Limari R, Victor

Universidad, año: Universidad Austral de Chile, 2004.

Resumen: En la investigación realizada por Limari y Victor (2004) se analizo las diferentes formas de implementación de una VPN mediante el protocolo IPSec que hacen posible crear túneles a través de medios considerados como poco seguro para quien necesite que sus datos no sean dañados, leídos o tergiversados. Estudiándose así, tanto los modelos como la estructura que adopta la información al momento de considerarse listo para viajar por el medio inseguro.

Correlación: Esta tesis ayudo a darnos un concepto amplio del funcionamiento de una VPN, tanto en la implementación, estructura, diseño y seguridad de una VPN entre locales remotos.

b) **Título:** Servicio VPN de acceso remoto basado en SSL mediante OpenVPN

Autor: Tomás C, Juan.

Universidad, año: Universidad Politécnica de Cartagena, 2008.

Resumen: En la investigación realizada por Tomás (2008) se evaluó las posibilidades que ofrece la aplicación tecnológica OpenVPN para

construir conexiones seguras a través de la infraestructura de redes públicas, por medio de conexiones seguras mediante el protocolo SSL.
Correlación: Esta tesis, tiene relación directa con la que se propone, puesto que en ambas se ha utilizado la herramienta tecnológica OpenVPN para la implementación de la VPN, además muestra la configuración de la implementación de esta herramienta, así como la seguridad que se debe tener para implementar una VPN.

2.2. Antecedentes de aplicación:

2.2.1. Locales.

a) **Título**: Desarrollo de red VPN para Perales Huancaruca SAC.
Autor: SORCIER.
Empresa, año: Perales Huancaruna SAC, 2011.
Resumen: La compañía SORCIER implementó una VPN para la empresa Perales Huancaruna SAC (Perhusac), empresa líder en la exportación de café peruano, en la cual se desarrollo de una solución de red que les permitiera acceder en cualquier momento a los sistemas de sus centros de acopio desde su sede central en Chiclayo.
Perales Huancaruna tuvo dos necesidades básicas para solicitar este desarrollo: Necesitaban centralizar de forma más rápida y eficiente los datos de transacciones en zonas de acopio y por otro lado, mejorar el soporte informático al poder hacerlo de forma remota.
Sorcier Empresas suministró, instaló y configuró equipos de red que le permite ahora al personal de Sistemas de Chiclayo ingresar en cualquier momento a los sistemas de zonas de acopio, esto a pesar del pésimo servicio de Internet disponible en muchas de las zonas de nuestra selva Oriental y Central.
Correlación: Esta investigación ayudo a la tesis propuesta, ya que da a conocer cómo el proceso de centralización de datos ayuda a que la transacción entre zonas dispersas sea más rápida y eficiente.

b) **Título:** Instalación de una VPN para el BBVA Banco Continental sede Chiclayo.
Autor: Telefónica del Perú.
Empresa: BBVA Banco Continental.
Resumen: La empresa telefónica implementó el servicio de VPN (Red Privada Virtual), en el Banco Continental sede de Chiclayo para la integración con las demás oficinas en el Perú.
Correlación: Este caso de éxito ayudo a la tesis propuesta en la descripción de la implementan de una VPN, además dio a conocer cómo la integración de locales en diversas aéreas mejora, a través de la VPN, los procesos y servicios internos, lo cual ayudo a la investigación para poder dar a conocer la importancia de este tipo de implementación.

2.2.2. Nacionales

a) **Título:** Implementación de servicio de VPN Roadwarrior para Perú y Chile.
Autor: Consultoría NET SRL.
Empresa, año: CinePlanet, 2005.
Resumen: La empresa Consultora NET implementó una VPN para CinePlanet en Mayo del 2005, como parte de su estrategia de expansión regional, CinePlanet ingreso al mercado chileno bajo la marca Movieland. En la primera etapa, la puesta en marcha de Movieland fue en la ciudad de Santiago, Valdivia y Temuco, inaugurando a la fecha 04 complejos, CONSULTORIA NET implementó una solución para que los usuarios móviles de Perú y Chile puedan acceder a sus aplicaciones y red interna, de manera segura, a través de un enlace VPN Roadwarrior.
Correlación: Este caso de éxito ayudo en la investigación, ya que describe la implementación de una VPN NET to NET, la misma planteada en esta investigación, la cual permite unir distantes redes a través de un canal seguro.

b) **Título:** Instalación de una VPN para el BBVA Banco Continental.
Autor: Telefónica del Perú.
Empresa: BBVA Banco Continental.
Resumen: La empresa telefónica implementó dos servicios de VPN (Red Privada Virtual) uno para servicios de voz y datos con cobertura local y nacional y otro para la integración de las oficinas en Perú con BBVA de España. 2005.
Correlación: Este caso de éxito tiene relación directa con esta investigación, ya que ambas implementan una solución VPN para la integración de locales en diversas aéreas para la mejora de procesos y mejora de servicios internos.

2.2.3. Internacionales.

a) **Título:** Implementación de una solución basada en una red VPN con tecnología Cisco a la empresa CF Consultores.
Autor: E-Corp S.A., partner de Cisco,
Empresa, año: CF Consultores, 2006.
Resumen: E-Corp S.A., partner de Cisco, desarrolló e implementó una solución para la empresa española CF Consultores, la cual le permitió contar con un enlace seguro vía Internet (VPN) para realizar sus transacciones electrónicas. Esta solución, basada en tecnología de Cisco, redujo drásticamente los costos en un 60% y mantuvo todos los requerimientos de seguridad que el sistema demandaba. La implementación de la red VPN incluyó un dispositivo de seguridad Cisco PIX 501 para cada sucursal y un Cisco PIX 515 para la casa central. E-Corp S.A. tuvo a su cargo el relevamiento inicial, la configuración, el desarrollo de la solución, la ingeniería, la integración, la implementación y el soporte técnico. Había un grupo de clientes que no tenían enlace dedicado y debían validar las tarjetas en forma telefónica. Para ellos el cambio fue muy importante, ya que les permitió tener validación directa vía PostNet,

Correlación: Este caso de éxito, guarda relación directa con la tesis que se propone, ya que esta empresa implementó una VPN y tuvo datos específicos que ayudaron a maximizar sus procesos, además ayudo a que en la investigación se pueda tener idea de lo que se puede lograr implementando una VPN.

b) **Título;** Instalación de dos AbarConnect para unir sus dos delegaciones de Bilbao y Vitoria.
Autor: ABARTIA TEAM,
Empresa, año: KOPAS, 2008.
Resumen: Se instálalo dos soluciones VPN llamadas AbarConnect para unir dos de sus delegaciones de la empresa ABRTIA TEAM, en las ciudades de Bilbao y Vitoria; el problema fue la necesidad de compartir recursos informáticos entre sus dos centros de trabajo; la solución fue configurado dos equipos AbarConnect para que trabajen conjuntamente como si fuese una oficina única.
Correlación: Este caso de éxito, guarda relación directa con la tesis que se propone, ya que se demuestra una problemática de interconexión entre las oficinas de la empresa ABRTIA TEAM, y cómo una VPN da solución a esta.

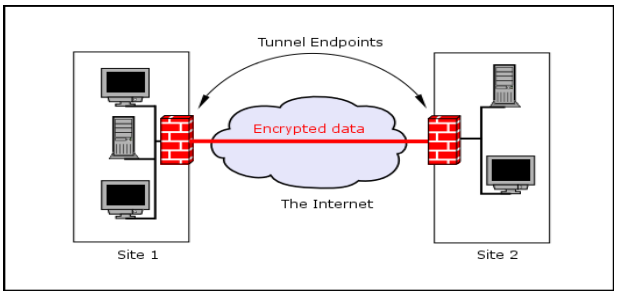
2.3. Bases teóricas

2.3.1. VPN Concepto:

Saber el concepto de VPN es muy importante para entender esta investigación, de acuerdo a la definición estándar provista por la Fuerza de Trabajos de Ingeniería de Internet (IETF por sus siglas en inglés), un VPN es "Una emulación de una Red de Área Amplia (WAN) usando facilidades IP públicas o compartidas, tal como la Internet o columnas IP privadas".
En términos más simples, un VPN es una extensión de una intranet privada a través de una red pública (la Internet) que asegura conectividad segura y de costo efectivo entre los dos fines comunicadores. La intranet privada se extiende con la ayuda de túneles lógicos privados. Estos túneles permiten que los dos fines comunicantes intercambien información de manera que parezca comunicación de punto a punto.

Las VPN atraviesan un proceso cifrado, esto se debe a que cualquier comunicación entre dos nodos con VPN está encriptado y es este mismo proceso lo que garantiza la seguridad y la integridad de los datos. Estos datos pasan a través de una red abierta, insegura (internet).

Otra forma de ver a la VPN es como el proceso más sencillo para enviar datos cifrados de un punto a otro me manera segura.



Fuente: Belnet, 2005

Figura N°01: Configuración típica VPN.

La figura anterior da a conocer el diagrama de la estructura lógica de una Red Privada Virtual VPN. Según García, Raya y Rodrigo (2002), las dos características más importantes, desde el punto de vista del usuario de una VPN son:

- Seguridad: Este punto implica aislamiento, es decir, que sus datos son suyos y, por tanto, no son accesibles al resto del mundo.
- Privacidad: Significa que el usuario siente que los enlaces utilizados para construir la red son solo suyos.

2.3.2. Evolución de los VPN

Se tiene que tener en cuenta al momento de desarrollar una VPN los conceptos que maneja y cómo esta se ha ido desarrollando a través del tiempo. Las VPN no son exactamente una nueva tecnología. En contradicción a lo que la mayoría de nosotros cree, Según Gupta (2003) "el concepto VPN ha existido los últimos 15 años y ha tomado varias generaciones el que llegue a su forma más reciente".
Las primeras VPN conocidas fueron ofrecidas por la empresa AT&T en los años 80 y eran conocidas como Redes Definidas con Software (SDNs).

La segunda generación de VPN llegó con el auge de las tecnologías [1]X.25 y Red Digital de Servicios Integrados (ISDN) a inicios de los años 90. Estas dos tecnologías permitían la transmisión de líneas de paquete a través de una red pública compartida. Por ello, la idea de las transmisiones de bajo costo a través de una red pública ganó popularidad dentro de la comunidad trabajadora en internet muy rápido. Por algún tiempo pareció que a pesar que el protocolo X.25 sobre el ISDN sería establecido como el protocolo VPN nativo. Sin embargo, los niveles de transmisión fallaron al nivel esperado de desempeño y la segunda generación de VPN de corta vida pasó.

Después de la segunda generación, el mercado de VPN se hizo lento hasta la emergencia de tecnologías basadas en células (o celdas): Transmisión de Marcos (FR) y [2]Modo de Transferencia Asincrónico (ATM). La tercera generación de VPN estaba basada en estas dos tecnologías. Estas estaban basadas en el concepto del cambio de circuitos virtual, en el cual los

1 X.25: Es un estándar ITU-T para redes de área amplia de conmutación de paquetes
[2] ATM: Permite la transferencia simultánea de datos y voz a través de la misma línea

paquetes de información no contienen las direcciones de fuente o destino. En vez de estos, llevan indicadores a los circuitos virtuales donde están localizados los nodos de fuente y destino involucrados en la transacción se hallan.

La generación actual de VPN se enfrenta a todos estos requerimientos usando la tecnología de túneles. Ahora, las organizaciones de gran escala y las pequeñas que una vez pudieron mal-costear soluciones basadas en líneas de arrendamiento muy costoso, pueden marcar su presencia en el mercado global.

La técnica de túneles consiste en encapsular un paquete de información en un protocolo de tuneleo, como seguridad IP (IPSec), protocolo SSL/TLS, protocolo de Tuneleo de Punto-a-Punto (PPTP), o Protocolo De Tuneleo de Capa 2 (L2TP), y finalmente empaquetando el paquete tuneleado en un paquete IP. El paquete resultante es llevado luego a la red de destino usando la información IP overlying. Ya que el paquete de información original puede ser de cualquier tipo, el tuneleo puede aportar el tráfico multi-protocolo, incluyendo IP, ISDN, FR, y ATM.

2.3.3. Ventajas y Desventajas de los VPN

Es necesario entender las ventajas y desventajas que se tiene al implementar una VPN y tenerlas en cuenta al momento de implementar este tipo de tecnología. Las principales ventajas y desventajas de las VPN son:

- Costo de implementación reducido: Cuestan considerablemente menos que las soluciones tradicionales, que están basadas en líneas arrendadas, ATM o ISDN. Esto porque los VPN eliminan la necesidad de conexiones de larga distancia reemplazándolas con conexiones locales a una red transportista, [3]ISP o EL Punto de Presencia de ISP (POP).
- Costos de personal y administración reducidos: Mediante la reducción de los costos de telecomunicación de larga distancia, los VPN bajan considerablemente los costos de las operaciones de red basadas en WAN. En adición, una organización puede reducir el costo total de la red si el equipo WAN usado en el VPN es administrado por el ISP. La razón detrás del costo reducido es explicada por el hecho que la organización no necesita emplear tanto personal entrenado y caro como si el VPN fuese manejado por la misma organización.
- Conectividad realzada: Los VPN usan la Internet para interconectividad entre partes lejanas de una intranet. Debido a que la Internet es globalmente accesible, incluso las oficinas más lejanas, usuarios, y usuarios de móviles (como los vendedores) pueden fácilmente conectarse a la intranet corporativa.
- Seguridad de transacción: Ya que los VPN usan la tecnología de tuneleo para transmitir datos a través de redes públicas "inseguras", las transacciones de información son seguras hasta un alcance. Además de la

[3] ISP: Proveedor de servicios de Internet; es una empresa que brinda conexión a Internet a sus clientes.

tecnología de tuneleo, los VPN usan medidas de seguridad extensivas, como la codificación, autenticación y autorización para salvaguardar la seguridad, confidencialidad e integridad de la información transmitida. Como resultado, los VPN ofrecen una transacción de una seguridad de un grado considerablemente alto.

- Uso efectivo de banda ancha: En el caso de la conectividad en Internet basada en líneas arrendadas, la banda ancha es enteramente desperdiciada en la ausencia de una conexión de Internet activa. Los VPN, por otro lado, crean túneles lógicos para transmitir datos cómo y cuando se requieren. Como resultado, la red de banda ancha es usada sólo cuando hay una conexión de Internet activa. Por ello, hay mucha menos oportunidad de que la red de banda ancha disponible se desperdicie.
- Escalabilidad realzada: Ya que los VPN están basados en Internet, permiten a una intranet evolucionar y crecer cómo y cuando el negocio necesita cambio, con gastos mínimos en equipamiento extra. Esto hace las intranets basadas en VPN altamente escalables y adaptables al futuro crecimiento, sin poner mucha tensión en el presupuesto de la red de la organización.

  A pesar del número de ventajas ofrecidas por los VPN, unas cuantas desventajas son también asociadas con ellos, que han hecho a muchos usuarios escépticos sobre su uso. Estas incluyen:

- Alta dependencia en la Internet: El desempeño de la red basada en VPN es altamente dependiente del desempeño de la Internet. Las líneas arrendadas garantizan la banda ancha que es especificada en un contrato entre el ISP y la organización. Sin embargo, ninguno puede garantizar el desempeño de la Internet. Una sobrecarga de tráfico y congestión puede afectar negativamente el desempeño de la entera red basada en VPN.
- Falta de soporte a los protocolos de legado: Los VPN de hoy están enteramente basados en la tecnología IP. Sin embargo, muchas organizaciones continúan usando ordenadores centrales y otros similares dispositivos de legado y protocolos en sus transacciones diarias. Como resultado, los VPN son largamente incompatibles con los dispositivos y protocolos de legado.

Se tiene que tener una serie de consideraciones al momento de implementar una VPN, entre las más importantes tenemos:

- Seguridad: Ya que información importante de la compañía debe viajar a través de una red extremadamente insegura, como la Internet, la seguridad es la mayor preocupación en los administradores de organizaciones y redes. Las medidas apropiadas deben ser tomadas para asegurar que la información no sea interceptada o dañada en el viaje. Fuertes mecanismos de codificación deben ser empleados para codificar la información.
- Compatibilidad: Otra fuerte preocupación en el seleccionar una solución basada en VPN para la red de tu empresa es que la solución escogida

debe ser compatible con las soluciones de infraestructura y seguridad de la red, tales como firewalls, proxies, softwares anti-virus, y otros sistemas de detección de intrusión. Otro punto para recordar es que la solución entera debe ser administrable mediante el uso de una sola aplicación.

- Interoperabilidad de dispositivos de múltiples vendedores: Si existe la más mínima falta de interoperabilidad entre dispositivos usados para implementar el VPN, la Calidad de Servicio (QoS) es difícil de proveer. Por ello, los dispositivos deben ser probados profundamente por interoperabilidad antes de implementarlos en el VPN. Los expertos recomiendan que en la medida de lo posible, los equipos usados para implementar un VPN deberían ser de un vendedor. Esto asegura la completa interoperabilidad de los equipos y el alto desempeño garantizado.
- Administración centralizada de los VPN: Debe ser posible configurar, administrar, y resolver los problemas relacionados a VPN. Además, es importante que el software de administración genere todos los registros. Estos registros ayudan al administrador de red a localizar y resolver proactivamente antes que el desempeño de la red entera sea negativamente afectado.
- Fácil implementación: Este punto es muy importante, la solución VPN debe ser fácil de implementar y configurar. Si estás implementando soluciones de larga escala, debes asegurar que el software de administración sea capaz de guardar y hacer un seguimiento del gran número de túneles que el sistema implemente.
- Fácil uso: El software VPN, especialmente el del cliente, debe ser simple y no complicado para que incluso los usuarios fin puedan implementarlo, si es necesario. Además, los procesos de autenticación y las interfaces deben ser fáciles de entender y usar.
- Escalabilidad: El VPN existente debe poder adaptarse a demandas y adiciones futuras con el cambio mínimo de la infraestructura actual.
- Desempeño: La codificación, que es un aspecto muy importante de los VPN, es una operación de CPU intensa. Por ello, es necesario seleccionar dispositivos que no sólo sean interoperables, pero también capaces de realizar tareas, tales como codificación de información, rápida y eficientemente. Si no, el bajo nivel de desempeño puede afectar negativamente el desempeño total del VPN.
- Administración de la banda ancha: Para asegurar el alto desempeño, alta disponibilidad y QoS garantizados, es esencial administrar la banda ancha eficientemente. La administración de banda ancha tiene muchos aspectos. Incluyen administración por parte de los usuarios, de grupos, y aplicaciones, de modo que sea posible priorizar usuarios, grupos y aplicaciones por política de compañía.
- Escogiendo un ISP: El ISP que escojas para tu VPN debe ser fiable y capaz de proveer apoyo a los usuarios de VPN y a los administradores de red en cualquier momento. Esto puede incluso ser más crucial si tu ISP te brinda servicios administrados.

- Protegiendo la red de información no solicitada: Estando directamente conectados con la Internet, los VPN pueden ser bloqueados por información no solicitada impidiendo que la red se desempeñe bien. En casos extremos, esta información puede inundar la intranet entera llevando a la interrupción de la conexión y los servicios. Como resultado, los túneles VPN deberían proveer un mecanismo para filtrar el tráfico que no sea de VPN.

2.3.4. Arquitectura VPN

Al momento de elegir la arquitectura de la VPN para la investigación se tuvo que tener en cuenta los siguientes conceptos. Según Brown (2001), existen cinco tipos de arquitectura VPN.

2.3.4.1. VPN basado en cortafuego

Los VPN basados en cortafuego probablemente son la forma más común de arquitectura VPN, y muchos proveedores ofrecen este tipo de configuración. Esto no significa que los VPN basados en cortafuego sean superiores a otras formas de VPN, sino más bien se trata de una base establecida a partir de la cual se puede crecer. Actualmente sería difícil encontrar una organización conectada a Internet que no utilice algún tipo de cortafuego. Debido a que estas organizaciones ya están conectadas a Internet todo lo que se necesitaría es añadir a software de cifrado. Lo más probable, si su organización ha adquirido recientemente un cortafuego, es que incluya la capacidad para implementar tecnología descifrado VPN. Muchos proveedores incluyen su tecnología descifrado propietaria sin costo adicional con el producto.

Un aspecto importante de la seguridad es el sistema operativo subyacente, para esto tenemos que hacernos las siguientes preguntas: ¿En qué plataforma se está ejecutando el cortafuego?, ¿Se trata de un dispositivo basado en UNIX, basado en NT o en algún otro dispositivo basado en plataforma, y cuáles son los puntos vulnerables potenciales de este sistema operativo? No existe un dispositivo que sea 100 por ciento seguro, así que si crea un VPN en ese dispositivo, necesitara asegurarse de que el sistema operativo subyacente sea seguro.

2.3.4.2. VPN basado en caja negra

En el escenario de caja negra, un proveedor ofrece exactamente eso una caja negra. Se trata básicamente de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen con software que se ejecuta en un equipo cliente de escritorio para ayudar a administrar ese dispositivo, y otras pueden configurarse a través de un explorador Web. Se cree que estos dispositivos de cifrado con mayor rapidez. Aunque eso puede ser verdad, no todos ofrecen una característica de administración centralizada, y por lo general no soportan el acceso a sí mismos; es necesario enviar estos accesos a una base de datos para consulta. También se requiere otro servidor si se desea llevar a cabo la autentificación, aunque algunos dispositivos permiten añadir usuarios si así lo desean.

2.3.4.3. VPN basados enrutador

Los VPN basados enrutador son adecuadas para una organización que ha hecho una gran inversión en enrutadores y cuyo personal de TI tiene experiencia en ello. Existen dos tipos de VPN basados en enrutadores. En uno de ellos el software se añade al enrutador para permitir que el acceso de cifrado ocurra. El segundo método se inserta una tarjeta externa de otro proveedor en el mismo chasis que el enrutador.

2.3.4.4. VPN basado en acceso remoto

El acceso remoto, como su nombre indica, significa que alguien de afuera está tratando de crear un flujo de paquetes de datos cifrados hacia su organización. Así que, de manera más literal, tal vez el termino se aplique al software que se ejecuta en las maquinas de los usuarios remotos, las cuales están tratando de crear un túnel hacia su organización y a un dispositivo en su red que permita esa conexión.

2.3.4.5. VPN basados en software

Una VPN basada en software clásicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general se utiliza desde un cliente a un servidor.

Por ejemplo, en una VPN de PPTP, el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión de VPN.

Cuando se seleccione una VPN de software necesitara tener procesos de administración de claves adecuadas y posiblemente una autoridad emisora de certificados en sus oficinas. Con los otros tipos de VPN, por ejemplo, de cortafuego/VPN a cortafuego/VPN, las únicas claves que se necesitan son de VPN a VPN. Esto significa que el tráfico en su red interna se descifra, así que solo necesita las claves para dispositivos VPN. Pero en el caso de cliente servidor, cada estación posiblemente podría tener un propio par de claves privadas/públicas; solo se requiere hacer planes para este tipo de instalación. Este tipo de VPN fue el escogido para esta investigación.

2.3.5. Tipos de VPN

2.3.5.1. Despliegue VPN de usuario

Las VPN de usuario son redes privadas virtuales entre la máquina de un usuario individual y la red o el sitio de una organización. Con frecuencia las VPN de usuario son utilizadas por los empleados que viajan o que trabajan desde casa. El servidor de VPN puede ser el muro de fuego de la organización o puede ser un servidor de VPN separado. EL usuario se conecta de Internet mediante un ISP por teléfono, por una línea DSL o un módem de cable e inicia un VPN hacia el sitio de la organización por medio de Internet.

El sitio de la organización solicita la autentificación del usuario y, si tiene éxito, permite que esta tenga acceso a la red interna de la organización como si dicho usuario estuviera dentro del sitio y físicamente en la red.

Las VPN de usuario pueden permitir que la organización limite los sistemas o archivos a los que pueda tener acceso el usuario remoto. Esta limitación debería estar basada en políticas de la organización y depende de las capacidades del producto de VPN.

2.3.5.2. Despliegue VPN de sitio

Las VPN de sitio son empleadas por las organizaciones para conectar sitios remotos, sin la necesidad de costosas líneas arrendadas o para conectar dos organizaciones diferentes que deseen comunicarse con algún propósito de negocio.

Para iniciar la conexión, un sitio intenta enviar tráfico hacia otro. Esto causa que los dos extremos inicien la VPN. Los dos extremos negociaran parámetros de la conexión dependiendo de la política de los dos sitios. Los dos sitios también se autenticaran entre sí utilizando algún secreto compartido que haya sido configurado previamente, o bien mediante certificado de clave pública. A este tipo de VPN se le conoce como VPN NET to NET y fue esta la escogida para esta investigación.

2.3.6. Protocolos de túnel

Es muy importante saber que protocolos utiliza la VPN que se implementará y la diferencia entre ellos. Según Tomás (2008), "en la actualidad existen varias tecnologías que permiten implementar una VPN, implementando con técnicas diferentes los túneles y la seguridad que ofrecerá esta VPN. Algunas tecnologías no están abiertas a los desarrolladores porque son propietarias, como pueden ser muchas de las soluciones VPN que Cisco incorpora en sus dispositivos. Como tecnologías VPN más utilizadas en la actualidad se describirán, sin entrar en mucho detalle, PPTP, L2F, L2TP, MPLS, GRE, SSH e IPSec y el protocolo SSL."

A continuación se hablara de los principales protocolos de túnel para VPN.

2.3.6.1. Protocolos de capa 2:

- PPTP (Point-to-Point Tunneling Protocol): Este protocolo trabaja en capa 2, es un protocolo propietario de Microsoft diseñado específicamente para implementar VPN. PPTP depende del protocolo de enlace de datos PPP (Poin-to-Point-Protocol). En cuanto a seguridad, la autentificación de usuarios se realiza a través de los protocolos PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) y MS-CHAP (versión de Microsoft de CHAP). PPTP utiliza túneles [4]GRE para implementar el túnel de una VPN, encapsulando tramas PPP y utiliza un cifrado RC-4 bastante débil. Otro inconveniente es que solo permite una conexión por túnel.
  La especificación para el protocolo PPTP fue publicada por el RFC 2637, aunque no ha sido ratificada como estándar por el IETF (Internet Engineering Task Force).
  La seguridad de PPTP ha sido totalmente rota y los sistemas con PPTP deberían ser sustituidos por otra tecnología de VPN. Existen incluso

4 GRE: Es un protocolo para el establecimiento de túneles a través de Internet

herramientas para ejemplo, la herramienta ASLEAP permite obtener claves durante el establecimiento de la conexión.

- L2F (Layer 2 Forwarding): Como PPTP, L2F fue diseñado, por Cisco, para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas.
  La especificación para el protocolo L2F fue publicada por el RFC 2341. La principal diferencia entre PPTP y L2F es que, como el establecimiento de túneles de L2F no depende de IP, es capaz de trabajar directamente con otros medios, como [5]Frame Relay o ATM.
  Utiliza el protocolo PPP para la autenticación entre usuarios remotos por lo que implementa los protocolos de autenticación PAP (Password Authentication Protocol) y CHAP (Challenge Handshake Authentication Protocol). Una característica que difiere L2F de PPTP es que L2F permite más de una conexión por túnel.

  En L2F se utilizan dos niveles de autenticación, primero por parte del ISP (proveedor de servicio de red), anterior al establecimiento del túnel, y posteriormente, cuando se ha establecido la conexión con la [6]pasarela corporativa. Como L2F es un protocolo de nivel de enlace de datos según el modelo de referencia OSI, ofrece a los usuarios la misma flexibilidad que PPTP para manejar protocolos distintos a IP, como IPX.

- L2TP (Layer 2 Tunneling Protocol): Este es un protocolo normalizado por la IETF como RFC 2661 y cabe destacar que utiliza el protocolo PPP para proporcionar una envoltura inicial de los datos y luego incluir los encabezados adicionales a fin de transportarlos a través de la red. L2TP puede transportar una gran variedad de protocolos y, además, es capaz de trabajar directamente con otros medios, como X.25, Frame Relay o ATM.

  L2TP puede usar certificados de seguridad de clave pública para cifrar los datos y garantizar la autenticidad de los usuarios de la VPN. Para potenciar el cifrado y la autenticación, L2TP suele implementarse junto con IPSec, otra tecnología VPN. Otra característica que hay que destacar es que permite establecer múltiples túneles entre dos puntos finales pudiendo proporcionar diferentes calidades de servicio (QoS).

  L2TP no presenta unas características criptográficas especialmente robustas si no es implementado junto a IPSec ya que sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel. Además, sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio (DoS) por medio de mensajes falsos de control que den por acabado el túnel L2TP o la

[5] Frame Relay: Transmite una variedad de tamaños de tramas o marcos ("frames") para datos, perfecto para la transmisión de grandes cantidades de datos.
[6] Pasarela: es un sistema de hardware/software para conectar dos redes entre sí y para que funcionen como una interfaz entre diferentes protocolos de red.

conexión PPP subyacente. Por otra parte, L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos. Por último, a pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

2.3.6.2. VPN Basadas en IPSec

IPSec (de las siglas en inglés Internet Protocol Security) según Tomás, 2008 "es un conjunto de estándares abiertos que trabajan de forma conjunta para garantizar entre entidades pares en el nivel de red confidencialidad, integridad y autenticación independientemente de cuál sea el medio de transporte (Frame Relay, PPP, xDSL, ATM,…). El objetivo para el que fue diseñado IPSec fue para las comunicaciones sobre el protocolo de Internet (IP). IPSec y los protocolos que implementa se han especificado en numerosos RFCs entre los que se encuentran 1826, 1827, 2401, 2402, 2406, 2408, 4301 y 4309".

El protocolo IPSec permite definir un túnel entre dos pasarelas. Una pasarela IPSec consistiría normalmente en un router de acceso o un cortafuego en el que esté implementado el protocolo IPSec. Las pasarelas IPSec están situadas entre la red privada del usuario y la red compartida del operador.

Los túneles IPSec se establecen dinámicamente y se liberan cuando no están en uso. Para establecer un túnel IPSec, dos pasarelas deben autentificarse y definir los algoritmos de seguridad y las claves que utilizarán para el túnel. El paquete IP original es cifrado en su totalidad e incorporado en encabezamientos de autentificación y encriptación IPSec. Se obtiene así la carga útil de un nuevo paquete IP cuyas direcciones IP de origen y destino son las direcciones IP de red pública de las pasarelas IPSec. Se establece así la separación lógica entre los flujos de tráfico de la VPN en una red IP compartida. Seguidamente, se utiliza un encaminamiento IP tradicional entre los extremos del túnel.

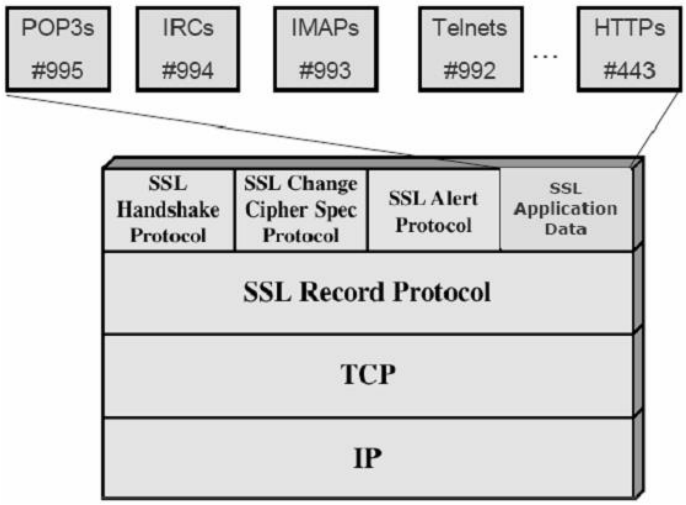
2.3.6.3. VPN Basadas en SSL/TLS

Los protocolos SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de la capa de transporte que proporcionan comunicaciones seguras en Internet. SSL fue diseñado por Netscape en 1996 y, aunque no es un protocolo estandarizado por el IETF, éste lo estandarizó en 1999 con ligeras modificaciones, aunque el protocolo funcionaba de la misma manera. Según Tomás, 2008 "La primera definición de TLS apareció en el RFC 2246, aunque se han ido publicando otras definiciones relacionadas con la compatibilidad de TLS con otros protocolos y técnicas criptográficas. SSL/TLS permite la autenticación tanto de cliente como servidor, usando claves públicas y certificados digitales y proporciona comunicación segura mediante el

cifrado de la información entre emisor y receptor. SSL/TLS funciona por encima del protocolo de transporte (normalmente TCP) y por debajo de los protocolos de aplicación. Este protocolo está muy extendido para realizar actividades de comercio electrónico de tal manera que Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet".

Según Tomás, 2008, SSL/TLS se compone de cuatro protocolos. Estos protocolos funcionan de manera idéntica en SSL y en TLS pero incorporan algunos detalles en TLS para su mejor funcionamiento. A continuación se definen estos cuatro protocolos sin entrar en mucho detalle:

- **Record Protocol:** Encapsula los protocolos de nivel más alto y construye un canal de comunicaciones seguro. Se podría decir que es un protocolo de transporte.
- **Handshake Protocol:** Se encarga de gestionar la negociación de los algoritmos de cifrado y la autenticación entre cliente y servidor. Define las claves de sesión utilizadas para cifrar. Se podría decir que es un protocolo de autenticación.
- **Change Cipher Spec Protocol:** Es un mensaje de un byte para notificar cambios en la estrategia de cifrado.
- **Alert Protocol:** Señaliza alertas y errores en la sesión establecida.



Fuente: Tomás, 2008

Figura Nº 02: Situación de SSL/TLS en la pila de protocolos OSI

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución siendo una de las más populares la biblioteca OpenSSL.
SSL es capaz de trabajar con la mayoría de protocolos que trabajan sobre TCP de tal manera que el [7]IANA les tiene asignado un número de puerto por defecto, por ejemplo el protocolo HTTP sobre SSL ha sido denominado HTTPS y tiene como puerto el 443.
SSL se basa en un esquema de clave pública para el intercambio de claves de sesión. En primer lugar cliente y servidor intercambian una clave de longitud suficiente mediante un algoritmo de cifrado asimétrico como RSA o Diffie-Hellman utilizando certificados. Mediante esa clave se establece un canal seguro, utilizando para ello un algoritmo simétrico previamente negociado. Los mensajes a ser transmitidos, se fragmentan en bloques, se comprimen y se les aplica un algoritmo Hash para obtener un resumen (MAC del mensaje) para asegurar la integridad.

Es importante especificar las diferencias entre SSL/TLS con otros protocolos ya que SSL/TLS fue escogido para la implementación de la VPN en esta investigación.

2.3.6.4. VPN SSL/TLS y VPN PPTP

PPTP funciona con casi todo tipo de sistemas operativos y, en la mayoría de casos, su uso no requiere de ningún software adicional. También funciona con muchos sistemas móviles, como Iphone, Ipad y Windows Mobile, y es fácil de configurar. En contraste, la configuración de OpenVPN basada en SSL, puede ser un poco más complicada comparada con la de PPTP, pero con las instrucciones adecuadas, cualquiera podría configurar la conexión sin mayor dificultad.

El método de cifrado de PPTP usa una contraseña como clave y su datastream lleva una contraseña hash recuperable. Si alguien del exterior interceptara tu tráfico y crackeara el cifrado (que aunque no sea fácil de hacer, es posible), podría descifrar tu tráfico. Sin embargo, OpenVPN usa un método de cifrado (blowfish por defecto) muy seguro. Incluso si alguien consiguiera interceptar tu tráfico, no podrían hacer nada con el mismo. Esto hace que OpenVPN sea más seguro que PPTP. Según TuVPN (2011), en 1998, Bruce Schneier and Mudge realizaron un análisis de Microsoft PPTP en la cual destaco "La implementación de Microsoft es seriamente defectuoso en varios niveles", según Bruce Schneier (1999), presidente de Sistemas de Counterpane. "Se utiliza la autenticación y el cifrado débil pobres. Por ejemplo, utilizan la contraseña del usuario como una clave de cifrado en lugar de utilizar cualquiera de las alternativas conocidas y más seguro", explicó Schneier.

7 IANA: Registro central de protocolos, puertos, números de protocolos y códigos de Internet.

Según el equipo que hizo el criptoanálisis, hay por lo menos cinco fallas principales en esta aplicación. Ellos son:

- Hash de la clave - algoritmos débiles permiten espías para saber la contraseña del usuario
- Desafío / Respuesta de autenticación del protocolo - un defecto de diseño permite a un atacante hacerse pasar por el servidor
- Cifrado - errores de aplicación permiten que los datos cifrados por recuperar
- Clave de cifrado - contraseñas comunes de rendimiento claves frágil, incluso para el cifrado de 128 bits
- Canal de control - los mensajes permiten a los atacantes no autenticados accidente servidores PPTP

2.3.6.5. VPN SSL/TLS y VPN IPSec

A continuación se dará algunas ventajas y desventajas de SSL Y IPSec, que servirán para comparar cual es la mejor tecnología a implementar en nuestra investigación.

Ventajas de SSL/TLS:

- OpenVPN basado en SSL no opera en el kernel, sino que opera en el espacio de usuario incrementando de esta manera la seguridad y la escalabilidad. Según el autor, James Yonan, "uno de los mayores frenos de IPSec es que añade una gran complejidad en kernel". La complejidad es el enemigo de la seguridad. El problema de añadir dicha complejidad de seguridad software en el kernel es que se ignora un importante principio de los sistemas de seguridad: nunca se ha de diseñar un sistema en el que si uno de los componentes cae pueda poner en peligro todo el sistema.
  Un simple desbordamiento de un buffer en el espacio del kernel provocaría un compromiso total en la seguridad del sistema. Es por esta razón que OpenVPN ubica su complejidad y ejecuta su código dentro del espacio de usuario pudiendo contener los fallos en este espacio más rápidamente sin comprometer la seguridad del sistema.
- Ofrece confidencialidad (cifrado simétrico), autenticación del servidor y del cliente (este último opcional) e integridad de los mensajes brindando unos niveles de seguridad excelentes que permiten el establecimiento de extranets con confianza y tranquilidad.
- Bajos costes de mantenimiento y no requiere mantenimiento en los clientes además de tener una buena interoperabilidad.
- Se pueden encontrar en Internet numerosas implementaciones de libre distribución para implementar redes privadas virtuales basadas en SSL/TLS.
- Muchas implementaciones de VPN basadas en SSL/TLS ofrecen mecanismos para defenderse frente a ataques del tipo "man in the middle" y ataques de denegación de servicio (DoS)

Desventajas de SSL/TLS:

- Protección parcial, ya que garantiza la integridad y confidencialidad de los datos únicamente durante el tránsito de los mismos, pero no los protege una vez recibidos por el servidor. Por tanto, un hacker podría manipular tranquilamente un servidor por lo expuesto anteriormente, pero a se implementa una buena seguridad en la red, esto no será problema.
- No es una solución totalmente transparente para el usuario final.
- Tiene problemas con algunos protocolos de la capa de transporte y con ciertas aplicaciones, sobre todo con protocolos no orientados a conexión.

Aplicaciones en la Actualidad de SSL/TLS:

- SSL puede ser usado para tunelizar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.
- Se usa en la mayoría de los casos junto a HTTP para formar HTTPS. HTTPS es usado para asegurar páginas Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.
- La mayoría de las aplicaciones son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el http, nntp, ldap, imap, pop3.
- SSL/TLS se puede utilizar en aplicaciones como: Applets de Java, controles ActiveX, Microsoft FrontPage o Adobe PageMill, o FileMaker Pro de Claris.
- Librerías multiplataforma como OpenSSL.

Ventajas de IPSec:

- IPSec ofrece confidencialidad (cifrado), autenticación e integridad.
- Basado en estándares y muy adecuado para tráficos totalmente IP.
- IPSec está debajo de la capa de transporte, por lo que resulta transparente para las aplicaciones.
- IPSec puede ser transparente a los usuarios finales.
- Compatible con la infraestructura de claves públicas.
- Provee un alto grado de encriptación a bajo nivel.
- Estándar abierto del sector. IPSec proporciona una alternativa de estándar industrial abierto ante las tecnologías de cifrado IP patentadas. Los administradores de la red aprovechan la interoperabilidad resultante.

Desventajas de IPSec:

- En la mayoría de los casos, su implementación necesita modificaciones críticas al kernell.

- IPSec no es seguro si el sistema no lo es. Los gateways de seguridad deben estar en perfectas condiciones para poder confiar en el buen funcionamiento de IPSec.
- Puede ser vulnerable a ataques del tipo "man in the middle" y de denegación de servicio (DoS).
- Es un protocolo complejo de entender, su configuración es complicada y además requiere una configuración minuciosa en el cliente. Su administración suele ser lenta y complicada.
- Tiene un alto coste de implementación y de mantenimiento.
- IPSec autentica máquinas, no usuarios: el concepto de identificación y contraseña de usuarios no es entendido por IPSec, si lo que se necesita es limitar el acceso a recursos dependiendo del usuario que quiere ingresar, entonces habrá que utilizar otros mecanismos de autenticación en combinación con IPSec.
- Problemas con traducción de direcciones NAT (Network Address Translation).
- Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre sí.
- Necesita del uso de muchos puertos y protocolos en el sistema hardware que lo implemente (router, firewall,...).

Aplicaciones en la Actualidad de IPSec:

- El proyecto FreeS/WAN es la primera implementación completa y de código abierto de IPsec para Linux.
- Desarrolla y depura aplicaciones web ASP.NET en Delphi 2005 mediante
- Comercio electrónico de negocio a negocio pero con menos influencia que SSL/TLS.

2.3.7. Servidores VPN bajo software libre

Según la revista Linux Journal (2008), existen varios servicios de los cuales nos permite crear estos túneles en GNU/Linux, los más conocidos son:

a) **OpenVPN:** Es un proyecto de código abierto creado por James Yonan. Proporciona una solución VPN basada en SSL / TLS.
La capa de transporte Security (TLS) y su predecesor Secure Sockets Layer (SSL), son protocolos criptográficos que proporcionan comunicaciones seguras de transferencia de datos en Internet. SSL ha estado en existencia desde principios de los 90; el modelo de red OpenVPN se basa en TUN / TAP, los dispositivos virtuales TUN / TAP son parte del kernel de Linux.

b) **Openswan:** Es un proyecto de código abierto que proporciona una aplicación de las herramientas de usuario para Linux de IPsec. Se puede crear un VPN con herramientas Openswan. El proyecto Openswan se inició en 2003 por el ex FreeS / WAN desarrolladores. FreeS / WAN es el predecesor de Openswan. S / WAN significa seguridad de red de área extensa, que en realidad es

una marca comercial de RSA. Openswan se ejecuta en muchas diferentes plataformas.

2.3.8. OpenVPN

Es importante saber el concepto de OpenVPN y cuál es la estructura que la forma, ya que esta herramienta ha sido escogida para la investigación. Es un proyecto de código abierto creado por James Yonan. Proporciona una solución VPN basada en SSL / TLS. Como ya se menciono, la capa de transporte Security (TLS) y su predecesor Secure Sockets Layer (SSL), son protocolos criptográficos que proporcionan comunicaciones seguras de transferencia de datos en Internet. SSL ha estado en existencia desde principios de los 90; el modelo de red OpenVPN se basa en TUN / TAP, los dispositivos virtuales TUN / TAP son parte del kernel de Linux.

OPENVPN está basado en software libre, según GNU el término de software libre es una cuestión de la libertad de los usuarios de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Más precisamente, significa que los usuarios de programas tienen las cuatro libertades esenciales. La libertad de ejecutar el programa, para cualquier propósito:

- La libertad de estudiar cómo trabaja el programa, y cambiarlo para que haga lo que usted quiera. El acceso al código fuente es una condición necesaria para ello.
- La libertad de redistribuir copias para que pueda ayudar al prójimo.
- La libertad de distribuir copias de sus versiones modificadas a terceros. Si lo hace, puede dar a toda la comunidad una oportunidad de beneficiarse de sus cambios. El acceso al código fuente es una condición necesaria para ello.

2.3.8.1. VENTAJAS DE OPENVPN

Según Feilner y Graf (2009), "con la llegada de OPENVPN una nueva generación de VPN entro en escena. Mientras otras soluciones VPN suelen usar mecanismos propietarios o no-estándar, OPENVPN tiene un concepto modular, tanto para subrayar la seguridad como para trabajo de red (networking). OPENVPN usa los seguros, estables y alabados mecanismos SSL/TLS y los combina en su propia base de confianza. No sufre de la complejidad que caracteriza otras implementaciones VPN como el líder de mercado IPSec. Al mismo tiempo, ofrece posibilidades que van más allá del ámbito de aplicación de otras implementaciones VPN.693."

- Capa VPN 2 y 3: OPENVPN ofrece dos modos básicos, que funcionan como Capa 2 o 3. Así, los túneles de OPENVPN en la Capa 2 también pueden transportar marcos Ethernet, paquetes IPX, y paquetes de Windows de Navegación en la Red (Windows Network Browsing), todos los cuales son problemas en la mayoría de otras soluciones VPN.
- Protegiendo los trabajadores de campo con el firewall interno: Un trabajador de campo conectado a la rama central de su compañía con un túnel PVN puede cambiar la configuración de la red en su laptop

para que todo su tráfico de red sea enviado por el túnel. Una vez que VPN ha establecido un túnel, el firewall central en la rama central de la compañía puede proteger la laptop, incluso si no es una maquina local. Solo el puerto de red debe estar abierto a la red local por el trabajador de campo. El empleado es protegido por la firewall central cuando sea que se conecte al VPN. Incluso mejor, el administrador del servidor VPN de la centran puede forzar al cliente a usar el firewall central imponiendo opciones de configuración a los clientes.

- Conexiones VPN abiertas pueden ser tuneleadas a través de casi todos los firewall y proxy: Si tienes accedo a internet y puedes acceder sitios web HTTPS, entonces los túneles OPENVPN deben funcionar. Las configuraciones en que túneles OPENVPN están prohibidos son muy raras. OPENVPN tiene total soporte proxy incluyendo autenticación.
- Modo cliente y servidor, soporte UDP y TCP: OPENVPN puede ser configurado para funcionar como TCP o UDP y como un servidor o cliente. Como servidor simplemente espera hasta que un cliente pida conexión, mientas el cliente establece conexión de acuerdo a su configuración. Un servidor en el internet puede ser completamente apagado de cualquier otra máquina excepto las que están en su red virtual privada, lo que extiende el nivel de seguridad de tales sistemas enormemente.
- Sólo un puerto en la firewall debe ser abierto para permitir conexiones entrantes: Desde que OPENVPN2.0, el modo de servidor especial, permite múltiples conexiones entrantes en el mismo puerto TCP o UDP, mientras sigue usando diferentes configuraciones para cada conexión.
- No hay problemas con NAT: OPENVPN y los clientes pueden estar dentro de una red usando solo direcciones IP privadas. Cada firewall puede ser usada para enviar el tráfico de túnel al punto final del túnel.
- Interfaces virtuales permiten flexible y específicas redes y casi cada regla de firewall imaginable: Todas las restricciones, mecanismos como reenvío, y conceptos como NAT (Traducción de Dirección de Red) o paquetes mangling (cambiar la metadatos de los datagramas como algunas firewalls hacen) puede ser usado con y dentro de túneles OPENVPN. Cualquier Protocolo IP es posible. Sí, tu puedes tunelear VPN, como IPsec, dentro de un túnel OPENVPN.
- Alta flexibilidad con posibilidades extensas de secuencias de comandos (scripting): OPENVPN ofrece numerosos puntos durante la configuración de conexión para iniciar secuencias de comandos individuales. Estas secuencias de comandos pueden ser usadas para una gran variedad de propósitos de autenticación a conmutación por error y más.
- Soporte transparente y de alto desempeño para IPs dinámico: Usando OPENVPN, no hay más necesidad de usar IPs estático y caro en ningún lado del túnel. Ambos puntos finales del túnel pueden tener acceso DSL barato con IPs dinámicos. Los usuarios rara vez notaran un cambio de IP en algún punto final, las sesiones del Windows Terminal Server y Secure Shell (SSH), solo parecerán sostenerse por unos segundos, pero no se terminaran y seguirán con la acción pedida

luego de una corta pausa. Todo tráfico puede ser comprimido a través de la biblioteca LZO y un OPENVPN continuamente chequea si la compresión ha sido exitosa. La compresión llamada adaptativa meramente Zipeaa la información no comprimida para evitar una recarga innecesaria.

- Instalación simple en cualquier plataforma: Uso e instalación son increíblemente simples. Especialmente, si has intentado configurar conexiones IPsec con diferentes implementaciones, encontraras atractivo el OPENVPN.
- Diseño modular: El diseño modular con un alto grado de simplicidad en seguridad y red es sobresaliente. Ninguna otra solución VPN ofrece las mismas opciones en este nivel de seguridad.
- Soporte para móvil e incrustado: Más y más dispositivos móviles son soportados. Paquetes para Windows Mobile y la plataforma de Nokia Maemo, y sistemas operantes incrustados como IPENWRT/FREEWRT han sido todos proveídos recientemente, y hay muchos otros en desarrollo
- Comunidad muy activa: OPENVPN ha adquirido una gran cantidad de fans en los últimos años. Hay instalaciones con usuarios de alto volumen con alta disponibilidad

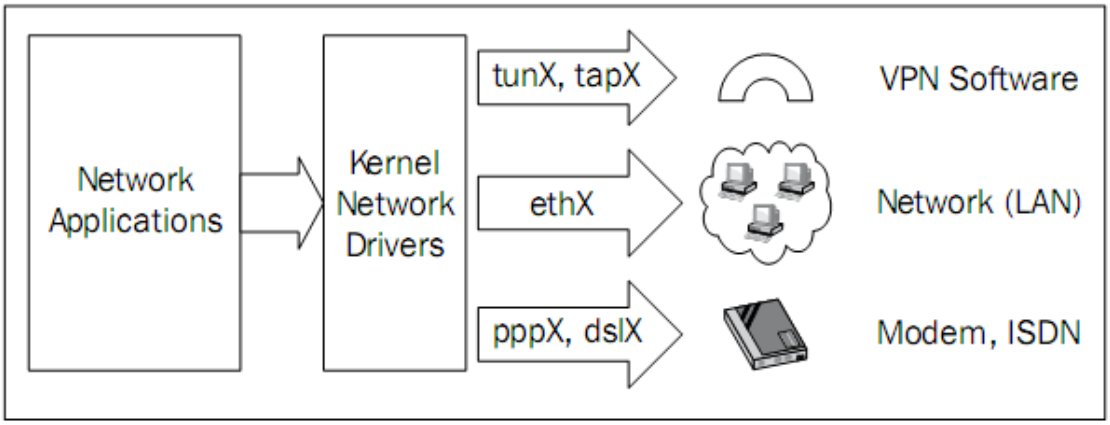
2.3.8.2. Networking con OPENVPN

La estructura modular de OpenVPN no solo puede ser encontrada en su modelo de seguridad, sino también en el esquema de networking. James Yonan eligió el driver universal TUN/TAP para la capa de networking de OpenVPN.

El driver TUN/TAP es proyecto de fuente abierta (Open Source) que está incluido en todas las distribuciones Linux/UNIX, es usado en muchos proyectos, y por ello está continuamente siendo mejorado, y nuevas funciones le son añadidas. El uso de dispositivos TUN/TAP quita mucha de la complejidad de la estructura de OpenVPN. Su estructura simple trae seguridad aumentada cuando se compara a otras soluciones VPN. La complejidad es siempre el primer enemigo de la seguridad. Por ejemplo, IPsec tiene una estructura compleja con modificaciones complejas en la central (kernel) y el stack (pila, montón) IP, creando muchas escapatorias de seguridad posibles.

El driver universal TUN/TAP es uno de los principales factores que hace a OpenVPN muy fácil de entender, fácil de configurar y, al mismo tiempo, muy seguro.

La siguiente figura grafica a OpenVPN usando interfaces estándar:



Fuente: Feilner y Graf, 2009

Figura Nº 03: Paquete IP en IPSec para Modo Túnel

2.3.8.3. OPENVPN Y FIREWALLS

Openvpn trabaja perfectamente con firewalls. Hay algunas soluciones VPN que pueden decir tener un soporte de firewall similar, pero ningún otro puede ofrecer el mismo nivel de seguridad.

Que es un firewall? Hay una famosa y simple definición:
Un firewall es un router que sólo rota información de internet seleccionada. Las reglas firewall definen como manejar información específica y trafico.

Los firewalls pueden ser dispositivos o software en las computadoras, servidores, o en otros dispositivos, un firewall cuida la información que ha sido recibida y la observa más de cerca. Los firewalls modernos son como filtros de paquetes, firewalls de inspección con estado (stateful inspection firewalls). Dependiendo de la capa OSI en que está operando, el firewall puede pasar decisiones basada en la información que es encontrada en los encabezados de los paquetes o datos de aplicación. Los firewall de filtro de paquetes usualmente operan leyendo el encabezado de la información IP. La inspección con estado es un mecanismo para recordar los estados de conexión. En esta forma, las redes internas pueden ser protegidas de redes externas. Mientras las conexiones de internet iniciadas de dentro pueden ser permitidas, toda no autorizada conexión del exterior puede ser rechazada. Al mismo tiempo, información entrante pedida por un miembro de la red local es pasado (porque el firewall recuerda el estado de la petición)

Bajo Linux, la mayoría de firewalls están basadas en el programa IPTABLES. Esta es una interface user-space para la funcionalidad de firewall de filtro de red de la central de Linux, y ofrece todo lo que las firewalls modernas deberían. Probablemente la mejor manera de proteger tu LAN es escribiendo una lista de reglas IPTABLES con un libreto de caparazón (Shell script). Sin embargo, la usabilidad de tal

libreto no es perfecta. La mayoría de administradores quiere una interfaz de usuario grafica (GUI) para control de firewall y todos los firewalls de hardware ofrecen esto. Las herramientas y firewalls Linux más resaltantes son:

- El proyecto Shorewall (shoreline firewall) está basado en código abierto, es un herramienta para Linux que se basa en los Netfilter (iptables o ipchains) incorporado en el kernel de Linux, por lo que es más fácil de manejar esquemas de configuración más complejas.
  Los trabajadores gente del proyecto Shorewall, Simon Matter y Ton Eastep, han escrito una guía muy útil para la integración de túneles OpenVPN.
- IPCop es un prometedor sistema de firewall Linux independiente, fácil-de-configurar, que está también equipado con un GUI profesional. Ha tenido gran éxito en proyectos de tercer mundo como Linux4Africa y en otras organizaciones de medio tamaño. Instalación estandarizada, estructuras simples, hacen este un proyecto de rápido crecimiento, y con la ayuda de OpenVPN, el firewall IPCop se convierte un verdadero servidor VPN.
- Herramientas como Fwbuilder (constructor de firewall) te ayudan a construir, manejar y distribuir tus libretos IPtables (IPtables scripts) por ti mismo. Fwbuilder hace incluso más. Puede trabajar independientemente de tu plataforma y es capaz de traducir reglas Linux a Cisco, BSD, u otros idiomas firewall. Esto en verdad vale mucho.

2.3.8.4. PROBLEMAS CON OPENVPN

Según Markus y Norbert G.2009, OpenVPN tiene algunas debilidades:

- No es compatible con IPsec, e IPsec es la solución VPN estándar. Muchos dispositivos como los routers Cisco y Bintec usan IPsec y pueden conectarse a aplicaciones de otros manufactureros o clientes de IPsec software. Al menos deben poder, porque en la práctica muchos manufactureros tienden a desarrollar sus propias extensiones propietarias a IPsec, lo que hace sus implementos prácticamente incompatibles con otros dispositivos IPsec.
- OpenVpn no está definido por ningún RFC. Pero para el futuro, Yonan ha anunciado varias veces que RFC 4347 (DTLS –Datagram Tranport Layer Security) ofrece una especificación muy prometedora con módulos compatibles tomados en cuenta.
- Sigue habiendo unas cuantas personas que saben cómo usar OpenVPN, especialmente en escenarios difíciles (a pesar de que estos tienden a ser raros).
- No hay GUI de clase de empresa para administración (Enterprise class GUI), pero hay algunos proyectos prometedores.
- Hoy puedes solo conectarte a otros computadores. Pero esto está cambiando, hay compañías trabajando en dispositivos con clientes OpenVPN integrados.

- OpenVPN funciona en espacio de usuario y todo el tráfico de red necesita ir desde el espacio de la central al espacio de usuario y de vuelta.

Como se puede ver, las principales debilidades de OpenVPN son la incompatibilidad con IPsec y falta de conocimiento del público sobre sus funciones y sus manufactureros de hardware. El primero probablemente nunca cambiara porque las arquitecturas difieren mucho, pero el segundo esta ya cambiando.

2.3.8.5. OPENVPN COMPARADO CON VPN IPSEC

A pesar de que IPsec es el estándar de hecho, hay muchos argumentos para usar OpenVPN. Si quieres convencer a tu gerencia sobre por qué tus ramas deberían estar conectadas a través de OpenVPN en vez de VPN IPSec, entonces la siguiente tabla puede ayudar a tu argumento (los puntos precedidos por "+" son ventajas y los precedidos por "-"son desventajas). Según Markus, F., y Norbert, G.2009, las principales diferencias:

IPSEC VPN	OPEN VPN
+ La tecnología VPN estándar.	-Sigue casi desconocido, no compatible con Ipsec, de repente pronto sea estandarizada en parte por el uso de DTLS.
+ Plataformas de hardware (dispositivos, aplicaciones)	-Solo en computadoras, pero en todos los sistemas disponibles. -Nueva tecnología, aun creciendo y levantándose.
+ Tecnología bien conocida	-Tecnología nueva y aun en crecimiento.
+Muchos GUI para administración.	-Ningún GUI profesional, sin embargo, hay algunos interesantes y prometedores proyectos
-Modificación compleja de la pila IP (pila, montón)	+Tecnología simple.
-Modificación critica del	+Interfaces de red y paquetes

kernel necesaria.	estandarizados.
-Se necesitan privilegios de administrador.	+El software Openvpn puede funcionar en espacio de usuario, y puede ser chroot-ed.
-Diferentes implementaciones Ipsec de diferentes proveedores pueden ser incompatibles.	+Tecnologías de codificación estandarizadas.
-Configuración compleja, tecnología compleja.	+Tecnología fácil, bien estructurada y configuración sencilla.
-Curva de aprendizaje escarpada para novatos.	+Fácil de aprender y éxito rápido para principiantes
-Varios puertos y protocolos en firewall son necesarios.	+ Solo se necesita un puerto en firewall.
-Problemas con direcciones dinámicas en ambos lados.	+ dyndns (dns dinámico) trabaja sin fallas, y se reconecta rápido.
-Problemas de seguridad con tecnologías Ipsec.	+SSL/TLS como capa criptográfica estándar de industria.
	+ Modelado de trafico
	+Rapidez (hasta 20 mbps en una maquina de 1ghz)
	+Compatibilidad con firewalls y proxies
	+Sin problemas con NAT (ambos lados pueden estar en redes nateadas)

	+Posibilidades para Road Warriors.

Probablemente el mejor argumento es que puedes usar ambas soluciones VPN paralelamente, siempre y cuando estés usando UNIX o una aplicación basada en LINUX. Debido a los acercamientos diferentes a networking, no hay conflictos entre los dos sistemas.

2.3.8.6. ESPACIO DE USUARIO VS ESPACIO DE KERNEL

OpenVPN al operar en capa usuario incrementa la seguridad y la escalabilidad. Según el autor, James Yonan, "uno de los mayores frenos de IPSec es que añade una gran complejidad en kernel. La complejidad es el enemigo de la seguridad". El problema de añadir dicha complejidad de seguridad software en el kernel es que se ignora un importante principio de los sistemas de seguridad: nunca se ha de diseñar un sistema en el que si uno de los componentes cae pueda poner en peligro todo el sistema.
Un simple desbordamiento de un buffer en el espacio del kernel provocaría un compromiso total en la seguridad del sistema. Es por esta razón que OpenVPN ubica su complejidad y ejecuta su código dentro del espacio de usuario pudiendo contener los fallos en este espacio más rápidamente sin comprometer la seguridad del sistema.

2.3.8.7. Requerimientos de hardware

Según la empresa NettixPeru, 2005, para realizar esta conexión es necesario que en cada local se tenga una conexión a internet de calidad. Adicionalmente se requiere que haya un PC o Servidor como mínimo Pentium 4 con 256Mb de memoria y disco duro de 80Gb en Linux que haga el enlace VPN hacia la(s) otra(s) red(es).
El servidor VPN, cifrara y comprimirá de manera segura la información enviándola al sitio remoto que se desea, todo esto de manera transparente a los usuarios y como si todos estuvieran en el mismo local.

III. MATERIALES Y MÉTODOS

En el desarrollo y aplicación de la investigación se empleó software libre, utilizando el sistema operativo LINUX en su distribución CentOS 5.4 con la ayuda de la solución OpenVPN, la cual fue adecuada a la realidad de la Corporación ADEU.

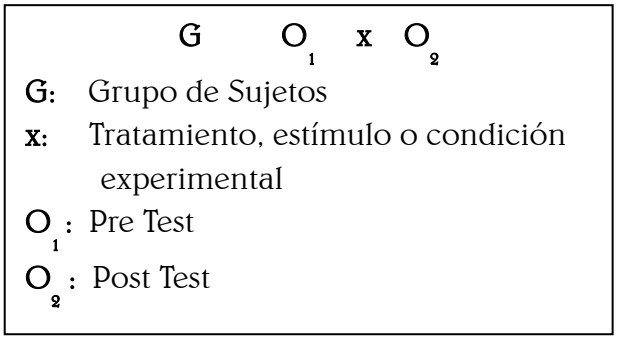
Se realizó una prueba piloto, en la cual se siguieron una serie de pasos de acuerdo la metodología" ¿Cómo desarrollar una red segura?" desarrollada por la empresa CYBSEC .Se implementó la herramienta OpenVPN en redes distintas, instalando un usuario y un servidor para la conexión y efectuando el pase de datos entre los locales, para demostrar el mejor acceso a la información. También se efectuaron pruebas de evaluación de seguridad y vulnerabilidad de la red, para demostrar la seguridad en el pase de la información. Por último se compraró nuestra implementación con un servicio contratado para constatar la rentabilidad en los costos de su instalación.

3.1. Tipo de investigación y diseño de contrastación de hipótesis

Para el empleo de la VPN fue necesaria una serie de pruebas para analizar la eficiencia de la innovación tecnológica de la herramienta OpenVPN, ante un problema concreto que surge en las necesidades de la corporación ADEU. Por ello, esta investigación es de tipo tecnológica, como lo manifiesta Dean, (2005), "la innovación tecnológica designa la incorporación del conocimiento científico y tecnológico, propio o ajeno, con el objeto de crear o modificar un proceso productivo, un artefacto o una máquina, para cumplir un fin valioso para una sociedad"

Con investigación tecnológica en las ciencias de la ingeniería se designa un ámbito de producción de conocimiento tecnológico validado, que incluye tanto el producto cognitivo, teorías, técnicas, tecnologías, etc. como las actividades que desarrollan los ingenieros para producir y validar dichos productos y conocimientos".

De acuerdo al diseño de contrastación se emplearon Pre test - Post test con un sólo grupo, tal como se muestra en la Figura N°03. Este diseño fue planteado por Hernández , (2003).



Fuente: Hernández, 2003

Figura Nº 04: Diseño de contrastación Pre Test – Post Test con un sólo grupo.

Según este tipo de diseño, se realizaron 3 pasos, los cuales consistieron en:

- Analizar el impacto de las variables dependientes a ser estudiadas.
- Aplicar la variable independiente, es decir, implementar la VPN.
- Realizar un nuevo análisis de las variables dependientes que fueron estudiadas. De esta manera se obtuvieron los resultados que posteriormente son explicados a detalle.

3.2. Población y muestra de estudio

La población y la muestra serán la misma para esta investigación debido a que se entrevisto solamente a los integrantes del área de sistemas de la corporación ADEU, los cuales ascienden a la cantidad de 5 y desempeñan los siguientes cargos: Administrador del sistemas, desarrollador Web y 3 colaboradores. Por ser un número reducido de personal, se consideró que todos ellos formen parte de la muestra de la investigación.

3.3. Hipótesis

La implementación de una VPN bajo software libre OpenVPN, optimizará el acceso a los datos entre los locales de la corporación Educativa ADEU.

3.4. Indicadores

Variable	Indicador	Descripción	Unidad de Medida
Acceso a la información entre los locales	Satisfacción en el acceso a la información entre los locales.	Se evalúa la mejoría en el acceso a la información entre los locales	Cualitativa
Seguridad en la transferencia de los datos	Satisfacción respecto a la seguridad del medio utilizado.	Se evalúa la satisfacción con respecto a la seguridad.	Cualitativa
	Nivel de seguridad que brinda el medio de conexión.	Se evalúa el nivel de seguridad que brinda el medio a utilizar para la conexión.	Cualitativa
Minimización de los costos en la implantación tecnología VPN	Costo en la implementación de la VPN	Se evalúa los cotos en la implementación de la VPN.	Cuantitativo

3.5. Métodos Técnicas e Instrumentos de recolección de datos

La presente investigación, en su primera etapa estuvo centrada en la recolección de datos; para ello se empleó la entrevista a los trabajadores del área de sistemas del Colegio ADEU. Identificada la necesidad, se propuso y se implementó el servidor OPENVPN, el cual mediante indicadores fue evaluado para garantizar la conexión y el paso de información a través de la red. Posteriormente, con la ayuda de softwares de monitoreo de información, tales como WIRESHARK y ZENMAP, se procedió a la respectiva evaluación para garantizar la seguridad de la VPN.Implementada la solución propuesta, se decidió comparar los costos de instalación de OpenVPN con una VPN arrendada, de modo que quede documentada, establecida y sustentada la viabilidad de la implementación posterior de la misma.

El procesamiento para análisis de datos se hizó de la siguiente manera:

- Entrevista no estructurada: Se entrevisto a cada uno de los integrantes del área de sistemas y se analizó las preguntas para constrastarlas con la investigación. El tiempo asignado para las entrevistas con los encargados fue de acuerdo al tiempo que dispusieron estos para brindar la información.
- Software de monitoreo: Se implantó un software para monitorear el uso de la información, es decir, la confiabilidad del pase de informacion por el medio designado y la vulnerabilidad de los datos al pasar por este medio. Este software se empleó despues de realizar la VPN, para analizar los datos obtenidos.

3.6. Plan de procesamiento para análisis de datos

Para realizar un mayor análisis de la información obtenida en los resultados de la investigación se hizo uso de:

- Microsoft Office Excel 2007; software ofimático empleado para la realización de tablas y gráficos por cada uno de los criterios que fueron evaluados en la investigación.
- Microsoft Office Visio 2007; software ofimático que permite documentar, diseñar y comprender de forma visual el estado de los sistemas y procesos empresariales con una gran variedad de diagramas de flujo de proceso empresarial, diagramas de red, diagramas de flujo de trabajo, modelos de bases de datos y diagramas de software, entre otros.
- Wireshark; es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica para educación.
- ZENMAP 5.51; software de aplicación gráfica para manejar Nmap (Es un escáner de puertos que nos puede dar mucha información acerca de una PC. Además de averiguar el estado de los puertos, podemos saber el servicio que se está corriendo en ese puerto y a veces hasta el sistema operativo que utiliza.
- Packet tracer; herramienta de aprendizaje y simulación de redes. Esta herramienta permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

IV. RESULTADOS

Para la aplicación del sistema, se tuvo como referencia la metodología planteada por la empresa CYBSEC S.A.(2001).

4.1. Fase 1: Diseño de la arquitectura de red.

Se implemento una VPN entre las dos oficinas del la Corporación educativa ADEU, para mejorar el acceso a la información entre los locales.

Figura Nº 5: Ubicación de la Corporación.

Las oficinas están ubicadas en Calle Juan Cuglievan #651 la "Academia ADEU" y en la Av.Grau#135 el "Colegio ADEU".

Cada una de estas oficinas tendrá implementado un servidor VPN bajo software libre utilizando el sistema operativo LINUX en su distribución CentOS 5.4 con la ayuda de la solución OpenVPN.

A continuación se dará el esquema físico de la red que se propone (Figura Nº 10):

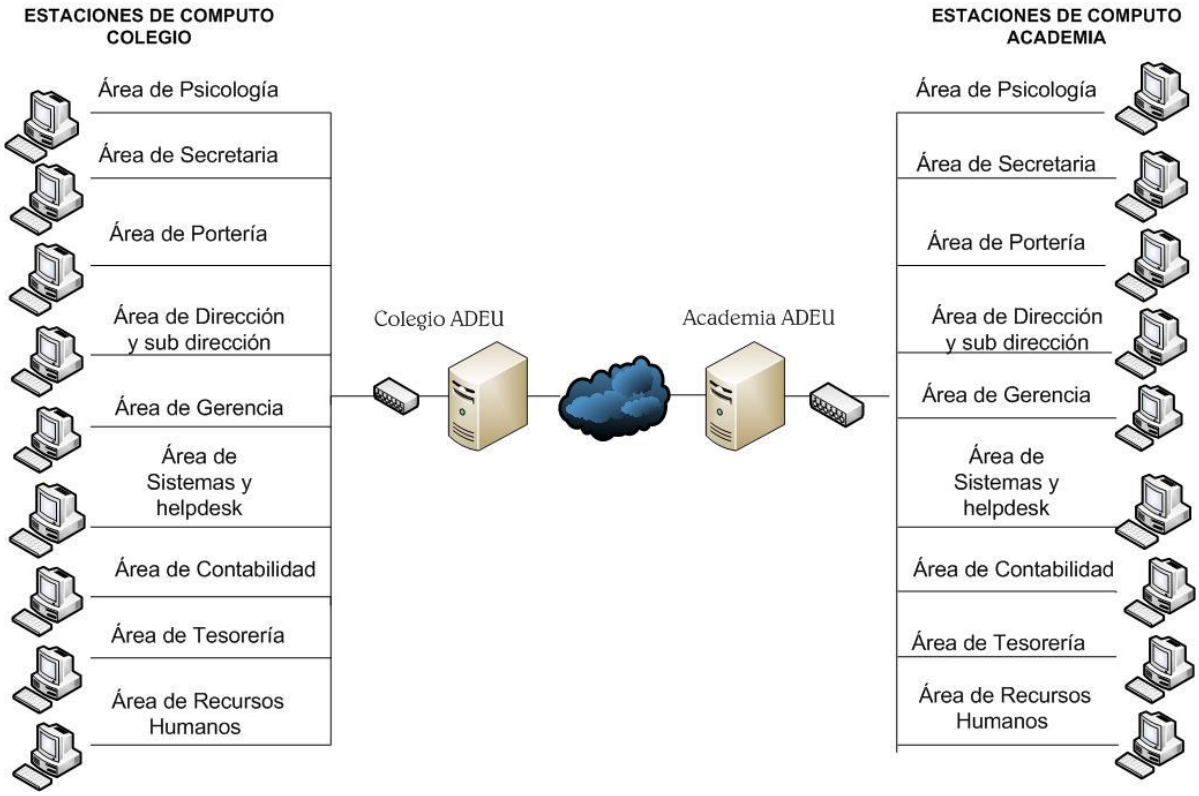


Figura Nº 6: Esquema físico de la red.

La grafica muestra el esquema físico de la red, en la cual se contó esencialmente con un Router, un Switch y un servidor para cada local.
Las oficinas del colegio ADEU se enlazaran con las oficinas de la academia ADEU a través de la VPN.
La topología que se propone para la simulación en cada oficina es la "Topología estrella" (Figura Nº 0 11).

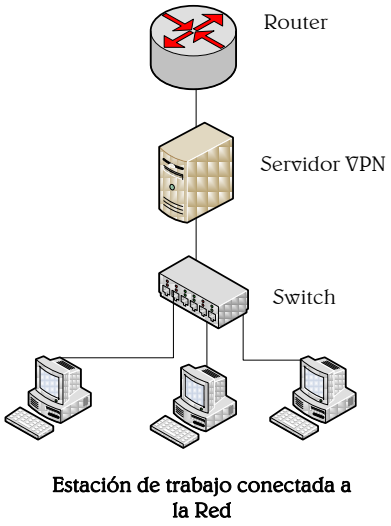


Figura Nº 7: Topología estrella utilizada en cada local.

La misma metodología se propuso para la simulación de ambas VPN:

1.- El Router se conectó al servidor VPN.
2.- El servidor VPN se conectó al Switch.
3.- Los clientes se conectaron al Switch, el número de clientes para la prueba fueron 2.

Para la implementación de la VPN se recomienda el siguiente hardware:

Hardware	Descripción
2 Servidores	Servidor HP ProLiant, con las siguientes características: DL120 G7 E3-1220, 4GB-U, 250 GB, LFF, conexión en frío, SATA B110i RAID, 400 W. Procesador: Intel® Xeon® E3-1220 (4 núcleos, 3,1 GHz, 8 MB, 80 W, 1333/t) Controlador de almacenamiento: (1) Smart Array B110i SATA RAID Unidades de disco duro incluidas: (1) SATA LFF; Conexión en caliente.
2 Switch	Switch de 24 puertos para la conexión del servidor y los clientes.
2 Tarjetas de red	Tarjetas de red de 100 MB, para la mejor transferencia de datos.
1 Conexión internet en cada oficina.	La conexión internet dependerá de la institución, pero se recomendó un servicio de Speedy Business para la mejor transferencia de datos.

A continuación se da a conocer el diseño Lógico de la Red que se propone (Figura N° 12):

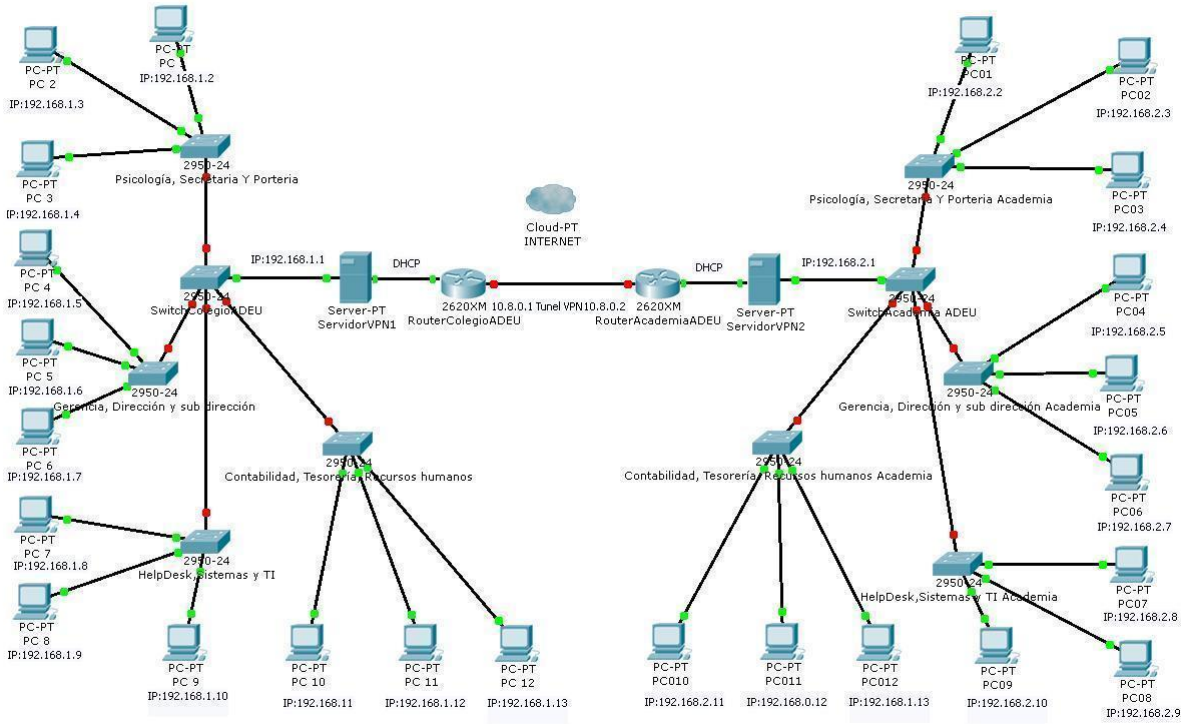


Figura N° 8: Diseño lógico de la Red.

Las configuraciones de los IP fue de la siguiente manera:
Para cada servidor se coniguro dos tarjetas de red.

Servidor 1

Eth0: IP Público, configurado como DHCP
Eth1: IP, 192.168.1.1
TAP: Tunneling VPN, 10.8.0.1
Cliente1 IP: 192.168.1.2

Servidor 2

Eth0: IP Público, configurado como DHCP
Eth1: IP, 192.168.2.1
TAP: Tunneling VPN, 10.8.0.2
Cliente2 IP: 192.168.2.2

Además del diseño de la red, es importante aplicar técnicas para el desarrollo de arquitecturas de una red segura, para esto se tuvo en cuenta dos aspectos importantes en la seguridad física de la red tales como acceso físico o alteraciones del entorno que puedan dañar nuestra red física.
Para cubrir estos inconvenientes se optó por una VPN NET to NET la cual se configuró en los servidores ya que la instalación de cliente a cliente podria resultar perjudicial, esto evita posibles instalaciones en maquinas ajenas a la corporación o que se sustraiga alguna maquina y se pueda conectar a nuestra red.

4.2. Fase 2: Evaluación de flujos de información.

El flujo de la información se realizó de la siguiente manera (Figura Nº 13):

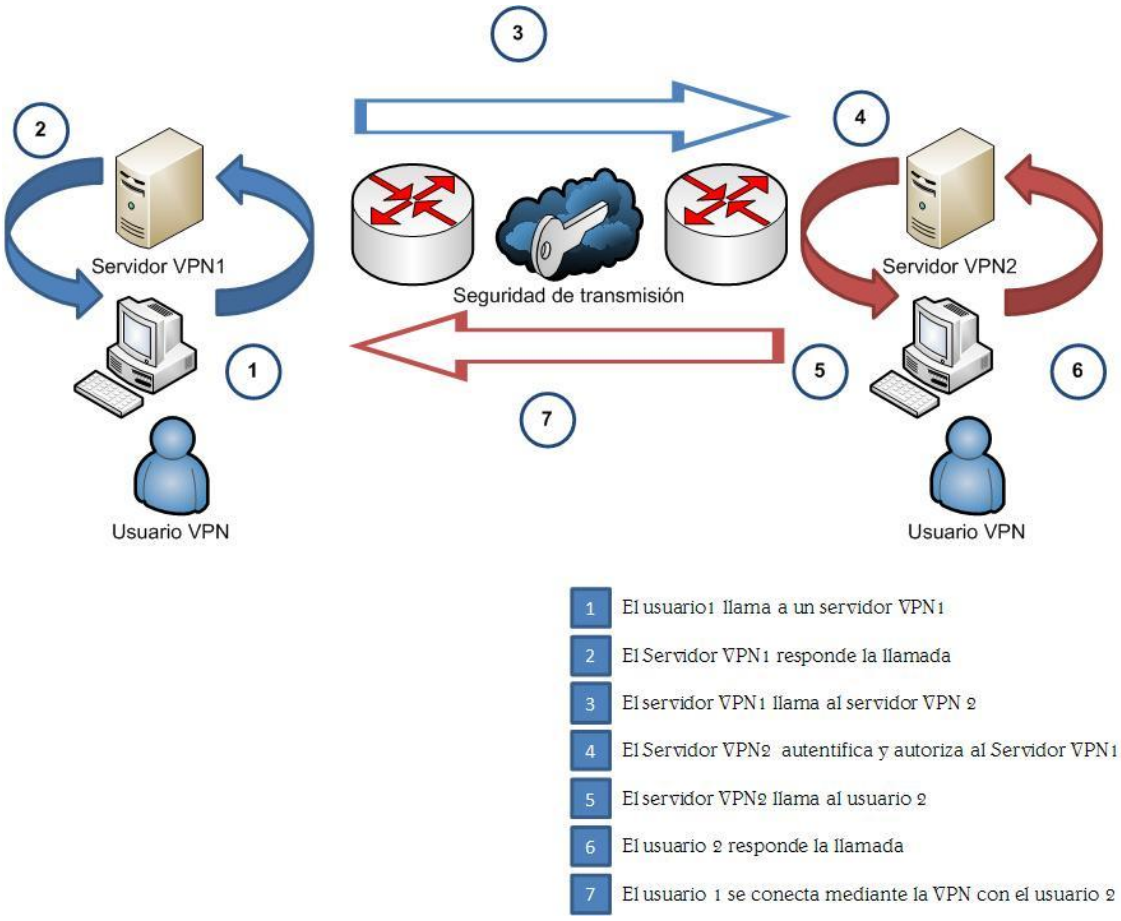


Figura Nº 9: Diagrama de flujo de información.

Para que la información llegue de un lugar a otro primero se debe hacer un pedido por parte del usuario1 solicitando la información al otro usuario. A continuación, el sevidor1 se conectará con el servidor2 el cual verificará si este pertenece a la VPN corporativa. Habiendo hecho la verificación, se conectará al usuario 2 el cual enviará la información solicitada por el ususario1.Este proceso puede darse de igual forma por parte del otro usuario, esto dependerá de quien pida la información.

4.3. Fase 3: Desarrollo para la implementación.

Para la implementación de la VPN bajo software libre utilizando el sistema operativo LINUX en su distribución CentOS 5.4 con la ayuda de la solución OpenVPN, se desarrolló un manual tanto para el Servidor1 y para el Servidor2, también se detalló la configuración para los clientes que se conecten a la Red. Este Manual se detalla en el Anexo 1.

4.4. Fase 4: Validacion de variables

4.4.1. Fase 4.1: Implementación de la VPN para mejorar el acceso a la información.

Una vez terminado el diseño de la red se procede a las pruebas de conexión, en esta etapa se realizaron diferentes pruebas para constatar la conexión exitosa de la VPN y así mejorar el acceso a la información entre los locales.

En esta etapa se efectuó una entrevista al ingeniero de la corporación educativa ADEU, quien mostró insatisfacción por los inconvenientes que ocasiona no tener un canal directo para transferir datos entre locales y, en ves de esto utilizar medios tales como correos electrónicos para su difusión, manifestando siguientes:

"Existe una deficiencia en la transferencia de datos, ya que resulta molesto acceder a la información sin tener un medio directo, retrasando la transmisión de los reportes de notas, asistencias, pagos, reporte de alumnos y de profesores, reportes administrativos y de planillas", señaló.

Después de analizar estos hechos, se implementó una VPN para mejorar el servicio en el acceso a la información entre los locales de la corporación ADEU.

Estas pruebas fueron medidas en función a la satisfacción del personal entrevistado y la forma en que les ayuda la implementación de esta herramienta, a mejorar el acceso a la información que manejan.

<u>Prueba</u>

Para la prueba se implementaron dos servidores, del Colegio ADEU y la Academia ADEU, la asignación de IP fue la siguiente:

	Red 1 Colegio ADEU	Red 2 Academia ADEU
Servidor	**192.168.1.1**	**192.168.2.1**
Usuario	**192.168.1.3**	**192.168.2.3**

Prueba del servicio OpenVPN: Mediante esta prueba verificamos si nuestro servicio OpenVPN corre.

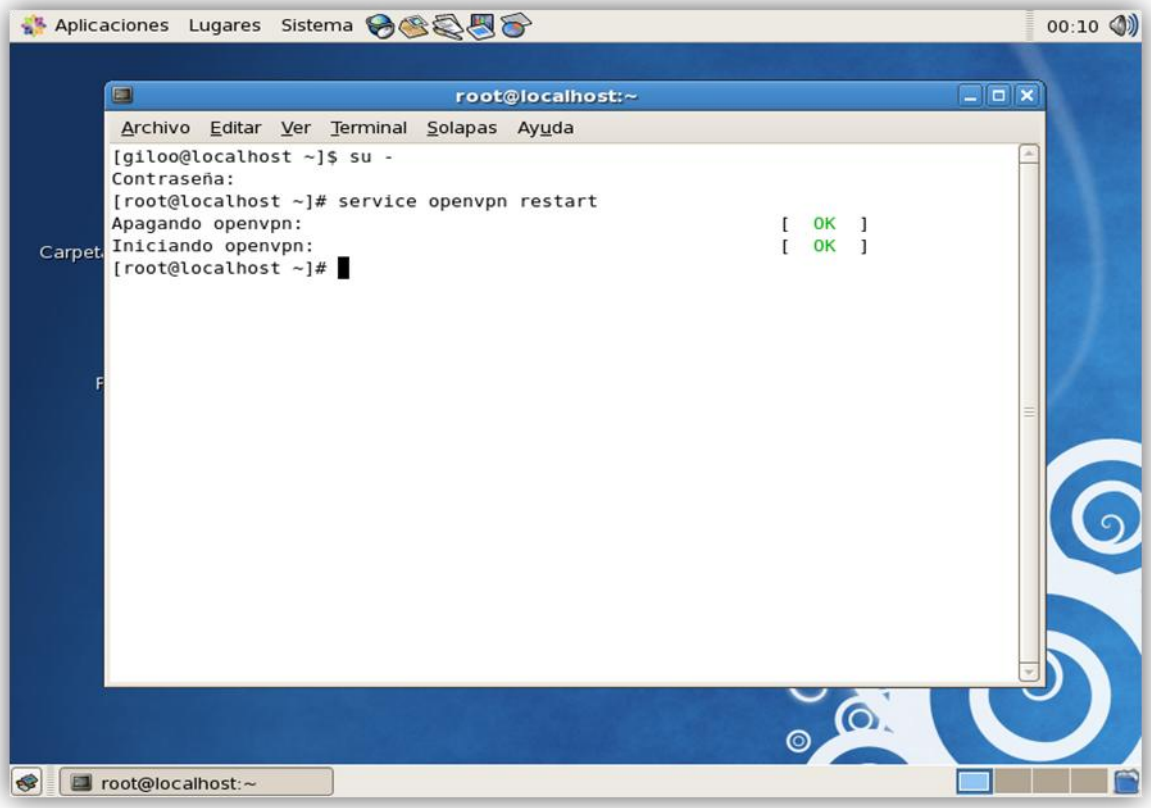


Figura Nº 10: Servicio OpenVPN

En la figura Nº 14 se puede observar que el servicio de OpenVPN está levantando, para verificar esto, primero reseteamos el servidor mediante el comando "*service openvpn restart*" y luego nos muestra que el servicio está iniciando.

Pruebas de ping: Esta prueba se realizó con el fin de constatar si existía una conexión entre los Host ubicados en distintas zonas geográficas mediante la VPN. El ping es una utilidad que comprueba en redes de computadoras el estado de la conexión del host local con uno o varios equipos remotos de una red TCP/IP por medio del envío de paquetes de Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) de solicitud y de respuesta.
Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada.
Ejecutando Ping de solicitud, el Host local envía un mensaje ICMP, incrustado en un paquete IP. El mensaje ICMP de solicitud incluye, además del tipo de mensaje y el código del mismo, un número identificador y una secuencia de números, de 32 bits, que deberán coincidir con el mensaje ICMP de respuesta; además de un espacio opcional para datos.
Mediante esto podemos comprobar que existe una conexión entre los servidores y los host.

Verificando el IP del servidor 1:

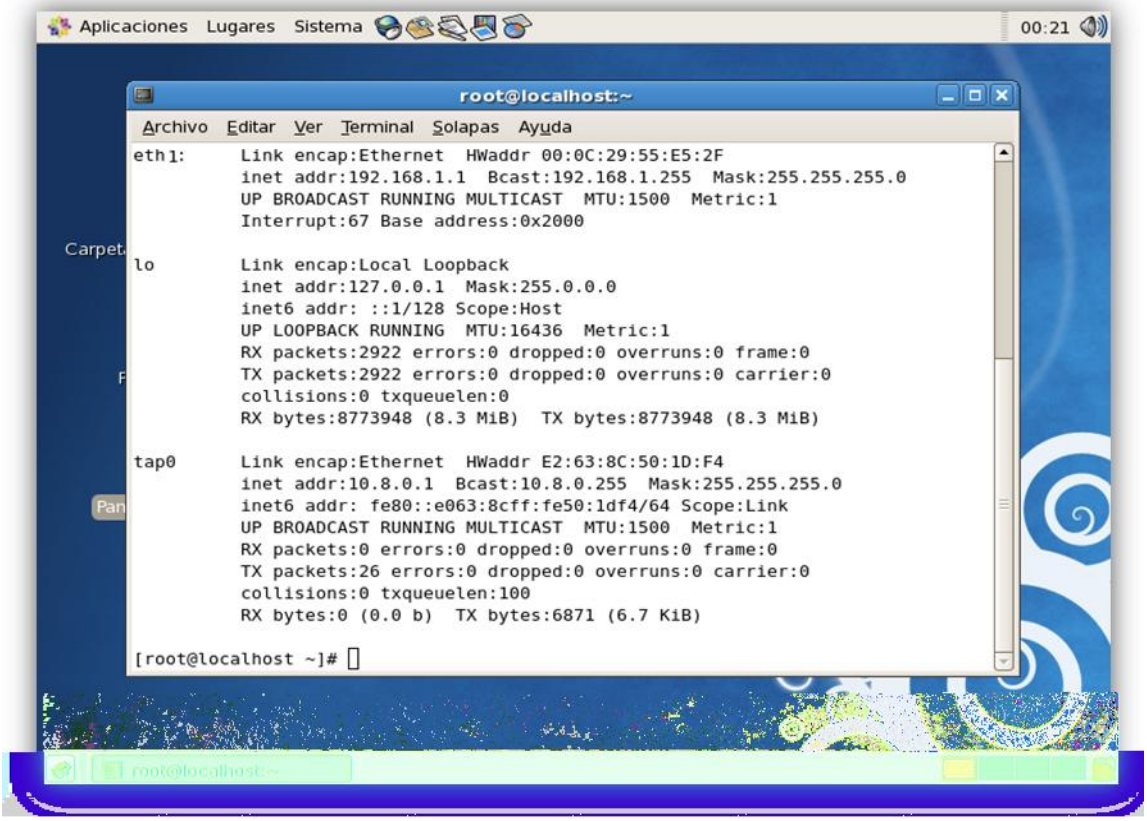


Figura Nº 11: IP servidor 1

Mediante el comando "*ifconfig*", constatamos que el IP del servidor 1 es el 192.168.1.1

Verificando el IP del servidor 2:

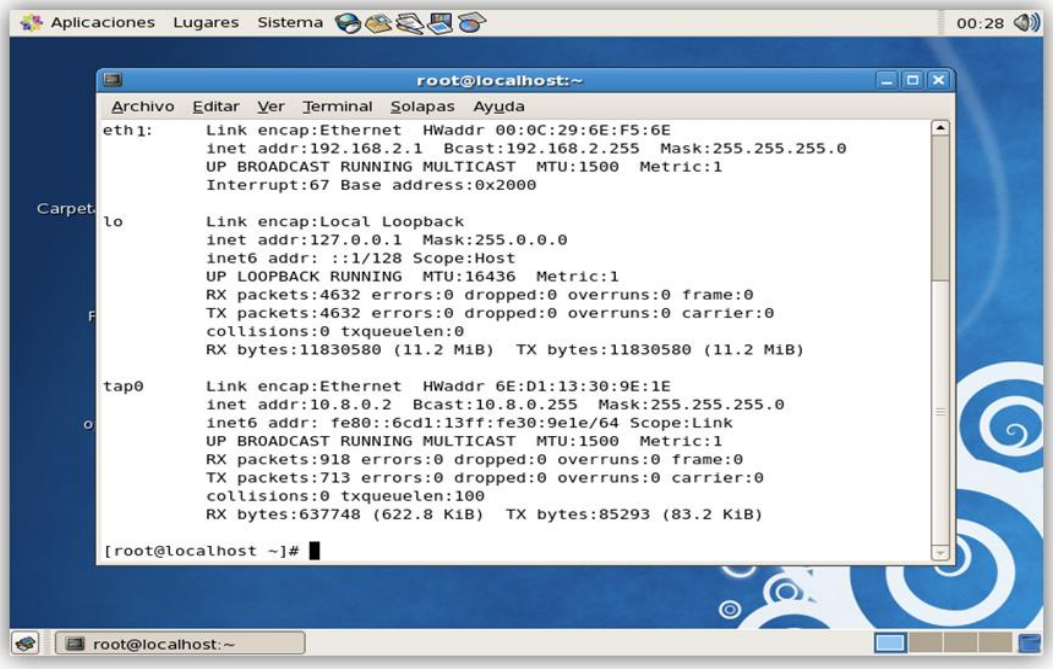


Figura Nº 12: IP servidor 2

Constatamos que el IP del servidor 2 es el 192.168.2.1
A continuación verificamos que exista conexión entre los servidores:

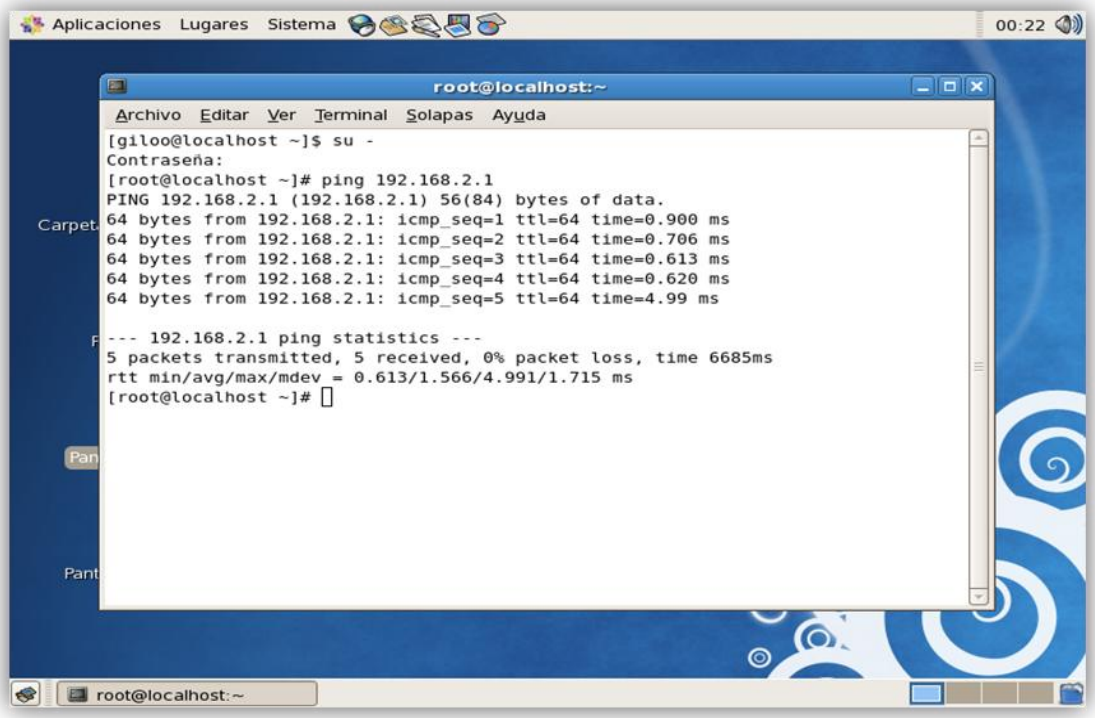


Figura Nº 13: Ping entre el servidor 192.168.1.1 y el servidor 192.168.2.1

En la figura Nº 17 se puede observar que el servidor 1 con el IP: 192.168.1.1 efectúa satisfactoriamente el ping al servidor 2 con el IP: 192.168.2.1

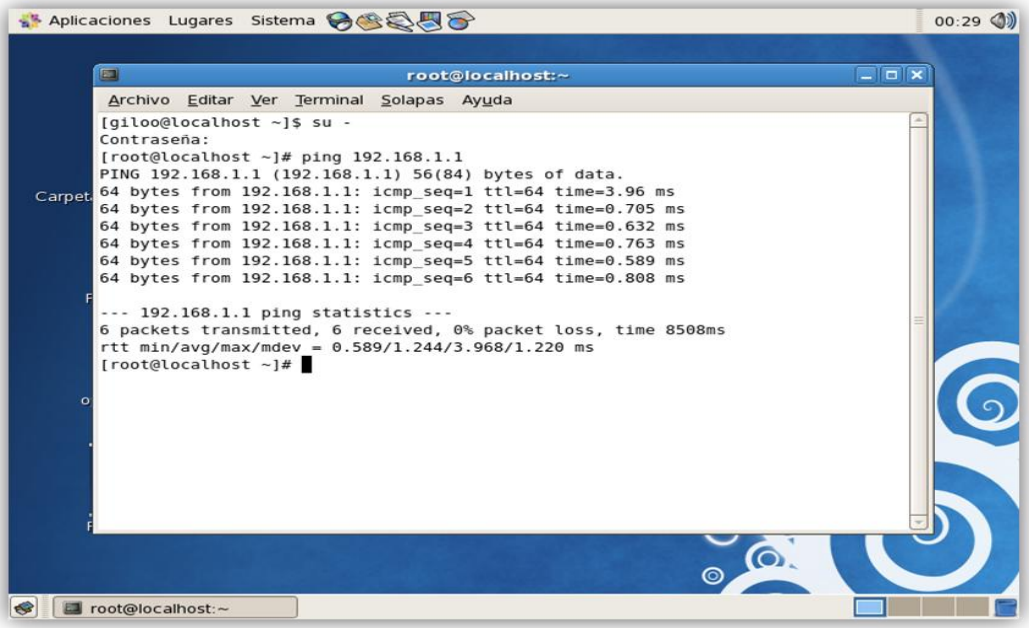


Figura Nº14: Ping entre el servidor 192.168.2.1 y el servidor192.168.1.1

En la figura Nº 18 se puede observar que el servidor 2 con el IP: 192.168.2.1 efectúa satisfactoriamente el ping al servidor 1 con el IP: 192.168.1.1

Luego verificamos que exista conexión entre los Host:

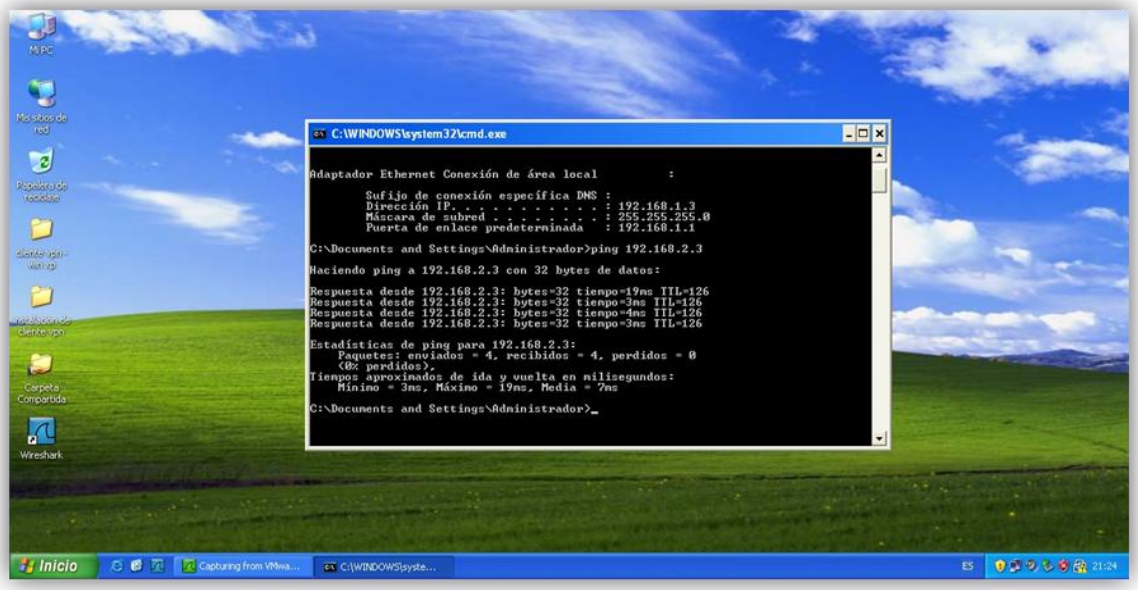


Figura Nº 15 Ping entre el host 192.168.1.3 y el host 192.168.2.3

En la figura Nº 19 se puede observar que el usuario 1 con el IP: 192.168.1.3 efectúa satisfactoriamente el ping al usuario 2 con el IP: 192.168.2.3

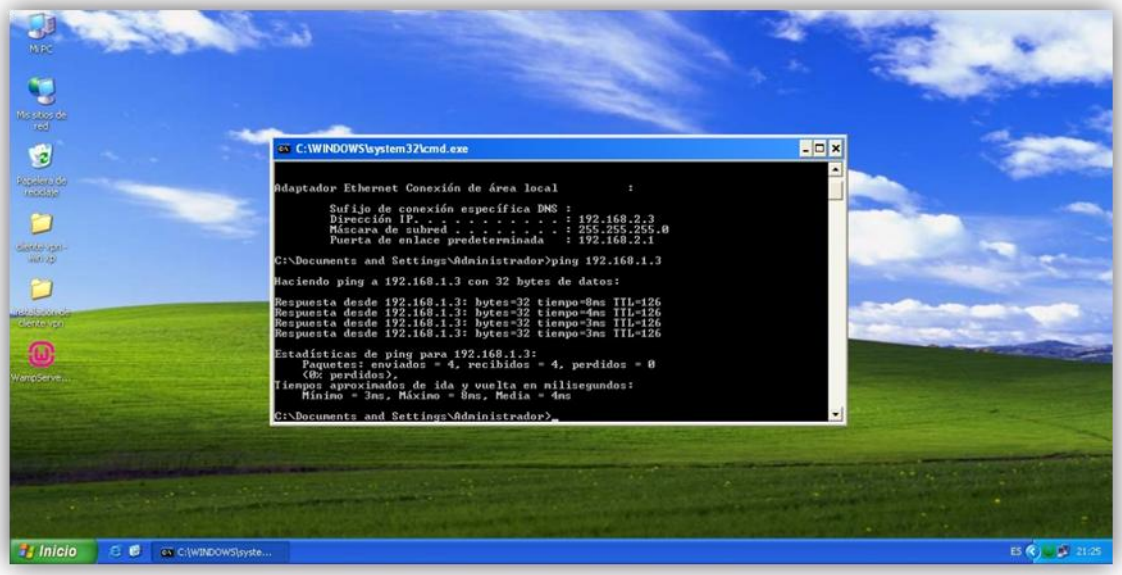


Figura Nº 16: Ping entre el host 192.168.2.3 y el host 192.168.1.3

En la figura Nº 20 se puede observar que el usuario 2 con el IP: 192.168.2.3 efectúa satisfactoriamente el ping al usuario 1 con el IP: 192.168.1.3

Mediante la prueba del ping se pudo verificar que no existe perdia de paquetes siendo la conexión VPN satisfactoria, esto nos permite que a través el servidor VPN podemos conectarnos entre dos redes ubicadas en distintas zonas; gracias

a esto, podemos extender una red local sobre una red pública no controlada, como es la Internet y asi poder mejorar el acceso a los datos..

<u>Prueba de transferencia de archivos:</u> Esta prueba consiste en compartir un archivo entre la red 192.168.1.0 y la red 192.168.2.0. Primero compartimos una carpeta en el Host 192.168.1.1, con una archivo que pesa 882 MB, luego accedemos a ésta a través de la VPN desde el Host 192.168.2.

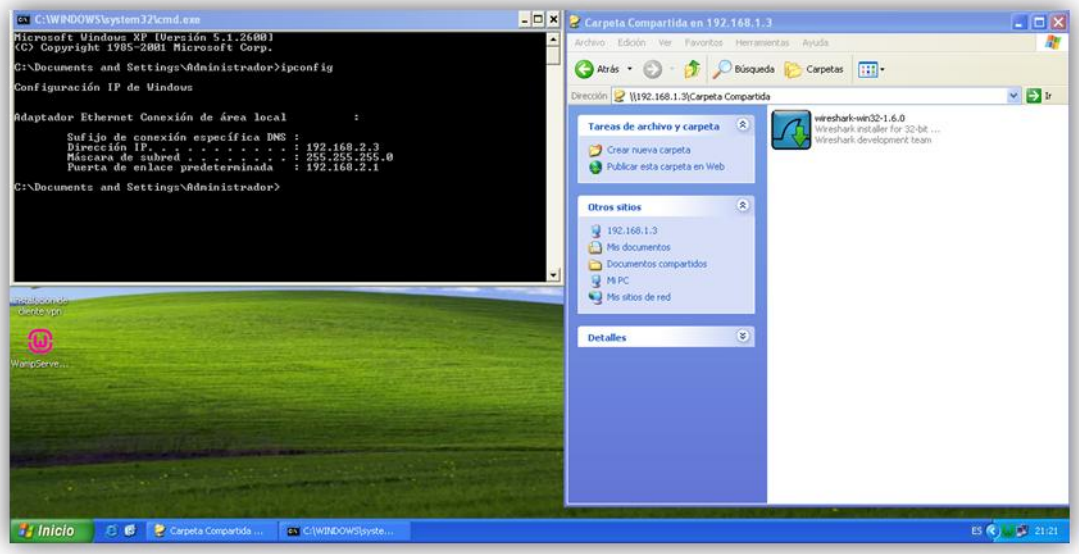


Figura Nº 17: Archivos compartidos

Como podemos observar, el traslado de información fue satisfactorio, el Host con el IP 192.168.2.3 a podido acceder a la carpeta compartida por el Host 192.168.1.3, esto no sería posible sin el canal de la VPN que permite una extensión de la red local sobre una red pública (uniendo dos redes ubicadas en distintas zonas geográficas), permitiendo la integridad de los datos.

Despues de analizar este conjunto de pruebas, se pudo apreciar que el proceso de creación de la VPN fue satisfactorio, se logró unir dos redes separadas a través de una red pubica con una transferencia de datos factible, con ayuda de la herramienta OpenVPN.

<u>Resultado</u>

Después de analizar este conjunto de resultados se pudo constatar que existe una buena aceptación por parte del personal entrevistado, ya que mediante la VPN pudieron acceder a diferentes recursos entre los locales de la institución de manera directa. Además se logró tener una vía de acceso que sirva como soporte para enlazar futuras implementaciones tecnológicas como sus bases de datos, sistemas de notas, pagos, registro de personal, matriculas, así como telefonía VOIP las cuales se pueden enlazar garantizando la mejora del proceso de gestión de datos.

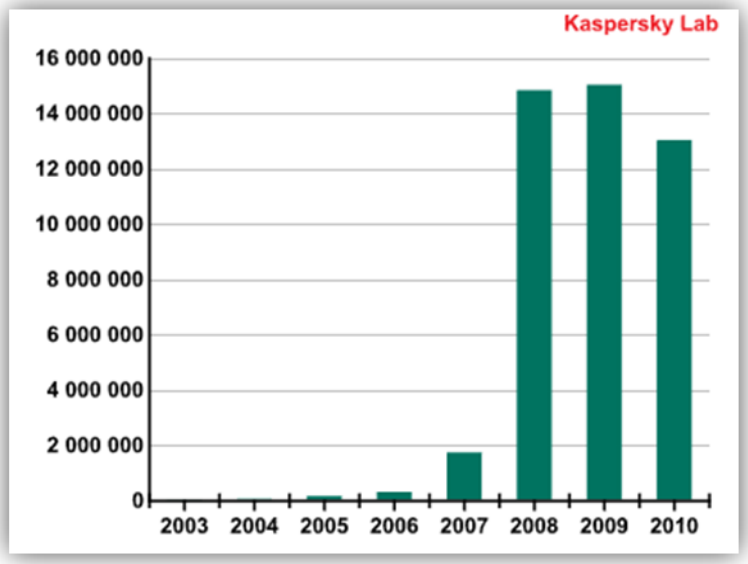
4.4.2. Fase 4.2: Evaluación de seguridad de la red.

Una vez que la implementación ha finalizado, es conveniente realizar una evaluación de satisfacción a los trabajadores, con respecto a la seguridad del canal utilizado para la transferencia de datos y el nivel de seguridad que brinda la herramienta implementada.

Al ser entrevistado jefe del área de sistemas de la corporación ADEU, manifestó que se han registrado con anterioridad algunos casos de pérdida de información en la institución, producidos por enviar datos por correo electrónico, lo que representa inseguridad y genera insatisfacción respecto al canal de comunicación utilizado. Pero debido a que no se tiene un sustento para demostrarlo, esta investigación se baso en un estudio pre-test hecho por la compañía Kaspersky Security

<u>Prueba</u>

Según un estudio de la empresa Kaspersky, el 2010 ha sido el año de las vulnerabilidades informáticas y cada año será mayor el peligro a combatir.
.



Fuente: Kaspersky Security, 2010
Figura Nº 18: Cuadro comparativo de ataques vía internet

El cuadro anterior muestra los ataques producidos a usuarios mediante internet, se puede observar que del año 2008 al 2010 los ataques han ido aumentando, es necesario distinguir cuatro tipos de incidentes:

- Ataques realizados mediante Internet (registrados por medio del antivirus para la web)
- Incidentes locales (registrados en los ordenadores de los usuarios)
- Ataques de red (registrados con la ayuda de IDS)

- Incidentes en el correo electrónico

Entre estos incidentes destacan los ataques al correo electrónico, uno de los principales medios para la transferencia de archivos usados entre las oficinas de la corporación ADEU.

Cabe destacar que el uso de las VPN no va a reemplazar el uso de los correos electrónicos, pero si podrá reducir el uso de los correos para la transferencia de datos de importancia institucional.

Gracias a que OpenVPN integra mecanismos de seguridad, proporciona un tipo de clave estática pre-compartida de 2048 bits, la cual es mostrada en el anexo nº 01, haciendo difícil el acceso de personas ajenas a la institución a la red corporativa.

Después analizar el tipo de seguridad que maneja OpenVPN se demostrara los resultados que se podría obtener al ser implementado.

OpenVPN proporciona una encriptación de 256 bits esto quiere decir que abra la posibilidad de crear 2^{256} combinaciones, teniendo en cuenta que la manera más usual para descifrar estas claves es mediante el método de fuerza bruta, el cual consiste en la introducción de todas las claves posibles una a una hasta que se encuentre la correcta. Según CertStopShop, 2008, *"si un solo procesador, por fuerza bruta, puede descifrar una llave de cifrado de 40 bits en 0.015 segundos, le tomaría 149,745,258,842,898 años en descifrar una llave de 128 bits*", esto quiere decir que una llave de 256 tomara mucho mas tiempo ser descifrarda.

Resultado

Después de analizar estos resultados y mostrarlos al jefe de sistemas de la corporación ADEU, este señaló que el tipo de seguridad que brinda la herramienta OpenVPN tubo una mejor aceptación por parte del personal, ya que sienten mayor seguridad al pasar sus datos por este canal.

Otro punto a tratar es el nivel de seguridad que brinda la herramienta OpenVPN. A continuación se procedió a analizar el nivel de seguridad que tiene OpenVPN al transferir archivos.

Para las pruebas de evaluación de seguridad de la red se utilizó la herramienta Wireshark, el cual es un analizador de protocolos y permite examinar datos de una red o de un archivo que sea enviado a través de ésta, además se puede analizar la información capturada a través de los detalles y sumarios por cada paquete.

Prueba

Se instalara la herramienta para el test en un servidor y se efectuara el intercambio de la información entre los usuarios, los cuales se conectaran a través de la VPN, esta información no podrá ser visible por su paso entre los servidores ya que es encriptada.
Primero se mostrara el paso de la información entre dos maquinas con IP: 192.168.164.128 y la maquina con IP: 192.168.164.143 utilizando la herramienta Wireshark.

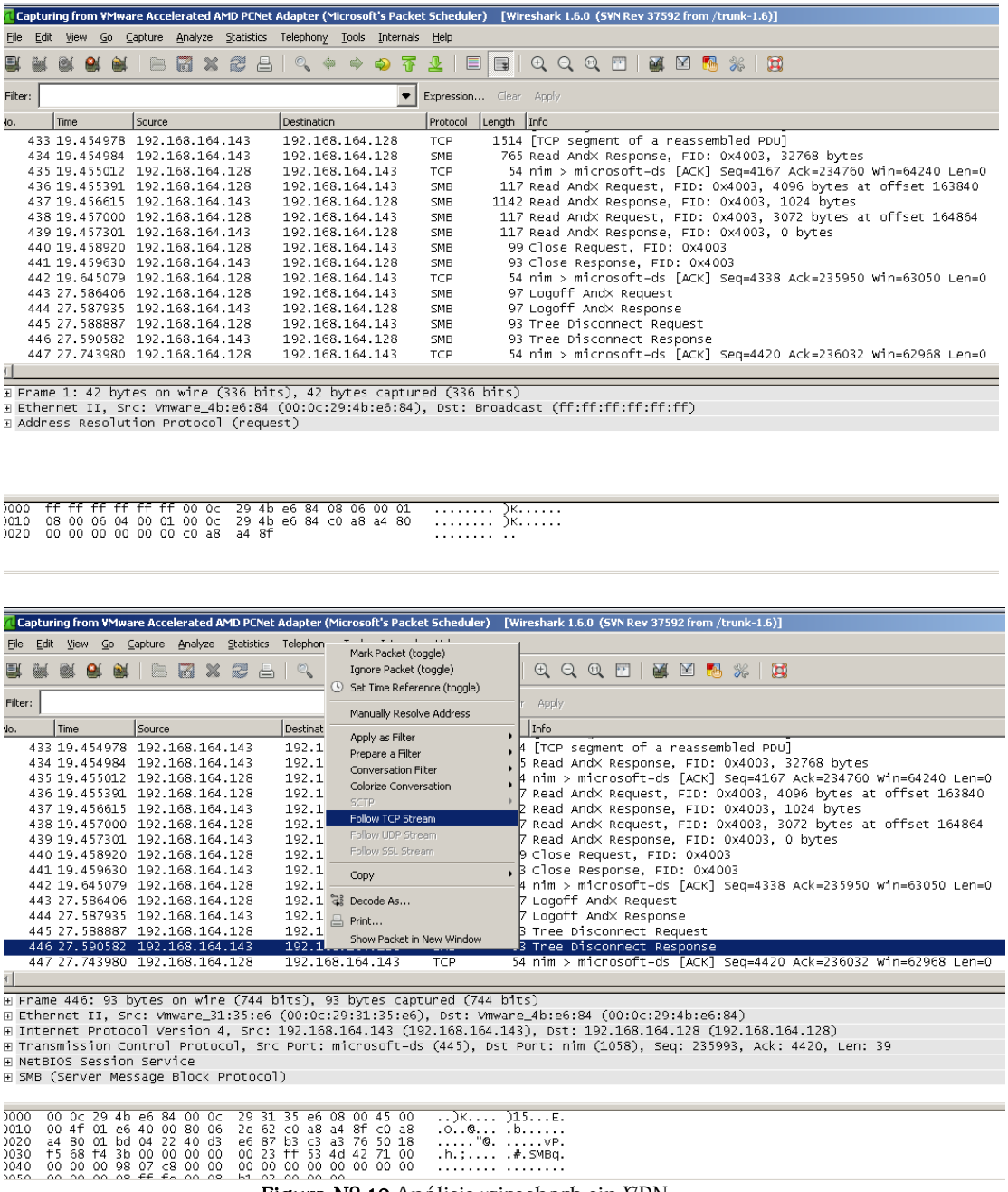


Figura N° 19 Análisis wireshark sin VPN

A continuación procedemos a efectuar un Follow stream para seguir el flujo de la información.

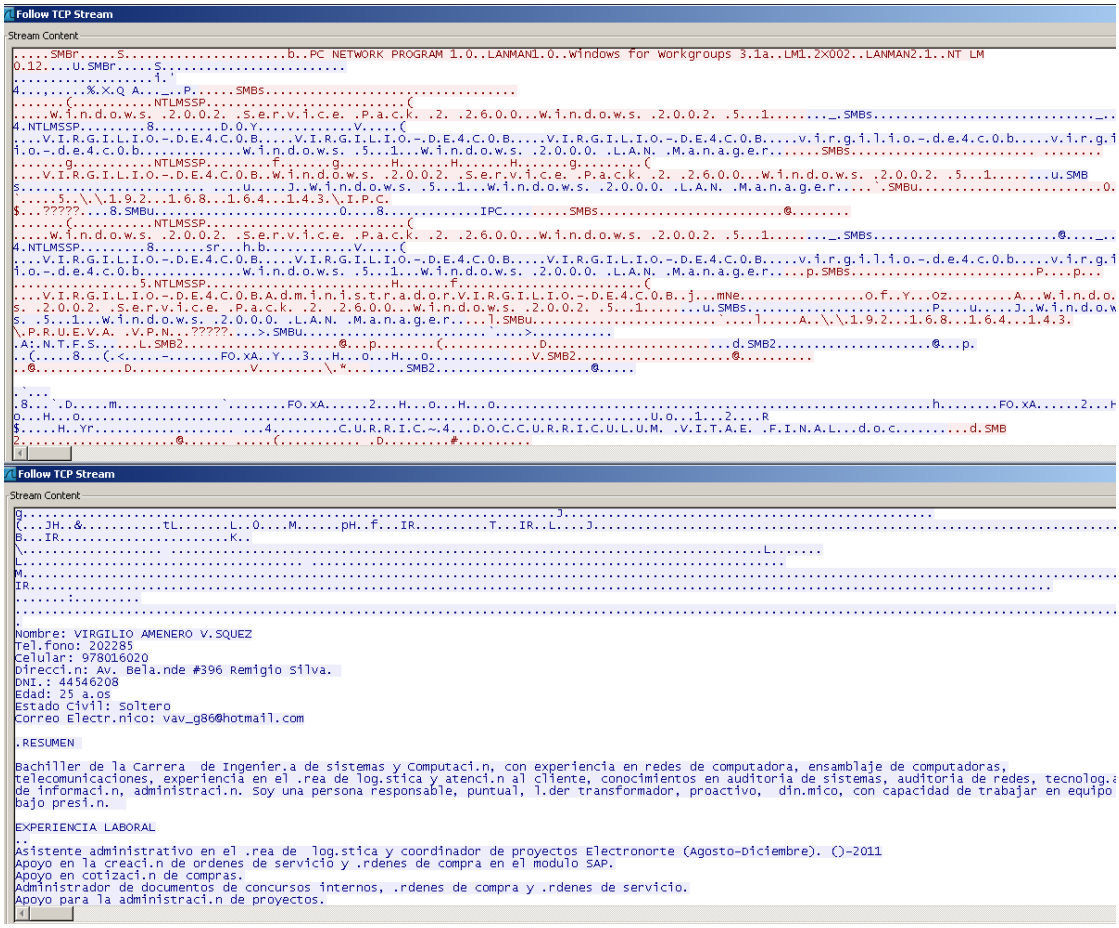


Figura N° 20: Resultados del análisis wireshark sin VPN

Como se puede apreciar a través del wireshark, la información compartida entre las máquinas en red sin VPN es analizada mediante el protocolo que utilizan para el envío de la información, esta información es visible, por lo cual podría ser extraída por personas ajenas con objetivos maliciosas para la institución.

A continuación se instalará la herramienta en un servidor para la evaluación de seguridad de la red y se efectuará el intercambio de la información entre los usuarios.

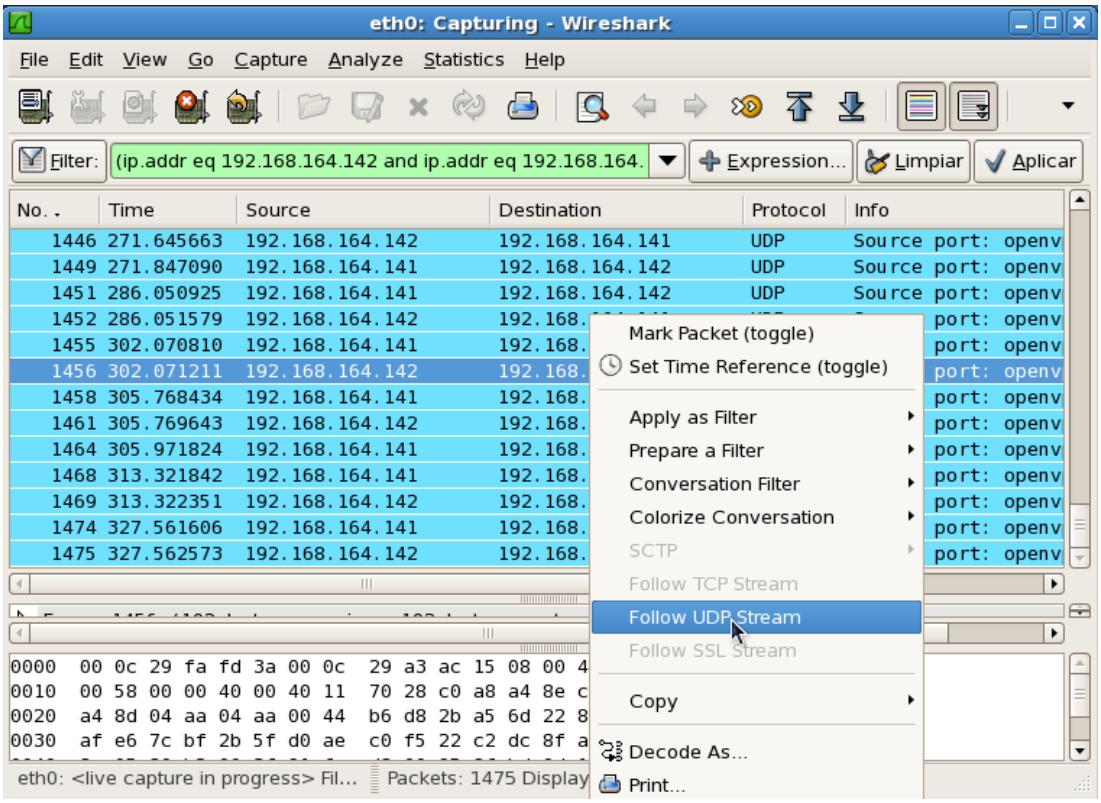


Figura Nº 21: Análisis wireshark con VPN

A continuación procedemos a hace un Follow stream para seguir el flujo de la información.

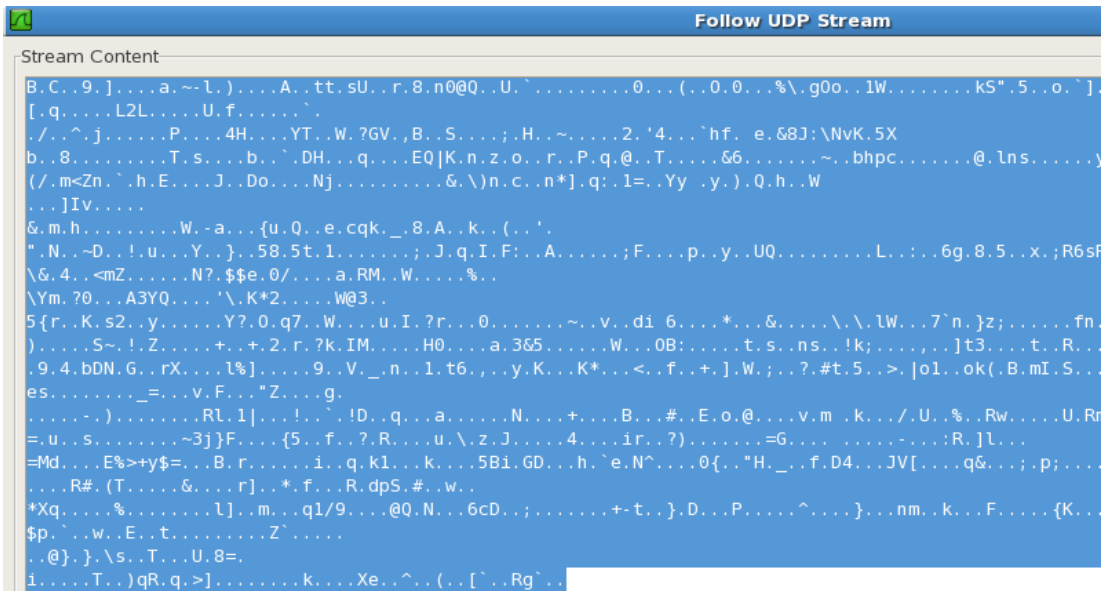


Figura Nº 22: Resultados del análisis wireshark con VPN

Como se puede apreciar a través del wireshark, la información compartida entre las máquinas enlazadas por la VPN es analizada mediante el protocolo que utilizan para el envío de información, esta información aparece encriptada.

Resultado

Analizando estas pruebas se puede demostrar que el paso de la información por la VPN se da a través de un canal seguro, el cual evita los problemas de extracción de la información o de ataques externos.

Como aporte a esta investigación se optó por demostrar cómo es posible que nuestra red se vuelva más segura ante ataques externos.

Tener vigilados los puertos del ordenador es muy importante tanto para evitar intrusiones desde Internet como para tener controlado en todo momento el ordenador.

Luego de analizar el paso de la información a través de la VPN se deben asegurar los diferentes protocolos que pasan a través de la red, ya que podrían ser un medio de vulnerabilidad que pueden ser aprovechados y violentados por personas con motivos maliciosos. Para este análisis sirve la herramienta ZENMAP 5.51, la cual es una aplicación gráfica para manejar Nmap: un escáner de puertos que nos puede dar mucha información acerca de una máquina.

Prueba

Se efectuó un test con la herramienta ZENMAP, esta herramienta se ejecuta desde un usuario ubicado en la misma red publica de los servidores.

Acontinuación se efectúa el testeo:

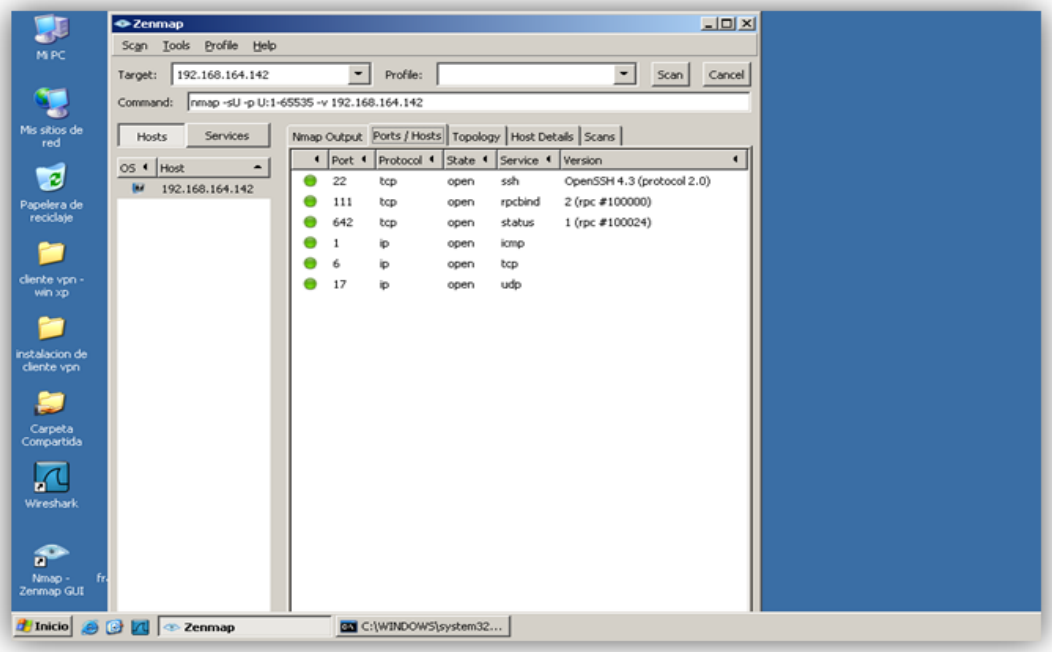


Figura Nº 23: Pre Testeo

En la figura se puede observar que existen muchos puertos abiertos visibles al exterior, lo cual resulta una amenaza al servidor ante posibles ataques externos. Entre los puertos abiertos más importantes se encuentran:

Puerto	Descripción
Puerto TCP 22 SSH:	SSH (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix yWindows) corriendo.
Puerto TCP 111 RPCBIND:	RPCBIND se utiliza para la "Llamada a procedimiento remoto", al igual que para NFS y otros servicios similares.
Puerto TCP 981:	Servicios de gestión.

Como se puede verificar mediante estos puertos se podría romper parte de la seguridad de la VPN, es por eso que se optó por usar Iptables. Iptables es el nombre de la herramienta de espacio de usuario (User Space, es decir, área de memoria donde todas las aplicaciones, en modo de usuario, pueden ser intercambiadas hacia memoria virtual cuando sea necesario) a través de la cual los administradores crean reglas para cada filtrado de paquetes y módulos de NAT. Es es la herramienta estándar de todas las distribuciones modernas de GNU/Linux.

Primero se configuró el firewall para que termine las conexiones hacia el túnel de la VPN, aquí ya depende del administrador del sistema qué tipo de firewall se use, pero actualmente se siguen utilizando reglas de iptables.

Se inicia la creación de reglas para nuestro firewall por medio de iptables. Aceptamos el tráfico de entrada y salida por el protocolo UDP por el servicio OpenVPN:

```
[root@localhost ~]# iptables -A INPUT -i eth0 -p udp --dport 1194 -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -0 eth0 -p udp --sport 1194 -j ACCEPT
```

Permitimos la conexión desde cualquier equipo por la interfaz tun.

```
[root@localhost ~]# iptables -A INPUT -i tun+ -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -o tun+ -j ACCEPT
```

Permitimos que los equipos de las otras redes accedan a nuestra red.

```
[root@localhost ~]# iptables -A FORWARD -i tun+ -j ACCEPT
[root@localhost ~]# iptables -A FORWARD -o tun+ -j ACCEPT
```

Generamos el archivo de reglas del firewall.

```
[root@ localhost ~]# iptables-save > iptables
```

Movemos el archivo generado a /etc/sysconfig

```
[root@ localhost ~]# mv iptables /etc/sysconfig
```

Reiniciamos el servicio de firewall.

```
[root@localhost ~]# /etc/init.d/iptables restart
Expurgar reglas del cortafuegos:                    [  OK  ]
Configuración de cadenas a la política ACCEPT: filter      [  OK  ]
Descargando módulos iptables:                       [  OK  ]
Aplicando reglas del cortafuegos iptables:              [  OK  ]
Cargando módulos iptables adicionales:ip_conntrack_netbios_[  OK  ]
[root@localhost ~]#
```

Con esto ya se habrá creado el firewall para nuestro servicio de VPN.

Verificando la configuración del Firewall:

La forma más sencilla y rápida para poder verificar que realmente se aplicaron las reglas Iptables para el firewall, es ejecutar el siguiente comando:

```
[root@localhost ~]# iptables -nL | grep 1194
ACCEPT     udp  --  0.0.0.0/0           0.0.0.0/0           udp dpt:1194
[root@localhost ~]#
```

Ahora que se tienen las reglas estableciadas para que los equipos entren a la VPN, se pueden configurar los iptables generando reglas para los puertos que estan habiertos.

La forma más obvia de prevenir el acceso al host, es permitiendo las conexiones de un reducido grupo de direcciones IP, además de lo siguiente:

- Aceptar conexiones SSH y RPCBIND entrantes desde direcciones confiables.
- Prohibir el acceso de las demas conexiones.

Usando los comandos del firewall iptables de la siguiente manera:
Todas las conexiones desde la direccion 192.168.2.1 o 192.168.1.1 al puerto 22 (SSH), el IP dependera desde que Host estamos accediendo.

```
[root@localhost ~]# iptables -A INPUT -p tcp -m state --state NEW –source
192.168.2.1 --dport 22 –j ACEPPT
```

Denegar las demás conexiones a SSH

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 22-j DROP
```

Todas las conexiones desde la direccion 192.168.2.1 o 192.168.1.1 al puerto 111(RPCBIND).

```
[root@localhost ~]# iptables -A INPUT -p tcp -m state --state NEW –source 192.168.2.1 --dport 111 –j ACEPPT
```

Denegar las demás conexiones a 111(RPCBIND).

```
[root@localhost ~]# iptables -A INPUT -p tcp --dport 111-j DROP
```

Generamos el archivo de reglas del firewall.

```
[root@ localhost ~]# iptables-save > iptables
```

A continuación nuevamente se efectua el testeo con la herramienta ZENMAP y se obtienen los siguientes resultados:

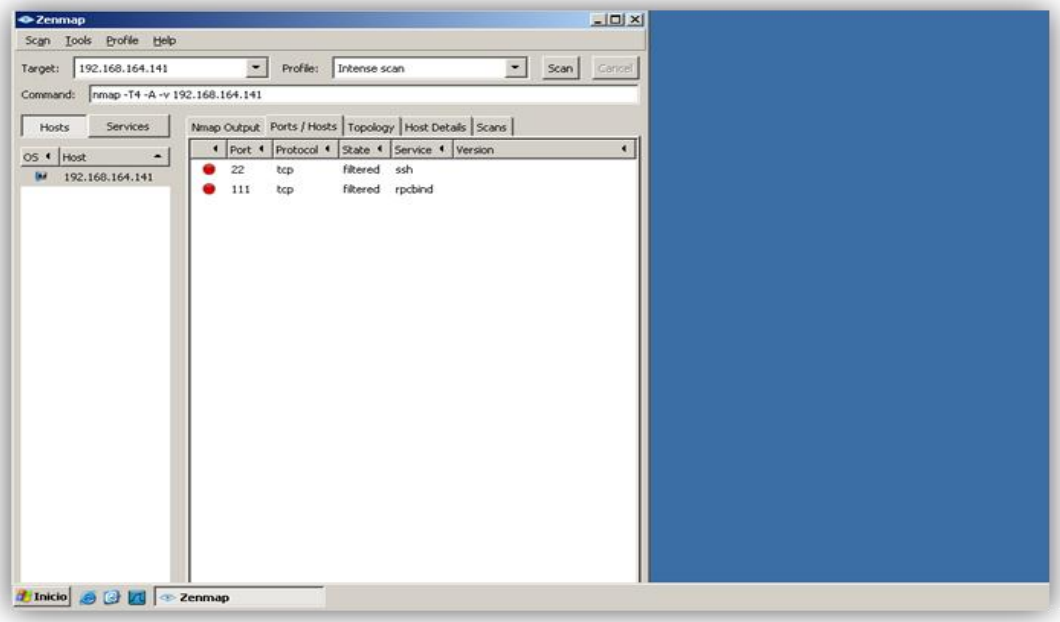


Figura Nº 24: Post Testeo

Es posible verificar que la herramienta ZENMAP testeó los puertos de los servidores y arrojó los siguientes resultados:

- Se pudo cerrar puertos que podrían ser vulnerables a ataques externos.
- Se pudo bloquear los puertos 22 y 111 (SSH y RPCBIND), mediante reglas de Iptables.

Resultado

En conclusión se afirma que 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.

4.4.3. Fase 4.3: Rentabilidad de la Red.

Según la entrevista efectuada al jefe de sistemas de la corporación ADEU, se quería una VPN arrendada, pero deseaban una opción que redujera costos de implementación.

En esta etapa se comparan los costos en la implementación de OpenVPN contra los costos en la implementación de líneas contratadas VPN. La corporación, al querer implementar dicha tecnología, deseaba saber qué tipo de tecnología es la más económica y eficiente, por lo tanto se efectuó la comparación económica para verificar la factibilidad de la implementación.

Prueba

Solución 1

Utilizar un proveedor de servicios de comunicación para facilitar el medio de transmisión y los equipos necesarios para interconectar ambas oficinas y a la vez nos ofrezca el servicio de VPN.

Se contactó con Telefónica del Perú para averiguar los servicios que brinda en interconexión VPN. Telefónica del Perú informó ofrece un servicio VPN hasta 128 KBPS.

		Pagos por única vez		Pagos Mensuales	
Descripción	Cant.	Precio US $	Sub-Total US $	Precio US $	Sub-Total US $
Local 1	1	500	500	545.47	545.47
Conectividad					
Conexión a red por par telefónico dedicado	1	0	0	0	0
Instalación del circuito por puerta	1	0	0	0	0
Por puerta acceso caudal LDN datosbronce		0	0	370.67	370.67
Equipos 1					

Modem HDSL velocidad variable		0	0	111.6	111.6
Equipos 2					
Renta mensual cisco 1905		0	0	63.2	63.2
Instalación Equipos					
Servicio de instalación cisco 1905		500	500	0	0
Local remoto		3,200.00	3,200.00	1,605.60	1,605.60
Conectividad					
Instalación del servicio	1	3,200.00	3,700.00	2,151.07	2,151.07
Servicio IP VPN por puerta hasta 128 KBPS	1	0	0	1,605.60	1,605.60
Sub Total US$		**3,700.00**	**3,700.00**	**2,151.07**	**2,151.07**
Total US$ INC.IGV 18%			**4,366.00**		**2,538.26**
Sub Total S/.		**11,100.00**	**11,100.00**	**6,453.21**	**64,353.21**
Total S/. INC.IGV 18%			**13,098.00**		**7,614.79**

Nota: La inversión inicial implica servicio de instalación.

El primer pago da el total de S/. 20712.79, el cual se reducirá el siguiente mes.

Solución 2

Utilizar un proveedor de servicios de comunicación para facilitar el medio de transmisión y los equipos necesarios para interconectar ambas oficinas para la instalación de OpenVPN.

En esta alternativa se contactó con Telefónica del Perú para averiguar los servicios que brinda en interconexión con servicio ADSL. Telefónica del Perú manifestó que ofrece dicho servicio para el enlace entre los locales (Servicio Speedy Business) que utiliza tecnología ADSL, con velocidad de transmisión de 5 Mbps y una tasa garantizada del 25% o 50% a horas de alto tráfico.

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

Nota: La inversión inicial implica la compra de los equipos Modem Router y la instalación.

Para la instalación de OpenVPN se efectuará un gasto de 2000 soles el cual corresponde a instalación, manual de usuario y mantenimiento por 5 meses.

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

El primer pago da el total de S/. 7,096.56, el cual se reducirá el siguiente mes.

Cuadro comparativo

	PAGO EN MESES				
	I MES	II MES	III MES	IV MES	V MES
Solución 1	20,712.79	7,614.79	7,614.79	7,614.79	7,614.79
Solución 2	7,096.56	2,766.55	2,766.55	2,766.55	2,766.55

Como se puede apreciar, la instalación de la solución OpenVPN resulta más económica, además el pago de los equipos y de la instalación se efectúa por única vez, reduciendo casi en un 60% la tarifa para el siguiente mes.

Resultado

En conclusión, la alternativa elegida para la interconexión segura entre las redes de los locales, utilizando Internet como medio de enlace y que se acomoda a nuestras necesidades, en cuanto a costo, es la solución 2. De este modo se efectuará la implementación de la solución 2 con un producto OpenVPN que además proporciona flexibilidad, pues es personalizada y diversificada de acuerdo a nuestras necesidades.

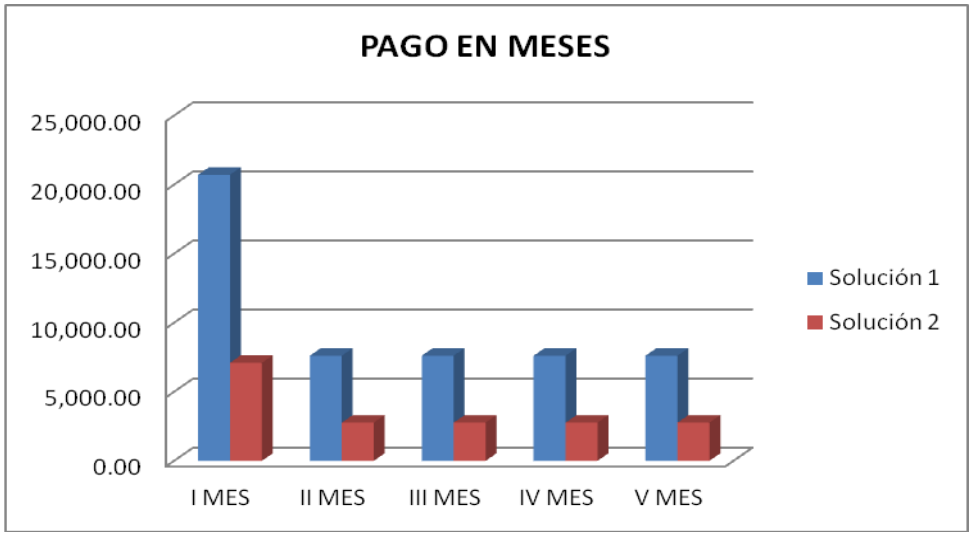


Figura Nº 25: Cuadro comparativo costos

V. DISCUSIÓN

En el desarrollo de la investigación se puso de manifiesto que actualmente las grandes Corporaciones, tienen la necesidad de interactuar entre sus locales, enviando y recibiendo información muchas veces por medios no seguros como lo es el Internet, para que sus procesos sean optimizados y a la vez se pueda tener una visión global de la organización en cuanto a la información, tal como lo afirma Tomás (2008), el cual da a conocer que "las comunicaciones a través de las redes de información resultan de vital importancia para un gran número de empresas y organizaciones. Para llegar a su destino, ese tráfico debe atravesar, muy a menudo, una infraestructura de redes públicas (como Internet), lo que lo hace vulnerable a los ataques de usuarios mal intencionados".

Ante ese peligro potencial, resulta imprescindible poseer herramientas que permitan proteger el contenido de dicho tráfico. Para asegurar tanto sU privacidad como su integridad en las comunicaciones de extremo a extremo. Es en ello en lo que esta investigación se enfocó, al emplear OpenVPN en una Corporación educativa, quedando demostrado que con el empleo de este tipo de soluciones se optimiza el acceso a la información, asegurando la conectividad y la seguridad, tal como lo afirma Internet Engineering Task Force (IETF por sus siglas en inglés): una VPN es "Una emulación de una Red de Área Amplia (WAN) que usa IP públicas o compartidas, tal como el Internet o columnas IP privadas". En términos más simples, una VPN es una extensión de una Intranet privada a través de una red pública (la Internet) que asegura conectividad segura y de costo efectivo entre los dos fines comunicadores. La intranet privada se extiende con la ayuda de "túneles" lógicos privados. Estos túneles permiten que los dos fines comunicantes intercambien información de manera que parezca comunicación de punto a punto.

Jon (2005), afirma que el mecanismo fundamental que nos permite tener comunicaciones seguras en Internet es la noción de un túnel. Los túneles son una forma de superposición de una red lógica o virtual en la parte superior de una red física. Una vez que tenemos un túnel, se puede asegurar mediante la encriptación y la autenticación del tráfico de red que fluye a través de él, recreando así la seguridad de las líneas privadas alquiladas.

Las VPN no son exactamente una nueva tecnología. Contrariamente a lo que la mayoría de nosotros cree, según Gupta (2003), "el concepto VPN ha existido desde la época de los 80 y ha tomado varias generaciones el que llegue a su forma más reciente".
En contraste a esto, la solución OpenVPN tiene pocos años de creación, según Feilner y Graf (2009), OPENVPN entró en la escena en mayo 13, 2001 con un lanzamiento inicial que podía apenas tunelear paquetes IP en UDP. Pero se optó por utilizar esta herramienta debido a la evolución, la simplicidad y el auge que ha tenido en los últimos años. Según Feilner y Graf (2009), con la llegada de OPENVPN una nueva generación de VPN entró en escena.

Mientras otras soluciones VPN suelen usar mecanismos propietarios o no-estándar, OPENVPN tiene un concepto modular, tanto para subrayar la seguridad

como para trabajo de red (networking). No sufre de la complejidad que caracteriza otras implementaciones VPN como el líder de mercado IPSec.

Ahora bien, de acuerdo a los resultados obtenidos en cada uno de los criterios evaluados en la etapa anterior y teniendo en cuenta el orden en el que se dan, en primer lugar se hará referencia al aspecto de mejora de la comunicación entre los locales.

Según la entrevista realizada al jefe del área de sistemas de la corporación ADEU, al utilizar correo electrónico para la transferencia de la información, la Corporación siente que no cubre sus necesidades, trayendo como consecuencia que se pierda tiempo en el acceso a la información y del trabajo, reduciendo la eficiencia de la corporación.

En los resultados que se observa en las figuras 14 a la 21, mediante la implementación de la VPN se logró unificar estas dos redes geográficamente dispersas, esto proporciona una canal que permite acceder a diferentes recursos entre las oficinas de manera directa, óptima y eficaz, sin perder el tiempo en pedir la información de un local a otro y pasarlo por medio de vías tales como los correos electrónicos. Es necesario resaltar que la información cumple un papel muy importante para el manejo de las grandes corporaciones, y poder acceder a esta a través de los diferentes puntos corporativos, tales como: oficinas, locales y cedes. Así se expresa Tomas (2008), al decir que las comunicaciones a través de las redes de información resultan de vital importancia para un gran número de empresas y organizaciones, y muchas veces tener la información al alcance de las manos, puede garantizarnos el éxito de una empresa.
Según la figura 23 en un análisis que hizo la empresa Kaspersky Security 2010, en el aspecto de seguridad en la transferencia de los datos, se puede destacar el nivel de vulnerabilidad que existe al utilizar internet, de acuerdo a las necesidades que tenga empresa al acceder a este medio. Al tener una VPN los datos viajan seguros de acuerdo a las políticas que establecidas. En este caso, se puede verificar en el ANEXO N°1, el cual recalca el tipo y la función que cumple la seguridad en la VPN. A través de la herramienta wireshark, mostrada en las figuras 23 y 26, se demuestra que el paso de la información por de la VPN se da a través de un canal seguro encriptado el cual evita los problemas de pérdidas de información o de ataques externos.
También se implantaron políticas de Iptables tales como las mostradas en la Fase 4.2: La evaluación de seguridad de la red, que destaca, en las figuras 28 y 29, el funcionanmiento de la herramienta ZENMAP para verificar el nivel de seguridad que tiene nuestra red ante posibles amenazas, dando resultados satisfactorios.
Por último, con respecto a minimizar costos en la implantación de una tecnología VPN se pudo constatar en la Fase 4.3., Rentabilidad de la red, que la solución elegida es la más rentable y se acomoda a nuestras necesidades, en cuanto a costos.
Teniendo en cuenta la comparación de los resultados obtenidos de estos indicadores, se confirmó la hipótesis de que mediante la implementación de una VPN bajo software libre OpenVPN, se optimizará la comunicación entre los locales en la corporación Educativa ADEU, con un mejor acceso a la información.

VI. PROPUESTA

Al haber sido favorables los resultados obtenidos del empleo de la solución OpenVPN en la Corporación educativa ADEU, se puede afirmar que la aplicabilidad de ello en otras Corporaciones e instituciones tendrá buenos resultados, y no necesariamente en entidades educativas, si no que su uso puede ser extendido tanto como empresas del sector primario, del sector industrial, o como es este caso, del sector de servicio.

Los principales elementos a tener en cuenta para poder llevar a cabo el empleo de VPN en las Corporaciones son:

- Infraestructura tecnológica.
- Recursos Humanos.

- **Infraestructura tecnológica:**
  Se refiere a que las instituciones deben de contar con los recursos tecnológicos (computadoras) que proporcionen las características necesarias para la implementación de la VPN.

  Existen 2 alternativas que pueden tomarse en cuenta; la primera es que ya exista un área de sistemas está equipado con servidores que están deteriorados por lo cual se recomienda adquirir nuevos servidores los cuales incurrirán en un solo gasto que a la larga beneficiara a la corporación; la otra alternativa es que, si la corporación no cuenta con servidores adecuados y necesita probar dicha solución puede hacerlo mediante computadoras acopladas para su implementación, ya que esta no necesita de mucha capacidad para ser implementada.

  Para una u otra alternativa, se debe de tener en cuenta que los equipos de cómputo a emplear, mínimamente deben de contar con los siguientes requerimientos técnicos:

Hardware	Descripción
2 Servidores	Servidor HP ProLiant, con las siguientes características: DL120 G7 E3-1220, 4GB-U, 250 GB, LFF, conexión en frío, SATA B110i RAID, 400 W. Procesador: Intel® Xeon® E3-1220 (4 núcleos, 3,1 GHz, 8 MB, 80 W, 1333/t) Controlador de almacenamiento: (1) Smart Array B110i SATA RAID Unidades de disco duro incluidas: (1) SATA LFF; Conexión en caliente.
2 Switch	Switch de 24 puertos para la conexión del servidor y los clientes.

2 Tarjetas de red	Tarjetas de red de 100 MB, para la mejor transferencia de datos.
1 Conexión internet en cada oficina.	La conexión internet dependerá de la institución, pero se recomendó un servicio de Speedy Business para la mejor transferencia de datos.

Software necesario:

- CentOS 5.4.
- OpenVPN.
- Herramienta de testeo Wireshark.
- Herramientas de testeo, tal como ZENMAP 5.51.

- Recursos Humanos:

  Al hablar de recursos humanos se hace referencia propiamente a que el administrador del sistema y sus encargados deben familiarizarse con las herramientas de software y tener una visión global de lo que se quiere logar con esto.

  Tanto el administrador del sistema como sus encargados son los que ayudarán a la implementación y manejo de dicha solución, pero además deben contar con conocimientos previos sobre servidores en software libre, comandos que se utilizan en dichos sistemas y guías y documentación que facilite el manejo de la administración de la VPN.

  Tanto el docente como el auxiliar deben de ser personas tolerantes, pacientes, comunicativas, capaces de dar solución a problemas futuros tras la implementación de la VPN, para que de esta manera contribuyan positivamente funcionamiento de ésta.

  En cuanto a las actividades a tener en cuenta para lograr el éxito de la integración de la solución OpenVPN en la Corporación, tenemos:

- Contratación de un ISP O proveedor de servicios de Internet: El personal experto en sistemas de la institución, debe buscar un ISP, el cual brinde una conexión eficaz y eficiente a internet y a su vez otorgue un ancho de banda que permita el buen funcionamiento de la VPN.
- Familiarización con OpenVPN: Es tarea del administrador del sistemas y sus encargados de familiarizarse con la solución OpenVPN, para que de esta manera puedan conocer los pasos de su instalación y qué tipo de información requiere para su implementación. También pueden ayudarse de manuales de usuario, de los cuales existen muchos en Internet, ente ellos tenemos al que se encuentra disponible la web de OpenVPN dirigido a estudiantes y profesionales que quieren envolverse en el mundo del software libre.
  Una vez que el administrador del sistema conoce y domina la solución, está en condiciones de seleccionar el tipo de seguridad, restricciones y cambiar la configuración de esta solución de acuerdo a los criterios que le convenga

- El administrador es responsable de la fiabilidad de la VPN, para ello, debe constantemente repasar manuales, revisar en foros y hacer pruebas en maquinas virtuales, con el fin de mejorar el manejo y la seguridad de la solución.
- Familiarización con Sistema operativo Linux: El administrador del sistema y sus encargados deben familiarizase con el sistema operativo Linux, tanto en Centos como en sus diferentes distribuciones, y dominar el conjunto de comandos para realizar las diferentes tareas de administración del servidor VPN implementado.
- Familiarización con herramientas de testeo de seguridad: Es tarea del administrador del sistema y sus encargados de familiarizarse con herramientas de testeo que ayuden a mejorar el nivel de seguridad que brinda la solución implementada, para que así pueda tomar las medidas necesarias ante posibles amenazas y vulnerabilidades de la VPN.
- Asignación de servidores: Es tarea del administrador del sistema asignar políticas de seguridad en cuanto a los servidores que enlazarán la VPN, compartiendo correctamente las llaves de acceso y configurando correctamente la ruta de envío de paquetes tal como los muestra el ANEXO N°1; se debería tomar en cuenta políticas de seguridad de los usuarios que accederán al servicio a la vez del uso que hagan a este.
- Asignar seguridad a la VPN: Es tarea del administrador del sistema brindar seguridad al servidor VPN así como a los usuarios que se conecten a este, tales como asignación de llaves y seguridad en los puertos abiertos, ante posibles ataques externos.
- Asignar la actualización de las versiones: El administrador del sistema debe tener actualizado las versiones de OpenVPN, así como los nuevos paquetes y repositorios para instalar esta solución.

A pesar de que los resultados obtenidos sean favorables, también se tiene que describir las limitaciones que se tuvo para la implementación de la propuesta dada, para que otras corporaciones e instituciones hagan un hincapié en estos puntos:

- Capacidad de almacenamiento de la computadora para las pruebas: Se tiene que tener en cuenta la capacidad de la computadora usada para la prueba, ya que puede limitar la implementación de la misma.
- Rapidez de la Internet: Se tiene que tener en cuenta la rapidez de la internet para las pruebas de la VPN entre locales, ya que esta puede limitar el paso de información y el funcionamiento de la VPN.
- Conocimiento en la implementación de OPENVPN: Se debe tener en cuenta al implementar OPENVPN, el conocimiento adecuado de comandos para su configuración en nuestro servidor Linux.

VII. CONCLUSIONES

De acuerdo a la investigación desarrollada y a los resultados obtenidos, se llegó a las siguientes conclusiones:

1. La herramienta OpenVPN permite acceder la información de manera óptima y eficaz, accediendo a diferentes recursos entre los locales de la institución de manera directa. Además provee una vía de acceso que sirva como soporte para enlazar futuras implementaciones tecnológicas, las cuales se pueden enlazar garantizando la mejora del proceso de acceso a los datos de la corporación entre locales.

2. La herramienta OpenVPN hace posible la confidencialidad y seguridad en la transmisión de los datos, mediante el tipo de seguridad y el nivel de encriptación que maneja, la cual puede ser reforzada mediante la utilización de Iptables.

3. Con la implementación de la solución OpenVPN se pudo constatar la rentabilidad en los costos de su instalación, haciendo que la corporación incurra en menos gastos que al instalar una VPN contratada.

4. Mediante la implementación y configuración de la solución OpenVPN se logró tener conocimiento del funcionamiento de las VPN, no sólo físico si no también lógico, para poder así transmitirlo a futuras investigaciones en el área de tecnologías de la información y comunicación.

VIII. REFERENCIAS BIBLIOGRÁFICAS

- Markus, F., y Norbert, G.2009.Beginning OpenVPN 2.0.9: Build and integrate Virtual Private Networks using.UK. Packt Publishing.
- Meeta, G. 2003. Building a Virtual Private Network. Packt Publishing.EEUU. Premier Press.
- Richard D .2006. The Complete Cisco VPN Configuration Guide. EEUU. Cisco Press.
- Jon C .2005. VPN Illustrated: Tunnels, VPN, and IPsec. EEUU. Addison Wesley Professional.
- Linux Journal.2009. Creating VPN with IPsec. EEUU. SPECIAL SYSTEM ADMINISTRATION ISSUE.30-33.
- García J. T., Raya J. L. C and Rodrigo V. R. 2002. Alta velocidad y calidad de servicio en redes IP. México. AlfaOmega Grupo editorial.
- Brown S. 2001. Implementación de redes privadas virtuales. México. McGRAW-HILL Interamericana Editores S.A. de C. V.
- Maiwald E. 2005. Fundamentos de seguridad de redes. México. McGraw-Hill interamericana editores.
- Maños J. 2004.Mundo IP. Madrid. Ediciones Nowtilus.
- Lic. Ardita C.2001. Metodología para la implementación de redes seguras. ¿Cómo desarrollar una red segura? . Argentina. CYBSEC.
- Etheridge D, Errol S. 1992. Metodología de Diseño de Red. Prentice Hall.
- Bruce, S.1999.Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). Universidad de Berkeley.
- Barrainkua Z.2009. OpenVPN Túneles Cifrados Hacia la Escuela. Eusko Jaurlaritza – Gobierno Vasco. Creative Commons – BY-SA-NC.
- Vinvanco M.2003. Desarrollo de una virtual private network (vpn) para la interconexión de una empresa con sus sucursales en provincias. Facultad de ingeniería de sistemas e informática. Universidad Nacional Mayor de San Marcos
- Trujillo M.2006.Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSEC. Título de ingeniero en informática. Escuela de ingeniería. Escuela politécnica Nacional.
- Tomás, C.2008.Servicio VPN de acceso remoto basado en SSL mediante OpenVPN. Tesis de Bachiller.Escuela técnica superior de ingeniería de telecomunicación. Universidad politécnica de Cartagena.
- Limari R.2004. Protocolos de seguridad para redes privadas virtuales. Tesis para optar al título de Ingeniero electrónico Facultad de ciencias en la ingeniería. Universidad Austral de Chile.
- Facultad Regional Santa Fe – Departamento Sistemas Cátedra de comunicaciones.2001. Conceptos básicos sobre Redes. Universidad Tecnológica Nacional.
- Michael E, Herbert J.1999.Principles of information. Course Technology.
- MillerR. 2008. Redes académicas de alta velocidad y tecnología avanzada como recurso para la investigación y el desarrollo regional. Tesis Ingeniero de Sistemas y Computación. Facultad de ingenierías eléctrica, electrónica, física y ciencias de la computación programa de ingeniería de sistema. Universidad tecnológica de Pereira.

- OpenVPN.2002. ¿Why SSL VPN?. http://openvpn.net/index.php/open-source/339-why-ssl-vpn.html. (Consultado 05/01/2011).
- Armando M, Sánchez M.(2001). Creación de Redes Privadas Virtuales en GNU/Linux con OpenVPN. http://tuxjm.net/docs/Creacion_de_Redes_Privadas_Virtuales_en_GNU_Linux_con_OpenVPN/html-onechunk/. (Consultado 10/01/2011).
- Tuvpn.2011.¿OpenVPN o PPTP?. http://blog.tuvpn.com/2010/06/%C2%BFopenvpn-o-pptp/?lang=es. (Consultado 10/01/011).
- Ernesto C . 210. Servidor Virtual Private Network (VPN). http://www2.linuxparatodos.net/web/comunidad/base-de-conocimiento/-/wiki/Base%20de%20Conocimiento/Servidor%20Virtual%20Private%20Network%20(VPN).(Consultado 05/02/2011).
- NettixPeru.2005.Red Privada Virtual o VPN.http://www.nettix.com.pe/index.php/vpn.html.(Consultado 07/02/2011).
- OpenVPN.2008. http://openvpn.net/index.php/open-source/documentation/miscellaneous/79-management-interface.html.(Consultado 20/02/2011).
- JamesY.2004.OpenVPNCOMO. http://laurel.datsi.fi.upm.es/~rpons/openvpn_como/.(Consultado 25/02/2011).
- Yury N.2010.Kaspersky Security Bulletin 2010 Principales Estadísticas de 2010.http://www.viruslist.com/sp/analysis?pubid=207271114.(Consultado 27/02/2011).
- Gestiopolis.2007.VPN la información de su empresa donde la necesite. http://www.gestiopolis.com/administracion-estrategia/estrategia/redes-virtuales-privadas-suministrando-informacion.htm.(Consultado 02/03/2011).
- Sorcier Empresas.2011.Desarrollo de red VPN para Perales Huancaruna SAC. http://www.sorcier.com.pe/blog/desarrollo-de-red-vpn-para-perales-huancaruca-sac.html.(Consultado 05/03/011).
- Guatewireless.2007.Prevenir ataques de diccionario sobre ssh.http://www.guatewireless.org/os/linux/ssh-acceso-seguro/.(Consultado 20/03/2011).
- Corporación educativa ADEU. 2000. Historia.http://www.ADEU.edu.pe/online/corp/lacorporacion.php.(Consultado 20/03/2011).
- GNU Operating System.2011.La Definición de Software Libre. http://www.gnu.org/philosophy/free-sw.es.html. (Consultado05/01/2011).
- Kaspersky Lab. 2012. Kaspersky Security Bulletin. Spam en 2011.http://www.viruslist.com/sp/analysis?pubid=207271164.
- certstopshop .2008. seguridad SSL 128 bits. http://www.certstopshop.com/SeguridadSSL128bits.aspx.(Consultado 23/05/2012)
- Raúl A.Dean. 2005. La invetsigacion tecnologica en la invetsigacion cientifica.http://www.unrc.edu.ar/publicar/23/dossidos.html. .(Consultado 23/05/2012)

IX. ANEXOS

Anexo Nº 01: Manual para la implementación de OpenVPN.

CONFIGURACIÓN PARA EL SERVIDOR

CONFIGURACIÓN DE INTERFACES VIRTUALES

Procedemos a la configuración de las interfaces Virtuales recordemos que necesitamos como mínimo 02 tarjetas de Red para que el servidor Interactué como Gateway o puerta de enlace y así otros equipos puedan conectarse a la VPN.
En el servidor OPENVPN necesitaremos estas 02 Interfaces:
Eth0: IP Publico: Comunicación con el Internet (192.168.164.130)
Eth0:1: IP privado estático: Comunicación con la Red LAN INTERNA (192.168.1.1)

Configurando la eth0:
Ingresamos

```
[root@localhost openvpn]# nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

Y luego agregamos los siguientes parámetros:

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:55:E5:2F
ONBOOT=yes
```

Esto quiere decir que la estamos dejando como DHCP para que VMWARE nos direccione una IP PUBLICA FIJA

Configurando la eth0:1
Hacemos una copia del eth0 de la siguiente manera

```
[root@localhost openvpn]# cp -rf /etc/sysconfig/network-scripts/ifcfg-eth0
etc/sysconfig/network-scripts/ifcfg-eth0:1
```

Y luego configuramos la interfaz virtual eth0:1 de la siguiente manera
Ingresamos a nano /etc/sysconfig/network-scripts/ifcfg-eth0:1

```
[root@localhost openvpn]# nano /etc/sysconfig/network-scripts/ifcfg-
eth0:1
```

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0:1
BOOTPROTO=static
IPADDR=192.168.1.1
NETMASK=255.255.255.0
ONBOOT=yes
```

Una vez hecho esto probamos si las interfaces están activas con el comando ifconfig

```
[root@localhost openvpn]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:55:E5:2F
          inet addr:192.168.164.141  Bcast:192.168.164.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe55:e52f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2697 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1867 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2849815 (2.7 MiB)  TX bytes:112015 (109.3 KiB)
          Interrupt:67 Base address:0x2000

eth0:1    Link encap:Ethernet  HWaddr 00:0C:29:55:E5:2F
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:67 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2752 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2752 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8918608 (8.5 MiB)  TX bytes:8918608 (8.5 MiB)
```

Como vemos las interfaces están ya activas.

CONFIGURACION DE REPOSITORIOS YUM

Primero descargamos openvpn

```
[root@localhost openvpn]# yum -y install openvpn
```

Los repositorios son los sites de internet donde el manejador de paquetes YUM buscara los programas para instalarlo, es necesario mantenerlo actualizado de lo contrario no podrás instalar paquetes adicionales. Aquí les mostraremos cómo actualizar esos repositorios.

Descargamos el paquete

```
wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

Luego lo instalamos

```
rpm -ivh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

INSTALACION DE PAQUETE OPENVPN

```
[root@localhost openvpn]# yum -y install openvpn
```

Con esa línea se procede a instalar el paquete openvpn donde se creara un directorio en la carpeta /etc/openvpn/

Creacion de la llave GENKEY, Construcción de una clave estática pre-compartida.

Genere una clave estática con el siguiente comando:

```
root@localhost openvpn]# openvpn --genkey --secret secret.key
```

La clave estática está formateada en ascii y tiene un aspecto como éste:

```
-----BEGIN OpenVPN Static key V1-----
e5e4d6af39289d53
171ecc237a8f996a
97743d146661405e
c724d5913c550a0c
30a48e52dfbeceb6
e2e7bd4a8357df78
4609fe35bbe99c32
bdf974952ade8fb9
71c204aaf4f256ba
eeda7aed4822ff98
fd66da2efa9bf8c5
e70996353e0f96a9
c94c9f9afb17637b
283da25cc99b37bf
6f7e15b38aedc3e8
e6adb40fca5c5463
-----END OpenVPN Static key V1-----
```

Con esa línea creamos la llave que luego copiaremos al otro servidor. La llave será encriptada y se llamara secret.key. Hay que tener en cuenta que esa línea se ejecuta dentro del directorio /etc/openvpn/ para que ahí cree secret.key si se hace fuera de este sitio se procedería a copiar.

Copie secret.key al otro extremo por medio de un medio seguro tal como copiar-pegar en una conexión ssh

CONFIGURACION DE ARCHIVO SERVER.CONF

Como el directorio /etc/openvpn esta vacio procedemos a copiar los archivos que necesitamos para poder instalar. Estos archivos que necesitamos es el server.conf y está dentro de la ruta /usr/share/docs/openvpn[version]/simple-config-files/

Los copiamos de la siguiente manera:

```
[root@localhost openvpn]# cp -rf /usr/share/doc/openvpn-2.1.4/sample-config-files/server.conf .
```

Luego procedemos a su configuración agregaremos los siguientes parámetros.

```
#  Copiamos la dirección IP de la red local del servidor 1
local 192.168.164.141
#  Copiamos la dirección IP de la red local del servidor 2
remote 192.168.164.142
# OpenVPN también soporta dispositivos Ethernet virtuales "tap", por
# medio de este dispositivo se crea el tunel.
dev tap
# Copiamos el IP y la máscara de subred del túnel
ifconfig  10.8.0.1   255.255.255.0
# Copiamos la ruta de la clave pre compartida
secret /etc/openvpn/secret.key
#  Por defecto OpenVPN utiliza el puerto UDP
port 1194
# Separación de privilegios para el servidor OpenVPN , después de que el
# servicio haya sido inicializado.
user nobody
group nobody
#  Siguen al DNS  si cambia su dirección IP.
float
disable-occ
#  Para una conexión más fiable cuando el sistema pierde su conexión.
ping 10
ping-restart 120
push "ping 10"
push "ping-restart 60"
# Rutiamos hacia el servidor donde deseemos hacer conexión.
route 192.168.2.0 255.255.255.0 10.8.0.2
# Nivel de severidad para logs de OpenVPN, en este caso 5 que es usado
#para  problemas de conectividad.
verb 5
```

Una vez hecho esto procedemos a reiniciar el servidor openvpn de la siguiente manera y debería darnos OK en ambos casos

```
[root@localhost openvpn]# service openvpn restart
Apagando openvpn:                                          [  OK  ]
Iniciando openvpn:                                         [  OK  ]
```

CONFIGURACION PARA EL SERVIDOR RECEPTOR

CONFIGURACIÓN DE INTERFACES VIRTUALES

Procedemos a la configuración de las interfaces Virtuales recordemos que necesitamos como mínimo 02 tarjetas de Red para que el servidor Interactué como Gateway o puerta de enlace y así otros equipos puedan conectarse a la VPN.
En el servidor OPENVPN necesitaremos estas 02 Interfaces:
Eth0: IP Publico: Comunicación con el Internet (192.168.164.131)
Eth0:1: IP privado estático: Comunicación con la Red LAN INTERNA (192.168.2.1)

Configurando la eth0:
Ingresamos

```
[root@localhost openvpn]# nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

Y luego agregamos los siguientes parámetros

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:6e:f5:6e
ONBOOT=yes
```

Esto quiere decir que la estamos dejando como DHCP para que VMWARE nos direccione una IP PUBLICA FIJA

Configurando la eth0:1

Hacemos una copia del eth0 de la siguiente manera:

```
[root@localhost openvpn]# cp -rf /etc/sysconfig/network-scripts/ifcfg-eth0
etc/sysconfig/network-scripts/ifcfg-eth0:1
```

Y luego configuramos la interfaz virtual eth0:1 de la siguiente manera
Ingresamos a nano /etc/sysconfig/network-scripts/ifcfg-eth0:1

```
[root@localhost openvpn]# nano /etc/sysconfig/network-scripts/ifcfg-
eth0:1
```

```
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0:1
BOOTPROTO=static
IPADDR=192.168.2.1
NETMASK=255.255.255.0
ONBOOT=yes
```

Una vez hecho esto probamos si las interfaces están activas con el comando ifconfig

```
[root@localhost openvpn]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:6E:F5:6E
          inet addr:192.168.164.142  Bcast:192.168.164.255
Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6e:f56e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6781 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6474251 (6.1 MiB)  TX bytes:522852 (510.5 KiB)
          Interrupt:67 Base address:0x2000

eth0:1    Link encap:Ethernet  HWaddr 00:0C:29:6E:F5:6E
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:67 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2632 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2632 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8766992 (8.3 MiB)  TX bytes:8766992 (8.3 MiB)
```

Como vemos las interfaces están ya activas.

CONFIGURACION DE REPOSITORIOS YUM

Primero descargamos openvpn

```
[root@localhost openvpn]# yum -y install openvpn
```

Los repositorios son los sites de internet donde el manejador de paquetes YUM buscara los programas para instalarlo, es necesario mantenerlo actualizado de lo contrario no podrás instalar paquetes adicionales. Aquí les mostraremos como actualizar esos repositorios.

Descargamos el paquete

```
wget http://packages.sw.be/rpmforge-release/rpmforge-release-0.3.6-
1.el5.rf.i386.rpm
```

Luego lo instalamos

```
rpm -ivh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

INSTALACION DE PAQUETE OPENVPN

```
[root@localhost openvpn]# yum -y install openvpn
```

Con esa línea se procede a instalar el paquete openvpn donde se creara un directorio en la carpeta /etc/openvpn/

INSTALAMOS EL OPENSSH

Es necesario instalar el openssh como servidor para poder establecer la conexión desde el server y copiar el genkey de un servidor a otro

```
[root@localhost openvpn]#yum –y install openssh
```

COPIAMOS EL GENKEY

Este paso lo realizamos desde el servidor hacia el cliente y hacemos lo siguiente

```
Scp llave.txt root@192.168.164.142:/etc/openvpn/
```

Luego verificamos si copio el kengey en el cliente:

```
[root@localhost openvpn]# ls
secret.key
```

CONFIGURACION DE ARCHIVO client.CONF

Como el directorio /etc/openvpn esta vacio procedemos a copiar los archivos que necesitamos para poder instalar. Estos archivos que necesitamos es el client.conf y está dentro de la ruta:

```
/usr/share/docs/openvpn[version]/simple-config-files/
```

Los copiamos de la siguiente manera:

```
[root@localhost openvpn]# cp -rf /usr/share/doc/openvpn-2.1.4/sample-config-files/client.conf .
```

Luego procedemos a su configuración agregaremos los siguientes parámetros.

```
# Copiamos la dirección IP de la red local del servidor 1
local 192.168.164.142
# Copiamos la dirección IP de la red local del servidor 2
remote 192.168.164.141
# Por defecto OpenVPN utiliza el puerto UDP
port 1194
# OpenVPN también soporta dispositivos Ethernet virtuales "tap", por
# medio de este dispositivo se crea el tunel.
dev tap
# Copiamos el IP y la máscara de subred del túnel
ifconfig 10.8.0.2 255.255.255.0
# Siguen al DNS si cambia su dirección IP.
float
disable-occ
# Copiamos la ruta de la clave pre compartida
secret /etc/openvpn/secret.key
# Para una conexión más fiable cuando el sistema pierde su conexión.
ping 10
ping-restart 120
push "ping 10"
push "ping-restart 120"
# Rutiamos hacia el servidor donde deseemos hacer conexión.
route 192.168.1.0 255.255.255.0 10.8.0.1
# Nivel de severidad para logs de OpenVPN, en este caso 5 que es usado
# para problemas de conectividad.
verb 5
```

Una vez hecho esto procedemos a reiniciar el servidor openvpn de la siguiente manera y debería darnos OK en ambos casos

```
[root@localhost openvpn]# service openvpn restart
Apagando openvpn:                                          [  OK  ]
Iniciando openvpn:                                         [  OK  ]
```

CONFIGURACIÓN DE CLIENTES

Se configuraran los clientes de la red, cada cliente tiene que estar en la misma red que está configurado el servido.

Cliente1 de la red1 enlazado con el servidor 1 tomara el siguiente IP: 192.168.1.2
Cliente2 de la red1 enlazado con el servidor 1 tomara el siguiente IP: 192.168.1.3
Cliente3 de la red1 enlazado con el servidor 1 tomara el siguiente IP: 192.168.1.4
Cliente1 de la red2 enlazado con el servidor 2 tomara el siguiente IP: 192.168.2.2
Cliente2 de la red2 enlazado con el servidor 2 tomara el siguiente IP: 192.168.2.3
Cliente3 de la red2 enlazado con el servidor 2 tomara el siguiente IP: 192.168.2.4

Para la seguridad de OpenVPN proporcionara una clave estática pre-compartida de tipo HMAC de 2048 bits, la cual se copiara en cada servidor:

```
-----BEGIN OpenVPN Static key V1-----
e5e4d6af39289d53
171ecc237a8f996a
97743d146661405e
c724d5913c550a0c
30a48e52dfbeceb6
e2e7bd4a8357df78
4609fe35bbe99c32
bdf974952ade8fb9
71c204aaf4f256ba
eeda7aed4822ff98
fd66da2efa9bf8c5
e70996353e0f96a9
c94c9f9afb17637b
283da25cc99b37bf
6f7e15b38aedc3e8
e6adb40fca5c5463
-----END OpenVPN Static key V1-----
```

Mediante esta clave solo podrán acceder a la VPN corporativa aquellos que tengan la clave pre compartida.
OpenVPN proporciona una encriptación de 256 bits la cual es fiable, incluso en redes con una latencia alta y en largas distancias.