UNIVERSIDAD NACIONAL DE LOJA

AREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

Ingeniería en Sistemas

"IMPLEMENTACIÓN DE UN SERVIDOR VPN QUE PERMITA LA MOVILIDAD DE USUARIOS DE LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA Y SU INTEGRACIÓN CON EL SERVIDOR DE VoIP. "

Tesis de grado previa a la obtención del Grado de Ingeniero en Sistemas

Marco Xavier Rojas Vivanco
Manuel Agustín Valarezo Salinas

AUTORES

Ing. Ketty Delfina Palacios Montalván

DIRECTORA

Loja - Ecuador **2009**

CERTIFICACIÓN

Sra. Ing.

Ketty Delfina Palacios Montalván
DIRECTORA DE TESIS

CERTIFICA:

Que el presente proyecto de tesis elaborado previa la obtención del título en Ingeniería en Sistemas, titulada: **"IMPLEMENTACIÓN DE UN SERVIDOR VPN QUE PERMITA LA MOVILIDAD DE USUARIOS DE LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA Y SU INTEGRACIÓN CON EL SERVIDOR DE VoIP",** realizada por los postulantes: Marco Xavier Rojas Vivanco y Manuel Agustín Valarezo Salinas, cumple con los requisitos establecidos por la normas generales para la graduación en la Universidad Nacional de Loja, tanto en aspecto de forma como de contenido.

Por lo tanto, autorizo proseguir los trámites legales pertinentes para su presentación y defensa.

Loja, Julio del 2009.

Ing. Ketty Delfina Palacios Montalván
DIRECTORA DE TESIS

AUTORÍA

Las expresiones, opiniones, ideas, análisis crítico, interpretaciones y contenidos en el presente trabajo son de exclusiva responsabilidad de los autores.

Marco Xavier Rojas Vivanco

Manuel Agustín Valarezo Salinas

CESIÓN DE DERECHOS

Marco Xavier Rojas Vivanco y Manuel Agustín Valarezo Salinas, Egresados de la Carrera de Ingeniería en Sistemas, conceden todos los derechos de autor de la tesis, cuya problemática versa sobre el tema: **"IMPLEMENTACIÓN DE UN SERVIDOR VPN QUE PERMITA LA MOVILIDAD DE USUARIOS DE LA RED DE DATOS DE LA UNIVERSIDAD NACIONAL DE LOJA Y SU INTEGRACIÓN CON EL SERVIDOR DE VoIP",** a la Universidad Nacional de Loja, para los fines que la institución considere necesarios.

Loja, Julio de 2009.

Marco Xavier Rojas Vivanco

EGDO. CARRERA DE INGENIERÍA EN SISTEMAS

Manuel Agustín Valarezo Salinas

EGDO. CARRERA DE INGENIERÍA EN SISTEMAS

AGRADECIMIENTO

Queremos expresar nuestro más profundo agradecimiento a la Universidad Nacional de Loja, al Área de la Energía, las Industrias y los Recursos Naturales no Renovables y a la Carrera de Ingeniería en Sistemas.

De la misma manera nuestra eterna gratitud a todos los directivos y docentes del Área de la Energía, las Industrias y los Recursos Naturales no Renovables por brindarnos su ayuda y conocimientos y permitirnos culminar esta etapa en nuestra vida profesional.

A nuestros padres, familiares y amigos por ser quienes nos inspiraron a seguir adelante en la lucha de alcanzar nuevas metas y objetivos en la vida.

A nuestra Directora de Tesis Ing. Ketty Palacios Montalván, por su acertada ayuda y asesoría durante todo el proceso de desarrollo de este trabajo, ya que gracias a sus conocimientos y sugerencias hemos logrado tener nitidez y claridad en toda nuestra investigación.

De manera especial queremos hacer llegar nuestro más sincero sentimiento de admiración y estima a todo el personal de la Jefatura de Informática de la Universidad Nacional de Loja y a su Director el Lic. Jamil Ramón Carrión, por la desinteresada apertura que se nos ha dado y así poder terminar este proyecto.

DEDICATORIA

"A Dios por ser la mayor inspiración en mi vida, a mi esposa Yasmira y a mi hija Camila por estar a mi lado dándome fuerzas siempre con su ternura, a mis padres Marco y Luz que con amor supieron guiarme para bien, a mis hermanos Daniel y Santiago con quienes he aprendido a luchar para ser una mejor persona y a mis amigos por ser los hermanos que Dios me permitió elegir"

Marco Xavier Rojas Vivanco

A mi Madre.

Manuel Agustín Valarezo Salinas

1. RESUMEN

El siguiente Proyecto de Desarrollo tiene como finalidad encontrar una solución a las necesidades de acceso externo, por parte de los usuarios, a los servicios que brinda la red de datos de la Universidad Nacional de Loja, tales como: Servidor de Correos (SMTP), Software para Bibliotecas, Software de Bodegas, Sistema de Gestión Académico (SGA) y puntualmente al Servidor Asterisk para Voz sobre IP (VoIP). Para así lograr tener una mayor accesibilidad a los recursos, con bajo presupuesto y sin descuidar la seguridad e integridad de la información que se maneja.

La tecnología y las nuevas tendencias en seguridad informática nos permiten encontrar soluciones robustas a la hora decidir la mejor opción en la implementación de una Red Privada Virtual (VPN), es por ello que fue indispensable realizar un estudio de las posibles medidas a tomar de acuerdo a las particularidades de la red de datos.

Resulta imprescindible optar siempre por Software Libre, es por ello que destacamos su uso, por las bondades que ofrece, puesto que ha venido determinando las nuevas directrices en el desarrollo de sistemas y soluciones informáticas de calidad en todo sentido.

La creación de usuarios VPN conlleva a la implementación de seguridades con el fin de garantizar el acceso sin ningún peligro de vulnerabilidad al momento de establecer los túneles virtuales de ingreso hacia le red de datos de la universidad.

Así mismo las conclusiones a las que hemos llegado nos han demostrado que es posible encontrar soluciones libres con bajo presupuesto con las garantías suficientes de que el ingreso a la red sea únicamente a usuarios autorizados.

Llegando finalmente a dar algunas recomendaciones para futuras problemáticas que se puedan presentar y algunas sugerencias para lograr un mejor funcionamiento de la Red Privada Virtual (VPN) implementada en la Universidad Nacional de Loja

2. ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

3. INTRODUCCIÓN

El presente proyecto de desarrollo ha sido efectuado en vista a la eminente demanda de tecnología y soluciones informáticas, enfocadas al máximo aprovechamiento de los recursos y servicios que brinda la red de datos de la Universidad Nacional de Loja y a la implementación de un servidor de Redes Privadas Virtuales (VPN´s) como una herramienta fundamental para lograr el acceso a la red con las seguridades suficientes como para garantizar la integridad de datos y así mismo certificar que éstos no puedan ser vulnerados.

A nivel mundial las Redes Privadas Virtuales se han constituido en uno de los mayores logros del desarrollo de tecnologías informáticas ya que han dado paso a un sinnúmero de nuevas formas de trabajo, de acceso a redes, de integración de datos principalmente en empresas e instituciones que ven necesaria la unificación de sus diferentes sucursales, delegaciones o agencias con su matriz como si se tratase de una sola red interna, así mismo han permitido la unión entre diferentes entidades que requieren estar enlazadas para sincronizar procesos y compartir recursos; por otra parte, el Teletrabajo se está instituyendo como una de las mayores tendencias de contratación de empleados en las grandes compañías ya que éstos pueden realizar sus tareas y labores desde sus casas únicamente requiriendo para ello una conexión a internet y de tener establecida una VPN con su entidad empleadora optimizando y ahorrando recursos, tanto económicos como de tiempo.

Con lo antes expuesto y en vista de la problemática que se ha venido dando al momento tratar de enlazar las diferentes extensiones universitarias con la matriz y de pretender dar movilidad a los usuarios, hemos considerado como indispensable el uso de una Red Privada Virtual.

La principal aspiración es el de implementar un servidor VPN con la finalidad de permitir el acceso a los usuarios externos de la red de datos y así mismo hacer uso de los recursos y servicios que ella brinda, fundamentalmente el de la Telefonía IP.

Para ello fue necesario hacer un estudio detallado con la finalidad de conocer los conceptos, requerimiento y los diferentes tipos de VPN y solamente luego de esto si hacer una comparativa de la mejor opción a implementar en nuestro caso particular.

Una vez elegido el mejor método para éste propósito se hizo la instalación y las configuraciones para la puesta en marcha de la misma, y seguidamente se realizaron pruebas permitiendo autenticar a los usuarios en el servidor OpenVPN y de esta manera poder hacer uso de todos los beneficios.

El Proyecto está estructurado de la siguiente forma:

Arrancamos haciendo una explicación de **La Metodología** a utilizar en el transcurso tanto de la investigación, como de la implementación y desarrollo del presente trabajo, para de esta forma establecer los lineamientos que permitieron obtener resultados de la investigación realizada.

La Fundamentación Teórica se ha desarrollado con la finalidad de esclarecer y conocer a fondo los conceptos y definiciones que mostrarían un mejor panorama de la situación de tal forma que se llegue a tener un mayor dominio de los conocimientos que se usaran para este proceso.

En la Evaluación del Objeto de Investigación realizamos un pequeño análisis de la situación actual en la red de datos de la Universidad Nacional de Loja, así como un recuento de la problemática que se ha venido dando y de la misma forma se describe la facilidad que se brindó a los investigadores para que se pueda trabajar sin ningún impedimento en éste trabajo.

La Propuesta Alternativa nos narra de manera puntual la solución que se dió a la necesidad de dar acceso a usuarios externos a la red de manera segura y sin afectar a la integridad de la información que en ella se maneja, de tal forma que se indica paso a paso las instalaciones, configuraciones y diferentes parámetros a establecer para llegar a este propósito. Se muestran además algunos de los posibles problemas que se podrían presentar al momento de hacer la ejecución de estos pasos.

La Valoración Técnico-Económica nos indica los datos técnicos específicos que incurrieron en este transcurso y de la misma forma un conciso estudio económico que nos revela los gastos reales que intervinieron.

Finalmente las **Conclusiones y Recomendaciones** son en si los recursos más importantes al momento de evaluar los verdaderos resultados de todo este proyecto de desarrollo ya que nos detallan la esencia de los productos logrados.

4. METODOLOGÍA

4.1. METODOLOGÍA PARA LA INVESTIGACIÓN

El hombre a través de la historia, se ha caracterizado por su afán de conocer su realidad y el entorno en el cual se encuentra inmerso.

Averiguar y saber cuál es el objeto de su existencia y el resultado de sus acciones han sido elementos clave en su que hacer histórico.

La fuente de esta necesidad de conocer y de saber surge de su curiosidad, elemento fundamental en la personalidad del investigador que lo lleva a cuestionar, a indagar y por ende a adquirir los conocimientos que le permitan evolucionar y trascender. De hecho el conocimiento que le ha sido legado a la humanidad y por el cual se ha logrado el desarrollo que se vive en la actualidad tiene como base las investigaciones y descubrimientos que se encuentran plasmados en la historia de la humanidad.

El siguiente trabajo será desarrollado tomando en cuenta la mejor forma de describir los procesos en él realizados para así obtener un resultado óptimo y listo a resolver las necesidades de comunicación.

Esta investigación es de carácter práctica y científica a la vez por lo que resultó indispensable realizar la respectiva investigación de campo para luego de esto plantear un diseño de las mejores soluciones.

Para obtener una mejor idea de cómo funciona la red interna de la universidad fue necesario empaparnos totalmente de la operatividad de todos y cada uno de los componentes que forman esta red, el mismo que fue realizado gracias al hecho de tener acceso a muchos de los centros informáticos que funcionan actualmente en la universidad, con las restricciones del caso por tratarse de información confidencial y para evitar vulnerar las seguridades de la misma.

Si bien es cierto la propuesta de realizar un túnel virtual se debe a la necesidad de interconectar la Web (Internet) con la red interna de la Universidad, es necesario realizar un minucioso estudio de las posibles vulnerabilidades de este servicio, aunque en el desarrollo de la presente investigación se demostrará la seguridad que ofrece nuestra solución.

4.2. MOMENTOS EN UNA INVESTIGACIÓN

Según Carlos Sabino en su libro "El Proceso de Investigación" existen cuatro momentos en una investigación, los cuales hemos aplicado en nuestra investigación:

1. **Lógico**.- se ordenan las preguntas, se organiza la información, se definen los sujetos y objetos.
2. **Metodológico.-** se fijan las estrategias y formula un modelo operativo.
3. **Técnico.-** se recolecta y organiza la información.
4. **Análisis y reformulación teórica.-** se analizan los resultados, se aceptan o rechazan las hipótesis y se confirma las teorías.

4.3. METODOLOGÍA PARA EL DESARROLLO DE LA INVESTIGACIÓN

Para el desarrollo de la investigación se tomo en cuenta principalmente los siguientes métodos de investigación:

El Método Científico.- Proporciona al hombre la posibilidad de comprender los más diversos fenómenos de la realidad. Al analizar los fenómenos de la naturaleza, de la sociedad y del pensamiento permite descubrir sus verdaderas leyes y las fuerzas motrices del desarrollo de la realidad.

El Método Científico busca siempre la demostración de la verdad mediante la aplicación de técnicas conocidas y sencillas como lo son la observación directa y la entrevista hacia quienes están a cargo del manejo, diseño, implementación y mantenimiento de la red informática de la universidad así como de los usuarios de la

misma ya que es aquí precisamente donde nace la necesidad de movilidad a nivel mundial.

También como parte del Método Científico tenemos las pruebas para apoyar las afirmaciones que proponen las hipótesis planteadas en base a técnicas ya establecidas para éste tipo de investigaciones.

Proceso de Construcción del Conocimiento Científico.- El proceso de construcción del conocimiento científico sirve para orientar el trabajo de investigación. Bunge dice "El arte de formular preguntas y de probar respuestas esto es, el método científico..."

El Método Inductivo.- Es el método por el cual, a partir de varios casos observados, se obtiene una ley general, válida también para los casos no observados. Consiste, pues, en una acción generalizadora, o más simplemente, en una generalización.

Este método parte desde lo particular y específico hacia lo general o universal, es por esto que mediante la observación directa se pudo determinar cuáles podrían ser los posibles errores, necesidades y soluciones especificas a problemas particulares para luego de haber pasado por un proceso de análisis basado en pruebas y demás técnicas llegar a determinar la generalización de estos hechos.

La inducción parte de un supuesto o principio. Si de algunos pasamos a todos, es porque creemos que el curso de la naturaleza es uniforme; si del hecho pasamos a su forzosidad, es porque nada de lo que sucede en la naturaleza hubiera podido no suceder, o sea que en la naturaleza todo está determinado; si del hecho pasamos a la ley, es porque consideramos que la naturaleza obedece a las leyes, y que en todo hecho se expresa una ley, es por esta razón que podemos determinar por ejemplo que si alguna de las soluciones encontradas en esta investigación en un caso especifico, también puede servir como solución para problemas similares, por lo que podemos llegar a generalizar estas afirmaciones.

El Método Deductivo.- Es un proceso analítico sintético que presentan conceptos, definiciones, leyes o normas generales, de las cuales se extraen conclusiones o se examina casos particulares sobre la base de Afirmaciones generales ya presentadas.

Parte de una teoría unificada basada en información general y considera cada hipótesis en el marco de la teoría para llegar a observaciones empíricas que confirmen o refuten cada hipótesis.

Procede de la formulación de enunciados generales ha hipótesis más específicas que se deriven lógicamente de los enunciados generales, este método requiere de procesos de investigación lógicos y sistemáticos, ayuda a explicar, predecir y controlar fenómenos.

Éste método fue de singular ayuda ya que mediante la utilización de conceptos generales en redes, seguridades, etc. nos permiten llegar a proponer soluciones específicas.

El Método Analítico-Sintético.- En este caso partimos desde una síntesis para luego analizar hechos concretos observando casos anteriormente ocurridos que tienen relación con nuestro objeto de investigación, para en base a sus conclusiones y recomendaciones llegar a proponer soluciones aplicables a nuestro caso.

4.4. TÉCNICAS E INSTRUMENTOS UTILIZADOS

A lo Largo de todo el proceso de investigación nos fuimos encontrando con la necesidad de aplicar diversas técnicas de investigación y valernos de algunos instrumentos para poder continuar con la búsqueda de la elección de la mejor solución frente a los problemas planteados.

4.5. BÚSQUEDA DE LA INFORMACIÓN

Para la búsqueda de información tomamos en cuenta lo siguiente:

La Unidad de Análisis.- Este es el elemento mínimo de estudio en relación con otros elementos de su mismo tipo.

La Medición.- Está relacionada con la unidad de análisis. Se le asignan unas variables que pueden ser: Nominales, Ordinales y de Intervalo.

Tipos de información.- Existen dos tipos de información: la primaria que es la que se obtiene del contacto directo con el objeto de estudio y la secundaria que se obtiene de la búsqueda de la información.

4.6. TÉCNICAS PARA RECOLECTAR LA INFORMACIÓN.

Las técnicas para la recolección de información utilizadas son las siguientes:

La Observación.- Se mide el fenómeno, ya que se obtiene información de la unidad de análisis. Existen dos tipos: la no estructurada que es utilizada en investigaciones exploratorias, no se tiene conocimiento del fenómeno y la estructurada que quiere información más precisa y especifica.

La que hemos utilizado es la estructurada ya que hemos querido obtener soluciones específicas más óptimas y sin necesidad de utilizar la técnica de "ensayo error".

La Entrevista.- Este es un reporte verbal de una persona para obtener información, involucra aspectos más complejos y emocionales que los de una encuesta.

La cual ha sido realizada a quienes manejan la red interna de la universidad, ya que por su rol nos pudieron dar información clave en este proceso.

La Encuesta.- Se realizó mediante un formato establecido. Se tuvo claro el objetivo de la encuesta y su relación con el marco teórico y la hipótesis.

Análisis de los Datos.- Una vez obtenida la información la tabulamos y comenzamos a trabajar con ella.

5. FUNDAMENTACIÓN TEÓRICA

5.1 DESCRIPCIÓN DE LA RED INTERNA DE LA UNIVERSIDAD NACIONAL DE LOJA Y SUS SERVICIOS

5.1.1 INTRODUCCIÓN

La Universidad Nacional de Loja se ha visto inmersa en procesos de modernización tanto en su estructura organizacional como en el soporte tecnológico a las diferentes actividades académico administrativas, lo que ha dado paso a la implementación de una red de datos que permite la comunicación de los usuarios, así como la necesidad de estar inmersos en el mundo de la información global como Internet.

Teniendo en cuenta la necesidad de comunicación de los usuarios el presente proyecto propone la implementación de un servidor de redes privadas virtuales que además permita la movilidad de los usuarios de la red de datos de la Universidad Nacional de Loja, y el aprovechamiento de los servicios de la red; puntualmente realizar la integración con el servidor de voz sobre IP.

5.1.2 ADMINISTRACIÓN CENTRAL

La Jefatura de Informática es el punto central de la red universitaria. Es aquí donde existen los siguientes equipos instalados:

- Un Router Cisco 1800, que es el que permite la interconexión con Internet comercial e Internet2. El manejo de este equipo de uso exclusivo del proveedor de Internet para la Universidad, TELCONET. El proveedor llega al campus universitario por medio de fibra óptica como medio de comunicación.

- Un Switch D-Link, Gigabit, uso exclusive de Telconet

- Un Switch D-Link des-1016r, que se encuentra conectado a la interfaz LAN del Router. Los equipos que se conectan a este switch son principalmente: el Firewall (Fw), el servidor web, el servidor de correo, y el switch central de la Red Interna. Además aquí se conecta todos los servidores que la universidad necesite tener con una ip pública, para que puedan ser accedidos desde el exterior.

- El Fw que es el servidor que permite tener la barrera entre la red pública y la red interna de datos, aquí constan las reglas que optimizan el uso del Internet en la Universidad.

  Es en este equipo donde se pretende implementar el Servidor VPN

  Las características del Fw son:

  - ✓ Sistema Operativo Linux Fedora Core 3
  - ✓ Intel(R) Xeon (TM) CPU 3.2 GHZ
  - ✓ RAM 1Gb
  - ✓ HDD 160 GB

- Un Servidor Web, donde se encuentra instalada la página web de la Universidad. Las características las describimos a continuación:

  - ✓ Sistema Operativo Linux Fedora Core 3
  - ✓ Intel(R) Xeon (TM) CU 3.2 GHZ
  - ✓ RAM 1Gb
  - ✓ HDD 160 *G*B

- Un Servidor de Correo. Este servidor permite tener a los usuarios correos bajo el dominio de la universidad, por ejemplo **informatica@unl.edu.ec**.

- Switch principal Intel Express 410T Standalone, desde aquí nace la Backone de la red Interna, es decir, desde este equipo inicia la interconexión con la diferentes áreas académicos administrativas.

- Switch catalyst 2950 conectado al switch principal, permite la conexión con el área de energía por medio de un par de hilos de cobre. (preguntar).

- Switch 3com 3300, conectado al switch principal, que permite la conexión con el bloque uno de la Administración Central

- Switch des – 3624, conectado al switch principal, que permite la conexión con el bloque dos de la Administración Central

- Switch des – 3624i, conectado al switch principal, que permite la conexión con los equipos y servidores internos de la jefatura de Informática Central.

- Transaiver mc102xl fast Ethernet media converter, conectado al switch principal, este permite la conexión con el área agropecuaria por medio de fibra óptica

- Transaiver d-link def-855, conectado al switch principal, este permite la conexión con el área educativa por medio de fibra óptica

- Transaiver d-link def-855, conectado al switch principal, este permite la conexión con el área jurídica por medio de fibra óptica.

- Un Radio (ROR) conectado al swicth principal y a una antena que permite tener comunicación con el área de la salud.

- Un servidor de DHCP, que permite asignar dinámicamente direcciones de red a cada computador, por medio de la MAC de la interfaz de red. Características:
  - ✓ Sistema Operativo Linux Fedora Core 6
  - ✓ Intel(R) Pentium (r) D CPU 3.4 GHZ
  - ✓ RAM 1GB
  - ✓ HDD 160GB.

- Un Servidor para el control de contenido. utiliza el software Squid y Dansguardian. Este servidor permite tener un control efectivo en el acceso a páginas pornográficas

y de contenido malicioso principalmente, así como se evita un consumo excesivo de ancho de banda. Este control se lo hace en cada una de los servidores de las áreas, como apoyo del mismo.

5.1.3 ÁREA AGROPECUARIA Y RECURSOS NATURALES RENOVABLES

La interconexión con esta área es por intermedio de fibra óptica. Los principales equipos que se encuentran en esta área son:

- Una caja multimedia donde llega la fibra óptica.
- Un transaiver d-link def-855 conectado a la caja multimedia y conectado a Switch 3com.
- El Switch 3Com se conecta con el servidor del Área Agropecuaria
- Un switch D-link de 16 puertos (Switch Principal).
- Un servidor que tiene instalado el servicio de Squid y Dansguardian que sirve para el control de Contenido. El servidor se conecta con el Switch 3com.

Las características del servidor son:

- ✓ Sistema Operativo Linux Fedora Core 6
- ✓ Intel(R) Pentium (r) 4 CPU 3.0 GHZ
- ✓ RAM 512Mb
- ✓ HDD 160 GB

- Existe un transaiver d-link def-855 conectado al Switch Principal, el mismo permite conectar por medio de fibra óptica a otros puntos del área.

- Un multipunto que permite conectar inalámbricamente con el nivel de postgrado del área agropecuaria y con el ex Cater.

5.1.4 ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

A esta área se llega desde la administración central por medio de hilos de cobre. Se parte desde el Switch catalyst 2950 de la Administración Central hasta un Modem Cisco - 673 que está conectado al servidor del área.

- Existe un servidor que tiene instalado el servicio de Squid y Dansguardian que sirve para el control de Contenido.

5.1.5 ÁREA DE EDUCACIÓN, ARTE Y COMUNICACIÓN

La interconexión con esta área es por intermedio de fibra óptica. Existen dos secciones de red en esta área, la primera tiene como punto central la biblioteca del área y la segunda en el centro de cómputo del área. Los principales equipos que se encuentran en esta área son:

Biblioteca del Área Educativa:

Dos cajas multimedia donde llega la fibra óptica.

- Un transaiver d-link def-855 conectado a la caja multimedia (1).

- Un switch D-Link de 8 puertos que está conectado al servidor y a un transaiver d-link def-855.

- Switch 3Com de 16 puertos (Switch Principal)

- Existe un servidor que tiene instalado el servicio de Squid y Dansguardian que sirve para el control de Contenido. El servidor se conecta al Switch Principal.

  Las características del servidor son:

  - ✓ Sistema Operativo Linux Fedora Core 6
  - ✓ Intel(R) Pentium (r) 4 CPU 3.0 GHZ
  - ✓ RAM 512Mb
  - ✓ HDD 80gb

- Un transaiver d-link def-855 conectado con la caja multimedia (2), que lleva la fibra óptica al Centro de Cómputo de Área Educativa

Centro de Cómputo del Área Educativa:

- Tres cajas multimedia donde llega la fibra óptica

- Un transaiver d-link def-855 que está conectado a la caja multimedia.

- Switch D-Link de 8 puertos (Switch Principal Área Educativa 2).

Además existe en esta área un multipunto que permite conectar inalámbricamente con:

- El nivel de de pregrado del área educativa

- El nivel de de postgrado del área educativa

- Colegio Manuel Cabrera Lozano.

5.1.6 ÁREA JURÍDICA SOCIAL Y ADMINISTRATIVA

La interconexión con esta área es por intermedio de fibra óptica. Existen dos secciones de red en esta área, la primera tiene como punto central la biblioteca del área y la segunda en el nivel de postgrado del área. Los principales equipos que se encuentran en esta área son:

Biblioteca del Área Jurídica:

- Una caja multimedia donde llega la fibra óptica.

- Un transaiver D-Link def-855 conectado a la caja multimedia.

- Un switch D-Link que está conectado al servidor y a un transaiver D-Link def-855.

- Existe un servidor que tiene instalado el servicio de Squid y Dansguardian que sirve para el control de Contenido. EL servidor se conecta al Switch Principal.

  Las características del servidor son:

  - ✓ Sistema Operativo Linux Fedora Core 6
  - ✓ Intel(R) Pentium (r) 4 CPU 3.0 GHZ

- ✓ RAM 512Mb
- ✓ Disco 80gb

- Un transaiver d-link def-855 conectado con la caja multimedia (2), que lleva la fibra óptica al nivel de postgrado del Área Jurídica (Parte del Nivel de Postgrado del Área Jurídica, Social y Administrativa)

Nivel de Postgrado del Área Jurídica, Social y Administrativa

- Dos cajas multimedia donde llega la fibra óptica.

- Un transaiver d-link def-855 conectado a la caja multimedia.

- Un Switch D-Link que está conectado a un transaiver d-link def-855.

Además existe en esta área dos multipuntos que permite conectar inalámbricamente los bloques estos son:

Multipunto Uno

- Bloque principal del área.

- Centro de Computo principal del área

- Bloque Modalidad de Estudios a Distancia.

Multipunto Dos

- Carrera de Contabilidad

- Carrera de Banca y Finanzas.

5.1.7 BIENESTAR ESTUDIANTIL

La interconexión con Bienestar Estudiantil es por intermedio de un enlace inalámbrico utilizando para ello un Access Point D-Link 2100 AP+.

Existe un servidor que tiene instalado el servicio de Squid y Dansguardian que sirve para el control de contenido. EL servidor se conecta al Switch Principal.
Las características del servidor son:

- ✓ Sistema Operativo Linux Fedora Core 6
- ✓ Intel(R) Pentium (r) 4 CPU 2.8 GHZ
- ✓ RAM 512Mb
- ✓ HDD 80gb

5.1.8 ÁREA DE LA SALUD HUMANA

Con el área de la Salud Humana se tiene una conexión inalámbrica. A través de dos BackHoul Canopy. A continuación detallamos los principales componentes de red:

- Un switch 3Com (Switch Principal) conectado al BackHoul Slave.

- Un radio D-link multipunto, que permite tener comunicación con el Instituto de Idiomas y la Editorial Universitaria.

- Existe un servidor que tiene instalado el servicio de Squid y Dansguardian que sirve para el control de Contenido. EL servidor se conecta al Switch Principal.

  Las características del servidor son:
  - ✓ Sistema Operativo Linux Fedora Core 3
  - ✓ Intel(R) Pentium (r) 4 CPU 2.8 GHZ
  - ✓ RAM 512Mb
  - ✓ HDD 80gb

5.2 RED PRIVADA VIRTUAL

5.2.1 INTRODUCCIÓN

VPN son las siglas en inglés de Red Privada Virtual (Virtual Private Network). Las VPN's representan una enorme ventaja de negocios para las empresas. Una VPN ayuda a las empresas a reducir costos de capital y operación ya que convergen redes tradicionales heterogéneas en una VPN, y aumentan la productividad soportando aplicaciones como VoIP, mensajería unificada, videoconferencias, y aplicaciones de servicio para los clientes.[1]

Este servicio consiste en la extensión de una red informática a ordenadores que no estén ubicados físicamente en ésta. De esta forma se permite a los usuarios de la red conectarse desde un ordenador externo de forma sencilla y transparente, formando parte de todos los servicios que preste la red. (Ver Fig. 5.1)

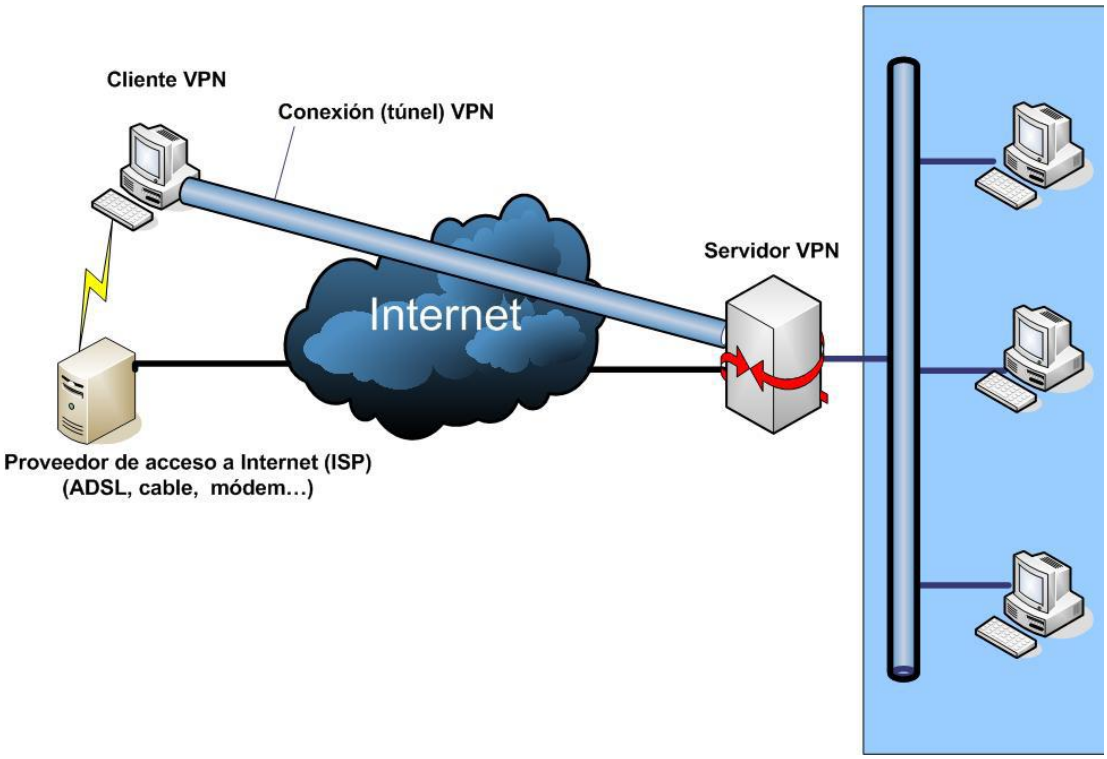

Fig. 5.1 Topología de una Red Privada Virtual

[1] www.cisco.com/web/LA/docs/doc/IP**VPN**SalesToolkitFINAL.doc

Con una Red Privada Virtual (VPN), los usuarios remotos, que pertenecen a una red privada, pueden comunicarse de forma libre y segura entre redes remotas a través de redes públicas.

Una VPN normalmente usa la red Internet como transporte para establecer enlaces seguros, extendiendo las comunicaciones a oficinas aisladas. Significativamente, decrece el coste de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.

Una Red Privada Virtual transporta -- de manera segura por Internet -- por un túnel establecido entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte. Una VPN permite el acceso remoto a servicios de red de forma transparente y segura con el grado de conveniencia y seguridad que los usuarios conectados elijan.

La velocidad de acceso dependerá del tipo de conexión a Internet que utilice el usuario.

5.2.2 DEFINICIÓN DE RED PRIVADA VIRTUAL (VPN)

"Una VPN es una red privada desplegada sobre una infraestructura pública compartida que proporciona niveles de privacidad, seguridad, QoS, y administración en forma similar a las redes construidas sobre instalaciones dedicadas, arrendadas o que son propiedad privada."[2]

Los servicios VPN se componen de dos grupos genéricos, que no son mutuamente excluyentes:

- *VPN de sitio-a-sitio*: Conectan las instalaciones de la oficina central y de las sucursales sobre una infraestructura compartida de un proveedor de servicios o a través de Internet utilizando una conexión siempre activa; las VPN's de sitio-a-sitio también pueden conectar a una empresa con sus clientes, proveedores, y asociados de negocios

[2] www.cisco.com/web/LA/docs/doc/IP**VPN**SalesToolkitFINAL.doc

- *VPN de acceso remoto*: Conectan a los trabajadores remotos y usuarios móviles a los recursos disponibles en una red corporativa mediante acceso dialup, DSL de banda ancha, cable, o inalámbrico a través de la red de un proveedor de servicios

5.2.3 REQUERIMIENTOS BÁSICOS DE UNA RED PRIVADA VIRTUAL

Una Red Privada Virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones y situaciones puedes obviarse algunos.

- Autentificación de usuarios, verificar la identidad de los usuarios, para poder restringir el acceso a la VPN solo a los usuarios autorizados.

- Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.

- Encriptación de datos, los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.

- Administración de claves, debe mantener un mantenimiento de claves de encriptación para los clientes y los servidores.

- Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando las red pública, por ejemplo IPX, IP, etc.

5.2.4 PROTOCOLOS

Han sido implementados varios protocolos de red para el uso de las VPN. Estos protocolos continúan compitiendo por la aceptación, ya que ninguno de ellos ha sido más admitido que otro.

Estos protocolos son los siguientes:

- Point-to-Point Tunneling Protocol (PPTP): PPTP es una especificación de protocolo desarrollada por varias compañías. Normalmente, se asocia PPTP con Microsoft, ya que Windows incluye soporte para este protocolo. Los primeros inicios de PPTP para Windows contenían características de seguridad demasiado débiles para usos serios. Por eso, Microsoft continúa mejorando el soporte PPTP. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. Sin embargo, el principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar: dos productos que acceden con la especificación PPTP pueden llegar a ser completamente incompatibles simplemente porque la encriptación de los datos sea diferente.

- Layer Two Tunneling Protocol (L2TP): El principal competidor de PPTP en soluciones VPN fue L2F, desarrollado por Cisco. Con el fin de mejorar L2F, se combinaron las mejores características de PPTP y L2F para crear un nuevo estándar llamado L2TP. L2TP existe en el nivel de enlace del modelo OSI. L2TP, al igual que PPTP soporta clientes no IP, pero también da problemas al definir una encriptación estándar.

- Internet Protocol Security (IPsec): IPsec es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de red en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.

- VPN’s SSL: No existe un estándar para VPN’s SSL, sino varias implementaciones distintas y se destaca por su sencillez de configuración e implantación.

OpenVPN es una de las implementaciones más extendidas y la sencillez de su utilización la hace idónea para el desarrollo de este proyecto.

5.2.4.1 PROTOCOLOS IMPLEMENTADOS SOBRE CAPA 2

Point-to-Point Tunneling Protocol (PPTP):

El PPTP es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas del IP para transmisión sobre una red IP, como la de Internet. También se puede utilizar el PPTP en una red privada de LAN a LAN.

El PPTP se documenta en el RFC preliminar, "Protocolo de túnel de punto a punto" (pptp-draft-ietf - ppext - pptp - 02.txt). Este proyecto se presentó ante el IETF en junio de 1996 por parte de las compañías miembros del Foro PPTP incluyendo Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics y US Robotics (ahora 3Com).[3]

Protocolo de túnel de punto a punto (PPTP) utiliza una conexión TCP para mantenimiento del túnel y tramas del PPP encapsuladas de Encapsulación de enrutamiento genérico (GRE) para datos de túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas del PPP encapsulado. La Figura muestra la forma en que se ensambla el paquete del PPTP antes de la transmisión.

La figura 5.2 muestra un cliente de marcación que crea un túnel a través de una red. El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

[3] http://issuu.com/chonybmx/docs/mibetatest.blogspot.com/16

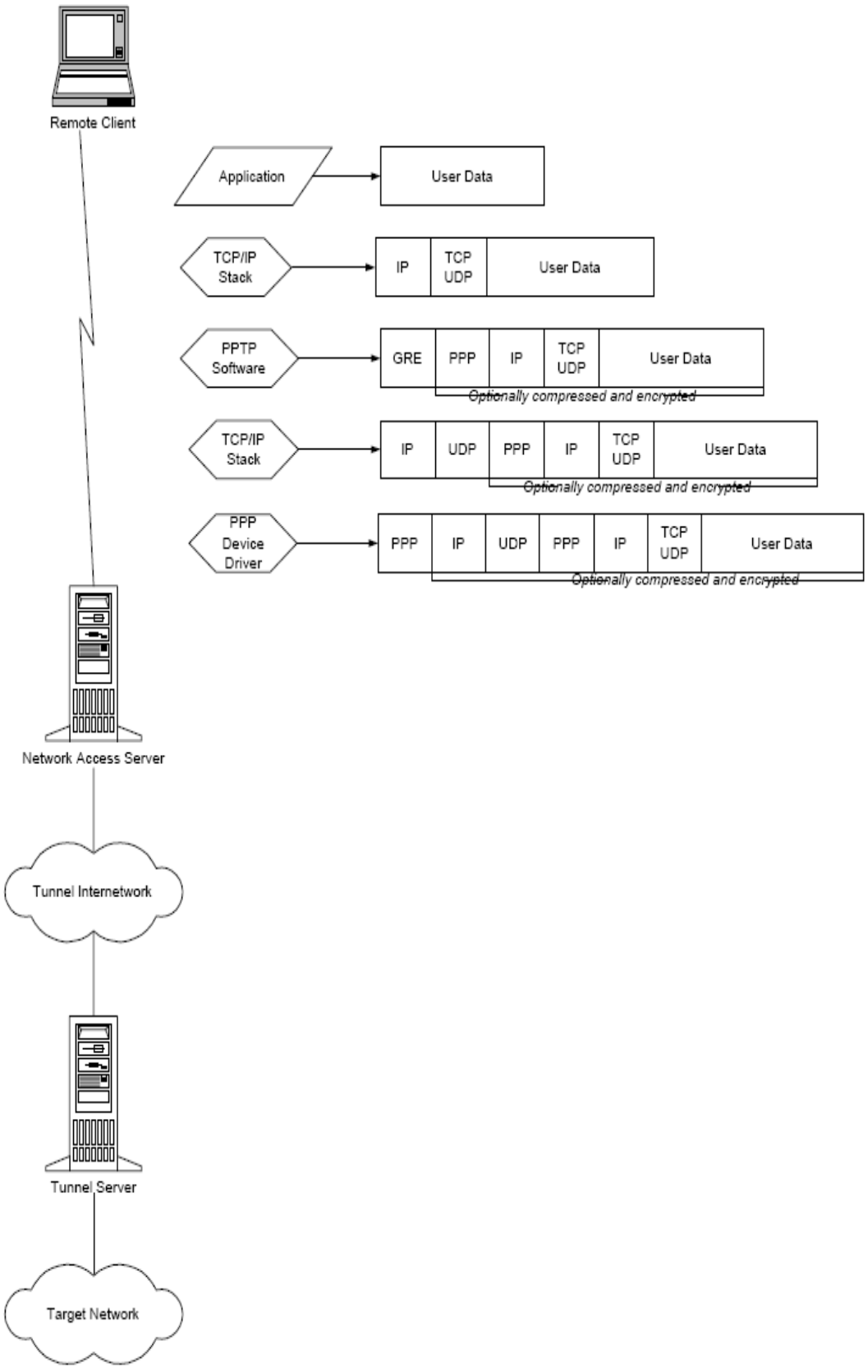

Fig. 5.2 Túnel utilizando el protocolo de túnel punto a punto (PPTP)

Layer Two Tunneling Protocol (L2TP):

L2TP es una combinación del PPTP y L2F. Sus diseñadores esperan que el L2TP represente las mejores funciones del PPTP y L2F.

L2TP es un protocolo de red que encapsula las tramas del PPP que se enviarán sobre redes IP, X.25, *Frame Relay* o Modo de transferencia asíncrona (ATM).

Cuando está configurado para utilizar al IP como su transporte de datagrama, L2TP se puede utilizar como un protocolo de túnel sobre Internet. También se puede utilizar al L2TP directamente sobre varios medios WAN (como *Frame Relay*) sin nivel de transporte IP.

El L2TP se documenta en el proyecto del RFC, el *Protocolo de túnel nivel 2 "L2TP"* (draft-ietf-pppext-l2tp-09.txt). Este documento se presentó al IETF en enero de 1998.[4]

El 2TP sobre las redes IP utilizan UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. El L2TP también utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas. La Figura 5.3 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

[4] http://issuu.com/chonybmx/docs/mibetatest.blogspot.com/16

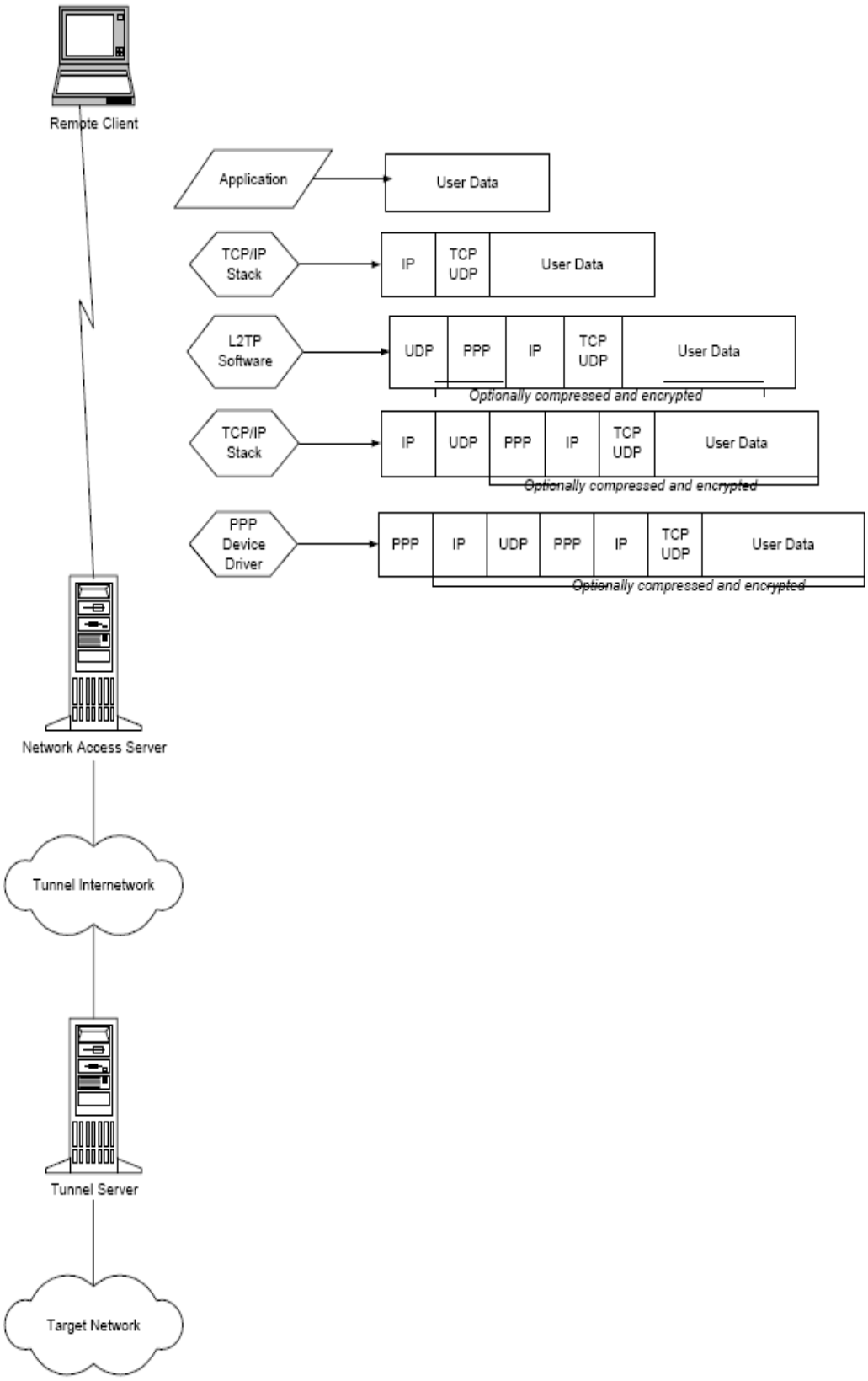

Fig. 5.3 Túnel utilizando el protocolo Layer Two Tunneling Protocol (L2TP)

5.2.4.2 PROTOCOLO IMPLEMENTADOS SOBRE CAPA 3

Internet Protocol Security (IPsec):

Modo del túnel de seguridad de protocolo para Internet (IPsec)

El IPSec es un estándar de protocolo de Nivel 3 que da soporte a la transferencia protegida de información a través de una red IP. En su conjunto se describe con mayor detalle en la sección de Seguridad avanzada más adelante. Sin embargo, hay un aspecto del IPSec que debe analizarse en el contexto de los protocolos de túnel. Además de su definición de mecanismos de encriptación para tráfico IP, IPSec define el formato de paquete para un modo de túnel IP sobre IP, generalmente referido como un *modo de túnel IPSec*. Un túnel IPSec consiste en un cliente de túnel y un servidor de túnel, ambos configurados para utilizar los túneles IPSec y un mecanismo negociado de encriptación.[5]

El modo del túnel del IPSec utiliza el método de seguridad negociada (de existir) para encapsular y encriptar todos los paquetes IP para una transferencia segura a través de una red privada o pública IP. Entonces, se vuelve a encapsular la carga útil encriptada con un encabezado IP de texto y se envía en la red para su entrega a un servidor de túnel. Al recibir este datagrama, el servidor del túnel procesa y descarta el encabezado IP de texto y luego desencripta su contenido para recuperar el paquete original IP de carga útil. Entonces, se procesa el paquete IP de carga útil de manera normal y se enruta su destino en la red objetivo. El modo de túnel IPSec tiene las siguientes funciones y limitaciones:

- Sólo da soporte a tráfico IP.

- Funciona en el fondo de la pila IP; por lo tanto, las aplicaciones y protocolos de niveles más altos heredan su comportamiento.

- Está controlado por una *política de seguridad*—un conjunto de reglas que se

[5] http://www.scribd.com/doc/3265245/Redes-Privadas-Virtuales-VPN-descripcion

cumplen a través de filtros. Esta política de seguridad establece los mecanismos de encriptación y de túnel disponibles en orden de preferencia y los métodos de autenticación disponibles, también en orden de preferencia.

- Tan pronto como existe tráfico, los dos equipos realizan una autenticación mutua, y luego negocian los métodos de encriptación que se utilizarán. En lo subsecuente, se encripta todo el tráfico utilizando el mecanismo negociado de encriptación y luego se envuelve en un encabezado de túnel.

Seguridad IP (IPSec)

La Seguridad de protocolo de Internet (IPSec) fue diseñada por el IETF (Internet Engineering Task Force, en castellano Grupo de Trabajo en Ingeniería de Internet) como un mecanismo de extremo a extremo para garantizar la seguridad de los datos en comunicaciones basadas en IP. Se ha definido a IPSec en una serie de RFCs, especialmente RFCs 1825, 1826 y 1827, las cuales definen la arquitectura global, un encabezado de autenticación para verificar la integridad de los datos, y Carga útil de seguridad de encapsulación tanto para la integridad de los datos como para la encriptación de los mismos.

La IPSec define dos funciones que aseguran la confidencialidad: encriptación de datos e integridad de datos. Como lo definió Internet Engineering Task Force, IPSec utiliza un Encabezado de autenticación (AH) para proporcionar la autenticación e integridad de la fuente sin encriptación, y la Carga útil de seguridad encapsulada (ESP) para proporcionar la autenticación y la integridad junto con la encriptación. Con la Seguridad IP, sólo el remitente y el receptor conocen las llaves de seguridad. Si los datos de autenticación son válidos, el receptor sabe que la comunicación provino del remitente, y que no se cambió en su tránsito.

Se puede considerar que IPSec es un nivel inferior a la pila TCP/IP. Este nivel está controlado por una política de seguridad en cada equipo y una asociación negociada de seguridad entre el remitente y el receptor. La política consiste en un conjunto de filtros y comportamientos de seguridad asociados. Si la dirección IP, el protocolo y el número de

puerto de un paquete corresponde con un filtro, entonces el paquete está sujeto al comportamiento de seguridad asociado.

5.2.4.3 PROTOCOLOS IMPLEMENTADOS SOBRE CAPA 7

También es posible establecer túneles en la capa de aplicación y de hecho son ampliamente utilizados hoy en día siendo algunas aproximaciones soluciones como SSL6 y TLS7. El usuario accede a la VPN de la organización a través de un browser iniciando la conexión en un sitio web seguro (HTTPS-Secured website).

Además, existen otros productos como SSL-Explorer y otros que ofrecen una combinación de gran flexibilidad, seguridad fuerte y facilidad de configuración. La seguridad es lograda mediante cifrado del tráfico usando mecanismos SSL/TLS, los cuales han probado ser muy seguros y están siendo constantemente sometidos a mejoras y pruebas.

Implementación OpenVPN

"OpenVPN es una excelente nueva solución para VPN que implementa conexiones de capa 2 o 3, usa los estándares de la industria SSL/TLS para cifrar y combina todos las características mencionadas anteriormente en las otras soluciones VPN. Su principal desventaja por el momento es que hay muy pocos fabricantes de hardware que lo integren en sus soluciones. De todos modos no hay que preocuparse siempre que contemos con un Linux en el cual podremos implementarlo sin ningún problema mediante software."

5.2.5 CLIENTES / SERVIDORES EN VPN

Un Servidor VPN normalmente es un componente hardware, aunque también lo puede ser software. Puede actuar como un gateway en una red o en un único computador. Debe estar siempre conectado y esperando a que clientes VPN se conecten a él. El software para el Servidor VPN es bastante frecuente.

Un Cliente VPN es en la mayoría de los casos un componente software, aunque puede ser también un componente hardware. Un cliente realiza una llamada al servidor y se conecta. Entonces la computadora cliente podrá comunicarse con el Servidor VPN, ya que ellos se encuentran en la misma red virtual. El software para un cliente VPN es bastante común. Cuando se carga en la computadora este software permite crear un túnel seguro VPN a través de Internet para poder comunicarse con el Servidor VPN.

5.2.6 VENTAJAS Y DESVENTAJAS

5.2.6.1 VENTAJAS

Las VPN proporcionan principalmente las siguientes ventajas:

Bajo coste de una VPN: Una forma de reducir coste en las VPN es eliminando la necesidad de largas líneas de coste elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio.

Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada local.

Escalabilidad de las VPN's: Las redes VPN evitan el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet.

5.2.6.2 DESVENTAJAS

Las VPN's contraen éstos inconvenientes:

Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones en su desarrollo.

Las VPN dependen de un área externa a la organización, Internet en particular, y por lo tanto depende de factores externos al control de la organización.

Las diferentes tecnologías de VPN podrían no trabajar bien juntas.

Las redes VPN necesitan diferentes protocolos que los de IP.

5.3 SEGURIDAD CON VPN

5.3.1 INTRODUCCIÓN

Sea cual fuere el sistema de conexión, no podemos olvidar que en esos ordenadores puede haber muchos elementos que no están controlados por los administradores de red y pueden no cumplir las políticas de seguridad establecidas en la empresa.

Y, lo que es peor, en muchos casos los usuarios de estos ordenadores desactivan las medidas de seguridad (antivirus, firewall, etc.) para obtener un mejor rendimiento. En poco tiempo, los códigos maliciosos se apoderan del sistema.
Cuando el ordenador infectado se conecta de nuevo a la red empresarial, bien sea a través de una conexión remota o directamente en la red de la oficina, el peligro de propagación de esos códigos maliciosos instalados en el ordenador es muy alto.

Al igual que los empleados que se desplazan, los tele-trabajadores también pueden ser un peligro. El tele-trabajo es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional en el domicilio del trabajador. Engloba una amplia gama de actividades, e implica el uso de ordenadores y la conexión permanente entre el trabajador y la empresa.

Otro peligro que suele plantearse es el problema de la posible intercepción de la comunicación entre la oficina y el tele-trabajador, o el empleado desplazado. La sola

posibilidad de que un hacker pudiera hacerse con, por ejemplo, un plan estratégico, haría temblar a los directivos de cualquier empresa.

No hay manera de evitar al 100% que una conexión sea interceptada, cualquier usuario de una comunicación (sea postal, telegráfica, e-mail, etc.) lo sabe. Por ello se establecen sistemas de cifrado que hagan incomprensible la información a aquellos que no están implicados. Gracias a estos sistemas, puede asegurarse que aunque alguien pueda llegar a acceder a los datos transmitidos, éstos van a ser ininteligibles.

Uno de los sistemas más utilizados por las empresas para garantizar el secreto de las comunicaciones con empleados remotos son las Redes privadas virtuales.
VPN tiene dos modos considerados seguros, uno basado en claves estáticas precompartidas y otro en SSL/TLS usando certificados y claves RSA.
Cuando ambos lados usan la misma clave para encriptar y desencriptar los datos, estamos usando el mecanismo conocido como "clave simétrica" y dicha clave debe ser instalada en todas las máquinas que tomarán parte en la conexión VPN.
Si bien SSL/TLS + claves RSA es por lejos la opción más segura, las claves estáticas cuentan con la ventaja de la simplicidad.

5.3.2 ENCRIPTACIÓN DE TRÁFICO

5.3.2.1 ENCRIPTACIÓN SIMÉTRICA

Cualquiera que posea la clave podrá desencriptar el tráfico, por lo que si un atacante la obtuviese comprometería el tráfico completo de la organización ya que tomaría parte como un integrante más de la VPN.[6]

[6] http://es.wikibooks.org/wiki/OpenVPN/Marco_Te%C3%B3rico

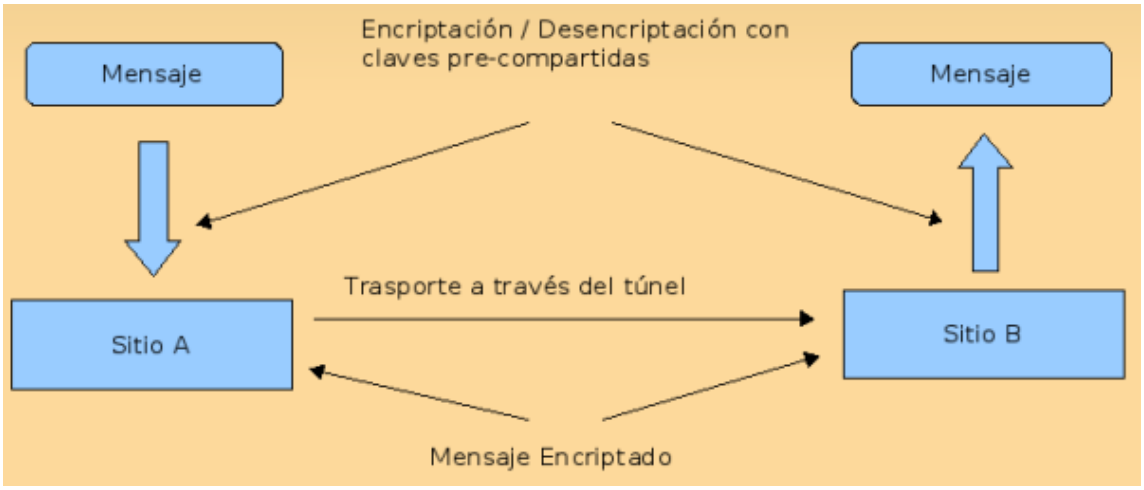

Fig. 5.4 Encriptación / Desencriptacion con claves pre-compartidas

Es por ello que mecanismos como IPsec cambian las claves cada cierto período de tiempo asociando a las mismas ciertos períodos de tiempo de validez llamados "tiempo de vida" o "lifetime". Una buena combinación de tiempo de vida y largo de la clave asegurarán que un atacante no pueda desencriptar la clave a tiempo, haciendo que cuando finalmente la obtenga (porque lo hará), ya no le sirva por estar fuera de vigencia. IPSec utiliza su propio protocolo para intercambiar claves llamado IKE9 que ha sido desarrollado desde mediados de los noventa y aun no ha sido terminado.

5.3.2.2 ENCRIPTACIÓN ASIMÉTRICA CON SSL/TLS

SSL/TLS usa una de las mejores tecnologías de encriptación para asegurar la identidad de los integrantes de la VPN.

Cada integrante tiene dos claves, una pública y otra privada.

La pública es distribuida y usada por cualquiera para encriptar los datos que serán enviados a la contraparte quien conoce la clave privada que es la única que sirve para desencriptar los datos. El par de clave pública/privada es generado a partir de algoritmos matemáticos que aseguran que solo con la clave privada es posible leer los datos originales. El día que alguien encuentre algún defecto a ese algoritmo, todos aquellos conectados a Internet estarán comprometidos en forma instantánea.[7]

[7] http://es.wikibooks.org/wiki/OpenVPN/Marco_Te%C3%B3rico

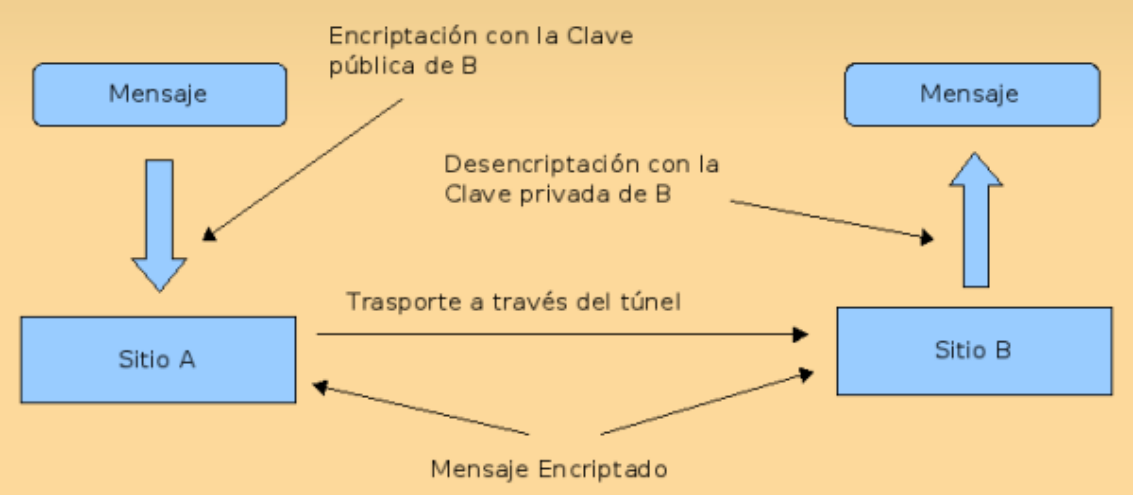

Fig. 5.5 Encriptación Asimétrica con SSL/TLS (claves públicas)

Es de destacar que la clave privada debe permanecer secreta mientras que la clave pública debe ser intercambiada para que nos puedan enviar mensajes.

El protocolo SSL

Fue originalmente diseñado por Netscape para establecer comunicaciones seguras con protocolos como HTTP o FTP. Permite negociar qué algoritmos se van a emplear, intercambiar las claves de encriptación y la autentificación de clientes y servidores.

Existen tres versiones del protocolo, la cuarta es una mejora del SSLv3 y se conoce con el nombre de TLS, que es la especificación que vamos a estudiar.

El protocolo TLS

El protocolo TLS (*Transport Layer Security*) es una evolución del protocolo SSL (*Secure Sockets Layer*).

Los objetivos del protocolo son varios:

1. **Seguridad criptográfica**. El protocolo se debe emplear para establecer una conexión segura entre dos partes.

2. **Interoperabilidad**. Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.

3. **Extensibilidad**. El protocolo permite la incorporación de nuevos algoritmos criptográficos.

4. **Eficiencia**. Los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de *cache de sesiones* para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

El protocolo está dividido en dos niveles:

- **Protocolo de registro TLS** (*TLS Record Protocol*).
- **Protocolo de mutuo acuerdo TLS** (*TLS Handshake Protocol*).

El de más bajo nivel es el *Protocolo de Registro*, que se implementa sobre un protocolo de transporte fiable como el TCP. El protocolo proporciona seguridad en la conexión con dos propiedades fundamentales:

1. **La conexión es privada**. Para encriptar los datos se usan algoritmos de cifrado simétrico. Las claves se generan para cada conexión y se basan en un secreto negociado por otro protocolo (como el de mutuo acuerdo). El protocolo también se puede usar sin encriptación.

2. **La conexión es fiable**. El transporte de mensajes incluye una verificación de integridad.

El *protocolo de registro* se emplea para encapsular varios protocolos de más alto nivel, uno de ellos, el *protocolo de mutuo acuerdo*, permite al servidor y al cliente autentificarse mutuamente y negociar un algoritmo de encriptación y sus claves antes de que el protocolo de aplicación transmita o reciba datos.
El *protocolo de mutuo acuerdo* proporciona seguridad en la conexión con tres propiedades básicas:

1. La identidad del interlocutor puede ser autentificada usando criptografía de clave pública. Esta autentificación puede ser opcional, pero generalmente es necesaria al menos para uno de los interlocutores.

2. La negociación de un secreto compartido es segura.

3. La negociación es fiable, nadie puede modificar la negociación sin ser detectado por los interlocutores.

El protocolo de registro TLS

El protocolo de registro TLS es un protocolo por capas. En cada nivel los mensajes incluyen campos para el tamaño, descripción y contenido. El protocolo toma un mensaje para ser transmitido, lo divide en bloques, comprime los datos (opcionalmente), los encripta, genera un MAC y transmite el resultado.

En el lado del receptor se sigue un proceso inverso: descifrado, verificación, descompresión y reensamblaje.

El estándar describe cuatro clientes del protocolo:
1. El protocolo de mutuo acuerdo
2. El protocolo de alerta
3. El protocolo de cambio de especificaciones criptográficas
4. El protocolo de datos de aplicación

El protocolo de mutuo acuerdo TLS

El protocolo consta de tres subprotocolos que se emplean para permitir que los interlocutores lleguen a un acuerdo respecto a los parámetros de seguridad para el nivel de registro, se autentifiquen, instancien parámetros de seguridad negociados y se comuniquen condiciones de error.
El protocolo es responsable de negociar una sesión que consta de los siguientes ítems:

1. **Identificador de sesión**. Secuencia de bytes aleatoria elegida por el servidor para identificar el estado de una sesión activa o reanudable.

2. **Certificado del interlocutor**. Certificado X.509 v3 del interlocutor. Este elemento puede ser nulo.

3. **Método de compresión**. Algoritmo empleado para comprimir los datos antes de encriptarlos.

4. **Especificaciones del algoritmo de encriptación**. Especifica el algoritmo de encriptación (nulo, DES, etc.) y el algoritmo de firmado (MD5 o SHA). También define atributos criptográficos como el tamaño de la clave de la función de dispersión.

5. **Secreto principal**. Clave secreta de 48 bytes compartida entre el cliente y el servidor.

6. **Reutilizable**. Valor que indica si la sesión puede ser empleada para iniciar nuevas conexiones.

Protocolo de cambio de especificaciones criptográficas

Este protocolo marca las transiciones entre distintas estrategias de cifrado. Consta de un mensaje que se encripta y comprime con las especificaciones actuales de la conexión (no las pendientes).

Cuando el destinatario recibe este mensaje la capa de registro copia el estado de lectura pendiente al estado de lectura actual. De forma similar, el emisor cambia su estado de escritura al enviar este mensaje.

Este mensaje se envía durante el acuerdo, después de haber acordado los parámetros de seguridad pero antes de que se envíe el mensaje de verificación finalizada.

Protocolo de alerta

Uno de los tipos de mensaje que soporta la capa de registro es el de alerta. Estos mensajes incluyen la severidad de la alerta y una descripción de la misma. Los mensajes de alerta con nivel de fatal provocan la inmediata terminación de la comunicación.

Existen distintos tipos de alertas:

- **Alerta de cierre**. El cliente y el servidor deben saber que la conexión se está cerrando para evitar un ataque de truncado. Cualquiera de los dos puede iniciar el intercambio de mensajes de cierre. Cualquier información recibida después de la alerta de cierre es ignorada.

- **Alerta de error**. La gestión de errores en el protocolo de mutuo acuerdo es muy simple, cuando uno de los interlocutores detecta un error lo envía al otro y, si se trata de un error fatal, cierran la conexión.

Protocolo de mutuo acuerdo

Los parámetros del estado de la sesión son producidos por este protocolo, que opera sobre el protocolo de registro TLS. Cuando un cliente y un servidor empiezan a comunicarse, acuerdan la versión del protocolo, selección de algoritmos criptográficos, opcionalmente se autentifican mutuamente y emplean algoritmos de clave pública para generar secretos compartidos.

El protocolo de mutuo acuerdo consta de los siguientes pasos:

1. Intercambio de *mensajes de saludo* (*hello messages*) para acordar los algoritmos a emplear, intercambiar valores aleatorios y verificar si es una sesión reanudada.

2. Intercambiar los parámetros criptográficos necesarios para permitir que el cliente y el servidor acuerden un pre-secreto.

3. Intercambio de certificados e información criptográfica para permitir que cliente y servidor se autentifiquen.

4. Generar un secreto principal a partir del pre-secreto e intercambiar valores aleatorios.

5. Proporcionar los parámetros de seguridad a la capa de registro.

6. Permitir al cliente y al servidor verificar que su interlocutor ha calculado los mismos parámetros de seguridad y que el acuerdo se produjo sin alteraciones por parte de un tercero.

Protocolo de datos de aplicación

Los mensajes de datos de la aplicación son transportados por la capa de registro y son fragmentados, comprimidos y encriptados basándose en el estado actual de la conexión. Los mensajes se tratan como datos transparentes para la capa de registro.

Aplicaciones e implementaciones

El protocolo SSL/TLS tiene multitud de aplicaciones en uso actualmente. La mayoría de ellas 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, etc.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución. Una de las más populares es la biblioteca **openssl**, escrita en C y disponible bajo licencia GNU. Incluye todas las versiones del SSL y el TLS y un gran número de algoritmos criptográficos, algunos de los cuales ni tan sólo son empleados en el estándar TLS. La biblioteca está disponible en el URL http://www.openssl.org. En esa misma dirección se puede encontrar una lista de referencias a otras implementaciones gratuitas y comerciales de los protocolos SSL y TLS y aplicaciones que los emplean.

5.4 OPENVPN

5.4.1 INTRODUCCIÓN

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo la licencia GPL, de software libre.

OpenVPN, es un excelente producto de software creado por James Yonan en el año 2001 y que ha estado siendo mejorado desde entonces.

Ninguna otra solución ofrece una mezcla semejante de seguridad a nivel empresarial, seguridad, usabilidad y riqueza de características.

Es una solución multiplataforma que ha simplificado mucho la configuración de VPN's dejando atrás los tiempos de otras soluciones difíciles de configurar como IPsec y haciéndola más accesible para gente inexperta en este tipo de tecnología.
Supongamos que necesitamos comunicar diferentes sucursales de una organización. A continuación veremos algunas soluciones que se han ofrecido como respuesta a este tipo de necesidades.

En el pasado las comunicaciones se realizaban por correo, teléfono o fax. Hoy en día hay factores que hacen necesaria la implementación de soluciones más sofisticadas de conectividad entre las oficinas de las organizaciones a lo largo del mundo.

Dichos factores son:

- La aceleración de los procesos de negocios y su consecuente aumento en la necesidad de intercambio flexible y rápido de información.

- Muchas organizaciones tienen varias sucursales en diferentes ubicaciones así como

también tele trabajadores remotos desde sus casas, quienes necesitan intercambiar información sin ninguna demora, como si estuvieran físicamente juntos.

La necesidad de las redes de computación de cumplir altos estándares de seguridad que aseguren la autenticidad, integridad y disponibilidad[8]

5.4.2 VENTAJAS Y DESVENTAJAS DE OPENVPN

5.4.2.1 VENTAJAS

OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de IPsec.

Además ofrece ventajas que van más allá que cualquier otra solución como ser:

- Posibilidad de implementar dos modos básicos en capa 2 o capa 3 con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).

- Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aun cuando no es un equipo de la red local. Por otra parte, solo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.

- Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.

- Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).

- Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que

[8] http://es.wikipedia.org/wiki/OpenVPN

desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.

- Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.

- Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.
- Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.

- Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.

- Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.

Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso son increíblemente simples.

Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.

5.4.2.2 DESVENTAJAS

Entre las desventajas podríamos citar las siguientes:

- No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.
- Falta de masa crítica.
- Todavía existe poca gente que conoce cómo usar OpenVPN.
- Actualmente sólo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

5.4.3 COMPARACIÓN ENTRE OPENVPN E IPSEC VPN

Tabla 5.1 Comparación entre OpenVPN e IPsec VPN

IPsec	OpenVPN
Estándar de la tecnología VPN	Aún desconocida y no compatible con IPsec
Plataformas de hardware (dispositivos, aparatos)	Solo en computadoras, pero en todos los sistemas operativos disponibles
Tecnología conocida y probada	Tecnología nueva y aún en crecimiento
Muchas interfaces gráficas disponibles	Sin interfaces gráficas profesionales, aunque ya existen algunos proyectos prometedores
Modificación compleja del stack IP	Tecnología sencilla
Necesidad de modificaciones críticas al kernel	Interfaces de red y paquetes estandarizados
Necesidad de permisos de administrador	Ejecuta en el espacio del usuario y puede ser chroot-ed
Diferentes implementaciones de distintos proveedores pueden ser incompatibles entre si	Tecnologías de cifrado estandarizadas
Configuración compleja y tecnología compleja	Facilidad, buena estructuración, tecnología modular y facilidad de configuración
Curva de aprendizaje muy pronunciada	Fácil de aprender y éxito rápido para principiantes
Necesidad de uso de muchos puertos y protocolos en el firewall	Utiliza solo un puerto del firewall
Problemas con direcciones dinámicas en	Trabaja con servidores de nombres dinámicos

ambas puntas	como DynDNS o No-IP con reconecciones rápidas y transparentes
Problemas de seguridad de las tecnologías IPsec	SSL/TLS como estándar de criptografía

Además citamos algunas otras ventajas de OpenVPN sobre IPSec:

- Control de tráfico (Traffic shaping)
- Velocidad (más de 20 Mbps en máquinas de 1Ghz)
- Compatibilidad con firewall y proxies
- Ningún problema con NAT (ambos lados puede ser redes NATeadas)
- Posibilidades para hackers y road warriors

5.5 SERVIDOR VPN

5.5.1 INTRODUCCIÓN

OpenVPN es una implementación de VPN SSL la cual usa las extensiones OSI capa 2 ó 3 para asegurar redes la cual usa los protocolos SSL/TLS, soporta diferentes medios de autenticación como certificados, smart cards, y/o usuarios/contraseñas, y permite políticas de control de acceso para usuarios o grupos usando reglas de firewall aplicadas a las interfaces virtuales de la VPN. OpenVPN 2.0 permite conectar múltiples clientes a un solo servidor (proceso) OpenVPN sobre un simple puerto TCP o UDP.[9]

5.5.2 INSTALACIÓN DEL OPENVPN

Instalar OpenVPN en nuestro Linux CentOS es realmente fácil. Solamente debemos tener instalado el repositorio DAG y emitir el comando:

```
yum install openvpn
```

[9] http://es.wikipedia.org/wiki/OpenVPN

Después de unos minutos, tendremos listo el paquete de OpenVPN

```
yum –y install openvpn
```

Una vez instalado, podemos proceder a la creación de las claves de encriptación en el servidor y cliente.

5.5.3 ACTIVANDO OPENVPN

Aunque **todavía no es el momento de activarlo**, cuando hayamos configurado el OpenVPN podemos activarlo con:

```
service openvpn start
chkconfig openvpn on
```

Con estos dos simples comandos podemos arrancar el OpenVPN en ambos extremos.
Si necesitáramos reiniciarlo (para que lea de nuevo la configuración) podríamos hacerlo con:

```
service openvpn restart
```

5.5.4 FORMAS DE CONEXIÓN

5.5.4.1 HOST A HOST

Es el método más simple, nos permite encriptar la comunicación entre dos PC las cuales deberán solamente tener conexión; es decir: ambas PC deben poderse enviar paquetes directamente ya sea porque estén conectadas en la misma red local, o porque ambas estén conectadas al internet y sean alcanzables entre sí.

Generación de clave de encriptación.

En el caso de una conexión host a host, podemos sencillamente generar una clave compartida en el servidor, y copiarla hacia el cliente. Con esta clave se encriptarían los datos sin mayor problema o inconveniente:

```
openvpn --genkey --secret secret.key
```

Este archivo "secret.key" tiene que ser copiado hacia el directorio /etc/openvpn del cliente y del servidor.

```
cp secret.key /etc/openvpn
scp secret.key IPDELSERVIDOR:/etc/openvpn/
```

Configuración Host a Host

En la configuración host a host, lo que lograremos es que el intercambio de paquetes entre dos máquinas se realice de forma encriptada.

Para esto, crearemos una interfaz virtual con una IP privada en cada extremo:

* 10.8.0.1 para el servidor.
* 10.8.0.2 para el cliente

Y cualquier paquete que circule entre el cliente y el servidor vía esas direcciones IP, viajará encriptado.

Configuración del servidor

El archivo */etc/openvpn/server.conf* lo podemos dejar de la siguiente forma:

```
# dispositivo de tunel
dev tun
# usamos: ifconfig ipdelserver ipdelcliente
ifconfig 10.8.0.1 10.8.0.2

# Clave del servidor
secret /etc/openvpn/secret.key
#puerto
```

```
port 1194

#usuario bajo el cual ejecutaremos
user nobody
group nobody

# opciones, comprimir con lzo, ping cada 15 segs, verbose 1 (bajo)
comp-lzo
ping 15
verb 4
```

En este caso lo fundamental es que estamos indicándole al servidor que escuche en su puerto usuario (1194/udp) y que la IP que tomará la interfaz de VPN (tun) será 10.8.0.1 y le dará al cliente la 10.8.0.2

Configuración del cliente

Antes de configurar el cliente, en este caso el cliente 1, debemos traer del servidor los archivos */etc/openvpn/secret.key* hacia el directorio */etc/openvpn* del cliente. Sugiero traerlo con el comando scp

```
scp IPDELSERVIDOR:/etc/openvpn/secret.key /etc/openvpn
```

El archivo */etc/openvpn/client1.conf* quedaría como sigue:

```
# IP publica del servidor, poner IP real de su servidor!
remote 200.100.50.25

# puerto
port 1194

# dispositivo tunel
dev tun

# usamos ifconfig ipdelcliente ipdelservidor
```

```
tun-mtu 1500
ifconfig 10.8.0.2 10.8.0.1



# clave privada, client1.key para éste ejemplo, recuerde cada usuario debe
#tener su propia .key generada. El ejemplo de win esta comentado.
#secret "c:\program files\company branded vpn\config\key.txt"
secret /etc/openvpn/secret.key

# ping cada 10 segs
ping 10

# compresión lzo
comp-lzo

# verbose moderado, callar más de 10 mensajes iguales
verb 4
mute 10
```

Probando el enlace

Tanto en el cliente como en el servidor ponemos:

```
service openvpn start
chkconfig  openvpn on
```

Podemos verificar en */var/log/messages* que todo haya ido ok.

Una vez levantemos los demonios en ambos lados, podemos hacer ping hacia la interfaz tun (10.8.0.1 en el servidor ó 10.8.0.2 en el cliente):

desde el servidor:

ping 10.8.0.2

desde el cliente:

ping 10.8.0.1

Si el ping responde, todo está bien. Sino sugerimos revisar en /var/log/messages para verificar porque no funciona.

5.5.4.2 ROAD WARRIOR

Es una de las formas más utilizadas. Es el permitir que una máquina de alguien que esté fuera de nuestra red (de forma temporal o permanente) pueda comunicarse con el servidor OpenVPN de nuestra red y una vez autenticado pueda entrar a ver y acceder los recursos de nuestra red local.

Consideraciones preliminares

En el servidor OpenVPN necesitamos crear una serie de claves y certificados iniciales, para poder autenticar y encriptar la información que transitará desde/hacia el servidor/clientes

Contamos con una serie de scripts en el directorio /usr/share/doc/openvpn-2*/easy-rsa los cuales nos ayudarán mucho a ejecutar ésta tarea inicial.

Como primer paso, sugerimos copiar ese directorio (easy-rsa) hacia /etc/openvpn y cambiarnos a ese directorio:

```
cp -a /usr/share/doc/openvpn-2*/easy-rsa /etc/openvpn
cd /etc/openvpn/easy-rsa
```

Creando el CA

Una vez dentro de éste directorio procedemos a ejecutar los siguientes pasos:

```
. vars
sh clean-all
sh build-ca
```

Con ellos lo que haremos es:

- Inicializar variables de ambiente para poder trabajar con los siguientes scripts de shell para generar las variables

- Inicializar el directorio de las claves (borrando potenciales archivos viejos)
- build-ca: procedemos a generar el certificado CA

En éste último paso se nos pedirá una serie de información sobre nuestra red/empresa que debemos llenar lo más fielmente posible:

```
Generating a 1024 bit RSA private key
.....
.....+++++++.....+++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:EC
State or Province Name (full name) [NA]:LOJA
Locality Name (eg, city) [BISHKEK]:Loja
Organization Name (eg, company) [OpenVPN-TEST]:UNL
Organizational Unit Name (eg, section) []:JefaturaInformatica
Common Name (eg, your name or your server's hostname) []:redes
Email Address [me@myhost.mydomain]:marco@unl.edu.ec
```

La variable que debemos explícitamente llenar (no dejar en blanco) es: Common Name.

Generación del certificado y de la clave de encriptación para el servidor

Siguiente a la generación del Certificado de autoridad, procedemos a crear el certificado del servidor y de su clave de encriptación:

```
sh build-key-server server
Generating a 1024 bit RSA private key
```

.....++++++

.....++++++

writing new private key to 'server.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [KG]:EC

State or Province Name (full name) [NA]:LOJA

Locality Name (eg, city) [BISHKEK]:Loja

Organization Name (eg, company) [OpenVPN-TEST]:UNL

Organizational Unit Name (eg, section) []:JefaturaInformatica

Common Name (eg, your name or your server's hostname) []:server

[me@myhost.mydomain]:info@ecuaLinux.com Please enter the following 'extra'

attributes to be sent with your certificate request A challenge password []: An optional

company name []: Using configuration from /etc/openvpn/easy-rsa/openssl.cnf Check

that the request matches the signature Signature ok The Subject's Distinguished Name is

as follows countryName :PRINTABLE:'EC' stateOrProvinceName

:PRINTABLE:'LOJA' localityName :PRINTABLE:'Loja' organizationName

:PRINTABLE:'EcuaLinux' organizationalUnitName:PRINTABLE:'IT' commonName

:PRINTABLE:'server' emailAddress :IA5STRING:'marcoxvaiunl.edu.ec' The

stateOrProvinceName field needed to be the same in the CA certificate

(LOJA) and the request (LOJA)

En éste paso, también se nos pedirá nuevamente información sobre el certificado propio del servidor. En éste caso por favor, escoger en Common Name un nombre diferente al anteriormente escogido. En nuestro caso escogimos: server

Este paso nos generará dos archivos en el directorio */etc/openvpn/easy-rsa/keys/* que se copiarán dentro del mismo servidor hacia /etc/openvpn, ellos son:

- *server.crt*
- *server.key*

Generando certificados y claves privadas para los clientes

Cada cliente debe tener su propio certificado y clave de seguridad, para cara cliente que tengamos deberemos repetir el siguiente paso. **Los archivos obtenidos debemos copiarlos hacia el directorio /etc/openvpn/ de los clientes!**

En el caso de que nuestros clientes sean en Windows, debemos copiarlos hacia c:\program files\openvpn\

Para generar el certificado y claves privadas ejecutamos en nuestro servidor, dentro del directorio */etc/openvpn/easy-rsa/*

```
sh build-key client1

Generating a 1024 bit RSA private key

.....++++++

.....++++++

writing new private key to 'client1.key'

-----

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
```

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [KG]:EC

State or Province Name (full name) [NA]:LOJA

Locality Name (eg, city) [BISHKEK]:Loja

Organization Name (eg, company) [OpenVPN-TEST]:UNL

Organizational Unit Name (eg, section) []:JefaturaInformatica

Common Name (eg, your name or your server's hostname) []:client1

Email Address [me@myhost.mydomain]:cliente1@unl.edu.ec

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /etc/openvpn/easy-rsa/openssl.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName :PRINTABLE:'EC'

stateOrProvinceName :PRINTABLE:'LOJA'

localityName :PRINTABLE:'Loja'

organizationName :PRINTABLE:'UNL'

organizationalUnitName:PRINTABLE:'IT'

commonName :PRINTABLE:'client1'

emailAddress :IA5STRING:'cliente1@unl.edu.ec'

Certificate is to be certified until Nov 24 05:25:40 2016 GMT (3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

En el ejemplo anterior generamos la clave y el certificado para un cliente llamado **client1.**

Debemos hacer notar que al ejecutar el programa sh build-key, le pasamos como parámetro el nombre del cliente (client1 en el ejemplo anterior) el cual debe ser diferente para cada cliente. En el common name ponemos el nombre del cliente (client1 en éste ejemplo) tal y como le pasamos de parámetro.

Se pueden generar tantas claves como sean necesarias:

```
sh build-key client2

sh build-key client3
```

Ésto nos generará dos claves y certificados más, para client2 y client3, por favor, en common name debemos poner **client2** ó **client3** para cada caso.

Generando parámetros de Diffie-Hellman

El parámetro de Diffie-Hellman debemos generarlo así:

```
sh build-dh

Generating DH parameters, 1024 bit long safe prime, generator 2

This is going to take a long time

.....+.....+.....
```

Archivos a copiar al servidor

Hacia el directorio /etc/openvpn del servidor copiamos los siguientes archivos:

- ca.crt
- ca.key
- server.key
- server.crt

- dh1024.pem

Estos archivos están presentes en: */etc/openvpn/easy-rsa/keys*

Archivos a copiar al cliente

Hacia el directorio /etc/openvpn de cada cliente copiamos los siguientes archivos:

- ca.crt
- client**X**.crt
- client**X**.key

Tenga en cuenta que **X** es un número que se corresponde con el cliente (para el cliente 2 sería: client2.crt y client2.key por ejemplo).

Estos 3 archivos deben copiarse de forma segura hacia el cliente, quizá mediante scp o algún medio magnético seguro. No deben enviarse por mail puesto que contienen la clave (.key) de encriptación del cliente.

Estos archivos están presentes en: */etc/openvpn/easy-rsa/keys* **del servidor**.

Para la configuración en modo roadwarrior las configuraciones del cliente y el servidor varían un poco:

Configuración del servidor:

El archivo */etc/openvpn/server.conf* quedará así:

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
#Direcciones que se asignaran a los
#clientes, el server es .1
server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt
```

```
#Ruta para que los clientes alcancen la red local del server (32.0/20)
push "route 172.16.32.0 255.255.240.0"
keepalive 10 120
comp-lzo
user nobody
group nobody
persist-key
persist-tun
status openvpn-status.log
verb 4
```

Como podemos ver, hay nuevos parámetros, los más importantes son:

- un **push** de la ruta hacia la red local interna del servidor. Esa ruta estática permitirá que el road warrior vea a las máquinas de la red interna
- **server**: Indica el rango de direcciones que se asignará a los clientes que se conecten, deben ser direcciones no similares a las de la red local.

Configuración del cliente:

En el caso del cliente, así quedaría el archivo de configuración:

```
client
dev tun
proto udp
remote 192.188.49.5 1194
resolv-retry infinite
nobind
#Las dos siguientes opciones no van en Windows
#user nobody
#group nobody

persist-key
```

```
persist-tun
ca ca.crt
cert client1.crt
key client1.key
comp-lzo
verb 4
```

Las configuraciones más interesantes son:

- **Client**: indica que algunas configuraciones las tomará del servidor.
- **nobind**: que no actúe como servidor, que solamente vaya como cliente.
- **Recordar que cert y key deben ser únicas para cada cliente**

El orden en que van los parámetros no importa, el OpenVPN es muy noble en el cómo pones los parámetros.

5.5.4.3 RED A RED

Uno de los métodos más usados. Mediante ésta forma dos redes separadas en el espacio pueden comunicarse como si estuvieran unidas por un cable virtual (de ahi la V de VPN); la comunicación entre ambas redes viajará encriptada una vez salgan de los Servidores de OpenVPN y hasta que lleguen a su otro extremo.

OpenVPN y su relación con iptables

Hay que habilitar el tráfico hacia las interfaces TUN/TAP pues sino no se conectan las máquinas.
Agregar estas líneas en el servidor (quizá en el cliente también en el caso de que no se establezca la conexión):

```
iptables -A INPUT -i tun+ -j ACCEPT

iptables -A FORWARD -i tun+ -j ACCEPT

iptables -A INPUT -i tap+ -j ACCEPT

iptables -A FORWARD -i tap+ -j ACCEPT

iptables -A INPUT -p udp --dport 1194 -j ACCEPT
```

Con ellas lo que logras es abrir el puerto 1194/UDP para que entre la conexión de los clientes. Y además aceptar conexiones tun/tap. Aunque realmente con las tun basta pues son las que usamos en estos ejemplos.

5.5.5 OPENVPN Y WINDOWS

OpenVPN puede trabajar tanto como cliente o como servidor en máquinas Windows y Linux. Es decir puede quedar cualquier combinación: Windows Windows, Windows Linux, Linux Windows o la mejor: Linux-Linux.

La mejor opción es Linux-Linux pues tenemos más herramientas para trabajar y verificar. Una solución es, una vez configurado bien un cliente en Linux, mover los archivos de /etc/openvpn hacia la máquina de Windows
En el caso de Windows los archivos de configuración deben ir en c:\program files\openvpn\config

Se sugiere que una vez movidos los archivos de configuración de cliente Linux al cliente Windows, borrar estos archivos del cliente Linux.

Recordemos que los archivos de configuración y claves deben ser particulares para cada cliente, no debe usarse en dos clientes, por eso es necesario borrarlos del cliente Linux.

En el caso de Windows hay dos parámetros de configuración que no aplican y no se pueden poner en las configuraciones son:

- User
- Group

Ellos dos permiten degradar los privilegios a un usuario diferente del de administrador, pero en Windows esto no se puede hacer, openvpn corre como administrador.

5.5.6 OPENVPN GUI FOR WINDOWS

5.5.6.1 INTRODUCCIÓN

OpenVPN es una solución completamente equipada SSL VPN que puede dar cabida a una amplia gama de configuraciones, incluyendo acceso remoto, sitio a sitio VPN, Wi-Fi de seguridad, y de la empresa escala de soluciones de acceso remoto con balanceo de carga, failover, y de grano fino de acceso -controles.[10]

OpenVPN normalmente se ejecuta en una ventana de consola, que puede ser un poco molesto que se extiende en la barra de tareas todo el tiempo. OpenVPN GUI le permite ejecutar OpenVPN sin la ventana de consola. En lugar de obtener un icono en el área de notificación (el área en la parte derecha de la barra de tareas) a partir de la cual se puede controlar OpenVPN para iniciar / detener sus túneles VPN, ver el registro, cambiar las contraseña y otras cosas útiles.

OpenVPN GUI es un proyecto Open Source y está licenciado bajo GPL.

Última versión estable: **1.0.3** con OpenVPN 2.0.9 (2006-10-17)

[10] http://blog.bitcomet.com/indagator/post_77373/

El desarrollo más reciente edición: **1.0.3** con OpenVPN 2.1_beta7 (2005-12-03)

5.5.6.2 CARACTERÍSTICAS EN OPENVPN GUI

Entre las características podremos citar las siguientes:

- Permite mostrar un icono en el área de notificación a partir de la cual usted puede controlar OpenVPN.
- Admite manejar múltiples conexiones simultáneas.
- Oculta la ventana de la consola.
- Es un visor de archivos de registro.
- Permite editar las configuraciones (con un texteditor).
- Tiene la opción Start / Stop / Reinicie el Servicio OpenVPN.
- Proporciona diálogos para introducir la contraseña de clave privada.
- Pone a disposición el diálogo para introducir nombre de usuario / contraseña de autenticación de credenciales
- Soporta cambiar la contraseña utilizada para proteger la clave privada (Ambos PEM y PKCS # 12 archivos).
- Se puede configurar proxy de la GUI.
- Utilizar Internet Explorer proxy (sólo en caso de configurar manualmente en IE).
- Ejecutar un archivo por lotes antes / después de conectar y antes de desconectar.
- Cmd-line que es una opción para una conexión automática en el inicio (- conectar).
- Cmd-line op
- ciones para anular la configuración del Registro.
- Mostrar la información de conexión en el icono de cuadro de herramientas.

5.5.6.3 REQUISITOS DEL SISTEMA

OpenVPN GUI está escrito en C puro Win32 código, por lo que no requiere ningún tiempo de ejecución de library's a trabajar. Es un solo archivo .exe (unos 100kb).

Entre algunas de las versiones de este software encontramos:

- OpenVPN 1.5 o superior. (Podría funcionar con las versiones anteriores, pero esto no se ha probado)
- OpenVPN 2.0 beta6 o superior para apoyar múltiples conexiones simultáneas.
- OpenVPN 2.0 beta11 o superior para mostrar el "Conectado" msg sólo después de las rutas se han añadido al sistema.

6. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN

La Universidad Nacional de Loja, ofrece una formación que se realiza en base a una investigación científico–técnica sobre los problemas del entorno de nuestra realidad, con calidad, pertinencia y equidad, a fin de coadyuvar al desarrollo sustentable de la Región Sur y del país, interactuando con la comunidad, generando propuestas alternativas a los problemas nacionales, con responsabilidad social; reconociendo y promoviendo la diversidad cultural y étnica, apoyándose en el avance científico y tecnológico, en procura de mejorar la calidad de vida del pueblo ecuatoriano y en especial de la Región Sur del País, es decir su misión se inspira en los ideales de la democracia y la justicia social, y propiciará la paz y la solidaridad humana, contribuyendo a la superación de la sociedad y a formar profesionales con consciencia crítica y propositiva, al servicio de la sociedad.

En esta perspectiva la Carrera de Ingeniería en Sistemas del Área de la Energía, las Industrias y los Recursos Naturales no Renovables, cumpliendo con los postulados previstos en la misión y visión institucional, forma profesionales con un elevado conocimiento en la problemática actual en la estructura, desarrollo y particularidades del diseño e implementación de nuevas herramientas informáticas y redes virtuales, quienes llevan a la práctica los conocimientos adquiridos en las aulas Universitarias, durante su vida estudiantil, a través de la implementación de un servidor VPN que permita la movilidad de usuarios de la red de datos de nuestra Alma Mater y su integración con el servidor VoIP, la misma que permite tener acceso a los servicios de la red universitaria como son internet, voz sobre IP, correo electrónico.

Al no contar con una red de acceso a estos servicios, se identificó que el objeto de investigación es la “La carencia de una red privada virtual para la red de datos de la Universidad Nacional de Loja, limita la utilización del servicio como el de telefonía IP.

Cabe destacar que para cumplir con los objetivos planteados se gestionó el apoyo del Departamento de la Jefatura de Informática de la Universidad Nacional de Loja, quienes se comprometieron a proporcionar toda la información y materiales necesarios para el desarrollo de nuestro proyecto, adicionalmente se procedió a la compra de 5 teléfonos de voz sobre IP, a fin de cumplir con un objetivo de autentificación en el Servidor de Voz sobre IP y puedan hacer uso del servicio de Telefonía IP.

Los teléfonos de Voz sobre IP están funcionando de acuerdo a la siguiente distribución:

- Uno en la Secretaria del Departamento General de Informática.
- Uno en la Sección de Mantenimiento de Hardware del Departamento General de Informática.
- Tres en la oficina del Equipo de Desarrollo del Sistema de Gestión Académico de la Universidad Nacional de Loja

7. DESARROLLO DE LA PROPUESTA ALTERNATIVA

7.1. INTRODUCCIÓN.

Siguiendo con el desarrollo de nuestra investigación y con la finalidad de implementar las soluciones encontradas, a continuación se detallarán todos y cada uno de los pasos a seguir para la implementación del servidor VPN.

Se describirá la instalación del software OpenVPN, las configuraciones necesarias para su puesta a punto y las diferentes soluciones a problemas que se pudieren dar al momento de la configuración y uso de OpenVPN.

Se tendrá en cuenta además la instalación y configuración de los clientes OpenVPN en uno de los más utilizados Sistemas Operativos como es Windows así como también nos referiremos a la creación de certificaciones y llaves de acceso para la autenticación de los clientes en la VPN.

En el presente trabajo mostraremos la implementación de una red privada virtual tanto del lado del cliente como del servidor, incluyendo la generación de certificados de seguridad.

7.2. UBICACIÓN DEL SERVIDOR VPN EN LA RED

En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos. En este caso el servidor VPN es un software el cual va a estar instalado en el Firewall de la Universidad Nacional de Loja tal como se muestra en la Figura 7.1

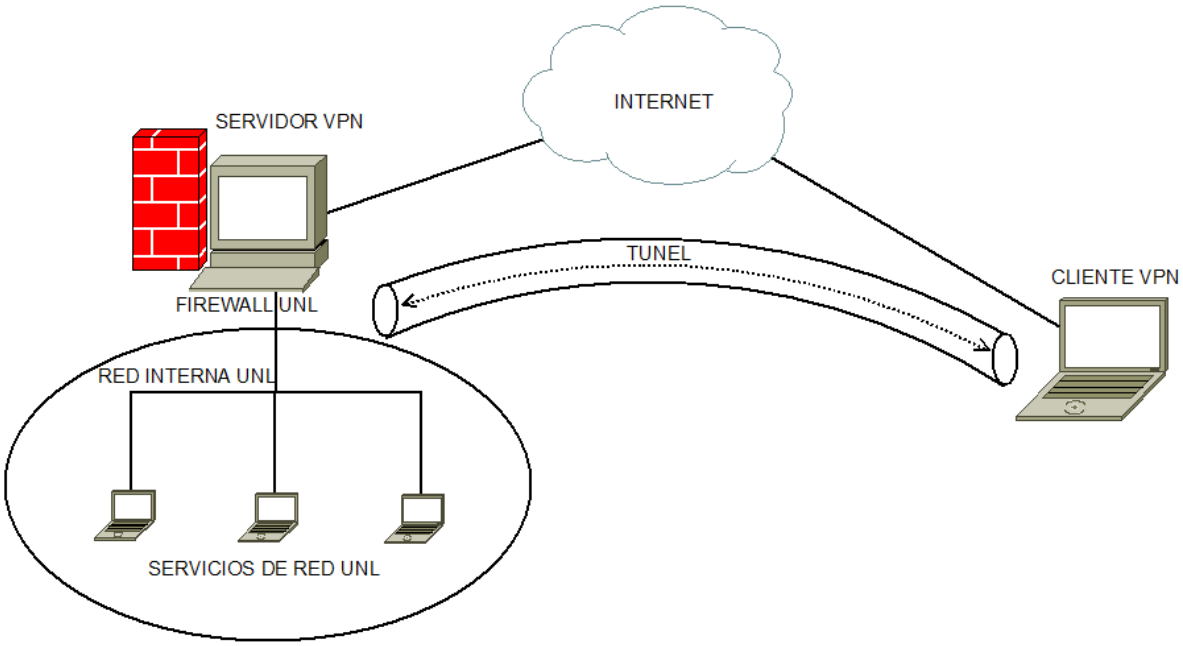

Fig. 7.1 Ubicación del Servidor VPN en la Red de Datos de la UNL.

7.3. INSTALACIÓN DEL SOFTWARE SERVIDOR OPENVPN

Antes que nada se actualizará todo nuestro sistema, puesto que el Firewall de la Universidad Nacional de Loja cuenta con acceso a Internet así como también tiene correctamente configurado sus repositorios por lo que se hizo de la siguiente forma:

```
yum -y update
```

El comando anterior descarga las actualizaciones directamente de Internet y lo así como sus dependencias en caso de ser necesario.

Una vez que tengamos actualizado nuestro sistema, procedemos a instalar el software de OpenVPN de la siguiente manera:

```
yum -y install openvpn
```

Los paquetes necesarios para que funcione correctamente el servidor VPN y que con la actualización que se le hace al sistema, se instalaron, son:

- Librerias LZO
- OpenSSL
- Controlador Tun/Tap, ya viene incluido en el kernel superior a 2.4.7

7.4. CONFIGURACIÓN DEL SERVIDOR OPENVPN

7.4.1. PREPARACIÓN DE LOS SCRIPTS RSA.

Como se explico en la aproximación teórica previa, existen dos formas de lograr seguridad, uno basado en SSL/TLS mediante certificados y claves RSA y otro mediante claves estáticas pre-compartidas. En este caso usaremos SSL/TLS ya que es más seguro.

Para la administración de los certificados y claves RSA, usaremos los scripts que vienen junto con OpenVPN (easy-rsa), la versión reciente trae consigo muchas mejoras, es esta easy-rsa 2.1.

```
cp -Rp /usr/share/doc/openvpn-2.1/easy-rsa/ /etc/openvpn
```

A continuación modificamos la Autoridad Certificadora (**CA**) para generar las llaves, para esto se edita el fichero /etc/openvpn/easy-rsa/vars de la siguiente forma:

```
export KEY_COUNTRY=EC
export KEY_PROVINCE=EC
export KEY_CITY=Loja
export KEY_ORG="unl.edu.ec"
export KEY_EMAIL="marcoxavi@unl.edu.ec"
```

De lo anterior, cada elemento significa lo siguiente:

• **KEY_COUNTRY:** Especifica el país donde se encuentra el servidor

VPN

- **KEY_PROVINCE:** Provincia o estado donde se encuentra este.
- **KEY_CITY:** Ciudad ubicado el servidor VPN.
- **KEY_ORG:** Dominio o departamento de la organización/Empresa.
- **KEY_MAIL:** Correo electrónico de la organización/empresa.

Importante*: Se deben llenar todos los parámetros ya que son indispensables para los certificados que serán creados.*

Seguidamente se ejecutarán los scripts para generar las llaves correspondientes de la siguiente forma:

7.4.2. INICIALIZANDO AUTORIDAD CERTIFICADORA (CA)

Para generar el CA deberá realizar los siguientes pasos:

```
- cd /etc/openvpn/easy-rsa/2.0/
- source ./vars
- sh clean-all # Al ejecutar esto nos crea un directorio keys dentro de este directorio
- sh build-ca
- cd /etc/openvp
```

7.4.3. GENERANDO PARÁMETROS DIFFIE HELLMAN.

Los parámetros ***Diffie Hellman*** deben de ser generados en el Servidor OpenVPN, para realizar esto deberá ejecutar el script de la siguiente forma:

```
sh build-dh
```

7.4.4. GENERACIÓN DE LLAVES.

Para generar el certificado (.crt) y llave (.key) privada para el **servidor** será de la siguiente forma**:**

```
sh build-key-server server
```

En donde [server] es la variable que utilizamos para identificar la llave privada del servidor.

Para generar el certificado y llave para los **clientes** se hace de la siguiente forma:

Recomendación: Cada cliente deberá tener su propia llave:

```
sh build-key cliente1
sh build-key cliente2
sh build-key marco
sh build-key davireto
sh build-key jramon
sh build-key manuelmax
sh build-key pato
sh build-key peche
```

Una vez que se han generado las llaves correspondientes a los clientes y servidor, se podrá obtener éstas en el directorio /etc/openvpn/easy-rsa/2.0/keys

7.4.5. ARCHIVOS A COPIAR.

Se deben copiar al directorio /etc/openvpn los siguientes archivos localizados en /etc/openvpn/easy-rsa/2.0/:

- ca.crt

- dh1024.pem
- server.crt
- server.key

7.4.6. ARCHIVO DE CONFIGURACIÓN DEL SERVIDOR VPN

Para la creación del servidor OpenVPN se deberá crear un archivo de configuración en el directorio ***/etc/openvpn/*** con el nombre:

server.conf

```
port 1194

proto udp

dev tun

ca ca.crt

cert server.crt

key server.key

dh dh1024.pem

client-to-client

server 10.8.0.0 255.255.0.0

ifconfig-pool-persist ipp.txt

push "route 172.16.32.0 255.255.240.0"
```

```
keepalive 10 120

comp-lzo

user nobody

group nobody

persist-key

persist-tun

status /var/log/openvpn-status.log

verb 5
```

Descripción del archivo de configuración del Servidor VPN:

Port: Especifica el puerto que será utilizado para que los clientes vpn puedan conectarse al servidor.

Proto: tipo de protocolo que se empleará en a conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que se utilizará en el servidor OpenVPN.

ca: Especifica la ubicación exacta del fichero de Autoridad Certificadora.[.ca]

cert: Especifica la ubicación del fichero [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor

OpenVPN.

dh: Ruta exacta del fichero [.pem] el cual contiene el formato de Diffie Hellman (requerido para **--tls-server** solamente).

server: Se asigna el rango IP virtual que se utilizará en la red del túnel VPN.

Ifconfig-pool-persist: Fichero en donde quedarán registradas las direcciones IP de los clientes que se encuentran conectados al servidor OpenVPN.

Keepalive 10 120: Envía los paquetes que se manejan por la red una vez cada 10 segundos; y asuma que el acoplamiento es abajo si ninguna respuesta ocurre por 120 segundos.

comp-lzo: Especifica los datos que recorren el túnel VPN será compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los scripts up/down

status: fichero donde se almacenará los eventos y datos sobre la conexión del servidor [.log]

verb: Nivel de información (default=1). Cada nivel demuestra todo el Info de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.

0: No muestra una salida excepto errores fatales.

1 – 4: Rango de uso normal.

5: Salida **R** y **W** caracteres en la consola para los paquetes de lectura y escritura, mayúsculas son usadas por paquetes TCP/UDP y minúsculas son usadas para paquetes TUN/TAP.

Para que funcione el servidor VPN tiene que estar habilitado el **"IP forwarding"**, pero como se trata del Firewall de la Universidad Nacional de Loja, esta configuración ya está habilitada.

7.4.7 INICIALIZANDO EL SERVIDOR VPN

cuando hayamos configurado el openvpn podemos activarlo con:

```
service openvpn start

chkconfig openvpn on
```

Si necesitáramos reiniciarlo (para que lea de nuevo la configuración por ejemplo) podríamos hacerlo con:

```
service openvpn restart
```

O si necesitáramos detenerlo, escribimos:

```
service openvpn stop
```

7.5. CONFIGURACIÓN DE CLIENTES VPN CON OPENVPN

7.5.1. CLIENTES WINDOWS

Para la configuración de clientes OpenVPN utilizaremos el programa OpenVPN GUI para Windows.

OpenVPN GUI para Windows corre normalmente en una ventana de consola, al ser conectado al servidor remoto/local VPN le da un aviso en el área de notificación (el área de abajo a la derecha por el reloj en la barra), desde allí se puede tener el control de iniciar/parar el Cliente OpenVPN, consultar los avisos (log), incluso cambiar su contraseña.

Puede ser descargado en el sitio OpenVPN GUI for Windows [http://openvpn.se/].

Preparativos y configuración

A continuación deberá copiar los siguientes ficheros:

- ca.crt.
- cliente1.crt.
- cliente1.key.

Estos fueron creados en el directorio /etc/openvpn/easy-rsa/2.0/keys y deberán ser colocados en la máquina cliente dentro de C:\ProgramFiles\OpenVPN\config o a su vez en C:\Archivos de Programa\OpenVPN\config

Se creará un fichero de configuración cliente para el OpenVPN dentro del directorio ***C:\|Archivos de Programa\OpenVPN\config*** con el nombre de **cliente1.ovpn.**

Tendrá la siguiente configuración:

```
Float

client

dev tun

proto udp

remote 192.188.49.5 1194

resolv-retry infinite

nobind

persist-key

persist-tun
```

```
#------ SECCION DE LLAVES --------

ca ca.crt

cert cliente.crt

key cliente.key

ns-cert-type server

#--------- Soluciones encontradas para Windows Vista
route-method exe
route-delay 2
#---------------------------------

comp-lzo

verb 5
```

Descripción del archivo de configuración del cliente VPN:

client: Especifica el tipo de configuración, en este caso tipo cliente OpenVPN.

Port: Especifica el puerto que será utilizado para que los clientes VPN puedan conectarse al servidor.

Proto: Tipo de protocolo que se empleará en la conexión a través de VPN

dev: Tipo de interfaz de conexión virtual que utilizará el servidor OpenVPN.

remote: Host remoto o dirección IP en el cliente, el cual especifica al

servidor OpenVPN.
El cliente OpenVPN puede tratar de conectar al servidor con **host:port** en el orden especificado de las opciones de la opción **--remote**.

float: Este le dice a OpenVPN que acepte los paquetes autenticados de cualquier dirección, no solamente la dirección que fue especificada en la opción **--remote**.

resolv-retry: Si la resolución del hostname falla para **-- remote**, la resolución antes de fallar hace una re-comprobación de n segundos.

nobind: No agrega bind a la dirección local y al puerto.

ca: Especifica la ubicación exacta del fichero de Autoridad Certificadora [.ca].

cert: Especifica la ubicación del fichero [.crt] creado para el servidor.

key: Especifica la ubicación de la llave [.key] creada para el servidor OpenVPN.

remote: Especifica el dominio o IP del servidor así como el puerto que escuchará las peticiones para servicio VPN.

comp-lzo: Especifica los datos que recorren el túnel VPN y serán compactados durante la trasferencia de estos paquetes.

persist-key: Esta opción soluciona el problema por llaves que persisten a través de los reajustes SIGUSR1, así que no necesitan ser releídos.

Persist-tun: Permite que no se cierre y re-abre los dispositivos TAP/TUN al correr los guiones up/down

verb: Nivel de información (default=1). Cada nivel demuestra toda la Información de los niveles anteriores. Se recomienda el nivel 3 si usted desea un buen resumen de qué está sucediendo.
0 --No muestra una salida excepto errores fatales.
1 to 4 –Rango de uso normal.
5 --Salida **R**y **W** caracteres en la consola par los paquetes de lectura y escritura, mayúsculas es usada por paquetes TCP/UDP minúsculas es

usada para paquetes TUN/TAP.

Una vez configurado el cliente VPN con Windows, deberá ir al área de notificación (el área de abajo a la derecha por el reloj en la barra de Windows) y dar un click derecho al icono del cliente OpenVPN, allí aparecerá un menú en el cual podrá elegir la opción **conectar** [connect].

7.6 PRUEBAS Y VALIDACIÓN

7.6.1 PRUEBAS

Luego de realizar la instalación y configuración del servidor VPN se procedió a realizar las pruebas necesarias para determinar su funcionalidad.

Las pruebas consistieron en la instalación y configuración de varios clientes VPN, la instalación de un softphone y de la realización de una llamada hacia y desde dicho softphone.

El software que se instaló se denomina OpenVPN GUI versión 1.0.3 (openvpn-2.0.9-gui-1.0.3-install.exe). También se instaló el software denominado X-Lite. El mismo que luego de ser configurado nos sirvió para confirmar el estado de la conexión del cliente VPN con el servidor VPN de la Universidad Nacional de Loja. El X-Lite fue debidamente configurado con una extensión que consta dentro del Dial Plan del Servidor Asterisk de la Universidad Nacional de Loja. Se utilizaron las extensiones 1026 y 1027 que les corresponde a los usuarios VPN dentro del plan de marcado.

Se realizó cinco pruebas de conectividad cliente-servidor. Éstas se realizaron en tres Cybers de la ciudad y en dos lugares privados, todos con diferentes proveedores de Internet dentro de la Ciudad de Loja.

A continuación detallamos los lugares y los resultados de las pruebas realizadas:

Prueba 1.

Lugar: Cyber Charly's Net

Dirección: Sucre y Mercadillo (esquina)

Fecha: 16 de Mayo del 2009

ISP: Grupo TV Cable

Resultado: Exitoso

Calidad: Buena (El retardo de la voz es mínimo)

Procedimiento:

Se instaló y configuró OpenVPN GUI y X-Lite la máquina # 2 del cyber. Se realizaron varias llamadas desde y hacia la extensión 1026. Las llamadas fueron realizadas al teléfono número 2547252 ext 128 sub-ext 7, desde las operadoras PORTA, Movistar y Pacifictel. El resultado de las pruebas de conexión con el comando Ping Fueron satisfactorias. Las conversaciones se llevaron a cabo con toda normalidad dejándose notar en lo mínimo el retardo en la voz.

Prueba 2.

Lugar: Cyber Fononet

Dirección: 18 de noviembre y Mercadillo (esquina)

Fecha: 16 de Mayo del 2009

ISP: TELCONET

Resultado: Exitoso

Calidad: Mala (El retardo de la voz es muy perceptible)

Procedimiento:

Se instaló y configuró OpenVPN GUI y X-Lite en una computadora portátil personal. Se realizaron varias llamadas desde y hacia la extensión 1026. Las llamadas fueron realizadas al teléfono número 2547252 ext 128 sub-ext 7, desde las operadoras PORTA, Movistar y Pacifictel. El resultado en la verificación del estado de la conexión con el comando Ping fue complaciente. Pero la conversación fue imposible por el retardo en la voz fue demasiado obvio.

Prueba 3.

Lugar: Cyber Sport Net

Dirección: Miguel Riofrío e/ Bolívar y Bernardo Valdivieso

Fecha: 16 de Mayo del 2009

ISP: ADSL Pacifictel

Resultado: Exitoso

Calidad: Muy Buena (El retardo de la voz es casi nulo)

Procedimiento:

Se instaló y configuró OpenVPN GUI y X-Lite la máquina # 5 del cyber. Se realizaron varias llamadas desde y hacia la extensión 1026. Las llamadas fueron realizadas al teléfono número 2547252 ext 128 sub-ext 7, desde las operadoras PORTA, Movistar y Pacifictel. El resultado de las pruebas de conexión con el comando Ping Fueron muy satisfactorias. Las conversaciones se llevaron a cabo con toda normalidad dejándose notar mínimos momentos el retardo en la voz.

Prueba 4.

Lugar: Privado (Domicilio)

Dirección: Av. Eduardo Kingman e/ Gonzanamá y Saraguro

ISP: Net Plus

Fecha: 17 de Mayo del 2009

Resultado: Exitoso

Calidad: Buena (El retardo de la voz es poco frecuente)

Procedimiento:

Se instaló y configuró OpenVPN GUI y X-Lite un equipo portátil. Se realizaron varias llamadas desde y hacia la extensión 1027. Las llamadas fueron realizadas al teléfono número 2547252 ext 128 sub-ext 8, desde las operadoras PORTA, Movistar y Pacifictel. El resultado de las pruebas de conexión con el comando Ping fueron elevadas en ocasiones. Las conversaciones se llevaron a cabo con toda normalidad dejándose notar en frecuentes momentos el retardo en la voz.

Prueba 5.

Lugar: Privado (Domicilio)

Dirección: Sucre e/ Gonzanamá y Saraguro

Fecha: 17 de Mayo del 2009

ISP: Easy Net

Resultado: Exitoso

Calidad: Buena (El retardo de la voz es poco notorio)

Procedimiento:

Se instaló y configuró OpenVPN GUI y X-Lite un computador de escritorio. Se realizaron varias llamadas desde y hacia la extensión 1027. Las llamadas fueron realizadas al teléfono número 2547252 ext 128 sub-ext 8, desde las operadoras PORTA, Movistar y Pacifictel. El resultado de las pruebas de conexión con el comando Ping fueron aceptables. Las conversaciones se llevaron con toda normalidad notándose escaso retardo en la voz.

7.6.2 VALIDACIÓN

7.6.2.1 VALIDACIÓN DE LOS CLIENTES

Luego de realizadas las pruebas se procedió a realizar una encuesta a los clientes VPN las cuales se anexan al final de este trabajo.

1. **Considera usted que el servicio VPN, implementado en la Universidad Nacional de Loja es útil?**

Tabla 7.1 Tabla de Resultados de la pregunta 1 en la validación de los clientes

Opciones	Frecuencia	Porcentaje
Si	7	100
No	0	0
Total	7	100

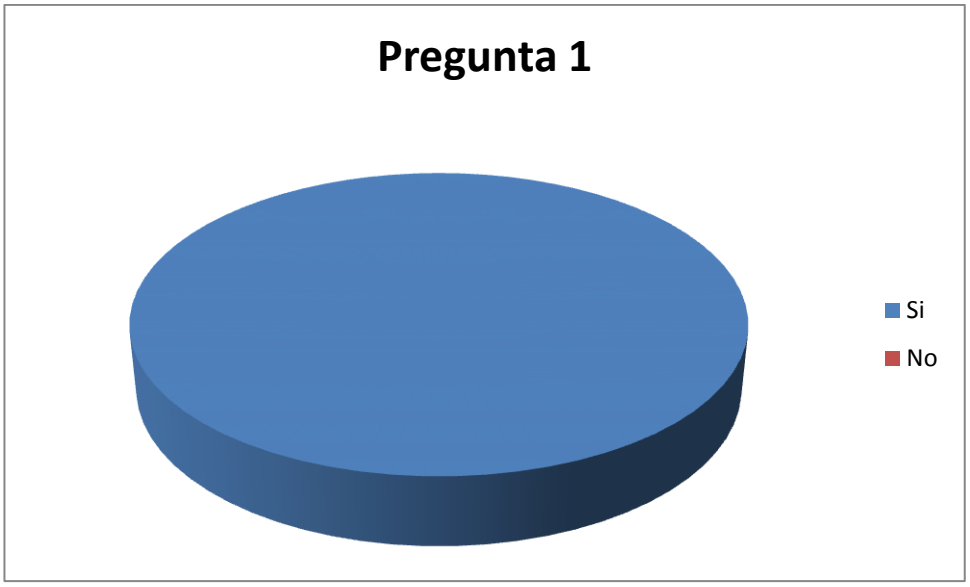

Fig. 7.2 Grafico de Resultados de la pregunta 1 en la validación de los clientes

Análisis de la pregunta 1.

Una vez tabulado los datos podemos mencionar que el 100% de los encuestados consideran que el servidor VPN implementado en la Universidad Nacional de Loja es útil.

Al explicar los encuestados el porqué, describen lo siguiente:

- Permita la movilidad y el acceso de los usuarios a la red de la Universidad desde cualquier parte del mundo donde se tenga un acceso a internet.
- Es económica porque no se necesita infraestructura para redes WAN.

2. Ud. como usuario considera que el manejo a la conexión del servidor VPN a través de la OpenVPN GUI es:

Fácil ( )

Difícil ( )

Tabla 7.2 Tabla de Resultados de la pregunta 2 en la validación de los clientes

Opciones	Frecuencia	Porcentaje
Fácil	7	100
Difícil	0	0
Total	7	100

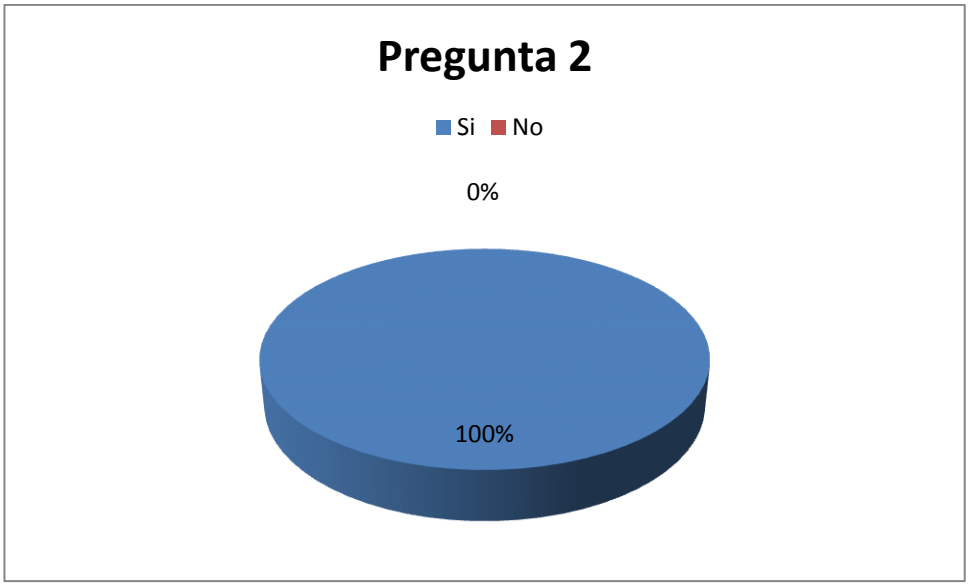

Fig. 7.3 Gráfico de Resultados de la pregunta 2 en la validación de los clientes

Análisis de la pregunta 2.

Una vez analizado los datos de la tabla hemos logrado determinar que el manejo del OpenVPN GUI es relativamente fácil porque los pasos para la establecer conexión son sencillos y mínimos.

3. ¿La autentificación de su cliente de voz sobre IP ser realizo con éxito?

Si ( )

No ( )

Tabla 7.3 Tabla de Resultados de la pregunta 3 en la validación de los clientes

Opciones	Frecuencia	Porcentaje
Si	7	100
No	0	0
Total	7	100

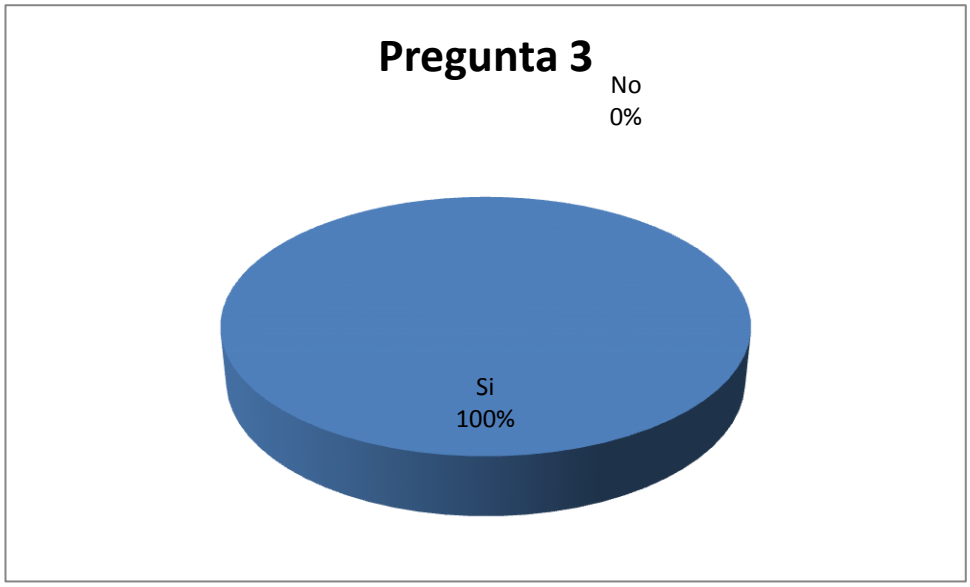

Fig. 7.4 Grafico de Resultados de la pregunta 3 en la validación de los clientes

Análisis de la Pregunta 3:

Una vez realizado la tabulación de datos podemos determinar que 7 usuarios que representan el 100% opinan que la autentificación de los clientes sobre voz sobre IP se realizó sin presentar ningún problema.

4. Tuvo problemas al realizar su llamada desde y hacia su cliente de Voz sobre IP

Si ( )

No ( )

Tabla 7.4 Tabla de Resultados de la pregunta 4 en la validación de los clientes

Opciones	Frecuencia	Porcentaje
Si	6	86
No	1	14
Total	7	100

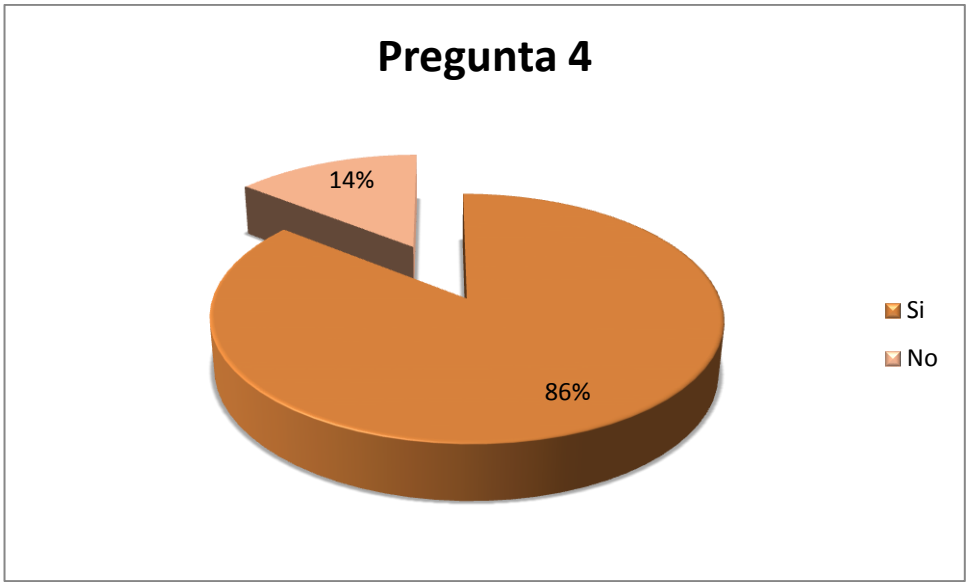

Fig. 7.5 Grafico de Resultados de la pregunta 4 en la validación de los clientes

Análisis de la pregunta 4.

Una vez realizado la tabulación de datos podemos determinar que 6 usuarios que representan el 86% opinan que no tuvieron problemas para realizar las llamadas desde y hacia su servidor de Voz sobre IP, mientras 1 usuario que representa el 14% opinaron que tuvieron algún tipo de problema al realizar la llamada por el tráfico de voz con Telconet.

5. La calidad de la llamada establecida fue:

Muy Buena ( )

Buena ( )

Mala ( )

Tabla 7.5 Tabla de Resultados de la pregunta 5 en la validación de los clientes

Opciones	Frecuencia	Porcentaje
Muy Buena	2	29
Buena	4	57
Mala	1	14
Total	7	100

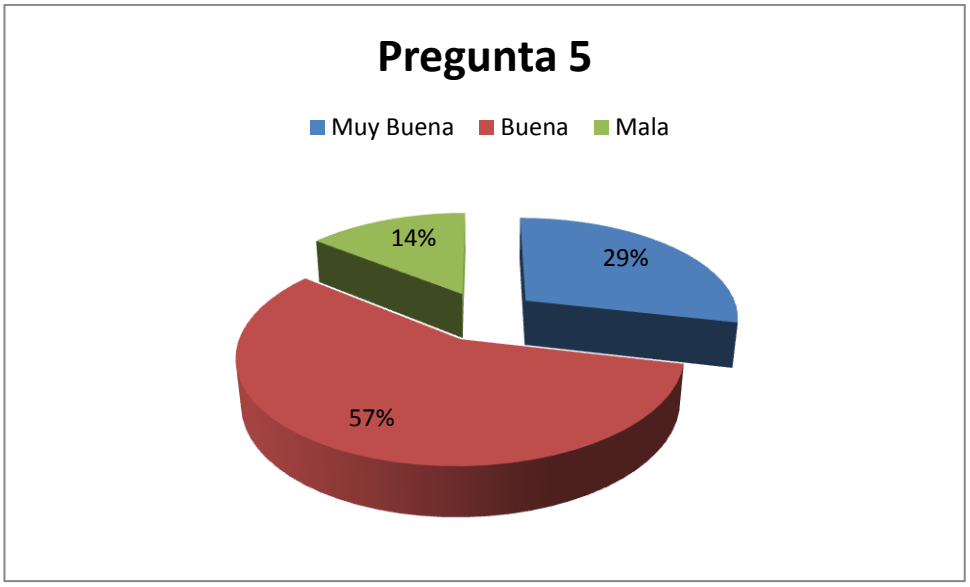

Fig. 7.6 Grafico de Resultados de la pregunta 5 en la validación de los clientes

Análisis de la pregunta 5.

Una vez realizado la tabulación de datos podemos analizar que 2 usuarios que representan el 29% opinan que la calidad de las conversaciones que realizaron hacia el servidor se llevaron con toda normalidad dejándose notar mínimos momentos el retardo en la voz, mientras 4 usuarios que representan el 57% que la conversación que realizaron fue buena porque el retardo de la voz es mínimo, y por último un usuario encuestado que representa al 14% opinó que la calidad de conversación fue mala porque el retardo de la voz es muy perceptible

7.6.2.1 VALIDACIÓN DEL ADMINISTRADOR

Dentro de la fase de validación de acuerdo con la planificación de nuestro proyecto de tesis y con los objetivos planteados se realizaron las pruebas de validación el Viernes 15 de Mayo del 2009 en el Firewall de la Jefatura de Informática de la Universidad Nacional de Loja teniendo como responsable al Tecnólogo Daniel Reyes responsable de la sección de redes de la Universidad Nacional de Loja.

Dicha prueba de administrador fue aplicada a un solo Administrador de la VPN, para la de generación de certificados y llaves de cada cliente.

La aplicación de las encuesta fue realizada después de haberse utilizado la VPN por parte del administrador de la red. La instalación de la VPN es una instalación simple de Windows, en el manual de usuario se detalla de mejor manera.

Dentro de las pruebas realizadas no se encontraron errores al momento de instalar el software OpenVPN GUI, la generación de certificados y llaves, los Usuarios realizaron observaciones en cuanto a la conexión y el acceso a la VPN, lo que se tomó en cuenta para corregir y mejorar en nuestro proyecto de tesis.

Por otra parte luego de realizadas las validaciones y como parte de las pruebas, tenemos en la Figura 7.7 una pantalla tomada desde el computador del Administrador de la Red el lunes 1 de junio del 2009, la misma que fue capturada en el momento que se hizo el acceso desde la Ciudad de Quito debido a que el Tecnólogo Daniel Reyes responsable de la sección de redes de la Universidad Nacional de Loja se encontraba en un curso y como allí se muestra se pudo autenticar en el Servidor VPN, además se ingresó al Firewall de la red y así mismo se hizo uso Servicio de Voz sobre IP (Asterisk).

Finalizado las pruebas se concluyó que la IMPLEMENTACION DE UN SERVIDOR VPN QUE PERMITA LA MOVILIDAD DE USUARIOS DE LA RED DE DATOS

DE LA UNIVERSIDAD NACIONAL DE LOJA Y SU INTEGRACIÓN CON EL SERVIDOR DE VoIP**,** cumple con todos los requerimientos planteados en el proyecto.

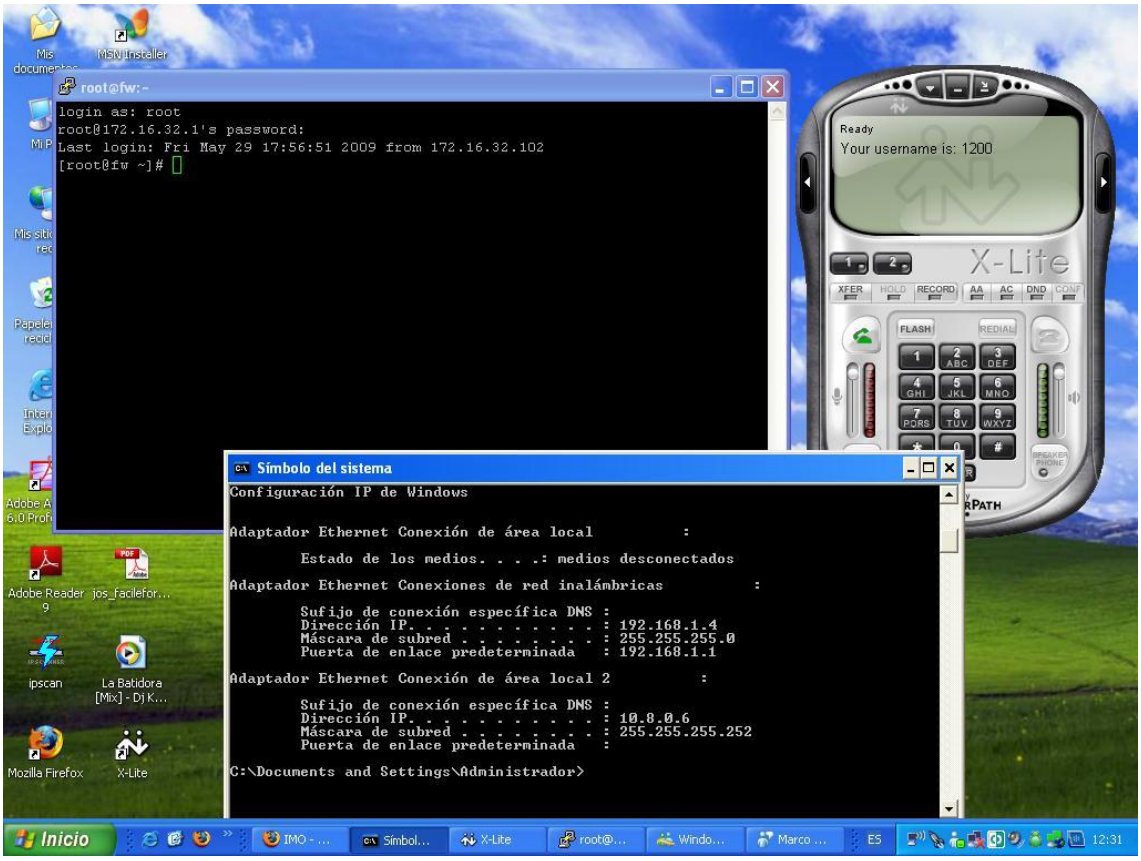

Fig. 7.7 Grafico de prueba del Administrador de la Red desde la Ciudad de Quito

8. VALORACIÓN TÉCNICA ECONÓMICA

Para la construcción e implementación de la VPN el grupo de desarrollo detallará los recursos humanos, técnicos, materiales, tecnológicos y varios que intervinieron en el costo real del presente proyecto.

En esta lista mostraremos los costos aproximados del desarrollo de la VPN

8.1 RECURSOS HUMANOS.

Tabla 8.1 Descripción Económica de Recursos Humanos

DESCRIPCIÓN	CANTIDAD	# HORAS	V/u	V/T
Grupo de Desarrollo	2	250	3	1500,00
Directora del Proyecto	1	---	---	---
Asesoría	1	25	10	250,00

8.2 RECURSOS TÉCNICOS

8.2.1 HARDWARE

Tabla 8.2 Descripción Económica de Hardware

COMPONENTE	CARACTERÍSTICA	CANTIDAD	V/U	V/T
Servidor	HP Intel(R) Xeon (TM) CPU 3.2 GHZ, RAM 1Gb HDD 160 GB	1	---	---
Teléfono IP	D-LINK DPH-150SE	5	108.87	544,35
Impresora	Cannon 1500	1	45	45

Computador Portátil HP COMPAQ	AMD turión, 512 RAM, 120 GB sata	1	960	960
Flash Memory	Kingston 4 GB	1	35	35

8.2.2 SOFTWARE

Tabla 8.3 Descripción Económica de Software

NOMBRE	CANTIDAD	V/U	V/T
OpenVPN	1	---	---
OpenVPN gui	*	---	---

8.2.3 RECURSOS MATERIALES

Tabla 8.4 Descripción Económica de los Recursos Materiales

DESCRIPCIÓN	CANTIDAD	V/u	V/T
Resmas 500 hojas de papel 75 g/m2 tamaño A4	2	4	16,00
Caja de CD's	1	15	15,00
Carpetas	5	0,25	1,00
Portaminas	4	1	4,00

8.2.4 RECURSOS TECNOLÓGICOS

Tabla 8.5 Descripción Económica de Recursos Tecnológicos

DESCRIPCIÓN	CANTIDAD	V/u	V/T
Internet	100	0,80	80,00

8.2.5 ADICIONALES

Tabla 8.6 Descripción Económica de gastos adicionales

DESCRIPCIÓN	V/T
Servicios Básicos	50,00
Transporte	10,00
Imprevistos	200,00

Tabla 8.7 Tabla de Subtotales

DESCRIPCIÓN	V/T
Recursos Humanos	1750,00
Recursos Técnicos	1584,35
Software	---
Recursos Materiales	36,00
Recursos Tecnológicos	80
Adicionales	260
TOTAL	**3710,35**

El costo real del proyecto es de **3710,35**

9. CONCLUSIONES

Al finalizar el presente trabajo investigativo se concluye que:

- ✓ Se consideró como la mejor opción a la utilización del paquete OpenVPN en el servidor **VPN** porque se adaptan completamente a las condiciones de la red de datos de la Universidad.

- ✓ OpenVPN vuelve innecesaria la adquisición de hardware dedicado o software propietario, resultando una solución más económica, simple, flexible y escalable.

- ✓ Al implementar el servidor VPN se ha expandido el límite de la movilidad de los usuarios de la red universitaria, hacia cualquier parte del mundo dónde exista una conexión a Internet porque puede acceder a los servicios de la red sin tener que estar físicamente dentro de ella

- ✓ Los usuarios de la VPN pueden acceder de manera segura y confiable a los servicios de la red, puntualmente al servicio de voz sobre IP.

- ✓ Al tener un servidor VPN, los servicios informáticos que brinda la Universidad Nacional de Loja no se limiten a ser accedidos sólo dentro del Campus Universitario, por lo que es factible la creación de clientes VPN en las Extensiones Universitarias permitiendo el uso de los recursos principalmente del Sistema de Gestión Académica (SGA).

- ✓ La realización de éste proyecto de desarrollo nos ha permitido adquirir conocimientos básicos sobre GNU/Linux, TCP/IP y de Seguridad en Internet (firewall/iptables).

- ✓ Es muy factible utilizar clientes OpenVPN para interconectar aplicaciones de forma segura y transparente. Gracias a la encriptación como a la autenticación

10. RECOMENDACIONES

Se recomienda lo siguiente:

- ✓ Crear para cada cliente su propia llave y certificado por razones de seguridad. La entidad encargada de generar estos archivos es la Jefatura General de Informática de la Universidad Nacional de Loja, puesto que es aquí en donde queda implementado el Servidor VPN.

- ✓ Realizar la distribución de los archivos de configuración cómo son: ca.crt (unidad certificadora), cliente.key y cliente.crt de los clientes de manera segura, en lo posible de manera personal y no utilizar medios vulnerables como por ejemplo correo electrónico.

- ✓ Utilizar la VPN para solucionar costes operativos de red, ya que ofrece economía, flexibilidad, escalabilidad y capacidad de adaptación que las tradicionales WAN´s.

- ✓ Analizar la posibilidad de implementar la modalidad de Teletrabajo en la Universidad Nacional de Loja dejándose de enfocar por "horas en la oficina" a "horas dedicadas al trabajo", ya que las tareas pueden ser realizadas a distancia utilizando TIC (Tecnologías de la Información y la Comunicación) como por ejemplo la implementación de un servidor VPN planteado en nuestro proyecto.

- ✓ Que la instalación y configuración del cliente VPN sea realizado por el Administrador de la red de la Universidad Nacional de Loja, con la finalidad de garantizar la conexión al momento de autenticarse en el servidor VPN.

- ✓ Se realice la adquisición del códec G729 para mejorar la calidad de voz para el uso del Servidor de Telefonía IP (Asterisk)

- ✓ Realizar la conexión con un ancho de banda mínimo de 256 Kbps principalmente para telefonía IP, para obtener mejores resultados al momento del enlace

11. BIBLIOGRAFÍA

SITIOS WEB:

- FEILNER, Markus, 2006, OpenVPN: Building and Integrating Virtual Private Networks, Editorial Packt Publishing, 258 p.

- COMO INSTALAR Y CONFIGURAR OPENVPN, 2007, [http://www.ecualug.org/2007/02/06/comos/centos/c_mo_instalar_y_configurar_openvpn], [Consulta: 19 de mayo, 2009].

- OPENVPN, 2006, [http://es.wikipedia.org/wiki/OpenVPN], [Consulta:25 de Julio, 2008].

- RED PRIVADA VIRTUAL, 2008, [http://es.wikipedia.org/wiki/Red_privada_virtual], [Consulta: 06 de Abril, 2009].

- OPENVPN COMO, Copyright (C) 2002-2004, [http://laurel.datsi.fi.upm.es/~rpons/openvpn_como/], [Consulta: 10 de Junio, 2008].

- OPENVPN TECHNOLOGIES SECURE YOUR CONNECTIVITY, 2002, [http://openvpn.net/howto.html], [Consulta: 08 de Agosto, 2008].

- OPENVPN TECHNOLOGIES SECURE YOUR CONNECTIVITY, 2002, [http://openvpn.net/index.php/documentation/manuals/openvpn-20x-manpage.html], [Consulta: 07 de Agosto, 2008].

- FEDORA WIKI LATAM, 2008, [http://proyectofedora.org/wiki/index.php/Redes/VPNyTuneles/OpenVPN], [Consulta: 15 de Junio, 2009].

- [http://www.ubuntu-es.org/node/5290], [Consulta: 10 de Septiembre, 2008].

12. ANEXOS