Universidad Michoacán de San Nicolás de Hidalgo

Facultad de Contaduría y Ciencias Administrativas

Tesina

Uso de Software Libre para transmisión de datos mediante VPN´s

Medida contingente para mantener activo el servicio a socios (clientes externos)

Que para obtener el título de Licenciatura en Informática Administrativa.

Presenta:

Alejandro Piñón Méndez

Asesor(a): Dra. Ma. Hilda Rodales Trujillo

Morelia, Mich., Enero de 2012

Dedicatoria y agradecimientos

Dedico el presente proyecto a:

Mis dos hijos, Brandon e Ian, quienes me han abierto la conciencia a un mundo que desconocía, a mi esposa, Jen, ya que a su lado he tenido una vida plena y enriquecedora, quien me motiva día con día a explorar mi yo interno y que con su ayuda he logrado conseguir por fin llegar a esta meta.

A mis padres quienes con su amor y consejos, con su férrea lucha por darnos lo mejor que podían a mi hermano, hermanas y a mí, me enseñaron que pase lo que pase jamás debemos rendirnos ante las inclemencias de la vida, ya que solamente son experiencias nuevas que debemos adquirir.

Por ultimo e igual de importante que a los demás, dedico sobre todo este proyecto a mi abuelo (que este en santa gloria) Martiniano Méndez quien no dejo de luchar hasta el final y que me enseño la felicidad viene en pequeñas partes y de modos diferentes y que tenemos que aprovecharla cuando se presente, que si queremos conseguir algo hay que luchar aun teniendo todo en contra.

Agradezco también: a todas aquellas personas que de una u otra forma han contribuido a que me encuentre en este proceso:

A Dios, por darme una familia como la que tengo, por darme esperanzas cuando me encuentro perdido, por darme vida.

A mis padres (Mercedes y Samuel) por brindarme su apoyo en todo momento, por educarme como lo hicieron y por darme la oportunidad de tomar mis propias decisiones desde joven aunque no sin dejar de guiarme.

A mis hermanas y hermano que sin saberlo abiertamente fueron parte del motivo que me llevo a cursar esta carrera con la intensión de darles ejemplo de que podemos conseguir lo que deseamos y nos esforzamos por tener.

A mi esposa Janeth por todas aquellas horas de desvelo que sin querer compartió conmigo, por apoyarme sin contemplaciones y por darme motivación ya que sin ella no lo hubiera conseguido.

A la UMSNH, ya que mediante la FCCA y el personal docente y administrativo pude obtener los conocimientos, habilidades y aptitudes que ahora poseo y que me permiten desenvolverme con facilidad en el ámbito no solo laboral sino personal. Gracias por compartir tanto experiencias como conocimientos conmigo.

A mis amigos Perla, Reyna, Héctor Ismael, Ignacio, Héctor, Andrés con quienes compartí más de 4 años de aventura y aprendizaje, quienes me apresuraban el paso cuando me iba rezagando y con quienes he vivido alegrías, tristezas, molestias y pesares, han sido y serán parte importante en mi vida.

A Esme quien me motivo a cursar la carrera y me introdujo en el hábito de la lectura, quien compartió conmigo momentos inocentes y amenos de amistad y cariño.

A Lupita quien me motivo a cursar la carrera y quien me hizo prometerle que conseguiría un doctorado, quien con su desordenado esfuerzo logra darme ejemplo de tenacidad y lucha.

A Sandy quien me informo sobre la licenciatura en esta mi Universidad logrando gracias a ello el estar ahora a punto de lograr mis objetivos iniciales.

Especial agradecimiento a Nadia que con su cariño, alegría, apertura a nuevas ideas y ansias de superación ha reforzado mi propia existencia y apreciación de la vida y de las personas que me rodean.

A Mauricio, Luis, Rosy, Tita, Cuco, Vero, Cris, Yuri y demás compañeros de trabajo que tuvieron la paciencia de aguantar el tiempo en que pudiera atenderlos aun en casos de necesidad de soporte y a quienes en situación de amistad me ha brindado apoyo y ánimo para seguir adelante.

Por último y en especial atención, a todas aquellas personas que dudaron que lo lograría, aquellas personas que me decían que no podría hacerlo, que sería difícil y que hicieron que realmente me fuera difícil tanto en lo personal como en lo laboral, ya que gracias a ellas adquirí más fuerza y voluntad para conseguirlo, ya que por cada ocasión que escuchaba un no, ganaba más fuerza de voluntad para decir ¡SI!

Contenido

Capitulo I.- Introducción

Introducción

Actualmente, para muchas empresas resulta fundamental disponer de comunicaciones a través de las redes de información. Las telecomunicaciones como parte de las TI, constituyen una herramienta fundamental en el desarrollo de cualquier actividad empresarial, facilitando el intercambio de información entre los miembros de la entidad y entre estos y el entorno con el que se relacionan, así como están presentes en muchos aspectos de nuestra vida cotidiana ***(Moya, 2005).*** Por sus bajos costos y escalabilidad se opta muchas veces por la instalación de enlaces privados. El uso de redes privadas supone la implantación de un nuevo enlace cada vez que se quiera conectar un nuevo miembro a la red de una organización, con los consiguientes elevados costos. La solución en estos casos es hacer llegar este tráfico de red atravesando redes públicas (como Internet) todo esto susceptible a ataques de usuarios malintencionados por la vulnerabilidad que presenta. Para evitar esto, es imprescindible proteger el tráfico que circulará por las redes públicas.

La solución más óptima son las Redes Privadas Virtuales (VPN en su acrónimo en inglés de "Virtual Private Network"), que permiten crear conexiones seguras a través de la infraestructura de redes públicas mediante una herramienta de comunicación segura, bajo costo y alta privacidad. Una VPN permite crear enlaces punto a punto, conectar distintas redes locales entre sí, o permitir por ejemplo a un empleado remoto conectarse a la sede de su empresa desde cualquier acceso a Internet (caso conocido como roadwarrior).

La implementación de una VPN está basada en "túneles", donde la información que atraviesa las redes públicas viaja encapsulada en paquetes de forma que el contenido resulta invisible hasta llegar a su destino. Una vez el paquete llega a su destino, este se des encapsula y la información vuelve a ser visible.

El presente proyecto de investigación obedece a la necesidad de que Caja Popular Lagunillas S. C. de A. P. de R. L. de C. V. cuente con los medios necesarios para lograr una continuidad del negocio además de la atención sin interrupciones a sus socios (clientes externos), ya que como se sabe por experiencia, todas las herramientas tecnológicas nos proporcionan avances y mejoras pero no están susceptibles de fallas, es una de esas fallas (perdida de conexión) la que atañe a este proyecto, ya que en muchas ocasiones por cuestiones ambientales, de energía eléctrica, de falta de mantenimiento, etc., se puede y ha producido una pérdida de conexión con el servidor de datos, lo que ocasiona primeramente que no se pueda brindar el servicio a los socios y también perdidas económicas a la cooperativa.

El proyecto tiende hacia el uso de software libre, ya que este cuenta con diversas características que pueden beneficiar no solo a la cooperativa en la que se implementó, sino que también a otras cooperativas o empresas del sector en las que pudieran aplicarse las situaciones de Caja Popular Lagunillas.

Es importante mencionar que este proyecto tiene la finalidad de cubrir también una parte del Plan de Continuidad de Negocios y del Plan de Contingencias, ya que lo que se pretende finalmente es que la cooperativa continúe laborando en caso de presentarse algún imprevisto con la tecnología existente que proporciona la conexión a los servidores centralizados de datos.

Planteamiento del Problema

Desde que Caja Popular Lagunillas apertura sus nuevas sucursales, ha sido imperiosa la necesidad de que se tenga conexión constante con estas con la finalidad de brindar nuevos servicios, contar con información actualizada en tiempo real, evitar duplicidad de información y procesos.

Específicamente, se cuenta con tecnología (antenas de radio y microondas) que permite realizar dicha conexión constante y "permanente", pero como todo, es falible, y muestra de ello es que durante la temporada de lluvias surge una problemática de todos los días prácticamente, donde si llueve se pierde la transmisión de datos a la Oficina Matriz y con las demás sucursales.

En cuanto a su solución, se cuenta con un plan de contingencias, pero dicho plan no se ha actualizado desde hace varios años y además no cuenta con la autorización correspondiente. El Centro de Cómputo tiene hasta cierto punto la posibilidad de implementar mecanismos que permitan solucionar la problemática existente, pero no hay apertura a trabajar de esta manera, por lo que se pretende cambiar este esquema presentando y aplicando una solución efectiva.

Además, para que la cooperativa refleje un buen funcionamiento y brinde confianza a sus socios y buena calidad de sus servicios, es necesario que se trabaje de manera conjunta con las áreas gerenciales y se desarrolle una estrategia (llámese proceso, tecnología, mecanismo, sistema), que permita cumplir con su función de manera adecuada. De esta manera, si se desea otorgar satisfacción total a los socios (clientes externos), es necesario se empiece a tomar conciencia sobre el uso de tecnologías que permitan lograr dicho objetivo.

El propósito del presente proyecto se dirigirá a las siguientes sucursales de la cooperativa:

- Oficina Matriz
- Sucursal Morelia Centro
- Sucursal Morelia Siervo de la Nación

Esto con el propósito de solucionar la problemática que se tiene en esas sucursales, mediante las variables antes mencionadas.

Objetivo General

Implementar una solución efectiva y permanente mediante Software Libre a través de una VPN que permita desarrollar las actividades inherentes a Caja Popular Lagunillas en atención a sus socios.

Objetivos Específicos

- Analizar las ventajas de la tecnología existente dentro de la cooperativa y su desempeño como base para establecer una nueva herramienta.
- Analizar y seleccionar un sistema, mecanismo, herramienta, estrategia que permita solucionar problemas de conexión con el servidor de datos.
- Brindar atención continua y en tiempo real a los socios de la cooperativa.

- Contar con un medio de comunicación/conexión adicional que brinde soluciones en caso de presentarse alguna contingencia.

Hipótesis

"La implementación de una VPN con software libre Software Libre proveerá a Caja Popular Lagunillas de una medida alterna para mantener un enlace dedicado con la Oficina Matriz".

Justificación

El ¿porque realizar la presente investigación? se responde presentando los siguientes argumentos:

- Las tecnologías que emplea actualmente la cooperativa son susceptibles de fallas debido al medio ambiente (Vientos, lluvias, cielo nublado, etc.).
- Toda tecnología presenta fallos en alguna ocasión y partimos de que nada es 100% efectivo o seguro.
- La atención al público debe permanecer en el horario fijado, siempre y cuando no se presenten desastres naturales, contingencias que afecten la integridad del personal empleado o por indicación de las áreas gerenciales y directivas.
- Se debe garantizar un alto nivel de fiabilidad y disponibilidad del sistema informático para la transmisión de datos.

El objetivo que se pretende lograr, es que en el momento de presentarse alguna falla de la tecnología actual empleada en la transmisión de datos, se tenga una alternativa que permita de manera rápida, eficiente y transparente, reanudar las labores en el menor tiempo posible.

Debido a la gran cantidad de Socios (Clientes externos) que tiene la cooperativa, es necesario que se tengan bien asegurados los métodos y procesos que se efectuaran a fin de brindar los servicios correspondientes, lo cual permitirá disminuir los aspectos que pueden causar conflictos en la atención al público.

El estudio que se realizara ayudara a la cooperativa para mejorar sus actividades y procesos de atención al socio tanto por sucursal así como de los que se realizan en conjunto. Las ventajas con que cuenta este proyecto son:

- Una conexión constante a los servidores de datos.
- Recuperación de la conexión en caso de falla ya sea por conexión mediante las antenas de microondas o por VPN.
- Atención al público sin necesidad de realizar llamadas al centro de soporte.
- Cambio transparente entre un medio de comunicación y otro.
- Seguridad en la transmisión de datos.

Preguntas de Investigación

1. ¿Es posible implementar una aplicación de Software Libre que permita mediante una VPN mantener un enlace dedicado y seguro con el servidor de datos?
2. ¿Disminuirán con esto las incidencias de conexión que se presenten en las sucursales de la cooperativa?
3. ¿Cuáles serán los beneficios que se obtendrán al realizar la implementación de una VPN de esta manera?

Alcances

- El proyecto se realizara solamente en 2 de las sucursales de Morelia y Lagunillas, Michoacán, pudiendo extender su alcance en un futuro en caso de obtener resultados satisfactorios.
- Se trabajara únicamente con las herramientas: Internet, Software Libre y equipo disponible en cada sucursal (switches, routers, firewalls, PC´s, Servidores).
- Se analizaran máximo 3 aplicaciones de software libre para su posible implementación dentro de la cooperativa.

Limitaciones

- Esta investigación se llevara a cabo en las instalaciones de Caja Popular Lagunillas S. C. de A. P. de R. L. de C. V., Oficina Matriz, sucursales Morelia Centro y Morelia Siervo de la Nación.
- Incluirá solamente equipo de cómputo existente.
- Únicamente se tomaran en cuenta los aspectos relacionados con la conexión (enlace dedicado) a los servidores de datos ubicados en la Oficina Matriz y lo relacionado para establecer dicho enlace.

Capitulo II.- Marco Teórico

Generalidades

El uso de las tecnologías de información en las empresas ha abierto un amplio espectro de servicios y productos de los cuales se puede beneficiar, ya sea directamente en sus ingresos, posicionándose en el mercado, incrementando la membresía de clientes, etc., todo esto con el uso de tecnologías como el internet, las redes sociales, ventas online entre otros.

Aunado a esto, muchas empresas se encuentran en un dilema, en el que si no se incursiona en este mercado, poco a poco se irán quedando obsoletas.

Internet brinda un sinfín de posibilidades como ya se mencionó, pero debemos recordar que la importancia de la población de internet no radica en su carácter cuantitativo (cuantas personas están conectadas a la red), sino en su carácter cualitativo (posición social, status, poder económico, capacidad de decisión, etc.), por lo que las empresas deben voltear más bien a quienes y no a cuantas personas son las que navegan en internet ***(Cafassi, 1998).***

En los últimos años, muchos cambios fundamentales han ocurrido también en la comunicación de datos y redes que darán forma al futuro de las próximas décadas. La creación de aplicaciones de red tales como Internet ha disparado el mundo de los negocios. Módems de alta velocidad proporcionan velocidades de datos en megabits (millones de bits por segundo) a lo largo de líneas regulares de teléfono y TV por cable. Las nuevas redes de área local (LAN) y las tecnologías de red troncal proporcionan velocidades Gigabit (mil millones de bits por segundo). También están disponibles las tecnologías de red de área metropolitana (MAN) y redes de área amplia (WAN) que ofrecen velocidades Terabit (trillones de bits por segundo) a Petabit (trillones de bits por segundo). La integración de voz y comunicación de datos se está moviendo rápidamente.

Quizás el cambio más importante ha sido el reconocimiento de la importancia estratégica de las comunicaciones y redes, tanto en el sector público y privado. Hoy en día, casi todas las computadoras están conectadas en red. Al mirar hacia atrás en los años 1990, nos damos cuenta de que la importancia del equipo fue superado por la importancia de la red. ***(Jerry FitzGerald, 2008)***

Redes de Datos

Tecnologías de Red

Las comunicaciones de datos es el movimiento de información de una computadora de un punto a otro por medio de sistemas de transmisión eléctrica u óptica. Estos sistemas a menudo se llaman redes de comunicaciones de datos. Esto está en contraste con el término más amplio de las telecomunicaciones, que incluye la transmisión de voz y vídeo (imágenes y gráficos), así como de datos y por lo general implica largas distancias. En general, las redes de comunicaciones de datos recopilan datos de micro computadoras y otros dispositivos y transmiten esos datos a un servidor que cuenta con un microprocesador más potente, minicomputadora o computadora central, o realiza el proceso inverso, o alguna combinación de los dos. Las redes de comunicaciones de datos facilitan un uso más eficiente de las computadoras y mejoran el control del día a día de un negocio, proporcionando un flujo de información más rápido. También proporcionan servicios

de transferencia de mensajes para permitir a los usuarios de las computadoras comunicarse entre sí a través de correo electrónico, chat, y streaming de vídeo (videoconferencias).

Componentes de una red

Existen tres componentes básicos de hardware para una red de comunicaciones de datos: un servidor o el equipo host (por ejemplo, una microcomputadora, mainframe), un cliente (por ejemplo, una microcomputadora, terminal), y un circuito (por ejemplo, cable, módem) sobre el cual pasan los mensajes. El servidor y el cliente también necesitan de un software de propósito especial de red que les permite comunicarse.

El servidor (o host) almacena los datos o software para que sea accesado por los clientes. En la arquitectura cliente-servidor, varios servidores pueden trabajar juntos en la red con un equipo cliente para apoyar la aplicación empresarial.

El cliente es el dispositivo hardware de entrada y salida que permite al usuario el mantener un circuito de comunicaciones. Por lo general proporciona a los usuarios el acceso a la red, los datos y el software en el servidor.

El circuito es el camino a través del cual viajan los mensajes. Está comúnmente basado en cables de cobre, aunque también se puede trabajar sobre fibra óptica o transmisión inalámbrica que cada vez se hace más común.

Existen muchos aparatos en el circuito que realizan funciones especiales, tales como switches y los routers.

En sentido estricto, una red no necesita un servidor. Algunas redes utilizan un nuevo diseño para conectar un conjunto de equipos similares que comparten sus datos y software entre otros. A tales redes se les llama peer-to-peer ya que los equipos funcionan como iguales, en lugar de confiar en un servidor central o una computadora host para almacenar los datos necesarios.

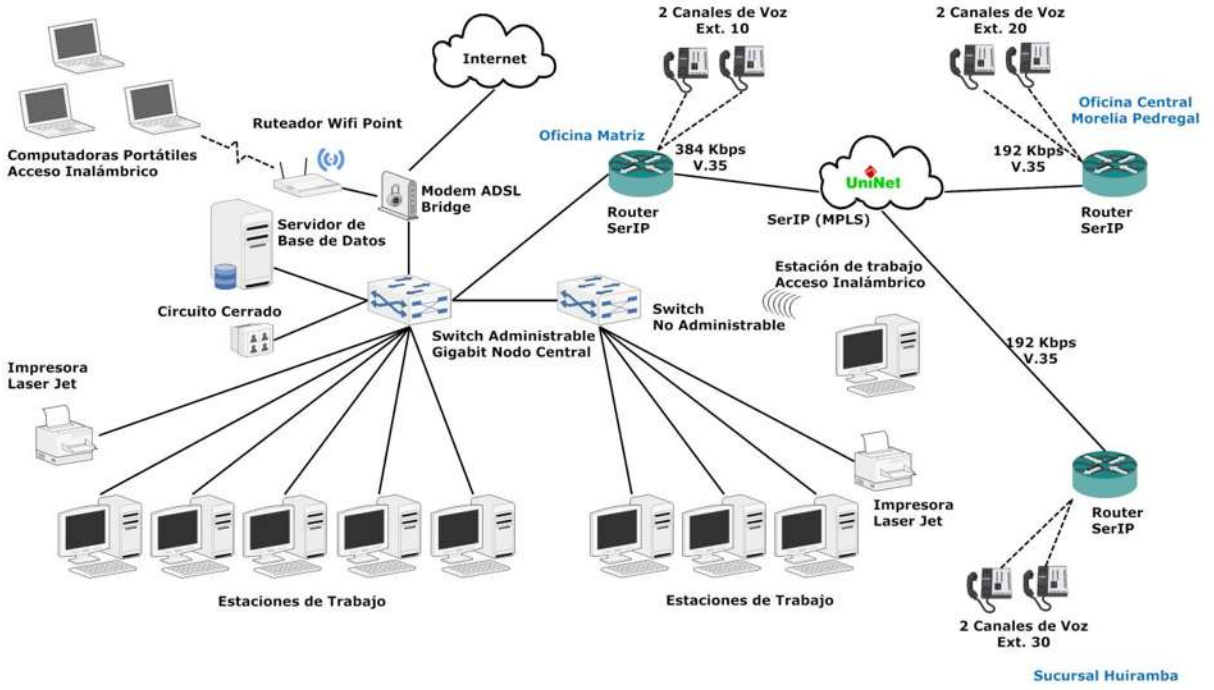


Ilustración 1: Red de datos

La ilustración 1 Muestra una pequeña red que cuenta con varias computadoras (clientes) conectados por un switch y cables (circuito). En esta red, los mensajes se mueven a través del switch y de las computadoras. Todos los equipos comparten el mismo circuito y deben turnarse para enviar mensajes. El router es un dispositivo especial que conectan dos o más redes. El router permite que los equipos de esta red (Corporativo) se puedan comunicar con equipos de otras redes (Por ejemplo, Internet o alguna sucursal).

La red en la Ilustración 1 tiene un servidor de base de datos. Aunque un servidor puede realizar muchas funciones, las redes suelen estar diseñados para que un equipo independiente proporcione los diferentes servicios. El servidor almacena los datos que pueden ser utilizados por los equipos en la red.

Los servidores suelen ser micro computadoras (a menudo más poderosas que otras de las computadoras en la red), pero también pueden ser mainframes.

Comunicación de redes

Una red se compone de dos partes principales, los nodos y los enlaces. Un nodo es cualquier tipo de dispositivo de red como una computadora personal. Los nodos pueden comunicar entre ellos a través de enlaces, como son los cables. Hay básicamente dos técnicas de redes diferentes para establecer comunicación entre dos nodos de una red: las técnicas de redes de conmutación de circuitos y las de redes de conmutación de paquetes. La primera es la más antigua y es la que se usa en la red telefónica y la segunda es la que se usa en las redes basadas en IP.

Una red de conmutación de circuitos crea un circuito cerrado entre dos nodos de la red para establecer una conexión. La conexión establecida está dedicada a la comunicación entre los dos

nodos. Uno de los problemas inmediatos de los circuitos dedicados es la pérdida de capacidad, dado que casi ninguna transmisión usa el 100% del circuito todo el tiempo.

Además, si un circuito falla en el medio de una transmisión, la conexión entera se pierde y debe establecerse una nueva.

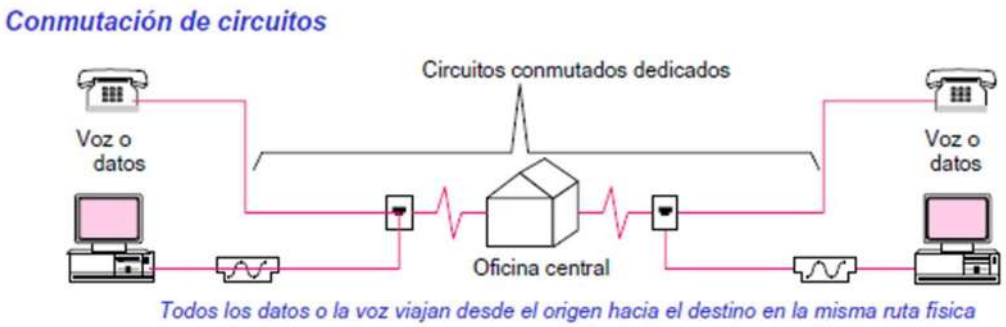


Ilustración 2: Red de conmutación de circuitos

Por otra parte las redes basadas en IP utilizan la tecnología de conmutación de paquetes, que usa la capacidad disponible de una forma mucho más eficiente y que minimiza el riesgo de posibles problemas como la desconexión. Los mensajes enviados a través de una red de conmutación de paquetes se dividen primero en paquetes que contienen la dirección de destino. Entonces, cada paquete se envía a través de la red y cada nodo intermedio o router de la red determina a dónde va el paquete. Un paquete no necesita ser enrutado sobre los mismos nodos que los otros paquetes relacionados. De esta forma, los paquetes enviados entre dos dispositivos de red pueden ser transmitidos por diferentes rutas en el caso de que se caiga un nodo o no funcione adecuadamente.

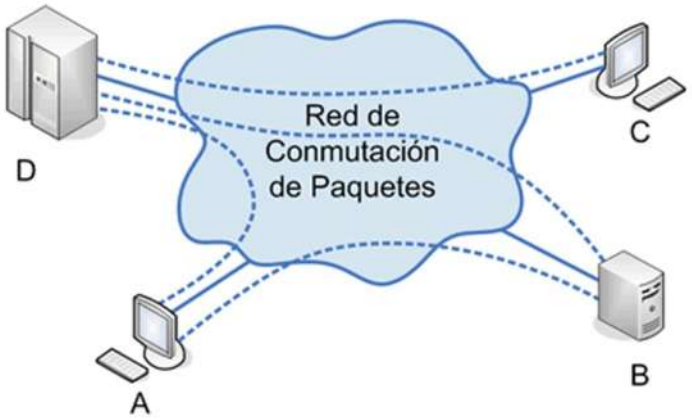


Ilustración 3: Red de conmutación de paquetes

Ha sido tan importante el auge de las redes que es posible afirmar y constatar que desde su aparición a la fecha, se han producido nuevos espacios públicos basados en la interacción de redes tanto sociales (Facebook) como de comunicación (Intranets en las Universidades); desarrollos de

redes basadas en el software libre para la creación de espacios de trabajo cooperativo, etc. ***(Halcón, 2006).***

Infraestructura de la Red de Área Local (LAN)

Las Redes de Área Local (Local Area Networks, LANs) se utilizan para conectar dispositivos de red relativamente próximos. Típicamente una LAN opera en un espacio limitado, como puede ser en un edificio de oficinas, en una escuela o en un domicilio. Las LANs sueles pertenecer y ser gestionadas por una única persona u organización. Utilizan también ciertas tecnologías de conectividad y a menudo algunos tipos de medios compartidos.

Una característica importante de las LANs es su topología, donde el término topología refiere al nivel al que están conectados los dispositivos a la red ***(Martínez, 2002).*** Podemos pensar en las topologías como las formas que puede tener la red. Las topologías de red pueden ser categorizadas en los siguientes tipos básicos:

- **La topología de bus** utiliza un medio de comunicación compartido, a menudo denominado "bus común", para conectar todos los dispositivos de la red. Un dispositivo que quiera comunicar con otro enviará paquetes a través del bus. Todos los dispositivos conectados al bus recibirán el paquete enviado pero sólo el que es el receptor aceptará y procesará estos paquetes.

Ilustración 4: Topología de bus

- **La topología de anillo** está estructurada de la misma forma en la que cada dispositivo de la red tiene exactamente dos vecinos para los propósitos de comunicación. Todos los paquetes viajan en la misma dirección dentro del anillo.

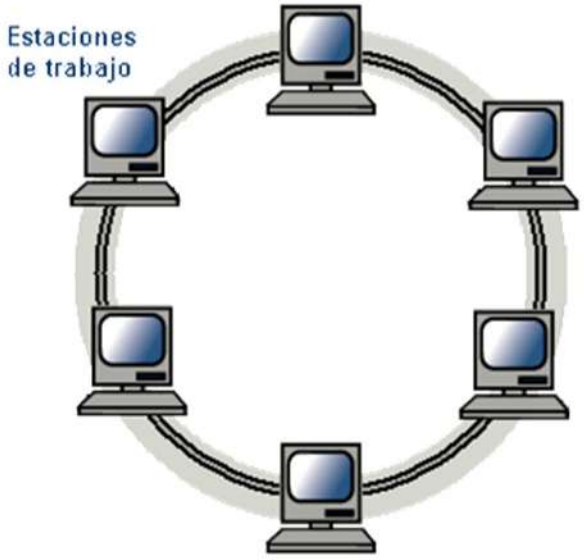


Ilustración 5: Topología de Anillo

- **La topología de estrella** establece un centro lógico de comunicaciones al que están directamente conectados todos los dispositivos de la red. Cada dispositivo necesita un cable separado al punto central y consecuentemente todos los paquetes viajarán a través de centro de comunicación.

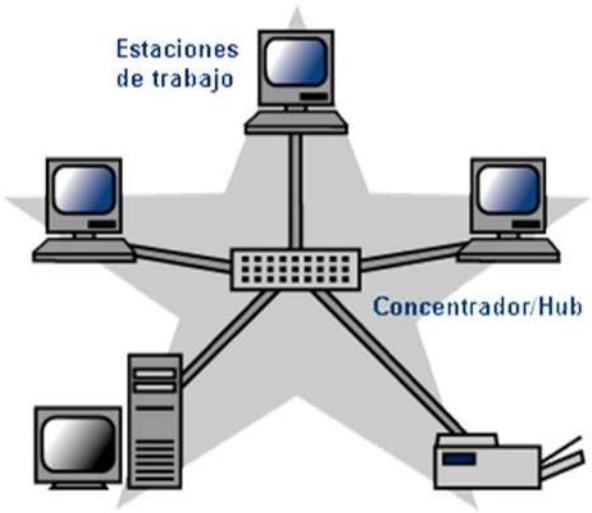


Ilustración 6: Topología de Estrella

- **La topología de árbol** combina características de la topología de estrella con la de bus. Consiste en un conjunto de subredes estrella conectadas a un bus.

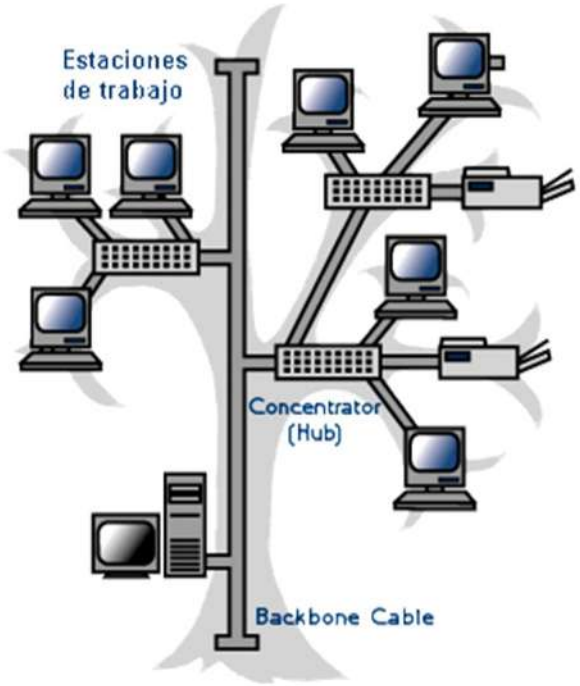


Ilustración 7: Topología de Árbol

Existen diferentes protocolos que pueden utilizarse conjuntamente a cualquier topología de red. Además de identificar los estándares de comunicación entre los dispositivos de la red, el protocolo establece las especificaciones técnicas necesarias para la transmisión de datos en una red. Para transmitir un mensaje a otro dispositivo de la red, el mensaje se divide en paquetes de datos. Estos paquetes después serán transmitidos a través del medio de comunicación y se re-ensamblarán de nuevo cuando termine la recepción.

El protocolo Internet (IP)

Internet es un concepto inseparable de los términos TCP/IP e IP. Se trata del protocolo de transmisión de internet que regula el intercambio de datos entre computadoras (***Lackerbauer, 2001)***.

El protocolo Internet (IP) es el protocolo de red más popular del mundo. IP permite que se transmitan los datos a través y entre redes de área local, de ahí su nombre, inter-net protocol (protocolo entre redes). Los datos viajan sobre una red basada en IP en forma de paquetes IP (unidad de datos). Cada paquete IP incorpora una cabecera y los datos del propio mensaje, y en la cabecera se especifican el origen, el destino y otra información acerca de los datos.

IP es un protocolo sin conexión de manera que cada paquete se trata como una entidad separada, como un servicio postal. Todos los mecanismos para asegurar que los datos enviados llegan de forma correcta e intactos los proporciona los protocolos de más alto nivel dentro de la suite.

Cada dispositivo de red tiene al menos una dirección IP que lo identifica de forma única del resto de dispositivos de la red. De esta manera, los nodos intermedios pueden guiar correctamente un paquete enviado desde el origen a su destino.

El protocolo de Transporte

El Protocolo de Control del Transporte (Transport Control Protocol, TCP) es el protocolo más común para asegurar que un paquete IP llega de forma correcta e intacto. TCP ofrece la transmisión fiable de datos para los niveles superiores de aplicaciones y servicios en un entorno IP. TCP proporciona fiabilidad en la forma de un envío de paquetes de extremo a extremo orientado a conexión a través de una red interconectada.

El protocolo Internet proporciona una adaptación a los protocolos de nivel de transmisión y ofrece una arquitectura estandarizada para las comunicaciones a través de una colección de LAN interconectadas. Esto representa un avance tremendo, principalmente por ser capaces de conectar y comunicar a través de diferentes conexiones físicas de una forma estandarizada. Con IP como base, el Protocolo Internet ofrece el tercer bloque de construcción para unas comunicaciones digitales idóneas, el Nivel IP.

Internet

Internet se ha convertido en el factor más potente que guía el proceso de convergencia. Se ha convertido en parte inherente de nuestra vida actual (***John R. Levine, 2010)***. Esto es debido principalmente al hecho de que la suite del protocolo Internet se ha erigido como un estándar utilizado en casi cualquier servicio. La suite del protocolo Internet está compuesto principalmente por el protocolo Internet (IP), y el protocolo de control del transporte (TCP); consecuentemente el término TCP/IP refiere a la familia del protocolo al completo.

Las redes basadas en IP tienen una gran importancia en la sociedad de la información actual. A primera vista esta tecnología puede parecer un poco confusa y abrumadora pero empezaremos por presentar los componentes de red subyacentes sobre los que está construida esta tecnología.

Internet, también llamado Autopista de la información, Net, Ciberespacio..., designa un conjunto de redes informáticas relacionadas entre sí, cuya finalidad es permitir que los usuarios de todo el mundo puedan comunicarse entre sí. Se trata del conjunto de redes interconectadas más vasto del mundo. Internet, al contrario de la mayoría de redes, es una red abierta: todo el mundo puede conectarse a ella para disfrutar de sus servicios.

La red internet no se concibió teniendo en mente la posibilidad de que se convirtiera en lo que ha llegado a ser. Inicialmente se pretendía ser una infraestructura que permitiera conectar entre si agencias dispersas del gobierno estadounidense en el caso de un fallo catastrófico de los sistemas de comunicación tradicionales, primando por tanto la conectividad frente a otros parámetros como la seguridad, la capacidad o la eficiencia ***(Aníbal R. Figueiras Vidal, 2002).***

Internet no pertenece a nadie. Está regido por organismos que definen sus normas técnicas.

Cada porción de esta red corresponde a un organismo, público o privado, que financia su funcionamiento.

Historia

En 1969, el departamento estadounidense de defensa decide desarrollar una red experimental que permita el intercambio de información entre centros de investigación y desarrollo alejados entre sí y que funcione sin interrupciones, incluso aunque la red sufra una destrucción parcial. Esta nueva red se llamó ARPANET.

La descentralización de las transmisiones debía ser la base de dicha red: cada vez que una línea de comunicación no pueda utilizarse, los equipos buscan una nueva ruta para transferir los datos.

En 1972, como resultado de una conferencia sobre la posibilidad de intercomunicar todos las computadoras y todas las redes entre sí, nace el protocolo TCP/IP.

A principios de los ochenta, al intercomunicar varias redes entre sí, ARPANET se convierte en INTERNET (International Network).

Un cierto número de empresas de tamaño medio y de particulares con pasión por la comunicación, decidieron unirse para crear unos servicios privados, lo que dio lugar a los proveedores privados de acceso a Internet, llamados «Provider».

Con la aparición, en 1992, de la Web y otras herramientas de sencillo manejo, la red ha crecido a una velocidad vertiginosa.

Los principales servicios de Internet

Servicios web es el nombre dado a un conjunto de tecnologías que permite que algunas aplicaciones se comuniquen con otros servicios web y puedan crear conexiones capaces de mantener la funcionalidad y acceso a los datos ***(Bidgoli, 2004)***.

- ✓ **Correo electrónico:** este servicio, también llamado e-mail, se utiliza para enviar y recibir mensajes o archivos en una red. Para ello, es necesario utilizar un programa de correo electrónico (Mozilla Thunderbird).
- ✓ **Búsqueda de documentación:** Internet permite descubrir el mundo a través de textos, imágenes, vídeo, sonido... que podemos encontrar navegando por la Web.
- ✓ **Transferencia de archivos:** Internet permite recibir (descargar) y enviar archivos que contengan texto, imágenes, vídeo, sonido, programas. Esta transferencia de información es posible gracias al protocolo FTP (File Transfer Protocol).
- ✓ **Grupos de noticias o foros de discusión:** permiten entablar conversaciones libres o temáticas sobre asuntos muy diversos. La transferencia de información se realiza por medio de Usenet, una red estrechamente vinculada con Internet.
- ✓ **Mensajería en directo:** gracias al protocolo de comunicación IRC, Internet permite conversar en tiempo real y por escrito con uno o varios usuarios de cualquier parte del mundo.
- ✓ Actualmente, gracias al desarrollo de nuevas tecnologías, están apareciendo nuevos servicios: blogs, wikis, podcastings, fuentes RSS, posibilidad de utilizar una hoja de cálculo o un programa de tratamiento de textos en línea... Éstos son los principales servicios que ofrece la Web 2.0.

Además de estos existen muchos otros servicios que tienen la misma base, el internet y que son de mucha utilidad.

¿Que son las VPN?

Las Redes Privadas Virtuales (VPN – Virtual Private Networks) plantean una solución que permite conectar diferentes y variados dispositivos con la red local (LAN – Local Area Network) de una empresa creando un camino físico que proporciona mecanismos de autenticación, encriptación y el uso de túneles para las conexiones.

Actualmente las VPN son muy usadas utilizando protocolos que operan sobre medios cableados como Frame Relay, RDSI, ADSL, el sistema telefónico convencional, pares aislados de cobre, entre otros, aunque pocas son las implementaciones que usan tecnologías inalámbricas.

Una de las necesidades más importantes de toda organización, es la de poder compartir información, y más aún, si se trata de organizaciones que poseen sucursales en diferentes zonas y/o secciones que no se encuentran en el mismo entorno físico.

Inicialmente, las compañías con diferentes sucursales, tenían redes LAN independientes en cada una de ellas, pero con el paso del tiempo, la información crece cada vez más y por consiguiente, la administración de esta, se hace cada vez más dispendiosa; debido a esto, las empresas se han visto en la necesidad de que sus redes LAN trasciendan más allá del ámbito de la oficina, de que su información este centralizada y sea más fácil de mantener, dada esta necesidad, las grandes organizaciones empezaron a implementar sistemas de acceso remoto entre sus sucursales a través de líneas dedicadas, a muy altos costos, privilegio del que se veían privadas las organizaciones de menor tamaño y con recursos técnicos y económicos más escasos.

Las últimas alternativas de comunicación, como ADSL, han hecho que la desventaja operativa desaparezca, permitiendo ya a pequeñas y medianas empresas disponer de su propia red de comunicación privada. Ahora, las matrices y sucursales disponen de su propia red de comunicación privada. Ahora, pueden intercomunicarse y compartir información de forma sencilla y segura, con inversiones muy inferiores a las de hace muy poco tiempo.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras sin pensar en la seguridad de la información; pero internet no es seguro, por lo tanto las VPN usan protocolos especiales que permiten encriptar información y permitir únicamente a la persona autorizada desencriptar esa información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

Una Red Privada Virtual (VPN – Virtual Private Network) es un sistema para simular una red privada sobre una red pública, por ejemplo, internet. La idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

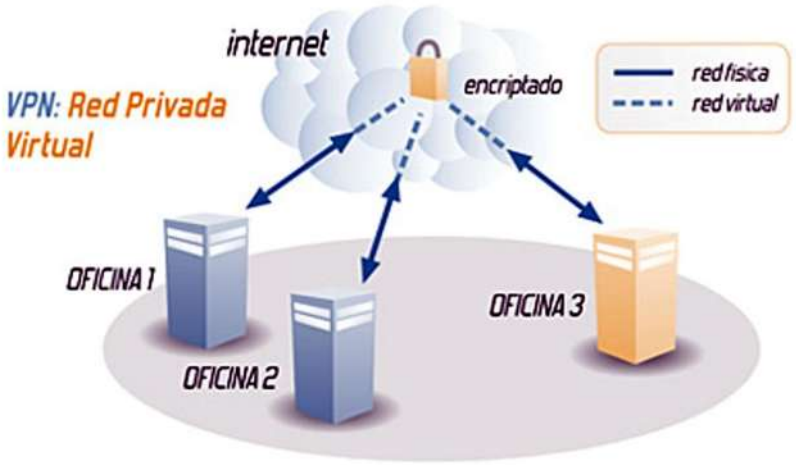


Ilustración 8: Esquema de una VPN

Las VPN también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en la LAN dentro de una oficina de la empresa donde se implementa la VPN, a este tipo de implementación se le conoce como VPN móvil (MVPN). Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, cobradores, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autenticación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

El principio de funcionamiento para el proceso de túnel es el siguiente: para enviar un paquete IP a una Pc2, una Pc1 construye el paquete que contiene la dirección IP de la Pc2, lo inserta en un marco Ethernet dirigido al enrutador multiprotocolo que enlaza la sucursal1 y lo pone en el Ethernet. Cuando el enrutador multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la WAN, y dirige este último a la dirección de la WAN del enrutador multiprotocolo que enlaza con la Oficina Central. Al llegar ahí, el enrutador retira el paquete IP y lo envía a la Pc2 en un marco Ethernet.

La WAN puede visualizarse como un gran túnel que se extiende de un enrutador multiprotocolo a otro. El paquete IP simplemente viaja de un extremo del túnel al otro. Solo el enrutador multiprotocolo tiene que entender los paquetes IP y WAN.

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. La tecnología de túneles (Tunneling) es un modo de transferir datos entre dos redes similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado (encapsulación), ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

El uso de la encriptación en la conexión VPN puede ser necesario en aquellos casos en los que la información que se vaya a pasar por el túnel sea sensible y requiera privacidad. La conexión encriptada VPN requiere de bastantes recursos tanto en el servidor del túnel como en la computadora cliente de VPN a parte de requerir la instalación de software especial en el cliente.

Existen muchas aplicaciones y programas que ya hacen dicha encriptación y el encriptar el túnel VPN no nos aporta seguridad adicional. Aplicaciones tales como el correo seguro leído por medio de una interfaz web seguro o una conexión SSH a una maquina multiusuario son suficientemente seguros para no requerir la encriptación adicional, a parte que al encriptar entre el servidor de la aplicación y el cliente de la misma conexión es absolutamente segura en todo su recorrido, mientras que en una conexión VPN segura la encriptación solo tiene lugar entre el servidor del túnel y el cliente VPN y la conexión entre el servidor de túneles, y el servidor de la aplicación se realiza sin encriptación.

En términos generales, las VPN ayudan a conectarse de forma segura a las oficinas a los usuarios remotos y socios comerciales. Las VPN se han convertido en la principal solución para la conectividad remota para empresas de cualquier tamaño, utilizando el acceso de terceros a Internet y de manera económica.

Las soluciones basadas en VPN proporcionan seguridad excepcional a través de tecnologías de cifrado y autenticación que protegen los datos en tránsito del acceso no autorizado y los ataques.

Una VPN ayuda a los negocios a:

- El uso de comunicaciones de alta seguridad, con los derechos de acceso adaptadas a los usuarios individuales.
- Agregar rápidamente nuevos sitios o usuarios, sin aumentar significativamente la expansión de la infraestructura existente.
- Mejorar la productividad mediante la ampliación de las redes corporativas, aplicaciones y herramientas de colaboración.
- Reducir los costos de las comunicaciones y aumentar la flexibilidad.

Una VPN se puede crear mediante hardware o software.

Las creadas por hardware pueden conseguir un mayor rendimiento y a su vez son fáciles de configurar, pero sin embargo tienen más limitaciones que las creadas por software, ya que disponen de menos parámetros configurables.

Existe una gran variedad de productos que permiten la creación de VPN por hardware, como pueden ser los productos de Cisco, Linksys, Symantec, U.S. Robotics, D-link, etc.

Existen dos formas de crear una VPN por software. La primera es mediante las opciones que vienen en los propios S.O. como pueden ser Windows XP, Windows 2003 server, Windows Vista, GNU/Linux y Unix, aunque estas redes suelen ser algo limitadas. Y la otra opción, y más recomendable debido a sus características, es mediante aplicaciones de código abierto, como por ejemplo OpenVPN, OpenSSH, Vtun, Hamachi, FreeS/Wan, etc.

Dos de las tecnologías de VPN que están actualmente en uso son: **VPN de sitio a sitio y VPN de acceso remoto.**

VPN de Sitio a Sitio

Las VPN de sitio a sitio proporcionan una infraestructura WAN basada en Internet para ampliar los recursos de la red de sucursales, oficinas en casa, y los sitios de socios de negocios. Todo el tráfico entre sitios se cifra mediante el protocolo IPsec e integra las funciones de red tales como enrutamiento, calidad de servicio y soporte multicast.

Ilustración 9: VPN Sitio a Sitio

VPN de Acceso Remoto

Las VPN de acceso remoto se extienden a los datos, voz, o aplicaciones de vídeo para el escritorio remoto, emulando el escritorio de la oficina principal. Con este tipo de VPN, se puede proporcionar alta seguridad, acceso remoto personalizable a cualquier persona, en cualquier momento y en cualquier lugar, con casi cualquier dispositivo.

Se crea una experiencia de usuario remoto que emula el trabajar en el escritorio de la oficina principal.

Seguridad

Esta es la característica más importante de una VPN. Para garantizar la seguridad son necesarios los siguientes puntos:

- La integridad de los datos, es decir que los datos que llegan hasta el receptor no hayan sido alterados. Para ello se utilizan funciones de Hash. Las más usadas son Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA), siendo SHA más seguro, debido a que la longitud de la función de hash es mayor.
- La encriptación se consigue mediante el cifrado que permite que los datos puedan ser descifrados por el receptor y entenderlos correctamente. Esto es necesario ya que como los datos viajan por Internet, cualquier usuario malintencionado podría interceptarlos. Se utilizan algoritmos de cifrado como Data Encryption Standard (DES) que es un algoritmo que toma un texto en claro de una longitud fija de bits y

lo transforma mediante una serie de complicadas operaciones en otro texto cifrado de la misma longitud, Triple DES (3DES) y Advanced Encryption Standard (AES), que consisten en variaciones de DES. AES es el más seguro y utilizado hoy en día. No se entrará en detalle fondo este tipo de cifrados porque es muy complejo y se extendería demasiado.

- La autenticación, de forma que solo el destinatario sea el que recibe los datos. Se ha implantado mediante usuarios de los distintos S.O (sistemas operativos) y limitando el acceso de los programas utilizados sólo para nuestra red privada.

Los puntos anteriores son necesarios para la creación de una VPN, pero aún es posible aumentar la seguridad. Para ello:

- Utilizar una firma digital, de forma que el emisor no puede negar que él haya sido el emisor de la información (no repudio).
- Usar certificados de autenticación (claves de seguridad) para realizar la conexión.
- Revocar las claves de seguridad. Las claves deben ser generadas y renovadas cada cierto tiempo, de forma que al cambiar las claves se aumenta la seguridad de la red. Ya que en caso de que algún usuario malintencionado se apropie de una clave, al revocarla nuevamente, la clave anteriormente conseguida por ese usuario ya no le será válida. El administrador del Centro de Cómputo será el encargado de definir cada cuanto tiempo se deberán revocar las claves.

Los datos viajan encapsulados por el túnel, con una cabecera que contiene información sobre su destino y la ruta que debe tomar hasta llegar a él.

En una VPN cada cliente tiene una dirección IP de forma que esta dirección sólo podrá ser vista por los componentes de la VPN, y no podrá ser accesible desde fuera.

Análisis del software con las funcionalidades requeridas

OpenVPN

Con la llegada de Internet y la baja de costos en conectividad se desarrollaron nuevas tecnologías. Surgió entonces la idea de utilizar a Internet como medio de comunicación entre los diferentes sitios de la organización. Surge así la idea de las VPN's que son "Virtuales" y "Privadas". Virtuales porque no son redes directas reales entre partes, sino solo conexiones virtuales provistas mediante software sobre la red Internet. Además son privadas porque solo la gente debidamente autorizada puede leer los datos transferidos por este tipo de red logrando la seguridad mediante la utilización de modernos mecanismos de criptografía. Retomando el ejemplo anterior de una organización con cuatro sitios, ahora solo necesitamos cuatro conexiones a Internet en lugar de las seis dedicadas de antes. Además los que se conectan temporalmente, también lo hacen mediante una conexión a Internet, mucho más barata y accesible desde muchos lugares, como por ejemplo de cyber cafés ***(Feilner, 2006)***.

OpenVPN Technologies es una compañía privada con sede en Pleasanton, California, integra un conjunto de redes de vanguardia y tecnologías de software. OpenVPN Technologies ha diseñado e implementado un software de red virtual que proporciona servicios de comunicación segura,

confiable y escalable, no sólo cumple con los requisitos de la tradicional red privada virtual (VPN) del mercado, sino también frente a las exigencias de la nueva ola de servicios VPN web. OpenVPN, su galardonado producto de código abierto VPN, se ha establecido como un estándar de facto en el espacio de origen de red abierta, con más de 3 millones de descargas desde su creación. OpenVPN Technologies es el proveedor de servicios de próxima generación de comunicaciones seguras y escalables, la aplicación de su plan de negocio a través de alianzas estratégicas con proveedores de aplicaciones de software y la comercialización de su producto para mercado SMB a través de su sitio web OpenVPN que está experimentando más de 250.000 nuevos usuarios de las PYMES, perspectivas y de clientes al mes.

La creación con éxito del proyecto OpenVPN en 2002, se debe a Francis Dinha y James Yonan co-fundadores de OpenVPN Technologies, Inc. (OpenVPN Technologies I. , 2002).

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 encriptar 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.

Datos sobre OpenVPN

- La comunidad OpenVPN ha llegado a 5 millones de usuarios.
- Experiencia del Sitio web de OpenVPN de más de 500.000 visitas y 150.000 descargas al mes.
- Según www.alexa.com, el tráfico del sitio OpenVPN está un puesto más alto de Checkpoint y F5.
- OpenVPN se anunció como ganador de "Best SSL VPN" en 2007 uno de los mejores Premios de Software Abierto por InfoWorld (InfoWorld, 2007).
- lifehacker.com lista OpenVPN como la mejor herramienta VPN 2010 (Fitzpatrick, 2010).

Seguridad en VPN

Para encriptar datos se usan Passwords o claves de encriptación.

OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas 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.

Encriptación simétrica y claves pre-compartidas

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.

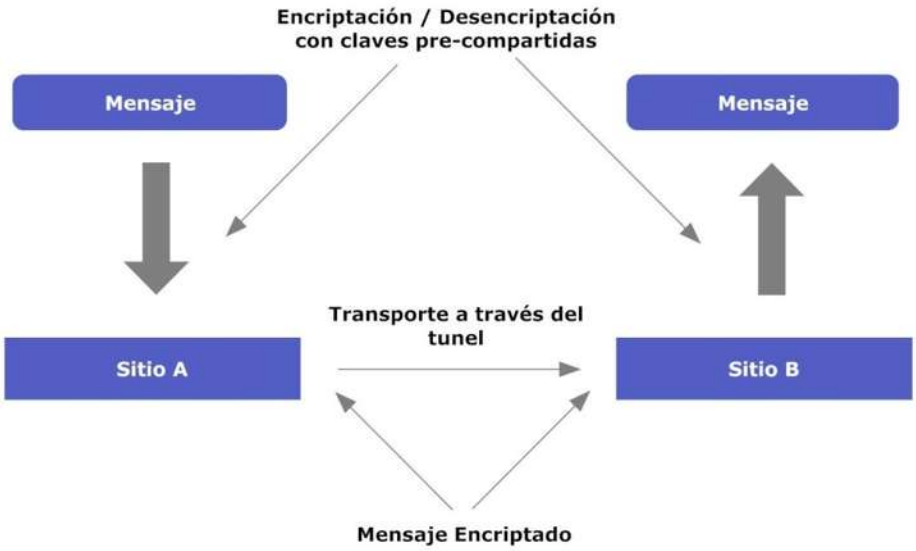


Ilustración 10: Clave pre compartida

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 aún no ha sido terminado.

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 esos algoritmos, todos aquellos conectados a Internet estarán comprometidos en forma instantánea.

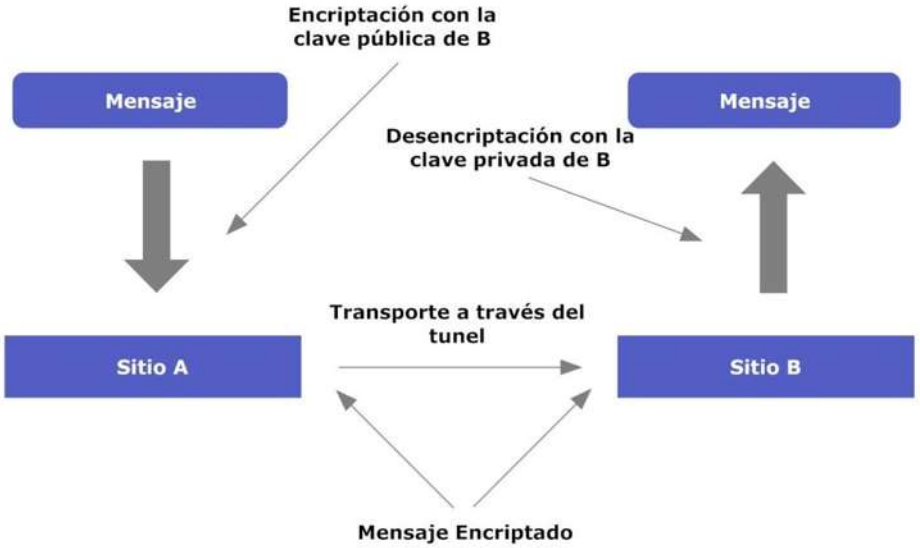


Ilustración 11: Clave asimétrica

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

Seguridad SSL/TLS

Las bibliotecas SSL/TLS son parte del software Open SSL que vienen instaladas en cualquier sistema moderno e implementan mecanismos de encriptación y autenticación basadas en certificados. Los certificados generalmente son emitidos por entidades de reconocida confiabilidad aunque también podemos emitirlos nosotros mismos y usarlos en nuestra propia VPN. Con un certificado firmado, el dueño del mismo es capaz de probar su identidad a todos aquellos que confíen en la autoridad certificadora que lo emitió.

Ventajas y Desventajas de OpenVPN

Ventajas: OpenVPN provee seguridad, estabilidad y comprobados mecanismos de encriptación 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 la PC remota 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 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.

Desventajas: No es IPsec-compatible siendo que justamente IPsec es el estándar actual para soluciones VPN. Falta de masa crítica. Todavía existe poca gente que conoce cómo usar OpenVPN. Aún no posee interfaz gráfica. Aunque esto para algunos pueda significar en realidad una "ventaja". Al día de hoy solo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

Logmein Hamachi

LogMeIn Hamachi permite establecer una conexión segura y fiable entre dos o más computadoras, además de poder utilizar archivos compartidos o enviar archivos de una PC a otra como si estuvieran conectados físicamente en la misma red local.

La conexión que establece LogMeIn Hamachi no se ve afectada por firewalls, routers u otros elementos presentes en la red, de hecho crea una "nueva" conexión.

LogMeIn Hamachi es un servicio VPN hospedado que conecta dispositivos y redes de forma segura, y amplía la conectividad de red de tipo LAN a usuarios móviles, equipos distribuidos y aplicaciones empresariales. Puede crear fácilmente redes virtuales seguras mediante solicitud a través de redes públicas y privadas. Hamachi se gestiona y mantiene de forma segura desde cualquier sitio a través de la web.

Hamachi es un sistema VPN de administración centralizada que consiste en un clúster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en las computadoras de los usuarios.

El software cliente agrega una interfaz de red virtual a la computadora que es utilizada tanto para interceptar el tráfico VPN saliente como para inyectar el tráfico VPN entrante. El tráfico saliente enviado por el sistema operativo a esta interfaz es entregado al software cliente, que lo cifra y lo autentifica y luego lo envía al nodo VPN de destino a través de una conexión UDP iniciada a tal efecto. Hamachi se encarga del tunelamiento del tráfico IP, incluido el broadcast (difusión) y el multicast (multidifusión). La versión Windows reconoce y tunela, además, el tráfico IPX.

Gestión basada en web

- **Redes mediante solicitud.** Permite crear y gestionar redes virtuales mediante solicitud según las necesidades de la empresa.
- **Instalación centralizada de software.** Es posible proporcionar software cliente de red virtual de manera rápida y sencilla a nuevas computadoras sin necesidad de desplazarse. Simplemente se envía a los usuarios finales un vínculo para que descarguen e instalen el cliente para participar en una red virtual específica.
- **Gestión y restauración de redes.** Posibilidad de gestionar y restaurar redes virtuales para usuarios finales con un solo clic, desde cualquier sitio a través de la web.

Opciones múltiples para redes gestionadas e instantáneas

- **Redes virtuales de puerta de enlace.** Permite proporcionar a los usuarios remotos acceso seguro a la red privada/LAN, incluidos los recursos que se encuentran en ella, desde una puerta de enlace centralizada de LogMeIn Hamachi sin modificar cortafuegos ni routers de red.
- **Redes virtuales de concentrador y radio**. Permite proporcionar a los usuarios remotos acceso seguro a computadoras específicas de la red, desde cualquier ubicación, sin modificar cortafuegos ni routers de red.
- **Redes de malla.** Brinda la posibilidad de conectar a todos los clientes de la red entre sí. Facilidad para crear de forma rápida y sencilla una simple red de malla virtual que permite que los equipos remotos se conecten directamente entre sí y poder ofrecer a los usuarios acceso de red básico a todos los recursos de red que necesiten.

Seguridad incorporada

- **Comunicaciones cifradas.** Comunicaciones seguras mediante el cifrado AES de 256 bits a través de redes públicas y privadas.
- **Controles de acceso centralizados**. Posibilidad de controlar el acceso y la utilización de la red, incluyendo la gestión de contraseñas, la autenticación y el bloqueo de red y la suscripción de red continuada.
- **Gestión de configuración de red /cliente**. Facilidad para configurar los ajustes predeterminados para redes individuales y clientes, con soporte para modos de interfaz de cliente mínimos, limitados o completos.

Como parte del compromiso de Logmein Hamachi en cuanto a la seguridad, empresas acreditadas e independientes de auditoría externa revisan continuamente sus centros de datos y códigos fuente para garantizar que se mantenga la confidencialidad de la información.

Todas las comunicaciones de los productos de LogMeIn utilizan algoritmos y protocolos estándar del sector para el cifrado y la autenticación. Nadie podrá ver ni tener acceso a los datos que se transmiten entre las computadoras, ni siquiera Logmein.

Arquitectura

La seguridad de LogMeIn Hamachi es de extremo a extremo: dos nodos de Hamachi intercambian información entre sí tras una autenticación mutua y un acuerdo de claves de sesión. Mientras que el tráfico de nodo a nodo (es decir, flujo VPN regular) suele evitar a los servidores de LogMeIn y se envía directamente de un punto a otro, incluso el tráfico que debe retransmitirse a través de un servidor se asegura y cifra en los terminales.

Autenticación

La autenticación, en resumen, es el proceso de verificación de identidades de terminales, usuarios y servidores. Este paso, al comienzo de una conexión, garantiza que los datos solo se intercambien entre las partes correctas.

La autenticación sirve para garantizar que se verifican las identidades de todos los integrantes de las redes Hamachi, desde los servidores de LogMeIn Hamachi hasta los nodos Hamachi.

Los servidores LogMeIn autentican los nodos de Hamachi con un par de claves RSA. Para iniciar sesión, el nodo envía un identificador de Hamachi y utiliza una clave privada para firmar el desafío del servidor. El servidor verifica la firma y autentica al cliente.

Los nodos de Hamachi autentican los servidores LogMeIn con un par de claves RSA. Cuando el nodo se conecta con el servidor, anuncia la clave que espera que tenga el servidor. Si el servidor posee la clave solicitada, comienza la secuencia de inicio de sesión.

Cifrado

El cifrado es un método que codifica y descodifica varios fragmentos de información para poder enviarlos de forma segura de un punto a otro.

Cuando cualquiera de las dos entidades intercambia datos entre sí, se produce un protocolo de intercambio de claves junto con la fase de autenticación obligatoria que se describe anteriormente. El protocolo de intercambio de claves es Diffie-Hellman con el grupo MODP de 2048 bits como se define en RFC 3526.

Una vez que se ha establecido una clave de sesión, se utiliza el cifrado AES-256-CBC para el cifrado y descifrado de datos, con el relleno estilo ESP como se define en RFC 2406.

Los paquetes se autentican con la variante HMAC-SHA-1-96 (RFC 2404) de HMAC-SHA1 (RFC 2104).

Los paquetes se enumeran para evitar ataques de retransmisión.

Administración

Todos los nodos de LogMeIn Hamachi tienen opciones de administración para ayudar a mantener la seguridad de las redes Hamachi. Las siguientes funciones están disponibles para las redes basadas en clientes:

- **Protección de contraseña:** solo los usuarios que conozcan la contraseña de red pueden unirse a la red.
- **Bloqueo de red:** evita que los usuarios se unan a una red en particular.
- **Aprobación de miembros:** los nuevos nodos envían una solicitud de admisión que debe aprobarse manualmente en el nodo del propietario de la red. Es posible verificar la huella dactilar de la clave RSA del nuevo nodo antes de la aprobación.
- **Expulsión / prohibición de miembros:** Expulsar o prohibir permanentemente un nodo de la red.

Administración centralizada

Con Hamachi, la forma recomendada de gestionar redes virtuales es con LogMeIn.com. Una cuenta (como una empresa) puede poseer varios nodos y varias redes. Los controles de red estándar, descritos anteriormente, también están disponibles a través de la interfaz Web. Con LogMeIn Central, es posible definir varios usuarios que pueden iniciar la sesión para administrar la(s) red(es).

Ventajas y Desventajas de Hamachi

Ventajas:

- **Sin necesidad de configuración.-** No es necesario abrir puertos, ni configurar routers ni desactivar Firewalls para poder conectarte con la VPN.
- Portabilidad. Funciona en varios sistemas operativos
- Facilidad de uso. Es realmente muy sencillo utilizar hamachi, ya que no requiere de mucho conocimiento para instalarlo, configurarlo y usarlo.

Desventajas:

- Está limitado a un cierto número de equipos conectados a la VPN en su versión gratuita.
- Es gratuito pero No es OpenSource.

Tabla comparativa de las dos opciones presentadas

Tabla 1: Comparativa entre opciones de VPN

Características	OpenVPN	LogMein Hamachi
Licencia	OpenSource bajo la licencia GPL	Freeware
Gratuito	Si	Si
Seguridad	Uno basado en claves estáticas pre- compartidas y otro en SSL/TLS usando certificados y claves RSA	Comunicaciones cifradas mediante cifrado AES de 256 bits. Controles de acceso centralizados. Gestión de configuración de red /cliente.
Portabilidad	Multiplataforma	Multiplataforma
Limite en la cantidad de equipos conectados	No	Si[1] Hamachi es gratis para uso no comercial y limitado a 16 computadoras por red. La versión comercial ofrece una retransmisión rápida, le permite conectar en red hasta 256 computadoras y está Sujeta al pago de una cuota de suscripción anual.
Configuración de Firewall	Utiliza solo un puerto del firewall	No
Soporte para proxy	Si	Si
Plataforma usada	Software	Software
Interfaz grafica	Si[2]	Si
Usabilidad	Facilidad, buena estructuración, tecnología modular y facilidad de configuración	No es necesario abrir puertos, ni configurar routers ni desactivar Firewalls para poder conectarte con la VPN.
Conexiones con IP dinámica	Trabaja con servidores de nombres dinámicos como DynDNS con reconexiones rápidas y transparentes	Sin problemas ya que la instalación del software proporciona conexiones sin problemas.
Control de trafico	Permitido	No permitido
Uso de Servidores	Servidores internos o externos. En el caso de usar un servidor interno se tiene la ventaja de acceder y modificar la configuración del mismo sin problemas.	Para que el producto funcione es necesaria la "mediación del servidor", el cual es operado por el vendedor.
Administración web	No	Si

[1] En la versión gratuita se presenta la limitante de permitir la conexión a un número reducido de equipos.
[2] Existe una interfaz gráfica para Windows, aunque carece de mucha funcionalidad. Dicha interfaz se incluye en la descarga del software de OpenVPN o a través de la dirección http://openvpn.se/

Capitulo III.- Datos de la Empresa

Giro

Caja Popular Lagunillas es una Sociedad de Ahorro y Préstamo que brinda a sus asociados servicios financieros a tasas competitivas.

Ubicación

Las instalaciones de Caja Popular Lagunillas se encuentran ubicadas en:

Tabla 2: Domicilio Fiscal

Calle:	**Nicolás Bravo**
Número:	335
Colonia:	Centro
Ciudad:	Lagunillas
Estado:	Michoacán
Teléfono:	434 342-4585
C. P.:	58450
e-mail:	cplagunillas_alianza@prodigy.net.mx
Página web:	http://www.cplagunillas.co.cc

Además cuenta con sucursales en los siguientes municipios:

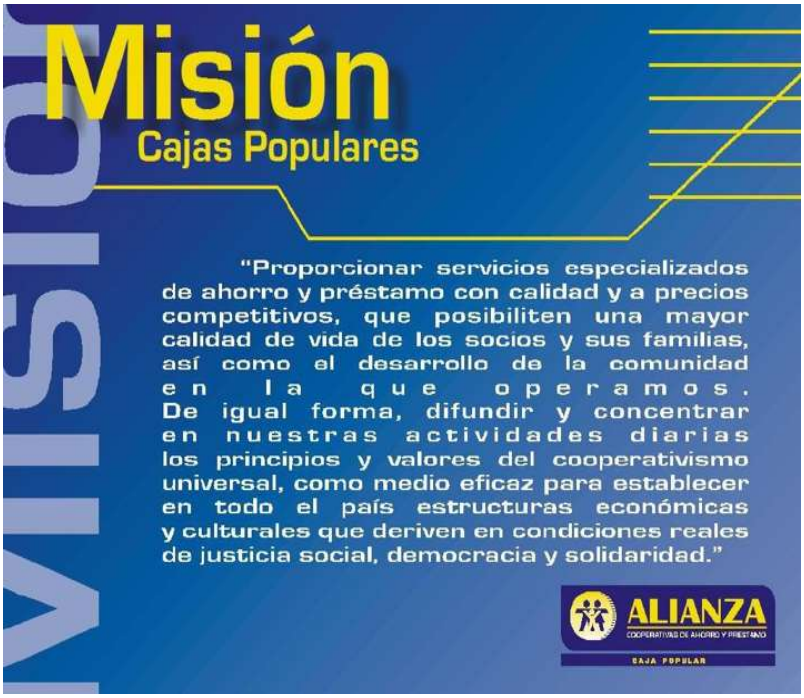
- **Erongarícuaro.-** Salazar # 28, Centro, Erongarícuaro, Mich., C. P. 61630, Tel: 434 344-0086, e-mail: suc_erongaricuaro@cplagunillas.mitmx.net.
- **Huiramba.-** Melchor Ocampo, esq. Privada de Allende, Centro, Huiramba, Mich., C. P. 61640, Tel: 434 343-5123, e-mail: suc_huiramba@cplagunillas.mitmx.net.
- **Morelia (3 Sucursales)**
  - **Morelia Centro.-** Miguel de Cervantes Saavedra # 103, Centro, Morelia, Mich., C. P. 58000, Tel/Fax: 443 317-8672, e-mail: cpmorcentro@prodigy.net.mx.
  - **Morelia Pedregal.-** Avenida Pedregal # 175, Colonia Emiliano Zapata, Morelia, Mich., C. P. 58148, Tel: 443 298-1993, e-mail: suc_pedregal@cplagunillas.mitmx.net.
  - **Morelia Siervo de la Nación.-** Avenida Siervo de la Nación # 1106, Colonia Libertad, Morelia, Mich., C. P. 58178, Tel: 443 299-7399, e-mail: cpsiervo07@prodigy.net.mx.
- **Tzintzuntzan.-** Avenida Lázaro Cárdenas # 2, Colonia Centro, Tzintzuntzan, Mich., C. P. 58440, Tel: 434 344-3433, e-mail: cptzin_5@prodigy.net.mx.
- **Opopeo.-** Galeana # 37, Opopeo, Salvador Escalante, Mich., C. P. 61820, Tel: 434 343-8438, e-mail: suc_opopeo@cplagunillas.mitmx.net.

Historia

- El Sistema Cooperativo surge en Inglaterra en el año de 1844 bajo un esquema de Cooperativas de producción rural.

- En Alemania se retoma el esquema de la Cooperación rural, pero lo convierten en sistema Cooperativo de Ahorro y Préstamo.
- Este sistema fue implantado en el Continente Americano en 1854, siendo Canadá el país más representativo de éxito de nuestro Continente.
- En el año de 1920 se crean en México las primeras Cajas Populares al cobijo de la Iglesia Católica, adoptando el sistema de las Cajas de Ahorro Alemanas, sin embargo las mismas perecieron debido a la persecución religiosa.
- Tiempo después, en 1951, se retomó en México el presente movimiento de Cajas Populares, por gestión de dos sacerdotes mexicanos que estudiaron las Cajas Populares de Canadá y de Estados Unidos y en especial el Movimiento de Educación Popular de Canadá. Al final del mismo año, quedaron constituidas las tres primeras Cajas Populares en la Ciudad de México.
- Nace en 1965, cuando el Padre Jesús Molina formo un grupo de 15 personas y un cuerpo Directivo el 19 de septiembre del mismo año.
- Al inicio no se contaba con personalidad jurídica.
- El Consejo de Administración era el encargado de dar el servicio, el cual únicamente era los días domingos ya que aún no se contaba con empleados. La prestación del servicio fue encomendado al Sr. Miguel Castejón Pineda.
- En el año de 1970 el Consejo de Administración contrato a la Sra. Laura Cerna Domínguez como secretaria para que el servicio se otorgara diariamente.
- Después se contrataron a las Sras. María Guadalupe Ponce Rodríguez y Martha Morales Chávez como secretarias.
- En el año de 1977 se nombró como Gerente al Sr. Miguel Castejón Pineda, quien se encargaba de llevar la contabilidad con anterioridad por ser el Tesorero del Consejo de Administración.
- De los primero 100 socios iniciales, aun contamos con la afiliación del Sr. Onésimo Piñón Chávez quien es el socio número 0000000071.
- En sus inicios la cooperativa solamente admitía socios del Municipio de Lagunillas.
- En sus inicios la cooperativa estaba unida a la Federación GUAMICH que contaba con afiliación de cajas en los estados de Guanajuato y Michoacán,
- Posteriormente la Federación cambio el nombre a Alianza y en la actualidad cuenta con una membrecía de 22 cajas.

Misión



Visión

Valores

Valor	Descripción
Autoayuda	El desarrollo social solo se puede lograr en unión con otras personas trabajando juntas para un mismo fin.
Autoresponsabilidad	Los miembros tienen a su cargo la promoción de su cooperativa así como garantizarle su funcionamiento e independencia pública o privada.
Democracia	Los cooperativistas participan democráticamente tomando decisiones y trabajando en conjunto.
Igualdad	Los miembros de una cooperativa tienen Derecho a participar, a ser informados, a ser escuchados, a tomar decisiones en forma igualitaria sin distinciones entre ellos.
Equidad	Se refiere a la forma en que se trata a los miembros dentro de la cooperativa, a la forma como se distribuyen las ganancias o riquezas con base a la participación, es decir, recibe más quien trabaja más y se compromete más.
Solidaridad	Los cooperativistas y las cooperativas se mantienen juntos, luchando por conseguir una mejor calidad de vida.

Filosofía (Principios)

Membrecía abierta y voluntaria

Las cooperativas son organizaciones voluntarias abiertas para todas aquellas personas dispuestas a utilizar sus servicios y dispuestas a aceptar las responsabilidades que conlleva la membrecía sin discriminación de género, raza, clase social, posición política o religiosa.

Control democrático de los miembros

Las cooperativas son organizaciones democráticas controladas por sus miembros quienes participan activamente en la definición de las políticas y en la toma de decisiones. Los hombres y mujeres elegidos para representar a su cooperativa responden ante los miembros. En las cooperativas de base los miembros tienen igual derecho de voto (un miembro, un voto), mientras en las cooperativas de otros niveles también se organizan con procedimientos democráticos.

Participación económica de los miembros

Los miembros contribuyen de manera equitativa y controlan de manera democrática el capital de la cooperativa. Por lo menos una parte de ese capital es propiedad común de la cooperativa. Usualmente reciben una compensación limitada, si es que la hay, sobre el capital suscrito como condición de membrecía.

Los miembros asignan excedentes para cualquiera de los siguientes propósitos: el desarrollo de la cooperativa mediante la posible creación de reservas, de la cual al menos una parte debe ser indivisible; los beneficios para los miembros en proporción con sus transacciones con la cooperativa; y el apoyo a otras actividades según lo apruebe la membrecía.

Autonomía e independencia

Las cooperativas son organizaciones autónomas de ayuda mutua, controladas por sus miembros. Si entran en acuerdos con otras organizaciones (incluyendo gobiernos) o tienen capital de fuentes externas, lo realizan en términos que aseguren el control democrático por parte de sus miembros y mantengan la autonomía de la cooperativa.

Educación, entrenamiento e información

Las cooperativas brindan educación y entrenamiento a sus miembros, a sus dirigentes electos, gerentes y empleados, de tal forma que contribuyan eficazmente al desarrollo de sus cooperativas. Las cooperativas informan al público en general -particularmente a jóvenes y creadores de opinión- acerca de la naturaleza y beneficios del cooperativismo.

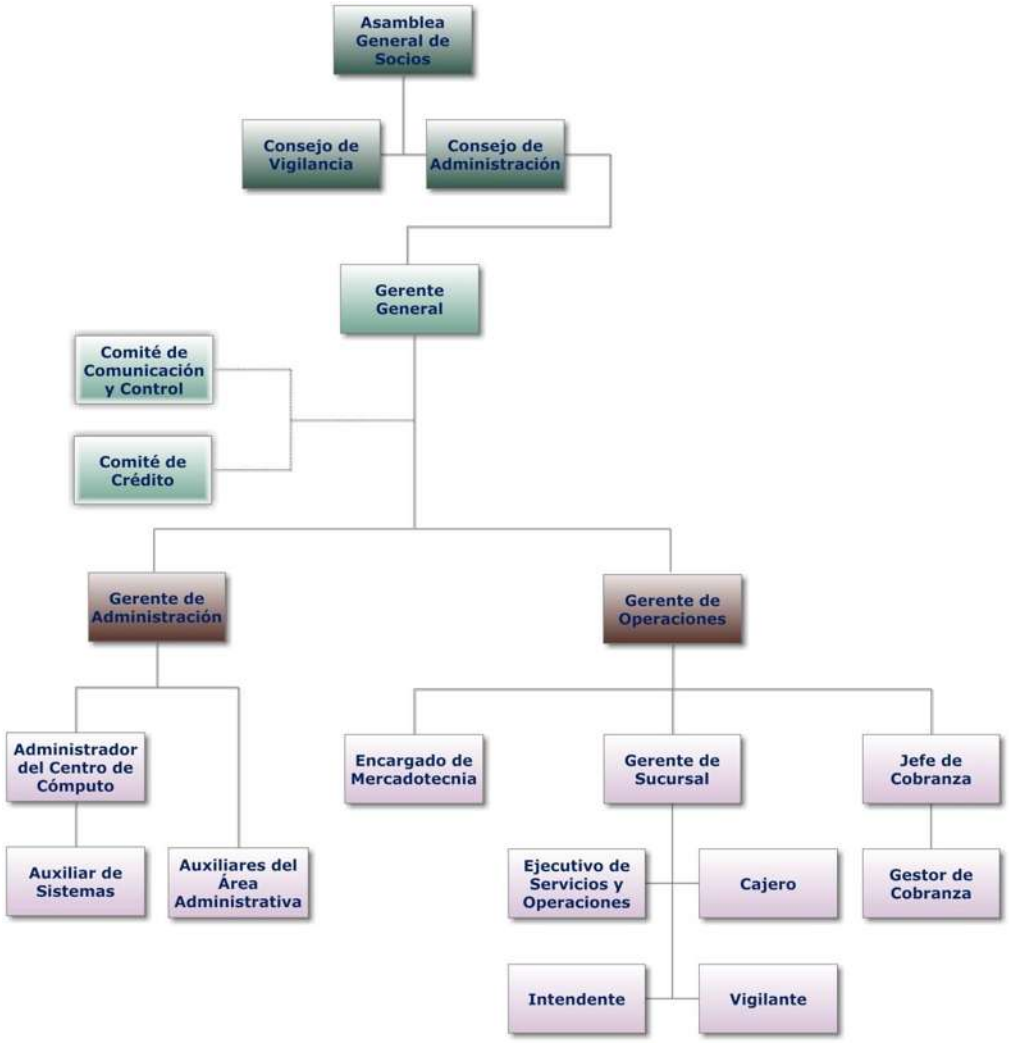
Cooperación entre cooperativas

Las cooperativas sirven a sus miembros más eficazmente y fortalecen el movimiento cooperativo, trabajando de manera conjunta por medio de estructuras locales, nacionales, regionales e internacionales.

Compromiso con la comunidad

La cooperativa trabaja para el desarrollo sostenible de su comunidad por medio de políticas aceptadas por sus miembros.

Organigrama general de la empresa



Datos Técnicos

Para la planeación, desarrollo e implementación del proyecto, se realiza un análisis de la infraestructura actual de la cooperativa, de manera que se detalle cómo se trabaja antes de la implementación del proyecto aquí señalado.

Caja Popular Lagunillas cuenta con la siguiente infraestructura[3] en las sucursales enlistadas en el proyecto:

- Sucursal Morelia Siervo de la Nación.
  - 4 computadoras cliente con sistemas operativos Windows (DD 80 GB, PIV o superior a 3Ghz, 2 GB o superior de RAM, S.O. Windows XP o Superior)[4].
  - 1 PC de escritorio con instalación de SO Windows Server 2003 o superior como servidor de base de datos SQL Server.

[3] Todas las computadoras, switches y servidores son marca Dell
[4] Estas son las características generales de todos los equipos.

- 1 Switch gigabit (10/100/1000) de 8 puertos.
- Internet de banda ancha infinitum de 2 MB contratado al proveedor Telmex.

- Sucursal Morelia Centro.
  - 4 computadoras cliente con sistemas operativos Windows (DD 80 GB, PIV o superior a 3Ghz, 2 GB o superior de RAM, S.O. Windows XP o Superior).
  - 1 PC de escritorio con instalación de SO Windows Server 2003 o superior como servidor de base de datos SQL Server.
  - 1 Switch gigabit (10/100/1000) de 8 puertos.
  - Internet de banda ancha infinitum de 2 MB contratado al proveedor Telmex.
- Oficina Matriz.
  - 21 computadoras cliente con sistemas operativos Windows (DD 80 GB, PIV o superior a 3Ghz, 2 GB o superior de RAM, S.O. Windows XP o Superior)[5].
  - 3 Servidores con instalación de SO Windows Server 2003 o superior como servidor de base de datos SQL Server.
  - 1 Switch gigabit (10/100/1000) de 24 puertos.
  - 1 Switch Ethernet 3com (10/100) de 24 puertos.
  - Internet de banda ancha infinitum de 4 MB (4 Mb en descarga y 684 en subida) contratado al proveedor Telmex.

También se describe de manera general como está estructurada o definida la red de la cooperativa.

Actualmente cada sucursal así como la Oficina Matriz cuenta con instalaciones físicas en los edificios en donde se presta el servicio localizados en los domicilios detallados en este mismo documento.

En cada uno de los edificios, existen en sus sótanos habitaciones destinadas a albergar el hardware relacionado con la electrónica de red, aunque no se cuenta con espacio suficiente, solamente en la Oficina Matriz se cuenta con un "Site". En este Site hay instalados racks de comunicaciones y de servidores en los que se encuentra el patch panel que contiene los puntos de red de todos las computadoras del edificio en cuestión. Este patch panel va conectado a los switches (dispositivos electrónicos de interconexión de red). En las sucursales de Morelia, se tiene un área específica para los equipos de telecomunicaciones y red, aunque no se cuenta a la fecha con racks ni patch panel. Se está considerando la adecuación de un Site en cada sucursal para la instalación de racks. Como los edificios son de dos plantas, no es necesario poner en ninguna de ellas un nuevo armario con switches para evitar que la señal de red se atenúe, ya que los edificios no son muy altos y las distancias hasta el sótano no superan los teóricos 100 metros permitidos en este tipo de cableado de red UTP.

El cableado en los edificios es UTP categoría 5 y 6, aunque no es cableado estructurado.

A continuación se explican los rangos de IP's de cada sucursal:

- ✓ Oficina Matriz.-

[5] Realmente no es necesario detallar estos equipos ya que no interfieren con el desempeño de la VPN al estar conectados de manera local a través de la LAN, solamente se ponen como referencia, lo relevante de la infraestructura de la Oficina Matriz son los servidores y las telecomunicaciones.

- ✓ Sucursal Morelia Centro.-
- ✓ Sucursal Morelia Siervo.-

En cuanto a seguridad, no hay implantado ningún firewall a nivel de hardware, solamente se manejan firewalls incluidos en los ruteadores/módems que proporciona el proveedor del servicio de internet (Telmex) y un router Linksys que además filtra el acceso a páginas web.

La IP de los routers/módems es la puerta de enlace que usan las computadoras de cada sucursal para poder conectar a Internet y al resto de equipos.

Metodología existente de transmisión de la información

Caja Popular Lagunillas utiliza un Sistema de desarrollo propio o interno para el control y administración de los socios y sus diferentes cuentas, el cual está desarrollado en Visual Studio.

Dicho Sistema mantiene registros históricos de todos los movimientos (transacciones) realizados, así como el registro de los intereses de las cuentas tanto de captación como de crédito en una base de datos almacenada en un servidor para tal fin.

La base de datos es administrada mediante Microsoft SQL Server 2008.

Cada computadora cliente está conectada a un servidor que funge como Controlador de Dominio con active directory debiendo primeramente autenticarse en él para posteriormente poder acceder a los servicios de red.

El Sistema Institucional realiza el enlace a la base de datos mediante parámetros establecidos y una correcta configuración de los parámetros de la red, así como utilizando credenciales válidas para autenticación en SQL Server.

En la configuración del equipo cliente se debe establecer el nombre del servidor y la base de datos, así como también las direcciones IP dentro del segmento de red y el DNS para la resolución de los nombres de los equipos.

A grandes rasgos, el procedimiento de atención a socios es como el común de las instituciones de este tipo, el cual se describe de manera general a continuación:

1. El socio se presenta a en la entidad y consulta sus saldos con un ejecutivo.
2. Posteriormente se presenta en el área de cajas a realizar sus transacciones dependiendo de la cuenta en la que quiera realizarlas.
3. Si requiere de algún crédito, requiere de asistencia de un ejecutivo.
4. Realiza transacciones correspondientes o tramite de créditos.
5. Se le imprime, y entrega un comprobante.

Todo esto queda registrado en el Sistema antes descrito, pero al no contar con un enlace permanente con las sucursales sujetas del presente proyecto, la información de las ultimas transacciones que han realizado los socios pudiera decirse que ***"no se realizan en tiempo real"***, en estas sucursales, ya que cada sucursal cuenta con una base de datos independiente de la base de datos de la Oficina Matriz, empero debiendo actualizarse la base de datos de esta con la información de las ultimas transacciones realizadas en las sucursales diariamente.

Para realizar esta actualización, el Sistema cuenta con un módulo que llamaremos importación/exportación, el cual permite generar al término del día un archivo (cifrado claro está) que contiene todas las transacciones, movimientos, trámites, registros o como quiera llamársele que han realizado los socios en cada una de las sucursales, para lo cual se sigue el procedimiento siguiente:

1. Al término de las actividades diarias, un encargado genera un archivo de exportación con la información de las transacciones del día.
2. El encargado envía vía correo electrónico institucional al Administrador del Centro de Cómputo el archivo cifrado.
3. El Administrador del Centro de Cómputo importa el archivo en cuestión, el cual actualiza la base de datos de la Oficina Matriz agregando todos los registros de las transacciones realizadas en la sucursal.
4. Se realiza comparación de los Saldos en ambos sitios para corroborar que no existan diferencias por incoherencias al momento de la actualización de la base de datos.

Aunque a la fecha el procedimiento es totalmente efectivo al 100%, esto no evita que se pudieran presentar algunos inconvenientes como los que se detallan a continuación:

- Errores en la generación o en el cifrado del archivo de exportación/importación.
- Aplicación de movimientos en la sucursal posteriores a la generación del archivo de importación.
- Olvido por parte del encargado de la sucursal de enviar a tiempo el archivo de exportación/importación a la Oficina Matriz.
- Socios malintencionados podrían presentarse tanto en la sucursal como en la Oficina Matriz para tratar de realizar retiros de las cuentas con la intensión de duplicar el monto del retiro al no actualizarse en tiempo real la información.

Estos y algunos otros podrían ser los posibles problemas a presentarse y de hecho algunos ya se han llegado a presentar en la cooperativa.

Además de esto, se tienen otros inconvenientes al no contar con un enlace dedicado con las sucursales como son:

- La base de datos de las sucursales no está actualizada con la información de los socios de otras sucursales o la misma Oficina Matriz, ya que esta base de datos se actualiza solamente cada mes.
- Creación de una copia de la base de datos para restaurar en la sucursal cada mes.
- No es posible realizar transacciones a los socios en tiempo real.
- Deficiencias en la atención a los socios.
- Realización de procedimientos adicionales por ejemplo como para la autorización de algún crédito, ya que si se requiere autorizar alguno, se tiene que realizar una conexión externa a la base de datos de la sucursal.

A grandes rasgos esta es la situación actual de la cooperativa[6], la cual se presenta como fundamento para la implementación del presente proyecto de manera que demuestre la necesidad de crear y mantener una conexión permanente de las Sucursales con la Oficina Matriz.

Políticas de Planeación de la Cooperativa

Dentro del marco de regulación y operación de Caja Popular Lagunillas, se elaboran (en coordinación con la Federación de Cajas Populares Alianza) año con año las "Políticas de Planeación" para cada ejercicio con la finalidad de establecer los lineamientos a seguir para la mejora continua en el desempeño de las operaciones propias del giro de la empresa.

En dichas políticas se establece para cada área o departamento que conforma a la cooperativa, los procesos de mejora a ejercer durante el ejercicio con la intensión de lograr poco a poco la excelencia buscada por muchas empresas, para lo cual se realizan análisis FODA a nivel de la red Alianza y se determinan los aspectos en donde hace falta trabajar un poco más.

Desde hace algunos años, dentro de las "Políticas de Planeación" se establece que para lograr la mejora en los servicios, se deberá de contar con algún método de conectividad que permita mantener la información actualizada en tiempo real, dichos métodos pueden ser mediante VPN´s, Antenas de radio o microondas, Frame Relay, etc., además de que independientemente del método, se debe establecer también un método alternativo o de redundancia que supla al método principal en caso de contingencia.

Debido a lo anterior, queda justificado que la cooperativa requiere la propuesta que se plantea en el presente proyecto.

Casos de Éxito

Se desea hacer mención de una metodología implementada en la cooperativa desde hace algún tiempo como medida para mantener un enlace permanente de las sucursales con la base de datos de la Oficina Matriz, el cual se manejó a través de una infraestructura nueva basada en Atenas de Radio o Microondas y que en un principio funciono y atendió las necesidades de la cooperativa.

Dicho proyecto surgió también como respuesta a la necesidad de la cooperativa de un enlace permanente que proveyera a las sucursales con una conexión a la base de datos actualizada en tiempo real.

El proyecto estuvo primeramente a cargo de un proveedor de la ciudad de León, Guanajuato, quien instalo 4 antenas de microondas entre las sucursales que llamaremos Morelia Centro, Morelia Siervo y Morelia Pedregal, esta última conectada a la Oficina Matriz mediante un enlace dedicado mediante MPLS contratado al proveedor Telmex.

El método a grandes rasgos fue el siguiente de acuerdo a la memoria técnica presentada por el proveedor:

[6] No se presenta toda la información tal cual es por cuestiones de privacidad, seguridad y ética, pero se presenta la información relevante para la documentación del presente proyecto.

- Las antenas de Morelia Siervo y Morelia Centro conectan respectivamente con la sucursal de Morelia Pedregal a través de dos antenas colocadas en esta última sucursal con línea de vista enfocada a cada una de las primeras dos.
- La infraestructura empleada maneja antenas de Capa 3 con capacidad de ruteo, switch gigabit y torres de hasta 18 metros de altura colocadas en el techo de cada sucursal en cuestión.
- La sucursal de Morelia Pedregal cuenta con un ruteador marca Teldat que se encarga de realizar la conexión a la Oficina Matriz con otro ruteador marca Cisco, mismo que conecta a la LAN y por consiguiente a la base de datos de socios.
- Una vez conectadas todas las antenas, se establece "ruteo" usando como intermediario el ruteador Teldat de la sucursal Morelia Pedregal, para que este encamine todos los datos hacia el servidor de la base de datos de la Oficina Matriz.

Durante alrededor de dos años, este método satisfizo las necesidades de la cooperativa aunque con sus consiguientes fallas mismas que se detallan a continuación:

- Lentitud en la conexión a la base de datos al pasar por varios medios de comunicación (antenas, ruteadores, switches).
- La más fuerte de todas, cada temporada de lluvias, se tenían bastantes problemas debido a que este tipo de equipos (antenas) dependen en gran medida de que exista un clima despejado y cuando se presentaban algunos vientos, lluvias o simplemente estaba nublado, se reducía considerablemente la calidad de la transmisión e incluso se llegaba a perder la conexión volviendo a establecerse esta una vez que terminaba de llover.
- Cuando se requería de soporte por parte del proveedor, tenían que pasar en ocasiones varios días para que se pudiera presentar, ya que el traslado desde la ciudad de León, Gto., hacía difícil la solución rápida de los problemas que llegasen a presentarse.
- También con motivo de las distancias, el costo se hacía más elevado ya que había que pagar viáticos al proveedor que en ocasiones tenía que quedarse más de un día solucionando el problema.

Varios de estos inconvenientes obligaron a la cooperativa a buscar algún proveedor local que diera soporte en caso de problemas y hasta en una ocasión fue necesario el reemplazo de las antenas debido a la falla total que sufrieron, pero el escenario fue prácticamente el mismo.

Otro caso de éxito fue la contratación del servicio basado en MPLS ofrecido por el proveedor Uninet filial de Telmex, mediante el cual se mantiene un enlace dedicado con un ancho de banda fijo y estable los 365 días del año, mismo que se contrató para otras dos sucursales diferentes a las del presente proyecto.

Dichos enlaces han estado funcionando de manera continua y eficiente, proveyendo a la cooperativa del tipo de conexión que satisfaga sus necesidades. El único inconveniente es el alto costo de dicho servicio, ya que mensualmente se está pagando alrededor de $ 25,000.00 lo que hace por demás difícil el mantener este tipo de enlaces en todas las sucursales.

Capitulo IV.- Metodología e implementación

Planeación para la implementación

El proyecto aquí descrito contiene varios elementos que requieren de un análisis anterior a su implementación, es por ello que a continuación se detalla la manera en que se estructurara el trabajo:

1. Analizar la infraestructura y su utilidad para el presente proyecto. Se verificara si la implementación de la VPN funcionara con la infraestructura actual.
2. Análisis de software gratuito y OpenSource con las funcionalidades requeridas. Se analizaran máximo 3 sistemas diferentes que permitan realizar la VPN sin costos elevados o inexistentes de ser posible.
3. Análisis de la seguridad de dichos sistemas frente a ataques externos. Se estudiarán los puntos débiles, y la forma de mejorarlos.
4. Instalación de la VPN, en la que se tendrán que analizar los pros y contras de las distintas opciones disponibles. Se deberá decidir el programa a usar.
5. Potenciar y optimizar los recursos de cada computadora con la VPN. Al finalizar el trabajo, se deberá establecer una red privada virtual segura que permita maximizar los recursos de cada computadora.

Planeación del proyecto

Número	Actividad	Recursos	Inicio	Fin	Duración en días	2011		
						Agosto	Septiembre	Octubre
1	Analizar la infraestructura y su utilidad para el proyecto		25/8/2011	31/8/2011	5			
2	Análisis de software gratuito y OpenSource con las funcionalidades requeridas		1/9/2011	10/9/2011	7			
3	Análisis de la seguridad de dichos sistemas frente a ataques externos		11/9/2011	17/9/2011	5			
4	Instalación de la VPN, en donde se tendrán que analizar los pros y contras de las distintas opciones disponibles.		18/9/2011	24/9/2011	5			
5	Potenciar y optimizar los recursos de cada computadora con la VPN		25/9/2011	30/9/2011	5			

Ilustración 12: Diagrama de Gantt para las actividades

Instalación del Sistema Seleccionado

Como objetivo principal se pretende realizar en enlace dedicado estable y económico mediante VPN que permita realizar transmisión de datos entre la Oficina Matriz de Caja Popular Lagunillas y sus sucursales.

Este enlace deberá permitir que el Sistema/Software institucional realice conexión a la base de datos SQL Server de la cooperativa y acceda a la información, además de realizar las funciones principales de Insertar, actualizar y eliminar datos a través del Sistema antes mencionado.

Debido a la comparativa realizada con anterioridad, el sistema seleccionado para la implementación del presente proyecto es OpenVPN, ya que presenta características que satisfacen las necesidades de la cooperativa en cuanto al establecimiento de una VPN, tanto por la

infraestructura, los requisitos necesarios de instalación, el tipo de software (OpenSource) y por último aunque no porque sea lo correcto, el costo de la solución.

Es de software libre, es decir, puede ser usado, copiado, cambiado/mejorado y redistribuido libremente. No hay que confundirlo con software gratuito ya que no es obligatorio que todo software libre sea gratuito. Sin embargo OpenVPN también es gratuito. Todo esto hace que esté en continua mejora, ya que millones de personas lo utilizan diariamente en el mundo, por lo que se podrá disponer de futuras actualizaciones de una herramienta a la que se tendrá acceso de manera fácil y gratuita. Es de fácil uso y configuración para usuarios inexpertos, respecto a otras opciones, como puede ser el uso del protocolo IPSEC, que aunque es uno de los más conocidos (el estándar para crear una VPN), es más complejo y requiere mayor experiencia para su uso.

OpenVPN es un software basado en SSL/TLS que permite crear VPN LAN to LAN, VPN de acceso remoto y VPN interna (para redes inalámbricas). TLS está desarrollado a partir de SSL, que en un principio solo se usaba para aplicaciones Web. Esto hizo que se estudiaran profundamente los problemas que tenían, y hoy en día su uso ya no está limitado exclusivamente a aplicaciones Web. Además esto ha permitido que se utilice para la autenticación e intercambio de claves.

Es un software para crear redes seguras en la capa 2 o 3 del modelo OSI (según se use: Túnel o Bridge). Por tanto un cliente no podrá realizar una conexión al servidor VPN mediante un navegador Web, ya que OpenVPN no opera en la capa 7 (Aplicación) de la pila OSI.

Por cuestiones de seguridad, administración y costos, se opta por manejar un servidor interno, ya que se cuenta con el equipo adecuado.

Requisitos de Instalación de OpenVPN

OpenVPN utiliza los controladores virtuales TUN/TAP para establecer el túnel entre los dos extremos. Con una interfaz de red virtual se pueden obtener varias direcciones IP's con una sola tarjeta de red física.

OpenVPN para implementar una VPN utiliza el espacio de usuario y enlaza una interfaz de red virtual punto a punto llamada "tun", con otra interfaz de red virtual punto a punto ("tun") remota, como si fuera una línea dedicada entre los dos puntos. A una interfaz virtual se le puede aplicar reglas, firewall, rutas, etc., como si fuera una tarjeta de red física Ethernet instalada en la máquina. El funcionamiento del interfaz virtual "tun" es que si desde una máquina se quieren enviar datos a otra, primero se copian los datos desde el interfaz virtual hasta el socket de red del S.O., se envían los datos, se reciben en el socket de red del S.O. de la otra máquina, y se pasan los datos a la interfaz virtual.

Se le llama "tap" cuando trabaja en modo bridge o puente, emulando a un adaptador de red Ethernet en lugar de una interfaz punto a punto, como si hubiera una red Ethernet entre los dos extremos.

Se hará una explicación de la instalación realizada tanto en el servidor, como en los clientes con Windows, junto a imágenes de apoyo. Se modificaran los archivos de configuración que vienen por default, ya que será necesario modificarlos a nuestras necesidades.

Como ya se ha comentado anteriormente, OpenVPN es un software libre, y por tanto se puede descargar directamente desde su página Web: http://openvpn.net. Existe también un manual de OpenVPN y también hay disponible una sección de FAQ (Frequently Asked Question – preguntas más frecuentes), y un foro para resolver dudas, etc.

Los requisitos son:

- ✓ Soporta las versiones 2000, XP y Vista de Windows.
- ✓ Soportar los drivers TUN/TAP. Casi todas las versiones de Linux con un kernel superior o igual a 2.4, soporta estos drivers. El problema es si se tiene alguna versión de Linux con Kernel inferior a 2.4, o un kernel que se haya modificado y no se le haya dado soporte para estos drivers. Para solucionar esto, se puede instalar la aplicación VTUN disponible en http://vtun.sourceforge.net/tun.
- ✓ Será necesario tener instaladas las librerías Open SSL, en caso de querer usar algún tipo de cifrado, ya sea simétrico o asimétrico. Es muy recomendable tener instalada esta librería y usar algún tipo de cifrado (mucho más seguro el asimétrico). En caso de no tener instaladas dichas librerías, se pueden encontrar en: http://www.openssl.org. Implementación de una red privada virtual para 32 el control remoto de equipos de laboratorio.
- ✓ En caso de querer usar la compresión de datos en tiempo real, se necesita tener instaladas las librerías LZO. En caso de necesitarla se puede encontrar en la Web: http://www.oberhumer.com/opensource/lzo.

Instalación de OpenVPN

La instalación de OpenVPN se realizó primeramente en un servidor que será el servidor de la VPN y en él se crearon los certificados y las claves de acceso.

Posterior a la instalación del servidor, cada computadora que se conectó al servidor de VPN también fue provista con el software de OpenVPN.

La instalación del software es idéntica tanto en el servidor como en los clientes, la única variación es la configuración que se realice en cada uno.

El proceso de instalación de OpenVPN es realmente sencillo, primeramente de descargo el programa desde la página del producto en la siguiente dirección: http://www.openvpn.net/index.php/open-source/downloads.html

Una vez en el sitio, se debe descargar el programa de instalación para Windows como se muestra en la Ilustración 13.

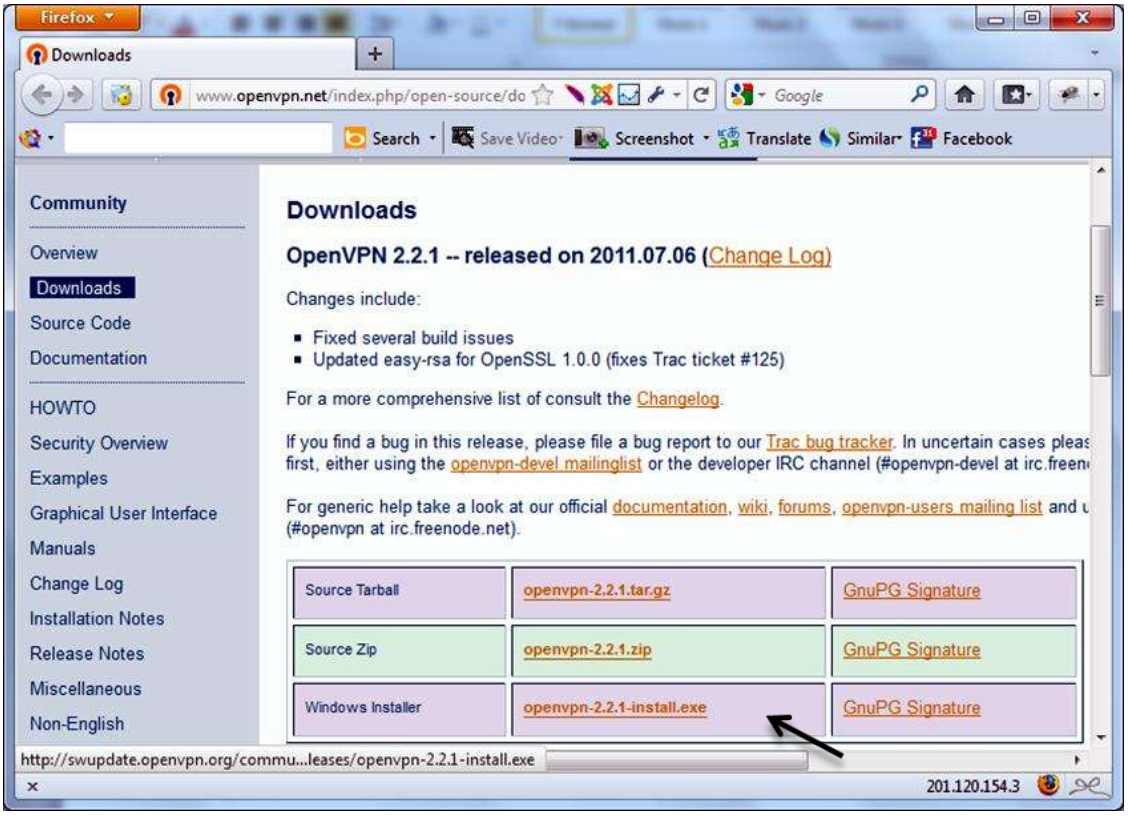


Ilustración 13: Descarga de OpenVPN

Se recomienda guardar el archivo de instalación para tenerlo a la mano y poder realizar la instalación en todas las computadoras en donde se requiera. Lo cual se hizo.

Ilustración 14: Guardar el archivo

La versión actual o más reciente mostrada en la página del producto es la 2.2.1 con fecha de liberación del 06 de Julio de este año.

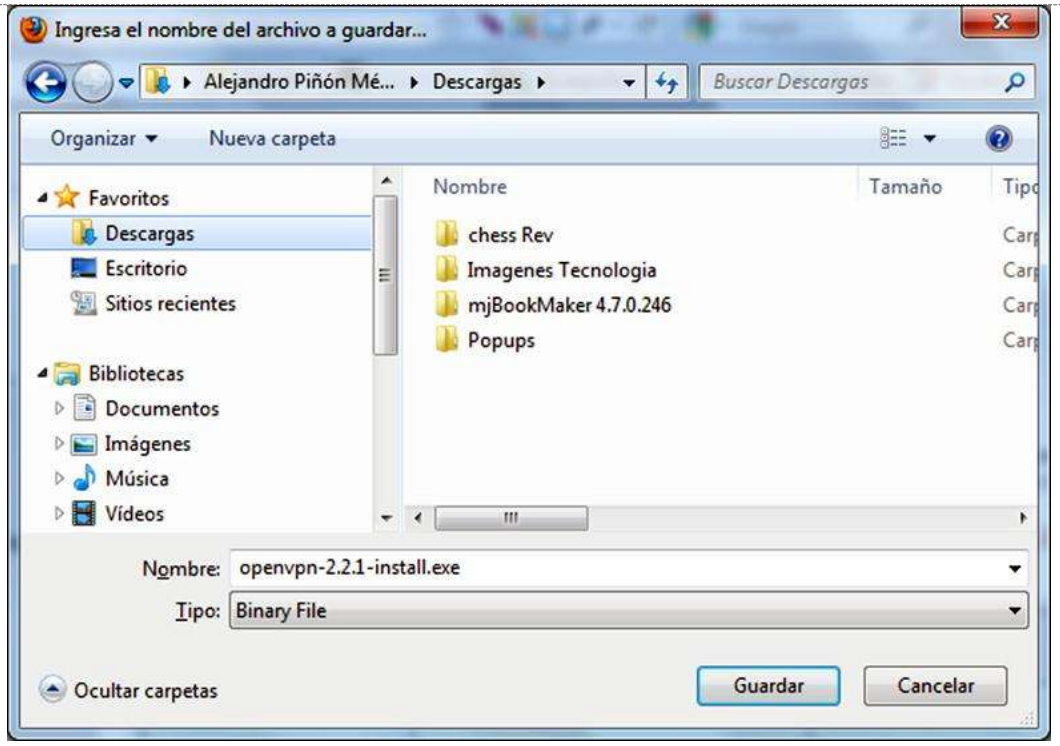


Ilustración 15: Carpeta de descargas

Se ubicó una carpeta en donde se almacenar el archivo.

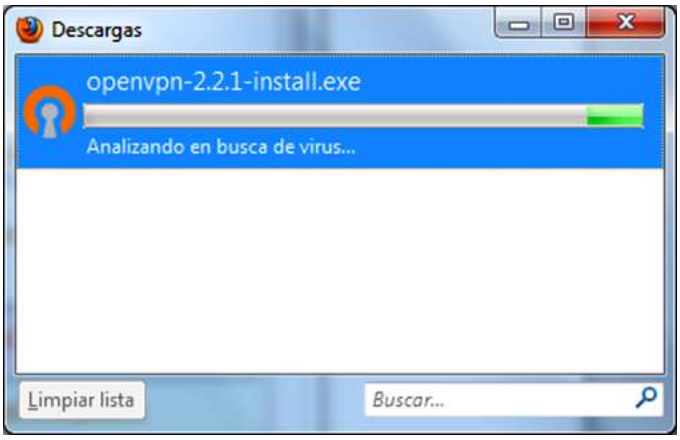


Ilustración 16: Archivo descargado

Una vez descargado el archivo, se procedió a ejecutarlo dando doble clic sobre el para iniciar el proceso de instalación.

Ilustración 17: Advertencia de Seguridad

Al iniciar el proceso de instalación, se recibió una advertencia de seguridad del Sistema Operativo preguntando si se desea ejecutar el archivo, a lo cual se procedió dando clic en el botón ejecutar.

Se inició el Asistente de Instalación, mediante el cual y siguiendo unos pocos y sencillos pasos, se configuro la instalación, así como los componentes necesarios para su correcto funcionamiento.

Ilustración 18: Asistente de Instalación

Para proceder basta con dar clic en el botón de siguiente para pasar al próximo paso, en donde se muestra el contrato de licencia.

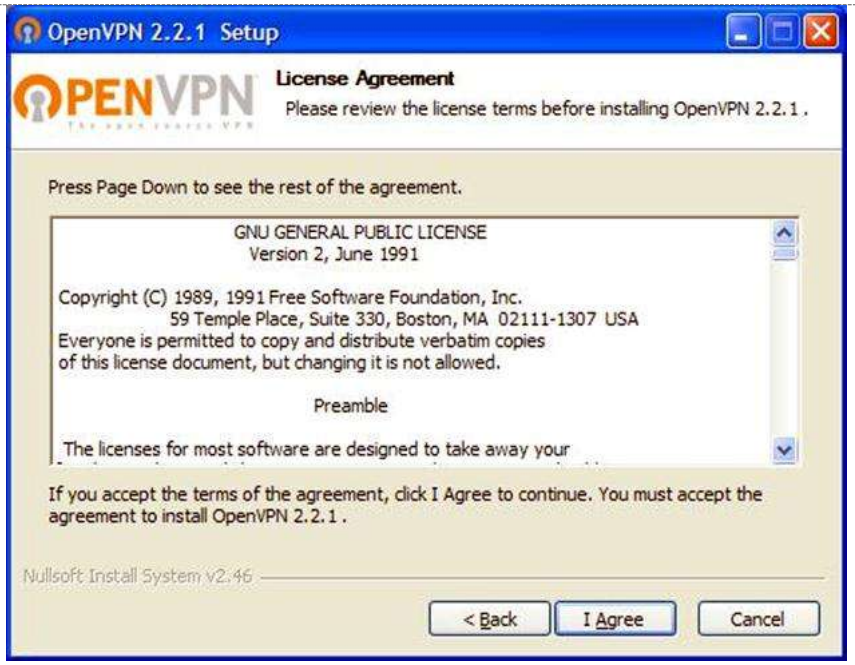


Ilustración 19: Contrato de Licencia

Es importante leer el contrato de licencia, ya que ahí se detallan los términos de uso del software. Una vez leído el contrato se debe procedió al paso siguiente dando clic en el botón I Agree.

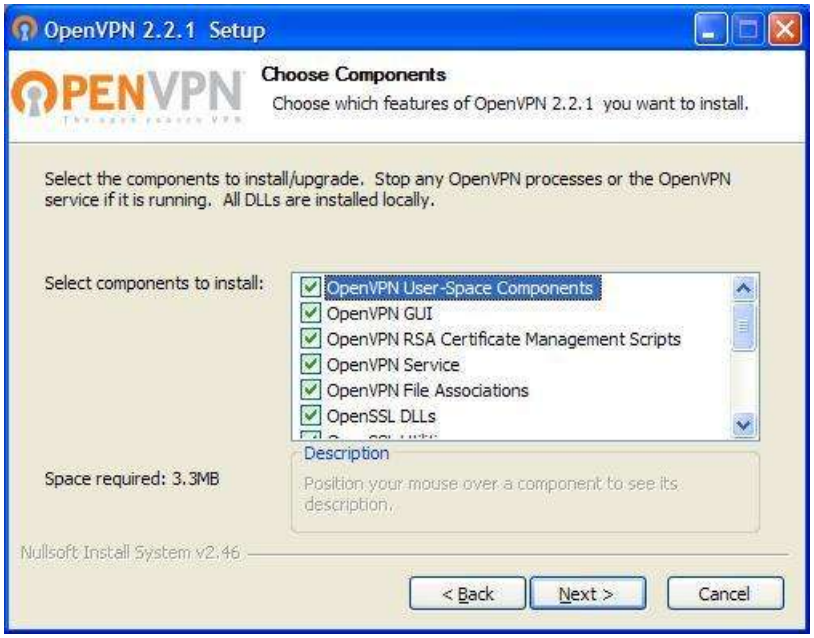


Ilustración 20: Componentes a instalar

En la Ilustración 20 se muestran todos los componentes que se instalaron en el sistema. Cabe señalar que es importante seleccionarlos todos para una funcionalidad completa en Windows. Una vez seleccionados los componentes se procedió a dar clic en el botón Next.

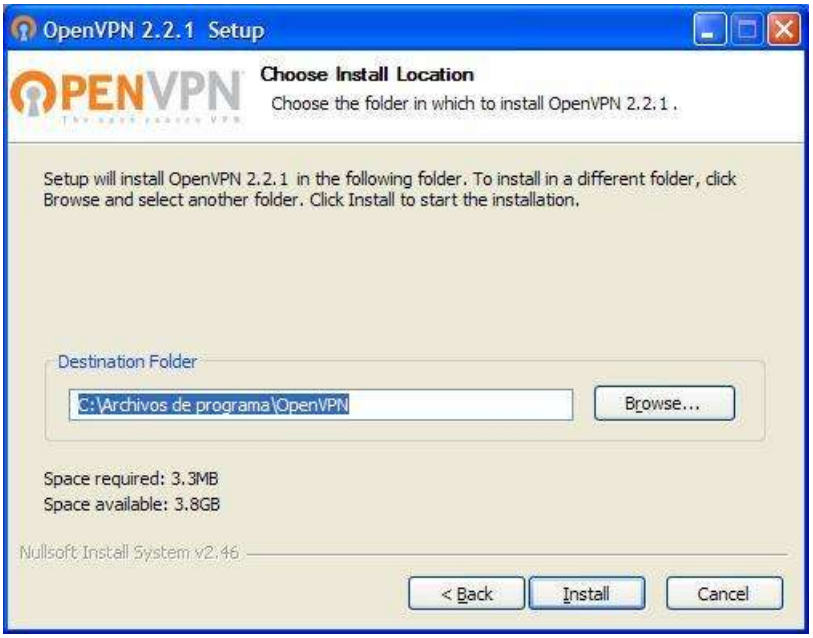


Ilustración 21: Ruta de instalación

Uno de los pasos importantes durante la instalación de cualquier programa es la ruta de instalación del mismo, en donde se debe especificar la ruta donde se guardaran todos los archivos y componentes que darán funcionalidad al programa. En el caso de OpenVPN, esto es aún más importante, ya que en la ruta de instalación deberemos también crear los archivos de configuración tanto del servidor como de los clientes de la VPN.

Ilustración 22: Instalación de OpenVPN

Al término de la configuración del asistente, este inicio el proceso de instalación. Algo que se debe tener en cuenta es que al instalar OpenVPN se crea una nueva interface de red virtual con los controladores TAP descritos anteriormente misma que deberemos considerar para la configuración de la VPN, ya que es mediante esta que se establecerá el túnel.

Ilustración 23: Asistente completado

Terminado el proceso de instalación se procedió a cerrar el asistente dando clic en el botón Finish.

¿Claves y Certificados?

Para construir una VPN con OpenVPN 2.2.1 es necesario crear una PKI (Infraestructura de Clave Pública - Public Key Infrastructure). Esta PKI está formada por:

- Un certificado (conocido como clave pública) y una clave privada para el servidor y para cada cliente.
- Un Certificado para la CA y su clave, que se usará para firmar los certificados del servidor y los clientes.

A partir de ahora todo el proceso de generación de claves, certificados, y firma digital, se realizará desde el servidor u otra máquina designada para ello, que no sea un cliente. Esto es por seguridad, ya que no es conveniente que un cliente contenga todas las claves y certificados. En el presente proyecto, se ha hecho desde el servidor de la VPN. Por tanto será servidor de la VPN y Unidad Certificadora.

Configuración Inicial

Una vez terminada la instalación se realizaron algunas configuraciones iniciales para asegurar el funcionamiento y mantener un control más avanzado sobre la VPN.

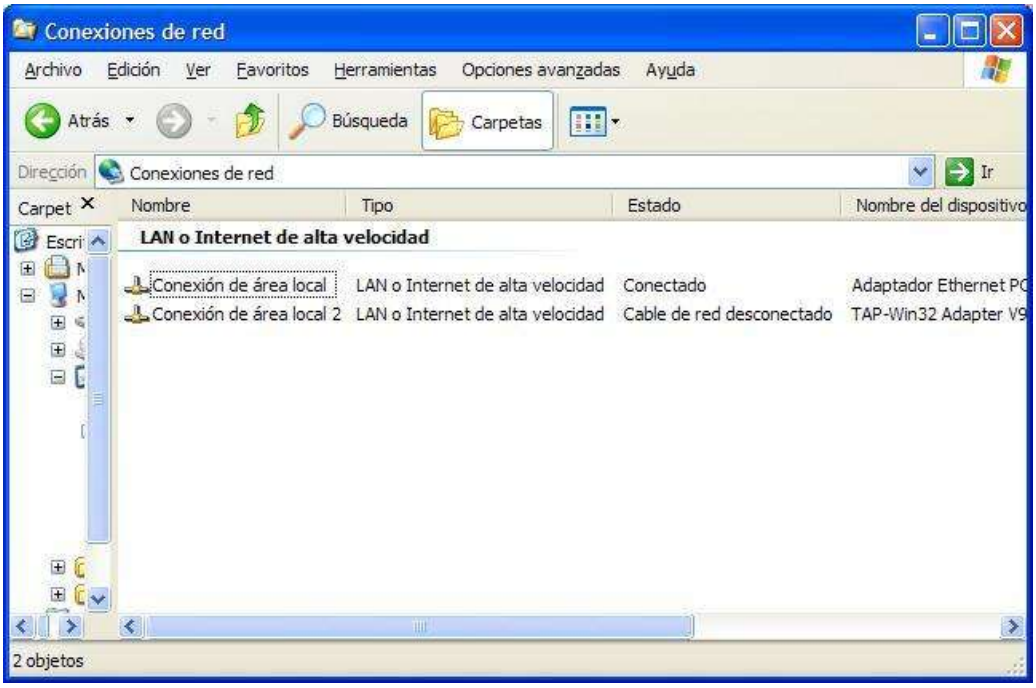


Ilustración 24: Nueva interface de red

Lo primero es verificar que se creó la nueva interface de red, lo cual se hizo accediendo al panel de control – Conexiones de red e internet – Conexiones de red. Para reconocer la nueva interface, podremos apreciar que en la etiqueta "Nombre del dispositivo" se muestra TAP-Win32 Adapter y en el nombre de la interface "Conexión de área local 2" la cual se renombro a OpenVPN.

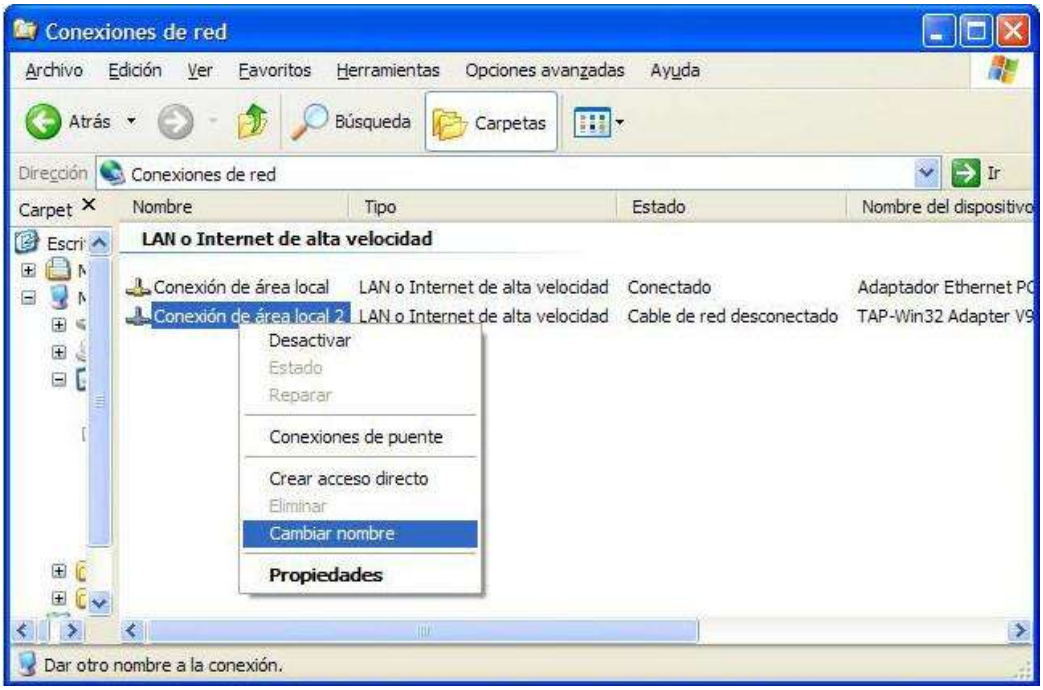


Ilustración 25: Cambiar Nombre

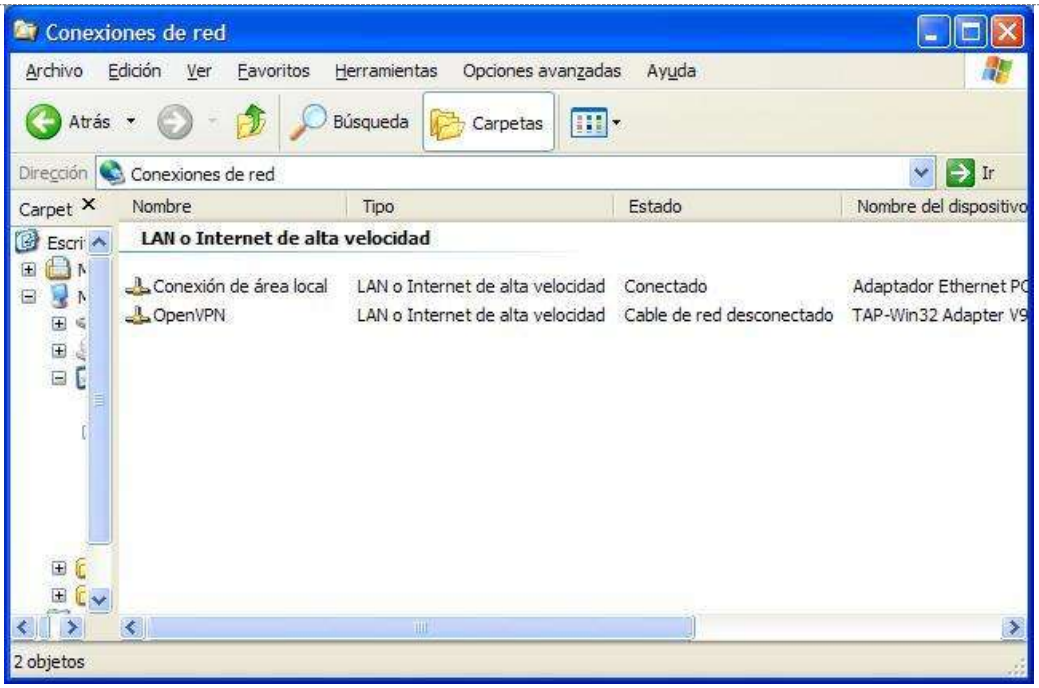


Ilustración 26: Interface renombrada a OpenVPN

Algunas consideraciones se deben de tener hasta aquí:

1. El cambio del nombre del nombre de la interface de red no es necesario, pero es mejor ya que facilita el realizar la configuración de OpenVPN.
2. El cambio del nombre de la interface se deberá ejecutar tanto en el servidor como en los clientes de la VPN.
3. Se debe tener especial cuidado en el nombre que se asigne, ya que OpenVPN y su configuración son case sensitive, por lo que si se utilizan como en este caso mayúsculas y minúsculas, se debe hacer también en la configuración de OpenVPN.

Continuando con la configuración inicial, en la misma PC que tiene el rol de servidor de la VPN, se revisó la ruta C:\Program Files\OpenVPN\sample-config o la ruta en donde se instaló el software, misma que se vio en la parte de instalación.

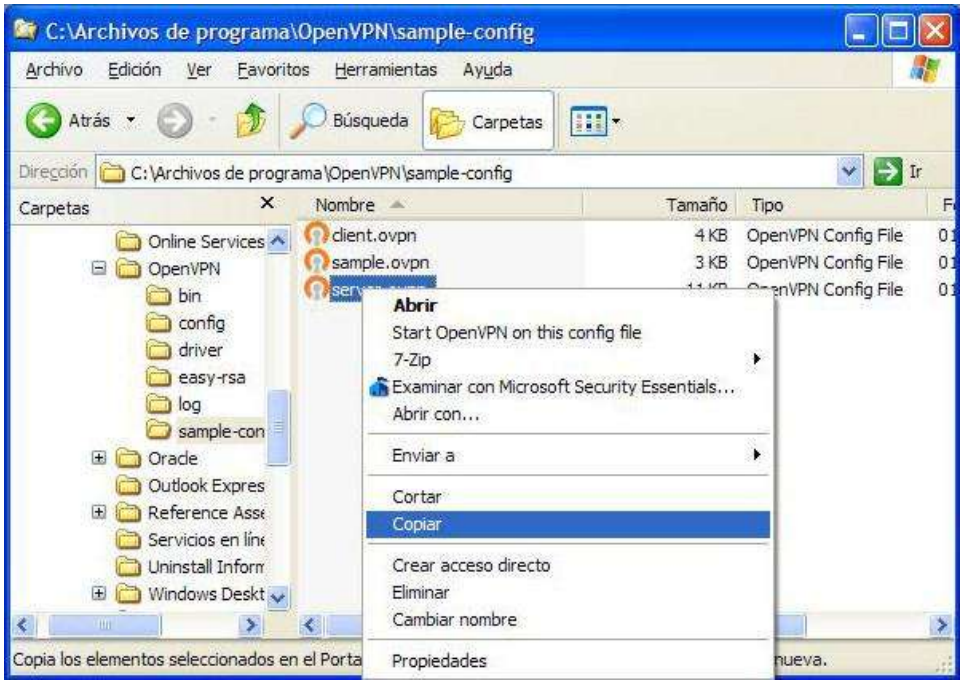


Ilustración 27: Ejemplos de configuración

En esa carpeta (simple-config) se proporcionan archivos de ejemplo de configuración de OpenVPN, los cuales se usaron para la configuración de las computadoras.

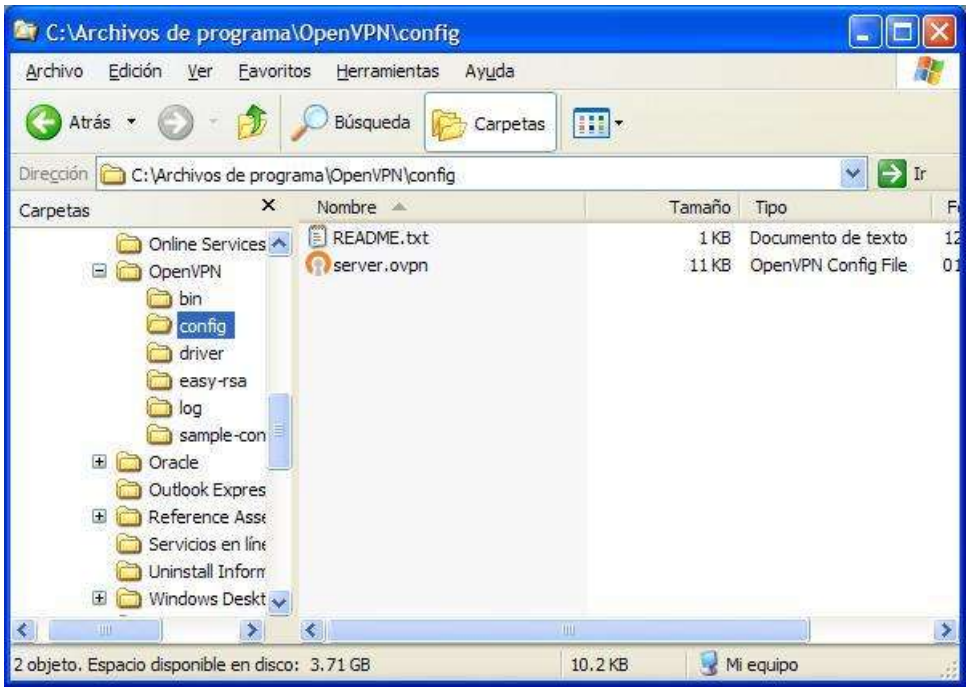


Ilustración 28: server.ovpn

Se copió el archivo server.ovpn en la ruta C:\Program Files\OpenVPN\config. Dicho archivo contiene la configuración básica para el servidor, la cual se editó considerando lo siguiente:

- **port 1194** Es el puerto a usar, el cual se abrió en los firewalls correspondientes apuntando a la IP del servidor.
- **proto tcp** es para especificar el tipo de puerto entre TCP y UDP. En este caso se manejó el tipo tcp.
- **dev tun** se usa para especificar el tipo de dispositivo de la interface de red virtual, pudiendo usar TUN o TAP dependiendo de las necesidades. Para este caso lo dejamos tal cual.
- **dev-node MyTap**. Se debe especificar el nombre que tendrá la interface de red, la cual nombramos a OpenVPN
- **cert NombreCertificado.crt y key NombreLlave.key** deben de renombrarse de acuerdo a los nombres que se ponen al crear los certificados y llaves correspondientes.
- **server 10.8.1.0 255.255.255.0** Es el segmento de IPs que se asignaran automáticamente a los clientes, tomando la 1 para el servidor.
- **max-clients 50** Es el máximo de clientes que estarán conectados al mismo tiempo al server.

Crear Certificado de autoridad, Claves y Certificados de Servidor y Clientes

Al terminar de realizar la configuración inicial, se procedió a crear los certificados y llaves de seguridad para garantizar la confiabilidad de la conexión.

Lo primero fue crear la entidad certificadora y el certificado de autoridad, lo cual se realiza con algunos scripts que ya incluye la instalación de OpenVPN en la misma ruta donde se instaló (C:\Archivos de programa\OpenVPN\easy-rsa) en donde se ejecutaron mediante línea de comandos de la manera siguiente:

1. Init-config ┘

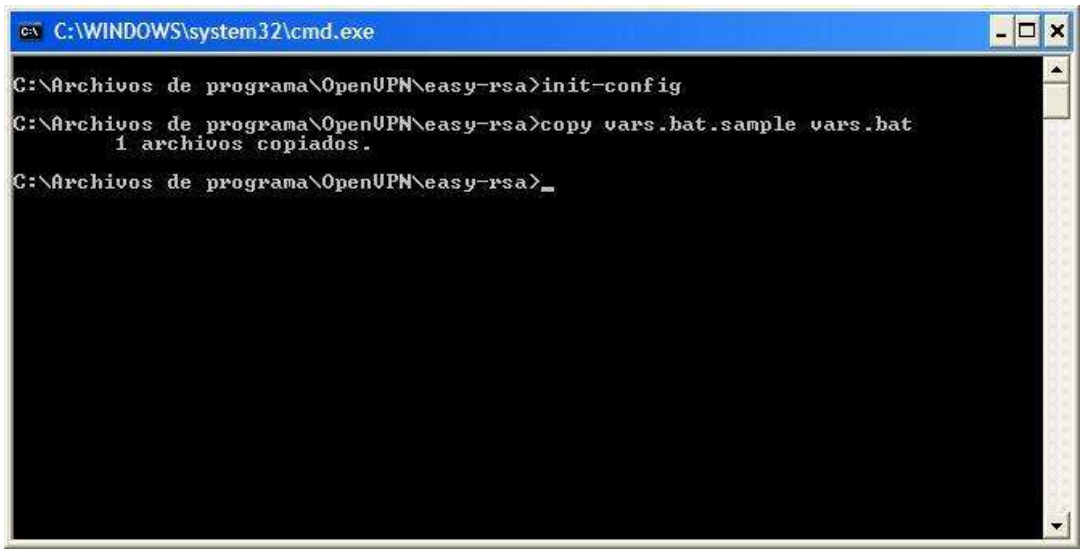


Ilustración 29: Script init-config

Y posteriormente.

2. notepad vars.bat ↵

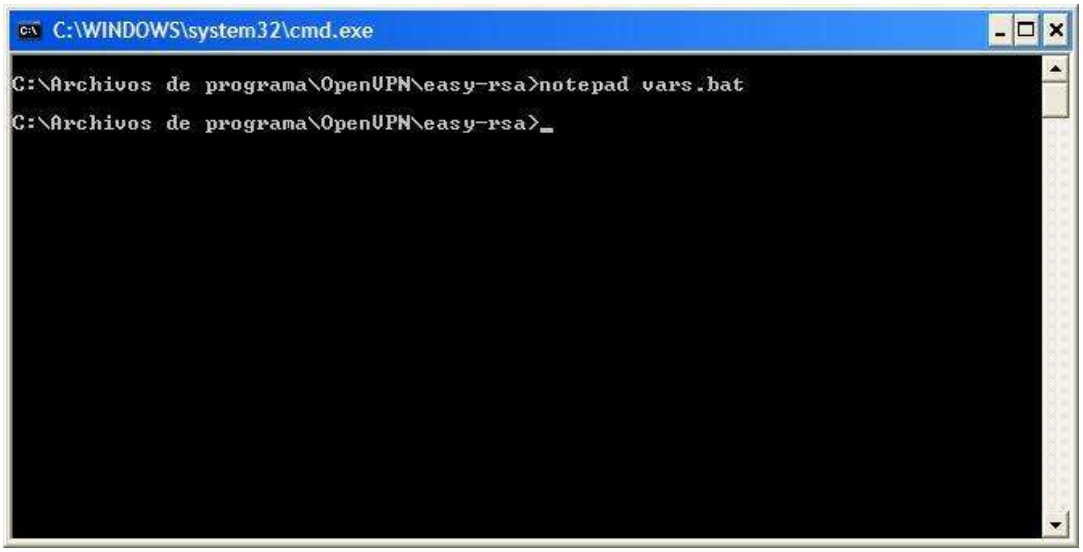


Ilustración 30: Comando para editar el archivo vars.bat

Este último comando abre el block de notas con el archivo vars.bat para editarlo, donde se editan las últimas líneas en lo referente a la ubicación, país, estado, ciudad, etc. y una vez terminado se guardan los cambios.

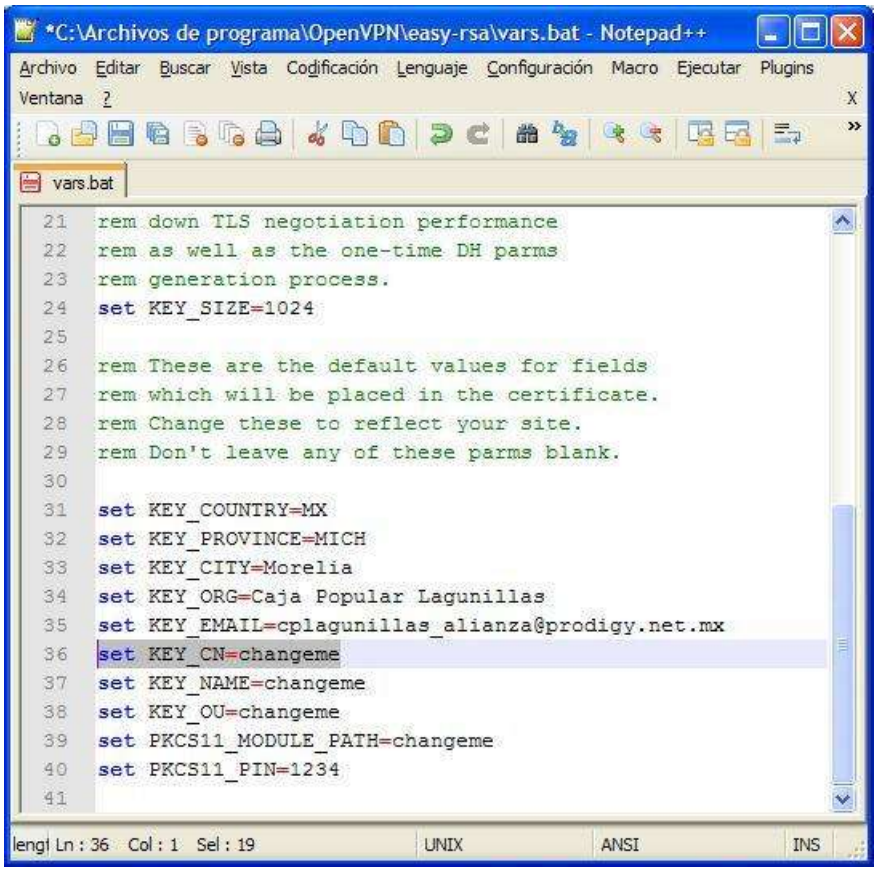


Ilustración 31: Edición de vars.bat

Es importante ingresar los datos de la Organización reales (para ser prolijos) y teniendo especial atención en el parámetro ***Common Name*** el cual deberá ser distinto para el caso de la CA, Servidor y los Clientes.

Después para crear la entidad certificadora y siguiendo el mismo procedimiento referido en el How to de OpenVPN, se ejecutaron los comandos siguientes:

3. **vars** ↵
4. **clean-all** ↵
5. **build-ca** ↵

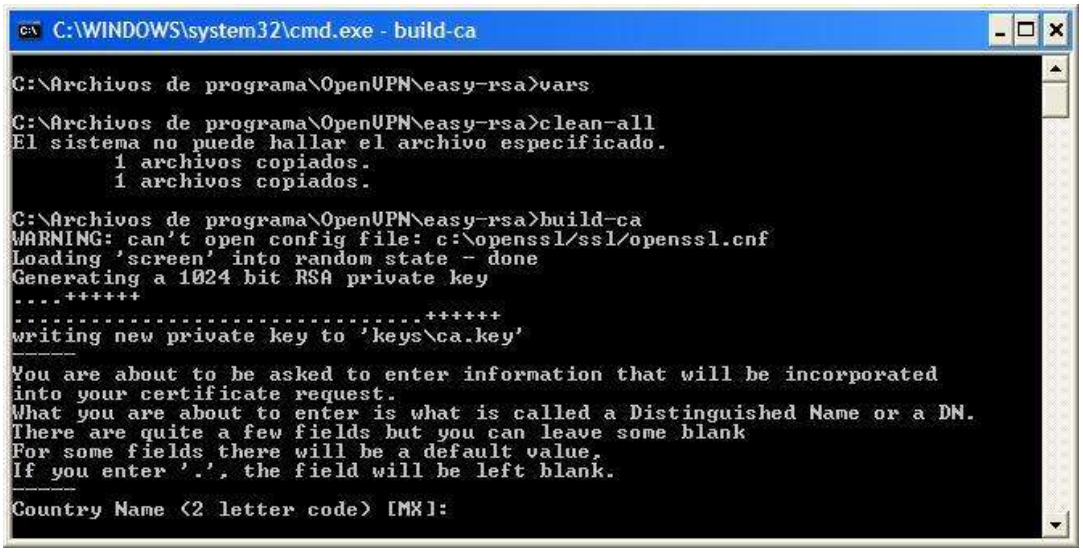


Ilustración 32: Creación de la entidad certificadora

El comando build-ca pide datos como el país, estado, ciudad, organización, depto., nombre del Servidor y correo electrónico, todos estos valores hay que repetirlos durante todo el proceso de creación de certificados y llaves o cuando lo pide, a excepción del nombre del host (hostname) que cambia en la parte de configuración de las llaves del cliente. (Estos datos se capturaron al editar el archivo vars.bat, pero no todos, así es que al crear los certificados y llaves de los clientes se deben de cambiar los que falten como el hostname).

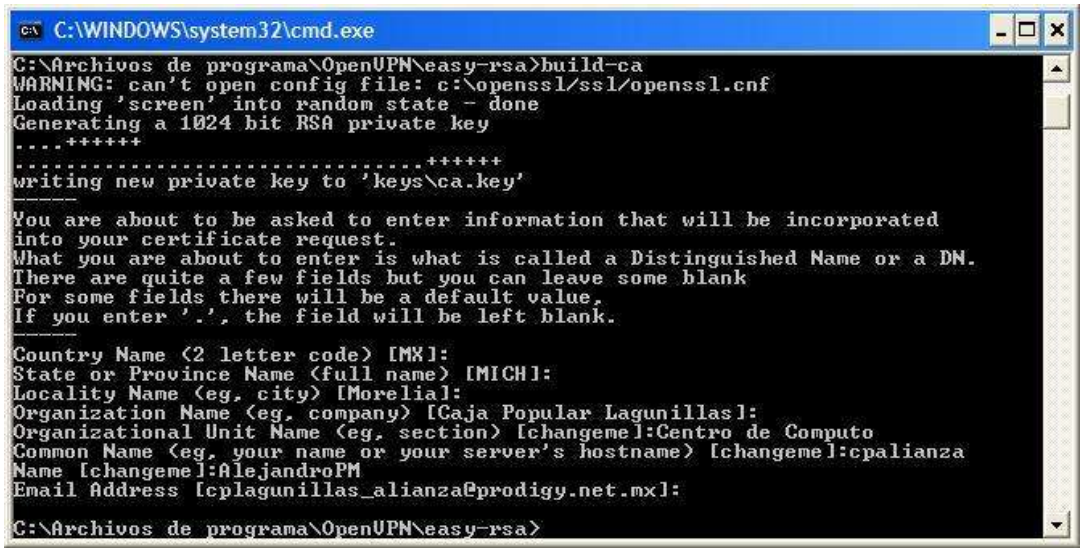


Ilustración 33: Captura de datos CA

Lo que se hizo fue crear el Certificado de Autoridad, el cual se creó en la ruta C:\Archivos de Programa\OpenVPN\easy-rsa\keys

El siguiente paso realizado fue crear la llave privada y certificado del servidor, para hacer esto se ejecutaron los siguientes comandos:

6. **vars** ↵
7. **build-key-server NombreDelServidor** ↵

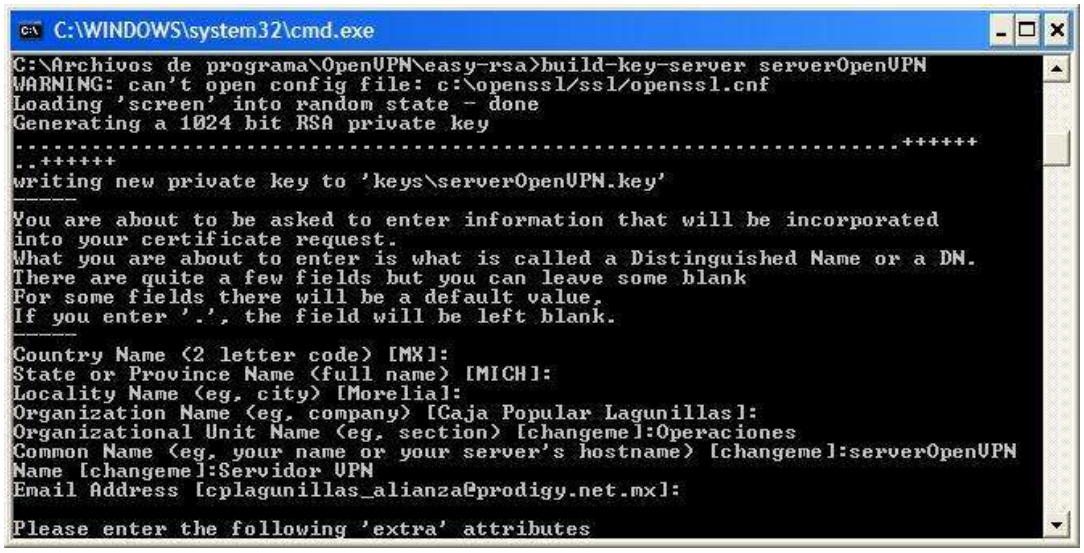


Ilustración 34: build-key-server

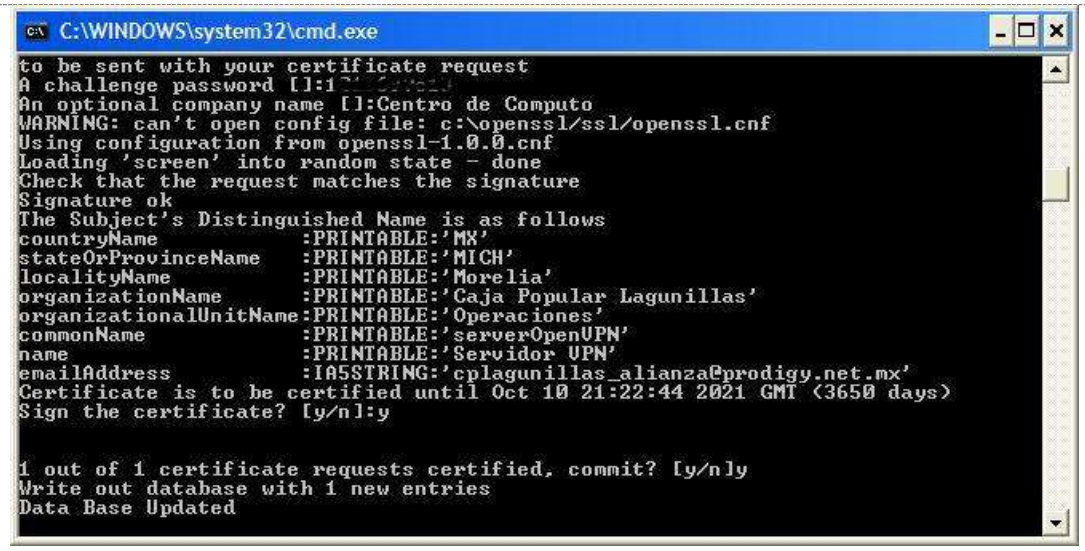


Ilustración 35: Captura de datos

Al ejecutar el último comando, una vez capturados los datos, pregunta si se desea firmar el certificado a lo que se responde que sí, y también a la pregunta siguiente.

Posteriormente se generaron los parámetros Diffie Helman para el servidor ejecutando el siguiente comando:

8. build-dh ↵

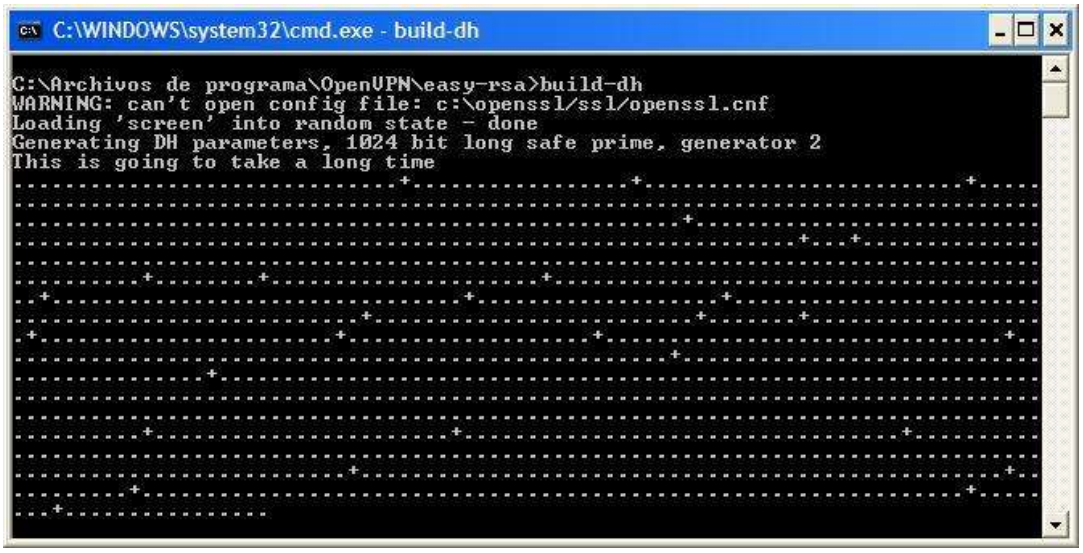


Ilustración 36: comando build-dh

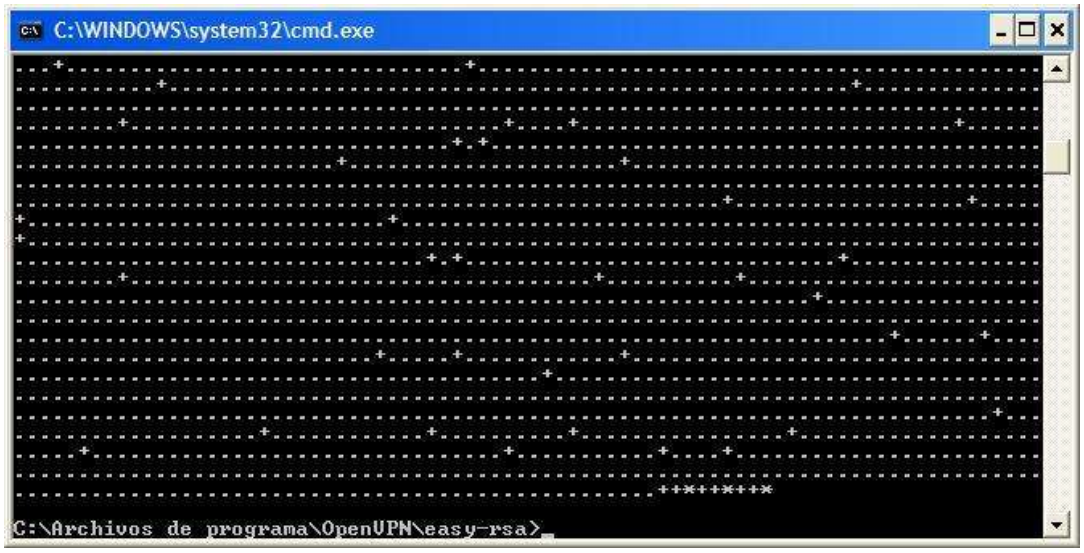


Ilustración 37: Generación de parametros Diffie Helman

En este punto ya han sido creadas todas las llaves para el servidor, por lo que se procederá a crear las llaves y certificados para los clientes mediante los comandos siguientes:

9. **vars** ↵
10. **build-key NombreDelCliente** ↵

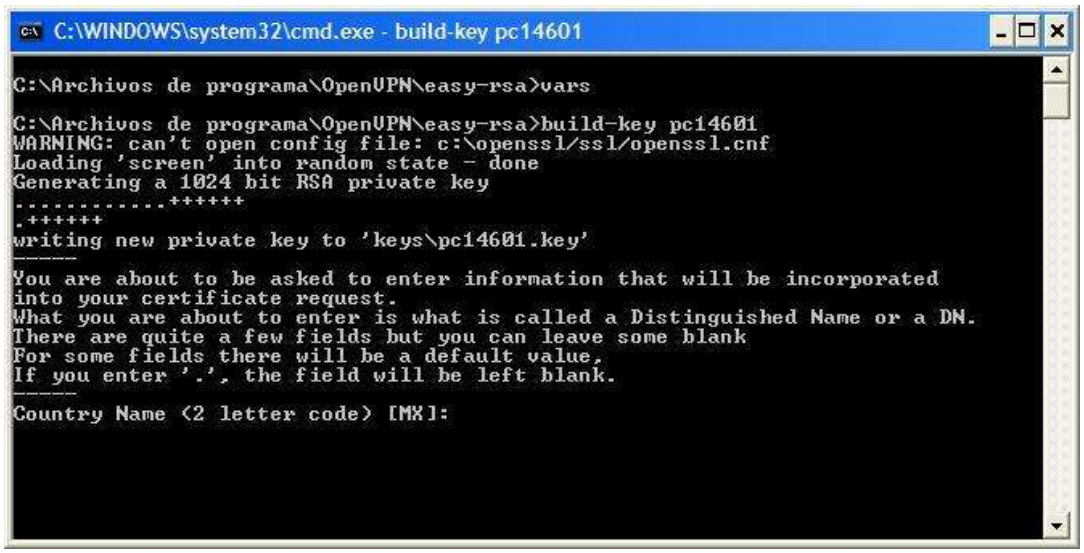


Ilustración 38: Creación del certificado de un cliente

En la creación de los certificados y llaves de los clientes se siguieron los mismos parámetros para todos los clientes, tomando como nombre de los certificados el nombre del equipo.

Se capturan los datos solicitados y se firma el certificado.

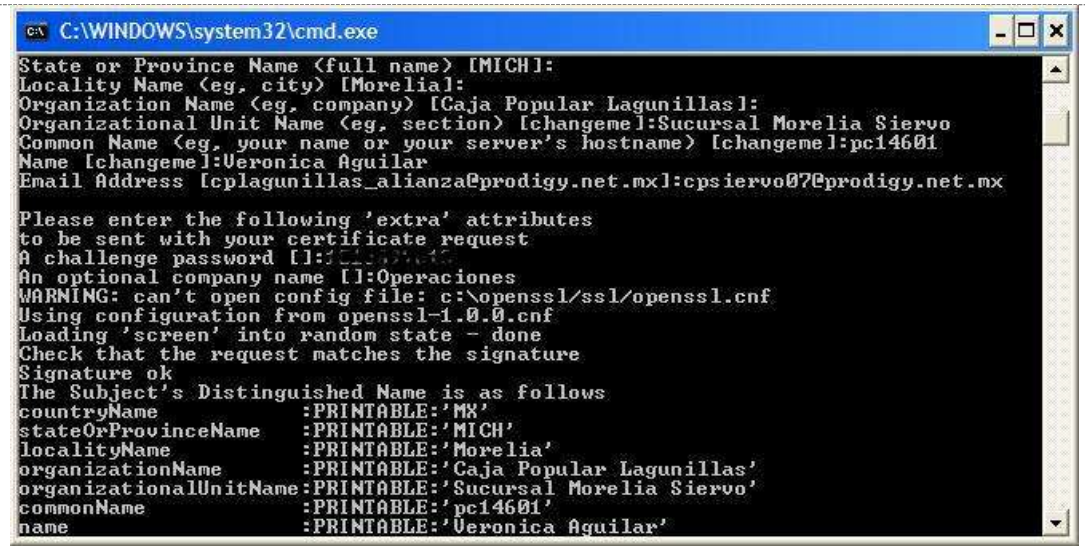


Ilustración 39: Captura de datos requeridos

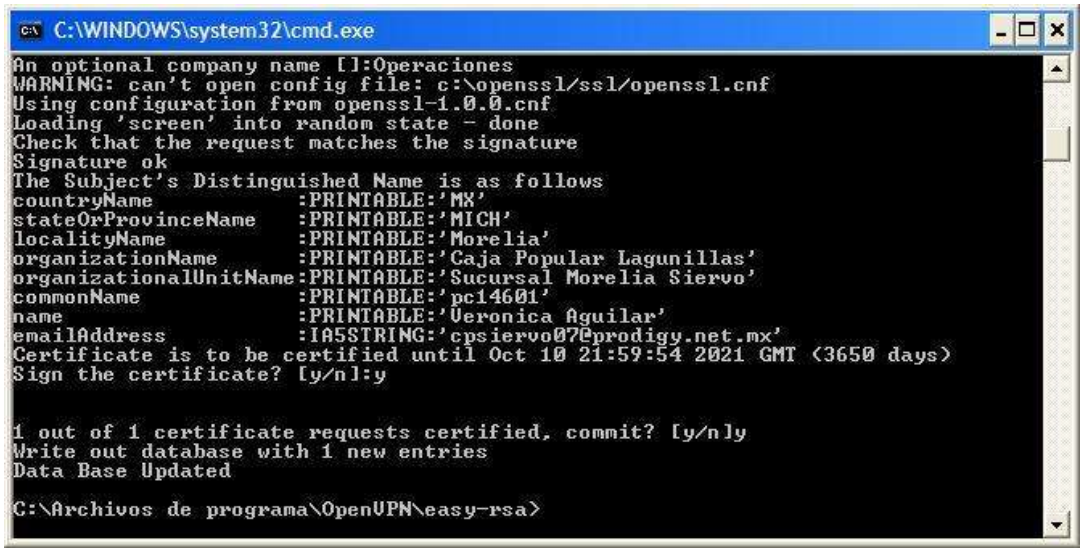


Ilustración 40: Llaves y certificados de cliente creados

Una vez terminada la creación de los certificados de todos los clientes a conectar se verifico su existencia en la carpeta correspondiente de la ruta de instalación C:\Archivos de programa\OpenVPN\easy-rsa\keys.

De todos los archivos generados, los más importantes son los siguientes:

- NombreDelServidor.crt
- NombreDelServidor.key
- ca.crt
- dh1024.pem
- NombreDelCliente.crt
- NombreDelCliente.key

Esto es importante, porque todos estos archivos son los que garantizan la seguridad de la VPN. Estos archivos se copiaron en la ruta C:\Archivos de programa\OpenVPN\config junto con los parámetros de configuración del servidor

Además en cada equipo cliente también se copiaron en la misma ruta antes mencionada los archivos siguientes:

- ca.crt
- NombreDelCliente.crt
- NombreDelCliente.key

Configuración de OpenVPN en el servidor

Como ya se comento anteriormente, el servidor debe contener un archivo con extension .ovpn en la ruta C:\Archivos de programa\OpenVPN\config, al cual se le asignó el nombre de server.ovpn.

Los parámetros de configuración del servidor están contenidos en el archivo mencionado el párrafo anterior y es lo que permite que se pueda establecer la conexión VPN con los clientes.

Para realizar la configuración se revisó el manual de configuración de OpenVPN que fue lo que sirvió de apoyo para el proyecto, pudiendo crear la red privada virtual de manera satisfactoria.

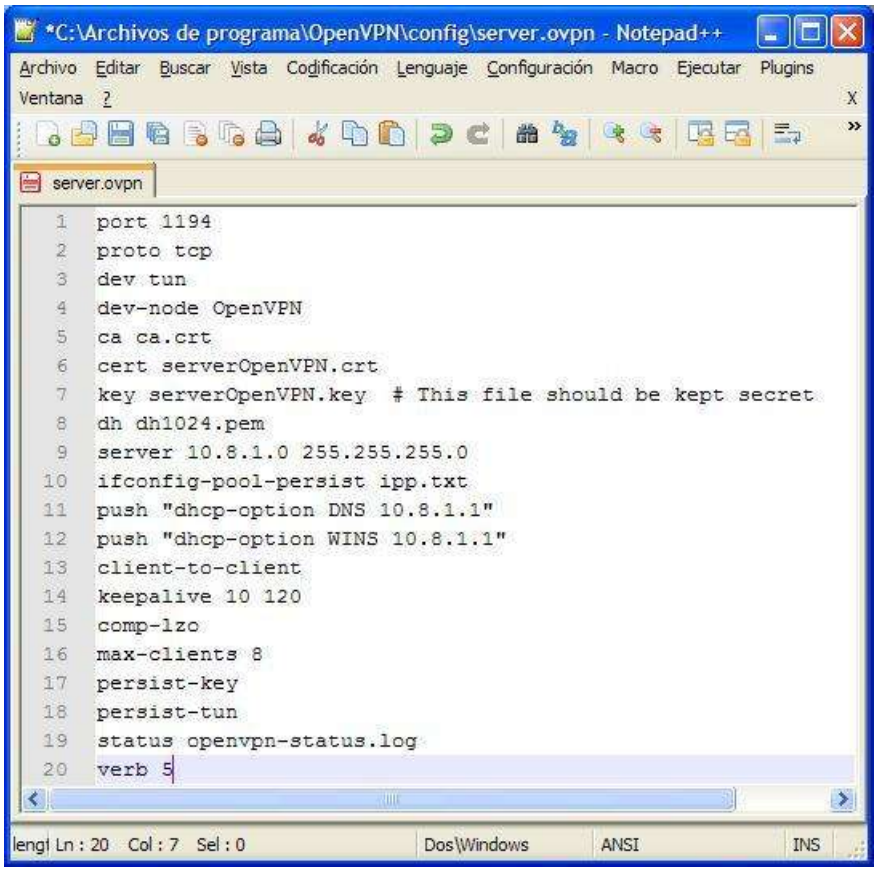


Ilustración 41: Archivo de configuración del server

Como parte de la configuración del servidor, aunque realmente no funge como tal, está el abrir el puerto 1194 necesario para poder realizar la conexión de OpenVPN, el cual se especificó en el firewall.

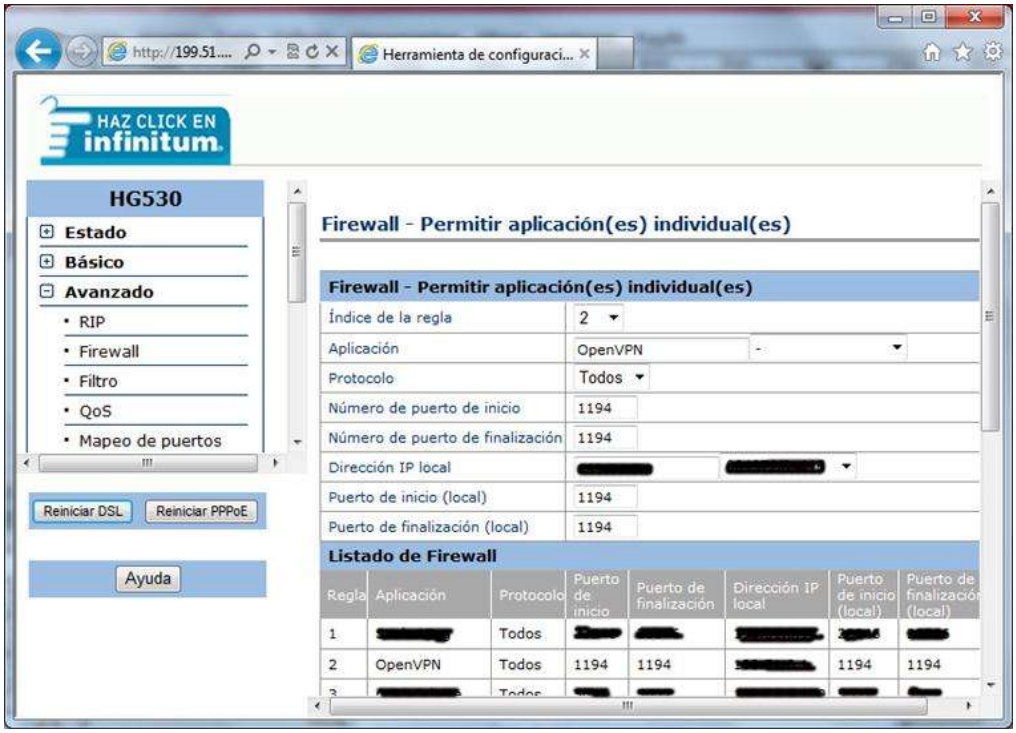


Ilustración 42: Listado de Firewall

Configuración de OpenVPN en el cliente

Para la configuración de los clientes es bastante sencillo. El procedimiento realizado fue de la manera siguiente:

1. Se instaló OpenVPN tal como en el proceso de instalación del servidor.
2. Se renombrar la interface de red TAP a OpenVPN.
3. Se copiaron los archivos ca.crt, NombreDelCliente.crt, NombreDelCliente.key y cliente.ovpn en la ruta C:\Archivos de programa\OpenVPN\config.

El archivo cliente.ovpn es similar al de server.ovpn y también se encuentra en los archivos de ejemplo mencionados con anterioridad, al cual se le realizaron modificaciones en los parámetros de configuración para establecer la conexión al servidor de la VPN a través de internet estableciendo el túnel.

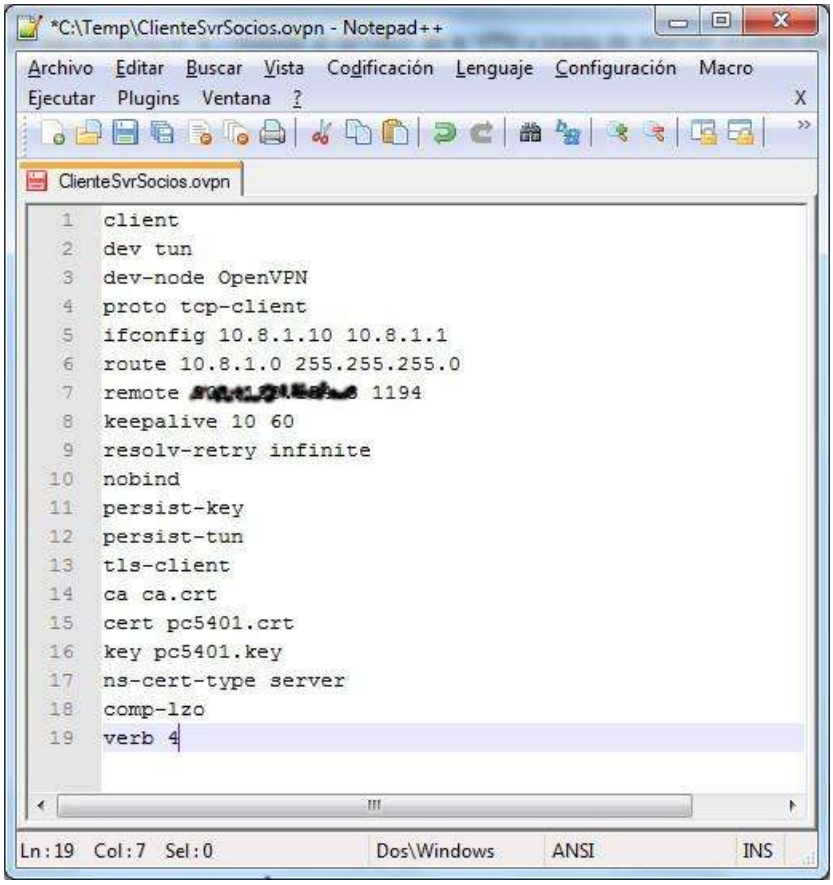


Ilustración 43: Configuración del cliente

El archivo de configuración cliente.ovpn se renombro a VPNOficinaMatriz.ovpn para ubicarlo con facilidad.

Para establecer la conexión con el servidor de la VPN se ejecuta el acceso directo que se encuentra en el escritorio OpenVPN GUI.

Ilustración 44: Acceso directo a la conexión VPN

Cuando se ejecuta la interfaz gráfica de OpenVPN, se posiciona sobre la bandeja del sistema un icono idéntico al del acceso directo en el que se debe dar clic derecho y hacer la conexión al servidor requerido. Esto se realizó tanto el servidor como en los clientes.

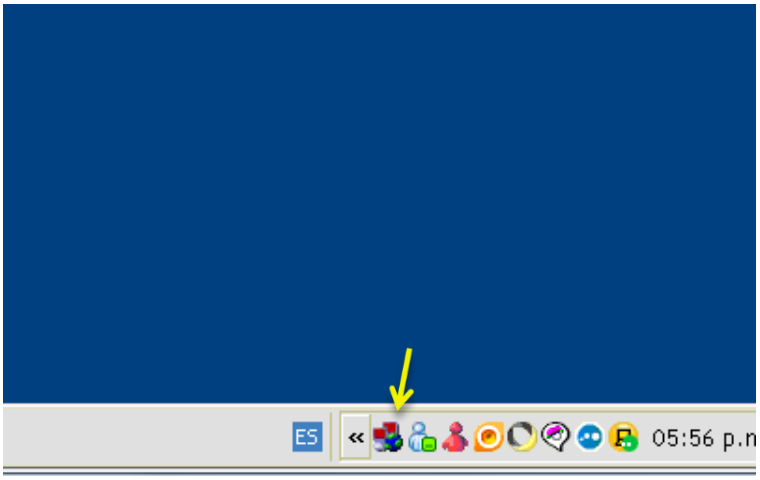


Ilustración 45: GUI de OpenVPN

La manera de establecer la conexión es dar clic con el botón derecho encima del icono de la bandeja y clic en la opción connect.

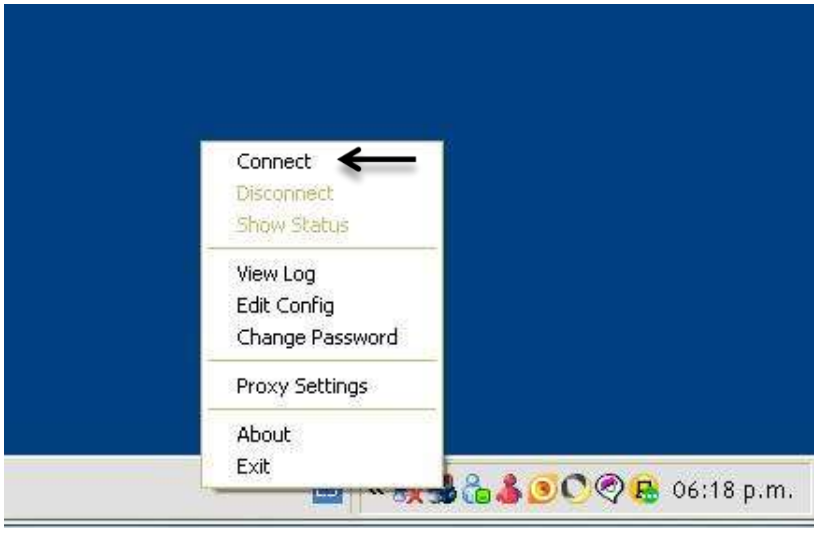


Ilustración 46: Conectar al servidor

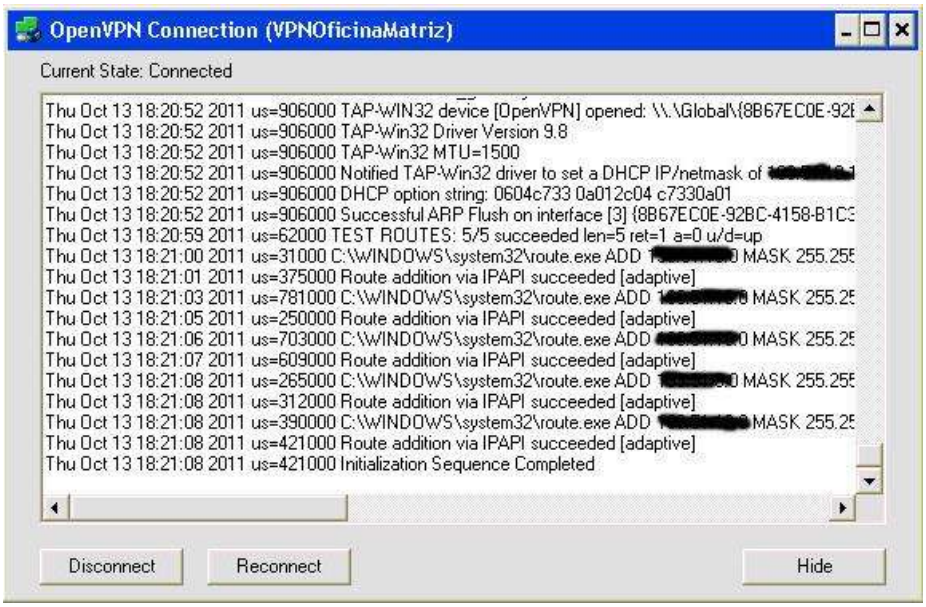


Ilustración 47: Conexión realizada con éxito

Una vez que se realizó la conexión se procedió a realizar la prueba correspondiente para constatar que efectivamente se estableció el túnel VPN de manera exitosa y también se realizaron los ajustes en los parámetros de configuración del Sistema Institucional para realizar la conexión a la base de datos SQL Server mediante la VPN.

Comandos para iniciar la conexión automáticamente

Como mejora adicional, se configuraron los clientes para que al inicio de la sesión se establezca de manera automática la conexión al servidor de VPN y base de datos.

Para ello se adicionaron parámetros al icono del acceso directo para que al ejecutarse este, automáticamente se realizara la conexión, los parámetros adicionales son:

cd\

cd "Archivos de programa\OpenVPN\bin"

openvpn-gui-1.0.3 --connect ClienteServerLagu.ovpn --silent_connection 1

Lo cual ya visto gráficamente, quedaría de la manera siguiente:

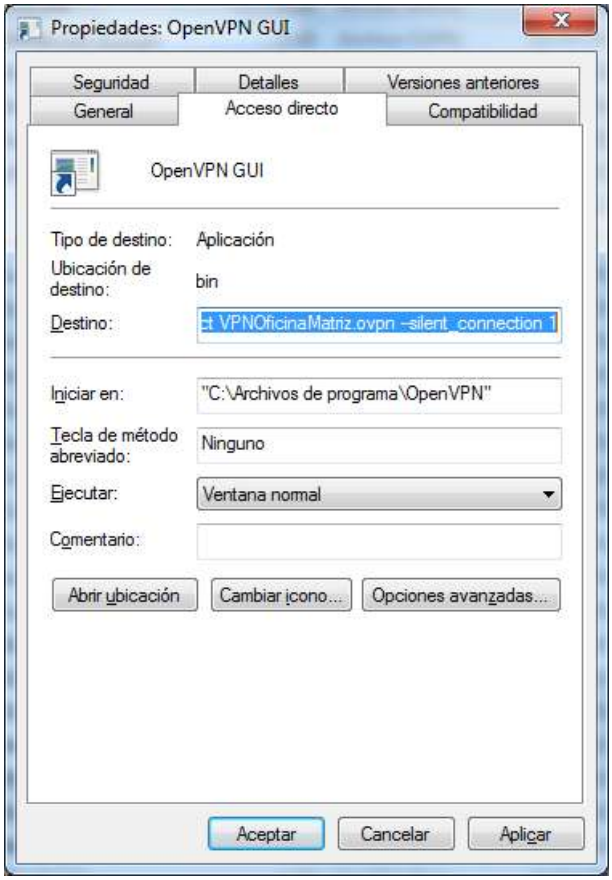


Ilustración 48: Parámetros del acceso directo

* En el campo Destino: "C:\Program Files\OpenVPN\bin\openvpn-gui-1.0.3.exe" --connect VPNOficinaMatriz.ovpn --silent_connection 1

** En el caso del servidor seria "C:\Program Files\OpenVPN\bin\openvpn-gui-1.0.3.exe" --connect server.ovpn --silent_connection 1

Este icono a su vez se copea a la carpeta Inicio que está en Inicio - Todos los programas - inicio, con lo cual al encender la PC, se ejecutara OpenVPN y automáticamente realizara la conexión al servidor de la Oficina Matriz.

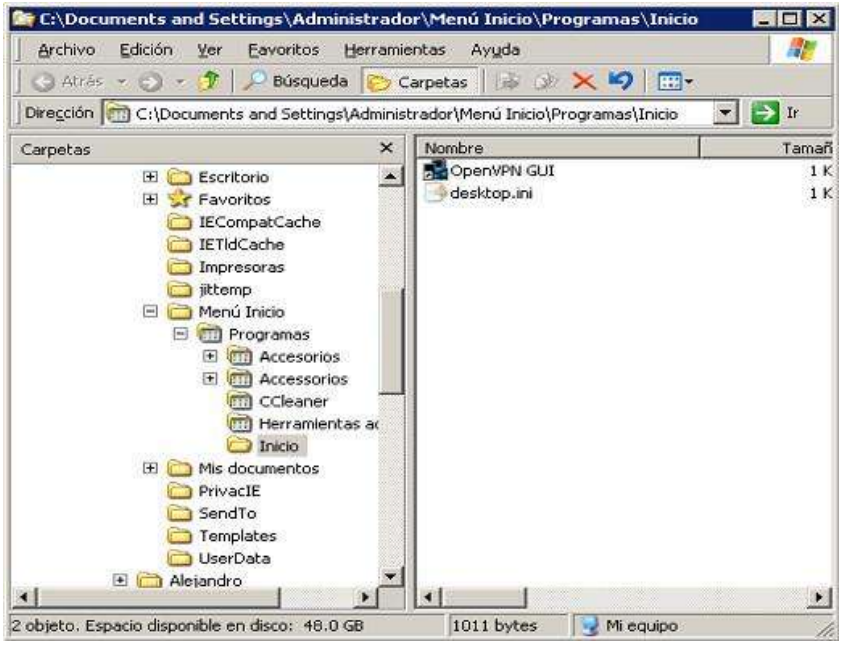


Ilustración 49: Inicio automático

Otra manera de que la conexión se realice de manera automática, es configurar OpenVPN como un servicio, para ello, hay que dar clic en inicio, ejecutar, services.msc y aceptar.

Una vez abierta la consola de servicios, se puede establecer el servicio OpenVPN Service para que inicie de manera automática al iniciar sesión en el equipo.

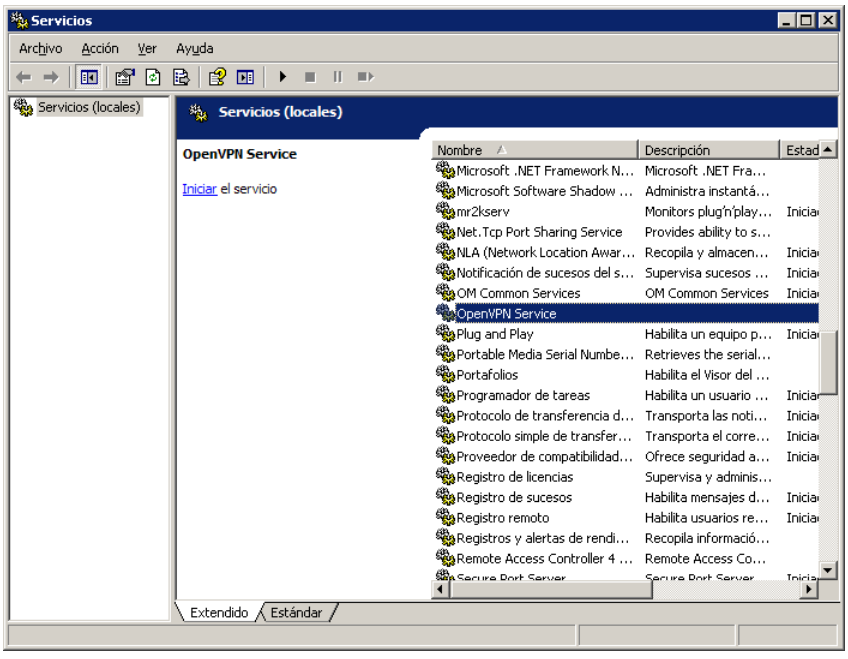


Ilustración 50: Consola de Servicios

Una vez hecho esto, la conexión VPN se establecerá automáticamente sin necesidad de interacción del usuario.

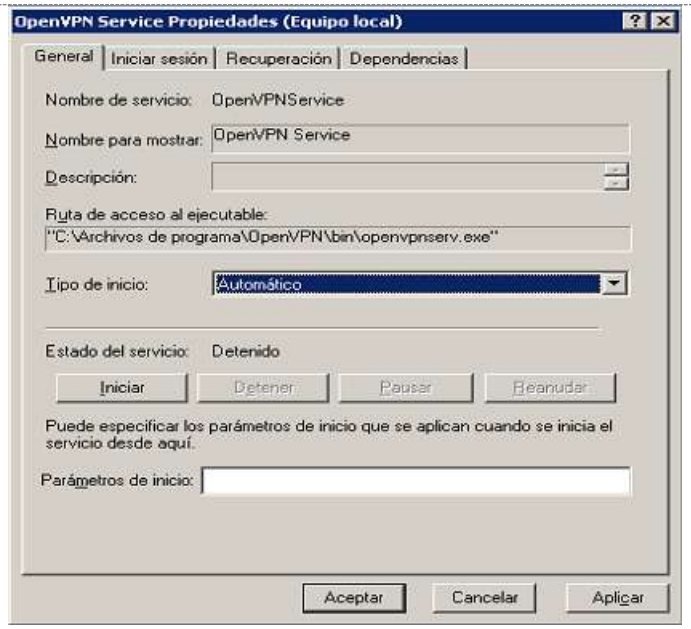


Ilustración 51: Propiedades del servicio OpenVPN

Capítulo V.- Resultados

Durante el desarrollo del proyecto se presentaron algunos problemas como fue el caso de la disminución del rendimiento de la VPN (bajo la velocidad considerablemente por las tardes).

Esto se debió a que se contaba con poco ancho de banda (1 MB) pero se atendió en coordinación con el proveedor del servicio de Internet (Telmex) quien realizo algunos ajustes, además se realizó un incremento del ancho de banda para evitar problemas de saturación y disminución del rendimiento en el futuro.

Los resultados han sido favorables, ya que se cumplió el objetivo deseado obteniendo además algunas otras mejoras y ventajas con el ahorro en la cuestión monetaria y la posibilidad de manejar este sistema de conexión VPN de manera redundante con otros métodos para cumplir tanto con las políticas de planeación como con el Plan de Continuidad del Negocio que se pretende implementar en el futuro.

Estadísticas

Tabla 3: Estadística de fallas del servicio del mes de Agosto

Sucursal	Antena*	Frame Relay**	VPN
Oficina Matriz	0	1	3
Morelia Centro	12	0	5
Morelia Siervo	18	0	8

* Se presentaron fallas prácticamente todos los días por la mañana y por las tardes, además de los días lluviosos.
* Se presentaron fallas prácticamente todos los días por la mañana y por las tardes, además de los días lluviosos.

Tabla 4: Estadística de Fallas

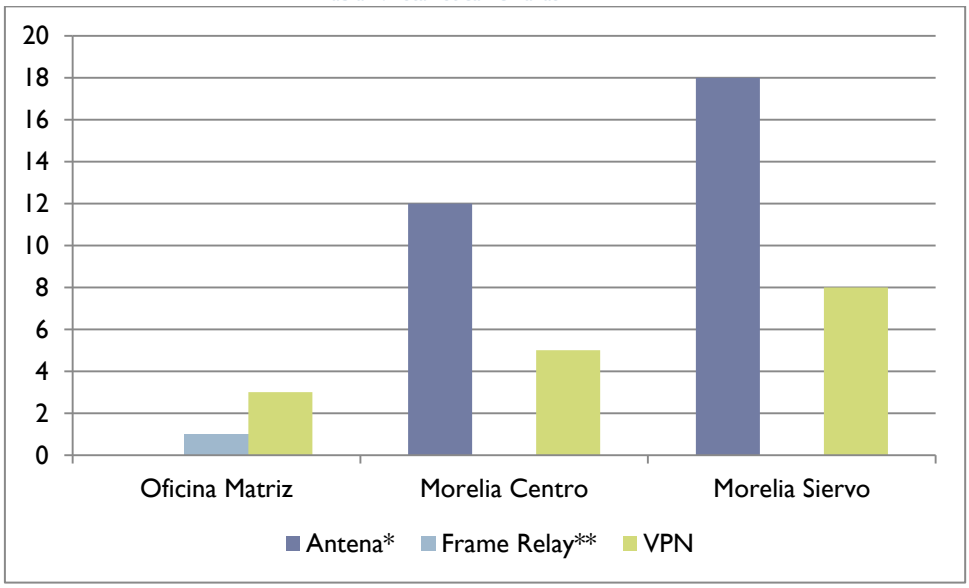


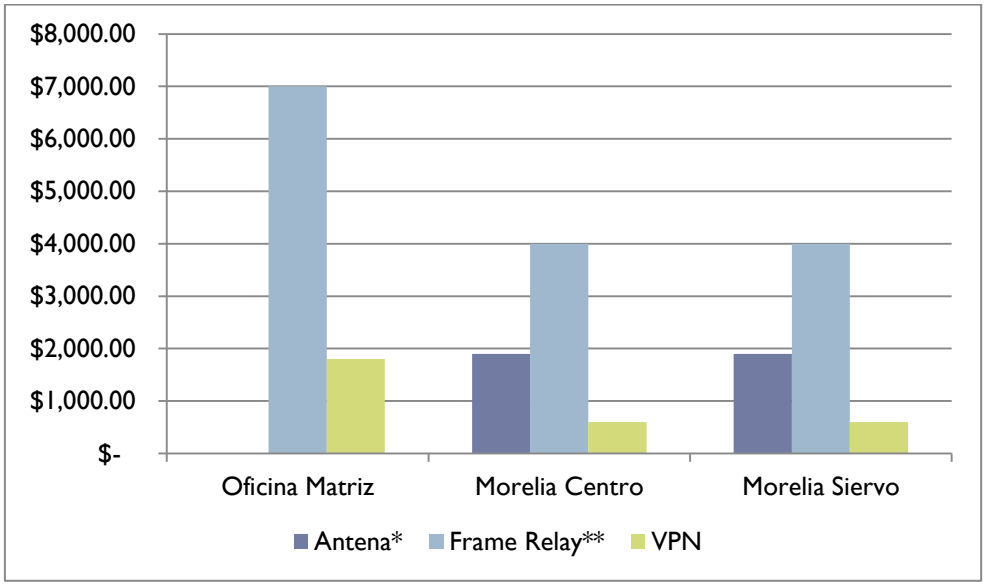
Tabla 5: Estadística de costo beneficio

Sucursal	Antena*	Frame Relay**	VPN
Oficina Matriz	$ -	$ 7,000.00	$ 1,800.00
Morelia Centro	$ 1,900.00	$ 4,000.00	$ 600.00
Morelia Siervo	$ 1,900.00	$ 4,000.00	$ 600.00

* Se maneja un costo mensual de la antena, ya que es la depreciación que se realizaría mensualmente debido a que las antenas se adquieren y son propiedad de la cooperativa.

** El frame relay no está contratado en Morelia Centro ni en Morelia Siervo, pero se establece el costo de renta mensual como parámetro de comparación.

Tabla 6: Estadística de Costos



Capítulo VI.- Conclusiones y Recomendaciones

Conclusiones

De acuerdo a los objetivos planteados al inicio del proyecto, concluyo con lo siguiente:

- ✓ Se implementó una solución de VPN, efectiva y permanente basada en software libre, lo cual ha permitido desde entonces el mantener un enlace con la Oficina Matriz y la base de datos en la cual se registran las transacciones de los movimientos realizados a los socios, con lo cual se logró desarrollar las actividades inherentes a la cooperativa.
- ✓ Aunado a lo anterior y antes de la implementación final, se analizaron las ventajas de la tecnología existente dentro de la cooperativa, con lo cual se logró determinar la base tecnológica para establecer la herramienta más adecuada que satisficiera las necesidades en cuanto a conectividad se requería.
- ✓ Con base al análisis de la tecnología existente en la cooperativa y también analizando las herramientas de software libre que se pudieran haber utilizado para este proyecto, se seleccionó un sistema/aplicación, que de manera satisfactoria soluciono los problemas de conexión con el servidor de base de datos que se tenían.
- ✓ Como consecuencia de lo anterior, se logró brindar un mejor servicio y atención continua en tiempo real a los socios de la cooperativa dentro de las sucursales que participaron de este proyecto.
- ✓ De acuerdo a las políticas de planeación y al plan de continuidad del negocio[7], se cuenta a partir de la conclusión de este proyecto, con un medio de comunicación/conexión adicional que brinda solución en caso de presentarse alguna contingencia dentro de la cooperativa.

Al inicio del caso práctico analice varias opciones, entre las cuales figuraban el montar una plataforma para impartición de cursos a manera de capacitación al personal, el desarrollo de una aplicación para la gestión de cobranza, entre algunas otras, pero al final me decidí a desarrollar el presente tema, primero porque me llama la atención sobremanera el estudio y diseño de redes de datos, el cómo es posible trasmitir información desde lugares distantes y llegar a colaborar con otras personas en tiempo real, aunque más me llama la atención los mecanismos de seguridad que se emplean para proteger los datos que se transmiten por medio de una red.

Con el presente proyecto se pretendía dar solución a una necesidad real y actual de Caja Popular Lagunillas que data de hace varios años y que al paso del tiempo se ha hecho más grande pero por los altos costos no se había podido implementar algún servicio que satisfará tal necesidad, lo cual se logró al realizar este proyecto.

Al inicio del documento, se explicó en que consiste una VPN, así como un estudio de la situación actual de la cooperativa, para así valorar las posibles soluciones al crear la VPN.

[7] Se había comentado en apartados anteriores sobre el plan de continuidad del negocio sobre que este aun está en proceso de elaboración. Se cuenta con un avance en este aspecto, pero aun no está autorizado.

Debido a que la parte más difícil se presentaba en los costos, se optó por enfocarse en el software Open Source y además gratuito (que no es lo mismo), decidiéndose finalmente por implementar OpenVPN por las características y ventajas que presenta respecto de otras aplicaciones, además de que se tenía la limitante también de que debería de implementarse la VPN con la infraestructura existente.

Considero que existen muchas alternativas en el mundo del Open Source que pueden ayudar a las empresas a reducir sus costos y rellenar todas esas lagunas tecnológicas que se presentan y que de alguna manera limitan su crecimiento.

En cuanto a las VPN existe mucha información que muestran sus ventajas y desventajas pero son una herramienta tecnológica que abre muchos campos de acción como el establecer conexiones seguras al lugar de trabajo para los empleados, pudiendo dar lugar al trabajo a distancia que aún no está muy difundido en nuestro país. Tal vez pudiera decirse que las VPN no son muy seguras, pero nos hemos dado cuenta a través de los años, que nada es 100% seguro y que aunque vean la luz nuevas tecnologías que permitan establecer mecanismos de protección más avanzados, siempre existirán otros mecanismos que permitan burlarlos.

Aunado a lo anterior está el desconocimiento de la gente, ya que se difunde el comentario de que las VPN no son seguras y se extiende el temor, pero no se investiga y me he dado cuenta de que una VPN bien configurada y en conjunto con otros dispositivos y/o aplicaciones, puede ser bastante segura.

Realizar este proyecto me ha permitido por un lado poner en práctica los conocimientos adquiridos durante la carrera, gracias al personal docente, el impulso que me ha dado la gente que me rodeo y un poco mis ganas de aprender y superarme, y por otro una nueva gama de conocimientos nuevos relacionados con el área de mi interés, la Informática y las TI.

Gracias a este proyecto tengo la capacidad y los conocimientos de implantar una VPN, además de haberlo podido constatar y probar tanto su funcionamiento como utilidad al aplicarlo en una empresa real como es Caja Popular Lagunillas.

Desde la instalación de la VPN a la fecha, se ha trabajado de manera eficiente y el servicio de la VPN ha dado frutos, ya que en un inicio se conectó solamente una sucursal (Morelia Siervo) como prueba, pero al ver su desempeño y ventajas, se implementó también en más sucursales (Morelia centro, Tzintzuntzan y Erongarícuaro), además de que hablando en términos económicos, a la fecha se han eliminado gastos a la cooperativa de un aproximado de $ 30,000.00, considerando que prácticamente son dos meses desde la implementación, y que la renta de un enlace dedicado con Uninet (Telmex) es de $ 7,500 mensuales por cada nodo, y si se considera esto, en el transcurso de dos años el ahorro ascendería a aproximadamente $ 360,000.00.

Por ultimo me gustaría comentar que me es grato el poder comprobar que los conocimientos adquiridos a través de mi paso por la UMSNH ya han dado sus primeros frutos al aplicarse en algo útil y me siento ahora con mayor capacidad que me motiva a buscar algo más allá de lo que ahora tengo y hago en mis actividades diarias.

Recomendaciones y Consideraciones Finales

- ✓ Primeramente y analizando las causas principales del desarrollo de este proyecto, sería muy recomendable aunque tal vez a largo plazo, el que se contrate un servicio adicional de conectividad, un enlace dedicado que brinde redundancia a las conexiones, ya que al depender la VPN del servicio de internet, si este falla, se pierde la conexión, lo que ocasionaría problemas en la atención a los socios.
- ✓ Considerar proteger más aun la VPN restringiendo el acceso mediante autenticación con usuario y contraseña.
- ✓ Sería recomendable la contratación de un servicio adicional de internet para separar lo que es la conexión normal al internet para los usuarios y lo que es la conexión de la VPN, esto aumentaría el rendimiento de la misma y se tendrá mayor control sobre ella.
- ✓ Otro factor que considero importante, es el que se trabaje sobre servidores Linux, ya que aparte de contar con distribuciones bastante robustas, también son opensource y cuentan con herramientas de administración y control de las conexiones mediante firewalls y proxies.
- ✓ El proyecto aquí presentado va encaminado solamente a la realización del caso práctico establecido en un principio, que es la conexión VPN sitio a sitio con lo cual se permita realizar la transmisión de datos al servidor SQL, cosa que se consiguió. Es por esta delimitación del caso, que no se entra en detalles más allá de lo ya establecido.

Glosario de Términos

Actualizar

Sustituir el software o firmware existente con una versión más moderna.

Adaptador

Dispositivo que añada funcionalidad de red a su equipo.

Ad-hoc

Grupo de dispositivos inalámbricos que se comunican directamente entre ellos (punto a punto) sin la utilización de un punto de acceso.

AES (Estándar avanzado de cifrado)

Técnica de cifrado de datos simétrica de bloque de 256 bits.

Ancho de banda

Capacidad de transmisión de un dispositivo o red determinado.

Banda ancha

Conexión a Internet de alta velocidad y siempre activa.

Banda ISM

Banda de radio utilizada en las transmisiones de redes inalámbricas.

Base de datos

Recopilación de datos que puede organizarse de forma que pueda sus contenidos puedan accederse, gestionarse y actualizarse fácilmente.

Bit (dígito binario)

La unidad más pequeña de información de una máquina.

Byte

Una unidad de datos que suele ser de ocho bits.

Cargar

Transmitir un archivo a través de una red.

Cifrado

Cifrado es la manipulación de datos para evitar que cualquiera de los usuarios a quienes no están dirigidos los datos, puedan realizar una interpretación precisa.

Conectividad

Estado que permite la transferencia de datos entre dos computadoras.

Conmutador (Switch)

1. Dispositivo que es el punto central de conexión de equipos y otros dispositivos de una red, de forma que los datos puedan transmitirse a velocidad de transmisión completa.
2. Dispositivo para realizar, interrumpir o modificar las conexiones de un circuito eléctrico.

DDNS (Sistema dinámico de nombres de dominio)

Permite albergar un sitio Web, servidor FTP o servidor de correo electrónico con un nombre de dominio fijo (por ejemplo, www.xyz.com) y una dirección IP dinámica.

Descargar

Recibir un archivo transmitido a través de una red.

DHCP (Protocolo de configuración dinámica de host)

Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.

Dirección IP

Dirección que se utiliza para identificar un equipo o dispositivo en una red.

Dirección IP dinámica

Dirección IP temporal que asigna un servidor DHCP.

Dirección IP estática

Dirección fija asignada a un equipo o dispositivo conectado a una red.

Dispersión de secuencia

Técnica de frecuencia de radio de banda ancha que se utiliza para la transmisión más fiable y segura de datos.

DNS (Servidor de nombres de dominio)

La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.

Dominio

Grupo de computadoras de la red que está administrada y controlada por el mismo servidor de red. Puede tener varios servidores pero una administración única para el control de permisos, recursos y seguridad.

DSL (Línea de suscriptor digital)

Conexión de banda ancha permanente a través de las líneas de teléfono tradicionales.

Dúplex competo

La disponibilidad de un dispositivo de red para recibir y transmitir datos de forma simultánea.

Dúplex medio

Transmisión de datos que puede producirse en dos direcciones a través de una única línea, pero sólo en una dirección cada vez.

EAP (Protocolo de autenticación extensible)

Protocolo general de autenticación que se utiliza para controlar el acceso a redes. Muchos métodos de autenticación específicos trabajan dentro de este marco.

EAP-PEAP (Protocolo de autenticación extensible-Protocolo de autenticación extensible protegido)

Método de autenticación mutua que utiliza una combinación de certificados digitales y otros sistemas, como contraseñas.

EAP-TLS (Protocolo de autenticación extensible-Seguridad de la capa de transporte)

Método de autenticación mutua que utiliza certificados digitales.

Enrutador (Ruteador)

Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

Enrutamiento estático

Reenvío de datos de una red a través de una ruta fija.

Ethernet

Protocolo de red estándar de IEEE que especifica la forma en que se colocan los datos y se recuperan de un medio de transmisión común.

Firewall

Sinónimo de dispositivo de software o hardware encargado de proteger cualquier sistema de la entrada de personas no autorizadas. Regula, según las necesidades, los niveles internos de restricción a la información y autoriza el acceso a cierto tipo de datos.

Fragmentación

Dividir un paquete en unidades menores al transmitirlas a través de un medio de red que no puede admitir el tamaño original del paquete.

Frame Relay

Paquetes retrasados. Protocolo de comunicación asíncrono con dispositivo especial que atrasa el envío de grupos de información para mandarlos en paquetes de tamaño fijo.

Frase secreta

se utiliza con mucha frecuencia como una contraseña, ya que una frase secreta simplifica el proceso de cifrado WEP generando de forma automática las claves del cifrado WEP para los productos Linksys.

FTP (Protocolo de transferencia de archivos)

Protocolo estándar de envío de archivos entre equipos a través de redes TCP/IP e Internet.

GUI

Medio de desplegar las salidas para presentar al usuario un formato gráfico.

Hardware

El aspecto físico de equipos, telecomunicaciones y otros dispositivos de tecnologías de la información.

HTTP (Protocolo de transferencia de hipertexto)

Protocolo de comunicaciones utilizado para conectarse a servidores de la World Wide Web.

IEEE (Instituto de ingenieros eléctricos y electrónicos)

Instituto independiente que desarrolla estándares de redes.

Infraestructura

Equipo de red e informático actualmente instalado.

Inicio

Iniciar un dispositivo y provocar que comience a ejecutar instrucciones.

Interface

Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.

Internet

Red de redes con base en TCP/IP y acceso público mundial.

IP (Protocolo Internet)

Protocolo utilizado para enviar datos a través de una red.

IPCONFIG

Utilidad de Windows 2000 y XP que muestra la dirección IP de un dispositivo de red concreto.

IPSec (Seguridad del protocolo Internet)

Protocolo VPN utilizado para implementar el intercambio seguro de paquetes en la capa IP.

ISP (Proveedor de servicios de Internet)

Compañía que proporciona acceso a Internet.

LAN (Red de área local)

Los equipos y productos de red que componen la red doméstica o de oficina.

LEAP (Protocolo de autenticación extensible ligero)

Método de autenticación mutua que utiliza un sistema de usuario y contraseña.

MAC (Dirección de control de acceso al medio)

Una dirección MAC es la dirección de hardware de un dispositivo conectado a un medio de red compartido.

Máscara de subred

Código de dirección que determina el tamaño de la red.

Mbps (Megabits por segundo)

Un millón de bits por segundo, unidad de medida de transmisión de datos.

Módem

Modulador-Demodulador. Dispositivo que convierte señales binarias a tonos transmisibles por vía telefónica.

Modo infraestructura

Configuración en la que se realiza un puente entre una red inalámbrica y una red con cable a través de un punto de acceso.

Multidifusión

Envío de datos a un grupo de destinos a la vez.

NAT

Corresponde a Network Address Translation - Traducción de Dirección de Red. Se trata de un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos, que incluyen información de direcciones dentro de la conversación del protocolo.

Navegador

Programa de aplicación que proporciona una forma de consultar e interactuar con la información de la World Wide Web.

Nodo

Unión de red o punto de conexión, habitualmente un equipo o estación de trabajo.

Paquete

Un paquete es un pequeño bloque de datos transmitido en una red de conmutación de paquetes.

Patch Panel

Centro de empalme. Lugar donde llegan todos los cableados para conexión a la infraestructura de red.

Peer-to-peer (p2p)

Igual a igual. Forma de comunicación de red donde cada uno tiene las mismas tareas en el proceso.

Ping (Buscador de paquetes de Internet)

Utilidad de Internet que se utiliza para determinar si una dirección IP determinada está en línea.

Pirata informático

Un término de jerga para un entusiasta informático. También hace referencia a los individuos que obtienen acceso no autorizado a sistemas informáticos con el fin de robar y corromper datos.

POP3 (Protocolo de oficina de correo 3)

Protocolo estándar utilizado para recuperar correo electrónico almacenado en un servidor de correo.

PPPoE (Protocolo a través de Ethernet punto a punto)

Tipo de conexión de banda ancha que proporciona autenticación (usuario y contraseña) además de transporte de datos.

PPTP (Protocolo de túnel punto a punto)

Protocolo VPN que permite tunelar el protocolo Punto a punto (PPP) a través de una red IP. Este protocolo se utiliza también como tipo de conexión de banda ancha en Europa.

Propietario

Término utilizado en computación para decir que la tecnología utilizada es desarrollada por la marca propia y no es similar a los estándares.

Protocolo

Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.

Puente

Dispositivo que conecta dos tipos diferentes de redes locales, como por ejemplo una red inalámbrica a una red Ethernet con cable.

Puerta de enlace

Un dispositivo que interconecta redes con protocolos de comunicaciones diferentes e incompatibles.

Puerta de enlace predeterminada

Dispositivo que redirecciona tráfico de Internet desde su red de área local.

Puerto

Punto de conexión en un equipo o dispositivo de red utilizado para conectar un cable o adaptador.

Punto de acceso

Dispositivo que permite a los equipos y a otros dispositivos equipados con función inalámbrica comunicarse con una red con cable. También se utiliza para ampliar el alcance de una red inalámbrica.

RADIUS (Servicio de usuario de marcado con autenticación remota)

Protocolo que utiliza un servidor de autenticación para controlar acceso a redes.

Red

Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.

Rendimiento

Cantidad de datos que se han movido correctamente de un nodo a otro en un periodo de tiempo determinado.

RJ-45 (Toma registrada 45)

Conector Ethernet que alberga hasta ocho hilos.

RTP (Protocolo de tiempo real)

Un protocolo que permite especializar aplicaciones tales como llamadas telefónicas, vídeo y audio a través de Internet que están teniendo lugar a tiempo real.

Servidor

Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.

Servidor de seguridad

Un servidor de seguridad es cualquiera de los esquemas de seguridad que evitan a los usuarios no autorizados obtener acceso a una red de equipos o que supervisa la transferencia de información hacia y desde la red.

SMTP (Protocolo simple de transferencia de correo)

Protocolo de correo electrónico estándar de Internet.

SNMP (Protocolo simple de administración de redes)

Protocolo de control y supervisión de redes ampliamente extendido.

Software

Instrucciones para el equipo. Se denomina "programa" al conjunto de instrucciones que realizan una tarea determinada.

SQL

El lenguaje de consulta a la base de datos cliente/servidor más conocido.

Tasa TX

Tasa de transferencia.

TCP (Protocolo de control de transporte)

Un protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

TCP/IP (Protocolo de control de transporte/Protocolo Internet)

Protocolo de red para la transmisión de datos que requiere la confirmación del destinatario de los datos enviados.

Telnet

Comando de usuario y protocolo TCP/IP que se utiliza para acceder a equipos remotos.

Tiempo Real

Dominación de aquellos procesos que suceden simultáneamente o con una diferencia imperceptible de tiempo. Internet ofrece tiempo real dentro de muchos servicios donde a la ejecución de una acción existe una respuesta inmediata (llegada de correo electrónico).

TLS (Seguridad de capa de transporte)

Protocolo que garantiza la privacidad y la integridad de los datos entre aplicaciones cliente/servidor que se comunican a través de Internet.

Topología

Distribución física de una red.

UDP (Protocolo de datagramas de usuario)

Protocolo de red para la transmisión de datos que no requieren la confirmación del destinatario de los datos enviados.

URL (Localizador uniforme de recursos)

Dirección de un archivo situado en Internet.

VPN (Red privada virtual)

Medida de seguridad para proteger los datos a medida que abandona una red y pasa otra a través de Internet.

WAN (Red de área extensa)

Grupo de equipos conectados en red en un área geográfica extensa. El mejor ejemplo de WAN es Internet.

Bibliografía

Aníbal R. Figueiras Vidal, A. A. (2002). *Una panorámica de las telecomunicaciones.* Madrid, España: Pearson Educación.

Bidgoli, H. (2004). *The Internet encyclopedia, volumen 1*. Hoboken, New Jersey: John Wiley and Sons.

Cafassi, E. (1998). *Internet: Políticas y Comunicación.* Buenos Aires, Argentina: Editorial Biblos.

Feilner, M. (2006). *Open VPN: building and operating virtual private networks.* Birmingham: Packt Publishing Ltd.

Fitzpatrick, J. (09 de Marzo de 2010). *lifehacker*. Recuperado el 28 de Agosto de 2011, de lifehacker: http://lifehacker.com/5489252/best-vpn-tool-openvpn

Halcón, J. P. (2006). *Devenires cíborg: arquitectura, urbanismo y redes de comunicación.* Sevilla, España: Universidad de Sevilla.

InfoWorld. (10 de Septiembre de 2007). *InfoWorld*. Recuperado el 28 de Agosto de 2011, de InfoWorld: http://www.infoworld.com/d/security-central/best-open-source-in-security-122?page=0,1

Jerry FitzGerald, A. D. (2008). *Business Data Communications and Networking.* Bloomington, Indiana: John Wiley and Sons.

John R. Levine, M. L. (2010). *The Internet For Dummies 12th Edition.* Hoboken, New Jersey: Wiley Publishing, Inc.

Lackerbauer, I. (2001). *Internet.* Barcelona: Marcombo.

Martínez, J. (2002). *Redes de Comunicaciones.* Valencia: Universidad Politécnica de Valencia.

Merlos, J. M. (01 de Octubre de 2005). *http://www.merlos.org.* Recuperado el 20 de Septiembre de 2011, de http://www.merlos.org: http://www.merlos.org/documentos/linux/28-configuracion-de-una-red-privada-virtual-con-openvpn.html

Moya, J. M. (2005). *Sistemas telemáticos.* Madrir, España: Editorial Paraninfo.

OpenVPN Technologies, I. (25 de Marzo de 2002). *OpenVPN Technologies*. Recuperado el 18 de Agosto de 2011, de OpenVPN Technologies: http://www.openvpn.net/

OpenVPN Technologies, I. (01 de Enero de 2008). *http://openvpn.net*. Recuperado el 03 de Septiembre de 2011, de http://openvpn.net: http://openvpn.net/index.php/open-source/documentation/howto.html#examples

OpenVPN Technologies, I. (17 de Noviembre de 2008). *http://www.openvpn.net*. Recuperado el 15 de Septiembre de 2011, de http://www.openvpn.net: http://www.openvpn.net/index.php/open-source/documentation/manuals/69-openvpn-21.html

Tomás Cánovas, J. J. (2008). *Servicio VPN de acceso remoto basado en SSL mediante OpenVPN.* Cartagena: 2008.

TRUSTe. (18 de Octubre de 2010). *http://www.truste.com*. Recuperado el 02 de Diciembre de 2010, de http://www.truste.com: http://www.truste.com/about_TRUSTe/press-room/news_truste_2010_survey_snsprivacy.html

Anexos

- ✓ **Políticas de Planeación 2010.**
- ✓ **Documentos probatorios de la implementación de la VPN y su correcto funcionamiento.**