UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

TEMA:

"VPN PARA FACILITAR LA COMUNICACIÓN ENTRE LAS OFICINAS CENTRALES Y LAS BODEGAS DE LA CONSTRUCTORA LOPEZ CÍA. LTDA."

Trabajo estructurado de manera independiente, como requisito previo a la obtención del Título de Ingeniero en Sistemas Computacionales e Informáticos.

Autor: Sr. Paúl Espinoza.

Tutor: Ing. David Guevara.

Ambato- Ecuador

Febrero - 2010

APROBACIÓN DEL TUTOR

En calidad de Tutor del tema de investigación: “VPN PARA FACILITAR LA COMUNICACIÓN ENTRE LAS OFICINAS CENTRALES Y LAS BODEGAS DE LA CONSTRUCTORA LOPEZ CÍA. LTDA.”, del Sr. Paúl Fernando Espinoza Romero, estudiante de la carrera de Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, considero que el informe investigativo se encuentra listo para la evaluación de conformidad con el Art. 68 del Capítulo IV Pasantías del Reglamento de Graduación de Pre-grado de la Universidad Técnica de Ambato.

.

Ambato, Febrero del 2010

Tutor

_____

Ing. David Guevara A. Msc.

AUTORÍA

El presente trabajo de investigación: “VPN PARA FACILITAR LA COMUNICACIÓN ENTRE LAS OFICINAS CENTRALES Y LAS BODEGAS DE LA CONSTRUCTORA LOPEZ CIA. LTDA.”, es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Febrero 2010

_____

Paúl Espinoza

C.C. 1803548104

APROBACIÓN DEL TRIBUNAL DE CALIFICACIÓN

El Tribunal de calificación conformado por los señores: Ing. Clay Aldás, Ing. Carlos Gordón, aprueban el presente trabajo de graduación o titulación Trabajo Estructurado de Manera Independiente titulado: “VPN PARA FACILITAR LA COMUNICACIÓN ENTRE LAS OFICINAS CENTRALES Y LAS BODEGAS DE LA CONSTRUCTORA LOPEZ CIA. LTDA.”, presentado por el Sr. Paúl Fernando Espinoza Romero.

Ambato, Febrero 2010

_____

Ing. M.Sc. Oswaldo Paredes
PRESIDENTE DEL TRIBUNAL

_____ _____

Ing. M.Sc. Clay Aldás
MIEMBRO DEL TRIBUNAL

Ing. M.Sc. Carlos Gordón
MIEMBRO DEL TRIBUNAL

DEDICATORIA

Este trabajo lo dedico a mis padres Fernando y Carmita, a mis hermanos, Víctor y David, ya que ellos son y serán siempre el motivo por el cual debo superarme; a mis abuelitos “Papi Beto”, “Mami Tela” y a mi tía Mony, porque ellos han estado, están y estarán a mi lado siempre.

AGRADECIMIENTO

Agradezco a Dios por haberme permitido llegar hasta aquí, al Ing. David Guevara por su valioso aporte para el desarrollo de este trabajo, al Ing. Carlos López por abrirme las puertas de su empresa y brindarme todo el apoyo para la elaboración de esta investigación, a Caro porque ha estado siempre a mi lado en las buenas y las malas, a mis amigos y compañeros:, Cindy, Roberto, Carlos y Oscar; por haber sido un apoyo incondicional durante mi carrera.

ÍNDICE GENERAL

CAPÍTULO III. METODOLOGÍA

CAPÍTULO IV. ANÁLISIS E INTERPRETACION DE RESULTADOS

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES.

CAPÍTULO VI. PROPUESTA

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

El ingeniero Carlos López tiene 50 años, lleva ya 25 de profesional, graduado de la Universidad Central de Quito en el año de 1982. En el año 1983 fue Director de Obras Públicas del cantón Patate y desde 1988 se desempeñó como constructor privado dedicado por entero a la contratación pública.

La Constructora tiene 25 años de existencia y se ha ido fortaleciendo en cuanto a infraestructura y personal. Cuenta con personal técnico y un gran equipo administrativo.

Tiene maquinaria moderna, equipo de choferes y operadores con experiencia, personal altamente calificado. La Constructora López construye sistemas de agua potable y alcantarillado, urbanizaciones, edificios. Es importante destacar el servicio de agregados en materiales como arena, ripio, piedra, en maquinaria como concretera, vibrador, elevador, compactador, encofrados, y equipos como retroexcavadoras, cargadoras y volquetas.

Debido al crecimiento de la Constructora, ésta ha adquirido el problema de la comunicación entre las oficinas centrales y la bodega. Todavía no existe una propuesta clara y concisa para resolver este problema. Por esta razón, los empleados se ven afectados en el correcto cumplimiento de sus labores en la Constructora; ya que la comunicación entre las oficinas centrales y la bodega se da de una manera deficiente.

Por esta razón se diseñará una VPN para facilitar la comunicación entre las oficinas centrales y la bodega tomando como referencia los conocimientos adquiridos. Con este trabajo se logrará un enriquecimiento profesional ayudando a la solución de este problema.

INTRODUCCIÓN

CAPÍTULO I “EL PROBLEMA”

En el desarrollo de este capítulo se explica la situación actual de la Constructora, es decir, la forma de comunicarse entre las diferentes dependencias de la empresa. Por esta razón se presenta el planteamiento de problema, así como la justificación del mismo, exponiendo el estudio y desarrollo de la investigación.

CAPÍTULO II “MARCO TEORICO”

Este capítulo expresa los conceptos, términos y software en los que se basa la presente investigación para su desarrollo.

CAPÍTULO III “METODOLOGIA”

Aquí se da a conocer la forma en que se hizo la investigación, estableciendo los instrumentos, modalidades y procesamiento de la información.

CAPÍTULO IV “ANALISIS E INTERPRETACIÓN DE RESULTADOS”

Se sintetiza el análisis de transferencia de información a través de la VPN y todo lo que conlleva este proceso; para finalmente interpretarlo y obtener conclusiones.

CAPÍTULO V “CONCLUSIONES Y RECOMENDACIONES”

Este capítulo hace referencia a las soluciones y sugerencias de los conceptos más importantes de esta investigación.

CAPÍTULO VI “PROPUESTA”

Se muestra la alternativa para la solución del problema de la empresa, dando a conocer sus beneficios prácticos.

CAPÍTULO I
EL PROBLEMA

1.1 Tema.

“VPN PARA FACILITAR LA COMUNICACIÓN ENTRE LAS OFICINAS CENTRALES Y LAS BODEGAS DE LA CONSTRUCTORA LOPEZ CIA. LTDA.”.

1.2 Planteamiento del Problema.

Inadecuado sistema de comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda.

1.2.1 Contextualización.

La Constructora López Cía. Ltda. en la actualidad está experimentando un crecimiento en las necesidades de uso de recursos informáticos y de comunicación, por cuanto se ha planteado la necesidad de participar de los procesos administrativos y financieros a todo el personal que lo requiere, para brindar un óptimo servicio a sus usuarios a través de la correcta compartición de los recursos informáticos en los departamentos de la Constructora.

Desde este punto de vista se requiere implementar un sistema de comunicación que permita llegar a los objetivos de automatización de las transacciones, las mismas que requieren un proceso de información rápido, eficiente y con gran disponibilidad; por tal motivo se implantará un medio de comunicación acorde a dichos requerimientos, que en muchos casos es complejo y conlleva un gran número de transacciones.

Hoy en día en el Ecuador, especialmente en las empresas se cuenta con un sistema de comunicación saturado y a veces lento, por las transacciones que se realizan a diario.

La estructura de comunicación con la que trabaja actualmente la Constructora López Cía. Ltda., no cumple con las necesidades que tiene esta, consecuentemente surge la necesidad de proponer el análisis y diseño de una VPN para modernizar y mejorar la comunicación entre los diferentes ambientes de trabajo, que físicamente están en lugares diferentes.

Por lo mencionado anteriormente, para el análisis y diseño de una VPN en la institución, se aplicará la estrategia de funcionamiento de una Red Privada Virtual, que permitirá mejorar la comunicación entre las oficinas centrales y las bodegas de manera óptima, segura y fiable.

1.2.2 Análisis Crítico.

La demora en la asignación de materiales de construcción en la institución se debe a que no existe un sistema de comunicación que permita interconectar las oficinas centrales con las bodegas, ya que en la actualidad se comunican por medio de la vía telefónica.

En la institución, varias veces se da, el desconocimiento por parte de las oficinas centrales de la existencia de material depositado en las bodegas; como efecto de esto se da el gasto innecesario en la asignación de los recursos en los diferentes proyectos que realiza la Constructora.

La comunicación inadecuada entre las oficinas centrales y las bodegas, la podemos asociar con el inadecuado proceso de comunicación que nos brinda la vía telefónica; ya que esta alternativa de comunicación varias veces colapsa y provoca pérdida de tiempo y trabajo.

1.2.3 Prognosis

Si no se implementase una VPN para la empresa, se produciría pérdidas económicas cada vez más importantes, influyendo de esta manera en el extravío de información valiosa para la institución debido a las fallas de dicho sistema de comunicación.

1.3 Formulación del Problema.

¿Cuáles son los inconvenientes que causa la falta de un adecuado sistema de comunicación entre las oficinas centrales y las bodegas de la Constructora López?

1.4 Delimitación del Problema.

Campo: Constructora López Cía. Ltda.

Aspecto: VPN (Red Privada Virtual).

Tema: VPN para facilitar la comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda.

Problema: Inadecuado sistema de comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda.

Espacial: VPN para la Constructora López Cía. Ltda., que está ubicada en la Cdla. Cristóbal Colón, calle Vasco Núñez de Balboa 171 y Rodrigo de Triana, en la ciudad de Ambato, provincia de Tungurahua.

Temporal: El presente proyecto tendrá una duración estimada de ocho meses, iniciándose en el mes de Julio del año 2009 hasta el mes de Febrero del año 2010.

Social: El estudio se realizará en la Constructora López Cía. Ltda.

1.5 Justificación.

Uno de los aspectos que toda empresa debe considerar como elemento de proyección a la sociedad, es la calidad en los servicios que oferta. Disponer de un sistema de comunicación eficiente, dinámico, seguro, acorde a las nuevas necesidades de la sociedad resulta ser de vital importancia; ya que posibilita ampliar la calidad en los servicios a través del desarrollo de nuevas aplicaciones, mejora en la velocidad de acceso y sobre todo, dar solución a los problemas inherentes al crecimiento en la oferta de servicios referentes a la construcción en la sociedad.

Durante el proceso para realizar una transacción en la Constructora; tanto el cliente como el empleado requieren de un constante intercambio de información, dicho intercambio se vuelve más frecuente si se presentan ciertos cambios en los requerimientos de la transacción, ya que en esta actividad se involucran aspectos como el tiempo de espera en la respuesta a la petición de información, incremento en el papeleo y aumento en el uso de los recursos necesarios para conocer el estado de la transacción de datos para la correcta realización del trámite que el cliente requiere.

Por los aspectos expuestos anteriormente, se realizará el análisis y diseño de una VPN, que es imprescindible para la correcta comunicación entre las oficinas centrales y las bodegas, buscando de esta manera maximizar la fiabilidad y eficiencia del sistema de comunicación de la institución.

Debido que en el país se ha provocado un gran avance tecnológico en el campo de las comunicaciones, la Constructora ha creído pertinente llevar a cabo la ejecución de una VPN que satisfaga las necesidades de compartición de recursos informáticos.

La consecución del presente trabajo investigativo aportará al correcto funcionamiento de todas las actividades que se realiza en la Constructora López Cía. Ltda., logrando que estas se cumplan de manera eficiente, dinámica y segura; garantizando el trabajo efectivo para dar solución al problema tomando como referencia los conocimientos adquiridos durante los años de estudio.

1.6 Objetivos de la Investigación.

1.6.1 Objetivo General.

Diseñar una Red Privada Virtual (VPN) para facilitar la comunicación entre oficinas centrales y bodegas de la constructora López Cía. Ltda.

1.6.2 Objetivos Específicos.

- Analizar los procesos y niveles de comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda.
- Realizar un estudio sobre los requerimientos, bondades técnicas y seguridades de una VPN en los procesos de comunicación entre oficinas.
- Plantear una propuesta que facilite la comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda. mediante el diseño de una VPN.

CAPÍTULO II.
MARCO TEÓRICO.

2.1 Antecedentes Investigativos.

Luego de realizar una consulta previa para revisar temas semejantes a la presente investigación, se encontró que existe un proyecto similar a este titulado: “ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE VPN´s A TRAVÉS DE INTERNET EN LA OPERADORA DE TURISMO QUIMBAYA TOURS INTERNATIONAL HOLDING”, realizado por: Cecilia Díaz y Mónica García; lo que servirá como referencia para el desarrollo de una VPN en la Constructora López Cía. Ltda.

2.2 Fundamentación Legal

El presente proyecto se fundamenta en las siguientes leyes y reglamentos:

- La Constructora López Cía. Ltda. está constituida legalmente, inscrita en el registro mercantil #701 y registrada en la Superintendencia de Compañías.
- Estatuto de la Universidad Técnica de Ambato para la realización de trabajo estructurado de manera independiente.

2.3 Categorías Fundamentales.

2.3.1 Fundamentación de una VPN (Red Privada Virtual).

2.3.1.1 Redes de Computadoras.

Una red de computadoras es una interconexión de computadoras para compartir información, recursos y servicios. Esta interconexión puede ser a través de un enlace físico o inalámbrico.

2.3.1.2 Clasificación de las Redes.

Red de Área Local (LAN).

Es la interconexión de varios computadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de 200 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadores personales y estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

En una empresa suelen existir muchos computadores, los cuales necesitan de su propia impresora para imprimir informes, los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa, por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de dos usuarios, la ocupación de los recursos de almacenamiento en disco se multiplican, los computadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos, etc.

La solución a estos problemas se llama red de área local, esta permite compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia de software) y periféricos como puede ser un módem, una tarjeta RDSI (Red Digital de Servicios Integrados), una impresora, etc. (se elimina la redundancia de hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.

Además una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de banda ancha compartida por varios computadores conectados en red.

Entre las características más importantes tenemos:

- Tecnología broadcast (difusión) con el medio de transmisión compartido.
- Cableado específico instalado normalmente a propósito.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km.
- Uso de un medio de comunicación privado.
- La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
- La facilidad con que se pueden efectuar cambios en el hardware y el software.
- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.
- Limitante de 100 m.

Red de Área Metropolitana (MAN).

es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas, por su baja latencia (entre 1 y 50ms), gran estabilidad y la carencia de interferencias radioeléctricas, las redes MAN BUCLE, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

Disponibilidad referida al porcentaje de tiempo en el cual la red trabaja sin fallos. Las redes de área metropolitana tienen mecanismos automáticos de recuperación frente a fallos, en el caso del cable de cobre se utiliza el bonding EFM (Ethernet Fórum Metro), permitiendo la agregación de caudal en múltiples cables. El bonding EFM permite a la red recuperar la operación normal, ante la rotura de uno de los cables. Cualquier fallo en un nodo de acceso o cable es detectado rápidamente y aislado. Las redes MAN son apropiadas para entornos como control de tráfico aéreo, aprovisionamiento de almacenes, bancos y otras aplicaciones comerciales donde la indisponibilidad de la red tiene graves consecuencias.

Fiabilidad referida a la tasa de error de la red mientras se encuentra en operación. Se entiende por tasa de error el número de bits erróneos que se transmiten por la red. En general la tasa de error para fibra óptica es menor que la del cable de cobre a igualdad de longitud. La tasa de error no detectada por los mecanismos de detección de errores es del orden de 10-20. Esta característica permite a la redes de área metropolitana trabajar en entornos donde los errores pueden resultar desastrosos como es el caso del control de tráfico aéreo. La creación de redes metropolitanas municipales, permitirá a los Ayuntamientos contar con una infraestructura de altas prestaciones, se trata de construir una infraestructura, parecida a la de los operadores de la localidad, para "autoprestación", de esta

forma el ayuntamiento puede conectar nuevas sedes, usuarios remotos, videocámaras en la vía pública y un largo etc. en la vida de las TIC (Tecnologías de Información y Comunicación).

La fibra óptica y el cable, son un medio seguro, porque no es posible leer o cambiar la señal sin interrumpir físicamente el enlace. La rotura de un cable y la inserción de mecanismos ajenos a la red implica una caída del enlace de forma temporal, además se requiere acceso y actuación sobre el cable físico, aun que este tipo de actuaciones pasen fácilmente desapercibidas.

Red de Área Amplia (WAN).

Es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente. Un ejemplo de este tipo de redes sería red iris, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

En una empresa suelen existir muchos computadores, los cuales necesitan de su propia impresora para imprimir informes (redundancia de hardware), los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa, por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de dos usuarios, la ocupación de los recursos de almacenamiento en disco se multiplican (redundancia de datos), los computadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos (redundancia de software), etc.

La solución a estos problemas se llama red de área local, esta permite compartir bases de datos (se elimina la redundancia de datos), programas (se elimina la redundancia de software) y periféricos como puede ser un módem, una tarjeta

RDSI, una impresora, etc. (se elimina la redundancia de hardware); poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.

Además una red de área local conlleva un importante ahorro, tanto de tiempo, ya que se logra gestión de la información y del trabajo, como de dinero, ya que no es preciso comprar muchos periféricos, se consume menos papel, y en una conexión a Internet se puede utilizar una única conexión telefónica o de banda ancha compartida por varios computadores conectados en red.

Ente las características más importantes están:

- Tecnología broadcast (difusión) con el medio de transmisión compartido.
- Cableado específico instalado normalmente a propósito.
- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Extensión máxima no superior a 3 km.
- Uso de un medio de comunicación privado.
- La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
- La facilidad con que se pueden efectuar cambios en el hardware y el software.
- Gran variedad y número de dispositivos conectados.
- Posibilidad de conexión con otras redes.

DSL (Línea de Suscripción Digital).

DSL (Línea del Subscriptor Digital) Una línea de DSL puede llevar datos y signos de la voz y los datos parten de la línea se conecta continuamente. Las instalaciones de DSL empezaron en 1998 y continuarán a un paso grandemente aumentado a través de la próxima década en varios comunidades en el EE.UU. y en otra parte del mundo. Compaq, Intel, y Microsoft que trabajan con las compañías del teléfono han desarrollado una norma más fácil, se espera que DSL reemplace RDSI en muchas áreas y para competir con el módem del cable trayendo multimedios y 3-D a casas y los negocios pequeños.

Básicamente el funcionamiento es el siguiente:

Un dispositivo de la entrada como una toma fijas telefónicas un signo acústico (qué es un signo analógico natural) y convertido él en un equivalente eléctrico por lo que se refiere al volumen (la amplitud señalada) y diapasón (la frecuencia de cambio de la ola). Desde que la compañía del teléfono está señalando ya es fijo a para esta transmisión de la ola analógica, es más fácil para él usar que como la manera de volver la información entre su teléfono y la compañía del teléfono. Eso es por qué su computadora tiene que tener un módem - para que pueda modular el signo analógico y puede convertir sus valores en el cordón de 0 y 1.

La transmisión analógica sólo usa una porción pequeña de la cantidad disponible de información que podría transmitirse encima de los alambres de cobre, la cantidad máxima de datos que usted puede recibir usando los módems ordinarios es aproximadamente 56 Kbps. La habilidad de su computadora de recibir la información está encogida por el hecho que la compañía del teléfono se filtra información que llega como los datos digitales, lo pone en la forma analógica para su línea telefónica, y exige a su módem cambiarlo atrás en digital. En otros términos, la transmisión analógica entre su casa o negocio y la compañía telefónica es un cuello de botella del banda ancha.

La Línea del Subscriptor digital es una tecnología que asume los datos digitales no requiere el cambio en la forma analógica. Los datos digitales se transmite directamente a su computadora como los datos análogos y esto permite la compañía telefónica usar una banda ancha para transmitirlo al usuario.

La banda ancha apoyado por un típico par cobrizo es 1 megahertzio (MHz), y el banda ancha es hendido en tres pedazos. Cuando usted hace una llamada telefónica, el sonido se envía terminado de estos pedazos a las frecuencias debajo de 4 kilohertzio (KHz). Los datos enviado de una computadora de la casa al Internet usa otro pedazo del banda ancha, y el datos enviado del Internet a la computadora de la casa usa un tercer pedazo. Esto da usted la habilidad de hablar por teléfono mientras transmitiendo un archivo sin interferir con la velocidad de ser transmitida.

ADSL (Línea de Suscripción Digital Asimétrica).

ADSL es un tipo de línea DSL. Consiste en una transmisión de datos digitales (la transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 km. medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

Frecuencias usadas en ADSL. El área roja es el área usada por la voz en telefonía normal, el verde es el upstream o subida de datos y el azul es para el downstream o descarga de datos.

Es una tecnología de acceso a Internet de banda ancha, lo que implica una mayor velocidad en la transferencia de datos. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3800 Hz), función que realiza el Router ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro (llamado splitter o discriminador) que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL.

Esta tecnología se denomina asimétrica debido a que la capacidad de descarga (desde la Red hasta el usuario) y de subida de datos (en sentido inverso) no

coinciden. Normalmente, la capacidad de bajada (descarga) es mayor que la de subida.

En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal.

ADSL presenta una serie de ventajas y también algunos inconvenientes, respecto a la conexión telefónica a Internet por medio de un modem.

Ventajas

- Ofrece la posibilidad de hablar por teléfono mientras se navega por Internet, ya que, como se ha indicado anteriormente, voz y datos trabajan en bandas separadas, lo cual implica canales por separados.
- Usa una infraestructura existente (la de la red telefónica básica). Esto es ventajoso, tanto para los operadores que no tienen que afrontar grandes gastos para la implantación de esta tecnología, como para los usuarios, ya que el costo y el tiempo que tardan en tener disponible el servicio es menor que si el operador tuviese que emprender obras para generar nueva infraestructura.
- Los usuarios de ADSL disponen de conexión permanente a Internet, al no tener que establecer esta conexión mediante marcación o señalización hacia la red. Esto es posible porque se dispone de conexión punto a punto, por lo que la línea existente entre la central y el usuario no es compartida, lo que además garantiza un ancho de banda dedicado a cada usuario, y aumenta la calidad del servicio. Esto es comparable con una arquitectura de red conmutada.
- Ofrece una velocidad de conexión mucho mayor que la obtenida mediante marcación telefónica a Internet. Éste es el aspecto más interesante para los usuarios.
- La posibilidad de usar la telefonía IP para llamadas de larga distancia (antes demasiado costosas), hace que el servicio telefónico básico se ofrezca actualmente por las operadoras como un servicio añadido, más que un uso principal, ofertándose tarifas planas para su uso.

Inconvenientes

- En algunos países, no existe la posibilidad de dar de alta el ADSL independientemente de la línea de teléfono fijo.
- No todas las líneas telefónicas pueden ofrecer este servicio, debido a que las exigencias de calidad del par, tanto de ruido como de atenuación, por distancia a la central, son más estrictas que para el servicio telefónico básico. De hecho, el límite teórico para un servicio aceptable, equivale a 5 km.
- Debido que requieren estas líneas, el servicio no es económico en países con pocas o malas infraestructuras, sobre todo si lo comparamos con los precios en otros países con infraestructuras más avanzadas.
- El router necesario para disponer de conexión, o en su defecto, el módem ADSL, es caro (en menor medida en el caso del módem). No obstante, en algunos países es frecuente que los ISP´s subvencionen ambos aparatos.
- Se requiere una línea telefónica para su funcionamiento, aunque puede utilizarse para cursar llamadas.
- El servicio no es muy estable.

Internet.

Internet es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP (Protocolo de Control de Transferencia/Protocolo de Internet), garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada), entre tres universidades en California y una en Utah, Estados Unidos.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre

ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto.

2.3.1.3 Red Privada Virtual (VPN).

2.3.1.3.1 Introducción.

Con una red privada virtual (VPN), los usuarios remotos, que pertenecen a una red privada, puedes comunicarse de una forma libre y segura entre redes remotas, a través de redes públicas (Internet).

Una VPN normalmente usa el Internet como transporte para establecer enlaces seguros, extendiendo las comunicaciones a oficinas aisladas. Decrece significativamente el coste de las comunicaciones, porque el acceso a Internet el local y mucho más barato que las conexiones mediante acceso remoto a servidores.

Una red privada virtual transporta de manera segura por medio de Internet a través de un túnel establecido entre dos puntos, con un esquema de encriptación y autenticación para dicho transporte. Una VPN permite el acceso remoto a servicios de red de forma transparente y segura con seguridad. Las VPN´s están implementadas con firewalls, routers, para lograr esa encriptación y autenticación deseada.

2.3.1.3.2 Características de una VPN.

Las VPN´s permiten:

- La administración y ampliación de la red corporativa al mejor costo-beneficio.
- La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas.

- Los requisitos indispensables para esta interconectividad son: Políticas de seguridad.
- Requerimiento de aplicaciones en tiempo real. Compartir datos, aplicaciones y recursos.
- Servidor de acceso y autentificación.

2.3.1.3.3 Conexiones Remotas.

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentica al servidor de acceso remoto, y el servidor se autentica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall ASA a firewall ASA

Una conexión VPN firewall ASA (Adaptive Security Appliance) a firewall ASA es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentica ante el que responde y éste a su vez se autentica ante el llamante.

2.3.1.3.4 Fundamentos Básicos.

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

Los datos son codificados o cifrados e inmediatamente enviados a través de la conexión, para de esa manera asegurar la información y la contraseña que se esté enviando.

Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet. Esto reduce el trabajo y riesgo en una gestión de red.

La tecnología de túneles esta basado en estándares. Esta tecnología permite transmitir datos entre dos redes similares. A esto también se llama "encapsulación", es decir, a la tecnología que coloca algún tipo de paquetes dentro de otro protocolo (TCP). Aparte de todo esto, también se añade otra información necesaria para poder descifrar la información que se encuentra codificada. Estos paquetes llegan a su destino después de haber atravesado Internet, pero para verificar que ha llegado al destino correcto se realiza un proceso de autentificación.

Las VPN´s son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios porque por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Chile, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más

económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre si.

2.3.1.3.5 Requerimientos Básicos.

Por lo general cuando se desea implantar una VPN hay que asegurarse que esta proporcione:

- Identificación de usuario.
- Administración de direcciones.
- Codificación de datos.
- Administración de claves.
- Soporte a protocolos múltiples.
- Identificación de usuario.
- La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, que información y cuando.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Codificación de datos

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet (IP), el intercambio de paquete de Internet (IPX) entre otros.

2.3.1.3.6 Tipos de VPN.

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

Tunneling

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP (Protocolo de Transferencia de Hipertexto), FTP (Protocolo de Transferencia de Achivos), POP3 (Protocolo 3 de Correo) y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in the middle), como es el caso de la red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las

máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida.

Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos. Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling.

Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (Secure Shell), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de ssh) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos.

VPN interna VLAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

VPN Dinámicas

Proporciona además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPN´s Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información. Alguna de las características que se proporciona son las siguientes: Proporciona una seguridad importante para la empresa. Se ajusta dinámicamente al colectivo dispar de usuarios. Permite la posibilidad de intercambio de información en diversos formatos. El ajuste que hace para cada usuario lo consigue gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc. Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple pero controlado. Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

2.3.1.3.7 Internet como medio de Interconexión de una VPN.

Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos computadores son encriptados por el Point-to-Point Protocol, también conocido como PPP, un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP. Una Red Privada Virtual es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes

localizaciones geográficas. Es una red de datos de gran seguridad que permite la transmisión de información confidencial entre la empresa y sus sucursales, socios, proveedores, distribuidores, empleados y clientes, utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Así, las VPN constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y lo escalable del acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPN´s una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización.

2.3.1.3.8 Funcionamiento Básico de una VPN.

1. El usuario remoto marca a su ISP local y se conecta a la red del ISP de forma normal.

2. Cuando desea conectarse a la red corporativa, el usuario inicia el túnel mandando una petición a un servidor VPN de la red corporativa.

3. El servidor VPN autentica al usuario y crea el otro extremo del túnel.

4. El usuario comienza a enviar datos a través del túnel, que son cifrados por el software VPN (del cliente) antes de ser enviados sobre la conexión del ISP.

5. En el destino, el servidor VPN recibe los datos y los descifra, propagando los datos hacia la red corporativa. Cualquier información enviada de vuelta al usuario remoto también es cifrada antes de enviarse por Internet.

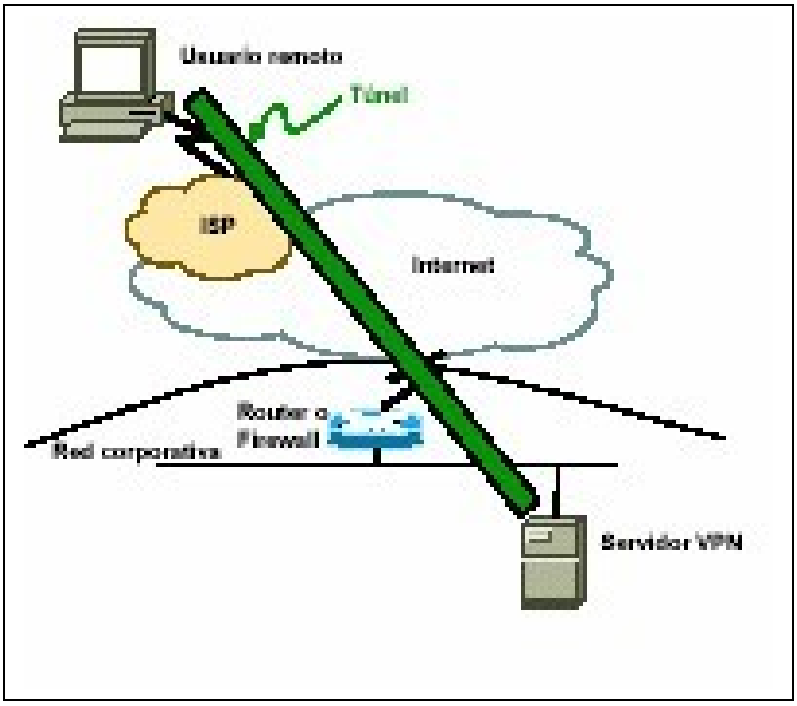


Fig. 2.1 Esquema básico de una VPN

2.3.1.3.9 Seguridad en una VPN.

La solidez de la seguridad de las soluciones VPN permite que las organizaciones aprovechen al máximo la conveniencia y ahorros en los costos de conexión por el túnel a través del Internet, sin permitir el acceso no autorizado.

Un túnel VPN funciona mediante la encapsulación de datos dentro de paquetes IP para transportar información que no cumple de ninguna forma con los estándares

de direccionamiento en Internet. Posteriormente, estos paquetes encapsulados se transportan entre una red, o cliente único, y otra red sobre una red intermedia. A todo este proceso de encapsulación y transmisión de paquetes se le conoce como conexión por túnel. Un túnel es una conexión a través del Internet. El resultado es que los usuarios remotos se convierten en nodos virtuales en la red a la que han sido conectados por túnel. Desde la perspectiva del usuario, la naturaleza de la red física que ha sido conectada por túnel es irrelevante ya que aparece como si la información haya sido enviada sobre una red privada dedicada.

La comunicación a través de Internet requiere que, tanto la encapsulación como la encriptación de flujo de datos, sea viable. PPTP (Protocolo de Túnel Point to Point) y L2TP (Protocolo de Túnel Capa 2) proporcionan servicios de encapsulación, a fin de facilitar las comunicaciones de protocolos múltiples mediante Internet. La encapsulación permite que los paquetes de datos no basados en IP se comuniquen a través de Internet basada en IP desde un cliente remoto a una LAN corporativa privada, la cual permite que las redes no basadas en IP aprovechen al máximo el Internet.

2.3.1.4 OpenVPN.

2.3.1.4.1 Introducción.

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

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

Es una solución multiplataforma que ha simplificado mucho la configuración de VPN´s dejando atrás los tiempos de otras soluciones difíciles de configurar como IPsec (Protocolo de Internet Seguro) y haciéndola más accesible para gente inexperta en este tipo de tecnología.

Supongamos que necesitamos comunicar diferentes sucursales de una organización. A continuación veremos algunas soluciones que se han ofrecido como respuesta a este tipo de necesidades.

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

Dichos factores son:

- La aceleración de los procesos de negocios y su consecuente aumento en la necesidad de intercambio flexible y rápido de información.
- Muchas organizaciones tienen varias sucursales en diferentes ubicaciones así como también tele trabajadores remotos desde sus casas, quienes necesitan intercambiar información sin ninguna demora, como si estuvieran físicamente juntos.
- La necesidad de las redes de computación de cumplir altos estándares de seguridad que aseguren la autenticidad, integridad y disponibilidad.

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.

2.3.1.4.2 Seguridad OpenVPN.

OpenVPN tiene dos modos considerados seguros, uno basado en claves estáticas pre-compartidas y otro en SSL/TLS (Secure Sockets Layer/Transport Layer Security) usando certificados y claves RSA (Rivest Shamir Adelman).

Cuando ambos lados usan la misma clave para cifrar y descifrar 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.

Veremos a continuación ese método y otros que aportan mayor seguridad y facilidad de distribución.

Cifrado simétrico y claves pre-compartidas

Cualquiera que posea la clave podrá descifrar 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.

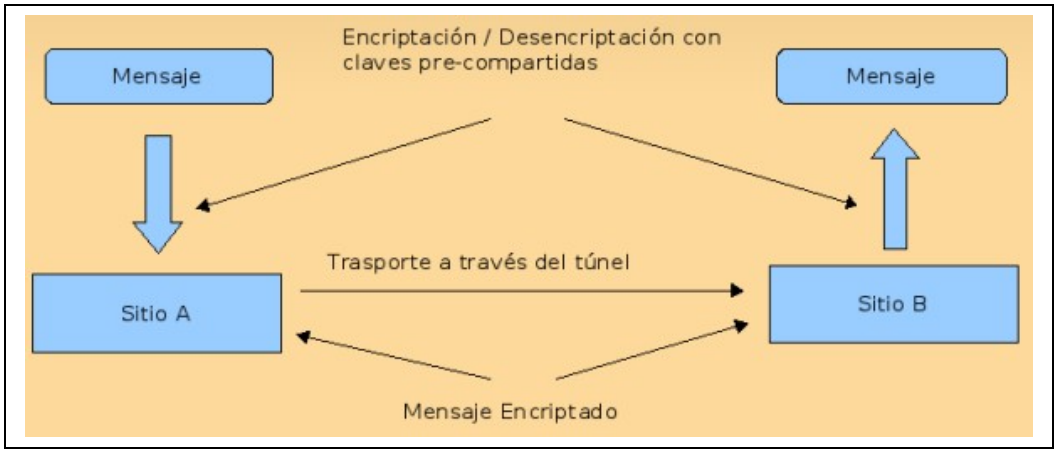


Fig. 2.2 Esquema de cifrado simétrico y claves pre-compartidas.

Es por ello que mecanismos como IPsec cambian las claves cada cierto período de tiempo, asociando a las mismas ciertos períodos de tiempo de validez, llamados “tiempo de vida” o “lifetime”. Una buena combinación de tiempo de vida y largo de la clave asegurarán que un atacante no pueda descifrar 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.

Cifrado asimétrico con SSL/TLS

SSL/TLS usa una de las mejores tecnologías de cifrado 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 cifrar los datos que serán enviados a la contraparte quien conoce la clave privada que es la única que sirve para descifrar los datos. El par de clave pública/privada es generado a partir de algoritmos matemáticos que aseguran que solo con la clave privada es posible leer los datos originales. El día que alguien encuentre algún defecto a ese algoritmo, todos aquellos conectados a Internet estarán comprometidos en forma instantánea.

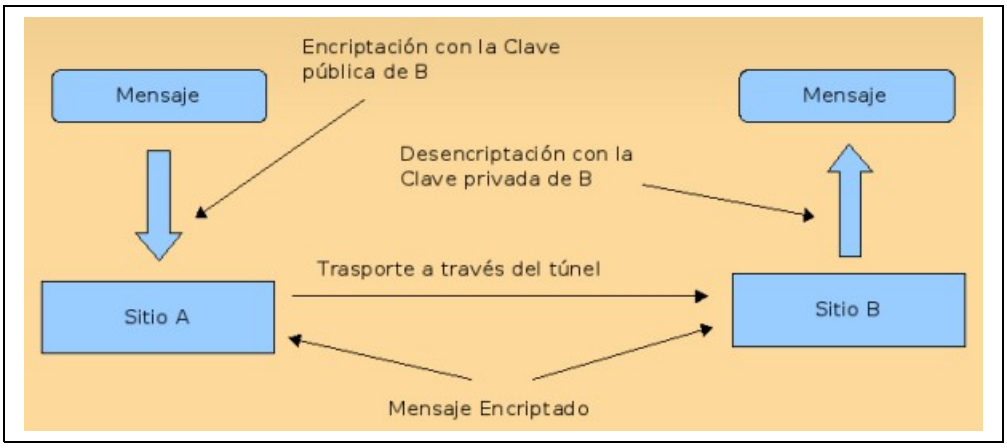


Fig. 2.3 Esquema de cifrado asimétrico con SSL/TLS.

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 sofware OpenSSL que vienen instaladas en cualquier sistema moderno e implementan mecanismos de cifrado 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 demostrar su identidad a todos aquellos que confíen en la autoridad certificadora que lo emitió.

2.3.1.4.3 Ventajas y Desventajas de OpenVPN.

Ventajas

- 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 (Intercambio de paquetes inter-red) o broadcast (NETBIOS).

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

- Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.
- Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).
- Solo un puerto en el firewall debe ser abierto para permitir conexiones, dado que 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 NAT 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 IP´s 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 IP´s 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 tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.
- Falta de masa crítica.
- Todavía existe poca gente que conoce como usar OpenVPN.

Al día de hoy sólo se puede conectar a otras computadoras. Pero esto está cambiando, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.

2.3.1.5 SSL (Security Socket Layer).

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente (phishing) y alterar la integridad del mensaje.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- Con funciones hash: MD5 o de la familia SHA.

Historia y Desarrollo.

Desarrollado por Netscape, SSL versión 3.0 se publicó en 1996, que más tarde sirvió como base para desarrollar TLS versión 1.0, un estándar protocolo IETF definido por primera vez en el RFC 2246. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.

SSL opera de una manera modular: sus autores lo diseñaron extensible, con soporte para compatibilidad hacia delante y hacia atrás, y negociación entre las partes (peer-to-peer).

Algunas primeras implementaciones de SSL podían usar claves simétricas con un máximo de sólo 40-bit debido a las restricciones del gobierno de los Estados Unidos sobre la exportación de tecnología criptográfica. Dicho gobierno impuso una clave de 40-bit lo suficientemente pequeña para ser “rota” por un ataque de fuerza bruta por las agencias de seguridad nacional que desearan leer el tráfico cifrado, a la vez que representaban un obstáculo para atacantes con menos medios. Una limitación similar se aplicó a Lotus Notes en versiones para la exportación. Después de varios años de controversia pública, una serie de pleitos, y el reconocimiento del gobierno de Estados Unidos de cambios en la disponibilidad en el mercado de 'mejores' productos criptográficos producidos fuera del país, las autoridades relajaron algunos aspectos de las restricciones de exportación. La limitación de claves de 40-bit en su mayoría ha desaparecido. Las implementaciones modernas usan claves de 128-bit (o más) para claves de cifrado simétricas.

Como funciona.

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autentificación del mensaje (MAC). Cada registro tiene un campo de content_type que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo handshake, que tiene el content_type 22.

El cliente envía y recibe varias estructuras handshake:

- Envía un mensaje ClientHello especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde

(llamados Challenge de Cliente o Reto). Además puede incluir el identificador de la sesión.

- Después, recibe un registro ServerHello, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.

- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.
- El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autentificada.
- Cliente y servidor negocian una clave secreta (simétrica) común llamada master secret, posiblemente usando el resultado de un intercambio Diffie-Hellman, o simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este master secret (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una función pseudoaleatoria cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).
- Protección contra varios ataques conocidos (incluyendo ataques man-in-the-middle), como los que implican un degradado del protocolo a

versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.

- El mensaje que finaliza el protocolo handshake (Finished) envía un hash de todos los datos intercambiados y vistos por ambas partes.
- La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

Aplicaciones.

SSL se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP (Protocolo Simple de Transferencia de Correo), NNTP (Network News Transport Protocol) y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS (Protocolo Seguro de Transferencia de Hipertexto). HTTPS es usado para asegurar páginas World Wide Web para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos.

Aunque un número creciente de productos clientes y servidores pueden proporcionar SSL de forma nativa, muchos aún no lo permiten. En estos casos, un usuario podría querer usar una aplicación SSL independiente como Stunnel para proporcionar cifrado. No obstante, el Internet Engineering Task Force recomendó en 1997 que los protocolos de aplicación ofrecieran una forma de actualizar a TLS a partir de una conexión sin cifrado (plaintext), en vez de usar un puerto diferente para cifrar las comunicaciones – esto evitaría el uso de envolturas (wrappers) como Stunnel.

SSL también puede ser usado para tunelizar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

2.3.1.6 Monitores de Ancho de Banda.

Una red en la que transmite o recibe los datos que se denomina ancho de banda de red. Ancho de banda y la latencia son dos parámetros importantes para medir la velocidad de las redes. Cuanto mayor sea el ancho de banda, mayor será el coste de la red. Por lo tanto, el desperdicio de ancho de banda es un criterio clave de medición para la optimización de cualquier red.

Un ancho de banda de red ayuda a controlar el seguimiento de la utilización de ancho de banda. Ancho de banda de red se ejecutan en monitores de computadoras para las 24 horas del día y realizar un seguimiento continuo de los parámetros de uso de la red. Este seguimiento de la información se almacena en una base de datos interna para futuros análisis. Monitores de red de ancho de banda lo que puede rastrear los servidores de aplicaciones y está utilizando el ancho de banda de red. Que ayudan a recibir el ancho de banda y uso de la red de datos que optimiza la eficiencia de la red. Ancho de banda de red de vigilancia es una actividad muy crítica de una empresa el administrador de la red. Con ancho de banda de red de vigilancia, un administrador de red es instantáneo informes sobre el uso del ancho de banda de cada aplicación y de acogida. Este informe ayuda a tomar decisiones sobre el acceso o la planificación de la capacidad de planificación. Ancho de banda de red controlar el software puede visualizar el estado de la red, y se da automáticamente las alertas de los problemas en el ancho de banda. El análisis de los datos ayuda a la planificación futura. El monitor puede ser configurado para enviar mensajes de correo electrónico.

La mayoría de los monitores de red de banda ancha con cualquier función SNMP (Simple Network Management Protocol), tales como puertas de enlace, los

routers, NAS (Network Attached Storage), impresoras, servidores y mucho más. Toda la información recogida por software Monitor de red de ancho de banda se pueden ver, imprimir y guardar para su posterior análisis y planificación de ancho de banda. Ancho de banda de red controlar el software también supervisa el tráfico entre el computador y de Internet. Red de monitoreo de ancho de banda es muy beneficioso para los que acceder a Internet en una transferencia (mensual) base. Un ancho de banda de red controlar, con un solo clic, identifica superior aplicaciones, protocolos de arriba, arriba y más seguimiento. Un ancho de banda de red puede controlar configurar un perfil exacto de vigilancia, el seguimiento de los límites de ancho de banda que son fijados por un proveedor de servicios Internet (ISP).

Uso de ancho de banda es muy variable de tiempo en tiempo, y es muy difícil de medir con precisión. Ancho de banda de red monitores son herramientas que permiten la medición precisa de ancho de banda de red y sus patrones de uso.

2.3.1.7 Conexiones a Internet.

Junto con la conexión por módem telefónico básica existen varias posibilidades más para conectarse a Internet. Algunas están ya en marcha, otras se están empezando a comercializar y otras son parte de un futuro prometedor.

Cuanto más ancho de banda ofrece un tipo de conexión más cara suele resultar, pero ante el empuje de las nuevas tecnologías cada vez se están reduciendo los precios y esperemos que pronto podamos disponer de un ancho de banda aceptable a buen precio. Así podremos hablar de una vez de las autopistas de la información como algo accesible para la mayoría.

Vamos a explicar cada tipo de conexión partiendo de esta clasificación según el medio que utilizan.

a) Línea telefónica.

1) Línea convencional.

RTB red telefónica básica.

2) Línea digital.

RDSI

ADSL

b) Cable.

c) Telefonía móvil.

1) GPS

2) GPRS

3) UMTS

d) Satélite.

e) Red eléctrica.

f) Redes inalámbricas.

A continuación vamos a describir cada uno de estos tipos.

Red telefónica básica (RTB).

Es un sistema bastante utilizado, principalmente porque es el más barato y porque casi todos los lugares disponen de la línea telefónica básica. Es un sistema lento y no permite utilizar el teléfono mientras se está conectado a Internet, ya que es el módem el que está ocupando la línea telefónica llamando al servidor de Internet.

Los módems actuales tienen una velocidad de transferencia máxima de 56 Kbps, aunque debido a la saturación de la línea telefónica o a la capacidad limitada del proveedor del servicio casi nunca se alcanza esa velocidad.

Una de las ventajas de este tipo de conexión es que, prácticamente, las líneas telefónicas llegan a casi todas partes. Además al utilizar una infraestructura que ya existía, antes de ser usada para la conexión a Internet, es más barata que otros nuevos sistemas de conexión que tienen que crear toda su infraestructura partiendo de cero.

En el punto "Configurar el módem y la conexión" te damos más información sobre cómo instalar una conexión de este tipo.

RDSI (Red Digital de Servicios Integrados).

Este tipo de conexión también utiliza la línea telefónica pero mientras en el caso anterior la línea es analógica, en este caso la línea es digital, lo que se traduce en una transmisión más rápida, segura y eficaz. Por otra parte sólo es posible utilizar esta tecnología si el lugar donde se encuentra la conexión dispone de una línea RDSI, ya que este tipo de líneas no están tan extendidas como las líneas básicas.

Una línea RDSI dispone de dos canales de 64 Kbps, con lo cual se puede utilizar un canal para hablar por teléfono y el otro canal para Internet. Utilizando los dos canales para Internet se consiguen velocidades de hasta 128 Kbps. Además estas velocidades teóricas, al contrario que sucede con los módem telefónicos, si se suelen alcanzar de forma constante.

Este tipo de conexión cada vez se utiliza menos debido al auge del ADSL.

ADSL (Asimetric Digital Suscriber Line).

Este tipo de conexión utiliza la línea telefónica básica pero permite que los datos se transmitan de forma asimétrica con lo cual se aprovecha mejor el ancho de banda disponible.

Cuando estamos conectados a Internet el flujo de datos es asimétrico, la mayor parte de los datos viajan en sentido Internet a usuario, mientras que unos pocos datos viajan en sentido usuario a Internet. Es decir, cuando hacemos una petición para ver una página enviamos pocos datos, la dirección de la página y poco más, mientras que al recibir esa página recibimos muchos datos, imágenes, texto, etc.

Mediante ADSL se logra aprovechar esta asimetría estableciendo tres canales en la línea telefónica, dos para datos (uno para el sentido Internet-usuario y otro de usuario-Internet) y otro canal para la voz. El canal en sentido Internet usuario tiene más capacidad que el de usuario Internet.

Una ventaja de esta tecnología es que la conexión es permanente, 24 h. al día, y no necesitamos marcar cada vez el número de teléfono para conectarnos. Además podemos hablar por teléfono a la vez que navegamos por Internet.

Con este tipo de conexión se consiguen velocidades desde 256 Kbps hasta 20 Mbps en sentido Internet-usuario, según la modalidad que se contrate.

Para poder contratar este servicio la centralita de la que depende nuestro teléfono debe estar adaptada a esta tecnología, además tu teléfono debe estar a menos de 3 Km. de ella. Si cumples estas condiciones sólo será necesario instalar un módem específico para ADSL conectado a la línea telefónica.

Conexión por cable.

Mientras que las tecnologías vistas hasta aquí utilizan el cable del teléfono tradicional, esta utiliza un cable de fibra óptica que tiene que ser instalado de nuevo, salvo que ya estuviese instalado para ver la televisión por cable. La compañía suministradora instala el cable hasta el interior del domicilio y este se conecta a una tarjeta de red ethernet que hay que instalar en el computador.

Igual que sucede con ADSL, al encender el computador ya estamos conectados, directamente podemos hacer clic en el navegador para entrar en Internet, sin tener que esperar a que se efectúe la llamada telefónica, como sucede con el módem de RTB.

Conexión a través de teléfonos móviles.

Al hablar de Internet a través del teléfono móvil hay que distinguir entre tres formatos distintos Web, Wap y i-mode.

El formato Web es el que conocemos a través del computador personal y que está escrito en HTML.

El formato Wap está pensado para las pequeñas pantallas de los teléfonos móviles y está escrito en WML, que sólo permite texto y gráficos simples. Este formato puede ser útil para recibir un tipo de información concreta: corta y de texto. Como, por ejemplo, las cotizaciones de bolsa, horarios de transportes públicos, resultados deportivos, etc. Hasta el momento este formato no ha tenido el éxito que se esperaba.

Ambos formatos son incompatibles entre sí, en un móvil no podemos ver el formato Web y en una conexión común a Internet no podemos ver el formato Wap. Además la información a la que se puede acceder es distinta, con Wap sólo podemos acceder a los portales diseñados específicamente para Wap.

Sin embargo, sí podemos utilizar el teléfono móvil para conectar un computador portátil a la Web. En este caso el teléfono móvil hace las funciones de módem.

La tecnología i-mode viene desde Japón donde ha tenido un gran éxito y se esta extendiendo por Europa.

Los distintos fabricantes de teléfonos móviles están incorporando diversos sistemas de navegación web en sus móviles, por ejemplo Sony-Ericsson ofrece Internet Access NetFront en su modelo T650i.

Una vez aclarado estos conceptos vamos a ver los diferentes tipos de sistemas de móviles, actuales y futuros. Con cualquiera de estos sistemas podemos acceder a Wap y conectar un portátil a la Web. También se puede conectar el portátil a través de una tarjeta-módem tipo PCMCIA o de un modem USB sin necesidad de utilizar un teléfono móvil. Si quieres más información sobre Wap y cómo utilizar un simulador de Wap para Windows.

También se puede acceder a Internet utilizando dispositivos portátiles del tipo Pocket Pc o PDA (Personal Digital Assistant). Estos aparatos tienen un tamaño intermedio entre un teléfono móvil y un computador portátil. Se pueden llevar en el bolsillo y tienen un pantalla mucho más grande que un teléfono móvil, en la que se puede escribir o señalar con un pequeño lápiz.

Estos dispositivos tienen algunas limitaciones en cuanto al tipo de páginas que pueden visualizar, por ejemplo no permiten páginas con Flash y aplicaciones Java. Para conectarse a Internet pueden utilizar un teléfono móvil o una tarjeta compacta que actúa como módem para conectar a una línea telefónica o a una red local.

Teléfonos móviles GSM.

El sistema GSM (Global System Mobile) fue el primer sistema que consiguió establecer un estándar común en las comunicaciones móviles. Antes había varios sistemas incompatibles entre sí como el NMT y el TACS (El sistema que utilizaba Moviline de Telefónica es TACS). Con GSM hubo un acuerdo en que el ancho de banda que se debía utilizar era de 900 Mhz, luego se amplió a 1800 Mhz. Esto ocurría en 1982 y hasta 1992 no se entró en la fase comercial.

El GSM permitió, por fin, la comunicación entre móviles de distintos países con un sistema común. El GSM se le conoce como segunda generación en sistemas de telefonía para móviles. Con GSM la velocidad de transmisión alcanza los 9,6 Kbps.

Actualmente se puede conectar a Internet un computador a través de los teléfonos móviles con sistema GSM pero hay que pagar los minutos a precio de llamada desde móvil y puede resultar un poco lento. Aunque puede ser útil para conectar los computadores portátiles durante los viajes, sobre todo para gestionar el correo y hacer consultas puntuales, como las cotizaciones de bolsa o un horario de trenes. Se puede utilizar un teléfono que lleve el módem integrado, o instalar un software que realiza la función de módem en el portátil, mediante un cable se conecta el móvil al portátil.

También se puede acceder a Internet en formato Wap desde el propio teléfono móvil en los terminales que lo soportan.

Teléfonos móviles GPRS.

El sistema GPRS (General Packet Radio Service) permite una velocidad máxima de 144 Kbps, aunque la velocidad real a la que empezará a funcionar será entre 18 y 53 Kbps.

Se conoce como la segunda generación y media en sistemas móviles. Esta tecnología es una evolución del sistema GSM al que se le han añadido mejoras en la transmisión de datos. El sistema GPRS utiliza básicamente la misma red que el sistema GSM, lo cual permitirá reducir los costes de implantación.

El sistema GSM utiliza una conexión por circuito, es decir, se ocupa una línea durante el tiempo que está abierta la conexión, al acabar, la línea se libera para que la pueda utilizar otra llamada. Por esto se cobra por tiempo de conexión. Sin embargo el sistema GPRS establece una conexión por paquetes, es decir, los datos a enviar se trocean en paquetes y estos se envían de forma independiente, al llegar al destino son ordenados. Así los paquetes de varias conexiones pueden viajar por la misma línea.

Esto conlleva una mejor utilización de las líneas que en la conexión por circuito, en la que durante los instantes que ninguno de los comunicantes está enviando información la línea sigue ocupada. También implica que la conexión se estable al encender el terminal y finaliza al apagar el terminal. El GPRS permite el cobro por cantidad de datos transmitidos, en lugar de por tiempo de conexión. GPRS es compatible con GSM, podemos seguir utilizando SMS, Wap, buzón de voz, etc.

Teléfonos móviles UMTS, HSDPA.

UMTS (Universal Mobile Telecommunications System) se la conoce como la tercera generación en tecnología para móviles y va a suponer un salto importante respecto del GPRS.

Así como la tecnología GPRS era una evolución de la GSM, la tecnología UMTS es nueva y emplea lenguajes y protocolos nuevos. En sus primeras versiones permitirá velocidades de alrededor de 380 Kbps para datos y posteriormente podrá llegar hasta velocidades de 2 Mbps.

El ancho de banda del UMTS permite aplicaciones que hasta ahora nos parecían imposibles en un móvil, como por ejemplo, la vídeoconferencia.

UMTS permite el cobro por cantidad de datos transmitidos, probablemente se establezcan diferentes tipos de tarifas con diferentes velocidades de transmisión.

El despliegue de la tecnología UMTS supone un cambio importante en todas las infraestructuras de telefonía móvil, ya que implica la implantación de Redes totalmente nuevas tanto para el Acceso como para la Conmutación.

El UMTS puede competir en velocidad, aunque no en precio, con el acceso a Internet de banda ancha con los sistemas que existen actualmente en conexiones fijas, como el cable y el ADSL.

Mediante tajetas UMTS (3G) conectadas a computadores portátiles ya es posible conectarse sin cable a Internet con la alta velocidad que proporciona UMTS.

La mayor capacidad en la transmisión de datos del UMTS hará que se incrementen y mejoren los servicios que se pueden prestar, tanto a través de un portátil como a través de teléfonos móviles, ya que la resolución de las pantallas de los teléfonos móviles va a ir aumentando.

La evolución del UMTS ya está en marcha y se llama HSDPA (High Speed Downlink Packet Access) aunque también se la conoce como tecnología 3,5 G. Promete una velocidad de 14 Mbps y ya está siendo ofrecida por diversos operadores en las áreas más pobladas.

La tecnología HSDPA+ es una mejora que permite llegar hasta los 80 Mbps y está empezando a desplegarse. Para los próximos años se promete que la cuarta generación LTE llegará hasta los 140 Mbps.

Red eléctrica.

Ya se puede aprovechar las líneas eléctricas para transmitir datos a alta velocidad.

El sistema para transmitir señales telefónicas por la red eléctrica (PCL Line Communication) no es nuevo, ya se utiliza desde hace años para conectar centrales hidroeléctricas aisladas a las que no llega el teléfono. Pero hasta hace poco había problemas de interferencias entre los cables eléctricos y electrodomésticos y otros aparatos eléctricos.

Conexión vía Satélite.

En la conexión de Internet por satélite hay que distinguir entre la señal que llega al usuario de Internet y la señal que envía el usuario a Internet.

En las conexiones unidireccionales la señal de Internet al usuario se recibe a través del satélite mediante una antena parabólica y un módem específico, mientras que la señal desde el usuario a Internet se envía por un medio clásico, línea telefónica, ADSL, RDSI, etc.

También existe la posibilidad de conexiones bidireccionales, en las que la señal usuario a Internet también va por el satélite, aunque son bastante más caras que las unidireccionales.

La velocidad de recepción a través de la antena parabólica puede ser muy alta, teóricamente hasta 38 Mbps. Para este tipo de conexión es conveniente un computador de gama media-alta, lo que junto con el precio del módem y la antena parabólica suma una cantidad elevada para el usuario doméstico. Más información en Satconxion.

Otra posibilidad de conexión a Internet utilizando el satélite es a través del teléfono móvil conectado a un computador portátil. Los datos son enviados al satélite por el teléfono móvil. Este sistema permite la conexión desde prácticamente cualquier lugar del mundo, a una velocidad de hasta 10 Kbps.

También podemos conectarnos a través del satélite mediante los servicios que proporcionan las plataformas de televisión digital. En este caso recibimos los datos de Internet a usuario por la misma antena parabólica que utilizamos para recibir la señal de televisión. Las páginas las vemos en la pantalla de la televisión. Para enviar los datos desde el usuario a Internet debemos utilizar la

línea telefónica. El proveedor nos proporcionará un teclado inalámbrico para que escribamos la información que queremos enviar. Hay que tener en cuenta que la resolución de una televisión es más baja que la de un monitor de computador, por lo tanto las imágenes las veremos peor que en nuestro computador.

Redes inalámbricas. WIFI.

Las Redes inalámbricas se están extendiendo muchísimo estos últimos días. Unas red inalámbrica utiliza la tecnología WIFI (Wireless Fidelity), también llamada WLAN (wireless lan, red inalámbrica) o estándar IEEE 802.11. Su velocidad y alcance, unos 100-300 metros utilizando hardware asequible, lo convierten en una fórmula perfecta para el acceso a Internet sin cables.

Para poder conectarnos a una red WIFI necesitamos un dispositivo WIFI instalado en nuestro computador, de esta forma estaremos preparados para recibir la señal. Una vez encontremos un punto de acceso, es decir, un dispositivo que emita y reciba señales de Internet, si no está protegida, podremos conectarnos con un par de clics.

Una de las características más importantes de este tipo de conexión es que puede emitirse junto a un protocolo de seguridad que obliga al usuario de la red a introducir una contraseña para poder utilizar la conexión. Este método se usa bastante en las redes inalámbricas montadas en los hogares. Pero existe toda una iniciativa mundial para liberalizar estas redes y poder tener acceso a Internet en cualquier sitio donde nos encontremos.

Existe un estándar similar que aun tiene que abrirse paso en el mercado, WIMAX. Este método de transmisión promete alcances de hasta 50 kilómetros, velocidades superiores a 70 Mbps y es capaz de dar conexión a más de 100

usuarios de forma simultánea. Esto, claro, teóricamente. Si esta tecnología funciona correctamente será un gran avance para abaratar los costes de conexión en áreas muy amplias, pues una sola antena podría abastecer a más familias que kilómetros de cable.

2.3.1.8 Herramientas de Desarrollo.

2.3.1.8.1 SmoothWall Express 3.0

SmoothWall Express es un firewall de código fuente abierto basado en el GNU / Linux. Diseñado para usarlo fácilmente, SmoothWall Express está configurado a través de una GUI basada en Web y de requiere absolutamente ningún conocimiento de Linux para instalar o utilizar.

SmoothWall Express le permite construir fácilmente un firewall para conectarse de forma segura una red de computadoras a través de Internet.

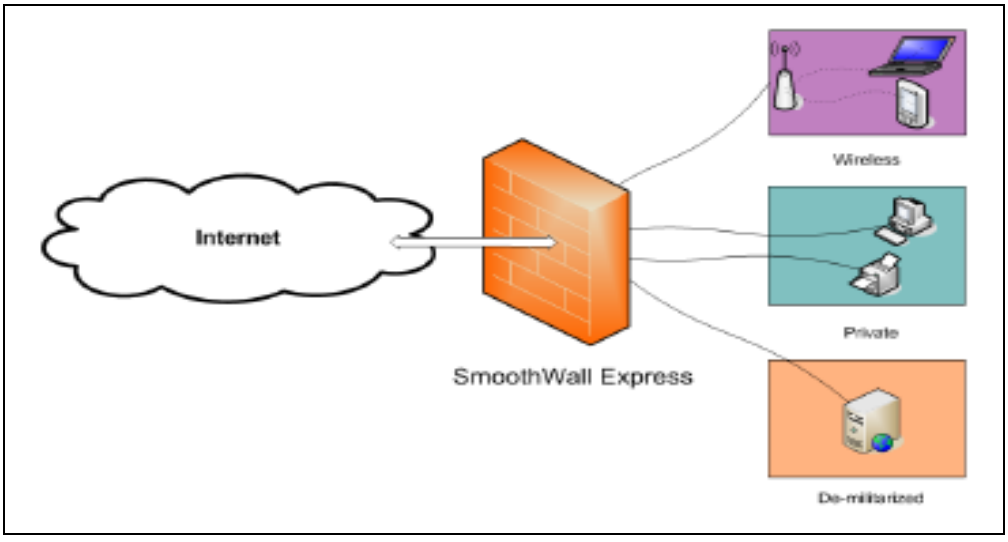


Fig. 2.4 Firewall SmoothWall Express

Casi cualquier PC clase Pentium se puede utilizar, por ejemplo, un viejo computador de especificaciones bajas, puede trabajar como una estación de trabajo o servidor. SmoothWall Express crea un firewall de seguridad dedicado,

ofreciendo las instalaciones y las seguridades, asociados con los dispositivos de hardware.

SmoothWall Express viene pre-configurado para detener todo el tráfico entrante que no es el resultado de una solicitud de salida. Los archivos de normas que implementan esta política son parte del sistema de configuración y normalmente no deberían ser editados por otro procedimiento de configuración.

2.3.1.8.2 CommView 6.0

CommView es un programa que permite monitorear la actividad de Internet y redes de área local (Local Area Network) siendo capaz de capturar y analizar paquetes de red. El mismo recoge información acerca del tráfico de datos a través de su conexión telefónica o su tarjeta Ethernet y decodifica los datos analizados.

Con CommView puede ver la lista de conexiones de red y estadísticas vitales de IP y examinar paquetes individuales. Los paquetes son decodificados hasta el nivel más bajo con un análisis profundo de los protocolos más difundidos. También provee un completo acceso a datos sin depurar. Los paquetes capturados pueden ser guardados en archivos de registro para análisis futuros. Un sistema flexible de filtros hace posible eliminar paquetes que no necesita, o capturar solo aquellos paquetes que desea. Alarmas configurables pueden notificar eventos importantes, tales como paquetes sospechosos, utilización excesiva del ancho de banda, o direcciones desconocidas.

CommView es una herramienta valiosa para administradores de LAN, profesionales de seguridad, programadores de redes, o cualquiera que quiera tener una visión completa del tráfico que pasa a través de una PC o segmento de LAN.

2.3.2 Fundamentación de la Empresa.

La Constructora López Cía. Ltda. es una empresa que brinda servicios en el área de la construcción, que cuenta con recursos humanos, materiales y tecnología de punta, satisfaciendo las necesidades del cliente.
Como empresa de servicios integrales ha creado renovadoras técnicas para ofreces a sus clientes un servicio de alta calidad.

Objetivo General.

Construir obras integrales de calidad con tecnología de punta, servicios personalizados y con profesionales calificados.

Objetivos Específicos.

- Mejorar las condiciones de vida de los habitantes, mediante la construcción y prestación de servicios.

- Investigar las características y mejor uso de los materiales de construcción y los métodos de aprovechamiento de estos.

- Definir las estrategias informáticas para el desarrollo de proyectos, en base a los resultados de la evaluación de la situación actual.

- Estudiar y desarrollar constantemente nuevas soluciones para adaptarse a las cambiantes necesidades del mercado.

La empresa está constituida por:

- Ing. Carlos E. López – Gerente
- Ing. Carlos A. López – Presidente
- Ing. Nancy Sánchez – Gerente Administrativa
- Dra. Silvia Arboleda – Contadora

- Dra. Giselle Proaño – Asesora Jurídica
- Ing. Guille Proaño – Dpto. Técnico

2.4 Hipótesis.

Una VPN optimizará la comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda., haciéndola eficiente, rápida y segura.

2.5 Variables.

2.5.1 Variable Independiente.

“Diseño de una VPN”.

2.5.2 Variable Dependiente.

“Comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda.**”.**

CAPÍTULO III
METODOLOGIA

3.1 Enfoque.

El presente trabajo se enmarca en un enfoque cualitativo, porque a través de encuestas se podrá conocer el problema de la empresa; fundamentado en la aceptación o rechazo de la misma.

3.2 Modalidad básica de la Investigación.

3.2.1 Investigación de Campo.

En la investigación utilizaré la observación de campo, análisis de los proceso de comunicación de la Constructora, con el que desarrollaré un estudio sistemático para diagnosticar el problema de la Constructora López Cía. Ltda., tomando datos confiables al ponerme en contacto directo con la realidad de la Constructora.

3.2.2 Investigación Documental.

Para complementar y profundizar la idea sobre el problema, se consultará y analizará en libros e Internet; así como también en trabajos elaborados anteriormente sobre VPN´s. El uso de la investigación bibliográfica es importante para el desarrollo del proyecto.

3.2.3 Proyecto Factible.

Dentro de este estudio se experimentará el control y funcionamiento de la comunicación en la Constructora. El proyecto se enmarca dentro de la factibilidad, debido a que me permitirá resolver un problema sustentado en una base teórica, obtenida después de la evaluación a la información.

3.3 Nivel o tipo de Investigación.

El nivel exploratorio me permitirá conocer y contextualizar el problema, el nivel descriptivo facilita la identificación de las variables, el análisis crítico de la situación; el nivel correlacional ayuda a establecer relaciones entre causas y efectos del problema, así como también entre la variable independiente y dependiente. Finalmente se pretende llegar al nivel explicativo con la comprobación de la hipótesis.

3.4 Población y Muestra.

3.4.1 Población.

La población que va a intervenir en el desarrollo de esta investigación son dos personas, el Ing. Carlos Enrique López y el Ing. Carlos Alberto López, que nos permitan comprobar el correcto funcionamiento de esta.

3.4.2 Muestra

Como la población es reducida pasa a formar parte de la .muestra.

3.5 Recolección de Información.

3.5.1 Plan de Recolección de Información.

Para la recolección de información de los procesos de comunicación que se realiza en la empresa, la mejor opción es realizar la observación de campo que permitirá obtener la mayor información posible relacionada directamente con el tema del proyecto.

3.5.2 Plan de Procesamiento de Información.

Luego de haber realizado la observación de campo se procederá a realizar el siguiente proceso:

- Análisis crítico de la información.
- Organizar la información.
- Documentar la información.

3.6 Procesamiento y Análisis.

Una vez obtenidos los resultados de la observación de campo se puede llegar a comprobar la hipótesis planteada y además permite establecer conclusiones y recomendaciones que me ayudarán de mejor manera a la implementación de una VPN para facilitar la comunicación entre las oficinas centrales y las bodegas de la Constructora López Cía. Ltda.

CAPÍTULO IV
ANALISIS E INTERPRETACION DE RESULTADOS.

4.1 Información del proceso.

La comunicación entre las oficinas centrales y la bodega de la Constructora se lo hace vía telefónica o celular, por ejemplo para el proceso de Entrega/Recepción de equipos y maquinaria, un obrero pide cierta maquinaria al bodeguero; este envía una hoja de control y autorización a la oficina central para ser verificada y firmada. Una vez firmada la hoja de control retorna al bodeguero y este expide una orden de salida de la maquinaria. Para poder saber los materiales que existen en la bodega, se debe llamar al bodeguero responsable vía telefónica si existe el material necesario.

4.2 Análisis del Problema.

Durante la investigación de campo se determinó que la comunicación entre las oficinas centrales y la bodega es inadecuada y muy costosa, ya que a cada instante que es necesario saber la ubicación y existencia de los materiales y la maquinaria se debe contactar con el bodeguero responsable para que envíe un listado a las oficinas centrales, proceso que es muy demorado.

4.3 Interpretación de Resultados.

Después del análisis previo, se da como alternativa de solución; el estudio de factibilidad para la implementación de una VPN sobre la distribución SmoothWall Express 3.0, ya que por ser software libre, no tiene costo.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones.

- Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos.

- Las VPN prácticamente se ha vuelto un tema importante en las empresas, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

- El único inconveniente que pudieran tener las VPN es el establecimiento correcto de las políticas de seguridad y de acceso a la información.

- Las redes VPN disminuyen significativamente costos adicionales por comunicación y/o compartición de recursos entre dependencias de una misma empresa que se encuentran geográficamente distantes.

- La VPN permite el acceso remoto para facilitar la comunicación entre un empleado fuera de la empresa y los servicios de la red LAN interna.

- Con las VPN´s, una organización sólo necesita una conexión relativamente pequeña con el proveedor del servicio (ISP).

- La interconexión de redes constituye una tendencia fuerte en el manejo de transporte de información. Debido a que los requerimientos de los usuarios son más complejos día a día y varían rápidamente, las soluciones de interconexión deben ser cada día más cómodas y fáciles de implementar. Las redes privadas virtuales ofrecen una nueva alternativa en este aspecto, debido a su flexibilidad y a la filosofía con las que han sido creadas: VPN aprovecha diferentes tecnologías de manera transparente al usuario con el fin de ofrecer servicios en un ambiente constituido por seguridad, disponibilidad, escalabilidad y compatibilidad.

5.2 Recomendaciones.

- Se recomienda brindar servicios adicionales aprovechando el túnel establecido, como por ejemplo: servicio de escritorio remoto, video conferencia, compartición de recursos como documentos e impresoras, etc.

- Se recomienda que las contraseñas tengan un periodo corto de duración, de esta manera se evita que algún usuario no autorizado acceda al túnel.

- Se debe tener un monitoreo de la red, de tal manera que se conozca el ancho de banda que se requiere para la transmisión de información a través del túnel.

- Es recomendable una VPN cuando se tienen trabajadores que viajen constantemente, abaratando notablemente el costo de la conexión permitiendo una comunicación continua con la empresa.

- Implementar una solución VPN basada en software libre para reducir notablemente los costos.

CAPITULO VI
PROPUESTA

6.1 Análisis de Requerimientos.

Constructora López Cía. Ltda. es una empresa que brinda servicios en el área de la construcción, que cuenta con recursos humanos, materiales y tecnología de punta, satisfaciendo las necesidades del cliente.

El proceso de Entrega/Recepción de equipos y maquinaria se lo realiza de forma manual, es decir, un obrero pide cierta maquinaria al bodeguero; este envía una hoja de control y autorización a la oficina central para ser verificada y firmada. Una vez firmada la hoja de control retorna al bodeguero y este expide una orden de salida de la maquinaria.

Si se requiere conocer los materiales que existen por bodega, se debe llamar a los bodegueros responsables para saber si existe el material necesario, este proceso consume mucho tiempo, retrasando la ejecución del los proyectos.

El objetivo del proyecto es desarrollar una VPN que permita establecer la comunicación a través de un entorno computacional entre las oficinas centrales y las bodegas, mediante la implementación de las seguridades necesarias a la VPN y sobre todo a la base de datos y demás componentes internos de la empresa.

6.2 Diseño de la VPN

6.2.1 Especificaciones de Hardware y de Sistema.

Sistema/Hardware	**Requerimiento/recomendaciones**
Procesador	Intel Pentium 200 o procesadores compatibles.
Memoria	128 megabytes de RAM. Más memoria es requerida para servicios adicionales.
Almacenamiento	2 gigabytes de disco duro. Soporta dispositivos IDE y SCSI.
Interfaz de Red	Un mínimo de una tarjeta de red (NIC). Si la conexión a Internet es a través de un dispositivo de banda ancha como un cable módem, ADSL, se necesita una segunda NIC.
Teclado	Si el BIOS del sistema soporta de arranque sin teclado, esto es sólo necesario para la instalación inicial.
Tarjeta de Video	Solo se requiere cuando se instala SmoothWall Express.
Monitor	Solo se requiere cuando se instala SmoothWall Express.
CD-ROM	Solo se requiere cuando se instala SmoothWall Express.
Floppy	Recomendado para actualizar desde versiones anteriores.

Tipo de conexión a Internet	Internet	Una NIC adecuada es requerida.
	ADSL	Una tarjeta PCI compatible o un módem USB es requerido.
	ISDN	Una tarjeta RDSI o el apoyo externo del puerto RS232 o USB adaptador conectado es necesario.
	Modem	Un módem RS232, módem ISA o PCI es requerido.

Tabla 6.1 Requerimientos de Hardware y de Sistema.

6.2.2 Instalando SmoothWall Express.

La instalación de SmoothWall Express está diseñada para ejecutarse en una estación de trabajo con un CD-ROM.

1 Vaya a http://www.smoothwall.org/, descargue y grabe un CD de SmoothWall Express.

2 Inserte el CD en la unidad de CD de la estación de trabajo que desea utilizar como un dispositivo de firewall y reinicie el sistema. Aparecerá la siguiente pantalla:

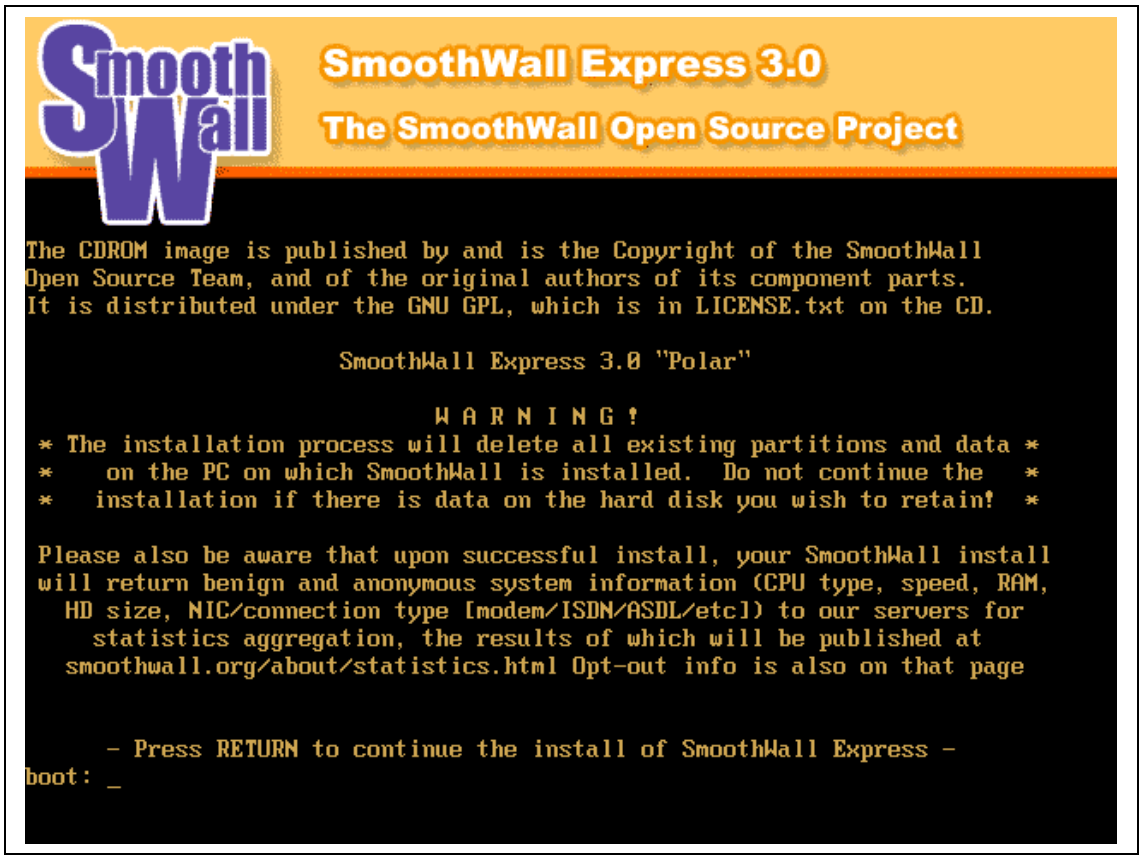


Fig. 6.1 Instalación de SmoothWall Express 3.0

3 Después de leer la información, pulse ENTER. El siguiente cuadro de diálogo se abre:

Fig. 6.2 Bienvenida a la instalación.

4 Pulse ENTER para continuar el siguiente cuadro de diálogo se abre:

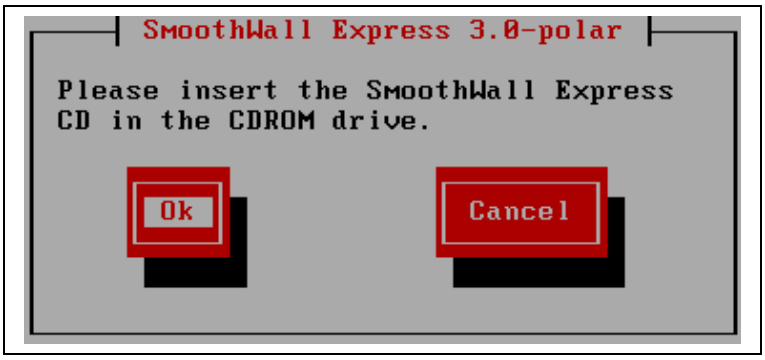


Fig. 6.3 Inicio de la instalación.

5 Pulse ENTER para continuar. El siguiente cuadro de diálogo se abre:

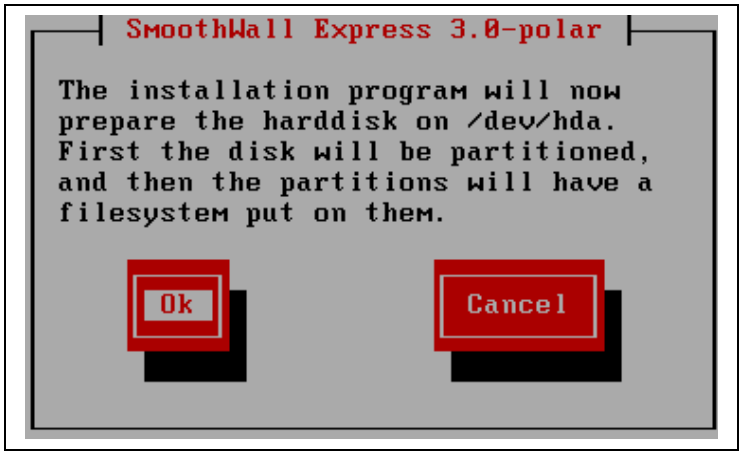


Fig. 6.4 Preparación del disco.

6 Pulse ENTER para continuar. El siguiente cuadro de diálogo se abre:

Fig. 6.5 Particionamiento del disco.

7 Pulse ENTER para continuar. Los archivos de SmoothWall Express están instalados. Cuando se complete, se abre el siguiente cuadro de diálogo:

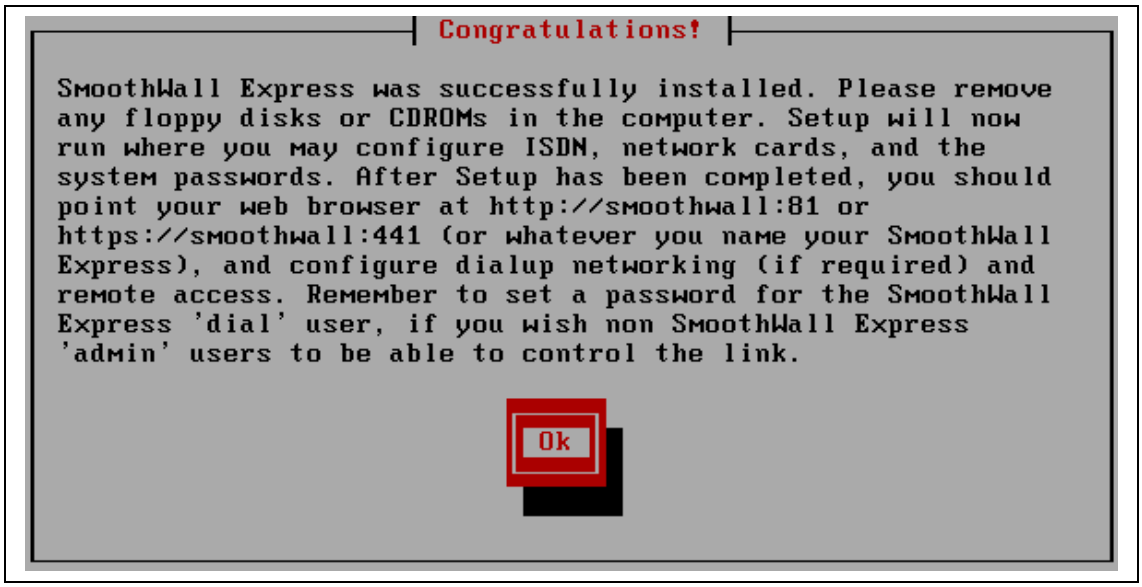


Fig. 6.6 Fin de la instalación.

8 Pulse ENTER. El siguiente cuadro de diálogo se abre:

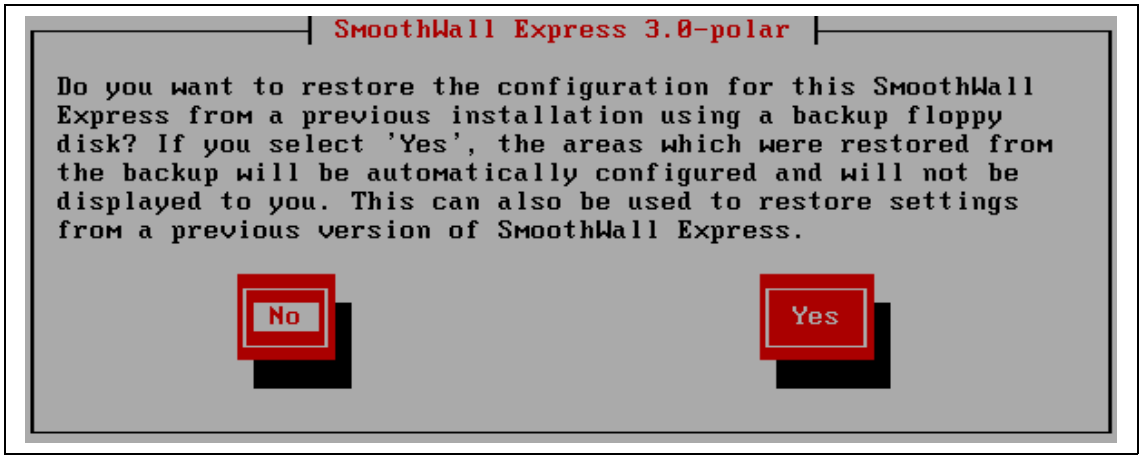


Fig.6.7 Inicio de la configuración.

9 Seleccione No y pulse ENTER para comenzar a configurar la nueva instalación de SmoothWall Express. El cuadro de asignación de teclado se abre:

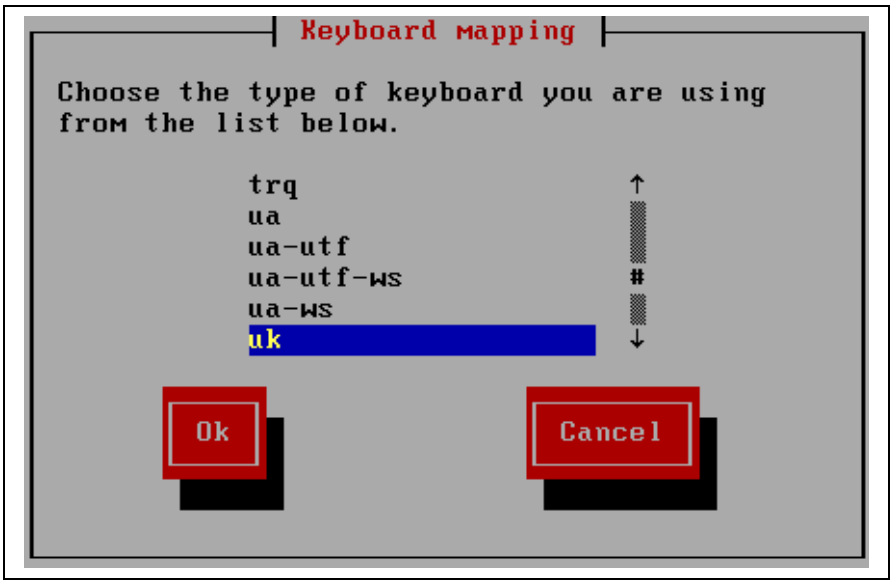


Fig. 6.8 Selección del lenguaje del teclado.

10 Seleccione el tipo de teclado (español) y pulse ENTER para continuar. Se abre el cuadro de diálogo Nombre de host:

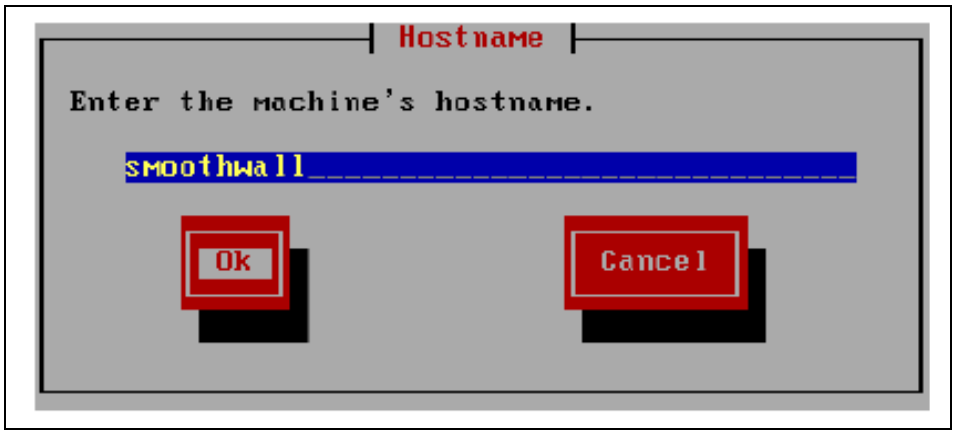


Fig. 6.9 Hostname de la máquina.

Aquí especifica el hostname par SmoothWall Express (smoothwallrouter).

Le recomendamos que sólo utilice caracteres en minúsculas en el nombre del host. Usted puede utilizar guiones "-" y puntos ".". No puede utilizar números, espacios, guiones bajos '_' o cualquier otro signo de puntuación ".".

El nombre de host por defecto es smoothwall. Si tiene varios sistemas de SmoothWall Express, utilice nombres de host único.

11 Si desea utilizar un nombre de equipo diferente, ingréselo. Seleccione OK y presione ENTER para continuar.

El cuadro de diálogo de la política de seguridad por defecto se abre:

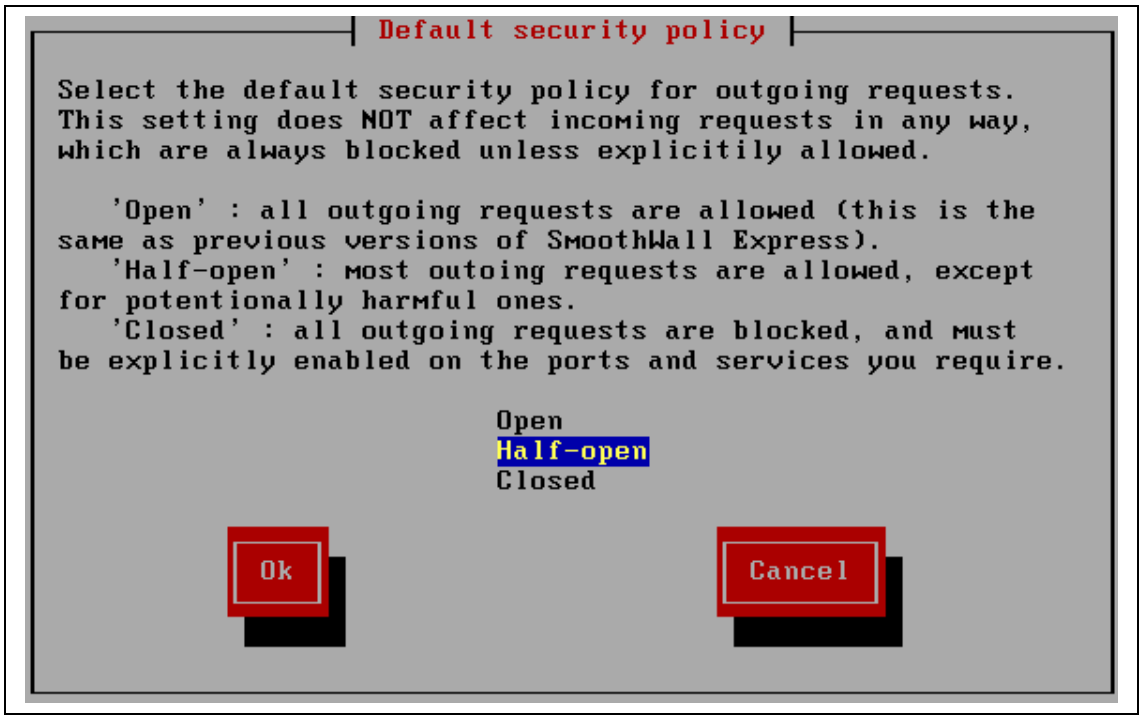


Fig. 6.10 Políticas de seguridad.

Las siguientes políticas están disponibles:

Política	**Descripción**
Open	SmoothWall Express permite todas las solicitudes outgoing.
Half-open	La política por defecto, SmoothWall Express permite más peticiones outgoing y bloquea peticiones potencialmente dañinas.
Closed	SmoothWall Express bloquea todas las solicitudes outgoing. Cualquier cosa que se permitiera debe ser expresamente permitido.

Tabla 6.2 Políticas de Seguridad.

La política de seguridad que se escogió fue **Open** ya que la VPN va a permitir solamente dos solicitudes outgoing de usuarios propios de la empresa.

12 Seleccione la política de seguridad que se adapte a tus necesidades. Seleccione OK y presione ENTER. El menú de configuración de red se abre:

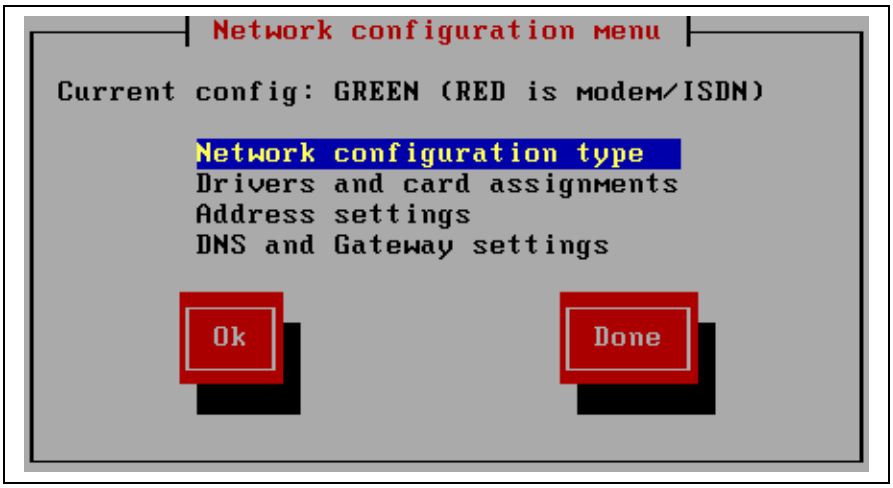


Fig. 6.11 Menú de configuración de red.

13 seleccione el tipo de configuración de red y presione ENTER. Se abre el cuadro de diálogo de tipo de configuración de red:

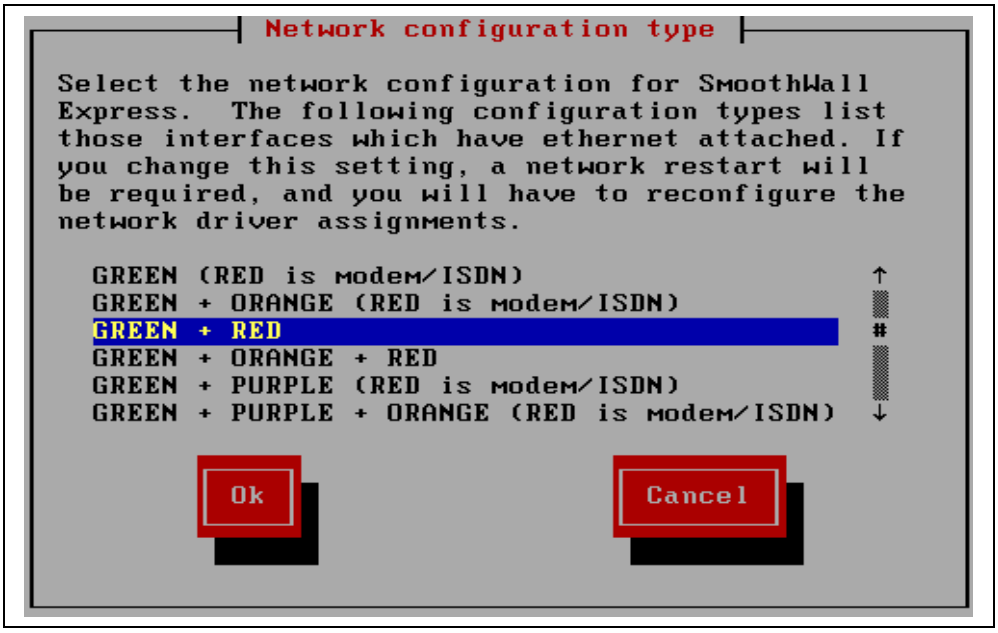


Fig. 6.12 Tipo de configuración de red.

SmoothWall Express es compatible con los siguientes tipos de configuración de red:

Tipo	**Explicación**

Green (Red is modem/ISDN)	Seleccione si SmoothWall Express utilizará: • Una tarjeta de interfaz de red (NIC) para conectarse a la red interna que está protegiendo. • Una tarjeta de módem o RDSI para conectarse a Internet o red externa.
Green + Orange (Red is modem/ISDN)	Seleccione si SmoothWall Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta de módem o RDSI para conectarse a Internet o red externa.
Green +Red	Seleccione si SmoothWall Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a Internet o red externa.
Green + Orange + Red	Seleccione si SmoothWall Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta NIC para conectarse a Internet o red externa.
Green + Purple (Red is modem/ISDN)	Seleccione si SmoothWall Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta de módem o RDSI para conectarse a Internet o red externa.
Green + Purple + Orange (Red is modem/ ISDN)	Seleccione si SmoothWall Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta de módem o RDSI para conectarse a Internet o red externa.
Green + Purple	Seleccione si SmoothWall Express utilizará:

+ Red	• Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta NIC para conectarse a Internet o red externa.
Green + Purple + Orange + Red	Seleccione si SmoothWall Express utilizará: • Una tarjeta NIC para conectarse a la red interna que está protegiendo. • Una tarjeta NIC para conectarse a una red inalámbrica. • Una tarjeta NIC para conectarse a una zona desmilitarizada. • Una tarjeta NIC para conectarse a Internet o red externa.

Tabla 6.3 Tipos de Configuración de Red.

14 Seleccione el tipo de configuración que se adapte a su red (Green + Red). Seleccione OK y presione ENTER. Volverá al menú de configuración de red.

15 Seleccione las tareas tarjeta y pulse ENTER para continuar. El cuadro de diálogo de asignación de las tarjetas se abre:

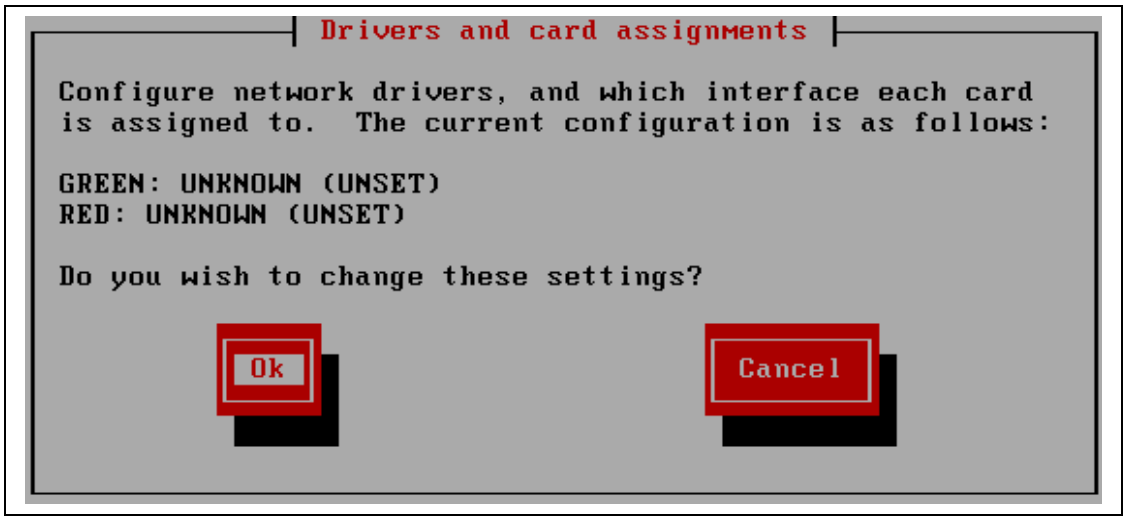


Fig. 6.13 Asignación de interfaces de red.

Dependiendo del tipo de configuración de red que ha seleccionado, se le pedirá que configurar los controladores de red y las interfaces necesarias.

16 Seleccionar OK y pulse ENTER para continuar. Se abre el cuadro de diálogo de asignación de la tarjeta:

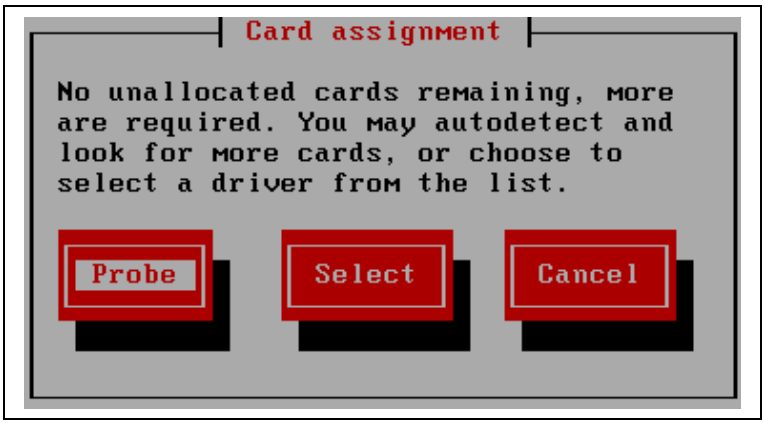


Fig. 6.14 Localización de interfaces de red.

17 Seleccione probar y pulse ENTER para detectar automáticamente tarjetas de red. Se muestra la información sobre las NIC (s) detectada (s), por ejemplo:

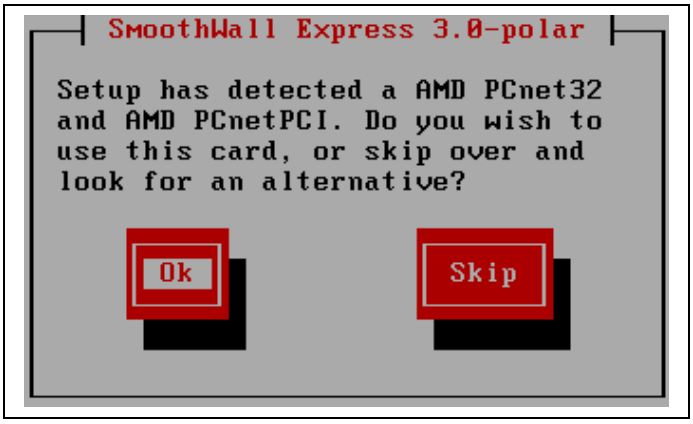


Fig. 6.15 Detección de las interfaces de red.

18 Seleccionar OK y pulse ENTER para continuar. El cuadro de diálogo abre el cuadro de asignación de tarjetas.

Fig. 6.16 Tarjetas de red.

19 Seleccionar GREEN y pulse ENTER. Repita los pasos anteriores para asignar las tarjetas a las interfaces de red. Cuando este completo, el siguiente cuadro de diálogo se abre.

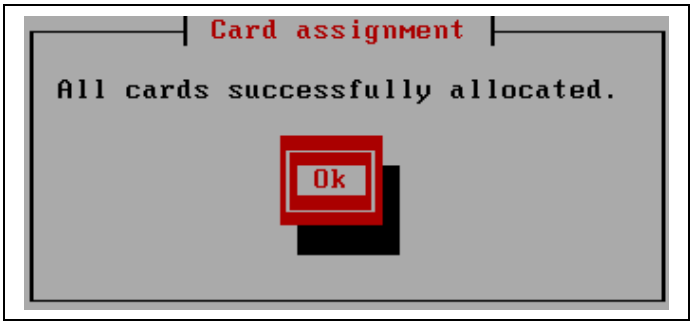


Fig. 6.17 Localización satisfactoria de las interfaces de red.

20 Pulse ENTER para volver al menú de configuración de red. Seleccione Ajustes de dirección y pulse ENTER. La configuración de direcciones se muestra.

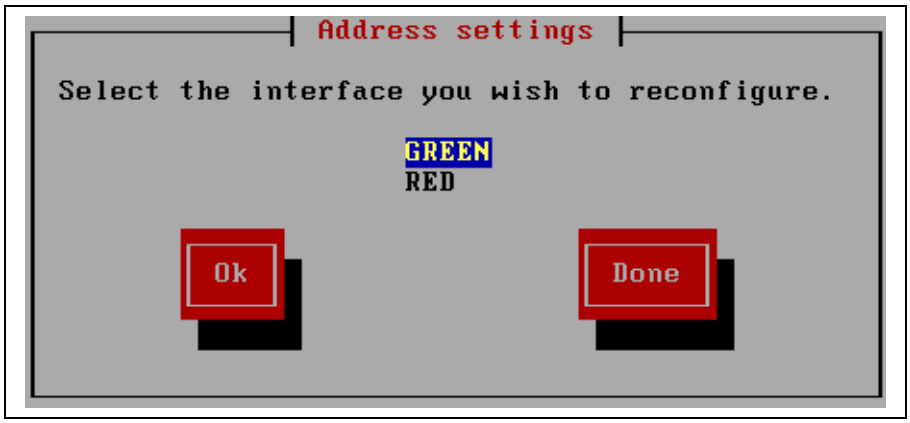


Fig. 6.18 Configuración de dirección interfaz “GREEN”.

21 Seleccionar GREEN y pulse ENTER. El siguiente cuadro de diálogo se abre:

Fig. 6.19 Aviso.

22. Presione ENTER para continuar. El cuadro de diálogo de interfaces se abre:

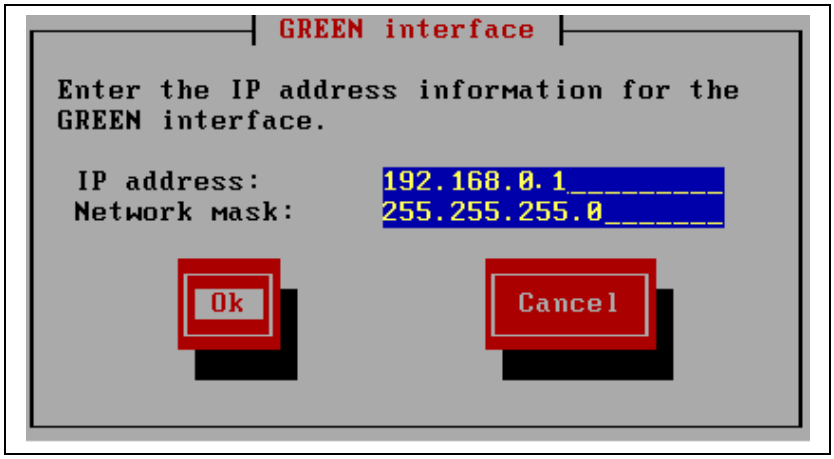


Fig. 6.20 Interfaz “GREEN”.

23 Seleccione OK y pulse ENTER. Volverá al cuadro de diálogo de configuración de direcciones:

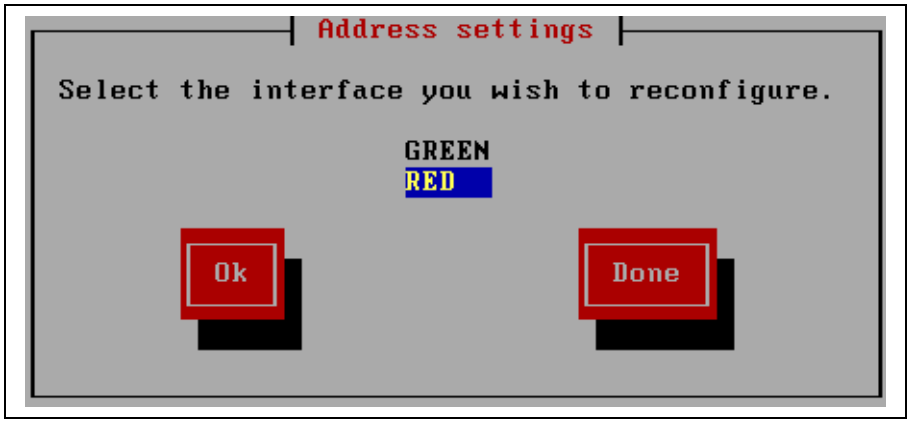


Fig. 6.21 Configuración de dirección interfaz “RED”.

24 Seleccione RED y pulse ENTER. El siguiente cuadro de diálogo se abre:

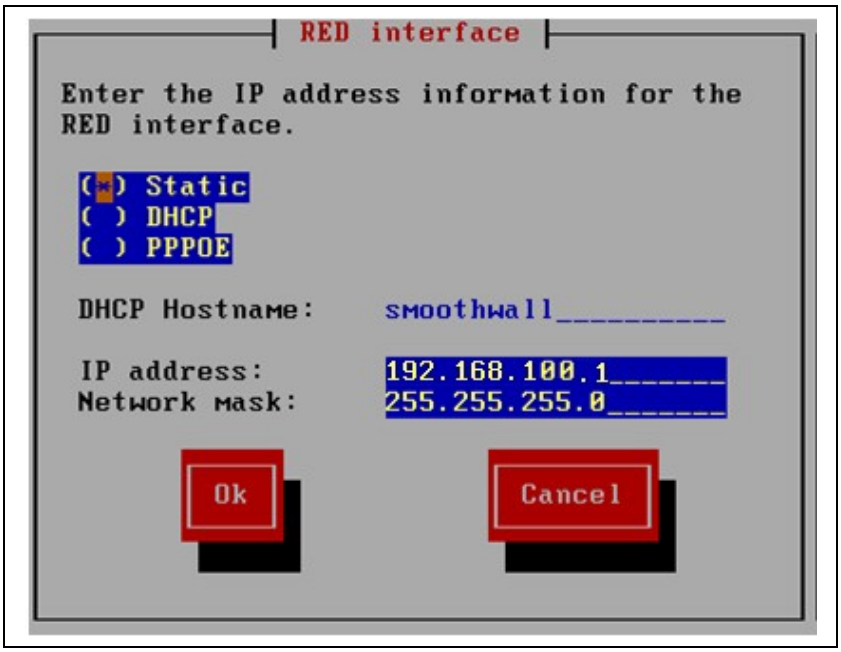


Fig. 6.22 Interfaz “RED”.

25. Las siguientes opciones están disponibles:

Opción	**Explicación**
Static	Seleccione esta opción si desea SmoothWall Express para usar una

	dirección IP estática que ha sido asignado por su proveedor de servicios de Internet (ISP).
DHCP	Seleccione esta opción si su ISP asigna dinámicamente una dirección IP diferente cada vez que se conecte a Internet.
PPPOE	Seleccione esta opción si su ISP usa Point-to-Point Protocol sobre Ethernet (PPPoE) para conectarse a Internet.
DHCP Hostname	Si ha seleccionado DHCP, puede cambiar el nombre de servidor aquí.
IP address	Si ha seleccionado Static, escriba la dirección IP estática para ser utilizado..
Network mask	Si ha seleccionado Static, acepte el valor predeterminado o introduzca una nueva máscara de red que se utilizará.

Tabla 6.4 Opciones de Configuración de la Interfaz “RED”.

26 Cuando termine, seleccione OK y pulse ENTER. En el cuadro de diálogo de configuración de direcciones, seleccione HECHO y pulse ENTER. El menú de la sección se muestra:

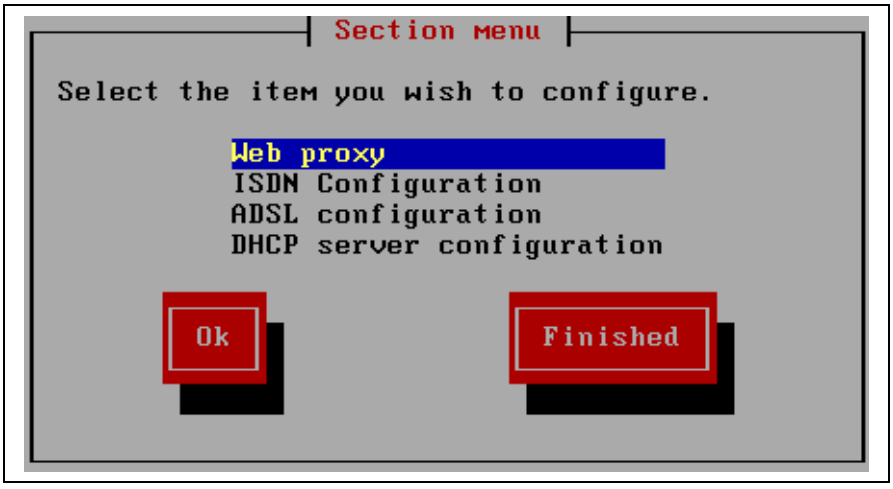


Fig. 6.23 Menú de configuración.

27 Seleccione FINALIZAR y pulse ENTER para continuar con el proceso de instalación. El siguiente cuadro de diálogo se abre:

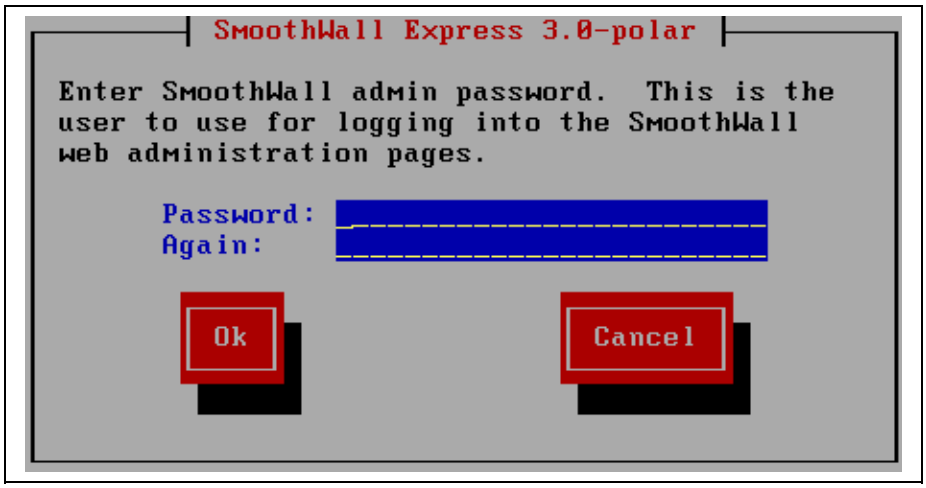


Fig. 6.24 Contraseña de la cuenta de usuario “admin” de SmoothWall.

28. Ingrese la siguiente información:

Campo	**Explicación**
Password	Escriba una contraseña segura para la cuenta de administrador. Mínimo = 6 caracteres Máximo = 25 caracteres La cuenta de administrador se utiliza para acceder SmoothWall Express a través de un navegador web y llevar a cabo la rutina de configuración y gestión.
Again	Vuelva a introducir la contraseña para confirmarla.

Tabla 6.5 Contraseña de la cuenta de usuario admin de SmoothWall.

29 Seleccionar OK y pulse ENTER. El siguiente cuadro de dialogo se abre:

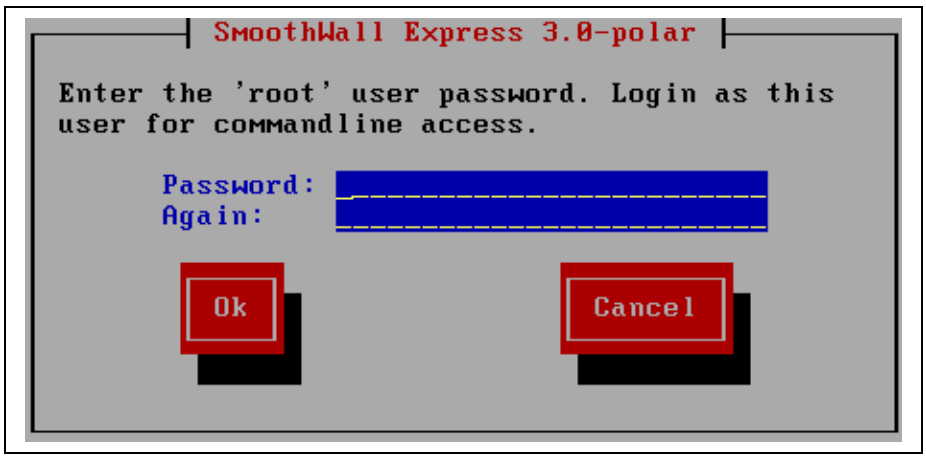


Fig. 6.25 Contraseña de la cuenta de usuario “root” de SmoothWall.

30. Ingrese la siguiente información:

Campo	Explicación
Password	Escriba una contraseña segura para la cuenta de administrador. Mínimo = 6 caracteres Máximo = 25 caracteres La cuenta de root tiene control total de SmoothWall Express y se utiliza para iniciar sesión en la consola de SmoothWall Express a través de SSH en el puerto no estándar 222.
Again	Vuelva a introducir la contraseña para confirmarla.

Tabla 6.6 Contraseña de la cuenta de usuario “root”.

31 Seleccionar OK y pulse ENTER. El siguiente cuadro de dialogo se abre:

Fig. 6.26 Configuración completa.

32 Seleccionar OK y pulse ENTER para reiniciar la estación de trabajo. Después de reiniciar, puede acceder a SmoothWall Express desde un cliente de red que ejecute un navegador web.

6.2.3 Acceso a SmoothWall Express por Primera Vez

1 En el navegador de su elección, escriba la dirección de su SmoothWall Express.

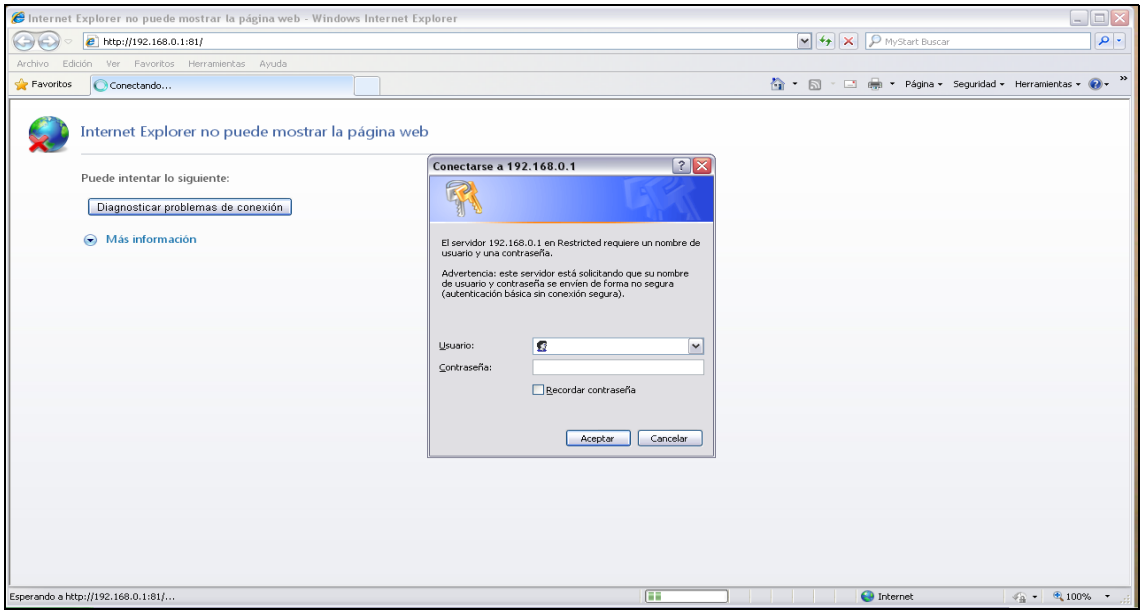


Fig. 6.27 Acceso a SmoothWall vía web.

2 Cuando se le pregunta por su navegador, introduzca la siguiente información:

Campo	**Información**
Usuario	Ingrese admin. Este es el nombre por defecto de la cuanta de administración de SmoothWall Express.
Contraseña	Ingrese la contraseña que especificó para la cuenta admin durante la instalación de SmoothWall Express.

Tabla 6.7 Usuario y contraseña de la cuenta admin.

3 Click en ACEPTAR. Se abre la página principal de control:

Fig. 6.28 Página de inicio de SmoothWall vía web.

6.2.4 Conexiones Roadwarrior con SmoothWall Express y Zerina.

Lo primero que debemos haces es descargarnos el addon de Zerina desde esta dirección http://www.zerina.de/zerina/files/alpha/ZERINA-0.9.7a14-Installer.tar.gz, una vez que descargamos el paquetes lo debemos copiar a una carpeta de nuestro SmoothWall Express, por lo general lo pondremos en /tmp para hacer esto usaremos el WinSCP. A continuación explico la forma de hacerlo:

Si no tiene el WinSCP instalado lo descargamos desde aquí http://winscp.net/eng/download.php, lo instalamos en nuestra PC y lo ejecutamos. Nos aparecerá una imagen como esta:

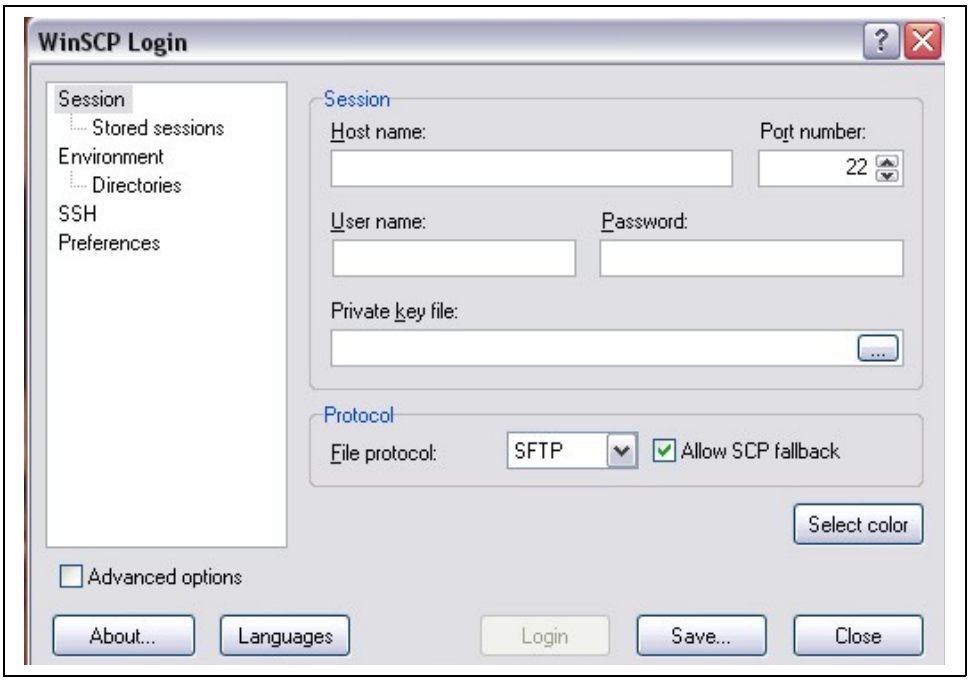


Fig. 6.29 Aplicación WinSCP.

Cabe indicar que se debe poner la IP o el nombre que le asignaron al SmoothWall Express, el puerto (222), nombre de usuario (root) y la contraseña, una vez suministrados esos datos presionamos en el botón “Login”, si es la primera vez que ingresamos aparecerá un mensaje avisándonos que no se conoce el servidor pero le presionamos el botón “Si” ya que si ingresamos los datos correctamente efectivamente será nuestro servidor, este mensaje solo aparece la primera vez que nos conectamos y luego se genera una clave que se usa para validar cada vez que nos reconectemos.

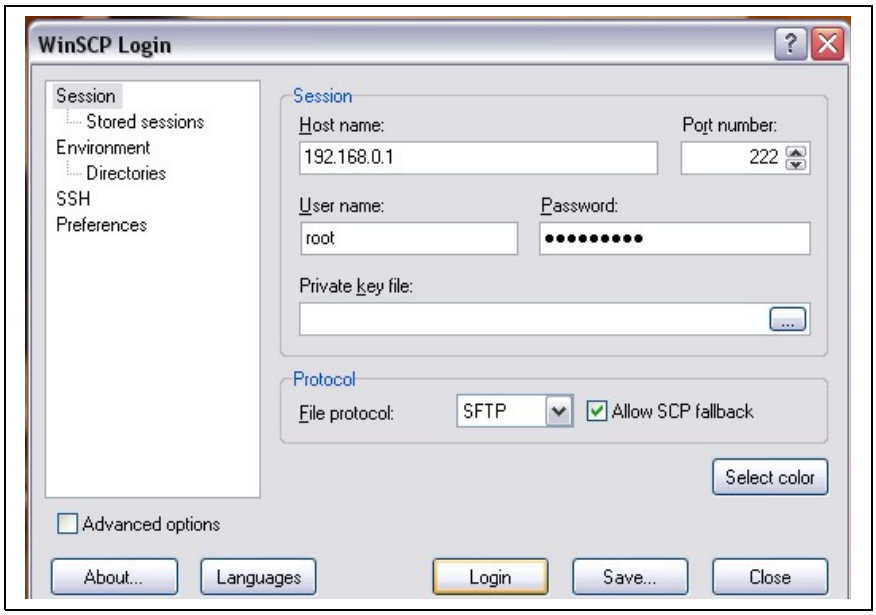


Fig. 6.30 Accesando a SmoothWall mediante WinSCP.

A continuación se nos presentará una pantalla en la cual deberemos buscar el lugar de origen del archivo que queremos copiar y el de destino, una vez especificado el lugar donde se copiara el archivo simplemente lo arrastramos, aparecerá una ventana con un mensaje y ahí presionaremos el botón “Copiar”.

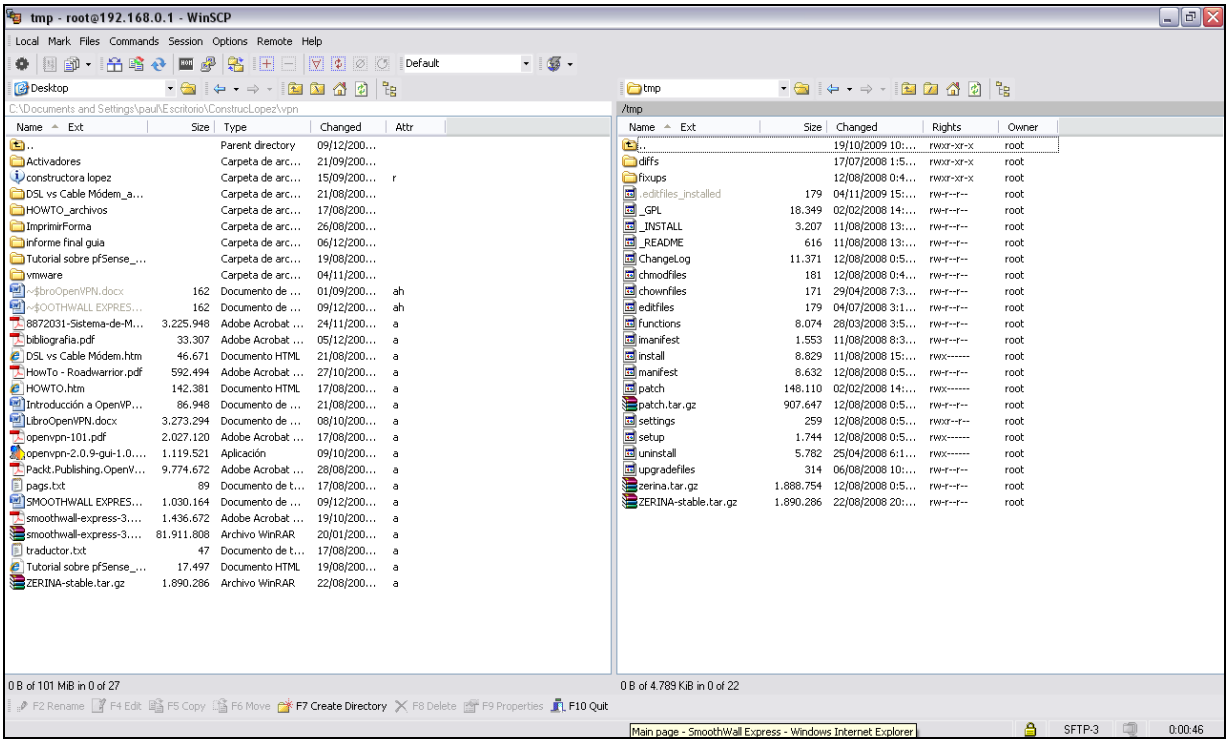


Fig. 6.31 Compartición de ZERINA.

Si todo salió bien nos vamos a la consola de nuestro SmoothWall Express, entonces lo que resta hacer ahora es movernos hasta el lugar en donde copiamos el add-on de Zerina (cd /tmp). Una vez que nos encontramos ahí debemos extraer el contenido del archivo para poder luego instalarlo, lo hacemos de la siguiente manera:

tar xzf ZERINA-0.9.7a14-Installer.tar

Ahora que ya esta descomprimido el archivo debemos instalarlo, para ello ejecutaremos:

./install.

Ya debería estar instalado el add-on, para corroborar esto accederemos a nuestro SmoothWall Express desde un navegador como lo explique antes y verán que en la solapa VPN´s se agrego una entrada más que dice “OpenVPN”.

Fig. 6.32 Paquete de OpenVPN para SmoothWall.

6.2.5 Configuración Inicial

En la sección “**Autoridades Certificadoras”** deberemos crear los correspondientes certificados, para ellos presionaremos sobre el botón **“Generar certificados de Raíz/Anfitrión”**, en la pantalla que se muestra a continuación debemos llenar los datos que son obligatorios, como se muestra en la siguiente imagen:

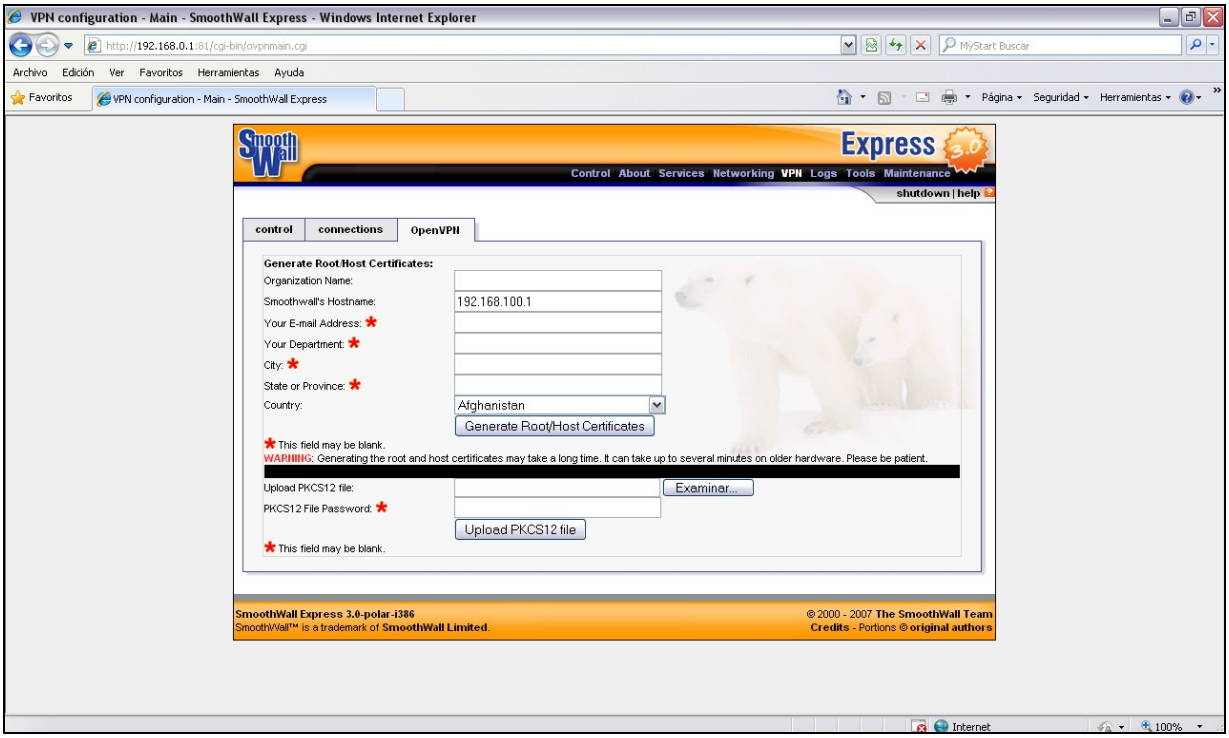


Fig. 6.33 Autoridades certificadoras.

En el primer campo pondremos algún nombre que nos identifique, en el segundo debemos indicar la IP de la placa RED de nuestro SmoothWall Express y como último dato obligatorio debemos seleccionar el país. Los demás campos no son necesarios completar pero es buena idea hacerlo. Por último hacemos click en el botón **“Generar certificados de Raíz/Anfitrión”**.

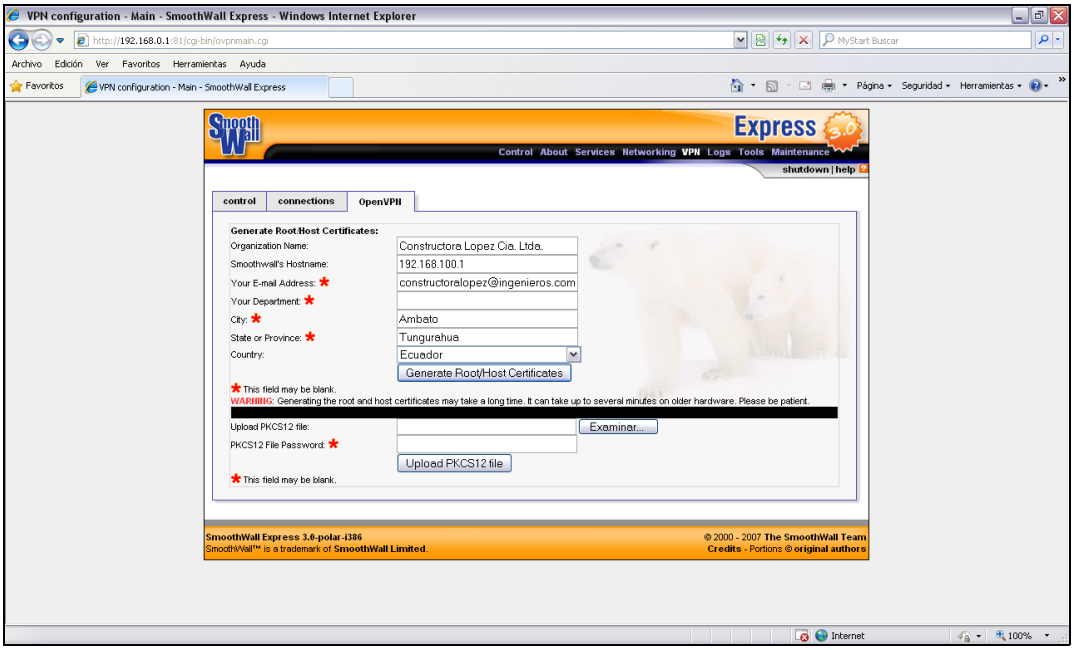


Fig. 6.34 Generación del certificado.

Si todo salió bien se habrán creado los certificados y se muestran en la página principal, en la sección correspondiente.

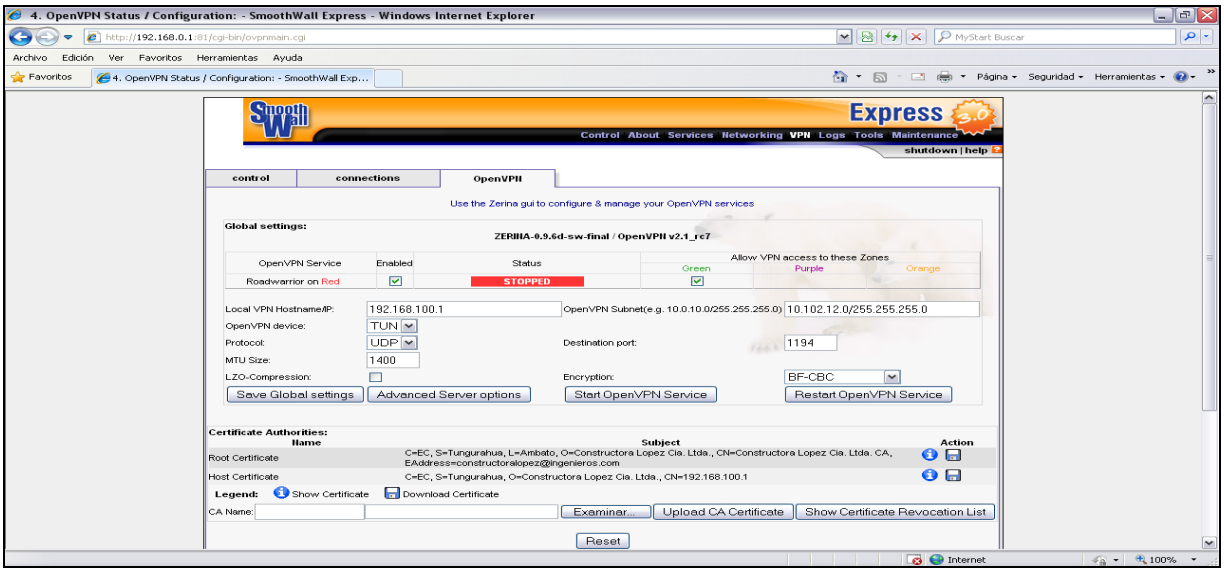


Fig. 6.35 Comprobación de creación del certificado.

Lo que sigue ahora es configurar el servidor **Roadwarrior**, para ello nos dirigimos la sección de **"Configuración Global"**, como se muestra en la imagen a continuación:

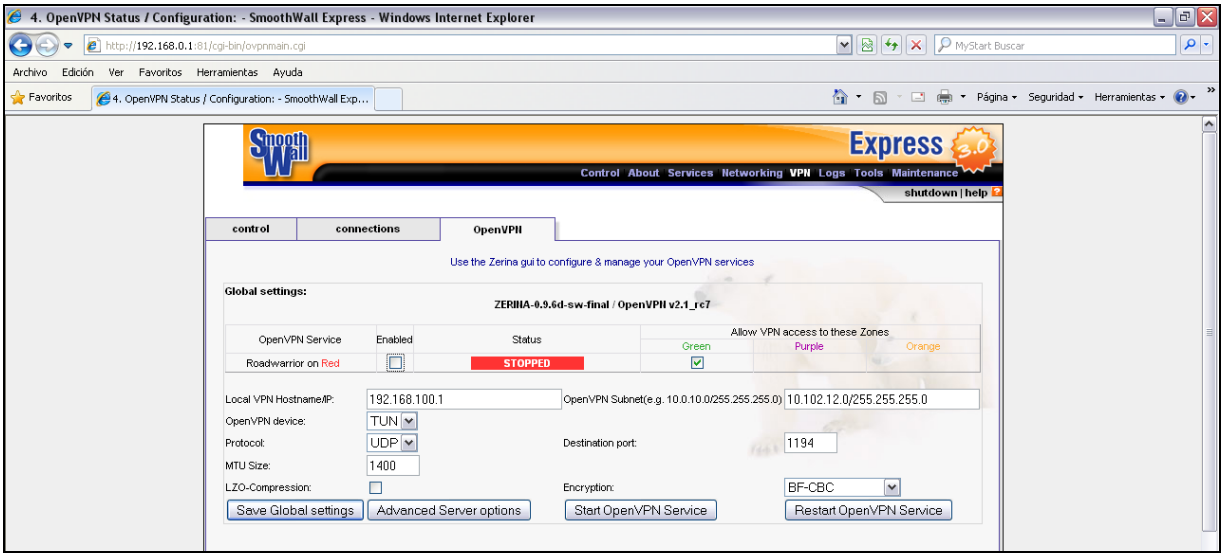


Fig. 6.36 Configuración Roadwarrior.

Lo que debemos hacer es tildar la opción "OpenVPN en interfaz RED", en el campo "Local VPN Hostname IP" debemos poner la IP de la interfaz RED de nuestro Smooth WallExpress, así como también en el campo "OpenVPN Subnet" debemos ingresar una red con su respectiva máscara.

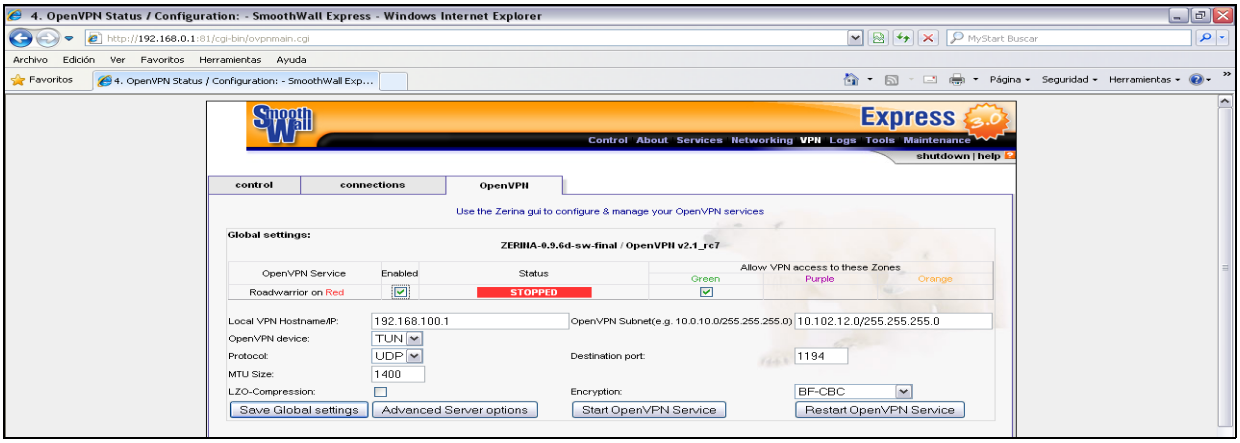


Fig. 6.37 Configuración global.

Lo que sigue a continuación es iniciar el Servidor para que escuche a los clientes que se quieran conectar, para esto simplemente hacemos click en el botón “Start OpenVPN Service” y automáticamente se observa que donde dice **“Status”** cambia de STOPPED a RUNNING . Esto significa que todo está bien, ahora nos resta agregar el cliente y establecer la conexión.

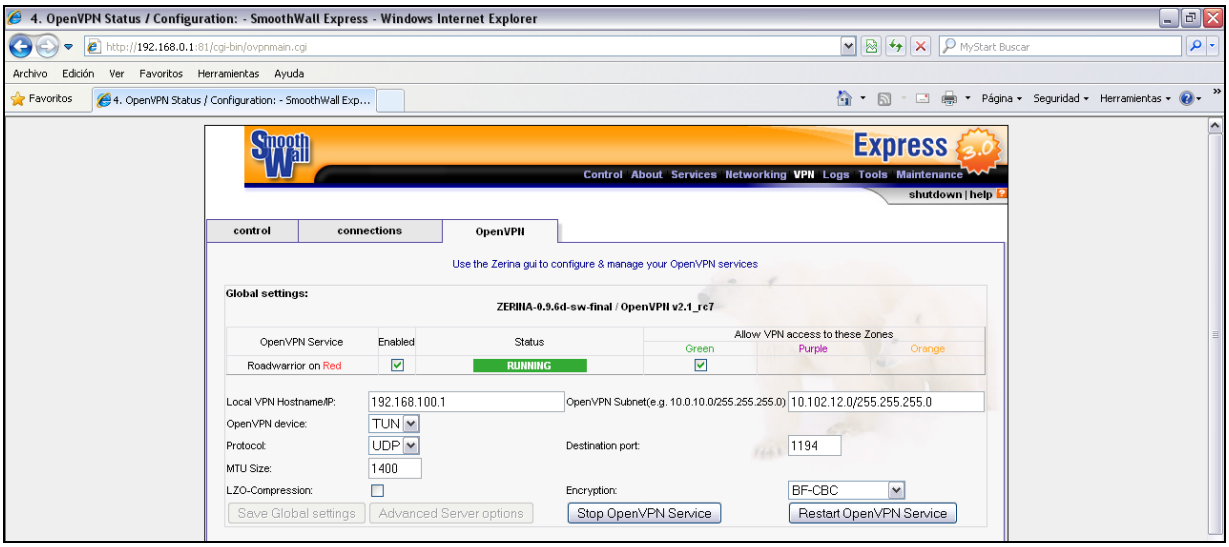


Fig. 6.38 Inicio de OpenVPN Service.

6.2.6 Agregar un cliente

En la sección “**Client status and control”** presionaremos en el botón “Add”.

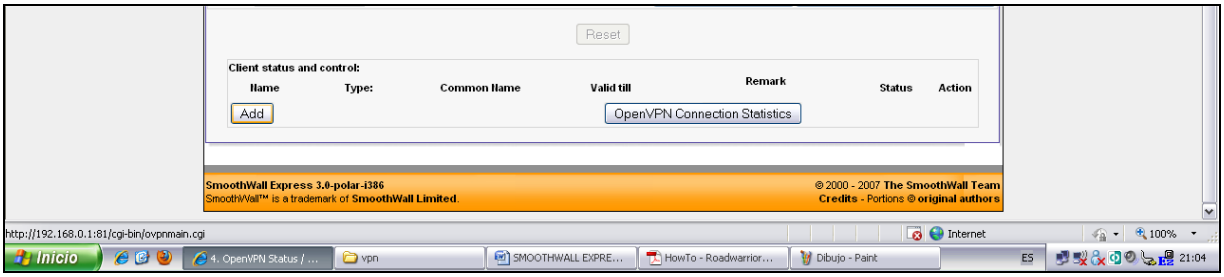


Fig. 6.39 Agregar cliente.

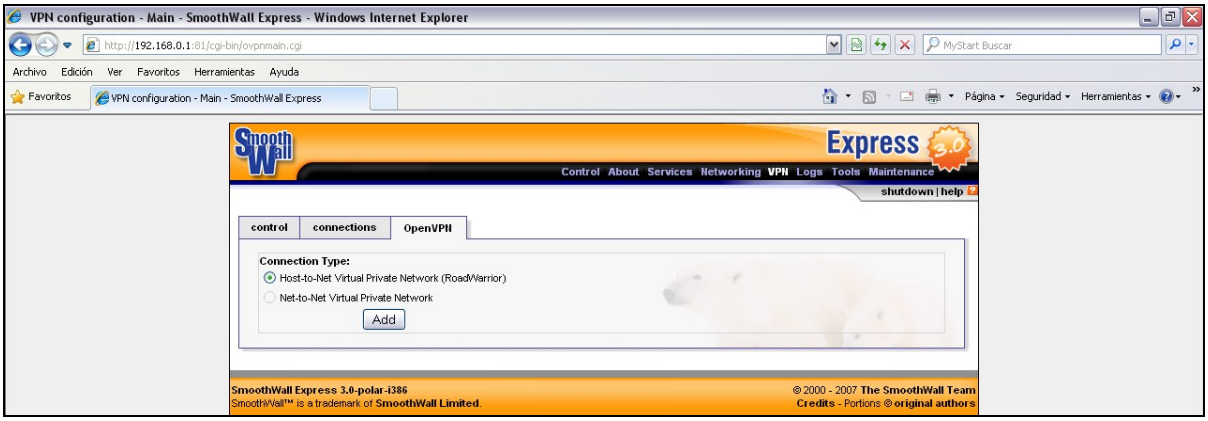


Fig. 6.40 Tipo de conexión.

Se nos presentara una ventana nueva como la siguiente:

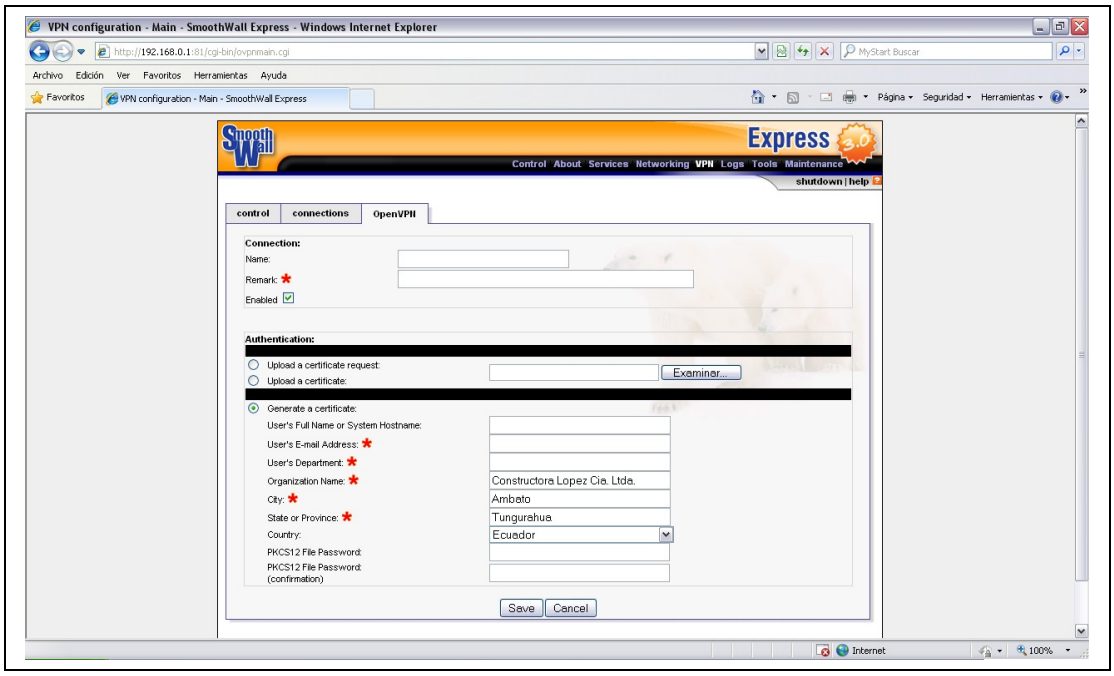


Fig. 6.41 Configuración del cliente.

Aquí llenaremos los datos para el cliente, en el campo **“Nombre”** pondremos cualquier nombre que identifique al cliente, por ejemplo cliente1. Si deseamos le agregamos una descripción en el campo de abajo y dejamos tildado la opción **“Enabled”**. El siguiente campo que llenaremos es el que dice **“User´s Full Name or System Hostname”,** aquí pondremos el mismo que pusimos arriba (cliente1). En el combo de **“País”** seleccionamos nuestro país. Ahora los últimos dos campos son para que al momento de conectarse pida una contraseña al cliente, los podemos dejar en blanco pero no es recomendable.

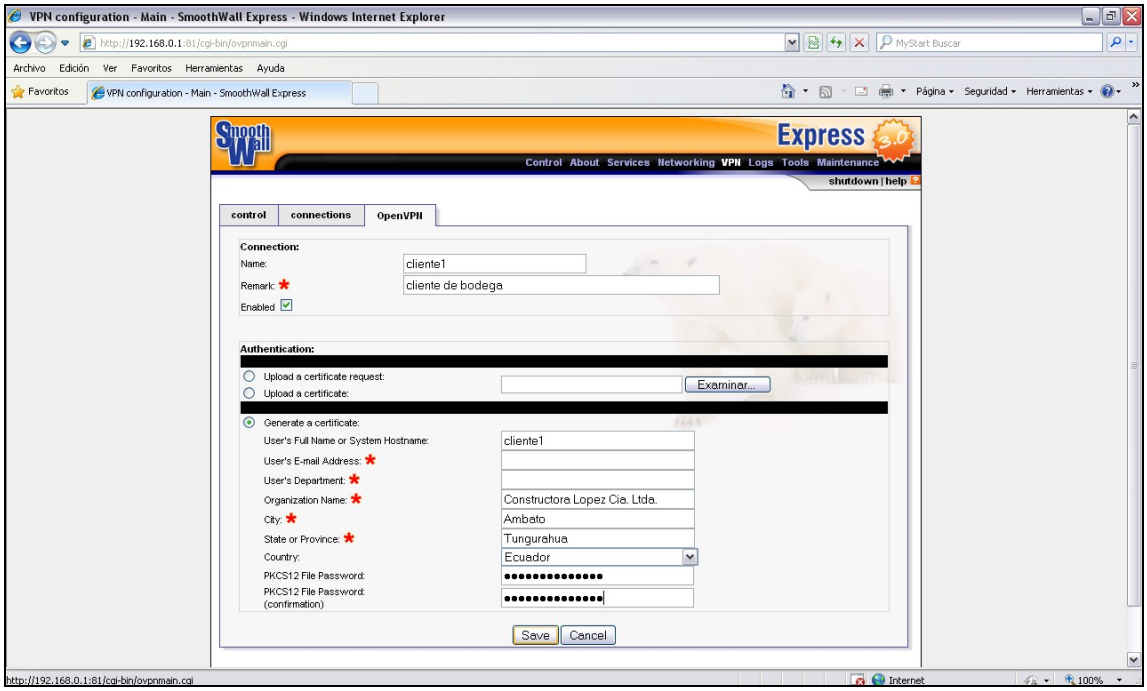


Fig. 6.42 Generación del cliente.

Una vez completados estos campos presionamos el botón “Save”. Si todo salió bien en la pantalla principal, en la sección **“Client status and control”** deberá estar agregado el cliente que configuramos anteriormente.

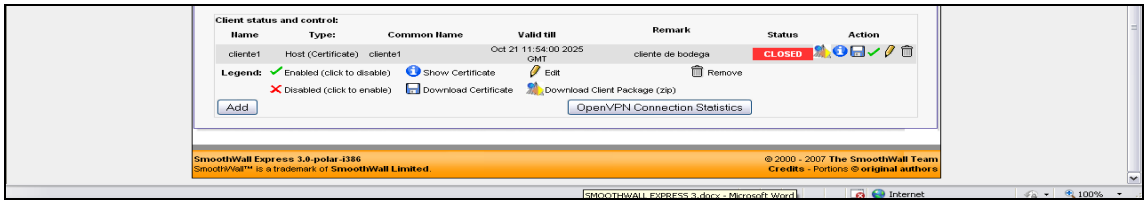


Fig. 6.43 Cliente agregado.

Lo que sigue ahora es descargarnos el archivo que usaremos para conectarnos, hacemos click en el icono de VPN. Como se muestra en la siguiente imagen:

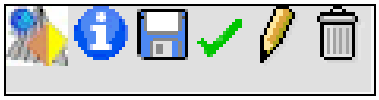


Fig. 6.44 Icono de descarga de archivos de configuración.

Guardamos este archivo en algún lugar de nuestra PC ya que lo usaremos a continuación.

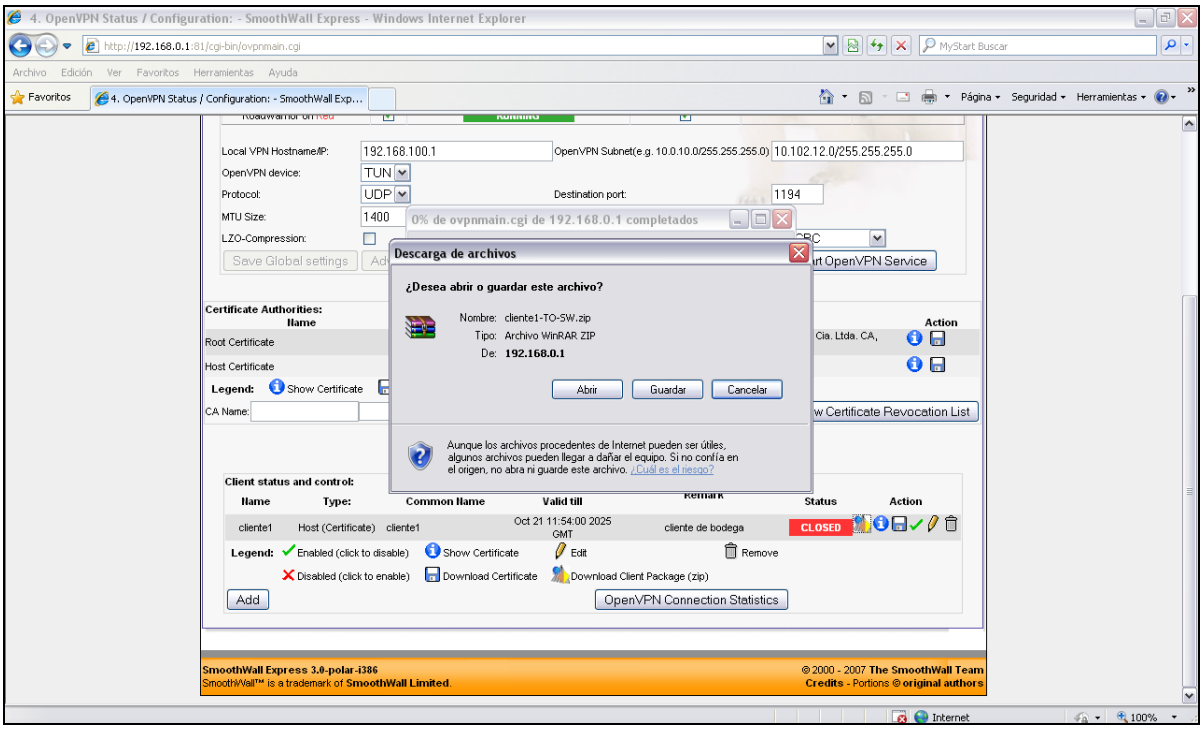


Fig. 6.45 Descarga de archivos de configuración.

6.2.7 Instalando OpenVPN en el Cliente

Para establecer la conexión con el servidor necesitaremos un cliente VPN que maneje y establezca la conexión.

Si desea instalar OpenVPN en Windows, una buena opción es OpenVPN GUI, se puede descargar desde aquí **http://openvpn.se/files/install_packages/openvpn-**

2.0.9-gui-1.0.3-install.exe. Este paquete contiene el software de OpenVPN además de una interfaz gráfica de usuario para abrir o cerrar los túneles.

OpenVPN puede ejecutarse como un servicio en una computadora de Windows, lo que significa que se ejecuta automáticamente al iniciar. Puede ser configurado para que el túnel se habilite de forma automática o forzado para hacerlopor medion de un click. La instalación es bastante sencilla y no debería plantear ningún problema para el usuario de Windows con experiencia. En las secciones siguientes se dará un proceso de instalación guiada.

6.2.7.1 Empezando la instalación

Inicie la sesión como administrador o usuario privilegiado y haga doble click en el archivo descargado para iniciar el asistente de configuración. Si usted está usando un firewall de escritorio, se le pide que permita a OpenVPN ser instalado.

Fig. 6.46 Inicio de instalación de OpenVPN GUI.

El asistente de instalación de OpenVPN GUI, probablemente es la forma más conveniente para instalar OpenVPN en Windows. Haga click en NEXT para continuar.

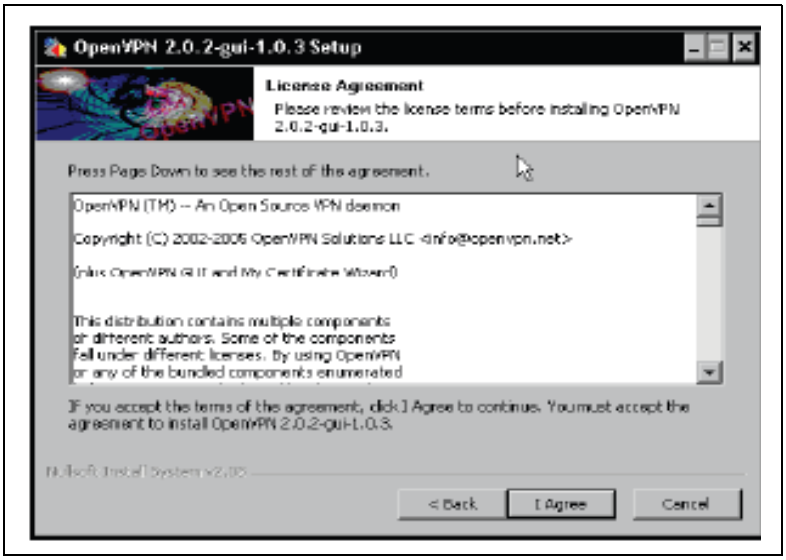


Fig. 6.47 Acuerdo de licencia OpenVPN GUI.

A pesar de que OpenVPN y el GUI son completamente disponibles en el marco del código abierto Licencia Pública General (GPL), usted tiene que aceptar un acuerdo de licencia. Usted debe leer la licencia para asegurarse de que la utilización prevista de OpenVPN se ajusta a él. Haga click en I AGREE para continuar.

6.2.7.2 Selección de componentes y ubicación

El siguiente cuadro de diálogo ofrece una selección de los componentes de OpenVPN que desee instalar. Así, la selección estándar de los componentes tiene sentido en casi todos los casos.

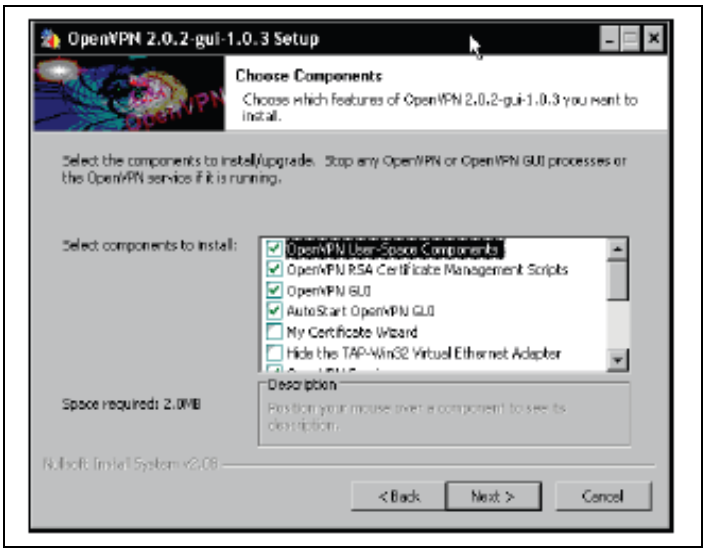


Fig. 6.48 Componentes de OpenVPN GUI.

En este diálogo, usted tiene varias opciones para escoger. La siguiente tabla da una visión general de las entradas, cuando se debe instalar y sus prestaciones. El cliente de instalación es un sistema que sólo se conecta a otro sistema de OpenVPN, mientras que la instalación del servidor OpenVPN es un sistema que permite las conexiones entrantes.

Opción	**Característica**
OpenVPN en espacio de usuario de componentes	El programa de OpenVPN
OpenVPN RSA Certificado de gestión de secuencias de comandos	fácil de RSA para Windows
OpenVPN GUI	La interfaz gráfica de usuario
AutoStart OpenVPN GUI	Link para el inicio automático
Mi Asistente para certificados	Las solicitudes de certificado de una autoridad de certificación
Hide the TAP-Win32 VEA	La interfaz no se muestra en la

	configuración de la red
Servicio OpenVPN	Configurar OpenVPN como un servicio
OpenVPN asociaciones de archivos	Los archivos de configuración (*. ovpn) están asociados con OpenVPN
OpenSSL DLL	Bibliotecas de vínculos dinámicos
TAP-WIN32 VEA	Interfaz de red virtual
Añadir OpenVPN con el PATH	Openvpn.exe está en el camino de la línea de comandos de cada usuario
Añadir accesos directos al menú Inicio	Acceso directo al menú Inicio

Tabla 6.8 Componentes de OpenVPN GUI.

Como puede ver, las únicas diferencias son la gestión de RSA y la opción de ejecutar OpenVPN como un servicio. Ambos pueden ser configurados con diferentes medios, como el archivo de configuración, la gestión del sistema de Windows.

Pulse NEXT para continuar la instalación.

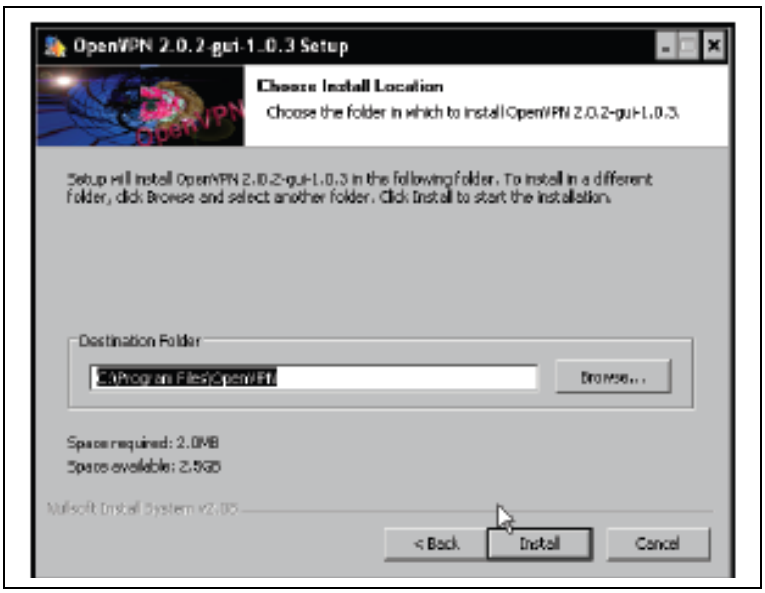


Fig. 6.49 Path de instalación.

Ahora tiene que seleccionar un directorio de instalación de OpenVPN. La ruta de instalación estándar de OpenVPN en Windows es C: \ Archivos de programa \ OpenVPN, y esto debería funcionar bien en casi todos los casos. Sin embargo, usted puede definir el camino a su gusto. Después de hacer click en "INSTALL", se inicia el proceso de instalación.

6.2.7.3 Finalizando la instalación

Mientras OpenVPN se está instalando, puede leer la salida en la ventana de instalación y seguir con la creación de carpetas, archivos, accesos directos y la instalación de controladores (TAP) para la creación de redes.

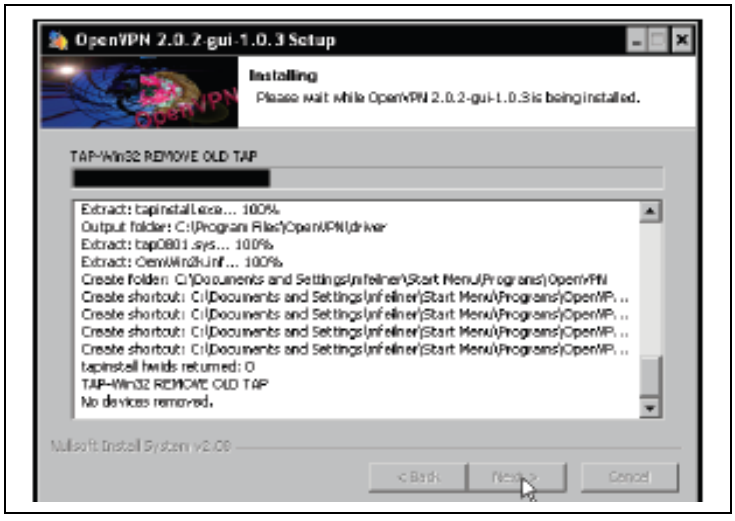


Fig. 6.50 Finalizando la instalación.

Si usted ha hecho esto hasta ahora, ha instalado OpenVPN en su sistema Windows. Si desea leer el archivo readme, active la casilla de verificación mostrar readme antes de hacer click en FINISH.

6.3 Pruebas.

6.3.1 Pruebas de Conectividad.

Después de la instalación de OpenVPN GUI, OpenVPN se inicia y un applet del panel se crea. En la siguiente captura de pantalla, es el icono a la izquierda:

Fig. 6.51 Icono de OpenVPN GUI.

Una vez que haya configurado una conexión en primer lugar, este menú se rellenará con las nuevas entradas. Con las entradas de conexión y desconexión puede iniciar y detener los túneles configurados.

Fig. 6.52 Menú de OpenVPN GUI.

Ahora lo que debemos hacer es colocar el certificado que descargamos de nuestro SmoothWall Express y colocarlo en la siguiente dirección: **"C:\Archivos de programa\OpenVPN\config".** Una vez que lo hayamos copiado ahí debemos descomprimirlo con lo cual nos quedaran dos archivos:

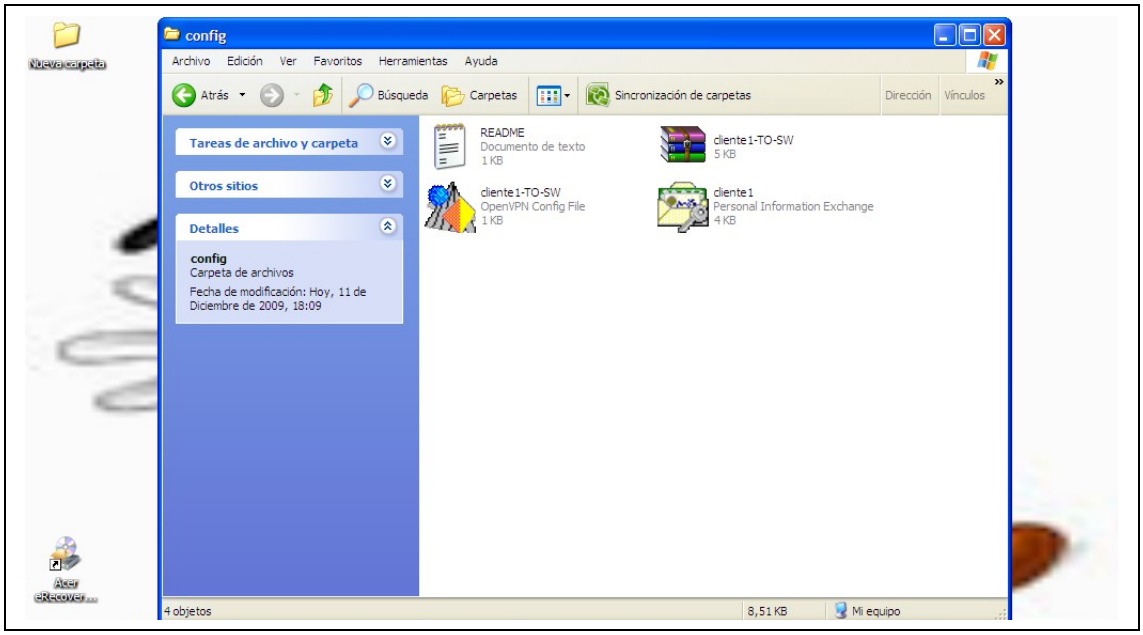


Fig. 6.53 Archivos de configuración del cliente.

Lo que sigue ahora es conectarnos, para ellos simplemente nos dirigimos al icono que mencionamos antes, y hacemos click con el botón derecho del mouse nos aparecerá un menú en el cual seleccionaremos la opción que dice **"Connect"**:

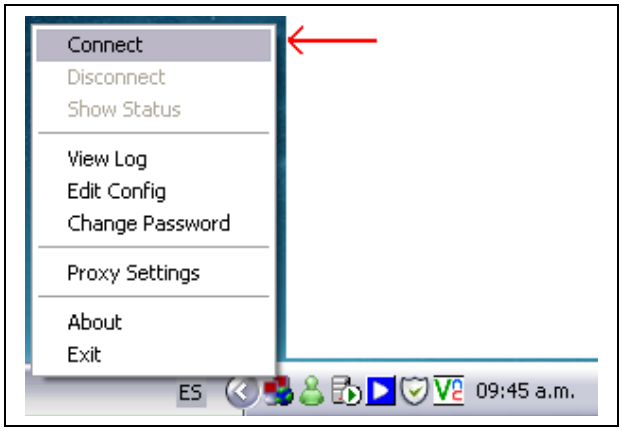


Fig. 6.54 Conexión con el servidor VPN.

A continuación se abrirá una pantalla en la cual se tratará de establecer la conexión, pero antes de esto nos solicitara la contraseña que le creamos al momento de hacer el certificado:

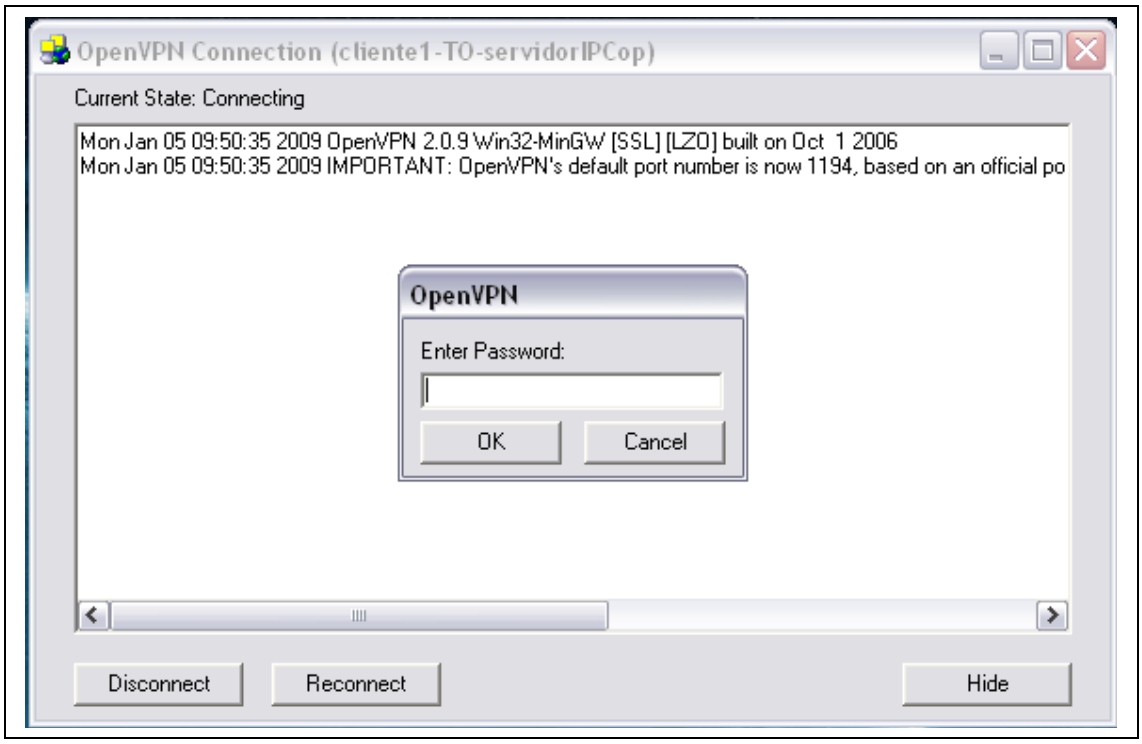


Fig. 6.55 Estableciendo la conexión con el servidor VPN.

A continuación verán que se establece la conexión y como el icono de la OpenVPN GUI cambia a un color verde, además de todo esto aparecerá un cartel informándonos que la conexión ha sido exitosa, igual que este:

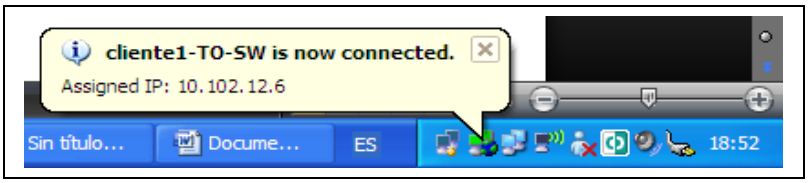


Fig. 6.56 Aviso de conexión exitosa.

En este momento están en condiciones de acceder a cualquier recurso compartido de la red y para chequear definitivamente que estamos conectados revisamos la pagina de administración de nuestro SmoothWall Express.

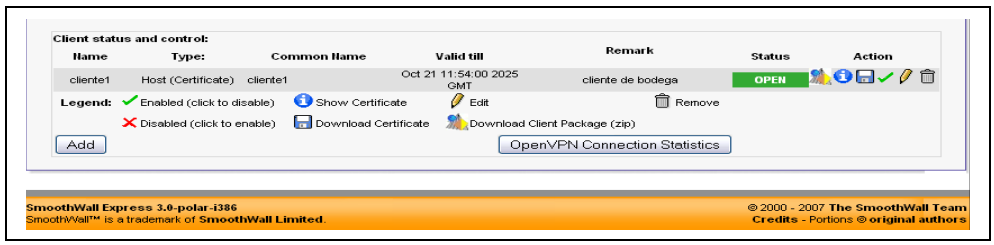


Fig. 6.57 Cliente conectado.

Observen como el estado cambió de CLOSED a OPEN, esto nos indica que estamos conectados.

6.3.2 Pruebas de Medición de Ancho de Banda.

Formato de la trama Ethernet.

Preámbulo	SOF	Destino	Origen	Longitud	Datos	Relleno	FCS
7 bytes	1	6	6	2 bytes	0 a 1500	0 a 46	4

	byte	bytes	bytes		bytes	bytes	bytes

Fig. 6.58 Formato de la trama Ethernet.

Preámbulo

Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es:
10101010 10101010 10101010 10101010 10101010 10101010 10101010

Estos bits se transmiten en orden, de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

SOF (Start Of Frame) Inicio de Trama

Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de dirección MAC de destino.

Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

Dirección de destino

Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo multicast o la dirección de broadcast de la red.

Cada estación examina este campo para determinar si debe aceptar la trama (si es la estación destinataria).

Dirección de origen

Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 desde la que se envía la trama. La estación que deba aceptar la trama conoce por este campo la dirección de la estación origen con la cual intercambiará datos.

Tipo

Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con la trama o, en su defecto, la longitud del campo de datos. La capa de enlace de datos interpreta este campo. (En la IEEE 802.3 es el campo longitud y debe ser menor o igual a 1526 bytes.)

Datos

Campo de 0 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

Relleno

Campo de 0 a 46 bytes que se utiliza cuando la trama Ethernet no alcanza los 64 bytes mínimos para que no se presenten problemas de detección de colisiones cuando la trama es muy corta.

FCS (Frame Check Sequence - Secuencia de Verificación de Trama)

Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (Control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida.

ADSL (*Asymmetric Digital Subscriber Line*) Línea de Suscripción Digital Asimétrica

ADSL es un tipo de línea DSL. Consiste en una transmisión de datos digitales (la transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 km. medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

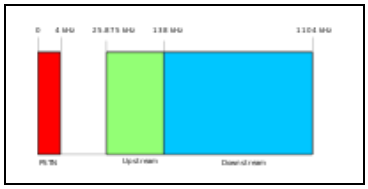


Fig. 6.59 Frecuencias usadas en ADSL.

El área roja es el área usada por la voz en telefonía normal, el verde es el *upstream* o subida de datos y el azul es para el *downstream* o descarga de datos.

Es una tecnología de acceso a Internet de banda ancha, lo que implica una mayor velocidad en la transferencia de datos. Esto se consigue mediante una modulación de las señales de datos en una banda de frecuencias más alta que la utilizada en las conversaciones telefónicas convencionales (300-3800 Hz), función que realiza el Router ADSL. Para evitar distorsiones en las señales transmitidas, es necesaria la instalación de un filtro (llamado *splitter* o discriminador) que se encarga de separar la señal telefónica convencional de las señales moduladas de la conexión mediante ADSL.

Esta tecnología se denomina *asimétrica* debido a que la capacidad de descarga (desde la Red hasta el usuario) y de subida de datos (en sentido inverso) no coinciden. Normalmente, la capacidad de bajada (descarga) es mayor que la de subida.

En una línea ADSL se establecen tres canales de comunicación, que son el de envío de datos, el de recepción de datos y el de servicio telefónico normal.

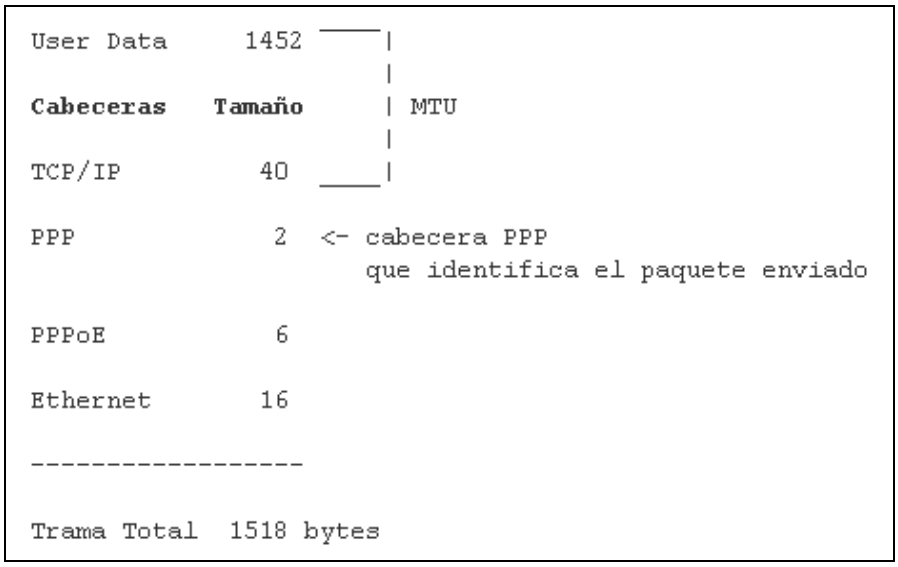


Fig. 6.60 MTU ADSL.

El rendimiento de una conexión nunca es del 100%. Hay que tener en cuenta que en estos tipos de conexiones se utilizan diversos protocolos, que ocupan ancho de banda (entre un 2% y un 20% del total, según el tipo de conexión protocolo utilizado), con lo que se reduce el ancho de banda útil para la transmisión de datos.

Debemos tener en cuenta que la medición de velocidad de transferencia se presenta en KBps (Kilobytes por segundo) y la velocidad de conexión se la identifica en Kbps (Kilobits por segundo). Para convertir de KBps a Kbps se debe multiplicar por 8.

Conexión en KBps	Ancho de banda útil
256 KBps	32 Kbps
512 KBps	64 Kbps
1Mega (1024KBps)	128 Kbps
2 Megas (2048KBps)	256 Kbps
5 Megas (5120KBps)	540 Kbps

Tabla 6.9 Tasa de transferencia.

Cada tipo de conexión utiliza diversos protocolos (PPP, TCP/IP, etc.) que utilizan entre un 2% y un 20% de la velocidad de conexión para establecer y mantener el propio enlace.

Es común denominar ancho de banda a la cantidad de datos que se pueden transmitir en una unidad de tiempo. Por ejemplo, una línea ADSL de 256 kbps puede, teóricamente, enviar 256000 bits por segundo. Esto es en realidad la tasa de transferencia máxima permitida, que depende del ancho de banda, de la potencia de la señal, de la potencia de ruido y de la codificación de canal.

Cada tipo de conexión tiene su propio ancho de banda y su tasa de transferencia máxima. El ancho de banda y la saturación de la red son dos factores que influyen directamente sobre la calidad de los enlaces.

Por ende el tiempo de transferencia de datos va a ser directamente proporcional al tipo de conexión que tenga, el cálculo es simple; el número de bytes transmitidos lo transformamos a bits, el ancho de banda útil lo transformamos a bps (bits por segundo) y finalmente dividimos los bits para los bits por segundo.

Para la realización de las pruebas se tomó en cuenta los siguientes escenarios con una conexión de 100 Mbps:

Escenario 1. Ingreso al sistema.

Tiempo: 2.6 seg

 # bits: 2888 bytes → 23104 bits

32 Kbps: 32000 bps

64 Kbps: 64000 bps

128 Kbps: 128000 bps

Cálculos:

t = 23104 / 32000 = 0.722 segundos.

t = 23104 / 64000 = 0.361 segundos.

t = 23104 / 128000 = 0.181 segundos.

# bits transmitidos 23104	**Ancho de banda teórico**		
	256 Kbps	**512 Kbps**	**1024 Kbps**
	Ancho de banda útil		
	32 Kbps	**64 Kbps**	**128 Kbps**
Tiempo (segundos)	0.722	0.361	0.181

Tabla 6.10 Tiempos Escenario 1 ingreso al sistema.

Escenario 2. Plantilla de rubros.

Tiempo: 5.2 seg

 # bits: 145499 bytes → 1163992 bits

32 Kbps: 32000 bps

64 Kbps: 64000 bps

128 Kbps: 128000 bps

Cálculos:

t = 1163992 / 32000 = 36.375 segundos.

t = 1163992 / 64000 = 18.187 segundos.

t = 1163992 / 128000 = 9.094 segundos.

# bits transmitidos 1163992	**Ancho de banda teórico**		
	256 Kbps	**512 Kbps**	**1024 Kbps**
	Ancho de banda útil		
	32 Kbps	**64 Kbps**	**128 Kbps**
Tiempo (segundos)	36.375	18.187	9.094

Tabla 6.11 Tiempos Escenario 2 plantilla rubros.

Escenario 3. Propuesta.

Tiempo: 9.4 seg

 # bits: 192216 bytes → 1537728 bits

32 Kbps: 32000 bps

64 Kbps: 64000 bps

128 Kbps: 128000 bps

Cálculos:

t = 1537728 / 32000 = 48.054 segundos.

t = 1537728 / 64000 = 24.027 segundos.

t = 1537728 / 128000 = 12.014 segundos.

# bits transmitidos 1537728	**Ancho de banda teórico**		
	256 Kbps	**512 Kbps**	**1024 Kbps**
	Ancho de banda útil		
	32 Kbps	**64 Kbps**	**128 Kbps**
Tiempo (segundos)	48.054	24.027	12.014

Tabla 6.12 Tiempos Escenario 3 propuesta.

Escenario 4. Reporte Entrega/Recepción Equipos y Maquinaría.

Tiempo: 10.1 seg

 # bits: 671246 bytes → 5369968 bits

32 Kbps: 32000 bps

64 Kbps: 64000 bps

128 Kbps: 128000 bps

Cálculos:

t = 5369968 / 32000 = 167.812 segundos → 2.796 minutos.

t = 5369968 / 64000 = 83.906 segundos → 1.398 minutos.

t = 5369968 / 32000 = 41.953 segundos.

# bits transmitidos 5369968	**Ancho de banda teórico**		
	256 Kbps	**512 Kbps**	**1024 Kbps**
	Ancho de banda útil		
	32 Kbps	**64 Kbps**	**128 Kbps**
Tiempo (segundos)	2.796 min	1.398 min	41.953

Tabla 6.13 Tiempos Escenario 4 reporte entrega/recepción equipos y maquinaría.

Conclusiones.

- Mediante OpenVPN podemos crear redes virtuales privadas seguras y a muy bajo costo, de hecho, el software usado es gratis y además open source, por lo que no pagamos por concepto de licencias de software, además de ser multiplataforma.
- El uso de los mecanismos de seguridad que se proveen permiten estar preparados frente a ataques del tipo DOS o escaneo de puertos en busca de vulnerabilidades, lo cual deja nuestra red bastante más segura.
- Además OpenVPN nos provee de un mecanismo muy simple tanto para generar pares de llave/certificado para clientes así como la revocación de los mismos.
- La sobrecarga causada por el software de VPN depende de la cantidad de datos de la organización y la codificación utilizada, es decir, cuanto mejor sea el cifrado que utiliza, mayor es la carga que va a producir.

Recomendaciones.

- Se recomienda usar un límite de 16 kbps, para una conexión DSL con un ancho de banda máximo de subida de 512KBits/s, estableciendo este límite, permite disponer casi de la mitad del ancho de banda para otros servicios.

- Se recomienda la asignación de un equipo con características básicas para el servidor VPN, ya que la distribución utilizada es liviana.

- Las políticas de seguridad fueron establecidas de manera diferenciada, a fin de que cubran aspectos específicos de la red (software, hardware, usuarios, etc.).

- Se recomienda cambiar frecuentemente la clave de acceso para la VPN para mantener la seguridad de la información de la empresa.

Bibliografía.

Libros.

Redes de Computadoras, TANENBAUM Andrew S, 2003, Cuarta edición, Pearson educación, Modelos de referencia.

Redes de Computadoras, TANENBAUM Andrew S, 2003, Cuarta edición, Pearson educación, Estandarización de redes.

Redes de Computadoras, TANENBAUM Andrew S, 2003, Cuarta edición, Pearson educación, Cuestiones de diseño en la capa de enlace de datos.

Redes de Computadoras, TANENBAUM Andrew S, 2003, Cuarta edición, Pearson educación, Ethernet.

Ingeniería de tráfico de telecomunicaciones, CARRION Hugo, Julio 2005, Carrión & Carrión Consultores, Trafico de Telecomunicaciones.

OpenVPN Building and Integrating Virtual Private Networks, FEILNER Markus**,** 2006, Packt Publishing, Learn how to build secure VPNs using this powerful Open Source application

Internet.

http://es.wikipedia.org/wiki/Red_de_computadoras, REDES DE COMPUTADORES, 17-07-09

http://members.xoom.com/peejhd/Dsl.html, DSL, 20-07-09

http://www.newedgenetworks.com, Redes, 20-07-09

http://www.uswest.com/products/data/dsl/fast_facts.html, DSL, 20-07-09

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/c600s/c675/c675inop/0467501.htm, DSL PRODUCTOS, 20-07-09

http://laurel.datsi.fi.upm.es/~rpons/openvpn_como/, OpenVPN COMO, 21-07-09

http://es.wikipedia.org/wiki/Data_Encryption_Standard, Data Encryption Standard, 21-07-09

http://www.teldat.es/docs/products/pdf/ancho_banda.pdf, Ancho de Banda, 21-07-09

Glosario de Términos.

ADSL.- Son las siglas de Asymmetric Digital Subscriber Line ("Línea de Suscripción Digital Asimétrica"). ADSL es un tipo de línea DSL. Consiste en una transmisión de datos digitales (la transmisión es analógica) apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando el alcance no supere los 5,5 km. medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

Broadcast.- Transmisión de un paquete que será recibido por todos los dispositivos en una red.

DSL.- Siglas de **Digital Subscriber Line**, "línea de suscripción digital" es un

término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica básica o conmutada.

FDDI.- Fiber Distributed Data Interface es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex. Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

FTP.- Sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

GNU/Linux.- Es uno de los términos empleados para referirse al sistema operativo libre similar a Unix que usualmente utiliza herramientas de sistema GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (Licencia Pública General de GNU) y otras licencias libres.

GPRS.- General Packet Radio Service o servicio general de paquetes vía radio es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes).

GSM.- El Sistema Global para las Comunicaciones Móviles (GSM, proviene de "Groupe Special Mobile") es un sistema estándar, completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital. Por

ser digital cualquier cliente de GSM puede conectarse a través de su teléfono con su computador y puede hacer, enviar y recibir mensajes por e-mail, faxes, navegar por Internet, acceso seguro a la red informática de una compañía (LAN/Intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el Servicio de Mensajes Cortos (SMS) o mensajes de texto.

GUI.- Sigla que denomina a los sistemas operativos o aplicaciones que despliegan una interfaz (o diálogo) gráfica con el usuario mediante una serie de recursos visuales, tales como ventanas, íconos, cajas de diálogo, botones, menús desplegables, etc. Se operan con el mouse, y tienen como objetivo simplificar y facilitar la tarea de los usuarios de computadoras.

HSDPA.- Alto-Speed Downlink Packet Access, es también conocido como de alta velocidad Protocolo de acceso de bajada. HSDPA es un protocolo para teléfonos móviles. Es una de tercera generación (3G) de alta velocidad de acceso de paquetes de tecnología diseñada para acelerar la capacidad de la red y tasa de transmisión de datos de teléfonos celulares.

HTTP.- El protocolo de transferencia de hipertexto (HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW).

HTTPS.- Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

IETF.- Grupo de Trabajo en Ingeniería de Internet es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

IPSEC.- abreviatura de Internet Protocol security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también

incluye protocolos para el establecimiento de claves de cifrado.

ISP.- Internet Service Provider es una empresa dedicada a conectar a Internet a los usuarios, o las distintas redes que tengan, y a dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrece servicios relacionados, como alojamiento web o registro de dominios, entre otros.

L2TP.- Layer 2 Tunneling Protocol fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F.

MAC.- Media Access Control (Control de acceso al medio). Identificador hexadecimal de 48 bits que corresponde de manera única a cualquier interfaz o dispositivo de red (routers, switch, tarjetas de red). Esto equivale a 2^48 direcciones posibles, cuya nomenclatura es XX:XX:XX:XX:XX:XX.

MD5.- Algoritmo de Resumen del Mensaje 5; es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

NAT.- Traducción de Dirección de Red, es 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.

NETBIOS.- "Network Basic Input/Output System", es, en sentido estricto, una especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

PCMCIA.- Personal Computer Memory Card International Association, una asociación Internacional centrada en el desarrollo de tarjetas de memoria para computadores personales que permiten añadir al computador nuevas funciones.

Existen muchos tipos de dispositivos disponibles en formato de tarjeta PCMCIA: módems, tarjeta de sonido, tarjeta de red.

POP3.- Protocolo de la oficina de correo en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en la Pila OSI.

PPP.- Conexión a Internet de acceso telefónico que utiliza el protocolo TCP/IP.

PPTP.- Es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

RDSI.- Tecnología que combina servicios de voz y datos digitales a través de la red en un solo medio, haciendo posible ofrecer a los clientes servicios digitales de datos así como conexiones de voz a través de un sólo "cable".

RSA.- Es un sistema criptográfico de clave pública desarrollado en 1977 por ingenieros estadounidenses. En la actualidad, RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

SHA.- Algoritmo de Hash Seguro es un sistema de funciones hash criptográficas relacionadas de la Agencia de Seguridad Nacional de los Estados Unidos y publicadas por el National Institute of Standards and Technology (NIST).

SMTP.- Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.).

SNMP.- Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su

crecimiento.

SSL/TLS.- Protocolo de Capa de Conexión Segura- (SSL) y Transport Layer Security -Seguridad de la Capa de Transporte- (TLS), su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

TACS.- Siglas de Total Access Communication System. Estándar británico para teléfonos móviles analógicos basado en el estándar americano AMPS.

TCP.- Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 - 1974 por Vint Cerf y Robert Kahn.

UDP.- User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

UMTS.- Sistema Universal de Telecomunicaciones, es una de las tecnologías usadas por los móviles de tercera generación (3G, también llamado W-CDMA), sucesora de GSM. Sucesora debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación.

VPN.- Red Privada Virtual, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

WIFI.- Siglas en inglés de Wireless Fidelity, es un sistema de envío de datos sobre redes computacionales que utiliza ondas de radio en lugar de cables, además es una marca de la Wi-Fi Alliance (anteriormente la WECA: Wireless Ethernet Compatibility Alliance), la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

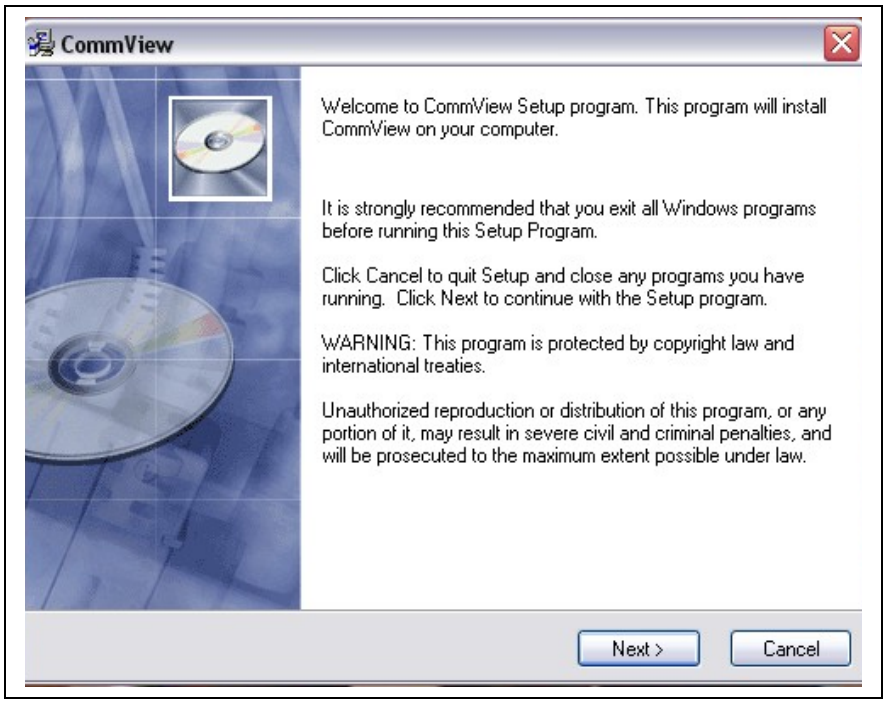
WIMAX.- Son las siglas de Worldwide Interoperability for Microwave Access

(interoperabilidad mundial para acceso por microondas). Es una norma de transmisión de datos usando ondas de radio.

ANEXOS

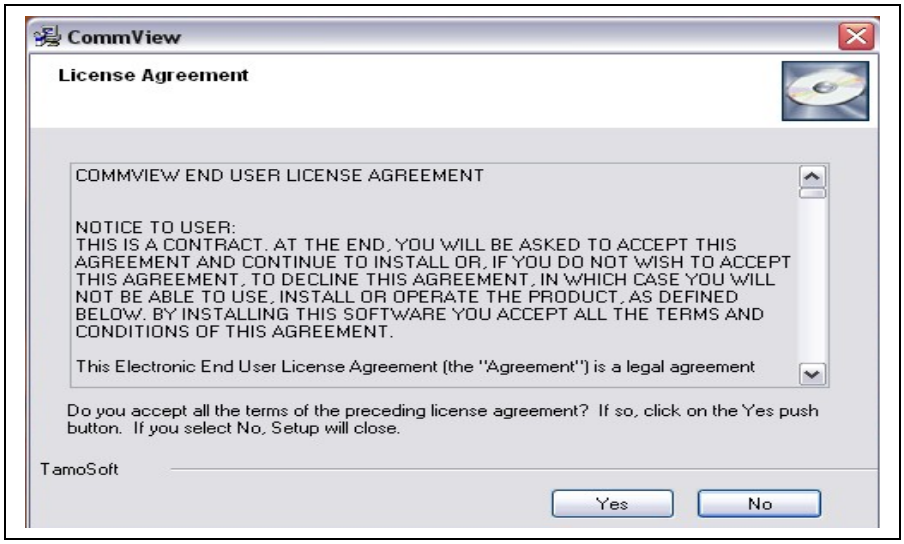
Anexo 1. Instalación CommView 6.

1 Damos doble click sobre el archivo ejecutable de la aplicación y se nos presenta la siguiente ventana:



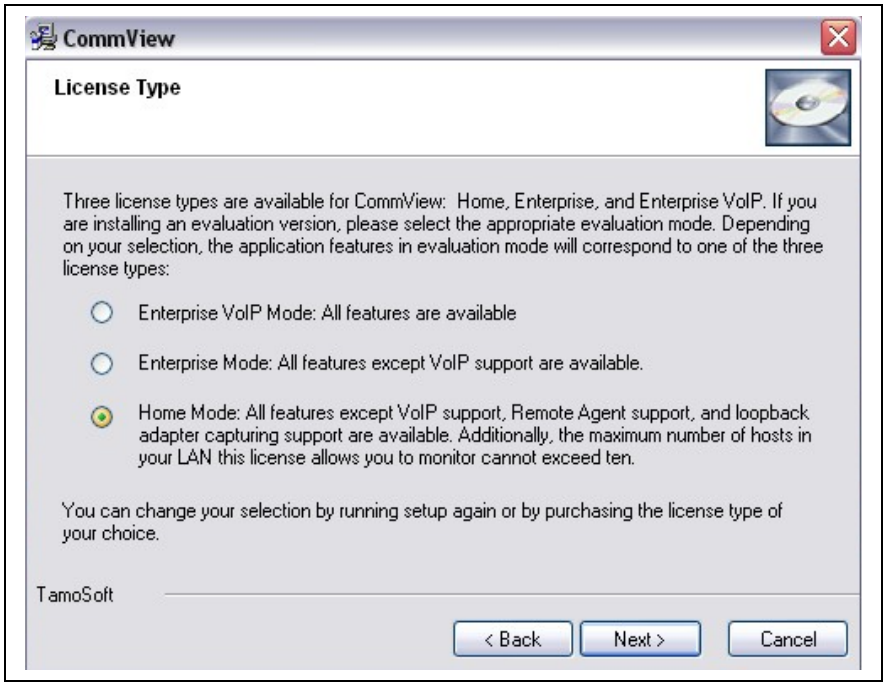
Inicio del asistente de instalación de CommView.

2 Presionamos en el botón “NEXT” y se nos despliega la siguiente ventana en la que está el acuerdo de licencia de nuestro CommView.



Acuerdo de licencia.

3 Presionamos “YES” y aparece la siguiente ventana en la que debemos escoger el tipo de licencia de nuestro CommView.

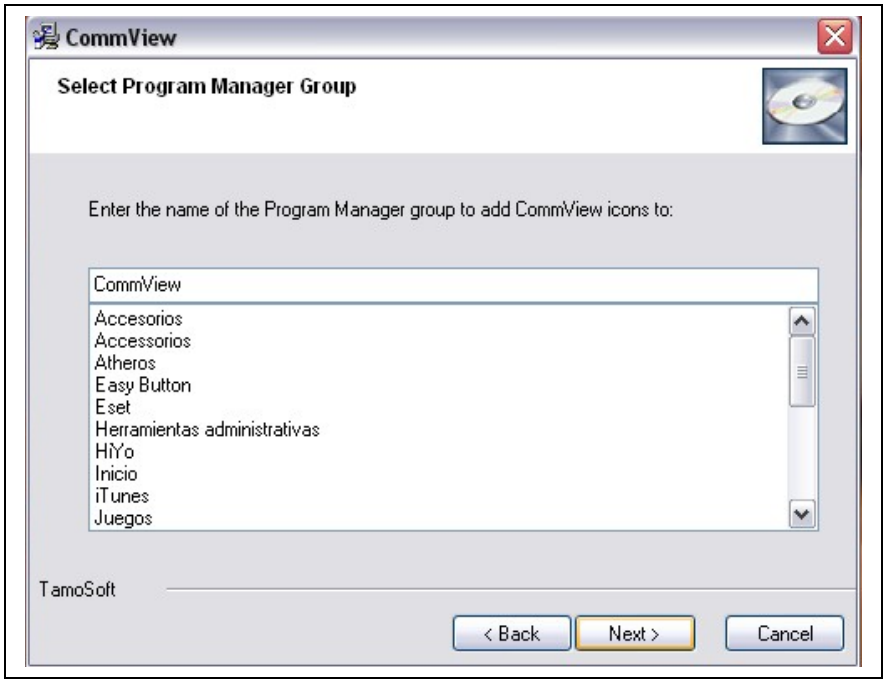


Selección del tipo de licencia.

4 Click en “NEXT” y se despliega la ventana en la cual no indica el path en el cual se va instala la aplicación.

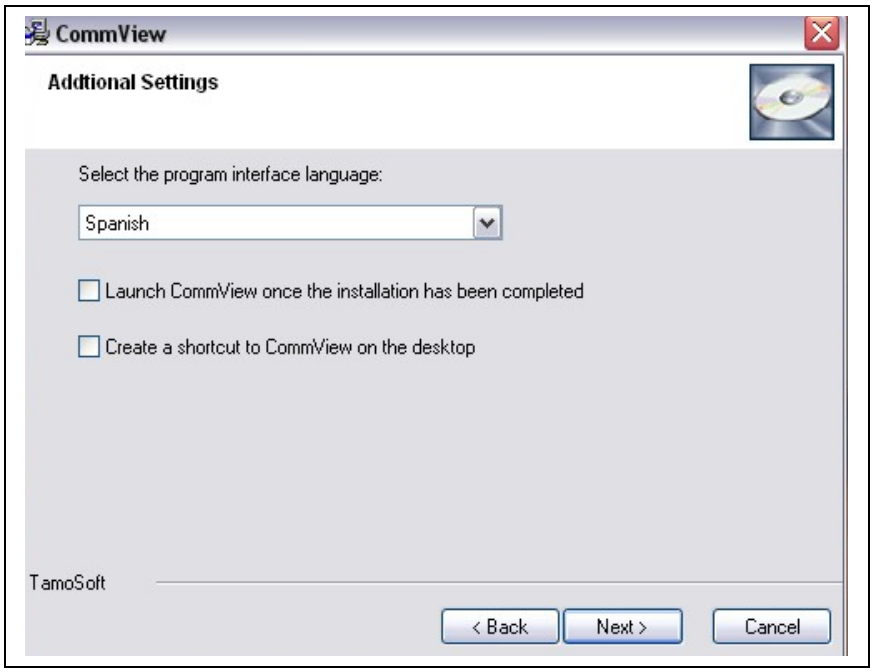
Path de la instalación.

5 Presionamos “NEXT” y aparece la ventana en la cual seleccionamos el nombre del administrador de grupo para el programa CommView.



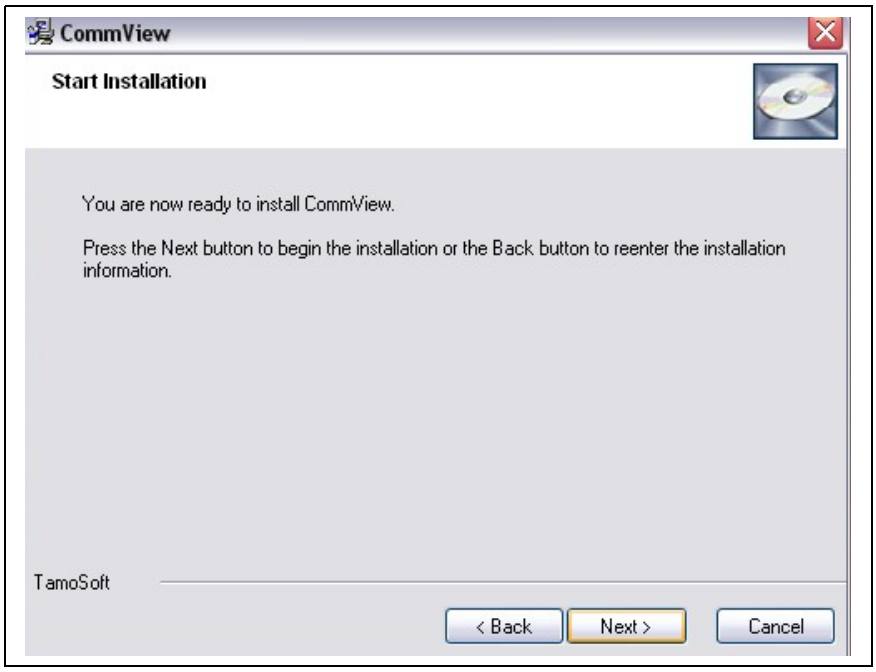
Selección administrador de grupo para el programa CommView.

6 Click en “Next” y se despliega la pantalla de configuraciones adicionales.



Selección del lenguaje de CommView.

7 Aquí seleccionamos el idioma de la interfaz del programa y presionamos "NEXT".

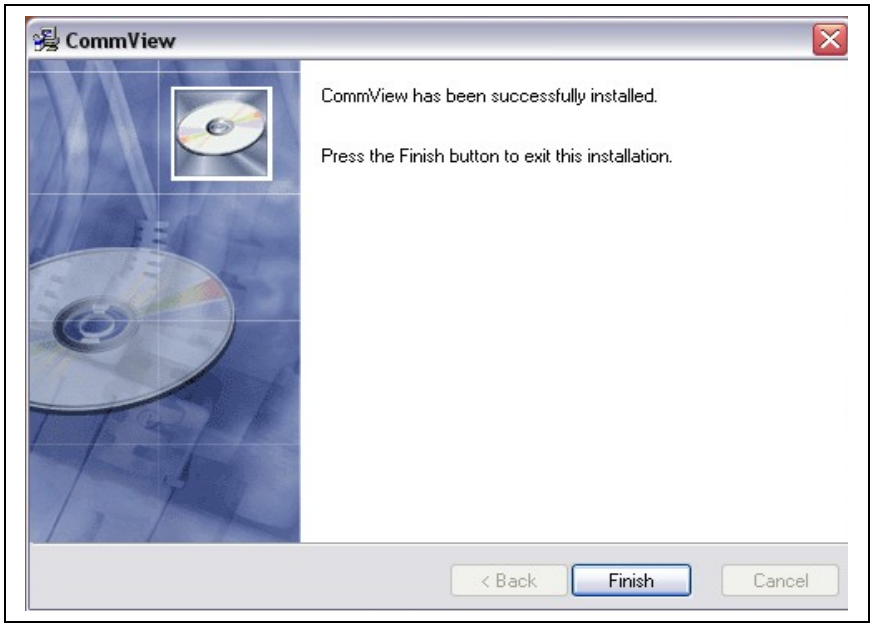


Ventana para iniciar la Instalación.

8 El asistente de instalación nos indica que estamos listos para instalar nuestro CommView y se despliega la ventana en la cual se puede observar el avance de la instalación.

Proceso de Instalación.

9 Finalmente aparece la siguiente ventana en la cual el asistente de instalación nos da a conocer que la instalación del programa ha ocurrido satisfactoriamente.

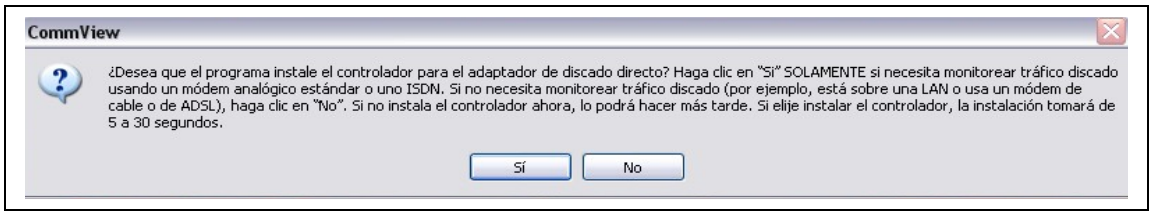


Finalización de la Instalación.

10 Presionamos “FINISH” para terminar la instalación.

La primera vez que se accede a la aplicación se nos despliega la siguiente ventana, en la cual nos pregunta si deseamos que el programa instale el controlador para el

adaptador de disco directo, solo si necesitamos monitorear el tráfico usando un módem analógico estándar o ISDN.



Ventana para instalación de disco directo.

11 Click en "YES" y estamos listos para utilizar nuestro CommView.

Anexo 2. Plan Internet corporativo empresa CNT.

PLANES TARIFARIOS

Tarifas FAST BOY

Tarifas ADSL CORPORATIVO

PLANES	INSCRIPCIÓN	COSTO
ADSL 128/64 Básico	$ 50,00	$ 49,90
ADSL 256/128 Básico	$ 50,00	$ 79,90
ADSL 512/256 Básico	$ 50,00	$ 99,90
ADSL 128/64 Premium	$ 100,00	$ 126,00

Estos planes no incluyen impuestos

NOTA: Tenemos Planes Corporativos que se ajustan a las necesidades de su empresa. Para mayor información comuníquese al 1-800-100-100 y usted recibirá información personalizada de nuestros asesores.

Anexo 3. Plan Internet corporativo empresa ASAPTEL S.A.

PLANES CORPORATIVOS

Nuestros planes de Internet Corporativo son servicios de conexión a Internet orientado a medianas y grandes empresas que requieren de una calidad garantizada de velocidad para publicar sus propios contenidos Web, y ubicar sus propios servidores de correo dentro de la empresa.

COSTOS CONEXIONES DEDICADAS SIMETRICAS ASAPTEL S.A.

PLAN CLEAR CHANNEL

- **Ancho de banda:** 64 kbps -> **Mensualidad:** $250,oo
- **Ancho de banda:** 96 kbps -> **Mensualidad:** $320,oo
- **Ancho de banda:** 128 kbps -> **Mensualidad:** $385,oo
- **Ancho de banda:** 256 kbps -> **Mensualidad:** $700,oo

COSTOS CONEXIONES DEDICADAS ASIMETRICAS ASAPTEL S.A

PLAN VSAT

- **Ancho de banda:** 256x192 kbps **Mensualidad:**$150,oo
- **Ancho de banda:** 384x256 kbps **Mensualidad:**$250,oo
- **Ancho de banda:** 512x384 kbps **Mensualidad:**$350,oo.

Estos precios incluyen iva.