UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO E IMPLEMENTACION DE ENLACES VPN PARA MEJORA DE OPERACIONES EN EMPRESA DISTRIBUIDORA PERUFARMA S.A.

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

CESAR OSWALDO CHARCAPE PIZARRO

PROMOCIÓN
1983 - I

LIMA – PERÚ
2006

Estudio e implementación de enlaces VPN para mejora de operaciones en empresa distribuidora Perufarma S.A.

Dedico este trabajo:

A mis queridos padres que son mi inspiración, ejemplo de lucha y sacrifico.
A mi esposa por su amor, compresión y apoyo incondicional en mi carrera.
A mis hijos Cesar y Claudia, los pilares de mi vida.

SUMARIO

El presente trabajo pretende describir la implementación de enlaces VPN para la empresa Perufarma S.A., bajo protocolo IPSec, que se ha convertido en uno de los estándares de esta industria.

En el Capítulo I se describe la problemática que origina la búsqueda de una solución a los continuos problemas de comunicación que existían entonces a nivel de las operaciones de la empresa.

En el Capítulo II se describe el estado inicial en el que se encontraba la red de comunicaciones de la empresa.

En el Capítulo III se establece el Marco Teórico, se explica brevemente conceptos de la Internet y Seguridad en Internet

En el Capítulo IV se expone el concepto de Redes Privadas Virtuales (VPN) y se describen su arquitectura y el concepto de tunelamiento.

En el Capítulo V se describen la seguridad en redes VPN: autenticación, cifrado, control de acceso así como las tecnologías existentes mas importantes.

En el Capítulo VI se describe el proceso de implementación de los enlaces VPN en Perufarma S.A., partiendo desde el análisis de las diversas opciones disponibles, pasando por la definición de los productos de hardware a adquirir, así como la implementación recomendada para los accesos dedicados a Internet en cada oficina (local o remota). Finalmente se detalla el proceso de implementación, describiendo las configuraciones y pruebas realizadas

INDICE

PRÓLOGO

El hombre se ha intentado comunicar con sus semejantes desde el inicio de los tiempos, mediante gráficos, señales, ruidos, gestos, etc. Desde aquel entonces, fue creando sus propias formas de comunicación, las cuales fueron desarrollando hasta llegar a nuestros tiempos, la era de las comunicaciones y avances tecnológicos. Es precisamente aquí donde se ha notado un avance vertiginoso durante los últimos años, llegando a lo que actualmente existe, la Internet.

El desarrollo tecnológico ha favorecido la globalización, cada vez es mucho mas necesario disponer de información exacta y actualizada de cualquier tema en el cual nos veamos inmersos, ya que las decisiones precisamente mejoran si se dispone de la información en el momento oportuno.

El desarrollo de las telecomunicaciones, constituye un punto fundamental en el desarrollo de la economía mundial. Perú no es ni puede ser ajeno a esta evolución tecnológica, de hecho, tratamos de seguirla obteniendo información especializada de diversos rubros, y tratando de aplicarla en nuestro medio.

El Perú ha tenido un marcado desarrollo durante los dos últimos años en materia de expansión y conocimiento de lo que ahora se conoce como la "red de redes", Internet. Estamos en una época en donde parte de la población ya puede acceder a tener un canal dedicado de acceso a Internet a un costo razonable, o incluso acceso vía telefónica (dial-up) con tarifas bajas, las cuales incluso pueden seguir reduciéndose dependiendo de la oferta y demanda del mercado.

Este desarrollo ha contribuido a facilitar la posibilidad de que las empresas, sean pequeñas, medianas o grandes, tiendan a utilizar la Internet como un medio de comunicación a través del cual pueden implementar redes corporativas a muy bajo costo, y con la seguridad y confiabilidad que antes solo podían brindar las empresas de telecomunicaciones a través de enlaces dedicados (***leased lines***) o de tipo Frame Relay.

En el informe se describe el proceso de implementación de enlaces VPN en la empresa distribuidora Perufarma S.A., proyecto que tuvo una duración aproximada de año y medio, debido a que se decidió implementar cada requerimiento en forma secuencial, reduciendo el impacto económico que podría haber implicado una adquisición conjunta de todos los bienes y servicios que finalmente componen nuestra actual red corporativa.

Aquí se ha tratado de demostrar que los puntos teóricos descritos acerca de los estándares de la industria tales como IPSec, PPTP, L2TP, 3DES, etc., que actualmente conforman la amplia lista de conceptos disponibles para la implementación de una red corporativa basada en VPN sobre Internet, pueden llegar a operar eficientemente y brindar una estabilidad en las comunicaciones que permiten "simular" una red WAN a muy bajo costo, solamente con el uso de los nuevos estándares tecnológicos y un medio público como es la Internet.

Los capítulos I y II tratan la problemática y estado inicial de la red de comunicaciones de la empresa Perufarma S.A., describen brevemente las limitaciones que padecían y la inestabilidad de operación. El capítulo III establece el marco teórico del proyecto, describe brevemente la Internet, su evolución y cambios hasta ser lo que hoy es, así como definiciones de seguridad de la información en medios públicos como Internet, en los cuales la transmisión de datos podría estar sujeta a diversos ataque que afectarían su privacidad y confiabilidad del enlace.

Los capítulos IV y V describen los conceptos de VPN, los esquemas de seguridad ahora disponibles así como la explicación del porque son aceptados como estándares que ofrecen precisamente mantener la privacidad y confiabilidad en la transmisión de datos usando medios públicos. Las tecnologías y protocolos esenciales usados en VPN son también descritos, con el fin de dejar claras las bases sobre las cuales se efectúa la implementación de los enlaces VPN en Perufarma S.A.

Finalmente, el capítulo VI trata de consolidar todo el desarrollo del proyecto, demostrando la afectividad de la implementación y describiendo los detalles en cada caso, con el fin de que se logre comprender que, si bien puede resultar un poco complicado entender los conceptos primordiales de las Redes Privadas Virtuales, ellos son esenciales para poder comprender la forma de operación que presentan los equipos y software involucrado en esta implementación, así como también poder llegar a determinar los eventuales problemas que podrían sucederse en implementaciones de este tipo.

Mi agradecimiento a los directivos de Perufarma S.A., por permitirme utilizar el presente proyecto como base de mi informe de suficiencia; fueron ellos quienes con la confianza que me brindaron permitieron que se lograra concluir con el presente proyecto de manera exitosa.

CAPITULO I
PROBLEMÁTICA

1.1. Introducción

Perufarma S.A. fue fundada el 4 de enero de 1971, con el propósito de distribuir en exclusividad los productos del Laboratorio farmacéutico **ABEEFE S.A**.

Hasta 1994, se podría definir a **Perufarma S.A.** básicamente como una distribuidora de productos farmacéuticos, pues a partir de 1995 se inicia una diversificación con nuevas líneas de distribución, inicialmente destinada al canal de boticas y farmacias.

A finales de 1997 con la fusión entre *Abeefe* y *Bristol-Myers Squibb* Perú, asumen la distribución exclusiva a nivel nacional de este nuevo laboratorio.

A mediados de 1998 se da un importante incremento en las líneas que distribuyen, con la incorporación de varias representaciones de vinos y licores de procedencias sud-americanas y europeas. Es así que se comienza a consolidar su presencia en autoservicios, licorerías, restaurantes, bares y discotecas.

En ese mismo año, y como consecuencia de la necesidad de llevar varios productos de ésta cartera a otros canales, como los de abarrotes, **Perufarma S.A.** empieza a incursionar en bodegas, tiendas de conveniencia en estaciones de servicio, mercados y mayoristas.

Hoy, **Perufarma S.A.** es proveedor de todas las cadenas de autoservicios y principales mayoristas y minoristas en todo el Perú, siempre manteniendo su posicionamiento como uno de los principales distribuidores de fármacos.

Debido a la diversidad de productos que ahora distribuye, y la necesidad de mantener operaciones en línea de parte de todo su personal de ventas con el fin de registrar pedidos de productos, consultas de estado de cuentas de clientes, estado de despacho de pedidos, y otras operaciones diarias, era notable la necesidad de crear una red de comunicaciones que permita sostener dichas operaciones día a día, con la mayor velocidad en tiempo de respuesta y la confiabilidad de la transmisión de datos. Al año 2003, algunas soluciones

habían logrado ser implementadas permitiendo mantener dichas operaciones a un ritmo sostenible, pero la necesidad de mejorarlas era evidente.

En ésta necesidad de mejorar las comunicaciones es donde se observa la posibilidad de utilizar un concepto ya bastante maduro y que permitiría la creación de una red de comunicaciones equivalente a una WAN, con el fin de mantener la conexión en línea de sus oficinas de provincias y otras oficinas remotas ubicadas en la ciudad de Lima. El concepto al cual nos referimos son las Redes Privadas Virtuales (*Virtual Private Network*).

El informe describe en detalle los pormenores de dicha implementación, indicando los motivos que nos conducen a tomarla como solución luego de haber evaluado otras opciones posibles.

1.2. Descripción de la problemática

La necesidad de intercambio de información es sumamente importante en cualquier empresa hoy en día, y garantizar que dicho intercambio se realice bajo las previsiones de seguridad y confiabilidad resulta sumamente crítico.

Perufarma S.A. no es ajena a esta necesidad, esencialmente si se toma en cuenta que el crecimiento y sostenimiento del liderazgo alcanzado en los últimos años depende mucho de la continua mejora en sus procesos internos, basándose principalmente en el uso de la tecnología disponible.

Es por esto que en los últimos años, la necesidad de mejorar el sistema de comunicaciones de la empresa se hizo latente, a fin de que permitiese que las operaciones a nivel nacional tuviesen un mejor desempeño y mucha mayor fluidez, así como lograr que el personal que labora en otras locaciones a nivel nacional se sintiese integrado al proceso diario de trabajo de la empresa en general.

1.2.1. El Sistema de pedidos de provincias

Al año 2003, **Perufarma S.A.** está conformada por dos oficinas ubicadas en la ciudad de Lima; la oficina principal ubicada en el cercado de Lima y una oficina sucursal ubicada en el distrito de San Isidro. Asimismo, varias otras oficinas en determinadas ciudades de provincias, tales como: Piura, Trujillo, Chiclayo, Arequipa, Huancayo, Cuzco, Iquitos. Todas ellas centralizaban las operaciones por zona, logrando llevar el seguimiento de las acciones de cada representante de ventas de la empresa, a nivel nacional. Cada oficina centralizaba las solicitudes de

pedidos recogidas por los agentes de ventas, así como también las cobranzas realizadas durante cada día. Las secretarias de cada oficina se encargaban del registro de los pedidos mediante una aplicación "hecha-en-casa" a la medida de la necesidad; esta aplicación basada en Microsoft Visual Basic tenía por denominación: "*Sistema de Pedidos de provincias*".

La forma de operación de éste sistema se basaba en que diariamente se debía preparar la información pertinente de carteras de clientes y ruta a seguir por cada agente de ventas en cada provincia, ya que se debía cubrir la zona esperada y completar las operaciones ya definidas por la Gerencia de Ventas. La preparación de dicha información estaba a cargo de una persona en particular, quien una vez completada esta información, la compactaba y copiaba hacia un directorio especial ubicado en un equipo ubicado en la sala de cómputo, en el cual se procesaban mensajes y comunicaciones con diversos usuarios, proveedores y/o clientes. La información así compactada, era enviada al sitio Web de la empresa, el cual se encuentra en modalidad de "hosting" en un conocido ISP; la información así preparada se enviaba hasta en tres oportunidades durante un día, ya que se trataba de mantener actualizados la parte de información de la Base de Datos que se les transmitía a cada provincia.

La información que se ubicaba en el sitio Web, era recogida por un proceso automatizado desde el "*Sistema de pedidos de provincia*" instalado en cada PC de las oficinas remotas, este proceso hacía el "download" del archivo correspondiente a determinada oficina y se procesaba actualizando la información de la pequeña base de datos MS Access que era pieza fundamental de este pequeño aplicativo. Con ésta información, se procesaban los pedidos en cada oficina y éstos eran enviados por el mismo aplicativo vía correo electrónico, a una casilla de correo en particular desde la cual se recopilaban todos los pedidos que llegaban y se insertaban en la Base de Datos central de la empresa. Luego de completar este ciclo, y una vez insertado el pedido, se enviaba un mensaje indicando "pedido procesado", el cual llegaba directamente al vendedor vía su celular (o RPM) y a la casilla de correo de la secretaria de la oficina en cuestión.

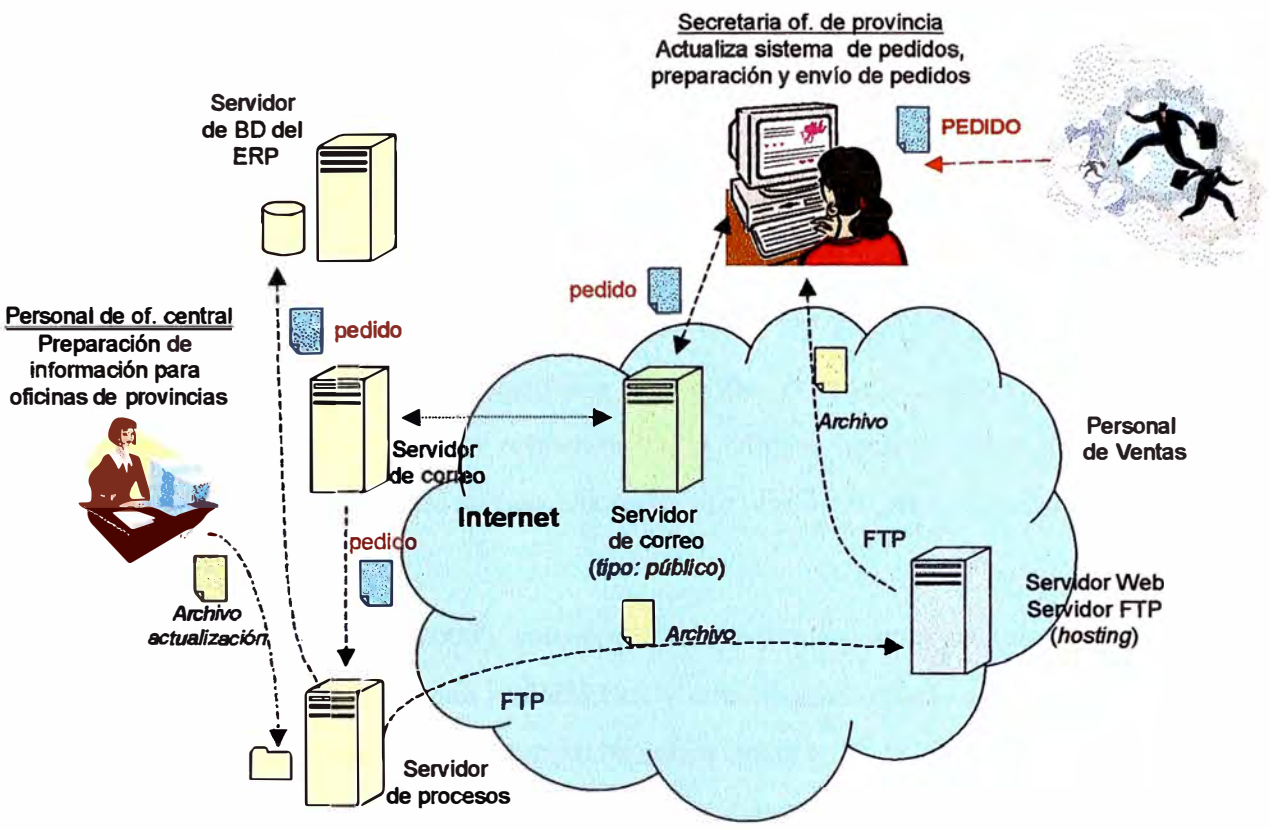

Fig. 1.1. Diagrama funcional del Sistema de Pedidos de provincia

Como se puede apreciar, si bien el proceso resultaba funcionalmente aceptable, presentaba ciertas complicaciones mayormente por los imprevistos que se sucedían:

- La preparación de la información de "ruteros" y "carteras" para cada oficina remota tomaba cierto tiempo, y obligaba a que una persona estuviese dedicada a ello casi permanentemente.
- En varias ocasiones, y debido a que los errores de operador se suelen producir, la información de ruteros y carteras resultaba con errores, no se lograba actualizar correctamente.
- En algunos casos, el archivo que se bajaba de Internet en la oficina de provincia correspondiente, podía resultar corrupto, imposibilitando el hecho de actualizar el Sistema de pedidos en dicha oficina.
- En los casos donde la información no llegaba a las oficinas remotas, éstas no podían completar sus labores adecuadamente y según lo ya programado por sus Supervisores y/o Jefaturas de Ventas.

- El no tener la información actualizada y disponible, obligaba a que los pedidos sean registrados por cada oficina por vía telefónica, efectuando llamadas de Discado Directo Nacional a fin de contactar a una de las Televendedoras de la oficina central e ir pasando los pedidos uno por uno para que sean registrados en el sistema. En su defecto, usaban el correo electrónico con el consiguiente peligro de retraso en los despachos y entrega del pedido al cliente.
- Otro problema que se presentaba a menudo, eran los procesos de liquidaciones y cobros que debían ser reportados a la oficina central. Estas liquidaciones se hacían mediante el mismo *Sistema de Pedidos de provincias* o por vía telefónica.

En aquella época (año 2003), solo dos oficinas de provincia contaban con conexión a Internet dedicado, por vía inalámbrica y con un ancho de banda bastante discreto, 32Kbps. El ISP contratado garantizaba sobre estos enlaces solo el 30% del ancho de banda, lo que permitía al menos ganar conexión hacia la oficina central vía servicios de Terminal Server, implementados en un equipo PC con sistema operativo Windows 2000 Server. En este servidor se había implementado perfiles para un usuario por provincia que les permitían el acceso al sistema ERP central, pudiendo registrar sus pedidos y preparar sus liquidaciones directamente. Estas dos oficinas solo utilizaban el "*Sistema de Pedidos de provincias*" en caso no pudiesen trabajar con el servidor de Terminales, mayormente por problemas de transmisión debido a saturación del enlace.

Otras oficinas de provincias: Cuzco, Huancayo, Arequipa, Piura e Iquitos, solo podían tener acceso a Internet vía telefónica. Ellas solo podían utilizar el "*Sistema de pedidos de provincias*"

1.2.2. Objetivos generales

Dentro de los objetivos generales que se contemplaron en el presente proyecto, se tuvo los siguientes:

- Examinar los problemas de comunicaciones y rediseñar la red de comunicaciones de la empresa con el fin de lograr la interconexión de todas o la mayoría de sus oficinas a nivel nacional
- Garantizar que el intercambio de datos se realice de manera fluida, manteniendo la privacidad de la transmisión de la información.

- Permitir el acceso a más de un recurso centralizado en la empresa, siempre que esto sea posible de acuerdo a las políticas internas de la misma.
- Realizar la evaluación del costo-beneficio que este cambio involucra, evaluando todas las alternativas tecnológicas disponibles.

CAPITULO II
ESTADO INICIAL

2.1. La red de comunicaciones

Perufarma S.A. contaba ya con una red de comunicaciones que fue creciendo sin un diseño previo, básicamente según las necesidades que se presentaban en aquella época. En este capítulo se presentará una breve reseña del estado de la red de comunicaciones al año 2004.

2.1.1. Topología de red

La red de datos de Perufarma S.A. estaba basada en una red LAN ubicada en el local central, localizado en el Cercado de Lima. Esta red LAN configurada en base a topología estrella, con conmutadores (switches) y concentradores (hubs) 100BASE-T de marca 3Com, permitían la operación de aproximadamente 180 estaciones de trabajo en dicho local. Un grupo de aproximadamente nueve servidores, que albergaban diversos aplicativos, recursos y servicios, permitían compartir y procesar la información del negocio en la red LAN.

Perufarma S.A. contaba desde aquel entonces con un Sistema ERP (*Enterprise Resource Planning*) centralizado en la oficina principal. Las suite ERP son arquitecturas de software que facilitan el flujo de información entre las funciones de manufactura, logística, finanzas, recursos humanos y otros, dentro de una empresa, el sistema ERP que utiliza Perufarma, contiene diversos módulos que fueron implementados en el año 2000, con la finalidad de mejorar la información y planeación de los procesos de negocio. Dicho ERP, está implementado en un servidor IBM RISC RS/6000, con almacenamiento externo de disco basado en tecnología SSA (*Serial Storage Architecture*)

Asimismo, y tal como se explica en el capítulo anterior, contaba con una aplicación hecha a medida, basada en *Microsoft Visual Basic*, la cual tenía por nombre "*Sistema de Pedidos de provincias*".

El acceso a Internet en la oficina principal estaba conformado por un enlace dedicado de 256 Kbps, simétrico, provisto por uno de los principales ISP (*Internet Service Provider*) de Lima.

Una oficina sucursal en Lima se ubica el distrito de San Isidro, en ella cerca de 15 usuarios trabajan esencialmente en el marketing de ciertos productos. En dicha oficina, una pequeña red LAN basada en configuración estrella 100BASE-T soportaba el trabajo diario.

Para los usuarios de la oficina sucursal de San Isidro, la única forma de acceder al sistema ERP centralizado, ubicado en la oficina principal, era mediante conexiones hacia un Servidor de Terminales implementado en el local central, basado en sistema operativo *Microsoft Windows 2000 Server*. En la oficina de San Isidro se contaba con conexión dedicada hacia Internet mediante un enlace *Speedy Business* ADSL , de 512 / 128 Kbps

Asimismo, Perufarma S.A. contaba con oficinas en algunas provincias, entre las cuales se encuentran:

- Oficina de la ciudad de Piura
- Oficina de la ciudad de Arequipa
- Oficina de la ciudad de Huancayo
- Oficina de la ciudad del Cuzco
- Oficina de la ciudad de Iquitos,

Todas ellas tenían conexión a Internet por vía telefónica, vía los servicios de ISP de *Telefónica del Perú*.

Las oficinas de las provincias de Trujillo y Chiclayo contaban con acceso a Internet dedicado, vía enlace inalámbrico, provisto por la empresa Millicom. Dichos enlaces eran desde ya bastante discretos, el ancho de banda era de 32 Kbps, y del cual el proveedor solo garantizaba el 30%.

El Servidor de Terminales configurado en base al sistema operativo *Microsoft Windows 2000 Server*, ejercía también la labor de VPN Server, ya que se buscaba proteger la transmisión de datos en base a este concepto. La funcionalidad que brindaba esta solución permitía un mínimo de operatividad al menos con la oficina de San Isidro, y las oficinas de las ciudades de Trujillo y Chiclayo, a pesar de algunos problemas frecuentes que se eran experimentados por los usuarios de éstas locaciones.

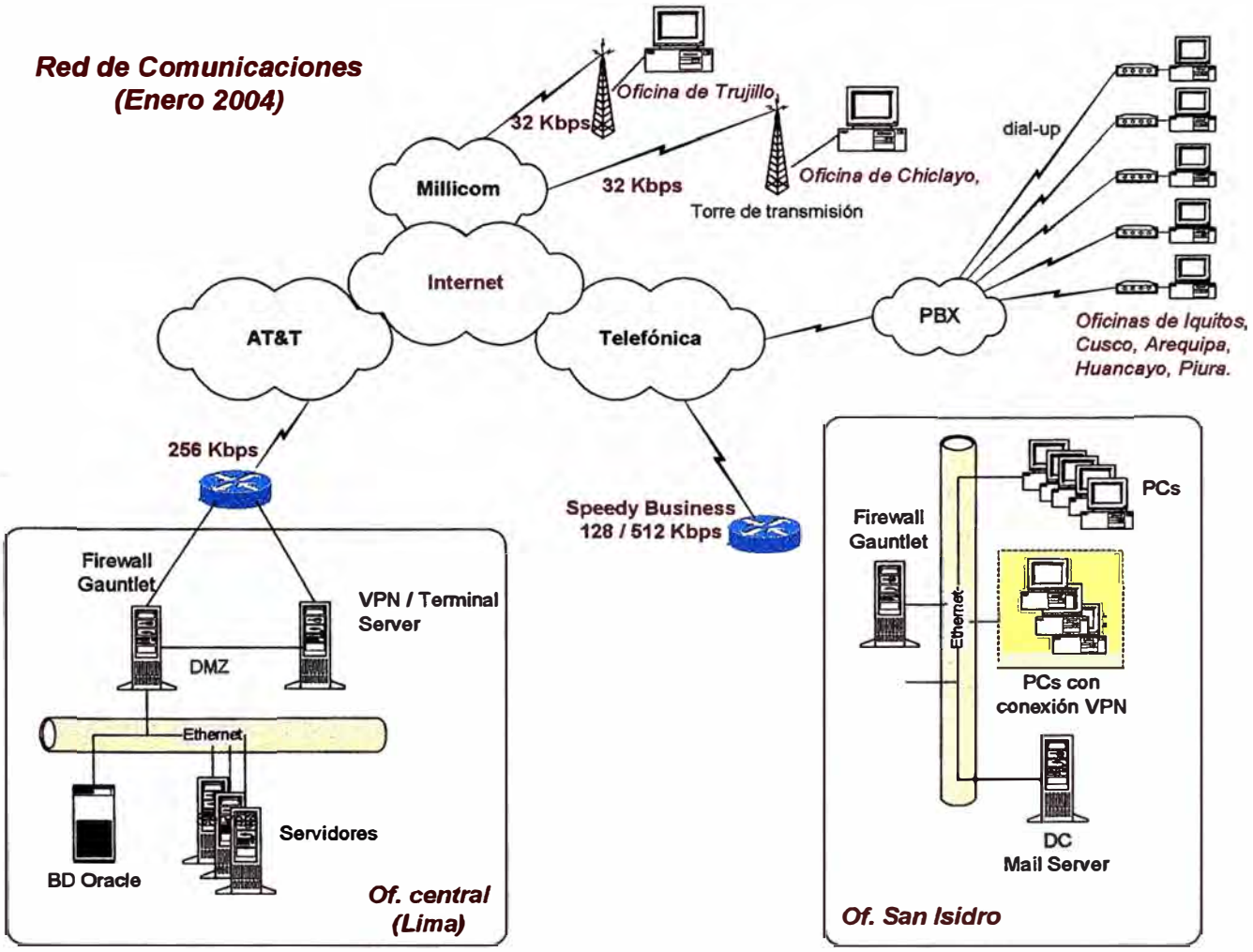

Fig. 2.1.: Red de comunicaciones de Perufarma S.A. en el 2004

Los enlaces VPN basados en protocolo PPTP que se habían implementado son mostrados en la Figura 2.2.

Los enlaces VPN se muestran en líneas punteadas. Se trataba de enlaces VPN basados en protocolo PPTP, el cual se autentificaba únicamente bajo el esquema de seguridad de Windows. Este tipo de enlace no representaba la mejor opción en

materia de seguridad, pero era el que había sido implementado el 2002 por personal externo a la empresa.

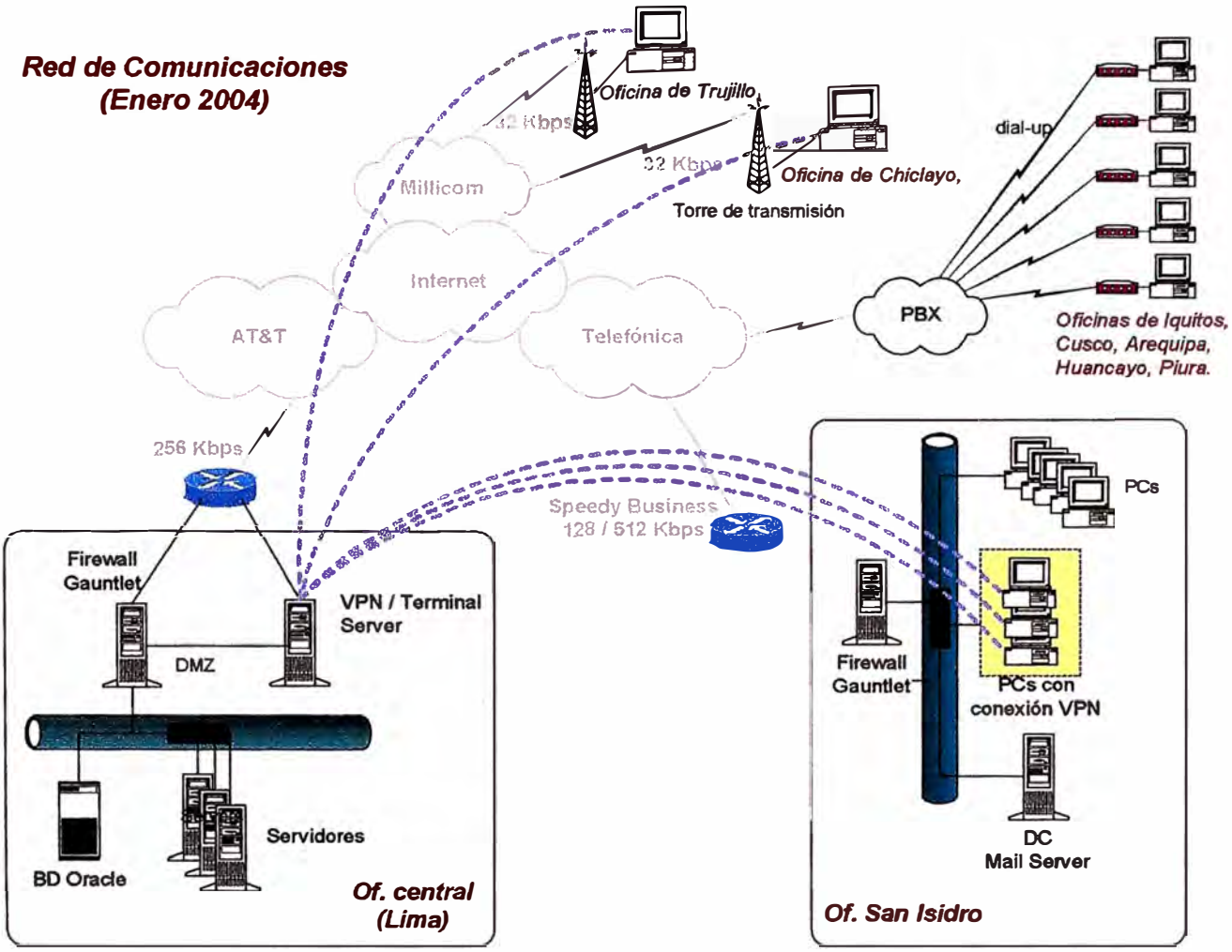

Fig. 2.2.: Enlaces VPN basados en PPTP

Estos enlaces se activaban según el usuario lo requiriese, no se trataba de enlaces permanentes sino se realizaban solo cuando el usuario requería utilizar el sistema ERP de la oficina central

2.1.2. Arquitectura de red

La arquitectura de red para su estado inicial, era la siguiente:

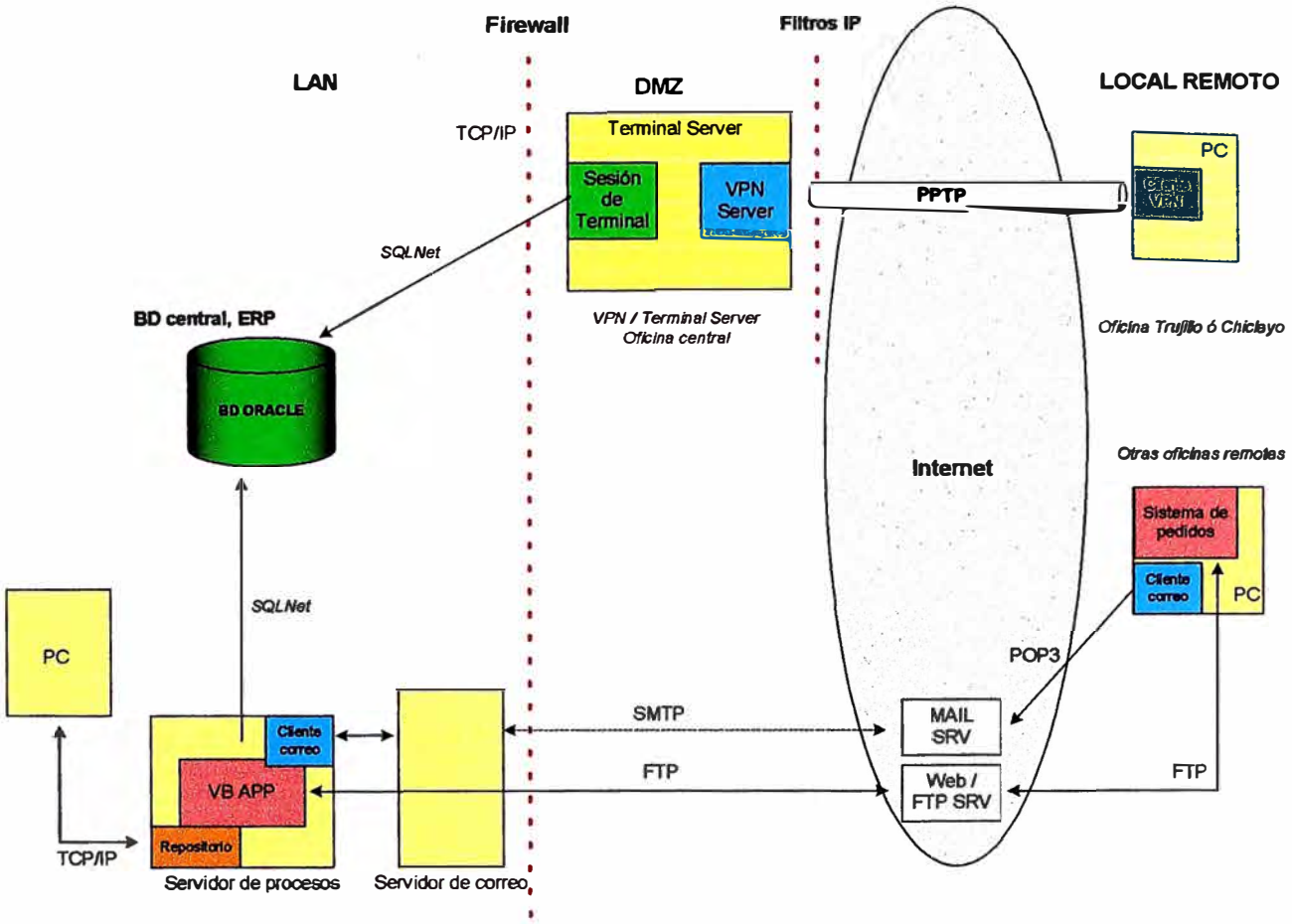

Fig. 2.3.: Arquitectura de red Perufarma (2004)

2.2. Requerimientos del negocio

Toda empresa de pequeña, mediana o de gran envergadura hoy en día requiere aplicar de la mejor manera posible el uso de la tecnología existente; con el fin de lograr llegar a sus clientes donde quiera que estos se ubiquen.

Perufarma S.A. no es ajeno a esto, y por ello resultaba sumamente importante examinar las opciones disponibles con el fin de establecer interconexiones de red entre sus oficinas a nivel nacional. Tal como se explicó en el primer capítulo, el uso de aplicaciones hechas a medida, y la implementación de enlaces básicos VPN a través de Internet, solucionaba parcialmente la necesidad de intercambio de información entre las distintas locaciones, así como un acceso indirecto a parte de la información centralizada que se manejaba en la oficina principal, en Lima.

Por otro lado, resultaba necesaria la integración entre las oficinas remotas con la oficina central, lo que apuntaba a buscar una solución equivalente a la creación de una red WAN a nivel nacional.

CAPITULO III
MARCO TEÓRICO

3.1. Internet: la red de redes

Lo que se conoce hoy como Internet es en realidad un conjunto de redes independientes (de área local y área extensa) que se encuentran conectadas entre sí, permitiendo el intercambio de datos y constituyendo por lo tanto una red mundial que resulta el medio idóneo para el intercambio de información, distribución de datos de todo tipo e interacción personal entre usuarios.

3.1.1. Breve historia

Empezó en los Estados Unidos de América en 1969, como un proyecto puramente militar. En la época de la guerra fría, la tecnología en cuanto a ordenadores no era muy avanzada, y para poder aprovechar los recursos informáticos al máximo y distribuirlos (porque entonces los ordenadores eran muy caros) se pensó en compartirlos, es decir, conectarlos físicamente. ARPA (Agencia de Proyectos de Investigación Avanzados - del Departamento de Defensa) conectó a principio de los sesenta unas cuantas universidades y un instituto que investigaban para ARPA, creando lo que se llamó ARPAnet.

Además de compartir los gastos militares, la ARPAnet era un experimento que funcionaba sobre el mismo principio que las autopistas interestatales norteamericanas. Estas enormes autopistas, al igual que la ARPAnet, tenían una doble utilidad: la de uso público y la de transporte de material militar pesado (en el caso de la ARPAnet el transporte sería de información científica y de información militar clasificada). En caso de un ataque nuclear directo (sobre territorio norteamericano) deberían sobrevivir, es decir que el flujo no se debería interrumpir, aún cuando se eliminasen poblaciones enteras. Además, las rutas en cualquier caso deberían ser seguras. Esto se traducía en dos ideas:

- No podía existir un control central (cuartel general), ya que si éste era eliminado la red quedaría destruida inmediatamente.
- No se podía conocer el camino que iba a tomar el flujo de material (información) ya que de conocerse de antemano se podría destruir fácilmente.

ARPAnet se desarrolló, y como los militares observaron que funcionaba, y como querían una red propia (y no mezclada con los investigadores), ARPAnet se dividió en dos en la década de los `80, convirtiéndose en la ARPAnet, dedicada a la investigación, y la MIlnet, dedicada a los temas militares.

Cabe mencionar que además de la ARPAnet, coexistían otras redes importantes por su tamaño, como la BITNET (la ``Because It's Time" network, la red ``Porque Ya Era Hora"), que conectaba centros de investigación con máquinas IBM, y la USENET (User's Net, Red de los Usuarios), que empezó como un proyecto de dos estudiantes que querían conectar algunos ordenadores que funcionaban en Unix, y que ahora cuenta con unos cientos de miles.

El siguiente paso importante para el desarrollo de la Internet fue la creación en 1986 de la NSFNET (National Science Foundation Network, Red de la Fundación Nacional de Ciencia), cuyo fin era conectar las supercomputadoras norteamericanas. Fue una gran idea ya que se podían incluir a los investigadores de todas partes para que los gastos de desplazamiento no fuesen tan grandes. Tuvo tanto éxito que en 1990 suplantó a la ARPAnet, la cual fue desmantelada. En 1991, el entonces senador Al Gore usó la NSFNET para construir sobre ella la NREN (National Research and Education Network, Red Nacional de Investigación y Educación), incluyendo colegios, bibliotecas e institutos de bachillerato.
Hoy en día la NREN coexiste con muchas otras redes (además de la BITNET y USENET), dentro y fuera de norteamérica, y cada vez se van sumando más redes. la mayoría de carácter comercial, es decir, pertenecientes a empresas.

3.1.2. Funcionamiento

El fundamento de Internet es el TCP/IP, un protocolo de transmisión de datos que asigna a cada máquina que se conecta un número específico, llamado dirección IP (que actúa a modo de "número teléfono único") como por ejemplo 192.555.26.11.

El protocolo TCP/IP sirve para establecer una comunicación entre dos puntos remotos mediante el envío de información en paquetes. Al transmitir un mensaje o

una página con imágenes por ejemplo, el bloque completo de datos se divide en pequeños bloques que viajan de un punto a otro de la red, entre dos números IP determinados, siguiendo cualquiera de las posibles rutas. La información viaja por muchos nodos intermedios a modo de repetidores hasta alcanzar su destino, lugar en el que todos los paquetes se reúnen, reordenan y convierten en la información original. Millones de comunicaciones se establecen entre puntos distintos cada día, pasando por cientos de nodos intermedios.

La ventaja del protocolo TCP/IP es que es un protocolo "inteligente". Como cada intercambio de datos está marcado con números IP determinados, las comunicaciones no tienen por qué cruzarse. Y si los paquetes no encuentran una ruta directa, los nodos intermedios prueban vías alternativas. Se realizan comprobaciones en cada bloque para que la información llegue intacta, y en caso de que se pierda alguno, el protocolo lo solicita de nuevo hasta que se obtiene la información completa.

TCP/IP es la base de todas las máquinas y software sobre el que funciona Internet: los programas de correo electrónico, transferencia de archivos y transmisión de páginas con texto e imágenes y enlaces de hipertexto. Servicios como DNS convierten direcciones IP en nombres mas inteligibles para su fácil recordación.

Toda Internet funciona a través de TCP/IP, y razones históricas hacen que está muy ligado al sistema operativo Unix (y sus variantes).

3.2. Seguridad en Internet

3.2.1. El problema de los medios de transmisión públicos

Desde que Internet es un medio público de comunicación, como todo medio de ésta índole presenta riesgos a quienes, por razones laborales o personales, debemos utilizar este medio de comunicación.

Los eventos mas comunes son los ataques de "hackers" o "crackers" a los sistemas de gobierno o de empresas comerciales, robo de claves de acceso a tarjetas de crédito, envíos de correos electrónicos maliciosos, etc. El desarrollo que ha tenido Internet durante estos últimos años ha venido de la mano con la diversidad de formas que estos hackers y crackers tiene para cometer sus delitos.

Hay varias organizaciones dedicadas a examinar y evaluar este tema, proponiendo medidas de seguridad que permitan reducir lo mas posible el riesgo existente, a fin de que los usuarios podamos utilizar este excelente medio de comunicación.

3.2.2. Amenazas a la seguridad de la información

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo) [REF 1]. La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las cuatro categorías generales de amenazas o ataques se muestran en la figura 3.1:

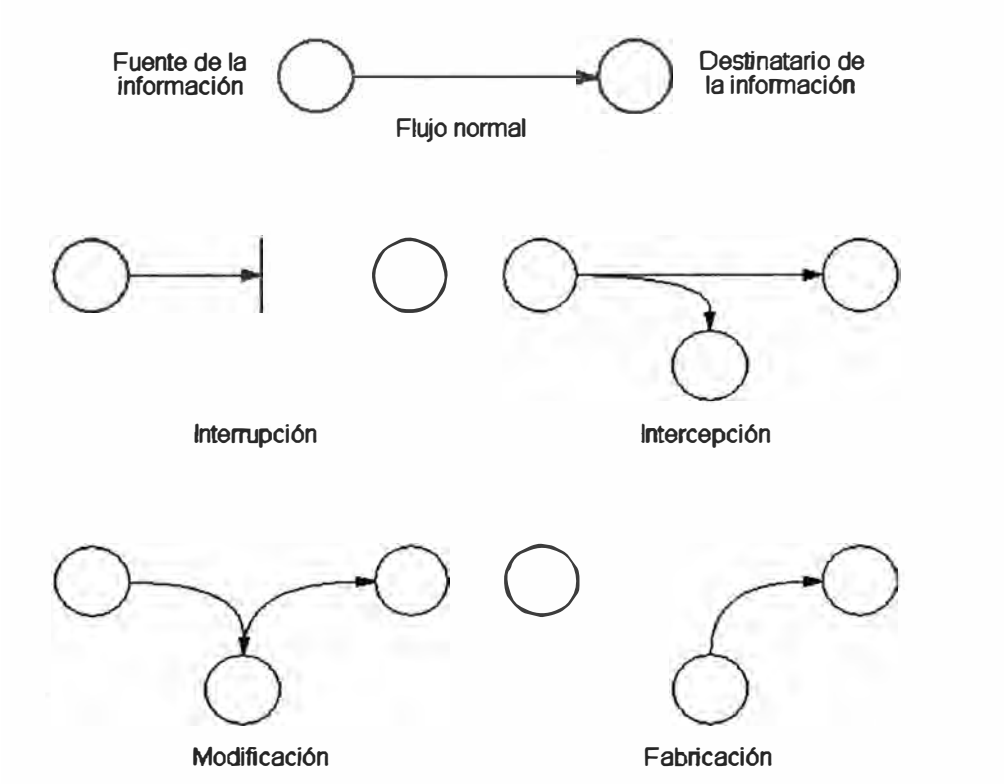

Fig. 3.1.: Categorías generales de ataques o amenazas.

- **Interrupción**: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la **disponibilidad**. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

- **Intercepción**: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la **confidencialidad**. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son, conectarse s una línea para capturar los datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para averiguar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).
- **Modificación**: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la **integridad**. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación**: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la **autenticidad**. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

a) Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza (***sniffing***), para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

b) Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad (*spoofing*)**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de

ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

- **Reactuación**: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado.
- **Modificación de mensajes**: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
- **Degradación fraudulenta del servicio**: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Entre estos ataques se encuentran los de **denegación de servicio**, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

3.2.3. Aspectos fundamentales de seguridad de la información

Para hacer frente a las amenazas a la seguridad se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente:

a) Confidencialidad

Requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado.

b) Autenticación

Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.

c) Integridad

Requiere que la información sólo pueda ser modificada por las entidades autorizadas.

d) Disponibilidad

Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten

3.2.4. Mecanismos de seguridad

No existe un único mecanismo capaz de proveer todos los aspectos anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes:

- **Autenticación**: corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser.

- **Cifrado**: garantiza que la información no es inteligible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto legible mediante un proceso de cifrado en un texto no legible, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

- **Control de acceso,** permite que solo los usuarios a quienes se les haya permitido el acceso a determinado recurso o sistema, puedan acceder a él. Esto

se logra mediante la autenticación del usuario y configuraciones de políticas de acceso.

3.3. Resumen del capítulo

En este capítulo se describe el marco teórico del medio de comunicaciones que se usará en el desarrollo del proyecto: Internet

Se describe conceptos básicos, breve reseña histórica de su nacimiento y progresos hasta la fecha, así como el protocolo de comunicaciones sobre el cual se soporta. Asimismo, se describe los aspectos a tomar en cuenta respecto de la seguridad de la información en un medio público, como es Internet.

CAPITULO IV
REDES PRIVADAS VIRTUALES

4.1. La Red Privada Virtual (*VPN*): breve historia

Red Privada Virtual, más conocida por su nombre en inglés: ***Virtual Private Network (VPN)***, resulta ser uno de las opciones de interconexión de redes mas utilizada hoy en día por empresas de pequeña, mediana y gran envergadura.

El término ha sido asociado en el pasado con otros servicios de conexión remota, tales como la Red Pública de Telefonía y los circuitos privados virtuales de Frame Relay, pero finalmente ha sido asociado como un sinónimo de interconexión de redes basado en protocolo IP. Antes de ello, las grandes corporaciones gastaban considerables recursos para configurar complejas redes privadas, ahora mas conocidas como **Intranets**. Esas redes fueron instaladas utilizando costosos servicios de líneas dedicadas, Frame Relay o ATM para incorporar usuarios remotos Para oficinas pequeñas y usuarios móviles las compañías implementaban servidores de acceso remoto o enlaces ISDN. Asimismo, las pequeñas y medianas empresas, que no podían solventar esos tremendos costos, fueron relegadas a utilizar los servicios de líneas conmutadas, las cuales tienen como mayor problema su baja velocidad.

A medida que Internet llegó a ser más y más accesible y sus capacidades de ancho de banda se incrementaron, las empresas empezaron a descargar sus Intranets hacia sitios Webs y crear lo que ahora conocemos con el nombre de **Extranet,** que interconecta usuarios internos y externos. Sin embargo, si como es una buena opción costo-beneficio y tiene una implementación relativamente rápida, hay un problema fundamental: la seguridad.

Hoy en día, las soluciones para Redes Privadas Virtuales han avanzado mucho para resolver este factor de seguridad. Actualmente se usan protocolos de tunelamiento y complejos procedimientos de encriptación, la integridad y privacidad de la transmisión de datos se obtiene gracias a que estos protocolos equivalen a un enlace de tipo línea dedicada

punto a punto, y debido a que estas operaciones ocurren sobre una red pública, los costos de implementación de VPN resultan mucho mas bajos que la implementación de una línea dedicada equivalente.

Usando la Internet, las empresas pueden conectar sus oficinas remotas, socios de negocios, clientes hacia la red corporativa. Los usuarios móviles y trabajadores que puedan estar de viaje pueden lograr acceso seguro a los recursos de la red corporativa.

4.2. Arquitecturas VPN

El éxito en la implementación de una VPN depende de una adecuada elección de la tecnología y del escenario, siempre acordes a las necesidades que se tengan. La tecnología implica: técnicas de tunelamiento, autenticación, control de acceso, y seguridad de los datos; y los escenarios que se pueden construir son: Intranet VPN (LAN-to-LAN VPN), Acceso Remoto VPN y Extranet VPN.

4.2.1. Intranet VPN (LAN-to-LAN VPN):

En este escenario, varias redes remotas de una misma corporación son interconectadas utilizando medios de enlace público. Esto permite unir las redes convirtiéndolas en una sola red LAN corporativa, como si estuviesen interconectadas vía líneas dedicadas.

Tradicionalmente, para conectar dos o más oficinas remotas de una misma compañía se han necesitado contratar enlaces dedicados, por ejemplo, Circuitos Virtuales Permanentes (PVCs) Frame Relay. Se pueden adoptar diversas topologías de red para establecer los enlaces entre las redes de una empresa: Enlaces punto-a-punto, de estrella, de malla parcial y de malla completa. **Las figuras 4.1, 4.2, 4.3 y 4.4 d**etallan cada una de las topologías anteriormente mencionadas.

Fig. 4.1.: Enlace punto a punto

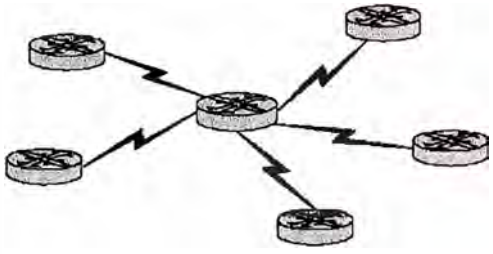

Fig. 4.2.: Enlace tipo estrella

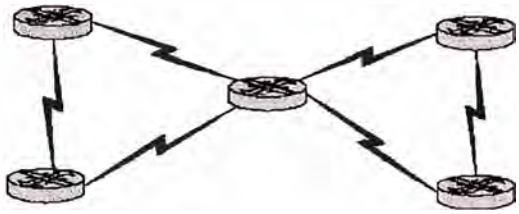

Fig. 4.3.: Enlace malla parcial

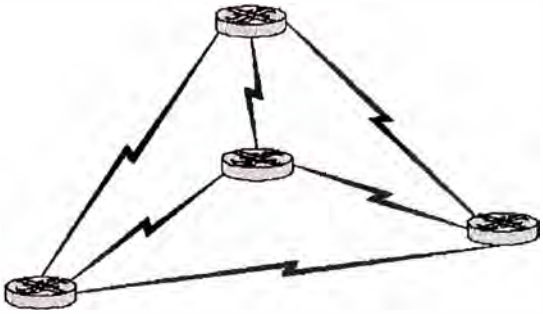

Fig. 4.4.: Enlace malla completa

La figura 4.5. muestra la conexión de tres oficinas de una misma compañía usando una arquitectura LAN-to-LAN VPN. Nótese que los túneles VPN que aparecen señalados no son enlaces físicos sino lógicos que viajan por Internet.

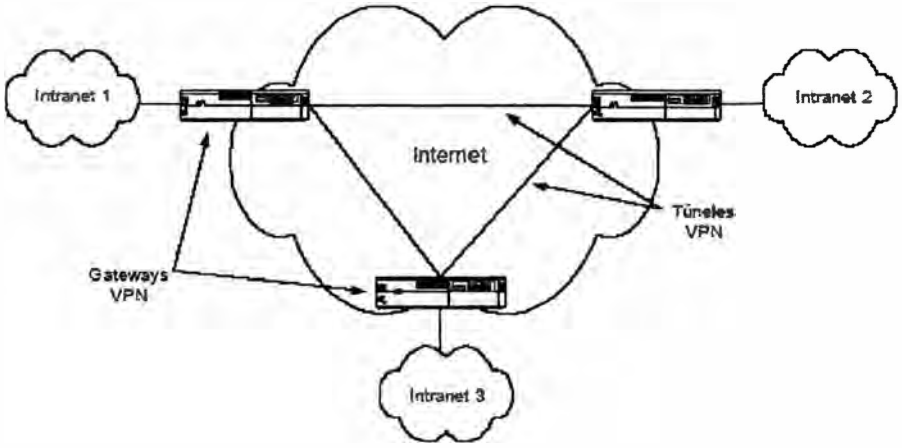

Fig. 4.5.: Esquema de una solución intranet, enlace LAN-to-LAN

4.2.2. Acceso Remoto VPN

En este tipo de conexión, un host remoto establece un túnel para ganar acceso a la intranet corporativa. El host remoto utiliza un software de tipo cliente para establecer la VPN; usando conexión física de tipo conmutada (vía telefónica) o enlaces de banda ancha permanente (por ejemplo: tipo speedy)

El acceso remoto VPN se vio claramente impulsado por el auge de la Internet que ha hecho que prácticamente en todas partes del mundo se obtenga fácil acceso a la misma. Con el acceso remoto VPN un trabajador que se haya desplazado a otro país, por ejemplo, y que quiere acceder a la base de datos de su compañía, o al

correo interno, o a cualquier otro recurso de su red corporativa, solo tiene que conectarse a Internet con una simple llamada local a la ISP de la ciudad en la que se encuentre, y ejecutar su cliente de marcación VPN. El sistema operativo Microsoft incorporó a partir de la versión Windows 98, un cliente de marcación VPN que funciona con el protocolo de tunelamiento PPTP. Todos los gateways VPN vienen con software VPN clientes para ser instalados en los distintos sistemas operativos presentes en el mercado.

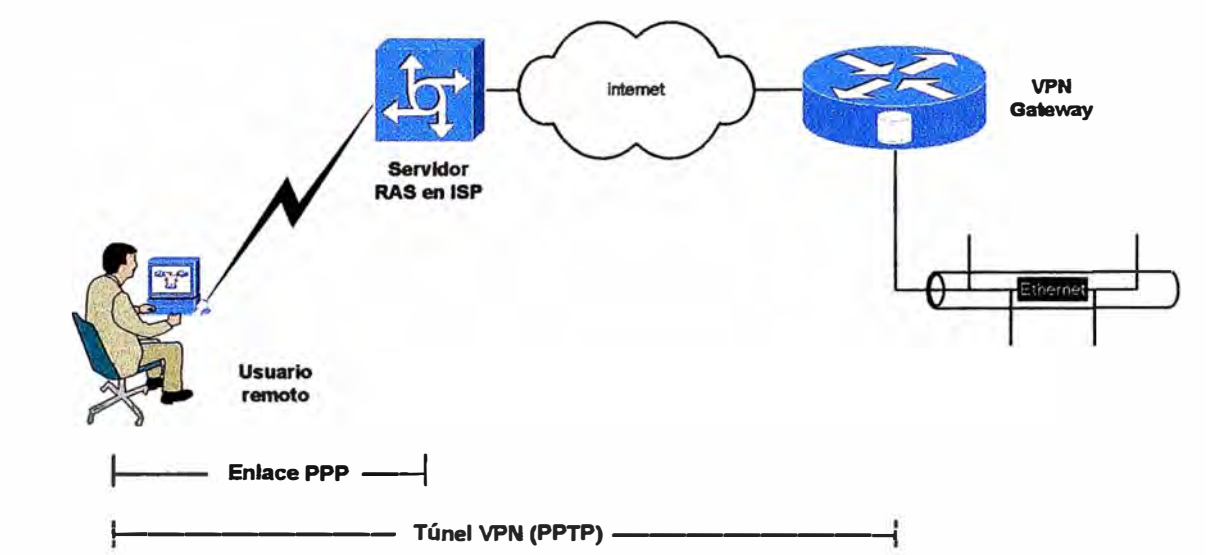

Fig. 4.6.: Esquema de una solución de acceso remoto, enlace Host-to-LAN

La figura 4.6 muestra la creación de un túnel VPN a través de conexión conmutada. En este caso, se usa un cliente PPTP implementado en el computador remoto. Primero se realiza la conexión PPP hacia el ISP, y luego un enlace PPTP hacia el gateway VPN de la empresa corporativa.

La gran ventaja de este tipo de acceso es que permite el uso de enlaces de tipo xDSL, y también de cable módem.

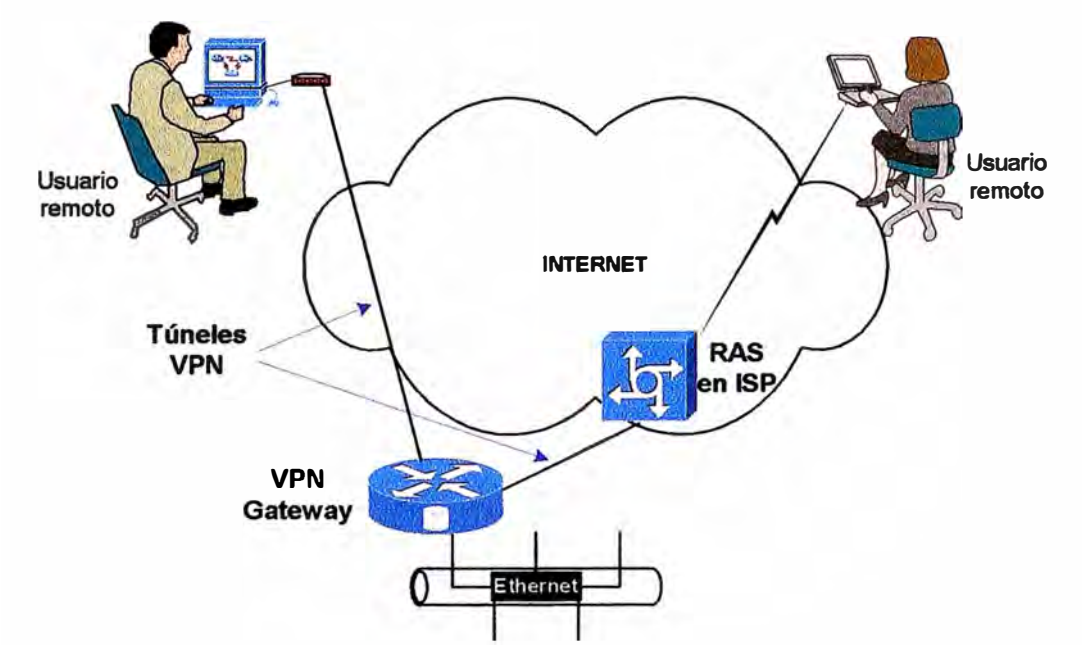

Fig. 4.7.: Esquema de solución, enlaces remotos

La figura 4.7 ilustra dos tipos de accesos remotos VPN, uno de banda ancha, donde el usuario remoto que crea el túnel tiene una conexión cable módem (también aplica xDSL) hacia la ISP; y otro acceso por medio de un módem análogo común, en este caso el usuario remoto podría estar en otra ciudad o incluso en otro país.

4.2.3. Extranet VPN

El intercambio de información a veces también hace necesario que algunos recursos de la empresa sean accesados por sus proveedores y/o clientes, en este caso, estamos frente a la necesidad de la implementación de una Extranet.

La necesidad de intercambiar información y realizar transacciones entre empresas obliga a buscar la implementación de este tipo de enlaces, Extranet VPN. Pero es preciso tomar en cuenta todos los detalles relativos al control de acceso y autenticación. Ya que es sumamente riesgoso exponer los recursos de una corporación a terceros, estos temas deben ser profundamente estudiados antes de ponerlos en producción.

Ejemplos de conexiones dinámicas seguras y que son conocidos como Extranet VPNs se muestran en la figura 4.8.

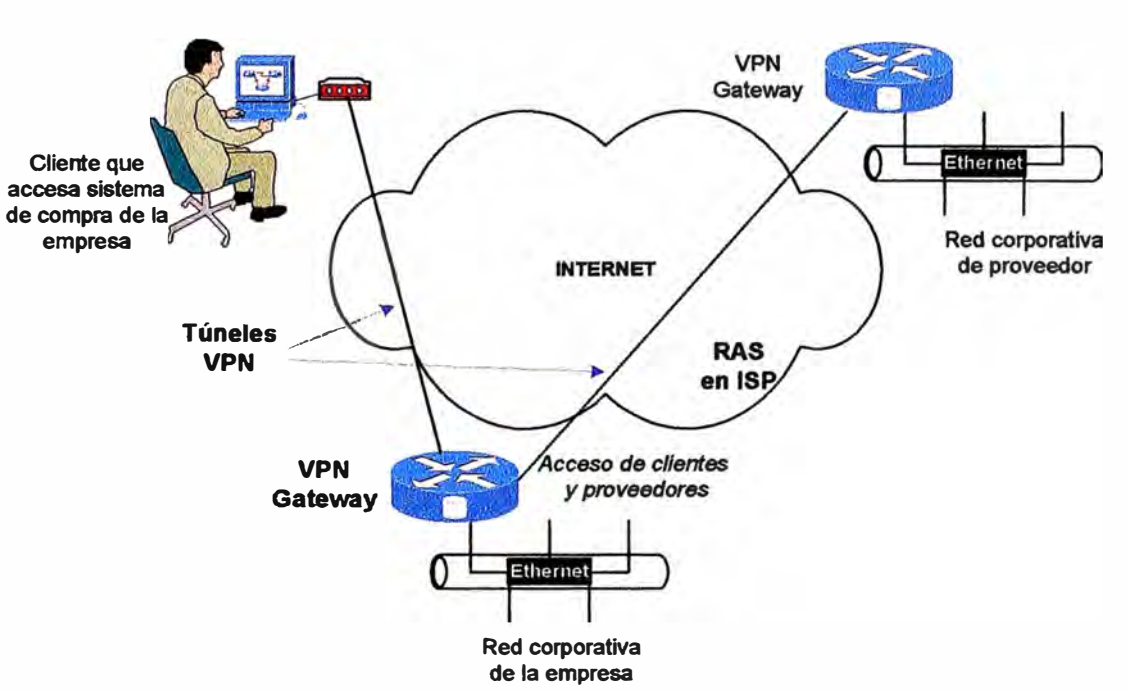

Fig. 4.8.: Conexiones dinámicas seguras

Para lograr la implementación de una conexión de éste tipo, es preciso que ambas empresas posean equipamiento de tipo gateway que permita lograr la interconexión necesaria. Además de esto, es sumamente importante garantizar que ninguna de las empresas podrá acceder a los recursos críticos de la otra empresa, por ello, es preciso elevar los niveles de seguridad de la configuración de acceso, a fin de evitar problemas posteriores.

4.3. Tunelamiento

VPN usa "túneles" entre dos puntos para proteger la privacidad de los datos mientras viajan por Internet. Tunelamiento es el proceso de encapsular y encriptar los paquetes de datos haciéndolos ilegibles para cualquier usuario. Adicionalmente, en las Redes Privadas Virtuales (VPN) los sitios de terminación (terminadores) de los túneles son aquellos donde se toman las decisiones de autenticación, las políticas de control de acceso y donde los servicios de seguridad son negociados y otorgados.

En la práctica hay tres tipos posibles de servicios de seguridad que dependen de la ubicación de los terminadores. El primer caso es aquel donde el terminador está en el host mismo, donde los datos se originan y terminan. En el segundo caso el terminador está en el gateway de la LAN corporativa donde todo el tráfico converge en un solo enlace. El tercer

caso es aquel donde el terminador está localizado fuera de la red corporativa, es decir en un Punto de Presencia (POP) del ISP.

Dado que un túnel VPN se compone de dos terminadores, se pueden obtener seis tipos de modelos de seguridad derivados de la posible combinación de las diferentes localizaciones: End-to-End, End-to-LAN, End-to-POP, LAN-to- LAN, LAN-to-POP y POP-to-POP, en la figura 4.9. se nota cada uno de ellos:

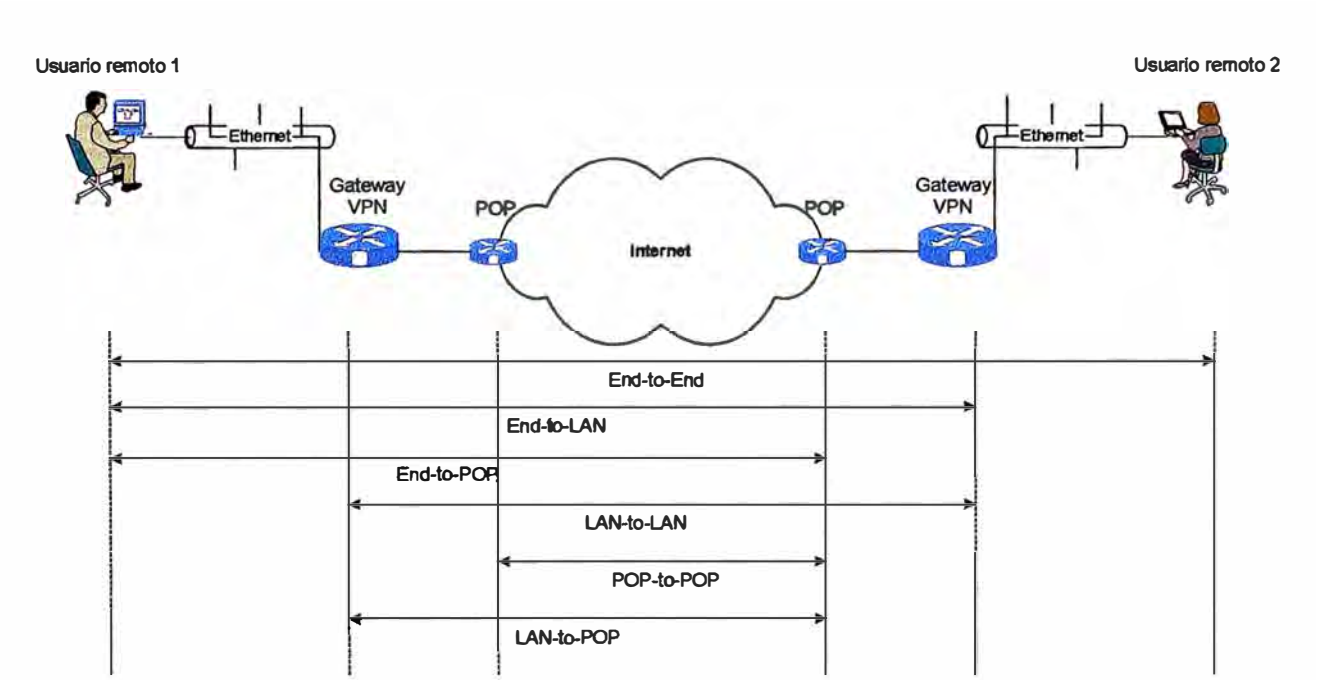

Fig 4.9. : Modelos de seguridad de conexión

En el modelo End-to-End el túnel va desde un extremo hasta el otro del sistema. Por lo tanto, los servicios de seguridad son negociados y obtenidos en la fuente y en el destino de la comunicación. Este escenario presenta el más alto nivel de seguridad dado que los datos siempre están seguros en todos los segmentos de la red, bien sea pública o privada.

En el modelo End-to-LAN, el túnel comienza en un host y termina en el perímetro de una LAN en la cual reside el host destino. Un dispositivo VPN localizado en el perímetro de la red es el responsable de la negociación y obtención de los servicios de seguridad de los host remotos. De esta manera, la seguridad de un gran número de dispositivos en una red corporativa puede ser manejada en un único punto, facilitando así la escalabilidad del mismo. Dado que la red corporativa es considerada un sitio seguro, comúnmente no hay

necesidad de encriptar la información que transita dentro de ella. La mayoría de implementaciones de acceso remoto VPN trabajan con este modelo.

El modelo de tunelamiento End-to-POP es aquel en el cual un host remoto termina el túnel en un POP de la ISP. Un dispositivo VPN o un equipo con funciones de terminador VPN y que se encuentra en la red de la ISP es el responsable por la negociación y concesión de los servicios de seguridad. La entrega de los datos desde el POP hasta el host destino es por lo general asegurada con infraestructura física, la cual separa el tráfico del resto de la red pública. Por lo general en este caso el ISP administra los permisos y controla el acceso según las directivas de los administradores de red de las empresas clientes. La arquitectura de acceso remoto VPN también usa este modelo.

En el modelo LAN-to-LAN ambos hosts usan dispositivos VPNs situados en la frontera de la red corporativa para negociar y conceder servicios de seguridad. De esta manera, las funciones de seguridad no necesitan ser implementadas en los hosts finales donde los datos son generados y recibidos. La implementación de los servicios de seguridad es completamente transparente para los hosts. Esta implementación reduce drásticamente la complejidad en el manejo de las políticas de seguridad. La arquitectura Intranet VPN encaja en este modelo.

En el caso de LAN-to-POP el túnel comienza en un dispositivo VPN localizado en la frontera de la red corporativa y termina en un dispositivo VPN el cual se encuentra en un POP de la ISP. En la actualidad prácticamente este modelo de tunelamiento no es aplicado.

Finalmente, en el modelo POP-to-POP ambos dispositivos VPN son localizados en la propia red de la ISP. Por lo tanto los servicios de seguridad son completamente transparentes para los usuarios finales del túnel. Este modelo permite a los proveedores de servicio implementar valores agregados a los clientes sin que éstos alteren la infraestructura de sus redes.

De los seis modelos anteriores el End-to-LAN y el LAN-to-LAN son los más extensamente usados en las soluciones VPN. Sin embargo, el POP-to-POP o modelo de seguridad basado en red, ha cobrado vigencia últimamente dado que permite a los ISPs implementar servicios de valores agregados para sus clientes.

4.4. Resumen del capítulo

En este capítulo, se describe brevemente los conceptos de **Red Privada Virtual** (*Virtual Private Network, VPN*), breve historia, las distintas arquitecturas que pueden utilizar dependiendo de la aplicación, tales como Intranet VPN, Acceso Remoto VPN y Extranet VPN. Asimismo, se describe los conceptos de tunelamiento como punto esencial en el establecimiento de una Red Privada Virtual (*VPN*); y descripción de las diversas opciones de creación de túneles.

CAPITULO V
SEGURIDAD Y TECNOLOGÍAS VPN

5.1. Cifrado, autenticación, control de acceso

Debido a que la Internet facilita la creación de VPNs desde cualquier lugar, las redes de datos necesitan reforzar sus niveles de seguridad para prevenir accesos indeseados a redes privadas y proteger de ésta manera los datos que deben intercambiarse vía la red pública. Los datos que viajan por Internet pueden atravesar varios servidores antes de llegar a su destino, con la potencial posibilidad de que dichos datos puedan ser observados, es preciso protegerlos mediante algún medio de cifrado.

5.1.1. Cifrado

Cifrado [REF 2] es una técnica para codificar y decodificar información. La información decodificada es llamada "texto-legible", y la información codificada es llamada "texto-cifrado". En un extremo del túnel VPN se codifica la información en modo de "texto – cifrado" antes de enviar dicha información codificada a través del túnel sobre la Internet. En el otro extremo, dicha información se decodifica obteniéndose la misma en "texto –legible". Al principio, las compañías mantenían en secreto sus algoritmos de cifrado; desafortunadamente, una vez que éstos se conocían toda su información se tornaba vulnerable. Por tanto, la industria empezó a publicar algoritmos de cifrado muy bien probados, tales como el popular Data Encription Standard (DES). Pero, si todos conocen el algoritmo de cifrado, ¿cómo puede mantenerse los datos seguros?; la respuesta son las claves que sirven para crearlos, que se denominan **llaves (*keys*).** A continuación se describen brevemente los algoritmos de encriptación mas conocidos y utilizados por la industria.

a) DES (Data Encryption Standard) y 3DES

El algoritmo DES usa llaves (*keys*) simétricas de 56 bits, para codificar datos en bloques de 64 bits. La llave de 56 bits provee 72,057'594,037'927,900 de posibles combinaciones. DES ha sido desarrollado aún más, llegando a

obtenerse el sistema 3DES [REF 3] ("triple DES"), que codifica información múltiples veces. Por ejemplo, con 3DES, los datos son codificados una vez usando la llave de 56 bits. El "texto-cifrado" resultante es luego decodificado usando una segunda llave de 56 bits, el resultado en realidad no se parece en nada a los datos originales. Finalmente estos datos son nuevamente codificados usando una tercera llave de 56 bits. Esta técnica de codificar, decodificar, y codificar (EDE en inglés, *encrypting, decrypting, encrypting*) incrementa la longitud de la llave de 56 bits a 168 bits. El algoritmo DES fue aceptado como medio de encriptación estándar por el gobierno de los EE.UU. en 1977. A partir del 2002, la Secretaría de Comercio de los EE.UU. declaró como estándar el protocolo AES

b) AES (Advanced Encryption Standard)

AES [REF 4] Es un algoritmo de encriptación aprobado para proteger información delicada, aunque no clasificada, por las agencias gubernamentales de USA. La criptografía para las comunicaciones clasificadas, incluyendo las militares, es gestionada por algoritmos secretos. En enero de 1997, El NIST (National Institute of Standards and Technology) inició un proceso para encontrar un algoritmo más robusto que reemplazara a DES y en menor medida a triple DES (3DES). La especificación solicitaba un algoritmo simétrico usando encriptación por bloques de 128 bits de tamaño, que soportara como mínimo claves de 128, 192 y 256 bits. Debía ser royalty-free para su uso en todo el mundo, y ofrecer un nivel de seguridad suficiente para los próximos 20 ó 30 años. Que fuera sencillo de implementar por hardware y software, así como en entornos restringidos (cómo smart cards, por ejemplo), y ofrecer buenas defensas contra diversas técnicas de ataque. De los algoritmos presentados (MARS de IBM research, RC6 de RSA Security, Rijndael de dos criptógrafos belgas: Joan Daemen y Vincent Rijmen, Serpent de Ross Andersen, Eli Biham y Lars Knudsen, y Twofish de un amplio equipo de criptógrafos entre los que se encuentra Bruce Schneier de Counterpane) se seleccionó a **Rijndael** como el candidato propuesto como AES. En Diciembre de 2001, el NIST (National Institute of Standards and Technology, instituto nacional de estándares y tecnología) convirtió al AES en un estándar norteamericano oficial. Para sorpresa de muchos, el algoritmo fue desarrollado

por dos criptógrafos europeos, en detrimento de productos genuinamente norteamericanos.

c) Llaves (*Keys*)

Una llave es el código secreto que un algoritmo de cifrado utiliza para crear una única versión del "texto-cifrado". Por tanto, en el proceso de cifrado en las VPN, el método puede ser el mismo (*DES, 3DES, AES*, etc.) pero las llaves (*keys*) son diferentes. Las llaves deben tener mas de tres números en su combinación, pues de hecho, la seguridad de la transmisión de datos depende de la longitud de las claves que se usen: Por ejemplo:

Llaves de 8 bits = 256 combinaciones (2^8)

Llaves de 16 bits = 65,536 combinaciones (2^{16})

Llaves de 56 bits = 72,057'594,037'927,900 combinaciones (2^{56})

En otras palabras, si se usa llaves de 16 bits, se deberían hacer 65,536 intentos para lograr romper la combinación, lo cual resulta verdaderamente simple para cualquier computadora hoy en día. Es por eso que muchos fabricantes de productos para VPN utilizan llaves de 168 bits (3DES), creando: 374,144, 419,156,711,000,000,000,000,000,000,000,000,000,000,000,000 posibles combinaciones. Existen varias empresas que van aún más allá de eso.

- **Llaves simétricas.-**

  Llaves simétricas implica el uso de la misma llave en ambos extremos del túnel, para codificar y decodificar la información. Debido a que una llave simétrica necesita ser compartida por ambas partes, debe existir un entendimiento entre ambas para tomar los pasos necesarios a fin de mantener esta llave en secreto; ésta es la razón por la cual las llaves simétricas son a menudo llamadas "llaves compartidas" (*shared keys* o *shared secrets*). Este tipo de llaves son mas difíciles de distribuir, desde que ellas deben mantenerse en secreto. Una técnica llamada "división de llaves" podría ser empleada para reducir el riesgo de descubrimiento de la llave en tránsito, ya que comúnmente estas se transmiten usando medios tales como papel, o medios removibles (diskettes, CDs, etc.).

- **Llaves asimétricas.-**

  Este tipo de llave es un tanto mas complicada, pero logísticamente mucho mas simple de administrar. Este tipo de llaves permiten codificar la

información con una llave y decodificarla con otra distinta. Las dos llaves usadas en este escenario se conocen como *llave privada* y *llave pública*. La llave pública sirve para codificar la información, y la privada sirve para decodificarla, garantizando de este modo que solo quien tenga la llave privada pueda descifrar la información.

d) Administración de llaves

Configurar llaves compartidas (*shared keys*) en pequeñas VPN no requiere necesariamente de algún software que automatice el proceso o una gran inversión en infraestructura, de hecho para el proyecto que se describirá en este documento se utiliza precisamente esta modalidad. Sin embargo, una opción bastante utilizada en empresas de mayor envergadura (y que pueden solventar los costos que involucra) es la creación de una Infraestructura de Llaves Públicas (*Public Key Infraestructure*, **PKI**), la cual permite crear, distribuir y darle seguimiento a los certificados digitales que se pueden crear para cada usuario.

Si se decide utilizar certificados, existen opciones. Por ejemplo, se puede utilizar servicios de terceros para la emisión de estos certificados, éstas entidades se llaman Certificate Authority (CA). O podemos crear nuestra propia CA usando software como Entrust, Xcert o Baltimore Technologies. Cualquiera de estas opciones puede ayudar a establecer una adecuada PKI, la cual es especialmente útil en grandes organizaciones que requieren extender sus seguridad más allá de sus usuarios de red, a sus socios de negocios y clientes.

e) Infraestructura de llaves públicas (PKI)

El comercio electrónico y la transmisión de datos privados sobre Internet ha crecido vertiginosamente, por tanto la autenticación ha cobrado un papel crucial en este proceso. La criptografía de llaves públicas ofrecen una gran herramienta matemática para facilitar la autenticidad, pero surge un gran problema y es el cómo manejar y publicar dichas llaves para cada persona o entidad que las necesiten. Brevemente se explicará la Arquitectura de una PKI.

- **Arquitectura de una PKI**

  El acrónimo PKI deriva de "Public Key Infrastructure" (Infraestructura de Clave Pública) y es la forma común de referirse a un sistema complejo

necesario para la gestión de Certificados Digitales y aplicaciones de la Firma Digital.

Una PKI bien construida debe proporcionar:

Autenticidad. La firma digital tendrá la misma validez que la manuscrita.

Confidencialidad, de la información transmitida entre las partes.

Integridad. Debe asegurarse la capacidad de detectar si un documento firmado ha sido manipulado.

No Repudio, de un documento firmado digitalmente.

- **Cifrado asimétrico**

La base tecnológica para la Firma Digital está fundamentada principalmente en el uso de ciertos algoritmos criptográficos, con unas características que permiten obtener el nivel de seguridad requerido.

A diferencia de los algoritmos de cifrado simétrico, en los que la información se cifra y descifra con la misma llave, los algoritmos asimétricos basan su funcionamiento en un par de llaves (matemáticas dependientes) para cada usuario, con la característica de que la información cifrada con una llave, sólo puede descifrarse con la otra del mismo par.

A cada usuario se debe asignar un par de llaves, que se denominan **Llave Pública** y **Llave Privada**. Como indican sus nombres, la Llave Pública puede ser conocida por todo el mundo, mientras que la Llave Privada debe ser custodiada por el usuario y nunca hacerse pública.

Si se desea enviar información confidencial a un usuario, se le enviará la información cifrada con su llave pública, de tal forma que sólo ese usuario, que posee la llave Privada correspondiente, podrá descifrar la información.

Por otra parte, si un usuario envía información cifrada con su llave privada, al descifrarla con su llave pública (acción que puede realizar cualquiera que conozca dicha clave), puede asegurarse que ha sido ese usuario quién envió la información, ya que sólo él posee la llave privada.

- **Firma digital**

Una Firma Digital[1] tiene dos características principales:

Sólo puede ser generada por el poseedor de la llave privada y puede ser verificada por cualquiera que conozca la llave pública del firmante.

Es dependiente del documento a firmar (la Firma Digital de un documento no puede emplearse para firmar otro documento).

El proceso de generación de una Firma Digital consiste en dos pasos:

Empleando un algoritmo de **"Hashing" se genera un resumen**, de tamaño fijo, del documento.

Se cifra el Hash empleando la llave privada del usuario.

Deberá transmitirse o almacenarse el documento original y la firma.

Deben realizarse los siguientes pasos:

A partir del Documento Original, se genera de nuevo el Hash.

Empleando la llave pública del firmante, se descifra la firma digital.

Se comprueba si ambos "Hashes" coinciden, si es así, la firma es auténtica, si no lo es, el documento ha sido modificado y/o la firma es falsa.

Adicionalmente, debe comprobarse que el Certificado Digital es válido.

El Certificado puede haber caducado, o puede haber sido revocado por una de las partes.

- **Certificados digitales**

Las técnicas anteriormente indicadas, si bien son técnicamente correctas, implican un grave problema a nivel de seguridad: ¿Cómo se puede asegurar que una llave pública pertenece a un usuario dado?. Es necesario poder vincular la llave pública de un usuario con su identidad y para esto surge el concepto de "Certificado Digital", que contiene la siguiente información:

Identidad del usuario (Nombre, NIF, etc...).

Clave Pública del usuario.

Periodo de Validez del Certificado.

Identidad de la Autoridad Certificadora (entidad que emite el certificado).

---

[1] La Firma Digital es un paquete de información de tamaño fijo, dependiente del documento original y sólo puede generarse por el poseedor de la llave privada.

Firma digital del certificado (los datos anteriores más otras posibles extensiones personalizables, por ejemplo: la dirección de correo electrónico), generada por la **Autoridad Certificadora.**

Esta información se encapsula en un formato estándar, definido por la norma **ISO X.509 versión 3.** Generalmente existirá un repositorio (p.e. directorio LDAP) en el que se publican todos los certificados gestionados por la PKI y puede ser consultado por otros usuarios de la PKI que quieran enviar información cifrada o verificar firmas digitales.

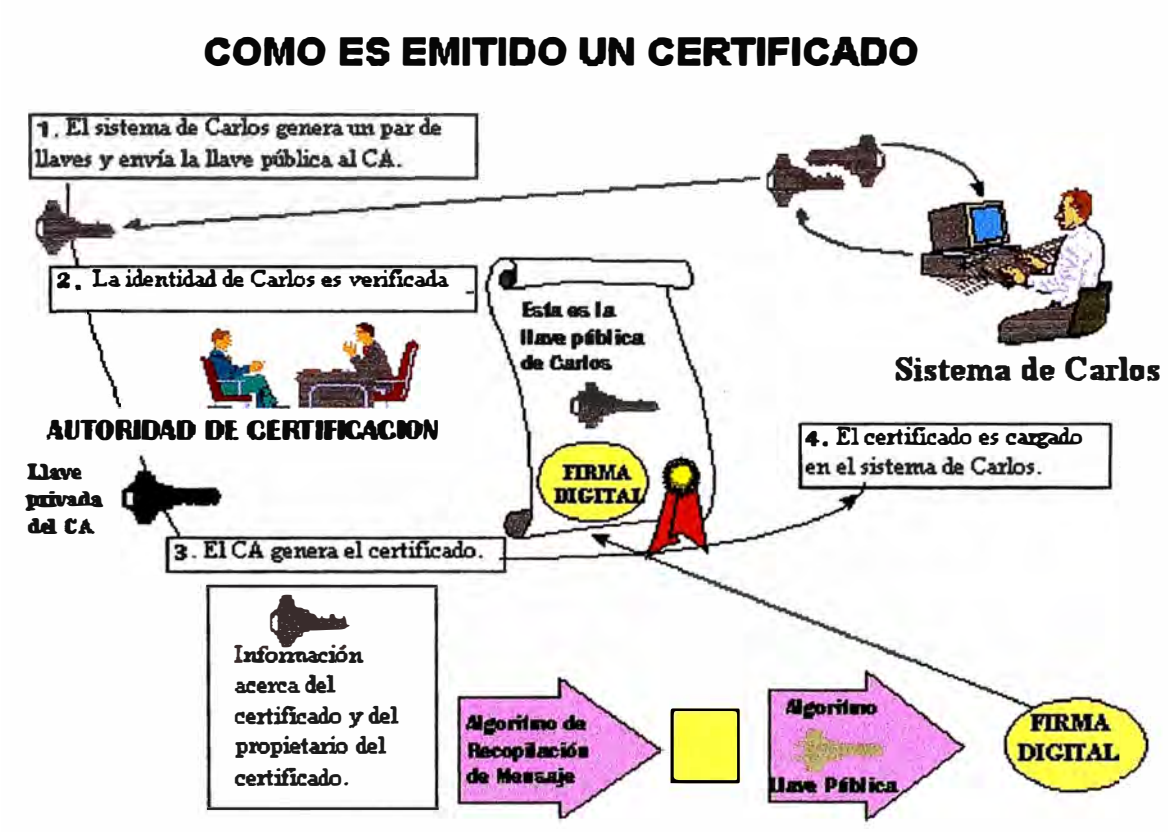

Fig.5.1.: Forma de gestionar un Certificado

- **La Autoridad Certificadora**

La Autoridad Certificadora (*Certificate Authority*), es la entidad que asegura la identidad de los usuarios de los certificados digitales. Posee su propio par de llaves y firma digitalmente los certificados con su llave privada. Confiando en la Firma Digital de la Autoridad Certificadora, puede confiarse en cualquier certificado generado por la misma.

Las tareas realizadas por la Autoridad Certificadora son, entre otras, las siguientes:

Procesa peticiones de Certificado a través de la Autoridad de Registro (*Register Authority*). Estas solicitudes están compuestas básicamente por los datos de identificación y la llave pública del solicitante.

Genera los Certificados y los almacena en el repositorio público (por ejemplo: LDAP).

Gestiona la caducidad y renovación de certificados.

Gestiona la revocación de certificados (por ejemplo: por quedar comprometida la llave privada del usuario al serle sustraída su SmartCard).

Toda la fiabilidad de la Autoridad de Certificación se basa en la inviolabilidad de su propia llave privada, la cual resulta crítico proteger empleando medios técnicos y humanos.

- **La Autoridad de Registro**

En toda PKI deben establecerse los mecanismos para que los usuarios soliciten su propio certificado, de tal forma que se asegure la identidad de dicho usuario. A este procedimiento se le denomina "Proceso de Registro" y se realiza a través de la denominada "Autoridad de Registro".

Existen dos tipos principales de registro:

Registro Clásico. El solicitante acude en persona a una "Oficina de Registro", donde, tras acreditar su identidad, se le proporciona de forma segura su clave privada y su certificado.

Registro Remoto. El usuario, a través de Internet, realiza una solicitud de certificado. Para esto empleará un software (por ejemplo: un navegador) que generará el par de claves y enviará su clave pública a la Autoridad de Registro para que sea firmada por la Autoridad Certificadora y le sea devuelto su certificado.

La validez de la Firma Digital estará condicionada por la calidad del proceso de registro, siendo obligatorio para asegurar la validez legal de la firma, algún tipo de registro "Cara a Cara", ya que es el único que asegura la identidad del solicitante. Por otra parte, la validez de la firma digital también

estará condicionada a la firma manuscrita de un "contrato" por el que el solicitante acepta su certificado y las condiciones de uso del mismo.

La Autoridad de Registro se compone de una serie de elementos tecnológicos (hardware y software específico) y unos medios humanos (los Operadores de Registro). Es el punto de comunicación entre los usuarios de la PKI y la Autoridad certificadora.

- **Componentes de una PKI**

Los sistemas anteriormente descritos deben englobarse en un único sistema, al que se denomina "Infraestructura de Clave Pública" (PKI), cuyo elementos se pueden ilustrar en la siguiente figura.

Fig.5.2.: Componentes de una PKI

Existen multitud de componentes adicionales, y cada elemento es un sistema complejo en si mismo. Los componentes básicos pueden resumirse en:

La Autoridad de Certificación. La pieza central, y la que proporciona la base de confianza en la PKI. Constituido por elementos hardware, software y, evidentemente, humanos.

Publicación de Certificados. El repositorio de certificados permite a los usuarios operar entre ellos, y es un requisito legal que cuente con una total disponibilidad de acceso.

Soporte de la Clave Privada. La elección de un buen soporte para que los usuarios custodien su llave privada es un punto esencial y complejo en si mismo.

Aplicaciones "PKI-Enabled". Se denomina así a las aplicaciones de software capaces de operar con certificados digitales. Estas aplicaciones son las que dan el valor real de la PKI frente al usuario.

Políticas de Certificación. Deben diseñarse una serie de políticas, o procedimientos operativos, que rigen el funcionamiento de la PKI y establecen los compromisos entre la Autoridad Certificadora y los Usuarios Finales. Estos documentos tendrán un carácter tanto técnico como legal.

El Proceso de Construcción de una PKI deberá siempre partir de la definición de las Políticas Operativas y contemplar como requerimiento esencial el asegurar la calidad y seguridad de las operaciones que los usuarios finales realizan con sus claves privadas.

f) Funciones de resumen (hashing)

Hashing es el proceso por el cual se transforma una cadena de caracteres en un valor de una longitud pre-establecida o clave de la cadena original.

El algoritmo Hash, llamado función hash, se utiliza para los procesos de encriptación y decriptación de firmas digitales (utilizadas para autentificar quienes envían/reciben mensajes digitales). La firma digital se transforma a través de una función hash en un número único que es decriptado en el otro extremo del mensaje utilizando el mismo algoritmo y posteriormente verificado con el agente autentificador que almacena estos datos. Entre ellas están:

- **SHA y SHA1**

El SHA (*Secure Hash Algorithm*) es un algoritmo de resumen seguro desarrollado por el NIST. El SHA-1 es una versión corregida del algoritmo publicada en 1994. El algoritmo es un estándar ANSI.

El algoritmo toma un mensaje de menos de 2^{64} bits y genera un resumen de 160 bits. Es más lento que el MD5, pero la mayor longitud de clave lo hace más resistente a ataques de colisión por fuerza bruta y de inversión.

- **MD2, MD4 y MD5**

Los tres son algoritmos de resumen de mensajes (el MD viene de *Message Digest*) desarrollados por Rivest.

Los tres toman un mensaje de longitud arbitraria y generan un resumen de 128 bits. El MD2 está optimizado para máquinas de 8 bits, mientras que el MD4 y MD5 son para arquitecturas de 32 bits. El código para los tres algoritmos se puede encontrar en los RFCs 1319, 1320 y 1321.

El MD2 funciona rellenando el mensaje para que tenga una longitud en bytes múltiplo de 16. Sobre ese mensaje se calcula un checksum de 16 bytes que se añade al mensaje y la función de dispersión se aplica al mensaje resultante. El único problema que se le conoce es que si se omite el checksum se pueden obtener colisiones.

El MD4 fue desarrollado en 1990 por Rivest. El mensaje se rellena para que su longitud en bits más 448 sea divisible por 512. Una representación de la longitud del mensaje de 64 bits se concatena entonces con el mensaje. El mensaje se procesa iterativamente en bloques de 512 bits y cada bloque es procesado en tres rotaciones distintas. El algoritmo ha sido criptoanalizado y se han encontrado debilidades, de hecho es posible encontrar colisiones en menos de un minuto en máquinas modernas, por lo que el algoritmo se considera a todos los efectos roto.

El MD5 fue desarrollado en 1991 por Rivest. Es básicamente el MD4 con mejoras en la seguridad, aunque es más lento que este. El tamaño del resumen y la necesidad del relleno son iguales que en el MD4. Consta de cuatro rotaciones que tienen un diseño ligeramente diferente a las del MD4. El algoritmo ha sido criptoanalizado con técnicas similares a las del MD4 y se han encontrado pseudo-colisiones en la función de compresión, pero no en el algoritmo completo. Adicionalmente, se ha estimado que es posible construir una máquina capaz de atacar el algoritmo por fuerza bruta y encontrar una colisión en 24 días, aunque el costo de la máquina era de 10 millones de dólares en 1994.

5.1.2. Autenticación

La autenticación es el proceso por el que se comprueba la identidad de alguien o algo, para ver si es lo que dice ser. Ese "alguien" o "algo" se denomina principal. La autenticación requiere pruebas de identidad, denominadas credenciales. Por ejemplo, una aplicación cliente puede presentar una contraseña como sus credenciales. Si la aplicación cliente presenta las credenciales correctas, se asume que es quien dice ser.

En un mundo de tantos billones de personas no es suficiente simplemente declarar que se es quien se dice ser, es necesario probarlo. La autenticación involucra usualmente la interacción entre dos entidades: el objeto de la autenticación (un usuario o un cliente) que afirma su identidad y un autenticador realizando la verificación de la identidad. El usuario entrega información de autenticación la cual incluye la identidad proclamada y la información que soporta dicha identidad al autenticador. En la labor de verificación, el autenticador aplica una función de autenticación F que le entrega información y luego compara el resultado de esta operación con el resultado esperado.

Si el resultado de la función F concuerda con el resultado esperado, la identidad del usuario se considera verificada. La modalidad de autenticación puede ser un simple password o un grupo completo de parámetros y mensajes. Del mismo modo, la función F puede ser una simple función como en el caso de la comparación de claves, o la aplicación de complejos algoritmos criptográficos, como en el caso de firmas digitales.

a) Sistemas de autenticación

La autenticación es una parte vital en la estructura de seguridad de una VPN; sin ella no se podría controlar el acceso a los recursos de la red corporativa y evitar el acceso de usuarios no autorizados

Los sistemas de autenticación [REF 5] pueden estar basados en uno de los siguientes tres atributos: algo que el usuario tiene (por ejemplo la llave de una puerta); algo que el usuario sabe (por ejemplo una clave); ó algo que el usuario es (por ejemplo sistemas de reconocimiento de voz ó barrido de retinas). Es generalmente aceptado el uso de un método sencillo de autenticación tal como el password, pero no es adecuado para proteger sistemas. Los expertos

recomiendan los llamados sistemas de autenticación complejos, los cuales usan al menos dos de los atributos de autenticación anteriores.

A continuación se describen los sistemas de autenticación más comúnmente usados en los ambientes de redes: passwords tradicionales, passwords únicos, PAP, CHAP y Radius

- **Passwords tradicionales**

Son la forma más simple de autenticar pero es un método inadecuado para garantizar la seguridad en el acceso a una red, dado que los passwords pueden ser adivinados e interceptados durante transmisiones en la red.

Por ejemplo, servicios tales como FTP y Telnet transmiten los nombres y las claves en texto plano, haciéndolos fácilmente interceptables.

- **Passwords únicos**

Una forma de prevenir el uso no autorizado de Passwords interceptados es evitar que sean reutilizados. Los sistemas de Passwords Únicos restringen el uso de un password a una sola sesión de comunicación, es decir que se requiere un password nuevo para cada nueva sesión. Estos sistemas, de los cuales S/KEY es el mejor ejemplo, facilitan al usuario la escogencia de un nuevo password para la siguiente sesión generando automáticamente una lista de posibles passwords para el usuario

- **S/KEY**

S/Key es un esquema de contraseña de un solo uso basado en una función de hash de sentido único.

El propósito de S/Key es eliminar la necesidad que un mismo password sea enviado sobre la red cada vez que se requiere un password para acceso. Una serie de passwords son creados a la vez, y cada password es usado solo una vez, por lo tanto, si alguna persona obtiene uno de los passwords no le es posible utilizarlo debido a que ya no son válidos una vez que fue utilizado por primera vez.

- **PAP**

Password Authentication Protocol, provee un método simple para establecer la identidad de un equipo usando un método de dos vías en una

conexión PPP. Esto solamente es posible una vez que el enlace ha sido establecido.

Una vez que el enlace ha sido establecido, una pareja de ID/password es enviada repetidamente por el equipo hacia el autenticador hasta que la autenticación es reconocida o la conexión terminada.

PAP no es un método de autenticación fuerte. Los passwords se envían en texto plano via el circuito de enlace y no hay protección. El equipo origen es quien está en control de la frecuencia y tiempo de los intentos.

- **CHAP**

Challenge-Handshake Athentication Protocol, es un esquema de autenticación usado por servidores con protocolo PPP para validar la identidad del equipo que originó la conexión, durante la misma o en cualquier momento durante el tiempo de conexión.

CHAP aplica un procedimiento de tres vías. Después que el enlace está establecido, el servidor envía un mensaje de "desafío" (*challenge*) al equipo que originó de la conexión. El equipo origen responde con un valor calculado usando una función "hash" de una vía. El servidor chequea la respuesta contra su propio cálculo del valor "hash" esperado. Si el valor es el mismo, la autenticación es aceptada, en caso contrario, la conexión usualmente es terminada.

CHAP provee protección contra ataques "playback" a través del uso de un identificador cambiante incrementalmente y un valor de desafío variable. El equipo autenticador es quien está en control de la frecuencia y tiempo de los desafíos. CHAP provee una mayor seguridad que PAP

- **MS-CHAP**

Microsoft creó el **Microsoft Challenge Handshake Authentication Protocol** (MS-CHAP), una extension de CHAP para autenticar estaciones Windows remotas. Es un protocolo de autenticación de password cifrado, no reversible. El desafío (*challenge*) trabaja como sigue:

El autenticador (el Servidor RAS o IAS) envía un desafío (*challenge*) al cliente remoto, que consiste en un identificador de sesión y una cadena de caracteres arbitraria.

El cliente remoto envía una respuesta que contiene el nombre de usuario y un cifrado no reversible de la cadena de caracteres, el identificador de sesión y el password.

El autenticador verifica la respuesta y, si es válida, autentica las credenciales del usuario.

- **MS-CHAP v2**

MS-CHAP v2 es un protocolo de autenticación mutua, lo cual significa que tanto el cliente como el servidor deben probar que tienen conocimiento del password del usuario. Primero, el servidor de acceso remoto (RAS) desafía al cliente remoto a la prueba. Luego el cliente remoto hace la misma consulta al servidor RAS enviándole el desafío, y respondiendo a la prueba emitida por el servidor. Si el servidor no responde acertadamente, la conexión es terminada.

- **EAP**

Extensible Authentication Protocol es una extension del protocolo punto a punto (*Point to Point Protocol, PPP*). Fue desarrollado en respuesta a la demanda por autenticación de usuarios remotos que usan otros fabricantes de equipos de seguridad. EAP provee un mecanismo estándar para soporte de métodos de autenticación adicionales dentro de PPP. Usando EAP, se puede añadir un número de esquemas de autenticación, como "token cards", "passwords únicos", autenticación de llave pública usando tarjetas inteligentes, certificados y otros

- **RADIUS**

Remote Authentication Dial-In User Service, RADIUS fue desarrollado por Livingston Enterprise, ahora una división de Lucent Technologies, RADIUS usa una arquitectura cliente – servidor e incluye dos componentes: un servidor de autenticación y un protocolo cliente. Es un protocolo de autenticación, autorización y "accounting" para aplicaciones de acceso remoto a la red en las que intervienen servidores NAS (*Network Access Server*)

Las características esenciales de RADIUS son:

Modelo Cliente / Servidor.- Un NAS opera como cliente del RADIUS. El cliente es responsable de pasar la información del usuario a los

servidores RADIUS designados, y luego actuar con la respuesta que se obtenga. Los servidores RADIUS son responsables de recibir las solicitudes de conexión, autenticar al usuario utilizando protocolos PAP, CHAP o EAP y luego retornar toda la configuración necesaria para que el cliente brinde servicio al usuario. Un servidor RADIUS puede actuar como cliente "proxy" a otros servidores RADIUS u otros tipos de servidores de autenticación.

Seguridad de red.- Las transacciones entre el cliente y el servidor RADIUS son autenticadas a través del uso de la técnica "shared secret", llave que nunca se envía sobre la red. Además, todos los passwords de usuarios son enviados cifrados enre el cliente y el RADIUS Server, para evitar la posibilidad de que alguien pueda intentar descubrir algún password de usuario.

Mecanismos de autenticación flexibles.- El servidor RADIUS puede soportar una variedad de mecanismos para autenticar un usuario; puede soportar PPP PAP o CHAP, login de UNIX, y otros mecanismos de autenticación.

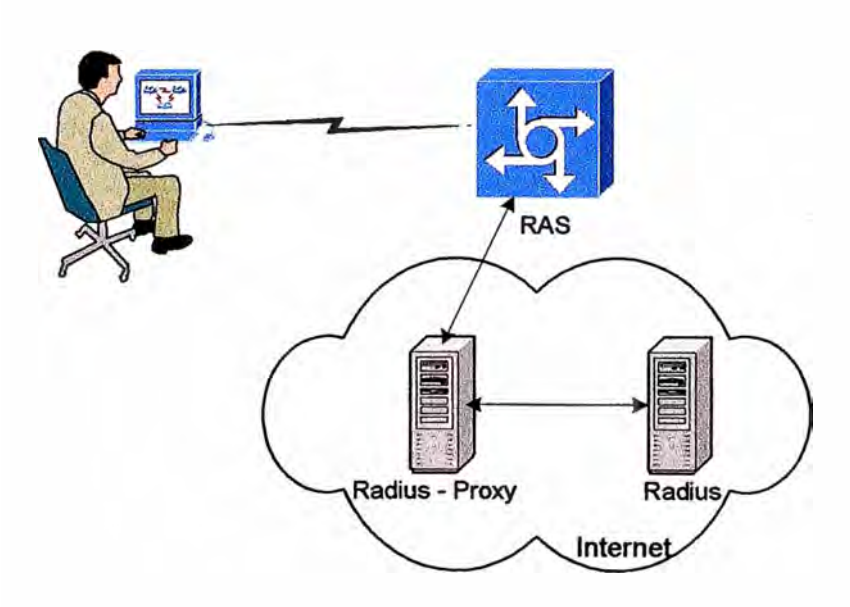

Fig.5.3.: Autenticación vía RADIUS

5.1.3. Control de acceso

El control de acceso está compuesto por un conjunto de políticas y mecanismos que permiten garantizar el acceso autorizado a determinados recursos de la red corporativa.

La figura 5.4 muestra un control de acceso en un modelo cliente-servidor. Se considera usuario a cualquier entidad (usuario o aplicación trabajando en nombre de ese usuario) que desee acceder al recurso. Se determina por recurso a cualquier objeto que puede ser manipulado de alguna manera, tales como lectura, escritura o modificación, causadas por la realización de alguna acción, tales como la ejecución de un programa o el envío de un mensaje.

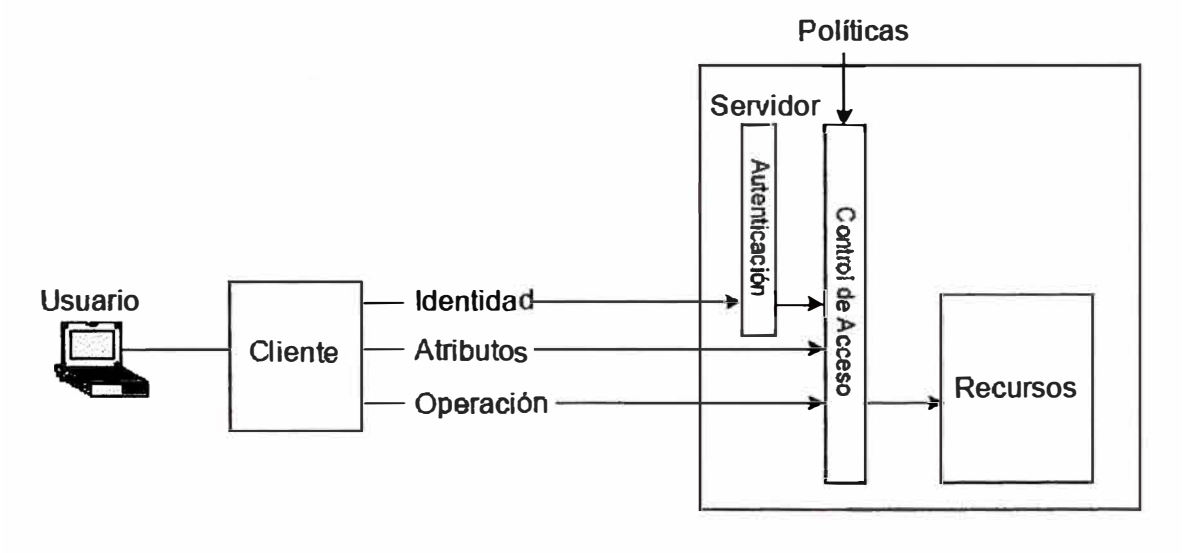

Fig. 5.4.: Control de acceso en sistema cliente-servidor

Un usuario tiene una identidad y un conjunto de atributos asociados. El cliente envía la identificación del usuario, los atributos y el requerimiento de una operación al servidor. El servidor puede autenticar la identidad del usuario y remitirlo junto con los atributos y el requerimiento solicitado a los mecanismos de control de acceso. Las políticas son preestablecidas en el mecanismo de control de acceso; la información del usuario es comparada con las reglas de las políticas para determinar los derechos de acceso del usuario a ese recurso.

5.2. Tecnologías VPN

Definimos tres grandes tecnologías VPN [REF 6]: VPN de Confianza (*Trusted VPN*), VPN Segura (*Secure VPN*), y VPN Híbrida (*Hybrid VPN*), las hemos puesto con sus nombres en inglés porque de ese modo serán mejor reconocidas. Es importante notar que *VPN Segura*

y una *VPN de Confianza* no están técnicamente relacionadas y pueden co-existir en un único paquete de servicio.

Antes que la Internet llegase a ser lo que es hoy, una VPN consistía de uno o más circuitos dedicados rentados por el cliente a un proveedor de servicio de Telecomunicaciones, quien le ofrecía administrar las conexiones que se requiriesen. El cliente confiaba en que el proveedor de servicio mantendría la integridad de los enlaces y aplicaría lo último en tecnología para evitar que se pierda la privacidad de los datos que se transmitan, por tanto, este tipo de VPNs se denominan **VPN de Confianza (*Trusted VPN*)**. Este tipo de VPNs incluye:

- Capa 2 (Layer 2)

  Circuitos ATM

  Circuitos Frame Relay

  Transporte de tramas de capa 2 sobre MPLS, como se describe en draft-martini-l2circuit-trans-mpls
- Capa 3 (Layer 3)

  MPLS con distribución reducida de información de ruteo a través de BGP, como se describe en el draft-ietf-ppvpn-rfc2547bis

Se asume que ambas opciones se convertirán en estándares en el futuro.

A medida que Internet se hizo mas popular como medio corporativo de comunicación, la seguridad se convirtió en un tema esencial tanto para los clientes como los proveedores Viendo que las *Trusted VPN* no ofrecían una seguridad real, los fabricantes empezaron a crear protocolos que permitiesen al tráfico de datos ser encriptado (cifrado) en el perímetro de una red o en la computadora origen, mover dichos datos como cualquier otro a través de la red pública, y luego desencriptarlos (descifrarlos) cuando llegasen a su destino. Este tráfico cifrado actúa como un túnel entre las redes; aún si algún atacante pudiese ver o capturar los paquetes de datos, no podrá leerlos. Los enlaces construidos en base a cifrado de datos se conocen como **VPN Segura (*Secure VPN*)**. Este tipo de VPN incluye:

- **IPSec** con cifrado (encriptación), en los modos de túnel o transporte. Las Asociaciones de Seguridad (*Security Association*) pueden se configuradas de manera manual o mediante el protocolo IKE usando certificados o llaves compartidas (*Shared Secrets*). IPSec es descrita en varios RFC, tales como: 2401, 2406, 2407, 2408, y 2409.

- **IPSec dentro de LPT2**, como se describe en el RFC 3193, ha tenido bastante difusión en implementaciones de VPN segura para acceso remoto de tipo cliente –servidor.
- **SSL 3.0** ó **TLS** con cifrado, TLS [REF 7] es descrita en el RFC 2246

Muchas de estas opciones son estándares de IETF

Recientemente, proveedores de servicio han empezado a ofrecer un nuevo tipo de servicio *Trusted VPN*, ésta vez usando la Internet en vez de las líneas telefónicas convencionales. Estas nuevas *Trusted VPN* aún no ofrecen seguridad pero brindan a los clientes un modo sencillo de configurar segmentos de red equivalentes a una WAN. Las técnicas de una red del tipo *Secure VPN* puede formar parte de una *Trusted VPN* como la que acabamos de describir, creando un tercer tipo de VPN, que se conoce como **VPN Híbrida (*Hybrid VPN*)**. La parte segura de éste tipo de VPN podría ser controlada por el cliente o por el mismo proveedor de servicio que provee la *Trusted VPN*.

5.2.1. Protocolos

Aquí haremos un breve resumen de los protocolos mas utilizados para el establecimiento de configuraciones VPN. En nuestro proyecto, la implementación se ha basado en IPSec el cual casi se ha estandarizado como el mas utilizado, pero existen otros que fueron utilizados por mucho tiempo antes de la aparición del IPSec.

a) PPTP

PPTP [REF 8], es quizá el protocolo más sencillo de tunelamiento de paquetes.

El protocolo PPTP fue propuesto por el Foro PPTP (PPTP Forum), compuesto por 3Com, Ascend (ahora Lucent), Microsoft, ECI Telematics y USRobotics. Debido a la integración que hizo Microsoft en sus sistemas operativos Windows NT, y luego en Windows98 y posteriores, PPTP tuvo gran acogida en el mercado mundial, a tal punto que un protocolo de capa 2 lanzado por Cisco Systems al mismo tiempo, prácticamente no se conoció, L2F (Layer-2-Forwarding).

En el escenario típico de PPTP, el cliente establecerá una conexión dial-up con el servidor de acceso a red (NAS) del proveedor del servicio, empleando para ello el protocolo PPP. Una vez conectado, el cliente establecerá una segunda conexión con el servidor PPTP el cual estará situado en la red privada. Dicho servidor será utilizado como intermediario de la conexión, recibiendo los datos

del cliente externo y transmitiéndolos al correspondiente destino en la red privada.

PPTP encapsula los paquetes PPP en datagramas IP. Una vez que los datagramas llegan al servidor PPTP, son desensamblados con el fin de obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido. El protocolo PPTP especifica además una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP. Estos mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. De este modo, los paquetes de control almacenan la cabecera IP, la cabecera TCP, el mensaje de control PPTP.

La autenticación PPTP está basada en el sistema de acceso de Windows NT, en el cual todos los clientes deben proporcionar un par login/password. La autenticación remota de clientes PPTP es realizada empleando los mismos métodos de autenticación utilizados por cualquier otro tipo de servidor de acceso remoto (RAS). En cuanto a la encriptación de datos, PPTP utiliza el proceso de encriptación de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. Dicha clave es generada empleando el estándar RSA RC-4 a partir del password del usuario. La longitud de dicha clave puede ser 128 bits (para usuarios de Estados Unidos y Canadá) o 40 bits (para el resto de usuarios).

La figura 5.5 muestra una conexión PPP entre un host y un RAS.

Como se puede ver, es una conexión sencilla punto a punto donde lo primero que se realiza es una autenticación sencilla previa al envío y recibo de tramas PPP de datos.

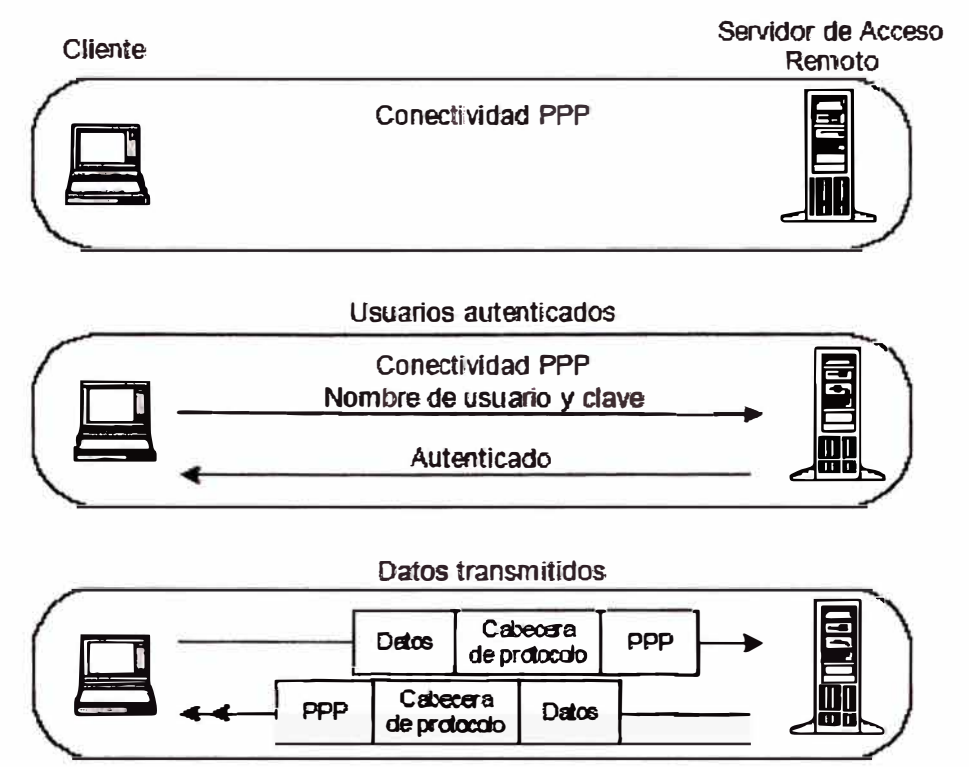

Fig. 5.5.: Conexión PPTP Típica entre un host y un RAS

PPTP utiliza los mecanismos de autenticación que generalmente están asociados a PPP tales como PAP y CHAP, una versión mejorada de CHAP llamada MS-CHAP y desarrollada por Microsoft se encuentra en sus sistemas operativos Windows NT, 2000 y XP. Otra mejora que le ha hecho Microsoft al protocolo PPTP es la incorporación del método de cifrado MPPE (Microsoft Point-to-Point Encription).

Una de las ventajas que tiene PPTP por ser un protocolo de nivel 2, es que puede transmitir protocolos diferentes a IP en sus túneles, a diferencia de IPSec que se restringe a trabajar solamente con paquetes IP.

La figura 5.6 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulación PPTP desde el sistema cliente hasta la LAN corporativa.

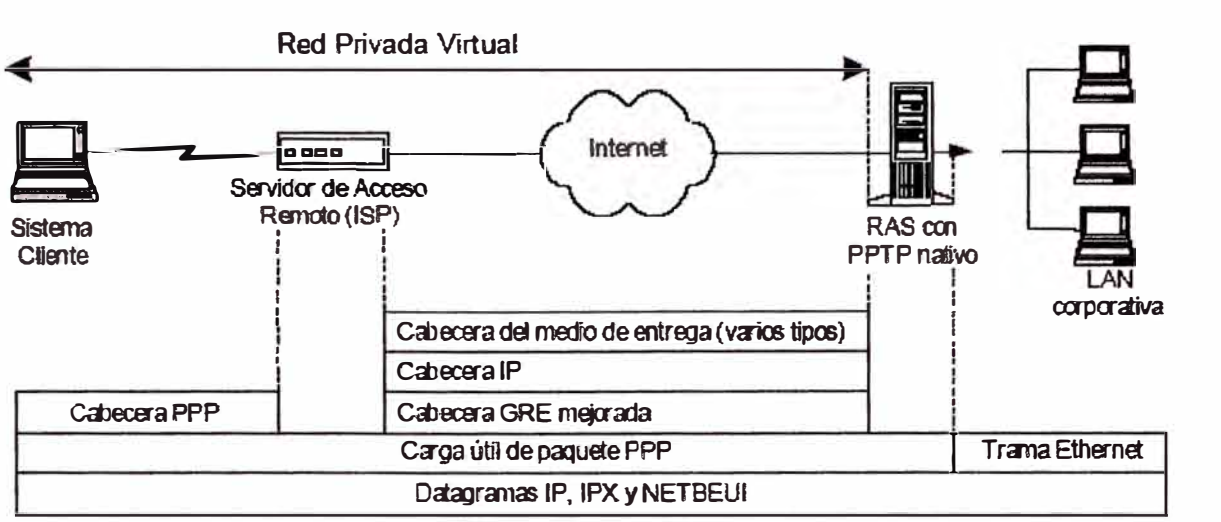

Fig. 5.6.: Estructura de un túnel PPTP

b) L2TP (Layer 2 Tunneling Protocol)

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 de estos protocolos y establecerse como un estándar aprobado por el IETF. 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. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, Frame Relay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.

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

A causa de estos inconvenientes, el grupo del IETF que trabaja en el desarrollo de PPP consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP del mismo estilo de los que se están realizando para IPSec, y dado la duplicación del trabajo respecto al propio grupo de desarrollo de IPSec que supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

La figura 5.7 muestra la arquitectura de un enlace VPN basado en L2TP.

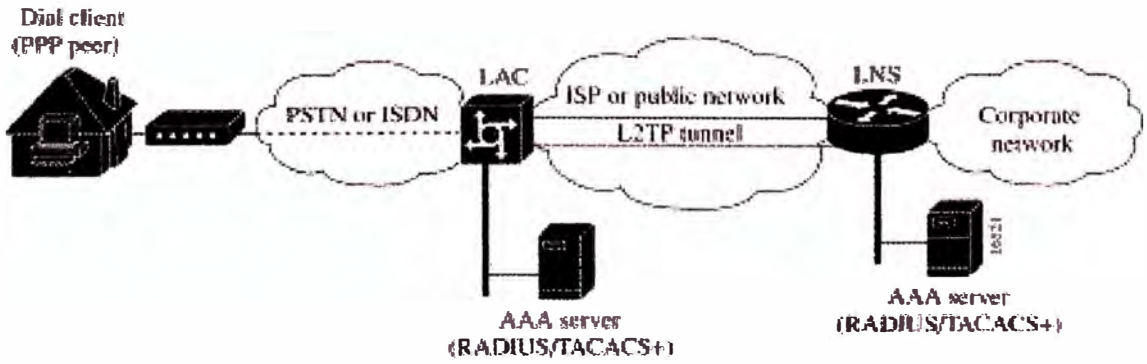

Fig. 5.7.: Arquitectura de un enlace VPN basado en L2TP

L2TP Access Concentrator (LAC), es un dispositivo hacia donde el cliente se conecta directamente y donde las tramas PPP son tunelizadas

hacia el L2TP Network Server (LNS). El LAC necesita solamente implementar el medio sobre el cual L2TP opera para pasar el tráfico a uno o mas LNSs. Puede tunelizar cualquier protocolo transportado con PPP. LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas de salida. Análogo al L2F Network Access Server (NAS)

L2TP Network Server (LNS), es el punto de terminación del túnel L2TP y el punto de acceso donde las tramas son procesadas y pasadas protocolos de mayor nivel. Un LNS opera en cualquier plataforma capaz de ofrecer una terminación PPP. El LNS maneja el lado "servidor" del protocolo L2TP. El LNS puede tener una simple interfase LAN o WAN, y aún ser capaz de ser el punto terminal de las llamadas que llegan a cualquiera de los LACs llenos de interfaces PPP (asíncronas, síncronas, etc.). El LNS es el iniciador de las llamadas de salida y receptor de las llamadas de entrada. Análogo al Layer 2 Forwarding (L2F) Home Gateway (HGW)

c) IPSec

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos.

IPSec es un conjunto de protocolos diseñados para proveer una seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPSec está incluido en IPv6.

Entre los servicios de seguridad definidos en IPSec se encuentran: control de acceso, integridad de datos, autenticación del origen de los datos, protección antirepetición y confidencialidad en los datos. Entre las ventajas de IPSec están la modularidad del protocolo, ya que no depende de un algoritmo criptográfico específico.

- **Componentes de IPSec**

IPSec está compuesto por tres componentes básicos: los protocolos de seguridad (AH y ESP), las asociaciones de seguridad (SAs) y las bases de datos de seguridad; cada uno de los cuales, trabaja de la mano con los demás.

Protocolos de seguridad.-

IPSec es un conjunto de protocolos que provee varios servicios de seguridad. Esos servicios de seguridad trabajan gracias a dos protocolos, el Authentication Header (AH) y el Encapsulating Security Payload (ESP), y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (Internet Key Exchange Protocol). El éxito de una implementación IPSec depende en gran medida de una adecuada elección del protocolo de seguridad y de la forma como se intercambian las llaves criptográficas.

AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee integridad parcial para prevenir ataques de repetición. Este protocolo es apropiado cuando se requiere autenticación en vez de confidencialidad.

ESP provee confidencialidad para el tráfico IP, al igual que autenticación tal cual como lo hace AH, pero solo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo.

IKE es un protocolo que permite a dos entidades IPSec negociar dinámicamente sus servicios de seguridad y sus llaves de cifrado al igual que la autenticación de la sesión misma

Asociaciones de Seguridad (SA)

El concepto de asociación de seguridad (SA) es clave en IPSec. Una SA define las medidas de seguridad que deberían ser aplicadas a los paquetes IP basados en quién los envía, hacia donde van y qué tipo de carga útil ellos transportan. El conjunto de servicios de seguridad ofrecidos por una SA dependen de los protocolos de seguridad y del modo en el cual ellos operan definidos por la SA misma. La figura 5.8 muestra los dos modos en los cuales un protocolo de seguridad puede operar: transporte y túnel; la diferencia radica en la manera como cada uno de ellos altera el paquete IP original. El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP. En modo túnel, el paquete IP original se convierte en la carga útil de un nuevo paquete IP. Esto le permite al paquete IP inicial, "ocultar" su cabecera IP para que sea encriptada,

considerando que el paquete IP externo sirve de guía a los datos a través de la red.

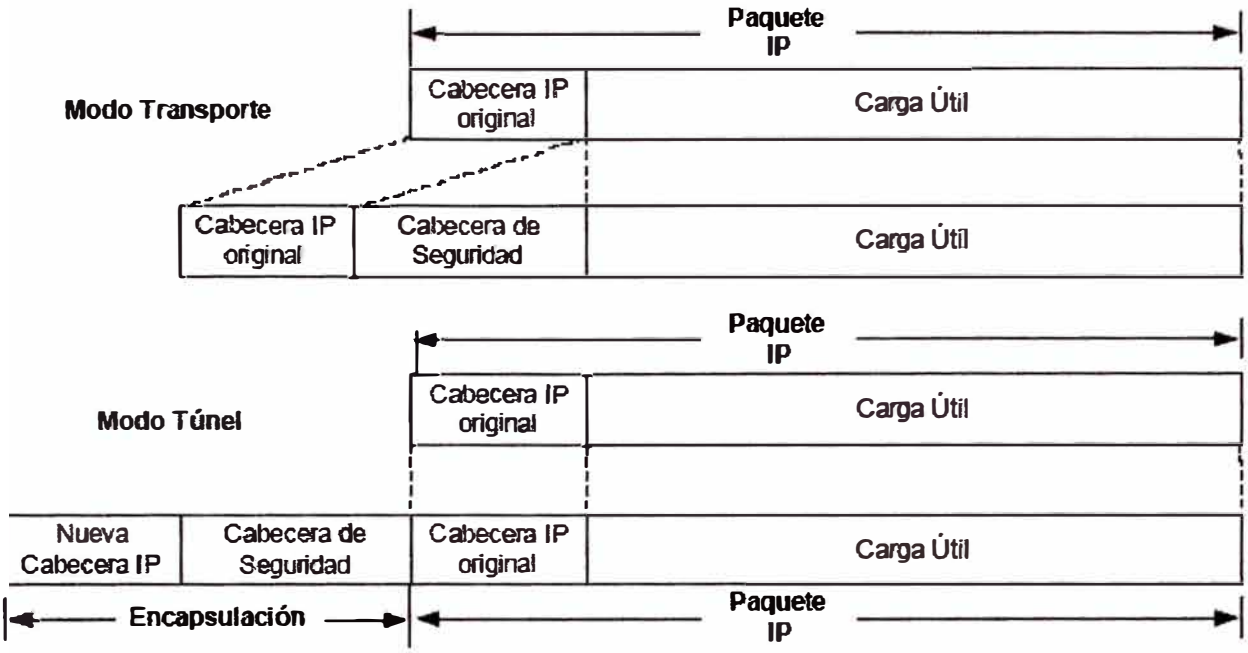

Fig. 5.8.: Estructura del paquete IP en modo de transporte y túnel

Las SAs pueden ser negociadas entre dos entidades IPSec dinámicamente, para lo cual se basan en políticas de seguridad dadas por el administrador del sistema o estáticamente especificadas por el administrador directamente.

Una SA es únicamente identificada por tres parámetros: una dirección IP de destino, un identificador del protocolo de seguridad y un índice del parámetro de seguridad (SPI). La dirección IP de destino es aquella por la cual se identifica el punto final de la SA, el SPI es un número de 32 bits usualmente escogido por el punto final de destino de la SA y que solo tiene significado local dentro de ese punto destino. El identificador del protocolo de seguridad es un número con el cual se define cada uno de ellos, 51 para AH o 50 para ESP.

Como se nota, la dirección IP del origen no se usa para definir una SA, esto dado que una SA se define entre dos host o gateways para datos enviados en una sola dirección, de aquí que, si dos dispositivos necesitan intercambiar información en ambas direcciones usando IPSec, requerirán de dos SAs, una para cada sentido. En modo de transporte, la cabecera IP original se mantiene intacta y una cabecera de seguridad es colocada entre la cabecera

IP misma y su carga útil. La cabecera IP original es modificada para que el receptor del paquete entienda que antes de la carga útil se encuentra una cabecera de seguridad. En modo túnel, el paquete IP original se convierte en la carga útil de un paquete IP encapsulado. La cabecera IP nueva le indica al receptor del paquete que una cabecera de seguridad se encuentra a continuación de ella.

Varias SAs pueden ser aplicadas en serie para incrementar los servicios de seguridad del tráfico IP. En estas situaciones una SA es encerrada por otra. El protocolo IPSec define dos formas: transporte adyacente y túneles iterados.

En transporte adyacente se usan tanto AH como ESP y ellos son aplicados por el mismo host. Es de anotar que trabajar con adyacencias de transporte AH sobre AH o ESP sobre ESP no trae beneficios adicionales. Lo deseable en este caso es aplicar AH después de ESP.

En túneles iterados, se puede combina cualquier cantidad de túneles con lo cual se logra proveer de capas anidadas de seguridad. Los puntos finales del túnel pueden ser en la misma o en diferentes locaciones. Por ejemplo, un túnel host-to-host puede ser entunelado por un túnel gateway-to-gateway; y un túnel gateway-to-gateway puede de nuevo ser tunelizado por otro túnel gateway-to-gateway.

Bases de Datos de Seguridad

IPSec trabaja con dos bases de datos de seguridad, en una se encuentran las políticas de seguridad y en la otra las asociaciones de seguridad, SPD (Security Policy Database) y SAD (Security Association Database) respectivamente. El administrador de políticas define un conjunto de servicios de seguridad para ser aplicados al tráfico IP tanto entrante como saliente. Esas políticas son guardadas en las SPDs y son usadas por las SAs cuando éstas se crean. Todas las SAs son registradas en la SAD.

- **Bases de Datos de SA (SAD)**

  La base de datos de asociaciones de seguridad almacena todos los parámetros concernientes a las SAs, cada una de ellas tiene una entrada en la SAD donde se especifican todos los parámetros necesarios para que IPSec realice el procesamiento de paquetes IP

que son gobernados por esa SA. Entre los parámetros que se encuentran en una SAD se tienen:

- El índice de parámetro de seguridad.
- El protocolo a ser usado por la SA (ESP o AH).
- El modo en el cual el protocolo es operado (túnel o transporte).
- Un contador numérico secuencial.
- La dirección IP fuente y destino de la SA.
- El algoritmo de autenticación y la llave de autenticación usadas.
- El algoritmo de cifrado y su llave.
- El tiempo de vida de las llaves de autenticación y de cifrado.
- El tiempo de vida de la SA.

Para el procesamiento de los paquetes IP entrantes una SA apropiada es encontrada en la SAD tal que concuerde con los siguientes tres valores: la dirección IP destino, el tipo de protocolo IPSec y el SPI. La dirección IP de destino y el tipo de protocolo IPSec son obtenidos de la cabecera IP y el SPI se obtiene de la cabecera AH o ESP. Si una SA es encontrada para el paquete IP entrante en mención, éste es procesado de acuerdo a los servicios de seguridad especificados. Luego se aplican al paquete todas las reglas descritas en la SPD para la SA que lo gobierna.

Para el procesamiento de paquetes IP salientes, primero se aplica el procesamiento relacionado con la SPD. Si se encuentra una política para el paquete de salida que especifique que un procesamiento IPSec es necesario, la SAD es buscada para determinar si una asociación de seguridad ha sido previamente establecida. Si una entrada es encontrada, el paquete es procesado de acuerdo a la SA. Si por lo contrario no se encuentra ninguna entrada para este paquete una nueva SA es negociada y luego guardada en la SAD.

- **Base de Datos de Políticas de Seguridad (SPD)**

Una base de datos de políticas de seguridad es una lista ordenada de políticas de seguridad a ser aplicadas a los paquetes IP. Dichas políticas son en general reglas que especifican como los paquetes IP

deben ser procesados. La SPD es mantenida por el administrador del dispositivo IPSec.

Una entrada SPD tiene dos componentes: un juego de selectores y una acción. Los selectores clasifican un paquete IP sobre una acción. Un selector es un parámetro y el valor o rango de valores para éste parámetro. Los parámetros generalmente se encuentran dentro de una de éstas dos categorías:

- Aquellos que se encuentran dentro de un paquete IP, tales como, la dirección IP, número de protocolo y números de puertos de capas superiores.
- Aquellos que se derivan de la credencial de autenticación de una entidad de comunicación, tales como, una dirección de correo o un nombre distinguido DN (Distinguished Name) en certificados digitales

Diferentes operadores lógicos como AND, OR y NOT pueden ser aplicados a las políticas para combinar más de un selector. Cuando un paquete IP contiene valores que concuerdan con los especificados por algún selector de una entrada, la acción que se especifica en dicha entrada es aplicada al paquete. Hay tres opciones: aplicar el servicio de seguridad IPSec, descartar el paquete IP o permitir que el paquete IP omita el procesamiento IPSec.

La figura 5.9 muestra una entrada en una base de datos de políticas de seguridad para un paquete entrante y saliente, claramente se notan las partes que componen un selector como lo son los parámetros y su correspondiente valor, al frente se encuentra la acción que IPSec tomaría si los paquetes IP concuerdan con los valores de los selectores

Entrantes	Selectores	Acción
	dirección_IP fuente = 10.0.0.92 *AND* dirección de e-mail fuente = financiera@telesat.com.co	IPSec (ESP, 3DES, HMAC-SHA-1)
	nombre_distinguido fuente = Andrés Gómez	IPSec (ESP, 3DES, HMAC-MD5)
	dirección_IP destino = 192.89.0.169	Omitir

Salientes	Selectores	Acción
	dirección_IP destino = 10.0.0.92	IPSec (ESP, 3DES, HMAC-SHA-1)
	nombre_distinguido destino = Andrés Gómez	IPSec (ESP, 3DES, HMAC-MD5)
	dirección_IP fuente = 192.89.0.169	Omitir

Fig. 5.9.: Ejemplos de entradas en una base de datos de políticas de seguridad

Es posible que un paquete IP concuerde con más de una entrada en la SPD. Por esto, se debe tener en cuenta el orden de las entradas en una SPD, ya que la primera concordancia será la política seleccionada. En adición, una política por defecto debe ser aplicada para el nodo y ésta se aplica cuando el paquete IP no concuerda con ninguna de las entradas de una SPD. Usualmente, esta política por defecto es descartar el paquete IP.

La SPD trata al tráfico saliente y entrante de manera separada, esto es, que se deben aplicar políticas de seguridad distintivas de entrada y de salida por cada interfaz de red. Cuando un paquete IP llega a una interfaz de red, IPSec primero busca en la SAD la apropiada SA, cuando la encuentra, el sistema inicia los procesos SAD y SPD. Después del procesamiento SPD, el sistema reenvía el paquete al siguiente salto o le aplica procedimientos adicionales tales como las reglas de algún firewall.

El procesamiento PSD se realiza primero en paquetes salientes. Si la entrada SPD que concuerda especifica que un procesamiento IPSec es necesario, la SAD es consultada para determinar si una SA ha sido

previamente establecida, en caso contrario se negocia una nueva SA para el paquete.

Dado que los procesos SPD son realizados tanto para los paquetes IP salientes como entrantes, este procedimiento puede alterar negativamente el desempeño de un dispositivo IPSec. De hecho, el procesamiento SPD es el cuello de botella más representativo en una implementación IPSec.

d) MPLS

MPLS es una tecnología que modifica el reenvío tradicional de paquetes que analiza la dirección IP de destino contenida en la cabecera de la capa de red de cada paquete y por medio de la cual un paquete viaja desde la fuente hasta su destino final. En el análisis tradicional para el reenvío de un paquete IP cada proceso de estos es realizado en cada punto de la red. Los protocolos de enrutamiento dinámicos o estáticos construyen una base de datos necesaria, la cual se analiza para tomar una decisión hacia donde va el paquete IP según dirección de destino, dicha tabla se conoce como tabla de enrutamiento.

El reenvío tradicional de paquetes que realiza la capa de red, confía en la información que le proveen los protocolos de enrutamiento tales como OSPF (Open Shortest Path First) o BGP (Border Gateway Protocol) o a las rutas estáticas configuradas en cada router, para tomar la decisión de reenvío entre los mismos. Es decir, que la decisión de reenvío está basada única y exclusivamente en la dirección IP de destino. Todos los paquetes para el mismo destino siguen el mismo camino a través de la red si no existen otros caminos de igual costo. Si un router tiene dos caminos de igual costo hacia un mismo destino, los paquetes podrían tomar uno solo o ambos, trayendo como consecuencia una degradación en la velocidad debido al proceso de balanceo de cargas.

Los routers son dispositivos que trabajan a nivel de la capa de red, ellos se encargan de recolectar y distribuir la información de enrutamiento y de la conmutación a nivel 3 basada en el contenido de la cabecera de la capa de red de cada paquete.

Los routers se pueden conectar directamente por medio de enlaces punto-apunto o redes de área local. También pueden ser conectados a través de switches LAN

o WAN. Esos switches LAN o WAN de Capa 2 no tienen la capacidad de mantener la información de enrutamiento de Capa 3 o de seleccionar el camino que debería de tomar un paquete partiendo del análisis de su dirección de destino Capa 3. Es decir, los switches de Capa 2 no se pueden involucrar en el proceso de reenvío de paquetes a nivel de Capa 3.

En el caso de una red WAN el diseñador de la red tiene entonces que establecer trayectos a nivel 2 manualmente a través de toda la red WAN. Por esos trayectos o paths es por donde los enrutadores que están conectados físicamente a la Capa 2, reenvían sus paquetes a nivel de la Capa 3.

El establecimiento de un path en una red WAN de Capa 2 se realiza por medio de un enlace punto-a-punto, que en la mayoría de redes WAN es llamado un circuito virtual y que se establece únicamente por medio de una configuración manual. Cualquier dispositivo de enrutamiento que se encuentre conectado en los límites de una red de Capa 2 y que quiera reenviar sus paquetes a nivel de Capa 3 a otro dispositivo de enrutamiento, necesita establecer una conexión directa a través de la red.

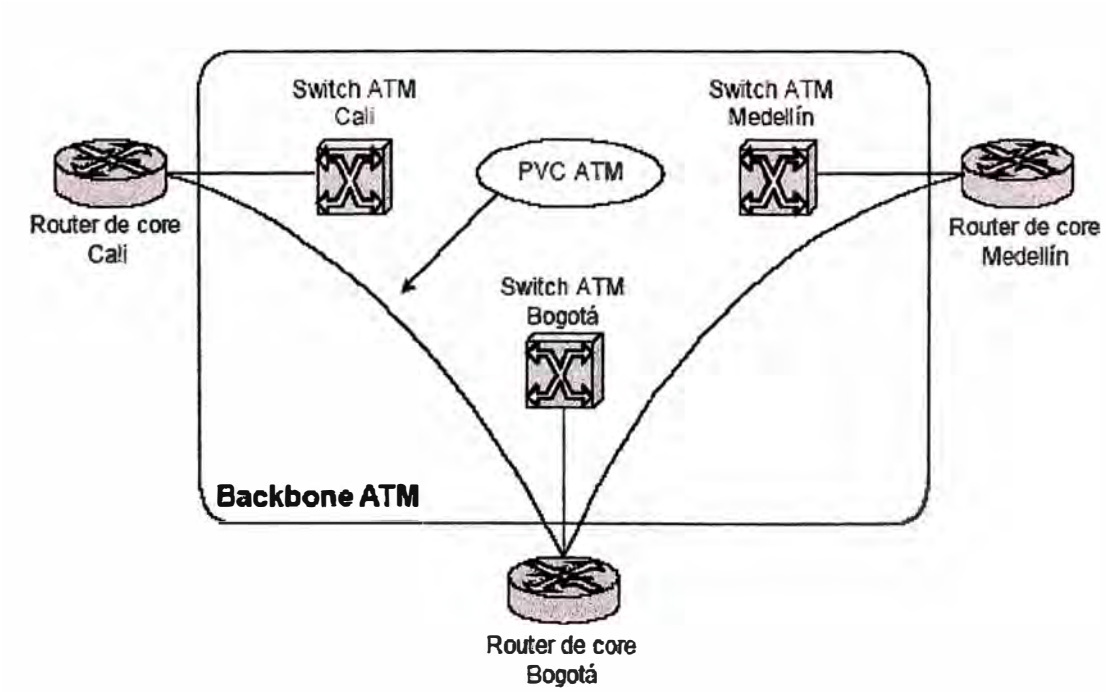

Fig.5.9.: Red IP basada en un backbone ATM

Los problemas de escalabilidad que se pueden encontrar en redes de este tipo son:

Cada vez que un nuevo router es conectado a la red WAN, un circuito virtual debe ser establecido entre este router y cada uno de los demás, si se busca un enrutamiento óptimo.

En la mayoría de protocolos de enrutamiento, cada router conectado ala red WAN a nivel de Capa 2, necesita un circuito virtual dedicado a cada uno de los otros routers. Con esto se logra la redundancia deseada configurando una adyacencia a cada uno de los otros routers. Como resultado de esta necesidad, se obtienen enrutadores con múltiples vecinos y a su vez, cantidades de tráfico de enrutamiento circulando entre ellos.

Otro problema frecuente es la dificultad que se tiene para hacer el aprovisionamiento de ancho de banda o de circuitos virtuales entre los routers de una red Capa 3, por cuanto es difícil predecir la cantidad exacta de tráfico entre dos routers. Esto conlleva a que algunos proveedores de servicio no opten por ofrecer un servicio de calidad garantizada dado por su red, sino que se busca que el ancho de banda sea limitado por la capacidad de la última milla.

5.3. Resumen del capítulo.

Los conceptos teóricos esenciales a tener en cuenta para la elección de una solución basada en Redes Privadas Virtuales se han descrito en este capítulo con cierta profundidad. Conceptos como cifrado de datos, autenticación y control de acceso, que permiten garantizar la seguridad del intercambio de datos a través de este tipo de enlaces y por tanto "simular" enlaces dedicados, son analizados en cada caso.

Las diversas tecnologías VPN así como los protocolos de comunicación mas utilizados se han desarrollado en este capítulo, marcando una mayor profundidad en el protocolo IPSec, el cual utilizaremos para la implementación del proyecto que describimos en el informe.

CAPITULO VI
IMPLEMENTACION DE ENLACES VPN EN PERUFARMA S.A.

6.1. Análisis de soluciones disponibles

De acuerdo a la problemática definida en los primeros capítulos, se deduce que el requerimiento de interconexión de las redes LAN ubicadas en Lima, así como la conexión de los usuarios de las oficinas de provincia con la oficina central en Lima, se hacía indispensable. Para lograr determinar cual resultaba ser la mejor opción costo beneficio, se procedió a realizar un análisis de las opciones disponibles; entre ellas están:

- Enlace vía línea dedicada para las oficinas de Lima
- Enlace inalámbrico entre las oficinas de Lima
- Enlaces IP-VPN de cada oficina remota con la oficina central
- Enlaces VPN a través de Internet.

6.1.1. Opción 1: Enlaces vía línea dedicada

Las opciones de enlaces dedicados, más conocidos como "leased lines", sugieren una buena opción disponible en el ámbito de interconexión de locales. Bajo este tipo de conexiones, se puede establecer enlaces privados de punto a punto cuya velocidad varía entre desde unos pocos Kilobits por segundo hasta varios Megabits por segundo. Dado que en este tipo de conexiones, el usuario no comparte esta conexión con nadie más, la empresa que ofrece el servicio puede garantizar un nivel de calidad determinado para la transmisión de datos.

En nuestro caso, el uso de líneas dedicadas suponía la solución para el enlace de red entre la oficina central de Perufarma S.A. y la oficina ubicada en San Isidro.

La propuesta analizada para la interconexión de la oficina de San Isidro con la Oficina central estaba valorizada en (aproximadamente): **US$ 950.00** mensuales, adicionando costo de instalación **US$ 700.00** por cada sitio por única vez. El ancho de banda contratado sería de 128 Kbps.

Estos costos resultaban ser elevados para ser aplicados como parte de la solución general, ya que la inversión solo por un enlace sería de aproximadamente US$

11,400.00 anuales, y aún faltaba definir el tema de las oficinas de provincia. Debido a esto se decidió no optar por este tipo de solución.

6.1.2. Opción 2: Enlace Wireless LAN

La posibilidad de interconectar dos oficinas mediante un enlace inalámbrico nos permitiría "extender" la red LAN de la oficina central, con velocidades cercanas a la que se obtendría en una red local. Es decir, 11Mbps, 22Mbps, 54Mbps u otra mayor. Actualmente, esta posibilidad es una de las mejores opciones disponibles para lograr una excelente conexión entre locales remotos con un índice costo – beneficio bastante aceptable.

Como toda interconexión física, tiene sus limitaciones en cuanto a la distancia entre los locales, efectos de los obstáculos que podrían impedir la transmisión punto a punto, el tamaño requerido para las torres, ubicación de antenas, alimentación eléctrica, efectos ambientales, etc.

Para nuestro caso, se hizo la evaluación o estudio de campo para la instalación de dicho enlace entre la oficina ubicada en San Isidro y el local central. Para esto se solicitó el servicio de una empresa de reconocido prestigio en éste ámbito, dicha empresa, realizó el estudio de campo y finalmente emitió su informe, el cual indicaba lo siguiente (se adjunta el texto del mismo):

Estimado César:

Te envío el perfil del estudio de campo de PERUFARMA, de acuerdo a los datos obtenidos:

1.- Perufarma cuenta en el local de la Av.Universitaria y Venezuela con un edificio de 12 metros de altura.
2.- En el otro punto Calle 21 cuadra 7 en San Borja, se cuenta con un edificio de 8 metros de altura aproximadamente.

Según el perfil de la línea de vista existen obstáculos, y para poder pasarlos es necesario contar con una torre de 40
metros en el punto de la Av . Universitaria y Venezuela, y otra torre de 70 metros en el punto de Calle 21.
Debido a la complejidad de implementar estas torres por su envergadura y porque técnicamente la distancia de conexión entre las antenas y los respectivos equipos atenuaría la señal, no recomendamos una instalación de wireless entre ambos puntos, quedando sin embargo, abierta la posibilidad de utilizar un punto repetidor intermedio.

Quedamos a la espera de cualquier duda o comentario y agradeceremos comunicarse nuevamente si hubiera la posibilidad de contar con la alternativa señalada.
En breve te estaremos enviando nuestra carta de presentación a fin de poder ser una alternativa para futuros proyectos en telecomunicaciones.

Saludos cordiales

Oscar Maldonado Zúñiga
Consultor en Telecomunicaciones
División Empresa
BMP INGENIEROS S.A.
Mail to: omaldonado@bmp.com.pe
Phone: (51-1) 612-8585 ext. 214
Fax: (51-1) 475-1513
Web: www.bmp.com.pe

El cuadro mostrado es la transcripción del informe real, emitido por el consultor de la empresa especialista.

El gráfico que a continuación se muestra indica precisamente el resultado del estudio de campo.

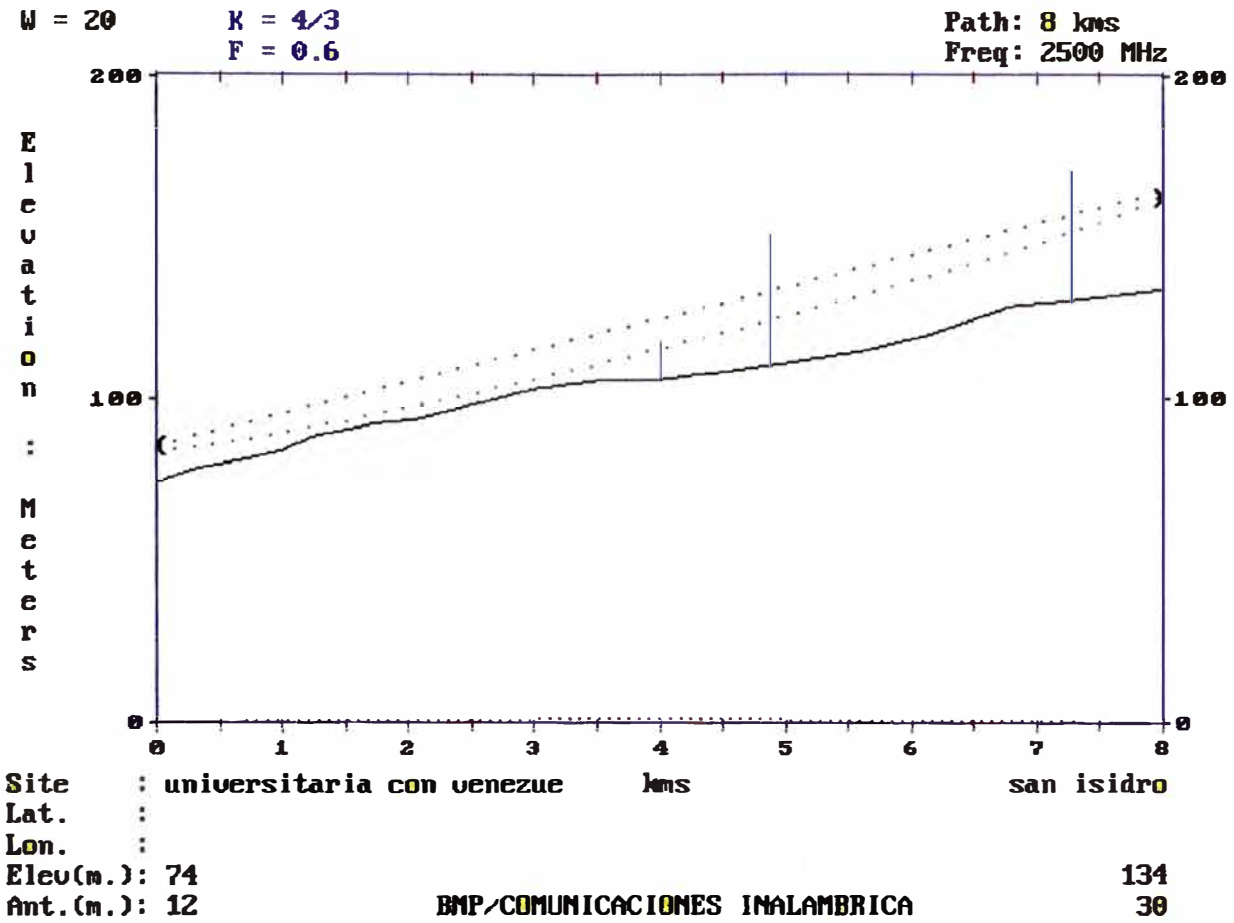

Fig. 6.1.: Resultado del estudio de campo realizado por BMP Ingenieros

Con el estudio de campo realizado, se determinaba que no era recomendable técnicamente la implementación de una torre tan elevada en cada local, esencialmente en el lado de San Isidro; esto hacía imposible la implementación de la opción de interconexión Wireless LAN.

Ante este impase, se decidió continuar el examen de otras opciones.

6.1.3. Opción 3: Enlaces IP-VPN

Este tipo de enlace fue una propuesta hecha por Telefónica del Perú, basado en su actual red MPLS. Existe la posibilidad de implementar enlaces VPN administrados por el proveedor, el cual, utilizando su propia infraestructura y equipamiento de borde, llega a configurar este tipo de enlaces. Estos enlaces por lo regular son simétricos, aunque existe también la posibilidad de crear enlaces asimétricos de tipo ADSL.

Telefónica del Perú nos hizo un presupuesto para la implementación de una configuración de este tipo, a continuación se detalla la propuesta.

El diseño propuesto se indica en la figura 6.2

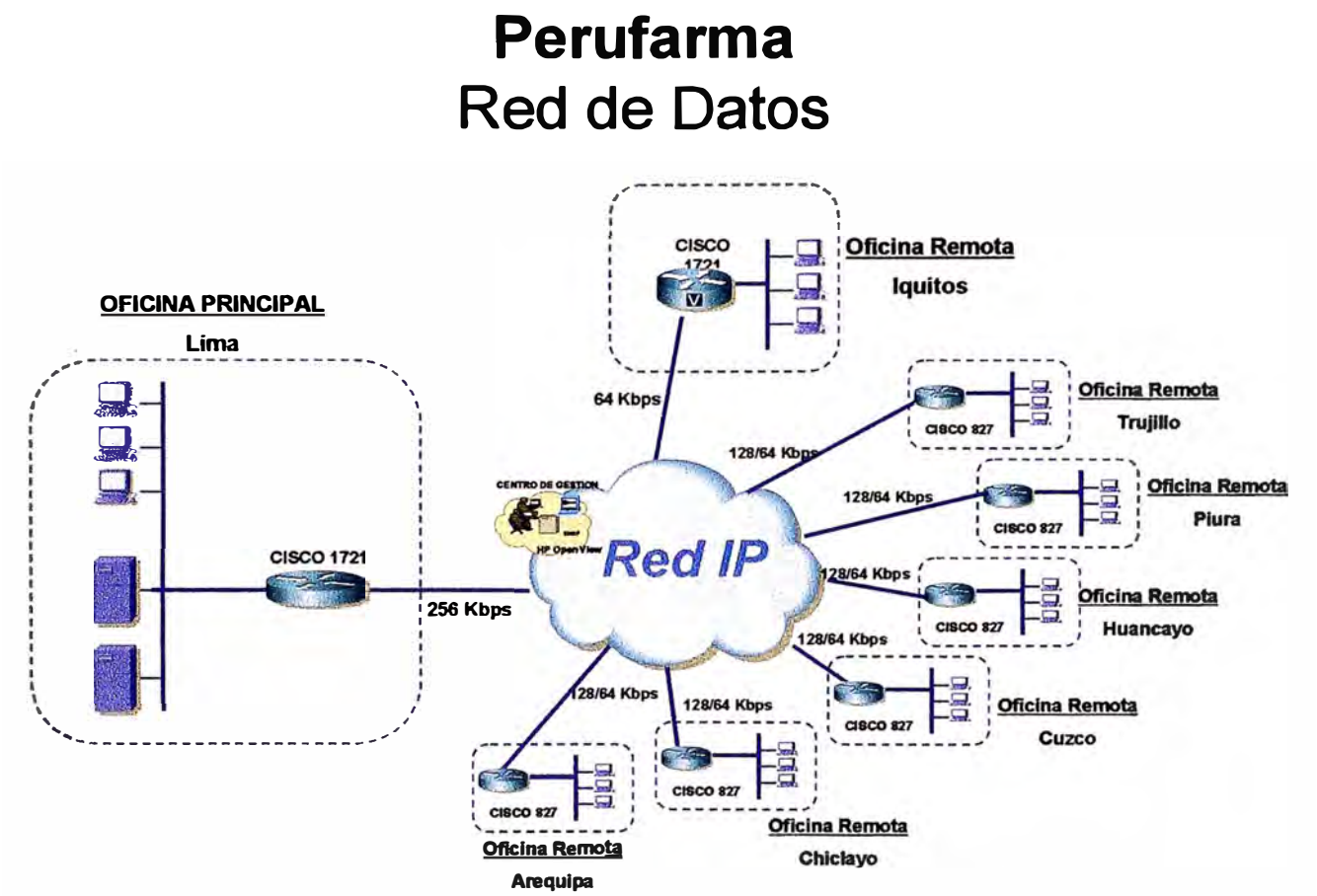

Fig. 6.2.: Red IP-VPN propuesta por Telefónica empresas.

Este diseño contemplaba el uso de:

- Enlace IP-VPN simétrico en el local central, con velocidad de 256 Kbps
- Enlace IP-VPN simétrico en la oficina de Iquitos, con velociad de 64Kbps
- Enlace IP-VPN con acceso ADSL en cada una de las demás oficinas de provincias (Arequipa, Chiclayo, Cuzco, Huancayo, Piura, Trujillo), con velocidad de 128/64 Kbps.

En ésta evaluación no se incluyó a la oficina sucursal de San Isidro.

La ventaja de este tipo de enlace está en que se garantiza un caudal de tráfico mínimo, el cual según la elección, deberá permitir satisfacer las necesidades de

comunicación entre los distintos locales. Más aún, pueden manejar la priorización de tráfico de voz y video de ser necesario.

La seguridad se asume que es garantizada por el proveedor, ya que él será quien genere el tunelamiento y aplicará las políticas de seguridad de interconexión entre los equipos que conformen los enlaces VPN a fin de mantener toda la transmisión de datos aislada de posibles interferencias y/o ataques.

Para ésta opción, los costos resultaron ser sumamente elevados, teniéndose (como resumen) lo siguiente[2]:

- Costos de instalación (total) **US$ 3,610.00**
- Costos de renta mensual (total) **US$ 3,690.00**

Estos costos estaban sujetos a la firma de contrato por 3 años, y dependientes de las facilidades técnicas que existan.

Como se puede apreciar, los costos de renta mensual por implementar una red IP_VPN como la sugerida, resultaban en un gasto anual aproximado de **US$ 44,280.00**. Esta opción quedó descartada por superar ampliamente las expectativas de inversión de la empresa.

6.1.4. Opción 4: Enlaces VPN sobre Internet

El crecimiento acelerado de la Internet durante los últimos años, ha dado como resultado que actualmente existan diversos modos de poder acceder a conectarse a ella. Ya no es novedad los juegos en red, "chatear" con gente de otros países, acceder a información de diverso tipo de una manera muy sencilla. Por ello, y dado que ahora existen protocolos de tunelamiento y encriptación que permiten establecer un buen nivel de seguridad y confidencialidad en la transmisión de datos a través de medios públicos, es que la Internet puede ser utilizada precisamente como un posible medio de conexión para transmisión de datos a nivel corporativo.

Analizando la posibilidad de usar este medio para el objetivo deseado, consideramos lo siguiente:

- La red de la oficina central de Perufarma ya poseía servicio de acceso a Internet, con velocidad de 256 Kbps, simétrico.

---

[2] Los costos que aquí se mostrarán son de Agosto del 2004, y solo mostraremos costos globales

- La red de la oficina de San Isidro, contaba con servicio de acceso tipo Speedy Business Class (enlace asimétrico), con ancho de banda 512 / 128 Kbps, garantizado al 30% del ancho de banda
- Las demás oficinas no contaban con enlaces adecuados para este tipo de conexión. Solo las oficinas de Trujillo y Chiclayo contaban con acceso a internet inalámbrico vía Millicom pero el ancho de banda era de 32 Kbps, con 30% del ancho de banda garantizado. Esto daba como resultado que las conexiones al servidor de terminales fuesen inestables.

Realizando un primer ejercicio de costos involucrados en la implementación de una posible "red" basada en enlaces VPN a través de medios públicos (como Internet), pudimos obtener lo siguiente:

Tabla 6.1. Costo mensual enlaces a Internet, diversas oficinas.

Oficina	¿Acceso dedicado?	Costo mensual (US$) a Enero 2004 (con IGV)	Ancho de banda (Kbps)	Tipo
Of. Principal, Lima	Si	1,205.00	256	Simétrico 2:1
Of. San isidro	Si	416.17	512 / 128	Speedy class (30%)
Of. Trujillo	Si	107.10	32	Millicom (30%)
Of Chiclayo	Si	107.10	32	Millicom (30%)
Of. Arequipa	No	-	-	
Of. Huancayo	No	-	-	
Of. Cuzco	No	-	-	
Of. Piura	No	-	-	
Of. Iquitos	No	-	-	
Total mensual (Enero 2004)		**US$ 1,835.37**		

Los costos involucrados con los servicios de Internet dedicado en la fecha de evaluación eran aceptables desde un punto de vista financiero, siempre que estos se utilizaran prioritariamente para proveer los servicios de comunicación antes que los de navegación por Internet, que para la empresa pasaba a ser un tema no prioritario. Este último servicio debería quedar restringido solo al personal que requiere el uso de este recurso como parte de su trabajo diario.

6.2. Proceso de implementación de los enlaces

Luego de haberse analizado las diferentes opciones, se decidió por la implementación de un sistema de comunicaciones basado en enlaces VPN a través de Internet, ya que se notaba que los montos de inversión eran aceptables.

Se acordó que los enlaces dedicados a Internet fuesen cambiados y establecidos con un solo proveedor, con el fin de trabajar únicamente sobre la infraestructura de dicho proveedor. Esto se decidió debido a que con la configuración actual, todas las comunicaciones tenían que pasar por el NAP, punto que podría influir en la velocidad de comunicación precisamente en horas punta.

A la fecha de tomar esta decisión, los proveedores de servicio Internet dedicado con quienes se había implementado el sistema de comunicaciones que operaba en esos momentos, mantenían aún contratos con la empresa. Se decidió entonces planificar los cambios de manera paulatina, cancelando los convenios según convenga y planificando la migración respectiva a fin de que las operaciones diarias no se viesen interrumpidas en ningún momento.

6.2.1. Primeras tareas

Como punto de partida, se realizaron las siguientes tareas:

- Carta de no renovación de contrato de servicio dedicado a Internet, para el local central (ubicado en Lima – Cercado), con el proveedor que en ese momento brindaba el servicio: AT&T. Esto se realizó en Febrero del 2004
- Contratación de nuevo servicio dedicado a Internet, para el local central, con Telefónica del Perú. El contrato se firmó en Febrero del 2004, acordándose la instalación del servicio InfoInternet, de 512 Kbps [3]. Esta instalación se completó a fines de Marzo del 2004.
- Instalación de servicio Internet dedicado en la oficina de Arequipa, en Agosto del 2004.
- Instalación de servicio Internet dedicado en las oficinas de Cuzco y Piura, en Octubre del 2004
- Carta de no renovación por el servicio de acceso dedicado a Internet, dirigida a Millicom S.A., correspondiente a las oficinas de Trujillo y Chiclayo; en Octubre del 2004. El servicio estuvo vigente hasta Noviembre del mismo año.
- Instalación de servicio Internet dedicado en las oficinas de Trujillo y Chiclayo, en Noviembre del 2004.

---

[3] Es preciso acotar que el ancho de banda inicial de este enlace se acordó que sería de 256 Kbps, el cual se cambiaría a 512 Kbps luego de 3 meses, en los cuales se debería confirmar la buena operación de éste nuevo enlace.

En todas las oficinas de provincia (excepto en la oficina de Iquitos) se instaló el servicio dedicado a Internet Speedy Business, modalidad 400 / 128 Kbps. Este servicio sería modificado por Telefónica el año siguiente, quedando en la modalidad de 900 / 256 Kbps en todas las oficinas mencionadas.

En el local central, se implementó un enlace InfoInternet dedicado, de 512 Kbps, simétrico y con "overbooking" 1:1.

Para todos los casos, la instalación del nuevo servicio precedía al retiro de los equipos del proveedor anterior. En el caso del local central, el cambio de proveedor implicó el cambio de las direcciones IP públicas, por lo que se tuvo que realizar coordinaciones e instalaciones temporales adecuadas con el fin de que ninguno de los servicios - tales como el servicio de correo, acceso a servicios de Terminal (via VPN) - tuviese problemas.

A medida que se avanzaba con los primeros cambios, todas las nuevas conexiones permitían que los usuarios de éstas oficinas se conectaran directamente al servidor de Terminales vía el servicio Routing & Remote Access Server (RRAS) implementado en el mismo equipo. Los enlaces VPN que se mantenían implementados estaban basados en protocolo PPTP. El acceso a este servidor de Terminales les permitía acceder a uso del sistema ERP que la empresa tiene en el local central..

Tal como se esperaba, el cambio de los enlaces dedicados trajo como consecuencia que la estabilidad de los mismos fuese notoria; los usuarios no reportaban problemas de pérdida de conexión ni "caída del enlace", por tanto, podían trabajar sin mayor inconveniente. Los inconvenientes por "caída" de los enlaces ADSL (Speedy), sucedían pero con muy poca frecuencia.

A Diciembre del 2004, el estado de implementación de enlaces dedicados era el siguiente:

Tabla 6.2.: Costos mensuales acceso a Internet, finales del 2004

Oficina	Fecha de instalación	Costo mensual US$ (incluído IGV)	Ancho de banda (Kbps)	Tipo
Of. San isidro	*Anterior al 2003*	416.17	512 / 128 Kbps	ADSL, 30%
Of. Lima	Marzo 2004	951.00	512	Simétrico, 1:1
Of. Arequipa	Agosto 2004	116.00	400 / 128	ADSL, 10%
Of. Huancayo	Agosto 2004	116.00	400 / 128	ADSL, 10%
Of. Piura	Octubre 2004	116.00	400 / 128	ADSL, 10%
Of. Cuzco	Octubre 2004	116.00	400 / 128	ADSL, 10%
Of. Trujillo	Noviembre 2004	116.00	400 / 128	ADSL, 10%
Of Chiclayo	Noviembre 2004	116.00	400 / 128	ADSL, 10%
Of. Iquitos	No	-	-	
Costo mensual total (actual)		**US$ 2,063.17**		

6.2.2. Adquisición de hardware

Luego de los cambios realizados durante el año 2004, y habiéndose comprobado que los resultados fueron los esperados en cuanto a costo y operación; se procedió a evaluar productos Firewall / VPN que pemitieran completar el proyecto.

Se procedió entonces a la evaluación de productos Firewall / VPN que nos permitieran, en base a un monto de inversión no muy elevado, completar la implementación de los enlaces VPN. Es en este momento en donde se elige IPSec como protocolo de base para ésta implementación, ya que resultaba ser el protocolo que mejores características de seguridad brindaba.

a) Evaluación de equipos Firewall / VPN

La empresa contaba al año 2004 con dos Firewalls:

- Un Firewall para la oficina central, en el cercado de Lima, implementado sobre un equipo IBM Netfinity 3000, con 192 MB RAM y 9.1 GB de espacio en disco (dos discos de 9.1GB cada uno en espejo). Este equipo mantenía instalado el software Firewall Gauntlet v5.5 for Windows NT 4.0. Este producto, ya era obsoleto y no existía la posibillidad de actualización de "parches", ya no poseía soporte y por tanto debería ser reemplazado.
- Un Firewall para la oficina sucursal de San Isidro, implementado sobre un equipo IBM PC 300GL, con 128MB RAM y 10GB de disco (IDE).

Este equipo mantenía instalado el mismo software de seguridad, Firewall Gauntlet v5.5 for Windows NT 4.0.

Se evaluó entonces productos equivalentes a fin de encontrar su opción de reemplazo. El equipo que fuese elegido, debería tener soporte para configurar VPNs bajo IPSec Se hicieron pruebas con diversos productos, y se analizó los costos de cada uno de ellos. La siguiente tabla comparativa muestra las características y costo referencial de cada producto evaluado:

Tabla 6.3: Cuadro comparativo de productos firewall

	Applicartion proxies Circuit Level Proxy Packet Filter	Checkpoint (Firewall 1)	Cisco PIX	Sonicwall	Linux Proxy Linux iptables/ netfilter + Fresswan
Precios	Producto + instalación	> US$ 19,000	US$ 8,250	US$ 5,550	US$ 2,500
	Costo de Soporte 24 x 7 (anual)	US$ 2,100	US$ 1,200	US$ 1,051	US$ 1,000
Características	Consola de Administración	gráfica	gráfica / texto	gráfica	Texto
	VPN	incluida	incluida	incluida	-
	NAT	Soportado	Soportado	Soportado	Soportado
	Throughtput	-	~ 188 Mbps	~ 190 Mbps	-
	Bandwidth management	No	No	Si	No
	User level authentication	Si	No	Si	-
	Stateful Packet inspection	Si	Si	Si	Si
	High Availability (fail over) option	Opcional	Opcional	Si	No
	Antivirus protection	Si	No	Integrada con McAfee	Opción de McAfee
	Servicios, protocolos y aplicaciones preconfigurados	> 240	Los más conocidos	Los más conocidos	Los más conocidos
	Facilidad de respaldo	Si	Si	?	Si
	Posibilidad de recuperación ante falla grave del equipo	Instalación en otra PC	Reemplazo del equipo	Reemplazo del equipo	Instalación en otra PC
Requerimientos	Requerimiento de HW + SW	SW S.O. + PCs	ninguno	ninguno	Dos PCs x local
Actualización y mantenimiento	Actualización (solo updates) Mantenimiento (nuevas versiones + updates)	Pago anual	Gratuita	> US$ 900	Gratuita -
Instrucción	Necesidad de curso para su administración	Si	Si	Si	Si
	Inversión por curso de entrenamiento para administración de Firewall	US$ 600	US$ 1500	Incluído	US$ 300
Opciones adicionales que son necesarias	IDS	No	No	No	-
	Proxy	Si	No	No	-
	Filtro de contenido	No	No	Incluído (nivel básico)	-
Comentario	Cubre requerimientos actuales de Perufarma y permite escalabilidad	Excede	Parcialmente	Parcialmente	Si

Los costos indicados en la tabla corresponden a la fecha de evaluación, mediados del 2004. Los productos que se evaluaron fueron:

Firewall-1, de Checkpoint

Cisco PIX Mod. PIX-515E-R-DMZ-BUN

Sonicwall Pro2040

Firewall basado en Linux, con iptables / netfilter y Freeswan para configuración de VPN con IPSec

Luego de examinar los detalles, se decidió por los productos de marca **Sonicwall.**

Dado que los productos a reemplazar serían los Firewall de las oficinas del cercado de Lima y San Isidro, se eligió el producto **Sonicwall Pro2040** para la oficina principal, y el producto **Sonicwall TZ170** para la oficina de San Isidro, en donde la cantidad de usuarios es pequeña.

6.2.3. Proceso de instalación de Firewalls

Se inició la tarea de levantamiento de información con respecto a la configuración de cada uno de los equipos Firewalls que se encontraban operativos a la fecha, en cada caso, se detalló cada parámetro de configuración con el fin de que esto se reflejase en los nuevos equipos.

Se preparó una documentación completa de las reglas de acceso configuradas en el firewall que se estaba retirando, basados en esta información, se realizó la configuración de los nuevos equipos. No la incluimos aquí por no ser relevante para efectos de la configuración de los enlaces VPN, tema central del presente informe.

a) Instalación de los equipos Firewall

Los equipos Firewall estuvieron disponibles a fines de Febrero del 2005, por lo que se programó la instalación de ambos equipos en el mes de Marzo de ese año.

- **Instalación de equipo Sonicwall Pro2040**

Este equipo se instaló en el local central de Perufarma, para su instalación se estableció inicialmente la configuración de red que se muestra en la Fig. 6.3

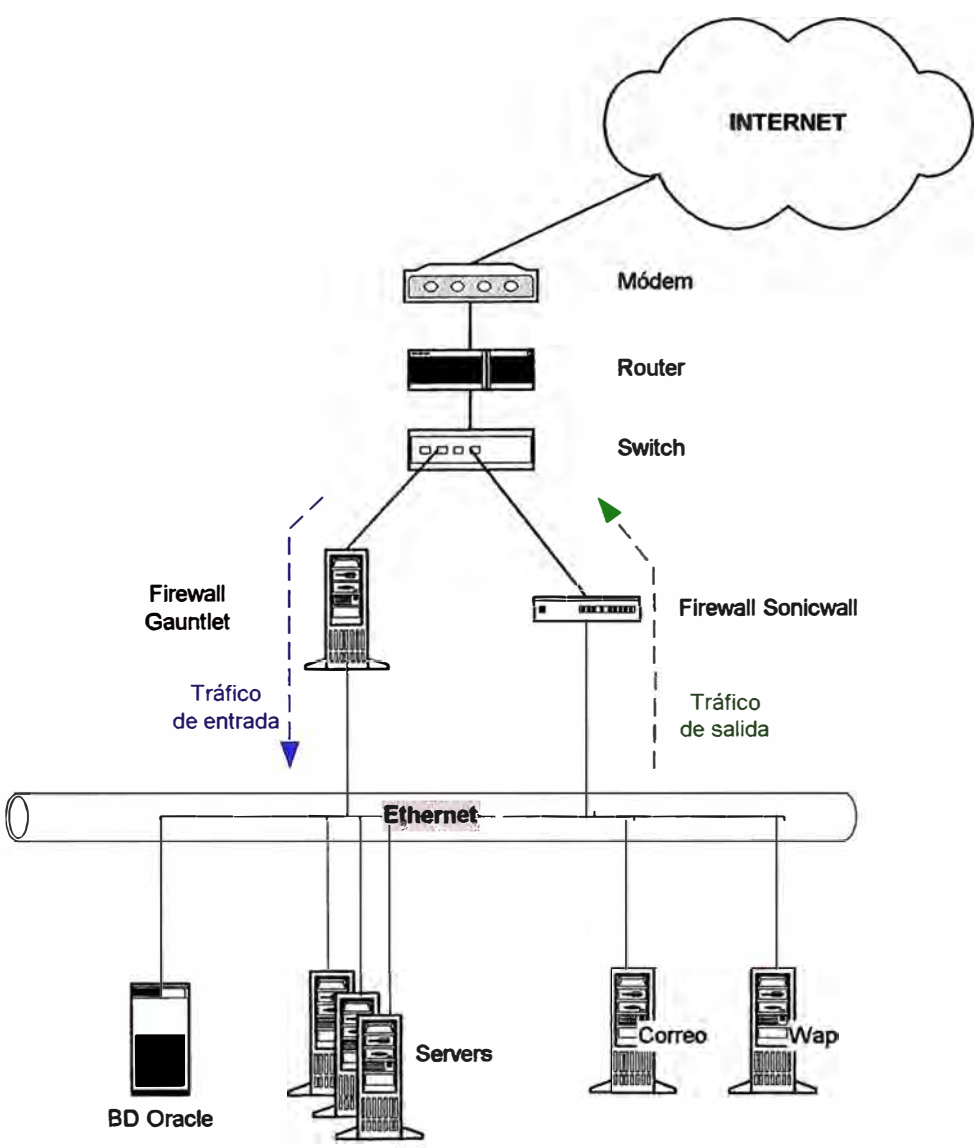

Fig. 6.3.: Configuración de red para proceder al cambio de equipos.

Se replicó la configuración del firewall anterior en el nuevo equipo, a fin de que podamos orientar el tráfico de salida por el nuevo equipo, y el tráfico de ingreso por el equipo que sería retirado en breve, esto evitaba que las operaciones se viesen afectadas y nos permitía probar la estabilidad del nuevo equipo. El tráfico de salida estaba compuesto básicamente por tráfico HTTP, FTP y SMTP, relativo a los procesos de navegación por Internet y el servicio de correo. El tráfico de entrada estaba compuesto por tráfico HTTP y SMTP, relativos al servicio WAP y el ingreso de mensajes hacia nuestro servidor de correo electrónico.

Esta configuración se mantuvo por el lapso de dos semanas a fin de verificar la estabilidad del nuevo equipo, luego de ello, se completó el cambio.

- **Instalación de equipo Sonicwall TZ170**

Para instalar este equipo se replicó la configuración del servidor Firewall anterior, similar a lo que se hizo en el Firewall Sonicwall de la Of. Central. En este caso, dado que en la red LAN de la oficina sucursal de San Isidro solo se ubican pocos usuarios, y no se tienen servicios adicionales, el cambio fue muy simple y casi inmediato.

6.2.4. Configuración de enlace VPN Site-to-Site

Una vez completada la etapa de instalación de los nuevos equipos Firewall, se procedió a la configuración de los enlaces VPN. Se inició por la configuración del enlace Site-to-Site entre la oficina del cercado de Lima (local central) y la oficina sucursal de San Isidro. Tal como se había mencionado, la implementación se basaría en el protocolo IPSec, por ser uno de actuales estándares de la industria en materia de enlaces seguros VPN.

a) Configuración de enlace site-to-site

Para esta configuración se definieron los siguientes parámetros tomando en cuenta recomendaciones de Sonicwall [REF 9]:

Modo de negociación de intercambio de llaves (*keying mode*)	IKE Preshared secret
Modo de intercambio de llaves (*IKE mode*)	Main Mode
Modo de autenticación SA (*SA Authentication mode*)	Preshared key
Grupo de negociación de intercambio de llaves (*keying group*)	DH (Diffie-Hellman) Group 2
Cifrado e integridad de datos	ESP 3DES con SHA1

- **Configuración lado oficina central (Cercado de Lima)**

El producto Sonicwall presenta una interfase Web que sirve para la administración del equipo, siguiendo las recomendaciones del fabricante, se configuraron los parámetros del enlace:

- Keying mode: IKE, usando *pre-shared secret*
- IPSec primary gateway: 201.230.66.148 (*Dirección IP pública del enlace a internet, oficina de San Isidro*)

- Destination network: 192.168.2.0 (*Dirección de red de LAN en Of. de San Isidro*)

Esta configuración se muestra en el gráfico de la Fig. 6.4

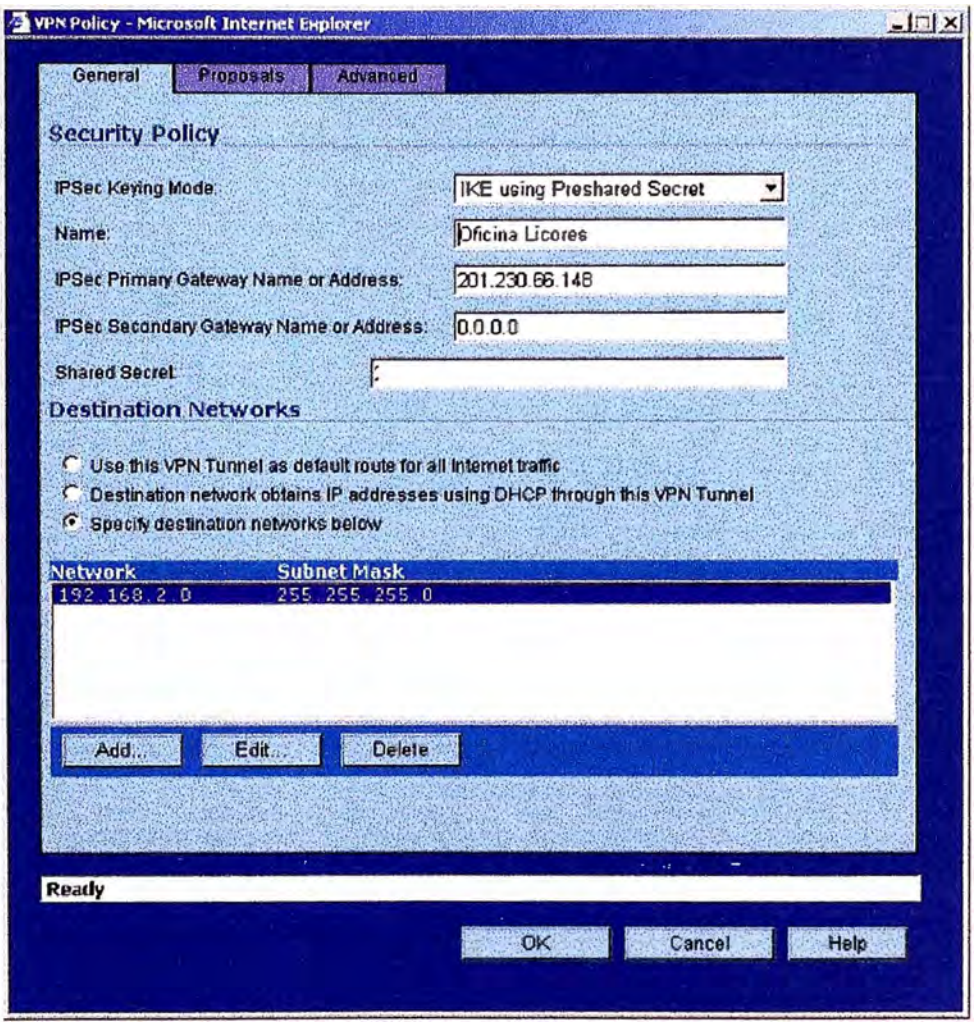

Fig. 6.4.: Configuración general de VPN en firewall Pro 2040 (Of. Central)

Por razones de seguridad, el parámetro "*Shared Secret*" se ha borrado de la figura 6.4.

En ésta primera parte, se configura la modalidad de negociación de intercambio de llaves, el nombre del enlace (aquí se ha colocado el nombre de la oficina sucursal de San Isidro, con el fin de poder reconocer a que oficina corresponde el enlace), la dirección IP del Gateway remoto (dirección IP pública de la oficina sucursal) a través del cual se envía el tráfico de datos, y la red LAN de destino

Luego se continúa con la configuración de los parámetros correspondientes a las fases de autenticación y cifrado:

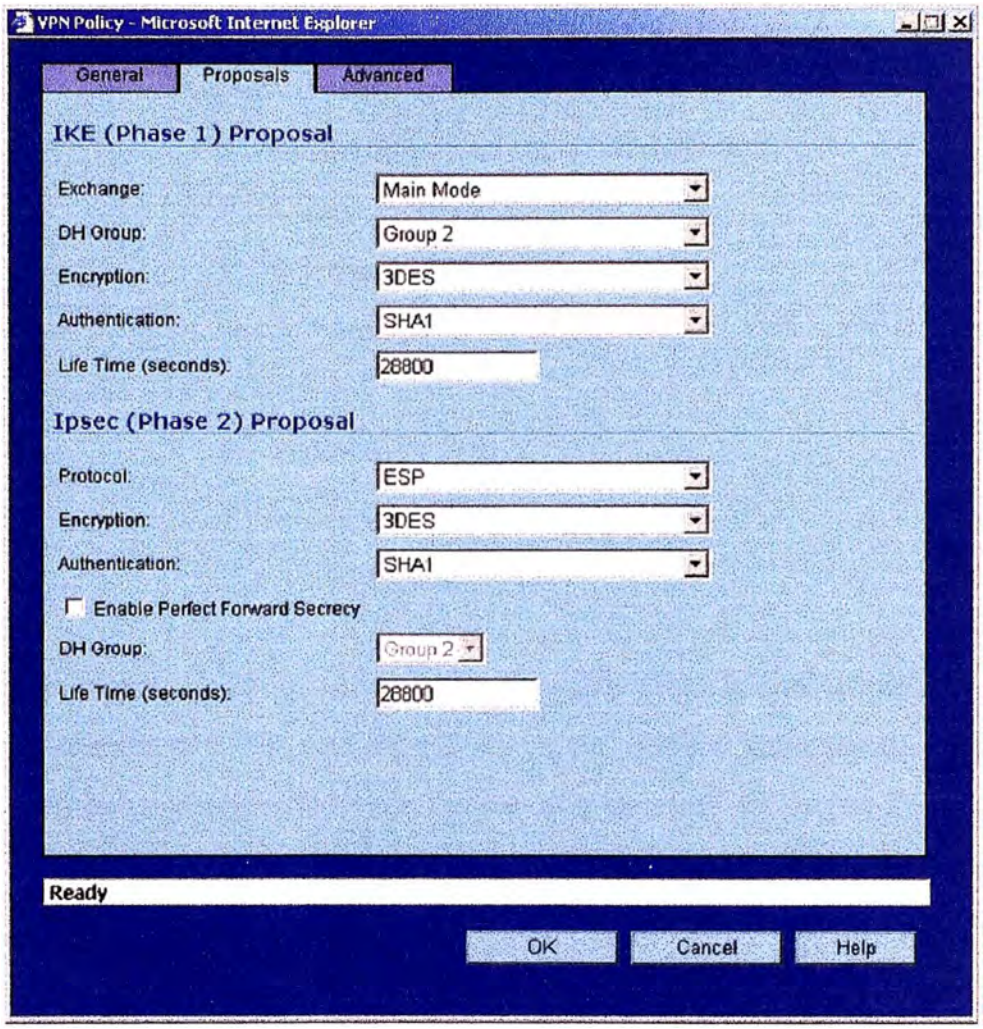

Fig. 6.5.: Configuración de parámetros de las Asociaciones de Seguridad (SA)

Una Asociación de Seguridad (*Security Association, SA*), como hemos visto, es una relación entre dos o más entidades que describe como las entidades utilizarán servicios de seguridad para comunicarse.

En la fase 1, IKE crea un canal autenticado y seguro entre dos puntos, esto se conoce como IKE SA (*IKE Security Association*). EL acuerdo en base a Diffie-Hellman siempre se realiza en esta fase. Con esto se crea un canal seguro para la negociación de los IPSec SA en la fase 2.

En la fase 2, IKE negocia la Asociación de Seguridad IPSec (*IPSec Security Association*) y genera el material clave requerido para el IPSec SA. Un

nuevo acuerdo Diffie- Hellman se realiza en esta etapa, o las claves se derivan del "shared secret" usado en la fase 1

En esta parte de la configuración se inscribieron los siguientes parámetros:

- IKE fase 1:
  - Modo de Intercambio : Main mode
  - Diffie- Hellman Group : Group 2
  - Cifrado : 3DES
  - Autenticación : SHA1
- IPSec fase 2:
  - Protocolo : ESP
  - Cifrado : 3DES
  - Autenticación: SHA1

Finalmente, en el menú "avanzado" se completó la configuración tomando en cuenta que las conexiones desde la oficina sucursal de San Isidro servirían para que pudiesen accesar los recursos de la red LAN y DMZ (donde se encontraría el servidor de Terminales), se configuró para la terminación del enlace fuese en LAN/DMZ.

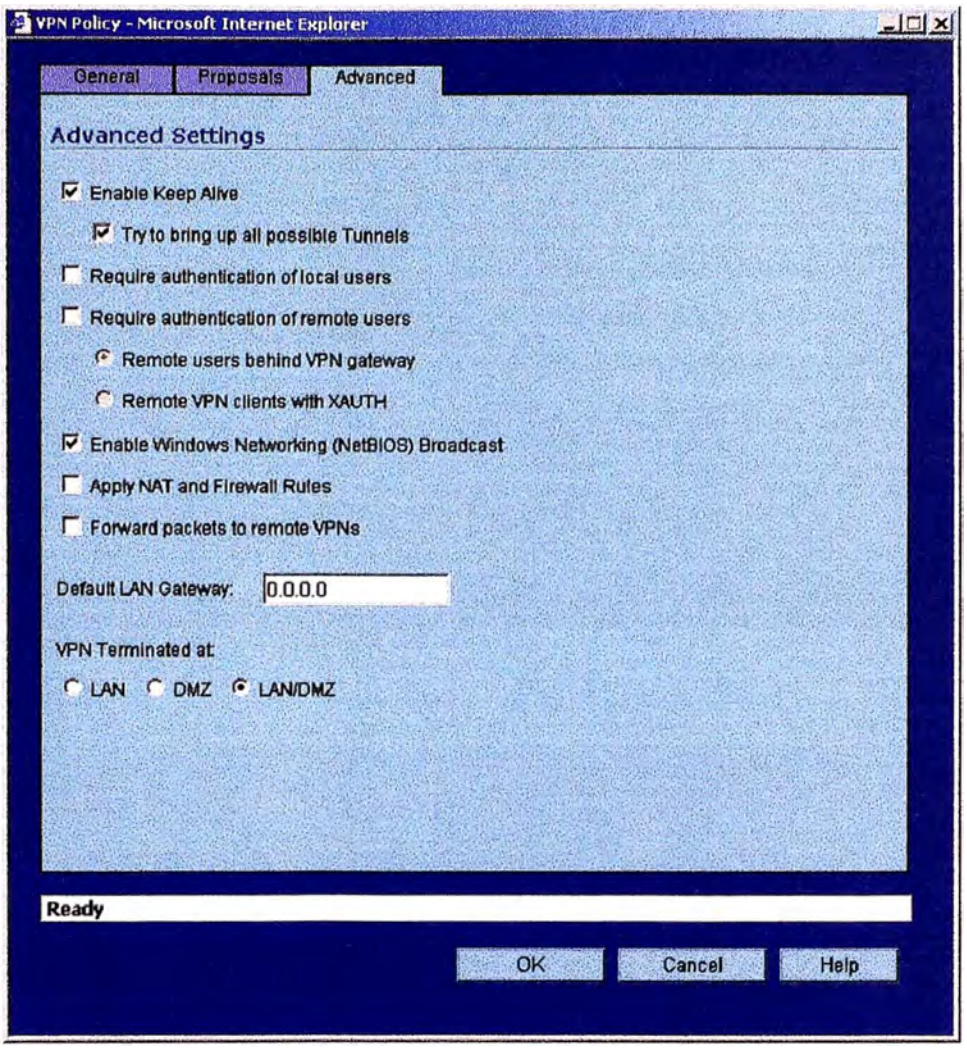

Fig. 6.6.: Configuración de parámetros avanzados

Con esto se concluía la configuración del equipo Sonicwall Pro 2040 en cuanto al enlace VPN corresponde.

- **Configuración lado oficina sucursal (San Isidro)**

En el lado de la oficina sucursal de San Isidro, se realizaron los mismos pasos, los cuales se muestran en la Fig 6.7.

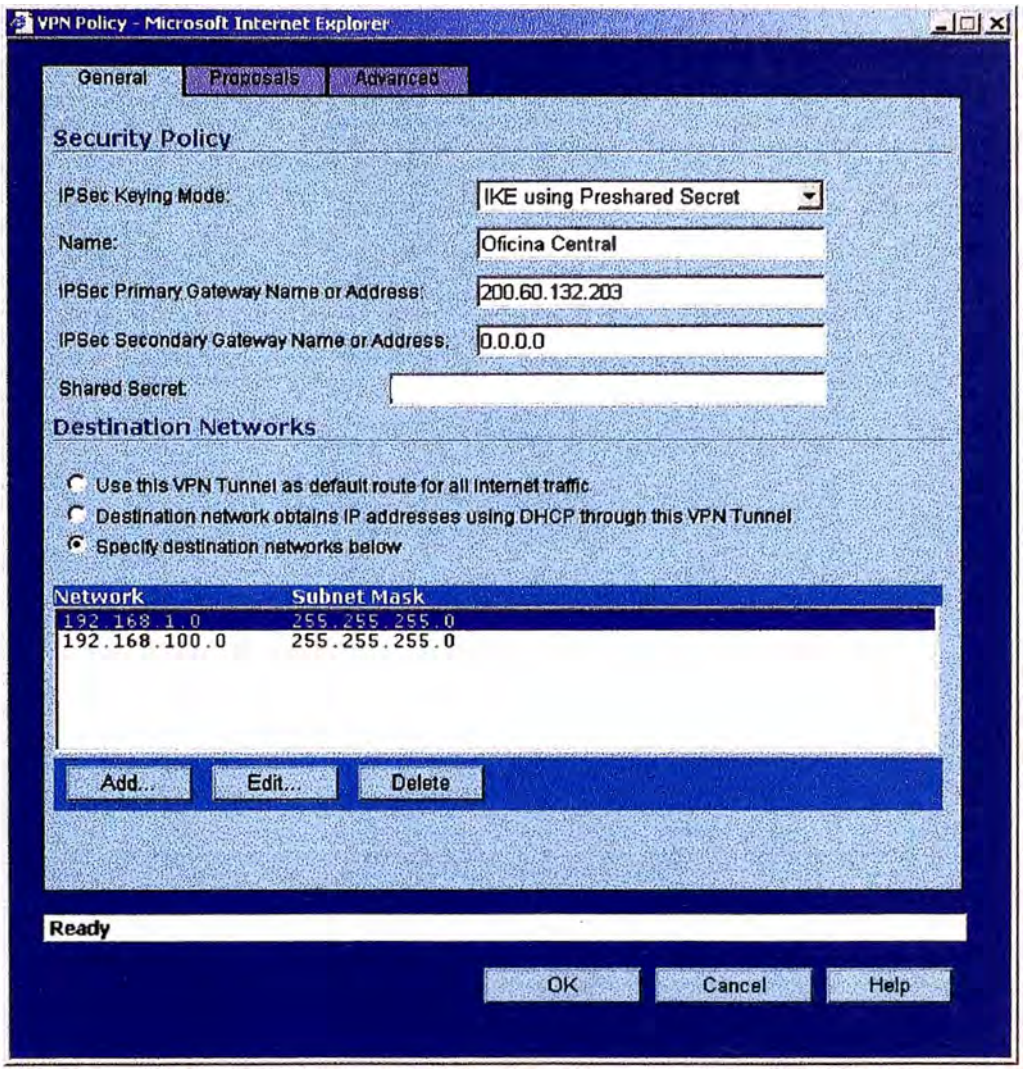

Fig. 6.7.: Configuración general de VPN en firewall TZ 170 (Of. San Isidro)

En ésta primera parte, se configura la modalidad de negociación de intercambio de llaves, el nombre del enlace (aquí se ha colocado el nombre de la oficina central, con el fin de poder reconocer a que oficina corresponde el enlace), la dirección IP del Gateway remoto (dirección IP pública de la oficina central) a través del cual se envía el tráfico de datos, y la red LAN de destino (en este caso las direcciones TCP/IP de la redes LAN y DMZ en la oficina central)

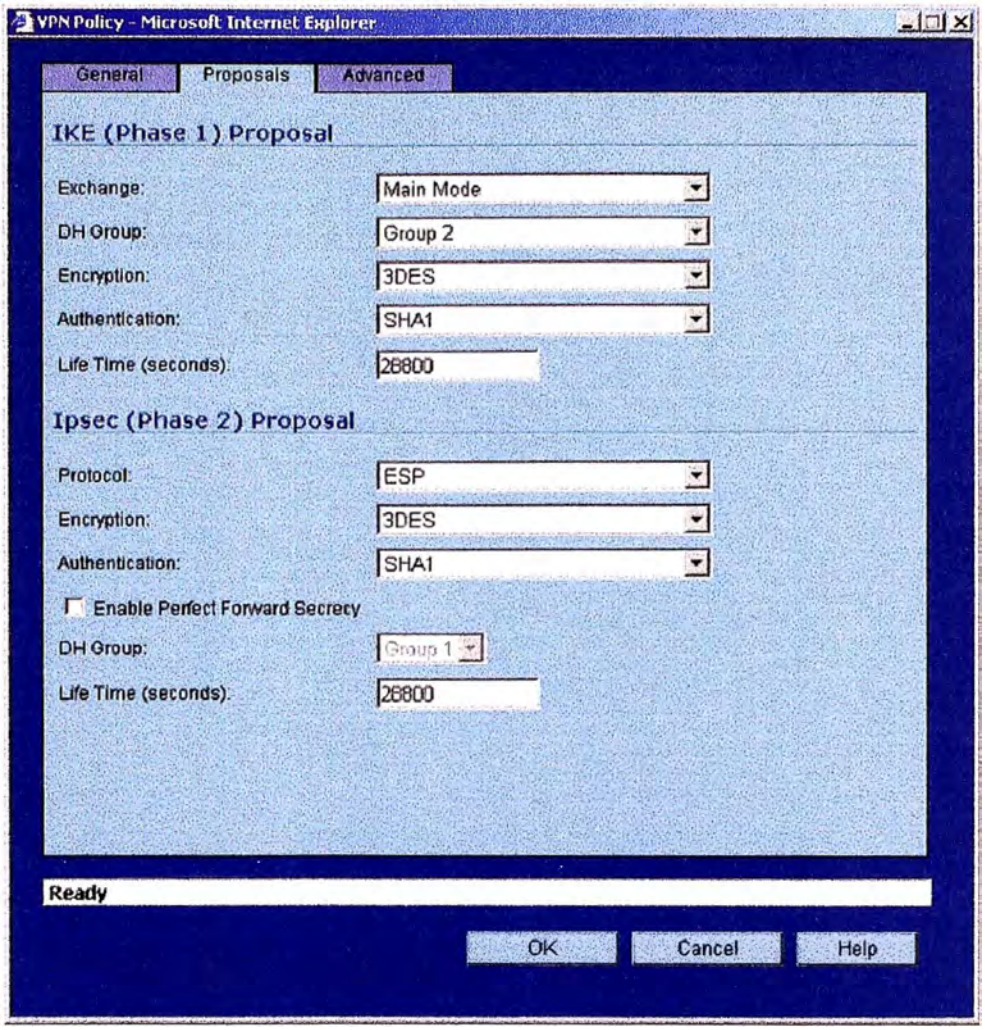

Fig. 6.8.: Configuración de parámetros de las Asociaciones de Seguridad (SA)

Luego se configuraron los parámetros del enlace VPN correspondientes a las Asociaciones de Seguridad (SA). Esto se muestra en la Fig 6.8

Finalmente, la configuración avanzada, se completaron los parámetros necesarios indicando que la terminación del VPN en este lado sería la red LAN, (no existe DMZ en la red de la oficina sucursal). Esto se muestra en la fig 6.9

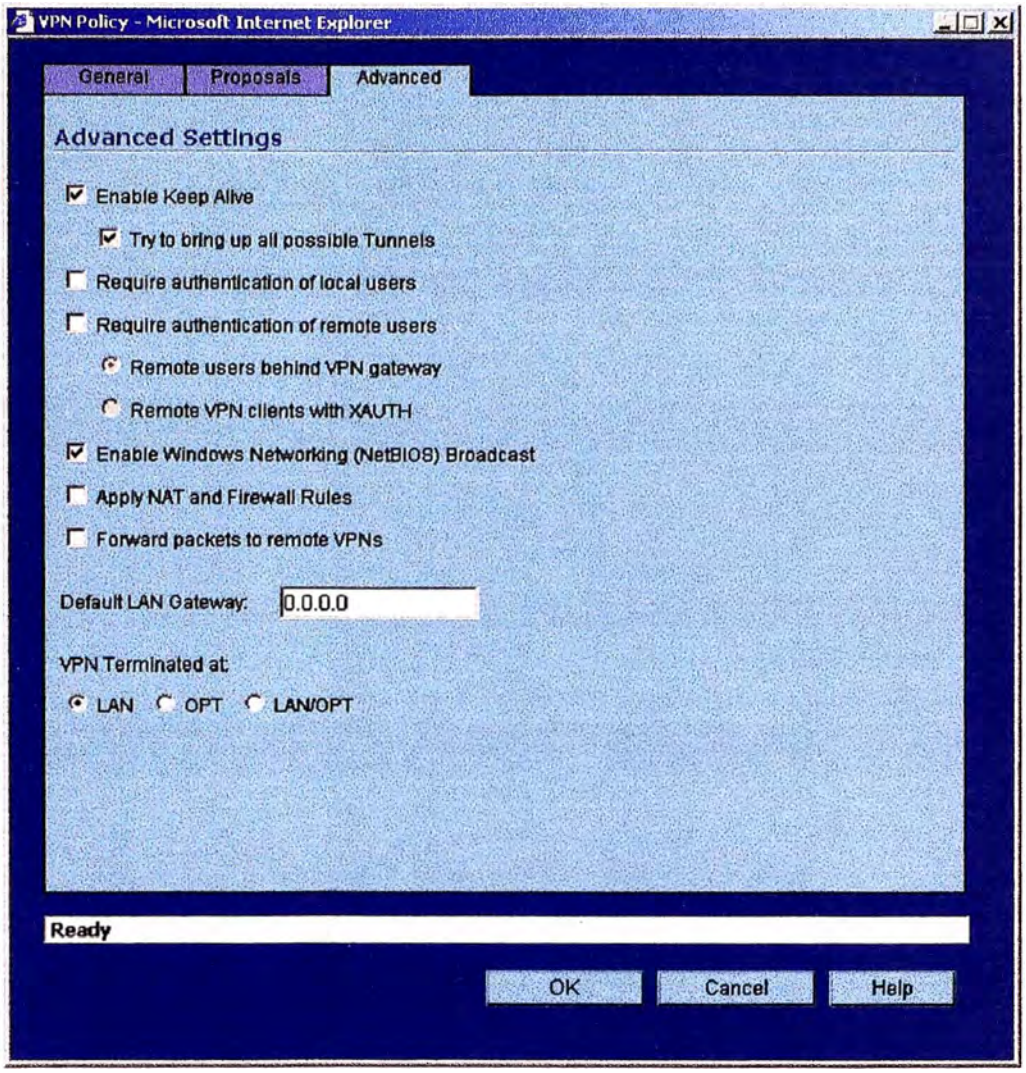

Fig. 6.9.: Configuración de parámetros avanzados

b) Verificación del enlace establecido

Una vez que se completó la configuración, el enlace se establece rápidamente, quedando las redes de datos de ambas oficinas interconectadas vía un enlace VPN bajo IPSec a través de Internet

La fig.6.10 muestra el estado de los enlaces a través del Web Management del Firewall TZ170, correspondiente a la oficina sucursal de San Isidro:

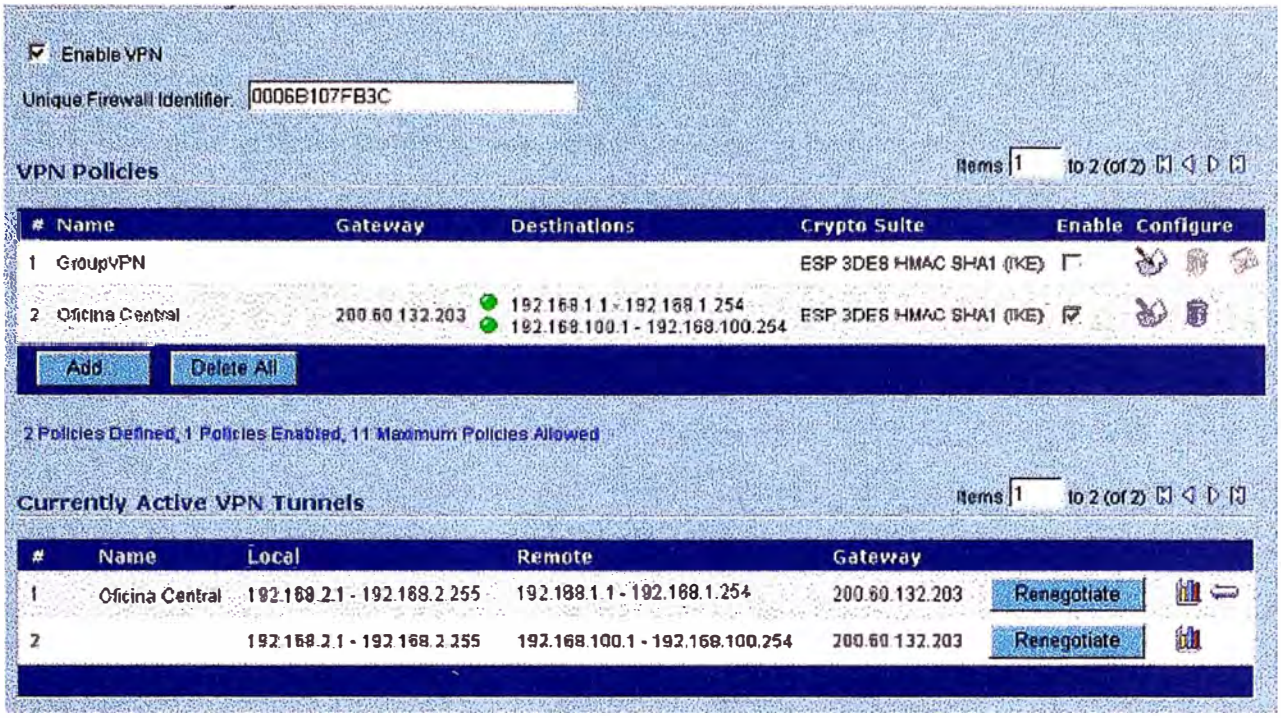

Fig. 6.10.: Estado del enlace VPN Site – to – Site

Se ha cortado esta imagen para poder visualizarla mejor, aquí se observa que el enlace está activo y está conectándose con la redes LAN y DMZ de la oficina central del cercado de Lima.

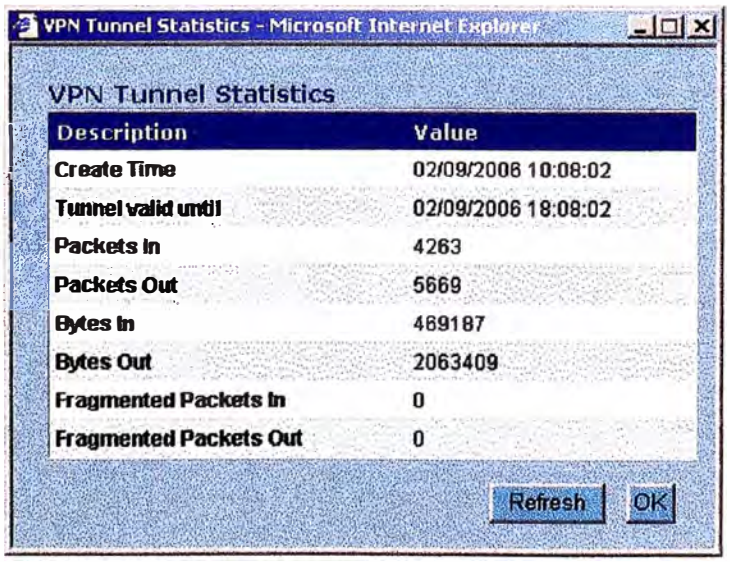

Fig. 6.11.: Estadísticas del enlace VPN Site – to – Site

Una muestra de las estadísticas del enlace establecido se puede observar en la Fig 6.11

Esta estadística ha sido obtenida en la fecha indicada, y se observa la hora de establecimiento del enlace y la hora hasta la cual es válido y en la cual se debe renovar el proceso de autentificación y validación. También se muestra el tráfico en cantidad de paquetes, bytes, y si existen o no paquetes fragmentados.

El proceso de establecimiento del enlace queda registrado en el "registro de eventos" del equipo, tal como se muestra en la figs.6.12, 6.13 y 6.14.

Aquí se observa que el inicio de autenticación del enlace se da en el registro 197, en el cual se registra: "IKE Responder Received Main Mode request (Phase 1)", aquí equipo Firewall de la oficina remota inicia el proceso, este concluye en el registro #192 "IKE Responder Main Mode complete (Phase 1)", luego viene "IKE Responder Received Quick mode request (Phase 2)", luego "IKE Responder: Accepting IPSec proposal (Phase 2)", luego "IKE negotiation complete, adding IPSec SA (Phase 2)".

Luego "IKE Responder Received Quick mode request (Phase 2)" – para el enlace al DMZ- luego "IKE Responder: Accepting IPSec proposal (Phase 2)", luego "IKE negotiation complete, adding IPSec SA (Phase 2)"

#	Date	Time	Message	Source	Destination	Notes
168	02/11/2006	12:02:55	TCP connection dropped	192.168.100.200, 3120, LAN, PERUFARM_RED.central.perufarma.com.pe	192.168.100.200, 25, LAN, PERUFARM_RED.central.perufarma.com.pe	TCP Port: 25
169	02/11/2006	12:02:42	SENDING>>>> ISAKMP OAK INFO (InitCookie 0xa933cacded3370ff, MsgID: 0x5D548F68) *(HASH, NOTIFY:DPD_ACK)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
170	02/11/2006	12:02:42	RECEIVED<<< ISAKMP OAK INFO (InitCookie 0xa933cacded3370ff, MsgID: 0x5CD0A0AE) *(HASH, NOTIFY:DPD_REQUEST)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
171	02/11/2006	12:02:36	Possible port scan dropped	67.72.120.62, 80, WAN	200.60.132.200, 42931, WAN	TCP scanned port list, 41864, 54717, 54959, 55267, 41864
172	02/11/2006	12:02:33	IKE negotiation complete. Adding IPSec SA (Phase 2)	200.60.132.203	201.230.66.148, client-201.230.66.148.speedy.net.pe	ESP:3DES, HMAC_SHA1, lifeSeconds=28800 Local SPI:0x78ca0376 Remote SPI:0x96913a0f
173	02/11/2006	12:02:33	IKE Responder: Accepting IPSec proposal (Phase 2)	201.230.66.148, client-201.230.66.148.speedy.net.pe	200.60.132.203	192.168.2.0/24 -> 192.168.1.0/24
174	02/11/2006	12:02:33	RECEIVED<<< ISAKMP OAK QM (InitCookie 0xa933cacded3370ff, MsgID: 0xFB087990) *(HASH)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
175	02/11/2006	12:02:33	Loading IPSec SA (Message ID = 0xfb087990, Local SPI = 0x78ca0376, Remote SPI = 0x96913a0f)			
176	02/11/2006	12:02:33	SENDING>>>> ISAKMP OAK QM (InitCookie 0xa933cacded3370ff, MsgID: 0xFB087990) *(HASH, SA, NON, ID, ID)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
177	02/11/2006	12:02:33	RECEIVED<<< ISAKMP OAK QM (InitCookie 0xa933cacded3370ff, MsgID: 0xFB087990) *(HASH, SA, NON, ID, ID)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
178	02/11/2006	12:02:33	IKE Responder: Received Quick Mode Request (Phase 2)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	

Fig. 6.12.: Registro de eventos, mostrando proceso de establecimiento del enlace VPN

#	Date	Time	Message	Source	Destination	Notes
179	02/11/2006	12:02:31	DNS packet allowed	192.168.100.216, 1080, LAN, perufarm_dc2.central.perufarma.com.pe	200.48.225.146, 53, WAN, huandoy.tdp.net.pe	UDP Port: 53
180	02/11/2006	12:02:21	UDP packet from LAN dropped	192.168.100.215, 53, LAN, perufarm_dc1.central.perufarma.com.pe	192.168.100.251, 4279, LAN	UDP Port: 4279
181	02/11/2006	12:01:53	TCP connection dropped	200.60.46.162, 3205, WAN	200.60.132.203, 139, WAN	TCP Port: 139
182	02/11/2006	12:01:42	SENDING>>>> ISAKMP OAK INFO (InitCookie 0xa933cacded3370ff, MsgID: 0x300E1784) *(HASH, NOTIFY:DPD_ACK)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
183	02/11/2006	12:01:42	RECEIVED<<< ISAKMP OAK INFO (InitCookie 0xa933cacded3370ff, MsgID: 0x73F7B199) *(HASH, NOTIFY:DPD_REQUEST)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
184	02/11/2006	12:01:30	IKE negotiation complete. Adding IPSec SA (Phase 2)	200.60.132.203	201.230.66.148, client-201.230.66.148.speedy.net.pe	ESP:3DES, HMAC_SHA1, lifeSeconds=28800 Local SPI:0x47aa74d2 Remote SPI:0x538ed3cd
185	02/11/2006	12:01:30	IKE Responder: Accepting IPSec proposal (Phase 2)	201.230.66.148, client-201.230.66.148.speedy.net.pe	200.60.132.203	192.168.2.0/24 -> 192.168.100.0/24
186	02/11/2006	12:01:30	RECEIVED<<< ISAKMP OAK QM (InitCookie 0xa933cacded3370ff, MsgID: 0x3C08E62B) *(HASH)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
187	02/11/2006	12:01:30	Loading IPSec SA (Message ID = 0x3c08e62b, Local SPI = 0x47aa74d2, Remote SPI = 0x538ed3cd)			

Fig. 6.13.: Registro de eventos, mostrando proceso de establecimiento del enlace VPN

#	Date	Time	Message	Source	Destination	Notes
188	02/11/2006	12:01:30	SENDING>>>> ISAKMP OAK QM (InitCookie 0xa933cacded3370ff, MsgID: 0x3C08E62B) *(HASH, SA, NON, ID, ID)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
189	02/11/2006	12:01:30	RECEIVED<<< ISAKMP OAK QM (InitCookie 0xa933cacded3370ff, MsgID: 0x3C08E62B) *(HASH, SA, NON, ID, ID)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
190	02/11/2006	12:01:30	IKE Responder: Received Quick Mode Request (Phase 2)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
191	02/11/2006	12:01:30	SENDING>>>> ISAKMP OAK MM (InitCookie 0xa933cacded3370ff, MsgID: 0x0) *(ID, HASH)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
192	02/11/2006	12:01:30	IKE Responder: Main Mode complete (Phase 1)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	3DES SHA1 Group 2 lifeSeconds=28800
193	02/11/2006	12:01:30	RECEIVED<<< ISAKMP OAK MM (InitCookie 0xa933cacded3370ff, MsgID: 0x0) *(ID, HASH)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
194	02/11/2006	12:01:30	SENDING>>>> ISAKMP OAK MM (InitCookie 0xa933cacded3370ff, MsgID: 0x0) (KE, NON, VID, VID, VID)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
195	02/11/2006	12:01:30	RECEIVED<<< ISAKMP OAK MM (InitCookie 0xa933cacded3370ff, MsgID: 0x0) (KE, NON, VID, VID, VID)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	
196	02/11/2006	12:01:29	SENDING>>>> ISAKMP OAK MM (InitCookie 0xa933cacded3370ff, MsgID: 0x0) (SA)	200.60.132.203, 500	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	
197	02/11/2006	12:01:29	IKE Responder: Received Main Mode request (Phase 1)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 62465	
198	02/11/2006	12:01:29	RECEIVED<<< ISAKMP OAK MM (InitCookie 0xa933cacded3370ff, MsgID: 0x0) (SA)	201.230.66.148, 500, client-201.230.66.148.speedy.net.pe	200.60.132.203, 500	

Fig. 6.14.: Registro de eventos, mostrando proceso de establecimiento del enlace VPN

6.2.5. Configuración de enlace PC – to - LAN

Para este caso, mostraremos la configuración de ejemplo que serviría para una PC remota.

a) Configuración de Servicio de acceso remoto

En este caso, el servidor de acceso remoto será el Firewall, el cual servirá como puerta de enlace (gateway) hacia la red LAN y sus recursos disponibles. Es necesario comentar en este caso que la configuración que se muestra a continuación será destinada únicamente a equipos remotos de usuarios móviles que se pre-configuren en la ciudad de Lima y para los cuales sea extremadamente necesario tener disponibilidad de acceso a los recursos centralizados a pesar de no encontrarse fisicamente en la Oficina central.

No recomendamos que este tipo de configuración se realice en PCs remotas sobre las que no podamos tener administración directa o sobre las cuales no se hayan aplicado políticas previas de seguridad, que garanticen que se efectuarán accesos únicamente a los recursos para los cuales se les ha autorizado.

Para PCs remotas que deban tener acceso a recursos específicos, se preparará la configuración de acceso únicamente a través de la zona DMZ.

- **Configuración de equipo Sonicwall en local central**

El equipo Sonicwall posee un cliente VPN y una metodología de configuración que facilita sustancialmente el proceso. Este cliente, el cual se denomina *Global VPN Client* requiere del uso de los servicios de un DHCP server.

Entonces, partimos configurando el servidor DHCP Server interno del equipo Sonicwall, tal como mostramos en la Fig. 6.15:

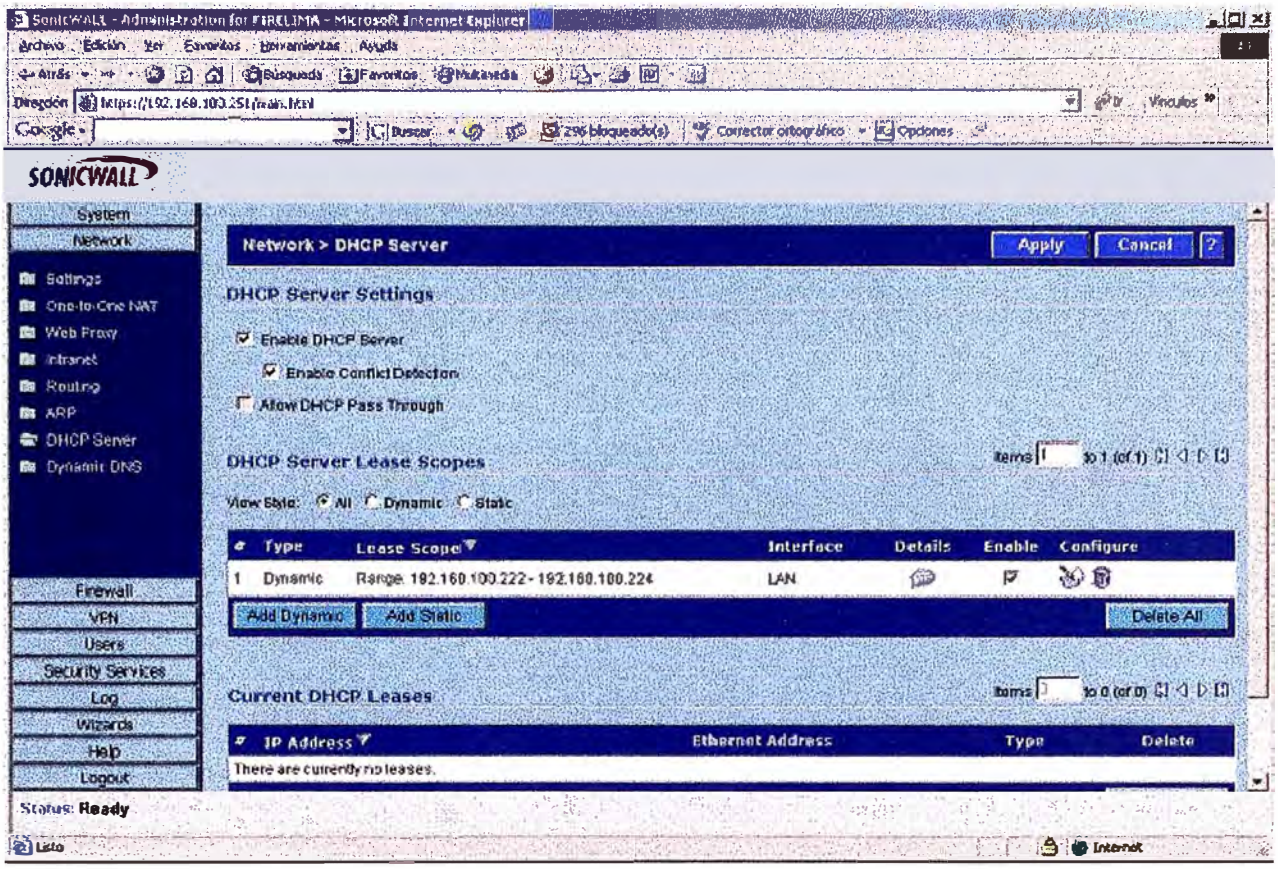

Fig. 6.15: Configuración de DHCP Server en equipo Sonicwall

Como se observa, se toma un rango dinámico de direcciones IP correspondientes a la red LAN del local central.

Luego se debe configurar la opción *DHCP over VPN* que posee el equipo, esto a fin de garantizar que una dirección IP dinámica le será asignada al PC remoto a través del canal seguro que se cree entre el equipo PC remoto y el equipo Sonicwall. La fig. 6.16 muestra el detalle de la configuración.

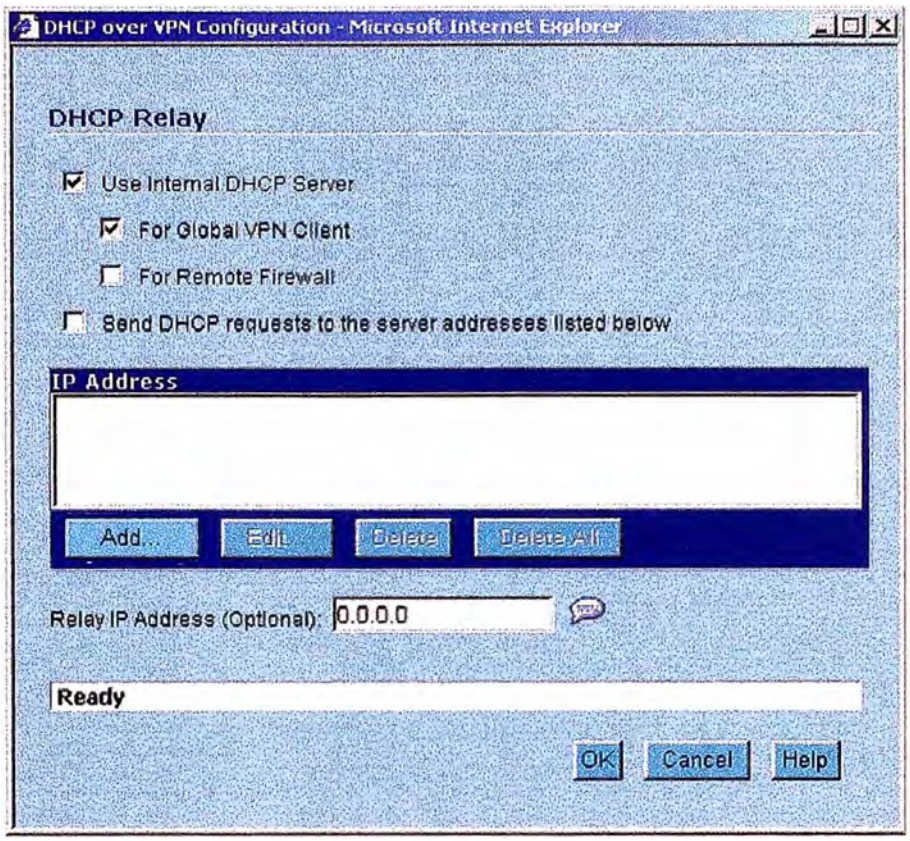

Fig. 6.16: Configuración de opción *DHCP over VPN*

Luego, es preciso configurar un medio de autenticación del usuario remoto, para ello definimos el uso de RADIUS. En este caso particular, el servicio ***IAS Server*** se ha habilitado en el Controlador de Dominio de la red Windows 2000 Active Directory que se encuentra en la oficina central. Este servicio brinda las prestaciones de un Servidor RADIUS con la ventaja que se valida en el Directorio Activo del dominio Windows 2000; por tanto, podemos tener gestión centralizada de los usuarios remotos.

En este documento no detallamos los pasos de configuración del Servicio ***IAS Server,*** pero estos pueden ser revisados en el siguiente link:

http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/ias.mspx

Es necesario configurar el equipo Sonicwall como cliente RADIUS, a fin de que los usuarios remotos se puedan validar en este servicio:

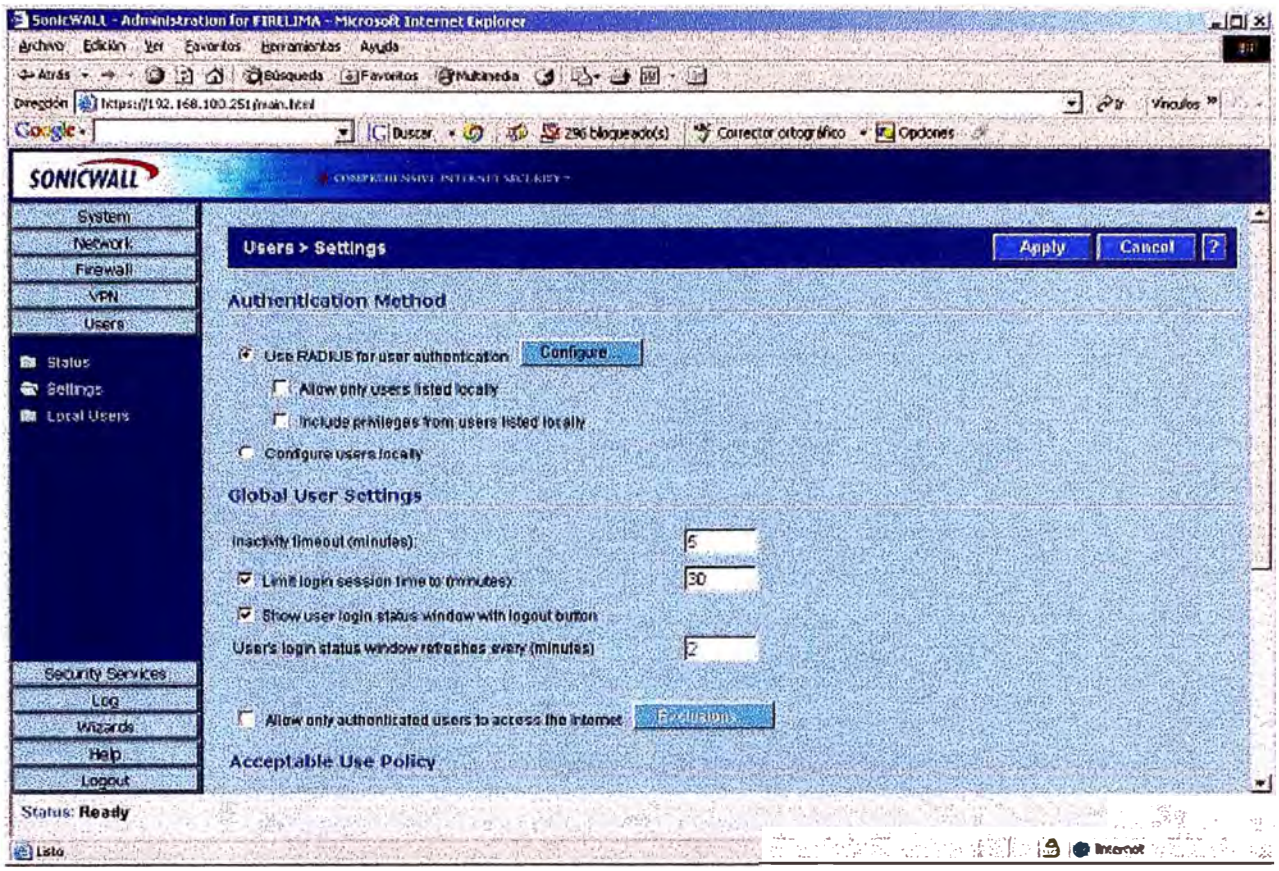

Fig. 6.17.: Activación del método de autenticación en el firewall

En la Fig. 6.17 se observa la etapa de configuración del método de autenticación, activamos la opción de usar RADIUS para autenticación, luego presionando el botón "configure" completamos los parámetros necesarios:

La fig. 6.18. muestra la configuración de los parámetros principales en el equipo Sonicwall para poder autenticar vía RADIUS, esencialmente la dirección IP del servidor RADIUS (en este caso, IAS Server) y el puerto a través del cual se realizará la comunicación, son definidos. Asimismo, se definen los valores de "timeout" (tiempo máximo de espera) y "retries" (reintentos).

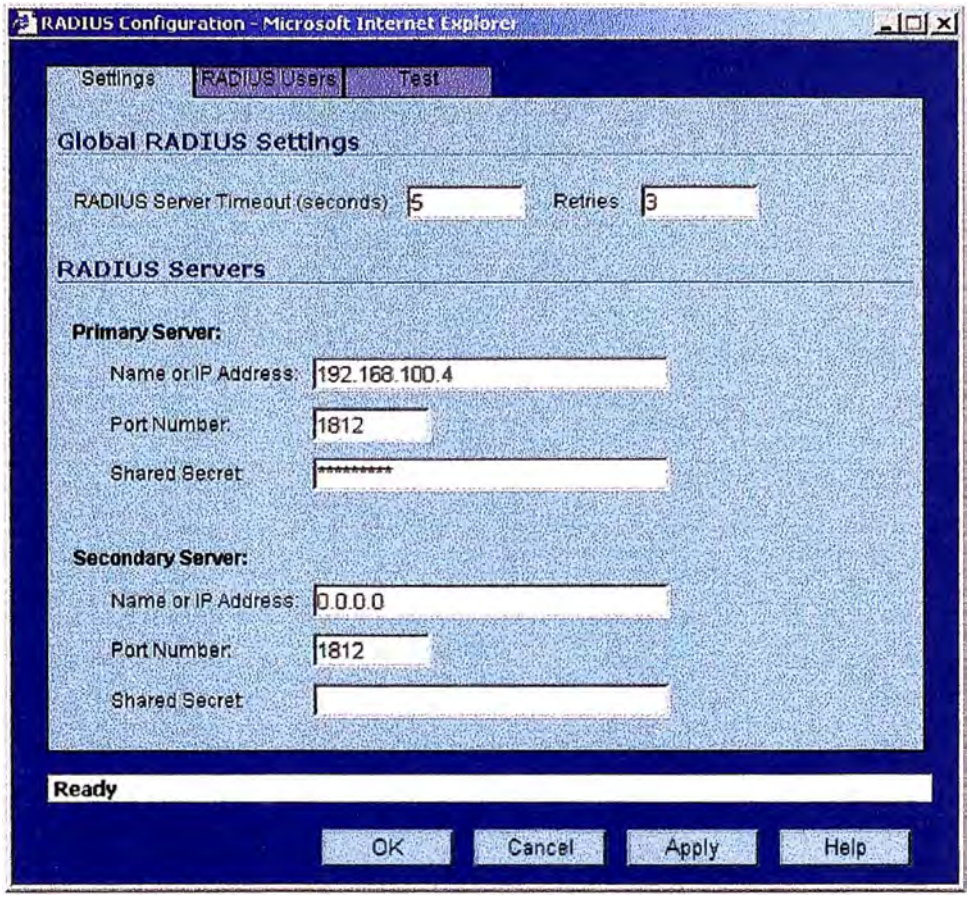

Fig. 6.18.: Parámetros configuración RADIUS en Sonicwall

Luego, se define que el acceso de los clientes se realizará vía el cliente VPN propietario del equipo con XAUTH. Esta opción permitirá que se ejecute el proceso necesario de autenticación del cliente remoto. La fig. 6.19 muestra el detalle de la configuración realizada.

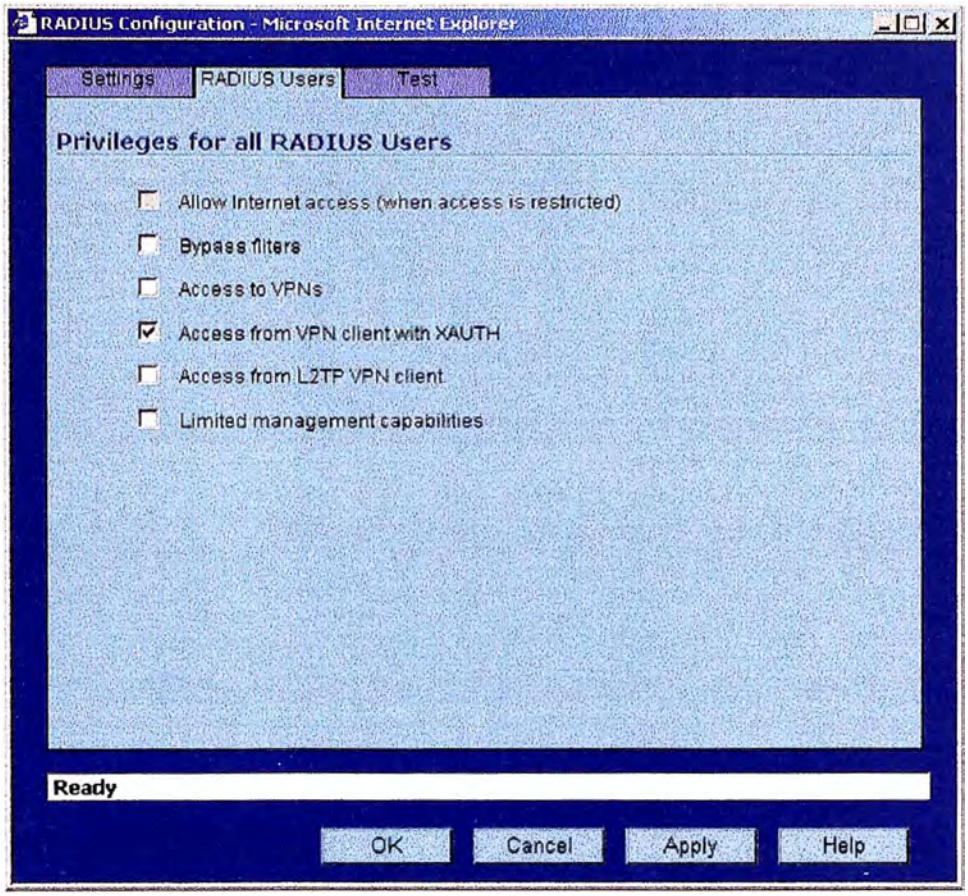

Fig. 6.19.: Parámetros configuración RADIUS users

Ahora, es preciso configurar el equipo Sonicwall para que acepte la función de puerta de enlace (gateway) de los usuarios remotos. Para ello, se configura la opción ***GroupVPN*** disponible en el equipo. Esta opción viene preconfigurada para permitir que el equipo trabaje como se espera para el enlace de los clientes remotos, únicamente será preciso establecer los parámetros del enlace. La fig. 6.20 muestra la habilitación de la opción GroupVPN, primer paso de ésta configuración:

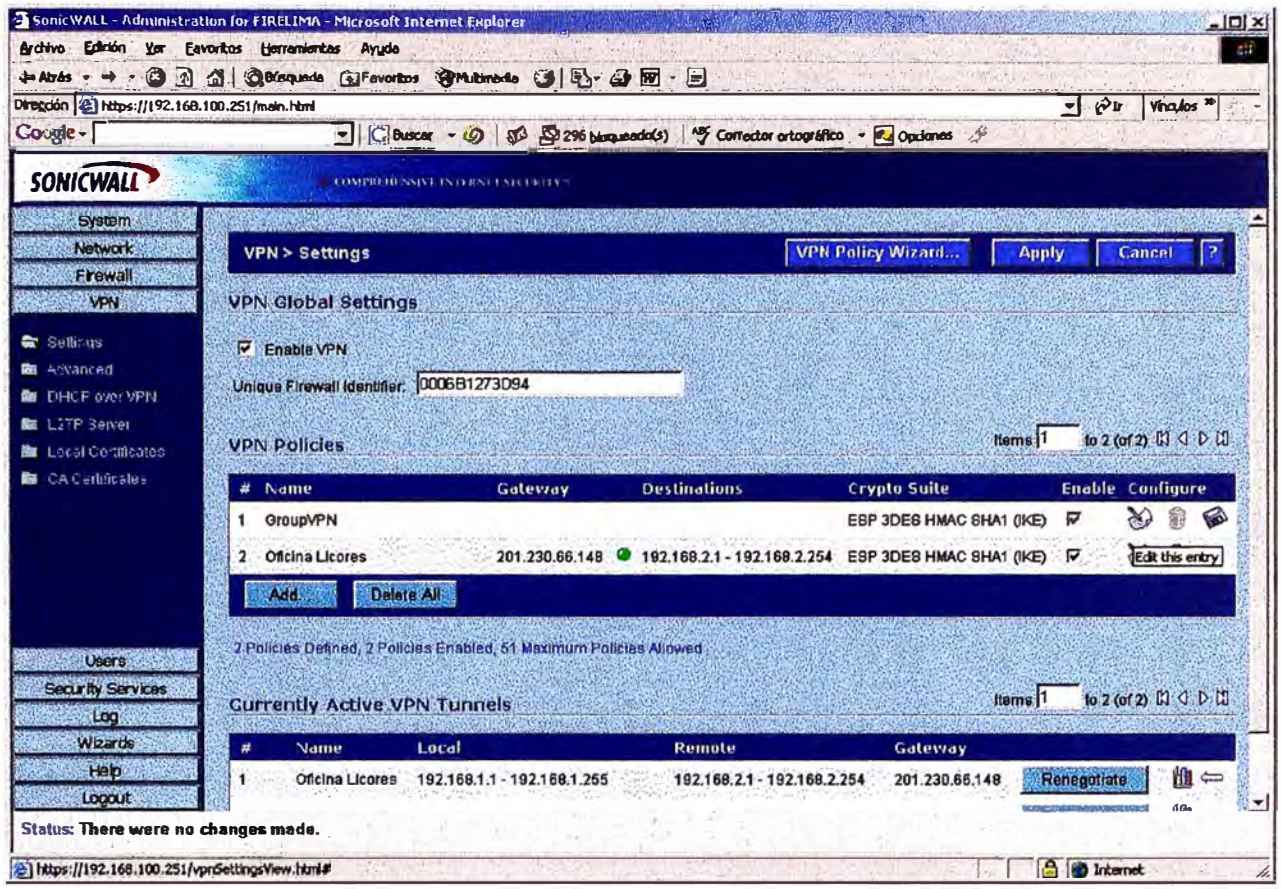

Fig. 6.20.: Activación de GroupVPN en Firewall Sonicwall

Luego, se definirán los parámetros del enlace VPN (tal como se hizo con el enlace VPN Site-ot-Site). La fig. 6.21 muestra el detalle de configuración; se elige en este caso IKE como el "keying mode" usando *preshared secret.* Aquí se muestra el *shared secret* utilizado.

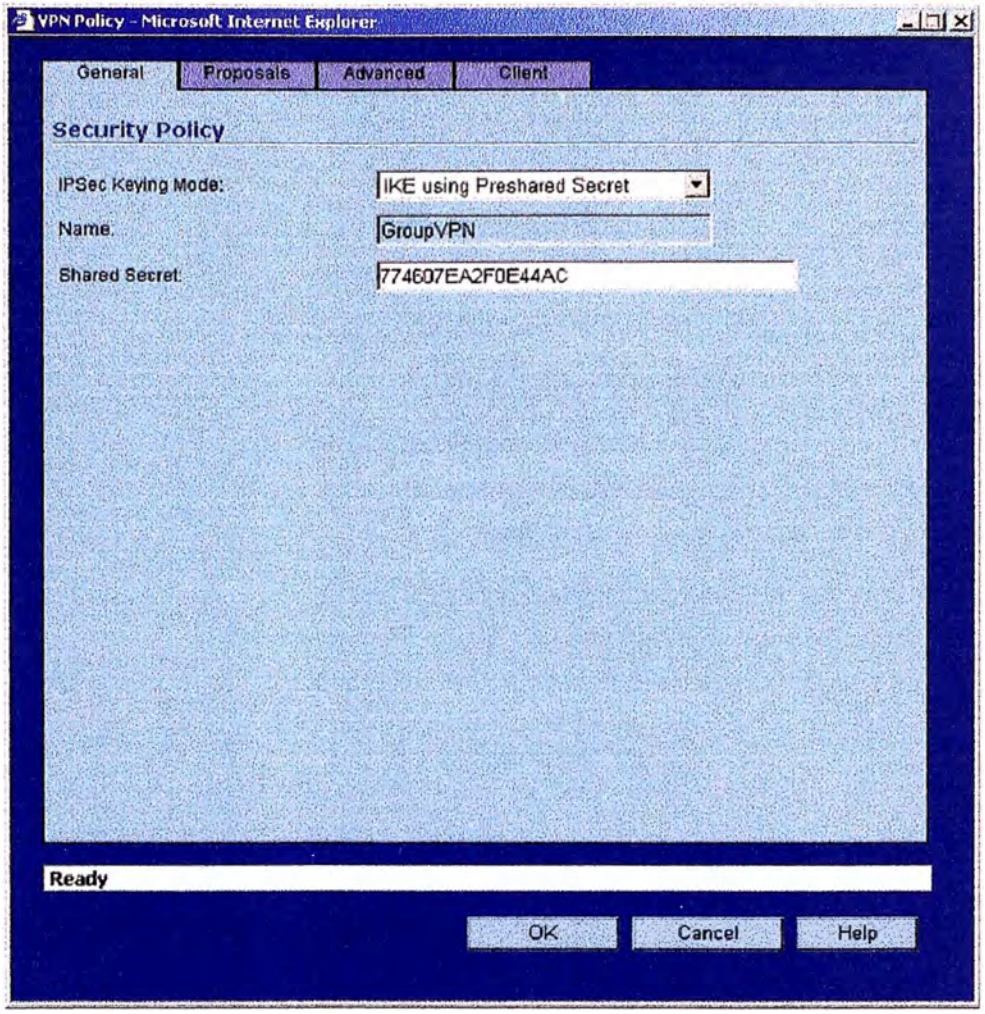

Fig. 6.21.:Parámetros generales del enlace VPN para PCs remotos

Ahora, la fig. 6.22. muestra los parámetros configurados para el establecimiento de la Asociaciones de Seguridad (*Security Association*)

- IKE fase 1
  - Grupo Diffie Hellman: Group 2
  - Cifrado : 3DES
  - Autenticación : SHA1
  - Tiempo de vida (Lifetime): 28,800 segundos
- IPSec fase 2
  - Protocolo: ESP
  - Crifrado : 3DES
  - Autenticación: SHA1

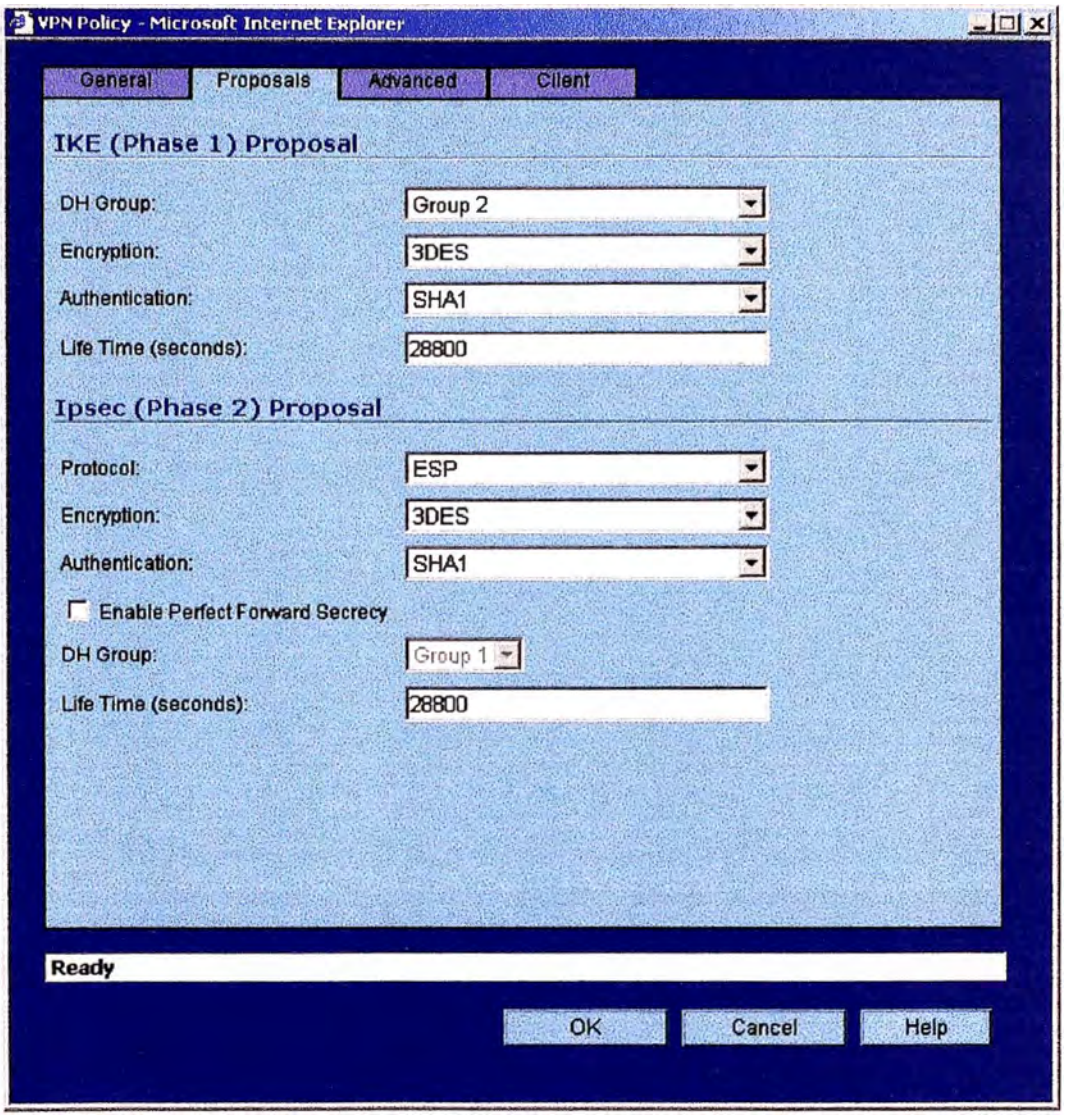

Fig. 6.22.: Parámetros para los SA

Finalmente, en los parámetros avanzados solo definimos que la terminación de este enlace VPN, en la oficina central, sea en la red LAN y la DMZ.

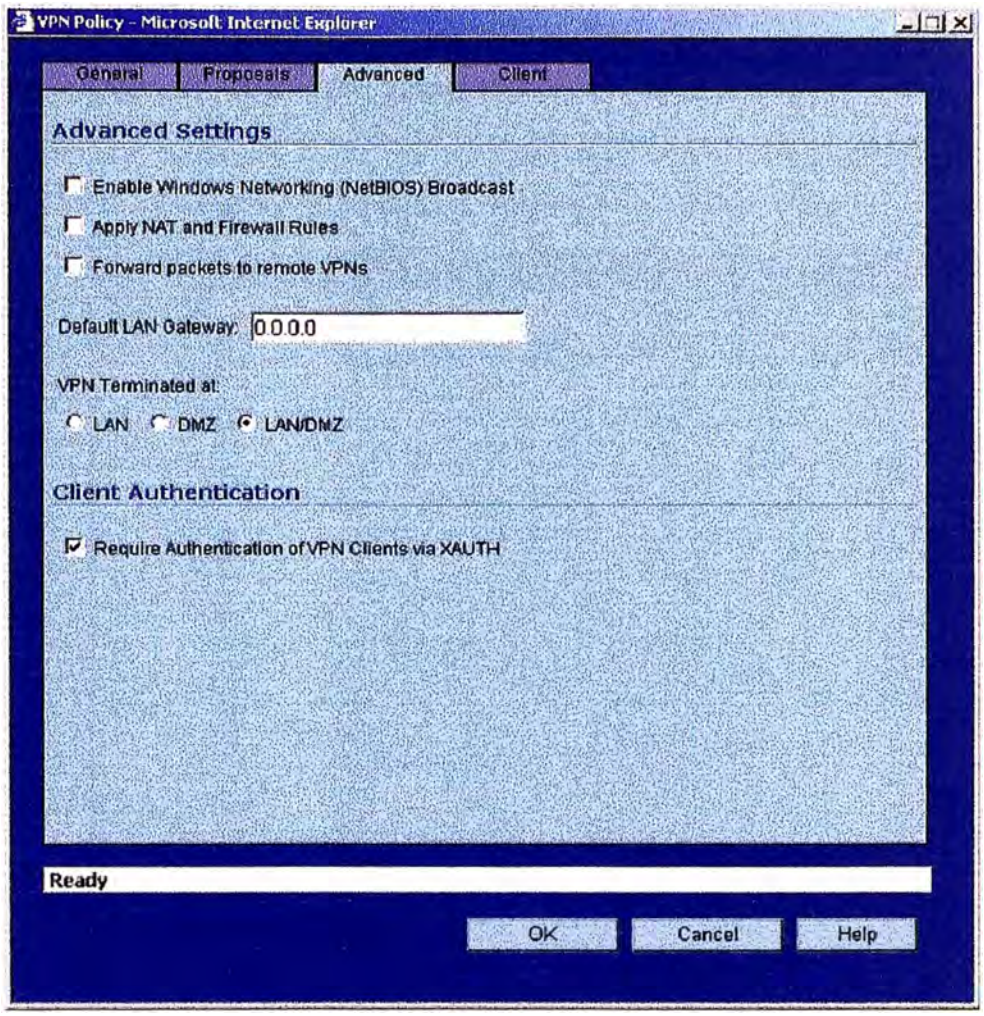

Fig. 6.23.: Parámetros de Terminación en el enlace VPN

Luego de esto, se procede con la instalación del cliente VPN en el equipo PC remoto. Para esto, es preciso recordar que estos enlaces los estamos definiendo en base a una clave de tipo "*preshared secret*", lo cual permite que ambos equipos mantengan una llave común que facilita el establecimiento del enlace y mantiene la seguridad del mismo, siempre que esta llave común no sea conocida por más de una o dos personas. Por tanto, a fin de desplegar este tipo de configuración, el equipo Sonicwall viene preparado con una característica que le permite que el cliente VPN propietario que posee, se intente conectar inicialmente al equipo Firewall obteniéndo de él mismo la llave compartida, sin que el usuario se entere. Esta facilidad debe ser gestionada por el administrador del equipo, ya que se debe activar únicamente en el momento en que se debe intentar establecer el enlace por primera vez.

- **Configuración de PC cliente remoto**

Para la configuración del cliente remoto, se utiliza el software Global VPN client [REF 10], de Sonicwall. Primero se debe instalar el cliente, este paso es sumamente sencillo. Luego, será necesario configurarlo:

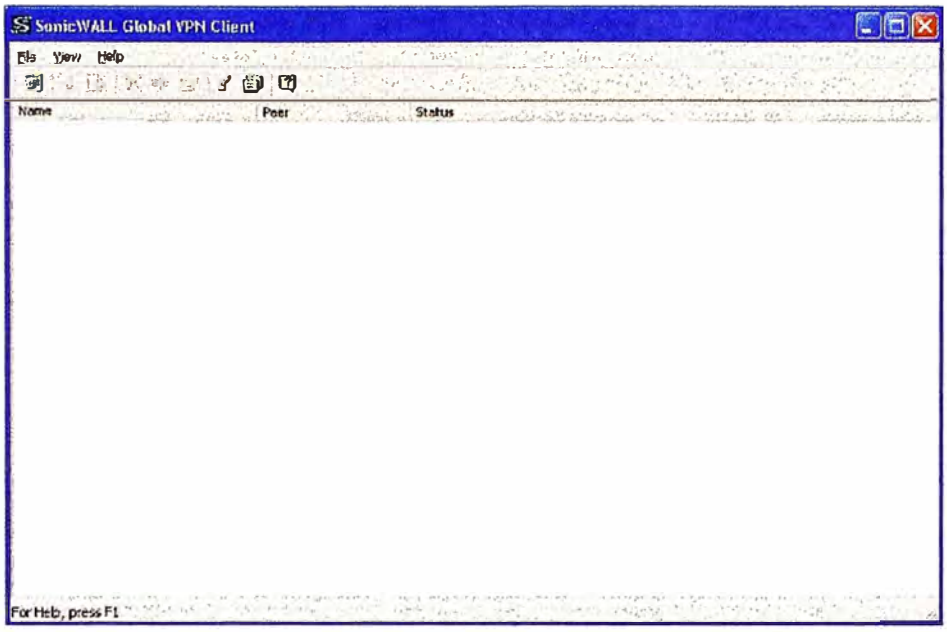

Fig. 6.24.: Ventana de configuración, cliente GVC

La figura 6.24 muestra la ventana de configuración disponible, inscribimos una nueva conexión, la fig. 6.25 muestra el inicio de dicha configuración:

Fig. 6.25.: Preparación de una nueva conexión

Se escoge el escenario en el cual se preparará la conexión (Fig. 6.26):

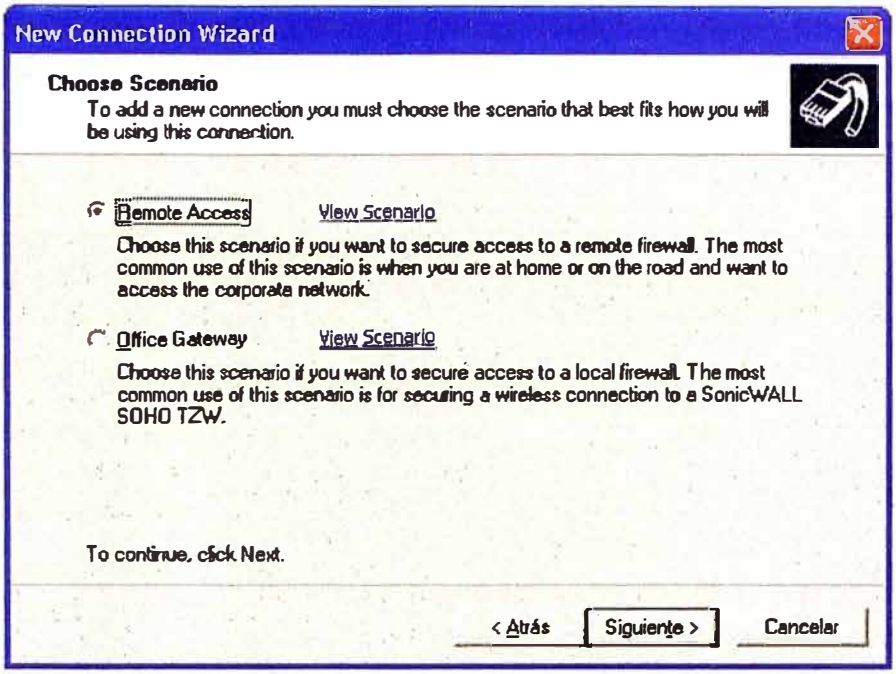

Fig. 6.26.: Elección del escenario para configuración del enlace

En este caso, se elige Remote Access.

Luego configuramos el punto de acceso remoto (para la PC), en este caso, dicho punto será la dirección IP público del Firewall, ya que hacia él se dirigirán los intentos de conexión:

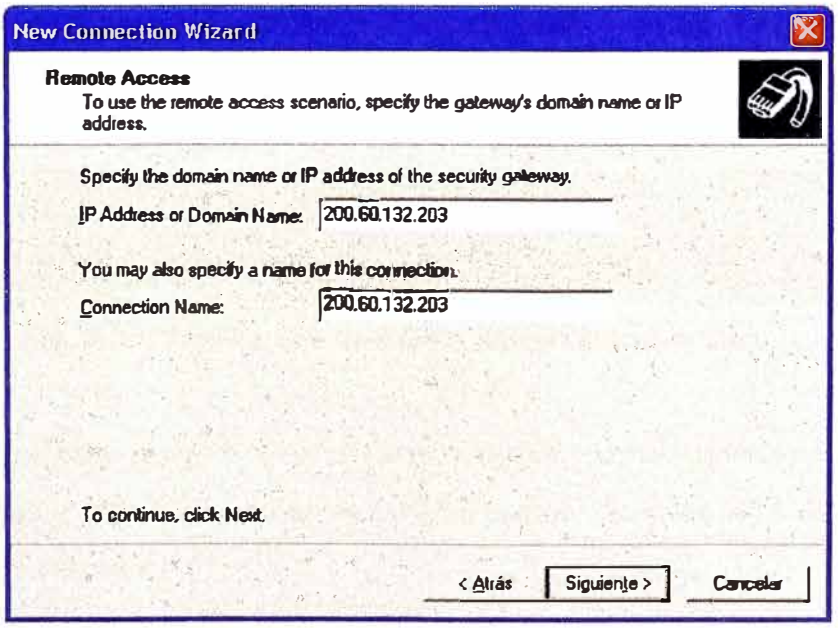

Fig. 6.27.: Dirección IP del punto de acceso remoto

Con eso se completa la configuración. Inmediatamente el equipo PC remoto intenta concretar la conexión, para este momento, la activación de la característica "Client Initial Provisioning" debe estar activa, observe la figura 6.28.

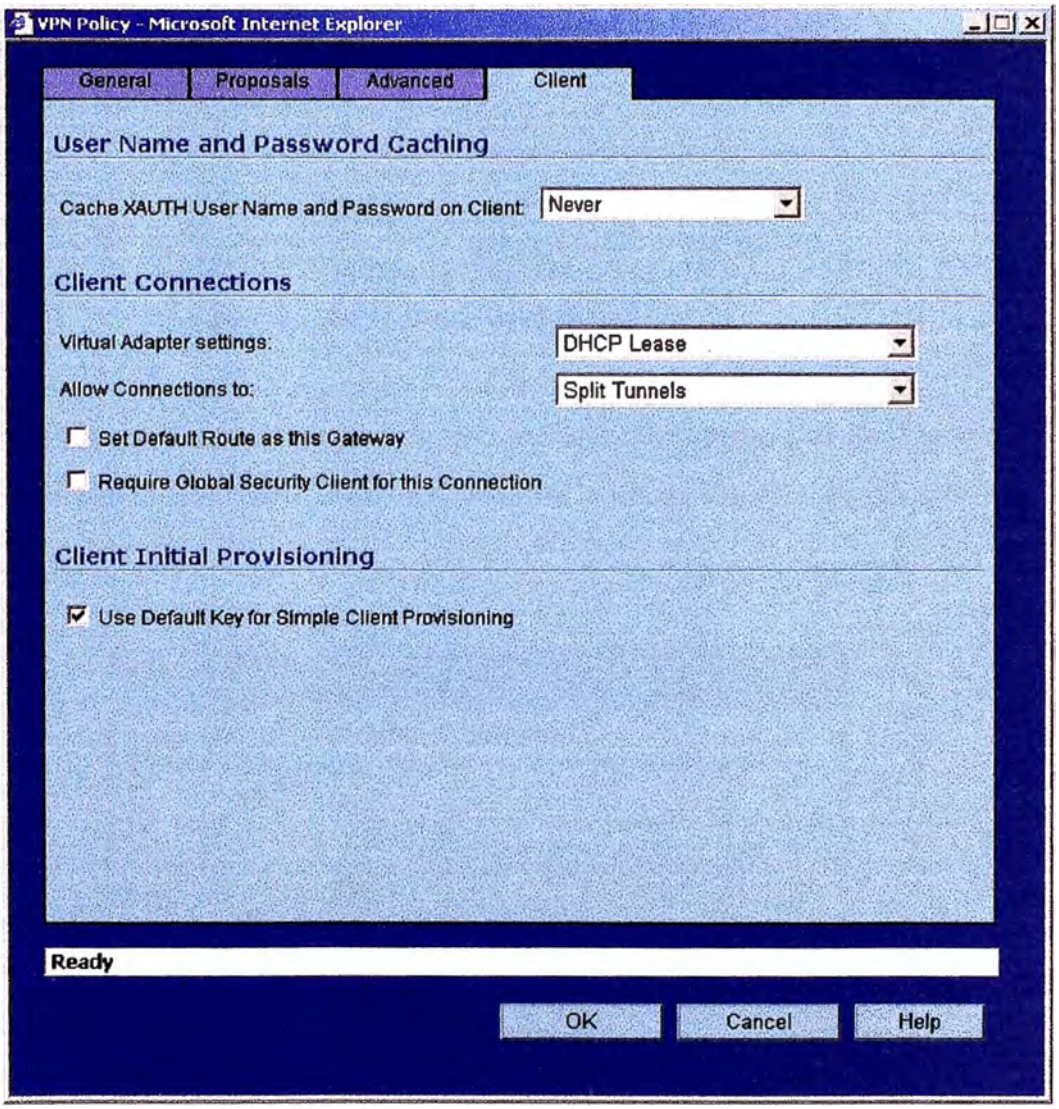

Fig. 6.28. Activación de Client Initial Provisioning

Esta característica permite que el cliente remoto pueda intercambiar los datos básicos y esenciales, como el "shared secret" sin necesidad de que el instalador lo conozca.

La fig. 6.29 muestra el intento de enlace que ocurre en la PC remota luego que se ha completado la configuración del cliente Global VPN client:

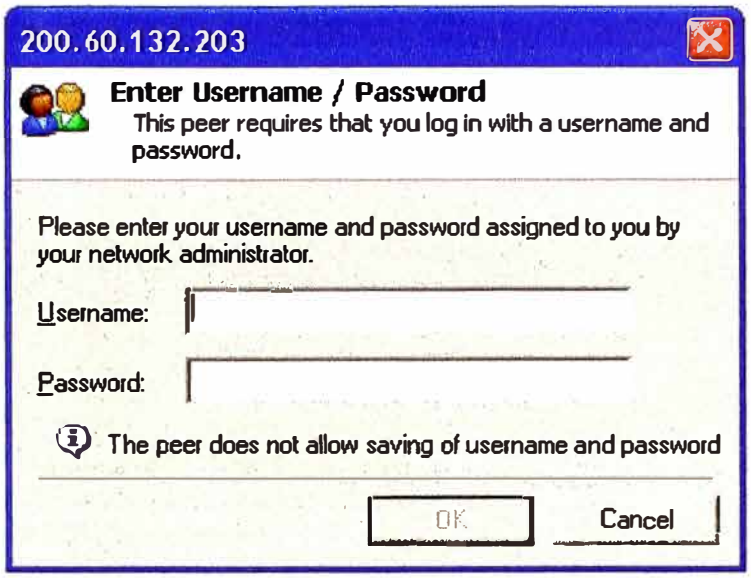

Fig. 6.29.: Intento de conexión

Aquí se ingresa con el usuario que se haya configurado en Active Directory y al cual se le haya dado permisos de acceso. En este caso es el usuario "provincia":

Fig. 6.30.: Ingreso de usuario y clave

El proceso de enlace se observa en el registro de eventos del cliente, según se muestra en la Fig. 6.31. Aquí se observa las dos fases que permiten el establecimiento del enlace, se observa que luego de haber completado la primera fase (IKE fase 1), se exige nuevamente que el usuario ingrese sus datos (nombre de usuario y clave), para concretar la culminación de esta

fase. Luego de esto, se gestiona la fase 2, y luego de completada se ha establecido la asociación de seguridad (SA), y la PC ya está conectada a la red central.

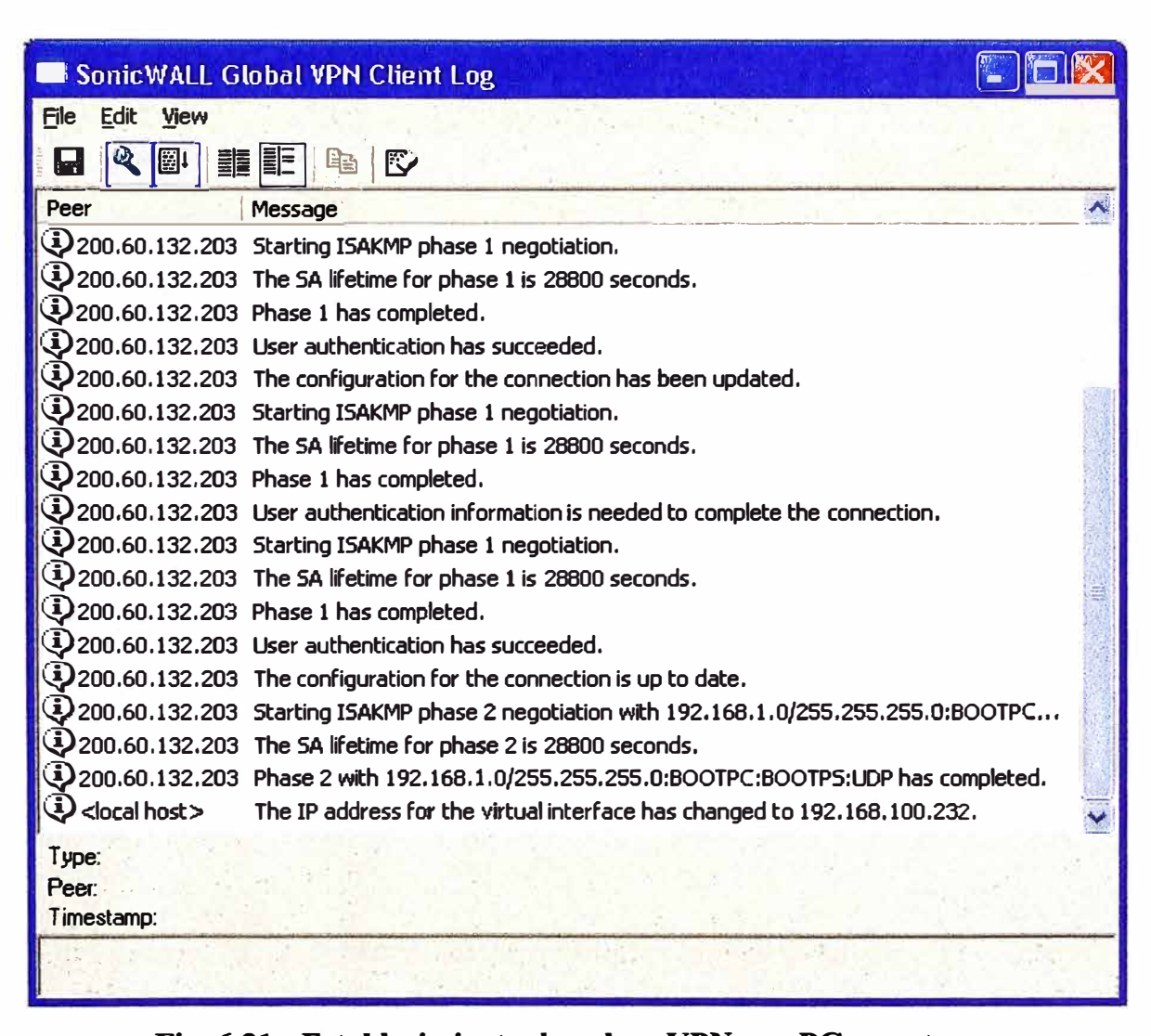

Fig. 6.31.: Establecimiento de enlace VPN con PC remota

Este proceso de configuración se repetirá en los equipos remotos que se designen de acuerdo a las políticas de seguridad interna

6.3. Estado final de implementación

El estado final de la implementación de estos enlaces se muestra en la Figura 6.32.

La idea inicial de formar una red corporativa en base a los enlaces VPN se logra finalmente.

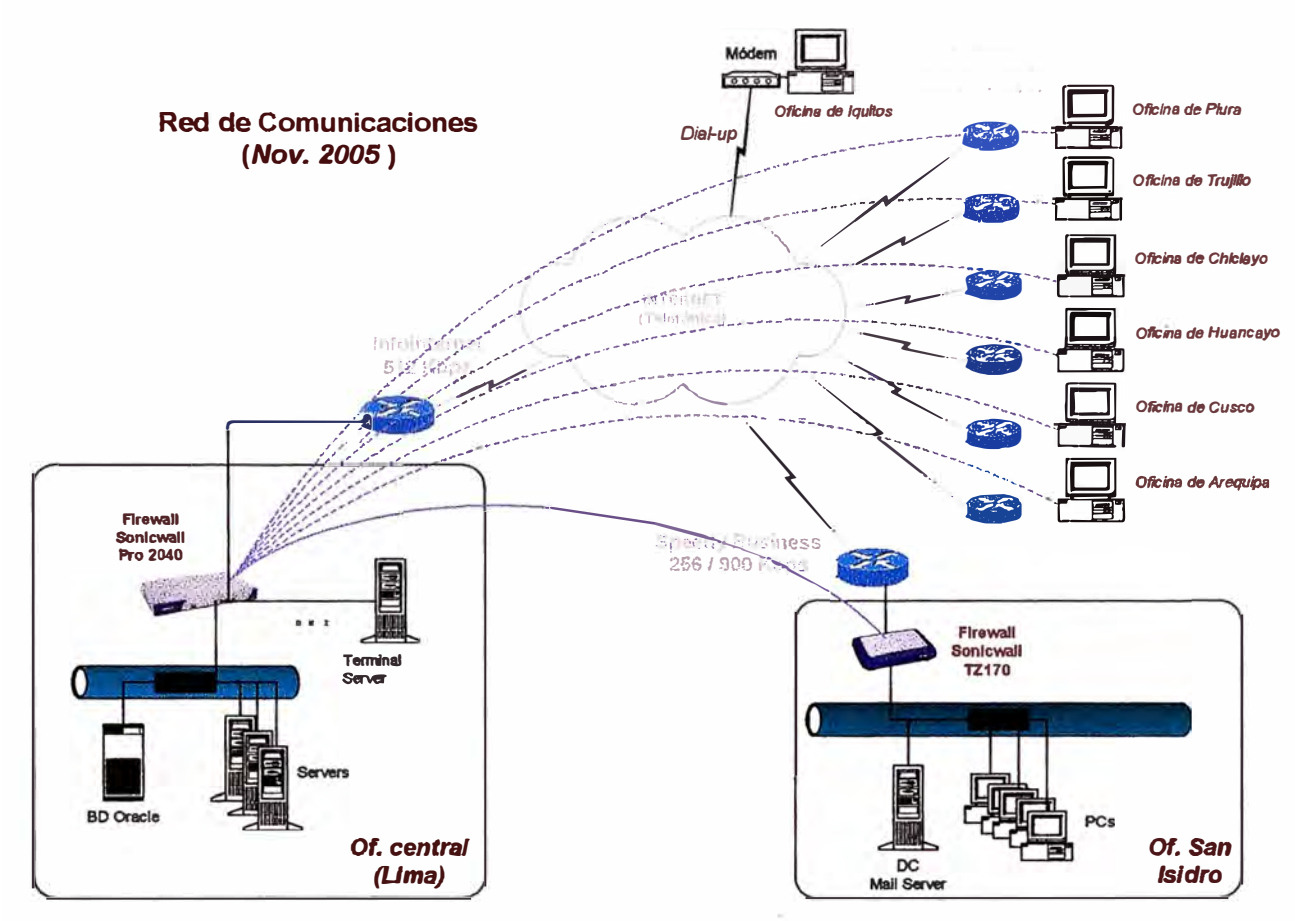

Fig. 6.32.: Esquema final de la red corporativa de la empresa.

Para nuestro caso, la implementación ha resultado exitosa y ha permitido integrar al personal que labora en otras oficinas, a la realidad de las operaciones principales realizadas en el local cenbtral, ahora disponen de uso de recursos que antes no se hubieran podido disponer. Estos cambios continuarán afinándose en los siguientes meses.

CONCLUSIONES

1. El desarrollo de la Internet ha cambiado mucho la forma en que las personas se comunican hoy en día, ya no es novedad "chatear" con algún amigo que se encuentra en algún otro lugar del mundo, simplemente a través de la Internet. La globalización se ha acelerado debido a su desarrollo.

   El caso es que mayormente se establecen muchas comunicaciones personales a través de Internet, comunicaciones que no requieren de elevados niveles de seguridad y/o confidencialidad.

   Pero actualmente, las empresas requieren que todos sus empleados estén interconectados, que sus comunicaciones sean seguras y mantengan un alto grado de confidencialidad, pero que esta necesidad no supere sus capacidades económicas destinadas a este objetivo. Por ello, la aparición de las VPN o Redes Privadas Virtuales sobre medios públicos como Internet les dieron la solución a esta necesidad. La aparición y desarrollo de protocolos tales como PPTP, L2TP, IPSec, etc., permitieron que el IPv4 adquiriese características de seguridad que antes nunca había tenido, facilitando con esto la posibilidad de que los usuarios remotos y oficinas puedan accesar recursos de información centralizados en la empresa.
2. Los antiguamente elevados costos por un enlace de acceso a Internet se han reducido notablemente, actualmente existe posibilidad de tener enlaces de 512Kbps o más con precios que parten de 750 dólares mensuales, lo cual es alcanzable para muchas empresas. Hoy es factible tener incluso enlace dedicado y permanente a Internet en las casas, debido a la expansión de enlaces de tipo ADSL; esto ha permitido que la información esté al alcance de todos.
3. Aquí en Perú, la empresa Telefónica del Perú ofrece sus servicios de IP-VPN a empresas que no deseen administrar dichos enlaces directamente, dejando en las manos de Telefónica la gestión de todos los detalles de conexión, seguridad, etc. que este tipo de enlaces requiere. Esto, si bien es una buena opción dado que el ancho de banda

ofertado es de uso único para el suscriptor, los costos siguen superando las espectativas de muchos, quedando fuera del alcance para la mayoría.

Por ello, cada vez mas empresas tratan de utilizar la Internet como medio de comunicaciones corporativas, creando redes WAN conformadas por enlaces dedicados a Internet y equipamiento que permita establecer enlaces VPN seguros.

4. El presente trabajo me ha permitido experimentar esencialmente con la opción actualmente mas difundida para la conformación de VPNs, la cual es el protocolo IPSec. Este protocolo es el que al momento es el más usado debido a que permite establecer enlaces seguros, y estables. En nuestro caso, los equipos adquiridos para actuar como Firewalls / VPN servers están cumpliendo de forma muy estable el objetivo deseado, y han permitido que los usuarios de la empresa se integren más con el rutina diaria de la misma. Ya no se percibe el efecto de aislamiento que existía antes, ya que ellos se ubicaban en oficinas lejanas, distintas y no disponían de acceso a los sistemas centralizados.
5. Actualmente Perufarma cuenta con 6 oficinas remotas (provincias) conectadas vía VPN hacia la oficina central en Lima, y tenemos una sucursal en San Isidro interconectada permanentemente con la oficina central accediendo incluso al sistema central ERP, a la Base de Datos estadística (OLAP) que se encuentra en MS SQL Server 2000, también tiene acceso a la intranet de la empresa, la cual ha requerido iniciar nuevamente un proceso periódico de actualización a fin de que todos el personal de la empresa, no importando si se encuentra en Lima o provincias, pueda acceder a toda la información que allí se encuentra. El enlace VPN Site-to-Site que se ha implementado, opera equivalentemente a un enlace dedicado de 128Kbps, velocidad determinada luego de la evaluación correspondiente.
6. En suma, este pequeño proyecto continúa su proceso de mejoramiento, se sigue analizando los temas críticos de seguridad y tratando de buscar una opción de monitoreo adecuada, ya que ésta al momento no existe. Sin embargo, la estabilidad lograda en los enlaces establecidos, nos alientan a seguir buscando opciones costo-beneficio que permitan mejorar cada vez mas el entorno de comunicaciones corporativas.

BIBLIOGRAFIA

[1] http://www.iec.csic.es, Departamento de Tratamiento de la Información y Codificación; Consej Superior de Investigaciones Científicas, España.

[2] http://www.iec.csic.es/criptonomicon/correo/cifrado.html, Cifrado, teoría, año 2000

[3] RFC 2420, The PPP Triple-DES Encryption Protocol, año 1998

[4] Federal Information Processing Standards Publication 197, Nov. 2001. Announcing Advance Encryption Standard (AES)

[5] www.microsoft.com, Web oficial de Microsoft Corporation, referencias de protocolos VPN PPTP, L2TP, IPSec, así como protocolos de autenticación de tipo PAP, CHAP, EAP, RADIUS.

[6] VPN Technologies, Definitions and Requirements, VPN Consortium White Paper January 2006. http://www.vpnc.org

[7] RFC 2246, The TLS Protocol, v1.0, año 1999

[8] MCSE Training Kit Windows 2000 Server, IT Study Guide.

[9] SonicOS Standard 3.1 Administration Guide, Manual de Administrador de equpos Sonicwall, versión año 2005

[10] Sonicwall GVC 3.1 Administration Guide, Manual de Administrador de software Global VPN Client, de Sonicwall, versión año 2005

Otras fuentes de información

Sitios Web

http://www.itprc.com/vpn.htm, **ITPRC.COM, The Information Technology Professional Resource Center**. Fuente de información sobre IPSec e IKE

http://www.vpnc.org, **VPN Consortium**, Asociación internacional de los fabricantes de productos VPN. Los siguientes documentos sirvieron de base: