ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Autentificación: El proceso para determinar la identidad de un usuario que está intentando acceder a un sistema.

Autorización: Proceso destinado a determinar que tipos de actividades se permiten. Normalmente, la autorización, está en el contexto de la autentificación: una vez autentificado el usuario en cuestión, se les puede autorizar realizar diferentes tipos de acceso o actividades.

CHAP *Challenge Handshake Authentication Protocol*, protocolo usado para la autentificación de usuarios remotos.

Detección de intrusión Detección de rupturas o intentos de rupturas bien sea manual o vía sistemas expertos de software que atentan contra las actividades que se producen en la red o contra la información disponible en la misma.

Enrutador Dispositivo destinado a conectar 2 o más redes de área local y que se utiliza para enlutar la información que atraviesa dicho dispositivo.

Firewall	O también denominado cortafuego, es un sistema o combinación de sistemas que implementan una frontera entre 2 o más redes.
IPSec	Protocolo criptográfico de red, usado para proteger paquetes IP.
ISP	*Internet Service Provider*, Compañía que provee servicios de acceso a Internet a usuarios finales o empresas.
L2F	*Layer2 Forwarding*, protocolo para manejo de túneles desarrollado por "**Cisco**".
L2TP	*Layer2 Tunneling Protocol,* Protocolo de manejo de túneles que combina las características del protocolo *L2F* y el protocolo *PPTP*, además también necesita del protocolo *IPSec* para la encripción de los paquetes.
Logging	El proceso de almacenamiento de información sobre eventos que ocurren en el cortafuegos o en la red.
Modo agresivo	Es el nombre del mecanismo usado en la primer fase al establecer una asociación de seguridad.
PAP	*Password Authentication Protocol,* Protocolo de autenticación sencilla, que usas claves usando un intercambio de dos vías, las claves son transmitidas

	sin encripción, de donde este protocolo no da seguridad.
Política:	Reglas de gobierno a nivel empresarial/organizativo que afectan a los recursos informáticos, prácticas de seguridad y procedimientos operativos.
POP	*Point of Presence,* (punto de presencia) punto de acceso local a las redes de comunicaciones como Internet.
PPP	*Point to Point Protocol,* Protocolo usado para enmarcar los paquetes de datos en enlaces punto a punto, como lo son los enlaces con módems.
PPTP	*Point to Point Tunneling Protocol,* protocolo para manejo de túneles desarrollado por "**Ascend**" y "**Microsoft**", depende del protocolo *PPP* para sus funciones básicas.
Proxy	Un agente de software que actúa en beneficio de un usuario. Los *Proxy* típicos, aceptan una conexión de un usuario, toman una decisión al respecto de si el usuario o cliente *IP* es o no un usuario del *Proxy*, quizás realicen procesos de autentificación adicionales y entonces completan una conexión entre el usuario y el destino remoto.

SA	*Security Associations,* (asociaciones de seguridad) usadas en el protocolo *IPSec* para hacer acuerdos entre dos equipos que se están comunicando, en la cual se indican que tipo de autentificación y algoritmos de encripción se usarán.
Servidor Bastión	Un sistema que ha sido configurado para resistir los ataques y que se encuentra instalado en una red en la que se prevé que habrá ataques. Frecuentemente, los servidores bastión son componentes de las firewalls, o pueden ser servidores Web "exteriores" o sistemas de acceso público.
Túnel Obligatorio	Túnel creado sin el consentimiento del usuario, el cual puede ser transparente al usuario final.
Túnel Voluntario	Son configurados según el requerimiento del usuario final. Los extremos de los túneles residen en las computadoras de los usuarios finales.

RESUMEN

Este trabajo de investigación, consiste en la presentación de una forma diferente de manejar las redes privadas, siendo esta nueva forma las redes privadas virtuales. El tema, trata sobre el uso de diferentes tecnologías como lo son: Los métodos de encripción, protocolos de seguridad, cortafuegos y la plataforma de Internet. Proporcionando todas estas tecnologías juntas el medio adecuado para que puedan operar las redes privadas virtuales.

El desarrollo de la tesis, se inicia con un capítulo donde se detallan los fundamentos esenciales del funcionamiento como lo son, la plataforma de Internet, los fundamentos de las redes privadas virtuales donde se describen su operación, sus principales componentes y distintos tipos de interconexión en estas redes.

En el siguiente capítulo de autentificación se detallan los temas, los distintos sistemas de verificación de usuarios, así como también, los diferentes métodos de encripción para proporcionar la seguridad de la información transmitida entre las redes públicas.

Luego, se llega al capítulo sobre los protocolos, en éste, se describen los principales protocolos que intervienen en la elaboración de las redes privadas virtuales, los protocolos descritos son: el protocolo *IPSec*, el protocolo *PPTP* y el protocolo *L2TP* que esencialmente es una variante mejorada del protocolo *PPTP*.

Posteriormente, se trata el tema de los cortafuegos y enrutadores, estando en estos equipos la tarea de la interconexión física de las redes privadas con las redes públicas, y que se encargan de brindar la seguridad a las redes privadas a través de sus políticas de seguridad.

En el último capítulo se presenta el escenario de una red privada virtual partiendo de una red privada con sus enlaces dedicados luego, se elabora un análisis económico en el cual se estudia el costo de la inversión inicial de esta nueva red y se evalúan sus costos de operación contra los costos de la red privada tradicional, esto, para poder determinar si puede llegar a ser una opción factible y rentable de llegar a usar estas nuevas formas para manejar las comunicaciones de un modo seguro a través de redes públicas.

INTRODUCCIÓN

La relación entre los trabajadores y sus empresas ha dejado de seguir los criterios tradicionales desde que se introdujo la terminología *"mobile user"* o usuario móvil en el mercado de las telecomunicaciones. Los accesos remotos o móviles se han convertido en uno de los aspectos con mayor énfasis en el desarrollo de tecnologías de compañías en crecimiento.

Desafortunada o "afortunadamente" el costo de este acceso privado es tan alto que es necesario recurrir a diferentes alternativas como el uso de Redes Virtuales Privadas las cuales son una manera más económica e igual o similarmente segura para el acceso privado a una red. Internet, como era de esperarse, ha probado ser el medio de comunicaciones que está facilitando esta clase de acceso. No obstante, siempre existen ciertas dudas cuando el uso de esta red pública y mundial se relaciona con transacciones privadas que exigen un uso más seguro y administrado.

En una red privada virtual, todos los usuarios parecen estar en el mismo segmento de *LAN* pero en realidad están a varias redes de distancia (generalmente redes públicas). Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas: primero, deben ser capaces de pasar paquetes *IP* a través de un túnel en la red pública, de manera que dos segmentos de *LAN* remotos no parezcan estar separados por una red pública, segundo, la solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación, de modo que un adversario no pueda acceder a los recursos del sistema, y por último la solución

debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado.

Las razones que impulsan al mercado en ese sentido son, fundamentalmente, la reducción de costos de operación, es mucho más barato interconectar filiales utilizando una infraestructura pública que desplegar una red físicamente privada. Por otro lado, como es lógico, es necesario exigir ciertos criterios de privacidad y seguridad, por lo que normalmente se debe recurrir al uso de la criptografía.

Una red privada virtual conecta los componentes de una red sobre otra red, estas redes, lo logran al permitir que el usuario haga un túnel a través de Internet u otra red pública, de manera que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas, siendo estas funciones más económicas, hacen a las redes privadas virtuales una nueva vía para las comunicaciones seguras.

1. FUNDAMENTOS

1.1. El ambiente en el medio de los negocios

En la actualidad, los negocios son completamente diferentes a como lo eran tiempo atrás. Ya que con la automatización y el incremento de pequeñas empresas, así como las fusiones a gran escala, una tendencia de todo esto es que se tenga una buena flexibilidad en sus organizaciones.

Un punto importante de la flexibilidad de los negocios es una red de comunicaciones que sea adaptable. El establecimiento de una red bien diseñada puede ayudar a la interacción del negocio con muchos de los cambios en el ambiente actual como por ejemplo, mejores relaciones entre el cliente y el socio, una fuerza de trabajo cada vez más móvil, estructuras de organización planas, equipos virtuales, etc.

Las empresas se hacen frente, no solamente con proyectos y mercados que cambian rápidamente sino que, también con sociedades a corto plazo, con los proveedores y otros socios de negocios mientras que tratan de competir. Los clientes exigen más y no sólo más calidad y variedad en productos sino que también más información sobre ellos.

Mientras que los clientes exigen más, también pueden ofrecer más a los vendedores; los vendedores inteligentes miran incrementar la interactividad con los clientes para aprender más de sus necesidades, el inclinarse hacia más individualidad y tratar a cada cliente más bien como un mercado que una gran cantidad de individuos aglomerados en un solo grupo con los mismos gustos y necesidades.

Mientras que las empresas luchan con estas fuentes y lagunas de la información, encuentran a sus propios empleados dispersados a través del planeta, intentando conectar sus trabajos a los mercados que han llegado a ser cada vez más globales.

Las personas de negocios en este mundo físico en el cual se valora la presencia, se encuentran con una fuerza de trabajo cada vez más móvil, la cual viaja grandes distancias a las reuniones de negocios obligadas. Y en medio de todo este recorrido a través del planeta, cada empleado necesita permanecer en contacto con su oficina física, dondequiera que esté.

Una de las tendencias comunes de los negocios en la última década ha sido el de aplanar la estructura de la organización, con lo que se ha pasado de una estructura de gerencia jerárquica a una estructura incluyendo pocos encargados y de más equipos que trabajan recíprocamente. Organizaciones más planas, requieren más coordinación y comunicación para funcionar correctamente, proporcionando otra razón para el crecimiento de las redes.

En las organizaciones con estructuras jerárquicas más planas, no está fuera de lo común ver un incremento del número de los equipos

formados. Estos equipos, que se forman rápidamente para atacar un problema determinado y después se disuelven, están constituidos por los miembros dispersados a través de la compañía, a menudo en más de un país. Mucho de su trabajo y coordinación se maneja electrónicamente, transmitido a través de las redes en cualquier momento o en todo el día.

Las compañías dependen no sólo de la comunicación para ejecutar sus asuntos internos, sino que también tienen que comunicarse con sus proveedores, clientes, y mercados si esperan permanecer en el negocio. Lo que hace que la comunicación sea el corazón de las empresas.

En la actualidad, Internet se ha convertido en la estrella de la comunicación, ha capturado la atención de las personas individuales y personas de negocios como un nuevo medio para comunicarse con los clientes así como con sus socios. Pero, Internet es una plataforma que mezcla varias de las diversas tecnologías existentes.

Muchas de las tecnologías necesarias para las comunicaciones confiables, todavía están en el proceso de ser llevadas para el uso rutinario. El uso diario del Internet para la comunicación de los negocios representa una gran promesa, pero todavía se tiene que alcanzar la etapa de la conectividad para muchas aplicaciones de negocios del Internet.

Los avances de hoy en la tecnología en todos los niveles de la red, pueden hacer esto difícil, y si no imposible, el encontrar una sola solución integrada para las necesidades de una empresa. Así, se encuentra una época en la cual están no sólo los nuevos medios de más altas velocidades que son introducidos para la comunicación residencial y de negocios, sino qué en ambientes donde las nuevas aplicaciones, tales

como el Web, que ofrece valores agregados tales como los nuevos mercados y canales de ventas encontrados en el comercio electrónico.

1.2. Fundamentos de Internet

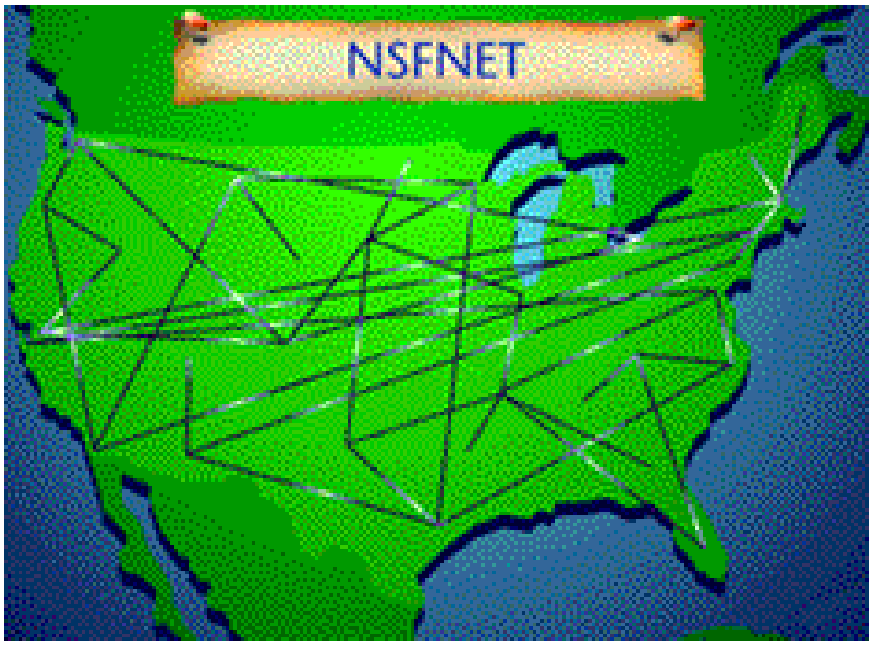
Internet tiene una historia relativamente corta pero asombrosa hasta el momento. Se desarrolló a partir de un experimento impulsado a principios de los años 70 por el Departamento de Defensa de los Estados Unidos. El Departamento de Defensa quería crear una red informática que pudiera seguir funcionando en caso de un desastre. Otra condición era que si parte de la red era dañada o destruida, el resto del sistema debía de seguir en funcionamiento.

La primera propuesta fue de Paul Barán en 1964. Todos los ordenadores serían igual de importantes y todos tendrían el mismo papel. La información se dividiría en "paquetes" que, al igual que los paquetes en el mundo real, llevarían un remitente (origen) y un destinatario (destino). La ruta que el paquete tomara debería ser irrelevante, y los paquetes irían de ordenador a ordenador hasta llegar al destino.

La idea gustó y el *ARPA* (*Advanced Reseach Projects Agency*) decidió respaldar el proyecto. Por lo que esta red fue llamada *ARPANET*, y puso por primera vez en contacto a los investigadores científicos y académicos estadounidenses. Fue, además, la predecesora de la red Internet que conocemos hoy.

En 1985, la *National Science Foundation* (*NSF*) creó *NSFNET*, una serie de redes informáticas dedicadas a la difusión de los nuevos descubrimientos y la educación. Basada en los protocolos de comunicación de *ARPANET*, la *NSFNET* creó una plataforma de red nacional, ofrecido gratuitamente a cualquier institución americana de investigación o educación. Al mismo tiempo, otras redes regionales fueron apareciendo con el fin de poder enlazar el tráfico electrónico de instituciones individuales con el esqueleto de red nacional.

Figura 1. Red *NSFNET*



La *NSFNET* creció rápidamente a la par con el descubrimiento por parte del público de su potencial y con la creación de nuevas aplicaciones que permitían más fácil acceso.

Corporaciones como “**Sprint”** y “**MCI**“ empezaron a construir sus propias redes, que enlazaron con *NSFNET*. Mientras firmas comerciales y otros proveedores de red regionales han empezado a hacerse cargo de las operaciones de las mayores arterias de Internet, *NSF* ha ido dejando de dar soporte al esqueleto de la red.

A principios de los ochenta, Internet solamente contaba con 200 *Host* o computadoras centrales. A finales de esta década, el número de computadoras conectadas a Internet creció drásticamente, y a principios de los noventa, había más de 300.000 conectadas a la red. Las últimas estimaciones indican que existen más de 3.200.000. Estas computadoras pertenecen a gobiernos, universidades, grandes empresas (tales como “**IBM**” o “**Microsoft**”), empresas comerciales que se encargan de proporcionar acceso a usuarios particulares, etc.

Internet se ha extendido por todo el mundo de forma imparable conectando las redes de computadoras de todos los continentes. Esta expansión significa que con una computadora se puede viajar a cualquiera de estas computadoras, por ejemplo, para consultar: bibliotecas públicas o privadas; bases de datos que contienen los artículos de revistas científicas, noticias de actualidad; y un sinfín de cosas más sin que tengamos que salir de nuestro domicilio.

1.2.1. La infraestructura del Internet

El Internet es global en alcance y se descentraliza fuertemente sin ningún cuerpo sencillo que la gobierne. Se puede, decir que Internet son millones de ordenadores conectados a miles de redes. O, por decirlo de

otras palabras, Internet es una red mayor (de área amplia) de redes menores (locales).

Evidentemente, no existe una red principal a la que todos los ordenadores se conectan, sino que son redes de ordenadores que se interconectan entre sí.

Este es un factor de éxito añadido. La inexistencia de una red principal, funciona como una defensa contra al malfuncionamiento. De hecho que si una red se "cae" (por algún razón deja de funcionar efectivamente), el resto sigue funcionando aunque, evidentemente, no pudieran acceder a la red menor que esta fuera del servicio.

No obstante, aunque no haya una red primaria, sí hay una serie de redes, que por su localización, calidad e importancia, se consideran fundamentales. Son las que forman la "espina dorsal de Internet", que también se conocen como las “autopistas de Internet”, de la que se conectan otras redes menos importantes. Por ello, si no hay una red principal, no hay ordenadores principales, ni centros de control.

Internet ofrece a sus usuarios una amplia gama de opciones de conectividad, muchas a bajo costo. Estas opciones se extienden desde una conexión directa de alta velocidad (Mega *bits* por segundo) a la plataforma de Internet, para soportar el intercambio de datos y aplicaciones multimedia entre los sitios a las terminales con la opción de usar una conexión a través de líneas telefónicas regulares en las velocidades de 9.600 a 56.000 bits por segundo.

La ubicación cercana de Internet hace la creación de conexiones mucho más fáciles que con cualquier otra red de datos. Éstas podían ser conexiones permanentes para las sucursales o conexiones temporales para sus trabajadores móviles. Mientras que la cobertura del Internet no es igual a través del mundo, Internet permite alcanzar conectividad global a un costo más bajo si el negocio crea su propia red global.

Según lo mencionado antes, Internet se construye en una serie de protocolos abiertos. Este fundamento ha hecho mucho más fácil para que los desarrolladores realicen las aplicaciones de red para cualquier plataforma de computación, promoviendo una gran interoperabilidad. No es inusual encontrar una amplia gama de las aplicaciones del Internet que se ejecutan en todos los sistemas operativos importantes.

La Web ha ido incluso más lejos ofreciendo a los desarrolladores y a diseñadores igualmente la posibilidad de trabajar dentro de un solo interfaz de usuario y extenderse sobre múltiples sistemas operativos también.

Internet también ofrece la oportunidad de tener una red más manejable. Porque se tiene una fuente externa dedicada a los problemas de la conectividad nacional y global que es el *ISP*, y entonces se puede centrar más la atención en otros problemas internos del manejo de la red.

Internet no está sin sus defectos, de muchas maneras, se siente bien una víctima de su propio éxito. Por ejemplo, el ancho de banda disponible en la plataforma de Internet y ofrecido por muchos *ISP* ha podido ser capaz de continuar con el aumento explosivo en el uso del Internet que se ha dado durante los últimos años.

Eso, alternadamente, ha levantado algunas preocupaciones por la confiabilidad del tráfico del Internet, las caídas y otras interrupciones de la red han ocurrido, pero con nuevos equipos y políticas se continúa mejorando la robustez de las conexiones del Internet.

Un punto de interés ha sido la capacidad del Internet para manejar el tráfico de multimedia, especialmente multimedia interactiva en tiempo real. En general, los retardos de las transmisiones de datos sobre el Internet hacen transmisiones en tiempo real de multimedia difíciles, pero ciertas redes de la *ISP* se han diseñado con tales aplicaciones en mente, y los esfuerzos en mejorar la calidad del servicio han comenzado a tratar el problema. Actualmente, el funcionamiento garantizado es restringido por la mayoría de los *ISP* a la red.

Un principal problema es el de la seguridad. Obviamente, en Internet se transmite en claro y puede ser interceptada la mayoría de datos transmitidos en el Internet por otros. Muchas de las intrusiones ilegales señaladas en redes son debidas más a las políticas mal puestas en ejecución de la seguridad que a cualquier inseguridad inherente del Internet.

1.3. La evolución de las redes privadas

Durante las últimas tres décadas, la naturaleza y la configuración de las redes corporativas privadas se han desarrollado mientras que las nuevas tecnologías han llegado a estar disponibles y los ambientes comerciales han cambiado. Lo qué comenzó como las redes privadas que

usaban las líneas telefónicas arrendadas, son redes privadas virtuales ahora convertidas usando Internet como el medio de comunicaciones primario.

Si se rastreara el establecimiento de una red corporativa de nuevo a los años 60, se vería que los encargados de negocios tenían pocas opciones ya que conectarían sus sitios usando líneas telefónicas analógicas y módems arrendados de 2,400 Bps. Eventualmente, como las políticas de monopolio del gobierno acerca de la telefonía cambiaron, otras compañías empujaron la tecnología del módem, permitiendo a los negocios conectar sus sitios a velocidades más altas, alcanzando 9,600 BPS en el comienzo de los 80s.

Aunque se puede estar acostumbrado a la idea de usar una computadora portátil y un módem dondequiera que se este actualmente, muchas conexiones basadas en módems hace 30 años eran de conexión estáticamente definidas entre los sitios fijos, no como el móvil dinámico de hoy.

Las líneas analógicas de la mejor calidad eran especialmente seleccionadas, para que fueran interconectadas con alambre permanentemente a un sitio; también no había trabajadores móviles que se conectaban alrededor de las computadoras portátiles y los módems.

Para la mayoría, las líneas arrendadas usadas para la conectividad corporativa de los sitios eran los circuitos dedicados que conectaban dos puntos extremos en una red.

Figura 2. Enlaces dedicados

Ya que los circuitos dedicados no eran intercambiados vía la *PSTN* (*Public Switch Telephone Networks*) o Redes de telefonía pública, eran configuradas para el uso de tiempo completo por un solo cliente corporativo. El ancho de banda de ese circuito era dedicado al uso del cliente y no era compartido con otros clientes.

La ventaja de esta configuración es que el cliente tiene ancho de banda y aislamiento garantizados en la conexión. Una desventaja es que el cliente debe pagar el ancho de banda completo en la línea siempre, incluso cuando la línea no es utilizada.

Aunque estas redes eran privadas, ya que consistían en conexiones punto a punto para las líneas dedicadas sólo al tráfico del cliente, estas redes no se podrían llamar redes privadas virtuales, porque más de un cliente del proveedor de red (es decir las compañías telefónicas) no compartían los medios de transmisión.

El siguiente avance significativo para la conexión de los sitios vino con la introducción del servicio de datos digitales (*DDS Digital Data Service*) a mediados de los años 70. El *DDS* era el primer servicio digital para las aplicaciones de la línea privada, ofreciendo las conexiones de 56Kbps a los clientes corporativos.

Mientras que los servicios digitales llegaron a estar más fácilmente disponibles, el interés en las redes de área amplia (*WAN* por sus siglas en inglés) que usaban estos servicios creció. Las conexiones que usaban los servicios E1 que se trabajaban en 2.048 Mbps eran particularmente útiles. Una secuencia de datos E1 consiste en 32 canales separados, cada uno de los cuales puede llevar hasta 64 Kbps de tráfico (llamado una secuencia o canal), voz o datos. Porque estos canales se podrían asignar a diversas aplicaciones. Una compañía podría utilizar una sola línea E1 para ambos servicios de voz y datos, según sus necesidades de la red, asignando diversos números de canales, a cada uso según sus requisitos internos.

A comienzos de los años 90, la fuerza impulsora para las redes privadas eran las comunicaciones de voz, y no de datos. Las compañías telefónicas tradicionalmente vendieron los servicios E1 a los clientes corporativos como manera de crear sus propios sistemas de telefonía privadas a un costo más bajo, precisando que los ahorros de costo de este acercamiento a las comunicaciones de voz permitieron a los clientes dejar el tráfico de datos entre los sitios que llevan de otra manera el ancho de banda sin usar de las conexiones E1.

Pero, como los mercados cambiaron y el costo de las comunicaciones de voz, los ahorros en los costos de las redes privadas de voz desapareció, o fueron reducidos por lo menos grandemente. En el mismo tiempo, el tráfico de los datos había aumentado, y el interés al usar E1s o líneas de 33.6 Kbps para principalmente el tráfico de los datos creció.

Durante el pasado, otras tecnologías del establecimiento de una red como *Frame Relay* y el Modo de Transferencia Asíncrona (*ATM*) han llegado a estar disponibles para formar redes corporativas. El *Frame Relay* ha llegado a ser particularmente popular para conectar diversos sitios juntos. Menos equipo es necesario en cada extremo, porque un enrutador en cada extremo puede tomar el cuidado de dirigir el tráfico a más de un destino. Eso es porque el proveedor de servicio mantiene una "nube" de las conexiones del *Frame Relay*, y las conexiones se asignan solamente según lo necesitado.

Porque se asignan las conexiones del Frame Relay solamente cuando son necesitadas, las redes corporativas del Frame Relay son probablemente las primeras redes privadas virtuales del día moderno.

Aunque esta red del *Frame Relay* puede simplificar algunas conexiones cuando está comparada con el acoplamiento de líneas arrendadas porque el cliente necesita conectar solamente cada sitio con la nube del *Frame Relay* del proveedor y aunque ofrece menos conectividad costosa que líneas arrendadas, la red del *Frame Relay* no trata las necesidades de los trabajadores o de los equipos móviles que requieren conexiones dinámicas al sitio. Usando las redes privadas de líneas arrendadas con conexiones *Frame Relay*, una compañía todavía tiene que mantener los bancos de módems para proporcionar la conectividad a los trabajadores móviles, que se han convertido en más de un problema mientras que la demanda para las comunicaciones móviles y el acceso alejado ha aumentado.

La respuesta convencional al crecimiento corporativo que agrega otro banco de módems o enlace *Frame Relay* no se acopla bien con los ambientes de negocios dinámicos de hoy. El problema con las líneas arrendadas y el *Frame Relay* es que configurarlas toma demasiado tiempo. E, igual si los circuitos de *Frame Relay* se pudieran instalar rápidamente, cada interfaz *WAN* es costosa y requiere la atención, no solamente durante la conexión sino también para el mantenimiento.

Aunque los módems se pueden instalar bastante rápido, pueden no utilizar el ancho de banda necesitado, y pueden implicar gastos indirectos de administración más altos en la forma de ayuda al usuario remoto.

Hoy en día, la situación ha cambiado suficientemente para hacer de la expansión adicional de líneas arrendadas y bancos de módems más grandes un asunto costoso y un requerimiento mayor de administración y recursos de soporte. Y, si arreglos de negocios flexibles son requeridos

con los socios o las oficinas temporales, o los equipos móviles de trabajadores son necesarios, los retardos asociados con el requerimiento e instalación de nuevas líneas arrendadas o conexiones de *Frame Relay* se convierten en contadores productivos si no son claramente inaceptables. Lo que se requiere es una sola solución que no sólo mantenga la seguridad de tráfico corporativo sino que también proporcione la flexibilidad de configuración y conectividad que el negocio de hoy requiere. Esa solución es la red privada virtual.

1.4. Fundamentos de las redes privadas virtuales

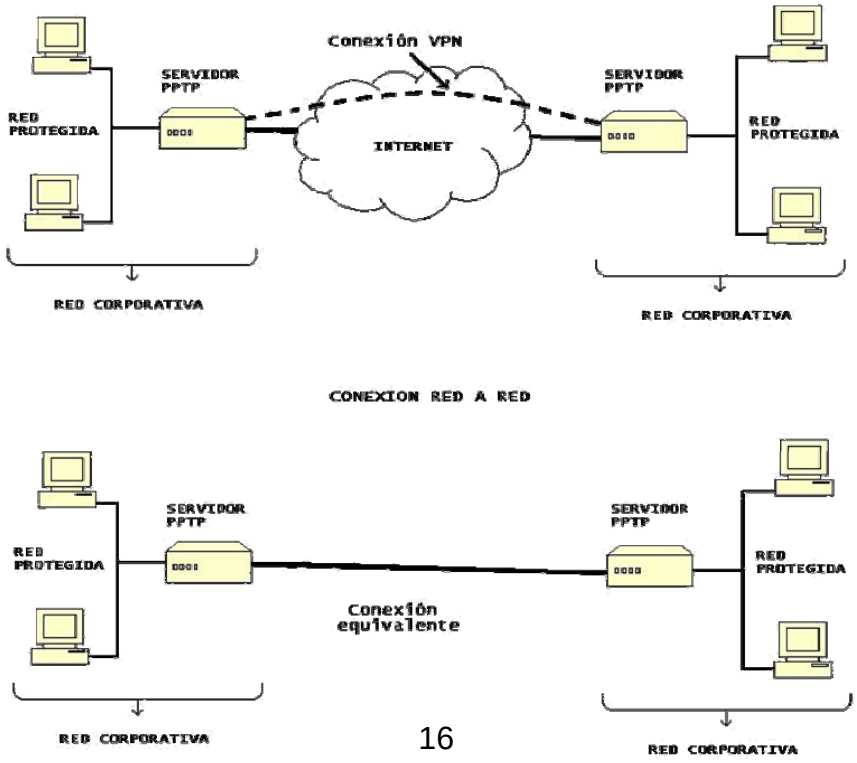
En una red privada virtual o *VPN* de sus siglas en inglés (*Virtual Private Network*) los usuarios parecen estar en una misma red *LAN* (*Local Access Network*), pero en realidad están a varias redes de distancia, estas redes normalmente son públicas. Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe concretarse a tres tareas siendo éstas:

La primera, deben ser capaces de pasas paquetes *IP* a través de un túnel en la red pública; segunda, la solución debe agregar encriptación, de manera que el tráfico que cruce por la red pública no pueda ser espiado, interceptado ni leído o modificado; y la tercera sería la solución debe ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de modo que alguien ajeno a la red no pueda acceder a los recursos del sistema.

Las razones que impulsan al mercado en ese sentido son, fundamentalmente, de costos: es mucho más barato interconectar filiales utilizando una infraestructura pública que desplegar una red físicamente privada. Por otro lado, como es lógico, es necesario exigir ciertos criterios de privacidad y seguridad, por lo que normalmente debemos recurrir al uso de la criptografía.

Una red privada virtual o *VPN* conecta los componentes de una red sobre otra red. Estas redes lo logran al permitir que el usuario haga un túnel a través de Internet u otra red pública, de manera que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas, en la siguiente figura se puede observar el equivalente a una red privada y una virtual.

Figura 3. Red privada virtual equivalente a la red privada



El proceso que siguen las redes privadas virtuales para lograr esto es como sigue:

1) Un servidor protegido envía el tráfico claro a un equipo de *VPN* (el dispositivo de la fuente) localizado en el punto de la conexión a la red pública.

2) El dispositivo de la fuente examina los datos según reglas especificadas por el gerente de la red, asegurando la información o permitiéndole pasar sin afectarla.

3) Cuando la protección de los datos es requerida, el dispositivo encriptador de origen (codifica) y autentica (adjunta una firma digital) el paquete entero, incluso los datos transmitidos así como la dirección de origen y la dirección de destino *IP*.

4) El dispositivo origen adjunta un nuevo encabezado a los datos, incluso la información que el dispositivo de destino requiere para las funciones de seguridad e inicialización del proceso.

5) El equipo de origen *VPN* encapsula lo encriptado y autentifica el paquete con la dirección de origen y destino. Esto da como resultado un túnel virtual a través de la red pública.

6) Cuando el dato llega al dispositivo de destino, es desencapsulado, su firma digital es verificada y el paquete es desencriptado.

Las *VPN* permiten a los usuarios que trabajan en el hogar o en lugares remotos conectarse en una forma segura a un servidor corporativo

remoto, mediante la infraestructura de enrutamiento que proporciona una red pública.

Desde la perspectiva del usuario, la *VPN* es una conexión de punto a punto entre la computadora del usuario y un servidor corporativo. Por su parte, la naturaleza de la red intermedia es irrelevante para el usuario, debido a que aparece como si los datos se estuvieran enviando sobre un enlace privado dedicado.

En ambos casos, una conexión segura a través de la red aparece ante el usuario como una comunicación de red privada, no obstante que esta comunicación sucede sobre una red pública, de ahí el nombre de Red Privada Virtual.

La tecnología de la *VPN* está diseñada para tratar temas relacionados con la tendencia actual de negocios hacia mayores telecomunicaciones, operaciones globales ampliamente distribuidas y operaciones con una alta interdependencia de socios, donde los trabajadores deben conectarse a recursos centrales y comunicarse entre sí.

Para proporcionar a los empleados la capacidad de conectarse a recursos de cómputo corporativos sin importar su ubicación, una compañía debe instalar una solución de acceso remoto que sea confiable y escalable. Por lo común, las compañías eligen una solución basada en:

1) Un departamento de sistemas que está encargado de adquirir, instalar y mantener los conjuntos de módems corporativos y la infraestructura de red privada.

2) Eligen una solución de red de valor agregado, donde contratan a una compañía externa para adquirir, instalar y mantener los conjuntos de módems y una infraestructura de telecomunicaciones.

Sin embargo, ninguna de estas soluciones proporciona la escalabilidad necesaria en términos de costo, la flexibilidad de la administración y gestión, así con la demanda de conexiones. Por tanto, tiene sentido encontrar un terreno intermedio donde la organización complemente sus inversiones actuales en conjuntos de módems y su infraestructura de red privada, con una solución menos costosa basada en tecnología de Internet. De esta manera, las empresas se pueden enfocar a su negocio principal con la garantía de que nunca se comprometerá su accesibilidad y que se instalen las soluciones más económicas.

La disponibilidad de una solución de Internet permite pocas conexiones a Internet (a través de Proveedores Independientes de Servicio, *PSI*) y la implementación de varias computadoras de servidor *VPN* en el borde de la red, a fin de dar servicio a las necesidades remotas de red de cientos o hasta miles de clientes y sucursales remotas.

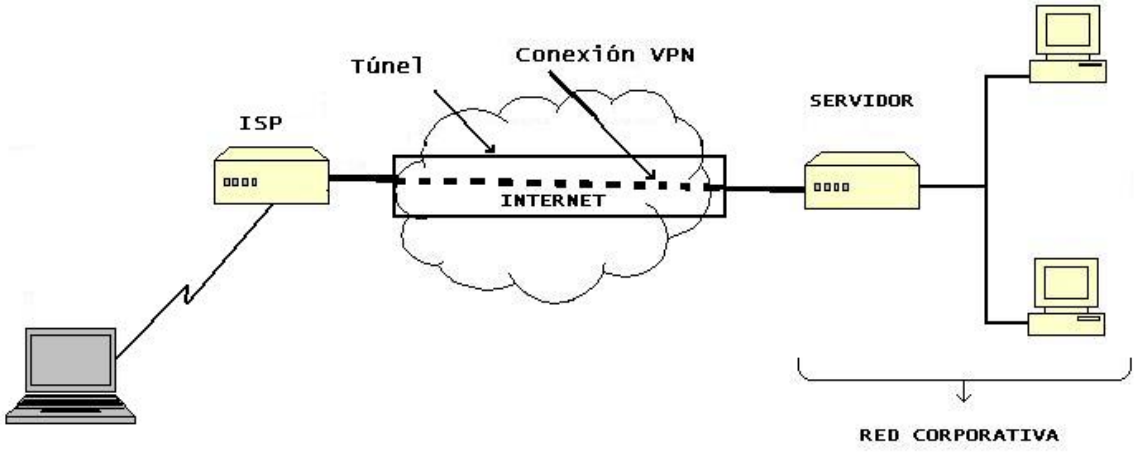
1.4.1. Usos comunes de las redes privadas virtuales

1.4.1.1. Acceso remoto del usuario sobre Internet

Las *VPN* proporcionan acceso remoto a recursos corporativos sobre Internet público, y mantienen al mismo tiempo la privacidad de la

información. La figura 4 muestra una *VPN* utilizada para conectar a un usuario remoto con una red corporativa.

Figura 4. Acceso remoto de un usuario a una red corporativa



fuente: "Microsoft"

En lugar de hacer una llamada de larga distancia a un Servidor de Acceso de Red (*NAS Network Access Server*) corporativo o externo, el usuario llama al *ISP* local. Al utilizar la conexión local al *ISP*, el software de la *VPN* crea una red privada virtual entre el usuario que realiza la llamada y el servidor *VPN* corporativo a través de Internet.

1.4.2. Conexiones de las redes privadas virtuales en Internet

Hay dos métodos para utilizar redes virtuales privadas a fin de conectar redes de área local a sitios remotos:

1.4.2.1. Uso de líneas dedicadas para conectar una sucursal a una LAN corporativa

En lugar de utilizar un circuito dedicado de arrastre extenso entre la sucursal y el servidor corporativo, tanto los ruteadores del servidor de la sucursal como el corporativo pueden emplear un circuito dedicado local e *ISP* local para conectarse a Internet. El software *VPN* utiliza las conexiones *ISP* locales y el Internet público, con el propósito de crear una red privada virtual entre el ruteador de la sucursal y el del servidor corporativo.

1.4.2.2. Uso de una línea telefónica para conectar una sucursal a una LAN corporativa

A cambio de que el ruteador en la sucursal realice una llamada de larga distancia a un *NAS* corporativo o externo el ruteador en la sucursal puede llamar al *ISP* local.

El software *VPN* utiliza la conexión al *ISP* local para crear una red privada virtual entre el ruteador de la sucursal y el del servidor corporativo, a través de Internet.

En ambos casos las facilidades que conectan la sucursal y la oficina corporativa a Internet son locales; se recomienda que el ruteador del

servidor corporativo que actúa como un servidor *VPN* se conecte a un *ISP* local con una línea dedicada. Este servidor *VPN* puede estar listo 24 horas al día para el tráfico *VPN* entrante.

2. SEGURIDAD EN LAS VPN

2.1. Sistemas de autentificación

La autentificación es una parte vital de la estructura de seguridad de las *VPN*. A menos que el sistema no pueda realizar la autentificación de usuarios, servicios y redes, no se podrá controlar el acceso a los recursos corporativos y mantener a los usuarios no autorizados fuera de la red.

La autentificación está basada en uno de los siguientes tres atributos: algo que se posee (una llave de una puerta o una tarjeta); algo que se sabe (una clave); o alguna característica propia (reconocedores de voz, reconocedores de retinas). Esto es generalmente aceptado por expertos de seguridad ya que, un método sencillo de autentificación, tal como una clave, no es adecuado para proteger sistemas, aunque ellos recomiendan que se use por lo menos dos de los atributos mencionados.

La variedad de sistemas *VPN* actualmente disponibles dependen de diferentes métodos de autentificación o combinaciones de ellos. Los sistemas mayormente usados son Claves Tradicionales, Claves de Una Sesión (*S/Key*), sistemas de claves (*PAP, CHAP y RADIUS*), sistemas basados en hardware (tarjetas inteligentes y Tarjetas de Computadora) y sistemas de reconocimiento biométrico (huellas, voz y retina).

2.1.1. Claves tradicionales

Este es, generalmente reconocido por su forma simple de autentificación (por ejemplo nombre de usuario y clave) es inadecuado para seguridad de acceso a las redes. Las claves pueden ser descifradas e interceptadas durante transmisiones de red.

Cuando los usuarios son sumamente cuidadosos de resguardar sus claves, ellos no pueden usar los servicios de Internet ofrecidos sin protección para sus claves. Por ejemplo, servicios tales como *FTP* y *Telnet* transmiten sus identificadores y claves como textos planos, haciéndolos más fácil de usar cuando se intercepta.

Los Sistemas de Clave de Una Sesión, restringen la validación de una clave en una sesión sencilla, puede ser una buena solución para algunos de los problemas alrededor del uso de claves tradicionales.

2.1.2. Claves de una sesión

Una manera de prevenir el uso no autorizado de una clave interceptada es prevenirla de ser rehusada. Uno esperaría del nombre, sistemas de clave de una sesión que apuntan directamente a lo que se tiene que hacer, porque se requiere una clave nueva para cada nueva sesión. Estos sistemas, despejan al usuario de la dificultad de siempre elegir una nueva clave para la siguiente sesión ya que automáticamente se genera una lista de claves aceptables para el usuario.

El uso de una frase secreta, generada por el usuario, genera una secuencia de claves de una sesión. La frase secreta del usuario nunca viaja a través de su computadora local y no viaja a través de la red; de allí que la frase secreta no está sujeta a ataques. Además, porque una diferente clave es generada para cada sesión, una clave interceptada no puede ser usada de nuevo, y no le da al atacante ninguna información sobre la siguiente clave a ser usada.

Una secuencia de claves de una sesión es producida por la aplicación de una función segura "*Hash*", múltiples veces a el cuerpo del mensaje, producida en el paso inicial. En otras palabras, la primer clave es producida pasando el cuerpo del mensaje a través de la función *Hash* N veces, donde N es especificado por el usuario. La siguiente clave es generada pasando el mensaje a través de la función *Hash* N-1 veces, y así sucesivamente hasta N claves generadas.

Cuando un usuario intenta ingresar en una red, el servidor de la red que es el servidor de claves habilita al organizador que protege la entrada a la red, presenta un texto que consiste en un número y un arreglo caracteres que se llama la semilla.

En respuesta al servidor de claves, el usuario entra el texto más su frase secreta en el software generador de claves que ejecuta en su computadora. El programa generador, entonces combina la frase con la semilla e interacciona la función *hash* repitiendo la operación él número de veces correspondientes a él número dado por el servidor. El resultado del cálculo es una contraseña que asume la forma de seis palabras en inglés.

La clave es enviada al servidor de red, éste le aplica la función *hash* y compara el resultado con la clave almacenada que fue usada, para el más reciente ingreso. Si ellas concuerdan, al usuario se le permite ingresar a la red. El número entonces se decrementa y la última clave se guarda para la siguiente sesión.

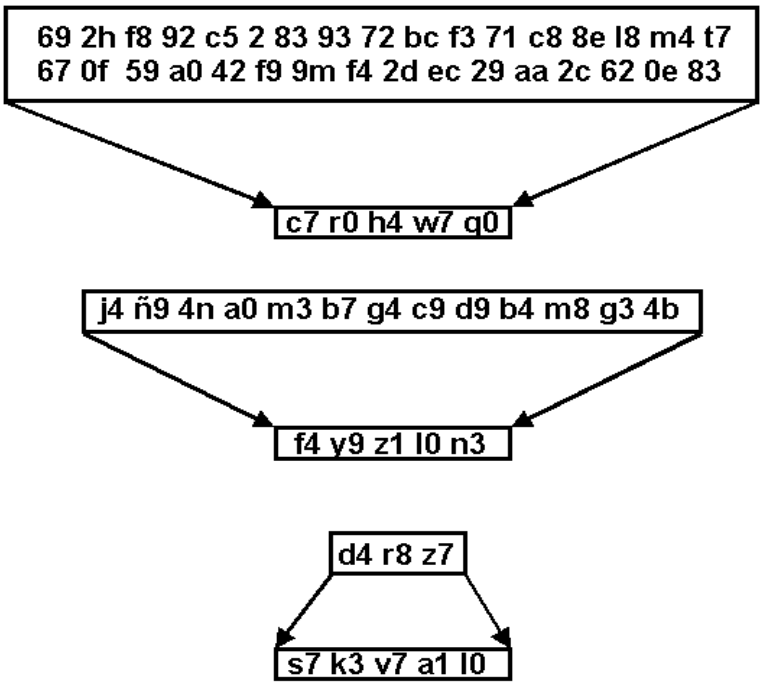
2.1.3. Funciones *Hash*

Las funciones *hash* o también llamadas funciones resumen, son usadas principalmente para resolver el problema de la integridad de los mensajes, así como la autenticidad de mensajes y de su origen.

Una función *hash* es también ampliamente usada para la firma digital, ya que los documentos a firmar son en general demasiado grandes, la función *hash* les asocia una cadena de longitud 160 *bits* que los hace más manejables para el propósito de firma digital.

De forma gráfica la función *hash* efectúa lo siguiente:

Figura 5. Muestra de una función *Hash*



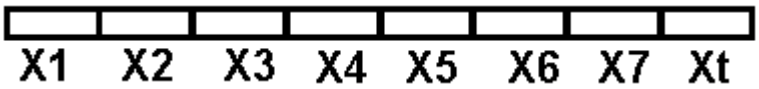
Esto es, un mensaje de longitud arbitraria lo transforma de forma "única" a un mensaje de longitud constante.

La forma de hacerlo es de la siguiente forma:

La función *hash* toma como entrada una cadena de longitud arbitraria, por ejemplo: 4773 bits, luego divide éste mensaje en partes iguales, como de 150bits; como en este caso y en general el mensaje original no será un múltiplo de 150, entonces para completar un número entero de partes de 150 bits al último se le agrega un relleno, podría ser como de puros ceros. En nuestro caso en 4773 caben 31 partes de 160 *bits* y sobran 123, entonces se agregarán 27 ceros más.

Entonces el mensaje toma la forma X = X1, X2, X3,…,Xt donde cada Xi tiene igual longitud (150 *bits* por ejemplo).

Figura 6. Mensaje dividido en tramas iguales



Posteriormente se asocia un valor constante a un vector inicial IV y

$$H0=IV$$

Ahora se obtiene H1 que es el resultado de combinar H0 con X1 usando una función de compresión *f*

$$H1 = f(H0,X1)$$

Luego se obtiene H2, combinando H1 y X2 con *f*

$$H2 = f(H1,X2)$$

Se hace lo mismo para obtener H3

$$H3 = f(H2,X3)$$

Hasta llegar a Ht

$$Ht = f(Ht-1, Xt)$$

Entonces el valor *hash* será *h*(M) = Ht

De alguna forma lo que se hace es tomar el mensaje partirlo en pedazos de longitud constante y combinar de alguna forma pedazo por pedazo hasta obtener un solo mensaje de longitud fija.

Los sistemas de contraseña como el *S/Key* requieren que el software del servidor sea modificado para realizar los cálculos requeridos y que cada computadora remota tenga una copia del programa de cliente. Estos sistemas no pueden ser muy escalables que porque es difícil de administrar la lista de contraseñas para un número grande de usuarios.

2.1.4. Protocolo de autentificación de claves (*Password Authentication Protocol PAP*)

PAP fue originalmente diseñado como un método simple para verificar la identidad del otro extremo, cuando el protocolo punto a punto (*PPP*) es usado como el protocolo de comunicación. El *PAP* es un protocolo de entrelazamiento, el servidor hace la conexión enviando un nombre y su clave al sistema designado con el cual se intenta establecer una conexión, y entonces el sistema autentificador reconoce la computadora y aprueba la comunicación.

Tras la fase de establecimiento de la conexión un par de identificador/contraseña (*login/password*) es enviado al otro extremo, esperando su asentimiento. Esto tiene lugar sólo una vez, inmediatamente después del establecimiento de la conexión.

PAP no es un método del todo seguro, ya que las contraseñas se envían por el medio sin ningún tipo de encriptación, además, no existe ninguna protección contra la repetición de intentos.

El formato de un paquete *PAP* es como sigue:

Código	Identificador	Longitud	Datos
8 *bits*	8 *bits*	16 *bits*	Long. variable

- **Código.**

Este campo ocupa un octeto, e indica el tipo de paquete *PAP*:

***Authenticate-Request*.**

Este tipo de paquete se usa para iniciar el mecanismo del protocolo *PAP*. Si se requiere verificación, cada extremo que requiera identificarse debe enviar un paquete *Authenticate-Request*, conteniendo el identificador y la contraseña. Si los datos son los esperados, se enviará un paquete *Authenticate-Ack.* Como éste último puede perderse, los paquetes *Authenticate-Request* se envían repetidamente hasta conseguir el asentimiento.

***Authenticate-Ack* y *Authenticate-Nak*.**

Si el par identificador/contraseña es reconocible y aceptable, el receptor envía un paquete *Authenticate-Ack*, mostrando su conformidad. Si los datos son irreconocibles o no válidos, el receptor envía un paquete *Authenticate-Nak.*

- **Identificador**

  Este campo ocupa un octeto, y realiza una función de apoyo en la gestión de envíos/respuestas.

- **Longitud.**

  Este campo ocupa dos octetos, e indica la longitud del paquete PAP, incluyendo a los campos código, identificador, longitud y datos.

- **Datos**

  Este campo consta de cero o más octetos. Su formato varía según el tipo de paquete (especificado en el campo *tipo*).

2.1.5. Protocolo de autentificación de entrelazamiento *CHAP*

El protocolo de autenticación *CHAP* (*Challenge-Handshake Authentication Protocol*) es usado para verificar periódicamente la identidad del otro extremo de la conexión. La verificación se produce inmediatamente después de la fase de establecimiento de la conexión, y puede repetirse en cualquier momento, con el enlace ya establecido.

Los pasos a seguir son:

1) El extremo que quiere verificar la identidad del otro equipo, le envía un mensaje de prueba.

2) El equipo que se esta verificando responde con un valor calculado mediante un algoritmo.

3) El autentificador compara la respuesta de su par con su propio cálculo del valor correcto. Si los valores coinciden, el autentificador envía un asentimiento, indicando su conformidad. Si no se ha recibido el valor correcto, la conexión debe terminarse.

4) A intervalos aleatorios, el autentificador envía un nuevo mensaje a el equipo con el que se está comunicando, y se repiten los pasos 1 y 3.

2.1.5.1. Ventajas del protocolo *CHAP*

El protocolo *CHAP* provee protección contra la repetición de intentos por parte del par que debe ser autenticado, mediante el uso de un identificador que se va incrementando en cada mensaje y un valor variable para la prueba.

El tiempo que transcurre entre una autenticación y otra es el límite para un posible intento de violar la protección. El autentificador es el que decide la frecuencia de los mensajes de prueba.

Este método de autenticación depende de una contraseña conocida únicamente por el autentificador y el par con el que se realiza la comunicación, esta contraseña no es enviada por el enlace. El protocolo *CHAP* funciona básicamente en un solo sentido, pero puede negociarse el uso de la misma contraseña para ser usada en una autenticación mutua, en dos direcciones.

2.1.5.2. Desventajas

El protocolo *CHAP* requiere que la contraseña no esté encriptada. Cuando se desee autenticar todas las conexiones que se producen en instalaciones grandes, cada posible contraseña debe estar presente en todos los posibles extremos. Para evitar esto, es recomendable que los mensajes de prueba y sus respuestas sean examinados en un servidor central. Si no es así, las contraseñas deben enviarse a cada posible extremo mediante alguna forma de encriptación.

2.1.5.3. Requerimientos del formato *CHAP*

El algoritmo de *CHAP* requiere que la longitud de la contraseña sea al menos de un octeto, aunque en la realidad se usan valores mayores. En la actualidad, se usa un valor de contraseña de 16 octetos. La contraseña debe ser lo suficientemente larga para que exista una protección fiable contra la repetición de intentos.

Cada valor para un mensaje de prueba debe ser único, de otra forma se podría violar la protección interceptando un mensaje de respuesta con el que se podría responder a un mensaje de prueba.

Además, el valor de la contraseña debe ser totalmente impredecible, para evitar que pueda ser calculado, de otra forma podría enviarse un mensaje con un valor futuro, interceptar la respuesta y usarla para responder a un mensaje de prueba.

El formato de un paquete *CHAP* es como sigue:

Código	Identificador	Longitud	Datos
1 octeto	1 octeto	2 octetos	Long. variable

- **Código**

  Este campo ocupa 1 octeto, e identifica el tipo de paquete *CHAP*, lo códigos son:

  1 Prueba
  2 Respuesta
  3 Asentimiento
  4 Fallo

- **Identificador**

  Este campo ocupa un octeto. Su valor sirve de apoyo en la gestión de las pruebas, respuestas y réplicas.

- **Longitud**

  Este campo ocupa 2 octetos, e indica la longitud del paquete *CHAP*, incluidos los campos de código, identificador, longitud y datos. Cualquier octeto fuera del rango indicado por este campo debe ser tratado como de relleno.

- **Datos**

  Este campo ocupa 1 o más octetos. Su formato es dependiente del tipo de paquete *CHAP*, indicado en el campo código.

En modo de prueba/respuesta varía de la siguiente forma:

Código	Identificador	Longitud	Long. Valor	Valor	Nombre
1 octeto	1 octeto	2 octetos	1 octeto	Long. Variable	Long. variable

Estos nuevos campos usados en lugar del campo de Datos son los siguientes:

- **Longitud del valor**

  Este campo ocupa 2 octetos, e indica la longitud del valor usado.

- **Valor.**

  Este campo ocupa 1 o más octetos. El valor debe cambiarse en cada nuevo paquete de prueba. En el paquete de respuesta, el valor es calculado en base al identificador, al valor de la contraseña y al valor en el mensaje de prueba.

- **Nombre**

  Este campo ocupa 1 o más octetos, e identifica al sistema que envía el paquete.

El paquete de prueba es usado para iniciar el protocolo *CHAP*. El autentificador envía un paquete *CHAP* con código 1 (prueba). Debe repetirse el envío hasta que se reciba un mensaje de respuesta o expire un contador de reintentos.

Un paquete *CHAP* de prueba puede enviarse en cualquier momento de la conexión. Cuando se recibe un mensaje de prueba, debe enviarse un mensaje *CHAP* con el campo código 2 (respuesta). Cuando el autentificador recibe el mensaje de respuesta. Compara el valor de la respuesta con el que ha calculado, y envía un mensaje de asentimiento o de fallo.

Como el asentimiento puede perderse, el extremo que es verificado debe enviar paquetes de respuesta hasta que reciba el asentimiento o el fallo. Para gestionar la comunicación, todos los mensajes repetidos tanto de prueba como de respuesta deben tener el mismo identificador.

En modo de asentimiento y fallo el campo de datos queda de la misma forma.

Código	Identificador	Longitud	Datos
1 octeto	1 octeto	2 octetos	long. variable

El campo datos ocupa cero o más octetos, y su contenido está pensado para ser leído por una persona, su longitud recomendada es entre 32 y 126 caracteres. Este campo no afecta al funcionamiento del protocolo.

Si el valor recibido en el mensaje de respuesta es igual al esperado, el autentificador envía un paquete *CHAP* con el código 3 (asentimiento).

Si el valor recibido en la respuesta no es igual al esperado, el autentificador envía un paquete con el código 4 (fallo), y toma las acciones para terminar la conexión.

2.1.6. Servicio de autentificación de usuario remoto vía telefónica (*RADIUS*)

Este protocolo (llamado *RADIUS*) permite usar un modelo de cliente / servidor para autenticar firmemente y administrar la conexión y sesiones de usuarios de red remotos. El protocolo es una manera de hacer el control de acceso más manejable, y puede soportar otros tipos de autenticación del usuario, incluso el protocolo *PAP* y el *CHAP*.

Este modelo de cliente / servidor usa un servidor de acceso de red (*NAS Network Access Server*) para administrar las conexiones de usuarios. Aunque el *NAS* funciona como un servidor para proveer acceso a la red, este también funciona como un cliente para el protocolo.

El *NAS* es responsable de aceptar los requerimientos de conexión del usuario, consiguiendo el identificador del usuario y contraseña y pasando la información seguramente al servidor *RADIUS*. El servidor *RADIUS* retorna el estado de la autenticación aprobada o denegada, así como cualquier configuración de datos requeridos por el *NAS* para proporcionar servicios al usuario final.

El cliente y el servidor se comunican seguros, usando contraseñas compartidas para autenticación y encriptación para transmitir las contraseñas de los usuarios.

El protocolo *RADIUS* crea una base de datos centralizada de usuarios y servicios disponibles, una característica particularmente importante para redes que incluyen un gran banco de módems y más de un servidor para comunicaciones remotas. El servidor *RADIUS*, es el que administra la autenticación del usuario y el acceso a los servicios de una locación. Porque cualquier dispositivo que soporte *RADIUS* puede ser un cliente, un usuario remoto tendrá acceso a los mismos servicios desde cualquier servidor de comunicaciones que se comunique con el servidor.

2.2. Introducción a la Criptografía

2.2.1. Encripción

La encripción o codificación de la información es usada para prevenir que esta sea leída por personas no autorizadas.

Para que la encripción trabaje apropiadamente, ambos el emisor y el receptor tienen que saber que conjunto de reglas, llamado cifrador, fue usado para transformar la información original a esta forma codificada, a veces es llamada cifrador de texto. Un simple cifrador puede agregar un número arbitrario de caracteres, al total de caracteres del mensaje. Con tal de que el receptor sepa lo que el emisor le hizo al mensaje, la parte receptora puede revertir el proceso para extraer el mensaje original.

La encripción está basada en dos componentes: un algoritmo y una clave. Un algoritmo criptográfico es una función matemática que combina información legible con una cadena de dígitos llamada clave para producir texto cifrado. La clave y el algoritmo usados son cruciales para la encripción.

Aunque algunos algoritmos para encripción no usan una clave para existir, los algoritmos que usan claves son particularmente importantes. La encripción en sistemas basados de claves ofrece dos importantes ventajas:

Primera, los algoritmos de encripción son difíciles de desarrollar; por lo que no se quisiera hacer un nuevo algoritmo cada vez que se desea comunicar privadamente. Usando una clave, se puede usar el mismo algoritmo para comunicarse con muchas personas; todos tienen que usar una clave diferente para cada uno.

Segunda, si alguien interviene el mensaje encriptado, todos tienen que volverse a conectar con una nueva clave para empezar a encriptar los mensajes, todos de nuevo; uno no tiene que conectarse con un nuevo algoritmo, a menos que sea el algoritmo el que demuestre no ser seguro.

El número de posibles claves que cada algoritmo puede soportar depende del número de *bits* de la clave. Por ejemplo una clave de 7 *bits* permite 128 posibles combinaciones numéricas o claves. Mayor número de llaves posibles hace más difícil que el mensaje encriptado sea roto.

El nivel de dificultad por consiguiente depende en la longitud de la clave. No tomaría a una computadora mucho suponer cada una de las 128 posibles claves y desencriptar secuencialmente el mensaje para ver si tiene sentido. Pero, si una clave de 128 *bits* fuera usada, que es igual a buscar 2^{128} claves, y

si la computadora pudiera suponer 1 millón de claves cada segundo, podría tardar muchos siglos realmente para descubrir la clave correcta.

La seguridad de un algoritmo de encripción está unida con la longitud de la clave. Porque conociendo que una clave es de n *bits* de largo, da una idea de que cuanto tiempo se esperaría para quebrantar el código.

Si la seguridad dependiera de muchas cosas como lo secreto del algoritmo, o la inaccesibilidad del cifrador de texto, personas no autorizadas podrían derivar esa información de publicaciones o de análisis de patrones de los mensajes, o ellos podrían recolectar la información de otras maneras como monitorear el tráfico. Cuando la información esta en sus manos, ellos pueden usarla para desencriptar las comunicaciones.

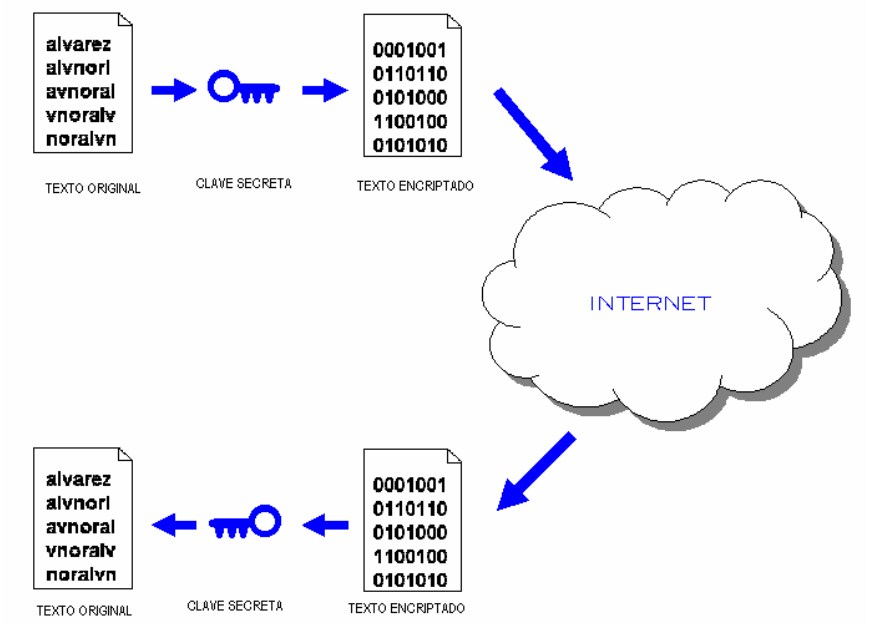
La criptografía se encuentra dividida en dos áreas principales: Criptografía simétrica y Criptografía asimétrica o de claves públicas.

2.2.2. Criptografía simétrica

La forma más antigua de criptografía basada en claves es llamada de claves secretas o encripción simétrica. En este caso, ambos el emisor y receptor poseen la misma clave, lo que significa que ambas partes pueden encriptar y desencriptar datos con la clave. Pero este método tiene ciertos inconvenientes como: ambas partes deben estar de acuerdo en compartir dicha clave.

Si se tienen n usuarios entonces se tiene que guardar una lista de n claves, una para cada usuario. Si se usa la misma clave para más de un usuario, entonces ellos podrán leer la información de los otros.

Figura 7. Claves secretas



La encripción simétrica tiene un problema con la autenticidad, porque la identidad del origen del mensaje o el receptor no puede ser probada. Esto porque ambos poseen la misma clave, ambos pueden crear y encriptar un mensaje y clamar que otra persona lo envió. La forma de resolver este problema es usar la Criptografía de claves públicas.

2.2.3. Criptografía asimétrica o claves públicas

La criptografía asimétrica o de claves públicas fue inventada en 1976 por los matemáticos Whit Diffie y Martin Hellman y es la base de la moderna criptografía.

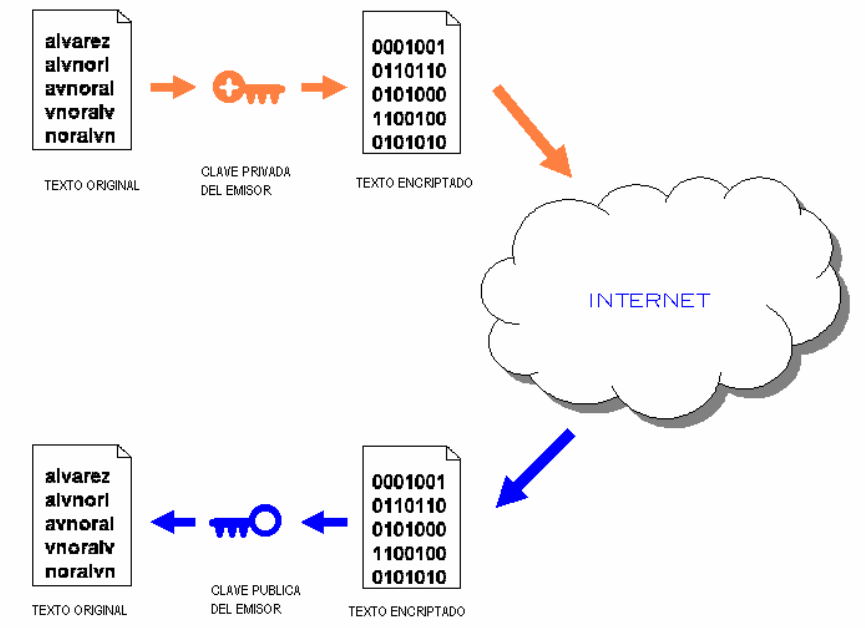
La criptografía asimétrica utiliza dos claves complementarias llamadas clave privada y clave pública. Lo que está codificado con una clave privada necesita su correspondiente clave pública para ser descodificado. Y viceversa, lo codificado con una clave pública sólo puede ser descodificado con su clave privada.

Las claves privadas deben ser conocidas únicamente por su propietario, mientras que la correspondiente clave pública puede ser dada a conocer abiertamente.

La criptografía asimétrica está basada en la utilización de números primos muy grandes. Si multiplicamos entre sí dos números primos muy grandes, el resultado obtenido no puede descomponerse eficazmente. El proceso será más seguro cuanto mayor sea el tamaño de los números primos utilizados. Los protocolos modernos de encriptación utilizan claves generadas con números primos de un tamaño tal que los haga completamente inquebrantables.

El problema de las claves asimétricas es que cuando el texto a tratar es largo, el proceso de codificación es muy lento. Los protocolos modernos codifican el texto base con una clave simétrica y utilizan las claves asimétricas para la comunicación de la clave simétrica utilizada.

Figura 8. Claves públicas



Estas claves pueden ser usadas en dos diferentes maneras: proveer un mensaje confidencialmente y proveer la autenticidad del origen del mensaje. En el primer caso, el emisor usa la clave pública de receptor para encriptar un mensaje que se mantendrá confidencial hasta que sea decodificado por el receptor con la clave privada. En la segunda parte, el emisor encripta un mensaje usando la clave privada, una clave de la cual sólo el emisor tiene acceso.

Aunque encriptar un mensaje con un par de claves públicas no es muy diferente de usar el sistema de encripción de clave secreta, los sistemas de clave pública ofrecen algunas ventajas.

Por ejemplo, la clave pública de nuestro par de claves puede ser completamente distribuida sin sentir que se compromete el uso de las claves

privadas. Por lo que no se tiene que enviar una copia de la clave pública a todos, ellos pueden conseguirlas de un servidor de claves mantenidas por la compañía o por un proveedor de servicio.

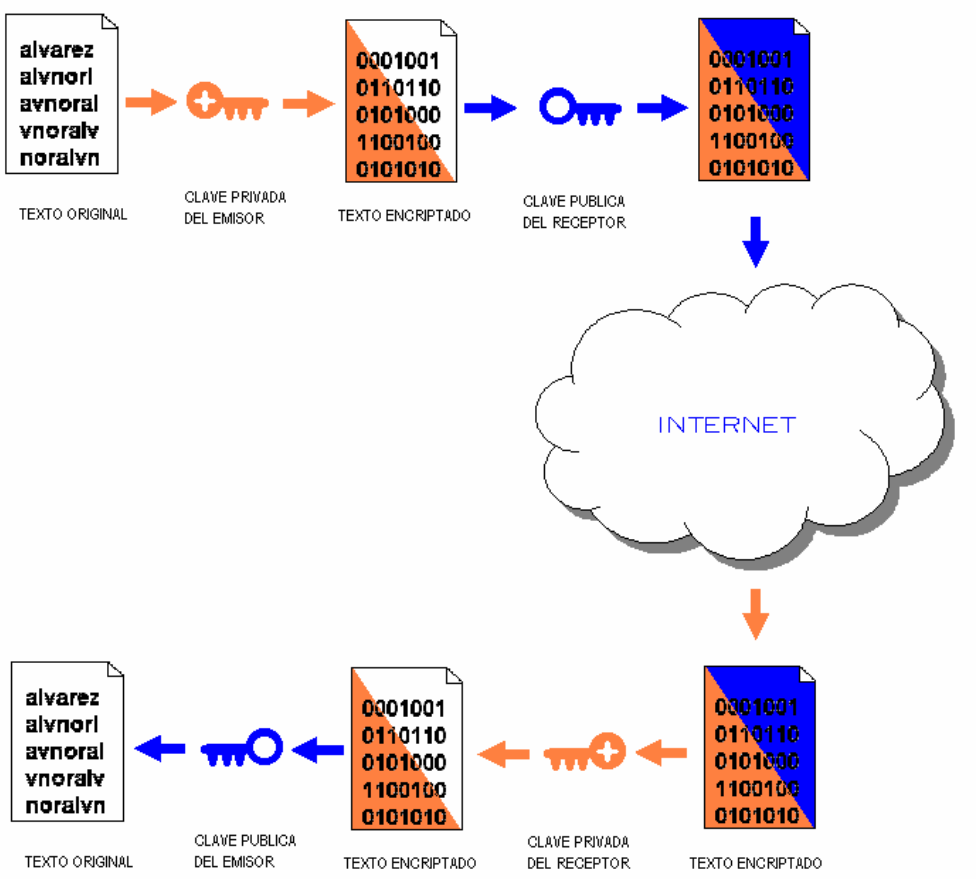
Otra ventaja de este sistema es que permite autentificar el origen del mensaje. La idea básica es que como el emisor es la única persona quien puede encriptar algo con su clave privada, cualquiera usando su clave publica para desencriptar el mensaje, puede estar seguro que el mensaje viene del emisor conocido.

Pero existe el problema que todos los que posean la clave pública del emisor podrían ver el mensaje, para evitar esto el emisor primero encripta el mensaje con su clave privada y posteriormente con la clave pública del receptor a quien desea enviarle el mensaje. El receptor al recibir el mensaje debe de usar su clave privada para poder desencriptarlo y posteriormente usar la clave pública del emisor para recuperar el mensaje.

El uso de una clave privada en un documento electrónico es similar a usar un documento en papel firmado. El receptor entonces certificará que el mensaje viene del emisor conocido pero no puede estar seguro que alguien lo haya leído, esto se puede observar en la figura 8.

Algunos algoritmos de criptografía rápida para generar mensajes “resumidos” son conocidos como funciones *hash* de una vía. El mensaje resumido puede decirle al propietario de este que el mensaje no ha sido alterado, pero las firmas digitales son más confiables. Si se codifica el mensaje resumido con una llave privada, uno ha conseguido una firma digital.

Figura 9. Encripción del mensaje con dos claves



2.2.4. Criptografía de llaves públicas *RSA*

Su nombre viene de sus tres desarrolladores Ron Rivest, Adir Shamir, and Leonard Adelman. La seguridad de ésta está basada en el hecho de que puede ser relativamente fácil multiplicar números primos grandes juntos, pero es casi imposible de factorizar el producto resultante. Esta técnica produce llaves públicas que están atadas a llaves privadas específicas.

Esto da la ventaja de habilitar al poseedor de una llave privada para encriptar los datos, así que nadie con una copia de la llave pública puede desencriptarlo.

Las llaves *RSA* consisten de tres valores numéricos especiales que son usados en pares para encriptar o desencriptar la información. La llave pública *RSA* consiste de un valor de llave pública y un módulo. El módulo es el producto de dos números primos grandes, elegidos al azar, esos están matemáticamente relacionados para elegir la llave pública. La llave privada es calculada de los dos números primos que son generados por el módulo y el valor de llave pública.

En la práctica la llave privada no puede ser derivada porque no hay manera práctica de calcular los valores de los dos primeros números seleccionados factorizando el módulo.

2.2.5. Infraestructura de claves públicas

Los servicios de seguridad que hacen posible la generación de claves están bajo la sombra del término de Infraestructura de claves públicas (*PKI Public Key Infraestructure*). Un *PKI* permite a las organizaciones definir los dominios de la seguridad en la cual ellos emiten claves y los certificados asociados, los cuales son objetos electrónicos usados para emitir y validar claves públicas.

Un *PKI* hace esto posible no únicamente para usar claves y certificados, también permite administrar claves, certificados y políticas de seguridad. Sin tal

sistema, el uso de claves públicas podría ser caótico, ineficiente y probablemente no sería seguro.

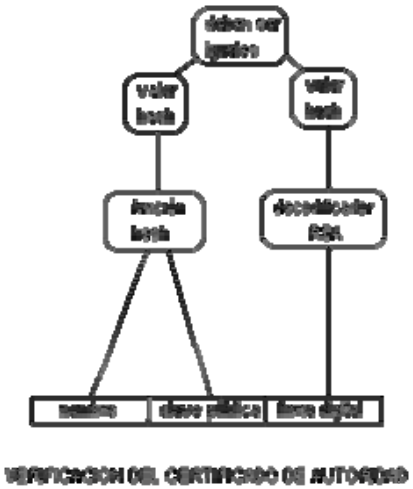
2.2.6. Certificados de claves públicas

Estos son especialmente formados de bloques de datos que nos dice el valor de una clave pública, el nombre del propietario de la clave, y una firma digital de la organización que la emitió, todo esto es llamado certificado de autoridad (*CA*).

Estos certificados son usados para identificar al propietario de una clave pública particular. Con que se tenga una copia de la clave publica de autoría, se puede usarla para verificar los certificados que se firmó.

Cualquier programa de codificación que se usa debe tener una copia de la clave pública del certificado de autoridad para verificar la firma digital de un certificado.

Figura 10. Verificación de los certificados de autoridad



2.2.7. Generación de claves públicas

Para usar criptografía de claves públicas, se necesita generar una clave pública y una clave privada. Después de haberlas generado, se tiene la responsabilidad de mantener seguras las claves privadas y no permitirle a nadie mas verlas. Entonces se tiene que decidir como distribuir las claves públicas a sus corresponsales.

Hay dos temas a tratar con la generación de claves públicas: algunos sistemas las generan en el servidor que pertenece al propietario de la clave, y otros generan las claves como parte de la generación de certificados.

Primero se puede generar la clave en la computadora del propietario. El usuario genera un par de claves públicas guardando la clave privada, y enviando la clave pública al autorizador de certificados para producir un certificado.

El segundo método es que la autoridad de certificados tiene que generar el par de claves públicas, produce el certificado firmado, y entonces envía ambos el par de claves y el certificado del usuario.

2.2.8. Selección de los métodos de encripción

En la tabla I se detallan algunas de las ventajas y desventajas de cada tipo de encripción.

Al seleccionar un apropiado algoritmo para usar, la regla general es: primero, determinar que tan sensitivos son los datos, por cuanto tiempo serán sensitivos y por cuanto deberán ser protegidos.

Tabla I. Ventajas y desventajas de los métodos de encripción

TIPO DE ENCRIPCIÓN	VENTAJAS	DESVENTAJAS
	Es rápido	Ambas claves son iguales
SIMÉTRICO	Puede ser fácilmente implementado	Dificultad para la distribución de las claves
		No soporta firmas digitales
	Usa dos claves diferentes	Programación lenta y compleja
ASIMÉTRICO	Relativamente fácil para distribuir sus claves	
	Provee integridad	

Cuando se ha determinado eso, se selecciona un algoritmo y la longitud de la llave para la cual tomará mucho más tiempo que el tiempo para el que sus datos serán sensibles de romper.

En la tabla II se detallan la longitud de claves usadas en los sistemas simétricos y asimétricos para el mismo nivel de seguridad.

Tabla II. Longitudes de claves de los métodos de encripción

SIMÉTRICO	ASIMÉTRICO
56 *BITS*	384 *BITS*
64 *BITS*	512 *BITS*
80 *BITS*	768 *BITS*
112 *BITS*	1762 *BITS*
128 *BITS*	2304 *BITS*

Cuando se selecciona los programas o el equipo, se debe recordar que más de un sistema de encripción puede ser usado en el producto. Eso es una práctica común de los diferentes requerimientos de computación para algoritmos de claves secretas o públicas.

2.3. Administración de la seguridad

2.3.1. Políticas corporativas de seguridad

La seguridad en la red es solo una parte, aunque una parte importante en estos días, de seguridad corporativa y debe concordar con las políticas de seguridad de la corporación.

Una política sólida de seguridad debe de hacer lo siguiente:

Ver lo que se intenta proteger
Ver lo de que se necesita proteger
Determinar como son probablemente las amenazas

Implementar medidas que protegerán los recursos en una forma costo-efectividad
Debe revisar el proceso continuamente
Debe mejorar aspectos cada vez que se encuentre una debilidad.

Una política tradicional identifica todo de los recursos en la información de la infraestructura corporativa que están siendo protegidos, los equipos de computación y las bases de datos corporativas. Esta política debe incluir todo desde el acceso físico a la propiedad, acceso general a los sistemas de información y acceso específico a los servicios de esos sistemas.

Pero, como los sistemas de información se han hecho mas distribuidos, las políticas de seguridad han tenido que incluir guías en los departamentos gobernantes de las *LAN* también. Esto significa agregar políticas para quienes usan los recursos pertenecientes a diferentes departamentos.

Cuando se definen las políticas de seguridad de la red, se deben identificar todos los puntos de acceso a los sistemas de información y definir las directrices políticas para proteger esos puntos de entrada/salida. No se debe pasar por alto los módems que los empleados pueden tener en sus oficinas, los cuales pueden invitar a personas no autorizadas a ingresar a estos puntos como usuarios de servicios en línea.

Uno de los nuevos problemas en política de seguridad que surge al crear una red privada virtual es la administración de claves. En el pasado, si una línea arrendada era usada, la capa de encripción del enlace pudo haber sido usada, lo cual no requería intercambio de claves encriptadas. Pero, la naturaleza más dinámica y agregada flexibilidad de la *VPN* basada en Internet requiere una amplia distribución de claves y más frecuente recodificación, lo

cual requiere sistemas más complicados para administrar claves. Esto es verdadero sobre todo cuando los usuarios remotos son involucrados.

El tráfico entre servidores debe de protegerse contra ataques como lo son los virus informáticos, y debería ser una parte importante de las políticas de seguridad. Los virus están aquí para quedarse, así para impedir las costosas infecciones, los programas antivirus deben ser incluidos en la aplicación de seguridad.

2.3.2. Longitud de las claves

Se debe determinar la sensibilidad de los datos así que se debe calcular cuánto tiempo serán sensibles y cuánto tiempo tendrán que ser protegidos. Cuando se ha deducido eso, se puede seleccionar un algoritmo de encripción y la longitud de clave que deben tomar mucho más tiempo para que puedan romperse, que la longitud de tiempo del cual los datos serán sensibles.

Tabla III. Tiempo requerido para descifrar claves

Long, de Clave	Número de posibles claves	Tiempo requerido con 1 encrip/ us	Tiempo requerido con 10^6 encrip/us
32	$2^{32} = 4.3 \times 10^9$	2^{32} us = 35.8 min	2.15 miliseg
56	$2^{56} = 7.2 \times 10^{16}$	2^{56} us = 1,142 años	10.01 horas
128	$2^{128} = 3.4 \times 10^{38}$	2^{128} us= 3.4×10^{24} años	5.4×10^{24} años

2.3.3. Administración de claves para compuertas

Un número de claves son usualmente requeridas para asegurar las comunicaciones entre dos compuertas. Primero es el par de claves que identifican dos compuertas para cada una de otra, estas pueden ser intercambiadas manualmente o ser transmitidas vía los certificados digitales. Segundo esta la sesión de claves requerida para autentificación y codificación de los paquetes transmitidos entre compuertas.

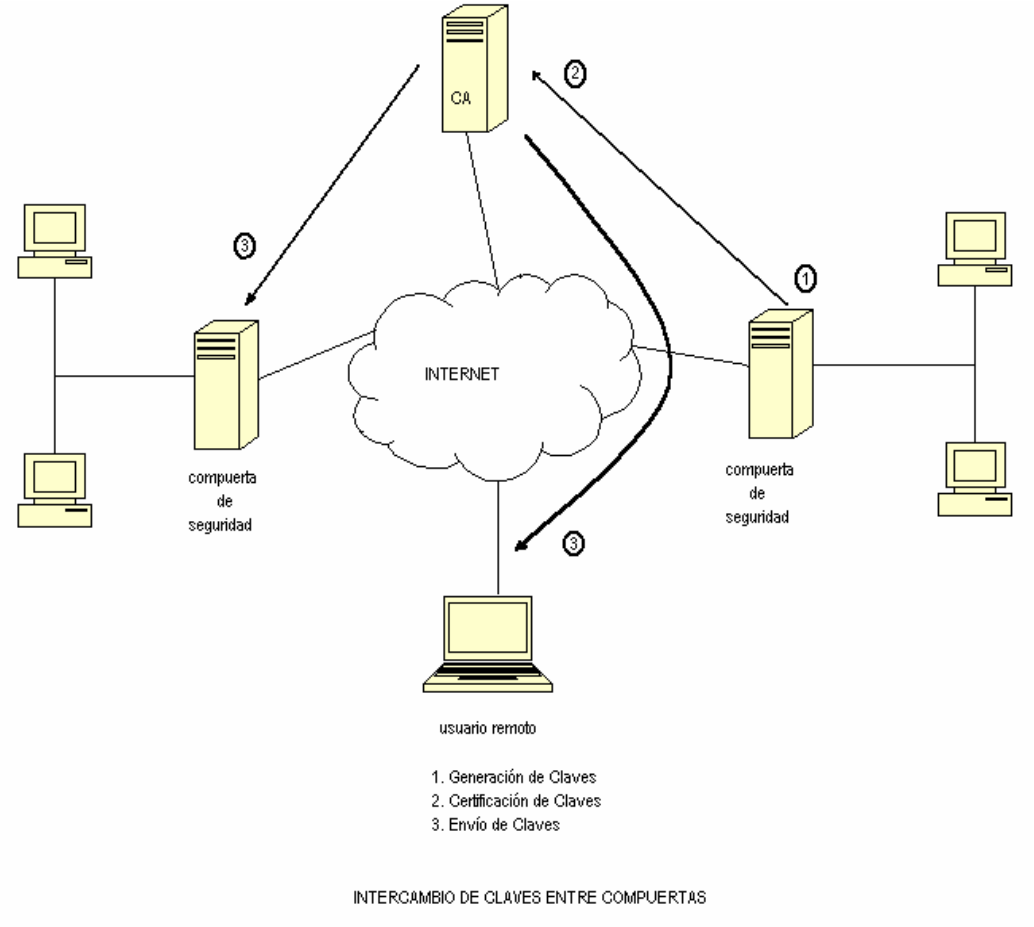
2.3.3.1. Identificación de compuertas

Después de establecido un túnel seguro entre dos compuertas, los dispositivos deben ser autentificados y estar de acuerdo con una clave. Las compuertas que usan pares de claves públicas pueden ser autentificadas manualmente. En tales casos el par de claves son usualmente enviadas en el dispositivo.

El administrador de red entonces registra el nuevo dispositivo con otras compuertas de seguridad en la *VPN*, dando la clave pública a esas compuertas estos pueden hacer el intercambio de sesión de claves.

Si una compuerta no es enviada con su par de claves, la compuerta debe generar su propio par al azar. Y el certificado digital debería ser firmado con la clave privada y enviarse a la apropiada autoridad certificadora. Cuando el certificado es aprobado, ese certificado está disponible en la autoridad certificadora para ser usada por otras compuertas seguras y clientes remotos para autentificar el sitio después que cualquier dato sea intercambiado, como se puede observar en la figura 11.

Figura 11. Intercambio de claves entre compuertas



2.3.4. Control de acceso

Aunque una *VPN* es construida para proveer comunicación entre servidores y compuertas seguras, es probable que se quiera mantener algún control sobre el acceso que cada usuario de la *VPN* tiene a una red de recursos.

Por ejemplo, si al departamento de ventas no le están permitidos ciertos recursos cuando ellos están en una *LAN*, ellos aún deberían permanecer limitados a esos recursos aunque ingresen vía remota a la *VPN*.

Esto significa que se tendrá que unir el control de las nuevas rutas de acceso proporcionadas por la *VPN* con el control de acceso actualmente programado en sus enrutadores y muros cortafuegos.

El tráfico puede ser manejado en dos diferentes caminos por un muro de fuego, como paquetes sin filtrar o paquetes filtrados. En los paquetes sin filtrar el tráfico de la *VPN* es manejado de la misma manera como en un enrutador; esto es así: los datos protegidos son transferidos directamente a la red interna sin ningún filtro o controles en su contenido.

En los paquetes filtrados el filtro de los muros de fuego y controles Proxy son aplicados al tráfico de la *VPN* antes de que se permita ingresar a la red interna. Filtrar el tráfico de la *VPN* puede ser particularmente útil si las políticas de seguridad son pasar únicamente ciertos tipos de tráfico entre sitios *VPN*. Filtrar puede ser útil para controlar el tráfico intercambiado con socios si la *VPN* se expande a una Extranet.

Si se coloca una compuerta entre el Internet y el enrutador; entonces el enrutador puede ser usado para filtrar ambos tráficos de redes *VPN* y redes normales con las mismas reglas; la compuerta proveerá encripción transparente y servicio de desencripción al sitio entero.

También el enrutador no necesita ser reconfigurado para pasar tráfico del túnel especial, el cual es el caso entre una compuerta instalada atrás del

enrutador. Si este enlace está manejando trafico *VPN* y público, entonces la entrada del *VPN* necesita ser configurada para pasar el tráfico publico.

2.3.5. Protección de clientes contra robos

Porque las computadoras personales son particularmente susceptibles a robos, ellas tienen un especial riesgo ante la seguridad de la *VPN*, esto es porque las claves almacenadas podrían ser usadas para acceder a los recursos corporativos vía la *VPN*.

Hay esencialmente tres técnicas para protección de las claves de un robo.

1. Almacenar las claves en un dispositivo removible como un disco o tarjeta y llevarla separadamente de la computadora portátil.

2. Encriptar las claves con una clave secreta o frase y requerir al cliente verificar la clave antes de que pueda ser usado el protocolo.

3. Encriptar las claves con una clave secreta y dejar que el protocolo presente una falla en el proceso si es usada una clave incorrecta.

De estas opciones, la tercera es la más segura. Pero esto puede ser lo más molesto a un usuario legítimo si él entra en una contraseña equivocada accidentalmente porque él no puede poder discernir la razón de un fallo ocurrido en la comunicación.

3. PROTOCOLOS

3.1. Protocolo *IPSec*

IPSec es un grupo de extensiones de la familia del protocolo *IP*. *IPSec* provee servicios criptográficos de seguridad. Estos servicios permiten la autentificación, integridad, control de acceso, y confidencialidad. *IPSec* es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de *IPSec* para poder usarlo. Se puede usar cualquier protocolo *IP* sobre *IPSec*. Con este protocolo se pueden crear túneles cifrados (importante para las *VPN*), o un cifrado simple entre computadoras. Debido a que se dispone de tantas opciones, *IPSec* es más bien complejo.

De un modo lógico, *IPSec* funciona en cualquiera de estos tres modos:

- Usuario-a-Usuario
- Usuario-a-Red
- Red-a-Red

En cualquier escenario en el que haya una red, el concepto de enrutador está implícito, como en Usuario-a-Enrutador (y este enrutador controla y cifra el tráfico para una Red particular).

Como se puede ver, *IPSec* se puede usar como túnel de tráfico para conexiones de redes privadas virtuales. Sin embargo, su utilidad va más allá de las *VPN*. Con un registro central de Intercambio de Claves de Internet (*IKE*, *Internet Key Exchange*), cada máquina en Internet podría comunicarse con otra y usar cifrado y autenticación fuerte.

El protocolo de Internet, *IP*, también conocido como *IPv4*, no provee por sí mismo de ninguna protección a sus transferencias de datos. Ni siquiera puede garantizar que el remitente sea quien dice ser. *IPSec* intenta remediarlo. Estos servicios vienen tratados como dos servicios distintos, pero IPSec ofrece soporte para ambos de un modo uniforme.

3.1.1. Confidencialidad

Se debe asegurar que sea difícil para todos comprender qué datos se han comunicado, excepto para el receptor. Ya que no se quiere que nadie vea las contraseñas cuando se ingresan en una máquina remota a través de Internet.

3.1.2. Integridad

Se debe garantizar que los datos no puedan ser cambiados en el camino. Si se encuentra en una línea que lleve datos sobre facturación, seguro que se quiere estar seguro de que las cantidades y cifras de contabilidad son las correctas, y que no han podido ser alteradas durante el tránsito.

3.1.3. Autenticidad

Se debe firmar los datos de modo que otros puedan verificar que es realmente uno quien los envió. Es agradable saber que los documentos no son falsos.

3.1.4. Protección a la réplica

Se necesitan modos para asegurar que una transacción sólo se puede llevar a cabo una vez, a menos que se autorice que la repitan. Nadie debería poder grabar una transacción, y luego replicarla al pie de la letra, con el propósito que pareciera como si se hubieran recibido múltiples transacciones del remitente original. Por ejemplo si el atacante conoce cuál es el motivo del tráfico por medios distintos al de poder descifrarlo, y que el tráfico causará sucesos favorables para el, como depositar dinero en su cuenta. Se tiene que asegurar que no puedan replicar ese tráfico más tarde.

IPSec provee confidencialidad, integridad, autenticidad, y protección a la réplica a través de dos protocolos. Estos protocolos se llaman encabezado de autentificación (*AH, Authentication Heade*") y encapsulado de seguridad de la carga (*ESP, Encapsulated Security Payload*) .

AH provee autentificación, integridad, y protección a la réplica, pero no confidencialidad. Su principal diferencia con *ESP* es que *AH* también asegura partes del encabezado *IP* del paquete (como las direcciones de origen o destino).

ESP puede proveer autenticación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue al encabezado en el paquete). La protección a la réplica requiere autenticación e integridad (éstas dos van siempre juntas). La confidencialidad (cifrado) se puede usar con o sin autenticación y / o integridad. Del mismo modo, se puede usar la autenticación y / o la integridad con o sin la confidencialidad.

El encabezado de autentificación (*AH*) viene del encabezado básico *IP* y contiene resúmenes criptográficos ("*Hash*") de los datos e información de identificación. Los resúmenes criptográficos también pueden cubrir las partes invariables del mismo encabezado de *IP*.

El encabezado del encapsulado de seguridad de la carga (*ESP*) permite volver a escribir la carga en modo cifrado. El *ESP* no considera los campos del encabezado *IP* que van delante, y por lo tanto no garantiza nada excepto la carga. Un encabezado *ESP* también puede proveer autenticación para la carga (pero no la cabecera exterior).

Una división ortogonal (en su mayor parte) de funcionalidad de *IPSec*, se aplica dependiendo de sí el extremo que está llevando a cabo la encapsulación *IPSec* es la fuente original de los datos o una pasarela:

- El modo transporte es el que usa un anfitrión que genera los paquetes. En modo transporte, los encabezados de seguridad se añaden antes que los encabezados de la capa de transporte (*TCP, UDP*), antes de que el encabezado *IP* sea añadido al paquete. En otras palabras, un *AH* añadido al paquete cubrirá el resumen criptográfico del encabezado *TCP* y algunos campos del encabezado *IP* extremo-a-extremo, y un

encabezado *ESP* cubrirá el cifrado del encabezado *TCP* y los datos, pero no el encabezado IP extremo-a-extremo.

- El modo túnel se usa cuando el encabezado IP extremo-a-extremo ya ha sido adjuntado al paquete, y uno de los extremos de la conexión segura es solamente una pasarela. En este modo, los encabezados *AH* y *ESP* se usan para cubrir todo el paquete, incluido el encabezado extremo-a-extremo, y se añade un nuevo encabezado IP al paquete que cubre sólo el salto al otro extremo de la conexión segura.

Los enlaces seguros de *IPSec* se definen en términos de asociaciones de seguridad (*SA Security Associations*). Cada *SA* viene definida por un único flujo unidireccional de datos, y por regla general desde un único punto hasta otro. Todo el flujo de tráfico sobre un único *SA* se trata del mismo modo. Algo del tráfico puede estar sujeto a varios *SA*, cada uno de los cuales aplica algún tipo de transformación criptográfica. Un grupo de *SA* se conoce como un Haz ("*SA* Empaquetado").

Un ejemplo de un paquete *AH* en modo túnel es:

encabezado*IP*	***AH***	encabezado2*IP*	encabezado*TCP*	datos

Un ejemplo de un paquete *AH* en modo transporte es:

encabezado*IP*	***AH***	encabezado*TCP*	datos

Debido a que un encabezado *ESP* no puede autenticar el encabezado *IP* exterior, es útil combinar un encabezado *AH* y uno *ESP* para obtener lo siguiente:

encabezado*IP*	***AH***	***ESP***	encabezado*TCP*	datos

A esto se le llama adyacencia de transporte. La versión del túnel sería algo así:

encabezado*IP*	***AH***	***ESP***	encabezado2*IP*	encabezado*TCP*	datos

Como ocurre con la adyacencia de transporte, esto autenticaría todo el paquete excepto unos cuantos encabezados del encabezado *IP*, y también cifraría la carga. Cuando un encabezado *AH* y un *ESP* se aplican juntas directamente como en este caso, el orden de los encabezados debería ser como el que se ha mostrado.

3.1.5. *ISAKMPD*

ISAKMPD, también conocido como intercambio de claves por Internet (*IKE, Internet Key Exchange*) es el mecanismo de intercambio para la *VPN*. *ISAKMPD* gestiona el intercambio de claves criptográficas, para ello hace uso de un proceso en dos fases para establecer parámetros de *IPSec* entre dos nodos de *IPSec*.

Fase 1 - Los dos extremos de conexiones *ISAKMPD* establecen un canal seguro, autenticado. Esto establece una Asociación de Seguridad (*SA*) entre ambos anfitriones. Los métodos usados para

establecer este canal son el modo principal y el modo agresivo. El modo principal envía la variada información sobre autenticación en una cierta secuencia, al tiempo que provee protección para la identidad. El modo agresivo no provee esta protección a la identidad porque toda la información sobre la autenticación se envía al mismo tiempo. El modo agresivo sólo se debería usar en casos en los que preocupe el ancho de banda de la red.

Fase 2 - Las asociaciones de seguridad se negocian en nombre de *IPSec*. La fase 2 establece túneles entre anfitriones *IPSec*. El modo rápido se usa en la fase 2 porque no es necesario repetir una autenticación total debido a que la fase 1 ya ha establecido las *SA*.

Entonces, la fase 1 se usa para obtener un canal seguro en el que llevar a cabo las configuraciones (más rápidas) de la fase 2. Puede haber múltiples configuraciones de la fase 2 en el mismo canal que la fase 1. La fase 2 se usa para configurar los túneles. En la fase 1, sus nodos de *IPSec* establecen una conexión en la que intercambian autenticación.

Esto permite que cada extremo se asegure de que el otro extremo sea autenticado. La fase 2 es un intercambio de claves que determinan cómo se cifran los datos entre los dos.

3.1.5.1. Modo principal

Este modo provee un mecanismo para establecer la primera fase de un *SA ISAKMPD*, el cual es usado para negociar comunicaciones futuras, los pasos son los siguientes

Usar el modo principal para asegurar el inicio de una *SA ISAKMPD* para una comunicación temporal.

Usar el modo rápido con el *SA ISAKMPD* para negociar una *SA* general.

Usar la *SA* del paso anterior para comunicarse desde ahora hasta que se expire la comunicación.

El primer paso, asegurar una *SA* usando el modo principal, se da en intercambios de tres vías entre el iniciador y el receptor. En el primer intercambio los dos acuerdan en algoritmos básicos. En el segundo intercambio, ellos intercambian llaves públicas esto es, números aleatorios que la otra parte debe firmar y retornar para proveer sus identidades. En la tercera parte del intercambio ellos verifican esas identidades y el intercambio es completado.

En todos estos pasos, un encabezado precede el resto del paquete identificando el paso tomado. Cada uno de los pasos es llevado en su propia carga, pero se puede empacar cualquier número de estas cargas en un paquete sencillo.

Las partes usan las llaves compartidas en tres permutaciones, una vez ellos la derivan. Generando primero una llave de derivación (para ser usado en la generación de llaves adicionales en el modo rápido) luego una llave de autentificación y finalmente la llave de encripción para ser usada en la *SA*.

El modo principal protege el intercambio de las identidades de la comunicación de las partes.

3.1.5.2. Modo agresivo

Este provee los mismos servicios que el modo principal, ya que establece el original *SA*. Este modo se ve como el modo principal excepto que este lo completa en dos intercambios en lugar de tres, con únicamente una vuelta, para un total de tres paquetes en lugar de seis.

En el modo agresivo, se genera un par de algoritmos en el inicio del el intercambio y hace un poco más práctico con ese primer paquete proponiendo un *SA*, pasando el valor público, envía un numero aleatorio para que la otra parte lo firme, y envía un identificador del paquete que el receptor puede usar para verificar su identidad con una tercera parte. El receptor envía de regreso todo lo necesario para completar el intercambio; esta respuesta combina todos los tres pasos de respuesta en el modo principal, para que la única cosa que el iniciador tenga que hacer sea confirmar el intercambio.

Desde el modo agresivo no provee protección de identidad para las partes que se comunican, esto es necesario ya que se intercambian información de identificación antes de establecer una Asociación de Seguridad, en la cual se encripta. Así alguien controlando un intercambio agresivo puede identificar quien exactamente formó una nueva *SA*. La ventaja del modo agresivo como siempre es la velocidad.

3.1.5.3. Modo rápido

Después de que las dos partes tienen establecida una asociación de seguridad usando el modo agresivo o principal, ellos pueden usar el modo rápido.

El modo rápido tiene dos propósitos: negociar los servicios de seguridad IPSec y generar un nuevo material de claves.

El modo rápido es considerablemente más simple que los otros modos. Porque esto esta listo dentro de un túnel seguro, esto también puede ofrecer un poco más de flexibilidad.

Los paquetes son encriptados siempre y siempre empiezan con una carga resumida. La carga resumida es compuesta usando una función "*Hash*" a la carga y la autentificación de clave para la *SA*. La carga resumida es usada para autentificar el resto del paquete.

La regeneración de claves puede ser hecha en una o dos vías. Las dos partes pueden intercambiar números aleatorios a través del canal seguro y usar estos para aplicar a las llaves existentes.

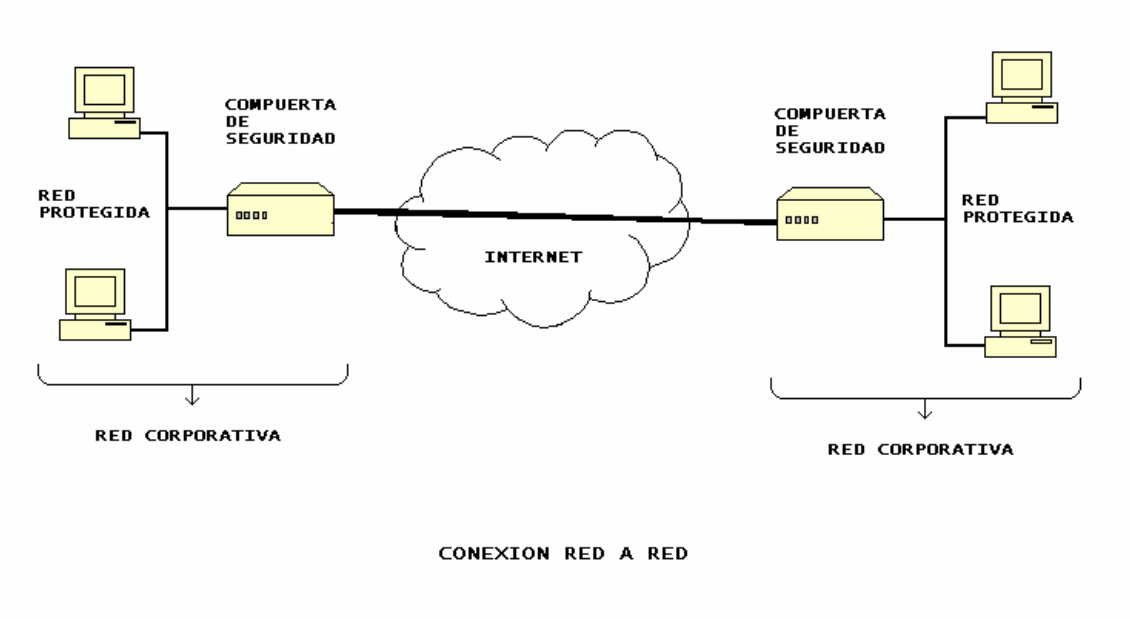
Las principales partes para usar el *IPSec* son las compuertas de seguridad como vemos en la siguiente gráfica esto si es un caso de interconectar dos redes.

Aunque si la principal necesidad es comunicar clientes móviles únicamente se necesita instalar el software de *IPSec* para clientes en las computadoras que se necesite.

3.1.6. Componentes de una *VPN* con protocolo *IPSec*

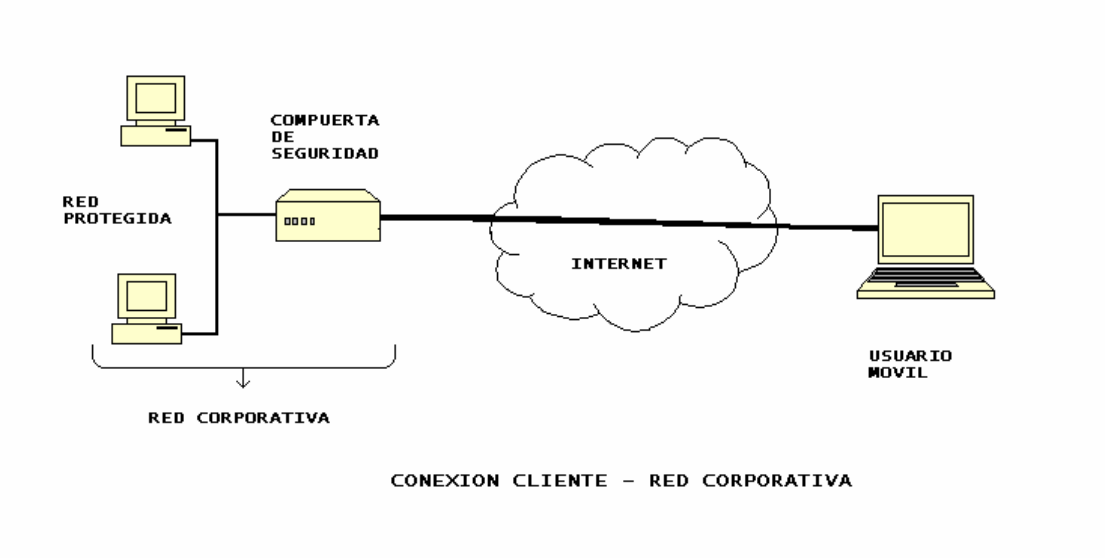
Al usar este tipo de protocolo hay dos escenarios principales uno es el de conexión red a red y el otro es el de cliente a red, como se puede observar en la figura 12 puede observar la conexión red a red

Figura 12. Conexión red a red con *IPSec*



En el escenario de red a red son esenciales las compuertas de seguridad en cada red y serán más que suficientes para este tipo, en la figura 13 se puede observar el tipo de conexión Cliente a Red con este protocolo.

Figura 13. Conexión cliente a red con *IPSec*



En el escenario de cliente a red es necesario además de que la red tenga su compuerta de seguridad que los usuarios móviles tenga instalados el software de cliente *IPSec*, Este escenario también es usado para pequeñas oficinas que se interconectan vía telefónica y debe ser instalado también el software de cliente *IPSec* en las computadoras que sean necesarias.

3.1.7. Puertas de enlace de seguridad

Las puertas de enlace de seguridad o compuertas de seguridad son un dispositivo de red, como un enrutador o cortafuego que separan la red interna, protegiéndola de todo lo externo y realiza la criptografía en nombre de los usuarios autorizados con la red interna.

Usar *IPSec* en una compuerta de seguridad significa que el tráfico de varios servidores es canalizado a través de un solo servidor de encripción antes de que cruce la red desprotegida. Al construir una *VPN*, se instalaría una

compuerta de seguridad a cada una de las oficinas principales y entonces se establecerían las asociaciones de seguridad entre cada compuerta.

Las compuertas establecerán y mantendrán las asociaciones de seguridad individuales entre sí. En otros términos, las compuertas usarán la misma asociación de seguridad para las claves criptográficas relacionadas. Ya que sin esto cada usuario tendría que crear su propia asociación de seguridad para comunicarse con otro. Esto reduce la complejidad de la administración de claves.

Estas compuertas pueden transferir paquetes de *IPSec* usando el modo de transporte o el modo túnel. Seleccionar el modo túnel o modo de transporte para las conexiones entre sus compuertas de seguridad depende de las necesidades que se tenga. Para la seguridad fundamental, el modo túnel se prefiere porque oculta las direcciones de *IP* del emisor y receptor ya que protege contra los ataques. Pero, el modo del túnel requiere de configuración adicional a la compuerta y aumenta el tamaño de los paquetes.

Además, los paquetes en el extremo de un túnel de *IPSec* siempre debe rutarse a la entrada del otro extremo del túnel, ya que no hay ningún mecanismo para remitir un paquete de modo túnel si la entrada de destino se carga excesivamente o choca, pero, si se configura a las compuertas de seguridad para compartir asociaciones de seguridad y claves asociadas entre si, el direccionador de *IP* puede entregar los paquetes a una compuerta auxiliar.

Usando el modo de transporte entre las compuertas reduce el sobrecargar las comunicaciones pero no esconde las direcciones de *IP* de la fuente y destino.

Cuando se revisan las características y capacidades de las compuertas de seguridad, así como los enrutadores, estas son unas cosas que se debe buscar:

- Soporte para las conexiones de la red para textos planos y cifradores de texto.
- La disponibilidad de tamaños de claves debe ser consistente con la sensibilidad de la información que se transmitirá por enlace.
- Si se decide que el algoritmo de encripción predefinido no satisface las necesidades, el dispositivo debe soportar algoritmos alternativos.
- Ambos protocolos *AH* y *ESP* deben ser soportados.
- Debe ser soportada la entrada manual de *SA*, si no se cuenta con *WildCards SA*.
- Deben ser incluidos mecanismos para proteger las claves secretas y privadas.
- Un sistema para el intercambio de claves automática y periódicamente hará la administración de claves más fácil y más segura.
- Una compuerta de seguridad debe incluir un poco de soporte para fallas al registrar cuando se procesa un encabezado; o mejor aun, alguna clase de alarma para fallas persistentes debe ser incluida.

3.1.8. El acceso remoto

Cuando se está como usuario móvil o en una rama de la oficina central que usa conexión por línea telefónica a la *VPN* corporativa, es improbable que se tenga un cortafuego o enrutador instalado en la computadora para servir como una compuerta de seguridad. Las entradas de seguridad se usan proteger *LAN*, no para computadoras individuales. Esto significa que el software *IPSec*

de cliente tiene que ser instalado en la computadora si se va a conectar a una *VPN* protegida por *IPSec*.

Un punto principal al ocuparse del acceso del cliente remoto es cómo distribuir las asociaciones de seguridad requeridas. Algo práctico es tener un sitio central para generar todos los parámetros de *SA* y entonces los enviarlos a los clientes.

Otro problema potencial es ocuparse de las direcciones de *IP* para los clientes remotos. Porque es probable que muchos clientes móviles marquen en el *VPN* vía su *ISP* local, ellos se asignarán a menudo una dirección de *IP* inconstante que sólo es bueno para esa conexión. Así, la *SA* del cliente con el sitio central tiene que poder trabajar con una variedad de direcciones de *IP* algunos de los cuales no podrían conocerse adelantado. Una solución es para el cliente no hacer las asunciones sobre su dirección local y usar una especificación del salvaje-tarjeta de direcciones del sitio centrales.

Las *WildCards SA* o Tarjetas Salvajes de asociaciones de seguridad se usan para simplificar las comunicaciones entre servidores que estén protegidos por las entradas de seguridad. En lugar que se asocie una *SA* con una dirección *IP* de un servidor específico, la tarjeta salvaje *SA* es asociada con todos los servidores de una *LAN* usados con una entrada de seguridad.

3.2. Protocolo *PPTP*

El Protocolo de Túnel Punto a Punto, fue creado por un grupo de compañías llamadas “El Foro *PPTP*”. El grupo consistió de “**3Com**”, “**Ascend Communications**”, “**Microsoft**”, “**ECI Telematics**”, y “**US Robotics**”.

La idea básica del *PPTP* fue dividirse las funciones de acceso remoto de igual manera para que los individuos y las corporaciones pudieran aprovechar la infraestructura del Internet para proporcionar la conectividad segura entre los clientes remotos y las redes privadas. Los usuarios remotos simplemente marcarían el número local de su *ISP* y podrían entrar por un túnel seguro en su red corporativa.

El protocolo mas comúnmente usado para acceso vía discado a el Internet es el Protocolo Punto a Punto *PPP*. *PPTP* construido en la funcionalidad del *PPP* provee acceso vía discado ya que puede hacer un túnel a través del Internet hacia el sitio destino. El *PPTP* encapsula los paquetes *PPP* lo que le da la flexibilidad y manejo de protocolos como *IP*, *IPX* y *NETBEUI*.

Debido a su dependencia del *PPP*, El *PPTP* confía en los mecanismos de autentificación con *PPP*, llamados *PAP* y *CHAP*, de allí que existe una fuerte línea entre *PPTP* y "**Windows NT**", una versión mejorada de *CHAP* la *MS-CHAP* es usada. Esta versión utiliza información con dominios NT para seguridad. Similarmente, el *PPTP* puede usar *PPP* para encriptar información, pero "**Microsoft**" también ha incorporado un método de encripción, *Microsoft Point to Point Encryption* (*MPPE*) para ser usado con *PPTP*.

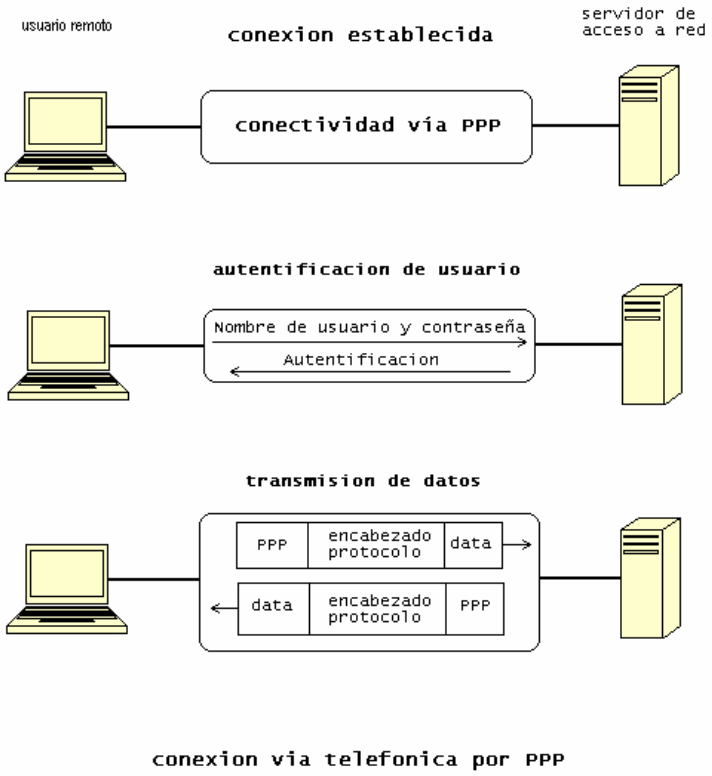
Aparte de la relativa simplicidad del soporte de cliente para *PPTP*, una de las ventajas principales es que esta diseñado para correr en la capa 2 o en la capa de enlace, opuesto a como lo hace *IPSec* en la Capa 3. Soportando comunicación en la capa 2, el protocolo puede transmitir otros protocolos *IP* entre los túneles.

El protocolo *PPP* como es el mas usado para acceso vía discado a Internet y otras redes *TCP/IP*, este incluye métodos para encapsular varios

tipos de datos para transferirlos en los enlaces. Sus especificaciones definen dos protocolos: El protocolo de control de enlance (*LCP Link Control Protocol*) para establecer, configurar y examinar la conexión, y el Protocolo de Control de Red (*NCP Network Control Protocol*) usado para estableces y configurar diferentes protocolos de capa de red.

El *PPP* encapsula paquetes entre cuadros *PPP* y envía los paquetes encapsulados creando enlaces punto a punto entre el emisor y el receptor, como se puede observar en la figura 14, para establecer una comunicación sobre un enlace, cada extremo debe primero enviar paquetes *LCP* para configurar y examinar el enlace de datos.

Figura 14. Conexión vía telefónica con PPP



Cuando el enlace ha sido establecido el usuario es autenticado, esta autentificación puede ser hecha vía el protocolo *PAP* o *CHAP*. En un esfuerzo por acomodar mejor, métodos más robustos de autentificación con *PPP*, la *IETF* ha definido el Protocolo de Autentificación Extensible (*EAP Extensible Authentication Protocol*), este protocolo soporta múltiples mecanismos de autentificación, pospone la autentificación permitiendo al autentificador requiere mas información antes de determinar el mecanismo específico para autentificar.

El protocolo *PPTP* depende del *PPP* para crear la conexión vía discado entre el cliente y el servidor de acceso. *PPTP* espera que el protocolo *PPP* realice las siguientes funciones:

Estableces y terminar la conexión física
Autentificar a los usuarios
Crear los datagramas *PPP*

Después que el protocolo *PPP* ha establecido la conexión, *PPTP* toma el trabajo de encapsular los paquetes *PPP* para transmitirlos en el túnel. Para tomar ventaja del enlace creado por el protocolo *PPP*, el *PPTP* define dos tipos de paquetes: paquetes de control y paquetes de datos, y les asigna dos canales diferentes. Luego este protocolo separa los canales de control y datos encausando un flujo de control que corre en *TCP* y un flujo de datos que corre en *IP*. Una simple conexión *TCP* es creada entre el cliente *PPTP* y el servidor *PPTP*, esta conexión es usada para intercambiar mensajes de control.

Los paquetes de datos contienen los datos del usuario, los paquetes de control son usados para enviar directrices básicas a los dispositivos e información de la configuración entre los extremos del túnel. Los mensajes de control establecen, mantienen y finalizan el túnel *PPTP*.

El canal de control requerido para configurar un túnel conecta el cliente *PPTP* al servidor *PPTP*. La ubicación del cliente determina la naturaleza del túnel y el control que ambos el usuario remoto y el *ISP* tienen sobre el túnel.

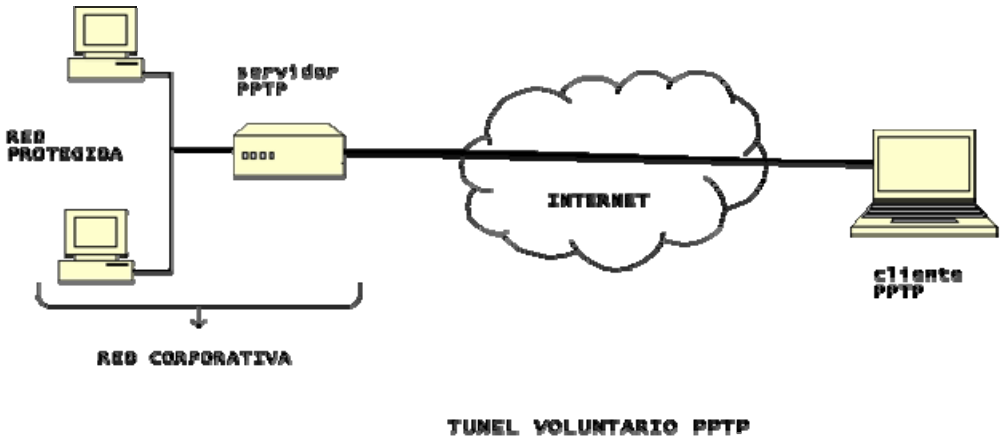
Después que el túnel *PPTP* es establecido, la información del usuario es transmitida entre el cliente y el servidor *PPTP*.

3.2.1. Túneles con protocolo *PPTP*

El protocolo *PPTP* permite al usuario y al *ISP* crear una variedad de distintos tipos de túneles basados en las capacidades del usuario y del soporte del *ISP* para el protocolo *PPTP*. El usuario determine donde esta localizado el punto final del túnel ya sea en la computadora del usuario si tiene el software de cliente *PPTP* o en el servidor de acceso remoto del *ISP* (*RAS Remote Access Server*) si la computadora solo soporta el protocolo *PPP*. En el segundo caso, el servidor de acceso tiene que soportar el protocolo *PPTP*.

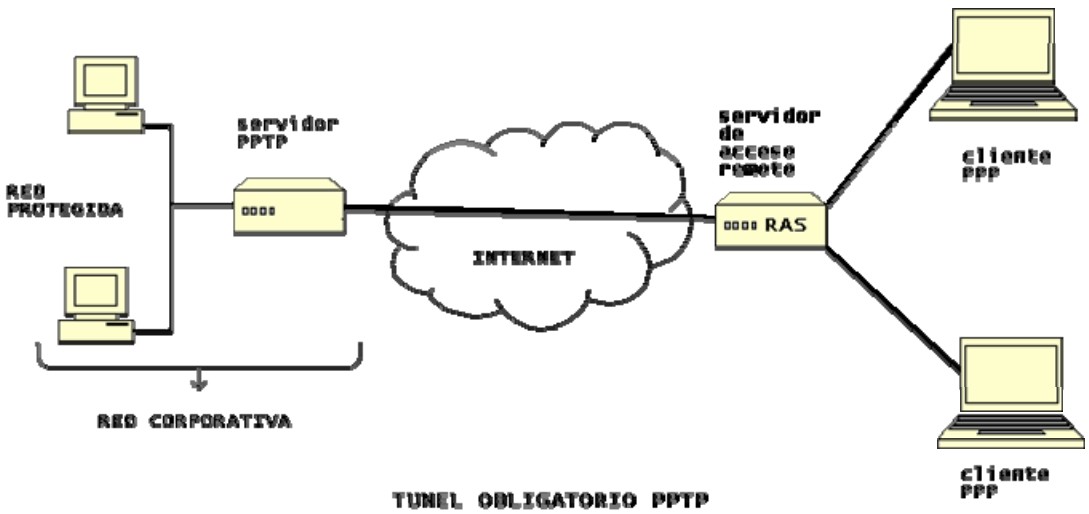
Esto produce una división de túneles en las clases de Voluntario y Obligatorio. Los túneles voluntarios son creados según los requerimientos específicos del usuario (como puede verse en la figura 15).

Figura 15. Túnel voluntario *PPTP*



Los túneles obligatorios son creados automáticamente sin ninguna intervención del usuario, y lo más importante, sin permitirle al usuario cualquier elección, este tipo de túnel puede verse en la figura 16 que se muestra a continuación.

Figura 16. Túnel obligatorio *PPTP*



Cuando se usa un túnel voluntario, el usuario final puede simultáneamente abrir un túnel seguro a través de Internet y acceder a otro servidor de Internet vía los protocolos *TCP/IP* sin túnel. Los túneles voluntarios son frecuentemente usados para proveer privacidad e integridad a la información del tráfico que es enviado sobre Internet.

Como los túneles obligatorios son creados sin el consentimiento del usuario ellos pueden ser transparentes para el usuario. Todo el tráfico originado desde el usuario es enviado en el túnel *PPTP* por medio del *RAS*.

Debido a que los túneles tienen puntos finales predeterminados y el usuario no puede acceder otras partes del Internet, estos túneles ofrecen mejor control acceso que los túneles voluntarios.

Si es parte de la política de seguridad que los empleados no tengan acceso al Internet público, ya que estos túneles podrían mantenerlos fuera del Internet público y a la vez les permitiría usar Internet para acceder a su *VPN*.

Otra ventaja de estos túneles es que múltiples conexiones pueden llevarse a cabo sobre un túnel sencillo. Esta característica reduce el ancho de banda requerido para transmitir múltiples sesiones, una desventaja es que el inicio del enlace se hace fuera del túnel y de esto es que es más vulnerable a los ataques.

Al usar *RADIUS* para proveer los túneles obligatorios se tienen varias ventajas, los túneles pueden ser definidos y auditados en base de los usuarios autentificados, la autentificación y asignación de cuenta puede ser vía telefónica.

3.2.2. Servidores *RADIUS*

El modelo de cliente/ servidor de *RADIUS* usa un servidor de acceso de red (*NAS Network Access Server*) para administrar las conexiones. Aunque el *NAS* funciona como un servidor para proveer acceso a la red, este también funciona como un cliente de *RADIUS*.

El *NAS* es responsable de aceptar las conexiones de usuario requeridas, obteniendo la identificación de usuario y su contraseña, y luego envía la información segura al servidor *RADIUS*.

El servidor *RADIUS* retorna el estado de la autentificación y cualquier dato de configuración requerido por el *NAS* para proveerle servicio al usuario.

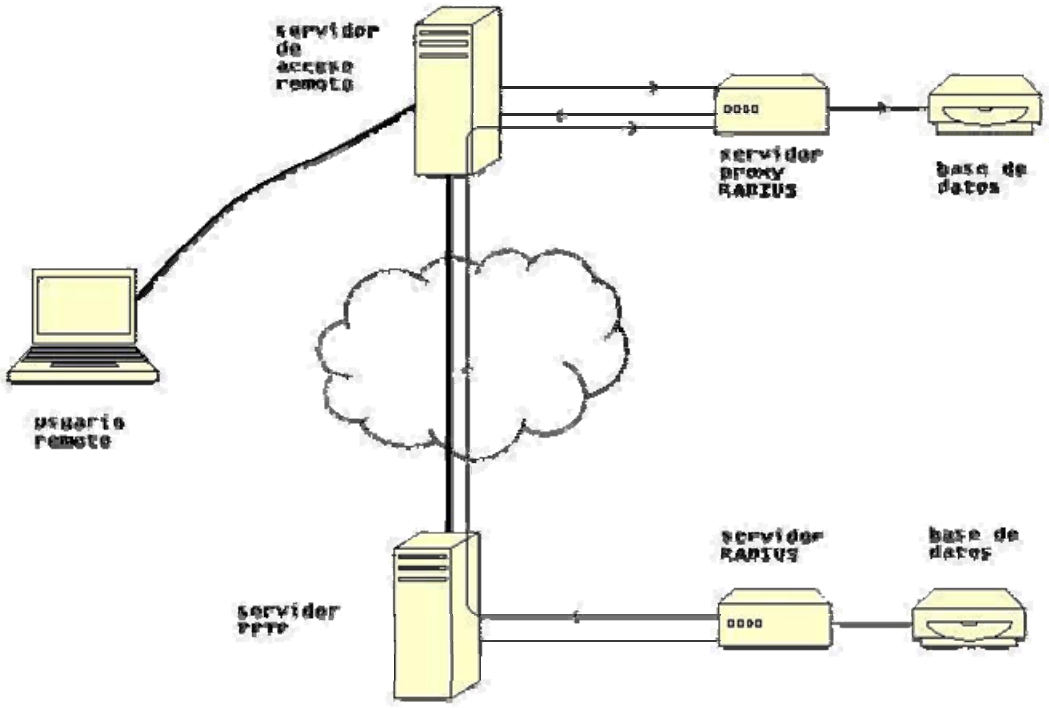
El *RADIUS* crea una sola base de datos centralmente localizada de usuarios y servicios disponibles, una característica importante para las redes que incluyen un gran banco de módems y más de un servidor de comunicaciones remotas. Un usuario remoto tendrá acceso a los mismos servicios desde cualquier servidor de acceso comunicándose con el servidor *RADIUS.*

RADIUS soporta el uso de servidores Proxy, los cuales almacenan la información del usuario para propósitos de autentificación y pueden ser usados para crear cuentas y autorizarlas, pero no pueden permitir el cambio de datos.

Un servidor Proxy depende de actualizaciones periódicas de la base de datos de un servidor *RADIUS* principal (como se puede observar en la figura 17).

Por lo que la corporación debe mantener un servidor *RADIUS* y un conjunto de información del usuario en este, y el *ISP* debe tener un servidor Proxy *RADIUS* que recibe la actualización del servidor corporativo.

Figura 17. Interacción cliente/servidor *RADIUS*



INTERACCIÓN DEL MODELO CLIENTE / SERVIDOR RADIUS

3.2.3. Componentes de una *VPN* con protocolo *PPTP*

Debido a que el mayor punto de interés del *PPTP* es proveer acceso seguro vía telefónica a los recursos privados de la corporación, estos compones de una *VPN* con *PPTP* están organizados un poco diferente a como lo están en una *VPN* con *IPSec*. Los componentes más importantes son los que definen los extremos del túnel ya que sí un punto de estos es el equipo del *ISP*, esto requerirá menos software para los usuarios móviles pero requerirá colaboración entre la corporación y el *ISP* para la autentificación de usuarios.

Por lo general las *VPN* con protocolo *PPTP* requieren 3 partes principales que son: Servidor de Acceso a Red *NAS*, Servidor *PPTP* y un cliente *PPTP*. Aunque el servidor de *PPTP* debe de estar instalado y mantenido por miembros de la corporación, el servidor de acceso a red *NAS* debe ser responsabilidad del *ISP*.

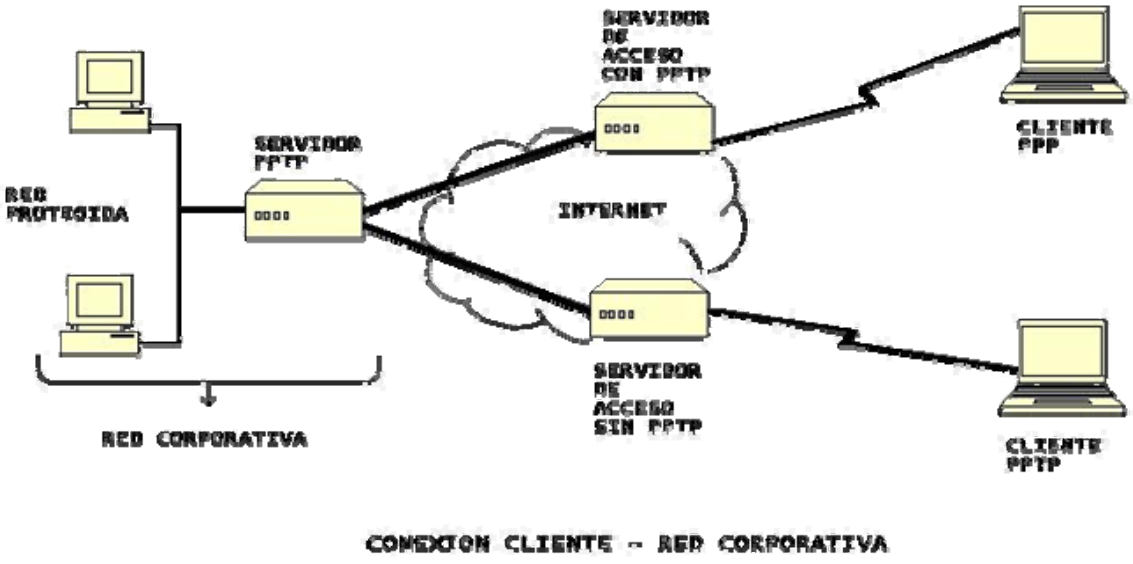
De hecho si elige instalar el software de cliente *PPTP* en los servidores remotos, el *ISP* no necesita proveer ningún soporte específico para *PPTP*.

En estos tipos de redes se cuenta con tres principales escenarios:

En el primero es la conexión cliente a red con servidores de acceso a red *NAS* que tienen soporte *PPTP* en este se necesitan primordialmente un servidor *PPTP* en la red corporativa y el *ISP* debe contar con soporte *PPTP* en su servidor por último el cliente remoto debe tener únicamente instalado un software de cliente *PPP*.

En el segundo es la conexión cliente a red con servidores de acceso sin soporte para el protocolo *PPTP* en este caso se necesita de igual forma un servidor *PPTP* en el lado de la red corporativa y el usuario móvil debe de tener instalado el software de cliente *PPTP*. Como se puede observar en la figura 18 aparecen estos dos escenarios.

Figura 18. Conexiones cliente / red con *PPTP*

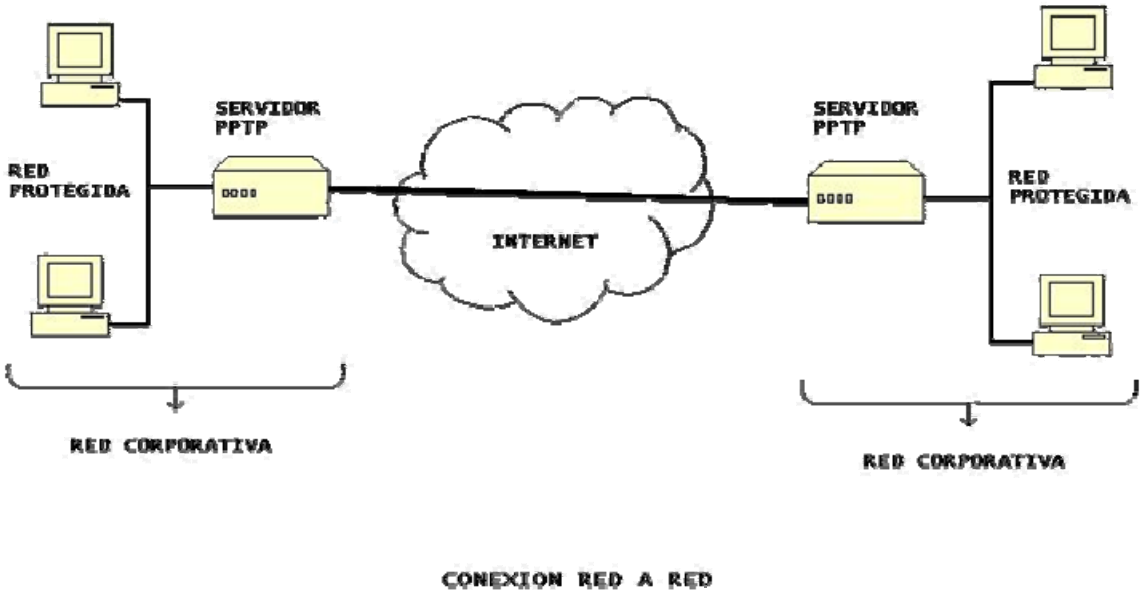


CONEXION CLIENTE – RED CORPORATIVA

En esta gráfica pueden observarse las dos distintas situaciones para una conexión cliente a red.

En el tercer caso se tiene la conexión red a red en esta es únicamente necesario un servidor *PPTP* en cada una de las redes corporativas como se puede observar en la figura 19.

Figura 19. Conexión red a red con *PPTP*



3.3. Protocolo *L2TP*

Un componente de creación importante para las *VPN* de acceso es Protocolo de Túneles para la Capa 2 (*L2TP Layer 2 Protocol Tunneling*), una extensión del protocolo Punto a Punto, fundamental para la creación de *VPN*. *L2TP* combina las mejores funciones de los otros dos protocolos de túnel. El *L2F Layer 2 Forwarding* de "**Cisco Systems**" y el *PPTP Point-to-Point Tunneling* de "**Microsoft**". *L2TP* es un estándar emergente en la *IETF Internet Engineering Task Force*, y que cuenta con el respaldo de "**Cisco Systems**", "**Microsoft**", "**3Com**" y otros líderes en la industria de la conectividad.

3.3.1. Descripción del protocolo *L2TP*

Los componentes principales del protocolo *L2TP* son similares al *PPTP*
Protocolo Punto a Punto *PPP*
Túneles
Sistemas de Autentificación

Usado principalmente para incrementar la seguridad de tráfico.

PPP al trabajar con la capa 2 del modelo OSI, incluye métodos de encapsulado para diversos tipos de datagramas para transferir sobre enlaces seriales. *PPP* encapsula los paquetes entre marcos *PPP* y puede enviarlos creando un enlace punto a punto entre el emisor y el receptor.

L2TP depende en gran parte del *PPP* para crear las conexiones vía telefónica entre el cliente y el servidor de acceso a red *NAS*. *L2TP* deja que el protocolo *PPP* establezca la conexión física, ejecute la primera fase de autentificación, cree los datagramas de *PPP* y cierre la conexión cuando la sesión es finalizada.

Cuando *PPP* ha establecido la conexión el protocolo *L2TP* toma el control. Primero determina si el servidor del sitio corporativo reconoce al usuario móvil y es determinado como un extremo del túnel. Si el túnel puede ser creado, el protocolo *L2TP* encapsula los paquetes *PPP* para transmitirlos en el medio que el *ISP* ha asignado para el túnel.

Como el protocolo *L2TP* crea el túnel entre el Concentrador de Acceso del *ISP* y el servidor del sitio corporativo, este puede asignar más de una sesión en un túnel.

L2TP crea un identificador de llamada para cada sesión en inserta este identificador en el encabezado del *L2TP* de cada paquete para indicar a que sesión pertenece.

El protocolo *L2TP* similarmente al *PPTP* identifica dos tipos de mensajes: mensajes de control y mensajes de datos, los cuales se usan para configurar y mantener los túneles así como la transmisión de datos. Este protocolo transmite ambos mensajes como parte de un mismo flujo.

Los mensajes de control son responsables de establecer, mantener y liberar las sesiones llevadas a través del túnel, así como el control del estado del túnel.

En los mensajes de datos los paquetes de carga son esencialmente los paquetes *PPP*. *L2TP* ayuda a reducir el tráfico de la red y permite a los servidores manejar la congestión implementando controles de flujo entre el servidor de acceso a red *NAS* que sería un Concentrador de Acceso *L2TP* (*LAC, L2TP Access Concentrador*) y el servidor de acceso corporativo sería Servidor de Acceso *L2TP* (*LNS, L2TP Network Acces*s).

3.3.2. Túneles con el protocolo *L2TP*

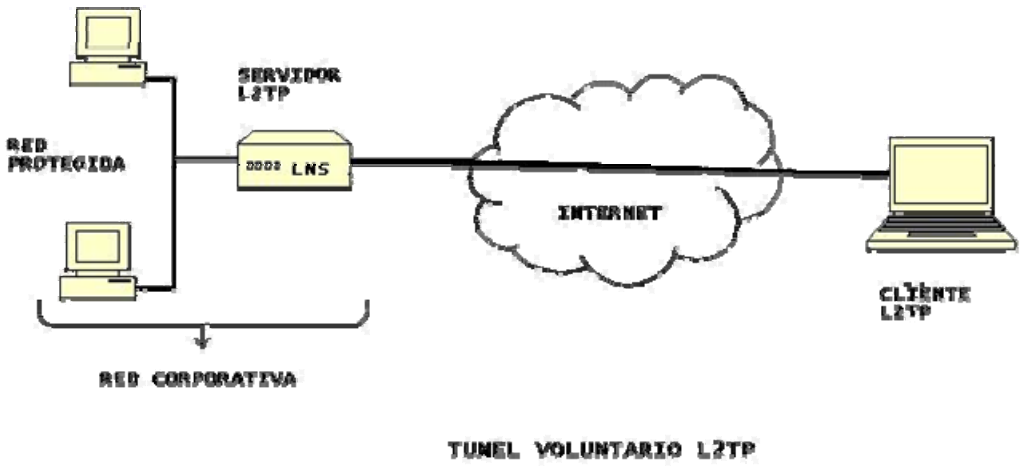
Los túneles con el protocolo *L2TP* son denominados Voluntarios y Obligatorios dependiendo de la iniciación de conexión del usuario, ya sea como cliente *PPP* o cliente *L2TP*.

Los túneles voluntarios son creados por el requerimiento del usuario para un uso específico. Los túneles obligatorios son creados automáticamente sin el requerimiento del usuario y sin permitirle cualquier elección.

Los túneles voluntarios son configurados según los requerimientos del usuario. El usuario puede abrir simultáneamente un túnel seguro a través del Internet y tener acceso a otros servidores de Internet vía los protocolos básico del *TCP/IP* sin túneles.

El extremo del lado del cliente de un túnel voluntario reside en la computadora del usuario. En la gráfica 20 se puede observar este tipo de túnel.

Figura 20. Túnel voluntario con *L2TP*

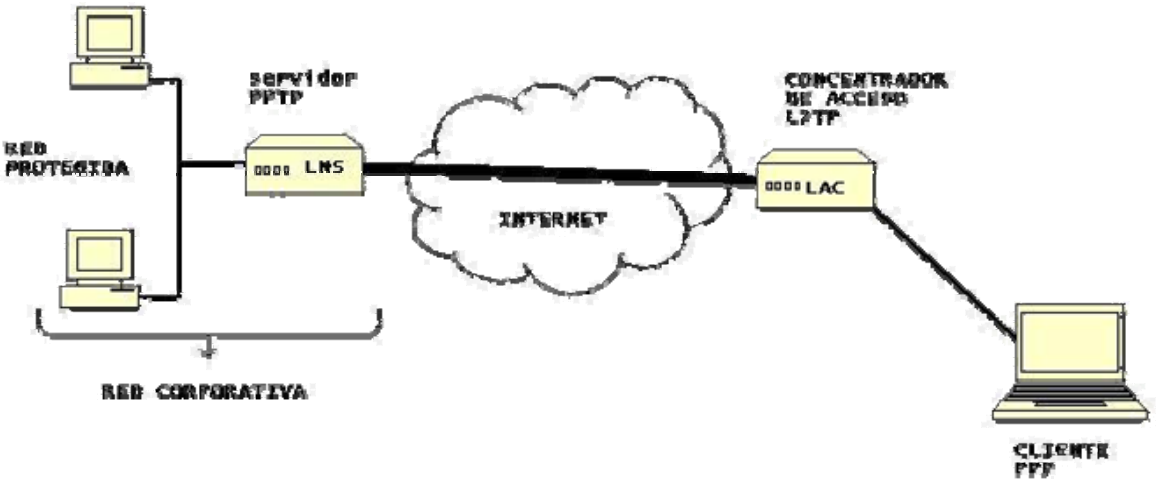


Debido a que los túneles obligatorios son creados sin el consentimiento del usuario, ellos pueden ser transparentes al usuario final. El extremo del lado

del cliente se encuentra en el Concentrador de Acceso *LAC* del *ISP*. Todo el tráfico originado desde la computadora del usuario es enviado a través del túnel *L2TP* por el *LAC*.

El acceso a otros servicios fuera de la Intranet debe ser controlado por los administradores de red. En la gráfica 21 se puede ver este tipo de túnel.

Figura 21. Túnel obligatorio con *L2TP*



Como los túneles obligatorios tienen determinados sus extremos y el usuario no puede acceder a otros partes del Internet, estos túneles ofrecen mejor control que los voluntarios, otra ventaja es que conexiones múltiples pueden ser llevadas a cabo en el mismo túnel. Esta característica reduce el ancho de banda requerida para transmitir múltiples sesiones.

Una desventaja es que el enlace inicial de la conexión es dada fuera del túnel y de allí que es mas vulnerable a los ataques, esta es una de las razones del porque *L2TP* incluye soporte para usar *IPSec* para proteger el tráfico.

3.3.3. Autentificación y encripción

La autentificación de usuarios se da principalmente en dos fases en el protocolo *L2TP*: la primera en el *ISP*, y la segunda se da en el servidor de red del sitio corporativo.

En la primera fase, el *ISP* puede usar el número de teléfono del usuario, o el nombre de usuario determina el tipo de servicio *L2TP* que es requerido y entonces se debe iniciar una conexión vía túnel para el servidor de red apropiado. Cuando el túnel es establecido, el concentrador de acceso *LAC* del *ISP* debe localizar un nuevo identificador de llamada para identifica la conexión con quien el túnel debe de iniciar una sesión para enviar la información de autentificación.

El servidor de red realiza la segunda fase de autentificación decidiendo si acepta o no la llamada, aunque estas fases puede garantizar que el usuario, el ISP y el servidor son quienes dicen ser, nada hasta este punto ha sido hecho para proteger los datos contra observación o alteración.

Los extremos del túnel pueden ser autentificados durante el establecimiento del túnel. Esta autentificación tiene los mismos atributos de seguridad que el protocolo *CHAP* y ofrece una protección razonable contra ataques mientras dura el proceso de establecer el túnel.

Pero aún así es relativamente fácil para un atacante ver la información e introducir paquetes en el túnel después de haber sido completado el túnel.

Solos los protocolos *L2TP* y el *PPP* no reúnen los requisitos de autentificación y encripción de una *VPN*. Aunque la autentificación de *L2TP* pueda manejar mutua autentificación de un *LAC* y un *LNS* durante la configuración del túnel, esto no protege el control y tráfico de datos. Esta falta de protección deja a los túneles abiertos a una variedad de ataques.

Para los túneles *L2TP* sobre *IP*, usando *IPSec* provee una protección más fuerte del túnel. Esta seguridad no requiere modificación al protocolo *L2TP*. Diversos ataques pueden llevarse a cabo en los paquetes del *PPP* enviados en el enlace entre el cliente y el *NAS*, previo a la encapsulación de los paquetes dentro de un túnel de *L2TP*. Esto lleva a la propuesta de usar el protocolo *IPSec* para encriptar los paquetes, por lo menos para los túneles basados en *IP*.

En los túneles obligatorios, el usuario envía paquetes *PPP* al *LAC* y no esta completamente seguro de que el túnel haya sido creado entre el *LAC* y el *LNS*. Una asociación de seguridad puede configurarse entre el *LAC* y el *LNS* basada en los requerimientos del usuario.

Debido a que el usuario no podría estar seguro que los servicios de seguridad están colocados entre el *LAC* y el *LNS* para el tráfico, lo mejor para el usuario es contar con iniciar *IPSec* en la computadora. Pero no todos los extremos pueden estar capacitados para manejar *IPSec*, lo cual puede forzar a renegociar el uso de encripción *PPP* únicamente. En ambos casos el concentrador de acceso *LAC* podría aplicar la autentificación de encabezado de *IPSec* para el tráfico que viaja a través del túnel creado,

En el caso de los túneles voluntarios, el usuario sirve como el extremo del túnel *L2TP* y de allí puede negociar una asociación de seguridad con el *LNS* en el sitio corporativo. Pero, la negociación de las asociaciones de seguridad claves depende en si o no ambos extremos soportan *IPSec*.

Como la computadora del usuario sirve de extremo la autentificación de encabezado del *IPSec* es aplicada a esta estación de trabajo, no en los dispositivos del *ISP*, el cual en este caso es un servidor de acceso a red *NAS*, y no un Concentrador de Acceso *LAC*. Si el receptor no soporta *IPSec*, entonces la encripción *ESP* protege únicamente a los paquetes hasta que encuentren el servidor de la empresa.

3.3.4. Administración de claves

Cuando las dos partes que quieren tener comunicaciones seguras, se necesita estar seguro que se procesará la información en la misma vía. Las dos partes tienen que usar los mismos algoritmos, longitudes de claves y las mismas claves si ellos están seguros que intercambiaran los datos con éxito. Esto es manejado vía una asociación de seguridad.

Aunque las asociaciones de seguridad ayudan a las dos partes a definir la criptografía que usarán para comunicarse, el procedimiento para intercambiar y negociar las Asociaciones de seguridad así como las claves involucradas son definidas por *IKE* (*Internet Key Exchange*) que se diseña para proporcionar cuatro características:

Mantener los medios para que las partes estén de acuerdo en que protocolos, algoritmos, y llaves usar.
Asegurar desde el principio del intercambio que se está hablando con la persona correcta.
Manejar esas llaves después de que han sido acordadas.
Asegurar que de ese intercambio de la llave se manejen seguramente.

Como se podría esperar, el intercambio de llaves se relaciona estrechamente a la administración de las asociaciones de seguridad. Cuando se necesita crear una *SA*, se necesita intercambiar las llaves. Así la estructura de *IKE* los junta y los entrega como un paquete integrado.

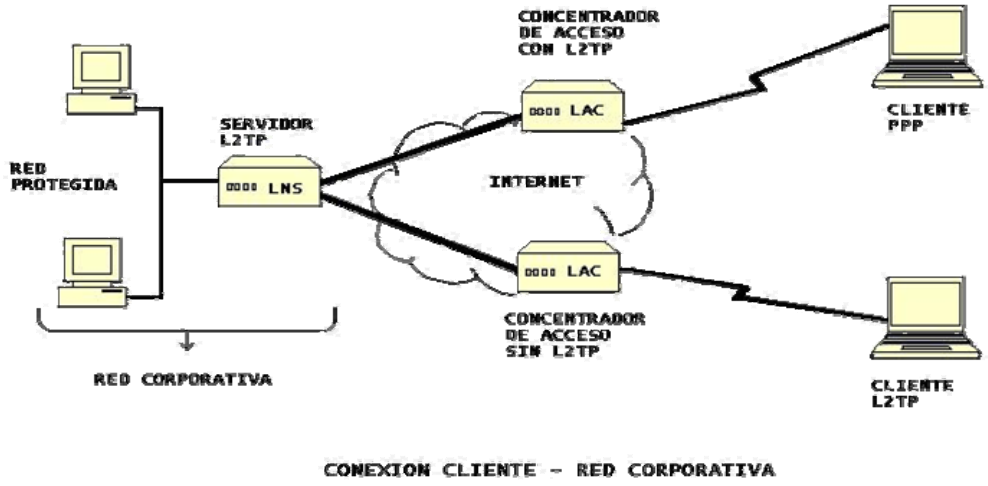
3.3.5. Complementos de una red al usar *L2TP*

Existen dos escenarios posibles en estos tipos de red, uno es la conexión usuario a una red y el otro es el de red a red.

Los componentes más importantes que definen los extremos de un túnel en el primer caso son: el Concentrador de Acceso *LAC* y el Servidor de Red *LNS*. Como uno de estos extremos puede ser el equipo del *ISP*, el software necesario para clientes móviles puede reducirse, lo que requiere un arreglo entre el *ISP* y la corporación.

Si se necesita instalar el software de cliente *L2TP* en las computadoras de los usuarios móviles, el *ISP* no necesita proveer soporte para *L2TP*. En la gráfica 22 se puede ver este tipo de conexión.

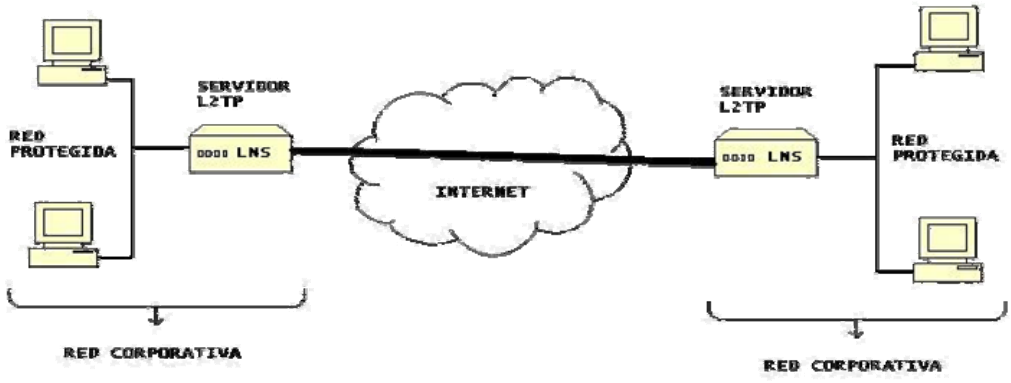
Figura 22. Conexión cliente a red con *L2TP*



CONEXION CLIENTE – RED CORPORATIVA

En el segundo caso únicamente un Servidor de Red *LNS* en cada red para poder intercomunicarse ambas redes, en este caso tampoco es necesario que el *ISP* provea soporte para *L2TP*. En la gráfica 23 presentada a continuación se puede ver esta conexión.

Figura 23. Conexión red a red con *L2TP*



CONEXION RED A RED

3.3.6. Servidores de red *L2TP*

Un servidor de red *L2TP* (*LNS*) tiene dos roles principales: actuar como el extremo de un túnel, y enviar los paquetes hasta la red privada. El servidor envía los paquetes a una computadora de destino procesando el paquete de *L2TP* para obtener el nombre de la computadora de la red privada o información de su dirección en el paquete encapsulado *PPP*. Cualquier plataforma capaz de terminar las sesiones del *PPP* puede operar como un *LNS*.

A diferencia del protocolo *PPTP*, el *L2TP* no está diseñado para filtrar los paquetes, en cambio, la arquitectura del sistema deja que trabaja como un cortafuego.

Cuando viene integrado con el servidor de red con un cortafuego, el protocolo *L2TP* tiene algunas ventajas sobre el *PPTP*.

Primero, *L2TP* no demanda que únicamente un puerto específico puede ser asignado para el cortafuego para pasar el tráfico *L2TP* como lo hace el *PPTP*. Los administradores de red tienen la opción de seleccionar un diferente número de puerto para pasar el tráfico, haciendo más difícil para los atacantes. Segundo, debido a que el tráfico de datos y control pasa sobre un canal sencillo UDP, la configuración del cortafuego es sencilla.

3.3.6.1. Software para clientes *L2TP*

Si el equipo del *ISP* soporta *L2TP*, no es necesario software o dispositivos adicionales en el lado del cliente; únicamente el software *PPP* es necesario. Esta configuración podría no soportar la encripción de datos vía *IPSec*, lo cual significa que se pueda tener que estar en observación con los

clientes *PPP* al hacer la mayoría del proceso *L2TP*. De otra manera, si el *ISP* no soporta el protocolo *L2TP*, entonces un compilador *IPSec* para clientes *L2TP* puede ser usado para crear los túneles del *LNS* corporativo.

3.3.6.2. Concentradores de acceso para red

En muchos casos el diseño de una *VPN* depende del soporte del protocolo ofrecidos por el *ISP*. Este soporte es particularmente importante si los trabajadores móviles pueden usar un cliente *PPP* pero no tienen clientes *L2TP* instalados. Esto también es importante cuando se considera que métodos de encripción usar para proteger los datos.

Debido a que el *ISP* puede ofrecer servicios *L2TP* sin soporte a los servidores de acceso, lo que debe requerir que todos los clientes usen software para clientes *L2TP* en las computadoras. Esto puede ser una ventaja porque les permite a los clientes usar más de un *ISP* si la cobertura geográfica de un *ISP* primario no es la adecuada.

Además con ello los clientes pueden configurar los túneles voluntarios; si se quiere desea controlar el acceso a Internet de los usuarios, entonces se tendrá que recurrir a los túneles obligatorios.

La elección de un *ISP* para una *VPN* con protocolo *L2TP* puede depender del grado que se desea proteger la información. Si se desea encripción de extremo a extremo, se debe instalar un compilador *IPSec* en los usuarios móviles y tener en cuenta que el *ISP* maneja los paquetes encriptados desde los clientes a los servidores de red deseados.

Si menor seguridad se puede tolerar y sólo se quiere proteger los datos cuando viajan a través del túnel por Internet, entonces se debe tratar con un *ISP* que tenga instalado un concentrador de acceso *L2TP* que soporte *IPSec* y encripte el tráfico entre el *LAC* y el *LNS* de la empresa.

4. ISP Y CORTAFUEGOS

4.1. Fundamentos y consideraciones de los *ISP*

Los *ISP* son los proveedores de servicio de Internet (*Internet Service Provider*). Los proveedores de servicio cuyas redes constituyen parte del Internet son clasificados según las capacidades de su red y el tipo de conectividad de Internet que ellos proveen.

Algunos proveedores de servicio tienen hechos sus propios arreglos para intercambio de tráfico esquivando los puntos de acceso a red *NAP* (*Network Access Point*), los cuales pueden ser un cuello de botella. Esos puntos pueden ayudar a llevar alguna carga de los *NA*P. La independencia creada por las redes nacionales también les da a estos proveedores una ventaja adicional cuando ofrecen servicios como *VPN* a sus clientes porque ellos pueden controlar el tráfico que corre en sus redes y la fiabilidad de la red es mejor que si una serie de redes fueran usadas para manejar el tráfico.

Se debe tomar en cuenta que ninguno de los *NAP* proveen conexión a Internet a las industrias, empresas o usuario final, ya que ellos únicamente sirven para ordenar el intercambio de tráfico entre esas organización que mantienen la plataforma nacional.

Un proveedor de grado dos es una compañía que compra su conectividad de Internet de uno de los proveedores Grado Uno y entonces proporciona acceso residencial vía telefónica, o revende el ancho de banda. Estos proveedores regionales típicamente operan plataformas con una región o varias regiones. Ellos también pueden conectarse a los *NAP* pero usualmente con no más de uno.

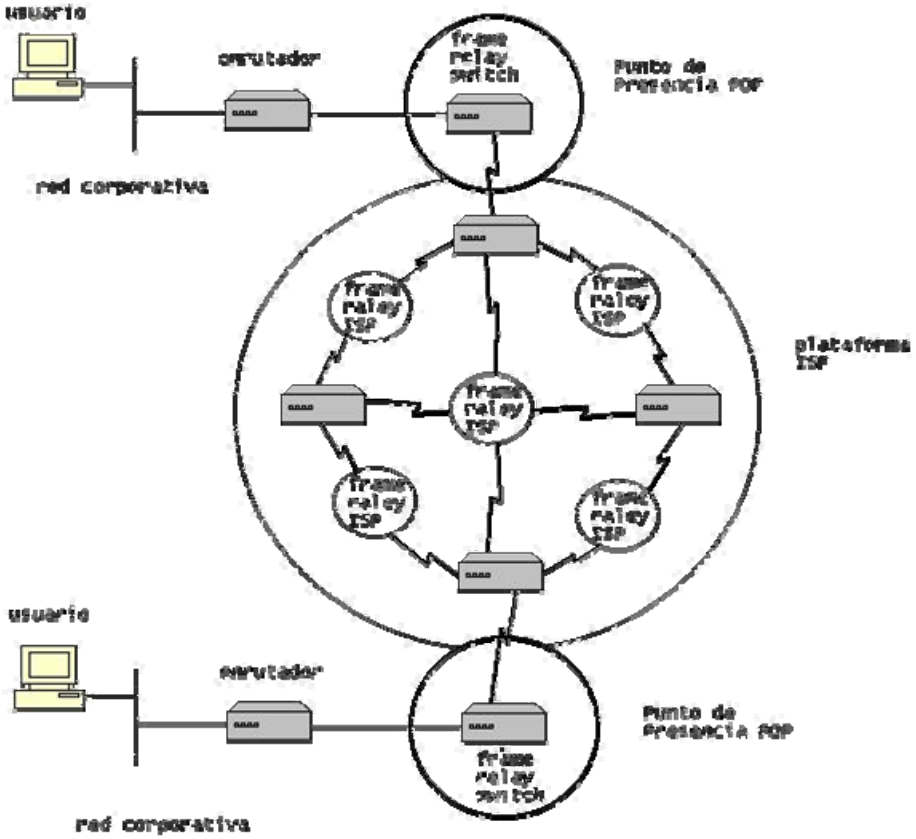
Debajo de los proveedores de grado Dos están los proveedores de servicio de Internet individuales, los cuales pueden ser de dos o tres personas corriendo un punto de presencia *POP* (*Point of Presence*) vía telefónica o más grande soportando miles de usuarios. Estos proveedores generalmente no operan una plataforma regional, si ellos ofrecen servicio nacional, ellos usan *POP* y plataformas de otros operadores mayores con los cuales ellos están asociados.

Para un negocio con un enlace a tiempo completo de Internet o un trabajador individual en su casa o usuario móvil que se conecta vía telefónica a Internet, el *POP* del proveedor de servicio de Internet *ISP*, es un importante engranaje en el uso del Internet. El *POP* está donde el *ISP* maneja los diferentes tipos de medios que el cliente usa para acceder y desde donde el *ISP* envía todo el tráfico del cliente a la plataforma de red, la cual conecta al resto de Internet en un punto. El esquema de la plataforma puede verse en la figura 24.

Algunos Puntos de Presencia *POP* contienen diferentes equipos para cada transmisión de medios que ellos soportan, tales como bancos de módems para accesos vía telefónica, etc.; además para manejar diferentes medios para el tráfico del cliente, El *POP* incluye enrutadores o conmutadores para conectar la red privada del *POP* a el resto de la red del *ISP*. En algunos casos, el *POP*

incluirá servidores de correo, noticias, sitios *Web*, y servidores de autentificación *RADIUS*, etc.

Figura 24. Esquema e la plataforma de los ISP



PLATAFORMA TIPICA DEL ISP

El servicio fundamental de un proveedor de servicio de Internet *ISP* es dar la conectividad a Internet, esta conectividad puede tomar la simple forma de proveer acceso vía telefónica para usuarios individuales con un módem o línea *ISDN*, o puede también ser por líneas dedicadas de E1 o más, conectándose desde la red corporativa a el punto de presencia del *ISP* y de allí al resto de Internet.

El rango de conexiones posibles ofrecidas por un *ISP* es importante para tomar en cuenta en el desarrollo de la *VPN* corporativa, debido a que se pueden tener diferentes requerimientos que difieren de sitio a sitio y de usuario a usuario.

Simplemente tener un *ISP* que provea el acceso a Internet puede ser suficiente para el diseño de una *VPN* si se esta planeando hacer todo internamente. Pero puede ser que un *ISP* provea además servicios de seguridad usando cortafuegos para la protección de los sitios, así como también podría brindar el servicio de instalación completa de la *VPN*.

Otras cosas para tener en mente es el equipo de soporte del *ISP*, ya que los usuarios móviles pueden requerir soporte cuando este tratando de tener acceso a Internet. Debido a que Internet es un grupo de diferentes circuitos administrados por una variedad de corporaciones o entidades académicas, el funcionamiento del tráfico en el Internet varía grandemente.

El tipo de acceso que la corporación requiere, debido a que si se necesitará acceso vía telefónica para los usuarios móviles, se debe de estar seguro que el *ISP* pueda proveer los suficientes puertos para los módems y Puntos de Presencia para los usuarios.

La mayor parte de los *ISP* se especializan en servicios de negocios, venden un rango completo de opciones posibles, con productos que van desde 56Kbps, 64Kbps, 128Kbps, E1, etc. Y también se debe tomar en cuenta que equipos proporcionará el *ISP* para la conexión o cuales debe adquirir la empresa.

Y si se está planeando implementar la *VPN* con soporte interno, o si se quiere algún soporte externo, y si se está planeando una *VPN* usando *IPSec* cualquier *ISP* podría dar el servicio de conectividad a Internet que se requiera.

Pero si se planea usar *PPTP* o *L2TP* hay que hacer una selección de proveedores que puedan dar soporte para estos protocolos.

Además se deben de considerar dos tareas claves de los requerimientos de operación cuando se dividen las responsabilidades entre el proveedor de servicio y la red privada como lo son: la administración y el control de la configuración.

Los requerimientos de administración incluyen tareas como la administración de cuentas, soporte y asistencia para resolución de problemas. Lo más importante es como coordinar el soporte entre el proveedor y la empresa.

Como las empresas y los proveedores de servicio se mueven en una red compartida lo que caracteriza a una *VPN*, esto será importante para crear un soporte efectivo que permita que la información fluya en las dos vías.

Otro factor administrativo es el manejo del acceso, o el manejo de la arquitectura que soportará la arquitectura pública del Internet. Manejar el

acceso tiene un rol principal para determinar ambos donde serán situadas las herramientas de control y como serán resueltos los problemas.

4.2. Enrutadores O *Routers*

En el modelo de Internet, las redes están interconectadas por enrutadores de datagramas *IP* llamados *Routers*. Anteriormente en Internet se referían a estos como *Gateways* o Puertas de Enlace. Un enrutador conecta dos o más interfases lógicas, representadas por subredes *IP* o innumerables líneas punto a punto.

Enviar un datagrama *IP* generalmente necesita la elección de una dirección y la interfase del siguiente enrutador o servidor de destino. Esta elección llamada reenvío depende de una base de datos de rutas que posee el enrutador. La base de datos del enrutador es también llamada tabla de ruteo o de reenvío.

El término *Router* deriva del proceso de construcción de esta base de datos; protocolos de ruteo y configuración interactúan en un proceso llamado ruteo.

La tabla de ruteo debe ser mantenida dinámicamente para reflejar la topología del sistema de Internet que corre.

4.2.1. Tablas de reenvío

Los enrutadores contienen una tabla en la que encuentran la información necesaria para reenviar el datagrama por el camino correcto. Estas tablas guardan información de cómo llegar hasta la red destino, no contienen información para cada anfitrión sino que sólo informan de cómo alcanzar la red donde esta situado el anfitrión.

Esto es debido a que sino las tablas tendrían tamaños demasiado grandes y todo el proceso de reenvío se volvería demasiado lento.

Además, sólo enviando el datagrama hacia el enrutador que se encuentra en la red del anfitrión destino, éste ya se encarga de entregárselo individualmente. Esta información la encuentra gracias a los diferentes registros que tiene la tabla, estos registros son:

- Dirección *IP*.
- Máscara.
- Dirección *IP* del salto siguiente.
- Interfase.

En la dirección *IP* se encuentra la dirección *IP* de la red a la que se quiere llegar. La máscara es la de la red anterior, la dirección *IP* del salto siguiente corresponde con la dirección *IP* del siguiente enrutador de la ruta, y la interfase es el número de la interfase por la que ha de salir el datagrama para encontrar el enrutador.

Por lo tanto la tabla de ruteo sólo especifica un paso a lo largo del camino desde el enrutador a la red de destino, el enrutador no conoce el camino completo hacia el destino.

Es importante entender que cada registro de la tabla de ruteo apunta hacia un enrutador que se puede alcanzar a través de una sola red. Esto significa que todos los enrutadores listados en la tabla de ruteo del enrutador deben residir en las redes con las que éste se conecta de manera directa.

Cuando un datagrama esta listo para dejar el enrutador inicial, el software *IP* localiza la dirección *IP* de destino y extrae la porción de red. Luego, el enrutador utiliza la porción de red para tomar una decisión de ruteo, seleccionando un enrutador que se pueda alcanzar directamente.

4.2.2. Características de un enrutador

Un enrutador debe tener las siguientes características:

- Contener protocolos de Internet específicos como, protocolo de Internet (*IP, Internet Protocol*), Protocolo de Internet de Control de Mensajes (*ICMP, Internet Control Message Protocol*), y otros si es necesario.
- Interfases para dos ó más redes de paquetes. Para cada red conectada al enrutador debe implementar las funciones requeridas por esta red. Esas funciones normalmente incluyen:

  Encapsulado y desencapsulado de datagramas IP con las tramas de las redes conectadas.

Enviar y recibir datagramas con un tamaño máximo permitido por la red, este tamaño es la Unidad de transmisión Máxima de la red (*MTU*, *Network´s Maximum Transmission Unit*).

- Traducir una dirección *IP* destino a una apropiada dirección de red para la red conectada, si es necesario.
- Responder al control de flujo y las indicaciones de errores de la red, si los hay.
- Recibir y enviar datagramas *IP*.
- Reconocer las condiciones de error y generar mensajes de error *ICMP* y de información si es requerido.
- Destruir los datagramas cuyos campos de tiempo de vida hayan llegado a cero.
- Fragmentar los datagramas cuando sea necesario para cumplir con el *MTU* de la siguiente red.
- Escoger el siguiente salto de destino para cada uno de los datagramas, basándose en la información de la tabla de ruteo.

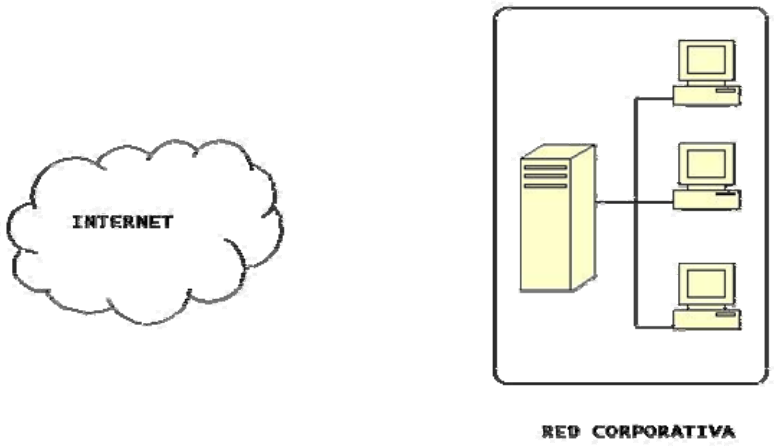
4.3. *Firewalls* o Cortafuegos

Los cortafuegos son sistemas de seguridad para evitar incendios que consisten en establecer una barrera física, no inflamable, separando la zona que se quiere proteger de la zona de donde puede venir el fuego. En informática, un cortafuego o *firewall* es cualquier sistema utilizado para separar una máquina o una red privada de cualquier otra red externa (como Internet) para protegerla de intrusiones externas que puedan suponer una amenaza a la seguridad. La zona protegida se llama "perímetro de seguridad" y la protección

se realiza separándola de una zona externa, no protegida, llamada “zona de riesgo”.

Evidentemente la forma de aislamiento más efectiva para cualquier política de seguridad consiste en el aislamiento físico, es decir, no tener conectada la máquina o la subred a otros equipos o a Internet. Pero de lo que se trata es, precisamente, de proteger datos archivados que tienen que estar disponibles para ser transportados, como se puede observar en la figura 25.

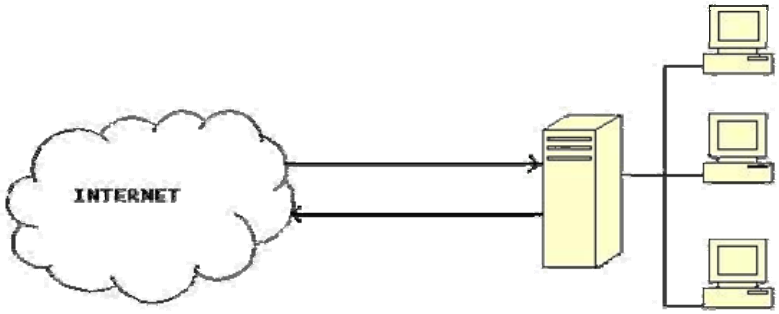
Figura 25. Red aislada físicamente



AISLAMIENTO FISICO DE LA RED AL EXTERIOR

El punto opuesto consistiría en una conectividad completa con la red, lo que desde el punto de vista de la seguridad es muy problemático: cualquiera, desde cualquier parte del mundo, puede potencialmente tener acceso a nuestros recursos, esto puede verse en la figura 26.

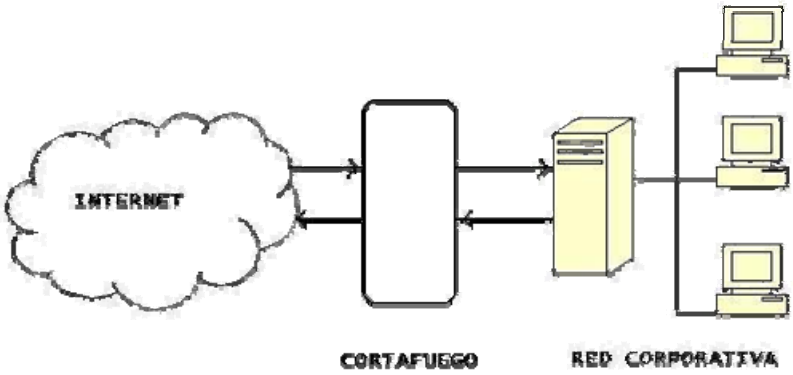
Figura 26. Red conectada completamente al exterior



RED SIN NINGUN AISLAMIENTO FISICO

Un punto medio entre ambas aproximaciones consiste en implementar cierta separación lógica mediante un cortafuego, en la gráfica 27 se puede observar este caso:

Figura 27. Red conectada con aislamiento lógico



RED CON AISLAMIENTO LÓGICO

El cortafuego permite al administrador de la red definir un "*choke point*" o embudo, manteniendo al margen a los usuarios no autorizados (como., atacantes, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al asegurar los servicios de la red, y proporcionar la protección para diversos ataques que puedan llevarse a cabo. El cortafuego puede estar basado en hardware o software o en una combinación de ambos.

El espacio protegido, denominado perímetro de seguridad, suele ser propiedad de la misma organización, y la protección se realiza contra una red externa, no confiable, llamada zona de riesgo.

Para que un cortafuego sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El objetivo principal de un cortafuego es implementar una política de seguridad determinada.

El cortafuego ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos.

La política de seguridad más segura a aplicar es no permitir cualquier acción a no ser que esté permitida expresamente. Esta es la política que debería utilizarse en cualquier caso, puesto que los posibles agujeros de seguridad son más fácilmente identificables con esta política.

4.3.1. Filtrado de paquetes

Es la tarea que realiza un dispositivo (generalmente enrutadores) para controlar de forma selectiva el flujo de datos hacia y desde una red.

Los filtros permiten o bloquean los paquetes, en general mientras se enrutan de una red a otra (normalmente desde Internet a una red privada y viceversa).

El filtrado de paquetes se realiza en base a una serie de reglas que especifican qué tipo de paquetes van a permitirse y qué tipo van a ser rechazados. Normalmente estas reglas se basan en las direcciones de los paquetes y en los puertos o servicios para permitir o rechazar paquetes.

4.3.2. Pasarela traductora de direcciones

Una de las principales ventajas de utilizar un servidor *Proxy* es la capacidad de ocultar la red interna a proteger desde el exterior, debido a que todos los paquetes que atraviesan el *Proxy*, aparecen en el exterior con la dirección de origen del *Proxy*. Sin embargo, ocultar direcciones *IP* internas es una técnica que puede aplicarse sin un servidor *Proxy*, utilizando un *gateway* o pasarela de traducción de direcciones.

Normalmente un servidor *Proxy* es un programa que trabaja con servidores externos en nombre de clientes internos. Los clientes *Proxy* se comunican con los servidores *Proxy*, los cuales, a su vez, transmiten solicitudes aprobadas de clientes a servidores auténticos y luego transmiten de nuevo las respuestas a los clientes.

La pasarela se sitúa entre el interfaz interno y la red exterior. Cuando un paquete con destino a la red exterior y origen una máquina interna llega al interfaz, la pasarela asigna una dirección de su base de datos de direcciones al servidor interno. La pasarela retiene la correspondencia entre direcciones y envía el paquete hacia su destino con la nueva dirección de origen. Cuando llega el paquete de respuesta desde el exterior, la pasarela comprueba la correspondencia de direcciones y re escribe el paquete con su dirección de destino interna correcta antes de introducirlo en la red interna.

4.3.3. Combinaciones de técnicas y tecnologías

El filtrado de paquetes, la utilización de servidores *Proxy* y las pasarelas de traducción de direcciones son, en la actualidad, las técnicas más utilizadas a la hora de diseñar y construir cortafuegos.

Sin embargo, la mejor solución para construir un cortafuego raramente es una sola técnica. Normalmente, se utiliza una combinación de técnicas desarrolladas para solucionar diferentes problemas. Estos problemas a resolver dependen de los servicios que quiera proporcionarse a los usuarios y el nivel de riesgo fijado por las políticas de seguridad.

Algunos protocolos, como por ejemplo *Telnet* y *SNMP*, se pueden manejar con más efectividad con filtrado de paquetes. Otros (como *FTP*, *Archie, Gopher* o *HTTP*) se manejan con más efectividad con servidores *Proxy*.

La mayoría de los cortafuegos emplean una combinación de técnicas para llevar a cabo su labor de la forma más eficiente y segura.

4.3.4. Consideraciones en los cortafuegos

La primera decisión técnica a la que se ve en la hora de instalar un cortafuego es elemental, ya que se debe analizar dónde se situará el cortafuego para que cumpla eficientemente su cometido.

Evidentemente, si se aprovecha como cortafuegos un equipo ya existente en la red, que podría ser un enrutador, no se tienen muchas posibilidades de elección: con toda seguridad se ha de tener que dejar donde ya está; si por el contrario se utiliza una máquina con un cortafuegos implementado en ella, se tienen varias posibilidades para situarla con respecto a la red externa y a la interna. Sin importar donde se sitúe al sistema se debe de recordar siempre que los equipos que queden fuera del cortafuegos, lo que es la zona de riesgo, serán igual de vulnerables que antes de instalar el cortafuego, por lo que este punto debe ser elegido cuidadosamente para proteger al máximo posible toda la red privada.

Una vez que se ha decidido dónde situar el cortafuego se debe elegir qué elemento o elementos físicos utilizar como bastión; para tomar esta decisión existen dos principios básicos: mínima complejidad y máxima seguridad.

Cuanto más simple sea el servidor bastión, cuanto menos servicios ofrezca, más fácil será su mantenimiento y por tanto mayor su seguridad; mantener esta máquina especialmente asegurada es algo vital para que el cortafuegos funcione correctamente, ya que va a soportar por sí sola todos los ataques que se efectúen contra la red al ser elemento más accesible de ésta.

Si la seguridad del servidor bastión se ve comprometida, la amenaza se traslada inmediatamente a todos los equipos dentro del perímetro de seguridad.

Evidentemente, a la vez que se elige un servidor bastión para el cortafuego se debe de decidir qué elemento utilizar como “embudo”; generalmente suele ser un enrutador con capacidad para filtrar paquetes.

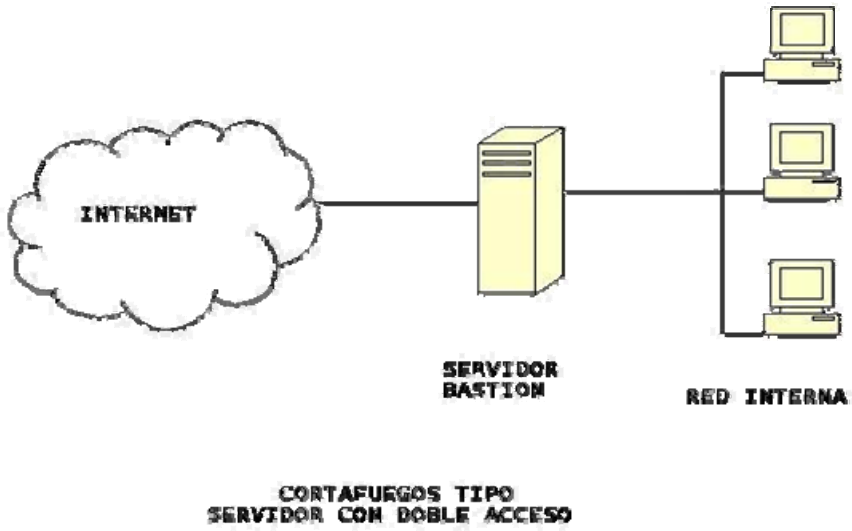
4.3.5. Arquitectura de cortafuegos

A continuación se presentan las distintas arquitecturas básicas con las que se construyen redes protegidas con cortafuegos.

4.3.5.1. Servidor con doble acceso

Esta arquitectura se construye a partir de un ordenador que dispone de al menos dos interfaces de red. El servidor se coloca entre la red interna a proteger y la red externa como muestra la figura 28.

Figura 28. Cortafuegos tipo servidor con doble acceso



El servidor podría actuar como enrutador entre la red interna y la externa, sin embargo se desactiva esta opción. Es decir, los ordenadores de la red interna pueden comunicarse con el servidor igual que los de la red externa, pero no puede establecerse una comunicación directa entre máquinas de la red interna y la externa.

Los anfitriones con doble acceso proporcionan un alto nivel de control. Si no se permite que los paquetes pasen entre redes externas e internas, puede tenerse la seguridad que cualquier paquete en la red interna que tenga como origen una dirección externa es evidencia de algún problema de seguridad.

Un anfitrión con doble acceso sólo puede actuar como servidor *Proxy* o hacer que los usuarios inicien una sesión directa con él para después poder acceder a máquinas en la red externa. De todos modos esta segunda opción es totalmente desaconsejable por el riesgo que supone tener cuentas de usuario en el anfitrión.

4.3.5.2. Servidor de protección

En este tipo de arquitectura la red interna se encuentra separada de la externa por un enrutador. La seguridad la proporciona el filtrado de paquetes que se lleva a cabo en el enrutador, y el anfitrión de protección.

El filtrado de paquetes no es más que la tarea que realiza un dispositivo (generalmente enrutadores) para controlar de forma selectiva el flujo de datos hacia y desde una red. Los filtros permiten o bloquean los paquetes, en general mientras se enrutan de una red a otra (normalmente desde Internet a una rede privada).

El filtrado de paquetes se realiza en base a una serie de reglas que especifican qué tipo de paquetes van a permitirse y qué tipo van a ser rechazados. Normalmente estas reglas se basan en las direcciones de los paquetes y en los puertos o servicios para permitir o rechazar paquetes.

En este caso, el servidor bastión (servidor de correo, *Web*, etc.) también se encuentra en la red el servidor bastión es un sistema informático que debe ser altamente seguro porque es vulnerable a un ataque, por lo general debido a que está expuesto a Internet o cualquier otra red pública y es el punto principal de contacto para usuarios de redes internas.

El servidor contiene la información que se quiere hacer accesible a través de la red pública de datos como por ejemplo sería el caso de un servidor de correo o un servidor *HTTP*.

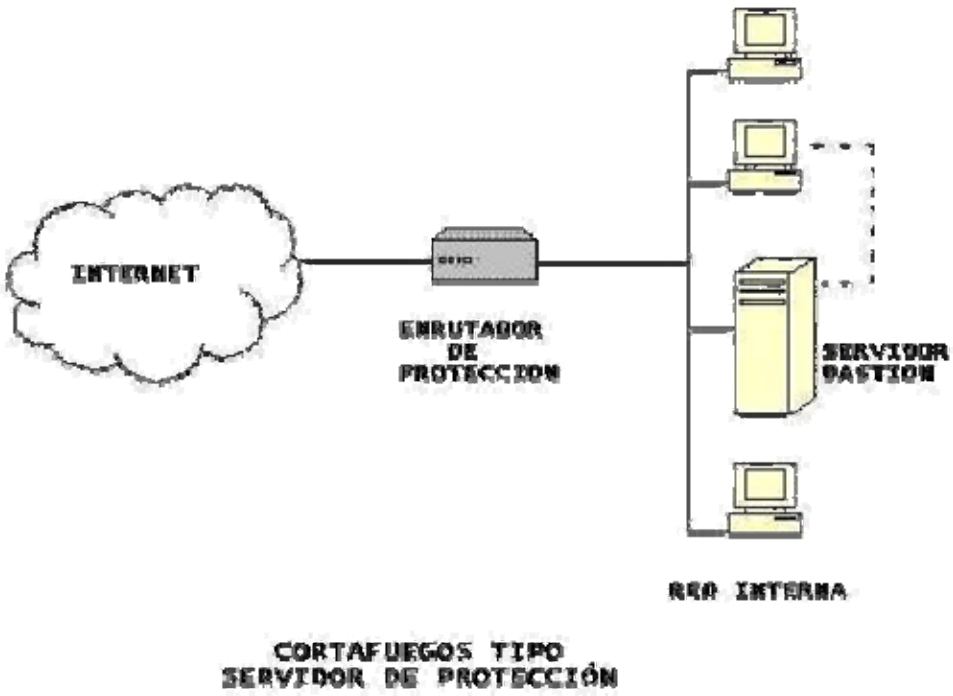
El filtrado de paquetes en el enrutador se configura de tal manera que sólo pueda accederse desde la red exterior al servidor bastión y únicamente determinadas direcciones *IP*. Para permitir la salida de las estaciones de la red interna hacia la red exterior se puede habilitar un servicio de Proxy en el servidor bastión.

En el enrutador de protección el filtrado de paquetes puede configurarse de dos maneras:

Permitir que máquinas internas puedan abrir conexiones con máquinas de la red exterior para ciertos servicios (permitiendo estos servicios a través del filtrado de paquetes).

No permitir conexiones de máquinas internas, obligándoles a utilizar los servicios *Proxy* del servidor bastión (como se muestra en la figura 29).

Figura 29. Cortafuegos tipo servidor de protección



Las líneas discontinuas indican los únicos caminos permitidos desde/hacia el exterior. El servidor bastión actúa como servidor *Proxy*.

Una opción es mezclar estas dos políticas, permitiendo para determinados servicios (normalmente para los que no dispongan de servidor *Proxy*) una conexión directa entre máquinas internas y externas a través del filtrado de paquetes y permitir otros servicios sólo a través del *Proxy*.

A simple vista esta arquitectura parece mucho más peligrosa que la de servidor con doble acceso por el hecho de permitir conexiones directas desde la red externa a la interna. Sin embargo, en la práctica, la arquitectura de anfitrión con doble acceso también es propensa a fallas que permiten que, en realidad,

pasen los paquetes de la red externa a la interna (debido a que la falla es inesperada, es poco probable que existan protecciones contra este tipo de ataques). Además resulta menos complicado defender un enrutador, que proporciona un conjunto muy limitado de servicios, que defender un anfitrión.

Para casi todos los propósitos la arquitectura de servidor de protección proporciona mejor seguridad y mejor uso que la arquitectura de servidor con doble acceso.

Los principales inconvenientes que presenta esta arquitectura de servidor de protección es que si un atacante logra penetrar en el servidor bastión tendrá acceso al resto de máquinas internas. En el enrutador además se presenta un riesgo adicional: si el filtrado no se configura de forma correcta y queda algún punto de entrada, toda la red interna estará a merced de un atacante.

3.3.6.3. Arquitectura de subred de protección

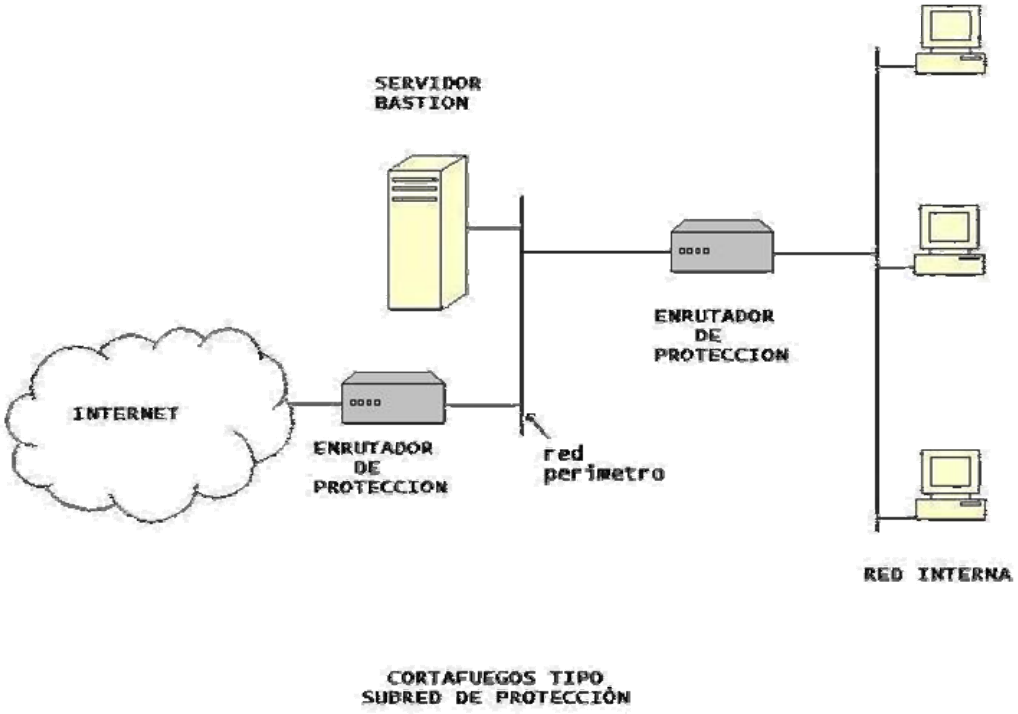
Este tipo de arquitectura proporciona una capa adicional de seguridad a la arquitectura de servidor de protección. Esta capa adicional se consigue añadiendo una red de perímetro o zona desmilitarizada que aísla aún más la red interna a proteger de la externa.

En la red de perímetro deber situarse el servidor bastión puesto que se trata de las máquinas más vulnerables de toda la red y las que cuentan con mayor probabilidad de ser atacadas.

La red perímetro es una red adicional entre una red protegida y una red externa a fin de proporcionar una seguridad adicional. A este tipo de redes

también se las conoce por las siglas *DMZ* (*De-Militarized Zone*, zona desmilitarizada).

Figura 30. Cortafuego tipo subred de protección



De este modo, se protege mejor al servidor bastión y, en consecuencia, a las máquinas de la red interna frente a la arquitectura de servidor de conexión.

La arquitectura de subred de protección clásica se basa en dos enrutadores de protección (con sus correspondientes filtros de paquetes) conectados a la red de perímetro. Uno se encuentra conectado a la red interna y a la de perímetro mientras que el otro se conecta a la red externa y a la de

perímetro. De este modo, un atacante tendría que violar la seguridad de los dos enrutadores antes de poder acceder a la red interna.

En algunas instalaciones puede crearse una serie de capas de redes de perímetro entre la red externa y la interna. Los servicios menos confiables y más vulnerables se colocan en las redes de perímetro exteriores, más lejos de la red interior. De este modo, al atacante que logre acceder a una máquina de perímetro exterior, le costará más trabajo atacar con éxito las máquinas internas debido a las capas adicionales de seguridad entre perímetro exterior y la red interna, siempre y cuando, las capas de filtrado en los enrutadores sean las adecuadas.

Aunque los cortafuegos deberían se consideradas parte de la solución de seguridad corporativa, estos solos no ofrecen lo suficiente para crear una *VPN*. Ya que esto es porque un cortafuego no previene los cambios de los datos que pueden ocurrir en un paquete que cruza el Internet, y ningún cortafuego genérico incluye encripción.

Además aun cuando se haya instalado encripción en todas las computadoras, se necesitará un cortafuego en la organización. Los cortafuegos dan fuerza a las políticas de seguridad de una empresa. El protocolo *IPSec* puede proveer en todas las computadoras privacidad y autentificación pero no puede asegurar que las políticas de seguridad sean reforzadas, como lo serían: que servicios son permitidos, cuando forzar a la búsqueda de virus, etc. Los cortafuegos están disponibles para fortalecer una política que requiera enlaces privados entre redes aún cuando los usuarios no puedan o no usen una conexión encriptada.

5. ANÁLISIS DE COSTOS

5.1. Diseño de una red privada virtual corporativa de cobertura internacional

5.1.1. Consideraciones Iniciales de selección

Primero es adecuado tomar en cuenta las siguientes consideraciones que deberían de cumplir la mayoría de equipos que se usarían para conformar una red privada virtual, para esta red en particular se estimará usar equipos como los son las *VPN* integradas ya que con esto se reducirá la adquisición de equipos y sobrecargados trabajos de configuración de ellos y su propia administración.

A continuación se describe una lista para verificar las características requeridas que se necesitarían en una *VPN* completamente integrada:

- Soporte para multiprotocolos *IPSec, L2TP, y PPTP*.
- Seguridad (*IPSec*) provista también de encripción de paquetes y autenticación para los túneles multiprotocolo.
- Protección de cortafuego integrada.
- Software actualizable para ser usado según con las nuevas normas emergentes para las redes *VPN*.
- Descargas remotas para actualización de software vía la *VPN*.

- Administración local y remota para minimizar costos y tiempos de actualización.
- Capacidad adecuada para manejar anticipadamente los volúmenes de tráfico.
- Interfase de *Ethernet LAN* para acoplarse a la red local.
- Soporte para la opción de conexión más rentable deseada, como T1 / E1, *ISDN*, *xDSL*, X.25, etc.
- Una gama compatible de productos que puedan ser escalables para satisfacer una variedad de tipos de sitios y tamaños.

Otro punto para tomar en cuenta es la administración de la red *VPN*.

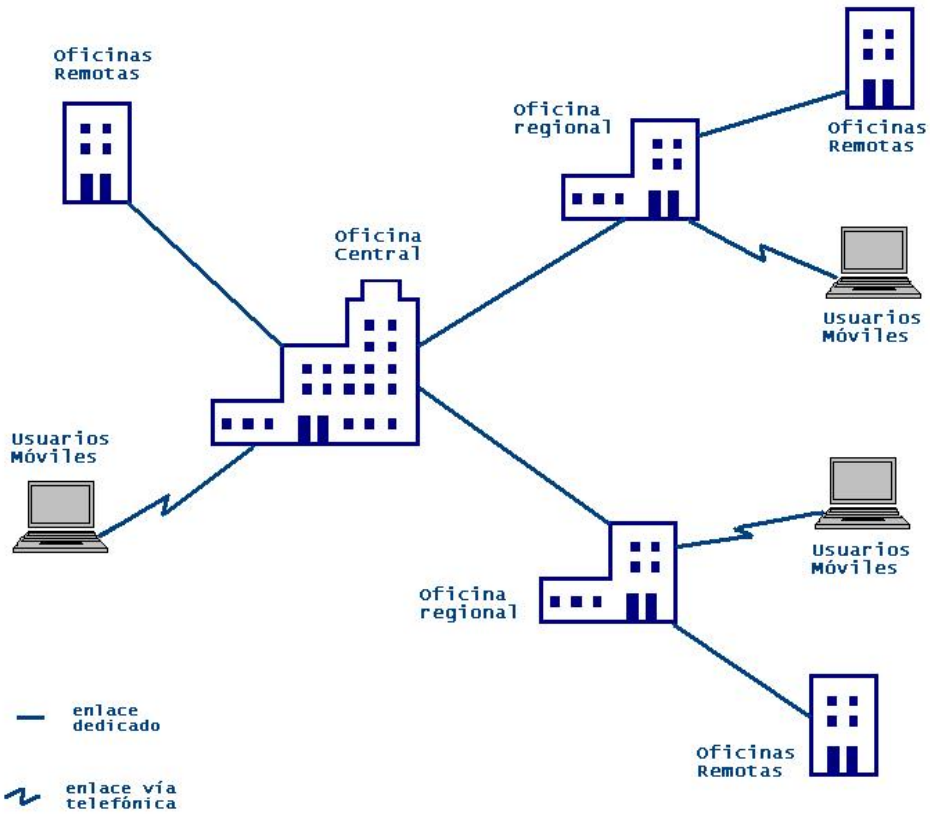
La administración de una *VPN* es normalmente compartida entre el proveedor de servicio *ISP* y la organización o subscriptor. Un sistema de monitoreo y gestión debería ser capaz de manejar la mayoría de las características listadas a continuación:

- Utilización de una interfase de navegador *Web* para un uso fácil que minimice los requerimientos de entrenamiento.
- Medidas de seguridad que incluyan la disponibilidad un conjunto de acceso para leer o escribir en todas las bases de datos y registros de estado de los equipos de red.
- Un mapeo de la topología extremo a extremo de la red de todos los equipos y enlaces.
- Monitoreo de la red en tiempo real de los enlaces físicos y lógico, condiciones de tráfico, con alertas de fallas.
- Una función que rastree el tráfico a través de la red, extremo a extremo para ayudar a aislar los cuellos de botella y otros problemas.

5.1.2. Estructuración de la red privada virtual

Tomando como punto de partida un escenario de una red privada compuesta por una oficina central, dos oficinas regionales, unas doce oficinas remotas divididas de la siguiente forma 6 remotas en la oficina central, 2 en una oficina regional y las 4 restantes en la otra oficina regional, además de un grupo de usuarios móviles, en la figura 31 se ve el esquema de cómo estaría conformada esta red privada.

Figura 31. Esquema de una red privada



Para la red privada virtual se diseñará en base al protocolo *IPSec* con lo cual se reducirá la adquisición de equipo, ya que como se pudo observar con el uso de los protocolos *PPTP* y *L2TP* se necesitará hacer acuerdos con los proveedores que puedan tener soporte para estos protocolos así como un servidor *RADIUS* tanto en la red corporativa como en la red del proveedor, además se considerará usar equipos *VPN* integrados con lo que se minimiza en gran parte la configuración de equipos.

Para este diseño se usaran los equipos *VPN* integrados de *"**SonicWall**"*, estos proveen la primera línea de defensa para las redes, cuentan con certificados *ICSA*, inspección de paquetes con cortafuegos integrados y combinada con el protocolo *IPSec* brinda el acceso remoto a los usuarios, además posee una interfase *Web* para configurar y administrar los equipos.

Para elegir el equipo adecuado, hay ciertas indicaciones que se deben cumplir, como lo son:

- El número de usuarios de red debe acoplar con el número de usuarios con seguridad de Internet
- El número de túneles *VPN* requeridos en cada sitio con los equipos *VPN* integrados usados

La tabla IV mostrada a continuación determina los números de usuarios y números de túneles proporcionados por cada equipo y con ello establecer cual es el adecuado para cada sitio de la red.

Tabla IV. Selección de VPN integradas

Equipo *VPN* Integrado	No. Máx. de Usuarios con Seguridad de Internet	No. Máx. Túneles *VPN*
TELE3	5	5
SOHO3	10/50	10
PRO 100	Ilimitado	50
PRO 230	Ilimitado	500
PRO 300	Ilimitado	1000

fuente : "***SonicWall***".

Para los usuarios remotos ellos contarán con el software para clientes *VPN*, instalada en cada una de sus computadoras.

Cada túnel soporta una conexión de *LAN* a *LAN* entre dos equipos *VPN* integrados con múltiples usuarios en cada *LAN*.

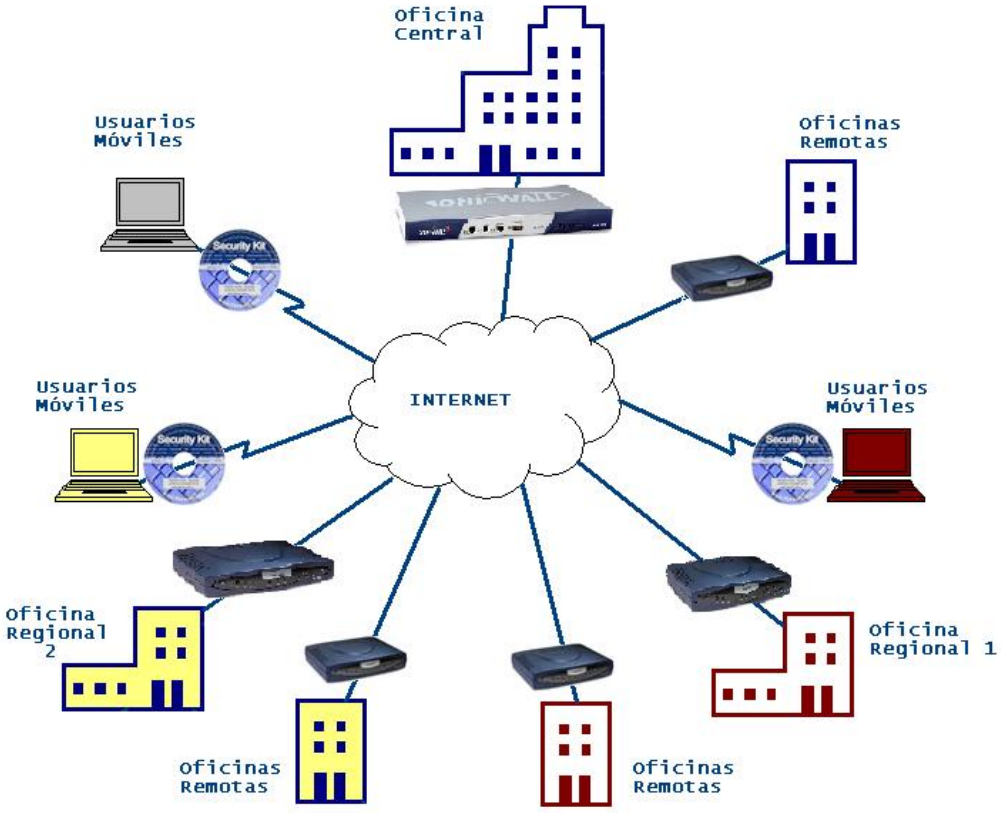
La autentificación usado por estos equipos es con el método de Llaves Públicas *PKI* y certificados digitales integrados en éstos. El servicio de autentificación es hecho en colaboración con "**VeriSign**" (compañía que es de las mayormente usadas para verificar la autentificación de servicios en sitios de Internet).

La administración de la red *VPN* es manejada por su Sistema de Administración Global (*GMS Global Management System*), este sistema de gestión permite a los administradores de red definir uniformemente y reforzar las políticas de seguridad desde una oficina central.

5.1.3. Descripción de los sitios

Acá se detalla la forma en que están compuestos cada uno de los sitios de la red y que equipos serán los adecuados para cada uno de ellos y que puedan integrarse a la red privada virtual, el esquema de la red que sustituiría la red privada es la mostrada en la figura 32.

Figura 32. Esquema de la red privada virtual



5.1.3.1. Oficina central

Si se estima que esté compuesta por alrededor de 100 empleados y se necesita que esté en contacto a tiempo completo con las sucursales y sus 6 oficinas remotas estas conexiones serían consideradas túneles fijos y en cuanto a sus usuarios móviles los cuales podrían ser alrededor de unos 30 usuarios, en estos se ve el tipo de soporte que incluya la *VPN* integrada ya que podría dar acceso por separado a estos usuarios o bien pueden ser tomados como túneles separados según la configuración que ofrezca la *VPN* integrada, para la oficina central se usará una *VPN* integrada del modelo *PRO 230* que cuenta con las siguientes características

Número de usuarios con seguridad de Internet Ilimitado
Procesador "**RISC**" -233 MHz
Memoria RAM de 64 MB
Número de túneles VPN: 500
Puertos para *LAN , DMZ/LAN*, Serial.
Software *IPSec* para *VPN.*
Estándares que maneja : *IPSec, PPTP, IKE, PKI, RADIUS, TCP/IP*,
Certificados usados *ICSA*.

5.1.3.2. Oficina regional 1

Si se estima que esta sea de unos 30 usuarios de red, 2 oficinas remotas y unos 5 usuarios móviles, esta oficina debe estar en contacto con la oficina central y la otra oficina sucursal con estos serán 2 túneles mas los 7 de las oficinas remotas y sus usuarios móviles darán 9 túneles, por lo que para esta oficina se usará el modelo *SOHO3* con la opción de 50 usuarios con seguridad

de Internet ya que este da 10 túneles, este equipo de *VPN* integrado cuenta con las siguientes características:

Número de usuarios con seguridad de Internet Ilimitado
Procesador "**Toshiba**"-133 MHz
Memoria *RAM* de 16 MB
Número de túneles VPN: 10
Puertos 2 *LAN* (10/100 base-T), Serial.
Software *IPSec* para *VPN*.
Estándares que maneja: *IPSec, PPTP, IKE, PKI, RADIUS, TCP/IP,*
Certificados usados *ICSA*.

5.1.3.3. Oficina regional 2

Si se estima que esta sea de unos 60 usuarios de red, que cuente con 4 oficinas remotas y unos 20 usuarios móviles, esta oficina debe estar en contacto con la oficina central y la otra oficina sucursal con estos serán 2 túneles mas los 14 de las oficinas remotas y sus usuarios móviles darán 16 túneles, por lo que para esta oficina se usará el modelo *PRO 100* con el que se tiene capacidad para un número ilimitado de usuarios con seguridad en Internet y cuenta con 50 túneles lo que sería mas que adecuado, este equipo de *VPN* integrado cuenta con las siguientes características:

Número de usuarios con seguridad de Internet Ilimitado
Procesador "**Toshiba**" -133 MHz
Memoria *RAM* de 16 MB
Número de túneles *VPN*: 50
Puertos 2 *LAN* (10/100 base-T), 1 puerto *DMZ*, Serial.
Software *IPSec* para *VPN*.

Estándares que maneja: *IPSec, PPTP, IKE, PKI, RADIUS, TCP/IP*,
Certificados usados *ICSA*.

5.1.3.4. Oficinas remotas

Para estas oficinas se estima que cada una tenga entre 1 y 5 usuarios y como esta oficina principalmente estará conectada con su oficina necesitará un túnel, por lo que se usará un equipo del modelo *TELE3* que está capacitado para 5 usuarios con seguridad en Internet y 5 túneles, las características de este equipo son:

Número de usuarios con seguridad de Internet: 5
Procesador: "**Toshiba**" -133 MHz
Memoria *RAM*: 16 MB
Número de túneles *VPN*: 5
Puertos 2 *LAN* (10/100 base-T), 1 Serial.
Software *IPSec* para *VPN*.
Estándares que maneja: *IPSec, PPTP, IKE, PKI, RADIUS, TCP/IP,*
Certificados usados *ICSA*.
Interfase Web para configuración y puede ser gestionada desde la oficina central.

Para estas oficinas remotas se necesitará en total 12 equipos *TELE3* uno para cada oficina remota.

5.1.3.5. Usuarios móviles

Para los usuarios móviles lo único que es necesario adicional a los módems que ya cuentan con ello, es el software para clientes *VPN* que provee un enlace seguro entre el usuario y la oficina a la que pertenece, este software usa el protocolo *IPSec* las características de él se detallan a continuación:

Número de túneles *VPN*: 1
Software *IPSec* para *VPN*.
Estándares que maneja: *IPSec, PPTP, IKE, PKI, RADIUS, TCP/IP,*
Certificados usados *ICSA*.
Autentificación en Modo Túnel de *ESP*.
Encriptación con opción de 56bits y 128 bits.
Interfase Web para configuración y puede ser gestionada desde la oficina central.

Para estos usuarios móviles se necesitará en total 55 licencias para clientes *VPN*, instalados en cada una de las maquinas de los usuarios móviles.

5.2. Escalabilidad

Para proteger la seguridad y la inversión hecha en una red privada virtual, se debe considerar el crecimiento que tendrá en el futuro la organización, para que la solución de seguridad se capaz de crecer con la organización, de ser capaz de escalar en términos de numero de usuarios o del tamaño de red que soporte.

Cualquier plataforma de seguridad que se escoge debe mantener un camino de actualización que soporte a más usuarios así como la integración de

nuevos servicios de seguridad, como lo serían la protección contra virus y filtrado de los contenidos.

Elegir una plataforma que no sea capaz de escalar se traduce en más gastos para su actualización o desarrollo de múltiples dispositivos donde un dispositivo sencillo debería ser suficiente para ello.

Debido a que las redes virtuales privadas usan los mismos medios de comunicación y las tecnologías involucradas con el Internet, estas redes pueden ofrecer dos puntos de escalabilidad que es difícil lograr por otro medio en las redes corporativas.

Primero está la escalabilidad geográfica. Con una *VPN*, las oficinas, los equipos, y los usuarios móviles pueden volverse parte de una red privada virtual dondequiera que un *ISP* ofrezca un Punto-de-Presencia (*POP*). La mayoría de los proveedores de Internet grandes tiene un número significante de puntos de acceso esparcidos.

Esta escalabilidad también puede ser dinámica; ya que una oficina en el sitio de un cliente puede enlazarse fácilmente al proveedor de Internet local dentro de unos pocos minutos (usando una línea telefónica normal y un módem, por ejemplo) y así de fácilmente removerla de la *VPN* cuando se cierra la oficina.

Claro que los enlaces de ancho de banda más grandes pueden tomar más mucho tiempo para configurarse, pero la tarea es a menudo más fácil que instalar una línea arrendada.

Segundo, hay escalabilidad del ancho de banda. Como los proveedores de Internet pueden ofrecer rápidamente opciones de anchos de banda según las necesidades de los sitios.

Una oficina regional puede requerir un E1 u otra conexión, por ejemplo, mientras sus oficinas remotas podrían poder sobrevivir con una línea telefónica vía módem o una línea de *ISDN* y si una oficina remota requiere más ancho de banda, puede actualizarse de una línea telefónica de 33.6 Kbps a una de 56 Kbps o de *ISDN* a un E1.

La red puede crecer tanto como sea necesario; desde que no se alambrados físicamente los enlaces entre cada sitio, no se tiene que actualizar los equipos en todos los sitios para soportar los cambios en un solo sitio.

5.3. Reducción de equipo

Ofreciendo una sola solución para la red corporativa, tanto para acceso vía línea telefónica, y acceso a Internet, las redes virtuales privadas requieren menos equipo.

En lugar que estar manteniendo bancos de módems separados, adaptadores de terminales, y los servidores de acceso remoto, una red corporativa puede configurarse para un solo medio, como una línea de E1 y el resto de conexiones las maneja el proveedor de Internet.

El equipo a cargo de la red puede reducir la configuración de conexiones *WAN* y su mantenimiento reemplazando el banco de módems y los múltiples circuitos *Frame-Relay* con un solo enlace por medio del Internet que llega al usuario remoto, *LAN* a *LAN*, y tráfico de Internet al mismo tiempo.

A continuación se muestra en la tabla V los equipos que se reducen al usar una red privada virtual en lugar de la red privada.

Tabla V. Comparación de requerimientos de equipo para redes privadas virtuales contra redes privadas

OFICINA CENTRAL	**Red Privada**	**Red Privada Virtual**
Interconexión entre Sitios	Enrutador *WAN* con multipuesto	
Acceso Remoto de *LAN*	Concentrador de Acceso	Con una sola *VPN* integrada es suficiente para dar estas opciones
Acceso a Internet	Enrutador por separado y/o Cortafuego	
OFICINA REGIONAL		
Interconexión	Enrutador *WAN*	
Acceso Remoto de *LAN*	Banco de Módems o Un Concentrador de Acceso pequeño	Con una sola *VPN* integrada es suficiente para dar estas opciones
Acceso a Internet	Enrutador por separado y/o un Cortafuego	
OFICINAS REMOTAS		
Conectadas a tiempo completo	Enrutador *ISDN*	Se usa una *VPN* integrada para pequeñas oficinas
USUARIOS MOVILES		
Acceso a la Red	Módem	Se usa el mismo con el agregado del Software para cliente *VPN*

Como se puede observar con un solo equipo se puede proveer las opciones que dan los otros equipos en una red privada con lo que se reduce en gran parte la cantidad de equipo, haciendo su configuración de red menos compleja.

Y además con esta reducción de equipo también se puede reducir la demanda para los recursos de asistencia técnica. Mucha de esta reducción proviene de la estandarización en un tipo de conexión (*IP*) de los usuarios móviles al Punto de Presencia del proveedor y los requisitos de seguridad estandarizados, ya que con una sola conexión es más sencillo de administrar los recursos y soporte que necesiten los usuarios.

5.4. Expectativas

Cuando se va a integrar cualquier nueva tecnología en una red corporativa, varios puntos toman principal interés, estos puntos son: las normas, la manejabilidad, escalabilidad, integración, fiabilidad y funcionamiento.

A los administradores de la red corporativa les gusta ver que los productos y servicios obedecen las normas actuales, en parte asegurar la vida útil de los productos, pero también, y quizás más primordialmente, para asegurar que los productos de los diferentes vendedores puedan ínter operar entre sí. Aunque muchas compañías todavía escogen ir con un solo vendedor por la gestión de su equipo de redes, mientras se reduce la demanda así la interoperabilidad entre equipos diversos.

Como las redes se van convirtiendo cada vez más complicadas y el número de usuarios va incrementándose, los administradores de red se encuentran en lugares más complejos. No sólo tiene que administrar,

monitorear y configurar más dispositivos de red, si no que usualmente tienen que ejecutar esas tareas con un número de personal fijo o a veces hasta reducido, así, agregando cualquier nuevo componente o servicios a la red tienen que encajar en los sistemas de administración de red existentes o, mejor aun, las tareas de administración existentes tienen que ser simplificadas.

Los administradores de red deben planear su crecimiento y verificarlos con los equipos y servicios de la red. Ya que lo que se busca es no encontrarse en pocos meses el tener que cambiar de equipos si la demanda de servicios se incrementa.

Usar el mismo software, pero en un servidor más rápido es un tema de escalabilidad que los administradores pueden encontrarse ya que esto es mejor que desechar ambos, o también con un vendedor que ofrece una serie de equipos que ofrecen las mismas funciones pero soportan mas usuarios o anchos de banda mas rápidos, a menudo encaja mejor en el plan de un diseñador de red que una compañía que ofrece una sola solución.

Como en estos días, pocos o casi ninguna empresa se dan el lujo de empezar una infraestructura de red desde el principio. Por lo normal hay gran cantidad de datos, sistemas, y redes antiguas que normalmente tienen que ser soportados para que una compañía continúe operando.

Estos sistemas tienen que mezclarse con los nuevos sistemas de alguna forma. Y como se ve con las soluciones *VPN* ofrecen mejores elecciones ya que soportan múltiples protocolos, haciendo un mejor conjunto de integración con redes ya puestas en funcionamiento.

Otro factor de gran importancia para los administradores de red es la confiabilidad de los equipos o servicios. Para las *VPN*, la confiabilidad se enfoca en dos diferentes componentes, El hardware como lo son las *VPN* integradas y los servicios de comunicación como lo es la plataforma de Internet.

Usar componentes estándar es importante así como el mantenimiento de estos equipos, la construcción modular de un dispositivo es una ventaja, como lo es la capacidad para mantener alguna parte en operación continua mientras el dispositivo está en mantenimiento.

En lo relacionado al Internet, es la garantía de su funcionamiento, como todo administrador de red, lo que desea es estar seguro que el trafico de datos camina como lo esperado, con el correcto ancho de banda asignado.

5.5. Estimación de costos de una red privada virtual

En esta sección se evalúa el costo global de lo que se tendría que hacer para poder emigrar de una red privada con enlaces dedicados a una red privada virtual usando el Internet como plataforma principal para la unión de todos los sitios que conforman la red y así como la integración de los usuarios móviles a la misma.

El costo global y el ahorro de costos de operación son presentados en dos fases típicas del proyecto: la inversión inicial de equipo y los gastos de operación, a continuación se detallan estas fases.

5.5.1. Costos de inversión inicial

Para los costos iniciales de la red privada virtual se detallan en la tabla VI, según los equipos determinados en la sección de estructuración de la red privada virtual, para cada sitio y usuario con una solución de *VPN* integrada, que cuenta con cortafuegos, Túneles y autenticación, a través del protocolo *IPSec*, para los usuarios móviles se usa software para clientes *VPN IPSec*, con ello se minimiza en gran parte costos de implementación de más equipos y configuración de los mismos.

Tabla VI. Costos Iniciales para la red privada virtual

Cantidad	Sitio / Usuario	Equipo necesario	Costo Inicial	Totales
1	Oficina Central	*VPN* integrada modelo *PRO 230*	$ 1,660.00	$ 1,660.00
1	Oficina Regional 1	*VPN* integrada modelo *SOHO3-50*	$ 745.00	$ 745.00
1	Oficina Regional 2	*VPN* integrada modelo PRO 100	$ 1,410.00	$ 1,410.00
12	Oficinas Remotas	VPN integrada modelo *TELE3*	$ 500.00	$ 6,000.00
55	Usuarios móviles	Software de Cliente *VPN*	$ 42.00	$ 2,310.00
1	Centro de Gestión	Software para Gestión de la red	$ 4,000.00	$ 4,000.00
69	Túneles	Instalación y Configuración	$ 225.00	$ 15,525.00

fuente: "***SonicWall***"

Como se puede observar en esta tabla VI, la inversión inicial da un costo total de equipos con su centro de gestión por valor de $ 16,125.00, para los costos de instalación y configuración de los túneles necesarios entre sitio a sitio y sitio a usuario móvil se tienen un valor de $ 15,525.00, estos costos son dados por la instalación y configuración de cada uno de los túneles que operaran dentro de la red privada virtual para conectar a los usuarios y oficinas de una forma segura dentro de la red de Internet, estos costos de inversión ascienden a un total de $ 31,650.00.

Usando una tasa de Q8.00 X $1.00 la inversión inicial en moneda local sería de alrededor de Q 253,200.00.

5.5.2. Costos de operación de una red privada virtual

En esta parte se describen los costos de operación que se dan en la red privada virtual, como lo son los costos por acceso de servicio de Internet para los distintos sitios que componen la red y para cada uno de los usuarios móviles, así como el servicio de telefonía que se requiere en los usuarios móviles, con ello se puede tener una idea clara de lo que se estará gastando mensualmente al operar este tipo de red, en la tabla VII se detallan los costos.

Tabla VII Costos de operación de la red privada virtual

Cantidad	Sitio / Usuario	Tipo de Conexión	Costo mensual de Servicio de Internet	Costo Servicio de Telefonía	Totales Mensuales
1	Oficina Central	1 E1	$ 900.00		$ 900.00
1	Oficina Regional 1	128 Kbps	$ 150.00		$ 150.00
1	Oficina Regional 2	256 Kbps	$ 190.00		$ 190.00
12	Oficinas Remotas	128 Kbps	$ 150.00		$ 1800.00
55	Usuarios Móviles	56 Kbps vía telefónica	$ 20.00	$ 34.10 ($1.55 por hora diaria X 1 X 22)	$ 2,975.50

Como se puede observar en la tabla VII, esto produce un total de costos de operación por un monto mensual de $ 6,015.50 para dar un total anual de $ 72,186.00, en moneda local esto seria alrededor de Q 577,488.00.

En estos costos solo se ha incluido el cargo de servició de telefonía a los usuarios móviles por las llamadas locales que harán a los proveedores de servicio donde se encuentren en ese momento y se estima que usen alrededor de una hora diarias al estar de viaje, además de que siempre se les incluye un costo de servicio de Internet para mantener sus cuentas activas con el proveedor de Internet local, que administrará las cuentas de Internet.

Ahora con los otros sitios estos no necesitan de costos de telefonía ya que tendrán servicio fijo de Internet, (esto es solo para permanecer las redes interconectadas, acá no se toman en cuenta los gastos de telefonía que usan normalmente para estar en contacto con sus clientes y proveedores).

5.5.3. Costos de operación de la red privada

En esta parte se detallan los costos de operación mensuales de una red privada que ofrece las mismas conexiones que la red privada virtual, estos valores son dados por enlace dedicado para cada uno de los sitios que conforman la red, y también son incluidos los costos de los usuarios móviles como lo son los servicios de telefonía de larga distancia.

Estos costos servirán de medida para su comparación y análisis para establecer si es económicamente factible llegar a cambiar la forma de comunicarse en las redes corporativas, en la tabla VIII se muestran los costos de operación de la red privada.

Tabla VIII. Costos de operación de una red privada

Cantidad	Sitio / Usuario	Tipo de Conexión	Costo mensual de Servicio de Enlace dedicado	Costo Servicio de Telefonía	Totales Mensuales
1	Oficina Central	1 E1	$ 1500.00		$ 1,500.00
1	Oficina Regional 1	128 Kbps	$ 300.00		$ 300.00
1	Oficina Regional 2	256 Kbps	$ 500.00		$ 500.00
12	Oficinas Remotas	128 Kbps	$ 300.00		$ 3,600.00
55	Usuarios Móviles	56 Kbps vía telefónica	$ 20.00	$ 132.00 ($6 por hora diaria X 1 X 22)	$ 8,360.00

Estos costos de operación dan un gasto mensual de $ 14,260.00, lo que produce un costo anual por un monto de $ 177,120.00, tanto para los enlaces dedicados usados para estar interconectados los sitios corporativos como también se incluyen los costos de larga distancia de los usuarios móviles para poder interconectarse a sus oficinas, estimando que los usuarios móviles usen en promedio una hora diaria por 22 días en el periodo de un mes.

Usando la misa tasa de Q8.00 X $1.00 estos costos de operación anuales alcanzarían un monto de Q 1,416,960.00.

5.6. Análisis comparativo de costos y recuperación de la inversión

Acá se hace el análisis económico el cual servirá para evaluar la factibilidad de si es o no adecuado cambiar la tecnología de red privada a una red privada virtual, en base a los datos obtenidos en las secciones anteriores para realizar este análisis se tomarán en cuenta tres aspectos principales como lo son: El período de retorno de la inversión, el porcentaje de retorno de inversión en el primer año de operación, así como también el porcentaje de ahorro mensual de costos de operación, a continuación se presenta una tabla IX conteniendo el resumen de los costos de operación de la red privada y la red privada virtual.

Tabla IX. Resumen comparativo sobre los costos de operación

Sitios	Red Privada Costos Mensuales	Red Privada Virtual Costos Mensuales
Oficina Central	$ 1,500.00	$ 900.00
Oficina Regional 1	$ 300.00	$ 150.00
Oficina Regional 2	$ 500.00	$ 190.00
Oficinas Remotas	$ 3,600.00	$ 1,800.00
Usuarios Móviles	$ 8,360.00	$ 2,975.50
Totales Mensuales	$ 14,260.00	$ 6,015.50

Como puede observarse en este resumen los costos de operación mensual de las redes privadas ascienden a $ 14,260.00, mientras que los

costos de operación para las redes privadas virtuales ascienden a solamente $ 6,015.50 como se ve existe un fuerte decremento en los costos de operación al usar las redes privadas virtuales, esta disminución de costos mensuales haciende a $ 8,244.50 que en moneda local sería Q 65,956.00 lo cual es una suma atractiva para la reducción de costos.

5.6.1. Período de retorno de la inversión

Este análisis sirve para saber en cuanto tiempo puede llegar o no a recuperarse el costo de inversión hecha para hacer el cambio de la red privada a una red privada virtual, para poder realizarlo se usa la siguiente fórmula:

$$PRI = CIRPV / (COMRP\text{-}COMRPV)$$

fuente : “TimeStep Corp”.

Donde,

PRI = Periodo de retorno de inversión dado en meses
CIRPV = Costo de Inversión de la red privada virtual
COMRP = Costo de operación mensual de la red privada
COMRPV = Costo de operación mensual de la red privada Virtual

Esto da un valor de

PRI = $ 31650.00 / ($ 14,260.00 - $ 6,015.50)
PRI = 3.84 meses

Como se puede observar en un período aproximado de 4 meses se habrá recuperado la inversión efectuada con la nueva red privada virtual, esto es en base a los ahorros presentados mensualmente con esta nueva red.

5.6.2. Porcentaje del retorno de la inversión en el primer año

Esta herramienta dará un panorama de que porcentaje se obtiene en la recuperación del capital invertido en este cambio de la forma de manejar las comunicaciones corporativas, en el primer año de operación, para establecer este porcentaje se usa la siguiente fórmula:

$$ROI = \{ [12*(AMCO)– CIRPV] / CIRPV \} 100\%$$

fuente : "**TimeStep Corp**".

Donde,

PRI = Porcentaje de Retorno de la Inversión
CIRPV = Costos de Inversión de la Red Privada Virtual
AMCO = Ahorro Mensual de Costos de Operación, este cálculo viene de:
AMCO = *CORP – CORPV*

Y de donde estos son,

CORP = Costos de Operación Mensual de la Red Privada
CORPV = Costos de Operación Mensual de la Red Privada Virtual

De los datos obtenidos anteriormente estas fórmulas dan los siguientes resultados:

AMCO = $ 14,260.00 - $ 6,6015.50

AMCO = $ 8,244.50

Y el porcentaje de retorno queda de la siguiente forma:

PRI = { [12*(8,244.5) - $ 31,650.00] / $ 31,650.00 }

PRI = 208%

Como se observa en el primer año de operación se tiene un alto porcentaje de recuperación que alcanza los 208%.

5.6.3. Porcentaje de ahorro mensual en gastos de operación

Esta parte servirá para determinar en que porcentaje se tienen reducción de costos de operación con lo que se tendrá un panorama de que tan rentable es hacer el cambio a una red privada virtual. Para poder determinar este porcentaje se usa la siguiente fórmula:

PAGO = [(*CORP-CORPV*) / *CORP*]* 100%

fuente : “**TimeStep Corp**”.

Donde,

PAGO = Porcentaje de Ahorro de Gastos de Operación

CORPV = Costos de Operación de Red Privada Virtual

CORP = Costos de Operación de la Red Privada

De los datos obtenidos se tiene lo siguiente:

PAGO = [($ 14,260.00 - $ 6,015.5) / $ 14,260.00] * 100%
PAGO = 57%

Con lo que se puede observar un alto índice de disminución en los costos de operación mensual, haciendo justificable para los administradores de red el cambio del manejo de las redes privadas a redes privadas virtuales, ya que estos tendrían la posibilidad de reducir en mas de la mitad sus costos de operación.

CONCLUSIONES

1. Los servicios de las redes privadas virtuales permiten que los usuarios o las organizaciones se conecten de manera confiable a redes remotas sobre redes públicas y privadas, al mismo tiempo que ofrecen una comunicación segura y esta conexión se muestra ante el usuario como una comunicación de red privada sobre una red pública.

2. Una red privada virtual puede llegar a reducir los costos de operación de una red privada tradicional en un 50%, al usar los servicios de las redes públicas como parte de su interconexión entre sitios pertenecientes a la organización, con ello, le da a las corporaciones un tiempo corto para la recuperación de la inversión realizada con este cambio del manejo de sus redes.

3. Las redes privadas virtuales pueden tender a ser una herramienta principal que les provea a las organizaciones multinacionales o las que desean crecer a nuevos territorios, una nueva vía de comunicaciones seguras, ya que estas corporaciones se encuentran cada día en un medio en el cual, uno de los puntos principales es la reducción de costos.

4. Estas redes dan una mejor opción al elegir la escalabilidad ya que fácilmente se pueden ir ampliando su cobertura de red sin tener que perjudicar a toda la red al configurar un nuevo sitio que se enlace a la red privada virtual.

5. El usar la tecnología de túneles por medio del protocolo *IPSec* hace a estas redes menos complejas, siendo su configuración más simple y con ello, se logra también, reducir la adquisición de equipos extras como es el caso de usar el protocolo *PPTP* en el cual se hace uso de un servidor extra, para ser manejado como servidor *RADIUS*.

6. La tecnología de las redes privadas virtuales se ha diseñado para estar con la tendencia actual de negocios hacia operaciones comerciales que abarquen mayores territorios, donde los trabajadores deben conectarse a recursos centrales y comunicarse entre sí, para contar con una información actualizada y poseer un alto grado de respuesta al tomar decisiones locales.

RECOMENDACIONES

1. Para tener un máximo de ahorro de costos y que estas redes sean menos complejas en su configuración una buena forma de lograrlo es con la selección de equipos *VPN* integrados.

2. Al elegir usar *VPN* integradas se debe tomar en cuenta que provea un sistema de cortafuegos, soporte para los distintos protocolos, y diversos métodos de autentificación y encripción, con lo que podrá integrarse a distintos proveedores y no se dependerá de única solución.

3. Uno de los protocolos que cuentan con la mayor fuente de herramientas de seguridad es el *IPSec* por lo que al momento de elegir el tipo de protocolo para una red privada virtual, este es una buena elección, ya que minimiza adquisición de equipos y se necesita menos soporte por parte del proveedor de servicio de Internet.

4. Si se está planeando una *VPN* con *IPSec* cualquier *ISP* podría dar el servicio de conectividad a Internet que se requiera. Pero si se planea usar *PPTP* o *L2TP* hay que hacer una selección de proveedores que puedan dar soporte para estos protocolos.

BIBLIOGRAFÍA

1. Brown Steven, **"Implementing Virtual Private Networks"**
Primera Edición, Editorial McGraw-Hill, mayo 1999

2. Clark, David Leon **"It Manager's Guide to Virtual Private Networks"**
Primera Edición, Editorial McGraw-Hill, agosto 1999

3. Jentjens K, Karl-Heinz, **"Redes privadas virtuales''** PCMagazine, USA 88-102, mayo 2000

4. Kosiur, Dave, **"Building and Managing Virtual Private Networks"**
Primera Edición, Editorial Wiley Computer Publishing, 1998

5. McDysan, David E. "**VPN Applications Guide: Real Solutions for Enterprise Networks"**
Primera Edición, Editorial John Wiley & Sons, mayo 2000

6. Murhammer, Martín **"A Guide to Virtual Private Networks"**
Primera Edición, Editorial Prentice Hall, febrero 1999

7. Shinder, Thomas W. **"Building a VPN Windows 2000" ,**
Editorial Syngress Publishing, Mayo 2001.