UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

MONOGRAFÍA

"SEGURIDAD EN REDES VIRTUALES PRIVADAS (VPNs)"

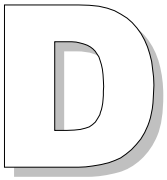
QUE PARA OBTENER EL TÍTULO DE
LIC. EN SISTEMAS COMPUTACIONALES

PRESENTA:
ALEJANDRA RUGERIO JUÁREZ

ASESOR:
M. C. C. GONZÁLO A. TORRES SAMPERIO

PACHUCA DE SOTO, HGO., ABRIL 2006

Dedicatoria



A Dios, quien me ha permitido llegar a este momento tan crucial en mi vida, y con quien siempre he contado en todo momento, y sobre todo por permitir seguir aquí para disfrutar de cada detalle de la vida que me ha elegido, y que deseo siga guiando mi camino.

A mis padres, quienes me han dado amor, apoyo incondicional sobre mis locas decisiones, y que sin ellos no podría estar en donde estoy. Gracias, los amo!

A mis hermanas y hermanito, que me han apoyado en todo momento, a pesar de las rabietas que les he hecho pasar a cada uno durante el trayecto de este trabajo. Los quiero mucho!!

A mi Sami, Yessi, Janiha y mi lindo niño **Saúl**, quienes me aguantaron mi mal humor durante el trayecto de este trabajo. Los quiero mucho y son unos angelitos muy especiales para mí cada uno de ustedes.

A mis profesores, que sin escatimar esfuerzo alguno han sacrificado parte de su vida para formarme, educarme y así, llegar a ser una persona de provecho. Y más aún, quienes fueron mi ejemplo a seguir: Lic. Isaías Pérez, Ing. Edgar Olguín, Lic. Theira Samperio, Lic. Norma Rodríguez, Dra. Luz Muñoz.

A mis amigos: Susi, Yadis, Dennis, Daniel, quienes me han apoyado en los momentos cruciales de mi vida, y haber reído y llorado conmigo para lograr una superación personal. Y que con su cariño mutuo, su guía, sabiduría y apoyo incondicional, han formado parte de mi vida, haciendo más interesante esta aventura, hasta llegar a la meta que creí inalcanzable. Gracias a cada uno de ustedes!! Y… ya no se pongan celosos!! ☺ Cada uno es muy especial para mi!!

A mi asesor M.C.C. Gonzalo A. Torres, que a pesar de ser tan importante, ya que es muy solicitado. Tenia tiempo para mi! Y claro, darle muchos dolores de cabeza, para darle forma a este trabajo. Por fin, tiene pies y cabeza!! Gracias master!!

Atte. **Alexxa R. J.**

Índice general

IG

LISTADO DE FIGURAS.

Capítulo 1.

Capitulo 2.

Capitulo 3.

LISTADO DE TABLAS.

Capitulo 1.

Capitulo 3.

Marco Teórico

I

Introducción al campo de estudio.

La tecnología existente en Internet como las intranets, han llegado a ser una parte esencial de los sistemas de información corporativos de hoy en día. Sin embargo, Internet no fue diseñada, originalmente para el ámbito de negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios.

Es un tema peligroso para los negocios el establecer y mantener la confianza en un entorno que fue diseñado desde el comienzo para permitir un acceso libre a la información es decir, de conseguir seguridad en una Intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperabilidad y facilidad de uso.

La respuesta a estos puntos se centra en la instalación de Redes Virtuales Privadas, mejor conocidas como VPN (*Virtual Private Network*). Con su empleo, se manejan conceptos como encapsulamiento, encriptación y el empleo de túneles, con la finalidad de mantener la información de una manera más segura, confiable y por supuesto con la confianza de que la información llegara a su destino sin problemas y manteniéndola alejada de situaciones ó personas no deseadas dentro de la corporación que puedan beneficiarse.

Objetivo general.

Efectuar una investigación minuciosa sobre la tecnología de Redes Virtuales Privadas aplicadas a la seguridad en una red de datos, para generar un documento que muestre las principales características de la encriptación, encapsulamiento y protocolos de túnel.

Objetivos específicos.

- Dar a conocer los estándares y protocolos de una red de computadoras.
- Mostrar la seguridad en las redes actuales y su relación con los *firewalls*.
- Describir el funcionamiento de una Red Virtual Privada (VPN).
- Mostrar los requerimientos necesarios para instalar una VPN.
- Proporcionar elementos conceptuales para la implementación de una VPN en una Institución.

Justificación.

Internet es una red de datos mundial por el cual transita a diario información vital para muchas organizaciones, como información privada para bancos, la realización de transacciones, compras en línea, etc. Las redes de computadoras hace posible compartir este tipo de información en un tiempo récord. Es importante mantener una seguridad interna como de manera externa para con la red. Se cuenta con diversos tipos de seguridad para proteger la información, es tan fácil que alguien entre a una Intranet y la sabotee, por ello la tecnología ha creado una red más segura y económica para conectar intranets dentro de Internet, naciendo la Red Virtual Privada (VPN).

La tecnología de la VPN crea túneles. Un túnel asegura la confidencialidad llegando de manera segura a su destino. Un túnel primero debe crearse,

mantenerse y finalmente cerrarse, con ello se logra que tanto su emisor como receptor estén seguros de que se esta enviando la información correcta sin alteraciones en su camino. El túnel emplea el manejo de llaves por ambos lados de la comunicación, se encapsula la información, y se envía por la red intermedia (Internet), cuando llega a su destino se desencapsula y es enviado a su red destino. Un proceso de un túnel completo consiste en: la encapsulación, transmisión y desencapsulación de la información en una conexión fácil y económica.

Para agregar más seguridad se emplean varios métodos mas antes de enviar la información a través del túnel como llaves privadas y publicas, la encriptación, funciones *hash*, y manejo de protocolos como L2TP, PPTP, PPP e IPSec entre los más conocidos.

Alcance.

El alcance en este trabajo es, proporcionar información sobre la seguridad que existe en las Redes Virtuales Privadas, ya que emplea Internet para enviar su información a través de túneles para cada sesión de trabajo.

Delimitación.

Se delimita el estudio a la Seguridad en las Redes de Datos, tomándose como base para conocer como la Seguridad que tienen las VPN, influye en las organizaciones que desean expandir su mercado en el mundo a través de Internet.

Capítulo

1

Introducción a las redes de computadoras.

La tecnología de las redes actuales ha evolucionado hacia Redes Virtuales Privadas (VPNs). La tecnología que emplea esta red es conocido, emplea el modelo OSI, estándares conocidos, con protocolos de punto a punto, topologías, todo o parte de redes existentes o por crear en la empresa. Esta red envía su información a otro punto creando túneles, que se encargan de la Autenticación, encriptación, claves o llaves, para verificar a quien o hacia quien va dirigida la información y sobre todo de quien la envía es una persona confiable y segura. Antes de conocer más a las VPNs, es importante saber como están creadas las redes actuales para conocer como funcionan y sobre todo saber de donde parte una VPN.

1. Introducción a las redes de computadoras.

Una red de computadoras es un conjunto de computadoras, equipos de comunicaciones y otros dispositivos que se pueden comunicar entre sí, a través de un medio en particular. Una red debe ser [3], [14], [URL1] confiable, confidencial e integra. En el manejo de la información [1], [10] es confiable, consistente, capaz de identificarse entre sí y existe una forma estándar de nombrar e identificar las partes de la red.

El objetivo de toda red es el compartir recursos, como discos, impresoras, trazadores, otros más dispositivos y existen además otras razones [URL1] como la disponibilidad del software de red, el trabajo en común, la actualización del software, una copia de seguridad de los datos, el control de los datos, el correo electrónico y difusión de mensajes, Ampliación del uso con terminales tontas y sobre todo la Seguridad en la misma (Figura 1.1).

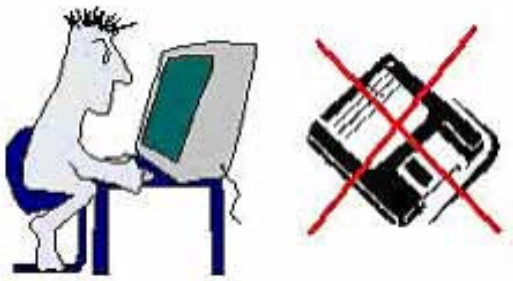


Figura 1.1 Seguridad y no copias de archivos.

El Sistema Operativo de una red se define como el programa más importante que se carga en la computadora al arrancar, y se encarga de administrar los dispositivos conectados. Sirve para que el usuario se entienda de alguna manera con la computadora [5,12]. Da acceso a las funciones más importantes del sistema a los programas que operan por encima del Sistema Operativo. Los Sistemas Operativos más conocidos son: MsDos, Windows 3.1., Windows 95, OS/2, UNIX, *Novell Netware, Lantastic*, Windows NT, Windows 2000 (sucesor de Windows NT 4.0) y la familia de los sistemas UNIX.

Entre las opciones de un Sistema Operativo de red, destacan que debe ser un sistema tolerante a fallos, debe tener una optimización de acceso a disco, un buen sistema de control de transacciones y seguro, permitir la compartición de recursos y derechos sobre estos [URL3]. Los Sistemas Operativos de Red se dividen en dos grupos [5]: en Sistemas que utilizan el Modelo Cliente - Servidor y en Sistemas que utilizan el Modelo Punto a Punto.

Para conectar redes con redes o para la creación de una red local es necesario considerar con que dispositivos se contaran en ella. En LANs tendremos a los repetidores, puentes (*Bridges*), ruteadores (*Router*), compuertas o pasarelas

(*Gateways*), y Conmutadores de Datos (*Data Switch*). En una WAN, se tendrán concentradores, módems, multiplexores y satélites. Se define cada dispositivo de conexión a continuación:

1.1 Topología de Redes.

Una Topología de red es la forma en la que se distribuyen los cables de la red, para conectarse con el servidor y con cada una de las estaciones de trabajo, así como su sitio físico [URL1]. Al instalar una red hay que tomar en cuenta las necesidades que requiere la organización para poder definir que topología conviene más. Las topologías puras son tres [1], [2], [3]: topología en bus, en estrella y en anillo. A partir de estas tres se generan otras como son: anillo - estrella, bus - estrella, etc.

La **topología en bus** consiste en un cable al que se conectan todos los nodos de la red. Esta topología resulta fácil de instalar y mantener, solo que cuando el bus se abre toda la red cae [4] junto con el sistema (Figura 1.2).

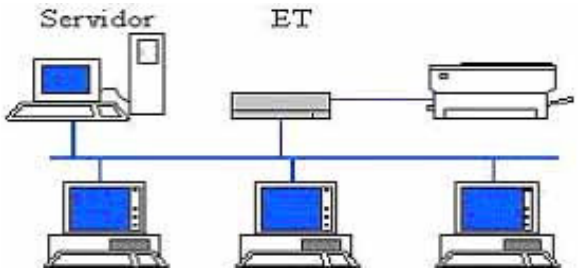


Figura 1.2 Topología de bus

La **topología en Anillo**, consiste en un cable en el que se juntan el origen con el extremo, formando un anillo cerrado [4]. A él se conectan los nodos de la red (Figura 1.3). Tiene el mismo problema que la topología en bus.

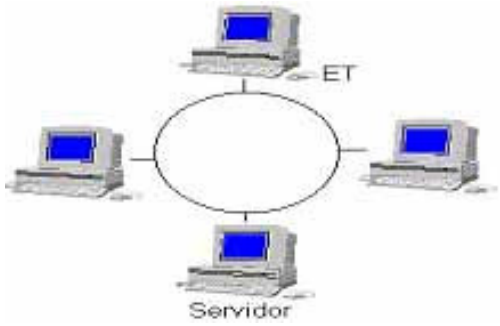


Figura 1.3 Topología de anillo.

En la **topología de Estrella**, cada nodo de la red se conecta a un punto central, formando una especie de estrella [4]. Este punto es tan sólo un dispositivo de conexiones, o uno del mismo tipo más una estación de trabajo (Figura 1.4). La principal ventaja de esta topología frente a las otras consiste en que cuando el cable de un nodo se desconecta o rompe, dicho nodo es el único que queda desconectado de la red.

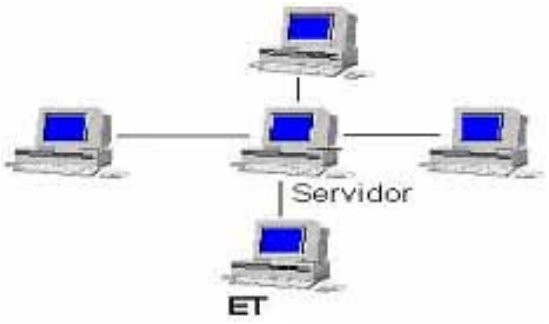


Figura 1.4 Topología de estrella

1.2 Clasificación de las Redes.

Existen varios criterios para clasificar las redes [URL1]. Entre los que se encuentra: tipo de transmisión, cobertura, tipo de tráfico y aplicación.

En la clasificación por el **tipo de transmisión** están los Sistemas Punto a Punto y por Difusión [URL1]. En el sistema Punto a Punto cualquier estación funciona como servidor y comparte recursos con las demás estaciones. En los sistemas por Difusión ó *Broadcasting* se tiene un canal de comunicación que es compartido por las demás máquinas de la red, se emplean en topologías de bus, satélite o radio y anillo.

En la clasificación por **tipo de propiedad** están las redes públicas y privadas. Las primeras prestan servicios a terceros y las otras corresponden a empresas o entidades particulares.

En las de **tipo de tráfico** abarcan la transmisión de voz, video y datos. Para cada tráfico varia en ancho de banda disponible en la red [URL1].

En las de **tipo de cobertura** se encuentran [4] las LAN, MAN y WAN. Las redes LAN abarcan pocos kilómetros y se emplean para crear redes privadas en las organizaciones y emplea estándares comunes son el IEEE 802.3 (*Ethernet*), IEEE 802.4 (*Token Bus*), IEEE 802.5 (*Token Ring*). Las redes MAN son LANs más grandes, son públicas o privadas y adoptan el estándar DQDB ó IEEE 802.6. Las redes WAN son más extensas, abarcan grandes áreas geográficas.

1.3 Medios Físicos de Transmisión.

Un medio de transmisión es el medio o cable que permite enviar-recibir información de una red a otra y/o de equipo a equipo [12], [1], [2], [3], [7]. Hay medios de transmisión guiados como el cable coaxial grueso y delgado, par trenzado y fibra óptica. Los medios de transmisión no guiados son los enlaces de radio, de microondas o satélites y emplean el aire para propagarse.

El **cable coaxial** [2] consiste en un cable conductor interno cilíndrico separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre por otra capa aislante que es la funda del cable (Figura 1.5).

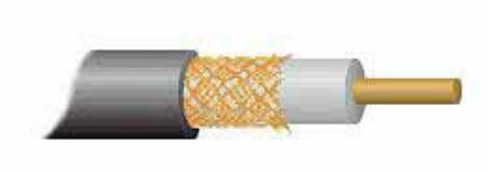


Figura 1.5 Cable Coaxial.

Se utiliza para transmitir señales analógicas o digitales. Sus inconvenientes son: atenuación, ruido térmico, ruido de intermodulación.

El **par trenzado** [2] son dos hilos de cobre aislados y trenzados entre sí, y envueltos por una cubierta protectora. Se utiliza tanto para transmisión analógica como digital, y su ancho de banda depende de la sección de cobre utilizado y de la distancia que tenga que recorrer. (Fig. 1.6)

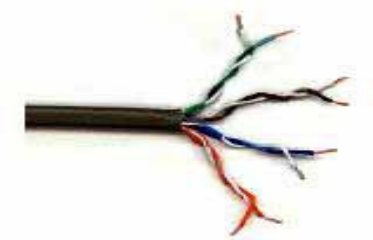


Figura 1.6 Cable Par Trenzado.

La **fibra óptica** [2] es un medio flexible y fino que conduce energía óptica. Tiene forma cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos, abrasiones, humedad, etcétera (Fig. 1.7).

Figura. 1.7 Fibra Óptica.

Sus beneficios son: ancho de banda mayor; menor tamaño, peso y atenuación; aislamiento electromagnético; y una mayor distancia entre repetidores. El rango de frecuencias es todo el espectro visible y parte del infrarrojo. El método de transmisión es monomodal, multimodal y multimodo de indice gradual.

Para **enlaces punto a punto** [2] se suelen utilizar microondas (altas frecuencias). Para enlaces con varios receptores posibles se utilizan las ondas de radio (bajas frecuencias). Los infrarrojos se utilizan para transmisiones a muy corta distancia (en una misma habitación).

Las **ondas de radio** [2] son fáciles de generar, viajan distancias largas, y penetran edificios fácilmente, son omnidireccionales. Las propiedades de ondas son dependientes de la frecuencia. Debido a su habilidad viajan grandes distancias, y la interferencia entre los usuarios es un problema.

Las **microondas** [2] viajan en una línea recta, se necesitan repetidoras periódicamente. Mientras más altas sean las torres, más distantes pueden estar. Esto las hace relativamente baratas. Se usan para la comunicación de teléfono a larga distancia, teléfonos celulares y distribución de la televisión.

Un **satélite** [3] de comunicación puede ser pensado como un repetidor de microondas en el cielo. El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario. Se suele utilizar este sistema para difusión de televisión, transmisión telefónica a larga distancia y Redes privadas.

Los **infrarrojos y ondas milimétricas** [3] son ampliamente usados en la comunicación de corto rango, son direccionales, baratos y fáciles de construir, pero su mayor inconveniente es que no atraviesan objetos sólidos. Estas propiedades han hecho del infrarrojo un candidato interesante para LANs inalámbricas

En la Tabla 1.1, se muestran las características de los distintos medios de transmisión.

MEDIO	CAPACIDAD	INTERFERENCIAS	LONGITUD	COSTE
Coaxial Grueso	Alta	Bajas	500 m.	Medio
Coaxial Fino	Alta	Bajas	200 m.	Bajo
Par Trenzado	Media/Baja	Muy Altas	20 – 30 m.	Muy Bajo
Par Trenzado Apantallado	Media	Altas	100 m.	Bajo
Fibra Óptica	Muy Alta	Ninguna	500 m.	Muy alto
Radio	Media/alta	Medias	10m. -10Km.	Alto
Infrarrojos	Media	Medias	20 m.	Alto

Tabla 1.1. Tabla comparativa entre distintos medios de transmisión.

1.4 Tecnología de redes.

Cada tecnología opera de manera diferente debido a que fueron desarrolladas en distintos ambientes y con métodos de acceso diferentes. Como cada tecnología se desarrolló por una compañía diferente, las organizaciones internacionales como la ISO, IEEE, y otros organismos, generaron reglas de la forma en que deben operar este tipo de tecnologías en cualquier ambiente [4], [3], [8]. Según la NIC: los mensajes, pasan a ser datos y en partes más pequeñas *frames* y tramás. El tamaño de tramás en una red de tipo: *Token Ring* es de 4096 *bytes* como tamaño máximo, para *Ethernet* el tamaño máximo es de 1514 *bytes*. Cada tarjeta de red debe tener una dirección única ya codificada desde fabricación.

El sistema ***Ethernet*** fue originalmente creado por D.I.X. La norma 802.3 de IEEE define una red similar, aunque ligeramente diferente que usa un formato alternativo de trama. *Ethernet* presenta un rendimiento de 10 Mbits/seg. Utiliza un método sensible a la señal portadora. El Método de acceso múltiple con detección de portadora y detección de colisiones se utiliza para arbitrar el acceso al cable. Es un sistema económico y fácil de instalar [4].

Las redes *Ethernet* pueden ser cableadas con diferentes tipos de cable. Cada uno con sus ventajas e inconvenientes. Una desventaja es cuando hay muchos usuarios, la hace más lenta y puede haber usuarios frustrados. La nomenclatura de los cables *Ethernet* esta formada por 3 partes: la primera indica la velocidad en Mbits/seg, la segunda indica si la transmisión es en banda base (BASE) o en banda ancha (BROAD), y la tercera los metros de segmento multiplicados por 100.

Algunas especificaciones de *Ethernet* se pueden observar en la Tabla 1.2.

TIPO	CARACTERÍSTICAS
10-BASE-5	Cable coaxial grueso (*Ethernet* grueso). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 500 metros.
10-BASE-2	Cable coaxial fino (*Ethernet* fino). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 185 metros.
10-BROAD-36	Cable coaxial. Segmentos: máximo de 3600 metros. Velocidad de transmisión: 10 Mb/seg.
100-BASE-X	*Fast Ethernet.* Velocidad de transmisión: 100 Mb/seg.

Tabla 1.2 Especificaciones de *Ethernet*.

Las redes ***Token Ring*** a diferencia de las redes *Ethernet*, son deterministicas y no probabilísticas. [4] El anillo con testigo le corresponde la norma 802.5 del IEEE. Una red en anillo con paso de testigo se puede configurar en una topología en estrella. Aunque la red físicamente aparece como una configuración en estrella, internamente las señales viajan alrededor de la red de una estación a la siguiente. La configuración del cableado y la adicion o supresión de un equipo debe asegurar que se mantiene en anillo lógico. Las estaciones de trabajo se conectan a los concentradores centrales llamados MAU (Unidades de acceso multiestación).

Realiza un diagnostico y detección de problemas. Es de 3 o 5 veces mayor el costo en comparación a la *Ethernet*. Este tipo de red está en el 25% de las redes. Los requerimientos básicos de hardware son una tarjeta de red compatible con el sistema *Token ring*, Cable (UTP) y una MAU.

Las redes **FDDI** son redes de alta velocidad, creadas para transmitir a mayor velocidad [4], [7] para aplicaciones gráficas y de video. Son redes costosas y la tecnología de acceso al medio es IEEE 802.8 paso de testigo. Trabaja con banda ancha (*broad band*), emplea la multiplexación en el canal (varias transmisiones a la vez), las transmisiones son bidireccionales, y se transmite a cualquier tiempo.

Hace uso de la topología Bus o Estrella. Las colisiones las hace a través de CSMA / CD, el cual los detecta y elimina. Los tipos de FDDI son FDDI Tipo 1 (Transmite a 100 Mbps) y FDDI Tipo 2 (Transmite de 600 a 800 Mbps).

Las redes **ATM** son redes de tercera generación, usa un método muy flexible para transportar los tipos de información (voz, video, datos) entre los dispositivos de una LAN a WAN. La tecnología que emplea se le conoce como intercambio de celdas (*cell switching*) y son de tamaño fijo. Las redes ATM son

redes orientadas a la conexión, primero establecen la conexión con la estacion con la que desean intercambiar información y validan que la conexión sea exitosa. ATM es una nueva tecnología con la capacidad de soportar cualquier tipo de tráfico a las más altas velocidades dentro de una red [4].

1.5 Las Redes e Internet.

Internet es una red mundial de computadoras que actualmente conecta entre 30 y 40 millones de personas. Construida por el Departamento de Defensa de los Estados Unidos [URL1], [URL33], [URL38].

Internet es una serie de redes privadas de computadoras (LANs, MAN's y WAN's) conectadas dentro de una organización. Cada organización solamente se hace responsable de las computadoras en su esfera de influencia [1], [12], [13].

Internet emplea un protocolo común: TCP/IP. Este protocolo hace posible la interconexión de los ordenadores con diferencias físicas y lógicas.

Debido a que millones de personas de todo el mundo navegan por esta red se le conoce también como "La Autopista de la Información".

Una de las ventajas de Internet es que posibilita la conexión con todo tipo de ordenadores, desde los personales, hasta los más grandes que ocupan habitaciones enteras, incluso se pueden ver conectados a la red cámaras de video, robots, máquinas de refresco, etc. Internet no tiene propietario, la información que circula por la red es libre e ilimitada. Los contenidos y las transmisiones se realizan entre computadoras interconectadas desde todas las partes del mundo. Un proveedor de Internet es quien da acceso a Internet a otras personas o particulares con un costo determinado, tienen la capacidad de crear e introducir contenidos dentro de la red. Y un usuario de Internet es la quien a través de un proveedor accede a Internet y a la demás información y servicio de la misma.

Las posibilidades que ofrece Internet se denominan **servicios**. Cada servicio es una manera de sacarle provecho a la red independiente de las demás [13], [URL3]. Una persona puede especializarse en el manejo de un servicio sin saber nada de los otros.

Los servicios que ofrece Internet son diversos. Los principales y más importantes servicios son [URL13]:

- **WWW**. Es un servicio basado en el Sistema de hipertexto, método para presentar información a través de la conexión entre documentos. Los creadores de WWW introducen además de texto, fotos, sonido y video. Permite ampliar la información de lo seleccionado, es una de las características del hipertexto.
- **Correo Electrónico**. (E-mail). Son servicios que permiten conectar computadoras mediante un sistema de correo personal. Cada usuario tiene

asignada una dirección en la que recibe todos los mensajes que se le envíen en cuestión de minutos.

- ***Mailing List*** (Lista de Correo). Este servicio envía en forma de correo electrónico todos los mensajes de las áreas temáticas que interesen. Los gestores del servidor se limitan a recoger todos los mensajes y a distribuir copias a los que están suscritos a las listas.
- Los ***Usenet News***. Es un sistema de conferencias, que permiten agrupar a personas interesadas en diversas áreas. Una conferencia es un foro multimedia a través del que se intercambia información de muy diversa naturaleza.
- El ***Chat*** es un sistema de conferencia que se establece entre los usuarios de las terminales que se encuentra disponibles en el ciberespacio y que permite el intercambio de información en tiempo real.
- ***Gopher***. Es un sistema de organización jerárquica de información e Internet. Permite acceder o menú carpetas donde están incluidos todos los documentos de la red que se pueden visualizar e imprimir. Es un buscador a nivel FTP.
- ***Telnet***. Es un protocolo que permite conectarse con otra computadora de la red de Internet.
- **FTP.** Es un protocolo que permite la transferencia de ficheros de una computadora a otra.

Las ventajas de las empresas al conectarse a Internet es que eliminan costes de ventas, la vía de comunicación es rápida y en dos direcciones, el servidor es más ágil. Es el único canal universal de comunicación y comercialización de productos que existe. Es rápido, flexible, y barato.

1.6 Arquitectura de protocolos.

Para la comunicación entre dos entidades situadas en sistemas diferentes, se necesita definir y utilizar un protocolo. Los puntos que definen un protocolo son la **sintaxis**, la **semántica**, y la **temporización.** Estas tareas se subdividen y a todo se le llama **arquitectura del protocolo**.

El protocolo [1], [URL1] es un: “Conjunto de reglas predeterminadas que hacen posible el intercambio coordinado de mensajes entre usuarios, procesos, máquinas, esto incluye mecanismos de control de las relaciones entre las entidades comunicantes, la localización de los recursos y el flujo ordenado d*e la comunicación*.”

Debido a la complejidad de una comunicación segura entre computadoras, se puede dividir esta complejidad en **niveles ó capas**, y el número de niveles y la función, varían de una red a otra [1].

El propósito de cada nivel es ofrecer determinados servicios al nivel inmediatamente superior, ocultando todos los detalles de implementación de estos servicios. A los elementos activos de cada capa se denominan **entidades**, pueden

ser *Hardware* o *Software*. Dos entidades en el mismo nivel en máquinas diferentes se denominan **entidades compañeras** o **procesos pares**.

Un **servicio** es un conjunto de operaciones (primitivas) que un nivel provee al nivel superior. Una **interfaz** corresponde a la separación o división entre dos capas de un modelo de comunicación, y es la encargada de definir las operaciones básicas y los servicios que el nivel inferior ofrece a la capa superior del modelo.

Las capas ofrecen servicios de dos tipos: **orientados a la conexión** (*Connection oriented*) y **no orientados a la conexión** (*Connectionless*). Además, cada uno de estos servicios puede ser caracterizado por cierta calidad de servicio que ofrecen. Así, se pueden tener **servicios confiables** y **servicios no confiables**.

Toda comunicación que se haga entre computadoras lo hace a través de servicios mejor conocidos como **primitivas de servicio.** Un servicio esta formalmente especificado por un conjunto de primitivas (operaciones), a disposición de todos los usuarios o de otras entidades para acceder al servicio.

Estas primitivas le indican al servicio que debe efectuar una acción o notifican la acción tomada por una entidad par. Como se muestra en la Tabla 1.3, las primitivas de servicio en el modelo OSI pueden dividirse en cuatro clases.

Primitiva	**Significado**
Solicitud	Una entidad desea que el servicio realice un trabajo.
Indicación	Una entidad es informada acerca de un evento.
Respuesta	Una entidad desea responder a un evento.
Confirmación	Una entidad va a ser informada acerca de su solicitud.

Tabla 1.3 Primitivas de servicio

1.7 Arquitecturas de redes

Al conjunto de todos los protocolos y niveles se les denomina "Arquitectura de Redes" y dan lugar a una solución completa en la implementación de sistemas informáticos, algunas de estas arquitecturas o familias de protocolos son [9], [11], [6], [URL43]: OSI de ISO, TCP/IP de ARPANET, XNS de Xerox, SNA de IBM, DNA de DEC, y algunas variaciones: Redes Microsoft, Novell y Banyan.

1.7.1 El Modelo TCP/IP

El éxito inicial de TCP/IP fue debido a su inclusión en las diferentes variedades del Sistema Operativo UNIX y fue impulsado por que su implantación

resultó más cómoda y económica que los protocolos equivalentes. TCP/IP [6], [9] emplea un modelo de enrutamiento basado en datagramas (paquetes) en lugar de circuitos virtuales. TCP/IP brinda a los arquitectos de sistemas e ingenieros de comunicaciones una independencia del hardware utilizado. Este protocolo es el esqueleto de otros múltiples subprotocolos que se apoyan en él, se convierte es un estándar muy propagado en E.E.U.U. alrededor de 1983 gracias a su gran flexibilidad.

TCP/IP se basa en una transferencia de información dividida en varios grupos llamados “paquetes”. Cada paquete tiene como cabecera la dirección del equipo destinatario. Estas unidades de pequeño tamaño proporcionan grandes ventajas a la hora de transmitir información a través de un solo medio físico de transmisión, usado por más de una computadora. La transmisión de paquetes evita que la información se mezcle entre sí. Ya que fluyen en orden uno tras de otro y se diferencian entre sí desde el principio y fin de cada paquete.

El origen del sistema de comunicación es fiable y resistente. TCP/IP [9] no es más que un sistema de protocolos, donde TCP e IP son los más destacados. La misión de IP es transferir datos a través de una red, de diversos nodos que se van pasando la información de una a otra, y la tarea de TCP es que se envíe la información correctamente entre un computador de origen al de destino TCP/IP, se ha convertido en el estándar de intercomunicación de redes de área extensa y es el único protocolo de enlace y transporte permitido en Internet[1].

La figura 1.8, muestra las diferentes capas del conjunto TCP/IP. Cada capa del *stack* de protocolo de la computadora de origen se comunica con la misma capa de la computadora destino. Las capas que se encuentran al mismo nivel en el ordenador de origen y de destino son pares. Así mismo, la aplicación de la computadora origen y la del destino son pares. Desde el punto de vista del usuario o programador, la transferencia de paquetes se efectúa directamente de una capa par a otra.

Las capas del modelo TCP/IP se dividen en cuatro: Capa Interfaz de Red o Host a Red, Capa de Red o Internet, Capa de Transporte y Capa de Aplicación.

La **capa inferior** [9], se relaciona con la capa física respecto del modelo OSI, y contienen varios estándares del IEEE como son el 802.3 llamado *Ethernet* que establece las reglas para enviar datos por cable coaxial delgado (10Base2), cable coaxial grueso (10Base5), par trenzado (10Base-T), fibra óptica (10Base-F) y su propio método de acceso al medio físico. El 802.4 llamado *Token Bus* puede usar estos mismos medios, pero con un método de acceso diferente y otros estándares genéricamente como 802.X.

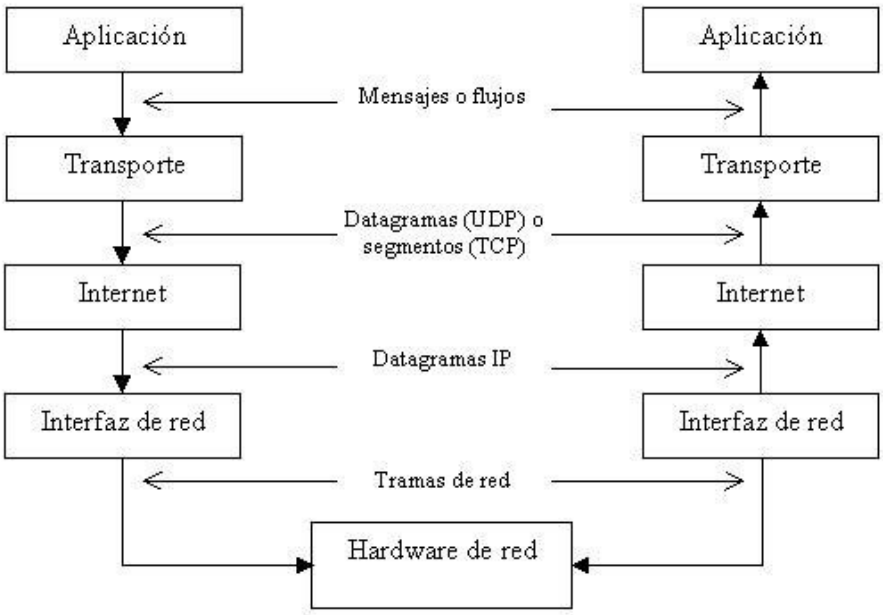


Figura 1.8 Capas de protocolos TCP/IP.

La **capa de Red** [9] cumple junto con la anterior, los niveles 1,2 y 3 del Modelo OSI. En este nivel se define el protocolo IP y es responsabilidad de entregar los paquetes en los destinos indicados, realizando las operaciones apropiadas de Ruteo y la solucion de problemás como Congestion o Caidas de enlace.

En la **capa de Transporte** [6] esta formada por dos protocolos: TCP y UDP. TCP es un protocolo confiable y orientado a conexión, lo que significa que ofrece un medio libre de errores para enviar paquetes. UDP es un protocolo no orientado a conexión y no es confiable.

En la **capa de Aplicación** [6] se encuentran decenas de aplicaciones ampliamente conocidas como WWW, FTP, Telnet, DNS, el Servicio de Correo Electrónico (SMTP, *Simple Mail Transference Protocol*), etc.

El conjunto de protocolos TCP/IP corresponde con el modelo de comunicaciones de red definido por la ISO [12]. Este modelo se denomina modelo de referencia OSI. El modelo OSI describe un sistema de redes ideal que permite establecer una comunicación entre procesos de capas distintas y fáciles de identificar. En el *host*, las capas prestan servicios a capas superiores y reciben servicios de capas inferiores.

La comparación entre los modelos OSI y TCP/IP se puede observar en la Figura 1.9.

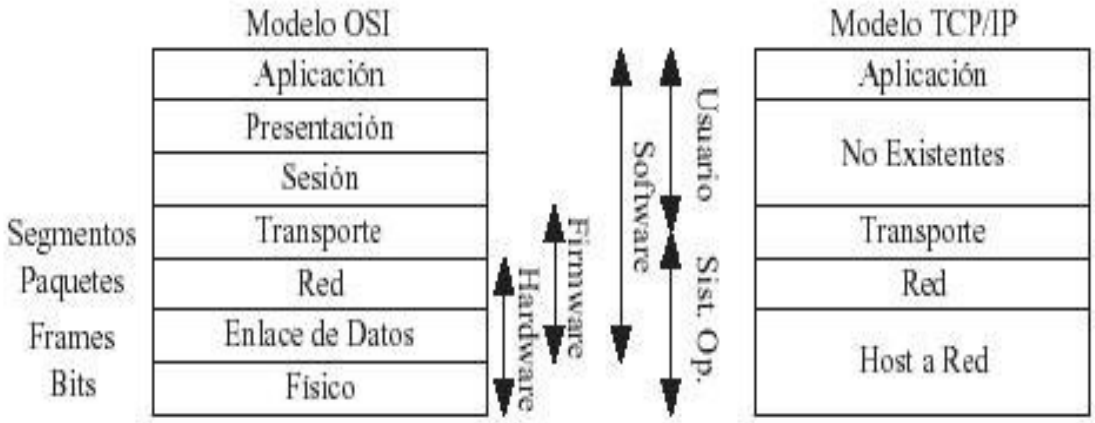


Figura 1.9 Comparación Entre los Modelos OSI y TCP/IP.

La figura 1.10, [12] muestra las siete capas del modelo de referencia OSI y su correspondencia general con las capas del conjunto de protocolos TCP/IP.

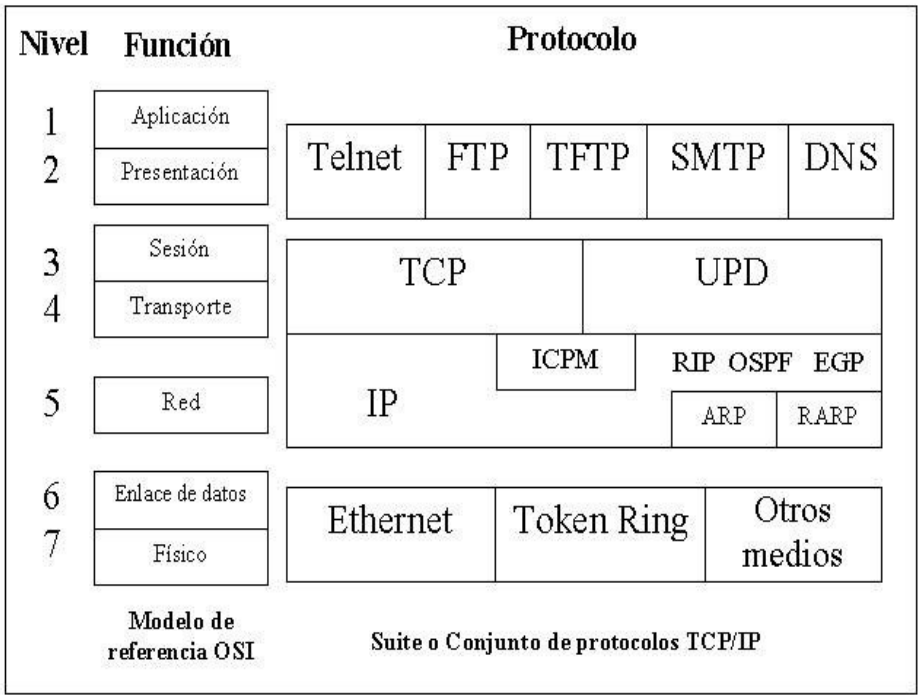


Figura 1.10 Modelo OSI y las Capas de TCP/IP.

El sistema para determinar capas permite a los programadores concentrar sus esfuerzos en las funciones de una capa determinada [URL6].

En la Tabla 1.4, se enumeran los protocolos más comunes del conjunto de protocolos TCP/IP [12], [16] y los servicios que proporcionan.

Protocolo TCP/IP	Servicio
IP	Proporciona servicios para la entrega de paquetes (encaminamiento) entre nodos.
ICMP	Regula la transmisión de mensajes de error y control entre los *host* y los *gateways*
ARP	Asigna direcciones Internet a direcciones físicas.
RARP	Asigna direcciones físicas a direcciones de Internet.
TCP	Proporciona servicios de envió de flujos fiables entre los clientes.
UDP	Proporciona servicio de entrega de datagramas no fiable entre clientes.
FTP	Proporciona servicios de nivel de aplicación para la transferencia de archivos.
TELNET	Proporciona un método de emulación de terminal.
RIP	Permite el intercambio de información de encaminamiento de vectores de distancia entre *routers*.
OPSF	Permite el intercambio de información de encaminamiento de estado del enlace entre *routers*
EGP	Permite el intercambio de información entre *routers* externos.
SLIP	Permite la transmisión de paquetes pequeños en la segunda capa. No tiene control de flujo ni seguridad.
PPP	Igual que SLIP, pero tiene el control de errores y los recupera.
PPTP	Permite a usuarios remotos conectarse a Internet a una red privada. Usa técnicas de cifrado y compresión.

Tabla 1.4. Protocolos más comunes del conjunto de protocolos de TCP/IP.

Las aplicaciones que se desarrollan con TCP/IP, normalmente usan varios protocolos del conjunto. La suma de las capas del conjunto de protocolos se conoce también como el *stack* del protocolo. Las aplicaciones definidas por el usuario se comunican con la capa superior del conjunto de protocolos. La capa de nivel superior del protocolo de la computadora origen traspasa la información a las capas inferiores del *stack,* que a su vez la pasan a la red física. La red física traspasa la información a la computadora destino. Las capas inferiores del *stack* de protocolo de la computadora destino pasan la información a las capas superiores, que a su vez la pasan a la aplicación de destino.

Las aplicaciones para el nivel 5 son [16]:

- **HTTP.** Consulta de hipertexto, enlaces con más información. Trafico de hipertexto (bajar o subir información a través de Internet).
- **NTP**. Permite que varios sistemas sincronicen su reloj de acuerdo al servidor de horario.
- **RPC**. Se ejecutan procedimientos que no están en la máquina que hace la llamada. Se necesitan dos máquinas. El Cliente hace una llamada al servidor este ejecuta un procedimiento y obtiene resultados entonces envía una respuesta al cliente.

- **SMTP.** Protocolo de correo electrónico, especifica el formato exacto de los mensajes que un cliente debe enviar desde un ordenador al servidor de otro, pero no especifica como debe almacenarse el correo ni con que frecuencia se debe intentar el envío de los mensajes.
- **TELNET**. Permite que un usuario, desde una terminal, acceda a los recursos y aplicaciones de otros ordenadores. Una vez que la conexión queda establecida, actúa de intermediario entre ambos ordenadores.
- **FTP**. Se utiliza para la transferencia de ficheros proporcionando acceso interactivo, especificaciones de formato y control de autentificaron (aunque es posible conectarse como el usuario *anonymous* que no necesita contraseña).
- **NFS**. Desarrollado por *Sun Microsystems Incorporated* y autoriza a los usuarios el acceso en línea a archivos que se encuentran en sistemas remotos.
- **SNMP**. Sirve para administrar los sistemas de forma remota. También se puede utilizar para supervisar el tráfico de la red.
- **TFTP**. Es un protocolo destinado a la transferencia de ficheros pero sin permitir tanta interacción entre cliente y servidor como la que existe en FTP. Otra diferencia es que en lugar de utilizar el protocolo TCP, utiliza el UDP.
- **NIS.** Sistema de información de red. Anteriormente conocido como *yellow pages* es un servicio de autentificación utilizado frecuentemente para complementar los servicios NFS. Provee una base centralizada de las cuentas de los usuarios y los nodos, la cual puede ser consultada por otros nodos de la red.
- **Gopher.** Es un FTP mejorado. A diferencia de FTP, no se requiere conocer el nombre del servidor del que se desea copiar un archivo. El servidor *Gopher* se encarga de informar al cliente *Gopher* del verdadero destino de algún archivo para que pueda realizar la conexión y recuperar los datos. Esta flexibilidad simplifica la búsqueda y recuperación de datos.
- **Pop.** Instrucciones que permiten recuperar un elemento del servidor. Permite accesar al correo electrónico al servidor de correo de la red.
- **WWW.** Es similar a *Gopher* en cuanto a accesar información almacenada en muchos nodos diferentes, pero además ofrece una elegante interfaz con fuentes, gráficas, sonidos y ligas de tipo hipertexto a otros documentos.

1.7.2 Modelo OSI.

El modelo OSI no garantiza la comunicación entre equipos pero pone las bases para una mejor estructuración de los protocolos de comunicación [11], [12], [URL43].

El Modelo OSI está compuesto por siete capas basadas en los siguientes principios (Figura 1.11):

- Una capa se creará en situaciones en donde se necesita un nivel diferente de Abstracción.
- Cada capa efectuará una función diferente.

- La función que realizará cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.
- Los límites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfases.
- El número de capas deberá ser lo suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa y, por otra parte, también deberá ser lo suficientemente pequeño para que su arquitectura no llegue a ser difícil de manejar.

El modelo OSI [5], [10], [8] por si mismo no es una arquitectura de red, solo indica lo que cada capa deberá hacer. Describe como se transfiere la información desde una aplicación de software a través del medio de transmisión hasta la aplicación en otro elemento de la red.

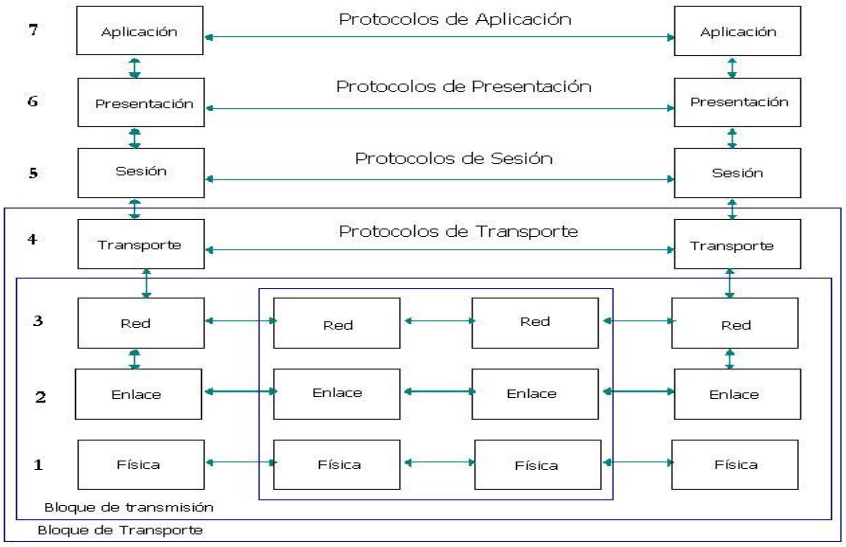


Figura 1.11 Arquitectura de red basada en el Modelo OSI.

Para su mejor estudio las siete capas del modelo OSI se dividen [4] en tres bloques (Figura 1.12) en:

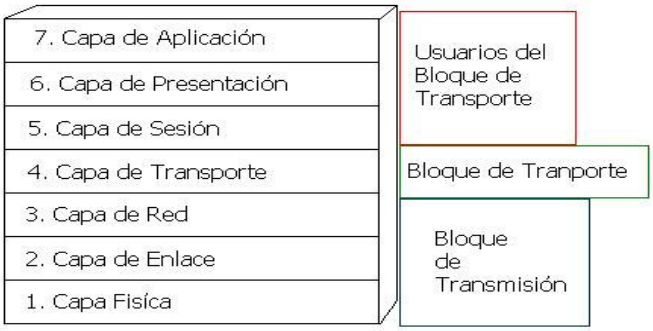


Figura 1.12. Los siete niveles del modelo OSI.

La **Capa Física** tiene que ver con el envío de bits en un medio físico de transmisión y se asegura que estos se transmitan y reciban libres de errores; en esta capa se definen y materializan las características mecánicas, eléctricas funcionales asociados con el medio y los conectores; así como tiempos aprobados para enviar o recibir una señal. Se especifica si el medio permite la comunicación [8] simplex, *half duplex* o *full duplex*.

En la **Capa de enlace** se toman los bits que entrega la capa física y los agrupa en algunos cientos o miles de bits para formar los *frames* (tramas). Aquí se realiza un chequeo de errores y se devuelven reconocimientos al emisor. Esta capa es la encargada de detectar si un *frame* se pierde o se daña en el medio físico, y de retransmitirlo. En este nivel se decide cómo accesar al medio físico.

La **Capa de Red** se encarga de controlar la operación de la subred. Su tarea principal es decidir cómo hacer que los paquetes lleguen a su destino, de un origen y a un destino en un formato predefinido por un protocolo. Y resuelve los cuellos de botella.

La obligación de la **Capa de transporte** es tomar datos de la capa de sesión y asegurarse que dichos datos lleguen a su destino, multiplexar varias conexiones que tienen diferentes capacidades de transmisión para ofrecer una velocidad de transmisión adecuada a la capa de sesión, y es ofrecer un mecanismo que sirva para identificar y diferenciar las múltiples conexiones existentes, así como determinar en que momento se inician y se terminan las conversaciones.

La **Capa de Sesión** establece, administra y finaliza las sesiones de comunicación entre las entidades de la capa de presentación. Las sesiones de comunicación constan de solicitudes y respuestas de servicio que se presentan entre aplicaciones ubicadas en diferentes dispositivos de red. Estas sesiones están coordinadas por protocolos implementados en esta capa. Aparte de la sincronización y establecimiento de puntos de chequeo.

La **Capa de Presentación** provee servicios que permiten transmitir datos con alguna sintaxis y semántica propia para las aplicaciones o para el nodo en que se esta trabajando. En esta capa se convierten los datos a un formato independiente de los nodos que intervienen en la transmisión.

En la **Capa de Aplicación** se encuentran aplicaciones de red que permiten explotar los recursos de otros nodos. La comunicación entre los procesos se realiza mediante un determinado protocolo.

En la Tabla 1.5 se observan los dispositivos así como los protocolos que se emplean en cada Capa o Nivel del Modelo OSI [10].

Los protocolos [URL5] que emplea el Modelo de OSI en cada capa son diferentes, entre estos protocolos se encuentra:

- **LAP.** (Nivel 1,2). Protocolo de acceso de enlace que proporciona los servicios básicos de transmisión de paquetes entre nodos de la red, así también permite la identificación de los nodos en forma dinámica con 8 bits.
- **AARP.** (Nivel 1, 2). Protocolo que realiza la traducción de la identificación de los nodos de *AppleTalk* a los de una red *Ethernet* o *Token Ring* la identificación se realiza con 48 bits.
- **TLAP.** (Nivel 1, 2). Permite comunicación con maquinas *Token Ring*.

Nivel	Nombre	Función	Dispositivos y protocolos
1	Físico	Se ocupa de la transmisión del flujo de bits a través del medio.	Cables, tarjetas y repetidores RS-232, X.21
2	Enlace	Divide el flujo de bits en unidades con formato (tramás) intercambiando estas unidades mediante el empleo de protocolos.	Puentes HDLC y LLC.
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red.	Encaminador, IP, IPX.
4	Transporte	La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido. Envía de nuevo lo que no haya llegado correctamente.	Pasarela, UDP, TCP, SPX.
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Pasarela.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Pasarela, compresión, encriptado, VT100, X.400.
7	Aplicación	Este nivel proporciona servicios estandarizados para poder realizar funciones específicas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (envío de un archivo). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha recomendado (enviar el archivo).	

Tabla 1.5 Funciones y dispositivos de las capas del modelo OSI.

- **ELAP.** (Nivel 1, 2). Permite comunicación con maquinas *Ethernet*.
- **DDP.** (Nivel 3). Es el protocolo que entrega los datagramas con un tamaño máximo de 586 *bytes*, en la cabecera del paquete se incluye la información de dirección destino y comprobación de errores.
- **AEP.** (Nivel 4). Determina si un nodo va a estar disponible para la comunicación. También se utiliza para determinar el tiempo que emplea un paquete en alcanzar un nodo de la red.
- **NBP.** (Nivel 4). Traduce la dirección numérica de Internet de un nodo en una dirección con nombre.
- **ATP.** (Nivel 4). Maneja solicitudes, respuestas y liberación de transacciones para garantizar la entrega de los paquetes.
- **RTMP.** (Nivel 4). Mantiene la tabla de encaminamiento con las direcciones y se comunica con otros encaminadores para determinar el estado de la red.
- **ASP.** (Nivel 5). Es un cliente de ATP que permite establecer sesiones entre 2 nodos en otras palabras permite inicializar y terminar una sesión.
- **ZTP.** (Nivel 5). Es el encargado de mantener el mapa de red en lo referente al control y al encaminamiento.
- **ADSP.** *AppleTalk Data Stream Protocol*. (Nivel 5). Gestiona la transmisión de datos entre 2 ordenadores permitiendo que ambos transmitan a la vez.
- **PAP.** (Nivel 5). Mantiene la comunicación entre una estación de trabajo y la impresora de la red.
- **AFP.** (Nivel 6, 7). Permite el acceso a archivos remotos en los servidores de la red.

En la Figura 1.13, se muestran los protocolos [10] que emplea cada Capa del Modelo OSI:

CAPAS	PROTOCOLOS
Aplicación	AFP, Servicios de Impresión
Presentación	AFP, Servicio de Impresión
Sesión	ADSP, ZIP, ASP, PAP
Transporte	RTMP, AEP, ATP, NBP
Red	DDP
Enlace	LAP, AARP, TLAP, ELAP
Física	*TokenTalk, EtherTalk, LocalTalk*

Figura 1.13 Capas del Modelo OSI y sus Protocolos.

1.8 La Seguridad en las Redes.

Los tipos de seguridad que existen en las redes se dividen [19], [URL36], [URL42], [URL44] en **Seguridad Física,** contra daños materiales y **Seguridad lógica** que es el control de datos a fin de reducir el riesgo de transferencia, modificación, pérdida o divulgación de los datos.

Los principales riesgos que se corre al no asegurar la información en las redes [2], [3], [15], [18] son: la **facilidad de hacer Réplicas de datos digitales, Redes sin auditorias, Redes conectada a Internet sin *firewalls*, Virus,** diversos **Ataques TCP/IP, Ingeniería social, Usuarios descuidados, Computadoras sin asegurar, Datos sin asegurar (sin respaldo), Ataques sin malicia, y Ataques maliciosos**.

La creación de un programa de seguridad debe contener las siguientes medidas: la **clasificación de personal, un sistema de control de acceso de usuarios** (*passwords*)**, sistemas de protección de tiempo de espera en la Terminal, encriptación de archivos, restricción del tiempo de acceso, detección y expulsión de intrusos, asignación de propiedades, métodos de respaldo, control de virus, control de software, monitoreo y auditoria de sistemas**.

Para asegurar la permanencia de la información se debe tener [URL44]: un **disco de Sistema, un programa de antivirus actualizado y fuente de información sobre virus, un programa de respaldo de áreas criticas, respaldos, discos nuevos, una revisión de los programas que se obtengan por medio del módem o a través de redes**, y finalmente una **revisión periódica de la computadora** [URL7].

La información corre riesgos sobre todo con los virus y los piratas informáticos (*crackers*) [4], [20], [URL39].

Un **virus** es un programa o código el cual ingresa a través de diversas vías a otros sistemas y se autoreproduce a si mismo creando varias copias y dañando, modificando e incluso elimina la información en la memoria, la mayoría de las veces el usuario se de cuenta hasta que es demasiado tarde.

Las características que se necesitan para que un virus sea virus son: que sea **dañino**, se **autoreproduzca**, y sea **subrepticio**. Los virus son generalmente el “juguete dañino” de cualquier programador que quiere probar sus habilidades y que al final lo único que logra es dañar a cientos de personas [URL8], [5], [URL7].

Entre los virus más comunes están los del **sector de arranque**, los virus **EXE**, y los **macro virus**. En los tres casos, el efecto puede ser mínimo hasta la corrupción o eliminación de datos.

El **antivirus** [20] es un programa que tiene como fin, encontrar, clasificar y destruir cualquier organismo, en este caso al virus, que trate de ingresar al sistema del usuario [URL8], [5].Los antivirus funcionan de acuerdo a diversos sistemas para detectar la presencia del virus. La forma de operar de un antivirus se conforma por lo general en dos módulos: Módulo de control y Módulo de respuesta.

La presencia de **piratas informáticos** conocidos [23], [20] como *hackers* [URL40], [15]y *crackers*, es el problema mayor que un virus; son personas con un alto grado de conocimiento en el campo de la informática, usan sus conocimientos para el bien como para el mal [URL9].

Los *hackers* no son criminales en el mejor de los casos, son los incentivadores, probadores y aprobadores de las mejores y más nuevas tecnologías. Los *hackers* pueden ser traviesos, perversos y delincuentes curiosos. Los delitos que llega a cometer un pirata informático son variados. Una persona que posee más conocimiento puede realizar acciones más elaboradas y peligrosas como son el acceso a informaciones confidenciales y la destrucción de datos o de software. [URL8].

Dada la globalización de los recursos computacionales por el Internet, estos piratas informáticos son cada vez más peligrosos ya que en la actualidad poseen avanzadas herramientas de *crackeo* y en muchos de los casos son los principales creadores de virus que no poseen otro fin más que el de destruir. Algunos delitos [URL8], [URL9] en redes computacionales reconocidos son [23], [20]: **Virus, Gusanos, Bomba lógica o cronológica, *Address Spoofing*,** y los **Caballos de Troya.**

TCP se diseño para ofrecer una conectividad razonable, pero no se diseño como un protocolo seguro. Así que los *crackers* [23] han descubiertos muchos trucos técnicos que les permiten sortear la seguridad o bien hacer caer por completo el sistema. Hay dos tipos de ataques de TCP/IP. El primero es el ataque de negación de servicio y el otro es el ataque furtivo [9].

Se debe tener en cuenta dentro de la organización las inseguridades que existen y revisar las **principales vulnerabilidades de seguridad.** El descuidar uno de estos puntos, significaría un potencial de entrada no autorizado a la red corporativa [URL10], [URL11].

Las Principales vulnerabilidades de seguridad son: un control de acceso inadecuado al ruteador, puntos de acceso no seguros, filtración de información, servicios innecesarios, una mala política de utilización de contraseñas, cuentas de prueba, servidores mal configurados, *firewalls* mal configurados, aplicaciones sin corregir, excesivos controles de acceso, excesivas relaciones de confianza, servicios sin autenticar, registro inadecuado, y por último la falta de políticas de seguridad.

1.8.1 Legislación jurídica de delitos informáticos.

El manejo de recursos informáticos se ha convertido en un arma de doble filo para todos, ayuda a realizar muchas cosas y al mismo tiempo deja información confidencial al alcance de personas sin escrúpulos y con malos propósitos

capaces de ocasionar grandes disturbios con sus acciones, por estos motivos muchos países han tomado medidas en sus legislaciones contra los delitos informáticos como [URL7]:

- **Acceso no autorizado**. Uso ilegitimo de *passwords* y la entrada de un sistema informático sin la autorización del propietario.
- **Destrucción de datos.** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- **Infracción al copyright de bases de datos.** Uso no autorizado de información almacenada en una base de datos.
- **Interceptación de e-mail.** Lectura de un mensaje electrónico ajeno.
- **Estafas electrónicas.** A través de compras realizadas haciendo uso de la red.
- **Transferencias de fondos.** Engaños en la realización de este tipo de transacciones.

Por otro lado, Internet permite dar soporte para la comisión de otro tipo de delitos:

- **Espionaje.** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo.** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- **Narcotráfico.** Transmisión de fórmulas para la fabricación de estupefacientes, blanqueo de dinero y la coordinación de entregas y recogidas.

Una solución para proteger todo el sistema consiste en no permitir ningún acceso desde el exterior al interior, de esta forma solo se podrían mandar solicitudes pero no se podrían recibir el contenido de las mismas. Otra opción es permitir ciertas clases de accesos y negar otros, eliminando así el problema, y se puede implementar mediante un *firewall*.

1.8.2 *Firewalls*.

Un ***firewall*** [18] en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. Determina cuál de los servicios de red pueden ser accesados dentro de ésta por los que están fuera de la organización.

Para que un *firewall* sea efectivo, todo tráfico de información a través de Internet deberá pasar a través del *firewall* donde podrá ser inspeccionada la información. El *firewall* podrá únicamente autorizar el paso del tráfico, y podrá ser inmune a la penetración [URL12], [15]. Este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este (Figura 1.14).

La mayoría de empresas utilizan un *firewall* para conectar una red interna a Internet de forma segura, pero al igual se puede utilizar un *firewall* para asegurar una red interna ante otra red de una Intranet [URL12], [URL13].

Los *firewalls* y los *proxies* representan un poderoso muro de protección entre la computadora o la red interna e Internet, barrera que conviene instalar en todo sistema que esté conectado a Internet 24 horas al día, por modesto que sea [URL13].

Un ***proxy*** es una aplicación o un dispositivo hardware que hace de intermediario entre los usuarios, normalmente de una red local, e Internet.

La función de un *proxy* es recibir peticiones de usuarios y redirigirlas a Internet, y es "transparente" al usuario. Los últimos *proxies* que han aparecido en el mercado realizan además funciones de filtrado, esta característica muchas veces hace que se confundan con un cortafuego [URL14], [URL10].

Figura 1.14 Localización de un firewall.

El **objetivo principal de un *firewall*** [15] es proteger a una red de otra. Por lo general, la red que se está protegiendo le pertenece a uno, y la red contra la que se protege es una red externa en la que no puede confiarse y desde la que se pueden originar intrusiones de seguridad.

Para proteger la red se debe evitar que usuarios no autorizados tengan acceso a datos delicados, mientras que se permite que usuarios legítimos tengan acceso a los recursos de la red [URL12], [URL13].

Un *firewall* es el principal instrumento utilizado para la implementación de una política de seguridad de la red de una organización y se necesitan técnicas de mejoramiento para la autenticación, seguridad y la privacía para aumentar la seguridad de la red [15], [URL14], [URL10].

El *firewall* ofrece [16], [18] un **aislamiento de Internet,** crea un **cuello de botella** o *choke-point*, mantiene una **auditoria y registro de uso**, crea una

seguridad de contenidos, permite una **autenticación** para ambos lados, y finalmente realiza una **traducción de direcciones de red** (NAT).

Un *firewall* actúa como un punto de cierre que monitorea y rechaza el tráfico de red a nivel de aplicación. Puede operar en las capas de red y transporte en cuyo caso examinan los encabezados de IP y de TCP de paquetes entrantes y salientes, y rechazan o pasan paquetes con base en las reglas de filtración de paquetes programadas (Figura 1.15).

Los *firewall* son la primera línea de defensa frente a los atacantes. Y deben estar óptimamente configurados para ser efectivos, de lo contrario es posible que un atacante aproveche las vulnerabilidades para lograr entrar a la red interna. [URL11].

Al definir la estrategia de un *firewall*, [18] se cree que es suficiente con prohibir todo lo que represente un riesgo para la organización y permitir lo demás. Sin embargo, ya que los piratas informáticos crean nuevos métodos de ataque constantemente, se deben de anticipar métodos para evitar tales ataques.

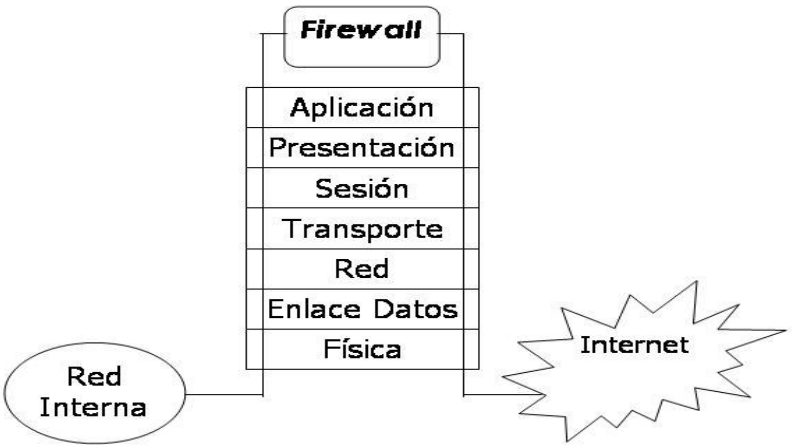


Figura 1.15 El *firewall* de la red a nivel de aplicación.

Debido a la funcionalidad del *firewall*, debe ser capaz de ofrecer una serie de características mínimas [15], como el empleo de una adecuada **política de seguridad**, y ofrecer servicios que contengan el **registro de las operaciones** que vaya realizando, que posea una **interfaz** fácil e intuitiva que reduzca al mínimo la posibilidad de que el operario se equivoque a la hora de configurarlo y mantenerlo, además de una **autenticación de usuarios**, y una **correlación de direcciones**, para mantener **restricciones de día y hora**, con un **control de carga,** y una **canalización** para combinar los servicios de aplicación en una sola conexión.

Un *firewall* no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación [16]. Este tipo de conexiones derivan la seguridad

provista por un *firewall* construido cuidadosamente, creando así una puerta de ataque.

Los usuarios pueden estar conscientes de que este tipo de conexiones no son permitidas como parte integral de la arquitectura de la seguridad en la organización. (Figura 1.16)

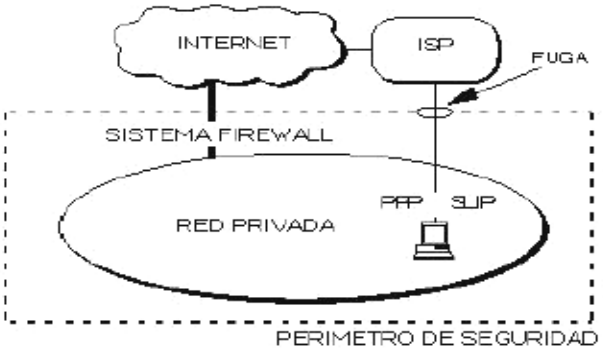


Figura 1.16 Conexión circunvecina al *firewall*.

Un *firewall* no puede protegerse contra **amenazas** por traidores o usuarios inconscientes, **ataques de Ingeniería Social,** por **Virus** a través de archivos y **software por medio de Internet**, y finalmente **ataques posibles en la Transferencia de Datos**.

Si se tiene funcionando un programa *firewall* de cualquier tipo, no hay que pensar que el sistema está protegido, la seguridad total es imposible. La forma de garantizar una seguridad total es no estar conectado a nada [16].

La principal amenaza de un *firewall* es el *hacker*, un joven inexperto con mucho tiempo disponible quién intentará meterse a un sistema por la emoción que representa el reto.

Probablemente el *hacker* intente atacar por alguno de los agujeros ya conocidos y seguramente es cubierto por un *firewall* convencional. Pero hay *hackers* que están a la última de riesgos de seguridad y tienen las más novedosas herramientas de *cracking*, tanto que diseñan sus propios ataques específicos, hacen sus programas y no aprovechan las fisuras de seguridad conocidas sino que descubren otras nuevas.

Así que surgen nuevas amenazas y un *firewall* no será capaz de protegerse contra ellas, hay que tener en cuenta que continuamente se descubren nuevas fisuras por las que se puede acceder a un sistema [16].

Una lista de **herramientas de un *hacker*** que puede usar para colectar esa información [15] es: el protocolo **SNMP,** el programa ***TraceRoute,*** el protocolo ***Whois***, los **Servidores DNS**, el protocolo ***Finger***, y el programa ***Ping***.

Un *hacker* después que obtiene la información de la red de la organización, trata de probar cada uno de los servidores para debilitar la seguridad. Para ello cuenta con programas en Internet como ISS y SATAN que determinan la debilidad de cada sistema con respecto a vulnerabilidades comunes en un sistema.

Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde esta debilitada su seguridad y así determinar que servidores necesitan ser remendados y actualizados con un *software* [15].

La filosofía fundamental de la **Seguridad en la Organización** [15] es:

- **Todo lo que no es específicamente permitido se niega**, el *firewall* puede obstruir todo el tráfico y cada uno de los servicios deseados necesariamente para ser implementadas básicamente caso por caso, se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.
- **Todo lo que no es específicamente negado se permite**, en esta filosofía se crean ambientes más flexibles al disponer más servicios para los usuarios de la comunidad y esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas.

Una política de seguridad se basará en una cuidadosa conducción analizando la seguridad, la asesoría en caso de riesgo y la situación del negocio. Si no se poseé una información detallada de la política a seguir, aunque sea un *firewall* cuidadosamente desarrollado y armado, se estará exponiendo la red privada a un posible atentado, depende de todos los servicios que presta y del contexto en el cual se esta. Ya que es diferente diseñar un *firewall* para proteger una ISP que las subdivisiones de una empresa.

El costo de un *firewall* depende del número de servicios que se quiere filtrar y de la tecnología electrónica del mismo, además se necesita que continuamente tenga soporte administrativo, mantenimiento general, actualizaciones de software y parches de seguridad [URL10], [URL12], [URL13].

Los *firewalls* permiten la implementación de DMZ. Un DMZ es un grupo de servidores a los cuales el *firewall* permite un acceso parcial, generalmente se emplea para servidores WWW, servidores FTP y servidores de correo.

La función del *firewall* es evitar que existan desde el exterior conexiones diferentes a las permitidas, y establecer menos restricciones hacia ciertos servidores, hacia el interior hay una total protección evitando todo tipo de conexión desde el exterior.

Otra cualidad es la posibilidad de establecer canales seguros encriptados, punto a punto entre los *firewalls*, también llamados VPN. Las VPNs se

implementan para el manejo de información confidencial sobre canales inseguros tales como Internet.

Es importante saber que un *firewall* esta compuesto por hardware y software que utilizado conjuntamente, impide el acceso no autorizado a una parte de la red.

El hardware del *firewall* consta normalmente de un sistema aparte, dedicado a ejecutar las funciones del software del *firewall,* el software puede constar de todas o alguna aplicación como filtros de paquetes, Servidores *Proxy,* Servidores SOCKS, Servicios de Conversión de direcciones de red (NAT), Software de anotaciones y supervisión, Servicios de Red privada virtual (VPN).

Existen tres tipos fundamentales de *firewalls*, y se catalogan en función al nivel en el que se encuentran. Esto no siempre es cierto, ya que un *firewall* para ser completo, deberá estar presente en todos los niveles [15]. Un *firewall* típico se compone de uno, o una combinación de los siguientes obstáculos: Ruteador Filtra-paquetes, *Gateway* a Nivel-aplicación y *Gateway* a Nivel-circuito.

Los **enrutadores de filtrado de paquetes** sirven para enrutar paquetes entre las máquinas internas y las externas, pero de forma selectiva, para ello toman los paquetes IP y les aplican unas reglas de filtrado, que permiten o rechazan ciertos paquetes según los criterios reflejados en la política de seguridad de la empresa a proteger. Es decir, trabajan a nivel de red.

El *firewall* contiene en su interior una lista de filtros a aplicar. Estos filtros se aplican a los paquetes secuenciales, de forma que si el paquete es aceptado por uno de ellos pasará al sistema, mientras que si no es así se le aplicará el siguiente filtro. Como es obvio, el ultimo filtro no va a permitir el acceso a nada (Figura 1.17).

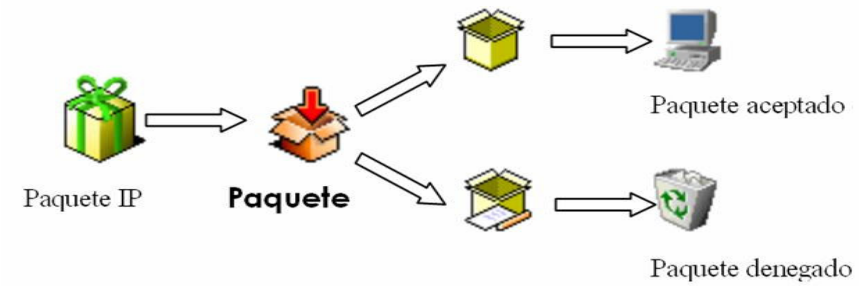


Figura 1.17 Funcionamiento de un Filtrador de Paquetes

Las **pasarelas a nivel de aplicación** es el extremo opuesto a los filtradores de paquetes. En lugar de filtrar el flujo de paquetes, tratan los servicios por separado, utilizando el código adecuado en cada uno de ellos. Es probablemente el sistema más seguro, ya que no necesitan utilizar complicadas listas de acceso y centraliza en un solo punto la gestión del servicio, además de que permite controlar y conocer información de cada uno de los servicios por separado.

Las pasarelas de nivel de aplicación a menudo se denominan bastiones, en cuanto que están especialmente protegidas ante ataques, diseñadas con la máxima seguridad posible. A la hora de trabajar con este sistema de protección se establece una puerta de acceso para cada servicio. Esta puerta es de uso obligatorio, y se puede establecer sobre ella los criterios de control que mejor convenga. Una vez sobrepasada la puerta, puede ocurrir que la propia pasarela ofrezca el servicio de forma segura o que se establezca una conexión con un ordenador interno que realmente ofrezca el servicio, teniendo a éste último configurado para aceptar conexiones tan solo de dentro a afuera (Figura 1.18).

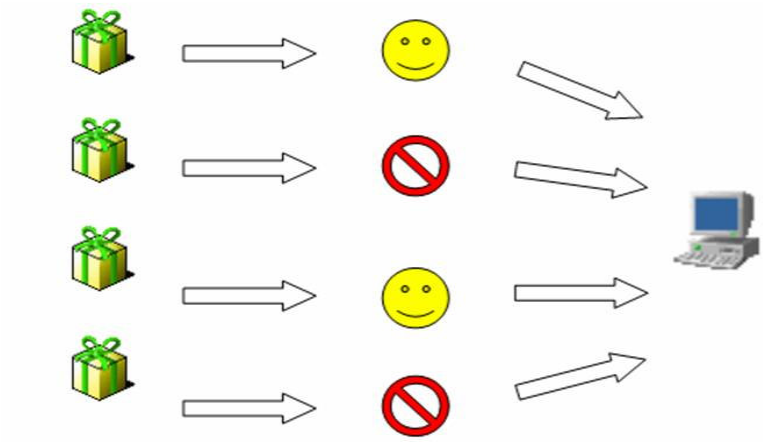


Figura 1.18 Pasarela a nivel de aplicación.

Las **pasarelas a Nivel de Red** se basan en el control de las conexiones TCP y su funcionamiento es que por un lado reciben las peticiones de conexión a un puerto TCP y por el otro se establecen las conexiones con el destinatario deseado si se han cumplido las restricciones de acceso establecidas.

Este tipo de *firewalls* trabaja junto a los servidores *proxy*. Si la acreditación es positiva se entabla la conexión. Por su forma de trabajar son muy adecuados para la obtención de información. Este *firewall* suele ser el más adecuado para el tratamiento de conexiones salientes, y con él no será nada complicado establecer restricciones sobre los ordenadores a los que se puede acceder o limitar el máximo de accesos permitidos.

Cuando se instala un *firewall* [18] suelen emplearse todos o algunos de estos tres tipos [7], y se debe a que cada uno de ellos realiza la protección a un nivel distinto, desde los paquetes de red, pasando por los puertos y llegando hasta el servicio propiamente dicho. De esta forma, cuanta más seguridad se desee, más componentes se deberán emplear en el *firewall* (Figura 1.19).

El futuro de las *firewalls* se encuentra a medio camino, entre las *firewalls* a nivel de red y las *firewalls* a nivel de aplicación, empleando filtradores de paquetes. El resultado será un sistema rápido de protección de paquetes que conecte y audite datos que pasan a través de él.

Los *firewalls* tanto a nivel de red como de aplicación, incorporan encriptación de modo que pueden proteger el tráfico que se produce entre ellos e Internet. Este tipo de *firewall* se puede utilizar por organizaciones con múltiples puntos de conexión a Internet, para utilizar a Internet como una "central privada" donde no sea necesario preocuparse de que los datos o contraseñas puedan ser capturados.

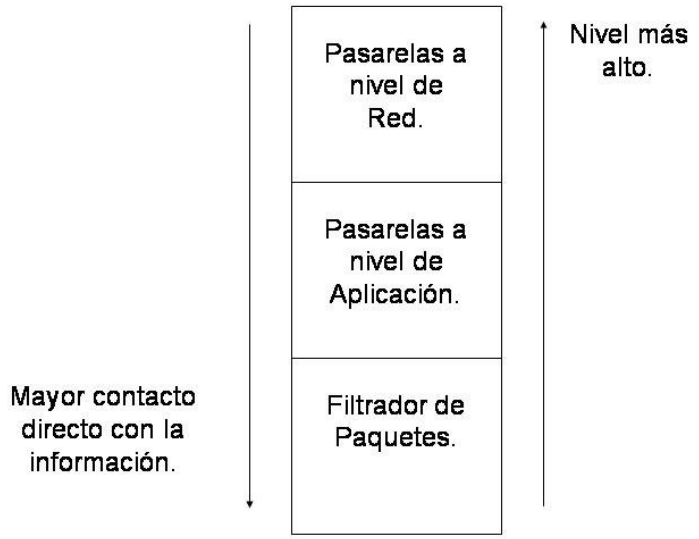


Figura 1.19 Un *firewall* completo.

La mayoría de los autores y los administradores con experiencia de campo en la utilización de *firewalls,* establecen una serie de consejos en cuanto a la configuración tanto de *firewalls* como de *routers,* de manera que no se dejen puertas traseras que permitan el ingreso no autorizado y que no se puedan rastrear, así como las arquitecturas que eviten que el tráfico de red se someta al análisis del mismo [18], [15].

Capítulo

2

Tecnología VPN.

En la actualidad las redes reducen tiempo y costos, con un mayor alcance de desarrollo para la empresa, logrando descentralizar su información manteniéndola al día y accesible. Esto se logra por medio de VPNs.

Significa una gran ventaja para las organizaciones que cuentan con oficinas remotas, pero también es cierto que este tipo de redes han despertado la curiosidad de algunas personas que se dedican a atacar servidores y redes para obtener información confidencial.

La seguridad de una VPN se logra con software (encripta, certifica y autentica), con *firewalls* y con hardware como los *gateways*, que logra hacer a la red “impenetrable”, hasta que encuentren una puerta trasera para dañarla. Estas redes son ideales para todo tipo de organización que desee

2. Introducción a las VPNs.

En estos días la tecnología avanza rápidamente, y con ello la inseguridad en las redes, debido a esto surge una tecnología en software y hardware que proporciona la velocidad y la seguridad de la información. Surge entonces el término de Red Virtual Privada (VPN), que ya forma parte del glosario de la Industria de Telecomunicaciones y Redes de Servicio [URL15].

La VPN se basa en los protocolos de Nivel 3 del Modelo OSI. Esta tecnología busca implementar redes de servicios privadas particionando redes públicas o compartidas de IP, donde la red pública IP más empleada es Internet. Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Una Red Virtual Privada es aquella red privada construida sobre una red pública que conecta los componentes de una red con otra red [17], [URL17], mantenida y controlada por la organización a la que sirve. Y a su vez la red privada requiere de sus propios equipos de conmutación y comunicación, sus propios servicios de comunicación o alquiler los servicios de una red pública o de redes privadas que tengan sus propias líneas de comunicación.

Las VPNs constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y además del gran alcance, lo asequible y escalable del acceso a través de Internet. Esta combinación hace de las VPNs una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización [URL16].

En una VPN todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia.

Para lograr esta funcionalidad y que sea segura debe completar tres tareas:

1. Debe ser capaz de pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos parezcan estar separados por una red pública.
2. La solución debe agregar encriptación de manera que el tráfico que cruce por la red pública no pueda ser encriptado, leído o modificado.
3. 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 (Figura 2.1).

Las VPNs permiten a usuarios que trabajan en casa o lejos conectarse de un modo seguro a un servidor corporativo remoto que usa la infraestructura de la asignación de ruta proporcionados por una red pública (Internet).

Desde la perspectiva del usuario, la VPN es una conexión del punto a punto entre la computadora del usuario y un servidor corporativo, ya que aparece como si los datos están siendo enviados sobre un enlace privado dedicado [URL18].

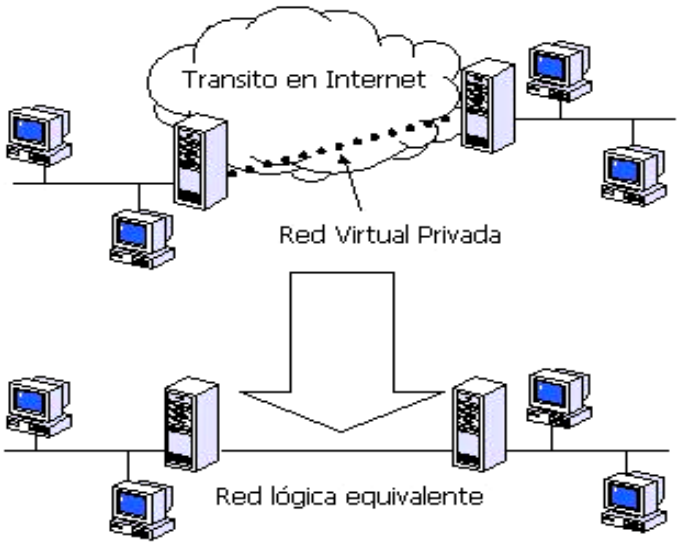


Figura 2.1 Red virtual privada.

Una VPN permite a la corporación conectarse a sucursales o a otras compañías (extranets) sobre una red pública, manteniendo las comunicaciones de manera segura. Esta conexión opera lógicamente como un enlace de WAN entre los sitios.

En ambos casos, la conexión segura por la red aparece al usuario como una comunicación en red privada (la comunicación ocurre sobre una red pública) de ahí su nombre de Red Privada Virtual [URL18].

Una VPN esta 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 los recursos centrales y entre sí.

Hay dos formas de conexión de VPN para una organización: la conexión de las redes sobre Internet y la conexión de las computadoras sobre Intranet.

A. Conexión de las redes sobre Internet.

Las VPNs proporcionan acceso remoto a los recursos corporativos sobre el Internet, mientras mantiene privacidad en la información (Figura 2.2).

En lugar de hacer una llamada de larga distancia para llamar a una compañía o a un NAS, el usuario llama a un ISP local. Usando la conexión del ISP local, el Software VPN crea una VPN entre el usuario telefónico y el Servidor VPN Corporativo a través del Internet (Figura 2.3).

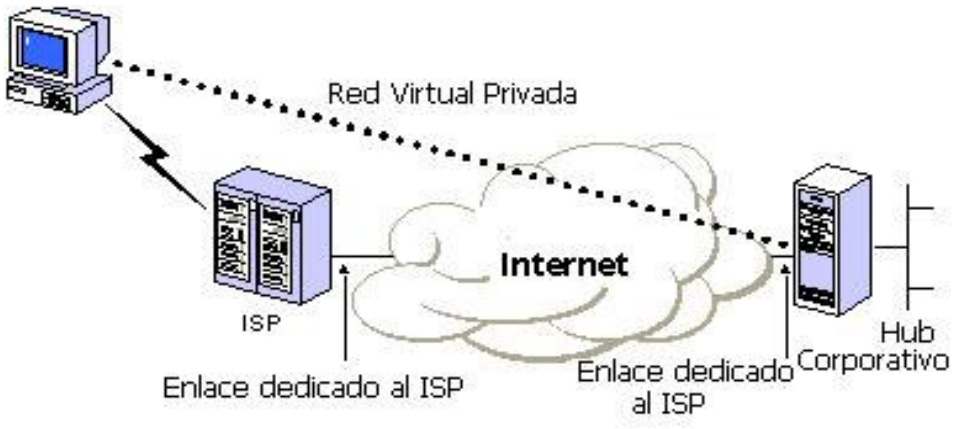


Figura 2.2 Conexión VPN de un cliente a una LAN privada

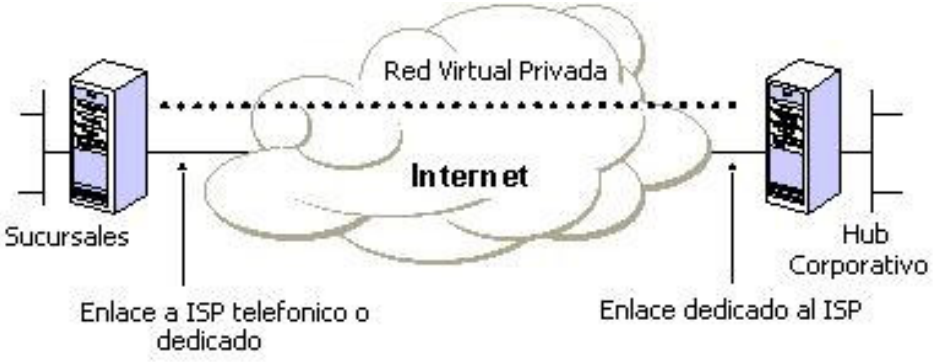


Figura 2.3 VPN para conectar dos sitios remotos.

Hay dos formas de emplear una VPN para conectar redes LAN a sitios remotos:

- **Uso de líneas dedicadas para conectar una sucursal a un LAN corporativa**. En lugar de usar un circuito especializado entre la sucursal y el *hub* de la corporación, tanto los ruteadores del *hub* de la sucursal como el corporativo, pueden emplear un circuito dedicado local e ISP local para conectarse a Internet. El software de VPN usa las conexiones de ISP locales y el Internet público, para crear una VPN entre el ruteador de la sucursal y ruteador de la *hub* corporativo.
- **Uso de una línea de marcación para conectar una sucursal a una LAN corporativa**. El ruteador en la sucursal llama al ISP local. El Software VPN utiliza la conexión al ISP local para crear una VPN entre la ruteador de la sucursal y el ruteador del hub corporativo, a través de Internet.

En ambos casos, los medios que conectan la sucursal y oficinas de la organización al Internet son locales. El ruteador del *hub* corporativo que actúa como un servidor de VPN debe conectarse a un ISP local con una línea dedicada.

Este servidor VPN debe estar listo las 24 horas por día para tráfico de VPN entrante.

B. Conexión de computadoras sobre Intranet

Hay que tener en cuenta que en algunas redes corporativas los datos departamentales son tan sensibles, que la LAN está físicamente desconectada del resto de la red corporativa. Mientras esta protege la información confidencial del departamento, se crea problemas de acceso a la información para otros usuarios que no están conectados en forma física a la LAN separada.

La VPN permite a la LAN del departamento estar conectada físicamente a la Intranet corporativa, pero separada por un servidor VPN. El servidor VPN no actúa como un ruteador entre la intranet corporativa y la LAN del departamento. Al utilizar una VPN el administrador de la red puede asegurar que sólo usuarios asignados de la Intranet corporativa puedan establecer una VPN con el servidor de VPN y tener acceso a los recursos protegidos del departamento. Además, la comunicación por el VPN puede ser encriptado para la confidencialidad de los datos. Y los usuarios no asignados no puedan tener acceso a la sección LAN. (Figura 2.4)

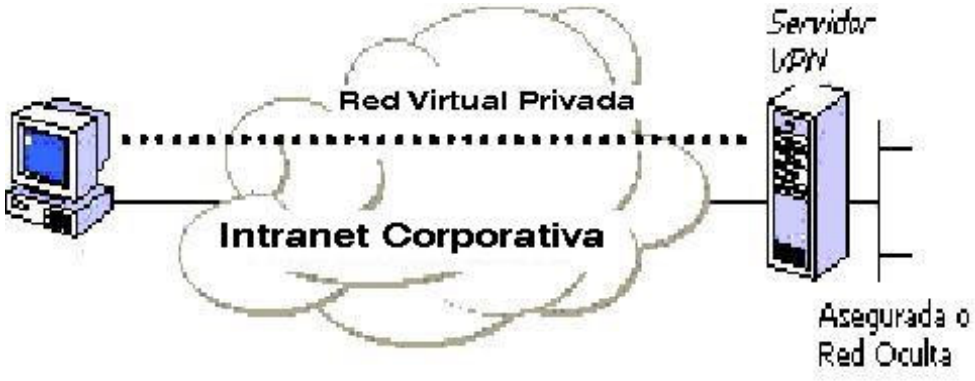


Figura 2.4 VPN para conectar dos computadoras en la misma LAN.

C. VPN según su conectividad

Las redes privadas virtuales se dividen en 3 categorías: (figura 2.5):

Una **VPN de Acceso Remoto** provee acceso remoto a la Intranet o Extranet corporativa a través de una infraestructura pública, conservando las mismas políticas, seguridad y calidad de servicio, que en la red privada [URL20]. Permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o IP para la conexión segura de usuarios móviles, teleconmutadores o sucursales remotas a los recursos corporativos (Figura 2.6)

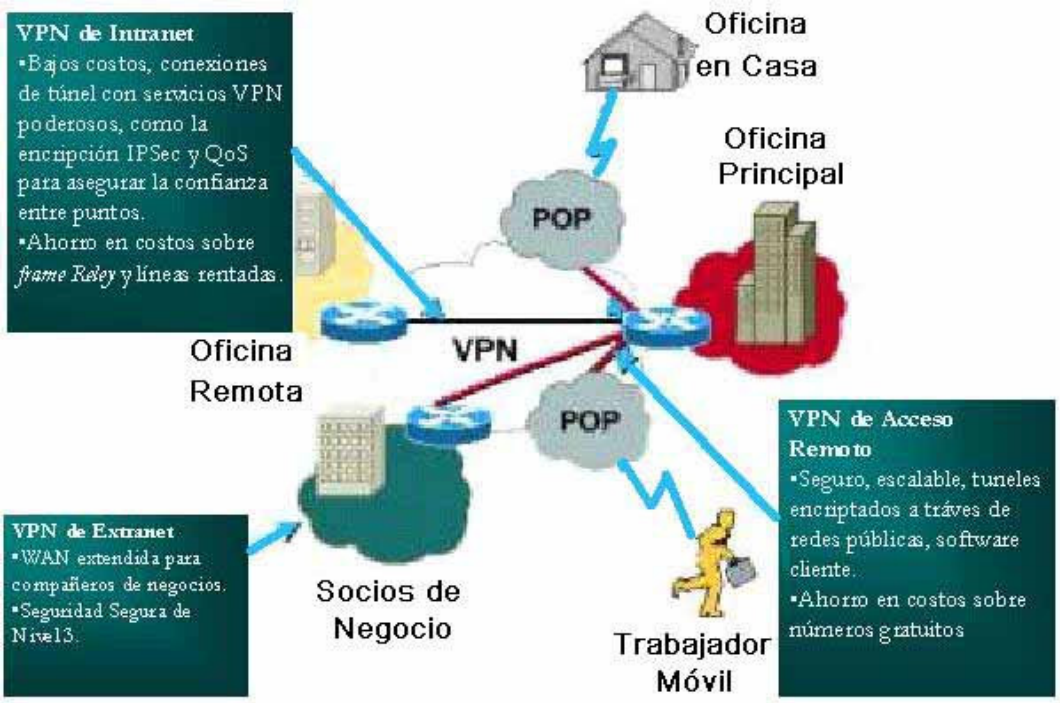


Figura 2.5 Tipos de VPN.

Se caracteriza por que la mantiene un Proveedor Externo de Acceso remoto (figura 2.7) por medio de llamadas locales o gratuitas y por Ubicuidad del acceso. Una Instalación y soporte del Proveedor de servicio, Acceso único al nodo central, tecnologías de acceso como: RTC, ISDN, xDSL; movilidad IP que permite conectarse a usuarios individuales a la Central a través de Internet o de otras redes públicas con servicio seguro. Y una Seguridad reforzada por el cliente. Sus beneficios son el Ahorro económico para reemplazar Servidores RAS y conexiones de larga distancia (*dial-up*) con conexiones ISP locales [URL21].

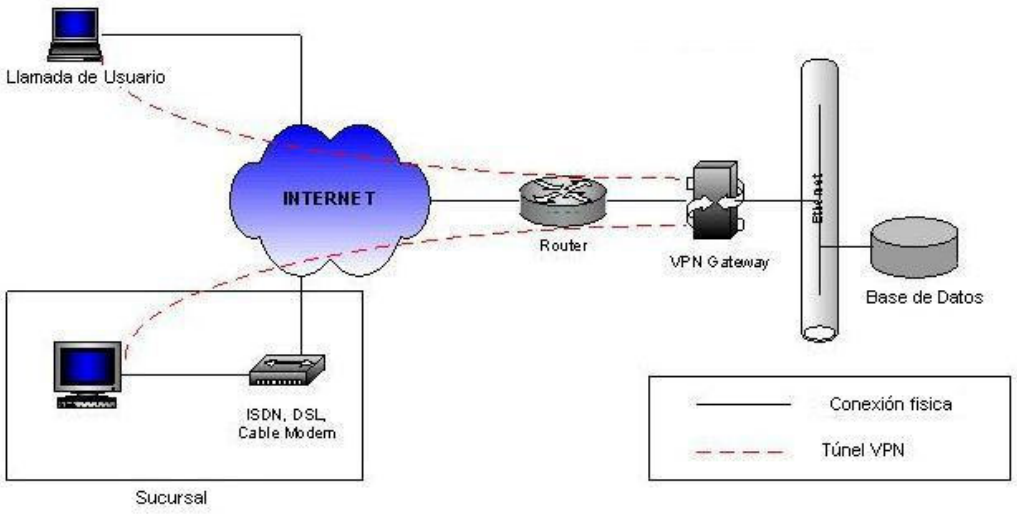


Figura 2.6 VPN de acceso remoto.

Seguridad en VPNs

Una **VPN de Intranet** vincula la oficina remota o sucursal a la red corporativa, a través de una red pública, mediante un enlace dedicado al Proveedor de Servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio y disponibilidad, entre otras (Figura 2.7).

Se caracteriza por que extiende el modelo IP a través de Internet o de otra red pública segura. En cuanto a los beneficios el Ahorro económico por reemplazo de llamadas de larga distancia por conexiones locales ISP [URL21].

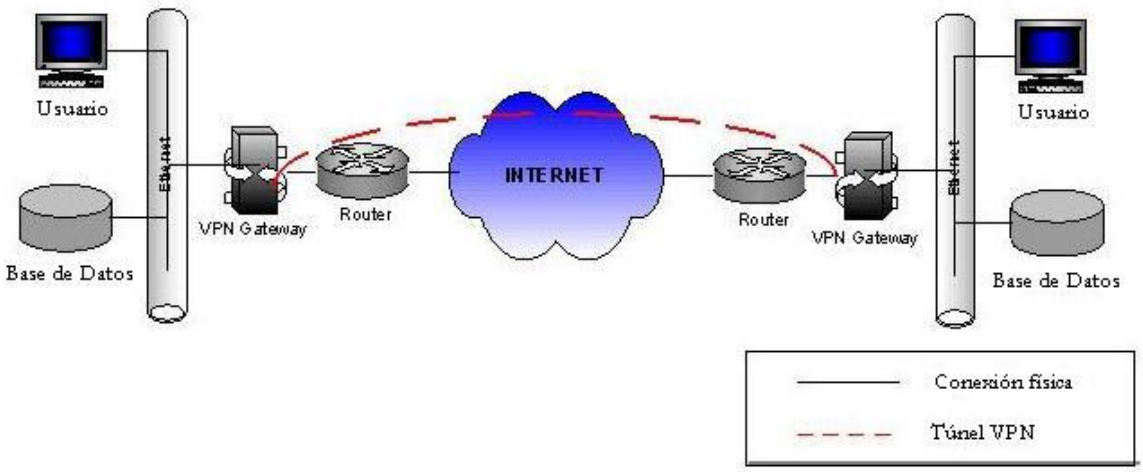


Figura 2.7 VPN de Intranet

Una **VPN de Extranet** permite la conexión de clientes, proveedores, distribuidores o demás comunidades de interés a la intranet corporativa a través de una red pública (Figura 2.8).

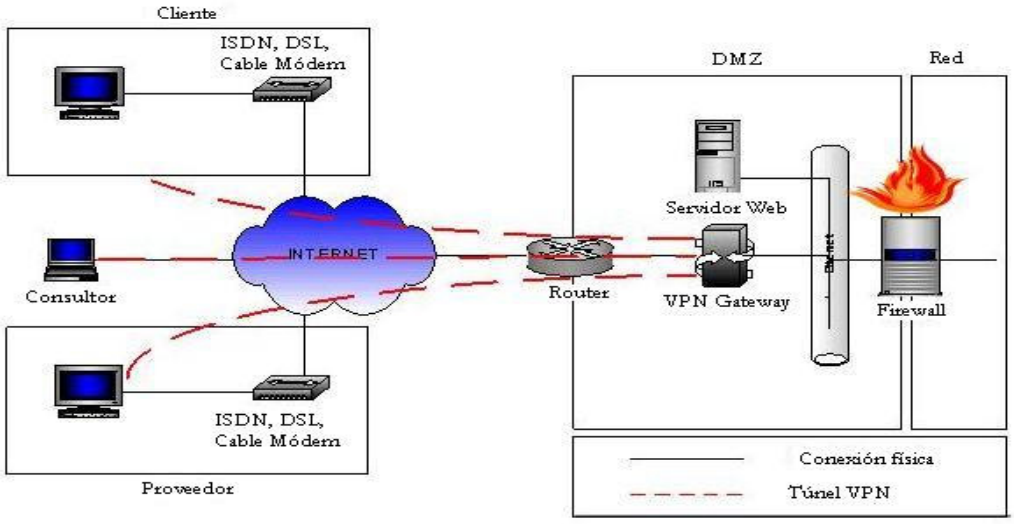


Figura 2.8 VPN de Extranet.

Su característica es que extiende la conectividad a proveedores y clientes sobre una infraestructura compartida usando Conexiones Virtuales Dedicadas. A

los socios se les asigna Niveles de Autorización: Acceso de Control de Listas, *firewalls*, filtros, según decida la empresa. Permitiendo una conexión segura con socios de negocios, proveedores y clientes.

Sus beneficios son el incremento de la Economía por extender la Intranet, con el propósito del comercio electrónico [URL21].

Las VPNs pueden ser relativamente nuevas, pero la tecnología de túneles está basada en estándares preestablecidos.

2.1 Requerimientos básicos en VPNs.

Por lo general, al implementar una solución de red remota, una compañía necesita facilitar el acceso controlado a los recursos corporativos e información. La solución debe permitir la libertar de conectar a clientes remotos a la red LAN, así como las oficinas remotas se conecten entre sí para compartir recursos e información (conexión de LAN a LAN).

Además, la solución debe garantizar la privacidad e integridad de datos cuando atraviesa el Internet público. Lo mismo se aplica en el caso de datos sensibles que cruzan una Intranet corporativa.

Por lo tanto, una **solución de VPN** debe proporcionar todo lo siguiente:

- **Autenticación del Usuario.** La solución deberá verificar la identidad del usuario y restringir el acceso a la VPN para que sólo permita a los usuarios autorizados, además de proporcionar auditorias y grabar la contabilidad para mostrar quien accedió a qué información y cuando.
- **Manejo de Direcciones.** La solución deberá asignar una dirección al cliente en la red privada, y asegurarse que estas direcciones privadas se mantengan privadas.
- **Encriptación de Datos.** Los datos que viajan en la red pública no podrán ser leídos por clientes no autorizados en la red.
- **Administración de Llaves.** La solución debe generar y renovar las llaves de encriptación para el cliente y servidor.
- **Soporte de protocolo múltiple.** La solución debe poder manejar protocolos comunes utilizados en la red pública. Como son IP, IPX y sucesivamente.

En Internet la solución de VPN basada en el Protocolo de Punto-a-punto (PPTP, *Point-to-Point Protocol*) o la Capa 2 Protocolo de Túnel (L2TP [URL37], *Layer 2 Tunneling Protocol*) reúne todos estos requisitos básicos, y se aprovecha de la amplia disponibilidad de Internet a nivel mundial. Otras soluciones, incluso el nuevo IP Protocolo de Seguridad (IPSec, *Security Protocol*), reúnen algunos de estos requisitos.

2.2 Bases de túnel.

Tunneling o Bases de Túnel es un método para usar una infraestructura de la intranet para transferir datos de una red sobre otra red. Los datos transferidos (*Payload*) pueden ser los *frame*s (paquetes) de otro protocolo. En lugar de enviar un *frame* a medida que es producido por el nodo origen, el protocolo de túnel encapsula el *frame* en una Cabecera Adicional. La Cabecera Adicional proporciona información para que el *payload* encapsulada viaje por la red intermedia.

Los paquetes encapsulados están enrutados entre los puntos finales del túnel sobre Internet. A la trayectoria lógica a través de cual los paquetes encapsulados viajan a través de la Internet se le llama **túnel**. Cuando los *frame*s encapsulados llegan a su destino en la Internet, el *frame* es desencapsulado y enviado a su destino final. El método *tunneling* incluye un proceso completo: encapsulación, transmisión, y desencapsulación de paquetes.

Algunos ejemplos de tecnologías maduras incluyen:

- **Túnel SNA sobre interredes IP**. Cuando el tráfico de la Arquitectura de Sistema de Red (SNA) es enviado a través de una Red Corporativa IP, el *frame* SNA se encapsula en una Cabecera UDP e IP.
- **Túnel IPX para *Novell NetWare* sobre interredes IP**. Cuando un paquete de IPX es enviado a un Servidor de *NetWare* o Ruteador IPX, el Servidor o Ruteador envuelve el paquete IPX en una cabecera UDP e IP, y lo envía a través de una interred IP. El Rúter destino IP-IPX remueve la cabecera UDP e IP, y envía el paquete al destino IPX.

Se han introducido nuevas Tecnologías de Túnel como:

- **PPTP**. Que permite encriptar tráfico IP, IPX o NetBEUI, y luego se encapsula en una cabecera IP para ser enviado a través de una interred IP corporativa o una interred IP pública como el Internet.
- **L2TP.** [URL37] Permite que se encripte el trafico IP, IPX o NetBEUI y luego se enviará sobre cualquier medio que de el soporte a la entrega de datagramas punto a punto, como IP, X.25, *Frame Relay*, o ATM.
- **IPSec**. El Modo de Túnel IPSec deja encriptar los *payloads* y después encapsularlos en una cabecera IP para enviarse a través de una interred corporativa IP o una interred pública IP como el Internet.

2.2.1 Protocolos de túnel.

Para establecer un túnel, tanto el túnel del cliente y el túnel del servidor deberán utilizar el mismo protocolo de Túnel. La tecnología de Túnel se puede basar en el Protocolo de Túnel de Nivel 2 ó 3 que corresponden al Modelo de Referencia OSI.

El protocolo de Nivel 2 corresponde al Nivel de Enlace de Datos, y usa *frame*s como su unidad de intercambio. PPTP, L2TP [URL37] y L2F son de Nivel 2. Estos protocolos encapsulan el *payload* en un PPP que será enviado por la interred.

El protocolo de Nivel 3 corresponde al Nivel de Red y utilizan paquetes. IPSec e IP sobre IP son de Nivel 3. Estos protocolos encapsulan los paquetes IP en una cabecera IP adicional antes de enviarlos por una interred IP.

Para los protocolos de Túnel de Nivel 2 como PPTP y L2TP [URL37], un túnel es similar a una sesión; los dos puntos finales del túnel deben aceptar el túnel y negociar variables de la configuración, tal como asignación de dirección o los parámetros de encriptación o de compresión. En ambos casos los datos transferidos atraviesan el túnel enviado usando un protocolo de datagrama. El protocolo de mantenimiento del túnel es usado como un mecanismo para administrar el túnel. El túnel debe ser creado, mantenido y después terminado.

Para los protocolos de Túnel de Nivel 3 generalmente supone todas las cuestiones de configuración son manejadas fuera de banda, a menudo por procesos manuales. Para estos procesos, no hay fase de mantenimiento de túnel.

Una vez que el túnel se establece, los datos del túnel pueden ser enviados. El túnel cliente o servidor utilizan un protocolo de transferencia de datos del túnel a fin de preparar los datos para la transferencia.

Por ejemplo, cuando el túnel cliente envía un *payload* al túnel servidor, primero el túnel cliente le agrega un encabezado de protocolo de transferencia de datos de túnel a la carga. Luego el cliente envía la carga encapsulada resultante a través de la interred, que lo dirige al túnel servidor. El túnel servidor acepta los paquetes, elimina el encabezado del protocolo de transferencia, y envía la carga a la red designada. La información enviada entre el túnel servidor y el túnel cliente se comporta semejantemente

A. Protocolos y requerimientos básicos de túnel.

Se basan en el protocolo de PPP, el protocolo de Nivel 2 (PPTP y L2TP [URL37]) heredan un conjunto de características útiles. Estas características, y sus contrapartes de Nivel 3 cubren los requerimientos de VPN básicos:

- **Autenticación de Usuario.** Los protocolos de túnel de nivel 2 heredan al usuario la autenticación de esquemas PPP, incluso los métodos de EAP. Los esquemas de túnel de Nivel 3 asumen que los puntos finales (*endpoints*) son conocidos (y autenticados) antes que el túnel se establezca.
- **Soporte de tarjeta de señales.** Usando EAP, el protocolo de túnel de Nivel 2 soporta una amplia variedad de métodos de autenticación, y las contraseñas de "una sola vez", calculadoras criptográficas, y tarjetas inteligentes. Los protocolos de túnel de Nivel 3 usan métodos similares.
- **Asignación de Dirección Dinámica.** El túnel de nivel 2 apoya la asignación dinámica de direcciones del cliente basados en el Protocolo de Control de la Red (NCP, *Network Control Protocol*) del mecanismo de la negociación. Los esquemas de túnel de nivel 3 asumen que una dirección ya ha sido asignada anteriormente para inicializar el túnel.
- **Compresión de Datos.** Los protocolos de túnel nivel 2 soportan esquemas basados en esquemas de compresión PPP. El IETF está investigando mecanismos similares para los protocolos de túnel nivel 3.
- **Encriptación de Datos.** Los protocolos de túnel de nivel 2 soportan mecanismos basados en la encriptación de datos PPP. Los protocolos de túnel nivel 3 pueden usan métodos similares.
- **Administración de llaves.** MPPE, un protocolo de Nivel 2, se basa en las claves iniciales generadas durante la autenticación del usuario, y luego la renueva periódicamente. IPSec, explícitamente negocia una llave común durante el intercambio de ISAKMP, y también la renueva periódicamente.
- **Soporte de protocolo múltiple.** Los protocolos de túnel de nivel 2 soportan múltiples cargas de protocolos, lo cual hace sencillo para los clientes del túnel accesar a la red de la corporación usando IP, IPX, NetBEUI, y más. Los protocolos de túnel de nivel 3 como el modo de túnel IPSec, soporta solo tarjetas de redes que usan el protocolo de IP.

B. Tipos de túnel.

Diversos proveedores que venden servidores de acceso de marcación han implementado la capacidad para crear un túnel en nombre del cliente de marcación. La computadora o el dispositivo de red que proporciona el túnel para la computadora del cliente se conoce como Procesador Frontal (FEP) en PPTP, Concentrador de Acceso L2TP [URL37] en L2TP [URL37], ó un *gateway* de Seguridad en IP en IPSec. FEP describe esta función sin tomar en cuenta el protocolo de túnel.

FEP debe tener instalado el protocolo de túnel apropiado y ser capaz de establecer el túnel cuando se conecte la computadora cliente (Figura 2.9). FEP puede establecer túneles a través de Internet a un servidor de túnel conectado a la red privada de la corporación, y así logra fortalecer las llamadas de diversas zonas geográficas en una sola conexión a Internet en la red corporativa.

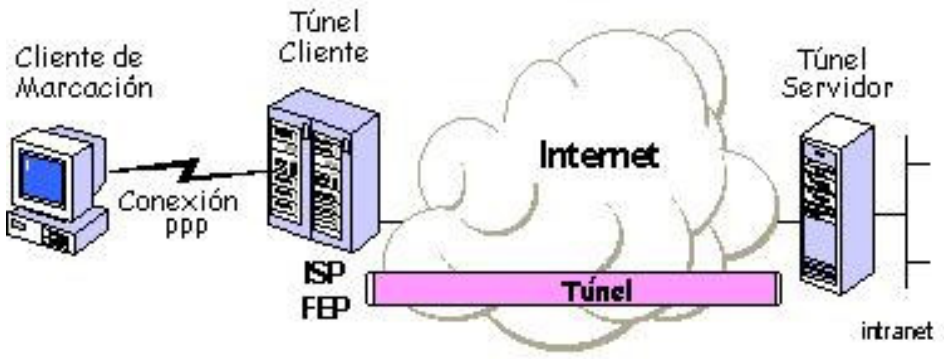


Figura 2.9 Túnel obligatorio.

Esta configuración se conoce como **Túnel Obligatorio**, debido a que el cliente esta obligado a usar el túnel creado por el FEP. Una vez la conexión inicial esta hecha, todo el tráfico de la red para y del cliente es enviado automáticamente a través del túnel. Con túneles obligatorios, la computadora del cliente hace una simple conexión PPP, y cuando un cliente marca al NAS, un túnel es creado y todo el tráfico es automáticamente enrutado a través del túnel. El FEP puede ser configurado para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. Además el FEP podría hacer túneles individuales de clientes basados en el nombre o destino del usuario.

Un túnel entre el FEP y servidor del túnel puede ser compartido por múltiples clientes de marcación. Cuando un segundo cliente marca al FEP para alcanzar un destino para el cual un túnel ya existe, no hay ninguna necesidad de crear una nueva instancia del túnel entre el FEP y servidor del túnel.

El tráfico de datos para el nuevo cliente es llevado sobre un túnel existente y puede haber múltiples clientes en un solo túnel, pero el túnel no es terminado hasta que el último usuario se desconecta del túnel.

Un servidor de acceso de marcación VPN capaz configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario no es un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel es el punto terminal del túnel y actúa como el cliente del túnel.

Un **túnel voluntario** ocurre cuando una estación de trabajo o ruteador de servidor utiliza el software del cliente del túnel, para crear una conexión virtual al servidor del túnel objetivo. Para esto, el protocolo de túnel apropiado debe ser instalado en la computadora del cliente. Para los túneles voluntarios se requiere una conexión IP (a través de una LAN o por marcación).

En una situación de marcación (*dial-up)*, el cliente debe establecer una conexión de marcación antes que el cliente pueda establecer un túnel.

En una PC conectada a una LAN, el cliente ya tiene una conexión a la interred que puede proporcionar enrutamiento a las *payloads* encapsuladas al servidor del túnel LAN escogido.

Es un concepto erróneo común que las VPN requieran una conexión de marcación. Solo se requiere una red IP. Algunos clientes (PCs de casa) usan conexiones de marcación a Internet para establecer transporte IP. Éste es un paso preliminar en la preparación para crear un túnel, y no es parte del protocolo del túnel mismo.

2.2.2 Protocolo de punto a punto (PPP).

PPP es un protocolo de Nivel 2, diseñado para enviar datos a través de conexiones de marcación o de Punto a Punto dedicadas. PPP encapsula paquetes IP, IPX, y NetBEUI dentro de *frames* de PPP, luego transmite los paquetes PPP encapsulados a través de un enlace punto a punto. PPP se usa entre un cliente telefónico y un NAS.

Hay cuatro fases distintas de negociación en una sesión telefónica PPP, y deben completarse exitosamente antes que la conexión PPP esté lista para transferir los datos del usuario.

- **Fase 1: Establecer un enlace PPP**. PPP usa el Protocolo de Control de Enlace (LCP, *Link Control Protocol*) para establecer, mantener, y terminar la conexión física. En la fase inicial de LCP, se seleccionan opciones de comunicación básicas.

Durante la Fase 1, se seleccionan los protocolos de autenticación, pero no se llevan a cabo hasta la fase de autenticación de conexión (Fase 2). De manera similar, durante una decisión LCP se toma una decisión acerca de que si dos iguales negociarán el uso de compresión y/o encriptación. La elección real de algoritmos de compresión / encriptación y otros detalles ocurre durante la Fase 4.

- **Fase 2: Autenticar al usuario.** La PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Un esquema de autenticación seguro proporciona protección contra ataques de repetición y personificación de clientes remotos.

Muchas de las implementaciones de PPP proporcionan métodos de autenticación limitados como PAP, CHAP y MSCHAP.

PAP es un esquema simple y claro de autenticación de texto, este esquema de autenticación no es seguro porque una tercera parte pudiera capturar el nombre del usuario y contraseña y podría usarlo para conseguirle acceso subsecuente al NAS y a todos los recursos proporcionados por el NAS. PAP no proporciona ninguna protección contra el ataque de reproducción o la personificación del cliente remoto una vez que se compone la contraseña del usuario.

CHAP (Figura 2.10) es un mecanismo de autenticación encriptado que evita la transmisión de contraseñas reales en la conexión. El NAS envía una petición (*challenge*) que consiste de una ID de sesión y una cadena de petición arbitraria, para el cliente remoto. El cliente remoto debe usar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación de la petición, la sesión ID, y la contraseña del cliente. El nombre del usuario se envía sin digerir (*unhashed*).

CHAP es una mejora sobre PAP en cuanto a que no envía la contraseña del texto claro sobre el enlace. Y la contraseña se usa para crear un *hash* encriptado para la petición original. CHAP protege contra los ataques de reproducción empleando una cadena de petición arbitraria para cada intento de autenticación. CHAP protege contra la personificación del cliente remoto de manera impredecible enviando repetidamente peticiones al cliente remoto por todas partes durante la conexión.

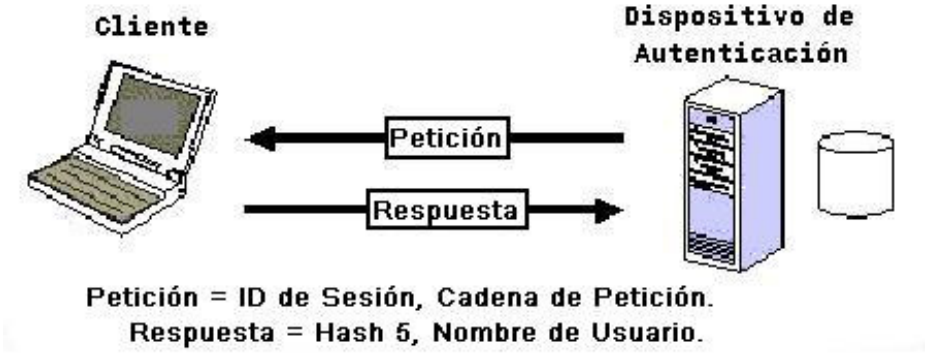


Figura 2.10 Proceso CHAP.

MS-CHAP es un mecanismo de autenticación de encriptación muy similar al CHAP. Este diseño manipula una verificación del MD4 de la contraseña, proporciona un nivel adicional de seguridad, porque permite al servidor guardar contraseñas verificadas en lugar de las contraseñas del texto transparentes. El MS-CHAP proporciona códigos adicionales de error, códigos de contraseñas ya expiradas y mensajes adicionales de cliente-servidor encriptadas que permite a los usuarios cambiar sus contraseñas.

Durante la fase 2 de la configuración del enlace de PPP, el NAS recopila los datos de autenticación y luego valida los datos contra su propia base de datos del usuario o contra un servidor central de base de datos de autenticación.

- **Fase 3: Control de Retorno de PPP.** En esta fase se utiliza el Protocolo de Control de Retorno de Llamada (CBCP) inmediatamente después de la fase de autenticación. Esto proporciona un nivel adicional de seguridad para las redes de marcación. NAS permite conexiones de clientes remotos que residen físicamente sólo en números telefónicos específicos.

- **Fase 4: Invocación de Protocolos de Nivel de Red.** Una vez que las fases anteriores se han completado, PPP invoca varios Protocolos de Control de Red (NCP) que son seleccionados durante la fase de establecimiento de enlace (Fase 1) para configurar protocolos usados por el cliente remoto.
- **Fase de transferencia de datos.** Una vez se han completado las cuatro fases de negociación, PPP empieza a transmitir datos hacia y desde las dos partes. Cada paquete de datos transmitido se encapsula en un encabezado de PPP que es eliminado por el sistema receptor. Si la compresión de datos se seleccionó en la fase 1 y se negoció en la fase 4 los datos serán comprimidos antes de la transmisión. Pero si se seleccionó y se negoció de manera similar la encriptación de datos, los datos (opcionalmente comprimidos) se encriptarán antes de la transmisión.

2.2.3 Protocolo de túnel de punto a punto.

PPTP [URL21] es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas del IP para transmisión sobre una red IP, como la de Internet. También se puede utilizar en una red privada de LAN a LAN. La mejor característica de PPTP radica en su habilidad para soportar protocolos no IP. El principal inconveniente de PPTP es su fallo a elegir una única encriptación y autentificación estándar.

PPTP utiliza una conexión TCP para mantenimiento del túnel y tramas de PPP encapsuladas con Encapsulación de Enrutamiento Genérico (GRE, *Generic Routing Encapsulation*) destinadas a los datos en el túnel. Se pueden encriptar y/o comprimir las cargas (*payloads*) de las tramas de PPP encapsulado.

La figura 2.11 muestra la forma en que se ensambla el paquete del PPTP antes de la transmisión (el cliente de marcación crea un túnel a través de una red). La trama final muestra la encapsulamiento para un cliente de marcación. PPTP encapsula los paquetes PPP en datagramas IP. Cuando llegan al servidor PPTP son desensamblados, para obtener el paquete PPP y desencriptados de acuerdo al protocolo de red transmitido. PPTP soporta los protocolos de red IP, IPX, y NetBEUI.

PPTP especifica una serie de mensajes de control con el fin de establecer, mantener y destruir el túnel PPTP. Los mensajes son transmitidos en paquetes de control en el interior de segmentos TCP. Los paquetes de control almacenan la cabecera IP, la cabecera TCP, el mensaje de control PPTP y los trailers apropiados.

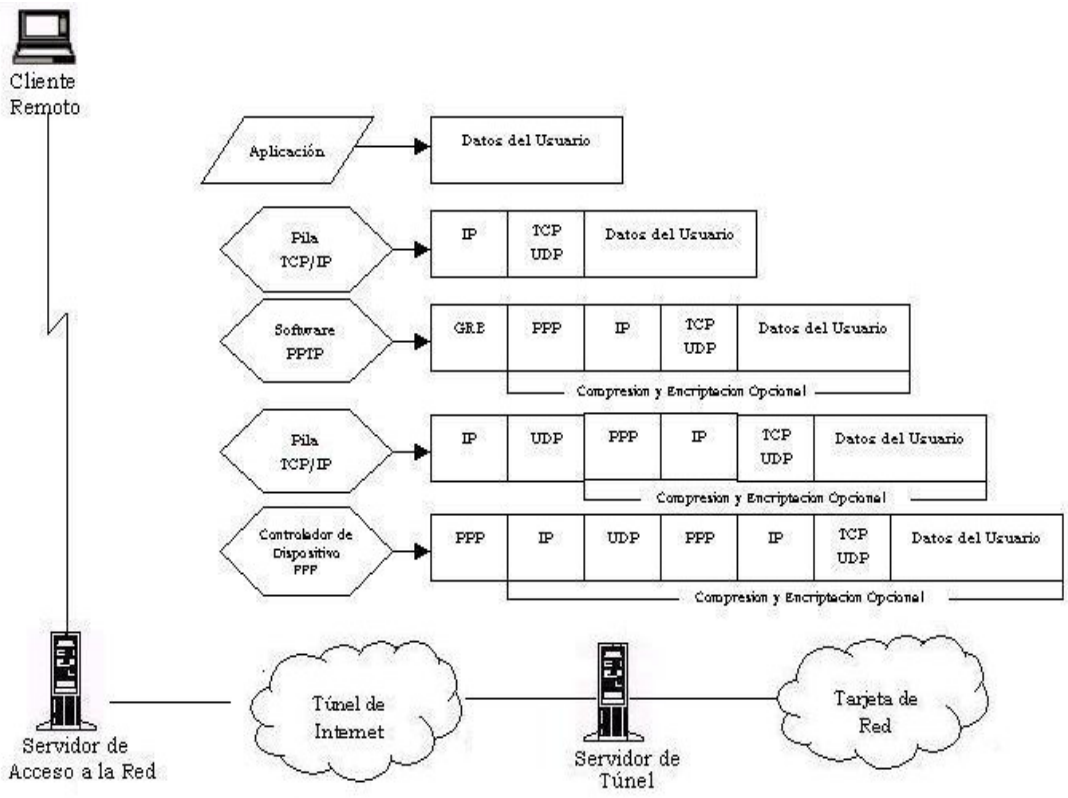


Figura 2.11 Construcción de un paquete PPTP.

La autenticación PPTP está basada en el sistema de acceso de Windows NT, en el cual todos los clientes deben proporcionar un par login/password. La autenticación remota de clientes PPTP es realizada empleando los mismos métodos de autenticación utilizados por cualquier otro tipo de servidor de acceso remoto (RAS).

PPTP utiliza el proceso de encriptación de datos de secreto compartido en el cual sólo los extremos de la conexión comparten la clave. La clave es generada empleando el estándar RSA RC-4 a partir del *password* del usuario. La longitud de la clave puede ser 128 bits (usuarios de EE. UU y Canadá) ó 40 bits (para los demás).

Además, puede defenderse a la red privada de un uso malintencionado habilitando el filtrado PPTP del servidor. El servidor acepta y enruta paquetes enviados por usuarios validados.

PPTP se complementa con el uso del *firewall*, que cubre otro tipo de seguridad. PPTP asegura la privacidad de los datos entre el cliente y el servidor a través de Internet. Combinado la seguridad del *firewall* (en la defensa de la red privada de paquetes extraños) y la del PPTP (respecto a la seguridad de los paquetes que llegan a la red, a través de la red pública Internet). [URL15], [URL22].

2.2.4 Transmisión de nivel 2.

L2F es una tecnología propuesta por Cisco, protocolo de transmisión que permite marcar a los servidores de acceso para empaquetar el tráfico de marcación en PPP y transmitirlo sobre enlaces WAN a un servidor L2F o router. El servidor L2F entonces desenvuelve los paquetes y los transmite a través de la red. A diferencia del PPTP y del L2TP, el L2F no tiene un cliente definido. L2F sólo funciona en túneles obligatorios [URL26].

2.2.5 Protocolo de la capa 2 de túnel.

Una combinación de las mejores características PPTP y L2F fue formada para crear L2TP. L2TP [URL37] es un protocolo de red que encapsula las tramas de PPP para enviarlas a través de redes de IP, X.25, *Frame Relay* o de modo de transferencia asíncrona (ATM) [URL23]. L2TP es un protocolo de Túnel de Nivel 2. L2TP al igual que PPTP soporta clientes no IP, pero da problemas al definir una encriptación estándar [URL24].

L2TP [URL37] encapsula datos de aplicación, datagramas de protocolos LAN e información de tramas punto a punto dentro de un paquete que, además contiene una cabecera de entrega, una cabecera IP y una cabecera GRE (*Generic Routing Encapsulation*). La cabecera de entrega mantiene la información de tramas para el medio a través del cual se establece el túnel. La cabecera IP contiene las direcciones IP de fuente y destino. GRE incluye extensiones como la de señalización de llamada, que añaden inteligencia de conexión.

L2TP no encripta los datos como parte de su administración de túnel, es capaz de transportar numerosos protocolos de Nivel IP, IPX, NetBEUI, etc. L2TP [URL37] ha sido definido para el uso sobre varios paquetes de media incluyendo PPP, X.25, *Frame Relay,* y ATM. Muchas implementaciones se enfocan al uso de UDP sobre IP.

La Figura 2.12 muestra cómo un paquete L2TP se forma antes de la transmisión. Se muestra a un cliente remoto que crea un túnel a través de una interred. La capa final de la trama muestra la encapsulación para el cliente (Controlador de Dispositivo PPP). La encapsulación asume L2TP [URL37] sobre IP.

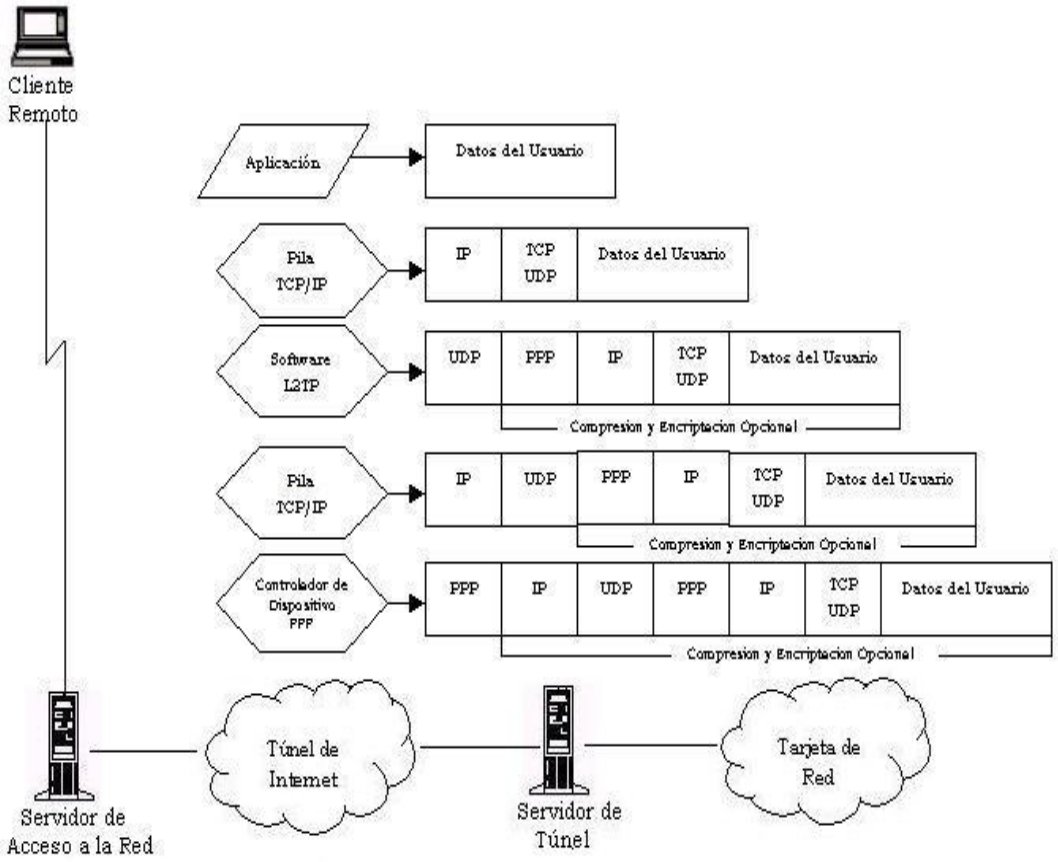


Figura 2.12 Paquete L2TP.

A. Elementos de una red L2TP.

Para formar un túnel, L2TP [URL37] emplea dos funciones básicas: LAC (Concentrador de acceso L2TP) y LNS (Servidor de red L2TP). LAC realiza funciones de servidor de línea para el cliente (figura 2.13), mientras que LNS actúa como servidor de red en el lado del servidor (figura 2.14).

Por ejemplo si L2TP reside en el LAC de un punto de presencia del operador, LAC iniciará un túnel cuando el usuario remoto active una conexión PPP con un proveedor de servicios Internet. Después de realizar la autenticación inicial, LAC acepta la llamada y añade las diferentes cabeceras comentadas a la carga útil de PPP, y establece un túnel hacia el dispositivo de terminación LNS del extremo de la red corporativa. El LNS puede ser un Servidor de Acceso Remoto, un Conmutador VPN especializado ó un *router* convencional.

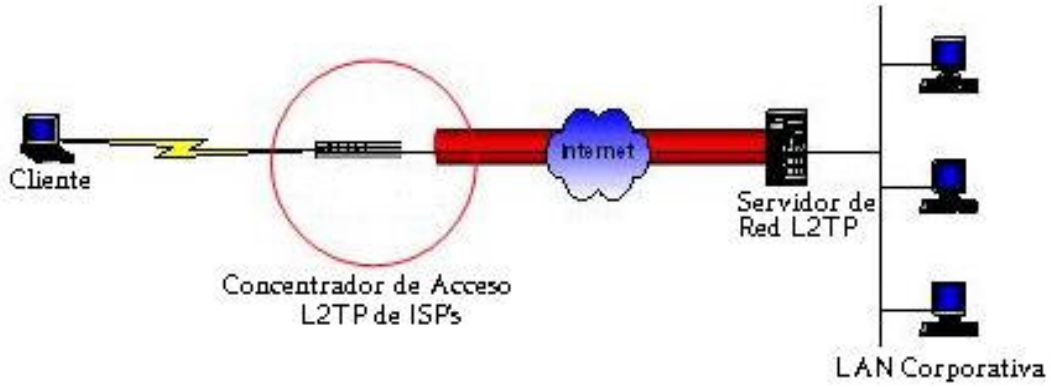


Figura 2.13 LAC.

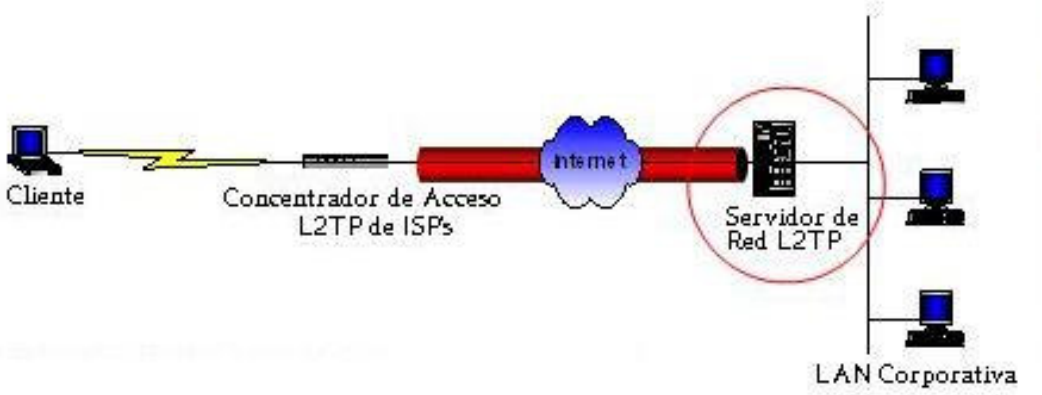


Figura 2.14 LNS.

Un **túnel obligatorio** existe entre una pareja de LAC/LNS. Y consiste de una conexión de control y cero o más sesiones L2TP. El túnel lleva datagramas encapsuladas PPP y mensajes de control entre el LAC y el LNS (figura 2.15).

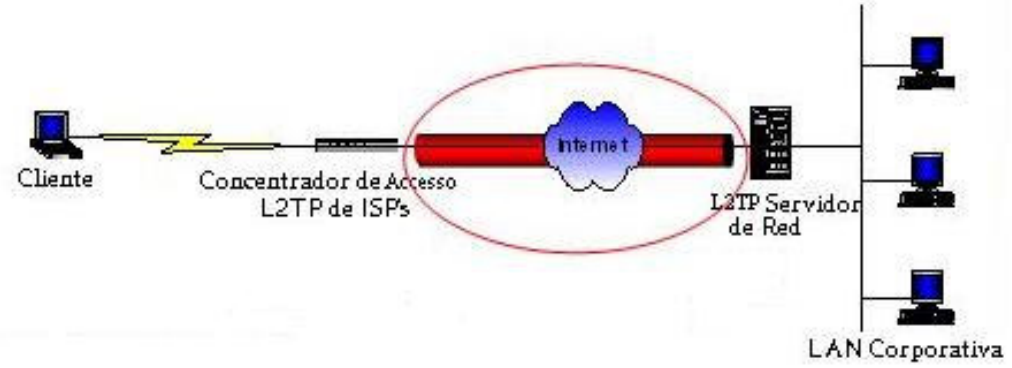


Figura 2.15 Túnel obligatorio.

Una computadora de usuario o del cliente puede emitir una solicitud *VPN* para configurar y crear un **túnel voluntario**. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel. Un *host* que corre L2TP puede participar en túnel para la LAN sin usar una LAC separada.

En este caso, el *host* contiene el software cliente LAC que ya ha sido conectada al Internet público. Una conexión PPP virtual es creada y el software LAC cliente del L2TP [URL37] local crea un túnel al LNS (figura 2.16). Este tipo de túneles voluntarios están demostrando ser el tipo más popular de túnel.

Una **Sesión L2TP** es creada entre el LAC y LNS cuando una conexión PPP extremo a extremo es establecida entre el sistema remoto y el LNS. (Figura 2.16) Los datagramas relacionados para la conexión PPP son enviados sobre un túnel entre el LAC y LNS.

Una vez establecido el túnel, un servicio de nombres de seguridad o el servicio de nombres y la seguridad integrada en Windows NT, se autentifica las identidades del usuario y del punto final. LNS acepta el túnel y establece una interfaz virtual para el *payload* PPP. A las tramas entrantes se les elimina la información de cabecera de L2TP y se les procesa como si fueran tramas PPP normales. Entonces se asigna a la sesión una dirección IP corporativa local. (Figura 2.17)

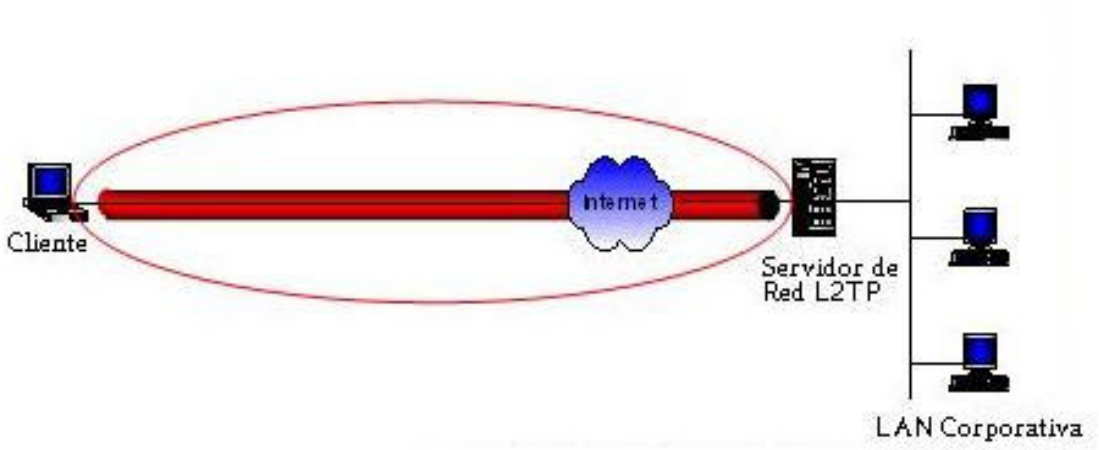


Figura 2.16 Túnel voluntario.

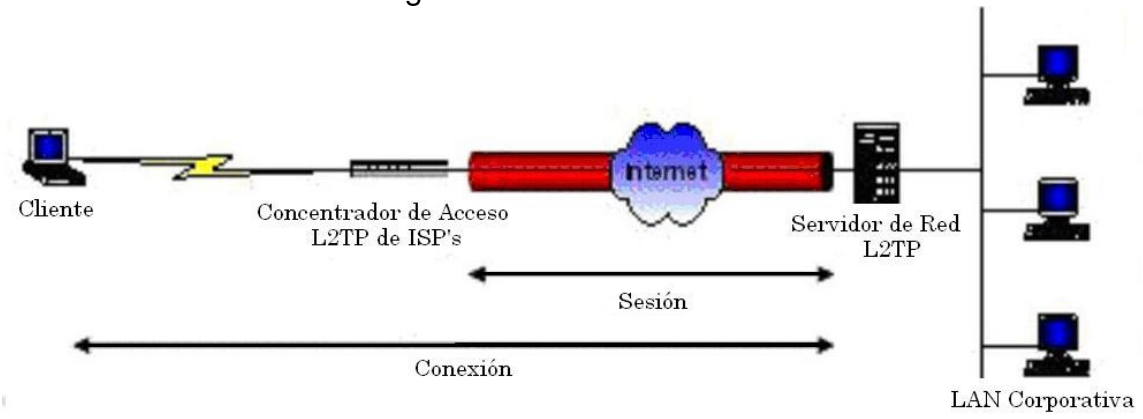


Figura 2.17 Sesión L2TP.

En el **Proceso L2TP** usa PPP para crear una conexión de marcación entre el cliente y el RAS. Estableciendo una conexión física, y se realiza una primera

autenticación, se crean datagramas PPP y se termina la conexión. Cuando se usa L2TP [URL37] para establecer un túnel, primero se encapsulan paquetes PPP para usar sobre un medio de transmisión, se Intercambian mensajes de control para instalar y mantener un túnel. Se crea una llamada ID y/o un identificador de túnel para cada sesión y se incluye en la cabecera de L2TP.

L2TP [URL37] junto con IPSec provee la funcionalidad y la protección que le hace falta, en la autenticación de paquete a paquete cuando salen de los túneles abiertos haciéndolos vulnerables a ataques como fisgoneos, modificación de datos y secuestro de sesiones. L2TP incluye un túnel identificador para cada túnel individual y así puede ser identificado desde una sola fuente (Fig. 2.18).

PPP define un mecanismo de encapsulación para transportación de paquetes de multiprotocolos a través del Nivel 2 con enlaces de punto a punto. Un beneficio obvio de cada separación es que en lugar de requerir la conexión de Nivel 2 terminada del NAS (requiere un cargo de larga distancia) la conexión quizá termine con un circuito concentrador local, el cual extiende la sesión lógica PPP sobre una infraestructura compartida, el cual es un Circuito *Frame Relay* o de Internet. Desde la perspectiva del usuario no hay una diferencia funcional entre el circuito de Nivel 2 terminado en un NAS directamente o usando L2TP [URL37] [URL21].

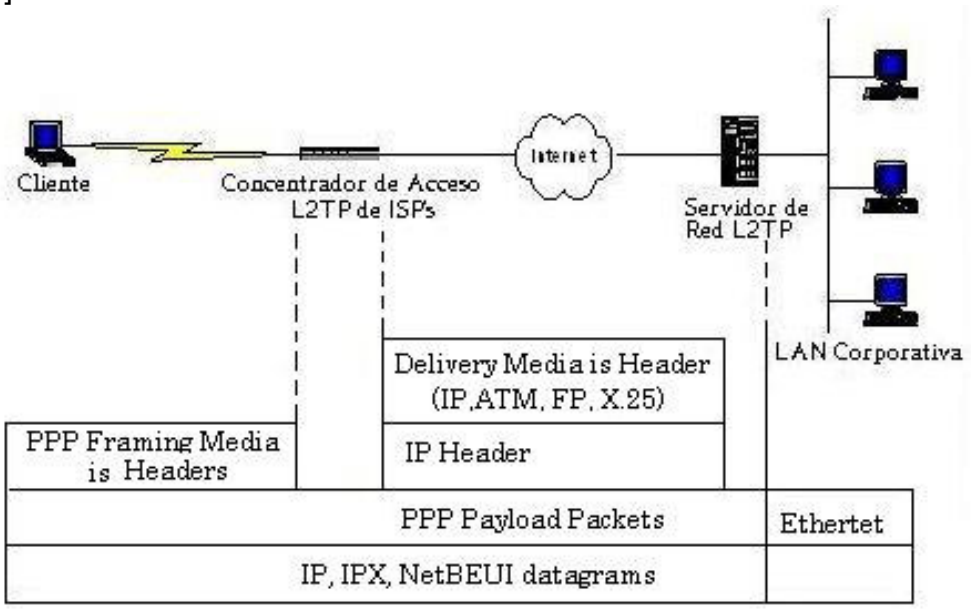


Figura 2.18 Proceso L2TP.

B. Fases de la Autenticación L2TP.

☙ **Fase 1.** Un ISP autentifica una llamada a un número telefónico, el número llamado, o nombre de usuario para determinar o no, si el servicio L2TP [URL37] es requerido.

- **Fase 2.** El Servidor de la red corporativa decide o no, aceptar la llamada, basada en CHAP, PAP, EAP u otra información de autenticación desde el ISP.
- **Fase 3.** Después la llamada es aceptada, el servidor de red puede inicializar otra fase de autenticación para el nivel PPP.

C. PPTP y L2TP.

Tanto PPTP y L2TP [URL37] usan PPP para mantener un nivel inicial de los datos, y luego incluir encabezados adicionales para transportarse a través de la interred. Ambos protocolos son similares, pero existen diferencias.

PPTP requiere que la interred sea de tipo IP, y L2TP requiere que los medios de comunicación del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (uso de UDP), Circuitos Virtuales Permanentes (PVCs), Circuitos Virtuales X.25 (VCs), o ATM VCs. PPTP sólo puede soportar un sencillo túnel entre los puntos terminales.

L2TP [URL37] permite el uso de múltiples túneles entre los puntos terminales y se pueden crear diferentes túneles para diferentes calidades de servicio. Proporciona la compresión de encabezados. Cuando la compresión se habilita L2TP opera con 4 bytes adicionales, y PPTP con 6 bytes. L2TP proporciona la autenticación de túnel, mientras PPTP no lo hace.

Cuando se utiliza cualquier protocolo sobre IPSec, se proporciona la autenticación del túnel por IPSec.

2.2.6 Protocolo de seguridad de Internet.

IPsec es una colección de múltiples protocolos relacionados. Es usado como una solución completa de protocolo VPN ó simplemente como un esquema de encriptación para L2TP o PPTP. IPsec es un protocolo de túnel de nivel 3. Válido para IPv4 como IPv6, permite definir los protocolos de seguridad, los algoritmos criptográficos y las claves manejadas entre los sistemas que se comunican.

IPSec soporta la transferencia protegida de información a través de una interred IP, y define el formato del paquete para un IP sobre un modo de túnel IP, generalmente llamado como Modo de túnel IPSec. Un túnel IPSec consiste en un cliente del túnel y servidor del túnel, ambos configurados para usar los túneles IPSec y un mecanismo de encriptación negociado.

El modo de túnel IPSec usa el método de seguridad negociado para encapsular y encriptar los paquetes IP, para una transferencia segura por una interred IP privada o pública. Así el *payload* encriptado se encapsula con un encabezado IP de texto y se envía en la interred para la entrega al servidor del túnel. Al recibir este datagrama, el servidor del túnel procesa y descarta el encabezado IP de texto y luego desencripta su contenido, para recuperar del

paquete el *payload* original IP. Enseguida se procesa el paquete de *Payload* de IP de manera normal y se enruta a su destino en la red designada.

El **Modo de Túnel IPSec** soporta solamente trafico IP, funciona al fondo de la pila IP. Es controlado por una política de seguridad que establece los mecanismos de encriptación y del túnel disponible en orden preferencial así como los métodos de autenticación disponibles. .

Una de las características más importantes de IPSec es su compatibilidad con las redes IP actuales. IPSec puede dividirse básicamente en mecanismos de gestión de claves, mecanismo de creación de asociaciones seguras y algoritmos criptográficos para autenticación y cifrado. Estos servicios son provistos de IP de nivel 2 y ofrecen protección para IP y para los protocolos de niveles superiores [URL15].

Los protocolos de seguridad definen la información que se ha de añadir a la cabecera de un paquete IP para proporcionar los servicios de seguridad requeridos (AH y ESP).

La gestión de claves puede ser manual o automática. La gestión automática de claves se realiza mediante IKE (*Internal Key Exchange*). Los mecanismos criptográficos que emplea IPSec son el intercambio de claves basado en el algoritmo Diffie-Hellman, criptografía de clave público, algoritmos simétricos de cifrado de datos (DES, IDEA...), algoritmos *hash* con clave (HMAC), y otros más tradicionales (MD5 y SHA), para proporcionar autenticación de paquetes, y manejo de certificados digitales.

IPSec combina estos mecanismos criptográficos para ofrecer confidencialidad, integridad y autenticidad a los datagramas IP. IPSec no define los algoritmos específicos a utilizar, sino que proporciona un mecanismo para que las entidades negocien aquellos que emplearán en su comunicación.

A. Cabeceras IPSec.

IPSec hace uso de dos cabeceras: la cabecera de Autenticación (AH, *Authentication Header*) para autenticar usuarios y la Carga de Encripcion Segura (ESP, *Encryption Security Payload*) para proveer confidencialidad. Esas nuevas cabeceras se colocan después de la cabecera IP y antes de la de nivel de transporte.

La autenticación permite un sistema final o dispositivo de red para autenticar a usuarios y filtros correspondientes. Ayuda en la prevención de los ataques de redes basadas en el *spoofing* o reproducción. La autenticación se realiza basándose en un secreto compartido.

Algunas formas son: criptografía de clave pública, firma digital, MPPE (protocolo que sirve para encriptar los datos de las transmisiones), MSCHAP v1. y

v2. (sirve para establecer la conexión segura y el intercambio de las claves), IPIP(protocolo de encapsulamiento de IP sobre tramas IP, y sirve para hacer el túnel que se marca como uno de los requisitos de VPN), IP-GRE (protocolo de encapsulamiento de otros protocolos sobre IP, útil en el que se tienen redes de otro tipo además de IP y funcionar con una VPN), y SOCKS (proporciona otra alternativa a los protocolos de VPN se aloja en el Nivel de Sesión de OSI, permite a los administradores limitar el tráfico VPN).

B. Modos de IPSec.

Las especificaciones IPSec en perfil de AH y ESP son aplicadas de dos maneras llamados Modos:

- El **Modo de Transporte.** La protección es permitida para el Nivel de Transporte para el paquete y porciones seleccionadas de la cabecera IP. Este modo es utilizado entre los dispositivos finales de una comunicación que cumplen el estándar IPSec. Empleado en ambos *hosts* ó en la configuración de *gateways*. La dirección fuente y destino IP pueden ser abiertas para algunas formas de ataque.
- El **Modo de Túnel.** La protección es permitida para el paquete original entero IP para la pre-espera de la cabecera original IP con una nueva. Este modo permite que un dispositivo actúe como proxy IPSec en beneficio de máquinas que no soporten el estándar.

IPSec requiere varias combinaciones de Transporte y Modos de Túnel para maximizar la seguridad. El aplicar AH (Fig. 2.19) ó ESP (Fig. 2.20) en Modo de Túnel para autenticar/encriptar el dato original IP, y/o el aplicar AH (Fig. 2.21) ó ESP (Fig. 2.22) en Modo de Transporte para proteger la recién cabecera generada. En Modo de transporte IPSec usa IP tipo 51 para AH y usa IP tipo 50 para ESP.

Los dos sistemas comunicantes deben estar de acuerdo en los algoritmos que se usarán, así como en la clave de sesión que han de compartir. Una vez realizado este proceso se ha creado una asociación segura (SA) entre las dos entidades. Durante este proceso se crea un túnel seguro entre los dos sistemas y se negocia la SA para IPSec.

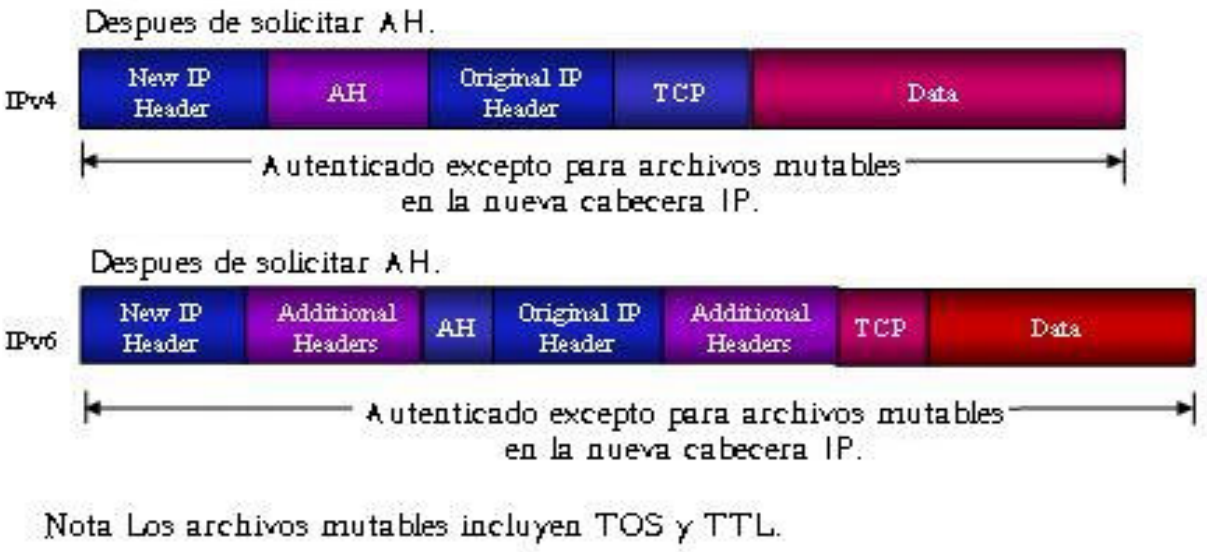


Figura 2.19 Autenticando AH en modo de túnel.

Figura 2.20 Asegurando la carga encapsulada con ESP.

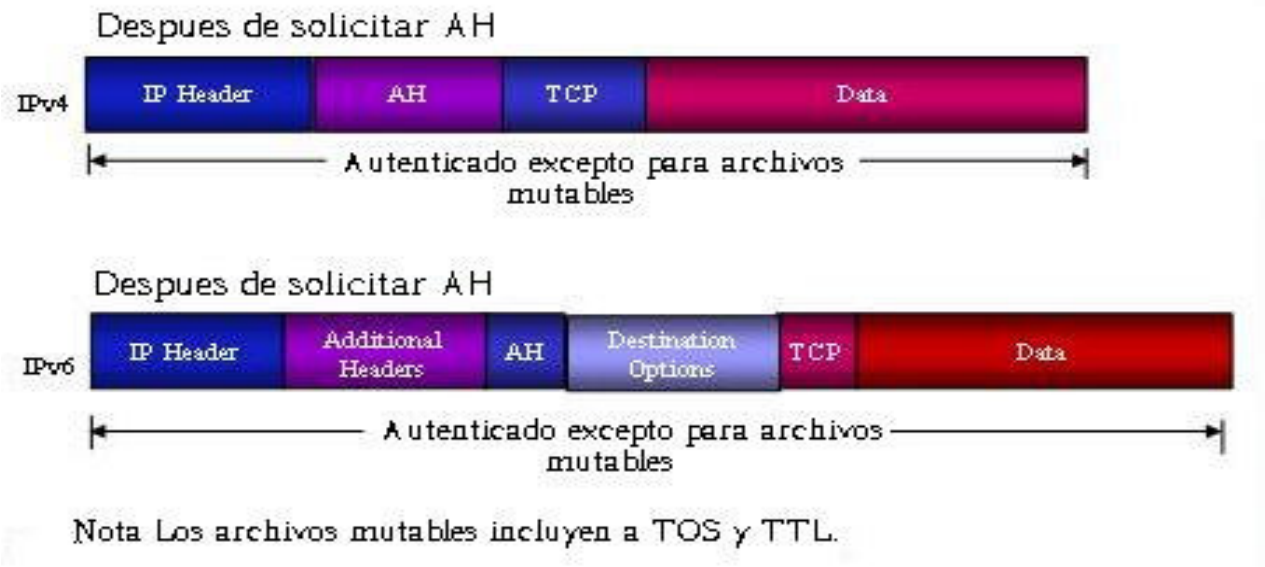


Figura 2.21 Autenticando AH en modo de transporte.

C. Administración de Comunicaciones Seguras.

Los servicios de seguridad que provee IPSec dependen de valores secretos compartidos o llaves que pueden ser implementadas antes de asegurar las comunicaciones que pueden tomar. Las dos partes deben tener reglas bien definidas para intercambiar información. Estas reglas son definidas con una Asociación Segura (SA) que pertenece a los parámetros requeridos para la autenticación y encripción en ambos modos de transporte y túnel.

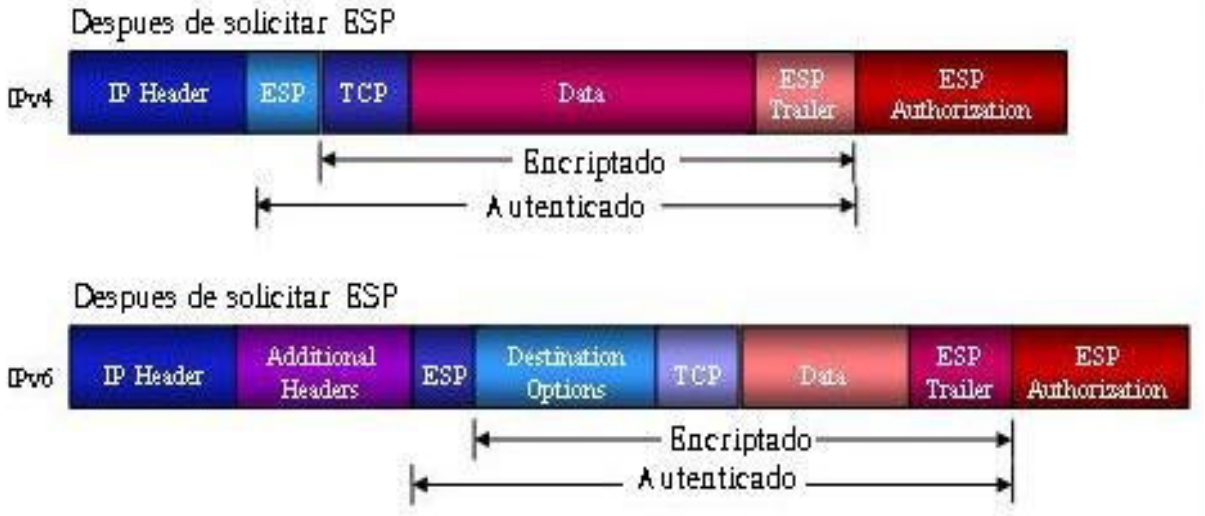


Figura 2.22 Asegurando la carga encapsulada con ESP.

D. Asociación de Seguridad.

Una SA, es una manera de relación entre un remitente y un destinatario que permite servicios de seguridad para el trafico que porta en el. Si se requiere seguridad bidireccional, un SA es requerido para cada dirección. Los servicios de seguridad son permitidos para un SA usar AH ó ESP, pero no ambas. Un SA se identifica por tres parámetros:

- **Parámetro de SPI.** Una serie de bits permiten que una estación receptora para seleccionar el apropiado SA con el cual se procesa el paquete.
- **Dirección de destino IP**. Es la dirección de destino IP de un punto final del SA.
- **Protocolo identificador de Seguridad.** Indica si el SA es para AH o ESP.

Una SA es una relación que existe entre dos estaciones. Cuando las estaciones accesan a estos atributos, se hace referencia al SPI que sirve como un punto a SA. Estas entidades pueden ser cualquier *host* o pasarela. Las conexiones pueden existir entre dos pasarelas. Estas conexiones pueden existir en dos modos (transporte o túnel).

En el **Modo de Transporte**, la SA es una conexión que existe entre dos *hosts*. En este Modo si se usa AH la protección permite todos los protocolos por encima del nivel IP, y el seleccionar partes de la cabecera IP. Al usar ESP se provee protección sólo para estos protocolos por encima del nivel IP.

En Modo de Túnel, una nueva cabecera IP exterior es agregada a los datos para ser transmitidos entre dos estaciones. La cabecera IP externa especifica la pasarela responsable para procesar el tráfico, mientras la cabecera interna especifica el destino final. Cuando se emplea AH, la protección es permitida sobre todos los protocolos de Nivel IP y también selecciona partes de la cabecera IP. Cuando se usa ESP solo la cabecera IP interna es protegida.

Cuando el final es una conexión *gateway*, las conexiones deben ser en Modo de Túnel. Tantas conexiones entre dos pasarelas ó entre un *host* y un *gateway* existen en modo de túnel. La excepción de la regla es, si el *gateway* es el destino final de los datos en caso que el *gateway* este actuando como un *host*. En este caso se empleará el Modo de Transporte.

2.3 Arquitectura de seguridad de VPN.

La Arquitectura de Seguridad en VPNs se debe basar en elementos esenciales de la tecnología para proteger la privacidad, mantener la calidad y confiabilidad, y asegurar la operatoria de la red en toda la empresa.

Las VPNs usan varios procedimientos criptográficos para autenticar usuarios y asegurar los datos privados [URL21].

Varios protocolos han sido desarrollados para proveer:

- **Confidencialidad:** los mensajes pueden solo ser leídos para envíos y recepción.
- **Autenticación:** los mensajes son de un origen esperado.
- **Autorización:** A los usuarios se les permite el acceso a varios recursos e la red.
- **Integridad:** Los mensajes no son alterados en el camino
- **Denegación:** El origen no puede denegar la creación del mensaje.

Estos protocolos hacen uso de llaves (*keys*) compartidas para proteger los datos. Las llaves proveen:

- **Seguridad:** como el uso de túneles, encriptación de datos, autenticación de usuarios y paquetes, control de acceso.
- La **Calidad de Servicio:** en uso de colas, manejo de congestión de red, priorización de tráfico, clasificación de paquetes.
- La **Gestión:** en implementación y mantenimiento de las políticas de seguridad y calidad de servicio a lo largo de la VPN.

El Internet facilita la creación de VPNs desde cualquier lugar. Por tanto, las redes necesitan características fuertes en seguridad para prevenir accesos no deseados a las redes privadas y protección a datos privados cuando cruzan por la red pública. Para lograr esto, se fortalece la autenticación y las capacidades de encriptación disponibles con EAP e IPSec.

2.3.1 Encriptación simétrica vs. Encriptación asimétrica.

La **Encriptación Simétrica**, ó llaves privadas (conocida como encriptación convencional), se basa en una llave secreta que es compartida por ambas partes de la comunicación. La parte que transmite utiliza la clave o llave secreta como parte de la operación matemática para encriptar (cifrar) texto plano en texto codificado. La parte receptora utiliza la misma clave secreta para decodificar (descifrar) el texto codificado en texto plano (Figura 2.23).

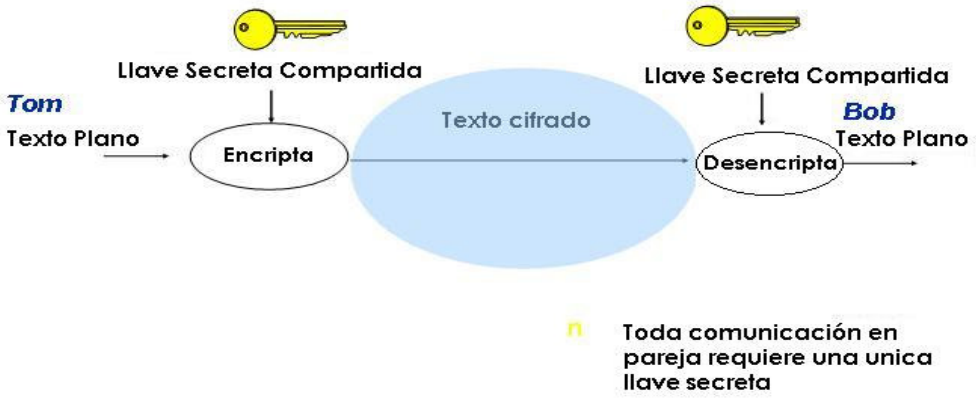


Figura 2.23 Llave simétrica.

La **Encriptación Asimétrica** ó llaves públicas utilizan dos diferentes llaves para cada usuario. Una llave es privada y conocida sólo por el usuario. La otra es, una llave pública que es accesible a cualquiera. Las llaves privada y pública están matemáticamente relacionadas por un algoritmo de codificación. Una llave se utiliza para codificación y la otra para decodificar, dependiendo de la naturaleza del servicio de comunicación que se esté implementando (Figura 2.24).

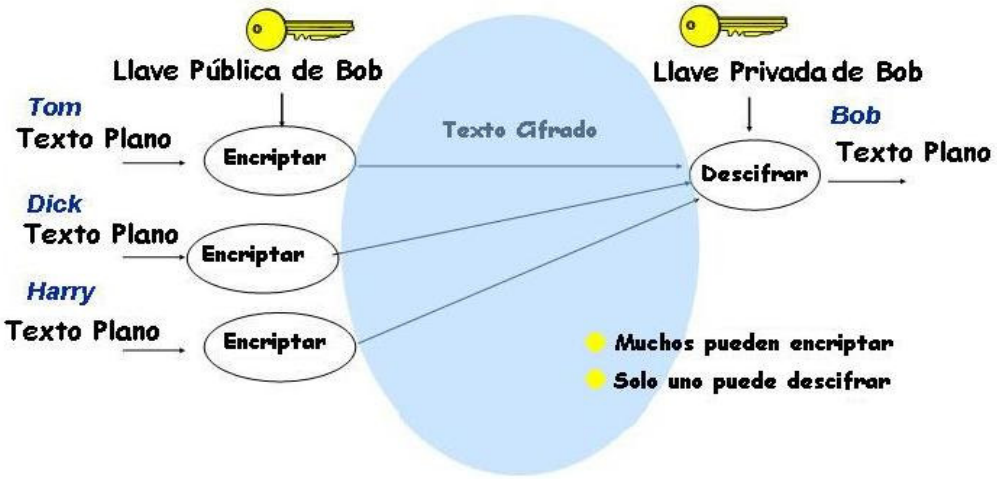


Figura 2.24 Llave asimétrica, encriptación y desencriptación.

Las tecnologías de codificación de llaves públicas permiten que las firmas digitales se coloquen en los mensajes. Una firma digital utiliza la llave privada del que envía el mensaje para codificar parte del mismo. Cuando el mensaje es recibido, el receptor utiliza la clave pública del transmisor para descifrar la firma digital como una forma de verificar la identidad del transmisor.

A. Encriptación estándar de datos.

DES, es un algoritmo simétrico que provee una fuerte encriptación. Requiere que ambas partes de la comunicación compartan una llave común. La llave es de 64 bits, 56 bits usados para encriptación y los otros 8 bits son para el chequeo de paridad.

La encriptación es realizada para hacer unas series de iteraciones complejas, operadas en bloques de 64 bits de datos en el momento.

El algoritmo Lucifer desarrollado por IBM, usa una llave larga igual que DES, haciéndolo más seguro. Por la intervención de *National Security Agency*(NSA), la llave fue limitada a 56 bits para proveer una fuerte encriptación para corporaciones y usuarios.

Hay dos escuelas pensadas con respecto a una fuerte encriptación:

☙ La primera es que el usuario tenga una correcta privacidad, sin estimación como para que este siendo ocultada.

☙ La segunda es, que se necesita privacidad para mirarla de frente en seguridad y legalidad.

Ambas escuelas tienen sus meritos y el debate es continuo (figura 2.25).

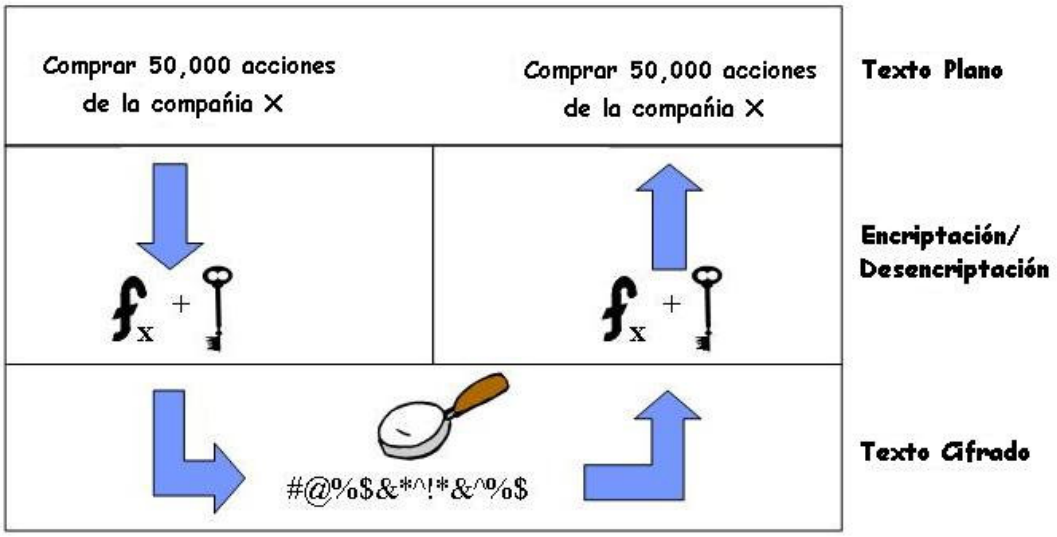


Figura 2.25 Encriptación básica.

B. Función *Hash*.

La función *hash* es un algoritmo que toma un mensaje de largo arbitrario y produce una compleja salida larga conocida como un *fingerprint* ó mensaje digerido.

Es imposible considerar que puede producir dos mensajes con el mismo mensaje digerido, o produzca cualquier mensaje teniendo un predeterminado resumen.

Las funciones *Hash* son usadas en aplicaciones de las firmas digitales para comprimir largas sumas de datos antes de la encriptación con una llave privada (secreta) (Figura 2.26).

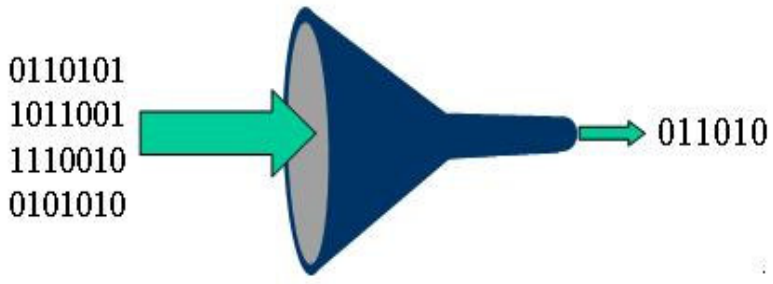


Figura 2.26 Algoritmo Hash.

Las Funciones *Hash* más comunes usadas en la criptografía de llaves públicas incluyen: MD-2 –128bits *hash*, MD-5 – 128 bits *hash*, SHA-1-160 bit *hash*. Estos algoritmos son colisiones relativamente libres, esto significa que es improbable que dos mensajes separados al ser limpiados tengan el mismo *fingerprint.*

Ha habido algunos ataques desarrollados por MD-2 que quizá produzcan una colisión. En este punto, la suma del chequeo es el último obstáculo que frustra el ataque. MD-2 no es recomendado. MD-5 es también sujeto de muchas discusiones. SHA-1 es el más fuerte de las funciones *Hash* y es recomendado por la documentación X.509.

Desarrollos adicionales por IBM, han introducido el concepto de combinar múltiples pasos del algoritmo *hash* mientras se agregan textos secretos a las llaves, es una aprobación conocida como HMAC.

2.3.2 Certificados.

Con la encriptación o **codificación simétrica**, el transmisor y el receptor tienen una clave secreta compartida. La distribución de la clave secreta debe hacerse antes de cualquier comunicación codificada.

Con la **codificación asimétrica** el transmisor utiliza una clave privada para codificar o firmar digitalmente mensajes, mientras que el receptor utiliza una clave pública para descifrar estos mensajes. La clave pública puede distribuirse libremente a cualquiera que necesite recibir los mensajes codificados o con firma digital. El transmisor sólo necesita proteger cuidadosamente la clave privada.

Para asegurar la integridad de la clave pública, se pública con un certificado el cual es una estructura de datos firmada digitalmente por una autoridad de certificación, en la cual los usuarios del certificado pueden confiar. Este certificado contiene el Nombre y Uso del Certificado, información que identifica al propietario de la clave pública, la clave pública en sí, una fecha de expiración y el nombre de la utilidad de certificación. La autoridad de certificación utiliza su clave privada para firmar el certificado. Si el receptor conoce la clave pública de la autoridad de certificación, entonces puede verificar que el certificado es en realidad confiable y, por lo tanto, contiene información segura y una clave pública válida.

2.3.3 Protocolo de autentificación extensible.

EAP es una extensión propuesta por la IETF para el PPP que permite que los mecanismos de autenticación arbitraria se utilicen para la validación de una conexión de PPP. Diseñado para permitir la adición dinámica de módulos de conexión de autenticación en ambos extremos de clientes y de servidor de una conexión, permitiendo a los distribuidores proveer un nuevo esquema de autenticación en cualquier momento, proporcionando la flexibilidad más alta en particularidad y variación de autenticación.

2.3.4 Seguridad de nivel de operaciones.

Con el EAP-TLS, un cliente presenta un certificado de usuario al servidor de marcación, al tiempo que el servidor presenta un certificado de servidor al cliente. El primero proporciona autenticación sólida de usuario al servidor y el segundo certeza de que el usuario ha contactado el servidor que esperaba. Ambos sistemas se basan en una cadena de autoridades confiables para verificar la validez del certificado ofrecido.

El certificado del usuario puede almacenarse en la PC de cliente de marcación o en una tarjeta inteligente externa. Y este certificado no puede ser accesado sin alguna forma de identificación de usuario entre el usuario y la PC del cliente.

2.3.5 Seguridad del protocolo de Internet.

IPSec es un mecanismo Punto a Punto que certifica la confiabilidad de los datos en comunicaciones basadas en IP. IPSec ha sido definido en una serie de RFC's (1825, 1826, 1827), que definen: una Arquitectura Global, un Encabezado de Autenticación para verificar la integridad de datos y una Encapsulación segura de cargas para la integración de ambos datos y la Encripción de los mismos.

IPSec define dos funciones que aseguran la confidencialidad: la encriptación de datos y la integridad de datos. IPSec usa un encabezado de Autenticación (AH) para proporcionar fuentes de autenticación e integridad sin encriptación, y la Carga Segura Encapsulada (ESP) que proporciona la autenticación e integridad junto con encriptación. Con IPSec sólo el remitente y destinatario saben la llave de seguridad. Si los datos de la autenticación son válidos, el destinatario sabe que la comunicación vino del remitente, y que no cambió en el camino.

IPSec puede visualizarse como una capa debajo de la pila de TCP/IP. Esta capa es controlada por una política de seguridad en cada máquina y una asociación de seguridad negociada entre el remitente y receptor. La política consiste en un conjunto de filtros y las conductas de seguridad asociadas. Si los paquetes tienen una dirección IP, protocolo y número de puerto, esto se iguala a un filtro y entonces el paquete esta sujeto a la conducta de seguridad asociada.

A. Asociación de seguridad negociada.

ISAKMP/Oakley es el protocolo estándar para realizar una asociación de seguridad entre el transmisor y el receptor. Durante un intercambio las dos máquinas acuerdan los métodos de autenticación y seguridad de datos, realizan una autenticación mutua y después generan una clave compartida para la codificación de datos subsecuente.

Después de establecer la asociación de seguridad, la transmisión de datos puede proceder para cada máquina aplicando tratamiento de seguridad de datos a los paquetes que transmite al receptor remoto. El tratamiento puede simplemente asegurar la integridad de los datos transmitidos o puede codificarlos también.

B. Encabezado de Autenticación.

La integridad de los datos y autenticación de los datos para cargas IP pueden ser proporcionadas por AH localizado entre el encabezado IP y el encabezado de transporte. AH incluye la autenticación de los datos y un número secuencial, que juntos se utilizan para verificar al remitente, asegurando que el mensaje no ha sido modificado en el camino, y previene un ataque de reproducción.

El AH de IPSec no proporciona ninguna encriptación de datos; pueden enviarse mensajes del texto claros y AH asegura que se originaron de un usuario específico y no se modificaron en el camino.

C. Seguridad en el encabezado de Encapsulación.

Para ambos, la confidencialidad y protección de los datos de una tercera parte, ESP proporciona un mecanismo para encriptar la carga IP. ESP proporciona autenticación de los datos y servicios de integridad de datos; por consiguiente los encabezados de ESP son una alternativa para los encabezados AH en paquetes de IPSec.

D. La política de seguridad IPSec en Bases de Datos.

El trafico IP es relacionado para especificar SAs ó permitir el desvío SA basado en la información contenida en la política de seguridad de bases de datos (SPD, *Security Policy Database*). El SPD contiene información que define un subconjunto del tráfico IP que debe procesarse acorde a las especificaciones SA. Cada entrada SPD es definida por un conjunto de valores llamados selectores.

Los valores de los selectores SPD son: Protocolo IPSec, puertos fuente y destino, clase IPv6, flujo de la etiqueta IPv6, Tipo de Servicio IPv4, Dirección destino IP, Dirección fuente IP, ID de Usuario, Nivel de Sensibilidad de datos, Protocolo de Nivel de Transporte.

La SA usa dos bases de datos: la Política de Seguridad en Bases de Datos y la Asociación de Seguridad en Bases de Datos.

La SPD especifica los servicios de seguridad que son proporcionados por paquetes IP. Esta base de datos contiene una lista ordenada de políticas de entrada. Cada entrada incluye información acerca del tipo de paquete, la política se aplicara, tal que las direcciones fuente y destino. Una política de entrada

IPSec, también incluirá una lista de especificaciones SA de protocolos IPSec, el modo (túnel o transporte) y la seguridad de algoritmos a emplear.

El SPD define los parámetros asociados con cada SA. Cada SA tiene una entrada en el SPD. Cada especificación SA en el SPD apunta a un SA, o paquete de SAs, en el SPD.

E. Creando una SA IPSec.

La Arquitectura de Seguridad IPSec ofrece dos estrategias para crear SAs y distribuir las llaves requeridas para la autenticación y encripción [URL22], [URL25].

Estas incluyen:

- **Llave manual**. Los nodos de comunicación son configurados con material de claves apropiado y la administración de datos SA.
- **Administración de llaves automatizadas.** Una técnica de administración de llave automatizada se usa para crear y distribuir llaves.

La arquitectura de seguridad IPSec especifica la Asociación de Seguridad de Internet y Protocolo de Administración de llaves ISAKMP/Oakley ó Llave de Intercambio de Internet (IKE, *Internet Key Exchange*), pero otros algoritmos de llaves públicas pueden ser empleados. Ambos métodos son requisitos obligatorios de IPSec.

IPSec especifica a IKE para una administración de llave automática. Otros algoritmos de llave pública que son definidos incluyen Kerberos y SKIP.

Para la **llave Manual** con IPsec, se necesitan tomar en cuanta determinar los tipos de llaves requeridos y sus asociaciones de usuarios, un método de seguridad para crear y almacenar las llaves requeridas, y un significado de seguridad en la distribución de llaves.

Sus métodos de distribución son por Documentos, Media removible y el Acoplo de hardware. La seguridad de llaves es fundamental para la seguridad total de la red.

Cuando se construye una VPN usando llaves manuales, es importante considerar los tipos de llaves que son usadas, como se crearan, se almacenarán y serán distribuidas. Se requieren métodos apropiados para cada paso ó la seguridad de red puede ser comprometida.

Las llaves manuales pueden ser distribuidas por discusión, por media removible y acoplación. El usuario final no tiene que darse cuenta del contenido de

discos, así es menos probable para una clave poner en peligro, el disco puede fácilmente ser destruido.

La acoplación de hardware es única para un sistema particular de hardware y los usuarios restringidos con llaves vistas, pares de llaves autenticadas y provee seguridad al almacenarse durante la distribución, pero no es un método común. Las llaves manuales con un formato sugerido es el orden para facilitar la distribución de llaves manuales.

Para las **llaves Automatizadas** con IPSec se necesita proveer un significado para el cual dos estaciones de comunicación pueden negociar protocolos, algoritmos y llaves. Provean un significado del cual dos partes pueden ser autenticadas, con un canal seguro sobre el cual las llaves puedan ser intercambiadas y se administren las llaves una vez han sido acordadas. El método de distribución es por el Intercambio de Laves de Internet (IKE).

IPSec especifica a IKE como un medio predeterminado de negociación automática en SA. IKE evoluciona fuera de dos protocolos separados llamados:

- **ISAKMP** *(Internet Security Association and Key Management Protocol*). Define dos fases que sirven como una estructura para la autenticación y el intercambio de llaves:

  - Fase I: Dos partes establecen una ISAKMP SA (un canal seguro para llevar a cabo operaciones ISAKMP).
  - Fase II: Las dos partes negocian un propósito general SA (el SA que será usado para subsecuentes comunicaciones).

- **Protocolo Oakley.** Describe varios modos o intercambio de llaves:

  - **Modo principal**. Usado en la fase I ISAKMP intercambia para crear un canal seguro.
  - **Modo Agresivo.** Usado en la fase II ISAKMP intercambia (similar al modo principal) sin identificar la protección para la negociación de nodos.
  - **Modo Rápido**. Usado en la fase III ISAKMP intercambia para negociar un propósito general SA para comunicaciones subsecuentes.
  - **Modo Grupo Nuevo**. Sigue una fase I ISAKMP intercambia y es incluido como un medio para definir grupos privados para un Intercambio Diffie-Hellman.

El modo principal (figura 2.27) realiza la primera Fase I de Intercambio ISAKMP. Un modo principal de intercambio usa 3 maneras de intercambio, cada una de las cuales es precedida por la cabecera que identifica el paso a tomar. En el primer intercambio (1-2), las dos partes determinan los algoritmos básicos, los *hashes*, y las funciones. En el segundo intercambio (3-4), pasan información pública que será usada para un intercambio *Diffie-Hellman-Merkle* como los

nonces (un valor aleatorio usado para derrotar ataques repetidos). En la tercera fase (5-6), las identidades son verificadas y el proceso es completado.

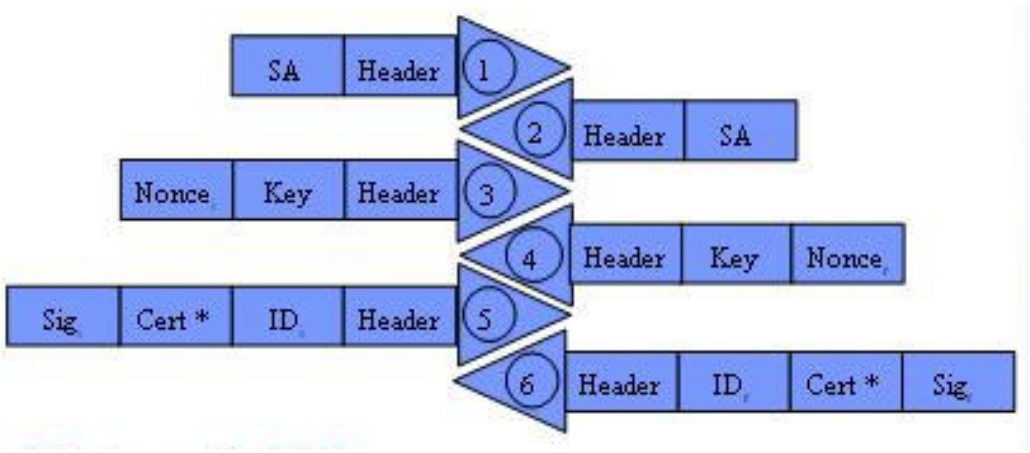


Figura 2.27 Modo principal.

Un **modo agresivo** (figura 2.28) puede usarse para conseguir una Fase I de intercambio ISAKMP. Es similar al modo principal sin embargo, el modo agresivo consigue iniciar una SA usando solamente tres intercambios de paquetes y un viaje redondo. La principal diferencia es que el modo agresivo no provee protección de identidad para la comunicación de las partes.

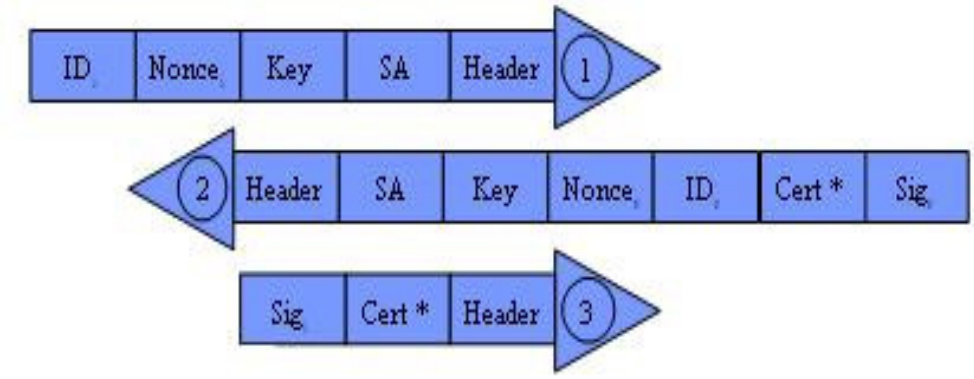


Figura 2.28 Ejemplo de modo agresivo.

El **modo rápido** (figura 2.29) es usado, después de cualquier modo principal o agresivo. Se emplea para construir el inicial ISAKMP de la Fase I en SA, para establecer un propósito general SA que será usada para comunicaciones subsecuentes. Usando el modo rápido, las dos partes pueden elegir continuar el uso de SA que usará en la Fase I de Negación. O, si la seguridad perfecta es requerida, nuevos materiales de llaves pueden ser generados y pasados sobre un túnel seguro.

Una PKI (*Public Key Infrastructure*) define los servicios de seguridad que hacen posible hacer:

- Interactuar con una autoridad de certificado.
- Generar, distribuir y administrar llaves públicas.
- Numerar, validar, y revocar certificados digitales.

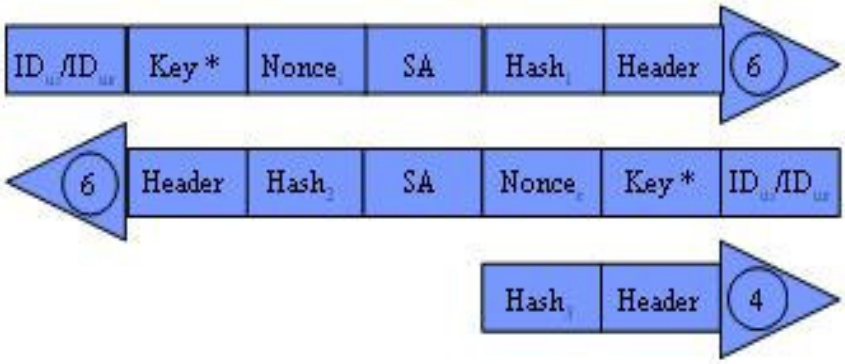


Figura 2.29 Ejemplo de modo rápido.

Sin algún tipo de PKI, la distribución y mantenimiento de llaves públicas y certificados usados para muchas implementaciones VPN serán inmensamente complicados y compromiso potencial de seguridad de una red.

F. Un certificado de Autoridad.

Una tercera parte en una compañía u organización acepta las llaves públicas, junto con pruebas de identidad, y a su vez crea un certificado digital que será usado para identificarse. El CA (*Certificate Authority*) sirve como un repositorio para todo de estos miembros certificados.

El CA firma todos los certificados de los miembros con estas llaves privadas, hay *vouching* para la identidad de los títulos de los certificados. Todos los que usan CA reciben una copia de las llaves públicas. A su vez usan una llave pública CA para autenticar a los usuarios de la CA para decodificar la firma CA en sus certificados.

Algún certificado firmado por el CA, valida al certificado y al usuario. Los usuarios pueden compartir comunes CA o los CAs pueden formar certificados de jerarquía donde un certificado CA muestra otros CAs por debajo.

G. Certificados Digitales.

Es un documento electrónico, usado para establecer la identidad de una persona o compañía para verificar una llave pública. Los certificados digitales contienen el valor de una llave pública, nombre de un propietario de llave, firma digital de la organización emitida.

Un Certificado Digital ofrece:

- **Autenticación**. Asegura los datos actuales de la fuente que reclama la llegada.
- **Integridad**. Los datos comienzan a enviarse sin haber cambiado en su camino.
- **No repudio**. Provee irrevocables pruebas de origen de un mensaje. Protege también algún intento para el creador para subsecuentemente revocar el mensaje o su contenido.

Cuando un certificado es emitido, se espera su uso para periodos enteros válidos. Varias circunstancias pueden causar un certificado inválido previo a la expiración del periodo de validación. Tales circunstancias incluyen cambios de nombre, cargo de asociación entre sujetos y CA (un empleado termina el trabajo en una organización), y compromiso o suspende compromiso de la llave privada correspondiente. Bajo tales circunstancias, el CA necesita revocar el certificado.

X.509 define un método de revocación de certificado. Este método envuelve cada CA periódicamente emitido en una estructura de datos firmados llamado Lista de Certificados de Revocación (CRL, *certificate revocation list*). Un CRL es una lista de identificadores sellados, el cuál es firmado por un CA y libremente disponible en una base de datos público.

Cada certificado revocado es identificado en una CRL, por este certificado serial numérico. Un CA emite un nuevo CRL en un periodo regular (cada hora, cada día, o cada semana). Una entrada es agregada para el CRL como parte de una actualización siguiente de notificación de revocación. Y la entrada puede ser removida desde el CRL apareciendo en un programa CRL emitido más allá del periodo de validación de revocación de certificado.

Una ventaja de este método de revocación es que los CRLs puedan ser distribuidos por el mismo medio como certificados propios.

H. Expidiendo certificados y distribución de llaves públicas.

Dos aproximaciones han sido desarrolladas para emitir certificados y distribución de llaves públicas:

- **Llaves de Usuarios generadas**. Las parejas de llaves público/privadas son creadas en una estación final. Las llaves públicas son desarrolladas en un CA seguro, mientras las llaves privadas permanecen confidenciales. El CA genera un certificado y lo envía a los usuarios.
- **Llaves CA generadas**. La pareja de llaves públicas/privadas son creadas por un CA como parte de la certificación creando procesos, ambas llaves y certificados son desarrollados para el usuario.

I. Certificados Digitales.

Actualmente hay cuatro tipos de certificados que pueden ser numerados (figura 2.30):

- **Tipo 1**. Certificados que son fáciles de llevar y tiene una verificación limitada o de identidad.
- **Tipo 2 y 3**. Certificados que requieren más fondos de comprobación y más difíciles de llevar.
- **Tipo 4**. Certificados actualmente definidos, y su verificación no requiere ser definida.

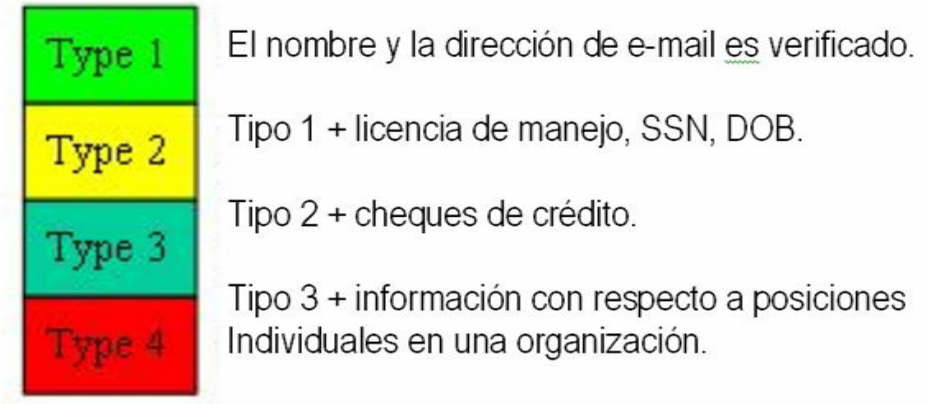


Figura 2.30 Tipos de certificados.

Los certificados se envían y reciben del Cliente al Servidor y viceversa, como se observa en la figura 2.31.

Figura 2.31 Validando certificados digitales.

J. Validación de Certificados Digitales.

Cuando los usuarios pertenecen al mismo CA, se verifica la identidad de un usuario (Alice) y el otro usuario (Bob) solo necesita verificar la firma CA en el certificado de Alice. (Figura 2.32).

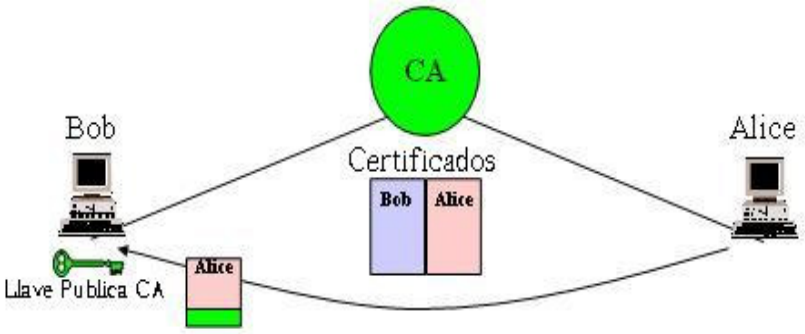


Figura 2.32 Usuarios comparten un CA común.

En la figura 2.33, cada CA tiene una firma certificada para el CA encima de este y todos de estos por debajo de él. Alice y Bob usan esto para verificar sus identidades para subirse al árbol, para un punto en común, y descender de regreso otra vez.

Figura 2.33 Validación en una jerarquía CA.

El usuario de un servicio de seguridad requiere el conocimiento de una llave pública, para obtener y validar un certificado conteniendo la llave pública requerida.

En general, una cadena de múltiples certificados puede necesitar y comprimir un certificado del propietario de la llave pública (fin de la entidad) firmado por un CA, o más certificados adicionales de CAs firmados por otros CAs. Tales cadenas llamados caminos certificados, son requeridas ya que un usuario de llave pública es inicializado con un número limitado de llaves públicas CA.

Cuando los certificados son expedidos, son esperados para validar por el periodo de tiempo designado en de/para archivo en el certificado [URL25]. Los certificados pueden ser revocados por varias razones.

Es recomendable que una CRL sea publicada en una base de datos común que puede ser accesada para sistemas participativos. El CRL identifica certificados revocados usando certificados numerados serialmente. Como parte del proceso de verificación certificado, el certificado usa los sistemas y compara los certificados recibidos contra los sistemas recientes CRL y verifica que el certificado serial numerado no aparece en el CRL.

2.3.6 Administración de usuarios.

Hay que considerar los aspectos administrativos antes de elegir el tipo de VPN que se va a implementar, ya que las redes grandes necesitan almacenar información de directorio por usuario en un almacén de datos centralizado, o servicio de directorio, para que los administradores y las aplicaciones puedan agregar, modificar o solicitar dicha información.

Cada acceso o servidor de túnel deberá mantener su propia base de datos interna de propiedades por usuario como: nombre, contraseña y atributos de autorización de marcación. La mayoría de los administradores establecen una base de datos de cuentas maestras en el servidor de directorio o controlador de dominio principal, o en servidor de RADIUS [URL40].

A. Soporte en RAS.

El RAS (*Remote Access Server*) de Microsoft está diseñado para funcionar con información individual de usuario almacenada en el controlador de dominio o en un servidor de RADIUS. Utilizar un controlador de dominio, simplifica la administración del sistema ya que los permisos de marcación son un subconjunto de la información por usuario que el administrador ya administra en una sola base de datos.

El protocolo ligero de acceso a directorio (LDAP) es un protocolo estándar en la industria para acceder a servicios de directorio, es extensible, independiente del distribuidor y se basa en los estándares. Permitiendo que un administrador asigne una variedad de propiedades de conexión para sesiones de marcación o de VPN destinadas a usuarios individuales o grupos. Estas propiedades definen los filtros por usuario, la autenticación requerida o los métodos de codificación, entre otras.

B. Radius.

El Protocolo de Servicio de Autenticación de Usuario Remoto de Marcación (RADIUS) es un método basado en el UDP para administrar la autenticación y autorización de usuarios remotos. Los servidores de RADIUS pueden localizarse en cualquier lugar de Internet y proporcionan autenticación para el NAS de cliente. Al mismo tiempo, los servidores de RADIUS pueden proporcionar un servicio *proxy* para transmitir las solicitudes de autenticación a servidores distantes de RADIUS.

C. Escabilidad.

La Redundancia y el balanceo de carga es logrado usando un ciclo Robin DNS para una división de demandas entre varios servidores de túnel VPN que comparten un perímetro de seguridad común. Un perímetro de seguridad tiene un nombre DNS externo por ejemplo: vpnx.support.bigcompany.com; las diversas direcciones IP y las cargas son distribuidas aleatoriamente a través de las direcciones IP. Los servidores pueden autenticar las demandas de acceso contra la base de datos compartida.

2.4 Hackeo de acceso telefónico.

El *hacking* mediante conexión telefónica se realiza de la misma manera que cualquier tipo de *hacking*: identifica, examina, enumera y explora. Todo el proceso puede automatizarse con ayuda de herramientas tradicionales de *hacking* llamadas *wardialers* o *daemon dialers*. Estas herramientas, que de forma automática marcan una gran cantidad de números telefónicos, registran conexiones de datos válidos (portadoras), intentan identificarse al sistema situado al otro lado de la línea telefónica e iniciar una sesión adivinando nombres de usuario y contraseñas sencillas.

El proceso de *hacking* a un acceso telefónico inicia con la identificación del rango de números que se van a introducir en un *wardialer*. Los *hackers* comienzan con el nombre de una compañía y recopilan una lista de posibles rangos de números a partir de toda fuente imaginable. Identificado un número telefónico principal, los atacantes llaman de forma agresiva al entorno completo numérico que engloba a dicho número. Otra táctica es llamar al proveedor telefónico local y averiguar la información de la cuenta de teléfono corporativa, aprovechándose de un servicio de atención al cliente despreocupado [15].

La mejor defensa contra la identificación telefónica es evitar la filtración innecesaria de información. Hay que asegurar que la compañía telefónica públique los números adecuadas, establezca una lista de personal autorizado para gestionar cuentas y pedir una contraseña cuando se hagan preguntas sobre una cuenta.

Además de crear un grupo que controle las filtraciones de información dentro del departamento de informática encargado de impedir la públicación de

cierta información sensible en sus servidores web, servicios de guía telefónica, titulares del servidor de acceso remoto, etc. Contactar con InterNIC y verificar la información de contacto que aparezca públicada. Recordarles a los usuarios que el teléfono no es siempre amigo, y que sean extremadamente prudentes con los comunicantes no identificados que soliciten información, sin importar lo inocuo que esta información pueda parecer.

El *wardialing* se reduce a una cuestión de elección de herramientas, como *ToneLoc*, *THC-Scan* y *PhoneSweep.*

El hardware es el principal factor a la hora de condicionar la velocidad y la eficacia. Las aplicaciones de *wardialing* son configuradas para ser extremadamente discretas, manteniéndose en espera durante un tiempo determinado antes de continuar con el número siguiente, de manera que no se pierdan objetivos potenciales debido a líneas ruidosas o a otros factores.

La elección del **hardware** del MODEM puede afectar enormemente a la eficacia. Los módems de gran calidad pueden detectar respuestas de voz, tonos de segunda marcación, y si está sonando un número remoto. La detección de voz, permite al software del *wardialing* registrar inmediatamente un número telefónico como “voz”, colgar y continuar marcando el número siguiente sin que transcurra el tiempo de espera especificado.

En los temas legales, es importante que cualquiera que deseé explorar este tipo de actividad, con fines legítimos, debe obtener primero algún tipo de permiso escrito de las entidades afectadas para poder llevar a cabo tales pruebas. Debiendo incluir en el documento firmado los grupos de números telefónicos aceptados de común acuerdo, y cualquier desviación de los mismos se produzca bajo su responsabilidad. Además de especificar la hora del día en que se permite esta actividad de conexión telefónica, se sugiere utilizar las horas nocturnas y las previas al amanecer. No hay que olvidar los costes adicionales telefónicos asociados con las llamadas realizadas, que pueden ser elevados, especialmente si los objetivos se encuentran a larga distancia.

El **software** que se emplea en los *wardialing* son programas propios para cada sistema operativo, y en *scripts* desarrollados por el usuario. Es de gran valor contar con los conocimientos necesarios para programar estas marcaciones automáticas de una forma flexible y ser capaz de reanudarlas en el punto en que los trabajos de marcación se detuvieron en la noche anterior.

Las herramientas gratuitas *ToneLoc* y *THC-Scan* anotan los resultados de las actividades realizadas y, de forma regular almacenan esta información en archivos de datos, permitiendo posteriormente una fácil reanudación de la tarea. *PhoneSweep* automatiza completamente estas actividades de programación.

2.4.1 Toneloc.

Primera y más popular herramientas de *wardialing*, de Minos Treta & Mucho Maas (abreviatura de *Tone Locator,* localizador de tono). Esta herramienta ha dejado de existir, puede hallarse en sitios especiales de Internet, Toneloc trabaja bajo DOS de cualquier sistema operativo, y tanto los *hackers* como los consultores en seguridad han comprobado, que se trata de una herramienta muy eficaz. ToneLoc es sencillo de configurar y usar para el acceso telefónico básico, es un poco complicado si se desean utilizar funciones más avanzadas. Funciona muy bien como un marcador masivo de números de teléfono utilizando la configuración básica. ToneLoc puede averiguar códigos de hasta cuatro dígitos [15].

2.4.2 THC-Scan.

Al desaparecer Toneloc, surgio THC-Scan, de van Hauser del grupo de *hacking* alemán: *The Hacker's Choice*. Al igual que ToneLoc, THC-Scan se configura y ejecuta bajo DOS en cualquier sistema operativo.

La mayor parte de las operaciones de configuración son sencillas, para llevar a cabo configuraciones no estándar resulta muy práctico conocer los detalles y complejidades del puerto COM de la PC.

La sintaxis de los mandatos de THC-Scan es muy similar a las de ToneLoc, pero incluyen diferentes mejoras. THC-Scan se parece mucho a ToneLoc incluso cuando se ejecuta. La programación diaria del *wardialing* es un proceso manual que utiliza parámetros para especificar las horas de inicio y finalización del programa, para reiniciar las exploraciones cada día a la hora indicada. Los parámetros de THC-Scan los escriben los programadores en un sencillo archivo de proceso por lotes, al que se llama mediante el programador de tareas (AT).

Lo más importante a recordar sobre la programación de THC-SCAN.EXE es que sólo busca el archivo .CFG en el directorio actual. Cuando se están buscando portadoras, THC-Scan puede enviar a un módem de respuesta ciertas cadenas especificadas en el archivo .CFG.

Una vez finalizada la exploración, se deberán examinar los diversos registros. Una de las funciones más potentes de THC-Scan es su capacidad para capturar y almacenar indicadores de terminal en un archivo de texto para su examen posterior. Se exige que en las funciones de gestión el usuario realice numerosas entradas manuales.

Las operaciones de *wardialing* pueden generar una enorme cantidad de datos que será necesario cotejar, incluyendo la lista de los números marcados, las portadoras encontradas, los tipos de sistemas identificados.

THC-Scan escribe esta información en tres tipos de archivos: un archivo .DAT delimitado, un archivo opcional .DB, que debe importarse a una base de datos compatible con ODBC y varios archivos de texto .LOG, que contienen listas de los números que estaban ocupados, las portadoras y el archivo del indicador del terminal de la portadora.

La gestión de los datos es un asunto importante cuando se usan varios módems. A pesar de los pequeños inconvenientes, THC-Scan es una herramienta increíble para ser gratis y disponible para el público [15].

2.4.3 *PhoneSweep.*

Si se piensa que THC-Scan da mucho trabajo, *PhoneSweep* (barrido telefonico) es el indicado.

Las funciones críticas que hacen que *PhoneSweep* destaque son: sencilla interfaz grafica, programación automatizada, la penetración de portadora, el manejo simultaneo de varios módems y los elegantes informes que es capaz de elaborar.

PhoneSweep se configura fácilmente para marcar durante el horario laboral, horas valle, fines de semana, o en los tres periodos. Identifica automáticamente hasta 120 marcas y modelos de dispositivos de acceso remoto. Ejecuta un ataque de diccionario contra los módems identificados. Otra función útil es la base de datos SQL, integrada en el *wardialing* es en la que se podrán registrar los resultados de todas las llamadas realizadas por todos los módems disponibles.

La mayor diferencia entre *PhoneSweep* y las herramientas *freeeware* está en su coste. *PhoneSweep* cuenta con dos versiones: *PhoneSweep Basic*, capaz de utilizar un módem y 800 números por perfil por 980 dólares americanos, y *PhoneSweep Plus*, que permite utilizar hasta cuatro módems y 10,000 números por perfil por 2,800 dólares americanos [15].

2.4.4 Técnicas de explotación de la portadora.

Las operaciones de *wardialing*, pueden descubrir módems fácilmente accesibles, pero con frecuencia, hay que examinar con cuidado los informes y realizar una posterior investigación manual para determinar la vulnerabilidad de una determinada conexión. Las portadoras no son los únicos elementos de interés que pueden surgir de una exploración de tipo *wardialing*. Muchos sistemas de correo de voz y PBX son también trofeos clave muy buscados por los atacantes.

Las PBX configuradas permiten una marcación remota y responderán con un segundo tono de marcación cuando se introduzca el código correcto. Con una seguridad inadecuada, estas funciones pueden permitir a los intrusos realizar

llamadas de larga distancia a cualquier lugar del mundo a cuenta del dinero de otro.

En los sistemas de conexión telefónica no es aconsejable efectuar intromisiones de este tipo que produzcan tanto ruido, es ilegal asaltar sistemas que no le pertenecen. Otro modo más efectivo para penetrar en los sistemas de acceso telefónico, es la ingeniería social [15].

2.4.5 Medidas de seguridad para marcación telefónica.

Hay que tomar en cuenta los puntos siguientes para realizar una comprobación de la seguridad de los sistemas de conexión telefónica de la empresa.

Una lista por orden de dificultad de implantación, que va desde lo más sencillo a lo más difícil, de manera que sean primero las tareas sencillas y, después las iniciativas más ambiciosas. Esta lista se asemeja mucho a una directiva de seguridad de acceso telefónico [15], [23].

1. Hacer un inventario de las líneas de conexión telefónica existentes.
2. Reunir todas las conexiones de acceso telefónico en un banco central de módem, ubicar este banco como conexión no fiable fuera de la red interna. Utilizar la técnica de detección de intrusiones y un *firewall* para limitar y vigilar las conexiones con subredes de confianza.
3. Dificultar la localización de líneas analógicas; no hay que colocar los números en el mismo rango que los números telefónicos de la empresa y no proporcionar los números de teléfono correspondientes al nombre de dominio al registro InterNIC. Proteger, mediante el empleo de contraseñas, las cuentas telefónicas de la empresa.
4. Verificar que los armarios de los equipos de telecomunicaciones son físicamente seguros, muchas empresas ubican sus líneas en armarios desprotegidos, en zonas de acceso público.
5. Supervisar con regularidad las funciones de registro existentes dentro de la aplicación de acceso telefónico. Buscar intentos fallidos de inicio de sesión, actividad nocturna y esquemas de utilización poco usuales. Utilizar el ID del sistema que ha realizado la llamada para almacenar todos los números de teléfonos entrantes.
6. Para las líneas que se utilizan con fines empresariales, hay que desactivar cualquier información que aparece al iniciarse la conexión, reemplazándola por el más inescrutable indicador de inicio de sesión que se pueda ocurrir. Utilizar un aviso amenazando con acciones legales en caso de uso no autorizado.
7. Para todos los accesos remotos, se solicita un sistema de autenticaron basado en dos factores. Esta autenticación de dos factores requiere que los usuarios presenten dos credenciales para poder acceder al sistema (algo que tienen y algo que saben). No existe otro mecanismo que elimine virtualmente la mayoría de los problemas que se han analizado hasta ahora.

Si es imposible implantar esa medida de seguridad, deberá imponer una estricta política de contraseñas complejas.

8. Solicitar autenticación *dial-back* (devolución de llamada). *Dial-back* significa que el sistema de acceso remoto se ha configurado para cortar la comunicaron ante cualquier llamada e, inmediatamente, conectarse con un número predeterminado (donde se encuentra quien llamo anteriormente). Para mejorar la seguridad, se utiliza un conjunto de módems independientes para la función de *dial-back*, y no permitir el acceso interno a estos módems (utilizando el *hardware* del módem o el propio sistema telefónico). Esta es también una de esas soluciones difíciles de llevar a la práctica, especialmente en multitud de empresas modernas que cuentan con numerosos usuarios móviles.
9. Asegurar que el servicio técnico de la compañía es consciente de lo delicado que resulta conceder o reconfigurar las credenciales de acceso remoto.
10. Centralizar los servicios de acceso telefónico (desde los faxes a los sistemas de correo verbal) en un departamento de su empresa que sea consciente de la necesidad de seguridad.
11. Definir directivas de seguridad muy estrictas para el funcionamiento de la división central, de tal forma que la concesión de la línea POTS (*Plain Old Telephone Service*) sea prácticamente un milagro o una decisión directa del presidente de la empresa.
12. Retroceda al paso 1, las directivas de seguridad diseñadas con elegancia son magnificas, pero la única forma de asegurarse de que alguien no se las esta saltando es realizar practicas de *wardialing* de forma regular. Se recomienda que se realice una vez cada seis meses para empresas con 10,000 o más líneas telefónicas, aunque no perjudicará el hecho de realizarla con mayor frecuencia.

El establecer un hábito de una conexión telefónica es sencillo, y se puede reflejar en un plan de doce pasos. Algunos de estos pasos son bastante difíciles de llevar a cabo pero al realizar *wardialing* con sus módems puede ser el paso más importante para la mejora de la seguridad de la red.

2.5 *Hacking* a la VPN.

Debido a la estabilidad y la omnipresencia de la red telefónica, las conexiones POTS se mantendrán todavía durante bastante tiempo. Con el tiempo la conexión telefónica será sustituida por el mecanismo de acceso remoto: una Red Privada Virtual (VPN, *Virtual Private Networking*).

Una VPN es un concepto más amplio que implica la tunelización de los datos privados a través de Internet con cifrado opcional [23]. Las principales ventajas de la VPN son su comodidad y el ahorro en costes. Las dos técnicas de tunelización más ampliamente aceptadas son el borrador del estándar IPSec y L2TP, que sustituyen a PPTP y L2F.

La tunelización implica la encapsulación de un datagrama encriptado dentro de otro, sea un IP dentro de un IP (IPSec), o un PPP dentro de un GRE (PPTP).

Este estudio es sólo aplicable a la implantación específica del PPTP de Microsoft [15]. Aunque es una tecnología orientada hacia la seguridad, muchas personas piensan que el diseño e implantación de la tecnología VPN escogida es impenetrable.

La nota de Schnëier y Mudge es una llamada de atención todas las personas que piensen así. Estas dos personas estudiaron la interacción de un cliente/servidor PPTP (no una arquitectura *gateway* de servidor a servidor).

Se presupone que la conexión cliente se produce sobre un distribuidor de Internet directo, y no de acceso telefónico. Además, algunos de los ataques propuestos se basaban en la capacidad de escuchar libremente en una sesión PPTP.

Aunque ninguna de estas hipótesis afecta dramáticamente en sus conclusiones, es importante tener en cuenta que un adversario con la capacidad de escuchar indiscretamente tales comunicaciones, supuestamente ha superado ya, una buena parte de la seguridad.

Las conclusiones importantes a las que llegaron son [15]:

- El protocolo de autenticación segura de Microsoft **MS-CHAP**, se basa en el legado de funciones criptográficas que han sido superadas previamente con relativa facilidad (el punto débil del *hash* de LanManager descubierto y violado con la herramienta L0phtcrack).
- El material seleccionado para las **claves de la sesión** utilizado para encriptar los datos de la red se genera a partir de las contraseñas proporcionadas por el usuario, disminuyendo la longitud práctica en bits de las claves por debajo de 40 y 128 bits de longitud declarados.
- El **algoritmo de encriptación** de sesión elegido (algoritmo simétrico RC4 de RSA) se encontraba muy debilitado debido a la reutilización de las claves de sesión, tanto en la dirección de envío como en la dirección de recepción, haciéndolo vulnerable a un ataque criptográfico común.
- El **canal de contro**l (puerto 1723 TCP) utilizado para negociar y administrar las conexiones, está sin autenticar y es vulnerable a los ataques de negación de servicios (DoS, *Denial of Service*) y de *spoofing* (engaño).
- Solamente la **carga útil de datos** se encuentra encriptada, permitiendo a los espías la obtención de mucha información útil de tráfico del canal de control.
- Se realizó la hipótesis de que los clientes que se conectaban a la red utilizando servidores PPTP podrían **actuar como una puerta trasera** en estas redes.

Estas conclusiones son específicas en la implantación PPTP de Microsoft.

Microsoft ha editado posteriormente un parche para los servidores y clientes de Windows NT.

Los clientes PPTP de Windows 9x deberían actualizarse a la versión 1.3 de acceso telefónico a redes para ser compatibles con las medidas de seguridad más exigentes del lado del servidor.

Aunque a pesar de este tropiezo con PPTP, IPSec es una mejor alternativa para evitar estas intrusiones. Solo el tiempo dirá que tan seguro es IPSec y averiguar en si habrá alguna falla que alguien detecte para que no sea tan seguro.

2.6 Ventajas y desventajas de una VPN.

Las VPNs surgen como una alternativa a los servicios de comunicaciones tradicionales de red WAN de enlaces dedicados. Este tipo de comunicaciones presentan múltiples ventajas y beneficios para los usuarios:

- **Bajo costo**. Reduce el costo del servicio de comunicación o del ancho de banda de transporte, y también el de la infraestructura y operación de las comunicaciones.
- **Flexibilidad.** Se puede optar por múltiples tecnologías o proveedores de servicio. Esa independencia posibilita que la red se adapte a los requerimientos de los negocios, y se puede elegir el medio de acceso más adecuado
- **Implementación rápida.** El tiempo de implementación de un *backbone* de WAN para una empresa es muy alto frente a la implementación de una red privada virtual sobre un *backbone* ya existente de un proveedor de servicio. Más aún, la flexibilidad de esta arquitectura permite implementar nuevos servicios de manera muy rápida, que concuerdan con los tiempos del negocio de la empresa.
- **Escalabilidad.** El desarrollo masivo de redes como Internet permite que la empresa tenga puntos de presencia en todo tipo de lugares. Por otro lado, la independencia con respecto a la tecnología de acceso posibilita escalar el ancho de banda de la red de acuerdo con el requerimiento del usuario. Además, la escalabilidad de la red no incide en la operatoria y gestión de ésta, dado que la infraestructura de la WAN es responsabilidad del proveedor del servicio.

Como en toda tecnología, existen aspectos positivos que llaman la atención y justifican su uso, como también hay aspectos negativos que pueden ser críticos para la migración hacia estas nuevas tecnologías [URL19].

Entre los **aspectos positivos** en las VPNs están:

- El **ahorro económico** que provee un VPN del punto de vista del cliente, donde toda la infraestructura y equipos necesarios yacen con el proveedor.
- **Mínimo control por parte del cliente**, donde esta labor pasaría a manos del proveedor.
- El **acceso por medio de VPN** puede ser extendido a todas partes del mundo aunque la compañía no tenga presencia sólida en ese punto geográfico.
- El **acceso** es solamente necesario **al POP del proveedor** donde se canaliza la información directamente a la Intranet y su conexión es, con respecto al usuario es como si estuviese conectado directamente a la Intranet.
- El **uso de una red pública** como Internet, para el transporte de esta información privada, no requiere mucha capacitación con entrenamientos puesto que Internet es muy conocido.

Y entre los **aspectos negativos**, tienen que ser analizados con cautela:

- El dar total **control administrativo y de seguridad al proveedor.** Una fuente externa VPN, puede traer problemas.
- **Bases de datos** con todos los parámetros de todos los usuarios pueden ser **comprometidas** y utilizadas en forma destructiva.
- **Internet como medio público**, tiene sus embotellamientos algunas veces causando que la información de ciertos VPNs quede afectados. Aunque se puede enrutar en Internet por múltiples direcciones, el **tráfico** no sería deliberado con la rapidez necesaria.

Capítulo

3

Diseño e Implementación de una VPN.

En esta parte se lleva a cabo la realización de un análisis detallado para el diseño e implementación de una VPN en una institución. Donde se aplican los conocimientos adquiridos a través de esta investigación.

Al conocer los requerimientos de la institución se proponen algunas alternativas de solución dependiendo de la tecnología con la que se cuente y con la capacidad de la red que se tenga instalada.

3. Introducción.

La tecnología en redes busca la comunicación, difusión y conocimientos sobre la información importante y vital para quienes es necesario estar al día. Sin contar que existen fugas de información como la alteración parcial, temporal o permanente el daño que se cause a la misma a través de una red privada o pública como es Internet. El aplicar y seguir políticas de seguridad junto con *firewalls*, hace más fuerte la red privada [1], [14], [10].

Al conectarse una red privada propia hacia otra por medio de Internet se logra una conexión virtual y más aun con una seguridad extra, con ayuda de varios mecanismos lógicos y físicos, creando así una VPN. Con esta red de propone una mejoría a la organización y una garantía de confiabilidad en el manejo de la información y un mejor desarrollo de la misma en cualquier parte del país con acceso a ella sin importar cuan lejos este el personal.

3.1 Introducción al instituto ITESA.

ITESA [URL27] es una institución educativa que, bajo un estudio de factibilidad realizado por IHEMSYS satisface la demanda de la sociedad en esta parte del Estado de hidalgo.

El estar a la vanguardia tecnológica, hace que el instituto al igual que otros organismos requiera en un futuro la instalación de una Red Virtual Privada (VPN), para un mejor desarrollo educativo tanto para maestros como alumnos. Hay que sabe que el instituto opera con ayuda de IHEMSYS, la cual acaba de autorizar el acceso a Internet Satelital, con Internet e-México.

Se espera que en poco tiempo este disponible ya el acceso a Internet, así como una implantación de una red local que permita una mayor comunicación en las áreas académicas, para mantenerse al tanto de desarrollos tecnológicos para una mejoría en educación para enorgullecer al plantel y al alumno mismo.

3.1.1 Historia.

Por gestiones del Gobierno Municipal de Apan y del Gobierno Estatal, con base en el estudio de factibilidad realizado por el IHEMSYS, el Gobierno federal autoriza la apertura del ITESA para ofrecer a nivel licenciatura las carreras: Ingeniería Electromecánica (IE) e Ingeniería en Sistemas Computacionales (ISC) previa promoción del ITESA y sus Carreras a partir del 17 de julio 1999, en diferentes medios de difusión, el instituto inicia actividades el 6 de septiembre en forma provisional, en instalaciones que pertenecen a la Secundaria de Trabajadores y al Centro Regional de Maestros, con mobiliario y equipo prestado por estas Instituciones y otras pertenecientes al IHEMSYS.

De conformidad con el estudio de factibilidad y su respectiva actualización, para diversificar la oferta educativa, la Coordinación de Institutos Descentralizados aprueba, por parte de la SEP del Gobierno Federal, la apertura, a partir del periodo escolar que inicia en Agosto 2001, de las Licenciaturas de Ingeniería en Industrias Alimentarías (IIA) e Ingeniería Civil (IC) [URL27].

3.1.2 Visión.

Ser una Institución [URL27] que consolide y diversifique sus programas académicos, genere conocimiento para el desarrollo del sector productivo y social; que cubre las expectativas de los alumnos y la comunidad, logrando egresados con potencial profesional y desarrollo humano, confirmando su pertenencia al impactar de manera favorable en lo económico social y cultural, que se traduzca en un mayor reconocimiento y aceptación en la región, el estado y el país.

3.1.3 Misión.

Ser lideres [URL27] en la formación de profesionistas con conocimientos, habilidades, actitudes y comportamiento acordes con los valores Institucionales, teniendo como fundamento proyectos académicos vigentes, consistentes y congruentes, que impulsen el desarrollo humano y el espíritu creativo y emprendedor, que le permita al egresado cubrir sus expectativas, participar exitosamente en el mejoramiento de la región, obtener reconocimiento social y con ello, prestigiar la Institución.

3.1.4 Valores Institucionales.

- **Honestidad.** Comportamiento consecuente entre lo que se piensa, siente dice y hace, en el marco de los valores del Instituto.
- **Pertenencia.** Sentirse identificado y orgulloso de ser parte del Instituto.
- **Servir.** Comportamiento de colaboración incondicional de la comunidad del Instituto, indispensable para el logro de sus objetivos.

- **Compromiso.** Involucrarse consciente y convencido, en el logro de los objetivos del Instituto aceptando el riesgo inherente.
- **Alumno.** Razón de ser en el quehacer del Instituto [URL27].

3.2 Análisis de las necesidades de la Institución.

En este punto se conocen las necesidades de la institución [URL27], como de los servicios que cuenta, y las características que tienen o se desea para los equipos de computadoras para la instalación de la VPN [URL41], [URL29].

3.2.1 Usos y beneficios de una red de computadoras.

Los usos principales para este instituto es el poder mantener actualizado el *software* en los equipos para un mejor aprendizaje y dominio de dicho *software* para los alumnos en general; así como para los de ISC, el aprender a instalar redes y manejar principales sistemas operativos y *software* de desarrollo [URL31], [URL46].

Los beneficios que se esperan son muchos, pero principalmente a los que se refieren al aprovechamiento de aprendizaje de los alumnos de ISC, que están próximos a salir y para los que actualmente están estudiando.

3.2.2 Características de los equipos existentes.

Las características de los equipos con los que se cuenta son:

Equipo	Cantidad	Características
Servidor	1	Procesador *Xeon* doble de 2.8 Ghz. 512Mb en RAM. 72 Gb. en Disco duro.
Computadoras personales	40	Procesador Pentium 4. 256 en RAM. 40 Gb. Disco duro.
Switch CISCO	2	24 puertos.
Patch Panels	2	
Riack	1	
Cable par trenzado		
Impresora láser	2	
Plotter	1	Inyección de tinta

Tabla 3.1 Equipo actual para la red local.

El equipo con el que actualmente se cuenta es para uso totalmente académico.

El *software* con el que se cuenta es: Office, Autocad, Mathlab, de Simulación y Compiladores. Para el aprendizaje en las materias de Redes de computadoras: Sistemas Operativos, Bases de Datos y de Especialidad.

El diseño de la red local a instalar es topología de estrella con par trenzado con los 2 *Switch* Cisco con UTP 5e, dentro del Centro de Cómputo en el que actualmente está.

Cuando se diseña una red hay que tomar en cuenta tres objetivos:

- **Primero:** las exigencias de la red, las razones de su desarrollo. Objetivo obligatorio. Por ejemplo: la interconexión de los diferentes servicios de la institución.
- **Segundo:** las ventajas que la red puede aportar a la compañía y que solo necesita poco o ninguna inversión adicional. Objetivo recomendable. Por ejemplo: el servicio de fax.
- **Tercero:** las exigencias futuras, las funciones que podría asumir la red, y que no estén vigentes por el momento. Objetivo recomendable para un futuro cercano. Por ejemplo: acceso directo a Internet, comunicación satelital propia y la Realidad Virtual.

Aplicando estos objetivos para la red [URL41]:

- **Primer objetivo:** es con el fin de compartir recursos e información académica dentro del instituto y fuera de él.
- **Segundo objetivo:** los beneficios de la red, se verán reflejados en una compartición de información en el área académica e institucional por medio de becas, servicio social a importantes empresas, creación de vínculos con otros institutos, academias, actualizaciones curriculares y de materias, así como un mejoramiento académico para con los alumnos.
- **Tercer objetivo:** es que con ayuda de esta red privada y algunas adiciones tecnológicas como la introducción de Internet a toda la red, la implementación de una VPN, la cual es nuestro objetivo principal.

3.2.3 Consideración para la elección de equipo.

Para la elección del equipo se debe contar con apoyo tecnológico de IHEMSYS. Antes presentar una justificación del proyecto ante COSNET e IHEMSYS para aprobar el proyecto y así contar con Internet [URL42].

Requisitos Estructurales.

Para establecer una VPN, ya sea entre varias subredes o entre una LAN y un *host* "móvil", son necesarios algunos requisitos:

Con respecto al *hardware* es necesario tener [URL42] un *router* a internet, que va a ser la pieza clave de la VPN. Cualquier tipo de *router*, será suficiente. Es necesario el soporte físico para la comunicación entre las dos *subredes* o entre la LAN y el *host* "móvil".

En cuanto al *software*, se debe tener un sistema de transporte “opaco” entre los dos puntos a unir por la VPN, es decir actúa sólo como transporte, sin explorar dentro de los datos que va a transportar. El transporte debe asegurar una cierta calidad de servicio, y debe proporcionar seguridad (encriptación) a los datos. En los *routers* se debe disponer de un tipo de encapsulamiento disponible para la red de transporte intermedia (*dialup*, internet) para que entregue los paquetes entre los dos *routers* de la VPN, sin examinar dentro de los datos de transmisión que estarán encriptados [URL22].

Requisitos Funcionales.

Para que una VPN proporcione la comunicación que se espera, el sistema ha implantar ha de contemplar varios aspectos de funcionamiento para determinar que una buena solución [URL41], [URL42].

- **Transparente a las aplicaciones:** es decir que las aplicaciones no necesiten adaptarse a este nuevo mecanismo sin afectar el correcto funcionamiento de las aplicaciones.
- **Confidencialidad:** los datos que circulan por el canal sólo pueden ser leídos por emisor y receptor. La manera de conseguir esto es mediante técnicas de encriptación.
- **Autentificación:** el emisor y receptor son capaces de determinar de forma inequívoca sus identidades, de tal manera que no exista duda sobre las mismas. Se consigue mediante firmas digitales o aplicando mecanismos desafío-respuesta (CHAP).
- **Integridad:** la capacidad para validar los datos esto es, que los datos que le llegan al receptor sean exactamente los que el emisor transmitió por el canal. Se pueden utilizar firmas digitales.
- **No repudio:** cuando un mensaje va firmado, el que lo firma no puede negar que el mensaje lo emitió él.
- **Control de acceso:** la capacidad para controlar el acceso de los usuarios a distintos recursos.
- **Viabilidad:** la capacidad para garantizar el servicio. Por decir, las aplicaciones de tiempo real.

3.3 Propuestas de Solución.

En este punto se estudian algunas alternativas para mejorar la red [URL41]:

3.3.1 Alternativas.

Las soluciones que se proponen para mejorar la red son:

- Internet por medio de un proveedor local.
- Internet e-México por medio de un CCD.
- Una VPN.

3.3.2 Evaluación de alternativas.

En este punto se evalúa cada alternativa viendo el lado económico, operativo, técnico, financiero y temporal, con el fin de ayudar a escoger la mejor opción para la red.

- **Técnico:** se analiza y determina el tipo de *hardware* y *software* que es necesario para la implementación del Centro de Cómputo como de la red actual [URL31].

En lo que respecta de *hardware*, se hace un análisis de todo lo referente al tipo de computadoras, terminales, módems, multiplexores, servidores, tipo de cable, etc.

Para el *software* se analiza la arquitectura de protocolos (OSI, SNA, Novell, etc), el sistema operativo usado para la red, el tipo de *software* para el servidor, así como para las aplicaciones en el servidor Web, y los tipos de interconexión.

- **Operacional:** se analiza el efecto de la nueva red sobre la estructura organizacional, en las relaciones humanas y de trabajo, a fin determinar cuales pueden ser los puntos positivos o negativos dentro de la organización al implementar la red de manera definitiva. Este punto esta garantizado en funcionamiento de la red, ya que el personal esta consciente de la necesidad de modernización para realizar un mejor trabajo.
- **Económico:** se realiza un estudio costo-beneficio sobre el efecto de la nueva red, a fin de demostrar que los beneficios serán mayores que los costos y así garantizar la nueva inversión.
- **Financiero:** es importante determinar de que forma se obtendrá el capital necesario para la implementación de la red y que tan rentable es llevarla a cabo, esto será más fácil una vez que se tenga el estudio económico.
- **Temporal:** es la realidad de las oportunidades.

3.3.3 Viabilidad.

Antes de elegir una opción de cambio de red, se estudian las propuestas anteriores con base a los puntos anteriores.

La **primera opción** para obtener el acceso a Internet es por medio de un proveedor local. Se puede contratar el servicio por medio de TELMEX, los servicios son *Prodigy* o *Prodigy Infinitud*. Actualmente debido a la infraestructura se cuenta con solo en algunas computadoras y su acceso al Internet es restringido. Sólo el rector y algunos profesores tienen acceso con tiempo establecido, además que es muy lento.

La **segunda opción** es Internet e-México por medio del CCD [21], [22], [URL30]. Un CCD pretende ayudar en las tareas que todo profesor tiene, para ayudarle con problemas escolares, financieros, pagos, convocatorias entre escuelas. El CCD ayuda a hacer todo esto y mucho más, de manera sencilla, rápida y profesional. En este lugar se cuenta con computadoras e Internet sin necesidad de saber computación, ya que siempre hay un asesor en línea [URL30].

El sistema nacional e-México es un conjunto de estrategias, acciones y metas en el que participan los gobiernos federal, estatal y municipal, las Secretarías de Estado, las instituciones privadas y la población en general para propiciar, mantener y fortalecer el uso de las computadoras y la Internet, generando una sociedad inmersa en los beneficios que ofrecen los avances tecnológicos de la comunicación y disminuyendo así la brecha digital [URL30].

Este sistema apoya en las actividades, brinda información y servicios que permitan estrechar la relación entre ciudadanos y autoridades, a través de portales de e-gobierno, e-salud, e-economía, e-aprendizaje.

Internet es un sistema cooperativo mundial de redes de computadoras conectadas entre sí por diversos medios y equipos de comunicación. e-México [URL30] provee la conectividad terrestre o satelital de banda ancha a bajo costo en centros educativos y culturales, biblioteca, plazas comunitarias, centros de salud, oficinas postales y de telégrafos, entre otros, para brindar atención al público a través de un CCD.

El propósito fundamental del Sistema Nacional e-México, es lograr que toda la población acceda a los servicios de Internet y a las computadoras a bajos costos por medio de un CCD.

En esta opción no se necesita saber mucho del manejo de redes y sobre todo se tiene a un especialista en línea que ayuda al usuario a conocer el manejo de computadoras e Internet.

La **tercera opción** es la VPN [URL28]. Para este tipo de red es necesario contar con Internet, para hacer el enlace de la conexión virtual hacia otra universidad, organismo o empresa para compartir información para la misma institución como para el crecimiento estudiantil.

Esta opción es muy tentadora para la institución, solo que no es viable debido a que aún no se cuenta aun con Internet para el instituto para la red local, su acceso es restringido. Se está en la creación de un centro de cómputo para los alumnos y una red local en la misma.

Se espera que con ayuda de IHEMSYS se instale el servicio de Internet en la misma, solo disponible en la dirección y algunas oficinas de coordinación de las carreras. Aunque se cuenta con un enlace a la página web dentro del portal de IHEMSYS, en la cual solo se encuentra información sobre el instituto y las carreras sin ningún otro enlace para que tanto alumnos como catedráticos interactúen para su retroalimentación, como muchas otras páginas web de distintos institutos educativos.

Esta traba económica y tecnológica pone un alto operacional y financiero. Pero no un alto a la alternativa técnica y operativa de una red VPN. Y se espera que en un futuro próximo sí se adquiere la tecnología necesaria se implemente una VPN para el crecimiento del instituto.

3.4 Diseño detallado de la red.

Una VPN emplea tres tipos básicos de topologías: *host-host, host*-red y red-red [URL28], [19], [20], [URL41].

3.4.1 Medio físico y equipo empleado.

HOST-HOST

La implementación más sencilla de una VPN es de un *host* a otro. Simplificando, se asume que los *hosts* están conectados por medio de *ethernet* a una LAN que después se conecta a Internet (figura 3.1).

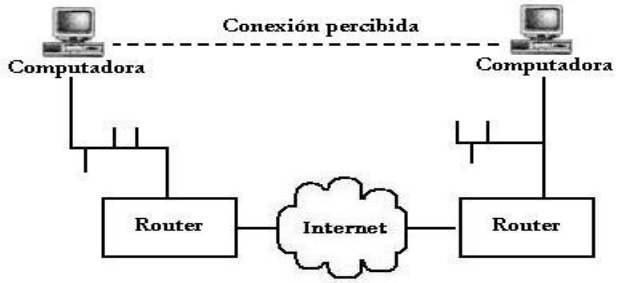


Figura 3.1 VPN *Host-Host*.

En una situación real, la comunicación se produce a través de *hubs*, conmutadores, *routers* y nubes WAN. Además, si los *hosts* están conectados directamente mediante un cable *ethernet* de CAT5 (categoría 5), el único riesgo que se disminuye con una VPN son las escuchas sobre el tendido: una habilidad difícil de encontrar y de ejecutar. [URL20], [URL29], [URL39].

En un escenario *host-host* (figura 3.1), [URL20] se tienen dos *host*s conectados a Internet en su punto más íntimo, ya sea mediante una línea dedicada o mediante una conexión de marcado telefónico. La comunicación entre estos dos *host*s no es segura y es blanco de los piratas de Internet.

Al implementar una VPN *host-host*, todas las comunicaciones entre ambos *host*s quedan protegidas por el transporte VPN autenticado y cifrado. La aplicación de este tipo de configuración no es fácil de explicar.

Un ejemplo de dónde podría ser apropiada una VPN *host-host* es cuando existen dos servidores, cada uno protegido por un *firewall,* responsables de la contabilidad financiera. Es raro que dichos *host*s tengan que comunicarse para sincronizar los datos. Los servidores están conectados a la LAN *ethernet* de cada oficina, con una puerta de enlace de Internet con una conexión RDSI de 128 K.

La creación de una VPN red-red podría ser excesiva porque no hay tráfico de una LAN a otra excepto en lo que respecta a la sincronización de los servidores financieros y además, una VPN red-red necesitaría *hardware* dedicado. Por tanto, al ser una implementación que sólo implica *software*, la VPN *host-host* es la mejor solución.

HOST-RED

Un método fácil [URL20] para ofrecer a los usuarios móviles la capacidad de conectar con la red de la empresa es mediante una red virtual segura, o una VPN *Host*-Red.

En esta configuración (figura 3.2), cada *host* se conecta independientemente con una LAN mediante una puerta de enlace VPN. Se autentica cada *host*, y los túneles VPN se inician para cada uno de ellos. El *host* móvil puede conectarse mediante cualquier tipo de conexión, ya sea de marcación telefónica, una conexión LAN o un enlace inalámbrico. Las VPN *host*-red se encuentran en situaciones de acceso remoto.

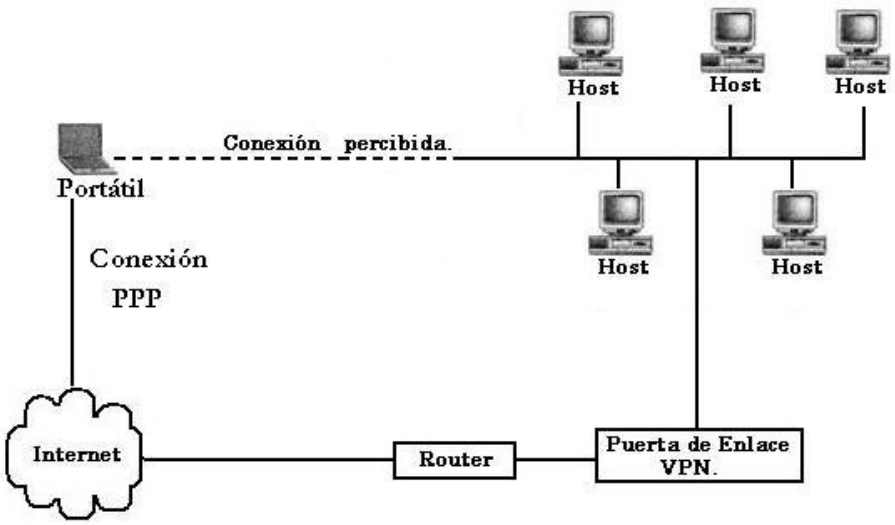


Figura 3.2 VPN *Host*-Red.

Un usuario móvil puede tener *software* de VPN en su portátil y conectar con la Intranet a través de una puerta de enlace VPN. También se utiliza esta topología VPN para los empleados que trabajan desde casa.

El lento y constante crecimiento de los clientes de ADSL y el cable hace que trabajar desde casa sea una opción atractiva. Una VPN puede hacer que el tráfico sea privado e ilegible hasta que llega a la puerta de enlace VPN de la empresa [URL20].

RED-RED

La tercera topología [URL20] VPN es la red-red. En esta configuración (figura 3.3), cada puerta de enlace se ubica en un extremo de una red y proporciona un canal de comunicación seguro entre las dos (o más) redes.

Este tipo de comunicación es el que mejor se adapta a la conexión de redes LAN separadas geográficamente.

Una ventaja importante de esta configuración es que las LAN remotas de la VPN son transparentes para el usuario final. Las puertas de enlace VPN tienen la apariencia de *routers* para los usuarios.

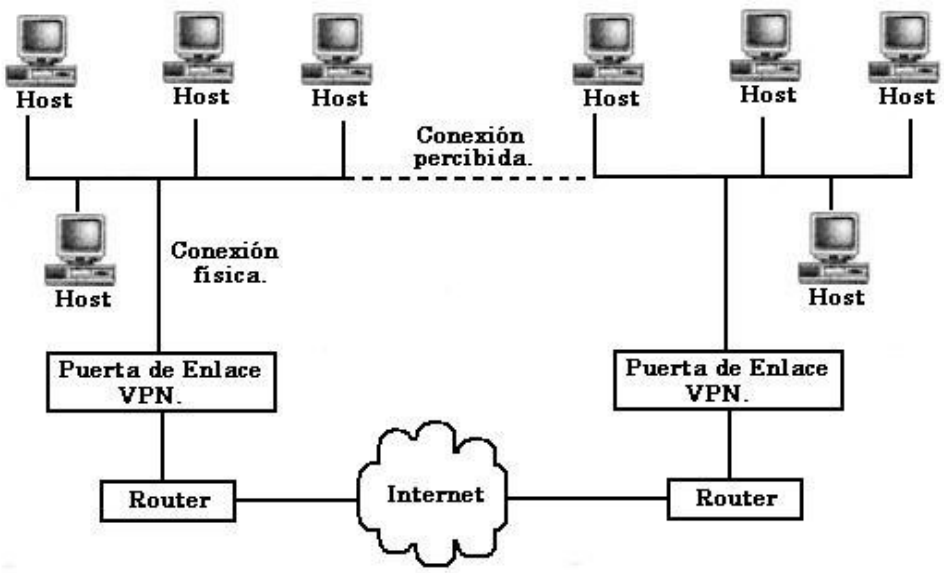


Figura 3.3 VPN Red-Red.

Se utilizan las VPN red-red para conectar intranets, lo que hace es que parece que las redes son adyacentes. Los datos transferidos entre las intranets son confidenciales durante el tránsito. También se utiliza esta topología para extranets entre varias empresas, en caso de que cada empresa comparta recursos particulares sólo con los socios de negocio. [URL28], [URL29], [16], [17], [URL20].

3.4.2 Consideraciones en el diseño de VPN.

Existen diferentes formas de diseñar la ubicación de una VPN dentro de una organización, algunas formas de hacerlo se muestran a continuación [URL36], [URL20], [URL29], [URL39], [20]:

VPN *gateway* detrás de un *firewall*.

Un VPN de pasarela o VPN *gateway* requiere una dirección IP pública. Necesita ser configurado para el paso no permitido del tráfico a la VPN. El *firewall* debe ser configurado para el tráfico VPN. No puede filtrar el tráfico VPN para las aplicaciones (figura 3.4).

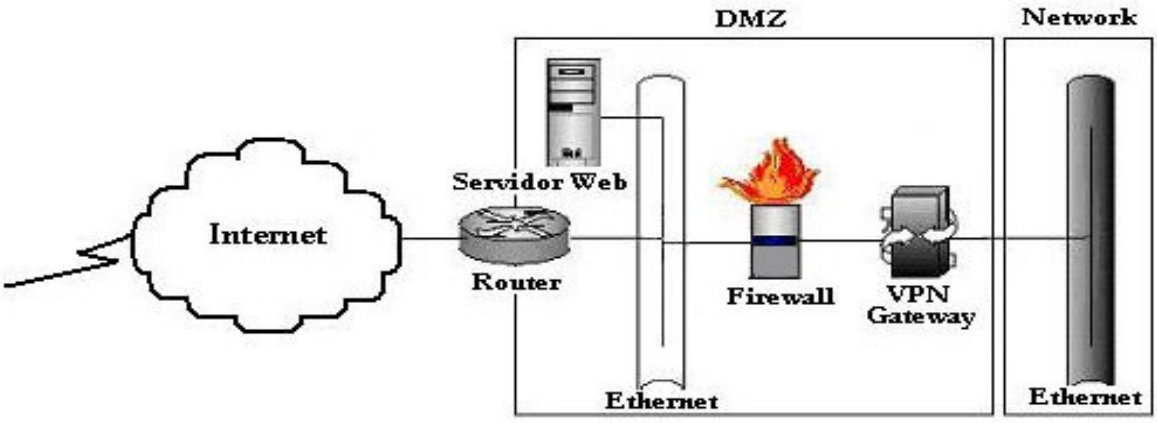


Figura 3.4 Una VPN detrás de un *firewall.*

VPN *gateway* frente a un *firewall*.

Una VPN *gateway* puede tener dos direcciones IP. No debe pasar el tráfico a la VPN. Requiere rutas estáticas para todas las redes internas (figura 3.5).

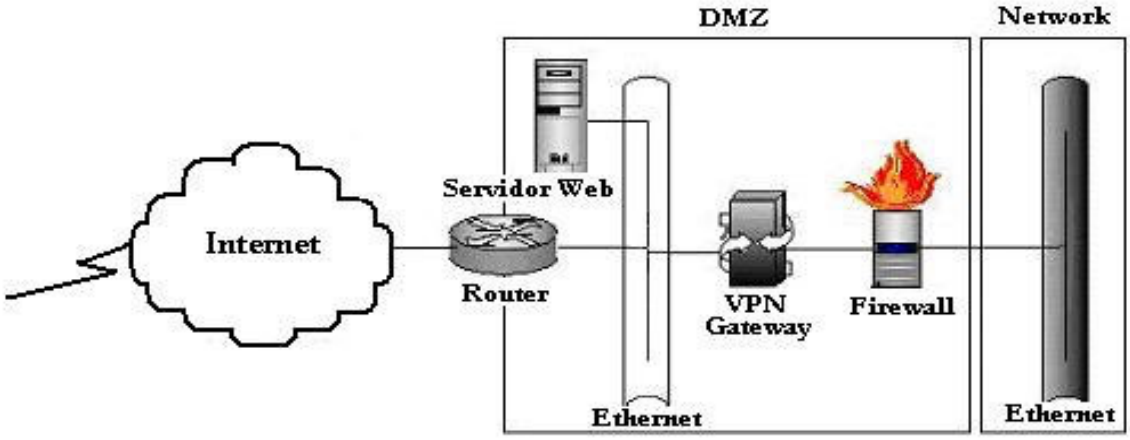


Figura 3.5 Una VPN frente a un *firewall.*

VPN *gateway* en paralelo con un *firewall*.

Una VPN de pasarela tiene una dirección pública tanto como una dirección privada. Debe bloquear casi todo el tráfico de la VPN. El *firewall* debe bloquear todo el trafico VPN (figura 3.6).

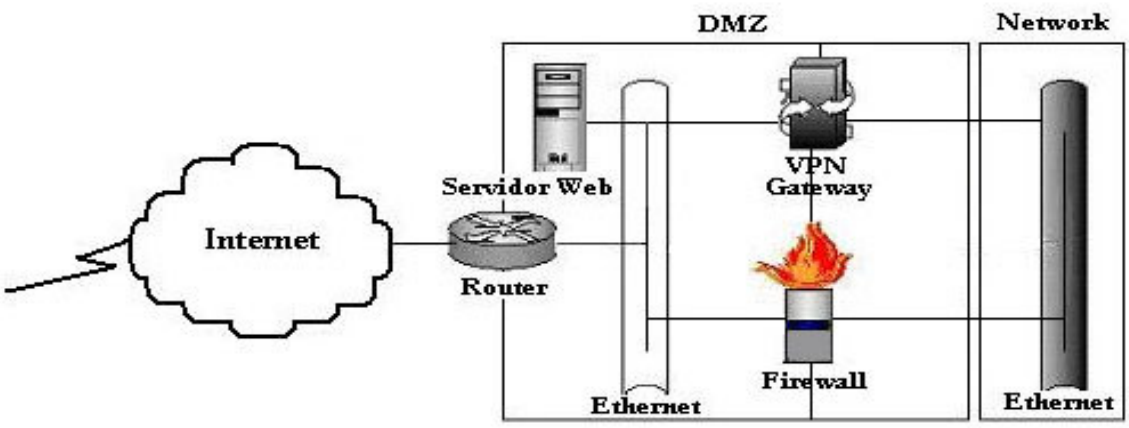


Figura 3.6 Una VPN en paralelo con un *firewall*.

Combinación de VPN *Gateway/Firewall*.

El VPN *gateway* debe no bloquear todo el tráfico VPN. El *firewall* puede filtrar el trafico VPN en el nivel de aplicación (figura 3.7).

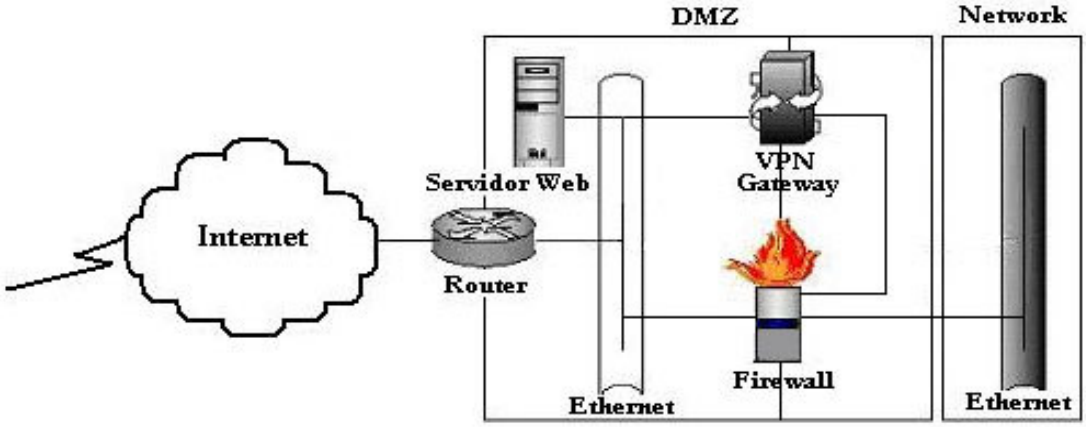


Figura 3.7 Combinación de VPN *Gateway/Firewall.*

Gateway armado como VPN.

El *firewall* puede filtrar trafico VPN en el nivel de aplicación e incrementa la carga en el *firewall* (figura 3.8).

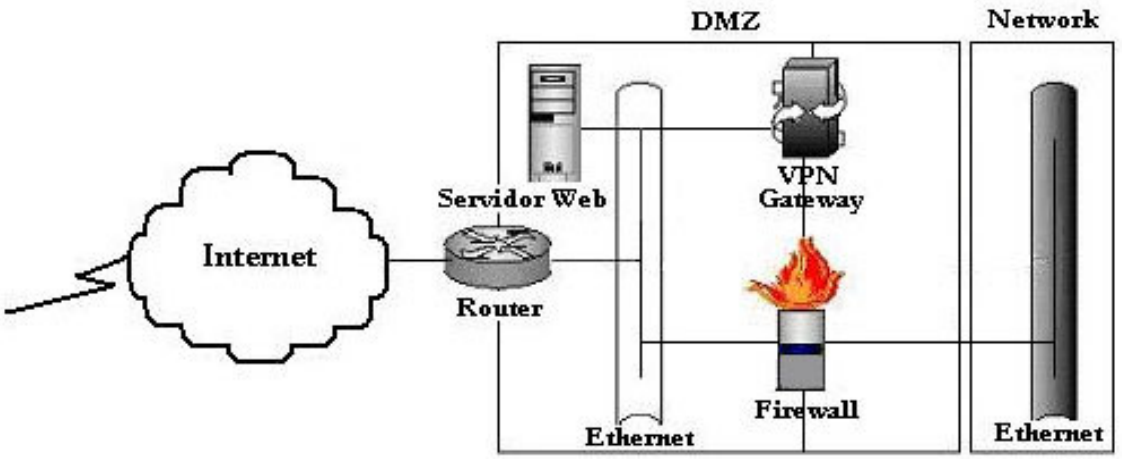


Figura 3.8 *Gateway* armado como VPN.

3.4.3 Equipos para Redes privadas virtuales

Algunos equipos para VPN son [URL22], [23]:

- ***VPN gateway:*** dispositivos con un *software* y *hardware* especial para proveer capacidad a la VPN. Varias funciones son optimizadas sobre varios componentes de *software* y *hardware*.

Algunos ejemplos de esto tenemos Alcatel 7130 (figura 3.9), Altiga C10, VPN-1 *Gateway*, *Lucent* VPN *Gateway*, Intel Shiva Lan Rover VPN *Gateway Plus*, *TimeStep Permit/Gate* 4620 y *VPNet VPNware* VSU-1010, las cuales incluyen el *software* y *hardware* necesario para realizar y administra VPN.

Figura 3.9 Acatel 7130 *gateway* de VPN.

- **Sólo *Software***: el *software* está sobre una plataforma PC o *Workstation*, el *software* desempeña todas las funciones de la VPN. Ejemplos: el Sistema Operativo Windows 9x, ME, NT, 2000 y XP

- **Basado en *Firewall***: funciones adicionales son agregadas al *firewall* para habilitar capacidades de VPN. Algunos ejemplos de esto son los modelos PIX de Cisco como 506, 515, 525 y 535 (figura 3.10).

Figura 3.10 Cisco 535 *Secure PIX Firewall* 535.

- **Basado en *Router***: Funciones adicionales son agregadas al *router* para habilitar capacidades de VPN, las cuales se encuentran en el IOS de los *router* de Cisco como los modelos 804, 806, 827, 905, 1710, 1720, 1750, 2611, 2621, 2651, 3620, 3640, 3660, 7120, 7140 y 7200 (figura 3.11).

Figura 3.11 *Router* cisco Serie 7200.

Aunque los router son mejores que los concentradores, existen algunos capaces de realizar VPN (figura 3.12) como los modelos 3005, 3015, 3030, 3060 y 3080.

Figura 3.12 Concentrador Cisco Serie 3000.

3.4.4 Soporte de estándares.

En una VPN hay que tener en cuenta los estándares que puede soportar nuestra red y saber los puntos fuertes y débiles del mismo. Se hace una comparativa global en la Tabla 3.2, entre las diferentes tecnologías VPN para escoger el estándar que llevara la red [URL25], [URL29].

Tecnología	Puntos fuertes	Puntos débiles	En desarrollo
IPSEC	☞ Opera independiente de las aplicaciones de niveles superiores. ☞ Subconjunto de IPv6. ☞ Ocultación de direcciones de red sin emplear NAT. ☞ Acoplamiento con las técnicas criptográficas existentes y futuras.	☞ No proporciona la gestión de usuarios. ☞ Interoperabilidad entre los fabricantes. ☞ No estandarizado.	☞ Estandarización de todas las facetas de PKI, incluyendo los protocolos de intercambio de certificados y el formato de éstos. ☞ El IETF está en su desarrollo.
Cortafuegos	☞ Gestión centralizada de los parámetros de seguridad, autenticación y acceso. ☞ Disponibilidad de una interfaz común para la modificación de las reglas del túnel. ☞ Disponibilidad de ACLs para usuarios remotos.	☞ Reducción del modo de operación debida a la encriptación *software*. ☞ Precisa un alto control con los cambios al añadir nuevas reglas VPN.	☞ Mismos objetivos que IPSec. ☞ Soluciones capaces de realizar la encriptación por medio del *hardware.*
PPTP	☞ Soporta *tunneling* extremo a extremo y entre servidores. ☞ Posibilidad de valor añadido para el acceso remoto. ☞ Proporciona una capacidad multiprotocolo. ☞ Empleo de encriptación RSA RC-4.	☞ No proporciona encriptación de datos para los servidores de acceso remoto. ☞ Precisa un servidor NT como terminador del túnel. ☞ Sólo usa encriptación RSA RC-4.	☞ Integración con *IPSec.*
L2F	☞ Habilita el *tunneling* multiprotocolo. ☞ Soportado por la gran mayoría de fabricantes.	☞ No posee encriptación. ☞ Autenticación débil. ☞ No dispone de control de flujo sobre el túnel.	☞ Implementaciones que empleen el nombre de usuario y dominio en el establecimiento del túnel.
L2TP	☞ Combina L2F y PPTP. ☞ Necesidad de únicamente una red de paquetes para operar bajo X.25 y *Frame Relay.*	☞ Aún no implementado.	☞ Estandarización y operación en proceso. ☞ Será adoptado por los fabricantes para el acceso remoto una vez completo.
VTCP/Secure	☞ Mecanismos de encriptación y autenticación fuerte. ☞ Proporciona seguridad extremo a extremo. ☞ *Tunneling* basado en nombre de dominio.	☞ Protocolo propietario. ☞ Las configuraciones LAN-LAN no están permitidas. ☞ No es multiprotocolo.	☞ Compatibilidad con *IPSec*.

Tabla 3.2 Comparativa entre tecnologías de VPN.

3.4.5 Elección del SITE.

La VPN se implementará dentro del Centro de Cómputo. En un futuro se espera que se construya o asigne un área especial para el equipo de la VPN (*firewall, router*, *switch*), aparte de los que ya se cuente en la red [19], [22], [15], [URL29].

3.4.6 Ubicación de las estaciones de trabajo.

La ubicación será la siguiente [22]:

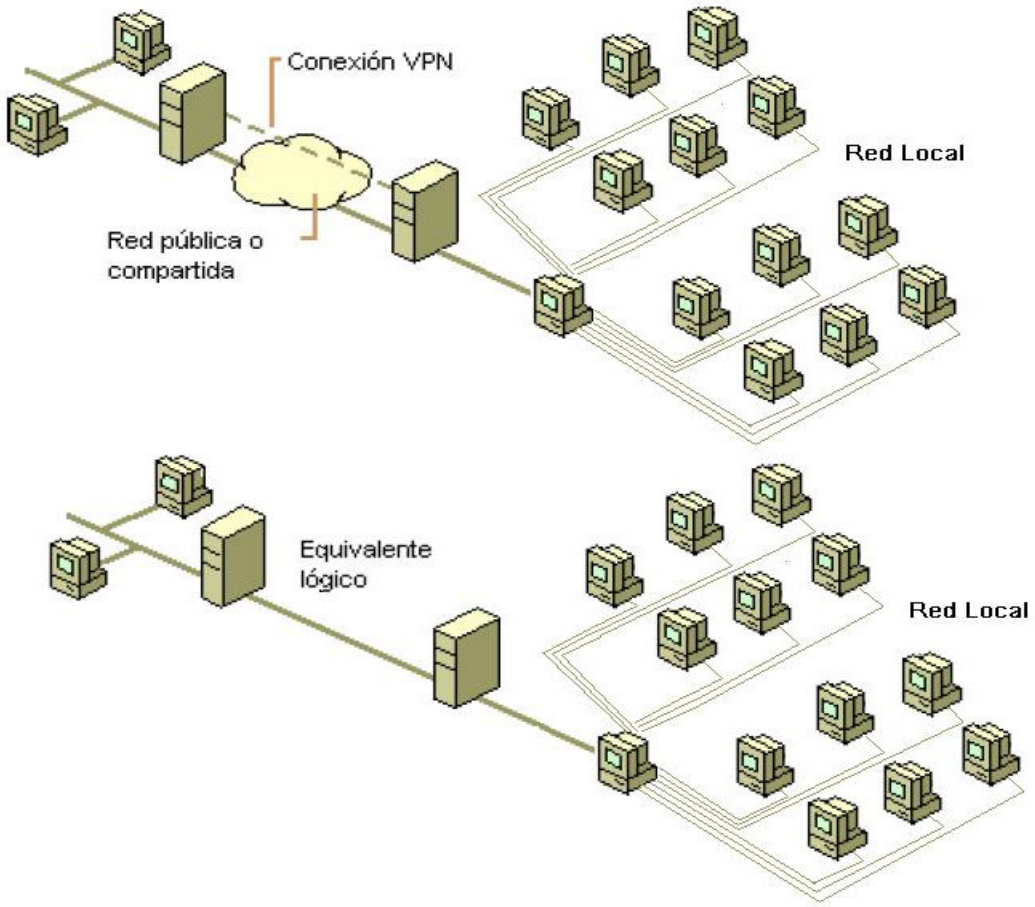


Figura 3.13 Distribución del SITE

3.4.7 Instalaciones eléctricas.

Las instalaciones eléctricas se harán según el diseño del esquema anterior, empleando canaletas, *switches*, cable par trenzado con UTP 5e, una topología de estrella para que pueda hacerse alguna otra corrección al agregar algo de *hardware* y sea factible la estructura inicial [22], [URL29].

3.5 Preparación del lugar y medidas de seguridad.

En lo que se refiere a la preparación del lugar se espera que cuente con vigilancia para entrada de personal, ventanas de protección, ventilación adecuada, es decir una protección física del lugar. En lo referente al equipo e información se pide una lista de acceso restringida al área del servidor y a las demás áreas, creación de programas de seguridad. Encriptación de archivos, respaldos de información, antivirus, control de software y licencias, monitoreo del sistema y una auditoria al sistema [22], [URL39].

No hay que pasar por alto ninguna regla de seguridad, por muy sencilla que parezca e inofensiva que parezca [URL36], [URL15].

3.6 Instalación del Hardware.

En lo referente a la instalación del *hardware* de los *host* clientes, se instalarán según el manual del equipo [URL18], [URL29].

En la instalación de la VPN se tiene dos maneras de implementación: en mecanismos de *hardware* y los sistemas basados en *firewalls*.

Una **VPN mediante mecanismos *hardware***, se basan normalmente en *routers* con encriptación, que tienen la ventaja de ser lo más parecido a equipos *plug&play*. Su única tarea es encriptar y desencriptar las tramas que pasan a través de ellos, por lo que tienen buenas prestaciones y no introducen demasiados retardos en la red. No tienen tanta flexibilidad como los sistemas basados en *software*.

Los **sistemas basados en *Firewalls*,** son sistemas que aprovechan las ventajas del *firewall* como la restricción de acceso a la red o generación de registros de posibles amenazas, y ofrecen otras ventajas como traducción de direcciones o facilidades de autentificación fuerte. El hecho de insertar el servicio de VPN dentro de un *firewall* puede afectar en mayor o menor medida al rendimiento del sistema, lo que puede o no ser un problema dependiendo de las necesidades.

Si se convierte en un problema, algunos fabricantes de *firewalls* ofrecen procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema [URL22], [URL28], [3], [17].

3.7 Instalación del Software.

Existen fabricantes que proporcionan soluciones basadas en *hardware*, pero que incluyen clientes *software* para VPN e incluso características que sólo se encuentran en los sistemas basados en *firewalls*. La introducción del protocolo IPSec está facilitando la mezcla de distintos productos VPN [URL28], [3], [6].

Los sistemas puramente *software* son ideales en los casos en los que los dos extremos de la comunicación no pertenecen a la misma organización, o cuando aun estando dentro de la misma organización, las tecnologías de *routers* y/o *firewalls* difieren [URL31].

Esta solución permite mayor flexibilidad en cuanto a la decisión de qué tráfico enviar o no por el túnel seguro, pudiendo decidir por protocolo o por dirección, a diferencia de los sistemas *hardware*, que normalmente sólo permiten decidir por dirección. Puede ser conveniente en situaciones donde la VPN es útil en algunos casos (consultas a una base de datos) pero irrelevante en otros (navegación normal por la Web).

Es útil en los casos en los que la conexión se realiza por líneas lentas. Los sistemas *software* son difíciles de administrar, ya que se requiere estar familiarizado con el sistema operativo cliente, la aplicación VPN y los mecanismos de seguridad adecuados. Algunos paquetes VPN requieren cambios en las tablas de encaminamiento y los esquemas de traducción de direcciones [16], [17].

La instalación y configuración de la red se verá desde dos puntos [URL41]:

- Instalación y configuración del servidor VPN.
- Instalación y configuración de los clientes de acceso remoto.

En la **Instalación y configuración del servidor VPN**, para que los empleados puedan acceder a la intranet de la empresa desde fuera, el servidor VPN debe estar conectado permanentemente a Internet y además debe tener un dirección IP fija, la cual usarán los clientes de acceso remoto para iniciar la conexión VPN [17].

El servidor se conecta a Internet a través de un MODEM que estará conectado al ISP continuamente y conectado a la red LAN con una tarjeta de red. En la máquina servidor se instalará el paquete Windows 2000 Server el cual incluirá el servicio de servidor de acceso remoto (RAS) y los protocolos necesarios para la conexión (PPTP, L2TP, IPsec).

Cuando un cliente pide una conexión VPN al servidor central, el servidor VPN lo autentica y a partir de entonces se reciben paquetes del cliente, el servidor desencapsula y desencripta los paquetes y, los coloca en la red.

En la **Instalación y configuración de los clientes de acceso remoto**, [17] el equipo del cliente de acceso remoto consta de un ordenador portátil con el paquete de Windows 2000 instalado, una tarjeta PCMCIA, un teléfono móvil y un cable de datos para conectar el portátil con el teléfono. En la ranura PCMCIA del ordenador portátil elegido se insertará la tarjeta PCMCIA, necesaria para realizar la conexión teléfono- PC portátil, éste posee un MODEM por si existe la posibilidad de realizar la conexión a Internet a través de la Red Telefónica Básica, lo cual abarata más el coste de la comunicación.

Un cliente de acceso remoto realiza una conexión VPN de acceso remoto que conecta a la red privada mediante la creación de una conexión de acceso telefónico a redes, la cual incluye la dirección de Internet de la red local de la empresa, los protocolos y *software* necesarios, para realizarlo está incluido en el paquete de Windows 2000.

El servidor VPN proporciona acceso a los recursos del servidor VPN o a toda la red a la que está conectado el servidor VPN. Los paquetes enviados desde el cliente remoto a través de la conexión VPN se originan en el equipo cliente de acceso remoto.

El cliente de acceso remoto (cliente VPN) se autentica ante el servidor de acceso remoto (servidor VPN) y, para realizar la autenticación mutua, el servidor se autentica ante el cliente.

El cliente esta conectado a la red local de la empresa y aparece como un usuario más de la misma, con los mismos privilegios y recursos disponibles, sin importar en qué lugar del mundo se encuentre.

3.8 Configuración.

La arquitectura de la VPN se debe basar en elementos esenciales de la tecnología para proteger la privacidad, mantener la calidad y confiabilidad, y asegurar la operatoria de la red en toda la empresa [URL15], [URL16], [URL17], [URL18].

Estos elementos son:

- **Seguridad**: [URL36], [URL39] uso de túneles, encripción de datos, autenticación de usuarios y paquetes, control de acceso.
- **Calidad de Servicio**: uso de colas, manejo de congestión de red, priorización de tráfico, clasificación de paquetes.
- **Gestión**: implementación y mantenimiento de las políticas de seguridad y calidad de servicio a lo largo de la VPN.

La **Seguridad** en la VPN [URL39] en un punto fundamental, es el particionamiento de las redes públicas o de uso compartido para implementar las

VPNs que son disjuntas. Esto se logra mediante el uso de túneles que no son ni más ni menos que técnicas de encapsulado del trafico.

Las técnicas que se utilizan son: GRE que permite que cualquier protocolo sea transportado entre dos puntos de la red encapsulada en otro protocolo, típicamente IP. Y L2TP que permute el armado de túneles para las sesiones PPP remotas, y por ultimo IPSec para la generación de túneles que emplea la autenticación y encriptado de datos.

La **calidad de servicio** permite la asignación eficiente de los recursos de la red pública las distintas VPNs para que obtengan una representación predecible. A su vez, las VPNs asignaran distintas **políticas de calidad** de servicio a sus usuarios, aplicación e o servicios. Las componentes tecnológicas básicas son:

- **Clasificación de Paquetes**: asignación de prioridades a los paquetes basados en la política corporativa. Se pueden definir hasta siete clases de prioridades utilizando el campo de *IP precedence* dentro del encabezado del paquete IP.
- **CAR**: garantiza un ancho de banda mínimo para aplicaciones o usuarios basándose en la política corporativa.
- **WFQ**: determina la velocidad de salida de los paquetes en base a la prioridad asignada a éstos, mediante el encolado de los paquetes.
- **WRED**: complementa las funciones de TCP en la prevención y manejo de la congestión de la red, mediante el descarte de paquetes de baja prioridad.
- **GTS**: reduce la velocidad de salida de los paquetes con el fin de reducir posibles congestiones de la red que tengan como consecuencia el descarte de paquetes. [URL15]

3.9 Pruebas a la red.

Para poder medir los resultados del diseño e implantación de una red, es necesario establecer criterios de evaluación, para ello se muestran algunos de los criterios usados para la evaluación del proyecto en la tabla 3.3 y 3.3b [1], [10], [URL36], [URL39], [URL41].

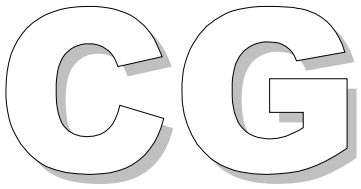
Evaluación en:	**Tenemos:**
Tiempos	Reducción del tiempo en: ☙ Uso de la red por una estación. ☙ De respuesta. ☙ De procesamiento.
Costos	Disminución del costo: ☙ Por operación anual, ☙ De mantenimiento. ☙ De inversión.
Capacidad de expansión	Adaptación de la expansión e la red. Interconexión de funciones o servicios de la compañía.
Eficacia	Eficacia de la red con relación a la precedente.
Productividad	Mejora de la productividad: ☙ De usuarios ☙ De administradores ☙ Rapidez en toma de decisiones.
Integridad	Reducción del número de errores.
Confiabilidad	Capacidad para soportar la carga de trabajo.
Rendimiento	Capacidad para cargar la carga de trabajo.
Aceptación	Aceptación de la red por: ☙ Clientes y proveedores. ☙ Usuarios. ☙ Administradores.

Tabla 3.3 Criterios para evaluar una red.

Evaluación en:	**Tenemos:**
Flexibilidad	Nuevas funciones: comunicación satelital.
Capacitación	Adaptación y actualización de los manuales de capacitación.
Calidad	Mejor calidad de: ☙ Información ☙ Productos o servicios.
Documentación	Pertinencia de la descripción de los componentes de la red como dispositivos, *software*, protocolos, circuitos, etc.
Seguridad y control	Medidas juiciosas de prevención y detección de: ☙ Errores, ☙ Fraudes ☙ Perdidas de datos ☙ Virus.
Discreción	Administración de derechos de acceso a: ☙ Grupos de usuarios ☙ Directorios ☙ Archivos

Tabla 3.3b Continuación de criterios para evaluar una red.

Conclusión General



Las redes de computadoras se han empleado para intercambiar información de manera local. Las redes se clasifican por su topología, medio físico de transmisión, su tecnología y su cobertura. A su vez cuentan con los servicios de Internet. Están basadas en una arquitectura de protocolos como TCP/IP y OSI para la comunicación entre ellas.

Las redes tienen políticas de seguridad internas como externas para proteger la información que exista dentro de la red. Hay dos tipos de seguridad, la seguridad física que se encarga del hardware y, la seguridad lógica que evita el daño al software existente del equipo y de la red. Los principales enemigos de nustra información son los virus, los piratas informáticos, los antivirus no actualizados, incluso los mismos usuarios.

El uso de un *firewall* como mecanismo de seguridad, hace más fuerte a la red contra intrusiones de cualquier tipo y dependiendo de la forma en que se programé dentro de la red, la hará "impenetrable" a los peligros que existen dentro y fuera de la red.

Una red se puede conectar a otra red en un sitio remoto a través de un enlace virtual por medio de una interred, esto se conoce como una "**Red Virtual Privada (VPN)**".

Una VPN es el sueño ideal de cualquier administrador de red, puesto que es una combinación entre la seguridad y una red privada, haciendo a las VPN una red confiable y de bajo costo que satisface las necesidades de comunicación de la organización a través de Internet.

Una VPN mantienen comunicaciones seguras (autenticación de usuario, manejo de direcciones, encriptación de datos, administración de llaves y un soporte de protocolo múltiple) tan estricta que es difícil alterar la información en el trayecto. A menos que se logre capturar la información con las llaves apropiadas, el túnel y su encriptación, es posible dañarla en su totalidad.

Dependiendo de cómo se la conectividad de una VPN, esta podrá ser VPN de Intranet, VPN de Extranet o una VPN de Acceso remoto.

El empleo de túneles para la comunicación de una VPN la hace mas segura. Y se puede crear un túnel obligatorio ó voluntario. A su vez emplea protocolos como PPTP, L2TP. IPSec, L2F.

En la arquitectura de seguridad de una VPN se emplean tecnicas para el ocultamiento de la información, ya sea por encriptación, uso de llaves, algoritmos *hash*, certificados, IPSec, EAP y EAP-TLS. Y sobre todo con una buena administración de los usuarios.

Un peligro son los *hackers* que hacen uso del *hackeo* telefónico. Un antídoto para saber si se esta siendo atacado es con el empleo de *wardialers*. El w*ardialing* hace uso de herramientas como *Toneloc*, THC-*Scan* y *PhoneSweep* para recabar información sobre el atacante, de dónde es, la hora, entre otros datos que se almacenan en un archivo para su análisis posterior y sobre todo recordar las medidas de seguridad para la marcación telefónica.

Aunque una VPN empleando PPTP la hace vulnerable, con el empleo de IPSec se evitarán futuros dolores de cabeza ó hasta que en IPSec se encuentren puertas traseras

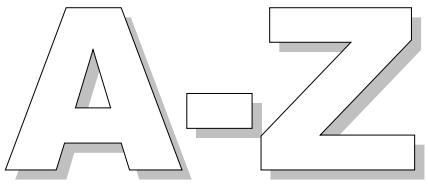
En el estudio que se hizo para llevar a cabo el diseño de una VPN en ITESA, se observó desde el inicio la imposibilidad de implantarla, debido a que este Instituto depende económicamente de la región, así como de otros organismos para beneficiar a la misma. Además de trabas tecnológicas temporales.

Se espera que este estudio sirva como base, para que en un futuro se lleve a cabo la implementación de la VPN y, dependiendo de la tecnología futura un rediseño de la red, dependiendo de las necesidades de la institución. En estos días, la instalación de una red local ya es un hecho, la conexión a Internet es demasiado lenta. Y solo el Centro de Cómputo y el área académica mantienen una conexión para el acceso a Internet. La oportunidad de una VPN, hará tanto a académicos como alumnos disfruten de los beneficios de contar con una VPN.

No hay que olvidar que una solución VPN para cualquier empresa, organización e institución reduce costos económicos en comparación con las conexiones telefónicas, de punto a punto. Así como otros costos que se han estado generando debido a la falta de una VPN en la empresa.

Entre las aplicaciones reales de una VPN están el teletrabajo y las VPN empresas que se adaptan a las necesidades de la empresa.

Siglario



A

AARP.
Protocolo de traducción de la dirección de *AppleTalk*, *AppleTalk Address Resolution Protocol.*
ADSP.
AppleTalk Data Stream Protocol.
AEP.
AppleTalk Echo Protocol.
AFP.
AppleTalk Filling Protocol.
AH.
Cabecera de Autenticación, *Authentication Header.*
ARP.
Protocolo de Resolución de direcciones.
ASP.
AppleTalk Session Protocol.
ATM.
Modo de transferencia Asíncrona, *Asynchronous Transfer Mode.*
ATP.
AppleTalk Trandsction Protocol.

C

CAR.
Committed Access Rate.
CBCP.
Protocolo de retorno de Control, *Callback Control Protocol.*
CCD.
Centro Comunitario Digital.
CHAP.
Protocolo de Autenticación de Saludo, *Challenge Handshake Authentication Protocol*
COSNET.
Consejo Nacional de Educación y Tecnología.

D

DDP.
Protocolo de entrega de datagramas, *Datagram Delivery Protocolo.*
DES.
Encriptación de datos estandar, *Data Encryption Standard.*
D.I.X.
Digital Intel Xerox.
DMZ.
Zonas desmilitarizadas, *Demilitarized Zone.*
DNA.
Arquitectura de Red Digital, *Digital Network Architecture.*
DQDB.
Distributed Queue Dual Bus.

E

EAP.
Protocolo de Autenticación extensible, *Extensible Authentication Protocol.*

EGP.
Protocolo *Gateway* externo.
ELAP.
Ethernet Link Address Protocol.
ESP.
Encapsulación de carga segura,
Encapsulating Security Payload.
ET.
Estación Terminal.

F

FDDI.
Fiber Distributed Data Interface.
FEP.
Front End Processor.
FPS.
Servidor Apoderado del *firewall,*
Firewall Proxy Server.
FTP.
Protocolo de transferencia de archivos,
File Transfer Protocol.

G

Gopher.
Ardilla de tierra, del ingles *go for*, ve y trae.
GRE.
Generic Routing Encapsulation.
GTS.
Generic Traffic Shaping.

H

HTTP.
Hyper Text Transfer Protocol.

I

ICMP.
Protocolo de control de mensaje Internet.
IHEMSYS.
Instituto Hidalguense de Educación Media Superior y Superior.
IP.
Protocolo de Internet,
Internet Protocol.
IPCP.
Protocolo de Control IP.
IPSec.
IP Security.
IPX.
Internet Packet Exchange.
ISP.
Proveedor de Servicio Independientes,
Independent Service Providers.
ISS.
Rastreador de Seguridad en Internet,
Internet Security Scanner.
ITESA.
Instituto Tecnológico Superior de Apan.

L

LAN.
Red de Área Local.
LAP.
Acces Protocol Layer.
L2F.
Layer Forwarding 2.
L2TP.
Layer 2 Tunneling Protocol.

M

MAC.
Técnica de Acceso al Medio.
MAN.
Red metropolitana.
MAU.
Unidades de Acceso Multiestación.
MPPC.
Microsoft Point-to-Point Encrypted.

MPPE.
Encriptación de Punto a punto de Microsoft,
Microsoft Point-to –Point Encryption
MSCHAP.
Protocolo Microsoft de Autenticación,
Microsoft Challenge Hanshake Authentication Protocol.
MTU.
Maximum Transmission Unit

N

NAS.
Servidor de Acceso a la Red,
Network Access Server.
NAT.
Network Address Translation.
NBP.
Name Binding Protocol.
NCP.
Protocolos de Control de Red.
NIC.
Network Interface Card.
NIS.
Network Information System.
NFS.
Network File System.
NTP.
Network Time Protocol.

O

OPSF.
Protocolo Abrir la vía más corta primero.
OSI.
Open System Interconnection.

P

PAC.
Concentrador de acceso de PPTP,
PPTP Access Concentrator.
PAP.
Protocolo de Autenticación de Contraseña, *Password Authentication Protocol.*
PAP.
Protocolo de acceso de impresión,
Printer Access Protocol.
PDC.
Controlador del Dominio Primario,
Primary Domain Controller.
PNS.
Servidor para red de PPTP,
PPTP Network Server.
POP.
Punto de presencia.
PPP.
Protocolo de Punto a Punto.
PPTP.
Protocolo de Túnel Punto a Punto,
Point-to-Point Tunneling Protocol.

R

RADIUS.
Remote Authentication Dial-in User Service.
RARP.
Protocolo de direcciones invertidas.
RAS.
Servidor de Acceso Remoto,
Remote Access Server.
RIP.
Protocolo de información de encaminamiento.
RPC.
Procedimiento de llamada remota,
Remote Procedure Call.
RTMP.
Routing Table Maintenance Protocol.

S

SA.
Asociación Segura,
Security Assosiation.

SATAN.
Herramienta para Análisis de Seguridad para Auditar Redes,
Security Analysis Tool for Auditing Networks.
SLIP.
Protocolo de Internet Lineal de Serie.
SMTP.
Protocolo de transferencia de correo,
Simple Mail Transfer Protocol.
SNA.
Arquitectura del sistema de red,
System Network Architecture.
SNMP.
Protocolo de administración de red,
Simple Network Management Protocol.
SOCKS.
Protocolo de seguridad de red,
Networks Security Protocol.
SPI.
Índice de parámetro de seguridad,
Security Parameter Index.

T

TCP.
Protocolo de control de transmisión,
Transmission Control Protocol.
TCP/IP.
Protocolo de transmisión de control y protocolo de Internet,
Transmision Control Protocol/Internet Protocol.
TLAP.
Protocolo de dirección de enlace de *Token Ring*,
Token Ring Link Address Protocol.

U

UDP.
Protocolo de datagrama de usuario.

V

VAN.
Red de Valor Agregada,
Value Added Network
VPN.
Red Virtual Privada,
Virtual Private Network.

W

WAN*.*
Red de área extensa.
WFQ.
Weighted Fair Queuing.
WRED.
Weighted Random Early Detection.
WWW.
Red Mundial Amplia,
World Wide Web.

X

XNS.
Sistema de red Xerox,
Xerox Network System.

Z

ZTP.
Protocolo de información de zona,
Zone Information Protocol.

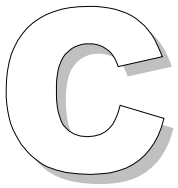
Bibliografía

B

[1]	Long, L. (1995) "Introducción a las computadoras y al Procesamiento de la Información". Editorial Prentice Hall Hispanoamericana. 4ta. Edición. México. pp. 211-248, 485-511.
[2]	Black, U. (2000) "Redes de computadores: Protocolos, normas e interfaces". Editorial Prentice Hall. 2da. Edición. España. Pp. 1-31, 159-200, 349-383, 429-488.
[3]	Rábago, J. (2001) "Guía practica para usuarios: Introducción a las redes locales". Edición Grupo Anaya multimedia. 2da. Edición. Pp. 21-258.
[4]	Rodríguez, J. (1996) "Introducción a las Redes de área local". Editores McGraw Hill Interamericana. México. 105-200
[5]	Raya, J. (1995) "Redes Locales y TCP/IP". Editorial Ra-ma. España. Pp. 1-46, 61-66, 93-147.
[6]	Parker, T. (1995) "Aprendiendo TCP/IP en 14 días". Editorial Prentice Hall Hispanoamericana. México. pp. 1-26, 29-59, 63-86, 89-111, 247-261.
[7]	Beltrão, J. (1991) "Redes Locales de Computadoras: Protocolos de alto nivel y evaluación de prestaciones". Editorial McGraw Hill/Interamericana. España. Pp. 7-45, 48-92, 95-217.
[8]	St-Pierre, A. (2001) "Redes Locales e Internet: Introducción a la comunicación de datos". Editorial Trillas. México. pp. 5-77, 83-208, 215-263.
[9]	Comer, D. (2000) "Diseño e Implementación: Interconectividad de Redes con TCP/IP". Editorial Pearson. Volumen II. México.
[10]	Raya, J. (2003) "Redes Locales" Editorial Ra-ma. 2da. Edición. México. pp. 37-189.
[11]	Halscill, F. (2000) "Comunicación de datos, redes de computadoras y sistemas abiertos". Editorial Addison Wesley Longman. 4ta. Edición.
[12]	Alonso, M. (1998) "TCP/IP en Unix: Programación de aplicaciones distribuidas". Editorial Ra-ma. España. pp. 8-20
[13]	Baños, R. (2002) "Como enseñar a investigar en Internet". Editorial Trillas. México. pp. 107-120.
[14]	Ureña, L. (1999) "Fundamentos de informática" Editorial Ra-ma. España. pp. 257-286.
[15]	Mc Clure, S. (2001) "Hackers: Secretos y Soluciones para la seguridad de las redes". Editorial McGraw Hill/Osborne.

[16]	Comer, D. (1995) "Internetworking with TCP/IP Principes, protocols & architectures". Editorial Prentice Hall. Volúmen 1.
[17]	Kolesnikov. (2002) "Redes Virtuales con Linux". Editorial Prentice Hall. 1ra. Edición. España.
[18]	Ziegler, R. (2000) "Guia Avanzada: Firewalls Linux". Editorial Prentice Hall. España. Pp. 3-256, 353-362.
[19]	Mediavilla, M. (1998) "Seguridad en Unix". Editorial Ra-ma. España. pp. 15-24.
[20]	Gratton, P. (1998) "Protección informática: en datos y programas; en gestión y operación; en equipos y redes; en internet". Editorial Trillas. México. pp. 31-263
[21]	Direccion General de Bibliotecas e Instituto de la Comunicación Educativo. (2004) "Introducción al Programa de Acceso a Servicios Digitales en Bibliotecas públicas: Manual para el bibliotecario". Editorial Hill & Melinda Gates Foundation. 1ra. Edición. México. pp. 15-21, 33-34.
[22]	Roque, E. (2006) "Plan táctico y operativo para el rediseño del Laboratorio de informática el Plantel Atotonilco de Tula, hgo., COBAEH". Universidad Autónoma del Estado de Hidalgo. México. pp. 118-128.
[23]	Zemánek, J (2001)"Cracking sin secretos: Ataque y Defensa de Software", Editorial McGraw Hill. México

Cibergrafía



[URL1] Naranjo, A. "Redes de computadoras". Recuperado Abril 2005, de http://www.monografias.com/trabajos5/redes/redes.shtml

[URL2] Monterrosas, A. "Comunicación de Datos". Recuperado Enero 2003, de http://www.monografias.com/trabajos3/comunidatos/comunicdatos.shtml

[URL3] Emiro, J. "Introducción a Redes". Recuperado Enero 2003, de http://www.monografias.com/trabajos/introredes/introredes.shtml

[URL4] González, L."Redes de computadoras". Recuperado Junio 2005, de http://www.monografías.com/trabajos24/redes-computadoras/redes-computadoras.shtml

[URL5] "Curso de Redes de Computadoras II: Protocolos de Red". Recuperado Enero 2003, de http://mapaches.itz.edu.mx/~memo/redesII.html

[URL6] "Protocolos de Red". Recuperado Enero 2003, de http://www.garriwp.com/protocolos_red/

[URL7] Arámbula, J. "Seguridad en redes de computadoras". Recuperado Enero 2003, de http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml

[URL8] Mendoza, A. "Virus y Antivirus". Recuperado Noviembre 2004, de http://monografias.com/trabajos18/virus-antivirus/virus-antivirus.shtml

[URL9] Per System S.A. (1986-2006) "Hackers, crackers, piratas, pheakers, spoofer y delincuentes informáticos". Lima, Perú. Recuperado Febrero 2003, de http://www.perantivirus.com/sosvirus/general/hackers.htm

[URL10] Raulex. "Seguridad de redes: Firewalls". España. Universidad de Alcalá de Henares. Recuperado Febrero 2004, de http://apuntes.rincondelvago.com/seguridad-de-redes_firewall.html

[URL11] Cotarelo, G. "Redes y conectividad: Firewalls". México. Recuperado Febrero 2003, de http://apuntes.rincondelvago.com/arquitectura-de-firewalls.html

[URL12] Villafañe, J. "Arquitectura de Firewalls". Argentina. Universidad Católica de Salta. Recuperado Abril 2004, de http://apuntes.rincondelvago.com/arquitectura-de-firewalls.html

[URL13] "Firewalls y NAT en Linux" Recuperado Mayo 2004, de http://www.teredes.com/josemi/documents/firewall.pdf

[URL14] Cisco Systems Latinoamericana, "Seguridad y VPNs". España. Recuperado Mayo 2004, de

http://www.cisco.com/global/IE/solutions/ent/awid_solutions/vpn_home.shtml
[URL15] Espinosa, M. "Redes Virtuales Privadas". México. Recuperado Junio 2003, de http://apuntes.rincondelvago.com/redes-virtuales-privadas.html
[URL16] Koleta. "Red privada virtual". Universidad de Jaén. España. Recuperado Marzo 2004, de http://apuntes.rincondelvago.com/red-privada-virtual.html#
[URL17] Cea, J. (1997-2006) "Redes Privadas Virtuales". Argo: Redes y Servicios Telemáticos S.A. España. Recuperado Diciembre 2001, de http://www.argo.es/~jcea/artic/vpn1.htm
[URL18] "Conexiones de red privada virtual (VPN)". España. Recuperado Mayo 2003, de http://www.microsoft.com/windows2000/es/advanced/help/conn_vpn.htm
[URL19] Farrasa. "Tecnología VPN". Colombia. Recuperado Marzo 2002, de http://apuntes.rincondelvago.com/tecnologia-vpn.html
[URL20] Howstuffwoks, Inc. (1998-2006) "How Virtual Private Networks Work". Recuperado Julio 2004, de http://computer.howstuffworks.com/vpn1.htm
[URL21] Imagen Interactive. (2002) "Undestanding Virtual Private Networks". A Foundation In Security, Communicatte visualy. Maine, US. Recuperado Junio 2004, de http://www.imagen-interactive.com/assets/powerpoint/vpn_introduction_file/frame.htm
[URL22] Mako. "Redes Privadas Virtuales". Chile. Universidad Mayor. Recuperado Mayo 2004, de http://apuntes.rincondelvago.com/redes-privadas-virtuales.html
[URL23] IETF. "Layer Two Tunneling Protocol (L2TP)". Lucent Technologies. Cisco Systems. Recuperado Marzo 2005, de http://www.ietf.org/rfc/rfc3931.txt
[URL24] Hevia, M. (1997) "Virtual Private Networks (VPN)". Argentina. Recuperado Septiembre 2002, de http://monografias.com/trabajos12/monvpn/monvpn.shtml
[URL25] VPNC: Virtual Private Network Consortium. (1999) "VPN Protocols". VPN Consortium. CA, USA. Recuperado Julio 2003, de http://www.vpnc.org/vpn-standards.html
[URL26] Cisco Systems. (1992-1999) "L2F". Cisco System. Recuperado Mayo 2005, de http://www.cisco.com/warp/public/732/L2F/index.html
[URL27] IHEMSYS. "ITESA. Instituto Tecnologico Superior de Apan". IHEMSYS. México. Recuperado Enero 2005, de http://www.ihemsys.gob.mx/ITESA.htm
[URL28] Cisco. (1992-2005) "Soluciones VPN". Cisco System. México. Recuperado Febrero 2005, de http://www.cico.com/mx/svpn/index.shtml
[URL29] Dobarro, A. (2003) "Cómo crear una red privada virtual (VPN) en Windows XP". Recuperado Marzo 2003, de http://www.elrincondelprogramador.com/default.asp?pag=articulos/leer.asp&id=55
[URL30] "Centro Comunitario Digital. La respuesta a tus necesidades". México. Recuperado Abril 2005, de http://www.e-mexico.gob.mx/wb2/eMex/eMex_Ubica_tu_CCD
[URL31] Maldonado, F. (2003) "Las Redes de Computadoras". Venezuela. Recuperado

Junio 2003, de http://www.ing.ula.ve/~mfrand/

[URL32] Nodo50.net (2000)"Introducción a Internet: Origen y Evolución de internet" Recuperado Febrero 2002, de http://www.nodo50.org/manuales/internet/1.htm

[URL33] Prime Publicaciones electrónicas – copyright (1998-2005) "DARPA y la historia de Internet". Recuperado Marzo 2005, de http://www.paralibros.com/passim/p20-tec/pg2058dr.htm

[URL34] Mundo VPN. "Cabecera de Autenticación" Recuperado Octubre 2001, de http://mundovpn.com/queesvpn_glo.html/#repe

[URL35] ANSI. "American Nacional Standards Institute -ANSI" Recuperado Noviembre 2001, de http://www.ansi.org/

[URL36] Microsoft. "Glosario de Seguridad y Privacidad". Recuperado Febrero 2002, de http://www.microsoft.com/seguridad/glosario/glossary_p.asp

[URL37] Cisco. "L2TP". (Junio 16, 2003) Cisco System. Recuperado Mayo 2004, de http://cisco.com/univercd/cc/td/doc/product/software/ios120/120newft /120t/120t1/l2tp.htm

[URL38] Prime Publicaciones electrónicas – copyright (1998-2005) "Historia de Internet-Cronología abreviada". Recuperado Marzo 2005, de http://www.paralibros.com/passim/p20-tec/pg2058ei.htm

[URL39] Cisco System. "VPN Seguridad". Cisco Systems Latinoamericana. Recuperado Mayo 2002, de http://www.cisco.com/global/LA/productos/sol/emp/grandes/seguridad.shtml

[URL40] Esdras. "Hackers". Universidad de Córdoba, España. Recuperado Junio 2002, de http://apuntes.rincondelvago.com/hackers_5.html

[URL41] "Estudio de la VPN". Recuperado Octubre 2001, de http://redes-linux.all-ione.net/manuales/vpn/Estudio_VPN.pdf

[URL42] Cisco System. "Seguridad de la red". Cisco Systems Latinoamericana. Recuperado Noviembre 2001, de http://www.cisco.com/global/LA/productos/sol/red/seguridad.shtml

[URL43] "Comunicación de datos". Recuperado Enero 2003, de http://html.rincondelvago.com/comunicacion-de-datos_2.html#

[URL44] Fontanet, J. (2002) "Monografía sobre el desarrollo de una tecnología virus, antivirus y efectos emocionales en el área de trabajo". Recuperado Marzo 2005, de http://monografias.com/trabajos12/virus/virus.shtml

[URL45] Bustillos, A. "Las Redes" Recuperado Marzo 2005, de http://www.monografias.com/trabajos15/redes_clasif/redes-clasif.shtml

[URL46] Morales, E. "Las redes de computadoras". Recuperado Marzo 2005, de http://www.monografias.com/trabajos18/redes-computadoras/redes-computadoras2.shtml#biblio

Glosario

A

Abuso de privilegio. Se produce cuando un usuario realiza una acción que no tiene asignada de acuerdo a la política organizativa o a la ley.

***Accountig*.** Registro o contabilidad de las operaciones.

Aceite de serpiente,* Snake oil*. El nombre tiene su origen en las curas de charlatán o buhonero del siglo XIX, en los aceites milagrosos que lo curaban todo. En criptografía, se aplica a un producto cuyos desarrolladores describen con terminología técnica engañosa, inconsistente o incorrecta.

***AH,* Authentication Header.** Encabezamiento contenido en IPSEC que se utiliza para verificar que el contenido de un paquete no ha sido modificado durante la transmisión. AH firma digitalmente el contenido completo de cada paquete, protegiendo la red contra tres tipos de ataques:

1. Repetición o Reply: el atacante captura los paquetes, los guarda y los vuelve a enviar, permitiendo que se introduzca en una máquina cuando ya no está en la red, y AH lo evita incluyendo un hash en clave del paquete, para que nadie pueda reenviar los paquetes.
2. Manipulación o Tampering: el mecanismo del hash en clave del IPSEC asegura que nadie haya cambiado el contenido de un paquete después de ser enviado.
3. Engaño o Spoofing: AH autentica por dos vías, de modo que el cliente y el servidor puedan verificar la identidad de uno y otro.

***Algoritmo,* Algorithm.** Procedimiento. Un algoritmo enb criptografía se refiere a un procedimiento especial para encriptar o desencriptar datos. Algunos algoritmos específicos son DES, IDEA, RC4, SKIPJACK.

***Algoritmo asimétrico,* Asymmetric algorithm**. Algoritmo que utiliza dos claves diferentes, una para encriptación y otra para desencriptación. La primera se llama clave pública y la segunda clave privada. Un ejemplo es el algoritmo RSA.

***Algoritmo de clave pública,* Public key algorithm.** Algoritmo que utiliza dos claves diferentes, una para encriptación y otra para desencriptación. La primera se llama clave pública y la segunda clave privada. Un ejemplo es el algoritmo RSA. También llamado "algoritmo asimétrico".

***Algoritmo de clave secreta,* Secret key algorithm.** Algoritmo de cifrado que utiliza la misma clave para cifrar y descrifrar datos. También se le llama "algoritmo simétrico".

***Algoritmo de flujo,* Stream cipher.** Algoritmo que trabaja sobre un flujo de datos continúo en lugar de procesar los bloques de datos uno por uno. También se encuentra como "cifrado simétrico continuo", "algoritmo de cifrado en flujo" o "codificador de flujo".

***Algoritmo simétrico,* Symmetric algorithm.** Algoritmo de cifrado que utiliza la misma clave para cifrar y descrifrar datos. También se le llama "algoritmo de clave secreta".

***Amenazas pasivas*, Passive attack.** Ataque que afecta a la confidencialidad de la información, en el que los datos son observados pero no modificados. Es el tipo de ataque llevado a cabo por Peeping Tom.

ANSI, American National Standards Institute. Organización dedicada a la creación y publicación de estándares para varias industrias [URL35].

ANSI X9.17
Estándar de ANSI para intercambio de claves secretas utilizando el algoritmo DES.

Anti-repetición, **Anti-replay.** Función de seguridad que detecta un ataque por sustitución o repetición. Este consiste en copiar un paquete autenticado y retransmitirlo después. Por lo tanto detecta cuándo un mensaje ha sido recibido más de una vez.

Ancho de banda. Termino que use utiliza para describir la velocidad máxima a la que un determinado dispositivo puede transferir datos. El ancho de banda se mide en kilobits por segundo o megabits por segundo.

ARPANET. Aplicación escrita en JAVS y compilada.

Ataque interior. Es un ataque originado desde dentro de la propia red protegida.

Autentificación. Proceso que determina la identidad de un usuario que está intentando acceder a un sistema.

ATM. Asyncronous Transmisión Mode. Modo de transmisión Asincrona, sistema de transmisión de datos usado en bada ancha para aprovechar al máximo la capacidad de una linea. Se trata de un sistema de conmutación de paquetes.

Autenticación. Proceso de asegurar, tanto como sea posible, que los acceso y mensajes provenientes de un usuario(como una contraseña o correo electrónico) se originan de una fuente autorizada.

Autenticidad, authenticity. La habilidad para asegurar que la información dada, fue de hecho producida por la entidad cuyo nombre lo lleva y que no fue falsificada o modificada.

Autokey. Bloque de cifrado en el cual el cifrado es usado para generar la llave del flujo. Tambien llamada modo de retroalimentación de producción (output feedback (OFB)).

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

Aplicación crítica, **Critical application.** Aplicación informática en la que un atacante puede haber causado daños severos, incluída su desactivación.

Aplicación de bajo riesgo, **Low risk application**. Aplicación informática que, si se ejecuta en un sistema, no causa daños serios al mismo.

Aplicación de alto riesgo**, High risk application**. Aplicación informática que ha sufrido un incidente de seguridad informática y por tanto los datos que maneja pueden sufrir pérdidas significativas. También se llama así a aplicaciones que, una vez abiertas, pueden hacer que el usuario sea vulnerable a brechas de seguridad.

Aplicación de riesgo medio, **Medium risk application**. Aplicación en la que una obstrucción u otro problema de seguridad puede causar pérdidas a la empresa, y algunas de estas pérdidas pueden ser afrontadas bajo control.

Aplicación de encripción. **application encryption.** Funciones criptográficas construidas dentro de los protocolos de comunicación para una aplicación

especifica, como el correo electrónico. Incluyendo por ejemplo: PEM, PGP, y SHTTP.

Aplicación de software, *application software.* Software que provee un servicio a un usuario, como un opuesto de software de nivel inferior que hace útiles a los servicios posibles.

***ARPA*, Advanced Research Projects Agency**. Agencia de Proyectos de Investigación Avanzados. Organismo del Departamento de Defensa de los Estados Unidos que promueve la investigación en áreas de interés para aplicación militar. ARPA, en concreto ARPANET, dio lugar a lo que hoy conocemos como Internet. [URL33]

ARPANET. Red de comunicación por ordenador desarrollada por ARPA, que representa el germen de la moderna Internet. Muchos de sus protocolos se adaptaron para lo que hoy conocemos por Internet, incluyendo los protocolos para e-mail, FTP y conexiones de terminales remotos. Diseñada, implementada y puesta en funcionamiento por Bolt, Baranek y Newman.

ASN.1, **Abstract Syntax Notation (1)**. Lenguaje de definición de notaciones que describe datos que se utilizan en muchos otros estándares. Se trata de un conjunto de expresiones que se presentan en la forma: nombre::= regla.

***Ataque activo,* Active Attack**. Ataque a un sistema a través de cual, se pueden introducir informaciones falsas, o producir daños en las informaciones.

***Ataque por fuerza bruta,* Brute force cracking.** Proceso por el que se trata de deducir una clave criptográfica intentando todas las posibilidades razonables. También se le llama "craqueo por el método elemental" o "crack por fuerza bruta".

***Ataque programado,* Programmed attack.** Ataque en un dispositivo informático o protocolo que puede ser incorporado a un programa de software. Estos ataques son simples y pueden ser utilizados por atacantes con poca experiencia.

***Autenticación,* Authentication.** El proceso que nos permite verificar con una seguridad razonable que un nombre de usuario o dispositivo que está pidiendo acceso realmente pertenece a alguien. Se refiere a los métodos que aseguran que cualquier conexión a la red sea autorizada.

*A**utoridad de certificación,* Certification authority**. Entidad que permite la creación de certificados digitales creando certificados de claves públicas.

B

Back door. Un agujero de seguridad en un sistema que permite el acceso continúo de un intruso.

***Bailey the Switcher**.* Ataca el tráfico de redes para modificar el contenido de los mensajes de otras personas.

Bastion Host. 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. Normalmente, un bastion host está ejecutando alguna aplicación o sistema operativo de propósito general (como: UNIX o WNT) más que un sistema operativo de firewall.

Brecha de seguridad. *Entering wedge.* Debilidad de un sistema criptográfico u otro sistema de seguridad que proporciona al atacante una forma de romper algunos de los sistemas de protección.

Bridges, *puentes.* Permiten dos cosas: primero, conectar dos o más redes entre sí, aún teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red. Segundo, segmentar una red en subredes, mejorando la circulación de la información en tramos muy congestionados y evitando los cuellos de botellas en donde existan demasiados nodos. Los puentes se pueden crear incorporando una segunda tarjeta de red dentro del mismo servidor. Existen dos tipos de puentes: locales y remotos. Los puentes locales sirven para segmentar una red y para interconectar redes que se encuentran en un espacio físico pequeño, mientras que los remotos permiten interconectar redes lejanas.

Browser. Es la aplicación software (application software) del cliente para accesar datos en la WWW.

Brute force cracking.El proceso de tratar de recuperar una llave encriptada para intentar todas las posibilidades razonables,

Bucket brigade. Ataque contra un intercambio entre claves públicas en el que el atacante sustituye su propia clave pública con la clave pública requerida. También se le llama "brigada de cubos" o "brigada de bomberos". Además se le llama ataque "Man-in-Middle" o MIM.

Bufer. El buffer es un espacio de memoria que se utiliza de sistema de almacenamiento intermedio y provisional entre los dispositivos de un computador. Como puede ser el caso de la memoria que es enviada a una impresora o en los casos de la necesidad de tener memoria en el buffer para prepararse a enviar o recibir determinada información a la espera de que el equipo receptor tenga tiempo suficiente para recibirlo o procesarlo sin bajar el rendimiento de la transferencia.

Bypass. Defecto en un sistema de seguridad que permite que los mensajes violen los mecanismos de seguridad. En Criptografía se refiere a un método de funcionamiento que permite pasar texto en claro (plaintext) a través de él sin

modificarlo. Este método sirve para poder efectuar pruebas desde un terminal de datos.

Byte. Unidad elemental de memoria. Apenas se usa.

C

Caballo de Troya, Trojan horse. Programa con funciones secretas que accede subrepticiamente a la información sin el conocimiento del usuario, normalmente para violar las protecciones de seguridad. También llamado genéricamente "Troyano".

Cabeceras, Headers. Información contenida en la parte inicial de un mensaje enviado a través de una red de ordenadores. Las cabeceras contienen información utilizada para enviar y procesar correctamente los datos que se envían, como longitud, claves, etc. También se llaman "encabezamiento" y "encabezados".

CAPSTONE. Circuito integrado, también conocido como MYK-80, que utiliza el estándar EES e incorpora funciones criptográficas como el uso del algoritmo SKIPJACK, y del algoritmo de firma digital (DSA). Proporciona funciones criptográficas útiles para comercio electrónico y otras aplicaciones. La primera aplicación del chip fue la tarjeta Fortezza. Ya no se fabrica.

CAST, Carlisle Adams y Stafford Tavares. Algoritmo de encriptación criptográfica que es una parte opcional de algunos estándares. Ha sido patentado por Entrust Technologies, quienes permiten su uso libre.

CBC, Cipher Block Chaining. Literalmente, cifrado en bloque encadenado. Modo de cifrado en bloque que combina el bloque previo de texto cifrado con el bloque actual o texto en claro antes de encriptarlo. Es especialmente útil para encriptar ficheros, donde incrementa significativamente la seguridad por encima de ECB. Ampliamente utilizado.

CCITT, Consulting Committee, International Telephone and Telegraph. Literalmente, Comité Consultivo Internacional sobre Telegrafía y Telefonía. Organización internacional encargada de establecer estándares y normas en materia de telefonía y sistemas de comunicación.

CERT, Computer Emergency Response Team. Organización estadounidense formada por DARPA en 1988, que recopila y distribuye información sobre incidentes de seguridad informática y problemas de software relacionados con redes de uso público como Internet. URL: http://www.cert.org/.

Certificado, Certificate. Bloque de datos de formato especial cifrado con una firma digital proporcionada por la autoridad de certificación. Contiene una clave pública y el nombre de su propietario.

CFB, Cipher FeedBack. Modo de cifrado en bloque que utiliza un registro de desplazamiento previamente encriptado mediante cifrado en bloque para generar la clave que encripta el próximo bloque de texto cifrado. También se llama CTAK.

CIAC, Computer Incident Advisory Capability. Organismo del Departamento de Energía de los Estados Unidos que registra e informa de eventos y situaciones sobre seguridad informática. URL: www.ciac.org/ciac/.

Cifrado, Cipher. Procedimiento de seguridad que transforma una información en texto en claro en otra en texto cifrado mediante un algoritmo criptográfico. También llamado "cifra".

Cifrado autoclave, Autokey cipher. Modo de cifrado en bloque en el que el cifrado se utiliza para generar el flujo de claves. También se le llama "modo de salida realimentada o output feedback (OFB)", "cifra con autoclave" o "cifra en serie".

Cifrado en bloque, Block cipher. Cifrado que encripta datos en bloques de un tamaño fijo y por separado. Ejemplos: DES, IDEA, y SKIPJACK. También llamado "cifra en bloque".

Cifrado Vernam, Vernam cipher. Cifrado desarrollado para encriptar tráfico en teletipos utilizando el exclusive or de los bits de datos y los bits de clave. Es un sistema común para aproximarse a la construcción de algoritmos de flujo.
Cifrar, Encipher. Convertir texto en claro en texto cifrado. También se dice "encriptar" (encrypt) y "codificar" (encode).

Ciberespacio. El mundo de las computadoras y la sociedad entorno a éste. Normalmente se refiere a todo lo relacionado con Internet.

Clave, Key. Parámetro generado en conjunción con un algoritmo para encriptar o desencriptar información con el fin de validarla, autenticarla, cifrarla o descifrarla.

Clave de datos, Data key. Clave criptográfica utilizada para la autenticación o para la encriptación y desencriptación.

Clave de sesión, Session key. Clave criptográfica utilizada para la autenticación o encriptación y desencriptación de datos por un periodo limitado de tiempo, normalmente sólo para una sesión de comunicación entre dos usuarios. Cuando la sesión termine, la clave será descartada y se establecerá una nueva cuando se abra una nueva sesión. También se le llama "clave de datos".

Clave privada, **Private key.** Clave utilizada en cifrado de claves públicas que pertenece a un usuario individual y sólo es conocida por él.

Clave pública, Public key. Clave utilizada en cifrado de claves públicas que pertenece a un usuario pero se conoce públicamente. También se pueden utilizar

las claves públicas para encriptar datos que sólo el propietario de la clave puede desencriptar.

Clave secreta, Secret key. Clave cifrada que se utiliza en un algoritmo de clave secreta (simétrico) para cifrar y descifrar un mensaje.

Cliente, Client. Se refiere a la entidad informática dentro de una red que necesita utilizar recursos de otras entidades en la misma red. El software cliente generalmente se instala en ordenadores personales conectados y se usa para que éstos contacten con los servidores para recuperar información o realizar otras actividades.
Ordenador que se conecta a Internet para recibir información de la Red.

CLIPPER. Circuito integrado con funciones de cifrado para voz y teléfono que utiliza el cifrado SKIPJACK y el EES. El gobierno de los Estados Unidos intentó hacerlo obligatorio sin éxito y ya no se fabrica.

Codificar, Encode. Convertir texto en claro en texto cifrado. También se dice "encriptar" (encrypt) y "cifrar" (encypher)

Compresión, Compression. Proceso utilizado para eliminar la redundancia de un mensaje plano. Mejora el funcionamiento de la red y optimiza el almacenamiento.

Confidencialidad, Confidentiality. Servicio de seguridad que asegura que una información no sea descubierta ni esté disponible para usuarios, entidades o procesos no autorizados.

Configurar. Definir opciones y parámetros para el correcto funcionamiento de un programa o para ajustar a nuestras necesidades el modo de operar del ordenador.

Conmutación de paquetes, Packet switching. Proceso por el que los datos se separan en paquetes para ser transmitidos. Cada paquete contiene la información (dirección de origen, dirección de destino), para viajar al mismo sitio y volver a unirse con los paquetes emparentados. Esto permite que los paquetes viajen del origen al destino por cualquier ruta inmediatamente disponible, y paquetes diferentes del mismo mensaje pueden tomar diferentes rutas, sin tener que viajar como una secuencia de datos, como en la alternativa tradicional.

Contraseña. Es una clave secreta que sólo debe conocer el propietario de un acceso a un ordenador o de una cuenta de correo electrónico o de una cuenta de conexión a Internet, el Nombre de Usuario (Login) siempre va unido a la contraseña (Password). Esto significa que cuando solicitamos acceso a un ordenador en Internet, se nos pedirán tanto el Nombre de Usuario como la contraseña. Esta es la norma de seguridad establecida para acceder a sistemas privados. Si se introduce un Nombre de Usuario o una Contraseña incorrecta, no se permitirá la entrada al sistema.

Contenido ejecutable, Executable contents. Datos cuyo contenido representa un programa de ordenador capaz de modificar datos persistentes en un host.

Contraseña, Password o Passcode. Palabra o cadena de caracteres secretos que un medio automático reconoce con el fin de autenticar a un usuario para permitirle acceso a información restringida. También llamada "clave".

Contraseña de un sólo uso, One time password. Contraseña que sólo puede utilizarse una vez, normalmente creada por software especial de generación de contraseñas o por un testigo de hardware. También llamada "contraseña de utilización única", "contraseña desechable", "contraseña de uso de una sola vez", "clave de un solo uso" o "clave de uso único".

Contraseña reutilizable, Reusable password. Contraseña que puede ser utilizada una y otra vez, en oposición a la contraseña de un solo uso. La mayor parte de las contraseñas que se utilizan hoy son contraseñas reutilizables.

Controladores. Ficheros que contienen la información que necesita un ordenador para manejar adecuadamente un periférico, o sea para saber como transmitir información entre el periférico y la propia computadora.

Controlador de dispositivos, Device driver. Componente de software que controla un dispositivo periférico. Para dispositivos de enlace de datos, gestiona el proceso de enviar y recibir datos a través del mismo.

Cookie. Pequeño trozo de datos que entrega el programa servidor de HTTP al navegador WWW para que este lo guarde. Normalmente se trata de información sobre la conexión o los datos requeridos, de esta manera puede saber que hizo el usuario en la ultima visitan.

Cortafuegos, Firewall. Mecanismo (desde un simple router a varias redes en serie) utilizado para separar una máquina o subred del resto, aplicando reglas de control al tráfico de red que fluye en ambas direcciones para proteger la máquina o subred de acciones o protocolos externos que puedan representar una amenaza para su seguridad. La mayoría de los que hay en el mercado se fabrican para manejar protocolos de Internet.

Correo Electrónico. Servicio de Internet que nos permite enviar y recibir cartas a otros usuarios de Internet por medio de la Red. la recepción es casi instantáneas.

Cracker. Navegante de Internet que intenta piratear programas o introducir virus en otros ordenadores o en la Red. Otra definición: Individuo con amplios conocimientos informáticos que desprotege, piratea programas o produce daños en sistemas o redes.

Craqueo, Cracking. Proceso de violación de una medida de seguridad. Craquear una clave es un intento de recuperar el valor de la misma. Craquear texto cifrado es un intento de recuperar el correspondiente texto en claro. También se encuentra como "crack".

Criptoanálisis, Cryptanalysis. Técnicas de ataque orientadas a la recuperación de claves criptográficas o texto en claro sin conocer el sistema de cifrado o la clave. En particular se aplica a la obtención de textos en claro a partir de la intercepción de textos cifrados.

Criptoanálisis diferencial, Differential cryptanalysis. Técnica de ataque de un cifrado que consiste en utilizar texto en claro escogido para buscar patrones en el texto cifrado.

Criptografía, Criptography.

1. Rama de la ciencia que estudia las técnicas de mantenimiento de la seguridad de los datos, por las que dos entes pueden comunicarse de forma segura a través de un canal inseguro. Tiene dos aplicaciones principales: privacidad (prevención de uso no autorizado de datos) y autenticación (comprobación de la identidad de un usuario para poder acceder a los datos).
2. Mecanismo de protección de información mediante la aplicación de transformaciones para hacerla difícil de descifrar sin tener conocimiento de la clave utilizada.

Criptografía de clave pública, Public key cryptography. Método de seguridad mediante el cual se crean dos claves (también llamado "clave doble" o key pair), la clave pública y la clave privada, que se utilizan para encriptar y desencriptar mensajes. Para encriptar un mensaje para un destinatario, se utiliza su clave pública, pero sólo se puede desencriptar el mensaje si se tiene su clave privada (la

del destinatario). Para firmar digitalmente un mensaje, se utiliza la clave privada del remitente, y sólo se puede verificar la firma si se tiene la su clave pública (la del remitente). También se encuentra como "criptografía de claves públicas" y "sistema criptográfico público".

Criptoperiodo, Cryptoperiod. Lapso de tiempo durante el cual se utiliza una clave específica o permanecen en vigor las claves de un sistema. A veces se refiere a la cantidad de datos encriptados con esa clave.

CTAK, CipherText AutoKey. Literalmente, cifrado de texto con autoclave. Modo de cifrado en bloque que utiliza un registro de desplazamiento previamente encriptado mediante cifrado en bloque para generar la clave que encripta el próximo bloque de texto cifrado. También se llama CFB.

Cut and paste (ataque). Ataque en el que se combinan varias piezas de mensajes cifrados con la misma clave para crear un nuevo mensaje que pueda desencriptarse. Puede que el atacante no entienda el mensaje completo pero puede hacerse una idea del efecto que tuvieron al ser recibidos.

D

Datagrama, Datagram. En conmutación de paquetes, un mensaje autocontenido independiente, enviado a través de la red, cuya llegada, momento de llegada y contenido no están garantizados. Lleva información suficiente para guiarse desde el remitente hasta el destinatario por sí mismo. Paquete de IP que contiene toda la información de control de la conexión y el segmento de datos TCP/UDP

Depósito de claves, Key escrow. Sistema ideado para guardar copias de claves cifradas con la idea de que un usuario pueda recuperarlas en caso necesario para interpretar una información cifrada.

DES, Data Encryption Standard. Algoritmo público de encriptación criptográfica ampliamente utilizado en sistemas comerciales. Es un estándar en los Estados Unidos por la FIPS, por lo que es aceptado por muchas instituciones financieras. Sin embargo, su longitud de clave (56 bits) lo hace vulnerable a ataques. Sus modos de funcionamiento (ECB, CBC, OFB, CFB) están regulados por la norma FIPS PUB 81.

Desencriptar, Decrypt. Reconvertir texto cifrado en texto en claro. También se dice "descifrar" (decipher), "descodificar" o "decodificar" (decode).

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.

DH, Diffie-Hellman. Algoritmo de clave pública que genera un mensaje secreto compartido entre dos entidades después de que hayan compartido públicamente datos generados de forma aleatoria. Véase también X9.42.

Dial-up. Acceso por la red telefónica.

Dirección física de red, Physical network address. Dirección del host en un enlace de datos. También se encuentra como "dirección de red física".

Dirección IP, IP address. Dirección de host de 32 bits definida por IP en STD 5, RFC 791. Se trata de un número único e irrepetible por el que se identifica la red en la que se encuentra un host. Número identificativo de un ordenador conectado a Internet.

División, Splitting. Segmentación de una clave cifrada en dos claves separadas para que el atacante no pueda reconstruir la clave cifrada real incluso si una de los segmentos de clave es interceptado.

DMS, Defense Message System. Sistema digital de mensajería desarrollado por el Departamento de Defensa de los Estados Unidos para proporcionar servicios de e-mail seguros para aplicaciones críticas.

DNS. Domain Name Systems. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección númerica IP. Ejemplo: 12.120.10.1

Dominio. Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente estan organizados de derecha a izquierda. Por ejemplo: arrakis.es.

DSA, Digital Signature Algorithm. Algoritmo asimétrico que sólo se puede utilizar con firma digital. Utiliza más parámetros que el RSA y así se consigue un grado de mayor seguridad. Véase también DSS.

DSS, Digital Signature Standard. Sistema de firma digital adoptado como estándar por el NIST. Utiliza la función Hash SHA y el algoritmo asimétrico DSA.

Dual Homed Gateway. Es un sistema que tiene 2 o más interfaces de red, cada uno de los cuales está conectado a una red diferente. En las configuraciones firewall, un "dual homed gateway" actúa generalmente, como bloqueo o filtrador de parte o del total del tráfico que intenta pasar entre las redes.

E

ECB, Electronic Code Book. Modo de cifrado en bloque que consiste en aplicar el cifrado a bloques de datos, uno tras otro, individualmente.

EES, Escrowed Encryption Standard. Estándar para sistemas de cifrado desarrollado por la NSA y publicado por el NIST, que permite a las agencias legales o autorizadas intervenir las comunicaciones encriptadas. EES proporciona un método para recuperar las claves cifradas que se utilizan. Este estándar ya no se utiliza. También llamado "estándar de cifrado con depósito".

Encapsulado IP-in-IP. Método utilizado en el modo túnel que consiste en insertar una cabecera IP adicional antes de la cabecera original del paquete inicial. También se pueden insertar otras cabeceras entre las dos anteriores.

Encriptación. Base de la seguridad en la Red. la encriptación codifica los paquetes de información que fluyen por la red, con el fin de evitar que accedan a dicha información terceras personas.

Encriptar, Encrypt. Convertir texto en claro en texto cifrado. También se dice "cifrar" (encipher) y "codificar" (encode).

Encriptador automático, In line encryptor. Producto que encripta automáticamente todos los datos que pasan por un enlace de datos.

Encriptación de programas, Application encryption. Funciones criptográficas creadas en los protocolos de comunicaciones para un programa específico, como por ejemplo e-mail. Ejemplos son PGP o SHTTP.

Encriptación de red, Network encryption. Servicios de encriptación aplicados a la información que se mueve sobre el nivel del enlace de datos pero por debajo del nivel del software. Su propósito es evitar que agentes externos conecten con la red y proteger el tráfico de la misma. Esto permite a los usuarios de la red utilizar servicios y aplicaciones en red de forma segura y transparente. Las grandes empresas usan normalmente algún tipo de software con VPN, con encriptación

propia, para evitar brechas de seguridad. A la encriptación de red también se le llama "encripción de red" o "cifrado de red".

Encriptación de transporte, Transport encryption. Servicios de encriptación aplicados a información sobre el nivel de red pero bajo el nivel del software de aplicaciones. Esto permite que se puedan cifrar protocolos de aplicación existentes, así como que se utilicen la pila de protocolo de red existente y los servicios de red subyacentes. La encriptación de transporte suele venir incluida en la aplicación que protege. También llamada "cifrado de transporte".

Encriptación del canal de comunicaciones, Link encryption. Servicios de cifrado que encriptan totalmente datos mientras viajan por enlaces de datos. También se llama "encripción del canal" y "cifrado del canal".

Encriptación fuerte, Strong crypto. Encriptación que, cifrando a 128 bits, sobrepasa los estándares para encriptaciones ligeras o medias y por lo tanto se encuentran con restricciones significativas en las leyes de exportación de varios países. Fue desarrollada inicialmente por las fuerzas armadas de los Estados Unidos. También se le llama "cifrado fuerte", "cripto fuerte", "codificación fuerte" o "encripción fuerte".

Enlace de datos, Data link. Red de interconexión y distintas instalaciones terminales, que permite el intercambio de información seguro entre terminales, enviando bloques de datos y llevando a cabo la sincronización, el control de errores y de flujo necesarios.

ESP, Encapsulating Security Payload. Estándar de IPSEC para cifrado y validación, que encripta el contenido de un paquete IP. Funciona en la capa de red o en la de transporte de la OSI y puede cifrar datos creados por cualquier protocolo de la capa superior. En la capa de transporte se puede insertar una cabecera ESP entre las cabeceras IP y TCP para cifrar toda la información de TCP y los datos

contenidos en el paquete. En la capa de red se obtiene la funcionalidad y privacidad de VPN, al poder ocultar la dirección IP exacta de los paquetes. Las implementaciones más recientes de IPSEC pueden proporcionar también protección de autenticación y anti-repetición del AH a los paquetes. También se llama "carga de seguridad encapsuladora".

e-mail, Electronic mail. Literalmente, correo electrónico. Sistema que transmite mensajes desde un terminal a sus destinatarios, redireccionándolos, y permitiendo su almacenamiento y gestión.

F

Factor de trabajo, Work factor. Estimación de la cantidad de trabajo que un atacante con experiencia y recursos concretos puede realizar para violar unas medidas de seguridad.

Falsificación, Forgery. Información modificada por un atacante para hacer creer al destinatario que lo que está recibiendo viene de otro remitente.

FAQ, Frequently Asked Questions. Literalmente, preguntas más frecuentes. Se trata de un documento que lista las preguntas más frecuentes que se suelen dar sobre un tema y sus respuestas.

Fichero. Información agrupada con un solo nombre. Por ejemplo, un documento de texto, un sonido, un video, o un programa.

Fichero de Texto. Un fichero que contiene únicamente letras, una detrás de otra, formando frases. Los ficheros de texto, suelen tener una extensión .txt. Esto indica que sólo contienen letras, pero no formato, o sea, no se puede definir ni el tipo de letra, ni el color, ni el tamaño, ni el subrayado. Esa posibilidad sólo la encontramos

en los Ficheros de Documentos, que contienen texto con formato, e incluso imágenes.

Filtrado de paquetes. Característica que permite a un router realizar decisiones del tipo pasa no-pasa para cada paquete IP, basándose en la información contenida en el header del mismo.

FIPS, Federal Information Processing Standard. Estándares para los sistemas de ordenadores del gobierno de los Estados Unidos publicados por el NIST.

Firewall. Sistema o grupo de ellos enfocados hacia una política de control de acceso entre la red de la organización e Internet.

Firma digital, Digital signature. Es el resultado de encriptar la suma de control con la clave privada del emisor del mensaje. Es un método de comprobación de que el dueño de una clave privada es el mismo que ha originado un mensaje, incluyendo el proceso de firmado y el de verificación de la firma.

FORTEZZA. Tarjeta de PC que contiene el algoritmo de encriptación SKIPJACK y proporciona servicios de cifrado necesarios para soporte de aplicaciones de e-mail.

FTP, File Transfer Protocol. Literalmente, protocolo de transferencia de ficheros. Protocolo de red que opera en las capas 5 a 7 del modelo OSI, que se utiliza para transferir archivos entre ordenadores de una red. También se le llama así a la aplicación que utiliza para dicha transferencia.

G

Gateways, pasarelas. Permiten interconectar redes de diferentes arquitectura, es decir, con topología y protocolos distintos.

GigaByte (Gb). Mil Mbs. Ningun fichero ocupa tanto. Esta unidad se usa para medir tamaños de Discos Duros. Un discoi duro moderno suele tener mas de 1 Gb.

Gusano, Worm. Programa informático que se autoduplica y se autopropaga por los hosts de una red.

H

Hash. Suma de control mejorada por la que se dificulta al atacante la construcción de bloques de datos que generen una suma de control determinada o valor hash. La función Hash es una función matemática que selecciona, de manera aparentemente aleatoria, unos valores dentro de un amplio rango.

Header. Encabezado de los paquetes de IP.

Henry the Forger. Atacante que genera mensajes de red completamente falsos para engañar a sus destinatarios.

Hijacking. Ataque en el que se toma bajo control una conexión en directo entre dos usuarios de forma que el atacante puede suplantar a uno de los usuarios.

Hipertexto. Documento que contiene texto, imágenes y enlaces a otros hipertextos. También puede contener otros tipos de elementos multimedia, como pueden ser video, sonido, etc.

Hosts. En líneas generales, servidor conectado a la red. Sistema informático parte de una red y capaz de comunicarse independientemente con otros sistemas en la red. También llamado "sistema central" o "sistema anfitrión".

Host address. Literalmente, dirección del host. La dirección utilizada por usuarios de la red para comunicarse con un host concreto.

HTML, HyperText Markup Language. Lenguaje de código utilizado para crear documentos hipertexto y páginas web para la WWW.

HTTP, HyperText Transfer Protocol. Protocolo basado en una estructura cliente-servidor utilizado para transferir archivos o documentos hipertexto en la WWW.

I

IAB, Internet Architecture Board. Literalmente, Comité de Arquitectura de Internet. El cuerpo que ayuda a definir la arquitectura y diseño general de los protocolos de Internet. El IAB es el grupo asesor técnico del ISOC y se encarga de supervisar sus otras secciones [URL32].

IANA, Internet Address and Numbering Authority. Organización administrativa que asigna direcciones de host y otras constantes numéricas utilizadas en los protocolos de Internet [URL32].

IDEA, International Data Encryption Algorithm. Cifrado en bloque desarrollado en Suiza y utilizado en PGP. Hasta ahora ha resistido mucho mejor los ataques que otros métodos de cifrado. Además es más resistente que DES a ataques de criptoanálisis diferencial y lineal.

IESG, Internet Engineering Steering Group. El grupo que supervisa al IETF y determina qué proposiciones serán admitidas como estándares.

IETF, Internet Engineering Task Force. Organismo técnico que establece y mantiene los estándares de protocolos para Internet.

IKE, Internet Key Exchange. Protocolo de gestión de claves simétricas para IPSEC basado en ISAKMP, que administra la seguridad de una transacción,

autenticando a cada participante, negociando las normas de seguridad y gestionando el intercambio de claves de sesión.

INFOSEC, Information Security. Medidas técnicas de seguridad que implican seguridad en las comunicaciones, criptografía y seguridad informática.

Integridad, Integrity. Servicio que asegura que la información sólo es modificada por personas autorizadas y que garantiza que la información no ha sido mutilada o alterada de manera no autorizada.

Interfaz de conexión, Socket interface. El interfaz de software entre una pila de protocolo de red de un host y los programas de aplicación que utiliza la red. También se encuentra como "interfaz de conexión lógica de red".

Interfaz de controlador de dispositivos, Device driver interface. Interfaz estándar utilizado por el software de un host para comunicarse con dispositivos periféricos, incluyendo dispositivos en un enlace de datos. Veáse también "controlador de dispositivos".

Internet. Red de comunicaciones virtual de ámbito mundial, no gestionada por ninguna organización específica y que utiliza los protocolos TCP/IP.

Internet Draft. Documento que se envía al IETF para su revisión.

Interred. Es una colección de LAN conectadas por una WAN. Se forma una interred cuando se conectan distintas redes entre sí. [URL9]

Interoperatividad. Permite que diversos tipos de sistemas operativos monopuesto funcionen sobre la misma red.

Intranet. Red privada virtual, normalmente dentro de una organización, que permite la comunicación entre diferentes usuarios de una empresa y que utiliza utiliza protocolos de internet aunque no se conecta directamente a Internet.

IP, Internet Protocol. Protocolo que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino.

IPSEC, IP Security Protocol. Protocolo cifrado de red para proteger paquetes IP utilizando servicios criptográficos de seguridad que permiten la autenticación, integridad, control de acceso y confidencialidad. A nivel de redes provee servicios similares a SSL.

ISAKMP, Internet Security Association Key Management Protocol. Protocolo de aplicaciones de gestión de claves para IPSEC respaldado por el IETF como una parte importante de cualquier implementación IPSEC. Para VPN, es la base de IKE e intercambia la información de claves entre dos nodos, de forma que se establece una conexión segura encriptada entre los nodos y se intercambia la información de claves para la conexión.

ISO, International Standards Organization. Organización Internacional de Normalización, fundada en Ginebra, que publica un gran número de estándares y promociona el comercio global de 90 países. Los estándares que publica para red (los protocolos OSI), son en su mayor parte incompatibles con los protocolos de Internet. Los protocolos desarrollados por la CCITT son generalmente protocolos ISO. URL: http://www.iso.org/.

ISOC, Internet Society. La organización más antigua de promoción de uso de Internet. Su misión es promocionar el desarrollo, evolución y uso abiertos de Internet. URL: http://www.isoc-es.org/.

i18n. Abreviatura de "internationalization". Se refiere a todos los atributos relacionados con la propuesta de internacionalización.

K

Kilobit. Mil bits.

KiloByte(Kb). Mil Bytes. Cualquier fichero suele ocupar varios Kbs.

Kbps. Kb/s. Kilobits por segundo. Velocidad de transferencia de información.

KDC, Key Distribution Center. Dispositivo encargado de distribuir claves secretas a usuarios para permitir a pares de hosts encriptar el tráfico directamente entre ellos. Esta es la base del sistema Kerberos. También llamada "autoridad certificante".

KEK, Key Encrypting Key. Clave cifrada utilizada para encriptar claves de sesión o de datos, y nunca se utilizan para encriptar los datos en sí. Su misión es proteger dichas claves durante su transmisión o almacenamiento. También llamada "clave cifrado de claves".

L

LAN, Local Area Network. Red direccional de comunicaciones que opera en una zona restringida y permite a los usuarios intercambiar información con cualquier usuario conectado a ella y compartir recursos periféricos. También se llama "red de área local".

Latencia, Latency. El tiempo transcurrido entre la transmisión y recepción de datos en una red. En Internet, la latencia se puede deber a retrasos en nodos, colisiones en la red, y congestiones en los proveedores de servicio (entre otras

cosas). La latencia puede llevar a un rendimiento inaceptable en VPN, especialmente para aplicaciones de bases de datos distribuidas y protocolos multimedia.

LDAP, Lightweight Directory Access Protocol. Un protocolo de acceso a directorios más simple que X.500 para acceso a directorios.

Limite solar anular, annual solar limit . Se refiere a la cantidad total de energía producida por el sol en un año. Es posible calcular las condiciones menos favorables mediante el número de claves que pueden probarse con esa cantidad de energía: 2^192 claves. De esto se deduce que una clave secreta que contenga 192 bits es prácticamente imposible de craquear utilizando métodos elementales.

Línea alquilada, Leased line. Línea punto a punto, entre dos ubicaciones para un uso privado de una compañía de telecomunicaciones. También llamada "línea arrendada".

Linux. Sistema operativo UNÍS para PC. Es gratuito. Se puede conseguir por Internetñ. Es bastante complicado de poner en marcha, aunque ofrece un rendimiento espectacular.

Otra definición: Versión Shareware del conocido Sistema operativo Unís. Es un sistema multitarea y multiusuario de 32 bits para PC.

Llave de un solo uso, One time pad. Cifrado Vernam en el que se utiliza un bit de clave nuevo aleatorio por cada bit de datos que se encripta. También llamada "libreta de un solo uso" o "cifra de uso único".

Logging. El proceso de almacenamiento de información sobre eventos que ocurren en el firewall o en la red.

L2TP, Layer 2 Tunnelling Protocol. Protocolo híbrido creado combinando PPTP y el Layer 2 Forwarding (L2F) de Cisco, que permite realizar tunneling

encapsulando el PPP (Protocolo Punto a Punto) estándar para enviar datos encriptados estableciendo una VPN a través de Internet. También llamado "protocolo de túnel de capa 2".

M

MacOs. Sistema operativo de las Macintosh.

Mb/s. Velocidad de transferencia de datos, medida en unidades de Megabits por segundo.

MD5, Message Digest #5. Algoritmo hash de una vía ampliamente utilizado en aplicaciones de cifrado. Es el utilizado en el protocolo de cifrado PGP para firmar mensajes con claves de tipo RSA; también se utiliza como autenticador de mensajes en el protocolo SSL. También se llama "función resumen MD5".

MegaByte(Mb). Mil Kbs. Las grandes programas o ficheros ocupan varios megas (Mb).

Mensaje, Message. Información enviada de una entidad a otra en una red. Un mensaje puede ser dividido en varios paquetes para enviarlo al destinatario y luego recompuesto por el host que lo recibe.

Menú. Lista de opciones a elegir durante la ejecución de un programa. Estas opciones suelen aparecer en una barra horizontal en la parte superior de la ventana del programa. Al seleccionar una de las opciones, `pueden aparecer más sub-opciones.

Mhz (Mega Hertzios). Unidad de medida de la velocidadde un procesador. Un Pentium a 200 Mhz ejecuta los programas el doble de rápido que un Pentium a

100 Mhz. Hoy en día todas las computadoras que se comercializan disponen de un Pentium entre 120 y 200 Mhz.

MIM, Man In Middle. Ataque contra un intercambio entre claves públicas en el que el atacante sustituye su propia clave pública con la clave pública requerida. Literalmente, el enemigo se sitúa entre el emisor y el receptor manipulando la comunicación. También llamado "bucket brigade", "brigada de cubos" o "brigada de bomberos".

MIME, Multipurpouse Internet Mail Extensions. Extensiones Multiproposito de Correo Internet. Extensiones del protocolo de correo de Internet que permiten incluir información adicional al simple texto. Formato estándar estructurado para transmisión de mensajes que permite que un mensaje contenga muchas partes.

Mínimo privilegio, Least privilege. Función de un sistema en cuyas operaciones se garantizan el mínimo de permisos posibles para realizar sus tareas. Cada operación tiene sólo los privilegios que requiere para llevar a cabo su función y cada usuario tiene la categoría de manipulación que necesita para hacer su trabajo.

Módem. Dispositivo que se conecta al ordenador y a la linea telefónica. Permite que se realice la conexión a Internet desde casa o desde la empresa.

Modo, Mode. Indica cómo procesar bloques al aplicarlos a un flujo de datos. Algunas opciones son: CBC, CFB y OFB. También llamado "modo de operación" o "modo de cifrado".

Modo transporte, Transport mode. Modo ESP de seguridad para paquetes IP que cifra los contenidos de datos de un paquete y deja las direcciones IP originales en texto en claro. Este método no protege totalmente la cabecera IP y sólo es

aplicable a terminales (sólo se incluyen los routers cuando también funcionan como terminales).

Modo túnel, Tunnel mode. Modo ESP de seguridad para paquetes IP que cifra un paquete IP entero incluyendo la cabecera IP. Se crea un nuevo paquete IP utilizando el método de túnel de encapsulado IP-in-IP, protegiendo todo el paquete IP interno original. Es el mejor modo de crear VPN seguras.
Módulo, Modulus. En cifrado de claves públicas, se refiere a una parte de la clave pública.

MsDos (Microsoft Disk Operating System). El sistema operativo más usado hasta 1995 para las PC's. En 1995 se empezó a usar Windows 95. MsDos no es un sistema Operativo gráfico(es decir, con iconos, dibujos y ratón), sino basado en texto.

MSP, Message Security Protocol. Protocolo de cifrado de e-mails desarrollado como parte del programa SDNS y utilizado en el DMS. Proporciona seguridad emisor-receptor para el sistema de tratamiento de mensajes (MHS).

Munición, Munition. Cualquier elemento útil en una guerra. Los sistemas de cifrado son municiones según la ley de los Estados Unidos.

N

Navegador, Browser. Software cliente para acceso a datos en la World Wide Web.

NCSC, National Computer Security Center. Literalmente, Centro Nacional para la Seguridad Informática. Organismo del gobierno de Estados Unidos, división de la NSA, que evalúa los equipos informáticos para aplicaciones de alta seguridad y

publica documentos sobre los requisitos de seguridad de los sistemas informáticos. También se llama NISC (NSA INFOSEC Service Center).

NIST, National Institute of Standards and Technology. Organismo del gobierno de los Estados Unidos que establece estándares nacionales. URL: http://www.nist.gov/.

Nodo. Es cualquier estación de trabajo, terminal, impresora o cualquier otro dispositivo que pueda ser conectado a la red, ya sea de forma directa o indirecta (estando a disposición de la red al pertenecer a un dispositivo ya conectado a ella).

Nombre de dominio, Domain name. El nombre textual asignado a un host en Internet. Este nombre corresponde a una dirección IP numérica y el encargado de traducir este número en el nombre de dominio es el protocolo DNS (Domain Name Service).

Nonce. Valor aleatorio enviado en intercambio de protocolos, a menudo utilizado para detectar ataques de respuesta. Como el valor cambia con el tiempo, es fácil comprobar si el intento de reproducción un archivo está permitido, el tiempo actual puede compararse con el nonce. Si no excede o no existe el nonce, el intento se autoriza. Si sucede lo contrario, el intento no se autoriza.

NSA, National Security Agency. Organismo del gobierno de los Estados Unidos responsable de interceptar comunicaciones extranjeras por razones de seguridad y para desarrollar sistemas de cifrado para proteger las comunicaciones del gobierno.

Número aleatorio, Random number. Un número cuyo valor no puede ser predecido. Los verdaderos números aleatorios son a menudo generados por sistemas físicos que realmente sean aleatorios.

Número de puerto, Port number. Número único de identificación asignado a un puerto. En protocolos de transporte de Internet se utiliza para identificar qué servicio o programa está previsto que reciba un paquete. Algunos números de puerto son permanentes, asignados por el IANA. Por ejemplo, el e-mail, generalmente utiliza el puerto 25 y los servicios de web usan tradicionalmente el puerto 80.

O

Oakley. Protocolo por el que dos partes autenticadas pueden acordar claves secretas y seguras.

OFB, Output FeedBack. Modo de cifrado en bloque por el cual el cifrado se utiliza para generar el flujo de claves. También se llama "salida realimentada".

Ordenador. Conjunto formado por un monitos, un teclado, un ratón y una CPU. Permite manejar todo tipo de información.

One way hash. Función hash para la que es extremadamente difícil construir dos bloques de datos que den exactamente el mismo resultado hash. Idealmente, requeriría una búsqueda por fuerza bruta para encontrar dos bloques de datos que den el mismo resultado. Se puede encontrar como "función unidireccional de resumen".

OR Exclusiva, Exclusive OR. Operación computacional en bits que añade los dos bits juntos y descarta el que lleva. Es la base del cifrado Vernam y de la división de claves. También "XOR".

OSI, Open System Interconnection. Literalmente, Interconexión de Sistemas Abiertos. Convenio de protocolos de comunicaciones, desarrollados por los comités ISO, para ser el estándar internacional de la red de ordenadores.

OS/2: Operating System 2. Sistema operativo de 32 bits multitarea creado por IBM. Creado para PC con entorno gráfico de usuario. La versión 4 soporta ordenes habladas y dictado. Sistema operativo menos conocido que Windows, aunque un poco más potente.

P

PAC, Concentrador de acceso PPTP. Dispositivo que asocia una o más líneas capaces de soportar PPP y manejo del protocolo PPTP. PAC necesita solamente TCP/IP para pasar sobre el tráfico de una o más PNS.

Paquete, packet. Es una pequeña parte de la información que cada usuario desea transmitir. Cada paquete se compone de la información, el identificador del destino y algunos caracteres de control. Un bloque de datos transportado por una red. Cuando un host envía un mensaje a otro, el mensaje se rompe en uno o más paquetes que son enviados individualmente por la red.

Password sniffing. Ataque en el que el atacante, mediante un programa "password sniffer" monitoriza el tráfico IP de su segmento de red y captura contraseñas, normalmente para utilizarlas después en suplantaciones. También llamado "husmeo de claves".

Pc (Personal Computer). Ordenador orientado al uso doméstico. Esta en competencia con los Macintosh. Es el tipo de ordenador más vendido en los últimos años.

PC card, Tarjeta periférica plug-in de pequeño tamaño a menudo utilizada en ordenadores portátiles, pero también en PCs. Una utilidad muy extendida son los módems. También se utilizan para mantener funciones de cifrado y guardar

material de claves de forma segura. También se puede encontrar como "PCMCIA card", "Tarjeta PC" o "Tarjeta de PC".

Peeping Tom. Literalmente "fisgón" o "voyeur". Atacante cuyos ataques se basan en examinar el tráfico de datos. Por ejemplo utiliza el password sniffing.

PEM, Privacy Enhanced Mail. Protocolo de cifrado de e-mails similar a MIME y desarrollado por la IETF en paralelo a éste. Ha sido ya superado por PGP, MSP y S/MIME.

Perímetro, Perimeter. Límite físico entre el interior y el exterior. Las medidas de seguridad confían en los perímetros para depositar su confianza hasta ciertos niveles en usuarios dentro de los mismos.

PGP, Pretty Good Privacy. Protocolo de cifrado de e-mails que utiliza RSA e IDEA, incluido en paquetes de software ampliamente distribuidos por Internet.

Pila de protocolo de red, Network protocol stack. Paquete de software básico que proporciona servicios de red de propósito general a software, independiente del tipo particular de enlaces de datos utilizados.

PKCS, Public Key Cryptography Standards. Conjunto de estándares publicados por la RSADSI sobre la implementación de algoritmos de claves públicas en una forma fiable, segura e interoperable.

PKI, Public Key Infrastructure. Infraestructura de seguridad, basada en criptografía de clave pública, que permite la gestión de certificados digitales. Se utiliza tanto para permitir a un destinatario de un mensaje firmado que confirme en la firma como para permitir al remitente encontrar la clave de encripción para enviar el mensaje al destinatario.

PKIX, Internet X.509 Public Key Infrastructure. El nombre del grupo de trabajo de la IETF que crea los estándares para PKI en Internet.

Play-it-again Sam. Atacante cuyas acciones se basan en interceptar mensajes legítimos y transmitirlos repetidamente para engañar al sistema o sus usuarios.

Plug-In. Es un componenete de un programa mayor. Por ejemplo, el navegador Netscape admite que se le añadan plug-in's permitiendo asi incorporar más funciones, como por ejemplo, oir ficheros especiales de sonido o ver videos directamente desde la ventana del navegador.

PNS, **Servidor para red de PPTP.** Sirve para operar sobre computadoras de propósito general y plataformas de servidores. PNS dirige la parte del servidor del protocolo PPTP mientras PPTP confía completamente TCP/IP y es independiente de la interfaz de Hardware, el PNS puede usar cualquier combinación de hardware de interfaz IP, incluyendo dispositivos LAN y WAN.

Política. Reglas de gobierno a nivel empresarial / organizativo que afectan a los recursos informáticos, prácticas de seguridad y procedimientos operativos.

POP, Post Office Protocol. Protocolo de Oficina de Correos, protocolo usado por ordenadores personales para manejar el correo sobre todo en recepción. Protocolo de Internet para recuperar e-mail desde un host de servidor, sin tener que entrar en él ni utilizar programas de e-mail. Complementa a SMTP, que se encarga de enviar los correos.

PPP, Point to Point Protocol. Protocolo Punto a Punto. Protocolo Internet para establecer enlace entre dos puntos.

PPTP, Point to Point Tunneling Protocol. Protocolo de tunneling IP diseñado para encapsular IPX de protocolos LAN y Apple Talk dentro de una IP, para

transmisiones por Internet u otras redes basadas en IP. Proporciona un medio de tráfico por túneles IP en la capa 2 y puede ser utilizado por IPSEC para proporcionar autenticación.

PRNG, Pseudo Random Number Generator. Literalmente, generador de números pseudoaleatorios. Algoritmo que genera una secuencia de valores numéricos aleatorios. Los PRNGs criptográficos generan idealmente secuencias que son casi imposibles de predecir. Sin embargo, al utilizar la mayoría de los PRNGs de software comercial métodos estadísticos, sus secuencias podrían ser predecibles.

Programa. Fichero ejecutable. Por ejemplo, un procesador de textos, un navegador de Internet, o un juego de ordenador.

Protección obligatoria, Mandatory protection. Mecanismo de seguridad en un ordenador que bloquea automáticamente algunas acciones de usuarios externos o internos. Sirve para prevenir ataques a servidores de Internet y evitar que se activen procesos no deseados en el host.

Protocolo. Establece las directrices que determinan cómo y cuándo una estación de trabajo puede acceder al cable y enviar paquetes de datos. Los protocolos se diferencian por el punto en que reside el control y en la forma de acceso al cable.

Proxy. Utilidad que proporciona indirectamente algún servicio. El cifrado proxy se aplica a servicios de cifrado para tráfico de red sin hosts individuales y daría soporte a dichos servicios. Los proxies cortafuegos (o "proxy firewall") proporcionan acceso a servicios de Internet que están al otro lado del cortafuegos mientras controlan el acceso a servicios en cualquier dirección. Un agente software que actúa en beneficio de un usuario. Los proxies 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.

Proxy Server. Servicio de propósito especial, código de aplicación instalado en un firewall. El proxy server permite que el administrador de la red permita o rechace determinados servicios de una aplicación en particular.
Puente. Dispositivo que enlaza redes diferentes para formar una sola red lógica.

Puerto. Conector en la parte trasera de la caja del ordenador. Sirve para enchufar periféricos externos. Hay de dos tipos, serie y paralelos.

Puerto Serie. El puerto serie puede ser de 9 a 25 pines (un pin es un alambre o extremo del conector). Sirve para por ejemplo un ratón o un módem externo.

PVC, Private Virtual Circuit. Conexión lógica bidireccional, entre dos ubicaciones (punto a punto o frame relay) constituida sobre una línea privada de red conmutada digital. La dirección y velocidad del enlace son definidas por cada conexión, pero la ruta física tomada entre las dos ubicaciones es determinada por la necesidad de ancho de banda dedicado. También se encuentra como "circuitos privados virtuales" o "circuitos virtuales privados".

Q

QoS, Quality of Service. Literalmente, "calidad de servicio". En general, se trata de la repercusión global de un servicio sobre el grado de satisfacción de sus usuarios. En lo que se refiere a VPN, QoS generalmente significa la cantidad de caudal y/o número de conexiones simultáneas que pueden sostenerse en una conexión que utilice IPSEC, para conseguir un control más eficaz de la red. Por ejemplo, con Qos, se puede garantizar que una aplicación tenga la prioridad más alta de la red y reservar un ancho de banda específico a un departamento

concreto, o asignar la prioridad más baja a otros servicios, poniendo límites en el ancho de banda a utilizar.

R

RADIUS, Remote Access Dial-In User Service. Protocolo estándar de dominio público que básicamente identifica usuarios que accedan remotamente a una red, permitiéndoles asignar direcciones de red dinámicamente. Proporciona un punto central de administración para usuarios de acceso remoto a servidores y otros dispositivos.

RC2, Rivest Cipher #2. Cifrado en bloque diseñado por Ron Rivest, de RSADSI. Se utilizaba para encriptamiento rápido en bloques, más veloz que DES y con una clave criptográfica de 40 bits.

RC4, Rivest Cipher #4. Algoritmo de flujo diseñado por Ron Rivest en RSADSI para encriptamiento rápido. Con una clave de 40 bits, proporciona cifrado ligero en browsers web típicos y es 10 veces más más rápido que DES. Ampliamente utilizado en productos comerciales.

RDSI, ISDN. Integrated Services Digital Network. Literalmente, Red Digital de Servicios Integrados. Estándar que facilita conexiones digitales entre usuario y red para transmisiones simultáneas de señales de voz, datos y vídeo digitales sobre circuitos de telefonía estándar.

Recuperación de clave, Key recovery. Sistema que determina la clave utilizada para cifrar datos, posiblemente utilizando una clave de depósito.

Red/black separation. Concepto de diseño de sistemas criptográficos que mantiene las porciones del sistema que manejan texto en claro rigidamente

separadas de las porciones que manejan el texto cifrado. Las porciones que manejan ambas se minimizan y después se implementan cuidadosamente.

Red corporativa. Es una red que interconecta todos los equipos de una Organización (empresa), independientemente del lugar en el que se encuentren.
Red interconectada. Son dos o más redes que interactúan entre sí para formar un sistema en red. También se puede subdividir una red extensa en otras más pequeñas para optimizar el rendimiento y la gestión. Las interconexiones pueden establecerse entre distintas ciudades.

Red de Área Amplia (RAA ó WAN). Red de ordenadores de gran alcance. Generalmente entre ciudades o países. Por ejemplo, la red de ordenadores de un Banco.

Red de Área Local (RAL ó LAN). red de ordenadores del tamaño de una habitación o como mucho, de un edificio. Por ejemplo, una oficina o una sala de ordenadores de una colegio.

Reescritura, Rewrite. Ataque que modifica el contenido de un mensaje encriptado sin desencriptarlo antes.

RFC, Request For Comments. Notas y comentarios iniciados hacia 1969, acerca de la entonces ARPANET (hoy de Internet), en los que se habla de aspectos de informática y comunicación entre ordenadores, sobre todo de protocolos de red, procedimientos, programas y definiciones, entre otros asuntos de interés. Se trata del mecanismo primario utilizado por el IETF para publicar documentos, incluyendo estándares.

RFC 822. La especificación RFC (STD 11, RFC 822) para el formato estándar de cabeceras de mensajes de e-mail en Internet. Los expertos hablan de estos

mensajes como"mensajes 822". Este formato era conocido antes como "formato 733".

Repetición, Replay. Ataque que intenta engañar al sistema interceptando y retransmitiendo de nuevo un mensaje legítimo para suplantar al usuario que lo envió por primera vez. Algunos protocolos incluyen mecanismos anti-repetición para detectar y rechazar dichos ataques. También se encuentra como "ataque de reproducción" o "ataque de respuesta".

Repetidor. Dispositivo que permite que las redes se comuniquen de una manera razonablemente eficiente. Un repetidor amplifica y limpia las señales digitales y las envía hacia su destino.

Router - Encaminador -. Dispositivo destinado a conectar 2 o más redes de área local y que se utiliza para encaminar la información que atraviesa dicho dispositivo. Dispositivo que distribuye tráfico entre redes transportando paquetes IP cuando el host de destino de los paquetes está en la red receptora o cerca de ella. La distribución de los paquetes se hace basándose en información de nivel de red y tablas de direccionamiento. También se le llama "direccionador", "encaminador" o "enrutador".

Routing host. Host que encamina paquetes IP entre redes, además de proveer otros servicios.

RSA, Rivest, Shamir, Adelman. Algoritmo de clave pública utilizado en muchos protocolos de seguridad, que puede encriptar y desencriptar datos y también aplica o verifica una firma digital. Fue inventado en 1978 por Rivest, Shamir y Adleman, que le dan nombre, fundadores también de la RSADSI, que controla la patente.

RSADSI, RSA Data Security, Inc. La compañía formada por los creadores del algoritmo RSA, principalmente responsable de la venta y licencia de cifrados de claves públicas con propósitos comerciales. URL: http://www.rsa.com/.

Ruteadores. Dispositivos responsables de la determinación de que datos deben permanecer dentro de la red local y que datos deben transferirse hacia otras redes.**.** Dispositivo que administra el flujo de datos entre redes

S

Screened Host. Un host detrás de un router protegido. El grado en que el host puede ser accesible depende de las reglas de protección del router.

Screened Subnet. Una subred detrás de un router protegido. El grado en que la subred puede ser accesible depende de las reglas de protección del router.

Servidor de Bastión. Un firewall especialmente diseñado y armado para proteger contra ataques externos.

Seed random. Semilla para los generadores aleatorios. valor aleatorio utilizado cuando se genera una secuencia aleatoria de valores con un PRNG.

Servidor, Server. Unidad en una relación de red que proporciona servicios compartidos a clientes y otros usuarios de la red. El software de servidor generalmente se instala en los hosts con direcciones de red constantes y conocidas, de forma que los clientes puedan conectar con ellos de forma fiable.

Shim. Componente de software insertado en un interfaz conocido, entre otros dos componentes de software. Las versiones "Shim" de IPSEC son a menudo implementadas en el interfaz del controlador de dispositivos, bajo la pila de protocolo de red del TCP/IP del host.

SHTTP, Secure Hypertext Transfer Protocol. Literalmente, HTTP seguro. Mejora de HTTP con funciones de seguridad con algoritmo simétrico, para aplicar servicios de cifrado a datos y transacciones Web.

Sistema Operativo. El programa más importante que se carga en la computadora nada más al arrancar. Sirve para que el usuario se puede entender de alguna manera con la computadora. También da acceso a las funciones más importantes del sistema a los programas que operan por encima del Sistema Operativo. Los más conocidos son MsDos, Windows 3.1, Windows 95, OS/2, UNIX.

SKIP, Simple Key Interchange Protocol. Protocolo que establece claves de sesión para utilizar con cabeceras de protocolo IPSEC. Los datos SKIP son transportados en las cabeceras de los paquetes y viajan en todos los paquetes IPSEC protegidos.

SKIPJACK. Cifrado en bloque desarrollado por la NSA e incluido en los dispositivos CAPSTONE, CLIPPER y FORTEZZA.

SMTP. Simple Mail Transfer Protocol. Protocolo Simple de Transferencia de Correo. Protocolo de Internet para el envío de e-mail entre servidores de correo electrónico, complementando al protocolo POP, que se encarga de la recepción y almacenamiento de los e-mails.

Sniffing. Método de ataque pasivo por el que se captura información de mensajes de red haciendo copias de su contenido. El atacante no modifica la información, sino que la duplica para su análisis. El password sniffing es el más utilizado de estos ataques. También se le llama "husmeo".

Software de aplicaciones, Application software. Software que da un servicio a un usuario. En oposición a software de bajo nivel (lower level software) que posibilita los servicios útiles.

SSL, Secure Sockets Layer. Protocolo de encriptación y autenticación en conexiones de Internet, aplicado a datos en el interfaz de conexión. Proporciona seguridad cifrando los datos que se intercambian entre el servidor y el cliente con un algoritmo simétrico (RC4 o IDEA) y cifrando la clave de sesión mediante un algoritmo de clave pública (RSA). Además, se genera una clave de sesión distinta en cada transacción. A menudo viene incluido en aplicaciones y se utiliza mucho para proteger el tráfico Web. Fue diseñado y propuesto por Netscape Communications Corporation, y se encuentra en la pila OSI entre los niveles de TCP/IP y los protocolos HTTP, FTP o SMTP entre otros. Su versión estandarizada es TLS.

Suite de protocolos, Protocol suite. Colección de protocolos de comunicaciones que proporcionan los servicios necesarios para hacer posible el intercambio de información entre ordenadores, administrando conexiones físicas, servicios de comunicaciones y soporte de aplicaciones. Hay dos suites de protocolos conocidas ampliamente: Los protocolos de Internet (IP) y los protocolos ISO/OSI. También se llama "sucesión de protocolo".

Suma de control, Checksum. Valor numérico utilizado para verificar la integridad de un bloque de datos. El valor se calcula utilizando un procedimiento de suma de control. Una suma de control criptográfica incorpora información secreta en el proceso de suma de control de forma que no pueda reproducirse por quien no la conozca. También se puede encontrar como "digesto de mensaje".

Suplantación, Masquerade. Ataque en el que un usuario usurpa la identidad de otro usuario sin autorización. También llamado "suplantación de personalidad".

S/MIME, Secure Multipart Internet Message Extensions. Literalmente, MIME seguro. Protocolo estándar abierto para la transmisión de mensajes por e-mail, que permite firmar digitalmente y cifrar los mensajes y documentos adjuntos del e-mail, como garantía de seguridad. S/MIME forma parte de la estructura del estándar PKCS de RSA Labs.

T

TCP, Transmission Control Protocol. Protocolo de Control de Transmisión. Conjunto de protocolos de Internet que proporciona una conexión fiable entre un servidor y un cliente, encargándose de la seguridad y la integridad de los paquetes de datos que viajan por Internet.

TCP/IP. Acrónimo compuesto de TCP e IP, para el conjunto de protocolos de Internet para facilitar la comunicación entre usuarios diferentes.

Telnet. Aplicación estándar que soporta conexiones de terminales remotos, proporcionando un interfaz de terminal entre nodos que utilizan TCP/IP.

Texto cifrado, Ciphertext. Mensaje encriptado, texto encriptado mediante un cifrado, opuesto al texto en claro. También llamado "cripto" o "criptotexto".

Texto en claro, Plaintext. Datos que no han sido encriptados, o datos que han sido desencriptados desde un texto cifrado. También se encuentra como "texto plano" o "texto claro".

Tiempo Real. Proceso instantáneo. Por ejemplo, una charla en Tiempo Real es aquella en la que no hay que esperar mas que unos segundos para recibir respuesta de la persona con la que conversamos. El correo Electrónico es todo lo contrario a lo que se entiende cono Tiempo Real.

TLS, Transport Layer Security. Protocolo de Internet que asegura la privacidad en la comunicación entre aplicaciones y usuarios. Versión estandarizada de SSL y su sucesor.

Token. También llamado "testigo".

1. Tarjeta o dispositivo de hardware que genera una contraseña de un solo uso para autenticar a su propietario.
2. Software que genera contraseñas de un solo uso.
3. Información transportada en la cabecera de un mensaje que guarda una copia cifrada de la clave secreta utilizada para encriptar el mensaje, para identificar al remitente, y que normalmente se descifra con la clave pública del destinatario. También llamado "testigo de autenticación".

Transport encryption. Servicios criptograficos aplicados a la informacion encima del nivel de red pero abajo del nivel de software de aplicación (application software). Estas protecciones criptograficas permiten aplicarse a un protocolo de aplcicaoin existiente y tambien usar la pila de potocolos de red(network protocol stack) existente y los servicios implicitos de la red. La encripcion de transporte es tipicamente empacada con la aplicación que esta protegiendo.

Transport mode. El modo ESP encripta los datos contenidos de un paquete y permite la direccion IP original en el texto plano.

Triple DES (3DES). Algoritmo criptográfico que designa tres veces la cifra DES con una o dos claves DES diferentes. Es el estándar mundial de encriptación entre instituciones bancarias.

Tunnelling. En VPN se refiere a la transmisión de información que sigue un protocolo por medio de otro. Consiste en encapsular datagramas completos IP dentro de otros datagramas y se utiliza frecuentemente para transmitir protocolos no-IP a través de redes IP. Encapsulación de datagramas completos dentro de otros datagramas.

Tunnel mode, modo de tunel. El modo ESP que encripta un paquete entero IP incluyendo la cabecera IP.

U

Unicote. Codificación para escritos de prácticamente todas las lenguas del mundo. Unicode proporciona un número único para cada carácter, sin importar la plataforma, el programa o el idioma.

UNIX. Sistema Operativo de los grandes ordenadores, sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas más conocidos como MS-DOS están basados en este sistema mus extendido para grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

URL, Uniform Resource Locator. Sistema unificado de especificación de la ubicación de un recurso en Internet.

URI, Uniform Resource Identifier. Sistema unificado de identificación de recursos en la red. Aún no está implantado. Véase también URL.

URN, Uniform Resource Name. Sirve como identificadores persistentes, más basados en el contenido o características del recurso que en su ubicación. Su intención es sustituir al sistema URI/URL.

V

VENONA. Proyecto del ejército de los Estados Unidos desarrollado para analizar criptográficamente texto cifrado de llaves de un solo uso procedente de la URSS a partir de los años 40.

Versión. Numero que indica lo reciente que es un programa. Por ejemplo, Windows 3.0 es más antiguo que Windows 3.11, Windows 3.11 es básicamente el mismo Windows 3.0 pero con algunas mejoras.

Virus Programa que se copia a sí mismo y se disemina por una base de datos o red, infectando otros programas y puede causar la destrucción de datos o las averías en los equipos.

VPN, Virtual Private Network. Red privada construida sobre una red pública, y aún así proporcionando privacidad y/o autenticación a los usuarios de dicha red. Los hosts de la red privada utilizan encriptación para comunicarse con otros hosts, pero la encriptación excluye a los hosts del exterior de la red privada.

VPNC, Virtual Private Network Consortium. Asociación de comercio para fabricantes y proveedores del mercado VPN.

W

WAN, Wide Area Network. Red de Área Extensa. Red que conecta hosts en un área geográfica amplia.

WG, Working Group. Aplicado al IETF, grupos de trabajo en los que se divide dicho organismo, cada cual con una finalidad específica y agrupada en distintas áreas comunes, como aplicaciones, seguridad, estandarización, etc.

WWW, World Wide Web. Literalmente, Red Global. Red internacional de información que utiliza HTTP y HTML, y se ubica en hosts de Internet. En un principio se pensó como medio de distribución de información entre investigadores dispersos geográficamente, y se empezó a utilizar en el CERN (Centro Europeo de Investigación Nuclear).

X

X.400 Protocolo para e-mail desarrollado por el CCITT e incorporado por la ISO como parte de la familia de protocolos OSI. Define la forma de los mensajes y del correo electrónico.

X.500 Protocolo OSI diseñado para mantener directorios en línea de usuarios y recursos y para restaurar información en vez de actualizarla. Es necesario para soportar X.400.

X.509 Especificación de certificado de clave pública como parte de X.500 y a menudo utilizado en sistemas de clave pública.

X9.42 Especificación de métodos de uso de los algoritmos Diffie-Hellman.