UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO.

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGON

SISTEMA INTEGRAL DE REDES DE COMPUTADORAS (INTRANET – EXTRANET)

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

ESTHER GUIDO CRUZ

MARÍA TERESA RAMOS SÁNCHEZ

ASESOR DE TESIS
ING. JOSÉ GONZÁLEZ BEDOLLA

MÉXICO 2005

Cariñosamente a mis maestros.

Quienes me enseñaron con paciencia, dedicación y amor,
A escalar los peldaños rumbo a la cima de mi propia montaña.
Gracias..
Muchas gracias.

A mi querida Universidad.

Gracias por todas las enseñanzas que me diste,
En mi camino rumbo a la cima.

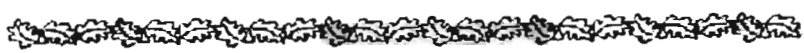
A mis padres cariñosamente.

Me dieron la vida, brindándome así
la gran oportunidad para mi desarrollo.

Los amo....

Gracias a Dios.

Por permitirme llegar hasta aquí.



Dedico este proyecto a mi familia
por su apoyo y comprensión para lograr
este sueño, que cuando lo inicie no creí concluir,
a mis padres por todos los sacrificios
que me brindaron a lo largo de toda mi vida.

A Toño por ser un gran compañero,
no lo habría logrado sin ti,
a Sergio y Daniel porque sólo verlos me
inyecta energía y valor para continuar.
a mis hermanos y amigos por estar ahí

Al Ing. José González Bedolla
Por creer en nosotras.

A la UNAM por ayudarme a hacer
realidad este sueño.

A Dios solamente gracias .....

Tere

ÍNDICE

OBJETIVO GENERAL:

" Conocer como se desarrolla un sistema integral de computadoras bajo el enlace Intranet-Extranet por medio de la tecnología VPN (Virtual Private Network), estableciendo la metodología para la comunicación de una empresa. Permitiendo con ello que el estudiante de la carrera de Ingeniería en Computación se involucre en el conocimiento de las mismas. "

OBJETIVOS ESPECÍFICOS:

" Identificar los diferentes tipos de redes que existen, profundizando en las redes privadas y públicas "

" Describir los aspectos más importantes sobre las tecnologías de Intranets y Extranets, partiendo de los conceptos básicos hasta sus aplicaciones, analizando los beneficios y limitaciones que ofrecen a la empresa "

" Vincular la tecnología VPN con la Extranet, para con ello establecer una metodología eficiente en la incorporación de la Extranet a la Intranet, llevando a cabo este proceso al abarcar las distintas áreas del enlace con la tecnología de las VPN "

INTRODUCCIÓN:

No cabe duda que las redes de computadoras, hoy por hoy, son una herramienta indispensable en las empresas que manejan grandes volúmenes de información.

En este nuevo milenio, se hace indispensable entender que el futuro de las comunicaciones en el mundo, están liderizadas por las redes. Desde el momento en que nos conectamos a Internet, somos una PC mas, en la red más grande que el hombre haya podido crear.

Hoy en día ya no es extraño entrar a una empresa y encontrar que exista instalada una red de área Local (LAN), si bien, al aumentar la demanda de procesar y obtener información, así como la necesidad de compartir recursos para convertirnos en parte importante de un equipo, ha llevado a mejorar las técnicas de procesamiento de datos, creando así los grandes avances de la tecnología informática, que han hecho de las comunicaciones digitales una de las herramientas más importantes de la era actual.

Así pues, a lo largo del presente trabajo se tratará de demostrar la importancia de las tecnologías empleadas en el mundo de las comunicaciones, pretendiendo con ello que el estudiante de la carrera de Ingeniería en Computación de la ENEP Aragón, se involucre en el conocimiento de éstas, como son las tecnologías de Intranet, Extranet y las redes privadas o VPN's. De la misma forma trataremos de dar a conocer una metodología que nos permita llevar a cabo la incorporación de la tecnología Extranet a la Intranet. Para ello, este trabajo se encuentra dividido en cinco secciones o capítulos, permitiendo con esto obtener el máximo aprovechamiento del mismo.

En el capítulo I, se establecen los conceptos fundamentales de los sistemas de comunicación, con la finalidad de que el lector no involucrado con el tema sea capaz de comprenderlos. Dentro de éstos, abarcaremos lo referente a los diversos tipos de redes, y en especial se tratarán las redes públicas y privadas permitiéndonos así introducirnos con el tema objeto de esta tesis.

En el capítulo II, se hace un estudio detallado de la tecnología de Intranets, abarcando desde sus fundamentos y aplicaciones, así como analizando los beneficios y limitaciones que ofrece dicha tecnología a la empresa.

De la misma forma que en la sección anterior, en el tercer capítulo se tratarán los conceptos fundamentales de la tecnología Extranet, así como sus aplicaciones. Además comenzaremos a introducirnos en la tecnología de las VPN's o redes privadas virtuales.

En cuanto al capítulo IV, considerado como uno de los más importantes, se hace un estudio detallado de las fases necesarias para la implantación de una metodología de enlace con la que nos permita incorporar la extranet a la Intranet, por medio de la tecnología de las redes privadas virtuales o VPN´s.

Y para concluir, en el quinto y último capítulo, se tratarán algunos aspectos importantes en cuanto al mantenimiento de la tecnología VPN, además de abarcar algunas tecnologías emergentes para dicha tecnología, con el fin de llevar a cabo un control adecuado de los recursos de nuestro sistema, es decir, contar con una administración eficiente del mismo.

CAPÍTULO I

DIFERENTES TIPOS DE REDES

CAPÍTULO I. DIFERENTES TIPOS DE REDES.

En este capítulo se pretende dar a conocer un panorama de los diferentes tipos de redes que existen, profundizando en las redes privadas y públicas que nos servirán para introducirnos en el tema objeto de esta tesis.

1.1 CONCEPTOS BÁSICOS.

1.1.1 Red

Una RED es un conjunto de equipos que están conectados entre sí a través de enlaces permanentes, utilizando software o protocolos compatibles, con el propósito de "compartir" recursos (ya sean archivos, impresoras, o cualquier recurso que pueda ser considerado de utilidad común para un grupo de usuarios) e información mediante el uso de técnicas específicas, permitiendo con esto, satisfacer las necesidades de funcionalidad, flexibilidad y economía. Por lo tanto, tiene aplicaciones en cualquier empresa, banco, gobierno, industrias, aeropuertos, etc.

Básicamente las redes se encuentran conformadas por nodos y enlaces:

1.1.2 Nodo

Los nodos son el punto de unión entre varias redes, los cuales interconectan enlaces, es decir, son los elementos de la red encargados de transferir la información desde un enlace a otro. Cualquier dispositivo conectado a la red generalmente recibe el nombre de nodo.

1.1.3 Enlace

Un enlace es el conjunto de medios de comunicación, que nos permite establecer uno o más canales de transmisión entre dos o más puntos de la red.

- Se pueden clasificar de dos formas: dependiendo de qué tipos de dispositivos, para qué fines y con qué rutas se esté enlazando, los enlaces podrán ser: **Troncales y de usuario.** Así mismo, se clasifican según cuántos ETD (Equipo Terminal de Datos) enlazan, teniendo con esto: ***Enlaces punto a punto:*** donde un enlace atiende un equipo en cada extremo; ***Enlaces multipunto***: un equipo primario (o maestro) está conectado a varios equipos secundarios (o esclavos) mediante un enlace, teniendo un extremo para el primario y varios extremos secundarios conectados en paralelo; ***Enlace difuso***: en el que varios equipos se conectan entre sí, pero no existe una jerarquía para los extremos de los enlaces ni para los equipos.

Enlace	lan	man	wan
PaP	**SI**	**SI**	**SI**
MP	**NO**	**NO**	**SI**
Difuso	**SI**	**SI**	**NO**

La relación que existe entre los enlaces y las redes se puede ver en la tabla.

Nota: La clasificación de las redes de acuerdo a su extensión geográfica (LAN, MAN y WAN) se verán con detalle en el apartado 1.2.1.1

Fig. 1.1 Enlace Punto a Punto

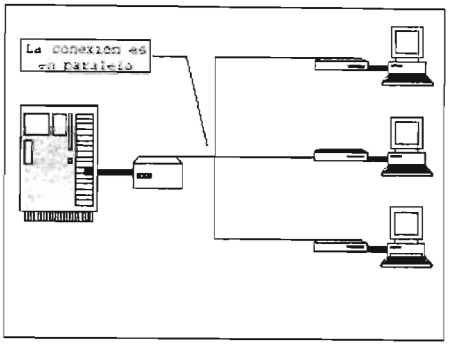


Fig. 1.2 Conexión Multipunto

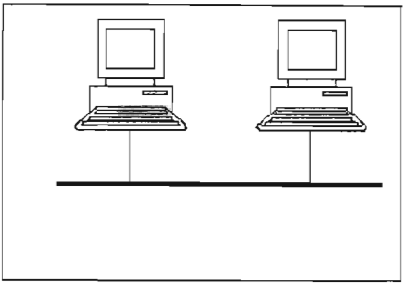


Fig. 1.3 Enlace Difuso

1.1.4 Medios de transmisión

El medio de transmisión constituye el elemento físico a través del cual se transporta la información. Sus parámetros más significativos a considerar son el ancho de banda, la longitud, la fiabilidad, seguridad, facilidad de instalación y coste.

Cable Coaxial.- Consta de un par de conductores de cobre o de aluminio. Uno de ellos forma un alma central y está rodeado por el segundo conductor constituido por una malla muy fina de hilos trenzados o una lámina metálica cilíndrica. Existe el cable coaxial delgado y el cable coaxial grueso.

Cable de Par trenzado.- Éste puede ser apantallado o sin apantallar. Al cable apantallado se le conoce frecuentemente por el acrónimo STP (shielded Twisted Pair), mientras que al cable no apantallado es conocido como UTP (Unshielded Twisted Pair). Por su menor sensibilidad a las interferencias y menor atenuación, el cable STP es más adecuado para mayores distancias y velocidades de transmisión, así como para operación en entornos con interferencias, si bien, la tendencia es utilizar cable UTP siempre que sea posible por su bajo costo y sencillez de instalación.

Cable de Fibra Óptica.- Constituye el medio de transmisión más reciente y el de mayor potencial para redes de alta velocidad. La fibra óptica está constituida por un núcleo circular muy fino de fibra de vidrio (silicio) transparente, capaz de conducir en su interior la energía óptica, rodeado por un revestimiento de otro tipo de vidrio, con diferente índice de refracción, y todo el conjunto se encuentra envuelto con una cubierta opaca y absorbente de luz.

Tecnología de radio.- En algunos entornos el tendido de cables puede resultar difícil, debido a los cambios de lugar de trabajo del personal. Una solución a este tipo de problemas puede ser la utilización de redes inalámbricas. Las principales técnicas utilizadas transmiten en los espectros UHF (Ultra High Frecuency, de 300 MHZ a 3 GHZ), y microondas (banda SHF, Super High Frecuency, de 3 GHZ a 30 GHZ).

1.2 CLASIFICACIÓN DE LAS REDES.

Para el estudio de las redes, se tienen o se pueden hacer distintos enfoques según las características que se analicen, y cada una de éstas da lugar a varios tipos de red específicos. Así podemos clasificarlas según se muestra en el cuadro sinóptico de la siguiente página.

1.2.1 Descripción General de los Diferentes Tipos de Redes.

Como hemos visto, no existe una regla o clasificación general dentro de la cual se abarquen todas las redes de computadoras, pero si podemos identificar una gran variedad de ellas.

Ahora bien, para nuestro estudio, sólo se dará un panorama amplio de estos tipos de redes, en el que se describirán los aspectos más importantes de cada clasificación de las redes:

1.2.1.1 POR SU EXTENSIÓN GEOGRÁFICA

Redes de área local (LAN, Local Area Network).- Son redes que interconectan equipos dentro de un entorno físico reducido. En general, no se extienden más allá de un edificio, recinto o campus, utilizan sólo un tipo de medio de transmisión.

Redes de área metropolitana (MAN, Metropolitan Area Network).- Son más grandes que una LAN y normalmente, cubren una ciudad. Por lo regular, se utilizan diferentes medios de transmisión y hardware, debido a las distancias que hay que recorrer y a las aplicaciones que tiene la red.

Redes de área extensa (WAN, Wide Area Network).- Son las que unen equipos instalados en distintos edificios e inclusive en distintas ciudades. Utilizan normalmente enlaces de telecomunicación de la compañía telefónica.
Se dice que interconectan LANs que pueden estar en lugares opuestos de un país o del mundo.

Cuadro Sinóptico

Clasificación de las Redes

- Por su extensión Geográfica
  - Red de área Local (LAN)
  - Red de área metropolitana (MAN)
  - Red de área amplia (WAN)
- De acuerdo a su Topología
  - Red tipo Barra o Bus
  - Red tipo Anillo
  - Red tipo Estrella
  - Red tipo Malla
- Por su técnica de Transmisión
  - Banda Base
  - Banda Ancha
- De acuerdo a su Método de Acceso
  - CSMA/CD
  - Token Bus
  - Token ring
  - Token Passing
- Según su modelo de Procesamiento
  - Procesamiento Centralizado
  - Procesamiento Distribuido
  - Procesamiento Colaborativo
- De acuerdo al Protocolo de Comunicación
  - Redes TCP/IP
  - Redes UDP/IP
  - Redes Apple Talk
  - Redes SNA
- De acuerdo a su uso
  - Redes Comerciales
  - Redes Educativas
  - Redes sociales
- De acuerdo a su Arquitectura o Tecnología
  - Redes Ethernet
  - Redes Arnet
  - Redes Token Ring
- Según el sistema Operativo que Utilizan
  - Windows
  - Unix
  - Netware
  - NT
  - Lantastic
- De acuerdo a su conmutación
  - Redes de conmutación de paquetes
  - Redes de conmutación de circuitos
- Según los servicios que satisfacen a los usuarios
  - Redes p/servicios básicos de Transmisión
  - Redes para servicios de Valor Añadido
- Por las señales que transportan
  - Redes Analógicas
  - Redes Digitales
- Por el servicio que se realice entorno a la empresa
  - Redes Interempresa
  - Redes Intraempresa

1.2.1.2 DE ACUERDO A SU TOPOLOGÍA

Este análisis depende de la estructura física o lógica de la red en que se encuentran conectados sus elementos constitutivos principales, nodos y enlaces, dando lugar a distintos tipos de redes, siendo básicamente cuatro:

Redes tipo Barra o Bus: Su diseño es simple, el cual se representa como una barra, en donde todas las estaciones se conectan a un único medio bidireccional lineal (cable largo llamado backbone troncal), a través del uso de conectores "T" o cable drop, Su medio de transmisión es de amplia cobertura (broadcast medium), esto es, todas las estaciones reciben la información que se transmite (una estación transmite y las restantes escuchan). Su desventaja es que puede quedar inhabilitada toda la red al existir algún daño en cualquier punto del cable.

Redes tipo Anillo: Esta es una estructura circular, donde la información viaja en un solo sentido a través de un único cable, por lo que el mensaje se repite y se transmite de terminal a terminal (cada estación recibe el dato y lo envía a la estación siguiente del anillo). En este tipo de red, los cuellos de botella son muy poco frecuentes, pero su mayor inconveniente es, que al existir una sola línea de comunicación, si falla un equipo o el propio cable, todas las estaciones quedarán incomunicadas.

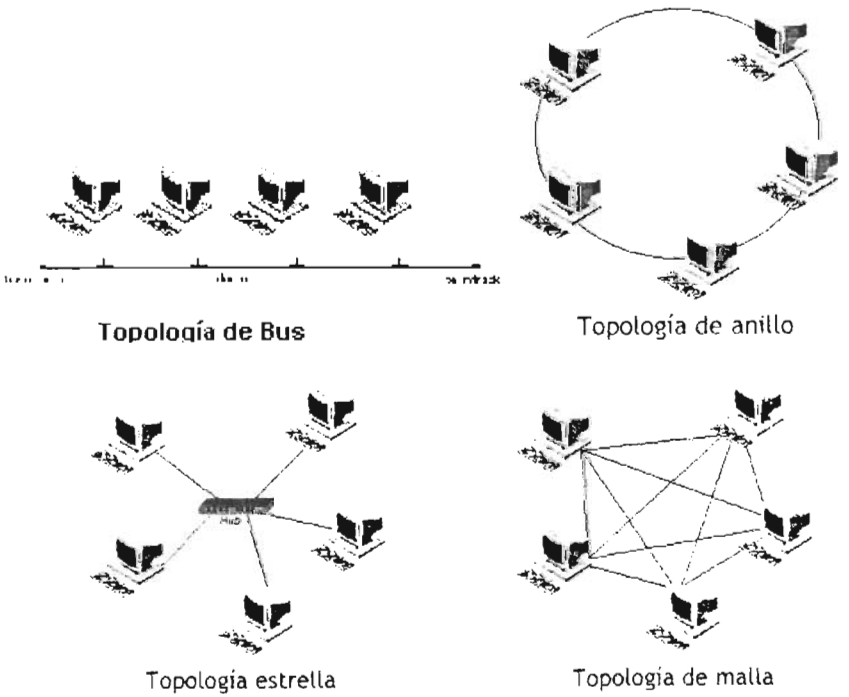


Fig. 1.4 Diferentes Topologías

Redes tipo Estrella: En esta estructura, todas las estaciones se encuentran conectadas mediante enlaces bidireccionales (conexión punto a punto) a un dispositivo central o host conocido como hub, concentrador o repetidor multipuerto, el cual está encargado de controlar el tráfico. La ventaja de emplear este tipo de red, es que si algún punto falla, la red seguirá funcionando de manera normal y sólo se inhabilitará la porción en fallo, de lo contrario, si el nodo central es el que llega a fallar, toda la red quedará incomunicada.

Redes tipo Malla: Este tipo de redes está formada por varios nodos, así como gran disponibilidad de enlaces punto a punto entre ellos (todos con todos), por su configuración estos nodos pueden ser terminales o finales (end node) y nodos de paso o intermediarios (intermediate node). Los nodos de estas redes pueden trabajar de dos formas, ya sea con un enlace activo a un tiempo, o todos activos al mismo tiempo, en cuyo caso los nodos son los encargados de llevar el control de la comunicación.

1.2.1.3 POR SU TÉCNICA DE TRANSMISIÓN

Son las redes que por su técnica de transmisión envían señales moduladas y sin modulación.

Redes de Banda Base.- En éstas, la señal se transmite sin modulación, por lo que cada vez que se realiza una transmisión se utiliza todo el ancho de banda del medio. La ventaja en este tipo de transmisión es su sencillez, ya que no requiere moduladores y demoduladores. La desventaja es la distorsión de la señal con la distancia, por lo que se utilizan repetidores para regenerar la señal. El sistema de codificación más empleado es el Manchester.

Redes de Banda Ancha.- Estas redes, utilizan señales analógicas moduladas y normalmente emplean como medio de transmisión el cable coaxial.
Las ventajas principales de este tipo de redes son, la posibilidad de integrar todo tipo de señales en un solo medio y la gama de distancias que pueden abarcar. Por otro lado la utilización de módems hace que la red resulte costosa, además requiere de una mayor planificación.

1.2.1.4 DE ACUERDO A SU MÉTODO DE ACCESO

Durante la transmisión de datos a través de una red, pueden surgir conflictos que afectan la comunicación, es por ello que existen ciertos mecanismos con el fin de resolverlos. Para el caso de una configuración en BUS, se emplea CSMA/CD y Token Bus, mientras que en una configuración anillo será Token Ring.

CSMA/CD (Acceso Múltiple Sensible a Portadora con Detección de Colisión): Este mecanismo consiste en redes con escucha de colisiones, lo cual significa que cada estación antes de transmitir debe cerciorarse si está libre o no el canal, si lo está, puede transmitir libremente y quedar escuchando posibles colisiones, de lo contrario, si el canal está ocupado, debe esperar un intervalo de tiempo y volver a reintentar la transmisión.

Token Bus: Este es un mecanismo más eficiente que el anterior, ya que evita el problema de las colisiones. En este caso, se emplea una trama de datos (Token), que pasa de estación en estación en forma cíclica (anillo lógico), donde únicamente la estación que tenga el Token podrá transmitir o recibir datos en un tiempo determinado, mientras que las demás esperarán su turno.

Token Ring: Este caso se utiliza en una configuración tipo anillo, donde las estaciones se conectan por una unidad de interfaz (RIU) encargadas de controlar el paso de los datos por ellas, regenerar la transmisión y pasarla a la siguiente estación. El mecanismo del Token Ring funciona de la manera siguiente: el Token pasa de estación en estación en forma cíclica en estado desocupado, si una de ellas quiere transmitir, su estado cambia a ocupado, agregando los datos atrás de la trama. Cuando el Token pasa nuevamente por la estación que transmitió, saca los datos y regresa a un estado desocupado.

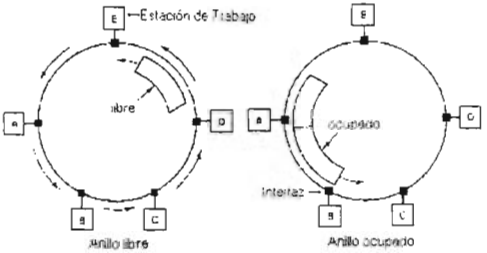


Fig.1.5 Método de Acceso Token Ring

Redes Token-Passing.- Las redes basadas en *token passing*, llevan el control de acceso al medio a través de la posesión del token, el cual permite transmitir determinada información a la estación que lo posee por un periodo limitado de tiempo, mientras que las demás estaciones deben esperar su turno para poder transmitir, por lo tanto, es difícil que se presenten colisiones.

El funcionamiento del Token-Passing se describe a continuación: Si una estación que posee el token desea transmitir, divide el token alterando un bit de éste, el cual cambia a una secuencia de start-of-frame, abre la información que se desea enviar, y la manda hacia la siguiente estación en el anillo, circulando así alrededor de la red hasta localizar la estación destino encargada de procesar dicha información. Una vez con ello, la información del frame es borrada cuando regresa a la estación desde la cuál se envió, checando si se encontró la estación destino y se entregó la información correspondiente (Acuse de recibo).

A diferencia de las redes que utilizan CSMA/CD (como Ethernet), las redes token-passing están caracterizadas por la posibilidad de calcular el máximo tiempo que pueden permanecer en una terminal esperando que éstas transmitan.

1.2.1.5 SEGÚN SU MODELO DE PROCESAMIENTO

Para el manejo de la información en el uso de redes, se debe tomar en cuenta el modelo de procesamiento que se emplea, siendo básicamente tres tipos de modelos los que existen: centralizado, distribuido y colaborativo.

Procesamiento Centralizado: Este modelo consiste de una computadora central (mainframe), quien es la encargada de llevar el control de la información (por ejemplo el almacenamiento). Así también se cuenta con terminales que son simples dispositivos remotos de entrada y salida.

Procesamiento Distribuido: En este caso, el procesamiento de la información se distribuye a varias computadoras y no a una sola, para que con ello cada una cumpla con una función específica, logrando así, alcanzar los mismos objetivos.

Procesamiento Colaborativo: Es un tipo de procesamiento distribuido, que a diferencia del anterior, emplea dos o más computadoras para lograr la misma tarea, ya que comparten habilidades de procesamiento.

1.2.1.6 DE ACUERDO AL PROTOCOLO DE COMUNICACIÓN

Son las redes que tienen el mismo conjunto de normas para la transmisión de mensajes y están presentes en todas las etapas necesarias para establecer una comunicación entre equipos de cómputo.

Redes TCP/IP.- El protocolo IP, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino. TCP, o Transmission Control Protocol, se asegura que los paquetes lleguen correctamente a su destino, es decir, se encarga del enrutamiento de los paquetes de información. Si TCP determina que un paquete no ha sido recibido, intentará volver a enviarlo hasta que sea recibido correctamente.

Sin debate TCP/IP es la suite de protocolos con soporte más amplia en el mundo, así también, es el estándar utilizado por UNIX y Linux por sus aplicaciones con redes locales (LAN).

TCP/IP presupone independencia del medio físico de comunicación. Internet es el mejor ejemplo de este tipo de redes.

Redes UDP/IP .- Estas al igual que TCP necesitan de IP para transmitirse (se dice que están en otra capa). Sólo que UDP se limita a enviar el paquete (aquí llamado *datagrama*), sin preocuparse si llega a su destino. Aunque parezca ilógico, UDP es necesario para cierto tipo de tareas.

Redes AppleTalk.- AppleTalk es un protocolo propio que se utiliza para conectar ordenadores Macintosh de Apple en redes locales. LocalTalk es un sistema de cableado fácilmente configurable, que permite conectar estaciones de trabajo y otros dispositivos, como impresoras o escáneres, a un entorno de red appletalk. Local talk se estructura en una topología de bus.

Redes SNA (System Network Architecture) .- Ésta es una arquitectura de red creada en 1974 por IBM, que permite la comunicación entre sistemas. Dicha arquitectura es compleja y rica en prestaciones, desarrollada con el protocolo SNAP (Protocolo de Internet), el cual opera entre una entidad de red de la subred y una entidad de Servicio de distribución SNA.

1.2.1.7 DE ACUERDO A SU USO

Comerciales: Las redes comerciales, básicamente proveen los servicios de "correo electrónico" (Compuserve, AT&T Mail, MCI Mail, GeoNet, CGNET, etc.) y de "bases de datos" (Dialog, DataStar, etc.). Este tipo de redes pueden ser excelentes fuentes de información sobre ciencia, tecnología o políticas gubernamentales publicadas en revistas comerciales; en muchos casos son accesibles utilizando redes de conmutación (packet switching networks); así también, pueden ser muy costosas para los países en desarrollo, pero bien, son ampliamente utilizadas en los países industrializados, donde su acceso es económico.

Educativas: La utilidad de este tipo de redes, es el facilitar el trabajo de los investigadores, ofreciendo una mayor rapidez en el intercambio de información, ya sea de forma directa (mensajería), global (conferencia electrónica), o compartiendo bases de datos o capacidades de cálculo. Permitiendo con esto, la creación de aplicaciones o redes de información específica en los campos de la investigación, por ejemplo, se encuentra la red de enlace y acción sobre el cáncer, un banco de datos de partituras de música clásica, un sistema de difusión de periódicos científicos, entre muchos otros ejemplos.
Las redes educativas existentes son la EARN interconectada con Europa y la BITNET, con vocación norteamericana, ambas conectadas a redes nacionales (JANET o DFN).

Sociales: Las redes sociales, son la integración de instituciones públicas y/o privadas, comunidades o líderes que coordinan, comparten e intercambian conocimientos, experiencias y recursos, con el propósito de alcanzar un objetivo común, en respuesta a una situación determinada. Estas redes, pueden ser gubernamentales, no gubernamentales e interinstitucionales, y a su vez pueden ser *temporales* cuando se integran varios actores (organizaciones o grupos de personas) alrededor de un programa o proyecto específico y *permanentes* cuando varios actores integran esfuerzos de mediano y largo plazo en función de objetivos y metas comunes.

1.2.1.8 DE ACUERDO A SU ARQUITECTURA O TECNOLOGÍA

Es el tipo de red, en que el conjunto de servicios y protocolos constituyen el soporte de su infraestructura.

Redes Ethernet.- Ethernet es el nombre de una de las redes de área local más populares hoy en día. Inventada por Xerox PARC a principios de los 70's. Esta versión fue estandarizada por Xerox Corporation, Intel Corporation y Digital Equipment Corporation en 1978. IEEE sacó una versión compatible con la norma bajo el número 802.3. La tecnología ethernet consiste fundamentalmente en un cable coaxial llamado *ether* de hasta 500 metros de longitud, la cual, dicha distancia puede ser extendida por medio de dispositivos llamados repetidores, que duplican señales eléctricas de un cable a otro. Sólo dos repetidores pueden ser usados entre dos computadoras, por lo que la longitud máxima de un ethernet es bastante moderada (1500 metros). Las redes modernas utilizan la tecnología Ethernet como medio. Ahora bien, se puede distinguir entre Ethernet (10 Mbps), Fast Ethernet (100 Mbps) y Gigabit-Ethernet(1000 Mbps).

Redes Token Ring.- Las redes Token Ring originalmente fueron desarrolladas por IBM en los años 1970´s. Éste fue el primer tipo de Red de Area Local de la tecnología IBM (LAN). En base a las especificaciones de esta red se modelo el estandar IEEE802.5. El término Token Ring es generalmente usado para referirnos a ambas redes, IBM's Token Ring e IEEE 802.5, aunque éstas no sean idénticas.

Redes Arnet.- Es una red de banda base que utiliza una topología mixta estrella/bus con protocolo de paso de testigo. Transmite a una velocidad de 2.5 Mbps y todas las computadoras han de estar conectadas a un concentrador (HUB activo). La distancia máxima entre la computadora y el hub activo no puede sobrepasar los 660 metros.

1.2.1.9 SEGÚN EL SISTEMA OPERATIVO QUE UTILIZAN

El **Sistema Operativo** es la base del funcionamiento de la computadora en general (por supuesto de la parte correspondiente al software), ya que es quien se encarga en principio de la gestión de los recursos del sistema y de realizar las operaciones que solicitan los programas. Por ejemplo, crear la infraestructura lógica que permitirá grabar datos en los discos y disquetes, así como generar, abrir, eliminar y mover archivos, administrar la memoria, manejar la interface, entre otras funciones.

La oferta de **sistemas operativos** disponible para computadoras personales en la actualidad no es demasiado amplia. La mayoría de las PC´s hogareñas cuentan con el famoso y popular Windows 9*/00/NT/ME/SE y ahora XP, los cuales tienen como ventaja, la facilidad de conexión en red. De todas maneras, existen otras marcas de S.O. especialmente diseñados para tareas especificas, como lo es "el trabajo en redes", donde encontramos: **NOVELL NETWARE, LANTASTIC, WINDOWS NT SERVER, y principalmente UNÍX junto con sus variantes, como SunOS, FreeBSD, NetBSD, OpenBSD y Mac OS X, donde vemos que cada vez más está creciendo su campo de uso, así también dentro del sistema operativo UNIX se crearon otros sistemas operativos como lo son Solaris, Linux, SCO, BSD, etc. quienes a su vez, su campo de empleo crece día con día.**

Cada uno de estos sistemas operativos de red tienen diferentes requerimientos de hardware para funcionar correctamente, si éstos no son satisfechos, el sistema puede no operar o trabajar en un nivel muy por debajo del esperado, ocasionando serios problemas en la red.

1.2.1.10 DE ACUERDO A SU CONMUTACIÓN

Redes de conmutación de paquetes.- Son redes en las que existen nodos de concentración con procesadores que regulan el tráfico de paquetes.

Redes de conmutación de circuitos.- Son redes en las que los centros de conmutación establecen un circuito dedicado entre dos estaciones que se comunican.

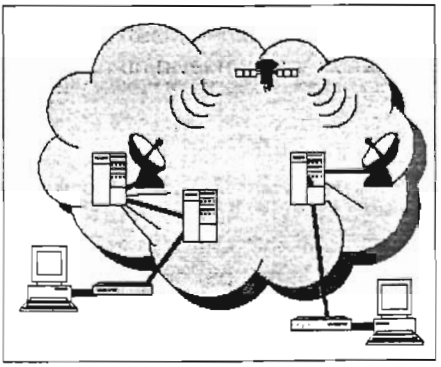


Fig. 1.6 Red Conmutada
Dos Equipos Terminales de Datos comunicados por un trayecto.

1.2.1.11 SEGÚN LOS SERVICIOS QUE SATISFACEN A LOS USUARIOS

Para esta clasificación, únicamente encontramos dos tipos de redes, los cuales dependen de la información, si se ve alterada o no, según el servicio que se ofrezca.

Redes Para Servicios Básicos de Transmisión: Son redes que dan servicio sin llegar a alterar la información que transmiten. Por ejemplo, tenemos la red telefónica, las redes dedicadas y las redes de conmutación de circuitos.

Redes Para Servicios de Valor Añadido: Como su nombre lo dice, son redes que no sólo realizan la transmisión de información, sino que además actúan sobre ella de algún modo. Como ejemplo encontramos a las redes que gestionan mensajes, la transferencia electrónica de fondos, el acceso a Bases de Datos, etc.

1.2.1.12 POR LAS SEÑALES QUE TRANSPORTAN

Redes Analógicas.- Utilizadas en un principio en las redes telefónicas. Las redes analógicas puras, a pesar de su uso extensivo durante casi un siglo, presentan dos graves inconvenientes intrínsecos a su misma naturaleza. Por un lado, el ruido que inevitablemente se introduce, resulta prácticamente imposible de eliminar, por otro, están las dificultades para el almacenamiento, la reproducción fidedigna y el análisis de las señales transmitidas. La combinación de ambos problemas, impide dar servicios como el ruteo y limita la detección de errores, imprescindibles para la transmisión de datos. Otro inconveniente es el de la multiplexión que resulta excesivamente compleja cuando se han de conmutar por separado varios canales.

Redes Digitales.- Éstas utilizan información convertida al código binario, es decir, cada bit se representa por una variación de voltaje. Las tecnologías digitales han demostrado ser más sólidas que sus equivalentes analógicas, simplemente porque resultan más fáciles de manipular y almacenar. La utilidad de los nodos digitales, que integran en una sola operación conmutación y transmisión, dió lugar a las denominadas "Integrated Digital Network" (IDN) o redes totalmente digitales de extremo a extremo. Si a estas redes les añadimos unos estándares universales de acceso, empezaremos a estar muy cerca de lo que se conoce como "Integrated Services Digital Network" (ISDN).

1.2.1.13 POR EL SERVICIO QUE SE REALICE EN TORNO A LA EMPRESA

Redes Intraempresa.- Son aquellas en las que el servicio de interconexión de equipos se realiza en el ámbito de la empresa.

Redes Interempresa.- Son las que proporcionan un servicio de interconexión de equipos entre dos o más empresas.

1.2.2 REDES PRIVADAS.

La clasificación de las redes según su carácter se hace de acuerdo al modo de ser utilizadas y compartidas, teniendo con ello, redes de carácter público o de carácter privado.

El desarrollo de las redes privadas surge por la necesitad de mantener un control eficiente y seguro en el manejo de la información "dentro" de una empresa, por lo que se busca restringir el acceso a ellas, es decir, estas redes sólo son operadas por personas particulares, empresas u organizaciones de índole privado, y tienen acceso únicamente las terminales de los propietarios.

1.2.2.1 ¿Qué son las Redes Privadas?

Una red privada es una red de comunicaciones privada construida, mantenida y controlada por la organización a la que sirve. Como mínimo una red privada requiere sus propios equipos de conmutación y de comunicaciones. Así mismo, puede emplear sus propios servicios de comunicación, o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus propias líneas de comunicaciones.

1.2.2.2 Objetivos

El objetivo principal del uso de las redes privadas, es que el dueño tiene el control completo, éste se encarga de establecer las normas que determinan cómo y cuándo usar la red, así como las computadoras que se conectan. De la misma manera, el dueño garantiza que la red está aislada de las computadoras ajenas a la organización y que una computadora no haga contacto accidental con otra de otra organización. El aislamiento refuerza la seguridad, pues mantiene protegidos los datos de la empresa y evita la interferencia de extraños en las computadoras y la comunicación de la misma.

Existen muchas compañías donde la **seguridad** es imperante, así como también lo es el **control sobre el tráfico de datos**, y son las líneas privadas las que constituyen la única garantía de un alto nivel de servicio.

1.2.2.3 Aplicación

Las redes privadas básicamente pueden utilizarse en infinidad de empresas, donde la necesidad de compartir y distribuir información a los empleados de una misma Corporación, debe ser de manera eficaz y segura.

1.2.3 REDES PÚBLICAS

Algunas razones para favorecer el desarrollo de redes de datos públicas es que el enfoque de redes privadas es muchas veces insuficiente para satisfacer las necesidades de comunicación de un usuario dado. La falta de interconectabilidad entre redes privadas y la demanda potencial de información entre ellas, en un futuro cercano favorecen el desarrollo de las redes públicas.

1.2.3.1 ¿Qué son las Redes Públicas?

Para este punto, primeramente hay que definir el término "público" aplicado a una red, el cual se refiere a la **disponibilidad del servicio y no a los datos transferidos**.

Entonces, las redes públicas pertenecen y son operadas por un proveedor de servicio, como puede ser una compañía privada de teléfonos, telégrafos, etc., y se encuentran disponibles a toda persona que se suscriba al servicio desde cualquier lugar. Si bien, este tipo de redes están abiertas a todos, pero ofrecen comunicación privada. -cuando 2 computadoras intercambian información entre redes públicas, sólo ellas reciben copias de los datos-.

Las redes públicas son generalmente de conmutación de paquetes o de conmutación de circuitos, y los servicios son prestados por compañías que se dedican a transportar señales, llamadas prestadores o carriers.

Dentro de estas compañías se incluyen:

- Compañías de servicios de comunicación local. Que dan cobertura urbana, por ejemplo TELCOR.
- Compañías de servicios de comunicación a larga distancia (IXC: Interexchange carriers) : Dan cobertura interurbana, como AT&T, MCI y US SPRINT.
- Proveedores de servicios de valor añadido (VACs: Value-added carriers): Están las compañías CompuServe Information y GE Information Services, las cuales ofrecen con frecuencia, servicios de comunicación de área amplia como complemento a su verdadero negocio.

Las ventajas principales de las redes públicas son: la flexibilidad, donde un número variable de suscriptores desde cualquier parte del mundo puede conectarse a la red, así como la posibilidad de servirse de la tecnología de conectividad más reciente.

1.2.3.2 Objetivos

Las redes públicas se han ido interconectando entre sí para conformar una red de redes de cobertura mundial, que ofrece actualmente múltiples servicios de transmisión de datos a sus usuarios. Estas redes tienden a evolucionar hacia una red de servicios integrados (con voz, datos, imagen y video). Así, millones de personas geográficamente distribuidas, en grandes distancias, pueden beneficiarse de servicios tales como:

- La consulta a bancos de datos
- El intercambio de archivos de información
- La transmisión de imágenes y voz
- La comunicación vía correo electrónico
- Las discusiones en grupos de trabajo internacionales
- Disponibilidad las 24 horas del día
- La elaboración de documentos en grupo
- El acceso remoto a equipo de cómputo

1.2.3.3 Aplicación

En la actualidad, **INTERNET**[1] es una de las redes públicas más extendida, así también, es considerada como un estándar de comunicación que permite conectar diversas redes del dominio público a distintas velocidades y bajo un protocolo de comunicación específico (de tipo TCP/IP). Abarca los cinco continentes del mundo, enlazando a 8000 redes de cómputo que cubren 45 países del globo terráqueo, y se estima que actualmente más de 25 millones de personas utilizan INTERNET para el intercambio de mensajes a lo largo y ancho del mundo.

El éxito de las redes públicas como INTERNET, se debe a que hoy en día hacen uso de ellas muchas empresas que no pueden establecer su propia red de cómputo privada, como lo hacen los bancos o las grandes transnacionales[2].

La topología actual de INTERNET engloba a otras redes como las del CONACYT, RED UNAM, la Red del ITESM, RUTyC y MEXNET, sin embargo, no existe todavía un plan rector de desarrollo para INTERNET en México. La mayoría de los centros de investigación y docencia del país no están integrados a las **redes públicas de cómputo,** y la actividad de éstas es aún muy incipiente en comparación con nuestro vecino país del norte.

---

[1] http://herzog.economia.unam.mx/enlinea/sualin/intronetead/3/3.htm Herramientas básicas de Internet para aprendizaje abierto y a distancia

[2] http://www.econ.uba.ar/www/departamentos/sistemas/plan97/tecn_informac/seoane/seoane/tp/yquiro/redes.htm

1.3 EJEMPLOS DE REDES.

Mencionaremos algunas de las redes más representativas que nos han permitido continuar su estudio, aplicación, y evolución de las mismas.

- ArpaNet - Advanced Research Projects Agency / Network del Depto. de Defensa de los EEUU.
- La red Datapac, canadiense, es la primera red pública en el mundo, que comenzó a operar en 1976, se desarrolla a partir de los conceptos estudiados en ArpaNet. Mas adelante aparecen las redes japonesa y europea.
- La red SITA Société Internationale de Telecommunications Aéronautiques, es una red privada de una organización cooperativa, que sirve a 248 aerolíneas en 154 países, para interconectar sus computadores y terminales de las agencias de venta de pasajes aéreos y asuntos relacionados con las operaciones de vuelo.

Teniendo los conocimientos básicos del área de redes tratados en este capítulo, es posible introducirnos al tema estudio de este proyecto de investigación, donde para continuar es necesario conocer los aspectos fundamentales de las tecnologías a tratar como son la Intranet y la Extranet. Para ello en los capítulos siguientes veremos desde sus fundamentos hasta sus aplicaciones.

CAPÍTULO II

INTRANETS

CAPÍTULO II. INTRANETS

En este capítulo, describiremos los aspectos más importantes sobre la tecnología de Intranets, partiendo de los conceptos básicos hasta sus aplicaciones, analizando los beneficios y limitaciones que ofrece a la empresa.

2.1 FUNDAMENTOS DE INTRANET

El término Intranet define el resultado de años de actividad y de muchos avances tecnológicos. Es en realidad, el producto de décadas de investigación, desarrollo y aplicaciones que han contribuido a llevar a la Intranet a una situación imposible de detener.

Uno de los primeros usos públicos reales del término Intranet se da en 1994, cuando Amdahl se refiere a su Internet interna o privada con el nombre de Intranet. También en 1994, en un artículo de William Safire que se publicó en The New York Times, se introduce el término como parte de un conjunto de nuevas tecnologías, a partir de todo esto, los medios de comunicación lo recogieron y este tipo de red se ha quedado con ese nombre.

Los medios de comunicación escribieron mucho sobre algunas de las primeras organizaciones que crearon redes internas, entre las que estaban Locked Hughes; el SAS Institute; Boeing, Schlumberger Ltd.; Weyerhauser Corp.; Sun Microsystems y Digital Equipment Corp.

Pero, ¿De dónde procede la idea de las redes Intranet?, para contestar esta pregunta, hablemos primero de la historia de Internet y de la Web. El gobierno de los Estados Unidos creó Internet en los años setenta por cuestiones de seguridad nacional, su propósito era proteger las comunicaciones militares en caso de un ataque nuclear. En los años ochenta, la National Science Foundation (NSF), amplió la red para poder incluir a las universidades y facilitar los estudios de investigación. A principios de los años noventa, la NSF permitió que entrasen en Internet intereses comerciales, lo que hizo que su taza de crecimiento aumentara rápidamente, debido al aumento de la comunidad en Internet, empieza a florecer el comercio en la Web.

La World Wide Web es creada en 1989, por Tim Barnes-Lee del Laboratorio Europeo para Física de Partículas, para hacer que el acceso a la información de la Web fuese más fácil, Marc Andreesen y un grupo de estudiantes del National Center for Supercomputing Applications (NCSA) de la Universidad de Illinois crearon un interfaz de usuario gráfico para la Web, al que llamaron Mosaic.

Con la aparición de Mosaic en 1993, algunos negocios se interesaron por las posibilidades de la WEB y de Mosaic. A veces, alguien familiarizado con las herramientas de Internet echaba a andar un programa piloto para determinar si las herramientas podían tener algún valor comercial. Pronto supieron que las herramientas resultaban muy útiles. Cuando se conoció la noticia otras compañías se mostraron interesadas.

En fin, compañías que van desde A (t & t) hasta Z (eneca) están instalando y usando redes Intranet. Estas y otras empresas han descubierto que las ventajas de la facilidad de uso de la tecnología, la flexibilidad del software, el bajo coste del hardware y del software, la habilidad para centralizar la gestión de la Intranet son particularmente convincentes, haciendo que la implantación de la Intranet sea prácticamente irresistible.

En este apartado se tratarán las características más importantes de la Tecnología Intranet, conociendo su significado, las diferencias que existen con la red de redes "Internet", así como los componentes esenciales que forman parte de ella.

2.1.1 ¿QUÉ ES UNA INTRANET?

Para explicar lo que es una Intranet, tomaremos en cuenta dos aspectos importantes, siendo el aspecto técnico y el organizacional.

La definición técnica nos dice, que una Intranet es un ambiente de computación heterogéneo, capaz de conectar diferentes plataformas de hardware, ambientes de sistema operativo e interfaces de usuario, y de esta manera, pueda existir comunicación ininterrumpida, colaboración, transacciones e innovación.

De la misma forma, el aspecto organizacional define a la Intranet como una organización de aprendizaje, que permite la integración de gente, procesos, procedimientos y principios, con el fin de establecer una mayor efectividad en la organización.

Entonces, una INTRANET es un sistema de información dentro de la empresa basado en tecnología Web, es decir, es una red de servicios internos para la empresa (una red privada), la cual se basa en estándares de Internet, sobre todo TCP/IP, donde cualquier usuario, ya sea un cliente, proveedor, personal, etc., podrá acceder a las diversas aplicaciones de la empresa, y el envío de la gran cantidad de recursos de información, será de forma transparente de la organización al escritorio de cada individuo, con un costo, un tiempo y un esfuerzo mínimos.

Para establecer una INTRANET, básicamente se requiere de un servidor Web que generalmente es proporcionado por empresas terceras de servicio; una red dentro de la empresa u organización y equipos de cómputo; también es necesario el uso de un sistema de bases de datos y mecanismos estrictos de seguridad; así como las aplicaciones de comunicación Web, ya sea de mensajería, conferencias, discusiones, búsquedas, directorios, etc.; y por último, se requiere del desarrollo de contenido, refiriéndonos a la publicación de documentos, normas formularios, datos técnicos, etc.

Con el paso del tiempo, se han ido abriendo nuevas ideas que dan pie a la innovación, descubriendo con esto nuevas opciones, y con ello, que las INTRANETS vayan evolucionando. Estos niveles se observan en la siguiente tabla:

Tabla 1. La Evolución de las Intranets.

	INTRANETS BÁSICAS	INTRANETS DE PUBLICACIÓN DE BIBLIOTECAS	INTRANETS PARA COLABORACIÓN	INTRANETS PARA TRANSACCIONES
Descripción	Sitio Web pequeño, de aprox. 50 páginas. Texto, vínculos, gráficos	Mucho más grande. Producción y acceso en línea a documentos y recursos de la empresa.	Sitios de grupos interdependientes. Páginas departamentales. Página de inicio de la intranet centralizada. Conjunto avanzado de herramientas.	Integrada con sistemas heredados y aplicaciones de red. Usa Java, Actives y otros generadores de APIs.[3]
Arquitectura	Servidor y navegador Web central. Software de servidor. Herramientas de edición. TCP/IP	Elementos básicos, software de publicación, administración de documentos, máquinas de búsqueda e integración de bases de datos.	Intranet de servicio completo con capacidades de administración de directorios, archivos, impresión y correo. Se integra con software para trabajo en grupo, software de administración de proyectos y sistemas de correo electrónico.	Servidor de intranet de servicio completo. Integración segura con bases de datos corporativas heredadas y todas sus aplicaciones.
Controladores de Costo	Inversión mínima en hardware y software.	Costos de empleados y herramientas. Aumento en equipo y proceso.	Aumento exponencial en costos generales de operación. Los costos de desarrollo se vuelven el eje central.	Integración completa de todos los costos de sistemas de información.
Limitaciones	Capacidad.	Exactitud.	Mantenimiento.	Seguridad.

NOTA: Esta evolución inicia con las Intranets básicas hasta las intranets extendidas o lo que hoy conocemos como Extranets. Las Extranets se verán con detalle en el capítulo 3 de este trabajo.

[3] APIS – Interfaces para Programación de aplicaciones.

2.1.2 DIFERENCIAS ENTRE INTERNET E INTRANET

Intranet es un Sistema de Comunicaciones idéntico a Internet, ambas están basadas en la tecnología de Internet, donde existen varios elementos estandarizados, como son: los protocolos de comunicación TCP/IP, HTTP, servidores y navegadores Web, edición de HTML y programación de aplicaciones Web. Por ello, podemos decir que estas dos tecnologías son iguales, pero lo que las separa es **"su uso y no su tecnología".**

Para establecer una comparación más amplia, es necesario conocer algunas de las características más significativas de estas dos tecnologías, Internet y la Intranet.

Primeramente, INTERNET se diseñó para el consumo público, siendo éste el consumidor, el cliente y el estudiante. Internet es una excelente fuente de investigación educativa puesto que es posible tener acceso a grandes bases de datos en todo el mundo, cuenta con un gran número de herramientas de búsqueda y la calidad de información es extraordinaria y de libre distribución. Así mismo, en esta tecnología, todo individuo puede presentar sus ideas, productos, mercancías, etc., para compartirlos con la comunidad.

Con la llegada de las transmisiones seguras en línea, Internet ha evolucionado hasta entrar en un ámbito de transacciones financieras, dando lugar al comercio electrónico, en el que es posible comprar productos a través de la red de una forma más sencilla y segura. Por lo tanto, "Internet es la tecnología que permite que la gente se concentre en la forma de hacer dinero y de ser más inteligente".

Por otro lado, las INTRANETS tienen el objetivo de mejorar los procesos de negocios y reducir los ciclos de vida del desarrollo, y aunque su aplicación al mundo de las organizaciones y entornos laborales es relativamente reciente, se puede decir que la Intranet apareció mucho antes que Internet, ya que las primeras redes que dieron base a la actual Internet se limitaban a entornos de investigación reducidos como universidades y organizaciones gubernamentales.

Esta tecnología se concentra en los empleados, con el fin de hacer más favorable el flujo de trabajo, permitiendo con esto, se vuelvan más hábiles en los procesos creativos y de desarrollo. Así también, las intranets se utilizan para el procesamiento en colaboración, ya que pueden mantenerse en un sitio Web los problemas, preguntas y respuestas, depuración de software, o bien, las conversaciones entrelazadas (mensajes de correo electrónico continuos) que junto con lo anterior, son de interés para los individuos que participan en un grupo, y logran con ello optimizar la efectividad de la organización.

Entonces, la tecnología Intranet depende de la información y la inteligencia interna de la empresa, por consiguiente, no toda la información de la compañía se encuentra abierta al público, sino por el contrario, se restringe el acceso de la misma, puesto que su conocimiento interno es la mayor ventaja competitiva que posee la empresa.

Tabla 2. Diferencias que existen entre una Intranet e Internet.

INTRANET	INTERNET
Información de propietario	Información pública
La seguridad es una misión crítica	La seguridad es una misión crítica y competitiva
Concentrada en comunicación entre empleados	Concentrada en la comunicación con el cliente
Transacciones en colaboración	Transacciones financieras
Diseñada para el flujo de trabajo	Diseñada para el flujo de la interacción con el cliente
Orientada a procesos	Orientada a ventas y mercadotecnia
Conexión opcional con Internet	Conexión básica con Internet
Transforma las organizaciones	Transforma el ciclo cliente/ventas
Énfasis en grupos de trabajo, equipos y flujo intradepartamental	Énfasis en un punto único de contacto con la organización y el perfil del usuario
Utilizada para el desarrollo	Utilizada para implantación
Crea una organización de aprendizaje	Crea una nueva conciencia y un estado de ciudadano de internet
Necesita estar altamente descentralizada	Necesita estar altamente centralizada

2.1.3 COMPONENTES DE UNA INTRANET

Como se ha visto, una Intranet es una tecnología cliente/servidor basada especificamente en los estándares de Internet, en el que se incluyen elementos de hardware, software, protocolos y estándares.

Para comprender mejor este punto, el siguiente diagrama ejemplifica una Intranet junto con sus diversos componentes:

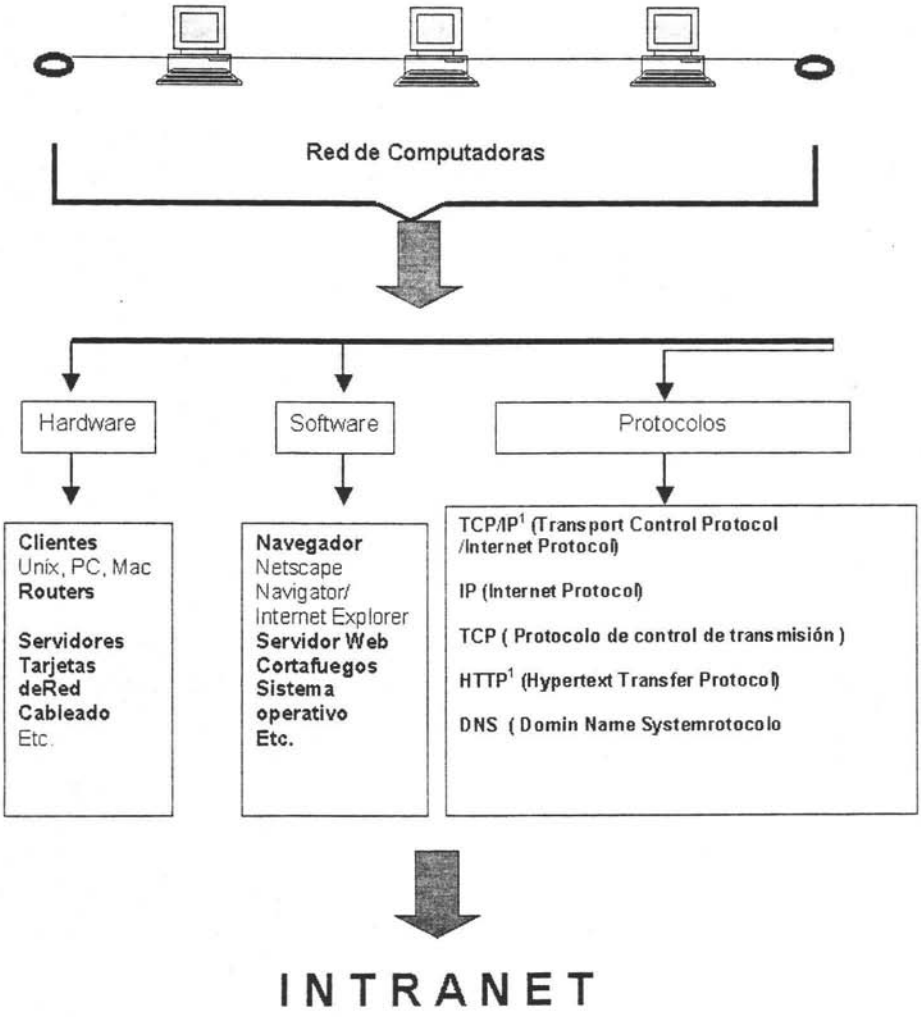


Fig. 2.1 Diagrama de una Intranet

2.1.3.1 Hardware

Cuando hablamos de hardware, nos referimos a los distintos componentes clientes y servidor de los niveles de una Intranet, por lo que las partes más importantes de hardware en esta tecnología lo constituyen los clientes, routers (encaminadores) y servidores, así como las tarjetas interfaz de red, cableado, etc.

En realidad, no se cuenta con un hardware específico para una Intranet, sino que muchos de los componentes de hardware que existen actualmente en el mercado son de uso general, desarrollados para redes locales (LAN) y de larga distancia (WAN), pero que han sido preparados y empaquetados para la implantación de una Intranet, y por lo mismo, gran parte de este hardware también se utiliza para conectarse a Internet.

2.1.3.2 Software

Existen diversos componentes de software en la arquitectura Intranet, pero tres de ellos son los más esenciales, por lo que solo se tratarán estos elementos más significativos.

El primero de ellos es el NAVEGADOR, el cual consiste en un programa utilizado generalmente para ver el contenido de los servidores de la Intranet (o de Internet), y por definición, son "Navegadores Web" es decir, pueden visualizar documentos de hipertexto.

Este software se ejecuta en un "ordenador cliente" , pudiendo ser una PC, una Macintosh, una estación de trabajo UNIX, u otro dispositivo de sobremesa. Los navegadores más populares son el Navigator de Netscape, y el Internet Explorer de Microsoft.

Otro componente importante, es el servidor HTTP, o también conocido como Servidor Web, cuya función es la de reunir todos los servidores de la World Wide Web.

Por último, está el software "CORTAFUEGOS" o firewall, encargado de la seguridad, el cual funciona en un servidor conectado a un router que a su vez se encuentra conectado a una red externa. La finalidad de este software es la de proteger la Intranet del tráfico, evitando que entren en ella transmisiones de red.

2.1.3.3 Protocolos

Son acuerdos tomados entre varias compañías para el desarrollo de los productos de software y hardware, permitiendo con esto, puedan trabajar conjuntamente sin necesidad de algún tipo de software intermedio especial o cualquier otro producto de traducción, facilitando así la intercomunicación entre ellos.

TCP/IP[4] *(Transport Control Protocol/Internet Protocol).-* Es un conjunto de protocolos, se le dio este nombre por que este es uno de los más importantes. Es un protocolo independiente del hardware y del software, es decir, no esta ligado a un sistema operativo y a ningún tipo de red. Es el protocolo de comunicación básico de Internet e Intranets, y permite la comunicación punto a punto entre los distintos nodos de una red. Cuando se implanta una infraestructura TCP/IP, se pueden utilizar los servicios Intranet como: web, mensajería, foros, listas de distribución, etc.

Protocolo IP (Internet Protocol).- El cual contiene las especificaciones o reglas que permiten que los paquetes de datos de un nodo atraviesen diversas redes hasta llegar a un nodo destino. IP solo está encargado de especificar el tamaño del paquete de datos a enviar, la composición de las direcciones Internet y otras reglas básicas.

Protocolo TCP (Protocolo de control de transmisión).- Es otro de los protocolos de mayor importancia, está orientado a conexiones para asegurar la fiabilidad de los datos transmitidos por IP, además se encarga de que los datos lleguen con mayor rapidez y precisión al extremo receptor, para ello divide los datos a enviar en trozos más pequeños y les asigna una identificación para incluirlos en un paquete IP.

HTTP[5] *(Hypertext Transfer Protocol).-* , Empleado para enlazar datos hipertextos a través de una Intranet o de Internet, es decir, es un protocolo Web que controla las peticiones y servicios de documentos HTML. Con HTTP se puede hipervincular todos los archivos, medios, paquetes, software, imágenes y fotos digitales, de modo que queden disponibles para cualquier persona de la compañía que la busque. El software de servidor HTTP se ubica en un nodo dedicado, conocido como "Servidor Web", y su función es ver que hiperenlaces se están transmitiendo a través de la Intranet, asegurando que el enlace sea adecuado con la información apropiada.

Protocolo DNS (Domin Name System).- "Sistema de Nombres de Dominio" es un sistema empleado para la traducción de nombres en inglés con el fin de convertirlos en direcciones IP y con ello facilitar su identificación, esto debido a que el protocolo IP sólo especifica una dirección constituida por cuatro números inferiores a 256, por ejemplo: 129.147.6.5 o 182.121.63.7.

De esta manera, el estándar DNS permite a diferentes grupos administrar nombres correspondientes a dichos números de IP de una forma más eficaz.

Protocolo UDP .- es otro protocolo de menor fiabilidad que TCP pero más simple, se utiliza principalmente para las aplicaciones de servicios IP, como el DNS (Domain Name Service), o el RIP (Routing Information Protocol). También se adapta para las aplicaciones llamadas de "tiempo real" (telefonía, videoconferencias), donde se requiere de velocidad, puesto que el protocolo UDP es bastante ligero y rápido, mientras que las funciones de seguridad de TCP no podrían aprovecharse.

[4] TCP/IP – Protocolo de Control de Transmisión/ Protocolo Internet

[5] HTTP - Protocolo de transferencia de Hipertexto

Cabe señalar, que los protocolos son cruciales para la Intranet, ya que la falta de ellos puede llegar a aumentar considerablemente los costos de la misma, así como producir problemas de compatibilidad con los socios de negocios.

2.2 FUNCIONES Y FINALIDAD DE LA INTRANET

Ya hemos hablado de lo "qué es una Intranet", ahora bien, es necesario conocer ¿Qué es lo que hace esta tecnología?.

En primer lugar, la contribución más impresionante de una Intranet a la organización, se ve reflejada en los beneficios relacionados con la comunicación y la colaboración. Esta tecnología es una herramienta que permite la **"unificación"**, tanto de la gente, como los procesos del negocio, el conocimiento corporativo, los proveedores, los socios y los clientes, siendo muy importante la seguridad, es decir, protegerse de los intrusos a través de un firewall (software cortafuegos).

También, una Intranet proporciona una tecnología para la colaboración y una infraestructura de comunicación (gente, procesos, procedimientos), con la finalidad de que la organización sea una sola entidad o grupo, donde se comparten conocimientos, estrategias, metas, procesos, relaciones, interacciones, proyectos, calendarios y objetivos de la misma, esto a través de una página Web de uso compartido en toda la empresa.

Otro aspecto importante, es que para ello utiliza una interfaz "única y universal", lo que hace que la Intranet se convierta en la voz e inteligencia de la organización. Lo cual significa, que su propósito es el de organizar el escritorio de cada individuo empleando el menor costo, tiempo, y esfuerzo posibles para obtener una mayor productividad y eficiencia en cuanto a costos, así como el ser más oportuno y competitivo, ya que gracias a esta tecnología es posible que la gente llegue a satisfacer sus propias necesidades de información, facilitando la localización de personas con intereses o habilidades similares a las que ellos necesitan. Así mismo, la tecnología Intranet permite explorar nuevas formas de hacer su trabajo y llega a ofrecer nuevas oportunidades de negocios.

2.3 ELEMENTOS Y SERVICIOS QUE CONSTITUYEN UNA INTRANET.

Existen muchas discrepancias en cuanto a los servicios y elementos que constituyen una Intranet, aquí presentamos los que creemos son los más importantes: Groupware, acceso remoto, transferencia de archivos y páginas Web.

Empezaremos definiendo el término Groupware.- Se denomina al conjunto formado por las distintas herramientas que ayudan a las personas a trabajar juntas de forma fácil y eficaz de manera que puedan comunicarse entre ellas, colaborar y coordinarse.

El problema que se ha visto con el groupware es que ha sido muy caro y difícil de implantar, pero con las intranet baratas y fáciles de construir, este ya no es el caso. Ahora se pueden obtener las ventajas del groupware en una Intranet, debemos mencionar que una red Intranet no necesariamente debe tener un groupware, sin embargo, es una herramienta muy poderosa que nos facilitará nuestras tareas.

El groupware se clasifica en función de la forma en que se va a utilizar:

- Herramientas de trabajo conjunto: Comprenden Los programas de calendario y planificación, las teleconferencias, las videoconferencias, los sistemas de reunión electrónica (EMS), las pizarras y los programas de conversación (chat).
- Herramientas de trabajo individual: Comprenden El correo electrónico, los grupos de noticias, las bases de datos, las herramientas de escritura en grupo y los programas de flujo de trabajo.

Profundizaremos un poco más en las herramientas que creemos son las más representativas del trabajo en Intranet: Correo electrónico, Programas de conversación (Chat) y grupos de noticias.

2.3.1 Correo Electrónico

El correo electrónico ha sido probablemente la primera herramienta de colaboración que la mayoría de las organizaciones han implantado. El correo electrónico ha sustituido a los memorandos y faxes en muchas organizaciones.

Aquí cada usuario puede contactar con cualquier otro usuario en algún lugar del mundo e intercambiar con él información, mensajes, imágenes y archivos. Permite comunicar información en vez de convocar una reunión, si lo que se desea es enviar el mismo mensaje a un grupo de personas, el tener que repetir el mismo mensaje varias veces o tener que escribir todas las direcciones de las personas que van a recibir el mismo mensaje resultaría una tarea larga y tediosa, éstas son pues, las principales causas de que esta herramienta sea llamada la más importante dentro de Intranet.

Hay muchos productos que soportan correo electrónico para Intranet, entre los que se encuentran : Lotus Notes y Domino, Netscape Navigator, Microsoft Exchange e Internet explorer, Novell GroupWise, entre otros.

2.3.2 Programas de Conversación (Chat)

Con la herramienta Internet Relay Chat (IRC) se puede conversar a través de Internet. La función Chat se aproxima a las comunicaciones en tiempo real y puede sustituir a las llamadas telefónicas de larga distancia que tan caras resultan, y a las teleconferencias entre varios lugares. Usando esta herramienta pueden celebrarse sesiones de discusión en las que los participantes están juntos al mismo tiempo, pero no están en el mismo lugar.

Es muy útil si por ejemplo surge un problema en producción, entonces, se recurre a esta herramienta y se realiza una tormenta de ideas en la que todos participarán y discutirán el problema.

Internet Relay Chat ha sido la herramienta de conversación predominante en las Intranet. Existen otras herramientas para conversación Chat como:

- **NetMeeting**.- Es una aplicación muy potente que permite entre otras opciones, establecer conferencias de audio y vídeo entre varias personas. La principal función de Micorosoft NetMeeting es realizar trabajo en grupo a través de una conferencia. Ésta podría definirse como una sesión establecida entre dos o más personas en las que pueden comunicarse (ya sea utilizando el teclado o por audio/vídeo), enviarse datos entre sí (documentos o cualquier tipo de archivo) y compartir aplicaciones. NetMeeting es una herramienta muy importante dentro del trabajo en grupo en una Intranet. Especialmente en los casos en los que la Intranet está distribuida dentro de todo un edificio, puede ser una herramienta importante para planear el trabajo en común

- **Microsoft Comic Chat**.- Es un programa de charla con texto, pero que emplea una muy original aproximación gráfica, ya que la charla se realiza como si se estuviese participando en un comic, usted y los demás participantes serán personajes de una tira animada. Podrán crear sus propios personajes y fondos.

- **Netscape Cooltalk**.- Es una herramienta de telefonía para Internet la cual provee de una gran calidad de audio para mantener conferencias, ofrece además una Pizarra electrónica, ésta permite que todos los miembros de la misma conferencia utilicen de manera conjunta una aplicación de dibujo básica (parecida al Paint de Windows), y herramientas para comunicación basados en texto.

2.3.3 Servicios o grupos de noticias

Con el servicio de noticias cada usuario puede suscribirse a los temas que le interesen, así como tener acceso diariamente a toda la información generada sobre ellos.

Un servidor newsgroup permite compartir información y crear debates sobre un tema concreto.

Hay dos tipos de grupos de noticias: con moderador, donde los artículos que envían los usuarios no se añaden automáticamente al grupo de noticias, sino que son previamente revisados por un moderador que determina si el artículo tiene interés para publicarse o no. El otro tipo es sin moderador, en el que todas las noticias se añaden directamente.

Existen muchos servidores NEWSGROUP que están replicados en todos los nodos de Internet. De esta forma, sólo es necesario conectarse al servidor NEWSGROUP más cercano, para poder participar en cualquier debate.

Se necesita un programa específico, además de la conexión al servidor NEWSGROUP más cercano, estos son algunos de los más conocidos:

RN.- Es el más antiguo de todos ellos, fue diseñado en 1983 y permite presentar los artículos de forma rápida y con una participación mínima del usuario.
TRN.-Es una revisión del programa RN realizada en 1990 con la incorporación de un seguimiento de los artículos que son contestación de otros.
NN.- Fue diseñado en 1984 y permite revisar de forma rápida un gran número de artículos.
TIN.- Fue diseñado en 1991 y permite manejar un gran número de grupos de noticias facilitando la labor de aquellas personas que están interesadas en seguir una gran variedad de temas.

Para acceder a este servicio se pueden utilizar: Lotus Notes, Netscape Navigator, Digital Alta Vista Forum, Microsoft Exchange e Internet Explorer.

Los grupos de noticias hacen las mismas cosas que los servicios de correo, uno hace preguntas o entra en discusiones, existen miles de grupos de noticias llamados USENET algunos son:

- Comp.groupware.- Discusión de software y hardware de groupware en general.
- Comp.groupware.groupwise. Discusión del producto Groupwise de Novell.
- Comp.groupware.lotus-notes.programmer.- Discusión sobre temas de programación para Lotus Notes.

2.3.4 Acceso Remoto (telnet)

La principal virtud de TCP/IP (*Transmisión Control Protocol/Internet Protocol),* estriba en que está diseñado para enlazar computadoras de diferentes tipos, incluyendo PCs, minis y mainframes, que ejecuten sistemas operativos distintos sobre redes de área local y redes de área extensa, por tanto, permite la conexión de equipos distantes geográficamente.

El protocolo TCP/IP es la base de Internet y por consiguiente de Intranet, su papel es controlar la transmisión de datos de un lugar a otro. Éste tiene un gran número de protocolos de los cuales solo explicaremos los más representativos de la forma en que trabaja una Intranet: *telnet (acceso remoto) y ftp (transferencia de archivos).*

A través del acceso remoto se puede conectar a otra computadora o a otra red situada en cualquier parte del mundo de la misma forma que si se tratara de una estación de trabajo de ella.

Para ello se utiliza el protocolo **telnet** de **TCP/IP**, éste permite que un usuario, desde un terminal, acceda a los recursos y aplicaciones de otras computadoras. Una vez que la conexión queda establecida, actúa de intermediario entre ambas computadoras.

2.3.5 Transferencia de Archivos (ftp)

Mediante la transferencia de archivos se pueden enviar archivos a otra computadora conectada, o bien recuperar sus propios archivos.

Para esto se utiliza el comando **ftp** de **TCP/IP**, (File Transfer Protocol), que es el más utilizado de todos los protocolos de aplicación y uno de los más antiguos.

Se utiliza para la transferencia de archivos proporcionando acceso interactivo, especificaciones de formato y control de autentificación (aunque es posible conectarse como el usuario anonymous que no necesita contraseña). Funciona muy bien con archivos grandes que no sería conveniente mandar por correo electrónico como por ejemplo dibujos técnicos y especificaciones. La herramienta ftp se puede usar en una Intranet para hacer lo siguiente:

- Proporcionar a los usuarios más avanzados la posibilidad de traer a su disco duro, software y actualizaciones.
- Cargar páginas web y otra información en el servidor.

2.3.6 Gopher

Gopher es un sistema que permite utilizar la mayoría de los recursos mediante menús, sin tener que preocuparse del uso de direcciones IP, nombres de dominio o qué programas hay que utilizar en cada caso.

Para acceder a un servidor *gopher* se requiere de un programa cliente, el cual mostrará un sistema de menús que irá dirigiendo las peticiones.
Cuando sea necesario, se conectará con el servidor *gopher* para recuperar la información que solicite y/o contactará con otras computadoras a través de ftp o telnet de forma totalmente transparente para el usuario.

Si lo que interesa es un archivo de texto, *gopher* accederá al archivo y lo mostrará, aunque para ello tenga que realizar un acceso remoto a otra computadora y poner en funcionamiento un editor de textos.

Si un usuario de *gopher* está interesado en un determinado tema, lo primero que deberá hacer es moverse entre todos los submenús que encuentre hasta llegar a la opción que le satisfaga. Esta forma puede ser dificultosa y tediosa ya que no hay ninguna norma común que indique como se deben organizar los menús y, por tanto, cada servidor *gopher* los tiene organizados de forma distinta. Para solucionar este problema existe una aplicación llamada VERÓNICA que se encargará de buscar de forma automática la opción *gopher* que interese.

2.3.7 La Web

La Web es otro de los elementos importantes en Intranet, básicamente las páginas Web están formadas por texto e imágenes, pero pueden añadirse sonidos y video para aumentar su atractivo.

La Web permite acceder de manera sencilla a la información mediante hipertexto, que es la función que enlaza la información. La característica más importante del hipertexto es que la computadora sabe donde encontrar la información. La Web consta de páginas iniciales o "Home page", que son simplemente los puntos de comienzo para localizar información. Los enlaces hipertexto de las páginas iniciales permiten acceder a todo tipo de información, que puede ser texto, imágenes, sonido y/o video.

El programa cliente que se utiliza recibe el nombre de navegador o explorador (BROWSER), mediante él, el usuario puede realizar una transferencia de archivos, iniciar una sesión remota o acceder a documentos que se encuentran en otro servidor WWW (World Wide Web).

Para la creación de páginas Web se pueden utilizar los lenguajes de programación HTML, JAVA, JAVASCRIPT, aunque también existen programas que permiten generar las páginas Web con cierta facilidad y sin tener grandes conocimientos de programación como es Microsoft FrontPage.

2.4 BENEFICIOS Y LIMITACIONES DE LAS INTRANETS.

La tecnología Intranet cuenta con una gran diversidad de aplicaciones, que más adelante serán tratadas, con lo que podemos darnos cuenta de los muchos beneficios que se derivan de dicha tecnología, principalmente en las áreas de comunicaciones y gestión de sistemas. No obstante, de la misma manera, se pueden apreciar ciertas limitaciones o desventajas para el desarrollo de una Intranet, pero que posiblemente tengan soluciones inmediatas.

2.4.1 Beneficios Tangibles e Intangibles

Debido a que el uso de una Intranet trae una gran cantidad de ventajas, es necesario separarlas en dos grupos, siendo el de los "Beneficios Tangibles", refiriéndose a aquellos que se pueden medir o cuantificar, mientras que el otro grupo será el de los "Beneficios Intangibles", los que no pueden medirse pero se sabe que tienen un impacto positivo. Estos últimos, son los que llegan a tener una mayor importancia para el aspecto económico, siendo los causantes del crecimiento de los negocios.

A continuación presentamos una tabla en la que se observan los beneficios más importantes tanto tangibles como intangibles de la tecnología Intranet, así como algunas de sus limitaciones:

Tabla 3. BENEFICIOS Y LIMITACIONES DE LAS INTRANETS

Beneficios			***Limitaciones***
Beneficios Tangibles		***Beneficios Intangibles***	
Son rápidas y fáciles de implantar	Baratas en su implantación.	Proporcionan mejor comunicación	Posibilidad que se produzca el caos.
Fáciles de usar.	Ahorran tiempo y costos	Proporcionan acceso a información exacta y precisa.	Riesgos de Seguridad
Permiten una mayor eficiencia operativa	Basadas en estándares abiertos[6].	Recogen y comparten conocimientos y experiencia	Desconfianza de la Dirección
Conectan y comunican plataformas diferentes	Permiten a los usuarios controlar sus datos	Proporcionan mejor coordinación y colaboración	Sobrecarga de la Información
Escalables.	Flexibles	Permiten una mayor creatividad e innovación	Complejidad y costo oculto o desconocido
Permiten utilizar toda la riqueza de la Multimedia para formación y comunicación.	Aseguran la inversión en infraestructura y aplicaciones	Permiten nuevas asociaciones de negocios	Una cobertura funcional parcial.
Son seguras		Permiten oportunidades de negocio.	

2.4.2 Limitaciones de las Intranets.

Para nuestro caso, también es importante hablar de la contraparte de las Intranets, ya que es en este punto donde nos damos cuenta que la Tecnología Intranet se ha ido volviendo "no insuficiente", pero si con ciertas limitaciones, debido a que no llegan a cubrir todas las necesidades del sistema de información.

[6] Para mayor información sobre el tema de Estándares abiertos, consultar el Libro INTRANETS Usos y Aplicaciones, de Randy J. Hinrichs. Pág.52

Hoy en día existe otra gran tecnología denominada "EXTRANET", ¿y por qué no hacer uso de ella?, entonces para contar con una tecnología de uso interno más favorable, ¿por qué no abrirla al exterior?, claro bajo un estricto control de seguridad y ciertas restricciones, permitiendo con ello que los flujos de información se aceleren, los individuos de una organización estén mejor informados, produzcan mejor y más de prisa, dándonos cuenta que **"la apertura es una ventaja primordial"**. Este tema se tratará con mayor detalle en los capítulos posteriores de nuestra investigación.

Otras limitaciones de la tecnología Intranet por mencionar de acuerdo a ciertos aspectos, además de las vistas en la tabla 3 son:

- ***Según el enfoque organizacional*:** Requiere administración de contenido y control de acceso a áreas de la organización que exigen seguridad.
- ***Los objetivos de la compañía*:** Requiere centralizarse a un alto nivel y afinar las visiones departamentales.
- ***La propiedad:*** Requiere la conversión de viejos sistemas y dispersa la responsabilidad.
- ***Los sistemas de medición***: El uso de estadísticas no está muy fortalecido.
- ***El flujo de trabajo*:** Puede crear bolsas o islas de excelencia.
- ***El uso*:** Tiene que usarse para que valga la pena.
- ***La comunicación*:** El inglés es el idioma predominante.
- ***La colaboración*:** Las Intranets no proporcionan respuestas, donde la versión más reciente está actualizada, proporcionando control de la versión.
- ***El desarrollo*:** HTML no tiene las opciones suficientes para desarrollar aplicaciones Web.

2.5 SEGURIDAD EN LA INTRANET

La seguridad es un punto clave en la utilización de una red Intranet, por ejemplo, no es posible poner en la Intranet información confidencial de la empresa como : la nómina, información personal de los empleados, prototipos de ingeniería ó secretos de la empresa, sin embargo, para que las redes Intranet resulten completamente funcionales, es necesario que esta información se encuentre en línea, pero debemos asegurarnos que únicamente los miembros autorizados tengan acceso a ella, además, las redes Intranet a menudo están conectadas a Internet para permitir a los empleados de la empresa comunicarse con el exterior.

Al conectar nuestra Intranet a Internet corremos el riesgo de que ciertos individuos intenten penetrar en nuestra Intranet para:

- Deshacer nuestra información.
- Saturarnos las máquinas, por ejemplo enviando mensajes electrónicos.
- Utilizar los recursos de nuestras máquinas.
- Robar informaciones confidenciales.
- Modificar informaciones confidenciales.

Deshacer nuestra información, no es el peor de los casos, al contrario, porque al menos se toma conciencia del daño. El robo de información confidencial sin que nos demos cuenta puede ser mucho más grave.

Es necesario proteger nuestra Intranet de estas intrusiones malintencionadas. Ésta es la función del "cortafuegos" o "firewall"

2.5.1 Cortafuegos o Firewalls

Un cortafuegos o firewall es un grupo de computadoras, software, routers y servicios, que todos juntos permiten conectar una red a otras redes, al mismo tiempo que se mantiene su seguridad e integridad.

El trabajo de un cortafuegos es definir y defender el perímetro de una red. Se encuentra situado normalmente entre una red Interna en la que se puede confiar, y una red externa, en la que no se confía. Los cortafuegos son como los porteros de una Intranet y todas las subredes internas. Un cortafuegos determina quién tiene la autorización para entrar o para salir de una red o subred protegida. Un cortafuegos puede proteger la intranet privada de Internet, pero también puede proteger distintas subredes de la Intranet.

El cortafuegos restringe los tipos de tráfico que se permiten en la Intranet. Determina que tipo de acceso (correo electrónico, telnet, ftp, etc.) es permisible para cada usuario. Administra el origen o el destino de los datos y siempre registra la hora de cada transacción.

Este método nos proporciona una protección óptima frente a los intentos externos de romper los sistemas de seguridad, aunque siempre cabe la posibilidad de acceder a la red desde "dentro".

Estos son algunos beneficios que proporcionan los sistemas firewall:

- Configuran una pared de seguridad entre el exterior y los servicios que usted utiliza para salir (correo electrónico, ftp y conexión remota)
- Autorizan acceso únicamente a usuarios o aplicaciones específicos
- Ocultan los nombres reales del usuario.
- Proporcionan encriptación y posibilidades de red privada.
- La encriptación mezcla los datos y requiere de códigos de acceso para desencriptarlos.
- Los sistemas firewall también pueden utilizarse dentro de la red de una empresa para proteger áreas clasificadas dentro de la Intranet.

La figura 2.2 muestra una arquitectura común de seguridad.

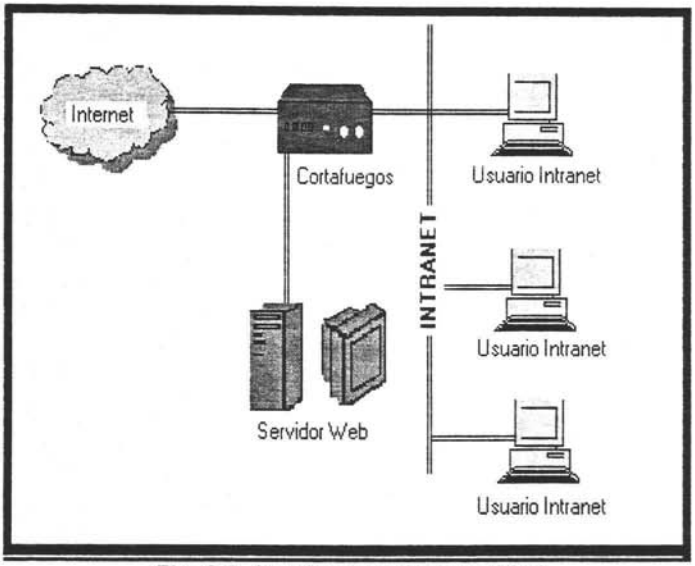


Fig. 2.2 Arquitectura de seguridad

La arquitectura de seguridad cumple varias funciones, la primera es la protección del servidor, los cortafuegos permiten filtrar las comunicaciones a varios niveles. Por ejemplo, a nivel físico y a nivel de TCP/IP. Existen 2 tipos de cortafuegos:

Cortafuegos que filtran paquetes.- Toda la información que se envía por la Intranet o por Internet se envía en pequeños trozos llamados paquetes. Cada paquete contiene una cabecera donde se incluye información como la dirección del Protocolo de Internet (IP), la dirección de IP del servidor http y el puerto del servidor al que se desea acceder. El servidor de http devuelve la página Web solicitada en forma de varios paquetes de información que se ensamblan de un formato que el visualizador Web puede interpretar. Un cortafuegos filtra paquetes, regula el transporte de estos datos entre los nodos de la red leyendo y reaccionando a la información que se encuentra en cada uno de los paquetes que lo atraviesa.

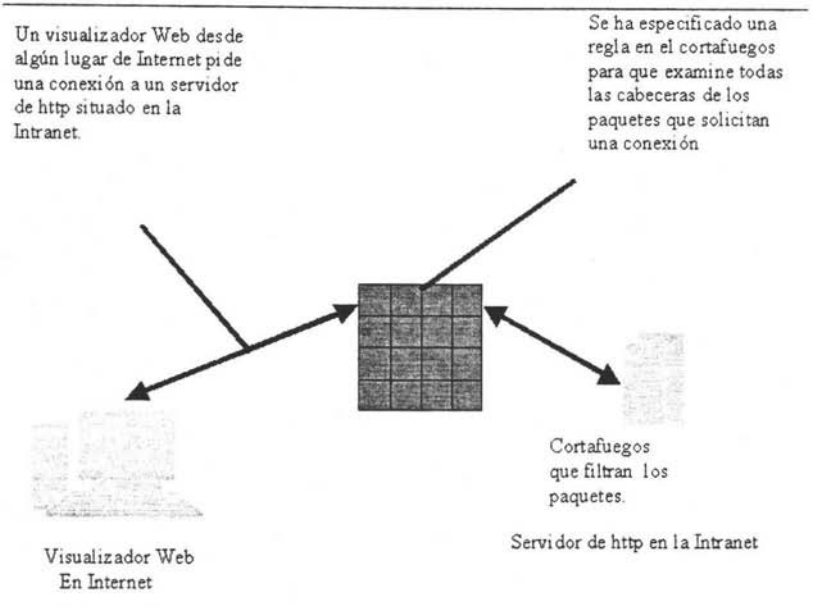


Fig. 2.3 Cortafuegos como Filtro de Mensajes

Servidores de aplicaciones proxy.- Los firewalls basados en arquitectura de proxy operan al nivel de aplicación en el modelo OSI. Los proxies de aplicación evalúan entre si los datos del contexto, éstos pueden tomar decisiones de acceso con base en diversos factores.

Los proxies de aplicación realizan las siguientes funciones:
1.- Examinan el contenido del paquete.
2.- Permiten o rechazan conexiones basadas en dirección IP, hora y tipo de servicio.
3.- Vigilan la dirección del servicio, por ejemplo, FTP. http.
4.- Registran todos los datos de la sesión.
5.- Proporcionan ocultación automática de la dirección.

Los proxies de aplicación, aunque efectivas, aún son vulnerables a ciertos ataques de nivel red o IP. Cuando se implantan VPNs, los firewalls basados en esta arquitectura también deben incluir algún tipo de mecanismo de filtrado de paquete como protección contra ataques que pueden surgir de los túneles de VPN con direcciones IP expuestas.

Se puede usar un servidor proxy por sí mismo o en conjunto con otro software o hardware cortafuegos. Por ejemplo, una compañía puede querer configurar un cortafuegos para filtrar los paquetes en el perímetro de seguridad y usarlo junto con un servidor proxy. El servidor proxy proporcionará una puerta controlada a través del cortafuegos y hacia fuera de la red externa desprotegida. Los servidores proxy trasladan los paquetes hacia y desde las computadoras fuente y destino al igual que los cortafuegos. La diferencia entre ambos es la siguiente:

- Un cortafuegos funciona con cada uno de los paquetes. Sólo controla el tráfico de paquetes y reacciona de acuerdo con las reglas que se le dan. Un cortafuegos no tiene en cuenta el contenido de los paquetes.

- Un servidor proxy se conecta tanto a la fuente como al destino. Recibe las peticiones de conexión de la computadora fuente. Al mismo tiempo, el servidor proxy establece una conexión con la computadora destino y de igual forma termina esa conexión. De esta forma se consigue una seguridad superior ya que las computadora fuente y destino no están nunca realmente conectadas.

El sistema firewall o cortafuegos nos proporciona una protección óptima frente a los intentos externos de romper los sistemas de seguridad, aunque siempre cabe la posibilidad de acceder a la red desde "dentro", pues se ha comprobado que los mayores ataques a una red son provocados internamente, por eso, la mejor seguridad que podemos implantar en nuestra Intranet es mantener una buena información en nuestros empleados y mantener una política de uso y seguridad que defina lo que constituye la utilización para el negocio y lo que no, es decir, lo que está estrictamente prohibido.

Son posibles dos políticas de seguridad: la primera consiste en autorizar los accesos a todos los servicios salvo a aquellos explícitamente prohibidos. La segunda se implanta cuando se prohíben todos los accesos, salvo aquellos explícitamente autorizados. Esta última es más segura, pero también más restrictiva y más difícil de gestionar.

2.5.2 Seguridad Física

Debemos tomar en cuenta, que existe la posibilidad de tener una amenaza física a nuestras instalaciones y a nuestra red Intranet.

Entre los ejemplos de amenazas físicas y a la infraestructura están las sobretensiones y los desastres naturales como las inundaciones y los rayos. El ataque físico o la destrucción de hardware, también entran dentro de esta categoría. Los respaldos del sistema son una forma sencilla de prevenir la pérdida de los datos de una Intranet debidas a estas imprevisibles amenazas.

No olvidemos este tipo de amenazas cuando se realice el sistema de seguridad.

2.5.3 Seguridad de sistema operativo

Hemos visto que el uso creciente de las redes de computadoras y la importancia del trafico cursado hace necesario proteger a los datos. Es aquí donde interviene la criptografía, la cual es especialmente útil en los sistemas multiusuario y en las redes de computadoras. Ésta se debe utilizar para proteger a las contraseñas, almacenándolas cifradas. Se puede utilizar también para proteger todos los datos almacenados en un sistema de computación; además se debe considerar el tiempo de cifrado / descifrado. También es aplicable en los protocolos de redes de capas que ofrecen varios niveles de cifrado.

Asimismo debido a la gran importancia que reside en la seguridad, las grandes compañías de software: UNIX y Microsoft Windows NT han agregado un nivel de seguridad incrustado en su software, proporcionando control de accesos, es decir, permiso de escritura y lectura de archivos y directorios, así como auditoría y controles de autentificación. Este nivel de seguridad se basa en uno de los 7 niveles de seguridad que el departamento de Defensa de los Estados Unidos define para su sistema operativo.

A continuación daremos a conocer los principales fallos genéricos funcionales de los sistemas, siendo los que se muestran en la tabla 4:

Tabla 4 Fallos Genéricos Funcionales

Fallos Genéricos	Descripción
Autentificación	Los usuarios no pueden determinar si el hardware y el software con que funcionan son los que deben ser. Un intruso podría reemplazar un programa sin conocimiento del usuario. Un usuario puede inadvertidamente teclear una contraseña en un programa de entrada falso.
Cifrado	No se almacena cifrada la lista maestra de contraseñas
Implantación	Implantación improcedente de un buen diseño de seguridad.
Confianza implícita	Una rutina supone que otra está funcionando correctamente cuando, de hecho, debería examinar los parámetros suministrados por la otra rutina.
Compartimiento implícito	El S. O. deposita inadvertidamente información importante del sistema en un espacio de direcciones del usuario.
Comunicación entre procesos	Usos inadecuados de los mecanismos de send / receive que pueden ser aprovechados por los intrusos.
Verificación de la legalidad	Validación insuficiente de los parámetros del usuario.
Desconexión de línea	Ante una desconexión de línea el S. O. debería: Dar de baja al usuario (o los usuarios) de la línea. Colocarlos en un estado tal que requieran la re - autorización para obtener nuevamente el control.
Descuido del operador	Un intruso podría engañar a un operador y hacer que le habilite determinados recursos.
Paso de parámetros por referencia en función de su valor.	Es más seguro pasar los parámetros directamente en registros que tener los registros apuntando a las áreas que contienen los parámetros. El paso por referencia puede permitir que los parámetros, estando aún en el área del usuario, puedan ser modificados antes de ser usados por el sistema

Cont. Tabla 4 Fallos Genéricos Funcionales

Fallos Genéricos	Descripción
Contraseñas	No deben ser fácilmente deducibles u obtenibles mediante ensayos repetidos.
Entrampamiento al intruso	Los S. O. Deben tener mecanismos de entrampamiento para atraer al intruso inexperto.
Privilegio	Cuando hay demasiados programas con demasiados privilegios se viola el principio del menor privilegio.
Confinamiento del programa	Un programa "prestado" de otro usuario puede actuar como un "Caballo de Troya".
Prohibiciones	Se advierte a los usuarios que no utilicen ciertas opciones porque los resultados podrían ser "indeterminados", pero no se bloquea su uso, con lo que puede robar o alterar datos.
Residuos.	Un intruso podría encontrar una lista de contraseñas con solo buscar en lugares tales como una "papelera": Del sistema o física. La información delicada debe ser sobrescrita o destruida antes de liberar o descartar el medio que ocupa
Blindaje	Los intrusos pueden conectarse a una línea de transmisión sin hacer contacto físico: Utilizan el campo inducido por la circulación de corriente en un cable. Se previene con un adecuado blindaje eléctrico.
Valores de umbral	Si no se dispone de valores umbral, no habrá: Límites al número de intentos fallidos de ingreso. Bloqueos a nuevos intentos. Comunicaciones al supervisor o administrador del sistema.

De la misma forma, es importante conocer ***los "Ataques Genéricos a los Sistemas Operativos***", encontrando entre los principales:

- Asincronismo: Se tienen procesos múltiples que progresan asincrónicamente. Un proceso podría modificar los parámetros ya validados por otro proceso pero aún no utilizados. Un proceso podría pasar valores malos a otro aún cuando el segundo realice una verificación extensa.
- Rastreo: Un usuario revisa el sistema intentando localizar información privilegiada.
- Entre líneas: Se utiliza una línea de comunicaciones mantenida por un usuario habilitado que está inactivo.
- Código clandestino: Se modifica el S. O. bajo una presunta depuración pero se incorpora código que permite ingresos no autorizados.
- Prohibición de acceso: Un usuario escribe un programa que bloquea el acceso o servicio a los usuarios legítimos mediante: Caídas del sistema, ciclos infinitos, monopolio de recursos, etc.
- Procesos sincronizados interactivos: Se utilizan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.
- Desconexión de línea: El intruso intenta acceder al trabajo de un usuario desconectado; luego de una desconexión de línea; y antes de que el sistema reconozca la desconexión.
- Disfraz: El intruso asume la identidad de un usuario legítimo luego de haber obtenido la identificación apropiada por medios clandestinos.
- Ataque "nak": Si el S. O. permite a un usuario: Interrumpir un proceso en ejecución mediante una "tecla" de "reconocimiento negativo"; realizar otra operación o reanudar el proceso interrumpido. Un intruso podría "encontrar" al sistema en un estado no protegido y hacerse con el control.
- Engaño al operador: Con un engaño se hace realizar al operador una acción que comprometa la seguridad del sistema.
- Parásito: Mediante equipamiento especial el intruso:Intercepta los mensajes entre un usuario habilitado y el procesador. Los modifica o reemplaza totalmente.
- Caballo de Troya: El intruso coloca un código dentro del sistema que luego le permita accesos no autorizados. Puede permanecer en el sistema, o borrar todo rastro de sí mismo luego de la penetración.
- Parámetros inesperados: El intruso suministra valores inesperados a una llamada al núcleo. Intenta aprovechar una debilidad de los mecanismos de verificación de la legalidad del S. O.

Con lo anterior, nos damos cuenta de la problemática que existe en cuestión de seguridad, lo cual resulta ser un tema muy extenso a tratar, sin embargo, no es la finalidad de este proyecto, pero si bien, en el siguiente apartado solo mencionaremos algunas de las técnicas de seguridad junto con las posibles soluciones que nos ofrecen[7].

[7] Para mayor información, consultar la siguiente dirección de Internet
http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SO14.htm

2.5.4 Técnicas de Seguridad

Además de los firewalls hay muchas técnicas de seguridad diferentes. A continuación analizaremos las diferentes técnicas de seguridad, los riesgos y las soluciones que nos ofrecen:

Tabla 5 Técnicas de Seguridad, Riesgo y Solución

Técnicas de seguridad	Riesgo	Solución
Contraseñas de acceso	Inundación de puertas de acceso. Los usuarios prestan la contraseña a otros.	Caducidad de contraseña Combinaciones mínimas y máximas de datos alfanuméricos. Diferentes contraseñas para diferentes partes de la Intranet.
Encriptación	Ataques de desencriptación por parte de supercomputadoras. Mensajes de correo electrónico no seguro	Contraseñas de 56 bits de longitud. Uso de encriptación PGP para encriptación de correo electrónico.
Autentificación	Los usuarios pueden no ser quienes dicen que son.	Diferentes contraseñas para diferentes partes de la Intranet.
Integridad	Los mensajes pueden ser alterados.	Firma Digital.
Privacía física	Riesgo mínimo	Asegura el secreto de la ubicación.
Autorización	Los impostores pueden entrar y recibir autorización ilegalmente	Utilice firmas digitales internamente.

2.6 ¿QUÉ EMPRESAS NECESITAN UNA INTRANET?

Para dar respuesta a esta cuestión, simplemente podemos decir que la tecnología Intranet puede ser empleada en cualquier empresa, especialmente para aquellas organizaciones que, por su gran tamaño o diversidad geográfica, necesiten un sistema tecnológico potente, que permita a sus empleados tener acceso y uso compartido y simultáneo de información y recursos. Aún así, esto también es posible cuando se trate de una sola persona que necesite compartir datos, documentos e información.

La nueva cuestión que nos lleva a responder es, ¿Por qué utilizar una Intranet como herramienta de comunicación en una empresa?. Contestar esta pregunta resulta sencilla si nos concentramos en los beneficios que trae consigo el uso de esta tecnología.

Como ya hemos mencionado anteriormente, sus beneficios o ventajas, en este momento nos enfocaremos solo en algunas de las principales. Primeramente, una de ellas es la disminución en la inversión de equipos de redes, así como en los costos de administración de redes de información interna en la empresa. Además, aumenta el acceso a la información interna de la organización, logrando ser accesada desde cualquier parte del mundo a través de un browser conectado a Internet.

Otro beneficio del uso de una Intranet, es que los costos asociados a la administración de ésta, son extremadamente inferiores a cualquier otro sistema de información. Por último, esta tecnología puede ser instalada en los servidores de la empresa, o bien, ser instalada en servidores externos mediante un ASP (Aplication Service Provide).

Estos son solo algunos de los beneficios que trae consigo esta tecnología, pero creemos son suficientes para poder decidir el por qué elegir una Intranet como herramienta de comunicación.

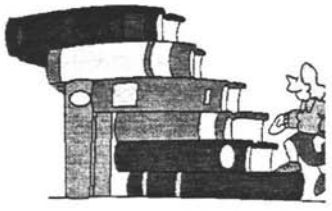
2.7 APLICACIONES DE LAS REDES INTRANET

Las aplicaciones de las redes Intranet son prácticamente ilimitadas, es decir, la mayor parte de las aplicaciones van dirigidas a proporcionar un tipo de funcionalidad: **compartir información**, éstas pueden presentar aspectos muy diferentes, pero la finalidad es la misma, publicar información o ampliar la comunicación.

Algunos de sus usos requieren únicamente páginas creadas con HTML, un lenguaje de creación de páginas sencillo, mientras que otros implican una programación muy sofisticada y enlaces con bases de datos. Una Intranet puede ser tan sencilla o tan sofisticada como uno desee.

Estas son algunas de las aplicaciones:

- Correo Electrónico
- Directorios
- Cuadros de organización
- Folletos informativos y publicaciones
- Noticias
- Manuales de personal
- Información sobre beneficios sociales
- Formación
- Ofertas de trabajo



Formación

- Memorandos
- Grupos de noticias
- Informes de ventas
- Informes financieros
- Información del cliente
- Folletos de marketing, vídeos y presentaciones
- Información de productos
- Información y dibujos sobre desarrollo de productos
- Información sobre proveedores
- Catálogos de suministros y componentes
- Información de inventario
- Estadísticas de calidad
- Documentación de usuario del sistema
- Gestión de la red.
- Gestión de fondos

Cuadros de organización

Cualquier organización puede utilizar la Intranet según sean sus necesidades, desde consultores, hasta fabricantes; desde vendedores hasta clientes; es decir, toda persona relacionada con la organización.

Mencionaremos algunas empresas exitosas que tienen como herramienta de trabajo una red Intranet :

- *Silicon Graphics* Fabricante de productos para Internet.
  Su Intranet da servicio a 7,200 empleados con más de 144,000 páginas Web almacenadas en 800 servidores Web internos. Esta Intranet Llamada Silicon Junction, pone a disposición de los empleados más de 25 bases de datos corporativas y envía mensajes de vídeo y audio a intervalos regulares a todos sus empleados.

- *General Electric Co.* Utiliza su Intranet la GE Information Network (o GEIN) para dar a sus empleados acceso a más y mejor información, así como proporcionarles un mayor acceso a la información corporativa y financiera. Por ejemplo: La GEIN contiene el informe anual de la compañía, además dela información financiera y comercial, que permite a los empleados que tienen acciones, preparen mejor sus inversiones.

- *Booz-Allen Hamilton* utiliza su Intranet como un repositorio electrónico para la base de conocimientos de la compañía. Los analistas de la firma utilizan la Intranet Knowledge On Line para buscar en las bases de datos temas como guías para realizar operaciones bancarias o reorganización de software en el negocio de los transportes. Los usuarios pueden también conseguir una lista de todos los proyectos en los que haya trabajado cualquier analista de Booz, todas las personas con las que ha trabajado un analista y la especialidad del analista dentro de la empresa.

- *Dreamworks SKG*, Compañía de Animación.
  Está desarrollando un sistema de producción de alta tecnología basado en una Intranet, para coordinar las muchas facetas de la primera película producida por la empresa. El sistema se utiliza para comprobar el estado diario de los proyectos, llevar el seguimiento de los objetos animados y para coordinar escenas. La Intranet se utiliza en toda la compañía para ayudar en la producción de películas de acción, música, programas de televisión y nuevos medios desarrollados en Dreamworks Interactive.

En este capítulo abarcamos los aspectos más importantes de la tecnología Intranet, permitiendo al lector tener el conocimiento necesario de la misma, ya que se trataron desde los conceptos básicos de la Intranet hasta sus aplicaciones, así como algunos aspectos de seguridad.

CAPÍTULO III

EXTRANETS

CAPÍTULO III La Extranet

Veremos un concepto de la Extranet y lo vincularemos con la VPN, profundizando en la teoría con la que se basa esta tecnología, así como algunos aspectos de la tecnología de Firewalls.

3.1 FUNDAMENTOS DE EXTRANET.

La razón más importante en la utilización de una Intranet extendida o mejor conocida como Extranet, es la **comunicación activa** entre los diferentes miembros de una empresa, es decir, los clientes por un lado y sus proveedores por el otro, a su vez ambos se encuentran enlazados con otros clientes y proveedores obteniéndose una red de comunicación activa. Esto hace ver un nuevo concepto de transacciones empresariales, lo que implica integrar a los clientes y proveedores en la cadena de producción, estableciendo más asociaciones con ellos, y permitiendo un mayor intercambio de información. Además demandan información oportuna en tiempo real y fiable, tomada de la fuente de donde surge.

Por otro lado, el valor añadido de la Extranet consiste en que a través de ella se alcanza un mayor grado de **conocimiento**, es decir, reúne información relevante de suministradores, clientes y otras fuentes de interés, la cual llega a los socios estratégicos, jefes de proyecto y demás departamentos con especial interés en este tipo de información, de tal manera que se pueda utilizar para la comercialización de productos en función de los cambios del mercado y de las necesidades del cliente, de forma más efectiva y económica que otras herramientas y tecnologías, acortando así los ciclos de desarrollo de productos y servicios.

Asimismo, posee la capacidad de prestar servicios profesionales y personales de tipo interactivo a todos sus miembros y la posibilidad de soportar documentos individualizados, pudiendo ser actualizados a través de consultas a bases de datos, incluir hipertexto e imágenes y otras herramientas, con el fin de aumentar el grado de **colaboración** existente entre los miembros de la red. Como fruto de esta colaboración se conseguirá mejorar el producto y servicio finales, lo que será sinónimo de mayor índice de cooperación, eficiencia y productividad. Otra característica relevante es que amplia el radio de acción más allá de la intranet, apoyando mayores beneficios inmediatos, como mejores relaciones de la empresa con los grupos, instituciones y asociaciones que participan en un escenario comercial común. Permite reducir costes de infraestructura por lo que el retorno de la inversión es rápido y mayor.

Hay mucho que se puede obtener al compartir información tanto interna como externamente. Una Extranet elimina esta diferencia y permite concentrarse en compartir información cuando y donde quiera que una buena comunicación sea lo importante, y la buena comunicación es importante casi en cualquier lugar.

3.1.1 ¿Qué es una Extranet ?

Existen dos configuraciones básicas de Extranets, la primera consiste en arrendar una línea directa, donde una empresa pueda tener un completo control físico sobre la línea que enlaza una Intranet con otra Intranet, mientras que la segunda, que es la más utilizada y la que analizaremos en este proyecto, consiste en establecer una Extranet mediante un vínculo seguro en Internet, donde la empresa utiliza Internet como un número privado universal. Si se usa la infraestructura existente de Intranet e Internet, una Extranet se convierte tan sólo en una cubierta lógica, definida solamente por los privilegios de acceso y las tablas de ruteo, en lugar de una red física completamente nueva. De tal manera, construir una Extranet resulta económico y relativamente sencillo.

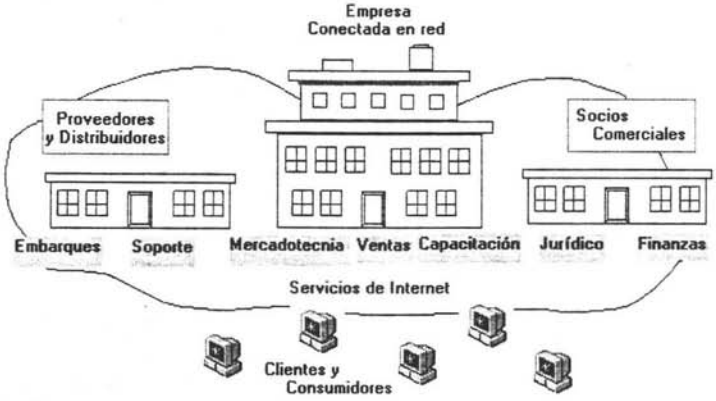


Fig. 3.1 Representación de una Extranet

La **Extranet** o **"Intranet extendida"**, es una estructura de **comunicación** y **colaboración,** resultante de ampliar la red Intranet a usuarios que están fuera de la empresa. Emplea la tecnología desarrollada para Internet, esto es, usa los protocolos de Internet y el sistema público de telecomunicaciones para compartir parte de la información de un negocio o las operaciones con proveedores, vendedores, socios, clientes u otro tipo de negocios, estableciendo diferentes niveles de acceso mediante el uso de passwords, números de identificación de usuarios o diferentes niveles de acceso a la información, como pueden ser bases de datos de la compañía, los catálogos on-line vía Internet de productos o servicios y fomentar así el comercio electrónico.

Hemos tratado de dar un concepto amplio de lo que es una Extranet, sin embargo, sería un error y complicaría las cosas el insistir en una definición rígida que cubra con precisión todos los aspectos.

3.2 SEGURIDAD EN LA EXTRANET.

La seguridad es un tema importante en el desarrollo de la tecnología Extranet, ya que de ésta depende la productividad de una empresa, puesto que a través de ella y en un ambiente seguro es posible realizar negocios que traen consigo aumento de utilidad y dependencia.

La falta de esta seguridad puede ocasionar consecuencias dañinas a la empresa, como son las grandes pérdidas financieras, debido a que siempre que se permita el acceso a la Extranet, se pondrán en riesgo los datos, la reputación y los recursos de la organización.

Entonces, se deben tomar en cuenta tres requisitos básicos que garanticen que la información de Extranet esté segura, siendo la *confidencialidad*, donde los datos sean vistos sólo por quienes estén autorizados para verlos, la *integridad* garantizando que la información sea exacta y, la *disponibilidad* la cual consiste en que la información se encuentre disponible siempre cuando se le requiera de forma inmediata e ininterrumpida.

Ahora bien, la verdad es que la amenaza más grande contra la seguridad de la Extranet no proviene de fuera de la empresa, sino de los propios empleados, clientes y socios industriales con acceso a ésta. Por ello, a continuación señalaremos los principales problemas o amenazas a los que pudiera enfrentarse esta tecnología.

3.2.1 Posibles Amenazas a la Extranet

Estos son sólo algunos tipos comunes de amenazas de seguridad a las Extranets, siendo:

- *Ignorancia y Accidentes*
- *Sus propios empleados y socios estratégicos.*
- *"Abrepuertas" por tanteo.* Estas son personas que por lo general sólo buscan diversión, como el poder irrumpir en un sitio popular, averiguar sobre un sistema raro o simplemente no tienen nada mejor que hacer, y aunque no tengan malas intenciones, puede llegar a ocasionar daños considerables.
- *Ataques Programados.* Son ataques comunes a las Extranets, los cuales son aquellos que incluyen procesos automatizados, por ejemplo, los *"ataques de negación de servicio"*, como los bombardeos, SPAMS y suplantaciones de correo electrónico, quienes llegan a saturar un sistema con grandes cantidades de mensajes, procesos o solicitudes a la red, ocasionando estragos al sistema y degradando así el rendimiento de la red. Así mismo, existen otros tipos de ataques que consisten en códigos diseñados para husmear los sistemas, con el fin de manipular los datos, haciendo que se multipliquen, modifiquen o destruyan.

Además, dentro de estos ataques programados, encontramos a las bombas lógicas, los gusanos de Troya, las puertas traseras, escotillas, bacterias (conocidas también como conejos) y los Virus, estos últimos representan una amenaza latente, ya que pueden llegar a atacar a una Extranet que no cuente con la protección apropiada, provocando daños importantes y pérdidas de datos, debido a que en el ambiente de Extranet, los virus pueden llegar a propagarse con gran rapidez. Por fortuna también se cuenta con una amplia gama de programas antivirus, aunque día con día surgen nuevas amenazas, por lo que se debe estar en una constante actualización.

Con todo esto nos damos cuenta de la gran importancia de contar con un sistema ampliamente seguro, que permita realizar todas las actividades requeridas en una empresa de manera confiable.

3.2.2 Mecanismos de Protección

Ya hemos visto algunas de las posibles amenazas que pueden llegar a perjudicar una Extranet en cuanto a seguridad, ahora como contraparte, también resulta importante tratar el tema de "Protección", a pesar de que, asegurar una Extranet signifique que pueda ser similar a proteger cualquier otro tipo de red. Sin embargo, dentro de este apartado veremos algunos mecanismos de protección empleadas en esta tecnología.

3.2.2.1 Seguridad mediante Oscuridad.

Este mecanismo de Protección es el de menor sentido pero no obstante es el más usado, éste consiste básicamente en la discreción, "Si no le cuento a nadie sobre mi sistema, lo que contiene o sus mecanismos de seguridad, nadie sabrá al respecto y el sistema estará seguro". Para ello, la empresa debe contar con un conjunto sólido de políticas y procedimientos de seguridad, que permitan el logro de un sistema protegido eficientemente. Además de requerir una capacitación adecuada de los usuarios, siendo ésta la mejor forma de combatir las amenazas de seguridad en cuanto a errores, ignorancia o accidentes.

3.2.2.2 Seguridad del Host.

La seguridad del host es un modelo que básicamente está enfocado en restringir el acceso a las máquinas una por una, lo que implica conocer todas las características de cada máquina host y ajustar las medidas de seguridad.

Este sistema por su naturaleza, trae ciertos problemas, su costo es alto, es difícil administrar, requiere una labor intensa en cuanto a configuración y mantenimiento y no se escala fácilmente. A pesar de ello, este modelo funciona y debe considerarse en cada estrategia de seguridad, ya que en ciertas circunstancias se requiere de una seguridad máxima del host para los sistemas de la extranet expuestos al exterior a través de la tecnología Internet.

Seguridad de la Red. Este modelo de seguridad está dirigido al control a nivel de la red, el cual consiste en métodos que incluyen medidas pasivas, como son los filtros, servidores proxy, registros y monitoreo de paquetes; así como medidas activas, por ejemplo, la autentificación por contraseñas y la encriptación, todo esto con el fin de proteger los archivos confidenciales.

También existe otro modelo muy común y eficaz en cuanto a la seguridad de la red, que consiste en la construcción de un firewall (cortafuegos) alrededor de la red interna.

Nota: Cada uno de estos métodos de seguridad solo se mencionan en este apartado, debido a que fueron tratados con anterioridad en la tecnología Intranet.

3.2.3 Los Firewalls y la Extranet

En esta parte no profundizaremos en el concepto de firewall o cortafuegos, ya que fueron vistos anteriormente, aquí sólo veremos algunos aspectos que nos parecen importantes en la relación firewall-Extranet.

La primera regla para trabajar con firewalls es no depender de ellos. El mayor problema con los cortafuegos es darlos por garantía, un firewall no es la única protección que necesita. Los firewalls requieren cuidado constante, son un tipo de filtro que permite pasar sólo los mensajes que cumplen las condiciones especificadas.

Como están sujetas a cambios constantes, debe cambiar las especificaciones de manera periódica. Un cortafuego no es algo que se pueda instalar y olvidar.
Hasta hace poco todavía existía una clasificación de firewalls: filtrado de paquetes y servidores proxy. Ahora la mayoría de los productos en el afán de mejorar son híbridos, ya que rebasan las clasificaciones convencionales y cambian constantemente.

La verdadera prueba de un cortafuego es la forma en que bloquea los intentos de acceso indeseables. Para resguardar de manera efectiva los recursos más importantes de las personas externas:

- *Control de acceso flexible.*- Se afinan las reglas con las que admite o rechaza a los posibles visitantes.
- *Facilidad de uso.*- La administración es una responsabilidad continua.
- *Respuesta al error.*- Un firewall no solo debe rechazar a los visitantes no autorizados. Debe informar de los intentos y hacer todo lo posible por identificar el origen.

La seguridad adicional de los cortafuegos internos tiene un precio, al separar las partes más pequeñas de la organización, este sistema dificulta la colaboración y compartir la información. Algunos fabricantes de firewalls están promoviendo los productos internos tratando de resolver el problema como una forma de tecnología que dinamiza en vez de obstaculizar.

Por ejemplo, puede establecer cortafuegos en dos sitios y crear un enlace directo entre ellos, encriptando los datos que pasan por ahí, a esta técnica se le llama entubar (tunneling), proporciona lo que un fabricante ofrece como el equivalente de una red privada virtual, que puede compartir información en un ambiente seguro. Puede utilizarla para brindar comunicación segura entre las sucursales y los socios comerciales externos.

Cuando dos organizaciones deciden trabajar juntas, deben ser capaces de compartir sus sistemas, información y otros recursos en tanto dure el proyecto. Sin embargo, no necesita compartir los recursos todo el tiempo, pues no significa que usted y sus socios decidieron combinar las organizaciones o abrir todas las operaciones de cada uno al otro. Un intruso en el sistema del socio puede encontrar un camino para entrar también a su sistema, lo cuál puede ser un problema aun entre los mejores socios. En tal situación, un cortafuegos interno puede limitar el peligro.

Debemos conocer la distribución de la red. Las contraseñas predeterminadas son sólo un portal, hay muchas otras. Los invasores pueden encontrar el camino al sistema a través de cualquier cosa que conecte una computadora a otra, esto incluye puentes, enrutadores y compuertas. Debe saber exactamente que tantos anfitriones TCP/IP soporta la red. Cada uno es un punto potencial de entrada, y si deja incluso uno sin proteger, es igual a abrirlos todos. Después de que identificó los puntos de peligro, puede hacer algo al respecto.

El desempeño del sistema es un tema de seguridad. Los firewalls inevitablemente reducen las velocidades de transmisión si la Extranet produce un aumento en el tráfico, este puede reducirse a una marcha lenta durante las horas pico. Un bajo desempeño ocasionará patrones deficientes tanto internos como externos y buscar solución a dicho problema puede ocasionar que se reduzca la seguridad y se aumente el desempeño. Los firewalls tienden a parecer más seguros de lo que son en realidad. Una razón es que necesitan tecnología de seguridad complementaria, como el control de acceso, también necesitan un proceso de respaldo como forma de supervisión y mantenimiento continuo.

3.2.3.1 Problemas de Seguridad en las Extranets y sus Posibles Soluciones

Las Extranets plantean un conjunto de retos de seguridad que son diferentes a los correspondientes a las intranets. Las Extranets tienen una capa adicional de complejidad, dado que ellos no sólo están mediando entre el mundo interno de una organización y el mundo externo de Internet, sino que también están mediando entre las culturas de diversas entidades de negocios. Ello significa múltiples capas de acceso y también diversos problemas. A continuación se delinean unos cuantos de los problemas inherentes a las Extranets:

► Con la Extranet, la seguridad es responsabilidad conjunta de las empresas que están en los puntos terminales de los túneles que enlazan a un grupo de intranets o de usuarios que acceden a la red. Como tal, es crucial que los ruteadores en los extremos sean muy seguros.

► Una Extranet comprende una población de usuarios locales y remotos que están distribuidos por todo el mundo y en diversas empresas. Es virtualmente imposible manejar o incluso prever los tipos de sistemas heterogéneos que se utilizarán para acceder a la Extranet. El rol de medidas de seguridad que se apeguen a estándares se vuelve primordial.

► Los administradores y usuarios de Extranets deben afrontar las querellas y sensibilidad política de sus socios comerciales electrónicos. Ello se complica por la diversidad de culturas corporativas y a veces extranjeras. La diplomacia electrónica se vuelve norma con las Extranets.

► Las capas adicionales de acceso para entidades de negocios múltiples se traducen en costos añadidos por sistemas de protección internos contra los visitantes no gratos.

► La vinculación electrónica de empresas en cibersociedades aumenta el riesgo de entrecruzar información de nivel competitivo, creando un hueco a nuestro sistema de seguridad.

► La seguridad de la Extranet debe ser extrema y más "evidente". El administrador de la Extranet debe "vender" constantemente a los usuarios ansiosos la idea de que es un sitio seguro.

► Los niveles múltiples de acceso a Extranets, basado en las diferentes posiciones de los socios, significa que deben crearse mecanismos con un nivel más fino, para controlar el acceso a la información de la Extranet .

Algunas posibles soluciones.

La clave para la seguridad de la Extranet es el acceso controlado estrictamente, aunado al impulso de la adopción de estándares entre los socios de la Extranet. Se observan varias herramientas de seguridad, nuevas creadas exclusivamente para Extranets, entre ellas una nueva casta de "ruteadores de Extranets", en que se combinan en un solo dispositivo la encriptación, autentificación, el túnel y la seguridad de firewall basados en estándares.

Existen también otras soluciones que algunas entidades han probado y podrían ser beneficiosas:

✓ Cada socio que accede a la Extranet tiene una dirección IP distinta. Debe ser capaz de programar su firewall de modo que sólo acepte paquetes de mensajes de estas direcciones específicas. También debe ser capaz de definirla todavía más, admitiendo solamente a ciertos individuos y verificando los tipos de aplicaciones que sus socios utilizan.

- ✓ Una empresa creó un firewall "complejo" basado en varias capas de seguridad, incluyendo filtros de paquetes y un algoritmo de encriptación desarrollado por Sun Microsystems, Inc. Llamado skip (administración sencilla de claves IP). Su firewall también se modificó para que reconociera la dirección IP de cada visitante y determinará quién tiene acceso a qué archivos.
- ✓ Otra empresa decidió utilizar un plan de ingeniería de rastreo de aplicaciones, instalarlo dentro de su firewall y agregarle un servidor para apoyarlo. De esa manera, ha podido tener un sistema de rastreo y control de acceso personalizado.
- ✓ Para Extranets que permitirán a sus socios tener acceso a información muy delicada. Incluye un dispositivo del tamaño de una tarjeta de crédito para los usuarios con una pantalla digital pequeña de seis dígitos que cambian cada dos minutos. Cuando los usuarios inician una sesión en el sistema, deben utilizar la contraseña que aparezca en la tarjeta en ese momento.

3.2.3.2 Tipos de firewalls en el mercado

Los firewalls que a continuación presentamos son diferentes en la manera en que se implantan y operan mientras manejan el tráfico de red. Uno de los que se presenta opera dentro de la infraestructura de la red, y no en su perímetro como normalmente lo hacen los firewalls. Debido a esta diferencia operacional, el firewall debe funcionar como un puente y no como un enrutador, lo que es la característica operacional normal de los firewalls.

3.2.3.2.1 El "ladrillo" de Lucent

Lucent lanzó un producto llamado el aparato Managed Firewall, o "el Ladrillo". El Ladrillo opera bajo el sistema operativo propietario de la empresa, pero no posee sistemas de archivos, registros de administrador ni teclado o dispositivo apuntador (ratón). El ladrillo se introduce en una nueva clase de firewall conocida como aparatos de seguridad. Es el primer producto de firewall que se diseña desde el principio para ser un componente de la infraestructura de red, y no sólo un mecanismo en el perímetro de una red. Lucent lanzó el Ladrillo para proporcionar a las empresas los medios para insertar con facilidad un firewall en cualquier parte de la infraestructura de la Intranet, Extranet o VPN. El ladrillo de Lucent opera como un puente, más que como un enrutador, que es la manera en que suele operar un firewall.

Los ladrillos pueden instalarse como componente de infraestructura de red, pueden administrarse también desde un punto de administración central. El sistema de administración puede configurarse y controlarse a través de una estación de trabajo de NT para definir controles de acceso en términos de zonas de seguridad. La gran ventaja de las zonas de seguridad es que cada una de ellas puede tener una política de seguridad y una administración separadas. Por estas razones, el Ladrillo es ideal para organizaciones con muchas conexiones de socios comerciales y suborganizaciones con diversos requisitos de seguridad.

3.2.3.2.2 Firewall de Demon ultrarápido de Optical Data Systems

Un desafío continuo para los sistemas de Firewall ha sido y siempre será el desempeño, sobre todo en sistemas de filtrado de paquetes. En general, las puertas de enlace de seguridad deben instalarse en servidores de alto desempeño porque en redes con mucho tráfico, la inspección de cada paquete puede entorpecer con facilidad un sistema, o lo que es peor, crear un cuello de botella.

Optical data System (ODS) está llevando a los firewalls a una nueva cima de alto desempeño al construirlas sobre conmutadores de alta velocidad. Debido a que la tendencia es establecer redes cada vez más rápidas.

La empresa también incluye una tarjeta complementaria que maneja procesos de decisión descargados por el conmutador. Por lo general, la tarjeta contiene un procesador Intel bajo un sistema operativo dedicado. Sin embargo, también podría funcionar con otros procesadores de "seguridad".

3.2.3.2.3 La solución extravagante de firewall de WatchGuard

La implantación actual de WatchGuard Technologies es un aparato de seguridad llamado Firebox II. El aparato de firewall de primera generación de WatchGuard se llamo Firebox Firewall. Firebox I fue uno de los primeros aparatos en su tipo, lanzado en 1996, también fue uno de los primeros en ofrecer una combinación de firewall/VPN. Firebox adquirió con rapidez la reputación de que tenía un sistema de firewall simple pero de buen funcionamiento.

Firebox II, introducido en mayo de 1998, está diseñado básicamente para instalación de firewall a gran escala en WANs de empresas. Fue el primer firewall de cualquier tipo en expedir una clave privada dentro de los confines del hardware del aparato. Con este movimiento WatchGuard reconocía el crecimiento y la importancia crítica de las autoridades de certificación. Desde luego la clave pública resultante se utiliza para autenticación y encriptación de las sesiones para configuración remota e inicialización de la política de seguridad de la empresa. El sistema criptográfico resultante también se utiliza para proporcionar autentificación y privacidad en actividades de administración subsecuentes y actualizaciones del sistema.

3.2.3.2.4 Administración externa de firewall/VPN

Después de que los firewalls están en operación durante un periodo, es fácil olvidarse de ellos, sobre todo si están haciendo el trabajo. La gente de seguridad de red se encarga de otras funciones o se asigna a diferentes proyectos. Por lo que en un tiempo la seguridad se vuelve una "papa caliente" que nadie quiere agarrar. Por lo tanto, las organizaciones están cediendo la administración de sus sistemas de Seguridad/Firewalls a PSI´s o empresas de servicios de seguridad.

Estas empresas de servicios son para corporaciones que están convencidas de la importancia de la seguridad y la necesitan las 24 horas del día, los 7 días de la semana, pero no desean hacer la inversión en la infraestructura. Algunos PSI´s ofrecen servicios de administración a un precio razonable; sin embargo, si agrega capacidades de VPN a su red, la responsabilidad adicional de soporte de su VPN empezará a volverse costosa.

Los firewalls han evolucionado hasta convertirse en dispositivos de procesamiento central que aceptan complementos, aplicaciones de terceros y tecnología de seguridad extendida. Estos componentes funcionan en conjunto para proporcionar un sistema robusto de seguridad de red para su organización.

3.3 Redes Privadas Virtuales o VPN´s

3.3.1 ¿Qué es una Red Privada Virtual?

El término Virtual Private Network (VPN) o Red Privada Virtual comenzó a forjar su camino a principios de 1997, pero hay ciertas confusiones como la fecha exacta en que apareció esta tecnología. Para explicar lo que es una VPN es necesario explicar un par de conceptos: cifrado y virtual.

Cifrado.- no es nada más que tomar un mensaje, por ejemplo "Llegaré tarde" y convertirlo en argot, algo como "2deR56Gtr2345´´hj5Uie04". El otro extremo de este proceso se llama descifrado y es el reverso del cifrado. El núcleo de la seguridad de las redes privadas virtuales es que nadie, a excepción del receptor, es capaz de completar la parte de descifrado del proceso.

Virtual.- se refiere a una situación "como si". Suponga que trabaja en su PC de escritorio y llama a una computadora central. La computadora espera cierto tipo de terminal, por ejemplo una VT-100. ¿Cómo puede comunicarse con la computadora central cuando usted utiliza una computadora de escritorio y la computadora central espera una terminal VT-100? Su computadora emula a una VT-100. lo que significa que su computadora (a través del software) actúa "como si fuese una VT-100", por lo tanto la computadora central nunca se dará cuenta que en realidad su computadora no es una terminal vt100.

Ahora que se han descrito los conceptos virtual y cifrado, se puede comenzar a ver la definición de **Red Privada Virtual**:

" Proceso de comunicación cifrado o encapsulado que transfiere datos desde un punto hacia otro de manera segura". La seguridad de los datos se logra gracias a una tecnología robusta de cifrado y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada.

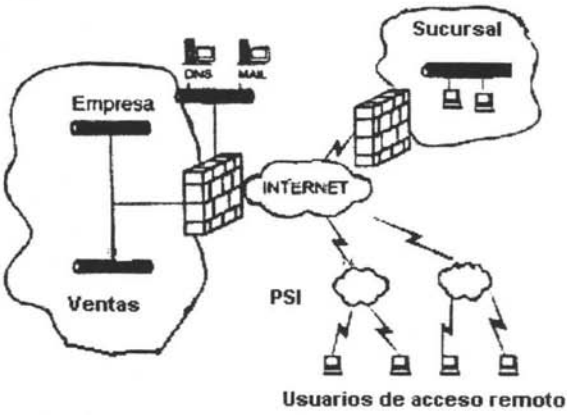


Fig. 3.2 VPN corporativa

La figura 3.2 muestra una red corporativa conectada a una red pública como transporte, Internet se utiliza como la compañía de transporte de la tecnología VPN, pero la nube Internet podría reemplazarse fácilmente por una nube ATM o de retransmisión de tramas.

Una gran característica de la tecnología VPN en su facilidad de ampliación. Conforme los proveedores de red incrementan el ancho de banda en sus redes de columna vertebral, las VPN pueden crecer y aprovechar este ancho de banda adicional. Además, puesto que las VPN son independientes de la plataforma y no dependen de ningún sistema operativo en particular, casi cualquier dispositivo en su compañía puede funcionar como cliente o como servidor de la VPN. Las VPN también dan cabida al crecimiento, muchos dispositivos de VPN manejarán cualquier servicio que se coloque en ellas. Le permitirán crear "túneles" o comunicaciones punto a punto con cifrado bajo demanda.

3.3.2 Clasificación o Áreas de Las VPN´s

Se utiliza el término área, puesto que así es cómo se describen las VPN en muchos artículos. Las áreas simplemente significan implantaciones comunes de VPN. Después de examinar las siguientes cuatro áreas, notará que los términos utilizados aquí son comunes a otros términos empleados para describir los servicios de Internet.

- **VPN de Intranet.-** Una VPN de Intranet se crea entre la oficina central corporativa y una oficina de ventas remota, o entre las oficinas centrales y las oficinas dependientes. La única diferencia es que se tiene acceso a la Intranet desde fuera de la red, lo que significa que el acceso viene desde el exterior. Normalmente sólo se utiliza dentro de la red de una compañía y únicamente acceden los empleados de la misma. A una VPN de Intranet sólo acceden los empleados, pero el acceso viene desde el exterior y no del interior.

- **VPN de Acceso Remoto**.- Una VPN de acceso remoto se crea entre las oficinas centrales y los usuarios móviles remotos. Con el software cargado en una laptop, un individuo establecerá un túnel cifrado al dispositivo de la VPN en las oficinas centrales corporativas.

- **VPN de Extranet.-** Una VPN de Extranet se crea entre la empresa y sus clientes o proveedores. Aquí es donde el comercio electrónico tiene su mayor impacto. Esta configuración le dará a la empresa la capacidad para realizar transacciones de manera segura y efectiva con sus principales socios comerciales y con clientes que generan ingresos.

- **VPN Interna.-** Una cuarta área de la cual no hacen uso las compañías actualmente, es una VPN Interna. Esto por cuestiones de seguridad con los propios empleados.

3.3.3 Arquitectura de VPN

En esta parte examinaremos algunas de las distintas arquitecturas de la tecnología VPN, incluyendo las VPN proporcionadas por los proveedores de servicios de red, las VPN basadas en cortafuegos, las VPN basadas en caja negra, las VPN basadas en acceso remoto/enrutador , las VPN conscientes de las aplicaciones, las VPN de servicios múltiples y las VPN basadas en software. Como puede ver existe una VPN para cada organización y cualquier tipo de infraestructura de red.

3.3.3.1 VPN basadas en cortafuego

Las VPN basadas en cortafuego probablemente son la forma más común de implantación de VPN hoy en día, y muchos proveedores ofrecen este tipo de configuración. Esto no significa que las VPN basadas en cortafuego sean superiores a otras formas de VPN, sino más bien se trata de una base establecida a partir de la cual se puede crecer. Actualmente sería difícil encontrar una organización conectada a Internet que no utilice algún tipo de cortafuego. Debido a que estas organizaciones ya están conectadas a Internet, todo lo que se necesitaría es añadir software de cifrado. Lo más probable, si su organización ha adquirido recientemente un cortafuego, es que incluya la capacidad para implantar tecnología de cifrado de VPN. Cuando decimos tecnología VPN, nos referimos a algún tipo de esquema de cifrado proporcionado con el dispositivo.

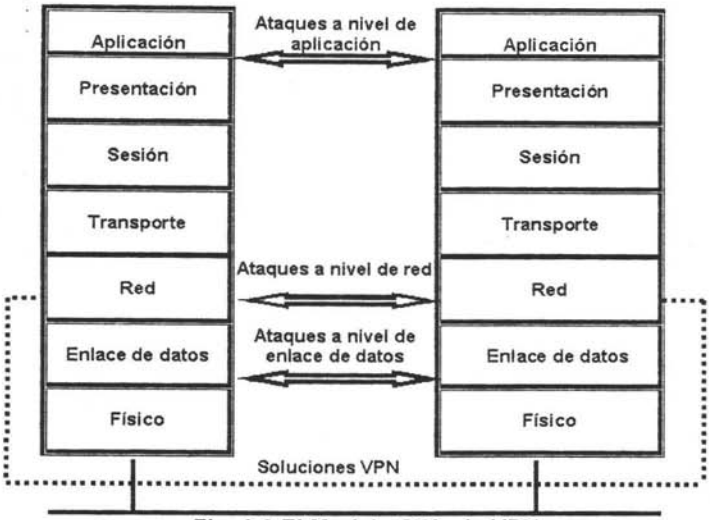


Fig. 3.3 El Modelo OSI y la VPN

Si observa la figura 3.3 podrá ver porque la tecnología VPN debería ubicarse en el nivel más bajo de la pila de OSI. Entre más arriba se encuentre en la pila, se presentarán mayores oportunidades que ocurran intrusiones en la seguridad de las capas inferiores de las que depende.

La implantación de una VPN basada en cortafuego aunque es muy común no es tan simple. La mayoría de las organizaciones tiene instalados estos sistemas, así que añadir el software de VPN no es muy difícil. Debe decidir que tipo de norma VPN desea. Por ejemplo ¿Desea utilizar la norma PPTP, L2TP o IPSec?. Recuerde que IPSec es un marco de referencia así que el cifrado DES podría utilizarse en un escenario IPSec.

Podría presentarse una confusión respecto a decir una solución de cortafuego/VPN. Cuando decimos que se debería añadir tecnología VPN a su cortafuego, se podría suponer que nos referimos a cualquier tecnología de cortafuego. Esto es incorrecto, hasta el momento existen tres tipos de implantaciones de cortafuego entre las cuales elegir: inspección de estados, proxy y filtrado de paquetes. Cuando se dice "añada tecnología VPN a un cortafuego", se refiere a añadir tecnología VPN únicamente a un cortafuego de inspección de estados. De la misma manera que la tecnología VPN en si misma se ejecuta en los niveles más bajos de la pila de OSI, el cortafuego debe hacerlo o puede caer en problemas de desempeño importantes. Un servidor proxy se ejecuta en el nivel 7, el nivel de aplicaciones del modelo OSI y el cortafuego de filtrado de paquetes también tiene que examinar el paquete completo cada vez que pasa. Un cortafuego de inspección de estados se ejecuta en los niveles 2 y 3. Debido a este requisito de procesamiento, usted sólo debería añadir tecnología VPN a un cortafuego de inspección de estados.

3.3.3.2 VPN basadas en caja negra

Se trata básicamente de un dispositivo cargado con software de cifrado para crear un túnel de VPN. Algunas cajas negras vienen con software que se ejecuta en un equipo cliente de escritorio para ayudar a administrar ese dispositivo, y otras pueden configurarse a través de un explorador web. Se cree que estos tipos de dispositivo de cifrado de hardware son más veloces que los tipos de software, ya que crean túneles más rápidos bajo demanda y ejecutan el proceso de cifrado con mayor rapidez. Aunque esto puede ser verdad, no todos ofrecen una característica de administración centralizada y por lo general no soportan el acceso a sí mismos. Es necesario enviar estos accesos a una base de datos para consultas. También se requiere otro servidor si se desea llevar a cabo la autenticación, aunque algunos dispositivos permiten añadir usuarios si así lo desea.

Con la mayoría de las instalaciones de caja negra es posible que se requiera un cortafuego independiente, aunque algunos proveedores están comenzando a incorporar VPN de caja negra con capacidades de cortafuego.

El dispositivo de VPN de caja negra se sitúa detrás del cortafuego. Aunque también puede situarse a un lado del mismo. El cortafuego proporciona seguridad a su organización, pero no provee seguridad para sus datos. Así mismo, su dispositivo VPN le brindará seguridad a sus datos pero no a su organización. Los proveedores están trabajando arduamente para hacer que estos dispositivos sean fáciles de usar.

3.3.3.3 VPN basadas en enrutador

Las VPN basadas en enrutador son adecuadas para una organización que ha hecho una gran inversión en enrutadores y cuyo personal de TI (Tecnologías de la Información) tiene experiencia en ellos. Existen 2 tipos de VPN basados en enrutadores. En uno de ellos el software se añade al enrutador para permitir que el proceso de cifrado ocurra. En el segundo, se inserta una tarjeta externa de otro proveedor en el mismo chasis que el enrutador. Tenga en mente que el desempeño puede ser un problema con las VPN basadas en enrutador. Debido a la adición de un proceso de cifrado al proceso de enrutamiento, usted puede agregar una carga más pesada al enrutador, especialmente si éste está manejando una gran cantidad de rutas o implantando un algoritmo de enrutamiento intensivo.

3.3.3.4 VPN basadas en acceso remoto

El acceso remoto, como su nombre lo indica, significa que alguien de fuera está tratando de crear un flujo de paquetes cifrados hacia su organización. Así que, de manera más literal, tal vez el término se aplique al software que se ejecuta en las máquinas de los usuarios remotos, en las cuales están tratando de crear un túnel hacia su organización y a un dispositivo en su red que permita esa conexión. Este túnel podría venir de Internet pero también podría venir de una línea de marcación, una línea ISDN o una red X.25

3.3.3.5 Aplicaciones de múltiples servicios con VPN

Ciertos proveedores empiezan a generar aplicaciones de múltiples propósitos que pueden residir en su dispositivo VPN basado en cortafuego, las cuales pueden considerarse como un valor agregado o como un problema potencial con el desempeño, dependiendo de que hace su VPN. Algunas de las aplicaciones de múltiples servicios para VPN son la filtración de contenido web y la revisión antivirus.

3.3.3.6 VPN basadas en software

Básicamente es un programa para establecer túneles o cifrado a otro anfitrión. Por lo general se utiliza desde un cliente a un servidor, por ejemplo, en una VPN de PPTP, el software cargado en el cliente se conecta al software cargado en el servidor y establece una sesión de VPN. Con los otros tipos de VPN, como el de Cortafuego/VPN a Cortafuego VPN, las únicas claves que se necesitan son de VPN a VPN. Esto significa que el tráfico en su red interna se descifra, así que sólo necesita las claves para los dispositivos VPN. Pero en caso de cliente a servidor, cada estación posiblemente podría tener su propio par de claves privada/pública.

3.3.3.7 Conmutadores de túnel para VPN

Este dispositivo tiene toda la funcionalidad tradicional de la arquitectura de VPN de hoy en día, con la característica agregada de estar en un único dispositivo físico. Esta arquitectura de VPN de múltiples propósitos está diseñada para combinar todas las características de los dispositivo de red tradicionales asociadas con la conexión a Internet. Los cortafuegos, el enrutamiento y la funcionalidad de VPN están combinados en un producto independiente para producir un escenario empresarial todo en uno, incluyendo el establecimiento de túneles de VPN de sitio a sitio, el acceso de usuarios remotos y el acceso a túneles en cualquier parte de su empresa. Están construidos para ampliarse a miles y posiblemente cientos de miles de usuarios, ya sea en un modo de encapsulamiento o en un modo de cifrado.

3.3.3.8 Ventajas y desventajas asociadas con la arquitectura de VPN

Tabla 1 Arquitectura de VPN, Ventajas y Desventajas

Arquitectura de VPN	Ventajas	Desventajas
Hardware	Buen desempeño; buena seguridad; carga de cifrado mínima para paquetes grandes, un poco de soporte para balanceo de cargas	Flexibilidad limitada, precio alto sin interfases ATM, FDI o Token ring, la mayoría son semiduplex; se necesitan reiniciar para que los cambios tengan efecto; algunos tienen problemas de desempeño importantes con paquetes pequeños de 64 bytes; funcionalidad de subred limitada; algunos carecen de NAT.
Software	Amplia variedad de plataformas, facilidad de instalación, buena para una amplia gama de compañías	Problemas de desempeño con el soporte NAT, algunos tienen tecnologías de cifrado viejas, propietario, algunos carecen de capacidad de administración remota; sin capacidad de supervisión
Enrutador	Uso del hardware existente, seguridad sólida disponible, bajo costo si se utilizan los enrutadores existentes	Algunos pueden necesitar tarjetas de cifrado adicionales, problemas de desempeño, pueden requerir una actualización aun enrutador más potente.
Cortafuego	Amplia variedad de plataformas, uso de hardware existente, soporte para balance de cargas y cortafuegos redundantes. IPSec de bajo costo	Posibles problemas de seguridad debidos al sistema operativo, no todos son completamente inter operables con soporte para RADIUS. Algunos tienen problemas de licencias.
Marcación	Fácil establecimiento de VPN, el costo es bajo	Problemas con compresión de datos, el soporte para RADIUS es mínimo.

La compatibilidad es muy importante desde el punto de vista de la seguridad. Si usted solo selecciona a IPSec, su solución no estará completa, la otra mitad es la administración de claves o el intercambio de claves de Internet (IKE). Con el propósito de contar con una solución de tecnología VPN completamente compatible, necesita ambos. IPSec cifrará y firmará los paquetes, pero IKE negociará el intercambio de claves entre los dispositivos terminales.

3.4 Topologías de VPN

Todas las opciones disponibles le dan la oportunidad de aprovechar completamente la tecnología VPN. Los dispositivos VPN pueden ser internos, lo que significa que puede dejar que pasen los paquetes cifrados a su red sin que sean modificados por un enrutador o un cortafuego.

Así como existen incontables maneras para adquirir e implantar una arquitectura de VPN, también existen muchas formas de colocar esta arquitectura en una topología de VPN. Debe saber que los dispositivos y las configuraciones tienen un lugar propio, y en donde necesite alguno, podrá encontrar el dispositivo más adecuado.

Al pensar dónde colocar su tecnología VPN, primero observe la topología de la red de su conexión a Internet. Después examine las oficinas remotas que tendrán su propia conexión a Internet y dónde quiere crear el túnel de VPN.

3.4.1 Topología de cortafuego/VPN a cliente

Empezaremos describiendo esta topología ya que es la de uso más común y prácticamente todas las organizaciones que implantan una VPN utilizarán este tipo de configuración. Casi todas las organizaciones conectadas a Internet tienen un cortafuego instalado, y todo lo que necesitan es agregar software de VPN al cortafuego.

Describiremos la forma en que trabaja una VPN típica: Un usuario en su equipo portátil remoto necesita el acceso a un servidor que se encuentra dentro de la red de la compañía, detrás de un cortafuego VPN. El usuario desea conectarse al servidor de la compañía y obtener un reporte confidencial.

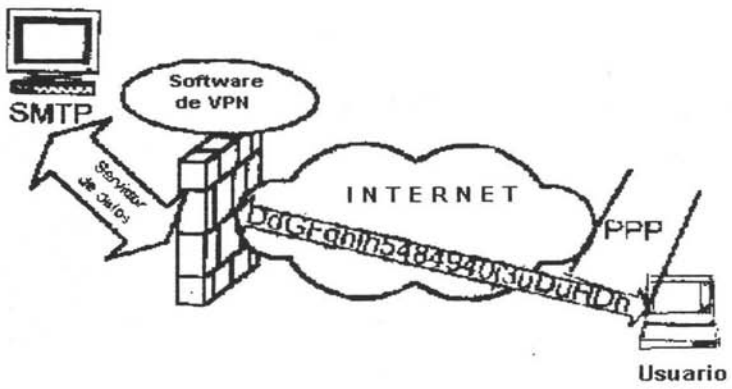


Fig. 3.4 Configuración cliente/VPN típica

En ella hay dos componentes que deben habilitarse para establecer la comunicación:

1.- El dispositivo de cortafuego/VPN debe ejecutar algún tipo de código VPN. Existen muchas formas de realizar esto; algunos cortafuegos tienen incluido en su código la capacidad de crear una VPN, así que las reglas deberán agregarse al cortafuego. Con algunos fabricantes será necesario agregar más software, por ejemplo, si utiliza un cortafuego antiguo que no incluye el cifrado. En este caso, tendrá que encontrar un fabricante cuyo software pueda ser añadido al cortafuego existente.

2.- El equipo portátil tiene una pila de VPN instalada. Se trata de una pila de VPN puesto que una aplicación de VPN implicaría que el código corriera en el nivel 7 (aplicación) del modelo OSI.

Los siguientes pasos describen el proceso de comunicación entre el equipo portátil y el servidor interno, una vez que se han completado las configuraciones:

1.- El usuario con el equipo portátil marca a su PSI local y establece una conexión PPP.

2.- El equipo portátil solicita las claves del dispositivo del cortafuego/VPN. Éste puede ser un paso manual realizado por el usuario o un paso automático configurado por el software.

3.- El cortafuegos responde con la clave apropiada

4.- El software de VPN instalado en el equipo portátil espera a que el usuario intente tener acceso al servidor interno (conocido como la dirección IP de destino). Si el usuario visita cualquier sitio distinto al de la red corporativa, no pasa nada, Ahora si el usuario desea hacer una conexión con el servidor interno, el software que se ejecuta en el equipo portátil ve la solicitud (de nuevo conocida dirección IP), cifra el paquete y lo envía a la dirección IP pública de la combinación cortafuego/VPN.

5.- El dispositivo de cortafuego/VPN le quita la dirección IP descifra al paquete y lo envía al servidor dentro de la LAN local.

6.- El servidor interno responde la solicitud y envía el documento de regreso.

7,.- El cortafuego/VPN examina el tráfico, por su tabla sabe que es una configuración de túnel de VPN. Así que toma el paquete, lo cifra y lo envía al equipo portátil.

8.- La pila de VPN en el equipo portátil ve el flujo de datos, sabe que viene del dispositivo del cortafuego/VPN descifra el paquete y lo maneja en aplicaciones de niveles superiores.

Esta configuración es la que permite que la VPN tenga una gran flexibilidad, puede utilizar Internet como su propia red privada.
¿ Desea utilizar la norma PPTP, L2TP IPSec que aún esta siendo desarrollada?. Recuerde que IPSec es un marco de referencia así que el cifrado DES podría utilizarse en un escenario IPSec.

Existen otro tipo de topologías como:

3.4.2 Topología de VPN/LAN a LAN. Esta topología es la 2da. más utilizada.

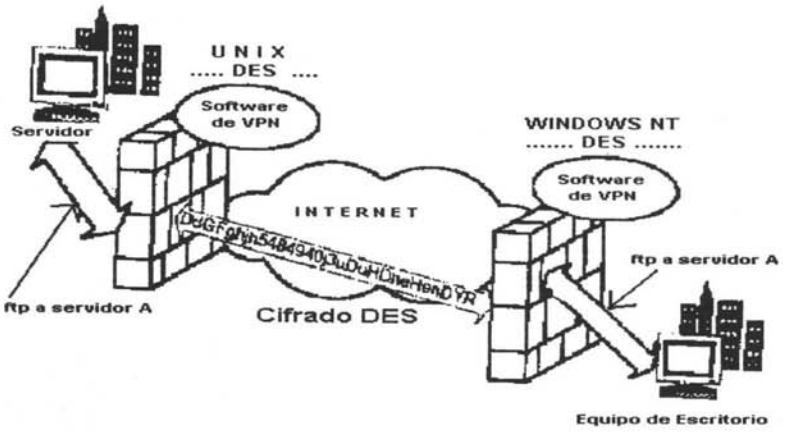


Fig. 3.5 **Topología de VPN/LAN a LAN.**

En la figura 3.5 aparece una organización con una oficina remota. Las dos tienen su cortafuego propio, una es una máquina basada en NT y la otra una máquina basada en UNIX. Ambas ejecutan software de VPN de distintos fabricantes y el algoritmo de cifrado en los productos VPN de los fabricantes es DES.

El ejemplo presenta a un usuario de la oficina remota que necesita conectarse al servidor de la otra oficina y hacer una transferencia FTP para transferir un archivo. Antes de realizar la comunicación, los componentes que deben habilitarse son los siguientes:

1.- El administrador de cada sitio está de acuerdo con el cifrado DES. El software de VPN de cada dispositivo crea una clave única.
2.- Si se trata de un producto de cortafuego/VPN, el administrador de cada oficina establece una regla, por ejemplo, que todo el tráfico destinado a la otra terminal debe cifrarse.
3.- El usuario final utiliza una aplicación FTP en su escritorio para intentar conectarse al servidor.
4.- El paquete abandona el escritorio en texto sencillo y llega al dispositivo de cortafuego/VPN.
5.- El paquete es cifrado y se envía a la dirección IP pública del dispositivo de cortafuego/VPN de la otra oficina.
6.- El cortafuego/VPN acepta y descifra el paquete y lo reenvía a su destino final.
7.- El servidor recibe el paquete y responde.
8.- Envía un paquete en texto sencillo a su dispositivo de cortafuego/VPN local.
9.- Después, el cortafuego/VPN lo cifra y lo envía al otro cortafuego/VPN.
10.- El cortafuego/VPN lo descifra y finalmente lo envía de regreso al usuario original.

Lo mejor de esto es que el usuario no tiene idea de que el cifrado se realiza, no hay nada que el usuario final deba hacer para efectuar esta tarea. En lo que concierne al usuario, el servidor está en su red. El servidor no necesita una configuración especial, puesto que cree que está recibiendo una solicitud y una respuesta normales. Los aspectos importantes son los relacionados con el enrutamiento, tanto la máquina del usuario como la del servidor deben saber a qué direcciones enrutar el dispositivo de cortafuego/VPN.

3.4.3 Topología de VPN/cortafuego a Intranet/Extranet

La única diferencia entre las intranets y Extranets VPN y no VPN, es el punto donde se efectúa el proceso de cifrado. Si es en la máquina, piense en la seguridad web como en un servidor web típico.

En un futuro desaparecerá la diferencia entre intranets y Extranets. ¿Cómo identificará a los empleados que requieren los servicios de Intranet pero que acceden a ellos externamente y a los clientes externos a quienes sólo se les permite el acceso a la Extranet?. En la figura 3.6, la Extranet se coloca en la zona DMZ junto con el servidor web. Los clientes y los proveedores tienen permiso para conectarse al servidor de la Extranet. El servidor web sólo es para tráfico web normal y está disponible para todos. La Intranet se ubica detrás del dispositivo VPN y sólo los usuarios internos que llegan de Internet la usan.

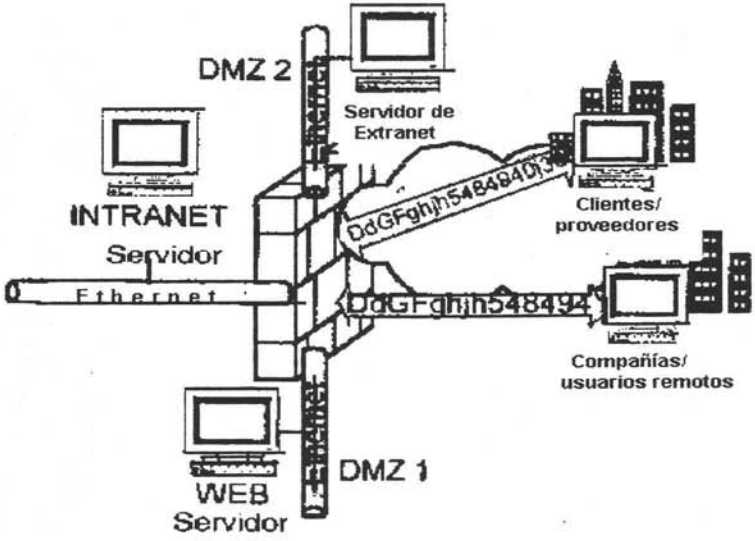


Fig. 3.6 Topología de VPN/cortafuego a Intranet/Extranet

Coloque los servidores de red de acuerdo con su función. Si está permitido el acceso público, colóquelos en una DMZ pública. Si hay clientes y proveedores, colóquelos en su propia DMZ. Si hay empleados, de nuevo colóquelos en su propia DMZ. Con máquinas bien instaladas puede tener varias zonas DMZ.

La Extranet se coloca en su propia red por separado. La seguridad que puede implantar aquí, es permitir que sólo aquellas direcciones de origen que considere necesarias pasen al dispositivo de cortafuego/VPN. Su Extranet se estableció entre ciertas compañías y fabricantes, así que lo más probable es que lleguen desde sus propias redes internas. Por lo tanto, puede restringir el acceso sólo a esas redes. En esta topología el cifrado se aplica al flujo de datos.

3.4.4 Topología de VPN/tramas o ATM

Un gran atributo de Internet es su flexibilidad para habilitar comunicaciones instantáneas. Sin embargo, algunos negocios no creen en la eficiencia de Internet para transmitir información crítica/comercial debido a sus aspectos de seguridad. Esta es la razón de porque las compañías construyen intranets empleando sólo líneas rentadas o enlaces basados en retransmisión de tramas para conectarse a sus sitios. Por lo tanto, las redes privadas virtuales pueden configurarse sobre una infraestructura tal como ATM o topologías de redes basadas en tramas. Los negocios que ejecutan sus propias intranets sobre esta topología de VPN tienen la misma seguridad, facilidad de administración y confiabilidad que en sus propias redes privadas.

3.4.5 Topología de VPN de hardware (caja negra)

Las VPN de hardware, o cajas negras, son dispositivos independientes que implantan algoritmos de tecnología VPN. Algunas soportan normas de cifrado DES de 40 bits (internacional) y 3DES (Estados Unidos y Canadá). Se cree que los dispositivos de hardware son capaces de completar más rápido el proceso de cifrado/descifrado que los dispositivos de software de las VPN. Los dispositivos de hardware tienen servicios adicionales como cortafuegos, antivirus y capacidad de enrutamiento. Los dispositivos de hardware por lo general incluyen software adicional que se instala en el equipo de escritorio para permitir la configuración y el mantenimiento de ese dispositivo.

3.4.6 Topología de conmutación de VPN

Son conmutadores de nivel 3 que crean túneles bajo solicitud. Tienen la capacidad para crear y asignar características de túneles y conmutar tráfico multiprotocolo, realizan cifrado, encapsulamiento y enrutamiento multiprotocolo a la velocidad del cable. Además tienen una característica útil para soportar una conmutación basadas en las políticas del protocolo de red. Estos conmutadores de VPN incluyen software para mantenimiento remoto que proporciona capacidad de planeación, tolerancia frente a las fallas e información estadística, como la utilización de túneles y la calidad de servicio de supervisión.

3.4.7 Balance de carga y sincronización

Del mismo modo en que cualquier compañía podría utilizar el balance de carga en sus servidores críticos, la tecnología VPN puede tener balance de carga. El balance de carga es el proceso de distribuir las necesidades de procesamiento de las VPN entre varios servidores. La sincronización es el proceso de sincronizar dispositivos VPN. La configuración de un brazo (en paralelo), es una topología típica cuando se utiliza el balance de carga y la sincronización. Esta es la razón por la cual las VPN pueden crecer.

3.4.7.1 Balance de carga

Existen tres formas de realizar un balance de carga.

- 1ro.Puede establecerse alguna política de enrutamiento en los enrutadores de la compañía.
- 2do. El dispositivo VPN puede enviar una consulta a un grupo de servidores para ver cuales servidores están cargados.

Por ejemplo: si se permiten VPN de Extranet y se considera que se podrían llegar a tener 5,000 usuarios simultáneos en cualquier momento. En este caso, quizá se disponga de dos o tres Extranets y el dispositivo VPN pregunta que servidor manejará la solicitud. En algunas configuraciones para balance de carga, el dispositivo VPN puede consultar secuencialmente en busca de un factor de carga o para determinar cual servidor responde más rápido.

- La tercera forma depende del propio dispositivo VPN. Cuando se realiza una conexión, el más rápido en responder será el utilizado para todas las comunicaciones posteriores o se puede ajustar el número máximo de conexiones. Si por ejemplo, cree que tendrá que soportar a 500 usuarios, puede ajustar cada dispositivo VPN para que maneje a 250 usuarios.

3.4.7.2 Sincronización

Es el dispositivo en el que ambos dispositivos VPN mantienen las mismas tablas de estado. De esta forma, si un dispositivo queda fuera de servicio, el otro puede responder las solicitudes que han sido enviadas al dispositivo descompuesto.

Existen muchas más topologías y más que se irán agregando conforme pase el tiempo, concluiremos diciendo que la única diferencia entre las dos primeras topologías y la topología de las VPN de Intranet y Extranet es que esta última solo agrega otra capa de cifrado a los servicios web.

Estas configuraciones de topologías pueden ser sencillas, lo cuál facilita la ubicación y el procedimiento de instalación, pero la contraparte es la capacidad de flexibilidad y de supervisión.

3.5 ¿Por qué utilizar Redes Privadas Virtuales, para realizar el enlace de la Intranet a la Extranet?

El enlace entre una Intranet y una Extranet lo haremos vía Red Privada Virtual o VPN y en este punto trataremos de justificar el porque de nuestra decisión.

Empezaremos retomando algunos conceptos:

Internet .- Es un sistema de telecomunicaciones abierto de tecnologías y protocolos, que permite a los usuarios de computadoras disímiles con sistemas operativos disímiles acceder a los sitios de información de los demás a través de interfases gráficas que conocemos como exploradores. Internet también hospeda funcionalidad de transferencia de archivo, correo electrónico, salas de charla y la diseminación de información gráfica y multimedia. Cuando la WAN interna de una empresa se basa en las tecnologías y los protocolos de Internet, a la red resultante se le conoce como **Intranet**.

Extranet .- se establece cuando una empresa conecta a organizaciones externas, como socios comerciales, clientes preferidos o proveedores, con aplicaciones internas que se ejecutan en su Intranet segura. La vinculación de empresas separadas en una red unificada está revolucionando la manera en que las empresas se comunican, acceden información, colaboran, conducen transacciones de negocio a negocio y realizan negocios en general.

El uso de Internet puede ser la manera más fácil y económica para implantar una columna vertebral de comunicaciones para su Extranet. Con los avances y los estándares que componen las tecnologías de VPN, junto con el respaldo de **ANX**[8], Internet aún puede cumplir su promesa de comunicación de datos ubicua, confiable y segura para la comunidad de negocios.

Existen varias maneras de establecer una Extranet. A continuación se muestra una lista de opciones de despliegue potenciales de la comunicación menos segura a la más segura:

1.- Acceso de marcado a través de un PSI que utiliza Internet
2.- Acceso marcado a través de un PSI que utiliza una red pública de datos, es decir, MCI Communications, CompuServe, UUNET, etc.
3.- Acceso de marcado a través de un PSI que utiliza Internet y autenticación de usuario.
4.- Acceso de Marcado a través de un PSI que utiliza líneas telefónicas digitales es decir, ISDN. DSL y líneas arrendadas.
5.- Acceso de marcado a través de un PSI que utiliza líneas telefónicas digitales y firewall.
6.- Acceso de marcado a través de un PSI que utiliza una VPN

[8] Redes Automotrices.

Aunque la segunda opción es un poco más segura que la primera, ninguna de las dos protege la información mientras pasa por Internet o por una red pública de datos. Las siguientes tres opciones agregan cierta disuasión adicional para intrusos y, con encriptación, usted podría alcanzar una cantidad decente de privacidad. Sin embargo, los intrusos aún podrían obtener acceso a la red. Más aún, las opciones 4 y 5 son implantaciones de red privada, que podrían ser excesivas o demasiado costosas para muchas empresas.

La implantación VPN podría soportarse directamente por una empresa o a través de un PSI. Esta última opción gana en seguridad y nuestro objetivo principal además de economizar es mantener una seguridad a toda prueba.

Un PSI puede ofrecer una solución VPN como una de sus ofertas de servicio. El establecimiento de una Extranet con esta opción es lo más seguro, porque incorpora entunelamiento, autenticación y encriptación para privatizar un canal de comunicación mediante Internet. Antes, cuando la tecnología de VPN apenas comenzaba, Extranet y VPN se utilizaban de manera indistinta. En la actualidad, Extranet se refiere sobre todo a una Intranet que vincula socios comerciales externos. Mientras que VPN se refiere más al método para lograr ese fin.

Las VPN's proporcionan a las empresas la seguridad, el desempeño, la disponibilidad y el ambiente de multi protocolo de una red privada a través de la económica y ubicua Internet. Para el registro, las VPN's proporcionan vínculos seguros de transporte de datos, llamados túneles, a través de las líneas de comunicación públicas de Internet. Los túneles seguros se establecen entre dos nodos o sitios de Internet mediante las tecnologías de encriptación, autenticación y validación de datos que trabajan en concierto. Las VPN's utilizan autenticación sólida para establecer el túnel, encriptan los paquetes o datagramas de IP para mezclar los datos para su protección, luego emplean verificaciones de integridad de datos para asegurar que los paquetes arriben sin alteración a su destino. En otras palabras permiten que la información privada se transmita a través de Internet pública sin sufrir ataques de hackers. En efecto, Internet se transforma en su propia red virtualmente privada.

En lo que respecta a seguridad de red, la protección proporcionada a través de VPN's es tan completa como se obtiene. Las VPN's protegen de manera primordial datos cuando utilizan túneles a través de las líneas de comunicación de Internet. Este proceso, aunque es muy efectivo con información en tránsito, no ofrece la mayor protección para la propia red. Como en el caso de redes privadas, un firewall ofrece el mejor potencial para la seguridad de VPN. Las VPN's y firewalls, que funcionan en conjunto, protegen datos en tránsito y detrás del firewall. Los firewalls logran protección y privacidad de red a través de control de acceso. Éste especifica la cantidad de libertad que tiene un usuario de la VPN, restringe ciertos tipos de tráfico y controla el acceso de socios, empleados y otros usuarios externos a aplicaciones de varios dominios de red. De este modo, el control de acceso no sólo protege los datos de la red, sino también protege todo el cúmulo de capital intelectual de la empresa al asegurar que los usuarios de la VPN tengan acceso completo a las aplicaciones que necesitan, pero nada más.

La capacidad de las VPN's y firewalls para proteger datos en tránsito y residentes, respectivamente, hace que sean en definitiva una pareja constituida en el ciberespacio.

Una de las premisas principales de las VPN's es proporcionar una columna vertebral de comunicaciones de costo accesible como alternativas a otras opciones de columna vertebral más costosas, como transmisión de tramas y redes IP públicas (diferentes de Internet). Un estudio de costos de VPN reciente conducido por la revista Data Communications reveló que una VPN puede ahorrar a las empresas más del 50% en costos de conectividad sobre una red basada en transmisión de tramas comparable.

Tabla 2 Comparación entre columnas vertebrales de comunicaciones de WAN

Atributos	Retrasmisión de tramas	Internet	Red de IP pública
Ubicuidad	Baja	Alta	Moderada
Costo	Moderado	Bajo	Moderado
Seguridad Inherente	Alta	Baja	Alta
Desempeño	Alto	Moderado bajo	Alto
Niveles de servicio garantizado	Sí	No	Sí

Como era de esperarse, Internet recibe una calificación "Baja" en "Seguridad Inherente". Sin embargo, cuando se consideran las VPN's, la seguridad es igual o mayor.

Con el análisis anterior pretendemos convencer al lector del porque esta tecnología fue escogida para llevar a cabo nuestro enlace de Intranet a Extranet. A lo largo de nuestro proyecto comprenderemos mejor esta tecnología.

3.5.1 Razones para implantar una VPN en su negocio

Las VPN juegan un papel importante en el proceso que permite a la compañía conducir sus negocios en una forma menos cara, ofrecen a las compañías una manera de reducir sus costos, mejorar sus servicios y mantener su base de clientes. Algunas de las razones por las que muchos negocios utilizarán las VPN para conducir sus negocios son las siguientes:

- Las VPN utilizan Internet como su medio de transporte.
- Internet es un medio propicio tanto para clientes comerciales como privados.
- Internet se extiende por todo el mundo
- La conductividad en Internet es extremadamente eficiente en el mercado actual, y muchos PSI procuran mantener la conexión.
- Las VPN son flexibles, dinámicas y escalables.
- La tecnología base de las VPN es el conjunto de protocolos TCP/IP de Internet, lo cuál la hace más fácil de comprender e implantar que una tecnología nueva.

3.5.2 Identificación de la necesidad de una VPN

¿Cómo convencerse de que su compañía necesita una VPN?, ¿ En realidad puede ayudar a su negocio a ampliarse y crecer? Aunque siempre existen beneficios potenciales para mejorar una compañía con la tecnología VPN, eso sólo puede ser benéfico en ciertas áreas y aplicaciones.

3.5.3 Áreas en las que la tecnología VPN puede ser benéfica para su organización

- Acceso remoto de usuarios
- Aplicaciones de Extranet
- Sitios Internacionales
- Base de usuarios geográficamente diversa
- La necesidad de soportar una base de clientes geográficamente diversa
- Expansión barata del mercado
- Requisitos razonables de ancho de banda.
- Necesidad de un alcance global de bajo costo
- Acceso a servicios externos
- Líneas rentadas virtuales.

Junto con las áreas de beneficio, también existen algunas áreas donde la tecnología VPN puede no ser recomendable para su compañía. Estas se aplican a la infraestructura interna y a sus requisitos particulares.

3.5.4 Áreas en las que la tecnología VPN quizá no sea benéfica

- Donde el desempeño es apremiante.
- Donde el estado latente es inaceptable
- Donde los protocolos sin normas no puedan encapsularse con el protocolo IP nativo de Internet.
- Principalmente en tráfico isócrono, como el teléfono

La diferencia entre un Servicio de VPN local y uno de VPN Internacional, es que se añade el perro guardián de los gobiernos. Como se mencionó anteriormente, las VPN son cifradas. El cifrado es considerado como arma, y los gobiernos regulan las armas.

De la misma forma que el capítulo anterior, en este apartado se trataron los aspectos fundamentales de la tecnología Extranet, además de introducirnos a la tecnología VPN, con lo cual permitirá al lector tener los conceptos necesarios para poder llevar a cabo el siguiente paso, el cual consiste en seguir una metodología que le permita realizar el enlace "Intranet – Extranet", a través del uso de la tecnología VPN.

CAPÍTULO IV

METODOLOGÍA DE ENLACE INTRANET-EXTRANET POR MEDIO DE UNA RED PRIVADA VIRTUAL

CAPITULO IV METODOLOGIA DE ENLACE INTRANET-EXTRANET POR MEDIO DE UNA RED PRIVADA VIRTUAL

En este apartado se establecerá una metodología para la incorporación de la Intranet a la Extranet, llevando a cabo este procedimiento en las distintas áreas del enlace con la tecnología de las VPN.

Metodología

Para llegar a la utilizada en nuestro proyecto, analizamos cada una de las siguientes metodologías, en cada una de ellas veremos cuales son sus características, sus ventajas y desventajas, y con ello justificaremos el uso del tipo de metodología en nuestro trabajo. Cada una de las sistemáticas analizadas han sido utilizadas para resolver problemas de manera general.

Metodología de May Consiste en cinco etapas importantes, que pueden resumirse de la siguiente manera:
Etapas
Definición del problema
Elegir los objetivos
Síntesis del sistema
Análisis del sistema
Seleccionar el sistema "óptimo"
Planear la acción

Metodología de RAND La metodología de análisis de sistemas RAND también se describe como una serie de etapas:
Etapas
Formulación (la fase conceptual)
Investigación
Valuación
Interpretación
Verificación

Ambas metodologías enfatizan un enfoque sistemático para la investigación de problemas. Dan considerable énfasis en la definición del problema y en la necesidad de consenso por los objetivos. Las metodologías detallan las etapas involucradas en un análisis completo, pero no muestran como debe emprenderse cada etapa. Por lo que queda en cada lector formarse un criterio y tratar de aplicarlo en su proyecto.

Metodología de Checkland.- Esta metodología se infirió en forma experimental y representa la culminación del aprendizaje alcanzado en un gran número de proyectos. En esencia, la metodología puede describirse como un proceso de siete etapas de análisis que emplean el concepto de un sistema de actividad humana como un medio de conseguir tanto "investigar" la situación como "efectuar acciones" para mejorarla.

La secuencia lógica ilustrada mediante la figura 4.1es una manera útil de describir la metodología pero no necesariamente representa la secuencia en que se usa. En realidad representa un patrón de actividades.

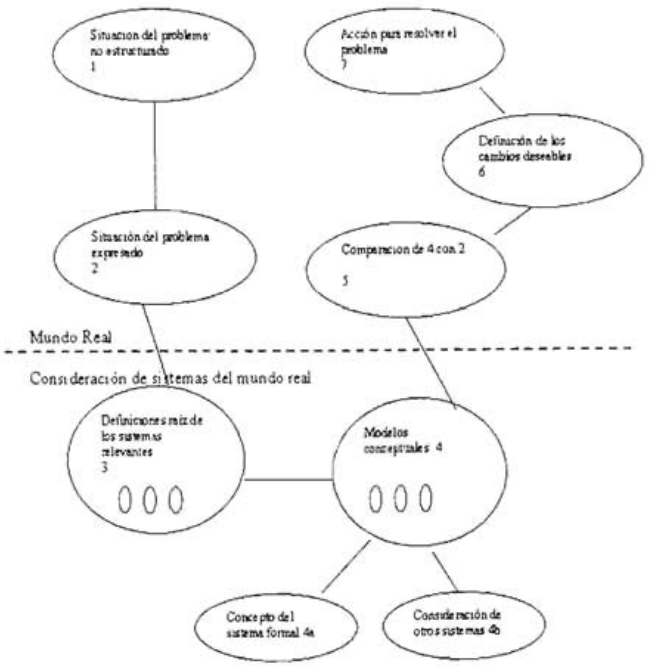


Fig. 4.1 Metodología de Checkland

Metodología Jenkins.- La metodología Jenkins consiste en las siguientes cuatro etapas importantes :

Etapas	Pasos a seguir
Análisis de los sistemas	* Formulación del problema * Organización del proyecto * Deficinión del sistema * Definición del sistema más amplio * Objetivos del sistema más amplio * Objetivos del sistema * Definición de un criterio económico global * Recopilación de información y datos
Diseño de los sistemas	* Pronóstico * Construcción del modelo y simulación * Optimización * Control * Confiabilidad
Implantación	* Documentación y aprobación de la autorización * Construcción
Operación	* Operación inicial * Apreciación retrospectiva * Operación mejorada

Esta metodología se basa en la idea de que la aplicación de la ingeniería al sistema en que se ubica el problema a resolver.

Por los pasos a seguir que se consideran en esta metodología, creemos que se adecua mejor a nuestro trabajo. Debemos mencionar que hemos tratado de ajustar las actividades, por lo que en algunos pasos, las formas de llevarlo a cabo cambiaron para lograr un mejor desarrollo del proyecto, siendo un tanto más explícito y fácil de digerir para los lectores.

La misma metodología es un sistema de aprendizaje y por tanto puede ser aplicable para muchas situaciones pendientes de resolver, pero está en cada lector formarse un criterio de cómo aplicarla, ya que muchas de las metodologías existentes dejan un gran margen al lector para enriquecer el proyecto.

El desarrollo de nuestro trabajo se resume de manera general a las siguientes etapas:

Etapas	Pasos a seguir
Análisis	• Razones para conectarnos a Internet • Etapa de preguntas y respuestas • Planteando el problema • Selección del tipo de configuración de la Extranet • Arquitectura VPN basada en Cortafuego • Elección del sistema operativo • Topología de cortafuego/VPN a cliente • El papel del firewall (cortafuegos) en la VPN • Compatibilidad con el hardware y el software • Interoperabilidad • Hardware para el servidor
Diseño	• Desarrollo del Diseño y Estructura de la Red • Diagrama de la situación actual de la red • Mapa de la distribución de los equipos • Estructuración del contenido • Selección de la información a la que se tendrá acceso
Implantación	• Inventario del equipo existente • Componentes que forman una VPN • Obtención y asignación de un espacio de dirección IP • Motivo para subdividir la red 230 • Implantación de una buena política de seguridad • Implantación de la administración del tráfico • Aspectos de la implantación SMTP y DNS • Implantación de la autenticación • La regla Drop All • Implantación de la regla VPN • VPN de la sucursal • VPN de usuarios remotos
Instalación	• Tipos de VPN • Instalación en Unix o Windows • Comparación genérica de vendedores de VPN
Mantenimiento	Capítulo 5

Podemos decir que todas las metodologías son buenas, cada una cumple su función al ser utilizadas, para este proyecto elegimos esta última.

4.1 ANALISIS

4.1.1 Razones para conectarnos a Internet

Objetivos de la empresa.

Este punto nos indica simplemente que la empresa ha decido crecer y pasar de una Intranet a una Extranet, para lograrlo ha de valerse de la poderosa herramienta llamada Red Privada Virtual o VPN.

4.1.2 Puntos a considerar antes de iniciar la implantación de la VPN

Existen innumerables opciones para la instalación de las VPN, desde las VPN independientes basadas en caja negra y VPN basadas en enrutador, hasta las VPN basadas en software y en cortafuego. Pero, ¿cuál es la mejor opción de VPN para implantarla en nuestro proyecto?

Además en un proceso de implantación de Red Privada Virtual (VPN), es necesario considerar las siguientes cuestiones:

¿Desea utilizar una VPN de retransmisión de tramas (frame-relay) o ATM?

Las VPN vienen en todas formas, tamaños y colores. Tal vez ya cuente con un proveedor de retransmisión de tramas y quizá desee instalar una VPN en ese transporte.

Cómo elegir los servicios de VPN.

El primer paso básico en la elección de un servicio de VPN es considerar ¿Cómo se llevarán los datos del punto A al punto B?, y por ende, también resulta importante conocer ¿Dónde están los puntos A y B?, debido a que no es lo mismo un servicio de VPN local y una VPN Internacional. La diferencia entre ambos servicios es que se añade el perro guardián de los gobiernos, ya que como se mencionó anteriormente, las VPN son cifradas.

Se necesita acceso remoto y/o LAN-to-LAN?, ¿Cuál es el presupuesto?

Dependiendo de la respuesta se debe escoger qué tipo de implante se realizará:
- Si solo se necesita acceso remoto, el presupuesto es bajo y la seguridad que se requiere es mínima, lo recomendable es montar una solución con un servidor PPTP bajo Windows NT Server ó 200X Server. Ya que es muy sencilla, requiere poca administración, es muy versátil dado que prácticamente todos los usuarios remotos tendrán PCs con ambientes Windows. Si se necesita mayor seguridad, bastaría con cambiar los tipos de puertos de PPTP a L2TP en el servidor VPN y habilitar la opción de IPSec.

- Si solo se necesita LAN-to-LAN y el presupuesto es bajo, lo recomendable es montar un gateway seguro IPSec bajo Linux en cada sede.

- Si se cuenta con los recursos se podría pensar en una solución por hardware como routers o equipos diseñados para hacer VPN como los de Netscreen. En LAN-to-LAN no se evalúa la seguridad necesaria, ya que se asume que esta debe ser alta, y bajo ese principio se parte.

¿Qué tipo de seguridad utilizará?

Algunos de los protocolos de seguridad que serán la norma son el Protocolo para establecimiento de túneles punto a punto (PPTP), el Protocolo para establecimiento de túneles de nivel 2 (L2TP) y el Protocolo de seguridad de Internet (Ipsec). ¿ Sabe cuál es la norma que utilizará? ¿Puede adivinar cuál es la que utilizarán sus socios de VPN? Si la tecnología VPN sólo es para conectarse a oficinas corporativas, entonces usted podría establecer una política corporativa que dictará la norma a utilizar. Si va a establecer conexiones con clientes potenciales y con socios comerciales a través de su tecnología VPN, no puede establecer una política corporativa. En una situación como esta, deseará esperar o instalar la tecnología VPN que pueda actualizarse para cualquier norma que se acepte.

¿Qué tipo de infraestructura de hardware soporta mi organización?

Comprender la infraestructura del sistema operativo de su organización es una consideración importante, ya que si decide que va a emprender este proyecto, su personal de soporte técnico debe tener las habilidades para la plataforma en particular.

¿Cuántos usuarios estima que utilizarán esta VPN?

Ante este problema, debe darse una idea del número de usuarios futuros de su tecnología y no sólo de los usuarios actuales. Si es un proveedor final y todos sus clientes tratarán con usted a través de la VPN, necesita crecer. Si es una empresa de ventas o una franquicia y todos sus puntos de venta utilizarán la tecnología VPN, necesitará ancho de banda. Si los usuarios remotos son pocos, se podría habilitar el servicio de acceso remoto en un servidor Windows NT, 2000 o Linux y colocar un par de módems. Si los empleados se conectan desde fuera de la oficina pero no salen de la ciudad, es decir, no se incurre en cargos de larga distancia tampoco sale rentable montar un acceso remoto VPN.
Si el tiempo de conexión de los trabajadores remotos es de unos pocos minutos, así estén fuera de la ciudad o incluso fuera del país, se deberá evaluar muy bien económicamente ambos casos. es decir, VPN o el sistema tradicional.

Esto involucra a su PSI[9] en los problemas de desempeño. ¿Puede obtener garantía de cualquier tipo de servicio o de cualquier tipo de contrato de calidad del servicio?. En este caso, debido a que una buena parte de su ingreso se derivará de las operaciones en la VPN deberá analizar los requisitos de ancho de banda con su PSI para asignarle un tamaño correcto a su conducto.

¿Cuántos usuarios hay en cada red LAN remota, y qué tipo de aplicaciones se manejarán entre ambas sedes?

La respuesta a estas preguntas sirve para dimensionar la capacidad del ancho de banda a contratar o el aumento del canal que ya se tiene. De todas maneras este valor está influenciado por apreciaciones probabilísticas sobre el uso simultáneo de los túneles por parte de los usuarios. En otras palabras es posible que se necesite el mismo ancho de banda para interconectar dos oficinas que tienen 5 usuarios cada una pero que acceden continuamente a una base de datos o intercambian archivos constantemente, que el necesario para unir dos oficinas con 30 usuarios cada una pero que rara vez acceden a los recursos remotos o que tienen aplicaciones en modo texto.

Existen muchas preguntas más que debe plantearse acerca de su organización, tales como:

¿Cuál es el propósito general de su red?, ¿Cuáles tipos de aplicaciones se soportan y cuáles funciones proporcionan?,¿Cuál es la mezcla de aplicación y cuál es el punto de equilibrio de la demografía de usuarios para cada aplicación? ¿Sus usuarios son una fuerza de trabajo móvil, o funcionan en lugares remotos?¿Son usuarios de poder, o tiene altas concentraciones de usuarios profesionales o administrativos o una combinación equilibrada?

Dependiendo de cómo responda a estas cuestiones su VPN comenzará a tomar forma y usted podrá empezar a limitar sus opciones sobre que tipo de arquitectura puede soportar y mantener. Debe tener un estimado del número de túneles de VPN que podría necesitar, así como qué tipo de solidez de cifrado necesita su organización en comparación con lo que puede utilizar.

¿Las oficinas a conectar ya cuentan con enlace a Internet?, ¿A qué velocidad?, ¿Es dedicado o conmutado?

Conocer esto, ayuda a dimensionar los costos iniciales de la solución, que en muchos casos es un factor que influye mucho en la toma de una decisión, sobre todo cuando se trata de una empresa pequeña que no tiene los recursos para invertir en una solución dedicada a Internet. En el montaje de una solución LAN-to-LAN lo más probable es que se necesiten soluciones de banda ancha para conectar las oficinas a Internet. Cuando el tráfico sea bajo o se esté montando una solución de acceso remoto VPN puede ser suficiente una conexión conmutada ISDN [10] en el lado del servidor VPN.

---

* PSI: Proveedor de Servicios de Internet

[10] Red Digital de Servicios Integrados

¿Qué tan confidencial y sensitiva es la información que se intercambia?

Con esta pregunta lo que se busca es escoger de manera adecuada los gateways VPN. Un algoritmo de cifrado fuerte como 3DES o DES es recomendable implantarlo con soluciones por hardware ya que estos equipos tienen circuitos integrados dedicados a la labor de cifrado, por lo tanto no se sacrifica el desempeño del enlace de manera dramática. Aquí también está involucrada la cantidad de tráfico a encriptar. Definitivamente soluciones con software para este tipo de necesidades no son adecuadas. Si se necesita acceso remoto altamente seguro es necesario instalar clientes IPSec en los equipos portátiles y descartar de plano soluciones con PPTP o L2TP así se habilite el cifrado de datos de Windows.

¿Qué tan criticas son las aplicaciones a ejecutar en la VPN para la compañia?

Esto sobre todo sirve para escoger el proveedor de acceso a Internet que se va a escoger. Si las aplicaciones que transitan por la VPN son criticas, por ejemplo, un sistema de cobro en línea, se tendrán que realizar una serie de exigencias al PSI tales como ofrecer backup en la última milla y el backbone a Internet, fijar una serie de cláusulas de cumplimiento a través de un SLA[11] y garantizar calidad de servicio.

VPN proporcionada por un proveedor de servicios de red

Esta puede ser una manera fácil y eficiente de conectar su organización a Internet y disfrutar los beneficios de una VPN. El PSI es el encargado de controlar el acceso a Internet de su empresa, lo cuál facilitará la solución de problemas.

En una solución de proveedor de servicios, el proveedor llevará a cabo todas las tareas del personal normal de seguridad en Internet, además de los puntos de conexión en Internet, mientras que al mismo tiempo hará recomendaciones valiosas y ofrecerá lineamientos sobre la seguridad.

¿Qué sucede si delega el esfuerzo completo en una fuente externa, como un PSI?, ¿ Cómo se compara esto con "crear" la aplicación usted mismo? ¿ Cuáles ventajas ofrece un PSI en seguridad? ¿Cuánto costaría soportar una VPN mediante un PSI? ¿Qué costo tendría una VPN si se implantará y manejara en casa? Las respuestas a éstas y otras preguntas de esta evaluación le proporcionarán la dirección óptima a su organización. Una última advertencia: debe incluir también los planes de negocios futuros.

[11] Contratos de nivel de servicios.- Cuantifican los objetivos específicos y las medidas de evaluación de la VPN.

Aplicaciones cliente

Con el fin de que las computadoras portátiles creen un túnel de VPN, será necesario utilizar software especial en ellas. ¿Quién preparará a todas estas laptops, equipos de escritorio y demás, y quién les dará mantenimiento? Sería imposible para su PSI lograr esta tarea, pero una vez que haya cargado el software, él le ayudará a resolver los problemas de las conexiones al dispositivo VPN. El principal problema ocurre si ya existe algún software cargado en esas máquinas que pudiera crear conflictos con el software de la VPN.

4.1.3 Planteando el problema

Para tener un panorama más amplio del funcionamiento de las VPN's observaremos paso a paso una implantación de Cortafuego/VPN[12]. Este ejemplo nos permitirá poner en práctica la metodología empleada para encontrar la VPN que cubra mejor nuestras necesidades, simplemente utilizamos el ejemplo de un cortafuego/VPN porque es una de las configuraciones más comunes.

El ejemplo fue modificado de acuerdo a nuestro interés, para permitir con ello observar claramente los pasos necesarios y así cubrir la metodología utilizada, y con esto lograr un fin éxitoso para nuestra empresa.

En el ejemplo iremos paso a paso acerca de un producto de cortafuego que tiene capacidades integradas para VPN, que se ejecuta en una plataforma UNIX. El cortafuego utilizará un servidor RADIUS independiente para la autenticación de la Red Interna, estará configurado para permitir acceso remoto a la red interna y utilizará las funciones de un servidor proxy de la red interna.

Es importante aclarar que no emplearemos productos específicos de un fabricante debido a dos razones, la primera es que si se menciona el nombre "*alguien*", podría parecer que tenemos inclinaciones por ese fabricante en particular. La segunda es que la tecnología cambia y para cuando se lea este proyecto quizá el producto de ese fabricante ya no sea el adecuado para su empresa.

Se ha intentado presentar a la tecnología como una caja negra en la medida de lo posible, usted solamente tiene que establecer un escenario y simplemente colocar un producto en su lugar.

[12] Este ejemplo lo tomamos del libro " Implementación de Redes Privadas Virtuales (RPV) ", de Steven Brown, página 193.

4.1.4 Selección del tipo de configuración de la Extranet

Las VPN se presentan en cuatro áreas. Cabe mencionar que las áreas simplemente significan implantaciones comunes de VPN y sólo son un término utilizado en muchos artículos.
Después de examinar las siguientes cuatro áreas, notará que los conceptos utilizados aquí son comunes a otros términos empleados para describir los servicios de Internet.

- **Intranet.**- Una VPN que permite a los empleados internos conectarse a un servidor interno desde oficinas remotas (por ejemplo, Intranet de LAN a LAN).
- **Acceso remoto.**- Una VPN que permite a los empleados internos conectarse a los servidores internos desde otra ciudad (por ejemplo, marcación de un PSI local y establecimiento de un túnel hacia su organización).
- **Extranet.-** Una VPN utilizada por fabricantes, proveedores y clientes externos para establecer un túnel a un servidor seguro (por ejemplo, comercio electrónico).
- **VPN Interna**.- Una cuarta área de la cuál no hacen uso las compañías actualmente, es una VPN Interna. Esto por cuestiones de seguridad con los propios empleados.

Con el planteamiento anterior y según nuestro problema implantaremos una VPN de Extranet, como ya sabemos esto sólo es un *concepto*.

4.1.5 Arquitectura VPN Basada en Cortafuego.

Se ha decidido instalar una VPN basada en cortafuego, la razón de ello es que probablemente sea la forma más común de implantación de VPN, y muchos proveedores ofrecen este tipo de configuración. Además, la configuración de cortafuego/VPN contiene todos los pasos necesarios para implantar la seguridad y la VPN.

Si la empresa ya cuenta con un cortafuego y sólo está agregando un dispositivo VPN independiente, entonces puede ser tan sencillo como conectar y usar. Esto no significa que las VPN basadas en cortafuego sean superiores a otras formas de VPN, sino más bien se trata de una base establecida a partir de la cual se puede crecer. Actualmente sería difícil encontrar una organización conectada a Internet que no utilice algún tipo de cortafuego.

4.1.6 Elección de sistema operativo

En nuestro ejemplo, se decidió trabajar sobre la plataforma UNIX. Esto, porque muchos de los informes disponibles de algunos proveedores mostraron que el sistema operativo UNIX crece mejor que otros sistemas, y puesto que la empresa tendrá cerca de 100,000 usuarios y l0.000 de ellos podrían utilizar la VPN en cualquier momento, resulta conveniente utilizar dicho sistema operativo (UNIX).

Existen muchos proveedores entre los cuales elegir cuando se considera una VPN basada en cortafuego, y cabe aclarar que los productos están disponibles en todas las plataformas. He aquí algunas consideraciones importantes al elegir el tipo de sistema operativo: ¿En qué plataforma se está ejecutando el cortafuego? ¿Se trata de un dispositivo basado en UNIX, basado en NT o en algún otro dispositivo y cuáles son los puntos vulnerables potenciales de ese sistema operativo?.

No existe un dispositivo que sea 100% seguro, así que si crea la VPN en ese dispositivo, necesitará asegurarse que el sistema operativo subyacente sea seguro.

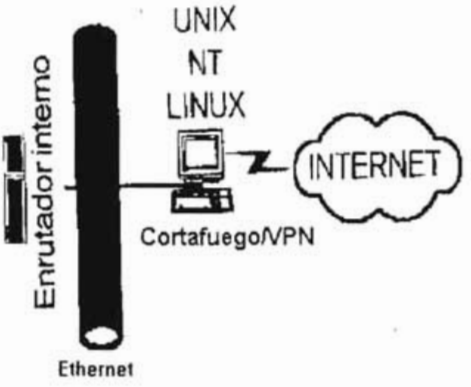


Fig. 4.2 VPN basada en Cortafuego

Aunque esta figura ilustra un producto VPN basado en cortafuego sencillo, su implantación no es tan simple.

Nota: *Los comentarios que manejamos en esta parte tratan de dar un panorama amplio de los sistemas operativos más comunes sin decir que uno es mejor que otro, eso lo dejamos al lector y a sus conocimientos en la materia.*

Windows NT.- Se ha convertido en una plataforma popular para los servidores Web. Los sorprendentes avances en cuanto a desempeño, escalabilidad y confiabilidad de los sistemas Windows NT, planeados por proveedores tradicionales de mini/mainframe como DEC, hacen que el futuro sea de lo más prometedor.

Su solución para VPN, el Servicio de enrutamiento y acceso remoto (RRAS, Routing and Remote Acces Service) legitimó el juego cuando hizo su debut. RRAS ofrece el protocolo de entunelamiento de punto a punto (pptp, Point-to-point Tunneling Protocol) a través de internet. Microsoft ofrece RRAS como descarga gratuita cuando compra e implanta el SO de NT 4.0 Server como sistema operativo de LAN/WAN. Se dice que RRAS y, en particular PPTP, no es tan robusto como Ipsec o, en este caso, el protocolo Layer 2 Forwarding (L2F) de Cisco, esto no se debe por completo a que sea gratuito, sino a que es reflejo de la estrategia de Internet.

Macintosh.- En general, el software de macintosh está diseñado para facilitar al máximo la instalación y uso.

Netware.- Si en la organización utilizan Netware, deberá considerar seriamente la posibilidad de emplear Intranet/ware de Novell.

Oracle.- presiona fuertemente para convertirse en el servidor corporativo de publicaciones de bases de datos Oracle, hay grandes probabilidades que los servidores oracle desempeñen un papel importante en la Intranet.

4.1.7 Topología de cortafuego/VPN a cliente

Así como existen incontables maneras para adquirir e implantar una arquitectura de VPN, también existen muchas formas de colocar esta arquitectura en una topología de VPN. Debe saber que los dispositivos y las configuraciones tienen un lugar propio, y en donde necesite alguno, podrá encontrar el dispositivo más adecuado.

Partiremos diciendo que casi todas las organizaciones conectadas a Internet tienen un cortafuego instalado, y todo lo que necesitan es agregar software de VPN al cortafuego, esta topología es la más común y posiblemente la más fácil de configurar para los que tienen un cortafuego colocado y solo desean la funcionalidad de la VPN.

En el ejemplo que presentamos a continuación tratamos de que observe la manera en que trabaja el cortafuego junto a la VPN, es decir, las funciones que realiza cada dispositivo, paso a paso en un proceso de comunicación.

Ejemplo: Un usuario en su equipo portátil remoto necesita el acceso a un servidor que se encuentra dentro de la red de la compañía, detrás de un cortafuego VPN. El usuario desea conectarse al servidor de la compañía y obtener un reporte confidencial. Esta es la configuración cliente/VPN típica.

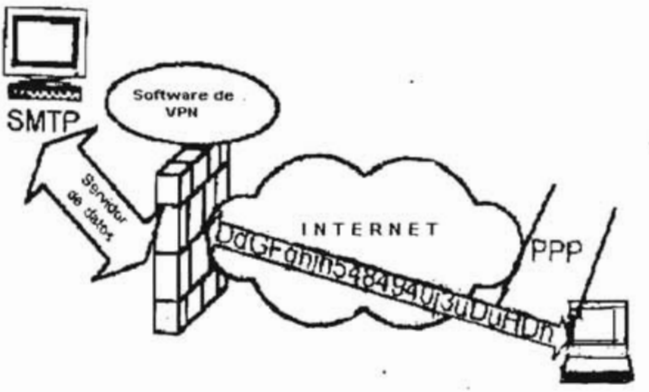


Fig. 4.3 Configuración Cliente/VPN típica

En ella hay dos componentes que deben habilitarse para establecer la comunicación:

1.- El dispositivo de cortafuegos/VPN debe ejecutar algún tipo de código VPN. Existen muchas formas de realizar esto; algunos cortafuegos tienen incluido en su código la capacidad de crear una VPN, así que las reglas deberán agregarse al cortafuego. Con algunos fabricantes será necesario agregar más software, por ejemplo, si utiliza un cortafuego antiguo que no incluye el cifrado, en este caso tendrá que encontrar un fabricante cuyo software pueda ser añadido al cortafuego existente.

2.- El equipo portátil tiene una pila de VPN instalada. Se trata de una pila de VPN puesto que una aplicación de VPN implicaría que el código corriera en el nivel 7 (aplicación) del modelo OSI.

Los siguientes pasos describen el proceso de comunicación entre el equipo portátil y el servidor interno una vez que se han completado las configuraciones:

1.- El usuario con el equipo portátil marca a su PSI local y establece una conexión PPP.

2.- El equipo portátil solicita las claves del dispositivo del cortafuego/VPN. Éste puede ser un paso manual realizado por el usuario o un paso automático configurado por el software.

3.- El cortafuegos responde con la clave apropiada

4.- El software de VPN instalado en el equipo portátil espera a que el usuario intente tener acceso al servidor interno (conocido como la dirección IP de destino). Si el usuario visita cualquier sitio distinto al de la red corporativa, no pasa nada, Ahora, el usuario quiere hacer una conexión con el servidor interno, el software que se ejecuta en el equipo portátil ve la solicitud (de nuevo conocida dirección IP), cifra el paquete y lo envía a la dirección IP pública de la combinación cortafuego/VPN.

5.- El dispositivo de cortafuego/VPN le quita la dirección IP descifra al paquete y lo envía al servidor dentro de la LAN local.

6.- El servidor interno responde la solicitud y envía el documento de regreso.

7.- El cortafuegos/VPN examina el tráfico, por su tabla sabe que es una configuración de túnel de VPN. Así que toma el paquete, lo cifra y lo envía al equipo portátil.

8.- La pila de VPN en el equipo portátil ve el flujo de datos, sabe que viene del dispositivo del cortafuegos/VPN descifra el paquete y lo maneja en aplicaciones de niveles superiores.

Esta configuración es la que permite que la VPN tenga una gran flexibilidad, además puede utilizar Internet como su propia red privada.

4.1.8 El papel del firewall (cortafuegos) en la VPN

La seguridad lo es todo en una VPN, desde el proceso de cifrado que implanta y los servicios de autenticación que se eligen, hasta las firmas digitales y las autoridades emisoras de certificados que utiliza. La seguridad también abarca el software que implanta los algoritmos de cifrado en el dispositivo de la VPN. Si emplea un sistema operativo basado en una VPN, ¿Cuáles son las partes vulnerables del mismo?

Tenemos básicamente cinco etapas para la configuración de un firewall:

1.- Definir los objetos de la red usando un administrador de objetos de red basado en GUI. Entre los objetos que se necesitan para construir la directiva de seguridad, se deben incluir objetos de red, servicios, recursos, servidores, usuarios y tiempo.
2.- Con el administrador de usuario, definir un esquema de ID de usuario/contraseñas o autenticación con el Firewall.
3.- Usando el editor de base de reglas, crear la base de reglas para reflejar política de seguridad.
4.- Instalar la base de reglas en una puerta de enlace de Firewall.
5.- Probar la configuración.

Los fabricantes saben que la amenaza de fuentes o empleados internos está creciendo con mayor rapidez que las fuentes externas de amenazas. Como resultado, el perímetro del firewall se vuelve cada vez más un límite departamental y no empresarial. De la misma manera, el reto para el administrador de seguridad de controlar los firewalls se va haciendo mayor, por lo que ha esto, los fabricantes han respondido con las siguientes innovaciones:

1.- Compatibilidad con sistemas operativos diferentes a UNIX, como NT
2.- Nuevas estrategias de hardware, como aparatos de seguridad.
3.- Integración con componentes de VPN más completos.

Los diferentes tipos de firewalls ya fueron mencionados en capítulos anteriores, y siguiendo con nuestra posición, no mencionaremos algún producto en especifico.

4.1.9 Compatibilidad con el hardware y el software

Debemos tomar en cuenta que para utilizar tecnologías VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet. Además, tiene que ser capaz de interpretar los protocolos de red de la compañía al nivel 3 (el nivel de red) del modelo de la Organización internacional de normalización (ISO). Esto implica que su compañía debe estar al tanto del IP y saber que si los protocolos SNA o IPX están en ejecución, no se puede establecer una conexión directa a Internet, a menos que convierta primero SNA o IPX.

4.1.10 Interoperabilidad

Existen muchos productos de proveedores que ofrecen hardware, software cifrado y esquemas de autenticación para la tecnología VPN, por lo tanto, es muy difícil elegir alguno. Una consideración importante es donde encaja la VPN en su organización. ¿Busca una interoperabilidad usuario final, o piensa en una conectividad de VPN LAN a LAN?. Tomar esto en consideración nos ayudará a determinar los vendedores, fabricantes, proveedores de software e incluso los requisitos de consulta.

Asegúrese de buscar una certificación, por ejemplo se encuentra la Asociación Internacional de Seguridad en computación (ICSA), la cual es una compañía aseguradora de seguridad, establecida desde 1989, encargada de certificar productos de seguridad en computación. Y cuya meta es mejorar la interoperabilidad de los productos de seguridad y certificarlos adecuadamente. Los proveedores envían sus productos a ICSA para obtener una certificación.

4.1.11 Hardware para el Servidor

En realidad no existen límites al seleccionar la clase de hardware para un servidor Web, casi cualquier sistema de computación moderno equipado para redes, entre estos el software de red TCP/IP, pueden albergar un servidor Web. Los sistemas utilizados con más frecuencia son máquinas UNÍX, con servidores o estaciones de trabajo Sun, IBM, Digital y Hewlett-Packard. No resulta sorprendente que los servidores UNÍX tengan más de la mitad de participación en el mercado, ya que son multitareas con software avanzado TCP/IP integrado y están específicamente adaptados para ser servidores Web.

4.2 DISEÑO

4.2.1 Desarrollo del Diseño y Estructura de la Red

Para comenzar deberá decidir si desea emplear para la VPN la misma estructura de información de los canales de comunicación vigentes en su compañía. Una de las opciones para poner en marcha el levantamiento de la estructura de una VPN, consiste en agrupar los contenidos en temas y categorías de mayor importancia. Después se puede conjuntar información adicional por departamento, función y proyecto, o por cualquier otro orden previamente determinado. Es importante involucrar a más de una persona en la tarea de la agrupación de temas. Si sólo un individuo establece los criterios de agrupación, es probable que otros estén en desacuerdo. Si en cambio, aplica el método de equipos al agrupamiento de la información, tendrá la certeza de que estos conjuntos de temas responderán a las necesidades de los usuarios y serán comprensibles para un amplio público. A estas alturas se supone que su Intranet ya tiene un tipo de administración de la información, éstas son sólo algunas ideas para el mejor enlace de la información.

Seguiremos con la exposición del ejemplo visto en la página 87

La empresa no tiene acceso a Internet, esto es común pues todas las comunicaciones se basan en infraestructuras de redes, como tramas/ATM o líneas rentadas. La empresa quiere remplazarlas utilizando Internet. Cuenta con dos oficinas principales: Las oficinas centrales de Guadalajara, Jalisco; y una división de las oficinas centrales en Monterrey, Nuevo León. También tiene una sucursal de ventas en el Distrito Federal. Se ha decidido instalar una VPN basada en cortafuego que se ejecute en una plataforma UNIX sobre Internet.

El dispositivo de cortafuego/VPN se colocó en las oficinas de Monterrey y en las del D.F. Monterrey se eligió debido a la gran base de empleados , y el D.F. porque no tiene un enlace WAN interno y necesita una forma de acceder a las oficinas centrales. Puesto que la VPN estará disponible para todos los usuarios, esto ayudará a mantener un nivel bajo del tráfico en el enlace WAN interno.

Otra manera en la que se puede controlar el nivel de tráfico en el enlace WAN interno seria la de contar con dos conexiones a Internet entre las oficinas centrales. Habrá un PSI en las oficinas centrales de Guadalajara, con aquellos usuarios que utilicen esa conexión a Internet para el tráfico que no es de VPN, y una conexión a la división de las oficinas centrales de Monterrey para el tráfico VPN. Puesto que la VPN del D.F. es reciente y no tiene un enlace interno, deberá conseguir un espacio de dirección pública. La VPN está diseñada de tal forma que cuando los usuarios del D.F. ingresen a Internet, las funciones de las VPN sólo ocurrirán si ellos establecen comunicación con la red de Monterrey.

4.2.2 Situación actual de la red

Fig. 4.4 Diagrama de la Red

Las oficinas centrales corporativas tienen su dirección pública registrada como **220.220.220.0**; con el tiempo se utilizó esta dirección de red para sus máquinas internas. Como una medida de seguridad, no desean que su dirección de red sea enrutada por Internet, así que la compañía consiguió una dirección nueva y decidió utilizar un grupo de traducción de direcciones de red.

La división de las oficinas centrales, que tiene una base de empleados mucho mayor, utiliza la red 10 para direccionar a sus clientes internos. Al igual que muchas empresas, la dividió en subredes entre los distintos departamentos. Además, necesita que su PSI le proporcione una dirección pública enrutable. Utilizará un grupo de traducciones de direcciones de red. Se estimó que, a lo mucho, sólo 10,000 usuarios podrían usar la VPN. Aún con eso, sólo utiliza una dirección IP y las especificaciones técnicas del proveedor aseguran que la VPN manejará fácilmente a los 10,000 usuarios.

4.2.3 Mapa de la distribución de los equipos

La sucursal del D.F. también necesita utilizar una dirección IP pública válida, puesto que la política corporativa es ocultar la dirección real detrás de un cortafuego. Además, necesita configurar la traducción de direcciones de red y direccionar separadamente su red interna.

Se requiere que cuatro servidores tengan acceso a la VPN. Existen dos servidores en Guadalajara, con direcciones 220.220.220.10 y 220.220.220.11, a los cuales accederán los empleados internos que estén en viajes de negocios. Dos servidores en Monterrey, con direcciones 10.0.0.11 y 10.0.0.12, también serán parte de la VPN.

Ya que la empresa se preocupa por el tiempo improductivo, desea ser capaz de vigilar el tráfico web originado desde el interior de sus redes. Puesto que las dos oficinas centrales tendrán un número sustancial de usuarios conectándose a Internet, los problemas de desempeño pueden afectar al dispositivo de cortafuego/VPN debido a una gran cantidad de registros. Por lo tanto, se configurará un servidor proxy especial que tendrá la función de vigilar el tráfico web. Este proxy también funcionará como servidor RADIUS de autenticación de usuarios para los usuarios que ingresen a la VPN. Además, la sucursal tendrá alguna forma de vigilancia de tráfico. Puesto que la oficina es pequeña, en lugar de utilizar un servidor independiente, utilizará el mismo cortafuego para vigilar el tráfico.

La empresa quiere aplicar una política donde sólo los usuarios autorizados tengan permiso para ingresar a Internet. Sin embargo, lo que esto significa es que cada usuario individual debe estar registrado en la base de datos de usuarios RADIUS. Otra solución potencial podría ser que el servidor RADIUS consultara a una base de datos central para determinar el acceso. Ninguna de estas opciones es viable. Debido a que en la empresa existe tal combinación de plataformas distintas, no hay una base de datos central. Para que alguien pudiera ingresar y eliminar a los usuarios en el servidor RADIUS se requeriría un puesto de tiempo completo. Por lo tanto, aunque la empresa no utiliza un direccionamiento IP dinámico, aún puede vigilar el tráfico, y los registros señalarán hacia la máquina que origina la entrada dentro de la red.

Además, esta empresa definió el tipo de tráfico que está permitido que fluya hacia la organización: tráfico DNS y SMTP[13]. También decidió configurar los servidores DNS y SMTP por separado en una zona DMZ, eliminando asi el tráfico directo al interior de la organización. Estos son los requisitos impuestos por la empresa. Al estudiarlos, se puede establecer una configuración como la que se muestra en la figura 4.5

[13] Protocolo simple de Transferencia de correspondencia

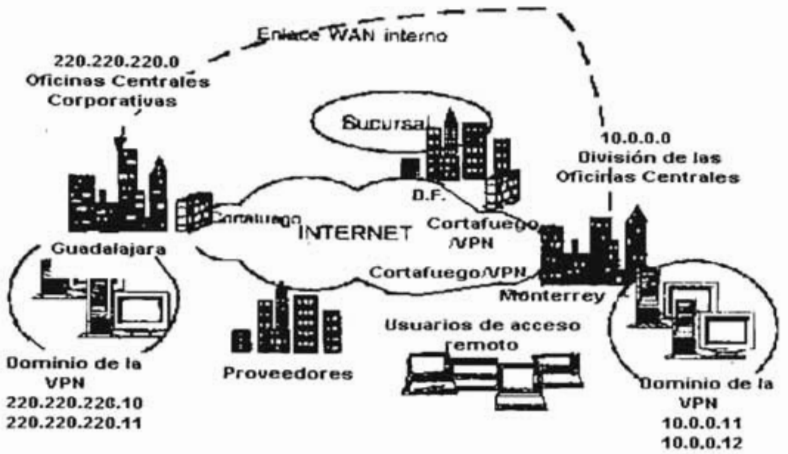


Fig. 4.5 Configuración con 2 Dispositivos de Cortafuego/VPN

Esta configuración establece dos dispositivos de cortafuego/VPN: uno en la sucursal del D.F. y el otro en la división de las oficinas centrales de Monterrey. Además, cualquier usuario remoto que necesite acceso a la VPN deberá cargar el software para crear el túnel hacia la VPN. El proveedor de VPN elegido incluye software para que los equipos portátiles puedan hacer esto. Sin embargo, puesto que el PSI local no puede ayudar a los usuarios finales una vez que éstos han establecido una conexión a Internet, esta responsabilidad recaerá en el departamento de soporte técnico de la empresa. La empresa asume que el departamento técnico también manejará esta tecnología nueva. Además, el dominio de la VPN se definió con servidores localizados en ambas oficinas centrales.

4.2.4 Estructuración del contenido

Llegado a este punto, ya habrá agrupado los temas de su VPN en grandes categorías. Ahora tendrá que reestructurar (ordenar) la información en tal forma que resulte natural para los usuarios. Son tres los modelos básicos de información que puede emplear para estructurar el contenido: Lineal, jerárquico y no lineal. No profundizaremos en esta parte, eso lo dejamos al lector.

Existen muchísimas herramientas para la organización del contenido de la red. Durante el proceso de desarrollo de la red se modificarán muchas veces la disposición y organización del contenido de la misma. Existen varias aplicaciones para diagramas de flujo que actualizan en forma automática un diagrama de flujo al hacer un cambio en el esquema del proyecto. También algunas herramientas de autoria del web ofrecen herramientas para diagramas de flujo y organigramas que pueden serle útiles.

El siguiente paso es definir el diseño, la funcionalidad e interfaz de usuario de la VPN. Desde el comienzo se debe adecuar el diseño a la imagen ya existente en la organización, usando para ello los materiales de comercialización disponibles, podrá incluir elementos como imágenes, logotipos e iconos empresariales, así como diseños similares, para infundirle al contenido de su red interna una apariencia familiar. Un story board sirve para describir el contenido, imágenes y ligas entre las páginas bajo la forma de un boceto. Se puede hacer uso de software como Microsoft Power Point u otro programa de presentaciones similar para elaborar su story board y ejemplos de sus páginas WEB. También es buena idea someter a prueba la interfaz del diseño para garantizar los iconos, botones y herramientas de navegación para que resulten lógicos y comprensibles para el usuario.

Estas son sólo ideas para lograr una mejor agrupación de la información, se supone que a estas alturas esto ya existe y usted sólo tiene que implantar la VPN.

4.2.5 Selección de la información a la que se tendrá acceso

Nuestra solución de VPN de Extranet conectará usuarios internos y externos, es decir, empleados internos, empleados remotos, proveedores, y clientes. Es necesario que en nuestra política de seguridad tengamos bien delimitados y ubicados a nuestros usuarios, pues no a todos vamos a permitirles la entrada a nuestros servidores, para esto se crea la política de seguridad, y con ello tengamos un conocimiento perfecto de quienes se conectan y hasta donde pueden llegar en la búsqueda de información.

4.3 IMPLANTACIÓN DE VPN

4.3.1 Inventario del equipo existente

Sin importar la tecnología de acceso, una Extranet necesita una lista sustancial de elementos físicos. Tal vez no todos sean necesarios, pero cualquiera es útil, mencionaremos algunos dispositivos físicos con los que deberá contar nuestra Extranet, en este caso nuestra VPN.

- *Una distribución universal de TCP/IP.*
- *Navegador Web.*
- *Servidor Web.*
- *Servidor de acceso remoto .*
- *Software cliente para uso telefónico.*
- *Enrutador*
- *Conexión de línea arrendada.*
- *Seguridad de firewall.*

Hasta este punto los elementos anteriores son los típicos en una Extranet. Sin embargo, como hemos mencionado en este documento, que debido a la tecnología necesaria para realizar un implante de esta naturaleza y haciendo un estudio concienzudo de los beneficios que se obtienen, implantando una Red Privada Virtual como medio para llevar a cabo una comunicación de Extranet, recordemos el concepto de VPN.

Las VPNs ofrecen flexibilidad, escalabilidad y ahorro de costos importantes cuando las empresas extienden su red para incluir clientes relevantes, socios comerciales estratégicos y empleados remotos. Además dada la facilidad de implantación y accesibilidad, creemos que es la mejor opción para lograr nuestro proyecto. Por lo que como parte muy importante agregamos a nuestra Extranet los siguientes elementos :

- *Software y Hardware de VPN.- En cada uno de los sitios a conectar.*
- *Tecnologías de VPN.- Encriptación, autenticación y técnicas de validación.*
- *Enrutadores Internos y Externos*
- *Conmutadores*

Asimismo, debemos tomar en cuenta que no existe una Extranet especifica para solo instalar y usar, sino por el contrario, el diseño de dicha tecnología es según las necesidades de cada empresa, de la cual se debe atender primeramente los objetivos empresariales importantes, así como identificar los componentes que serán integrados en la solución, incluyéndose en este ciclo de vida de desarrollo de la Extranet, la definición detallada de los requisitos, análisis, diseño y prototipo antes de su construcción, que es lo que pretendemos realizar en este proyecto.

4.3.2 Componentes que forman una VPN

Las VPN no solo consisten en hardware y software, sino que además requieren otro conjunto de componentes, los cuales son requisitos que garantizan que la VPN sea segura, esté disponible y sea fácil de mantener. Los requisitos actuales caen dentro de un rango de atributos que una organización debe considerar cuando implanta o diseña una VPN.

Disponibilidad.- Se aplica tanto al tiempo de actualización como al de acceso. No basta con que el usuario tenga autorización para acceder a los servidores corporativos las 24 horas del día los 7 días de la semana, si no puede conectarse debido a problemas en la red. Lamentablemente muchos de estos problemas están fuera de su control y a veces incluso de su PSI local.

Control.- Algunos ejecutivos temen que si alguien más administra y controla la VPN de su compañía, hay una mayor posibilidad de brechas de seguridad. En realidad, los servicios administrados de VPN pueden ser de gran ayuda para la compañía debido a la capacitación, la experiencia, supervisión meticulosa y funciones de alerta que ofrecen algunos proveedores de servicios administrados. Entonces nos preguntamos ¿Cuánto desea invertir en capacitación, certificación y equipo para que el departamento de soporte técnico acelere la tecnología y las cuestiones de seguridad de las VPN?

Compatibilidad.- Para utilizar tecnologías VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet. Además, debe ser capaz de interpretar los protocolos de red de la compañía al nivel 3 (el nivel de red) del modelo de la Organización internacional de normalización (ISO). Asimismo, si va a utilizar Internet, debe usar la convención de asignación de direcciones que utiliza Internet (basada en la estructura del direccionamiento del protocolo Internet).

Seguridad.- La seguridad lo es todo en una VPN, nunca será suficiente hacer hincapié en ello. Una VPN no es la red privada de una compañía, debemos tener muy en cuenta que otros pueden llegar a interceptar, recolectar y analizar los datos.

Confiabilidad.- Cuando una compañía decide instalar el producto VPN de un PSI, está a merced del PSI. Una frustración que sienten los ejecutivos es que cuando se cae la red, no tienen el control para supervisar o arreglar la situación.

Autenticación de datos y usuarios.- La autenticación de datos reafirma que el mensaje ha sido enviado completamente y que no ha sido alterado en ninguna forma. La autenticación de usuario es un proceso que permite que el usuario tenga acceso a la red.

Sobrecarga de tráfico.- En todo tipo de tecnologías existen sacrificios: velocidad contra desempeño, seguridad contra flexibilidad. Si la VPN encapsula cada paquete, puede incrementar el tamaño del paquete y por lo tanto afectar la utilización del ancho de banda. Un buen servicio de VPN le dará la opción de especificar qué tipo de datos se cifrarán que tipo de datos se autenticarán y que tipo de datos puede fluir libremente sin modificarse.

Mantenimiento.- Debe decidir qué tipo de tecnología y qué tipo de soporte necesita su compañía ¿Usará el servicio de VPN administrada por un PSI o la construirá usted mismo con los propios recursos de su compañía? Si decide implantar usted mismo la VPN, ¿Cuenta con el equipo de seguridad? ¿Puede responsabilizarse su departamento técnico de los aspectos de seguridad?. La actualización en la seguridad debe ser tan preocupante como lo es la revisión del software en busca de virus: sólo es bueno hasta el último virus conocido.

Sin repudio.- Es el proceso de identificar positivamente al emisor de tal manera que no pueda negarlo. Esto tiene enormes complicaciones para los proveedores, mayoristas, vendedores y para los principales socios comerciales. El comercio electrónico, los documentos legales y las negociaciones financieras se basan en saber quién realiza el pedido. Si existe, aunque sea un poco de incertidumbre, una compañía no puede garantizar quien realizó el pedido. Para que el comercio electrónico en Internet se vuelva una opción viable, debe existir un proceso *sin repudio*.

Servicio de ayuda para resolver problemas
Su empresa tendrá que establecer algún tipo de función de servicio de ayuda. El software para establecimiento de túneles de VPN no es el mismo que el software de red empleado para establecer una conexión PPP a un PSI. Los usuarios finales tendrán problemas y muchos PSI no están equipados para manejarlos.

4.3.3 Obtención y asignación de un espacio de dirección IP

Una vez que el modelo ha sido aprobado por la administración superior, las oficinas centrales y la sucursal tienen que contactar a sus PSI locales para obtener un espacio de dirección. Cuando se haya asignado la dirección IP, el personal técnico asignará el espacio de dirección pública a los distintos dispositivos de todos los departamentos. Para nuestro caso, los PSI asignaron las siguientes direcciones IP de red a las oficinas:

Oficinas centrales corporativas (Guadalajara)	235.235.235.0
División de las oficinas centrales (Monterrey)	230.230.230.0
Sucursal (D.F.)	247.247.247.0

Por lo general, el PSI local se encarga del direccionamiento IP entre el enlace serial del enrutador externo (llamado comúnmente SO) y su conexión. En la división de las oficinas centrales, se configuró el cortafuego/VPN y sus dispositivos asociados.

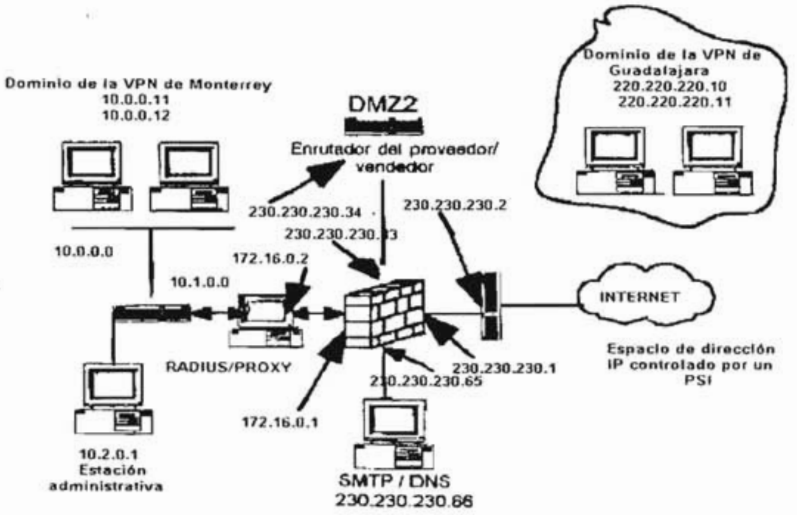


Fig. 4.6 Cortafuego/VPN de Monterrey

Comenzando con la división de las oficinas centrales, se tomó el espacio de dirección que proporcionó el PSI y se subdividió con la máscara de red 255.255.255.224. Esta máscara de red toma a la red 230.230.230.0 y la divide en 8 redes, cada una de las cuales cuenta con 30 anfitriones utilizables. Utilizable significa el direccionamiento IP actual que está disponible para las máquinas. Cualquier programa de computadora que realice cálculos de subredes revelará que la red 230.230.230.0 con una máscara de red 255.255.255.224 contiene 8 redes con 32 anfitriones cada una. Sin embargo, la primera dirección IP de esa red (230.230.230.0) es para el número de la red, mientras que la última dirección IP disponible (230.230.230.31), es para el número de transmisión. Por lo tanto, las direcciones IP que se pueden utilizar son n-2, donde n es el número total de direcciones IP disponibles por la red. Es importante que recuerde esto en caso de que su PSI le otorgue un grupo pequeño de direcciones. En este ejemplo, el PSI asignó una dirección clase C completa, con un total de 255 anfitriones o direcciones IP. Si su PSI le asigna una subred clase C, debe asegurarse de tener algunas direcciones válidas para los otros servidores en los que quiera direcciones IP válidas. Una vez que subdividimos a la red 230.230.230.0, se asignan direcciones IP con los siguientes puntos:

4.3.3.1 Los enlaces externos

Dispositivo de cortafuego/VPN : 230.230.230.1
Enrutador Externo: 230.230.230.2
Las direcciones IP están en la red 230.230.230.0, y la dirección de transmisión es 230.230.230.31

4.3.3.2 Los enlaces DMZ[14](1)

Interfaz de cortafuego/VPN de la DMZ1: 230.230.230.65
Servidor SMTP/DNS: 230.230.230.66
Las direcciones están en la red 230.230.230.64, y la dirección de transmisión es 230.230.230.91

4.3.3.3 La DMZ(2) o EDI/enlaces de comercio electrónico

Cortafuego/VPN de la DMZ2: 230.230.230.33
Enrutador DMZ2: 230.230.230.34
Las direcciones están en la red 230.230.230.32; y la dirección de transmisión es 230.230.230.63

4.3.3.4 Las interfaces internas

Interfaz Interna del cortafuego/VPN: 172.16.0.1
Servidor proxy (enrutador): 172.16.0.2

Las direcciones están en la red 172.16.0.0, y la dirección de transmisión es 172.16.255.255

Ahora, ¿Cuál es la razón para establecer este esquema de direccionamiento?.

4.3.4 Motivo para subdividir la red 230

El PSI asignó a la división de Monterrey una dirección de red clase C (230.230.230.0) que contiene 255 IP. Al subdividir esta red en una máscara de red 255.255.255.224 se tendrán ocho redes adicionales. El sacrificio se encuentra en el espacio de direcciones IP utilizable; ahora se cuenta con 30 direcciones IP utilizables por red. Si piensa en dónde se utiliza el espacio de dirección IP, quizá se dé cuenta que no se necesita un grupo grande de direcciones IP para cualquiera de las subredes. En muchas empresas sólo hay dos, tres, quizá cuatro dispositivos cerca del punto de conexión a Internet. Lo mismo sucede en la configuración de una VPN, no necesita muchas. Incluso si configura un grupo de servidores y tiene 20 servidores en esa subred, aún tendrá 30 direcciones IP utilizables. Si examina el razonamiento detrás del esquema de direccionamiento, verá que esto es verdad. Como nota final, de cualquier forma siempre puede utilizar un grupo NAT[15] y ocultar todos sus servidores detrás de una dirección IP.

[14] Por medio de una política de seguridad todo el tráfico será dirigido a la zona DMZ y de ahí sólo el tráfico necesario se redirigirá a las redes internas. Permite también que el tráfico entrante se revise primero de virus si es que se coloca un software antivirus.

[15] Traducción de direcciones de red.- Ofrece la posibilidad de tener acceso a Internet detrás de una dirección IP pública válida. Si su compañía tiene 10.000 nodos, puede ocultarlos detrás de una dirección IP válida.

4.3.4.1 Enlaces externos

Como se muestra en la figura 4.6, existe un enlace sencillo entre la interfaz externa del cortafuego/VPN y el enrutador externo. Por lo tanto se está asignando sólo dos direcciones IP para toda la red. Podría ser un desperdicio de espacio de direcciones IP tener toda esta clase C sólo en ese enlace. De hecho, esta configuración es un desperdicio de algunas direcciones; en este ejemplo hay 28 direcciones IP desperdiciadas.

4.3.4.2 Enlace de la zona DMZ1

Puesto que se utiliza la subred 230 en el enlace externo, se puede tomar la subred 230.230.230.64 y asignarla a la red DMZ1. Con esto se consiguen 30 direcciones IP anfitrionas, lo cuál podría ser más que suficiente para cualquier necesidad corporativa en la zona DMZ. Muchas empresas tienen DNS, un servidor web y quizá un servidor de correo o un servidor de FTP. Probablemente muchos de estos servicios se encuentren en la misma máquina; en este ejemplo se asigna la dirección 230.230.230.65 a la interfaz de cortafuego/VPN, y la dirección 230.230.230.66 al servidor SMTP/DNS. Así que de las 30 direcciones utilizables, sólo se han utilizado dos, lo cual deja mucho espacio para un crecimiento posterior.

4.3.4.3 DMZ2 o enlaces para comercio electrónico

Algunas empresas quieren restringir a sus clientes/proveedores/vendedores a sus propias redes. Este enlace DMZ2 es un lugar apropiado para un servidor de Extranet, o para cualquier actividad de comercio electrónico. En este tipo de configuración se tiene la flexibilidad de segmentar el tráfico no interno, verificar la autenticación externa y revisar las políticas mediante las reglas del cortafuego. En el dispositivo de cortafuego/VPN, pueden establecerse reglas que sólo admitan a ciertos usuarios y que los restrinjan a ciertas redes.

4.3.4.4 Interfaces internas

El direccionamiento de interfaces internas es sencillo, sólo se necesita utilizar una dirección IP disponible. Sin embargo, existe un problema mayor que ocurre con el enrutamiento de redes internas.

Los equipos portátiles no requieren una configuración IP, recibirán su dirección IP por parte del PSI local cuando se conecten.

4.3.5 Implantación de una buena política de seguridad

La política de reglas puede ir de la mano con la política corporativa. Primero, la regla que debe intentar aplicar (intentar, porque habrá situaciones que no se pueden evitar) es la de no tener tráfico externo que llegue directamente a su red.

Existe una forma tradicional para implantar una zona DMZ. Cada bit de tráfico llega a la zona DMZ y de ahí a la red. Por lo general existe un dispositivo entre el enrutador externo y la red privada. Su función es proteger a los anfitriones privados. Para implantar este tipo de seguridad, se utilizan listas de acceso en los enrutadores y servicios proxy, pero presentan ciertos problemas.

La siguiente ilustración muestra el modelo de configuración de una zona DMZ.

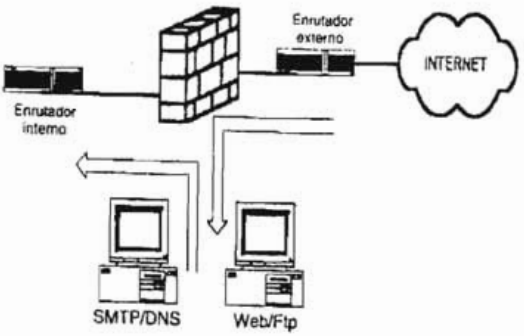


Fig. 4.7 Modelo de configuración de una zona DMZ

El enrutador interno se conecta a un puerto del cortafuego, el otro puerto del cortafuego se conecta al enrutador externo y el puerto serial del enrutador externo se conecta al PSI.

Esta configuración asegura que todo el tráfico sólo entra a la DMZ y después el dispositivo de la DMZ reenvía el tráfico apropiado a la red interna. Por ejemplo, el tráfico de correo se envía al servidor de correo en la DMZ y cuando es apropiado, el servidor de correo reenvía ese tráfico a la red interna. Decimos que es apropiado porque con esta configuración puede ajustarse el servidor de correo en la DMZ para que rechace o deseche cualquier correo que parezca ofensivo.

Si puede hacerlo, no debe permitir que el tráfico de Internet llegue directamente a la red. A continuación se describe un conjunto de reglas que se pueden aplicar al dispositivo. Estas reglas se describen en un formato que puede implantarse dentro de un cortafuego. Los términos aplicados son los siguientes:

- Origen. El lugar de dónde llega el tráfico. No es un origen absoluto, pero así lo ve el cortafuego. Por lo tanto, en un paquete de datos, si el sistema es responsable del tráfico DNS, puede verse como el origen de la transmisión. El siguiente paquete puede verse como el destino del tráfico. Si logra imaginar este flujo de datos, no tendrá problemas.

- Destino. El lugar a dónde se dirige el tráfico, lo opuesto al origen, según lo ve el cortafuego. Observe estos dos ejemplo donde ⟶ representa la dirección del flujo de datos:

  Servidor interno ⟶ *Envío de tráfico DNS* ⟶ *Cortafuego* ⟶ *Internet*
  - El cortafuego ve al servidor interno como el origen del tráfico.

  Servidor interno ⟶ *Recepción de tráfico DNS* ⟶ *Cortafuego* ⟶ *Internet*
  - El cortafuego ve al servidor interno como el destino del tráfico.

- Servicio. Los servicios que se permiten (por ejemplo, http, SMTP, DNS). Se implantan los tipos específicos de tráfico que tienen permiso para pasar. La palabra ANY implica todos.

- Acción. Lo que se debe hacer con el tráfico. Existen varias opciones, por ejemplo aceptar, descartar y rechazar el tráfico. Cuando estudie la política de reglas, verá a dónde pertenecen estas opciones.

- Registro. Registro del tráfico. Por lo general hay muchas opciones de registro, como corto y largo, que proporcionan el número total de campos registrados, o alertas, lo cual implica que cuando una regla especifica se activa, se envía una alerta o un mensaje de correo electrónico a un anfitrión o a un administrador específico.

4.3.6 Implantación de la administración de tráfico

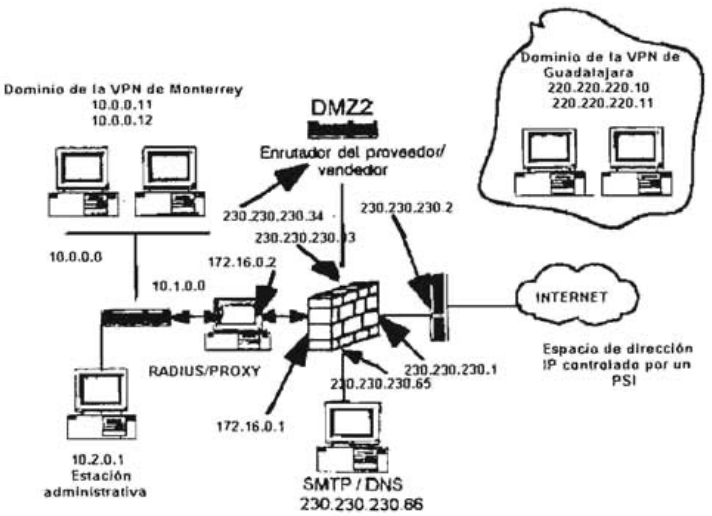


Fig. 4.8 Cortafuego/VPN de Monterrey

En la figura 4.8 se implantó un espacio de dirección IP al cortafuego/VPN de Monterrey y se configuró una estación de administración en la dirección IP 10.2.0.1. Esta puede ser un servidor de administración dedicado o la estación de trabajo del administrador de la red.

Es necesario tener un acceso de banda al dispositivo de cortafuego/VPN, y es una buena idea ponerlo como primera regla. Además, necesita una regla similar en el dispositivo de cortafuego/VPN de la sucursal, de modo que pueda administrar remotamente este dispositivo.

La primera regla permite que la estación administrativa (10.2.0.1) se conecte al dispositivo para administrarlo. También se permiten todos los servicios disponibles y se acepta (Accept) la acción.

La segunda regla descarta todo el tráfico dirigido a la dirección IP del dispositivo de cortafuego. Esta es la razón por la cuál se consideran como primeras reglas: cualquier tráfico dirigido específicamente al dispositivo de cortafuego/VPN (por ejemplo, el tráfico que no es VPN) debe registrarse y desecharse. En realidad el tráfico VPN se dirige al cortafuego, pero éste es un caso especial. La acción de descartar (Drop) es preferible, puesto que es cautelosa por naturaleza. Si acepta el rechazo (Reject), se enviará un mensaje de regreso al emisor. Aunque una opción como ésta, puede ayudar a legitimar la solución de problemas, asimismo sirve de indicación para los piratas potenciales, pues señala que ahí hay algo y no se les permite la entrada.

Las primeras dos reglas se parecen a esto:

Regla	Origen	Destino	Servicio	Acción	Registro
1	10.2.0.1	172.16.0.1	ANY	Accept	Short
2	ANY	172.16.0.1	ANY	Drop	Long

4.3.7 Aspectos de la implantación de SMTP y DNS

Las siguientes reglas establecen que sólo el tráfico SMTP y el DNS tienen permiso para pasar a través de la zona DMZ desde cualquier dirección. Además, la regla es restrictiva por naturaleza, lo cuál significa que:

1.- Sólo puede pasar tráfico SMTP o DNS a la DMZ.
2.- La dirección IP de destino del tráfico SMTP o DNS debe ser 230.230.230.66

Con esto, aunque se restrinja el tráfico, aún se permiten los servicio necesarios para trabajar y se agrega seguridad a la red. Primero es necesario asegurarse de que sólo el tráfico DNS o SMTP tienen permiso para pasar, y por lo tanto nadie tendrá la oportunidad de utilizar otro servicio que rodee la zona DMZ. Segundo, se les restringe a esa dirección IP sin permitir que un individuo comprometa otra máquina en ese puerto.

Las reglas se parecen a esto:

3	ANY	230.230.230.66	SMTP/DNS	Accept	Long
4	230.230.230.66	ANY	SMTP/DNS	Accept	Long

Si tiene un anfitrión interno SMTP/DNS (por ejemplo, una máquina con la dirección 10.2.0.2), puede imponer las siguientes restricciones posteriores a las reglas 3 y 4:

3	10.2.0.2	230.230.230.66	SMTP/DNS	Accept	YES
4	X 10.0.0.0	230.230.230.66	SMTP/DNS	Accept	YES
5	230.230.230.66	ANY	SMTP/DNS	Accept	YES

Las reglas 3 y 5 dirigen el tráfico en direcciones específicas.

Desde la dirección interna, sólo el servidor interno en la dirección IP 10.2.0.2 tiene permiso para enviar el tráfico SMTP y DNS al servidor de la zona DMZ. Cuando provenga de Internet, el cortafuego desechará cualquier tráfico que no sea dirigido específicamente a la DMZ. El **X** 10.0.0.0 es el operador de negación. Esto significa que cualquiera que no pertenezca ala red 10.0.0.0 (cualquiera que no sea de la red interna) puede enviar tráfico SMTP y DNS, pero sólo al servidor DMZ.

4.3. 8 Implantación de la autenticación

Al implantar la autenticación se involucran dos pasos. El primer paso es agregar las reglas apropiadas al cortafuego para permitir el acceso a la red. Después, debe agregar un grupo de usuarios a ese objeto de red para que el dispositivo vea el tráfico de red y le aplique las reglas de autenticación de usuarios. (Este proceso consiste en una sola regla, pero aquí se dividió en dos pasos para hacerla más comprensible). El servidor proxy/RADIUS realiza dos funciones: vigila todo el tráfico interno para Internet de modo que pueda registrarlo, y sirve como un dispositivo de autenticación tanto para el tráfico de entrada como para el de salida. Entonces ¿Por qué se necesita un servidor proxy para realizar los registros si se tiene la combinación de cortafuego/VPN?
Esta es una buena pregunta que contempla dos aspectos:

1. *Desempeño.*- Mientras que en este ejemplo se activó el registro, quizá no sea necesario activarlo para todo el tráfico. De nuevo, desde la perspectiva del desempeño, mientras más reglas se tengan, se obliga más al dispositivo de cortafuego/VPN a examinar cada paquete y enviarlo a otro lugar, ya sea a un archivo local o a un servidor independiente. Revisar todos los paquetes de ese dispositivo no necesariamente es una buena idea. Por esta razón se introduce el servidor proxy.

2. *Niveles de registro.*- Aunque el dispositivo tenga la capacidad para crear registros, no todos son iguales. Casi todos los registro soportan el registro de las direcciones IP de origen y de destino, pero algunos registros no soportan la autenticación de usuarios para direcciones IP. Esto significa que si instala la autenticación de usuarios en el dispositivo de cortafuego/VPN, éste obligará a que los usuarios se autentiquen.

Sin embargo, una vez que el usuario se autentica, no hay más registros con ese nombre, lo cuál equivale a que usted sabrá que un usuario en particular ha sido autenticado en ese momento, pero no tendrá registro alguno de los sitios que él visitó.

4.3.8.1 Tráfico Interno de usuarios autenticados

Cuando se implanta la autenticación de usuarios se dispone de varias opciones; puede utilizar el mismo dispositivo de cortafuego/VPN, un servidor proxy o un servidor RADIUS. Primero establezca las reglas para permitir el acceso a la red y después agregue un grupo de usuarios a ese objeto de la red para obligar a que los usuarios se autentiquen.

El siguiente ejemplo utiliza la implantación de un servidor RADIUS, se muestra el flujo de tráfico cuando un usuario interno intenta tener acceso a Internet:

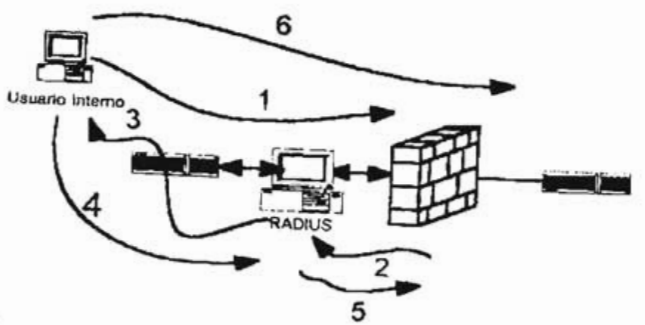


Fig. 4.9 Implantación de un Servidor RADIUS

1.- Un usuario envía un paquete de datos, e intenta obtener acceso a Internet.
2.- El dispositivo de cortafuego/VPN ha sido configurado para utilizar la autenticación RADIUS. Primero revisa la red de donde proviene el paquete de datos. Si la red tiene permisos, entonces revisa la autenticación del usuario. Envía una solicitud al servidor RADIUS y verifica si el usuario tiene permiso para acceder a Internet.
3.- El servidor RADIUS le solicita al usuario interno su nombre de usuario y su contraseña.

4.- El usuario introduce la combinación adecuada de nombre de usuario y contraseña.
5.- El servidor RADIUS revisa los permisos e informa al dispositivo de cortafuego/VPN que el usuario tiene autorización.
6.- El usuario puede salir de acuerdo con la política basada en reglas.

4.3.9 La regla Drop All

Esta regla significa que el dispositivo descarta cualquier tráfico que no está permitido explícitamente por reglas previas. Por lo general, puede utilizar DRP o REJECT, pero recuerde, REJECT envía un mensaje al emisor, así que sabrá que ahí hay un dispositivo. Si esa persona es un pirata informático, ahora sabe que en ese lugar hay algo que merece más atención. DROP sólo se deshace del paquete sin devolver un mensaje de respuesta; la persona nunca recibirá un mensaje del dispositivo con la(s) dirección(es) detrás de él. Muchos dispositivos descartarán implícitamente los paquetes a los que no se les haya permitido entrar en forma tácita. Aunque usted puede pensar, si de todas formas desechan los paquetes, entonces ¿porque los registran?. Si no instala esta regla e instala YES como la opción de registro, no podrá registrar el tráfico.

La regla Drop All es la siguiente:

9	ANY	ANY	ANY	DROP	YES

4.3.10 Implantación de la regla VPN

Ahora, antes de implantar la regla VPN, se debe configurar el dispositivo de cortafuego/VPN. Es necesario indicarle al cortafuego el tipo de algoritmo de cifrado que quiere utilizar, el tipo de sistemas de administración de claves y cuáles son las autoridades emisoras de certificados que quiere emplear. Una vez que haya decidido esto, se aplicará la regla para el tráfico de la VPN, y el dispositivo de cortafuego/VPN aplicará los algoritmos de cifrado que haya establecido. Aquí es donde se utilizan términos como PPTP, L2TP e IPSec, y se decide el tipo de implantación para su empresa. En el ejemplo se considera que el dispositivo de cortafuego/VPN utilizará la seguridad IPSec, la cuál actúa como su propia autoridad emisora de certificados y emplea ISAKMP/OAKLEY (IKE)[16] como mecanismo de intercambio de claves.

Los ajustes en las configuraciones de las implantaciones son distintos con cada fabricante, pero es imprescindible implantar los siguientes aspectos:

[16] Intercambio de claves de Internet.- Protocolo de administración de claves utilizado con IPSec.

- Defina el esquema de cifrado IPSec en el dispositivo de cortafuego/VPN. En este ejemplo, se establece que IPSec utilizará el cifrado DES. Cada configuración en la VPN deberá (o debería) tener la capacidad para crear IPSec utilizando el cifrado DES. Si lo desea puede elegir otros esquemas de cifrado, sólo recuerde, necesitará interoperabilidad a lo largo de todos los dispositivo que quieran utilizar la VPN.

- Cree un índice de parámetros de seguridad (SPI). La Asociación de Seguridad (SA) utiliza el SPI, y cada terminal de los socios de la VPN utiliza esta SA. El destino es responsable de crear un SPI único. En algunas configuraciones, es posible crear un SPI si se emplea entre dos dispositivos de cortafuego/VPN. EL SPI es un número hexadecimal de 32 bits, por ejemplo, 0 X 102, 0 x 103.

- Haga que el dispositivo de cortafuego/VPN actúe como su propia autoridad emisora de certificados, mientras sea una máquina confiable. Si siente que necesita otra, debe indicarlo.

- Defina a IKE como su mecanismo de intercambio de claves. Muchos tienen IPSec manual, SKIP[17] o sus propios mecanismo de administración para intercambio de claves.

- Defina un dominio de VPN en el cortafuego/VPN para una división. El dominio consiste en los anfitriones o redes a los cuales usted desea otorgar acceso. En este caso, son los cuatro servidores mencionados anteriormente. El dispositivo de cortafuego/VPN de la sucursal esta configurado de la misma manera que el cortafuego/VPN de Monterrey, con excepción del dominio de VPN. La razón es que entre las oficinas de Monterrey y del D.F., todo el tráfico está cifrado.

4.3.11 VPN de la sucursal

Una vez que los dispositivos de la VPN están configurados para utilizar el cifrado apropiado y la configuración de administración de claves, es necesario instalar las reglas VPN. Así, lo que se establecerá es una conexión al otro cortafuego/VPN en la sucursal, permitiendo con ello que los usuarios remotos tengan conectividad con la VPN.

El primer paso al crear una VPN de LAN a LAN es intercambiar las claves entre cada dispositivo de cortafuego/VPN, como se muestra en la figura 4.10

[17] Protocolo Internet de clave sencilla.- asegura la sesión de comunicaciones punto a punto al cifrar todo el trafico con una clave secreta compartida.

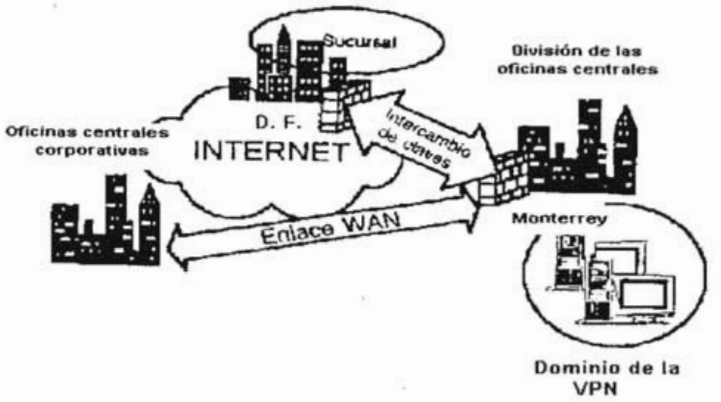


Fig. 4.10 Intercambio de Claves

Esto realiza el intercambio de claves entre los sitios y establece un túnel que se empleará con base en la demanda, que para este caso es un túnel basado en IPSec (DES). Cuando un usuario quiera conectarse a la oficina de la división desde la sucursal, el tráfico saldrá cifrado del dispositivo VPN de la sucursal, y al llegar a la división de las oficinas centrales, será descifrado. Los dispositivos de cortafuego/VPN cambian las claves periódicamente.
La regla de la VPN implantada en el dispositivo VPN del D.F. es la siguiente:

Regla	Origen	Destino	Servicio	Acción	Registro
#	172.17.0.0	230.230.230.1	HTTP	Encrypt	YES

La dirección de red 172.17.0.0 fue la red IP que se utilizó para direccionar a los anfitriones internos del D.F.. La dirección IP 230.230.230.1 es la dirección externa del dispositivo de cortafuego/VPN de Monterrey. Cuando un usuario abandona el cortafuego/VPN del D.F. y el destino es 230.230.230.1, que es la red de Monterrey, el cortafuego/VPN del D.F. lo cifra de acuerdo con la política de cifrado que se estableció en ese dispositivo. El cortafuego/VPN de la división verá que llega tráfico desde la dirección IP (247.247.247.1) y después lo descifrará. Recuerde que el único servicio garantizado es http.

La regla VPN implantada en el dispositivo VPN de Monterrey es la siguiente:

#	Ch_usuarios@247.247.247.1	230.230.230.1	HTTP	Encrypt	YES

El dispositivo de cortafuego/VPN de Monterrey verá llegar el tráfico de la dirección IP 247.247.247.1. Este ya ha sido configurado con las claves del dispositivo de cortafuego/VPN del D.F.. El grupo de usuarios es sólo un grupo en el servidor RADIUS. Descifrará los datos y obligará a que los usuarios se autentiquen en el servidor RADIUS. Revisará las autenticaciones, y una vez que los usuarios hayan sido autenticados, sólo se les permitirá el acceso http.

Nota sobre seguridad: En algunos dispositivos VPN, sólo se puede instalar un dominio de VPN. Es decir, si desea que algunos usuarios tengan acceso a un servidor y otros a otro, es necesario incluirlos a todos en el dominio de la VPN.

4.3.12 VPN de usuarios remotos

Casi hemos terminado de implantar una VPN en los requisitos de la compañía y se ha establecido una topología que lo permita. Lo último que falta por hacer, es permitir que los usuarios remotos tengan la capacidad de establecer una VPN con la red de Monterrey.

Estos pasos son los siguientes:

1.- Instalar el software VPN de un fabricante en los equipos portátiles remotos.
2.- Configurar el software.
3.- Añadir los usuarios a la base de datos.
4.- Instalar una política de reglas que permita hacer esto.

La figura 4.11 ilustra una sesión con un cliente. El software VPN instalado en el equipo portátil se configura con la dirección IP externa del dispositivo VPN, que para este caso es 230.230.230.1. El software VPN se inicia, y dependiendo de la configuración, el equipo portátil intercambia claves de seguridad con el dispositivo VPN. Durante la comunicación, se le indica al equipo portátil que el dominio de VPN consiste en los servidores 10.0.0.11, 10.0.0.12, 220.220.220.10 y 220.220.220.11.

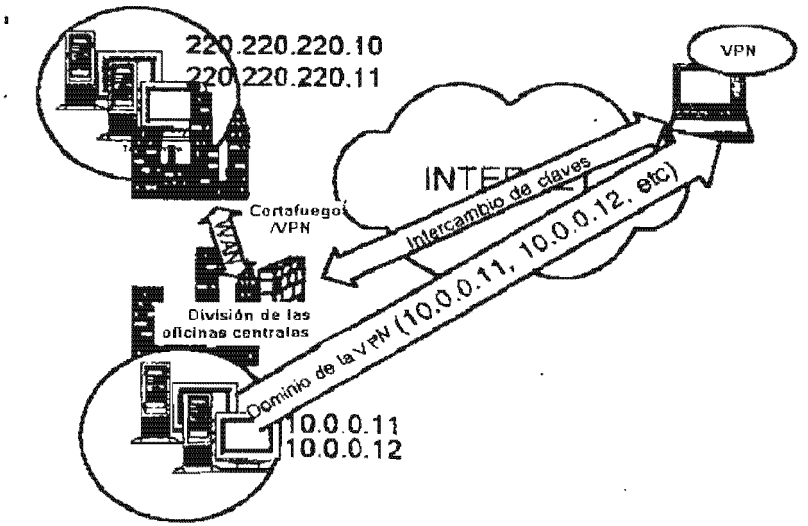


Fig. 4.11 Sesión con un Cliente

¿Cómo funciona?.- Durante una operación normal, el equipo portátil tiene acceso a diferentes sitios a Internet y no pasa nada con el software VPN. Sin embargo, si ahora el equipo portátil intenta ir a **http://10.0.0.11**. El software VPN sabe que la dirección IP 10.0.0.11 es parte del dominio de VPN que se encuentra en la división. Entonces, el software cifra el paquete y posiblemente lo encapsula. Después lo coloca en la dirección IP del dispositivo de cortafuego/VPN de la división (230.230.230.1) y lo envía. Cuando la división lo recibe, el dispositivo de cortafuego/VPN busca de dónde viene, y observa las reglas para decidir si tiene permiso para entrar:

#	VPN_usuarios@cualquiera	230.230.230.1	HTTP	Encrypt	YES

Verá un Nuevo origen así como un nuevo grupo de usuarios. Esto se debe a que los clientes remotos pueden llegar de cualquier lugar, es decir, de cualquier dirección IP, y como siempre, todos deben estar autenticados. El grupo nuevo, VPN_usuarios, es una base de datos independientes que se encuentra en el servidor RADIUS. Si lo desea, puede utilizar un grupo. Esta regla también tiene propósitos de seguridad. Establece que los usuarios deben autenticarse en el servidor RADIUS, y después sólo podrán utilizar el tráfico http para los dominios de la VPN.

Una nota acerca del software VPN: En capítulos anteriores se mencionó que la tecnología VPN necesita estar lo más abajo posible en la pila OSI. El software VPN se encuentra entre el nivel de red y el nivel de enlace de datos. Con el mismo dispositivo VPN, se puede probar y optimizar el software para que tenga capacidades específicas en el hardware y/o en el sistema operativo. Sin embargo, esto es diferente con los equipos portátiles, por lo general, las máquinas tienen cargadas muchas aplicaciones, y es posible que haya conflictos entre el software VPN y otras aplicaciones. En estas situaciones, a veces el proveedor puede ayudar; en otros casos, será necesario eliminar la aplicación conflictiva, aunque sea difícil de ubicar.

4.4 INSTALACIÓN DE LA VPN

La gran cantidad de productos independientes proporciona una amplia selección a una organización sobre el tipo de producto de VPN a adquirir e implantar en la compañía. He aquí un ejemplo de una VPN independiente:

Aventail Extranet Center

Le proporciona el poder para controlar el acceso de los socios, clientes, consultores y otros usuarios a los recursos de su red. En la parte medular de su producto está la capacidad para crear una política fácil de administrar, definida centralmente.

El componente principal de Aventail Extranet Center es el Extranet Server. Se trata de un servidor proxy SOCKS v5 que maneja la autenticación de usuarios y procesa todas las solicitudes de conexión. Además, contiene un módulo de capa de sóckets segura (segure Sockets Layer) v3.0, para el cifrado Aventail Extranet Server puede manejar tráfico de red tanto de entrada (usuarios externos que intentan alcanzar los recursos de red internos) como de salida (usuarios internos que intentan alcanzar los recursos de red externos).

Además **Aventail Extranet Center** cuenta con las siguientes herramientas:

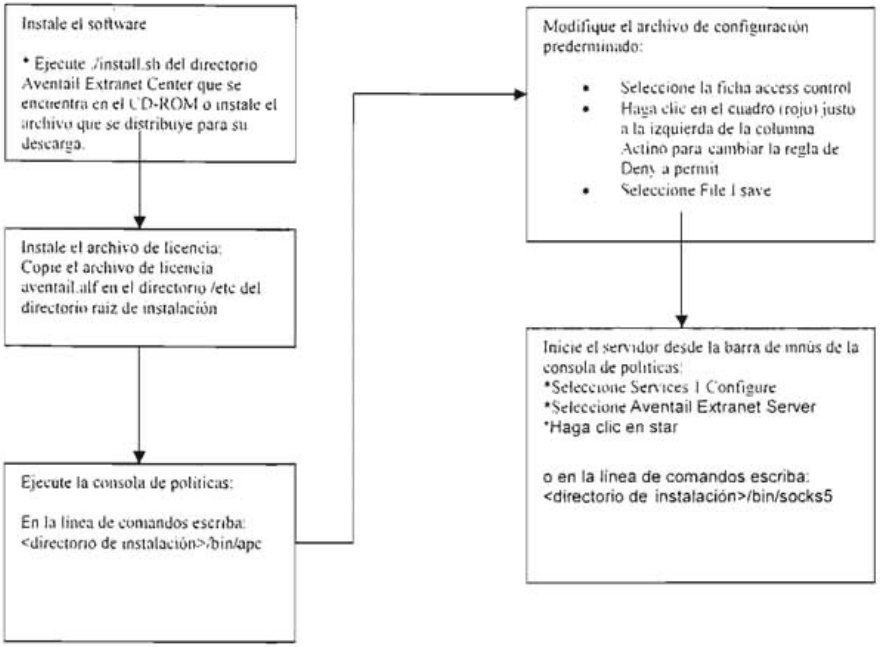
Aventail Policy Console.- Es la herramienta administrativa gráfica para crear, ver y administrar las políticas de su extranet. Puede ejecutarse ya sea en Windows NT o en UNIX y puede configurar un servidor Extranet Server en cualquier plataforma.

Aventail Management Server.- Es un servicio opcional que permite que los administradores manejen en forma remota un ExtraNet Server.

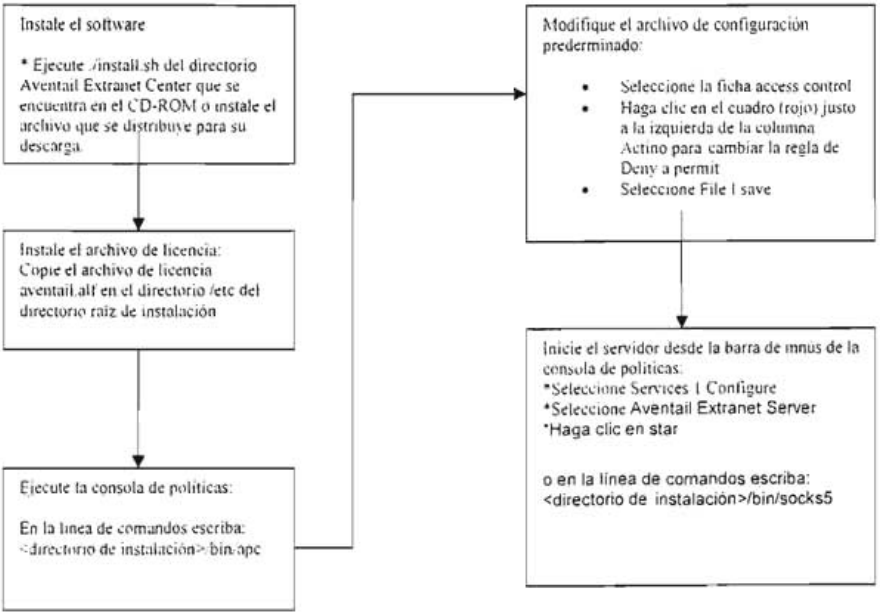
Aventail Management Server Config Tool.- Es un interfaz de usuario gráfica que permite modificar la configuración de Management Server. Está política determinará cuáles administradores puede manejar al Extranet Server, cómo deben autenticar y desde cuáles interfaces de red aceptará tráfico el servidor.

Aventail Connect.- Es el componente cliente de la solución Aventail Extranet Center. Es una aplicación que redirige todas las llamadas de aplicación TCP/IP a Extranet Server.

Instalación en Windows NT[18]



Instalación en UNIX



[18] Implementación de Redes Privadas Virtuales (RPV), Steven Brown, MacGraw-Hill, pág. 227

4.5 VPNS EN EL MERCADO

4.5.1 Windows NT 4.0 Server Y RRAS, Routing and Remote Acces Service:

La entrada de Microsoft en el juego de las redes privadas virtuales es sin duda un desarrollo propicio para una industria naciente pero fuerte. Siendo un gigante del software, llegó echando tiros con un producto de entunelamiento de VPN y el sistema operativo NT, que está favoreciendo con rapidez el estándar en el mercado para implantaciones del vendedor de firewalls. Su solución para VPN, el Servicio de enrutamiento y acceso remoto (RRAS, Routing and Remote Acces Service) legitimó el juego cuando hizo su debut. RRAS ofrece el protocolo de entunelamiento de PUNTO A PUNTO (PPTP, Point-to-point Tunneling Protocol) a través de Internet. Cómo sólo Microsoft podría hacerlo, RRAS se ofrece como descarga gratuita cuando compra e implanta el S.O. de NT 4.0 Server como sistema operativo de LAN/WAN. Se dice que RRAS y, en particular PPTP, no es tan robusto como IPSEC, en este caso, el protocolo Layer 2 Forwarding (L2F) de Cisco, esto no se debe por completo a que sea gratuito, sino a que es reflejo de la estrategia de Internet.

Pareciera que los productos estratégicos de Internet de Microsoft, como Internet Explorer y ahora RRAS, se obsequian como un complemento o como descarga gratuita, Así por naturaleza no serían tan robustos como un artículo comprado. Más aún, PPTP activa los túneles a través del TCP/IP de Internet encapsulando paquetes de PPP con IP . Esto permite a los usuarios remotos marcar telefónicamente a una LAN y utilizar de manera directa protocolos como IPX (Internetwork Protocol Exchange, intercambio de protocolo de red interna), NetBIOS (Network Basic Input/Output System, sistema básico de entrada/salida de red) y NetBEUI (Network BIOS Extended User Interface, interfase de usuario extendida de BIOS de red). Estos tres protocolos permiten a los usuarios remotos interactuar con el sistema de archivos, los componentes de hardware y los periféricos de una LAN, respectivamente, como si estuviera trabajando localmente en la LAN. Aunque la oferta inicial de PPTP no proporcionaba encriptación integrada para protocolos de IP de túnel y LAN, todavía es un buen método para una solución de VPN. Si bien una versión actual de PPTP proporciona encriptación, por desgracia PPTP posee algunas desventajas adicionales, como, mala implantación de autenticación de usuario, lo que podría comprometer la seguridad de las conexiones de VPN.

4.5.2 Servidores de Acceso de Compatible Systems (www.compatible.com)

Fundada en 1985 por Matt McConnell y Tim Schulz, Compatible Systems es el líder en la industria de las tecnologías de redes privadas virtuales (VPN) para acceso remoto y aplicaciones de sitio a sitio. Los servidores de acceso de VPN, enrutadores de sucursal de VPN, enrutadores de acceso a Internet, enrutadores de sitios de PSI, enrutadores de conmutación empresarial y enrutadores de conmutación y segmentación local ofrecen soluciones de Inter conectividad completas para miles de redes corporativas y proveedores de servicios de Internet (PSI) en todo el mundo.

Esta compañía es el único proveedor que ofrece una línea de productos de VPN completa e independiente. Esta tecnología innovadora, la amplia distribución y la importante base instalada le permitirán capturar un mercado inicial importante y capitalizar el crecimiento explosivo esperado para el sector de VPN.

La familia de productos de VPN de compatible Systems ofrece una solución de VPN independiente con un desempeño/precio superior. Los productos de Compatible ofrecen el soporte de plataforma cliente más amplio disponible hoy en día incluyendo todas las versiones de Windows anunciadas, Macintosh y Linux. Los productos también ofrecen soporte de protocolo amplio (IP, IPX, Apple Talk) y el establecimiento de puentes de protocolos no enrutables.

4.5.3 La familia Intraport de servidores de acceso de VPN

La familia Intraport de servidores de acceso de VPN, llamada VPN Access Servers, proporciona acceso remoto Basado en Internet y soluciones de LAN a LAN que varían en tamaño de 8 túneles simultáneos a más de 2,000 túneles simultáneos. Todos los productos Intraport presentan establecimiento de túneles Ipsec para los protocolos de red TCP/IP e IPX; enrutamiento integrado a través de RIP. RIP2 y OSPF; tres niveles de cifrado que incluyen la tecnología de la norma de cifrado triple de datos (triple DES); soporte ilimitado para cliente del usuario para Windows 95, Windows 98, Windows NT.MacOS y Linux, MD5/SHA, RADIUS y autenticación SecurID; y filtrado de paquetes completo.

4.5.4 Extranet Switch 4000 de Nortel Network (www.nortelnetworks.com/products/)

Contivity Extranet Switch de Bay Networks, una división de Nortel Networks Business, ofrece todas las características que se necesitan para satisfacer los retos de una Extranet de alto desempeño, escalable y segura, en un solo producto. Comparado con las soluciones previstas (los dispositivos externos como enrutadores y cortafuegos). Contivity Extranet Switch integra todas las tecnologías necesarias en una sola plataforma: enrutamiento, administración de ancho de banda y establecimiento de túneles seguros. Su arquitectura habilitada para directorios le permite determinar que nivel de desempeño, acceso y seguridad, con base en las necesidades de ese usuario. Esto permite la creación de "una Extranet personal", que puede adaptarse para satisfacer las diferentes necesidades de una amplia variedad de usuarios, sin importar la aplicación a la que cada usuario este tratando de acceder. La implantación de una Extranet con Contivity Extranet Switch permite que los clientes aprovechen a Internet para las aplicaciones actuales, tales como el acceso remoto. Al mismo tiempo proporciona la infraestructura segura necesaria para soportar aplicaciones de próxima generación como comercio electrónico, vinculando a la empresa con sus clientes y proveedores a través de Internet.

4.5.5 Ravlin de RedCreek

RedCreek Communications comenzó sus operaciones en julio de 1996. Sus productos aseguran privacidad de información conforme ésta se transmite a través de redes privadas y públicas, y proporcionan control de acceso a los recursos empresariales. Las soluciones de RedCreek se basan en una arquitectura revolucionaria, CryptoCore, asegurando velocidad de transmisión sin paralelo, autenticación transparente y facilidad de ampliación de red. La administración de red de los productos se lleva a cabo a través de una simple utilería de configuración de Windows 95/Windows NT 4.0 que soporta la norma de la industria SNMP para administración de dispositivos.

4.5.6 PERMIT Enterprise de Time Step (www.timestep.com)

TimeStep Corporation, es una compañía afiliada a NewBridge, es un proveedor líder de soluciones VPN seguras para intranets, Extranets y acceso remoto a Internet. Con la tecnología VPN de TimeStep, los negocios pueden enviar datos delicados a través de Internet, confiando que viajarán en forma segura.

El conjunto de productos PERMIT Enterprise permite utilizar redes públicas para:

- Acceso LAN remoto a Internet seguro.
- Conectividad de sucursales segura.
- Conectividad Extranet segura con socios comerciales, clientes y proveedores.

La administración de la VPN segura puede ser desde un solo punto o de múltiples puntos, y estar manejada desde un punto de contacto interno (en una LAN) o desde una estación remota en cualquier parte del globo (a través de Internet).

4.5.7 Comparación genérica de vendedores de VPN :

Tabla 1

Compañía	Solución de VPN	Solución Firewall	Plataforma	Familia de VPN
Digital Equip. Corporation	Alta Vista Túnel 98	AltaVista Firewall 98	Servidores: Digital UNIX v.4.0 o superior Windows NT 4.0 Clientes: Windows 95, NT Mac OS v.1.1.1 y 1.1.2 y v.1.2 o 1.3	Cliente de AVT 98 Servidor/de telecomunicador AVT98 Servidor de Extranet AVT 98
Cisco Systems Inc.	VPN de Cisco (el software IOS de Cisco proporciona encriptación y entunelamiento)	PIX Firewall 4.1 (dispositivo de firewall) Software de firewall IOS de Cisco	Enrutadores habilitados de VPN Enrutadores optimizados de VPN	Acceso de cliente: Serie Cisco 800 Serie:1700 Lan a Lan: Serie 1700, Serie 2600, 3600, 7200
NetGuard Inc.	VPN de Guardian	Guardian Firewall 3.0	Servidor(es): Windows NT 4.0 Cliente (s): Windows NT 4.0	Acceso de cliente: Cliente de autenticación Guardian Lan a Lan Guardian Agent
TimeStep Inc.	PERMIT Enterprise	Dispositivo de firewall PERMIT (Check Point Technologies OEM)	Servidor(es) Windows NT 4.0 Clientes (s) : Windows 95, 98, NT, Mac OS 7.1 más reciente	PERMIT/Cliente PERMIT/Puerta PERMIT/Suite de director
AXENT Technologies Inc.	Power VPN	Raptor Firewall 5.0	Servidor (es): Windows NT, Solaris, HP/UX, Linux, BSDI Cliente(s) : Windows 3.x,95,NT	Clientes de VPN: ---RaptorMobileVPN Power/VPN Puertas de enlace de VPN: Raptor Firewall Power VPN
CyberGuard Corporation	Stoplock Connect-IP	CyberGuard Firewall v.4	Servidor(es): Cliente (s): Windows 3x, 95 NT	IP de conexión Cliente móvil: Remoto a IP de conexión Cliente: Puerta de enlace de IP de conexión
Check Point Software Technologies LTD	VPN-1 v.4.0	Firewall-1 v.4.0	Servidor (es) : HP/UX 10.10,20 IBM AIX 4.21, 4.3 Solaris 2.5, 2.6 Windows NT Cliente (s): Windows NT, 95 X11R5	SecuRemote de VPN-1 RemoteLink de VPN-1 Puerta de enlace de VPN-1
WatchGuard Technologies Inc.	VPN de WatchGuard	WatchGuard Firewall	Servir(es): Dispositivo de firewall Firebox (puerta de enlace de seguridad) Clientes : Windows 95, NT	VPN de usuario remoto VPN sucursal de oficina . Firebox II, Firebox100

Cuantas veces mencionamos PPTP, L2TP e IPSec Aun cuando se mencionaron, sólo fue de una manera superficial. Las buenas noticias son que usted no tiene que preocuparse demasiado por estos protocolos, ya que los proveedores se encargan de eso. Las malas noticias son que si usted tiene dos proveedores diferentes debe preocuparse por los problemas de la interoperabilidad.

En este cuarto capítulo, para poder elegir la metodología que a nuestro parecer resultó ser la más adecuada, tuvimos que hacer un análisis de las distintas metodologías existentes. Así una vez con ello, a través del seguimiento de las etapas de análisis, diseño, implantación, instalación y mantenimiento, es posible que el lector sea apto de llevar a cabo el proceso de enlace entre la Intranet y la Extranet, pero es importante entender que esto es solo una propuesta, ya que si bien la diversidad de métodos aplicables dejan un gran margen al lector para enriquecer el proyecto.

CAPÍTULO V

ORGANIZACIÓN Y ADMINISTRACIÓN DEL SISTEMA INTEGRAL

CAPÍTULO V. ORGANIZACIÓN Y ADMINISTRACION DEL SISTEMA INTEGRAL

En este último capítulo, describiremos algunos aspectos en cuanto al mantenimiento de la tecnología VPN para llevar a cabo un control adecuado de los recursos del sistema.

Las organizaciones que creen que implantar y administrar una solución de VPN es fácil, encontrarán ciertas dificultades, ya que la administración de una VPN segura requiere un compromiso y comprensión de la misma para desarrollar e implantar las políticas necesarias y así poder ofrecer este servicio.

En general los problemas que debe enfrentar una organización son mucho mayores que los problemas locales y con frecuencia se convierten en problemas internacionales, por lo que resulta conveniente y necesario tener un conocimiento de las leyes y normativas internacionales para prevenir infracciones de leyes o normativas locales en algún lugar por uno de los usuarios de la organización.

La solución de los problemas no es banal y requiere un esfuerzo de equipo en cuanto a: administración, lo legal, seguridad y experiencia técnica, para poder designar, implantar y administrar su solución de VPN.

La Administración de la VPN.- La administración de la VPN supone la construcción de la política de seguridad de la empresa en una base de reglas, controlando el acceso a los bienes de información de la red, registrando la actividad diaria y disparando las alertas necesarias por la presencia de intrusos. La administración de VPN también supone la configuración y el mantenimiento de puntos de aplicación remotos.

Después de las actividades de configuración, la red está lista para ser administrada. Las soluciones de VPN suelen proporcionar la misma capacidad de administración; administración remota centralizada, vigilancia de red, desactivación de funciones de acceso, verificación de estado operacional y actividad de registro.

Tabla 1 Los puntos importantes para el administrador al controlar y administrar la VPN cuando ya está operando son los siguientes:

Enlaces redundantes	Crecimiento en la organización
Actualizaciones de software	Soporte técnico
Usuarios remotos	Compatibilidad
Supervisión	Alerta de intrusos
Registros	Correlación de eventos
Cifrado y encapsulamiento	Administración de claves
Números aleatorios	Certificados
Actualización de seguridad	Soporte para actualizaciones
Protocolos para establecer túneles	Dispositivos de administración
Rendimiento	Calidad de Servicio
Autenticación	Trabajo calificado

Los puntos que se mencionan en la tabla 1 son retomados más adelante, pues consideramos que esta es una de las más importantes dentro de la metodología que utilizamos.

La VPN funciona como cualquier empresa en la que se toman decisiones, donde el administrador debe organizar el sistema para que funcione de manera integral.

El sistema de control administrativo de la empresa lo describimos en la figura 5.1, donde podemos ver que el administrador es una pieza clave en el sistema ya que todas las acciones de control que cumple se relacionan con todas las áreas de manera directa.

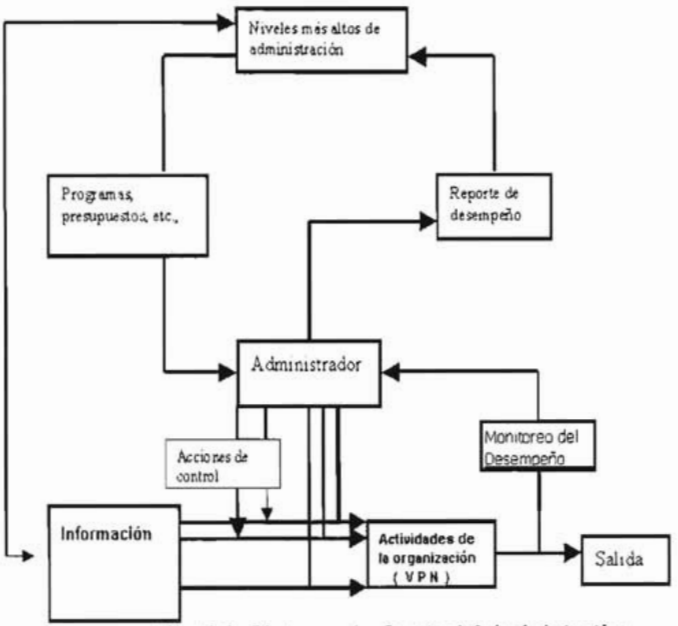


Fig 5.1 Sistema de Control Administrativo

5.1 SOLUCION DE PROBLEMAS DE LAS VPN

La infraestructura de una VPN consiste en enrutadores, conmutadores, usuarios remotos, dispositivos de autenticación, etc., por lo tanto, si asume que una VPN es sencillamente un algoritmo de cifrado, puede cometer el error de no ver los demás aspectos de la tecnología VPN.

La solución de problemas de las VPN siempre comienza con el aislamiento. Toma potencialmente un paquete de datos de un extremo de Internet y lo envía a su destino, pasando en el camino a través de enrutadores. Una vez que el paquete de datos llega al dispositivo, quizá éste se envie a otro dispositivo para autenticación y regrese de nuevo al dispositivo original para su verificación. Sin importar el dispositivo VPN que se instale, el paquete de datos seguirá esta ruta.

El 50 % de los problemas con las VPN no son problemas de VPN, es decir, no es el algoritmo de cifrado el que causa el mal funcionamiento, sino otra pieza del rompecabezas.

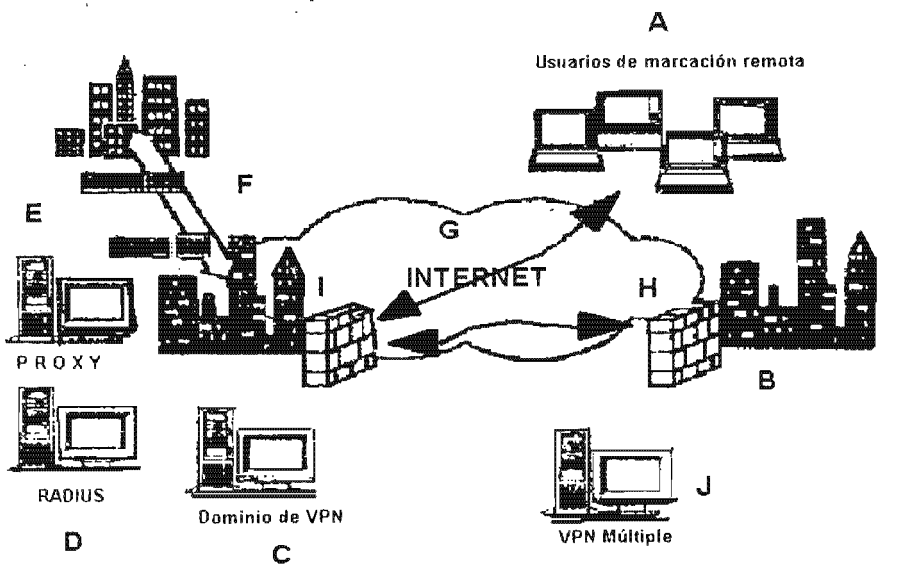


Fig. 5.2 Áreas Problemáticas Potenciales

En este caso, ¿dónde puede estar el problema, o dónde se puede comenzar a buscar?, la figura 5.2 muestra áreas problemáticas potenciales. Se necesita entender estas áreas para resolver los problema de las VPN de manera eficiente y efectiva.

La siguiente tabla muestra los principales problemas que se presentan con el uso de la tecnología VPN.

Tabla 2 Principales Problemas

PRINCIPALES PROBLEMAS	*DESCRIPCIÓN*
A. Usuarios de marcación remota	Los usuarios de marcación no pueden conectarse al dispositivo VPN para establecer un túnel cifrado.
B. VPN de LAN a LAN	Este es otro sitio geográfico que está conectado a otra VPN. Aquí es realmente necesario comprender la configuración para establecer la VPN de LAN a LAN. No importa si se trata de IPSec, PPTP o L2TP, si no entiende el protocolo empleado, no va a hacer que funcione la VPN.
C. Dominio de la VPN	Si los usuarios externos pueden establecer una conexión a la red corporativa pero no puede ir más allá o tener acceso a cualquier equipo, entonces no se ha configurado adecuadamente el dominio de la VPN. De alguna manera, su VPN tiene que decirle a los usuarios cuándo cifrar los datos.
D. Servicios de autenticación	Esta es otra cosa que se debe revisar una vez que se hayan configurado las conexiones de marcación remota a la VPN, las conexiones VPN de LAN a LAN y las conexiones de Extranet a la VPN. Estos usuarios deben estar autenticados. Si el dispositivo de autenticación no puede comunicarse con el dispositivo de la VPN o no puede responder lo suficientemente rápido, la comunicación se suspenderá en diversos periodos
E. Proxy.	Dependiendo del tipo de dispositivo que coloque junto al punto de acceso a Internet, puede confundir los problemas del proxy con los problemas de la VPN. En este caso, debe averiguar qué tanto pueden adentrarse los usuarios en la red.
F. Enrutamiento WAN interno	El enrutamiento es otra causa principal de los problemas en las VPN. Sin una configuración adecuada de una política de enrutamiento que envíe los paquetes que llegan a través del dispositivo VPN, no habrá comunicación.
G. Internet.	Algunos PSI bloquean los paquetes cifrados. Si un enrutador, suyo o de cualquiera en la trayectoria entre el usuario y la red corporativa, establece un filtro para bloquear estos paquetes, nunca habrá comunicación.
H. Problemas de cifrado	Entre dos VPN, puede haber problemas de cifrado los mecanismos de claves, los tiempos para realizar el intercambio de claves, los problemas de comunicación y las actualizaciones pueden afectar las comunicaciones entre los dos sitios.
I. Direccionamiento.	Antes de establecer una VPN necesita conocer los aspectos concernientes al direccionamiento

Cont. Tabla 2 Principales Problemas

PRINCIPALES PROBLEMAS	*DESCRIPCIÓN*
J. VPN múltiple	Si utiliza un dispositivo VPN múltiple como una estación UNIX y decide usarlo como una combinación cortafuego/VPN, y considera tener zonas DMZ múltiples, entonces debe considerar el flujo del tráfico, los aspectos del enrutamiento y los posibles aspectos de la NAT en la misma caja. Emplear una sola estación permite una administración flexible y fácil; sin embargo, puede ser difícil mantener la configuración.
K. Varios	Aunque K no es parte del diagrama, la categoría de varios abarca todos los aspectos de problemas con VPN, PPTP, PPP, DES, SKIP y MD5. Estos problemas están relacionados directamente con la tecnología VPN.

Existen muchas áreas donde se requieren habilidades para resolver problemas de las VPN. Podría decirse que el paso más importante en la solución de problemas de VPN es el aislamiento. Si no puede aislar el problema puede tomar mucho tiempo encontrarlo. En las siguientes secciones, avanzaremos con más detalle al abordar algunos de los problemas recién mencionados.

5.1.1 Usuarios de marcación remota

El dispositivo VPN se configura con los siguientes elementos:
1.- Dominio de la VPN.- La red o los servidores a los cuales tienen permitido conectarse los usuarios.
2.- Certificados y generación de claves. Configurará el dispositivo VPN para crear una clave, por ejemplo, Diffie-Hellman, y creará un certificado para el dispositivo. Aquí es donde aparece el factor confianza. Puede utilizar el mismo dispositivo VPN como autoridad emisora de certificados, o puede elegir un tercero, ya que algunos proveedores comienzan a implantar esta configuración.
3.- Servidor de autenticación. Es el servidor de autenticación al que se conectarán los usuarios.
4.- Cifrado o encapsulamiento.- Esto puede depender del proveedor de la VPN. Los productos de algunos proveedores obligan a encapsular a todos los usuarios de marcación, mientras que algunas VPN solo utilizan el cifrado.

Equipo portátil

1.- El equipo portátil necesita cargar software de VPN
2.- Tiene que establecer la opción de configuración del software VPN para que indique la dirección IP pública del dispositivo VPN.
3.- Necesita conseguir la clave del dispositivo VPN.

Solución de problemas:

Con frecuencia, los problemas son causados por fallas del software instalado en los equipos portátiles. Quizá el software no se instaló o se instaló pero parece no funcionar. Debido a la naturaleza del software, puede y debe interactuar con cualquier otra aplicación. Ya que éste se encuentra entre el nivel 2 (enlace de datos) y el nivel 3 (red), puede interactuar con otros dispositivos de la máquina. Si tiene problemas con el software elimínelo y encienda de nuevo la máquina. Cuando lo instale, asegúrese que no haya otra aplicación ejecutándose. Además, asegúrese de tener el software adecuado, no sólo la versión correcta, sino el algoritmo de cifrado correcto. Muchos fabricantes de VPN soportan distintos algoritmos de cifrado, por ejemplo: DES, 3DES, IDEA, etc., sin embargo, el software que cargó en su máquina puede tener un algoritmo distinto. Si utiliza 3DES en el dispositivo VPN, debe utilizar 3DES en el equipo portátil.

Como se autentica el equipo portátil:

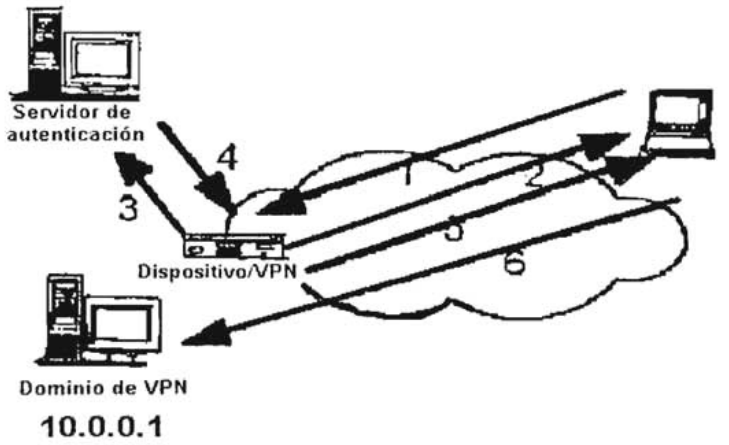


Fig. 5.3 Autenticamiento del Equipo Portátil

1.- El equipo portátil intenta tener acceso al servidor VPN en 10.0.0.1
2.- El dispositivo VPN le solicita al equipo portátil su nombre de usuario y su contraseña.
3.- Si el dispositivo VPN ha sido configurado para utilizar un servidor de autenticación, consultará con ese servidor.
4.- El servidor aprueba o rechaza la solicitud.
5.- El dispositivo VPN responde al equipo portátil ya sea aprobado o rechazado el acceso,.
6.- Finalmente, si se otorga el acceso, el equipo portátil puede utilizar http para transferencias con el servidor VPN en 10.0.0.1

Conforme avance el proceso de autenticación del equipo portátil, podrá proseguir al paso siguiente. Durante este paso de autenticación, revise los registros en el dispositivo de autenticación y/o en el dispositivo VPN, y si hay un mensaje "User test denied access" (acceso denegado al intento del usuario), sabrá que el problema radica en el mecanismo de autenticación.
Este tipo de errores ocurre debido a inicios de sesión incorrectos, contraseñas erróneas y tiempos agotados en el servidor de autenticación.

5.1.2 VPN de LAN a LAN

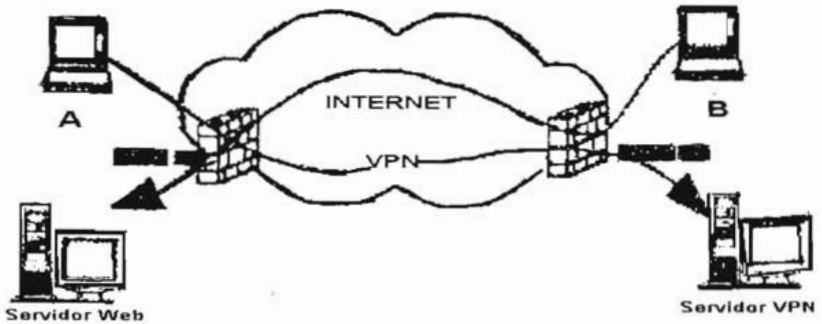


Fig. 5.4 VPN de LAN a LAN

La segunda configuración más común está estrechamente unida al desarrollo de la norma IPSec. IPSec viene del intercambio de redes automotrices (ANX). La meta era conectar varios fabricantes, proveedores y clientes para que intercambiarán datos de manera segura.

En la figura 5.4 se observa una VPN de LAN a LAN típica. Observe que no todo el tráfico esta cifrado y que la flecha tiene la etiqueta "VPN" en lugar de "túnel". Si encapsula los datos, creará un túnel, sin embargo una VPN sencilla puede ser de cifrado. Se involucran dos tipos de comunicaciones:

- Acceso al servidor web. Cuando el usuario B quiere conectarse al servidor web de la red del usuario A, el tráfico http está descifrado. El dispositivo VPN no debería cifrar este tráfico; este fluirá intacto.
- Acceso al servidor VPN. Cuando el usuario A quiere conectarse al servidor VPN de la red del usuario B, el dispositivo VPN deberá reconocer que ésta es una solicitud VPN y cifrar los paquetes.

En la figura 5.4 se eliminaron todos los protocolos, existen muchas formas de configurar una VPN con protocolos muy distintos PPTP y L2TP, son protocolos de nivel 2, e IPSec es un protocolo de nivel 3. Por lo tanto puede combinar ambos. Sin embargo, es posible que al combinarlos haya problemas en cualquier protocolo.

5.1.3 VPN con PPTP

El protocolo punto a punto (PPTP) se diseñó para permitir que los usuarios remotos marcarán a su PSI local y establecieran un túnel al servidor de la compañía. En este caso puede ser un cliente PPTP WinXX que establece un túnel a un servidor PPTP en la red de la empresa. PPTP utiliza la infraestructura de protocolos existente para permitir una conexión por marcación, llamada PPP. Luego toma estos paquetes PPP y los encapsula dentro de un encabezado con Encapsulamiento para Enrutamiento Genérico (GRE). Debido a la dependencia en PPP, PPTP utiliza algoritmos de cifrado, tales como PAP y CHAP para proporcionar el cifrado. Según la disponibilidad del PPTP en las estaciones NT y a la base de usuarios instalada, PPTP es un protocolo de VPN. PPTP viene en dos configuraciones: modo obligatorio y modo voluntario.

Tabla 3 Mensajes de control:

Tipo de mensaje	Significado
PPTP_START_SESSION_REQUEST	Inicia Sesión
PPTP_STAR_SESSION_REPLY	Responde a la solicitud
PPTP_ECHO_REQUEST	Mantiene la sesión
PPTP_ECHO_REPLY	Responde para mantener la sesión
PPTP_WAN_ERROR_NOTIFY	En la conexión a ocurrido un error en un enlace PPP
PPTP_SET_LINK_INFO	Configura la conexión entre cliente y servidor PPTP
PPTP_STOP_SESSION_REQUEST	Termina la sesión PPTP
PPTP_STOP_SESSION_REPLY	Responde
WAN_Error_Notify	Errores en la interfaz PPP de la WAN

Dentro de los mensajes de control hay códigos de errores adicionales que son de mucha ayuda para resolver problemas. Por ejemplo, Start-Control-Connection-Reply, tiene una lista de códigos que son resultado de agregar información adicional para resolver problemas como se muestra:

1.- Establecimiento exitoso del canal.
2.- Error general, el código de errores indica el problema.
3.-Ya existe el canal de comandos.
4.- El solicitante no está autorizado para establecer el canal de comandos.
5.- La versión del protocolo del solicitante no se soporta.

WAN-Error-Notify es una lista de mensajes de errores de control enviada desde el concentrador de acceso http (pac) al Servidor de red PPTP (PNS) para indicar las condiciones de errores en el enlace WAN. Si tiene problemas PPTP intermitentes, vigile estos contadores. Éstos pueden indicarle que se trata de problemas WAN en lugar de problemas PPTP. Las condiciones de error son las siguientes:

- Errores CRC El número de tramas PPP recibidas con CRC desde el comienzo de la sesión.
- Errores de tramas. El número de paquetes PPP entramados con formatos incorrectos.
- Desbordamiento del hardware. El número de desbordamiento de la memoria intermedia (buffer) recibido en el hardware desde el comienzo de la sesión.
- Desbordamiento de la memoria intermedia. El número de desbordamientos de la memoria intermedia desde el comienzo de la sesión.
- Errores por tiempo agotado. El número de periodos agotados desde el comienzo de la sesión.
- Errores de alineación.

Establecimiento de túneles PPTP de datos

Los túneles PPTP de datos son la etapa final de la transmisión, donde el protocolo PPTP forma los paquetes PPP que tienen paquetes PPTP cifrados y los envía al servidor PPTP. Entonces, el servidor PPTP descifra estos paquetes y los envía a los anfitriones respectivos.

Las comunicaciones PPTP dependen del tipo de modo que se emplee, ya sea voluntario u obligatorio, así que la solución de problemas dependerá de cómo se establecen las conexiones de control. En el caso del modo obligatorio, el FEP (procesador frontal) del PSI maneja las comunicaciones PPTP. En el caso del modo voluntario, el mismo equipo portátil maneja los mensajes de control PPTP. El siguiente es un conjunto de pasos típicos para manejar las comunicaciones PPTP:

1.- El equipo portátil crea una cuenta PPP de marcación a un PSI o a un PSI con FTP.
2.- EL FEP podría enviarle una señal al servidor PPTP con una PPTP_Start_Session_Request, y el servidor podría responder con una PPTP_Star_Session_Reply.
3.- Entonces, El FEP hace una solicitud al servidor PPTP.
4.- El servidor envía la respuesta al FEP.
5.- Comienza la comunicación de datos
6.- Finalmente, se envía un PPTP_Stop_Session_Request y se recibe un PPTP_Stop_session_Reply.

PPTP utiliza el protocolo IOP47, el cual es el protocolo GRE, y los puertos TCP 1723 0 5678. El puerto 1723 es para el servicio PPTP de Microsoft. PPTP tiene muchas áreas donde pueden presentarse problemas, no sólo en el protocolo en si, sino en la infraestructura que lo hace funcionar (por ejemplo, el cortafuego, el FEP, la conexión PPP). Cuando se resuelven problemas relacionados con PPTP, primero es necesario saber que tan lejos progresaron los paquetes. Si vigila el cortafuego y ni siquiera ve las conexiones de control de PPTP que llegan, el problema estará entre el FEP del PSI y el propio equipo portátil.

5.1.4 VPN con L2TP

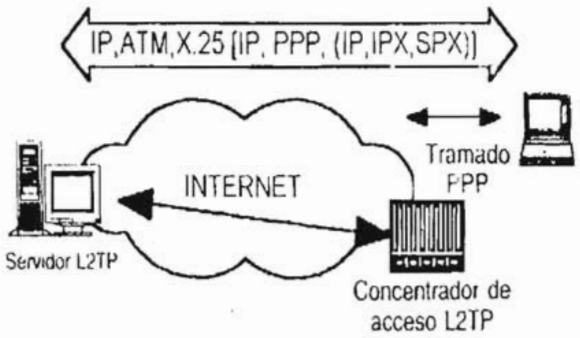


Fig. 5.5 VPN con L2TP

El protocolo para establecimiento de túneles de nivel 2 (na combinación de L2F y PPTP) es básicamente el mismo que PPTP. L2TP se apoya en PPP para establecer una conexión por marcación, pero a diferencia de PPTP, define su propio protocolo para establecer túneles. Utiliza PPP (PAP y CHAP) para autenticar usuarios, y puesto que es un protocolo de nivel 2, permite el transporte sobre protocolos que no son IP.

La configuración de la VPN con L2tp es muy parecida a la configuración de PPTP. El paquete de datos incluye la comunicación PPP inicial y PPP puede utilizarse para paquetes cifrados. L2TP es independiente del medio, por lo que se puede utilizar L2TP en ATM, tramas o IP. El servidor PPTP ha sido reemplazado por un servidor L2TP y que el FEP PPTP del PSI ha sido reemplazado por un concentrador de acceso L2TP. La VPN con L2TP permite varias conexiones dentro del túnel y asigna un identificador de llamadas único a cada sesión dentro del túnel. Al igual que PPTP, L2TP define los tipos de mensajes:

- Control.- Son responsables de cosas tales como la configuración, la terminación de la sesión y el estado del túnel. Los mensajes de control también se emplean para mantener las características dentro del túnel, como puede ser mantener el control del flujo y determinar la velocidad de transmisión y los parámetros de la memoria intermedia para los paquetes PPP de sesiones individuales.

- Datos.- Los mensajes de datos son paquetes PPP sin la información de tramas.

Tabla 4 Mensajes de control

Tipo de mensaje	Significado
Start_Control_Connection_Request	Inicia la sesión
Start_Control_Connection_Reply	Responde la solicitud
Start_Control_Connection_Connected	Responde la réplica; termina el reconocimiento del establecimiento del túnel
Stop_Control_Connection_Notification	Cierra la conexión de control
Hello Túnel	Está activo
Outgoing_Call_Request	LNS informa a LAC que debe establecer una llamada externa
Outgoing_Call_Reply	Respuesta del LAC

L2TP utiliza los mismos modos que PPTP (voluntario y obligatorio) y tiene su propia lista de mensajes de control. Además, L2TP utiliza una terminología especial para definir donde inicia y termina la comunicación. Un concentrador de acceso (LAC) L2TP se comunica con un servidor de red (LNS) L2TP para controlar las conexiones. Además el documento L2TP, draft-ietf-pppext-l2tp-12.txt, especifica algunos mensajes generales que pueden ser de utilidad para resolver problemas.

0.- No hay error general.
1.- Aún no existe una conexión de control para el par LAC-LNS.
2.- La extensión es errónea.
3.- Uno de los valores del campo está fuera del intervalo o el campo reservado era no cero.
4.- Recursos insuficientes para manejar esta operación ahora.
5.- El identificador de llamadas es inválido en ese contexto.
6.- Ocurrió un error genérico especifico del proveedor en el LAC.
7.- Pruebe con otro. Si LAC está al tanto de otros destinos LNS posibles, este debería intentar con uno de ellos.

5.1.5 VPN con IPSec

IPSec es sinónimo de interoperabilidad. El problema aparece cuando los proveedores eligen su propia ruta con el fin de dejar espacio libre para la interoperabilidad, lo cuál puede significar problemas con ésta última. En las VPN con PPTP y L2TP hay mensajes de control, mensajes de comunicación y otros mecanismos que son de utilidad para determinar en donde se ubican los problemas. En IPSec estos mensajes no existen, al menos no con el mismo detalle que otros algoritmos que tienen el propósito de ayudar en la configuración y el mantenimiento de la VPN. IPSec utiliza varias tecnología para establecer, y por consiguiente, para resolver problemas en las VPN:

- Intercambio de claves Diffie-Hellman
- Firmas digitales
- Cifrado DES
- Algoritmos cifrados con transformación del código
- Asociación de seguridad (SA)
- Dominio de interpretación (DOI)

Los principales problemas que se presentan en las VPN con IPSec se dan en el dominio de Interpretación (DOI). DOI es una agrupación de protocolos relacionados que se emplean para establecer una Asociación de Seguridad (SA) en particular. La asociación de seguridad es IPSec; puesto que será específica del proveedor, puede ser difícil resolver los problemas relacionados.

La Asociación de Seguridad es el primer paso en el establecimiento de la VPN con IPSec. Antes de que comience cualquier transferencia de datos, ambas partes deben estar de acuerdo en una SA. La SA es muy parecido al conjunto de reglas de un juego (cuánto dura, cuántos jugadores, quién va primero, etc.) .

Los mensajes de archivos de registro indican problemas con los algoritmos de cifrado y/o con las propiedades que se establecen en el dispositivo VPN (por ejemplo, aunque no sea posible activar el túnel, el túnel ya existe, se está empleando DES o el anfitrión terminal utiliza algo distinto a DES):

- No puede descifrar el encabezado
- No puede definir métodos para DES
- No puede obtener datos de la SA
- Falló al crear una clave secreta
- Certificado inválido
- Método de cifrado ilegal
- Método seleccionado ilegal
- Esquema desconocido
- No puede conseguir una sesión de claves desde la caché.
- Falló la activación del túnel.

Además, el dispositivo VPN no puede comunicarse con precisión con la otra terminal usando el algoritmo provisto. De la misma forma que el mensaje de control PPTP o L2TP indico un problema con el túnel, estos últimos mensajes indican un problema con el algoritmo involucrado.

5.1.6 Cortafuego/VPN múltiples

Los cortafuegos VPN múltiples son cortafuegos con zonas DMZ y que además de correr el código de ejecución del cortafuego también deben realizar el enrutamiento, el cifrado/descifrado y posiblemente las traducciones de direcciones de red.

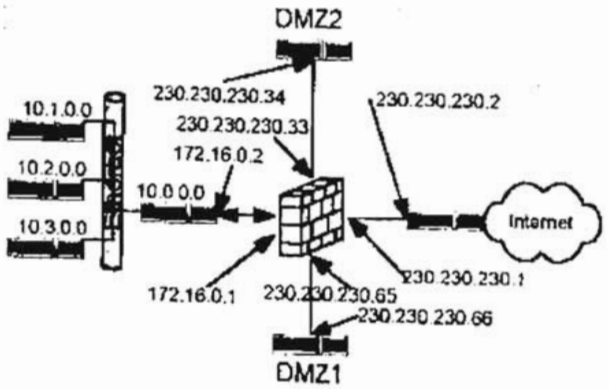


Fig. 5.6 Cortafuegos VPN Múltiples

Se concentra primero en el cortafuego y en la VPN. Además, notará que se introdujeron tres enrutadores nuevos en esta figura (10.1.0.0, 10.2.0.0 y 10.3.0.0). Antes de solucionar problemas debe asegurarse que la política de enrutamiento sea la correcta en todos los dispositivos.
La red interna ha sido direccionada de acuerdo con el RFC 1918 y a una clase B se le han dado 10 direcciones de subred:

1.- Todos los enrutadores en la organización han sido configurados para enrutarse a la red 172.l6.0.0 Recordará que debido al problema del Enmascaramiento de subredes de longitud variable (VLSM), se necesitó introducir otra red o enrutar de nuevo todas las redes en el cortafuego hacia los enrutadores internos.
2.- Todos los enrutadores (10.0.0.0, 10.1.0.0, 10.2.0.0 y 10.3.0.0) deben tener la misma política predeterminada que señala a 172.l6.0.1. La dirección IP interna del cortafuego es 172.l6.0.1 y se encarga de cualquier paquete que sea destinado a Internet con la política de enrutamiento que se instaló.
3.- El cortafuego debe tener una política con una ruta predeterminada al enrutador externo (230.230.230.2) y un enrutador interno para la red 10 con la dirección 172.l6.0.2
4.- En enrutador externo debe saber qué paquete debe enrutar de regreso al cortafuego (el enrutador no necesita saber de ningún espacio de dirección privada, sólo pública). En el ejemplo se asume que 230.230.230.0 es la dirección pública dada a la compañía y utilizada en el cortafuego.
Nota: *Dependiendo de cómo se configure la dirección externa en el enrutador, quizá necesite enrutar también las subredes a la dirección IP del cortafuego.*
5.- Dependiendo de cómo se emplea NAT, es posible que sea necesario otra ruta en el enrutador. Por ejemplo, si emplea la gama de direcciones del enrutador externo o del cortafuego (230.230.230.1-31), entonces, no se requiere otra ruta en el enrutador externo, puesto que esta directamente conectada a esa red. Si consigue nuevos espacios de direcciones públicas para utilizar NAT, entonces, deberá especificar una ruta en el enrutador externo, indicando esa red a la interfaz del cortafuego.

Una vez que esta configuración esté establecida, intente el enrutamiento desde cualquier anfitrión interno a Internet, y desde el cortafuego a cualquier anfitrión interno. No puede realizar el enrutamiento desde el enrutador externo a la red interna, puesto que eso significa que intenta enrutar a una red 10, lo cuál es ilegal. Este paso tiene que realizarse primero y debe tener éxito. Si no es así, no podrá establecerse VPN alguna.

En la solución de problemas de las VPN, el paso más importante es el aislamiento, determinar dónde se detienen los datos. Los mismos algoritmos de cifrado por lo general son un problema importante en la conectividad de las VPN. En esta parte incluimos algunos tipos de mensajes de error que pueden indicar los problemas de cifrado de las VPN, por ejemplo, no se pueden obtener los datos de SA, no se pueden crear las claves secretas y hay certificados no válidos. Muchos de éstos son problemas de conexión inicial que deben trabajarse. Con los problemas de túneles de VPN, es una buena idea vigilar cualquier tipo de contador que esté disponible con el proveedor especifico, como el WAN_Error_Notify en el protocolo PPTP.

Para terminar con la solución de problemas de las VPN: necesita toda la información posible sobre aspectos como archivos de registro, ventanas múltiples en el dispositivo, rastreadores de paquetes de datos y las distintas partes involucradas, puesto que quizá tenga que vigilar el dispositivo VPN mientras alguien intenta crear un túnel.

5.2 Mantenimiento de una VPN

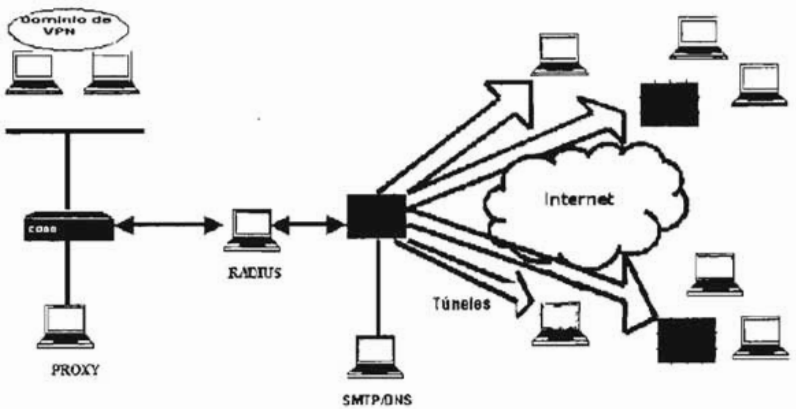


Fig. 5.7 Requisitos de mantenimiento de las VPN

Al igual que cualquier otro dispositivo de red, las VPN necesitan mantenimiento, pero a diferencia de los otros dispositivos, éstas no deben considerarse como un solo dispositivo aislado. Aún si se está utilizando un tipo de configuración de caja negra independiente, una VPN requiere mucho más mantenimiento que otros dispositivos.

Cuando usted instala una VPN, establece túneles, crea bases de datos de acceso para los usuarios e instala esquemas de cifrado y de administración de claves. Probablemente también instalará un tipo de software de supervisión y alertas, algún tipo de servidor de autenticación de usuarios como un servidor RADIUS. Las VPN deberian considerarse de naturaleza muy dinámica. La figura 5.7 muestra sólo algunos de los requisitos de mantenimiento de las VPN.

5.2.1 Enlaces redundantes

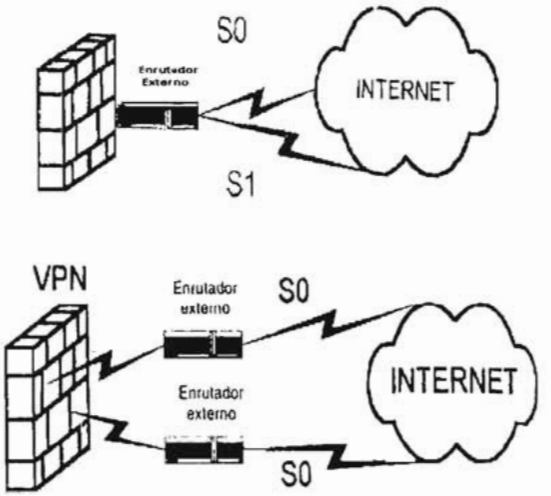


Fig. 5.8 Enlaces Redundantes

En la figura 5.8 podemos ver dos de las muchas opciones disponibles para una organización. Ambas son redundantes pero el nivel de redundancia cambia para cada configuración. Si no se está utilizando un mecanismo de cola de espera en los enrutadores, entonces es muy probable que un enlace sea la conexión principal a Internet y que se instalé un enlace secundario en caso de que exista una falla en el sistema principal.

La redundancia es el proceso de respaldar una línea principal. La siguiente figura ilustra el caso en el que no hay un solo punto de falla

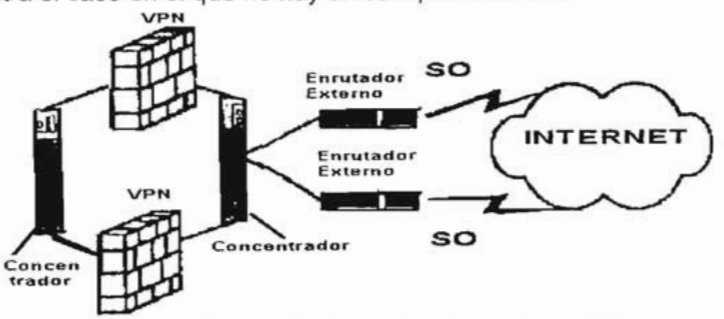


Fig. 5.9 Enlace Redundante sin Punto de Falla

5.2.2 Crecimiento en su organización

Conforme una organización crece, el tráfico de Internet indudablemente se incrementará más rápido de lo que su infraestructura de red física puede soportar.

Día a día crecen los usuarios en Internet, sin embargo, el espacio físico que puede destinar para su equipo de red (enrutadores, concentradores, conmutadores y otros dispositivos) es limitado. El tráfico de Internet crece sin límite, ¿de quién será la responsabilidad en su organización para manejar estas nuevas necesidades de conectividad en red?, ¿Puede añadir otro dispositivo en paralelo para manejar esta nueva carga? o ¿Su organización estará delimitada por el hardware existente y requerirá actualizar todo?.

El sitio web también tendrá un incremento en el tráfico. El simple hecho de tener una presencia en Internet junto con el número de mecanismo de búsqueda disponibles incrementará sus necesidades de ancho de banda.

Si además agrega el tráfico web de salida y la cantidad de tráfico DNS y SMTP que pasa, podrá darse una idea del tráfico generado. También los proveedores individuales proporcionarán los diversos tamaños de paquetes que añaden sus tecnología de cifrado a la cantidad de tráfico. Con todo esto podemos calcular lógicamente la cantidad de ancho de banda que se puede necesitar.

5.2.3 ACTUALIZACIONES DE SOFTWARE
5.2.3.1 VPN de Sistemas Operativos

Las actualizaciones de software pueden ser un proceso de múltiples pasos que probablemente necesiten soporte de varios fabricantes. En la configuración tenemos un sistema operativo que contiene una cierta revisión de software y una revisión de corrección determinada específicamente para ese sistema. Después añada a eso el código de cortafuego actual, junto con su última revisión de corrección. Después viene el software de VPN, el cual puede agregarse al producto de cortafuego o como un programa al sistema operativo. Considerando que este cortafuego/VPN es un producto de seguridad debería protegerlo con contraseña o implantar un proceso de autenticación de factor dos que añada de nuevo otra capa al dispositivo. Ahora agregue cualquier tipo de supervisión de dispositivo, filtrado de contenidos web y software de detección de intrusiones o antivirus. Con todo esto se puede ver cuántas piezas de software deben estudiarse y examinarse.

Es bien sabido que todos los sistemas operativos, en alguna ocasión, presenten un problema con los aspectos de seguridad. Ahora tome todas esas capas de software y trate de imaginar todos los aspectos de seguridad y comunicación posibles que le conciernen a cada una. Piense en todos los puntos vulnerables que cada una de ellas puede presentar.

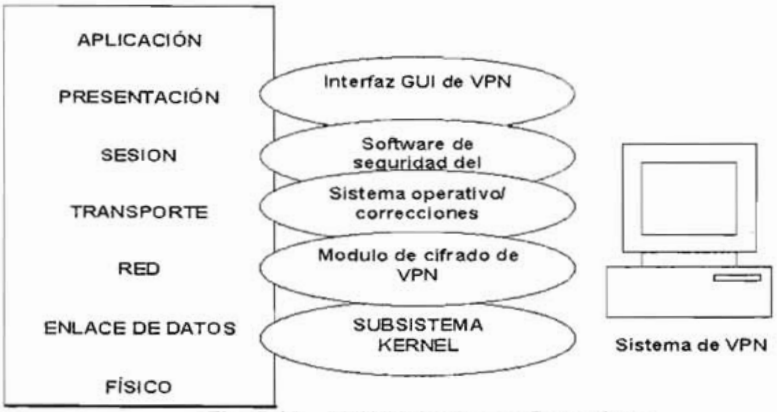


Fig. 5.10 VPN de Sistemas Operativos

En la figura 5.10 cada aplicación yace encima de la anterior; por consiguiente, si usted analiza una aplicación debe pensar en la que se encuentra inmediatamente arriba. Con un servidor típico, si existe incompatibilidad puede dar marcha atrás a la actualización, llevar al sistema fuera de línea. Con los servidores de seguridad, debemos enterarnos inmediatamente, a menos que deseemos darle a alguien una oportunidad para introducirse a la red.

5.2.3.2 VPN de caja negra

Al utilizar las VPN de caja negra se enfrentará a un arma de doble filo. Primero el s.o. subyacente es propietario, lo cual significa que usted probablemente no será capaz de añadir ninguna característica a menos que el proveedor la soporte. Esto no implica que los proveedores no tratan de soportar las características principales que los clientes desean, sino que es posible que no estén soportados todos los requisitos que usted tenga, así que primero debe establecer sus requisitos. También puede tener un conocimiento limitado acerca de la seguridad del sistema, los puntos vulnerables, los agujeros y los problemas de sobre flujo del búfer. Además, debe basarse en los fabricantes para obtener la información necesaria sobre seguridad de próxima aparición, y después realizar las actualizaciones y correcciones disponibles para ese sistema.

5.2.4 Soporte telefónico

El soporte telefónico es otra más de aquellas cosas en las que no se piensa hasta después. Lo que sucede el 80% del tiempo es que usted se decide sobre un producto de VPN y prepara los procedimientos y requisitos necesarios para el producto. Contrata a un experto o instala el sistema usted mismo y posteriormente pone en funcionamiento el dispositivo. Lo configura para un par de características y después se olvida de ello y se concentra en hacer otras tareas de red y del sistema. Finalmente, cuando necesita añadir otra característica crear túneles adicionales o implantar algunos procesos de autenticación de usuarios o de seguridad en su dispositivo VPN, su soporte telefónico gratuito por 90 días ha expirado o su consultor se ha ido ya que la tarea se ha completado.

5.2.5 Servicio de ayuda para resolver problemas de los usuarios remotos

Piense en la funcionalidad del servicio de ayuda para resolver problemas que tiene actualmente implantado. Normalmente sus usuarios se encuentran dentro de un rango geográfico cercano a los cuales puede llegar fácilmente y resolver sus problemas. Pero con los usuarios remotos debe dictar por teléfono los pasos que necesitan seguir. Por lo general, cuando llegue a la máquina de un usuario, observará los archivos de configuración, la instalación, etc., y tendrá que guiar a los usuarios a través de todos estos pasos y ser paciente. Esto significa que su organización deberá capacitar a su personal sobre cómo manejar esas funciones.

5.2.6 Aspectos de compatibilidad

En la instalación de su VPN puede tener muchos protocolos en su red y en sus sistemas operativos individuales. Generalmente en muchas organizaciones existen algunas formas de tipos de tráfico IP, IPX, SNA y NETBIOS entre otros. Debe decidir desde el principio si necesita encapsulamiento y/o cifrado y averigüe si su proveedor lo soporta.

Algunos PSI bloquean los paquetes cifrados de tal forma que en la resolución de este tipo de problemas puede ser apropiado involucrar al PSI. Además, si desea máquinas individuales para utilizar la funcionalidad de cifrado, puede necesitar controladores instalados en su sistema operativo. Si tiene una máquina de escritorio que viene con un tipo de cifrado de pila PPTP y desea utilizar algún otro tipo (por ejemplo DES o 3 DES), necesitará cargar algún software para implantar este esquema de cifrado.

5.2.7 Supervisión

La supervisión es un elemento crítico del proceso de VPN general y puede causar dificultades en la implantación. Sólo piense en la cantidad de tráfico que va a pasar por este dispositivo. Al estudiar la ubicación puede ver el flujo de tráfico que es probable que tenga que supervisar. Ahora considere qué tipo de tráfico desea supervisar: ¿Sólo el tráfico VPN o todo el tráfico que fluye a través del dispositivo?. Todos los dispositivos VPN ofrecen capacidades de supervisión, pero algunos ofrecen "el registro de todo el tráfico" y otros ofrecen "sin registro de tráfico. Si un proveedor incrementa una caracteristica con la cual usted puede supervisar sólo algunos tipos de tráfico, esto significa que el dispositivo tendrá que observar todo el tráfico y examinarlo, lo cual implica que todo el tráfico, incluyendo SMTP, DNS, http y VPN, se supervisará y almacenará en alguna parte.

5.2.8 Alertas

Todos los eventos registrados pueden desencadenar una alerta, pero es importante distinguir los distintos tipos de alertas. ¿ La alerta está causada por alguien que trata de interferir con el dispositivo?. Si éste es el caso, ¿Qué tipo de tráfico se está utilizando?.

Algunos dispositivos VPN soportan SNMP y aunque ha existido durante mucho tiempo, no soportará todas las capacidades requeridas para disparar con éxito alertas críticas para un empleado administrativo a cargo de la seguridad. Esto probablemente obliga a que una política de reglas establecida en un cortafuego emita una alerta de algún tipo sobre los paquetes denegados. Si usted instala un servidor RADIUS, ¿cuándo desencadenará RADIUS las alertas?, por ejemplo, ya sea por una contraseña incorrecta o un nombre de usuario erróneo. ¿Qué hay respecto a alguien que trata de enviar datos cifrados y omitir el cortafuego al mismo tiempo?. Todas estas alertas pueden dispararse desde RADIUS, pero usted también necesita ser advertido del tráfico que incluso no llega tan lejos. Además si esta utilizando un cortafuego, el cortafuego denegará el tráfico y puede provocar alertas en alguna parte. Es fácil ver como las alertas se pueden volver monstruosas. La emisión de alertas es un problema grande y hay muchos productos que emitirán alertas, enviarán mensajes de correo electrónico, enviarán una página, etc.

5.2.9 Registro

Mientras que la emisión de alertas es importante para cualquier organización, el registro es la característica más importante que se puede instalar. ¿Cómo sabe que uno de sus servidores está siendo penetrado por un intruso o si su servidor de correo se está utilizando para retransmitir el correo?. La respuesta es simple, usted no lo sabe, al menos no directamente. Si algo está saliendo mal (no está llegando al exterior o no está obteniendo ningún correo), lo más conveniente es investigar. Por lo tanto, los registros son los que cuentan la historia: quién, qué, dónde, cuándo, pero no porqué. Con el registro podemos regresar y ver que ha sucedido, quién puede ver los horarios, porqué dirección IP entraron y qué servidor fue al que intentaron atacar. Aun si falsificaron su dirección IP, puede decir de cuál PSI viene y al menos el PSI puede intentar ayudarle.

5.2.10 Correlación de eventos

¿Todas las alertas que usted ha obtenido indican un patrón o si está sucediendo algo serio?, ¿La alerta es causada por alguien que crea una ruta o utiliza ping extendido?, ¿Está observando el tráfico?, ¿Vienen en tráfico UDP o TCP?, ¿Intentan establecer una conexión en el puerto 25, lo cual es una indicación de que alguien puede estar intentando fisgonear en su servidor de correo?. Cuando usted se conecta a una red pública, debe esperar todo tipo de tráfico. Quizá alguien que está resolviendo un problema en un extremo tiene su dirección IP por alguna razón y usted piensa que está intentando penetrar en su red. Todas estas condiciones desencadenarán alertas y si alguien comienza a obtener cientos de alertas al día, naturalmente las cerrará. Ningún técnico altamente capacitado que pueda comprender e implantar una VPN se sentará y verá las alertas durante todo el día. Necesita establecer un paquete de correlación que se encargue de estas alertas potenciales, que las procese en forma lógica y que emita una alerta a un servicio de ayuda para resolver problemas con la condición de error. Existen varios paquetes buenos que tomarán como alertas de entrada lo que usted defina y asigne como medida.

5.2.11 Cifrado y encapsulamiento

El cifrado es el proceso de codificar un paquete de datos para transportarlo a través de Internet o de alguna otra red. El encapsulamiento es el proceso de tomar algún tráfico que no es IP y encapsularlo en un paquete IP, el cual puede o no cifrarse. El termino "túnel" se utiliza con frecuencia, he encontrado túnel haciendo referencia a un modo de encapsulamiento para paquetes IPX, SNA y los que no son IP, o empacados dentro de la porción de datos de un paquete IP.

5.2.12 Administración de claves

La administración de claves abarca el proceso de asegurar, generar, distribuir y almacenar claves. Las claves son los mecanismos de seguridad subyacentes en la tecnología VPN, así que se requiere un método muy seguro para garantizar su protección. Aunque los sistemas de claves privadas son más seguros, también son menos flexibles debido a su naturaleza. Las claves públicas que son muy flexibles también necesitan protección de seguridad. Con los sistemas de claves públicas su dispositivo VPN está tomando una clave pública desde otro dispositivo creyendo que de hecho es la clave pública para ese dispositivo. Aquí es donde las autoridades emisoras de certificados entran en juego; responden por esa clave de una manera muy parecida a lo que un notario público hace con su firma.

5.2.13 Generadores de números aleatorios

La seguridad de las claves que se utilizan en el cifrado depende de un generador de números aleatorios que añade seguridad a la clave. Los intrusos tratarán de encontrar un patrón en el texto cifrado para poder adivinar la clave. Al igual que con las contraseñas, la gente es predecible cuando genera claves. Por esta razón , los generadores de números aleatorios se utilizan de tal forma que no se establezca ningún patrón.

Los mejores generadores de números son aquellos que imitan a la naturaleza, un zumbido o una interferencia estática eléctrica. Este tipo de cosas es completamente aleatorio por naturaleza.

5.2.14 Certificados

Los certificados son documentos digitales que dan fe de la identidad de una clave pública y de la identidad de esa persona. Ayudan a validar una firma digital y aseguran que esa persona no esté suplantando a alguien más. Pueden ser jerárquicos de naturaleza donde una autoridad emisora de certificados valida a otra autoridad emisora de certificados. La norma aceptada internacionalmente para certificados es ITU-TX.509.

5.2.15 Actualización de la seguridad

La seguridad será el principal elemento de mantenimiento en la VPN, debe mantenerse actualizado sobre las últimas alertas de seguridad, los boletines de los proveedores, las acciones correctivas sugeridas y lo que está sucediendo en el mundo real. Debe mantenerse actualizado respecto a la seguridad debido a que ésta cambia constantemente.

5.2.16 Soporte para actualizaciones importantes

Suponga que con el fin de implantar una VPN se decidió utilizar los enrutadores existentes y ahorrar costos. Por lo tanto, necesitará asegurarse de que el individuo que instala el software de VPN conozca la tecnología del enrutador y sepa cómo resolver los problemas cuando el equipo falle. Ahora se tiene ya un problema de VPN o un problema de enrutador. ¿Qué sucede si decide añadir conmutadores de VPN en toda la organización?. Eso representa un impacto importante en el diseño de red, ya que está añadiendo dichos dispositivos justo antes de sus puntos de acceso a Internet. ¿Puede agregar estos conmutadores de VPN?, ¿Ínter operarán con su equipo existente?, ¿Los enrutadores necesitarán actualizarse para soportar cifrado o la carga será un problema?

5.2.17 Protocolos para establecimiento de túneles

Los tres protocolos principales para el establecimiento de túneles son: IPSec, PPTP y L2TP ¿Por cuál se decidirá y cuándo desea usar cada uno?. ¿Desea obtener una implantación que combine los diferentes tipos de protocolos? Dependiendo de su arquitectura interna y de sus equipos de escritorio, es posible que no desee o que no pueda soportar los distintos tipos disponibles. ¿Qué nivel de soporte tendrán los productos de un proveedor para cada protocolo para establecimiento de túneles y, cuando se terminen las normas, su equipo será actualizable?.

5.2.18 Dispositivos de administración

Es aconsejable contar con la capacidad de administrar sus dispositivos VPN desde una ubicación central. No obstante, tenga en mente que no todos los productos de VPN soportan características de administración centralizada. Por ejemplo, considere la forma en que actualmente configura y envía un dispositivo VPN a un edificio de oficinas distinto. Es probable que incluya instrucciones sobre cómo instalarlo o que lo configure en forma manual y transporte el dispositivo a ubicaciones geográficamente distintas dentro de sus organizaciones.

Normalmente se tienen una o dos formas en las cuales puede modificar y resolver los problemas del dispositivo. Puede crear un túnel a través de la red pública para configurarlo, lo cual implica que el proveedor le ha dado la opción de instalar un túnel de administración con base en algún algoritmo de cifrado estándar.

O debe ser capaz de conectar un módem al puerto de consola de ese dispositivo para administrarlo. Aquí simplemente ha abierto un problema de seguridad al añadir un módem en un dispositivo de seguridad. Necesita considerar el tipo de MODEM que utilizará, un modelo estándar listo para configurarse o algún tipo de módem de seguridad que cifra los datos entre los módems. ¿Estos módems son seguros?, ¿Se han probado?, ¿Confía en ellos?.

5.2.19 Rendimiento

La organización debe definir el rendimiento antes que el proveedor de VPN o el PSI aborden el tema. Al igual que con un automóvil,¿es el consumo de gasolina por cada kilómetro o la aceleración lo que definen el rendimiento?, ¿Cómo se define el rendimiento, por el tiempo de inactividad, la latencia, la utilización, el número de túneles creados?. En algunas estadísticas, el desempeño es el número de ciclos por segundo que su dispositivo VPN puede proporcionar, esto puede pensarse como el número de conexiones de túnel simultaneas, o el caudal de procesamiento medido por el número de usuarios por segundo. Cuando se coloca una medida precisa en el rendimiento al menos se cuenta con una prueba de evaluación comparativa para juzgarlo. Probablemente pueda obtener estadísticas sobre el rendimiento de su dispositivo VPN pero, ¿son comprensibles?, ¿Cómo se relacionan con el número real de usuarios que pasa a través de su VPN, conducto, túnel y así por el estilo?.

5.2.20 Calidad de servicio

¿Cómo puede un proveedor de VPN definir la calidad de servicio? Anteriormente se mencionó que la calidad de servicio se define por la latencia, el tiempo de inactividad de la red y el ancho de banda. Puede obtener garantías de ancho de banda por parte de su PSI. De su proveedor de VPN puede obtener el ancho de banda disponible del dispositivo en sí. Además, puede obtener garantías de tiempo de inactividad de la red por parte de su PSI y éste probablemente generará informes semanales si se desea. Lamentablemente la latencia no puede garantizarse a menos que utilice la columna vertebral de su PSI local. Si usted viaja fuera de la columna vertebral de su PSI, se introduce en la red de alguien más con sus propias medidas de rendimiento y configuración. Por supuesto, puede pedirle a su PSI información del historial respecto a la latencia y darse una buena idea de la probabilidad de los problemas de latencia futuros, pero cuando mucho son sólo cálculos aproximados.

5.2.21 Trabajo calificado

El trabajo calificado siempre es el valor más ignorado en cualquier organización. Mientras que usted está leyendo todas las cosas que debe considerar para el mantenimiento, tal vez ni siquiera haya pensado en los empleados técnicos. Así que a menos que tenga empleados sumamente motivados, hábiles técnicamente y que disfruten su trabajo, está exponiéndose a dolores de cabeza mayores.

5.3 Tiempo de vida de una VPN

Las VPN's pueden constituirse sólo cuando sean necesarias, o se constituyen por un determinado periodo de tiempo. Las organizaciones deben decidir el modelo operacional que necesitan, ya que cada modelo tiene un juego distinto de atributos de seguridad que la organización tiene que administrar.

En el caso de una VPN "puntual", en la que la VPN existe sólo durante el tiempo de transferencia de la información, la organización generalmente define un juego de políticas de acceso de usuario que dicta mecanismos de autenticación de usuario, restricciones de ubicación física para el usuario y tipo de información que puede ser transferida. El caso típico es el del usuario itinerante que se conecta para recuperar su correo, etc. En este caso generalmente existe un solo usuario para una determinada VPN.

En el caso de una VPN establecida permanentemente, o semi permanentemente, que generalmente vincula dos oficinas, probablemente existan múltiples usuarios ya que las dos oficinas comparten la misma LAN. En esta situación, pueden ser necesarios niveles adicionales de control para que algunos usuarios accedan a cierto tipo de información.

Una VPN activa no utilizada es una puerta abierta a cualquier persona malintencionada que desee atacar la organización, por lo que una norma de seguridad es minimizar el tiempo de vida de una VPN activa.

Entonces, vemos que el tiempo de vida de una VPN debe minimizarse para así satisfacer los requisitos comerciales.

5.4 Ataques a la seguridad de las VPN

Como podremos darnos cuenta hasta este punto, las VPN son más un marco de referencia que cualquier otra cosa, y dicho marco es lo que permite que una compañía utilice a Internet como un valor de negocios. Las oportunidades de negocios, los mercados, etc., se abren por el uso de la tecnología VPN, sin embargo, también resulta importante el abordar temas en cuanto a los aspectos de seguridad de las VPN, por ello en este apartado se verán los diversos tipos de ataques a las VPN.

Las Redes Privadas Virtuales y la política de seguridad son puntos en común. Existe una creencia generalizada entre las organizaciones que el uso de tecnologías de VPN protege de ataques. Si bien, esto es parcialmente verdad, ya que los ataques de terceros en una VPN establecida son difíciles, una VPN es en realidad un tubo a través del cual fluye la información sin vigilancia. Son estas dos últimas palabras las que infunden miedo a los ejecutivos de la seguridad corporativa.

5.4.1 Ataques de algoritmos criptográficos

Los algoritmos criptográficos son vulnerables y se encuentran sujetos a los ataques del mismo modo que cualquier otro software o hardware que se pueda tener en la red. Ahora bien, generalmente son tres las formas de atacar un algoritmo criptográfico:

- Ataques contra el Protocolo
- Ataques contra el Algoritmo
- Ataques contra la implantación

Estos tipos de ataque pueden llegar a dañar o debilitar el sistema, por ejemplo, los algoritmos de cifrado y los protocolos de intercambio de claves no garantizan necesariamente la seguridad por si mismos, y seleccionar una semilla insegura para la clave en la cual se basará, destruye la integridad del protocolo. Así también, el uso de claves débiles, es decir, el uso de una cantidad insuficiente del tamaño de datos y la alteración de las funciones de transformación del código, contribuyen al debilitamiento del sistema.

Si bien, uno de los principales problemas con los ataques criptográficos es que es posible que uno no esté conciente de que ha sido atacado. Al utilizar niveles de seguridad múltiples decimos que puede confiar en que sus datos llegarán seguros, a pesar de ello como ya hemos mencionado, al igual que los ataques contra otros sistemas, los algoritmos criptográficos están sujetos a los ataques. Aquí mencionamos sólo algunas de las categorías más comunes de ataques de algoritmos, siendo éstos: los ataques de sólo texto cifrado; de texto simple conocido; de texto simple seleccionado; de texto cifrado seleccionado; ataque de intermediario; de sincronización; de fuerza bruta; criptoanálisis diferencial, entre los más significativos.

Es importante conocer los diferentes tipos de ataques, por lo que recomendamos estudiar más a fondo este tema, ya que todo lo relacionado con la seguridad es de suma importancia para el momento de la toma de decisiones, y así lograr la implantación de una VPN segura. Por nuestro lado solo trataremos los ataques a los protocolos de seguridad IPSec y PPTP, debido a que son los dos protocolos más importantes, puesto que cada uno de ellos es un marco de referencia para lograr una VPN. Ni PPTP ni IPSec hacen cifrado, ninguno de los dos ofrece seguridad de paquetes de datos. Así que si fuera a ocurrir un ataque, se llevaría a cabo en la base de estos marcos de referencia.

5.4.2 Ataques al protocolo de seguridad de Internet (IPSec)

Este protocolo de seguridad no es un algoritmo de cifrado y tampoco es un algoritmo de autenticación. IPSec es un paradigma en el cual otros algoritmos protegen datos. Pero al igual que cualquier otro protocolo de seguridad, IPSec puede ser atacado y amenazado. Los principales tipos de ataques que llegan a ocurrir en este protocolo, son aquellos que se encuentran en la categoría de ataques contra la implantación. Otros tipo de ataques a este protocolo de seguridad, son los que se mencionan a continuación:

- *Ataques de Implantación*
- *Ataques de Administración*
- *Ataques de Recuperación de claves/leyes de Exportación*
- *Ataques de Administrador y de Comodín*

Una deficiencia de IPSec, es que solo soporta un conjunto muy pequeño de algoritmos y protocolos en su escenario predeterminado. Con el propósito de que IPSec se vuelva una identidad administrativa de corriente principal, tendrá que incluir más soporte, como el soporte para cliente, LDAP y múltiples algoritmos de cifrado predeterminados, así como soporte para otros mecanismos de autenticación como las tarjetas inteligentes y de señales. Hasta ahora IPSec sólo soporta firmas y certificados digitales. También tendrá que incluir un mayor soporte para los navegadores y equipos de escritorio con el fin de continuar haciéndolo una verdadera norma Internet interoperable. Lamentablemente, la flexibilidad y la seguridad se sacrifican. Los negocios no desean soportar muchas plataformas y protocolos de seguridad diferentes, pero intentar usar solo una plataforma y un protocolo aumenta el riesgo.

5.4.3 Ataques de protocolo de establecimiento de túneles punto a punto (PPTP)

Básicamente el protocolo PPTP sufre ataques en la categoría de implantación. Si bien, se puede argumentar que el protocolo punto a punto es bueno, pero aparentemente la implantación de Microsoft necesita mejorar como cualquier otro algoritmo criptográfico.

La VPN de PPTP de Microsoft está formada por varios componentes y de manera similar a IPSec, PPTP es un marco de referencia. No exige los algoritmos de cifrado y autenticación, esto se deja a los protocolos como: PAP, CHAP y MS-CHAP.

El protocolo punto a punto se emplea para asegurar las conexiones PPP a través de TCP/IP, lo cual se logra estableciendo una conexión de VPN del cliente al servidor, ya sea mediante una conexión de un PSI por marcación o directamente a través de Internet. PPTP encapsula los paquetes PPP, quienes a su vez son encapsulados en paquetes de "Encapsulamiento de Enrutamiento Genérico" (GRE). PPTP crea una instalación de conexión y controla el canal al servidor PPTP sobre el puerto TCP 1723. Además esta conexión no se autentica en ninguna forma.

Un punto vulnerable de PPTP, es que éste se basa en PPP. Antes de cualquier comunicación, PPP establece e inicializa los parámetros de comunicación y debido a que no tiene autenticación contra estos paquetes, pueden ocurrir ataques como los de intermediario y de falsificación.

5.4.4 Otros ataques

Existen otros ataques que no entran dentro de la categoría de negación del servicio pero que pueden llegar a obstaculizar la capacidad que tiene una compañía para dirigir sus negocios. Dentro de dichos ataques encontramos los siguientes:

- *Caballos de Troya.*- Este es un programa sin autorización oculto dentro de un programa legítimo, el cual ejecuta funciones desconocidas para el usuario. Generalmente están diseñados para encontrar información vital sobre un sistema o usuario. Cuando un programa legítimo ha sido alterado con la colocación de código no autorizado dentro de él, se considera un caballo de Troya.
- *Ataques remotos.*- Estos son ataques provenientes de otras máquinas. Tienen éxito debido a que la víctima por lo general proporciona la información para ser atacada en primera instancia. Utilerías como *host, finger, whois, showmount y rpcinfo* entre otras, pueden darle a un agresor la información más importante sobre la víctima y con ello el agresor es capaz de intentar desde forma remota cualquier tipo de amenaza que sea posible en esa máquina.
- *Ataques basados en Telnet.*- Telnet es una utilería diseñada para la comunicación simple. Si bien funciona a la perfección para lo que fue diseñada, no obstante, las consideraciones de seguridad nunca se integraron a Telnet.
- *Ataques de Aniversario.*- Este es un tipo de ataque de Fuerza Bruta en una función de transformación del código criptográfica, como MD5. Básicamente intenta encontrar dos mensajes que produzcan el mismo valor de transformación del código, provocando una colisión. Se le llama de Aniversario ya que el ataque se demuestra por lo general mediante el uso de una población. Reconoce el hecho de que es más fácil encontrar un conjunto de pares que coincidan, como la fecha de nacimiento, que un elemento individual.

5.5 Tecnologías Emergentes para las VPN

Hoy en día, la tecnología se ha vuelto cada vez más pequeña y más veloz, pero aún se basada en la tecnología de silicio. No obstante, en un futuro muy cercano se espera veamos computadoras basadas en fotones (partículas más pequeñas de la luz) y en cuantos (los bloques de construcción de los átomos). Logrando así que dichos desarrollos cambien el rostro de la tecnología, donde todos los dispositivos que existen y todos los algoritmos escritos tendrán que pensarse de nuevo y estudiarse de una manera diferente. Las velocidades increíbles y el poder de la computación que resultarán serán enormes.

A pesar de esto, mientras que los cambios pueden traer cosas buenas, también están aquellas cosas que nunca se van. Así por ejemplo, están las regulaciones gubernamentales que persisten y en lugar de facilitar el uso de las VPN, es posible que lo hagan más difícil. Aún cuando intentan proteger al público, tratan de imponer una política común para todos, lo cual simplemente no funcionará en el futuro.

Las amenazas y los ataques también van en aumento, ya no sólo una persona ataca un sitio, sino que ahora tenemos grupos de agresores que atacan varios sitios. La mayoría de los sistemas que se diseñaron para prevenirse en contra de los ataques tiene en mente el modelo de un solo agresor. Por lo tanto, se necesitarán desarrollar nuevas formas de pensamiento y nuevos sistemas para abordar las nuevas amenazas.

5.5.1 Avances en la computación

Uno de los mecanismos más seguros detrás de las redes privadas virtuales es la solidez de los algoritmos criptográficos en los que se basan, si bien dichos sistemas son seguros, pero lo que se busca es forzar los sistemas criptográficos creando nuevas formas de computación, estos sistemas ya se encuentran en desarrollo, sólo basta de tiempo antes de que estén listos para su producción.

Así pues tenemos la ***Computación de Cuantos***, la cual se basa en el comportamiento de átomos individuales, donde en lugar de tener dos estados (1 o 0), cada qubit (equivalente de cuantos a bits de computadora) estará en una superposición de estados. Por lo tanto, un qubit puede ser una superposición de los dos estados, y debido a dicha superposición lineal, se lleva a cabo un fenómeno conocido como paralelismo de cuantos, lo cual permite que una cantidad exponencial de cálculos se efectúe simultáneamente, incrementando así la velocidad de la computación.

Otro ejemplo es la ***Computación Fotónica,*** donde los sistemas fotónicos intentan aplicar la tecnología láser a la computación electrónica convencional existente, permitiendo con ello se presenten varias ventajas sobre la contraparte electrónica en cuanto aspectos de velocidad, costos, calor, ancho de banda e interoperabilidad.

5.5.2 Avances en los sistemas criptográficos

Algunos de los avances en la tecnología de la computación, como la computación Fotónica o la de Cuantos, provocará un cambio importante en la forma en que pensamos sobre las computadoras y en el poder que proporcionan. Todas las aplicaciones que se han escrito para la forma convencional de hacer programación cambiará, ya no serán simples cambios de estado, los programadores tendrán que lidiar con una manera totalmente diferente de ver a las computadoras y el poder que tienen.

Así pues, tenemos la Norma de cifrado avanzado (AES) que está desarrollando el Instituto Nacional de normas y tecnología de Estados Unidos (NIST), la cual busca remplazar a DES por este nuevo algoritmo del siglo XXI. Por lo que permanece en la búsqueda constante de una nueva cifra de criptografía que resulte de carácter público, es decir, un algoritmo que todos puedan utilizar, evaluar y analizar. Es por ello que el NIST abre una convocatoria para evaluar diversas propuestas y encontrar su óptimo, para esto, dichas propuestas deben cumplir un conjunto de requisitos mínimos, siendo:

1. "El algoritmo debe implantar la criptografía de clave simétrica (secreta)".
2. "El algoritmo debe ser una cifra de bloque".
3. "El algoritmo deberá ser capaz de soportar combinaciones de bloque-clave con tamaños de 128-128, 192-128 y 256-128 bits. El algoritmo propuesto puede soportar otros tamaños de bloques-clave y combinaciones, y tales características se tomarán en consideración durante el análisis".

Mientras se evalúan y consideran las nuevas propuestas, algunos se preguntan si es una pérdida de tiempo, y si el NIST será capaz de implantarlas. Aún cuando las normas del NIST se apliquen a las instalaciones gubernamentales, su uso puede extenderse al sector comercial.

5.5.2.1 Criptografía de curva elíptica

Este es un tipo de algoritmo criptográfico en el que se está trabajando actualmente, donde los criptosistemas de curva elíptica son una forma de criptosistema de clave pública, los cuales pueden utilizar tamaños de clave más pequeños y hacen un uso de recursos de cómputo menos intensivo que sus contrapartes, pero ofrecen el mismo grado de seguridad que los criptosistemas modernos. Además estos criptosistemas también son adecuados para situaciones en las cuales se cuenta con pocos recursos disponibles, como las tarjetas inteligentes. Así también como en todo criptosistema, los de curva elíptica presenta limitaciones, mientras que son más rápidos que otros algoritmos en la generación de firmas, son más lentos para verificarlas.

5.5.3 Private Doorbell

El plan de cifrado llamado "Private Doorbell", es una alternativa a la característica de recuperación de claves propugnada por la Administración Clinton, la cual se aplica al cifrado de red.

El cifrado de resuperación de claves requiere que los usuarios proporcionen la clave de descifrado para el cumplimiento de la ley conforme se requiera. Mientras que en Private Doorbell los datos están seguros hasta que los departamentos de seguridad del estado notifiquen a un operador de red con una orden judicial o con una orden de la corte para descifrar la información. Es decir, con esta tecnología se podría permitir que los administradores de red cifraran mensajes al dejar el enrutador, y cuando se les entregue una orden judicial, descifrarían el mensaje al llegar al enrutador final. Esto sólo es aplicable al cifrado de red y no así al cifrado de usuario.

Algunas compañías que tienen relaciones con Private Doorbell son: *Cisco Systems, con soporte de Ascend Communications, Sun, Novell, Bay Networks, 3Com, Intel, HP, Microsoft, Netscape, Network Associates, RedCreek Communications y Secure Computing.*

Quizá esta no sea la solución total, pero si es un paso en la dirección correcta y alivia algunas de las preocupaciones; aún así un problema con Private Doorbell es qué tan sólido puede ser el cifrado en el enrutador, si los intrusos saben esto, atacarán al enrutador. Vemos que cualquier algoritmo de cifrado es sujeto de ataque, y si la política de una compañía sobre el texto sencillo se impone en la LAN al enrutador Internet, cualquiera que penetre con malas intenciones en el enrutador podrá leer los datos. Más aún, la seguridad del administrador del enrutador es cuestionable. Si los administradores de red pueden descifrar la información, ¿qué pasa si no la descifran ya sea que se les entregue o no una orden de la corte?, por lo que si esto llega a involucrar un proceso de cifrado entre los enrutadores, entonces todas las propiedades asociadas con el cifrado entrarán en juego, como la generación de claves, la administración de claves, la clave secreta y más. Por lo que observamos un panorama no muy bueno para Private Doorbell, además de que este plan de cifrado no hace lo que el FBI o la NSA desean que haga.

5.5.4 Esteganografía

Primeramente diremos que la esteganografía no es criptografía, pero es aplicado a la confidencialidad del mensaje, donde en lugar de cifrar el mensaje, a través de la esteganografía se intenta ocultarlo, esto es, hacer que parezca que no hay mensaje. Entonces, la esteganografía no remplaza a la criptografía, en lugar de ello añade una capa de protección al mensaje. Si un agresor se da cuenta de que hay un mensaje esteganográfico, puede descubrirlo, pero no obstante, el mensaje todavía está cifrado con un algoritmo criptográfico que el agresor aún tendría que forzar.

Al igual que un sistema criptográfico, la solidez debe basarse en la confidencialidad del algoritmo y en la dificultad para aplicarle ingeniería inversa con el fin de descubrir los datos o una clave. Un sistema esteganográfico bien diseñado ocultaría el mensaje tan bien que quien se encuentre con el flujo de datos ni siquiera sabría que se trata de un mensaje.

Actualmente, gran parte de la investigación en los sistemas esteganográficos se ha realizado en sistemas de comunicación analógicos, ya que no ha habido tanto interés en los sistemas esteganográficos como lo ha sido en los sistemas criptográficos, pero no así, creemos que mientras más gobiernos y compañías restrinjan el uso de sistemas criptográficos, habrá un mayor desarrollo comercial en los sistemas esteganográficos.

Las herramientas que utiliza la tecnología de la esteganografía se muestran en la tabla 5. Algunas de ellas tienen funciones criptográficas incrustadas, las cuales son reguladas después por el gobierno de Estados Unidos. Así también, la mayoría de estas herramientas usadas por la esteganografía, emplea un tipo de formatos de imagen JPG, GIF o BMP y formatos de archivos de audio WAV, con lo que es posible ocultar el mensaje original.

Tabla 5 Herramientas que utiliza la Tecnología de la Esteganografía

Herramienta	Descripción
BPCS-Steganography	*Desarrollada por Eiji Kawaguchi en el Instituto Kyushu de Tecnología. Esta herramienta emplea una nueva tecnología esteganográfica que implica tomar el mensaje original y utilizar los planos de bits de las imágenes GIF y BMP.*
Contraband	*Toma un archivo de entrada y lo transforma a BMP de 24 bits.*
Encrypt Pic.	*Un algoritmo de cifrado Blowfish que oculta el mensaje en archivos BMP de 24 bits.*
Gif-It-Up	*Este programa toma los datos y los oculta en una imagen GIF, además ofrece un algoritmo de cifrado de datos.*
Hide and Seek for Win95	*Desarrollada por Colin Moroney, esta herramienta se basa en BMP y fue el algoritmo criptográfico Blowfish.*
In the Picture	*Empleo de múltiples claves, por lo que, es posible crear un mensaje para varios receptores. Oculta los mensajes en imágenes BMP.*
Jsteg Shel	*Desarrollado por Derek Upham. Es un intérprete de comandos para la versión DOS de Jsteg. Oculta los mensajes en formato JPG.*
MP3Stego	*Esta herramienta toma un mensaje y lo oculta en un archivo WAV que está formateado con MP3.*
PgpN123	*Es una pequeña aplicación de correo incrustada en programas de correo como Eudora y Agent. Después de que se cifra el mensaje con PGP, puede alimentarse en un programa esteganográfico.*

Herramienta	Descripción
Scramdisk	*Programa de cifrado que implanta los algoritmos Triple DES, IDEA y Blowfish. Después del proceso de cifrado, esta herramienta tiene la opción de convertir el mensaje en un archivo de audio formateado con WAV.*
Scytale	*Oculta el mensaje en una imagen PCX y elimina el archivo de texto sencillo original.*
Steganos for Win95	*Desarrollado por Deus Ex Machina Communications. Esta herramienta permite varios formatos para ocultar mensajes, como HTML, WAV y BMP. Y una vez que se ha realizado la conversión, eliminará el archivo de texto sencillo original.*
S-Tools4	*Herramienta muy popular la cual soporta imágenes BMP y GIF, y archivos WAV.*
wbStego	*Desarrollado por Werner Bailer. Tiene la capacidad de cifrado y puede ocultar mensajes en formatos de archivo BMP y HTML.*

5.5.5 ¿Cuáles son las nuevas amenazas?

Hasta ahora los ataques han sido los mismos que ocurren en Internet, la única diferencia son las fuentes, donde anteriormente solo un individuo conducía el ataque. Hasta este momento, la estrategia de ataque ha sido centrarse en un desarrollo de patrón en particular, pero en la actualidad pueden existir diversos patrones desarrollándose al mismo tiempo y estar distribuidos en todo el mundo. Así pues, surge una nueva forma de ataque conocida como ***ataque coordinado,*** donde varios sitios privados y gubernamentales son atacados en forma simultánea desde direcciones diferentes en todo el mundo.

Existen tres razones principales por las que pudiera darse esta forma de ataque, siendo:

- *Cautela*, ya que al emplear varias direcciones IP el agresor podría pasar inadvertido.
- *Potencia*, con la presencia de más de un ataque de dirección IP, uno o más sitios permitirán que los agresores realicen una gran cantidad de ataques en un marco de tiempo más pequeño que en ataques tradicionales.
- *Datos adicionales*, en el que al utilizar múltiples direcciones IP, es posible obtener más datos de un objetivo que en un solo ataque normal, e incluso al existir diferentes direcciones, es posible que una IP falle mientras la otra tenga éxito.

Algunos ejemplos de este tipo de ataques coordinados a los que podemos hacer mención son los siguientes:

- *Rutas Coordinadas*
- *Exploraciones de reinicio coordinadas*
- *Problemas coordinados*
- *Sondeo de un cortafuego*
- *Exploraciones DNS coordinadas*

Los cuales resultan preocupantes ya que son ataques que no provienen de una sola fuente, sino por el contrario, ahora diversos agresores parece que comienzan a unir fuerzas y a utilizar su talento para conducir ataques coordinados contra las redes. Esto resulta inquietante, debido a que todos los mecanismos de seguridad de defensa han sido diseñados para ofrecer protección contra los ataques de individuos, al estudiar una dirección IP y determinar si se ha plagiado. Pero ahora, se observan múltiples flujos de datos de diferentes direcciones IP. Es por ello que los proveedores que ofrecen seguridad tendrán que darse a la tarea de examinar estas nuevas formas de ataques y estudiar las características que pueden incorporarse en sus productos para protegerse contra ellos.

5.5.6 Regulaciones gubernamentales

Parecería que la amenaza más grande a su privacidad (la cual incluye a su VPN) será el papel que jueguen los gobiernos, como lo es el de Estados Unidos. Lamentablemente, la necesidad de detener terrorismo y de proteger las violaciones a los derechos de autor, podría tener un efecto negativo importante en cualquier aspecto de la seguridad, incluyendo todos sus dispositivos de autenticación, sus algoritmos de cifrado y sus tarjetas inteligentes. Cualquier cosa que tenga una característica de seguridad está potencialmente sujeta a la regulación, y usted talvez ya no será capaz de evaluar y examinar a fondo ese algoritmo de seguridad. Estas regulaciones se presentan en el Acuerdo Wassenaar, en el que participan 33 países quienes han llegado a producir algunos de los algoritmos criptográficos más importantes desarrollados hoy en día. Así como en el Tratado de la Organización Mundial de la Propiedad Intelectual, diseñado para detener la violación a los derechos de autor en Internet.
En ambos casos, pueden llegar a dificultar que las compañías vendan sus productos de cifrado, y desafortunadamente el Tratado de la Organización Mundial de la Propiedad Intelectual puede deshacer la seguridad existente.

5.5.7 VPN inalámbrica

Esta no es una nueva tecnología, el Sistema Local de Distribución Multipunto (LMDS) es una tecnología inalámbrica que emplea señales de microondas (señales de ondas milimétricas) para enviar datos. Utiliza el espectro de 28 GHz para el envío de voz, video y datos en un diámetro de 3 a 10 millas. LMDS es una tecnología similar al teléfono inalámbrico con superposición de celdas. Puede proporcionar programación de video para múltiples canales, telefonía, video y servicios de datos de dos sentidos. Se ofrece como un reemplazo de instalaciones inalámbricas.

LMDS posee la comunicación de dos sentidos, siendo ésta una ventaja al disponer de un conducto con un ancho de banda enorme y un costo menor al de los servicios tradicionales. Además no tiene problemas con la infraestructura existente, en donde se requiere una línea separada para enlazar las comunicaciones. La velocidad disponible a la que llegan los datos es increíble, algunas indicaciones son para un flujo de entrada de 1.5 Gbps y de salida de 200 Mbps. No obstante esta tecnología también presenta desaciertos, ya que es una tecnología de línea visual, la ubicación del transmisor y del receptor es crítica, debido a que los grandes árboles y otros obstáculos proyectan sombra y las señales LMDS pueden llegar a verse interrumpidas.

LMDS tiene un potencial enorme en la tecnología inalámbrica por lo que los fabricantes comenzarán a promoverla muy pronto. Algunos de los servicios que se ofrecen son redes virtuales, acceso a Internet y servicios de redes privadas virtuales.

CONCLUSIONES

Con el proyecto se pretendió dar una visión amplia de lo que son las redes, vistas en sus distintos tipos de aplicaciones, profundizando en las Redes Públicas y Privadas que nos servirán como base para adentrarnos en el tema objeto de esta tesis. Abarcando los fundamentos de una Intranet, los elementos que la constituyen, así como los beneficios y las limitantes de dicha tecnología. Tratamos de demostrar la importancia de las Redes Privadas Virtuales en el enlace de una Intranet con una Extranet, llevando a cabo el trabajo desde el análisis, el desarrollo, la implantación y el mantenimiento, para que el lector tenga una visión amplia del uso de estas herramientas, y así en su caso poder tomar decisiones.

Como hemos visto, vivimos en un mundo tan cambiante donde la tecnología siempre está a la vanguardia. Hoy por hoy una organización que tenga PCs interconectadas, y que lleven a cabo procesos determinados, implantando y explotando tan importante medio de comunicación, estará alcanzando niveles de eficiencia y efectividad notables, en comparación con aquellas que se rehúsen al cambio. De aquí surge la necesidad de conocer no nuevas tecnologías, pero si tecnologías actuales que permitan proporcionar mayores beneficios a quien las emplee, buscando como principal meta crear grupos de trabajo organizados que permitan llevar al éxito, tanto personal como institucional u organizacional.

" Por ello vemos la gran importancia de que el alumno de la carrera de ingeniería en Computación de la ENEP Aragón se mantenga actualizado en sus conocimientos, donde no basta conocer solo una pequeña área del mundo de las redes, sino por el contrario, con el presente proyecto pretendimos abordar un tema que despertara el interés del estudiante aportándole este material bibliográfico. "

" La instalación de una técnica que permita el exteriorizar la red interna de alguna compañía, implica un análisis previo, que involucra desde la elección de la topología dependiendo de la infraestructura que tenga la institución hasta su configuración, administración y mantenimiento preventivo como etapa final de la misma. Para ello hemos pretendido abordar cada uno de estos puntos, con la finalidad de dar a conocer las etapas que involucra la implantación de una metodología que permita llevar a cabo el proceso de enlace Intranet-Extranet. "

En este proyecto se decidió por el uso de la tecnología de las Redes Privadas Virtuales o RPV´s, para poder llevar a cabo dicho proceso de enlace entre la intranet y la extranet. Se compararon diversos métodos que nos podrían llevar a realizar tal proceso, permitiéndonos así optar por la técnica que a nuestro parecer resultó ser la mas adecuada. Un factor importante que influyó en la elección de la tecnología RPV fueron los bajos costos en comparación con las otras tecnologías, si bien al principio su implantación resulta algo costosa, pero a largo plazo dichos costos pueden llegar a convertirse en grandes beneficios para quien la emplee.

Esta tecnología es, desde su creación noble, pues, además de llegar a salvar la economía de las empresas al utilizar el Internet como su infraestructura, tiene una estrecha comunicación con las personas encargadas de fabricar, almacenar, vender y comprar un producto, es decir, cada una ha participado para que el producto sea el que cubra las expectativas en el mercado .

Las Redes Privadas Virtuales (RPV's) tienen una gran variedad de tecnologías en el mercado, es decir, se puede obtener un implante hecho a la medida, por lo que, siempre existirá una estructura para la compañía que desee lograr mayores ganancias y avances con la competencia. Las Redes Privadas Virtuales han llegado a aligerar a las empresas su situación económica y su necesidad de comunicación, pues en la actualidad la compañía que no cuenta con estas características no contará con un lugar en el mercado.

Este tema además de actual, tiene una gran trascendencia en el estudio de redes, pues la mayoría de las empresas cuentan cuando menos con una Intranet o están tratando de implantarla y además si conocemos como se realiza el enlace con la Extranet, la comunicación se abrirá y la compañía podrá ampliar sus horizontes y abarcar un mayor mercado, así el alumno tendrá un panorama más amplio de la guerra que se vive en las empresas por lograr ser más competitivos cada vez y ofrecer mayores garantías y beneficios en un producto, pues, esta guerra afectará de manera directa al profesionista que saldrá a enfrentarse a ese mundo.

" El estudio de este tema enriqueció nuestros conocimientos en la materia y nos permitió tener una idea más clara de las necesidades del mercado y del grado de competitividad que se requiere al finalizar la carrera e integrarse a la rama productiva. "

BIBLIOGRAFÍA

Como Construir una Intranet
Con Windows NT Server
José Luis Raya Cabrera
José Antonio Moreno Gutiérrez
Antonio López Sastre
Editorial ra-ma
1999

Kit de Recursos de Intranet
Prakash Ambegaonkar
Jesús Sánchez Allende
Pilar Moreno Díaz
Osborne MaGraw-Hill
1997

El libro Oficial de Soluciones Intranet
Utilizando Microsoft Office
McGraw-Hill Interamericana de España, S.A.
Micro Modeling Associates
1999

Así son las Intranets,
Tyson Greer
Microsoft Press
McGraw-Hill
Copyright 1997

Apuntes de la Materia de Redes de Computadoras
De la Carrera de Ing. En Computación impartida en la
E.N.E.P. Aragón por el Ing. José Manuel Quintero Cervantes

Construcción y Administración de la Intranet Corporativa
Ronald L. Wagner & Erick Engelmann
McGraw-Hill Interamericana Editores
Copyrigth 1998

Construcción de una Intranet Corporativa
Steve Guengerich,
Douglas Graham
Mitra Miller y Skipper McDonald
Anaya Multimedia
1997

Intranets, empresa y Gestión Documental
Mariano Siminiani
McGraw-Hill de Management
1997

El Proyecto Intranet
' Del análisis de las necesidades de la empresa a la implantación de soluciones'
Fréderic Alin
Denis Lafont
Jean-Francois Macarty
Ediciones Gestión 2000, S. A.
1997

Intranet como ventaja competitiva, Vía @ Internet
Sep Holz
Traducción: Sistemas de Imagen y Palabra
Ediciones Anaya Multimedia
1997

Intranets usos y aplicaciones
Randy J. Hinrichs
Prentice may
1998

Virtual Private Networks
Charlie Scott
Paul Wolfe y
Mike Erwin
2nd. Edition
O'REILLY

La Biblia de Intranet
Al Servati
Lynn Bremmer
Anthony Iasi
McGraw-Hill
1998

Building an Extranet
Connect your Intranet with vendors and customers
Julie Bort,
Bradley Felix
John Wiley & Sons, Inc
1997

Guía para el Administrador de Redes Privadas Virtuales (RPV)
David Leon Clark
McGraw-Hill
2000

Implementación de Redes Privadas Virtuales (RPV)
Steven Brown
McGraw-Hill
2000