INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

ESCUELA DE TELEMÁTICA

ESTUDIO DE SEGURIDAD EN LOS ENLACES DE BANDA ANCHA, APLICADA A LAS REDES PRIVADAS VIRTUALES.

POR:

ANA PAULINA QUINTANA VILLARROEL

Tesis presentada como requisito parcial para la obtención del Título de:

TECNÓLOGA EN TELEMÁTICA

2003

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Señorita QUINTANA VILLARROEL ANA PAULINA, como requerimiento parcial a la obtención del título de TECNÓLOGA TELEMÁTICA.

_____

ING. RAMIRO YEROVI

DIRECTOR

Latacunga, 19 de Agosto del 2002

DEDICATORIA

El presente trabajo se lo dedico a mis padres y mi hermano porque creen en mi y son quienes están apoyándome incondicionalmente en todo lo que hago.

Ana Paulina Quintana Villarroel.

AGRADECIMIENTO

Durante el desarrollo de mi proyecto de tesis atravesé muchos obstáculos e inconvenientes, sin embargo, gracias a muchas personas que intervinieron para darme una mano y gracias a Dios he llegado hasta este momento con bien y satisfecha de mi trabajo por eso agradezco y encomiendo mi porvenir a Dios para que guíe mis pasos por la vida. Agradezco a mis padres, que han sabido ser pacientes y comprensivos ante tantas vicisitudes, a mis maestros, quienes compartieron sus conocimientos y estuvieron presentes para solucionar problemas no solo académicos sino que también fueron oportunos brindándonos su amistad. Agradezco a aquellas personas y amigos que ayudaron de manera significativa para que esta tesis deje de ser proyecto y se haga realidad.

Ana Paulina Quintana Villarroel

ÍNDICE

CAPÍTULO III

INVESTIGACIÓN Y ESTUDIO DE UNA RED

CAPÍTULO IV

SEGURIDAD DE LA RED

CAPÍTULO V

ANÁLISIS ECONÓMICO FINANCIERO

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

LISTADO DE FIGURAS

CAPÍTULO II: Marco Teórico

CAPÍTULO III: Investigación y Estudio de una Red

LISTADO DE ANEXOS

ANEXO A: Fotografías

ANEXO B: Documentos Obtenidos del Internet

LISTADO DE PLANOS

INTRODUCCIÓN

Una red se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones).

La creación de las VPNs se ha convertido en una alternativa para cualquier organización ya que se pueden beneficiar de las facilidades que presta el Internet. Cada vez en mayor medida, las VPNs transmiten información vital, por tanto dichas redes deben cumplir con atributos tales como seguridad, fiabilidad, y efectividad en costos. Es sabido que las redes reducen en tiempo y dinero los gastos de las empresas, lo cual es una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que a lo largo de este estudio trataremos los famosos firewalls en las VPNs.

Tomemos en cuenta que el creciente uso y popularización de Internet ha ofrecido nuevas oportunidades a operadores, empresas y usuarios finales, que han visto la proliferación de nuevos servicios y aplicaciones basadas en el protocolo IP. Al mismo tiempo, los ISPs están ofreciendo servicios de conectividad cada vez más rápidos y asequibles, desde los accesos ADSL, Cable o Wireless, hasta conectividad Ethernet en redes metropolitanas, gracias al uso de infraestructuras de fibra óptica.

Esta nueva situación y disponibilidad de ancho de banda favorece la aparición de nuevas aplicaciones y servicios, sin embargo las necesidades tradicionales de seguridad siguen vigentes: control de acceso, autenticación y confidencialidad e integridad de la información.

Los sistemas de seguridad deben adaptarse a esta nueva situación, es decir, los sistemas de control de acceso han de tener un rendimiento acorde al crecimiento en ancho de banda.

CAPÍTULO I

1.1. Definición del Problema

Este estudio se ha planteado con el propósito de enfocar un tema trascendental como es la seguridad en las VPNs puesto que representan una gran solución para las empresas en cuanto confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro.

No obstante el problema radica en que primero se deben establecer correctamente las políticas de seguridad y de acceso en las VPNs, de lo contrario, si esto no esta bien definido pueden existir consecuencias serias.

1.2. Objetivos

General

- Estudiar la seguridad en los enlaces de banda ancha, aplicada a las redes privadas virtuales.

Específicos

- Conocer los aspectos básicos y específicos de las diversas tecnologías inalámbricas así como las nuevas tendencias, con especial énfasis en su integración con las redes de sistemas en banda ancha.
- Identificar cómo son las transmisiones de la información en banda ancha.
- Examinar las relaciones entre la velocidad de datos y el alcance de una transmisión en banda ancha.

- Considerar las formas de conectividad y los aspectos de seguridad de las redes inalámbricas en banda ancha.
- Investigar que métodos y técnicas utilizadas por los hackers y sus medidas de prevención.
- Realizar el estudio de una red privada virtual.

1.3. Justificación

Hoy es imposible hablar de un sistema ciento por ciento seguro, sobre todo cuando se trata de comunicación por banda ancha. Desde la aparición de accesos y redes MAN de banda ancha, la demanda de este nuevo servicio ha incrementado y actualmente es muy utilizada por su velocidad de transmisión, por lo que resulta importante el estudio de su seguridad.

Puede ser que el costo de la seguridad total sea muy alto y "por este motivo las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas. La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy limitado les impediría hacer más negocios", "Un riesgo representativo que corre una red privada virtual es atenerse a los daños y perjuicios que un hacker pueda provocar", esto también se ha tomado en cuenta en este estudio puesto que los hackers suelen gastar muchos miles de dólares en equipos para descifrar una encriptación, esta situación es o no posible controlarla?. ¿Cuánto hay que gastar para tratar de evitarlo?. Estas situaciones así como muchas otras muy importantes en la seguridad serán abordadas en este trabajo.

Entonces, existe alguna manera de obtener una buena seguridad y controlar las vulnerabilidades de la red, pero ¿Se logra la seguridad total?. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

1.4. Alcance

En este proyecto, el estudio detallado de la seguridad sobre enlaces de banda ancha en una red privada virtual proporcionará conclusiones definidas y recomendaciones específicas en muchos aspectos de estos enlaces de banda ancha a ser aplicados oportunamente.

CAPÍTULO II

MARCO TEÓRICO

2.1. TRANSMISIÓN DE BANDA ANCHA

Las necesidades han incrementado exponencialmente las demandas de acceso de banda ancha a Internet. Los servicios y aplicaciones como el flujo de audio y el vídeo, las copias de seguridad de sistemas domésticos y el control de la seguridad han llegado al límite de su expansión con el acceso telefónico tradicional. Las soluciones de banda ancha ayudan a llevar a cabo servicios, contenidos y aplicaciones de red de una manera rentable.

Se entiende por red, tecnología o servicio de banda ancha aquel que ofrece una velocidad igual o superior a los 2 Mbits/s (velocidad primaria). A partir de esta velocidad ya es posible ofrecer, con cierta calidad, servicios multimedia e interactivos, que combinen voz, datos e imágenes. Las redes de telecomunicaciones experimentan transformaciones encaminadas a proveer unos servicios más amplios y universales. Así, este cambio se refleja, por una parte, en la infraestructura de la red dotándola de una mayor capacidad de manejo de tráfico –banda ancha- y, por otra, en la aplicación de inteligencia y movilidad a la misma.

La oferta actual de servicios de telecomunicaciones no es más que un pequeño avance de lo que serán los servicios que puedan disfrutar los usuarios en la próxima década; se hace por tanto necesario racionalizar las infraestructuras sobre las que van a desarrollarse estos nuevos servicios.

Ello lleva a organizar las diversas redes en torno a un núcleo común de transmisión**,** grandes centrales de conmutación y ordenadores en donde residan las bases de datos de los proveedores de servicios; además, se necesitará estructuras de accesos flexibles para proporcionar la conectividad entre los usuarios (fijos o móviles) y la red, todo ello controlado desde un centro de gestión.

La red de acceso, la que más directamente se relaciona con los usuarios, presenta la tendencia en las redes fijas a incorporar medios (fibra óptica y comunicaciones por satélite) y tecnologías (por ejemplo ADSL, WDM, etc.) capaces de ofrecer el gran ancho de banda que se requiere para poner en casa o en la oficina todas las nuevas aplicaciones multimedia que los proveedores de servicios están desarrollando, siendo las más significativas el acceso a Internet, video bajo demanda y distribución de señales de TV por cable (CATV).

Pero el acceso por red fija no es el único, y cada día más, los usuarios demandan movilidad para acceder a la red desde cualquier punto; así la radio se ha convertido en el medio por excelencia para este fin. El crecimiento de este tipo de acceso es exponencial y, y si en un principio, se está empleando para comunicaciones telefónicas. Nada impide que lo sea también para las de datos. En la red de transporte los multiplexores constituyen el elemento principal para optimizar lo recursos; la aplicación de la fibra óptica y la incorporación de enlaces de microondas se vislumbra como las tecnologías que facilitarán todo el ancho de banda que se necesite, con la flexibilidad de poder combinar canales y obtener la velocidad requerida.

La conmutación es una parte fundamental en cualquier red, y lo que se exige a los nodos de conmutación es que sean capaces de conmutar más líneas y hacerlo a una mayor velocidad. La tecnóloga ATM (Modo de Transferencia Asíncrono), propia de la RDSI de Banda Ancha, se considera la más adecuada para cumplir estos requisitos y, de hecho, está siendo adoptada tanto para las redes públicas como privadas.

En definitiva, una red digital dotada de un ancho de banda casi sin límites (RDSI-BA), con interfases abiertos, una velocidad de conmutación suficiente para soportar cualquier aplicación y dotada de acceso universal, es la visión que se puede tener hoy de lo que serán las redes de la próxima década.

2.1.1. La RDSI de Banda Ancha (ATM)

La RDSI de banda ancha (RDSI-BA) es el resultado de la evolución dela RDSI (conocida ahora como RDSI de banda estrecha) para soportar mayores velocidades y posibilitar servicios avanzados como la transmisión de vídeo.

Fue en 1988 cuando el CCITT aprobó la primera recomendación para la RDSI-BA. En ella se define la RDSI-BA como “un servicio que requiere canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria”. Se definión ATM(Modo de Transferemcia Asíncrono) como la tecnología de conmutación que utilizaría la RDSI-BA y 155 Mbit/s la velocidad que debía soportar. A pesar de las diferencias entre la RDSI-BA y la RDSI-BE, ambas mantienen muchos puntos en común, ya qye la RDSI-BA es la evolución hacia la alta velocidad de la RDSI-BE.

Algunos de estos puntos son:

- El modelo de referencia para la configuración es similar, ya que la RDSI-BA asumió con algunas modificaciones la RDSI-BE.
- Ambas son de naturaleza conmutada y con conexión, utilizando un protocolo de señalización similar.

2.1.2. Banda Estrecha vs. Banda Ancha

Podemos referirnos a la Banda Estrecha y la Banda Ancha de acuerdo a la velocidad de la línea en sí, o lo que es lo mismo comparar qué tan rápido va la información por ella, de acuerdo a las necesidades que se tiene. No existe definición respecto al límite físico entre la Banda Estrecha y la Banda Ancha: este es un concepto relativo muy técnico. Aun así se puede dar una definición que nos permitirá aclarar el concepto.

a. Banda Estrecha

Dentro de la Banda Estrecha se va a determinar tres elementos claramente definidos:

- En primer lugar se tiene la Red Telefónica Básica (RTB), el teléfono de casa. Son líneas que nos permiten 3000 hz. de ancho de banda, mediante módems analógicos se transportan, sobre líneas analógicas, las señales digitales de los ordenadores.
- En segundo lugar las líneas RDSI, la Red Digital de Servicios Integrados, en los que cada uno posee dos canales de 64 kbps para voz y datos y de otro de 16 kbps para señales de control.

- Y en tercer lugar se va a tener los E1s (2 Mbps), pudiendo ir estos despeinados (separando n canales de 64 kbps los 2 Mbps iniciales), que nos permiten más de 30 líneas para voz y/o datos.

Es decir que dentro de la Banda Estrecha se tiene la RTB, la RDSI y los E1s.

b. Banda Ancha

Y dentro de la Banda Ancha, se va a definir tres nuevos elementos:

- En primer lugar los servicios de Broadcast de TV, que usan por canal 6 Mhz. Nos transportan grandes cantidades de información gracias a la nueva definición de TV digital a calidades y servicios interactivos muy superiores a la TV analógica convencional.
- En segundo lugar se tiene los sistemas de CATV, a 700 Mhz. Son sistemas en comunidades de vecinos que nos permiten, además de servicios de Broadcast, sistemas de ancho de banda para comunicaciones de datos avanzados e Internet.
- Y por último, y en tercer lugar se va a analizar los servicios de capacidad para enviar datos, voz y vídeo a muy alta velocidad. Se trata de aquellos capacitados como mínimo a sustentar servicios de 2 Mbps escalables hasta lo que demande el servicio del cliente, desde E1s y E3s (34 Mbps), hasta Gigabits por segundo.

Como se puede observar, las comunicaciones convencionales que se usan en el sector residencial y de la mayoría de las PYMEs, son Banda Estrecha, de acuerdo a esta definición.

2.1.3. Conexión de Banda Ancha

Las ofertas de conexión a Internet con banda ancha se multiplican y sus tarifas se han reducido hasta el punto de resultar una alternativa más que atractiva para los grandes navegantes. O los navegantes de altura que desean alta velocidad para surcar sin pausa por todas las páginas, incluso cuando están descargando varios archivos, y al mismo tiempo usar el teléfono. Pero, se debe aprender cómo lograr todo ello sin comprometer la seguridad.

La emoción por lograr un acceso de alta velocidad gracias a la conexión de banda ancha hace que muchos de los usuarios pasen por alto las medidas de seguridad adecuadas. Pero el peligro se incrementa en esta situación debido a que en este tipo de conexiones, las conexiones son permanentes, y además se dispone de una dirección IP fija. Factores todos ellos que colocan al Ínternauta en situación de alto riesgo si no se dispone de los medios adecuados.

2.1.4. Acceso y Redes de Banda Ancha

Existen diferentes niveles y tecnologías que constituyen las redes banda ancha, cuyo embrión lo constituyeron las redes cable pero que, actualmente, coexisten con otras tecnologías que permiten un gran ancho de banda, como son fibra óptica y la radio, además de xDSL para arovechar el bucle de abonado existente.

En primer lugar, el significado de la expresión “red de banda ancha” es una red la cual es un conjunto de recursos interconectados entre sí, que gestionados de algún modo, interaccionan para satisfacer las necesidades de los usuarios que la utilizan; por otra parte, el concepto de banda ancha es mucho más extenso que el de todo aquel medio físico que soporta más de un canal de voz.

Los tiempos actuales exigen un concepto de banda ancha mucho más amplio, en el cual se ponga de manifiesto la importancia de ser transparente al usuario, pues éste debe poder acceder a los servicios que tiene asignados sin problemas a través de esa red de banda ancha.

En segundo lugar, la integración adquiere un papel fundamental en el desarrollo actual y futuro de las redes de banda ancha. El concepto de integración debe ser entendido bajo varios puntos de vista: Integración como la variedad de servicios soportados sobre un medio de transporte digital común.

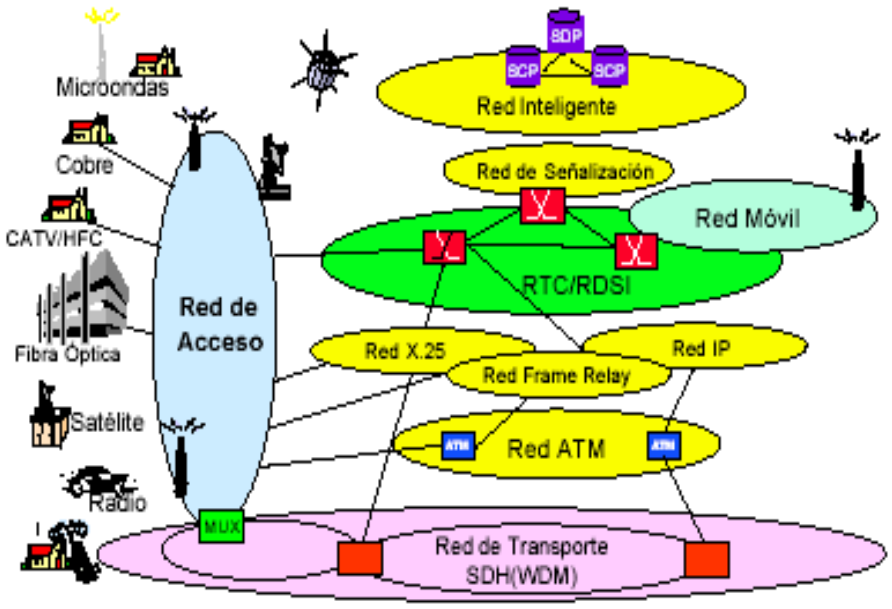


Figura 2.1. Red Completa de Telecomunicaciones

Las interfaces de usuario son los elementos finales de la red en el entorno de abonado que adaptan las señales a interfaces normalizadas de uso extendido, tales como el SetTopBox de las redes de TV por cable.

Así pues, de ahora en adelante identificaremos la interfaz de usuario con el SetTopBox (STB), que de esta forma engloba todas las funciones necesarias en la parte del cliente para hacer visible y controlable la aplicación para el usuario. Se puede decir que el STB es el encargado de codificar y decodificar la información proveniente de usuario (PC, línea telefónica, RDSI,...) o de la parte de la red o bucle de abonado, como son los distintos contenidos multimedia. También realiza funciones de gestión, mantenimiento, señalización y tasación. Las diferencias entre las redes de acceso existirán, al menos, durante un largo período en el que las tecnologías y las estrategias de negocio irán siendo probadas por el propio mercado.

De esta forma, con un mercado tan competitivo en las redes de acceso y en los equipos terminales, los dispositivos de interfaz jugarán un papel fundamental en el permitir que una gran variedad de equipos terminales se conecten a diferentes tipos de redes de acceso.

Un aspecto muy importante en el desarrollo de las redes de banda ancha es el hecho de que los servicios que demanda cada tipo de cliente son bastante diferentes, como lo son también los requisitos que imponen a las redes de soporte. Fundamentalmente, los usuarios residenciales van a enfocarse más a servicios relacionados con el ocio (televisión y juegos de todo tipo) y la gestión doméstica (teléfono, telecompra, etc.), que no van a requerir de la red cantidades de información en el sentido usuario / red que no sean manejables, en la mayoría de los casos, por la actual RDSI de banda estrecha. En cambio, las empresas y organizaciones de todo tipo precisarán de servicios multimedia para la transmisión bidireccional de toda clase de información.

Las exigencias que estas necesidades impondrán a las redes van a ser muy superiores a las que planteen los usuarios residenciales.

2.1.5. Clasificación de las Redes de Acceso

La información se genera a se recibe en un centro –cabecera- a partir del cual ha de distribuirse hasta el usuario final empleando la red tendida. La red telefónica, la de mayor capacidad, en su porción de acceso no se muestra capaz para soportar el ancho de banda que se necesita, por lo que se hace necesario tender otra que sí lo haga.

La red de acceso es la encargada de conectar el equipo de abonado con la red de conmutación de banda ancha.

A la hora de estudiar las diferentes redes de acceso, las clasificaremos en tres grupos:

- Las redes de acceso vía cobre: entre las que destacan las tecnologías xDSL.
- Las redes de acceso vía radio: tales como MMDS y LMDS.
- Las redes de acceso vía fibra óptica: tales como las redes HFC, las redes PON, y las redes HFR.

a. Redes de Acceso Vía Cobre

Dos acontecimientos importantes han impulsado a las tradicionales compañías operadoras telefónicas a investigar una tecnología que permitiera el acceso al servicio de banda ancha sobre sus tradicionales pares trenzados de cobre: *Las nuevas aplicaciones multimedia* y *el acceso rápido a contenidos de Internet.*

Las nuevas aplicaciones multimedia, que generan la necesidad de proporcionar velocidades de banda ancha (en Europa son los servicios por encima de E1, el límite de la RDSI de banda estrecha).

A pesar de que aún no se han logrado estandarizar por completo, los módems xDSL nos ofrecen la capacidad necesaria en términos de ancho de banda para acceder a toda clase de servicios multimedia interactivos a través de los accesos telefónicos tradicionales. En otras palabras, nos permiten convertir el bucle de abonado convencional, hoy utilizado únicamente para conectar el teléfono o un módem de hasta 33,6 kbit/s, en un potente sistema de acceso a los nuevos servicios multimedia o a las redes WAN de banda ancha. El factor común de todas las tecnologías DSL (Digital Subscriber Line) es que funcionan sobre par trenzado y usan la modulación para alcanzar elevadas velocidades de transmisión, aunque cada una de ellas con sus propias características de distancia operativa y configuración.

A pesar que entre ellas pueden existir solapamientos funcionales, todo parece indicar que su coexistencia está asegurada, lo cual obligará a los proveedores de estos servicios a engrandecerse por una u otra razón según el tipo de aplicación que se decidan a ofrecer.

Las diferentes tecnologías se caracterizan por la relación entre la distancia alcanzada entre módems, velocidad y simetrías entre el tráfico de descendente (el que va desde la central hasta el usuario) y el ascendente (en sentido contrario). Como consecuencia de estas características, cada tipo de módem DSL se adapta preferentemente a un tipo de aplicaciones:

- **HDSL (Highbitrate Digital Subscriber Line)**

Es una técnica para transmitir T1 o E1 sobre líneas de pares de cobre trenzados (T1 requiere dos y E1 tres), mediante el empleo de técnicas avanzadas de modulación sobre distancias de hasta 4 kilómetros, sin necesidad de emplear repetidores.

Aplicaciones típicas para HDSL serían para la conexión de centralitas PBX, las antenas situadas en las estaciones base de las redes telefónicas celulares, servidores de Internet, interconexión de LANs y redes privadas de datos.

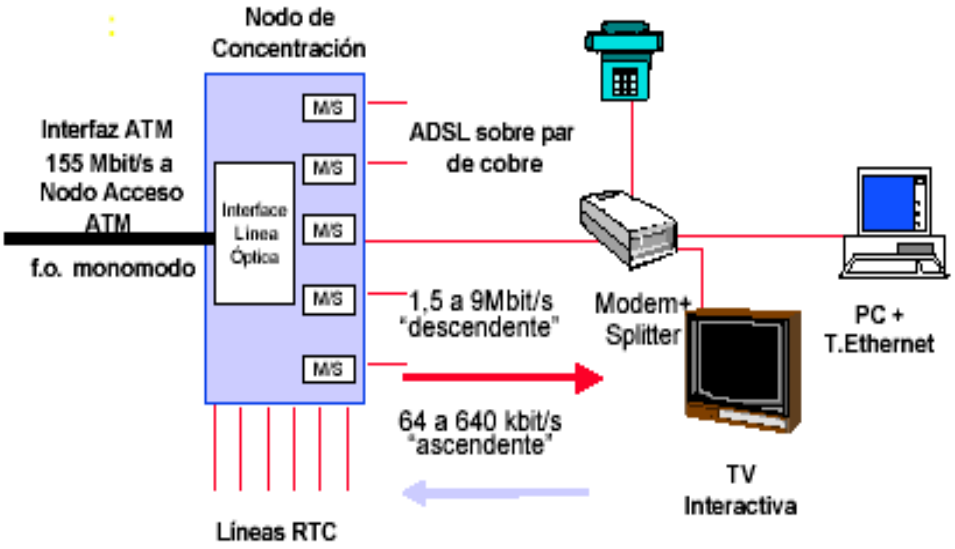


Figura 2.2. ADSL: Datos Asimétricos en el Bucle de Abonado

- **SDSL (Single line Digital Subscriber Line)**

Es prácticamente la misma tecnología que HDSL pero utiliza únicamente un par por lo que se sitúa estratégicamente en el segmento de los usuarios residenciales que sólo disponen de una línea telefónica.

- **RADSL/ADSL (Rate Adaptative/Asymmetric Digital Subscriber Line)**

Esta nueva tecnología ofrece velocidades de acceso mayores y una configuración de canales que se adapta mejor a los requerimientos de las aplicaciones dirigidas a los usuarios privados como vídeo simplex (o TV en modo distribución), vídeo bajo demanda o acceso a Internet.

Las típicas aplicaciones donde se necesitan unos anchos de banda elevados para recibir la información multimedia y solo unos pocos kilobits por segundo para seleccionarla.

- **VDSL (Very High Digital Subscriber Line)**

Esta tecnología, aún en fase experimental, coincide básicamente con ADSL y permitirá velocidades de hasta 52 Mbit/s aunque sobre distancias menores.

En resumen, las técnicas xDSL aumentan la capacidad de transmisión en el bucle de abonado empleando técnicas de modulación avanzadas y módems, sin embargo, tienen serias limitaciones en distancia.

b. Redes de Acceso Vía Radio

Los sistemas vía radio presentan una alternativa clara a las redes de cable para la difusión de múltiples canales de televisión y otros servicios multimedia, ya que soportan interactividad a través de los canales de retorno.

La ventaja clara de este tipo de sistemas es la reducción de los costes de infraestructura, además del pequeño margen de tiempo necesario para su funcionamiento, puesto que en el momento en que se dispone de la antena, se llega inmediatamente a miles de usuarios.

Los sistemas que se presentan y desarrollan en la actualidad para el acceso a los servicios de banda ancha son, fundamentalmente el MMDS (Microwave Multipoint Distribution System) y el LMDS (Local Multipoint Distribution System).

Los dos tipos de sistemas fueron inicialmente utilizados exclusivamente para la distribución de múltiples canales de televisión, en ambos casos como una alternativa potencial a los sistemas de televisión por cable. Ambos han evolucionado, y siguen evolucionando en direcciones diferentes y por motivos también diferentes.

Una de las áreas de mayor potencial en la evolución futura de las telecomunicaciones es la transmisión inalámbrica digital de banda ancha. Idealmente, un sistema inalámbrico de banda ancha que permitirá la transmisión de cualquier tipo de información digitalizada (audio, vídeo, datos) desde cualquier lugar y en cualquier momento, con posibilidad de transmitir en tiempo real de ser necesario. Entre las ventajas de un sistema inalámbrico sobre uno cableado podemos mencionar:

- Movilidad, la cual apoya la productividad y la efectividad con que se presta el servicio.
- Aunque los costos iniciales son mayores que los que supondría un sistema cableado, a lo largo del tiempo los gastos de operación pueden ser significativamente menores.
- Menor tiempo de instalación y puesta en marcha del sistema. La instalación es más sencilla.

- Existe completa flexibilidad en cuanto a la configuración del sistema. Se pueden tener diversas topologías para satisfacer los requerimientos de aplicaciones e instalaciones específicas.

La aparición de un sistema de esta naturaleza requiere la conjunción de varios factores, entre las que podemos mencionar:

- Desarrollo de sistemas de microondas económicos y compactos que operen a frecuencias cada vez más altas.
- Nuevos y mejores modelos de propagación que permitan una mejor predicción de los factores que afectan la calidad del servicio, tales como los efectos de trayectorias múltiples, pérdidas por ocultamiento y atenuación por lluvia, entre otros.
- Desarrollo de "antenas inteligentes" que compensen las variaciones en el canal de transmisión y que minimicen los efectos de la interferencia co-canal.
- Técnicas de modulación robustas que permitan altas velocidades de transmisión con bajo BER en presencia de condiciones adversas.
- Esquemas de enrutamiento apropiados que garanticen cobertura adecuada y al mismo tiempo calidad de servicio

b1. Sistemas MMDS

En la actualidad, la mayor parte de las licencias en la banda MMDS están dedicadas a la transmisión de señales de televisión analógicas, aunque existen excepciones. Es por esta razón que este servicio ha venido denominándose también cable inalámbrico.

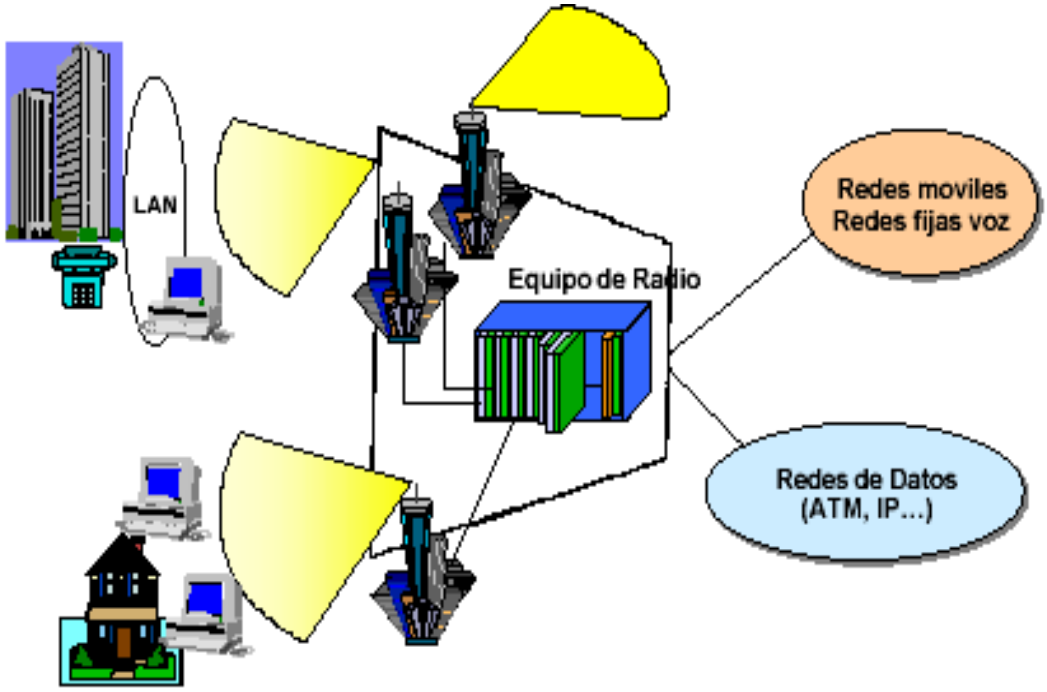


Figura 2.3. Sistema de Acceso Radio de Banda Ancha

MMDS (*Microwave Multipoint Distribution System*, Sistema de Distribución Multipunto de Microondas) es una tecnología inalámbrica originalmente concebida para la distribución de vídeo en aquellas zonas en las que no es factible realizar un cableado convencional. En los Estados Unidos MMDS opera en la banda de 2150 a 2686 MHz, mientras que en otros países se le ha asignado a este servicio un rango que va de 2 a 3 GHz. El sistema transmite vídeo en formato digital; de esta manera, es posible acomodar 5 canales de vídeo con la técnica de compresión MPEG2 y con resolución NTSC (la calidad de video asociada a un canal convencional de televisión) en un canal de 6 MHz.

- **Acceso a Internet de Alta Velocidad Vía MMDS**

La demanda por acceso a Internet crece exponencialmente. Cada vez más y más usuarios obtienen acceso a la Red a través de un proveedor de servicios de Internet (IPS, *Internet Services Provider*) utilizando las líneas telefónicas.

En el mejor de los casos, este esquema ofrece una velocidad de transmisión del orden de los 58 Kbps. Por otra parte, el sistema de telefonía pública conmutada (PSTN, *Public Switched Telephone Network*) está orientado a proveer una conexión bidireccional con un ancho de banda simétrico. Esto representa un desperdicio del ancho de banda disponible, ya que en una conexión a Internet el flujo de información es predominantemente unidireccional. De hecho, la información requerida por el usuario (texto, vídeo, imágenes, audio) puede necesitar un ancho de banda importante, en tanto que la información enviada por el usuario se limita muchas veces a los "clicks" del ratón sobre los ítems presentados en pantalla. Otro factor a tener en cuenta es que las centrales telefónicas están pensadas para manejar el tipo de tráfico originado por las llamadas convencionales de voz, cuya duración en promedio no va más allá de algunos minutos; en contraste una conexión a Internet representa una llamada cuya duración es mucho más larga, pero en la cual el canal es utilizado solamente en los momentos en los que hay intercambio de información.

Una solución a esta necesidad es la utilización de MMDS para proveer acceso de alta velocidad a Internet. Con MMDS, unos pocos canales con un ancho de banda de 6 MHz pueden servir para proveer acceso de alta velocidad a Internet (10 Mbps *downstream*), pudiéndose atender de 500 a 4000 suscriptores por canal.

- **Características del Sistema**

En un sistema MMDS los datos son transmitidos vía microondas utilizando un esquema de multiplexión por división de tiempo (TDM, *Time Division Multiplexing*).

Cada suscriptor dispone de un módem inalámbrico, el cual monitorea la señal recibida en espera de la información dirigida a un usuario particular. Los datos del canal de retorno (U/S, *upstreaming*) son enviados utilizando la línea telefónica, lo cual se ajusta a la asimetría inherente al acceso a Internet. El canal de D/S (*downstream*, información dirigida al usuario) está compartido, por lo que es necesario algún tipo de algoritmo para administrar el empleo del canal por parte de los suscriptores. Este algoritmo puede ser relativamente simple ya que sería ejecutado desde el extremo transmisor sin necesidad de realimentación por parte de los usuarios. Cada canal de 6 MHz podría ser modulado utilizando por ejemplo la técnica 64-QAM (*Quadrature Amplitude Modulation*, modulación de amplitud por cuadratura), lo cual representa una tasa de bits de 27 a 30 Mbps después de la respectiva corrección de errores.

En un sistema de este tipo el espectro disponible está limitado por las disposiciones de los organismos gubernamentales reguladores de las radiocomunicaciones, por lo que es imperativo utilizar algún método que permita aumentar la cobertura sin requerir frecuencias adicionales.

Uno de estos métodos es la *sectorización*, técnica en la cual se emplea un arreglo de antenas altamente direccionales para re-utilizar los canales de RF en una determinada zona geográfica. En este contexto, la re-utilización de frecuencias se refiere al envío de distinta información a diferentes usuarios utilizando varias veces los mismos canales de RF. Por ejemplo, supóngase que se dispone de un arreglo de antenas que permite dividir la zona a cubrir en 6 sectores de 60° cada uno; si se dispusiera solamente de un par de canales A y B, ello permitiría utilizar 3 veces cada canal para transmitir distinta información, lo cual triplica la capacidad de cada canal.

En un esquema de sectorización existirá un compromiso entre el incremento de la capacidad asociado al número de sectores cubiertos y el incremento de la capacidad asociado a la utilización de esquemas de modulación cada vez más complejos, cuya susceptibilidad al ruido e interferencia será cada vez mayor. Cuando se utiliza la sectorización es necesario contar con una adecuada separación entre sectores adyacentes, lo cual puede lograrse utilizando antenas lo suficientemente directivas y polarizaciones alternas. Por lo general, en un entorno libre de obstáculos y de trayectorias múltiples, una aislamiento entre sectores de 30 dB suele dar resultados satisfactorios.

Otra técnica empleada para aumentar el rendimiento del espectro de RF es la *celularización*. En ella se utilizan múltiples transmisores para enviar información a grupos de suscriptores que están geográficamente dispersos; cada grupo de suscriptores se halla dentro de una región o *celda*. El incremento en la capacidad se produce al enviar diferente información de RF desde distintas celdas utilizando los mismos canales de RF. En la práctica se acostumbra utilizar una combinación de técnicas de sectorización y celularización. Para utilizar un esquema de celularización es necesario contar con un enlace de banda ancha entre la estación central y cada una de las estaciones base, el cual permitirá acomodar el crecimiento del ancho de banda provocado por la re-utilización de frecuencias. Dicho enlace suele ser de fibra óptica o microonda punto-a-punto. Por supuesto, es necesario diseñar tomando en cuenta la presencia de señales ajenas a la deseada en cada una de las celdas, lo que no es un problema tan grave como en el caso de la telefonía celular, en el que cada uno de los usuarios dispone de antenas omnidireccionales: en MMDS cada suscriptor emplea antenas altamente direccionales, dirigidas hacia la respectiva estación base.

En un sistema celularizado podrían emplearse dos técnicas básicas de multicanalización: multicanalización por división de frecuencias (FDM, *Frequency Division Multiplexing*) y multicanalización por división de tiempo (TDM). La elección está dictada por el espectro disponible y el tamaño de las celdas a servir. Esto último es una función de factores tales como la potencia disponible para la transmisión, el formato de modulación, la ganancia de las antenas, el tipo de terreno, etc. Por razones de competitividad se requiere un tamaño de celda relativamente grande, ya que al reducir el tamaño de la celda suben los costos de infraestructura..

El empleo de MMDS no está de ninguna manera limitado a proveer acceso a Internet: también pueden tenerse aplicaciones que requieren de un tráfico simétrico, tales como telefonía, videoconferencia e interconexión de LANs.

b2. Sistemas LDMS

Es una tecnología muy similar al MMDS, pero con más potencial para la interactividad con el usuario, debido, sobre todo, a su mayor ancho de banda.

El sistema opera alrededor de la banda de los 26-28 GHz., siendo ésta la única tecnología de enlaces vía radio que permite un gran ancho de banda tanto en el canal de difusión de televisión como en el de retorno. El LMDS es capaz de ofrecer una gran variedad de servicios tales como vídeo multicanal digital, telefonía, vídeo bajo demanda, tele conferencia y servicios de datos de alta velocidad. Dada la posibilidad de utilizar un solo medio con alta capacidad para cubrir la "última milla" del bucle local, los modelos de los servicios a ofrecer dependen fundamentalmente de consideraciones locales (tipo de demanda, situación competitiva, densidad de posibles abonados, etc.).

La reciente disponibilidad comercial de tecnologías punto / multipunto es, en estos momentos, el factor más importante en el desarrollo comercial del LMDS.

Dado el carácter de terminal de red que tienen estos sistemas, no es sorprendente que los sistemas con protocolo ATM sean los preferidos por las empresas operadoras por su capacidad de combinar voz y datos manteniendo al mismo tiempo la calidad de servicio requerida.

Aparte del protocolo básico, una de las características dominantes de los sistemas punto / multipunto es un sistema de acceso que permita obtener la ganancia estadística basada en el ancho de banda bajo demanda o, al menos, en el ancho de banda compartido. Las características básicas de los sistemas de acceso líderes en cuanto a implantación son FDD, protocolo ATM, modulación QPSK junto con protocolo TDM en la bajada de la estación base al abonado y modulación QPSK junto con TDMA (con ancho de banda bajo demanda) en el sentido contrario.

Los sistemas LDMS son sistemas de estructura celular. El radio de la célula y la topografía del terreno determina el número de células necesarias para obtener la cobertura de una zona determinada. Para disminuir en lo posible la interferencia entre células adyacentes se utilizan técnicas de reutilización de frecuencia similares a las utilizadas en telefonía móvil celular.

Una de las decisiones fundamentales a nivel de diseño es precisamente el número y localización de las células y el método de interconexión entre ellas (fibra o microondas) y a las redes de datos, IP y telefonía.

Dentro de cada célula los parámetros más críticos son la densidad de abonados, las velocidades de datos promedio y las estadísticas del tráfico para cada categoría de abonado. En zonas de alta densidad de abonados se divide la célula en sectores que van desde los 180º hasta los 30º, cada uno de los cuales puede verse desde el punto de vista del sistema como una célula independiente.

c. Redes de Acceso Vía Fibra Óptica

La introducción de la fibra óptica en el nodo de acceso va a permitir el disponer de un medio de transmisión de gran ancho de banda para el soporte de servicios de banda ancha, tanto actuales como futuros.

La fibra óptica permite conexiones que utilizan distintos tipos de transmisión por Internet que pueden tener ya sea Protocolo Internet (IP, por sus siglas en inglés) o Frame Relay (que permite el envío punto a punto entre las sucursales de una empresa), entre otros.

En función de la extensión de la fibra en la red de acceso, podemos distinguir las siguientes topologías:

- **FTTH (Fiber To The Home):** se trata de llegar con fibra óptica hasta el hogar del abonado, directamente desde el nodo de servicio. Es la alternativa más directa, y también la de mayor coste a la hora de proporcionar acceso a banda ancha. Desde el punto de vista del operador, tiene el inconveniente de que requiere una fuerte inversión en obra civil.
- **FTTB (Fiber To The Building):** en este caso, la fibra llega hasta el interior de un edificio residencial o de negocios, existiendo una terminación de red óptica (ONU, Optical Network Termination) para todo el edificio.

- **FTTC (Fiber To The Curb):** el ONU y el tendido final de fibra son compartidos por varios abonados pertenecientes a una manzana de edificios o un área urbana de extensión reducida.
- **FTTCab (Fiber To The Cabinet):** configuración muy parecida a la anterior, con la diferencia de que el ONU es compartido por un mayor número de usuarios y que la red de cable eléctrico es de mayor extensión.
- **FTTExch (Fiber To The Exchange):** la fibra termina en el nodo de conmutación.

c.1. Redes Híbridas Fibra-Coaxial (HFC)

Una red de acceso HFC está constituida, genéricamente, por tres partes principales:

Elementos de red: dispositivos específicos para cada servicio que el operador conecta tanto en los puntos de origen de servicio como en los puntos de acceso al servicio.

Infraestructura HFC: incluye la fibra óptica y el cable coaxial, los transmisores ópticos, los nodos ópticos, los amplificadores de radiofrecuencia y elementos pasivos.

Terminal de usuario: SetTopBox, cable módems y unidades para integrar el servicio telefónico.

En la figura siguiente (figura 2.5.) se muestra un esquema típico de este tipo de redes:

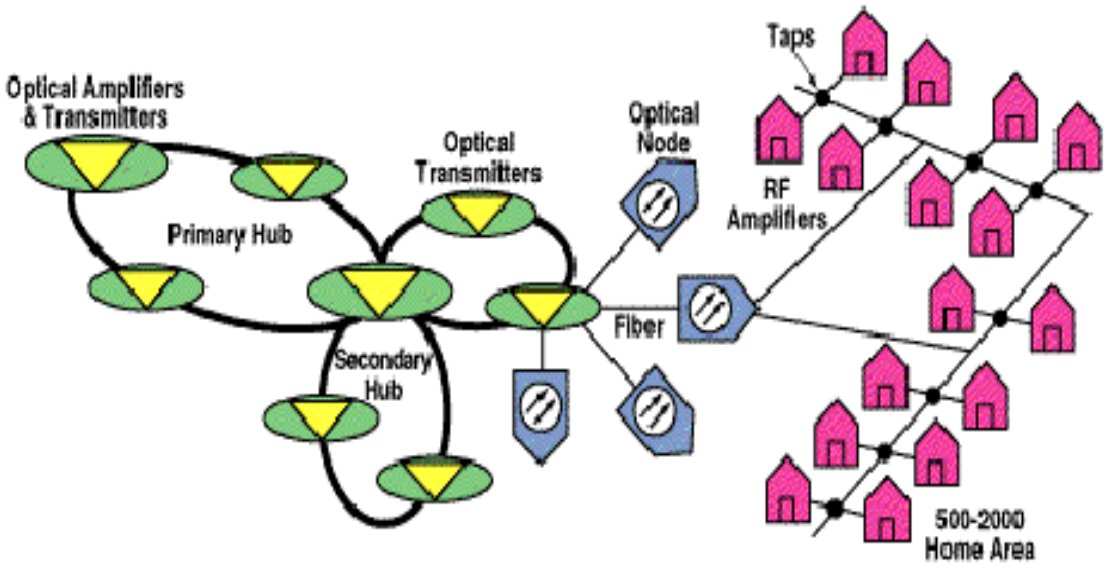


Figura 2.4. Esquema Típico Redes Híbridas Fibra-Coaxial (HFC)

Con mayor ancho de banda, los operadores disponen de mayor espectro en el que ofrecer servicios que generen beneficio. El ancho de banda de la red HFC es la clave en la que se fundamentan las ventajas de este tipo de redes, entre las que se incluyen:

- Posibilidad de ofrecer una amplia gama de servicios tanto analógicos como digitales.
- Soporte de servicios conmutados y de difusión.
- Capacidad de adaptación dinámica a los cambios de la demanda y del mercado, debido, en gran parte, a la gran flexibilidad y modularidad de que están dotadas este tipo de redes.

c.2. Redes Ópticas Pasivas (PON)

En el caso de usuarios residenciales se despliega la fibra hasta el domicilio del abonado y, mediante la unidad ótica de red (ONU) se le proporciona el servicio de vídeo a través del STB conectado al receptor de televisión, y servicio telefónico o de transmisión de datos. En este caso la técnica de transmisión más utilizada es la multiplexación por división en longitud de onda WDM (Wavelength Division Multiplexing) y la configuración punto a punto.

Los usuarios de negocios o comunidades científicas o educativas se suelen conectar a un anillo de distribución de fibra ótica que permite velocidades de varios cientos de Mbit/s. Al ser toda la infraestructura de fibra óptica, se proporciona una transmisión muy segura y libre de errores, con una alta capacidad de transferencia si se emplea, por ejemplo, ATM. El anillo se puede conectar a una LAN a través de un firewall para separar la Intranet de la Internet.

c.3. Redes Híbridas Fibra-Radio (HFR)

Las redes híbridas radiofibra se basan en una estructura de acceso vía radio junto con una estructura de transporte que emplea la fibra óptica como medio de transmisión. En esta línea, se están llevando a cabo importantes investigaciones y avances, entre los cuales merece ser destacado el proyecto FRANS (Fibre Radio ATM Networks and Services).

2.2. EQUIPOS Y PROCEDIMIENTOS UTILIZADOS EN LA SEGURIDAD DE REDES DE BANDA ANCHA

La llegada de la red digital de servicios integrados (RDSI), la conexión por cable y los sistemas de banda ancha (ADSL, DSL) ha hecho que la seguridad informática ya sea no sólo un tema de preocupación para las empresas. Cualquier usuario que posea una línea de este tipo está expuesto, además de a los ataques por parte de virus o troyanos, al mayor peligro que existe en Internet: los hackers.

Los ataques más frecuentes que puede sufrir un usuario que cuente con una línea de este tipo son las entradas no autorizadas para obtener datos confidenciales (como pueden ser las contraseñas que tengamos almacenadas) o los usos como "cabeza de turco" para atacar otras máquinas mientras la identidad del hacker queda oculta. Si esto ocurre, y el ataque es lo suficientemente grave, las autoridades que investiguen el caso lo primero que harán será mirar hacia la dirección IP de la máquina objeto de uso no autorizado. No es que la víctima de este manejo, en principio, vaya a acabar en la cárcel, pero sí que tendrá bastantes dolores de cabeza si ello sucede.

Los ataques se facilitan enormemente cuando el ordenador conectado a Internet tiene una dirección IP fija, tal y como ofrecen algunos proveedores de servicios de banda ancha. No todos ellos lo hacen así, por lo que este punto debe especificarse en el contrato que se firma con el proveedor. La dirección IP informa sobre la localización del ordenador pero en los accesos a través de módem telefónico el servidor la proporciona aleatoriamente, lo cual es una desventaja para un hacker. Por eso busca máquinas con IP fija, a las que puede tener perfectamente localizadas.

Lo primero que hace un usuario malicioso es localizar máquinas desprotegidas por medio de un programa automático o "mapeador" para buscar, en cientos de direcciones IP distintas, puertos de comunicaciones que le permitan llevar a cabo sus acciones. Un ordenador posee 65535 puertos (de los cuales algunos se utilizan para correo electrónico, otros para navegación web…); si alguno de ellos se encuentra innecesariamente abierto podría ser utilizado por un hacker para llevar a cabo su ataque.

La primera de las medidas básicas de prevención que se suelen indicar para evitar estos ataques es la instalación de un firewall personal que se encargue de bloquear los puertos que no estén en uso, o que, en un momento dado, pueda cortar todas las comunicaciones de manera rápida y eficaz. Sin embargo, los firewalls personales piden permiso al usuario para abrir puertos que algunos programas necesitan para sus propios fines, completamente lícitos. Esto, posteriormente, facilita que un usuario permita la apertura de un puerto engañado por un caballo de Troya o un hacker.

Así, como complemento al firewall también se recomienda algún software para "detectar intrusos", más útiles que el firewall personal, ya que el aviso se produce no por aperturas o cierres de puertos, sino solamente en el caso de estos intenten ser analizados por alguien con la intención de lanzar un ataque.

De cualquier manera, estas protecciones dan por sentado que alguien ha introducido código maligno, o quiere introducirlo, en nuestro equipo. Por tanto, la mejor solución es utilizar un programa antivirus reconocido y certificado que disponga de actualizaciones permanentes. Él no nos avisará de un puerto abierto, ni de un escaneo, pero en cuanto se introduzca en el sistema algún software que pueda dañar el equipo nos avisará inmediatamente.

Además de ello, es muy importante que el antivirus disponga de un servicio técnico que ofrezca una atención personalizada y permanente, y que actúe de forma rápida y eficaz. Las compañías de la industria antivirus deben tener en cuenta las nuevas necesidades de seguridad informática de los usuarios y por eso, entre otras características, los programas antivirus deberían analizar el correo electrónico entrante y saliente, permitir el bloqueo de servicios (ftp, http, etc.), y tener un buen comportamiento en la detección de virus en archivos comprimidos descargados de Internet empleando cualquiera de los navegadores de Internet más extendidos (Explorer, Netscape, Opera…).

Aunque para algunos servicios no parezca, salvo la velocidad, que hay mucha diferencia entre la antigua conexión por módem y la moderna de banda ancha, lo cierto es que existen distinciones importantes entre ambos. En las conexiones por módem se nos asigna una dirección IP diferente cada vez que nos conectamos, y por tanto no resulta nada sencillo rastrear a una persona, ya que cada nueva conexión tiene un identificador IP distinto.

Pero esto cambia al operar con una conexión de banda ancha que utiliza una dirección fija de Internet, ya que una vez localizado, el usuario siempre accede con el mismo número IP. Así que una vez localizado, resulta fácil buscar cualquier vulnerabilidad y encontrar un hueco para entrar de manera sigilosa en nuestro sistema. Una dirección IP fija es como un pato inmóvil en una cacería.

Para muchos despreocupados usuarios la única defensa es la simple estadística. “Con tantos servidores y usuarios con dirección fija, es altamente improbable que sea justo el mío el que despierte la atención de un hacker”.

Pero esta actitud no tiene en cuenta que hay programas que “automatizan” la búsqueda de servidores o direcciones Web, filtrando según cualquier criterio que desee el eventual atacante. Esto permite a un hacker dejar en marcha un programa de búsqueda de víctimas, que le devolverá números IP susceptibles de ser atacados, ya sea manual o automáticamente.

En rápidos pasos, el hacker descartará aquellos sistemas que exhiban un buen nivel de seguridad. Y obtendrá una lista de sistemas vulnerables. El siguiente paso será introducirse cautelosamente en su PC y dejar allí un “troyano”. Hay múltiples clases de troyanos, desde los que buscan datos confidenciales, como cuentas bancarias, tarjetas de crédito o claves de acceso a servicios Web, para enviarlos al atacante, hasta los que dejan un programa que permite que el PC sea controlado remotamente.

Un ordenador asaltado de esta forma podrá ser utilizado tanto para realizar envíos masivos de correo no solicitado, el conocido Spam, como para lanzar ataques a otros ordenadores o sitios Web. Y los receptores de tales prácticas verán que el “asaltante” es “nuestro” ordenador. Ya que puede ser fácilmente identificado, mediante su dirección IP, con una sencilla consulta al proveedor. Lo que nos coloca en el punto de mira de cualquier acción legal por daños sufridos.

Sin olvidar a los registradores de teclas, capaces de grabar todas las teclas que pulsamos. Como realizan esta misión desde una etapa muy temprana del arranque del ordenador, serán capaces de registrar y almacenar las claves de conexión, las contraseñas de acceso a servicios bancarios, y un largo etcétera.

2.2.1. Mecanismos de Defensa

El primero de los recursos que hay que mantener activado, pero no el último, es, como no, un buen antivirus. Con una conexión de banda ancha, resulta todavía más imperdonable no realizar actualización periódica de los archivos del antivirus. Se debe consultar la configuración de cómo se realiza ésta por si tuviera que reconfigurar el acceso para descargar los archivos nuevos del antivirus. Aunque en general los productos buscan el mejor camino, y el de la banda ancha se encuentra disponible tan pronto como arranca el ordenador, con lo que no hay retardos para establecer la conexión.

Pero esto no es todo. También se debe reforzar el perímetro. Lo que significa prestar atención a conceptos como firewall y eventualmente filtrado de contenidos. Un cortafuegos, o firewall, es el elemento básico y fundamental. Los cortafuegos personales cuentan con instalación automatizada y un sencillo interfase de usuario, con lo que, en general, no tendrá que ajustar crípticos parámetros. Ni se necesita tener elevados conocimientos de los conceptos de Internet, tan sólo saber leer, en inglés para la mayor parte de productos.

Hay asequibles cortafuegos personales de marcas comerciales bien conocidas. La compra de uno de estos productos garantiza tanto las actualizaciones como la disponibilidad de un servicio técnico que ayude para configurarlo correctamente. Si se prefiere las alternativas más económicas, es decir gratuitas, hay productos como ZoneAlarm que son fáciles de usar y son de libre uso para particulares (pero no para las empresas o las instituciones).

2.2.2. Seguridad Informática

Toda organización debe estar a la vanguardia de los procesos de cambio. Donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental.

La seguridad informática debe garantizar:

- *La* **Disponibilidad** *de los sistemas de información.*
- *El* **Recupero** *rápido y completo de los sistemas de información*
- *La* **Integridad** *de la información.*
- *La* **Confidencialidad** *de la información.*

Se debería tener en cuenta los siguientes aspectos:

- Implementación de políticas de Seguridad Informática.
- Identificación de problemas.
- Desarrollo del Plan de Seguridad Informática.
- Análisis de la seguridad en los equipos de computación.
- Auditoria y revisión de sistemas.

2.2.3. Seguridad Básica de la Red

Por definición, una red de área local (Lan) abarca un área local. Una Extranet representa el extremo opuesto. Las conexiones con los socios comerciales (de hecho, dentro una organización) se puede extender a otras partes del país, incluso a otros países.

La naturaleza de una Extranet implica que muchas reglas de seguridad en cómputo conocidas deben valorarse a escribir o por lo menos modificarse sustancialmente.

Las técnicas de *mainframe* construidas con el propósito de proteger sitios centrales son, a todas luces, insuficientes para proteger una computadora virtual que puede abarcar organizaciones completas. Las técnicas estándar para Lan hacen un buen trabajo al proteger las redes locales basadas en servidores cercanos, pero para proteger una Extranet requiere ampliar la visión en proporción geométrica.

Sin embargo, asegurar una Extranet también puede ser similar a proteger otro tipo de red. Las técnicas básicas de la seguridad en cómputo también son válidas. La Extranet simplemente requiere que las adopte y adapte, a veces estirándolas un poco. No es fácil pero se puede hacer, de hecho debe hacerse. Las Extranets continuarán difundiéndose, con o sin su participación.

a. Construir un Plan de Seguridad

Para enfrentar el reto de dar seguridad a la Extranet se empieza por un buen plan. Se debe incluir estos elementos:

- Adaptar los métodos conocidos a las nuevas necesidades. No por que se descentraliza la red debe descentralizar la administración de seguridad.
- Controlar el acceso de archivos. Los tipos de controles disponibles en una Lan son aún más importantes cuando la red se extiende.
- Establecer prioridades. Se debe poner concentración primero en las áreas más susceptibles a pérdidas.
- Hacer una auditoria del programa. Mantener un registro de quien se comporta o no de manera correcta.

- Hacer un uso efectivo de la encriptación. No se necesita encriptar todo lo que viaja a través de la Extranet, pero se lo debe hacer con cualquier forma de información importante.
- Mantener sencillo el sistema. Aquí hay una contradicción implícita pero es importante. Alentar a las personas a que sigan las medidas de seguridad facilitándoles su uso.

b. Funciones de Seguridad Importantes en las VPNs

El Instituto Nacional de Normas y Tecnología (NIST, National Institute for Standars and Technology) desarrolló lo que llama requerimientos mínimos de seguridad funcional para los sistemas operacionales multiusuario. Las precauciones de seguridad que indica no siempre son únicas para las extranets, pero construyó una lista de verificación útil para las funciones que se debe considerar para cuando se planee un sistema de seguridad. Las funciones principales son:

- Identificación y autenticación. Utilizar una contraseña o alguna otra forma de identificación para filtrar usuarios y revisar la autorización.
- Control de acceso. Evitar incluso a los usuarios autorizados el acceso a material que no deben ver.
- Responsabilidad. Enlazar las actividades en una red a la identidad del usuario.
- Rastros de auditoria. Determinar si ocurrió una violación a la seguridad y, en caso de haberla, qué se perdió?.
- Reutilización de los objetos. Asegurar que los recursos estén seguros en las manos de varios usuarios.
- Precisión. Proteger contra errores y modificaciones sin autorización.

- Confiable. Cuidar la monopolización de cualquier usuario.
- Intercambio de datos. Promover transmisiones seguras a través de los canales de comunicación.

c. Identifique al Usuario

La Extranet, como en la mayoría de las instalaciones la identificación del usuario es necesaria aunque no suficiente. Un sistema de identificación y autenticación casi siempre confía en las contraseñas aunque puede utilizar otras indicaciones, como insignias y medidas biométricas. Nada del resto del sistema de seguridad funcionará a menos que primero esté seguro de que puede determinar si un probable usuario tiene autorización para estar ahí.

Tener acceso no debe ser suficiente. Una vez que admite una persona , el sistema debe controlar su acceso a la información. Se debe utilizar la administración de control de privilegios para asegurar que el usuario tiene acceso a lo que necesita para hacer su trabajo, nada más. Puede hacer esto asignando juegos predefinidos de privilegios a las responsabilidades de un trabajo específico.

Asegurar la precisión puede ser uno de los retos más difíciles en la seguridad de la Extranet. A nadie debe permitirle modificar las páginas web excepto en condiciones rigurosamente controladas. Se debe ser inflexible con este privilegio. Esto es aún más importante si la extranet utiliza los recursos de la base de datos.

d. El papel de la Encriptación

La tarea más importante de la encriptación en una Extranet es proteger las contraseñas, los números de tarjetas de crédito y otra información con la que se puede proporcionar acceso adicional a la red. Se debe incluir los sistemas de generación y registro de contraseñas.

También se puede utilizar la encriptación para conservar la confidencialidad de la información transmitida entre navegadores y servidores. Esto también puede ayudar a protegerse de amenazas como intervenciones a la línea, detección electrónica sin permiso, envío por ruta equivocada, sustitución, modificación e inserción de mensajes. Así mismo, se puede utilizar algoritmos de encriptación para crear firmas digitales que le pueden ayudar a comprobar la identidad de las personas que envían y reciben mensajes.

e. Proteger la Comprobación de Identidad

Cuando las contraseñas u otra información conocida de un usuario autorizado se introducen al sistema, es posible que alguien la intercepte interviniendo la línea o mediante algún otro medio. Entonces el intruso puede utilizar la información para fingir ser un usuario autorizado.

La encriptación puede utilizarse para proteger la información desde el punto en que la deja el navegador o servidor y se transmite a su destino. Si ya se utiliza la encriptación para proteger información transmitida, esta misma capacidad puede ser adecuada para proteger la información de comprobación. El proceso de encriptación usado para proteger la información de comprobación se debe permitir que la información sea codificada de manera distinta en cada transmisión.

De otra manera, un intruso puede registrar la información encriptada en un punto de la ruta de transmisión y engañar al sistema simplemente insertando la misma información encriptada sin necesidad de descifrarla. En general, los sistemas de encriptación tienen medidas para lograr la variabilidad requerida.

Cuando un atributo personal se utiliza para comprobar una identidad, se obtiene un conjunto de valores medidos, luego si digitalizan y comparan con un perfil de referencia. Es evidente que un hábil intruso puede emplear esta información para simular los datos obtenidos de un usuario autorizado. Para resguardarse de esto, el equipo que mide el atributo debe estar protegido contra la intromisión para que la información no se pueda substraer mientras esta desocupada. Puede utilizar la encriptación para proteger esta información mientras se transmite.

Los sistemas de verificación basados en los atributos personales están configurados de diversas formas. En una configuración, el equipo de medición envía los valores medidos a un sistema central donde esta almacenado el perfil de referencia a donde hace la comparación. En este caso los valores medidos deben encriptarse para transmitirlos al sistema central. En otra configuración, el perfil de referencia se envía al equipo de medición donde se hace la comparación. En este caso el perfil de referencia debe estar encriptado para impedir que el intruso pueda insertar el perfil de referencia propio.

Además el equipo produce una señal de aprobado / rechazado, basada en el resultado de la comparación, y esto se transmite a otra parte; por ejemplo de regreso al sistema central que controla el acceso de la red.

Esta señal de aprobado / rechazado también debe estar encriptado de otra manera, un intruso puede simularla y producir una respuesta falsa de aprobación sin tener que engañar al equipo.

En general, el equipo sensorial del atributo personal es una parte integral de una terminal remota, o está asociado de manera cercana a una terminal similar. Se debe tomar precauciones para asegurar que las salas de equipo estén protegidos contra la intromisión y que no existan conductos expuestos que permitan a un intruso tomar información importante.

f. Firmas Digitales

Una forma de autenticación es la firma digital. La persona que envía el mensaje le adjunta una identificación codificada y encriptada de tal manera que solo el receptor deseado puede descifrarlo y comprobar la identidad del emisor. Una forma de hacer esto se basa en utilizar identificadores individuales de estación en el proceso de encriptación de llaves, que en cambio se utilizan para encriptar mensajes entre las estaciones. Debido a los arreglos de los equipos y los procesos de operación utilizados con este sistema, es posible que un remitente encripte una firma o cualquier otro mensaje de modo tal que solo el receptor predefinido puede descifrarlo de manera correcta.

Las firmas digitales también se pueden lograr a través de la encriptación de llaves. En este sistema, la llave para encriptar difiere de la llave para desencriptar (descifrar); conocer la llave par encriptar no implica conocer la llave para desencriptar. En un sistema público de llaves, los usuarios pueden publicarlas libremente para encriptar los mensajes que se les enviarán; pero, se mantendrá en secreto las llaves correspondientes para desencriptar.

Los procesos para encriptar y desencriptar en algunos sistemas públicos de llaves son inversos. En la práctica normal, primero se encripta un mensaje para transmitirlo y después se descifra al ser recibido para recuperar la información. Sin embargo, los procesos en estos sistemas se pueden aplicar en orden inverso: primero se utiliza el proceso de descifrado para ocultar la información y después el proceso de cifrado para recuperarla.

Una firma digital segura se puede lograr de esta manera: suponga que el usuario A quiere enviar una firma digital segura al usuario B. El usuario A primero pasa la firma a través de su proceso de desencriptación que, en efecto, la dejará incomprensible. Luego encripta la firma utilizando la llave pública para encriptar del usuario B se la envía.

El usuario B primero descifra la firma utilizando su propio proceso para desencriptar. Luego aplica la llave pública del usuario A y recupera la firma digital. En la práctica, es preferible aplicar este proceso a los mensajes completos en lugar de solo a la firma de verificación y así, evitar que una firma válida se adjunte a un mensaje falsificado.

g. Límites de Capacidades

En cuanto la identidad de un usuario se establece y autentica, puede tener acceso a la red y solicitar los distintos recursos disponibles. En estos recursos constan de varias entidades, como las computadoras anfitrión, áreas de memoria principal, archivos, programas, dispositivos de memoria auxiliares e instrucciones. En ocasiones a estos recursos se les denomina objetos.

Los usuarios deben tener la autorización adecuada para acceder a estos objetos. Cada usuario tiene asociado un conjunto de privilegios de acceso a los que tiene derecho. A esto se le puede llamar *perfil de capacidad.*

De forma similar, cada objeto viene con un conjunto de requerimientos para su uso, a los que se les puede llamar *perfil de requerimientos de acceso.* Una solicitud de acceso está autorizada cuando el perfil de capacidad del solicitante coincide con el perfil de requerimientos de acceso del objeto.

Un objeto puede tener distintas formas en las que puede ser utilizado, como leer datos en un archivo, escribir datos en un archivo, hacer una transacción, ejecutar o compilar un programa o llamar a varias rutinas del objeto, no todas serán autorizadas para que las ocupen todos los usuarios. Puede imaginar esta situación como una matriz tridimensional, con los usuarios a lo largo de una dimensión, los objetos a lo largo de otra y las capacidades a lo largo de la tercera.

2.2.4. Lista para Verificar la Seguridad de la Red

a. Redes de Área Local (Lan)

- Encriptar las contraseñas que se transmiten por la red.
- Relacionar las contraseñas con los registros de hora y adaptadores de dirección.
- Proporcionar el bloqueo de pantalla.
- Pedir que los usuarios vuelvan a entrar cuando el servidor no está disponible.
- Exigir que los usuarios salgan de la red cuando se alejen de las estaciones de trabajo.
- Prohibir los accesos mientras se le da mantenimiento al sistema.

b. Control de Acceso a Archivos

- Definir las reglas de acceso a los archivos para los controladores físicos y lógicos en los niveles de subdirectorio y archivos.
- Verificar que la seguridad de nivel de archivo soporte los comodines de nombre de archivo.
- Las reglas de acceso no deben volverse a escribir cuando se mueva los grupos de archivos o directorios.
- Limitar el número de usuarios actuales en los niveles de subdirectorio y archivo.
- Limitar la administración de la red local a un solo servidor.
- Reportar todos los intentos de acceso al dueño de los recursos.

c. Seguridad del Servidor

- Evitar todas las entradas al servidor sin identificación válida. Imponer este requerimiento para el ratón y el teclado.
- Guardar respaldos del sistema operativo del servidor y de los archivos de datos.
- Ejecutar respaldos programados y desatendidos del servidor.
- Utilizar una copia del disco tipo espejo para una recuperación rápida.
- Establecer respaldos programados de las estaciones de trabajo controlados por el servidor.

d. Asegure los Distintos Servidores

- No se debe pedir que los empleados utilicen nombres de usuario y contraseñas únicas para cada servidor. Se debe dar acceso para cada ocasión.
- Mantener un control local del acceso remoto.
- Otorgar poder al administrador para determinar si las reglas de acceso para un archivo específico se aplicarán a las copias o a la información extraída de él.

2.2.5. Sistemas de Detección de Intrusos

Existen numerosas medidas de seguridad para proteger los recursos informáticos de una empresa, pero aunque se sigan todas las recomendaciones de los expertos, no se descarta posibles ataques con éxito. Esto se debe a que conseguir un sistema virtualmente invulnerable es sumamente costoso, además de que las medidas de control reducirían la productividad de la empresa.

Dentro de las soluciones tecnológicas que en la actualidad están disponibles para reforzar la seguridad de una red, los firewalls son muy populares. Un firewall es un sistema encargado del cumplimiento de las políticas de control de acceso a la red, lo cual se hace a través de reglas. Un firewall actúa como guardia perimetral de una red: protege una red de ataques que provengan del exterior de ésta. Pero el escenario se puede complicar de la siguiente forma:

1. Un atacante puede lograr pasar el firewall, dejando la red a su merced.
2. Un firewall protege de los accesos no autorizados hacia la red interna, pero no protege a las máquinas ubicadas en la red perimetral como servidores web, servidores de correo, servidores FTP, en otras palabras, a las bases funcionales de Internet.

3. Un firewall no protege contra ataques desde adentro.

En estos casos lo que nos queda es detectar el ataque o la intrusión lo antes posible para que cause el menor daño en el sistema. Antes de continuar se va a definir qué se entiende normalmente por intrusión. Normalmente un intruso intenta:

- Acceder a una determinada información.
- Manipular cierta información.
- Hacer que el sistema no funcione de forma segura o inutilizarlo.

Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar debilidades y brechas en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación. La detección de intrusos se puede detectar a partir de la caracterización anómala del comportamiento y del uso que hacen de los recursos del sistema. Este tipo de detección pretende cuantificar el comportamiento normal de un usuario. Para una correcta distinción hay que tener en cuenta las tres distintas posibilidades que existen en un ataque, atendiendo a quién es el que lo lleva a cabo:

- *Penetración externa.* Que se define como la intrusión que se lleva a cabo a partir un usuario o un sistema de computadores no autorizado desde otra red.
- *Penetraciones internas.* Son aquellas que llevan a cabo por usuarios internos que no están autorizados al acceso.

- *Abuso de recursos.* Se define como el abuso que un usuario lleva a cabo sobre unos datos o recursos de un sistema al que está autorizado su acceso.

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un subconjunto de las actividades anómalas. Esto puede parecer razonable por el hecho de que si alguien consigue entrar de forma ilegal en el sistema, no actuará como un usuario normal. Sin embargo en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Idealmente el conjunto de actividades anómalas es el mismo del conjunto de actividades intrusivas, de todas formas esto no siempre es así:

1. *Intrusivas pero no anómalas.* Se les denomina *falsos negativos* y en este caso la actividad es intrusiva pero como no es anómala y no se consigue detectarla. Se denominan *falsos negativos* porque el sistema erróneamente indica ausencia de intrusión.
2. *No intrusivas pero anómalas.* Se denominan *falsos positivos* y en este caso la actividad es no intrusiva, pero como es anómala el sistema decide que es intrusiva. Se denominan *falsos positivos*, porque el sistema erróneamente indica la existencia de intrusión.
3. *Ni intrusiva ni anómala.* Son negativos verdaderos, la actividad es no intrusiva y se indica como tal.
4. *Intrusiva y anómala.* Se denominan positivos verdaderos, la actividad es intrusiva y es detectada.

Los primeros no son deseables, porque dan una falsa sensación de seguridad del sistema y el intruso en este caso puede operar libremente en el sistema. Los falsos positivos se deben de minimizar, en caso contrario lo que puede pasar es que se ignoren los avisos del sistema de seguridad, incluso cuando sean acertados.

Los detectores de intrusiones anómalas requieren mucho gasto computacional, porque se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal. Hoy día existe en el mercado una buena cantidad de productos conocidos como SDI (Sistemas de Detección de Intrusos) o en inglés IDS (Intrusión Detection System).

Estos sistemas basan su funcionamiento en la recolección y análisis de información de diferentes fuentes, que luego utilizan para determinar la posible existencia de un ataque o penetración de intrusos.

En caso de que exista la suficiente certeza de la detección de un incidente, el SDI tiene como función principal alertar al administrador o personal de seguridad, para que tome acciones al respecto. Otras implementaciones más complejas son capaces de ir más allá de la notificación de un posible ataque, es decir pueden ejecutar acciones automáticas que impidan el desarrollo de éste.

a. Clasificación de los SDI

Los SDI pueden clasificarse en base a varios aspectos: Método de detección, tipo de monitoreo y forma de recolección y análisis de la información.

Según el método de detección, los hay de detección de mal uso y detección de anomalías.

El modelo de detección de mal uso consiste en observar cualquier proceso que intente explotar los puntos débiles de un sistema en específico. Las diferentes acciones, que integran el mencionado proceso, comúnmente se denominan patrones o firmas del ataque.

Estas firmas pueden ser simples, como cadenas de caracteres, estructuras de memoria o bits, pero también pueden ser más complejas como vectores ó expresiones matemáticas. Una ventaja de este método es que permite centralizar las labores de detección en el conjunto de firmas que posee el SDI, minimizando así, la carga de procesamiento del sistema. Muchos productos comerciales utilizan este enfoque e inclusive periódicamente proporcionan actualizaciones de éstas firmas.

En cambio, el modelo de detección de anomalías se basa en constantemente monitorear el sistema para así detectar cualquier cambio en los patrones de utilización o el comportamiento del mismo. Si algunos de los parámetros monitoreados sale de su regularidad, el sistema generará una alarma que avisará al administrador de la red sobre la detección de una anomalía. Este tipo de detección es bastante complejo, debido a que la cuantificación de los parámetros a observar no es sencilla y a raíz de esto, se pueden presentar los siguientes inconvenientes:

- Pueden generarse falsas alarmas si el ambiente cambia repentinamente, por ejemplo, cambio en el horario de trabajo.
- Un atacante puede ir cambiando lentamente su comportamiento para así engañar al sistema.

Los inconvenientes antes mencionados pueden ser controlados mediante una implementación robusta y minuciosa.

Según el tipo de monitoreo, hay SDI con detección orientada al host o detección orientada a la red.

El modelo orientado al host se basa en el monitoreo y análisis de información, que refleja el estado del host donde éste reside. La mayoría de la información que este tipo de sistema recopila es obtenida a través del sistema operativo del host. Esto último causa complicaciones debido a que la información que se procesa no contiene registros del comportamiento, de bajo nivel, de la red.

Los SDI que utilizan el modelo orientado a red, fundamentan su monitoreo en información recolectada de la red. Generalmente, ésta información es capturada mediante mecanismos de "sniffing". El "sniffing" consiste en habilitar la interfaz de red en modo promiscuo para que así capture todos los paquetes que reciba, incluso aquellos que no le han sido destinados. En base al mecanismo antes expuesto, se pueden definir patrones o firmas de ataques, según la estructura, información y ocurrencia de los paquetes.

b. Características Deseables de un SDI

1. Debe ejecutarse continuamente sin intervención o supervisión de un operador humano.
2. Debe ser confiable, lo suficiente como para ejecutarse en background, pero no debe ser una caja negra, es decir, que su funcionamiento interno pueda ser examinado.
3. Debe ser capaz de tolerar fallas, en el sentido de que pueda sobrevivir a una caída del sistema, sin tener que reconstruir su base de datos de conocimientos al reiniciarse.

4. El sistema debe estar en capacidad de automonitorearse para asegurar su correcto funcionamiento.
5. Debe ser ligero, es decir su ejecución no debe cargar al sistema de una manera tal que le impida ejecutar otras tareas con relativa normalidad
6. Debe observar desviaciones del comportamiento estándar.
7. Debe poder adaptarse al comportamiento cambiante del sistema, es decir, si la configuración del sistema cambia, el SDI se adaptará.
8. Debe ser difícil de engañar.

c. Metodología para la Detección de Intrusos y para la Selección e Implantación de Sistemas IDS

La labor de un administrador o de la persona encargada de la seguridad de un sistema informático puede ser realmente frustrante. Sobre todo cuando el sistema a sido invadido por un intruso o hacker. En principio, si se ha configurado correctamente un servidor y se está al día en materia de seguridad, así como de fallas (bugs) que van surgiendo, no habrá problemas de que un intruso entre en el sistema. Realmente con un poco de esfuerzo se puede tener un servidor altamente seguro que evitará alrededor del 85% de los intentos de acceso no autorizados a los sistemas. Pero en muchas ocasiones el peligro viene de los propios usuarios internos del sistema, los cuales presentan un gran riesgo debido a que ya tiene acceso al sistema.

d. Pasos a Seguir para Detectar a un Intruso

Lo primero que se debe hacer es seguir una serie de pasos los cuales nos ayudarán a descubrir si realmente ha entrado un intruso, ya que en muchas ocasiones pensamos que ha entrado alguien, pero no es cierto. Por eso, ante todo calma; esto es lo más importante para un buen administrador.

Realmente en muchas ocasiones es fácil detectar a un intruso en ambiente Unix, ya que suelen seguir un patrón detectable, el cual podría ser el mostrado en la figura 2.5.

Este esquema representa básicamente los pasos que sigue de un intruso: Primero entra al sistema, y si sólo tiene acceso como usuario, explotará alguna debilidad o falla del sistema para así obtener ID 0 (o lo que es lo mismo, privilegios de root). En caso de entrar como root u obtenerlo de alguna otra manera, se dedicará a controlar el sistema, dejando algún mecanismo para volver cuando quiera. Seguramente copiará el archivo /etc/passwd y el /etc/shadow (en caso de que el sistema use "shadow"), luego le dará rienda suelta a su imaginación, como por ejemplo, instalar un sniffer, troyanos, leer mails ajenos, etc. Y en caso de ser un pirata malicioso puede causar desastres en el sistema, como sería modificar páginas web, borrar archivos o mails, producir un DoS (Denial of Service), cambiar passwords de usuarios legítimos, etc.

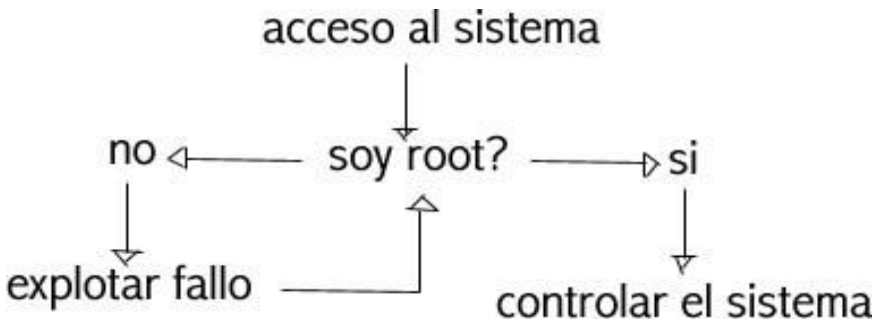


Figura 2.5. Detección de un Intruso en el Sistema

A continuación se exponen los diferentes pasos a seguir de acuerdo a los expertos en seguridad como son el CERT, ISS, etc.

Esto son los pasos a seguir del CERT (http//www.cert.org):

1. Examinar los archivos log como el 'last' log, contabilidad, syslog, y los C2 log buscando conexiones no usuales o cosas sospechosas en el sistema. Aunque hay que tener especial cuidado en guiarnos por los logs, ya que muchos intrusos utilizaran diversas herramientas para borrar sus huellas.
2. Buscar por el sistema archivos ocultos o no usuales (archivos que empiezan por un '.' (punto), no salen con un simple 'ls'), ya que puede ser usado para esconder herramientas para violar la seguridad del sistema, por ejemplo un crackeador puede contener el /etc/passwd del sistema o de otros sistemas al cual ha entrado el intruso. Muchos piratas suelen crear directorios ocultos utilizando nombres como '...' (punto-punto-punto), '..' (punto-punto), '..^g' (punto-punto control+G). En algunos casos un pirata ha utilizado nombres como '.x' o '.hacker' o incluso '.mail'.
3. Buscar archivos SET-UID por el sistema. Ya que en muchas ocasiones los piratas suelen copiar y dejar escondido copias del /bin/sh para obtener root. Podemos utilizar el comando 'find' para buscar este tipo de archivos por el sistema (el comando 'find' puede ser sustituido por un troyano para esconder archivos del pirata, por lo que no es totalmente confiable), para ello ejecutamos la siguiente línea: # find / -user root -perm -4000 -print

4. Revisar los archivos binarios del sistema para comprobar que no han sido sustituidos por un troyano, como por ejemplo los programas 'su', 'login', 'telnet' y otros programas vitales del sistema. (Existen varias herramientas conocidas como 'RootKit' que permite a un pirata cambiar los binarios del sistema por troyanos que son copias exactas de los originales). Lo recomendado es comparar con las copias de seguridad aunque puede que las copias de seguridad también hayan sido sustituidas por un troyano.
5. Examinar todos los archivos que son ejecutados por 'cron' y 'at'. Ya que algunos piratas depositan puertas traseras que le permiten volver al sistema aunque los hayamos echado del sistema. Asegurarse que todos los archivos pertenecen al sistema y no tienen permiso de escritura.
6. Examinar el archivo /etc/inetd.conf en busca de cambios, en especial aquellas entradas que ejecuten un shell (por ejemplo: /bin/sh o /bin/csh) y comprobar que todos los programas son legítimos del sistema y no troyanos.
7. Examinar los archivos del sistema y de configuración en busca de alteraciones. En particular, buscar entradas con el signo '+' o 'host names' no apropiados en archivos como /etc/hosts.equiv, /etc/hosts.lpd y en todos los archivos .rhost del sistema, con especial interés los de 'root', 'uucp', 'ftp' y otras cuentas del sistema. Estos archivos no deberían tener atributo de escritura.
8. Examinar cuidadosamente todos los computadores de nuestra red local en busca de indicios que nuestra red ha sido comprometida. En particular, aquellos sistemas que compartan NIS+ o NFS, o aquellos sistemas listados en el /etc/hosts.equiv. Lógicamente también revisar los sistemas informáticos que los usuarios comparten mediante el acceso del .rhost.

9. Examinar el archivo /etc/passwd, en busca de alteraciones en las cuentas de los usuarios o la creación de cuentas nuevas, especialmente aquellas cuentas con ID 0, las que no tienen password, etc.

Estos nueve puntos son los pasos a seguir recomendados por el CERT, los cuales están muy bien, pero se quedan un poco cortos de soluciones prácticas para el administrador.

e. Diversas Herramientas para la Tarea

Ahora se puede explicar las diferentes herramientas que están disponibles en el ciberespacio. Lo mejor es que casi todas son 'freeware' (gratis), por lo que no existe excusa alguna para no usarlas. Además usando habitualmente estas herramientas, se podrá mantener el sistema seguro.

Las herramientas que se describen a lo largo de este apartado son anti-zapper's, detectores de sniffers, detectores de troyanos, así como diversas herramientas de análisis, e incluso algunas herramientas que también utilizan los piratas, para el propio beneficio.

Debido a la gran cantidad de herramientas disponibles (no se ha citado todas las que existen, debido a que es imposible), no se ha incluido la utilización de las mismas, ya que este documento sería muy largo, por lo que se incluye la dirección en Internet donde se encontrará información mas detallada sobre estas herramientas.

e.1. Detectores de Sniffers.

- Se puede usar el comando 'netstat', pero no es 100% confiable.

- promisc.c: Es un programa escrito en lenguaje C, el cual puede ayudar a detectar un sniffer en nuestra red. (promisc.c).
- cpm (ftp://coast.cs.purdue.edu/pub/tools/unix/cpm/cpm.1.2.tar.gz).
- ifstatus (ftp://coast.cs.purdue.edu/pub/tools/unix/ifstatus/ifstatus.tar.Z).
- NePED: Es un detector de sniffers. (ftp://apostols.org/ AposTools/snapshots/neped/).

e.2. Detectores de Troyanos.

- Se puede usar el comando 'sum' pero tampoco es 100% confiable.
- También se puede usar el comando 'cmp', pero lo mismo que el comando anterior.
- El popular, y más aconsejable de usar, es el programa de verificación MD5.
- Otro, también bastante utilizado, es Tripwire. (Tripwire).

e.3. Detectores de Zapper's.

- Antizap.c
- Antizap2.c

e.4. Herramientas de Análisis.

- Satan111: Posiblemente la herramienta más conocida. (SATAN). xtensiones.(SATAN Extensions).
- TCP_Wrapper: Es un conjunto de utilidades para controlar nuestro servidor. (tcp_wrappers_7.6.tar.gz).

- Netcat 1.10: Para saber por dónde puede atacar un pirata, ya que este programa es capaz de crear cualquier tipo de conexión. (netcat 1.10 for Unix).
- COPS: Otro conjunto de herramientas de muy buena calidad. (ftp://info.cert.org/pub/tools/cops).
- Roses Software Check Tool V.1.2.2: Interesante herramienta de análisis para servidores Linux. (http://web.jet.es/~simon_roses/).
- Rhino9 Security Check Tool: Interesante programa. (http://rhino9.technotronic.com).
- Stalker Audit-Trail Tool: Interesante herramienta para auditar los log's. (http://www.haystack.com).
- IDES/NIDES (Intrusion-Detection Expert System/Next-Generation IDES): Una herramienta de detección de piratas en tiempo real. (http://www.sri.com).
- WatchDog: Herramienta para auditar los log's para SunOS. (http://www.infstream.com).
- Saint (Security Analisys INtegration Tool): Herramienta en español para auditar. (http://www.super.unam.mx).
- Asax (Advanced Security Audit Trail Analysis on Unix): Programa en francés. (http://www.info.fundp.ac.be/~cri/DOCS/asax.html).
- Aid (Adaptive Intrusion Detection System): Herramienta en alemán.
- (http://www.rnks.informatik.tucottbus.de/~sobirey/aid.e.html).
- NetSuite Professional Audit: Herramienta profesional para auditar. (http://www.netsuite.com/Pi/audit.htm).
- Audit Trails: Lo mismo que el anterior. (http://promatrix.com/audit.htm).

- ISS SafeSuite: Potente herramienta de análisis. (http://www.iss.net).
- Proyecto Nessus: Una recomendable herramienta de auditoria. (The Nessus Project).
- Firewalk: Interesante técnica para analizar una red. (Enterprise Security Services, Inc.).
- Lsof (List Open Files): Programa que lista todos los archivos abiertos, incluidos los sockets abiertos. (ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/).
- tcplist: Lista todos los puertos abiertos que se tiene, además de suministrar diversa información más. (ftp://ftp.cdf.toronto.edu/pub/tcplist).

e.5. Crakeadores de Passwords.

- Crack V5: Posiblemente el crakeador más conocido. (Crack v5 (Source)).
- John The Ripper: Un excelente crakeador. (John the Ripper 1.5 linux).

2.3. FIREWALLS

La seguridad ha sido el principal tema a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el número de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las páginas en el WWW y los servidores FTP de acceso público en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los Expertos de Internet (*Internet Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

2.3.1. Firewalls y Seguridad en Internet

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red puede ser accesado dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

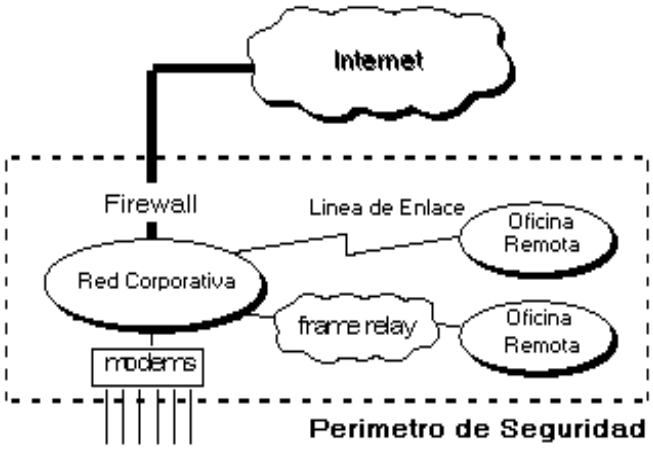


Figura 2.6. La Política De Seguridad Crea Un Perímetro De Defensa.

Esto es importante, ya que se debe notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información.

Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

a. Beneficios de un Firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "check point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado!.

- Concentra la seguridad Centraliza los accesos
- Genera alarmas de seguridad Traduce direcciones (NAT)
- Monitorea y registra el uso de Servicios de WWW y FTP.

Internet.

Figura 2.7. Beneficios De Un Firewall De Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs).

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando únicamente el acceso al Internet esta perdido.

La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso son puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

b. Limitaciones de un Firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet.

Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte integral de la arquitectura de la seguridad en la organización.

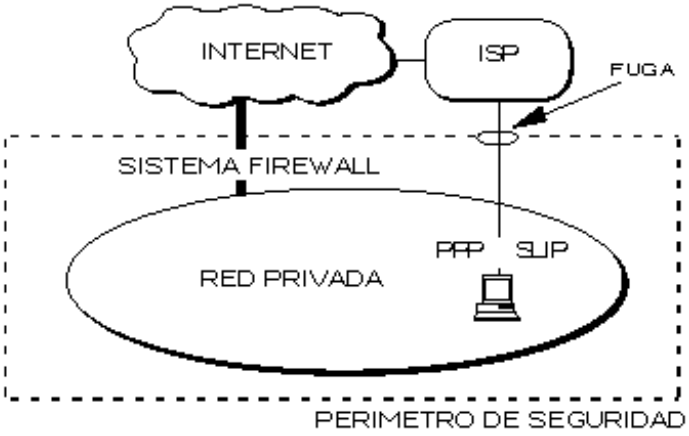


Figura 2.8. Conexión Circunvecina Al Firewall De Internet.

El firewall no puede proteger de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquetes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él.

La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inofensivos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema.

Como se puede ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

2.3.2. Bases para el Diseño Decisivo del Firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- Posturas sobre la política del Firewall.
- La política interna propia de la organización para la seguridad total.
- El costo financiero del Proyecto "Firewall".
- Los componentes o la construcción de secciones del Firewall.

a. Políticas del Firewall.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- "No todo lo específicamente permitido esta prohibido"
- "Ni todo lo específicamente prohibido esta permitido"

La primera postura asume que un firewall puede obstruir todo el tráfico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado número de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es más importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad.

La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad - del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primera propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas.

b. Política Interna de la Seguridad

Tan discutidamente escuchada, un firewall de Internet no esta solo, es parte de la política de seguridad total en una organización, la cual define todos los aspectos en correspondientes al perímetro de defensa. Para que esta sea exitosa, la organización debe de conocer que es lo que esta protegiendo. La política de seguridad se basará en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación del negocio. Si no se posee con la información detallada de la política a seguir, aunque sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

2.3.3. Costo del Firewall

Un simple paquete de filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya esta incluido como estándar del equipo.

Un sistema comercial de firewall provee un incremento más a la seguridad pero su costo puede ser dependiendo de la complejidad y el número de sistemas protegidos.

Si la organización posee al experto en casa, un firewall casero puede ser construido con software de dominio público pero este ahorro de recursos repercuten en términos del tiempo de desarrollo y el despliegue del sistema firewall. Finalmente requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad, e incidentes de manejo.

2.3.4. Componentes del Sistema Firewall

Después de las decisiones acerca de los ejemplos previos, la organización puede determinar específicamente los componentes del sistema. Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Ruteador Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito.

a. Ruteador Filtra-Paquetes

Este ruteador toma las decisiones de rehusar / permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP.

Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP / UDP, el tipo de mensaje ICMP, la interfase de entrada del paquete, y la interfase de salida del paquete.

Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si no se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

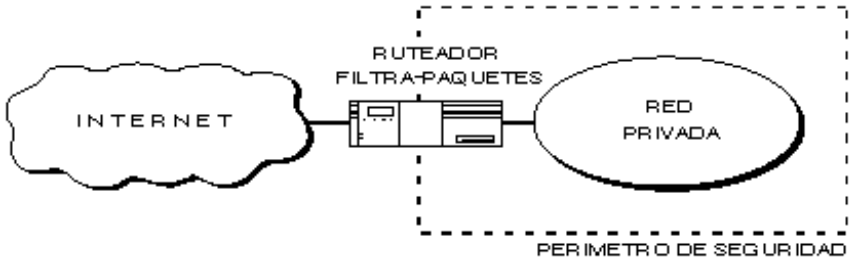


Figura 2.9. Ruteador Filtra-Paquetes.

- **Beneficios del Ruteador Filtra-Paquetes**

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el ruteador, sea este pequeño o no, el costo para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto.

Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el tráfico y definiendo menos filtros.

Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software específico que tenga que ser instalado en cada uno de los servidores.

- **Limitaciones del Ruteador Filtra-Paquetes**

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo más difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete que pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos. Haciendo memoria este tipo de ataques ocurren cuando los datos aparentemente inofensivos se desplazan por el ruteador a un servidor interno.

Los datos contienen instrucciones ocultas que pueden causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al ruteador disminuyen conforme el número de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interfase apropiada de la transmisión.

Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el tráfico. Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto / dato del servicio. Por ejemplo, un administrador de red necesita filtrar el tráfico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a Nivel-aplicación.

b. Gateways a Nivel-Aplicación

Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes.

Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de propósito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características específicas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Un aumento de seguridad de este tipo incrementa los costos en términos del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener los usuarios, dando como resultado un sistema carente de transparencia en el manejo de los usuarios en un ambiente "amigable". Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de "fácil de usar" demandado por la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamás podrán seccionar en el Gateway a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de firewall, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de Troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el filrewall.

Ejemplo: Telnet Proxy

La figura 2.10. ilustra la operación de un Telnet Proxy en un servidor de defensa. Para este ejemplo, un cliente externo ejecuta una sesión Telnet hacia un servidor integrado dentro del sistema de seguridad por el Gateway a nivel-aplicación.

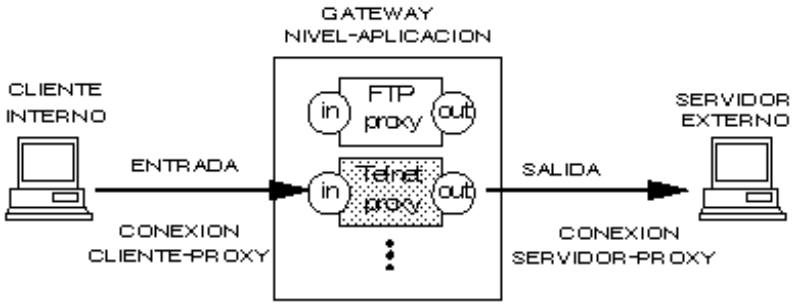


Figura 2.10. Telnet Proxy.

El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un Telnet al servidor de defensa donde es autorizado por la tecnología "una-sola vez" de contraseña. Después de ser autentificado, el cliente obtiene acceso a la interfase de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son disponibles para el acceso vía Telnet.

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, los comandos internos son desplazados hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet Proxy es un cliente externo.

Se presenta la salida en pantalla de la terminal de un cliente externo como la "conexión" al servidor interno una vez establecida. Nótese que el cliente no se está registrando al servidor de defensa - el usuario comienza su sesión autentificándose por el servidor de defensa e intercambia respuestas, una vez que se le ha permitido seccionar se comunica con el Telnet Proxy -. Después de pasar el intercambio de respuestas, el servidor Proxy limita un conjunto de comandos y destinos que están disponibles para los clientes externos.

La autenticación puede basarse en "algo conocido por los usuarios" (como una contraseña) o "algo que tengan" que posean físicamente (como una tarjeta electrónica) cualquiera de las dos. Ambas técnicas están sujetas a plagio, pero usando una combinación de ambos métodos se incrementa la probabilidad del uso correcto de la autenticación. En el ejemplo de Telnet, el Proxy transmite un requerimiento de registro y el usuario, con la ayuda de su tarjeta electrónica, obtendrá una respuesta de validación por un número. Típicamente, se le entrega al usuario su tarjeta desactivada para que él introduzca un PIN y se le regresa la tarjeta, basada en parte como llave "secreta" de encriptación y con un reloj interno propio, una vez que se establece la sesión se obtiene un valor de respuesta encriptado.

- **Beneficios del Gateway a Nivel-Aplicación**

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios.

Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado. Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho más fáciles de configurar y probar que en un ruteador filtra-paquetes.

- **Limitaciones del Gateway a Nivel-Aplicación**

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones del gateway transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de Telnet.

c. Gateway a Nivel-Circuito

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

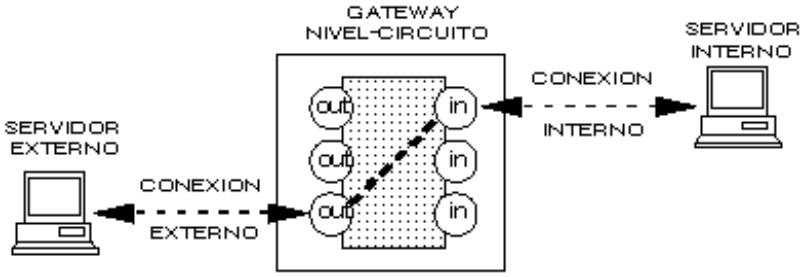


Figura 2.11. Gateway Nivel-Circuito.

La figura 2.11. muestra la operación de una conexión típica Telnet a través de un Gateway a nivel-circuito. Tal como se ha mencionado anteriormente, este gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como un cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar y encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

2.4. REDES PRIVADAS VIRTUALES

Una red se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones). En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones sobre todo las que cuentas con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que se escucha hablar tanto de los famosos firewalls y las VPNs.

2.4.1. Conceptos Básicos

Con los siguientes conceptos, se hace referencia a lo que es Internet, Intranet y Extranet. Planteando estos conceptos se puede establecer de una forma clara y concreta la diferencia entre estos tipos de redes.

a. Internet

Internet se podría definir como una red que engloba una serie de redes de computadores con la finalidad de permitir el libre intercambio de información entre sus usuarios.

Es posible tener acceso a cualquier información: desde las fotografías enviadas por el satélite Meteosat hasta información conseguida en una universidad americana o bien conseguir un programa de utilidad pública que se encuentre en un computador australiano.

Sin embargo, conectarse a Internet es como entrar en una inmensa biblioteca. Hay una gran cantidad de libros en interminables estanterías que contienen una cantidad enorme de información que si no se sabe como buscarla será totalmente inservible.

Además, Internet no es un servicio centralizado. No existe ninguna empresa a la que se pueda solicitar un catálogo de todos los servicios, de todas las bases de datos o un índice donde aparezcan todos los temas. Internet sólo se limita a establecer los procedimientos de interconexión, pero cada red o cada computador tiene su propio dueño.

El precio de conexión a Internet varía de acuerdo con el coste de mantenimiento de cada red, que es la que fija las tarifas a los usuarios que se conectan a ella. También es posible encontrar redes amparadas por los respectivos gobiernos, por lo que los centros que se conecten a ellas sólo pagan por la conexión al punto de acceso más cercano.

b. Intranet

Intranet es un término relativamente nuevo y puede utilizarse para definir red privada que utiliza el conjunto de protocolos TCP/IP y no está conectada a Internet.

Durante muchos años las redes con protocolos TCP/IP accedían a Internet para tener acceso a las múltiples utilidades que estaban disponibles.

A partir de 1994, empezó a ganar partidarios una opción que consistía en utilizar dichos protocolos y las posibilidades que brindaban los servicios disponibles en Internet, pero sin permitir el acceso a Internet. De esta manera surgió el concepto de Intranet.

Gracias a la sencillez de su construcción, de su uso y de su economía, su expansión ha sido rápida.

c. Extranet

El concepto de Extranet es una mezcla de Internet e Intranet y sirve para definir a una **Red Privada Virtual** que utiliza a Internet como medio de transporte de la información entre sus propios nodos. También recibe el nombre de VPN (Virtual Private Networks).

Gracias a una Extranet se puede unir dos Intranets que se encuentran situadas en distintas ubicaciones utilizando X25, RDSI, líneas punto a punto o frame-relay.

Para ello, es necesario que cada una de las Intranets disponga de acceso a un proveedor de acceso de Internet (ISP). Una vez en Internet, los datos serán transmitidos por distintas rutas alternativas hasta llegar a la sede destino.

Para evitar la conexión de personas no autorizadas a las Intranets será necesario contar con cortafuegos (firewalls) y proxies que autentifiquen los accesos, así como proceder a una encriptación de los paquetes que van a viajar desde una sede a la otra.

Uno de los protocolos que permiten crear un túnel seguro a través de Internet es el protocolo PPTP. De esta manera, se tendrá una gran reducción de costes para la empresa y una alta fiabilidad.

2.4.2. De Intranets a Extranets

Una Extranet tiene mucho en común con una Intranet. Aunque se ha dicho que las Intranets son algo que existe detrás de un firewall y operan con propósitos totalmente internos, en realidad no es así.

Al principio, cuando los constructores de las Intranets empezaron a aplicar la tecnología de la World Wide Web a necesidades específicas en las organizaciones, sus aplicaciones siempre incluyeron comunicación interna y externa.

Los negocios exitosos ya no existen como empresas aisladas, han reconocido el valor de la comunicación activa con sus proveedores, por un lado, y con sus clientes, por el otro. A la vez, estos clientes y proveedores están enlazados a otros clientes y proveedores. El resultado es una cadena vinculada de formas múltiples e impredecibles. Cualquier cosa que haga afecta un gran número de los demás.

Esta es la razón por la que las intranets nunca estuvieron limitadas estrictamente a las necesidades de la comunicación interna. También por la que una Extranet no puede estar limitada por completo a la comunicación externa. La diferencia entre la comunicación interna y externa nunca fue respetada en realidad y ha empezado a desaparecer. Al formar sociedades, empresas, proveedores y clientes, aún es notoria una muy leve distinción entre el interior y el exterior. Una Extranet otorga el reconocimiento formal a este hecho ya reconocido desde hace tiempo. La mayoría de los usuarios de intranets permiten ya el acceso externo o piensan hacerlo pronto.

a. Como han Evolucionado las Extranets

Todo inicia con Internet, un fenómeno que ha transformado la industria del cómputo y la manera en que las personas han ampliado el uso de las computadoras.

Al usar Internet y el World Wide Web, las organizaciones han aprendido a utilizar la tecnología web para distribuir información a sus empleados; al fincar intranets, han podido hacerlo a un costo mucho más bajo que los de medios tradicionales, como boletines y memorándums.

Esta es la razón por la que inicialmente las intranets se emplearon para distribuir información corporativa: boletines, políticas, manuales y directorios telefónicos internos.

b. Mejores Cosas del Web

Los desarrolladores de las intranets de primera generación mostraron como se puede utilizar la tecnología web y los métodos para desarrollar páginas web y mejorar la comunicación de grupo, tanto dentro como fuera de su organización. Las técnicas web han hecho más fácil lograr un objetivo a través de las cantidades masivas de información en Internet. Seguramente, pueden ayudar a algunas personas a lograrlo a través de cantidades menores de información que quieren intercambiar como empleados y socios comerciales externos.

En sus declaraciones más visionarias, Netscape prevé un modelo en el cual virtualmente toda la información corporativa estará almacenada en un servidor web. Crear una página web es similar a crear un documento en un procesador de palabras, y sin duda no es más difícil. Casi cualquier persona puede aprender a hacerlo.

Pero, y aquí esta el elemento clave, no cualquiera puede leer o editar la información. Un administrador web puede usar características de control de acceso moderno para determinar quién puede leer y quién puede editar un documento web.

La ventaja de este enfoque es que cualquier persona puede compartir información con facilidad con alguien que esté en el siguiente cubículo o en el siguiente país. Además, esta información puede ser fácil de encontrar y usar. Los beneficios de este enfoque incluyen la habilidad de:

- *Compartir información con menor esfuerzo.* Puede poner un documento en un servidor web y actualizarlo instantáneamente cuando sea necesario. No necesita enviar un correo electrónico a una lista de receptores, quienes ahora pueden “acudir” al mensaje.
- *Encontrar información con menor esfuerzo.* Ahora las herramientas de búsqueda están disponibles más fácilmente y pueden ayudar a encontrar información sin importar dónde esté. A diferencia de las formas anteriores de almacenamiento de datos, ni siquiera necesita saber que el recurso existe: las herramientas de búsqueda pueden encontrarlo de cualquier modo.
- *Reducir los costos de impresión y envío por correo.* Los documentos electrónicos tal vez no ahorren tanto papel y estampillas como algunos optimistas quieren pensar pero los ahorros todavía son posibles.

Desde luego, también hay desventajas potenciales. La seguridad y control de acceso son vitales si necesita proporcionar información a personas fuera de la organización. No obstante, también esto es importante en una Intranet estrictamente interna, así que los retos no son excesivos.

2.4.3. ¿Por qué una VPN?

Cuando se desea enlazar oficinas centrales con alguna sucursal u oficina remota se tiene tres opciones:

Módem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte no contaría con la calidad y velocidad adecuadas.

Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

a. Principio de las VPNs

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (Ver Figura 2.12.)

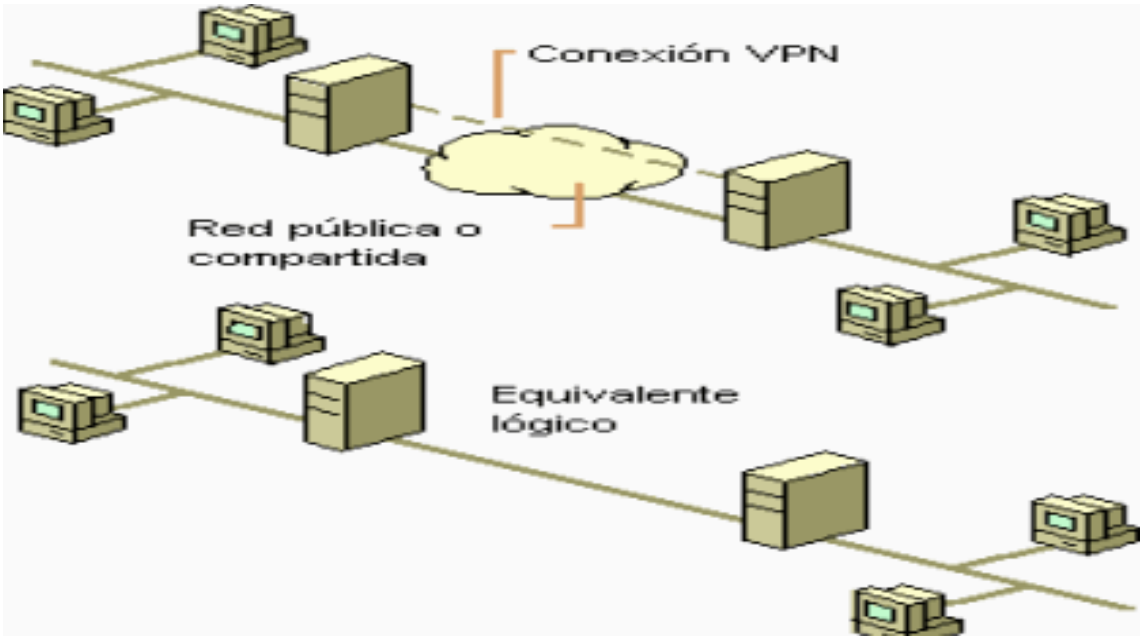


Figura 2.12. Interconexión entre Redes de Datos

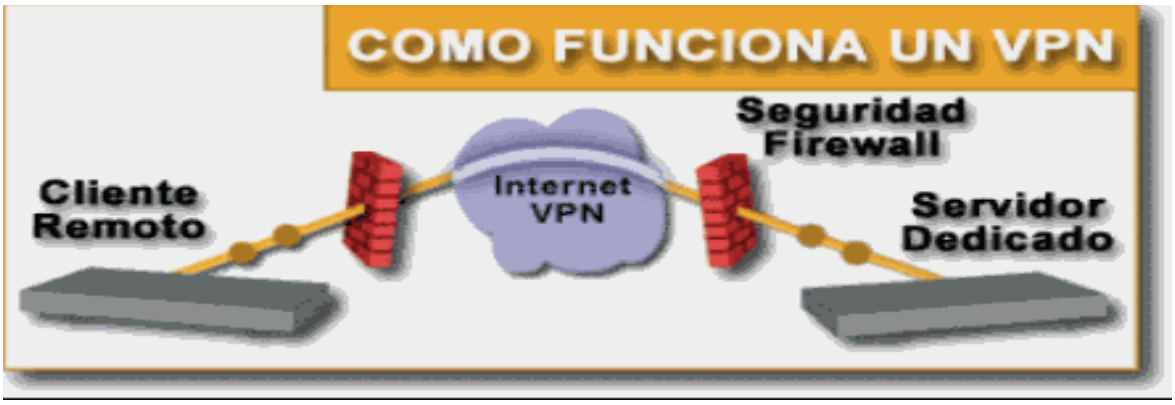


Figura 2.13. Trayectoria de los Datos en una VPN

En la Figura 2.13. se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos viajen con una velocidad garantizada, lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM como lo muestra la Figura 2.14.

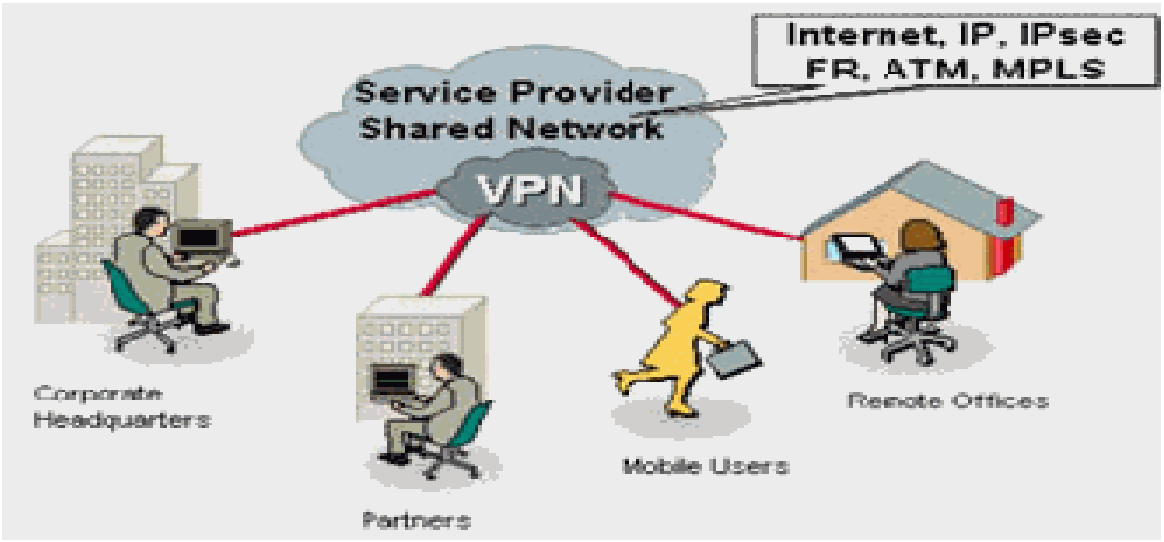


Figura 2.14. Tipos de Servicios en una VPN

b. Tecnología de Túnel

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños.

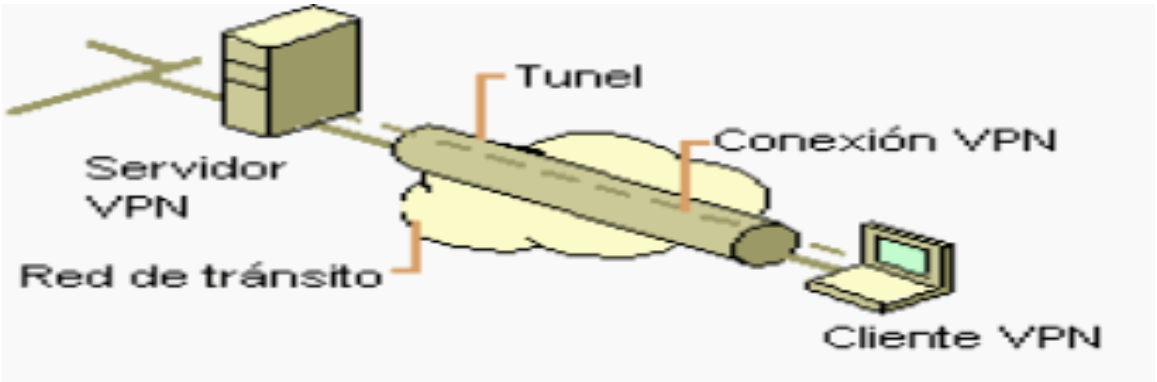


Figura 2.15. Tecnología Túnel

El servidor busca mediante un ruteador la dirección IP del cliente VPN y en la red de tránsito se envían los datos sin problemas.

c. Requerimientos Básicos de una VPN

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

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

Identificación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quién acceso, que información y cuando.

Administración de direcciones

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

Codificación de datos

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

Administración de claves

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

Soporte a protocolos múltiples

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

d. Herramientas de una VPN

- VPN Gateway
- Software
- Firewall
- Router

VPN Gateway

Dispositivos con un software y hardware especial para proveer de capacidad a la VPN.

Software

Esta sobre una plataforma PC o Workstation, el software desempeña todas las funciones de la VPN.

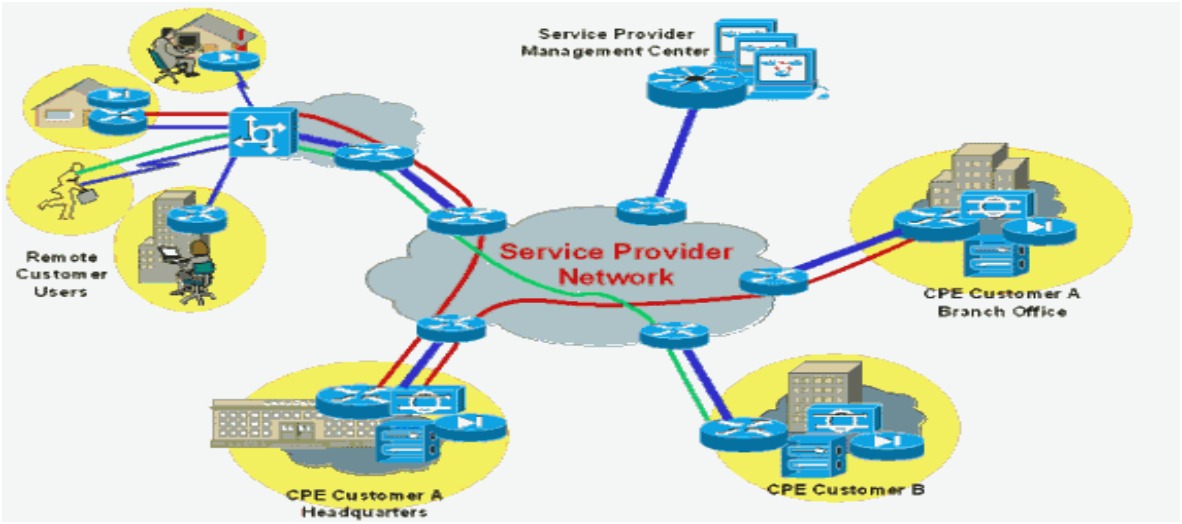


Figura 2.16. Proveedor de Servicio de Red

2.4.4. Como Convertir las Aplicaciones Internas en Externas

La gama de posibles aplicaciones de las Extranets es casi infinita. Casi cualquier cosa que se puede idear para una Intranet puede tener implicaciones externas. Sin embargo, las aplicaciones iniciales comúnmente entran en una de estas categorías:

- *Comunicación de uno o varios equipos, departamentos o corporaciones.* Se puede poner información en una página web, reduciendo el papeleo y obteniendo información disponible casi de inmediato. Los ahorros en costos de impresión pueden ser importantes, pero aun más importante es el ahorro que se hace patente en una mejor comunicación.

- *Aplicaciones que requieren de una interacción hacia ambos lados.* Si tal cosa existe como una aplicación clásica de las Extranets, esta es la ayuda y el soporte técnico. Muchas compañías orientadas a la computación han encontrado que es fácil y reduce costos poner en el web especificaciones e información para resolver problemas, y emplean el correo electrónico como vehículo para recibir y contestar preguntas. De otro modo un empleado necesita información para preparar un informe, analizar datos o documentarse sobre proveedores y clientes. Aquí, un sitio web vinculado a los recursos de la base de datos corporativa puede ser más fácil y rápido que confirmar en informes impresos.
- *Colaboración que requiere de interacciones de muchos a muchos.* En esta categoría están los equipos de noticias cuyos miembros intercambian información. Sus mensajes pueden formar una base de conocimientos valiosos para otras personas. Desde luego, a veces puede desear que los intercambios en información confidencial permanezcan dentro de un grupo controlado. Sin embargo, aún en este caso no siempre será necesario confirmar el grupo a miembros internos. Los proveedores y clientes de confianza pueden, y a veces deben, estar en la cadena de comunicación.

a. Tipos de Aplicaciones

Dentro de estas aplicaciones generales, el desarrollo de aplicaciones, hasta la fecha se ha enfocado a varios tipos específicos:

- Ventas y mercadotecnia
- Desarrollo de producto
- Servicios al cliente

- Recursos humanos
- Financieros

b. Por que la Tecnología Web es tan Atractiva

Los beneficios de una Extranet pueden incluir:

- Acceso inmediato a la información
- Libertad de elección
- Seguridad
- Facilidad de uso
- Costo de instalación moderada
- Costos de impresión y procesamiento más bajos
- Flujo de trabajo más simplificado
- Costos de capacitación más bajos
- Mejor dinámica de grupo

Acceso inmediato a la información

El fácil acceso de una Extranet a muchos tipos de medios pueden hacerla el vehículo idóneo tanto para la comunicación interna como externa. Una Extranet puede proporcionar información de manera:

- Inmediata
- Efectiva en cuanto a costo
- Fácil de usar
- Rica en formato
- Versátil

Libertad de elección

La tecnología web no lo encajona en un sistema de un solo fabricante, ni siquiera Netscape o Microsoft. La tecnología web está disponible para casi todos los sistemas operativos importantes y las plataformas de hardware, y puede mejorar el valor de los sistemas de bases de datos existentes.

Seguridad

El web no es tan insegura como a veces se dice, ni tan segura como sus más ardientes defensores desean. Este es un tema muy importante relacionado con las Extranets, ya que alguien podría querer controlar tanto el acceso al sistema como el tipo de este. Existen varias formas de hacer que una Extranet sea más segura.

Facilidad de uso

El hipertexto es un factor importante para facilitar el uso de una Extranet basada en el web. Los clientes y proveedores pueden aprender a seguir los vínculos de manera inmediata, muchos de ellos ya saben como. Además la tecnología web utiliza un sistema de navegación único. Una vez que se ha aprendido a utilizar esa herramienta, es posible utilizarla para todas las actividades en el web.

Costo de instalación moderado

Una Extranet no es una opción de tan bajo costo como puede parecer a primera vista. Puede ser muy barata o sorprendentemente cara.

Netscape sostiene que el costo típico de un sistema empresarial o de un departamento grande es una inversión moderada por usuario, lo cual es bastante menos que cualquier otra clase de sistema de comunicación o trabajo de grupo.

Costo de impresión y procesamiento más bajos

Los primeros usuarios de las intranets citaron esta ventaja, sobre todo cuando colocaron en línea los manuales impresos. El manual en línea del empleado es casi una plancha de las intranets. Otro terreno fértil para la economía en el costo son los directorios telefónicos (los cuales no necesitan estar registrados a listas internas), hojas de datos de seguridad de los materiales y encuestas entre empleados y clientes.

Flujo de trabajo más simplificado

Una Extranet puede simplificar el flujo de trabajo en labores como el pedido de suministros, archivo de informes y manejo de solicitudes de servicios al cliente.

Mejor dinámica de grupo

Grupos de discusión, periódicos murales, listas de correo y bases de conocimiento en línea facilitan a las personas aprender de otros. Estos vínculos pueden extenderse con facilidad para información externa cimentando el intercambio sencillo de información con los socios comerciales.

2.4.5. Aplicaciones de una VPN

Una Extranet puede ejecutar múltiples aplicaciones tanto ordinarias como hechas a la medida. Algunas son sugeridas por una gama de servicios disponibles a lo ancho de una Extranet.

Otras fueron desarrolladas en forma personalizada y otras más fueron compradas en tiendas especializadas. Estas aplicaciones pueden utilizarse en distintas necesidades comerciales:

- *Procesamiento de pedidos.* Los clientes necesitan información actualizada sobre productos y servicios. Una Extranet permite registrar pedidos, recibir facturas, trastear embarques y procesar pagos sin importar donde estén.
- *Proyectos conjuntos.* Los miembros de un equipo que desarrolla un producto nuevo pueden coordinarse con los proveedores sobre las especificaciones de éste y los métodos de producción. Una Extranet les permite compartir información para que puedan trabajar como un solo equipo, aunque representen distintas compañías. Los clientes se pueden sumar al equipo para asegurar que sus necesidades sean satisfechas.
- *Comunicación sin distorsión.* Las personas en distintas organizaciones necesitan un medio común para compartir información. Ya que está basada en la tecnología web ordinaria y puede trabajar en distintas plataformas, una Extranet puede proporcionar un terreno común para comunicarse con claridad.

- *Servicio y soporte al cliente.* Una Extranet puede proporcionar una forma para que los clientes obtengan una información de apoyo y soluciones a los problemas. Al mismo tiempo, el personal de soporte técnico puede usar los informes de problemas para rastrear las amarguras del cliente, asegurando así que todos se resuelvan de manera adecuada.
- *Correo electrónico.* Una organización grande puede tener con facilidad media docena de sistemas de correo electrónico, el correo electrónico particular es notable por la incompatibilidad con otros sistemas. Cuando aumentan los proveedores y clientes los problemas de compatibilidad pueden empeorar. Evalúe qué puede suceder cuando un empleado de soporte al cliente no tiene modo de saber que es lo qué ha prometido la fuerza de ventas a un cliente clave.
- *Acceso total.* Una organización puede mantener distintas bases de datos con información de clientes y sobre investigaciones de mercado. Una Extranet le proporciona a cualquier persona autorizada la posibilidad de ver todo esto.

Aplicaciones Nativas

La tecnología web utilizada en una Extranet incluye varias aplicaciones inherentes a ella:

- Correo electrónico
- Colaboración en grupo
- Comunicación de audio y video en tiempo real
- Publicar y compartir información
- Navegación de red
- Indización y búsqueda de textos

- Directorios

2.5. HACKERS

Los piratas ya no tienen un parche en su ojo ni un garfio en reemplazo de la mano. Tampoco existen los barcos ni los tesoros escondidos debajo del mar. Ahora, los piratas se presentan con un cerebro desarrollado, curioso y con muy pocas armas: una simple computadora y una línea telefónica. Hackers. Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.

Sólo basta con repasar unas pocas estadísticas. Durante 1997, el 54 por ciento de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas. Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año. El Pentágono, la CIA, UNICEF, La ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan. Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados.

Los medios de comunicación masivos prefieren tildarlos de delincuentes que interceptan códigos de tarjetas de crédito y los utilizan para beneficio propio. También están los que se intrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones. Pero he aquí la gran diferencia en cuestión. Los crackers (crack = destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Esos son los crackers. Adolescentes inquietos que aprenden rápidamente este complejo oficio. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente.

El avance de la era informática ha introducido nuevos términos en el vocabulario de cada día. Una de estas palabras, hacker, tiene que ver con los delitos informáticos. Pero se tiene la impresión de que el término "hacker" es uno de los peor entendidos, aplicados y, por tanto, usados en la era informática.

La cultura popular define a los hackers como aquellos que, con ayuda de sus conocimientos informáticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra. Los criminalistas, por otra parte, describen a los hackers en términos menos halagadores.

El término comenzó a usarse aplicándolo a un grupo de pioneros de la informática del MIT, a principios de la década de 1960. Desde entonces, y casi hasta finales de la década de 1970, un hacker era una persona obsesionada por conocer lo más posible sobre los sistemas informáticos. Pero a principios de la década de 1980, influenciados por la difusión de la película Juegos de Guerra, y el ampliamente publicado arresto de una "banda de hackers" conocida como la 414, los hackers pasaron a ser considerados como chicos jóvenes capaces de violar sistemas informáticos de grandes empresas y del gobierno. Desgraciadamente, los medios de información y la comunidad científica social no ha puesto mucho esfuerzo por variar esta definición. El problema para llegar a una definición más precisa radica, tanto en la poca información que hay sobre sus actividades diarias, como en el hecho de que lo que se conoce de ellos no siempre cabe bajo las etiquetas de los delitos conocidos. Es decir, no hay una definición legal que sea aplicable a los hackers, ni todas sus actividades conllevan la violación de las leyes. Esto lleva a que la aplicación del término varíe según los casos, dependiendo de los cargos que se puedan imputar y no a raíz de un claro entendimiento de lo que el término significa. Este problema, y la falta de entendimiento de lo que significa ser un hacker, convierte a esta en una etiqueta excesivamente utilizada para aplicar a muchos tipos de intrusiones informáticas.

Los términos, "hacker", "phreaker" y "pirata" se presentan y definen tal y como los entienden aquellos que se identifican con estos papeles. En primer lugar, el área de los hackers. En la tradición de esta comunidad informática, el hacker puede realizar dos tipos de actividades: bien acceder a un sistema informático, o bien algo más general, como explorar y aprender a utilizar un sistema informático.

En la primera connotación, el término lleva asociados las herramientas y trucos para obtener cuentas de usuarios validos de un sistema informático, que de otra forma serían inaccesibles para los hackers. Se podría pensar que esta palabra esta íntimamente relacionada con la naturaleza repetitiva de los intentos de acceso. Además, una vez que se ha conseguido acceder, las cuentas ilícitas a veces compartidas con otros asociados, denominándolas "frescas". Una visión estereotipada de los medios de comunicación de los hackers un joven de menos de veinte años, con conocimientos de informática, pegado al teclado de su ordenador, siempre en busca de una cuenta no usada o un punto débil en el sistema de seguridad. Aunque esta visión no es muy precisa, representa bastante bien el aspecto del término. La segunda dimensión del mencionado término se ocupa de lo que sucede una vez que se ha conseguido acceder al sistema cuando se ha conseguido una clave de acceso. Como el sistema esta siendo utilizado sin autorización, el hacker no suele tener, en términos generales, acceso a los manuales de operación y otros recursos disponibles para los usuarios legítimos del sistema. Por tanto, el usuario experimenta con estructuras de comandos y explora ficheros para conocer el uso que se da al sistema. En oposición con el primer aspecto del término, aquí no se trata solo de acceder al sistema (aunque alguno podría estar buscando niveles de acceso más restringidos), sino de aprender más sobre la operación general del sistema. Contrariamente a lo que piensan los medios de comunicación, la mayoría de los hackers no destruyen y no dañan deliberadamente los datos. Él hacerlo iría en contra de su intención de mezclarse con el usuario normal y atraería la atención sobre su presencia, haciendo que la cuenta usada sea borrada. Después de gastar un tiempo sustancioso en conseguir la cuenta, el hacker pone una alta

prioridad para que su uso no sea descubierto. Además de la obvia relación entre las dos acepciones, la palabra "hacker" se reserva generalmente a aquellos que se dedican al segundo tipo. En otras palabras, un hacker es una persona que tiene el conocimiento, habilidad y deseo de explorar completamente un sistema informático. El simple hecho de conseguir el acceso (adivinando la clave de acceso) no es suficiente para conseguir la denominación. Debe haber un deseo de liderar, explotar y usar el sistema después de haber accedido a él. Esta distinción parece lógica, ya que no todos los intrusos mantienen el interés una vez que han logrado acceder al sistema. En el submundo informático, las claves de acceso y las cuentas suelen intercambiarse y ponerse a disposición del uso general. Por tanto, el hecho de conseguir el acceso puede considerarse como la parte "fácil", por lo que aquellos que utilizan y exploran los sistemas son los que tienen un mayor prestigio. La segunda actividad es la de los phreakers telefónicos. Se trata de una forma de evitar los mecanismos de facturación de las compañías telefónicas. Permite llamar a de cualquier parte del mundo sin costo prácticamente.

En muchos casos, también evita, o al menos inhibe, la posibilidad de que se pueda trazar el camino de la llamada hasta su origen, evitando así la posibilidad de ser atrapado. Par la mayor parte de los miembros del submundo informático, esta es simplemente una herramienta para poder realizar llamadas de larga distancia sin tener que pagar enormes facturas. La cantidad de personas que se consideran phreakers, contrariamente a lo que sucede con los hackers, es relativamente pequeña. Pero aquellos que si se consideran phreakers lo hacen para explorar el sistema telefónico.

La mayoría de la gente, aunque usa el teléfono, sabe muy poco acerca de él. Los phreakers, por otra parte, quieren aprender mucho sobre él. Este deseo de conocimiento lo resume así un phreaker activo: "El sistema telefónico es la cosa más interesante y fascinante que conozco. Hay tantas cosas que aprender. Incluso los phreakers tienen diferentes áreas de conocimiento. Hay tantas cosas que se pueden conocer que en una tentativa puede aprenderse algo muy importante y en la siguiente no. O puede suceder lo contrario. Todo depende de como y donde obtener la información. Yo mismo quisiera trabajar para una empresa de telecomunicaciones, haciendo algo interesante, como programar una central de conmutación. Algo que no sea una tarea esclavizadora e insignificante. Algo que sea divertido. Pero hay que correr el riesgo para participar, a no ser que tengas la fortuna de trabajar para una de estas compañías. El tener acceso a las cosas de estas empresas, como manuales, etc., debe ser grandioso". La mayoría de la gente del submundo no se acerca al sistema telefónico con esa pasión. Solo están interesados en explorar sus debilidades para otros fines. En este caso, el sistema telefónico es un fin en sí mismo. Otro entrevistado que se identificaba a sí mismo como hacker, explicaba: "Sé muy poco sobre teléfonos simplemente soy un hacker. Mucha gente hace lo mismo. En mi caso, hacer de phreaker es una herramienta, muy utilizada, pero una herramienta al fin y al cabo". En el submundo informático, la posibilidad de actuar así se agradece, luego llegó el uso de la tarjeta telefónica. Estas tarjetas abrieron la puerta para realizar este tipo de actividades a gran escala. Hoy en día no hace falta ningún equipo especial. Solo un teléfono con marcación por tonos y un número de una de esas tarjetas, y con eso se puede llamar a cualquier parte del mundo. De igual forma que los participantes con más conocimientos y motivación son llamados hackers, aquellos

que desean conocer el sistema telefónico son denominados phreakers. El uso de las herramientas que les son propias no esta limitada a los phreakers, pero no es suficiente para merecer la distinción. Finalmente llegamos a la "tele piratería" del software. Consiste en la distribución ilegal de software protegido por los derechos de autor. No se refiere a la copia e intercambio de disquetes que se produce entre conocidos (que es igualmente ilegal), sino a la actividad que se realiza alrededor de los sistemas BBS que se especializan en este tipo de tráfico. El acceso a este tipo de servicios se consigue contribuyendo, a través de un módem telefónico, con una copia de un programa comercial. Este acto delictivo permite a los usuarios copiar, o "cargar", de tres a seis programas que otros hayan aportado.

Así, por el precio de una sola llamada telefónica, uno puede amontonar una gran cantidad de paquetes de software. En muchas ocasiones, incluso se evita pagar la llamada telefónica. Nótese que al contrario que las dos actividades de hacker y phreaker, no hay ninguna consideración al margen de "prestigio" o "motivación" en la tele piratería. En este caso, el cometer los actos basta para "merecer" el título.

La tele piratería esta hecha para las masas. Al contrario de lo que sucede con los hackers y los phreakers, no requiere ninguna habilidad especial. Cualquiera que tenga un ordenador con módem y algún software dispone de los elementos necesarios para entrar en el mundo de la tele piratería. Debido a que la tele piratería no requiere conocimientos especiales, el papel de los piratas no inspira ningún tipo de admiración o prestigio en el submundo informático. (Una posible excepción la constituyen aquellos que son capaces de quitar la protección del software comercial).

Aunque los hackers y los phreakers de la informática probablemente no desaprueben la piratería, y sin duda participen individualmente de alguna forma, son menos activos (o menos visibles) en los BBS que se dedican a la tele piratería. Tienden a evitarlos porque la mayoría de los tele piratas carecen de conocimientos informáticos especiales, y por tanto son conocidos por abusar en exceso de la red telefónica para conseguir el último programa de juegos.

Un hacker mantiene la teoría de que son estos piratas los culpables de la mayoría de los fraudes con tarjetas de crédito telefónicas. "Los medios de comunicación afirman que son únicamente los hackers los responsables de las pérdidas de las grandes compañías de telecomunicaciones y de los servicios de larga distancia. Este no es el caso. Los hackers representan solo una pequeña parte de estas pérdidas. El resto esta causado por "los piratas y ladrones que venden estos códigos en la calle." Otro hacker explica que el proceso de intercambiar grandes programas comerciales por módem normalmente lleva varias horas, y son estas llamadas, y no las que realizan los "entusiastas de telecomunicaciones", las que preocupan a las compañías telefónicas. Pero sin considerar la ausencia de conocimientos especiales, por la fama de abusar de la red, o por alguna otra razón, parece haber algún tipo de división entre los hackers / phreakers y los tele piratas. Después de haber descrito los tres papeles del submundo informático, se puede ver que la definición presentada al principio, según la cual un hacker era alguien que usaba una tarjeta de crédito telefónico robada para cargar alguno de los últimos juegos, no refleja las definiciones dadas en el propio submundo informático.

Obviamente, corresponde a la descripción de un tele pirata y no a las acciones propias de un hacker o un phreaker. En todo esto hay una serie de avisos. No se quiere dar la impresión de que un individuo es un hacker, un phreaker o un tele pirata exclusivamente.

Estas categorías no son mutuamente excluyentes. De hecho, muchos individuos son capaces de actuar en más de uno de estos papeles. Se cree que la respuesta se encuentra en buscar los objetivos que se han expuesto previamente. Recuérdese que el objetivo de un hacker no es entrar en un sistema, sino aprender como funciona. El objetivo de un phreaker no es realizar llamadas de larga distancia gratis, sino descubrir lo que la compañía telefónica no explica sobre su red y el objetivo de un tele pirata es obtener una copia del software más moderno para su ordenador. Así, aunque un individuo tenga un conocimiento especial sobre los sistemas telefónicos, cuando realiza una llamada de larga distancia gratis para cargar un juego, esta actuando como un tele pirata. En cierto modo, esto es un puro argumento semántico. Independientemente de que a un hacker se le etiquete erróneamente como tele pirata, los accesos ilegales y las copias no autorizadas de software comercial van a seguir produciéndose. Pero si queremos conocer los nuevos desarrollos de la era informática, se debe identificar y reconocer los tres tipos de actividades más comunes. El agrupar los tres tipos bajo una sola etiqueta es más que impreciso, ignora las relaciones funcionales y diferencias entre ellos. Hay que admitir, de todas formas, que siempre habrá alguien que este en desacuerdo con las diferencias que se han descrito entre los grupos.

Pero, de la misma forma que no se debe agrupar toda la actividad del submundo informático bajo la representación de hacker, tampoco se debe insistir en que nuestras definiciones sean exclusivas hasta el punto de ignorar lo que representan. Las definiciones que he presentado son amplias y necesitan ser depuradas. Pero representan un paso más en la representación precisa, especificación e identificación de las actividades que se dan en el submundo de la informática.

2.5.1. Que se Necesita para Ser un Hacker

Uno puede estar preguntándose ahora mismo si los hackers necesitan caros equipos informáticos y una estantería rellena de manuales técnicos. La respuesta es no! ,Hackear puede ser sorprendentemente fácil, mejor todavía, si se sabe cómo explorar el World Wide Web, se puede encontrar casi cualquier información relacionada totalmente gratis.

De hecho, hackear es tan fácil que si se tiene un servicio on-line y se sabe cómo enviar y leer un e-mail, se puede comenzar a hackear inmediatamente. A continuación se podrá encontrar una guía dónde puede bajarse programas especialmente apropiados para el hacker sobre Windows y que son totalmente gratis. Y trataremos también de explicar algunos trucos de hacker sencillos que puedan usarse sin provocar daños intencionales.

a. Los Diez Mandamientos del Hacker

I. Nunca destrozar nada intencionalmente en la computadora que estés hackeando.

II. Modificar solo los archivos que hagan falta para evitar que uno sea detectado y asegurar tu acceso futuro al sistema.

III. Nunca dejar la dirección real, nombre o teléfono en ningún sistema.

IV. Tener cuidado a quien se le pasa la información. A ser posible no pasar nada a nadie que no se conozca su voz, número de teléfono y nombre real.

V. Nunca dejar datos reales en un BBS, si no se conoce al sysop, se puede dejar un mensaje con una lista de gente que pueda responder de ti.

VI. Nunca hackear en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscar al violador del sistema mientras que las universidades y las empresas particulares no.

VII. No usar BlueBox a menos que no se tenga un servicio local. Si se abusa de la bluebox, se puede ser cazado.

VIII. No dejar en ningún BBS mucha información del sistema que se esta hackeando. Se debe decir sencillamente "estoy trabajando en un UNIX o en un COSMOS...." pero no se debe decir a quien pertenece ni el teléfono.

IX. No preguntar, nadie va a contestar, se debe pensar que por responder a una pregunta, se corre el riesgo de ser descubierto, o al que contesta o a ambos.

X. Punto final. Se puede navegar tranquilamente por el WEB, y mil cosas más, pero hasta que no se esté realmente hackeando, no se sabrá lo que es.

b. Pasos para Hackear

1.Introducirse en el sistema que tengamos como objetivo.

2.Una vez conseguido el acceso, obtener privilegios de root (superusuario).

3.Borrar las huellas.

4.Poner un sniffer para conseguir logins de otras personas.

2.5.2. Métodos y Herramientas de Ataque

En los primeros años, los ataques involucraban poca sofisticación técnica. Los insiders (empleados disconformes o personas externas con acceso a sistemas dentro de la empresa) utilizaban sus permisos para alterar archivos o registros. Los outsiders (personas que atacan desde afuera de la ubicación física de la organización) ingresaban a la red simplemente averiguando una password válida.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevo a la desaparición de aquellas organizaciones o empresas con altísimo grado de dependencia tecnológica (bancos, servicios automatizados, etc.).

Estos nuevos métodos de ataque han sido automatizados, por lo que en muchos casos sólo se necesita conocimiento técnico básico para realizarlos. El aprendiz de intruso tiene acceso ahora a numerosos programas y scripts de numerosos "hacker" bulletin boards y web sites, donde además encuentra todas las instrucciones para ejecutar ataques con las herramientas disponibles.

Los métodos de ataque descritos a continuación están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras.

Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derechos a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

a. Eavesdropping y Packet Sniffing

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

b. Snooping y Downloading

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes.

Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos más resonantes de este tipo de ataques fueron: el robo de un archivo con más de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

c. Tampering o Data Diddling

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders o outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples web sites han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos esta dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus, de reciente aparición.

d. Spoofing

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y en otro. Este proceso, llamado Looping, tiene la finalidad de evaporar la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

Otra consecuencia del looping es que una compañía o gobierno pueden suponer que están siendo atacados por un competidor o una agencia de gobierno extranjera, cuando en realidad están seguramente siendo atacado por un insider, o por un estudiante a miles de Km de distancia, pero que ha tomado la identidad de otros.

El looping hace su investigación casi imposible, ya que el investigador debe contar con la colaboración de cada administrador de cada red utilizada en la ruta, que pueden ser de distintas jurisdicciones.

Los protocolos de red también son vulnerables al spoofing. Con el IP spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete.

El envío de falsos e-mails es otra forma de spoofing permitida por las redes. Aquí el atacante envía a nombre de otra persona e-mails con otros objetivos. Tal fue el caso de una universidad en USA que en 1998 debió reprogramar una fecha completa de exámenes ya que alguien en nombre de la secretaría había cancelado la fecha verdadera y enviado el mensaje a toda la nómina (163 estudiantes).

Muchos ataques de este tipo comienzan con ingeniería social, y la falta de cultura por parte de los usuarios para facilitar a extraños sus identificaciones dentro del sistema. Esta primera información es usualmente conseguida a través de una simple llamada telefónica.

e. Jamming o Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

f. Caballos de Troya

Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (P.ej. Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

g. Bombas Lógicas

Este suele ser el procedimiento de sabotaje más comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificará la información o provocará el cuelgue del sistema.

h. Ingeniera Social

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Cómputo los administradores son amigos o conocidos.

i. Difusión de Virus

Si bien es un ataque de tipo tampering, difiere de este porque puede ser ingresado al sistema por un dispositivo externo (disquetes) o través de la red (e-mails u otros protocolos) sin intervención directa del atacante. Dado que el virus tiene como característica propia su auto reproducción, no necesita de mucha ayuda para propagarse a través de una LAN o WAN rápidamente, si es que no esta instalada una protección antivirus en los servidores, estaciones de trabajo, y los servidores de e-mail.

Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc.) y los sectores de boot-partition de discos y disquetes, pero aquellos que causan en estos tiempos más problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Además son multiplataforma, es decir, no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras. Cientos de virus son descubiertos mes a mes, y técnicas más complejas se desarrollan a una velocidad muy importante a medida que el avance tecnológico permite la creación de nuevas puertas de entrada. Por eso es indispensable contar con una herramienta antivirus actualizada y que pueda responder rápidamente ante cada nueva amenaza.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.

j. Explotación de Errores de Diseño, Implementación u Operación

Muchos sistemas están expuestos a "agujeros" de seguridad que son explotados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" han sido descubiertas en aplicaciones de software, sistemas operativos, protocolos de red, browsers de Internet, correo electrónico y toda clase de servicios en LAN o WANs.

Sistemas operativos abiertos como Unix tienen agujeros más conocidos y controlados que aquellos que existen en sistemas operativos cerrados, como Windows NT. Constantemente encontramos en Internet avisos de nuevos descubrimientos de problemas de seguridad (y herramientas de hacking que los explotan), por lo que hoy también se hace indispensable contar con productos que conocen esas debilidades y pueden diagnosticar un servidor, actualizando su base de datos de tests periódicamente.

Además de normas y procedimientos de seguridad en los procesos de diseño e implementación de proyectos de informática.

k. Obtención de Passwords, Códigos y Claves

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.

Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.

Por ser el uso de passwords la herramienta de seguridad más cercana a los usuarios, es aquí donde hay que poner énfasis en la parte "humana" con políticas claras (como se define una password?, a quién se esta autorizado a revelarla?) y una administración eficiente (cada cuánto se están cambiando?)

No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

I. Eliminar el Blanco

Ping mortal. Algunos ataques eliminan el blanco en lugar de inundarlo con trabajo. Un ejemplo de este tipo es el ping mortal, un paquete ping ilícitamente enorme, que hace que el equipo de destino se cuelgue. Muchas implementaciones de routers, la mayoría de los Unix y todas las versiones de Windows se mostraron vulnerables a este ataque cuando se lo descubrió por primera vez hace un par de años. A pesar de que los vendedores lanzaron parches de inmediato, hay todavía cantidades significativas de hosts "no corregidos" en las redes de producción (en especial, las que corren bajo el Windows 95).

TCP/IP permite un tamaño máximo de paquete de 64 kilobytes (KB, este máximo está dividido en piezas mucho más pequeñas a través de protocolos de capas más bajas, como Ethernet o token ring, pero dentro de una computadora, paquetes mucho más grandes son posibles). Para lidiar con un paquete de 64 KB, la cola TCP/IP asigna un buffer en memoria de 64 KB. Al recibir una cantidad ilícitamente grande de información, como un ping mortal, el buffer del equipo de destino se desborda y el sistema se puede colgar.

2.5.3. ¿Son Seguros los Software de Encriptación de Datos?

Según expertos argentinos, el software que importan algunas empresas argentinas desde los Estados Unidos para proteger sus datos confidenciales no tiene los niveles de seguridad esperados. Para Ariel Futoransky, del laboratorio de seguridad informática argentino Core SDI, por ejemplo, los programas de encriptación de datos que se importan de ese país pueden ser fácilmente violados.

"Esto es así porque en los Estados Unidos hay grandes restricciones para exportar este tipo de software. Tienen miedo de que en todo el mundo se usen los mismos programas que utilizan ellos y de este modo se puedan desarrollar métodos para interferir organismos oficiales clave, como los de inteligencia o seguridad".

La encriptación usa una técnica -la criptografía- que modifica un mensaje original mediante una o varias claves, de manera que resulte totalmente ilegible para cualquier persona. Y solamente lo pueda leer quien posea la clave correspondiente para descifrar el mensaje. Junto con la firma digital y las marcas de aguas digitales (digital watermark), la encriptación es una de las posibles soluciones para proteger datos cuando son enviados a través de redes como Internet.

La preocupación que tienen en los Estados Unidos por el uso indebido de estos programas es muy fuerte. El software de encriptación tiene las mismas restricciones de exportación que los planos de armas nucleares.

Con este panorama, no es alocado sospechar de la calidad de los programas que, a pesar de todas las restricciones, logran salir de los Estados Unidos. Porque si en ese país son tan celosos de su seguridad, se puede pensar que sólo exportarán los programas menos poderosos.

"Nosotros creemos que si el software salió de los Estados Unidos no es seguro. Si lo que se busca es proteger información importante, las empresas tienen que buscar otras estrategias de seguridad", agregó Futoransky.

2.5.4. Buscadores de Agujeros

En la Argentina existe un grupo de laboratorios y consultoras dedicado a buscar "agujeros" en los sistemas de seguridad. Core SDI tiene sus propios laboratorios, donde se investigan y evalúan las distintas tecnologías de seguridad informática para desarrollar otras en función de los resultados que obtienen.

Además de proveer software, Zampatti, Maida & Asociados ofrece servicios de consultoría, soporte técnico y capacitación. También envía por e-mail un resumen con las últimas noticias acerca de nuevos virus y problemas de seguridad en programas de encriptación.

Por su parte, la empresa GIF tiene servicios de seguridad informática, controla fraudes y desarrolla software para proteger la información, como Firewalls (barreras de seguridad entre una red interna conectada a Internet o a una intranet) y sistemas de encriptación.

Todas tienen el mismo objetivo: investigar las tecnologías de seguridad informática y adaptarlas (si se puede) a las necesidades.

Hoy, en muchas corporaciones, un hambre de información perpetuo e insaciable ha generado temas de seguridad graves y difíciles de solucionar. El crecimiento de Internet ha generado un aumento en las posibilidades de intrusión electrónica desde adentro y desde afuera de las empresas.

No cabe duda de que los gerentes de sistemas y de redes necesitan contar con métodos y mecanismos efectivos, capaces de detectar ataques y disminuir el riesgo de robo de información, sabotaje y todo acceso no deseado a datos de la empresa.

A pesar de que los "net management systems" (sistemas de administración de redes), los "routers" y los "firewalls" son capaces de registrar problemas de la red predefinidos, un nuevo tipo de software llamado intrusion detection system (IDS) (sistema de detección de intrusos) los supera en términos de qué es lo que detectan y cómo denuncian los problemas potenciales a los gerentes de redes.

Los productos IDS no eliminan todos los problemas de seguridad, pero ofrecen beneficios que los convierten en una opción que vale la pena considerar.

Para observar la conducta real de los IDS, NSTL Inc. (Conshohocken, PA) revisó de forma sistemática y probó cinco productos IDS de primera línea, fabricados por Anzen, Cisco, ISS e Internet Tools Inc. Estas pruebas proveen a los gerentes de redes de toda la información que necesitan para determinar de qué forma los productos IDS pueden servir a sus necesidades de protección de la red.

Los resultados de la prueba de NSTL permiten también a los gerentes de redes tomar prudentes decisiones de compra, basadas en "rated management capabilities" (capacidades nominales de administración) y "benchmarked performance" (performance de pruebas).

2.5.5. Los Malos También Saben Mucho

El nivel de importancia que se le da a la cuestión de la seguridad se generalizó en los últimos años. Esto significa que las empresas son cada vez más conscientes del tema y no escatiman esfuerzos para evitar ser vulneradas.

Esta conclusión lleva a pensar que la seguridad creció. Pero esto no es así, porque simultáneamente aumentó y se difundieron la tecnología y los conocimientos para hackear. Por lo tanto, el nivel de inseguridad aumentó.

"En el año 1995, con la ejecución de algunas herramientas específicas de ataque y penetración, se hallaron 150 puntos vulnerables en diversos sistemas de red. En el último año, las mismas herramientas fueron utilizadas sobre las nuevas versiones de los sistemas operativos y el resultado fue peor: se encontraron 450 puntos débiles, pese a los avances y la mejora tecnológica de los softwares".

Esto hace que las compañías de software presten cada vez más atención al problema. "El Windows 2000, por ejemplo, que aún no salió al mercado, ya fue sometido a pruebas de este tipo y se le detectaron problemas de seguridad".

a. La Inversión

Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Esto hace que la implementación de mecanismos de seguridad se dé prácticamente en todos los niveles. Empresas grandes, medianas, chicas y las multinacionales más grandes. Todas pueden acceder a las herramientas que necesitan y los costos (la inversión que cada empresa debe realizar) van de acuerdo con la empresa.

"Pero no es sólo una cuestión de costos. Los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad cada empresa deba actualizar permanentemente las herramientas con las que cuenta. Como los hackers mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico".

Según testers, "esto es tan importante como el tipo de elementos que se usen". Sin duda, éstos deben ser las que mejor se adapten al tipo de organización. Pero tan importante como eso es el hecho de conocer exactamente cómo funcionan y qué se puede hacer con ellos. "Es prioritario saber los riesgos que una nueva tecnología trae aparejados".

b. Las Regulaciones

Una de las herramientas de seguridad que se utiliza en la actualidad es la encriptación, pero esta técnica no es perfecta. En los Estados Unidos una serie de regulaciones le ponen un techo al nivel de encriptación.

El máximo nivel permitido hasta hace alguno tiempo (64 bits) perdió confiabilidad desde que se logró vulnerarlo.

En los Estados Unidos se está buscando un algoritmo de encriptación que permita unos diez años de tranquilidad. Es decir, que durante ese tiempo nadie logre tener los medios tecnológicos que le posibiliten descifrarlo. Además se está tratando de integrar a las empresas proveedoras de softwares con las compañías que los utilizan, o sea, unir a clientes y proveedores para encontrar opciones más seguras.

2.5.6. Restricciones Legales.

En algunos países existen muchas restricciones legales para el comercio electrónico, y esto impide la evolución del desarrollo de las aplicaciones y la implementación de software de seguridad para los negocios en línea.

Desgraciadamente, no sólo se enfrenta el problema técnico sino el legal porque cuando se utiliza una firma electrónica autorizada por las empresas involucradas en una transacción, por ejemplo, no se puede probar en un juicio que esta firma es auténtica. No existe una autoridad certificadora, éste es uno de los problemas más serios.

No se puede considerar que la seguridad sea cuestión de una sola cosa, ya que hay muchos elementos y soluciones en la infraestructura de informática de una empresa.

Por ejemplo, muchas de las claves en la criptología son fácilmente descifrables, se debe ver otras alternativas de tecnología de otros países de Europa, Israel, Rusia y no sólo en las soluciones americanas que presentan también muchas restricciones legales para su importación.

Algunas medidas para hacer frente al creciente problema de la falta de seguridad son: entre ellas la importancia de evaluar su vulnerabilidad interna y hacerse conscientes de que sí bien existen muchas violaciones externas y muchas soluciones tecnológicas, existe un porcentaje muy alto de inseguridad interna como resultado de problemas organizacionales.

Esto enmarca la importancia de contar con políticas internas específicas que cuenten con el apoyo de los altos directivos, así como la existencia de un responsable en la seguridad interna cuyas decisiones de protección se realicen en función de problemáticas específicas y no sujetas a ajustes económicos.

2.5.7. Barrera al Comercio Electrónico

Recientemente ha aparecido publicada una encuesta sobre las barreras al comercio electrónico, llevada a cabo por ITAA (Information Technology Association of America) y la consultora Ernst & Young.

Es un hecho que el comercio electrónico no ha experimentado todavía el crecimiento ni la aceptación que el entusiasmo inicial pronosticaba para el futuro inmediato.

La encuesta tenía por cometido el analizar cuáles eran los mayores factores que actúan de freno a la expansión de la actividad comercial en Internet y de acuerdo con los resultados obtenidos, la barrera más importante es, obviamente, la falta de confianza (señalada por el 62% de los encuestados).

Esta desconfianza hacia las nuevas tecnologías se articula en torno a tres temores fundamentales:

1. La privacidad (60%), que los usuarios finales sienten amenazada en la medida en que desconocen hasta qué punto los datos personales que suministran a un servidor de comercio electrónico serán tratados de forma confidencial. ¿Quién le asegura al comprador que sus datos no se almacenarán a la ligera, siendo accesibles fácilmente por un hacker o un empleado desleal? ¿Cómo saber que no se revenden a terceros?

2. La autenticación (56%), que inquieta a los usuarios, quienes dudan si la persona con la que se comunican es verdaderamente quien dice ser. Sin embargo, dada la relativa facilidad de falsificar una página web e incluso un sitio web completo, ¿cómo asegurarse de que se está comprando en una tienda virtual o en una imitación fiel?

3. La seguridad global (56%), que preocupa a los usuarios, pues temen que la tecnología no sea suficientemente robusta para protegerlos frente a ataques y apropiaciones indebidas de información confidencial, especialmente en lo que respecta a los medios de pago.

Es interesante el hecho de que de toda la actividad de compra, lo que más sigue preocupando es la operación de pago, es decir, el momento en el que el comprador se enfrenta a la ventana donde han introducido su número de tarjeta de crédito y duda a la hora de pulsar el botón de "Enviar". "¿Me robarán?, ¿seré víctima de un fraude?", se pregunta el usuario en el último momento.

Estos temores, qué duda cabe, tienen su fundamento real y su solución no resulta trivial. En el primer caso, la tecnología, y en concreto la criptografía, ofrecen las herramientas necesarias para la protección férrea de la información almacenada en las bases de datos corporativas, información como listas de clientes, sus datos personales y de pago, listas de pedidos, etc. Existen muchas técnicas de control de acceso que hábilmente implantadas garantizan el acceso a la información confidencial exclusivamente a aquellos usuarios autorizados para ello. Ahora bien, se han producido incidentes de servidores de comercio que almacenaron esta clase de información sensible ¡en archivos accesibles vía web por cualquier navegante! Por lo tanto, aunque la criptografía provee de medios aptos, depende en última instancia de la empresa el nivel de compromiso que adopte respecto a la seguridad de los datos que conserva en sus ficheros y su política de control de acceso. Así pues, éste es un temor bien presente y sin fácil respuesta. La tecnología nada tiene que decir si un comerciante decide vender su información a terceros. La delgada línea que protege la privacidad del usuario está constituida en este caso por la integridad moral de la empresa.

En el segundo caso, la solución inmediata que ofrece la criptografía viene de la mano de los certificados digitales. La tecnología de certificación está suficientemente madura como para autenticar adecuadamente a las partes involucradas en una transacción. La más comúnmente utilizada es SSL y a pesar de la tan golpeada limitación criptográfica fuera de Norteamérica de claves débiles de 40 bits, lo cierto es que a la hora de autenticar a las partes, principalmente al servidor, SSL funciona satisfactoriamente. Otro asunto es si asegura o no la confidencialidad, cuestión más que dudosa, si se tiene en cuenta que una clave de 40 bits se rompe en cuestión de horas, con lo que los datos por ella protegidos quedan al descubierto rápidamente. Otras tecnologías emergentes, ofrecen mucha mayor confianza en este campo y, de paso, dan solución al primer problema de la privacidad, ya que permite autenticar a las partes involucradas en la transacción de manera completamente segura, sin restricciones criptográficas debidas a absurdas leyes de exportación. Su mecanismo de firma dual garantiza además que el comerciante no conocerá los datos de pago (número de tarjeta de crédito), eliminando así la posibilidad de fraude por su parte. Esto garantiza así que el comerciante cobra por la venta y que el comprador no es estafado por el comerciante ni por hackers.

En cuanto al tercer temor, nuevamente la criptografía y los productos de seguridad proporcionan las soluciones a los problemas.

Otra cuestión es: ¿incorporan los servidores de comercio todas las medidas necesarias para asegurar las transacciones con el usuario?. Las herramientas ofrecen solución tecnológica a los retos que se le presentan a la seguridad en el comercio electrónico, pero ¿se usa correctamente? ¿Se usa en absoluto?

Por lo que parece, las verdaderas barreras al comercio electrónico no son tanto tecnológicas como humanas. Una vez más, el eslabón más débil de la cadena es de índole personal, no tecnológico.

2.5.8. El mayor Agujero de Seguridad

Reconozcámoslo sin complejos: El mayor agujero de seguridad no se encuentra en ningún producto de Microsoft.

La vulnerabilidad más grave está localizada en el cerebro de la persona que se sienta delante de la pantalla y desplaza el puntero del ratón con su mano.

Y es que, si lo pensamos con detenimiento, no deja de resultar increíble que se sigan produciendo, cada cierto tiempo, epidemias masivas de virus, troyanos y gusanos a través del correo electrónico. El ILOVEYOU fue todo un bombazo, pero es que antes de él estuvo Melissa, y PrettyPark, y CIH, y todos esos gusanos escritos en Visual Basic Script.

Todos estos intrusos necesitan que sea el usuario quien abra el fichero adjunto en el mensaje recibido, y es aquí donde surge el incuestionable delito; ojalá existiera algún invento de hardware o de software que, como una especie de Pepito Grillo cibernético, formulara al oído del usuario del PC preguntas como "¿Conoces a la persona que te envía ese archivo?", "¿Desde cuándo tu primo Manolo te escribe e-mails en inglés?", "¿Tienes la seguridad de que ese fichero realmente contiene una foto de la última vigilante de la playa desnuda?"

El ‘malware’ no necesita idear nuevas y complicadas técnicas de infección, ni avanzados mecanismos de ocultación. Simplemente aprovechando esta actitud que se critica y trabaja, con la llamada "Ingeniería Social" es posible convencer a cualquier usuario poco avezado para que haga exactamente lo que el intruso quiera; además, no se está únicamente ante atentados contra la privacidad o integridad de los datos (virus, gusanos y troyanos), sino también de una posible reducción de la productividad, sobre todo en entornos corporativos. Por ejemplo, todos hemos recibido esas famosas cartas en cadena, que piden ser reenviadas a otras 20 personas.

En definitiva, es el usuario, en último extremo, quien debe evaluar el alcance y las implicaciones de sus acciones.

2.5.9. Hechos Destacables

En 1996, la página Web de Kriesgman (http://www.kriesgam.com/), una de las principales fábricas de pieles de Estados Unidos fue hackeada por unos chicos que pusieron carteles y frases en defensa del animal y la ecología. También en noviembre de 1996 fue asaltada la página de la Agencia Central de Inteligencia de los EE. UU (CIA) (http://www.odci.gov/cia) y en su lugar ubicaron la frase "Welcome to the Central Stupidity Agency".

Las famosas cantantes inglesas de Spice Gilrs (http://www.spicegirls.com/) tampoco salieron indemnes de esta cruzada ideológica cuando en 1997 fue modificado su site para protestar contra "la cultura pop y el uso masivo de Internet".

Sin ir tan lejos, la Web principal del Ministerio de justicia local fue intervenida por el grupo x-team, colocando una fotografía de José Luis Cabezas el mismo día que se cumplía un año de su cruel asesinato. Debajo, se encontraba un texto donde supuestamente los funcionarios le pedían perdón al pueblo por trabar constantemente el esclarecimiento del caso. La pantalla, con la tristemente famosa mirada de Cabezas, permaneció allí 24 horas hasta que la removieron. Consultados los autores de ese hackeo dijeron que ellos "golpearon las puertas cibernéticas de la justicia".

Los Hackers pretenden que Internet sea un espacio de comunicación libre de toda censura y restricción conspirando contra todo medio contrario a ese pensamiento. Seguramente por eso, el presidente Bill Clinton, el principal mentor de intentar ponerle restricciones a la red mundial, es parodiado constantemente con fotos trucadas que hacen alusión al sexgate desatado tiempo atrás.

Estos personajes suelen ingresar también a un sistema dejando "evidencias" de que ellos estuvieron allí con el objetivo de que los encargados de la seguridad de la empresa sepan que pueden volver y destruir lo que se les plazca en el momento menos pensado. En ocasiones, muchos fueron contratados bajo altísimos sueldos por las empresas que fueron hackeadas para que ellos mismos construyan un sistema más seguro. Tienen mucho poder y lo saben. Por eso son perseguidos constantemente.

El gobierno de los Estados Unidos, en defensa de sus empresarios, ha decidido hace unos años tomar cartas en el asunto personalmente. Se creó una división especial en el FBI llamada National Computer Crime Squad que protege a las computadoras gubernamentales, financieras, de instituciones médicas, etc. Ya existen leyes que penalizan el accionar estos delitos, donde la legislación al respecto es nula. En 1996, el argentino Julio César Ardita penetró ilegalmente a la red del Pentágono de Estados Unidos mediante Internet y provocó el enojo de más de uno en el país del norte. Fue condenado allí a cinco años de prisión en suspenso y debió pagar una multa de 5000 dólares. A pesar de la sanción, Ardita tiene, a modo de homenaje y admiración, cientos de páginas en Internet construidas por personas de diferentes países donde se pueden ver sus fotos y datos personales.

Poseen su propia ética, su propio vocabulario y son por demás ilusorios. Tienen niveles de aprendizaje y detestan a aquellos que se animan a prejuzgarlos. Son solidarios entre sí y, cuando no están sentados frente a sus máquinas, estudian nuevas formas para penetrar en lugares inhóspitos. No son muy sociables y les causa mucho placer sentir que transgreden.

a. Hackers Atacan Sitio de Hillary Clinton

(28.07.99): Como es sabido, la primera dama estadounidense, Hillary Clinton, aspira a convertirse en senadora por Nueva York. Como parte de su campaña, su equipo creó un sitio web (http://www.hillary2000.com), que ya ha sido asaltado por piratas informáticos.

La intervención realizada por los hackers fue relativamente leve, ya que sólo implicó un redireccionamiento del URL, que hizo que quienes intentaran acceder al sitio web de la candidata fuesen llevados a una página web creada por "Los Amigos de Guiliani" –simpatizantes de Rudolph Giuliani– también candidato a una senaduría por Nueva York.

Jerry Irvine, experto consultado por CNN, señaló que lo más probable es que los hackers hayan recurrido a un truco conocido como *DNS poisoning*; es decir un "envenenamiento" del sistema de nombres de dominios (Domain Name Server), haciendo que al escribir una dirección en la web los usuarios sean llevados a una dirección distinta.

Los autores de la página web sobre Giuliani desmienten categóricamente ser los autores del sabotaje de la página de Hillary Clinton.

A la fecha, el problema no ha sido solucionado, por lo que la página de la candidata sólo presenta un mensaje en numerosos idiomas, con el texto "en construcción".

b. Hackers Controlan Satélite Militar Británico

(02.03.99): Satélite militar de comunicaciones está siendo controlado por piratas informáticos. El satélite sería usado para la defensa de Gran Bretaña en caso de un ataque nuclear.

Según el diario inglés Sunday Business, desconocidos alteraron el rumbo del satélite hace dos semanas, luego de lo cual las autoridades responsables recibieron una extorsión según la cual los hackers dejarían en paz el satélite a cambio de una fuerte suma de dinero en efectivo.

Expertos en seguridad y estrategas militares toman en serio la amenaza, recalcando que sería muy natural que enemigos interesados en atacar a Gran Bretaña con armas atómicas primero intentasen dejar fuera de servicio a los sistemas de comunicación.

Una fuente militar consultada por Sunday Business destacó el grave riesgo para la seguridad del país que implica que desconocidos logren apoderarse del control de un satélite. El hecho de que se trate de una extorsión agrava aún más las cosas, señaló.

Por el momento, tanto la policía británica como el Ministerio de Defensa se niegan a comentar los hechos.

c. Hackers Vulneran Sitio de Symantec

(03.08.99): El sitio web de Symantec fue alterado ayer por hackers. La noticia está causando revuelo en círculos informáticos, toda vez que la compañía es uno de los principales proveedores mundiales de software de seguridad y antivirus.

Como parte de su irrupción contra los servidores de Symantec, los hackers cambiaron la portada del sitio web corporativo con un texto único en que su acción es reivindicada como una victoria ("*… we own your ass, Symantec*").

Según BBC News, los piratas informáticos también lograron infiltrar los servidores de Symantec con un programa tipo "gusano", que automáticamente se propaga por sistemas interconectados y que está en condiciones de causar daños similares a los virus.

Consultado por BBC, un portavoz de Symantec confirmó la alteración del sitio web, aunque desmintió que los hackers hubieran logrado instalar un "gusano" en sus sistemas.

El portavoz intentó quitar importancia a la situación, señalando que siempre existe el riesgo de que una compañía se vea afectada por tales ataques y que lo importante es corregir el daño con prontitud y restablecer el sitio web original.

A juicio del portavoz, el prestigio de Symantec no se verá alterado por el ataque, a pesar de ser una compañía líder del rubro de la seguridad informática.

Symantec denunció el hecho al FBI, que inició de inmediato las investigaciones correspondientes.

2.5.10. Daniel Sentinelli

El FBI llegó a mandar a Buenos Aires a uno de sus agentes de su central regional instalada en Montevideo. Uno de los más conocidos hackers argentinos, apodado El Chacal, aceptó revelar su identidad (se llama Daniel Sentinelli) para realizar una demostración pública, en un cybercafé del barrio de Belgrano, de lo fácil que puede resultar a un conocedor en informática llegar a redes supuestamente secretas de gobiernos como el estadounidense. "Estas redes (como la mayoría de las que están en Internet) tienen un sector público (de acceso directo e irrestricto) y uno privado (sólo para usuarios autorizados).

Como ambos deben estar disponibles hay una brecha entre ellos que permite aprovechar los errores propios de los programas que usan". Si este asesor en informática de 30 años que en 1986 estuviera entre los fundadores de Piratas Unidos Argentinos decidió darse a conocer es porque cree que "se ha desatado una paranoia generalizada que puede derivar en una caza de brujas".

Detrás de los hackers, dice, "no hay ninguna clase de criminales. En todo caso respondemos a una curiosidad: la tecnología está ahí, al alcance de la mano y probar qué se puede hacer con ella es irresistible".

"Hay quienes intentan meter miedo, como un periodista argentino que cuando salió a luz el caso del muchacho que entró a la red de la Marina estadounidense clamó poco menos que el mundo está en poder de los hackers y que cualquiera puede ahora entrar a redes ultra secretas y disponer el envío de misiles nucleares." Sentinelli remata: "Internet no es segura porque en ella habitan los hackers. Nada de lo que usamos habitualmente es seguro: los autos, el sistema de gas, el de electricidad tienen fallas, pero no por eso dejamos de usarlos. Tratamos de informarnos de los riesgos de esas fallas. Con Internet se debe hacer lo mismo".

CAPÍTULO III

INVESTIGACIÓN Y ESTUDIO DE UNA RED

3.1. Red privada virtual de banda ancha.

El objeto de análisis para esta tesis es la empresa estatal PETROCOMERCIAL, la misma que es una filial de PETROECUADOR y que regula los procesos de los recursos naturales para su comercialización dentro y fuera del país siendo de gran importancia para el desarrollo del Ecuador.

Esta empresa posee una red provista de tecnología constantemente actualizada que va a la vanguardia de las necesidades, una de las tantas tecnologías aquí empleadas es la del tunneling la misma que se utiliza para la construcción de una VPN. Asimismo; cuenta con un ancho de banda muy amplio (banda ancha) que es el E1 por lo que resulta interesante realizar el estudio en PETROCOMERCIAL.

Debido a los elementos anteriormente mencionados, el estudio del presente tema de tesis se torna ideal ya que se facilita la obtención de información adecuada gracias a la colaboración y predisposición del ingeniero a cargo del área de sistemas en PETROCOMERCIAL, cabe recalcar que esta información constituye un sólido respaldo para el presente documento.

3.2. Condiciones actuales

Como anteriormente ya se ha mencionado, la empresa cuenta con tecnología de punta y con una constante actualización en todo lo concerniente a seguridad puesto que este es un punto de gran consideración dentro de la empresa porque un ataque inesperado causaría cuantiosas pérdidas.

La red se encuentra dotada de infraestructura propia, diferenciándola de una VPN (Red privada virtual) ya que una VPN utiliza infraestructura pública obtenida de un ISP (Proveedor del servicio de Internet).

La infraestructura de PETROCOMERCIAL enlaza sus redes LAN con antenas parabólicas, utiliza la conexión de E1 el mismo que permite 2.048 Mbits de ancho de banda, es decir banda ancha. Esta tecnología permite aplicaciones como el Telnet, DNS, Proxy, FTP entre otros.

3.3. Tecnología empleada

a. Dispositivos

Durante el período de implementación de la red fueron utilizados swiths, routers, y firewalls, estos dispositivos son complementados con el software indicado para la construcción de una red segura.

La información dentro de la empresa es base fundamental del buen desempeño por lo tanto se considera importante el almacenamiento de dicha información para lo cual utilizan cintas magnéticas, la razón para utilizar este tipo de dispositivo de almacenamiento es que es más económico y tiene mayor capacidad; aunque es lento con respecto a otros.

b. Equipos

La red de PETROCOMERCIAL consta de varias máquinas que desempeñan diferentes funciones pudiendo ser servidores o estaciones de trabajo. La red consta de:

4 Servidores Compac 3500

1 Servidor Netfinity 3500

1 Servidor Netfinity 7500

1 Servidor RS/600 para el firewall con sistema operativo AIX.

350 Estaciones de trabajo en Quito

100 Estaciones de trabajo en Guayaquil

150 Estaciones de trabajo en otras partes

c. Métodos

Para detectar la intromisión de personas desconocidas o el funcionamiento anormal de la red, la empresa se sirve de un Analizador de Tráfico que provee el mismo ISP el cual permite visualizar gráficamente los niveles de tráfico, es decir, la cantidad de entidades que quieren ingresar al sistema o que envían información estableciéndose así el porcentaje de personas que utilizan la red, ya sean de la misma empresa o ajenas a la empresa, lo cual es fácil distinguir ya que esta información se despliega en un color para personas de la empresa y otro color para personas particulares a esta, este es método muy útil porque permite al administrador del sistema verificar el tráfico de información y poner al administrador en alerta cuando este se sale de los parámetros normales.

Una aplicación práctica para demostrar la utilidad de este método es la detección del broadcast, el cual llevado a cabo con éxito y malas intenciones

puede colapsar el sistema.

El broadcast consiste en enviar una gran cantidad de información, excesiva, sin sentido y constantemente con el objeto de ocupar gran parte de la memoria del sistema procesando información inservible.

Quizás el más importante de todos los métodos utilizados para la construcción de una red segura es la planificación en base a necesidades que se van presentando pudiendo diseñar y rediseñar un plan de contingencia que ayude a plantear políticas de acceso tanto dentro de la empresa como fuera de esta tomando en cuenta aspectos como firmas digitales, encriptación de la información entre otros.

3.4. Seguridad actual

PETROCOMERCIAL cuenta con un Plan llamado de Contingencia que incluye la seguridad en varios niveles y aspectos los cuales serán descritos a continuación:

- **Seguridad física:**

Ubicación de los equipos en áreas adecuadas, en esta parte se ha tomado en cuenta que el cuarto de equipos cumpla con las reglas y requisitos necesarios para funcionar en condiciones normales, tales como temperatura, espacio físico adecuado, sistemas de protección contra incendios, etc.

Control de acceso de las personas al edificio (seguridad básica). No todas las personas dentro de la empresa tienen el mismo privilegio, sobre todo con algo tan delicado como el site de la empresa. Es entonces donde el acceso de ciertas personas al edificio es permitido y a otras es restringido. Esto es a lo que en la empresa conocen como seguridad básica.

Control de acceso de las personas al departamento de sistemas (seguridad rigurosa). Ahora, la seguridad se vuelve más celosa, puesto que dentro del departamento de sistemas, no todos los empleados tienen acceso al site porque siempre queda la duda de algún empleado infiel o de un empleado ingenuo que pueda de alguna maneta causar daños.

Seguridad Eléctrica abarca todo lo que son UPS y generadores, esto es de mucha utilidad cuando se producen los inesperados cortes de energía eléctrica, de no estar provistos con estos materiales, el inusitado corte de energía podría hacer que la empresa pierda valiosa información.

- **Seguridad lógica**

Backup o respaldos de toda la información y de todos los equipos. (Dentro del departamento de sistemas y fuera de él en el caso de incendio). Los backup o respaldos en la empresa son periódicos, es decir: diarios, semanales, mensuales y anuales. Se puede utilizar cualquier dispositivo de almacenamiento para este fin. El utilizado en la empresa es la cinta magnética, aquí, la información puede ser guardada como una réplica exacta o guardar los cambios realizados sobre la información incluyendo los paquetes de software.

También se utiliza backup para todos los dispositivos y equipos que se encuentren funcionando, es decir que si un servidor deja de funcionar, existe otro que puede reemplazarlo con las mismas características y evitar la paralización del sistema.

Validación de claves y usuarios considerando los diferentes niveles de seguridad que son administradores, programadores, usuarios con privilegios y usuarios finales.

Actualmente, en la empresa se viene tratando abiertamente todo lo que es personal interno que son aquellos que trabajan para PETROCOMERCIAL y separándolos o clasificándolos en empleados comunes y empleados capacitados. Se tiene menos probabilidades de que los empleados comunes puedan causar daños al sistema, sin embargo involuntariamente pueden causar algún tipo de prejuicio. Estos últimos, los empleados capacitados, pueden representar peligro teniendo en cuenta sus principios morales ya que deliberadamente pueden causar daño y perjudicar a la empresa ya sea insertando un programa para descubrir claves, borrar o copiar archivos, poner virus buscando beneficios, inclusive el usuario puede alterar o dañar la información casualmente. La fuga de información de las empresas es de lo más común y se trata de que ciertas personas buscando beneficios personales copia y vende la información a otra empresa. Esto seguramente no podrá salir a la luz pero en las empresas públicas es más común y menos peligroso que en las empresas privadas.

La intromisión de virus también pueden provocar que el sistema se caiga por lo cual el administrador del sistema se ve obligado a acudir a estrategias que prevengan este tipo de anomalías en el sistema. Generalmente, los virus son archivos que erróneamente son descargados en el sistema ya sea debido al intercambio de información o a los documentos que se bajan del Internet.

El sistema de red de PETROCOMERCIAL está provisto de un antivirus llamado SYMANTEK NORTON ANTIVIRUS CORPORATE EDITION el cual es programado para trabajar automáticamente, es decir en tiempo real, el antivirus puede no ser suficiente para evitar la penetración de dichos virus si no es corrido en tiempo real. La obtención de la licencia de Symantek permite una actualización diaria del software antivirus por medio del Internet, esta es una forma precavida de actuar, puesto que nuevos virus son creados diariamente, y son más comunes de lo que se puede imaginar.

Los firewall pueden ser hardware y software. En esta empresa se sirven de ambos métodos así como se puede apreciar en la figura 3.1.

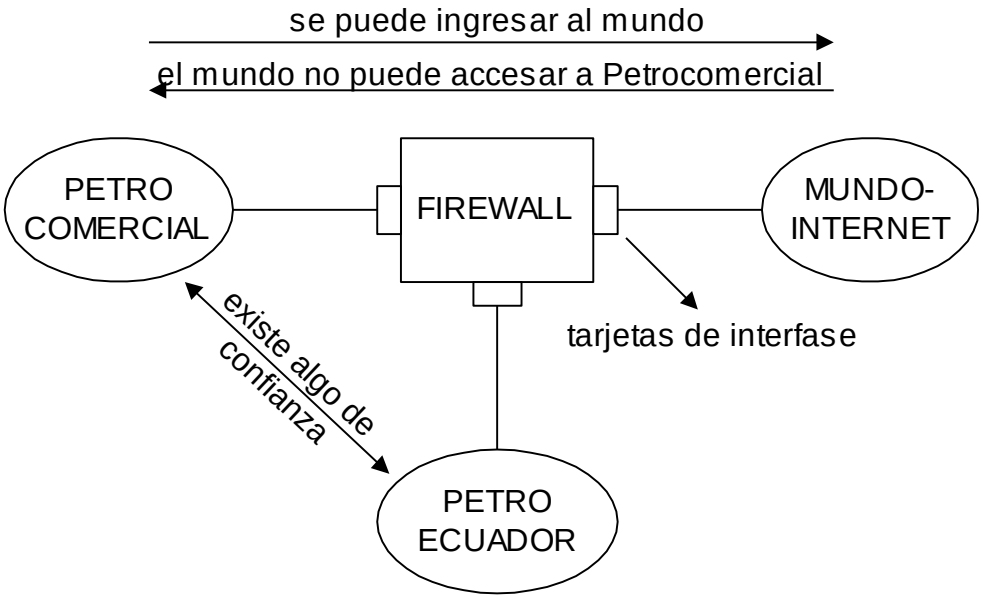


Figura 3.1. Redes Conectadas a un Firewall

La conexión de Internet tiene dos direcciones IP en caso de que en el ISP ocurra algún problema ya que el hecho de que el ISP se caiga no quiere decir que el sistema de la empresa deba caer también.

El sistema operativo del firewall es AIX y el software que utiliza es Secure Way (Similar al Check Point).

3.5. Necesidades

En cuanto a necesidades, se puede decir que esta empresa no sufre de deficiencia de tecnología, todo lo contrario, cuentan con una robusta infraestructura que sustenta las acciones que en el sistema se realizan. Aún así, la red no esta exenta de algún tipo de ataque. Lo que se podría tomar en cuenta como necesidad inmediata es el hecho de tener amplios conocimientos del software del firewall ya que este software (Secure Way) es garantizado pero nuevo en el mercado lo que limita abarcar todos los conocimientos para saber aprovechar y explotar todas sus aplicaciones y ventajas.

Una parte fundamental es la inversión que se hace o se piensa hacer, por lo cual es de gran ayuda un análisis en función del costo / beneficio, lo cual implica, proyectar la inversión a futuro.

Otra de las situaciones que se presenta es la actualización y chequeo constante de la información, este trabajo es realizado por el administrador del sistema, el mismo que rutinariamente debe tomar en cuenta este aspecto sin descuidarlo ni un solo día, no se presenta como necesidad sino más bien como obligación.

3.6. Problemas de la Falta de Seguridad

Se ha tratado anteriormente sobre la solidez que brinda la red de PETROCOMERCIAL, sin embargo no existe una red que sea cien por ciento segura, por lo cual esta empresa no escapó a la intrepidez de personas con conocimientos informáticos que vulneraron el sistema en algunas ocasiones como es la que se comenta a continuación:

En la página Web de PETROCOMERCIAL existen varias opciones que informan a la ciudadanía, entre ellas está la página de comentarios y sugerencias, la cual fue utilizada con malas intenciones por presuntos hackers. Esta intervención provocó la baja del sistema durante quince días en los cuales el sistema funcionaba irregularmente, es decir, funcionaba tres días y el sistema necesitaba un nuevo formateo e instalación de los programas. Lo que causó fallas en el sistema fue que el presunto hacker consiguió que los servidores procesaran basura mediante un broadcast (todo el mundo) valiéndose del mail de la empresa, este proceso saturaba el ancho de banda a pesar de ser muy amplio. En este suceso no se pudo identificar al responsable pero sirvió al administrador del sistema para tomar cartas en el asunto.

CAPÍTULO IV

SEGURIDAD DE LA RED

4.1. Elementos

- Políticas de Seguridad que toma en cuenta los niveles de seguridad brindando privilegios entre los empleados de la empresa y los usuarios externos y ajenos a esta y permitiendo el acceso a personar autorizadas.
- Seguridad Física que contempla la ubicación de los equipos en partes del edificio adecuadas con control de temperatura, sistemas en caso de incendios, etc.
- Seguridad Lógica que ayuda a validar la clave e identificación del usuario e inmediatamente determinar si puede o no ingresar al sistema.
- Firewalls, los cuales pueden ser hardware o software, e impiden el acceso a usuarios no autorizados y facilitan la desencriptación o encriptación de la información para recibirla o transmitirla.

Sobremanera

4.2. Características

- Tecnología moderna, que ayuda de sobremanera ya que los enemigos también están actualizados en todo sentido, y gracias a la tecnología se puede disminuir en grandes porcentajes el riesgo de un ataque con equipos más sofisticados.
- Equipos Garantizados tales como IBM, los equipos de marca pueden costar más pero también garantizan su estabilidad por un buen tiempo.

- Se utiliza un software poco común, que por el mismo hecho de que no es tan conocido, se evita que las personas ya sean particulares o de la misma empresa no tengan la opción de ingresar tan fácilmente a la red por su complejidad de manejo y operación.

4.3. Tecnologías (mejoras)

a. Dispositivos

Actualmente la empresa cuenta con dispositivos actualizados que son de marcas competitivas en el mercado tanto switchs, como routes o firewalls son innovados cada vez que sea necesario y que esos dispositivos se vuelvan obsoletos. Por ser esta empresa de mucha importancia para el desarrollo del país, el estado no escatima en gastos.

b. Equipos

La red que es objeto de estudio consta de varias máquinas que desempeñan diferentes funciones pudiendo ser servidores o estaciones de trabajo. La red consta de:

4 Servidores Compac 3500

1 Servidor Netfinity 3500

1 Servidor Netfinity 7500

1 Servidor RS/600 para el firewall con sistema operativo AIX.

350 Estaciones de trabajo en Quito

100 Estaciones de trabajo en Guayaquil

150 Estaciones de trabajo en otras partes

c. Métodos

Para detectar la intromisión de personas desconocidas o el funcionamiento anormal de la red, la empresa se sirve de un Analizador de Tráfico que provee el mismo ISP el cual permite visualizar gráficamente los niveles de tráfico para revisar el porcentaje de personas que utilizan la red ya sean de la misma empresa o ajenas a la empresa, lo cual es fácil distinguir ya que esta información se despliega en un color para personas de la empresa y otro color para personas particulares.

Otro método del que se valen, es la planificación en base a necesidades que se van presentando pudiendo diseñar y rediseñar un plan de contingencia.

4.4. Alternativas

Al trabajar la empresa en banda ancha, sus direcciones IP son fijas, por lo que puede resultar más fácil el intento de intromisión en el sistema. Actualmente la empresa utiliza infraestructura propia y un enlace dedicado de Internet. Utilizar infraestructura de telecomunicaciones propia representa una inversión inicial altísima, sin embargo las posibilidades de un ataque exitoso disminuyen a diferencia de utilizar un medio público que sería el ISP.

4.5. Ventajas

La principal ventaja de una VPN es que se debe pagar al ISP mensualmente por el servicio de VPN. Lo cual representa un desembolso relativamente pequeño y cómodo para los usuarios de la red.

Se obtiene el mismo resultado que con una infraestructura propia pero a menor costo y menor nivel de dificultad.

La seguridad de la red puede tornarse inquebrantable con un buen plan de contingencia para prever posibles accidentes con la información.

4.6. Desventajas

Al no tener una infraestructura de comunicaciones propia se debería pagar al ISP el ancho de banda utilizado y mientras más ancho es este más alto es el costo.

Al utilizar banda ancha para el enlace de redes, el ISP asigna a la empresa una dirección IP fija que identifica con mayor precisión al sistema, esto se convierte en desventaja porque un atacante puede localizar con mayor facilidad e intentar vulnerar la red mayor número de veces y por un prolongado tiempo hasta conseguirlo, lo que no sucede cuado se tiene un menor ancho de banda, puesto que con este método, el ISP se encarga de asignar aleatoriamente una dirección IP cada vez que el usuario necesita conexión al Internet lo cual dificulta la acción de un hacker.

CAPÍTULO V

ANÁLISIS ECONÓMICO FINANCIERO

5.1. Mejoramiento

La red puede dar un mejor rendimiento en cuanto a seguridad si es mejorada con mantenimiento de hardware y de software. Estar a la vanguardia de hardware implica nuevos conocimientos informáticos de lo contrario no se podría explotar al máximo sus servicios y aplicaciones. De igual manera en el software, con la diferencia de que la actualización de los paquetes es en un periodo más corto de tiempo.

5.2. Optimización

Cuando una red se nos cae debido a un ataque exitoso a la información, deberíamos tener disponible un backup o respaldo hardware pudiendo ser discos duros, o de software que sería un dispositivo de almacenamiento que contenga toda la información actualizada para que la caída de la red no represente mayores inconvenientes, ya que un ataque exitoso representa una inversión de tiempo y dinero muy crítica.

5.3. Inversión de un sistema de protección y seguridad

La inversión se debe ajustar a las necesidades de la empresa, por ejemplo en un centro de cómputo, la necesidad de seguridad no es tan grande como en la empresa que es objeto de estudio de esta tesis.

La confidencialidad de la información representa el 100% del éxito de la empresa, por lo cual es fundamental asegurar la red con la tecnología más avanzada ya que el costo de un equipo frente al costo de los datos que procesa ese equipo es mínimo.

5.4. Beneficio

En realidad el beneficio se ve cuando pasa el tiempo y se tiene la certeza de que la red nunca ha sido víctima de un hacker. Sin embargo no se debe confiar. La seguridad es un tema que genera grandes expectativas lo que nos empuja a estar siempre alerta y actualizando especialmente los paquetes de software. Si bien es cierto la tecnología cada vez da un paso hacia delante pero no se debe olvidar que los hackers también lo hacen. Con esto básicamente obtendríamos:

Protección de la información y los servicios de la red de ataques externos

Mantener la privacidad de la información

Impedir el uso abusivo de servicios

5.5. Justificación de la inversión

Vale la pena recalcar que la inversión en seguridad se torna necesaria para la empresa en cuestión, y que el valor de un equipo se vuelve mínimo con relación al valor que tienen los datos que se procesan especialmente a nivel administrativo.

Establecer una comparación entre una empresa que tiene información de gran importancia y otra que en verdad no necesita proteger sus datos ayuda a esclarecer lo fundamental de la inversión en seguridad, por ejemplo, un cyber café no necesita el mismo nivel de seguridad que una empresa estatal en donde son manejados datos confidenciales que involucra a una población entera y que sus vidas o la economía del todo un país se puede ver afectada por alteraciones en los datos.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Recomendaciones sobre la seguridad

La seguridad encierra varios temas que deben ser coordinados, no solo es un equipo o un software, también influyen en el control de seguridad las políticas que la empresa establezca, así como el control de ingreso al edificio y el control de ingreso a áreas importantes o tener cuidado con instalaciones eléctricas, todos estos puntos son solo una pequeña parte de lo que representa un verdadero sistema de seguridad en el cual debe se debe tener en cuenta el mínimo cuidado para elaborarlo.

6.2. Aspectos básicos

Como se ha relatado a lo largo de estos capítulos, aún con la tecnología más avanzada, los hackers buscan la forma de hacer de las suyas. No se puede hablar de una red totalmente segura. Se debe aclarar que el ancho de banda que utiliza la empresa es amplio (E1), esto asegura que la información viaje casi en tiempos reales entre las LANs remotas, pero no asegura que no puede ser hackeada.

El inconveniente de la banda ancha es que el ISP asigna a la empresa una dirección IP fija, lo cual permite a un hacker localizar con facilidad nuestra red las veces que él quiera y por lo tanto el hacker puede insistir en atacar a la red innumerables veces hasta que logre vulnerarla (si es perseverante), lo que no sucede cuando se tiene menor ancho de banda, puesto que el ISP asigna a la empresa una dirección IP aleatoria cada vez que se realiza una conexión al Internet y de esta manera dificultando la localización de la red a un hacker.

6.3. Mejoras específicas

Lo que aparece como necesidad es tener un dominio de software que se utiliza y poder aprovecharlo al máximo. Por ejemplo, el hecho de habilitar o deshabilitar una casilla del software del firewall que beneficios proporcionan, o lejos de dar beneficios, se está dando paso a que la red se vuelva más vulnerable.

Bloquear el acceso en determinadas estaciones de trabajo todo aquello que sea medios para almacenar información pudiendo ser el drive o CdWriter para evitar que la información que se considera confidencial se fugue de la empresa; llevar a cabo un control de acceso al Internet para evitar que paquetes de dudosa procedencia sean descargados en la red puesto que nadie nos asegura que ese software no tenga virus o que con esto estemos permitiendo que alguien más accese a la red. Poner algún tipo de filtro que impida el paso de determinados mails dañinos y tener siempre actualizado el antivirus son algunas recomendaciones que se toman muy en cuenta al momento de trabajar sobre la red.

6.4. Análisis costo / inversión

La inversión que se piense hacer en cualquier tipo de negocio debería tener en cuenta lo siguiente: ¿Cuento con el capital para asegurar mi red? ¿Hasta que punto se hace imprescindible que yo invierta en seguridad?

Obviamente, en este caso, la seguridad es un aspecto valioso ya que los datos que se encuentran almacenados en la red influyen en la estabilidad económica del país y por tanto se necesita seguridad a un nivel alto sin importar cuanto de dinero esto pueda representar.

a. Costo del hardware

Las máquinas que utilizan actualmente tienen magnificas características. El precio estimado de un sistema de seguridad en cuanto lo relacionado con equipos firewalls esta desde los 1200 dólares. Pero esto es solo una parte de seguridad.

b. Costo del software

El software también representa un egreso ya que aparte del servicio del software también necesitamos licencias. Un programa para configurar un firewall es el Check Point que es el software que tiene Andinanet en la ciudad de Quito es de 18.000 dólares y la obtención de la licencia de 4.000 dólares.

Pero un simple paquete de filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya esta incluido como estándar del equipo. Un sistema comercial de firewall provee un incremento más a la seguridad pero su costo puede ser de dependiendo de la complejidad y el número de sistemas protegidos. Estos precios son a nivel de usuarios, de lo contrario no sería accesibles para público.

6.5. Recomendaciones

- **Generales**

Durante el desarrollo de la presente tesis se puede constatar que los ataques a empresas son más comunes de lo que parece por lo cual resulta imprescindible estructurar un plan de seguridad tomando en cuenta de lo valiosa que es la información, considerando que no solo los extraños o particulares a la empresa pueden provocar daños, sino también los de propios de la empresa.

Para realizar este proyecto, la empresa PETROCOMERCIAL brindó las facilidades para obtener la información que respalda a este documento. Hay que tomar en cuenta que estos datos son expuestos de una forma muy generalizada y con total reserva, lo cual es totalmente comprensible.

Existe una diferencia marcada con respecto a lo que es una institución pública y una privada en cuanto a lo que es seguridad. Las instituciones privadas son más celosas en compartir información; la causa de esto es que las empresas privadas se encuentran en el mercado con la competencia y no quieren por ninguna razón que de alguna manera se divulguen los procesos internos.

- **Específicas**

La seguridad no gira alrededor del firewall en una red privada virtual, sino que es un conjunto de acciones y decisiones que complementan la acción de un buen plan de seguridad.

Los virus también son una amenaza para la información del sistema, por lo que hay que darles igual atención que a otras amenazas, para lo cual un antivirus se torna de mucha ayuda, hay que tomar en cuenta que este debe ser constantemente actualizado y ser corrido en tiempo real, porque de lo contrario sería obsoleto.

Los ataques a la información pueden realizarse por empleados internos o por atacantes externos, en cualquiera de estos dos casos se debe estar alerta cuando intercepten el tráfico de red, ya que pueden ingresar al sistema con diferentes intenciones, puede ser fraude, extorsión, robo de información, venganza, o el simple desafío de entrar a un sistema.

Los administradores del sistema tienen una gran responsabilidad, por lo que se deben encargar de verificar la seguridad en la red en forma diaria, y comprobar si algún empleado o usuario esta recurriendo a vías de acceso no autorizadas o si alguien insiste en ingresar al sistema en varias ocasiones con claves erróneas. Todos estos movimientos deben ser registrados por el operador o administrador del sistema.

Los hackers y telepiratas están provistos de muchas herramientas que inteligentemente utilizadas pueden causar serios daños al sistema; por este motivo se debe considerar que el valor de la información que se procesa es mucho más valiosa que un equipo o software que ayudará a obtener un poco más segura la red por lo tanto comprar software o hardware para proteger la red es una inversión y no un gasto.

La intromisión de un extraño con cualquier propósito que este ingresara o atacara al sistema se puede dar inusitadamente por lo que se debe permanecer alerta a cualquier variación y tráfico irregular o sospechoso.

ANEXOS

ANEXO B: Documentos Obtenidos del Internet

Anexo B1: Datos estadísticos de la concurrencia de hackers en diferentes países.

Port	AR	BO	BR	CK	CL	CO	CR	CV	EC	GT	HN	MX	NI	PA	PE	PY	SV	UY	VE	Total	Port
80	1446	324	4530	4	440	186	165	6	192	108	190	2453	3	95	540	11	42	74	653	**11462**	80
111	130	52	674		751	10	3		16			152			12					**1800**	111
4665	167		607			35	59					185		3					30	**1086**	4665
37												964								**964**	37
21	27		127		661							83								**898**	21
28800	178		465		30							106		1						**780**	28800
515			299		9							202								**510**	515
8080	1		342									2			5					**350**	8080
53	14		15		85	48	2					9		106	4					**283**	53
27374	205		9									33						2		**249**	27374
	2168	**376**	**7068**	**4**	**1976**	**279**	**229**	**6**	**208**	**108**	**190**	**4189**	**3**	**205**	**561**	**11**	**42**	**76**	**683**	**18382**	
	11%	**2%**	**38%**	**0%**	**10%**	**1%**	**1%**	**0%**	**1%**	**0%**	**1%**	**22%**	**0%**	**1%**	**3%**	**0%**	**0%**	**0%**	**3%**	**100%**	
Port	AR	BO	BR	CK	CL	CO	CR	CV	EC	GT	HN	MX	NI	PA	PE	PY	SV	UY	VE	Total	Port

Anexo B2: Lista de los firewall con certificación para aplicaciones empresariales en seguridad a feb 2002

Certified Product Names	Vendor Names
3Com Firewall Family	3Com Corporation
Access Point Family	Lucent Technologies
Avaya VPN Gateways	Avaya, Inc.
Basilisk F100	SecureWorx South Africa Ltd
BiMON Firewall	Linux Security
BorderWare Firewall Server	BorderWare Technologies
Check Point 2000 NT	Check Point Software
Check Point 2000 Solaris	Check Point Software
Cisco PIX Firewall Family	Cisco Systems, Inc.
CyberwallPLUS-IP	Network-1 Security Solutions, Inc.
eTrust Firewall for Windows 2000	Computer Associates International
eTrust Firewall for Windows NT	Computer Associates International
Firebox II LiveSecurity	Watchguard Technologies, Inc.
FoxBox	NetWolves Technologies
Gauntlet Firewall for Solaris	Network Associates, Inc. (NAI)
GNAT Box GB-100	Global Technology Associates, Inc.
iGateway Family	Intoto, Inc.
IM Firewall	Elron Software

Instagate EX Firewall Policy Manager	eSoft
Internet Security and Acceleration Server 2000	Microsoft Corporation
isec Gateway Family	SIGn Co., Ltd.
Lucent VPN Firewall	Lucent Technologies
Microsecure Firewall	Microsecure
N-Patrol Firewall	HackersLab Co., Ltd.
Nemesis Firewall Family	Allied Telesyn International
NETASQ F100-3	NETASQ
NetScreen Family	NetScreen Technologies
Netshelter	PFU Limited
NetStructure VPN Gateway	Intel
Nokia IP Series Routers	Nokia
Raptor Firewall for NT	Symantec Corporation
Raptor Firewall for Solaris	Symantec Corporation
secuiWALL	SECUi.COM
SecureIT	SLMsoft
SecuwayGate 1000	Future Systems, Inc.
ServGate SG200	ServGate Technologies, Inc.
ServGate SG300	ServGate Technologies, Inc.
Shasta 5000 Broadband Service Node (BSN)	Nortel Networks
Sidewinder	Secure Computing
SonicWALL Family	SonicWALL, Inc.
Springtide IP Service Switch	Lucent Technologies
StoneGate	Stonesoft Corporation
UniRo-Secure	UniSoft Co., Ltd.
WebGuard Firewall Solaris	GenNet

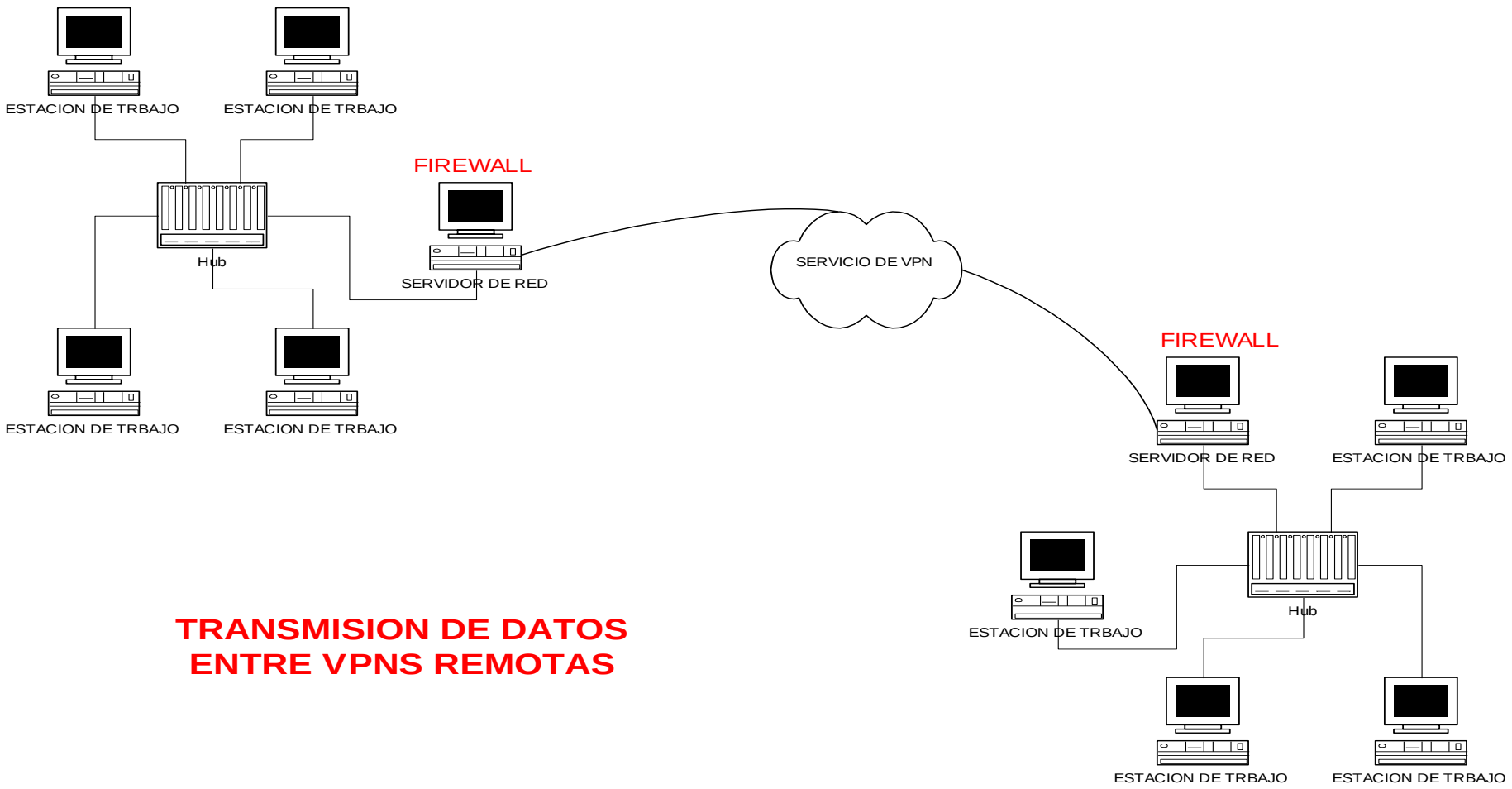
Anexo B3: Programas Utilizados para Hackear

PROGRAMA	DESCRIPCIÓN	S.O.
Cracker Jack 1.4	Descodificador de Passwords de Unix. Inglés.	Dos
Brute Forece 1.1	Descodificador de passwords Unix. Inglés.	Dos
John the Ripper 1.4	Posiblemente el mejor descodificador de password Unix.	Dos
Star Cracker 1.0	Otro descodificador de pass. Unix. Ing.	Dos
Hack486	Más descodificadores de pass. Éste incluye un fichero de password para probar. Muy rápido. Ing.	Dos
[Xit]v2.0	Más descodificadores..... Ing.	Dos
Crack v5.0	Otro descodificador pero de passwords ffb X. Ing.	Unix
Magic Cracker	Otro descodificador de passwords Unix. Ing.	Win95/NT
Jill20	Complemento para el Cracker Jack.Ing.	Dos
Unix Password analizer	Busca personas bastante importantes en un fichero password de Unix. Ing.	Dos
VMS crack 1.0	Descodificador password de sistemas VMS.	-
Crack CNX	Descodifica ficheros cnx del software de infovía para Win3.x. Ing.	Dos
Glide	Dicen que descodifica los passwords .PWL de W95. No es compatible con la versión OSR2. Ing.	Dos
PWL Viewer	Visualizador de los ficheros .PWL. Ing.	Dos/W95
PWL Tools	Como el anterior pero todo el kit, crackeador, y visualizador. La velocidad del cuál está limitada por el mal uso que se pueda hacer. Ing.	Dos/W95

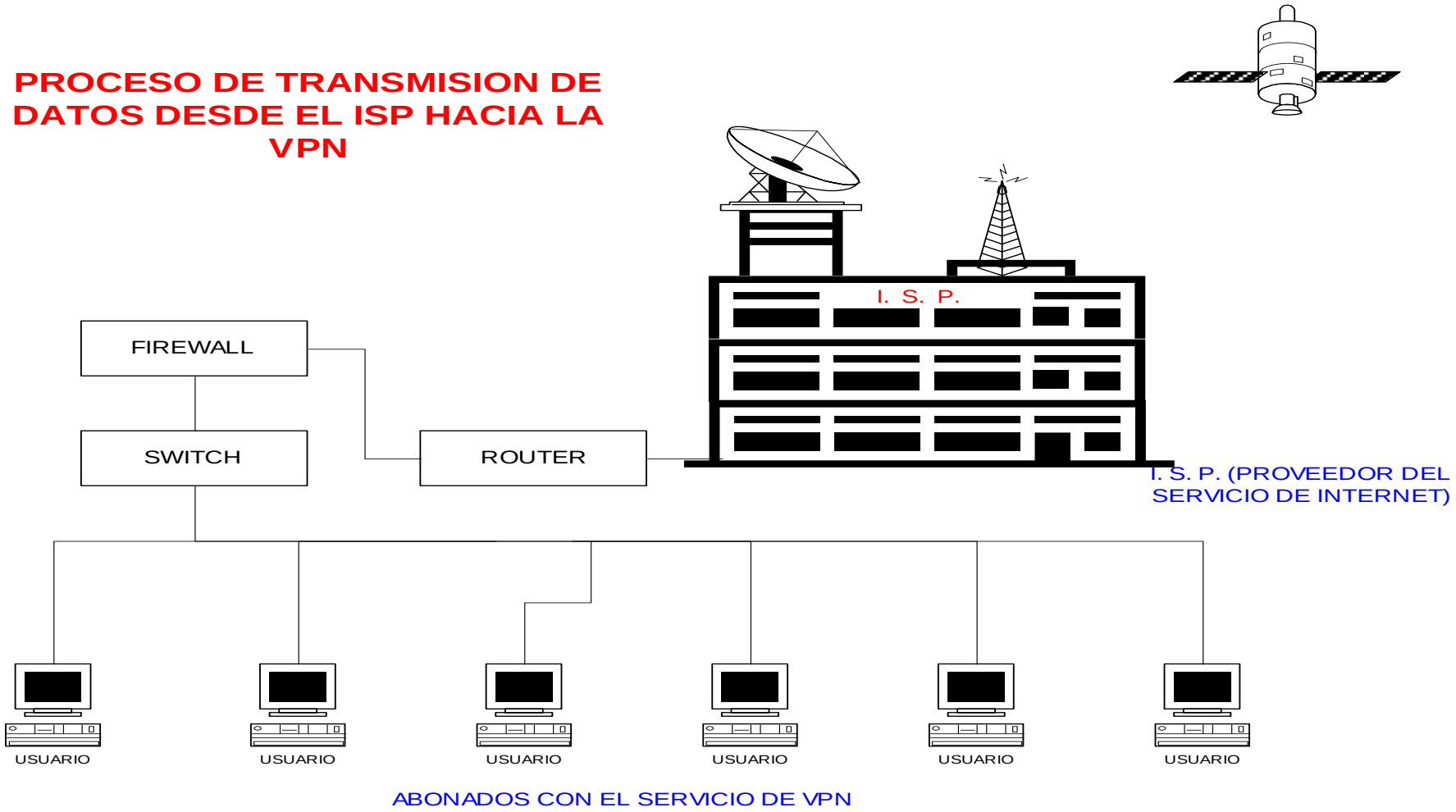
PopCrack v1.0	Cracker del Popmail Password. Ing.	Dos
Toneloc 1.10	Uno de los mejores War-Dialers de todos. Ing.	Dos
Phonetag v1.3	Otro escaneador de teléfonos. Ing.	Windows
THC scan v1.0	El mejor de todos. Sin ninguna duda. Pese a que es un poco difícil de configurar. Ing.	Dos
Keylog 95	Capturador de teclado. En el archivo figuran todas las teclas pulsadas. Ing.	Dos/Win 95
Keylog v2.0 95/NT	Como el anterior pero mejorado. Ing.	Win95/NT
Passgrab 1.0	Otro capturador de teclado.	-
Password Thief v1.0	Un buen capturador de teclado. Sharewar.	W95
Passbios	Este programa engaña al usuario para pillar la clave de la Bios. Se simula la Bios del ordenador para engañar. Esp.	W95
L0phtCrack 2.01	Pillar passwords en NT. Ing.	W95/NT
PortScan	Escanea los puertos abiertos de un ordenador remoto. Ing.	Dos
Winsock spy v0.91	Substituye el fichero wsock32.dll para espiar las comunicaciones de u PC. W95. Ing.	-
Satan v1.1.1	Herramienta muy útil para detectar posibles agujeros de seguridad. Ing.	UNIX
Netcat v1.1.0	Herramienta que escribe y lee datos de conexiones TCP/IP. w95/NT. Ing.Versión Unix	W95/UNIX
Netpack v2.0	Conjunto de utilidades. Ing.	W95/NT
Hacker's Utility	Muchas utilidades y descodificadores de pass. Ing. o Ital.	Win95/NT
Date Dictionary	Generador de listas, o diccionarios para los crackeadores de passwords. Ing.	Dos

Creator		
Wordlist Maker	Creador de listas de palabras de Ing.	Win3.x.
Diccionario	Un diccionario grande para utilizarlo para los crackeadores de passwords. .	Dos
Super Diccionario	Uno de los diccionarios más grandes. !!!!3'8Mb.¡¡¡	-
Manipulador de Passwords	Descodifica y modifica el fichero /etc/passwd. Esp.	Dos
NETLAB95	Conjunto de utilidades para chequear Redes, funciones finger, ping, etc...	W95

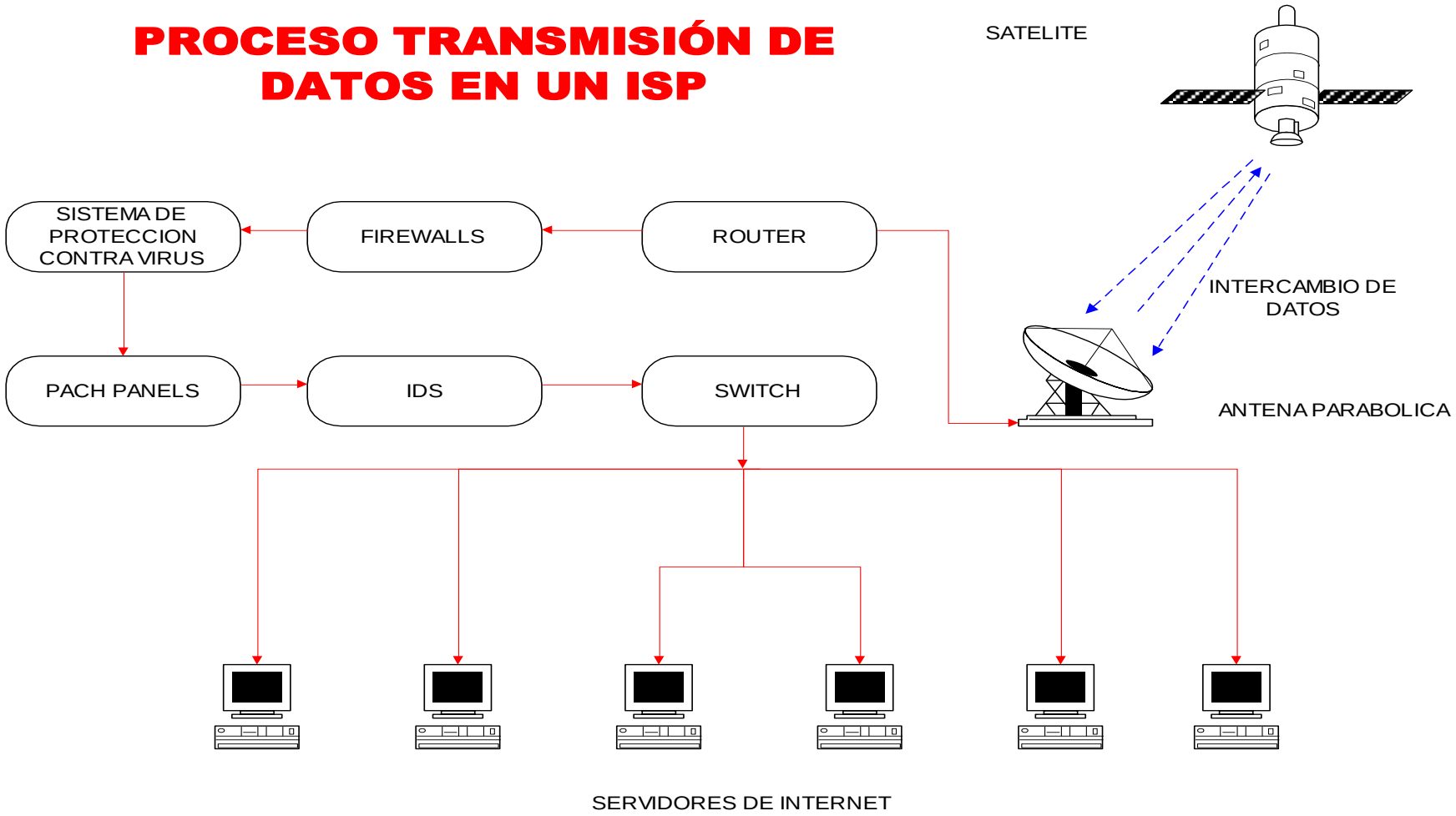
PLANOS



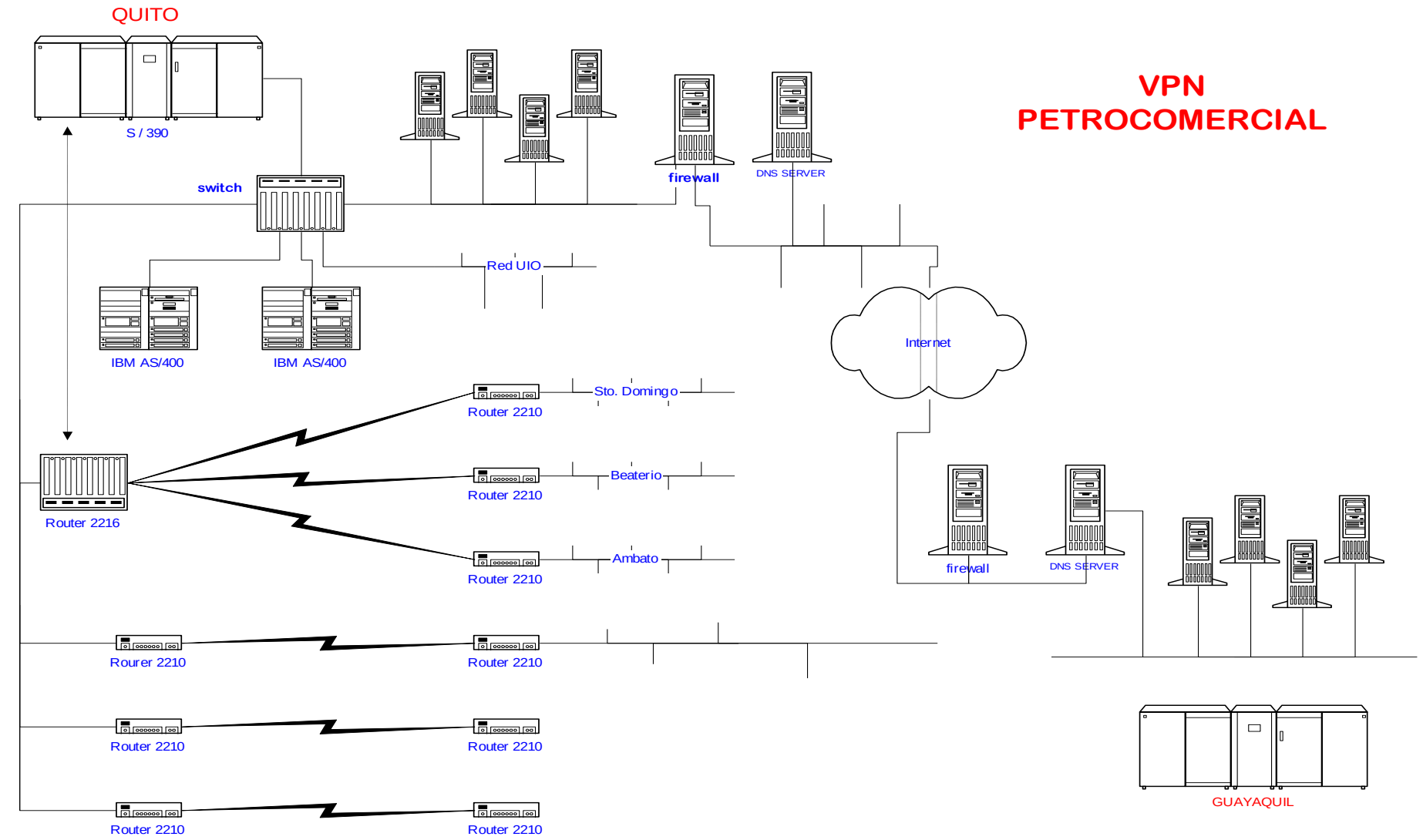
PLANO 1: Transmisión de datos entre VPNs remotas



PLANO 2: Proceso de transmisión de datos desde el ISP hacia la VPN



PLANO 3: Proceso de transmisión de datos en un ISP



PLANO 4: VPN PETROCOMERCIAL

GLOSARIO

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático.

ADSL: (Asymetric Digital Suscriber Line). Línea digital de abonado asimétrica; tecnología que permite la transmisión de señales analógicas y digitales en sentido descendente (hacia el abonado) a velocidades de 1.5 a 8 Mbits/s y ascendentes (hacia la central) de 16 a 140 Kbits/s, utilizando par de cobre trenzado.

ATM: (Asynchronous Transfer Mode). El modo de Transferencia definido para la RSDI de Banda Ancha, en el que la información se organiza en celdas de tamaño fijo (53 octetos). Es modo de transferencia específica orientado a paquetes que utiliza un multiplexado por división en el tiempo síncrono.

Backdoor: Puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal

Bajar o Download: Extraer un programa de un BBS vía módem.

BBS: (Bulletin Board System). Tablón de anuncios electrónico que proporciona entre otros, servicio de mensajería y transferencia de ficheros a través de la red telefónica.

Black Box: Aparato que engaña a la central telefónica haciéndole creer que no se levantó el teléfono cuando en realidad se está produciendo una comunicación.

Blue Box: Aparato (o programa de computadora) que emite tonos multifrecuencias que permite controlar las centrales telefónicas. Se utiliza para lograr comunicaciones gratuitas, entre otras cosas.

Boxes: Circuitos preparados para realizar phreaking. Destacan:

- Bluebox => Para llamar gratis
- Redbox => Emula la introducción de monedas en teléfonos

públicos

- Blackbox => El que llame a un teléfono con este dispositivo no pagará la llamada.

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

Bustear: Precinto o incubación de un BBS por parte de la policía.

Calling Card: Tarjeta de crédito emitida por una compañía telefónica que permite hacer llamadas y pagarlas después.

Carding: Uso de tarjetas de crédito de otras personas, generación de nuevas tarjetas de crédito para realizar pagos a sistemas de compra a distancia (principalmente). En general, cualquier actividad fraudulenta que tenga que ver con las tarjetas de crédito.

Cortafuegos (Firewall): Computadora que registra todos los paquetes de información que entran en una compañía para, una vez verificados, derivarlos a otra que tiene conexión interna y no recibe archivos que no provengan de aquella. Es como un embudo que mira si la información que desea entrar a un servidor tiene permiso para ello o no. Los hackers deben contar con gran creatividad para entrar ya sea buscando un bug (error de diseño) o mediante algún programa que le permita encontrar alguna clave válida.

Crack: Desprotección de un juego o programa.

Cracking: Modificar un programa para obtener beneficios. Normalmente se basa en quitar pantallas introductorias, protecciones o, como en unas modificaciones de cierto programa de comunicaciones, conseguir nuevos passwords de acceso a sistemas...

Cyberpunk: Corriente literaria dentro de la ciencia-ficción que, entre otras cosas,

se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

Datagrama: En las redes de conmutación de paquetes es una forma de encaminamiento, en la cual un paquete se dirige hacia su destino final, independientemente del resto, por los tramos de menor carga y retardo sin que previamente se haya establecido un circuito virtual o real.

Dial-up: Línea de datos que permite a un usuario acceder por módem a una red o a una computadora.

DIRECCIÓN IP. Un identificador universal representado por cuatro números con un valor entre 0 y 255 separados por un punto, que permite que cada elemento conectado a Internet sea reconocido de forma única.

DNS: (Domain Name System). Un servidor de sistema de nombres de dominio en internet es un ordenador que recibe como entrada un nombre de dominio y devuelve la dirección IP correspondiente. Convierten nombres fáciles de entender a direcciones IP, más complejas.

> **E1/T1:** Circuitos digitales alquilados de alta velocidad. E1 a 2.048 Mbits/s y T1 a 1.544 Mbits/s. E3 (34.368 Mbbits/s) y T3 (44.736 Mbits/s), son las versiones a mayor velocidad.

ENRUTADOR DE BANDA ANCHA: Cuando se está conectado a un módem ADSL o de cable externo, el enrutador de compartición de banda ancha permite a los usuarios compartir ancho de banda para acceso a Internet a través de una única dirección IP.

FIREWALL: cortafuegos. Programa, o combinación de software y hardware, que protegen y ocultan los recursos internos de la red de cara al exterior en la conexiones de Internet.

Frame Relay: (Retransmisión de Tramas) Técnicas de multiplexación y

conmutación de tramas en una red de área extensa, que proporciona gran velocidad y retardo mínimo. El estándar que es una simplificación del X.25 operando a nivel 2 del OSI, contempla los protocolos y el interfase.

FTP: (File Transfer Protocol). El protocolo de transferencia de ficheros permite a un usuario de un sistema acceder y transferir información a y desde otro sistema a través de una red de comunicaciones.

Gateway: (Pasarela). Dispositivo que permite enlazar dos redes con estructura física o protocolos diferentes, actuando como adaptador y traductor de la información.

Guest: Cuenta pública de un sistema, para que la use alguien que no tiene cuenta propia.

Gusano: Programa que se reproduce, sin infectar a otros en el intento.

Hacking: Acto de hackear. Básicamente consiste en entrar de forma ilegal en un sistema, para obtener información. No conlleva la destrucción de datos ni la instalación de virus, pero pueden instalarse troyanos que proporcionen passwords nuevos. También consiste en llevar una vida acorde con el hackmode.

Hackmode: Modo de actuar del hacker. No tiene por qué estar relacionado con las computadoras, es más bien un modo de interpretar la vida. Consiste en:

- No pagar lo que no es estrictamente necesario o pagar de forma "poco corriente".
- Ser un poco "paranoico".
- Actuar acorde con costumbres rigurosamente calculadas.

Ingeniería social: Arte de convencer a la gente de entregar información que no corresponde.

IP: (Internet Protocol). Protocolo de nivel 3 que contiene información de dirección

y control para el encaminamiento de los paquetes a través de la red. Suele asociarse a TCP.

IPX: (Internetwork Packet Exchange). Protocolo a nivel 3 de Novell, similar a XNS en IP.

ISDN: (Integrated Services Digital Network). Red digital de servicios integrados, que define una red conmutada de canales digitales que proporciona una serie de servicios integrados, siguiendo las recomendaciones Serie I del CCITT. El enlace básico consta de 2 canales B de 64 Kbit/s y uno D de 16 Kbit/s mientras que el primario consta de 30 canales B de 64 Kbit/s y uno D de 16 o 64 Kbit/s.

Lamer: Tonto, persona con pocos conocimientos. Principiante

Login: Procedimiento de identificarse frente a un sistema para luego usarlo. Este identificativo más el password o clave te permite acceder a información restringida.

Loops: Circuitos. Un loop (o bucle) de teléfonos son dos teléfonos que se comunican entre sí.

Módem: Dispositivo que transporta una señal digital en analógica y viceversa de tal forma que las primeras puedan ser transmitidas de una línea telefónica.

Operador: Persona que usa una computadora. A menudo se llama 'operador' al administrador del sistema.

Outdial: Modem de salida dentro de una misma red, que permite a un usuario de la misma salir a la red telefónica convencional. Los que permiten hacer llamadas a larga distancia se llaman 'global Outdial' (Outdial globales) o GOD.

Packet switching: Conmutación de paquetes.

Payload: Efecto visible de un software maligno.

Password: Clave. Palabra que sirve para verificar que un usuario es realmente

quien dice ser. Por eso mismo, el único que debe conocerla es ese mismo usuario.

Patch o Parche: Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

PBX: Private Branch Exchange. Centrales telefónicas internas de empresas.

PCMCIA: (Personal Computer Memory Card International Association). Tarjeta normalizada de tamaño reducido para dotar a los ordenadores portátiles de diversas funciones, tal como acceso a redes locales, capacidad de almacenamiento o comunicación.

Phreaking: Acto de llamar por teléfono gratuitamente y la realización de modificaciones a los aparatos telefónicos con el fin de obtener algún tipo de beneficio.

PPP: (Point to Point Protocol). Protocolo tipo IP, que sirve para la conexión encaminador- encaminador y ordenador-red, sobre circuitos asíncronos y síncronos.

Proxy: Elemento intermedio entre una LAN y una WAN (Internet) que realiza funciones de separación entre ambas y filtrado de paquetes, permitiendo el almacenamiento de páginas ya visitadas (caché) para ganar en velocidad de acceso. Puede ser un servidor proxy específico o un software en le PC del usuario.

RDSI: Véase ISDN.

Subir o Upload: Enviar un programa a un BBS vía módem.

TCP/IP: (Transmission Control Protocol / Internet Protocol). Serie de protocolos estándar de comunicaciones a nivel 3 y 4 del OSI, desarrollado por el departamento de defensa de EE.UU. para la interconexión de redes

multivendedor. TCP es un protocolo a nivel de transporte, orientado a conexión, e IP es un protocolo a nivel de red, no orientado a conexión.

Telnet: Programa para Internet basado en texto, usado para enlazarse a una máquina remota. Una vez conectada, la máquina se comporta como si el usuario estuviera realmente sentado frente a la otra, aun cuando se hallen en diferentes partes del mundo.

Tracear: Seguimiento exhaustivo. Se utiliza cuando se intenta desproteger un programa y se tiene instalado un Debugger. Este término también es utilizado en caso de que la línea telefónica esté pinchada por la policía.

UDP: (User Datagram Protocol). Protocolo orientado a la transmisión de datagramas en una red que utiliza el protocolo IP. No se garantiza el grado de servicios y los paquetes pueden llegar en un orden distinto al que han sido emitidos, ya que cada uno puede seguir un camino distinto dentro de la red. Es un protocolo no orientado a la conexión.

XNS: (Xerox Network System). Un protocolo de igual a igual, desarrollado por Xerox, que ha sido incorporado a varios esquemas de LAN. Ampliamente empleado, está siendo reemplazado por TCP/IP.

BIBLIOGRAFÍA

- http://www.cisco.com/global/ES/solutions/sp/techsols/vpn/vpn_home.shtml
- http://www.nortelnetworks.com/corporate/news/newsreleases/2001b/04_24_01 01310_carrier1_cas.html
- http://www.intel.com/es/pressroom/archive/releases/Int11000.htm
- http://216.239.37.100/search?q=cache:prIfqUSUo4IC:www.genuity-europe.com/sitemod/design/layouts/default/index.asp%3Fpid%3D2110+que+es+una+vpn&hl=es&lr=lang_es&ie=UTF-8
- http://www.lidernet.com.ar/extranet/
- http://216.239.37.100/search?q=cache:TnblFtLMIF8C:www.uv.es/ciuv/cas/vpn/+que+es+una+vpn&hl=es&lr=lang_es&ie=UTF-8
- IBM Secure Way, Firewall for Windows NT**,** User's Guide, Version 4

INFORMACIÓN DE BANDA ANCHA

- http://www.comunicaciones.unitronics.es/tecnologia/atm.htm
- http://www.reforma.com/tecnologia/articulo/232545/
- http://216.239.33.100/search?q=cache:r-jlhuDuoGIC:www.terra.co.cr/noticias/articulo/html/act108441.htm+transmision+en+banda+ancha&hl=es&start=19&lr=lang_es&ie=UTF-8
- http://216.239.33.100/search?q=cache:RN3DXs5M7FAC:es.gsmbox.com/news/mobile_news/all/10679.gsmbox+transmision+en+banda+ancha&hl=es&start=14&lr=lang_es&ie=UTF-8
- http://www.benq.es/ServiceAndSupport/FAQ/faq.cfm?productline=11&question=133#133 (preguntas de banda ancha)
- http://216.239.33.100/search?q=cache:m4DARe-qg7wC:www.diveo.net.ar/html/pr1023.html+transmision+en+banda+ancha&hl=

es&start=20&lr=lang_es&ie=UTF-8

- Hidrovo, José Manuel. Redes y Servicios de Telecomunicaciones. Tercera Edición, Paraninfo Thomson Learning.
- Monteros, Julian; López, Oscar; García, Santiago (2002). Técnico en Telecomunicaciones. Tercera Edición, Cultural S.A. Madrid-España.

INFORMACIÓN SOBRE FIREWALLS

- http://seguridad.internautas.org/firewall.php
- http://www.mindsoftweb.com/software/firewall.htm
- http://www.creangel.com/categories.php?op=newindex&catid=8
- http://www.monografias.com/trabajos3/firewalls/firewalls.shtml
- http://pronad.uson.mx/eventos/cozumel/seguridad/
- http://www.advance.com.ar/usuarios/fralunito/notas/internet,%20intranet,%20extranet.htm
- IBM Secure Way, Firewall for Windows NT, User's Guide, Version 4

INFORMACIÓN SOBRE HACKERS

- http://cultdeadcow.com
- http://diarioit.comftp://ftp.cdrom.comftp://ftp.coast.nethttp://hertz.njit.edu/%7ebxg3442/temp.html
- http://www.alpworld.com/infinity/void-neo.html
- http://www.danworld.com/nettools.html
- http://www.eskimo.com/~nwps/index.html
- http://www.geocities.com/siliconvalley/park/2613/links.html
- http://www.ilf.net/Toast/

- http://www.islandnet.com/~cliffmcc
- http://www.simtel.net/simtel.net
- http://www.supernet.net/cwsapps/cwsa.html
- http://www.trytel.com/hack/
- http://www.tucows.com
- http://www.windows95.com/apps/
- http://www2.southwind.net/%7emiker/hack.html