UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

MECANISMOS DE CONTROL DE ACCESO

A INTERNET UTILIZANDO FIREWALL Y PROXY

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

HUGO ENRIQUE VIZCARRA VALENCIA

PROMOCIÓN
1992 – I

LIMA – PERÚ
2006

MECANISMOS DE CONTROL DE ACCESO A INTERNET UTILIZANDO FIREWALL Y PROXY

Dedico este trabajo a:
Mi esposa por su constante apoyo y a mis hijos que son la motivación de mi vida.

SUMARIO

La seguridad frente a Internet es uno de los principales retos de la actualidad y este informe proporciona mecanismos que permiten optimizar el uso de los recursos de la red estableciendo políticas de seguridad. En el presente trabajo se describe los principales mecanismos utilizados para reducir el flujo de información indeseada entre una Lan e Internet a través de Firewalls y Proxy.

Se presenta la evolución histórica de la Internet, los fundamentos básicos de las redes TCP/IP, se analizan las fuentes indeseadas de información, se describen los mecanismos de control y políticas de seguridad, para finalmente describir una aplicación real de control de acceso a Internet utilizando Firewall y Proxy.

ÍNDICE

PRÓLOGO

El presente informe ha sido elaborado con el objetivo de brindar las herramientas necesarias para analizar y resolver problemas se seguridad en el acceso a Internet desde una red Lan.

Conciente de la relevancia de este problema en nuestra sociedad, es que este informe titulado ***Mecanismos de Control de Acceso a Internet Utilizando Firewall y Proxy***, hace un desarrollo de los tópicos necesarios para abordar esta problemática, así mismo cabe destacar que el contenido de este informe es adecuado para todos aquellos que deseen analizar el problema de seguridad en una empresa, definir con claridad sus necesidades y establecer políticas de seguridad para así, tener un acceso a Internet seguro y confiable.

En el capitulo I se ofrece una descripción general de los orígenes y funcionamiento de Internet, en el se encuentra una reseña histórica de su evolución.

En el capítulo II se describe su funcionamiento de las redes utilizando los protocolos TCP/IP.

En el capitulo III se analizan las fuentes de información indeseadas durante una conexión a Internet, se describe y clasificas a los virus, se analiza la problemática del spam, así como una descripción de los tipos habituales de ataque.

En el capitulo IV se describen los mecanismos de control que permitirían una conexión segura.

En el capitulo V de analiza un mecanismo de control a través de Firewall y Proxy.

Confió en que este informe, reflejo de la investigación y experiencia del autor, sea una ayuda para aquellas personas que requieran establecer niveles de seguridad en una conexión a Internet.

CAPÍTULO I
FUNDAMENTOS DE LAS REDES TCP/IP

1.1. Introducción

Internet se ha convertido en la entidad virtual más variada y utilizada que ha desarrollado el hombre. El numero de usuarios crece año a año en cientos de miles por todo el mundo, sin que esto parezca que vaya a dejar de aumentar. Internet es el lugar virtual donde todo el mundo es bienvenido para hacer negocios, comunicarse, buscar información o, simplemente, divertirse navegando sobre la red. La inmensidad de Internet, junto con las diferencias entre sus visitantes, crea una mezcla única. Sin embargo, la Internet también contiene un gran potencial para el uso indebido, el abuso y la actividad criminal. Esta capacidad para causar daños ha creado la necesidad de que existan prácticas de seguridad y dispositivos para proteger los recursos de Internet. En 1995 el CERT (Computer Emergency Response Team) recibió un total de 2 412 incidentes relacionados con computadoras y más de 12 000 sitios se vieron afectados. Esto hace que se continúe con el debate sobre la seguridad en Internet. Muchas empresas consideran que Internet no es segura para realizar negocios, otras consideran que Internet ofrece muchas posibilidades para disuadir a los posibles atacantes mediante elementos de seguridad, como un servidor Proxy o los Firewalls. Hoy en día debido al impresionante aumento de los host (servidores) en la red es muy difícil mantener un adecuado nivel de seguridad. Esto es porque la seguridad de los host no se dimensiona bien o no se realizan adecuadas políticas de seguridad.

Un proxy es un "Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red". Su importancia es la misma que la del caché de cualquier navegador cliente de Internet, realizando una consulta primero en el proxy (que es lo que 'tiene' más cerca), para, en caso de no encontrarlo, realizar la búsqueda en Internet. La acepción habitual es la de servidor proxy, que no es otra cosa que un ordenador que se encuentra instalado entre el equipo del usuario e Internet. De esta forma se encarga de gestionar las peticiones que se realizan a la red, administrando el tráfico hacia fuera y permitiendo una mayor velocidad de acceso.

Los Firewalls por su parte, se colocan entre Internet y la red privada, de esta manera conseguimos concentrar la seguridad de nuestra red en ese punto. Los Firewalls mantienen una cierta separación entre la red privada e Internet, lo cual conduce a un buen nivel de seguridad. Gracias a las distintas arquitecturas de los firewalls podremos dimensionar mejor la seguridad de nuestra red.

1.2. La historia de Internet

Alrededor del año 1960 los transistores comenzaron a reemplazar a los tubos de vacío reduciendo tanto el tamaño de las computadoras como su costo y haciéndolas al mismo tiempo mucho más poderosas. Paralelamente Internet, como la mayoría de las demás creaciones del hombre, resultó de la necesidad humana. La guerra fría alcanzo su temperatura más baja en 1962, año de la crisis de los misiles en Cuba, y una guerra nuclear parecía inminente. Es así como el Departamento de Defensa de E.E.U.U. se enfrentó a un problema: ¿cómo mantenerse comunicados en caso de un ataque nuclear por parte del enemigo? Así, surgió la necesidad de una red de comunicación que operara aún si la mayoría de sus enlaces y nodos fueran destruidos durante un ataque nuclear [1], ver figura 1.1.

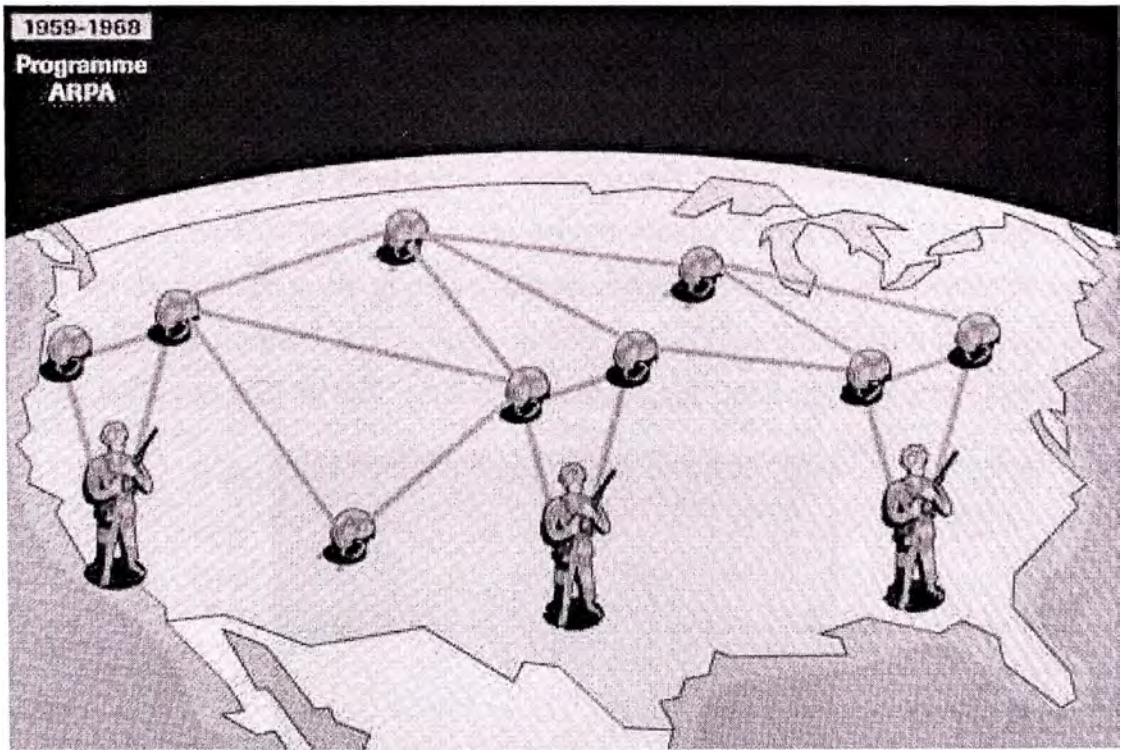

FIG. 1.1: RED MILITAR

Fue entonces cuando un grupo de científicos trabajaron juntos para que las computadoras pudieran comunicarse. A principio de los años 60, la idea flotaba entre diversas instituciones americanas, como el Instituto de Tecnología de Massachussetts (MIT, Massachussetts Institute of Technology, una de las universidades más prestigiosas del mundo) y la corporación RAND. Paúl Baran, un investigador de RAND, concibió entonces la idea de una red distribuida, autónoma y capaz de recibir, transmitir y enrutar la información, lo que posteriormente se desarrolló y convirtió en lo que hoy conocemos como Internet. En esta idea de red de comunicación, cada mensaje se quebraba en piezas de tamaño definido, y cada pieza sería transmitida como un paquete individualmente direccionado. Estas piezas encontrarían su camino a través de la red hacia el destinatario, por cualquier ruta que estuviera accesible, brincando de un nodo a otro hasta llegar a su destino final. De este modo, si un nodo era destruido, los paquetes de información encontrarían su ruta alternativa en la red. Al llegar a su destino final, estas piezas de información se reensamblarían a su posición original, recuperando el mensaje que se quería enviar. La idea de una red distribuida, así como la idea de "switcheo de paquetes" ó "conmutación de paquetes" (desmantelar cada mensaje y posteriormente ensamblarlo de nuevo para formar el mensaje original) se consideran como las aportaciones más importantes de Baran en el desarrollo de Internet.

Uno de los colaboradores de la Agencia de Proyectos de Investigación Avanzada del Pentágono (ARPA en sus siglas en inglés), Leonard Kleinrock, entonces un estudiante de doctorado en el MIT, conceptualizó la tecnología de "switcheo de paquetes" y publicó un paper sobre ello en 1961. El Pentágono, a través del ARPA financió la puesta en marcha de una prueba práctica. ARPA fue creada en respuesta al primer satélite artificial Sputnik, elaborado por la URSS y su objetivo consistía en mantener el liderazgo tecnológico estadounidense, ver figura 1.2. En 1969, el año que el hombre llego a la Luna, se abría el primer nodo de la red ARPANET, en la Universidad de California en Los Ángeles [2].

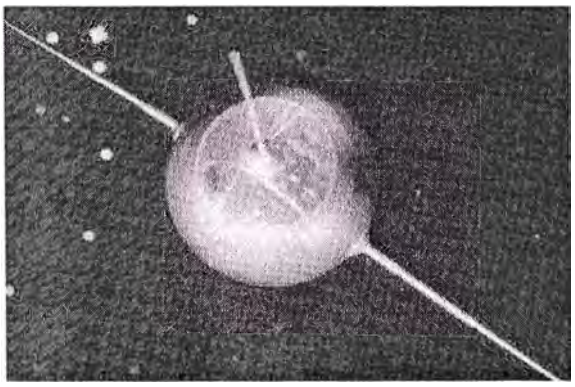

FIG. 1.2: SATÉLITE SPUTNIK

El segundo nodo de la red ARPANET fue en el Intitulo de Investigaciones de Stanford (IIS), donde trabajaba Douglas Engelbart en un proyecto sobre "ampliación del intelecto humano". Engelbart había inventado un poco antes el ratón, usado ahora por todas las computadoras, y se preocupaba por el trabajo en colaboración a través del hipertexto. No era un visionario aislado: en el MIT, J.C.R. Licklider ya discutía en 1962 su concepto de "Red Galáctica": un conjunto de computadoras interconectadas para dar acceso a almacenes de datos. De modo que esta red empezó a servir para algo realmente revolucionario: para comunicar personas más que computadoras.

En 1969 apareció en la Universidad de California en Los Ángeles el sistema de RFC (Request for Commentaries: petición de comentarios), que permitía a todos los participantes en el proyecto opinar sobre las temas técnicos (aunque además de estos comentarios florecieron pronto discusiones sobre ciencia ficción); la cultura llegaba pronto al nuevo medio. En 1971 Michael Hart creó el Proyecto Gutenberg, para crear y difundir gratuitamente textos electrónicos (el estándar ASCII databa de 1968). En 1972 fecha de la demostración pública de la red, apareció el primer programa de correo electrónico, que pronto se convirtió en una de las aplicaciones mas usadas; tres años después ya se discutía el problema de cómo bloquear el "correo basura" (spam). Mientras tanto, el primitivo proyecto ARPANET se preparaba para unirse con otras redes, siempre y cuando compartieran la "conmutación de paquetes". Es en 1983 cuando se considera que nació realmente la Internet, al separarse la parte militar y la civil de la red. En ese momento ya la compartían 500 servidores (computadoras interconectadas). En el mismo año se creó el sistema de nombres de dominios (.com, .edu, etc., más las siglas de los países), que prácticamente se ha mantenido hasta ahora. En 1984 William Gibson novelaba el nuevo mundo y acuñaba el término "ciberespacio". En la figura 1.3 se puede apreciar una gráfica que relaciona el número de servidores en función del tiempo.

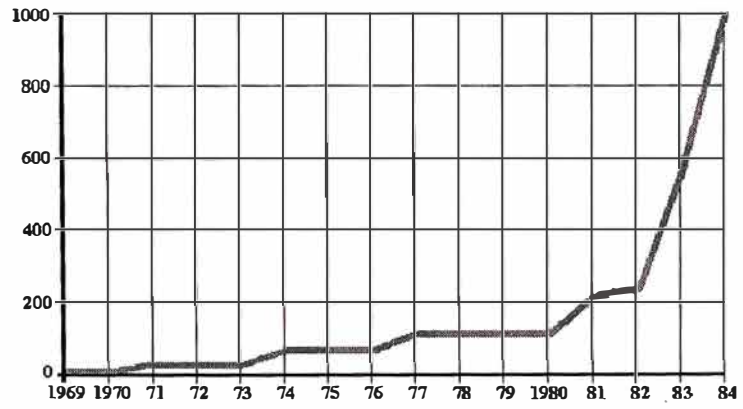

FIG. 1.3: SERVIDORES DE LA RED EN FUNCIÓN DEL TIEMPO

TABLA 1.1: RESUMEN DEL DESARROLLO DE INTERNET

Fecha	Suceso [1]
1957	La URSS lanzó Sputnik
1966	Experimentación con conmutación de paquetes en ARPA
1968	Primera red de conmutación de paquetes
1969	Nació ARPANET
1972	Primera demostración pública de correo electrónico sobre ARPANET
1973	Kahn y Cerf presentaron un artículo sobre Internet en la Primera Conexión Internacional de Internet
1975	Se fundo Microsoft. Aparece ya la preocupación por el correo basura (spam).
1976	Se fundo Apple
1979	Se creo UseNet
1980	Inicio de la fase experimental con TCP/IP
1981	Inclusión de nuevos nodos cada 20 días
1983	ARPANET emigró a TCP/IP y se dividió en ARPANET y MILNET Microsoft introduce Windows
1984	Internet excedió 1000 host. William Gibson escribió "Neuromancer". Se introdujo el Servidor de Nombres de Dominio (DNS)
1986	Creación de la parte troncal (backbone) de la NFSnet
1987	Internet excedió 10 000 host
1988	Un gusano ataco 6 000 de los 60 000 host de Internet
1989	Internet excedió 100 000 host
1990	ARPANET se desmanteló. Comenzó Archie (uno de los primeros servicios de Internet que permitía la búsqueda de archivos)
1991	Se creó WAIS. Se creó el Gopher (servicio de búsqueda de archivos)
1992	Internet excede 1 millón de host Se introduce el concepto "Web" creado por Tim Berners-Lee
1993	MOSAIC se desarrolló por Marc Andreesen InterNIC se fundó por NSF
1995	Privatización de la parte troncal de Internet

Al año siguiente se forjaba Well, la primera comunidad comercial de usuarios. ARPANET desapareció como tal en 1989, pero muchas instituciones (de la NASA al Departamento de Energía) ya habían creado sus propias redes que podían comunicarse entre sí. El número de servidores en la red superaba los 100 000. Ese mismo año, Tim Berners-Lee, investigador en el centro europeo CERN de Suiza, elaboró su propuesta de un sistema de hipertexto compartido; era el primer esbozo de la WWW. Como el ARPANET veinte años atrás, su propósito era poner en comunicación a los científicos. En 1992 con más de un millón de servidores en la red se creó la Internet Society, la "autoridad" de la red. Nacía como el lugar donde pactar los protocolos que harían posible la comunicación. Se trataba de una coordinación técnica, que no intervenía en los nacientes problemas de libre expresión: acababan de crearse la Fundación de Frontera Electrónica (Electronic Frontier Foundation), defensora de los "ciberderechos", y el más famoso sistema abierto de criptografía: Pretty Good Privacy. Con la extensión de las computadoras personales y el lanzamiento del primer navegador de la WWW popular, Mosaic, en 1993, ya había llegado el momento de "surfear en la Web" (la expresión se registró por primera vez ese mismo año). En 1994 se abre el primer ciberbanco. En 1997 ya hay 17 millones de servidores en la red. A partir de aquí las estadísticas se nublan: el tremendo crecimiento de la red, unido a la autonomía de su funcionamiento, hacen que grandes zonas de sus contenidos estén en la penumbra: según datos de 1999 el conjunto de los grandes buscadores de páginas en la Malla Mundial sólo conoce el contenido de menos del 50% de la red. La última iniciativa, Internet 2 [3], propone crear un espacio aparte y de más calidad en las comunicaciones para instituciones de investigación. Un resumen del desarrollo de Internet se muestra en la tabla 1.1.

1.2.1. La ARPANET

La ARPANET original consistió de cuatro servidores, la Universidad de California en los Ángeles (UCLA), el Instituto de Investigaciones de Stanford, la Universidad de California en Santa Bárbara y la Universidad de UTA, ver figura 1.4. Posteriormente, la red de ARPANET fue reemplazada por la NSFnet que culminó en lo que hoy es Internet. Esta pequeña red, usando el Protocolo de Control de Red (NCP, del inglés Network Control Protocol) proporcionó a sus usuarios la habilidad de entrar a un host remoto, imprimir en una impresora remota y transferir archivos.

FIG. 1.4: LA ARPANET ORIGINALMENTE CONSISTÍA EN CUATRO SERVIDORES.

Ray Tomlinson, un ingeniero de la compañía BBN, creó en 1971 el primer programa de correo electrónico. ARPANET funcionaba a partir del principio de "conmutación de paquetes" y estaba basada en un conjunto de pequeños computadores interconectados llamados procesadores de mensajes con interfaz (IMPs). Estos IMPs, son los precursores de los modernos dispositivos de enrutamiento. En su segundo año de operatividad, sin embargo, algo extraño sucedió. Los usuarios de ARPANET habían convertido la red en una oficina de correos electrónica de alta velocidad subvencionada federalmente.

La mayor parte del tráfico de ARPANET no era el proceso de datos a largas distancias. En vez de eso, lo que se movía por allí eran noticias y mensajes personales. Los investigadores estaban usando ARPANET para colaborar en proyectos e intercambiar notas sobre sus trabajos. La gente tenía sus propias cuentas personales en las computadoras de ARPANET y sus direcciones personales de correo electrónico. No es que sólo utilizaran ARPANET para la comunicación de persona a persona, pero había mucho entusiasmo por esta posibilidad – mucho mas que por la computación a larga distancia. Eso no pasó mucho antes del invento de las listas de distribución, una técnica de emisión de información por ARPANET mediante la cual un mismo mensaje se podía enviar automáticamente a una gran cantidad de subscriptores. Es interesante que una de las primeras listas de distribución masivas se llamara "Amantes de la Ciencia Ficción" (SF-LOVERS). Discutir sobre ciencia ficción en la red no tenía nada que ver con el trabajo y eso enfadaba a muchos administradores del sistema de ARPANET, pero eso no impediría que la cosa siguiera. Durante los 70s, ARPANET creció. Su estructura descentralizada facilitó la expansión. Contrariamente a las redes estándar de las empresas, la red de ARPA se podía acomodar a diferentes tipos de computadoras. En

tanto una máquina individual pudiese hablar el lenguaje de conmutación de paquetes de la nueva y anárquica red, su marca, contenidos e incluso su propietario eran irrelevantes. El éxito de la ARPANET [4] fue en si el catalizador para la investigación en redes dando como resultado un protocolo de emergencia: el TCP/IP, el cual se estableció firmemente en 1980. La naturaleza descentralizada de ARPANET y la disponibilidad sin costo de programas basados en TCP/IP permitió que ya en 1977, otro tipo de redes no necesariamente vinculadas al proyecto original, empezaran a conectarse. En 1983, el segmento militar de ARPANET decide separarse y formar su propia red que se conoció como MILNET. ARPANET completó su transición al TCP/IP en 1983, y en 1990 dejó de ser la espina dorsal de la red Internet.

1.2.2. Conmutación de paquetes

Una de las ideas brillantes de Baran [5] fue dividir los mensajes en "bloques de mensaje" antes de enviarlos a través de la red. Cada mensaje debería enviarse separadamente y reunirse para completar el mensaje cuando fueran recibidos en su destino, ver figura 1.5. Un británico llamado Donald Davies de forma independiente divisó un sistema muy similar, pera le llamo a los bloques de mensaje como "paquetes", un término que fue adoptado eventualmente en vez del término bloques de mensaje de Baran. Los paquetes permitieron una vía muy eficiente para transmitir datos. Las comunicaciones de datos son por naturaleza erráticas. La información es enviada en ráfagas, no en forma continua. Las líneas tradicionales de comunicación emplean líneas dedicadas, las redes telefónicas son un buen ejemplo, cuando se hace una llamada, una línea se dedica para esa llamada, nadie más puede usar esa línea mientras se está realizando la llamada. Si existe una pausa en la conversación, no se envían datos, pero la línea se mantiene en uso y no disponible. Esto representa un desperdicio en la capacidad de comunicación (la "capacidad de comunicación" se conoce como ancho de banda). Baran visionó a red con nodos autónomos que podrían actuar como interruptores ruteando paquetes de un nodo a otro hasta su destino final. Los nodos se diseñarían para guardar y enviar rápidamente, esquema que le llamó "ruteo de papa caliente". Cuando un nodo recibe un paquete, el nodo lo almacena; entonces determina la mejor ruta para su destino, y lo envía al siguiente nodo en el camino (de la mejor ruta). Usando computadores digitales como nodos, el proceso de ruteo podría hacerse muy rápidamente permitiendo transmisiones en tiempo real. Las computadoras podrían usar estadísticas, puestas al día de forma constante, de la red y cada uno de sus nodos para determinar la mejor ruta en cualquier momento. Si hubiese un problema con algún nodo (o si hubiese sido destruido) los paquetes podrían rutearse alrededor de él. El método de actualizar constantemente la

información de la red para el ruteo se conoce también como ruteo dinámico. En la ARPANET, varios años después, cuando Larry Roberts estaba comenzando a trabajar en la ARPANET, él había escuchado de las ideas de Baran. Roberts no diseño una red para uso en tiempo de guerra, sino para facilitar la comunicación en los investigadores de la ARPA y para permitirles el uso eficiente de recursos remotos. Pero las ideas de Baran afectaron a Roberts. Se adoptaron las ideas de Baran sobre una red distribuida y con un esquema de conmutación de paquetes, y Baran se convirtió en un consultante informal del proyecto ARPANET.

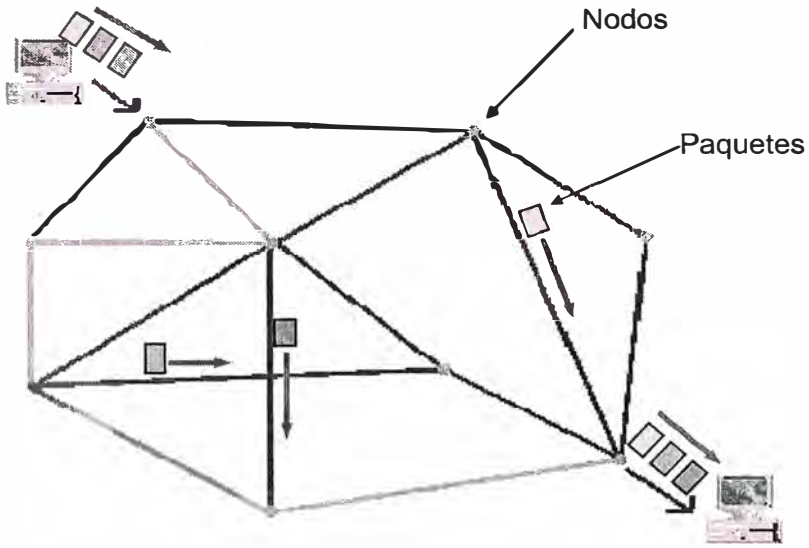

FIG. 1.5: CONMUTACIÓN POR PAQUETES

1.3 Inicios del TCP/IP

En 1974, justo cuatro años después del nacimiento de la ARPANET, Vinton Cref y Robert Kahn, ver figura 1.6, inventaron el Protocolo de Control de Transmisión (TCP, del inglés Transmission Control Protocol). En 1974 publicaron el proyecto sobre el TCP. El protocolo TCP fue diseñado para ser independiente de cualquier computadora o red. De este modo, ninguna computadora o red es esencial, ya que TCP/IP se adapta perfectamente a cualquier software o hardware.

Debido a esta increíble capacidad de adaptación a cualquier medio, TCP/IP fue implantado en la ARPANET solo tres años después de la publicación del primer artículo sobre éste, es decir, en 1977. En aquel entonces ARPANET funcionaba a base de NCP (Network Control Protocol). Con el tiempo, TCP/IP reemplazó a NCP, debido a que NCP no era capaz de manejar eficientemente el enorme tráfico que empezaba a producir la red [6]. Entre otras razones se encuentran el fácil mantenimiento y el bajo costo de implantación de TCP/IP. Los ajustes posteriores determinaron la incorporación del

apéndice IP, por Internet Protocol en 1978, convirtiendo TCP en lo que hoy conocemos como TCP/IP.

FIG. 1.6: VINTON CREF Y ROBERT KAHN INVENTARON EL PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP, DEL INGLÉS TRANSMISSION CONTROL PROTOCOL).

Un tiempo después ARPANET ya no estaba sola. Entidades estatales y académicas estadounidenses y europeas se sumaban al mundo de las redes. De este modo, se tenía que escoger un solo protocolo de red para que todas las redes pudieran trabajar juntas. Se escogió TCP/IP, debido a sus cualidades ya mencionadas. De esta manera, TCP/IP proveía un puente tecnológico que unía las pequeñas redes alrededor del mundo [7], ver figura 1.7.

En 1982, rendido ante la evidencia de la popularidad del protocolo y de la fuerza de las conexiones a la red, ARPA decidió desclasificar el TCP/IP y además dispuso que fuera de uso obligatorio para todas aquellas redes conectadas a ARPANET, para cualquier computadora dentro de ARPANET ó conectada a ARPANET, era obligada a cambiarse al protocolo TCP/IP dentro de un plazo de unos cuantos meses. Debido a las facilidades de este protocolo, muchos de los usuarios lo hicieron con éxito. En el año 1983, los usuarios empezaron a llamar a ARPANET y sus afiliados como Internet, y en ese mismo año, el cambio en el lenguaje se hace oficial. Fue entonces cuando nació la Internet.

FIG. 1.7: EL PROTOCOLO TCP/IP PROVEÍA UN PUENTE TECNOLÓGICO QUE UNÍA LAS PEQUEÑAS REDES ALREDEDOR DEL MUNDO.

1.3.1. Capas y protocolos de TCP/IP

El requisito previo para estudiar TCP/IP es comprender el modelo Interconexión de sistema abierto. TCP/IP es una familia de protocolos y aplicaciones que realizan funciones diferenciadas que corresponden a capas especificas del modelo OSI [9]. El modelo OSI representa una metodología jerárquica de siete capas para la transmisión de datos desde una aplicación que reside en un equipo a la aplicación que reside en otro equipo. En la parte superior del modelo (capa 7) están las interfaces de la aplicación para los servicios de red que utiliza. En la parte inferior (capa1) esta el alambre o el cable de fibra óptica que conecta los equipos. Todo lo que hay entre ellos proporciona los mecanismos para mover los datos desde la aplicación al cable y viceversa. La Figura 1.8 muestra una representación grafica del modelo de referencia OSI y su relación con TCP/IP.

En los siguientes párrafos, se describen los niveles del modelo OSI y como dichas capas se relacionan con TCP/IP [8].

La capa 1, la capa *física*, incluye todos los componentes eléctricos necesarios para transmitir y recibir datos de una red. Esto incluye el alambre y el cable, los diferentes métodos de cifrado y señalización, así como los transmisores, repetidores y receptores que se utilizan para transportar las señales al alambre y recibirlas desde este.

La capa 2, la capa *vínculo de datos*, tiene dos funciones principales. Primero la capa 2 proporciona la dirección que la red de la capa física necesita para conectar equipos para

que puedan ser identificados como únicos en la red. Los protocolos de red de área local (LAN, *Local Área Network*) más comunes, como Ethernet y Token Ring, utilizan una dirección de 48 bits para identificar cada nodo de la red. A menudo, a esta parte de la capa 2 se la denomina subcapa de *Control de acceso al medio físico* (MAC, *Media Access Control*), y estas direcciones se denominan *direcciones MAC*. La segunda función importante de la capa 2 es proporcionar un método básico para interconectar las LAN.

Modelo de referencia OSI	***Modelo TCP/IP***	***Descripción***
Capa 7 Aplicación	***La capa de aplicación***	Aquí están los programas que hacen uso de los servicios proporcionados por las capas inferiores • http (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), etc.
Capa 6 Presentación		
Capa 5 Sesión		
Capa 4 Transporte	***La capa de transporte***	Aquí se sitúa el TCP/UDP • Envía acuses de recibo • Reagrupa el mensaje en destino • Vuelve a mandar los paquetes perdidos o defectuosos.
Capa 3 Capa de red	***La capa de Internet (red)***	Es donde se sitúa el protocolo IP • Esquema de direcciones • Encaminamiento
Capa 2 Vínculo de datos	***La capa interfaz de red (liga de datos)***	Es la de mas bajo nivel • Representa el medio físico encargado de enviar en última instancia los 0 y 1 que componen cada mensaje. • Existen diversas tecnologías, ATM, Ethernet, etc.
Capa 1 Física		

FIG. 1.8: EL MODELO OSI Y SU RELACIÓN TCP/IP

Este modelo básico se denomina *puente*. El puente permite conectar mas de una LAN de nivel 1 entre si y evita que los paquetes viajen en bucles utilizando un protocolo rudimentario, como un árbol de expansión o puente de enrutamiento a origen. Un caso especial de puente es mas conocido como *conmutador*. Los conmutadores son, simplemente, puentes multipuerto, y cada puerto representa una LAN diferente. Los conmutadores mas actuales se implementan en el hardware, haciéndolos muy rápidos en comparación con los puentes de software. Normalmente cada puerto de un conmutador LAN se dedica a un solo host. Los conmutadores de una red de área extensa (WAN,

Wide Área Network), como los que se usan en la redes Frame Relay o Modo de transferencia asíncrona (ATM, *Asynchronous Transfer Mode*), se utilizan normalmente para interconectar Lan en diferentes ubicaciones geográficas.

La capa 3, la capa de *red*, también tiene dos funciones principales. La primera función, como la capa 2, es proporcionar una dirección única a cada host de la red. Sin embargo, la diferencia entre la capa 2 y la capa 3 es que los protocolos de la capa 3 proporcionan generalmente un medio para ensamblar una red de forma jerárquica. Allí donde las direcciones MAC son únicas, también son asignadas secuencialmente por los fabricantes y distribuidas de forma aleatoria en la red. Por otra parte, las direcciones de la capa 3 se asignan normalmente de tal forma que todos los host de una red concreta tienen direcciones que los identifica como miembros de dicha red. La capa 3 también proporciona un medio para conectar las redes de las capas 1 y 2 utilizando enrutadores. Los enrutadores ejecutan protocolos más complejos que los puentes y pueden interconectar de forma visual un número ilimitado de redes. IP es el protocolo de capa 3 más utilizado en todo el mundo.

La capa 4, la capa de *transporte*, es el punto de conexión entre los niveles inferiores, que comprenden la red, y los niveles superiores, que son las aplicaciones. Normalmente, los protocolos de nivel de transporte asignan protocolos de los niveles superiores y las aplicaciones a los números de los puertos. Estos números de puertos se transmiten a continuación junto con los datos a través de la red y los utiliza el host receptor para determinar que aplicación debiera recibir los datos.

En todo los casos, el modelo que sigue el protocolo TCP/IP no implementa estrictamente los niveles 5, 6 y 7 del modelo OSI como componentes independientes y diferenciados. Aunque el modelo OSI especifica las responsabilidades de cada nivel, las aplicaciones que utiliza TCP/IP normalmente implementan algunos de estos niveles, o con todos, dentro de la aplicación según sea necesario.

La capa 5, la capa de *sesión*, proporciona el recurso para que una entidad cree una sesión con otra a través de una red. Aunque TCP/IP se escribe normalmente como un protocolo de nivel de transporte, implementa la mayoría de la funcionalidad necesaria de la capa de sesión en el modelo OSI. Por tanto la pila del protocolo TCP/IP no contiene un protocolo de nivel de sesión diferente. Los primeros sistemas de red Microsoft e IBM incluían un protocolo de nivel de sesión y API llamado *Servicio básico de red de entrada/salida* (NetBios), que se utilizaba sin TCP/IP como protocolo LAN. NetBios aun

se utiliza normalmente en las redes de Microsoft, pero actualmente suele estar integrado en TCP/IP.

La capa 6, la capa de *presentación*, proporciona estándares para dar formato o codificar datos para transmitirlos a través de la red. Al utilizar TCP/IP muchas aplicaciones preceden a un nivel de presentación formal y transmiten los datos sin formato. Un ejemplo de protocolo de nivel de presentación es Extensiones multipropósito de correo Internet (MIME, *Multipurpose Internet Mail Extensions*), que proporciona un formato estándar para la transmisión de archivos adjuntos de correo electrónico.

La capa 7, la capa de *aplicación*, proporciona las interfaces para que las aplicaciones tengan acceso a servicios de red, como la transferencia de archivos entre host, el establecimiento de conexiones terminales, y los servicios de acceso a directorios.

1.3.2. El encabezado de TCP

En la figura 1.9 se muestra los componentes del encabezado TCP [8] y a continuación se enumeran sus funciones:

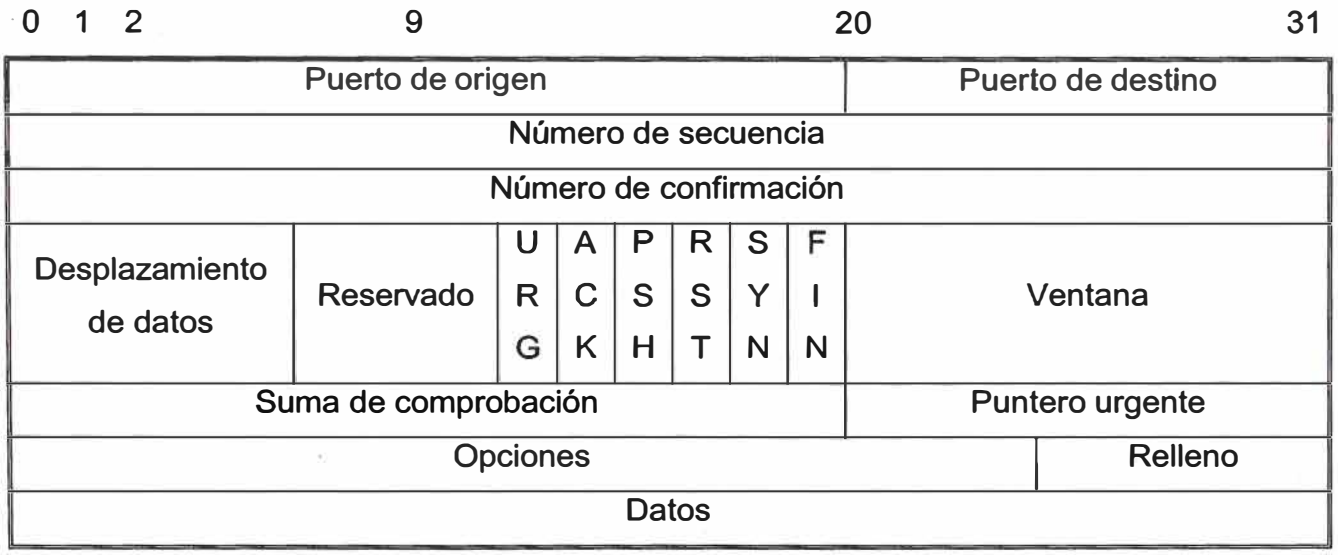

FIG. 1.9: EL ENCABEZADO DE TCP

- **Puerto de origen** El puerto de origen en TCP, al igual que en UDP, es una cantidad de 16 bits. Designa el puerto en el que el host de destino debería responder. Normalmente lo designa casi aleatoriamente el proceso TCP en el host de origen. Generalmente, el puerto de origen se asigna desde los números superiores a 1.023, aunque esto no es necesario. Por ejemplo, los host Unix de

estilo Berkeley Software Distribution (BSD) asignan de forma secuencial puertos de origen que comiencen por 1.024, pero otros, como los host Solaris, asignan los que comienzan en 32.768.

- **Puerto de destino** El host emisor asigna el puerto de destino. Se supone que el host de destino tiene una asociación con una aplicación o proceso para el puerto. Por este motivo, algunos puertos <<conocidos>> se utilizan universalmente. Por ejemplo, http utiliza el puerto 80. Todos los host que actúan como servidores Web escuchan el puerto 80, de forma predeterminada, para que los exploradores Web de todos los host puedan ver páginas en cualquier servidor sin necesidad de interacción por parte del usuario. El administrador de servidores puede cambiar esta configuración, pero, a continuación, un usuario con un explorador tendrá que especificar el puerto en el URL. Al escribir http://www.foo.com:81 se conectara al servidor www.foo.com que escucha a HTTP en el puerto 81. Anteriormente, los puertos conocidos abarcaban los números entre 1 y 1 024. Sin embargo, actualmente, hay más puertos conocidos. La lista de números de puertos TCP conocidos y las aplicaciones a las que están asociados están disponibles en RFC 1700, Assigned Numbers.

- **Número de secuencia** Este es uno de los parámetros que utiliza TCP para asegurar el transporte de forma ordenada y fiable. Cada octeto que se transmite incrementa el número de secuencia. En una conexión ya establecida, el número de secuencia transmitido es el número de secuencia del primer octeto de datos del paquete.

- **Número de confirmación** Es el siguiente numero de secuencia que espera recibir el emisor de la confirmación. Esto permite a un host confirmar todos los octetos recibidos hasta ese momento.

- **Desplazamiento** Es análogo al campo longitud en IP. Es el número de palabras de 32 bits en el encabezado TCP. Al igual que con IP, el encabezado TCP siempre se rellena para igualar un numero entero de palabras de 32 bits.

- **Reservado** Seis bits que siempre son cero.

- **Indicadores** También conocidos como *bits de control*, sirven para los siguientes propósitos cuando e definen:

    - **Urgent** Indica al receptor que examine el campo del puntero urgente. De lo contrario, se omite el campo.

    - **Ack** Indica al receptor que en ese campo hay un numero de confirmación. Ack siempre se define para conexiones establecidas.

    - **Push** Indica a TCP que envié los datos inmediatamente. Es útil si la aplicación necesita verificar que todo lo que ha enviado a TCP se ha enviado correctamente. De lo contrario TCP podría esperar hasta recibir suficientes datos para llenar la ventana antes de realizar el envió, provocando un retraso en las transacciones en las que el tiempo es crucial.

    - **Reset** Provoca que la sesión en curso se cierre.

    - **SYN** Son las siglas de Números de secuencia sincronizados (*Synchronize Séquense Numbers*). Este indicador se define en el primer paquete que se envía para intentar establecer una sesión TCP. El primer paquete contiene un número de secuencia del emisor. A continuación, el receptor debería confirmar el número de secuencia inicial mas uno. El bit SYN nunca se define en una conexión establecida.

    - **FIN** El emisor ha terminado de enviar los datos. Esto hará que la sesión finalice.

- **Ventana** Número de octetos que el receptor es capaz de aceptar. Se envía con cada paquete de confirmación. El emisor no puede enviar más datos que el tamaño de la ventana hasta que reciba otra confirmación con una nueva ventana que indica que tiene permiso para enviar más datos.

- **Total de control** Verifica la integridad del encabezado y los datos. A diferencia del total de control IP, que solo verifica el encabezado IP, el total de control TCP verifica el encabezado TCP y todos los datos que siguen al encabezado.

- **Puntero urgente** Apunta al lugar en los datos que la aplicación considera urgente. Solo se lee cuando se define el bit urgente.

- **Opciones** Permite implementar los parámetros opcionales. El que inicia la sesión puede especificar, por ejemplo, una longitud de segmento máxima.

- **Relleno** Se utiliza como relleno para agregar los finales de paquetes en los límites de 32 bits.

1.3.3. El encabezado de IP

Las direcciones IP de origen y destino solo forman una parte del encabezado IP [8]. El resto del encabezado contiene información adicional que ayuda a desplazar el paquete por la red, verifica la integridad de la información del encabezado y proporciona instrucciones de transporte a los niveles superiores para los datos. En la figura 1.10 se definen las partes del encabezado IP

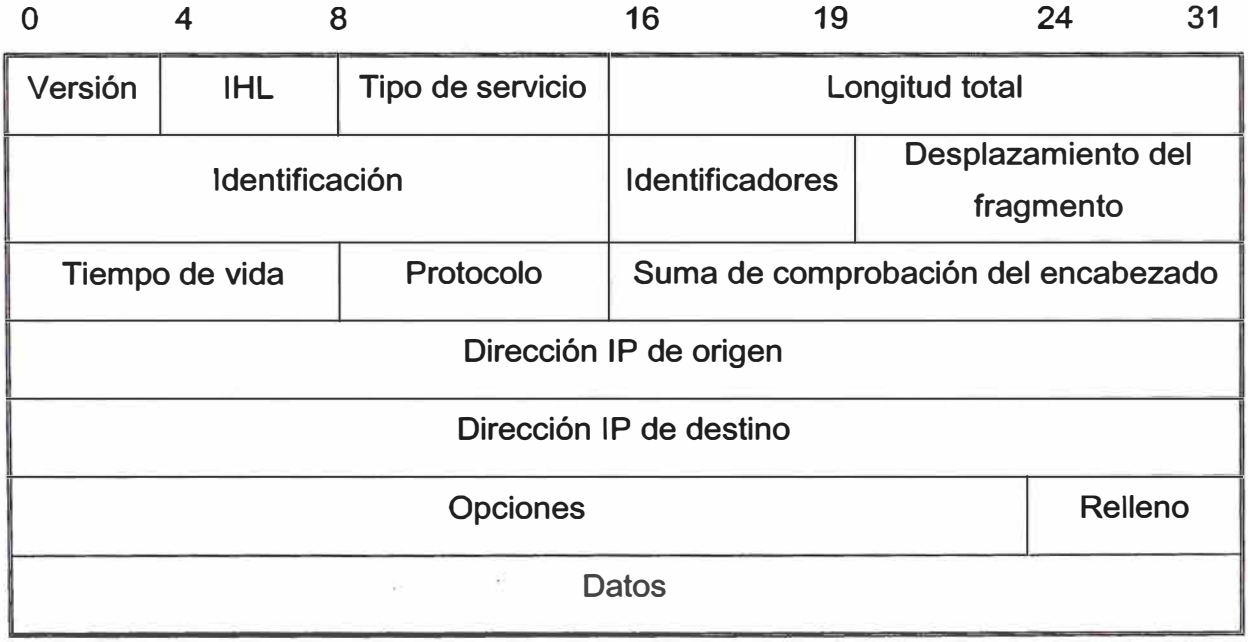

FIG. 1.10: EL ENCABEZADO DEL IP

- **Versión** Número de versión del protocolo IP. Para IPv4, siempre es 4.

- **Longitud del encabezado de Internet (IHL, *Internet Header Lench*)** Especifica la longitud de encabezado IP en palabras de 32 bits. Normalmente es 5, pero puede ser mayor si se agregan opciones al final del encabezado IP.

- **Tipo de servicio (*TOS, Type of Service*)** Es una cantidad de 8 bits que permite varias prioridades e información de procedencia para ser insertada en el encabezado. Mas recientemente, el campo diffserve, un intento por estandarizar IP basado en Calidad del servicio (QoS, *Quality of Service*), ha sustituido los diferentes componentes TOS.

- **Longitud total** Longitud total de la trama IP, incluidos los datos de la capa superior.

- **Identificación** Número de identificación que se utiliza en el reensamblado de paquetes fragmentados. Los enrutadores pueden fragmenta paquetes IP que son mayores que la unidad de transmisión máxima (MTU, *Maximum Transmisión Unit*) de cualquier medio LAN o WAN. Por ejemplo, un paquete de 4000 bits que originalmente se ha transmitido a una red FDI tendría que fragmentarse si un enrutador lo transmitiera a una red Ethernet, que tiene una MTU más pequeña de 1500 bits. El dispositivo IP de destino tiene la responsabilidad de reensamblar el paquete.

- **Identificadores** El primero de los tres bits de identificación siempre es cero. El segundo indica a los enrutadores si tendrán que fragmentar el paquete. Un paquete tendrá el conjunto de bits <<no fragmentar>> si ya es un fragmento de un paquete más grande. No esta permitido fragmentar el mismo paquete dos veces. En la práctica, el primer enrutador que fragmenta un paquete lo dividirá en fragmentos de 576 bits, el mínimo permitido para los medios que aceptan IP. De esta manera, se evita que otro enrutador tenga que fragmentarlo más.

- **Desplazamiento de fragmento** Un enrutador que fragmenta un paquete establece este campo como un número de bytes desde el principio del paquete original. Esto permite a la estación receptora reensamblar los fragmentos en orden.

- **Tiempo de vida (TTL, *Time of Live*)** Cantidad de 8 bits que será disminuida, normalmente en 1, por enrutador a medida que los paquetes los cruzan. El enrutador que disminuye el TTL a 0 tiene que descartarlo. Esto establece un límite superior de

256 saltos de enrutador que pueden atravesar los paquetes IP. Este campo pretende ser un punto de seguridad final frente a los interminables bucles de enrutamiento.

- **Protocolo** Cantidad de 8 bits que describe qué protocolo de nivel de transporte u otra aplicación ha pasado los datos a IP. IP los pasara de vuelta a dicho protocolo en el destino final. TCP/IP es el protocolo que se puede definir aquí.

- **Suma de comprobación** Verifica la integridad del encabezado IP.

- **Origen** Dirección IP del host transmisor.

- **Destino** Dirección IP del host receptor.

- **Opciones** Puede contener información adicional, según la haya definido el origen. La longitud de ese campo, en palabras de 32 bits, debe agregarse al campo IHL al principio del encabezado IP. Algunas opciones son la capacidad de incrustar una clasificación de seguridad en el encabezado (utilizada por el Departamento de Seguridad de Estados Unidos), la opción de especificar la ruta de acceso del enrutador que el paquete va a utilizar para viajar desde el origen al destino, y la capacidad para registrar cada salto con el propósito de solucionar problemas. Estas opciones no se utilizan casi nunca. Los paquetes con información de enrutamiento desde el origen se utilizan a veces con propósitos maliciosos, por lo que normalmente los enrutadores se configuran para hacer caso omiso de los campos de rutas de origen en los paquetes IP.

- **Relleno** Se utilizan como relleno para asegurarse la longitud de los paquetes a 32 bits.

Resumen cap. I

En este capitulo se hace un revisión del proceso de formación de lo que hoy conocemos como la Internet, se analiza la conmutación de paquetes y el surgimiento de un protocolo unificador, básicamente como una necesidad de estandarizar la comunicación. Finalmente se hace una revisión de los encabezados, tanto del TCP como del IP.

CAPÍTULO II
REDES UTILIZANDO TCP/IP

2.1. TCP/IP y sus beneficios

En la figura 2.1 se muestra una red conectada a Internet a través de un proveedor de Internet.

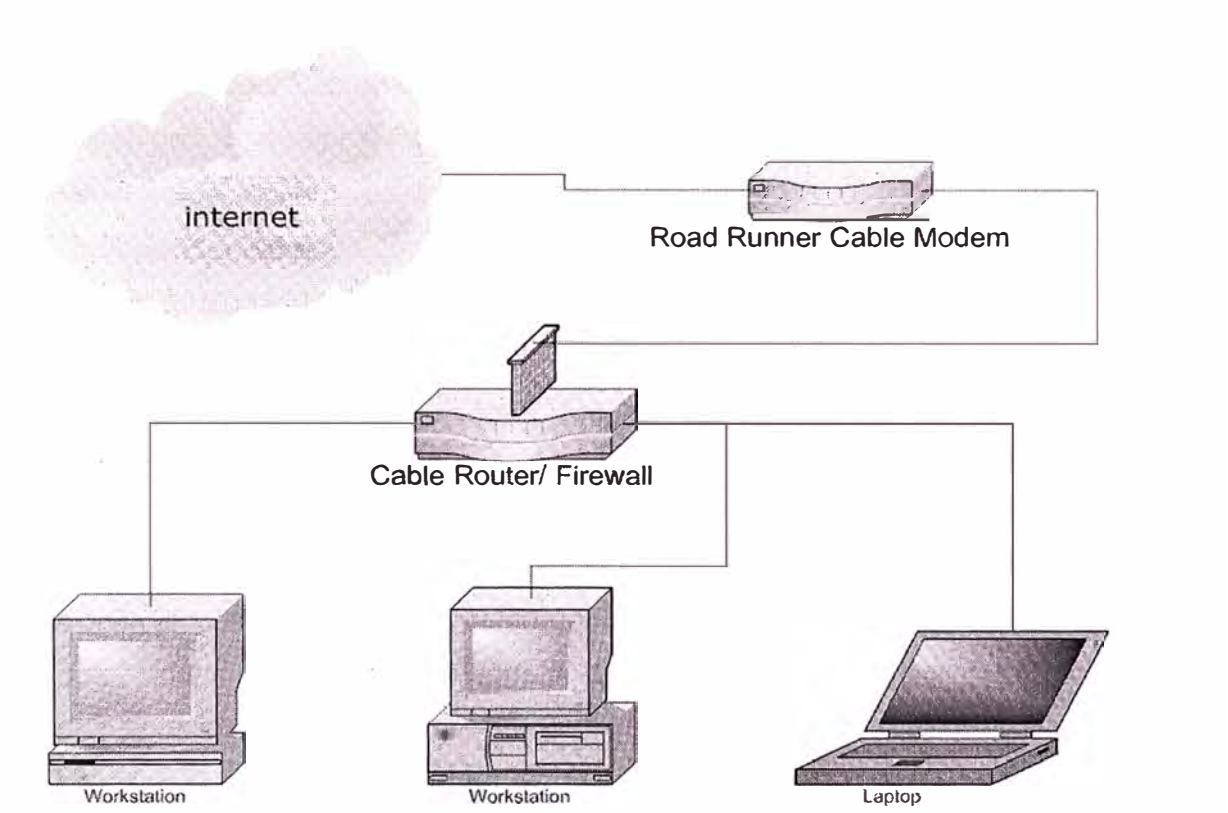

FIG: 2.1: ESQUEMA BÁSICO DE UNA RED

TCP/IP define una interfaz abstracta a través de la cual se puede acceder al hardware, esto a su vez es un mecanismo que oculta la diversidad de equipos que puede usarse en un ambiente de red [10]. Esta interfaz ofrece un conjunto de operaciones que es el mismo para todos los tipos de hardware y que trata básicamente con el envío y recepción de paquetes. Las interfaces PPP (que se usan para conectarse con un modem) tienen nombres como ppp0 y ppp1. Antes de usar una interfaz en una red, se debe asignar una dirección IP que sirve como su identificación cuando se comunican en el resto del mundo.

Esta dirección es diferente del nombre de la interfaz mencionada en el párrafo anterior; si se compara la interfaz con una puerta, la dirección es como la placa de identificación pegada a ella. Otros parámetros pueden ponerse para el dispositivo, tal como el tamaño máximo de los datagramas que pueden ser procesados por una pieza particular de hardware, el cual es conocido como la Unidad de Transferencia Máxima (Maximum Transfer Unit, MTU). Otros atributos se conocerán posteriormente. Afortunadamente, la mayoría de los atributos tienen valores por defecto funcionales.

TCP/IP permite plataformas-entrelazadas o administración de redes heterogéneas. Por ejemplo una red de Windows NT podría contener una computadora de Unix o Macintosh o hasta redes mixtas. TCP/IP también tiene las siguientes características:

- Buena recuperación de las fallas.
- Habilidad de añadir redes sin interrumpir los servicios ya existentes.
- Manejo de alto porcentaje de errores.
- Independencia de la plataforma
- Bajos gastos indirectos de información.

Debido a que originalmente TCP/IP fue diseñado por propósitos relacionados al Departamento de Defensa de Estados Unidos, lo que ahora llamamos características fueron de hecho requisitos de diseño. La idea detrás de "Buena recuperación de las fallas" fue que si una parte de red fuera dañada durante un ataque, las piezas de red restantes deben seguir funcionando adecuadamente. Lo mismo aplica para, la capacidad de añadir nuevas redes, sin interrupción a los servicios ya existentes. La habilidad de manejar gran porcentaje de errores fue implantado para que si un paquete de información se pierde al recorrer una ruta, habría un mecanismo que asegurara que éste llegará a su destino mediante otra ruta. Independencia de plataforma significa que las redes y los clientes pueden ser Windows, Unix, Macintosh o cualquier otra plataforma o combinación de ellas. La razón por la cual TCP/IP es tan eficiente son sus gastos indirectos bajos. Desempeño es la clave de cualquier red. TCP/IP no tiene una contraparte en su simplicidad y rapidez.

2.2. Números binarios y decimales

En base dos ó números binarios, ver figura 2.2, el valor representado por "1" es determinado por su posición. No es diferente de la base diez que todos conocemos, en la cual el primer numero desde la derecha enumera unidades, el segundo desde la derecha enumera decenas, el tercero centenas, y así hasta el infinito. Mientras el sistema decimal

provee 10 dígitos (de 0 a 9) para representar diferentes valores, el sistema binario solo ofrece dos dígitos validos: 0 y 1.

FIG. 2.2: EL SISTEMA BINARIO OFRECE DOS DÍGITOS VALIDOS 0 Y 1

Su posición, al igual que en el sistema decimal, determina el valor que representa. La posición que esta hasta la derecha, en términos decimales, representa 2. La siguiente posición a la izquierda 4, la siguiente 8, etc. Cada posición vale 2 veces más que su vecina derecha. El valor decimal de un numero binario se calcula sumando los valores decimales de los dígitos que tienen 1 en su posición. Matemáticamente, cada octeto de una dirección IPv4 (hay 4 de ellos) puede tener un valor máximo de 225 en el sistema decimal. Un número binario equivalente a 225 consiste de 8 bits, con todos los bits 1. Supongamos que se desea determinar el valor decimal del número binario 11111111. En la tabla 2.1 se muestra cada digito, su posición y su valor decimal.

TABLA 2.1: RELACIONA UN NÚMERO BINARIO Y SU VALOR DECIMAL

Posición del dígito	7	6	5	4	3	2	1	0
Dígito en binario	1	1	1	1	1	1	1	1
Valor decimal del dígito	128	64	32	16	8	4	2	1
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

El valor decimal del número binario 11111111 es la suma de los valores decimales de cada dígito 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1, es decir, 255.

Supongamos ahora que deseamos determinar el valor decimal del número binario 11101111. En la tabla 2.2 se muestra cada digito, su posición y su valor decimal.

TABLA 2.2: RELACIONA UN NÚMERO BINARIO Y SU VALOR DECIMAL

Posición del dígito	7	6	5	4	3	2	1	0
Dígito en binario	1	1	1	0	1	1	1	1
Valor decimal del dígito	128	64	32	16	8	4	2	1
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

El valor decimal del número binario 11101111 es la suma de los valores decimales de cada dígito 128 + 64 + 32 + 0 + 8 + 4 + 2 + 1, tomando en cuenta que el dígito en la posición 4 es 0, es decir, 239.

Esta relación entre números binarios y decimales es la base de la arquitectura de direcciones IP. Recuerde que hay 4 octetos binarios en cada dirección IPv4, incluyendo subredes enmascaradas. Por eso es necesario entender la relación entre estos sistemas básicos, la conversión del uno al otro, antes de estudiar distintas maneras de implantar dirección de IP.

2.3. Direcciones IP

El protocolo de red IP entiende las direcciones como números de 32 bits. Esta convención es para la versión 4 (IPv4) que será tratada en todo el curso. A cada máquina debe asignársele un número único en el ambiente de la red, ver figura 2.3.

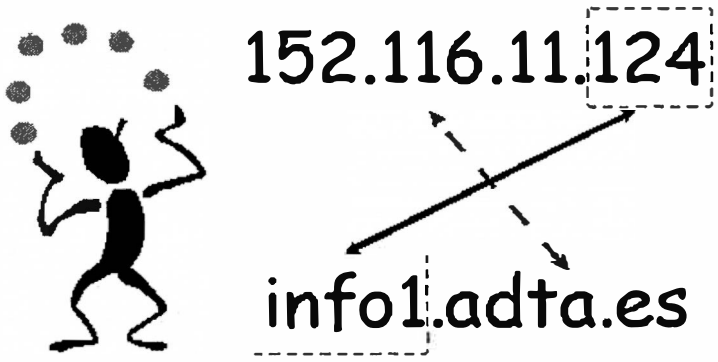

FIG: 2.3 DIRECCIÓN IP

Existen algunos intervalos de números IP que se han reservado para usarse en el diseño de intranets (ó redes privadas). Estos intervalos están listados en la tabla 2.4. Sin embargo, para sitios de Internet, los números eran asignados hace ya algunos años, por una autoridad central, el Centro de Información de la Red (NIC, Network Information Center). Actualmente los números que se usarán son asignados por el mismo proveedor de Internet al que se le compra la conectividad IP. Las direcciones IP se dividen por legibilidad en cuatro números de ocho bits, llamados octetos. Por ejemplo, luna.computacion.universidad.mx tiene la dirección 0x954C0C04, el cual se escribe como 149.76.12.4. Este formato se refiere frecuentemente como notación decimal puntuada.

De esta forma cada byte es convertido en un número decimal (0-255), despreciando los ceros a la izquierda a menos que el número en sí sea cero. Otra razón para esta notación es que una dirección IP se puede dividir en un número de red, la cual está contenida en los primeros octetos, y un número de host, que está en los restantes octetos. Cuando de requieren números IP y se les pide al NIC, este no asigna un número por cada host que se planea usar. En vez de ello se asigna un número de red y se permite asignar todas las direcciones IP válidas dentro del intervalo del número de host sobre su propia red, de acuerdo al diseño propio que se tenga. Al número de bits que comparten todas las direcciones de una red se le llama máscara de red (netmask), y su papel es determinar qué direcciones pertenecen a la red y cuáles no. Esto puede verse con el ejemplo mostrado en la tabla 2.3.

TABLA 2.3: EJEMPLO DE LA DIVISIÓN DE UNA DIRECCIÓN IP

Dirección IP	192.168.120.21
Mascara de red	255.255.255.0
Número de red	192.168.120
Host	.21

Cualquier dirección a la que se aplique una operación AND de bits con su máscara de red, revelará la dirección de la red a la que pertenece. La dirección de red es por tanto siempre el menor número de dirección dentro del intervalo de la red y siempre tiene la porción de host codificada toda con ceros. Por razones administrativas, durante el desarrollo inicial del protocolo IP se formaron, de forma arbitraria, algunos grupos de direcciones como redes, y estas redes se agruparon en las llamadas clases. Estas clases proporcionan un cierto número de redes de tamaño estándar que pueden ser reservadas. Los intervalos reservados pueden verse en la tabla 2.4.

TABLA 2.4: CLASES DE DIRECCIONES IP

Clase de red	Máscara de red	Direcciones de red
Clase A	255.0.0.0	1.0.0.0 - 126.255.255.255
Clase B	255.255.0.0	128.0.0.0 - 191.255.255.255
Clase C	255.255.255.0	192.0.0.0 - 223.255.255.255
Multicast	240.0.0.0	224.0.0.0 - 239.255.255.255

El número de host que permite cada clase es:

Clase A

La porción de red está contenida en el primer octeto. Esta clase provee una porción de host de 24 bits, permitiendo alrededor de 16 millones de host por red. Esta clase fue diseñada para redes extremadamente grandes.

Clase B

El número de red está en los primeros dos octetos. Esta clase permite 16320 redes con 65024 host cada una. Esta red fue diseñada para redes de tamaño moderado a grandes.

Clase C

El número de red está contenido en los primeros tres octetos. Esta clase permite cerca de 2 millones de redes con 254 host cada una. Esta clase fue diseñada para permitir cientos de redes de tamaño pequeño.

En el ejemplo dado anteriormente, para la dirección IP 149.76.12.4, la dirección de luna, se refiere al host 12.4 de la red clase B 149.76.0.0. No todos los números se permiten en la porción del host. Los octetos 0 y 255 están reservados para usos especiales. Una dirección donde todos los bits de la porción del host son 0 se refiere a la red, y una dirección donde todos los bits de la parte del host son 1 se llama una dirección de difusión (broadcast).

La dirección de difusión es una dirección especial a la que escucha todas las máquinas en la red además de a la suya propia. Esta dirección es a la que se envían los datagramas si se supone que todas las máquinas de la red lo deben recibir. Ciertos tipos de datos, como la información de encaminamiento y los mensajes de aviso son transmitidos a la dirección de difusión para que cada host en la red pueda recibirlo simultáneamente.

TABLA 2.5: LA DIRECCIÓN DE RED Y DE DIFUSIÓN

Dirección IP	192.168.120.21
Máscara de red	255.255.255.0
Número de red	192.168.120.
Número de host	.21
Dirección de Red	192.168.120.0
Dirección de Difusión	192.168.120.255

Hay dos estándares usados comúnmente al respecto de la dirección de difusión. El más ampliamente aceptado es el de usar la dirección más alta posible en la red. En el ejemplo de la Tabla 2.5 la dirección de difusión es 192.168.120.255. Por alguna razón, otras estaciones han adoptado la convencido de usar las direcciones de red como direcciones de difusión. En la práctica no importa mucho cual se use, pero hay que asegurarse de que cada máquina en la red está configurada con la misma. Otras direcciones de red reservados para usos especiales son la 0.0.0.0 y 127.0.0.0. La primera es llamada ruta por defecto y la segunda es la dirección propia (loopback). La red 127.0.0.0 esta reservada para el tráfico IP local en el host propio. Usualmente la dirección 127.0.0.1 será asignada a una interfaz especial en el host, la interfaz propia, la cual actúa como un circuito cerrado. Cualquier paquete IP manejado por esta interfaz será regresado a ella misma tal como si fuese recibido desde alguna otra red. Esto permite desarrollar y probar el software de red aún si no se tiene una red "real". La red propia también permite usar software de red sobre un host aislado. Algunos intervalos de direcciones para cada clase se han dejado fuera y se han asignado para direcciones "privadas". Estas direcciones se han reservado para ser usadas en redes privadas y no son ruteadas hacia Internet. Estas son usadas por las empresas para construir sus propias intranets, pero se usan aún en redes muy pequeñas. Estas direcciones reservadas se presentan en la tabla 2.6.

TABLA 2.6: DIRECCIONES RESERVADAS PARA INTRANETS

Clase	Mascara de red	Dirección de red
A	255.0.0.0	10.0.0.0
B	255.255.0.0	172.16.0.0 - 172.31.0.0
C	255.255.255.0	192.168.0.0 - 192.168.255.0

De la tabla 2.6 se desprende que hay una red reservada clase A, 16 redes reservadas clase B y 256 redes reservadas clase C. Para instalar un nuevo host en una red IP

existente, se debe contactar con los administradores de la red y preguntarles por la siguiente información

- Dirección IP del host
- Dirección IP de la red
- Dirección IP de broadcast (difusión)
- Máscara de red IP
- Dirección del encaminador (router)
- Dirección del Servidor de Nombre de Dominio (DNS)

Se debería configurar entonces el dispositivo de red del host con esos detalles. No pueden inventarse y esperar que la configuración funcione. Para construir una nueva red propia que nunca conectará con Internet, esto es, si está construyendo a red privada y no tiene intención de conectar nunca esa red a Internet, entonces puede elegir las direcciones que quiera. De todas maneras, por razones de seguridad y consistencia, se deben de usar las direcciones reservadas presentadas en la tabla 2.6.

2.4. Subredes

Una subred es un medio para tomar una sola dirección de red IP y localmente particionarla de forma que esta sola dirección IP pueda ser usada realmente en varias redes locales interconectadas. Recuerde que un número de red IP solo puede usarse sobre una sola red. El termino localmente implica que para todo el mundo fuera de las máquinas y las redes físicas cubiertas por la red IP puesta como subred, nada ha cambiado (es solo una red IP), es decir, hacer una subred es una configuración local que es invisible al resto del mundo.

Las razones detrás de las subredes vienen de las primeras especificaciones de IP, donde solo unos pocos sitios estaban ejecutando números de red clase A. Una red clase A permite millones de host conectados. Si todas las computadoras IP en un sitio grande tuviesen que estar conectadas a la misma red, resultaría obviamente tanto en un tráfico enorme como un problema de administración: tratar de manejar tal bestia enorme podría ser una pesadilla y la red podría (casi con certeza) colapsar bajo la carga de su propio tráfico (se saturaría). Entrando a las subredes: la direcciones de la red IP clase A podrían dividirse para permitir su distribución a través de varias (si no es que muchas) redes separadas. También la administración de cada red separada puede delegarse fácilmente. Esto permite tener redes pequeñas, manejables, que puedan establecerse, quizás usando tecnologías de red diferentes. Hay que recordar que no se pueden mezclar

Ethernet, Token Ring, FDDI, ATM, etc., sobre la misma red física. Sin embargo, las diferentes tecnologías si pueden interconectarse. Otras razones para la realización de subredes son:

La distribución física del sitio puede crear restricciones (el largo de los cables, por ejemplo) en términos de cómo la infraestructura física puede conectarse, requiriendo múltiples redes. Las subredes permiten realizar esto en un ambiente IP usando un solo número de red IP. Esto es de hecho de realización muy común entre los Proveedores de Internet, los cuales tienen que dar conectividad permanente a clientes con redes locales con números IP estáticos.

El tráfico de red es lo suficientemente alto para causar caídas significantes. Partiendo la red usando subredes, el tráfico que es local en un segmento de red puede mantenerse local, reduciendo el tráfico total y acelerando la conectividad de la red sin requerir más ancho de banda. Los requerimientos de seguridad bien pueden dictar que diferentes clases de usuarios no compartan la misma red, ya que el tráfico sobre una red puede siempre ser interceptado por un usuario experimentado. Las subredes proveen una forma de mantener el departamento de mercadotecnia fuera del fisgoneo de tráfico de red del departamento de Investigación y Desarrollo (o a los estudiantes fuera del fisgoneo sobre la red de administración). Se cuenta con equipos que usan tecnologías de red incompatibles y que es necesario interconectar.

2.4.1. Como realizar una subred de un número de red IP

Una vez que se ha decidido poner subredes en el número de red que se tenga, ahora ¿cómo ha de realizarse esto? De forma general tienen que realizarse los siguientes pasos (que luego se explicarían en detalle): Poner la conectividad física (cables de red e interconexiones, tales como ruteadores). Decidir que tan grande/pequeña se necesita cada subred en términos del número de dispositivos que se conectarán a ellas, esto es, cuantos números IP útiles se requieren para cada segmento individual. Calcular la máscara de red y las direcciones de red apropiadas. Asignar a cada interfaz sobre la red su propia dirección IP y la máscara de red apropiada. Configurar las rutas sobre los ruteadores y las compuertas apropiadas, las rutas y/o rutas por defecto sobre los dispositivos de red. Probar el sistema y arreglar los problemas. Para propósitos de ejemplo, se considerará que se crearán subredes sobre un número de red clase C: 192.168.1.0. Esto provee hasta un máximo de 256 interfaces conectadas, más el número de red obligatorio (192.168.1.0) y la dirección de difusión (192.168.1.255).

2.4.2. Tamaño de la subred

Existe un compromiso entre el número de redes que se pueden crear y los números IP "perdidos". Cada red IP individual tiene dos direcciones que no pueden usarse como direcciones para una interfaz (ó host), el número de red IP en sí mismo y la dirección de difusión. Cada subred tiene estas dos direcciones que no pueden usarse: su propio número de red y dirección de difusión, además de direcciones válidas en el intervalo proveído por la red IP que se quiera dividir en subredes. De esta forma, haciendo subredes de una dirección IP en dos subredes separadas existen ahora dos direcciones de red y dos direcciones de difusión, incrementando las direcciones "perdidas"; crear cuatro subredes crea ocho direcciones que no pueden usarse; etc. De hecho, la subred útil más pequeña conste de solo cuatro números IP: Dos números IP para las interfaces, una para la interfaz del ruteador sobre esta red y otro para la interfaz del host sobre la red. Un número de red. Una dirección de difusión. Para qué se quería crear una red tan pequeña ya es otra pregunta. Con solamente un host sobre la red, cualquier comunicación en red debe ir hacia otra red. Sin embargo, este ejemplo sirve para mostrar las leyes de disminución que se aplican a las subredes. Por principio, solamente se puede dividir una número de red IP en 2n (donde n es menor en uno que el número de bits de la parte del host del número de red IP que se esté manejando) subredes de igual tamaño (sin embargo, se pueden hacer subredes de una subred ó combinar subredes). Para ser realistas sobre el diseño de una red propia, se requiere el número mínimo de redes locales separadas que sea consistente con las restricciones de administración, físicas, de equipo y seguridad.

2.4.3. Cálculo de la máscara de subred y los números de red

La máscara de red es la que realiza toda la magia local de dividir una red IP en varias subredes. La máscara de red para un número de red IP sin subredes es simplemente un número de red que tiene todos los bits de red puestos a '1' y todos los bits del host puestos a '0'. Para las tres clases de redes IP, las máscaras de red estándar son:

- Clase A (8 bits de red) : 255.0.0.0
- Clase B (16 bits de red) : 255.255.0.0
- Clase C (24 bits de red) : 255.255.255.0

La forma en que una subred opera es tomar prestado uno o más de los bits del host disponibles y hacer que las interfaces localmente interpreten estos bits prestados como parte de los bits de red. De manera que para dividir un número de red en dos subredes, podríamos tomar prestado un bit del host poniendo a uno el bit apropiado en la máscara de red del primer bit del host. Para una red clase C, resultaría una máscara de red de

11111111.11111111.11111111.10000000, ó 255.255.255.128. Para la red de clase C, por ejemplo, 192.168.1.0, estas son algunas de las opciones que tenemos para realizar subredes, ver tabla 2.7:

TABLA 2.7 POSIBLES SUBREDES PARA UNA RED CLASE C CON IP 192.168.1.0

Redes	Host/red	Mascara de red
2	126	255.255.255.128 ff.ff.ff.10000000
4	62	255.255.255.192 ff.ff.ff.11000000
8	30	255.255.255.224 ff.ff.ff.11100000
16	14	255.255.255.240 ff.ff.ff.11110000
32	6	255.255.255.248 ff.ff.ff.11111000
64	2	255.255.255.252 ff.ff.ff.11111100

En principio, no hay ninguna razón para seguir el camino explicado para realizar la subred, donde los bits de las máscaras de red son adicionados en el bit del host más significante hacia el bit del host menos significante. Sin embargo, si no se realiza de esta manera, los números IP resultantes seguirán una secuencia bastante extraña.

TABLA 2.8: DIRECCIONES DE RED Y DE DIFUSIÓN DEFINIDAS, LA MASCARA DE RED APROPIADA

Mascara	Subredes	Red	Difusión	Min IP	Max IP	Host	Host totales
128	2	0 128	127 255	1 129	126 254	126 126	252
192	4	0 64 128 192	63 127 191 255	1 65 129 193	62 126 190 254	62 62 62 62	248
224	8	0 32 64 96 128 160 192 224	31 63 95 127 159 191 223 255	1 33 65 97 129 161 193 255	30 62 94 126 158 190 222 254	30 30 30 30 30 30 30 30	240

Esto lo hace extremadamente difícil, para nosotros los humanos, decidir cual subred pertenece un número IP, ya que nosotros no somos tan buenos para pensar en binario (las computadoras, por otro lado, se manejan igual de bien en cualquier esquema). Una

vez que se ha decidido por la máscara de red apropiada, se tienen que resolver las direcciones de red y de difusión, y el intervalo de números para cada una de las redes.

Considerando solamente un número de red clase C, y listando solo la parte final (la porción de host) se tiene, ver la tabla 2.8:

Como puede verse, existe una secuencia muy definida de estos números, lo cual los hace muy fáciles de chequear. La desventaja de las subredes también puede verse, ya que se reduce el número total de direcciones de host disponibles al mismo tiempo que se incrementa el número de subredes. Con toda esta información, ya se está en la posición de asignar números de host, números de redes IP y máscaras de red.

Resumen cap. II

En este capitulo analiza los beneficios de utilizar el protocolo TCP/IP en las redes, especificando las características de los números IP para IPv4, así como el procedimiento para realizar una subred, regular su tamaño y asignar los números de red.

CAPÍTULO III
FUENTES DE INFORMACIÓN INDESEADA Y TIPOS HABITUALES DE ATAQUE

3.1. Virus

Un virus de computadora es un programa que se replica a sí mismo, contiene código que explícitamente hace copias de sí mismo y que puede "infectar" otros programas modificándolos o cambiando su ambiente de forma que una llamada a un programa infectado implica una llamada a una posible copia evolucionada del virus. En la figura 3.1 se representa esquemáticamente un virus.

FIG.3.1: VIRUS DE COMPUTADORA, PROGRAMA QUE SE REPLICA A SI MISMO

3.1.1 Historia de los virus

El primer virus fue creado como parte de una tesis doctoral de un ingeniero electrónico. Luego una competencia de estudiantes cuyo objetivo fue crear un programa que consumiera la memoria del computador para convertirse en el ganador, también crearon nuevos programas del tipo virus. En la década de los 80' y hasta mediados de los 90' los virus se propagaban por medio de los disquetes, ya que era la forma de intercambiar información. Los virus de arranque como el Michelangelo, que apareció en Asia en 1991, infectaban las computadoras mediante la lectura de un disquete infectado. El Michelangelo tardó 2 años en llegar a América.

En la actualidad Internet se ha convertido en la autopista de la información y en el principal medio de propagación de la nueva generación de virus. En 1999 en virus Melissa provocó pérdidas por más de 80 millones de dólares y en el 2000 el famoso virus I Love You, afectó a miles de computadoras en todo el mundo, provocando pérdidas por

más de 15 mil millones de dólares. su difusión fue masiva gracias a Internet y el correo electrónico. En el 2001, el virus Kournikova tardó sólo dos horas para dar la vuelta al mundo por medio del correo electrónico.

Con el auge de Internet los virus tienden a propagarse a velocidades increíbles, siendo el correo electrónico la forma más utilizada para propagar virus. Miles de archivos infectados con virus viajan a través de Internet en todo momento, principalmente por e-mails dentro de los archivos adjuntos o anexados (attached). Mientras que para un usuario de Pc doméstico, una infección puede causarle desde un dolor de cabeza hasta perder la información de su Pc; para las grandes empresas y organismos estatales, el ataque de un virus puede causar pérdidas millonarias.

3.1.2. Clasificación de los virus

Aunque en la actualidad casi todos los virus tienen comportamientos complejos e incorporan características de varias clases, se podrían diferenciar los siguientes tipos de virus:

Troyanos: su nombre viene de la mitología griega, del Caballo de Troya, ver figura 3.2, ya que el virus viene enmascarado como un archivo aparentemente inofensivo. Es un programa potencialmente peligroso que se oculta dentro de otro para evitar ser detectado, e instalarse de forma permanente en nuestro sistema.

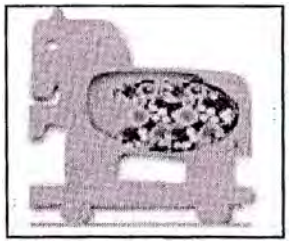

FIG. 3.2: TROYANO, VIRUS ENMASCARADO

Este tipo de software no suele realizar acciones destructivas por sí mismo, pero entre muchas otras funciones, tienen la capacidad de capturar datos, generalmente contraseñas e información privada, enviándolos a otro sitio. Otra de sus funciones es dejar indefenso nuestro sistema, abriendo brechas en la seguridad, de esta forma se puede tomar el control total de forma remota, ver figura 3.3, como si realmente se estuviera trabajando delante de nuestra pantalla.

FIG. 3.3: SE PUEDE TOMAR EL CONTROL TOTAL DE FORMA REMOTA

Virus de arranque o booteo: no afectan archivos sino que atacan el sector de arranque de los diskettes y el disco duro. Como el trágicamente famoso virus Michelangelo.

Bombas lógicas: permanecen inactivas hasta que se cumple un condición especial, que puede ser una combinación de teclas o una fecha específica.

Virus de sistema: afectan en primer lugar el archivo intérprete de comandos COMMAND.COM y posteriormente a otras áreas vitales del sistema como son el Sector de Boot o el Master Boot Record (MBR), otros archivos ejecutables de extensión .COM

Virus de archivos ejecutables: infectan los archivos de programas con extensión COM. y EXE. También llamados virus parásitos, porque se adosan a los archivos ejecutables y son los más habituales. Estos virus al ejecutarse se instalan en memoria y esperan a que el usuario ejecute otro programa utilizando un evento como un activador para infectar dicho programa.

Virus de archivos de datos: éstos virus a infectan los archivos de datos de diferentes extensiones. De acción menos notable ya que dañan los archivos que creamos con las aplicaciones, usando como medio el programa creador del mismo.

Virus de macros o macrovirus: creados con el lenguaje de programación que incluyen algunas utilidades como procesadores de texto o planillas de cálculo para ayudar a los usuarios a automatizar ciertas tareas, creando pequeños programas llamados macros. Un virus de macro es simplemente una macro para uno de estos programas con un código dañino. Cuando un documento o plantilla que contiene la macro infectada se abre en la aplicación de destino, el virus se ejecuta y causa el daño correspondiente. Además, está programado para copiarse a otros documentos, de modo que el uso continuo del programa da como resultado la distribución continua del virus. Backdoors: al instalarse en

el sistema inician un programa de tipo servidor que permite el acceso en forma remota por parte de terceros.

Gusanos (Worms): un *gusano* de computadora es un programa auto contenido (o puede ser un conjunto de programas), que es capaz de diseminar copias funcionales de él mismo o de sus segmentos a otros sistemas de computadoras (generalmente vía conexiones de red). Al contrario de un virus, un gusano no necesitan estar hospedado en algún programa. En la figura 3.4 se tiene una representación de un gusano. Existen dos clases de gusanos: gusanos de host y gusanos de red.

FIG. 3.4: GUSANO NO NECESITA ESTAR HOSPEDADO EN UN ARCHIVO

Los *gusanos de host* estén enteramente contenidos en la computadora donde se están ejecutando y usan únicamente la red para copiarse a otras computadoras. Los *gusanos de red* consisten de muchas partes (que se llaman *segmentos*), cada una ejecutándose en máquinas diferentes (y posiblemente realizando acciones diferentes) y estas partes usan la red para propósitos de comunicación. La propagación de un segmento de una máquina a otra es solamente uno de esos propósitos.

3.2 Spam

Es el correo electrónico no solicitado o no deseado, que se envía a múltiples usuarios con el propósito de hacer promociones comerciales o proponer ideas, ver figura 3.5. Generalmente, suelen ser: publicidad, ofertas o enlaces directos una página web. Estos mensajes son enviados a cientos de miles de destinatarios cada vez. El correo basura es molesto y roba recursos del sistema. Su distribución causa la perdida de ancho de banda en la Red, y multiplica el riesgo de infección por virus. Las personas o empresas que envían este tipo de emails, construyen sus listas usando varias fuentes. Normalmente, utilizan programas que recogen direcciones de correo desde Usenet, o recopilan las mismas de otras listas de distribución.

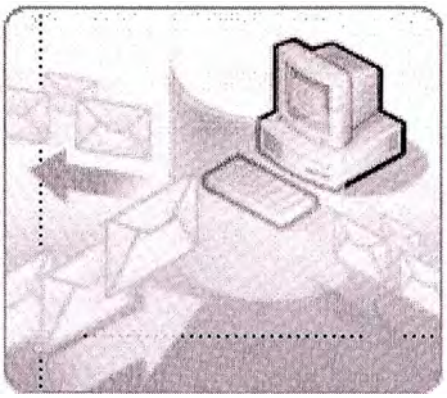

FIG. 3.5: CORREO ELECTRÓNICO NO DESEADO

Muchos de los mensajes no solicitados nos ofrecen la opción de eliminarnos. La experiencia demuestra que este método es una trampa, y que sólo sirve para verificar que la dirección de correo existe realmente, y se encuentra activa. Por otro lado, si respondemos alguno de estos emails, el resultado es idéntico, seremos colocados automáticamente en una nueva lista de distribución, confirmando nuestra dirección

3.3 Spyware

Los programas espía, ver figura 3.6, se instala en un ordenador sin el conocimiento del usuario, para recopilar información del mismo o de su ordenador, enviándola posteriormente al que controla dicha aplicación. Existen dos categorías de spyware: software de vigilancia y software publicitario. El primero se encarga de monitorizar todo el sistema mediante el uso de transcriptores de teclado, captura de pantallas y troyanos. Mientras, el segundo, también llamado "Adware", se instala de forma conjunta con otra aplicación o mediante controles ActiveX, para recoger información privada y mostrar anuncios.

FIG. 3.6: RECOPILA INFORMACIÓN Y LA REENVÍA

Este tipo de programas registran información sobre el usuario, incluyendo, contraseñas, direcciones de correo, historial de navegación por Internet, hábitos de compra, configuración de hardware y software, nombre, edad, sexo y otros datos secretos. Al igual

que el correo basura, el software publicitario, usa los recursos de nuestro sistema, haciendo que sea este el que pague el coste asociado de su funcionamiento. Además, utiliza el ancho de banda, tanto para enviar la información recopilada, como para descargar los banners publicitarios que nos mostrará.

Los mayores responsables de la difusión de spyware son los populares programas de intercambio de archivos (P2P) disponibles en la actualidad, tipo Kazaa, eDonkey o eMule.

3.4 Tipos habituales de ataque

¿Cómo obtienen los atacantes acceso no autorizado a los sistema? Las motivaciones para esos ataques son numerosas pudiendo variar desde un inofensivo "podré acceder a este sistema" hasta razones explícitamente maliciosas como realizar espionaje industrial, utilizar los sistemas comprometidos para atacar otros sistemas e incluso simplemente por perturbar y dañar sistemas.

Existen, literalmente, docenas de diferentes formas de que un intruso consiga tener acceso a un sistema. A continuación se proporciona un breve listado de los ataques más comunes:

- Ingeniería social. Un atacante engaña al administrador o a otro usuario autorizado de un sistema para que comparta sus credenciales de conexión o detalles de la operación del sistema.

- Errores de software. Un atacante explota un defecto de programación y obliga a una aplicación o servicio a ejecutar comandos no autorizados o no esperados. Estos ataques son incluso más peligrosos cuando el programa se ejecuta con privilegios adicionales o administrativos. A errores normalmente se hace referencia como ataques de desbordamiento del búfer o vulnerabilidades de la cadena de formato.

- Virus y código troyano. Un ataque engaña a un usuario legitimo al ejecutar un programa. La forma más común de este tipo de ataque es disfrazar el programa con el aspecto inocente de un correo electrónico o dentro de un virus. Una vez ejecutado, el programa puede hacer varias cosas, incluida la instalación de programas de puerta trasera, robando archivos y credenciales, o incluso borrándolos.

- Configuración pobre de sistema. Un atacante es capaz de explotar los errores de configuración de un sistema en los servicios y cuentas que estén disponibles. Entre los errores comunes tenemos el de no cambiar las contraseñas de las cuentas predeterminadas (tanto en cuanto a sistema como en cuanto a aplicaciones), el de no restringir el acceso a los programas de administración de aplicaciones, o el de no deshabilitar servicios innecesarios o que no se utilizan.

Además de intentar obtener acceso no autorizado a los sistemas, las personas maliciosas pueden intentar simplemente modificar los sistemas. En el caso de aplicaciones críticas y muy visibles, el coste para la empresa podría ser muy importante. A estos ataques se hace referencia como ataques de denegación de servicio (DoS, *Denial of Service*). Un ataque DoS es un ataque en el que un usuario, una red o una organización son privados de un recurso o servicio que normalmente tendrían. La pérdida de un servicio esta asociada normalmente a la incapacidad de un servicio de red individual para estar disponible, como el correo electrónico o el Web, o la pérdida temporal de conectividad o los servicios de red.

Resumen cap. III

En este capitulo se hace un revisión de las fuentes de información indeseada, se analiza a los virus, orígenes de los virus y clasificación, se hace un análisis del spam, los spyware y se resume los tipos habituales de ataques.

CAPÍTULO IV
MECANISMOS DE CONTROL

4.1 El CERT

En 1985, la Universidad de Carnegie Mellon, en los E.E.U.U., ganó una licitación para establecer el *CERT Coordination Center* [11] con el apoyo monetario del Departamento de Defensa de los E.E.U.U. El CERT/CC es un centro para reportar todos los problemas de seguridad en Internet. Su personal provee recomendaciones y respuestas coordinadas a compromisos de seguridad, identifica intento de actividad de intrusión, trabaja con otros expertos en seguridad para identificar soluciones a problemas de seguridad y disemina información hacia toda la comunidad. El CERT/CC también analiza vulnerabilidades en productos, publica documentos técnicos y presenta cursos de entrenamiento. El CERT/CC está dentro de Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon, en Pittsburgh, E.E.U.U. El CERT/CC publica que un sitio ideal en seguridad debe contar con:

1. Estar al día en parches
2. Usar firewall
3. Usar Proxy
4. Debe monitorearse la red.
5. Deben deshabilitarse los servicios y características que no son necesarios
6. Tener un software de antivirus instalado, configurado y actualizado.
7. Una política para la realización de respaldos.
8. Un equipo entrenado y con capacidad de respuesta a incidentes.

La seguridad de un sistema en red es un tema extenso. Este informe revisará con cierto detalle estos siete puntos para luego profundizar el relacionado con firewall y proxy. Los puntos 2, 3 4 y 5 pueden considerarse de vital importancia en una red que cuenta con uno o varios servidores y que está conectada a Internet. Típicamente los compromisos de seguridad provienen de Internet, donde alguna persona, muy preparada y con muchos conocimientos, podría ingresar sin permiso a nuestras computadoras. Si nuestra red no está conectada a Internet, entonces no deberíamos angustiarnos por estos puntos,

aunque sí preocuparnos si nuestros usuarios están muy preparados y podrían instalar programas que pueden comprometer la seguridad de la red. Así que además de los sistemas aquí presentados es necesario contar con un equipo de trabajo dedicado a la seguridad de la red. Y nuestra experiencia es que se puede pensar en tener una red segura si se tiene un equipo de trabajo que lleve a cabo las ideas de seguridad. Aquí se van a desarrollar los puntos siguientes:

4.2. Parches actualizados

Todo el software de un centro de cómputo conectado en red necesita estar actualizado en parches. Un parche es una parte corregida del código de un programa. En el mundo de los sistemas Windows y Mac generalmente se presentan los parches como un nuevo código ejecutable. Un parche corrige un problema o un fallo de seguridad del programa que se trate. Es muy importante bajar los parches de sitios de Internet que sean confiables, ya que podríamos instalar un programa que transmita un virus un gusano y comprometa la seguridad de toda nuestra red.

4.3. Antivirus

El antivirus es un programa que debe tenerse con las licencias actualizadas para garantizar tener las últimas versiones del mismo, ver figura 4.1. Todos nuestros sistemas Windows y Mac debiesen de tener el programa antivirus instalado, configurado y actualizado.

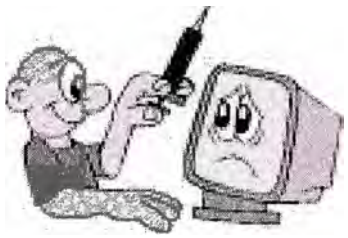

FIG. 4.1: ES NECESARIO TENER UN ANTIVIRUS INSTALADO

4.4. Respaldos

Uno de los métodos infalibles para luchar contra agujeros de seguridad, fallas de los sistemas, desastres físicos, virus, etc., es realizar respaldos (backups). Generalmente se deben de respaldar la información que es crucial para el sistema, como las bases de datos y los archivos de los usuarios. No es necesario guardar la información de sistema operativo ya que debemos de disponer de un medio (CDROM) para su reinstalación. Los dispositivos de almacenamiento que tenemos disponibles son:

1. Discos duros
2. Discos compactos
3. Discos de video digital (DVDs)
4. Cintas magnéticas

Los primeros se convierten en una opción dado al abaratamiento y la gran capacidad de los discos duros actuales. Se puede realizar un "espejeo" de disco o una técnica que se conoce como RAID [12]. RAID es el acrónico en inglés de *Redundant Arrays of Inexpensive Disks* (ó Arreglo Redundante de Discos Baratos). La idea básica de RAID es combinar múltiples discos, independientes y pequeños, en un arreglo de discos en el cual su rendimiento excede de un solo disco grande y caro. De forma adicional este arreglo de discos es visto por la computadora como un solo disco lógico. La técnica RAID incluye también una tolerancia a fallos por medio del almacenamiento de información redundante en los discos. Los discos compactos pueden ser una opción, la limitante son los 740MB de información que puede almacenarse en un CD. Claramente la opción con los DVD (que pueden almacenar hasta 4.7GB de información), que si disminuyen su precio pueden ser una clara opción para almacenar datos en ellos. La clásica opción que se tiene son las cintas magnéticas, que almacenas gigas y gigas de bytes en ellos, aunque su desventaja es que pueden ser muy lentas y su ventaja es que dan la mejor razón de precio/megabyte de información almacenada.

4.5. Personal entrenado y con capacidad de respuesta a incidentes

Algunos empresarios o responsables de entidades públicas consideran al mantenimiento y a la seguridad de una red, como actividades secundarias. Ejemplo de ello es que piensen que cualquier persona puede hacerse cargo del mantenimiento y la seguridad. O más aún, que cambien entre distinto personal, ya sea calificado o no, para la realización de estas dos importantes actividades. Hay que tomar en cuenta que quien da vida a una red es tanto sus usuarios, como el administrador (o administradores) de la red. El material humano es lo más importante para la buena realización de cualquier actividad. Para la administración y seguridad de una red es indispensable contar con personal entrenado y capaz para llevar a cabo y controlar las políticas de seguridad.

4.6. Firewall

La función básica de un firewall consiste en examinar las comunicaciones de red con el propósito de evitar el acceso no autorizado a una red de equipos. Los firewall ser de varias formas y tamaños, y, a veces, el firewall es en realidad un conjunto de varios

dispositivos. Se considerara que un firewall es el equipo, o equipos, que se encuentran entre redes de confianza (como redes internas) y redes que no son de confianza (como Internet), que inspeccionan todo el tráfico que fluye entre ellas, ver figura 4.2.

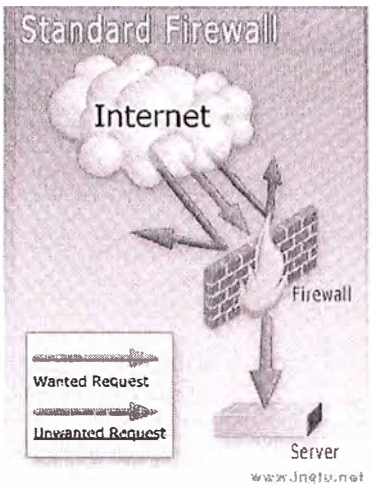

FIG. 4.2: EL FIREWALL EXAMINA LAS COMUNICACIONES DE RED

4.7. Proxy

Un proxy es un "Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red". Su importancia es la misma que la del caché de cualquier navegador cliente de Internet, realizando una consulta primero en el proxy (que es lo que 'tiene' más cerca), para en caso de no encontrarlo, realizar la búsqueda en Internet.

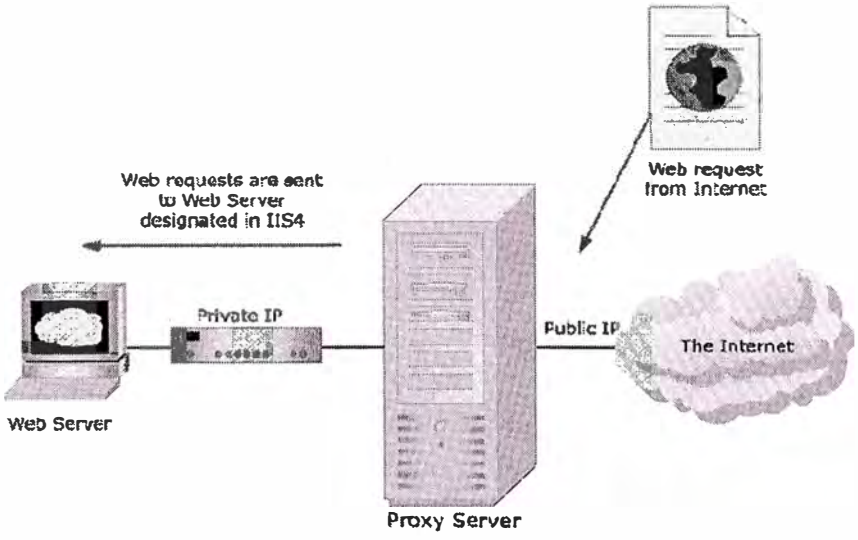

FIG. 4.3: CENTRALIZA EL TRÁFICO ENTRE INTERNET Y UNA RED PRIVADA

La acepción habitual es la de servidor proxy, que no es otra cosa que un ordenador que se encuentra instalado entre el equipo del usuario e Internet, ver figura 4.3. De esta forma se encarga de gestionar las peticiones que se realizan a la red, administrando el tráfico hacia fuera y permitiendo una mayor velocidad de acceso. Su característica principal es de tener una enorme memoria caché, en donde guarda un histórico de la información que ha sido solicitada por los usuarios.

Resumen cap. VI

En este capitulo se analiza las precauciones que se deben tener en cuenta para mejorar la seguridad de una red frente a su conexión hacia Internet. Se hace una descripción de la función de un firewall y u proxy en la red.

CAPÍTULO V
SEGURIDAD EN LA RED

5.1. Firewall

Un firewall es una combinación de hardware y software usado para realizar una política de seguridad y controlar el tráfico entre dos o más redes, algunas de las cuales pueden estar bajo control (nuestra red por ejemplo) o fuera de control (Internet por ejemplo). Un firewall de red comúnmente sirve como una primera línea de defensa contra tratamientos dañinos externos a los sistemas de cómputo propios, redes e información crítica. Los firewall pueden usarse también para particionar las redes internas, reduciendo el riesgo de ataques dentro de la red. El término de firewall se tomó de la analogía estructural cuyo propósito es hacer más lento el avance del fuego en un edificio. El término firewall se usará como un nombre, cuyo significado general es el concepto de un mecanismo tecnológico para el reforzamiento de la política de seguridad de una red. Los sistemas conectados a Internet son vulnerables a los intentos de acceso no autorizado por parte de usuarios ajenos. Esta práctica suele consistir en intentar introducirse en el sistema, o bien en interceptar información de usuarios remotos conectados al sistema en cuestión, así como modificar información, negar el servicio y abusar de este. El firewall es una forma de protección contra dichos ataques. Para construir un firewall primero necesitamos entender como se construyen *listas de acceso*, que serán explicadas a continuación. Para completar un firewall se necesita además levantar una *puerta*, así una puerta más listas de acceso nos resulta en un firewall.

Los firewall tienen los siguientes atributos:

- Todas las comunicaciones pasan a través de ellos.
- Solo se permiten el tráfico autorizado.
- Pueden resistir los ataques.

Dicho de una forma más simple, un firewall actúa como el búfer entre una red de confianza y una red que no lo es.

Un firewall puede ser un enrutador, un equipo personal, un host o un conjunto de host configurados específicamente para proteger una red privada frente a protocolos y servicios de los host que se encuentran fuera de la red de confianza. Normalmente, un sistema de firewall esta ubicado en el perímetro de una red, como, por ejemplo, la conexión a un sitio a Internet. Sin embargo los sistemas firewall pueden, y deberían, estar ubicados dentro del perímetro de la red para proporcionar protección adicional y más específica a un conjunto más pequeños de host.

La forma en que un firewall protege la red de confianza depende del propio firewall y de las directivas o reglas que se apliquen al mismo. A continuación se exponen las cuatro categorías principales de la tecnología de firewalls que actualmente están disponibles:

- Filtros de paquetes.
- Puertas de enlace a aplicaciones.
- Puertas de enlace entre circuitos.
- Motores de inspección de paquetes con estado.

Al igual que con todas las soluciones tecnológicas, la tecnología de los firewalls esta sujeta al avance y los ciclos de vida normales que los productos y las tecnologías sufren.

5.2. ¿Por qué utilizar un firewall?

La primera pregunta que la gente puede hacerse es ¿por qué utilizar un firewall? ¿Por qué no configurar simplemente sistemas individuales que hagan frente a los ataques? La respuesta más simple es que el firewall esta dedicado a una única cosa: decidir que comunicaciones son autorizadas y cuales no. Esto evita la necesidad de tener que comprometer la seguridad, el uso y la funcionalidad.

Sin un firewall, los sistemas se quedan solos con sus propios dispositivos y configuración de seguridad. El estos sistemas pueden estar ejecutando servicios que aumentan la funcionalidad o facilitan la administración, pero no son demasiado seguros y no son de confianza, o solo deberían ser accesibles desde ubicaciones especificas. Lo firewalls se utilizan para implementar este nivel de control de acceso.

Si un entorno carece de un firewall, la seguridad se basa enteramente en el host. La seguridad será tan fuerte como el host más débil. Cuanto más grande sea la red, más complejo es mantener todos los host al mismo nivel de seguridad. Dado que siempre existen descuidos (como simplemente aplicar un parche de seguridad indispensable a 14 de los 15 servidores de Web) las intromisiones ocurren debido a errores simples en la configuración y parches de seguridad inadecuados.

El firewall es el único punto de contacto con las redes que no son de confianza. Por tanto, en vez de asegurarse de que varias son lo más seguras posible, el administrador se puede centrar en el firewall. Esto no significa que los sistemas que están disponibles mediante el firewall no tengan que ser los mas seguro posible; simplemente proporcionan un nivel de protección frente a un error.

Los firewalls son unos auditores excelentes. Como todo el tráfico pasa a través de ellos, la información que contienen sus registros se puede utilizar para reconstruir eventos en caso de una violación de la seguridad.

En general los firewalls mitigan el riesgo de que los sistemas sean utilizados para propósitos no autorizados o indeseados (por ejemplo, ser atacados). ¿Cuáles son exactamente los riesgos de estos sistemas frente a los que los firewalls los defienden? Los sistemas y datos corporativos tienen tres atributos principales que un firewall protege:

- Riesgo de la confidencialidad

  Que una persona no autorizada tenga acceso a datos importantes o que se revelen de forma prematura. Una empresa podría perder fácilmente millones de dólares si el plan de su negocio, los secretos comerciales de su empresa o la información financiera, se viera expuesta.

- Riesgo de la integridad de datos

  El de una modificación no autorizada de los datos, como, por ejemplo, información financiera, especificaciones de los productos o el precio de los artículos en una pagina Web. Las empresas crecen y prosperan según la exactitud de la información que generan sus sistemas. ¿Cómo se pueden tomar las mejores decisiones si la información del sistema no es de confianza? (¿Cuáles son los niveles de ventas? ¿Qué cuentas por cobrar son exactas?).

- Riesgo de disponibilidad

  La disponibilidad de los sistemas asegura que estos sean lo suficientemente fuertes y que estén disponibles para los usuarios en el momento oportuno (es decir, cuando los usuarios necesiten). Los sistemas no disponibles cuestan a las empresas muchos dólares en pérdida de ingresos y productividad de los empleados, así como en formas intangibles, mediante la perdida de confianza de los consumidores y la publicidad negativa.

5.3. Ubicación del firewall

Los firewall pueden, y deben, instalarse en cualquier punto donde se interconecten dos redes con diferentes requisitos de seguridad, ver figura 5.1. El uso más común de un firewall es entre la conexión a Internet y la red de área local.

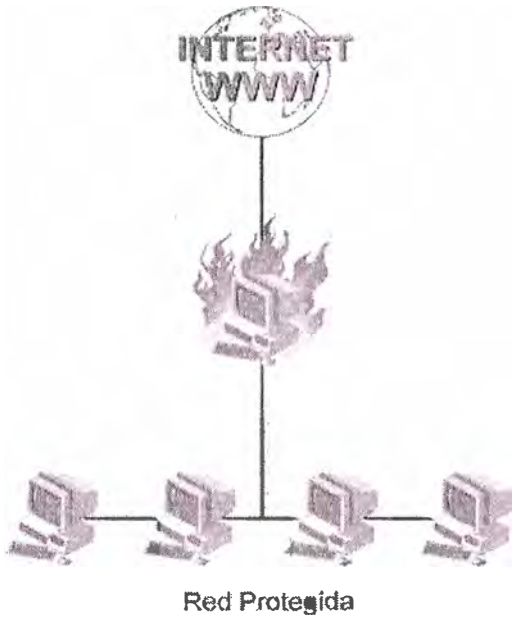

FIG. 5.1: EL USO MÁS COMÚN DE UN FIREWALL ES ENTRE LA CONEXIÓN A INTERNET Y LA RED DE ÁREA LOCAL

Otros usos comunes de los firewall son la protección de conexiones frente a terceras personas externas, como por ejemplo, los proveedores de datos del mercado, y entre áreas sensibles de una red interna.

Al hablar acerca de redes se utilizara el concepto *perímetro de red*, que es toda la frontera de la red de área local. Los puntos de entrada y salida se forman cuando la red de área local se conecta a otra red, como, por ejemplo, Internet.

Estos puntos de conexión casi siempre disponen de un firewall.

En apariencia, definir el perímetro de red parece simple. Sin embargo, con la llegada de las redes privadas virtuales, el perímetro real se convierte en algo borroso. Las tecnologías de la red privada virtual permiten a los usuarios remotos conectarse a través de un firewall como si estuvieran en la red local. Se han convertido en extensiones de la red corporativa, pero incluso los host están fuera de la protección que ofrece el firewall corporativo. Los administradores deberían pensar en instalar firewall personales locales en estos host para obtener un nivel de seguridad uniforme en el perímetro.

5.4. Puntos fuertes y débiles de un firewall

Un firewall solo es una parte de una arquitectura de seguridad general. Sin embargo, como pieza individual de la arquitectura, está diseñado para cumplir un requisito muy importante dentro del diseño general. Como todo, los firewall tienen puntos fuertes y puntos débiles.

5.4.1. Puntos fuertes

Los puntos fuertes de los firewalls son:

- Los firewall son excelentes para reforzar la política de seguridad de una empresa. Deberían configurarse para restringir la comunicación a lo que los administradores han determinado como aceptable.

- Los firewall se utilizan para restringir el acceso a servicios específicos. Por ejemplo, el firewall permite el acceso público a un servidor Web pero evita el acceso al Telnet y otros programas demonios no públicos. La mayoría de los firewall pueden incluso proporcionar acceso selectivo mediante las funciones de autenticación.

- Los firewalls solo tienen un propósito. Por tanto, no hay que comprometer ni la seguridad ni el uso.

- Los firewalls son excelentes auditores. Dada una gran cantidad de espacio de disco o capacidades de conexión remotas, un firewall puede registrar parte o todo el tráfico que pasa a través de él.

- Los firewalls son excelentes para alertar a las personas apropiadas acerca de los sucesos que se producen.

5.4.2. Puntos débiles

Los puntos débiles comunes a los firewalls son:

- Los firewalls no ofrecen protección ante lo que esta autorizado. Se estará preguntando que significa esto. Los firewalls protegen las aplicaciones y protegen el tráfico normal de comunicaciones hacia dichas aplicaciones; si no, ¿para que sirve? Si las propias aplicaciones tienen defectos, un firewall no detendrá el ataque dado que para el firewall la comunicación está autorizada.

- Los firewalls son tan eficaces como las reglas que tienen que aplicar de acuerdo con su configuración. Un conjunto de reglas demasiado permisivo disminuiría la efectividad del firewall.

- El firewall no puede detener la ingeniería social o a un usuario autorizado que utilice su acceso con propósitos maliciosos.

- Los firewalls no pueden solucionar las prácticas administrativas débiles o un diseño inadecuado de una directiva de seguridad.

- Los firewalls no pueden detener ataques si el tráfico no pasa a través de ellos.

5.5. Filtrado de paquetes

Cada servicio que provee un servidor, por ejemplo DNS, WEB, correo electrónico, acceso a través de SSH, etc., se identifica por un *número de puerto*. Así, el DNS va sobre el puerto 53, el WEB en el puerto 80, el correo electrónico sobre el 25 y un servidor de SSH va sobre el puerto 22. Todos los servicios abajo del puerto 1024 se consideran privilegiados y son usados por los principales servicios disponibles en Internet. Puertos arriba del 1024 se consideran no privilegiados y pueden usarse para realizar servicios propios. Los números de puertos asignados a los servicios, son de uso estándar; aunque cualquier administrador de red podría asignar otros números de puerto a sus servicios (y sus usuarios deberían de conocer esos números de puertos para poder usar los servicios en puertos no estándar). Además de los números de puerto, cada servicio va sobre los protocolos TCP y/o UDP. Aquí recordemos que los que se conoce como "TCP/IP" en realidad son un conjunto de protocolos, el básico es IP y sobre de el están TCP, UDP y ICMP. ICMP es el protocolo multicapa que fue diseñado para facilitar el control, prueba y funciones de manejo dentro de una red IP. Las aplicaciones de Internet están sobre los protocolos TCP y UDP. TCP es el protocolo altamente confiable y UDP es simple. TCP es complejo, UDP eficiente y mejor para entregar datagramas. UDP se dice que no es confiable porque no posee ninguno de los mecanismos de confiabilidad de TCP, este da acuse de recibo por cada datagrama recibido, resecuencia los datagramas recibidos si están fuera de orden y requisa retransmisiones para un paquete recibido que éste dañado. En otras palabras, no se garantiza que un datagrama de UDP alcance intacto su destino. Para transmitir un paquete de datos, se agregan unos identificadores al inicio del paquete; estos identificadores conforman un *encabezado*. Juntos el encabezado y los datos forman un *datagrama*. El datagrama de IP, en su encabezado, lleva la dirección IP

de la fuente y el destino del paquete. El datagrama de TCP, ó de UDP, llevan además el número de puerto del servicio, tanto del puerto fuente como puerto destino. Se le llama *regla* a una línea de texto que describe como se bloquean ciertas direcciones IP y/o servicios. Un conjunto de reglas forman una *lista de acceso*.

5.6. Usos del firewall

Como se ve en la Figura 5.2, un firewall se puede usar para proteger una red local. Todas las máquinas, o servidores, dentro de esta red forman una *zona desmilitarizada* (ZDM). Este firewall puede no tener asignada un número IP, entonces se le conocería como *firewall transparente* dado que no es necesario que se conozca su dirección IP desde Internet.

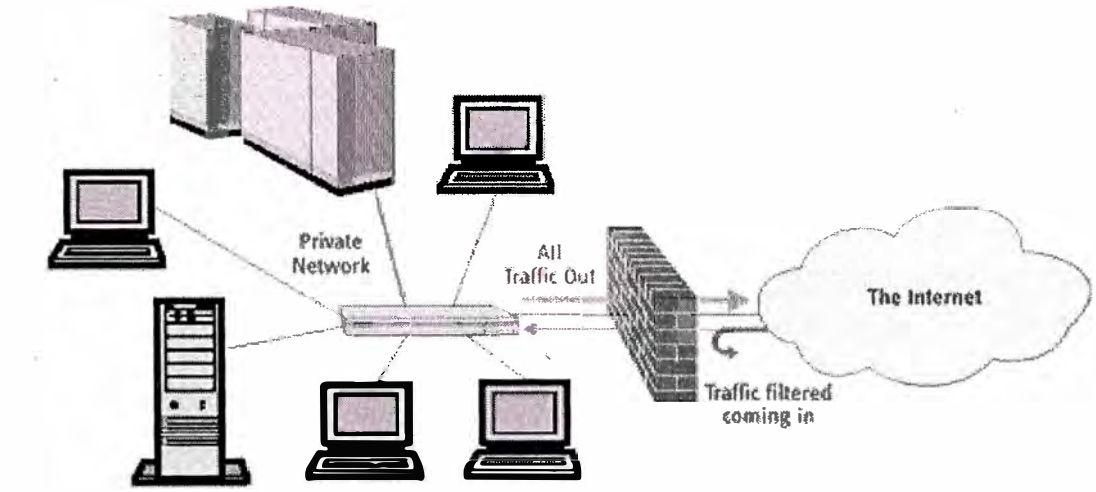

FIG. 5.2: UN FIREWALL USADO PARA PROTEGER UNA RED

Para administrar remotamente un firewall transparente es necesario construir una red alternativa, ya que no se puede accesar en la propia debido a que no tiene dirección IP. Para ello hay que poner otra tarjeta de red en el firewall y en la máquina desde donde se administraría remotamente (esto sería crear otra red, la red más simple, como ya sabemos). Otro uso de un firewall es el de dividir una red local, creando una red interna con dirección IP no válidas. Todas las máquinas dentro de esta red se lo conocen como *zona militarizada* (ZM). Las máquinas dentro de la zona militarizada pueden acceder a Internet pero ninguna máquina en Internet puede alcanzarlas. Eso hace que los servidores de la red local deban estar dentro de la zona desmilitarizada. El esquema de esta red puede verse en la Figura 5.3.

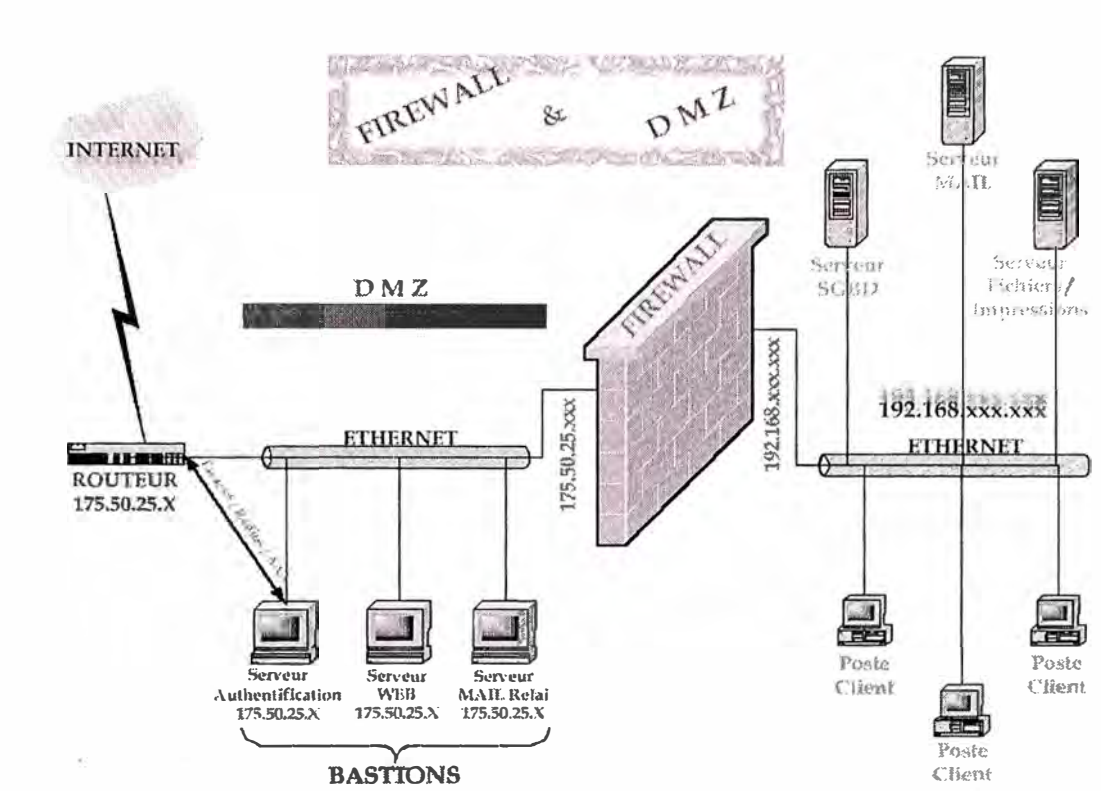

FIG. 5.3: USOS DE UN FIREWALL. LOS SERVIDORES DENTRO DE LA RED DMZ TIENEN DIRECCIONES IP VÁLIDAS Y LOS CLIENTES EN LA ZM TIENEN IP INVÁLIDAS.

El tener los clientes dentro de una ZM, como se muestra en la Fig. 5.3, con direcciones IP inválidas, presentan las siguientes ventajas:

1. Ninguna máquina desde Internet podría acceder a nuestras máquinas clientes.

2. Los clientes no podrían instalar ningún servidor propio (no será visto desde Internet).

3. Cada dirección IP válida tiene un costo, con este esquema reducimos el número de IP válidas para realizar nuestra red, solo requerimos las IP para el firewall y los servidores.

Este esquema también se conoce como Traducción de Direcciones de Red (TDR o NAT). Para instalar una red segura, las reglas deben habilitar la salida de los servicios WEB y SSH (puertos 80 y 22). De esta forma los clientes podrían acceder a Internet a través de su navegador y a servidores que tengan la comunicación encriptada del SSH. Los clientes también deben tener acceso a los servicios de POP3 e IMAP para el servidor local de correo electrónico, cualquier otro servicio debe ser denegado.

5.7. Monitoreo de la Red

Actualmente no puede verse una red como un equipo estático al que ponemos a funcionar y nos olvidamos de él. Esto es debido a que los ataques a las redes se han vuelto algo común por lo grande que es la Internet, o aún podemos tener ataques en una intranet por los mismos usuarios. Por estas razones necesitamos contar con una herramienta activa, que nos diga que paquetes están pasando por nuestra red en un instante y tomar las medidas necesarias si la red está sufriendo un ataque. Un esquema para el monitoreo de la red presentada en la Figura 5.3, es mostrado en la Figura 5.4. Aquí se aprovecha la situación de los dos firewall para realizar el registro de lo que está pasando por la red.

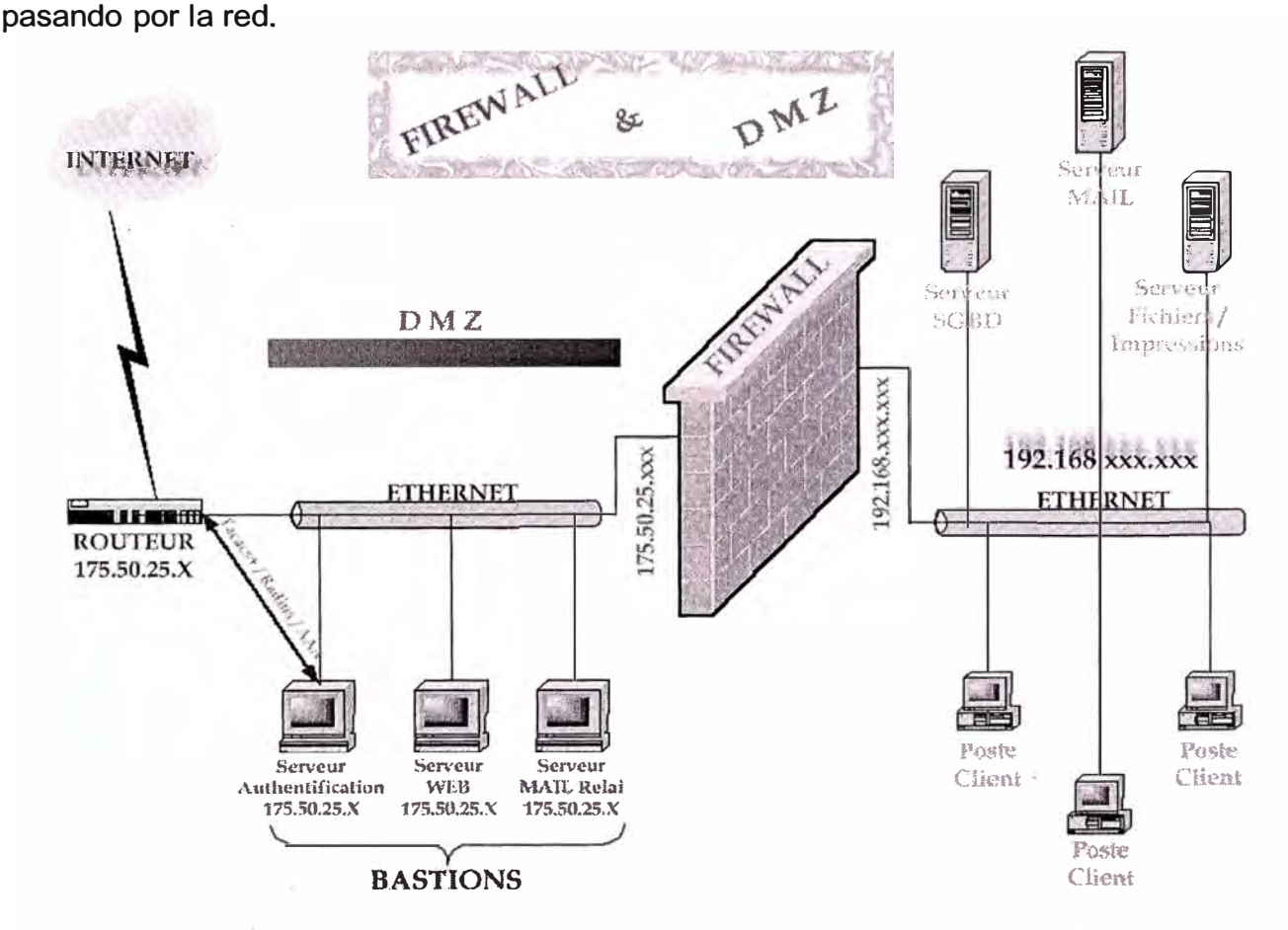

FIG. 5.4: ESQUEMA PARA REALIZAR EL MONITOREO DE UNA RED CON ZONAS DESMILITARIZADAS Y MILITARIZADAS: SE APROVECHAN LOS FIREWALL

El registro de los paquetes en la red de la figura 5.4 puede realizarse de dos formas:

1. Activando el registro de auditoria para los paquetes que son rechazados en los firewall

2. Activando el registro de todos los paquetes que pasan por la red.

Para la primera opción suponemos que los paquetes que permitimos circular por la red son "buenos". Aunque podría darse el caso, en un ataque que se conoce como *denegación de servicio* que precisamente en un servicio activado se presenten miles de peticiones, lo que congestiona el tráfico de la red y la vuelve al mismo tiempo invisibles (por no estar disponible) a todos. Así, con la primera opción tenemos el registro de cosas que están pasando por la red y que no están permitidas. En el segundo esquema podemos llevar estadísticas de todos los paquetes que están circulando por nuestra red, aunque no podemos ver su contenido. En ambas soluciones todavía es necesario contar con alguna herramienta que analice los datos y nos lo presente de forma amigable, tal vez en una página HTML en nuestro servidor WEB.

El esquema de monitoreo podría extenderse para que detectase automáticamente los abusos y mal funcionamiento de la red. Esta es aún un área activa de investigación en la que ya se tienen resultados parciales, aunque no definitivos.

5.8. Prácticas recomendadas de seguridad con firewall

Presentaremos varios conceptos importantes que pueden mejorar y mejoraran la seguridad general de un firewall.

Estos conceptos se aplican tanto a los firewalls como a los sistemas protegidos por los firewalls. Téngase también en cuenta que los siguientes conceptos y prácticas no son mutuamente excluyentes, y que cuando se implementan juntas de forma adecuada, se pueden obtener mejores niveles de seguridad.

5.8.1. ¿Cómo conseguir que los sistemas funcionen correctamente?

Excepto en casos muy extraños, los sistemas y las aplicaciones no se instalan con su configuración más segura. Además, de forma predeterminada se instalan y activan servicios innecesarios para las funciones deseadas de su sistema o aplicación. Una práctica recomendada consiste en activar solo los servicios y cuentas mínimas necesarias para el correcto funcionamiento del sistema. Se producen innumerables intrusiones debido a servicios no utilizados o cuentas innecesarias para el funcionamiento del sistema que se ha comprometido. La practica de desactivar los servicios innecesarios y volver a configurar otros servicios para obtener mayor seguridad se suele conocer como *asegurar el host*. A continuación se enumeran unos cuantos pasos a seguir para asegurar los host:

- Desactivar todos los servicios no necesarios.

- Eliminar cuentas y grupos no necesarios. Cambiar la contraseña y desactivar las aplicaciones y las cuentas de sistemas predeterminadas.

- Volver a configurar el resto de los servicios para aumentar la seguridad.

- Asegurar todas las funciones administrativas.

- Utilizar contraseñas seguras. Las contraseñas seguras son aquellas que tienen más de siete caracteres y una mezcla de letras mayúsculas y minúsculas, números y otros caracteres.

5.8.2. Equipo firewall frente a sistema operativo

Históricamente los firewalls se ejecutaban sobre un sistema operativo de propósito general, como Windows NT o Unix. Funcionaban modificando el núcleo del sistema y la pila TCP/IP para controlar el tráfico. Por tanto, estos firewalls estaban a merced de los problemas presentes en los sistemas operativos en los que se ejecutaban. Para conseguir un alto nivel de seguridad, era necesario asegurar, instalar parches y mantener el sistema operativo (como se ha descrito en la sección anterior). Esta tarea podía ser difícil y muy costosa en tiempo si se carecía de experiencia o tiempo para asegurar de forma adecuada y mantener un sistema operativo totalmente operativo. Sin embargo, actualmente, varios proveedores de firewalls distribuyen sus firewalls como equipos.

Los equipos integran el sistema operativo y el software del firewall creando un dispositivo de firewall totalmente asegurado y dedicado. El proceso de integración elimina cualquier función no necesaria para seleccionar y asegurar paquetes. Además, se proporciona una interfaz administrativa totalmente funcional para simplificar más la configuración y el mantenimiento del firewall. Los equipos de firewall no necesitan que se aseguren mucho los host cuando se implantan (normalmente, lo único necesario es cambiar las contraseñas predeterminadas). Los administradores se pueden centrar en desarrollar conjuntos de reglas en lugar de volver a configurar e instalar parches en un sistema operativo de propósito general. Los equipos reducen de forma significativa los costes operativos y de mantenimiento frente a los firewalls basados en el sistema operativo.

5.8.3. Defensa de capa

Aunque el firewall en si es una excelente herramienta de seguridad, no se debería confiar totalmente en ella. Como se ha dicho anteriormente, los firewalls no ofrecen protección frente a lo que esta autorizado. ¿Qué sucede si un intruso ignora el firewall? Piense en

una situación en la que un intruso es capaz de utilizar http para explorar sus servidores Web obteniendo acceso de shell a ese sistema. El firewall permitirá este trafico porque http esta permitido en el servidor Web, y el atacante puede utilizarlo como un conducto para atacar a otros servidores y sistemas de la red sin la protección del firewall. Si sistemas no están configurados de forma segura, no pasara mucho tiempo hasta que toda la infraestructura este comprometida.

Cuando se implantan sistemas, se recomienda implementar controles redundantes para limitar o evitar daños en el sistema en caso de errores en el control. (Es como tener un candado para el volante aunque en la puerta haya una cerradura).

Los controles redundantes incluyen lo siguiente:

- Asegurar los host internos para admitir ataques en caso de que el firewall falle o se pase por alto.

- Ejecutar servicios en entornos restringidos (por ejemplo, mediante el comando chroot de Unix) y con privilegios mínimos.

- Implementar varios firewalls de diferentes fabricantes o aplicar filtros d paquetes en los enrutadores de red. Esto reduce la exposición a defectos del propio firewall.

- Implementar controles humanos como la educación, el control de registros y las alertas.

- Colocar sistemas para que detecten y alerten a los administradores de forma automática ante actividades no autorizadas o maliciosas. A estos sistemas se hace referencia como *sistemas de detección de intrusión* (IDS, *Intrusión Detection System*).

5.8.4. Creación de una directiva de seguridad

La directiva de seguridad de información de la empresa es el fundamento que establece la información de la empresa como un valor que debe ser protegido. Define la vulnerabilidad de la empresa ante el peligro y las consecuencias de la violación de la seguridad. La directiva de seguridad también define como deberían protegerse los datos; el firewall es la implementación de esta directiva.

Para empresas más pequeñas que no disponen de una gran base de datos de directivas formalizadas, es increíblemente útil documentar los propósitos de la red y el uso del firewall para restringir el uso en función de esto.

Las directivas permiten a los administradores denegar muchas solicitudes de nuevo acceso al firewall que siempre se presentan. Si no se define claramente lo que se debería permitir y lo que no, la efectividad del firewall se reduce con el tiempo, ya que cada vez se permiten más servicios.

5.8.5. Supervisión y registro

Con suficiente tiempo y dinero se puede penetrar en cualquier sistema. Pero los intentos de penetración dejaran evidencia, entradas en los registros, etc. Si la gente controla los sistemas con diligencia, los ataques se pueden detectar y detener antes de que tengan éxito. Por tanto, es muy importante controlar la actividad del sistema. Las aplicaciones deberían registrar los eventos del sistema que tienen éxito y los que no. Un registro detallado y revisiones temporales de estos registros pueden alertar a los administradores acerca de actividades sospechosas antes de que se viole de forma importante la seguridad.

5.8.6. Auditoria y pruebas

Una de las cosas más importantes que se pueden hacer después de configurar el firewall, es asegurarse de que el nivel de seguridad que ha planeado conseguir es de hecho el que se ha obtenido, así como verificar que nada ha pasado por alto. Hay disponibles varias herramientas gratuitas y comerciales que se pueden utilizar para probar la seguridad del firewall y los sistemas que este protege.

La seguridad es un proceso continuo; cuando se ha implantado un sistema, es fundamental examinar de forma rigurosa la configuración. Utilice auditores para hacer pruebas periódicas de la evaluación de la seguridad.

5.9. Proxy

Un proxy no es más que un programa de software con la utilidad de "dar servicio", esto es, permitir algún tipo de acceso a una máquina (en la que está corriendo el programa) desde otras; sólo que en este caso, el ordenador que ejecuta el servicio no es el destino final en la comunicación, sino sólo una pasarela que facilita el tráfico hacia otros lugares de una red. Por ejemplo, en un ordenador conectado a Internet podemos ejecutar un *servidor web*, lo que permitirá que otros ordenadores (*clientes*) se puedan conectar al nuestro y leer mediante un determinado protocolo parte de la información contenida en

nuestro disco duro. En este caso el servidor, nuestro ordenador, es el destino final de la comunicación establecida desde esos ordenadores remotos. En cambio, si instalamos un *servidor proxy* en nuestra máquina los ordenadores que accedan a él, fundamentalmente no "querrán" leer nuestro disco duro, sino tener acceso a otros ordenadores a través del nuestro, por lo que nuestro equipo estará simplemente actuando como una pasarela. Todo servidor corriendo (estando abierto) en un equipo, genera un archivo de texto en el que se van registrando las peticiones de los ordenadores que acceden a él y el tipo de solicitud que le están haciendo. Básicamente, se registran: el momento de la comunicación (día y hora), la IP del ordenador que está accediendo al servidor, el protocolo empleado, los puertos utilizados (en el servidor y el cliente), y la solicitud que se hace, sea el acceso a ficheros en disco duro, o la petición de enlace a otra IP externa, etc. Es posible registrar más datos, pero estos son los más elementales. Estos archivos de texto, que reciben el nombre de *log*, son almacenados en el disco duro del ordenador servidor; además, es importante su almacenamiento por razones relacionadas con la seguridad.

5.10. ¿Por qué utilizar un servidor Proxy?

Una situación típica en la que es posible que sea necesario instalar un servidor proxy, es cuando se dispone de una red de varios ordenadores y sólo uno de ellos tiene posibilidad de salida a Internet. Dejando de lado el hecho de que hay sistemas mejores para hacerlo, puede que, por las circunstancias que sea, sólo haya una opción viable para hacer que los demás equipos puedan salir también a Internet: la de instalar un servidor proxy en el equipo que originalmente tiene el modem.

En este caso, en nuestra red, el equipo que tendría salida directa a Internet sería el que tiene instalado el proxy, mientras que los demás accederán a ese ordenador solicitándole que les dé acceso a Internet. El único ordenador que tendrá una IP pública en la Internet será el que está corriendo el proxy, los demás no serán "visibles" para Internet, porque será como si sólo hubiera un ordenador navegando.

En éste ejemplo, el servidor proxy tendría una utilidad meramente privada; accesible solamente desde los equipos que están en su red, y nada más.

Los servidores proxy existen en redes abiertas en Internet desde hace mucho tiempo. Una de las posibilidades de "acción" de este tipo de dispositivos es la de almacenar en su disco duro (u otro dispositivo de almacenamiento) las páginas web que los ordenadores clientes van solicitándole, aunque sean páginas que están en cualquier sitio de Internet. El servidor proxy, a medida que otro ordenador solicita que le muestre una página situada fuera de su red, la almacena para el caso de que otro ordenador vuelva a solicitarle la

misma página; entonces si eso sucede, el proxy, en lugar de ir a buscar la página fuera de su red, la leerá en su disco duro para servirla al ordenador que la solicitó, con lo que se gana tiempo. Es lo que se conoce como *proxy-caché*, ver figura 5.5.

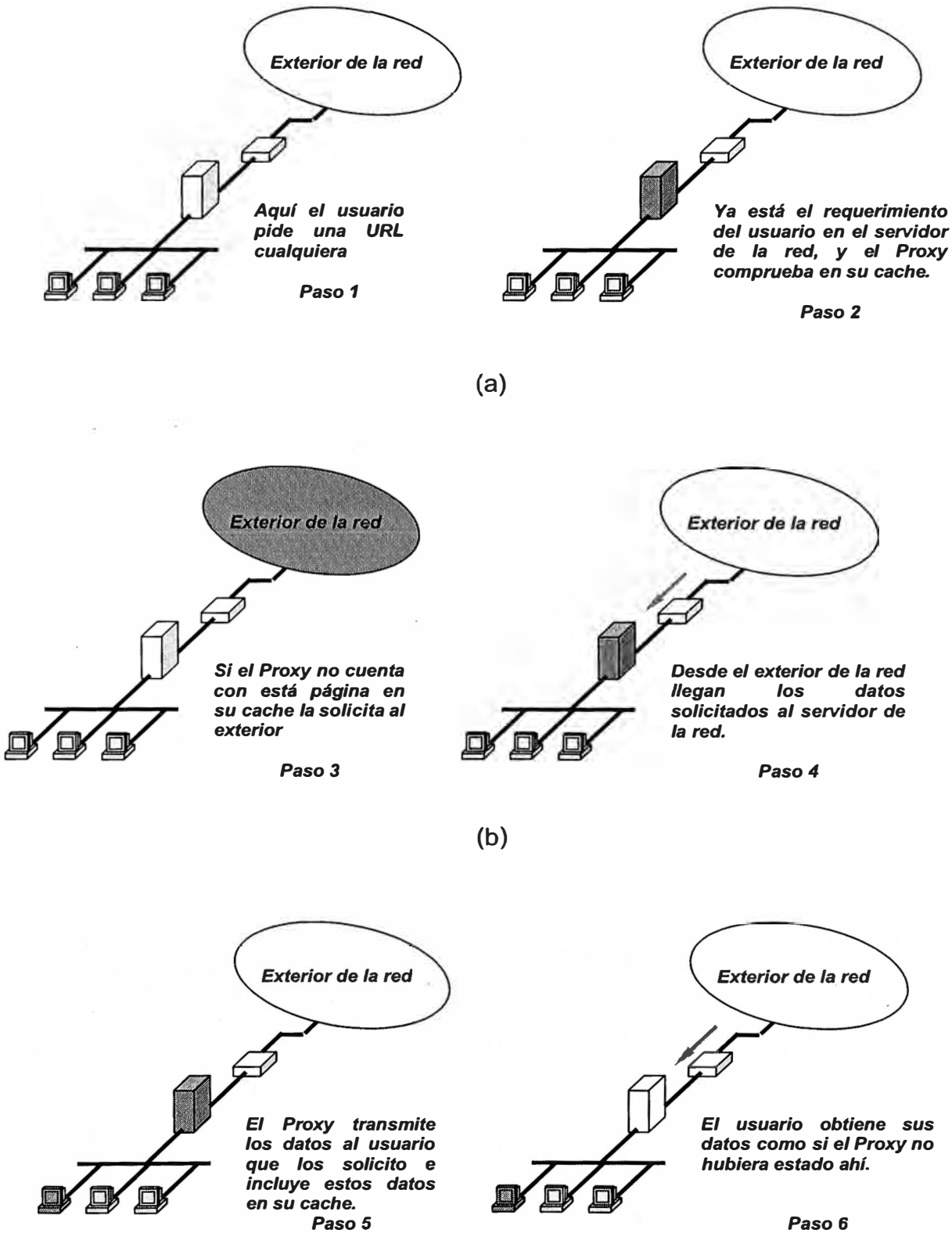

FIG. 5.5 FUNCIONAMIENTO DE UN SERVIDOR PROXY

El "cacheado" de archivos no es tan exótico como puede parecer, también nuestros ordenadores hacen un caché guardando las páginas que vamos visitando, de manera que si regresamos a una página que ya hemos visto con anterioridad durante la misma sesión, la página se cargará más rápido, puesto que el navegador va a leerla a nuestro disco duro, donde ya está almacenada. Dependiendo de cómo hayamos configurado el navegador, esas páginas almacenadas en nuestro equipo, podrán estar disponibles para otras sesiones o no. La diferencia reside en si activamos que se vacíe el caché de disco cada vez que cerramos el navegador (en cuyo caso no estarán disponibles de una sesión a otra) o no lo activamos (y entonces sí estarán disponibles entre sesiones). En Microsoft Internet Explorer, esa opción se encuentra en: *Herramientas --> Opciones de Internet --> Opciones avanzadas --> Vaciar la carpeta Archivos temporales de Internet cuando se cierre el explorador.*

Otra utilidad de un proxy público es la de hacer la navegación más anónima, puesto que como ya mencionábamos antes, al navegar a través de un proxy, todos los lugares visitados "creerán" que nuestra IP es la del proxy, y no la que en realidad tenemos. Aunque el anonimato no hay forma de entenderlo en términos absolutos pues, como dijimos antes, el proxy estará guardando un *log* en el que se registran nuestras solicitudes asociadas a nuestra IP.

5.11. ¿Puedo navegar a través de un proxy público?

Tendremos que configurar nuestro navegador para que haga sus solicitudes al proxy que elijamos para navegar. Vamos a explicar cómo se hace esto sólo en Microsoft Internet Explorer, ya que es el navegador más extendido y este documento va dirigido a los usuarios menos técnicos. De todos modos, una vez comprendido el uso de los proxies, no resulta difícil adaptar lo que comentaremos aquí a las circunstancias de cualquier otro *browser.*

Imaginemos la existencia de un proxy-caché cuya dirección podría ser **proxy.bandaancha.st:8080**. La parte de texto corresponde a la dirección del proxy (podrían ser números separados por puntos, o sea, simplemente una IP sin resolución DNS), y lo que hay detrás de los dos puntos es el puerto al que tenemos que llamar para comunicarnos con ese proxy. Abriendo nuestro navegador, bastará con que accedamos al menú **"Herramientas"** y allí a **"Opciones de Internet ..."**. Nos saldrá un cuadro de diálogo como el de la figura de abajo. Iremos a la pestaña **"Conexiones"**, en ella pulsaremos el botón **"Configuración LAN"** y activaremos las casillas subrayadas en la imagen. Al pulsar en el botón **"Opciones avanzadas..."** del nuevo cuadro de diálogo, nos saldrá un tercero donde tenemos que configurar algunos parámetros. Como es posible

observar, no sólo se puede navegar a través de un proxy; también está permitido hacer otras cosas, como conectarse a un FTP, a un HTTPS, etc. Terminada la configuración, pulsaremos en todos los botones **"Aceptar"** de los cuadros de diálogo para ir cerrándolos. Hecho esto, cuando naveguemos lo estaremos haciendo a través del *hipotético proxy de bandaancha.st*.

Sí. Algunos ISP colocan en sus redes proxies capaces de desviar hacia ellos todo el tráfico que se solicita a través de determinados puertos, habitualmente interceptan el tráfico solicitado a puerto :80, o sea, la navegación web. A estos proxies se les llama *proxies transparentes*, porque su utilización es transparente al usuario, éste no tiene que configurar nada, y no tiene forma de evitarlos, salvo utilizando otro proxy distinto configurado en su navegador como vimos antes, y siempre que las solicitudes se hagan por otro puerto diferente al :80 (o diferente a todos los puertos filtrados por el proxy transparente, si es que hay más).

Lo habitual es que los proxies transparentes sean también proxies-caché, puesto que tienen la finalidad de servir tráfico web dentro de la red del ISP sin salir a Internet si es posible, ahorrándose tráfico desde el exterior. El tráfico proveniente desde fuera de las redes determina el ancho de banda necesario para que un ISP pueda servir en condiciones óptimas las solicitudes de todos sus usuarios. Los ISPs contratan ese ancho de banda a sus *carriers*, y en función del caudal contratado su factura con ellos varía. Por lo tanto, los proxies-caché ahorran dinero al ISP.

5.12. **Proxy y firewall**

Las gateways [12] o servidores Proxy definen un concepto completamente diferente en términos de firewall. Con el fin de balancear algunas de las debilidades que presentan los enrutadores de filtrado de paquetes, usted puede utilizar ciertas aplicaciones de software en su firewall para reenviar y filtrar conexiones hacia servicios como Telnet y FTP. A estas aplicaciones se les llama servicio proxy, y al host que ejecuta el servicio Proxy se le conoce comúnmente como gateway de aplicación.

Existen muchas compañías que sólo utilizan un servicio proxy como firewall, mientras que otras simplemente se apoyan en el propio firewall. Dependiendo del entorno que utilice, del tamaño de su compañía y desnivel de protección que se desea alcanzar, cualquiera de estas opciones podría ser la solución que usted necesita. Sin embargo como regla general siempre se debe considerar la implementación de un servicio proxy en combinación con sus enrutadores de filtrado de paquetes (firewall), de modo que se pueda lograr un nivel mas robusto de defensa y un control de acceso mas flexible.

Por lo tanto la combinación de las gateway de aplicación con los enrutadores de filtrado de paquetes es la solución ideal para incrementar el nivel de seguridad y flexibilidad de su firewall, y lograr la máxima seguridad en Internet. Estas combinaciones con frecuencia se llaman gateway hibridas. De alguna forma son comunes debido a que proporcionan acceso sin obstrucciones desde los equipos internos hacia las redes no confiables, al mismo tiempo que aplican una seguridad muy robusta para las conexiones que llegan desde el exterior hasta la red protegida. Considere la figura 5.6 como un ejemplo de un sitio que utiliza un enrutador de filtrado de paquetes y que bloquea cualquier conexión de Telnet y FTP entrante. El enrutador permite que los paquetes telnet y FTP se dirijan únicamente a la gateway de aplicación Telnet/FTP. Un usuario que se conecta al sistema de un sitio, tendrá que conectarse primero a la gateway de aplicación y después al host de destino, de la siguiente forma:

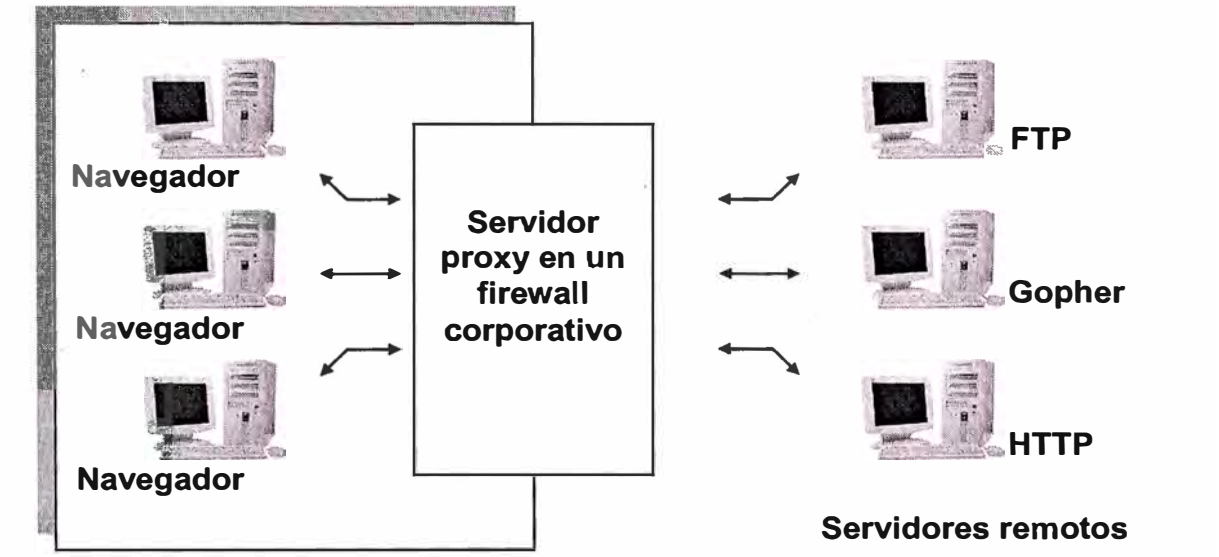

FIG. 5.6: CONEXIÓN VIRTUAL IMPLEMENTADA POR UNA GATEWAY Y POR LOS SERVICIOS PROXY

1. Un usuario solicita la conexión Telnet a la gateway de aplicación e introduce el nombre del host interno.
2. La gateway revisa la dirección IP de origen del usuario y la acepta o rechaza de acuerdo al criterio de acceso que se aplique.
3. Es posible que el usuario tenga que ser autenticado.
4. El servicio proxy establece una conexión Telnet entre la gateway y el servidor interno.
5. El servicio proxy transmite bytes entre las dos conexiones.
6. La gateway de aplicación registra la conexión.

5.13. Ventajas y desventajas de los servidores proxy

Existen muchas ventajas al utilizar gateways de aplicación frente al modo predeterminado que permite que el tráfico de aplicaciones llegue directamente a los hosts internos. He aquí las cinco ventajas principales:

1. Ocultar información. Los nombres de los sistemas internos (a través de DNS) quedan ocultos frente a los sistemas externos. Sólo el nombre del host de la interfaz externa de la gateway de aplicación debe ser conocido por los sistemas externos.

2. Autenticación y registro en bitácoras robustas. El tráfico puede ser autenticado previamente antes de que llegue a los host internos.

3. Economía. El software y el hardware de autenticación/conexión sólo se localiza en la gateway de aplicación.

4. Reglas de filtrado más inteligibles. Las reglas del enrutador de filtrado de paquetes son más legibles y comprensibles de lo que serían si los enrutadores filtraran y dirigieran el tráfico hacia varios sistemas específicos. Con las gateways de aplicaciones, el enrutador sólo necesita permitir el tráfico de la aplicación destinado a la gateway de aplicación mientras bloquea el resto.

5. Correo electrónico. Es posible centralizar la recolección y distribución del correo electrónico hacia host y correos internos. Todos los usuarios internos tendrían un correo electrónico con la estructura usuario@contenedordecorreo donde contenedor de correo es el nombre de la gateway de correo electrónico. La gateway recibirá el correo de los usuarios externos y después los enviará a los correos internos.

Sin embargo nada es perfecto. Las gateways de aplicación también tienen desventajas. Para conectarse a los protocolos cliente – servidor, se requiere de dos pasos, entrada o salida. Algunos incluso requieren la modificación del cliente, lo cual no es necesariamente el caso de una gateway de aplicación Telnet, pero si se requiere de modificaciones en la conducta del usuario. El usuario tendría que conectarse al firewall en lugar de conectarse directamente al host.

Resumen cap. V

En este capitulo se analiza los mecanismos de control de acceso, objeto de estudio en este informe, los firewalls y los proxy. En base a la información obtenida en los capítulos anteriores, es decir, como funcionan los protocolos con los que se comunican las redes, los tipos habituales de ataque y los problemas de seguridad a los que estamos sometidos al conectar una Lan a Internet, en este capitulo se hace un análisis de las formas en que estos sistemas nos brindan un acceso seguro, un control de la información que solicitamos de Internet y la que los usuarios de Internet soliciten de nuestra red.

CONCLUSIONES

1. Los numerosos ataques a los que estamos expuestos cuando se conectan dos redes, se basan en explotar algunas características de los protocolos de comunicación.

2. Estos ataques buscan: el cese de las actividades, los servicios que presta el ordenador atacado o bien conseguir un acceso dentro de la máquina, que le permita controlarla, utilizarla o tomar su información.

3. Este trabajo de investigación nos permite comprender el funcionamiento de las redes TCP/IP, ya que se ha profundizado en el estudio de los protocolos más importantes que permiten su funcionamiento, analizándolos globalmente, lo que nos permite examinar sus características, relaciones y roles en el transporte de la Información, por lo tanto, tomar consciencia de la importancia de los mecanismos de seguridad que se deben tomar en cuenta cuando dos redes con diferente nivel de confianza requieren comunicarse, compartir recursos o información.

4. Para hacer frente a la desenfrenada Internet y la cantidad cada vez más grande de problemas de seguridad que la red de redes nos genera, se desarrollan diversos mecanismos de seguridad, los cuales dependiendo de la naturaleza de la necesidad de recursos de la Internet, deben ser analizados y adoptados como mecanismos de control.

5. Dos mecanismos de control importantes para la seguridad de una red son el firewall y el proxy, siendo estos, entre otros, los más usados cuando se busca seguridad.

6. La seguridad utilizando firewall y proxy resulta poderosa y tiene varios frentes si se combinan adecuadamente, tal como se menciona en el capitulo 5.12. Estos mecanismos no son simplemente “paredes de fuego” que ahuyentan a los hackers, pueden ser mecanismos de autenticación o enrutadores de la información, la visión que nos da este trabajo de investigación es que estos sistemas pueden ser mucho más que cada una de estas acepciones individuales.

7. Es indispensable tener presente las ventajas y desventajas que estos sistemas nos brindan, tal como se menciona en los capítulos 5.4 y 5.13, ya que sólo así podemos establecer políticas de seguridad acertadas que permitan una conexión segura a Internet.

ANEXO A
PRODUCTOS FIREWALL EN EL MERCADO

1. Fire Wall-1 de check Point:

   Tecnologia Stateful Inspection

   Esta basado en la arquitectura de Stateful Inspection, la nueva generación de tecnologías de firewall inventada por Check Point. La tecnología de inspección de estado ofrece funcionalidad completa de firewall y asegura el nivel más alto para la seguridad de la red. El poderoso Inspection Module de FireWall 1 analiza todos los niveles de comunicación de paquetes y extrae la información relevante sobre las comunicaciones y el estado de la aplicación. El Inspection Module entiende y puede aprender sobre cualquier protocolo y aplicación.

2. Firewall Labyrinth de CYCON

   El sistema "Tipo Laberinto"

   El firewall CYCON Labyrinth es el primer sistema del mundo "tipo laberinto" que incorpora una verdadera *network address translation* (NAT, translación de direcciones de red) bidireccional con un poderoso firewall de *intelligent connection-tracking* (ICT, rastreo inteligente de conexiones) para crear un dispositivo de seguridad y de administración de la red. El firewall CYCON Labyrinth actualmente se utiliza en muchas de als principales corporaciones, proveedores de servicios de Internet e instituciones de investigación.

3. Guardian Firewall System de NetGuard

   Inspección de estado de nivel MAC

   NetGuard LTD., Es una compañía de software que se especializa en soluciones de seguridad para las redes corporativas de Internet. El Guardian Firewall System fue el primer producto que fue diseñadao para operar en la popular plataforma Windows NT y Microsoft lo recomienda como una solución Windows NT.

   NetGuard LTD., es una compañía subsidiaria de LandOptics Ltd., uno de los principales proveedores de concentradores y productos de red. NetGuardaprovecha

al máximo la enorme base de usuarios de LandOptics y su experiencia en el campo de los ambientes de red para ofrecer alta calidad y eficiencia.

4. CyberGuard Firewall de CyberGuard

   Fortalecimiento del sistema operativo

   CyberGuard Corporation es una empresa dedicada a proporcionar las soluciones de seguridad más robustas y más completas para Internet, las intranets y el comercio electrónico a las organizaciones que tienen redes de datos a un nivel empresarial.

   CyberGuard Firewall es una computadora segura de multiples niveles que reside entre las redes internas o entre una red o Internet con el fin de ofrecer un solo punto seguro de conexión a través del cual viajarán todos los datos. El firewall detecta y filtra todo el tráfico desde y hacia cualquier red pública antes de permitirle el paso, con el fin de evitar la posibilidad de que los datos sean robados o dañados. Los intentos no autorizados para comunicarse con la red interna quedan registrados y bloqueados.

5. El firewall de Raptor

   Una arquitectura de nivel de aplicación

   Raptor Systems fue una de las compañias lideres en la integración del software y de los servicios para la seguridad de los firewall. Raptor Firewall de AXENT contiene uno de los conjuntos más poderosos de aplicaciones proxy. Basada en arquitectura de firewall de nivel de aplicación, la familia Eagle incluye una suite de componentes modulares de software que proporciona seguridad de red en tiempo real para Internet, para los grupos de trabajo, para las computadoras móviles y para los dominios de oficinas remotas dentro de una empresa. Tagle se ejecuta en estaciones de trabajo de Sun Microsystem, Hewlett-Packard y Windows NT.

6. SecurIT FIREWALL de Milkyway

   Un núcleo BSDI fortalecido desde su fabricación

   Milkway Networks, es uno de los principales proveedores mundiales de aplicaciones de seguridad para Internet y para intranets que pretenden resguardar la información dentro de las empresas. La visión de la compañía consiste en ofrecer una sola solución de seguridad para el trabajo entre redes, sin importar la ubicación de los usuarios o de los servidores dentro de la red. SecurIT FIREWALL es la pieza central de la suite Milyway SecurIT, la primera suite integrada de la industria que cuenta con productos de seguridad y que aprovecha el poder de la tecnología Black Hole de

Milyway con un producto de acceso remoto y seguro y con una herramienta de auditoria de seguridad para redes.

7. Watchguard Firebox System de WatchGuard Technologies
   Combinación de los principales enfoques de firewall en firebox
   WatchGuard Technologies es una compañía que ofrece productos de seguridad de última generación para Internet/Intranets que eliminan el costo y la complejidad asociados con las ofertas actuales además de que incluyen una poderosa tecnología hibrida para firewall y una administración inteligente para la seguridad con un precio económico.

ANEXO B
PRODUCTOS PROXY EN EL MERCADO

1. Blue Coat Proxy*SG*

   La funcionalidad proxy más sólida: las soluciones proxy de Blue Coat se basan en un dispositivo optimizado con un sistema operativo especial diseñado específicamente sobre la base de los objetos Web. El ProxySG es compatible con todos los protocolos Web comunes incluida la mensajería instantánea (AOL, MSN, Yahoo!), HTTP, HTTPS, FTP, SOCKS, DNS, transmisión Real y transmisión Microsoft. Además, el ProxySG admite la conducción TCP, un método para controlar cualquier protocolo de aplicación que se ejecute sobre TCP sin compatibilidad de proxy nativo.

   Mejor granularidad de directivas: las directivas complejas y de acceso global pueden implementarse fácilmente. Mediante el BlueView™ Visual Policy Manager integrado, los administradores pueden crear e implementar rápidamente potentes directivas de proxy Web en toda la empresa. En el centro de la solución se encuentra el Policy Processing

   Engine™ (patente pendiente) de Blue Coat, que ofrece un control ampliable y granular para los entornos más exigentes.

   El coste de propiedad más bajo: inicialmente, el software proxy para un servidor de uso general puede ser más económico. Sin embargo, a medida que pase el tiempo, los costes adicionales de gestión y licencia pueden sobrepasar fácilmente el coste de adquisición de un dispositivo Blue Coat ProxySG. Asimismo, si se suma el coste del capital humano necesario para instalar, proporcionar soporte y mantener un producto de software y sus componentes, la solución Blue Coat se convierte en una solución muy rentable.

2. ABC Proxy

   Fácil, barato, seguro, rápido... todo esto puede utilizarse perfectamente para definir este software, el ABC Proxy. Este programa permite el uso compartido de una sola conexión a Internet por todos los usuarios de la red local. Soporta protocolos HTTP, HTTPS, IRC, SMTP, POP3 y mucho más. Incorpora un firewall para evitar ataques e

intrusiones desde el exterior de la red. Incorpora caché de sitios visitados para una más rápida navegación. Y muchas más opciones.

3. CProxy Server

   Este software CProxy Server además de un completísimo programa para conectar varios ordenadores a Internet a través de una única conexión, nos da velocidad y seguridad. Este programa incluye una caché en la que se almacenarán los sitios a los que más frecuentemente acudamos en Internet. Soporta los protocolos HTTP, HTTPS, FTP, SOCKS, NNTP, SMTP, POP3 y Real Audio.También incluye soporte de mapeado tanto sobre UDP como TCP, para servicios personalizados, entre otras muchas e importantes opciones.

4. GunnProxy

   GunnProxy es un magnífico programa de proxy con multitud de opciones que lo convierten prácticamente en una utilidad profesional. Alguna de dichas opciones son: caché HTTP; Soporte en línea con actualizaciones automáticas para, por ejemplo, la mejora de la velocidad; soporte SMTP, POP3, NNTP, FTP, IRC, HTTP, UDP, tunelling SSL, SOCKS 4 y 5, DNS, conexiones RealAudio/RealVídeo, PING, servidor de WEB y de Quake2. Y todo ello con soporte para varios usuarios conectados simultáneamente por red interna.

5. Interbase Encryption Proxy

   Interbase Encryption Proxy es un programa diseñado para encriptar conexiones del tipo Interbase sobre Internet, permitiendo así que los usuarios puedan trabajar en alta velocidad a través de la red. El programa permite manejar un servidor en el que haya hasta 50 módems diferentes, y hacerlos funcionar a todos a la mayor velocidad posible. De esta manera, es posible hacer funcionar programas diseñados para red local en Internet, y mediante la encriptación, hacerlo de una manera absolutamente segura.

6. MyProxy

   Es un sencillo servidor proxy para servicios HTTP, HTTPS, SMTP y POP3 que además te permite filtrar publicidad, ventanas de pop-up otras funciones interesantes. Gracias a su capacidad de filtrado de publicidad, puedes navegar más rápido, una velocidad que también se ve incrementada con la función de grabación local de DNS, lo que ahorra tráfico de red. Como servidor proxy, permite compartir una única

conexión a Internet entre dos o más ordenadores. El programa controla la existencia de posibles elementos de adware y spyware e impide el uso no autorizado de la conexión mediante contraseña.

BIBLIOGRAFÍA

[1] Jerry Honeycutt. Using internet.
http://docs.rinet.ru/UsingInternet/ch01/ch01.htm

[2] José Antonio Millán. El fruto caliente de guerra fría. Noviembre 1999.
http://jamillan.com/histoint.htm

[3] Corporación Universitaria para el Desarrollo de Internet (cudi). http://www.cudi.edu.mx/

[4] Bruce Sterling. Pequeña historia de Internet. 1992.
http://www.sindominio.net/biblioweb/telematica/hist_internet.html

[5] Internet pioneers: Paul Baran.
http://www.ibiblio.org/pioneers/baran.html

[6] John Plane Jr. Tcp/ip introduction and history.
http://www.certificationcenter.net/phpweb/tcphistory.php

[7] Christos J.P. *History of Internet. A chronology: 1843 to the present*. Moschovite Group, 2001.
http://www.historyoftheinternet.com/index.html

[8] Keith E. Strassberg. Firewalls. Mc Graw Hill. 2003

[9] Parker and M.Sportack. 2000.

[10] O. Kirch and T. Dawson. *Linux Network Administrators Guide*. O'Reilly, 2000.

[11] El Centro de Coordinación CERT para la seguridad en Internet. http://www.cert.org

[12] Software-RAID-HOWTO.
http://www.tldp.org