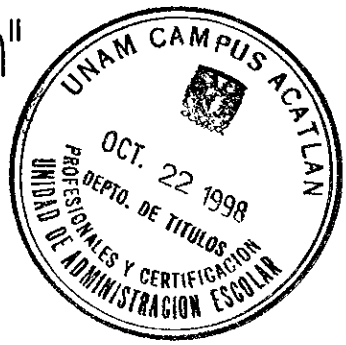
Universidad Nacional Autónoma de México.
Escuela Nacional de Estudios Profesionales.
"Acatlán"



Firewall, un esquema de seguridad para redes computacionales

TESINA

que para obtener el título de
Lic. en Matemáticas Aplicadas
y Computación

PRESENTA

Carlos Alberto Rangel Rojas

Sta. Cruz Acatlán, Estado de México, 1998.

Objetivo del trabajo

Dar a conocer un esquema de protección para una red con acceso a Internet y a su vez explicar de manera sencilla sus partes, su instalación y su funcionamiento y comparándolo con otros esquemas de protección

Índice

AGRADECIMIENTOS.

INTRODUCCIÓN. 1

1. Conceptos básicos de redes. 3

1.1 Introducción. 3
1.2 Historia de las redes. 3
1.3 Topologías de redes. 4
1.4 Tipos de computadoras en una red. 6
1.4.1 Estación de trabajo. 6
1.4.2 Servidor no dedicado. 6
1.4.3 Servidor dedicado. 6
1.4.4 Terminales. 6
1.5 Tipos de redes. 6
1.6 Especificaciones de red. 7
1.6.1 Ethernet. 7
1.6.2 Token Ring. 8
1.6.3 FDDI y CDDI. 8
1.6.4 ATM. 9
1.7 Conectores de red. 10
1.7.1 10BASE5 (Thick Ethernet). 10
1.7.2 10BASE2 (Thinnet). 10
1.7.3 10BASE-T (Par trenzado sin blindaje). 10
1.8 Modelo OSI. 10
1.8.1 Modos de servicio. 11
1.8.2 Capa física. 12
1.8.3 Capa de enlace. 12
1.8.4 Capa de red. 12
1.8.5 Capa de transporte. 12
1.8.6 Capa de sesión. 12
1.8.7 Capa de presentación. 13
1.8.8 Capa de aplicación. 13
1.9 Tipos de conexión. 13
1.10 El protocolo de comunicación TCP/IP. 13
1.11 Servicios comunes de Internet (servicios TCP/IP). 14
1.12 Servidores en Internet. 15
1.13 Usos del TCP/IP. 16
1.13.1 IP (Internet Protocol). 16
1.13.2 TCP (Transport Control Protocol). 16
1.13.3 UDP (User Datagram Program). 17
1.13.4 ICMP (Internet Protocol Message Program). 17
1.14 Direcciones de Internet (IP Address). 17
1.14.1 Direcciones alfanuméricas. 18
1.15 Utilerías de TCP/IP (Comandos de UNIX). 18
1.15.1 Introducción. 18
1.15.2 ping. 19
1.15.3 ruptime. 19
1.15.4 rwho. 19
1.15.5 finger. 19
1.15.6 netstat. 20
1.15.7 ifconfig. 21
1.15.8 traceroute. 21
1.15.9 arp. 22
1.15.10 rlogin. 22
1.15.11 rcp. 22

1.15.12 rsh. 23
1.15.13 telnet. 23
1.15.14 ftp. 23
1.15.15 spray. 23
1.16 Archivos de configuración de red. 24
1.16.1 hosts. 24
1.16.2 ethers. 24
1.16.3 networks. 25
1.16.4 protocols. 25
1.16.5 services. 25
1.16.6 inetd.conf. 26
1.17 Archivos de acceso a la red. 26
1.17.1 hosts.equiv 26
1.17.2 .rhosts 27
1.17.3 hosts.lpd 27
1.17.4 named.boot 27
1.17.5 fbtab (logindevperm) 27
1.17.6 X0.hosts 27
1.17.7 sendmail.cf 27
1.17.8 ftpusers 28
1.17.9 Archivos de inicialización del sistema. 28
1.17.10 Archivos en la cuenta del usuario. 28
1.17.11 Otros archivos a proteger. 28

2. Puntos a proteger de una red. 31

2.1 Introducción. 31
2.2 Niveles de seguridad. 31
2.2.1 Nivel D1. 31
2.2.2 Nivel C1. 31
2.2.3 Nivel C2. 31
2.2.4 Nivel B1. 32
2.2.5 Nivel B2. 32
2.2.6 Nivel B3. 32
2.2.7 Nivel A. 32
2.3 Características de la seguridad. 32
2.4 Tipos de usuarios en una red. 33
2.4.1 Administradores. 33
2.4.2 Supervisores de red. 33
2.4.3 Usuarios. 34
2.4.4 Hackers. 34
2.5 Políticas de seguridad de red. 35
2.6 Aseguramiento de la seguridad. 36
2.7 Análisis de riesgos. 37
2.8 Establecimiento de la política. 38
2.9 Incidentes de seguridad más usuales en Internet. 39
2.10 Puntos para una red segura. 43
2.11 Consideraciones importantes. 44
2.11.1 Respaldos. 44
2.11.2 Encriptamiento. 45
2.11.3 Passwords. 46
2.11.4 Internet. 46
2.12 Características de un sistema de seguridad. 48

3. Diseño de un firewall. 51

3.1 Componentes de un firewall. 51
3.1.1 Políticas de red. 51

3.1.1.1 Política de acceso a los servicios. 51
3.1.1.2 Diseño de la política de un firewall. 52
3.1.2 Medios de autentificación. 53
3.1.2.1 Autentificación In-Band. 54
3.1.2.2 Autentificación Out-of-Band. 54
3.1.3 Filtrado de paquetes (packets filtering). 54
3.1.3.1 Protocolos a filtrar. 55
3.1.3.2 Problemas con los ruteadores del filtrado de paquetes. 56
3.1.4 Aplicaciones gateway. 57
3.1.5 Puentes y ruteadores. 60
3.1.5.1 Diferencias. 60
3.1.6 Gateways. 62
3.1.7 LAN Switch. 64
3.2 Construcción de firewalls. 64
3.2.1 Filtrado de paquetes. 64
3.2.2 Gateway dual. 65
3.2.3 Firewall de host protegido. 66
3.2.4 Firewall de subred protegida. 67
3.2.5 Modems y firewalls. 69
3.2.6 Nuevas tecnologías. 71
3.3 Políticas del firewall. 72
3.3.1 Pasos en la creación de una política de acceso a los servicios. 73
3.3.2 Flexibilidad en la política. 73
3.3.3 Autentificación para usuarios remotos. 73
3.3.4 Conexiones remotas a la red. 74
3.3.5 Políticas del servidor de información. 74
3.3.6 Contenidos de un firewall. 75
3.4 Comprar o construir un firewall. 75
3.5 Pruebas del firewall. 76
3.5.1 Pruebas de caja negra. 76
3.5.1.1 Escaneo de puertos. 76
3.5.1.2 Escaneo baseline. 77
3.5.1.3 Escaneo en lugares múltiples. 77
3.5.2 Observación "on-the-wire". 77
3.5.2.1 Observación "Quiet Wire". 78
3.5.2.2 Pruebas de control. 78
3.5.2.3 Observaciones "Live Wire". 78
3.5.3 Verificación de los sistemas de identificación. 78
3.5.4 Prueba de la configuración. 79
3.5.5 Validaciones de terceros. 80
3.5.5.1 Validaciones periódicas. 80
3.5.5.2 Validaciones aleatorias. 80
3.5.5.3 Espionaje/ingeniería social. 80
3.5.5.4 Pruebas configurables. 81

4. Ventajas y desventajas frente a otras opciones. 83

4.1 Protección contra los servicios vulnerables. 83
4.2 Control de acceso a los sistemas del sitio. 83
4.3 Concentración de la seguridad. 83
4.4 Mejoras en la privacidad. 84
4.5 Accesos y estadísticas acerca del uso de la red. 84
4.6 Reforzamiento de las políticas. 84
4.7 Acceso restringido a servicios deseados. 84
4.8 Potencial de puertas abiertas. 85
4.9 Protección limitada contra atacantes internos. 85
4.10 MBONE (Multicast IP Transmissions). 85

4.11 Virus. 85
4.12 Cuellos de botella. 85
4.13 Centralización. 85
4.14 Gateway proxy Vs filtrado de paquetes. 85
4.15 Redes privadas virtuales. 86
4.16 Firewalls y el monitoreo del host. 87
4.17 Firewalls y la autentificación. 89
4.18 Firewalls y la encriptación. 89
4.19 Firewalls y NFS. 90
4.20 Multilayer Switches 91

5. Aplicación. 93

5.1 Características de un firewall. 93
5.1.1 Controles de acceso. 93
5.1.1.1 Listas o reglas de acceso. 93
5.1.1.2 Filtros de sesión. 93
5.1.1.3 Controles de alteración del host. 94
5.1.2 Servicios soportados. 94
5.1.3 Autentificación de usuarios. 94
5.1.4 Administración. 94
5.1.4.1 Interface. 94
5.1.4.2 Administración remota y central. 94
5.1.4.3 Asistencia en línea. 94
5.1.4.4 Reportes de configuración. 95
5.1.5 Auditorías y alarmas. 95
5.1.6 Integridad del firewall. 95
5.1.6.1 Sistema operativo endurecido (confiable). 95
5.1.6.2 Firewalls de host dual. 96
5.1.6.3 Scanner de integridad. 96
5.1.6.4 Invisibilidad. 96
5.1.7 Velocidad. 96
5.2 Lugares de implementación. 97
5.2.1 Firewalls internos. 97
5.2.2 Laboratorios de redes. 97
5.2.3 Redes de pruebas. 98
5.2.4 Redes inseguras. 98
5.2.5 Redes extraseguras. 98
5.3 Firewall freeware. 98
5.3.1 Ventajas y desventajas. 99
5.4 Firewall comercial. 100
5.4.1 Ventajas y desventajas. 101
5.5 Posibles errores en el firewall implementado. 101
5.6 Ejemplo de un firewall. 103
5.6.1. Herramientas de software. 104
5.6.1.1 SMAP. 104
5.6.1.2 netacl. 104
5.6.1.3 ftp-gw. 105
5.6.1.4 telnet-gw. 105
5.6.1.5 rlogin-gw. 105
5.6.1.6 plug-gw. 106
5.6.1.7 authsrv. 106
5.6.1.8 telnetd. 106
5.6.1.9 login. 106
5.6.1.10 ftpd. 107
5.6.1.11 syslogd. 107
5.6.2 Exposición del problema. 107

Conclusiones. 113

ANEXO I. 117
ANEXO II. 119
Glosario. 121
Indice de figuras. 125

Bibliografía 127

Agradecimientos

A Celestina y Pedro, por tantos sacrificios realizados, además del gran apoyo que tengo de ellos, en las buenas y en las malas.

A Edgar y Osvaldo, por compartir conmigo mis éxitos y mis fracasos.

A Pedro, Matilde, Jesús y Arturo, gracias a Internet tuve la gran oportunidad de conocerlos y me orientaran con su apoyo técnico que ofrecieron desinteresadamente; resultando en este trabajo que presento. En especial le agradezco a Fabian, que me apoyo en el último estirón.

A Blanca, Verónica y Lorenzo por las facilidades que me brindaron.

A Rosa, Judith, Juan Carlos, Ivar y Alma; gracias por las aportaciones y las orientaciones que hicieron en su momento a este trabajo.

A todas aquellas personas que retrasaron este trabajo -para bien o para mal-, esto me ha enseñado a no rendirme ante situaciones adversas.

A todos esos grandes amigos, ya que su ejemplo me motiva a seguir superándome.

Por último, a cualquier lector que considere este trabajo como referencia en otras investigaciones, por cuestiones culturales, de trabajo o escolares; ya que para emprender el largo viaje del éxito son necesarios la conciencia, los deseos de superación y el trabajo en equipo.

Introducción

Desde tiempos remotos, la información ha jugado un papel esencial en el continuo desarrollo de la humanidad y con ello su acceso regulado a ciertas personas (sacerdotes, shamanes) en determinados lugares (templos, santuarios). Hoy en día la información se protege; por ejemplo, con patentes, que es un registro de derechos de autor sobre algún medio innovador, esto se hace para proteger posibles ganancias o contra la piratería; en una biblioteca las personas (usuarios) deben de cumplir ciertos requisitos para poder accesar al local de esta y otros para pedir préstamo externo, en este caso al pedir un libro en esta condición, se tienen datos específicos del usuario (nombre, número de usuario, domicilio) y del libro (nombre, título, clasificación), de manera similar funciona un firewall.

La explosión innovadora que ha tenido Internet desde los años ochentas ha traído grandes beneficios a infinidad de organizaciones públicas y privadas de todo tipo. La información es consultada por cualquier persona interesada (dependiendo de las facilidades que tenga el "sitio"). Pero cada organización dependiendo de sus necesidades propias podría contar con servidores con características particulares, estar conectado bajo alguna topología en particular que pueda usar algún protocolo determinado y disponer de ciertos servicios (tener acceso a una red privada, enviar y recibir correo electrónico, entre otros) con los cuales se va a distribuir la información así como sus peligros inherentes.

Estos servicios son aprovechados en Internet y a la organización le interesa conocer quién y de dónde esta accesando a qué tipo de información. Se encuentran disponibles en servidores (o hosts dependiendo de la perspectiva) que se ejecutan bajo alguna variante del sistema operativo UNIX que fue uno de los primeros en salir al mercado y el primero en el que se utilizó el protocolo TCP/IP que contiene los servicios. Para algunas organizaciones (por ejemplo, el gobierno de los E.U.) UNIX es confiable debido a que es el sistema que más ataques ha sufrido y cumple con ciertos estándares (por ejemplo, que puede "endurecerce" el sistema operativo), pero esto no quiere decir que sea confiable totalmente.

Por ello es conveniente conocer e instalar (en la medida de las posibilidades y necesidades de la organización –empresa-) algún sistema de seguridad que aumente la confiabilidad de la información que tenga y genere la empresa. Existen varios sistemas de seguridad para una red de computadoras como la autentificación, la encriptación, el monitoreo continuo de la red, los firewalls y alguna otra nueva tecnología que se este desarrollando en alguna parte del mundo. Un buen esquema de seguridad es el que propone el firewall debido a que aprovecha características de diversos sistemas de seguridad existenetes, pero como todo desarrollo del hombre tiene sus detalles particulares. Los primeros intentos de instalar un firewall (algunos) se hicieron bajo UNIX, debido a su arquitectura abierta. Literalmente en español un firewall es una muralla de fuego, en resumen puede actuar como un "centinela" y puede realizar las tareas de monitorear y registrar los accesos que hay entre una red "confiable" (por ejemplo, la red corporativa de una organización) y una red no confiable (Internet, otra red con características confiables) - pudiendo implementarse dentro de la misma red confiable –, basándose en las políticas de seguridad que se tengan en el sitio o la organización.

La intención de este trabajo es hablar de su diseño, su arquitectura, sus ventajas y desventajas entre los diversos tipos de firewalls y frente a otras opciones de seguridad, así como terminología básica que es necesario conocer para adentrarse en el tema.La aportación de este trabajo es dar a conocer de una manera fácil y compacta esta nueva tecnología que esta teniendo gran aceptación, dada la enorme intercomunicación e interrelación que existen en las redes computacionales hoy en día. De esta manera se puede contar con un criterio más reforzado para poder evaluar de forma adecuada este esquema de seguridad o la situación actual que exista en el sitio o la organización ofreciendo tópicos básicos que deben conocer los usuarios (administradores, supervisores, usuarios y directivos de la organización).

Este trabajo está dirigido a todas aquellas personas que estén involucradas en la administración de redes, así como cualquier usuario que tenga que usar, conocer, evaluar o implementar una protección de este tipo.

Capítulo 1

Conceptos básicos de redes

1.1 Introducción.

En este primer capítulo se presentará algunos tópicos básicos que son necesarios conocer antes de adentrarse al tema de los firewall, se incluye una breve historia y una descripción de los diferentes tipos, topologías y elementos que son utilizados en una red. Asimismo se presenta una descripción del protocolo TCP/IP y algunas utilerías que están relacionadas con el tema de los firewalls así como los archivos de configuración relacionados. En esta parte se mencionan algunos comandos de UNIX, como se verá más adelante el primer sistema operativo en donde se implementó por primera vez este protocolo fue en UNIX, además de que se le considera como un sistema operativo que cumple diversos estándares del gobierno de los E.U. para poder utilizarlo en sus sistemas computacionales (algunas variantes de UNIX como Trusted Solaris 2.5).

1.2 Historia de las redes[9,10,12].

El primer medio para integrar y procesar la información en las computadoras fueron las tarjetas perforadas, representando cada una línea de código o datos del programa, esta información era leída en un sistema de macrocomputadora, procesándolas y enviando los resultados. Al proceso de leer y procesar la información como un todo es conocido como procesamiento por lotes, con esto se interrumpía la interacción con el usuario y la computadora, hasta generar los resultados.

Tiempo después se empezaron a usar computadoras conocidas como terminales tontas, facilitando así al usuario accesar la información específica. Estas terminales están conformadas por un monitor, que despliega los resultados; un teclado, por el cual se introducen los datos, y a su vez son conectadas a una computadora central de gran tamaño.

En los años sesenta empezó a difundirse un tipo de servicio de red comercial que era el *tiempo compartido*, este servicio permitió instalar las terminales en lugares alejados de la computadora central (servidor o anfitrión), la conexión se establecía con ayuda de líneas telefónicas dedicadas. El servidor asignaba y distribuía su tiempo entre las diferentes terminales que solicitaban servicios.

Durante este tiempo surgió otro tipo de procesamiento, conocido como procesamiento en tiempo real, permitiendo que el usuario viera la información en el momento que se tecleaba. Pero debido a la disponibilidad de varios servicios de tiempo compartido se tuvo el problema de que cada servidor tenía su propio método para comunicarse en las terminales. Entonces surgió el ASCII (American Standard Code for Information Interchange) adoptado por la oficina de patrones de los E.U., permitiendo así que 128 caracteres, incluyendo las letras del alfabeto, los dígitos (0-9) y otros símbolos puedan representarse en formato binario de 0 y 1.

Ya establecido el método estándar para transmitir caracteres, fue necesario otro estándar para especificar la manera en que los datos serían transmitidos por cable. Se creo el RS-232C para especificar los voltajes y los parámetros eléctricos de comunicación empleados para conectar los dispositivos, así permitió usar los modems y la conexión por conmutación telefónica. Un módem enlazaba a un terminal marcando el número del servidor, este tiene a su vez un módem que responderá al llamado y así quedaban conectadas entre sí; cuando se terminaba la comunicación, la línea telefónica era utilizada para otros propósitos.

A principio de la década de los ochentas, IBM introduce la primera computadora personal (PC, Personal Computer) que proporcionaba todas las ventajas de cómputo en una sola unidad para una sola persona, tenia un diseño de arquitectura abierta, significando esto que existía compatibilidad con componentes diseñados y fabricados por otras compañías. Su flexibilidad, adaptabilidad y el bajo precio marcó una nueva era en la historia de la computación. Aunque era

capaz de ejecutar y procesar datos sin la intervención de otra computadora, todavía era necesario enlazarse con un servidor, para esto se diseñó el software que emulara a la PC como una terminal tonta, y es capaz de intercambiar archivos entre la PC y el servidor remoto por medio del módem (a esto se le llama subir o bajar archivos).

Una red esta conformada por dos o más computadoras conectadas entre sí, permitiendo de esta manera compartir recursos e información, esta última consiste de archivos y datos; los recursos son los dispositivos o las áreas de almacenamiento de datos en una computadora, los cuales se comparten por medio de la red, estos recursos incluyen en la mayoría de los casos, dispositivos como unidades de disco, directorios e impresoras.

Una red esta conformada de uno o más servidores y estaciones de trabajo o terminales tontas, a cada uno de estos elementos se le conoce también como nodos de red.

1.3 Topologías de red[12].

Los nodos de red necesitan estar conectados para comunicarse, a este modo se le conoce como topología, una red tiene dos tipos; la física que es la manera en que los nodos están conectados unos con otros y la lógica es el método que utilizan para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los diferentes nodos de la red. Estas pueden ser iguales o diferentes.

Las topologías más usadas son las de tipo bus, de estrella y de anillo, puede haber combinaciones de estas; por ejemplo, una topología de árbol es la combinación de una topología de bus y una de estrella.

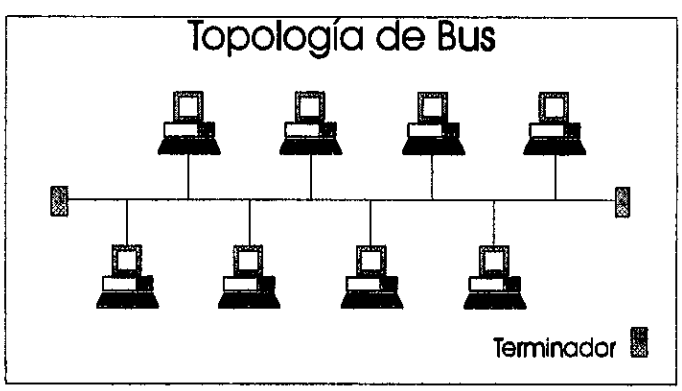


Fig. 1. Topología de bus.

En una topología de bus, cada computadora esta conectada a una parte común de la red, este se coloca con un cable que va de un lado a otro de la red y al cual se conecta cada nodo.

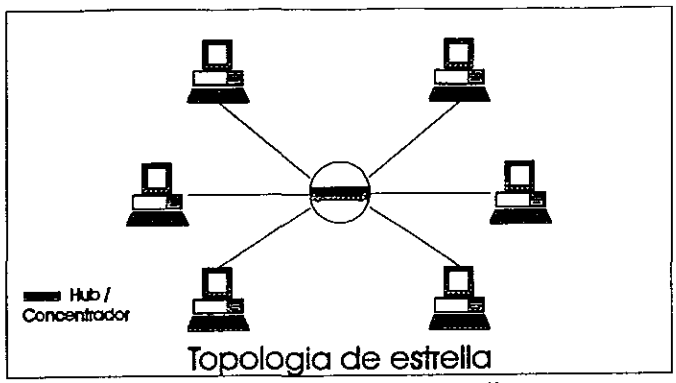


Fig. 2. Topología de estrella.

En una topología de estrella, cada computadora esta conectada a un concentrador (o hub), este es un dispositivo de hardware con varios puertos y se puede conectar un conector de cable de red en uno de ellos

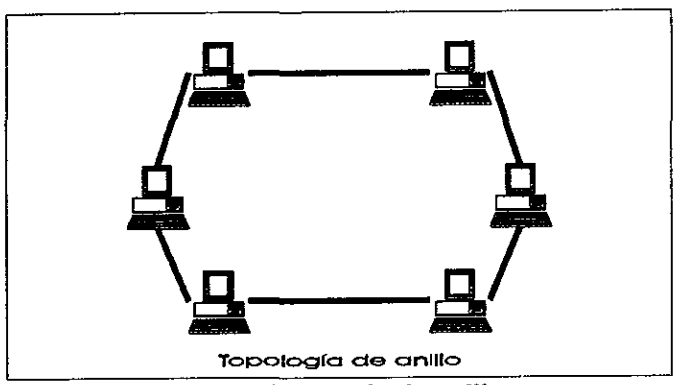


Fig. 3. Topología de anillo.

En una topología de anillo, cada terminal se conecta en forma de anillo a la red, esta casi siempre es lógica con la topología física de estrella.

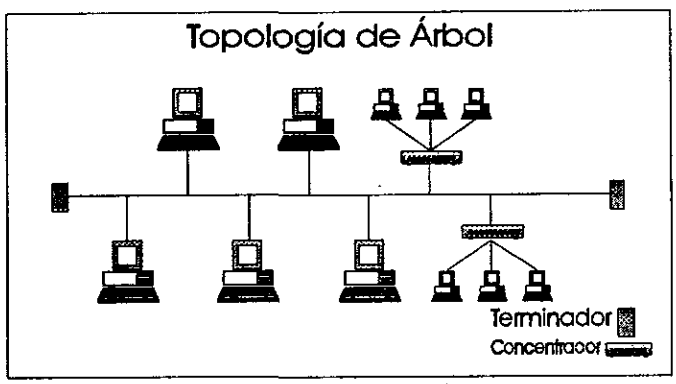


Fig. 4. Topología de árbol.

Una topología de árbol es la combinación de las topologías de bus y de estrella. Concentradores Ethernet con topología física de estrella también tienen un conector en la parte trasera que enlaza al concentrador a una red de topología física de bus.

1.4 Tipos de computadoras en una red[12].

En la mayoría de los casos, no se tiene una idea precisa al momento de evaluar qué hardware se necesita proteger de los elementos de una red, por ello se incluye esta parte.

1.4.1 Estación de trabajo.

Una estación de trabajo es una computadora capaz de aprovechar los recursos - unidades de disco o impresoras - de otras computadoras (los servidores), algunas veces puede trabajar como servidor, según las necesidades propias, la computadora en que se realiza algún trabajo puede considerarse como de este tipo

1.4.2 Servidor no dedicado.

Un servidor es una computadora capaz de compartir sus recursos con otras computadoras, estos recursos pueden ser las impresoras, unidades de disco, unidades de CD-ROM, directorios en el disco duro y archivos individuales; este puede operar como estación de trabajo y de esta manera se puede compartir sus recursos con otras computadoras.

1.4.3 Servidor dedicado.

Es un servidor que no puede ejecutar ningún otro trabajo aparte del requerido para compartir sus recursos con los nodos de la red, estos no pueden usarse como estaciones de trabajo, este tipo de servidores maneja una versión diferente de sistema operativo que optimiza la velocidad a la que se intercambian los datos entre el servidor y los otros nodos de la red, es usado solamente para las tareas relacionadas con la red, se elimina la sobrecarga adicional dando como resultado un mejor rendimiento.

1.4.4 Terminales.

Las hay de diferentes tipos: como terminales tontas (dumb terminals), estas no tienen capacidades de procesamiento, sólo acepta datos del CPU (de un servidor principal). Existen también terminales "dedicadas" (smart terminals) que constan de un monitor que tiene su propio procesador para algunas características especiales por ejemplo poner los caracteres en "negritas" y destacarlos; y las terminales inteligentes (intelligent terminals) estas tienen memoria y un procesador para desempeñar operaciones de especiales de despliegue, sirven para todo tipo de aplicaciones como procesamiento de palabras, gráficos, hojas de cálculo, comunicaciones, bases de datos, juegos, para trabajar con lenguaje ensamblador, con compiladores, con las distintas utilerías que tenga el servidor principal

1.5 Tipos de redes[10].

Estas se pueden clasificar sobre la base de su distribución geográfica, a su modo de transmisión y a la disponibilidad que tengan:

Geográficas.

Las LAN (Local Area Network), las MAN (Metropolitan Area Network) y las WAN (Wide Area Network).

En las LAN, se pueden tener varios usuarios, las máquinas pueden estar en una región geográfica pequeña (un edificio, un piso de un edificio), los canales de comunicación entre las máquinas son privados, los canales tienen alta capacidad (en MBit por segundo), además de estar libres de errores (con una tasa de 1 error por cada 10^9 bits transmitidos).

Las redes MAN son diseñadas para una parte de una ciudad o una ciudad completa. Es más grande que una LAN pero más pequeña que una WAN, se caracteriza por las conexiones de alta velocidad por medio de fibra óptica o algún otro medio digital.

Las redes WAN se caracterizan porque se pueden tener varios usuarios, las máquinas están separadas en una región geográfica muy amplia, los canales de comunicaciones son suministrados por algún proveedor (un proveedor de Internet, la compañía de teléfonos, etc.), los canales son de baja capacidad (en Kbit por segundo) además de tener una tendencia al error (con un promedio de 1 en cada 100,000 bits transmitidos).

Públicas o privadas.

Además se pueden clasificar las redes como públicas en donde una empresa renta su red al público o privadas en donde la empresa utiliza la red que ella administra.

Transmisión.

Redes de transmisión (broadcast). Transmite un sólo medio de comunicación a varios dispositivos (de uno a muchos); es decir un servidor transmite a varios receptores. Este tipo de redes se usan en donde se tengan computadoras que están muy cerca, debido a que es más fácil enviar la señal a todas las estaciones con un número pequeño de recursos.

Redes conmutadas. En donde una transmisión única es enviada a un dispositivo físico (un switch) el cual va a determinar cuál será la ruta que va a seguir la transmisión.

1.6 Especificaciones de red[12].

Son guías o reglas que se refieren al tipo de componentes que deben usarse, a la manera de conectar los componentes así como los protocolos de comunicación que se utilizan. Las especificaciones más usadas son Ethernet, Token Ring (estándares de la IEEE - Institute of Electrical and Electronic Engineers -) y la ARCnet (del ANSI - American National Standars Institute -)

1.6.1 Ethernet.

El ethernet es el estándar más popular para las LAN, este emplea una topología lógica de bus y una topología física de estrella o de bus, transmite los datos de la red a una velocidad de 10 Mbps (megabits por segundo), el método de transmisión que usa es el de Acceso Múltiple con Detección de Portadora y de Colisiones (CSMA/CD). Antes de que un nodo envíe algún dato a través de la red, primero escucha y se da cuenta si algún nodo esta transmitiendo información. En el caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de mandar el envío.

La topología lógica de bus permite que cada nodo tome su turno en la transmisión de información a través de la red, permitiendo de esta manera que no falle la red completa, pero si hay cargas puede llegar al punto de saturación. Existen tres tipos de Ethernet, 10BASE5, 10 BASE2 y 10 BASE-T, que definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar los nodos en la red.

Thicknet (10BASE5). Fue el primer ethernet que se utilizó, tiene un estándar de topología física de bus que consiste en un segmento de cable de red con terminadores en los extremos. Los terminadores incluyen una resistencia que disipa la señal de la red y no permite que se refleje de regreso al cable de red. La tarjeta de interfaz de red (NIC) en cada computadora es la interfaz de comunicaciones entre la computadora y el cable de red, y esta conectada a un transmisor-receptor (transceiver) externo por medio de un cable de suspensión. El transceiver esta conectado al segmento de cable Thick Ethernet y actúa para transmitir y recibir datos de la red entre la computadora y la red.

Thinnet (10BASE2). Se instala por medio de una topología física de bus, que consiste en segmentos de cable de red con terminaciones en cada extremo, la tarjeta de red de cada computadora esta conectada directamente al segmento de cable Thinnet, el transceptor esta integrado a la tarjeta de red.

Par Trenzado (10BASE-T). Conocido también como UTP (Par trenzado sin blindaje), se instala por medio de una topología física de estrella, cada nodo se conecta a un concentrador, y la tarjeta de red se conecta a este por medio de un segmento de cable de red. En caso de que se rompiera el cable afectaría a la computadora conectada a esa sección, este estándar es más barato para redes pequeñas pero requiere un concentrador adicional.

1.6.2 Token Ring.

Originado por el IEEE 802.5 opera a una velocidad del 4 Mbps a 16 Mbps, emplea una topología lógica de anillo y una topología física de estrella, la tarjeta de red se conecta a un cable que se enchufa a un hub central llamado unidad de acceso a multiestaciones (MAU), se basa en un esquema de paso de señales (token passing), haciendo pasar un token (o señal) a todas las computadoras de la red. La computadora que tenga el token puede transmitir información a otra computadora de la red, en cuanto termine lo pasa a la siguiente computadora del anillo, en caso de que tenga información procede a enviarla (conocido como frame).

Un frame esta constituido por:

- Delimitador de inicio. El cual consta de un código único para poder diferenciarlo.
- Control de acceso. Contiene información acerca de la prioridad del frame y una necesidad de almacenar futuros tokens que podrían garantizarse a otras estaciones si tienen una prioridad menor.
- Control del frame. Define el tipo de frame, la información MAC (Media Access Control) que puede ser leída por todas las estaciones de la red o la información para una estación específica.
- Dirección de destino. Contiene la dirección de la estación que va a recibir el frame, el cual puede ser direccionado a todas las estaciones de la red.
- Dirección de origen.
- Dato. Si es un frame MAC puede contener información de control adicional.
- Secuencia de revisión del frame. Tiene información que revisa los errores para asegurar la integridad del frame al receptor.
- Delimitador final.
- Estatus del frame. Indica si una o más estaciones del ring reconoce el frame, si es copiado o si no esta disponible la estación de destino.

1.6.3 FDDI y CDDI.

La interfaz de distribución de datos por fibra óptica (FDDI) es un estándar para la transferencia de datos por cable de fibra óptica, el estándar ANSI X3T9.5 especifica una velocidad de 100 Mbps, debido a las características de la fibra óptica de que no se degrada la señal y no

sufre de interferencia eléctrica se pueden usar cables más largos que otros estándares de red, tiene una topología lógica de anillo con paso de token, además de eso hay opción de operar un cable UTP a 100 Mbps (CDDI).

1.6.4 ATM.

El Modo de Transferencia Asíncrona es un conjunto de estándares internacionales para la transferencia de datos, voz y vídeo por medio de una red a velocidades muy altas, opera desde un rango de 1.5Mbps a 1.5 Gbps, se incorporan parte de los estándares Ethernet, Token Ring y FDDI para la transferencia de datos.

Sin embargo, hay otras tecnologías de altas velocidades que son *importantes de* mencionar pero por cuestiones de espacio y de objetividad se enlistan ventajas y desventajas en la fig. 5.

Tecnología.	Ventajas.	Desventajas.
FDDI/CDDI	➢ Es entendible y ampliamente desplegable. ➢ Tiene disponibilidad inmediata. ➢ Es conveniente para backbone. ➢ Característica ofrecida en servidores de fábrica (conectividad).	➢ Tiene un alto costo. ➢ No es escalable.
100 BASE T	➢ Efectividad en el entubamiento para los servidores y las estaciones de trabajo. ➢ Familiaridad con protocolos. ➢ Cuenta con amplio soporte.	➢ Tiende a fallar con exceso de nodos. ➢ Requiere cableado de categoría 5.
100 VGAny LAN.	➢ Adecuado para aplicaciones "delay-sensitive". ➢ Usa cableado categoría 3 "grado voz" (4 pares).	➢ No es muy usado. ➢ Soporte técnico limitado.
ATM	➢ Escalable. ➢ Puede mezclar voz, video y datos. ➢ Migración sin problemas desde token ring.	➢ Muy costoso. ➢ Poco entrenamiento. ➢ Limitadas opciones de configuración.

Fig. 5. Consideraciones importantes de tecnologías de punta en especificaciones de red.

1.7 Conectores de red.

Un conector es donde se conecta el cable de red al adaptador (por ejemplo a una tarjeta ethernet), los más comunes son:

1.7.1 10BASE5 (Thick Ethernet).

Utiliza un conector DB-15, el cual es un conector hembra tipo d de 15 pines, el cable thick ethernet se conecta a un transmisor-receptor (transceiver) externo y a su vez se conecta al DB-15 del adaptador de la red.

1.7.2 10BASE2 (Thinnet).

Conocido como conector BNC (que es muy parecido al conector para televisión), se enlaza al conector de la tarjeta del adaptador de la red con un conector TBNC. La parte inferior de la "T" esta conectada a la tarjeta adaptadora de red y las otras dos partes se encuentran conectadas a los otros nodos de la red.

1.7.3 10BASE-T (par trenzado sin blindaje).

Se utiliza un conector RJ-45, similar a los conectores que se utilizan en las instalaciones telefónicas (RJ-11); tiene ocho conductores, este conector se puede utilizar en los extremos de un cable UTP, puede servir de enlace entre la tarjeta de red y el concentrador.

1.8 Modelo OSI[35, 41].

A finales de la década de los setentas se desarrolló un modelo de referencia para interconexión de sistemas abiertos (OSI, Open Systems Interconnection). En un sistema abierto el diseño o los aspectos del sistema no son patentados, de hecho con este tipo de sistemas se proporciona la documentación y conexiones que se pueden utilizar para crear programas que ocupen o extiendan el sistema. Este modelo tiene sus orígenes en uno que era de la Organización Internacional de Normas (ISO, International Standars Organization), esta organización fundada en 1946 establece normas internacionales en todos los campos, excepto en la electrónica e ingeniería eléctrica.

Este modelo utiliza capas para organizar una red en módulos funcionales bien definidos, los diseñadores emplean las descripciones de las capas del modelo para construir redes reales, pero de acuerdo al propósito de la red se pueden hacer modificaciones del número, nombre y función de las capas; entonces, una red construida a partir del modelo OSI puede tener variaciones comparándolas con redes basadas en él. Las capas de las que esta conformado se muestran en la fig. 6.

#	Nombre
7	Capa de aplicación
6	Capa de presentación
5	Capa de sesión.
4	Capa de transporte
3	Capa de red
2	Capa de enlace (de datos)
1	Capa física

Fig. 6. Capas del modelo OSI.

En una red de capas, cada módulo proporciona funcionalidad específica o servicios a sus capas adyacentes, aparte de proteger a las capas superiores de los detalles de las inferiores. Toda comunicación entre computadoras se traduce a 1 y 0, dado que una red consta de una o más computadoras interconectadas se puede afirmar que las redes se comunican por medio del lenguaje binario, esto es conocido como un protocolo, o sea es un conjunto de reglas y convenciones para comunicarse.

En el modelo OSI se usa el nombre de la capa para identificar el protocolo, por ejemplo al protocolo de la capa de transporte se le define como protocolo de transporte. La comunicación entre capas se le llama conversación y los protocolos la definen.

Cuando dos servidores establecen comunicación, las capas correspondientes de cada uno también lo hacen, a esto se le conoce como procesos pares. La comunicación entre este tipo de procesos es conocida como comunicación virtual. Toda comunicación entre dos computadoras ocurre en la capa inferior de la red en donde existe la conexión real en hardware. Cada capa de red sigue los protocolos que definen los servicios que ofrece. Un servicio define la habilidad que la capa ofrece a la capa superior, como la detección de errores. Un protocolo, es el conjunto de reglas que la capa debe de seguir para poner en marcha el servicio.

La diferencia que hay entre un servicio y un protocolo es que un servicio de red define o describe una función y un propósito, como la detección de errores. Un protocolo de red describe el formato y la estructura del paquete de datos que los módulos del software de red emplean para proporcionar el servicio. En el caso del servicio de la detección de errores, el protocolo define las condiciones de error que detecta el servicio.

Lo mismo ocurre cuando una capa de red solicita algún servicio a la capa de arriba, los protocolos de las capas definen el formato de los paquetes y la estructura de datos que deben usarse para el servicio solicitado, al final todas estas solicitudes fluyen hacia abajo, a la capa física en donde se convierten en paquetes de datos.

1.8.1 Modos de servicio.

Estos son los distintos métodos que pueden emplear para proporcionar los mismos servicios de comunicación entre procesos pares, especificando cómo la capa ejecuta una operación. Un modo de servicio puede modificar errores, pero otro no; cuando se desee que un servicio ejecute una operación de manera determinada, se debe de especificar un protocolo que proporcione ese modo de servicio.

Los principios más importantes para desarrollar las capas en el modelo OSI son:

1. Se crea una nueva capa cada vez que el programa de red necesite un nivel de abstracción distinto.
2. Cada capa debe desempeñar una función bien definida.
3. Elegir la función de cada capa revisando la definición de protocolos estandarizados internacionalmente.
4. Elegir los límites de la capa para minimizar el flujo de información a través de las interfaces.
5. El número de capas debe ser lo suficientemente grande para que los diseñadores no necesiten colocar funciones distintas en la misma capa. De cualquier modo, el número de capas no debe ser tan grande como para que sea difícil de manejar. Pero cada capa realiza ciertas funciones:

1.8.2 Capa física.

Transmite datos a través del canal de comunicación de la red, determina las propiedades mecánicas y eléctricas de dicho canal y los procedimientos; es decir, cuántos pines o cables eléctricos utiliza una conexión de red, qué tipo de cables emplea la línea de transmisión y qué características tiene esta. Se determina cuál frecuencia de señal analógica representa un 1 y cuál un 0, se asegura esta capa de que el host de destino reciba cada dígito binario representando un 1 como un 1 (sincronización); además de que revisa si las transferencias de datos emplean modos de comunicación simplex, half-duplex o full duplex, incluyendo las señales de control, aquí se incluyen también las tecnologías de red (Ethernet, ARCNET y Token Ring) que definen parámetros para transmitir datos.

1.8.3 Capa de enlace.

Transfiere datos en bruto entre la capa física y la capa de red (tramas de datos), estas tramas tienen diferentes formatos dependiendo del protocolo utilizado; por ejemplo, una trama ethernet tiene las siguientes partes: preámbulo, dirección destino, dirección fuente, tipo de trama, datos de la trama y comprobación de redundancia cíclica. La tarjeta de interface de red representa el enlace de datos de la computadora. La función principal de la capa de enlace es evitar que la información dentro de la capa física se corrompa.

Ayuda a localizar la definición de información que fluye entre la capa física y la capa de red, minimizando el flujo de la información a través de los límites entre las capas físicas y de red. Por último, la capa de enlace permite ubicar estas funciones relacionadas en una capa propia; de otro modo necesitarían coloca arbitrariamente cada función en la capa física o en la red.

1.8.4 Capa de red.

Esta capa distribuye unidades de datos como paquetes individuales, los cuales contienen las direcciones de destino y de la fuente para fines de enrutamiento, esto se hace con ayuda de tablas en donde se buscará la mejor trayectoria de la ubicación actual de un paquete a cualquier destino en la red.

Define la interface entre las computadoras y toda la conmutación de paquetes que hay entre la dirección de origen y de destino. Verifica que los paquetes sean los correctos y la secuenciación adecuada.

1.8.5 Capa de transporte.

Conduce los datos al programa o aplicación correcta entre dos computadoras, maneja todos los problemas de administración de tráfico relacionados con el enrutamiento y la entrega. Divide los datos que vienen de la capa de sesión en partes más pequeñas para la capa de red, interactua y administra los datos para muchos programas en modo simultáneo. Administra la capacidad de transferencia (ancho de banda) basándose en la conexión de transporte pudiendo multiplexar (combinando varias señales en un solo canal de comunicación) y demultiplexar (el proceso inverso).

1.8.6 Capa de sesión.

Establece las conexiones entre los procesos y aplicaciones en diferentes hosts determinándose las tasas y el tipo de transferencia de datos (simplex, half duplex o full duplex) y el control de errores, además de manejar posibles cambios (ya sea por error o por necesidades de la aplicación). Autentifica ambos extremos del enlace y estos establecen una autorización para

usar la conexión o sesión especificada. A grosso modo, esta capa es la interface entre el usuario y la red.

1.8.7 Capa de presentación.

Maneja las conversiones de representación de datos; por ejemplo, es responsable de convertir entre el formato EBCDIC y ASCII; maneja detalles relacionados con la interface de red e impresoras, monitores y formatos de archivos; es decir, especifica cómo los datos van a aparecer al usuario.

Ofrece los servicios de cifrado de datos, asegurándose los programas de que los datos se cifran antes de ser visibles a las otras capas de red; la compresión de datos, reduciendo así la cantidad de datos que debe transportar la red; el ancho de banda, en donde se puede manejar con la ampliación del canal de comunicación o reducir el tamaño de los datos que debe transportar la red. Es muy usado el ASN.1 (Abstract Syntax Notation 1) para los formatos de expresión de datos en un formato de una computadora independiente.

1.8.8 Capa de aplicación.

Abarca las aplicaciones como un ASE (Application Service Elements), permite la comunicación entre aplicaciones por medio de capas más bajas. Las tres más importantes son:

ACSE Association Control Service Element. Asocia los nombres de las aplicaciones con otra para preparar la comunicación de aplicación a aplicación.

ROSE Remote Operations Service Element. Implementa mecanismos genéricos de requerimiento-respuesta que permita las operaciones remotas de manera similar como las llamadas de procedimiento remoto (RPC)-

*RTSE A*yuda a asegurar la distribución facilitando la construcción de capas de sesión.

1.9 Tipos de conexión[36].

SLIP (Serial Link Internet Protocol). Es un servicio único ofrecido por la mayoría de los proveedores de Internet; se puede accesar a un host de Internet sin tener una conexión directa. La conexión se realiza por medio de líneas telefónicas, con un módem de alta velocidad, este tipo de conexiones permite una dirección IP temporal; todas las transferencias de archivos pueden llegar a la PC - por ejemplo -, y las sesiones de Telnet pueden ser originadas desde el sitio al que nos conectamos. La ventaja de esto es que se puede seguir operando con la interface estándar de la máquina de donde se origine la conexión, sin las complicaciones que la emulación de terminal genera en conexiones más lentas.

Conexión directa. Esta es la mejor opción para una empresa que tiene un tamaño medio o mayor en donde se necesiten acceso completo a Internet. La conexión es hecha con un dispositivo que se llama router o ruteador a la LAN, en este nivel, la decisión de tomar el grado de servicios relacionándolos con el ancho de banda de la conexión física, son usadas por Network backbones y conexiones muy grandes para corporativos y universidades

1.10 El protocolo de comunicación TCP/IP[8].

El motivo que me orilla a hablar del protocolo TCP/IP es debido a que es el lenguaje de Internet. Es una familia de protocolos y dependiendo de las necesidades que se tengan; ya sea telnet, para realizar conexiones remotas a otro servidor; ftp, para la transferencia de archivos; http, para ver información en hipertexto (WWW) entre otros.

Esta forma de comunicación, como cualquier otra tiene fallas de seguridad, por tanto es importante conocer su funcionamiento (a manera de comando o una descripción corta). Además de que esta información puede ser complementaria para otros intereses distintos a los de la seguridad.

Internet comúnmente usa el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) para las comunicaciones. Fue creado inicialmente para ayudar en las comunicaciones entre el gobierno y los investigadores. Durante los años 80's se incluyeron las organizaciones de educación, agencias del gobierno, organizaciones comerciales y organizaciones internacionales. En los años 90's se marco el boom, el crecimiento es demasiado rápido que cualquier otra red que se haya creado (como la red de teléfonos) Varios millones de usuarios están ahora conectados al Internet. Además forma parte de la NII (National Information Infrastructure) de los E.U.

1.11 Servicios comunes de Internet (servicios TCP/IP)[1,8,23].

Hay servicios asociados con el TCP/IP y el Internet, el más usado es el e-mail (correo electrónico), ejecutado por el SMTP (Simple Mail Transfer Protocol); también el telnet (terminal emulation) para acceso a terminales remotas y el FTP (File Transfer Protocol) de uso intensivo. Sobre eso, hay otros servicios y protocolos que son usados para impresiones remotas, archivos remotos y compartición de discos, bases de datos distribuidas o administrativas y para servicios de información. Estos son:

SMTP. Simple Mail Transfer Protocol. Que es usado para mandar y recibir correo electrónico de un servidor a otro; los mensajes pueden ser recibidos con un cliente de correo usando el POP (Postal Office Protocol). Además es usado para enviar mensajes de un cliente de correo a un servidor de correo, esto se debe a que se tiene que especificar el servidor POP o IMAP y el servidor SMTP cuando se configure la aplicación de correo electrónico.

TELNET. Usado para conectar sistemas remotos por medio de la red, utiliza características de emuladores de terminal básicos.

FTP. File Transfer Protocol. Usado para recibir o almacenar archivos en sistemas de red (los dos últimos comandos se explican más adelante).

DNS. Domain Name Service, es utilizado por el telnet, FTP y otros servicios para traducir nombres de servidores (dirección alfanumérica) a la dirección IP (Dirección alfanumérica). Debido a que los nombres de los dominios son alfabéticos (son más fáciles de recordar) y a que las direcciones de Internet están basadas en direcciones IP. Cada vez que se use un nombre de dominio el DNS lo convertirá a su respectiva dirección IP. Este tipo de servicios se encuentran en algún servidor DNS, en caso de que no conozca la dirección IP, preguntará a otro servidor hasta que sea encontrada la dirección correcta.

Servicios de información:

Gopher. Browser de información de menú y servidores que ofrecen una interface amigable para otros servicios de información básicos.

WAIS. Wide Area Information Service. Usado para indexar y buscar en bases de datos.

WWW/http World Wide Web/HyperText Transport Protocol. Es un sistema de servidores de Internet que pueden soportar documentos con un formato especial, estos tienen un formato de un lenguaje llamado HTML (HyperText Markup Language) que permite enlaces a otros documentos como archivos de gráficos, de vídeo y de audio, permitiendo de esta manera se

pasa de un documento a otro con sólo dar un click en la sección de interés. No todos los servidores de Internet forman parte del WWW.

Servicios RPC (Remote Procedure Call):

NFS Network File System, es un sistema abierto diseñado por Sun Microsystems que permite a todos los usuarios de una red accesar a archivos almacenados que se deseen compartir entre diferentes computadoras, ofrece el acceso mediante una interface llamada VFS (Virtual File System) que se ejecuta sobre el TCP/IP; los usuarios pueden manipular los archivos compartidos como si estuvieran en el servidor de manera local. Con el NFS, los servidores conectados en la red operan como un cliente mientras accesan los archivos remotos, y como servidores cuando los usuarios remotos accesan a los archivos locales que están compartidos.

NIS Network Information Services, hace la administración de la red más manejable ofreciendo control centralizado sobre una gran variedad de información de la red. NIS almacena información de los nombres de las estaciones de trabajo, sus direcciones y acerca de los usuarios, esto es conocido como espacio NIS.

Sistema X Window, desarrollado por el Instituto Tecnológico de Massachusetts (MIT Massachusetts Institute of Technology) es un sistema gráfico de ventanas y un conjunto de librerías de aplicación para usarse en las estaciones de trabajo UNIX, algunas otras interfaces gráficas como el Motif y el Open Look están basadas de X Window. Actualmente se encuentra a disposición la versión X11R6.4.

Los servicios "r" como el rlogin, el rsh, etc.; que emplea un concepto de hosts de mutua confianza para ejecutar comandos en otros sistemas sin requerir un password para accesar.

El TCP/IP puede ser usado en una red de área local (LAN) o en ambientes de áreas grandes, para compartir archivos e impresiones en los niveles de la LAN, para correo electrónico y para acceso a terminales remotas como en los niveles de la red local o en la red geográfica.

Para una mejor comprensión del TCP/IP, se muestra un diagrama en el cual se ejemplifica como esta estructurado este protocolo:

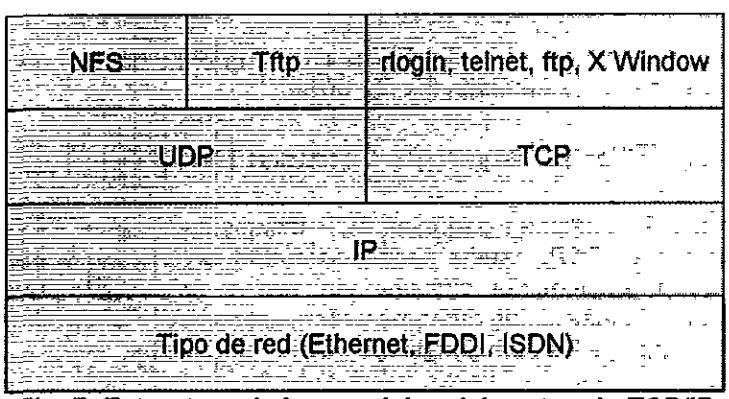


Fig. 7. Estructura de los servicios del protocolo TCP/IP.

1.12 Servidores en Internet.

Muchos servidores que están conectados a Internet corren bajo una versión del sistema operativo UNIX. El TCP/IP fue implementado primeramente en los 80's en la versión de UNIX desarrollada por la University of California at Berkeley conocido como el BSD (Berkeley Software

Distribution). Varias versiones modernas del UNIX se basaron del código fuente del BSD. Este UNIX provee un conjunto de servicios TCP/IP. Esta clase de estándar ha resultado en muchas versiones diferentes de UNIX con la misma vulnerabilidad - tratada más adelante -, sin embargo, ofrece medios comunes para implementar estrategias de firewalls como un filtrado de paquetes de IP.

UNIX no es el único sistema operativo, por ejemplo esta el VMS, NeXT, sistemas operativos de mainframe y S.O. de P.C. como el DOS o el sistema que soporta las computadoras Apple. Algunos sistemas de PC únicamente ofrecen servicios de cliente; por ejemplo, sólo puede usarse el TELNET para conectarse "desde" y no "a" otra PC, incrementando el poder de estas e inicialmente ofrecen a bajo costo los mismos servicios que en servidores de gran capacidad. Versiones de UNIX para PC como el Linux, FreeBSD y otros como el Windows NT ofrecen los mismos servicios y aplicaciones que este.

1.13 Usos del TCP/IP[8].

Parte de la popularidad del TCP/IP radica en que tiene la habilidad de implementar sobre una variedad de canales de comunicación y protocolos de bajo nivel como el T1 (transmite 1.5 Mbits por segundo) y el X.25, ethernet y líneas seriales de control RS-232. Muchos sitios usan las conexiones ethernet en una LAN para conectar los servidores y los sistemas de clientes, y son conectados a la red por medio de una línea T1 a una red regional (soporte TCP/IP) que conecta a otras redes organizacionales y soportes, hay sitios que ofrecen dos o más conexiones. Las velocidades de los modems se incrementan como los estándares de comunicación son aprovechados, estas versiones operan bajo la red de teléfonos conmutada que son más populares. Otros sitios y personas usan el PPP (Point-to Point Protocol) y el SLIP (Serial Line IP) para enlazar redes y estaciones de trabajo con otras redes usando la red conmutada de teléfonos.

Es más correctamente una serie de protocolos que incluye el TCP, IP, UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) y algunos otros.

1.13.1 IP (Internet Protocol)[9,1].

El IP recibe los paquetes de un estrato de bajo nivel como una tarjeta de Ethernet y pasa los paquetes hacia un estrato de nivel alto como el TCP o UDP.

Los paquetes IP son datagramas informales en que el IP no hace el chequeo de estos, son puestos en orden secuencial o no son dañados por errores.

1.13.2 TCP (Transport Control Protocol)[8,1].

Si los paquetes IP contienen paquetes TCP encapsulados, el software IP puede pasar hacia un estrato superior de TCP, ordena secuencialmente los paquetes y el desempeño de la corrección de errores, e implementa circuitos virtuales o conexiones entre servidores. Los paquetes TCP contienen secuencias de números y respuestas de paquetes recibidos y que los que están en desorden se corrijan y los dañados puedan ser retransmitidos.

El TCP pasa esta información a estratos de aplicaciones de alto nivel como un cliente o servicio de telnet, las aplicaciones pasan información tras el estrato del TCP el cual pasa la información bajo el estrato del IP.

Los servicios de conexión orientados, como el telnet, el FTP, rlogin, X Window y SMTP requieren un alto grado de confiabilidad y utilizan el TCP. El DNS lo ocupa en algunos casos (para

transmitir y recibir bases de datos de nombres de dominios), pero usa el UDP para transmitir información acerca de servidores individuales.

1.13.3 UDP (User Datagram Program)[8,1].

Interactúa con programas de aplicaciones en el mismo estrato que el TCP. Sin embargo, esto no es un error de corrección o retransmisión de paquetes desordenados o perdidos. Es usado para servicios que requieren una orientación de colas como el NFS, donde el número de mensajes relacionados con el intercambio es pequeño comparado con el telnet o el FTP. Los servicios que usan el UDP requieren los servicios básicos de RPC como el NIS y NFS, NTP (Network Time Protocol).

1.13.4 ICMP (Internet Control Message Protocol)[8,1].

Detecta las condiciones de error y los reporta, estos eventos pueden ser:

- Fallas de conectividad cuando el host de destino no puede ser "conseguido" (en cuanto a la dirección).
- Paquetes caídos es cuando los paquetes arriban muy rápido para ser procesados.
- Su propósito es transmitir la información necesaria para controlar el tráfico IP. Es usado principalmente para proveer información acerca de rutas de direcciones de destino.
- Redireccionar la información de los mensajes de hosts a otras rutas a otros sistemas.

1.14 Direcciones en Internet (IP Adress)[8].

Cada máquina si tiene acceso a Internet contar con una dirección distinta , como una dirección de una casa, para que la información destinada a esta pueda llegar a tiempo y con éxito. El esquema de la dirección esta controlada por el protocolo Internet (IP, Internet Protocol).

La dirección consiste de dos partes, el nombre del servidor o la estación de trabajo y el dominio al que pertenezca que describe a la red en donde se encuentra el servidor. Para asegurarse de que las direcciones sean únicas, una agencia central es responsable de la asignación de las mismas. Hay varios tipos de direcciones (Fig. 8) que se pueden emplear.

Direcciones clase A.	(1.0.0.0-127.0.0.0)
Direcciones clase B.	(128.0.0.0-191.0.0.0)
Direcciones clase C.	(192.0.0.0-253.0.0.0)

Fig. 8. Tipos de direcciones IP.

Además de direcciones especiales que son las máscaras de red:

Dirección.	Descripción.
Num.num.num.0	Identifica a la red completa.
num.num.num.255	Todos los anfitriones en la red especifica (dirección de la emisión)
255.255.255.255	Todos los anfitriones emiten hacia las redes actuales.

De acuerdo con la clase de red, pueden haber desde 253 hasta millones de anfitriones en una red. Pero como no se puede restringir el acceso de un tipo de red a otro, se desarrollaron las subredes, con el objetivo de dividir la porción del anfitrión de la dirección en redes adicionales.

Las subredes trabajan al tomar la porción de anfitrión de la dirección y la dividen luego por una máscara de red. Esta máscara mueve la línea divisoria entre la red y los anfitriones de un lugar a otro dentro de la dirección. Esto tiene el efecto de aumentar el número de redes disponibles, pero reduce el número de anfitriones que pueda conectarse con cada red.

Esto ofrece algunas ventajas. Varias organizaciones pequeñas sólo pueden obtener una dirección de clase C, pero que tienen oficinas que necesitan conectarse entre sí desde lugares remotos. Si cuentan con una sola dirección IP, un ruteador no podrá conectar al menos dos lugares, dado que se requiere que existan dos direcciones distintas; por medio de la división de redes en subredes estás pueden utilizar al ruteador para conectarse al ruteador ya que cuentan con direcciones de red distintas.

La subred se interpreta mediante la máscara de red o subred; si el bit está en posición de encendido en la máscara de red, ese bit equivalente en la dirección se interpreta como un bit de red; si el bit se encuentra en posición de apagado se le considera parte de la dirección del anfitrión; esto se establece en forma local, para el resto de Internet se ve como una dirección IP estándar.

1.14.1 Direcciones alfanuméricas[8].

A cada estación de trabajo conectada a Internet se le debe de asignar una dirección IP única, pero la mayoría de las veces son difíciles de recordar. Debido a esto se les asigna una dirección alfanumérica, la cual también permite conectarse al servidor deseado.

Para que el TCP/IP pueda desempeñarse, el nombre del servidor debe traducirse a la dirección IP correspondiente. Esto se logra con ayuda de un servidor de nombre de dominio (DNS, Domain Name Server).

Este nombre debe ser único y consiste de dos partes: el nombre real y el dominio. El dominio se asigna mediante un registro central que depende del país en el que se encuentre el servidor y el tipo de organización que se desea registrar. Los dominios más usados son el .com para empresas comerciales, .edu para centros de educación y .gov para oficinas de gobierno de los E.U.

A este respecto, el RFC 1178 (Request For Comment) sugiere una serie de lineamientos sobre la manera en la que hay que llamar a un sistema como:

- Utilizar palabras reales que sean cortas, fáciles de deletrear y de recordar, debido a que son más fáciles de recordar y de usar. Si tuvieran las características opuestas, anularían su finalidad.
- Que sean nombres temáticos, pueden ser verbos, nombres de caricaturas, comidas o cualquiera.
- El uso de nombres de proyecto, personales acrónimos deben ser evitados.

1.15 Utilerías de TCP/IP (Comandos de UNIX)[1,8,11].

1.15.1 Introducción.

Este protocolo es muy complejo debido a su amplia difusión en el mundo para interconectar las redes de distintas empresas con diferentes giros, utiliza varias opciones para entablar la comunicación entre servidores; es necesario conocer estos medios de comunicación ya

que es ahí en donde se originan parte de los problemas de seguridad. En esta sección se ponen los comandos que están implicados en este problema (y los de que alguna manera pueden monitorear las actividades de estos).

1.15.2 ping.

Su nombre se origina de un dispositivo de detección sonar que utiliza un pulso de sonido para localizar objetos en el área circundante. Es utilizado para enviar paquetes con el protocolo de control de mensajes de Internet (ICMP) de un servidor a otro. Este comando transmite los paquetes mediante el uso del comando ICMP ECHOP_REQUEST y espera obtener su contraparte de respuesta a cada paquete transmitido.

Su sintaxis es:

ping host [timeout]

En donde host es el nombre de la máquina en cuestión, la opción timeout indica el tiempo en segundos del tiempo de reinicio de la máquina 20 segundos por default.

opciones

-s Detecta la pérdida de paquetes y corrige el problema.

1.15.3 ruptime.

El comando ruptime utiliza las cualidades del servidor rwho para mostrar el estado de las máquinas locales en una red. Este comando imprime una línea de estado para cada anfitrión en su base de datos. Esta se construye mediante el uso de paquetes de emisión rwho, una vez cada uno o tres minutos. Las máquinas que no hayan informado de un estado en cinco minutos se señalarán como no activas. En caso de que no este activo el servidor rwho mostrara el mensaje de no hosts y se termina (las opciones de este comando se encuentran en la fig. 9), su sintaxis es:

ruptime [opciones]

Opciones	Descripción
a	Contabiliza a cada usuario que tienen un Id de una hora o más.
l	Formato corto del promedio encontrado.
r	Invierte el formato corto.
t	Muestra el despliegue en base al tiempo.
u	Muestra el despliegue en base al número de usuarios.

Fig. 9. Opciones de comando ruptime.

1.15.4 rwho.

El comando rwho hace una lista con los usuarios que se encuentran registrados en cada uno de los servidores de la red. Este comando muestra una salida similar al who, pero de todas las máquinas de la red, si no recibe un reporte de las estaciones en un lapso de 5 minutos considera a la misma que esta apagada.

-a Reporta a todos los usuarios si o no están en el sistema en la pasada hora.

1.15.5 finger.

Lista el login, el nombre completo, nombre de la terminal y estado de escritura de la terminal, tiempo de inactividad, tiempo de registro, situación de la oficina y número de teléfono (sí es conocido) para cada usuario activo; como despliega información valiosa del usuario se ha

optado deshabilitar su uso en algunos sitios. Las opciones para este comando se encuentran en la figura 10. Al ejecutar este comando despliega la siguiente información:

El nombre del usuario.
El nombre completo.
El nombre de la terminal (con un asterisco en caso de que los permisos de escritura estén negados).
El tiempo de identificación.
El nombre del host si esta realizando una conexión remota.

Opciones	Descripción.
-b	No imprime el directorio de trabajo del usuario y el shell.
-f	No imprime el encabezado.
-h	No imprime el contenido del archivo .project.
-i	Obliga a que el idle aparezca en el formato de la información, en donde es similar al formato corto, pero con el nombre, la terminal, el tiempo de conexión y el tiempo de identificación.
-l	Muestra el formato largo.
-m	Los argumentos son el nombre del usuario (en vez de los nombres y apellidos).
-p	Suprime la impresión del archivo .plan en el formato largo.
-q	Muestra el formato rápido (nombre, termina y tiempo de trabajo).
-s	Muestra el formato de salida corto.
-w	No muestra el nombre completo del usuario.

Fig. 10. Opciones del comando finger.

la sintaxis es:

finger [opciones] usuario@host

1.15.6 netstat.

Se utiliza para monitorear ciertos tipos de información en el subsistema de red. Despliega el estado de TCP, UDP, ICMP e IP en listas de tablas de enrutamiento, activar conexiones, flujos en uso y algunos otros dependiendo del sistema que este usando.

La sintaxis del comando es:

netstat [-a] [-m] [-n] [-s] [-i] -r] [-f familia_de_direcciones]

-a Despliega el estado de todos los sockets y todas las entradas de las tablas de enrutamiento, la interface, el host, la red y el ruteador predeterminado.

-i Despliega el estado de la interface de la red.

-r Despliega el estado de la tabla de enrutamiento.

-s Muestra estadísticas por protocolo, si se combina con –M despliega las estadísticas del ruteo multicast.

-n Muestra las direcciones de la red como números

-m Muestra las estadísticas STREAMS

-f Reporta estadísticas limitadas o bloques de control de direcciones en donde se especifica la "familia_de_direcciones", las cuales pueden ser:

inet Para la familia de dirección AF_INET
unix Para la familia de direcciones AF_UNIX

1.15.7 ifconfig

Despliega información acerca de la configuración de una interfaz específica y es usado para asignar una interfaz de red, sin opciones se define la dirección de red de todas las interfaces que tenga la computadora; si una "familia de protocolos" es especificada, despliega información relacionada a esta; como administrador se puede modificar la configuración de una interfaz de red.

La sintaxis es:

ifconfig interfaz [familia de protocolos]

Interfaz. Esta opción puede ponerse de dos maneras:

Unidad	Nombre
Física	le0
Física-lógica	le0:1

1.15.8 traceroute

Se utiliza para rastrear la ruta que debe seguir un paquete para llegar a su destino, trabaja mediante el uso del campo del tiempo de vida (TTL, Time To Live) del protocolo IP para provocar una respuesta ICMP TIME_EXCEEDED de cada compuerta a lo largo de la ruta hasta el anfitrión remoto. Las opciones para este comando se encuentran en la figura 11, la sintaxis puede ser la siguiente:

traceroute [-m max_ttl] [-n] [-p puerto] [-q ncolas] [-r] [-s src_addr] [-t tos] [-w tiempo_espera] host [tamaño_paquete]

Opciones	Descripción
-m	Máximo número de intentos a usarse en las pruebas de paquetes, el valor predeterminado es de 30 intentos (el mismo que es usado para las conexiones TCP).
-n	Imprime las direcciones numéricas tomadas del servidor de nombres.
-p	El número de puerto UDP usado para las pruebas (el predeterminado es el 33434), no espera respuesta en los puertos UDP que escuchan, puede usarse un puerto diferente.
-r	Despliega las tablas de enrutamiento y las envía directamente al host sobre la red adjunta, si el host no se encuentra directamente en la red generara un mensaje de error.
-s	Esta opción permite usar la dirección IP numérica como la dirección de origen para que la dirección IP de las interfaces donde se prueba el paquete que se envía.
-t	El tipo de servicio del que se van a probar los paquetes para el valor deseado que puede variar de 0 a 255, esta opción puede ser usada para ver el resultado de diferentes tipos de servicios en diferentes rutas.
-v	Modo verbose, se reciben los paquetes ICMP con el parámetro de TIME_EXCEEDED y UNREACHABLE.
-w	Se indica el tiempo en segundos para esperar la respuesta a la prueba (el valor predeterminado es de 3 segundos).

Fig. 11. Opciones del comando traceroute.

1.15.9 arp

Despliega y modifica la tabla de traslado de dirección Internet a ethernet, la cual por lo general se mantiene por el protocolo de resolución de dirección (arp). Cuando el único argumento es un nombre de servidor, se despliega la entrada ARP actual para ese servidor. Si no se encuentra en la tabla ARP actual, entonces este comando despliega un mensaje. Es utilizado para ayudar a depurar y diagnosticar problemas de conexión de la red. Esto se hace asignando la dirección Ethernet para un servidor dado. En la figura 12 vienen las opciones más comunes del comando arp.

Opciones.	Descripción
-a	Despliega todas las entradas actuales ARP. Las opciones que despliega son:
	P Publish, en donde se enlistan las direcciones IP del host y las direcciones que están añadidas con la opción -s. U Unresolved; espera por una respuesta ARP. M Mapping; Solo es usada por la entrada multicast desde la dirección 224.0.0.0 S Static; No es conocida desde el protocolo ARP.
-d	Borra una entrada desde el host. Esta opción sólo puede utilizarla el superusuario.
-f	Lee el archivo llamado filename y un conjunto de entradas múltiples en las tablas ARP. Estas entradas pueden ser de la forma host dirección_ethernet [temp] [pub] [trail]
-s	Crea una entrada ARP desde el host con la dirección ethernet, esta es un número separado por seis bytes hexadecimales separados por comas, esta entrada puede ser permanente a menos de que la palabra temp es puesta en el comando. Si es pub, la entrada se publica. Este sistema responda los requerimientos ARP del host si no es el mismo. trail indica que las encapsulaciones trailer pueden ser enviadas a este host. Esta opción puede ser utilizada por un proxi ARP cuando un host uno de los que se encuentran en la red no esta físicamente presente en la subred. Otra máquina que puede estar configurada para responder a estos requerimientos, es usada en configuraciones SLIP o PPP.

Fig. 12. Opciones del comando arp.

1.15.10 rlogin

Conecta la sesión local con una sesión remota en un servidor diferente, intenta identificar al usuario en el host remoto. Si no se suple con un id de usuario usando la opción –l (o –l para otras versiones del S.O.), el identificador de usuario local es el que se usará durante este proceso.

Si el host remoto no tiene un equivalente en el host de origen en el archivo "$HOME/.rhost" –explicado en la sección 1.17.2- se pedirá el password en el host remoto. Ya conectado el shell local se inhibe y se activa el remoto, para finalizar la sesión basta con presionar la combinación de teclas Control-D (^D) y regresará al usuario en el host local. La sintaxis es:

rlogin -ec [-l userid] host

-ec Se especifica un carácter de escape distinto "c", para la línea usada para desconectarse del host remoto.

-l Con esta opción se especifica un *userid* diferente para el servidor remoto.

1.15.11 rcp

Es un comando de copia remota, le permite al usuario copiar un archivo desde un servidor a otro. Su sintaxis es:

rcp [-p] archivo1 archivo2
rcp [-p][-r] arch... directorio.

Para el archivo remoto:

servidor_remoto:archivo

El archivo nombrado se copia hacia o desde el servidor remoto. Puede especificarse una ruta de directorio para copiar un archivo en específico. (-r).

Con la opción –p intenta que cada copia tenga el mismo tiempo de modificación, tiempo de acceso, modos y el ACL (Access Control List) en caso de que se aplique como el archivo original.

1.15.12 rsh

En algunos sistemas puede ser remsh o rcmd y sirve para ejecutar un comando en un sistema remoto. Copia su entrada estándar al comando remoto, la salida estándar del comando remoto a su salida estándar, y el error estándar del comando remoto al local. Su sintaxis es:

rsh [-l userid] host [comando]

1.15.13 telnet

Este comando tiene la capacidad de establece una conexión de doble vía con un puerto remoto. Si se omite al nombre del host pero se pone el puerto, se conectará al servidor telnet del host actual, el cual permite identificarse en la máquina remota, si no se agrega nada, entra directamente al modo de comando:

telnet>

Para entrar al modo de comando después de establecer una conexión, se presiona la combinación de teclas control] (^]) que es la secuencia para salir de telnet, y se posiciona en el modo de comando.

Su sintaxis es:

telnet [host [puerto]]

1.15.14 ftp (File Transfer Protocol)

El protocolo de transferencia de archivos es un protocolo genérico para la transmisión de archivos y tiene soporte para varios tipos de computadoras, se puede usar la transferencia de archivos desde el host actual a cualquier otro host remoto del cual se conozca la dirección de Internet del servidor ftp del host remoto. Permite manipular archivos y directorios en el host local y en el host remoto, y busca identificar al usuario en el host remoto con la identificación que tiene en el host actual, si no se cuenta con una cuenta anónima, se asume que se tiene una cuenta en ese host. Si es exitosa la identificación entra en el modo de comando (**ftp>**). Si no se especifica algún nombre de host, se coloca en el modo de comando para poder usar las opciones con que se cuenta. Su sintaxis es:

ftp [host]

1.15.15 spray

Este comando envía cadenas de una vía al host utilizando RPC, reportando cuantos paquetes se recibieron y cuál fue la transferencia promedio. Puede llevar cualquier tipo de dirección. Su sintaxis es la siguiente:

spray –c cantidad –d retardo –l –t nettype host

-c cantidad	Se especifican cuantos paquetes van a enviarse. El valor por default es de 100000 bytes.
-d retardo	Se especifica cuantos microsegundos de espacio se tendrá entre cada paquete enviado. El default es 0.
-l longitud	Este parámetro es el número de bytes en los paquetes Ethernet que permite llamar un mensaje RPC. Los datos son codificados usando el XDR en cantidades de 32 bits; si el tamaño es mayor a 1514 no puede encapsular como Ethernet. El valor por default es de 86 bytes (que es el tamaño de los encabezados de RPC y UDP).
-t nettype	Especifica la clase de transportes.

1.16 Archivos de configuración de red[8,37,44].

Estos archivos son utilizados por diversos comandos y utilerías, es muy probable que alguno de ellos sea utilizado para poder accesar al host desde Internet. Todos estos archivos se encuentran en el directorio /etc.

1.16.1 hosts.

Proporciona un nombre a la estación de trabajo o servidor, según sea el caso a la dirección IP. El empleo de estos nombres es por conveniencia y facilidad de uso. Cuando se utiliza un nombre de anfitrión. TCP/IP examina el contenido del archivo para encontrar la dirección IP para el servidor. Su formato es:

dirección *nombre oficial* *alias...*

Las columnas se refieren a la dirección IP, el nombre de dominio oficial y cualquier alias para la máquina.

Los alias incluyen la forma corta del nombre del servidor. Las rutinas de búsqueda evitan el texto inmediato a "#" que representa un comentario, así como líneas en blanco.

1.16.2 ethers.

Después de leer la dirección IP, es convertida en la dirección del hardware real cuando el anfitrión está en la red local. Esto se hace mediante el protocolo *ARP* o mediante la creación de una lista de todas las direcciones ethernet en el archivo *ethers*. El formato de ese archivo es la dirección ethernet seguida del nombre oficial del anfitrión, por ejemplo:

# Ethernet Address	Host Name
8:0:20:0:fc:6f	cronos

La información de este archivo es usada por el demonio *rarpd*. Sigue la forma de x:x:x:x:x:x donde x es un número hexadecimal que representa un byte en la dirección. Los bytes de dirección están siempre en orden de red y deberá de existir una entrada en el archivo del servidor para cada dispositivo de ese archivo.

1.16.3 networks.

Contiene una lista de direcciones IP y nombres para las redes en Internet. Cada línea brinda la información para una red específica o servidor en específico.

```
# NETWORK NAME                    IP ADDRESS
localhost                         132.248.80.194
condor.dgsca.unam.mx              132.248.10.3
```

Consiste de lo siguiente: dirección de red IP, el nombre para la red y cualquier alias.

1.16.4 protocols.

Almacena una lista de protocolos DARPA. Este archivo no deberá ser cambiado, puesto que brinda la información del DDN, cada línea contiene el nombre, el número y cualquier alias para el protocolo.

La sintaxis de este archivo es:

Nombre del protocolo *puerto* *alias*

Un emjemplo se muestra a continuación:

```
#
# Internet (IP) protocols
#
ip      0     IP        # Internet protocol, pseudo protocol number
icmp    1     ICMP      # Internet control message protocol
ggp     3     GGP       # gateway-gateway protocol
tcp     6     TCP       # Transmission control protocol
egp     8     EGP       # exterior gateway protocol
pup     12    PUP       # PARC universal packet protocol
udp     17    UDP       # user datagram protocol
hmp     20    HMP       # host monitoring protocol
xns-idp 22    XNS-IDP         # Xerox NS IDP
rdp     27    RDP       # "reliable datagram" protocol
```

1.16.5 services.

Es una lista de los servicios disponibles en el anfitrión. Para cada servicio, una línea en el archivo debe estar presente para proporcionar la siguiente información:

nombre oficial del servicio *número de puerto/nombre del protocolo* *alias*

Cada entrada se separa por un espacio. El número de puerto y el nombre del protocolo se consideran un sólo ítem y se utiliza una diagonal para separarlos, por ejemplo:

```
#
# Network services, Internet style
#
tcpmux          1/tcp
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
```

```
discard     9/udp       sink null
systat      11/tcp      users
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
chargen     19/tcp      ttytst source
chargen     19/udp      ttytst source
ftp-data    20/tcp
ftp         21/tcp
telnet      23/tcp
smtp        25/tcp      mail
time        37/tcp      timserver
time        37/udp      timserver
name        42/udp      nameserver
whois       43/tcp      nicname     # usually to sri-nic
domain      53/udp
```

Este archivo funciona con la información del archivo *protocols*. Si el servicio no está disponible, o se desea retirarle soporte, entonces hay que comentar la línea con #, pero en algunos casos hay que actualizar el archivo inetd.conf.

1.16.6 inetd.conf

Se utiliza para brindar la información al comando *inet*. Recibe las peticiones de un puerto específico e iniciará el comando adecuado cuando se reciba una solicitud. Esto ahorra recursos en el sistema al inicializar los demonios sólo cuando son necesarios.

La sistaxis de ese archivo es la siguiente:

Nombre del servicio	*Tipo de socket*	*Tipo de protocolo*	*Wait/nowait*	*Usuario*	*Nombre del comando y argumentos*

Un ejemplo del contenido de este archivo se muestra a continuación:

```
ftp     stream  tcp   nowait  root  /usr/sbin/in.ftpd      in.ftpd
telnet  stream  tcp   nowait  root  /usr/sbin/in.telnetd   in.telnetd
shell   stream  tcp   nowait  root  /usr/sbin/in.rshd      in.rshd
login   stream  tcp   nowait  root  /usr/sbin/in.rlogind   in.rlogind
exec    stream  tcp   nowait  root  /usr/sbin/in.rexecd    in.rexecd
comsat  dgram   udp   wait    root  /usr/sbin/in.comsat    in.comsat
```

1.17 Archivos de acceso a la red[8,44].

Con la debida modificación de estos archivos, se puede accesar a la red sin tener el password del usuario, una breve explicación mostrará la necesidad de poner atención a ellos.

1.17.1 hosts.equiv

Contiene una lista de servidores "confiables", es usado por los comandos que empiezan con "r", como rlogin, rcp, rsh y otros. Su formato consiste de una lista de nombres de máquina, uno por línea:

localhost
apolo
cronos

Este archivo se encuentra bajo el directorio /etc.

1.17.2 .rhosts

Este archivo es utilizado por cada usuario y esta contenido en el home de cada uno, el formato del archivo es el mismo que el anterior. La diferencia contra el hosts.equiv es que se emplea para proporcionar la equivalencia entre usuarios.

1.17.3 hosts.lpd

El sistema lpd de UNIX permite a los hosts "confiables" utilizar la impresora local, se debe de tener cuidado cuando el archivo contenga un "+" ya que esta opción permite que cualquier computadora que tenga acceso al host puede utilizar la impresora.

1.17.4 named.boot

Este archivo (que se encuentra en el subdirectorio /etc) es utilizado para bloquear zonas de transferencia del DNS. En caso de estar utilizando alguna versión de servidor de nombres de Berkeley se pude agregar la opción de xfrnets la cual permitirá una zona de transferencia al host que se especifique con esta opción, el cual puede ser un servidor de nombres secundario.

1.17.5 fbtab (logindevperm)

Esta es una lista de dispositivos que pueden ser cargados al momento de que el usuario accesa a su cuenta en un servidor UNIX.

1.17.6 X0.hosts

X Window mantiene una lista de control de acceso de los hosts que van a tener acceso al servidor X, esta lista puede modificarse por medio del comando *xhost* o de un archivo llamado X0.hosts (localizado en /etc). Si el nombre del host esta antecedido de un "-" se negara el acceso a dicho host; en caso contrario, se permitirá dicho acceso; si se configura con un "+" simple, se desactiva el control de acceso.

1.17.7 sendmail.cf

Este comando, como ya se dijo, tiene varios huecos de seguridad muy importantes, para combatirlo se debe de agregar una opción en el archivo sendmail.cf (el cual puede localizarse en /etc o /etc/mail) la cual es:

Onovrfy,noexpn,needmailhelo,retrictmailq

Novrfy deshabilita el comando *vrfy* el cual determina el nombre de los usuarios; *noexpn* deshabilita el comando *expn* que visualiza la dirección del reparto actual de las listas de correo y los alias; *needmailhelo* rechaza el correo a menos que el sitio de origen se identifique y *restrictmailq* elimina la opción de que cualquier persona vea el intercambio de correos entre el host

e Internet. Aunque por desgracia puede hacer otros huecos de seguridad que no se conozcan todavía.

1.17.8 ftpusers

Es una lista de los usuarios que no pueden ejecutar ftp en el host (este archivo se localiza en /etc), se recomienda que los siguientes usuarios aparezcan en la lista: root, uucp, bin, nobody, daemon y cualquier otra que tenga información o privilegios especiales.

1.17.9 Archivos de inicialización del sistema.

Si ocurre un acceso al host, es posible que el intruso agregue programas script que faciliten el acceso al sistema (en caso de que la asignación de permisos sea la incorrecta), al momento de reinicializar el sistema o cambiar de nivel de ejecución; regularmente, estos archivos en su nombre comienzan con *rc* y pueden encontrarse en:

/etc, /etc/init.d/

1.17.10 Archivos en la cuenta del usuario.

Estos archivos son ejecutados cuando el usuario entra por primera vez al sistema (que inicializan su cuenta, cuando accesa al host o cuando ejecuta otro shell), pueden ser susceptibles de agregarles programas script para accesar a la cuenta, estos pueden ser:

.login, .profile, /etc/profile, .cshrc, .kshrc

Existe software de correo electrónico (como el sendmail) que permite a los usuarios especificar encabezados de correo con la ayuda de archivos especiales en sus directorios de trabajo, en caso de que un atacante logre escribir en alguno de estos archivos puede obtener acceso a la cuenta del usuario, ejecutando un programa que genere un shell SUID que pueda utilizar después el hacker o craker, estos archivos son:

.forward y .procmailrc

1.17.11 Otros archivos a proteger[44].

Estos pueden ser:

- Cualquiera directorio que contenga comandos y bases de datos de NIS o NIS + (/usr/etc/yp* o /var/nis)
- Los que se encuentren en /usr/adm, /var/adm y cualquier subdirectorio que contenga las bitácoras de identificación y de conteo.
- Los archivos de la cola de correo (mqueue y mail).
- Todas las librerías (contenidas regularmente en un subdirectorio /lib) del sistema y de las aplicaciones existentes.
- Los directorios que contengan archivos crontab, debido a que pueden ejecutar tareas especificas a determinado tiempo con los privilegios de algún usuario (regularmente root), especificados en un subdirectorio cron.

- Los archivos que contengan los alias que son utilizados en los correos electrónicos, regularmente comienzan con "*aliases*" pueden localizarse en

/etc/, /usr/lib o /etc/sendmail

- Los archivos que son utilizados para inicializar cualquier editor que tenga UNIX como: .emacs (utilizado por el editor Emacs GNU) y el .exrc (utilizado por el editor vi), debido a que pueden implementarse programas que realicen otras funciones distintas.

- Así como los archivos de inicialización de cualquier aplicación que se encuentre instalada en el host.

Capítulo II

Puntos a proteger de una red

2.1 Introducción.

Los conocedores del tema afirman que la seguridad de la red recae en el administrador del sistema, pero esta responsabilidad es compartida por los usuarios y los directivos de la empresa u organización en donde se encuentre el medio a proteger, esta situación se debe a que los usuarios son los que van a hacer uso de los recursos computacionales y los directivos debido al hecho de que son ellos los que autorizan las políticas y procedimientos generales de la organización. Enseguida se presentarán algunos temas que son importantes conocer para poder tener una red segura, o al menos no tener ese cargo de conciencia. Por desgracia (como se verá más adelante), la falta de una política que responda efectivamente a estos incidentes son gran parte del problema de seguridad.

2.2 Niveles de seguridad[8].

Estos niveles son estándares, desarrollados por el Departamento de Defensa de los E.U. y protegen de un ataque al hardware, al software y a la información guardada en estos. Es conocido comúnmente como el "libro naranja". A continuación se presenta un breve resumen de cada nivel:

2.2.1 Nivel D1

Es la forma de seguridad más elemental disponible. Se parte de la base de que se asegura que todo el sistema no es confiable, no hay protección disponible para el hardware; el sistema operativo se compromete con facilidad, y no hay autentificación con respecto a los usuarios y sus derechos para tener el acceso a la información que se encuentra en la computadora. Este nivel lo tienen los sistemas operativos de PC como MS-DOS, Windows 3.x y System 7.x de Apple Macintosh.

2.2.2 Nivel C1

Conocido también por Sistema de protección de seguridad discrecional, detalla la seguridad disponible en un sistema UNIX. Existe algún nivel de protección para el hardware, puesto que no puede comprometerse tan fácil. Los usuarios se identifican en el sistema por medio de un nombre de registro (login) y un password, esto se utiliza para determinar que derechos de acceso a los programas e información tiene cada usuario, estos derechos son permisos para archivos y directorios (controles de acceso discrecional) que permiten al dueño del archivo o directorio, o al administrador del sistema, evitar que algunas personas tengan acceso a la información de otras personas. Pero la cuenta del administrador no esta restringida a ninguna regla en específico; en consecuencia, un administrador de sistemas sin escrúpulos puede comprometer con facilidad la seguridad del sistema sin que nadie se entere. Entre más administradores haya, es difícil determinar quien cometió el error o el incidente de seguridad.

2.2.3 Nivel C2

Tiene la capacidad de reforzar las restricciones a los usuarios en su ejecución de algunos comandos o el acceso a algunos archivos basándose en un nivel de autorización, además de los permisos. Adicionalmente se implementan auditorias con la consecuente creación de registros para cada evento que ocurra, como por ejemplo las actividades del administrador y la auditoria requiere autentificación adicional. La desventaja de esto es que se requiere un proceso adicional y recursos como disco duro y memoria.

Con el uso de niveles de autorización, es posible que los usuarios del sistema tengan la autoridad para realizar tareas de manejo del sistema sin necesidad de una contraseña raíz. Esto mejora el rastreo de las tareas relativas a la administración. Pero no se debe confundir con los permisos SGID y SUID que se pueden aplicar a un programa.

2.2.4 Nivel B1

La protección de seguridad por etiquetas soporta la seguridad de multinivel, como la secreta y la ultrasecreta. Este nivel parte del principio de que un objeto bajo control de acceso obligatorio no puede aceptar cambios en los permisos hechos por el dueño del archivo.

2.2.5 Nivel B2

La protección estructurada requiere que se etiquete cada objeto, dispositivos como discos duros o terminales podrán tener asignado un nivel sencillo o múltiple de seguridad. Este nivel empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto hacia un nivel inferior.

2.2.6 Nivel B3

El dominio de seguridad refuerza a los dominios con la instalación de hardware. Por ejemplo, el hardware de administración de memoria se usa para proteger el dominio de seguridad de un acceso no autorizado o la modificación de objetos en diferentes dominios de seguridad. Este nivel requiere que la terminal del usuario se conecte al sistema por medio de una ruta de acceso segura.

2.2.7 Nivel A.

El nivel de diseño verificado es el más alto de seguridad. Incluye un proceso exhaustivo de diseño, control y verificación. Para lograrlo, todos los componentes de los niveles inferiores deben incluirse; el diseño requiere ser verificado en forma matemática; además, es necesario realizar un análisis de los canales encubiertos y de la distribución confiable, esto significa que el hardware y el software esten protegidos para evitar violaciones a los sistemas de seguridad.

2.3 Características de la seguridad.

Básicamente se tiene que la protección a un sistema se basa en los siguientes requisitos:

Privacidad: Hay que asegurarse que la información que tenga la cuenta de un usuario, sea privada de manera tal que no se deben de otorgar privilegios de ningún tipo a estos archivos o directorios.

Integridad. Se tiene que proteger la información contra cualquier modificación que no este autorizada por el dueño o creador de la información.

Disponibilidad. Hay que salvaguardar los servicios de cómputo de modo que no se degraden o que no se encuentren a la disponibilidad de los usuarios.

Consistencia. Asegurarse que el sistema se comporte como se espera.

Regulación del acceso. Es necesario controlar quién utilizará el sistema y los recursos con que se cuentan.

Auditoria. Se tienen que contar con los mecanismos para poder determinar lo que esta sucediendo en el sistema, que hace cada usuario y en que tiempo se realizaron dichas modificaciones.

2.4 Tipos de usuarios en una red[38].

Los usuarios son aquellas personas de una organización que se dedican a manejar algún sistema que exista, utilizando el equipo que les corresponda. Existen diferentes tipos, para efectos de este trabajo se mostraran a los diferentes usuarios desde un punto de vista de seguridad.

2.4.1 Administradores.

Son responsables de la seguridad en la red, están limitados en sus peticiones en cuanto a software y descuidan la seguridad al no procurar pedir productos a este respecto.

Los administradores de muchos sitios creen tener experiencia en el manejo de software y les falta incluir en sus presupuestos todo el software que necesitan. En consecuencia, estos administradores por necesidad tienen que conseguir alguna copia sin licencia, y que esto se fomente en los usuarios.

Son parte del problema de seguridad porque suponen que una persona con experiencia en seguridad localizada en un lugar remoto (DGSCA) puede prevenir, detectar y recobrar las brechas de seguridad en la organización; otro caso es que se cuente con personal de seguridad pero sin autoridad, no podrá desempeñar bien su trabajo si no se puede evaluar una decisión; no pueda hacer recomendaciones o que no se les notifica cuando un usuario o empleado ha sido dado de baja, despedido o cambiado de empresa (deben de poder eliminar cuentas, proteger la información, etc.) y no puedan influenciar en las decisiones de compra.

La situación más peligrosa es cuando comprenden parte de los problemas de seguridad y dirigen la instalación de cualquier paquete de que ayude a resolverlos. Pero si no se entiende la extensión del problema pueden provocar una decisión costosa de un problema sin valor.

2.4.2 Supervisores de red.

Estos usuarios se dedican a supervisar el contenido de la red, dar soporte técnico preventivo de hardware y software a los usuarios y a los equipos, regularmente son gente sin experiencia, que tienen ese trabajo temporalmente y por tanto se pueden incurrir en alguno de los siguientes casos:

- Fallas al implementar el control.
- Fallas al implementar el control adecuadamente.
- Falta de conocimiento correcto del sistema de bitácoras.
- Fallas al seguir los procedimientos operacionales establecidos.
- Fallas al disciplinar a los usuarios acerca de violaciones de seguridad.

Es muy probable que estos problemas sean fallas de organización de los administradores o de los encargados de la administración del personal de la empresa.

2.4.3 Usuarios.

La computadora, mayoritariamente es manejada por usuarios inexpertos, los cuales por mero accidente borran los archivos del sistema, sobreescriben algún archivo cuando los copian, entre otras cosas que pueden suceder.

Son "los actores principales" de la seguridad de redes. Bajo el concepto de LAN son vistos en alguna estación de trabajo como una herramienta que tiene que hacer su trabajo, alguien a quien proveerle las herramientas para que desempeñe su trabajo, pero los supervisores de la red optan por las necesidades de la organización.

El usuario puede operar en un tiempo distinto, tiene un límite hoy, un límite mañana. Las organización puede cambiar de perfil un año, el siguiente. La organización se mueve lentamente, el usuario se mueve más rápido. El usuario aprecia al usuario primero, la organización aprecia a la organización primero.

El usuario puede ser promovido por la organización, la organización no puede ser promovida por el usuario. El usuario puede ser despedido, la organización no. En tiempos difíciles la organización puede sobrevivir sin el usuario.

Muchos usuarios han tenido accidentes en el ciclo de vida de un sistema, accidentes que afectan la confidencialidad, integridad o disponibilidad de la información. Los accidentes son por desgracia comunes, es necesario prevenir estas situaciones y tratar de estructurar sistemas que puedan restablecerse después de un accidente.

Por desgracia, las personas que se encuentran dentro de la organización son las que tienen más incidencia en problemas de seguridad, debido a que es la gente a la que se le tiene mayor "confianza".

2.4.4 Hackers.

Se puede obtener acceso a un sistema de computadoras si se intercepta un cable, obtener una cuenta de invitado, cambiar los atributos de un archivo, borrar un archivo encriptado, cambiar algunos números en la base de datos de la bitácora no es difícil. Prevenir estas acciones, detectarlas o recobrarse de ellas es lo difícil. Por desgracia hay diversos tipos de hackers de los cuales hay que tener cuidado, a lo mejor en la red interna a proteger nos podemos encontrar alguno de ellos (fig. 13).

¿Qué es un hacker?. Un hacker es una persona con los suficientes conocimientos computacionales que puede irrumpir en un sistema (por mera casualidad o a propósito) para comprobar sus conocimientos. Además en el mundo informático se oye mucho la palabra "craker", este es una persona que busca hacer algún daño en el sistema que entra con un fin específico, la clasificación de la fig. 13 se ajusta a un "craker".

Pueden atacar desde equipo como una simple PC, minis, Macintosh, mainframes o estaciones de trabajo.

Hay eventos que pueden determinar el acceso de un hacker como es:

- Pérdida de passwords.
- Descubrimiento de programas alterados.
- Datos destruidos.
- Mensajes o cambios distintos.
- Resultados de callback incorrectos.

Tipo.	Descripción.
Trainspotter	Es un hacker que desea tener acceso a diferentes sistemas como pueda. No regresa al lugar al que acceso.
Kilroy.	Disfruta de "limpiar" al lugar en donde accesa.
Usuario	Busca tener facilidades a equipos a los que no tiene acceso.
Espía.	Buscan información confidencial.
Fixer.	Intenta modificar un campo específico de datos, como un balance de un banco, registros criminales, exámenes escolares, etc.
Vándalo.	Busca causar daño en los sistemas que accesa.

Fig. 13. Tipos de hackers (y crakers).

Pero desgraciadamente, en la mayoría de los casos, se desconoce por completo estos eventos.

Además, pueden entrar a un sistema por medio de:

- Acceso dial-up.
- Conexiones LAN DOS.
- Conexiones LAN UNIX.
- Puertos de minis/mainframes.
- Redes relacionadas en Internet.
- Acceso físico directo.

Para protegerse y para prevenir ataques de hackers se puede utilizar:

- Passwords.
- Políticas de acceso.
- Computadoras o redes aisladas.
- Modems seguros.
- Archivos encriptados.
- Firewall

Algunos de estos últimos puntos se tratarán más adelante.

2.5 Políticas de seguridad de red[7].

Una organización puede contar con muchos sitios y cada uno contar con sus propias redes. Si la organización es grande, es probable que los sitios tengan diferentes administradores de red, con diferentes metas y objetivos. Si estos sitios no están conectados por una red interna, cada uno de ellos podrá tener sus políticas de seguridad; sin embargo, se encuentran conectados por una red interna, la política de seguridad deberá agrupar las metas de todos los sitios que están interconectados.

Es muy importante identificar los recursos con que se cuenta en el sitio o la organización, estos pueden ser:

- Estaciones de trabajo.

- Servidores.
- Dispositivos de interconexión: compuertas, ruteadores, repetidores.
- Servidores de terminal.
- Software para red y aplicaciones.
- Cables de red.
- Información en archivos y bases de datos.

Se debe de tomar en cuenta su protección dado que el sitio está conectado con otras redes, la política de seguridad debe considerar las necesidades y requerimientos de seguridad de todas las redes interconectadas.

Para plantear las políticas de seguridad se necesita desarrollar procedimientos y planes que salvaguarden los recursos de red contra pérdidas y daños. Para hacerlo posible se necesita analizar las siguientes preguntas:

- ✓ ¿Qué recursos se quieren proteger?
- ✓ ¿De qué personas necesita proteger los recursos?.
- ✓ ¿Qué tan reales son las amenazas?.
- ✓ ¿Qué tan importante es el recurso?.
- ✓ ¿Qué medidas se pueden implantar para proteger la información de una manera económica y oportuna?.

Adicionalmente es necesario examinar con frecuencia la política de seguridad de red para verificar si los objetivos y circunstancias en la red han cambiado.

Siempre, el costo de proteger la red de una amenaza debe ser menor que el costo de la recuperación, si es que se ve afectado por la amenaza de seguridad. Si no se tiene el conocimiento suficiente de lo que se desea proteger, y de las fuentes de la amenaza, podrá ser difícil lograr un nivel aceptable de seguridad – ver el anexo 2 -. Para eso hay que solicitar ayuda a personas especializadas en el tema.

Es importante involucrar al tipo adecuado de personas en el diseño de la política de seguridad de red, a lo mejor ya se cuenta con un grupo de usuarios que podrían considerar que su especialidad es la implantación de una política de seguridad de red. Estos grupos podrían incluir a aquellos individuos con cualidades de control de auditoria, grupos de sistemas de información de campo y organizaciones relacionadas con la seguridad física. Si se desea un soporte "universal" de la política de seguridad de red, es importante involucrar a estos grupos para contar con su cooperación y aceptación de la política de seguridad de red.

2.6 Aseguramiento de la política de seguridad[8].

La política de seguridad no puede anticipar todas las amenazas posibles, pero si garantizar que cada tipo de problema tiene a alguien que puede manejarlo de manera responsable y/o algún procedimiento a seguir; por ejemplo, cada usuario de la red es responsable del password de su cuenta, pero si la pone en riesgo, aumentará la probabilidad de comprometer otras cuentas y

recursos. Por otro lado, los administradores de red y del sistema son responsables de mantener la seguridad general de la red.

La política de seguridad *es el conjunto de decisiones que determina la postura de una organización en torno a la seguridad*, en otras palabras *son las normas que definen lo que está permitido y lo que no lo esta*. Es muy importante que cumpla los siguientes lineamientos:

1. Debe estar muy bien documentado, escrito en una forma clara evitando ambigüedades.
2. Debe definir claramente que esta permitido y que esta prohibido, aclarando qué lineamientos sigue aquello que no esta definido expresamente, esto implica en "esta permitido hacer todo lo que no esta prohibido o esta prohibido realizar cualquier acción que no se permite".
3. Debe estar reconocida la política como un documento oficial, aprobada por las autoridades correspondientes dentro de la organización.
4. Debe dársele amplia difusión a las áreas involucradas.
5. Debe estar acorde con la política general de la institución.
6. Debe ser dinámica para adaptarse a los continuos cambios que se presentan en el área de cómputo, además de estar planteada pensando en el mayor tiempo de vida posible.

Probablemente no se tengan datos importantes en el servidor a protegerse, no por ello hay que subestimar el valor de esta información debido a que si es valioso para el dueño y puede significar su robo o violación en gastos de tiempo y trabajo de más, inclusive para la organización.

Es importante señalar las diferentes restricciones que se deben de tomar en cuenta hacia el interior como al exterior del servidor, hay que tener en cuenta el riesgo que se puede tener al hecho de que un usuario externo utilice el servidor como trampolín hacía otros servidores. Es obligación de los administradores controlar este tipo de sucesos al máximo.

2.7 Análisis de riesgos[8,39].

Es necesario entender que para crear la política de seguridad se verifica que los esfuerzos invertidos en la seguridad son costeables, en esta parte se tiene que definir cuáles recursos valen la pena proteger, y que algunos recursos son más importantes que otros. Además de identificar la fuente de amenaza de la que se protege a los recursos. Es necesario señalar que varias encuestas indican que la pérdida real que proviene de los miembros de la organización es mucho mayor.

El análisis de riesgos debe tomar en cuenta lo siguiente:

⇒ ¿Qué se necesita proteger?.

⇒ ¿De quién se debe proteger?

⇒ ¿Cómo protegerlo?.

Los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. Hay que determinar los siguientes factores:

1. Estimación del riesgo de pérdida del recurso(r).
2. Estimación de la importancia del recurso(i).

Al riesgo de perder un recurso se le asigna un valor del 0 al 10, donde cero indica que no hay riesgo y el 10 es el riesgo más alto. De manera similar, a la importancia de un recurso (y) igual donde cero determina la poca importancia y el 10 en donde implica la importancia más alta. Esto dará la evaluación general (eg) del análisis.

$eg = r * y$

Y para calcular el riesgo general de los recursos de la red, se tiene:

$EG= (r_1i_1 + r_2i_2+ ... +r_ni_n) / (i_1 + i_2 + ... + i_n)$

Otros factores a considerar son la disponibilidad, su integridad y su carácter confidencial, la disponibilidad de un recurso es la medida de la importancia de tenerlo disponible todo el tiempo. La integridad de un recurso es que este o los datos del mismo sean consistentes, esto es importante para una base de datos.

Es importante identificar todos los recursos de la red que podrían ser afectados por un incidente de seguridad, el RFC 1244 lista los siguientes recursos de red que deben considerarse al estimar las amenazas a la seguridad general:

1. Hardware. Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, PC, impresoras, unidades de disco, líneas de comunicación, servidores, ruteadores.
2. Software. Programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicación.
3. Datos. Que pueden ser generados durante la ejecución, almacenados en línea, archivados fuera de línea, apoyos, bitácoras de auditoría, bases de datos, los cuales pueden estar en tránsito sobre algún medio de comunicación.
4. Personas. Usuarios, personas para operar sistemas.
5. Documentación. Sobre los programas, hardware, sistemas, procedimientos administrativos locales.
6. Accesorios. Papel, formas, cintas, información grabada.

Después, para determinar el potencial de pérdida que tiene cada recurso hay que identificar las amenazas a estos, identificando cuáles amenazas se trata de proteger a los recursos.

2.8 Establecimiento de la política[39].

Esta es una parte muy importante ya que aquí se establecen los derechos y las responsabilidades de los usuarios y administradores, así como las sanciones y las acciones a tomar en cuanto a la estructura de seguridad que se vaya a implementar. Se debe de contemplar al momento de establecer la política lo siguiente:

- ¿Quiénes están facultados para utilizar los recursos de la organización y cuáles son los usos que se les pueda dar?.

Aquí se debe de especificar las actividades que pueden hacer los distintos tipos de usuario, aunque sean obvias:

- ¿Está permitido descifrar (adivinar) passwords?

- ¿Está permitido compartir cuentas?.

- ¿Está permitido que un usuario deshabilite un servicio, máquina o subred?.

- ¿Puede un usuario copiar cualquier archivo con derechos de lectura, o modificar aquellos sobre los cuales tenga derechos de escritura aún cuando no es el propietario?.

- ¿Está permitido compartir programas que no le pertenecen?.

Se recomienda que lo anterior este prohibido.

- ¿Quién está facultado para habilitar el acceso al sistema y con qué condiciones?.

Se debe de especificar claramente cuáles son los derechos de privacia de los usuarios en cuanto a la información y correo, cuáles son los derechos y responsabilidades de un administrador y en que circunstancias puede revisar el contenido de un directorio, especificando además cualquier restricción sobre dicha búsqueda.

- Derechos y responsabilidades de las diferentes áreas de la organización.

Se tiene que definir los derechos y las obligaciones de los encargados de las distintas subredes, sobre todo si cuentan con autonomía.

- ¿Qué respuesta se le debe de dar a los incidentes de seguridad?

Se tiene que definir puntos acerca de sanciones a usuarios en caso de violaciones a normas estipuladas, así como los procedimientos que se tienen que seguir para restablecer el sistema a su integridad original.

Se puede optar por dos caminos, impedir que el atacante prosiga con sus acciones, o dejarlo con la finalidad de monitorear sus movimientos y en conjunto con los sistemas involucrados rastrear el origen de los incidentes.

2.9· Incidentes de seguridad más usuales en Internet[8,21].

Aquí se presenta una lista[22] de los tipos de ataques que pueden suceder a cualquier sitio que tenga acceso a Internet -originados por una configuración o debilidades en el sistema-:

➢ Ataques por password de invitado. Los passwords de invitado (como "servicio" de password a una cuenta llamada profesor, o los passwords que vienen predeterminados desde la instalación de cualquier sistema) pueden entrar con facilidad y es el medio más común por el cual un sistema es violado. El firewall puede establecer que no existan passwords de invitado que se usen en el sistema que va a ser protegido. Añadiéndose mecanismos de autentificación en ambas máquinas de autentificación (en la dirección ethernet) y el usuario. Se puede limitar el número de errores de identificación.

➢ Ataques de fuerza bruta a los passwords. Si se logra el acceso, se puede atacar el archivo que contiene a los passwords del sistema (/etc/passwd) usando una herramienta de craqueo conocida como CRACK, en si consta de una serie de bibliotecas con probables passwords. Estadísticamente hablando, se pueden obtener alrededor del 25% de los passwords, y algunos pueden ser utilizados para accesar a otros sistemas. El firewall debe proteger este archivo y prevenir su transmisión o alteración.

➢ Sesiones de terminal interferidas. Esta es una manera en que el hacker monitora la actividad de un usuario, capturando sus claves y observando la identificación (logeo) a otro sistema. Algunos ataques son posibles con la configuración de default de alguna versión "segura" de UNIX, como el OSF/1

➢ Captura del password vía TSR (Terminate and Stay Resident, son programas que pueden estar residentes en memoria). Las cadenas de caracteres del password capturadas por medio de TSR pueden ser realizada con herramientas como THIEF o GETIT, o una superkey de Borland. Con este tipo de ataque el hacker lo único que hace después es accesar al archivo que contiene las cadenas capturadas.

➢ Ataque con secuencia de números. Esto sucede cuando un hacker predice un punto de inicio que es una selección de un blanco, como en la dirección IP de origen y se compromete a cualquier protocolo que utilice esa dirección para autentificación (los comandos "r" de UNIX). Un firewall prevendría este tipo de ataque haciendo una autentificación más segura de la fuente.

➢ Paquetes UDP alterados (Spoofing UDP packets). Si alguna aplicación esta usando el UDP para transmitir información, este protocolo no utiliza handshaking o secuencias de números, y envía todos los paquetes a un puerto dado para el mismo proceso, descuidando la dirección de origen o el número de puerto. Se puede verificar independientemente la fuente de un paquete UDP después de procesarlo si la fuente se encuentra dentro de la organización.

➢ Conexiones ICMP separadas. EL ICMP es una herramienta que informa al host acerca de un mejor ruteo, finaliza las conexiones cuando hay problemas en la red y reportan problemas de ruteo. Versiones antiguas ignoran la información de una conexión en específico de un mensaje ICMP y redirigen todas las conexiones, cambiando la conexión original con una nueva.

➢ Conexiones ICMP redirigidas. Los mensaje ICMP pueden ser redirigidos estableciendo una ruta entre dos hosts. Algunos ruteadores responden a estas instrucciones. El firewall respondería sólo al ruteador propio (que, en teoría es confiable).

➢ Ataques sin indicios de la ruta de origen. Esto requiere que los hackers realicen una conexión TCP especificando una ruta de destino. Cuando es utilizado en el destino se invierte la ruta si la fuente es confiable (conforme al RFC 1122) Esto permite el acceso a una máquina protegida, con un firewall se puede anular esta ventaja.

➢ Ataques a los protocolos de información de ruteo. Con la inserción de paquetes RIP se puede hacer esto, el tráfico se desvía a la computadora del atacante. En algunos casos, el RIP no es un campo autentificado y no se comunica entre el par de hosts para establecer cualquier tipo de autentificación. En cuyo caso es posible establecer una ruta de un host en específico dificultando así su detección.

➢ Ataques a la zona de transferencias. El DNS es una base de datos distribuida que mapea el nombre del host y la dirección IP. Las colas de TCP de los servidores de respaldo pueden producir zonas de transferencia, en donde una copia completa de una parte de nombre de espacio es generada, con la que el servidor de respaldo puede trabajar. En este tipo de ataque, los hackers hacen requerimientos similares al respecto, obteniendo así una lista de hosts y de direcciones IP que pueden ser blancos potenciales.

➢ Ataques de árboles invertidos de mapeo. En algunos sistemas el DNS permite almacenar subárboles en otros servidores. Debido a que el DNS mantiene parejas de árboles mapeando los nombres de los hosts en las direcciones y en el otro mapea las direcciones en los nombres, un hacker puede modificar un registro inverso para mostrar el nombre de un servidor confiable hacia su dirección, utilizando el comando rlogin se puede engañar a los dispositivos de que la conexión se realiza desde un host confiable. Se puede prevenir esto protegiendo al DNS o aumentando la autentificación checando las direcciones IP.

➢ Ataques al cache del DNS. Es posible precontaminar el cache de respuestas del DNS al iniciar la llamada. Cuando el blanco checa el cache de respuestas válidas, busca un nombre semejante y permite el ataque. Un firewall usa nombres y direcciones autentificadas si son confiables.

➢ Ataques a las soluciones del DNS. Para ser más eficiente la solución del DNS se envía la conexión a los destinos en los cuales la igualdad en los nombres de dominios están incompletas. Un dominio con un nombre en común con un nombre en la dirección de destino deseada puede ser capaz de interceptar tráfico de manera intencional hacia otro destino.

➢ Sobrecargas al SMTP. El protocolo SMTP tiene la característica de transportar mensajes de 7 bits. El protocolo puede ser imitado fácilmente y si no es autentificado debidamente, los mensajes puede ser introducidos manualmente por un hacker, porque se puede especificar cualquier origen en el correo, es posible sobrecargar el sistema con mensajes, generando un ataque de servicio denegado. El sistema de correo pierde funcionalidad o el host se puede colapsar debido a la gran cantidad de mensajes recibidos.

➢ Expansión del alias. El SMTP permite tener alias para transmitir correo. El comando *vrfy* puede interpretar los alias de correo en nombres de identificación, *expn* expande los alias de las listas de correo electrónico. El firewall puede prevenir la expansión de los alias en nombres dentro de la organización para preservar la confidencialidad de quienes utilizan el sistema.

➢ Sendmail. Este demonio es el medio más común en que el SMTP es implementado, pero tiene muchos errores. Este no debe ser ejecutado como root a menos que sea de manera local. Existen versiones mejoradas del sendmail.

➢ Encabezados del MIME. Un demonio de correo recibe los mensajes que son codificados con MIME (Multipurpose Internet Mail Extensions) que lleva las instrucciones en el encabezado del mensaje MIME. Si no son evaluadas adecuadamente antes de la ejecución, pueden sobreescribir archivos rhosts en el directorio actual y ejecutar otras formas.

➢ Archivos ejecutables adjuntos al correo. Esto se da cuando el atacante adjunta a un mensaje un programa que ataque cualquier cosa que sea, con archivos de tipo "caballo de Troya"; este tipo de archivo puede captar los passwords como si fuera un programa residente o puede contener un virus que no puede ser detectado por el centinela de la maquina destino. Algunas veces este tipo de archivo es un programa dejado que contenga un virus; es decir, que el programa y el virus generalmente estén encriptados para prevenir algún tipo de detección, donde el programa se ejecute.

➢ Telnet corrompidos. Este comando comienza el acceso a una terminal, en un sistema inseguro este comando puede estar comprometido en el hecho de que un hacker puede capturar el nombre de un usuario, el password o incluso la sesión. O a lo mejor lo único que desea es obtener los privilegios que tiene la cuenta.

➢ Grabado de las ligas de comunicaciones. Si esto ocurre, los passwords que están desencriptados no pueden ser confiables. Esto se hace desde el backbone.

➢ Ataques NTP. Cuando un servicio de autentificación es sensitivo, en donde un valor diferente es usado diferentes veces, es la oportunidad para un hacker de capturar qué "cadena" fue usada para autentificar así como el tiempo, procurando dar instrucciones al host por medio del NTP (Network Time Protocol) esperando el tiempo de regreso para capturar el tiempo validado de las cadenas de autentificación. Los ataques de este tipo no se pueden prevenir con las últimas versiones del NTP.

➢ Ataques de finger. Este protocolo ofrece información de los usuarios que pudiera ser útil para el hacker (vistas en el capítulo 1 sección 1.15.5). Por este medio es como se pueden visualizar aquellas cuentas inactivas y las semejanzas existentes entre los nombres y los correos electrónicos que tienen password de invitado, es menos seguro que el servicio whois.

➢ Forzando los campos de autentificación de UNIX en los encabezados del RPC. El RPC (Remote Procedure Call) es un protocolo que tiene un diseño con medios para crear un servicio de red con el que se puede salir y ejecutar subrutinas en servidores remotos, cada mensaje de este tipo tiene un encabezado en el cual incluye información de autentificación. Esta podría ser nula para servicios anónimos o incluir información de "Autentificación de UNIX", incluyendo el número de identificador del usuario y de su grupo de la llamada y el nombre de la máquina que lo ejecuto.

Esta información puede ser obtenida por un hacker y los requerimientos del RPC pueden accesar a cualquier servicio disponible en el host.

➢ Reportes del portmapper para los atacantes por medio de rpcinfo. El comando portmapper despliega información de cada servicio que el servidor este ejecutando, su número de puerto y su número de versión. Esta información puede ser obtenida por medio del rpcinfo.

➢ Uso del portmapper para ocultar el lugar de origen. El uso del RPC necesita los requerimientos del viaje de ida y de vuelta del mensaje para determinar el número de puerto real del cliente, del origen o del atacante. Para evitar esto, el portmapper permite al origen requerir que se transfiera este requerimiento al servidor, transportando el portmapper su dirección de regreso, o sea la dirección de origen actual. Esta cualidad hace a los requerimientos locales indistinguibles de los externos, mientras algunas versiones del portmapper pueden filtrarse, otras no.

➢ Ataques de NIS en los cuales se obtiene el archivo de passwords, la tabla de direcciones del host o las bases de datos de las llaves públicas y privadas. Los servicios de información de red (NIS o YP, Yellow Pages) es un servicio que tiene bases de datos distribuidas desde un servidor central a sus clientes. Estas bases de datos incluyen el archivo de password, la tabla de direcciones del host y las llaves públicas y privadas usadas por el Secure RPC (RPC seguro de Sun Microsystems). Este ataque permite que por medio de NIS se obtengan estos archivos.

➢ Servidores de respaldo de NIS. Los clientes de NIS pueden usar diferentes servidores de NIS, esto puede ocasionar que se supla el archivo /etc/passwd entre otros que ya se mencionaron.

➢ Ataques RPC sobre el archivo "shadow" de passwords de NIS. Un archivo fantasma de password es una copia oculta del archivo de password que contiene los passwords desencriptados. Un atacante puede accesar a este archivo, y puede hacer repeticiones de requerimientos a servicios RPC usando varios passwords. Las aplicaciones revisan este archivo y se envía un reporte al atacante si el password es válido.

➢ Manipulación de archivos usando NFS. Para montar un volumen de un cliente, el servidor ejecuta el NFS (Network File System) el RPC monta el demonio y el servidor NFS pregunta al cliente el nombre y el sistema de archivos requeridos, se examina la lista de sustitutos del administrador y si el cliente se encuentra en esta lista se envía al cliente el archivo a manipularse desde el directorio de root. El cliente mantiene esta manipulación y la usa en requerimientos posteriores. Si el cliente la mantiene, se obtiene acceso permanente a root. La manipulación de los archivos de root puede compartirse y cualquier usuario lo puede hacer, las alternativas para eliminar este problema es el AFS (Andrew File System) que usa Kerberos para autentificar y ofrecer una escala, global y un sistema de archivos independientes. Estos archivos pueden estar en cualquier parte de la red capturando todo lo que ocurre de manera clara para el administrador.

➢ tftp. Este protocolo es un archivo de transferencia UDP que no tiene soporte para ser autentificado. Si no es restringido el acceso a este archivo, se puede obtener de manera fácil el archivo de los passwords.

➢ Uso del FTP anónimo. Es un sistema de distribución de archivos, el FTP anónimo permite hacer cualquier transferencia de archivos desde un área restringida del host sin pedir autorización. Si el ftp es configurado con un archivo o directorio con permisos de escritura o que sea el dueño el identificador del ftp, un hacker puede utilizarlo para grabar un archivo .rhosts que puede usarse para realizar, por ejemplo conexiones rsh en la máquina del ftp anónimo y de esta forma transferir todo tipo de archivos.

➢ Archivos no deseados en el área pública del ftp anónimo. Si se cuenta con un área donde el ftp anónimo puede llamar a los archivos, se puede asumir que se tiene copias piratas, archivos infectados entre otras cosas, esto en teoría es para el beneficio de la organización.

➢ rlogin. Este comando permite identificarse en una máquina remota sin password cumpliendo unas pocas condiciones: la máquina origen debe estar en la lista de los servidores confiables (/etc/hosts.equiv o $HOME/.rhosts) este llamado puede tener un puerto TCP especial. Es preferido por los usuarios porque no pide el password y permite el acceso a otras estaciones

remotas con sólo añadir el nombre del servidor de origen al archivo .rhosts de la maquina de destino, por lo mismo es preferido por los hackers ya que pueden revisar las listas de los archivos mencionados para poder accesar a otros sistemas.

➢ Servidores X11. Este sistema es el más popular debido a que permite el manejo de ventanas. El sistema asimila que el usuario es un servidor y permite a las aplicaciones interactuar entre sí, las aplicaciones son capaces de dirigir llaves, capturar ventanas, simular claves, etc. La protección principal de la mayoría de este tipo de servidores sólo permite que las máquinas confiables hagan los requerimientos. Estos servidores no son notificados de accesos denegados y no pueden verificar que proceso se usa. y cualquier persona puede buscarlos y controlarlos

➢ Túneles y encapsulados. Si se ejecuta un firewall que permita protocolos confiables, otros protocolos son capaces de pasar si están encapsulados con otros protocolos a menos que se examine el contenido de cada paquete antes de que se le permita el paso a través del firewall.

Aunque esta lista presenta un panorama desalentador, algunas recomendaciones importantes son muy útiles para poder contrarrestar esta situación; sin embargo, hay que estar al pendiente de nuevos tipos de ataques que puedan suceder en Internet y de nuevas fallas que se presenten en el software del sistema operativo y de las aplicaciones que se usen en el sitio o la organización.

2.10 Puntos para una red segura.

Algunos puntos que se deben de tomar en cuenta para tener una red segura son los siguientes:

⇒ Entrenamiento de usuarios. Debe conocerse la importancia de conectarse y desconectarse, y tener el password en secreto.

⇒ Instalación del software de administración. Una autoridad central debe ser la responsable de todas las instalaciones, conociendo los términos de la licencia y que el material se encuentre libre de virus.

⇒ El lugar en donde se encuentren los servidores tendrá las puertas aseguradas.

⇒ Se deben de buscar continuamente virus, en los nodos de la red así como los servidores.

⇒ El supervisor debe de garantizar los derechos de los usuarios como sea posible.

⇒ Cambiar todos los passwords por default que tengan las aplicaciones o sistemas operativos de red.

⇒ Utilizando un menú de aplicación front-end con control de construcción de passwords. Usar el menú para suplir el control disponible a través del sistema operativo.

⇒ Cuando los usuarios cierren sus aplicaciones, regresar al menú, no al sistema operativo. Esto reduce las oportunidades de daño, además es una oportunidad de vigilar los posibles daños causados por empleados que tengan pérdidas en el sistema.

⇒ Mantener un registro de los empleados que fallan al accesar su login, particularmente en lapsos de horas espaciadas.

⇒ Manteniendo el registro de uso de la red, donde, cuándo y por qué. Estos registros pueden ser valiosos dado que se pueden identificar los orígenes de un posible ataque.

⇒ Hacer respaldos en la medida posible y almacenarlos en un lugar seguro, fuera del servidor.

⇒ Se requiere que el password sea de un intervalo, y que tenga al menos 7 caracteres.

⇒ Tener un control de acceso al correo electrónico, así como a los folders y grupos, tal como se controlan los otros recursos de la red.

⇒ Tener la plena seguridad de que se envíen (o lleguen) los comunicados pertinentes de que alguna persona deja la empresa. Cancelar el acceso de la cuenta de la persona inmediatamente que se tenga noticia

⇒ Si el personal de staff tiene acceso vía dial-up, se debe de tener todas las precauciones de seguridad en cuanto al software, incluyendo passwords encriptados u ocultos así como rasgos dial-back. Si el software de comunicaciones que se use carece de esto, es indispensable buscar una alternativa.

⇒ Fomentar el uso de protectores de pantalla. No son necesarios para preservar los monitores, pero pueden tener una protección en contra de ataques random de datos críticos. También la mayoría de estos incluye protección de password.

⇒ Especificar las opciones de impresión disponibles, no se deben de tener trabajos de impresión hacia impresoras no existentes.

⇒ Garantizar la confiabilidad de derechos solamente a las personas que en realidad necesiten programas o información.

2.11 Consideraciones importantes.

2.11.1 Respaldos[40].

Un punto importante son los respaldos ya que en la medida en que se hagan, se va a poder realizar una recuperación inmediata, en caso de no se pueda restaurar el sistema de un ataque (o de algún otro suceso no previsto); hay diversos tipos de respaldos:

* Respaldo día cero: Es cuando el sistema se instalo por primera vez.
* Respaldo completo.
* Respaldo incremental. Se respalda cada archivo del sistema que se haya modificado basándose en una fecha en particular.

Pero el hacer un respaldo implica seguir ciertos lineamientos:

✓ Hacer los respaldos sobre la base de las políticas de la empresa.

✓ Planearlos debidamente, es decir:

a) ¿Quién puede hacer los respaldos?.

b) ¿Qué se debe de respaldar y cada cuándo?.

c) ¿Dónde se debe guardar los respaldos?.

d) ¿Cuánto tiempo se deben de guardar los respaldos?.

e) ¿Se tienen que asegurar los respaldos?.

f) Hay que determinar si se utilizan variantes del medio seleccionado.

g) Hay que asegurarse en caso de falla, de contar con un dispositivo de almacenamiento de reserva.

2.11.2 Encriptamiento[26].

Es la transformación de datos de manera tal que no puede ser leída por ningún medio, a menos que se tenga la clave correcta. La manera en que se haga el encriptado y el desencriptado va a depender del modelo de encriptamiento que utilice la aplicación con que cuente la organización.

Básicamente consta de las siguientes partes:

Llave de encriptamiento.

Es un valor numérico que es usado por un sistema de firmas digitales o de encriptamiento para proteger información. Estas tiene una administración confiable para que los usuarios requieran sus llaves en el tiempo y lugar que ellos determinen.

Criptografía simétrica o de llave secreta.

El intercambio de las llaves es conocido sólo por las partes involucradas y pueden usar esta llave para encriptar y desencriptar mensajes. Se tiene que asegurar que la compartición de esta llave secreta sea de manera confiable.

Modelo de llave pública y privada o asimétrico.

Este sistema opera por medio de dos llaves (una pública y una privada). La llave pública es usada por cualquiera que desee enviar un mensaje encriptado o desee verificar la firma digital de este. La llave privada es conocida por el usuario y es empleada para desencriptar mensajes enviados por el mismo usuario. Este modelo elimina la necesidad de usar una misma llave (que encripta y desencripta), de este modo se puede emplear con más usuarios que en el modelo anterior.

Firmas digitales.

Este elemento certifica la identidad de la persona que la emite y la integridad del mensaje, pueden ser creadas utilizando un sistema de encriptación de llaves públicas. Una autoridad certificadora "firma" el certificado con el cual se computa la firma digital para su propia llave privada, usando la llave pública cualquiera puede verificar la integridad de la firma.

2.11.3 Passwords[24].

Además se recomienda que los usuarios tengan concientización en cuanto al uso de los passwords, es decir:

- ◊ Educar a los usuarios que no usen passwords que sean fáciles de adivinar.
- ◊ Se debe de cuidar que tenga un tamaño adecuado.
- ◊ Acerca de ejecutar adivinadores de passwords.
- ◊ Es necesario utilizar un generador de passwords.
- ◊ *Se debe de tener la costumbre de usar mayúsculas y minúsculas.*
- ◊ Utilizar al menos dos caracteres no alfanuméricos (.,/#; etc.)
- ◊ No hay que usar palabras que aparezcan en un diccionario o que estén al revés.
- ◊ Nunca utilizar el nombre, dirección o cualquier dato que de algún modo pueda identificar al usuario o estar registrado en el sistema.

2.11.4 Internet[24,26].

Para la seguridad en cuanto a Internet, hay que seguir las siguientes consideraciones:

Autentificación.

Puede haber dos tipos de autentificación:

1) Por medio de TCP/IP (en el telnet y el FTP)

2) *Mensajes, transacciones y correos electrónicos que requieran autentificación de* la fuente.

Confidencialidad.

Para poder garantizar de cierta forma la privacidad o la información estratégica, se recomienda incluir métodos de encriptación si se utilizan correos electrónicos, transferencia de archivos (por FTP) y para las operaciones comerciales.

Integridad de los datos.

Hay que tener los mecanismos necesarios para asegurarse que los datos no sean alterados cuando sean transmitidos por Internet, proteger los servicios del FTP y de correo electrónico.

Rectificación del origen.

Se debe de proteger al emisor de datos negando el envío de los datos falsos y al receptor negando *la recepción de datos falsos.*

Acceso a Internet.

Es necesario un gateway para interceptar y examinar todos los mensajes que se generan desde y hacia Internet.

Hasta el momento se ha dado una serie de lineamientos de cómo hacer una política de seguridad de red, así como los tipos de ataques más comunes, resumiendo se pueden seguir ciertos pasos para la debida protección de los recursos de la red, por ejemplo:

- **Cuando un hacker se hace pasar por otra persona.** En este caso se recomienda mucho utilizar la autentificación o los certificados digitales, es decir, obligando al usuario a demostrar su identidad, con este medio se tiene la confianza que los usuarios autorizados podrán emplear los recursos de la organización.

- **Un hacker escucha una comunicación privada.** Para esto se recomienda la encriptación, Este tipo de ataque sucede cuando por algún medio (por un sniffer o un vampiro interceptor) se intercepta la comunicación que hay de un host a otro, pero con canales encriptados sólo los usuarios autorizados puede desencriptarlos.

- **Un hacker se "cuelga" entre dos hosts e intenta sustituir a alguno de ellos.** Se recomiendan los certificados o firmas digitales, para esto es necesario que ambas partes prueben que conocen la llave secreta. Esto se realiza por medio de un mensaje con una firma digital que es enviada a la otra y esta a su vez envía su mensaje certificado.

- **Alteración de direcciones.** Este ataque se caracteriza por el hecho de que el atacante adquiere una dirección de un sistema para usarse en otros con diversos propósitos; para contener esto, se usa un firewall que pueda rechazar los paquetes que contengan direcciones alteradas y también rechaza los intentos de los paquetes que salgan a través del firewall a una dirección conocida de la red interna.

- **Datos diddling.** Es cuando un hacker cambia los datos mientras son enrutados desde el origen al destino; se usa una recopilación de mensajes encriptados, los cuales usan segmentos aleatorios del mensaje original que el receptor puede comparar el mensaje recibido con el mensaje original. En una parte donde la información puede ser desencriptada, alterada y reencriptada. Además ofrece un medio de autentificación de la integridad de los datos.

- **Ataque de diccionario.** Donde el hacker utiliza combinaciones para adivinar un password, por ejemplo se puede tener un diccionario con un millón de passwords conocidos y tratar cual de ellos se ajusta a la implementación. Para contrarrestar esto se utilizan passwords fuertes, estos contienen números y letras además que no contienen nombres, palabras o referencias que sean fáciles de adivinar.

- **Ataque de réplica.** Donde el hacker captura un mensaje y tiempo después lo retransmite al destinatario original, no puede desencriptar el mensaje, pero puede beneficiarse de los servicios que presenta las réplicas de los mensajes. Se corrige con una secuencia de números o una marca de tiempo el cual indica cuándo fue enviado el mensaje y de esta manera alertar al destinatario de un ataque de este tipo.

- **Ataques de negación de servicio.** Donde el atacante trata de saturar el servidor con requerimientos o falsificarlos con requerimientos originales. Si el atacante no obtiene el servicio, este es negado a los demás usuarios. Para disminuir esta incidente, son utilizados la autentificación y los servicios de filtrado de paquetes. En el caso de la autentificación de los usuarios, sólo las partes autorizadas pueden enviar mensajes; monitoreando el origen de los mensajes a través de un filtrado de paquetes se puede configurar el servicio de tal manera que una organización puede rechazar los mensajes

con parámetros establecidos (el origen, la información del encabezado, el subject, el tamaño, etc.).

Además de eso, el firewall es muy útil para tener un control de los movimientos que hay entre una parte confiable (una red, un conjunto de redes o subredes) y una parte no confiable (Internet, canales privados) - en los dos siguientes capítulos se expondrán estos puntos -, pero también las aplicaciones son importantes, hoy en día se cuentan con diversos protocolos de Internet que tienen un estándar de seguridad:

S-HTTP[1], Secure HTTP. Transmite mensajes individuales, se puede complementar con el SSL, no todos los browsers lo soportan.

IPSEC, IP SECurity[27]. Es un protocolo que tiene servicios de encriptamiento que son flexibles con combinaciones de autentificación, integridad, control de acceso y confidencialidad.

PCT, Private Communication Technology[28]. Es una combinación de algoritmos de encriptamiento y llaves de sesión (simétricas) y se autentifica el servidor al cliente (y viceversa) con base en llaves públicas asimétricas certificadas. Cuando se empieza a transmitir el protocolo de la aplicación (HTTP, FTP, telnet, etc.) todos los datos son encriptados usando la llave de sesión. Cuenta con una "caja negra" que es capaz de disponer la validación de los certificados *recibidos de una manera satisfactoria para la implementación del usuario.*

S/MIME, Secure Multi-Purpose Internet Mail Extensions[1]. Es una versión nueva del protocolo MIME que tiene soporte para el encriptamiento de mensajes.

SKIP, Simple Key Management for Internet Protocol[29].

SSL, Secure Socket Layer[1]. Desarrollado por Netscape para transmitir documentos sobre Internet, utiliza una llave privada para encriptar los datos que se van a transmitir, los browsers más populares lo utilizan (Netscape e Internet Explorer), es empleado para obtener información confidencial del usuario, como su tarjeta de crédito. Por convención, una página que requiere una conexión de este tipo empieza con *https.*

En caso de las aplicaciones API (Application Programming Interface) se puede utilizar los siguientes estándares

- GSS-API, Generic Security Service API.
- SSPI, Security Support Programming Interface.
- CryptoAPI.

De la información que viaja por medio de Internet va necesitando certificados digitales que son obtenidos de una autoridad certificadora confiable para poder encriptar mensajes y autentificar los receptores y los remitentes. En caso de tener una llave privada comprometida se invalidan por medio de una lista de revocación de certificados (CRL, Certification Revocation Lists), esta lista forma parte de una infraestructura de llaves públicas la cual es usada para transacciones seguras en Internet.

2.12 Características de un sistema de seguridad[7].

Hay que tener en cuenta ciertas medidas que se deben de tomar si se planea tener un sistema de seguridad:

- Identificación y autentificación. Se tiene que usar un password o alguna otra forma de identificación en pantalla a los usuarios y checar las autorizaciones.

- Control de acceso. Los usuarios autorizados no puedan tener acceso al material que no ven.

- Bitácoras. Ligar las actividades de la red a la identidad del usuario.

- Determinar auditorias. Determinar cuando ha ocurrido una violación de seguridad y si hubo pérdidas.

- Reutilización de objetos. Asegurarse de que los recursos pueden ser seguros con los usuarios.

- Exactitud. Protección contra los errores y modificaciones no autorizadas.

- Confiabilidad. Tener una protección en contra de la monopolización de cualquier usuario.

- Intercambio de datos. Promover la transmisión segura de datos por canales de comunicación.

Capítulo III

Diseño de un firewall

Desde la década de los ochentas, el término firewall ha sido considerado para describir un dispositivo que bloquea el tráfico de la red no deseada mientras permite el tráfico a las otras. La primera descripción publicada de un "firewall" moderno, y el uso de este nombre fue incluido en el libro "Practical Unix Security" escrito en 1990 por Simson Garfinkel y Gene Spafford y publicado en 1991. La primera descripción de un firewall, fue hecha por Bill Cheswick.

Hoy en día un firewall es una combinación de componentes de hardware y software que ofrece un punto de control entre una red confiable (la red corporativa de una empresa) y una red no confiable (Internet) – o entre varias redes - por el cual puede fluir la información hacia ambos lados. No es costeable para muchas organizaciones adquirir una línea dedicada para realizar transacciones con sus clientes, proveedores y empleados, se tiene que emplear Internet como medio de transferencia; pero el acceso a Internet no es confiable por motivos ya vistos en el capítulo II de este trabajo.

3.1 Componentes de un firewall.[5,13,18,19]

Los componentes primarios de un firewall son:

- Políticas de red.
- Mecanismos de autentificación avanzados.
- Filtrado de paquetes (packets)
- Aplicaciones gateways.

Su descripción se explica a continuación:

3.1.1 Políticas de red.

Hay dos niveles de políticas de red que influencian directamente al diseño, la instalación y uso de un firewall. La política de alto nivel es un beneficio específico, la política de acceso a la red que define estos servicios que pueden ser accesados o negados explícitamente desde la red restringida, como estos servicios deben ser utilizados y las condiciones de excepción de esta política. La política de bajo nivel describe cómo el firewall puede actuar en las restricciones al acceso y filtrando los servicios que están definidos en la política de alto nivel.

Hay varios puntos a desarrollar, antes de elegir alguna arquitectura de firewall; los cuales se explican a continuación:

3.1.1.1 Política de acceso a los servicios.

La política de acceso a servicios enfocada en el uso específico de Internet y acaso todos los accesos externos en la red (conexiones dial-in, SLIP y PPP), es una extensión de la política organizacional que observa la protección de los recursos de información en la organización. Para que un firewall funcione, la norma debe de ser real y trazarse después de la implementación del firewall. Debe de balancear la protección de la red contra riesgos conocidos, mientras se permite el acceso a los recursos de la red por parte de los usuarios. Si se niega o se restringe el servicio, es indispensable la resistencia de la política de acceso a los servicios para prevenir el acceso a los controles del firewall. Sólo una administración cerrada puede prevenir esta situación.

Se puede implementar políticas de acceso a los servicios; por ejemplo, una norma es que se puede no permitir el acceso al sitio desde Internet, pero permitiendo el acceso desde el sitio hacia Internet. Otra política puede permitir algunos accesos desde Internet, pero solamente a los sistemas seleccionados como servidores de información y de e-mail. Frecuentemente se implementa la política de acceso a los servicios para permitir que algunos usuarios accesen de Internet al servidor interno, pero este acceso puede garantizarse y sólo si es necesario se combinará una autentificación más avanzada.

3.1.1.2 Diseño de la política del firewall.

Aquí se definen las reglas a usarse para implementar la política de acceso a los servicios. Se diseña esta política considerando las capacidades y limitaciones del firewall así como los peligros y las debilidades del TCP/IP, pero generalmente se implementan alguno de estos diseños básicos:

1. Permitir cualquier petición de servicios si no esta expresamente prohibido ó

2. Negar cualquier servicio si no esta expresamente permitido.

Si se implementase la primera política, permitiría que pasaran todas las peticiones al sitio por default, con la excepción de aquellos servicios que la política de acceso a los servicios ha identificado como deshabilitado. Si es el caso de la segunda política, niega todos los servicios por default, pero permite el paso a aquellos servicios que están identificados como "permitidos", esta política sigue el modelo de acceso clásico usado en todas las áreas de seguridad de información.

La primera política es menos deseable, dado que se puede accesar a nuevos servicios *que no estén contemplados en la política o ejecutar servicios que no estén en los puertos estándar* TCP/UDP que no tengan el estatus de "acceso denegado". Algunos servicios como X Window, FTP, Archie y RPC no pueden ser filtrados fácilmente y son mejor acomodados en la primera política. La segunda política es fuerte y segura, pero es más difícil de implementar y puede afectar a los usuarios en los servicios seguros (como los mencionados) que pueden ser bloqueados o restringidos.

La relación entre la política de acceso al servicio de alto nivel con el de bajo nivel se refleja en la relación existente a la implementación de la política de acceso al servicio; esto depende en gran medida de las capacidades y limitaciones del firewall, como los problemas de seguridad asociados con los servicios de Internet que son buscados. Por ejemplo, la búsqueda de servicios definen la política de acceso a los servicios que puede ser de negar el acceso si los problemas de seguridad en esos servicios pueden ser efectivamente controlados por la política de bajo nivel y la seguridad de la red toma precedencia sobre otros factores. En otras palabras si una empresa depende en gran medida de esos servicios, tiene que aceptar el alto riesgo y permitir el acceso a estos.

La política de acceso a los servicios es el componente más importante, otros componentes son usados para implementar y reforzar la política. La eficiencia del firewall al momento de proteger la red depende del tipo de implementación usada, el uso de los procedimientos exactos del firewall y la política de acceso a los servicios.

La política resultante[23] debe ser entendible, tomando en cuenta el contenido de la figura 14.

Por años, los usuarios son aconsejados en seleccionar passwords que sean difíciles de obtener; sin embargo, aunque los usuarios siguen este consejo, el hecho de que los intrusos puedan monitorear Internet en busca de passwords que son transmitidos desencriptados marca la obsolescencia de los passwords tradicionales.

¿Qué tipo de servicio de Internet se plantea usar?.
¿Dónde pueden ser utilizados estos servicios?. Es decir, de manera local, a través de Internet, acceso dial desde el hogar o desde otra red (que es externa).
¿Cuáles características adicionales - la encriptación – pueden ser soportadas?.
¿Cuáles riesgos están relacionados al ofrecer estos servicios y su respectivo acceso?.
¿Cuál es el costo, de control e impacto en la red al implementar un esquema de control?.
¿Qué suposiciones son hechas acerca de la seguridad contra la facilidad de uso?. Aquí puede ganar la seguridad si un servicio es muy riesgoso o muy costoso para asegurar.

Fig. 14 Cuestionamientos de una buena política de seguridad.

3.1.2 Medios de autentificación[13].

La autentificación confirma la identidad de un usuario que requiere algún servicio por medio del firewall. Hay tres métodos para verificar la identidad de una persona:

1. Es conocido como "something known", en donde se puede utilizar una contraseña secreta como el password. Hay dos tipos:

- **Password multiuso.** Son los más usados debido a que son baratos, fáciles de usar y administrar y no necesitan hardware especial; y los más comentados porque ese password no se modifica continuamente y alguien puede "verlo" al momento de transmitirlo desde un servidor remoto.

- **Password de un uso.** Fueron introducidos para contrarrestar a las debilidades del anterior y se puede utilizar una sola vez, es decir que el usuario carga una lista de passwords o tokens que generaran el siguiente password. S/Key es un ejemplo de este tipo de password en donde el host o el firewall necesitan el último password y la clave del usuario para validar el siguiente password.

2. Llamado "something possessed", el cual requiere una llave para un candado o una tarjeta inteligente (smartcard).

También conocidos como Hand-Held Authenticators (HHA) en donde se requiere introducir un número aleatorio o "reto" que es dado por el firewall durante el proceso de autentificación, este formula una respuesta basándose en una llave encriptada la cual es conocida por el dispositivo y el firewall y el usuario da la respuesta al firewall, es un método seguro debido a que se usan números aleatorios.

3. Nombrado "something embodied" que necesita una huella digital o el patrón de la retina del usuario.

Pero puede suceder un ataque del tipo hijacking en el cual se interceptan los paquetes, los cuales contienen la información de la identificación de la sesión y sustituye al usuario original, el atacante toma la "identidad" y los privilegios de este. Esto sucede si es en el mismo host con el "login" del usuario o en la ruta de la comunicación. Para esto se crearon las Redes Privadas

Virtuales (VPN, Virtual Private Network) en donde sea necesaria alguna modificación a un cliente de algún software o un medio especial adicional a la computadora.

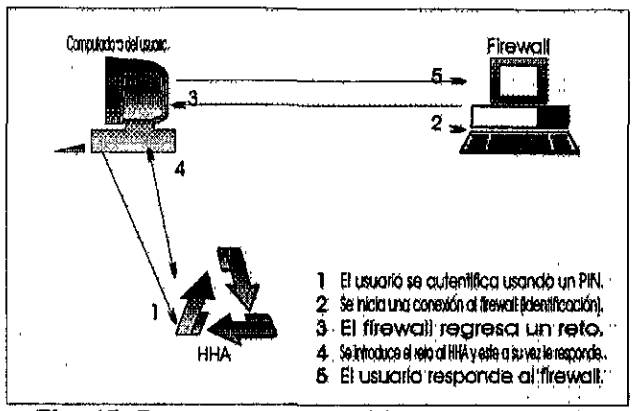


Fig. 15. Pasos para autentificar a un usuario.

Pero cómo puede el firewall requerir y obtener la información para autentificar debidamente al usuario, para eso se tiene que seguir uno de dos caminos:

3.1.2.1 Autentificación In-Band[13].

Consiste en que el firewall pide y obtiene la información de autentificación usando la conexión original, hay varios protocolos que utilizan este tipo de autentificación como el telnet y el FTP en donde se puede pedir en la misma conexión el login, el password o la respuesta que requiere el método HHA.

3.1.2.2 Autentificación Out-of-Band[13].

Consiste en otra conexión efectuada entre el firewall y el usuario o el host del usuario que requiera información, para este requerimiento es necesario que un programa este instalado en la estación de trabajo del usuario, aunque reduce el número de procesos de autentificación del usuario. En algunos casos se puede tener varias autentificaciones; por ejemplo, al accesar a la estación de trabajo propia, luego al firewall y por último al sistema; para desconcentrar este cuello de botella, se utilizaría la estación de trabajo para requerimientos que llegan y que sean requeridos desde algún firewall o sistema externo.

3.1.3 Filtrado de paquetes (packets filtering)[13,19,23].

El filtrado de los paquetes IP (fig. 16) es usado en un ruteador de filtrado de paquetes o en un firewall con filtrado de paquetes, este puede filtrar los paquetes basándose en algunos de los siguientes campos:

Dirección IP origen.
Dirección IP destino.
Puerto de origen TCP/UDP.
Puerto de destino TCP/UDP.

Un ejemplo de estas reglas puede verse a continuación:

Ejemplos de reglas de filtrado (archivo de configuración del TCP_Wrappers ver 7.6).

ALL: 132.248.80.198

in.rexecd: LOCAL, 132.248.80.161
rpcbind: 132.248.80.159
ALL: 148.213.18.149
ALL: 132.248.80.164

En donde se les permite todo tipo de servicios a las direcciones 132.248.80.198 132.248.80.164 y 148.213.18.149 y todo las demás esta negado el acceso a los servicios del host en donde se encuentre este archivo.

No todos los ruteadores de filtrado de paquetes actuales pueden filtrar el puerto de origen TCP/UDP. Algunos ruteadores examinan en cuales de las interfaces de red del ruteador llega un paquete, puede usarse como un criterio adicional de filtrado. Algunos servidores UNIX ofrecen esta cualidad.

El filtrado puede usarse en una variedad de formas para bloquear las conexiones desde o hacia una red o servidor en específico, y bloquear las conexiones en los puertos específicos. Un sitio puede bloquear las conexiones de alguna dirección, como los servidores o sitios que se consideren hostiles o no confiables. Adicionalmente, se pueden bloquear las conexiones del exterior (con excepción del protocolo SMTP para recibir correo electrónico).

3.1.3.1 Protocolos a filtrar.

Esto va a depender de la política de acceso a la red, en la cual los sistemas tienen acceso a Internet y el tipo de acceso a permitir (ya sea por telnet, ftp o e-mail –smtp -).

Los siguientes servicios tienen alguna vulnerabilidad – las cuales van surgiendo día a día - y son generalmente bloqueados por un firewall para accesar o separarlos del sitio:

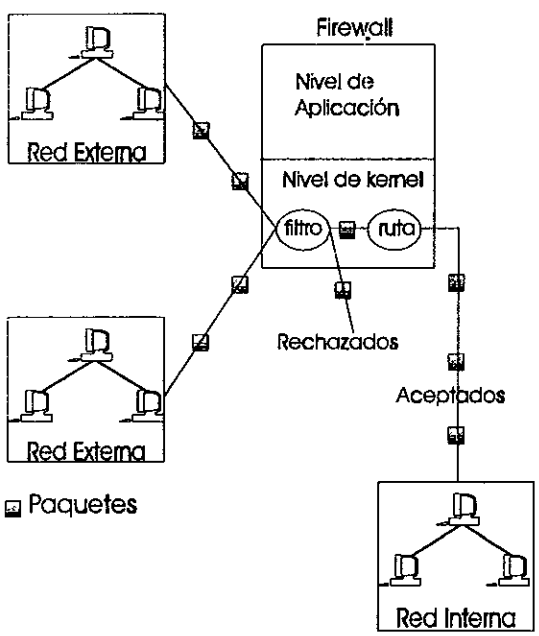


Fig. 16. Filtrado de paquetes.

tftp, puerto 69, trivial FTP, es usado para botear (inicializar) estaciones de trabajo, terminales y ruteadores, puede ser usado para leer cualquier archivo del sistema si es configurado incorrectamente.

X Window, Open Windows, puertos 6000+, puerto 2000, puede fugarse información del despliegue de X Window incluyendo todas las claves.

RPC, puerto 111, Remote Procedure Call esta incluido en NIS y en NFS, los cuales pueden ser usados para leer sistemas de información como los passwords, leer y escribir en los archivos, etc.

rlogin, rsh y rexec, puertos 513, 514 y 512, estos servicios, si se encuentran mal configurados pueden permitir accesos no autorizados a las cuentas y a los comandos.

Otros servicios, pueden ser filtrados y es posible restringir su acceso a los sistemas que lo necesiten, por ejemplo:

telnet, puerto 23, es frecuentemente restringido a los sistemas confiables.

SMTP, puerto 25, restringido a un servidor de correo electrónico central.

RIP, puerto 250, Routing Information Protocol, puede ser cambiado para direccionar el ruteo de paquetes.

DNS, puerto 53, zona de transferencia de servicio de nombres de dominio, contiene nombres de los servidores e información acerca de los servidores que puedan ayudar a los atacantes, puede ser alterado.

UUCP, puerto 540, Unix-to-Unix CoPy, mal configurado puede ser usado para acceso no autorizados.

NNTP, puerto 119, Network news Transfer Protocol, para accesar y leer noticias en la red y

gopher, http, puerto 70 y 80, información de los programas de clientes y servidores gopher y WWW, pueden ser restrictivos aplicando un gateway que contiene los servicios proxy.

Mientras algunos de estos servicios como el TELNET o el FTP tienen riesgos inherentes, el hecho de bloquear el acceso a estos servicios pueden ser completamente drástico en muchos sitios. No todos los sistemas requieren el acceso a estos servicios; por ejemplo, restringir el acceso a telnet o FTP desde Internet a aquellos sistemas que "piden" el acceso puede ofrecer seguridad sin afectar a la conveniencia del usuario. Si se restringe el NNTP a los sistemas que lo necesiten ayudaría a crear un ambiente de red más claro y reduciría el riesgo de explotación y del descubrimiento de vulnerabilidades y riesgos.

3.1.3.2 Problemas con los ruteadores de filtrado de paquetes.

Por desgracia esta aparente facilidad tiene varios problemas los cuales son:

A) Las reglas del filtrado de paquetes son complejas al especificarse y no se prueba fácilmente la verificación de lo correcto de las reglas (otros son probados manualmente). Algunos ruteadores no ofrecen la capacidad de logeo, si las reglas del ruteador permite pasar a los paquetes peligrosos, estos no pueden ser detectados mientras ocurre un rompimiento.

B) En otras ocasiones, las excepciones en las reglas se permiten tipos de accesos que regularmente son bloqueados, pero estas excepciones pueden hacer a las reglas de filtrado más complejas de lo que se pensaba.

C) Algunos ruteadores no filtran el puerto de origen TCP/UDP, lo que puede hacer de las reglas de filtrado mucho más complejas y abrir "agujeros" en el esquema del filtrado, por ejemplo, un problema en el que los sitios desean permitir ilimitadas conexiones SMTP, las conexiones TCP incluyen un puerto de origen y de destino. En el caso de un sistema que inicializa una conexión

SMTP al servidor, el puerto de origen puede ser escogido de manera aleatoria como el 1024 u el puerto de destino el 25, el puerto en que el servidor SMTP lo recibe. El servidor regresaría los paquetes con el puerto de origen número 25 y el puerto de destino al puerto escogido de manera aleatoriamente por el cliente. Si un sitio permite las conexiones SMTP de manera ilimitada y extralimitada, el ruteador permite en ambas direcciones un puerto de destino y un puerto de origen mayor a 1023. Si el ruteador puede filtrar el puerto de origen, se puede bloquear todos los paquetes que llegan al sitio que tengan un puerto de destino mayor a 1023 y un puerto de origen mayor a 25. Sin la habilidad de filtrar en el puerto de origen, el ruteador permite conexiones que usan un puerto de origen y destino mayores a 1024. Los usuarios podrían ejecutar servidores desde el puerto 1023 en adelante y estos rodearían la política del filtrado (el sistema de telnet de un sitio recibe las conexiones en el puerto 23 pero pueden recibirse en el puerto 9876; los usuarios en el Internet pueden hacer telnet si el ruteador bloquea el puerto de destino 23).

D) Otro problema es el número de servicios RPC que son difíciles de filtrar efectivamente, debido a la asociación de los servidores que reciben en los puertos que son asignados aleatoriamente al inicializar el sistema. El servicio *portmapper* mapea las llamadas iniciales a los servicios RPC al asignar el número de servicios, pero esto no es equivalente desde el ruteador de filtrado de paquetes. Debido a que el ruteador no puede interpretar los puertos en que el servicio reside y no es posible bloquear completamente esos servicios a menos que se bloquee todos los paquetes UDP (que usan los servicios RPC), esto bloquearía servicios como el DNS.

E) Los ruteadores con más de dos interfaces no tienen la capacidad de filtrar los paquetes debido a que no saben en cuál interface entraran los paquetes y en cuál interface los paquetes saldrían. Filtrando los paquetes (que llegan y que se van) simplifica las reglas de filtrado de paquetes y permitiría al ruteador determinar con más facilidad si una dirección IP es válida o es alterada; sin esta capacidad, los ruteadores impedirían implementar estrategias de filtrado.

Los ruteadores del filtrado de paquetes pueden implementarse en las políticas de alto nivel o de bajo nivel (hacer referencia) y entonces el conjunto de reglas tiene que ser menos flexible.

3.1.4 Aplicaciones gateways[13,19,23].

Para contrarrestar algunas de las debilidades asociadas con el filtrado de paquetes, el firewall necesita usar software de aplicación para adelantar y filtrar las conexiones de los servicios como TELNET o FTP. Esta aplicación es conocida como servicio proxy, mientras que el servidor que lo ejecuta es referido como una aplicación del gateway, estas y los ruteadores de filtrado de paquetes pueden combinarse para ofrecer grandes niveles de seguridad y flexibilidad en vez de que se usen individualmente.

Como un ejemplo, considérese un sitio que bloquea todas las conexiones TELNET y FTP usando un ruteador de filtrado de paquetes. El ruteador por medio de la aplicación gateway TELNET/FTP permite a los paquetes del TELNET y FTP ir solamente hasta un servidor. Un usuario que se desee conectar a un sitio tendría que conectarse primero en la aplicación gateway, y luego en el host destino, por ejemplo:

1. Primero un usuario se conecta por medio de TELNET a la aplicación gateway e ingresa su login en el host interno.

2. El gateway revisa la dirección IP de origen del usuario y acepta o niega de acuerdo a los criterios que se tengan.

3. El usuario puede necesitar una autentificación (posiblemente usando un dispositivo de password de un tiempo)

4. El servicio proxy crea una conexión TELNET entre el gateway y el host interno

5. El servicio proxy pasa los bytes entre las dos conexiones

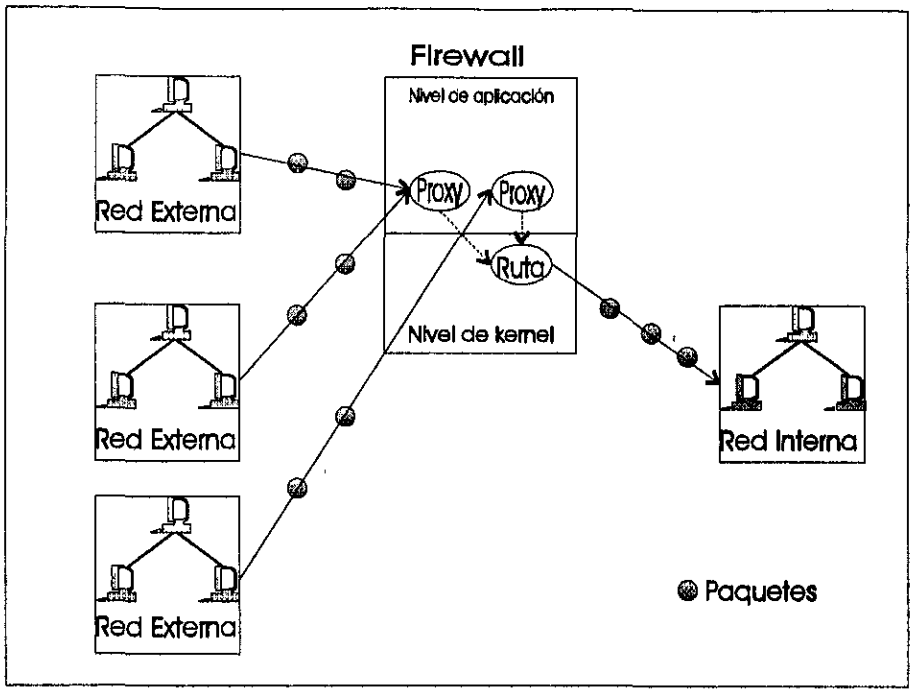


Fig. 17. Aplicación gateway.

6. La aplicación gateway identifica la conexión.

Por ejemplo, un beneficio de usar los servicios proxy (fig. 18) es que el protocolo puede ser filtrado. Por ejemplo, algunos firewalls pueden filtrar las conexiones FTP y negar el uso del comando put, lo cual se usa si se busca garantizar que los usuarios no puedan escribir por ejemplo en un FTP anónimo. Un ejemplo de la configuración del un servicio proxy puede verse a continuación:

Archivo de configuración netperm-table del fwtk ver 2.0

```
tn-gw:      denial-msg    /usr/local/etc/tn-deny.tx      #mensaje de negacion de servicio
tn-gw:      welcome-msg   /usr/local/etc/tn-welcome.txt  #mensaje de bienvenida
#tn-gw:     help-msg      /usr/local/etc/tn-help.txt     # mensaje de ayuda
tn-gw:      timeout 3600                                 # Tiempo maximo de "ocio"
netacl:     132.248.80.165 127.0.0.1
tn-gw:      * 132.248.80.* -passok –xok                  # permite el paso a cualquier red
```

Con la ayuda de este se puede configurar mensajes de bienvenida (*/usr/local/etc/tn-welcome.txt*) de negación del servicio y de permitir el paso a cualquier red al dominio 132.248.80.

Las aplicaciones gateway tienen ventajas sobre la base del modelo de permitir el tráfico de las aplicaciones directamente sobre el host interno, las cuales son:

Ocultamiento de la información. En la cual, el nombre de los sistemas internos no necesitan necesariamente conocerse por medio del DNS al exterior, debido a que la aplicación gateway puede tener el nombre del servidor que a su vez es conocido en el exterior.

Ventajas.	Desventajas.
Se pueden tener clientes modificados en la computadora del usuario.	Se tiene que desarrollar un proxy para cada servicio.
Puede ser que no se modifiquen los clientes, y el usuario no conoce la existencia del firewall.	
Los paquetes IP no pasan directamente entre el host de origen y el host de destino.	
El usuario no conoce como se manipulan las comunicaciones.	

Fig. 18. Ventajas y desventajas de los servicios proxi.

Identificación y autentificación robusta. La aplicación del tráfico puede ser preautentificada después si se busca el host interno y puede identificarse efectivamente en vez que se identifique por los métodos estándares.

Costo-efectividad. Debido a las partes del software o hardware para autentificación o identificación, necesitan localizarse en la aplicación gateway.

Reglas de filtrado menos complejas. En la cual las reglas del ruteador de filtrado de paquetes son menos complejas que se tendrían si el ruteador necesitase una aplicación de filtrado de tráfico y dirigirlo a los sistemas específicos. El ruteador necesita permitir el tráfico de la aplicación destinada a la aplicación gateway y negar el tránsito al resto.

La desventaja de todo esto, radica en que dos pasos son necesarios para conectar lo que va llegando o lo que va saliendo en el caso de los protocolos cliente-servidor como el TELNET. Algunas aplicaciones gateway requieren clientes modificados, los cuales pueden ser vistos como una desventaja o ventaja, dependiendo de la facilidad de uso de estos clientes en el firewall. Un TELNET de aplicación gateway (un proxy) no requiere necesariamente un cliente TELNET modificado, sin embargo si se requiere una modificación en la conducta del usuario, el usuario se conecta (sin identificarse) al firewall haciendo ver al usuario que no es posible conectarse directamente al host. Pero con un cliente TELNET modificado puede hacer transparente al firewall, permitiendo al usuario especificar el sistema de destino (lo contrario del firewall) dentro del comando TELNET. El firewall puede servir como ruteador al sistema de destino y así interceptar la conexión y con otros pasos adicionales como una cola del password de un tiempo. Sin embargo se requeriría un cliente modificado en cada sistema.

Las aplicaciones gateway – una clasificación se presenta en el anexo I - son usadas para FTP y correo electrónico (e-mail), X Window y otros servicios. Algunas aplicaciones de FTP incluyen las características de negar los comandos put y get a hosts específicos. Si un usuario externo establece una sesión FTP (por medio de la aplicación FTP del gateway) a un sistema interno como un servidor de FTP anónimo trataría de colocar sus archivos en el servidor. Se puede filtrar el protocolo FTP y negar todas las ejecuciones del comando put al servidor FTP anónimo dado así un alto grado de confiabilidad contando solamente sobre los permisos de los archivos sobre el FTP anónimo configurados correctamente.

Por ejemplo, un servidor de aplicación gateway de e-mail centraliza los mensajes y los distribuye al host interno y a los usuarios. Para los usuarios externos, todos los usuarios internos tendrían la dirección e-mail de la forma:

usuario@emailhost

Donde *emailhost* es el nombre del gateway de e-mail, el gateway aceptaría correos de usuarios externos y los adelantaría a través de otros sistemas internos si fuese necesario. Los usuarios que mandan correos desde algún sistema interno pueden enviarlos directamente desde sus respectivos hosts, o en el caso donde el nombre de los sistemas internos no son conocidos afuera de la subred protegida, el correo se enviaría a la aplicación gateway, los cuales se enviarían al host de destino. Algunos gateways de correo electrónico tienen una versión más segura del programa sendmail para poder aceptarlos.

3.1.5 Puentes y ruteadores[21].

Debido a que algunos de estos términos son nombrados por varios autores, se especifican algunas definiciones que pueden ser útiles.

La función del puente (bridge) en la capa 2 del modelo OSI, es la liga de datos de la subcapa de control de medios de acceso (MAC, Media Access Control)

Los ruteadores (routers) funcionan en la capa de red del modelo OSI.

Los gateways funcionan en la capa 4, la capa de transporte.

Los firewalls no tienen capa, pero previene el acceso de intrusos no deseados e incluyen puentes, ruteadores o gateways. Se puede buscar un dispositivo que proteja contra ataques hacia cualquier capa del modelo OSI, tomando en cuenta lo que hay que proteger, que es lo que se tiene y que se puede proporcionar. Los puentes son muy económicos, muy convenientes y los menos seguros en cuanto a protección; los ruteadores son intermedios y los gateways o pares de gateways pueden ser el menos económico, el menos conveniente pero la protección es más segura.

Los puentes, ruteadores surgieron tiempo atrás para conectar las LAN de una organización, ampliando las limitaciones que imponía el cableado de Token Ring y el Ethernet, pero filtrando a unos usuarios, estas implementaciones ofrecían el ancho de banda disponible sobre un segmento de red.

Las características comunes entre los ruteadores y los puentes son que pueden ligar físicamente LAN separadas.

Son programables, es decir que se puede configurar el filtrado de paquetes y pueden usarse para dividir grandes redes en pequeñas o para excluir usuario.

Debido a que los puentes operan en un bajo nivel, pueden tenerlos de diferentes marcas, pudiendo usar el PPP (Point-to-Point Protocol - un estándar de ruteador -), los más antiguos usan las especificaciones propias del fabricante

3.1.5.1 Diferencias.

Las diferencias que existen entre ellos son las siguientes:

El puente funciona en la capa 2 del modelo OSI (la capa de enlace de datos) y con esta en la subcapa de MAC. Los ruteadores funcionan en la capa 3, la capa de red y los gateways funcionan en la capa de transporte.

Los puentes leen la dirección de destino de 48 bits de capa paquete que se conecta a la red y lee la tabla de ruteo interno y toma la decisión. Los paquetes que entran desde direcciones conocidas son enviados a estas direcciones; las entradas de los paquetes de otras direcciones son reenviadas (todos los dispositivos Ethernet y algunos de token ring pueden considerarse para ser puentes). Construyen su propia tabla de ruteo interno vigilando la dirección de origen y de destino, cuando accesa un paquete de una dirección conocida, el dispositivo envía a esa dirección, si se busca una dirección que no se encuentre en la tabla, se permite al paquete continuar a través de la red.

Ventajas.		Desventajas.	
Puente	**Ruteador.**	**Puente.**	**Ruteador.**
➢ Ofrece transparencia para enlazar protocolos.	➢ Conecta cualquier cantidad de protocolos en cualquier medio.	➢ Sólo soporta la topología de árbol.	➢ Velocidad de transmisión de 9800 bits p/seg. cuando hay mucho tráfico.
➢ Soporta cualquier protocolo de transporte.	➢ Soporta varias topologías de red.	➢ No tiene soporte para una cantidad importante de subredes, estaciones y tráfico.	➢ No mantiene un registro de los intentos de acceso dificultando conocer cuales intentos no tienen éxito o si la red esta bajo ataque.
➢ Conecta redes usando varios medios y protocolos de enlace.	➢ Soporta más subredes, más estaciones y más tráfico.		
➢ Es fácil de instalar y fácil de adaptar en una reconfiguración.	➢ Puede programarse para filtrar paquetes.		
➢ Velocidad de transmisión de 19.2 bits.	➢ Debido a que usan el SNMP, pueden ser monitoreados, dados de baja o configurados por medio de control de software.		
➢ Baratos.			

Fig. 19. Consideraciones importantes del puente y del ruteador.

Los ruteadores son más rápidos que los puentes, que permiten los enlaces lógicos de redes separadas, el ruteador puede usarse para redirigir el tráfico en caso de que algún componente de la red falle, traducir un protocolo a otro, tiene además el OSPF (Open Shortest Path First), un estándar desarrollado por el Internet Engineering Task Force (IETF) que permite buscar al ruteador, por momentos el ruteo de bajo costo de un punto a otro, se puede implementar una topología de malla, pero es difícil de proteger. Debido a todo esto, el proceso de los paquetes con los ruteadores puede ser más lento que con los puentes.

Los ruteadores son normalmente filtros de una vía, y es directo en algunos mensajes y mandando otros sobre algunos procesos de basura para procesamiento futuro. Los puentes son transparentes para el usuario. La estación de trabajo rutea explícitamente las direcciones, y transmiten solamente los paquetes que contengan direcciones de destino autorizadas por el ruteador. Debido a que examinan el protocolo de cada paquete que reciben previenen el tráfico de la red que pasa entre las redes, teniendo un firewall para cada segmento individual. En el

ambiente de red donde pueden ser apartados los diferentes segmentos que ejecutan diferentes protocolos, el ruteador puede reforzar la seguridad filtrándolos. A grosso modo estas consideraciones se encuentran en la fig. 16.

3.1.6 Gateways[21].

Son computadoras diseñadas para administrar el enlace entre la red interna y una o más redes externas, algunos de ellos son diseñados para manipular las conexiones de red que transitan hacia dentro o fuera de la red, algunos otros manipulan las conexiones que salen. Para reforzar su seguridad, se tienen que eliminar cualquier medio conocido por los atacantes, por ejemplo:

- ✓ Deshabilitar el IP en el kernel del gateway para que los paquetes no puedan pasar en ninguna dirección.
- ✓ Se tiene que modificar el kernel para limitar las conexiones del TCP desde el exterior hacia un mínimo de puertos: smtp, uucp, named y hostname, Se recomienda no permitir protocolos como el tftp, sunrpc, printer, rlogin o rexec.
- ✓ Eliminar el protocolo de sendmail y reemplazarlo con upas.sendmail.
- ✓ Eliminar los archivos /etc/hosts.equiv y /etc/hosts.lpd
- ✓ Eliminar cualquier programa que no son esenciales para operar como el awk, cc, emacs, sed y similares.
- ✓ Eliminar cualquier demonio que no se necesite como el finger.
- ✓ Cambiar todos los permisos de los directorios al modo 711, los usuarios y los atacantes no pueden ver su contenido, pero el superusuario si, asegurarse que el chmod no este a disposición de cualquier usuario debido a que se pueden hacer cambios a los permisos de los archivos.
- ✓ Eliminar cualquier cosa de valor, ya que únicamente es una barrera y puede ser posible que sea vulnerable para explotarse si un requerimiento no autorizado no puede pasar hacia la red interna, hay que tener especial cuidado con los compiladores y las utilerías.
- ✓ Asegurarse de que el único modo de reprogramar la máquina sea desde el teclado, esto indica que debe de estar en un lugar seguro.

Ahora lo que se tiene que hacer es reemplazar algunas características:

- ✓ Añadir un servicio de "gate" en donde los usuarios internos puedan llamar, ofreciéndolo a las direcciones de Internet deseadas, puede conectar al Socket de un host remoto de Internet, que copie bytes desde el gate al host. El administrador de correos pueda reescribir los encabezados para hacer que todos los correos aparezcan desde el gateway (usuario@apolo.acatlan.unam.mx pueda mandarse como usuario@acatlan.unam.mx). Para manipular las entradas de correo electrónico, es necesario administrar una lista de alias para redireccionar las entradas de correo a los usuarios correctos y locaciones en la red interna; por ejemplo, los laboratorios Bell de AT&T usan atelnet y ptelnet que reemplazan al telnet estándar.

- ✓ El FTP tiene que reemplazarse debido a que se trataría de establecer una conexión entre el host y el gateway propio, lo cual el gateway no lo permite, puede usarse aftp y pftp que suplen a los servicios del FTP estándar.

- ✓ No crear ninguna cuenta de usuario en la maquina de gateway, mas que los que requieran conexiones de entrada como la cuenta de root y algunas otras que son esenciales (admin y syscon) -sysadmin en otros sistemas-.

- ✓ El montaje de los discos debe de ser de sólo lectura, algunos directorios pudieran necesitar el estatus de lectura-escritura, estos pueden localizarse en una partición simple.

- ✓ Actualizar el sistema a la última versión, dado que tiene soluciones para problemas que existían en versiones anteriores.

- ✓ Se tiene que considerar el hecho de reemplazar el password sobre Internet – implementando un servicio de autentificación -, debido a que se puede comprometer (interceptar) y después usarse.

- ✓ Puede ser que el gateway requiera un password encriptado, pero uno o más sistemas internos necesiten algún password, pero estos transitan desencriptados y viajar a través de Internet. Hay que determinar cuáles máquinas tienen passwords desencriptados y buscar el modo de encriptarlos, si no es posible, se tiene que cambiar los passwords frecuentemente, los intentos de acceso al monitor deben permitir una identificación o un nombre de usuario, al mismo tiempo asegurar a los usuarios seleccionados, mostrar a los usuarios su último acceso al sistema y reportar los movimientos que puedan comprometerlo y permitir a los usuarios que cambien el password si se sospecha que esta comprometido el host que actúa como gateway.

- ✓ Hay que considerar el uso de un ruteador para dirigir el tráfico hacia fuera por medio de un puerto sencillo sobre el gateway de la red, y enviarlos al tráfico que entra desde el gateway con ayuda de un controlador y/o un segundo gateway. Si es el caso de una segunda máquina puede tomarse la tarea de remarcar o juntar las conexiones hacia otras máquinas internas ya confirmadas, conectándose al puerto SMTP o a una identificación de destino. Esta segunda implementación puede ofrecer servicios como el uucp, mail y permitir algunos trabajos a los usuarios, pero hay que asegurarse que los servicios de gateway externo estén totalmente restringidos.

- ✓ Para evitar un ataque en el cual los intentos de las llamadas indiquen preparar el servidor gateway en el caso de que se colapse el sistema y prevenir que las identificaciones se actualicen, se tiene que usar sistemas de archivos separados para el directorio del FTP (que es público), la identificación y el directorio /var/spool.

- ✓ Hay que identificar todas las conexiones e intentos de acceso y grabarlas utilizando un archivo tipo log, se recomienda revisar su contenido diariamente para identificar los intentos fallidos registrados en este archivo.

- ✓ Es vital un seguimiento del proyecto.

- ✓ Inicializar la identificación del gateway, basándose en los procesos y los archivos de cuotas, haciendo auditorías de seguridad con regularidad, checando indicios de cambios desconocidos o errores de administración y haciendo ajustes de acuerdo a sus necesidades.

- ✓ Tener el acceso a los newsgroups acerca de los worms, ataques, hoyos de seguridad y parches del sistema con que se cuente en caso de amenazas para descubrir las debilidades.

- ✓ Hacer un respaldo del sistema a menudo para estar preparado a una restauración total del sistema en caso de un ataque.

- ✓ Revisar el gateway en busca de señales de falsificación, para esto se recomienda verificar los archivos críticos y comparar los resultados con los que se tengan almacenados.

- ✓ Si no se busca cualquier indicio en un lapso de tiempo, no es totalmente confiable el gateway y se puede asumir que un atacante ha irrumpido en el sistema pero no se ha detectado.

3.1.7 LAN Switch[43].

Anteriormente, se diseñaban las LAN para compartir recursos a un número relativamente pequeño de usuarios (menos de 50), los cuales podían ser compartir archivos y periféricos – por ejemplo, impresoras, modem -. Debido a los patrones de tráfico consistentes en aglomeraciones pequeñas de grandes cantidades de datos, estas influían en el trabajo de los usuarios debido a que se comparte un canal sencillo de comunicación el cual usaba todo el ancho de banda de la red; es decir, mientras un dispositivo envía datos, los demás esperaban a transmitir sus datos.

Hoy en día, los usuarios requieren un acceso en tiempo real a los recursos de la red, por tanto esta compartición del ancho de banda no es suficiente, el LAN switching permite la efectiva reducción de dispositivos de la red en un segmento compartido, de esta manera se dispone de un mayor ancho de banda y de esta forma puede soportar redes virtuales LAN (VLAN) y grupos distribuidos. Tiene tres arquitecturas: cross-bar (travesaño) con entrada de colas, self-route con memoria compartida y bus de alta velocidad.

3.2. CONSTRUCCIÓN DE FIREWALLS[13,19,23].

Algunos ejemplos de configuración de firewalls son los siguientes:

- Filtrado de paquetes.
- Gateway duales.
- Host protegidos.
- Subred protegida.

Adicionalmente, se puede tener acceso vía módem (dial-in)

3.2.1 Filtrado de paquetes.

El firewall de filtrado de paquetes es el más común y fácil de emplear por pequeño, en sitios sin complicaciones. Sin embargo, se tolera un número de desventajas y es menos deseable un firewall que otro. Básicamente se instala un ruteador de filtrado de paquetes en Internet (o cualquier subred) y se configuran las reglas del filtrado en el ruteador para bloquear o filtrar los protocolos y las direcciones. Los sistemas del sitio usualmente dirigen el acceso a Internet mientras todos o la mayoría de accesos al sistema es bloqueado, Sin embargo, el ruteador podría

seleccionar dependiendo de la política los accesos al sistema y a los servicios. Usualmente los servicios como NIS, NFS y X Window son bloqueados.

Un firewall de filtrado de paquetes presenta las mismas desventajas que el ruteador de filtrado de paquetes, debido a que pueden aumentar como las necesidades de seguridad de un sitio protegido pueden ser más complejas y largas. Incluyen lo siguiente:

- Son pequeños o no tienen capacidad de identificación, esto implica que un administrador no pueda determinar si el ruteador ha sido comprometido o esta bajo ataque.
- Las reglas de filtrado de paquetes son a menudo difíciles de probar, lo cual puede permitir a un sitio abierto tener puntos vulnerables no conocidos.
- Si las reglas de filtrado complejas son requeridas, están pueden ser difíciles de administrar
- Cada host directamente accesible desde Internet requeriría una copia de algún medio de autentificación avanzado.

3.2.2 Gateway dual.

Esta es una mejor alternativa que la anterior. Consiste de un sistema (host) con dos interfaces de red, y con la capacidad de transmitir el IP del host desactivada - las condiciones de default son que el host no puede tener una ruta larga de paquetes entre las dos conexiones de redes -. Además, el ruteador de filtrado de paquetes puede ser colocado en la conexión de Internet para ofrecer información adicional. Esto crea un interior, la subred protegida puede ser usada para localizar sistemas especializados como servidores de información y polos de modems.

Bloquea completamente el tráfico IP entre Internet y el sitio protegido. Los servicios y accesos son provistos por los servidores proxy sobre el gateway. Es un firewall sencillo y muy seguro. Este tipo de firewall implementa el segundo diseño de la política mencionada en la sección 3.1.1.1; negar todos los servicios a menos que estén específicamente permitidos, dado que no pasan los servicios excepto para aquellos que existan en el proxy. La capacidad del host para aceptar los paquetes enrutados desde el origen podría deshabilitarse, pero otros paquetes no podrían ser pasados por el host a la subred protegida. Se puede usar para ejecutar un alto grado de privacia con los ruteadores, para la subred protegida necesita estar contenido por el firewall y no por el sistema de Internet (debido a que Internet no pueden enrutar los paquetes directamente a los sistemas protegidos). Las direcciones IP y alfanuméricas de los sistema del sitio pueden ser ocultadas de los sistemas de Internet, a causa del firewall no pasaría la información del DNS.

Una configuración sencilla para un gateway dual podría ser la implementación de servicios como el telnet y el ftp, además de centralizar el servicio de e-mail en el cual el firewall aceptaría todos los correos del sitio y los remitiría. A causa del uso del sistema del host, el firewall puede alojar software que requieran los usuarios para usar discos de autentificación u otros medios de autentificación avanzados. También puede identificar el acceso y los intentos o pruebas al sistema que indique actividad de intrusos.

Tiene la capacidad de clasificar el tráfico a partir de la información de un servidor que genere otro tráfico hacia y desde el sitio. Un servidor de información puede localizarse sobre la subred entre el gateway y el ruteador. Asumiendo que el gateway ofrece los servicios proxy apropiados para el servidor de información (ftp, gopher o http), el ruteador puede ofrecer el acceso directo de Internet al firewall y forzar el acceso a través de él. Si el acceso directo es permitido al servidor (lo cual es la alternativa más insegura), entonces el nombre del servidor y la dirección IP pueden ser anunciadas por el DNS. Localizando la información del servidor también añade

seguridad del sitio, como cualquier penetración de un intruso al servidor de información para prevenir búsquedas de los sistemas del sitio por el gateway dual.

Su inflexibilidad puede ser una desventaja para algunos sitios. Dado que todos los servicios son bloqueados excepto aquellos que existan en el proxy, el acceso a otros servicios no puede ser abierto; los sistemas que requieran el acceso necesitarían localizarse del lado de Internet del gateway y del ruteador. Sin embargo, un ruteador puede usarse para crear una subred entre el gateway y el ruteador, y los sistemas que requieran servicios extras pueden localizarse en esta parte.

Otra consideración importante es que la seguridad del sistema del host desde el firewall puede ser muy segura, como usar cualquiera de los servicios vulnerables o las técnicas sobre el host pueden ser los primeros en romperlo. Si el firewall esta comprometido, un intruso puede potencialmente revelar el firewall y desempeñar alguna actividad no deseada como redisponer del ruteo IP.

3.2.3 Firewalls de host protegido.

El firewall de host protegido (fig. 20) es más flexible que el gateway dual, sin embargo esta característica es ejecutada con algunos riesgos de seguridad. Combina un ruteador de filtrado de paquetes con una aplicación gateway localizada en la subred protegida del sitio del ruteador. La aplicación gateway necesita una interface de red Los servicios proxy de la aplicación gateway pasan el TELNET, FTP y otros servicios que existen en el proxy, a los sistemas del sitio. El ruteador filtra o se protege de protocolos peligrosos que penetran la aplicación gateway y los sistemas del sitio. Se niega o se acepta el tráfico de la aplicación de acuerdo a las siguientes reglas:

- El tráfico de la aplicación desde los sitios de Internet a la aplicación gateway es enrutada.
- El tráfico restante desde los sitios de Internet es rechazado.
- Los ruteadores rechazan cualquier trafico de alguna aplicación originada del exterior a menos que provenga de la aplicación gateway.

La aplicación gateway necesita solamente una interface de red y no requiere una subred separada entre la aplicación gateway y el ruteador. Este permite al firewall ser más flexible pero ofrece menos seguridad permitiendo que el ruteador pase servicios confiables alrededor de la aplicación gateway y directamente a los sistemas del sitio. El servicio confiable puede ser aquel que en los servicios proxy no exista, y puede ser confiable en el sentido de que el riesgo de usar los servicios que están considerados y son aceptados. Por ejemplo, los servicios de bajo riesgo como el NTP pueden permitir el paso a través del ruteador a los sistemas del sitio. Si requieren acceso al DNS a Internet, el DNS puede permitirse en los sistemas del sitio. En esta configuración el firewall puede implementar una mezcla de los dos diseños de políticas, la proporción de la cual dependan sobre cuántos y qué tipos de servicios son enrutados directamente a los sistemas del sitio.

Esta flexibilidad tiene dos consecuencias. La primera es que ahora hay dos sistemas, el ruteador y la aplicación gateway que necesitan ser configurados adecuadamente; las reglas de filtrado pueden complicarse al configurarlas, dificultando las pruebas tendientes al error que originarían agujeros en el ruteador. Sin embargo, el ruteador necesita un tráfico limitado de aplicaciones hacia la aplicación gateway, el conjunto de reglas no puede ser complejo como para un sitio típico usando un filtrado de paquetes restrinja el tráfico de las aplicaciones a múltiples sistemas.

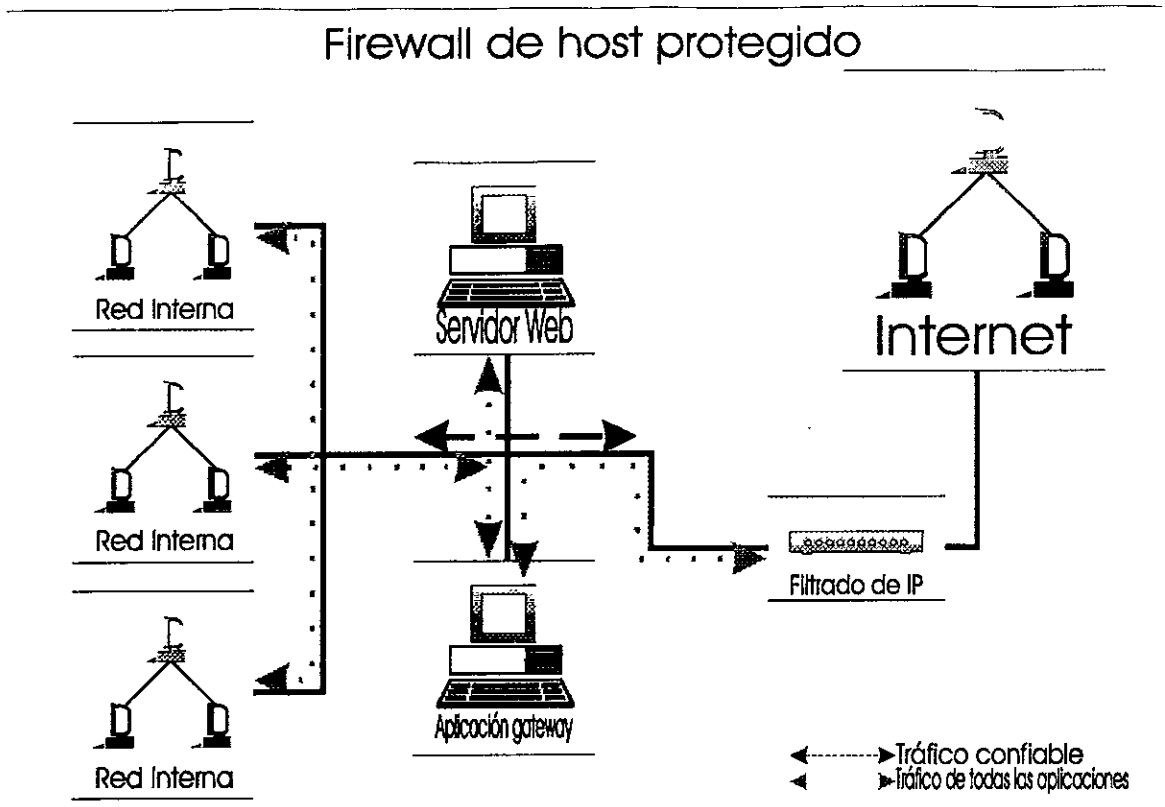


Fig. 20. Firewall de host protegido.

La segunda desventaja es que la flexibilidad abre la posibilidad que la política pueda ser violada, esto no es problema en el firewall de gateway dual dado que es imposible que pase el tráfico, una política más fuerte minimizaría el problema.

3.2.4 Firewall de subred protegida.

Este es una variación del gateway dual y del host protegido (fig. 21), se pueden usar para localizar cada componente del firewall sobre un sistema separado, con lo cual es más grande y flexible, también algunos costos se simplifican, pero cada componente del firewall necesita implementarse solamente para realizar una tarea específica, haciendo al sistema menos complejo para la configuración.

Son usados dos ruteadores para crear una red protegida (en algunos casos conocida como DMZ) contiene la aplicación gateway, servidores de información, colocación de modem y otros sistemas que requieren un acceso controlado. El ruteador muestra la manera en que el punto de conexión al Internet puede enrutar al tráfico de acuerdo con las siguientes reglas:

- El tráfico de la aplicación desde la aplicación gateway a los sistemas de Internet gana enrutamiento.
- El tráfico de correo electrónico desde el servidor e-mail a los sitios de Internet gana enrutamiento.
- El tráfico de las aplicaciones desde Internet a la aplicación gateway gana enrutamiento.
- El tráfico de correo electrónico desde Internet al servidor de correo electrónico gana enrutamiento.

- El tráfico de ftp, gopher, etc. desde INTERNET al servidor de información gana enrutamiento.
- Todo lo demás es denegado.

El otro ruteador restringe el acceso desde Internet a sistemas específicos de la subred protegida y bloquea todo el tráfico al Internet originado de los sistemas que no generen conexión alguna (como una colocación de módem, el servidor de información y los sistemas del sitio). También se puede usar para bloquear todos los paquetes del NIS, NFS o cualquier protocolo vulnerable que no necesite pasar hacia o desde los servidores en la subred protegida.

El ruteador interior dirige el tráfico hacia o desde los sistemas cercano a la subred protegida que funciona de acuerdo con las siguientes reglas:

- El tráfico de las aplicaciones desde la aplicación gateway a los sistemas del sitio ganan enrutamiento.
- El tráfico de correo electrónico desde el servidor e-mail a los sistemas del sitio ganan enrutamiento.
- El tráfico de las aplicaciones a la aplicación gateway desde los sistemas del sitio ganan enrutamiento.
- El tráfico de correo electrónico desde los sistemas del sitio al servidor de e-mail gana enrutamiento.
- Tráfico de ftp, gopher, etc. desde los sistemas del sitio al servidor de información ganan enrutamiento.
- Todo lo demás es denegado.

En el ejemplo anterior, el sistema del sitio no es directamente alcanzable desde Internet y viceversa, como en el gateway dual. La diferencia es que los ruteadores son usados para dirigir el tráfico al sistema indicado, eliminando de tal modo la necesidad de una aplicación gateway dual, si un ruteador es usado como un gateway para la subred protegida. En consecuencia, este tipo de firewall puede ser el más apropiado para aquellos sitios con grandes cantidades de tráfico o sitios que necesitan un tráfico muy rápido.

La ventaja de los ruteadores radica en que el atacante tendría que penetrar ambos para accesar al sistema; la aplicación gateway, el servidor de correo electrónico y el servidor Web pueden configurarse de manera que sean conocidos en Internet; en vez de sistemas que sean conocidos o que puedan usarse desde el exterior como la base de datos del DNS que puede accesarse desde sistemas externos. La aplicación gateway puede contener software de autentificación avanzada para autentificar todos las conexiones que llegan. Esto implica más configuración, pero el uso de sistemas separados por las aplicaciones gateways y el filtrado de paquetes mantiene las configuración más sencilla y manejable.

Este tipo de firewall así como el host protegido es más flexible, permitiendo servicios confiables que pasen entre Internet y los sistemas del sitio. Esta flexibilidad puede abrir puertas de excepción en la política, debilitando al firewall. El firewall de gateway dual es más requerido debido a que no puede ser debilitado (por el hecho de que no pueden pasar los servicios que no se encuentren en el proxy), el firewall de subred protegida es la mejor opción en donde los tiempos de proceso y la flexibilidad son importantes.

Como una alternativa para pasar directamente los servicios entre Internet y los sistemas del sitio, se localizan los sistemas que necesiten los servicios de la subred protegida; es decir, un sitio que no permita el tráfico de X Windows o NFS entre Internet y el sitio. Los sistemas pueden mantener todavía el acceso al sistema del sitio conectándose a la aplicación gateway y reconfigurar el ruteador interno como sea necesario. Aunque no puede ser la solución adecuada, pero es la indicada para sitios que requieran un alto grado de seguridad.

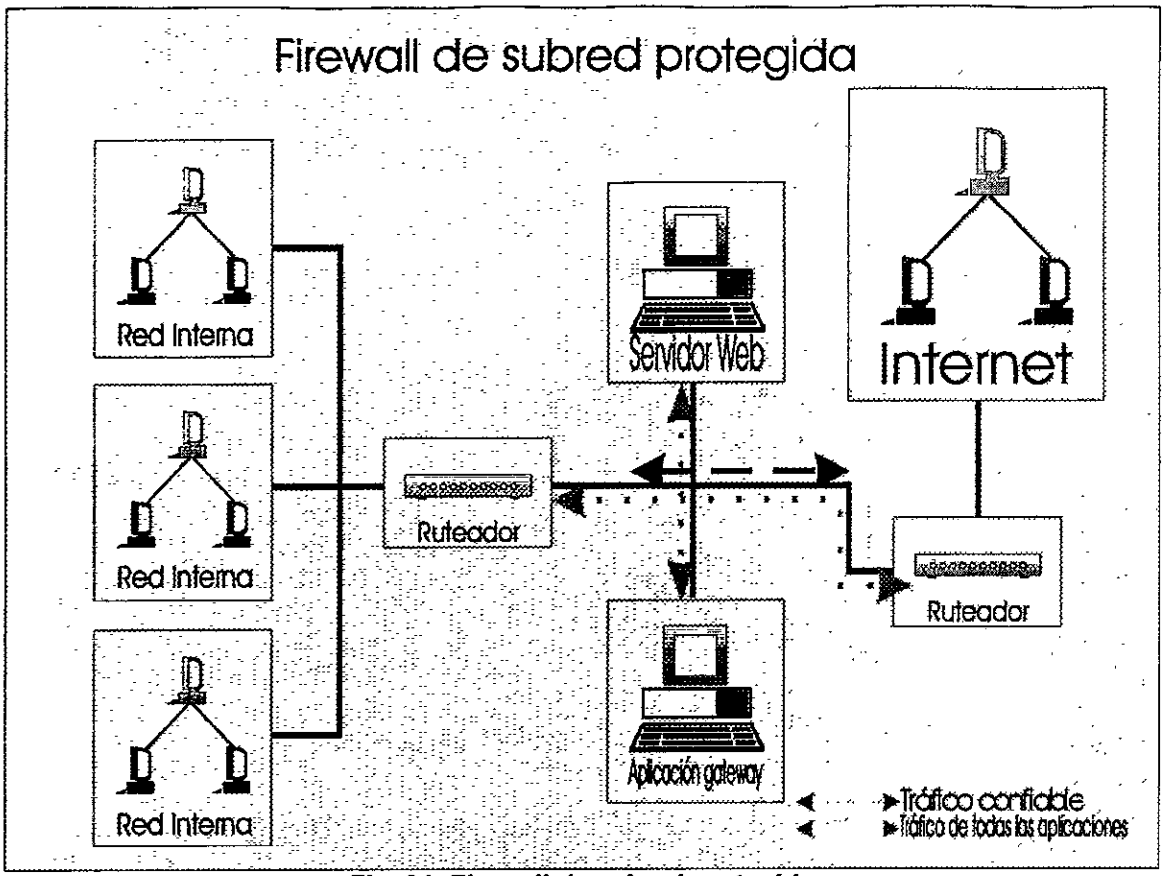


Fig. 21. Firewall de subred protegida.

Existen desventajas en cuanto a la subred protegida; primero, se pueden pasar servicios confiables a través de la aplicación gateway contactando los sistemas internos, con lo cual altera la política, se tiene un lugar en donde se alojan los sistemas que necesitan acceso directo a estos servicios; en segunda, es requerido más énfasis para ofrecer seguridad en los ruteadores de filtrado de paquetes, debido a que son más complejos para configurarlos y los errores pueden causar graves problemas de seguridad.

3.2.5 Modems y firewalls.

En muchos sitios se permite el acceso dial (por teléfono), esto es una potencial puerta trasera que puede desmoronar la protección de un firewall, hay que poner la debida atención en las conexiones de los modems y hacerlas seguras.

Estas conexiones consisten de modems conectados a un servidor de terminal, que es una computadora especializada para hacer conexiones de modem en la red en donde el usuario se conecta por teléfono al servidor, y se conecta a otros sistemas (por medio de telnet). Algunos servidores de terminal ofrecen facilidades que restringen las conexiones a sistemas seleccionados, o pide a los usuarios autentificarse. Alternamente, el servidor de terminal puede ser un sistema de host con modems conectados a él.

Un módem puede estar localizado en la parte de Internet de host protegido, dado que las conexiones desde los modems necesitan estar tratando con la misma suposición como las que se efectúan desde Internet, poniendo la conexión del módem en el exterior del firewall obligándolas a pasar a través del firewall.

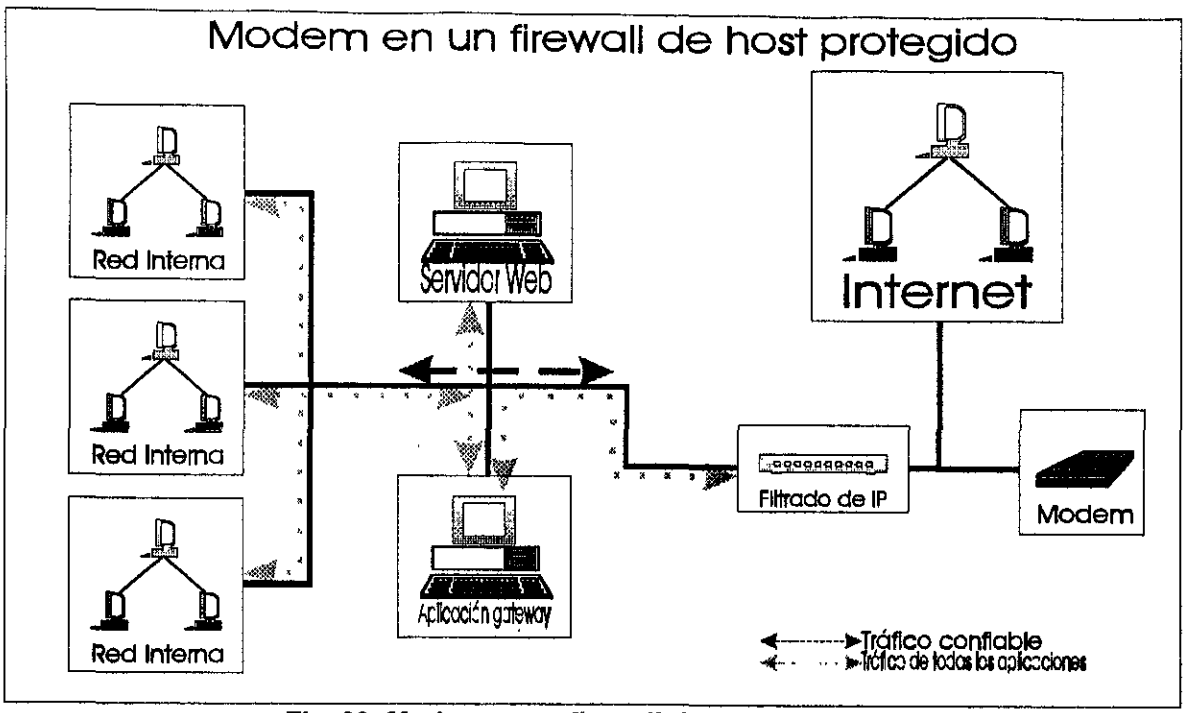


Fig. 22. Modem en un firewall de host protegido.

Los medios de autentificación avanzadas de las aplicaciones gateway pueden usarse para autentificar a los usuarios que se conectan con un módem desde Internet. El ruteador de filtrado de paquetes puede usarse para prevenir dentro de los sistemas las conexiones directas desde el modem.

La desventaja de esto es que el modem esta conectado directamente a Internet y esta más expuesto a un ataque. Si un intruso maneja la penetración del modem, el intruso puede usarlo como base y atacar otros sitios de Internet de tal modo que un servidor de terminal con cualidades de seguridad niegue las conexiones diales a cualquier sistema.

Un gateway dual y una subred protegida (fig. 21 y 22) ofrecen una mejor seguridad para las conexiones de módem, el servidor de terminal esta localizado en el interior de la subred protegida donde el acceso que se recibe o que sale desde la conexión de modem puede controlarse por los ruteadores y las aplicaciones gateway. El ruteador que se encuentra del lado de Internet protege la conexión para cualquier acceso desde Internet a excepción de la aplicación gateway además de prevenir el ruteo entre Internet y el modem. Con la subred protegida, el ruteador conectado al sitio prevendría el enrutamiento entre los sistemas y el modem; con el gateway dual, la aplicación gateway puede prevenir el ruteo. Los usuarios que utilicen una conexión de modem pueden conectarse al sistema o a Internet por medio de la conexión gateway, la cual podría usar medios de autentificación avanzados.

Si un sitio usa cualquiera de estos medios para proteger los accesos diales, es necesario reforzar la política para prevenir que cualquier usuario se conecte con un modem en la red protegida. Si el modem cuenta con características de seguridad, se puede realizar el esquema de seguridad más complejo.

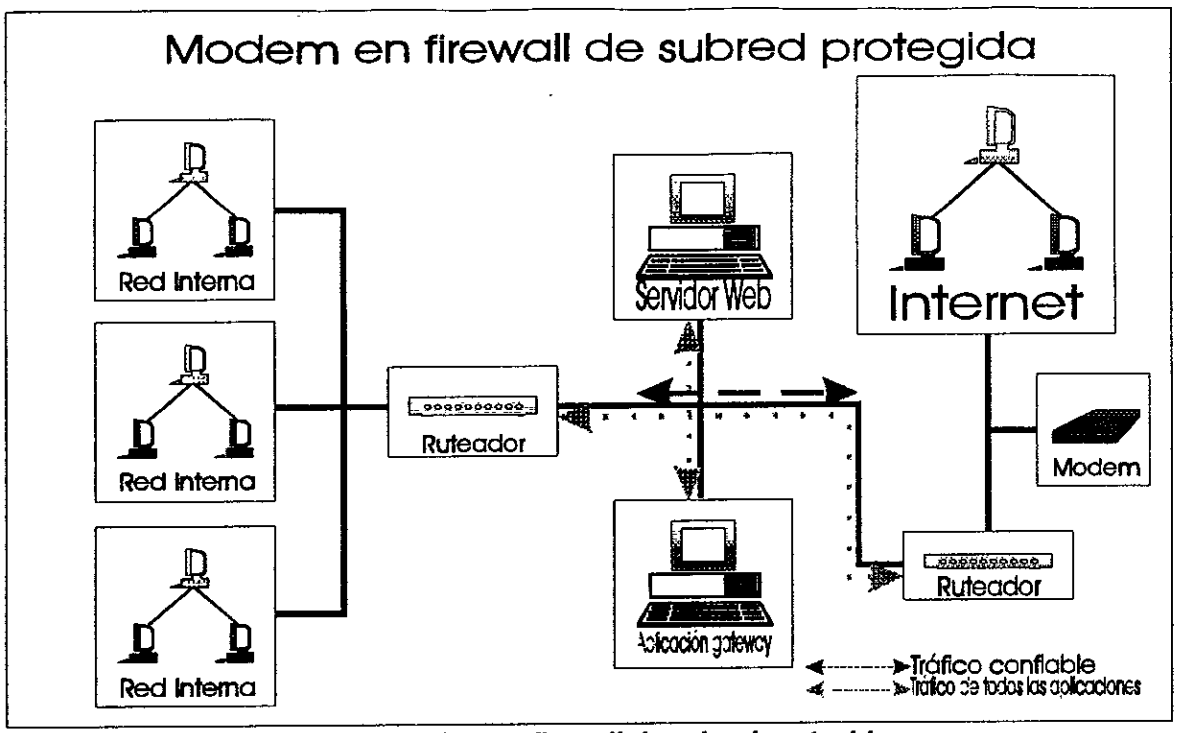


Fig. 23. Modem en firewall de subred protegida.

3.2.6 Nuevas tecnologías.

Afortunadamente, como en otras ramas del conocimiento humano, sigue avanzando las tecnologías, que acarrearon la construcción de firewalls híbridos, algunos ejemplos existentes en el mercado son mostrados a continuación:

Stateful inspection. Debido a que el firewall de filtrado de paquetes examina el tráfico de la red a bajo nivel, se examina cada paquete que llega a una interface, determinando la dirección IP de origen y destino, aplicando las reglas para determinar si pasa el paquete, esta tecnología es menos problemática y la menos segura.

Para eliminar esta debilidad, algunos firewall de filtrado de paquetes añaden nuevas tecnologías (stateful inspection, stateful filtering, stateful multi-layer inspection, cut through proxy y algoritmos de seguridad adaptativos). En este caso consisten de dos componentes:

1. Patrones comparables. El firewall examina todo el contenido del paquete, para conocer más el tipo de información de origen y de destino. La revisión es menos exhaustiva que la que aplica el proxy gateway.

2. Mantenimiento del estado. El firewall mantiene alguna información del estado acerca de los datos actuales de intercambio, esta característica la necesita el protocolo UDP; dado que algunos protocolos con desarrollados en UDP (ping) y en algunos sitios con firewall pueden pasar paquetes UDP a través de él.

En caso de que se ejecute el comando ping en la red protegida, se esperará obtener la información replicada, pero el firewall esta configurado para deshabilitar cualquier paquete ping que venga del exterior; entonces, ¿cómo conocerá el firewall que los paquetes del ping que vienen del exterior son una réplica de la ejecución del ping interior?, Para ello, el firewall mantiene un

estado para que los paquetes UDP puedan seguir los paquetes originales y los de réplica, mientras se previenen acciones en contra algún paquete desconocido.

El posible uso de los filtros del proxy crece y se tiene un mejor control sobre los paquetes de la red, pero no aumenta el poder de los firewalls de filtrado de paquetes; sin embargo, los gateways proxy tienen problemas con los protocolos basados en el UDP y dado que UDP es de bajo nivel es imposible construir un proxy para que se controle el tráfico tipo UDP.

Filtros de paquetes proxy (Proxying packet filters). Es una combinación del firewall de filtrado de paquetes y del firewall de proxy gateway. Aprovechando la cualidad del primero, se filtran paquetes específicos y la del segundo, para algún tipo de paquete específico es enviado al proxy sobre el firewall antes de enviarse a la máquina de destino donde es usado para autentificar.

Por ejemplo, en un sitio que tenga por objetivo permitir el servicio de telnet desde o hacia hosts específicos, pero solamente si el "visitante" primero se identifica por medio de un password de un sólo uso (S/Key, CryptoCard); será necesario un proxy debido a:

1. Se cuenta con un prompt especial para la información de la autentificación.
2. Puede entender el protocolo telnet, y pregunta la autentificación por medio del mismo protocolo.
3. Computa la consistencia de las respuestas de la autentificación.
4. Permite el servicio de telnet si la autentificación es correcta.

En este caso la tecnología de filtrado se usa para examinar el origen y el destino y determina si la conexión se permite, pero con el proxy permite el paso de las conexiones que están autentificadas.

Proxy gateway de filtrado (filtering proxy gateways). Se añaden al proxy gateway las características del filtrado de paquetes, esto no debilita la seguridad de este firewall. Si se establece un túnel de una VPN entre dos firewall (o un cliente) todas las comunicaciones del nivel IP entre los dos sitios son encriptados y cualquier protocolo de la capa IP (incluyendo los protocolos TCP y UDP) pueden pasar a través del túnel encriptado. Generalmente, el firewall no ofrece medios para limitar los protocolos que pueden ser "enviados"; pero si se establece un túnel cualquier protocolo se limita. La máquina externa al final del túnel VPN tiene las mismas capacidades como si estuviera dentro de la parte que protege el firewall y cada máquina es confiable por default debido a que son los extremos del túnel VPN.

Algunos proxy gateways (aplicaciones gateways) ofrecen el filtrado de túneles VPN pudiéndose especificar los protocolos que pueden ser permitidos o negados y la dirección de inicio puede especificarse así como las direcciones de origen y de destino y algún método de autentificación. Estas características permiten añadir control a las ventajas del VPN permitiendo los túneles VPN y mantener seguro el perímetro externo.

Un túnel VPN nulo hace más flexible el proceso de paquetes UDP en el firewall, como el proxy no permite el paso de paquetes UDP el VPN si lo hace debido a que trabaja en la capa de red.

3.3 Políticas del firewall[13,16,19,21,23].

Las decisiones de las políticas reflejan el uso del firewall que esta hecha en conjunción con las políticas de decisión necesarias para asegurar el sitio; esto incluye decisiones concernientes con los sistemas de seguridad del host, acceso dial-in, accesos a Internet, protección de la información fuera del sitio, seguridad de las comunicaciones de datos y otras. Una

política de espera no da efectividad al firewall, se necesita incorporar una política de seguridad fuerte.

3.3.1 Pasos en la creación de una política de acceso a los servicios.

Para llegar a un diseño de política de firewall y al final a un sistema firewall que la implemente, la organización NIST recomienda que el diseño de la política empieza con lo más seguro, negar todos los servicios excepto aquellos que están explícitamente permitidos. El diseño de la política debe de ser entendible y documentar lo siguiente:

- ¿Cuáles servicios de Internet planea usar la organización (TELNET, NFS, FTP)?.
- ¿Dónde los servicios podrían ser usados (en una base local, a través de Internet, acceso por teléfono o desde organizaciones remotas)?.
- Posibles necesidades adicionales como la encriptación o el soporte por teléfono.
- ¿Con qué riesgos se pueden implementar estos servicios y ser accesos?.
- ¿Qué costos hay en términos de controles e impacto en uso de la red para ofrecer la protección?.
- Suposiciones acerca de la seguridad contra la facilidad de uso, la seguridad gana si el servicio en particular es riesgoso o pierde cuando son muy costos para asegurar.

La creación de estos puntos es inmediata, siempre y cuando sea al mismo tiempo interactivo. Supongamos que dos sitios que usan el NFS a través de Internet, el diseño de la política de negar todo no permite el uso del NFS, pero los riesgos asociados con el NFS son aceptados en la organización, se requeriría cambiar el diseño de la política para una menor seguridad, permitiendo todos los servicios excepto aquellos que están específicamente negados y pasar el NFS a través del firewall sobre los sistemas del sitio. Puede tenerse un firewall que localice los sistemas que requiere el NFS en la subred protegida, esto preserva el diseño de la política de negar todo del resto de los sistemas del sitio o los riesgos de usar el NFS pueden ser grandes; el NFS puede tenerse en la lista de los servicios que se usan remotamente.

3.3.2 Flexibilidad en la política.

Cualquier política de seguridad tiene que ser flexible, que contemple el acceso a Internet, los servicios de Internet, el acceso a la red. Esta característica se debe a dos razones: Internet es un flujo de información y las necesidades de la organización pueden cambiar cuando Internet ofrece nuevos servicios y métodos para las actividades empresariales. Los nuevos protocolos y servicios están emergiendo sobre Internet, lo cual lleva a más beneficios para las organizaciones que usan el Internet, pero puede resultar en nuevos incidentes e intereses de seguridad. En este caso, la política necesita ser capaz de reflejar e incorporar estos nuevos paradigmas; otra razón para la flexibilidad es que el riesgo de la organización no permanece estático. El cambio en el riesgo puede ser el reflejo de mayores cambios como nuevas responsabilidades que empiezan a asumirse para la organización, o pequeños cambios como un cambio en la configuración de la red.

3.3.3 Autentificación para usuarios remotos.

Los usuarios remotos son aquellos quienes originan las conexiones al sitio desde cualquier lugar de Internet. Estas conexiones pueden provenir de cualquier fuente, de una línea telefónica, de usuario que se encuentre viajando o que se encuentre trabajando en su casa. Sin tomar en cuenta que todas las conexiones pueden usar la autentificación avanzada del firewall para accesar a los sistemas del sitio, considerando que los usuarios "remotos" no puedan accesar a través de módem no autorizados hacia el firewall. No hay excepciones en esta política, como se puede capturar un password o una línea de módem no controlada que habilita una puerta trasera en el firewall.

Tiene sus inconvenientes: se tiene que incrementar la capacitación al usuario para usar los medios de autentificación avanzada, aumentar los gastos si las claves de los usuarios pueden ser suplantados con discos de autentificación o tarjetas e incrementar la vigilancia en al acceso remoto a la administración del sistema. No se puede instalar un firewall y al mismo tiempo no controlar el acceso remoto.

Las facilidades para los usuarios autorizados es tener acceso remoto a los sistemas, las características de las conexiones diales permiten el acceso donde Internet no esta disponible, pero esto implica ventajas a los posibles atacantes para accesar a nuestros sistemas. Este tipo de usuarios debe de estar consciente de las debilidades que se pueden ocasionar si se descuida el acceso por módem, por ello se deben de tomar las precauciones debidas que son mencionadas en la sección 3.2.5.

Las entradas y las salidas por medio dial pueden y deben considerarse en el diseño de un firewall, el obligar a los usuarios a usar la autentificación avanzada del firewall puede ser reflejo de esta política. Esta puede prohibir el uso de modems no autorizados que estén conectados a los sistemas del host o a una PC si las capacidades del modem son activadas a través del firewall. Una política fuerte que limite los riesgos con un servicio efectivo del modem que limite el número de accesos no autorizados en todo el sitio o en la organización.

3.3.4 Conexiones remotas a la red.

El uso de las conexiones tipo SLIP y PPP mencionadas en la sección 1.8 necesitan considerarse en la política dado que son los modos de comunicación para conectarse por medio del firewall al sitio protegido.

3.3.5 Política del servidor de información.

Un sitio que ofrece acceso público a un servidor de información se puede incorporar en el diseño del firewall. Mientras a este servidor se le diseñan sus lineamientos de seguridad, el servidor de información puede ser que no tenga una vulnerabilidad de seguridad en el sitio protegido. La política refleja la filosofía de que la seguridad del sitio no esta comprometida en el hecho de ofrecer un servicio de información.

Se puede hacer una distinción del tráfico del servidor de información, el tráfico de la información obtenida de un servidor de información de una organización en específico, es fundamentalmente diferente de otros tráficos de "conductas de negocios" como el correo electrónico (u otro tráfico del servidor de información para propósitos de investigación de mercados). Los dos tipos de tráfico pueden tener sus propios riesgos y no necesitan ser incorporados entre sí.

Después de que la política ha sido delineada, hay un número de puntos a considerar para un firewall, algunos de estos son los mismos que se toman en cuenta para otros sistemas de software, estos pasos son:

- Definición de requerimientos.
- Análisis.
- Especificación del diseño.

Y otras consideraciones como:

3.3.6 Contenidos de un firewall.

Se tiene que ofrecer un nivel apropiado de protección de costo-beneficio; sin embargo, ¿qué características mínimas tendría?; por desgracia, no se puede hacer una recomendación especial debido a que cada organización tiene necesidades particulares, pero se debe de contemplar los siguientes requisitos generales:

- El firewall podría soportar el diseño de la política de negar todos los servicios excepto aquellos que están específicamente permitidos, si no es la política justa.
- El firewall podría soportar la política de seguridad, no imponerle una.
- El firewall podría ser flexible, y se dispusiera de nuevos servicios y necesidades si la política de seguridad de la organización cambia.
- El firewall podría contener medios de autentificación avanzados o tendría que contener las conexiones adecuadas para instalar medios de autentificación avanzados.
- El firewall podría emplear técnicas de filtrado que permitan el acceso o nieguen los servicios de un sistema especifico cuando se requiera.
- El lenguaje de filtrado de IP tendría que ser flexible, usar programas amigables y se filtrarían con la cantidad mayor de atributos como fuese posible, incluyendo la dirección IP fuente y destino, tipo de protocolo, puerto TCP/UDP de origen y destino e interfaces que llegan o que se van.
- El firewall usaría servicios proxy para servicios como el FTP y TELNET, que puedan emplearse medios de autentificación avanzados que centralicen el firewall; si los servicios como el NNTP, X Window, HTTP son requeridos, el firewall pueda contar con los servicios proxy correspondientes.
- Tendría la habilidad de accesar al SMTP de manera centralizada, para disminuir las conexiones SMTP entre el sitio y sistemas remotos.
- Se podría accesar públicamente al sitio, pudiendo proteger el servidor de información con el firewall además de negar el acceso a los sistemas que no requieran el acceso público.
- El firewall contendría la habilidad de concentrar y filtrar el acceso dial.
- Tendría mecanismos para identificar el tráfico y actividad sospechosa y tener mecanismos para reducir la identificación y que esta sea leíble y entendible.
- Si se requiere un sistema operativo como UNIX, una versión segura de este debe formar parte del firewall, además de otras herramientas de seguridad necesarias para asegurar la integridad del host del firewall. El sistema operativo debe de tener todos los parches instalados.

Estos son los más requeridos, pero muchos de estos deben de especificarse según las necesidades propias de cada sitio, una definición de requerimientos completa y un alto riesgo impuesto con identificación de más puntos y requerimientos; hay que hacer énfasis de que Internet es una red en constante cambio, nuevas debilidades pueden surgir y nuevos servicios y mejoras a otros servicios pueden representar dificultades potenciales para cualquier instalación de un firewall (y de cualquier esquema de seguridad); es aquí donde la flexibilidad es un punto a considerar para adaptar los cambios necesarios.

3.4 Comprar o construir un firewall[13,19,23].

Algunas organizaciones tienen la capacidad para construir un firewall usando componentes de software y equipamiento disponibles o desarrollar el firewall desde cero, a su vez hay vendedores que ofrecen este tipo de tecnología. Los servicios pueden limitarse teniendo el hardware y software necesario, ofreciendo servicios para desarrollar políticas de seguridad, análisis de riesgos, revisiones y entrenamiento de seguridad.

Antes de tomar una decisión se debe de desarrollar primero una política (explicado en el capítulo II y III) y contar con los requerimientos antes de proceder, si hay problemas en esta parte no hay que dudar en consultar a un experto (consulte el anexo II).

Si se cuenta con el personal capacitado para esta tarea, el costo-beneficio subiría dado que el personal entendería las especificaciones del diseño y uso del firewall, sin embargo puede ser costoso desde el punto de vista de construir y documentar el firewall, donde requiere un mantenimiento y añadirle características (como la autentificación); pero por desgracia la mayoría de las veces no son considerados estos costos, algunas organizaciones se equivocan al tomar en cuenta sólo el costo del equipo. En estos casos es mejor comprarlo.

Para decidir esto, las siguientes preguntas pueden ayudar a la organización si tiene los recursos para construir y operar un firewall:

- ¿Cómo se intentaría probar el firewall?, ¿Cómo se desea verificar que el firewall desempeña lo que se espera?.
- ¿Cómo se intentaría desempeñar el mantenimiento general del firewall - respaldos y reparaciones – ?.
- ¿Cómo se intentaría actualizar el firewall, para nuevos servicios proxy, nuevos parches u otras mejoras?.
- ¿Pueden los parches de seguridad y problemas ser corregidos en un tiempo razonable?.
- ¿Quién intentaría desempeñar el soporte a usuarios y/o entrenarlos?.

Algunos vendedores ofrecen servicios de mantenimiento con la instalación del firewall, la organización consideraría si tiene los recursos internos para desempeñarlos. En el capítulo V se expondrán características que deben ser tomadas en cuenta para escoger un firewall y el cómo adquirirlo.

3.5 Pruebas del firewall[23].

Esta es una parte importante en el buen funcionamiento de un sistema, ya que es una parte del mantenimiento del firewall; el hecho de confiar de cierta manera en una configuración que no fue validada o en donde fue validada solamente en la instalación es un riesgo muy importante; dado que cualquier cambio rápido de la configuración del firewall para dar el debido soporte a un proyecto especial o a modificaciones de autentificación puede tener efectos negativos en la seguridad de toda la configuración.

3.5.1 Pruebas de caja negra.

Este tipo de pruebas consta de dos partes:

3.5.1.1 El escaneo de puertos.

En donde se trabaja con todos los puertos posibles de conexión de servicios del TCP/IP en donde se conecte un host o un dispositivo, puede usarse por los hackers y los administradores del sistema, dado que se les muestra que tipos de ataques y servicios autentificados pueden estar disponibles en el host elegido.

Esto se hace por medio de software standalone de escaneo, esta disponible para varias plataformas, este software se añade en las herramientas de pruebas automáticas. El escaneo es importante debido a que ofrece un registro de donde se indica los resultados de este y se asegura cuales están autorizados bajo la política actual de la organización. El tipo de software a utilizarse va a depender del sistema operativo con que se cuente, a los servicios que tenga y que estén habilitados. Hay de diversos tipos:

3.5.1.2 Escaneo baseline.

Se ejecuta en cualquier configuración antes de conectarse a Internet, se hace un escaneo del firewall y de cualquier red que este conectada a esta, buscando cualquier indicio de cambio.

3.5.1.3 Escaneo en lugares múltiples.

Puede desempeñar al menos las siguientes funciones:

•Ubicar a usuarios en la red protegida.
•El DMZ, que es la red externa del firewall, algunos autores lo llaman el perímetro de defensa.
•Un sitio externo (en una cuenta de proveedor de Internet).

Para hacer esto se hacen las siguientes recomendaciones:

•Hay que revisar los intentos de todos los puertos desde el 0 al 65535, haciendo énfasis en el puerto 10000 debido a que es una sección del perímetro que no tiene monitoreo continuo.

•Hay que escanear todo, es decir que los servicios que se ofrecen dentro de la red son registrados de manera entendible.

•Revisión de la salida, los scripts de las pruebas de escaneo ahorran tiempo de ejecución, en el sentido de que se automatiza la función.

•Eliminar todas las herramientas que puedan usar los posibles atacantes, se deben generar reportes periódicos, las técnicas de las herramientas de protección pueden ser desde asignar permisos de sólo lectura a los archivos hasta remover partes del sistema operativo que no son necesarias.

•Se debe de guardan todos estos registros en un lugar seguro.

En este tipo de pruebas se recomienda utilizar el software SATAN y el portscan (que se encuentran disponibles en Internet).

3.5.2 Observación "on-the-wire".

En algunos sistemas operativos de red, se despliega información en el monitor de lo que esta pasando en el monitoreo de la red, esto es conocido como un sniffer, que es una herramienta que puede ser usada por cualquier persona para diversos propósitos.

Este software esta a disposición en distintos sistemas operativos como Solaris (snoop), pero hay una herramienta freeware conocida como tcpdump, se cuenta con el código fuente para poder adaptarlo a diferentes sistemas operativos UNIX. Las herramientas de bajo costo se aplican en las redes Ethernet que no están conectadas. Si la configuración que esta bajo prueba utiliza medios poco comunes, el monitoreo descrito puede requerir hardware especializado.

En esta parte pueden existir varios tipos de observación especializada:

3.5.2.1 Observación "Quiet Wire".

Hay que familiarizarse con la firma de la red, además de los puertos en los cuales esta activa (o sea que esta lista para responder a los requerimientos), los servicios que contengan información de la red puede ser un error que no afecte mucho, dependiendo de la configuración y puntos de conexión del host, ruteador y del firewall, donde pueden ser visibles los tipos de tráfico.

Si se desconecta el DMZ del ruteador externo, y los clientes no tienen tráfico inicial, el monitoreo de la red puede captar poco tráfico, de esta manera se puede conocer que tipo de tráfico o de las sesiones que son requeridas por los usuarios y que dispositivos originan estos requerimientos.

3.5.2.2 Pruebas de control.

Es útil para observar las trazas que deja una conexión que es originada desde un cliente interno que el firewall permite salir a una conexión externa donde la dirección de origen puede variar dependiendo del tipo de implementación del firewall, algunos productos causan que todas las sesiones aparezcan como si fueran originadas desde la dirección del firewall. Los productos que implementan el NAT (Network Address Translation) no permiten a los clientes ver las direcciones IP verdaderas en el DMZ.

Se produce la visualización del tráfico al observar el comportamiento de las conexiones que llegan, para ofrecer servicios o no desde el firewall.

3.5.2.3 Observaciones "Live Wire".

En una red activa, un monitoreo de red abierto compacta rápidamente información vieja; la vigilancia de todos los movimientos es limitada, con algunas excepciones; en algunos eventos que puede perjudicar al nivel del ISP o del backbone, es capaz de "ver" la dirección y el tipo de tráfico que pasa a través del firewall. Es una ventaja tener un software de monitoreo de red para observar, codificar y si es posible grabar este tráfico que indique eventos en donde el sistema de alerta o de identificación del firewall se activen.

3.5.3 Verificación de los sistemas de identificación.

Es muy importante que las personas que se van a encargar de administrar el firewall se familiaricen con los mensajes de los sistemas de alerta y de identificación, la configuración de estos sistemas es de gran apoyo para reducir la cantidad de mensajes que tiene que revisar el administrador, es importante verificar la clase de los eventos identificados por el sistema y el formato en el que deberán aparecer. Para identificar todo esto, se tiene que revisar lo siguiente:

A) Identificación sobre los proxies del FTP y del telnet.

Hay que hacer pruebas de identificación sobre los proxies del FTP y del telnet (si están disponibles) varias veces y con usuarios que no existan. Checar que los eventos están identificados como intentos fallidos y cada intento es identificado de manera separada, de esta manera se podrá visualizar si se ha tenido intentos de adivinar los passwords. Además, se tienen que realizar las pruebas al DMZ o perímetro de defensa desde un sitio remoto y desde la red interna. En los sistemas que no cuentan con el NAT pueden intentar la prueba hacia la dirección IP del firewall localizado en la red protegida.

B) Pruebas de protocolos que no tienen soporte.

Los intentos de usar un protocolo que no tiene soporte en la política de seguridad como el rlogin o el TFTP, la mayoría de los sistemas rechazan los intentos sin identificación. Se tiene que hacer esta prueba en el DMZ desde un sitio remoto y desde la red interna.

C) Prueba de la autentificación de tokens.

Es importante probar que ocurre cuando un ciclo de respuesta/reto invalido se usa en una cuenta de usuario.

D) Prueba de correo.

En las configuraciones con que se cuenten con proxies SMTP podría producir algún tipo de identificación:

telnet protegido.acatlan.unam.mx 25
200 <mensaje de bienvenida>
HELO hacker.net
220 <Mensaje de bienvenida, con el IP verdadero o la lista del nombre del host>
WIZ
500 <unknown command, possibly an insulting message>
DEBUG
500 <unknown command, likely a further insulting message>
QUIT

Esto es una muestra de un intento de engañar a una dirección de correo electrónico así como el uso de dos "bugs" del software SMTP que utiliza el sendmail.

E) Prueba con herramientas automatizadas.

Las herramientas automatizadas para las pruebas son muy útiles para verificar la capacidad del firewall al máximo, si se cuenta con alguna de estas, se debe de revisar las identificaciones que haga el firewall.

3.5.4 Prueba de la configuración.

En esta parte se tiene por objetivo el validar que los componentes de la configuración fueron los correctos así como la instalación del firewall, es común la mala ordenación de los sistemas en la configuración del MIS son de alto riesgo; hay que tener muy presente el riesgo de las direcciones confiables localizadas en el perímetro de la red debido a que este se puede incrementar por medio de ataques de alteración de dirección y ampliar la zona de exposición a cualquier servicio o host sobre el perímetro de la red que pueda comprometerse.

A) SOCKS.

En las configuraciones del firewall en donde se pueda usar SOCKS, se cuenta con una protección contra la alteración de direcciones y se puede usar como un cliente que pase a través del firewall. Al usar los clientes del SOCKS (como el telnet o el FTP) desde una red externa, se hay que configurar el parámetro del host para apuntar a la dirección IP externa del firewall, así como los intentos por accesar a una dirección IP dentro del firewall usando el cliente. La referencia de esta IP es mucho más confiable si se usa el nombre completo del dominio. Los intentos de la misma prueba especifican la dirección IP de la interface del firewall sobre la red protegida así como el host del SOCKS. Esta prueba se tiene que hacer en el perímetro de la red.

B) Proxies HTTP.

Se debe de configurar el browser para que pueda utilizar el proxy del firewall que se haya instalado. Los intentos de acceso al servidor Web dentro de la red interna así como los intentos de acceso fuera de la red protegida. La prueba indica la dirección del firewall sobre la red protegida, se debe de hacer la prueba desde el perímetro de defensa (DMZ).

C) DNS

Hay varios esquemas que soportan el DNS con algunos grados de complejidad, una prueba completa del DNS es altamente específica. Hay que asegurarse que los FQDN (Fully-Qualified-Domain Names) serán resueltos desde la red interna. Esto es la característica de telnet hacia un sitio externo por medio de la dirección IP, pero no indica al DNS un problema de configuración.

D) Servicios de usuario.

Hay que probar todo el software que utilicen los usuarios para el acceso externo de los servicios, es una validación acerca de cuáles servicios pasan por el firewall al exterior (y que los usuarios sean capaces de usar con los resultados esperados). Es de mucha ayuda para la validación revisar que los servicios provistos (o negados) a los requerimientos de cualquier acto (o falla) de alguna host externo, de acuerdo con la política de seguridad vigente en la organización.

3.5.5 Validaciones de terceros.

Hay servicios de seguridad que son ofrecidos por consultores y empresas especializadas, esto puede valorar la implementación de la política de seguridad, y de esta manera es utilizado con más confiabilidad para los clientes, administradores o accionistas. Estas opciones pueden ser:

3.5.5.1 Validaciones periódicas.

Esto puede ayudar a que cualquier ejecución uniforme y se descubren los cambios que no se tenían detectados.

3.5.5.2 Validaciones aleatorias.

Este tipo de pruebas es diseñado si se tiene el staff de seguridad dedicado a estas tareas y se puede incorporar en auditorías generales de la compañía. Se intenta con esto ver que pasa cuando se ataca sin anuncios.

3.5.5.3 Espionaje/ingeniería social.

Hasta el mejor equipo de los administradores de la red y el staff del MIS a menudo pueden tener errores debido a malas prácticas profesionales y la tendencia humana para subestimar las intenciones de otras personas. Estas pruebas deben considerarse si se tienen dudas acerca de cualquier persona o sospechas de cualquier competidor que esta desarrollando una tendencia al espionaje; sin embargo, hay que tener cuidado y la preparación debida para evitar daños morales y demandas por hostigamiento (en el caso de los E.U.).

3.5.5.4 Pruebas configurables.

En algunos casos se pueden tener necesidades especiales que requieren diseñar escenarios de prueba, en estos casos se debe seleccionar una compañía que demuestre que tenga un buen entendimiento del giro de la organización y las posibles amenazas; y no sólo de habilidades técnicas para proyectar la prueba.

Para una mejor compresión del tipo de pruebas que se pueden realizar con algunos comandos y aplicaciones que se pueden encontrar en el sistema o Internet revisar el contenido de la fig. 24.

Comando	Descripción	Evento esperado
ping	Envía paquetes al host, mostrando un mensaje si es exitoso o fallido.	Al menos debe mostrar la ejecución del comando y su origen en las bitácoras del sistema.
traceroute <host>	Muestra la ruta que sigue un determinado número de paquetes al "host" especificado.	Al menos debe mostar la ejecución del comando y su origen en las bitácoras del sistema.
netscan [-u] dominio	Envía paquetes a las estaciones de trabajo que conforman el dominio, mostrando su status (activas).	Muestra el status de las estaciones de trabajo que conforman el dominio especificado, además de registrar estos eventos en las bitácoras del firewall.
portscan <host>	Envía un número determinadp de paquetes a todos los puertos que conforman el host determinado - es recomendable especificar el host bastión -.	Debe mostrar el acceso a los puertos en las bitácoras del firewall.
telnet <host>	Efectúa una sesión remota en el "host interno"	Debe indicar un mensaje en las bitácoras del firewall (o en la consola del mismo) y señalar un mensaje de error a los usuarios que se conecten de algún host no autorizado.
ftp <host>	Efectúa transferencia de archivos entre el host local y el host remoto.	La ejecución de los subcomandos dependerá del tipo de política de seguridad con que se cuente; por ejemplo, si el sitio permite la ejecución del put desde el exterior. Además de mostrar un mensaje a cualquier acceso no autorizado.

Fig. 24. Ejemplos de pruebas para comprobar el funcionamiento de un firewall.

Capítulo IV

Ventajas y desventajas frente a otras opciones

Para asegurar el éxito de la implementación de cualquier sistema, es muy importante visualizar los factores críticos de éxito del mismo, con el objeto de tomar la mejor decisión en la elección de un tipo de firewall en especial.

Algunas aplicaciones adicionales pueden servir como un buen complemento para reforzar la seguridad del sitio (como la encriptaciòn o el "multilayer switches"), por razones que se explican en el presente capítulo.

4.1 Protección contra los servicios vulnerables.

Un firewall puede incrementar la seguridad de la red y reducir los riesgos del servidor en la subred filtrando los servicios inseguros. Como resultado, el ambiente de la red esta expuesto a algunos riesgos, dado que algunos protocolos seleccionados pueden pasar a través del firewall.

Por ejemplo, se puede prohibir los servicios vulnerables como el NFS para entrar o salir de la red protegida; esto previene que los servicios sean explotados por gente extraña a la organización, pero al mismo tiempo permite el uso de estos. Los servicios como el NIS y el NFS particularmente son usados en una red de área local para reducir la administración de la red (o redes) del sitio.

El firewall ofrece protección contra ataques de ruteo (routing-based) - la fuente de ruteo - e intentar redirigir las direcciones de ruteo al sitio comprometido por medio de una redirección ICMP. Se puede además negar todos los paquetes de origen y las redirecciones ICMP e informar a los administradores de los incidentes.

4.2 Control de acceso a los sistemas del "sitio".

Ofrece la cualidad para controlar el acceso al sistema del sitio. Por ejemplo, algunos servidores son buscados desde redes externas, considerando que pueden ser efectivamente sellados a partir de un acceso restringido. El sitio puede prevenir los accesos externos al servidor a excepción de casos especiales como servidores de correo electrónico o servidores de información (Web).

Esto lleva a una política de acceso en que son particularmente especiales los firewalls: negando el acceso al servidor o a los servicios que no requieren su ejecución; de otra manera, ¿quién ofrece acceso al host y a los servicios que pueden ser explotados por atacantes cuando el acceso no es usado o no es requerido?. Si por ejemplo, un usuario requiere o no el acceso al escritorio (desktop) de la estación de trabajo.

4.3 Concentración de la seguridad.

Actualmente un firewall es menos costoso en una organización en donde todo o la mayoría del software modificado y software de seguridad adicional puede utilizarse en los sistemas del firewall como soporte para empezar a distribuirse en varios hosts. Particularmente, los sistemas de password (one-time) y algún software de autentificación puede ser localizado en el firewall si tiene soporte de cada sistema que necesita ser accesado desde Internet.

Otras soluciones a la seguridad de la red, (como Kerberos) implica modificaciones en cada sistema de los hosts a protegerse. Mientras estas aplicaciones son consideradas por sus ventajas y puedan ser apropiadas para el firewall en situaciones precisas, tienden a ser simples los firewalls en su implementación, en donde solamente se necesita ejecutar software especializado.

4.4 Mejoras en la privacidad.

La privacidad es muy importante en un sitio (site) seguro, considerando que el poder de la información (innocuous) actualmente contiene guías que pueden ser usadas por un atacante (hacker); usando un firewall, algunos sitios bloquean servicios como el finger y el DNS (Domain Name Service), el comando finger despliega información de los usuarios - sección 1.15.5 del capítulo 1 -, pero puede fugarse información por parte de un atacante (hacker) acerca de cómo el sistema es usado, el sistema tiene usuarios activos conectados y el sistema puede ser atacado sin ser detectado.

Puede bloquearse la información del DNS relacionada con los sistemas del sitio, entonces los nombres y las direcciones IP de los sistemas del sitio no están disponibles en los hosts de Internet. Algunos sitios bloquean esta información, ocultando la que pueda ser usada por hackers.

4.5 Accesos y estadísticas acerca del uso de la red.

Si todos los accesos hacia y desde Internet pasan a través de un firewall, se pueden registrar y ofrecer estadísticas acerca del uso de la red. Un firewall con las alarmas apropiadas se activará cuando ocurran incidentes sospechosos que puedan aportar detalles sobre si el firewall o la red están siendo probados o atacados.

Es importante almacenar las estadísticas de uso de los distintos servicios que estén protegidos (proxy) y la evidencia de pruebas por varias razones:

- Primero es conocer si el firewall es objeto de pruebas o de ataques determinando si los controles del firewall son adecuados.
- Las estadísticas de uso de red son también importantes y pueden utilizarse como entradas en los estudios de requerimientos de la red y en el análisis de riesgos.

4.6 Reforzamiento de políticas.

El firewall ofrece los medios para implementar y reforzar la política de acceso a la red, dado que puede controlar el acceso a los servicios y a los usuarios. Sin el firewall, se necesitaría de la cooperación de los usuarios de la red.

4.7 Acceso restringido a servicios deseados.

La desventaja de un firewall es que se pueden bloquear servicios que los usuarios buscan, como el telnet, ftp, X Window, NFS, etcétera. Sin embargo, el acceso a la red puede restringirse por niveles, dependiendo de la política de seguridad del sitio; una política de seguridad bien planeada que concilie los requerimientos de seguridad con las necesidades del usuario puede ayudar a disminuir los problemas como el hecho de restringir el acceso a los servicios como el http (Web).

Algunos sitios pueden tener una topología que no necesite un firewall o puede usar servicios como el NFS en donde se requiera una mayor reestructuración del uso de la red; por ejemplo, un sitio que dependa del uso del NFS y NIS a través de grandes gateways. En esta situación, los costos relativos de añadir un firewall se necesitan compararse en contra de los costos asociados a la vulnerabilidad sin el firewall, como un análisis de riesgos, y la decisión tomada del análisis. Otras soluciones como el Kerberos puede ser adecuadas, pero puede acarrear desventajas.

4.8 Potencial de puertas traseras "abiertas".

No se puede proteger de puertas "traseras", si un modem con acceso sin restricciones esta instalado en una red protegida, los atacantes pueden colarse fácilmente a la red. Los modems de alta velocidad son más rápidos en hacer ejecuciones SLIP (Serial Line IP) y PPP (Point-to-Point Protocol), las conexiones de este tipo son importantes para la conexión con otra red y una potencial puerta trasera si su implementación no esta planificada debidamente.

4.9 Protección limitada contra atacantes internos.

El firewall esta diseñado para prevenir que personas externas obtengan datos importantes de la red, por tanto no es posible prevenir que algún usuario, por ejemplo haga una copia de un software con licencia, y la extraiga de la organización. Y es aquí en donde la política de seguridad interna entraría en acción.

4.10 MBONE (Multicast IP transmissions).

Transmisiones Multicast de vídeo y voz son encapsuladas en otro tipo de paquetes, generalmente se adelantan los paquetes sin examinar su contenido; este tipo de transmisiones representan una amenaza potencial si los paquetes contienen comandos que alteren los controles de seguridad y permitan el acceso a intrusos.

4.11 Virus.

No protegen en contra de virus que se encuentran en archivos de Internet o transferidos con programas añadidos en e-mail, debido a que estos programas pueden estar codificados o comprimidos de cualquier forma; un firewall no puede escanear programas para buscar firmas de virus sin ningún grado de exactitud. El problema del virus puede existir y es necesaria una política independiente al respecto. Sin embargo, nuevas tecnologías de firewall ofrecen esta opción (las cuales se mencionaron en la sección 3.1.6).

4.12 Cuello de botella.

El firewall representa un cuello de botella, todas las conexiones pasan a través de este, y en algunos casos examinados, pero pueden pasar los datos en niveles de T1 (1.5 megabits por segundo) y muchos sitios en Internet tienen esa velocidad o menos.

4.13 Centralización.

Concentra la seguridad en un solo lugar y es opuesto a distribuirse a través del sistema. Un firewall comprometido puede ser riesgoso para sistemas menos protegidos en la subred.

4.14 Gateways proxy Vs filtrado de paquetes.

El gateway proxy y el filtrado de paquetes tienen ciertas cualidades que valen la pena mencionar juntas (fig. 25) ya que son propiedades fundamentales que son retomadas en los nuevos firewalls.

Evento	Gateway proxy	Filtrado de paquetes	Otras consideraciones
Revisión del tráfico TCP	Se aplican reglas a la sesión TCP monitoreando los flujos de datos para determinar si cada comando con una sesión es permitido o es rechazado.	Se aplican las reglas a cada filtrado de paquetes, basándose en el puerto de origen y de destino, así como la dirección de donde provino y a donde va a dirigirse.	Los gateway proxy son más seguros y eficientes para el tráfico TCP.
Revisión del tráfico UDP	Los proxies genéricos permiten el tráfico UDP para ser controlados entre ambos puertos asegurados . No se puede manipular las variaciones del puerto.	Mantiene el estado de las comunicaciones del tipo UDP, reservando un canal abierto entre el remitente y el receptor manipulando el tráfico RPC	El protocolo UDP es menos seguro que el TCP, además de que los firewalls no ofrecen protección para UDP.
Flexibilidad	La fortaleza y la debilidad de un firewall es precisamente la falta de esta característica. Existe un proxy para cada protocolo o se usa un proxy genérico para otros protocolos o no pueden pasar estos.	Son muy flexibles, pero necesitan un "lugar" para configurar el MIS (Managament Information System)	El gateway proxy es mejor para dar el debido soporte a todos los protocolos que están pasando.
Facilidad de configuración	Necesita algunos cambios, pero generalmente es más fácil para configurar.	Son necesarios varios cambios.	Es indispensable tener experiencia para configurar el filtrado de paquetes; por ejemplo, ambos tipos de firewalls pueden ocultar las direcciones, pero el gateway proxy lo trae implementado por default, mientras que el filtrado de paquetes necesita configurarse esta opción.
Facilidad de administración	Es muy fácil de administrar, ya que cuenta con medios muy accesibles.	Se mantiene el paso de los protocolos y las reglas se implementan al mínimo para poder implementar la administración.	Ambos requieren conocimientos, experiencia y capacitación para poder administrarlo correctamente.
Otras cualidades...	Son libres para ocultar las direcciones, buenos para identificar y ofrecen avisos de alertas en potencia.	Se ocultan las direcciones por medio de opciones de configuración, identificación razonable y buenas señales de alerta.	

Fig. 25. Gateways proxy Vs filtrado de paquetes.

4.15 Redes privadas virtuales[30].

Con la implementación de las nuevas tecnologías de firewall se pueden implementar Redes Privadas Virtuales (VPN Virtual Private Networking), estos pueden usar varios grados de encriptación (que puede ser de código de 40 bit RC4 a triple DES -encriptación de 56 bits aplicada tres veces -). La desventaja de administrar estos VPN es que son necesarios túneles, y se necesita una llave de admón. que necesitan conocer los extremos del túnel para codificar los datos mientras los envían. Esta llave puede intercambiarse de manera segura, pero el reto es intercambiar esta llave sin tener una clave secreta.

Varios firewalls que implementan los túneles VPN necesitan una llave secreta para accesar manualmente en todos los extremos de la comunicación. Están llaves deben asegurarse para que la comunicación pueda empezar, es recomendable cambiar estas llaves para prevenir algún accidente y las nuevas llaves necesitan accesarse físicamente desde sistemas remotos.

Debido al estado actual de la industria, cada compañía establece su propio protocolo VPN, para esto algunos fabricantes decidieron implementar el IPSEC, para resolver el problema de que

todos los datos son encriptados entre los extremos del VPN; es decir, todos los datos de la capa IP (incluyendo protocolos TCP como el Telnet, el FTP y el SMTP) son encriptados en este túnel, por esto algunas compañías son capaces de establecer canales de datos encriptados, permitiendo usar el Internet, pero después de haber pasado por las reglas.

Algunos proxy gateway ofrecen el filtrado de paquetes de los túneles VPN, de esta forma se pueden especificar protocolos para permitir o negar su ejecución, así como la dirección de inicio. Las direcciones de origen y de destino pueden especificarse y usar un método de autentificación, esta combinación añade control al VPN y hace posible tener al túnel VPN y mantener asegurado el perímetro exterior.

Un túnel VPN nulo añade flexibilidad al firewall al procesar los UDP, debido a que el túnel trabaja en la capa baja de red , pueden pasar el UDP al crear al túnel con el firewall el UDP puede pasar y ser filtrado, y de esta manera protocolos como el ping pueden pasar desde y hacia algún hosts específico como si estuviese diseñado por el administrador del firewall. Aunque algunas otras características son incluidas:

- Análisis estadístico y gráfico de los patrones del tráfico de datos del firewall.
- Bloqueo sofisticado de sitios de Web no deseados.
- Filtrado de tipo MIME que es capaz de bloquear la transferencia de applets de Java.
- Software para escanear virus en los correos electrónicos para evaluar, bloquear o prevenir archivos binarios y correos electrónicos que contengan virus.

Escoger el firewall puede ser una tarea complicada, hay que empezar evaluando el tráfico que pasa a través del firewall y en la dirección en la que puede pasar; además de determinar si el firewall puede incrementar la seguridad global. Puede ser que no; todos estos aspectos necesitan cuidarse, hay que recordar que la instalación de un firewall no es lo único que hay que hacer para asegurar la red, es indispensable tener una política de seguridad y reforzarla por medio de pruebas y de otras aplicaciones que son complementarias. Hay compañías que ofrecen pruebas completas de acceso (SIAC, Science Applications International Corporation). Hay herramientas comerciales como el ISS; o el NetCat, que es de dominio público, aunque no es fuerte la aplicación si es muy útil para ir revisando los defectos de seguridad que tenga la red.

Pero hay cosas que no puede hacer el firewall, se deben de contar con las herramientas necesarias para no tener problemas al respecto, no se trata de generalizar el uso de estas, pero si mencionarlas como una alternativa para los sistemas UNIX, dada su aceptación en varias organizaciones y grupos de seguridad, aparte de que son software de tipo freeware y se cuenta con el código fuente para poder adaptarlo a las características propias del sistema. Y estas son:

4.16 Firewalls y el monitoreo del host.

La herramienta tripwire lo que hace es revisar las modificaciones que se le hagan a los archivos enlistados en una base de datos y muestras el estado de las modificaciones que se le hayan hecho, tiene las siguientes cualidades que son mostradas en la figura 26.

Es portable a varias plataformas de UNIX, las bases de datos que genera pueden ser leídas por cualquier editor de textos.

✓ Configuración y flexibilidad.

El software hace una distinción entre el archivo de configuración y la base de datos, es decir, las estaciones de trabajo pueden compartir el mismo archivo de configuración pero se generen bases de datos para cada una debido a que cada base se le revisa su integridad.

El archivo de configuración (tw.config) contiene una lista de opciones en donde se encuentran los archivos y directorios que van a ser revisados.

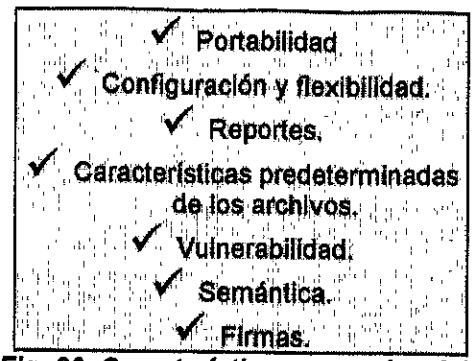


Fig. 26. Características generales del Tripwire.

Por default, se incluyen todos los directorios cuando la base de datos se genera, cada archivo es grabado en la base de datos con la misma bandera y firmas del directorio específico, de este modo se pueden hacer configuraciones más compactas e inclusive poder agrupar a los archivos de configuración del sistema.

✓ Reportes.

Se basan de la lista de archivos y directorios que se encuentren en el archivo tw.config en donde se puede especificar si van o no ser examinados (+ y - respectivamente).

Se hace un reporte con las siguientes salidas:

Cambios en los permisos y en los modos
Número de inodes.
Número de enlaces.
Dueño.
Grupo.
Tamaño del archivo.
Tiempo de modificación.
Firma 1 y 2.

Se pueden clasificar los archivos basándose en "características" predeterminadas del software, las cuales son mostradas en la figura 27.

Opción.	Descripción.
read-only files	El tiempo de acceso es ignorado.
log-files	Son ignorados los cambios al tamaño del archivo, tiempo de acceso y manipulación
Growing log files	En donde se ignoran los cambios de tiempo de acceso y modificación.
Ignore everything	Ignorar todo.
Ignore nothing.	No ignorar nada.

Fig. 27. Características predeterminadas del software Tripwire.

✓ Vulnerabilidad.

Por desgracia, si se llega a tener el acceso, el archivo de configuración y la base de datos pueden ser alteradas.

✓ Semántica.

Los cambios en la base de datos pueden ser categorizados en seis casos, cada uno de los cuales tiene acciones a tomar.

La actualización o el borrado de un archivo de la base de datos es integro. En donde se actualiza el archivo o directorio en cuestión, para esto se "cierra" el registro anterior.

Adicionar, borrar o actualizar las entradas es fácil, debido a las propiedades que presenta cualquier base de datos, la actualización se hace copiando el archivo. En caso de que el sistema falle, se puede reemplazar por la base de datos anterior.

✓ Firmas.

Con el tripwire se genera una herramienta que genera firmas para los archivos especificándose en la línea de comando, es conocida como siguen, esta se pude modificar para adicionar rutinas de firmas, incluyendo métodos cortos de criptografía y métodos hash, aceptando un total de 10 funciones.

4.17 Firewall y la autentificación[13].

Hay diversos mecanismos de autentificación que vienen incluidos en cualquier firewall y son los passwords convencionales, tarjetas inteligentes (smartcards) de reto-respuesta y servicios S/Key.

Las autentificaciones del tipo smartcard lo que hacen es regresar una respuesta única basada en un reto (un número aleatorio) generado por el firewall. El usuario ingresa el reto en un token el cual va a calcular la respuesta apropiada. Hay varias implementaciones de este tipo, las más populares son el SecurID de Security Dynamic que usa el tiempo actual como el reto para que el usuario no lo tenga que hacer.

El S/Key es una alternativa interesante - es desarrollado por Bellcore -, ya que el password utilizado es diferente en cada sesión que tenga el usuario.

4.18 Firewalls y la encriptación.

Por razones ya vistas en el capítulo II y III, la encriptación se emplea para establecer canales encriptados de las sesiones de red desde un host remoto al firewall, esta medio es requerido en la Intranet de alguna organización.

Una herramienta que es considerada por muchos como una de las mejores en cuanto al encriptamiento es el PGP (Pretty Good Privacy), es desarrollada por Phil Zimmerman, este programa utiliza los algoritmos de RSA e IDEA para el encriptado de datos y la revisión de su integridad. Tiene dos funciones primarias; se puede encriptar un archivo que no puede ser leído por ninguna persona a excepción del destinatario y puede verificar que un mensaje o archivo recibido de cualquier persona es en realidad el remitente del mensaje, el algoritmo RSA se generan dos llaves, la cuál puede estar en la cuenta personal (privada) o estar en varios lugares en el Internet (la pública), esta llave es un archivo con la extensión ASC.

El algoritmo RSA fue desarrollado por Ron Rivest, Adi Shamir y Len Adleman, investigadores del MIT.

El algoritmo IDEA fue desarrollado por Xuejia Lai y James Massey en el ETH en Zurich, este algoritmo es la llave del número simétrico usada con RSA en el PGP, no se conocen ataques de fuerza bruta que lo hayan afectado hasta la fecha y tiene un buen tamaño la llave resultante.

Kerberos es un protocolo de autentificación del nivel a aplicación desarrollado por el MIT (Massachusetts Institute of Technology), se usa un servidor de seguridad para generar llaves para que una aplicación cliente pueda tomarlo del host para autentificar a un usuario, el cual es encriptado. Debido a que Kerberos es un protocolo del nivel de aplicación, necesita aplicaciones de cliente y de servidor modificados para soportarlo, debido a esto no es muy utilizado.

4.19 Firewall y NFS.

Desgraciadamente este es un servicio que no protege el firewall (freeware), además de ser una potencial puerta de acceso en donde se puede accesar con privilegios de root - si se tiene mal configurado -, para esto Wleste Venema desarrolló una versión mejorada del rpcbind[25], en donde se tienen las siguientes características:

- ✓ Control de acceso al host por medio de la dirección IP, el host local se considera por default con autorización, este software requiere de una librería que es generada por la compilación del paquete TCP Wrapper.

- ✓ Los requerimientos que se adelantan por el proceso rpcbind son adelantados a un puerto sin privilegios.

- ✓ Se tiene la capacidad de negar todos los requerimientos de los demonios rpc que verifican el origen del requerimiento, se incluyen en la mayoría de los llamados a los demonios mountd/nfsd y a los demonios de NIS.

- ✓ No protege contra ataques directos sobre los demonios rpc debido a que la tarea principal del rpcbind es mantener una tabla de los servicios RPC disponibles y los puertos de la red que pueden percibir algo, pero dificulta un ataque usando los demonios RPC.

- ✓ Ya compilado se puede hacer uso de dos archivos /etc/hosts.allow y /etc/hosts.deny en donde se va a colocar cuales servidores tienen derecho a conectarse y cuales no respectivamente.

Se hace de la siguiente manera, estos archivos se pueden encontrar en el subdirectorio /etc del sistema a proteger:

hosts.allow

rpcbind: 123.456.78.

Esta configuración va a permitir solamente accesar a cualquier máquina que se encuentre en el dominio 123.456.78.

hosts.deny

rpcbind: ALL: (/ruta/safe_finger -l %h | /bin/mail root)&

En este ejemplo se va a negar la conexión al host que no corresponda al dominio 123.456.78, pero se va a enviar un correo al usuario root en donde contendrá la dirección del host remoto y los usuarios en sesión que en ese momento estaban en el momento que ocurre el incidente. La opción *ruta* indica el subdirectorio en donde se almaceno el binario *safe_finger*.

Para cualquier obtención y evaluación de estas herramientas de seguridad y algunas otras, se recomienda ampliamente los sitios especificados en el anexo II.

4.20 Multilayer switches[45].

Hoy en día, las transmisiones en Internet se van haciendo más complejas, esta características repercute sensiblemente en la velocidad de cualquier esquema de seguridad implantado en la red de cualquier organización o sitio.

Para atacar este problema, se estan desarrollando nuevo hardware que permita agilizar las comunicaciones, además de ofrecer características que tiene un firewall.

Con un switch multicapas (multilayer switch) es posible administrar y controlar la capa de transporte, de sesión, de presentación y de administración (referentes al modelo OSI), se tiene:

- ✓ Los puertos del switch pueden compartir una misma dirección IP.
- ✓ Se equilibran las comunicaciones de red.
- ✓ Redundancia en los servidores, done los datos llegan
- ✓ eficientemente a su destino.
- ✓ Hay seguridad.
- ✓ Se cuenta con políticas de servicio de calidad (si se cuenta con ATM o Gigabit Ethernet).

Este hardware permite establecer dos tipos de políticas:

1) De seguridad.

El switch va a ser capaz de revisar cualquier tipo de información que se transmita en los encabezados de paquetes. Con ayuda de este hardware especializado, se tiene una alta velocidad en el filtrado de paquetes. Examina cada paquete, basándose en un conjunto de reglas que establezcan los administradores, de acuerdo a las necesidades de la red (ya se que adelante, bloquee, bloquee y genere un reporte de los eventos) en base a una política de seguridad ya establecida.

En las políticas de seguridad se puede especificar:

a) Direcciones IP.
b) Redes/ subredes.
c) Tipos de aplicación (estándar -TCP, UDP- o de usuario - aplicaciones en Visual Basic que lean el contenido de una base de datos en un servidor central).
d) Estas políticas son asimétricas.

2) Servicio de calidad.

Es posibler asignar prioridades a varias cadenas de datos para reforzar las políticas de seguridad, considerando que se tenga ATM o Gigabit Ethernet:

- ✓ La prioridad que se asigne a aplicaciones predefinidas (http, ftp, telnet, smtp).
- ✓ La prioridad que se asigne a usuarios específicos (root, sysadmin).
- ✓ La prioridad que se le asigne a aplicaciones específicas (telefonía, videoconferencia, fax).
- ✓ La prioridad que se le asigne al número de ocurrencias diarias de un servicio o suceso previamente establecido en la política de seguridad.

El software que suministra la administración en los switch de este tipo puede ser:

Es complejo, por el número de equipos que tenga que administrarles sus datos.

Es más clara la planeación y el análisis del desempeño de la red.

El análisis del tráfico es posible, con ayuda de interfaces GUI se transforman los paquetes que transiten por el switch.

Se puede migrar a otra tecnología (ATM, Fast Ethernet, Gigabit Ethernet), añadir nuevos componentes y efectuar cambios en los segmentos de la red.

Y gracias a lo anterior, la detección y solución de problemas es resuelto en poco tiempo.

Capítulo V

Aplicación

5. Aplicación.

Hasta el momento se ha visto varios temas que son importantes conocer, para poder comprender de manera adecuada el hecho de como y donde funciona un firewall, a continuación se presentará una herramienta disponible en Internet, el TIS Internet Firewall Toolkit (FWTK) que es versión freeware; se mostrará un breve resumen de como funciona, su configuración y su *administración* y *mostraremos* las ventajas y desventajas de cada opción de adquisición de un firewall. Pero antes de elegir, es necesario mencionar algunas características deseables en un firewall:

5.1 Características de un firewall[13].

Para poder elegir algún tipo de firewall es necesario tener en cuenta algunos puntos básicos (fig. 28) que se desglosan más adelante.

Fig. 28. Características de un firewall.

5.1.1 Controles de acceso.

Pueden utilizarse varios métodos en los cuales se va a poder implementar este punto:

5.1.1.1. Listas o reglas de acceso.

Estas son usadas por el firewall de filtrado de paquetes, es fuerte y es muy flexible para controlarse, pueden soportar cualquier servicio debido a que son un número en la lista. A su vez, pueden ser de dos tipos:

- Listas de hosts (host-based list) en donde se describen los servicios que son permitidos por cada host o red.

- Listas de servicios (service-based lists) en donde se identifican los hosts o redes que pueden usar cada servicio.

Las listas de acceso solo soportan políticas de seguridad sencillas, pero son fáciles de entender y configurar.

5.1.1.2 Filtros de sesión.

Filtra los paquetes que contienen la información de cada sesión para habilitarlos y se toman las decisiones más inteligentes y más seguras; pero los firewalls no requieren esto porque operan en un nivel más alto. Algunos ruteadores tienen esta cualidad, pero la mayoría revisa la bandera *ack* del primer paquete TCP y en caso que no la tenga, la rechaza.

5.1.1.3 Controles de alteración de host.

Hay dos características del firewall que pueden reducir este tipo de situaciones;

La restricción del "source route option" que permite al host controlar la ruta que toma al regresar la dirección del host de origen.

Puede controlarse por la interface de red, incluyéndola en la lista de acceso que de alguna manera garantiza que un host externo no sustituya a un host de la red interna.

5.1.2 Servicios soportados.

La parte de soporte de servicios se trato en el capítulo III sección 3.1.3.1.

5.1.3 Autentificación de usuarios.

El capítulo III sección 3.1.2 trata sobre la autentificación de usuarios.

5.1.4 Administración.

Llegando a este punto se tiene que cualquier falla de seguridad puede ser atribuida al administrador del firewall; además puede tener varias características, con una buena administración front-end se reduce esta posibilidad y simplifica la administración.

5.1.4.1 Interface.

Pude ser de modo texto, pero debido a los sistemas operativos gráficos como Windows algunos otros utilizan X Window (X11) como interface de usuario, el despliegue puede ser visto en la consola o de manera remota a través de una red con el protocolo TCP/IP, la mayoría de las plataformas de X Window tienen un administrador de ventanas Motif el cual ofrece un estilo de presentación gráfica más amigable.

5.1.4.2 Administración remota y central.

La administración remota es elegida debido a la dispersión física de la organización o en caso de hacer respaldos que puedan fallar en algún punto, esto permite a la persona encargada administrar de manera "segura", se puede hacer por medio de una conexión encriptada o con ayuda de modems encriptadores.

Con la administración central su conveniencia radica en que puede compartirse una base de datos central que es distribuida a cada firewall de manera segura, es menos laborioso debido a que la configuración es la misma para todos los firewalls.

5.1.4.3 Asistencia en línea.

Por desgracia, pocos administradores conocen el protocolo TCP/IP y otras cuestiones de administración del sistema operativo que se vaya a utilizar, así como del hardware en donde se va a realizar la implementación del firewall; se recomienda ampliamente incluir las siguientes características:

- Configuraciones predeterminadas.
- Checadores de la integridad de los campos. Los campos de entrada son checados para validación y consistencia. Los mensajes de error son provistos al administrador.

• Capacidad de dar alias. Esto permite usar un alias descriptivo par algún valor o valores requeridos. Por ejemplo telnet puede ser alias del puerto 23.

• Grupos. Esto permite agrupar direcciones de host o los números de los puertos, por ejemplo se puede poner al departamento de contabilidad con un nombre de grupo igual, para poder identificar las máquinas de ese departamento.

5.1.4.4 Reportes de configuración.

Aquí se revisa la configuración en busca de inconsistencias y problemas potenciales.

5.1.5 Auditorías y alarmas.

Los registros de auditoria son una herramienta efectiva para evaluar la seguridad provista por el firewall, las características a tomarse son el tipo de eventos a registrarse y las herramientas disponibles para ver y seguir la auditoria.

Se debe de registrar la dirección del host de origen y de destino, el puerto de aplicación, protocolo, tiempo y duración del acceso y la acción tomada; además de ofrecer reportes diarios y a la semana.

Las alarmas permiten al administrador tomar una acción al identificar un evento, esto es conocido como alarmas de tiempo real, son generadas en un periodo corto de tiempo del evento actual, considerando las herramientas para detectar el evento y el tipo de acción disponible (fig. 27); en algunos casos es vinculado la detección del evento con el mecanismo de control de acceso, pero esto limita la efectividad de la alarma y hace el mecanismo de acceso más complejo aunque se puede optar por una alarma separada.

Las acciones a tomar pueden variar dependiendo del firewall, pero las más comunes son enunciadas en la fig. 29.

Fig. 29. Procedimientos al identificar un evento en el firewall.

5.1.6 Integridad del firewall.

Si el firewall es atacado con éxito, la integridad de la red estará gravemente afectada, para disminuir la probabilidad de que ocurra ese hecho se tiene que revisar lo siguiente:

5.1.6.1 Sistema operativo endurecido (confiable).

La mayoría de los firewalls están construidos y/o implementados en alguna variante de UNIX, *pero este sistema operativo tiene la peculiaridad de que tiene mala seguridad por sus* cualidades de un sistema abierto, pero algunos de estos sistemas están acreditados por el gobierno de los E.U. en el estándar de "endurecido", estos sistemas están diseñados con características especiales y pasan diversas pruebas para soportar distintos tipos de ataques.

Afortunadamente se puede agregar esta característica a cualquier sistema operativo, se puede usar una versión quitándole todo lo que no sea necesario para las funciones del firewall. Esto limita las herramientas que el hacker pueda usar para irrumpir en el firewall.

Un tipo especial de este sistema es el sistema operativo "empotrado" y este desempeña un propósito especial y características que pueden ser explotadas por un hacker, este tipo de sistemas son utilizados en los ruteadores ya que el sistema que utilizan soporta el ruteo y características de seguridad.

Otra estrategia es seguir los lineamientos que marca el "libro naranja" –resumido en la sección 2.1-, la NCSC (National Computer Security Center) ha desarrollado este estándar y se trata de dar un nivel de seguridad basándose en ciertas características de seguridad y confiabilidad al hardware y al software respecto al diseño y la prueba del producto, este tema ha sido tratado al principio del capítulo II para mayor referencia de los niveles de seguridad.

5.1.6.2 Firewalls de host dual.

Conocida también como circuit level gateway, es utilizada en caso de que no se cuente con un sistema operativo "endurecido", se aprovechan dos firewalls, y de esta manera el atacante necesitaría irrumpir en los dos para poder accesar a la red. Se establece una ruta privada entre dos hosts en donde se emplea una conexión especial en donde es difícil de accesar al segundo host, en caso de haber penetrado el primero. Otro método para implementarlo es usando un ruteador de filtrado al principio del host que contiene al firewall, este sistema limita el tráfico que es soportado por el firewall y los ataques más comunes no pueden afectarlo.

5.1.6.3 Scanner de integridad.

Es una aplicación que continuamente escanea el firewall en busca de cualquier cambio no autorizado a los archivos o a los dispositivos, es común encontrarlo en los servidores de red. Lo que hace es registrar un informe o secure hash por cada archivo protegido del sistema, indicándolo en caso de que este alterado, basándose en un registro anterior; otros sólo permiten el cambio del archivo sólo si se especifico en una lista.

5.1.6.4 Invisibilidad.

Los firewalls de filtrado de paquetes y de sesión son invisibles al usuario debido a que no están directamente direccionados y los paquetes no pasan por el nivel de aplicación, también existen proxies invisibles que aparecen como ruteadores, pero los paquetes pasan por el nivel de aplicación para ser procesados.

Pero el firewall puede tener una dirección IP y de esta manera es atacado por cualquier hacker, nuevas características del firewall ya no cuentan con dirección IP y pueden trabajar dentro del nivel de la LAN para recibir y transmitir los paquetes, esto disminuye la posibilidad de que el firewall que manipula los paquetes tenga menos probabilidad de falla.

5.1.7 Velocidad.

Por desgracia esto es una característica que no se tiene que dejar de lado, dado que por el WWW tienen que pasar datos con características gráficas, además de que es muy probable que en un futuro cercano tengan que pasar datos de audio y video y esto ocupa espacio de transmisión considerable.

5.2 Lugares de implementación[33].

Pero el firewall puede implementarse de dos maneras, interna y externa; donde la externa va a corresponder a la parte de la red de donde vengan los paquetes de información externos, el origen puede variar así como provenga de Internet o de otra empresa que establezca un túnel con la organización; la interna va a generarse de las circunstancias y necesidades particulares de cada sitio u organización, estas pueden variar, pero se recomienda tener atención a los siguientes casos:

5.2.1 Firewall Internos.

Hay situaciones en las cuales es importante proteger algunas partes (segmentos) internas de la red de otras, por ejemplo:

- Se tienen laboratorios de redes o redes de prueba, en donde puede haber personas ajenas a la organización.
- A lo mejor se tienen redes que son menos seguras que otras que se encuentran en la organización, como redes de enseñanza o de demostración, en donde usuarios externos hacen uso de esos recursos.
- Se tienen redes más seguras en la red interna como una red de proyectos secretos, o redes en donde los datos estratégicos pasan sobre esta (números de tarjeta de crédito, comunicados a los accionistas, etc.).
- En circunstancias donde se tienen dos o más organizaciones que comparten una red, o varias partes de una organización (contabilidad, recursos humanos, etc.), debido a la importancia del departamento.

5.2.2 Laboratorios de redes.

Los laboratorios de redes y las redes de prueba son, en algunas organizaciones, los primeros que se deben de separar del resto de la red interna; si se cuenta con experiencia de manejo de ruteadores, este tipo de firewall puede ser muy sencillo. Se necesitan una red perimetral y un host bastión debido a que no se espera una alteración (dado que los usuarios son internos) y no se necesita ofrecer ningún servicio (dado que no hay ninguna cuenta de usuario). Se podría buscar que un ruteador de filtrado de paquetes que permita cualquier conexión dentro de la red de prueba, pero solamente las conexiones que sean seguras (la seguridad de que dependa sobre lo que esta ejecutando la red de prueba, sobre consideraciones normales de seguridad mucho mayores).

Otro caso puede ser (si esta probándose el ancho de banda de la red) que se busque proteger la red de pruebas del tráfico externo que podría afectar las pruebas, en cuyo caso se pueden negar todas las conexiones que llegan, y permitir todas aquellas que salgan de la red de prueba.

En caso de que se usen ruteadores, es conveniente que se desconecte la red; si se desea evitar esta situación se tiene que hacer al menos que prevenir que el ruteador del firewall capte las rutas actualizadas desde la red de prueba; esto se puede implementar de diversas maneras dependiendo de las configuraciones de la red, qué es lo que esta probando y que ruteadores se tienen disponibles, se puede hacer lo siguiente:

- Usar un protocolo de ruteo diferente desde el primer ruteador bajo prueba y deshabilitar totalmente el protocolo bajo prueba.
- Hacer que el ruteador no acepte cualquier actualización de las rutas desde la interface que esta bajo prueba y filtrar todos los paquetes dentro del protocolo de ruteo.
- Especificar de cuales hosts el ruteador podría aceptar las actualizaciones.

5.2.3 Redes de pruebas.

Si se cuentan con varias redes de prueba, se puede optar por la red de perímetro y tomar un ruteador aparte que este sobre la red de perímetro y de esta manera si se presenta un caso en que se colapse el ruteador, el resto de la red pueda seguir funcionando.

Las redes de prueba son un riesgo, pero no pueden ser menos seguras, en caso de una empresa puede pensar que las redes de demostración, de laboratorio y de entrenamiento para clientes sean inseguras, pero necesariamente necesitaran interactuar con el resto de la organización.

5.2.4 Redes Inseguras.

Las redes de dormitorio y los laboratorios portátiles en donde tienen acceso permanente usuarios ocasionales y la posibilidad de utilizar las herramientas del sistema. La opción para solucionar este problema es una segunda conexión externa (pudiendo ser una nueva conexión al ruteador externo o un nuevo ruteador externo) o configurar un perímetro de red aparte, la ventaja de esto es que se pueden especificar que software se va a ejecutar en estas.

Las redes de demostración y los laboratorios de entrenamiento en donde los usuarios externos tienen un acceso breve, el cual esta supervisado y no puede manejar las herramientas, podrían ser más confiables. Se podría utilizar un ruteador de filtrado de paquetes o un host dual que prevenga que el tráfico confidencial fluya en estas redes. Además se puede optar por limitar el acceso a otros servidores de la red u optar por el servicio NFS para algún servidor o host en particular.

5.2.5 Redes extraseguras.

Por desgracia cualquier organización tiene puntos de su red interna que pueden ser inseguros y también tienen puntos donde es esencial la seguridad (fig. 30). Por ejemplo en las universidades en donde se tengan proyectos de investigación o en las empresas en los departamentos de desarrollo de nuevos productos y en cualquier parte en donde se tengan servidores que contengan datos financieros y contables.

Lugar	Sección
Universidad	Proyectos de investigación.
Empresas	Departamentos de desarrollo de nuevos productos.
Cualquiera	Servidores que contengan registros financieros y contables.
Lugar	Sección
Universidad	Proyectos de investigación.
Empresas	Departamentos de desarrollo de nuevos productos.
Cualquiera	Servidores que contengan registros financieros y contables.

Fig. 30. Ejemplos de redes extraseguras.

5.3 Firewall Freeware[2,13,16].

Amoroso describe una serie de pasos que me parecieron importantes mencionar tal y como se encuentran para poder implementar el firewall:

1. Localizar y obtener el software ya sea que se encuentre en Internet o CD-ROM.

2. Experiencia en cuando a un ambiente adecuado de programación (preferentemente lenguaje C).

3. Hay que modificar el código de manera que las opciones sean las correctas para que se compile y se ejecute en el sistema operativo y en el hardware en donde va a quedar el firewall.

4. Adaptar el código y la configuración de acuerdo a las políticas de seguridad y a los servicios que se desea tener en la organización, es aquí en donde se decide el tipo de autentificación, el control de acceso y el registro de los servicios.

5. Es necesario revisar la documentación relacionada a la instalación, pruebas y al funcionamiento de las opciones del firewall.

Tipo de firewall	Ventajas	Desventajas.
Firewall freeware/shareware	• Mejor evaluación en cuanto a la configuración e integración • Código fuente incluido. • Se ajusta a las necesidades de la organización	• No tiene soporte para un firewall comercial. • No tiene un mecanismo de distribución confiable. • Puede tener virus. • Sin documentación. • Errores en el código fuente.
Firewall Comercial	• Se busca el mejor precio. • Cuenta con soporte técnico. • Se tienen actualizaciones del producto. • Se ofrece entrenamiento de usuarios y del administrador. • Hay migración a otros ambientes.	• No es fácil su manejo, su uso y su entendimiento. • No se comprende totalmente su diseño y el desarrollo que se busca.
Sin firewall	• Menos problemas administrativos.	• No se detectan los accesos ilegales a la red. • La planeación de la recuperación de un ataque no se puede hacer debido a que no se cuentan con los mecanismos que indiquen en donde fue el ataque. • Se puede comprometer la confidencialidad del usuario. • Se pierden datos importantes. • Se pierde la confianza del usuario.

Fig. 31. Ventajas y desventajas de diferentes tipos de adquisición de un firewall.

5.3.1 Ventajas y desventajas.

La ventaja de usar este tipo de software (Fig. 31) es que los administradores y los desarrolladores tienen una mejor evaluación en cuanto a la configuración e integración debido a que cuentan con el código fuente y se tiene una base para adecuar o inclusive mejorar en cuanto a las necesidades de la organización.

La desventaja radica en que el firewall resultante no tiene soporte para un firewall comercial, no se tiene la plena seguridad de que tenga un mecanismo de distribución seguro y hay software que puede tener virus, errores de programación o no venir con documentación. Algunos

esquemas para reforzar la integridad que utilizan criptografía se han propuesto pero no son utilizados.

5.4 Firewall comercial[13].

Hay quien prefiere instalar un firewall comercial, se pueden encontrar de diferentes precios y para plataformas distintas, puede suceder que el firewall sea muy caro y no cumpla con las expectativas o que tenga servicios y confiabilidad. Estos productos se pueden dividir en:

- De hardware, en donde generalmente son ruteadores.
- Software, en donde se ofrecen servicios tipo proxy para distintas plataformas de UNIX
- Elementos de software y/o de hardware tipo plug and play que están configurados para trabajar al momento de que se instalan.

Según los expertos, las soluciones de hardware pueden ser rápidas, las de software son más fáciles de adaptar a un presupuesto restringido y las de tipo "plug and play" son las más seguras.

Es difícil determinar cual de este tipo de firewalls es el más conveniente para la organización, pero se dan algunos lineamientos que son importantes:

- ✓ Identificar los requerimientos de conectividad para la organización.
- ✓ Determinar los requerimientos de desempeño para la organización.
- ✓ Identificar los requerimientos administrativos y operacionales que puedan afectar al firewall.

Características	Descripción.
Escaneo de código.	Revisa el tráfico internetwork en busca de virus, caballos de Troya (sniffers) y applets "malos" desarrollados en Active X o Java.
Monitoreo de la navegación en Internet.	Esto es, se registra qué usuarios visitan qué páginas desde la conexión a Internet de la empresa. Esto puede ayudar a determinar o reforzar las políticas acerca del uso de los recursos de la organización.
Filtros a la navegación del Web	Se controla el acceso de los empleados desde la conexión a Internet de la empresa a sitios del Web que son inapropiados o improductivos.
Redes virtuales privadas.	Esto permite a las redes comunicarse en privado sobre Internet. Se utiliza la autentificación reforzada en las conexiones del firewall encriptando el tráfico entre las parte involucradas. Los estándares están mencionados en la sección 4.15 del capítulo 4. De esta manera, los firewalls de diferentes fabricantes se pueden ligar entre sí.

Fig. 32. Características adicionales de los firewalls comerciales.

5.4.1 Ventajas y desventajas.

Las ventajas son que se puede buscar el mejor precio además de cuidar aspectos como el soporte técnico, mantenimiento del producto, entrenamiento de los usuarios y del administrador y la migración a otros ambientes, además de otras carácterísticas mencionadas en la fig. 32.

La desventaja es que no se puede esperar que el firewall sea fácil de manejar, de usarse o de entenderse, aparte de que el administrador no pueda entender totalmente el diseño y el desarrollo que busca tener el producto.

5.5 Posibles errores en el firewall implementado[34].

Dependiendo de la elección que se haya hecho se puede incurrir en alguna equivocación u omisión en las partes de la planeación o implementación del firewall. En esta parte se presenta una lista de lo que puede suceder, así como consejos prácticos para llevar a cabo las tareas de manera más eficiente y confiable.

1. **Protocolos a usarse.** Hay que determinar los protocolos que se necesitan pasar a través del firewall y el origen y el destino de estos protocolos, una lista común de un esquema de protocolos es:

- Protocolos internos para Internet: telnet, HTTP, FTP, SMTP.
- De Internet para el servidor de correos: SMTP.
- Del Interior para el servidor de correos: POP
- De Internet para el Servidor Web: HTTP.

En donde la parte interna es la red que se piensa proteger con el firewall; para determinar si la lista anterior es la correcta, hay que tomar en cuenta las opiniones de los usuarios y del tráfico que se detecte en la red actual. A menudo los usuarios no conocen que protocolos se usan, sólo después de la instalación del firewall son deshabilitados ciertos protocolos que pudieran causar atención por la utilidad que le dan los usuarios.

2. **La arquitectura del firewall.** Puede incluir cuatro componentes: Internet, la red interna, el DMZ y el firewall. La inclusión en el diseño de todos los componentes de la red como la dirección IP de cada interface de interés, los netmasks, ruteadores y los ruteadores predeterminados. Es necesario pensar en todos estos componentes si se desea instalar un firewall uniforme. Es importante notar que cada interface del firewall puede estar conectada a una subred única, este requerimiento puede implantarse por malla si es necesario, pero su uso puede complicar la instalación y "ongoing" del firewall.

3. ¿Cuál es la conectividad actual entre Internet y las partes?.

Las posibles situaciones son:

Con conexión sin un firewall. Se tiene la difícil tarea de implementar un firewall sobre una conexión funcional de Internet, los usuarios podrían ser avisados a tiempo de la necesidad de implementar un firewall y de los servicios que podría permitirse o negarse para que pueda transitar información por medio de los proxies a través del firewall. Durante la implementación hay que tener cuidado con los cambios del DNS; en los campos TTL (Time To Live) de los registros del DNS, los datos del DNS son captados en periodos de 24 horas, cambiando las direcciones IP pueden desconocerse mientras la información del cache se actualiza, una posible solución es cambiar el TTL de los registros propios del DNS desde una hora hasta algunos días antes de la implementación del firewall, enseguida cambiar el DNS y reinicializar el TTL para 24 horas.

No hay conexiones oficiales. Aquí los usuarios no reconocen lo que se pierde y se pueden imponer restricciones sin decir comentario alguno. A lo mejor los usuarios se puedan conectar a Internet por medio de modems, estas conexiones son puertas traseras en la implementación (por motivos mencionados anteriormente); si no son deshabilitadas, el tráfico puede pasar a través de esta y perder el nivel de seguridad que se había logrado.

La conexión, con una actualización del firewall. Esta actualización puede ser e integrarse al monitorear la operación actual, de este modo se podría permitir al plan de seguridad moverse satisfactoriamente.

4. Hay que considerar ocultar la dirección IP. En la mayoría de los firewalls se implementa un cambio o la ocultación de la dirección, esta característica reescribe la dirección de origen en paquetes que empiezan a ser enviados a la red, la dirección vista en el Internet es la interface exterior que tiene el firewall y el paquete actual puede ser originado en cualquier parte de la implementación. Aparte de incrementar la seguridad, esta cualidad puede facilitar el direccionamiento del error; las direcciones privadas pueden usarse en todas las redes que están atrás del firewall. Sólo las direcciones IP que se pueden ver sobre el Internet son oficiales, la direcciones registradas internamente son "cubiertas" por la dirección que tenga asignado el firewall.

5. Especificar cuantas direcciones IP se desean proteger con el firewall. Este número va a depender del tamaño de la red (o segmento de red) a proteger, para calcular el tamaño de la licencia del firewall (en caso de comprarse); por ejemplo si se tienen 50 computadoras, cada una con dirección IP (estática o de distribución DHCP) y con posible conexión a Internet, entonces se va a tener que adquirir una licencia para 50 máquinas. Esta licencia se relaciona al número de servidores, estaciones de trabajo en los cuales el firewall puede pasar los paquetes de manera confiable.

6. La forma de las reglas. Dependiendo del firewall, las reglas pueden basarse en la información de la red (dirección IP, nombre del host, nombre del dominio) o del nombre del usuario; aunque las reglas básicas puedan ser temporales, estas pueden causar problemas, considerando la implementación que ofrecen las direcciones IP que cuentan con el DHCP. Si los usuarios tienen algunos derechos de acceso a Internet, el nombre del usuario es la única información estática que puede ser la base para las reglas de acceso. Desgraciadamente, cada acceso URL de HTTP crea una nueva conexión TCP. Puede ser que a algún usuario le pase que a cada URL que accese le pida el login y el password.

En caso de que se considere usar el VPN fuera de los E.U.; pero, por las restricciones de exportación del gobierno de ese país sólo esta permitido la exportación de tipos de autentificación y de encriptación que son débiles en comparación con los que se cuentan en el mercado estadounidense debido a que es un canal de autentificación, encriptado y se considera como arma militar ultrasecreta.

Algunos firewall no tienen la característica de permitir o negar el acceso a URL (Uniform Resource Locator, es la dirección global de documentos y otros recursos del World Wide Web) específicos, algunas presentaciones si tienen esta cualidad en varias categorías. La lista que se usa de URL en este programa es actualizada por medio de suscripción, otras utilizan listas estáticas de sitios "no recomendables" de los cuales se recomienda negar el acceso.

Varios métodos de autentificación pueden implementarse en el firewall, estos incluyen passwords estándar como el S/Key y métodos de token de hardware como el CryptoCard y SecurID; si se implementa la autentificación de usuario, el firewall podría fungir como un "request forwarder", adelantando los requerimientos del usuario al servidor de autentificación y dependiendo del resultado de la autentificación se le permitirá o se le deshabitará la conexión.

Si el firewall es un producto comercial, hay que asegurarse que el hardware que se planea usar tenga el soporte necesario, este criterio puede depender del producto y del uso que se le piense dar. Es decir si se piensa usar túneles VPN u otras formas de encriptación será necesario un sistema más rápido.

El DNS es importante tenerlo en cuenta para la implementación exitosa del firewall, hay varias opciones de servicios del DNS, muchas de las cuales están diseñadas del split-DNS. En el split-DNS hay dos nombres de espacios DNS separados, dentro de la implementación se necesita un nombre de servicio para las máquinas internas y es así como el servidor del DNS de esas máquinas puede resolver la cola de las direcciones de Internet; fuera de la implementación, los sitios que se encuentran en el Internet necesitan ser capaces de resolver las direcciones por su compañía de servicios públicos. Para solucionar este problema se agrega al servidor del ISP como el primario o al servidor DNS en segundo lugar. El firewall o la máquina interna puede servir como un servidor DNS interno, el único problema que quedaría es conseguir que el servidor interno pueda adelantar los requerimientos al firewall o al ISP para resolver los nombres de Internet, A menudo, el bajo desempeño de la conexión esta relacionado con la incorrecta configuración del DNS.

Es importante educar a los usuarios, por las siguientes razones: el firewall es el primer paso en la seguridad del sitio *y los usuarios necesitan estar informados que son parte de los problemas de seguridad y su posible solución*. Se debe informar que el firewall puede identificar y mostrar lo que esta haciendo el usuario entre la parte protegida y la que no lo esta.

5.6 Ejemplo de un firewall[2,42].

El software FWTK (FireWall ToolKit) lo desarrolla Marcus Ranum, un directivo de la empresa Trusted Information System en los Estados Unidos, con este paquete se arma un firewall sobre el sistema operativo UNIX, de esta manera el administrador de una red puede bajar esta implementación y usarla para construir el firewall que se adapte a las políticas del sitio o de la organización. Sigue una serie de principios (que se presentan como ventajas en el capitulo anterior), los cuales son:

- Simplicidad en el diseño.
- Administración centralizada de la configuración.
- Desconfianza acerca de puntos no claros en cuanto a seguridad.

Es un conjunto de programas que ayuda a la construcción de firewalls para redes computacionales, estos pueden ser usados solos o como parte de otros componentes de firewall, esta diseñado para ejecutarse en sistemas UNIX usando una interface Berkeley (socket).

Con este software se pueden hacer practicas de configuración, esto se entiende como la parte de configurar el sistema existente, mientras que un componente de la herramienta es un programa aparte el cual puede reemplazar y reforzar alguno ya existente. Se asume que cuando se hagan las prácticas se tiene que verificar que la parte a modificar soporte al software suplente, esto se podrá encontrar en la documentación del sistema operativo.

Instalar este software implica tener experiencia con la administración de sistemas UNIX y de redes TCP/IP. Como perfil mínimo se debe de estar familiarizado con la instalación del software y mantener en ejecución un sistema UNIX; dado que los componentes del software cuentan con su código fuente y es muy importante estar familiarizado con la construcción de estos paquetes. Hay que tener muy presente los requerimientos de instalación, topología de red hardware disponible y la administración debido a que estos son puntos que son diferentes de organización en organización. Dependiendo de como se configure el software, pueden ser ejecutados diferentes niveles de seguridad, esto va a depender en gran medida del entendimiento

que tenga el administrador del sistema acerca de las políticas de seguridad a proteger en cuanto a cuales son los riesgos aceptables, cuales no y conciliarlos con los requerimientos de los usuarios. Esto es la parte más crítica en la implementación de cualquier sistema de seguridad y en consecuencia sólo se cuentan con los componentes para construir una posible solución.

Arquitectura del firewall.

Este software soporta las siguientes arquitecturas:

- Firewall gateway dual.
- Firewall de host protegido.
- Firewalls gateway de subred protegida.

En estos, el factor común es el host bastión, el cual actúa como un "separador" de la aplicación, identificador del tráfico y proveedor del servicio; el mantenimiento de este es importante y es donde son importantes la mayoría de las configuraciones del firewall.

5.6.1 Herramientas de software.

Los componentes son programas que se ubican en el nivel de aplicaciones, pueden reemplazar o añadir software ya existente, algunos de los cuales existen para otros desarrollos que funcionan igual y que pueden ser usados adicionalmente a los componentes.

5.6.1.1 SMAP.

El SMTP esta conformado por dos herramientas: smap y smapd, este tiene una amenaza al sistema, hace que los correos se ejecuten con permisos de nivel de sistemas para entregar los mensajes de los usuarios en sus respectivos buzones, los direccionamientos que hacen estas dos herramientas aíslan al correo restringiéndolo en un directorio por medio del "chroot", con un usuario no privilegiado (nobody); no direccionan cualquier evento relacionado con la alteración del correo o ataques de negación de servicios por medio de correo. El propósito de la versión mejorada de SMAP es eliminar un bug del programa del cual se basan los hackers para atacar; el volumen de trabajo de proceso de correos lo desempeña el sendmail, en donde no se requieren modificaciones al sendmail o a su archivo de configuración. Cuando un sistema remoto se conecta al puerto SMTP, el sistema invoca al smap, en el cual chroot restringe al directorio y lo configura con un usuario no privilegiado, y así para smap no es necesario un archivo de configuración, el directorio restringido no debe de contener archivos diferentes a los que smap crea y no hay riesgo de que sea "engañado" para modificar archivos de sistema.

Tiene tareas muy definidas como interactuar con el SMTP de otros sistemas, concentrar los mensajes de correo, escribirlos al disco, generar bitácoras y salir, otra parte del sistema no se ejecuta en el directorio restringido y no requiere permisos; smapd se ocupa de escanear el directorio smap spool periódicamente y envía los mensajes enlistados para un reparto final. Si es configurado debidamente el sendmail y smapd se ejecuta con el identificador de correo UUCP puede ser entregado normalmente sin requerir smapd para ejecutarse con permisos reforzados. Cuando smapd envía el mensaje, es eliminado del área spool.

5.6.1.2 Netacl.

Por desgracia el inetd no tiene controles de acceso, es decir que cualquier sistema puede conectarse a un servicio que se encuentre listado en inetd.conf. Hay varias situaciones en donde es necesario el propósito general del control de acceso a los servicios de la red, y las herramientas para poder implementar este control están disponibles en Internet desde hace algunos años. Con netacl se permite especificar el control de accesos arbitrarios de cada servicio de red basándose

en la dirección de red del cliente del host y del servicio solicitado (con la dirección IP o el nombre del host), se puede invocar una versión diferente de telnetd cuando se conecta al puerto del servicio telnet en el firewall.

No cuenta con el control de acceso UDP, pero otras herramientas disponibles en Internet (como el TCP_Wrappers de Wietse Venema) soporta el control de acceso de algunos servicios UDP. Autentificar de manera confiable el origen del paquete UDP es imposible con la tecnología actual, debido a esto netacl mantiene la seguridad de los servicios UDP en "off".

La mayoría de los servicios están deshabilitados por default, como el finger, que puede estar habilitado para algunos hosts de una red privada; juega un papel importante en las prácticas de configuración empleadas por otros servicios como el FTP anónimo debido a la configuración del directorio restringido. Esta funcionalidad permite flexibilidad para servicios específicos que pueden ser ejecutados aisladamente; por ejemplo, un servicio proxy finger puede ser implementado para configurar al netacl para invocar al fingerd como un usuario no privilegiado y ejecutarse de manera aislada, si en fingerd hay una falla de seguridad no puede aprovecharse.

Se puede usar el netacl para bloquear todos los servicios, pero para algunos hosts puede permitir identificarse en el firewall por medio del telnet o rlogin, y es usado para hacer posible bloquear el acceso desde el sitio del hacker al momento de un ataque.

La seguridad se basa en los nombres del host y/o la dirección IP; la dirección IP es usada para el control de aplicaciones críticas para evitar el uso del DNS que altere la fuente de la conexión, por desgracia no protege contra ataques que alteren el origen del ruteo de la dirección IP o por otros medios; si el ataque es de interés, el ruteador es capaz de proteger los paquetes de la ruta de origen que se haya empleado. La seguridad de inetd es considerada en la configuración

5.6.1.3 ftp-gw.

Es utilizado para permitir la transferencia de datos a través del firewall sin comprometer la seguridad de este, Este proxy soporta el control de acceso basado en la dirección IP y/o la dirección alfanumérica, además de soportar un control secundario que permite que cualquier comando de FTP pueda ser seleccionado para bloquearse. Los destinos pueden ser selectivos también. Todas las conexiones y los bytes transferidos son identificados y registrados.

Aprovecha el directorio restringido de otras aplicaciones, además soporta la autentificación avanzada que puede ser agregada al gateway, para pedir la autentificación al usuario para exportar o importar los archivos. Puede ser implementada de acuerdo con una política de datos consistente. Además se incluye una versión modificada del demonio FTP el cual permite al administrador tener los servicios de FTP y del proxy FTP en el mismo sistema.

5.6.1.4 telnet-gw.

Se usa para permitir el acceso a las terminales remotas a través del firewall sin comprometer su integridad, su control de acceso se basa en la dirección IP y/o la dirección alfanumérica, adicionalmente permite un control secundario que permite seleccionar cualquier destino para ser bloqueado. Todas las conexiones y los bytes transferidos son registrados, cuando se conectan al telnet-gw se presenta un menú sencillo con opciones de ayuda al conectarse, las cuales no invoca subshells o programas, no ofrece acceso a un login interactivo sobre el sistema del firewall.

5.6.1.5 rlogin-gw.

Sirve para dar soporte al acceso a la terminal por medio del protocolo rlogin de BSD, por medio de revisiones de permisos y controles de acceso de la misma manera que el telnet; el

cliente de rlogin puede especificar un sistema remoto como parte de la conexión inicial al proxy, eliminando la necesidad de la interacción del usuario si la autentificación no es requerida.

5.6.1.6 plug-gw.

Los servicios regulares como el news Usenet son a menudo provistos a través del firewall, en esta situación el administrador cuenta con la opción de ejecutar el servicio sobre el firewall o instalar el servidor proxy. Hace que se ejecuten las news directamente sobre el firewall exponiendo al sistema a cualquier bug en el software de news, es confiable usar el proxy para el servicio gateway sobre un sistema seguro sobre la red protegida, este proxy puede ser empleado para propósitos generales.

Cuando un sistema externo se conecta al puerto del NNTP, se conecta al servidor de noticias diseñado sobre la red interna. Si el servidor de noticias en la red interna conecta para el puerto de noticias sobre el firewall, se conecta al servidor de noticias que esta sobre la red externa. Esta conexión recíproca se basa en la dirección IP del host que se conectó primero. Al conectarse copia los datos bajo un lado y del otro termina la conexión y ahí es el punto de salida. Se configura permitiendo o negando las conexiones basándose en la dirección IP o en la dirección alfanumérica. Todas las conexiones y los bytes transmitidos son registrados.

Puede fungir como un centinela entre la red protegida y la red externa, se debe de usar con precaución, trabaja sólo como un filtro de datos, no invoca subshells o procesos, para las noticias (news) ofrece una buena protección. De igual manera hace un registro de todos los movimientos.

5.6.1.7 Authsrv.

Es un servicio de autentificación para las aplicaciones de red, su uso es opcional y es requerido por los proxys de FTP y telnet. Ofrece una interface para múltiples formas de autentificación, es útil en el caso de grandes organizaciones debido al uso de una base de datos sencilla. Un shell administrativo permite manipular esta base de datos desde cualquier punto de la red, con soporte opcional para la autentificación de transacciones encriptadas.

Tiene un soporte para un grupo de administración; uno o más usuarios pueden ser identificados como el administrador de un grupo de usuarios y puede añadir, borrar, habilitar o deshabilitar a un usuario de un grupo. Internamente mantiene información de la última vez que el usuario se autentifico, cuantos intentos hizo y fallo y puede deshabilitar automáticamente las cuentas que tienen múltiples fallas; se obtienen registros detallados de todos los movimientos. Se recomienda la instalación de este en un host seguro, como el host bastión dado que la base de datos puede ser un punto de ataque.

5.6.1.8 telnetd.

Por razones administrativas es necesario tener el login activado para hacer el debido mantenimiento en la computadora que tenga instalado el firewall. El servidor (telnetd) puede ser configurado para ejecutarse en el firewall, en el archivo inetd.conf; se recomienda accesar al telnetd usando el netacl, con un número limitado de hosts a conectarse; además, el procedimiento de identificación sobre el firewall requiere de algún cambio de password con algún algoritmo de reto/respuesta para la autentificación.

5.6.1.9 login.

Se hace por medio del programa login-sh, da soporte a varios métodos de autentificación usando algún token como en SecurID de Security Dinamics, SecureNet de Digital Pathways y

otros. Lo que hace es adicionar una condición de autentificación para el usuario, con esto no son necesarias hacer modificaciones al sistema.

5.6.1.10 ftpd.

Era común que el ftp permitiese que el usuario se identificara como anónimo (anonymous) o ftp para poder accesar al sistema, el usuario accesa con privilegios de root en el directorio de la cuenta de FTP, en donde es controlado el acceso por medio del FTP anónimo; pero por desgracia puede existir un bug en el software

5.6.1.11 syslogd.

Tiene una versión de demonio del sistema de identificación el cual permite especificar una búsqueda de patrones de expresiones regulares en el archivo de configuración y cuando es recibida una identificación tiene la capacidad de invocar programas específicos permitiendo el escaneo en tiempo real de las identificaciones del sistema y alertas del mismo tipo. El llamado de los programas de los patrones y entradas de identificación es una poderosa herramienta que permite al administrador disparar una baja del sistema o redireccionar el mensaje a un beeper o correo electrónico.

Esto es una traducción de un software freeware, para ejemplificar su uso se plantea lo *siguiente:*

5.6.2 Exposición del problema.

Por ejemplo, supongamos que el único servicio que ofrece el sitio "inseguro" es telnet y se desea implementar un firewall con recursos que tenga la organización; para este caso, se va a utilizar un firewall de host "oculto" o protegido y un ruteador que filtre los paquetes y como proxy al tn-gw del software freeware que se explico anteriormente, las tareas que va a desempeñar el ruteador son las siguientes:

Lo primero que hay que hacer es reconfigurar la red (fig. 33) para eliminar la mayor parte de vulnerabilidades, se crea un segmento de red "externo" (el DMZ) en donde los sistemas que necesitan tener contacto con Internet son conectados (servidor Web, servidor de e-mail), se utilizará un ruteador para proteger las direcciones IP y los protocolos.

Luego se tiene que tener un host que va a trabajar como un gateway hacia Internet, promoviendo una separación de las redes haciendo del gateway un servidor proxy para los usuarios de las redes, hay que registrar todo el tráfico que llega a través de la conexión con Internet. Además hay que revisar (además de lo sugerido en el capitulo III en la parte que se habla del gateway) los siguientes puntos:

1. Ejecutar una versión "segura" del sistema operativo que utilice el hardware elegido, esto es para protegerse de las posibles debilidades del sistema y dar confiabilidad al firewall.
2. Se tiene que instalar sólo los servicios que el administrador de la red considere necesarios. Comúnmente se instala proxies de telnet, ftp, dns, smtp.
3. En esta parte es muy conveniente instalar software para autentificar a los usuarios, puede ser, dependiendo de las necesidades de la organización que se tenga que implementar autentificación para cada servicio proxy con que cuente el firewall.
4. Cada proxy debe de contar con opciones limitadas de los servicios a soportar.

5. Se debe de generar información que identifique todo el tráfico, la cantidad de conexiones realizadas y la duración de las mismas.

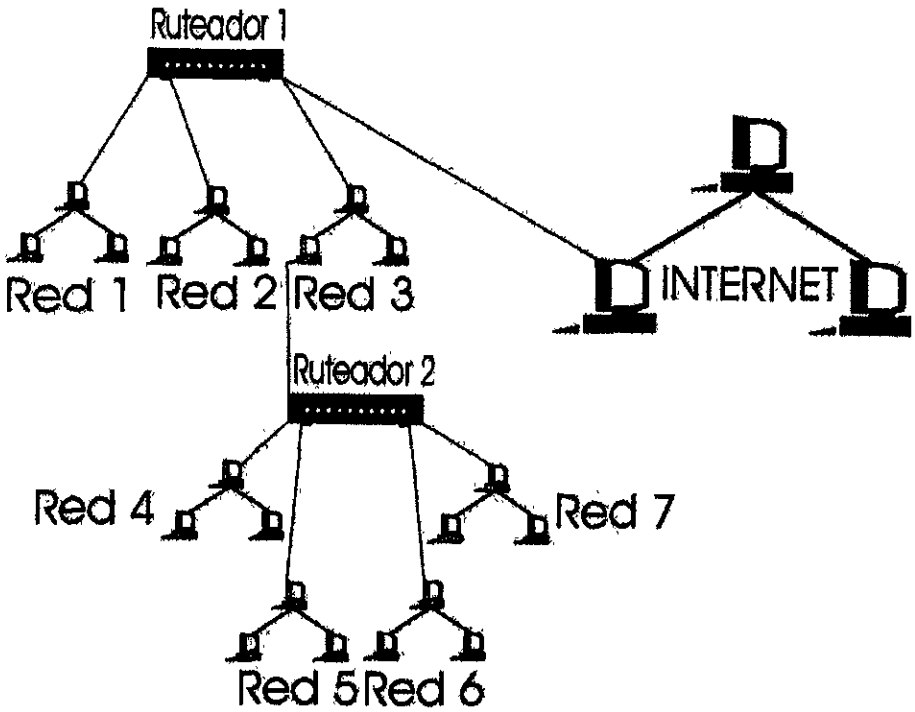


Fig. 33. Red original (ejemplo).

6. Se recomienda que el proxy a utilizar tenga el menor número de líneas posibles, debido a que es más fácil de buscar cualquier alteración o bug futuro que se llegase a encontrar.
7. Cada proxy debe ser independiente entre sí, es decir, un proxy para el servicio telnet, otro para el ftp y sucesivamente, debido a la posibilidad de un nuevo servicio a proteger.
8. El proxy debe de ejecutarse junto con la configuración de la máquina, de esta forma se evita la instalación de sniffers o cualquier otro programa que pueda comprometer al proxy.
9. Cada proxy se debe de ejecutar con un usuario no privilegiado (se recomienda el uso de nobody) y sobre un directorio seguro y privado (se recomienda el uso de chroot).

Es recomendable este host gateway para reforzar lo implementado, ya que puede ser el primer punto de revisión para el tráfico que pasa por el ruteador externo, puede protegerse todos los movimientos que necesite y en un segundo paso permitir el paso al tráfico hacia los sistemas en la red protegida. Por ejemplo, un usuario que se encuentre en el exterior que desee enviar un archivo a un host que se encuentra en la parte protegida, este movimiento se haría por medio del gateway y pasaría indirectamente hacia el host deseado. El gateway recibe el requerimiento de FTP y responde al usuario, con ayuda de un proxy el gateway hace el requerimiento de FTP al host que se encuentra en la parte protegida. Como el proxy hace todo el trabajo a la inversa, se puede ocultar la dirección de cualquier host que se encuentre en la parte protegida.

El gateway tendría que actuar como DNS para el exterior identificando algunos hosts (como el servidor Web o el servidor Mail)

Se debe de configurar un ruteador con las dirección IP a proteger todo el tráfico que va llegando al puerto del ruteador desde el acceso de Internet. para esto hay que verificar:

¿Cualquier puerto del ruteador puede conectar a los usuarios a otras redes que puedan tener acceso a Internet?.

¿Puede conectarse un servidor con un ISP por medio de un servicio privado o especializado?.

Se debe de identificar los hosts de Internet que van a tener acceso a la red protegida (o algún segmento), hay que realizar una tabla con las direcciones IP respectivas. Es decir:

1. Enrular los todos los paquetes al host bastión (partiendo del ruteador interno).
2. Negar el acceso a todas las rutas diferentes al host bastión (partiendo del ruteador externo).

Por ejemplo se tiene que configurar al ruteador para que sólo permita el tráfico que viene desde el host del ISP.

Después de haber cumplido los puntos anteriores al 100% se procederá a instalar al proxy de la siguiente manera:

1. El binario se deberá de almacenar en un subdirectorio que no sufra modificaciones intencionales o accidentales. Cualquiera que se utilice se especificará en el archivo instalador del mismo proxy.
2. Hay que hacer modificaciones en el archivo inetd.conf de la siguiente manera:

telnet stream tcp nowait root /usr/sbin/in.telnetd in.telnetd

a

telnet stream tcp nowait root /usr/local/sec/tn-gw tn-gw

y agregar:

authsrv stream tcp nowait root /usr/local/sec/authsrv authsrv

Esta última línea va a permitir utilizar un servidor de autentificación de usuarios.

3. Agregar al archivo *services*:

tn-gw 24/tcp
authsrv 7777/tcp

4. Y por último al archivo rc* que corresponda:

/etc/rc.local

Que es un script que ejecutará:

/usr/local/sec/netacl -daemon telnet telnetd &
/usr/local/sec/authsrv -daemon 7777 &

5. En el archivo netperm-table que se encuentra en el subdirectorio en el cual se instalo el proxy; por ejemplo, para permitir el acceso a un solo servidor se tiene:

```
tn-gw:      denial-msg    /usr/local/sec/tn-deny.txt      #mensaje de negacion de servicio
tn-gw:      welcome-msg   /usr/local/sec/tn-welcome.txt  #mensaje de bienvenida
tn-gw:      timeout 3600
netacl:     permit-hosts 127.0.0.1
tn-gw:      permit-hosts 132.248.80.165 –passok -xok
```

Este software sigue la segunda política que dice "Negar cualquier servicio si no esta expresamente permitido" si se desea permitir otros servicios como ftp, correo electrónico o http, hay que agregar los respectivos proxies. La configuración física final del ejemplo mostrado anteriormente se visualiza en la fig. 34.

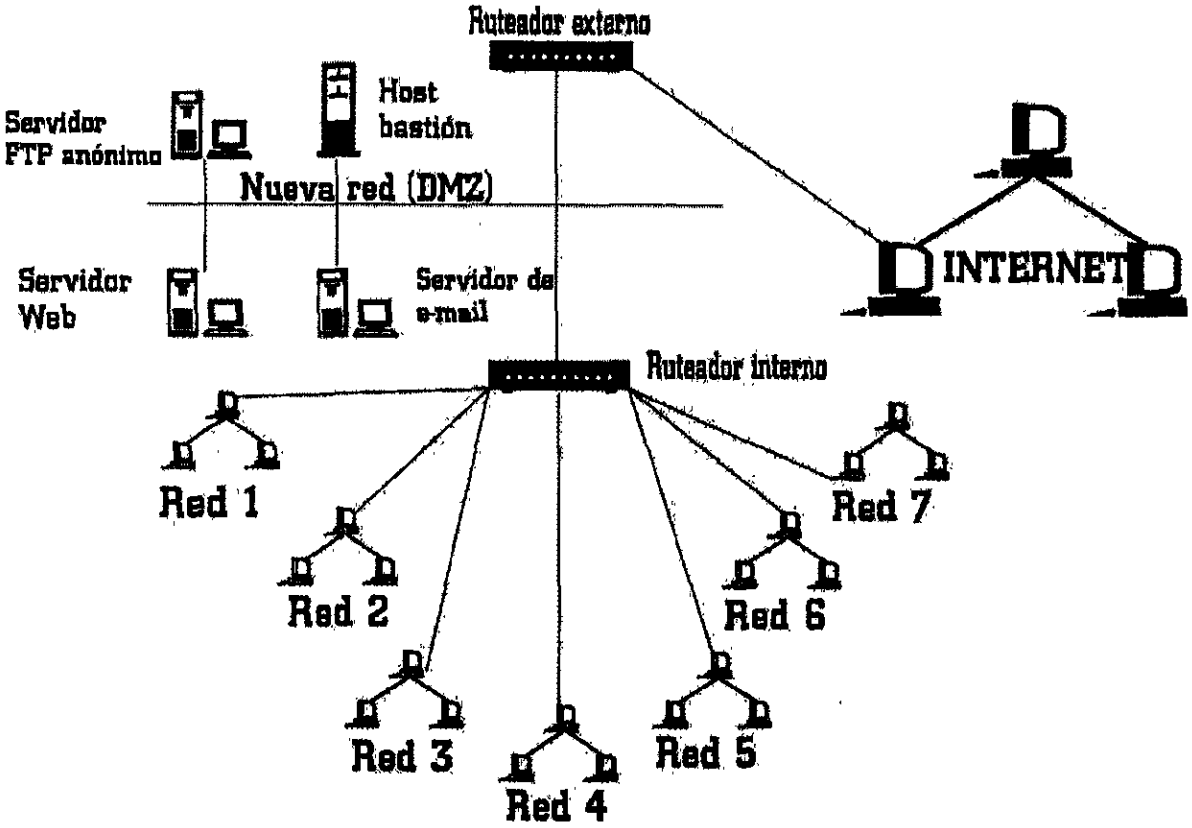


Fig. 34. Configuración final de la red (ejemplo).

Si se hace un telnet al host bastión desde el host con la dirección 123.456.78.9.123 vera lo siguiente:

```
telnet inseguro.acatlan.unam.mx
Trying 132.248.180.161...
Connected to firewall.acatlan.unam.mx.
Escape character is '^]'
Bienvenido a la red SUN de la ENEP Acatlan

Cualquier problema favor de enviar un correo electrónico a :

root@firewall.acatlan.unam.mx
tn-gw->
```

Y solamente se podrán utilizar las siguientes opciones en el proxy:

connect host [serv/puerto]	Conecta al *host* especificado en algún servicio o puerto.
telnet host [serv/puerto]	Lo mismo que el anterior.
x-gw [host/display]	Se especifica el host en donde se va a realizar el despliegue de las aplicaciones X Windows.
Password	Cambia de password, sólo permita esta opción desde el host que este especificado en el archivo netperm-table.
timeout segundos	Especifica los segundos en que el proxy identificará las conexiones después de que se terminen.
quit/exit	Es la salida del proxy.

Para conectarse a otro servidor se ejecuta:

tn-gw-> connect protegido
Trying 132.248.180.198 port 23 ...
Connected to protegido.
UNIX(r) System V Release 4.0 (protegido)
login:

Por desgracia, no se cuenta con el equipo suficiente para poder mostrar otro ejemplo, debido a los altos costos o a la falta de disposición de los mismos. Además que para todas las organizaciones que cuentan con algún tipo de implementación, consideran toda la información relacionada como estratégica y por tanto esta prohibida su distribución fuera de las personas que administran el firewall.

Conclusiones

Después del desarrollo de este trabajo de investigación acerca de los firewalls llegue a las siguientes conclusiones:

Antes de analizar la posible implementación de un firewall es muy importante identificar las necesidades de seguridad que tenga el sitio o la organización y desarrollar una estrategia para proteger la información, puede ser que los resultados obtenidos generen políticas y procedimientos que se necesiten especificar que indiquen la implementación de cualquier esquema de seguridad.

Las políticas y los procedimientos son la base de acción para poder responder a este tipo de incidentes ya que el tiempo que se pierde al restaurar el sistema (en caso de alguna modificación y su detección temprana) es muy valioso para la organización.

El *firewall es una buena opción para proteger una red contra* accesos no deseados, además de llevar un registro de todos los movimientos que haga cualquier usuario entre la red "confiable" y la red no confiable; pero antes, las personas involucradas deben de verificar los siguientes puntos:

Al momento de seleccionar un firewall se puede utilizar los servicios de un consultor; revisar los perfiles del personal que disponga la organización ya que se puede contar con alguien para efectuar este trabajo; afortunadamente, por cuestiones de mercado hay diferentes tecnologías de diferentes precios; es muy probable que exista la necesidad de adquirir hardware adicional y muy importante, el precio no implica poder, utilidad y velocidad. En caso de compra, debe de contar con la debida capacitación para los usuarios, así como el soporte técnico adecuado a las necesidades de la organización y facilidades adecuadas para configuración, implementación y prueba.

Algunos consejos prácticos, ya enunciados por algunas personas y otros mas, se presentan a continuación:

Para el administrador:

- ✓ Debe de contar con los conocimientos acerca del sistema operativo en donde se vaya a implantar el firewall, ya que son necesarias hacer algunas modificaciones a los archivos de configuración del sistema (en el caso de UNIX), actualizar o reforzar el sistema en cuanto a parches y correcciones de errores presentados, dependiendo de las necesidades que surjan se podrían utilizan algunas herramientas de UNIX (awk, grep, sed, etc.) para dar un formato adecuado al proceso de las auditorias que se presenten. Y esta experiencia a su vez, ahorra costos a la empresa (por soporte técnico).

- ✓ Contar con la experiencia en cuanto al manejo de hardware en donde se instale el sistema operativo, ya sea una estación de trabajo o un ruteador.

- ✓ Tener conocimientos de algún lenguaje de programación (preferentemente lenguaje C), ya que si se tiene la fortuna de contar con el código fuente del firewall serán necesarias hacerle algunas modificaciones para poder acoplarlo a las necesidades de la organización.

- ✓ Sugerir a las personas responsables, políticas y procedimientos para el buen funcionamiento del software y hardware con que cuenta la organización.

- ✓ Estar al pendiente de cualquier noticia relacionada a la seguridad del sistema en particular, para poder tomar acciones para corregir el problema encontrado.

- ✓ Mostrar a los usuarios cómo y de que manera serán afectados en su trabajo (en cuanto al uso del firewall) al momento que se haga la implementación del firewall, así como los lineamientos que tienen que seguir para poder utilizar los recursos de manera externa o de otra red interna, según se hayan hecho las implementaciones.

- ✓ El trabajo de los administradores del firewall puede ser muy alto, ampliamente se recomienda que haya al menos una persona que se encargue de estas labores.

- ✓ Para facilitar el trabajo de administración de un firewall hay que contemplar lo siguiente: Las auditorías deben ser legibles en su representación así como la información que se recaba con los eventos de alerta; Posibilidad de cambio de servicios en caso de ataques frecuentes o la generación de algún cambio en la política de seguridad y la flexibilidad de agregar nuevas características generadas por el surgimiento de nuevos servicios o correcciones de errores del mismo firewall.

- ✓ Es muy importante la capacitación de los usuarios involucrados (administradores y usuarios) ya que el inadecuado manejo del firewall puede generar una inseguridad mucho peor.

- ✓ Para comprobar que efectivamente las políticas de seguridad en general y en el caso particular del firewall se apliquen se debe de monitorear constantemente su funcionamiento, ya sea ejecutando herramientas que pueda usar un hacker, revisando los registros del firewall; se sugiere contemplar un periodo de pruebas periódicas, aleatorias y ejecutadas por "terceros" para cambiar las políticas y procedimientos vigentes en caso necesario.

Para el usuario:

- ✓ Se debe de estar al pendiente de las políticas en cuanto a cómputo para adecuarlas al trabajo diario.

- ✓ Procurar expresar las sugerencias y las dudas al respecto, ya que los servicios de cómputo son ofrecidos para apoyar las exigencias de las tareas encomendadas por la organización.

- ✓ En la medida de lo posible no elegir un password que sea fácil de adivinar, no olvidar su password ni prestarlo a nadie, ya que estos hechos originan grandes problemas en cuanto a la seguridad de una red (sitio).

- ✓ Como resultado de la implementación de las políticas de seguridad, pueden modificarse los servicios que se tengan en la organización; resultando en un cambio en sus opciones, su disponibilidad y en su desempeño.

Para los directivos de la organización:

- ✓ Tener en cuenta que la información que contiene el software o el hardware tiene diferentes grados de importancia, y basándose en ella se necesitarán ciertas medidas de seguridad que debe de tomarse e instituirse como políticas de la organización.

- ✓ Se debe de contar con los recursos suficientes para poder garantizar el correcto funcionamiento de los sistemas de información de la organización, aparte de los propuestos en este trabajo, se recomienda tener contratado un servicio de soporte técnico de todo aquel equipo que de alguna manera sea vital para la organización (servidores Web, servidores de correo electrónico, ruteadores, etc.). En caso de no ser posible esto, entrenar debidamente a las personas encargadas de su manejo.

- ✓ Es muy importante el nivel de las políticas de seguridad que tengan en la organización, es muy recomendable que se establezcan a nivel general, tomando en cuenta las necesidades de cada elemento además de contar con todo el apoyo de la planta directiva.

Por desgracia el firewall sólo protege contra los usuarios que pudieran hacer uso de la red – o redes – protegida de manera externa, pero es en la parte interna en donde se debe de poner especial atención, ya que la mayoría de los incidentes de seguridad que ocurren en una red se encuentra implicado un usuario de la red interna.

Se tiene que cortar el acceso a los recursos informáticos a los usuarios que ya no forman parte de la organización.

El administrador de estos recursos puede ser el responsable directo de que esta implementación falle, ya que por irresponsabilidad o ignorancia se corre el riesgo de perder la protección que se le dio al sistema (ya sea de manera física o de manera lógica).

Gracias a este trabajo, me fue posible conocer temas muy interesantes como el Modelo OSI, comandos y archivos de configuración de UNIX, tipos de ataques más comunes en Internet, las ventajas y desventajas que puede tener un firewall frente a otras opciones de seguridad (como el "multilayer Switching") y las validaciones que se tienen que hacer al momento de implementar un firewall (tener un sistema operativo con todos sus parches, tipos de administración entre otros). Hay otros temas que me hubiera gustado incluir en esta investigación como el SSH (Secure Shell), el uso de agentes en la seguridad de un sistema, el uso de clusters para agilizar los procedimientos de protección de un sistema; pero por razones de espacio no fue posible.

Por otro lado, la bibliografía relacionada con el tema es muy escasa en nuestro país y el envío del material bibliográfico desde los E.U. es bastante tardado. Las empresas que cuentan con una implementación de firewall, consideran toda la información relacionada como estratégica, resultando de ello el pequeño ejemplo que se expuso en la sección 5.6.2 del capítulo V.

Para finalizar estas conclusiones, me resta decir que la seguridad en los sistemas computacionales es un paradigma en constante cambio de acuerdo a los avances tecnológicos (en cuanto a software y hardware) resultando en una disponibilidad de nuevos servicios que en un futuro resulten en nuevos riesgos de seguridad y las necesidades de la organización. Le recomiendo a la persona que lea este trabajo que consulte la bibliografía así como el anexo II dado que la actualización es fundamental ya sea para elegir un firewall, implementarlo actualizarlo o simplemente para elegir una decisión adecuada basándose en las necesidades de corto, mediano y largo plazo de la organización.

Anexo I

Tipos de proxy (clasificación independiente).

Hay cinco niveles de proxies

- circuit-layer
- traffic-aware
- command-aware
- content type-aware
- policy-aware

Estas definiciones son un poco enredadas, debido a la conveniencia de los vendedores basándose en los argumentos que ofrecen en cuanto al soporte que tienen de un protocolo en particular, los cuales son:

Circuit layer proxy.

Esta clase de proxy no tiene ningún proceso especial de cualquier octeto en la cadena de datos, solo se entera de la información de los encabezados como la dirección de origen y de destino y los respectivos puertos, pueden guardar los vestigios de cuantos bytes son mandados o recibidos, en las demandas de los protocolos no son posibles en este proxy debido a que no se comunica el protocolo de la aplicación y no es necesario el puntero TCP.

Traffic-aware proxies.

Este tipo de proxy hace un procesamiento especial en algunos bytes de la cadena de datos, puede propagar los punteros TCP urgentes de manera adecuada y puede fluir el buffer en puntos adecuados de la cadena de datos, las demandas de los protocolos son posibles, pero la identificación o filtrado de los datos dada el final de la sesión no es establecida.

Command-aware proxies.

Esta clase de proxy entiende todos los comandos que pueden pasar a través del proxy, permiten los comandos legítimos y niegan los que no están legitimizados. Los comandos son identificados y el proxy los filtra, estos filtros pueden estar controlados por el administrador, las demandas de los protocolos son aceptadas pero el resultado y/o los datos transferidos asociados con los comandos no son filtrados o identificados.

Content type-aware proxies.

Entiende el formato general del contenido, pueden verificar que el contenido correcto este presente, si se pueden filtrar el contenido de los tipo o escanear el contenido del paquete para problemas de seguridad conocidos, por ejemplo escanear el correo electrónico para explorar el encabezado, transferencia de archivos por FTP, transferencia de tipos application/java en HTTP.

Policy-aware proxies.

Este tipo de proxy esta en sobreaviso del contenido que puedan tener los paquetes que recibe, pero solo tiene la capacidad de decodificar y rechazar el contenido de la transmisión por razones de la política local, esto podría incluir otros campos incluyendo política de hostigamiento sexual.

El caso más probable es escanear virus, a menos que alguna característica del proxy HTTP pueda buscar en el contenido del HTML y el hecho de "bajar" código de Java y removerlos

(por ejemplo los applets) en caso de que en la política se contemple que no se permite Java en la red.

Este caso se distingue del anterior en que el contenido de la transmisión es examinado, mientras que el anterior solo examina el contenido del paquete. Aquí se podría reconocer un documento de Word, mientras que el caso anterior removería solamente cualquier macro virus de Word.

Anexo II

Lugares de actualización de tópicos de seguridad [8,13,26]

Se recomienda tener el conocimiento de lugares y personas a las que se pueda consultar en caso de surgir alguna duda al respecto o para ampliar los conocimientos en cuanto a seguridad, aquí se ponen unos sitios en Internet que pueden ser de gran ayuda:

CERT, Computer Emergency Response Team.

ftp://info.cert.org/pub/cert_faq
http://www.sei.cmu.edu/SEI.programs/cert.html

CIAC, Computer Incident Advisory Capability del Departamento de Energía de los E.U.

http://ciac.llnl.gov

CPSR, Computer Professionals for Social Responsability.

http://cpsr.org.home

EFF, Electronic Frontier Foundation.

http://www.eff.org

EPIC, Electronic Privacy Information Center.

http://www.iss.net/epic.org

FIRST, Forum of Incident Response and Security Teams.

http://first.org/first

Internet Society

http://www.isoc.org

ICSA, International Computer Security Association.

http://www.icsa.net

MxCERT, Mexican Computer Emergency Response Team.

http://www.mxcert.org.mx

ASC, Área en Seguridad en Cómputo, DGSCA UNAM.

http://www.super.unam.mx/asc

Glosario

API, Application Program Interface. Es una Interface (semántica y sintaxis de un lenguaje de programación) que define cómo un programa o conjunto de servicios puedan ser usados por otros programas y servicios.

Aplicación front-end. Este tipo de aplicaciones esta enfocada al usuario final, esta presenta la interfaz de trabajo del usuario con que vaya a trabajar.

Archie. Es una base de datos que se ejecuta en algunas computadoras, las cuales almacenan listas de software o otros datos que están disponibles por medio de FTP anónimo.

Autentificación. Es el proceso que determina la identidad de un usuario que intenta accesar a un sistema en particular.

Autorización. Es un proceso que determina qué tipo de actividades son permitidas, relacionada con la autentificación es el hecho de que si es un usuario autentificado, se pueden autorizar diferentes tipos de acceso o actividad que va a depender del las políticas vigentes en la organización.

Backbone. Es el término genérico que sirve para distinguir la de alguna LAN o WAN entre subredes conectividad a través de la organización. Es el medio principal que conecta a los nodos de una red, es decir es un segmento de red que comparten varios concentradores, ruteadores etc. de una LAN.

Baudio. Es una unidad de velocidad de transmisión. Es el número de eventos de señales por segundo, el cual es medido en bits.

Broadcast. Es un paquete generado y enviado a todas las estaciones de una red.

Checksum. Es un valor computado que va a depender del contenido de un paquete, el cual es enviado junto cuando se transmite el paquete. Los sistemas receptores computan un nuevo chekcsum basándose en datos recibidos y lo comprara con la información que es enviada. Si los dos valores son iguales, el dato fue recibido de manera correcta.

Chroot. Técnica de UNIX que determina si un proceso es restringido permanentemente a una subdirectorio aparte del filesystem.

CSMA/CD, Carrier Sense Multiple Access/Collision Detection. Es un conjunto de reglas que determinan cómo los dispositivos de red respondan cuando dos dispositivos intentan usar al mismo tiempo un canal de datos (colisión). Cuando lo detecta, detiene los intentos de transmisión de los dispositivos. Cada dispositivo se le asigna un tiempo de retardo aleatorio con el cual el dispositivo intenta transmitir de nuevo.

DHCP, Dynamic Host Configuration Protocol. Sirve para asignar direcciones IP dinámicas a los dispositivos de una red, además puede tener una dirección IP diferente cada vez que se conecte a la red o puede cambiar mientras esta conectado el dispositivo. Ofrece un soporte para direcciones IP de tipo dinámica y estática. Este tipo de direcciones dinámicas es empleado por Proveedores de Acceso a Internet para asignar una dirección IP a las conexiones diales.

DMZ, DeMilitarized Zone. Es un término para describir un perímetro de defensa de red que puede ser utilizado en una Intranet o en un firewall de subred protegida.

DNS, Domain Name Server. Es un servicio distribuido de directorios jerárquico, usado para comparar direcciones numéricas (IP) con las direcciones alfanuméricas, es utilizado por el UDP y el TCP.

Dominio (Domain). Indica una subdivisión de los hosts de una red, esta puede ser física (LAN en locales diferentes) o lógicos (en donde el host se encuentra en un área administrativa particular con su propio nombre del grupo aunque se encuentren en la misma red).

Finger. Servicio que puede encontrarse disponible en algunos hosts de Internet, muestra información acerca de los usuarios de un host en particular a cualquiera que lo ejecute.

FTP, File Transference Protocol. Es una aplicación cliente /servidor que es usada para transferir archivos entre hosts por medio de conexiones TCP. El FTP anónimo es la configuración de un servidor FTP para dar acceso público a una determinada área en donde se encuentre información y en donde no es necesario tener una cuenta para accesar al servidor.

Gopher. Es un protocolo TCP que permite al usuario ejecutar un servidor Gopher para publicar información al resto de Internet.

HTTP, HyperText Transport Protocol. Protocolo TCP usado para transferir documentos por medio de hipertexto a través del World Wide Web.

ICMP, Internet Control Message Protocol. Es un protocolo de red que se ejecuta al lado del IP, es usado para guiar las conexiones de red, reportar los errores y las desconexiones de la red y prevenir que el tráfico fluya a través de enlaces de red lentos.

Interceptor vampiro, (Vampire Tap). Es un ataque al hardware que redirige una porción de la red.

Intranet, Es una red TPC/IP privada que emplea la arquitectura y los servicios parecidos a Internet.

IP, Internet Protocol. Es un protocolo de bajo nivel que conecta los paquetes de host a host, es el estándar de las comunicaciones entre los diversos sitios de Internet.

IRC, Internet Relay Chat. Es un sistema distribuido TCP en donde los usuarios con ayuda de un cliente se conectan a un servidor en donde se establece una plática (chat) de cualquier tipo.

Kernel. Son módulos y rutinas internas de bajo nivel en un sistema operativo, algunas veces el firewall es integrado al kernel de un sistema operativo.

MAC, Media Access Control. Es la vía de acceso que obtienen las estaciones de trabajo para poder transmitir. Un MAC Address es la dirección física de un dispositivo conectado a un medio compartido.

MIME, Multipurpose Internet Mail Extensions. Es el estándar multimedia para los sistemas de correo; ofrece soporte de audio, video y gráficos que pueden ser enviados usando las características MIME. Fue desarrollado en 1992 por el Internet Engineering Task Force (IETF).

Motif. Es una interfaz gráfica de usuario la cuál es un estándar en más de 200 plataformas de software y hardware, fue desarrollado por OSF (Open Software Foundation) en 1989 que especifica una serie de lineamientos para desarrollar una aplicación de X Window.

NIS, Network Information Service. Es un software de base de datos distribuido, es usado para distribuir en UNIX el password, los grupos y la información de la red a diversos hosts de una red, en un ambiente de campus.

NFS. Network File System. Es un protocolo RPC con el cual se pueden compartir archivos de un servidor a otro, por medio de la dirección IP.

Paquete (packet). Es la unidad básica de transmisión de datos en un ambiente de red como el TCP/IP.

Política. Son normas de la organización para el uso aceptable de los recursos computacionales, prácticas de seguridad y procedimientos operacionales.

POP, Post Office Protocol. Protocolo tipo TCP con el cual se puede enviar correo electrónico hacia o desde una PC.

RIP, Routing Information Protocol. Es un protocolo UDP que es usado por los hosts y los ruteadores para intercambiar y mantener las tablas de las rutas (en donde se tiene una descripción de la mejor ruta que el tráfico podrá tomar a través de la red).

RPC, Remote Procedure Call. Es una librería que contiene rutinas que permite a los programadores crear aplicaciones con las cuales se trabaje en un ambiente distribuido.

Las aplicaciones RPC utilizan el TCP o "UDP para transferir los datos a un servicio que se ejecuta en un host remoto; el servicio procesa el dato y regresa el resultado al usuario. El NFS es un ejemplo de esto.

RFC, Request For Comments. Es una serie de documentos de Internet que han sido usados para promover y difundir las tecnologías de Internet, estándares y procedimientos.

Ruteo (Routing). Es el proceso de distribuir un mensaje a través de alguna red o redes por la ruta más adecuada.

SMTP, Simple Mail Transfer Protocol. Protocolo TCP el cual es usado para transmitir correo electrónico entre los diferentes sitios de Internet.

SUID, Set UID; SGID, Set GID. La mayoría de los usuarios en UNIX tienen pocos privilegios, pero necesitan completar sus tareas con ayuda de programas que tienen privilegios de otro dueño o de otro grupo; para esto, UNIX asigna los privilegios de otro usuario a diversos programas, los procesos resultantes cuando se ejecutan pueden asumir otro UID (Identificador de usuario) u otro GID (identificador de grupo). Un programa que cambie su identificador de usuario es conocido como programa SUID así como programa SGID si cambia su identificador de grupo.

TCP, Transmition Control Protocol. Es un protocolo de comunicaciones virtuales, localizado arriba de la capa del IP, es usado para ofrecer seguridad y unicidad a las comunicaciones que hay entre los hosts que se encuentren conectados a Internet.

Telnet. Protocolo TCP de terminal virtual, despliega un acceso interactivo hacia una terminal remota a través de Internet, como si se conectase por medio de una línea serial.

TFTP, Trivial File Transfer Protocol. Es un protocolo de transferencia de archivos UDP, es usado para configurar la inicialización de estaciones de trabajo o terminales tontas, no es muy usado debido a que transmite los archivos a cualquier usuario que haga la petición de este servicio.

UDP, User Datagram Protocol. Es un servicio localizado sobre la capa del IP, ofrece un resumen de datos y un número de puerto de aplicación para algunos servicios básicos de IP.

Bajo el tráfico TCP, cada paquete UDP pasa y llega a su destino sin ningún proceso adicional, esta cualidad es la que hace que el tráfico UDP sea considerado como riesgoso.

WAN, Wide Area Network. Es una red que esta distribuida en una gran área geográfica.

WWW, World Wide Web. Es un sistema de hipertexto de Internet en el cual el acceso público a los demonios de hipertexto puede esperar usando el protocolo HTTP, en donde se regresan los resultados de las peticiones de información o servicios al usuario.

Índice de figuras

Figura.	Nombre de la figura.	página
Fig. 1.	Topología de bus.	4
Fig. 2.	Topología de estrella.	5
Fig. 3.	Topología de anillo.	5
Fig. 4.	Topología de árbol.	5
Fig. 5.	Consideraciones importantes de tecnologías de punta en especificaciones de red.	9
Fig. 6.	Capas del modelo OSI.	10
Fig. 7.	Estructura de los servicios del protocolo TCP/IP.	15
Fig. 8.	Tipos de direcciones IP.	17
Fig. 9.	Opciones del comando runtime.	19
Fig. 10.	Opciones del comando finger.	20
Fig. 11.	Opciones del comando traceroute.	21
Fig. 12.	Opciones del comando arp.	22
Fig. 13.	Tipos de hackers.	35
Fig. 14.	Cuestionamientos de una buena política de seguridad.	53
Fig. 15.	Pasos para autentificar a un usuario.	54
Fig. 16.	Filtrado de paquetes.	55
Fig. 17.	Aplicaciones gateway.	58
Fig. 18.	Ventajas y desventajas de los servicios proxy.	59
Fig. 19.	Consideraciones importantes del puente y del ruteador.	61
Fig. 20.	Firewall de host protegido.	67
Fig. 21.	Firewall de subred protegida.	69
Fig. 22.	Modem en un firewall de host protegido.	70
Fig. 23.	Modem en un firewall de subred protegida.	71
Fig. 24.	Ejemplos de pruebas para comprobar el funcionamiento de un firewall.	81
Fig. 25.	Gateways proxy Vs. filtrado de paquetes.	86
Fig. 26.	Características generales de Tripwire.	88
Fig. 27.	Características predeterminadas del software Tripwire.	88
Fig. 28.	Características de un firewall.	93
Fig. 29.	Procedimientos al identificar un evento en el firewall.	95
Fig. 30.	Ejemplos de redes extraseguras.	98
Fig. 31.	Ventajas y desventajas de diferentes tipos de adquisición de un firewall.	99
Fig. 32.	Características adicionales de los firewalls comerciales.	100
Fig. 33.	Red original (ejemplo).	108
Fig. 34.	Configuración final de la red (ejemplo).	110

Bibliografía

[1] http://www.sandybay.com/pc-web/
Enciclopedia en Internet

[2] Ranum, Marcus (Mc Graw Hill Co.); **"Open Computing 'Hands-On' Tutorial: September 1994, Internet Firewall Protection"**;
http://www.wcmh.com/uworld/archives/94/tutorial/09.txt.html

[3] a) Gavin, Peter; **"Tecnologías y métodos de firewall"**; E.U.; diciembre 1995; http://www.Sun.COM/sunworldonline/swol-12-1995/swol-12-security.html

[4] b) Gavin, Peter; **"Re-tooling?, The tools you need and the price is right"**; E.U.; octubre,1995;
http://www.Sun.COM/sunworldonline/swol-10-1995/swol-10-security.html

[5] Marcus J. Ranum; "**Internet firewalls Frequently Asked Questions**"
http://www.cis.ohio-state.edu/hypertext/faq/usenet/firewalls-faq/faq.html

[6] Madron Thomas William; **"Network Security in the 90's: issues and solutions for managers"**; Ed John Wilen NY, E.U.; 1992.

[7] Baker Richard H.; **"Network security: How to plan for it and archieve it"**; Mc Graw Hill N.Y. E.U. 1996.

[8] Karanjit Siyan y Chris Hare; **"Internet y seguridad en redes"**; Pretince Hall Hispanoamericana; *México, D.F.; 1995, 1997.*

[9] Black, Uyless; **"Redes de computadoras, protocolos, normas e interfaces"**; Ed. Macrobit; Madrid, España; 1987.

[10] Black, Uyless; **"Data communications and distributed networks"**; 3a edición; Ed. Pretince Hall; E.U.;1993.

[11] Glass, Graham; **"UNIX for programmers and users, A complete guide"**; Ed. Pretince Hall; E.U.; 1993.

[12] Stoltz, Kevin; **"Todo acerca de ... Redes de computación"**; Ed. Pretince Hall; México; 1994.

[13] Amoroso, Edward y Sharp, Ronald; **"PCweek Intranet and Internet Firewall Strategies"**; Ed Ziff-Davis Press; 1996.

[14] Richardson, Michael C; **"Rating Of Application layer proxies Document number: AT-0008, Rev. 2"**; 1996; Canadá http://www.sandelman.ottawa.on.ca/SSW/proxyrating/proxyrating.html

[15] ODwyer, Frank; **"Local Client/Server Firewalls"**; 1997; http://www.brd.ie/papers/splitfire/splitfire.html

[16] Trusted Information Systems; **"Firewall Papers"**; EU; 1997 http://www.tis.com/docs/products/gauntlet/papers.html

[17] Trusted Information Systems; **"A Toolkit and Methods for Internet Firewalls"**; EU.; 1997; http://www.tis.com/docs/products/gauntlet/Usenix.html

[18] Lodin, Steve (Proyecto COAST); **"COAST Hotlist - Internet Firewalls"**; EU; 1997; http://www.cs.purdue.edu/coast/firewalls/

[19] Wack, John P y Carnahan Lisa J.; **"Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls"**; NIST (National Institute of Standards and Technology) Publicación especial 800-10, Departamento de Comercio de los E.U; 1995; http://www.telstra.com.au/pub/docs/security/800-10/main.html

[20] Carleton, Les; **"Rotherwall: Freeware and Shareware Firewalls"**; Inglaterra; http://www.zeuros.co.uk/firewall/freeware.htm y **"The Rotherwick Firewall Resource - Point of Attack"** http://www.zeuros.co.uk/firewall/

[21] Stang, David J; **"Cheyenne Security Center"**; E.U.; 1997. http://www.cheyenne.com/security/thr&firw.html

[22] Molitor, Andrew; **"Firewall Performance"**; E.U. http://www.clark.net/pub/mjr/pubs/fwperf/molitor.htm

[23] National Computer Security Asociation; **"NCSA Firewall Policy Guide V 2.00"**; E.U.; 1997; http://www.ncsa.com/fpfs/fwpg.html

[24] ISS; **"ISS Security Library"**; E.U.; 1997; http://www.iss.net/vd/checklist.html

[25] **"Wieste's collection of tools and papers"**; Holanda; 1997 ftp://ftp.win.tue.nl/pub/security/index.html#software

[26] Open Horizon; **"Security Process: Threats"**; E.U.; 1997. http://www.securityinfo.com/threats.html

[27] **"IP Security Protocol (ipsec) Charter"**; EU; 1997. http://www.ietf.cnri.reston.va.us/html.charters/ipsec-charter.html

[28] **"The Private Communication Technology (PCT) Protocol"**; E.U.; 1997. http://www.graphcomp.com/info/specs/ms/pct.htm

[29] **"Simple Key-Management for Internet Protocol (SKIP)"**; E.U.; 1997. http://www.isoc.org/HMP/PAPER/244/

[30] C. Gavin, Peter; (SunWorld Online) ; **"Extinguishing firewall hyperbole"**; E.U.; Enero 1997. http://www.sun.com/sunworldonline/swol-01-1997/swol-01-security.html

[31] D. Gavin, Peter; (SunWorld Online); **"Distinguish firewall hype"**; E. U. Diciembre 1996. http://www.Sun.COM/sunworldonline/swol-12-1996/swol-12-security.html

[32] E. Peter Gavin (SunWorld Online); **"Watch Your Back Door"**; E.U.; Diciembre 1995; http://www.Sun.COM/sunworldonline/swol-12-1995/swol-12-security.html

[33] F. Chapman, Brent y Zwicky, Elizabeth (SunWorld Online); **"Firewall desing"**; E.U.; enero, 1996. http://www.Sun.COM:80/sunworldonline/ swol-12-1995/swol-12-security.html

[34] G. Peter Galvin(SunWorld Online); **"Avoid firewall pitfalls"**; E.U.; Junio 1997. http://www.Sun.COM/sunworldonline/swol-06-1997/swol-06-security.html

[35] Kris Jamsa, Ken Cope **"Programación en Internet"**; Ed Mc Graw Hill; 1996; México D.F.

[36] Mustafa, Javed Newell Thomas y Therthem Richard; **"The easy Internet Handbook"**; Ed. Hi Willow Research & Publishing; 1994.

[37] Ayuda en línea de Solaris (man, answerbook); UNIX Basic Administration; Sun Microsystems; E.U.; 1995.

[38] Stang, David J & Moon, Sylvia; **"Network Security Secrets"**; Ed. IDG Books; E.U.; 1993.

[39] Camacho Lara, Sylvia R; **"Aspectos fundamentales en la estructuración de un ambiente de seguridad en cómputo"**; Memorias del Día Internacional de la Seguridad en Cómputo; Cd. Universitaria México D.F.; 29 de noviembre de 1996; pp 99.

[40] Avila Castañeda, Sergio; "**Seguridad básica**"; Seminario de GASU; 6 de abril de 1997; Cd. Universitaria, UNAM; México D.F.

[41] Cisco Systems Inc; **"OSI Protocols"**; E.U.; 1996; http://www.cisco.com/univerdc/data/doc/cintrnet/ito/55165.htm#HDR11

[42] 3Com Technical Papers; **"Internet Firewalls and Security"**; E.U.; 1996; http://www.3com.com

[43] XYLAN; **"The Switching book"**; XYLAN; E.U.; 1996.

[44] Garfinkel & Spafford; **"Practical UNIX & Internet Securiry"**; Ed. O'Reilly; Segunda edición; E.U.; 1996.

[45] LANNET; **"Migrating to multi-layer Switched Networks"**; Apuntes de Conferencia.

Todos las investigaciones fueron hechas para fines educativos y demostrativos, no se persigue ningún tipo de lucro con el desarrollo de este trabajo.

*View this article in its entirety at:
A) http://www.sunworld.com/swol-12-1995/swol-12-security.html
B) http://www.sunworld.com/swol-10-1995/swol-10-security.html
C) http://www.sunworld.com/swol-01-1997/swol-01-security.html
D) http://www.sunworld.com/swol-12-1996/swol-12-security.html
E) http://www.sunworld.com/swol-12-1995/swol-12-security.html
F) http://www.sunworld.com/swol-12-1995/swol-12-security.html
G) http://www.sunworld.com/swol-06-1997/swol-06-security.html