CAPITULO IV

4	FIREWALLS
4.1	Introducción
4.2	Objetivos de los firewalls
4.3	Beneficios de un firewall
4.4	Limitaciones de un firewall
4.5	Firewalls de software y hardware
4.5.1	Firewalls de software
4.5.2	Firewalls de hardware
4.6	Clases de firewalls por tipos
4.6.1	Basados en filtrado de paquetes
4.6.1.1	Beneficios del filtrado de paquetes
4.6.1.2	Limitaciones del filtrado de paquetes
4.6.2	Basados en proxies
4.6.2.1.	Como funcionan los servicios proxy
4.6.2.2.	Beneficios de los proxies
4.6.2.3	Limitaciones de los proxies
4.6.3	Con transparencia
4.7	Arquitecturas de firewalls
4.7.1	Arquitectura de anfitrión con doble acceso
4.7.2	Arquitectura de anfitrión de protección
4.7.3	Arquitectura de subred de protección
4.8	Aspectos básicos para el diseño de un firewall
4.8.1	Postura sobre la política del firewall
4.8.2	Política interna de seguridad
4.8.3	Costo del firewall
4.8.4	Componentes de un firewall
4.9	Instalación y administración de un firewall
4.10	Mantenimiento del firewall
4.10.1	Mantenimiento
4.10.2	Monitoreo del sistema
4.10.3	Actualización

CAPITULO IV

4. FIREWALLS

4.1 INTRODUCCIÓN

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

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

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre una organización privada

y el Internet; el firewall determina cuales servicios de red pueden ser accesados por usuarios externos, es decir quien puede ingresar y utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información hacia el Internet, deberá pasar a través del cortafuego y este autorizará o denegará el flujo de información; el firewall podrá ser inmune a la penetración, pero desafortunadamente, este sistema no pude ofrecer protección alguna una vez que el agresor supere la protección.

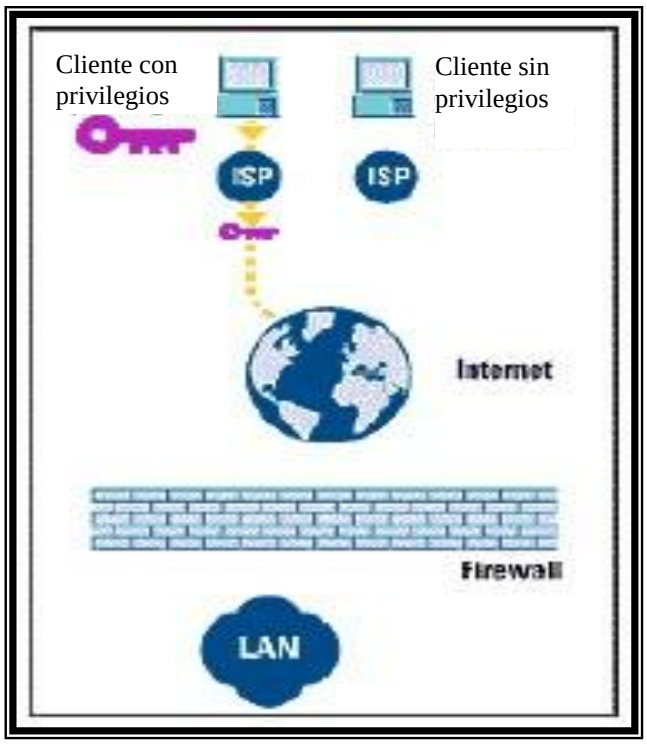

Fig. 4.01 Firewall

Esto es importante, ya que se debe notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa o una combinación de elementos que proveen seguridad para la red, el firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los

usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dialup, reglas de encriptación de datos y discos, normas de protección de virus y entrenamiento; todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

4.2 OBJETIVOS DE LOS FIREWALLS

Los firewalls son diseñados para alcanzar diferentes objetivos de seguridad, entre estos se pueden mencionar los siguientes:

1. Restringir la entrada a usuarios a puntos cuidadosamente controlados.

2. Ser un punto de decisiones de seguridad, porque todo el tráfico pasa a través de un único punto de chequeo.

3. Exigir políticas de seguridad, debido a que controla que servicios están habilitados para el uso de los clientes de la red.

4. Registrar la actividad en Internet, ya que provee una buena forma de recolectar las actividades que pasan entre la red interna e internet.

5. Limitar la exposición de la red interna protegiendo una sección de la red de la organización.

6. Reducir los costos que pueden implicar la implantación de otro tipo de medidas de seguridad.

7. Proteger de amenazas conocidas, debido a que estas siempre están presentes y en muchos casos ocasionan problemas difíciles de controlar.

4.3 BENEFICIOS DE UN FIREWALL

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

El firewall permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no autorizados (tales como: hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles.

Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran la red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa este generara una alarma ante la posibilidad de que ocurra un ataque o suceda algún problema en el tránsito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque, esto es

extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall.

Si el administrador de la red se toma el tiempo necesario para responder una alarma y examina regularmente los registros de base, se tendrá la seguridad de que se evitará un ataque o por lo menos se sabrá el momento exacto en que un intruso ingresó a la red y se logrará disminuir los terribles daños, que en último caso podrían causar a la organización.

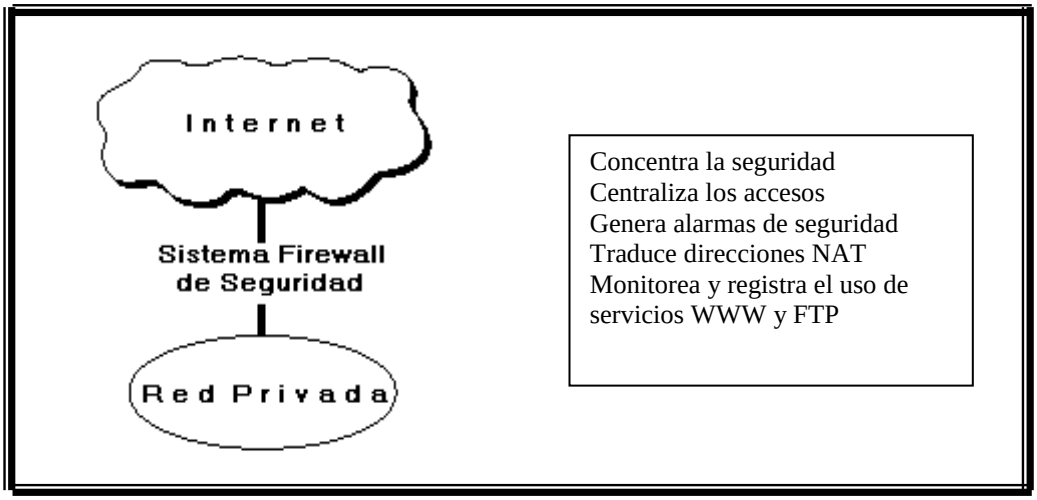

Fig. 4.02 Que hace un firewall

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

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

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

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

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

4.4 LIMITACIONES DE UN FIREWALL

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

Por ejemplo, si existe una conexión dial-up sin restricciones que permita la entrada a la red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se solicita una autenticación adicional

requerida por un Firewall Proxy, lo cual se puede ser provocado por un sistema de seguridad circunvecino que está incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones debilitan la seguridad provista por el firewall construido cuidadosamente para proteger la red interna, los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

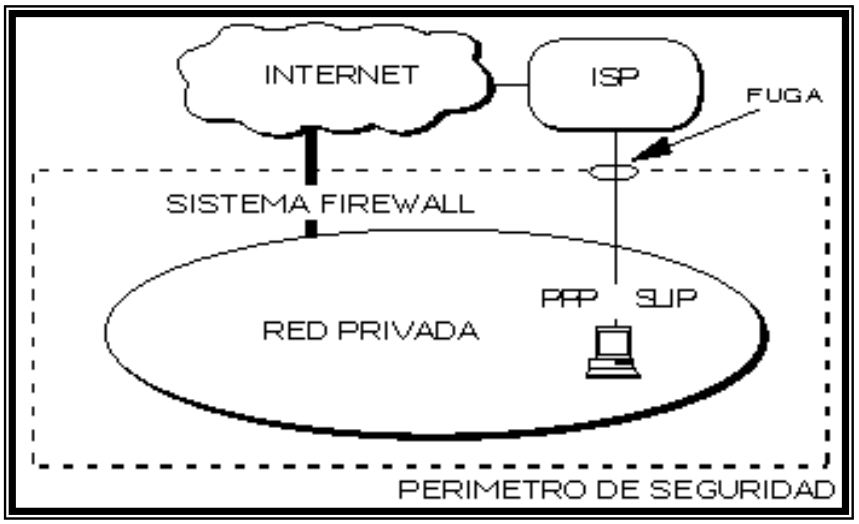

Fig. 4.03 Que no hace un firewall

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

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

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

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

La solución real está en que la organización debe ser consciente e instalar software antivirus en cada equipo para protegerse de los virus que llegan por medio de disquettes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados, despachando un ataque; por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

4.5 FIREWALLS DE SOFTWARE Y HARDWARE

Como se mencionó anteriormente un firewall puede proteger la red interna de los peligros que se presentan el momento de conectarse con el Internet. Estos protectores de red se implementan básicamente de dos maneras que son:

4.5.1 Firewalls de software

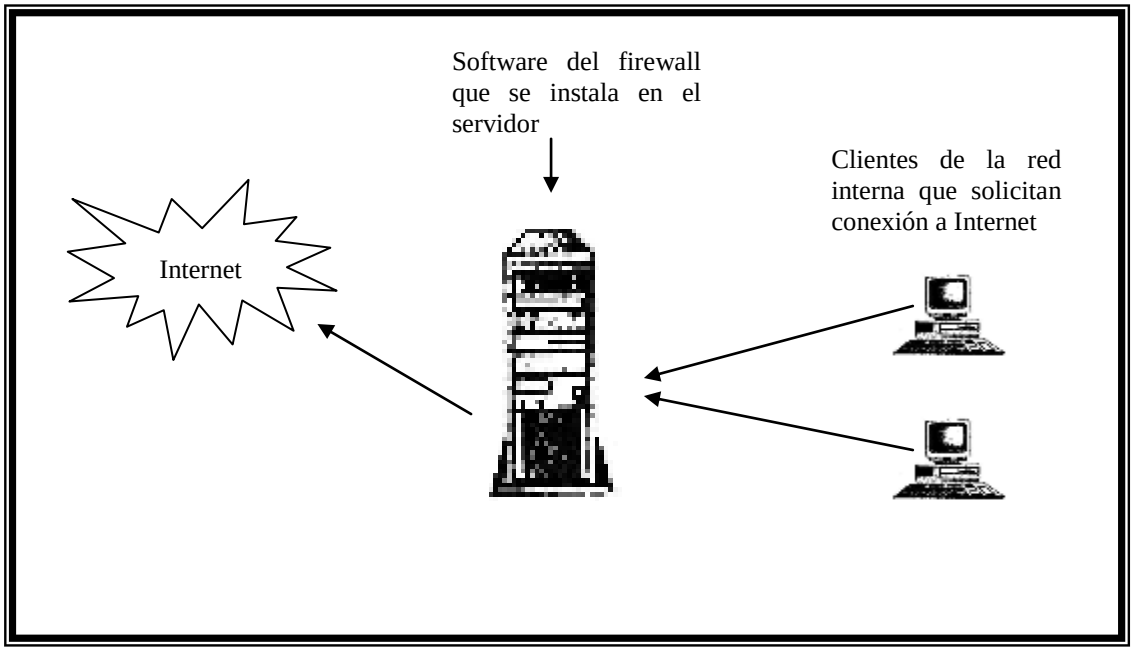

Fig. 4.04 Firewall de software

Un firewall de software es un simple programa que se carga en un computador y su función principal es interceptar todas las conexiones de red, tanto de entrada como de salida.

Los firewalls de software en ciertas ocasiones son simples de instalar pues no se necesita tener mayor conocimiento, generalmente se instala como cualquier otra aplicación estándar que existe en el mercado hoy en día; obviamente esto depende del firewall que se vaya a instalar, pues existen algunos programas que son bastante complicados tanto para instalar como para configurar y poner en funcionamiento el firewall.

Este tipo de aplicaciones generalmente son específicas para una versión de sistema operativo, lo cual los hace muy limitados, pues en el caso de desear en algún momento cambiarse de plataforma debido a los cambios de la tecnología, es complicado adquirir una nueva versión del programa para el sistema actual, debido a que las organizaciones encargadas del desarrollo de aplicaciones de este tipo pueden haber salido del mercado, lo cual obliga a cambiarse de producto, y sería necesario un nuevo aprendizaje del administrador para que adapte la nueva herramienta a las necesidades institucionales.

En algunas ocasiones si no se instala un firewall para red, es necesario instalar un firewall en cada una de las máquinas que se desea proteger, lo cual resulta muy costoso y además se necesitará trabajo adicional por parte del administrador tanto para la instalación como para el mantenimiento del programa.

Esta clase de software consume disco, memoria y recursos de CPU para su correcto funcionamiento, lo cual disminuye el rendimiento del computador en el cual se ejecuta el programa.

4.5.2 Firewalls de hardware

Fig. 4.05 Firewall de hardware

Un firewall de hardware es una pieza de hardware dedicada, la cual se ubica específicamente entre la conexión a internet y la red privada.

Esta clase de equipos proveen servicios adicionales como ruteo, NAT y muchos otros, que suelen ser complicados de implementarse a través de software.

Para su instalación no requieren de cambios en ningún computador de la red, no hay necesidad de preocuparse el momento que se decide cambiar de sistema operativo o actualizar una versión existente, no se realizan cambios cuando se añade o elimina software o hardware, no hay variaciones en el firewall cuando aparecen nuevos virus u otro tipo de software malicioso que ataca las redes y que no es función del firewall el detectarlos.

Este tipo de firewall es muy seguro pero tiene varias desventajas como el costo, pues suelen ser demasiado costosos y muy pocas veces están al alcance de cualquier persona, en este caso es necesario realizar un análisis para determinar si resulta conveniente una inversión tan costosa a cambio de obtener mayor seguridad para la red interna.

4.6 CLASES DE FIREWALLS POR TIPOS

Básicamente se conocen tres clases de firewalls:

Cada uno de estos tipos utiliza un método diferente para proteger la red, a continuación se detalla el funcionamiento de estos tres diferentes tipos.

4.6.1 Basados en filtrado de paquetes

El filtrado de paquetes es un mecanismo de seguridad de la red que funciona controlando que información puede fluir de y hacia una red. Un firewall basado en filtrado de paquetes examina las direcciones de los paquetes para determinar si el paquete debe pasar a la red local o se debe impedir el acceso.

Un paquete es la información que viaja a través del medio físico y que contiene la información a transmitir, la dirección IP del host emisor y la dirección IP del host receptor; los firewalls de este tipo utilizan esta información almacenada en los paquetes para controlar su acceso.

Los paquetes de datos transmitidos hacia Internet, pasarán a través de numerosos ruteadores a lo largo del camino, cada uno de los cuales toma la decisión de hacia donde dirigir el trabajo.

Los firewalls de filtrado de paquetes toman sus decisiones basándose en tablas de datos y reglas, por medio de filtros, por ejemplo, solo datos de una cierta dirección pueden pasar a través

del firewall, si el firewall puede generar un registro de accesos esto lo convierte en un valioso dispositivo de seguridad.

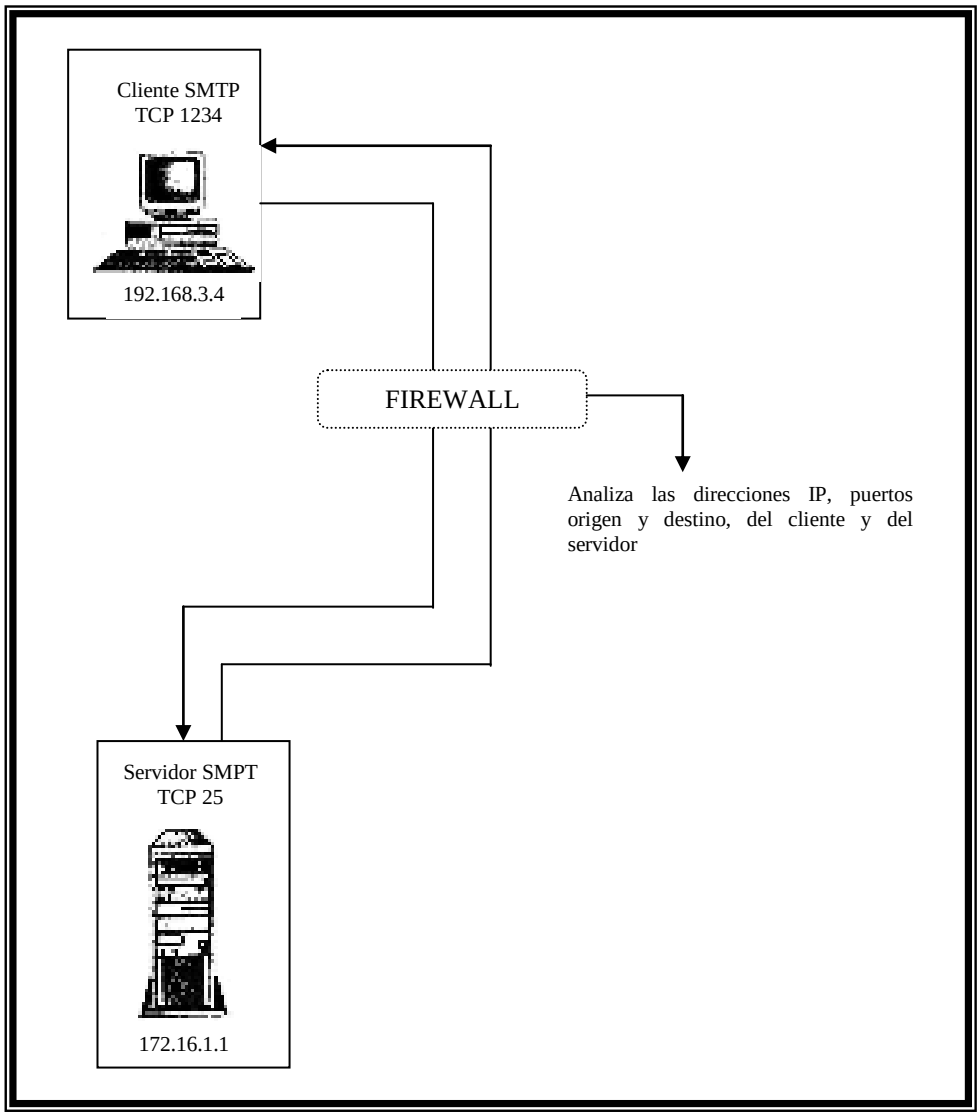

Fig. 4.06 Filtrado de paquetes SMTP de entrada

Si el servidor de Internet solicita información o bien la suministra hacia sistemas de bases de datos distribuidas, entonces esta conexión entre el servidor y la estación de trabajo debería ser protegida.

Un firewall filtrador de paquetes, usualmente puede filtrar paquetes IP con base en algunos o todos los criterios siguientes:

- dirección fuente IP,
- dirección destino IP,
- puerto fuente TCP/UDP, y
- Puerto destino TCP/UDP [Fig. 5.01 Pag. 270]

El filtrado puede bloquear conexiones desde o a las redes o anfitriones específicos y puede bloquear conexiones a puertos específicos. Un sitio podría desear bloquear las conexiones desde ciertas direcciones, tales como desde anfitriones o los sitios que consideraron hostiles o indignos de confianza. Alternativamente, un sitio puede desear bloquear conexiones desde todos las direcciones externas al sitio (con ciertas excepciones, tales como con SMTP para recibir e-mail).

Los servicios tales como telnet usualmente residen en puertos conocidos (puerto 23 para telnet), así si un firewall puede bloquear conexiones TCP o UDP a o desde puertos específicos, entonces el sitio puede hacer llamadas para asegurar los tipos de conexiones para ser hechas a ciertos anfitriones pero no a otros. Por ejemplo, una compañía podría desear bloquear todas las conexiones de entrada a todos los host a excepción de algunos sistemas conexos de firewall, a esos sistemas, quizás solo los servicios específicos serán permitidos, tal como SMTP para un sistema y conexiones telnet o FTP a otro sistema. Con filtrado sobre puertos TCP o UDP, esta política puede ser exitosa, en este estilo de firewall de filtrado de paquetes o un anfitrión con capacidad de filtrado de paquete.

Un ejemplo básico de filtrado de paquetes en telnet y SMTP pudiera ser permitir solo ciertas conexiones a una red de dirección 123.4.*.*. Las conexiones telnet serían permitidas a solo un host, 123.4.5.6, los cuales podrían ser una aplicación gateway en el sitio telnet, y las conexiones SMTP serían permitir a dos

hosts, 123.4.5.7 y 123.4.5.8, los cuales podrían ser dos sitios gateway e-mail, el firewall de filtrado de paquetes bloqueará cualquier otro servicio y paquete. Este ejemplo muy básico de filtrado de paquete puede volverse más complejo y flexible como el sitio fomente ajustes a las reglas de filtrado.

Desdichadamente, los firewalls de filtrado de paquetes no pueden hacer todo, ellos han sido tradicionalmente difíciles de usar en su configuración y mantenimiento, esto está cambiando, con los vendedores ya que están poniendo más atención a las interfaces.

Las reglas de filtrado de paquetes son inherentemente complejas para especificar y usualmente no existe facilidad de prueba para averiguar la corrección de las reglas (a excepción de la prueba exhaustiva por hand-see). Además, algunos firewalls no dan la capacidad para registrar (loggin), así que si las reglas de un firewall permiten paquetes peligrosos, los paquetes pueden no detectarse hasta que ocurra una caída del sistema. Los sitios que optan por usar firewalls de filtrado de paquetes deberán buscar uno que ofrezca registro (loggin) extensivo, una configuración simplificada y alguna forma de prueba de reglas.

Las excepciones a las reglas de filtración frecuentemente se necesitarán para permitir ciertos tipos de acceso que normalmente se bloquean, esas excepciones pueden hacer las reglas de filtración tan complejo como ser inmanejables. Por ejemplo, es relativamente directo la especificación de una regla para bloquear todas las conexiones encaminadas al puerto 23 (el servicio telnet), pero algunos sitios hacen excepciones para que ciertos sistemas especificados puedan aceptar conexiones telnet directamente, para hacer esto el administrador debe agregar una regla para cada sistema algunos sistemas de filtración de paquetes adjuntan la importancia a la orden secuencial de las reglas de filtrado, permitiendo al administrador poner una

excepción de permisos al sistema específico, seguido por una negación para todos los demás sistemas, la adición de ciertas reglas puede complicar el sistema entero de filtración. Algunos firewalls de filtración de paquetes no filtra en los puertos fuente TCP/UDP, el cual puede hacer el filtrado más complejo el conjunto de reglas y puede abrir hoyos en el esquema de filtración.

4.6.1.1 Beneficios del filtrado de paquetes

El filtrado de paquetes tiene una serie de ventajas, entre las cuales se pueden mencionar las siguientes:

a) Un enrutador de protección puede ayudar a proteger toda una red

Una de las ventajas clave del filtrado de paquetes es que en un solo enrutador con filtrado de paquetes colocado estratégicamente puede ayudar a proteger toda una red. Si sólo hay un enrutador que conecta toda la red interna, se logra una enorme ventaja de seguridad de la red, sin importar el tamaño de la misma al hacer el filtrado de paquetes en ese enrutador.

b) El filtrado de paquetes no necesita conocimiento o cooperación del usuario

El filtrado de paquetes no necesita ningún programa o configuración especial de las máquinas cliente, ni necesita algún adiestramiento especial o procedimiento por parte de los usuarios, lo ideal es que los usuarios ni siquiera se percaten de que está presente, a menos que intente hacer algo prohibido por la política de filtrado.

Esta transparencia quiere decir que el filtrado de paquetes puede hacerse sin la cooperación y con frecuencia sin el conocimiento de los usuarios, lo importante es que se puede hacer el filtrado de paquetes sin que ellos necesiten aprender algo nuevo para que funcione y sin la necesidad de depender de que ellos hagan (o no) algo para que funcione.

c) Muchos enrutadores disponen de filtrado de paquetes

Las capacidades de filtrado de paquetes están disponibles en muchos productos para enrutamiento de hardware y software, comerciales y/o disponibles gratuitamente en Internet. Muchos sitios ya cuentan con las capacidades de filtrado de paquetes en los enrutadores que usan.

4.6.1.2 Limitaciones del filtrado de paquetes

Aunque el filtrado de paquetes tiene muchas ventajas, existen algunas desventajas que se mencionan a continuación:

a) Las herramientas para filtrado de paquetes no son perfectas

A pesar de la amplia disponibilidad para filtrado de paquetes en varios productos de hardware y software, el filtrado aún no es un arma perfecta. En mayor o menor grado, la capacidad de filtrado de paquetes en muchos de estos productos comparten limitaciones comunes, entre las cuales se tienen:

- Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo.

- Las reglas para filtrado tienden a ser difíciles de configurar, si las necesidades de filtrado son muy complejas, se necesitará soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo más difícil su administración y comprensión.

- Una vez configuradas las reglas para filtrado de paquetes tienden a ser difíciles de probar, pudiéndose dejar una localidad abierta sin probar su vulnerabilidad.

- Las capacidades para filtrado de paquetes en muchos de los productos están incompletas, lo cual hace difícil o imposible la implementación de ciertos tipos de filtros sumamente deseables.

- Los programas para filtrado de paquetes pueden tener problemas, lo cuales son más propensos a convertirse en problemas de seguridad que los errores proxy. Por lo general, un proxy que falla simplemente deja de pasar información, mientras una falla de filtrado de paquetes podría permitir la entrada de paquetes que debieron rechazarse.

b) Algunas políticas no pueden aplicarse de inmediato por medio de enrutadores comunes con filtrado de paquetes

La información de que dispone un enrutador con filtrado de paquetes no permite especificar ciertas reglas que se pueden desear dentro de una organización. Por ejemplo, los paquetes dicen generalmente de que anfitrión viene pero no de que usuario, por eso no se puede aplicar restricciones a usuarios específicos. De modo similar, los paquetes muestran hacia qué puerto van pero no hacía que aplicación; cuando se aplican restricciones a los protocolos de nivel más alto, lo hace por el

número de puerto con la esperanza de que ningún otro programa esté ejecutándose en el puerto asignado a ese protocolo.

4.6.2 Basados en proxies

Un Servidor Proxy (algunas veces llamado "gateway" puerta de comunicación), es una aplicación que controla en tráfico que se produce en la red protegida e Internet. Un servidor proxy es un programa, que funciona normalmente como un servidor de seguridad y permite que varias máquinas conectadas a una misma red local puedan compartir un mismo acceso a Internet o conexión a Internet de manera simultánea.

Un servidor proxy proporciona a todos los clientes de la red local los mismos servicios que tendrían disponibles si estuviesen conectados directamente a través de un módem o tarjeta de red.

Los servicios proxy son una aplicación especializada o programas del servidor que se ejecutan en un equipo protegido por un firewall, dos interfaces de red, una para la red interna y otra para la red externa o algún servidor que sirve como bastión, el cual se encarga de realizar los accesos a Internet y permite el acceso a las máquinas de la red local. Estos programas toman las peticiones de los usuarios hacia el Internet (peticiones tales como FTP y telnet) y las mandan hacia afuera, de acuerdo a las políticas de cada sitio. Los proxy proveen regreso a su lugar de origen y actúan como puertas de enlace (gateway) de los servicios, por esta razón, los proxy son también conocidos como puertas de enlaces de nivel de aplicación.

La transparencia es el mayor beneficio de los servicios proxy, para el usuario un servidor proxy presenta la ilusión de que está tratando directamente con el servidor real, para el servidor real el

proxy presenta la ilusión de que éste trata directamente con un usuario que se encuentra dentro de una red privada.

El firewall basado en servicios proxy es un programa que trata con los servidores externos como intermediario por los clientes, los clientes del proxy solicitan dicho servicio a los servidores proxy y estos le contestan a los clientes con la aprobación o rechazo del servicio dependiendo de las políticas del sitio.

4.6.2.1 ¿Cómo funcionan los servicios proxy?

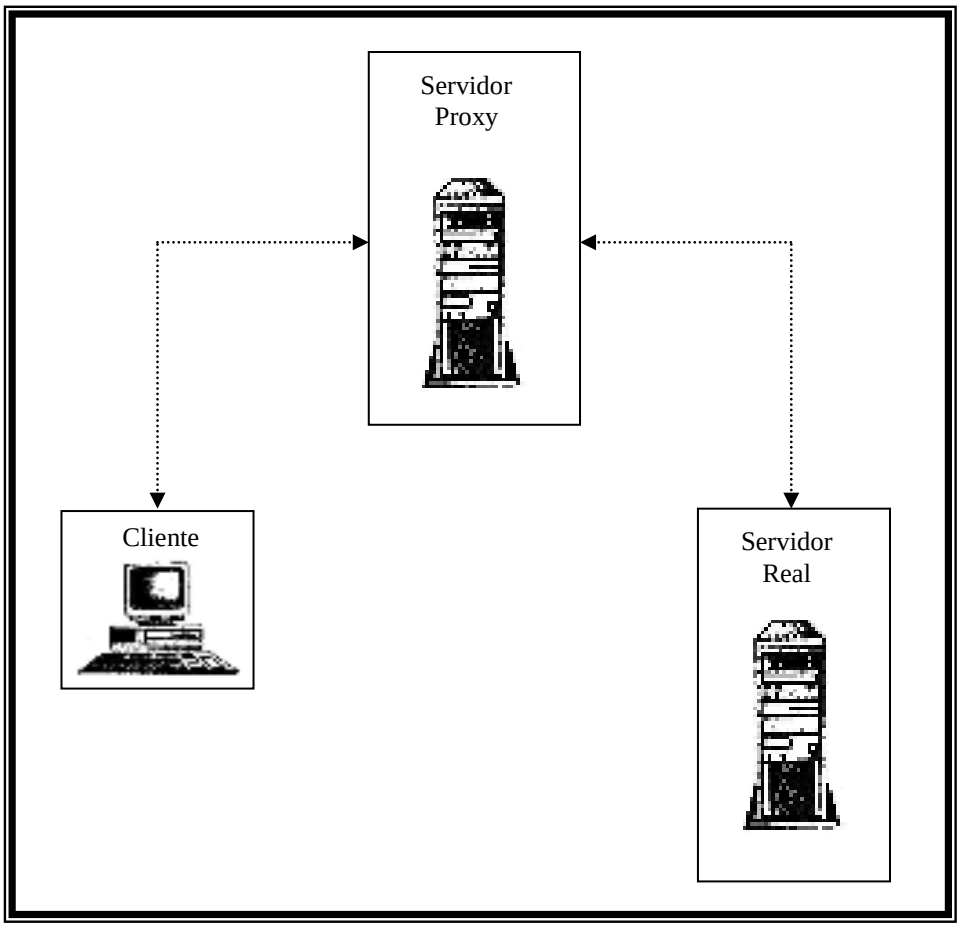

Fig. 4.07 Proxy: realidad e ilusión

Como se muestra en la figura 4.07 un servicio proxy requiere dos componentes: un cliente y un servidor. En la situación mostrada, el servidor proxy se ejecuta sobre un firewall del tipo "dual-homed". Un cliente proxy es una versión especial de un cliente normal de un programa (por ejemplo de un cliente de FTP o de

telnet) que habla con el servidor proxy en lugar de hablar con un servidor real dentro de Internet, los servidores proxy evalúan el requerimiento de los clientes y definen cual es autorizado y cual es denegado, si el requerimiento es aprobado el servidor proxy se conecta al servidor real y procede a regresar la respuesta al cliente proxy.

Un servicio proxy es una solución de software, no es una arquitectura firewall, por lo cual no es necesario contar con una arquitectura firewall para poder implementar un servidor proxy, sin embargo, estos son efectivos sólo cuando son usados en conjunto con algún método de restricción de tráfico entre los clientes y los servidores reales, tales como un screening router o un dual-homed host que no rutean paquetes.

Los servidores proxy pueden controlar lo que los usuarios hacen, dependiendo de las políticas de seguridad los requerimientos pueden ser permitidos o denegados

Los detalles de cómo trabaja proxy difieren de servicio a servicio. Algunos servicios proveen proxy fácil o automáticamente, para esos servicios, un proxy se instala al realizar cambios de configuración a los servidores normales; sin embargo, para la mayoría de los servicios la instalación de un proxy requiere de software apropiado para servidor proxy del lado servidor y, del lado cliente necesita uno de los siguiente componentes:

- Software cliente personalizado
- Procedimientos personalizados de usuario

Software cliente personalizado.- El software debe saber como contactar al servidor proxy en lugar de al servidor real cuando el usuario hace una solicitud (por ejemplo FTP o Telnet) y como

decirle al servidor proxy cual es el servidor real que debe contactar.

Procedimientos personalizados de usuario.- Los usuarios usan software estándar para hablar con el servidor proxy y decirle con que servidor real se debe conectar, en lugar de conectarse ellos directamente con el servidor real.

4.6.2.2 Beneficios de los proxies

Existen varias ventajas en el uso de servicios proxy:

a) Los servidores proxy permiten a los usuarios acceder a los servicios de Internet

Con los servicios proxy los usuarios creen que están comunicándose en forma directa con los servicios de Internet, aunque estos servicios proxy permiten a los usuarios el acceso a los servicios de Internet desde sus propios sistemas, lo hacen sin permitir que los paquetes pasen directamente entre el sistema del usuario e Internet.

b) Los servicios proxy son buenos para la contabilidad del sistema

Debido a que los servidores proxy comprenden el protocolo de niveles inferiores, permiten que se lleve la contabilidad del sistema de una forma muy efectiva. Por ejemplo, en lugar de registrar todos los datos transferidos, un servidor proxy FTP registra sólo los comandos emitidos y las respuestas recibidas del servidor; lo cual resulta en un registro mucho más pequeño y útil.

4.6.2.3 Limitaciones de los proxies

Los sistemas proxy también presentan algunas desventajas en su uso, entre estas se pueden mencionar las siguientes:

a) Los servicios proxy son más lentos que los servicios no proxy

Aunque los programas proxy están ampliamente disponibles para los servicios más viejos y simples, como FTP y Telnet, es más difícil encontrar software para servicios nuevos o poco comunes. Es usual que exista un rezago entre la introducción de un servicio y la disponibilidad de servidores proxy para él; esto dificulta que un sitio ofrezca nuevos servicio inmediatamente después de que estén disponibles. Hasta que no se disponga de un software proxy adecuado, un sistema que necesite nuevos servicios tal vez deba ponerse fuera del firewall, lo cual abre agujeros potenciales de seguridad.

b) Los servicios proxy podrían requerir servidores diferentes para cada servicio

Quizá se necesite un servidor proxy para cada protocolo, porque el servidor proxy debe comprender el protocolo para determinar qué permite y que no, y para hacerse pasar como cliente ante el verdadero servidor y como el verdadero servidor responde el cliente proxy. Coleccionar, instalar y configurar todos estos servidores puede requerir mucho trabajo.

c) Los servicios proxy por lo general requieren de modificaciones a los clientes, a los procedimientos o a ambos

Excepto por contados servicios diseñados para emplearse con proxy, los servidores proxy necesitan modificaciones a los clientes y/o procedimientos. Cualquier tipo de modificación tiene desventajas; las personas no siempre pueden utilizar las herramientas que están fácilmente disponibles con sus instrucciones normales.

Debido a estas modificaciones, las aplicaciones proxy no funcionan tan bien como aplicaciones no proxy, tienden a modificar las especificaciones de los protocolos y algunos clientes y servidores menos flexibles.

d) Los servicios proxy no funcionan para algunos servicios

Un servicio proxy depende de la habilidad para insertar el servidor proxy entre el cliente y el verdadero servidor, lo cual exige interacción relativamente directa entre los dos. Un servicio como talk, que tiene interacciones complicadas y desordenadas, quizá nunca pueda usarse como un servicio proxy.

e) Los servicio proxy no lo protegen de todas las debilidades de los protocolos

Como solución para la seguridad el uso de proxy depende de la habilidad para determinar qué operaciones son seguras en un protocolo, no todos los protocolos proporcionan formas fáciles de hacer esto. Por ejemplo el sistema X Windows provee un gran número de operaciones inseguras y esto dificulta el trabajo mientras se remueven las operaciones inseguras, el

proxy no puede comprender donde los datos inician y donde terminan y determinar si estos son peligrosos o no.

4.6.3 Con transparencia

Recientemente han aparecido en el mercado dispositivos que van un paso más allá en la tecnología de firewalls; se trata de los firewalls de tercera generación o transparentes. La característica primordial de estos sistemas es que admiten paquetes no destinados a ellos mismos, de forma similar a como lo hacen los routers, y en función de una serie de reglas y configuraciones, son capaces de arrancar los proxies correspondientes automáticamente y conectar con el destinatario inicial.

Aparentemente para el usuario, ha conectado con el servidor final, aunque realmente lo ha hecho con el proxy, que le devuelve los paquetes con dirección IP origen la del servidor final, esto implica que el programa cliente del usuario no requiere ningún tipo de configuración. En definitiva, se trata de firewalls basados en proxies, pero con apariencia y funcionalidad similar a los basados en filtrado de paquetes.

4.7 ARQUITECTURAS DE FIREWALLS

Existen diversas arquitecturas para construir firewalls, entre las más conocidas se tienen:

4.7.1 Arquitectura de anfitrión con doble acceso

Una arquitectura muy simple de firewall utiliza un Anfitrión con Doble Acceso, el cual es una computadora que cuenta con dos interfaces de red (tarjetas),cada una de las cuales está conectada a una red diferente. Tal host podría actuar como un ruteador entre las dos redes, sin embargo las funciones de ruteo son deshabilitadas cuando el anfitrión con doble acceso es usado como firewall.

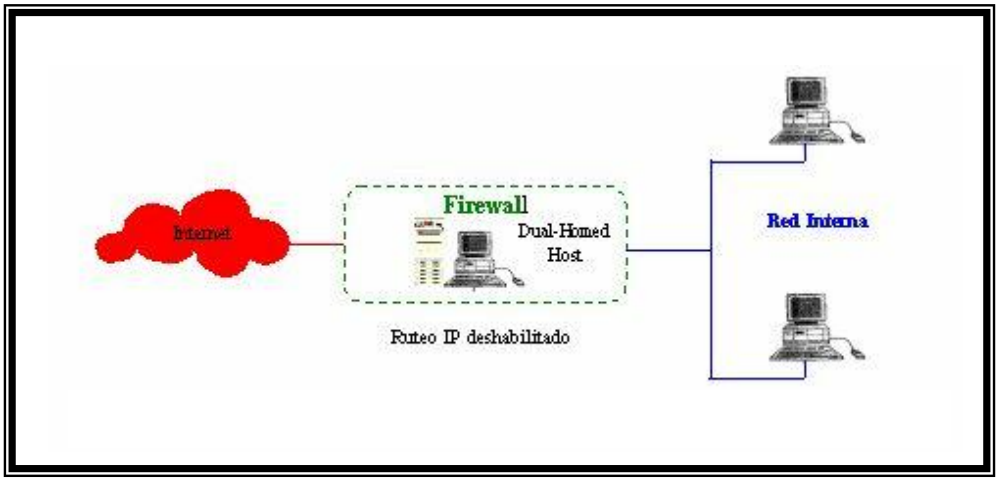

Fig. 4.08 Anfitrión con doble acceso

Debido a que las funciones de ruteo están deshabilitadas el host aísla las dos redes, mientras que posee la habilidad de ver el tráfico de ambas. Un sistema dentro de la red interna puede comunicarse con el anfitrión con doble acceso a través de una de las tarjetas, mientras que un sistema en Internet puede comunicarse a través de la otra tarjeta con el host, sin embargo ambos sistemas no pueden comunicarse directamente.

El anfitrión con doble acceso se puede utilizar para aislar una red interna de una red externa no confiable, debido a que el anfitrión con doble acceso no envía ningún tráfico de TCP/IP, bloquea completamente cualquier tráfico de IP entre la red interna y la red externa no confiable.

Los anfitriones con doble acceso pueden proporcionar un alto nivel de control, si no permiten que los paquetes pasen entre redes externas e internas, se puede tener la seguridad de que cualquier paquete en la red interna que tenga una fuente externa es evidencia de algún tipo de problema de seguridad. En algunos casos, un anfitrión con doble acceso permitirá que se rechacen conexiones que pretenden ser para un servicio específico pero que, en realidad no contienen el tipo correcto de dato.

Estos anfitriones con doble acceso generalmente utilizan servicios proxy para brindar acceso a los usuarios de la red interna.

4.7.2 Arquitectura de anfitrión de protección

Mientras una arquitectura con doble acceso proporciona servicios desde un anfitrión conectado a varias redes (pero con el enrutamiento desactivado), una arquitectura de anfitrión de protección proporciona servicios en un anfitrión conectado sólo a la red interna utilizando un enrutador independiente. En esta arquitectura, la seguridad principal la proporciona el filtrado de paquetes.

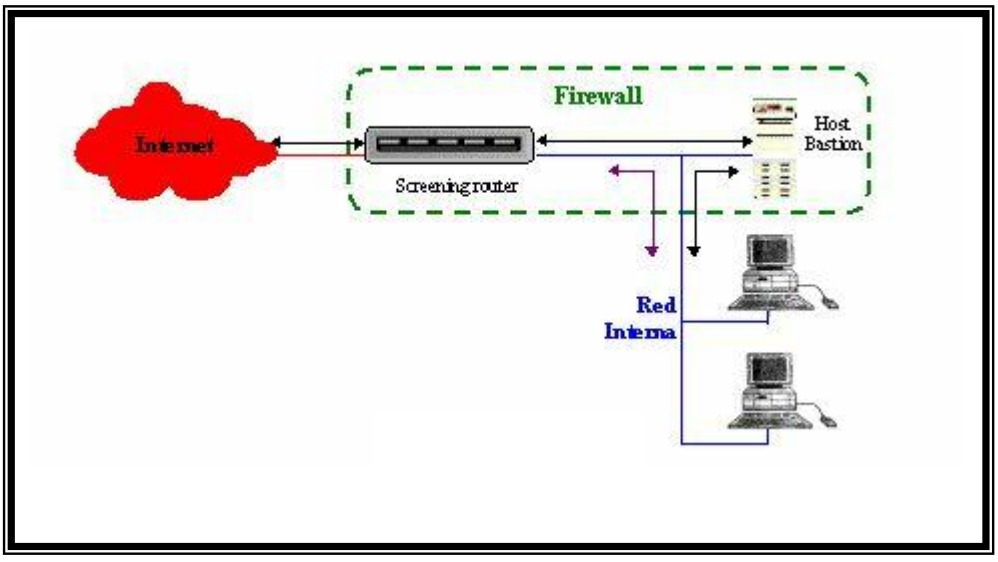

Fig. 4.09 Anfitrión de protección

El anfitrión bastión está colocado en la red interna; el filtrado de paquetes en el enrutador de protección está configurado de tal manera que el anfitrión bastión es el único sistema en la red interna con el que los anfitriones en Internet pueden abrir conexiones. Aún así, sólo están permitidas ciertos tipos de conexiones, cualquier sistema externo que intente tener acceso a los sistemas o servicios internos tendrá que conectarse con este anfitrión. Por lo tanto, el anfitrión bastión debe mantener un alto nivel de seguridad.

El filtrado de paquetes también permite que el anfitrión bastión abra conexiones permitidas al mundo exterior, dependiendo de la política de seguridad del sitio.

Las configuraciones para el filtrado de paquetes en el enrutador de protección puede hacer una de las siguientes tareas:

- Permitir que otros anfitriones internos abran conexiones con anfitriones en Internet para ciertos servicios.

- No permitir todas las conexiones de anfitriones internos.

Se puede mezclar e igualar estos enfoques para diferentes servicios; algunos pueden permitirse directamente por medio de filtrado de paquetes; otros pueden permitirse sólo de manera indirecta por medio de proxies, todo depende de la política específica del sitio.

Debido a que esta arquitectura permite que los paquetes se muevan de Internet a las redes internas, puede parecer más riesgoso que la arquitectura de anfitrión con doble acceso, diseñada para que ningún paquete externo alcance la red interna. Sin embargo, en la práctica, la arquitectura de anfitrión con doble acceso también es propensa a fallas que permiten que, en

realidad, pasen los paquetes de la red externa a la interna, debido a que esta clase de falla es inesperada, es poco probable que existan protecciones contra este tipo de ataques. Además, es más fácil defender un enrutador, que proporciona un conjunto muy limitado de servicios, que defender un anfitrión, para casi todos los propósitos, la arquitectura de anfitrión de protección proporciona mejor seguridad y mejor uso que la arquitectura de anfitrión con doble acceso.

Sin embargo, en comparación con otras arquitecturas, como la de subred de protección tiene algunas desventajas. La principal es que si un atacante logra penetrar el anfitrión bastión, no queda nada en la ruta de seguridad de la red entre ese anfitrión y el resto de anfitriones internos. El enrutador también presenta un solo punto de falla; si éste se halla en peligro, toda la red estará a merced de un atacante; por esta razón, la arquitectura de subred de protección se ha vuelto cada vez más popular.

4.7.3 Arquitectura de subred de protección

La arquitectura de subred de protección agrega una capa adicional de seguridad a la arquitectura de anfitrión de protección al añadir una red de perímetro que aisla aún más la red interna de Internet.

¿Por qué hacer esto? Por su naturaleza, los anfitriones bastión son las máquinas más vulnerables de la red, a pesar de hacer los mejores esfuerzos por protegerlos, son las máquinas que más probablemente sean atacadas. Si al igual que una arquitectura de protección, la red interna está totalmente abierta para ser atacada desde el anfitrión bastión, entonces éste es un blanco muy tentador, no hay otra defensa entre él y las máquinas internas. Al aislar al anfitrión bastión en una red de perímetro, se puede reducir el impacto de una entrada forzada a él.

Con la forma más sencilla de arquitectura de subred de protección, hay dos enrutadores de protección, uno conectado a la red de perímetro, no colocado entre la red de perímetro y la red interna, y el otro entre la red de perímetro y la red externa. Para entrar a la red interna con este tipo de arquitectura, un atacante tendría que penetrar ambos enrutadores; aunque logrará de alguna forma penetrar al anfitrión bastión, aún tendría que pasar al enrutador interno, no hay un punto vulnerable único que ponga en riesgo la red interna.

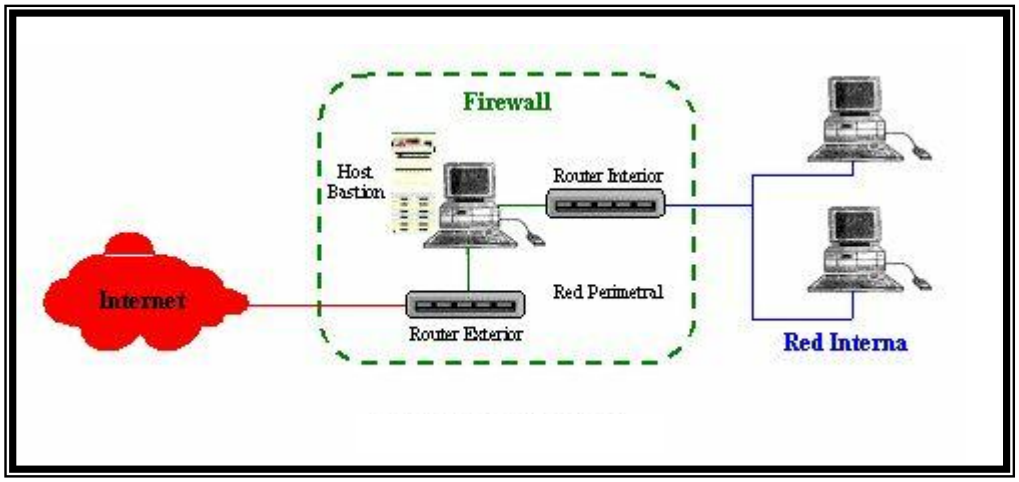

Fig. 4.10 Subred de protección

Algunos sitios van tan lejos como para crear una serie de capas de redes de perímetro entre el mundo exterior y su red interna. Los servicios menos confiables y más vulnerables se colocan en las redes de perímetro exteriores, más lejos de la red interior, la idea es que al atacante que penetre a una máquina en la red de perímetro exterior, le costará más trabajo atacar con éxito las máquinas internas debido a las capas adicionales de seguridad entre el perímetro exterior y la red interna. Sin embargo, esto es sólo cierto si las distintas capas tienen sentido; si los sistemas de filtrado entre cada capa permiten lo mismo entre todas las capas adicionales, las capas adicionales no proporcionan mayor seguridad.

4.8 ASPECTOS BÁSICOS PARA EL DISEÑO DE UN FIREWALL

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

4.8.1 Postura sobre la política del firewall.

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

- Postura de negación preestablecida: especifique sólo lo que permite y prohiba todo lo demás

- Postura de permiso preestablecido: especifique sólo lo que prohibe y permita todo lo demás

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

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

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso. Esta propuesta crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad - del sistema. Además, el administrador de la red está en la obligación de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

4.8.2 Política interna de la seguridad

Un firewall, el cual va a proteger una red interna de los peligros que se presentan el momento de conectarse a Internet, **"es parte de la política de seguridad total en una organización"**, la cual define todos los aspectos relacionados al perímetro de defensa.

Para que esta sea exitosa, la organización debe conocer que es lo se está protegiendo, la política de seguridad se basará en una conducción cuidadosa analizando la seguridad, la asesoría en caso de riesgo y la situación de la organización. Si no se posee información detallada de la política a seguir, aunque sea un

firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

Por lo tanto el primer paso a seguir en el establecimiento de la seguridad de una organización, es determinar la política de seguridad, debido a que el firewall únicamente será un complemento de todo el trabajo que se debe realizar para implementar la seguridad total.

4.8.3 Costo del firewall

Es importante intentar cuantificar y proponer soluciones en términos de cuanto cuesta comprar o implementar tal cosa u otra. Por ejemplo, un producto completo de firewall de red puede costar 10.000 dólares, pero este precio se trata de un firewall de altas prestaciones, a veces lo realmente necesario no es gastarse mucho dinero en un firewall muy potente, sino perder un poco de tiempo en evaluar las necesidades y encontrar un firewall que se adapte a la realidad de la organización.

En cuanto al asunto técnico, se debe tomar la decisión de colocar una máquina desprotegida en el exterior de la red para correr servicios proxy tales como telnet, ftp, news, etc., o bien colocar un router a modo de filtro, que permita comunicaciones con una o más máquinas internas.

Hay ventajas e inconvenientes en ambas opciones, con una máquina proxy se proporciona un gran nivel de auditoría y seguridad en cambio se incrementan los costos de configuración y disminuye el nivel de servicio que puede proporcionar

Finalmente es necesario analizar que se requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad e incidentes de

manejo y es conveniente realizar un estudio del costo que implicaría la contratación de personal capacitado para realizar este tipo de tareas.

Como se puede observar, el análisis del costo de la implementación de un firewall es muy importante, ya que de eso depende la seguridad de la organización; además la adquisición de un firewall debe constituirse en una inversión para la institución, ya que el gasto que implica la compra de este tipo de tecnología debe retribuirse a través de la seguridad y optimización de la conexión con Internet.

4.8.4 Componentes de un firewall

Los componentes para el diseño de un firewall van a depender del tipo de firewall que se decida implementar, estos se basarán en las necesidades que tenga la organización.

El primer punto de análisis será determinar si se desea un firewall de software o uno de hardware.

En el caso que se decida por un firewall de software es necesario realizar un estudio del lenguaje de programación que se utilizará para el desarrollo del mismo, pues hoy en día existen en el mercado una gran cantidad de programas que brindan grandes facilidades para el desarrollo de aplicaciones y no son muy costosos, incluso se pueden obtener gratuitamente a través de Internet.

Los firewalls de software también pueden adquirirse, no es necesario desarrollar uno, pero en el caso de que se decida la adquisición de uno de estos, es conveniente realizar un estudio a fondo, para de esta manera adquirir el que mejor protección brinde y que se adecue a las necesidades de la institución.

Si se decide por un firewall de hardware el estudio en este caso debe ser un poco más detallado, pues aquí es conveniente analizar la mayor cantidad de opciones posibles, para de esta manera adquirir el firewall que mejor seguridad brinde y que por supuesto no sea demasiado costoso, pues como se mencionó anteriormente un firewall de hardware es sumamente costoso y en muchos ocasiones no puede brindar las prestaciones que busca la organización.

Una vez que se ha escogido entre un firewall de software y uno de hardware, es momento de analizar el tipo de arquitectura que se empleará, como se indicó anteriormente existen tres arquitecturas básicas las mismas que tienen sus ventajas y desventajas, pero cada una de ellas brinda ciertas prestaciones con mayor seguridad y obviamente con un costo mayor debido a los requerimientos de hardware que se necesitan para armar cada una de estas, por lo tanto es necesario seleccionar una arquitectura de firewall de acuerdo a las capacidades económicas que tenga la institución.

En este momento es conveniente mencionar que en el mercado se pueden encontrar componentes económicos, pero que lamentablemente no prestan los servicios que se necesitan para construir una arquitectura firewall de buena calidad, por lo tanto el administrador de red en primer lugar deberá analizar las características técnicas de los componentes a adquirirse porque caso contrario no se estaría realizando una buena inversión y en el último de los casos sería conveniente no construir una arquitectura muy sofisticada, pero si una con elementos de buena calidad y que brinden la seguridad que se desea conseguir.

Finalmente dependiendo de la arquitectura y de si el firewall es de software o de hardware, el último punto de análisis será el determinar si se empleará filtrado de paquetes, servicios proxy o

ambos. Cada uno de estos tiene sus ventajas e inconvenientes pero de acuerdo al nivel de seguridad que se desee brindar y de los componentes que se disponga, se los puede usar juntos y de esta manera se aprovecharán los beneficios que cada uno de ellos brinda y se conseguirá una mayor seguridad.

4.9 INSTALACIÓN Y ADMINISTRACIÓN DE UN FIREWALL

Para **instalar** un firewall, en primer lugar se compran los equipos, se instala y se codifican las reglas planificadas. A las reglas que permiten tránsito se añaden alarmas en caso de detección de intrusos, ataques fallidos y comportamientos irregulares de los usuarios en general.

Con todo instalado, antes de pasar a la explotación, hay que pasar una serie de pruebas de aceptación, las cuales suelen ser laboriosas y tediosas. Para empezar hay que disponer de personal adecuado, las pruebas no puede hacerlas el que ha planificado el firewall, tiene que ser otra persona u otro equipo cuyo ánimo sea demostrar que no funciona.

Hay que probar que el tráfico permitido pasa sin problemas y deja los registros necesarios en particular el tráfico en tránsito entre terceras partes. Servicio por servicio, en cada una de las situaciones de autenticación previstas y con el número de conexiones que se haya estimado pertinentes. ¿Qué ocurre cuando hay más conexiones de las atendibles? ¿se pierden? ¿se sabe? ¿qué ocurre cuando los ficheros de log se saturan? ¿se detiene el firewall? ¿sigue operando sin dejar trazas? ¿se avisa al operador?.

Hay que probar por otra parte, que el tráfico no deseado es bloqueado, que se disparan las alarmas pertinentes, que queda el registro necesario y que el presunto intruso recibe la respuesta

adecuada, en ciertas ocasiones hay que rechazar con notificación explícita, otras veces, descartar en silencio; en otras simular un servicio que no es real, etc. No hay que olvidar tampoco ataques orientados a inhabilitar la simple capacidad de respuesta de los sistemas (denegación de servicio: inundación de sesión tcp, inundación syn, etc.).

Es particularmente importante analizar las interacciones entre servicios. ¿Qué ocurre cuando hago esto y luego lo otro?, bien por maldad, bien por accidente los usuarios acabarán utilizando el sistema de formas imprevistas y ello no puede ser perjudicial. Este tipo de pruebas de especial creatividad por parte del equipo probador y un aprendizaje continuo, ayudará a mejorar la seguridad.

El firewall, visto como sistema admite pruebas de caja negra en las que se van probando las diferentes facetas desde un punto de vista puramente funcional También admite pruebas de caja blanca en las que se va probando todas y cada una de las reglas de autorización/denegación de servicio, para de esta manera verificar que la penetración sólo llega a donde estaba previsto.

Pudiera ocurrir que en un sistema de defensa en profundidad la seguridad no sea realmente a varios niveles, sino que alguno de los niveles esté deficientemente configurado y en realidad todo la seguridad recaiga sobre otro; puede ser conveniente simular violaciones en situaciones de defensa en profundidad, analizando las consecuencias derivadas.

Estas pruebas deben quedar clasificadas, documentadas y automatizadas en la medida de lo posible, es particularmente importante la realización de pruebas de regresión cuando se introducen nuevas versiones o servicios.

La **administración** de un firewall responde al patrón convencional de un sistema informático complejo.

Requiere la instrumentación de tareas periódicas de realización de copias de seguridad (backups), análisis de operación y elaboración de informes. Por su propia naturaleza, requiere de tareas no planificables de observación para detectar comportamientos irregulares que pudieran ser síntomas de ataques en curso o de debilidades no previstas; las irregularidades conocidas pueden disparar alarmas, las imprevistas no.

Hay que llevar un control estricto de configuración, particularmente importante cuando el firewall es distribuido o hay varios elementos firewall que deben coordinarse. Control estricto de configuración conlleva identificación de versiones de los elementos constituyentes y del conjunto, planificación de los cambios, documentación de las actuaciones, registro de la retrocesión, realización de pruebas de integración, de aceptación y de regresión.

4.10 MANTENIMIENTO DEL FIREWALL

Las tareas de mantenimiento de un firewall se dividen en 3 categorías principales:

4.10.1 Mantenimiento
4.10.2 Monitoreo del Sistema
4.10.3 Actualización.

4.10.1 Mantenimiento

El mantenimiento es el eterno ciclo de pequeñas tareas que se deben hacer para mantener el firewall a salvo, hay tres tareas principales que deben cumplir una y otra vez, estas son:

a) Respaldar el firewall
b) Administrar cuentas
c) Administrar el espacio en disco

a) Respaldar el Firewall

Se deben respaldar todas las partes del firewall esto significa no solamente respaldar computadoras de propósito general como "bastion host" o servidores internos, sino también ruteadores y otros dispositivos de propósito especial.

Para las máquinas de propósito general, se pueden tener sistemas automatizados de respaldo que produzcan una notificación a través de correo electrónico cuando algún suceso ocurra. Las máquinas de propósito específico probablemente no necesiten un sistema automatizado de respaldo, esto debido a que no sufren tantos cambios de configuración, y cuando los sufren, el encargado de realizar éstos cambios debe generar el respaldo.

b) Administrar Cuentas

La administración de cuentas involucra la creación, eliminación, cambio de contraseña, etcétera. En un Firewall es crucial para su seguridad la adición correcta de nuevas cuentas, la eliminación de viejas y el cambio apropiado de contraseñas.

Se debe establecer un procedimiento para la creación de cuentas, de ser posible usar un programa para este propósito. Las cuentas deben ser revisadas cada cierto tiempo se debe instruir (o en su caso obligar) a los usuarios para que cambien su contraseña cada determinado tiempo; en algunos casos se puede llegar a restringir la creación de cuentas.

c) Administrar el espacio en disco

El crecimiento de la cantidad de datos puede llegar a llenar por completo el espacio disponible en disco. Uno de los principales problemas lo representan los archivos de bitácoras, estos archivos van creciendo dependiendo de la actividad de las máquinas y es una buena medida revisarlos periódicamente, no solo para saber el estado que guarda el sistema sino también para poder borrar aquellos eventos registrados que ya no sean útiles. Existen algunas herramientas (o configuraciones) que permiten que se realice la rotación de los archivos de bitácoras, eliminando aquellos que sean demasiado antiguos.

4.10.2 Monitoreo del Sistema

Otro aspecto en el mantenimiento del firewall involucra el monitoreo del sistema, para lo cual se deben tener en cuenta ciertos aspectos fundamentales, entre los cuales se tiene:

- ¿El firewall se ha visto comprometido alguna vez?
- ¿Qué clase de ataques han sido probados en el firewall?
- ¿El firewall trabaja en orden?
- ¿El Firewall se encuentra habilitado para proveer los servicios que el usuario necesita?

Para responder a estas preguntas, se debe saber cuál es el patrón de uso normal.

a) Monitoreo de Dispositivos Específicos

Se debe utilizar las herramientas de monitoreo y registro proporcionadas por las partes integrantes del firewall pero puede ser conveniente tener algunos dispositivos de monitoreo dedicado, por ejemplo, se puede colocar una estación de monitoreo en el perímetro de la red a fin de que pueda asegurarse de que sólo los paquetes que se espera pasen a través de ella.

¿Cómo se puede tener la certeza de que la máquina de monitoreo no es usada por un intruso?. En algunos dispositivos de red, es posible deshabilitar la transmisión en una interfaz de red, lo cual puede hacer que la máquina sea imposible de detectar y extremadamente difícil de ser empleada por un intruso si se cuenta con los fuentes del sistema operativo, se puede deshabilitar esta transmisión.

b) Que se debe Observar

Sería conveniente conocer absolutamente todas las cosas que pasan a través del firewall, todos los paquetes aceptados o negados, todas las conexiones requeridas, etc. pero debido a que esto no es posible, ya que es demasiada información, una buena alternativa constituye revisar constantemente los archivos de log que generan otras herramientas.

Dentro de estos archivos de log, se recomienda revisar principalmente:

- Todos los paquetes bloqueados, conexiones denegadas e intentos rechazados.

- La fecha y hora, el protocolo y el nombre de usuario para cada conexión exitosa hacia o a través del "host bastion"

- Todos los mensajes de error desde los ruteadores, el "host bastion" y cualquier programa proxy.

En Linux los archivos de log que se deben revisar periódicamente son:

Archivo	**Detalle**
/var/log/messages	Contiene las bitácoras de la mayoría de actividades del sistema.
/var/log/squid/access_log	Contiene un registro de los accesos de los clientes a través del servidor
/var/log/httpd/access_log	Contiene un registro de los clientes que han visitado nuestro Web Site
/var/log/httpd/error_log	Almacena los errores que se suscitan en los acceso al servidor web.
/var/log/xferlog	Graba la transferencia de archivos FTP

El administrador debe conocer cuales son los patrones usuales y debe estar alerta ante cualquier excepción a estos patrones es importante conocer los mensajes que son generados por la actividad normal del sistema, la mayoría de los sistemas producen mensajes de error que suenan peculiares y

amenazantes aún cuando se encuentren trabajando perfectamente.

Los mensajes generados por el sistema se pueden dividir en tres categorías:

Conocidos por ser correctos.- Estos mensajes deben ser ignorados, debido a que no representan ningún problema y provienen de actividades normales del sistema, un ejemplo de esto sería: "login succeeded for user prueba".

Conocidos por ser peligrosos.- Para estos mensajes se debe tomar alguna medida, que puede ser desde enviar un aviso por correo electrónico hasta la paralización del sistema hasta encontrar la solución, un ejemplo de estos mensajes puede ser "bad disk block at location 0x47c7a8"

Desconocidos.- Requieren de una investigación más profunda para determinar que es lo que está sucediendo, por ejemplo alguien envía paquetes UDP del puerto 20 a un puerto arbitrario arriba del 1024.

Existen algunas reglas no escritas basadas en la experiencia y el criterio de los administradores, algunas de éstas son:

- **Tener en cuenta los accesos de usuarios**

  Cuando se observa a un usuario tratar de tener acceso a altas horas de la noche y falla bueno puede ser normal, cuando lo intenta una vez más es probable que aún sea normal, pero tres o más intentos es una señal de que un intruso pretende pasar la seguridad del servidor. Esta regla se aplica, en su mayoría, a atentados en cuentas diferentes; los intentos obstinados del mismo usuario por hacer la misma cosa que no funciona tal vez

sólo indique que el usuario no es quien pretende ser y lo único que busca es ganar acceso, sin tener privilegios.

- **Los accidentes no tratan de cubrir sus huellas.**

Cuando hacen falta archivos de la bitácora, si se han borrado registros o si hay evidencia de que alguien está ocultando sus huellas, tal vez existe una intrusión, esta es una mala señal de que alguien ya entró en el servidor y seguramente ya aseguró su próxima entrada.

Para facilitar el trabajo de determinar si el servidor está corriendo peligro o no, los acontecimientos sospechosos se pueden clasificar de varias categorías:

- Se conoce que lo causa y no es un problema de seguridad.

- No se sabe que lo causa y probablemente nuca se sepa, pero no ha vuelto a suceder otra vez

- Alguien trata de entrar pero no con mucho insistencia, fue un sondeo.

- Alguien realmente trató de entrar y realizó un ataque serio

- Alguien actualmente está dentro.

Los límites entre estas categorías son inciertos a menos que se trate de los mensajes de la primera categoría, esto requiere de poco juicio la mayoría de las veces. Es imposible tener una lista

exhaustiva de los síntomas de estas situaciones pero las generalizaciones pueden ser útiles.

Se puede sospechar que alguien está sondeando una máquina si se nota que:

- Algunos intentos de acceso a servicios por puertos inseguros (intento de contactar portmapper en un X Server).

- Intentos de iniciar sesión con nombres de cuentas comunes como: guest o lp, la mayoría de intentos de iniciar sesión como "anonymous" son errores.

- Solicitudes para archivos tfpf o para transferir mapas NIS.

Un ataque podría estar ocurriendo si:

- Paquetes o comandos no usuales aceptados cuyo propósito no se comprende.

- Paquetes enviados a cada puerto dentro de un rango.

- Inicio de sesión exitosa desde un sitio inesperado.

- Varios intentos de iniciar sesión en cuentas válidas del servidor, en particular cuentas que se usan a través de Internet, o intentos en cuentas en el orden en que aparecen en el archivo de contraseña.

Se puede sospechar que alguien ya entró si:

- Archivos de inicio de sesión eliminados o modificados.

- Archivos de bitácora borrados o modificados

- Nuevos archivos de inicio de sesión que contienen información de password u otros paquetes que no se pueden explicar

- Directorios que contienen más entradas administrativas que las que deberían, por ejemplo en máquinas Linux, los directorios deben contener dos entradas "." y ".." indicando este directorio y directorio padre, pero puede no haber más que dos entradas por ejemplo "..." o ".. " si se ve esto indica que hay tres o más entradas para cada uno, la entrada extra probablemente tiene espacios en ella esto es usado para ocultar un archivo o un directorio de una observación casual

- Inesperados accesos como usuarios privilegiados, por ejemplo root, o usuarios inesperados quienes repentinamente obtienen esos privilegios.

- Pruebas aparentes o ataques que provienen de máquinas propias.

- Procesos extras con nombres que son variantes de procesos comunes de sistema, por ejemplo sendmail y Sendmail están corriendo, o init e initd, este es otro truco para introducir cosas a escondidas donde no las descubra el administrador.

- Un cambio inesperado en el login prompt de la máquina indica que el programa que despliega el prompt ha sido modificado.

c) Respondiendo a los sondeos

Inevitablemente, se detectarán aparentes pruebas en el firewall, paquetes enviados de servicios de internet que no se ofrecen, intentos de ingreso de cuentas que no existen, etc. Por lo

general los sondeadores intentan una o dos cosas, y si no obtienen una respuesta interesante, se van.

El administrador puede seguir la pista de los sondeos, pero puede que pase mucho tiempo persiguiendo incidentes que no son de mucha importancia y que no están generando ningún problema en el servidor.

Si se detectan sondeos persistentes de algún sitio, debe ponerse en contacto con la gerencia de este sitio para hacerles saber lo que ocurre, pero por lo normal es lo más lejos que debe ir una persona para responder a ese problema.

4.10.3 Actualización

El último aspecto importante del mantenimiento de los firewalls tiene que ver con estar actualizado, realmente es imperante mantener contacto con los distribuidores y compañías que proveen actualizaciones y parches .

Continuamente suceden cosas nuevas, se descubren y explotan nuevos errores, se llevan a cabo ataques nuevos, están disponibles más accesorios y arreglos para los sistemas, así como herramientas nuevas. Mantenerse actualizado con todos estos cambios, es sin duda, la parte que más tiempo absorbe del trabajo del administrador de firewalls.

El recabar la información de fuentes como listas de correo hace fácil el compartir experiencias, pero lo lamentable es que el nivel de estas listas es muy variante, solo un 10 por ciento, en el mejor de los casos, son expertos, la mayor parte ni siquiera participa, los foros de discusión son buenos, en especial los que piden requisitos de admisión ya que permiten un nivel alto y estandarizado de conocimiento.

Es cierto que los problemas son lentamente reconocidos ya que algunos presentan síntomas parecidos, así es que las fuentes confunden frecuentemente, no es poco común que la administración se base en la prueba y el error, sin embargo esta no debe ser la filosofía dominante.

Los parches no se deben aplicar sin razón, los agujeros deben combatirse cuando sea conveniente, debido a que algunos parches modifican el funcionamiento del Firewall, ya que hay cargas de trabajo que se eliminan pero igualmente puede suceder que se acumulen cargas a otras aplicaciones.

Además se debe recordar que unos parches requieren la preinstalación de otros parches, mientras que otros requieren que no se este usando cierto software o parche.

El monitoreo solo debe tomar pocos minutos mientras nada sospechoso se presente, obviamente el mantener al día el firewall así como aplicar pruebas con nuevos paquetes, tomarán cierto tiempo el cual debe estar planeado con anticipación.