Que es un firewall

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Un firewal es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewal examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con softwares específicos que lo único que hacen es monitorizar las comunicaciones entre redes.

Las Fases

La fase I consiste en presentar el funcionamiento del Firewall como sistema de seguridad de una red,

la fase II comprende los componentes del sistema Firewall,

la fase III relaciona las características y ventajas del Firewall,

la fase IV es el diseño de decisión de un Firewall de Internet y el ultimo tema Limitaciones del Firewall.

FASE I
Funcionamiento del Firewall como sistema de seguridad de una red.

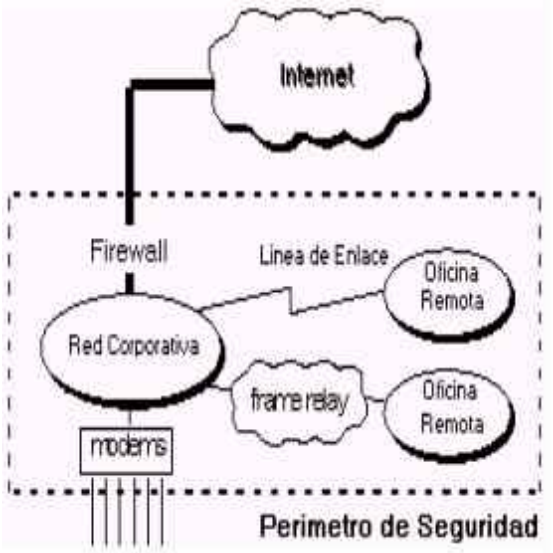

Figura 1

Un Firewall se conecta entre la red interna confiable y la red externa no confiable, (ver figura.1).Los Firewalls en Internet administran los accesos posibles del internet a la red privada. Si no contamos con un Firewall, cada uno de los servidores de nuestro sistema se exponen al ataque de otros servidores en internet.

El sistema Firewall opera en las capas superiores del modelo OSI y tienen información sobre las− funciones de la aplicación en la que basan sus decisiones.
Los Firewalls también operan en las capas de red y transporte en cuyo caso examinan los encabezados IP y TCP, (paquetes entrantes y salientes), y rechazan o pasan paquetes con base a reglas de filtración de paquetes programadas.

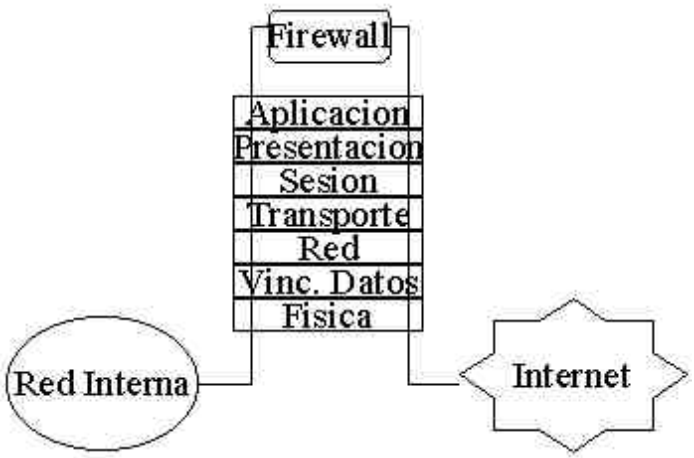

Figura 2

El firewall actúa como un punto de cierre que monitorea y rechaza el trafico de red a nivel de aplicación, (Ver Figura. 2).
Los Firewall son filtros que bloquean o permiten conexiones transmisiones de información por internet, los

filtros están diseñados para evitar que un usuario irreconocible ataque nuestro equipo por internet y al mismo tiempo podrá ser inmune a la penetración.

FASE II.
Los componentes del sistema Firewall.

Un Firewall típico se compone de uno, o una combinación, de:

- Ruteador Filtra−paquetes.
- Gateway a nivel−aplicación.
- Gateway a nivel−circuito.

El ruteador toma las decisiones de rehusar y permitir el paso de cada uno de los paquetes que son recibidos. Este sistema se basa en el examen de cada datagrama enviado y cuenta con una regla de revisión de información de los encabezados IP, si estos no corresponden a las reglas, se descarta o desplaza el paquete.(Ver figura. 3)

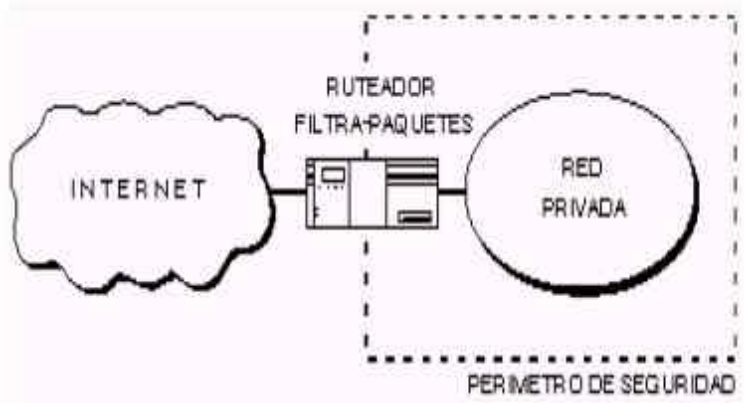

Figura 3

Gateways a nivel−aplicación

Los gateways nivel−aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra−paquetes.
Mucho mejor que depender de una herramienta genérica de filtra−paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de propósito−especial (un servicio Proxy) para cada aplicación deseada.

Gateway a nivel−circuito

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

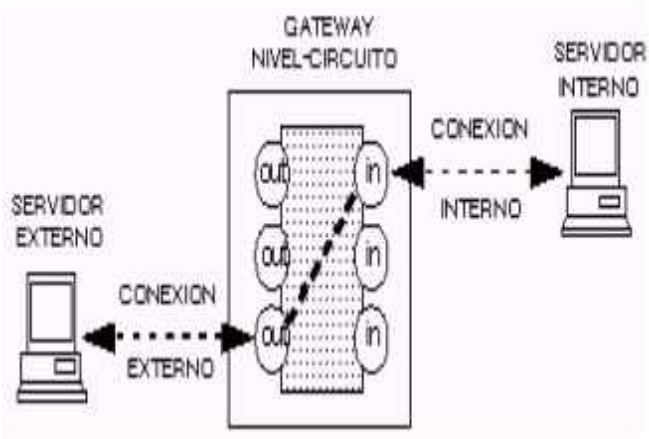

Figura 4

La figura 4 .− Muestra la operación de una conexión típica Telnet a través de un gateway a nivel−circuito. Tal como se menciono anteriormente, este gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet.
El gateway a nivel−circuito acciona como una cable copiando los bytes antes y después entre la conexión interna y la conexión externa.

FASE III.
Características y ventajas del Firewall.

Protección de la Red Mantiene alejados a los piratas informaticos (crakers) de su red al mismo tiempo que permite acceder a todo el personal de la oficina.

Control de acceso a los recursos de la red Al encargarse de filtrar, en primer nivel antes que lleguen los paquetes al resto de las computadoras de la red, el firewall es idóneo para implementar en el los controles de acceso.

Control de uso de internet Permite bloquear el material no− adecuado, determinar que sitios que puede visitar el usuario de la red interna y llevar un registro.

Concentra la seguridad.− El firewall facilita la labor a los responsables de seguridad, dado que su máxima preocupación de encarar los ataques externos y vigilar, mantener un monitoreo.

Control y estadísticas.− Permite controlar el uso de internet en el ámbito interno y conocer los intentos de conexiones desde el exterior y detectar actividades sospechosas.

Choke−Point Permite al administrador de la red definir un (embudo) manteniendo al margen los usuarios no−autorizados 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.

Genera Alarmas de Seguridad.− El administrador del firewall puede tomar el tiempo para responder una alarma y examina regularmente los registros de base.

Audita y registra internet Permite al administrador de red justificar el gasto que implica la conexión a internet, localizando con precisión los cuellos de botella potenciales del ancho de banda.

FASE IV.
Diseño de decisión de un Firewall de Internet.

Cuando se diseña un firewall de internet, se toma algunas decisiones que pueden ser asignadas por el administrador de red:

Las políticas que propone el Firewall
Posturas de la políticas No todo lo específicamente permitido esta prohibido y Ni todo lo específicamente prohibido esta permitido.

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

La segunda propuesta asume que el firewall puede desplazar todo el trafico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso.

La Política interna propia de la organización para la seguridad total
La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoria en caso de riesgo.

El costo Financiero del proyecto Firewall
Es el precio que puede ofrecer una organización por su seguridad, un simple paquete filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador− conectado al internet, y dicho paquete ya esta incluido como estándar del equipo.

FASE IV
Diseño de decisión de un Firewall de Internet.

Cuando se diseña un firewall de internet, se toma algunas decisiones que pueden ser asignadas por el administrador de red:

Las políticas que propone el Firewall
Posturas de la políticas No todo lo específicamente permitido esta prohibido y Ni todo lo específicamente prohibido esta permitido.

La primera postura asume que un firewall puede obstruir todo el trafico y cada uno de los servicios o aplicaciones deseadas necesariamente y ser aplicadas caso por caso.
La segunda propuesta asume que el firewall puede desplazar todo el trafico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso.

La Política interna propia de la organización para la seguridad total
La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoria en caso de riesgo.

El costo Financiero del proyecto Firewall
Es el precio que puede ofrecer una organización por su seguridad, un simple paquete filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador− conectado al internet, y dicho paquete ya esta incluido como estándar del equipo.

FASE V.
Limitaciones de un Firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación, en este caso:

- Conexión dial−out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al internet. Este tipo de conexiones derivan de la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque.
- El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes.
- El firewall no puede protegerse contra los ataques de la ingeniería social, en este caso, un craker que quiera ser un supervisor o aquel que persuade a los usuarios menos sofisticados.
- El firewall no puede protegerse de los ataques posibles a la red interna por virus informativos a través de archivos y software.
- Tampoco puede protegerse contra los ataques en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando el ataque.

Conclusiones

El Firewall le proporcionara la mayoria de las herramientas para complementar su seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red y hacia la red externa, es importante establecer que un monitoreo constante de el registro base, nos permitirá detectar un posible intruso y así proteger la información. Es inevitable que protejamos nuestra red de crakers cuando dentro de nuestra organización existe personal traidor y que puede sabotear nuestro sistema.

Bibliografía

- Karanjit Siyan y Chris Hare. (1997): Firewalls y la seguridad en internet, Prentice−hall Hispanoamericana, S.A.

- Karanjit Siyan y Chris Hare. (1997): Internet y la seguridad en redes, Prentice−hall Hispanoamericana, S.A.

- Http://www.symantec.com/region/mx/product/sdf/ Empresarial.htm Obtenido de la red Mundial (El día 24 de septiembre del 2001

- Http://lat.3com.com/br/products/firewalls/firewalls.html obtenido de la red Mundial (El día 24 de septiembre del 2001) Copyright © 1995−2001 3Com Corporación.

- Http://www.viared.cl/seguridad.htm
  Obtenido de la red Mundial (El día 24 de septiembre del 2001) Viared Computación LTDA.
  Huelen 222 Oficina 11, Providencia − CP: 6640340