Firewall / Cortafuegos

Osvaldo Callegari
Analista de Sistemas
ocalle@ar.inter.net

Quizás, uno de los elementos más publicitados a la hora de establecer seguridad en las redes. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

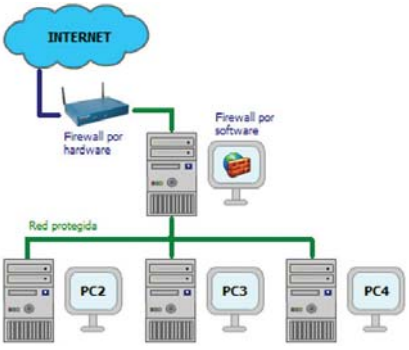
Un Cortafuegos (o Firewall en inglés) es un elemento de hardware o software cuya ubicación habitual es el punto de conexión de la red interna de la organización con la red exterior (Internet); de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades en los sistemas de red internos.

Objetivos

Un *Firewall* es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce una *política de seguridad* establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es *(por ejemplo Internet)*.

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera y viceversa, debe pasar a través de él.
- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.



Como puede observarse, un *Firewall*, sólo sirve de defensa perimetral de las redes, no defiende ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Políticas de Diseño de Firewalls

Generalmente se plantean algunas preguntas fundamentales que deben ser respondidas en cualquier política de seguridad:

• ***¿Qué se debe proteger?***

Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).

• ***¿De quién protegerse?***

De cualquier intento de acceso no autorizado desde el exterior. Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

• ***¿Cómo protegerse?***

Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

a. Paradigmas de seguridad

- Se permite cualquier servicio excepto aquellos expresamente prohibidos.
- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos.

b. Estrategias de seguridad

- *Paranoica:* se controla todo, no se permite nada.
- *Prudente:* se controla y se conoce todo lo que sucede.
- *Permisiva:* se controla pero se permite demasiado.
- *Promiscua:* no se controla (o se hace poco) y se permite todo.

• **¿Cuánto costará?**

Estimando en función de lo que se desea proteger se debe decidir cuanto es conveniente invertir.

Restricciones en el Firewall

La parte más importante de las tareas que realizan los *Firewalls*, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1. Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a las que se denomina *Trusted (validados)*. Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.

2. Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna. Es conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

Beneficios de un Firewall

Los *Firewalls* manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El *Firewall* es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Continúa en página 184

Continúa en página 180

Otra causa que ha hecho que el uso de *Firewalls* se halla convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "*traductor de direcciones*", el cual puede alojarse en el *Firewall.*

Los *Firewalls* también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "*consumido*" por el trafico de la red, y que procesos han influido más en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los *Firewalls* también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios www y ftp.

Limitaciones de un Firewall

La limitación más grande que tiene un *Firewall* sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los *Firewalls* no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje *Back Doors*, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el *Firewall* "*NO es contra humanos*", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del *Firewall* y difunde esta información, el *Firewall* no se dará cuenta.

El *Firewall* tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el *Firewall,* de algun antivirus.

Finalmente, un *Firewall* es vulnerable, él NO protege de la gente que está dentro de la red interna. El *Firewall* trabaja mejor si se complementa con una defensa interna.

Fuente: www.segu-info.com.ar

Tipos de Firewalls

1. Filtrado de Paquetes

Se utilizan *Routers* con filtros y reglas basadas en políticas de control de acceso. El *Router* es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

a. Protocolos utilizados.
b. Dirección IP de origen y de destino.
c. Puerto TCP-UDP de origen y de destino.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red.

2. Proxy-Gateways de Aplicaciones

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

3. Dual-Homed Host

Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP-Forwarding desactivado".

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará de puente entre éste y el usuario interior.

4. Screened Host

En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.

5. Screened Subnet

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.

En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

6. Inspección de Paquetes

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.

7. Firewalls Personales

Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.