GATEWAYS COMO FIREWALLS

Ricardo Sánchez Q.
Estudiante Ingeniería Telemática

Aunque las empresas que han experimentado un ataque a su red por mano de usuarios no deseados, son recientes a hablar sobre sus experiencias, el problema es real. Unos artículos del *New York Times* aparecidos en la Primavera del 1995, que hablaban de los ataques a redes de los ordenadores del Pentágono, demostraban la realidad. La seriedad de este problema han inspirado a una forma de defensa. La forma más efectiva de proporcionar una alta seguridad en un sistema informático, es el uso de los Firewalls.

Firewalls

Los Firewalls son barreras creadas entres redes privadas y redes públicas como Internet. Originalmente, fueron diseñados por los directores de informática de las propias empresas, buscando una solución de seguridad. Más recientemente, los sistemas de seguridad proporcionados por terceras empresas, son la solución más escogida.

Los Firewalls son simples en concepto, pero estructuralmente complejos. Examinan todo el tráfico de entrada y salida, permitiendo el paso solamente al tráfico autorizado. Los Firewalls son diseñados de forma que todo lo que no es expresamente autorizado, es prohibido por defecto.

Un Firewall protege la red interna de una organización, de los usuarios que residen en redes externas. Un Firewall permite el paso entre las dos redes a sólo los paquetes de información autorizados. Los Firewalls pueden ser usados

internamente, para formar una barrera de seguridad entre diferentes partes de una organización - como por ejemplo a estudiantes y usuarios administrativos de una universidad.

Los Firewalls reflejan un número de decisiones de diseño dependiendo del acceso, seguridad y transparencia. Un Firewall es diseñado para entregar un acceso seguro a los servicios ofrecidos por la red Internet con un mínimo esfuerzo adicional. La calidad de este "mínimo esfuerzo" es llamada la "transparencia" que significa que un usuario puede usar un gran número de software comercial sin modificaciones adicionales. Un Firewall puede mejorar significativamente el nivel de seguridad en la red y reducir los riesgos filtrando la falta de seguridad inherente en los servicios de Internet. UN Firewall implementa una política de acceso a la red, forzando que todas las conexiones a ésta, se realizan a través de él, mientras son examinadas y evaluadas.

Los Firewalls Usan Tres Tecnologías Diferentes

Los métodos son: Filtro de paquetes, Gateways a Nivel de Circuitos y Gateways a Nivel de Aplicación. A veces se usan de forma separada, a veces conjuntamente. El Filtro de Paquetes trabaja a nivel TCP/IP y no tienen control de qué aplicaciones están filtrando. Las Gateways a Nivel de Circuitos interceptan las sesiones y las pasan a través de los Firewall. Las Gateways a Nivel de Aplicación operan al nivel más alto, controlando las aplicaciones que han generado los paquetes.

Filtro de Paquetes

El Filtro de Paquetes trabaja al nivel TCP/IP. Aceptan paquetes pre-aprobados aquellos que vienen de fuentes particulares o que son direccionados a direcciones específicas de su red. El Filtro de Paquetes es transparente al usuario y puede ser instalado como parte de un Router que entrega la típica conexión a Internet.
De todas formas, como solución de seguridad, el Filtro de Paquetes por sí solo, tiene varios fallos. Primero, requieren

que el remitente sea pre-aprobado. Usted quizá quiera permitir el acceso a un servicio desde un usuario remoto, pero no a otros servicios. La solución requiere definiciones especiales de qué tipo de servicios pueden ser autorizados. Estas definiciones especiales pueden ser particularmente difíciles de aplicar. Además, se pueden tener problemas con servicios como FTP o DNS. Estas aplicaciones usan protocolos que son extremadamente difíciles de gestionar a nivel de paquetes.

Gateways a Nivel de Circuito

Las Gateways por definición son seguras. Todo el tráfico de entrada y salida está gobernado por una Gateway. Ya que no hay una conexión física directa entre las máquinas de su red interna y las redes externas, las conexiones de salida pueden ser todavía permitidas cuando el destino sea autorizado.

Las Gateways a Nivel de Circuito usan proxies para asegurar su red interna. Los llamantes establecen conexiones TCP/IP con la Gateway. Una puerta de la Gateway actúa como un agente para sus usuarios. Este agente verifica las transmisiones y las acepta dependiendo del usuario. La Gateway entrega luego los datos a la dirección apropiada de su red interna. Además, la dirección del agente es la única información transmitida externamente en los paquetes de salida. Los Proxies ayudan a limitar la cantidad de información de máquinas individuales que se enseña al mundo exterior. De todas formas, es posible que un usuario interno rompa esta seguridad usando una puerta no estándar o bien un servicio no autorizado.

Al contrario del Filtro de Paquetes, la Gateway a Nivel de Circuito no examina cada paquete de datos. Aceptan múltiples paquetes de datos una vez verificada la información de dirección.

Gateways a Nivel de Aplicación

Las Gateways a Nivel de Aplicación efectúan el mismo tipo de función de las Gateways a Nivel de Circuito con una adición. Examinan los contenidos de cada paquete cuando pasan por la Gateway.

Los Hackers no tienen la oportunidad de entrar a su sistema "escondiendo" datos destructivos entre la información aparentemente "sana". Esto es particularmente importante cuando se permite el acceso de correo electrónico externo a su red interna. SMTP no es un protocolo seguro, y es el sistema de vulnerabilidad más común.

La Gateway examina tanto los paquetes de salida como de entrada. Esto elimina la posibilidad de que usuarios internos accedan a servicios no autorizados que puedan crear un "agujero" en la seguridad. La Gateway a Nivel de Aplicación es el protocolo de filtro más seguro. Dado que efectúan un detallado análisis de los paquetes, son los más costosos en términos de tiempo y de equipo.

CONCLUCIONES

Ya decidida que política de seguridad se va a implementar, se necesita evaluar qué servicios se necesitan en un Firewall. Como mínimo, un firewall debe tener las siguientes características y atributos:

- Posibilidad de denegar todos los servicios, excepto aquellos específicamente permitidos por el administrador de sistemas
- Una administración flexible, para que los nuevos servicios o necesidades se puedan implementar fácilmente
- Soporte de técnicas líderes de autentificación
- El Filtro de IP debe ser flexible, fácil de programar y debe poder filtrar tantos atributos como sea posible, inluyendo dirección IP destino y fuente
- Uso de Proxies en servicios como FTP y Telnet
- Tener la posibilidad de centralizar el acceso SMTP
- Acomodar acceso público al sito
- Posibilidad de filtrar y concentrar accesos remotos por llamadas
- Contener mecanismos para guardar registros de tráfico y de actividad sospechosa

- Generar alarmas para detectar intrusos (el grado debe ser programado por el administrador de sistemas)
- Que se ejecute en un host dedicado
- Que se base en un sistema operativo seguro
- Que sea simple en el diseño por lo que puede ser comprendido y mantenido fácilmente
- Que pueda ser actualizado