Firewalls

La transmisión de información entre los equipos de cómputo se ha convertido en un asunto de seguridad muy serio. Si bien es cierto, los programas antivirus y *antispyware* representan una línea de defensa fundamental en la protección de *software* y datos, también lo es la instalación y actualización de *firewalls* para la protección de ataques o intrusiones de terceros a nuestra red interna y computadoras personales.

A diferencia de un programa antivirus, un *firewall* o cortafuegos es un *software* o *hardware* dedicado a filtrar información proveniente de una red o internet, permitiendo o denegando el acceso de acuerdo a la configuración establecida en él; es decir, todo el tráfico que salga o llegue a la red interna de una organización debe pasar por el *firewall*: con ello se logrará únicamente flujo de tráfico autorizado.

El filtrado de entrada o salida de información se realiza mediante la aplicación específica de políticas de seguridad previamente establecidas. Por ejemplo, una política puede ser la recepción o bloqueo de correos electrónicos entrantes o salientes en una red; o bien, la prohibición de transmisión de archivos a través del protocolo conocido como ftp, o tal vez el bloqueo al uso del *World Wide Web* a ciertos usuarios con direcciones IP específicas. (Recordemos que a cada equipo de cómputo que accede a la red, se le asigna una dirección IP única). Los *firewalls* también realizan registros del número de intentos que un usuario lleva a cabo para determinados recursos, efectúan filtrado de paquetes de datos con base en su dirección de origen o destino, y mantienen alejados de la red interna a usuarios no autorizados que intentan acceder indebidamente. Incluso existen *firewalls* con la capacidad de autorizar accesos a cierta información de la organización ubicadas en determinadas áreas de su red interna.

El *firewall* puede ser de *hardware*, es decir, un dispositivo dedicado al filtrado de información que destina sus recursos de memoria y procesamiento exclusivamente para esta función; o de *software*, que se instala en algún equipo de cómputo que comparte otras funcionalidades, y que tiene como limitante que los recursos de hardware empleados sean los mismos que la computadora del usuario, pudiendo repercutir negativamente en su rendimiento.

Asimismo, la programación del *firewall* debe realizarse con extremo cuidado pues cualquier política de seguridad mal aplicada, podría provocar el traspaso de usuarios no autorizados a la red o incluso fallas o bloqueos en la operación de la misma. Si esto llegara a ocurrir, el *firewall* se convertirá en un sistema de protección poco confiable e incluso inservible.

Por último, es importante mencionar que un *firewall* es sólo un recurso adicional a la protección de la red de cómputo y de ninguna manera

sustituye al resto de los sistemas de protección de datos como antivirus, *antispyware*, *antispam*, detector de intrusos, etc. Por ejemplo, un *firewall* no podrá proteger la red si alguno de sus usuarios introduce a su equipo una memoria USB con *malware*, pues además de infectarlo, seguramente se propagará a otras computadoras interconectadas. Es por ello que, aun teniendo *firewalls* altamente sofisticados, siempre será necesario mantener instalado y actualizado hardware y software de seguridad complementarios.

Revisión técnica: Ing. Fernando Maldonado Salgado

REFERENCIAS:

- Greensmith, J. (2005), Firewalls, Intrusion Detection Systems and Anti-virus Scanners, School of Computer Science and Information Technology, University of Nottingham. Tomado de: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.2262&rep=rep1&type=pdf
- Scarfone, K. (2009). Guidelines on Firewalls and Firewall Policy, National Institute of Standards and Technology. Tomado de: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
- Santillán, J. (2010). Firewalls, controlando el acceso a la red, Revista seguridad, defensa digital. Núm. 4 UNAM. Tomado de: http://revista.seguridad.unam.mx/numero-04/firewalls-controlando-el-acceso-la-red

OTRAS FUENTES:

- http://www.pcworld.com/article/117557/article.html
- http://www.pandasecurity.com/spain/homeusers/support/card?Id=31435
- http://windows.microsoft.com/es-xl/windows/what-is-firewall#1TC=windows-7