

Deteniendo intrusos: firewall personales



Autor: Cristian Borghello, Technical & Educational Manager de ESET para
Latinoamérica

Fecha: Lunes 29 de octubre del 2007

Cuando se habla de malware se hace referencia a una infinidad de códigos cuyo objetivo es ocasionar algún daño al sistema y, actualmente, la mayoría de ellos intenta producir algún beneficio económico a su creador mediante la estafa al usuario o el robo de información confidencial del mismo.

Si el usuario no se encuentra capacitado para saber diferenciar un engaño de un programa real y/o no cuenta con las herramientas apropiadas para su protección, seguramente será víctima de algunos de estos malware actuales.

La protección antivirus con capacidades proactivas, como ESET Smart Security y ESET NOD32 Antivirus, son un elemento indispensable en cualquier sistema informático actual, pero poco puede hacer la mejor protección antivirus en un sistema ya infectado por un malware cuyo objetivo puede ser:

- enviar información confidencial del usuario a un delincuente en algún lugar de Internet
- recibir actualizaciones de malware ya instalado en el sistema
- propagar el malware a toda una red interconectada
- utilizar el equipo infectado como servidor de archivos con material ilegal de diversa índole (warez, cracks, pedofilia, etc.)
- utilizar el equipo del usuario para lanzar ataques sincronizados a terceros (DoS - ataques de denegación de servicio)
- ser un equipo zombie y formar parte de una botnet destinada a distintos objetivos [1]

Si bien no fue el objetivo inicial, actualmente el firewall es la principal herramienta para prevenir el tipo de acciones descriptas: evitar la conexión de sujetos (programas o personas) indeseados a y desde el sistema.

Un firewall se puede definir como un sistema (hardware o software) instalado entre el sistema del usuario y la conexión exterior y que controla esta conexión hacia (entrada de datos) y desde (salida de datos) el sistema protegido. De esta forma, se crea una barrera que controla toda la información que atraviesa la red.

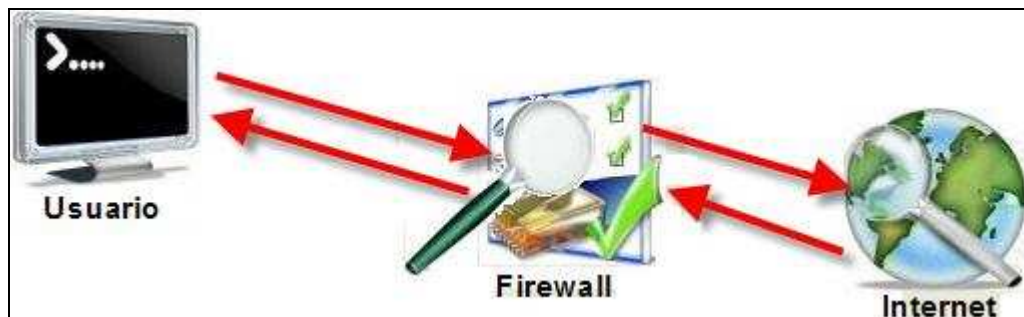


Imagen 1 – Esquema de un firewall

Estableciendo una conexión

Todas las computadoras tienen una dirección IP única, que consiste en 4 números de 0 a 255 separados por un punto (ej: 127.0.0.1 ó 20.125.89.100). Estas direcciones IP son comparables con las direcciones postales de las casas, o al número de los teléfonos.

Pero para que el host de destino pueda escoger la aplicación correcta, no sirve simplemente indicar la dirección IP; se necesitarán más especificaciones. Estas especificaciones harán necesaria la definición de un puerto, que se representa con un valor de 16 bits y hace a la diferencia entre los posibles receptores de un mensaje.

Actualmente, existen miles de puertos ocupados de los 2¹⁶ = 65535 posibles, de los que apenas unos cuantos son los más utilizados. Cada puerto puede ser manipulado por una aplicación específica (por ejemplo el puerto 21 para FTP, el 80 para HTTP, el 25 SMTP, etc.).

El objetivo del firewall es controlar cada uno de esos puertos y las aplicaciones para decidir si se permite o no el paso de cada comunicación establecida. Los puertos sobre los que se permite una conexión se dice que están abiertos y aquellos que no lo permiten, están cerrados o stealth (ocultos).

Enseñando al firewall

El firewall es el encargado de examinar cada conexión existente y verificar si se autoriza o se deniega la misma en base a un conjunto de reglas determinadas. Estas reglas pueden ser definidas explícitamente por el usuario (se enseñan) o incluso el mismo firewall puede configurarlas de manera "automática" en base a algunos conceptos previamente especificados por el desarrollador.

Es recomendable que estas reglas sean lo más restrictivas posible y si bien podría pensarse lo contrario, por lo general se afirma que *"lo que no está específicamente autorizado se deniega"*. Esta frase expresa que sólo ingresa o sale del sistema lo que el usuario autorice explícitamente y el firewall será el responsable de denegar cualquier conexión restante que intente establecerse.

Tipos de firewall

Actualmente se reconocen, a grandes rasgos, dos tipos de firewall: corporativos y personales.

Firewall corporativo

Como su nombre lo indica, son utilizados mayormente en sistemas interconectados de organizaciones y empresas en donde cierta cantidad de equipos podrían estar conectados en red compartiendo y accediendo a cientos de recursos simultáneamente.

Estos sistemas tienen el objetivo de filtrar las comunicaciones en el borde de la organización. Debido a que todo el tráfico que circula desde la red interna hacia fuera y viceversa es elevado, estos sistemas deben ser eficientes en el manejo de todas las conexiones.

Una de las ventajas de la utilización de estos dispositivos es que todos los equipos de la organización estarán protegidos por un único sistema, bloqueando o dejando pasar las comunicaciones que el administrador haya dispuesto para toda la organización.

Este tipo de dispositivos puede ser de software o hardware y su costo dependerá del tamaño y prestaciones brindadas.

Firewall personal

Si bien actualmente existe una infinidad de dispositivos (hardware) con algunas propiedades de filtrado de conexiones (como los provistos por algunos ISP) y que incluso pueden ser utilizados por usuarios individuales; a diferencia de los anteriores, y como su nombre lo indica, los firewall personales son aplicaciones (software) que se instalan en los equipos de los usuarios cumpliendo el mismo rol de examinar las conexiones.

El objetivo de los firewall personales es la de "aislar" el equipo del usuario y sólo autorizar aquellas conexiones permitidas asegurando así, que ningún proceso no autorizado envíe información al exterior y que tampoco se realicen conexiones extrañas hacia el sistema del usuario.

A modo de ejemplo, en la siguiente imagen una aplicación (Internet Explorer) solicita conectarse a Internet a través del puerto 80 (conexión saliente) y otra aplicación (Messenger) solicita ingresar desde Internet a través del puerto 1146.



Imagen 2 – Bloqueo de conexión saliente y entrante

El firewall pregunta qué acción tomar debido a que no existía una regla definida para esas conexiones. En esa sencilla pantalla, el usuario ya estará configurando una regla para que la aplicación no vuelva a preguntar en futuras conexiones de este tipo.

Como puede observarse, el beneficio de estas aplicaciones radica en que el usuario tiene el control total sobre las conexiones, pudiendo permitir aquellas que conozca, denegar las desconocidas e incluso bloquear todo tipo de conexión en casos extremos.

Ahora bien, los desarrolladores de firewall deben ser conscientes de que una aplicación que “no deja trabajar al usuario” y que continuamente “lo interrumpe con preguntas”, seguramente será una aplicación condenada a la desinstalación, debido a que sus beneficios no alcanzan a cubrir los problemas ocasionados.

En este caso, es fundamental que la aplicación posea el balance suficiente entre su capacidad de protección y la no invasión al usuario. Las preguntas deben ser la justas y necesarias y servir de base para futuras decisiones, de modo que el usuario no se sienta “moleestado” en sus tareas y que además esté correctamente protegido.

Un caso particular: el firewall de Windows XP y Windows Vista

Los firewall personales se comenzaron a popularizar entre los usuarios finales cuando Windows XP incluyó el suyo en el sistema operativo, siguiendo esta política en su sucesor Windows Vista.

Con respecto a estos firewall, se debe remarcar que el incluido en Windows XP solamente filtra las comunicaciones entrantes (y no las salientes) y si bien es una fortaleza importante, se debe tener en cuenta que no es suficiente cuando se trata de malware que está enviando información al exterior. Por su lado, Windows Vista sí filtra las comunicaciones entrantes y salientes.

Conclusiones

La utilización de un firewall es sumamente sencilla y los beneficios aparejados son inmediatos debido a que todas las conexiones establecidas serán controladas, y anuladas las innecesarias (puertos cerrados).

La gran proliferación de malware actual y su tendencia a realizar conexiones permanentemente, hacen del firewall una herramienta imprescindible para controlar el flujo de información y el compañero ideal de una protección antivirus con capacidades proactivas que controle las aplicaciones ejecutadas.

Más información:

[1] Botnets, redes organizadas para el crimen

<http://www.eset-la.com/threat-center/1573-botnets-redes-organizadas-crimen>