Firewalls personales

Un firewall es un programa que ayuda a proteger tu equipo de intrusos que podrían intentar eliminar información, hacer que deje de funcionar o hasta robar información personal, como contraseñas ó números de tarjeta de crédito.

¿Qué es un firewall?

En la actualidad, un firewall es una herramienta indispensable para proteger nuestra conexión a Internet. El hecho de hacer uso de una conexión a Internet puede ser causa de múltiples ataques a nuestro equipo de cómputo desde el exterior, cuanto más tiempo estemos en línea, mayor es la probabilidad de que la seguridad de nuestro sistema se vea comprometida por un intruso desconocido

Por lo tanto, ya no solamente es necesario tener instalado y actualizado un software antivirus y un software antispyware sino también es totalmente recomendable mantener instalado y actualizado un software de firewall.

Un firewall es un sistema diseñado para impedir el acceso no autorizado o el acceso desde una red privada. Pueden implementarse firewalls en hardware, software o en ambos. Los firewalls se utilizan con frecuencia para impedir que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet.

El firewall personal protege al equipo frente a ataques de Internet, contenidos Web peligrosos, análisis de puertos y otros compore mientos de naturaleza sospechosa.

¿Cómo funciona un firewall?

Un firewall constituye una especie de barrera delante de nuestro equipo, esta barrera ex mina todos y cada uno de los paquetes de información que tratan de atravesarlo. En función de reglas previamente establecidas, el firewall decide qué paquetes deben pasar y cuáles deben ser bloqueados.

Muchos tipos de firewalls son capaces de filtrar el tráfico de datos que intenta salir de nuestra red al exterior, evitando así que los diferentes tipos de código malicioso como caballos de Troya, virus y gusanos, entre otros, sean efectivos. El firewall actúa de intermediario entre nuestro equipo (o nuestra red local) e Internet, filtrando el tráfico que pasa por él.

Todas las comunicaciones de Internet se realizan mediante el intercambio de paquetes de información, que son la unidad mínima de datos transmitida por la red. Para que cada paquete pueda llegar a su destino, independientemente de donde se encuentren las máquinas que se comunican, debe llevar anexada la información referente a la dirección IP de cada máquina en comunicación, así como el puerto a través del que se comunican. La dirección IP de un dispositivo lo identifica de manera única dentro de una red. El puerto de comunicaciones es una abstracción lógica que podríamos comparar con la frecuencia en una emisión radiofónica: del mismo modo en que tenemos que sintonizar la frecuencia en que se transmite una emisión de

radio para poder escucharla, tenemos que utilizar el mismo puerto de comunicaciones que el equipo al que nos queremos conectar.

Un firewall, como ya se ha descrito, intercepta todos y cada uno de los paquetes destinados a nuestro equipo y los procedentes de él, realizando este trabajo antes de que algún otro servicio los pueda recibir.

De lo anterior podemos concluir que un firewall puede controlar todas las comunicaciones de un sistema a través de Internet.

Se dice que un puerto de comunicaciones está abierto si el sistema devuelve una respuesta al llegar un paquete de petición de establecimiento de conexión. En caso contrario el puerto se considera cerrado y nadie puede conectarse a él.

El punto fuerte de un firewall reside en que al analizar cada paquete que fluye a través del mismo, puede decidir si lo deja pasar en uno u otro sentido, y puede decidir si las peticiones de conexión a determinados puertos deben responderse o no.

Por ejemplo, si en nuestro equipo tenemos alojada una página Web personal podemos configurar un firewall para que sólo permita las comunicaciones a través del puerto de Web (puerto 80 y utiliza el protocolo HTTP), ya que es el único puerto que necesitamos.

http://www.tinysoftware.com

- **Panda Platinum Internet Security - Panda Software**

  http://www.pandasoftware.com

- **F-Secure Internet Security - F-Secure**

  http://www.f-secure.com

- **Personal Firewall Plus - McAfee**

  http://www.mcafee.com

- **eTrust EZ Firewall - Computer Associates**

  http://www.ca.com

Revisión histórica

- Liberación original: 2 de agosto de 2005
- Última revisión: septiembre de 2009

El Departamento de Seguridad en Computo/UNAM-CERT agradece el apoyo en la elaboración y revisión de este documento a:

- Jesús Ramón Jiménez Rojas
- Rocío del Pilar Soto Astorga

Para mayor información acerca de éste documento de seguridad contactar a:

UNAM CERT Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Códentao DGSCA- MNAM
DE-Mail