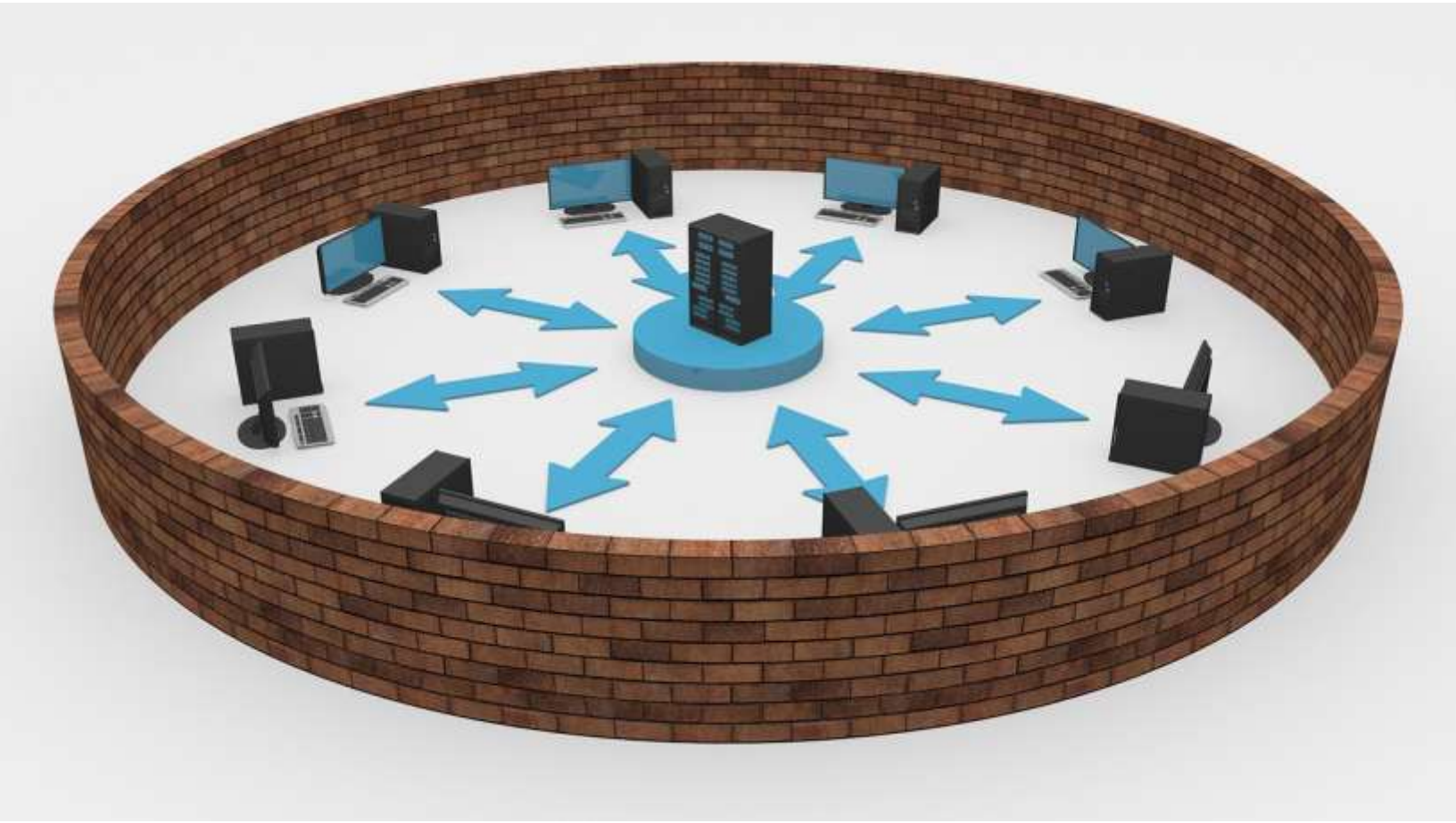
¿Qué es y para qué sirve un firewall?



QUE ES UN FIREWALL

Un firewall o cortafuegos es parte de una red o un sistema que su objetivo es el de bloquear un acceso que no esta autorizado. Este sistema se configura de tal manera con tal de permitir que se autorice el limitar y descifrar la totalidad de trafico entrante y saliente.

Si el tráfico entrante o saliente cumple con una serie de **Reglas** que se especifican, entonces se podrá acceder o salir de la red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.

A finales de los años 80 el internet siendo una tecnología muy nueva, inició a utilizar los routers como un tipo de seguridad para mantener las redes separadas entre sí. Se hicieron varias pruebas entre expertos de sistemas de como se podía manipular el internet. Por lo que fue hasta el año de 1988 que DEC publicó el primer firewall. Posterior a esta fecha se han hecho nuevos sistemas y mejoras con tal de que los mismos sean de gran resguardo para las personas, empresas e inclusive gobiernos.

Dentro de los objetivos primordiales por el cual se debe de colocar un firewall son:

- Preservar la seguridad y privacidad.
- Proteger nuestra red doméstica o empresarial.
- Mantener a salvo la información almacenada en nuestra red, servidores así como ordenadores.
- Evitar que los usuarios no deseados ingresen a nuestra red y ordenador.

Por medio de un firewall configurado apropiadamente podrá proteger a aquellos ataques de IP address Spoofing, Ataques Source Routing, etc.

Es importante tomar en cuenta que si una persona cuenta con un antivirus este no podrá proteger su equipo si el firewall no está configurado correctamente.

El firewall se encuentra instalado en el punto de unión entre 2 redes. Usualmente se puede observar como cada una de las subredes dentro de nuestra red puede tener otro firewall,. Es así como también cada uno de los equipos puede tener su propio firewall por software. De esta forma, en caso que quieran ingresar sin autorización, se puede evitar que los daños de una subred se propaguen a la otra. Es importante entonces que dentro del firewall se pueda conocer si el tráfico cumple con las **reglas** que se han configurado en los firewall el trafico podrá entrar o salir de nuestra red. Si el tráfico no cumple con las **reglas** que se han

configurado en los firewall entonces el tráfico se bloqueará no pudiendo llegar a su destino.

El firewall de hardware es una solución excelente para las empresas. Es una red que protegerá la totalidad de los equipos. Este podrá también realizar la configuración en un solo punto que será el mismo firewall. Se implementan funcionalidades interesantes como pueden ser CFS , ofrecer tecnologías SSL o VPN, antivirus integrados, antispam y control de carga.

Los firewall por software son los más comunes y los que tienden a ser utilizados en casa. Este se instala directamente en los ordenadores o servidores que queremos proteger y solo protegen el ordenador o servidor en el que lo hemos instalado. Las funcionalidades que acostumbran a proporcionar los firewall por software son más limitados. Es importante tomar en cuenta que media vez este está instalado, el software estará consumiendo recursos de nuestro ordenador.

REGLAS PARA IMPLEMENTAR EN UN FIREWALL

El tipo de reglas y funcionalidades que se pueden construir en un firewall son diversas, sin embargo se recomienda que:

- **Administrar los accesos de los usuarios a los servicios** privados **de la red**.

- **Registrar todos los intentos de entrada y salida** de una red. El log se le llama a la forma como se registran y almacenan todos estos intentos de entrada y salida.

- **Filtro de direcciones** se le llama al tipo de funciones en el cual se guardan por origen, destino, y número de puerto. Es así que con el filtro podemos bloquear o aceptar el acceso a nuestro equipo de la IP través de un puerto. Por conocimiento, es importante recordar que únicamente el puerto 22 suele ser el puerto de un servidor SSH.

- **Filtrado de protocolo** permite aceptar o rechazar el tráfico en función del protocolo que se está utilizando. Existen distintos tipos de protocolos que se pueden utilizar como lo son **http, https, Telnet, TCP, UDP, SSH, FTP**, entre otros.

- **Inspeccionar el numero de conexiones que se producen desde un mismo punto.** Las mismas se pueden bloquear si superan un determinado límite. Con lo anterior se puede evitar algunos ataques de denegación de servicio.

- **Controlar las aplicaciones para accesar a Internet**. Es así como podemos restringir el acceso a ciertas aplicaciones, como por ejemplo facebook, a un determinado grupo de usuarios.

- **Identificar y detener los puertos que están en escucha y que no deberían de estarlo**. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

LIMITACIONES DE LOS FIREWALL

Existen muchas limitaciones que cuenta un Firewall por lo que es importante que se tomen en cuenta para que no se tengan otras expectativas.

- Un firewall no necesariamente puede proteger ciertas vulnerabilidades internas. Un ejemplo de lo anterior puede ser que un usuario borre el contenido de todo el ordenador sin que el firewall lo pueda evitar. Por otro lado un usuario puede introducir un USB y robar información sin que se conozca.
- Un firewall solo nos protege frente a aquellos ataques que atraviesen el mismo. Con lo anterior nos referimos a que no puede evitar en su totalidad los ataques que recibe la red o servidor.
- Siempre es importante contar con sistemas de seguridad de forma paralela en caso que el firewall falla.

Fuente: http://geekland.eu/que-es-y-para-que-sirve-un-firewall/

Palabras: 948