FIREWALL

1. Definición

Un firewall (también llamado cortafuego), es un sistema que permite **proteger a una computadora o una red de computadoras de cualquier intento de acceso no autorizado, expresamente de Internet**. El firewall es un sistema que permite filtrar los paquetes de datos que andan por la red.

Puede ser un programa (software) o un equipo (hardware) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas.

El cortafuego proporciona un modo de filtrar la información que se comunica a través de la conexión de red. Cuando están presentes en un equipo individual, se denomina un **firewall personal**. Cuando los firewalls están presentes en una red empresarial para la protección de múltiples equipos se denomina **Firewall de red**.

2. Funcionamiento

**Un firewall funciona como una barrera entre internet u otras redes públicas y nuestra computadora.** Todo el tipo de tráfico que no esté en la lista permitida por el firewall, no entra ni sale de la computadora. Para ello, un sistema de firewall contiene un conjunto de reglas predefinidas que permiten:

* Autorizar una conexión **(Allow)**
* Bloquear una conexión **(Deny)**
* Re direccionar un pedido de conexión sin avisar al emisor **(Drop).**

El conjunto de estas reglas permite instalar un método de filtración dependiente de la [política de seguridad adoptada por la organización.](https://tecnologia-informatica.com/todo-sap-bussines-one/) Se distinguen habitualmente dos tipos de políticas de seguridad que permiten:

* Permitir únicamente las comunicaciones autorizadas explícitamente: **“Todo lo que no es autorizado explícitamente está prohibido”.**
* Impedir cualquier comunicación que fue explícitamente prohibida.

El primer método es el más seguro, pero requiere de una definición precisa de las necesidades de comunicación de toda la red.

3. Función

Básicamente la función de un firewall es **proteger los equipos individuales, servidores  o equipos conectados en red contra accesos no deseados de intrusos que nos pueden robar datos confidenciales, hacer perder información valiosa o incluso denegar servicios en nuestra red.**

Es recomendable que todo el mundo utilice un firewall por los siguientes motivos:

* Preservar nuestra seguridad y privacidad.
* Para proteger nuestra red doméstica o empresarial.
* Para tener a salvo la información almacenada en nuestra red, servidores u ordenadores.
* Para evitar intrusiones de usuarios no deseados en nuestra red y ordenador. Los usuarios no deseados tanto pueden ser hackers como usuarios pertenecientes a nuestra misma red.
* Para evitar posibles ataques de denegación de servicio.

4. TIPOS DE FIREWALL

Básicamente, existen dos tipos de firewalls, destinados a diferentes tipos de infraestructuras de datos y tamaños de red.

* Firewall por Software (tanto aplicaciones gratuitas como pagas)
* Firewall por Hardware (Es decir mediante la utilización de dispositivos)

**Firewall por Software**

Un firewall gratuito es un software que se puede instalar y utilizar libremente, o no, en la computadora. Son también llamados “Desktop firewall” o “Software firewall”.

Son firewalls básicos para pequeñas instalaciones hogareñas o de oficina que monitorean y bloquean, siempre que necesario, el tráfico de Internet. Casi todas las computadoras vienen con un firewall instalado independientemente del sistema operativo instalado en ellas.

**Firewall por Hardware**

Una firewall por Hardware viene normalmente instalada en los routers que utilizamos para acceder a Internet, lo que significa que [todas las computadoras que estén detrás del router estarán protegidas por un firewall que está incluido en el dispositivo.](https://tecnologia-informatica.com/conectarse-wifi-trucos-problemas-soluciones/) La mayoría de los routers vienen con un firewall instalado.

5. TIPOS DE REGLAS

El tipo de reglas y funcionalidades que se pueden construir en un firewall son las siguientes:

* Administrar los accesos de los usuarios a los servicios privados de la red como por ejemplo aplicaciones de un servidor.
* Registrar todos los intentos de entrada y salida de una red.
* Filtrar paquetes en función de su origen, destino, y número de puerto. Esto se conoce como filtro de direcciones.
* Filtrar determinados tipos de tráfico en nuestra red u ordenador personal. Esto también se conoce como filtrado de protocolo. El filtro de protocolo permite aceptar o rechazar el tráfico en función del protocolo utilizado
* Controlar el número de conexiones que se están produciendo desde un mismo punto y bloquearlas en el caso que superen un determinado límite. De este modo es posible evitar algunos ataques de denegación de servicio.
* Controlar las aplicaciones que pueden acceder a Internet. Así por lo tanto podemos restringir el acceso a ciertas aplicaciones.
* Detección de puertos que están en escucha y en principio no deberían estarlo. Así por lo tanto el firewall nos puede advertir que una aplicación quiere utilizar un puerto para esperar conexiones entrantes.

6. IMPORTANCIA DE UN FIREWALL

Uno de los aspectos fundamentales para la seguridad de nuestra computadora es la instalación de un **firewall** junto con un antivirus de calidad. Es importante instalar esta medida de protección cuando utiliza su computadora para el acceso a internet. El firewall crea una barrera entre los datos privados de nuestra computadora y las amenazas externas que nos pueden atacar cuando estamos conectados a una red.

PREGUNTAS A RESPONDER:

1. ¿Qué es un firewall?
2. ¿Cómo funciona y cuáles son los tipos de firewall que existen?
3. ¿Por qué creen que es importante el firewall?