## **¿Qué es un Firewall?**

Un firewall, también llamado cortafuegos, es un **sistema cuya función es prevenir y proteger a nuestra red privada**, de intrusiones o ataques de otras redes, bloqueando el acceso.

Permite el **tráfico entrante y saliente que hay entre redes** u ordenadores de una misma red. Si este tráfico cumple con las reglas previamente especificadas podrá acceder y salir de nuestra red, si no las cumple este tráfico es bloqueado.

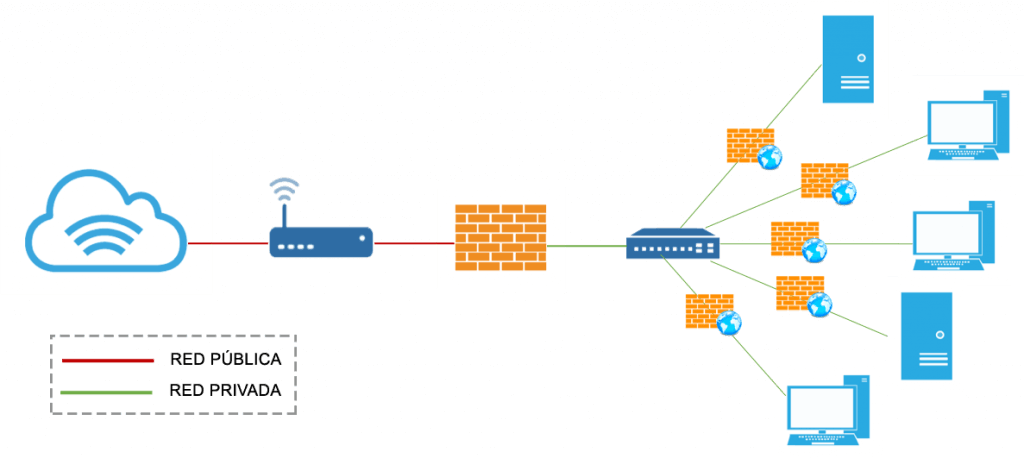
De esta manera impedimos que **usuarios no autorizados accedan a nuestras redes privadas** conectadas a internet

Se puede implementar en forma de hardware, de software o en una combinación de ambos.



## **¿Cuáles son las funciones de un Firewall?**

* Crear una **barrera que permita o bloquee intentos** para acceder a la información en su equipo.
* **Evitar usuarios no autorizados** accedan a los equipos y las redes de la organización que se conectan a Internet.
* Supervisar la **comunicación entre equipos** y otros equipos en Internet.
* **Visualizar y bloquear aplicaciones** que puedan generar riesgo
* Advertir de **intentos de conexión** desde otros equipos.
* Advertir de **intentos de conexión mediante las aplicaciones** en su equipo que se conectan a otros equipos.
* **Detectar aplicaciones y actualizar** rutas para añadir futuras fuentes de información
* Hacer frente a los **cambios en las amenazas** para la seguridad



## **Métodos de filtración del tráfico**

**Políticas de Firewall:**

Permiten bloquear o permitir determinados tipos de tráfico de red no especificados en una política de excepciones. EL cortafuegos suspende cualquier petición de comunicación que no provenga de la red interna o del propio sistema de modo Nadie va a poder escanear la red, desde el exterior sólo se ve la dirección IP del cortafuegos, no se ven recursos internos dentro de la red. También define qué funciones del cortafuegos se activan o desactivan.

**Anti-Spam Firewall:**

Este servicio protege contra el spam, phishing, la tecnología proviene de la detección de patrón recurrente (RPD).

Analiza la capacidad a través de millones de nuevos patrones a diario para bloquear todos los mensajes infectados en tiempo real. Además, el antispam se aplica a la IP remitente basado en reputación para eliminar más del 80% del correo electrónico no deseado, evitando mensajes sospechosos.

**Antivirus Firewall:**

Servicio que incorporan algunos Firewall, es la primera línea de defensa para proteger la red interna contra ataques que provengan de Internet o enlace WAN.

**Filtrado de Contenido:**

Permite a los administradores a través de un sistema de reglas de exclusión bloquear fácilmente algunos tipos de contenido web sin tener que hacerlo manualmente con cada URL individual. Se bloquean sitios web inapropiados y sitios web de redes sociales de forma rápida y sencilla. El firewall distingue entre los contenidos problemáticos, sospechosos o inseguros.

**Servicio Gestionado WAP:**

Permite controlar los dispositivos WAP (**estándar de comunicaciones sin hilos que permitirá la utilización de dispositivos móviles)** y administrar el uso para usuarios autorizados y servicios definidos.

Se llama así a los procedimientos de Inspección Profunda de Paquetes (IPP o DPI por sus siglas en inglés: *Deep Package Inspection*). Permite al administrador controlar aplicaciones específicas conocidas como troyanos y aplicaciones de puerta trasera que pueden infiltrarse en su

red interna.

Su función es añadir una segunda capa de seguridad al sistema, revisando el contenido profundo de los paquetes de información recibidos, proporcionando al administrador la flexibilidad para bloquear programas específicos que no están permitidos en la red.

## **Tipos de Firewall:**

**Diferenciamos dos tipos de firewalls**, destinados a diferentes tipos de infraestructuras y tamaños de red.

**Firewall por Hardware:**

Esta clase de sistema se instala en los routers que se utilizan para acceder a Internet, todos los ordenadores que están detrás del router estarán protegidos pero el firewall. La mayoría de routers ya vienen con el firewall instalado, es recomendable tener routers con el firewall ya instalado debido a la complejidad de instalar este posteriormente.



[**https://eu.protectli.com/**](https://eu.protectli.com/)

**Firewall por Software:**

Encontramos los gratuitos, son firewalls básicos para ordenadores de carácter personal, los cuales **monitorean y bloquean, siempre que necesario, el tráfico de Internet**. Actualmente la gran mayoría de las PC ya disponen de firewall instalado independientemente del sistema operativo instalado.

Los de pago, cuentan con similar funcionamiento, pero agregando **superiores niveles de control** y protección además de un **control muy superior sobre su configuración y funcionamiento**. Son utilizados a nivel empresarial para una **mayor protección de las organizaciones**, ya que los de uso gratuito se quedan cortos de prestaciones.

Pueden ser fácilmente **integrados con otros productos de seguridad** y no necesitan hardware para su instalación.

Es posible y muy recomendable tener un **firewall por hardware** y un **firewall por software** activos simultáneamente para lograr una mayor protección.

## **Beneficios**

Un Firewall configurado y administrado de forma correcta permite mantener a salvo la información confidencial de cualquier organización y de sus usuarios. Gracias al firewall podremos

* Definir una barrera manteniendo a un lado a los usuarios sin autorización.
* Monitorizar y registrar servicios utilizados para usar Internet, FTP y otros protocolos.
* Prevenir ataques hacia la red privada desde otras redes externas.
* Controlar la seguridad de tu red y equipos individualmente cuando se produce cualquier actividad sospechosa.
* Controlar el uso de Internet bloqueando o desbloqueando material inapropiado o apropiado.