# 

# 

# **Tipos de firewall: características y recomendaciones de uso**

Hoy día existen muchos tipos de firewall diferentes entre los que elegir. Sin embargo, la mayoría de los responsables de seguridad de la información son conscientes de que proteger los datos simplemente construyendo un cortafuegos alrededor de un sistema de información ya no es suficiente.

Aun así, siguen siendo un componente importante en la arquitectura de TI para salvaguardar la información.

Los cortafuegos han existido desde finales de la década de los 80, inicialmente erigidos alrededor de los perímetros de la red para controlar el flujo de tráfico y proteger los datos dentro de los ordenadores que actuaban como host. Pero la informática ha cambiado drásticamente desde que Digital Equipment Corp. desarrolló el firewall de filtro de paquetes en 1988.

Estos sistemas han evolucionado en los últimos años y, aunque su funcionalidad básica se ha mantenido igual, sus capacidades se han expandido enormemente.

Fuente: [Esenciales para garantizar seguridad, así son los tipos de firewall | OBS Business School](https://www.obsbusiness.school/blog/tipos-de-firewall-caracteristicas-y-recomendaciones-de-uso)

¿A qué nos exponemos? Sin un cortafuegos, tu sitio web e incluso tus dispositivos personales son vulnerables a los ataques DDoS, un vector de ataque que envía miles o millones de paquetes falsos para sobrecargar tu servidor y hacer que tu sitio web o Internet se caiga.

¿No te hemos convencido? El cortafuegos puede protegerte a ti o a tu sitio web frente a:

* Intrusiones: Los cortafuegos impiden a los usuarios no autorizados acceder a tu ordenador o servidor de forma remota y hacer lo que quieran.
* Malware: Los atacantes que logran infiltrarse pueden enviar malware para infectarte a ti o a tu servidor. El malware puede robar información personal, propagarse a otros usuarios o dañar de alguna manera tu computadora.
* Ataques de fuerza bruta: Intentos de los hackers de probar cientos de combinaciones de nombres de usuario y contraseñas para descubrir las credenciales de acceso de su administrador (o de otros usuarios).
* Ataques DDoS: Los cortafuegos (especialmente los de aplicaciones web) pueden intentar detectar la afluencia de tráfico falso que se produce durante un ataque DDoS.

## **Tipos de cortafuegos**

Hay muchos tipos diferentes de cortafuegos, cada uno está diseñado para una situación diferente. Algunos son mejores para ordenadores individuales, mientras que otros están hechos para filtrar toda la red.

* [Cortafuegos personal](https://kinsta.com/es/blog/que-es-un-cortafuegos/#cortafuegos-personal)
* [Hardware vs. Software Cortafuegos](https://kinsta.com/es/blog/que-es-un-cortafuegos/#hardware-vs-software-cortafuegos)
* [Cortafuegos de filtrado de paquetes](https://kinsta.com/es/blog/que-es-un-cortafuegos/#cortafuegos-de-filtrado-de-paquetes)
* [Cortafuegos de estado (stateful)](https://kinsta.com/es/blog/que-es-un-cortafuegos/#cortafuegos-de-estado-stateful)
* [Cortafuegos de aplicaciones web (WAF)](https://kinsta.com/es/blog/que-es-un-cortafuegos/#cortafuegos-de-aplicaciones-web-waf)
* [Cortafuegos de nueva generación](https://kinsta.com/es/blog/que-es-un-cortafuegos/#cortafuegos-de-nueva-generacin)

Todos funcionan de manera diferente y bloquean mejor diferentes tipos de tráfico. Si te preguntas qué deberías buscar, vamos a analizar todos los principales tipos de cortafuegos.

Aquí tenéis un rápido resumen: a menos que tengas tu propia pila de servidores (proporcionando un sitio web con tu propia Internet), el tipo de cortafuegos del que debes preocuparte principalmente son los cortafuegos personales, los cortafuegos de software y los cortafuegos de las aplicaciones web.

Estos tres son los más importantes. Sin embargo, lee más sobre el resto si quieres entender mejor cómo funciona un cortafuegos y cómo han evolucionado a lo largo de los años.

### **Cortafuegos personal**

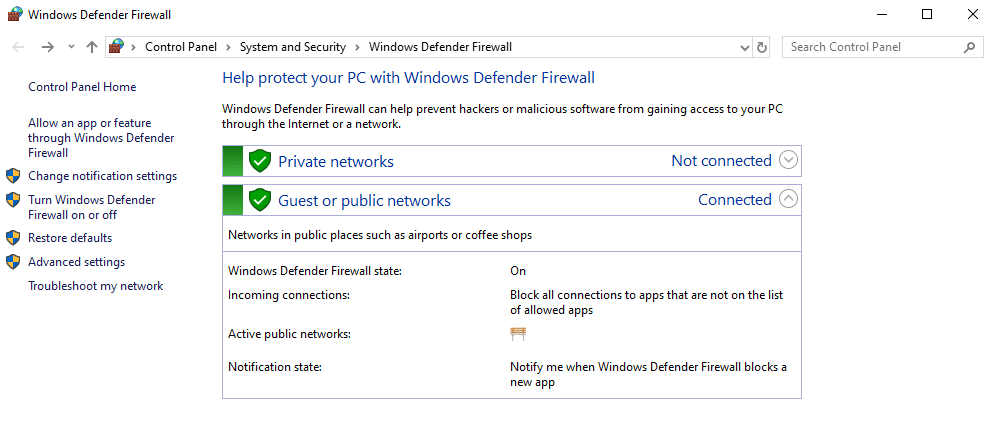
Los cortafuegos funcionan de forma muy diferente dependiendo de si son utilizados por ordenadores individuales, redes enteras (como dentro de una oficina comercial) o servidores web. Un cortafuegos personal está pensado para ser usado en un solo ordenador. Este es el firewall que viene preinstalado en las máquinas de Windows y Mac o con tu software antivirus.

Aunque funciona de manera similar a un cortafuegos de servidor – permitiendo o rechazando conexiones de otros dispositivos, aplicaciones e IPs basadas en un conjunto de reglas predefinidas – actúa de una manera un poco diferente.

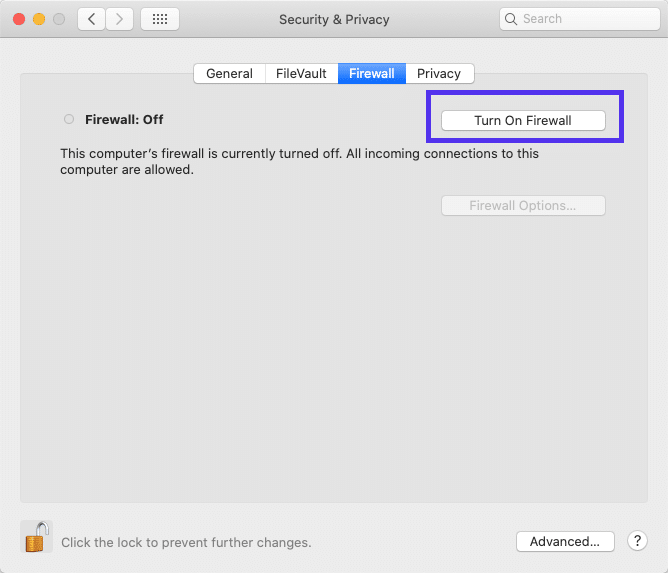
Los cortafuegos personales pueden proteger los puertos que utilizas para conectarte a sitios web y aplicaciones en línea (ocultándolos para que los atacantes no puedan ver que están abiertos), defenderse contra los ataques que se deslizan por la red, evitar que las personas accedan y se apoderen de tu equipo y analizar todo el tráfico entrante y saliente.

También actúan como aplicaciones de cortafuegos, monitoreando la actividad de las aplicaciones en tu dispositivo y negándose a permitir que se establezca una conexión con software inseguro o desconocido.

Hoy en día, obtener un cortafuegos personal es bastante fácil. Si usas cualquier versión moderna de Windows, ya debería haber uno por defecto.

Windows Defender Firewall

Los ordenadores Mac también vienen con uno, aunque tienes que encenderlo tú mismo. Para ello, navega a Preferencias del Sistema, haz clic en Seguridad y Privacidad y luego en Firewall:

Aplicación de cortafuegos en macOS

El software antivirus a menudo viene con el suyo propio también. Un ejemplo es el antivirus Avast: su software de cortafuegos es compatible con Windows y sirve como una segunda capa de defensa.

También existen cortafuegos personales de terceros, pero pueden causar un conflicto con la configuración predeterminada.

### **Hardware vs. Software Cortafuegos**

Los cortafuegos tienen dos formas distintas: cortafuegos de hardware y de software. Los cortafuegos de software son programas descargables para tu ordenador, monitoreando todo desde un panel de control central. Los cortafuegos de hardware proporcionan una funcionalidad similar, pero están físicamente instalados en el edificio.

Puede que no lo sepas, pero probablemente tengas una forma de cortafuegos de hardware en tu casa: tu router, el dispositivo que te permite conectarte a Internet. Si bien no es exactamente lo mismo que un dispositivo de cortafuegos de hardware dedicado, proporciona funciones similares de monitoreo y de permitir o negar conexiones.

Tanto el software como el hardware de los cortafuegos se sitúan entre el ordenador y el mundo exterior, analizando cuidadosamente cualquier conexión que intente colarse. Puedes tener uno o ambos funcionando en tu red.

Sin embargo, los cortafuegos de hardware tienen algunas desventajas. Son difíciles de instalar y requieren un mantenimiento continuo, por lo que no suelen ser adecuados para ordenadores individuales o empresas muy pequeñas sin un departamento de informática. Pueden causar problemas de rendimiento, especialmente cuando se aplican junto con un cortafuegos de software. Y no son adecuados para bloquear aplicaciones en un dispositivo, o restricciones basadas en el usuario.

Por otro lado, un cortafuegos de hardware protegerá toda su red de ordenadores fácilmente, mientras que la configuración del software para ello es una tarea más difícil. Y aunque un atacante puede deshabilitar el software si logra entrar, no puede manipular el dispositivo físico.

Los cortafuegos de software son, como su nombre indica, mejores para trabajar con programas en un ordenador. Bloquear aplicaciones, administrar usuarios, generar registros y monitorear usuarios en tu red son su especialidad. No son tan fáciles de configurar en toda la red, pero cuando se instalan en múltiples dispositivos, permiten un control más fino.

### **Cortafuegos de filtrado de paquetes**

El cortafuegos de filtrado de paquetes es el tipo más simple de cortafuegos, y está entre los primeros desarrollados. Un paquete es la información que se intercambia entre tu ordenador y un servidor. Cuando haces clic en un enlace, subes un archivo o envías un correo electrónico, envías un paquete al servidor. Y cuando cargas una página web, te envía paquetes a ti.

Un cortafuegos con filtro de paquetes analiza estos paquetes y los bloquea basándose en un conjunto de reglas predefinidas. Por ejemplo, podría bloquear los paquetes que se originan en un determinado servidor o dirección IP, o los que intentan llegar a un determinado destino en tu servidor.

La desventaja: Estos tipos de cortafuegos son simples y fáciles de engañar. No hay forma de aplicar reglas avanzadas. Si permites que el tráfico fluya a través de un determinado puerto, el cortafuegos de filtrado de paquetes dejará pasar cualquier cosa, incluso el tráfico que los cortafuegos modernos obviamente no dejarían pasar.

La única ventaja de estos es que son tan simples que casi no tienen impacto en el rendimiento. No inspeccionan el tráfico, no guardan registros ni ejecutan ninguna función avanzada. Hoy en día, los cortafuegos de filtrado de paquetes deberían evitarse o al menos usarse junto con algo más avanzado, ya que hay soluciones mucho mejores.

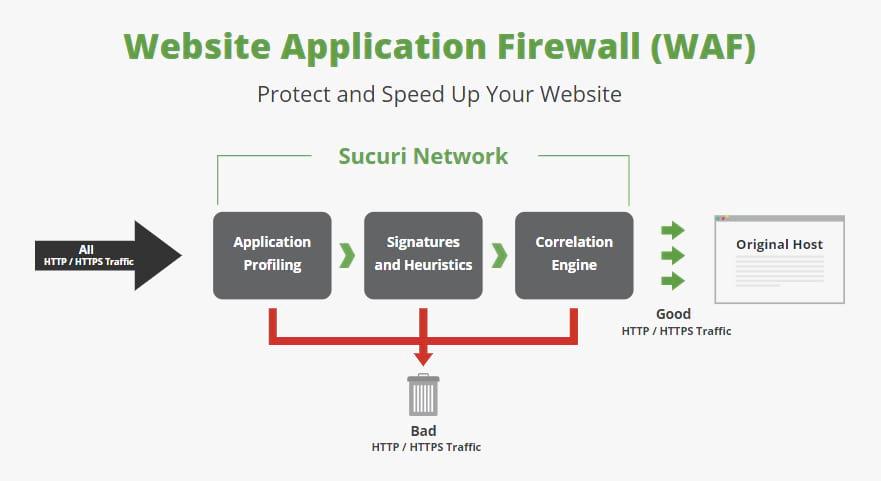
### **Cortafuegos de estado (stateful)**

Después de los «sin estado», los filtros de paquetes simples llegó la tecnología de los cortafuegos de estado. Esto fue revolucionario porque en lugar de analizar los paquetes a medida que pasan y rechazarlos basándose en parámetros simples, los cortafuegos de estado manejan información dinámica y continúan monitoreando los paquetes a medida que pasan por la red.

Un simple cortafuegos de filtrado de paquetes sólo puede bloquear [basado en información estática como la dirección IP](https://kinsta.com/es/base-de-conocimiento/bloquear-direccion-ip/) o el puerto. Los cortafuegos de estado son mejores para detectar y bloquear el tráfico ilegítimo porque reconocen patrones y otros conceptos avanzados.

Comparado con los cortafuegos sin estado, la desventaja es que son más intensivos debido a que almacenan paquetes de datos en la memoria y los analizan más rigurosamente, además de mantener registros de lo que se bloquea y lo que pasa a través de ellos. Pero son una solución mucho mejor.

### **Cortafuegos de aplicaciones web (WAF)**

****Cómo funcionan los WAF

Si bien la tecnología de estado se sigue utilizando hoy en día, ya no es suficiente por sí sola para mantener una red segura de manera efectiva. Los cortafuegos de aplicaciones y [los cortafuegos de aplicaciones web](https://kinsta.com/es/blog/sucuri-contra-wordfence/) fueron el siguiente gran paso.

Los cortafuegos tradicionales solo monitorean el tráfico general en una red. Luchan o fallan completamente en la detección del tráfico que entra o sale de una aplicación, servicio u otro software. Los cortafuegos de aplicaciones fueron diseñados para trabajar con estos programas, capturando los intentos de intrusión que se aprovechan de las [vulnerabilidades](https://kinsta.com/es/base-de-conocimiento/divulgar-vulnerabilidad-de-seguridad/) del software para pasar por encima de los cortafuegos más antiguos.

También podrían funcionar como un sistema de control parental para un negocio, bloqueando el acceso a ciertas aplicaciones y [sitios web por completo](https://kinsta.com/es/blog/bloquear-sitios-web-chrome/).

Los cortafuegos de aplicaciones web funcionan de manera similar, pero supervisan las aplicaciones web en lugar de los programas de un ordenador. Algunos ejemplos de aplicaciones web son los plugins de formularios o carritos de compras de terceros, que a veces pueden ser secuestrados para enviar malware a su servidor. Sin un WAF, eres vulnerable [a estos ataques](https://kinsta.com/es/blog/ajustes-cloudflare-wordpress/#how-to-configure-cloudflare-settings-for-wordpress).

Muchos WAF están basados en la nube, lo que significa que no necesitas hacer ningún cambio radical en tu servidor para configurarlos. Pero también pueden existir en el hardware o en el software del servidor.

Si necesitas un servicio de cortafuegos para proteger tu sitio web, busca un WAF basado en la nube como [Cloudflare](https://kinsta.com/es/blog/ajustes-cloudflare-wordpress/) o [Sucuri](https://kinsta.com/es/blog/sucuri-firewall/). Estos pueden ser instalados sin tener que jugar con configuraciones sensibles del host de la web o configurar hardware costoso.

### **Cortafuegos de nueva generación**

Por último, los cortafuegos de nueva generación (NGFW), son uno de los inventos más recientes de esta generación de tecnología de seguridad. Estas herramientas de grado empresarial son como todas las anteriores combinadas en una sola. El filtrado profundo de paquetes, la prevención de intrusos y el monitoreo de aplicaciones son solo algunas de sus enormes características de red.

Los cortafuegos de última generación en la nube existen como un servicio en línea, pero los WAF son mucho más comunes y proporcionan una funcionalidad similar. Pero si quieres la tecnología de cortafuegos más avanzada disponible, con un paquete [completo de protección de seguridad en un programa](https://kinsta.com/es/blog/seguridad-nube/), busca un NGFW.

## **Cómo conseguir un cortafuegos**

Para protegerse a sí mismo y a tu sitio web, necesitas un cortafuegos de alta calidad que mantenga alejado a los intrusos.

En lo que respecta a los cortafuegos personales, no suele ser necesario hacer un esfuerzo para conseguir uno. El cortafuegos incorporado de Windows funciona muy bien sin ninguna configuración. Y entre el cortafuegos de aplicaciones que suele venir con el software antivirus y el filtro de paquetes del router, el equipo suele estar más que protegido.

Solo asegúrate de que tu cortafuegos esté activado, que tengas un buen antivirus instalado y que tu router esté configurado correctamente. Lo mismo puede decirse de los usuarios de MacOS.

¿Pero qué pasa si tienes un [sitio web que necesita protección](https://kinsta.com/es/wordpress-hosting-seguro/)?

Es muy diferente entonces. No hay tantas herramientas incorporadas para protegerte, y a menudo depende de ti asegurar tu sitio web. Por ejemplo, si estás ejecutando WordPress, no hay un firewall ni nada que proteja tu servidor y [los plugins de seguridad](https://kinsta.com/es/wordpress-hosting-seguro/) son una de las opciones más comunes.

[Los desarrolladores de WordPress](https://kinsta.com/es/blog/contratar-desarrollador-de-wordpress/) hacen todo lo posible para mantener el código optimizado, pero cuando surgen vulnerabilidades, no tienes nada para evitar las intrusiones.

Todos los sitios pueden beneficiarse de una WAF. Servicios en línea como [Sucuri](https://kinsta.com/es/blog/sucuri-contra-wordfence/#sucuri-review), [Wordfence](https://kinsta.com/es/blog/sucuri-contra-wordfence/#wordfence-review), [Cloudflare](https://kinsta.com/es/base-de-conocimiento/instalar-cloudflare/) pueden tener uno instalado en tu servidor en minutos.