Cómo abrir y cerrar puertos en el firewall de Windows 10

Cada vez son más usuarios los que se preocupan por la seguridad de sus equipos, y es que hoy en día son muchas las amenazas que circulan por la red. En este sentido, utilizar el Firewall de Windows y un antivirus es muy recomendable para velar por nuestra seguridad. Sin embargo, en ciertas ocasiones puede que necesitemos abrir o cerrar ciertos puertos para permitir determinadas conexiones. Por eso, vamos a mostrar **cómo abrir y cerrar puertos en el Firewall de Windows 10**.

Hay muchas razones por las que puedes querer abrir o cerrar puertos, tanto para acelerar tus descargas como para jugar con mayor velocidad en Internet, optimizar tu conexión o acceder a algún programa específico o configuración que lo requiere. Abrir un puerto permitirá que más datos entren o salgan de tu ordenador y cerrarlos evite ataques por medio de ellos. Los puertos son como **la puerta de entrada y salida de los paquetes de datos** de nuestras conexiones. Es decir, si abrimos un puerto, podremos establecer una conexión a través de él permitiendo la entrada y salida de datos. En **Windows 10 podemos abrir o cerrar puertos del Firewall** de sistema desde el propio centro de seguridad o bien desde el antiguo panel de control.

¿Qué es el firewall o cortafuegos?

Como su propio nombre indica, el cortafuegos de un ordenador (o firewall en su término en inglés) es una tecnología o sistema de seguridad cuya finalidad es bloquear los **posibles accesos no autorizados** que se hagan a un ordenador. Es una medida de seguridad que podemos tener en nuestro equipo **para evitar malware o virus.** Especialmente pensado para redes locales o intranets y uno de los “primeros” antivirus utilizados en cualquier sistema, en marcha desde los años ochenta y que, en el caso de Windows, ya está instalado y no tenemos que hacer nada salvo saber cómo abrir o cerrar los puertos, tal y como veremos en los siguientes párrafos.

El **Firewall de Windows** es la herramienta perfecta para proteger el equipo ante virus cuando estás navegando por Internet. Previene los accesos no autorizados a una red para que otras personas no puedan controlar tus dispositivos y robar tus datos personales, entre muchas otras cosas. Es esencial para que las empresas se protejan de amenazas internas o externas. Lo más recomendable es **tenerlo activado**, e incluso configurarlo de acuerdo a tus necesidades si tienes mayores conocimientos informáticos.

Puede que una de las cosas que no sepas es que con esta herramienta de seguridad de tu ordenador puedes abrir o cerrar puertos a tu conveniencia, siempre sabiendo lo que haces, por lo que vamos a comentarte cómo puedes hacerlo fácilmente de dos formas diferentes. Abrir un puerto de tu firewall en concreto hará posible que más datos entran y salgan desde tu ordenador. Hay muchas razones por las que puedes querer abrir puertos, como facilitar el juego online con más personas, aunque también muchas otras por las que vas a querer cerrar puertos cuando no los necesites abiertos o para mayor seguridad. Lo mejor de todo es que para hacerlo no necesitas cambiar ningún proceso crítico de tu sistema operativo.

Funcionalidades prácticas para su uso

Antes de adentrarnos en profundidad en cómo podemos hacer para abrir o cerrar estos puertos, debes saber que **no es una configuración o un elemento común**, o mejor dicho: no es algo del que los usuarios habitualmente configuren o pongan en práctica.

La razón es porque estos no son elementos que nos permiten establecer una conexión entre el **ordenador y otro punto** como puedes ser páginas o servidores de correo electrónico. Por eso, y como cualquier otra actividad o acción en Internet o en el propio PC, antes de abrir puertos Windows 10 debemos de saber lo que estamos haciendo (y qué es lo que va a pasar).

Ante esto, y si nos decantamos por abrir o cerrar puertos Firewall Windows 10, hay que saber que los más conocidos serán fáciles de usar por otros usuarios. Así, si queremos que **nuestra red funcione a la perfección** y estar lo más seguros posible, podemos configurar su comportamiento, sobre todo para elegir los puertos a través de los cuales queremos que las aplicaciones se conecten a Internet, impidiendo que puedan comunicarse a través de los demás. Como veremos en su configuración, esto tiene varios usos:

- Acelerar las descargas
- Jugar con mayor velocidad en Internet
- Optimizar tu conexión
- Acceder a programas específico o configuraciones que lo requieran

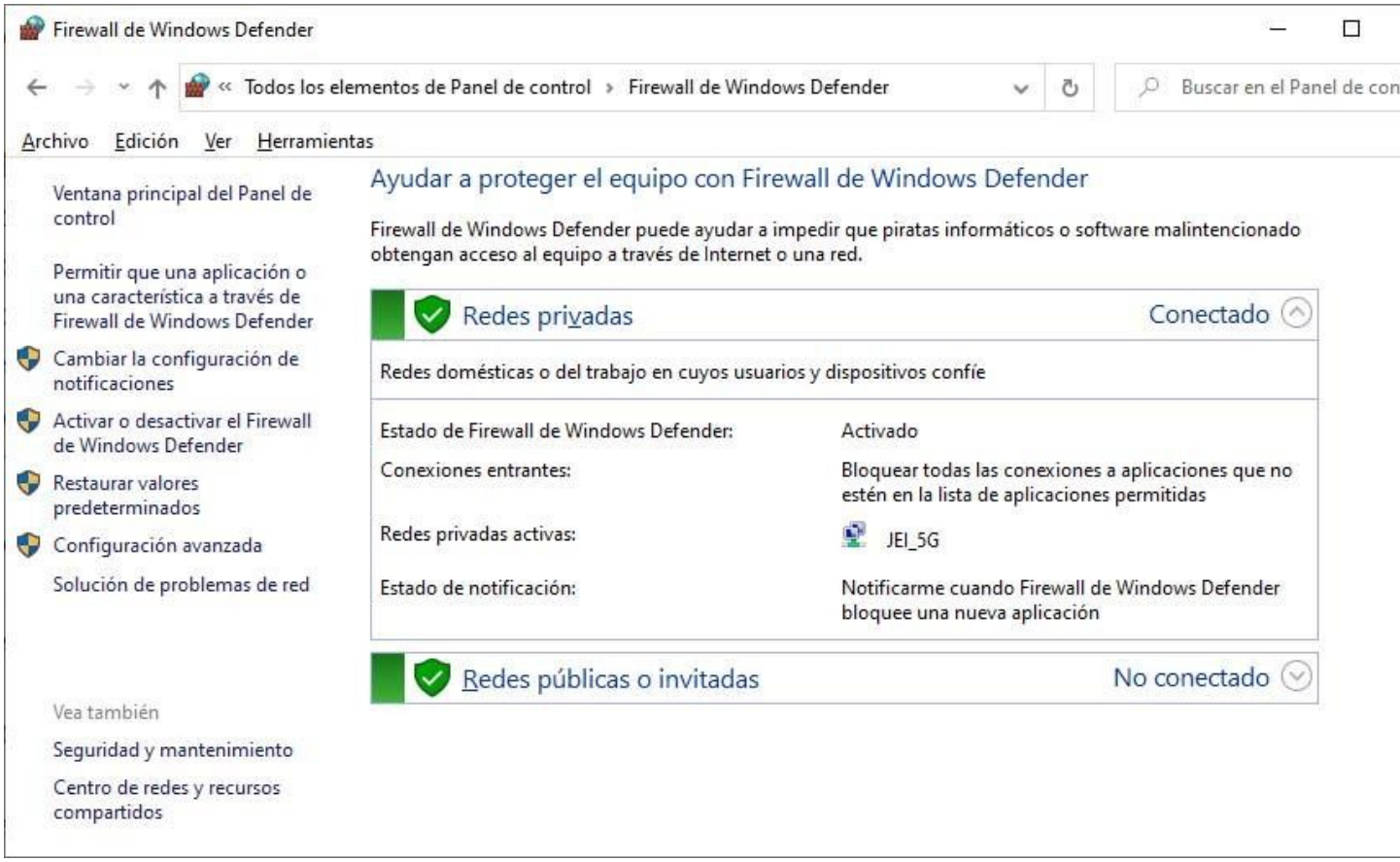
Abrir o cerrar puertos en Windows 10

Con la llegada de Windows 10, Microsoft incorporó la nueva **página de Configuración** del sistema, que se suponía iba a ser la que sustituiría al panel de control. Sin embargo, después de varios años, ambas opciones siguen conviviendo en el sistema.

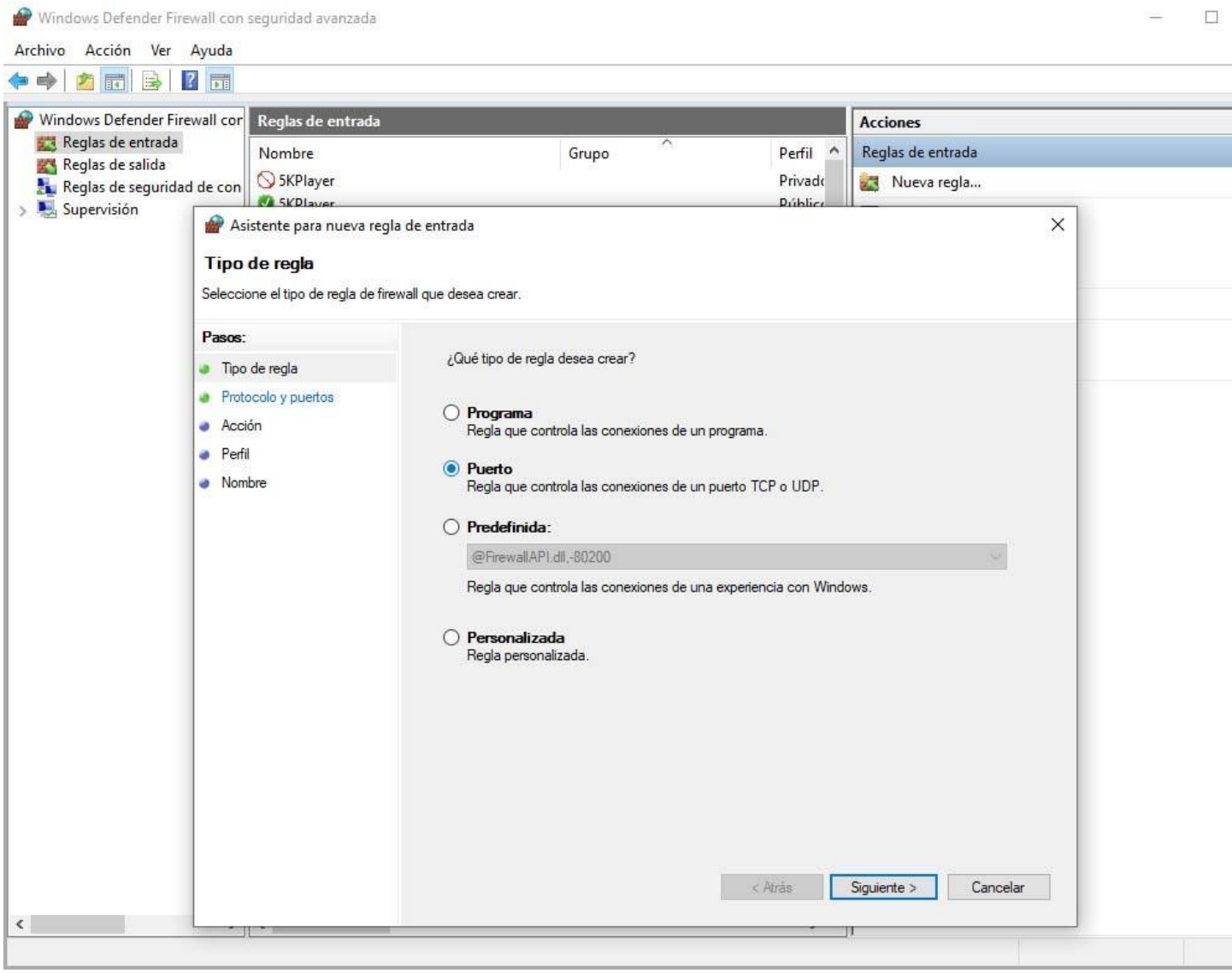
Haya ciertos ajustes que únicamente los encontramos en la página de configuración, mientras que otros solo están disponibles **en el panel de control**, pero en esta ocasión, es posible abrir o cerrar puertos en el Firewall de Windows 10 tanto desde un sitio como desde otro. Por lo tanto, si hemos instalado alguna aplicación, necesitamos realizar la descarga de ciertos archivos o necesitamos abrir algún puerto para poder disfrutar de algún juego, estos son los pasos que tenemos que seguir para ello.

Desde el panel de control

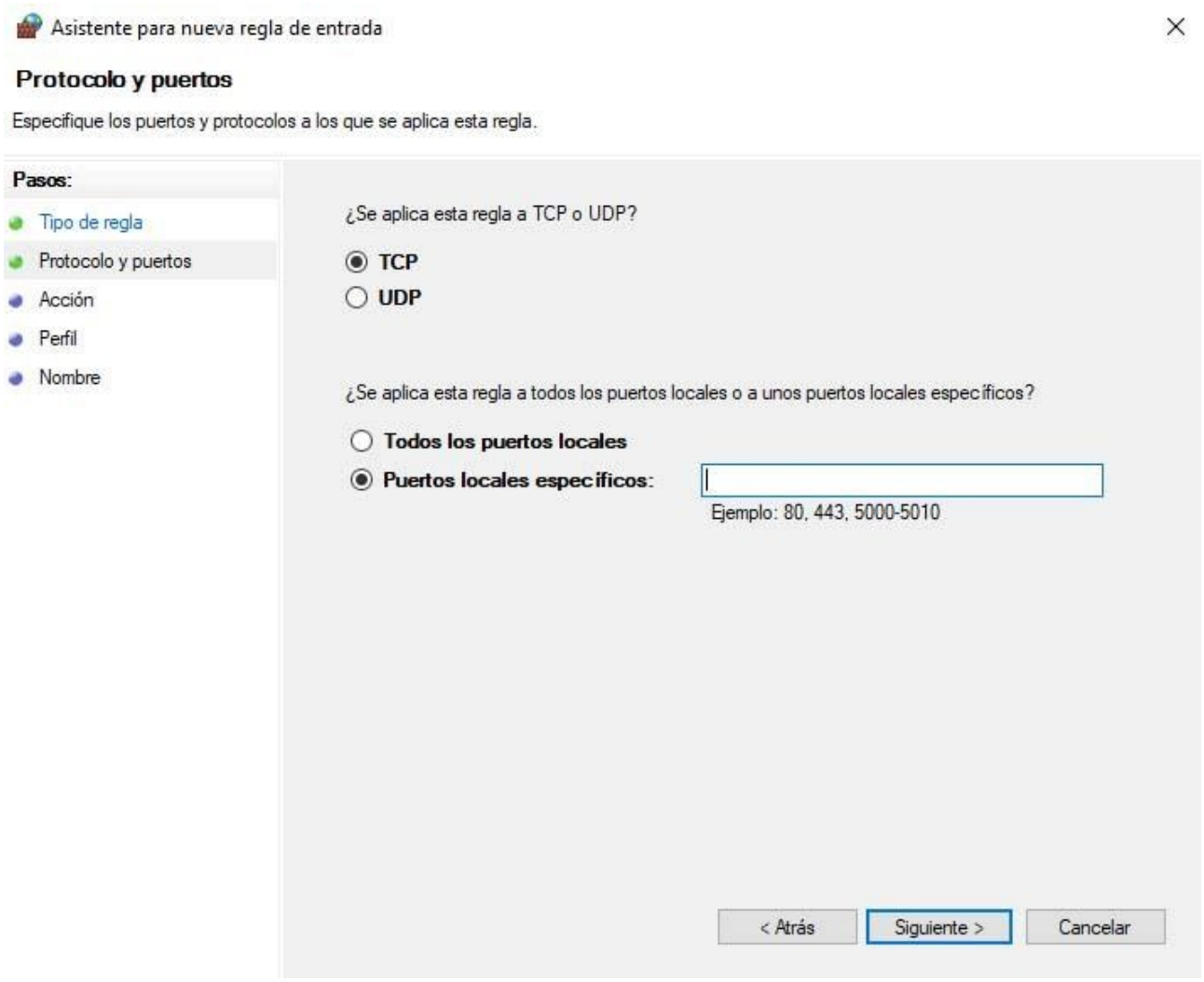
Para hacerlo desde el **Panel de control**, lo primero que tenemos que hacer es abrir el propio panel, y a continuación seleccionar la opción Firewall de Windows Defender. En la ventana que se nos muestra, hacemos clic en la opción Configuración avanzada del menú lateral izquierdo (tal y como puedes ver en la captura de pantalla siguiente) y esto nos abrirá el panel del Firewall de Windows 10. Una vez hecho esto, estos son los pasos a seguir:



- Seleccionamos **Reglas de Entrada** si queremos abrir un puerto o bien **Reglas de Salida** si lo que queremos es cerrarlo
- En el panel de la derecha hacemos clic en el apartado «nueva regla»
- A continuación, se nos pedirá que indiquemos el tipo de regla
- Seleccionamos **Puerto**
- Pulsamos en Siguiente para seguir configurándolo



- Ahora elegimos el tipo de **tráfico TCP o UDP**
- Elige también el número de puerto sobre el que queremos aplicar la regla que vamos a configurar
- En el siguiente paso, debemos definir si queremos **bloquear el tráfico, permitirlo o ambas cosas**.



- Pulsamos en siguiente y a continuación debemos indicar cuándo se aplicará la regla.
- Por último, le damos un nombre a la regla que acabamos de crear en el Firewall de Windows 10.

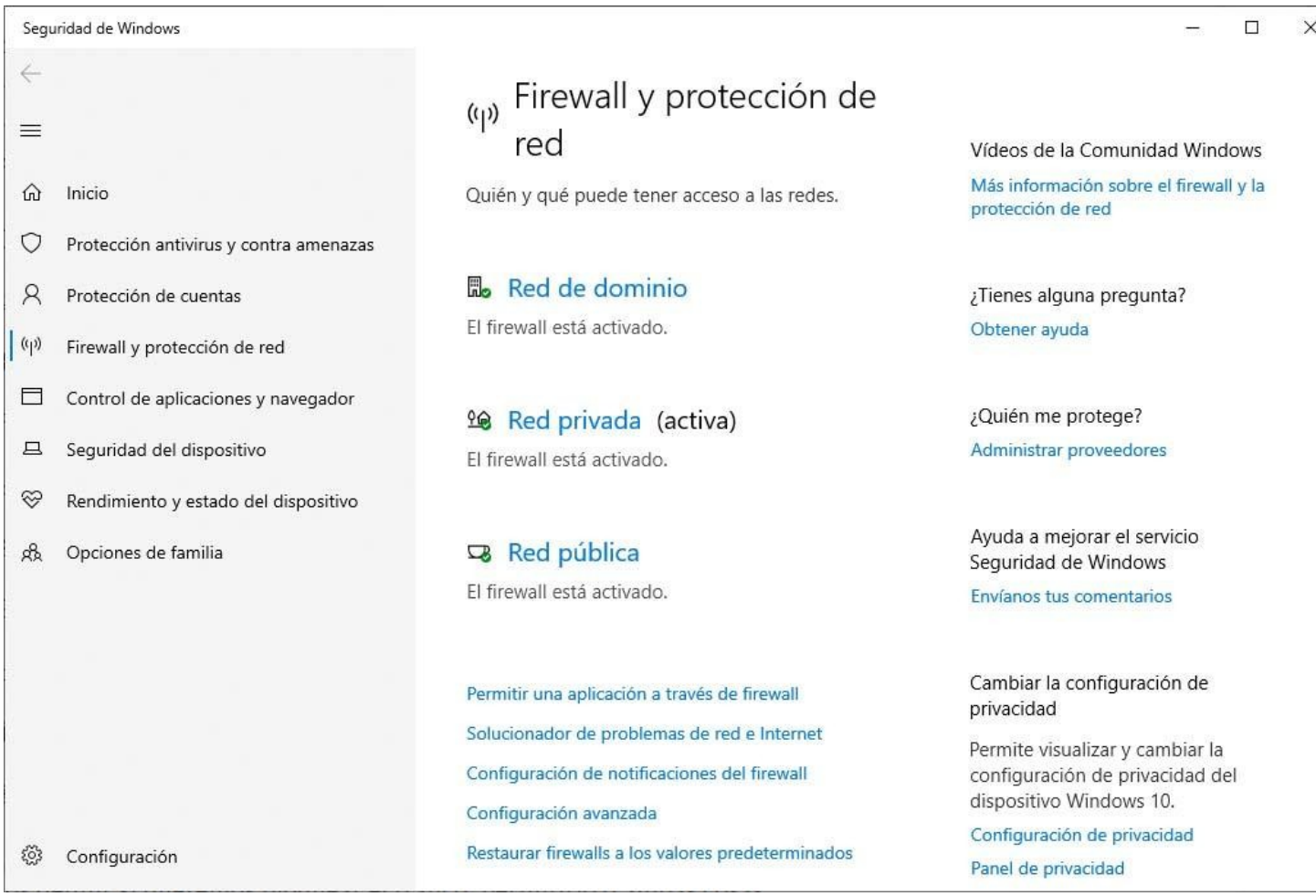
Si todo ha ido bien, veremos en el panel central de la ventana de configuración avanzada del Firewall la regla que hemos creado. Si lo que hemos hecho es permitir una conexión, **abrir puerto**, se mostrará con el icono en color verde, mientras que, si la regla ha sido para bloquear una conexión o cerrar un puerto, aparecerá el icono rojo con el símbolo de prohibido.

Desde la página de Configuración

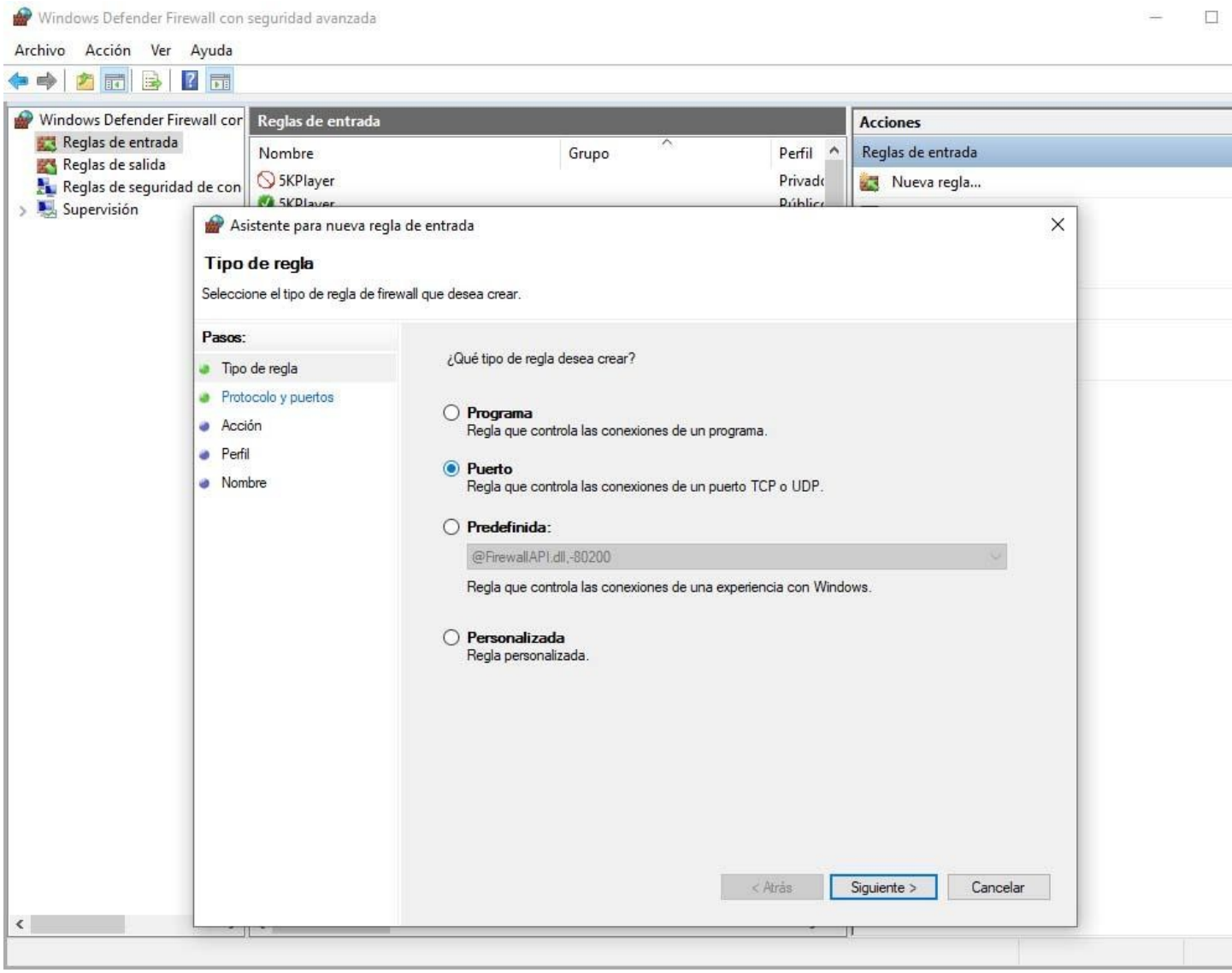
Otra opción recomendable para abrir o cerrar puertos del cortafuegos o firewall en Windows es hacerlo desde la Configuración del sistema. Si somos de los que ya nos hemos olvidado del Panel de Control, no sabemos cómo utilizarlo o nos parece complejo, hay alternativa. Si preferimos acceder a los ajustes para abrir o cerrar puertos de Firewall de Windows 10 desde la página de configuración, estos son los pasos a seguir para ello:

- Abrimos la página de Configuración del sistema, Win+I, o desde el Inicio en el icono de engranaje
- Seleccionamos la opción **Actualización y Seguridad.**

- Hacemos clic sobre la opción **Seguridad de Windows** del menú lateral izquierdo.
- Dentro del apartado Áreas de protección, seleccionamos la opción **Firewall y protección de red**.
- Esto nos abrirá el centro de seguridad de Windows Defender donde tenemos que hacer clic sobre la opción Configuración avanzada.



- Esto nos abrirá la ventana de **configuración avanzada** de Windows Defender Firewall.
- Seleccionamos **Reglas de Entrada o Salida** dentro de Windows Defender Firewall. En función si queremos abrir o cerrar puertos
- En el panel de la derecha hacemos clic en **nueva regla.**
- A continuación, se nos pedirá que indiquemos el tipo de regla. Seleccionamos **Puerto** y pulsamos en Siguiente.



- Ahora elegimos el tipo de **tráfico TCP o UDP** y el número de puerto sobre el que queremos aplicar la regla.
- En el siguiente paso, debemos definir si queremos **bloquear el tráfico, permitirlo o ambas cosas.**
- Pulsamos en siguiente y a continuación debemos indicar cuándo se aplicará la regla.
- Por último, le damos un nombre a la regla que acabamos de crear en el Firewall de Windows 10.

Si el proceso se realiza correctamente, veremos la regla que acabamos de crear para abrir o cerrar un puerto en el Firewall del sistema en el panel central de la ventana de configuración avanzada.

En cualquier caso, si queremos cerrar un puerto que hemos abierto mediante una regla de entrada, lo único que tenemos que hacer es ir al listado de reglas de entrada en el panel central, hacer clic sobre ella con el botón derecho del ratón y elegir la opción **Desactivar regla o Eliminar.**

Hacerlo desde el Símbolo del sistema

Aunque los métodos anteriores son los más indicados y sencillos, con los que sabrás qué estás haciendo en todo momento, si buscas otra forma de habilitar o deshabilitar puertos más allá de lo convencional debes saber que puedes hacerlo por medio de **comandos con el símbolo del sistema**.

Así que lo que debes hacer es buscar CMD o símbolo de sistema en el buscador y **ejecutarlo como administrador.** Una vez que se abre la ventana, comprobando que lo has hecho como administrador, debes escribir **Netstat -ano** para ver la lista de puertos disponibles y su PID asociado. Encontrarás información sobre los puertos, dirección local, remota, estado, protocolo y más.

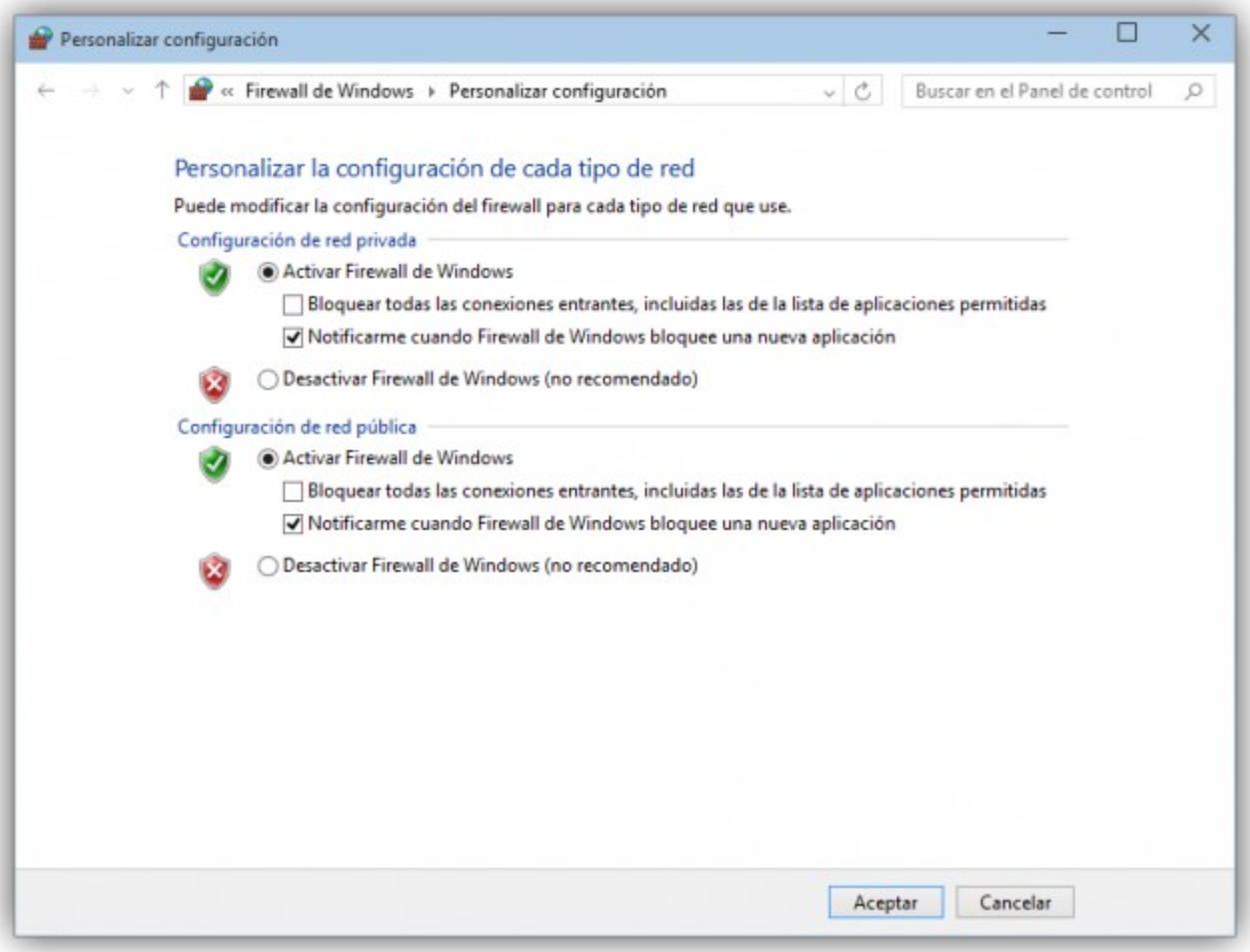
- Si buscas uno en concreto escribir *netstat -ano* | *find:xxxx* (donde las x son el número del puerto).
- Para abrir puertos, puedes escribir: *netsh advfirewall firewall add rule name=»Puerto TCP XXX» dir=in action=allow protocol=TCP localport=XXX*, donde *XXX* es el número de puerto.
- Para bloquear, es *block* donde pone *allow*. Para liberar un puerto, lo que tienes que hacer es escribir *taskkill /pid XXX /F* donde *XXX* es el PID asociado que debes conocer para realizar esta acción.

Otras opciones a configurar

Además de abrir puertos, esto es todo lo que podemos cambiar en la configuración utilizando esta herramienta de seguridad de tu sistema operativo y que debes tener en cuenta, desde su propia activación o desactivación hasta otras gestiones importantes. Puedes cerrar puertos de un proceso en concreto o realizar ciertas configuraciones clave con el cortafuegos de Windows.

Activar o desactivar el Firewall de Windows

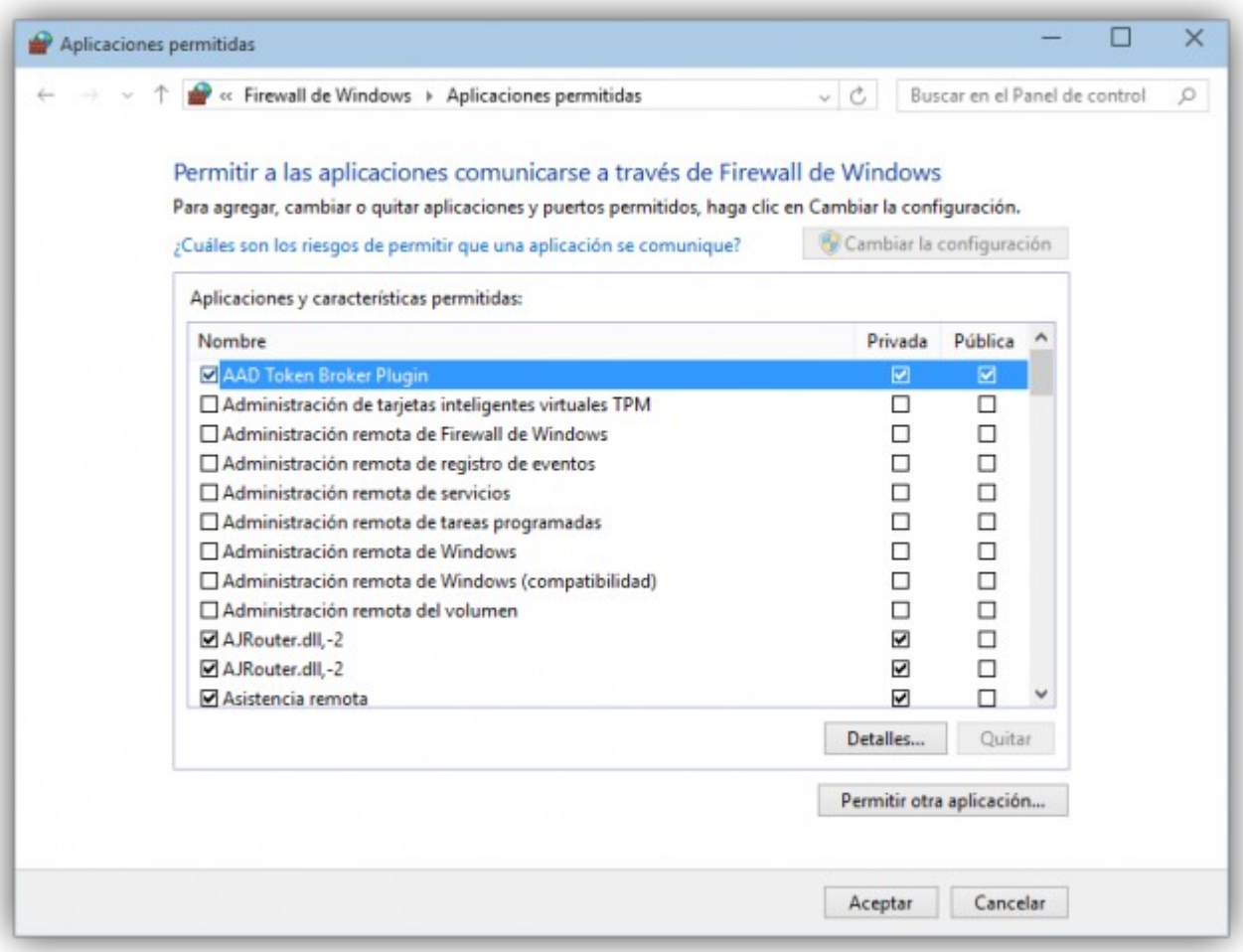
En la parte izquierda de la ventana disponemos de un menú con los diferentes apartados del mismo. Lo primero que vamos a hacer es pulsar sobre la opción **«Activar o desactivar Firewall de Windows»** para abrir una ventana desde donde podemos elegir si queremos activarlo o desactivarlo en las redes domésticas o en las redes públicas, así como si queremos bloquear todo el tráfico en alguna de ellas.



También puedes activar o desactivar el Firewall desde la **Configuración de Windows**, en actualización y seguridad, en Seguridad de Windows. Desde allí das a abrir seguridad de Windows y Firewall y protección de red. Desde ahí podrás dar a Red de dominio, red privada o red pública y dar a Activado (queda marcado en azul) o desactivado moviendo la opción desde la nueva pantalla que aparece. También puedes bloquear las conexiones entrantes o no en cada configuración.

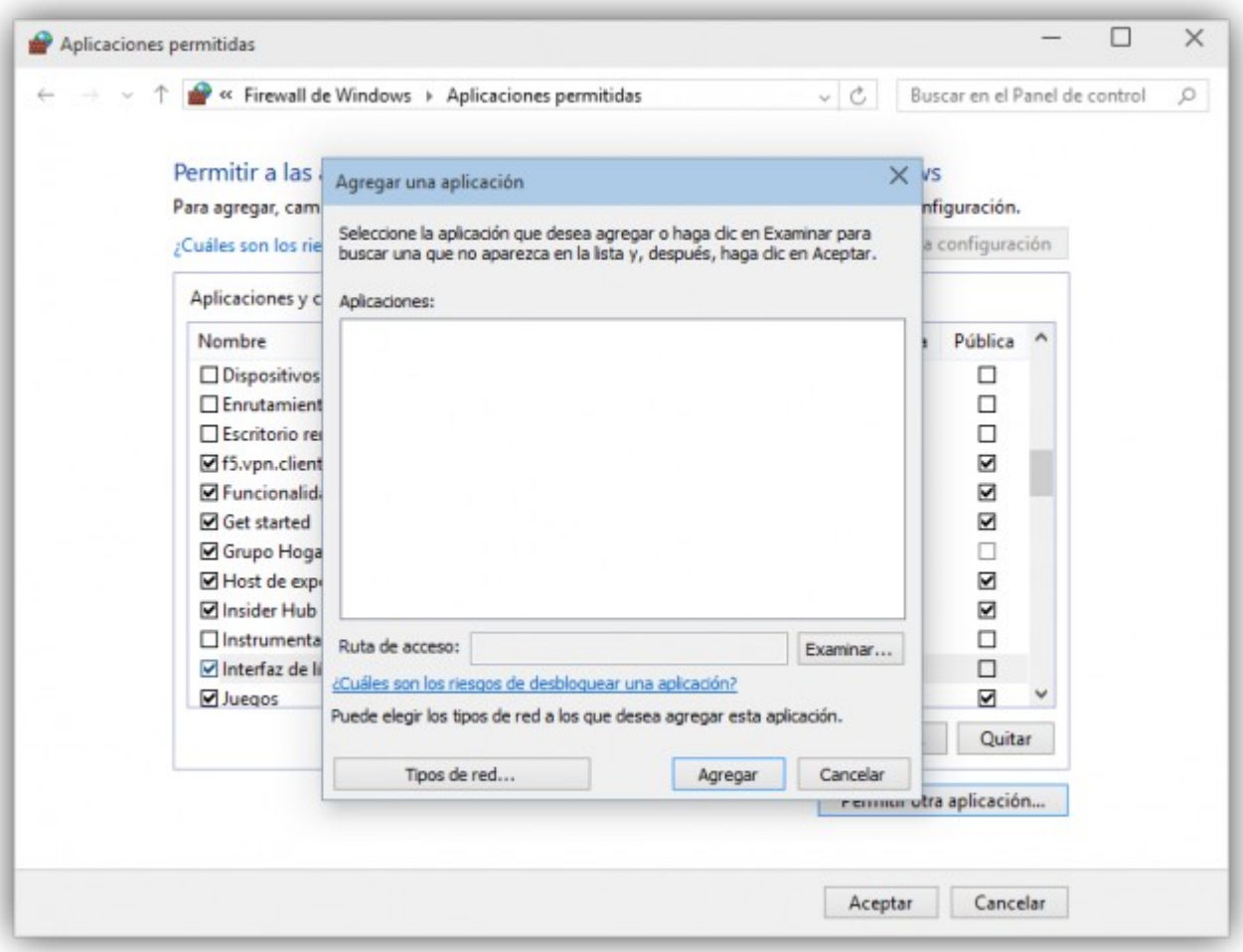
Permitir o bloquear el tráfico a aplicaciones o características

Volvemos a la ventana principal de configuración del Firewall de Windows y seleccionamos en el menú el apartado «Permitir una aplicación o una característica». Desde esta ventana vamos a poder ver todas las aplicaciones y servicios de Windows a la vez que añadir fácilmente nuevas aplicaciones que puedan conectarse a Internet fuera del filtro del cortafuegos.



Como podemos ver, nos aparece una **completa lista con todos los componentes** que, por defecto, vienen instalados en el sistema operativo y que pueden necesitar conexión a Internet para funcionar correctamente. Podemos elegir de cada componente si queremos que se conecte tanto desde una red privada personal como desde redes públicas e inseguras.

En la parte inferior podemos ver un botón llamado **«Permitir otra aplicación»** desde donde podemos añadir nuevas aplicaciones a esta lista.

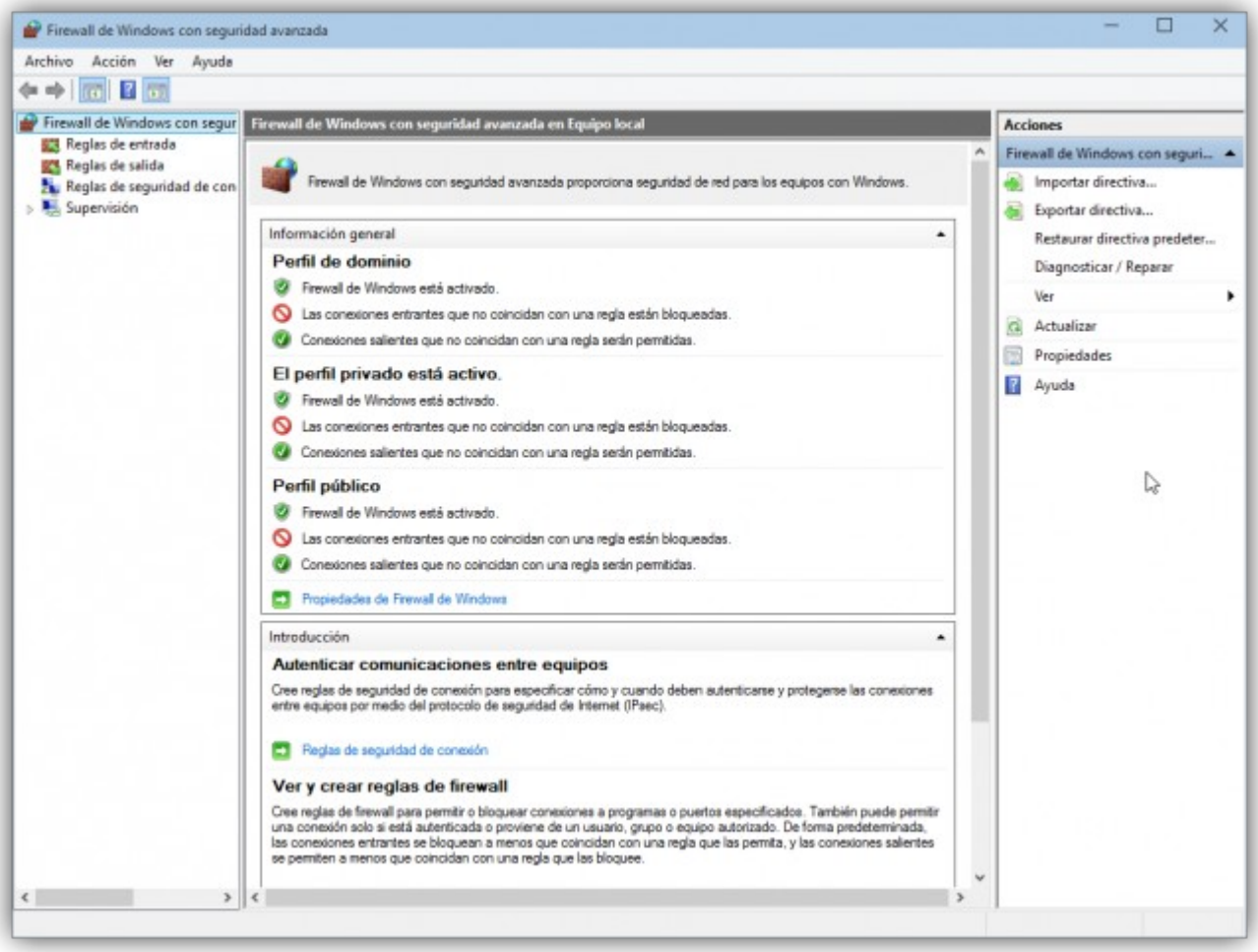


Otra forma de permitir a las aplicaciones a través de Firewall de Windows Defender es **abriendo puertos específicos** para estas aplicaciones o características, tal y como os hemos comentado más arriba. Pero esto supone un mayor riesgo. Cuando abrimos un puerto para una aplicación lo que estamos haciendo es permitir que el tráfico entre y salga de nuestro ordenador libremente, como si se tratara de un agujero en nuestro cortafuegos. Esto lo que va a provocar es que el PC sea menos seguro y que pueda generar oportunidades para que algún tipo de malware acceda a los archivos de nuestro sistema, e incluso que un hacker pueda hacer uso del dispositivo para propagar este software malicioso a otros dispositivos.

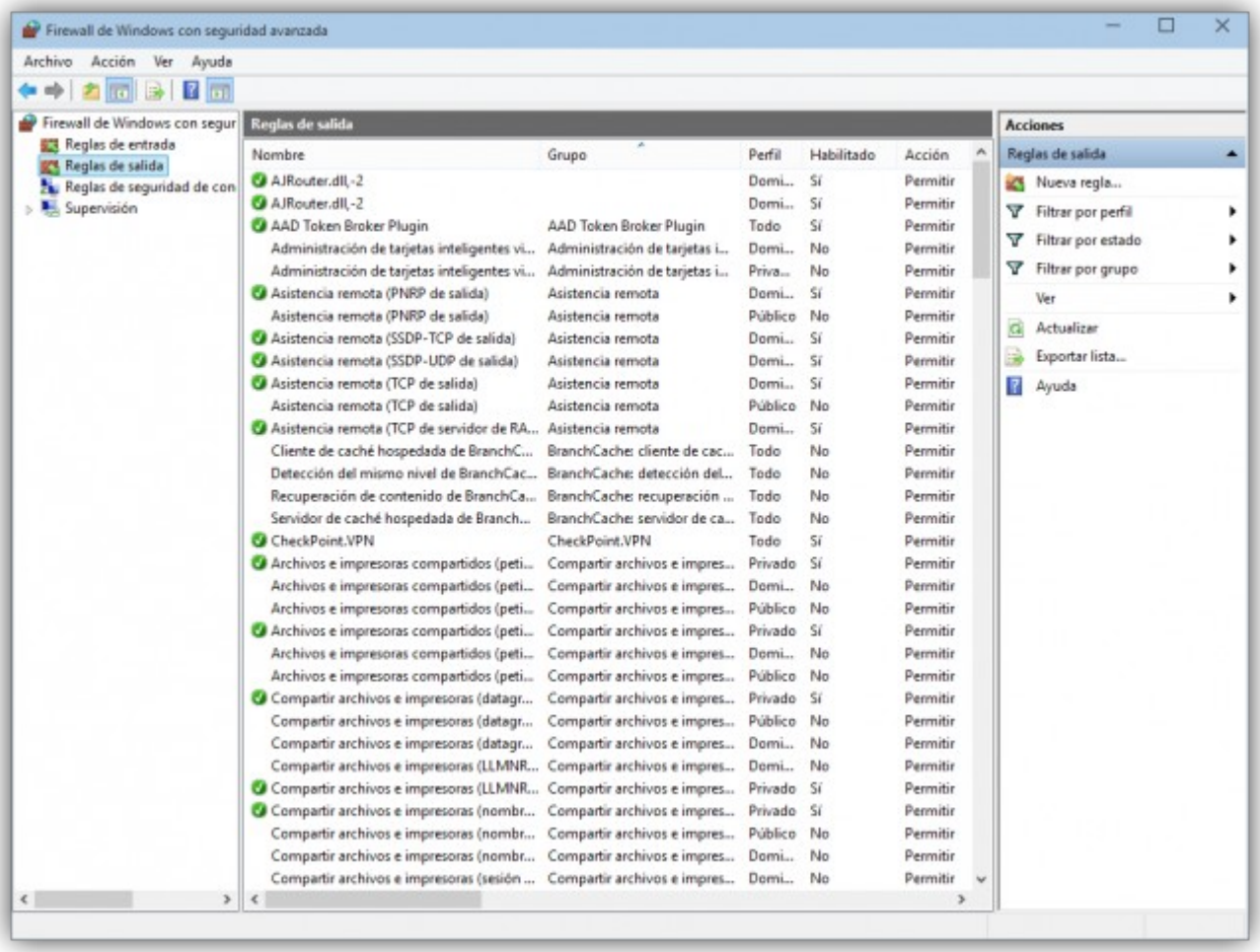
Por lo tanto, siempre que nos sea posible si queremos añadir una excepción a la lista de aplicaciones permitidas por el firewall lo haremos por el primer método. Cuando las añadimos manualmente el agujero de seguridad únicamente se abre cuando se usa la aplicación, pero si abrimos el puerto siempre estará abierto. Además, si es posible permite el acceso de las aplicaciones **sólo cuando te haga falta** y revisa de vez en cuando el listado de todas las que tienen permiso, ya que seguramente encuentras algunas a las que en su día les concediste el permiso, pero que ya no te haga falta. Es una forma de reducir riesgos que debemos tener en cuenta.

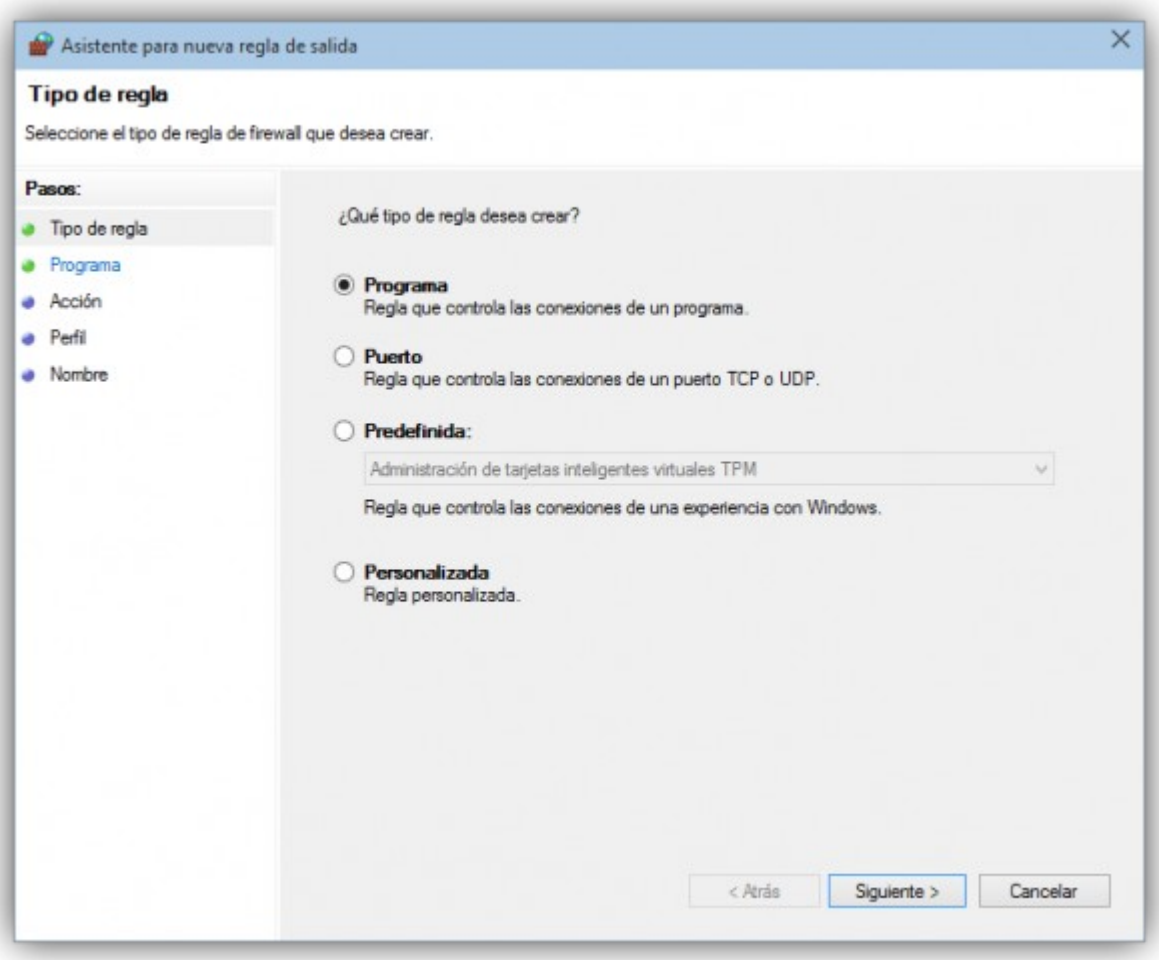
Acceder a la configuración avanzada del Firewall

Si queremos tener un control más avanzado sobre puertos y protocolos de conexión debemos abrir la ventana de configuración avanzada desde dicho apartado en la ventana principal de la **configuración.**



Desde aquí podremos ver todas las **reglas de entrada y de salida** con que cuenta nuestro cortafuegos. Podemos crear nuevas reglas personalizadas para las aplicaciones que queramos (por ejemplo, eMule o uTorrent) configurando los puertos y protocolos por los que queramos permitir (o bloquear) la conexión.


Firewall de Windows con seguridad avanzada
Archivo Acción Ver Ayuda
Firewall de Windows con segur
Reglas de entrada
Reglas de salida
Reglas de seguridad de con
Supervisión
Reglas de salida
Nombre Grupo Perfil Habilitado Acción
AJRouter.dll,-2 Domi... Sí Permitir
AJRouter.dll,-2 Domi... Sí Permitir
AAD Token Broker Plugin AAD Token Broker Plugin Todo Sí Permitir
Administración de tarjetas inteligentes vi... Administración de tarjetas i... Domi... No Permitir
Administración de tarjetas inteligentes vi... Administración de tarjetas i... Priva... No Permitir
Asistencia remota (PNRP de salida) Asistencia remota Domi... Sí Permitir
Asistencia remota (PNRP de salida) Asistencia remota Público No Permitir
Asistencia remota (SSDP-TCP de salida) Asistencia remota Domi... Sí Permitir
Asistencia remota (SSDP-UDP de salida) Asistencia remota Domi... Sí Permitir
Asistencia remota (TCP de salida) Asistencia remota Domi... Sí Permitir
Asistencia remota (TCP de salida) Asistencia remota Público No Permitir
Asistencia remota (TCP de servidor de RA... Asistencia remota Domi... Sí Permitir
Cliente de caché hospedada de BranchC... BranchCache: cliente de cac... Todo No Permitir
Detección del mismo nivel de BranchCac... BranchCache: detección del... Todo No Permitir
Recuperación de contenido de BranchCa... BranchCache: recuperación ... Todo No Permitir
Servidor de caché hospedada de Branch... BranchCache: servidor de ca... Todo No Permitir
CheckPoint.VPN CheckPoint.VPN Todo Sí Permitir
Archivos e impresoras compartidos (peti... Compartir archivos e impres... Privado Sí Permitir
Archivos e impresoras compartidos (peti... Compartir archivos e impres... Domi... No Permitir
Archivos e impresoras compartidos (peti... Compartir archivos e impres... Público No Permitir
Archivos e impresoras compartidos (peti... Compartir archivos e impres... Privado Sí Permitir
Archivos e impresoras compartidos (peti... Compartir archivos e impres... Domi... No Permitir
Archivos e impresoras compartidos (peti... Compartir archivos e impres... Público No Permitir
Compartir archivos e impresoras (datagr... Compartir archivos e impres... Privado Sí Permitir
Compartir archivos e impresoras (datagr... Compartir archivos e impres... Público No Permitir
Compartir archivos e impresoras (datagr... Compartir archivos e impres... Domi... No Permitir
Compartir archivos e impresoras (LLMNR... Compartir archivos e impres... Domi... No Permitir
Compartir archivos e impresoras (LLMNR... Compartir archivos e impres... Privado Sí Permitir
Compartir archivos e impresoras (nombr... Compartir archivos e impres... Privado Sí Permitir
Compartir archivos e impresoras (nombr... Compartir archivos e impres... Público No Permitir
Compartir archivos e impresoras (nombr... Compartir archivos e impres... Domi... No Permitir
Compartir archivos e impresoras (sesión ... Compartir archivos e impres... Domi... No Permitir
Acciones
Reglas de salida
Nueva regla...
Filtrar por perfil
Filtrar por estado
Filtrar por grupo
Ver
Actualizar
Exportar lista...
Ayuda



De esta manera, si no queremos tener que **gestionar un cortafuegos de terceros**, podremos configurar de la manera más óptima posible para permitir sólo las conexiones que de verdad queramos gestionar y bloquear aquellas que puedan resultar maliciosas o peligrosas para nuestro sistema.