INSTITUTO KHIPU

Semestre I

Sesión #28

CARRERA PROFESIONAL

DESARROLLO DE SISTEMAS DE INFORMACION

MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE HARDWARE Y SOFTWARE

Tema

CONFIGURACIÓN DE FIREWALL

CONFIGURACIÓN DE FIREWALL

Si en Windows 10 no instalamos ningún firewall en el equipo, por defecto actuará el propio firewall de Windows. Vamos a mostrar todas y cada una de las opciones de configuración que tenemos disponibles en el firewall de Windows 10. Podremos crear diferentes reglas de entrada y salida, con diferentes protocolos, y aplicados a diferentes tipos de perfiles (dominio, público y privado), por lo que vamos a tener una alta configurabilidad.

Índice

Mantener la seguridad en la red es fundamental y para ello podemos hacer uso de diferentes opciones. Siempre se puede instalar antivirus, pero también un cortafuegos. Esto puede evitar

problemas como son los accesos indeseados que puedan derivar en el robo de datos o infectar el sistema con cualquier otra amenaza.

¿Qué es un firewall?

Un firewall nos permite permitir o denegar el tráfico que va y viene desde una o varias interfaces de red, podremos controlar el tráfico de forma exhaustiva, porque el firewall se encarga de comprobar la cabecera de todos los paquetes para ver si cumple con las reglas definidas en el sistema.

Por ejemplo, podemos crear una lista con las aplicaciones que queremos bloquear para que no tengan acceso a Internet o las direcciones IP que no queremos que se conecten a una red. Se basa principalmente en reglas.

Cuando utilizamos un firewall en la red local, lo más normal es permitir todo el tráfico desde y hacia los equipos de la red local, porque es una red privada y confiable, sin embargo, es posible configurar una red local como «red pública», por tanto, el firewall se va a configurar de forma automática para denegar cualquier intento de comunicación desde fuera hacia nosotros, no obstante, se permitirá las respuestas al tráfico generado por nosotros. Los firewalls que permiten este funcionamiento se denominan SPI, y son los que hoy en día se utilizan ampliamente.

Los firewalls se pueden configurar de dos formas bien diferentes:

- Firewall permisivo: tendremos una regla de «permitir todo» implícita al final, por tanto, si queremos bloquear algo deberemos crear una regla específica para ello. Este tipo de configuración suelen estar en la LAN o en los equipos configurados como «red privada».
- Firewall restrictivo: tendremos una regla de «denegar todo» implícita al final, por tanto, si queremos permitir algo de tráfico, vamos a tener que crear una regla como mínimo para que podamos enviar y recibir datos. Este tipo de configuración suelen estar en la WAN de Internet en firewalls como pfSense, o en los equipos configurados como «red pública», para protegerlos de diferentes ataques.

El sistema operativo Windows 10 dispone de un firewall bastante avanzado que nos permitirá crear decenas de reglas con el objetivo de permitir o bloquear cierto tráfico, de esta forma, podremos controlar todas las conexiones entrantes y salientes en detalle. Además, a la hora de configurar un

firewall es muy importante conocer el sentido del tráfico, si no sabemos bien el sentido del tráfico (entrante o saliente, IP de origen o IP de destino etc.) seguramente no creemos bien las reglas necesarias, y no funcionará el firewall como nosotros hemos pensado, por tanto, lo primero que deberemos pensar es en el sentido del tráfico, y, posteriormente, crear las diferentes reglas.

¿Cómo de completo es el firewall de Windows?

Esta característica de seguridad que incorpora el sistema operativo de Microsoft, es utilizada para controlar el tráfico de entrada y salida en nuestro equipo. Este cuenta con muchas características, que hacen de él, un firewall muy válido para la gran mayoría de los usuarios. Incluso para pequeñas empresas, puede ser más que suficiente. Estas son:

- Control de entrada y salida: El firewall de Windows 10, cuenta con funciones que permiten definir reglas de entrada y salida. Esto quiere decir que puede controlar el tráfico de entrada y salida, desde el propio equipo.
- Filtrado de paquetes: Este firewall se utiliza para realizar un filtrado a los paquetes. Este los puede bloquear si es necesario, siempre basándose en los criterios que define el usuario. Tales como la dirección IP, los protocolos y los puertos.
- Monitorización: El firewall de Windows 10 puede realizar una monitorización de la actividad en línea, y así poder generar informes sobre los eventos de seguridad. Esto nos permite identificar y solucionar los problemas de seguridad, de una forma más efectiva.
- Protección de red pública: El firewall puede detectar y proteger las redes públicas de forma automática. Esto quiere decir, que puede configurarse para bloquear todos los accesos que no están autorizados a los servicios del equipo.
- Integración de herramientas: En esta herramienta, se integran otras funciones de seguridad de Windows. Tales como Windows Defender. Esto nos proporciona una protección más completa contra las posibles amenazas que nos podemos encontrar en Internet.

Incluso con estas capacidades, siempre debemos tener en cuenta que el firewall de Windows, no es totalmente infalible. Por lo cual no lo debemos considerar como la única herramienta de seguridad que necesitamos. Este es recomendable combinarlo con otras herramientas, como puede ser un antivirus o antispyware. Ayudando así a proteger el equipo de muchas más amenazas.

Ventajas de usar el firewall de Windows

Aunque normalmente utilizamos antivirus para protegernos de ataques externos e infecciones de virus en nuestros equipos, el firewall es la primera capa de seguridad de nuestro sistema y tiene una serie de ventajas que lo convierten en una herramienta fundamental para la seguridad de nuestro sistema operativo.

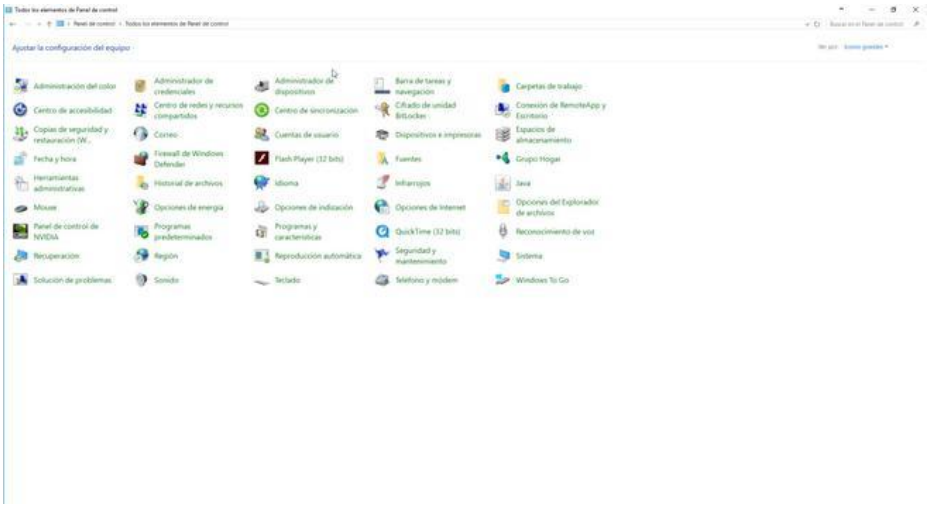
- Integración nativa: El firewall de Windows viene integrado de manera nativa en el sistema operativo, lo que significa que no es necesario descargar ni instalar ningún software adicional. Esto simplifica la gestión y asegura que cada sistema Windows tenga acceso a una capa básica de protección.
- Configuración fácil de usar: Su interfaz intuitiva facilita la configuración y personalización de las reglas de seguridad. Puedes definir reglas específicas para programas, puertos o protocolos, lo que te da un control más preciso sobre el tráfico permitido y bloqueado.
- Protección bidireccional: El firewall de Windows no solo controla el tráfico de entrada, sino también el de salida. Esto significa que no solo protege tu sistema contra amenazas externas, sino que también evita que aplicaciones no autorizadas envíen información no deseada desde tu ordenador.
- Filtro avanzado: Ofrece capacidades avanzadas de filtrado de paquetes, lo que permite detectar y bloquear tráfico no deseado o potencialmente peligroso. Puedes personalizar las reglas según tus necesidades específicas, ofreciendo más flexibilidad en la protección de tu sistema.
- Compatibilidad con perfiles en red: El firewall de Windows adapta su configuración según el tipo de red al que estés conectado, ya sea una red doméstica, de trabajo o pública. Esto garantiza que la seguridad se ajuste automáticamente a tu entorno, manteniendo un equilibrio entre protección y accesibilidad.

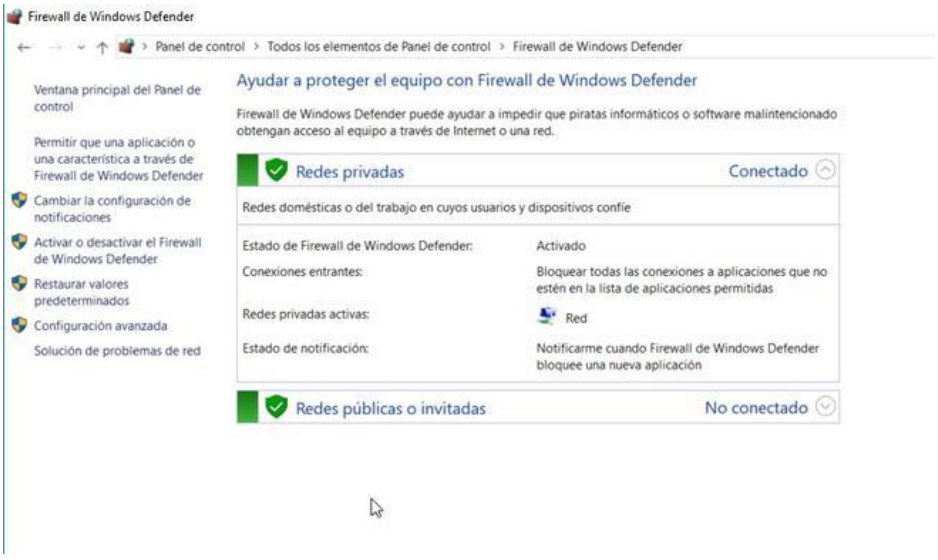
Registro de eventos: Registra eventos relacionados con la seguridad, lo que facilita la identificación y resolución de posibles problemas. Los registros permiten realizar un seguimiento de las actividades del firewall y proporciona información importante en caso de necesitar datos de seguridad.

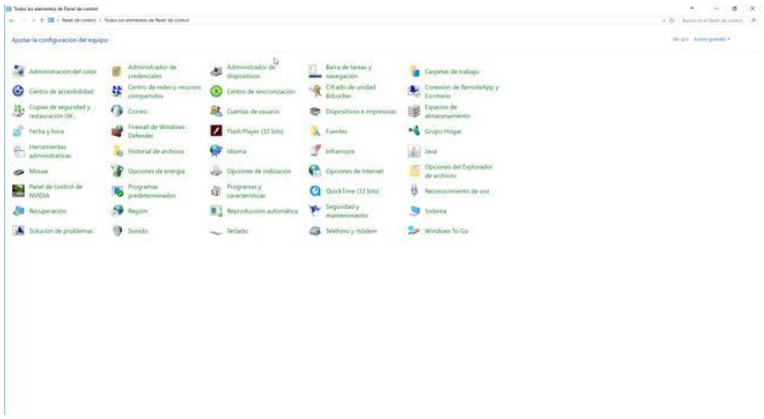
Configuración avanzada del firewall

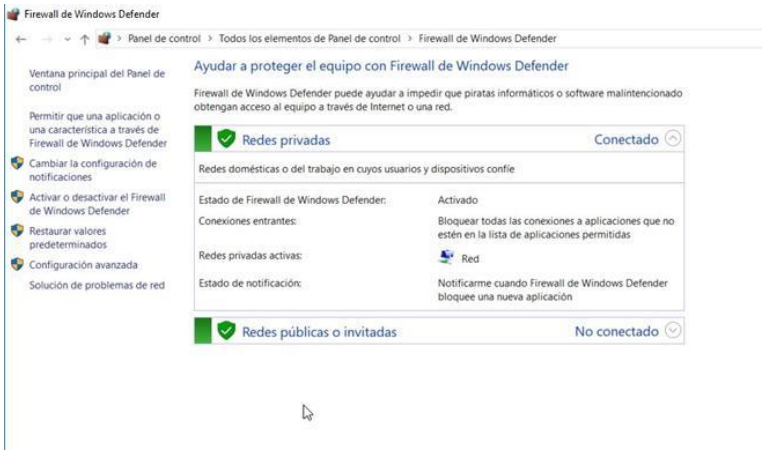
Lo primero que debemos hacer es acceder a la configuración avanzada del firewall de Windows 10. Para ello, nos vamos a «Panel de control», y pinchamos en «Firewall de Windows Defender». También podemos optar por escribir en la barra de búsqueda de Windows la palabra «firewall», y automáticamente nos llevará al menú principal del cortafuegos de Windows 10.

Una vez que estamos en el menú principal del firewall de Windows, podremos ver si estamos conectados a redes privadas o públicas, y la política de actuación que estamos teniendo en esos mismos instantes. En el menú principal del firewall debemos pinchar en «Configuración Avanzada» que está en la parte izquierda del menú.





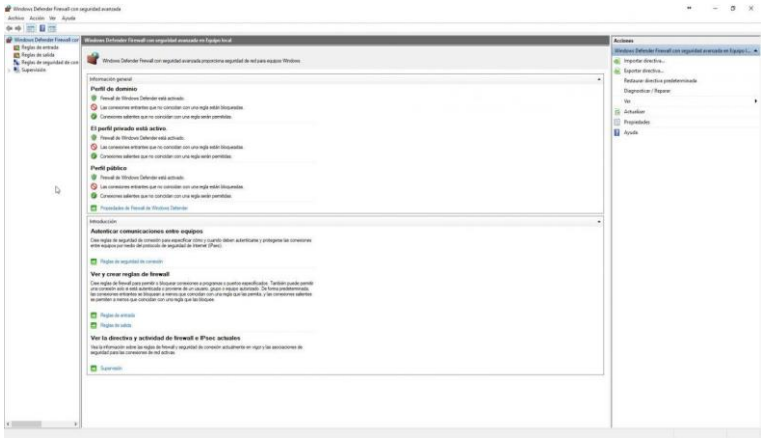




En el menú de configuración avanzada del firewall de Windows 10 tendremos acceso a todas las reglas de entrada, de salida, y el resumen de todas las reglas creadas tanto de entrada y salida en el firewall.

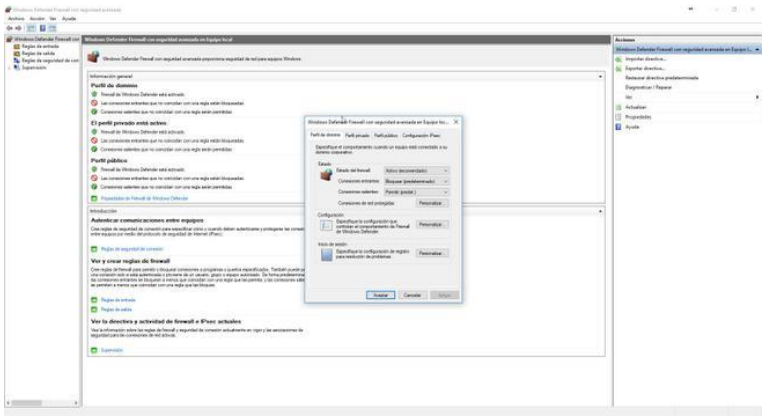
En el menú principal de esta configuración avanzada tenemos las políticas predeterminadas de los tres perfiles que tenemos disponibles: perfil de dominio, perfil privado, público. Dependiendo del perfil que tengamos asignado a nuestra red local, tendremos unos permisos u otros.

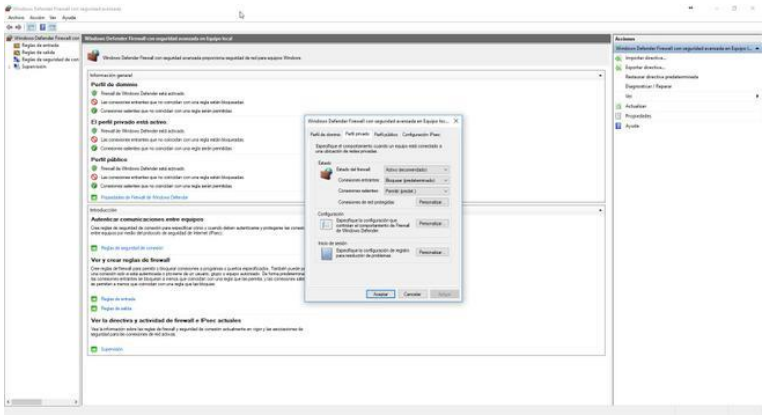
Por defecto, todos los perfiles están configurados con una política restrictiva en las reglas de entrada. Esto significa que todas las conexiones entrantes que no coincidan con una regla que haya predefinida, o que hayamos definido nosotros, serán bloqueadas. Respecto a las reglas de salida, utiliza una política permisiva, esto significa que todas las conexiones salientes que no coincidan con una regla serán permitidas, y solo las que hayamos definido específicamente para bloquearlas, se bloquearán.

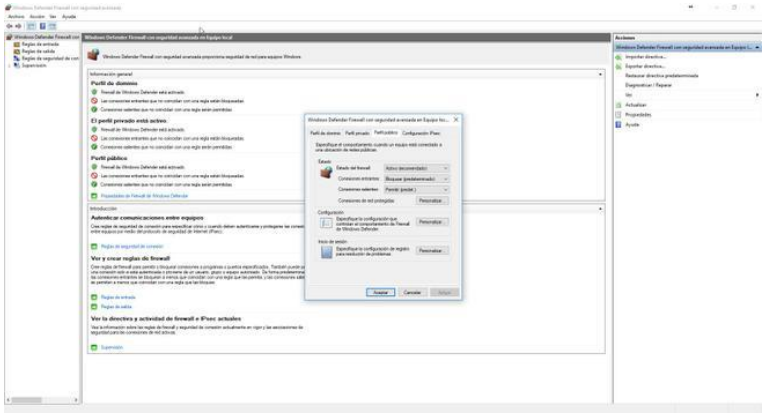


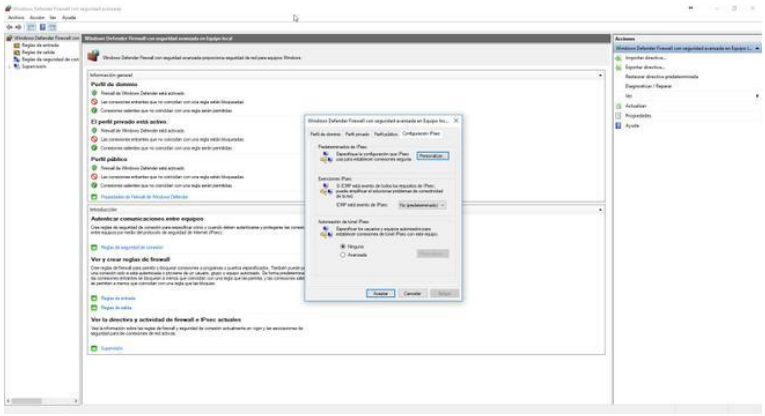
Si pinchamos en el botón de «Propiedades de Firewall de Windows Defender«, podremos cambiar las configuraciones globales de todos los perfiles. Tendremos la posibilidad de habilitar o deshabilitar el firewall dependiendo del perfil asignado, cambiar la política (permisiva o restrictiva) tanto de las conexiones entrantes como de las salientes, y también otras acciones como detectar conexiones de red protegidas donde seleccionamos las interfaces de red instaladas, configuración de las notificaciones del firewall, y el destino de los logs que registra el propio cortafuegos.

Por último, podremos configurar la política a seguir si establecemos un túnel VPN IPsec con el propio equipo, ya que este tipo de conexiones al estar autenticadas, son confiables y podremos configurar el firewall para que sea más permisivo si queremos.

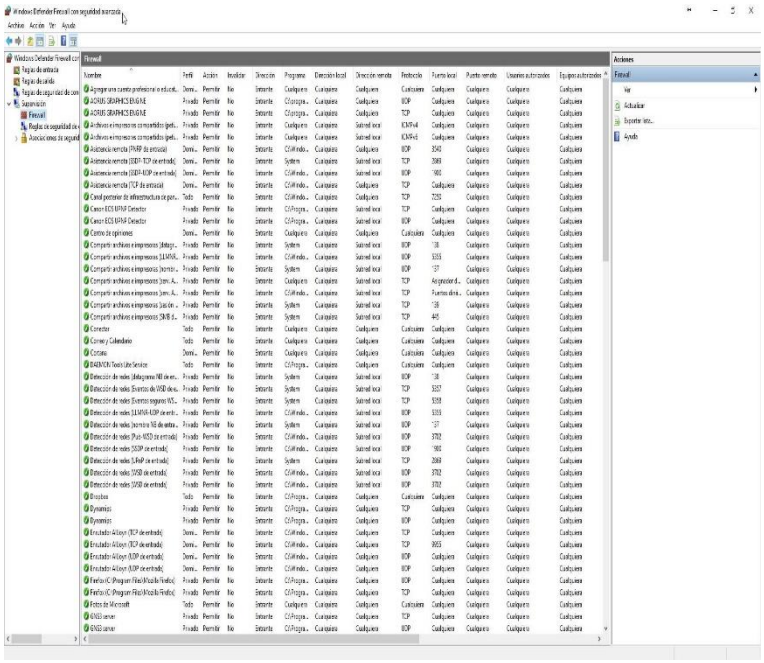








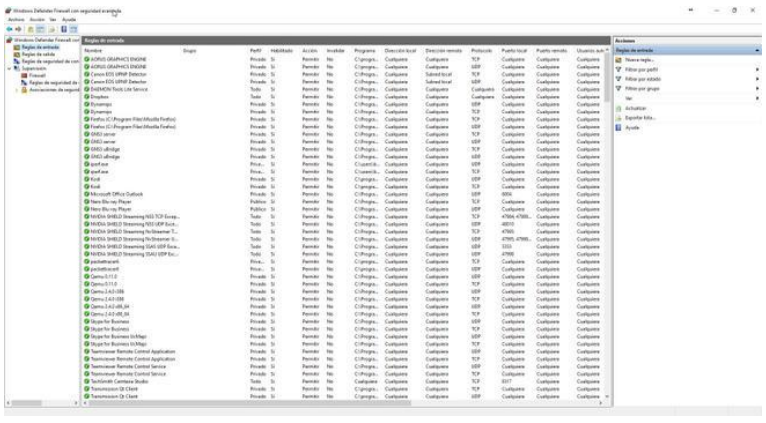
En la sección de «Supervisión / Firewall» podremos ver todas y cada una de las reglas que tenemos registradas en el firewall de Windows, todas las reglas activas aparecerán aquí, y podremos ver su configuración en detalle. Si queremos modificar una de estas reglas, simplemente tendremos que pinchar con el botón derecho del ratón sobre la regla en concreto, y pinchar en «Propiedades» para modificarla como queramos.

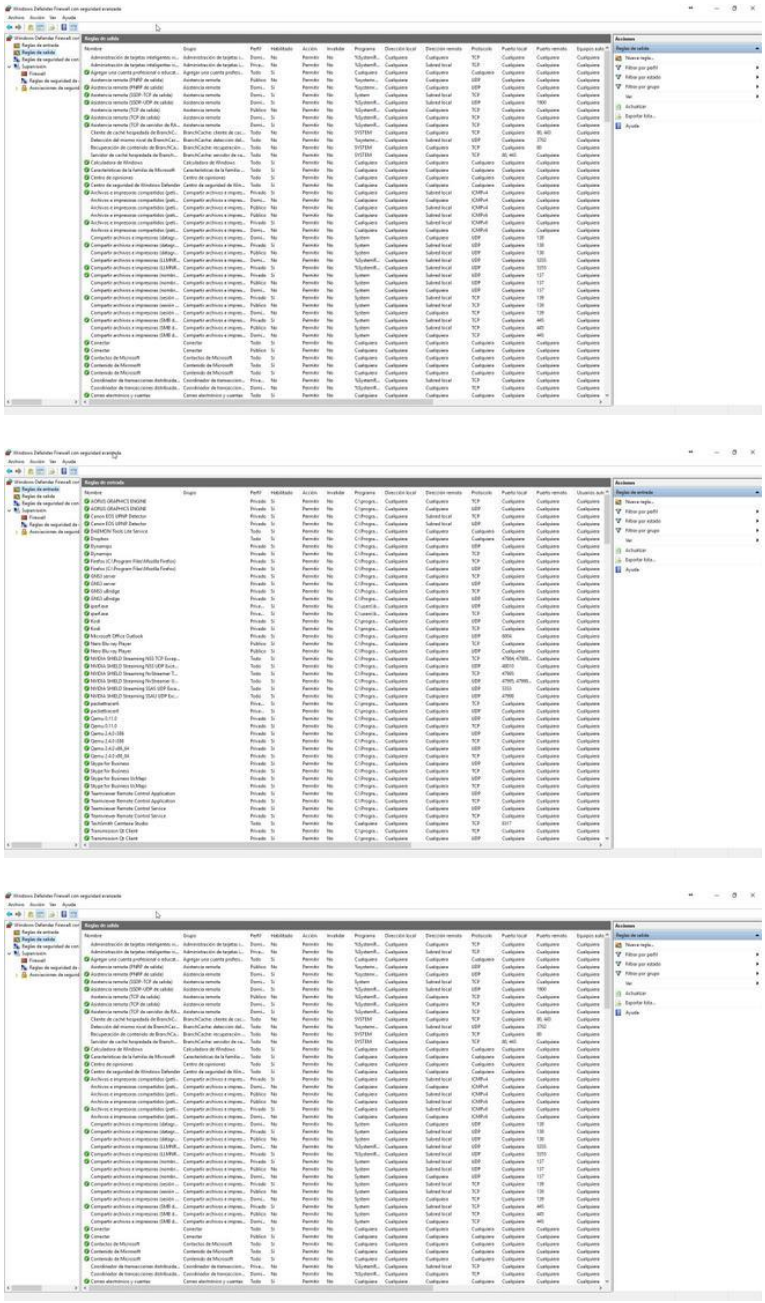


Reglas de entrada y reglas de salida

En la sección de «Reglas de entrada» y «Reglas de salida«, tendremos todas y cada una de las reglas que están actualmente dadas de alta, no obstante, algunas reglas pueden estar deshabilitadas, por tanto, no están en uso. Únicamente las reglas que tienen un «check» en verde son las que están habilitadas, las que no tienen ese «check» están deshabilitadas.

Es muy importante saber definir la regla correctamente dependiendo del sentido del tráfico. Si por ejemplo queremos impedir conexiones desde fuera hacia nosotros, debemos dar de alta reglas en «Reglas de entrada». Por el contrario, si queremos bloquear alguna comunicación desde nosotros hacia fuera, deberemos dar de alta una regla en «Reglas de salida». Es importantísimo saber bien el sentido del tráfico, porque podríamos dar de alta una regla que jamás se cumpla.





Cómo crear una regla personalizada

Aunque tenemos una gran cantidad de reglas que están dadas de alta, pero no se están utilizando, vamos a poder crear fácilmente una regla personalizada en función de varios parámetros. El firewall de Windows 10 nos va a permitir crear hasta cuatro tipos de reglas diferentes:

- Programa: Regla que controla las conexiones de un programa en concreto
- Puerto: regla que controla conexiones de un puerto TCP o UDP

- Predefinida: podremos seleccionar reglas predefinidas de Windows para sus servicios.
- Personalizada: regla que podremos configurar en detalle con todos los parámetros.

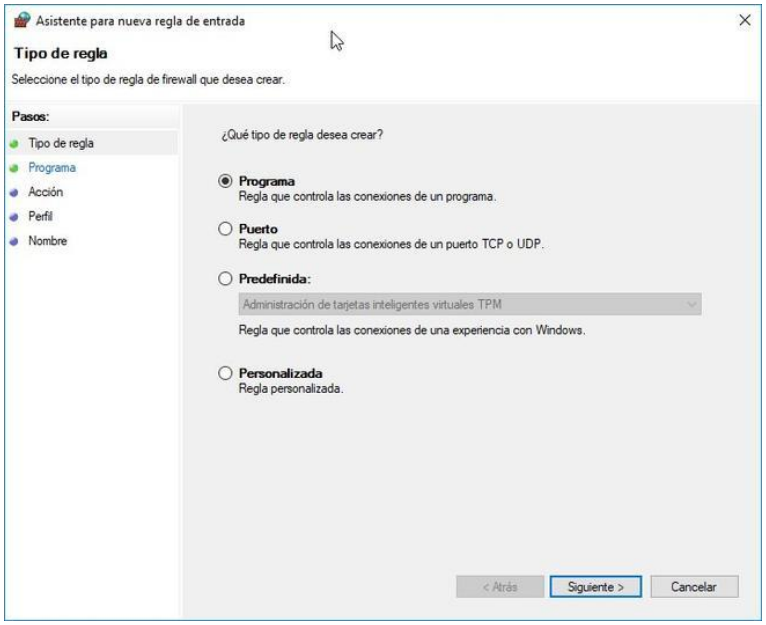
Para crear una nueva regla, pinchamos con el click derecho en «Reglas de entrada» o «reglas de salida» en «Nueva Regla«.

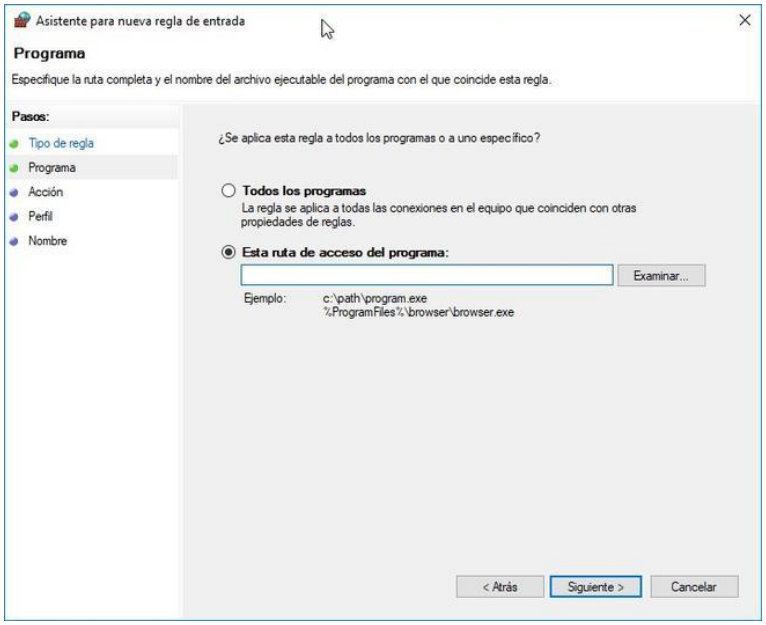
Reglas de Programa

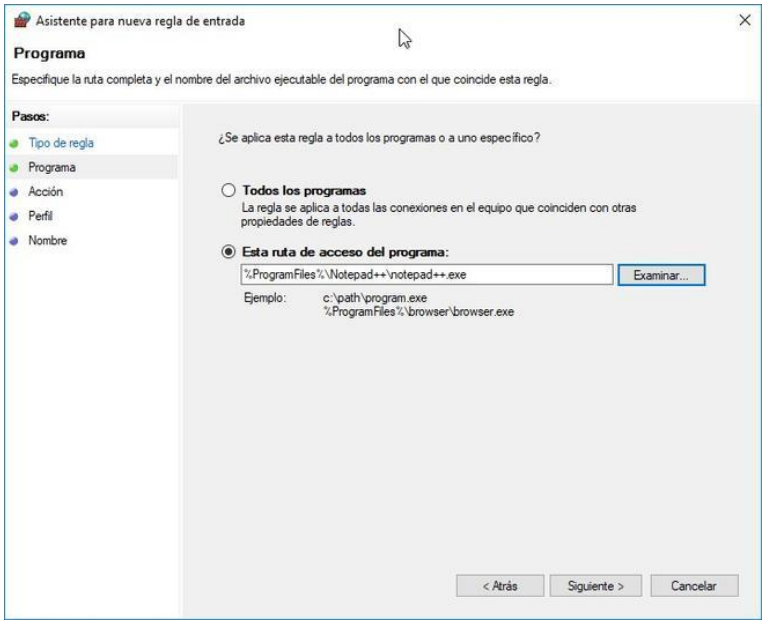
Si creamos una nueva «regla de programa», podremos permitir o denegar las conexiones de un determinado programa, tanto en las reglas de entrada como en las reglas de salida. Esta opción es ideal para no tener la necesidad de conocer los puertos TCP o UDP que utiliza un determinado programa.

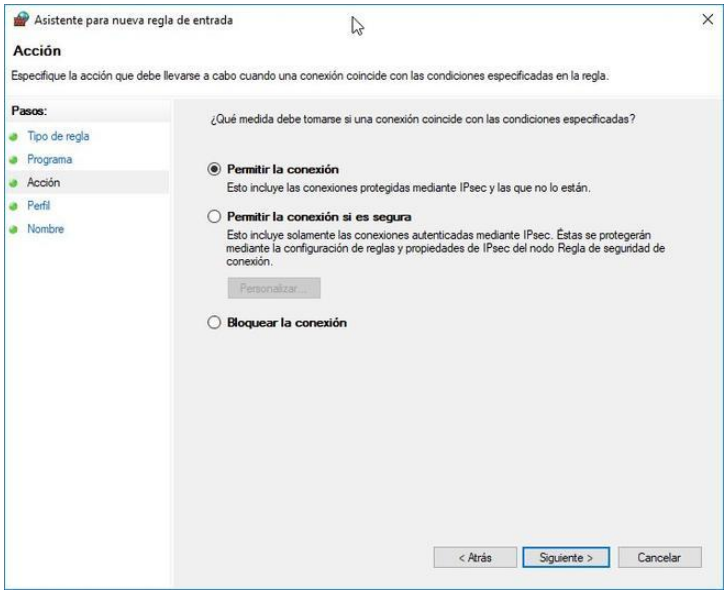
Simplemente debemos indicar si queremos que esta regla afecte a todos los programas instalados, o solo a uno en concreto. Una vez elegido, debemos decidir si queremos permitir la conexión, permitir la conexión si es segura (si usamos IPsec), o bloquear la conexión. Una vez definido si queremos permitir o denegar la conexión, debemos decidir en qué perfil (dominio, privado o público) queremos que esta regla se aplique. Por ejemplo, tal vez nos interese bloquear las conexiones únicamente en redes públicas.

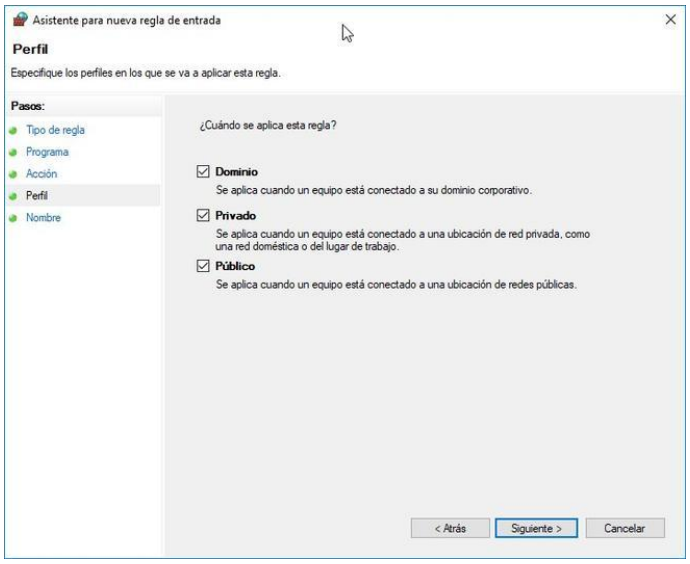
Por último, debemos proporcionar un nombre a la regla, y también una descripción opcional para saber rápidamente qué hace esa regla.

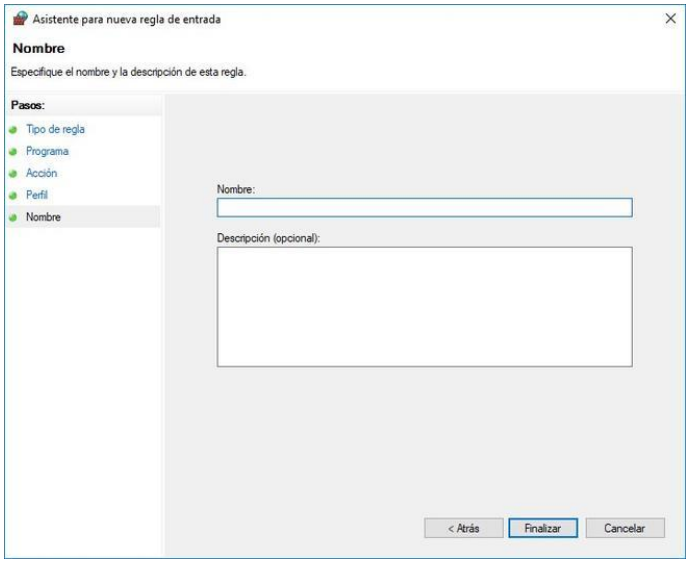



Asistente para nueva regla de entrada
Programa
Especifique la ruta completa y el nombre del archivo ejecutable del programa con el que coincide esta regla.
Pasos:
Tipo de regla
Programa
Acción
Perfil
Nombre
¿Se aplica esta regla a todos los programas o a uno específico?
Todos los programas
La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.
Esta ruta de acceso del programa:
Examinar...
Ejemplo: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de entrada
Programa
Especifique la ruta completa y el nombre del archivo ejecutable del programa con el que coincide esta regla.
Pasos:
Tipo de regla
Programa
Acción
Perfil
Nombre
¿Se aplica esta regla a todos los programas o a uno específico?
Todos los programas
La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.
Esta ruta de acceso del programa:
%ProgramFiles%\Notepad++\notepad++.exe
Examinar...
Ejemplo: c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de entrada
Acción
Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.
Pasos:
Tipo de regla
Programa
Acción
Perfil
Nombre
¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?
Permitir la conexión
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.
Permitir la conexión si es segura
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.
Personalizar...
Bloquear la conexión
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de entrada
Perfil
Especifique los perfiles en los que se va a aplicar esta regla.
Pasos:
Tipo de regla
Programa
Acción
Perfil
Nombre
¿Cuándo se aplica esta regla?
Dominio
Se aplica cuando un equipo está conectado a su dominio corporativo.
Privado
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.
Público
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.
< Atrás
Siguiente >
Cancelar

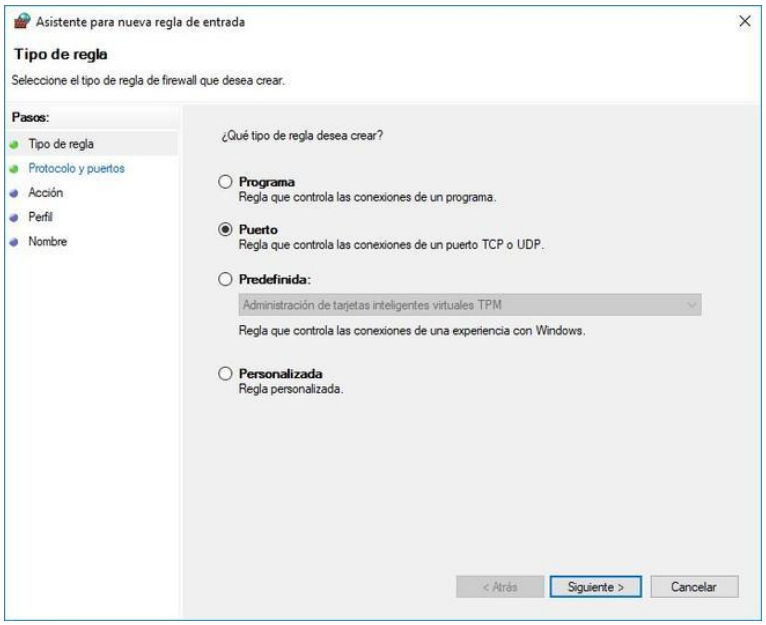

Asistente para nueva regla de entrada
Nombre
Especifique el nombre y la descripción de esta regla.
Pasos:
Tipo de regla
Programa
Acción
Perfil
Nombre
Nombre:
Descripción (opcional):
< Atrás
Finalizar
Cancelar

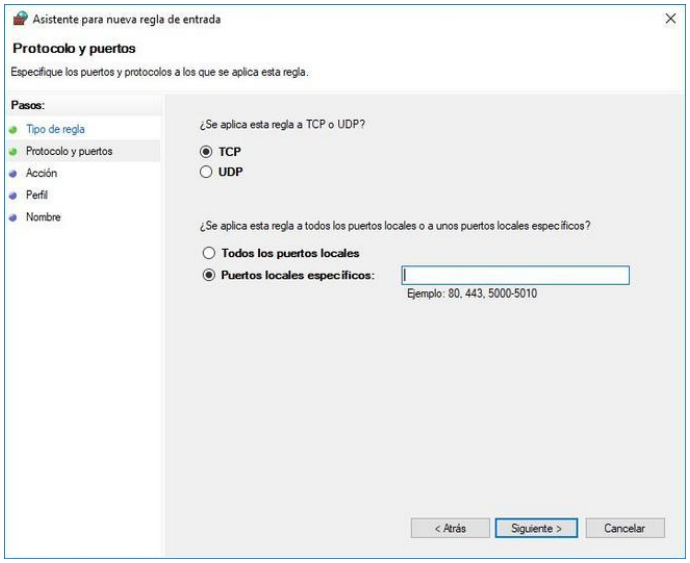
Reglas de Puerto

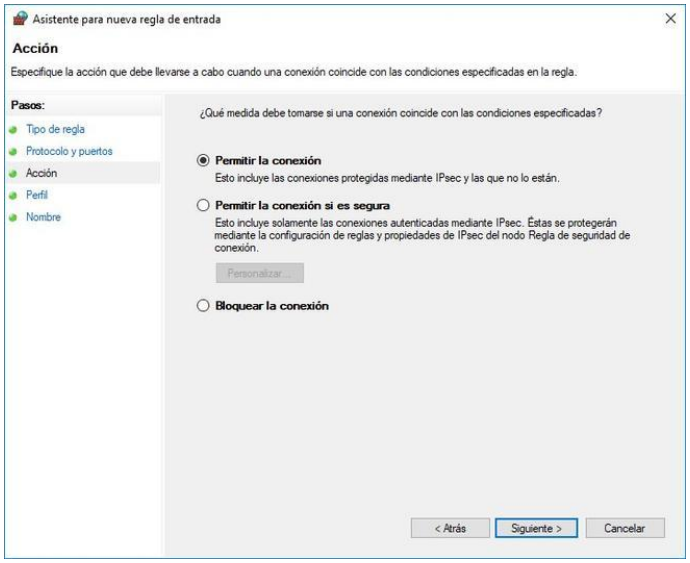
El firewall de Windows 10 también nos va a permitir filtrar puertos TCP o UDP, tanto en las reglas de entrada como en las reglas de salida.

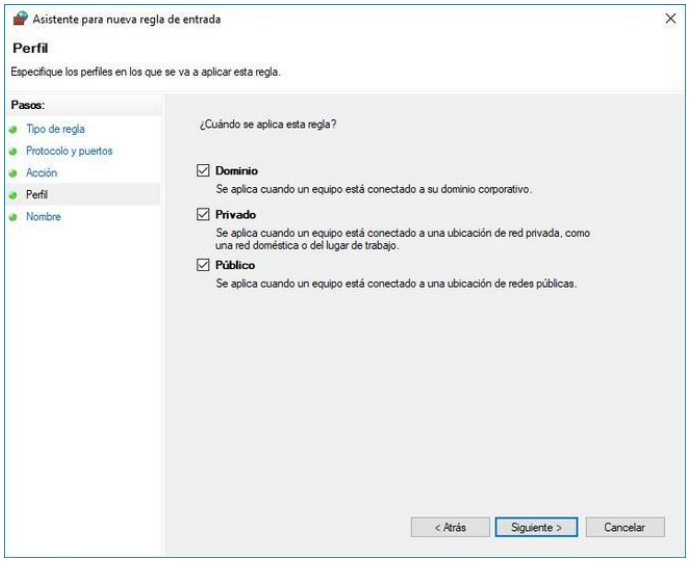
Para configurar el bloqueo de cualquier conexión entrante por el puerto 21 (por ejemplo), simplemente debemos elegir si queremos que este número de puerto sea TCP o UDP, y a continuación, definimos en «Puertos locales específicos» el número 21. El firewall nos va a permitir crear una misma regla para bloquear varios puertos con la sintaxis «21,20,22» por ejemplo, y también un rango de puertos con la sintaxis «5000-5100», además, vamos a poder definir también varios puertos y varios rangos de puertos en la misma regla.

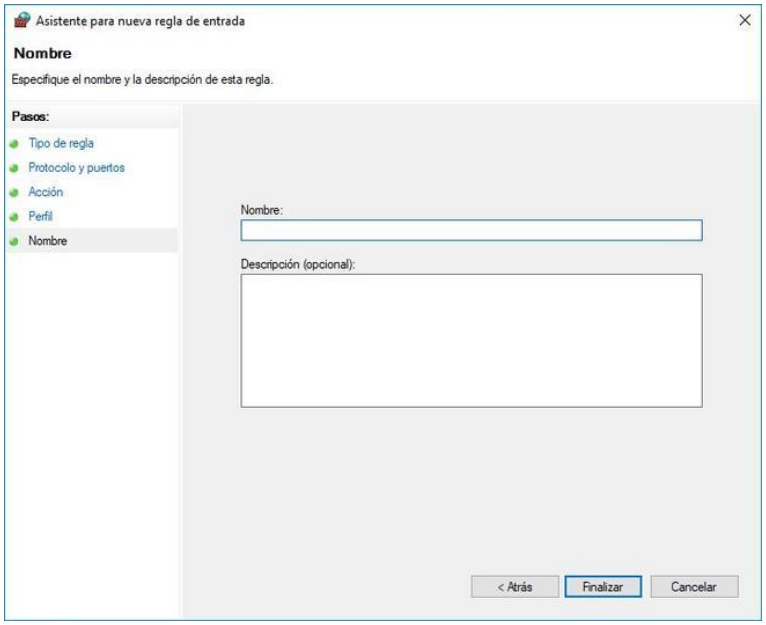
A continuación, podremos permitir la conexión, permitir la conexión si es segura (usamos IPsec), o bloquear la conexión. A continuación, definimos en qué perfil queremos que esta regla se aplique, si en perfil de dominio, perfil público o perfil privado. Por último, proporcionamos un nombre a esta regla, y una descripción opcional, para saber rápidamente qué hace la regla en concreto que hemos configurado.




Asistente para nueva regla de entrada
Protocolo y puertos
Especifique los puertos y protocolos a los que se aplica esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Se aplica esta regla a TCP o UDP?
TCP
UDP
¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?
Todos los puertos locales
Puertos locales específicos:
Ejemplo: 80, 443, 5000-5010
< Atrás
Siguiente >
Cancelar

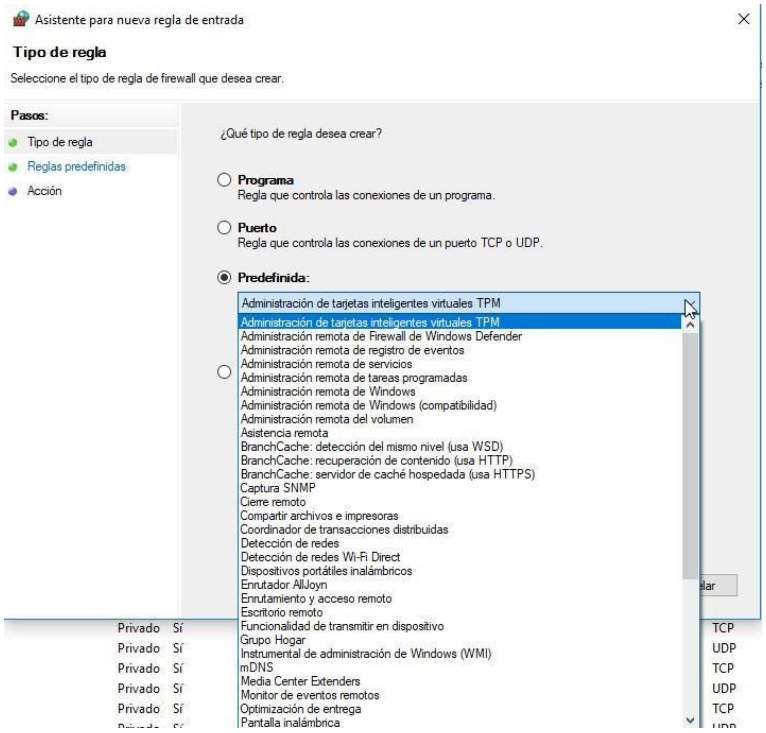

Asistente para nueva regla de entrada
Acción
Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?
Permitir la conexión
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.
Permitir la conexión si es segura
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.
Personalizar...
Bloquear la conexión
< Atrás
Siguiente >
Cancelar


Asistente para nueva regla de entrada
Perfil
Especifique los perfiles en los que se va a aplicar esta regla.
Pasos:
Tipo de regla
Protocolo y puertos
Acción
Perfil
Nombre
¿Cuándo se aplica esta regla?
Dominio
Se aplica cuando un equipo está conectado a su dominio corporativo.
Privado
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.
Público
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.
< Atrás
Siguiente >
Cancelar



Reglas predefinidas

En la sección de «Reglas predefinidas«, tendremos varias reglas que se corresponden con el propio sistema operativo de Windows. Si necesitamos habilitar o deshabilitar un determinado servicio, podremos hacerlo directamente desde aquí. Tal y como podéis ver, el listado de reglas es bastante extenso:

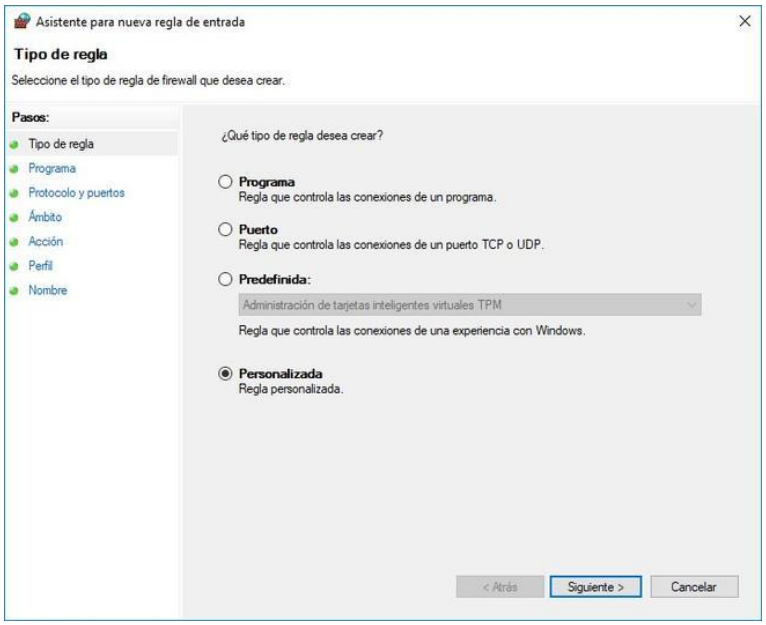


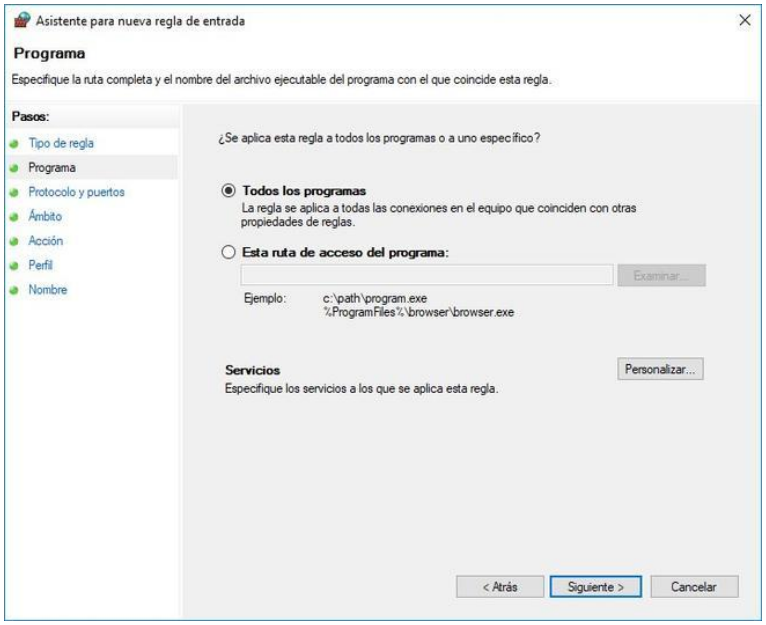
Una vez que hayamos seleccionado la regla, los siguientes pasos son los mismos que en las secciones anteriores, deberemos definir si queremos permitir, permitir con seguridad, o denegar. Después definimos dónde queremos aplicarla (dominio, privado o público), y, por último, proporcionar un nombre y descripción opcional.

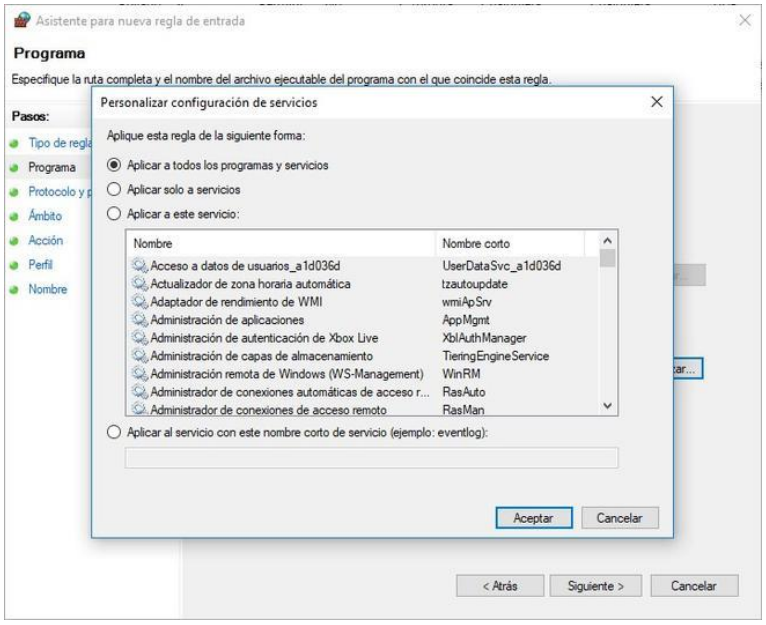
Reglas personalizadas

Las reglas personalizadas son las que mayor configurabilidad nos va a proporcionar. En esta sección podremos permitir o bloquear muy en detalle, cualquier programa, servicio de Windows, protocolo IP, IPv6, ICMPv4, ICMPv6 y un largo etcétera de opciones de configuración disponibles.

En el primer menú debemos seleccionar «Personalizada», a continuación, podremos elegir si esta regla queremos que se aplique a todos los programas, o solo a alguno de ellos. Además, si pinchamos en «Personalizar» también vamos a poder decidir si queremos aplicarla a todos los programas y servicios, aplicar solo a servicios, o aplicar a un servicio en concreto. Una vez que hayamos configurado esta regla, pasamos al siguiente menú para continuar con la creación de la regla.





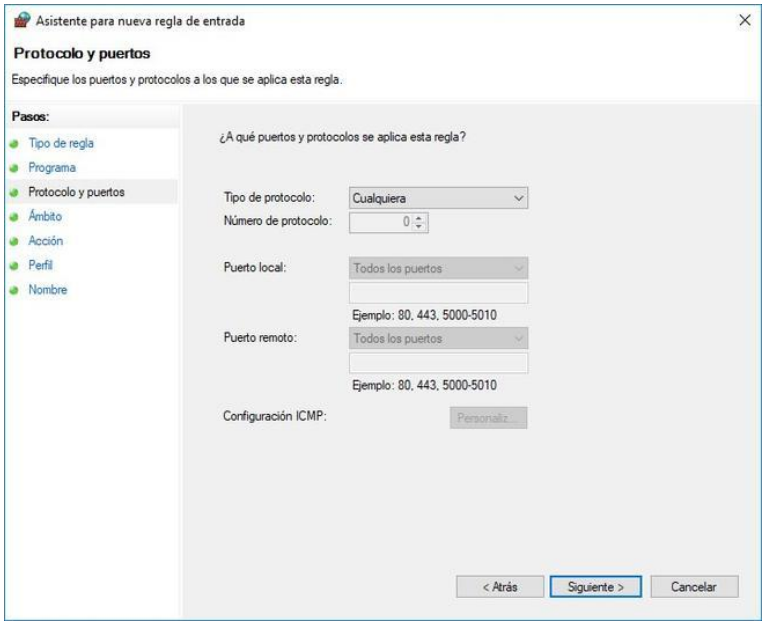


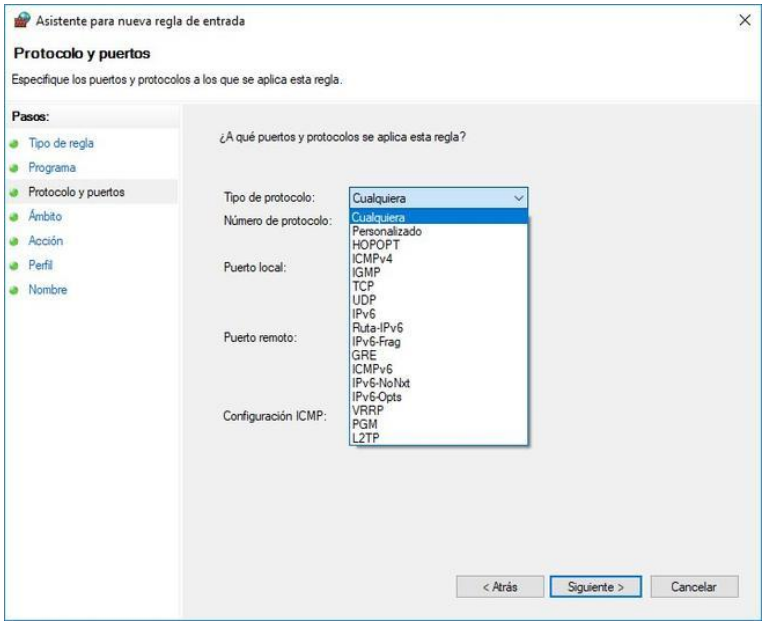
En este menú vamos a configurar el tipo de protocolo que queremos filtrar, tendremos una larga lista de protocolos que podremos permitir o denegar, concretamente el listado de protocolos son los siguientes:

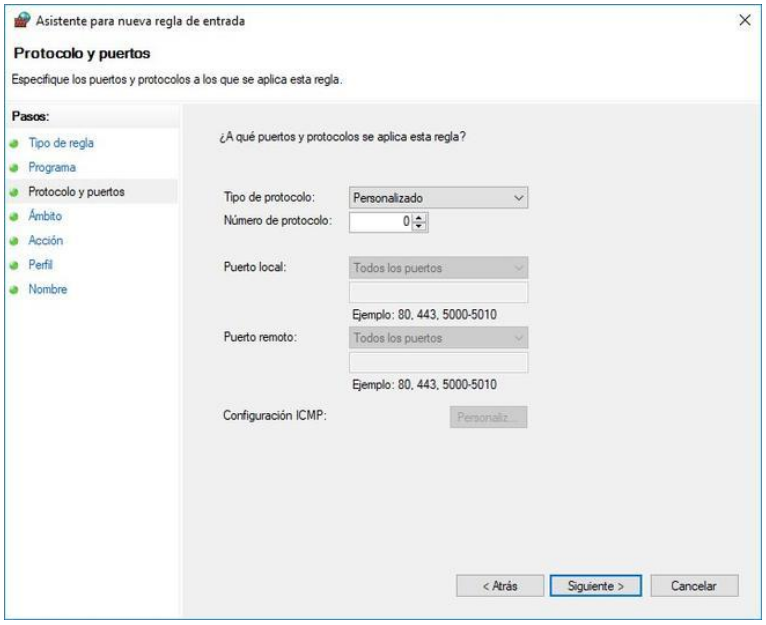
- Cualquiera: cualquier protocolo, filtra a nivel de red.
- Personalizado: podremos definir el número de protocolo que queremos bloquear, en caso de que en el listado no aparezca.
- HOPOPT

- ICMPv4
- IGMP
- TCP
- UDP
- IPv6
- Ruta-IPv6
- IPv6-Flag
- GRE
- ICMPv6
- IPv6-NoNxt
- IPv6-Opts
- VRRP
- PGM
- L2TP

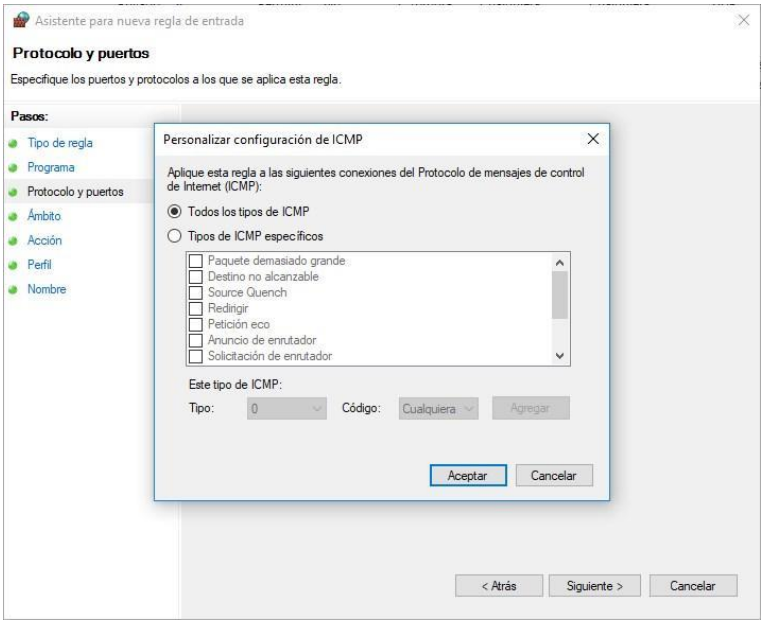
Dependiendo de qué hayamos elegido, nos va a permitir elegir un puerto local, y un puerto remoto.



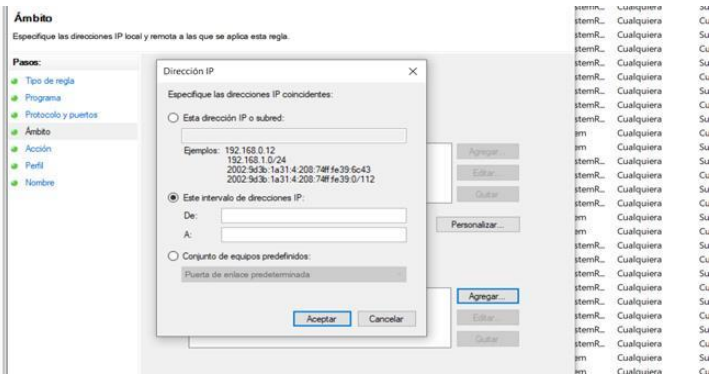




Además, si seleccionamos por ejemplo el protocolo ICMPv4, vamos a poder elegir si queremos permitir o denegar todos los tipos de ICMP, o solo unos específicos, tal y como podéis ver aquí:

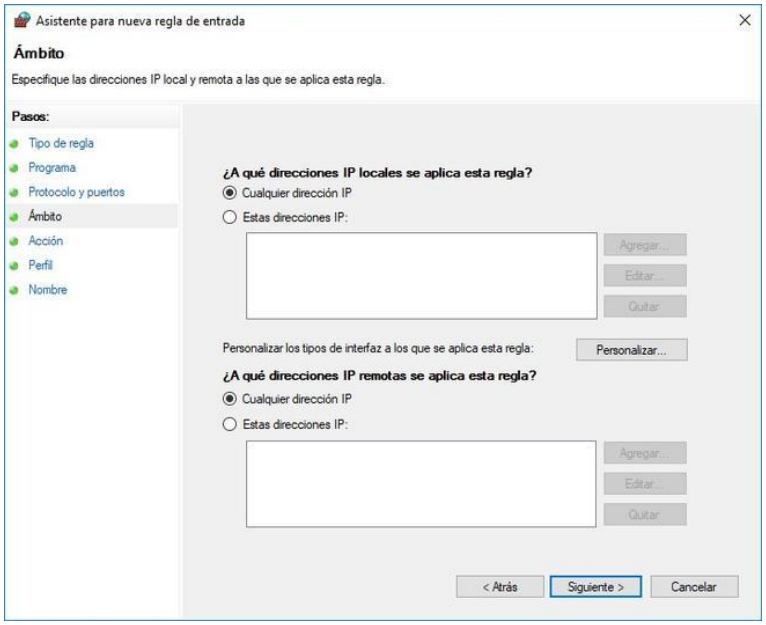


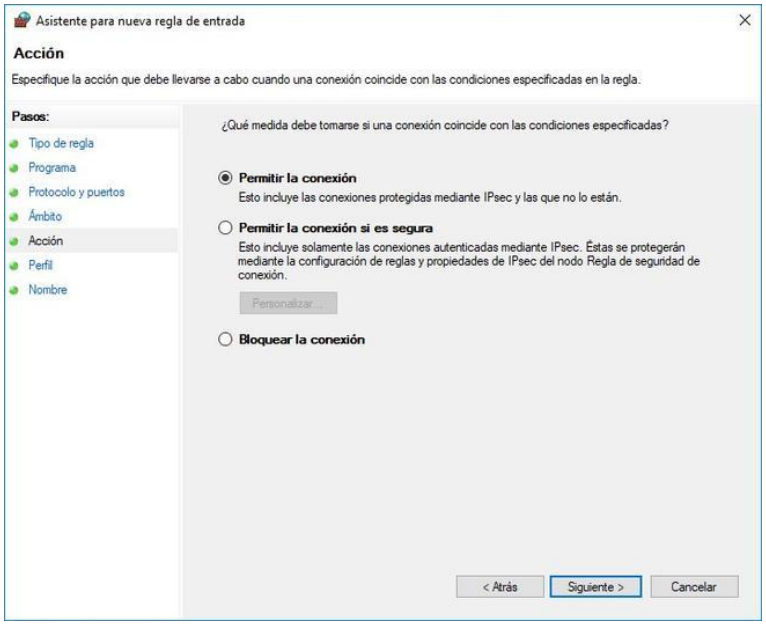
Una vez que hayamos elegido qué protocolo queremos utilizar, vamos a poder definir las direcciones IP locales y remotas donde esta regla debe aplicarse, de esta forma, vamos a tener el control total de cualquier tipo de conexión que hagan al sistema, o que hagamos desde el sistema. En el caso de querer crear un rango de direcciones IP también lo vamos a poder hacer de manera fácil y rápida en este menú de «ámbito», simplemente debemos seleccionar «Estas direcciones IP» y a continuación pinchar en «Agregar» y se nos desplegará un nuevo menú de configuración donde especificamos la subred o el rango de direcciones IP:

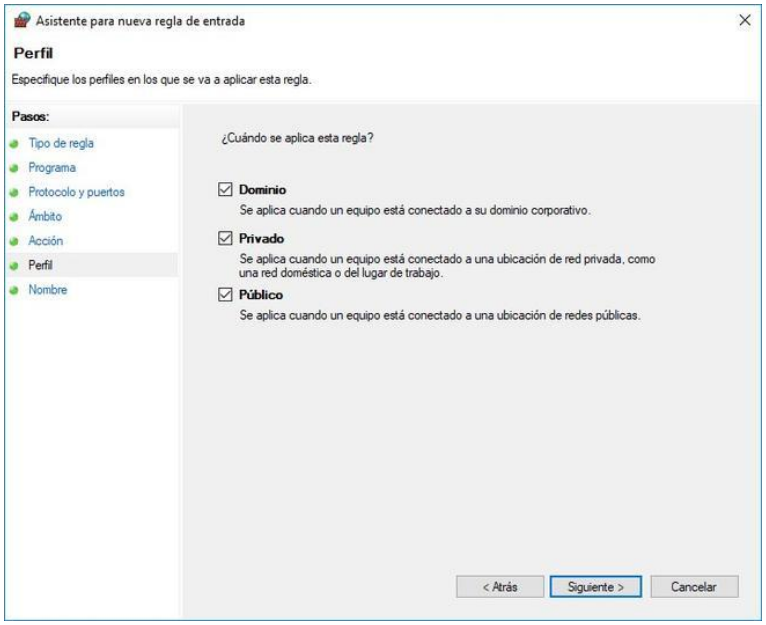


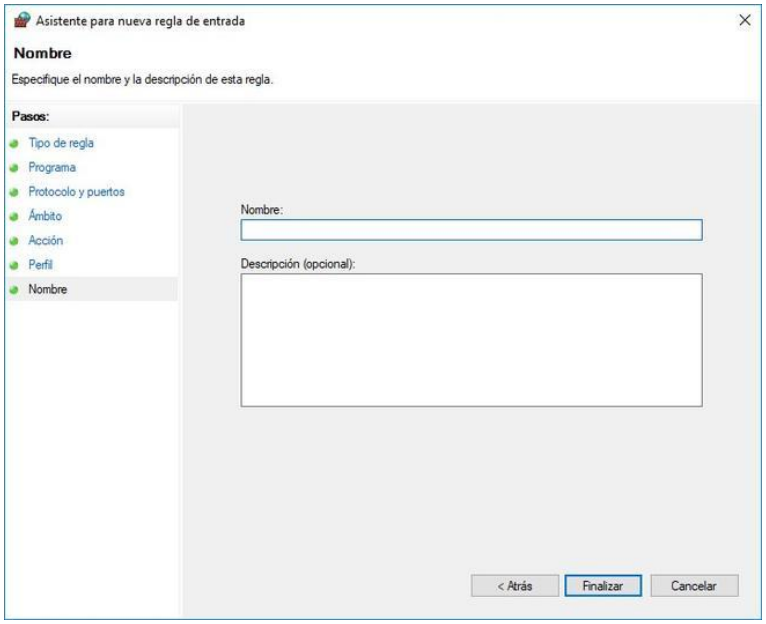
Una vez que hayamos terminado, pinchamos en «Aceptar» y ya habremos introducido todas las direcciones IP que nosotros queramos, de esta forma, habremos metido un rango de direcciones IP, ya sean direcciones IP de origen o destino. Ahora lo que tenemos que hacer es seguir con el asistente de configuración de las diferentes reglas.

A continuación, podremos permitir la conexión configurada, permitir la conexión si es segura, y bloquear la conexión, como en el resto de reglas que ya os hemos enseñado, y también podremos configurar esta regla para que actúe en los perfiles de dominio, público y privado. Por último, podremos ponerle un nombre a la regla y una descripción opcional.







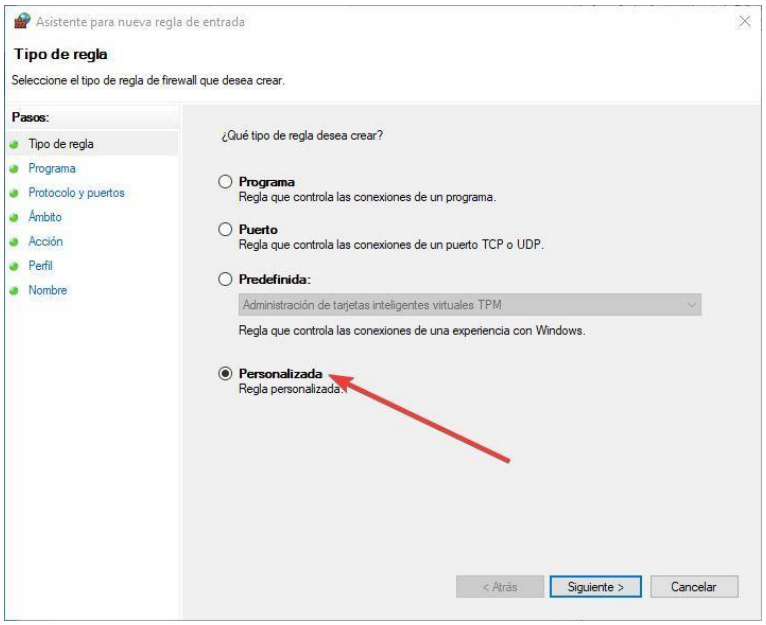


Abrir los puertos en Windows

Para abrir los puertos en este firewall pulsaremos sobre la opción «configuración avanzada» que aparece en el menú de la izquierda para llegar a las opciones de seguridad avanzadas dentro del cortafuegos de Windows.

Empezaremos creando una «regla de entrada». Seleccionamos esta categoría en la parte izquierda y crearemos una nueva regla. En la primera ventana que nos aparecerá seleccionaremos la opción «Personalizada» para poder crear una regla concreta por aplicación y puerto.

Lo ideal para tener la máxima seguridad sería crear dos reglas, una de entrada y otra de salida, bloqueando todo el tráfico que no esté definido en dichas reglas. También hay que especificar si queremos que la regla se aplique en redes públicas, privadas o dentro de un dominio (dejaremos marcadas las 3 casillas) y daremos un nombre para identificar la red.

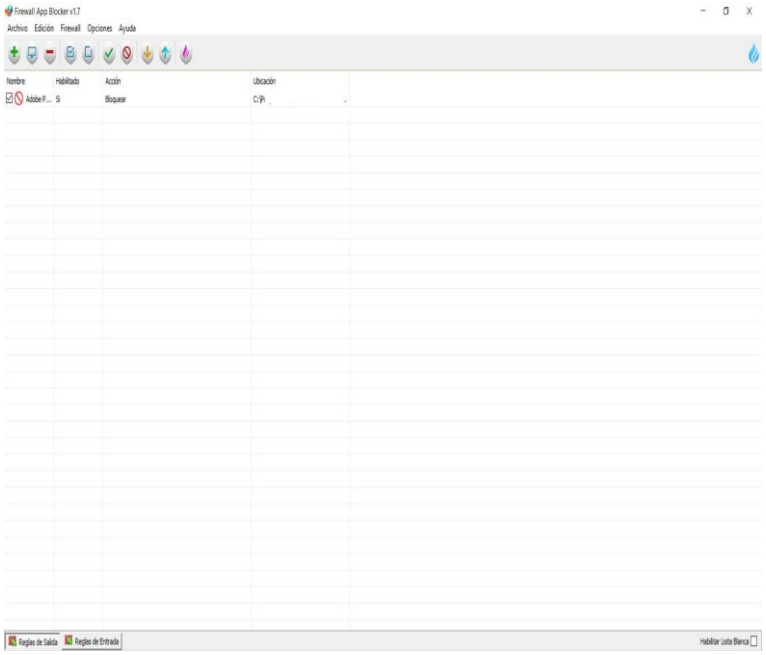


En caso de experimentar algún tipo de problema en la conexión de la aplicación (o de otras) y sospechar que puede ser por un problema de compatibilidad con las reglas que acabamos de crear, desde la lista de reglas del Firewall de Windows podemos deshabilitar la regla, desde las opciones que aparecen al pulsar sobre ella con el botón derecho, para comprobar si realmente el problema es de ella, en cuyo caso habría que afinar, seguramente, el tema de puertos.

Bloquear carpeta con firewall

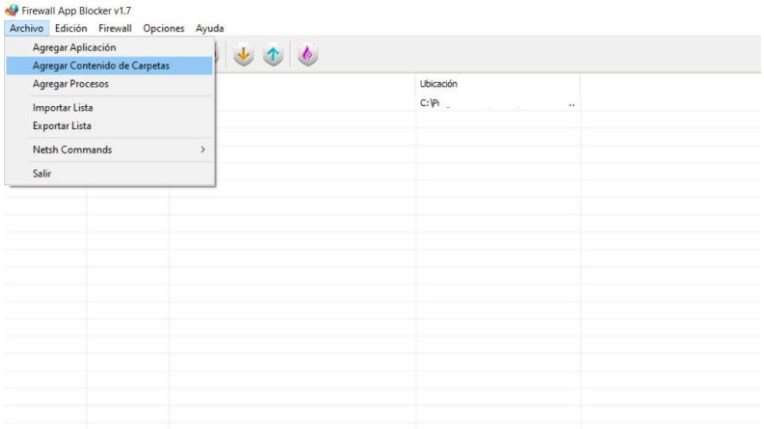
Si quieres bloquear una carpeta usando el firewall, lo vas a poder hacer, y es que en los sistemas operativos de Microsoft más recientes, como Windows 10 o Windows 11, se puede usar el cortafuegos que traen integrados. Funciona muy bien, es gratuito y lo podemos configurar como más nos interese para que pueda bloquear conexiones o crear listas. Una de esas opciones que podemos encontrar en este tipo de programas es bloquear una carpeta en concreto para que no tenga acceso a Internet.

Lo primero que tenemos que hacer es bajar el programa Fab firewall. Está disponible para las últimas versiones de Windows y es totalmente gratuito.



Posteriormente, tenemos que agregar las carpetas que nos interesen. Esto es muy útil si por ejemplo tenemos una serie de aplicaciones instaladas en una única carpeta y queremos que se bloquee el acceso a Internet en todas ellas y de esta forma ahorrar tiempo.

Para ello tenemos que ir a Archivo y pinchar en Agregar contenido de carpetas. Hecho esto, nos aparecerá una nueva ventana para seleccionar la carpeta dentro del equipo y elegir la que corresponda, la que queramos bloquear.



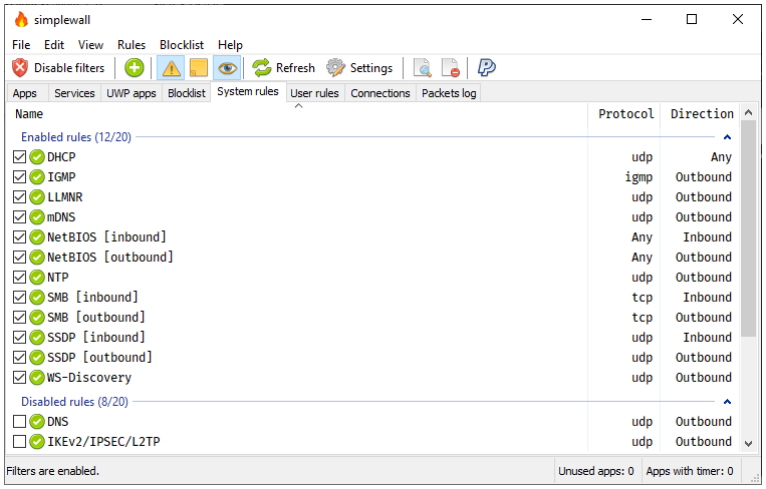
Cualquier programa que tuviéramos instalado y que estuviera dentro de esa carpeta, va a quedar bloqueado. No podrían tener acceso a Internet. Podremos bloquear de golpe tantos programas como queramos, ya que actúa sobre todos los que hay dentro de esa carpeta que hemos agregado.

Lo que hace Fab firewall es crear una nueva regla cada vez que le damos a añadir carpetas. Crea esas reglas tanto en su propia aplicación como en el firewall de Windows, por lo que podemos verlo también en la propia aplicación de Microsoft.

Qué es SimpleWall y cuáles son sus características

Tener un firewall en nuestro equipo Windows es una cuestión innegociable para mantener nuestra seguridad. Microsoft desde Windows XP comenzó con la implementación de un cortafuegos básico. A lo largo de los años, en sus diferentes versiones ha ido mejorando. Su función es controlar el uso que hacen las aplicaciones de nuestra conexión a Internet y también la de ofrecernos protección frente a posibles ataques informáticos provenientes de la red. La llegada de Windows 10 ha supuesto un antes y un después en el sistema operativo de Microsoft. El buen desempeño de Windows Defender y su cortafuegos ha conseguido que cada vez más usuarios le den su confianza. Por este motivo, para complementar este firewall que viene instalado y activado de forma predeterminada, por esto mismo toca hablar de SimpleWall.

En cuanto a SimpleWall podemos definirlo como una herramienta fácil de usar para configurar la plataforma de filtrado de Windows (WFP) que puede configurar la actividad de la red de tu ordenador. Un aspecto importante es que no se trata de una interfaz gráfica para el control del Firewall de Windows y no realiza ningún cambio en el mismo. Su funcionamiento, como ya hemos comentado antes, es sobre la plataforma de filtrado de Windows (WFP). Por si no lo sabéis, se trata de un conjunto de API y servicios del sistema que proporcionan una plataforma para crear aplicaciones de filtrado de red. Esta plataforma de filtrado no es un firewall en sí, pero gracias a SimpleWall vamos a poder crear nuestras reglas de red utilizando esta tecnología.



En cuanto a las características del programa tenemos:

- Es libre y de código abierto.
- Una interfaz gráfica sencilla en la que no hay presentes ventanas emergentes.
- Editor de reglas con el que podremos crear las nuestras.
- Tiene una lista de bloqueo interna para bloquear el espionaje y la telemetría de Windows.
- Cuenta con un registro de paquetes perdidos.
- Soporte para los servicios de Windows y su tienda.
- Compatible con IPv6 y soporte de localización.

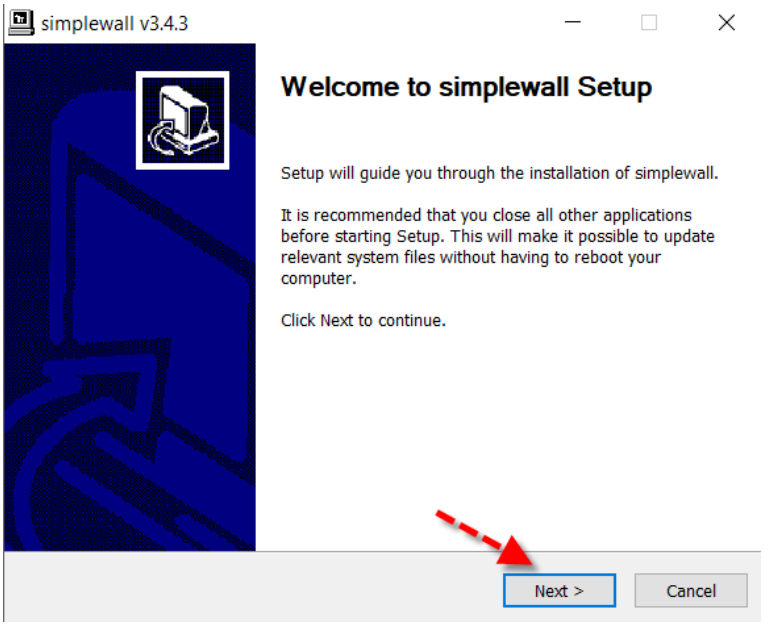
En cuanto a la instalación de reglas, podemos elegir de dos tipos. Unas son las permanentes que funcionan hasta que las desactives manualmente. Las otras son las temporales que desaparecen después de reiniciar. Respecto a si están bloqueadas las conexiones a Internet cuando no se está ejecutando simplewall, la respuesta es sí. Eso significa que, tras haber creado nuestras reglas, tenemos que tener abierta la herramienta.

Requisitos mínimos e instalación de la herramienta

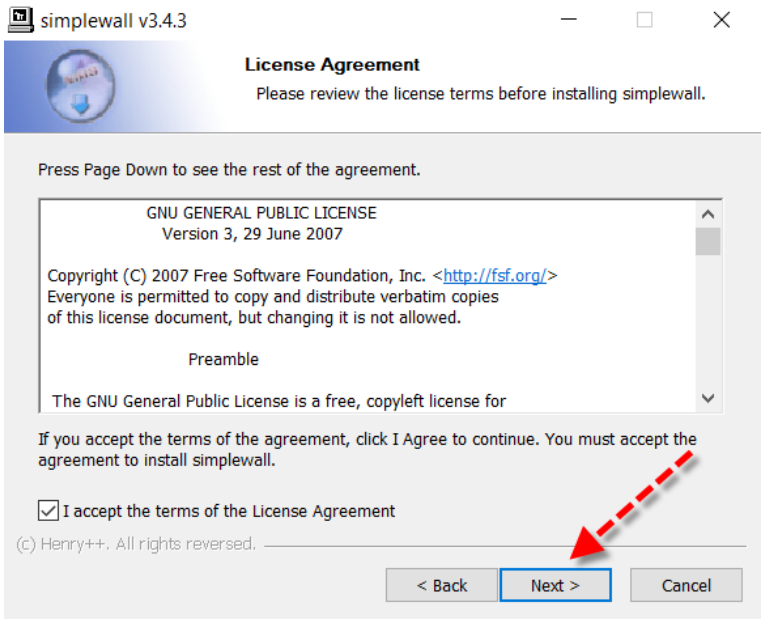
En cuanto a los requisitos mínimos para poder instalar este programa es tener instalado en nuestro equipo Windows 7, 8, 8.1 o 10. Respecto al espacio requerido en disco duro es muy poco, hay que tener en cuenta que su instalador ocupa menos de 1 MB. En nuestro caso la instalación me ha requerido 1.6 MB. La versión que vamos a utilizar para hacer este tutorial de simplewall es la 3.43 pero si hay una versión más reciente conviene que utilicemos la más moderna. Lo primero que tenemos que hacer es ir al sitio web del autor Henry ++ pulsando sobre el siguiente enlace.

Entonces bajamos hasta el apartado Download y descargamos la versión más moderna del programa que termina en setup.exe.

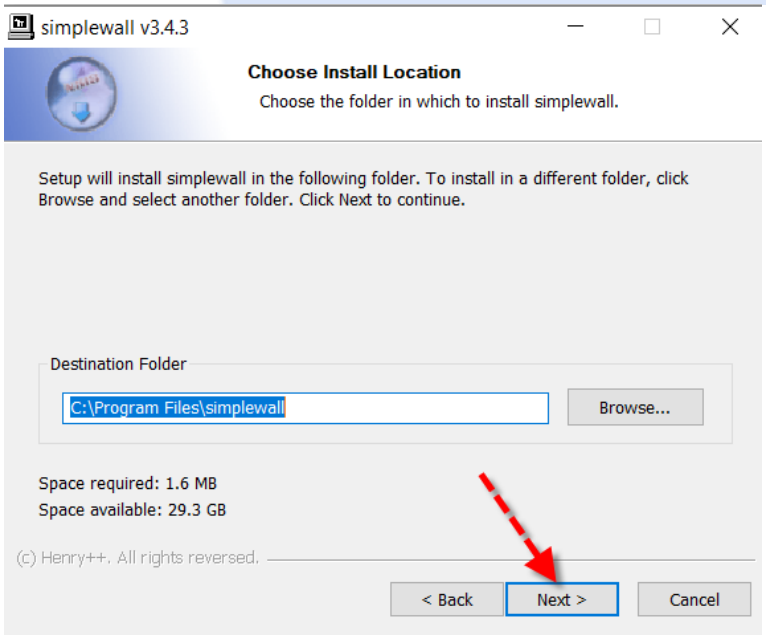
Una vez descargado el instalador lo ejecutamos y nos saldrá una pantalla de bienvenida como esta donde pulsaremos el botón Next:



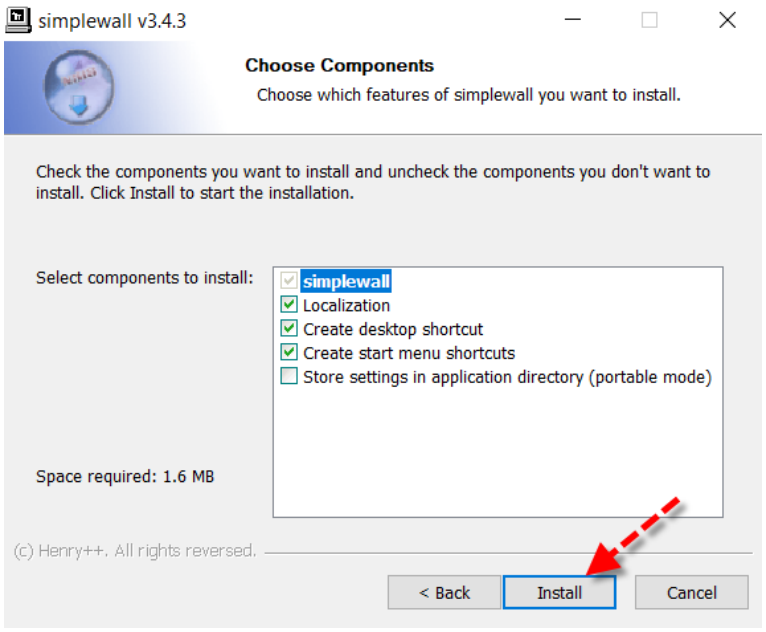
- Luego aceptamos el acuerdo de licencia activando la casilla correspondiente y pulsamos sobre el botón con la flecha roja.



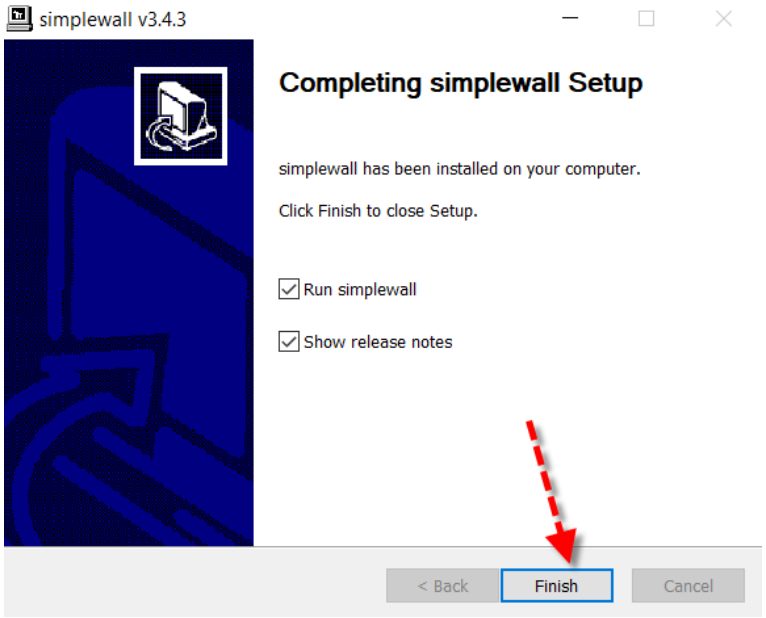
- A continuación, elegimos el directorio de instalación, salvo que haya un motivo especial dejaremos el que viene por defecto.



- Aquí lo dejamos con las opciones que marca, para que nos cree un acceso directo en el escritorio y en el menú de inicio de Windows.



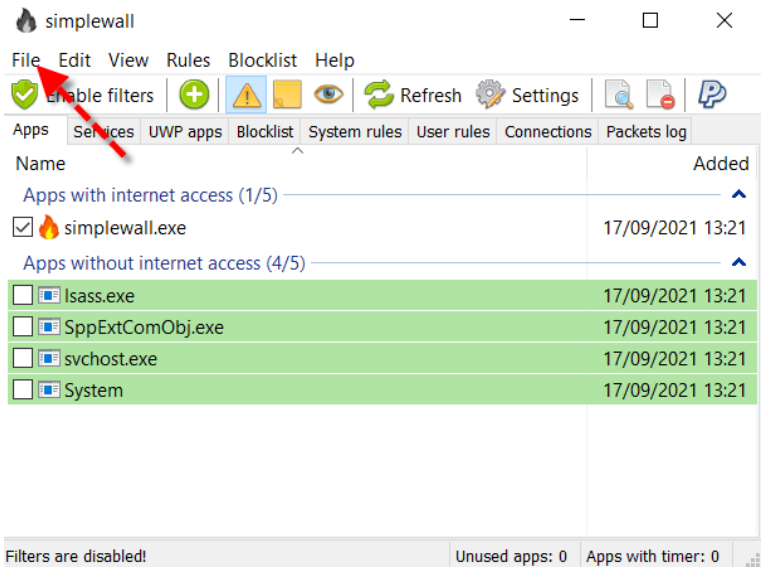
- En el momento que finalice la instalación con éxito de SimpleWall veremos una pantalla como esta.



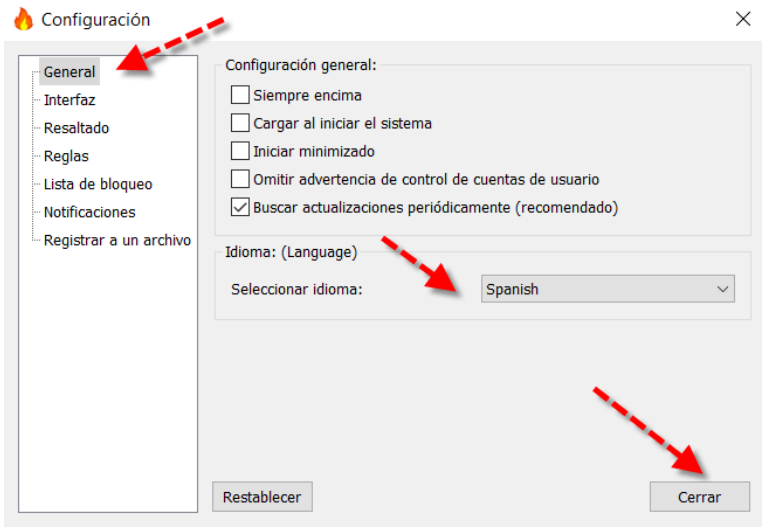
Si pulsamos como viene por defecto en el botón Finish para terminar la instalación se ejecutará por primera vez el programa.

Primeros pasos con SimpleWall para configurar el firewall

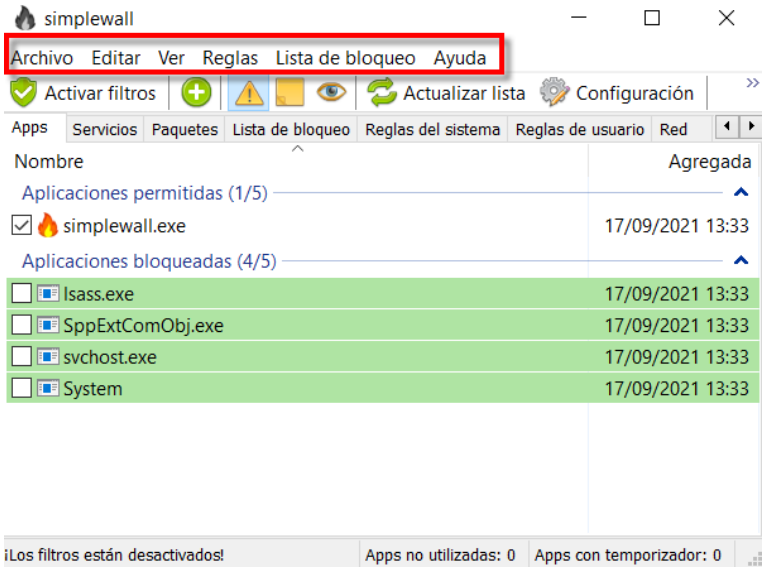
La primera vez que se inicie la herramienta veremos una pantalla como esta:



Como SimpleWall viene en inglés y se puede poner en español, aquí es por donde vamos a empezar. Para ello nos dirigimos a File y dentro seleccionamos Settings. En el apartado general en Language seleccionamos Spanish y le damos a cerrar. También una opción interesante que se usa mucho en «Configuración General» es Cargar al iniciar el sistema para que lo ejecute al arrancar Windows.



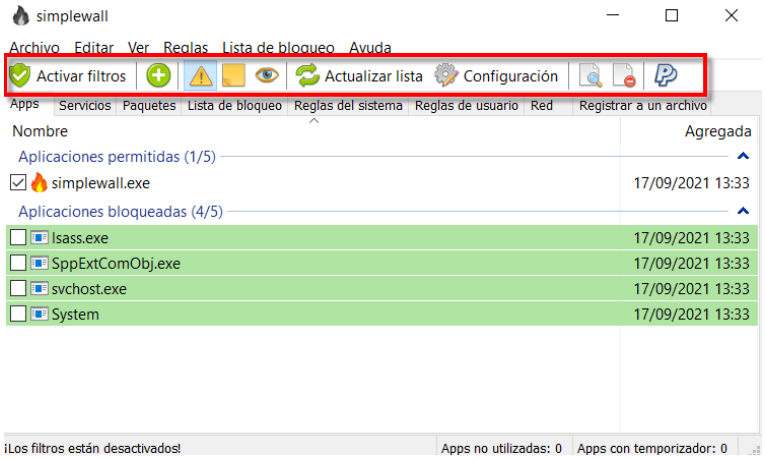
Ahora ya tenemos todo en castellano y vamos a ver el menú principal de esta herramienta que tenéis señalado con un recuadro rojo.



Aquí tenemos estas opciones:

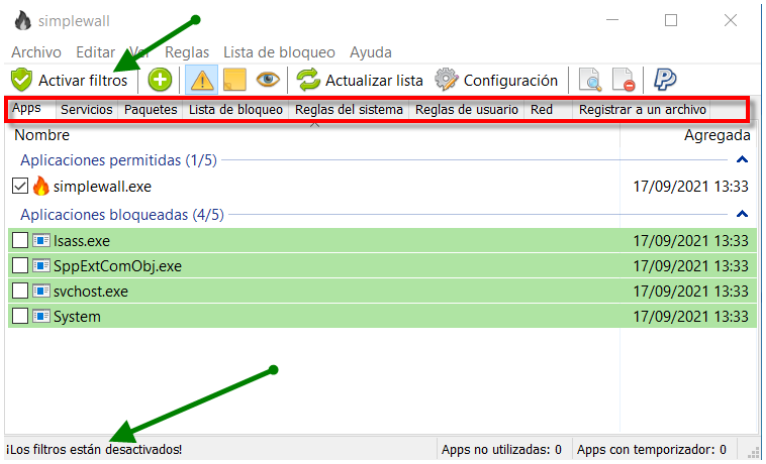
- Archivo: podemos acceder a la configuración de opciones y trabajar con archivos.
- Editar: para purgar apps no utilizadas, buscar y actualizar lista.
- Ver: sirve para elegir opciones de visualización y la fuente de letra.
- Reglas: para configurar como trabajan las reglas conviene dejarlo como viene por defecto.
- Lista de bloqueo: sirve para configurar cómo actúan las listas de bloqueo y conviene dejarlo como está.
- Ayuda: para ir a la web del autor para obtener información, comprobar si hay actualizaciones y ver qué versión tenemos instalada.

Justo debajo tenemos una botonera que simplemente lo que nos hace es ofrecernos accesos directos a las opciones más importantes del menú principal o de la creación de reglas. Por ejemplo, si pulsamos el botón «Configuración» iremos directamente al lugar donde se cambia el idioma y otros muchos más parámetros. Luego más adelante profundizaremos con algún botón más.



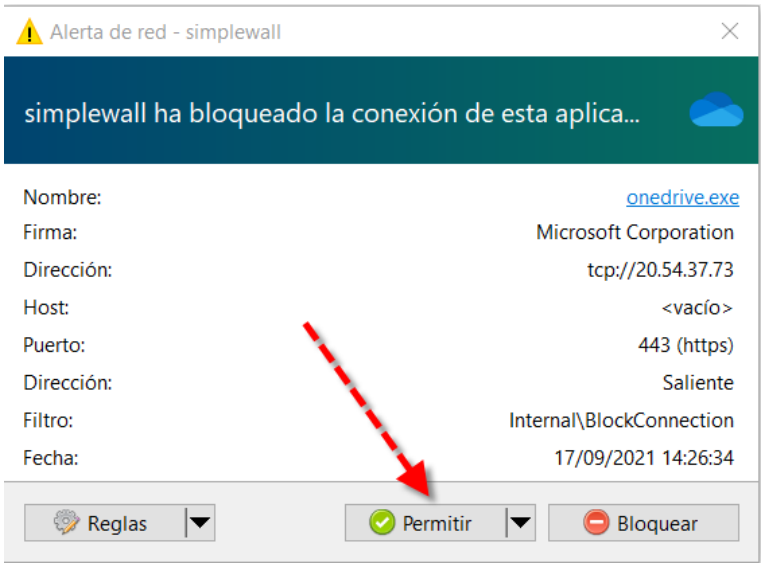
Cómo crear una regla, activar filtros y más

Ahora llega el momento de empezar a trabajar con SimpleWall. Debajo de la botonera tenéis una serie de pestañas señaladas con un recuadro con las que deberéis operar. Cada una de ellas tiene una función bien diferenciada.

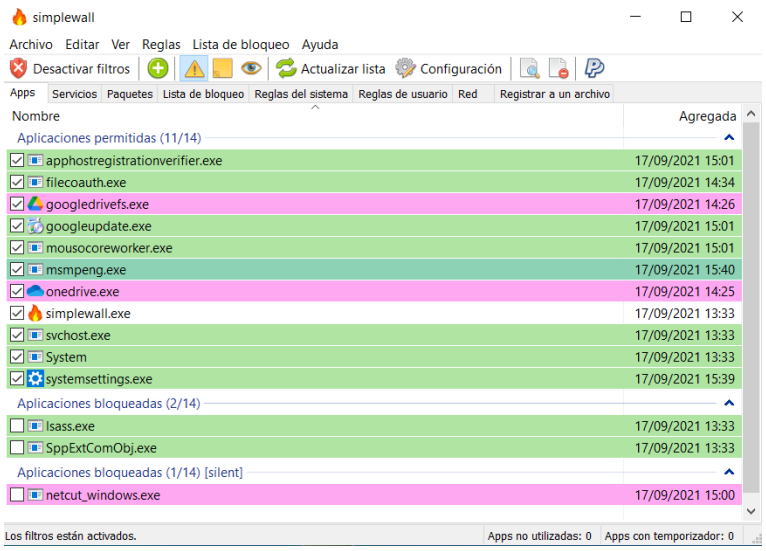


Según queremos trabajar con aplicaciones, servicios de Windows, lista de bloqueo y más, tendremos que seleccionar la pestaña adecuada. Por defecto, viene en el de Apps que se refiere a programas y que es con la que vamos a trabajar. Una cosa muy importante a tener en cuenta es que, en cualquiera de las pestañas como se aprecia en el lugar que señala la flecha verde abajo, los filtros están desactivados. Por lo tanto, si queréis que se apliquen deberéis pulsar sobre el botón Activar filtros.

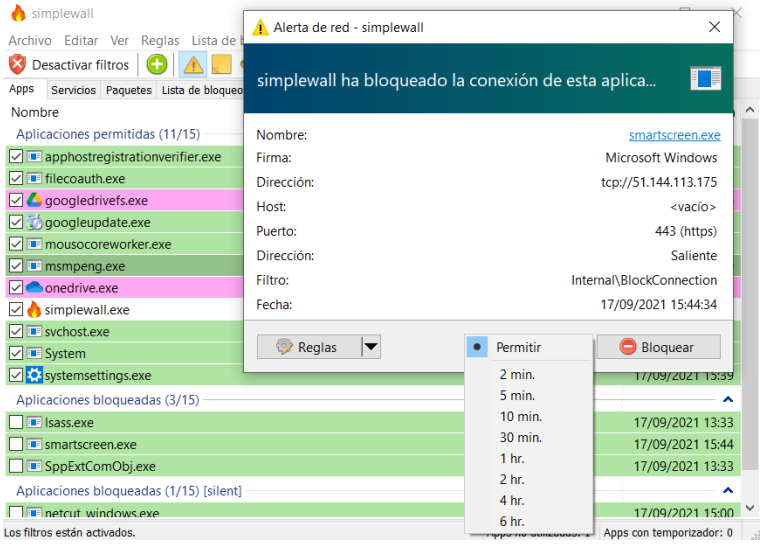
Seguidamente en ese momento SimpleWall ha bloqueado la conexión de la aplicación OneDrive de Microsoft. Como la que utilizo y me hace falta le he dado a Permitir para que me cree la regla. Justo después hemos hecho lo mismo con la de Google Drive.



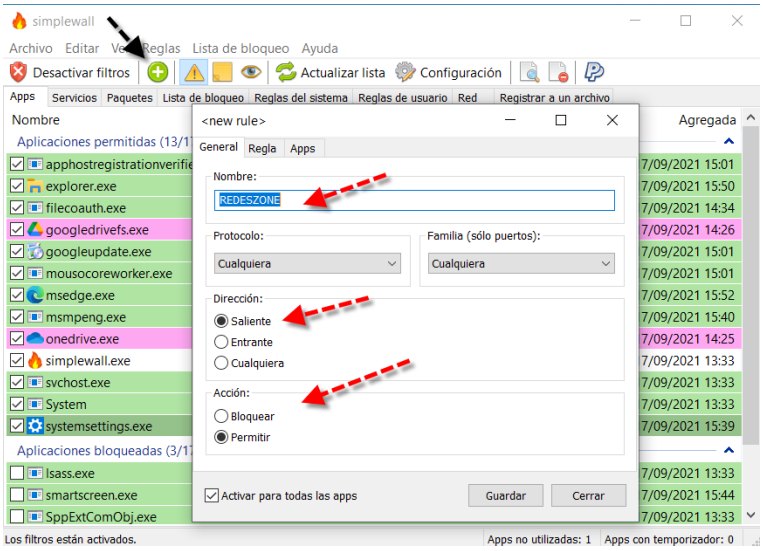
Luego tras varias peticiones que nos irá haciendo clasificará los programas en permitidos, bloqueados y bloqueados silenciosos. También activando la casilla de un programa pasará a permitidos.



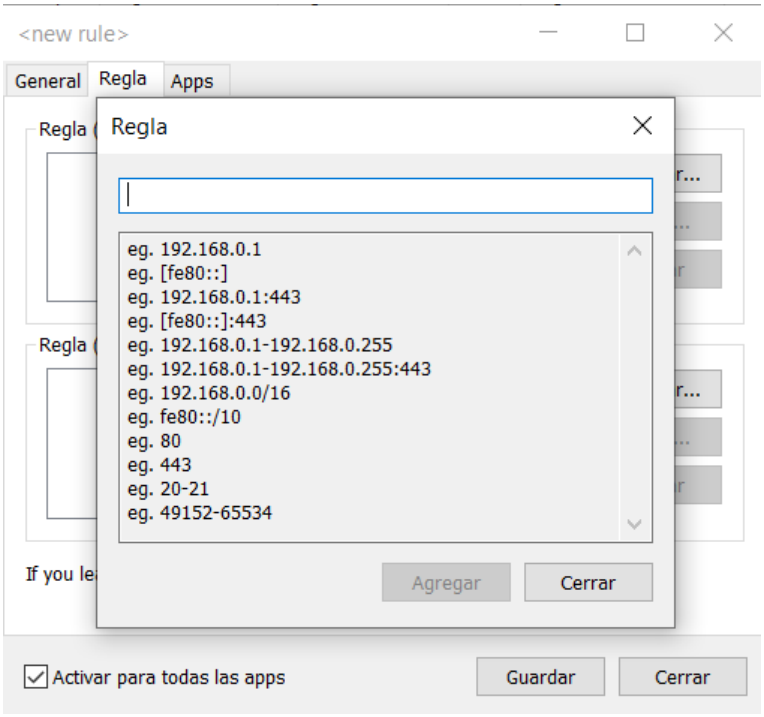
Además, a la hora de conceder acceso con nuestras reglas, el botón Permitir admite la creación de reglas temporales pulsando sobre el icono del triángulo negro invertido.



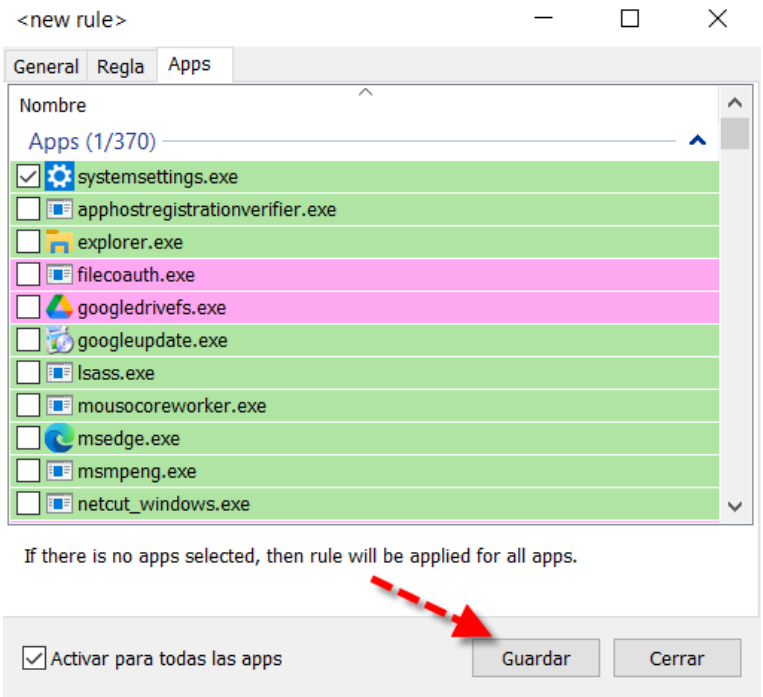
Por otra parte, si pulsamos sobre el botón con un + señalado con la flecha negra podremos crear nuestras reglas personales. En este caso para Apps, pero también podríamos hacerlas en otros apartados.



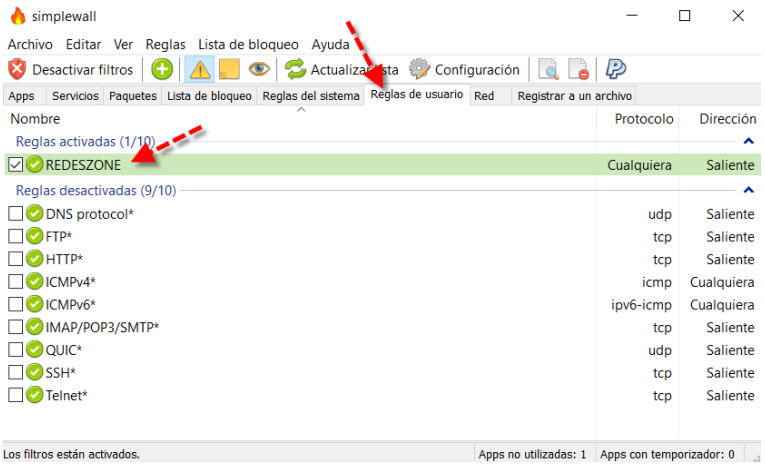
En General pones el nombre a la regla, luego el protocolo y la familia opcional. Entonces establecemos la dirección, ya sea entrante, saliente o cualquiera, y una acción que será permitir o bloquear. En la pestaña Regla podremos trabajar con IPs locales y remotas junto con su puerto si hace falta.



Por otra parte, en el apartado Apps podemos asignar que esa regla se aplique a un programa concreto. Si no se selecciona nada se aplica a todas las aplicaciones. Y cuando terminemos le damos a Guardar.



Por último, si queremos ver la regla que hemos creado iremos a la pestaña Reglas de usuario. Allí podremos borrarla, editarla y ver si está activa o no.



Tal y como habéis visto, SimpleWall nos permitirá administrar el firewall de Windows de manera muy fácil, avanzada y su funcionamiento es realmente intuitivo. Si no utilizas el firewall del propio Windows Defender, podéis usar este SimpleWall porque os facilitará enormemente la tarea de permitir o denegar las conexiones en tu PC con Windows.

Fuente:

- https://www.redeszone.net/tutoriales/seguridad/configuracion-firewall-windows-10/
- https://help.ovhcloud.com/csm/es-vps-firewall-windows?id=kb_article_view&sysparm_article=KB0056968

INSTITUTO

KHIPU