

**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

- ¿Qué es un firewall?
  - ¿Cómo de completo es el firewall de Windows?
  - Ventajas de usar el firewall de Windows
- Configuración avanzada del firewall
  - Reglas de entrada y reglas de salida
  - Cómo crear una regla personalizada
  - Bloquear carpeta con firewall
- Qué es SimpleWall y cuáles son sus características
  - Requisitos mínimos e instalación de la herramienta
  - Primeros pasos con SimpleWall para configurar el firewall
- Importancia de la seguridad
  - Comprueba que tu conexión a Internet es segura
  - Herramientas de seguridad y sistemas actualizados
  - Comprobar que el antivirus funciona correctamente
  - Observar las medidas de seguridad del router
  - Navegador fiable y actualizado
  - Usar VPN en redes públicas

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.

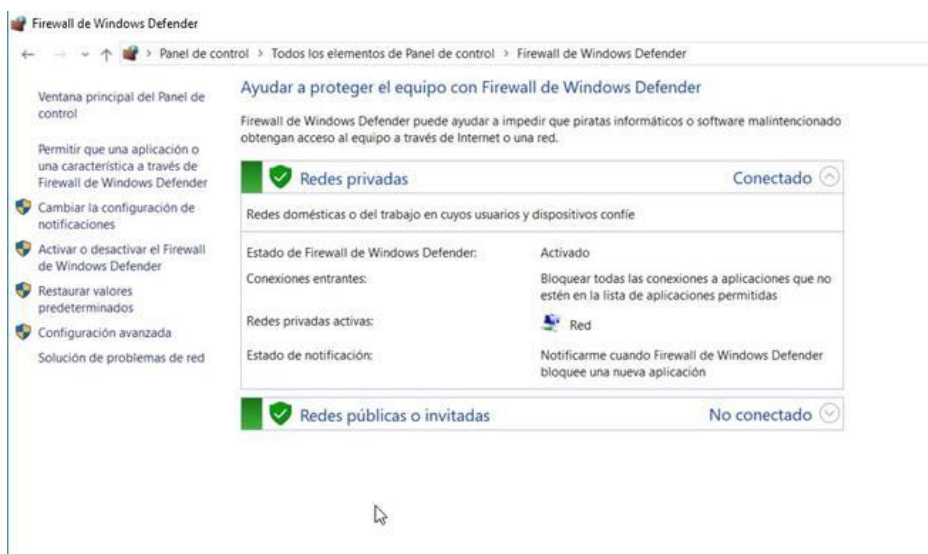
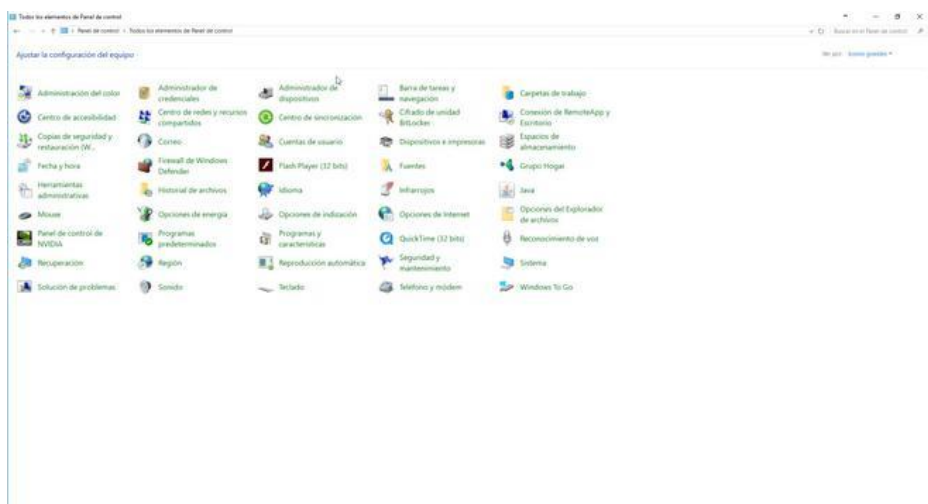
- **Integración nativa:** El firewall de Windows viene integrado de manera nativa en el sistema operativo, lo que significa que no es necesario descargar ni instalar ningún software adicional. Esto simplifica la gestión y asegura que cada sistema Windows tenga acceso a una capa básica de protección.
- **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.

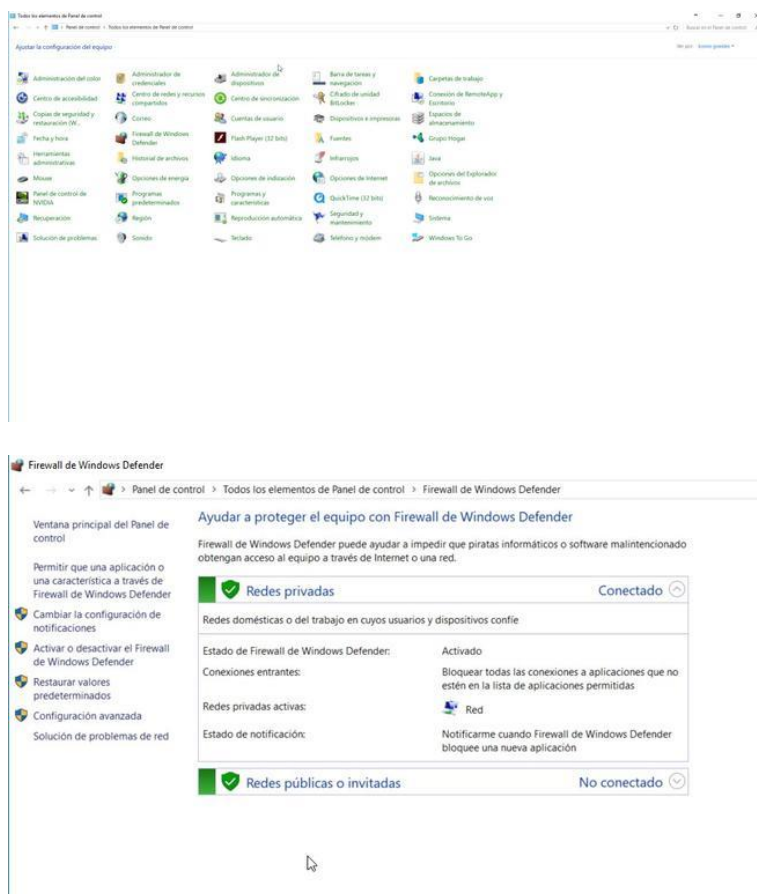
**Registro de eventos:** Registra eventos relacionados con la seguridad, lo que facilita la identificación y resolución de posibles problemas. Los registros permiten realizar un seguimiento de las actividades del firewall y proporciona información importante en caso de necesitar datos de seguridad.

### 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.

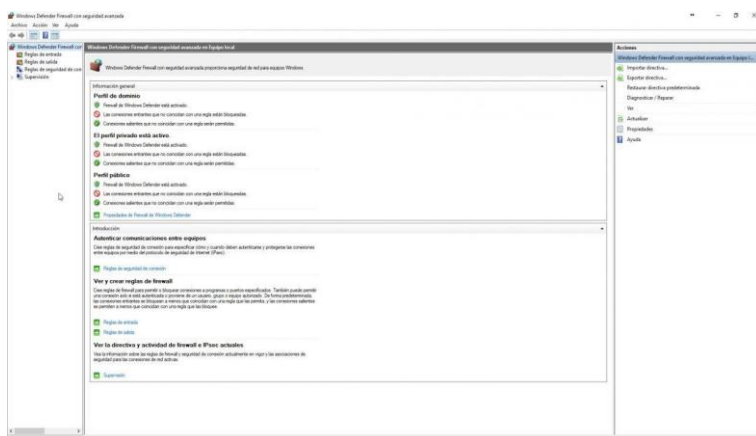




En el menú de configuración avanzada del firewall de Windows 10 tendremos acceso a todas las reglas de entrada, de salida, y el resumen de todas las reglas creadas tanto de entrada y salida en el firewall.

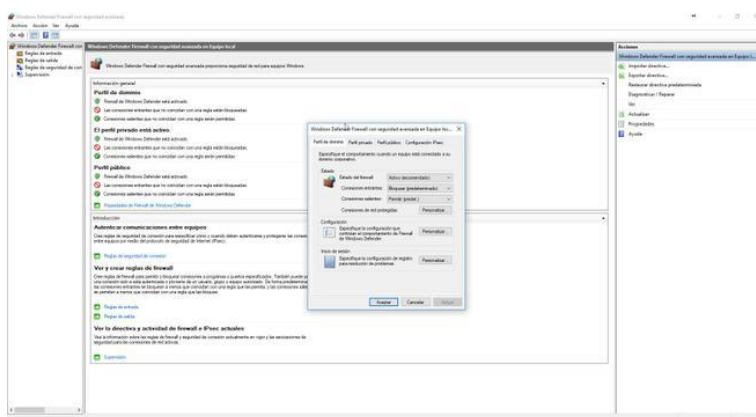
En el menú principal de esta configuración avanzada tenemos las políticas predeterminadas de los tres perfiles que tenemos disponibles: perfil de dominio, perfil privado, público. Dependiendo del perfil que tengamos asignado a nuestra red local, tendremos unos permisos u otros.

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.

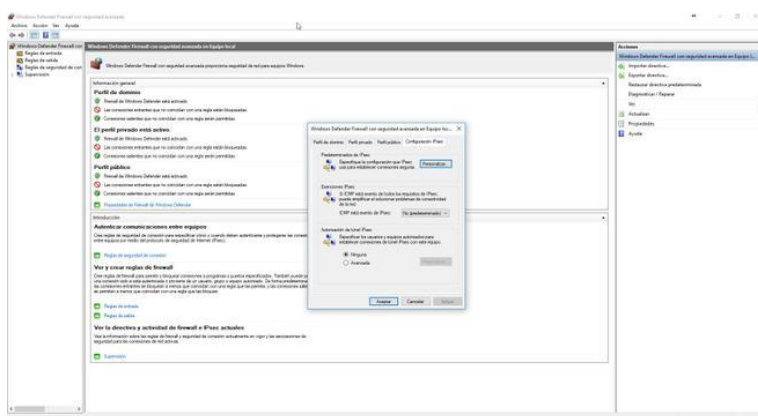
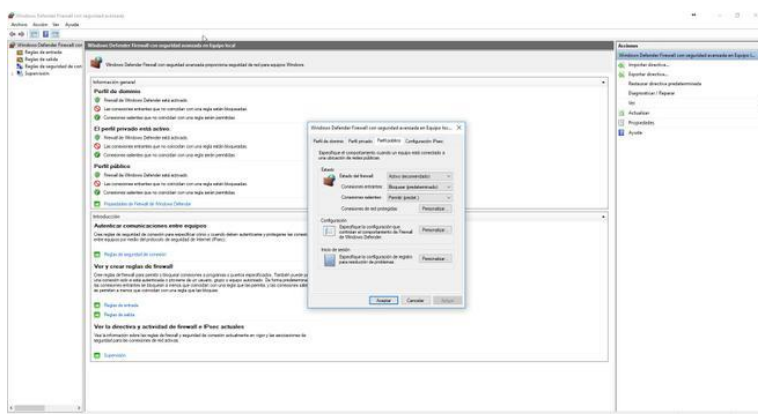
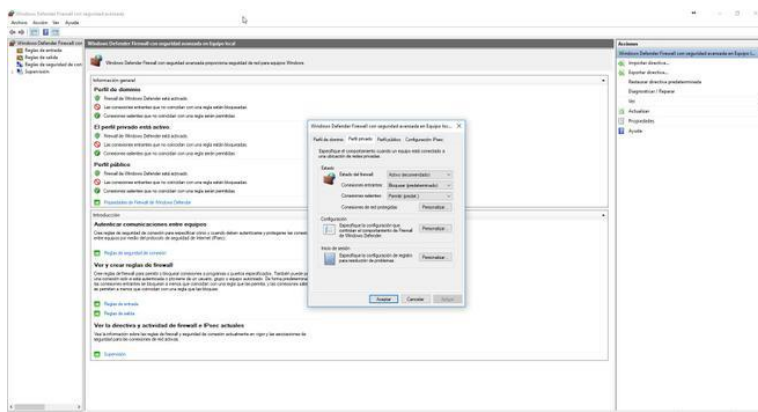


Si pinchamos en el botón de «Propiedades de Firewall de Windows Defender», podremos cambiar las configuraciones globales de todos los perfiles. Tendremos la posibilidad de habilitar o deshabilitar el firewall dependiendo del perfil asignado, cambiar la política (permisiva o restrictiva) tanto de las 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.

[illegible]

## 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.

[illegible]



## TEMA: CONFIGURACIÓN DE FIREWALL

[illegible][illegible]

Programa de Trabajo: Plan de desarrollo de competencias											
Programa de Trabajo											
Objeto de estudio											
Nombre	Equipo	Asesor	Actividad	Actividad	Programa	Descripción de la actividad	Procedimiento	Producto	Punto de control	Punto de entrega	España en el mundo
Elaboración de la programación de la asignatura	Equipo 1	Asesor 1	Actividad 1	Actividad 1	Programa 1	Descripción de la actividad 1	Procedimiento 1	Producto 1	Punto de control 1	Punto de entrega 1	España en el mundo 1
Elaboración de la programación de la asignatura	Equipo 2	Asesor 2	Actividad 2	Actividad 2	Programa 2	Descripción de la actividad 2	Procedimiento 2	Producto 2	Punto de control 2	Punto de entrega 2	España en el mundo 2
Elaboración de la programación de la asignatura	Equipo 3	Asesor 3	Actividad 3	Actividad 3	Programa 3	Descripción de la actividad 3	Procedimiento 3	Producto 3	Punto de control 3	Punto de entrega 3	España en el mundo 3
Elaboración de la programación de la asignatura	Equipo 4	Asesor 4	Actividad 4	Actividad 4	Programa 4	Descripción de la actividad 4	Procedimiento 4	Producto 4	Punto de control 4	Punto de entrega 4	España en el mundo 4
Elaboración de la programación de la asignatura	Equipo 5	Asesor 5	Actividad 5	Actividad 5	Programa 5	Descripción de la actividad 5	Procedimiento 5	Producto 5	Punto de control 5	Punto de entrega 5	España en el mundo 5
Elaboración de la programación de la asignatura	Equipo 6	Asesor 6	Actividad 6	Actividad 6	Programa 6	Descripción de la actividad 6	Procedimiento 6	Producto 6	Punto de control 6	Punto de entrega 6	España en el mundo 6
Elaboración de la programación de la asignatura	Equipo 7	Asesor 7	Actividad 7	Actividad 7	Programa 7	Descripción de la actividad 7	Procedimiento 7	Producto 7	Punto de control 7	Punto de entrega 7	España en el mundo 7
Elaboración de la programación de la asignatura	Equipo 8	Asesor 8	Actividad 8	Actividad 8	Programa 8	Descripción de la actividad 8	Procedimiento 8	Producto 8	Punto de control 8	Punto de entrega 8	España en el mundo 8
Elaboración de la programación de la asignatura	Equipo 9	Asesor 9	Actividad 9	Actividad 9	Programa 9	Descripción de la actividad 9	Procedimiento 9	Producto 9	Punto de control 9	Punto de entrega 9	España en el mundo 9
Elaboración de la programación de la asignatura	Equipo 10	Asesor 10	Actividad 10	Actividad 10	Programa 10	Descripción de la actividad 10	Procedimiento 10	Producto 10	Punto de control 10	Punto de entrega 10	España en el mundo 10
Elaboración de la programación de la asignatura	Equipo 11	Asesor 11	Actividad 11	Actividad 11	Programa 11	Descripción de la actividad 11	Procedimiento 11	Producto 11	Punto de control 11	Punto de entrega 11	España en el mundo 11
Elaboración de la programación de la asignatura	Equipo 12	Asesor 12	Actividad 12	Actividad 12	Programa 12	Descripción de la actividad 12	Procedimiento 12	Producto 12	Punto de control 12	Punto de entrega 12	España en el mundo 12
Elaboración de la programación de la asignatura	Equipo 13	Asesor 13	Actividad 13	Actividad 13	Programa 13	Descripción de la actividad 13	Procedimiento 13	Producto 13	Punto de control 13	Punto de entrega 13	España en el mundo 13
Elaboración de la programación de la asignatura	Equipo 14	Asesor 14	Actividad 14	Actividad 14	Programa 14	Descripción de la actividad 14	Procedimiento 14	Producto 14	Punto de control 14	Punto de entrega 14	España en el mundo 14
Elaboración de la programación de la asignatura	Equipo 15	Asesor 15	Actividad 15	Actividad 15	Programa 15	Descripción de la actividad 15	Procedimiento 15	Producto 15	Punto de control 15	Punto de entrega 15	España en el mundo 15
Elaboración de la programación de la asignatura	Equipo 16	Asesor 16	Actividad 16	Actividad 16	Programa 16	Descripción de la actividad 16	Procedimiento 16	Producto 16	Punto de control 16	Punto de entrega 16	España en el mundo 16
Elaboración de la programación de la asignatura	Equipo 17	Asesor 17	Actividad 17	Actividad 17	Programa 17	Descripción de la actividad 17	Procedimiento 17	Producto 17	Punto de control 17	Punto de entrega 17	España en el mundo 17
Elaboración de la programación de la asignatura	Equipo 18	Asesor 18	Actividad 18	Actividad 18	Programa 18	Descripción de la actividad 18	Procedimiento 18	Producto 18	Punto de control 18	Punto de entrega 18	España en el mundo 18
Elaboración de la programación de la asignatura	Equipo 19	Asesor 19	Actividad 19	Actividad 19	Programa 19	Descripción de la actividad 19	Procedimiento 19	Producto 19	Punto de control 19	Punto de entrega 19	España en el mundo 19
Elaboración de la programación de la asignatura	Equipo 20	Asesor 20	Actividad 20	Actividad 20	Programa 20	Descripción de la actividad 20	Procedimiento 20	Producto 20	Punto de control 20	Punto de entrega 20	España en el mundo 20
Elaboración de la programación de la asignatura	Equipo 21	Asesor 21	Actividad 21	Actividad 21	Programa 21	Descripción de la actividad 21	Procedimiento 21	Producto 21	Punto de control 21	Punto de entrega 21	España en el mundo 21
Elaboración de la programación de la asignatura	Equipo 22	Asesor 22	Actividad 22	Actividad 22	Programa 22	Descripción de la actividad 22	Procedimiento 22	Producto 22	Punto de control 22	Punto de entrega 22	España en el mundo 22
Elaboración de la programación de la asignatura	Equipo 23	Asesor 23	Actividad 23	Actividad 23	Programa 23	Descripción de la actividad 23	Procedimiento 23	Producto 23	Punto de control 23	Punto de entrega 23	España en el mundo 23
Elaboración de la programación de la asignatura	Equipo 24	Asesor 24	Actividad 24	Actividad 24	Programa 24	Descripción de la actividad 24	Procedimiento 24	Producto 24	Punto de control 24	Punto de entrega 24	España en el mundo 24
Elaboración de la programación de la asignatura	Equipo 25	Asesor 25	Actividad 25	Actividad 25	Programa 25	Descripción de la actividad 25	Procedimiento 25	Producto 25	Punto de control 25	Punto de entrega 25	España en el mundo 25
Elaboración de la programación de la asignatura	Equipo 26	Asesor 26	Actividad 26	Actividad 26	Programa 26	Descripción de la actividad 26	Procedimiento 26	Producto 26	Punto de control 26	Punto de entrega 26	España en el mundo 26
Elaboración de la programación de la asignatura	Equipo 27	Asesor 27	Actividad 27	Actividad 27	Programa 27	Descripción de la actividad 27	Procedimiento 27	Producto 27	Punto de control 27	Punto de entrega 27	España en el mundo 27
Elaboración de la programación de la asignatura	Equipo 28	Asesor 28	Actividad 28	Actividad 28	Programa 28	Descripción de la actividad 28	Procedimiento 28	Producto 28	Punto de control 28	Punto de entrega 28	España en el mundo 28
Elaboración de la programación de la asignatura	Equipo 29	Asesor 29	Actividad 29	Actividad 29	Programa 29	Descripción de la actividad 29	Procedimiento 29	Producto 29	Punto de control 29	Punto de entrega 29	España en el mundo 29
Elaboración de la programación de la asignatura	Equipo 30	Asesor 30	Actividad 30	Actividad 30	Programa 30	Descripción de la actividad 30	Procedimiento 30	Producto 30	Punto de control 30	Punto de entrega 30	España en el mundo 30
Elaboración de la programación de la asignatura	Equipo 31	Asesor 31	Actividad 31	Actividad 31	Programa 31	Descripción de la actividad 31	Procedimiento 31	Producto 31	Punto de control 31	Punto de entrega 31	España en el mundo 31
Elaboración de la programación de la asignatura	Equipo 32	Asesor 32	Actividad 32	Actividad 32	Programa 32	Descripción de la actividad 32	Procedimiento 32	Producto 32	Punto de control 32	Punto de entrega 32	España en el mundo 32
Elaboración de la programación de la asignatura	Equipo 33	Asesor 33	Actividad 33	Actividad 33	Programa 33	Descripción de la actividad 33	Procedimiento 33	Producto 33	Punto de control 33	Punto de entrega 33	España en el mundo 33
Elaboración de la programación de la asignatura	Equipo 34	Asesor 34	Actividad 34	Actividad 34	Programa 34	Descripción de la actividad 34	Procedimiento 34	Producto 34	Punto de control 34	Punto de entrega 34	España en el mundo 34
Elaboración de la programación de la asignatura	Equipo 35	Asesor 35	Actividad 35	Actividad 35	Programa 35	Descripción de la actividad 35	Procedimiento 35	Producto 35	Punto de control 35	Punto de entrega 35	España en el mundo 35
Elaboración de la programación de la asignatura	Equipo 36	Asesor 36	Actividad 36	Actividad 36	Programa 36	Descripción de la actividad 36	Procedimiento 36	Producto 36	Punto de control 36	Punto de entrega 36	España en el mundo 36
Elaboración de la programación de la asignatura	Equipo 37	Asesor 37	Actividad 37	Actividad 37	Programa 37	Descripción de la actividad 37	Procedimiento 37	Producto 37	Punto de control 37	Punto de entrega 37	España en el mundo 37
Elaboración de la programación de la asignatura	Equipo 38	Asesor 38	Actividad 38	Actividad 38	Programa 38	Descripción de la actividad 38	Procedimiento 38	Producto 38	Punto de control 38	Punto de entrega 38	España en el mundo 38
Elaboración de la programación de la asignatura	Equipo 39	Asesor 39	Actividad 39	Actividad 39	Programa 39	Descripción de la actividad 39	Procedimiento 39	Producto 39	Punto de control 39	Punto de entrega 39	España en el mundo 39
Elaboración de la programación de la asignatura	Equipo 40	Asesor 40	Actividad 40	Actividad 40	Programa 40	Descripción de la actividad 40	Procedimiento 40	Producto 40	Punto de control 40	Punto de entrega 40	España en el mundo 40
Elaboración de la programación de la asignatura	Equipo 41	Asesor 41	Actividad 41	Actividad 41	Programa 41	Descripción de la actividad 41	Procedimiento 41	Producto 41	Punto de control 41	Punto de entrega 41	España en el mundo 41
Elaboración de la programación de la asignatura	Equipo 42	Asesor 42	Actividad 42	Actividad 42	Programa 42	Descripción de la actividad 42	Procedimiento 42	Producto 42	Punto de control 42	Punto de entrega 42	España en el mundo 42
Elaboración de la programación de la asignatura	Equipo 43	Asesor 43	Actividad 43	Actividad 43	Programa 43	Descripción de la actividad 43	Procedimiento 43	Producto 43	Punto de control 43	Punto de entrega 43	España en el mundo 43
Elaboración de la programación de la asignatura	Equipo 44	Asesor 44	Actividad 44	Actividad 44	Programa 44	Descripción de la actividad 44	Procedimiento 44	Producto 44	Punto de control 44	Punto de entrega 44	España en el mundo 44
Elaboración de la programación de la asignatura	Equipo 45	Asesor 45	Actividad 45	Actividad 45	Programa 45	Descripción de la actividad 45	Procedimiento 45	Producto 45	Punto de control 45	Punto de entrega 45	España en el mundo 45
Elaboración de la programación de la asignatura	Equipo 46	Asesor 46	Actividad 46	Actividad 46	Programa 46	Descripción de la actividad 46	Procedimiento 46	Producto 46	Punto de control 46	Punto de entrega 46	España en el mundo 46
Elaboración de la programación de la asignatura	Equipo 47	Asesor 47	Actividad 47	Actividad 47	Programa 47	Descripción de la actividad 47	Procedimiento 47	Producto 47	Punto de control 47	Punto de entrega 47	España en el mundo 47
Elaboración de la programación de la asignatura	Equipo 48	Asesor 48	Actividad 48	Actividad 48	Programa 48	Descripción de la actividad 48	Procedimiento 48	Producto 48	Punto de control 48	Punto de entrega 48	España en el mundo 48
Elaboración de la programación de la asignatura	Equipo 49	Asesor 49	Actividad 49	Actividad 49	Programa 49	Descripción de la actividad 49	Procedimiento 49	Producto 49	Punto de control 49	Punto de entrega 49	España en el mundo 49
Elaboración de la programación de la asignatura	Equipo 50	Asesor 50	Actividad 50	Actividad 50	Programa 50	Descripción de la actividad 50	Procedimiento 50	Producto 50	Punto de control 50	Punto de entrega 50	España en el mundo 50
Elaboración de la programación de la asignatura	Equipo 51	Asesor 51	Actividad 51	Actividad 51	Programa 51	Descripción de la actividad 51	Procedimiento 51	Producto 51	Punto de control 51	Punto de entrega 51	España en el mundo 51
Elaboración de la programación de la asignatura	Equipo 52	Asesor 52	Actividad 52	Actividad 52	Programa 52	Descripción de la actividad 52	Procedimiento 52	Producto 52	Punto de control 52	Punto de entrega 52	España en el mundo 52
Elaboración de la programación de la asignatura	Equipo 53	Asesor 53	Actividad 53	Actividad 53	Programa 53	Descripción de la actividad 53	Procedimiento 53	Producto 53	Punto de control 53	Punto de entrega 53	España en el mundo 53
Elaboración de la programación de la asignatura	Equipo 54	Asesor 54	Actividad 54	Actividad 54	Programa 54	Descripción de la actividad 54	Procedimiento 54	Producto 54	Punto de control 54	Punto de entrega 54	España en el mundo 54
Elaboración de la programación de la asignatura	Equipo 55	Asesor 55	Actividad 55	Actividad 55	Programa 55	Descripción de la actividad 55	Procedimiento 55	Producto 55	Punto de control 55	Punto de entrega 55	España en el mundo 55
Elaboración de la programación de la asignatura	Equipo 56	Asesor 56	Actividad 56	Actividad 56	Programa 56	Descripción de la actividad 56	Procedimiento 56	Producto 56	Punto de control 56	Punto de entrega 56	España en el mundo 56
Elaboración de la programación de la asignatura	Equipo 57	Asesor 57	Actividad 57	Actividad 57	Programa 57	Descripción de la actividad 57	Procedimiento 57	Producto 57	Punto de control 57	Punto de entrega 57	España en el mundo 57
Elaboración de la programación de la asignatura	Equipo 58	Asesor 58	Actividad 58	Actividad 58	Programa 58	Descripción de la actividad 58	Procedimiento 58	Producto 58	Punto de control 58	Punto de entrega 58	España en el mundo 58
Elaboración de la programación de la asignatura	Equipo 59	Asesor 59	Actividad 59	Actividad 59	Programa 59	Descripción de la actividad 59	Procedimiento 59	Producto 59	Punto de control 59	Punto de entrega 59	España en el mundo 59
Elaboración de la programación de la asignatura	Equipo 60	Asesor 60	Actividad 60	Actividad 60	Programa 60	Descripción de la actividad 60	Procedimiento 60	Producto 60	Punto de control 60	Punto de entrega 60	España en el mundo 60
Elaboración de la programación de la asignatura	Equipo 61	Asesor 61	Actividad 61	Actividad 61	Programa 61	Descripción de la actividad 61	Procedimiento 61	Producto 61	Punto de control 61	Punto de entrega 61	España en el mundo 61
Elaboración de la programación de la asignatura	Equipo 62	Asesor 62	Actividad 62	Actividad 62	Programa 62	Descripción de la actividad 62	Procedimiento 62	Producto 62	Punto de control 62	Punto de entrega 62	España en el mundo 62
Elaboración de la programación de la asignatura	Equipo 63	Asesor 63	Actividad 63	Actividad 63	Programa 63	Descripción de la actividad 63	Procedimiento 63	Producto 63	Punto de control 63	Punto de entrega 63	España en el mundo 63
Elaboración de la programación de la asignatura	Equipo 64	Asesor 64	Actividad 64	Actividad 64	Programa 64	Descripción de la actividad 64	Procedimiento 64	Producto 64	Punto de control 64	Punto de entrega 64	España en el mundo 64
Elaboración de la programación de la asignatura	Equipo 65	Asesor 65	Actividad 65	Actividad 65	Programa 65	Descripción de la actividad 65	Procedimiento 65	Producto 65	Punto de control 65	Punto de entrega 65	España en el mundo 65
Elaboración de la programación de la asignatura	Equipo 66	Asesor 66	Actividad 66	Actividad 66	Programa 66	Descripción de la actividad 66	Procedimiento 66	Producto 66	Punto de control 66	Punto de entrega 66	España en el mundo 66
Elaboración de la programación de la asignatura	Equipo 67	Asesor 67	Actividad 67	Actividad 67	Programa 67	Descripción de la actividad 67	Procedimiento 67	Producto 67	Punto de control 67	Punto de entrega 67	España en el mundo 67
Elaboración de la programación de la asignatura	Equipo 68	Asesor 68	Actividad 68	Actividad 68	Programa 68	Descripción de la actividad 68	Procedimiento 68	Producto 68	Punto de control 68	Punto de entrega 68	España en el mundo 68
Elaboración de la programación de la asignatura	Equipo 69	Asesor 69	Actividad 69	Actividad 69	Programa 69	Descripción de la actividad 69	Procedimiento 69	Producto 69	Punto de control 69	Punto de entrega 69	España en el mundo 69
Elaboración de la programación de la asignatura	Equipo 70	Asesor 70	Actividad 70	Actividad 70	Programa 70	Descripción de la actividad 70	Procedimiento 70	Producto 70	Punto de control 70	Punto de entrega 70	España en el mundo 70
Elaboración de la programación de la asignatura	Equipo 71	Asesor 71	Actividad 71	Actividad 71	Programa 71	Descripción de la actividad 71	Procedimiento 71	Producto 71	Punto de control 71	Punto de entrega 71	España en el mundo 71
Elaboración de la programación de la asignatura	Equipo 72	Asesor 72	Actividad 72	Actividad 72	Programa 72	Descripción de la actividad 72	Procedimiento 72	Producto 72	Punto de control 72	Punto de entrega 72	España en el mundo 72
Elaboración de la programación de la asignatura	Equipo 73	Asesor 73	Actividad 73	Actividad 73	Programa 73	Descripción de la actividad 73	Procedimiento 73	Producto 73	Punto de control 73	Punto de entrega 73	España en el mundo 73
Elaboración de la programación de la asignatura	Equipo 74	Asesor 74	Actividad 74	Actividad 74	Programa 74	Descripción de la actividad 74	Procedimiento 74	Producto 74	Punto de control 74	Punto de entrega 74	España en el mundo 74
Elaboración de la programación de la asignatura	Equipo 75	Asesor 75	Actividad 75	Actividad 75	Programa 75	Descripción de la actividad 75	Procedimiento 75	Producto 75	Punto de control 75	Punto de entrega 75	España en el mundo 75
Elaboración de la programación de la asignatura	Equipo 76	Asesor 76	Actividad 76	Actividad 76	Programa 76	Descripción de la actividad 76	Procedimiento 76	Producto 76	Punto de control 76	Punto de entrega 76	España en el mundo 76
Elaboración de la programación de la asignatura	Equipo 77	Asesor 77	Actividad 77	Actividad 77	Programa 77	Descripción de la actividad 77	Procedimiento 77	Producto 77	Punto de control 77	Punto de entrega 77	España en el mundo 77
Elaboración de la programación de la asignatura	Equipo 78	Asesor 78	Actividad 78	Actividad 78	Programa 78	Descripción de la actividad 78	Procedimiento 78	Producto 78	Punto de control 78	Punto de entrega 78	España en el mundo 78
Elaboración de la programación de la asignatura	Equipo 79	Asesor 79	Actividad 79	Actividad 79	Programa 79	Descripción de la actividad 79	Procedimiento 79	Producto 79	Punto de control 79	Punto de entrega 79	España en el mundo 79
Elaboración de la programación de la asignatura	Equipo 80	Asesor 80	Actividad 80	Actividad 80	Programa 80	Descripción de la actividad 80	Procedimiento 80	Producto 80	Punto de control 80	Punto de entrega 80	España en el mundo 80
Elaboración de la programación de la asignatura	Equipo 81	Asesor 81	Actividad 81	Actividad 81	Programa 81	Descripción de la actividad 81	Procedimiento 81	Producto 81	Punto de control 81	Punto de entrega 81	España en el mundo 81
Elaboración de la programación de la asignatura	Equipo 82	Asesor 82	Actividad 82	Actividad 82	Programa 82	Descripción de la actividad 82	Procedimiento 82	Producto 82	Punto de control 82	Punto de entrega 82	España en el mundo 82
Elaboración de la programación de la asignatura	Equipo 83	Asesor 83	Actividad 83	Actividad 83	Programa 83	Descripción de la actividad 83	Procedimiento 83	Producto 83	Punto de control 83	Punto de entrega 83	España en el mundo 83
Elaboración de la programación de la asignatura	Equipo 84	Asesor 84	Actividad 84	Actividad 84	Programa 84	Descripción de la actividad 84	Procedimiento 84	Producto 84	Punto de control 84	Punto de entrega 84	España en el mundo 84
Elaboración de la programación de la asignatura	Equipo 85	Asesor 85	Actividad 85	Actividad 85	Programa 85	Descripción de la actividad 85	Procedimiento 85	Producto 85	Punto de control 85	Punto de entrega 85	España en el mundo 85
Elaboración de la programación de la asignatura	Equipo 86	Asesor 86	Actividad 86	Actividad 86	Programa 86	Descripción de la actividad 86	Procedimiento 86	Producto 86	Punto de control 86	Punto de entrega 86	España en el mundo 86
Elaboración de la programación de la asignatura	Equipo 87	Asesor 87	Actividad 87	Actividad 87	Programa 87	Descripción de la actividad 87	Procedimiento 87	Producto 87	Punto de control 87	Punto de entrega 87	España en el mundo 87
Elaboración de la programación de la asignatura	Equipo 88	Asesor 88	Actividad 88	Actividad 88	Programa 88	Descripción de la actividad 88	Procedimiento 88	Producto 88	Punto de control 88	Punto de entrega 88	España en el mundo 88
Elaboración de la programación de la asignatura	Equipo 89	Asesor 89	Actividad 89	Actividad 89							

## 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.

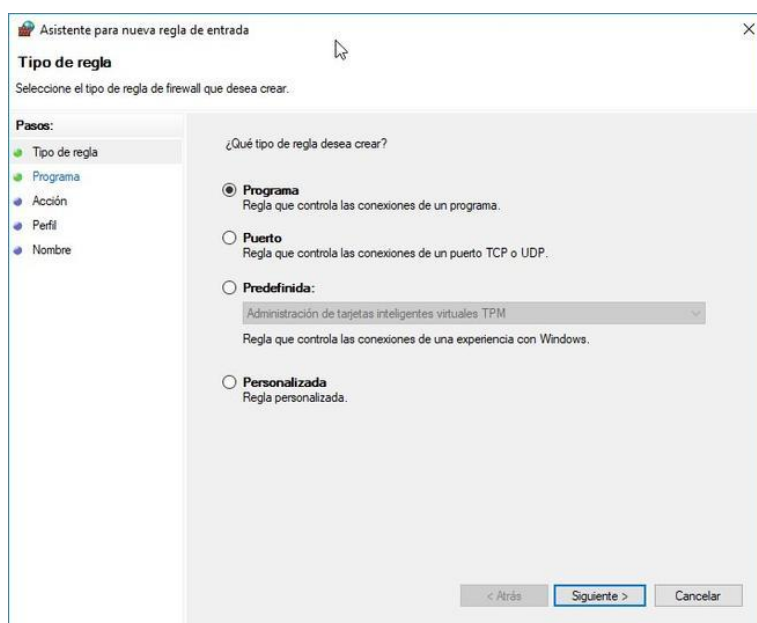
Para crear una nueva regla, pinchamos con el click derecho en «Reglas de entrada» o «reglas de salida» en «Nueva Regla».

### *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:**

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. Estas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

☐ **Bloquear la conexión**

[Personalizar](#)

< 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):

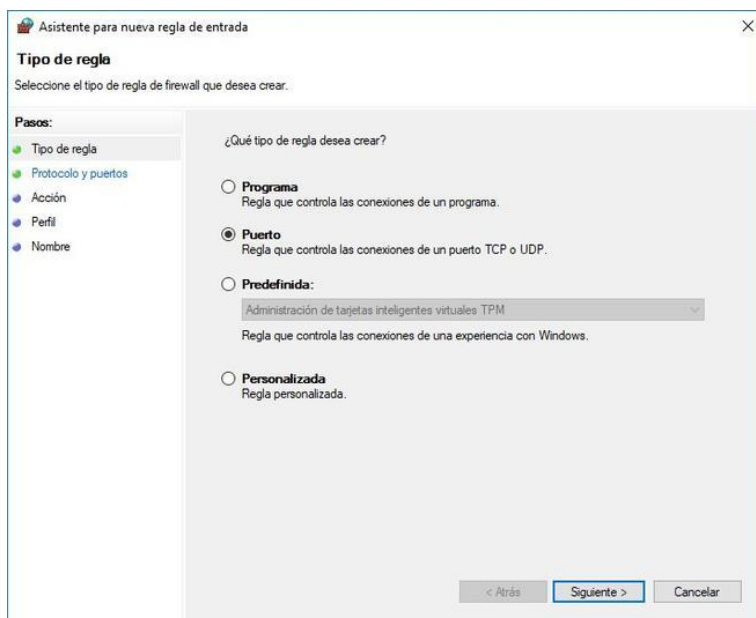
< Atrás **Finalizar** Cancelar

### 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:

< 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.

☐ **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**

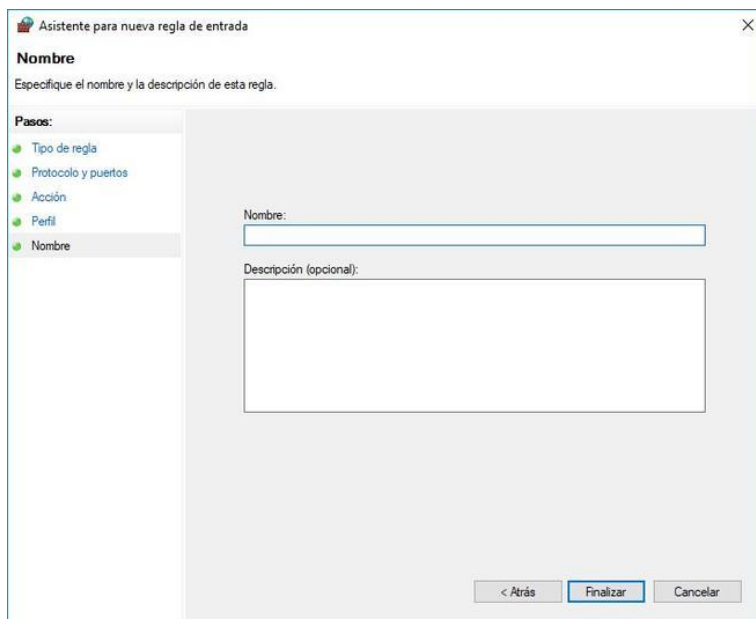
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

☒ **Público**

Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

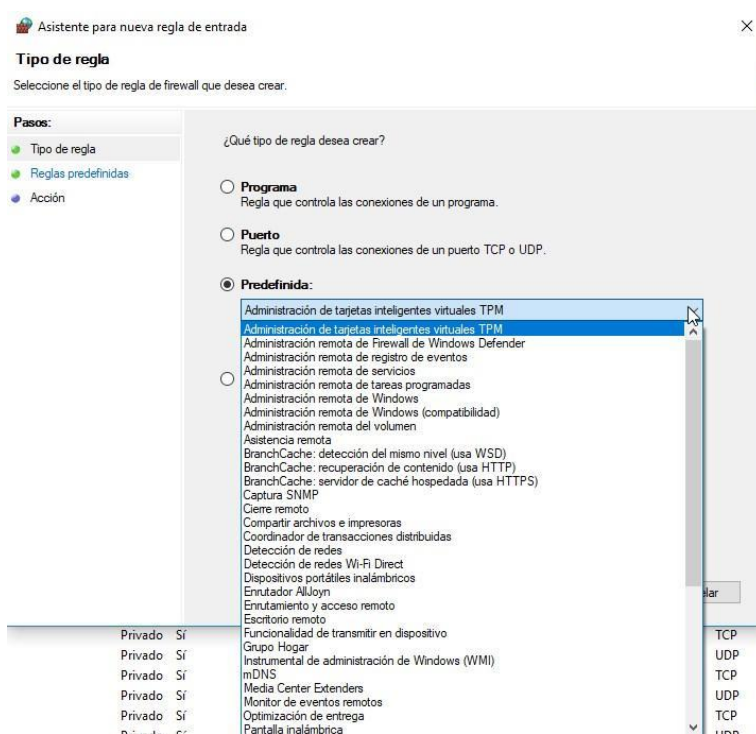
< Atrás   **Siguiente >**   Cancelar





### *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:



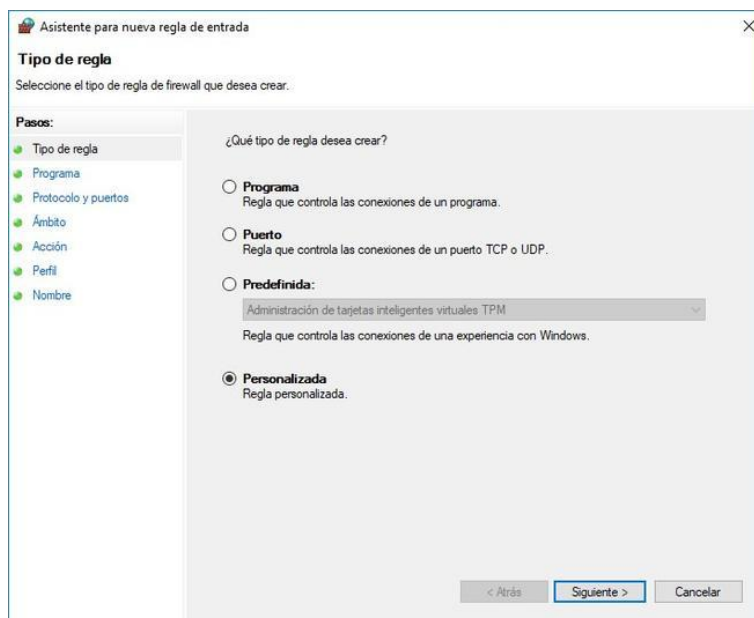
Privado	Sí	Administración de tarjetas inteligentes virtuales TPM	TCP
Privado	Sí	Administración de tarjetas inteligentes virtuales TPM	UDP
Privado	Sí	Administración remota de Firewall de Windows Defender	TCP
Privado	Sí	Administración remota de registro de eventos	UDP
Privado	Sí	Administración remota de servicios	TCP
Privado	Sí	Administración remota de tareas programadas	UDP
Privado	Sí	Administración remota de Windows	TCP
Privado	Sí	Administración remota de Windows (compatibilidad)	UDP
Privado	Sí	Administración remota del volumen	TCP
Privado	Sí	Asistencia remota	UDP
Privado	Sí	BranchCache: detección del mismo nivel (usa WSD)	TCP
Privado	Sí	BranchCache: recuperación de contenido (usa HTTP)	UDP
Privado	Sí	BranchCache: servidor de caché hospedada (usa HTTPS)	TCP
Privado	Sí	Captura SNMP	UDP
Privado	Sí	Cierre remoto	TCP
Privado	Sí	Compartir archivos e impresoras	UDP
Privado	Sí	Coordinador de transacciones distribuidas	TCP
Privado	Sí	Detección de redes	UDP
Privado	Sí	Detección de redes Wi-Fi Direct	TCP
Privado	Sí	Dispositivos portátiles inalámbricos	UDP
Privado	Sí	Enrutador AllJoyn	TCP
Privado	Sí	Enrutamiento y acceso remoto	UDP
Privado	Sí	Escritorio remoto	TCP
Privado	Sí	Funcionalidad de transmitir en dispositivo	UDP
Privado	Sí	Grupo Hogar	TCP
Privado	Sí	Instrumental de administración de Windows (WMI)	UDP
Privado	Sí	mDNS	TCP
Privado	Sí	Media Center Extenders	UDP
Privado	Sí	Monitor de eventos remotos	TCP
Privado	Sí	Optimización de entrega	UDP
Privado	Sí	Pantalla inalámbrica	TCP

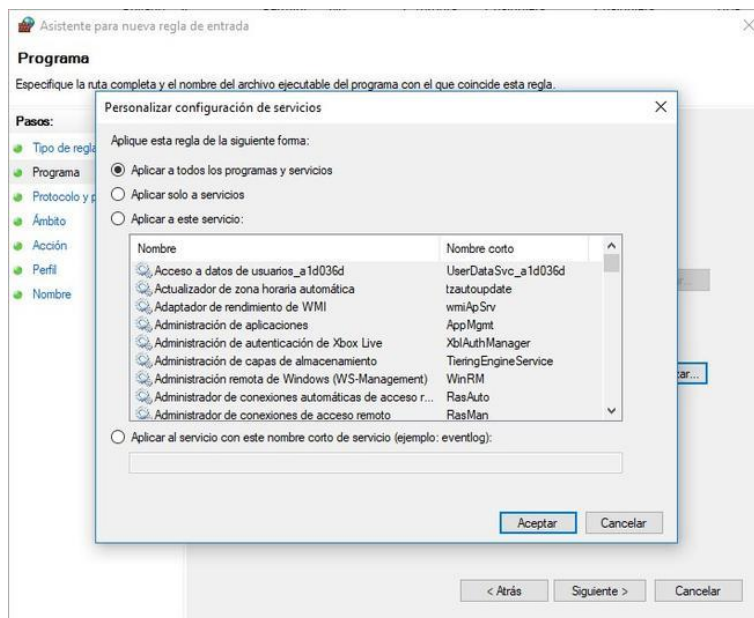
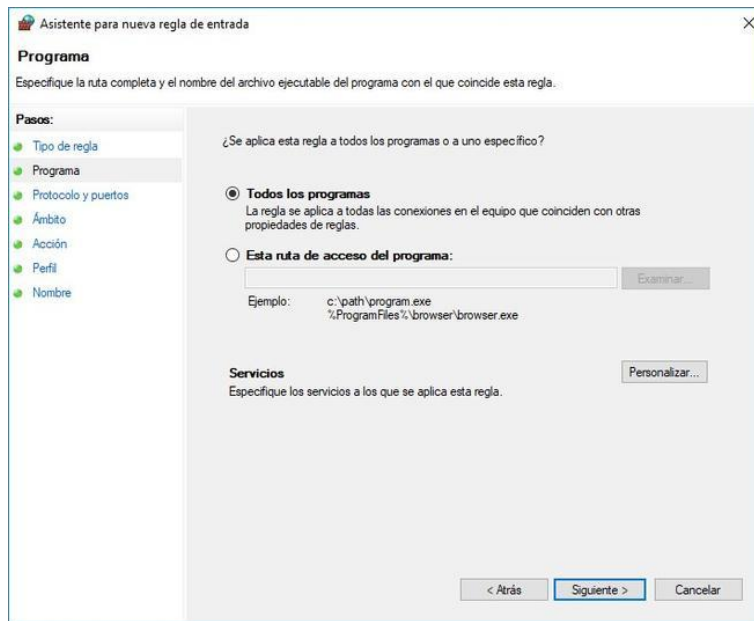
Una vez que hayamos seleccionado la regla, los siguientes pasos son los mismos que en las secciones anteriores, deberemos definir si queremos permitir, permitir con seguridad, o denegar. Después definimos dónde queremos aplicarla (dominio, privado o público), y, por último, proporcionar un nombre y descripción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

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
- Programa
- Protocolo y puertos
- Ámbito
- Acción
- Perfil
- Nombre

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo: **Cualquiera**

Número de protocolo: **Cualquiera**

Puerto local: **Cualquiera**

Puerto remoto: **Cualquiera**

Configuración ICMP: **Cualquiera**

< Atrás   **Siguiente >**   Cancelar

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
- Programa
- Protocolo y puertos
- Ámbito
- Acción
- Perfil
- Nombre

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo: **Personalizado**

Número de protocolo: **0**

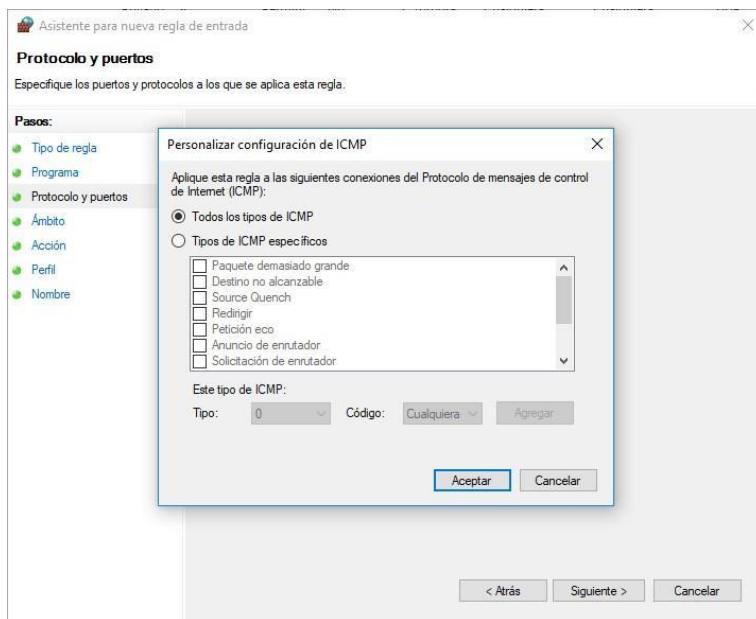
Puerto local: **Todos los puertos**

Puerto remoto: **Todos los puertos**

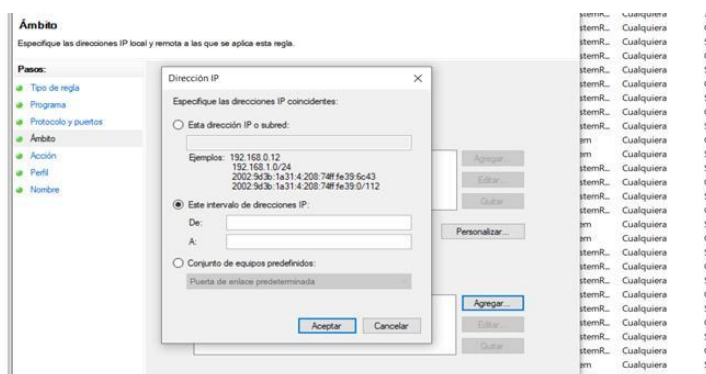
Configuración ICMP: **Personaliz...**

< Atrás   **Siguiente >**   Cancelar

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:

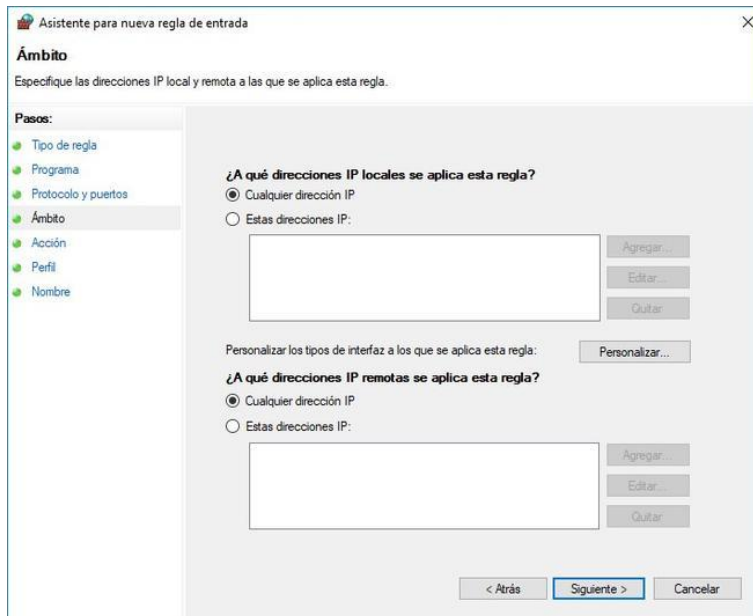
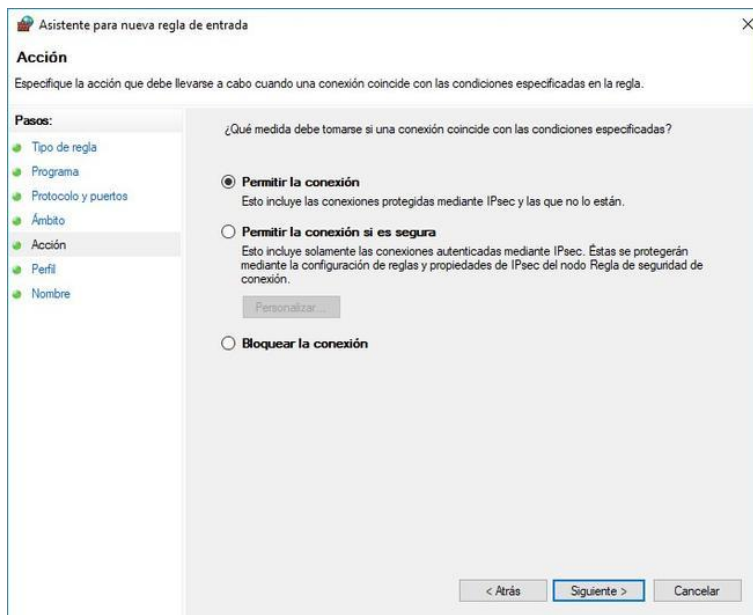


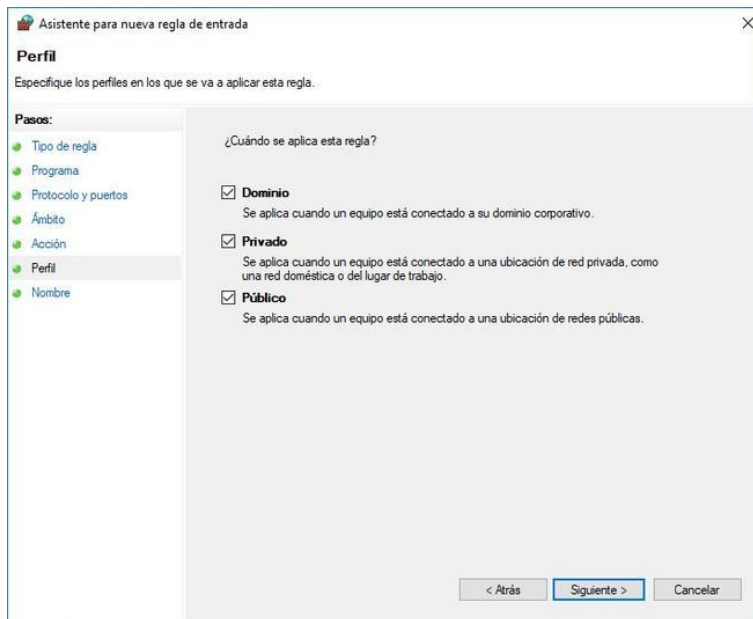
Una vez que hayamos elegido qué protocolo queremos utilizar, vamos a poder definir las direcciones IP locales y remotas donde esta regla debe aplicarse, de esta forma, vamos a tener el control total de cualquier tipo de conexión que hagan al sistema, o que hagamos desde el sistema. En el caso de querer 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.



Asistente para nueva regla de entrada

**Perfil**

Especifique los perfiles en los que se va a aplicar esta regla.

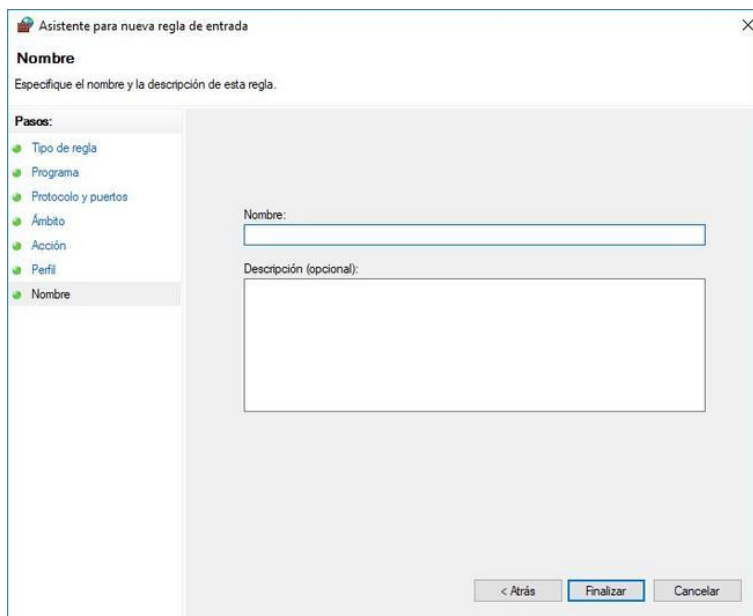
**Pasos:**

- Tipo de regla
- Programa
- Protocolo y puertos
- Ámbito
- 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
- Protocolo y puertos
- Ámbito
- Acción
- Perfil
- Nombre**

Nombre:

Descripción (opcional):

< Atrás   **Finalizar**   Cancelar

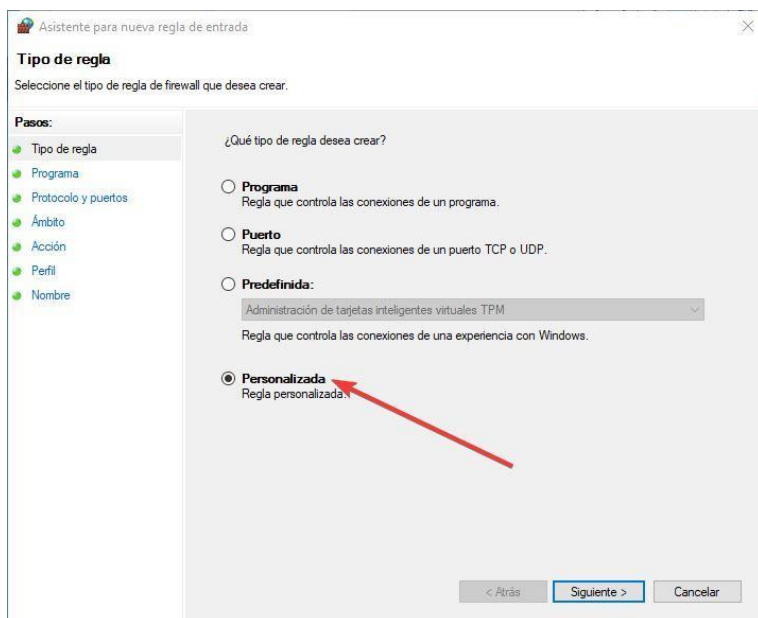
### *Abrir los puertos en Windows*

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.

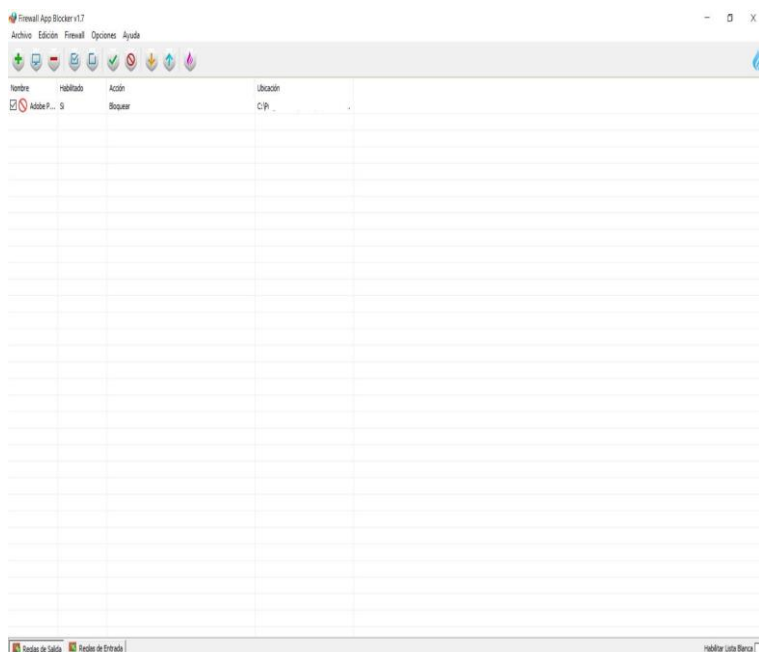


En caso de experimentar algún tipo de problema en la conexión de la aplicación (o de otras) y sospechar que puede ser por un problema de compatibilidad con las reglas que acabamos de crear, desde la lista de reglas del Firewall de Windows podemos deshabilitar la regla, desde las opciones que aparecen 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

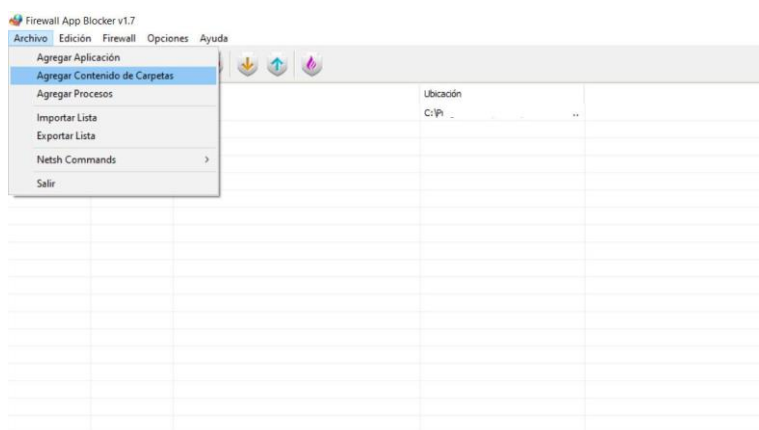
Si quieres bloquear una carpeta usando el firewall, lo vas a poder hacer, y es que en los sistemas operativos de Microsoft más recientes, como Windows 10 o Windows 11, se puede usar el cortafuegos que traen integrados. Funciona muy bien, es gratuito y lo podemos configurar como más nos interese para 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.



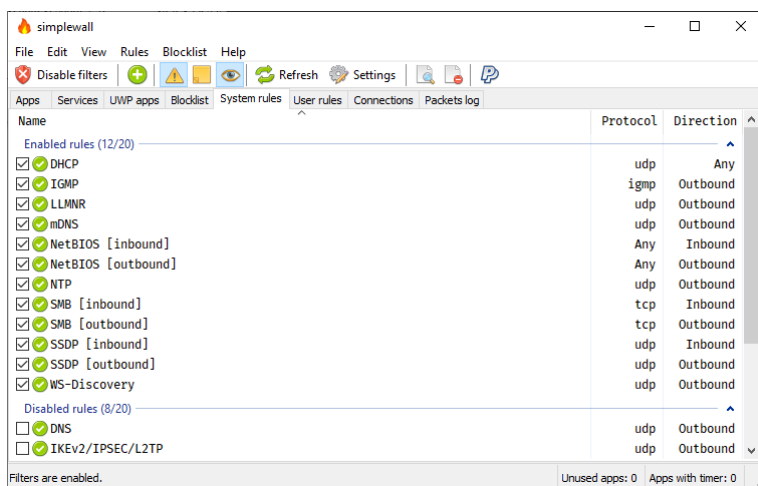
Cualquier programa que tuviéramos instalado y que estuviera dentro de esa carpeta, va a quedar bloqueado. No podrían tener acceso a Internet. Podremos bloquear de golpe tantos programas como queramos, ya que actúa sobre todos los que hay dentro de esa carpeta que hemos agregado.

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.

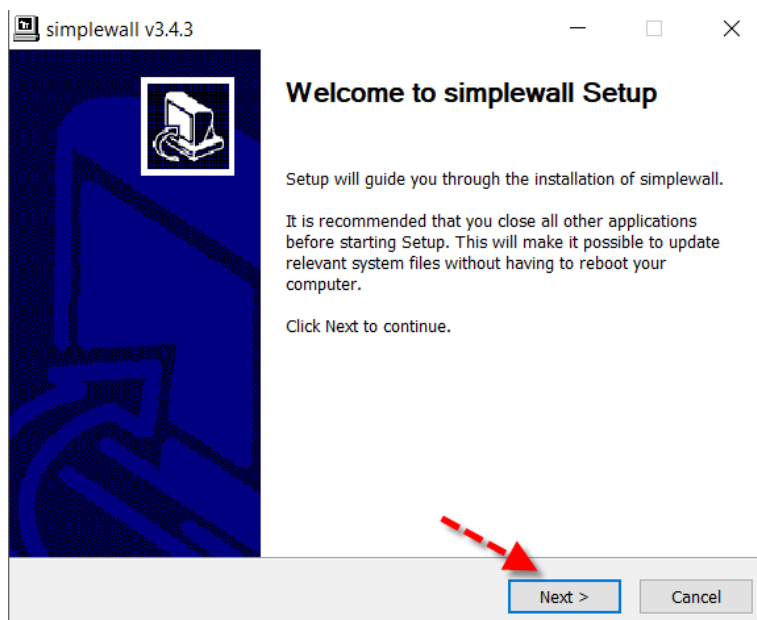
Entonces bajamos hasta el apartado Download y descargamos la versión más moderna del programa que termina en setup.exe.

## Download

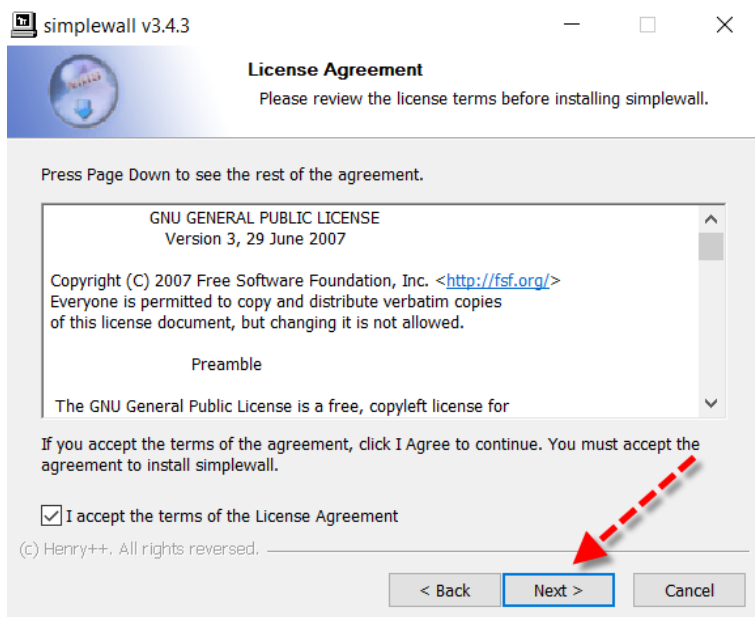
- [simplewall-3.4.3-bin.zip](#)
- [simplewall-3.4.3-setup.exe](#)
- [simplewall-3.4.3-setup.exe.sig](#)
- [simplewall-3.4.3-pdb.zip](#)
- [simplewall-3.4.3.sha256](#)

[Latest stable release is always here](#)

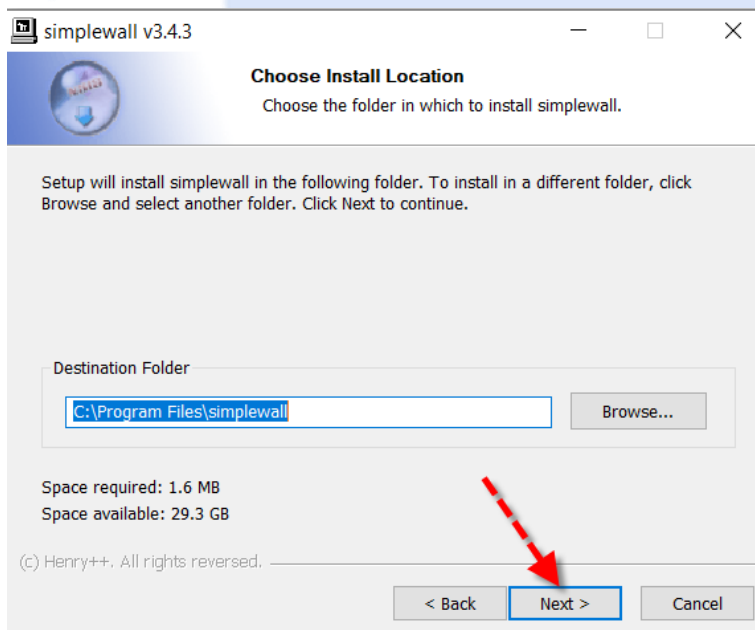
Una vez descargado el instalador lo ejecutamos y nos saldrá una pantalla de bienvenida como esta donde pulsaremos el botón Next:



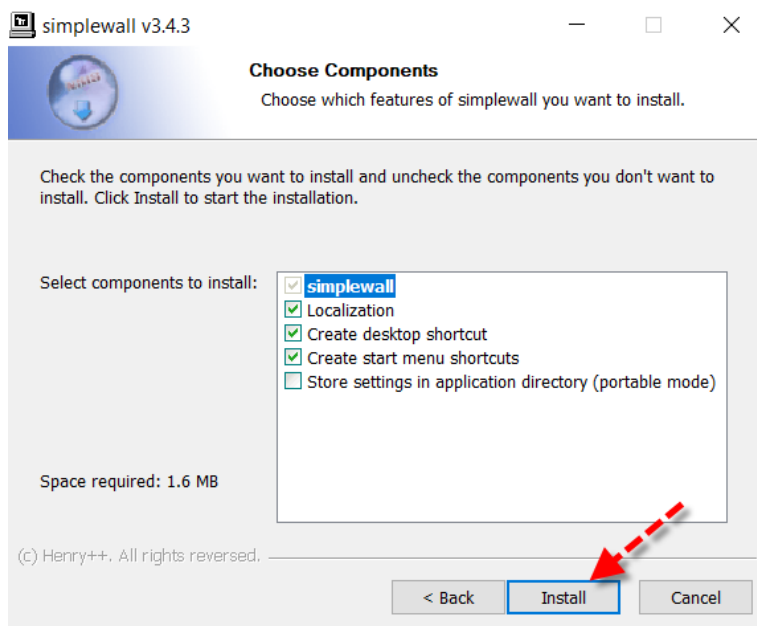
- Luego aceptamos el acuerdo de licencia activando la casilla correspondiente y pulsamos sobre el botón con la flecha roja.



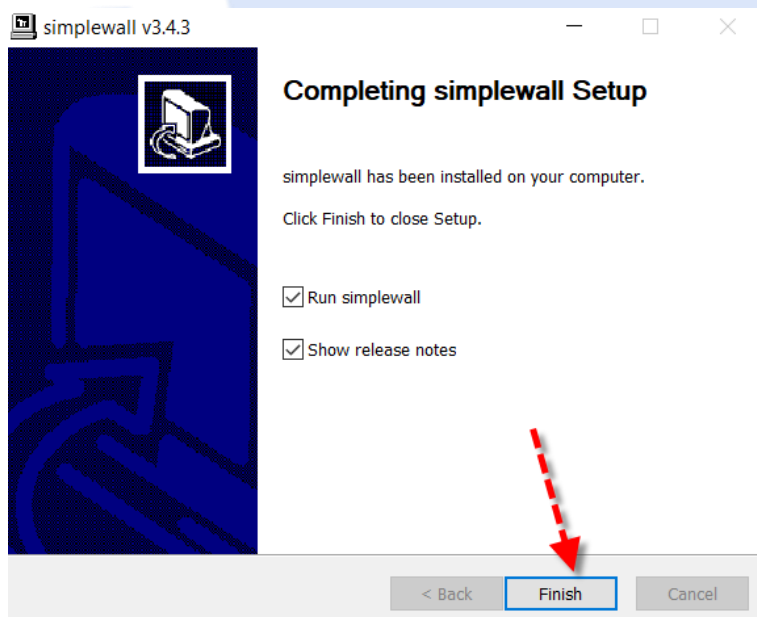
- A continuación, elegimos el directorio de instalación, salvo que haya un motivo especial dejaremos el que viene por defecto.



- 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.



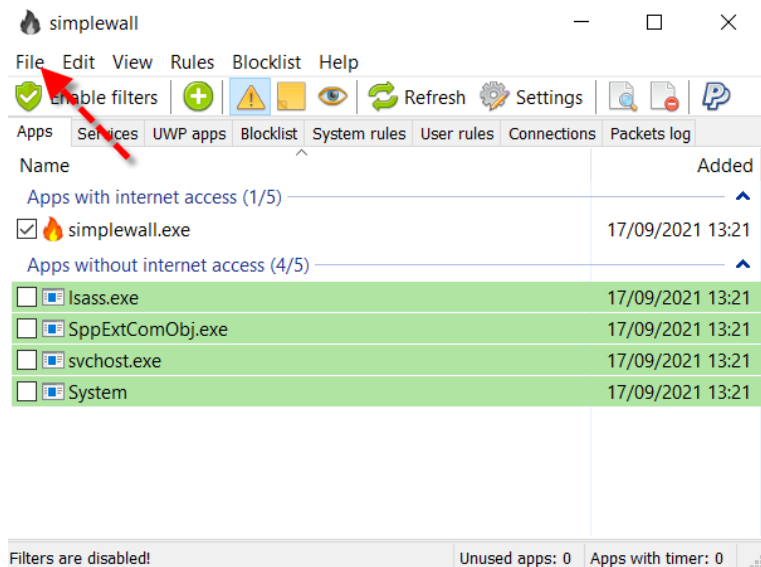
- En el momento que finalice la instalación con éxito de SimpleWall veremos una pantalla como esta.



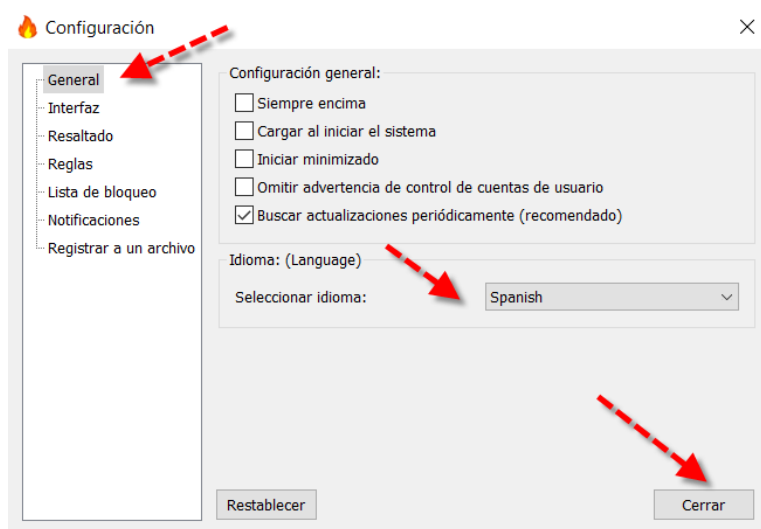
Si pulsamos como viene por defecto en el botón Finish para terminar la instalación se ejecutará por primera vez el programa.

Primeros pasos con SimpleWall para configurar el firewall

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

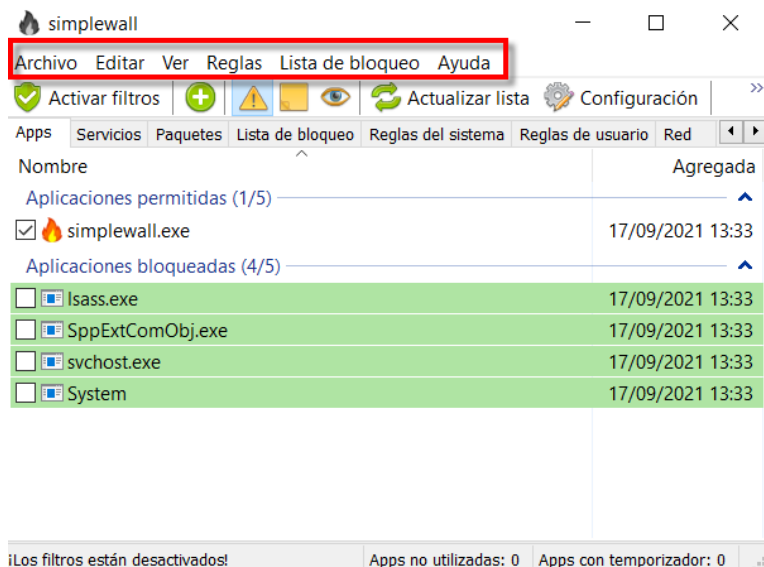


Como SimpleWall viene en inglés y se puede poner en español, aquí es por donde vamos a empezar. Para ello nos dirigimos a File y dentro seleccionamos Settings. En el apartado general en Language seleccionamos Spanish y le damos a cerrar. También una opción interesante que se usa mucho en «Configuración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

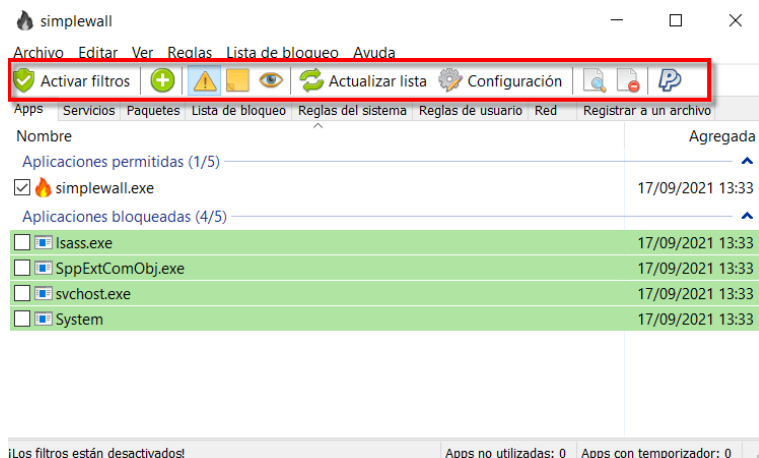




Aquí tenemos estas opciones:

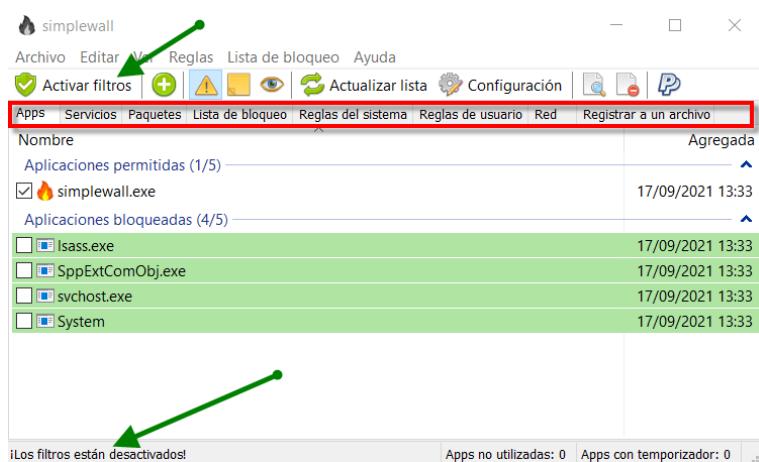
- Archivo: podemos acceder a la configuración de opciones y trabajar con archivos.
- Editar: para purgar apps no utilizadas, buscar y actualizar lista.
- Ver: sirve para elegir opciones de visualización y la fuente de letra.
- Reglas: para configurar como trabajan las reglas conviene dejarlo como viene 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.

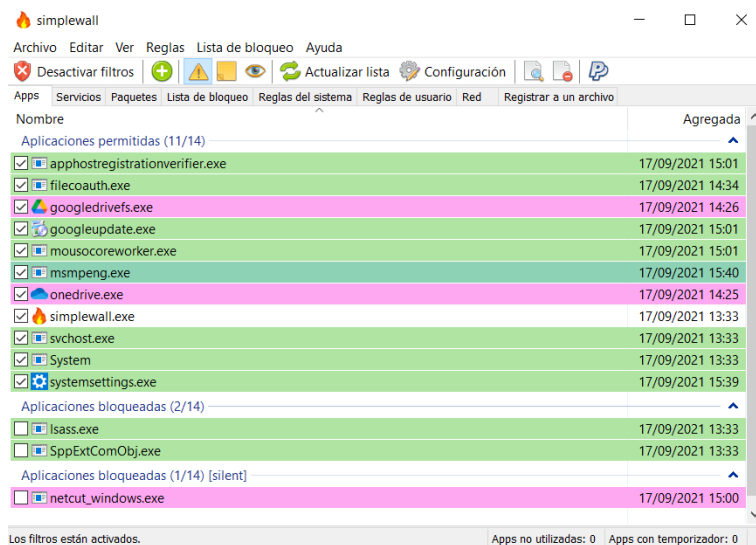


Según queremos trabajar con aplicaciones, servicios de Windows, lista de bloqueo y más, tendremos que seleccionar la pestaña adecuada. Por defecto, viene en el de Apps que se refiere a programas y que es con la que vamos a trabajar. Una cosa muy importante a tener en cuenta es que, en cualquiera de las 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.

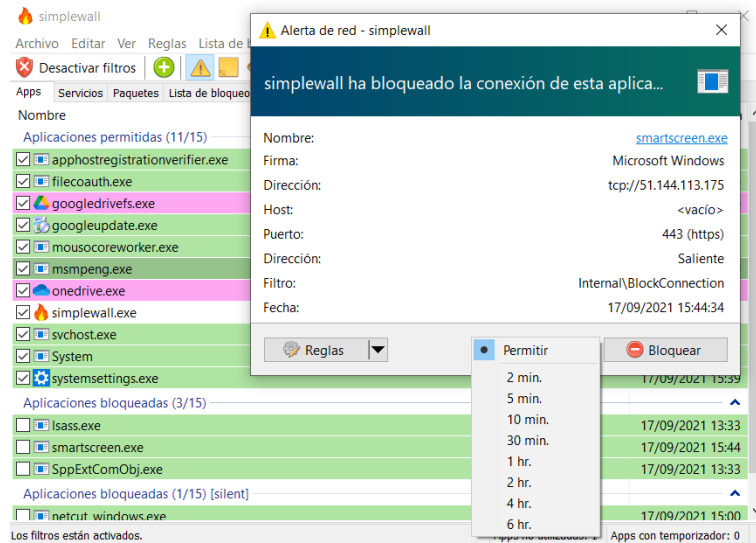
Seguidamente en ese momento SimpleWall ha bloqueado la conexión de la aplicación OneDrive de Microsoft. Como la que utilizo y me hace falta le he dado a Permitir para que me cree la regla. Justo después hemos hecho lo mismo con la de Google Drive.



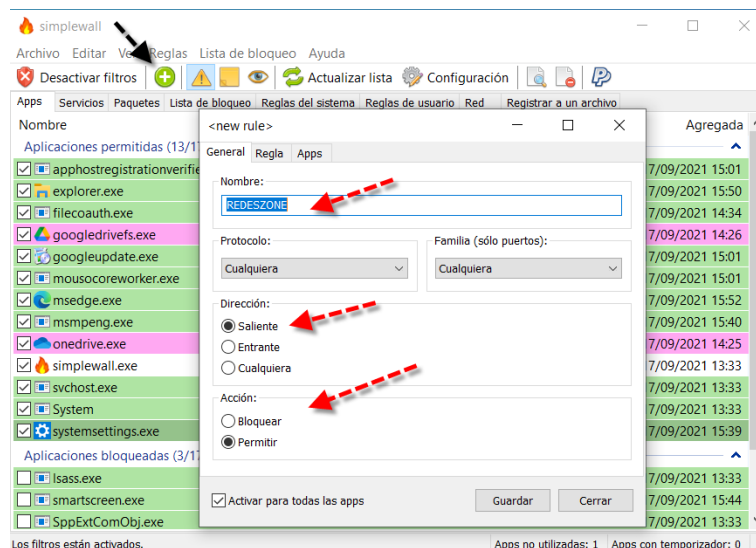
Luego tras varias peticiones que nos irá haciendo clasificará los programas en permitidos, bloqueados y bloqueados silenciosos. También activando la casilla de un programa pasará a permitidos.



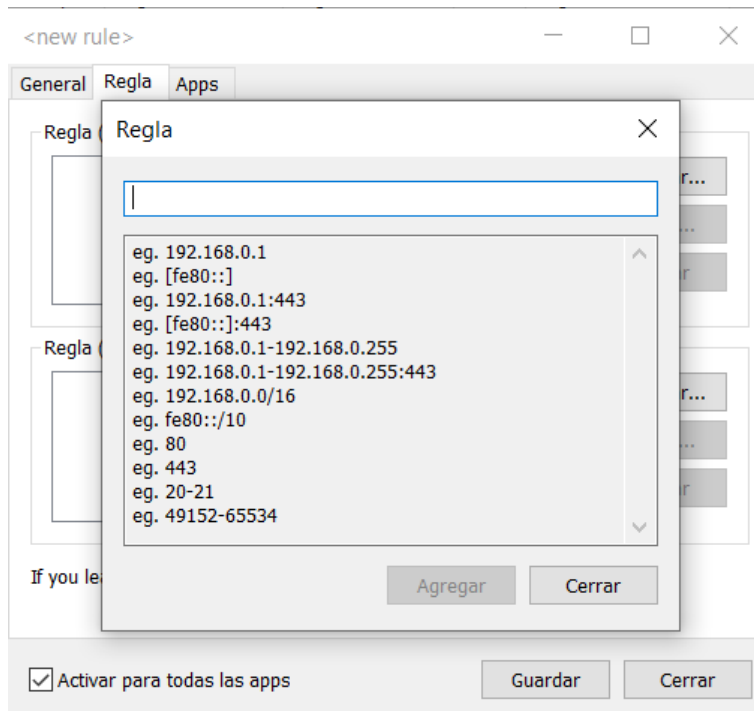
Además, a la hora de conceder acceso con nuestras reglas, el botón Permitir admite la creación de reglas temporales pulsando sobre el icono del triángulo negro invertido.



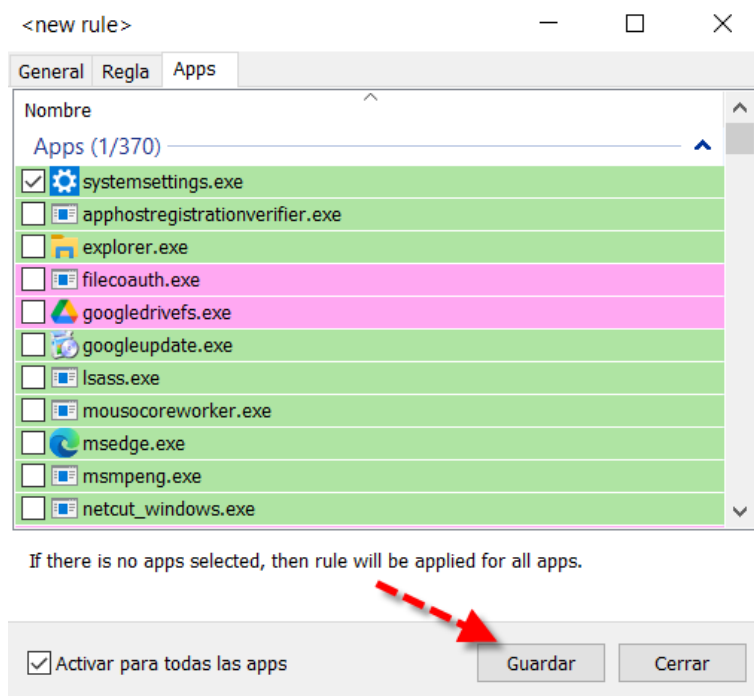
Por otra parte, si pulsamos sobre el botón con un + señalado con la flecha negra podremos crear nuestras reglas personales. En este caso para Apps, pero también podríamos hacerlas en otros apartados.



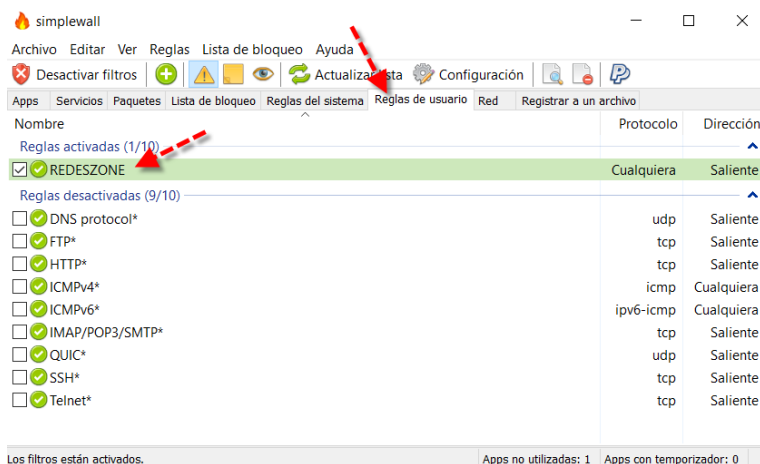
En General pones el nombre a la regla, luego el protocolo y la familia opcional. Entonces establecemos la dirección, ya sea entrante, saliente o cualquiera, y una acción que será permitir o bloquear. En la pestaña Regla podremos trabajar con IPs locales y remotas junto con su puerto si hace falta.



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](https://help.ovhcloud.com/csm/es-vps-firewall-windows?id=kb_article_view&sysparm_article=KB0056968)



INSTITUTO  
**KHIPU**