

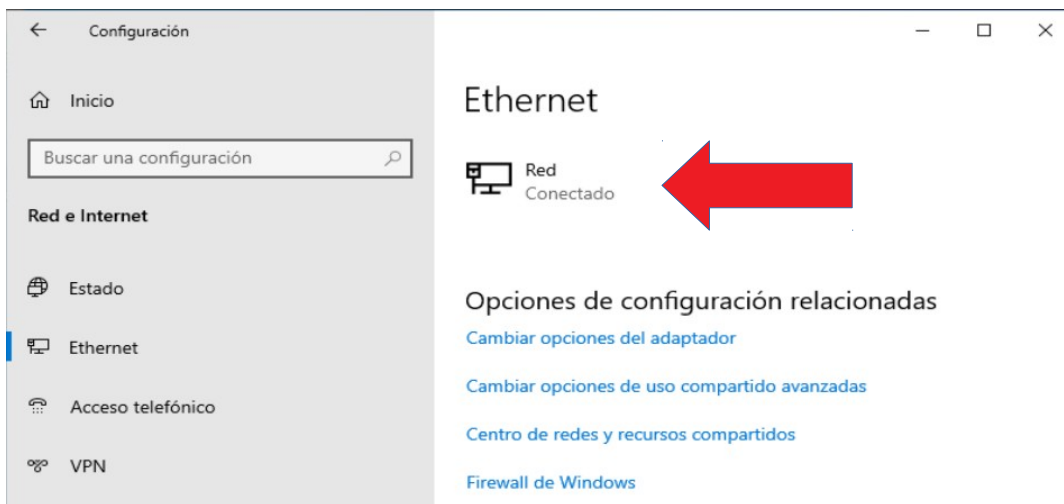
Seguridad en la red de Windows

Redes públicas y privadas:

Podemos establecer el nivel de seguridad de nuestra conexión a internet usando dos perfiles de seguridad diferentes: uno para redes de confianza, las privadas, y otro para redes no seguras como son las públicas.

Para cambiar nuestra conexión de un perfil a otro iremos a:

Ventana de Configuración → **Red e internet** → **Ethernet** y en la ventana que aparece hacemos clic sobre el icono que representa nuestra conexión de red

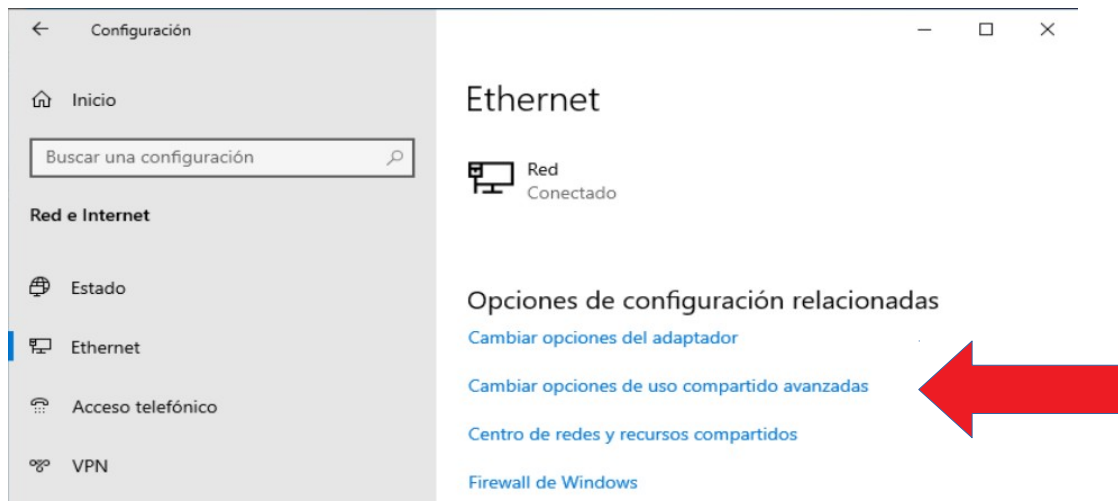


Y aparecerá la ventana que nos ofrece la posibilidad de cambiar entre ambos perfiles:

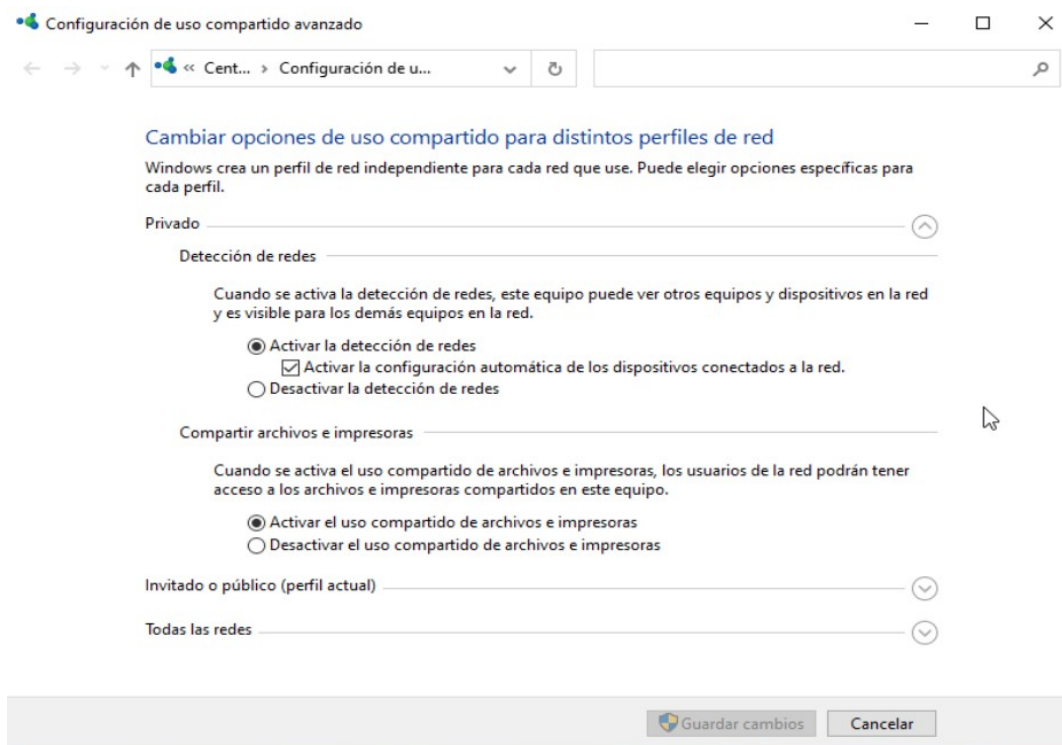


Uso compartido avanzado

Accediento a la ruta anterior **Ventana de Configuración** → **Red e internet** → **Ethernet** tenemos la posibilidad de pulsar sobre el enlace para cambiar las opciones de uso compartido avanzado

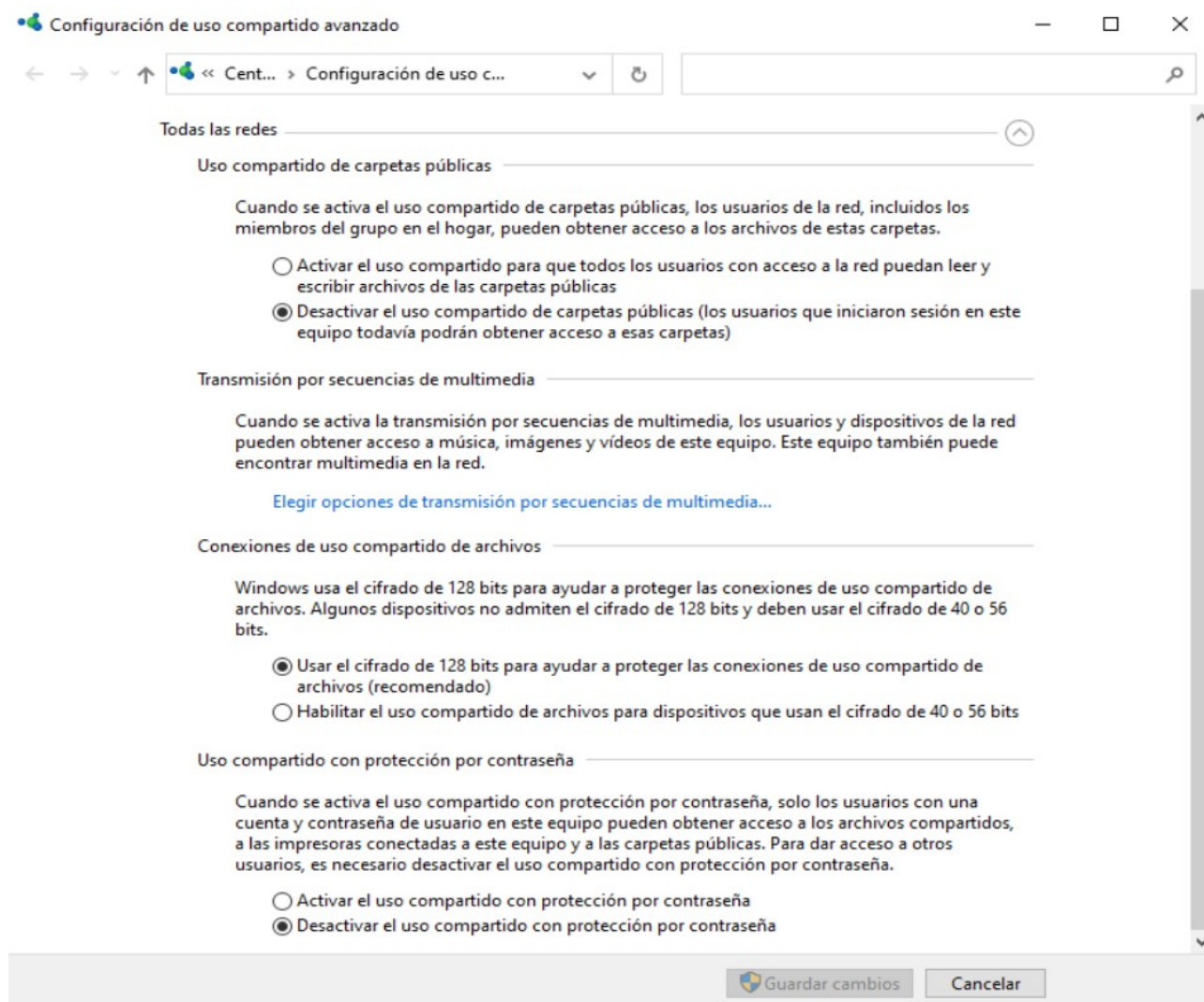


Ahí podremos configurar para el perfil privado o para el público, de forma independiente, la Detección de Redes y el uso compartido de archivos e impresoras.



La detección de redes hace visible nuestra máquina en la red de Windows y nos permite ver a otras máquinas que también la tengan activada.

Hay unas opciones comunes a ambos perfiles que aparecen en el tercer desplegable:



Se puede ver en la imagen la función que desempeña cada una de las opciones que se muestran en esta ventana.

El firewall de Windows

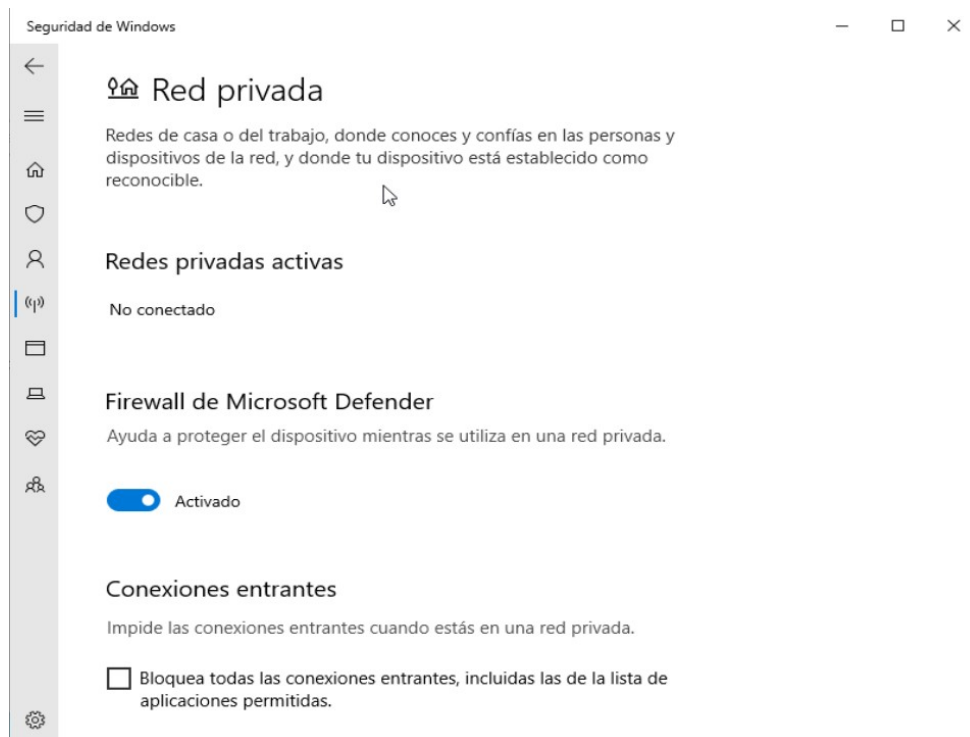
El firewall de windows nos va a permitir filtrar tráfico entrante o saliente siguiendo diversos criterios para seleccionar los paquetes que van a entrar o salir de nuestro sistema. Se puede acceder a la configuración básica siguiendo la ruta:

Ventana de Configuración → Red e internet → Ethernet → Firewall de Windows

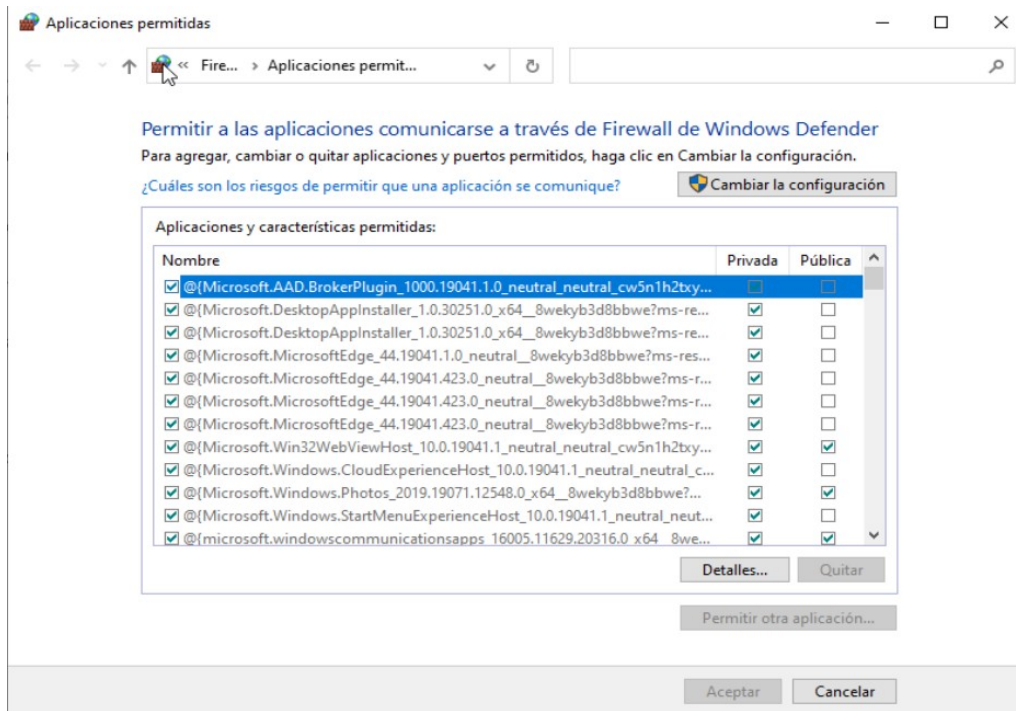
El firewall se va a poder activar o desactivar de forma independiente para las redes públicas o privadas como se muestra en la ventana de configuración:



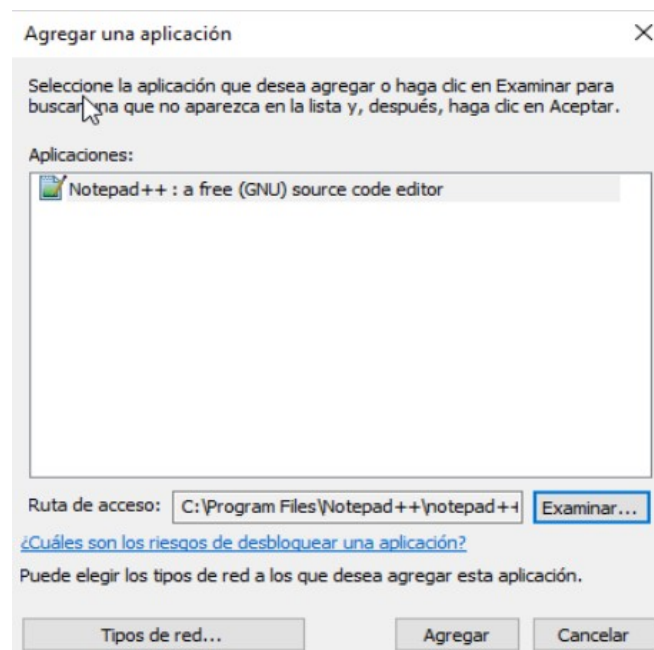
Si seleccionamos por ejemplo la configuración para la red privada podemos activar o desactivar el firewall y establecer un bloqueo total de conexiones entrantes para este perfil.



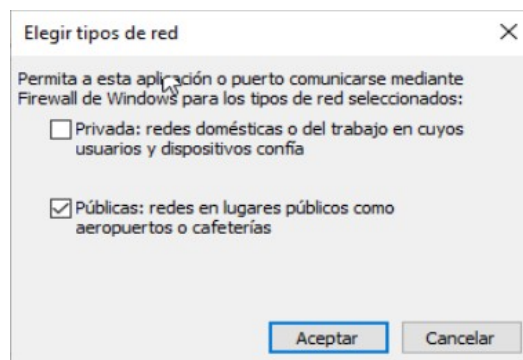
Volviendo a la ventana de configuración del firewall podemos autorizar a algún programa para que use la red (y atraviese el firewall sin problemas) usando el enlace de **Permitir una aplicación a través del firewall**



Pulsando el botón **Cambiar configuración** permitirá utilizar el botón **Permitir otra aplicación** y podremos seleccionar la aplicación que queremos autorizar:

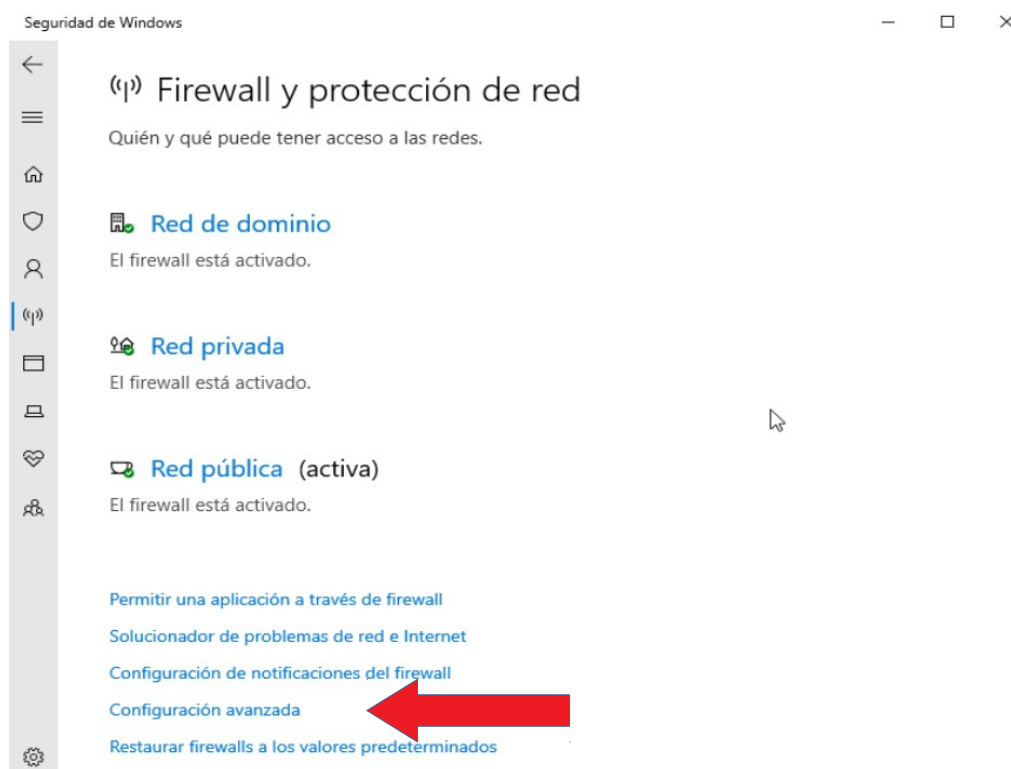


En esa última ventana, el botón Tipos de Red nos permite elegir a qué perfil vamos a asignar este cambio:

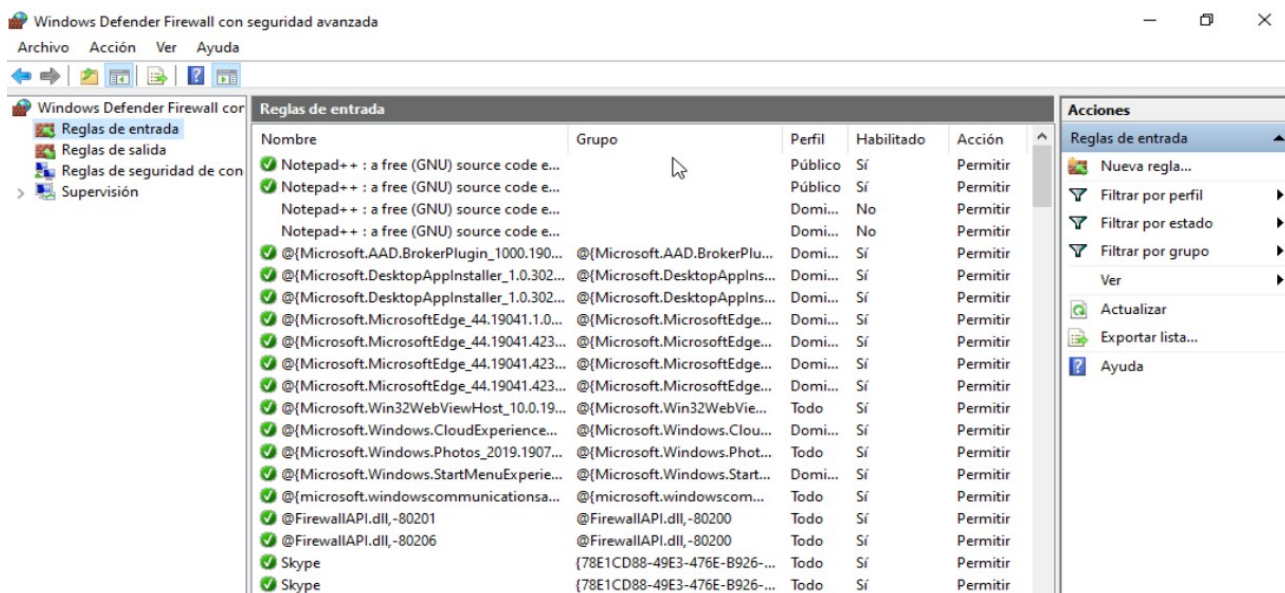


Configuración avanzada del Firewall de Windows

Desde la ventana de configuración del firewall podemos acceder a una ventana que nos permitirá crear reglas personalizadas para controlar el funcionamiento del firewall y activar o desactivar las existentes:



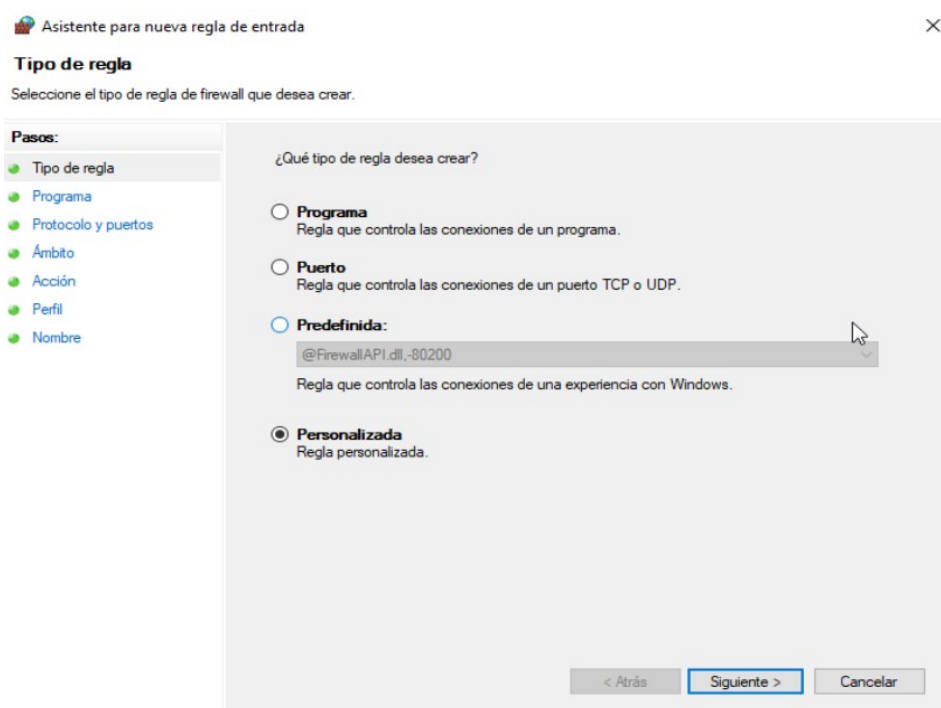
Al seleccionar esa opción veremos la herramienta de configuración avanzada del firewall. Con esta herramienta podemos crear reglas para el tráfico entrante o saliente o editar las que ya están creadas.



En el panel de la izquierda podemos seleccionar el tipo de reglas a visualizar, en la zona central vemos la lista de reglas correspondiente y en el panel de la derecha las operaciones disponibles para los elementos seleccionados.

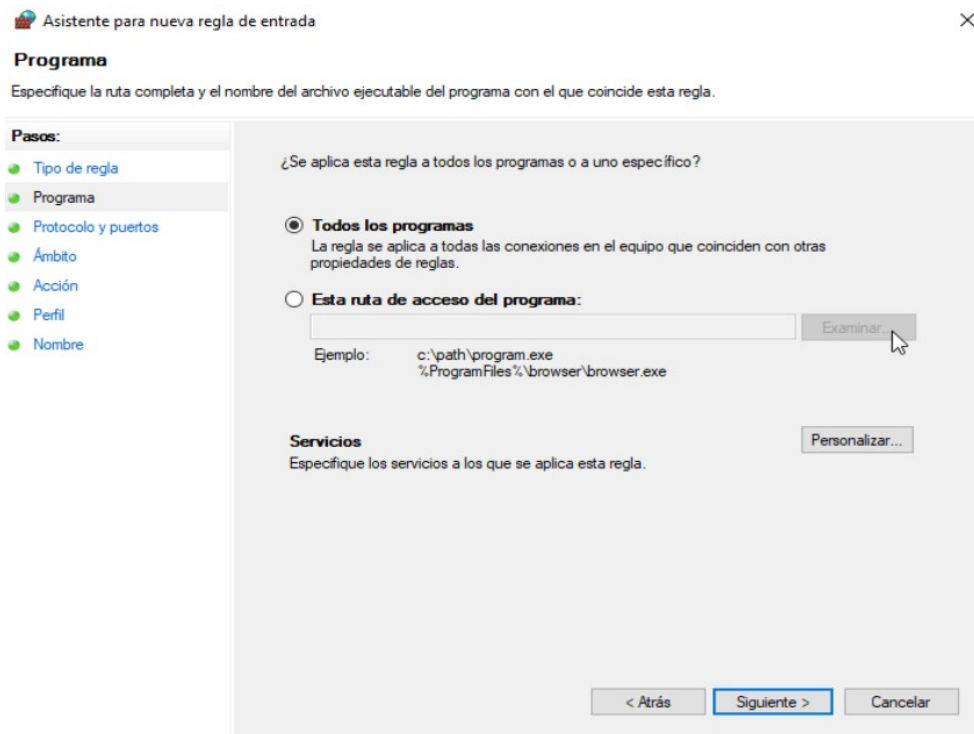
Crear una regla

Si seleccionamos la opción de crear una nueva regla (entrante si tenemos seleccionada esa opción en la zona de la izquierda) se mostrará la ventana del asistente de creación de regla en la que el primer paso es elegir el tipo:



Si queremos hacer una regla personalizada, por ejemplo, seleccionamos la opción correspondiente y pasamos al paso siguiente.

Podemos elegir que se aplique a un único programa o a todos sin excepción:



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
- Protocolo y puertos
- Ámbito
- 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:**

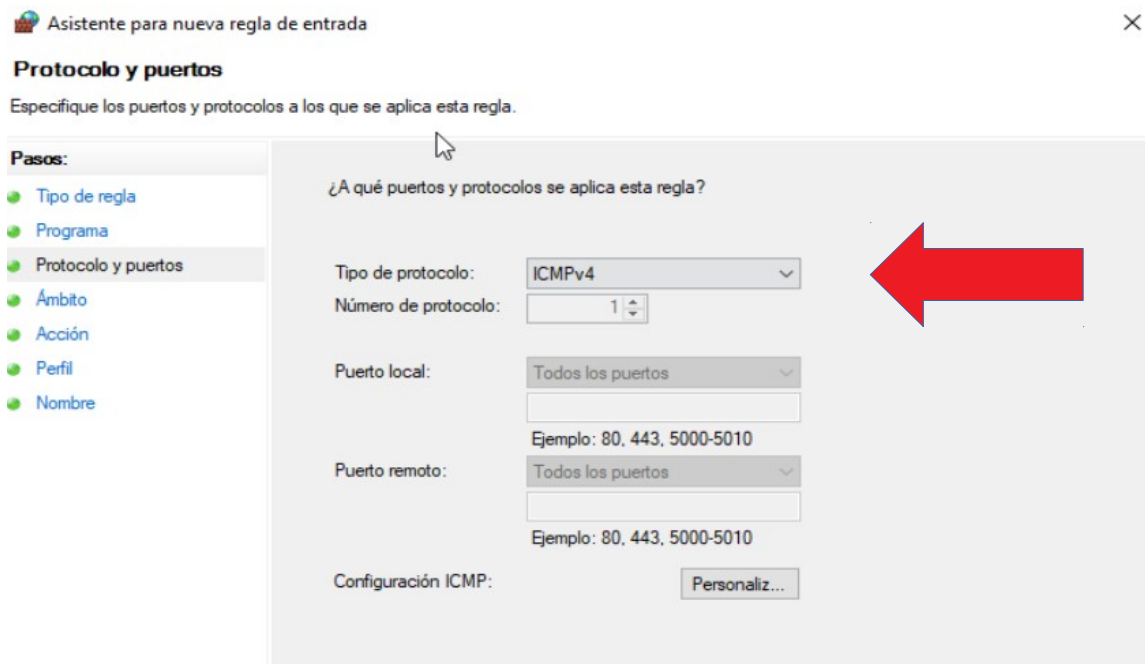
Ejemplo: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Examinar...

Personalizar...

< Atrás Siguiendo > Cancelar

Pasando al punto siguiente se elige el tipo de protocolo y los puertos que van a filtrarse. Si queremos bloquear el ping entrante podemos elegir el protocolo ICMP



Asistente para nueva regla de entrada

Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo: ICMPv4

Número de protocolo: 1

Puerto local: Todos los puertos

Ejemplo: 80, 443, 5000-5010

Puerto remoto: Todos los puertos

Ejemplo: 80, 443, 5000-5010

Configuración ICMP: Personalizar...

< Atrás Siguiendo > Cancelar

Continuando el asistente pasamos a la siguiente etapa en la que podemos seleccionar las Ips de origen y de destino a las que se aplicará esta regla:

Pasos:

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

¿A qué direcciones IP locales se aplica esta regla?

☒ Cualquier dirección IP

☐ Estas direcciones IP:

Agregar...
Editar...
Quitar

Personalizar los tipos de interfaz a los que se aplica esta regla: Personalizar...

¿A qué direcciones IP remotas se aplica esta regla?

☒ Cualquier dirección IP

☐ Estas direcciones IP:

Agregar...
Editar...
Quitar

Seguidamente se elige la acción a realizar: Bloquear o permitir

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
- Protocolo y puertos
- Ambito
- 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**

Seguidamente se elige el perfil de red en el que se aplicará la regla:

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.

Y finalmente se asigna un nombre y una descripción:

Asistente para nueva regla de entrada

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

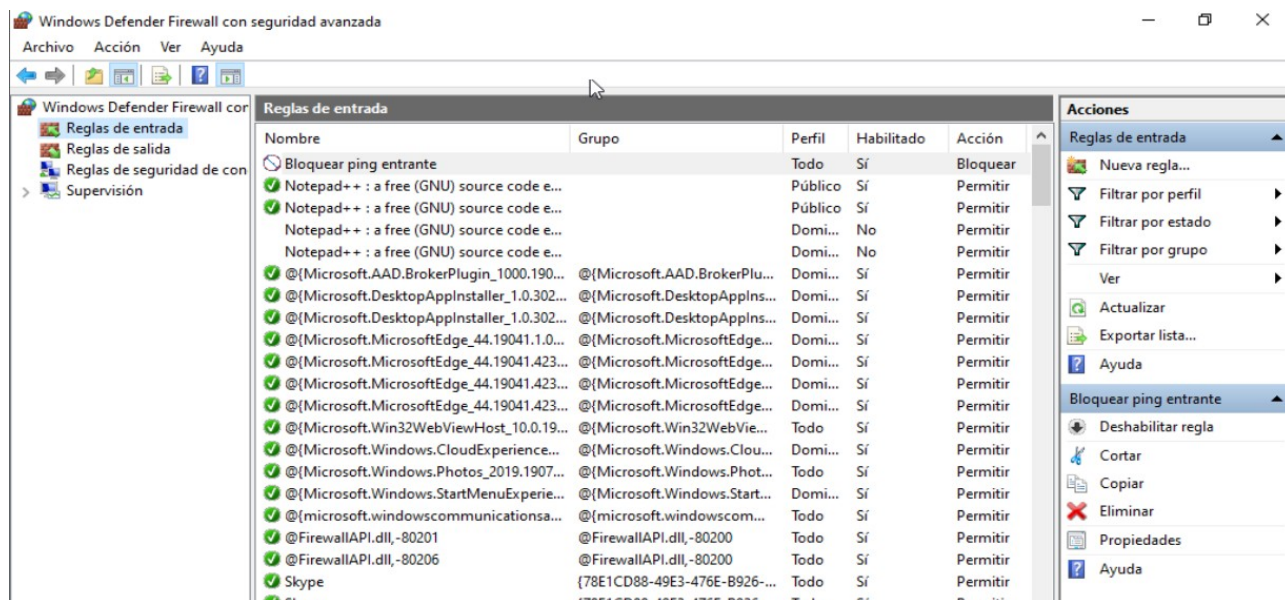
- Tipo de regla
- Programa
- Protocolo y puertos
- Ámbito
- Acción
- Perfil
- Nombre**

Nombre:
Bloquear ping entrante

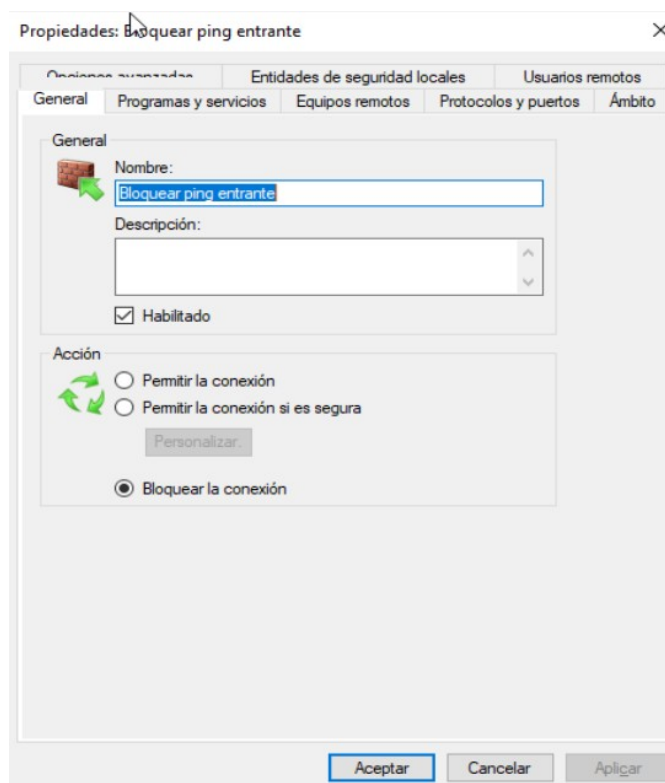
Descripción (opcional):

< Atrás Finalizar Cancelar

Operaciones sobre reglas:



Cuando se selecciona una regla se puede **Deshabilitar** para que no se aplique pero sin necesidad de eliminarla, **Cortar o Copiar** permite hacer una copia de la regla para pegarla más adelante, **Eliminar** la regla o ver sus **propiedades**:



En esta ventana se puede modificar la regla cambiando cualquiera de los parámetros definidos en el asistente de creación de una regla personalizada.