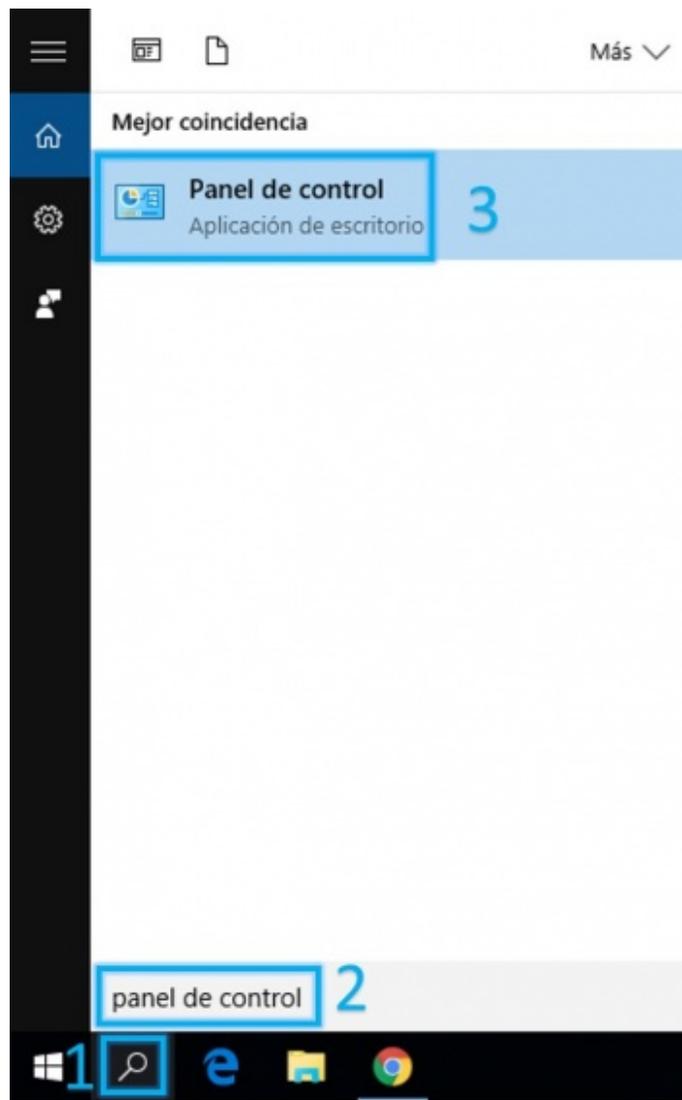

Firewall de Windows: Guía básica de uso

Un cortafuegos o firewall, no es más que un filtro que permite o deniega el tráfico de red dentro de un equipo. Forma parte importante de un sistema de comunicaciones y su administración es esencial para la seguridad y uso de aplicaciones en un sistema. En esta guía explicamos el uso y administración básica del firewall de Windows.

Acceder a la configuración del firewall de Windows

A continuación se muestran los pasos base para acceder a la interfaz de configuración del firewall de Windows y poder ejecutar otros procedimientos dentro de este tutorial:

- 1.** Haga clic en el botón de búsqueda de la barra de inicio y luego escriba "Panel de control". Seleccione el ícono del **Panel de control** una vez que aparezca en los resultados:



2. Luego seleccione **Sistema y Seguridad**:

Ajustar la configuración del equipo



Sistema y seguridad

Revisar el estado del equipo
Guardar copias de seguridad de los archivos con Historial de archivos
Copias de seguridad y restauración (Windows 7)
Buscar y corregir problemas



Redes e Internet

Ver el estado y las tareas de red
Elegir grupo en el hogar y opciones de uso compartido



Hardware y sonido

Ver dispositivos e impresoras
Agregar un dispositivo
Ajustar parámetros de configuración de movilidad de uso frecuente



Programas

Desinstalar un programa

3. Entre las opciones mostradas, seleccione Firewall de Windows:



Centro de actividades

Revisar el estado del equipo y resolver los problemas |
Cambiar configuración de Control de cuentas de usuario | Solucionar problemas habituales del equipo



Firewall de Windows

Comprobar estado del firewall | Permitir una aplicación a través de Firewall de Windows



Sistema

Ver la cantidad de memoria RAM y la velocidad del procesador | Permitir acceso remoto |
Iniciar asistencia remota | Mostrar el nombre de este equipo



Opciones de energía

Cambiar la configuración de batería | Requerir una contraseña cuando el equipo se reactiva |
Cambiar las acciones de los botones de inicio/apagado |
Cambiar la frecuencia con la que el equipo entra en estado de suspensión



Historial de archivos

Guardar copias de seguridad de los archivos con Historial de archivos |
Restaurar los archivos con Historial de archivos

Cómo desactivar y activar el firewall de Windows

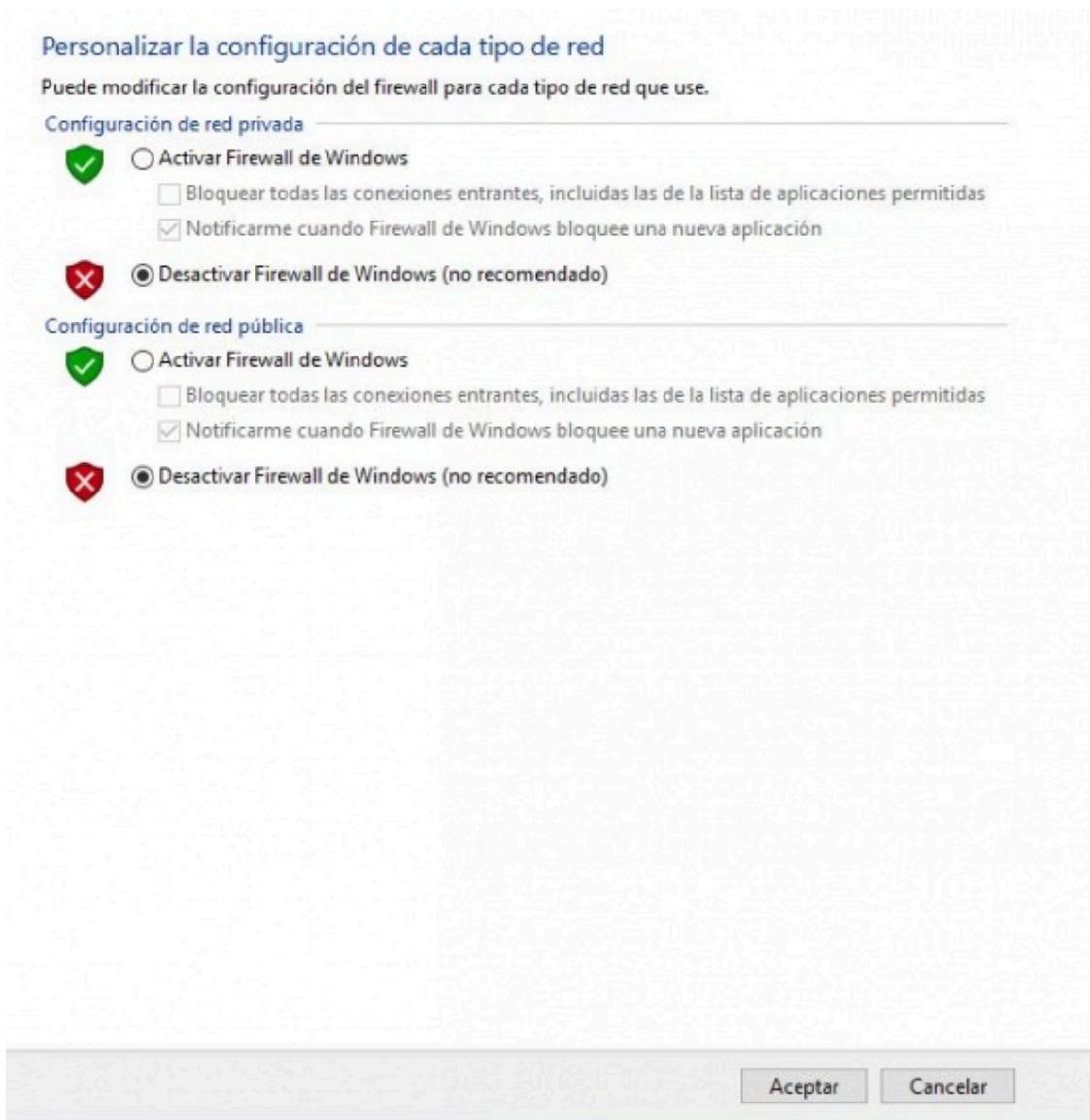
Muchas veces es necesario desactivar el firewall de Windows de manera temporal, para hacer pruebas en nuestros sitios o aplicaciones web, VPSs o plataformas. Recuerde que desactivar completamente el firewall de un equipo lo hace más vulnerable y propenso a riesgos de seguridad. Por lo tanto, recomendamos hacerlo temporalmente solo si es estrictamente necesario.

Para activar o desactivar el firewall en Windows 10 siga el procedimiento descrito a continuación:

1. Siga los pasos en Acceder a la configuración del firewall de Windows.
2. Desde el panel de opciones a la izquierda, seleccione **Activar o Desactivar Firewall de Windows** (debe ser el usuario administrador del equipo).



3. Generalmente, querrá activar o desactivar el firewall tanto en la red pública como en la red privada. Sin embargo, tendrá la opción de configurarlo individualmente, desde esta pantalla podrá activar o desactivar el Firewall según sea necesario. También puede mantener activo el firewall y bloquear todas las conexiones entrantes. Una vez que marque las casillas deseadas, haga clic en **Aceptar**. En este ejemplo se muestran las opciones necesarias para desactivar el firewall completamente (admitir las conexiones entrantes y salientes en todos los puertos):



Recuerde volver a activar el firewall para mantener la seguridad de su equipo. Las instrucciones para versiones de Windows recientes (como Windows 7 u 8) son muy similares pero no se abordan en este tutorial.

Cómo administrar las reglas de entrada y salida para abrir puertos específicos

El flujo de datos en una red suele estar regido por el protocolo de control de transmisión TCP (*Transmission Control Protocol*, por sus siglas en inglés) y el protocolo de datagrama de usuario UDP (*User Datagram Protocol*), ambos en la capa de Transporte. Cada uno de estos asigna puertos específicos para cada aplicación. Por ejemplo: los protocolos 20 y 21 para FTP, o el bien conocido *puerto 80* que permite escuchar peticiones HTTP, o en la práctica, establecer una conexión con un servidor web.

Cuando se instala una aplicación en Windows, se configuran automáticamente las reglas de entrada y salida en el firewall, sin embargo, en algunas ocasiones deberá establecer estas reglas manualmente:

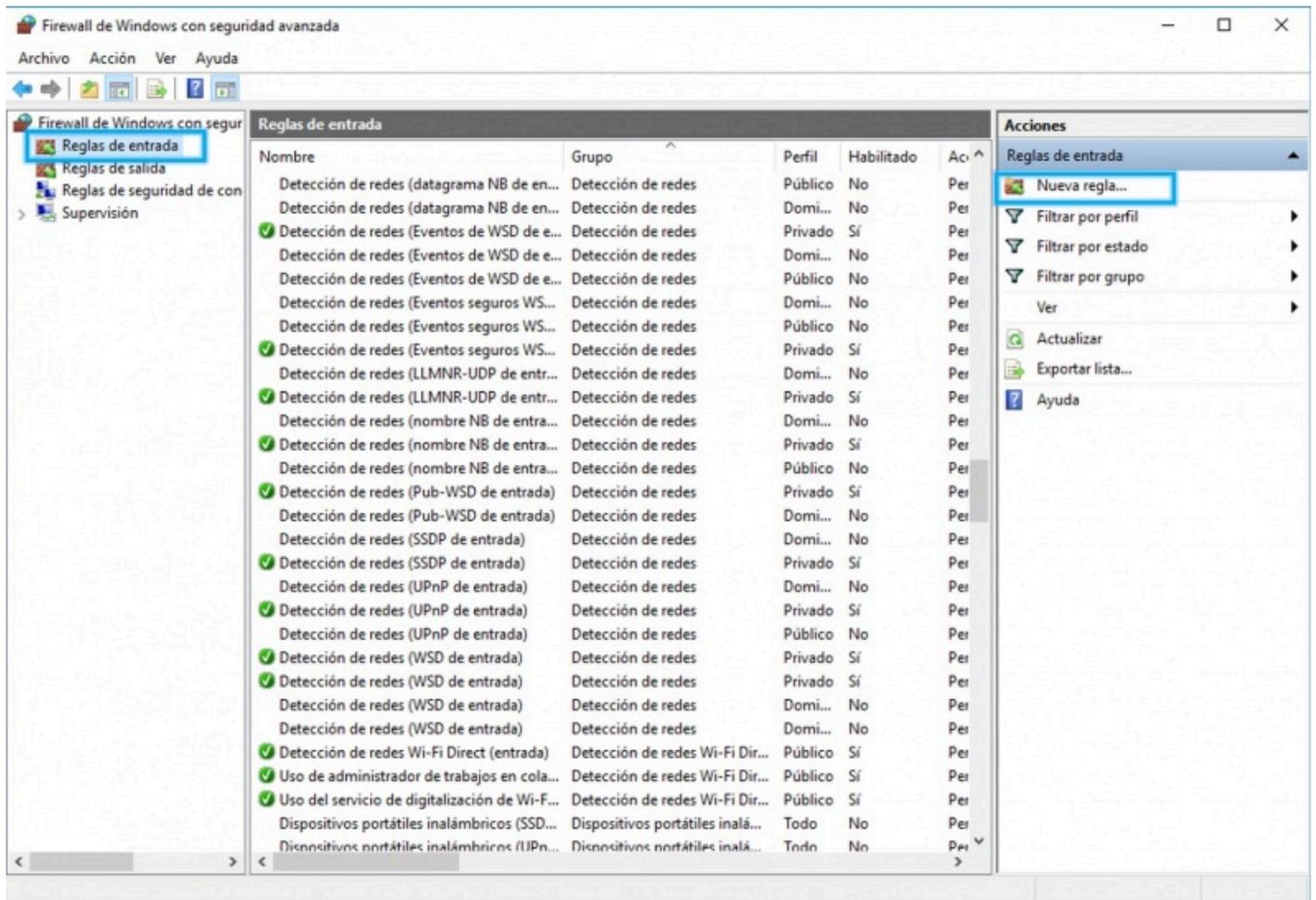
1. Siga los pasos en Acceder a la configuración del firewall de Windows.

2. En el panel izquierdo, seleccione **Configuración Avanzada**:



3. Se abrirá la ventana de configuración avanzada del firewall de Windows. Desde allí podrá editar, agregar o eliminar nuevas reglas de entrada y salida. En este tutorial haremos un ejemplo para permitir las conexiones de entrada en el puerto 80 TCP de nuestro computador. El procedimiento para abrir otros puertos es básicamente el mismo, simplemente debe cambiar si la regla es de entrada/salida y el número de puerto o protocolo (TCP o UDP).

4. Para agregar la nueva regla de entrada haga clic en **Reglas de entrada** en el panel de opciones a la izquierda, y luego haga clic en **Nueva regla** desde la pestaña de opciones a la derecha:



5. En la siguiente ventana, seleccione el tipo de regla "Puerto" para agregar conexiones TCP/UDP. Luego haga clic en **Siguiente**.

Asistente para nueva regla de entrada

Tipo de regla

Seleccione el tipo de regla de firewall que desea crear.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Qué tipo de regla desea crear?

Programa
Regla que controla las conexiones de un programa.

Puerto
Regla que controla las conexiones de un puerto TCP o UDP.

Predefinida:
Administración de tarjetas inteligentes virtuales TPM
Regla que controla las conexiones de una experiencia con Windows.

Personalizada
Regla personalizada.

< Atrás **Siguiente >** Cancelar

6. Marque la casilla según el protocolo que corresponda (TCP o UDP), y escriba el número de puerto en el cuadro de texto. En nuestro caso seleccionamos **TCP** y escribimos el número de puerto **80**:

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

Al terminar haga clic en **Siguiente**.

7. Asegúrese de que esté seleccionada la opción **Permitir la conexión** y haga clic en **Siguiente**:

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.

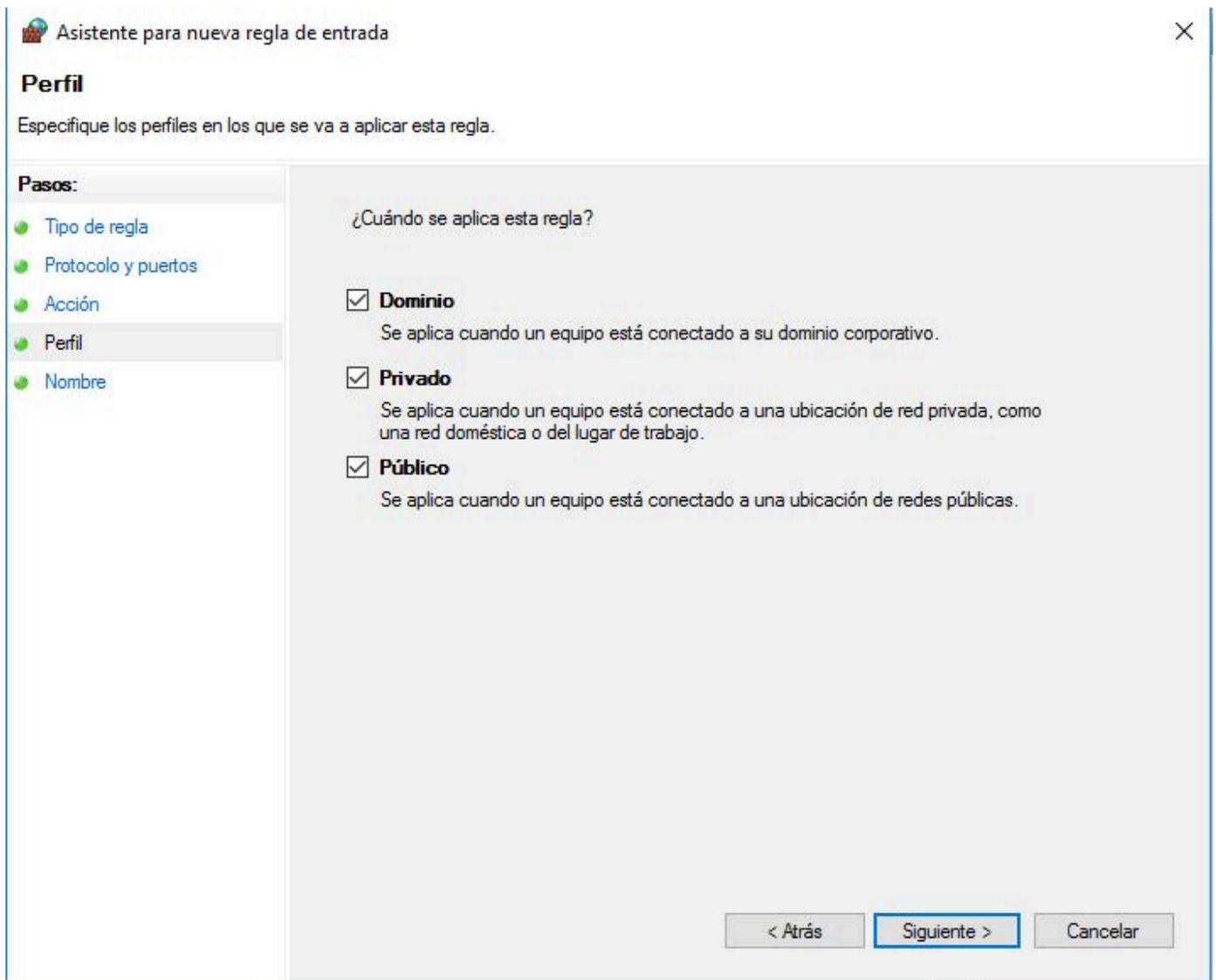
Permitir la conexión si es segura
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

Bloquear la conexión

< Atrás **Siguiente >** Cancelar

8. Generalmente, querrá mantener las opciones en la siguiente pantalla:



O haga los cambios que considere necesarios y continúe seleccionando **Siguiete**.

9. Agregue un nombre y descripción adecuados y haga clic en **Finalizar**.

Asistente para nueva regla de entrada

Nombre

Especifique el nombre y la descripción de esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

Nombre:
Conexiones entrantes puerto 80

Descripción (opcional):
Pruebas

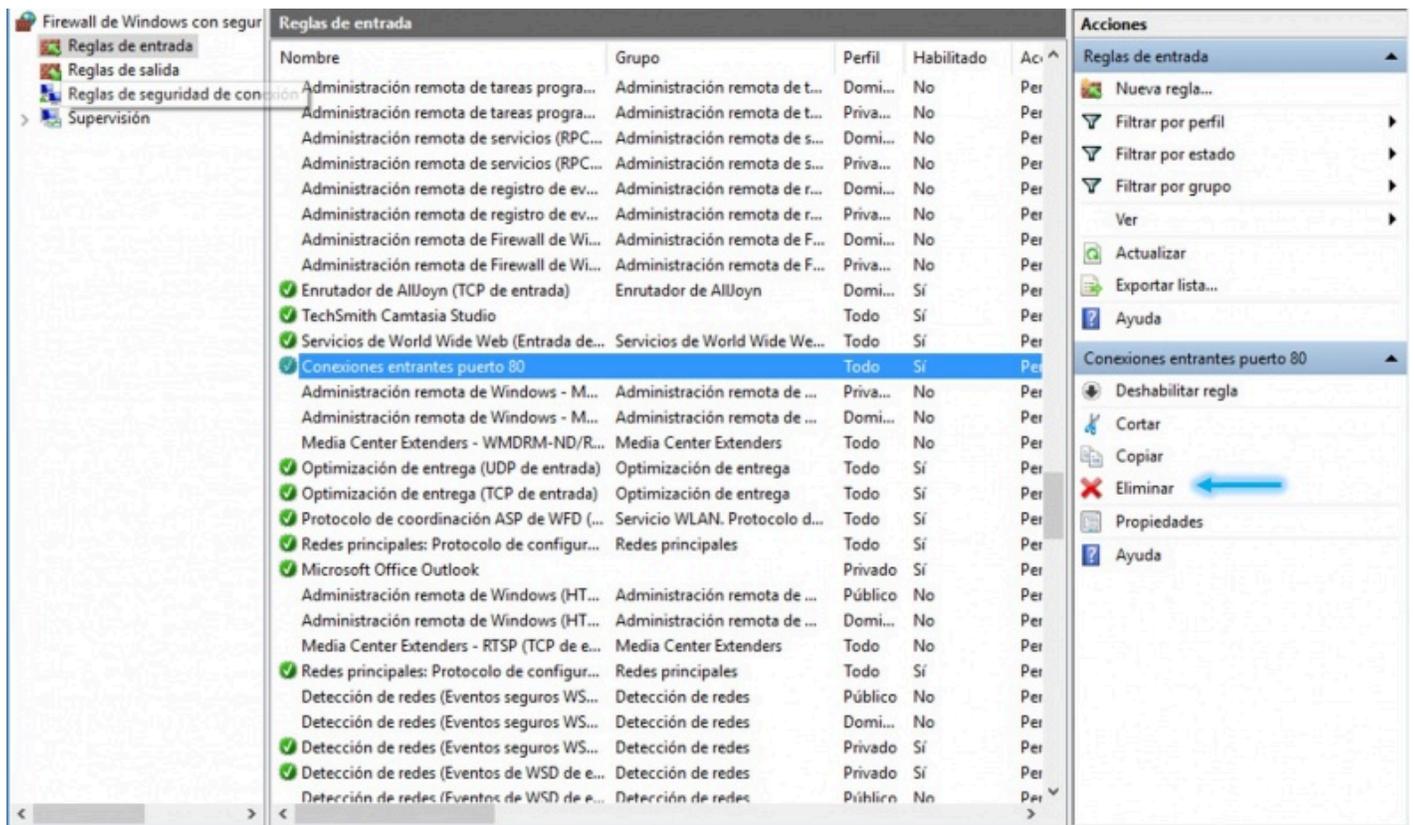
< Atrás Finalizar Cancelar

Para eliminar una regla siga el procedimiento:

1. Siga los pasos en Acceder a la configuración del firewall de Windows.
2. En el panel izquierdo, seleccione **Configuración Avanzada**.
3. Seleccione "Reglas de entrada" o "Reglas de salida" según corresponda. Observará una lista de las reglas disponibles. Puede usar los filtros a la derecha bajo **Acciones**, pero la opción más sencilla para encontrar la regla asociada a un puerto en particular es ordenar las reglas por puerto:

Programa	Dirección local	Dirección remota	Protocolo	Puerto local	Puerto remoto
%SystemR...	Cualquiera	Cualquiera	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Subred local	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Cualquiera	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Subred local	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Cualquiera	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Subred local	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Cualquiera	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Subred local	TCP	Asignador d...	Cualquiera
%SystemR...	Cualquiera	Cualquiera	TCP	9955	Cualquiera
Cualquiera	Cualquiera	Cualquiera	TCP	8317	Cualquiera
System	Cualquiera	Cualquiera	TCP	80	Cualquiera
Cualquiera	Cualquiera	Cualquiera	TCP	80	Cualquiera
System	Cualquiera	Subred local	TCP	80	Cualquiera
System	Cualquiera	Cualquiera	TCP	80	Cualquiera
%SystemR...	Cualquiera	Subred local	UDP	7777, 7778, 7...	Cualquiera
%SystemR...	Cualquiera	Cualquiera	UDP	7680	Cualquiera
%SystemR...	Cualquiera	Cualquiera	TCP	7680	Cualquiera
%systemr...	Cualquiera	Subred local	UDP	7235	7235
%SystemR...	Cualquiera	Cualquiera	UDP	68	67
C:\Progra...	Cualquiera	Cualquiera	UDP	6004	Cualquiera
System	Cualquiera	Subred local	TCP	5985	Cualquiera
System	Cualquiera	Cualquiera	TCP	5985	Cualquiera
%SystemR...	Cualquiera	Subred local	TCP	554, 8554, 85...	Cualquiera
%SystemR...	Cualquiera	Cualquiera	UDP	546	547
System	Cualquiera	Subred local	TCP	5358	Cualquiera
System	Cualquiera	Cualquiera	TCP	5358	Cualquiera
System	Cualquiera	Subred local	TCP	5358	Cualquiera
System	Cualquiera	Subred local	TCP	5357	Cualquiera
Svstem	Cualquiera	Subred local	TCP	5357	Cualquiera

4. Una vez encontrado el puerto, puede ver otras características de la regla en la misma lista o haciendo doble clic sobre la regla. Digamos que queremos eliminar la regla recién agregada. Haga clic sobre la regla y luego seleccione **Eliminar** desde el menú de acciones a la derecha:

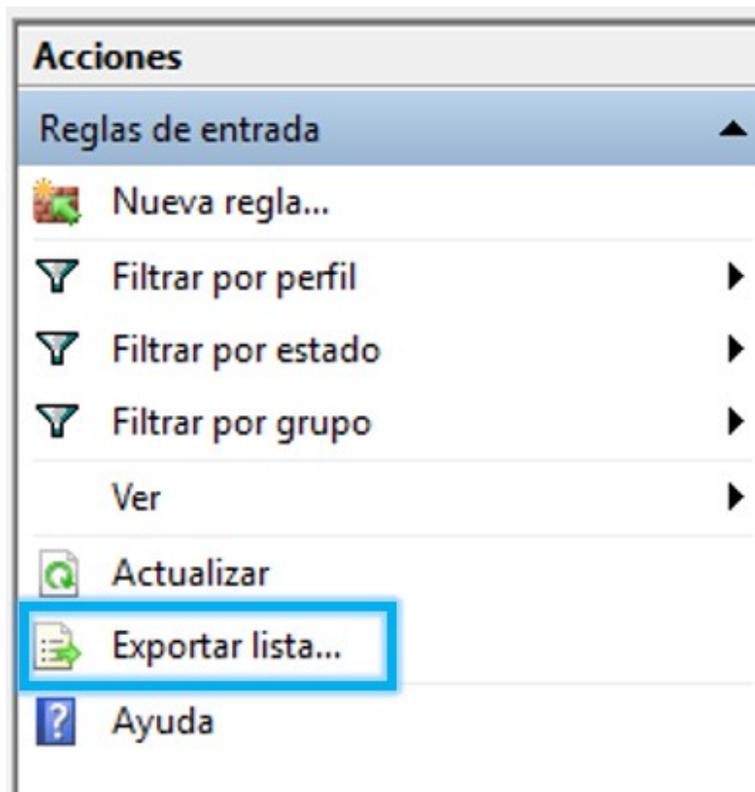


Confirme su decisión haciendo clic en **Sí** en el cuadro de diálogo emergente.

Otras opciones

Respaldar sus reglas de Firewall

Una recomendación antes de realizar cambios en sus reglas de conexiones entrantes y salientes es hacer un respaldo de sus reglas de firewall. También puede usar este respaldo si desea importarlo a otro equipo que requiera las mismas características. Utilice la opción **Exportar lista** tanto en las conexiones salientes como en las entrantes para mantener un respaldo de la configuración de su firewall antes de hacer cualquier cambio (podrá importar esta lista más tarde si ocurre algún error).



Restablecer la configuración predeterminada

1. Siga los pasos en [Acceder a la configuración del firewall de Windows](#).
2. Haga clic en **Restaurar valores predeterminados** desde el panel izquierdo.
3. Confirme en la siguiente pantalla haciendo clic en **Restaurar valores predeterminados**:

Restaurar configuración predeterminada

Si restauras la configuración predeterminada, se quitarán todas las opciones de configuración de Firewall de Windows que hayas configurado para todas las ubicaciones de red. Esto puede hacer que algunas aplicaciones dejen de funcionar.

Restaurar valores predeterminados

En esta guía se presentan algunas de las opciones básicas para administrar el firewall en Windows, otras opciones avanzadas se escapan del alcance de este material. Las instrucciones y capturas son hechas en un entorno Windows 10, aunque puede seguir los pasos para otras versiones recientes de Windows como Windows 7 y 8 - las instrucciones variarán solo en pequeños detalles.

Recursos adicionales

Puede consultar los siguientes recursos en busca de información adicional con respecto a este tema. Aunque este material es provisto esperando que sea útil, tome en cuenta que no podemos dar fe de la actualidad o precisión de los contenidos externos.