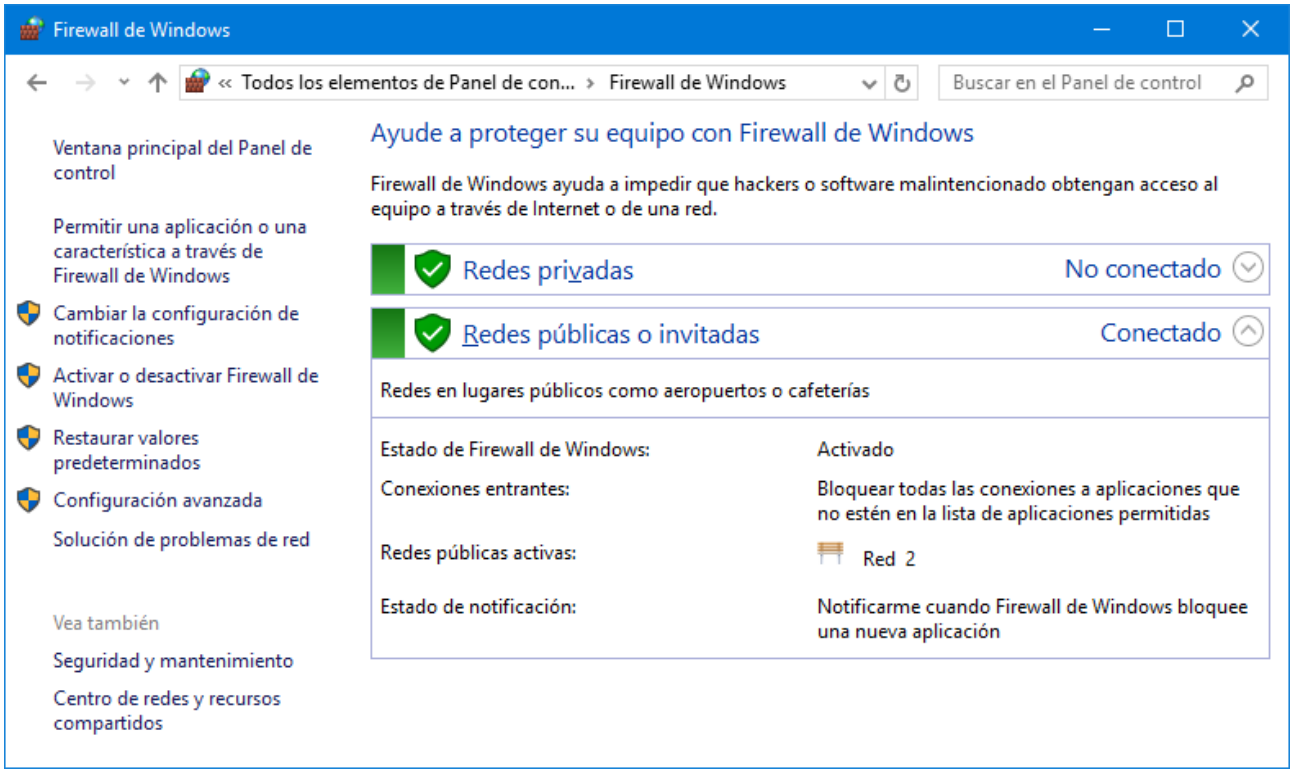
Configuración de un Cortafuegos
Práctica 10A

1. Objetivo

En esta práctica el alumno debe aprender a configurar un cortafuegos, o firewall en inglés, con el objeto de proteger adecuadamente un computador. Para ello se utilizará el firewall de Windows 10 en una **máquina virtual** a la que se pueda acceder como Administrador.

2. Acceso al Firewall

Acceder al Panel de Control > Firewall de Windows. Aparece la ventana siguiente:



Esta ventana permite realizar una configuración SIMPLIFICADA del firewall.

Antes de empezar a trabajar con el firewall hay que estudiar que son las "ubicaciones de red". Cuando un computador se conecta por primera vez a una red debe elegirse una ubicación de red. En función de la ubicación elegida se define automáticamente la configuración apropiada de firewall y seguridad.

Hay cuatro ubicaciones de red:

Red doméstica: se usa cuando se conoce y se confía en los usuarios y equipos de la red. La "detección de redes" está activada en la ubicación redes domésticas, permitiendo que cada equipo de la red vea a todos los demás.

Red de trabajo: se usa en pequeñas oficinas o en subredes de un lugar de trabajo. La detección de redes esta activada de forma predeterminada.

Red pública: se usa para las redes de lugares públicos, como cafeterías o aeropuertos. Con esta ubicación la detección de redes está desactivada, lo que oculta el equipo a los otros equipos que están usando la red.

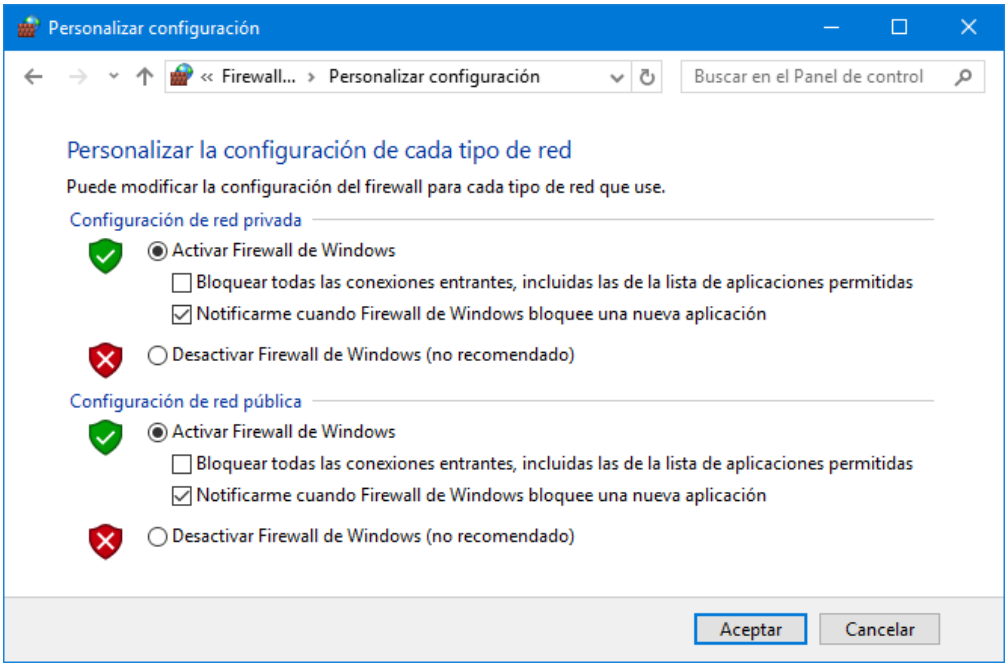
Dominio de red: se usa en redes de dominio, en las que un equipo actúa como controlador de la red.

Para la configuración del firewall, las redes domésticas y de trabajo se tratan del mismo modo y se denominan redes privadas. En esta práctica consideramos que el computador está conectado a una red pública.

En el panel izquierdo de la figura previa se pueden ver dos opciones:

- Cambiar la configuración de notificaciones
- Activar o desactivar Firewall de Windows

Ambas nos llevan a la misma pantalla siguiente:

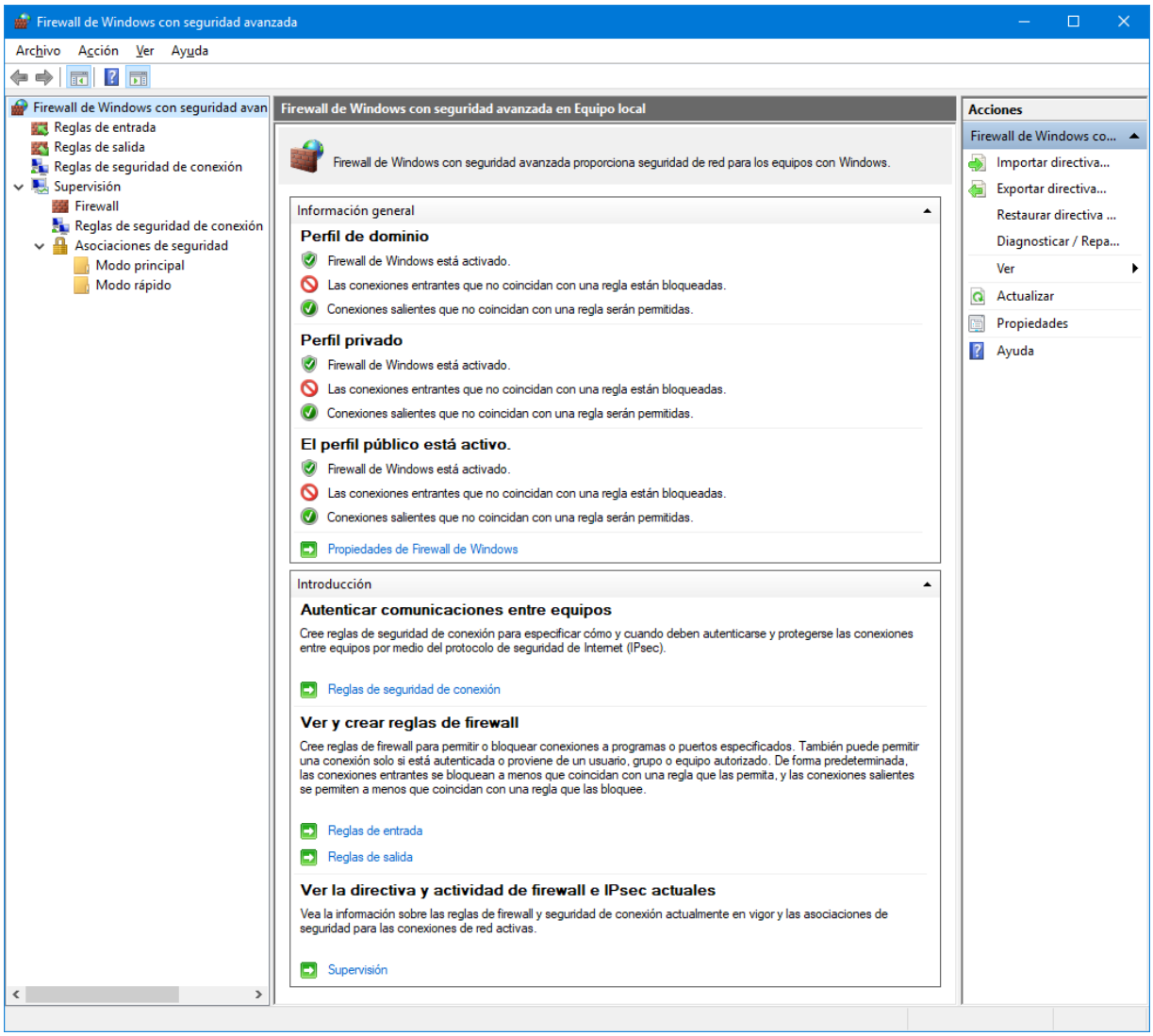


Las opciones de configuración disponibles son obvias. Observar que se configuran independientemente para cada tipo de red a la que está conectado el computador. Por ejemplo el firewall puede estar activado al conectarse a una red pública, pero estar desactivado al conectarse a una red privada.

3. Configuración avanzada

Para acceder a la configuración avanzada, seleccionar la opción "Configuración avanzada" que aparece en el panel izquierdo de la ventana "Firewall de Windows". Es la penúltima opción del panel y la última que tiene un escudo a su izquierda.

También se puede acceder directamente a la configuración avanzada pulsando la techa Windows+r y en el cuadro Ejecutar teclear **wf.msc** y pulsar Intro.



Para abrir la consola del Firewall de Windows con seguridad avanzada el usuario debe pertenecer al grupo de Administradores o al grupo de Operadores de red.

El Firewall inspecciona y filtra todos los paquetes IPv4 e IPv6 que intercambia el computador con la red. Filtrar significa permitir o bloquear el tráfico de paquetes basándose en reglas.

De forma predeterminada, el firewall bloquea el tráfico entrante, a menos que sea una respuesta a una solicitud del propio computador (tráfico solicitado) o esté permitido específicamente, es decir, que se haya creado una **regla de firewall** para permitir el tráfico.

El firewall también puede requerir, usando **reglas de seguridad de conexión**, que los equipos se autentiquen entre sí antes de establecer una comunicación y que cifren los datos que intercambian.

Reglas de Firewall

Las reglas de firewall permiten enviar o recibir tráfico a:

- programas
- servicios del sistema
- equipos
- usuarios
- puertos y protocolos

A cada conexión que coincida con los criterios de una regla se le aplica una acción:

- Permitir la conexión
- Permitir una conexión solo si está protegida con IPsec
- Bloquear la conexión

Se puede especificar el tipo de adaptador de red al que se aplicará la regla: red de área local (LAN), inalámbrica, acceso remoto, como una conexión de red privada virtual (VPN), o bien todos los tipos.

Reglas de seguridad de conexión

Definen como se deben autenticar dos equipos antes de que inicien las comunicaciones y como deben proteger (cifrar) la información que intercambian. Para ello utilizan el protocolo IPsec.

Las reglas de seguridad de conexión requieren que **los dos equipos** que se comunican dispongan de una directiva con reglas de seguridad de conexión (u otra directiva IPsec) que sea compatible con la del otro equipo. Por el contrario, las reglas de firewall actúan de forma unilateral, solamente en un equipo.

Es probable que se tenga que crear una regla de firewall para permitir el tráfico de red protegido por una regla de seguridad de conexión.

Perfiles de firewall

Un perfil de firewall es una forma de agrupar configuraciones, como reglas de firewall y reglas de seguridad de conexión, que se aplican al equipo dependiendo del tipo de la red a la que está conectado. Hay tres perfiles para el Firewall de Windows con seguridad avanzada:

- **Dominio:** Se aplica a un adaptador de red conectado a una red con controlador de dominio. Es el perfil menos restrictivo.
- **Privado:** Se aplica a un adaptador de red conectado a una red no conectada directamente a Internet, sino que se encuentra detrás de algún dispositivo de seguridad, como un enrutador NAT o un firewall hardware.
- **Público:** se aplica a un adaptador de red conectado directamente a Internet. Es el perfil más restrictivo, ya que el equipo está conectado a una red en la que no se puede controlar la seguridad.

A cada adaptador de red se le asigna el perfil de firewall que coincide con el tipo de red detectado. Si un adaptador de red se conecta a una red pública, todo el tráfico que tenga esa red como origen o destino se filtrará según las reglas de firewall asociadas con el perfil público.

4. Ver las reglas del firewall

El firewall de Windows aplica políticas (acciones) predeterminadas contrarias para el tráfico entrante y para el tráfico saliente.

Todo el tráfico entrante es bloqueado. Hay que crear reglas para permitir que los programas que actúan como servidores o servicios que escuchan en un puerto puedan funcionar.

Todo el tráfico saliente es permitido. Hay que crear reglas que limiten los programas que pueden enviar información a la red.

Ver las reglas de entrada

Seleccionar "Reglas de entrada" en el panel izquierdo o en el panel central dentro del bloque Introducción. Aparecen las reglas de entrada en el panel central. Para cada regla, de modo predeterminado, se puede ver:

- Nombre
- Grupo
- Perfil
- Habilitado
- Acción
- Invalidar
- Programa
- Dirección local
- Dirección remota
- Protocolo
- Puerto local
- Puerto remoto
- Usuarios autorizados
- Equipos autorizados
- Entidades de seguridad locales autorizadas
- Propietario de usuario local
- Paquete de la aplicación

Observar que cada regla tiene a la izquierda de su nombre un símbolo:

- Un círculo verde con OK si está habilitada y la acción es permitir o un círculo rojo (señal de tráfico de prohibición) si está habilitada y la acción es bloquear.
- Espacio en blanco si la regla está deshabilitada.

Seleccionar una regla pulsando el botón izquierdo del ratón sobre ella y luego pulsar el botón derecho. El menú contextual que aparece permite habilitar o deshabilitar la regla. También tiene una opción Propiedades, que abre una ventana con varias pestañas. También podemos abrir esta ventana pulsando dos veces el botón izquierdo del ratón sobre la regla.

En el **panel derecho de acciones** aplicar filtros para limitar el número de reglas que se pueden ver en el panel central. Los filtros, por perfil, estado y grupo que se seleccionan se aplican conjuntamente.

Usar la opción "Exportar lista..." para guardar la lista de reglas actualmente seleccionadas a un archivo de texto.

Usar la opción de Ver para personalizar las columnas que se muestran en el panel central de la consola.

5. Creación y eliminación automática de reglas al agregar y quitar programas

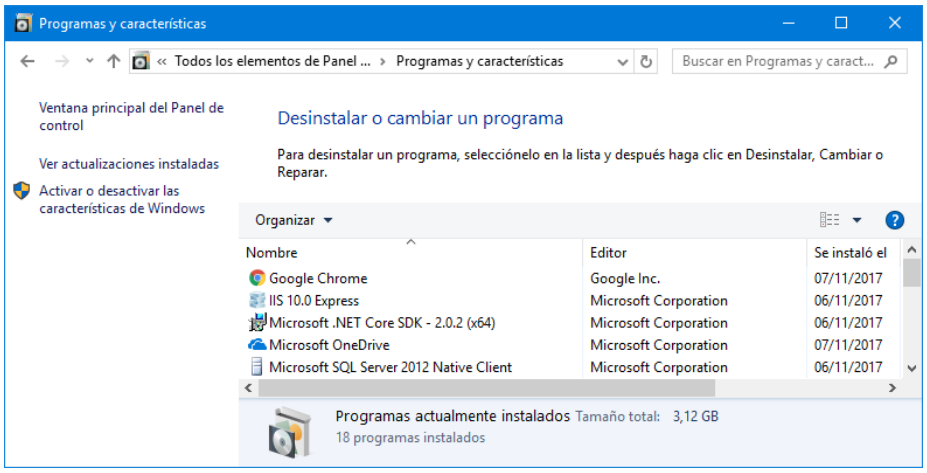
Es muy común que al instalar un nuevo programa que utilice la red, el instalador del programa cree y habilite las reglas necesarias en el firewall para que el programa pueda funcionar correctamente. Lo mismo ocurre cuando se habilitan nuevas características de Windows. Esto evita que los usuarios tengan que configurar el firewall con cada nuevo programa que utilicen.

Por ejemplo, para que un servidor IIS que se esté ejecutando en un computador sea accesible desde otros computadores es necesario abrir los protocolos y puertos adecuados en el Firewall de Windows. Para ello se realizarán diversas tareas en varias fases.

FASE 1: En primer lugar hay que comprobar que el servidor web IIS no esté activado en el sistema operativo. Para ello hacer:

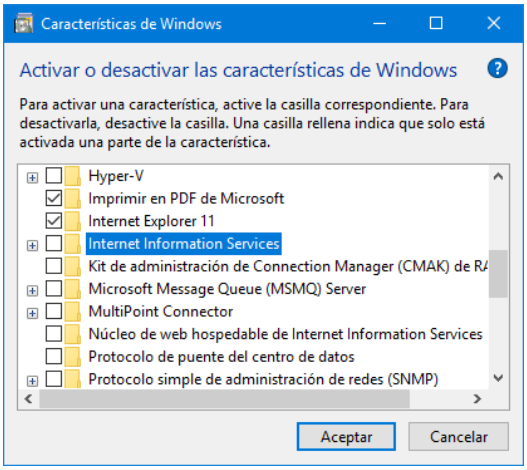
Inicio > Panel de control > Programas y características

Aparece la ventana siguiente:



Seleccionar "Activar o desactivar las características de Windows" en el panel izquierdo.

Aparece la ventana que se muestra a continuación:



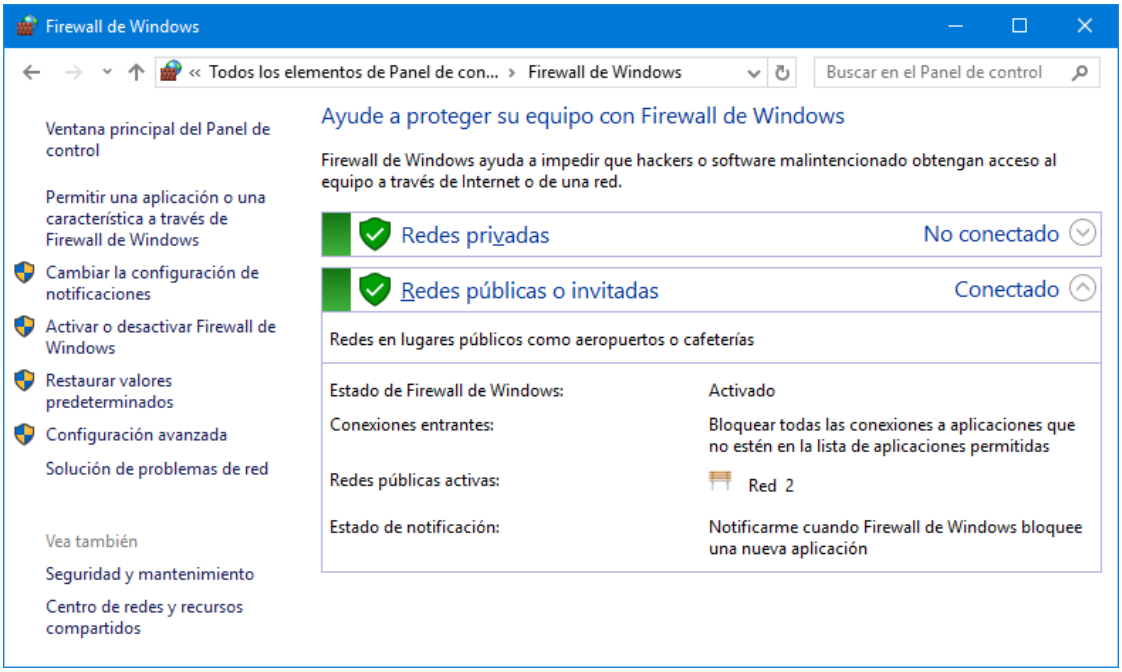
Comprobar que la casilla de selección "Internet Information Services" (IIS) está vacía. Si no lo estuviera deseleccionar IIS. Generalmente, será necesario reiniciar el computador para eliminar totalmente el IIS.

FASE 2: Comprobar que no hay reglas para un servicio que no está activado (instalado).

Arrancar el Firewall haciendo:

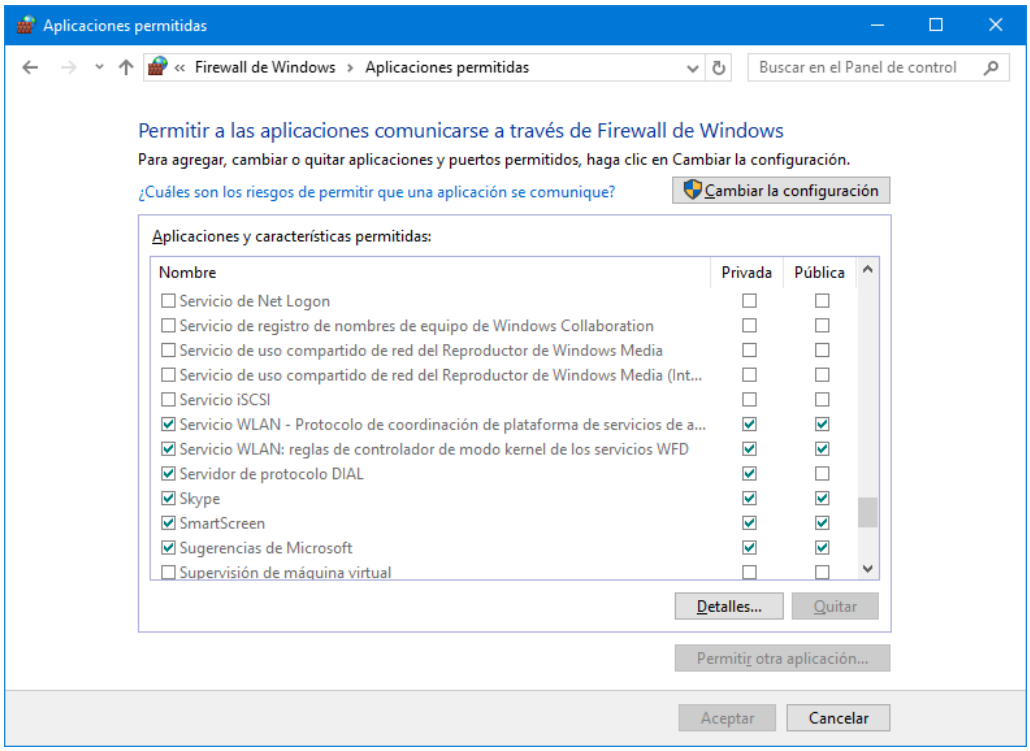
Panel de Control > Firewall de Windows

Aparece la ventana siguiente:



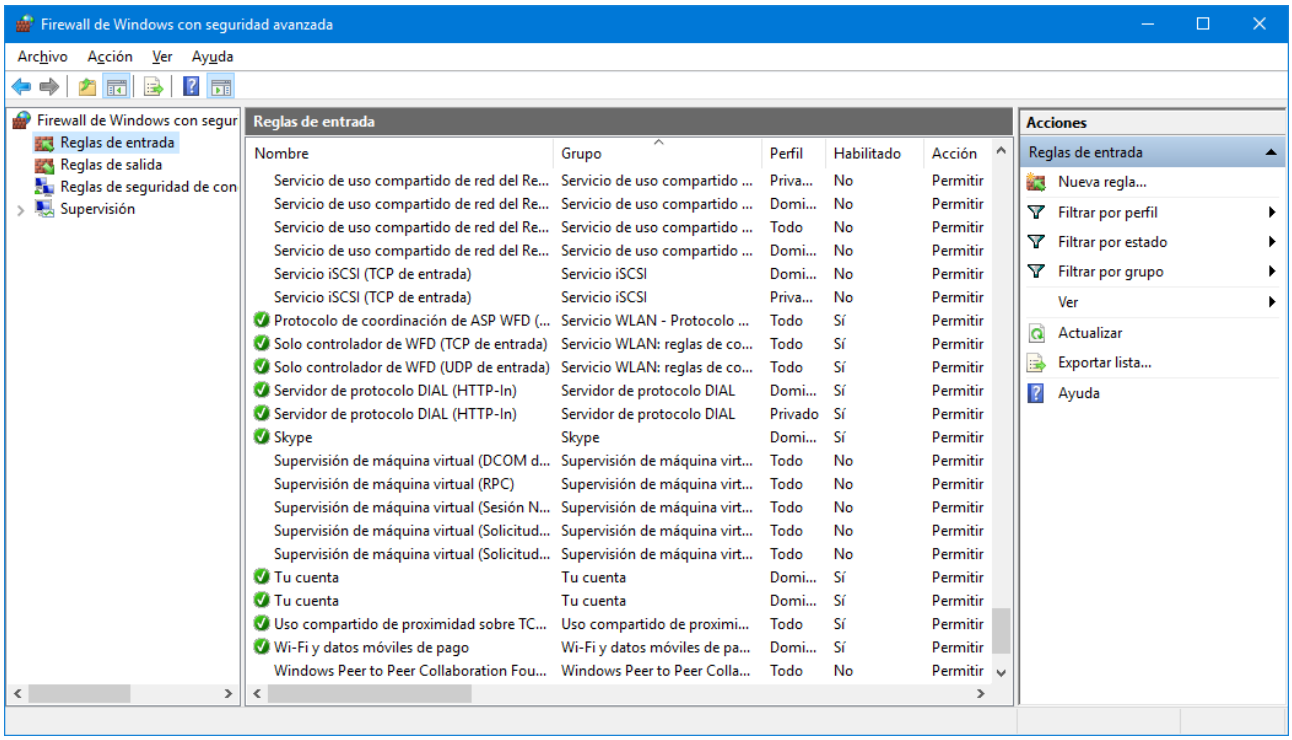
Selecciona "Permitir una aplicación o una característica a través de Firewall de Windows" en el panel izquierdo.

Aparece la ventana que se muestra a continuación:



En esta ventana se ha utilizado la barra de desplazamiento vertical para ir a los últimos programas y características permitidos. Observar que hay varios servicios, pero no aparecen los Servicios de World Wide Web, lo cual es lógico ya que no están activados.

Activar el "Firewall Avanzado" y mostrar las reglas de entrada. En el panel central visualizar las últimas reglas. Se puede observar lo siguiente:



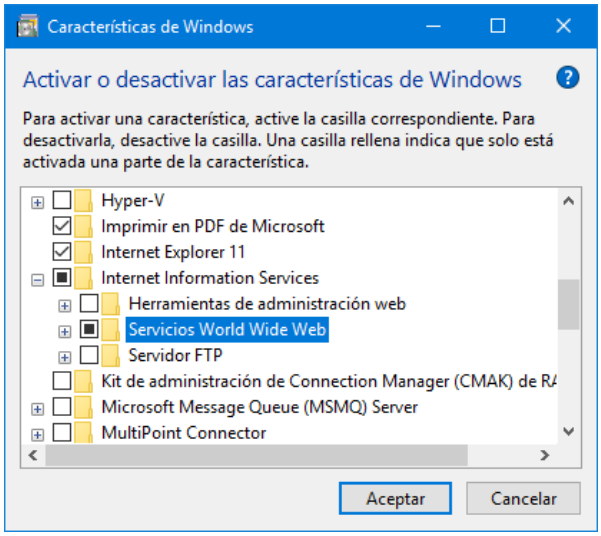
Esta pantalla muestra que no hay reglas que limiten el tráfico de los Servicios World Wide Web, ya que no están activados o instalados.

No obstante se puede comprobar que hay reglas no habilitadas para varios servicios como:

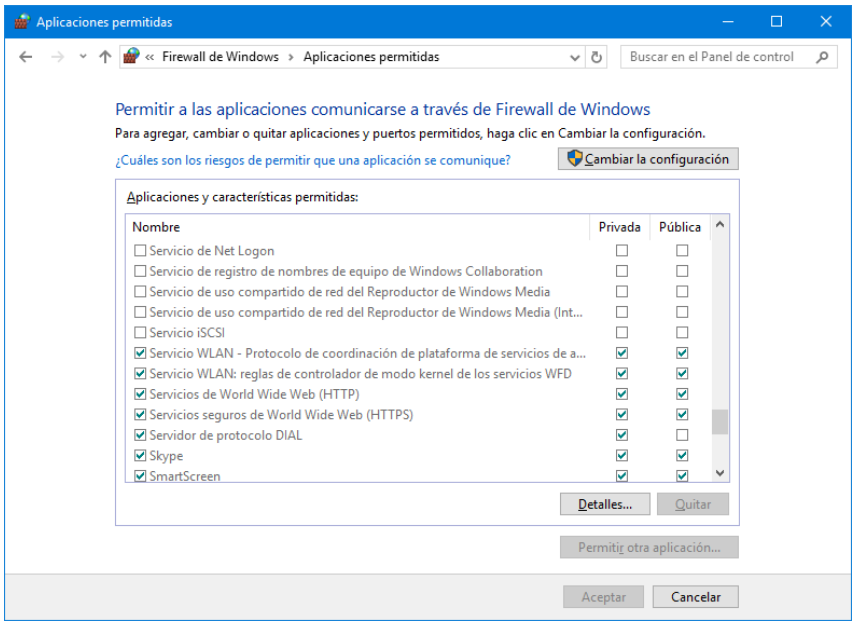
- Servicio de uso compartido de red del Reproductor de Windows Media
- Servicio iSCSI
- Supervisión de máquina virtual

Comprobar que estos servicios también están disponibles es la lista de "Aplicaciones y características permitidas" que muestra el Firewall Básico en la ventana "Aplicaciones permitidas". Observar que aparecen sin seleccionar, indicando que su tráfico no está habilitado.

FASE3: Activar (instalar) IIS seleccionándolo tal como se muestra en figura siguiente.



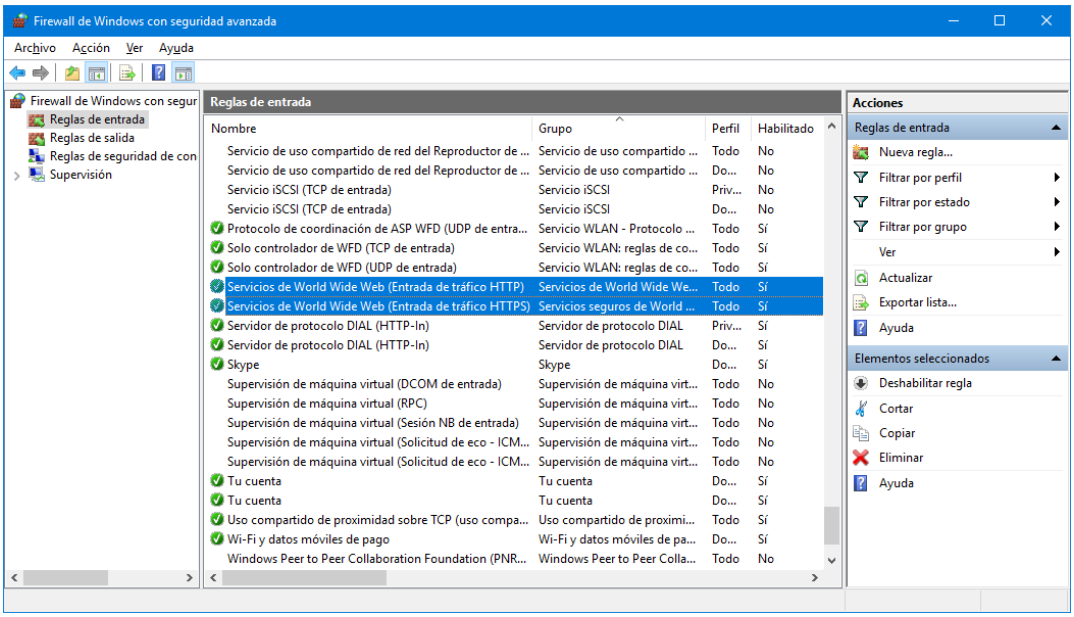
FASE 4: Comprobar que el Firewall ha incluido al IIS entre los servicios cuyo tráfico debe controlar. En el Firewall Básico aparecen nuevos servicios, como muestra la figura siguiente.



Observar que ahora se muestran dos nuevos servicios:

- Servicios de World Wide Web (HTTP)
- Servicios seguros de Word Wide Web (HTTPS)

Ambos servicios aparecen como seleccionados, por lo que el Firewall permitirá su tráfico, tanto en redes privadas como públicas. En el Firewall Avanzado aparecen nuevas reglas, como muestra la figura siguiente.



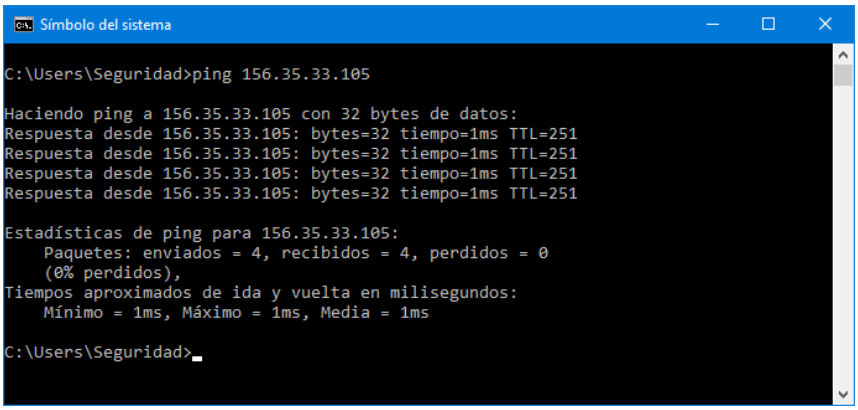
Observar las reglas con fondo azul. Son para controlar el tráfico entrante de los servicios de World Wide Web. Su Acción es Permitir el tráfico, y ya están Habilitadas.

FASE 5: Volver al estado inicial.

Ahora se puede eliminar el IIS del sistema, para devolver al sistema al estado inicial y comprobar que el Firewall elimina las reglas que no son necesarias.

6. (Des)activación del eco a Ping

La utilidad Ping (*Packet Internet Groper*) es muy útil para comprobar si un determinado host de una red es accesible. Para ello, Ping envía el mensaje *echo*, del tipo ICMPv4 (*Internet Control Message Protocol*) al host. La pantalla siguiente muestra un ejemplo.

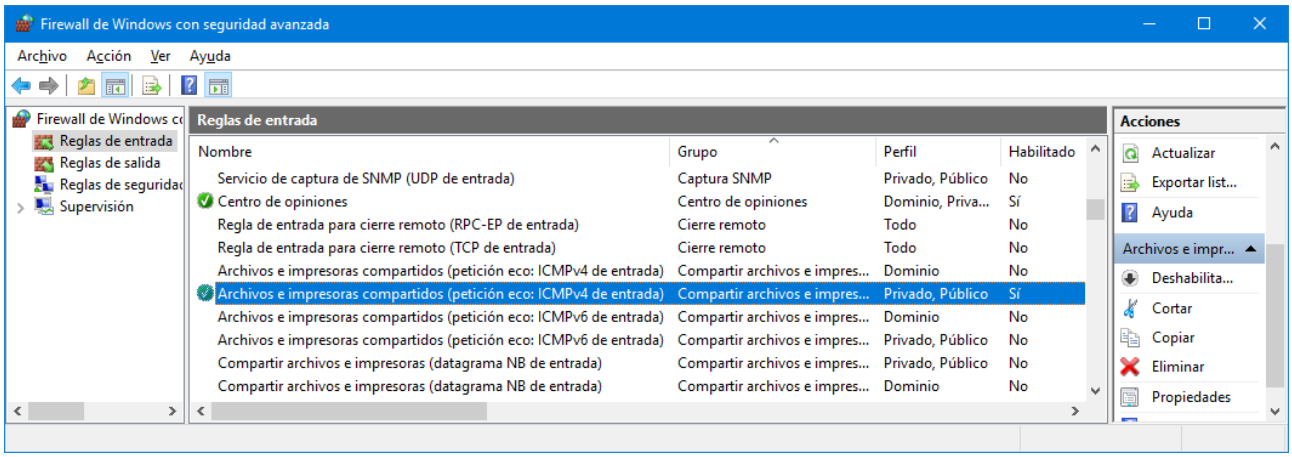


Pero si el firewall del host que recibe el mensaje *echo* no está configurado para recibirlo, Ping dará un error por time-out.

Un concepto muy importante a considerar es que no hay que abrir ningún número de puerto en el Firewall, pues Ping no utiliza puertos. Ping no funciona en las capas TCP o UDP donde tienen sentido los números de puertos. Ping trabaja solo en la capa IP.

En esta sección de la práctica se explica cómo indicar al Firewall de Windows que permita los mensajes eco de ICMPv4.

Abrir el Firewall avanzado y en el panel izquierdo seleccionar "Reglas de entrada". Entonces, el panel central muestra las reglas tal como se indica en la figura siguiente. Desplazarse hacia abajo en el panel central hasta alcanzar la regla: Archivos e impresoras compartidos (petición eco ICMPv4 de entrada). Hay dos reglas, una para el perfil de Dominio y otra para los perfiles Privado, Publico.



Se puede ver que la regla está habilitada. Comprueba que la MV responde al ping enviado desde la máquina física anfitrión por ejemplo.

Seleccionar la regla "Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada) de los perfiles Privado, Público. El fondo de la regla se pone en azul. Pulsar el panel derecho el botón "Deshabilitar regla". Comprueba que la MV no responde al ping.

Finalmente, vuelve a habilitar la regla y comprueba que la MV vuelve a responder al ping.

7. Permitir el tráfico de un programa

En esta sección de la práctica se aprende como crear las reglas que permiten comunicarse a programas específicos.

Para realizar esta sección de la práctica hay que desarrollar dos pequeños programas: un servidor y un cliente. Pero para acelerar el desarrollo de la práctica **se proporcionan en el campus virtual**.

FASE.-1 Programa Servidor (pServidor)

Crea un nuevo proyecto C# de consola y añade los espacios de nombres: System.Net, System.Net.Sockets, y System.Threading.

1) Declara la variable entera TamBuf y asígnale un valor reducido, por ejemplo 10. Crea dos arrays de bytes, Peticion y Respuesta del tamaño indicado en TamBuf.

Declara tres variables enteras, BytesRecibidos, BytesEnviados y NumConex, para uso posterior.

2) Declara el objeto DirLocal de la clase **IPAddress**, e inicialízalo con la dirección IP del servidor usando el método **Parse()** o permite que se utilice cualquier dirección IP disponible en el servidor inicializándolo con el comodín **IPAddress.Any**.

Declara la variable entera PuertoLocal e inicialízala con el número de puerto en el que escuchará el servidor, por ejemplo, 2459.

Crea EPLocal, un objeto de la clase **IPEndPoint** , extremo local de una comunicación, e inicialízalo con los objetos DirLocal y PuertoLocal.

3) Crea un objeto SocEscucha, de la clase **Socket**, usando en el constructor los parámetros siguientes: **AddressFamily.InterNetwork**, **SocketType.Stream**, y **ProtocolType.Tcp**.

4) Enlaza SocEscucha a EPLocal usando el método **Bind()**.

5) Haz que SocEscucha escuche peticiones de conexión usando el método **Listen()**.

6) Inicializa la variable NumConex a 0 y crea un bucle infinito **while(true)** en el que el servidor acepta conexiones y las procesa. Dentro del while(true) realiza las acciones siguientes:

7) Incrementa la variable NumConex.

8) Acepta conexiones en SocEscucha usando el método **Accept()** para obtener un nuevo socket para intercambiar datos denominado SocServicio.

9) Muestra la dirección y el puerto remotos de la conexión. Utiliza un objeto EPRemoto de la clase **IPEndPoint**, que se debe inicializar con la propiedad **RemoteEndPoint** de SocServicio haciendo el cast apropiado. Utiliza un objeto DirRemota de la clase **IPAddress**, e inicialízalo con la propiedad **Address** de EPRemoto. Vuelca a la consola DirRemota y el puerto.

10) Recibe mensajes llamando al método **Receive()** de SocServicio y muestra el número de bytes recibidos y los propios bytes recibidos en la consola.

11) Emula el tiempo de procesamiento del mensaje llamando al método estático **Sleep()** de la clase **Thread** y prepara el contenido del búfer Respuesta: todos sus bytes con cero, excepto el último que contendrá el valor de NumConex % 256. (% = Operador Resto de División Entera)

12) Envía el búfer Respuesta llamando al método **Send()** de SocServicio y muestra el número de bytes enviados y los propios bytes enviados en la consola.

13) Cierra SocServicio usando el método **Close()**.

FASE.-2 Programa Cliente (pCliente)

Crea un nuevo proyecto C# de consola y añade los espacios de nombres: System.Net, System.Net.Sockets, y System.Threading.

1) Declara la variable entera TamBuf y asígnale un valor reducido, por ejemplo 10. Crea dos arrays de bytes, Peticion y Respuesta del tamaño indicado en TamBuf.

Declara dos variables enteras, BytesRecibidos, y BytesEnviados, para uso posterior.

2) Utiliza un bucle **for(;;)** para realizar 5 conexiones sucesivas, usando la variable índice Conex. Realiza las siguientes operaciones dentro del bucle.

3) Crea un objeto SocServicio, de la clase **Socket**, usando en el constructor los parámetros siguientes: **AddressFamily.InterNetwork**, **SocketType.Stream**, y **ProtocolType.Tcp**.

4) Declara el objeto DirRemota de la clase **IPAddress**, e inicialízalo con la dirección IP del servidor usando el método **Parse()**.

Declara la variable entera PuertoRemoto e inicialízala con el número de puerto en el que escuchará el servidor, por ejemplo, 2459.

Crea EPRemoto, un objeto de la clase **IPEndPoint**, extremo remoto de una comunicación, e inicialízalo con los objetos DirRemoto y PuertoRemoto.

5) Conecta SocServicio mediante EPRemoto usando el método **Connect()**.

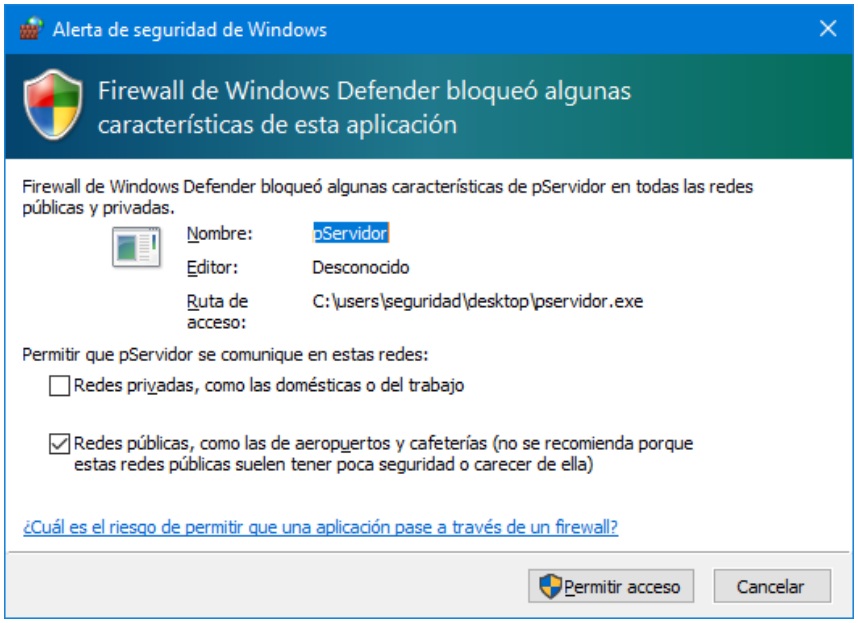
6) Prepara el contenido del búfer Petición: todos sus bytes con cero, excepto el primero que contendrá el valor de Conex % 256.

7) Envía el búfer Petición llamando al método **Send()** de SocServicio y muestra el número de bytes enviados y los propios bytes enviados en la consola.

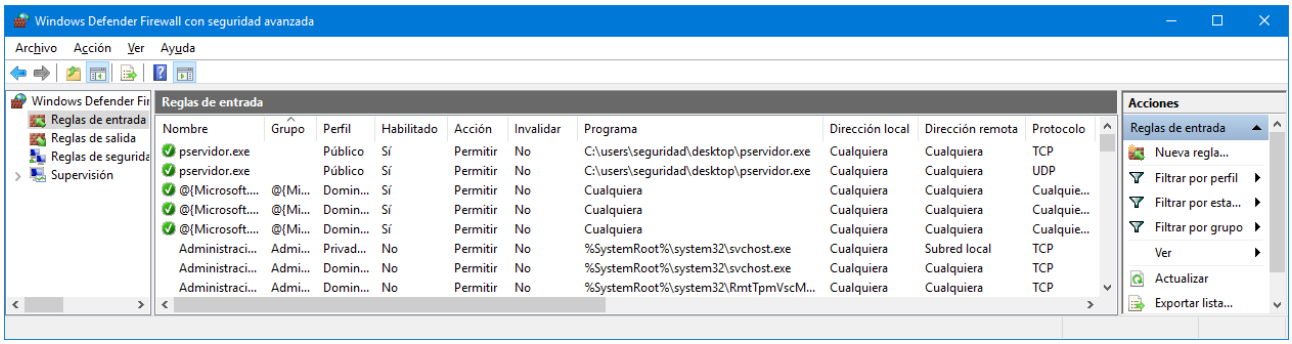
8) Recibe la respuesta del servidor llamando al método **Receive()** de SocServicio y muestra el número de bytes recibidos y los propios bytes recibidos en la consola.

9) Cierra SocServicio usando el método **Close()**.

Copia el fichero pServidor.exe en el escritorio de la Máquina Virtual. Al arrancar el programa pServidor el Firewall de Windows muestra la siguiente ventana:



Si se pulsa el botón "Permitir acceso" el Firewall crea el par de reglas de entrada que se muestran en la figura siguiente.



Como se puede ver, el nombre de las reglas coincide con el nombre del archivo ejecutable. Las reglas están habilitadas. La acción es permitir el tráfico de entrada. Observar que hay dos reglas, pues una es para el tráfico TCP, y otra para el tráfico UDP. Observar que las direcciones y puertos, tanto locales como remotos, pueden ser Cualquiera. Aunque no se ve en la figura anterior los Usuarios autorizados y los Equipos autorizados también pueden ser Cualquiera.

Arrancar pCliente en otro computador (máquina física o virtual). Observar que para las conexiones salientes, no ha sido necesario configurar el Firewall del computador cliente, ya que el Firewall de Windows permite el tráfico saliente de forma predeterminada.

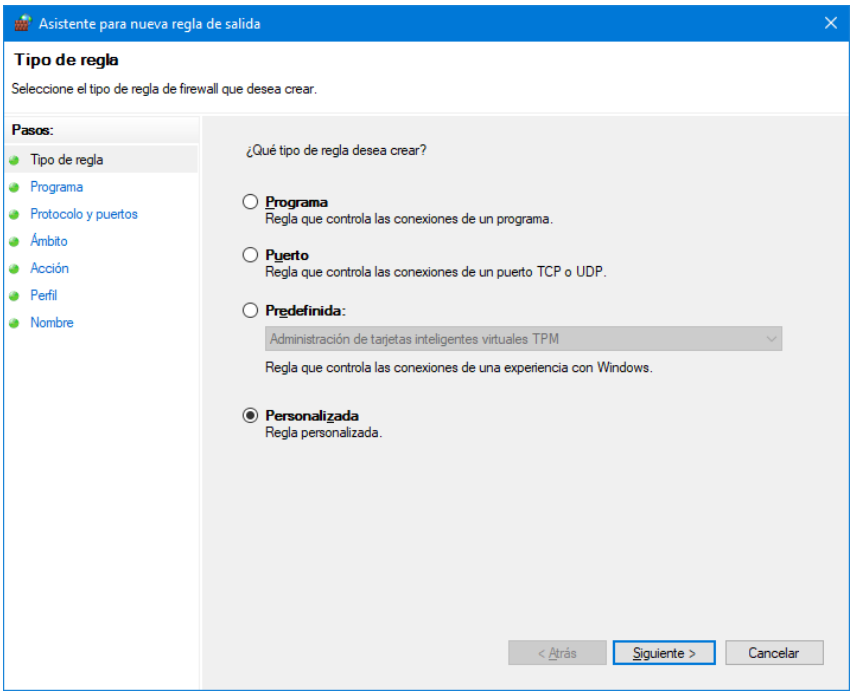
Pero conviene reflexionar sobre el hecho de que pCliente debe recibir las respuestas que le envía pServidor. No hay que hacer nada para recibir este tráfico entrante a través del Firewall.

Claramente el Firewall de Windows es un Firewall con estado y que por tanto recuerda que conexiones salientes están establecidas y permite de modo automático las respuestas.

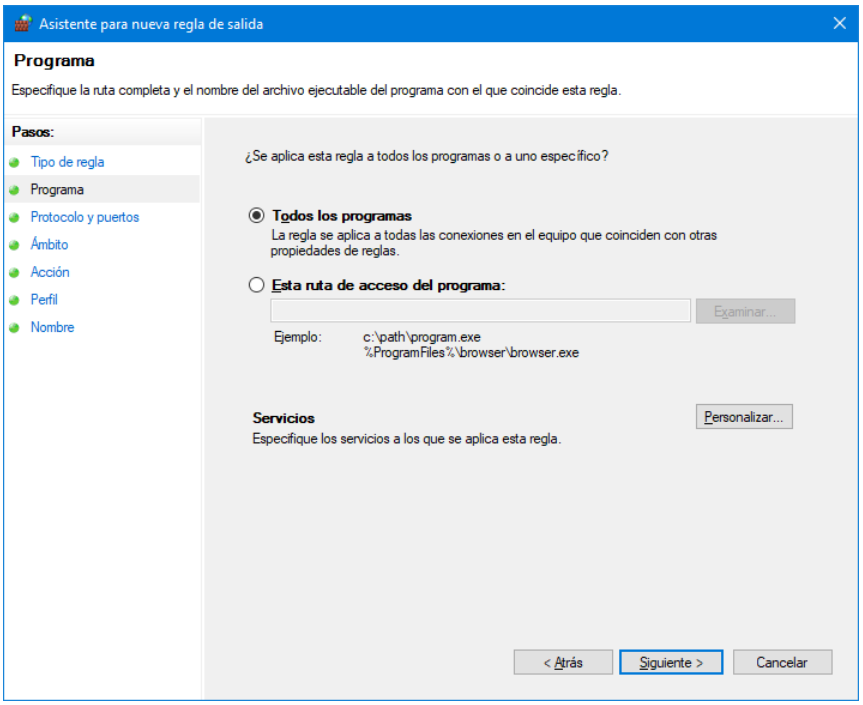
8. Bloquear la salida de un computador

En esta sección de la práctica se aprende como crear una regla particularizada. Como ejemplo se crea una regla para que un computador solo pueda comunicarse con una única IP. Esta configuración es típica en un entorno de alta seguridad en la que solo se permite a cada computador conectarse justo con los computadores con los que necesita intercambiar información.

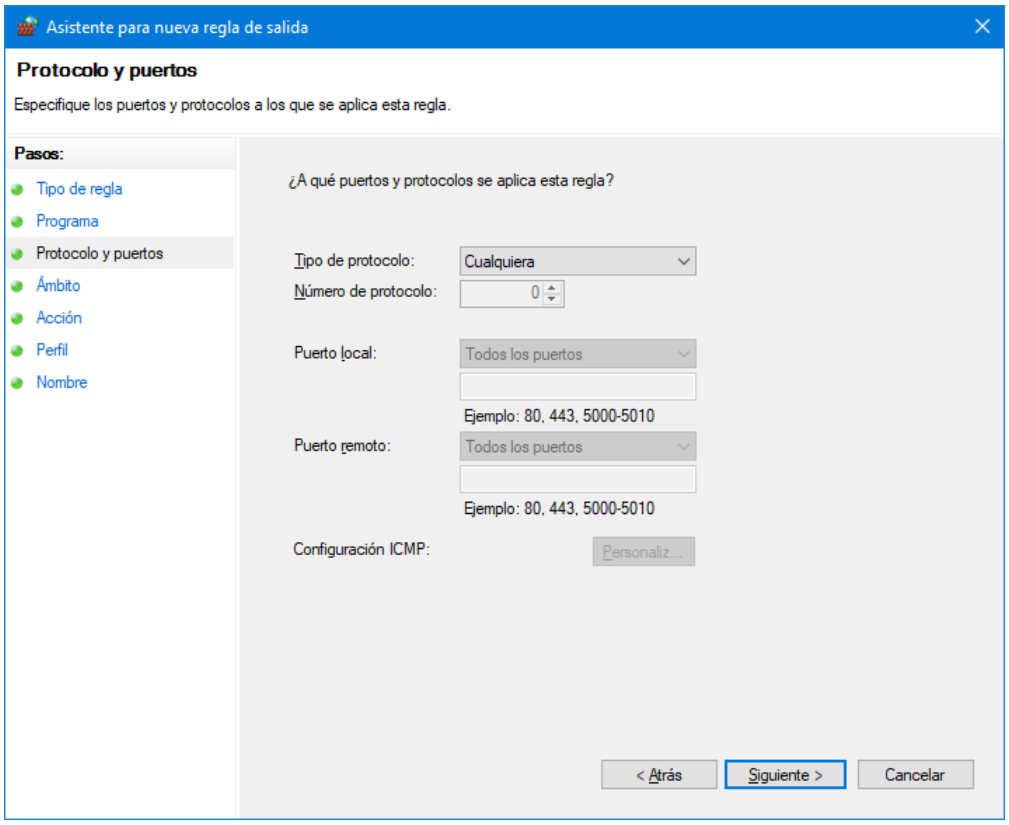
Crea una nueva regla de salida. Se abre la ventana "Asistente para nueva regla de salida". En el panel izquierdo aparecen los pasos sucesivos a realizar. Selecciona el tipo de regla: Personalizada.



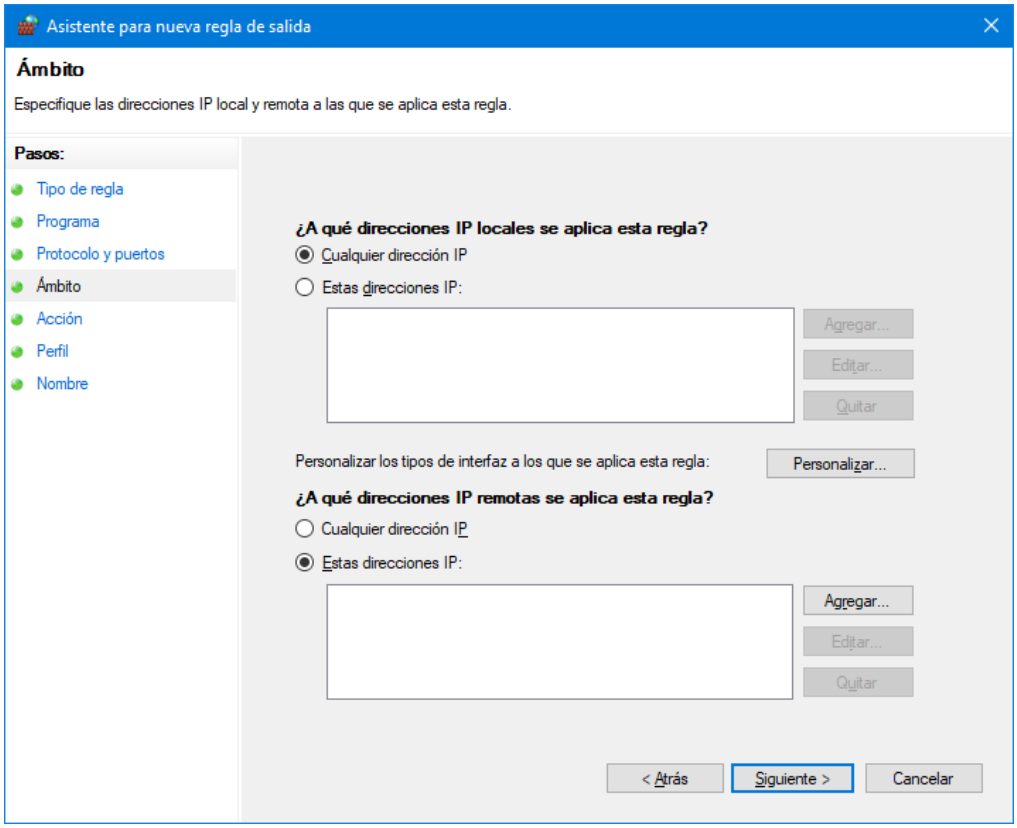
Pulsa el botón Siguiente. En la ventana que aparece selecciona los programas a los que se aplica: Todos los programas.



A continuación selecciona el protocolo y los puertos a los que se aplica: Cualquiera. Con esta opción no es necesario especificar puertos.

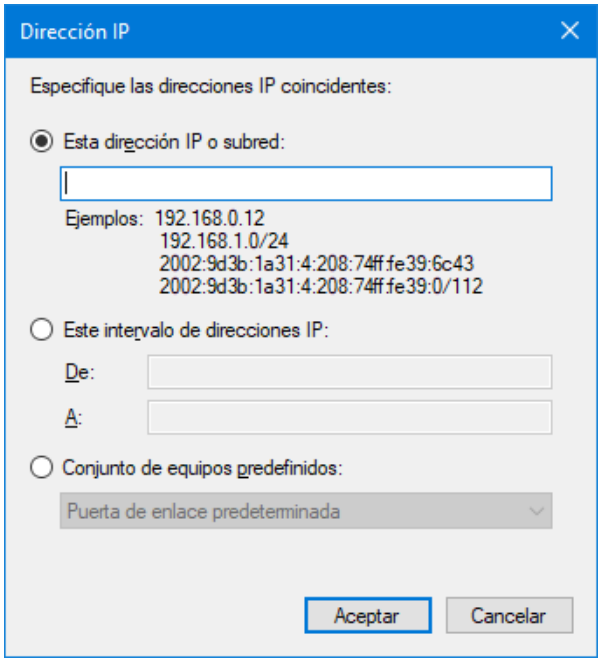


Selecciona el ámbito (direcciones IP locales y remotas) de la regla. Elije Cualquier dirección IP local y Estas direcciones IP remotas.

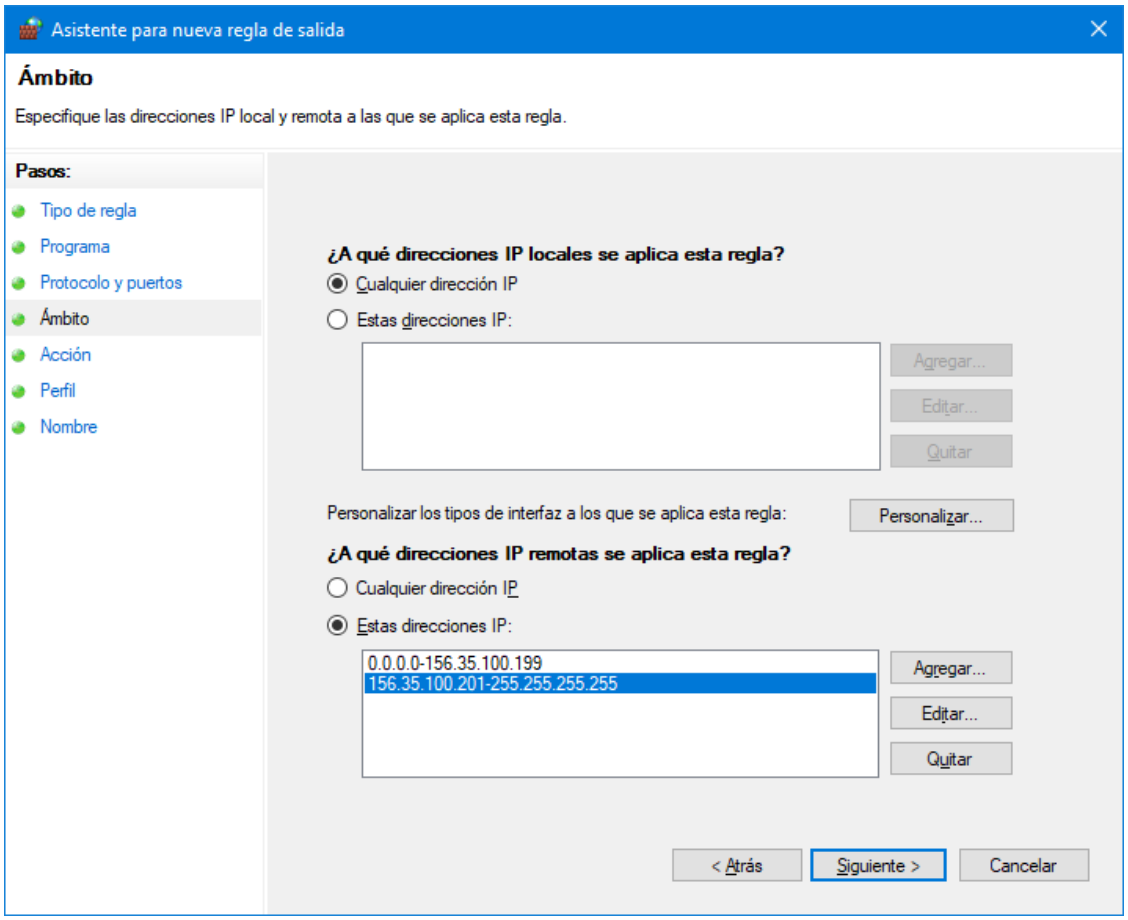


Pulsa el botón Agregar.

Aparece la ventana siguiente que permite seleccionar direcciones IP:

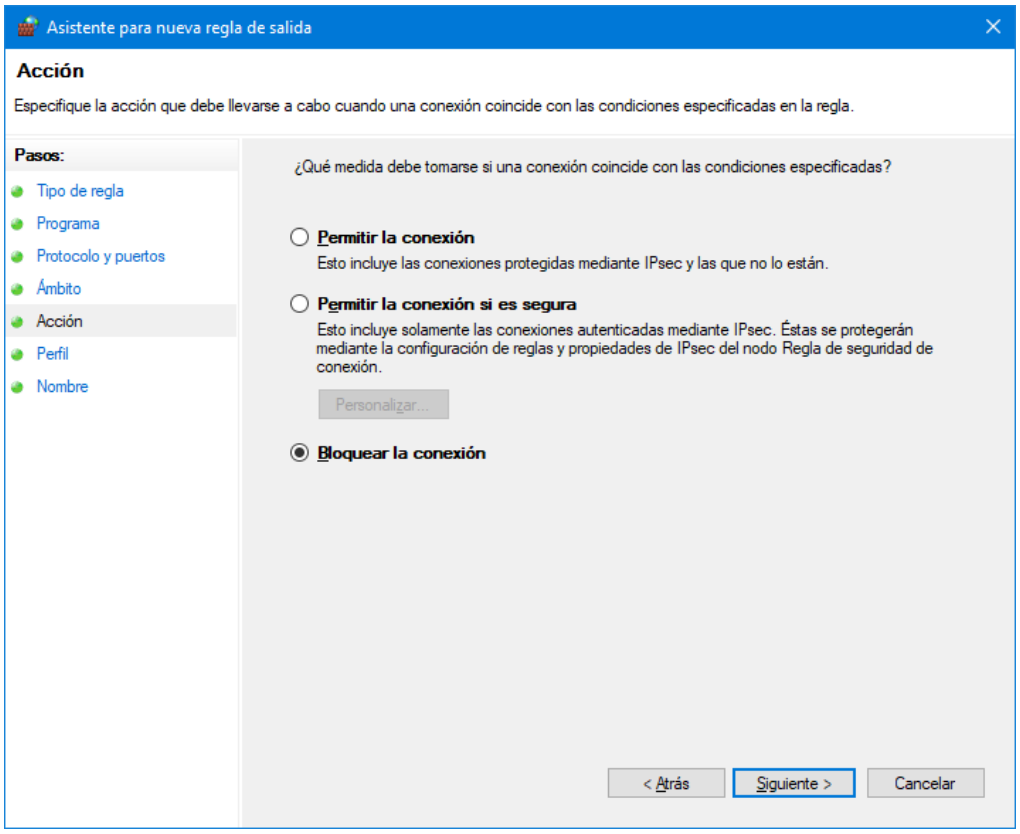


Selecciona "Este intervalo de direcciones IP" para introducir cada intervalo a usar. Por ejemplo, para permitir la conexión solo con la IP 156.35.100.200 hay que introducir dos rangos de direcciones a bloquear: 0.0.0.0 a 156.35.100.199 y 156.35.100.201 a 255.255.255.255.

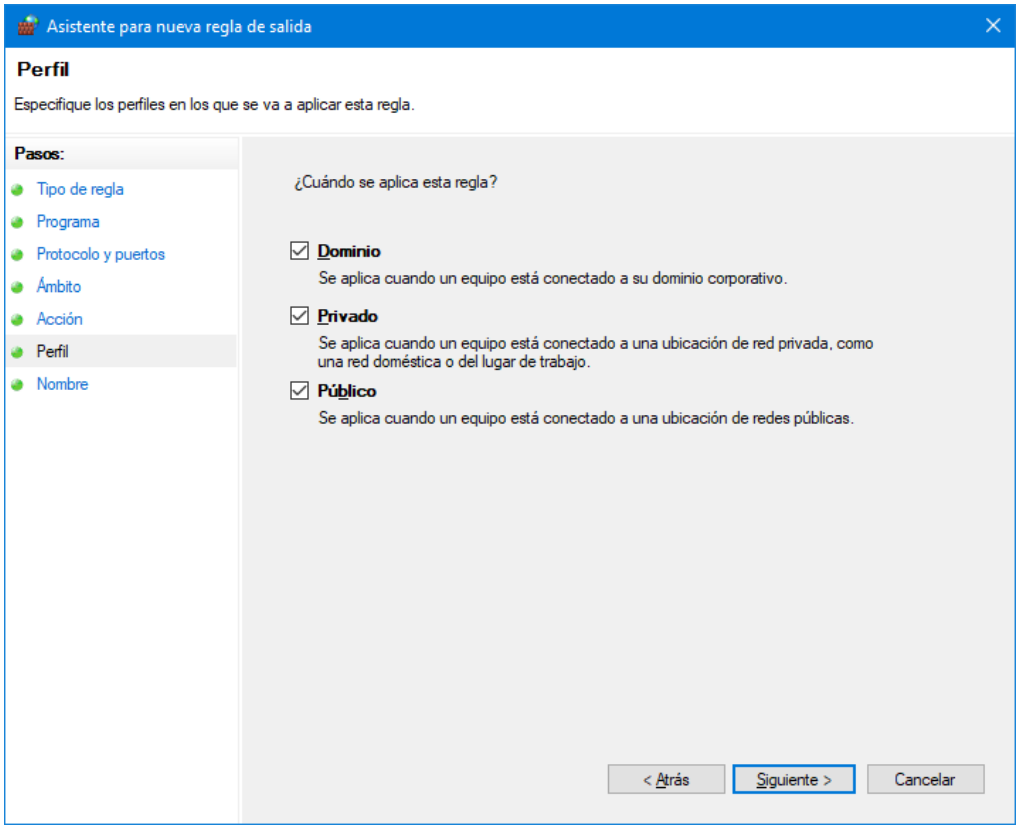


Comprueba la dirección IP que tiene la máquina física en la que se está ejecutando la máquina virtual y en la ventana de Ámbito define exactamente los dos rangos de direcciones IP que solo permiten el tráfico con la máquina física.

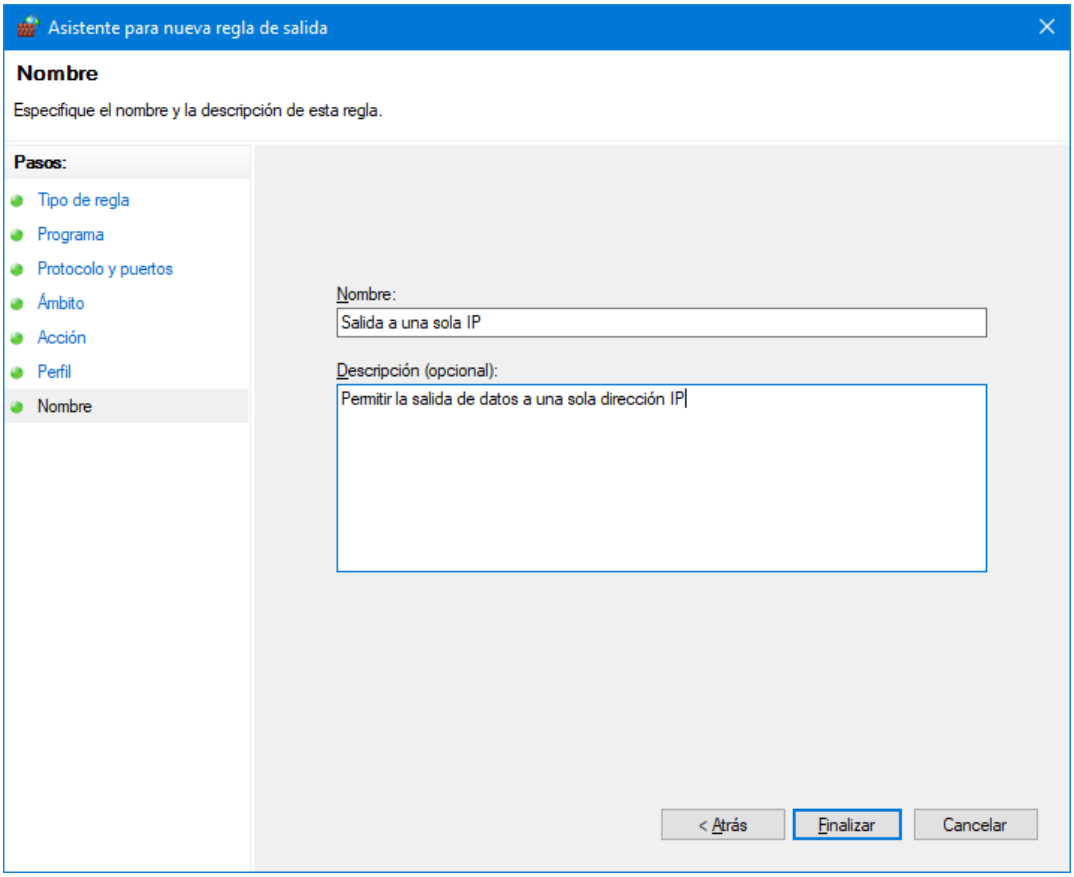
Selecciona la acción a tomar cuando los parámetros de una conexión coinciden con las indicadas en esta regla: Bloquear.



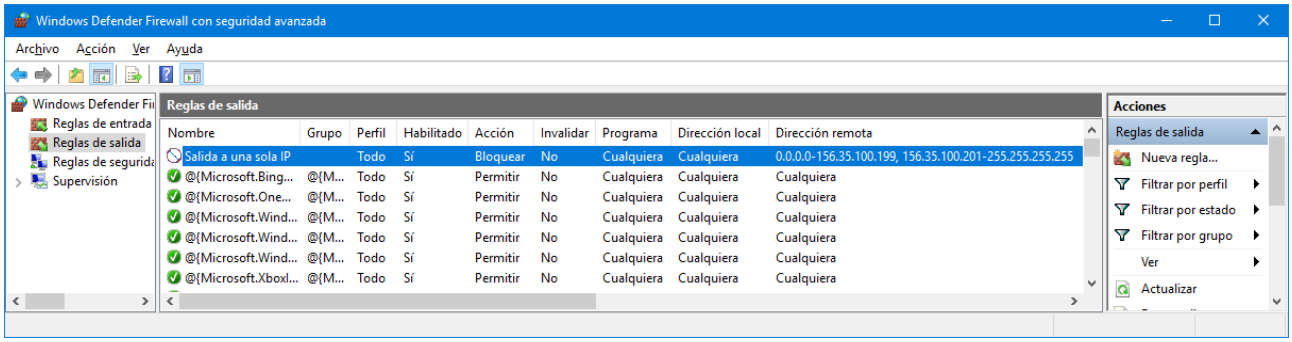
Especifica los perfiles (ubicaciones de red) en los que se aplica la regla: Todos.



Para terminar da un nombre a la regla y descríbela (documéntala).



Observa que en la ventana principal de las reglas de salida del Firewall aparece la nueva regla. Observa el disco de prohibición que indica que la acción es denegar y que la regla está habilitada.



Comprueba que la regla funciona:

Recompila el programa pCliente para que se conecte con pServidor que se ejecutará en la máquina física o en otra máquina virtual. Ejecuta el programa pCliente en la máquina virtual conectándose a la máquina física (la única con la que debe poder conectarse) y comprueba que puedes conectarte.

Conéctate a http://www.google.es y comprueba que no puedes conectarte.