Cortafuegos con Windows 2000 o XP

Por José Mariscal Prieto
i72maprj@uco.es Página Web
Todos los derechos reservados, este texto esta registrado.

1. Cómo montar un cortafuegos sin software adicional

Windows 2000, y Windows XP tienen la posibilidad de crear reglas de filtrado para montar un cortafuegos sin la necesidad de instalar un software adicional, así controlamos que instalamos. También aquellos usuarios que solo tengan un PC, si tienen varios en Red pueden que tengan problemas si no se configura correctamente. Esto va dirigido a los usuarios mas noveles, los administradores avanzados sabrán como modificar las directivas de seguridad, aunque seguramente usarán algún cortafuegos que es mucho mejor que esto. Además dispone de un asistente para agregar reglas de filtrado, el único inconveniente es que hay que bloquear puerto por puerto los que queramos bloquear. Para ello nos vamos al Panel de Control, y dentro de este Herramientas Administrativas, donde seleccionamos **Directiva de Seguridad local**.

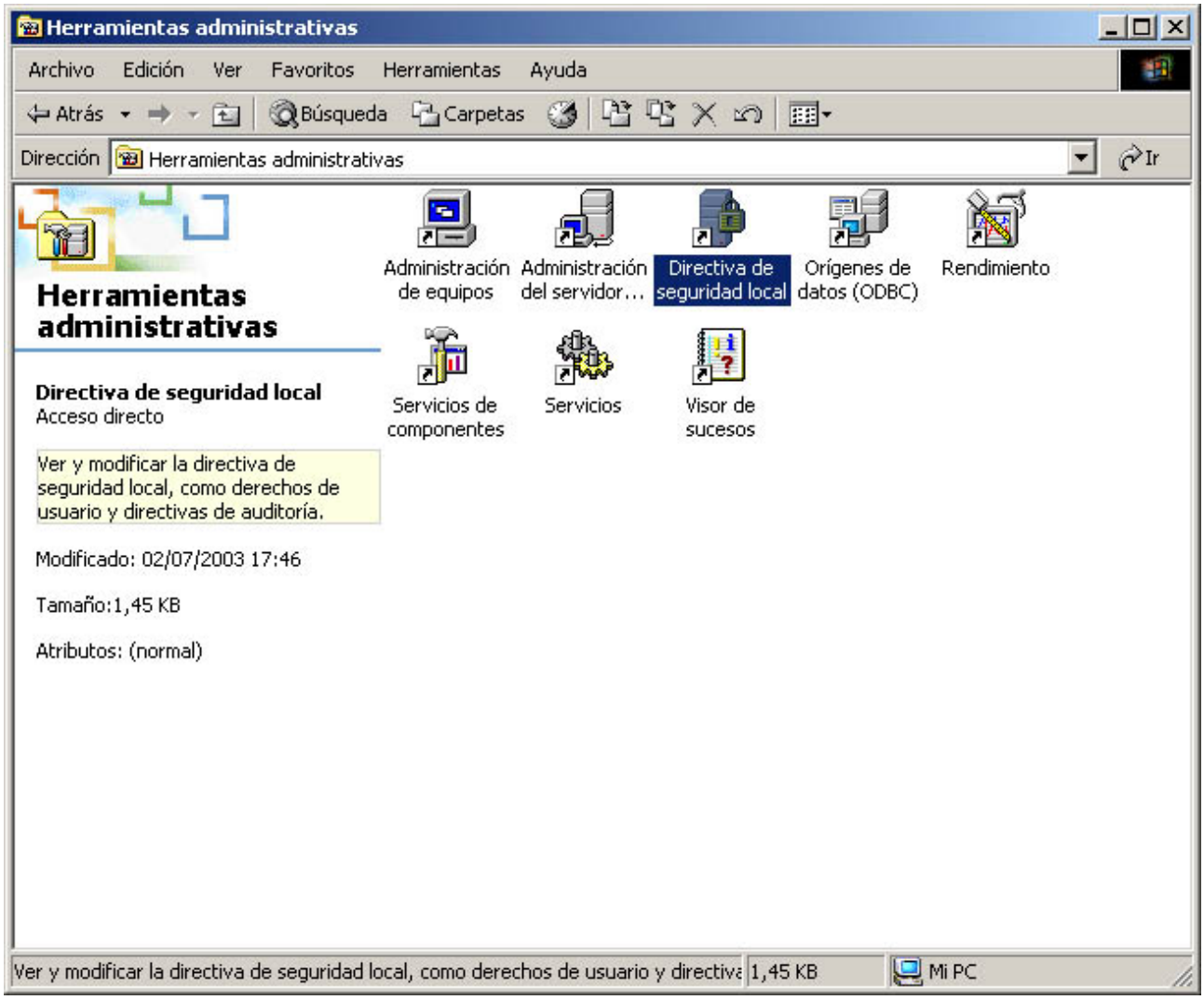

Figura 1: En la imagen Herramientas Administrativas, dentro del Panel de Control

Se nos abrirán las Directivas de Seguridad, entre estas la Directiva de Seguridad IP. Seleccionamos el icono de **Directivas de seguridad IP en la Máquina local**, y en la parte derecha hacemos click con el botón derecho, y le damos a **Crear directiva de seguridad IP**

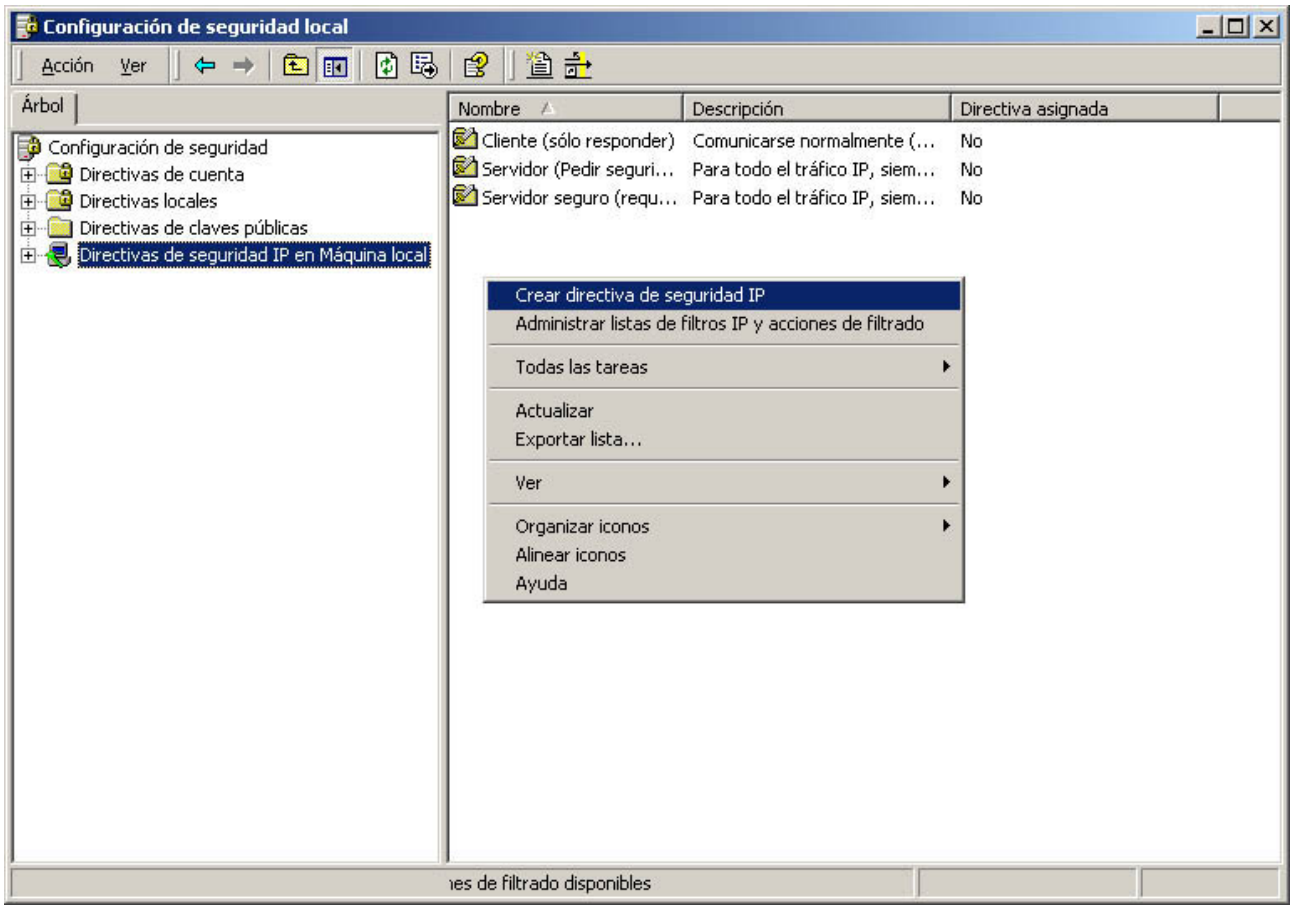

Figura 2: Las Directivas de Seguridad IP permiten crear nuevas opciones de Filtrado IP

Lo que vamos a hacer es crear un cortafuegos siguiendo los siguientes pasos:

1. Crear una Directiva de seguridad. **Cortafuegos**
2. Crear una Lista de Filtros. **No Dejar**
3. Crear una acción de Filtrado, aplicable a la lista de filtros. **Filtrado Bloquear**
4. Activar la Directiva de seguridad.

Ruego encarecidamente que si tu equipo esta dentro de una red corporativa, avisa a tu Administrador de Red ya que podrías generar conflictos en tu red y no podrían acceder a tus datos, según el diseño del sistema.

Windows posee un asistente que usaremos para crear una nueva directiva y bloquear un puerto de ejemplo. Este asistente se inicia de manera automática. Lo que haremos sera crear primero una directiva y luego ampliar esa directiva, con los puertos que queramos bloquear.

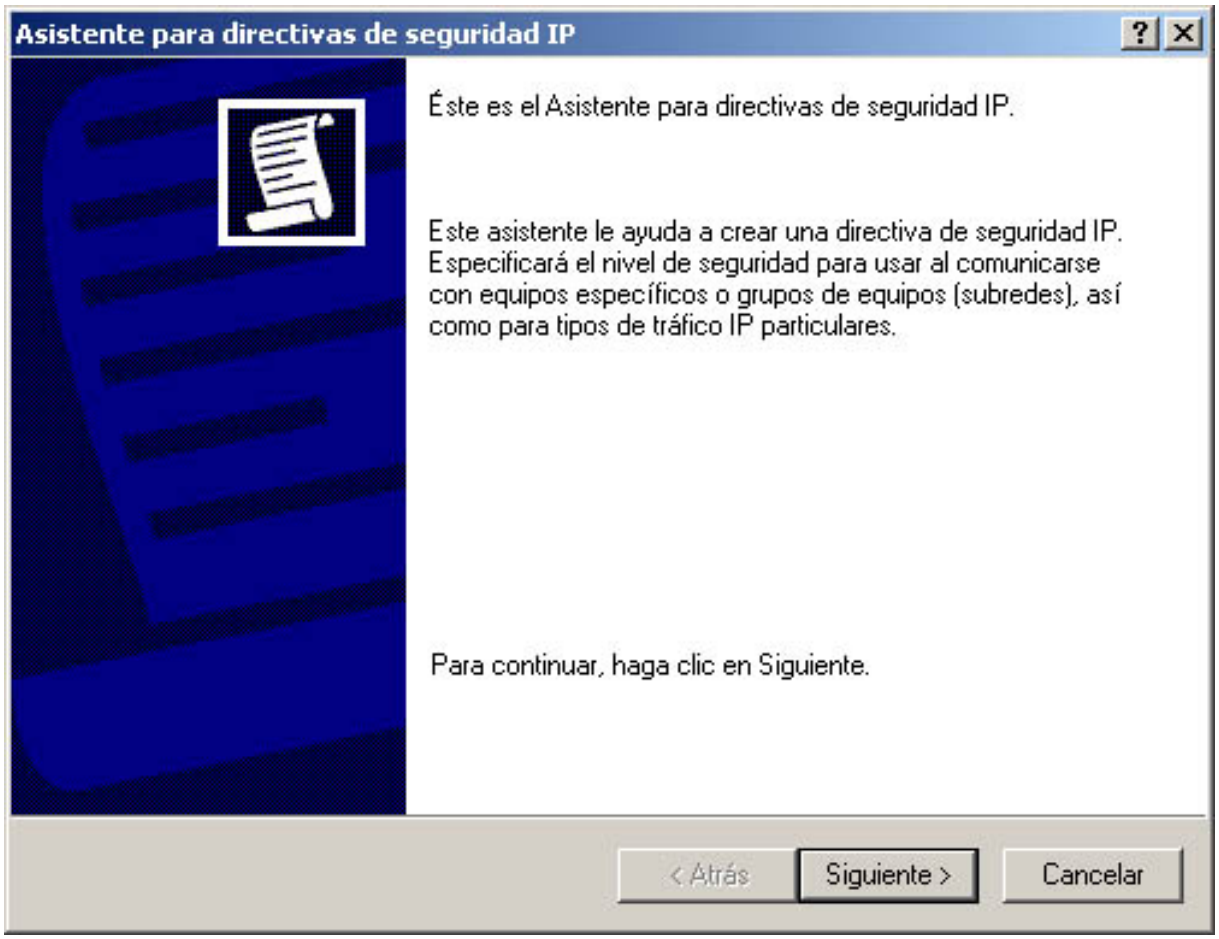

Figura 3: El asistente permite crear nuevas opciones de filtrado de manera sencilla.

Lo único que tendremos que decirle es el nombre de la directiva. Esta es la directiva que mencionamos al principio, es la que va a almacenar la lista de filtros, y la acción que hacer.

Podemos asignarle una descripción: Esta directiva, lo que va a hacer es bloquear los puertos mas proclives de ser atacados.

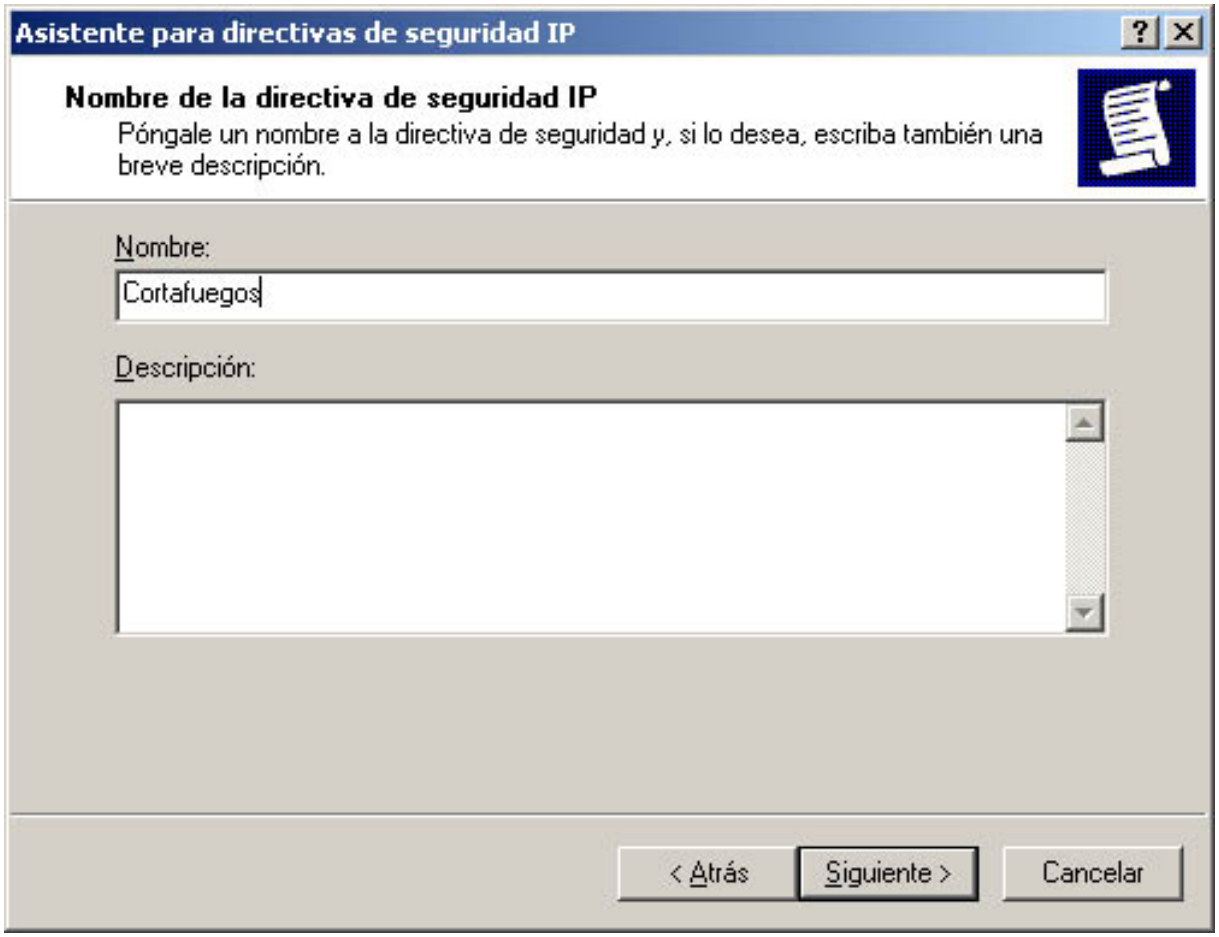

Figura 4: Le asignamos un nombre a la Directiva, por ejemplo Cortafuegos.

Los filtros podemos englobarlos, y ser utilizados dentro de una misma directiva. Podemos tener varias directivas pero sólo *una estará activa* en nuestro sistema, es decir no podremos utilizar varias directivas a la vez. Se explicará como activar una directiva en el último paso.

Eligiremos el método predeterminado, ya que no necesitaremos otra normativa mas avanzada.

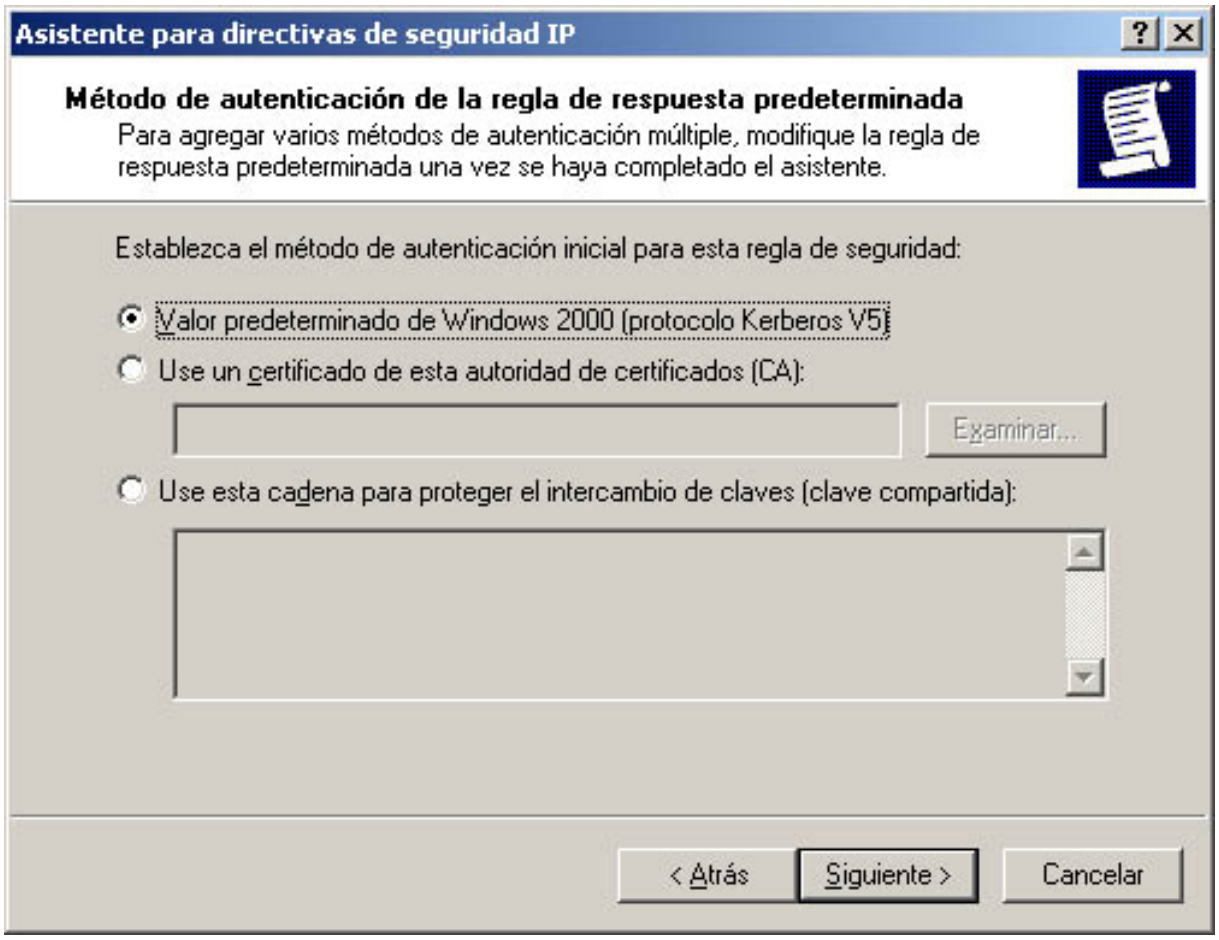

Figura 5: Windows soporta varios métodos de Autenticación, utilizaremos el predeterminado.

Seguramente nos saldrá una advertencia, nuestro equipo no está dentro de un Dominio, más si solo tenemos nuestro equipo, le damos a SI.

Ya disponemos de una directiva de seguridad IP, modificando sus propiedades podremos ampliar esta política para que bloquee los puertos que estimemos necesarios.

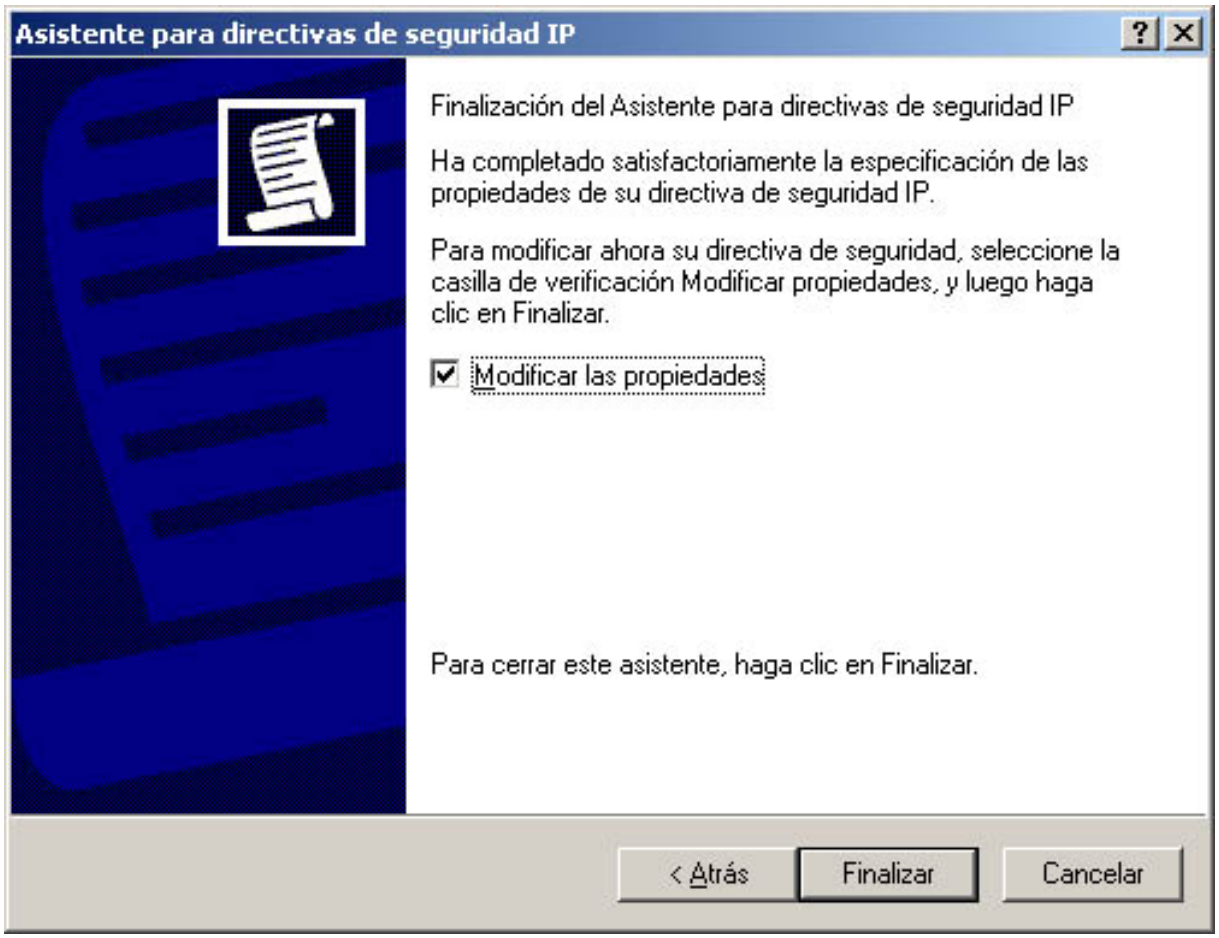

Figura 6: Tenemos la directiva de seguridad creada, solo hay que modificar sus propiedades.

Para bloquear los puertos que queramos crearemos filtros, en el ejemplo crearemos solo uno, y luego al final se dará un resumen sobre los puertos que debemos bloquear y que podrían poner en un aprieto a nuestro sistema.

Si todo ha ido bien, ya tenemos nuestra directiva de seguridad IP creada. Podemos eliminar la regla de Dinámico. Porque lo que queremos hacer es crea nuevos Filtros que nos permitan bloquear los puertos y protocolos que no queremos que accedan a nuestro ordenador.

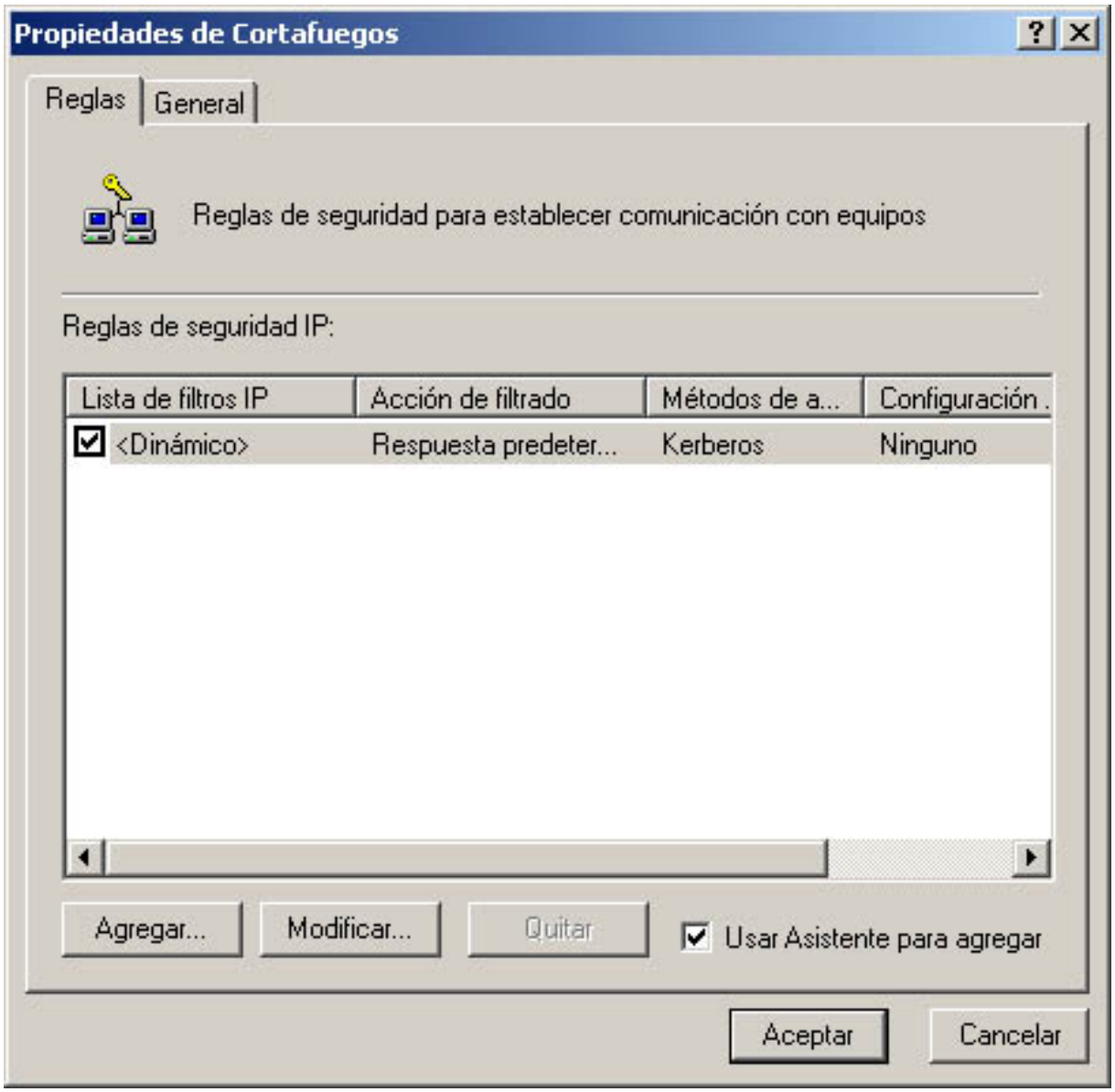

Figura 7: Esta es nuestra ventana, ya tenemos la directiva creada

Especificaremos que no utilice tunel, un tunel une dos redes separadas por Internet o otra red que haya de por medio, mediante un protocolo de seguridad como IPSec.

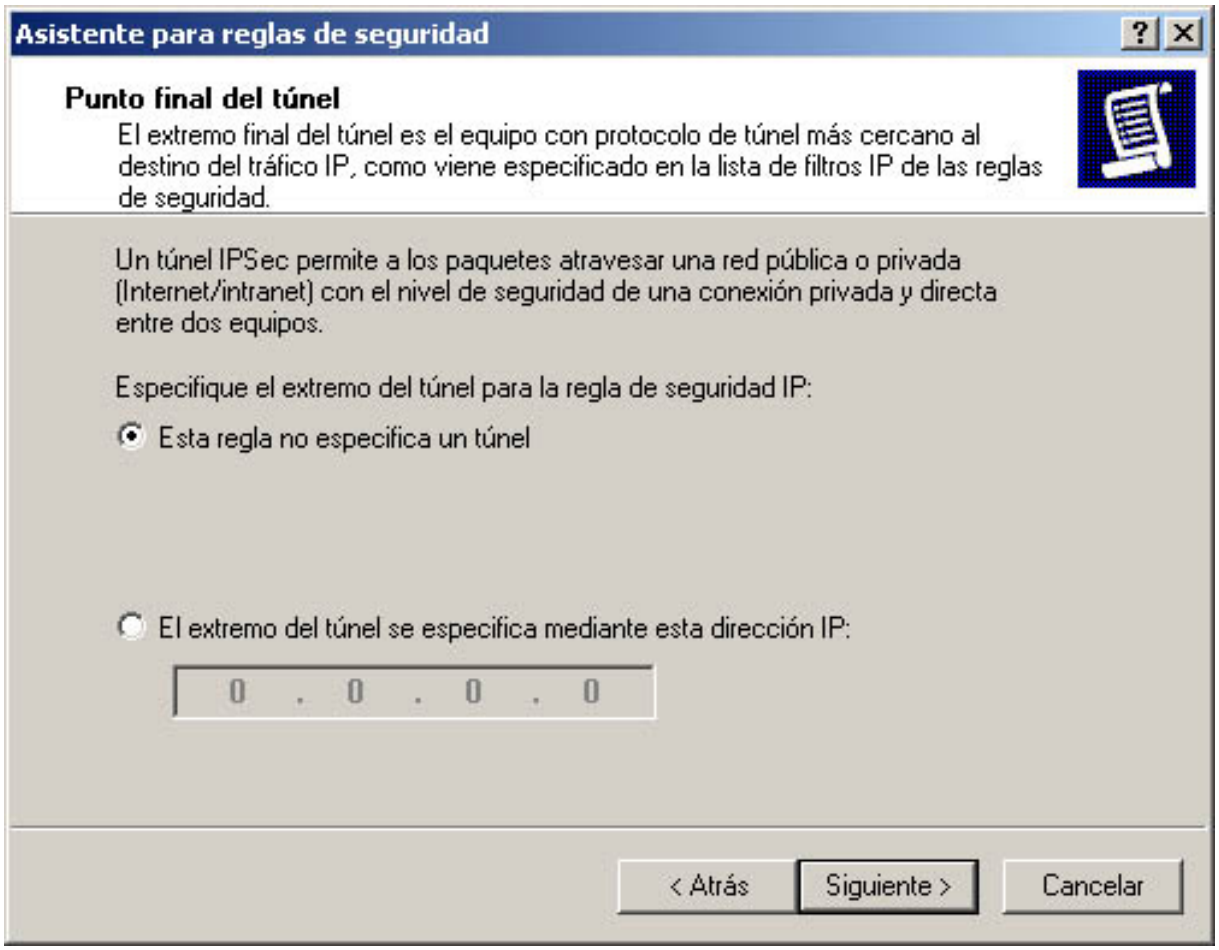

Figura 8: No especificaremos un tunel.

Si disponemos de una red interna, deberemos luego crear una regla que permita a la red Interna que tiene un rango de IPs poder acceder a nuestro equipo.

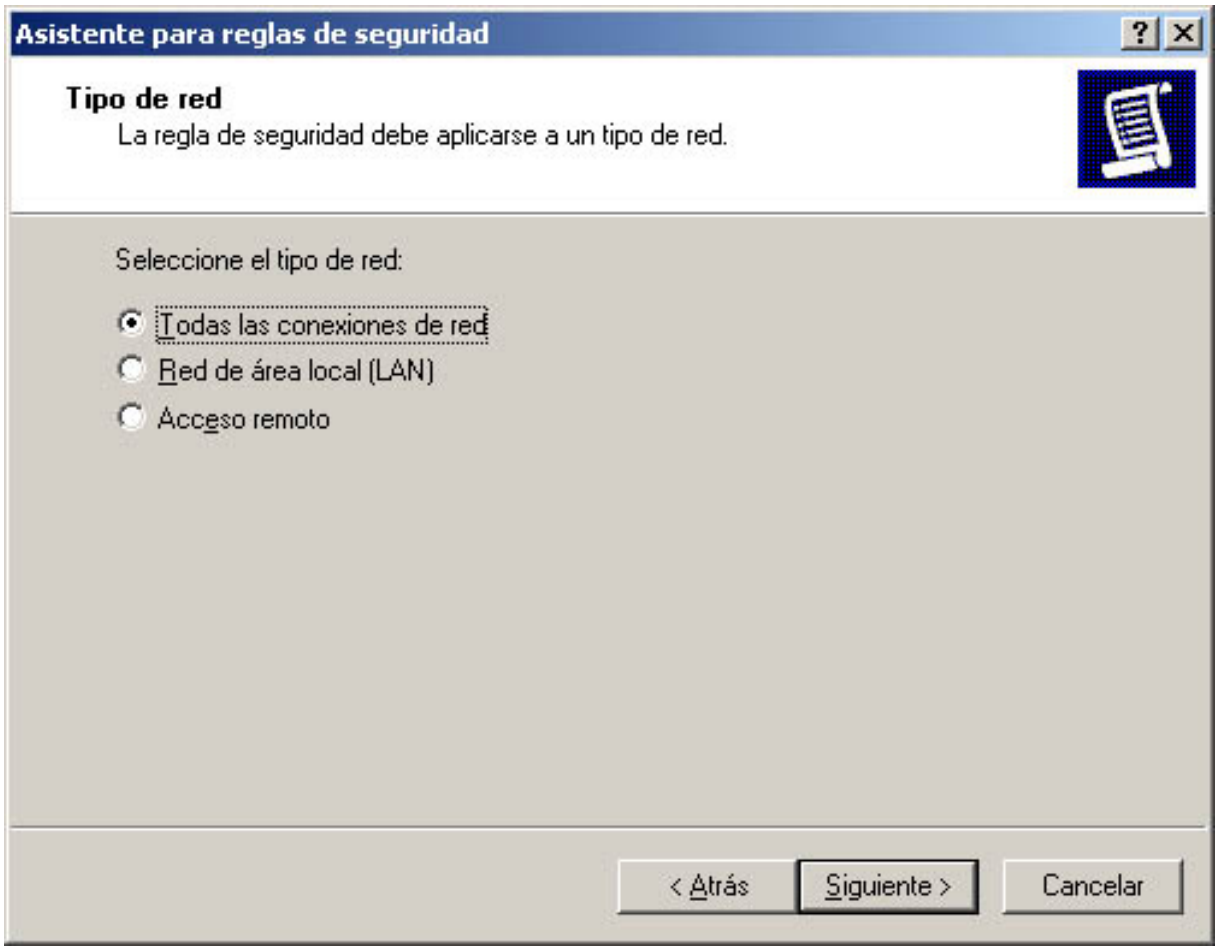

Figura 9: Por defecto pondremos Todas las conexiones de red.

Para Crear nuevos Filtros le damos a aceptar.

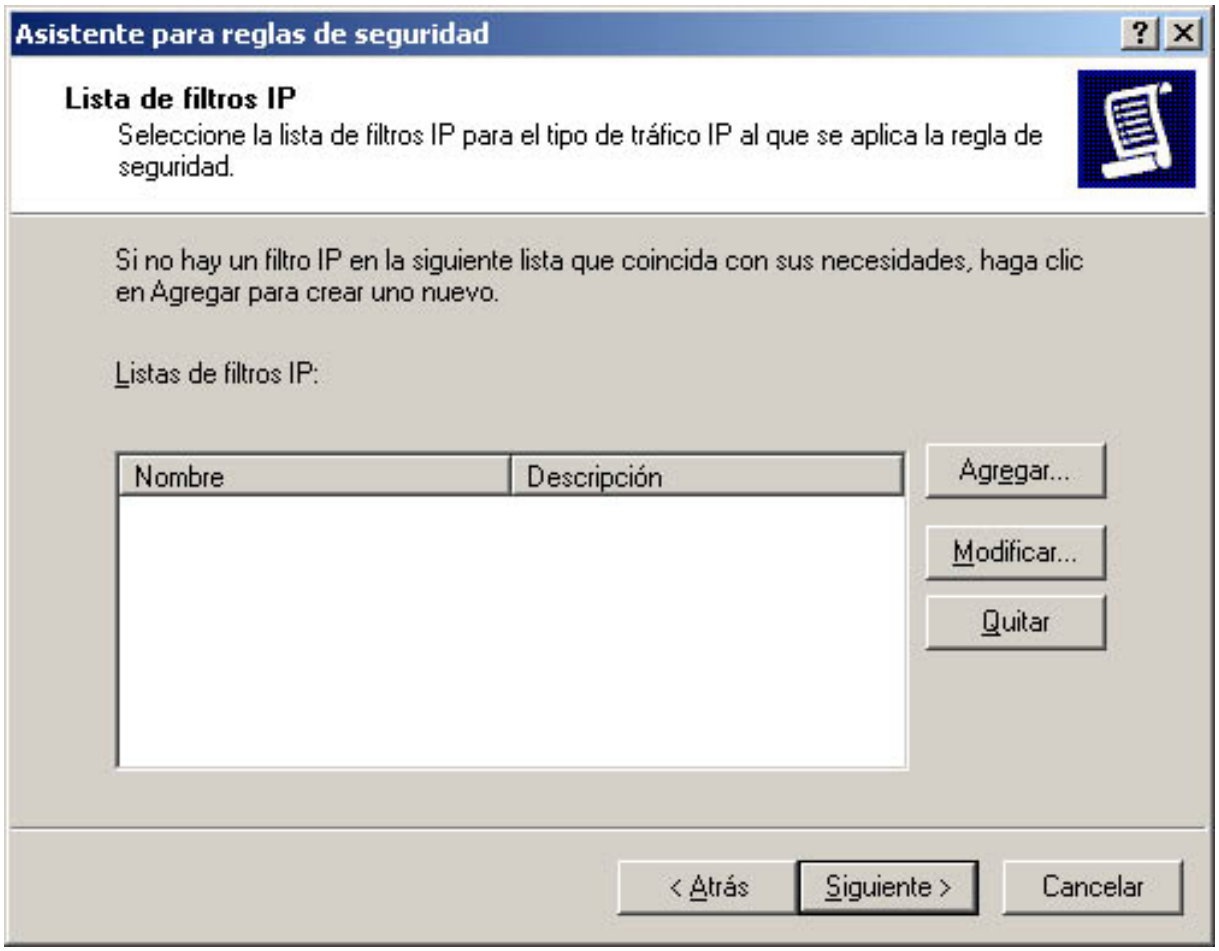

Figura 10: La lista de Filtros IP está vacia hay que crear nuevos.

Podemos tener varios filtros que engloben a varios puertos o bien, separandolos por protocolos. Sencillamente con esto podemos tener mejor organizada nuestros filtros. Pero por ejemplo en vez de no dejar, podíamos haberle puesto *No Dejar TCP* y meter todos los filtros de ese protocolo, y otro para el UDP.

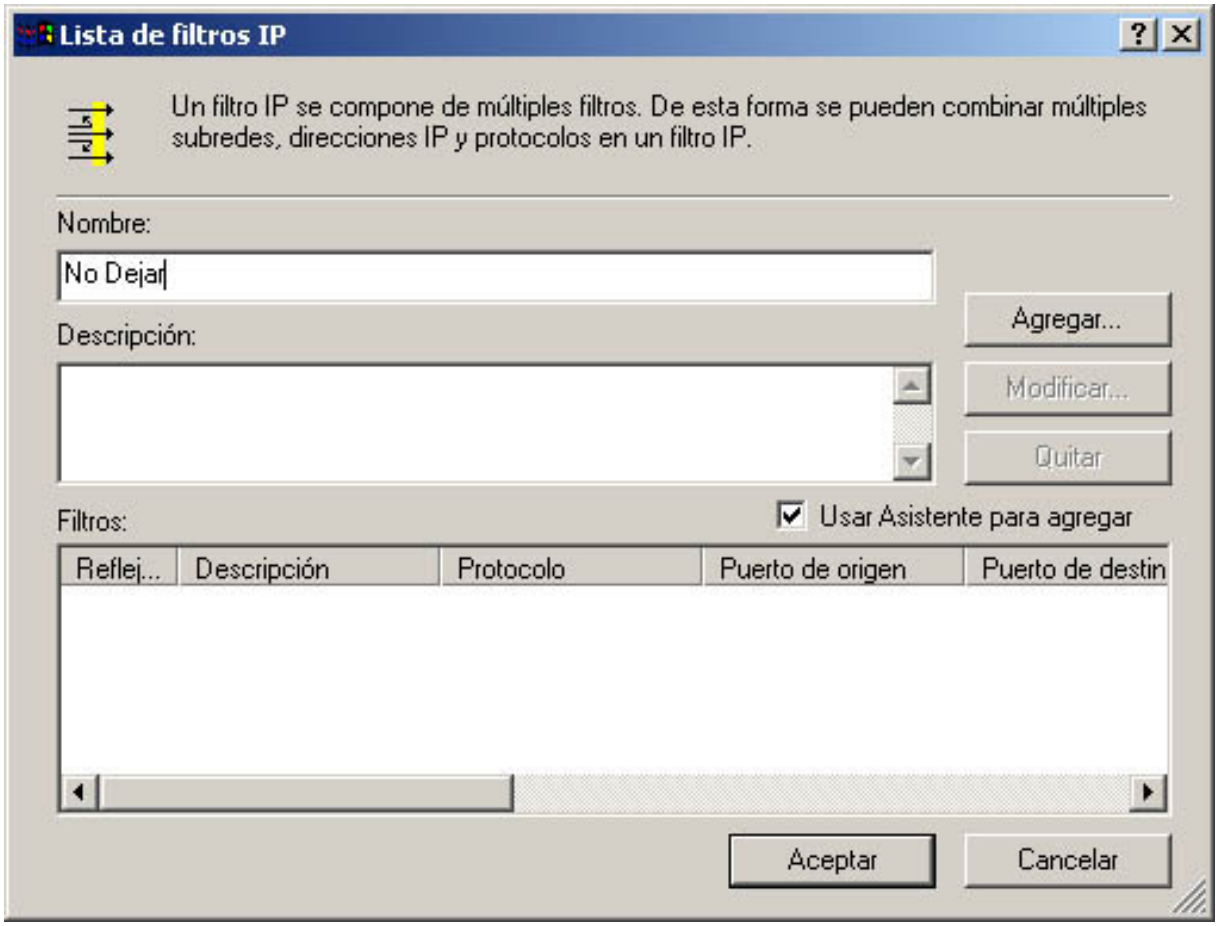

Figura 11: Le ponemos un nombre a nuestro filtro, por ejemplo No Dejar.

Como he dicho es mejor separar los protocolos en diferentes filtros por el hecho de que se han de añadir uno por uno y puede ser algo tedioso

Aquí conviene tener unas nociones básicas de internet. Una dirección IP es un numero identificativo que tiene cualquier ordenador conectado a internet. Es lo que nos identifica en Internet, si bien una IP puede ser fija o variable, dependiendo de nuestra conexión o como lo tengamos contratado.

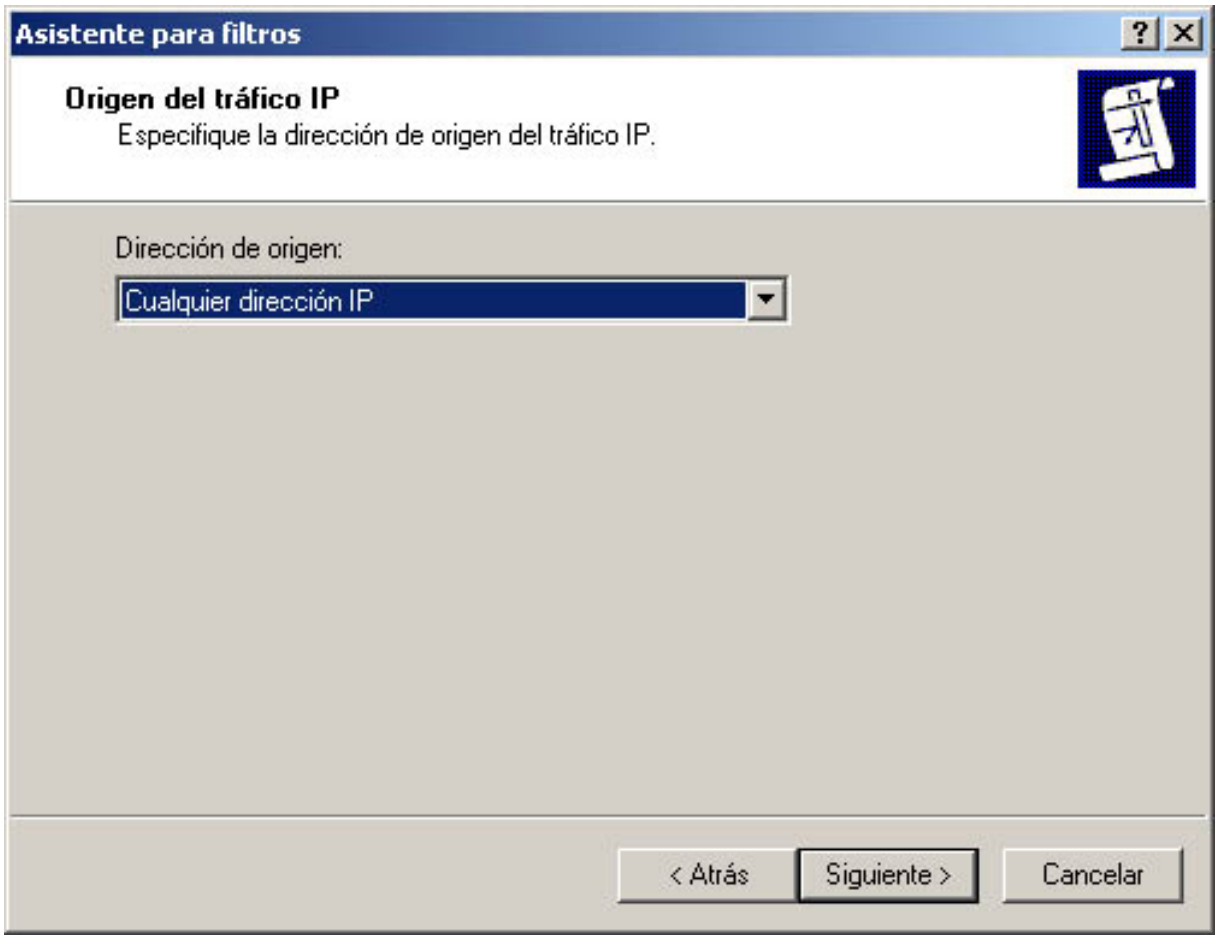

Figura 12: El origen Cualquier Direccion IP.

Para iniciar conexiones, una máquina es la que inicia la conexión, el origen. Expecificando cualquier dirección IP, estamos diciendo que puede ser cualquier ordenador de internet. En realidad especificamos la mascara 0.0.0.0 con esto se dice que puede ser cualquier ordenador.

El destino es el ordenador al cual va dirigida esa conexión. Este va a ser nuestro ordenador y la ip que tendra puede ser la nuestra, la que tenga nuestro ordenador.

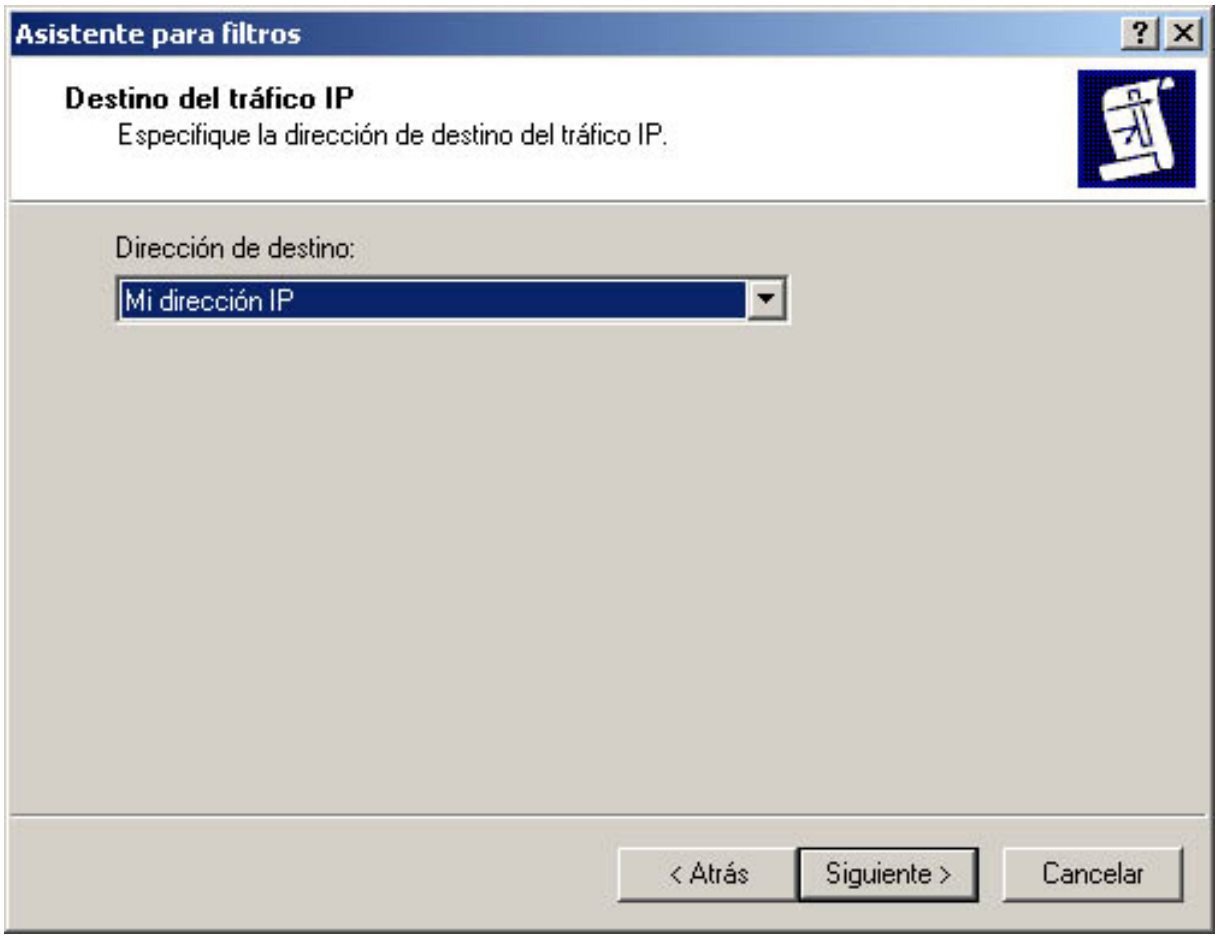

Figura 13: El destino Mi Dirección IP.

Puede que tengamos varias Interfaces de red o varias direcciones IP, aunque no las sepamos se aplicará a todas las direcciones IP que posea nuestra maquina, excepto la loopback [1]

[1]Loopback o la IP 127.0.0.1, es la dirección que tienen todos los ordenadores con si mismos y sólo ellos mismos pueden acceder, se utiliza para pruebas.

El protocolo TCP es un protocolo a nivel de transporte, no comviene confundirlo con los de aplicación por ejemplo, pop, http, smtp... Los de aplicación vienen definidos por un puerto.

Figura 14: Protocolo TCP

Aqui algunos protocolos a nivel de aplicación que utilizan TCP y sus puertos:

Nombre	**Explicación**	**Puerto**
FTP	Transferencia de Ficheros	21
SMTP	Envio de correo	25
HTTP	Web, páginas web	80
POP	Recepción de correo	110
IRC	Chat	6667

Estos son algunos de los mas utilizados del protocolo de transporte TCP.

Este puerto es el que usa una aplicación, un servicio que permite el acceso a recursos o información de nuestro sistema. El puerto 137 lo utiliza windows para los nombres de NetBIOS, es un protocolo de aplicación [2] utilizado por windows para cambiar ficheros. Piense que mientras mas bloquee un sistema mas difícil sera que puedan accederle, pero también piense que pierde desempeño en las labores que puede usted realizar.

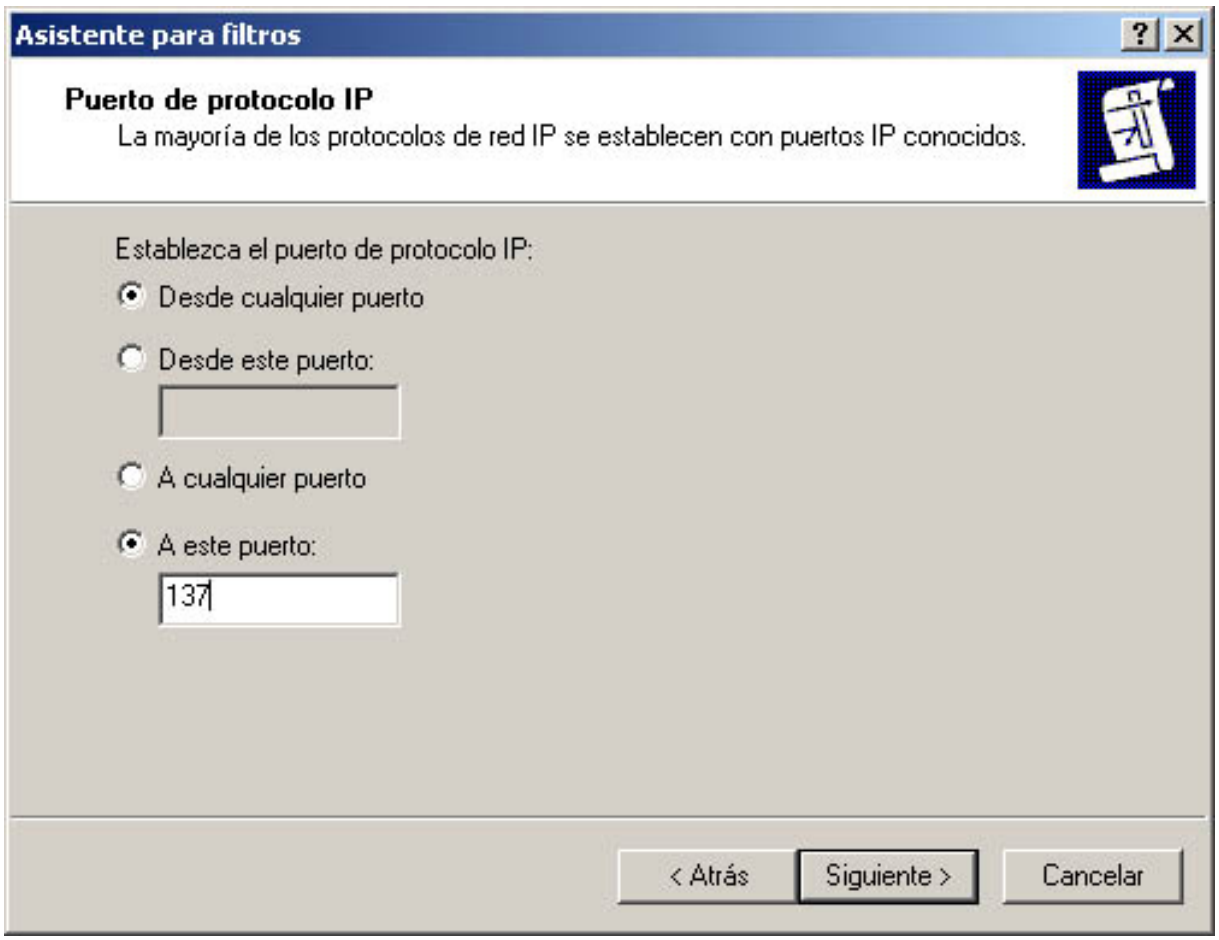

Figura 15: El puerto de Destino 137.

Puede que piense que puede tener un puerto activo y puede que no le soliciten información o aun asi que no puedan acceder, es una forma de pensar pero también existe la posibilidad de que se descubra un fallo que mandando una determinada petición cause el cuelge del sistema o el uso de todos sus recursos.

[2] Cada protocolo de aplicación tiene asignado un puerto, por ejemplo el 80 el web, o el 25 smtp (correo)

Ya tenemos el filtro creado, ahora debemos verificar las propiedades o agregar otro filtro adicional, por ejemplo agregando otro puerto el cual bloquear.

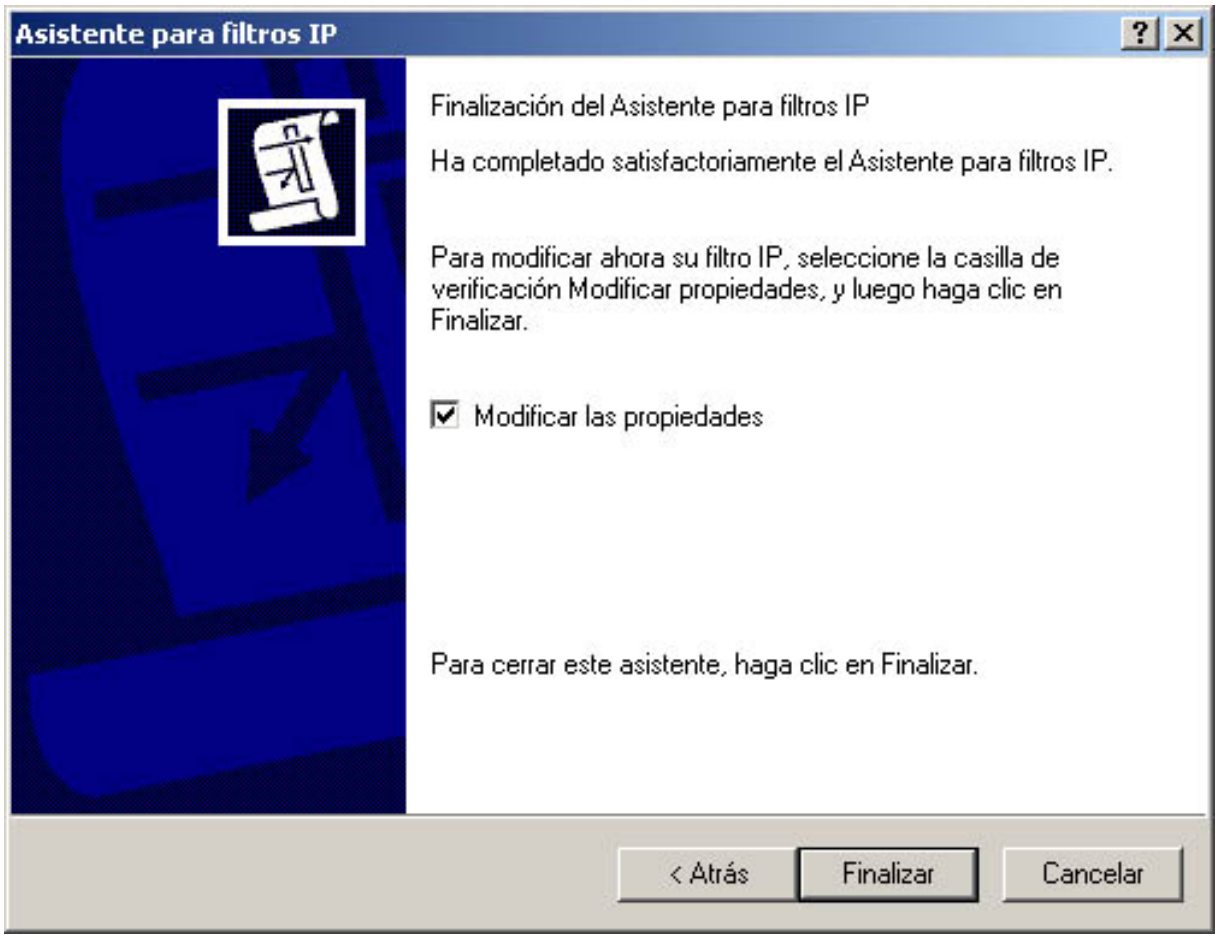

Figura 16: Verificamos las propiedades de nuestro filtro

Si bien esta creado, con esto no es sufuciente, debemos saber que hacer con estos filtros, en los siguientes pasos se explicará como crear politicas para estos tipos de filtros, es decir que vamos a hacer cuando nos llege una petición para esa conexión *aceptarla, denegarla, pedir permiso* esta útima puede ser demasiado cargante si por ejemplo se recibe un ataque. Por nuestro bien lo bloquearemos, esto quiere decir que el que manda la respuesta, no recibirá ninguna respuesta.

Cabe destacar la opción de **Reflejado**, sirve para cuando queremos aplicar la regla a la inversa, ademas se utiliza la regla inversa, cambiando origen y destino, esto por ejemplo es util por si algun virus o alquien con un troyano intenta montar unidades remotas.

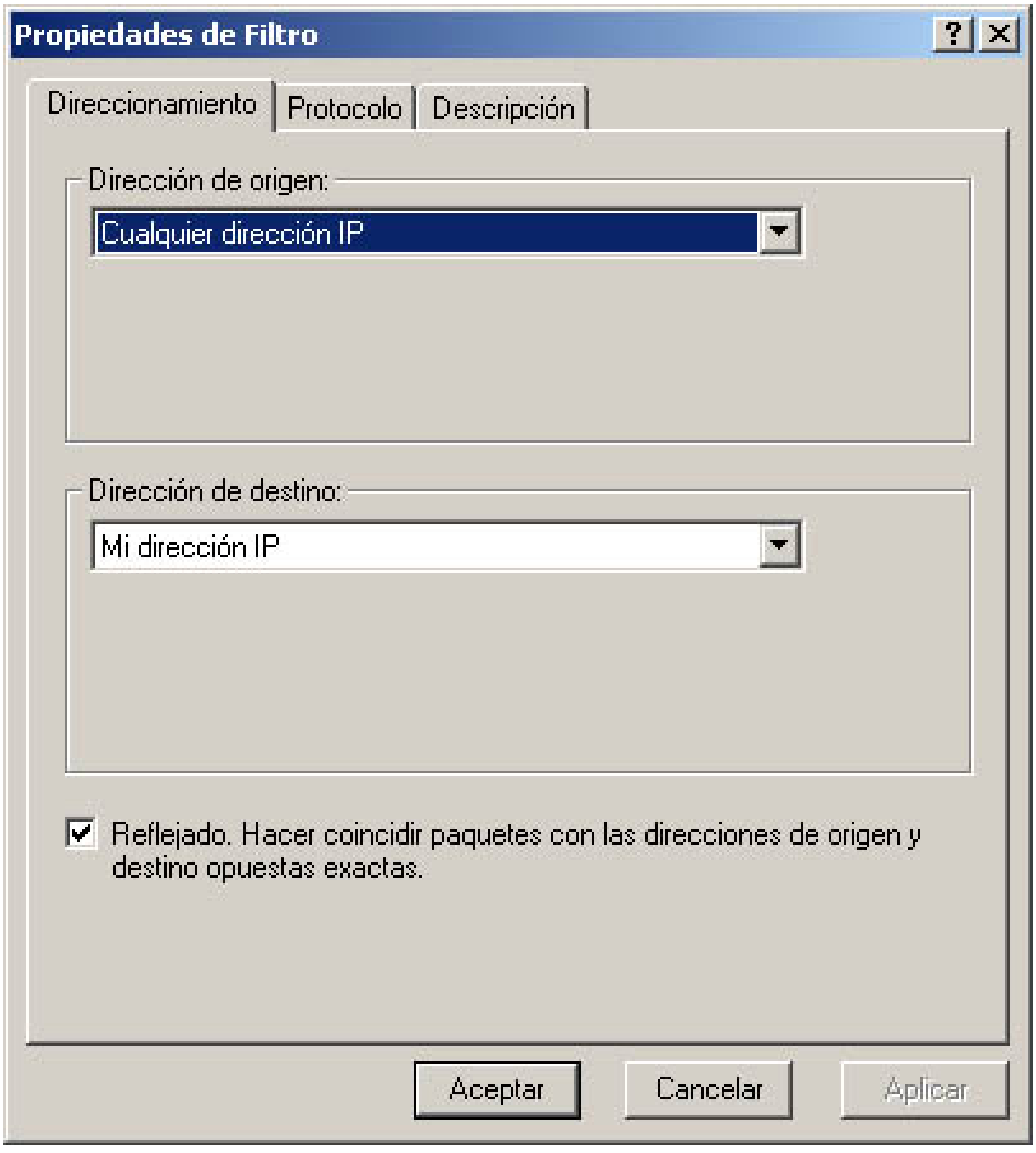

Figura 17: Reflejado sirve para crear directivas opuestas.

Por ejemplo si bloquease a partir de su dirección IP el puerto 80, y estubiese reflejado, usted no podría navegar, en cambio si no lo pone reflejado podrá navegar sin problemas, haga la prueba.

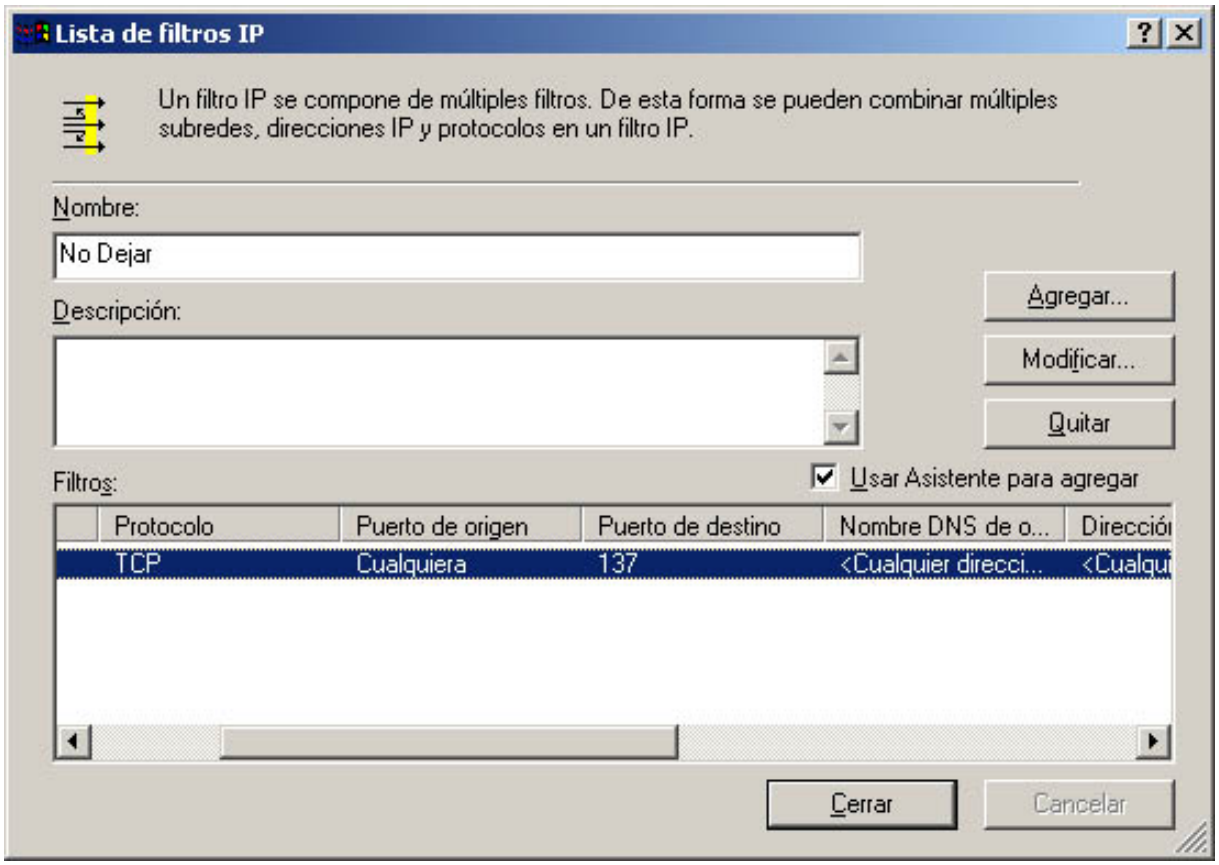

Figura 18: Ventana de nuestro filtro No Dejar y los puertos afectados.

Utilizaremos otro asistente para aplicar las reglas, sin los asistente la labor sería mas tediosa. O por lo menos mas difícil de entender.

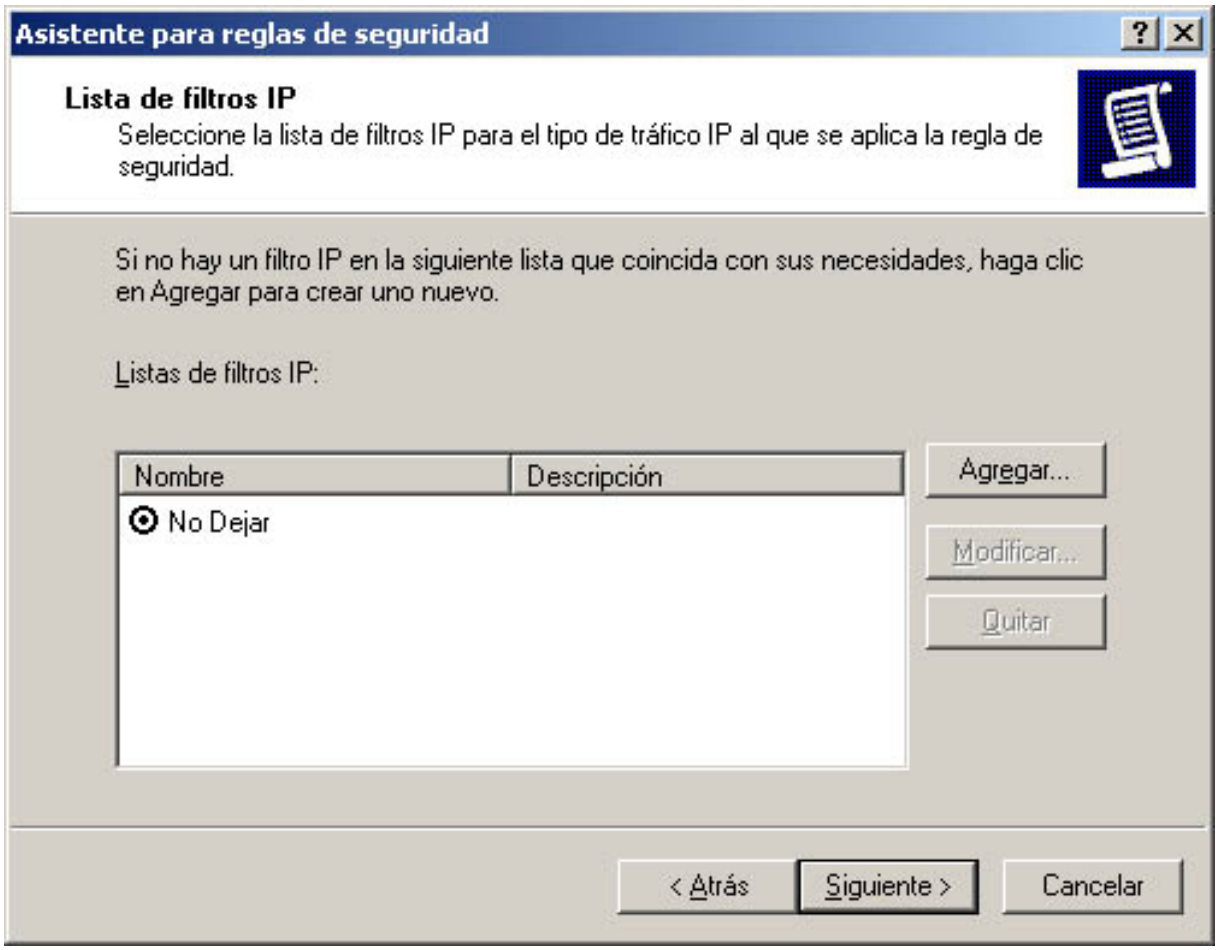

Figura 19: Asistente para reglas a aplicar.

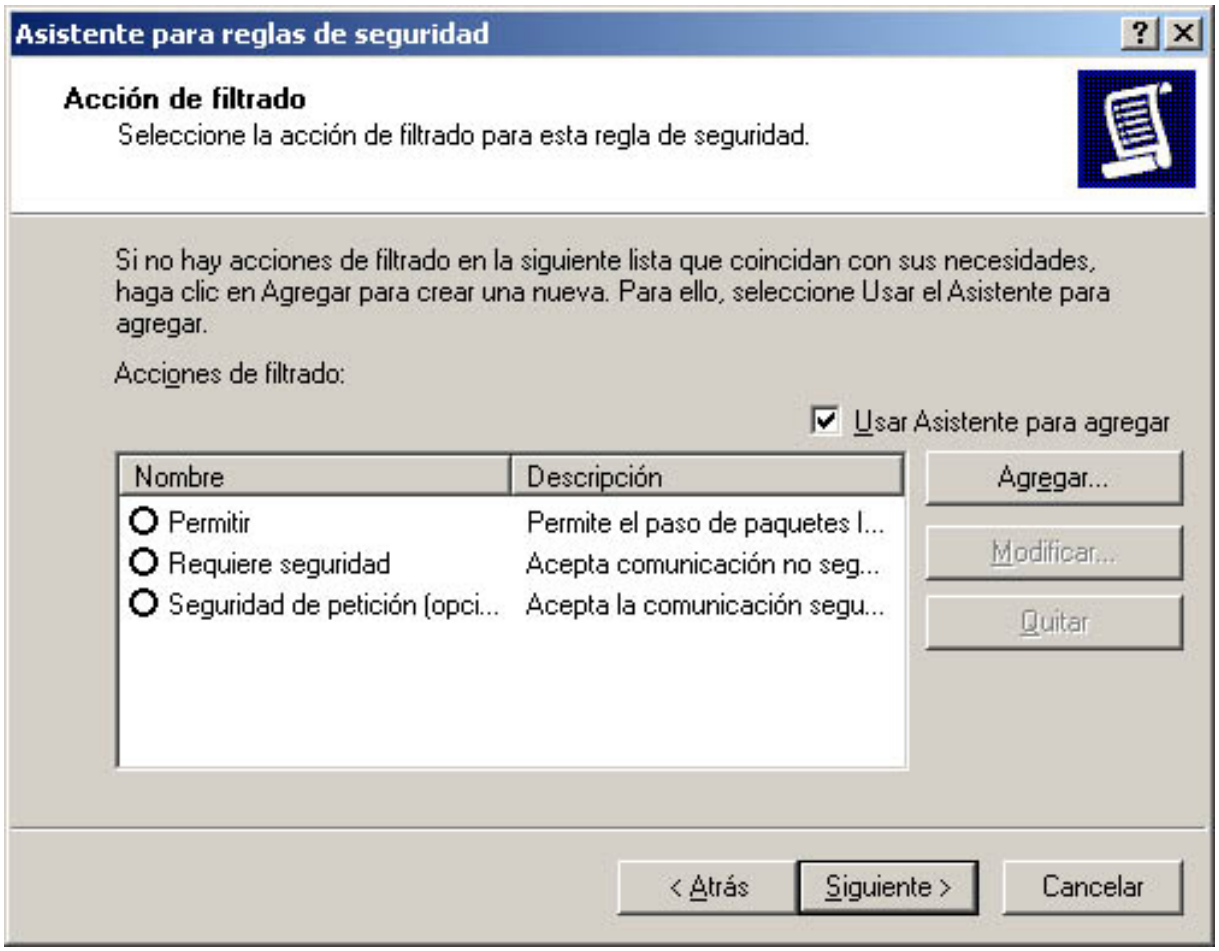

Figura 20: La acción de Filtrado decide que hacer con la directiva de seguridad creada.

Utilizaremos el asistente para crear una nueva acción de filtrado y le damos a Aceptar. Ya que la que nos interesa no esta creada.

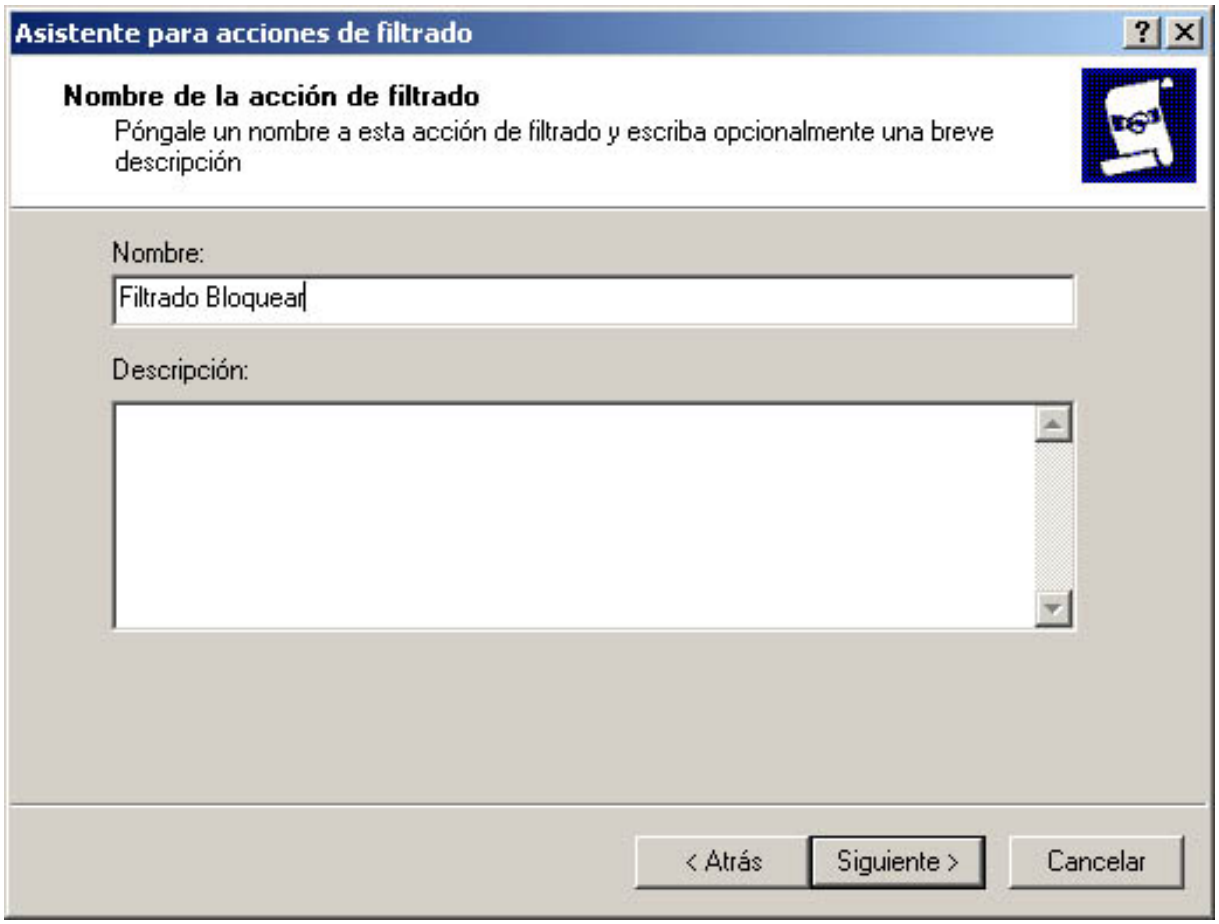

Figura 21: Asignamos un nombre a la acción de filtrado..

Que va a ser la que nos permita bloquear.

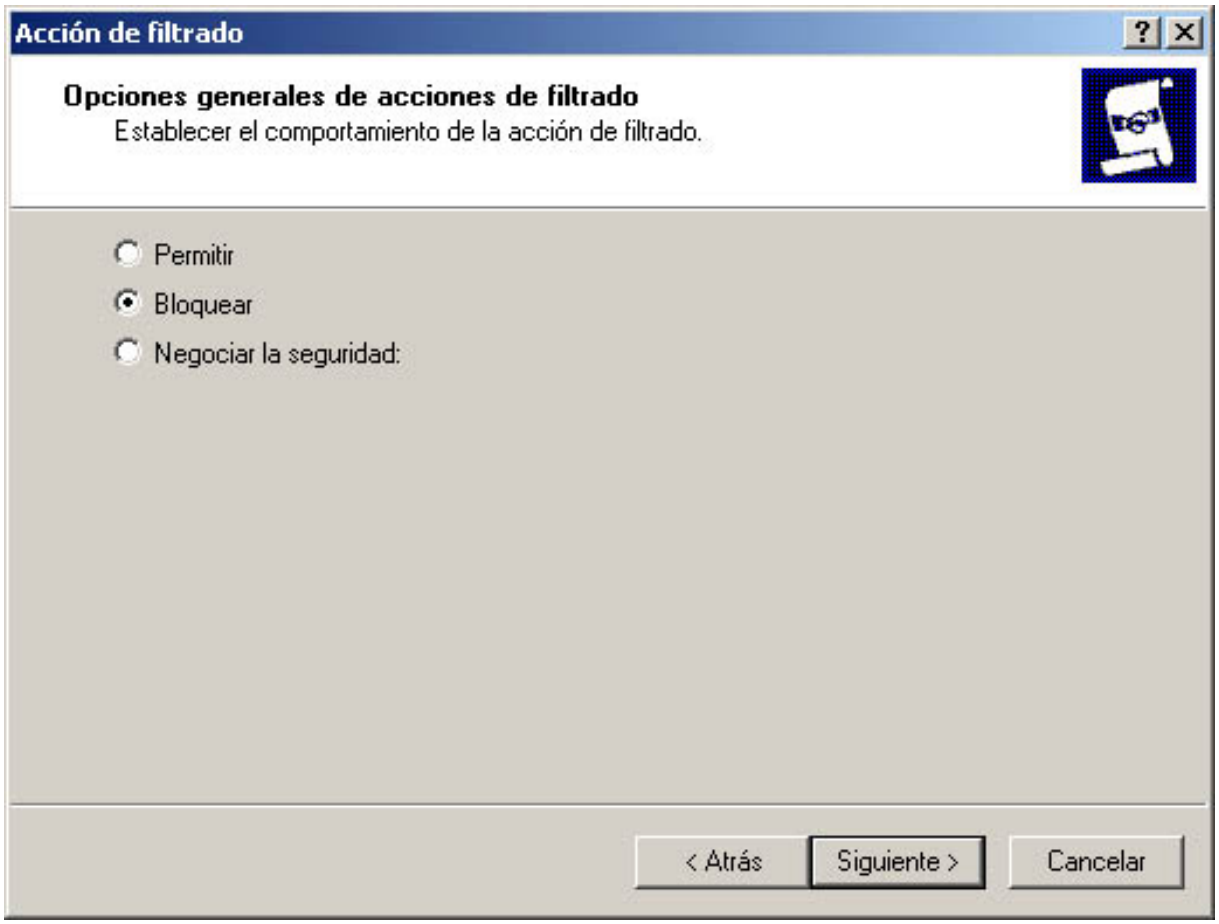

Figura 22: Seleccionamos Bloquear.

Asi lo que hará esta acción es bloquear las conexiones, impedir que se realicen.

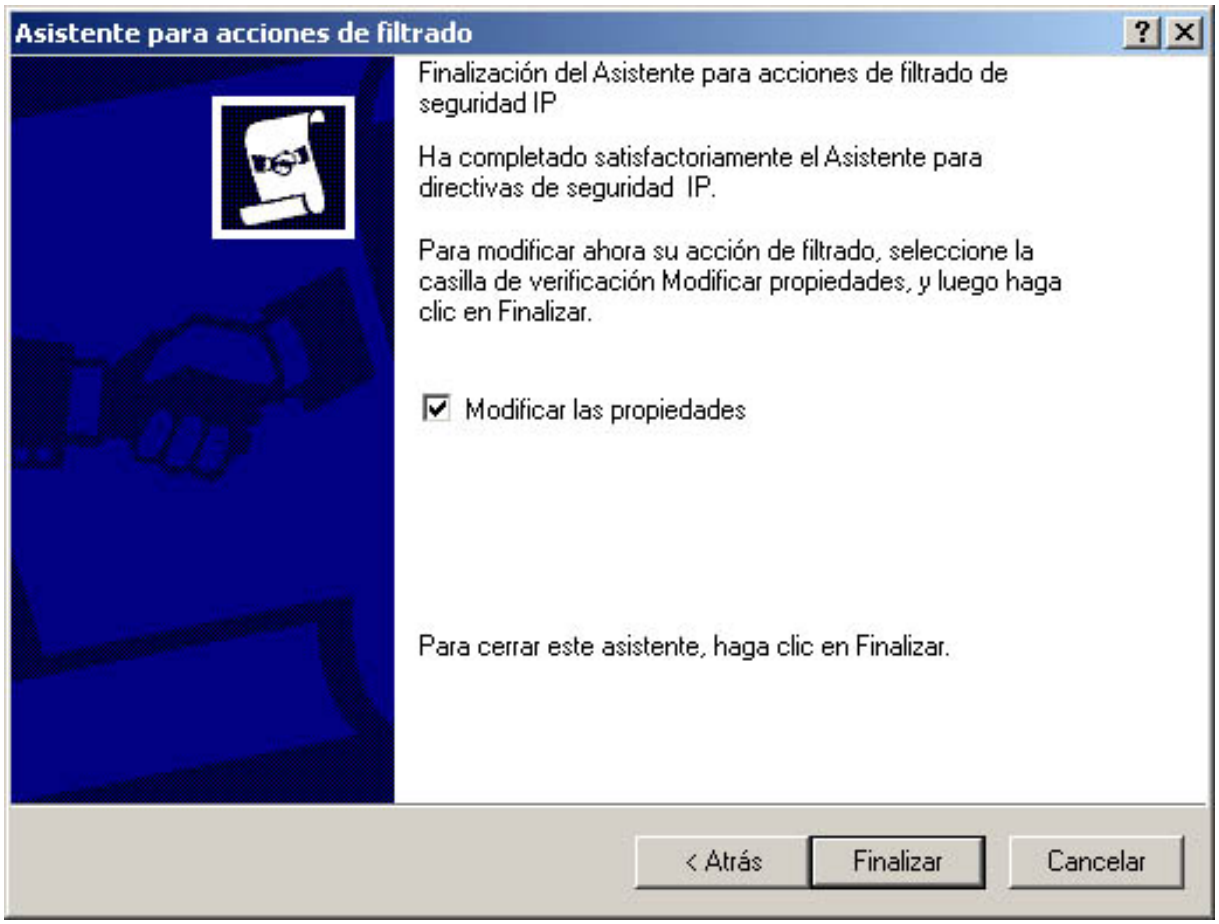

Figura 23: Ya tenemos nuestra acción de filtrado creada.

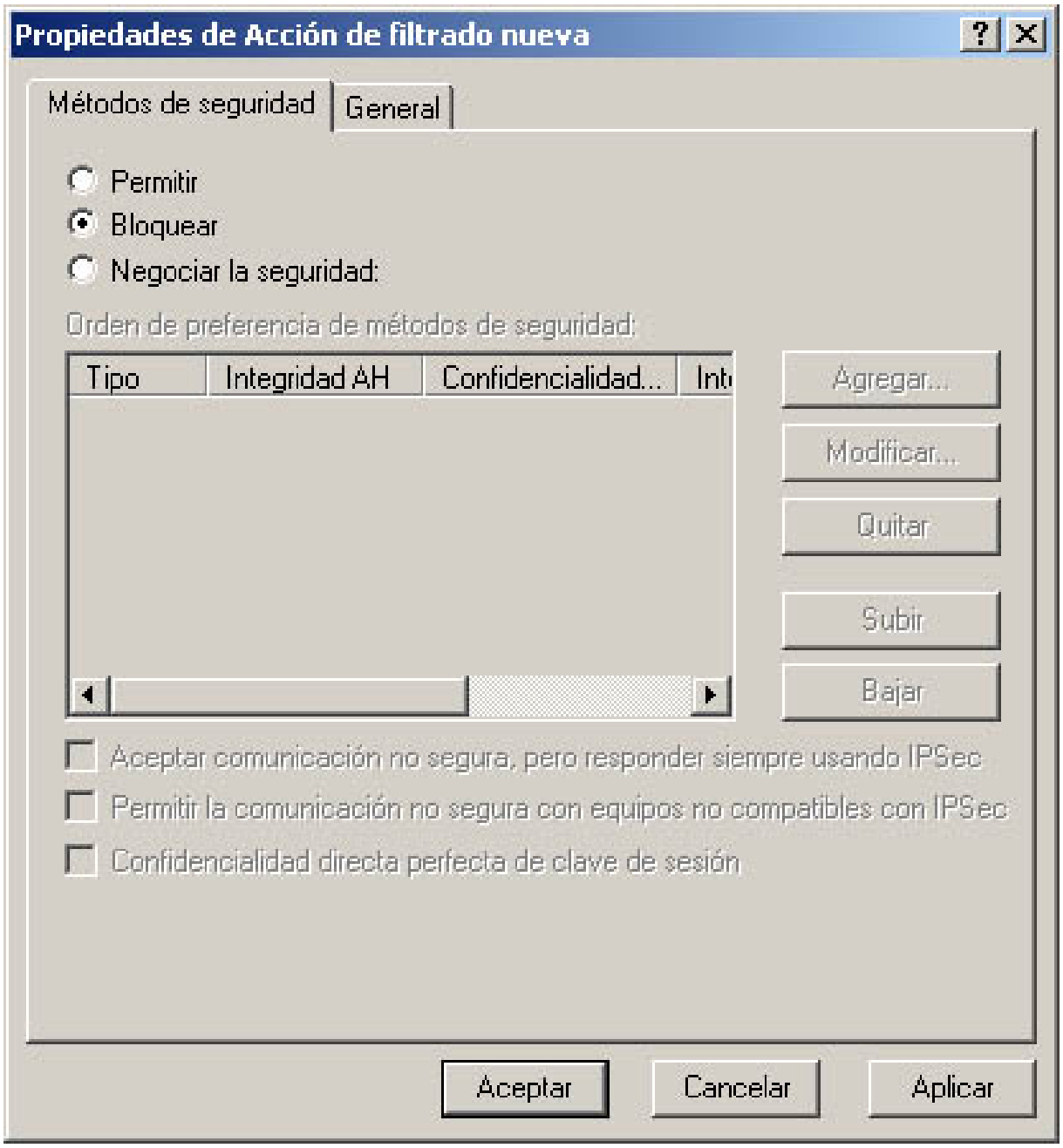

Figura 24: Dejamos tal como esta.

Como puede verse, si hubiesemos seleccionado otra como, pedir seguridad podemos habilitar mas opciones, sólo si utilizamos ciertas directivas de seguridad que se requieran.

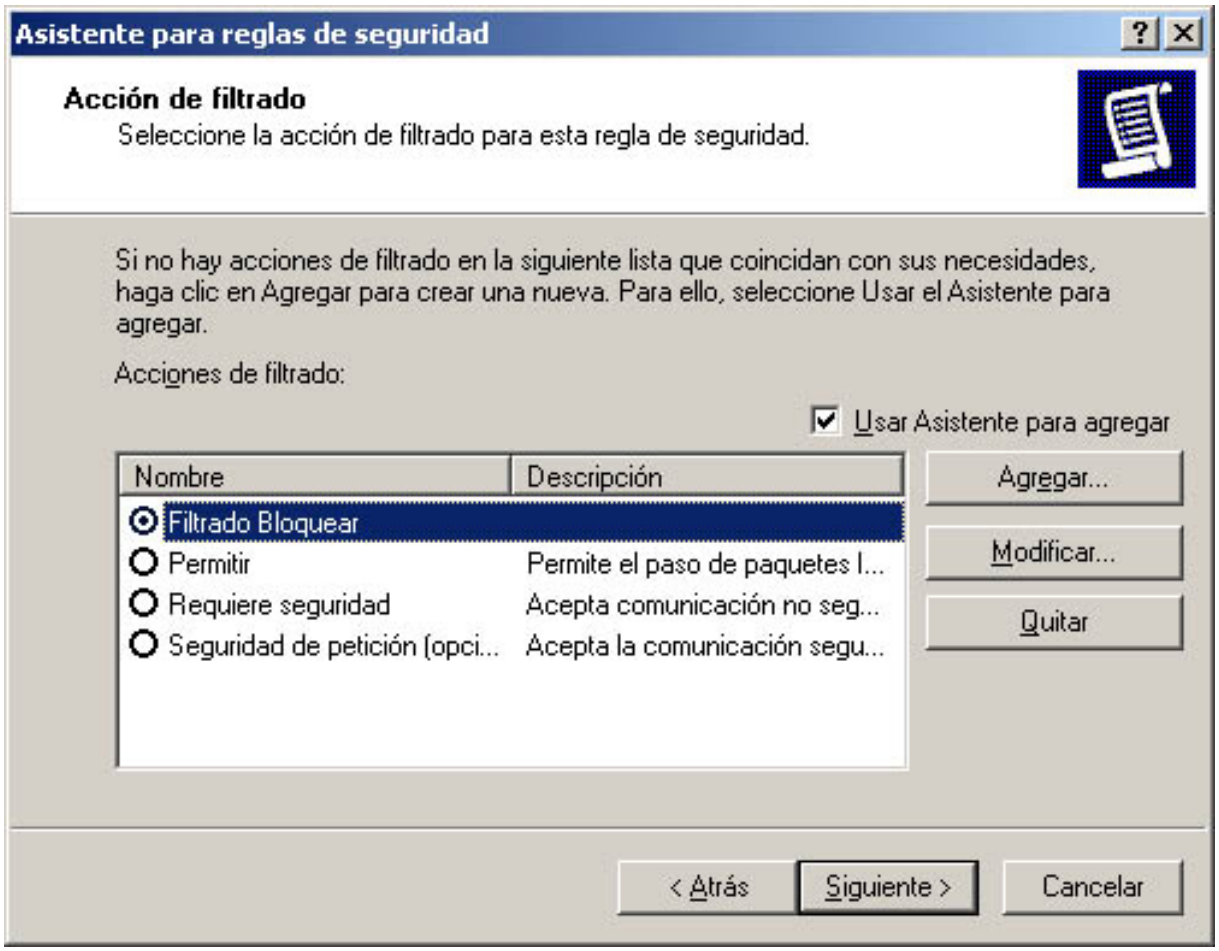

Figura 25: Seleccionamos la acción de Filtrado que para aplicar la regla No Dejar.

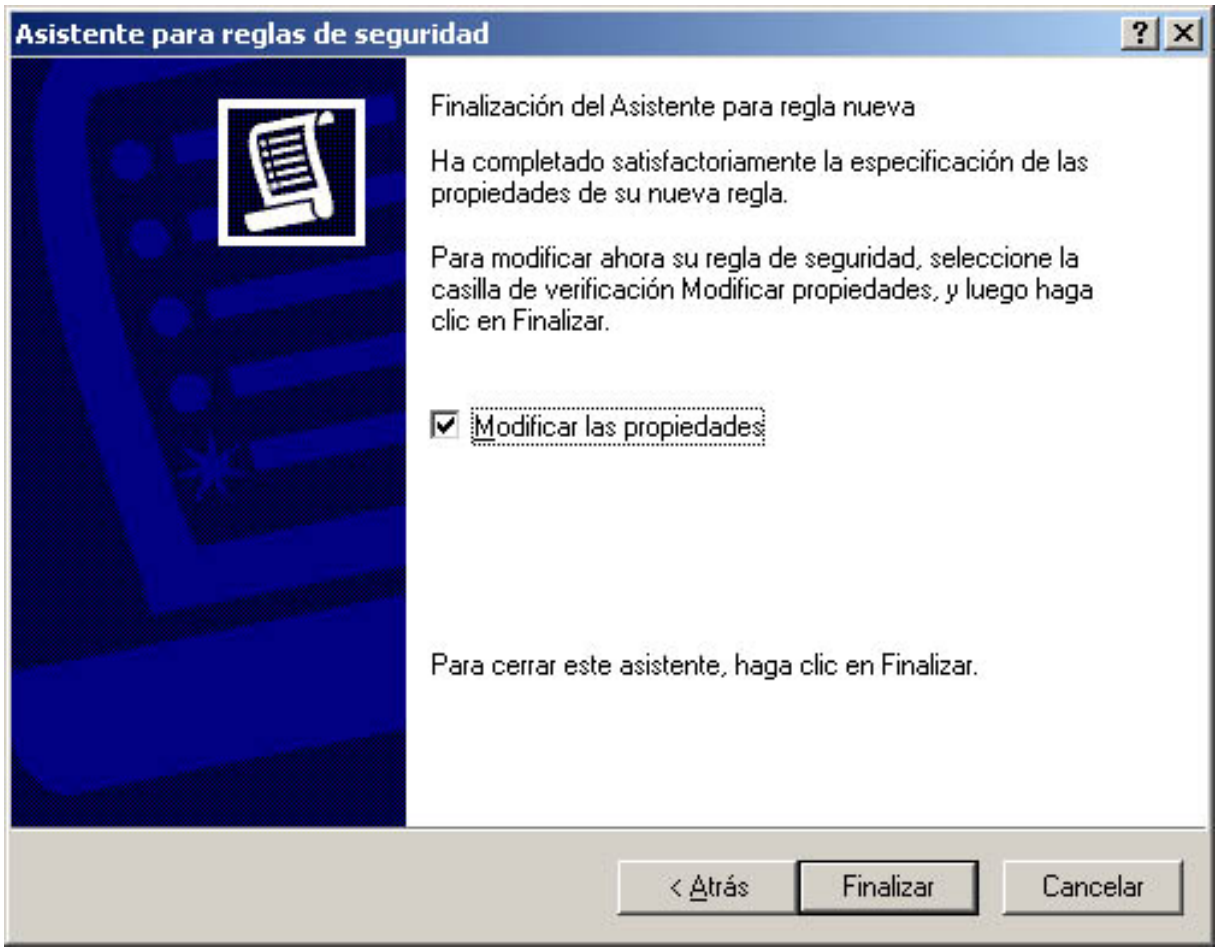

Figura 26: Y volvemos a lo mismo de antes.

Podemos crear reglas para separar los puertos, por ejemplo del tipo de protocolo TCP o UDP, en vez de tenerlas todas juntas.

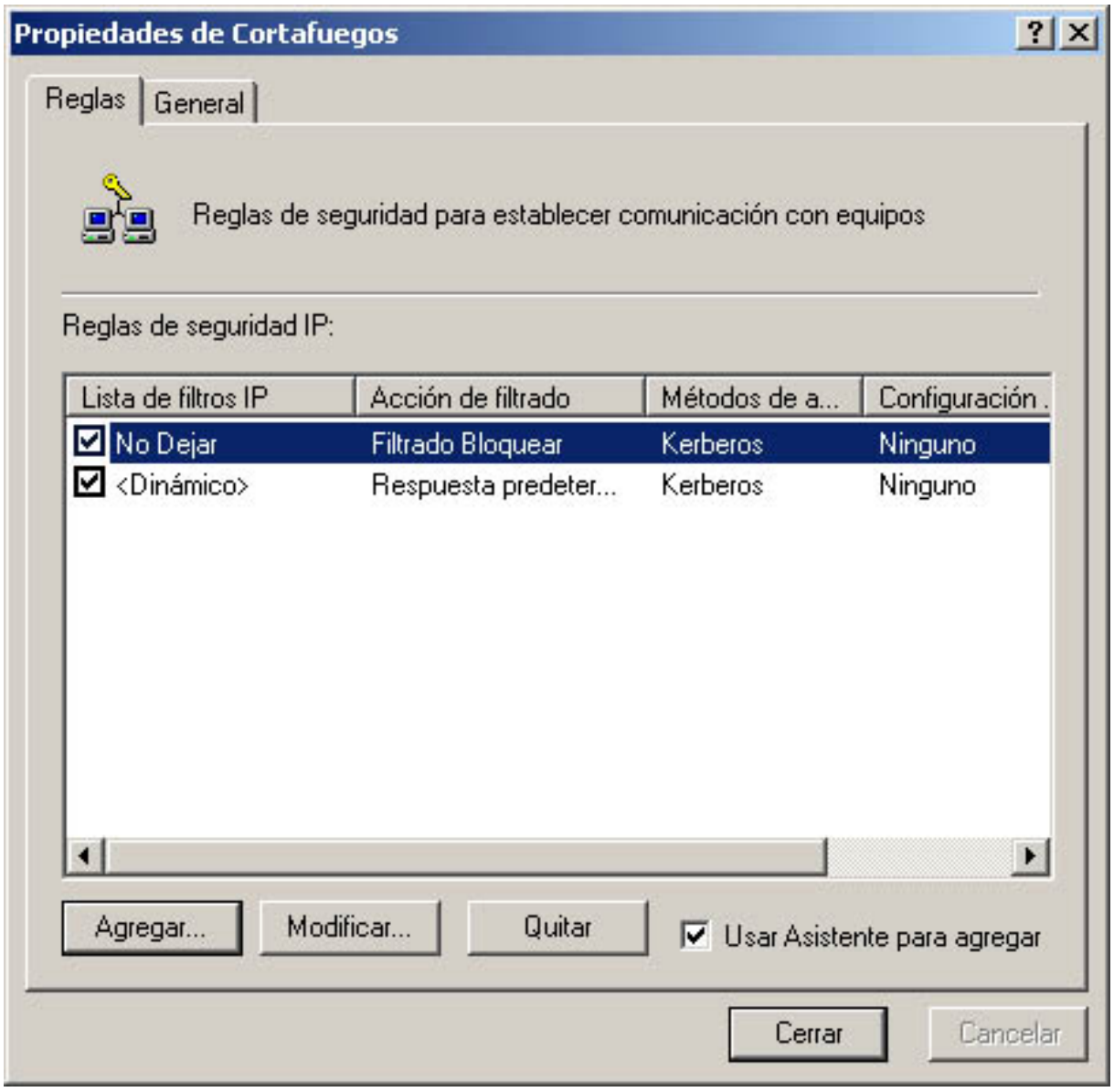

Figura 27: Si tenemos seleccionada nuestra regla, el cortafuegos esta listo

Le damos a Cerrar, el siguiente paso será activar la Directiva de Seguridad creada.

Como mencione anteriormente es conveniente crear varias reglas de filtrado basándose en los tipos de protocolo de aplicación (los puertos)

Sino activamos la regla creada de Cortafuegos, es como si no hubiésemos hecho nada, para ello seleccionarla y darle o bien al icono del interruptor o bien con el botón derecho en asignar.

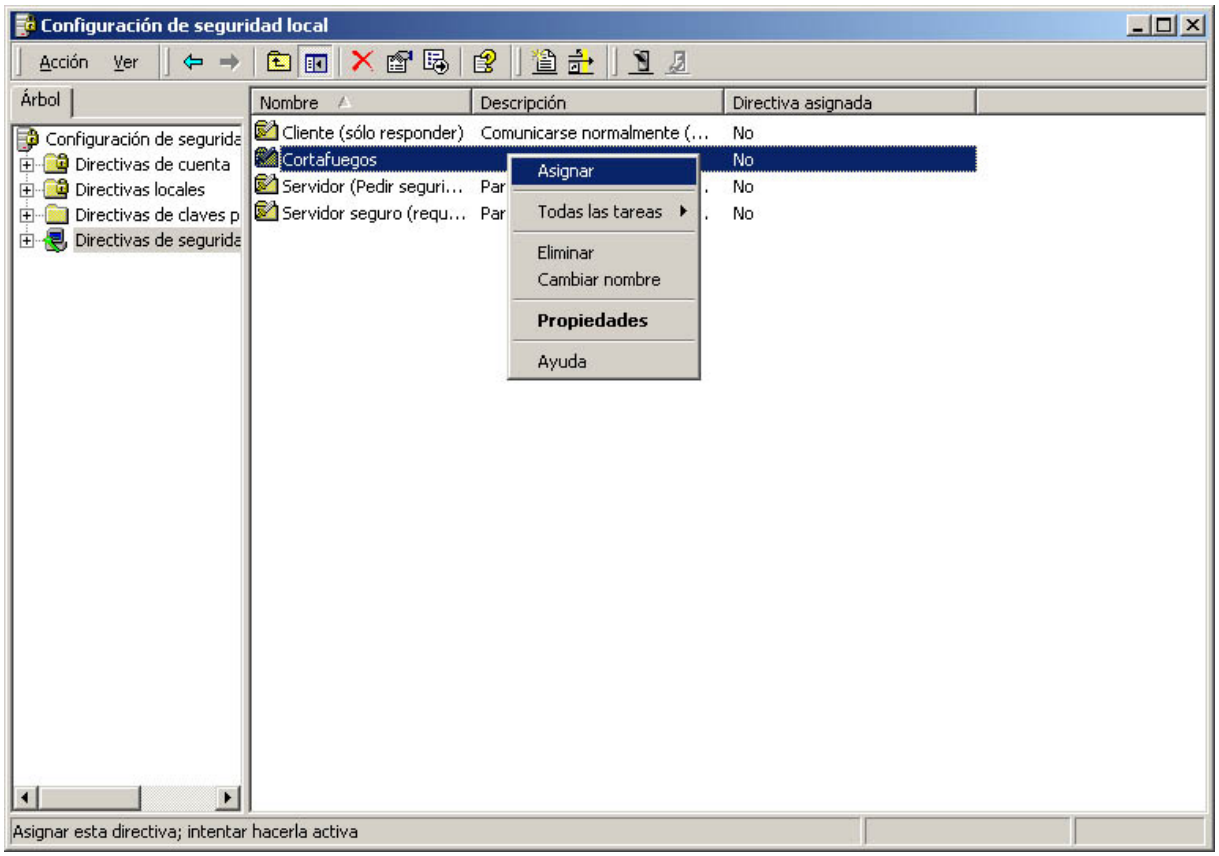

Figura 28: Asignado la directiva de seguridad, activaremos todas las reglas antes creadas

Aquí teneis unos cuantos puertos y protocolos que recomiendo que chapeis, para impedir que os causen daño o os accedan sin permiso.

Nombre	**Tipo**	**Puerto**	**Protocolo**
Netbios (RPC)	Windows	135	TCP / UDP
Netbios Nombre	Windows	137	TCP / UDP
Netbios Datagrama	Windows	138	TCP / UDP
Netbios Sesion	Windows	139	TCP / UDP
Microsoft-ds+	Windows	445	TCP / UDP
NetBus	Troyano	12345	TCP
BackOriffice	Troyano	31337	UDP

No obstante vosotros podréis ver que puertos tenéis activos, es decir os pueden acceder desde el exterior. Para esto existe un comando que dice que puertos están activos... basta con ejecutar:

Inicio → Ejecutar → cmd

Una vez dentro del intérprete simplemente:

netstat -an

Existe un listado extenso de puertos, definidos por la IANA, esto es una descripción de TODOS, pongo la referencia a título ilustrativo para que veáis la cantidad de puertos que existen.

Listado Completo de Puertos

Revisado a 11 de Julio de 2003. Si encuentra algún fallo o algo no queda lo suficientemente claro, por favor escriba a i72maprj@uco.es