GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN

SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL
INSTITUTO SUPERIOR DE FORMACIÓN Y RECURSOS EN RED PARA EL PROFESORADO

REDES DE ÁREA LOCAL. APLICACIONES Y SERVICIOS EN WINDOWS

Servicio de aceleración y seguridad en Internet

Formación en Red

Servicio de Aceleración y Seguridad en Internet (ISA)

Definición

Microsoft Internet Security and Acceleration Server (ISA Server) es una aplicación que puede ejercer las funciones de cortafuegos, proxy-caché y servidor VPN, diseñada para hacer más segura la publicación en Internet de servidores web, servidores de correo electrónico, etc.

Entre otras funciones, mediante "ISA Server 2004" podremos:

- Gestionar y configurar de modo preciso las comunicaciones de salida de nuestra red hacia Internet.
- Gestionar y configurar de modo preciso las comunicaciones de entrada a nuestra red desde Internet.
- Gestionar y configurar de modo preciso la caché inteligente y la caché planificada, así como realizar las funciones de proxy-caché y reverse proxy.
- Realizar la función de servidor VPN para el acceso desde Internet de usuarios remotos a la red de nuestra organización.

La aplicación "ISA Server 2004" dispone de destacadas características de seguridad que permiten realizar una inspección de paquetes a nivel de aplicación de forma dinámica e inteligente, para analizar todo el tráfico que atraviesa dicho cortafuegos o firewall; además "ISA Server 2004" va más allá del simple filtrado de aplicación al controlar el tráfico de cada tipo de aplicación, con filtros específicos que analizan los comandos de la aplicación y los datos, pudiendo dicho tráfico ser aceptado, rechazado, redirigido o modificado de acuerdo con su contenido mediante el filtrado inteligente del tráfico HTTP, FTP, SMTP, POP3, VPN, DNS, etc.

Las organizaciones que dispongan en Internet de servidores web, servidores de correo electrónico, etc. podrán proteger dichos servidores de ataques externos mediante la publicación en servidor seguro, pudiendo utilizar reglas de publicación web para proteger a los servidores web internos para especificar qué máquinas pueden ser accedidas, o pudiendo utilizar reglas de publicación de servidor para proteger a los servidores internos de determinados accesos por parte de usuarios externos.

Además de lo anterior, "ISA Server 2004" permitirá ofrecer acceso remoto de red privada virtual de "Windows Server 2003", soportando accesos seguros mediante VPN para conectar usuarios remotos a las redes corporativas de la organización.

"ISA Server 2004" también ofrece una caché web de alto rendimiento, acelerando el rendimiento para los clientes internos que acceden a servidores web de Internet, así como mejorando el rendimiento de usuarios externos que accedan a contenidos de servidores web

corporativos, pues realiza una gestión de la caché en memoria RAM muy rápida, y una gestión optimizada de la caché en el acceso a disco duro.

La caché de "ISA Server 2004" es una caché inteligente, que permite que los usuarios reciban el contenido web más reciente gracias al proceso de caché proactivo, mediante el cual la aplicación determina automáticamente los sitios web más accedidos y la frecuencia con la que debe refrescarse su contenido, basándose en el tiempo de permanencia en la caché, y recargando automáticamente dichos contenidos web en la caché en momentos de baja actividad del servidor.

También puede ser planificada la descarga de contenidos de sitios web completos siguiendo una planificación temporal, de modo que las descargas planificadas garantizan el acceso al contenido más actual para todos los usuarios, permitiendo además el acceso a dichos contenidos web sin necesidad de ocupar ancho de banda del sistema.

Para concluir, indicar que "ISA Server 2004" se integra perfectamente con Active Directory, y que permite un control de acceso basado en directivas de firewall, pudiendo controlar el acceso de entrada y salida a nivel de usuario, grupo, aplicación, dirección de origen y destino, contenido y planificación temporal, etc.; además los asistentes de directiva de firewall permiten especificar qué sitios y contenidos pueden ser accedidos, si un protocolo concreto es accesible en comunicación entrante o saliente, así como permitir o denegar la comunicación entre direcciones IP específicas, utilizando protocolos y puertos concretos.

Instalación de ISA Server 2004

En este apartado procederemos a la instalación del cortafuegos "ISA Server 2004" en el equipo "SERVIDOR".

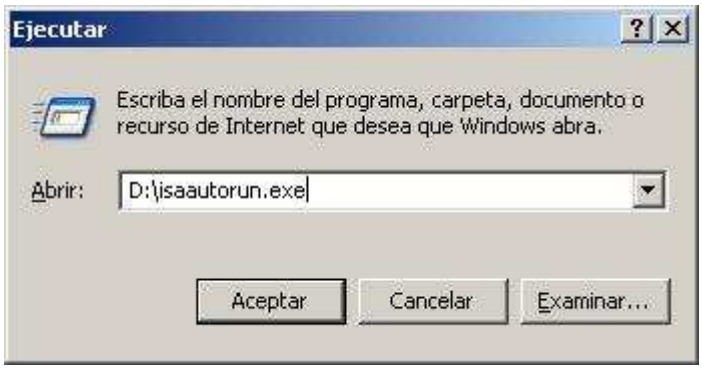
Mediante la aplicación "ISA Server 2004" podremos llevar a cabo un exhaustivo control de los accesos permitidos o denegados desde la red de nuestro centro hacia Internet, así como de los accesos desde Internet a los servidores de nuestro centro; además de lo anterior, esta aplicación nos dotará de un potente proxy y de un servidor VPN que habilitará el acceso de los usuarios deseados a la red de nuestro centro.

A continuación describiremos el proceso preciso para instalar la aplicación "ISA Server 2004" sobre el equipo "SERVIDOR", para lo cual en primer lugar deberemos introducir el CD de dicha aplicación en la unidad correspondiente del equipo "SERVIDOR".

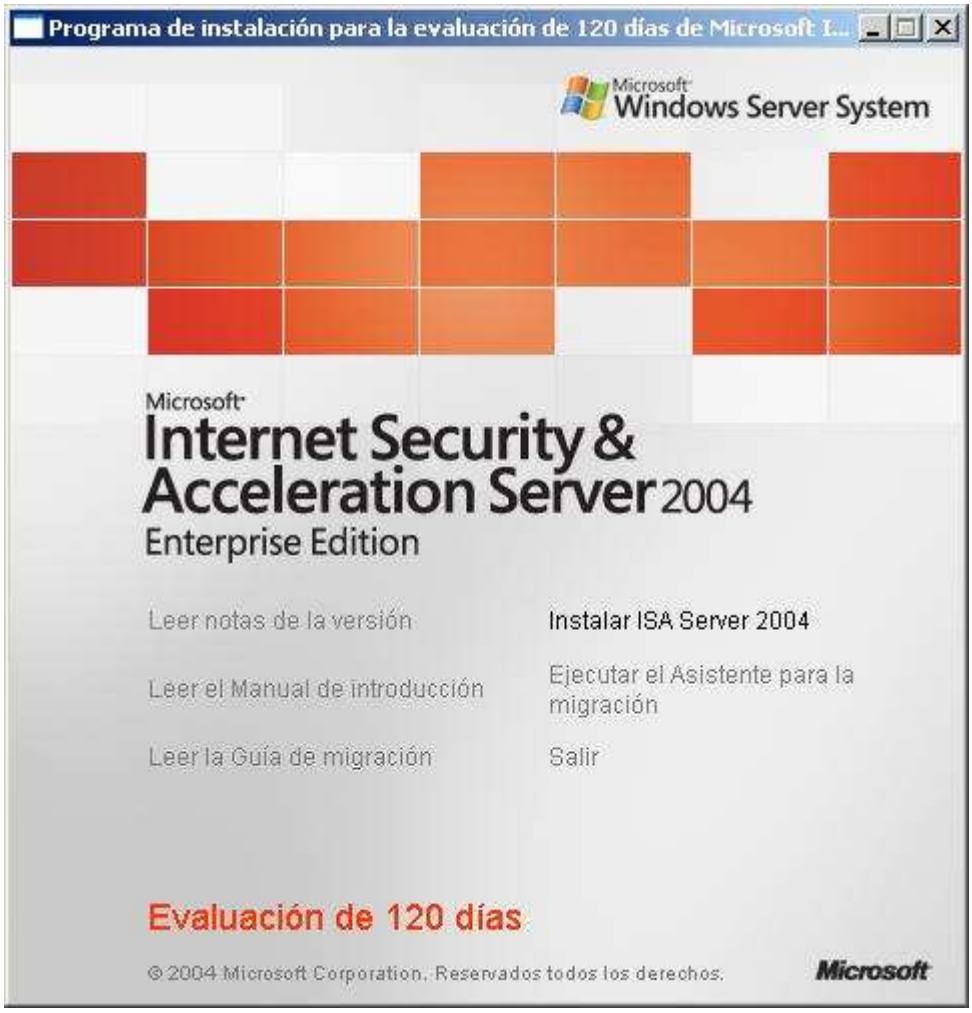
NOTA: Existen dos versiones de "ISA Server 2004", la versión "Enterprise" y la "Standard", pudiendo utilizar cualquiera de ellas para realizar este apartado, si bien en nuestro caso utilizaremos "Microsoft ISA Server 2004 Enterprise Edition". Evidentemente para poder llevar a cabo este proceso debemos disponer del CD de instalación de dicho producto, si bien en el momento de elaborar este documento, desde la URL http://www.microsoft.com/spain/isaserver/2004/info/trial.aspx podía ser descargada una versión de prueba de 180 días de ISA Server 2004 Enterprise.

Una vez que tengamos el CD de "Microsoft ISA Server 2004" en la unidad correspondiente del equipo "SERVIDOR", lanzaremos "Ejecutar" desde el botón de "Inicio", tecleando a continuación el comando "D:\isaautorun.exe", tal y como vemos en la imagen inferior, y tras

ello pulsaremos sobre el botón "Aceptar".



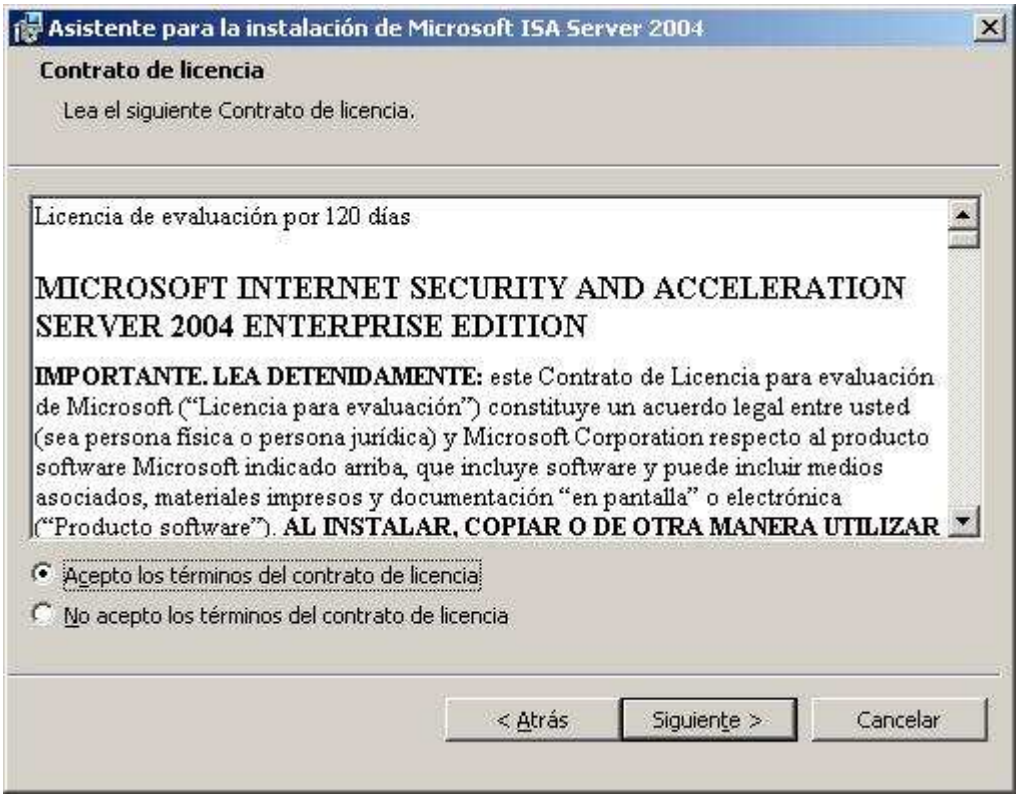
Como resultado de la acción anterior pasa a ser mostrada la siguiente ventana, en la que haremos clic sobre el enlace "Instalar ISA Server 2004" para proceder a instalar dicho producto.



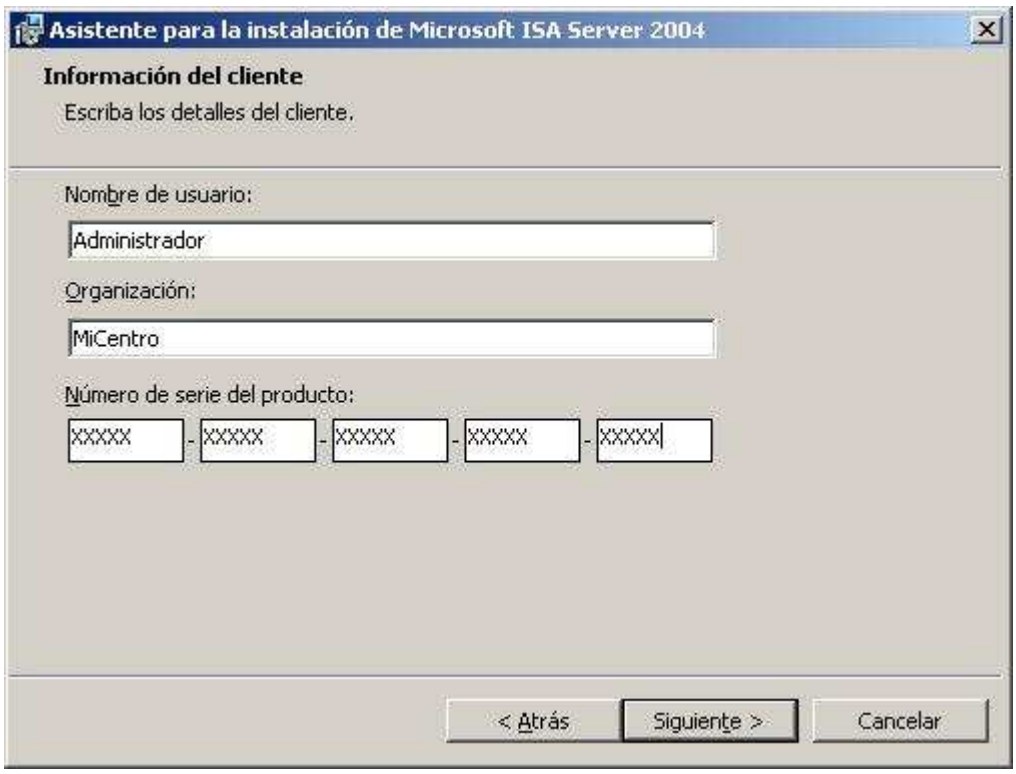
NOTA: Como podemos comprobar en la imagen superior, en nuestro caso hemos instalado una versión de prueba del producto "ISA Server 2004" de 120 días de duración.

A continuación se muestra la primera ventana del asistente de instalación, en la que pulsaremos directamente sobre el botón "Siguiente".

Posteriormente aceptaremos el contrato de licencia activando el radio botón "Acepto los términos del contrato de licencia" en la ventana de la imagen inferior, y tras ello pulsaremos sobre el botón "Siguiente".

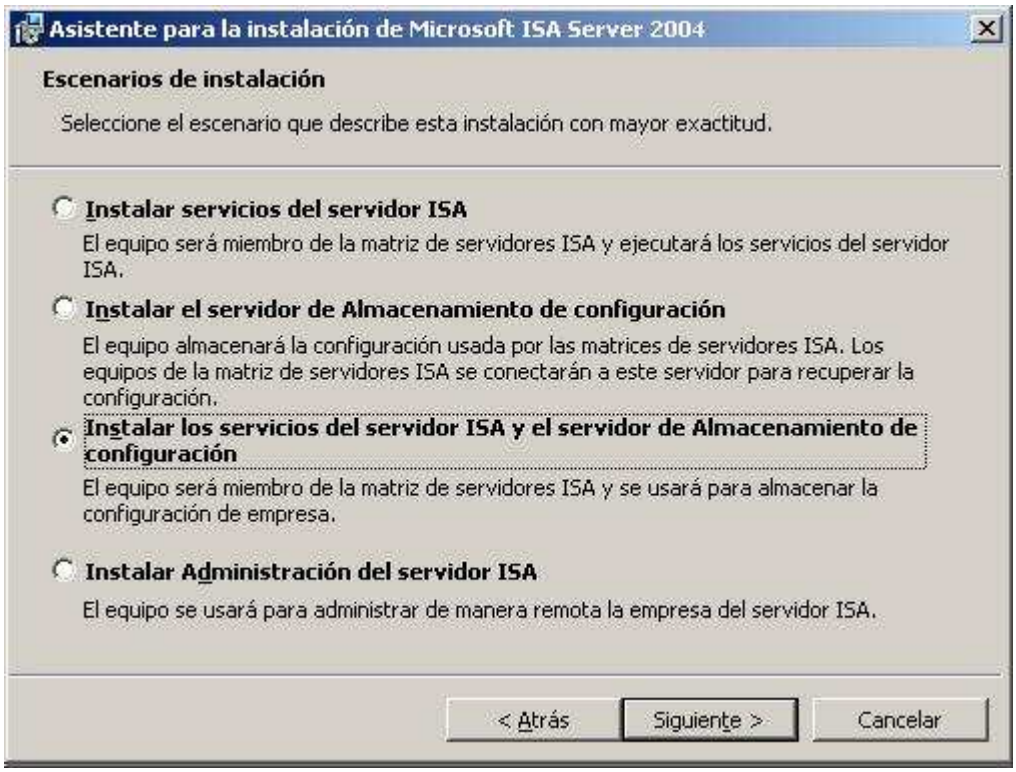


A continuación el asistente nos solicita el nombre de usuario, la organización a la que pertenece dicho usuario, así como el número de serie del producto, introduciendo en cada caja de texto los datos oportunos, tal y como vemos en la imagen inferior.



NOTA: En la imagen superior hemos introducido un código de producto incorrecto en la caja de texto "Número de serie del producto", debiendose introducir el que se tenga asociado a la copia que se posee de "ISA Server 2004".

A continuación debemos especificar el entorno o escenario en el cual se instalará este servidor, seleccionando en nuestro caso el radio botón "Instalar los servicios del servidor ISA y el servidor de Almacenamiento de configuración", pues precisamos de ambos servicios para el correcto funcionamiento de "ISA Server 2004" en el equipo "SERVIDOR".



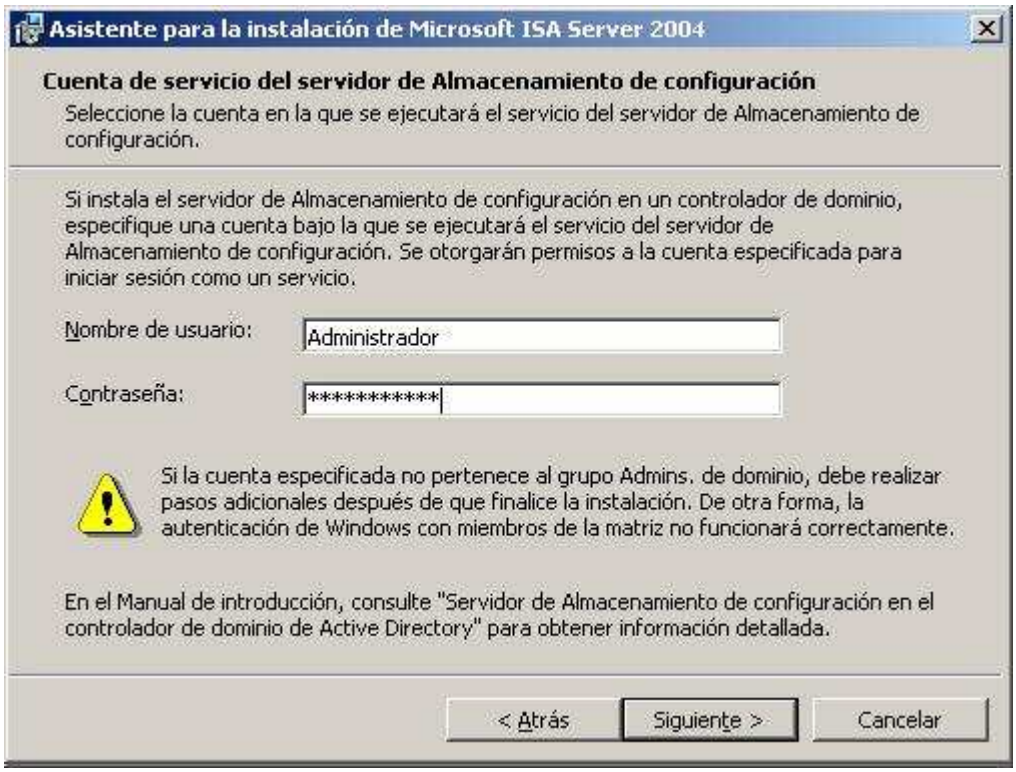
En la siguiente ventana podremos especificar los componentes que serán instalados, si bien en nuestro caso dejaremos seleccionados los componentes que por defecto nos ofrece el

asistente, y pulsaremos en dicha ventana directamente sobre el botón "Siguiente".

En la siguiente ventana dejaremos seleccionado el radio botón "Crear una nueva empresa del servidor ISA", y pulsaremos en ella directamente sobre el botón "Siguiente".

Posteriormente se nos mostrará una ventana que nos informa que el servidor "ISA Server 2004" será configurado como servidor de almacenamiento de configuración, opción que elegimos de modo expreso con anterioridad, así pues pulsaremos en dicha ventana directamente sobre el botón "Siguiente".

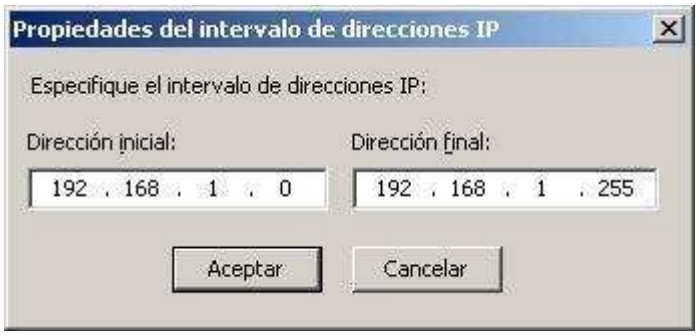
A continuación deberemos indicar el nombre de usuario que se encargará de la gestión del servidor "ISA Server 2004", debiendo especificar dicho nombre de usuario y su contraseña en las cajas de texto correspondiente; en nuestro caso teclearemos las credenciales del "Administrador" del equipo "SERVIDOR", y tras ello pulsaremos sobre el botón "Siguiente".



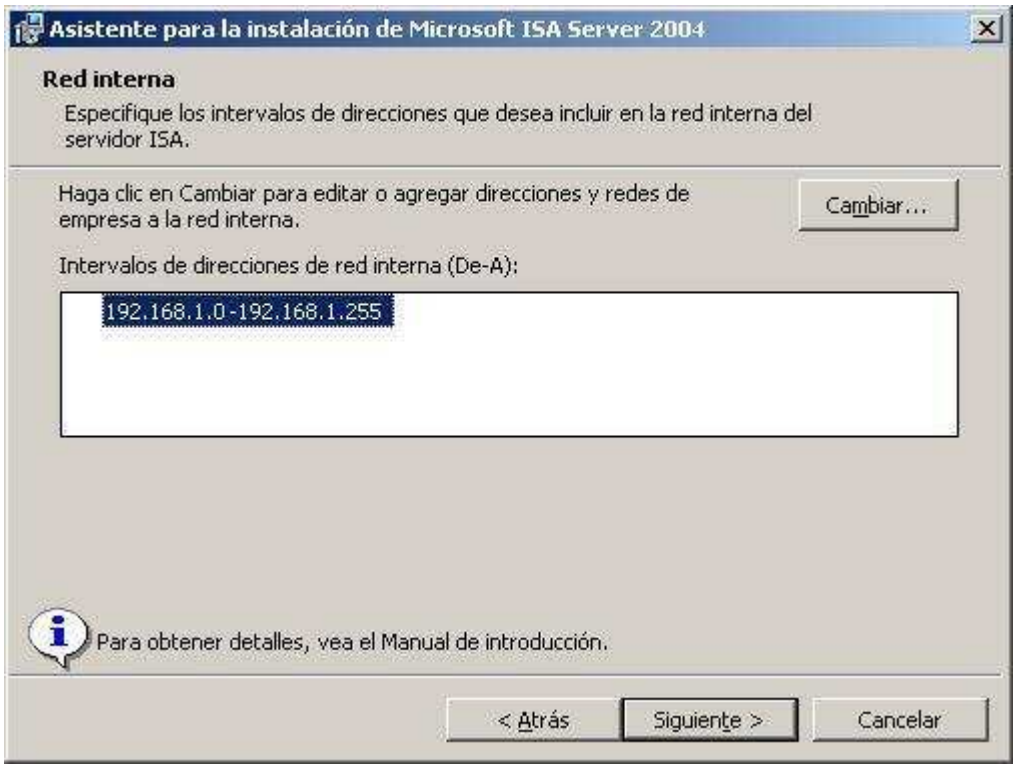
En la siguiente ventana debemos indicar el rango de direcciones IP de la red interna de nuestro centro, que será el rango de direcciones que gestionará el servidor ISA, así pues pulsaremos en dicha ventana sobre el botón "Agregar".

Como resultado de la acción anterior pasa a ser mostrada la siguiente ventana, en la que pulsaremos sobre el botón "Agregar intervalo" para indicar el rango de direccionamiento IP de la red interna de nuestro centro.

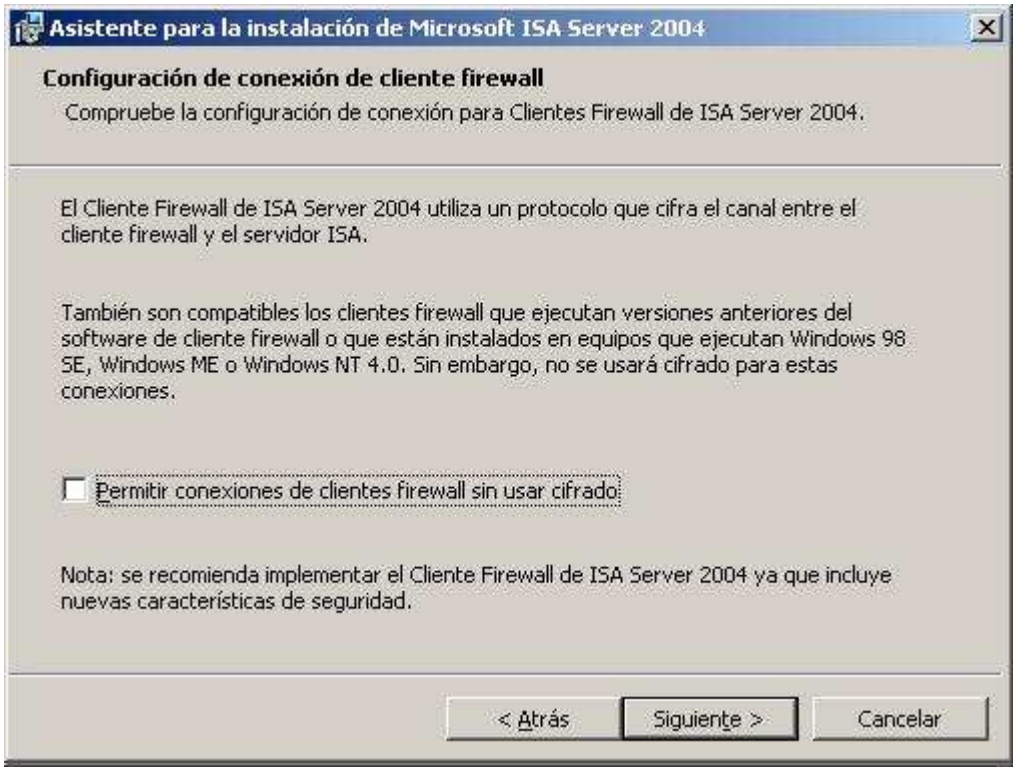
Una nueva ventana es mostrada a continuación, en la que teclearemos el rango de direccionamiento IP de la red interna de nuestro centro, en nuestro caso desde "192.168.1.0" a "192.168.1.255", tal y como vemos en la imagen inferior.



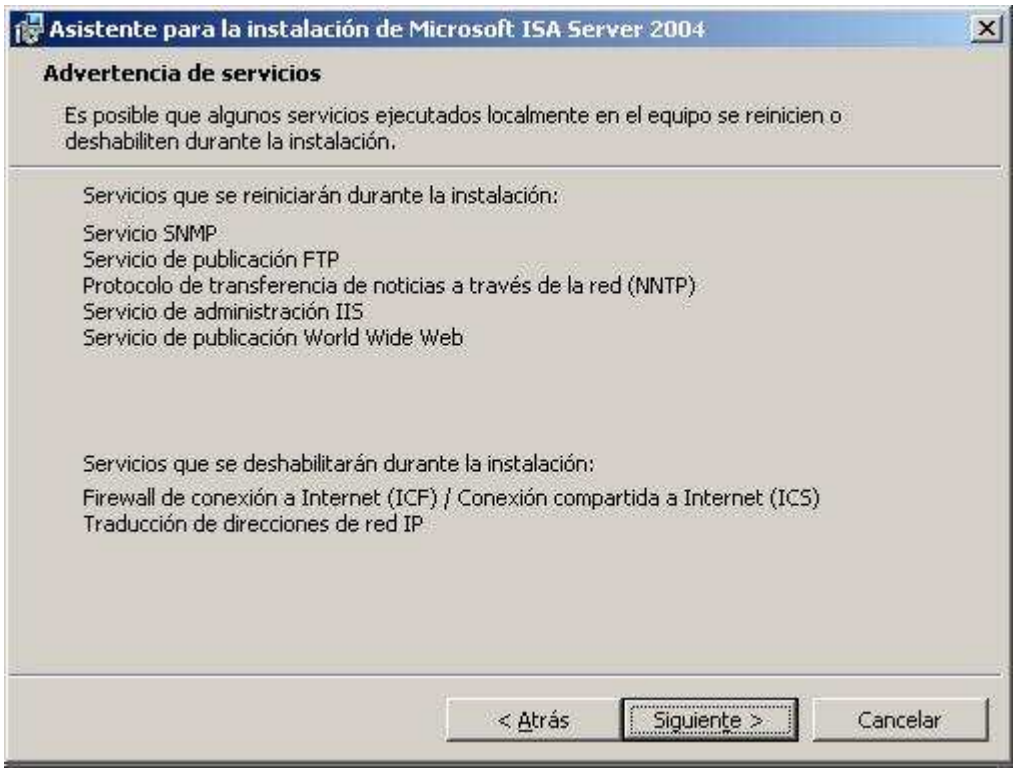
Iremos pulsando sobre los respectivos botones "Aceptar" en las ventanas que tuviéramos abiertas, de modo que de vuelta en la ventana donde especificamos el rango de direccionamiento IP, cuando ésta presente el siguiente aspecto, pulsaremos en ella sobre el botón "Siguiente".



A continuación se nos informa de la posibilidad de utilizar el cliente de firewall sin cifrado, pero dado que en nuestro caso NO utilizaremos dicho cliente de firewall, no realizaremos configuración alguna en este ventana, y pulsaremos en ella directamente sobre el botón "Siguiente".

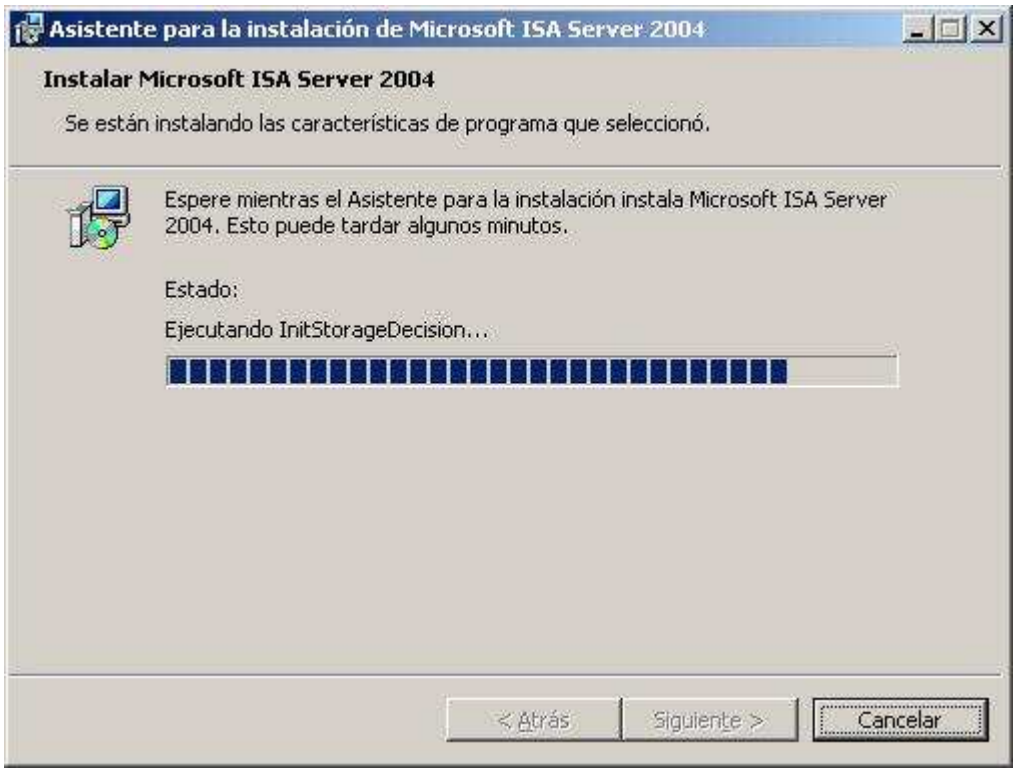


En la siguiente ventana el asistente nos informa de que ciertos servicios deben ser reiniciados en el equipo "SERVIDOR" para poder continuar con el proceso de instalación, debiendo pues pulsar en ella directamente sobre el botón "Siguiente" para proceder a la detección de dichos servicios.



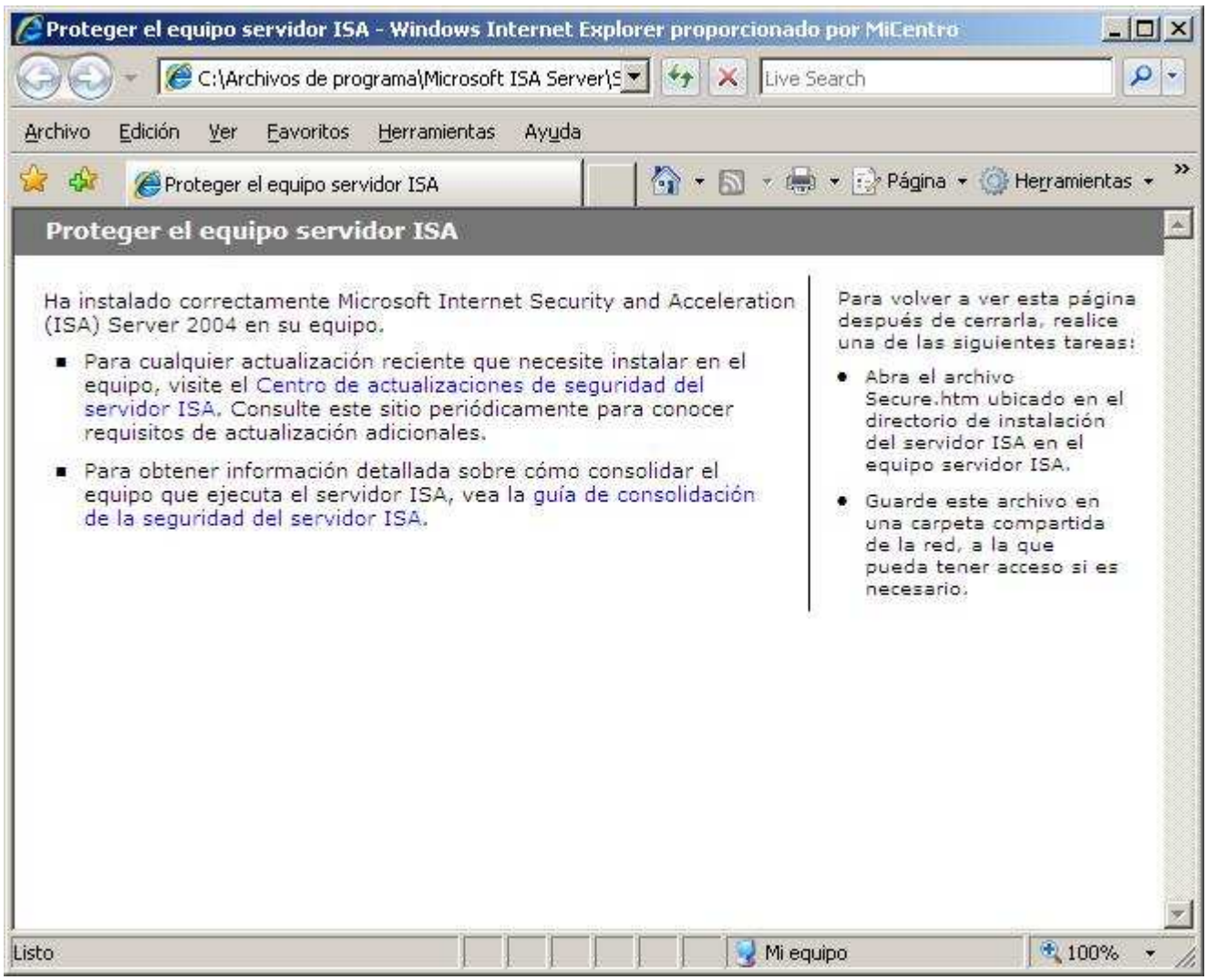
Finalmente en la siguiente ventana el asistente nos informa de que va a dar comienzo el proceso de instalación de "ISA Server 2004" con las opciones elegidas, así pues pulsaremos en ella sobre el botón "Instalar".

En este instante da comienzo el proceso de instalación de la aplicación "ISA Server 2004" en el equipo "SERVIDOR", proceso que puede durar alrededor de quince minutos aproximadamente.



Una vez completado el proceso de instalación de la aplicación, pasa a ser mostrada la siguiente ventana, en la que pulsaremos directamente sobre el botón "Finalizar".

Tras completarse exitosamente la instalación, se abrirá automáticamente la siguiente página web que nos informa de dicha circunstancia.



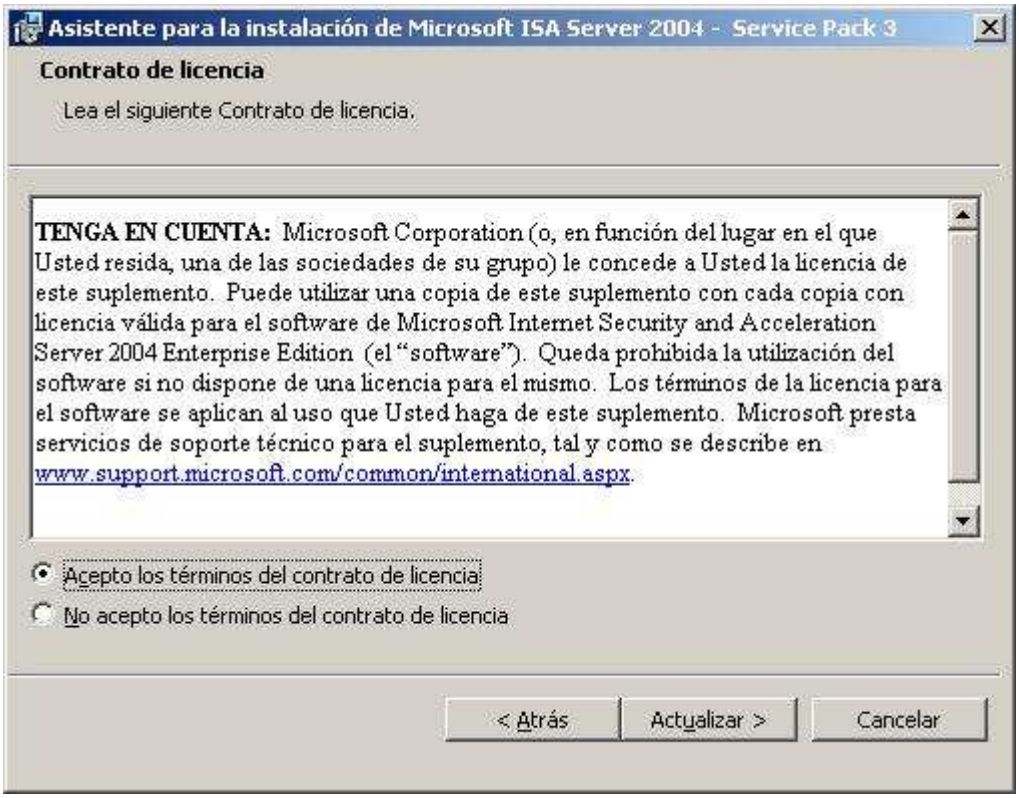
En este instante podemos a retirar el CD de instalación de "Microsoft ISA Server 2004" de la unidad correspondiente del equipo "SERVIDOR".

Tras completarse la instalación de "ISA Server 2004", el siguiente paso que debemos llevar a cabo en el proceso de instalación del producto, es la actualización del mismo con el SP3 de "ISA Server 2004".

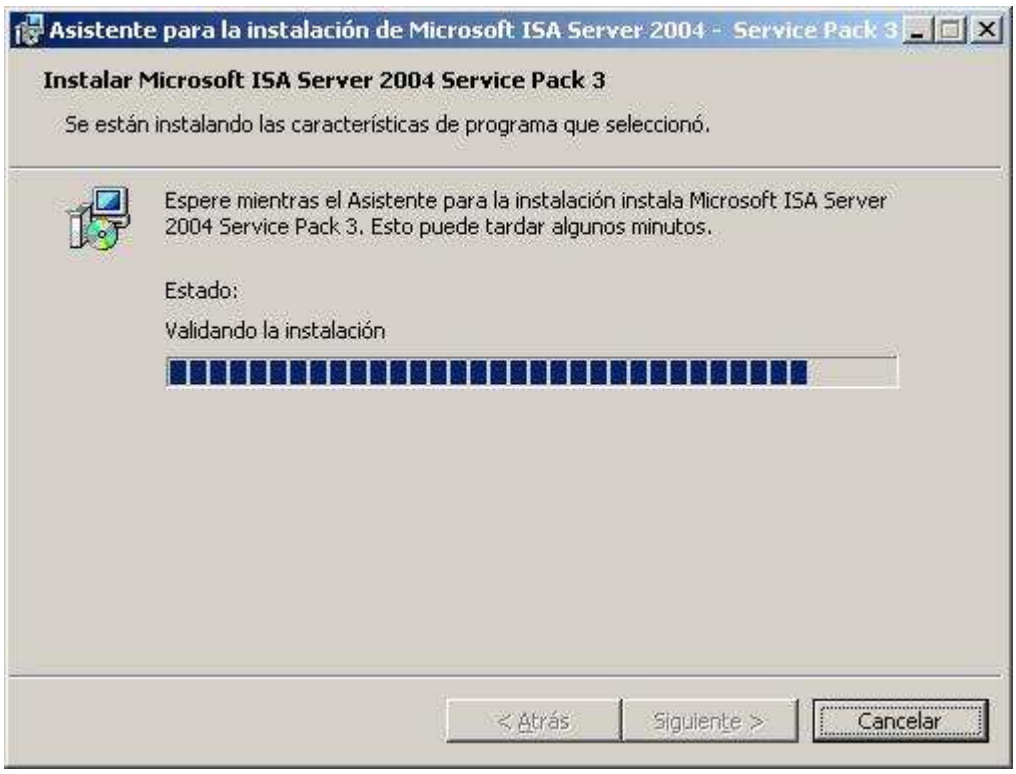
NOTA: Actualmente el SP3 de "Microsoft ISA Server 2004" puede ser descargado desde la URL "http://www.microsoft.com/downloads/details.aspx?FamilyID=a05a074a-5033-4792-af8b-58b90d841436&DisplayLang=es".

Así pues, una vez que dispongamos del fichero "ISA2004EE-KB924406-x86-ESN.msp" de instalación del SP3 de "Microsoft ISA Server 2004", lo copiamos al Escritorio del equipo "SERVIDOR", y tras ello haremos doble clic sobre el mismo, mostrándose la siguiente ventana, en la cual pulsaremos directamente sobre el botón "Siguiente".

A continuación aceptamos las condiciones de instalación seleccionando en la siguiente ventana el radio botón "Acepto los términos del contrato de licencia", y pulsando posteriormente sobre el botón "Actualizar".



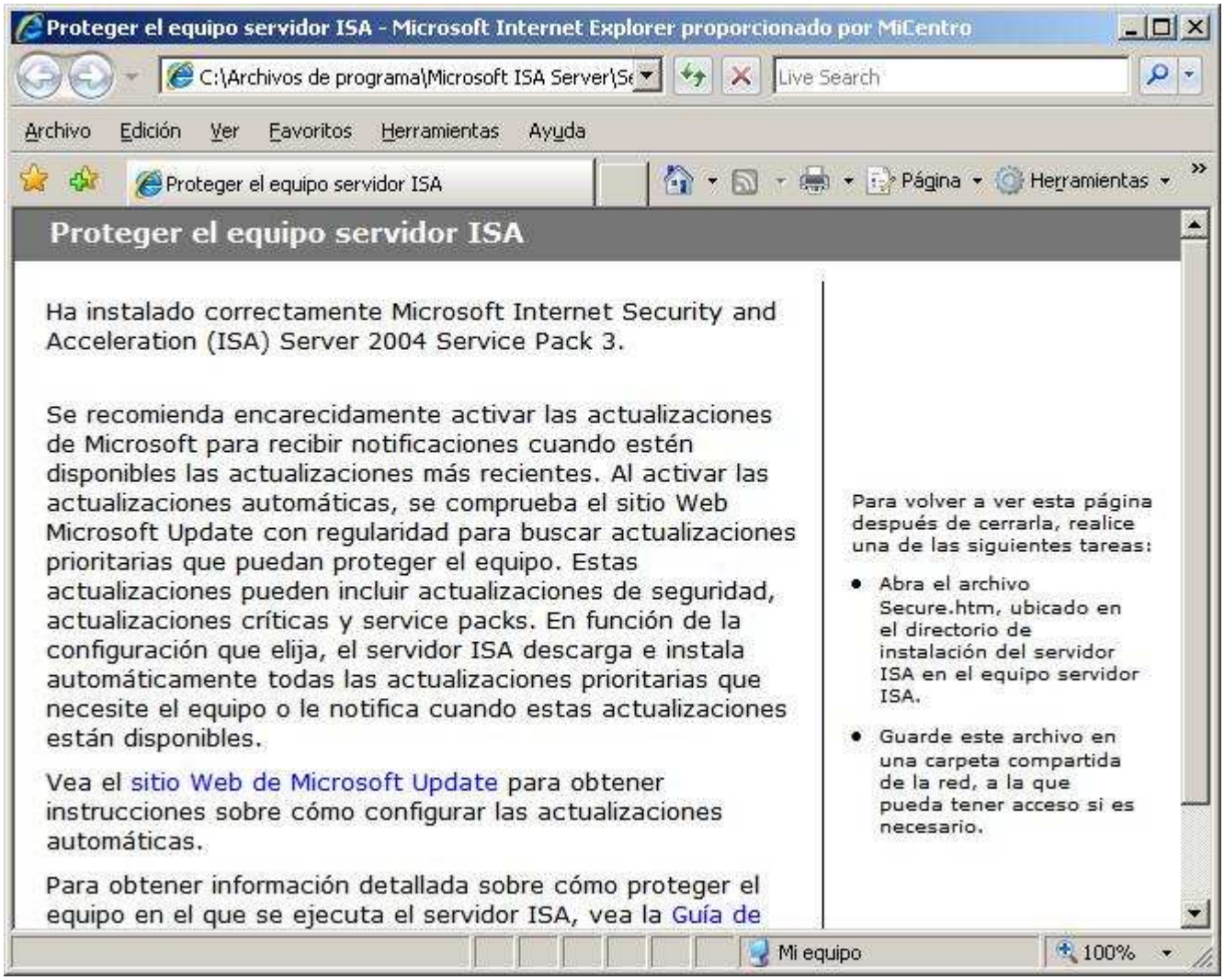
En este instante da comienzo la instalación del SP3 de "ISA Server 2004" en el equipo "SERVIDOR", proceso que durará alrededor de cinco minutos aproximadamente.



Tras completarse la instalación del SP3 de "ISA Server 2004", se mostrará la siguiente ventana, en la cual pulsaremos directamente sobre el botón "Finalizar".

Tras pulsar sobre el botón "Finalizar" en la ventana de la imagen anterior, se nos muestra la siguiente ventana, que nos indica que deberemos pulsar sobre el botón "Sí" para que los cambios realizados pasen a ser aplicados de modo efectivo, así pues pulsaremos en ella sobre el botón "Sí" para proceder con dicho reinicio.

Una vez completado el reinicio del equipo "SERVIDOR", automáticamente se nos mostrará la siguiente página web, que nos indica que el SP3 de "ISA Server 2004" ha sido correctamente instalado.



Cerraremos la ventana de la imagen anterior, tras lo cual procederemos a eliminar el fichero "ISA2004EE-KB924406-x86-ESN.msp" de instalación del SP3 de "ISA Server 2004" del Escritorio del equipo "SERVIDOR", pudiendo con ello dar por concluida la instalación de "ISA Server 2004 Enterprise Edition SP3".

Peticiones Salientes

Tras instalar en el apartado anterior "Microsoft ISA Server 2004 Enterprise Edition SP3" en el equipo "SERVIDOR", por defecto el cortafuegos impide la salida a Internet de la red interna de nuestro centro, así como el acceso desde Internet a nuestra red interna.

El motivo por el cual el cortafuegos cierra todo el tráfico de red, es debido a que la regla de acceso "Regla Predeterminada", que se aplica siempre en último lugar y que deniega todo el trafico de todas las redes a cualquier red para cualquier usuario, es la única regla activa.

Podemos comprobar lo que hemos indicado en el párrafo anterior, pulsando sobre el botón "Inicio" del equipo "SERVIDOR", para seleccionar "Todos los programas -> Microsoft ISA Server -> Administración del servidor ISA" en los desplegables correspondientes, pasando a ser mostrada como resultado de dicha acción la siguiente ventana, en la que nos situaremos sobre "Directiva de Firewall (SERVIDOR)" del apartado "SERVIDOR" en la entrada "Matrices", pudiendo comprobar la existencia de una única regla de firewall de denegación de todo el tráfico de red denominada "Regla predeterminada".

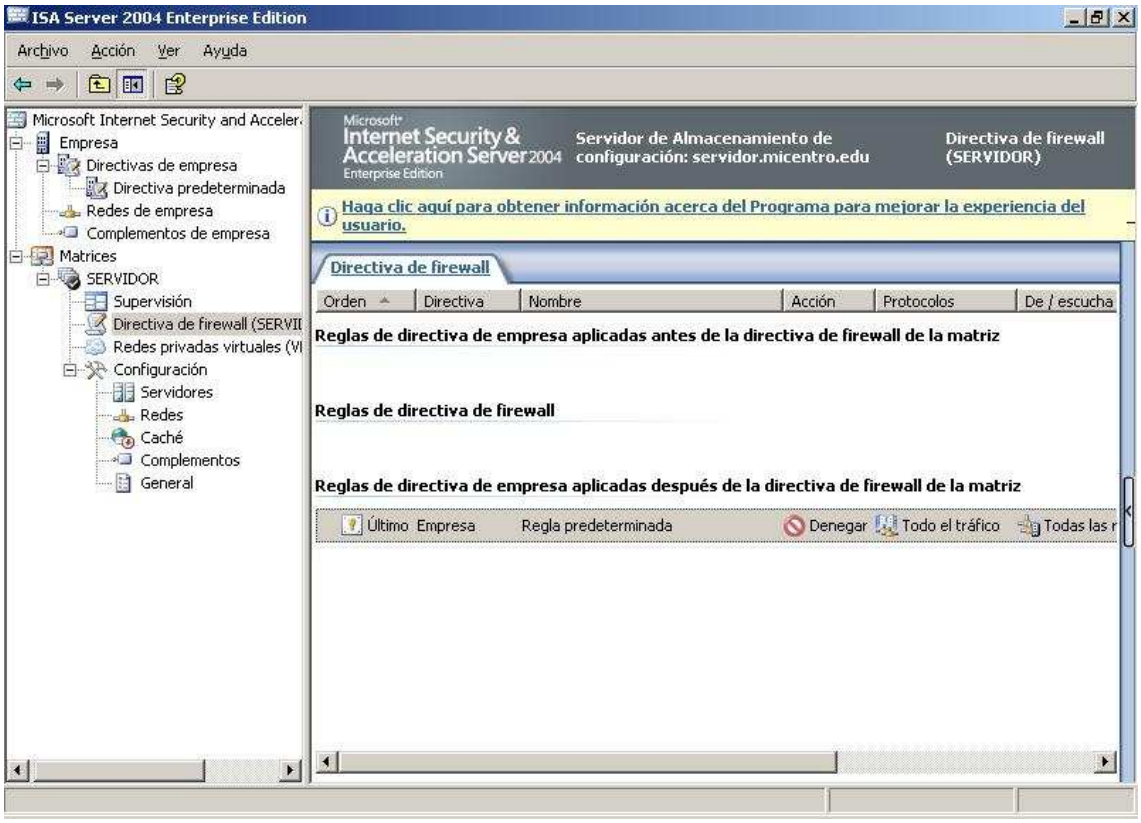


Imagen: ISA\salien01.JPG

Pese a la existencia de la regla citada anteriormente, se instala una política de sistema por defecto en el firewall de "ISA Server 2004" que permite el acceso a tareas elementales de administración de la red, tales como DHCP, DNS, etc.

Si deseamos visualizar la política de sistema por defecto del firewall citada en el párrafo

anterior, sobre la consola de administración de "ISA Server 2004" extenderemos la entrada "Matrices" y luego "SERVIDOR" en el panel de búsqueda, y pulsaremos a continuación sobre la entrada "Directiva de firewall (SERVIDOR)" con el botón derecho del ratón, seleccionando la opción "Ver", y luego "Mostrar reglas de directivas del sistema", en los desplegables correspondientes, pasando a visualizarse dichas directivas, tal y como vemos en la imagen inferior.

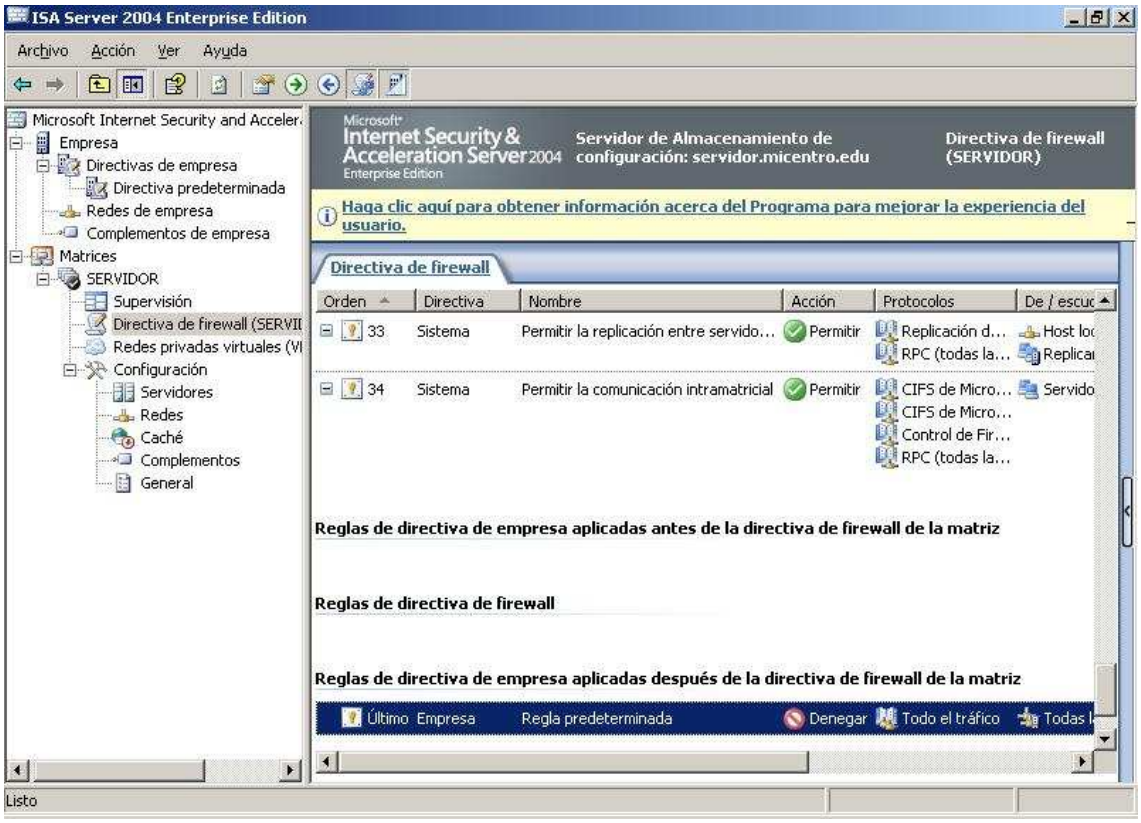


Imagen: ISA\salien02.JPG

Estas reglas de directivas del sistema permiten acceder a los clientes a servicios tan elementales como Active Directory, DNS o DHCP entre otros; como se puede observar dichas reglas se definen por parámetros tales como "Orden", "Nombre", "Acción" (permitir o denegar), "Protocolos", "Desde" (red o máquina origen), "Hacia" (sistema o red de destino) o "Condición" (a quién o a qué se aplica la regla); las reglas de política de sistema que están deshabilitadas por defecto tienen una flecha roja apuntando hacia abajo en su esquina inferior derecha, y serán activadas automáticamente cuando hagamos cambios de configuración en el firewall "ISA Server 2004".

Pese a lo comentado anteriormente, las reglas de política de sistema precisan de la creación de una regla de apertura que habilite el acceso a dichos servicios, pues "ISA Server 2004" bloquea por defecto el tráfico a todos los interfaces de red del equipo "SERVIDOR", incluida la tarjeta de red "Conexión LAN", y todos los servicios prestados sobre ella.

Así pues la primera configuración que llevaremos a cabo en "ISA Server 2004" será crear una regla que permita todo el tráfico de red de ida y vuelta entre la LAN (red "Interna") y el equipo "SERVIDOR" ("Host local"), para lo cual nos ubicaremos sobre la entrada "Directiva de Firewall (SERVIDOR)" de la matriz "SERVIDOR", pulsando sobre ella con el botón derecho del ratón

para elegir la opción "Nuevo", y luego "Regla de Acceso", en los desplegables correspondientes.

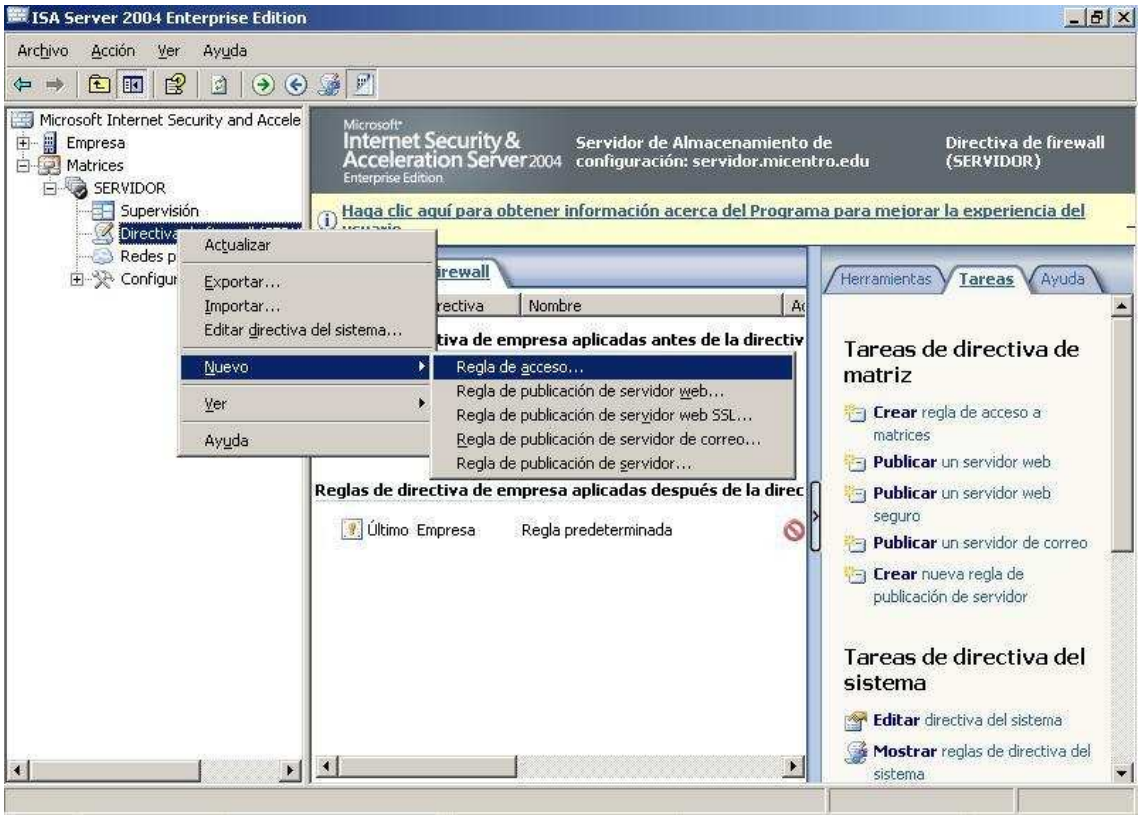


Imagen: ISA\salien03.JPG

Como resultado de la acción anterior, pasa ser mostrada la primera ventana del asistente de creación de nueva regla de acceso, en la cual especificaremos como nombre para la regla de acceso "Trafico LAN", y a continuación pulsaremos sobre el botón "Siguiente".

Imagen: ISA\salien04.JPG

En la siguiente ventana deberemos indicar si deseamos que la regla que estamos definiendo sea de permiso o de denegación de acceso; en este caso seleccionaremos el radio botón "Permitir", y a continuación pulsaremos sobre el botón "Siguiente".

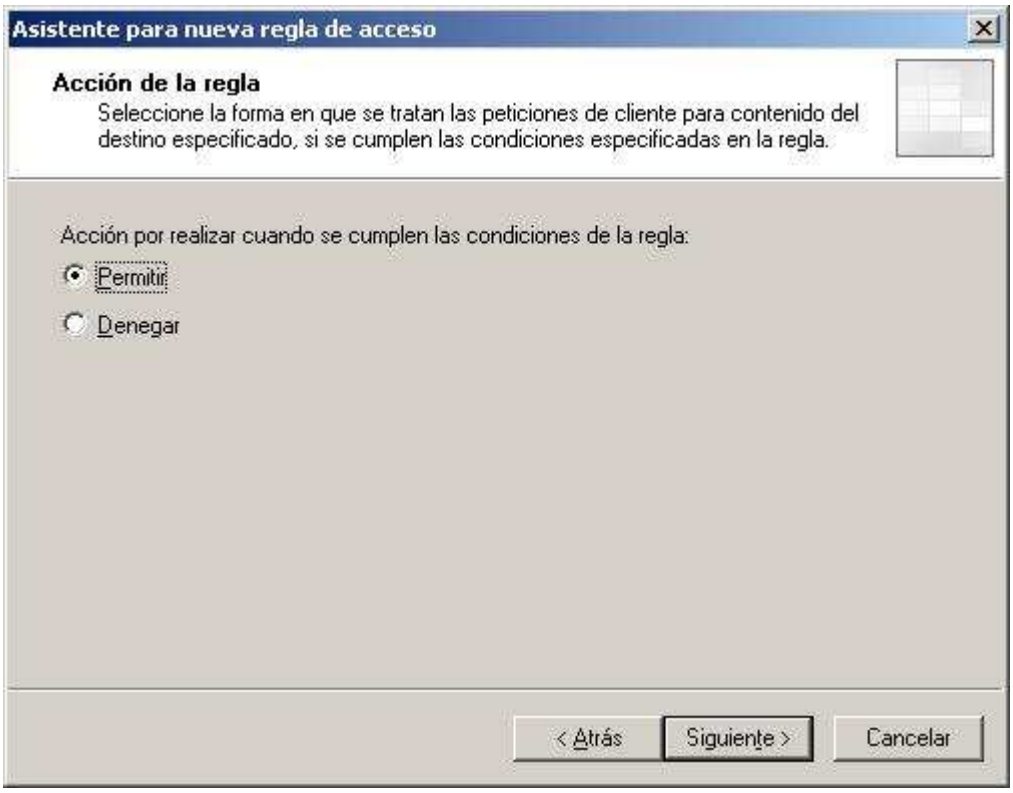


Imagen: ISA\salien05.JPG

A continuación deberemos especificar el tráfico de red al cual va a afectar la regla en cuestión, pudiendo elegir que afecte a determinados protocolos o incluso o determinados puertos (pulsando sobre el botón "Puertos"), aunque en este caso vamos a hacer que la regla se aplique a "Todo el tráfico saliente", seleccionando dicha opción en el desplegable correspondiente, y pulsando posteriormente sobre el botón "Siguiente".

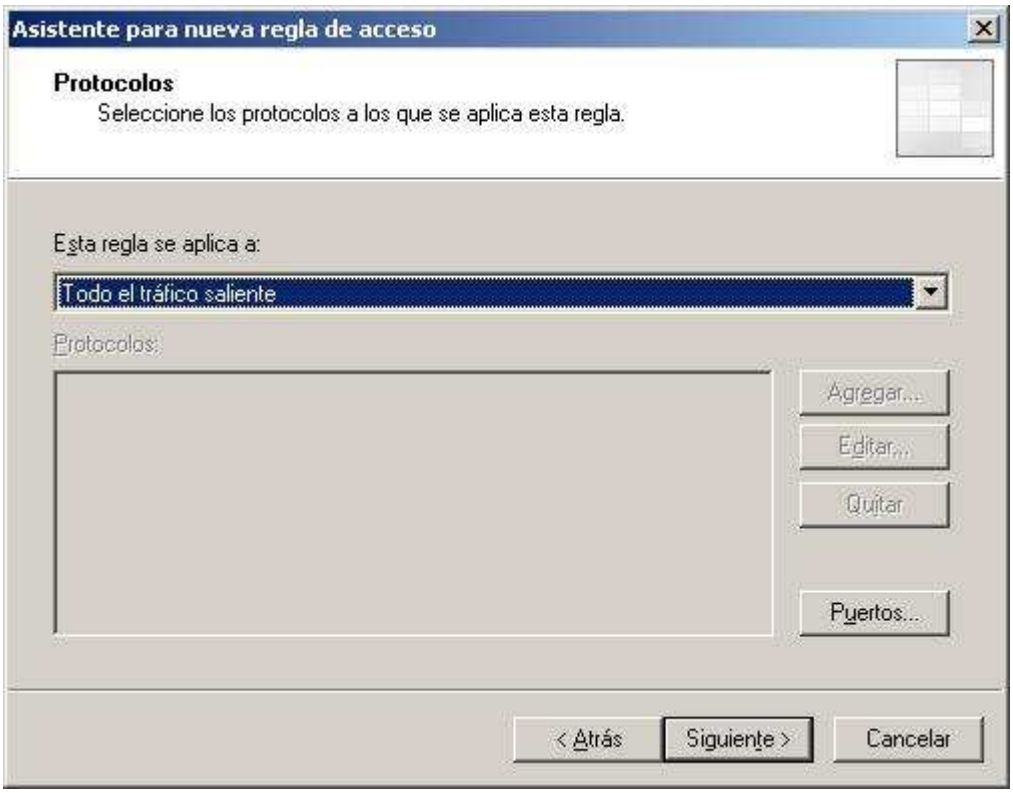


Imagen: ISA\salien06.JPG

En la siguiente ventana deberemos especificar los orígenes a los cuales será aplicada esta regla, para lo cual pulsaremos sobre el botón "Agregar", y en la nueva ventana mostrada haremos clic sobre la carpeta "Redes" para seleccionar "Interna" y "Host local", de modo que finalmente la ventana de selección del origen de la regla de acceso deberá quedar tal y como se muestra en la siguiente imagen.

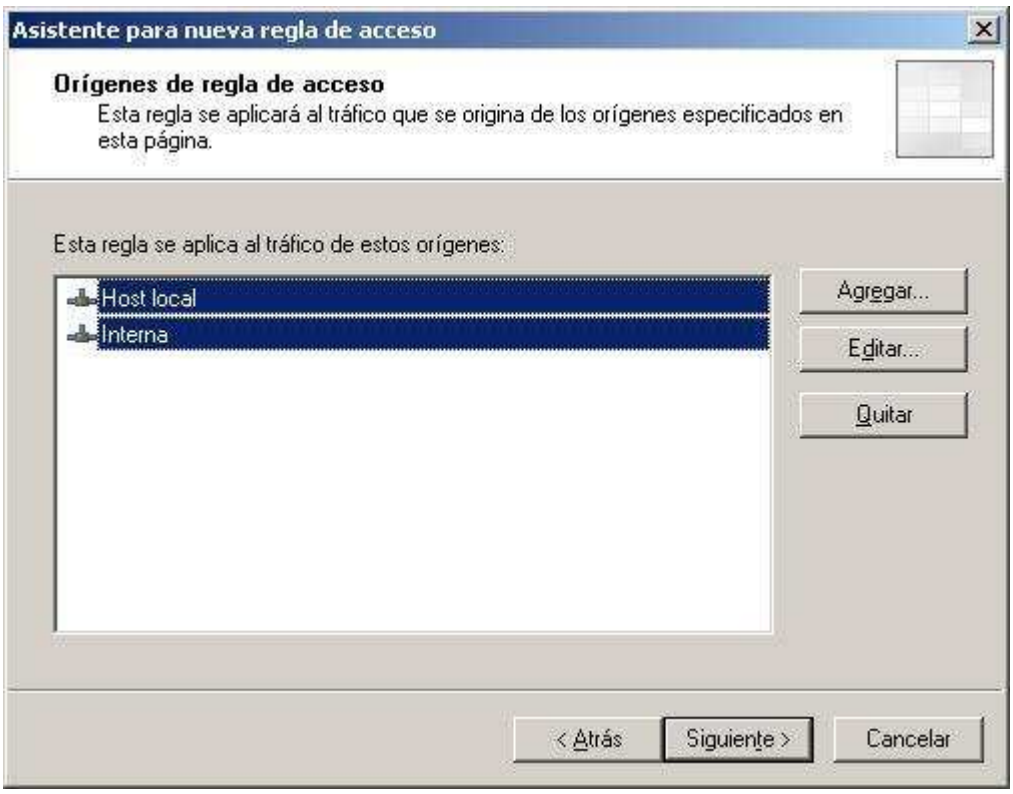


Imagen: ISA\salien07.JPG

En la siguiente ventana deberemos especificar los destinos a los cuales será aplicada esta regla, para lo cual pulsaremos sobre el botón "Agregar", y en la nueva ventana mostrada haremos clic sobre la carpeta "Redes" para seleccionar "Interna" y "Host local", de modo que finalmente la ventana de selección del destino de la regla de acceso deberá quedar tal y como se muestra en la siguiente imagen.

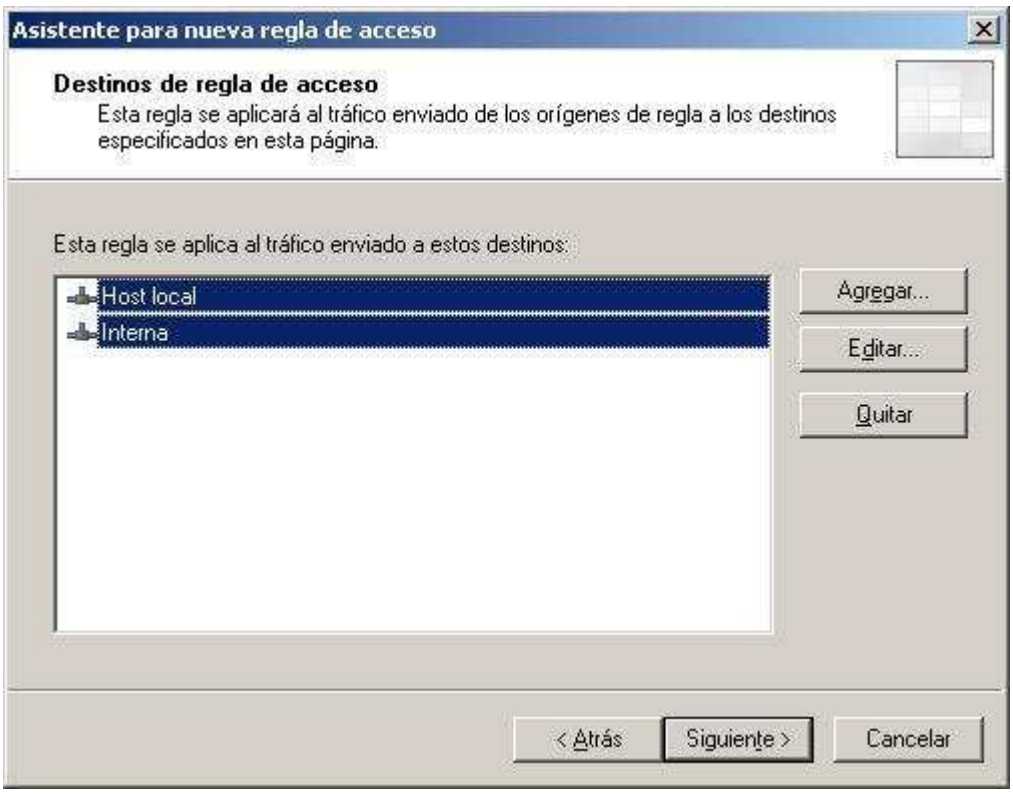


Imagen: ISA\salien08.JPG

La siguiente ventana nos permite especificar los usuarios a los cuales será aplicada esta regla, si bien en nuestro caso daremos por válida la opción "Todos los usuarios", ofertada por defecto por el asistente, y pulsaremos directamente en ella sobre el botón "Siguiente".

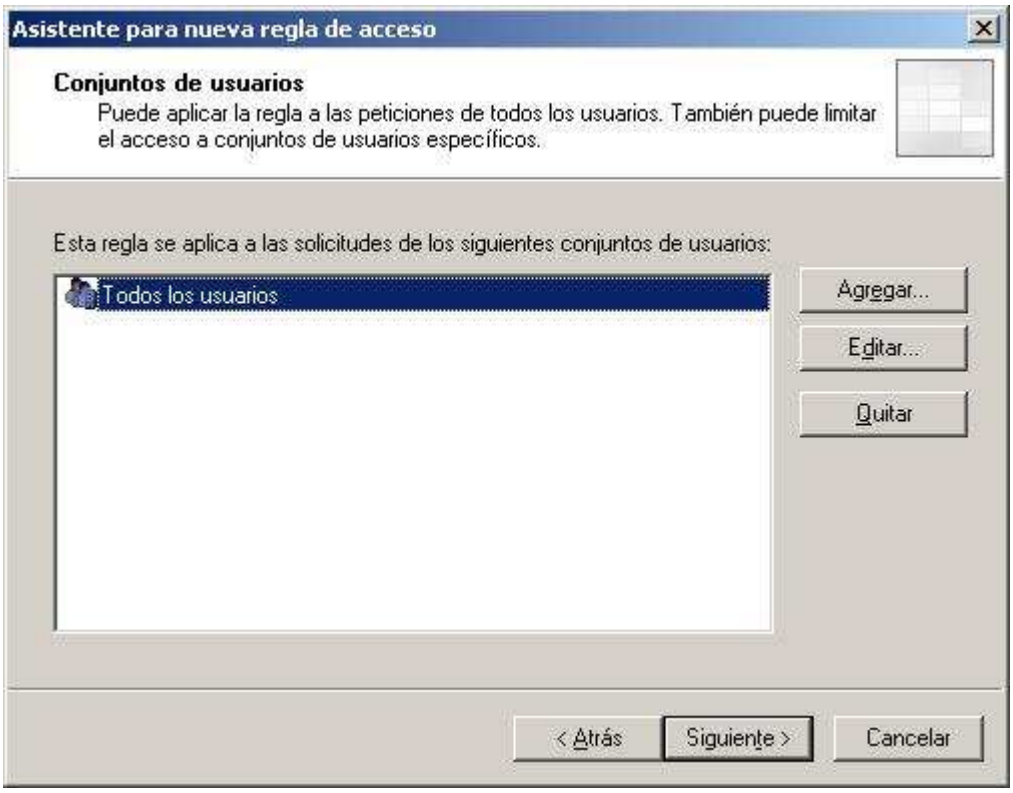


Imagen: ISA\salien09.JPG

Completaremos el proceso de creación de nueva regla, pulsando sobre el botón "Finalizar" en la siguiente ventana.

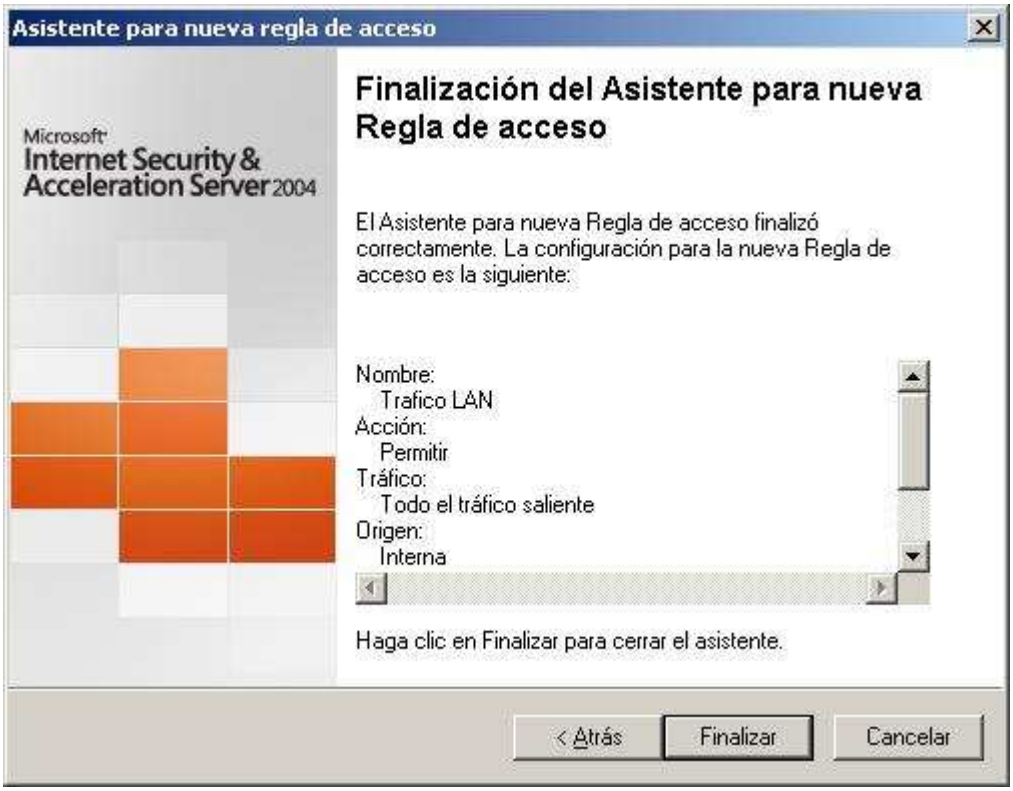


Imagen: ISA\salien10.JPG

Tras terminar de definir la regla "Tráfico LAN", en la parte superior de la ventana de administración de "ISA Server 2004" se nos muestra un mensaje que nos indica que deberemos pulsar sobre el botón "Aplicar" para que la regla pase a ser aplicada de modo efectivo, así pues pulsaremos sobre dicho botón para proceder a aplicar la regla definida.

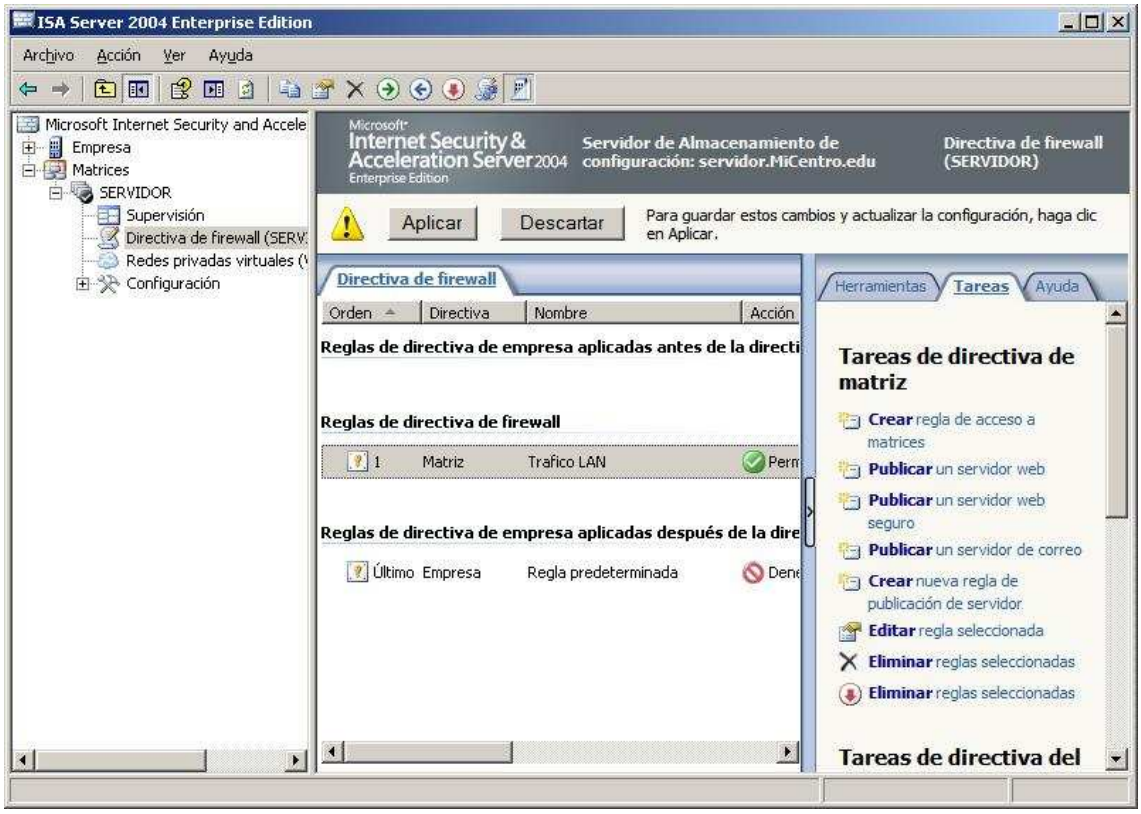


Imagen: ISA\salien11.JPG

Tras unos breves instantes se mostrará la siguiente ventana que nos informa de que los cambios realizados han pasado a ser aplicados en el servidor "ISA Server 2004"; pulsaremos en ella sobre el botón "Aceptar" para continuar.

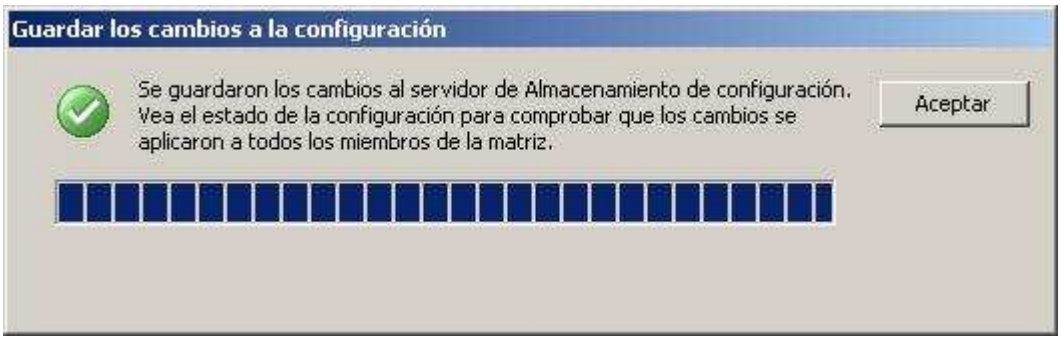


Imagen: ISA\salien12.JPG

La regla creada anteriormente consigue el acceso de los equipos clientes de la LAN a cualquier servicio prestado por el equipo "SERVIDOR" (DHCP, DNS, servidores web, etc.), pero no permite el acceso de los equipos de la LAN a Internet, de modo que si en este instante arrancáramos un equipo cliente del dominio, podríamos comprobar que comprobar que el servidor DHCP le asocia una dirección IP válida, que los usuarios pueden validarse en el dominio, que podemos acceder a las páginas web internas de los servidores web de nuestro centro, pero NO podríamos navegar por páginas web externas.

Así pues para lograr que los clientes de nuestra red interna tengan acceso a las páginas de Internet, debemos crear una nueva regla de acceso que permita dicha salida, para lo cual haremos doble clic sobre la matriz "SERVIDOR", situándonos a continuación sobre la entrada "Directiva de firewall (SERVIDOR)", pulsando sobre ella con el botón derecho del ratón para elegir "Nuevo", y luego "Regla de acceso" en los desplegables correspondientes, pasando a ser mostrada como resultado de dicha acción primera ventana del asistente de creación de nueva regla de acceso, en la que indicaremos como nombre para la misma "Trafico WAN".

Imagen: ISA\salien13.JPG

En la siguiente ventana indicaremos si la regla es de permiso o de denegación de acceso, siendo en nuestro caso de permiso de acceso, luego seleccionaremos el radio botón "Permitir" en la ventana de la imagen inferior, y tras ello pulsaremos sobre el botón "Siguiente".

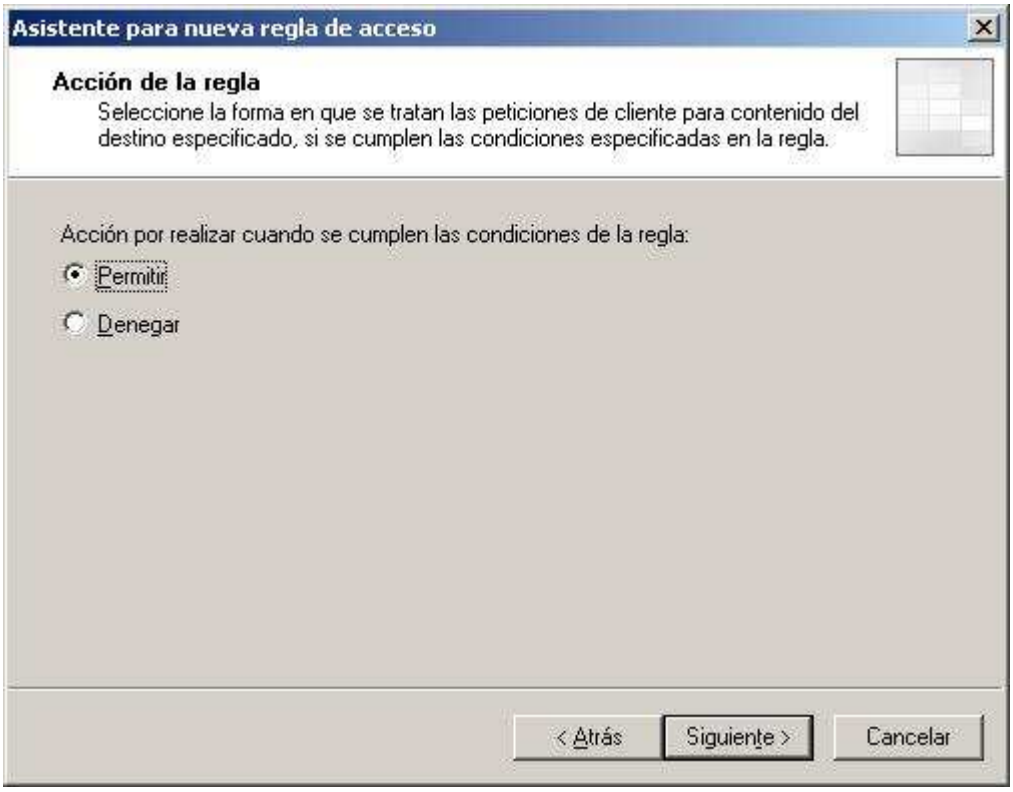


Imagen: ISA\salien14.JPG

En la siguiente ventana deberemos especificar los protocolos a los que afectará la regla en cuestión, así pues en la lista desplegable correspondiente seleccionaremos la opción deseada, en nuestro caso "Todo el tráfico saliente", y a continuación pulsaremos sobre el botón "Siguiente".

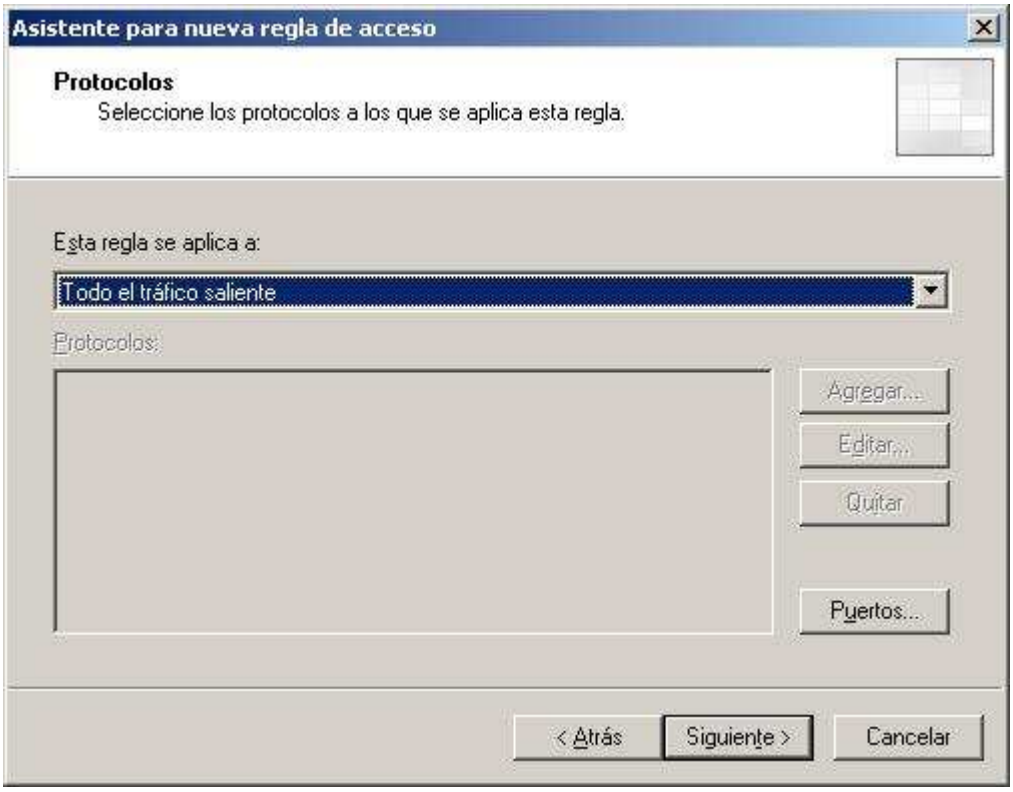


Imagen: ISA\salien15.JPG

En la siguiente ventana deberemos especificar los orígenes a los cuales será aplicada esta regla, para lo cual pulsaremos sobre el botón "Agregar", y en la nueva ventana mostrada haremos clic sobre la carpeta "Redes" para seleccionar "Interna" y "Host local", de modo que finalmente la ventana de selección del origen de la regla de acceso deberá quedar tal y como se muestra en la siguiente imagen.

Imagen: ISA\salien16.JPG

En la siguiente ventana deberemos especificar los destinos a los cuales será aplicada esta regla, para lo cual pulsaremos sobre el botón "Agregar", y en la nueva ventana mostrada haremos clic sobre la carpeta "Redes" para seleccionar "Externa", de modo que finalmente la ventana de selección del destino de la regla de acceso deberá quedar tal y como se muestra en la siguiente imagen.

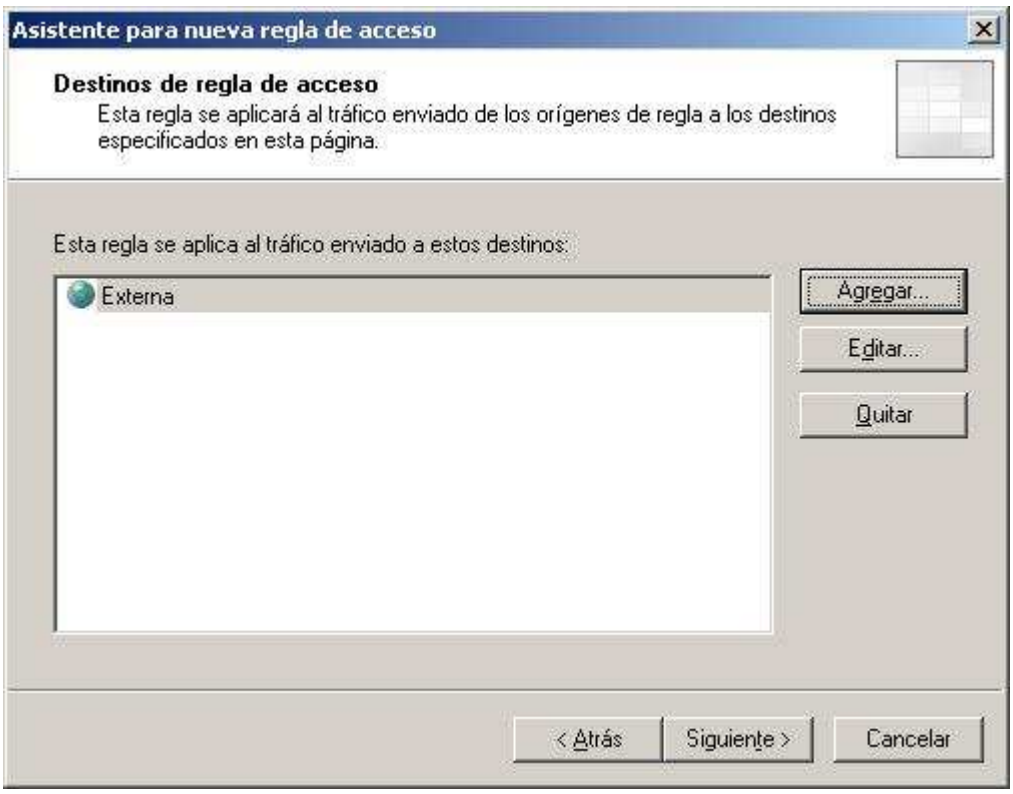


Imagen: ISA\salien17.JPG

La siguiente ventana nos permite especificar los usuarios a los cuales será aplicada esta regla, si bien en nuestro caso daremos por válida la opción "Todos los usuarios", ofertada por defecto por el asistente, y pulsaremos directamente en ella sobre el botón "Siguiente".

Imagen: ISA\salien18.JPG

Completaremos el proceso de creación de nueva regla pulsando sobre el botón "Finalizar" en la siguiente ventana.

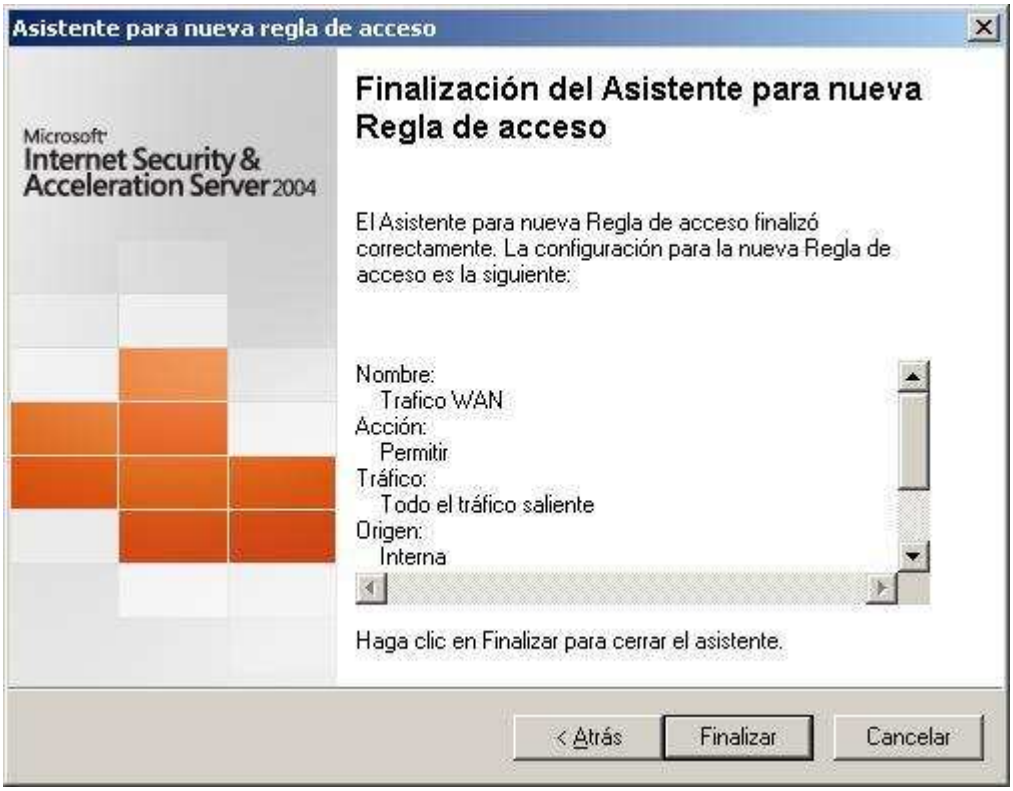


Imagen: ISA\salien19.JPG

Una vez completada la configuración de esta regla, para que pase a aplicarse deberemos recordar pulsar sobre el botón "Aplicar" en la ventana de administración de "ISA Server 2004".

Una vez que la regla haya sido aplicada, podremos acceder a Internet desde los equipos clientes de nuestro centro sin problema alguno, disponiendo de una configuración básica en el servidor "ISA Server 2004" que puede ser válida en líneas generales para cualquier centro.

Dado que a partir de este instante la salida a Internet de los equipos clientes de nuestro centro es posible, debemos indicar que la misma podríamos realizarla directamente a través del equipo "SERVIDOR", o bien utilizando el proxy-caché que instala "ISA Server 2004" en el equipo "SERVIDOR", logrando con esta segunda opción un mejor aprovechamiento del ancho de banda de la conexión a Internet.

Si deseamos configurar un equipo cliente del dominio para que utilice el proxy del "ISA Server 2004", desde el navegador "Internet Explorer" de dicho equipo cliente, deberemos pulsar sobre la opción "Herramientas" de su menú principal, y tras ello elegir "Opciones de Internet" en el desplegable correspondiente, pasando a ser mostrada la siguiente ventana, en la que nos ubicaremos en la pestaña "Conexiones", para a continuación pulsar sobre el botón

"Configuración de LAN".

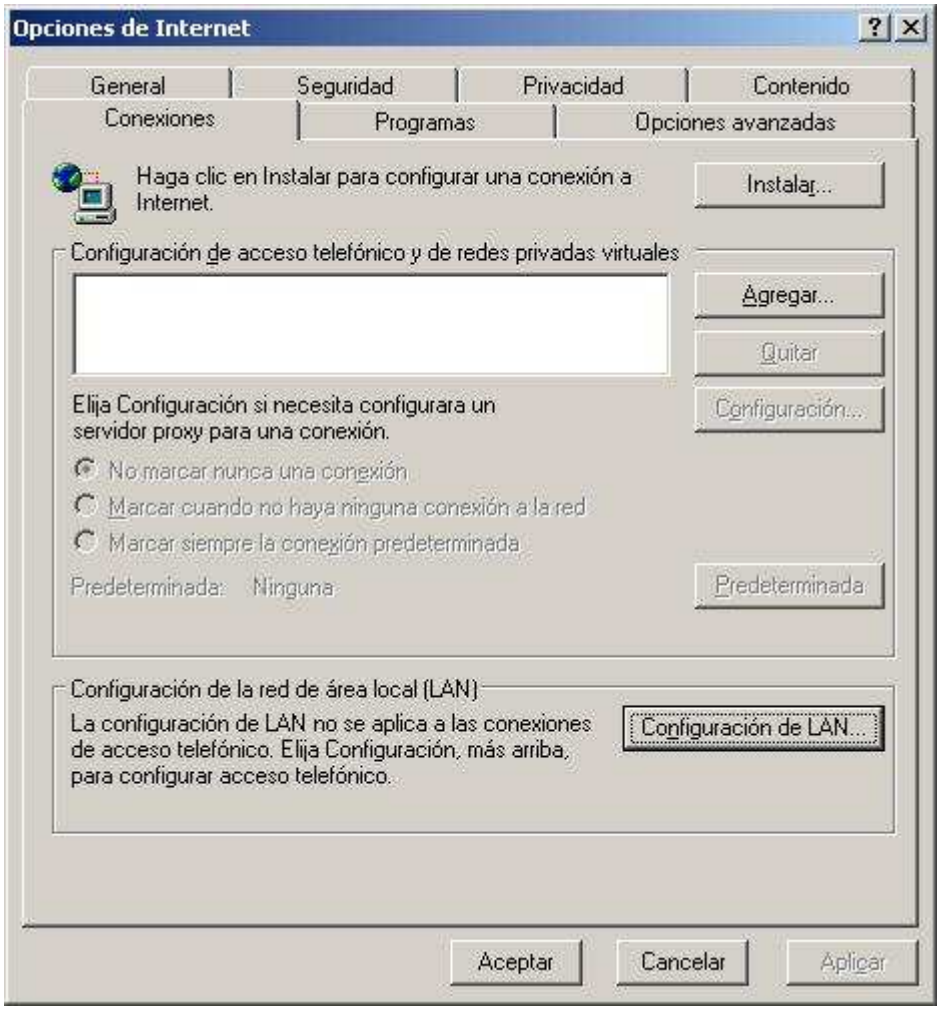


Imagen: ISA\salien20.JPG

En la nueva ventana mostrada como resultado de la acción anterior, activamos la casilla "Utilizar un servidor proxy para su LAN", tal y como vemos en la imagen inferior, y tras ello pulsaremos sobre el botón "Opciones avanzadas".

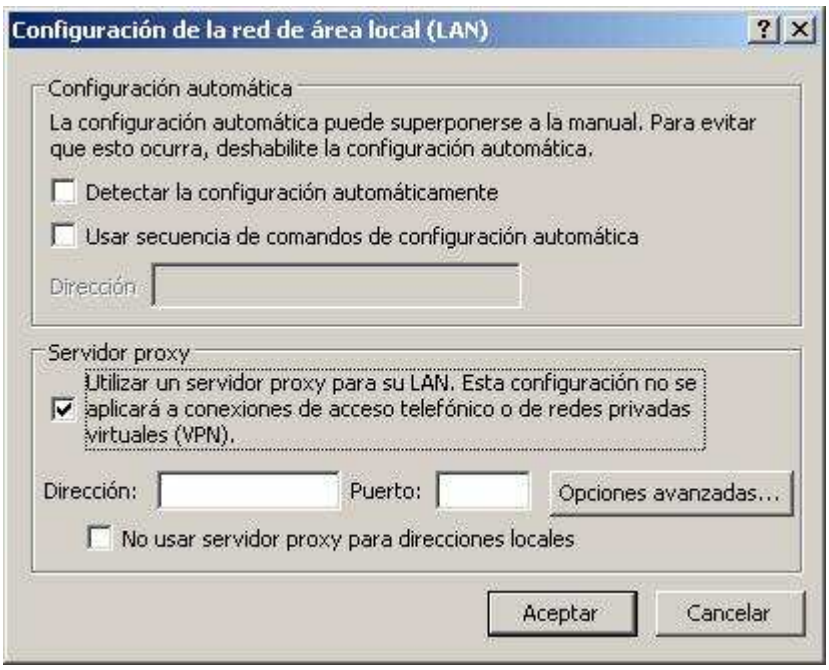


Imagen: ISA\salien21.JPG

A continuación deberemos indicar aquellos servicios para los cuales utilizaremos el proxy, especificando únicamente en nuestro caso el acceso a páginas web mediante el protocolo "HTTP", tecleando en las correspondientes cajas de texto "Dirección del servidor proxy" y "Puerto", los valores "servidor.micentro.edu" y "8080", tal y como vemos en la imagen inferior, tras lo cual iremos cerrando las ventanas que tuviéramos aun abiertas, pulsando sobre sus respectivos botones "Aceptar".

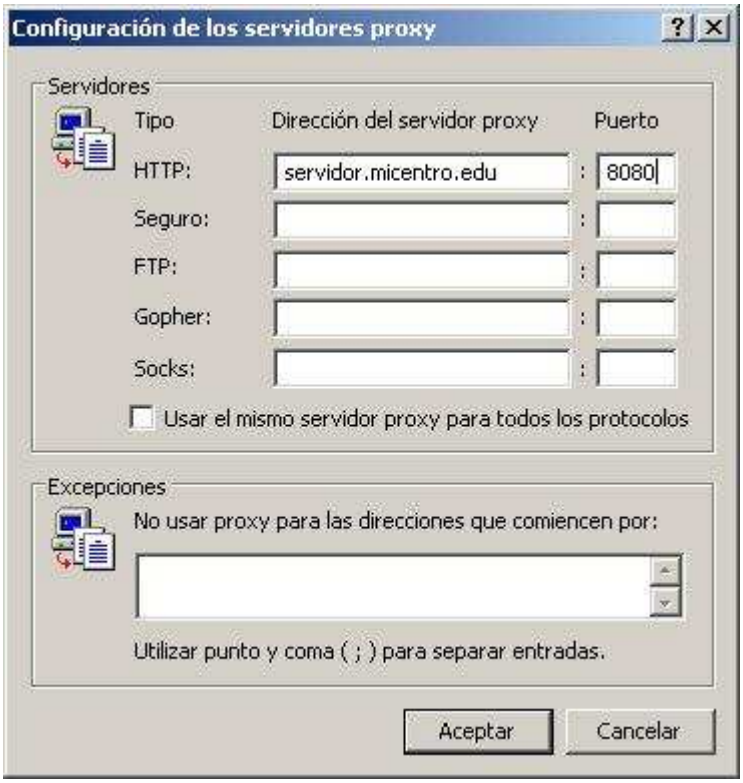


Imagen: ISA\salien22.JPG

NOTA: El proxy del servidor "ISA Server 2004" utiliza por defecto el puerto "8080" para escuchar peticiones, si bien podríamos cambiar dicha configuración si el puerto indicado estuviera ocupado por otro servicio.

A partir de este instante, el usuario que realizó la configuración anterior en el equipo cliente correspondiente, utilizará el proxy-caché del equipo "SERVIDOR" para su salida a Internet.

Si deseamos realizar la configuración anterior para todos los usuarios del dominio, de modo que éstos utilicen el proxy-caché para la salida a Internet, en el equipo "SERVIDOR" deberíamos editar el objeto directiva de grupo "Default Domain Policy" del dominio "MiCentro.edu" desde "Usuarios y equipos de Active Directory", para modificar la directiva "Configuración de los servidores proxy" ubicada en "Configuración de usuario -> Configuración de Windows -> Mantenimiento de Internet Explorer -> Conexión", asociándole las configuraciones mostradas en la imagen siguiente.

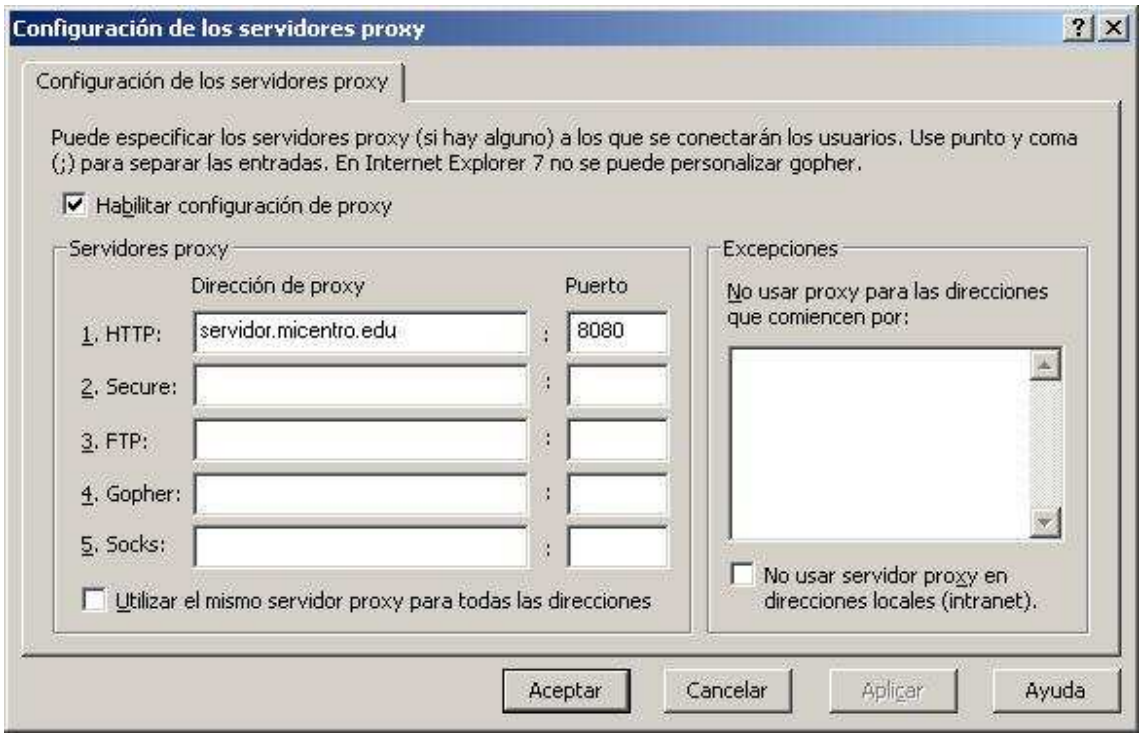


Imagen: ISA\salien23.JPG

NOTA: La directiva de grupo anterior, podría complementarse habilitando otra directiva de grupo denominada "Deshabilitar el cambio de configuración del proxy", ubicada en "Configuración de usuario -> Plantillas administrativas -> Componentes de Windows -> Internet Explorer", pues esta directiva de grupo evitaría que los usuarios pudieran modificar las configuraciones del proxy en el navegador de los equipos clientes.

Llegados a este punto vamos a indicar como llevar a cabo algunas configuraciones adicionales en el servidor "ISA Server 2004" para la salida a Internet, si bien realmente dichas

configuraciones no tengan mucho sentido en el ámbito de un centro educativo.

Otra posible configuración que puede resultar interesante es limitar el acceso a Internet desde la red interna a determinadas páginas, a determinados usuarios, a determinados equipos, o a determinadas horas.

Por ejemplo, supongamos que deseamos que las páginas del dominio de Canal Plus ("cplus.es") no sean accesibles desde la red interna de nuestro centro, para lo cual deberemos crear una nueva regla pulsando con el botón derecho del ratón sobre las "Directivas de firewall (SERVIDOR)" de la matriz "SERVIDOR", y seleccionando la opción "Nuevo", y luego "Regla de acceso" en los desplegables correspondientes.

Como resultado de la acción llevada a cabo en el párrafo anterior, pasa a ser mostrada la primera ventana del asistente de creación de nueva regla, en la cual indicaremos "Canal Plus" como nombre para la nueva regla que estamos creando.

Imagen: ISA\salien24.JPG

En la siguiente ventana dejaremos activado el radio botón "Denegar", y pulsaremos en ella directamente sobre el botón "Siguiente".

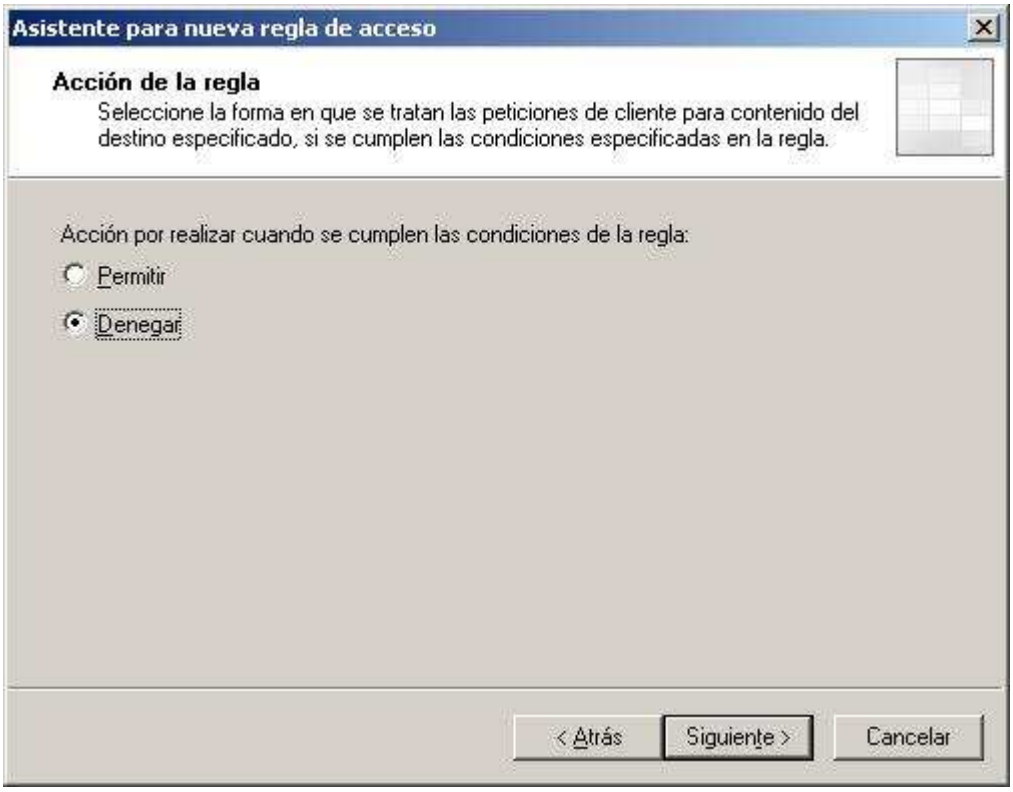


Imagen: ISA\salien25.JPG

En la siguiente ventana debemos especificar los protocolos a los que afectará la regla en cuestión, así pues en la lista desplegable correspondiente seleccionaremos la opción deseada, en nuestro caso "Todo el tráfico saliente", y a continuación pulsaremos sobre el botón "Siguiente".

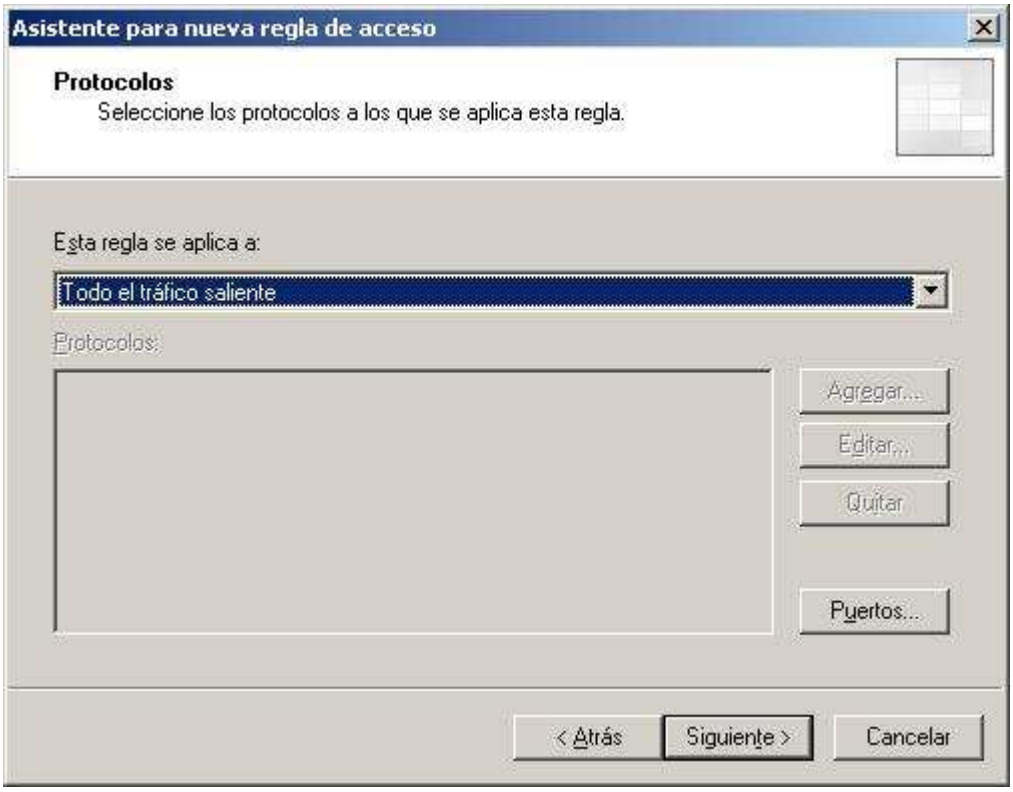


Imagen: ISA\salien26.JPG

En la siguiente ventana deberemos especificar los orígenes a los cuales será aplicada esta regla, para lo cual pulsaremos sobre el botón "Agregar", y en la nueva ventana mostrada haremos clic sobre la carpeta "Redes" para seleccionar "Interna", de modo que finalmente la ventana de selección del origen de la regla de acceso deberá quedar tal y como se muestra en la siguiente imagen.

Imagen: ISA\salien27.JPG

En la siguiente ventana deberemos especificar los destinos a los cuales será aplicada esta regla, para lo cual pulsaremos en ella sobre el botón "Agregar", pasando a ser mostrada la siguiente ventana, en la que haremos clic sobre la opción "Nuevo" del menú principal, y luego sobre "Conjunto de direcciones URL" en el desplegable correspondiente, tal y como vemos en la imagen inferior.

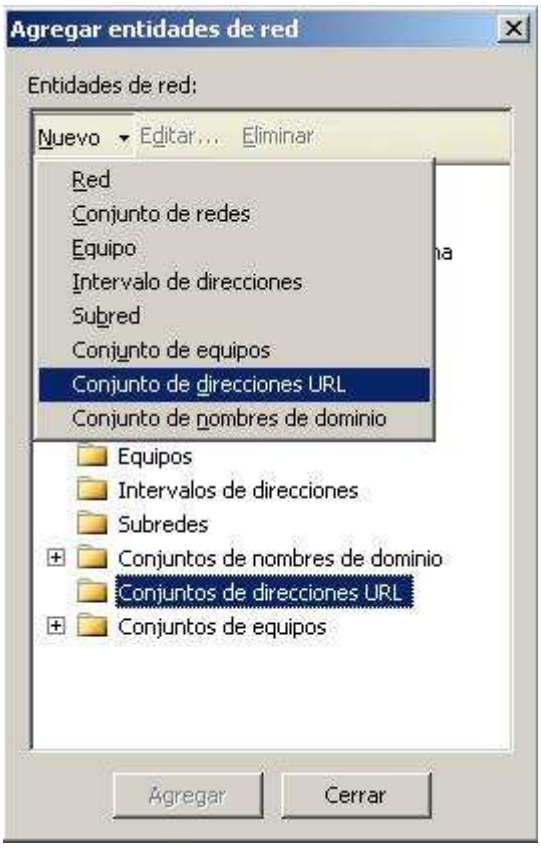


Imagen: ISA\salien28.JPG

Como resultado de la acción anterior se nos presenta la siguiente ventana, en la que teclearemos "Canal Plus" en la caja de texto "Nombre", y a continuación pulsaremos sobre el botón "Agregar" para especificar las direcciones URL a excluir, la cadena "*.cplus.es" en nuestro caso, para que dicha regla abarque a todo el dominio de "Canal Plus", de modo que cuando dicha ventana presente el aspecto mostrado en la imagen inferior, pulsaremos en ella sobre el botón "Aceptar".

Imagen: ISA\salien29.JPG

NOTA: La regla anterior abarca a todo el dominio "cplus.es"; si sólo deseáramos evitar el acceso a una determinada página web de dicho dominio, por ejemplo a la página web "http://www.cplus.es", especificaremos dicha URL en la ventana de la imagen superior.

De vuelta a la ventana anterior de "Agregar entidades de red", seleccionamos la nueva dirección URL "Canal Plus", abriendo la carpeta "Conjuntos de direcciones URL", y pulsando posteriormente sobre el botón "Agregar".

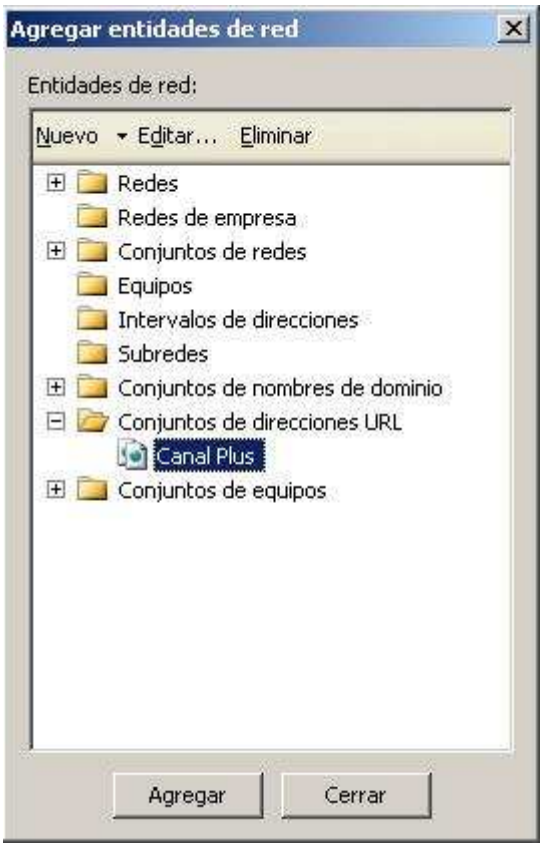


Imagen: ISA\salien30.JPG

Finalmente la ventana correspondiente al destino de la nueva regla debería quedar tal y como se muestra en la siguiente imagen, momento en el que pulsaremos sobre el botón "Siguiente" para continuar el proceso de creación de la nueva regla de acceso.

Imagen: ISA\salien31.JPG

La siguiente ventana nos permite especificar los usuarios a los cuales será aplicada esta regla, si bien en nuestro caso daremos por válida la opción "Todos los usuarios", ofertada por defecto por el asistente, y pulsaremos directamente en ella sobre el botón "Siguiente".

Imagen: ISA\salien32.JPG

Completaremos el proceso de creación de nueva regla pulsando sobre el botón "Finalizar" en la siguiente ventana.

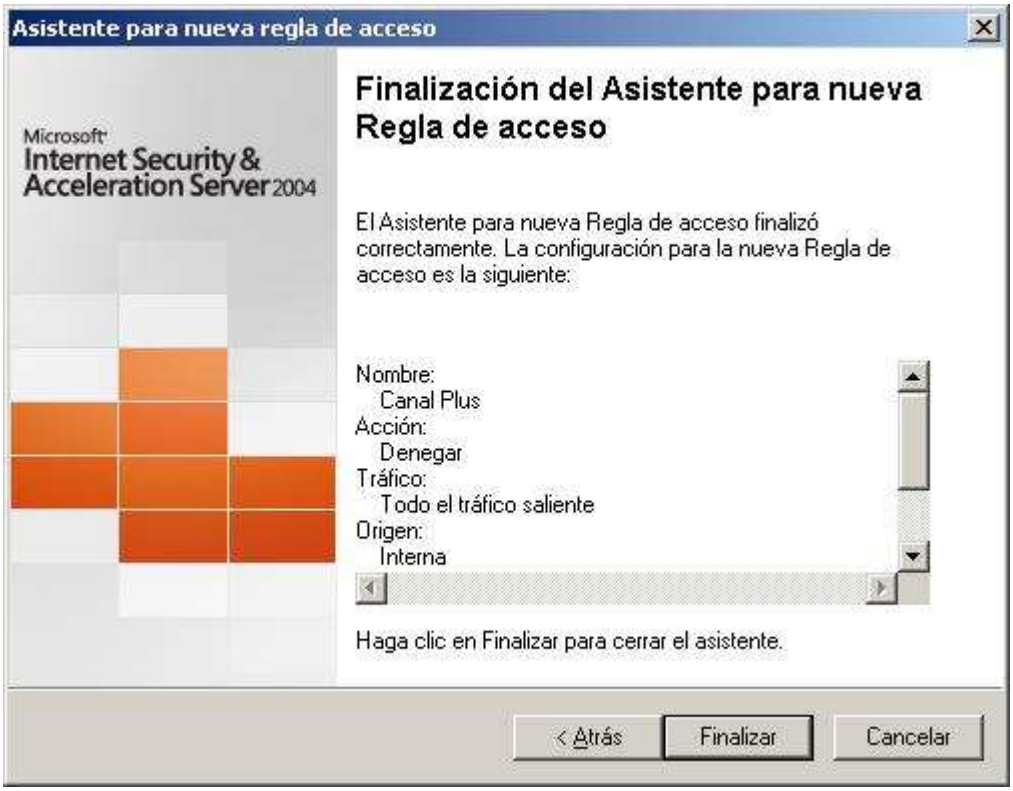


Imagen: ISA\salien33.JPG

Una vez completada la configuración de la nueva regla creada, y antes de pulsar sobre el botón "Aplicar" para que la regla de acceso definida pase a tener efecto, hemos de fijarnos en cómo están ordenadas las reglas existentes.

Podremos comprobar que el servidor "ISA Server 2004" aplica las reglas basándose en el orden numérico en el que están colocadas, de modo que cuando se encuentre una regla de acceso válida, es decir que cumpla las condiciones de la solicitud realizada, pasará a aplicarla, y NO evaluará las reglas posteriores existentes.

Así pues, tal cual tenemos actualmente situadas las reglas nunca llegaría a aplicarse la regla de denegación de acceso al dominio de "Canal Plus", pues antes de ella está colocada la regla "Trafico WAN" que permite todo el tráfico hacia la WAN, y como dicha regla sería válida para la solicitud de acceso a "Canal Plus" realizada desde un cliente, nunca llegaría a aplicarse la regla de denegación de acceso a "Canal Plus".

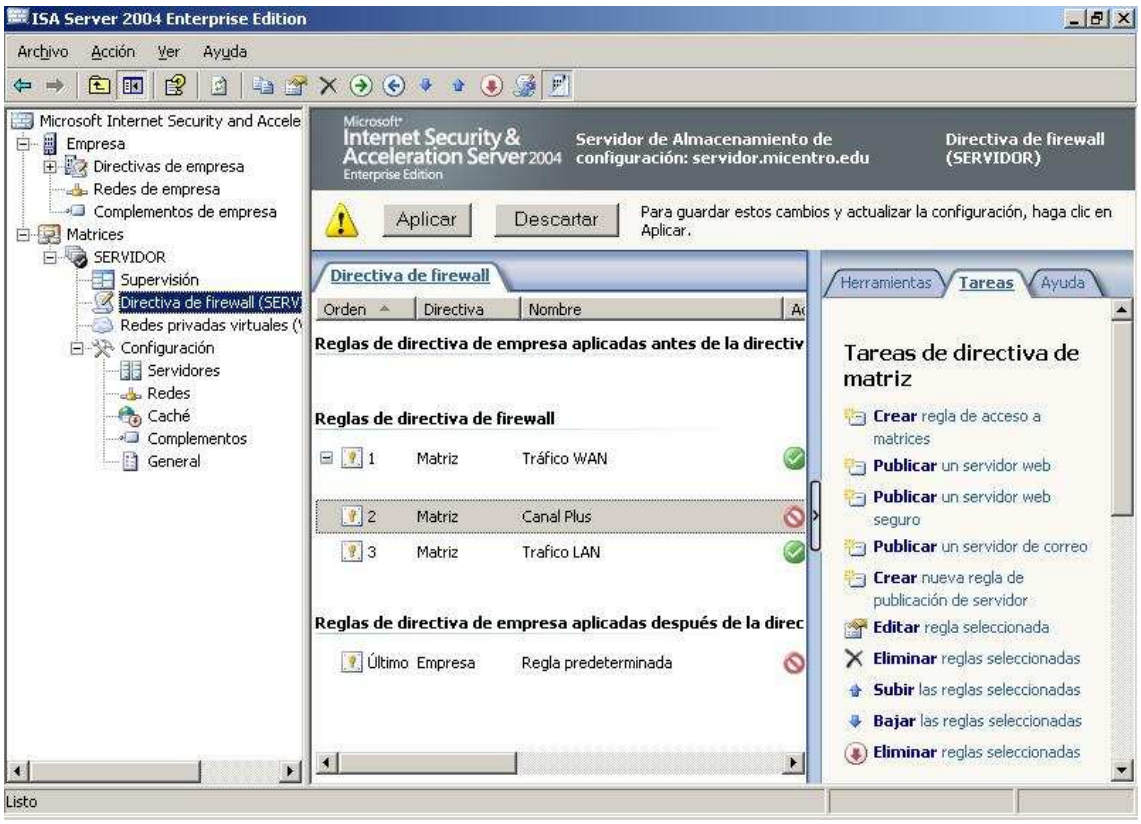


Imagen: ISA\salien34.JPG

Según lo comentado en el párrafo anterior, hemos de modificar el orden en el cual "ISA Server 2004" debe analizar las reglas, para lograr que la regla de denegación de acceso al dominio de "Canal Plus" esté ubicada antes que la regla "Trafico WAN", para que sea efectiva e imposibilite el acceso a las páginas de "Canal Plus" desde los equipos clientes de la red de nuestro centro.

Así pues reordenaremos las reglas de acceso moviendo la regla de denegación "Canal Plus" al primer lugar, y situando la regla "Trafico WAN" en segundo lugar, proceso que llevaremos a cabo pulsando con el botón derecho del ratón sobre la regla "Canal Plus", y seleccionando la opción "Subir" en el desplegable correspondiente.

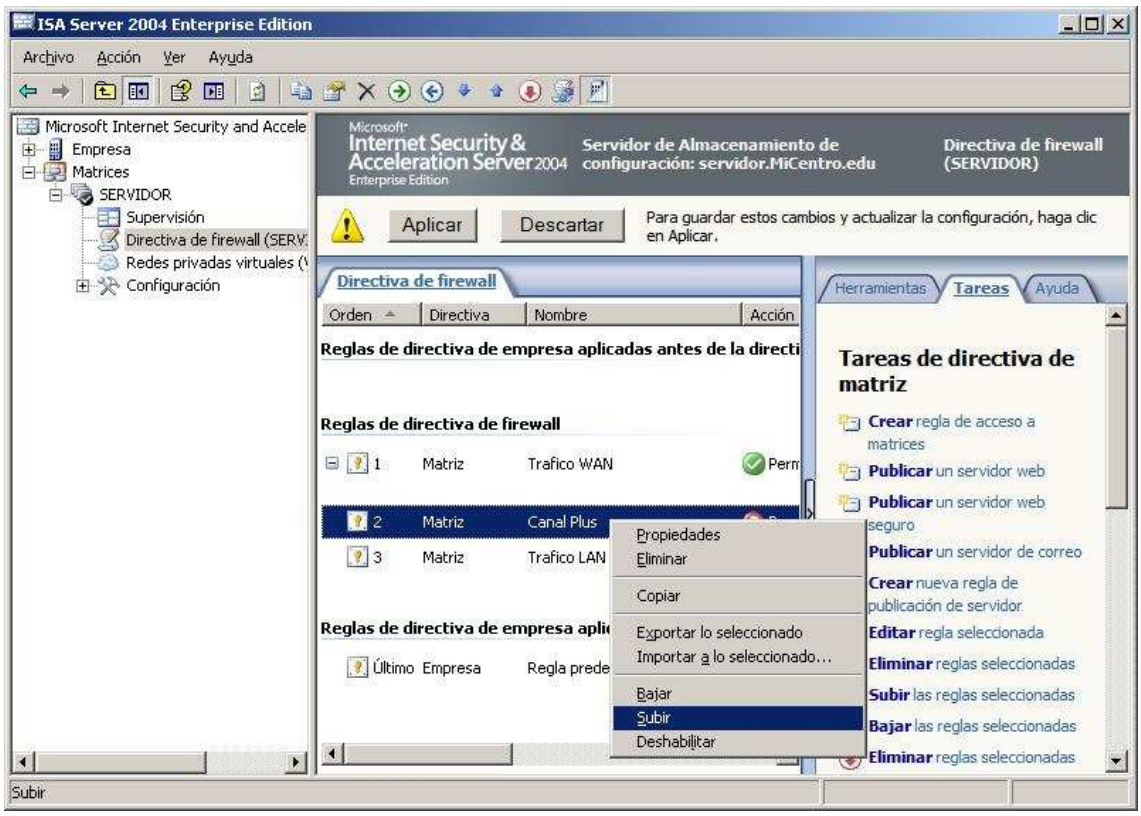


Imagen: ISA\salien35.JPG

Tras ello observaremos que la regla "Canal Plus" ha pasado al primer lugar de la lista, así pues ahora sí podremos pulsar sobre el botón "Aplicar" para que la regla pase a ser plenamente efectiva.

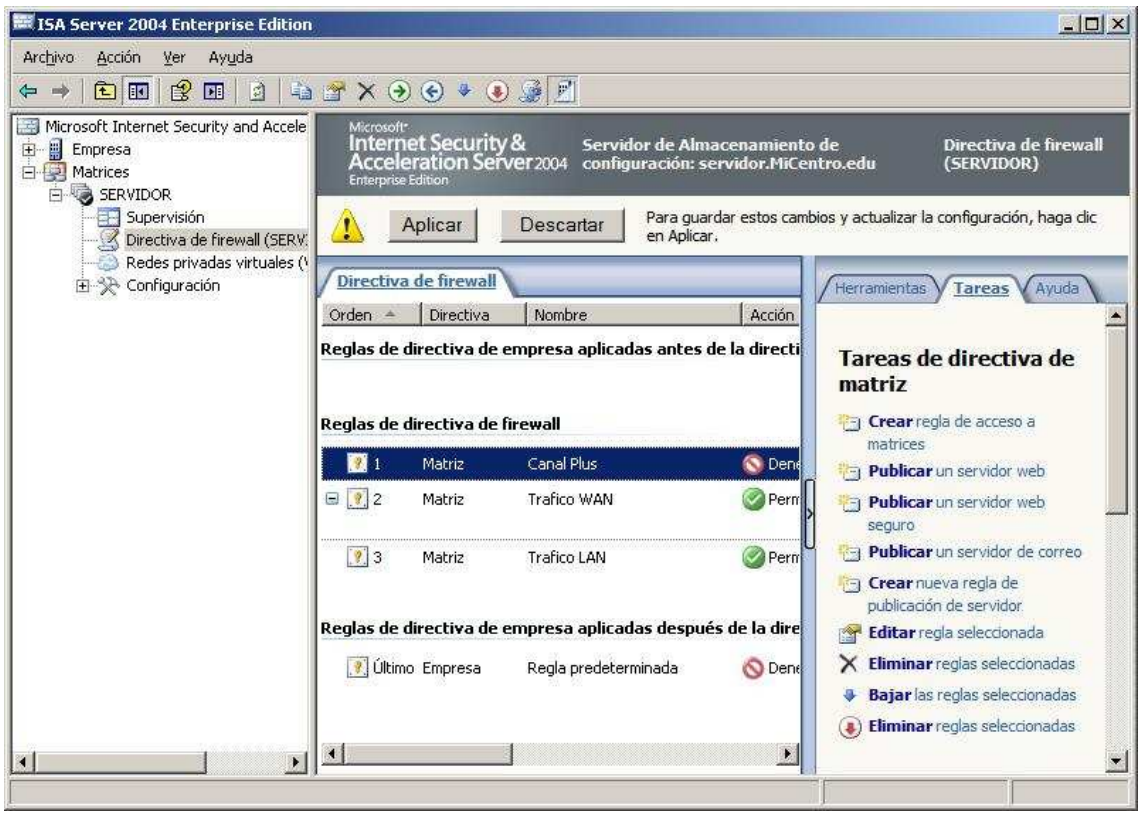


Imagen: ISA\salien36.JPG

A partir de este instante, si desde un equipo cliente del dominio intentáramos el acceso a la URL "http://www.cplus.es", obtendríamos como respuesta la siguiente página web que nos mostraría el proxy-caché del "ISA Server 2004", y en la que nos indica literalmente "El servidor ISA rechazó la dirección URL (Uniform Resource Locator) especificada".

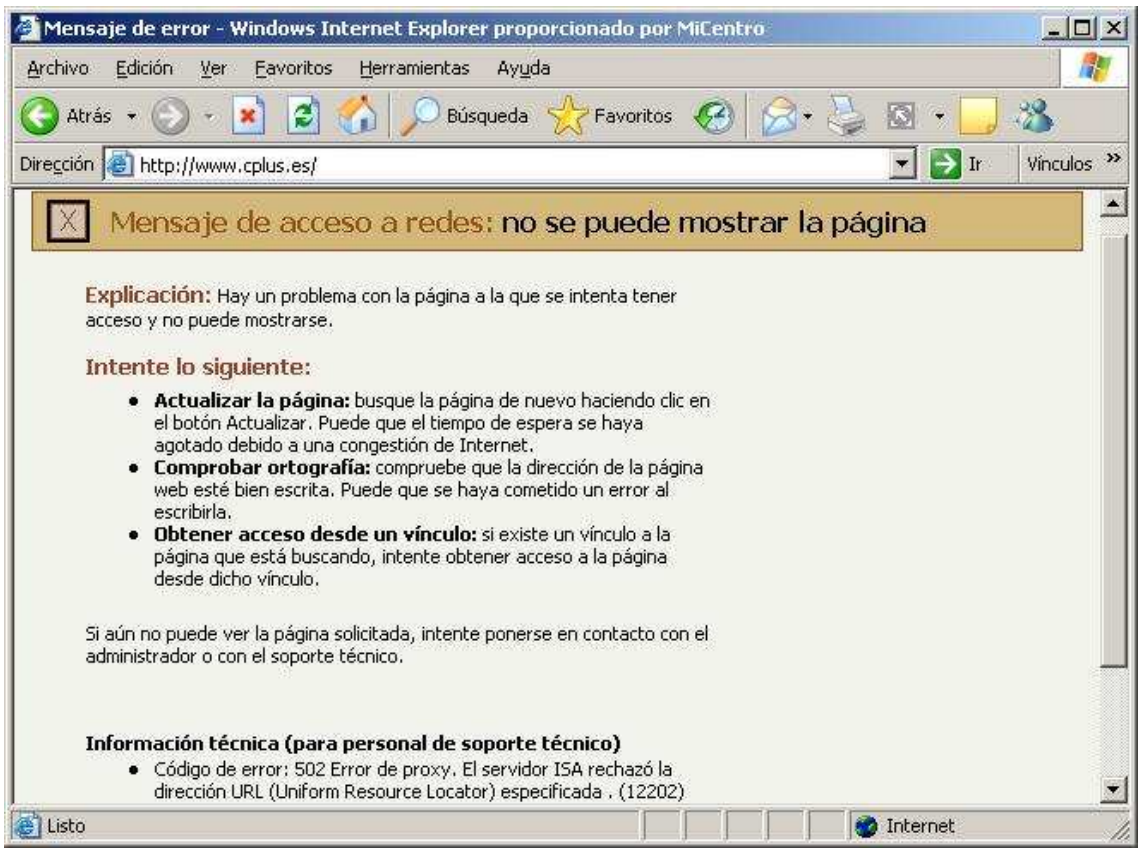


Imagen: ISA\salien37.JPG

NOTA: No es posible realizar una indicación válida para ordenar las reglas de "ISA Server 2004" de modo adecuado para que hagan lo que deseemos, pero con carácter general deberemos situar al final las reglas más generales y al principio las más particulares, tal y como hemos hecho en el ejemplo comentado.

Otra situación que podría darse en nuestro centro es que los accesos a Internet se hagan de forma indiscriminada e irracional, desaprovechando de ese modo el ancho de banda existente para la salida a Internet, imposibilitando que otros usuarios de nuestra red que desean hacer uso correcto del servicio, no puedan acceder en plenitud de condiciones al mismo; en este escenario una buena opción podría ser definir una regla que imposibilite el acceso a todos los sitios de Internet a determinadas horas a ciertos usuarios o equipos.

Como muestra de cómo se debe configurar una regla de acceso para lograr lo indicado en el párrafo anterior, NO crearemos una nueva regla, sino que por ejemplo modificaremos la regla de acceso que deniega el tráfico al dominio de "Canal Plus", para que se aplique los lunes desde 13,00 horas hasta las 15,00 horas a todos los profesores del centro.

Así pues, ubicados sobre la "Directiva de firewall (SERVIDOR)" de la matriz "SERVIDOR", pulsaremos con el botón derecho del ratón sobre la regla "Canal Plus", para elegir la opción "Propiedades" en el desplegable correspondiente, tal y como vemos en la imagen inferior.

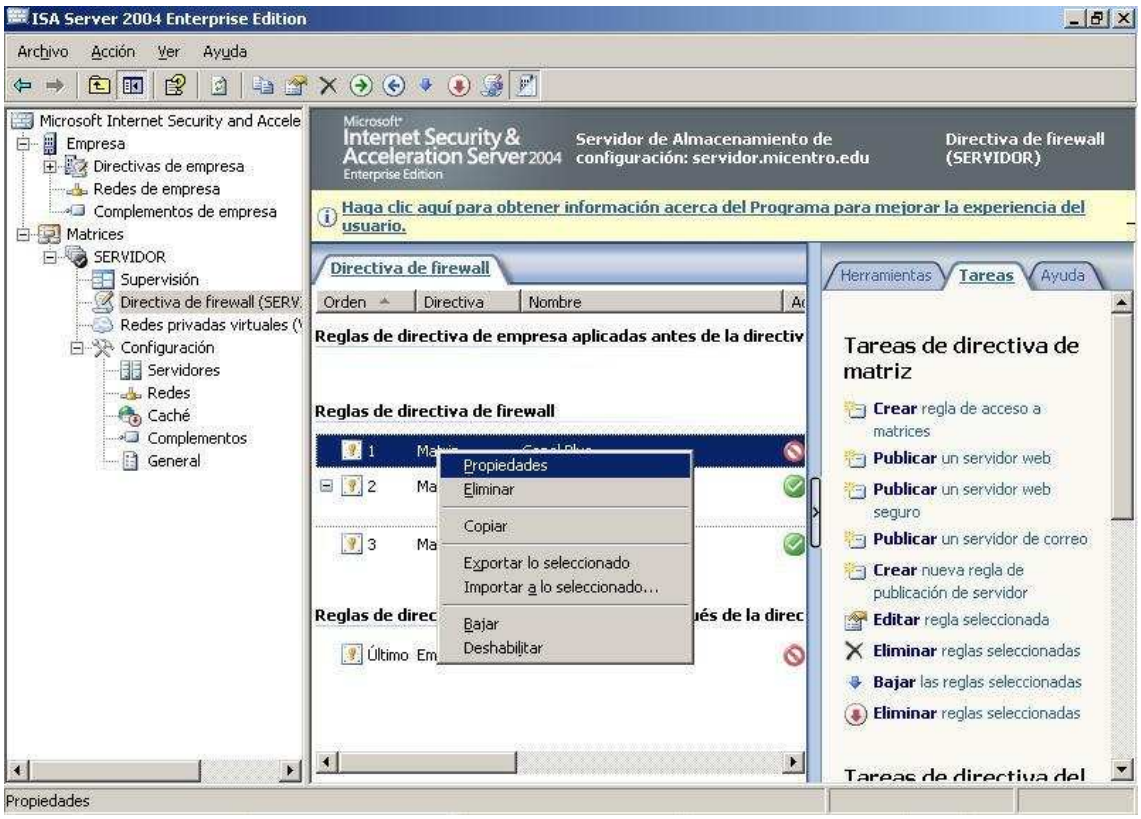


Imagen: ISA\salien38.JPG

En la ventana mostrada como resultado de la acción anterior, nos situaremos sobre la pestaña "Programación", y a continuación pulsaremos en ella sobre el botón "Nueva", pasando a ser mostrada en ese instante la siguiente ventana, en la que indicaremos como nombre de la programación "Lunes de 13 a 15", y activaremos en el calendario semanal las casillas correspondientes a dichas horas en los lunes, tal y como vemos en la imagen inferior, para finalmente pulsar sobre el botón "Aceptar".

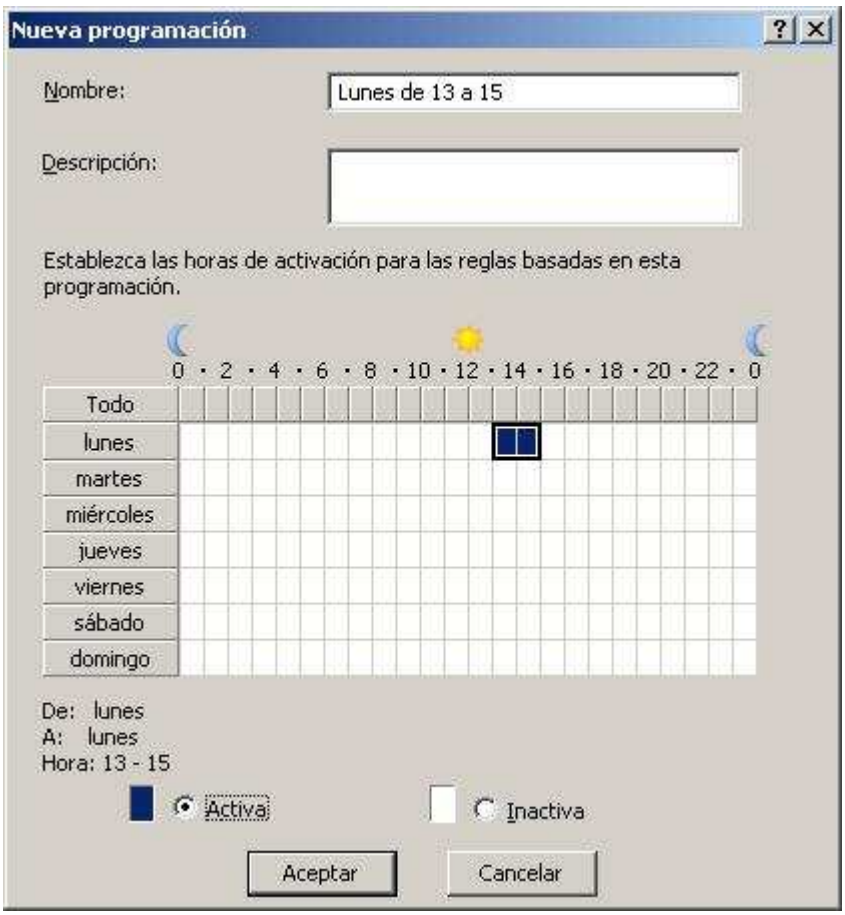


Imagen: ISA\salien39.JPG

De vuelta en la ventana de propiedades de la regla de acceso "Canal Plus", observamos que ya se está aplicando dicha regla a la programación temporal "Lunes de 13 a 15", luego sólo se negaría el acceso a las páginas de Canal Plus los lunes de 13 a 15 horas.

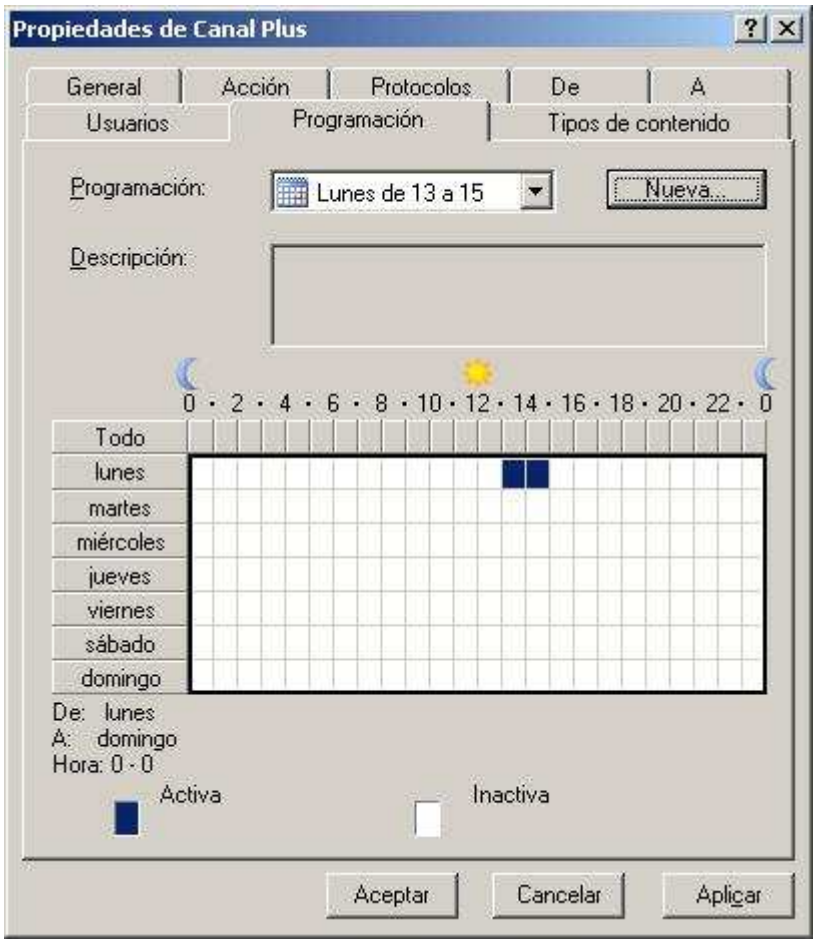


Imagen: ISA\salien40.JPG

A continuación, en la misma ventana de propiedades de la regla de acceso "Canal Plus", nos situaremos sobre la pestaña "Usuarios", y tras ello seleccionaremos al grupo "Todos los usuarios" para pulsar posteriormente sobre el botón "Quitar"; tras ello pulsaremos en dicha ventana sobre el botón "Agregar", pasando a ser mostrada la siguiente ventana de agregación de usuarios, en la que pulsaremos sobre la opción "Nuevo" de la parte superior de la misma.

Imagen: ISA\salien41.JPG

En este instante se lanza el asistente de agregación de un nuevo conjunto de usuarios, en el que indicaremos "Profesores" como nombre del nuevo conjunto de usuarios, y tras ello pulsaremos sobre el botón "Siguiente".

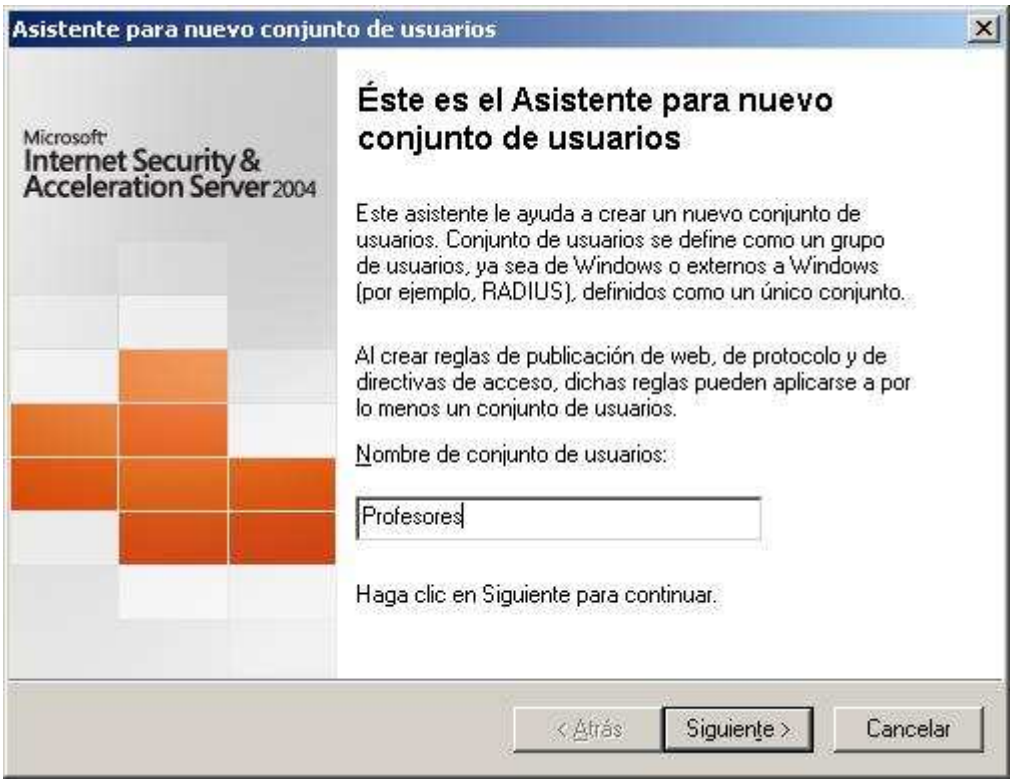


Imagen: ISA\salien42.JPG

En la nueva ventana mostrada pulsaremos sobre el botón "Agregar", y posteriormente en el desplegable adjunto seleccionamos "Usuarios y grupos de Windows", tal y como vemos en la imagen inferior.

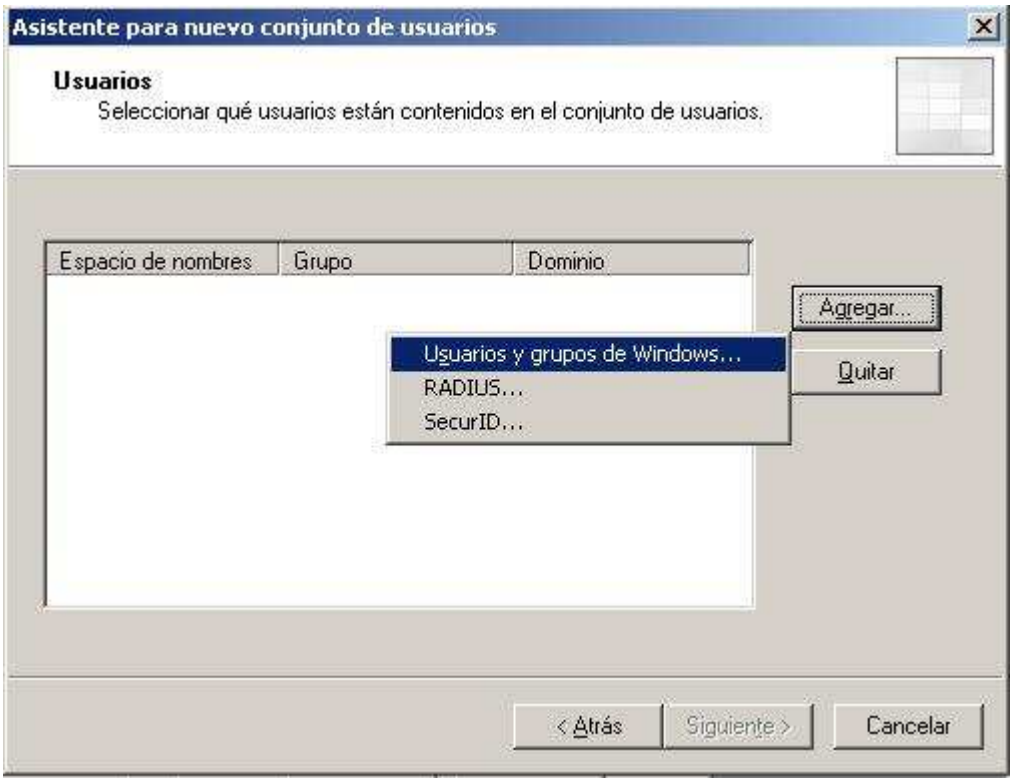


Imagen: ISA\salien43.JPG

En la nueva ventana mostrada teclearemos "Profesores", para añadir a dicho grupo al nuevo conjunto de usuarios que estamos creando para "ISA Server 2004", de modo que de vuelta a la ventana de asignación de usuarios, ésta presente el aspecto mostrado en la imagen inferior, momento en el cual pulsaremos en ella sobre el botón "Siguiente".

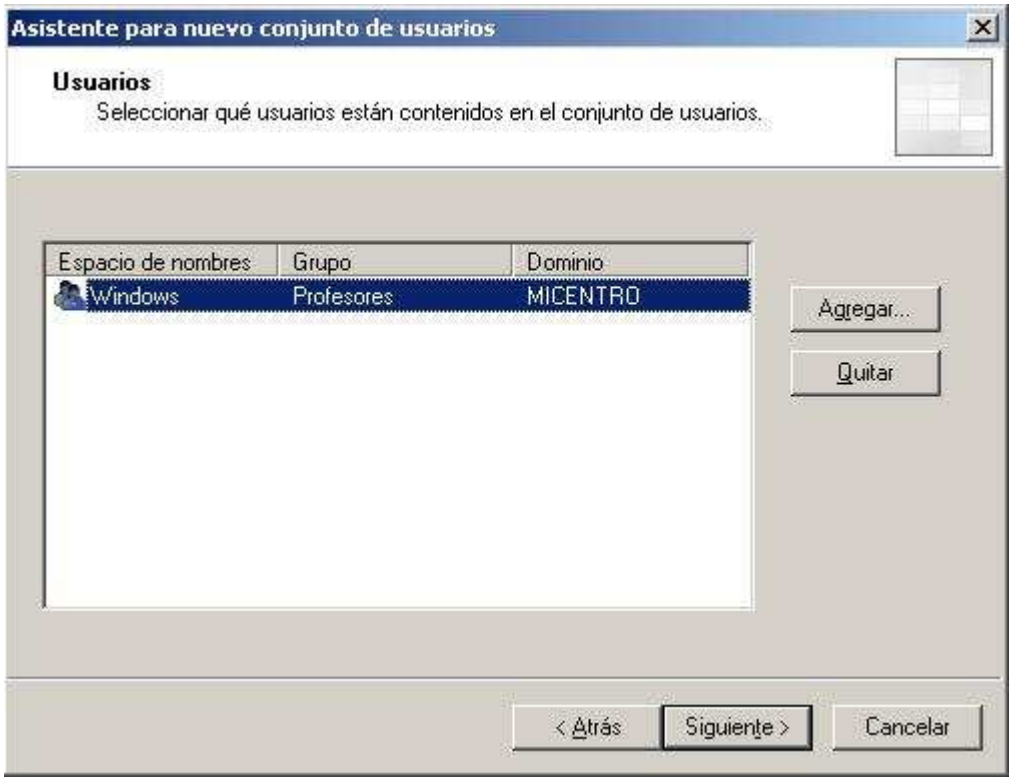


Imagen: ISA\salien44.JPG

Terminamos la definición del nuevo grupo de usuarios pulsando en la siguiente ventana sobre el botón "Finalizar".

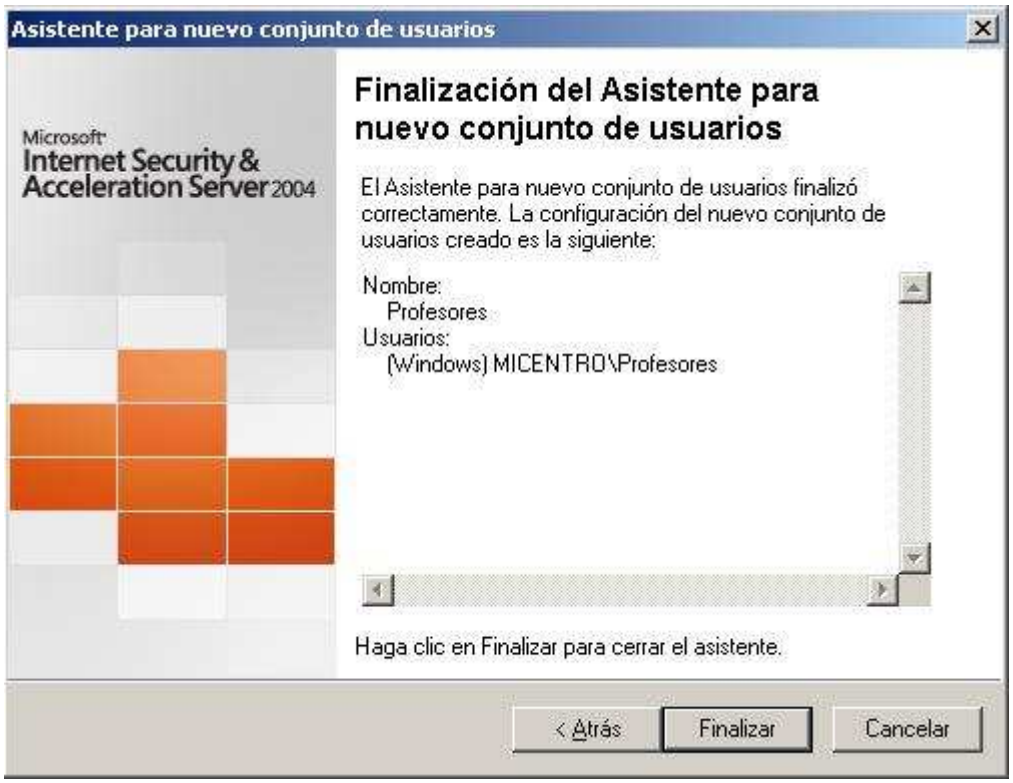


Imagen: ISA\salien45.JPG

Tras completar la acción anterior volveremos a la ventana de "Agregar usuarios", donde ya se mostrará el grupo "Profesores", así pues lo seleccionaremos y tras ello pulsaremos sobre el botón "Agregar".

Imagen: ISA\salien46.JPG

Así pues finalmente en la ventana de usuarios de la regla de "Canal Plus", deberá mostrarse únicamente al grupo "Profesores", tal y como vemos en la imagen inferior.

Imagen: ISA\salien47.JPG

Tras ello deberemos pulsar sobre el botón "Aplicar" para que los cambios pasen a ser efectivos, momento a partir del cual los miembros del grupo "Profesores" del dominio "MiCentro.edu", los lunes de 13 a 15 horas no podrán acceder a las páginas de "Canal Plus".

NOTA: Si desde un equipo cliente intentamos el acceso a la página web "http://www.cplus.es", el servidor "ISA Server 2004" asumirá como válidas las credenciales del usuario del dominio que se haya validado en sesión en dicho equipo cliente, para comprobar si dicho usuario es un profesor o no, a fin de permitirle o denegarle el acceso a la página web en cuestión a partir de la regla configurada.

Peticiones Entrantes

En el apartado anterior configuramos el servidor "ISA Server 2004" para que las peticiones de salida a Internet desde la red de nuestro centro funcionaran correctamente, y en este apartado analizaremos el modo en que deberemos configurar nuestro servidor "ISA Server 2004" para lograr el acceso desde Internet a los servicios prestados en la red interna de nuestro centro, configurando para ello las oportunas reglas de publicación.

Lo primero que hemos de tener en cuenta es que instalar el servidor "ISA Server 2004" sobre el mismo equipo donde se encuentran ubicados los servidores que vamos a publicar que no es una buena política de seguridad, pues el nivel de seguridad que se alcanza es menor que si ubicáramos los servidores a publicar (Web, FTP, correo, etc.) en equipos distintos del ordenador donde está instalado el "ISA Server 2004", de modo que dichos servidores deberían encontrarse en una zona intermedia y aislada de la LAN y la WAN, que normalmente se denomina DMZ (red desmilitarizada), de modo que con esta configuración el equipo "SERVIDOR" debería disponer de 3 tarjetas de red, una hacia la LAN, otra hacia la DMZ y una tercera hacia la WAN, tal y como se muestra en la siguiente imagen.

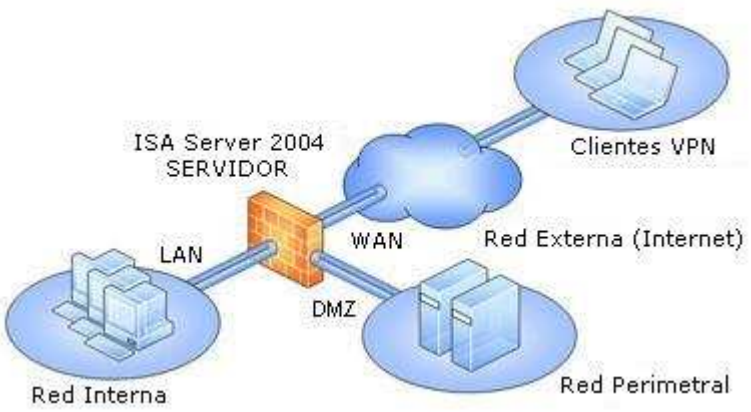


Imagen: ISA\entran01.JPG

En nuestro caso, dado que disponemos de un único equipo "SERVIDOR" que se va a situar entre la LAN y la WAN, NO crearemos una DMZ, pues los servidores (Web, FTP, correo, etc.) se encuentran instalados en el mismo equipo en el que hemos instalado "ISA Server 2004", pudiendo ser accedidos desde la LAN (proceso analizado en el apartado anterior), y desde la WAN (proceso que analizaremos en este apartado), de modo que con esta configuración el equipo "SERVIDOR" debería disponer de 2 tarjetas de red, una hacia la LAN y otra hacia la WAN, tal y como se muestra en la siguiente imagen.

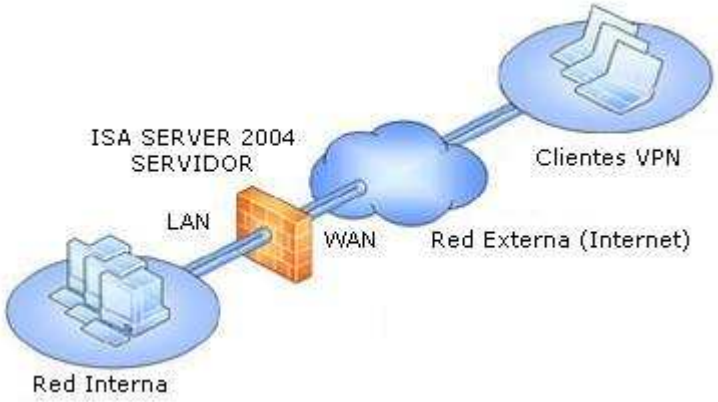


Imagen: ISA\entran02.JPG

Esta configuración de "ISA Server 2004", desde el punto de vista de la seguridad, es peor que si los servidores a publicar estuvieran ubicados físicamente en la DMZ, en equipos distintos del

equipo donde hemos instalado "ISA Server 2004", y además dado que en la misma máquina existen sitios web escuchando en el puerto 80 (en nuestro caso los sitios web "servidor.micentro.edu" y "www.micentro.edu"), esta configuración va a provocar que las reglas de publicación de servidores web del "ISA Server 2004", que por defecto utilizan dicho puerto, deban ser configuradas en otro puerto diferente para su acceso desde Internet, como posteriormente veremos.

NOTA: Si el servidor IIS estuviera instalado en un equipo distinto del equipo donde está instalado el "ISA Server 2004", y dicho servidor IIS tuviera algún servidor web escuchando en el puerto 80, el problema indicado en el párrafo anterior NO se produciría, pues cada tarjeta de red (la del equipo que tiene instalado el servidor IIS y la del equipo que tiene instalado "ISA Server 2004") que escucha en el puerto 80 lo harían para servicios diferentes.

Así pues, llegado a este punto, vamos a proceder a configurar diversas reglas de publicación para hacer accesibles ciertos servicios del equipo "SERVIDOR" desde Internet a través del servidor "ISA Server 2004".

El primer servicio que vamos a configurar es el servicio "Terminal Server", para habilitar el acceso desde Internet al equipo "SERVIDOR" a través de Escritorio Remoto, para lo cual nos situaremos sobre la entrada "Directiva de firewall (SERVIDOR) de la matriz "SERVIDOR", pulsando sobre la misma con el botón derecho del ratón para elegir la opción "Nuevo", y luego "Regla de publicación de servidor" en los desplegables correspondientes.

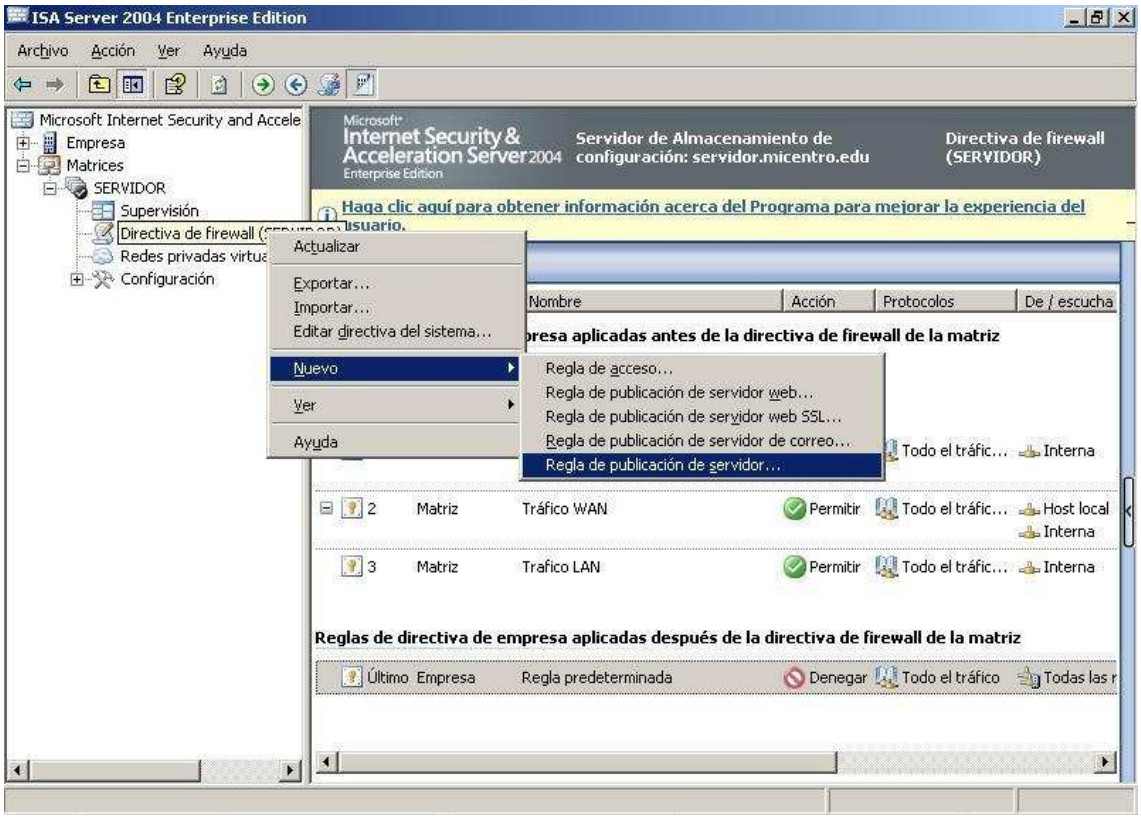


Imagen: ISA\entran03.JPG

Como resultado de dicha acción pasa a ser mostrada la primera ventana del asistente de

creación de nueva regla de publicación, en la que indicaremos como nombre para esta regla "Terminal Server", y tras ello pulsaremos sobre el botón "Siguiente".

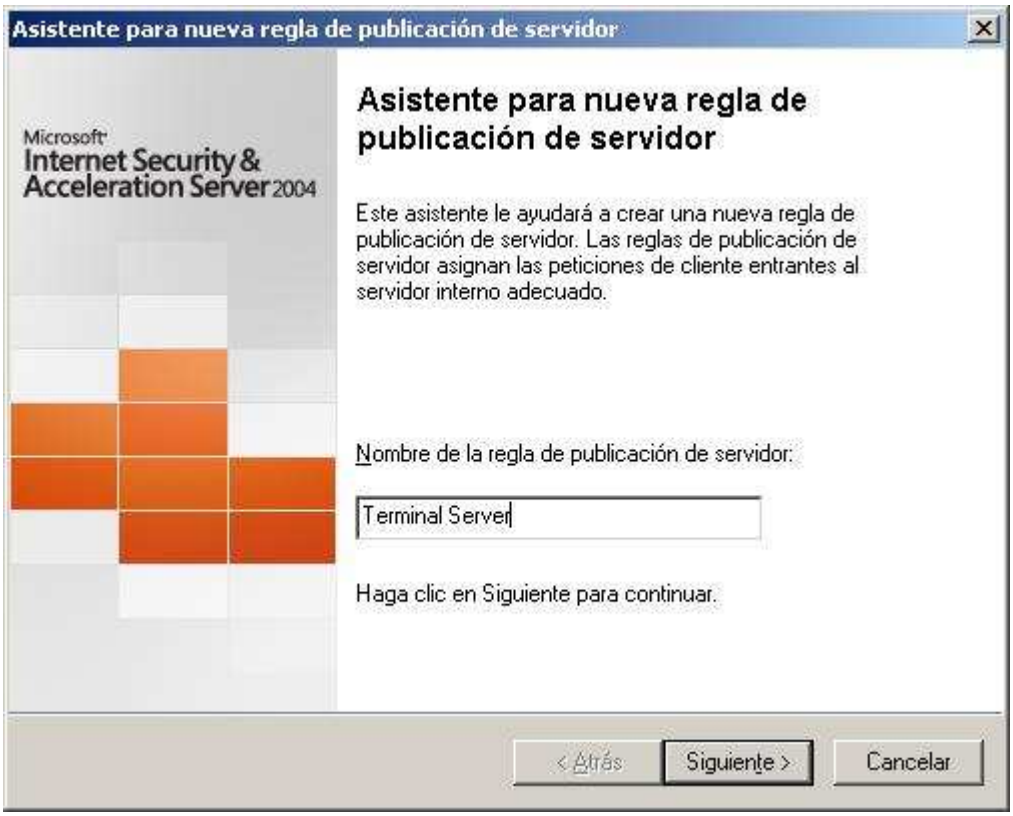


Imagen: ISA\entran04.JPG

A continuación deberemos especificar en la siguiente ventana la dirección IP del interfaz de red externo del equipo "SERVIDOR", en nuestro caso deberemos teclear "192.168.0.220", la dirección IP del interfaz de red "Conexión WAN", y tras ello pulsar sobre el botón "Siguiente".

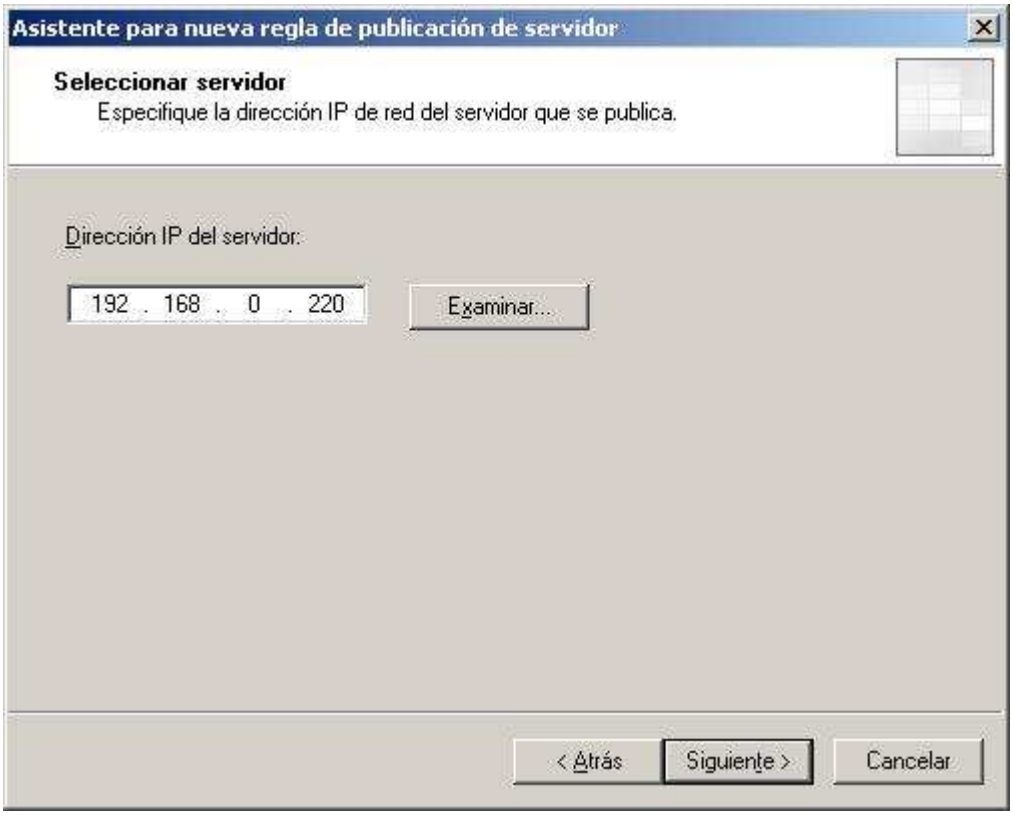


Imagen: ISA\entran05.JPG

En la siguiente ventana deberemos especificar el protocolo al cual deseamos acceder de modo remoto, seleccionando en este caso la opción "Servidor RDP (Servicios de Terminal Server)" en la lista desplegable correspondiente, y pulsando tras ello sobre el botón "Siguiente".

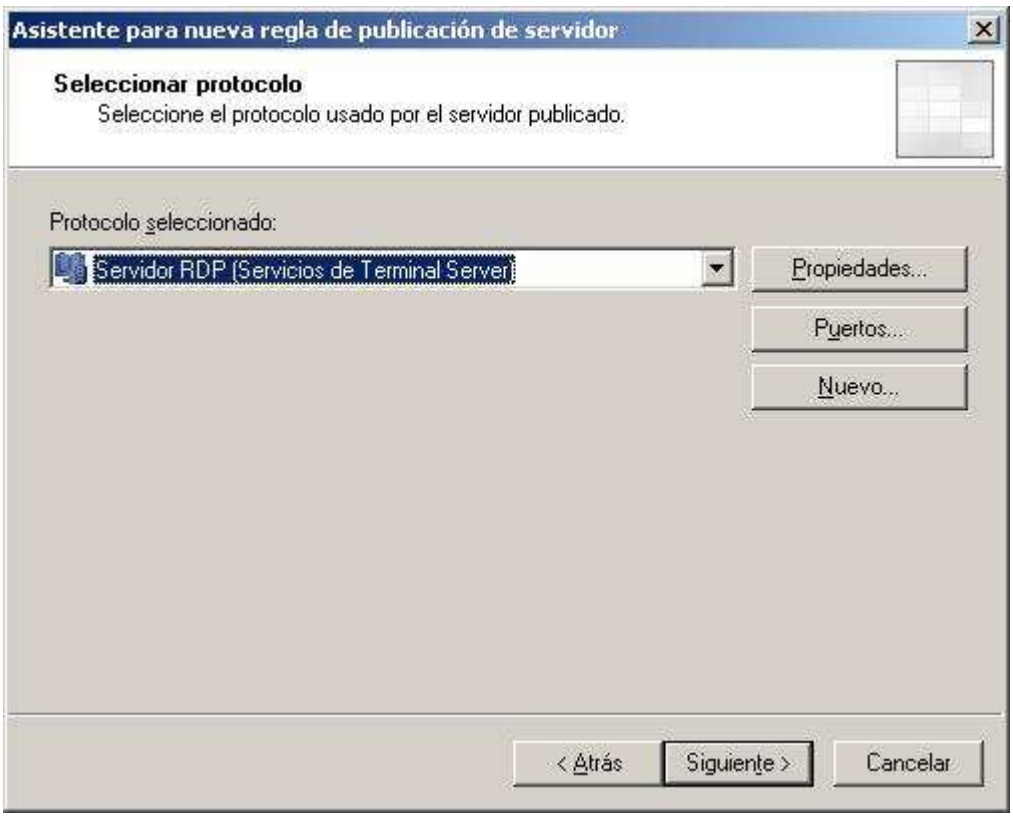


Imagen: ISA\entran06.JPG

NOTA: SI el protocolo a definir NO estuviera en la lista de la ventana anterior, podríamos definir un nuevo protocolo pulsando sobre el botón "Nuevo".

En la siguiente ventana indicaremos la red desde la que deseamos permitir dicho tipo de conexión, activando en nuestro caso la casilla "Externa", y pulsando posteriormente sobre el botón "Siguiente".

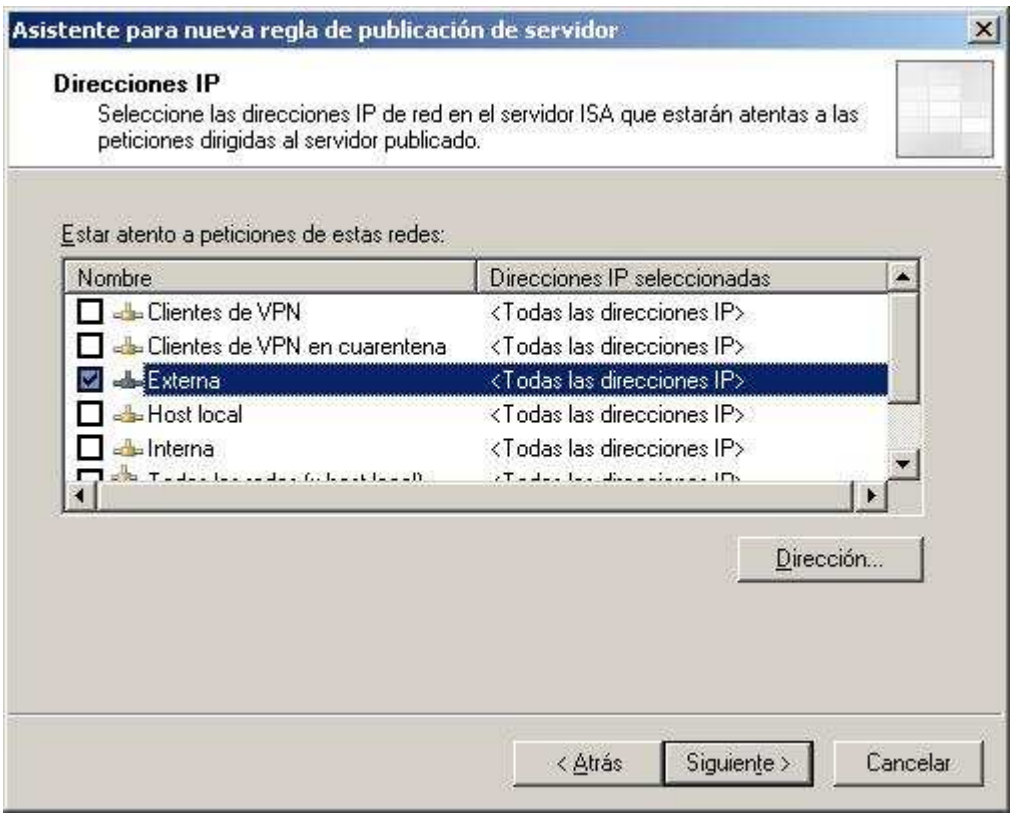


Imagen: ISA\entran07.JPG

En la última ventana del asistente pulsaremos directamente sobre el botón "Finalizar" para completar el proceso de creación de la regla de publicación correspondiente.

Imagen: ISA\entran08.JPG

Tras ello en la ventana de administración de "ISA Server 2004" observaremos la existencia de una nueva regla de publicación de servidor para el servicio "Terminal Server", debiendo recordar pulsar sobre el botón "Aplicar" para que la nueva regla creada pase a ser ejecutada de modo efectivo.

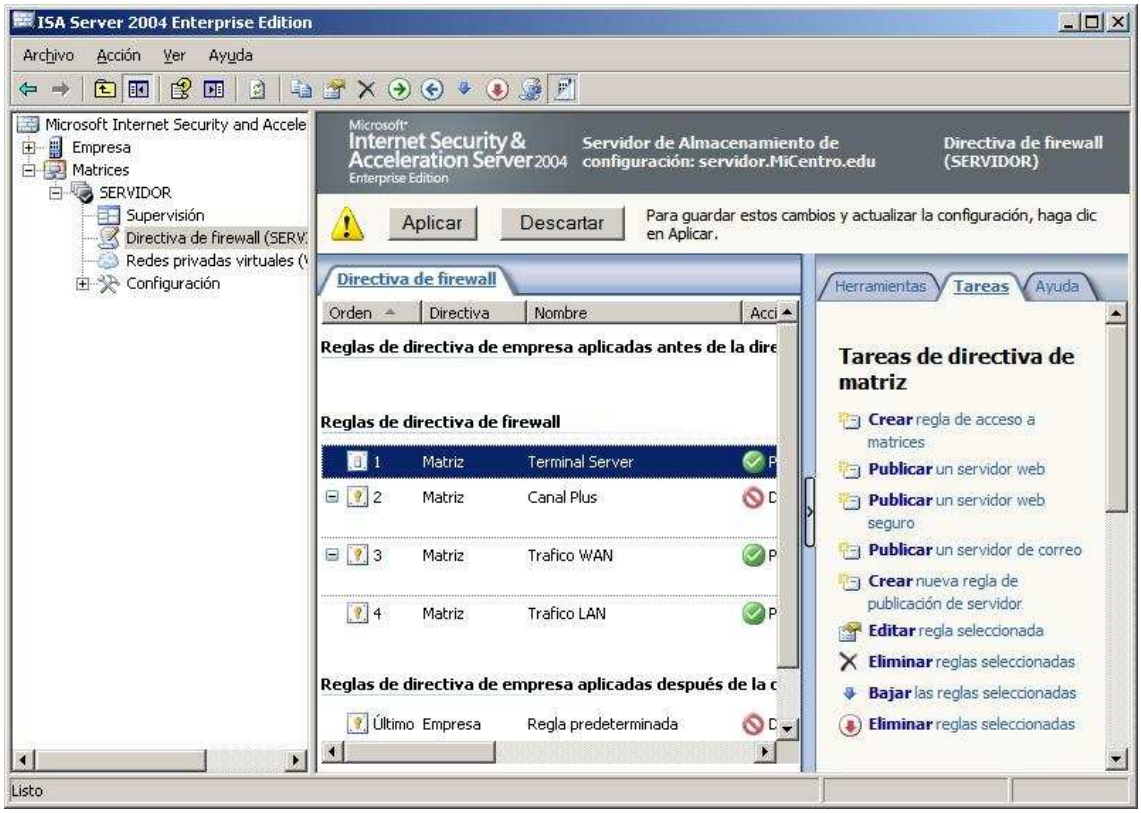


Imagen: ISA\entran09.JPG

A partir de este momento ya podríamos acceder desde Internet al equipo "SERVIDOR" por "Terminal Server" mediante el cliente de conexión a Escritorio Remoto.

Si estamos trabajando con máquinas virtuales, podremos probar fácilmente el correcto funcionamiento de la regla de publicación creada, editando para ello en primer lugar con el "Bloc de notas" el fichero "hosts" ubicado en la ruta "C:\Windows\System32\drivers\etc" del equipo ANFITRIÓN, e incluyendo al final del mismo una entrada con la dirección IP y el nombre del equipo al cual vamos a acceder ("192.168.0.220 servidor.micentro.edu SERVIDOR", tal y como vemos en la imagen inferior), y tras ello guardar los cambios realizados en dicho fichero.

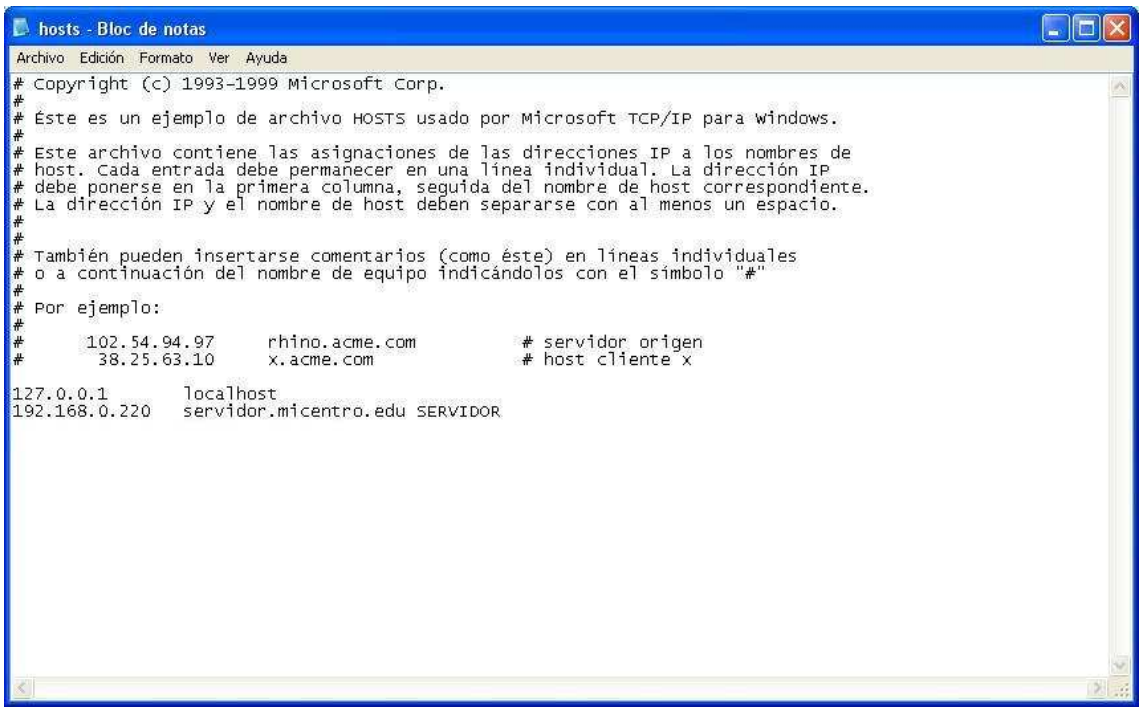


Imagen: ISA\entran10.JPG

NOTA: Dado que la resolución "servidor.micentro.edu" sólo es válida en el ámbito de la red interna de nuestro centro, debemos introducirla en el fichero de "hosts" de la máquina anfitriona desde la que vamos a acceder al servicio correspondiente para poder acceder mediante resolución en vez de mediante dirección IP.

Tras ello podremos establecer desde el equipo anfitrión una conexión de Escritorio Remoto a la máquina virtual "servidor.micentro.edu", tal y como vemos en la imagen inferior.

Imagen: ISA\entran11.JPG

La siguiente regla de publicación que vamos a definir permitirá habilitar el acceso desde Internet al sitio FTP "Sitio FTP Profesores" del servidor IIS, el cual escucha peticiones en el puerto 21 del equipo "SERVIDOR".

Para llevar a cabo lo indicado en el párrafo anterior, crearemos una nueva regla de publicación de servidor siguiendo los mismos pasos dados anteriormente para crear la regla de publicación de "Terminal Server", de modo que en la primera ventana del asistente indicaremos como nombre para dicha regla "Sitio FTP Profesores", y posteriormente pulsaremos sobre el botón "Siguiente".

Imagen: ISA\entran12.JPG

A continuación deberemos especificar en la siguiente ventana la dirección IP del interfaz de red externo del equipo "SERVIDOR", en nuestro caso deberemos teclear "192.168.0.220", la dirección IP del interfaz de red "Conexión WAN", y tras ello pulsar sobre el botón "Siguiente".

Imagen: ISA\entran13.JPG

En la siguiente ventana deberemos especificar el protocolo al cual deseamos acceder de modo remoto, seleccionando en este caso la opción "Servidor FTP" en la lista desplegable correspondiente, y pulsando tras ello sobre el botón "Siguiente".

Imagen: ISA\entran14.JPG

En la siguiente ventana indicaremos la red desde la que deseamos permitir dicho tipo de conexión, activando en nuestro caso la casilla "Externa", y pulsando posteriormente sobre el botón "Siguiente".

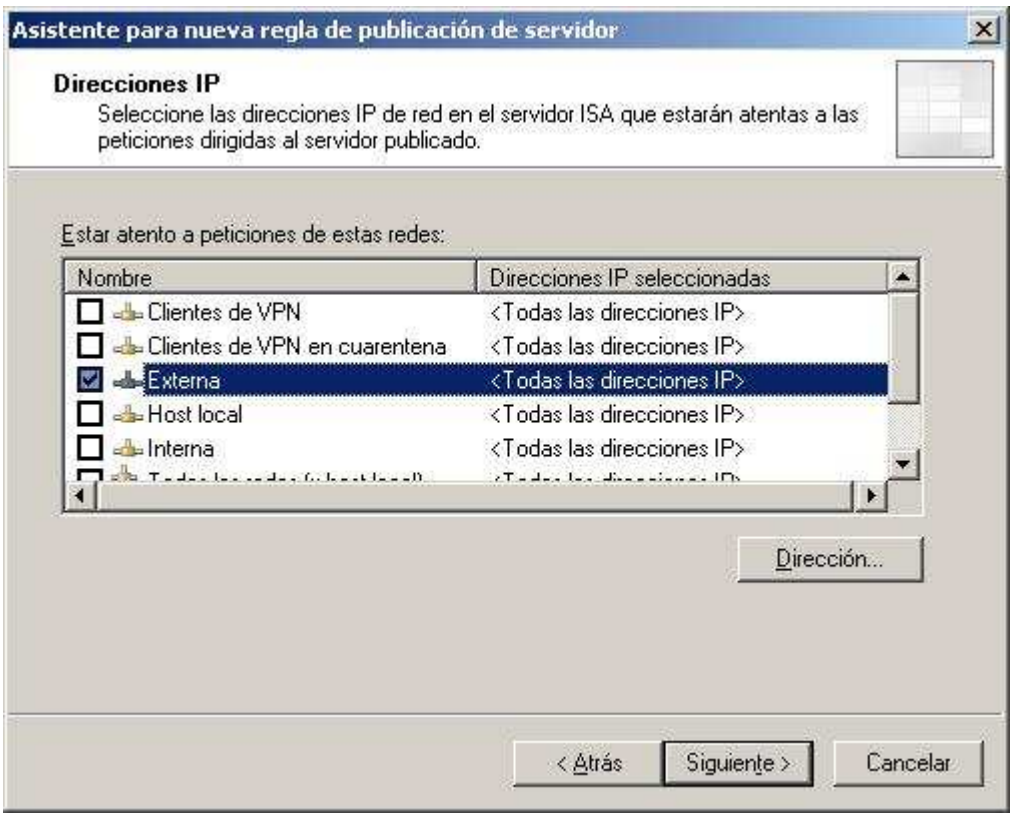


Imagen: ISA\entran15.JPG

En la última ventana del asistente pulsaremos directamente sobre el botón "Finalizar" para completar el proceso de creación de la regla de publicación correspondiente.

Imagen: ISA\entran16.JPG

Una vez completado el asistente de creación de la nueva regla de publicación "Sitio FTP Profesores", haremos doble clic sobre la misma, pasando a ser mostrada la siguiente ventana, en la que nos ubicaremos sobre la pestaña "Tráfico", tras lo cual pulsaremos sobre el botón "Filtrado", y luego sobre su entrada adjunta "Configurar FTP".

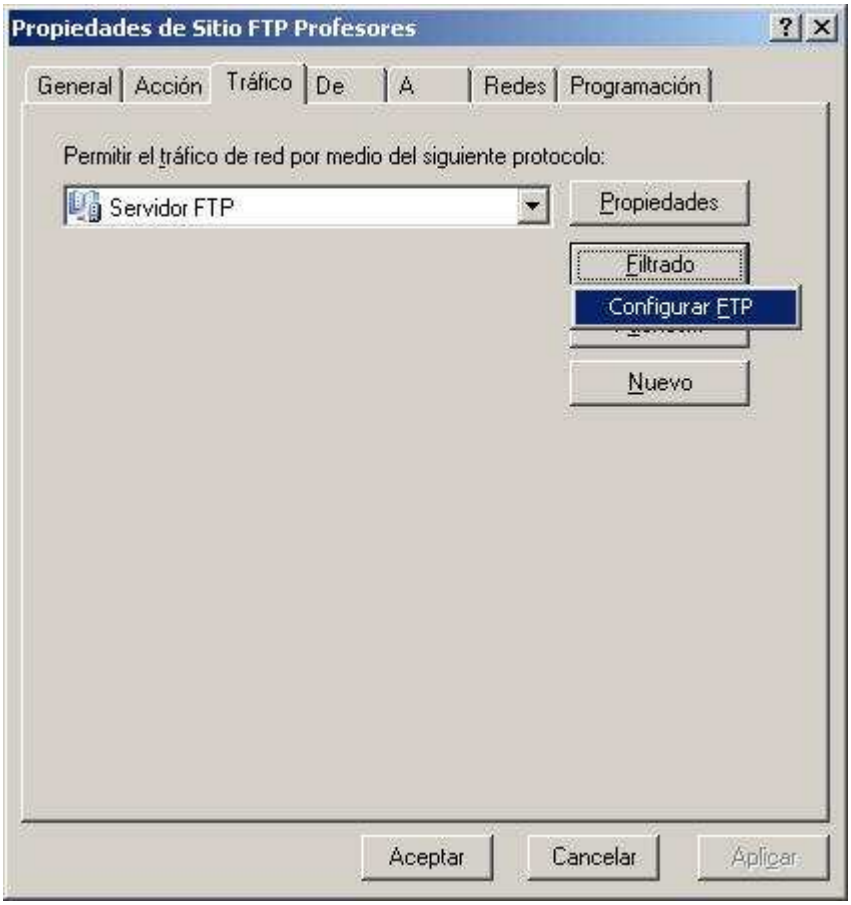


Imagen: ISA\entran17.JPG

En la nueva ventana mostrada desactivaremos la casilla "Sólo lectura", y tras ello iremos pulsando sobre los respectivos botones "Aceptar" en todas las ventanas que tuviéramos abiertas.

Imagen: ISA\entran18.JPG

NOTA: Esta última configuración realizada sobre la regla "Sitio FTP Profesores", permitirá grabar contenidos en el sitio FTP especificado desde Internet, a los usuarios habilitados para ello.

Finalmente deberemos recordar pulsar sobre el botón "Aplicar" en la ventana de administración de "ISA Server 2004", momento a partir del cual los usuarios autorizados podrán acceder desde Internet mediante FTP al sitio FTP "Sitio FTP Profesores".

Si estamos trabajando con máquinas virtuales, podremos probar fácilmente el correcto funcionamiento de la regla de publicación creada, lanzando el navegador de la máquina anfitriona que aloja a la máquina virtual "SERVIDOR", y estableciendo una conexión FTP a la dirección del interfaz de red externo del equipo "SERVIDOR", es decir tecleando en la URL del navegador del equipo anfitrión "ftp://servidor.micentro.edu", y autenticándonos tras con las credenciales de un usuario habilitado para dicho acceso FTP.

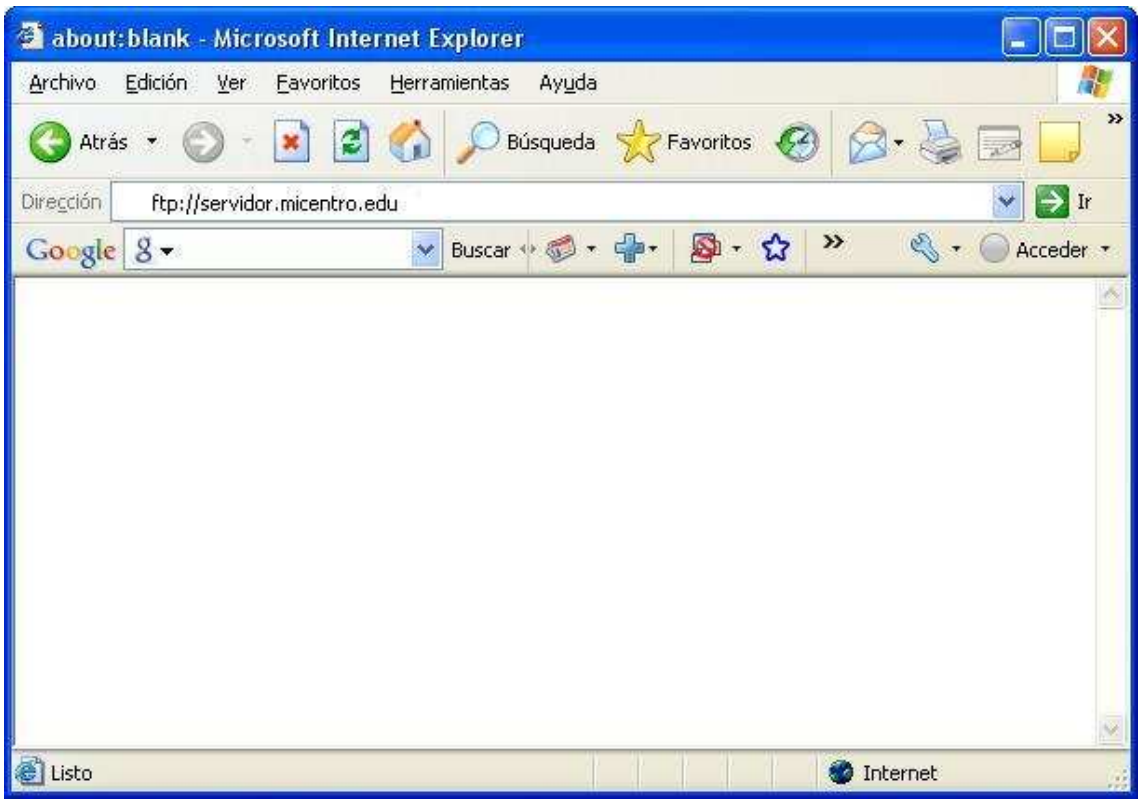


Imagen: ISA\entran19.JPG

Hasta este instante hemos indicado como definir las reglas de publicación para servicios predefinidos, tales como el servicio "Terminal Server" y el servicio "FTP", pero hemos de tener presente que hay ciertos servicios que para ser publicados precisan de la creación de una regla de publicación específica.

Concretamente los servidores web, los servidores web SSL y los servidores de correo, no serán publicados mediante una regla de publicación de servidores, sino que deberemos definir una regla específica para dichos tipos de servidores.

Por ejemplo vamos a comenzar con la publicación del servidor de correo "Microsoft Exchange 2003" para que esté accesible desde Internet, para lo cual en primer lugar deberemos situarnos sobre la entrada "Directivas de Firewall (SERVIDOR)" de la matriz "SERVIDOR", y pulsar sobre ella con el botón derecho del ratón para elegir la opción "Nuevo", y luego "Regla de publicación de servidor de correo" en los desplegables correspondientes.

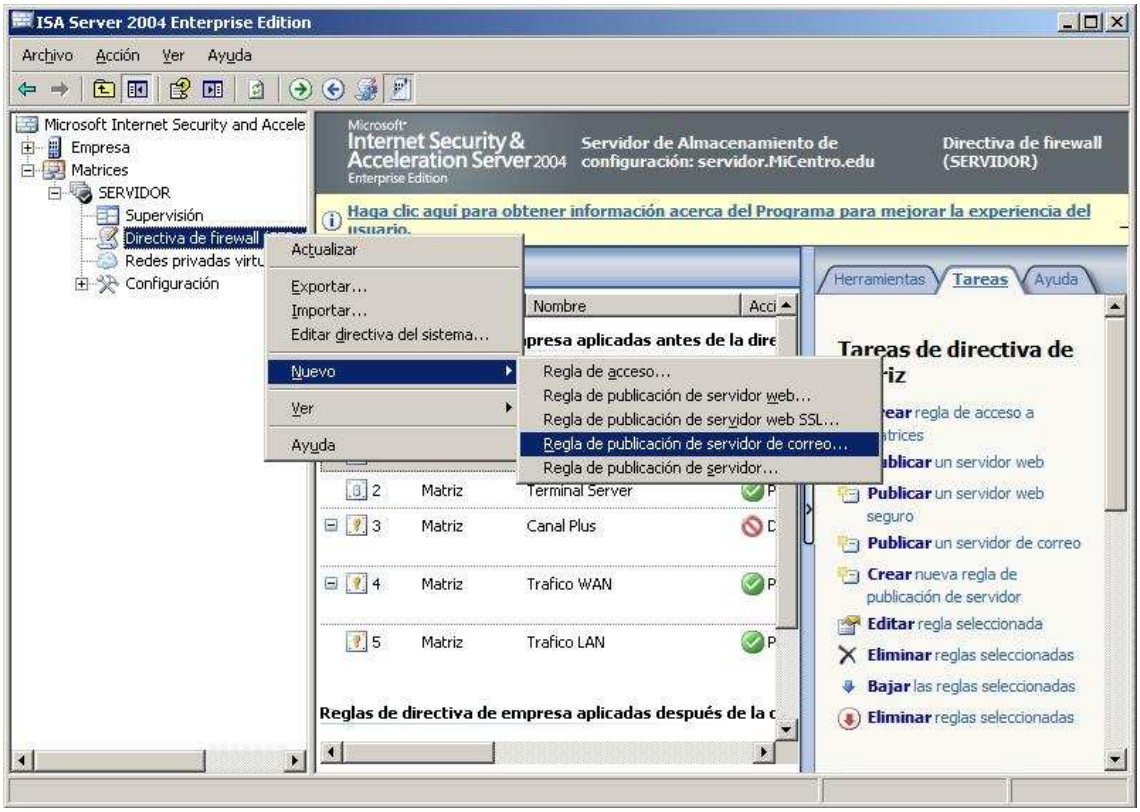


Imagen: ISA\entran20.JPG

Pasa a ser mostrada en este instante la primera ventana del asistente de publicación de servidor de correo, en la cual indicaremos como nombre para dicha regla "Correo Exchange", y posteriormente pulsaremos sobre el botón "Siguiente".

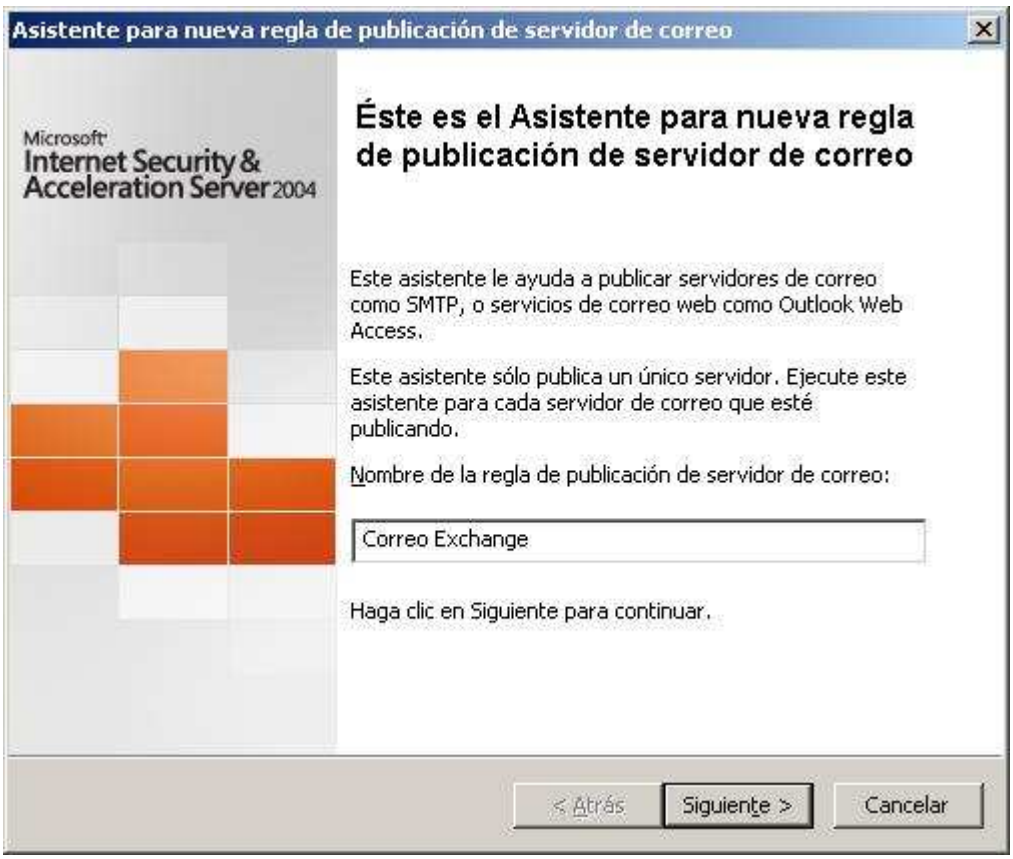


Imagen: ISA\entran21.JPG

En la siguiente ventana activaremos el radio botón correspondiente a "Acceso de cliente: RPC, IMAP, POP3, SMTP", para dar acceso al servidor de correo "Microsoft Exchange 2003" desde Internet a través de estos protocolos, y a continuación pulsaremos sobre el botón "Siguiente".

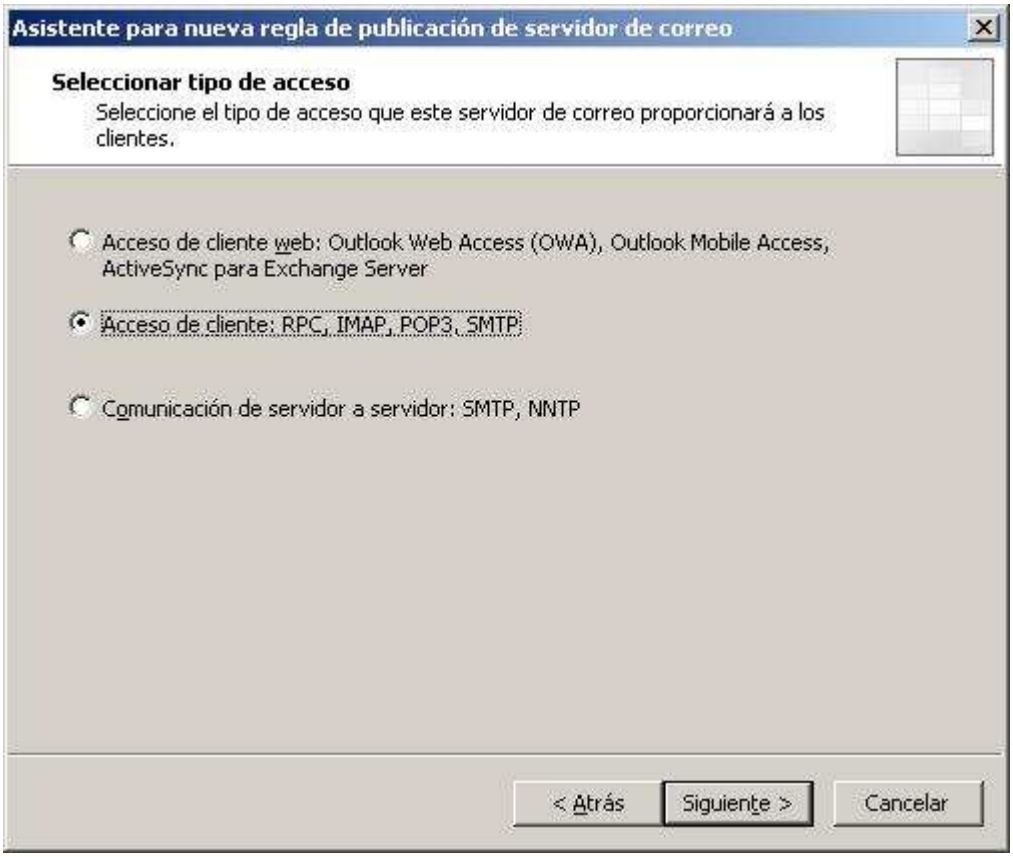


Imagen: ISA\entran22.JPG

A continuación se nos presenta la siguiente ventana, en la que activaremos todas las casillas para dar acceso a través de todos los protocolos especificados, seguros o no, tal y como se muestra en la siguiente imagen, y tras ello pulsaremos sobre el botón "Siguiente".

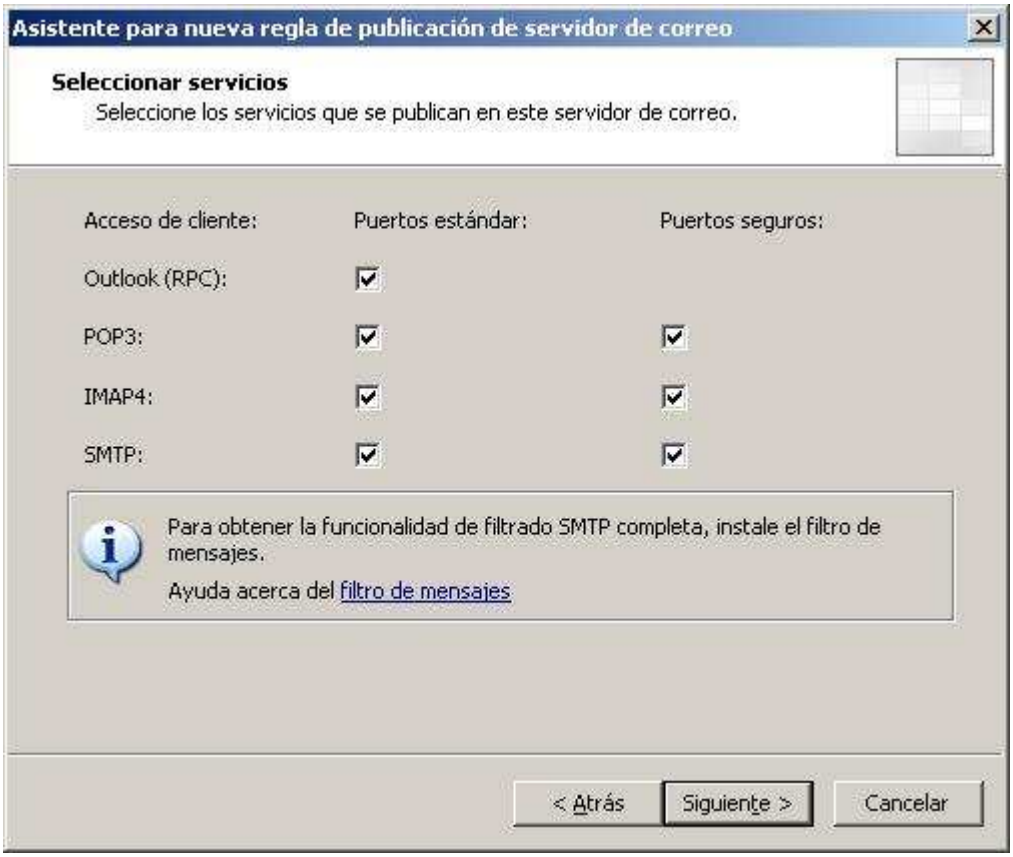


Imagen: ISA\entran23.JPG

A continuación deberemos especificar en la siguiente ventana la dirección IP del interfaz de red externo del equipo "SERVIDOR", en nuestro caso deberemos teclear "192.168.0.220", la dirección IP del interfaz de red "Conexión WAN", y tras ello pulsar sobre el botón "Siguiente".

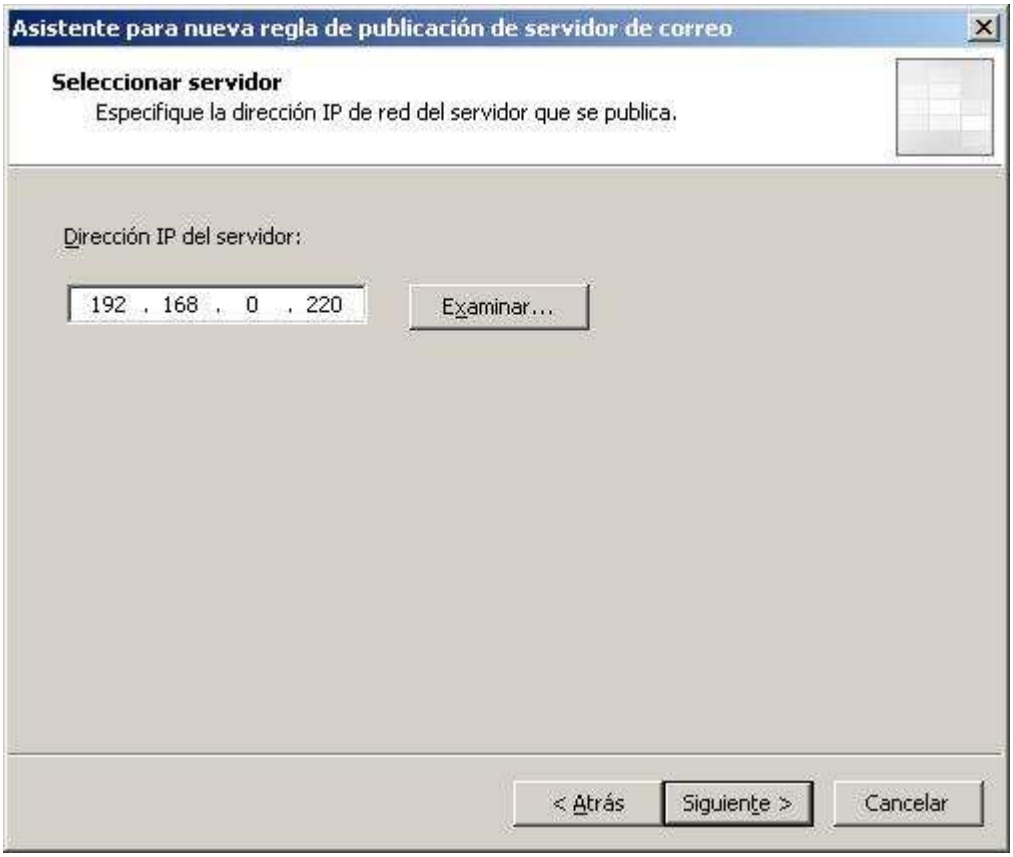


Imagen: ISA\entran24.JPG

En la siguiente ventana indicaremos la red desde la que deseamos permitir dicho tipo de conexión, activando en nuestro caso la casilla "Externa", y pulsando posteriormente sobre el botón "Siguiente".

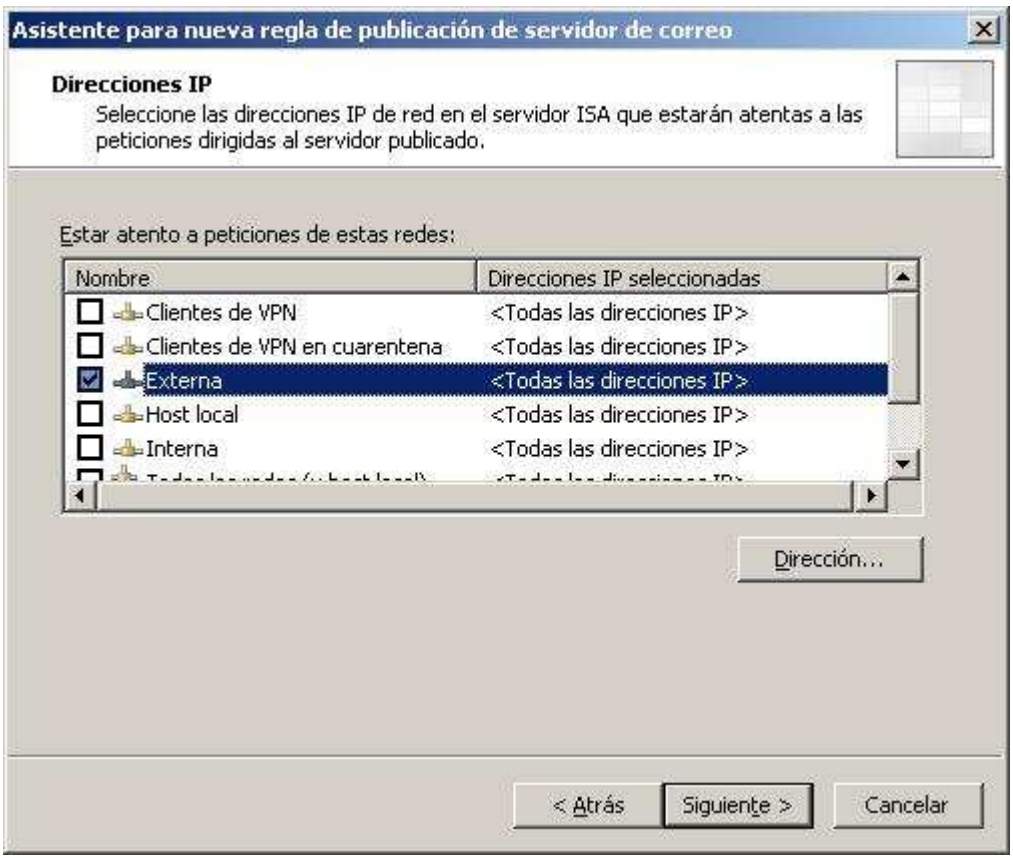


Imagen: ISA\entran25.JPG

En la última ventana del asistente pulsaremos directamente sobre el botón "Finalizar" para completar el proceso de creación de la nueva regla de publicación del servidor de correo.

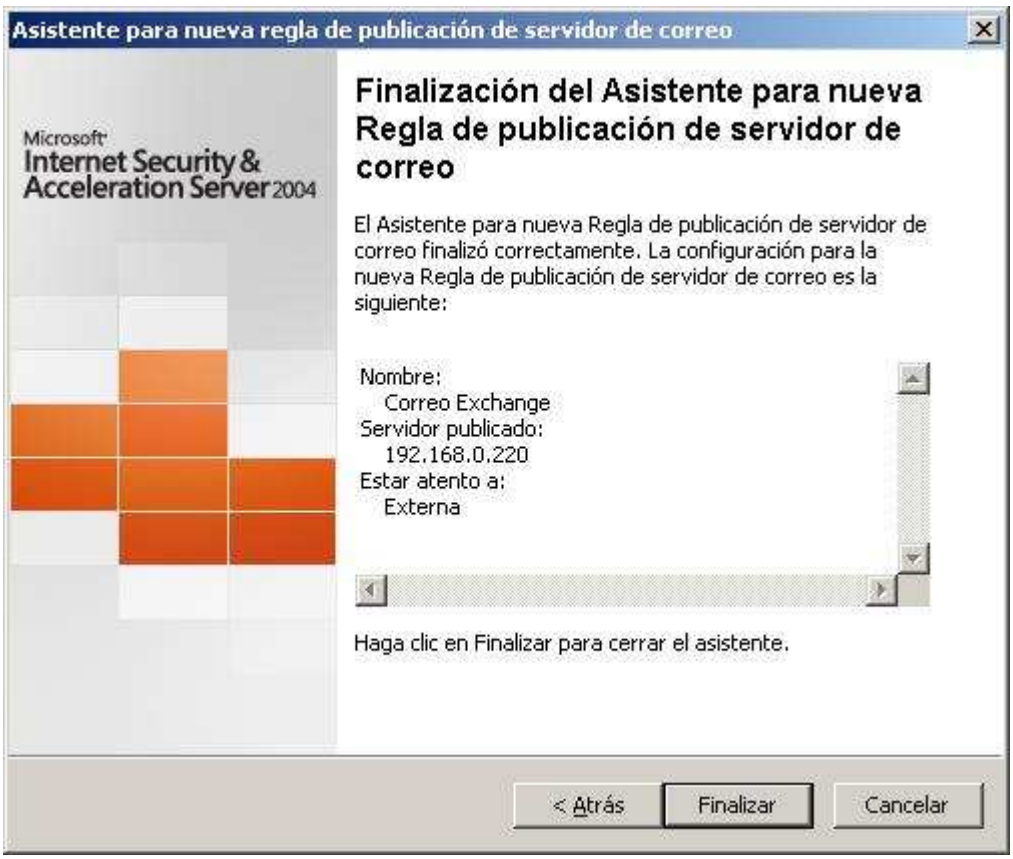


Imagen: ISA\entran26.JPG

A continuación pulsaremos sobre el botón "Aplicar" en la ventana de administración de "ISA Server 2004", momento a partir del cual podremos acceder desde Internet al servidor de correo "Microsoft Exchange 2003" a través de los protocolos especificados anteriormente en la regla de publicación de servidor de correo.

La regla que acabamos de definir genera un gran número de reglas de publicación del servidor de correo, debido al elevado número de protocolos de acceso que hemos habilitado en ella, tal y como podemos comprobar en la imagen siguiente.

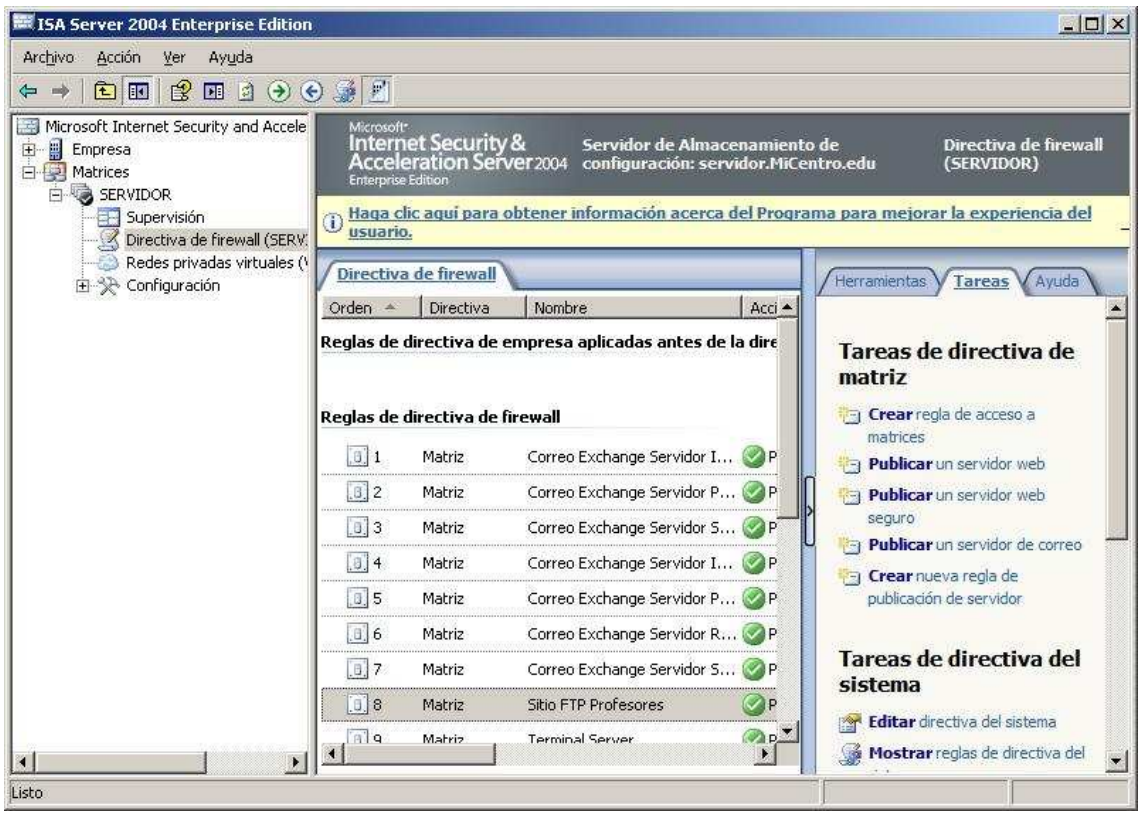


Imagen: ISA\entran27.JPG

Si deseamos probar el correcto funcionamiento de esta regla de correo, el proceso que deberemos seguir será más complejo que el que seguimos anteriormente para probar el correcto acceso desde Internet a los servicios "Terminal Server" y "Servidor FTP".

En primer lugar deberemos hacer doble clic sobre el icono "Correo" del "Panel de control" de la máquina anfitriona desde la cual estableceremos la conexión.

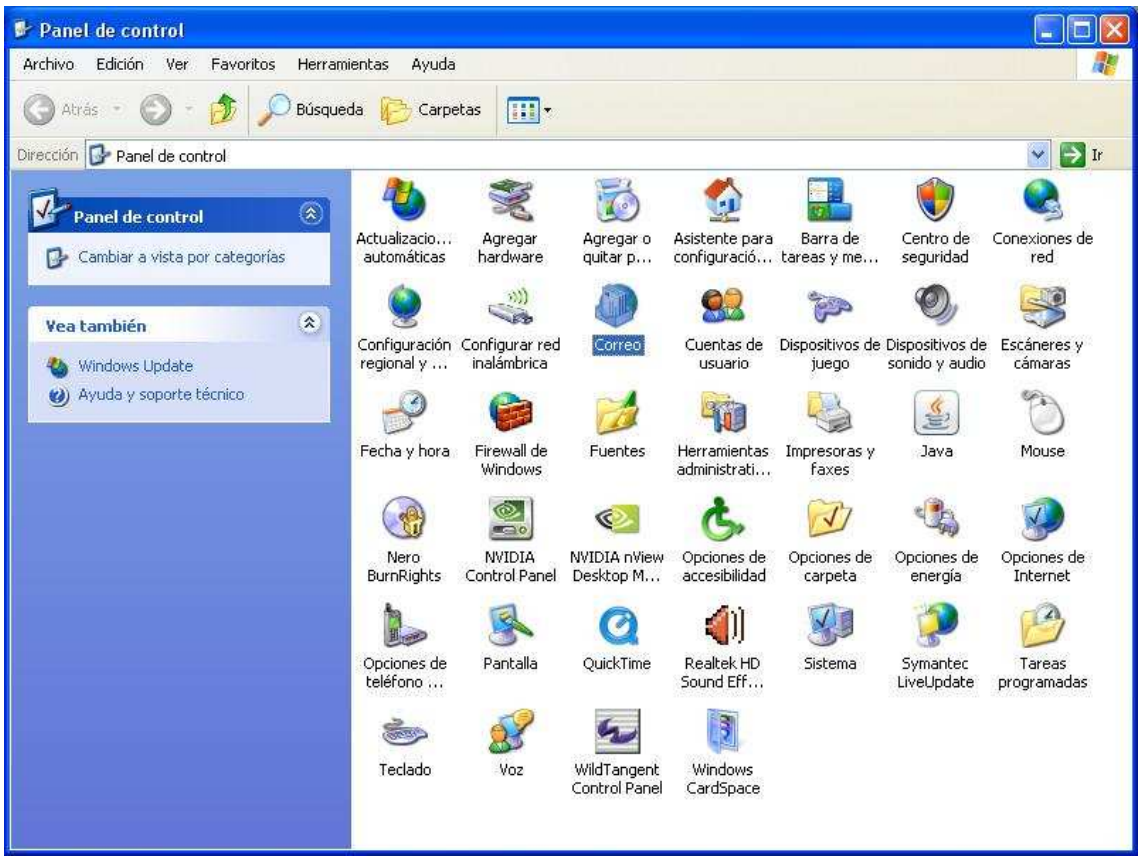


Imagen: ISA\entran28.JPG

Como resultado de la acción anterior, pasa a ser mostrada la siguiente ventana, en la que pulsaremos directamente sobre el botón "Cuentas de correo electrónico".

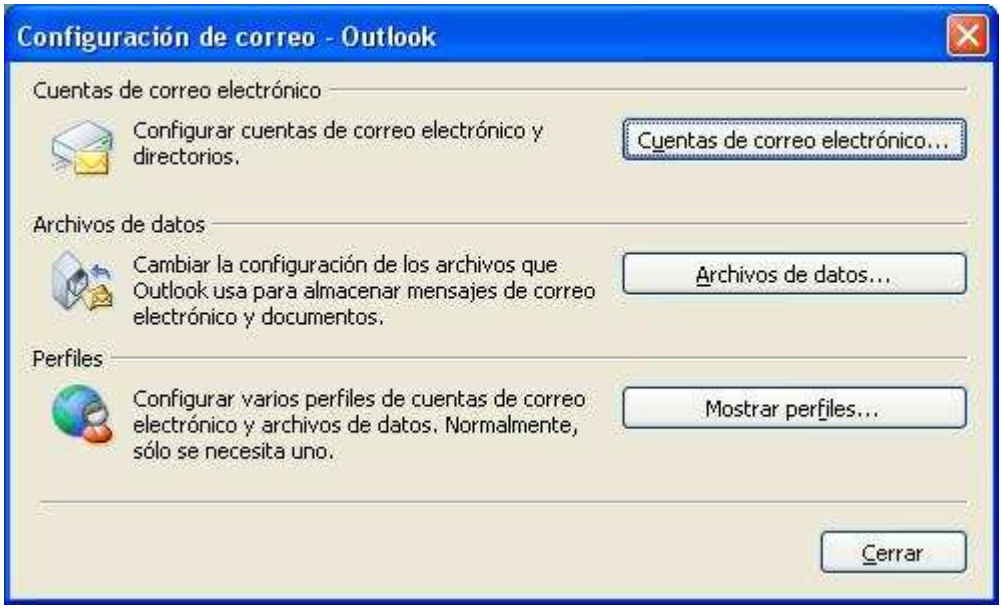


Imagen: ISA\entran29.JPG

Se lanza en ese instante el asistente de gestión de cuentas de correo electrónico, en el cual seleccionaremos el radio botón "Agregar una nueva cuenta de correo electrónico", y tras ello pulsaremos sobre el botón "Siguiente".

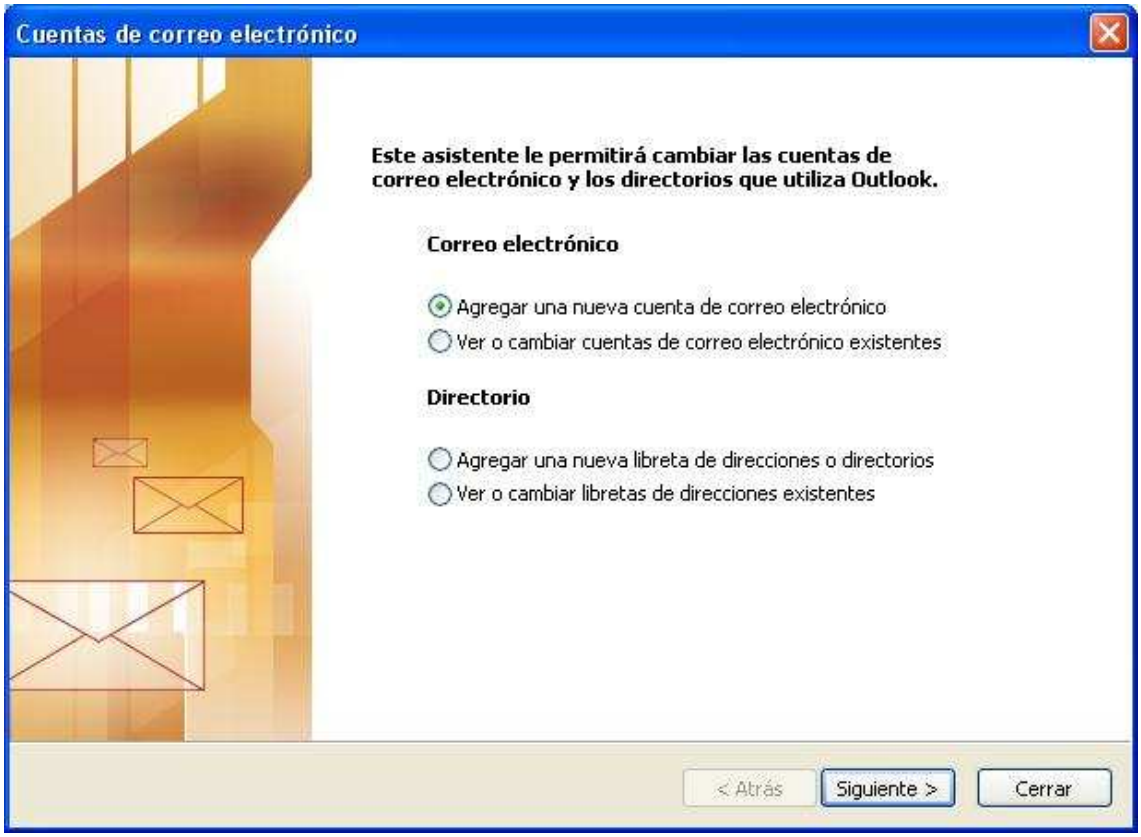


Imagen: ISA\entran30.JPG

En la siguiente ventana seleccionaremos el radio botón "Servidor de Microsoft Exchange", y tras ello pulsaremos sobre el botón "Siguiente".

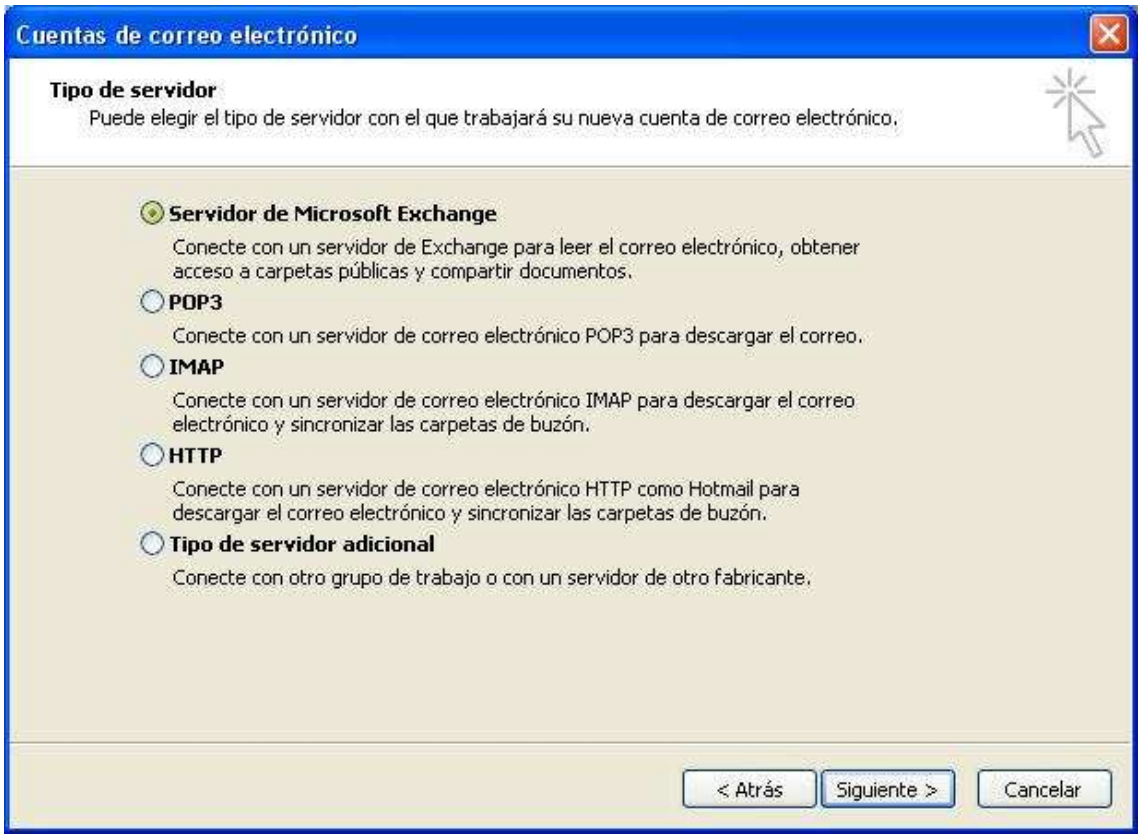


Imagen: ISA\entran31.JPG

A continuación en la siguiente ventana, indicaremos en la caja de texto "Microsoft Exchange Server" el nombre de nuestro servidor, es decir "servidor.micentro.edu" en nuestro caso, y tras ello en la caja de texto "Nombre de usuario" indicaremos el nombre del usuario de correo de dicho servidor cuya cuenta deseamos configurar, en este caso "Javier".

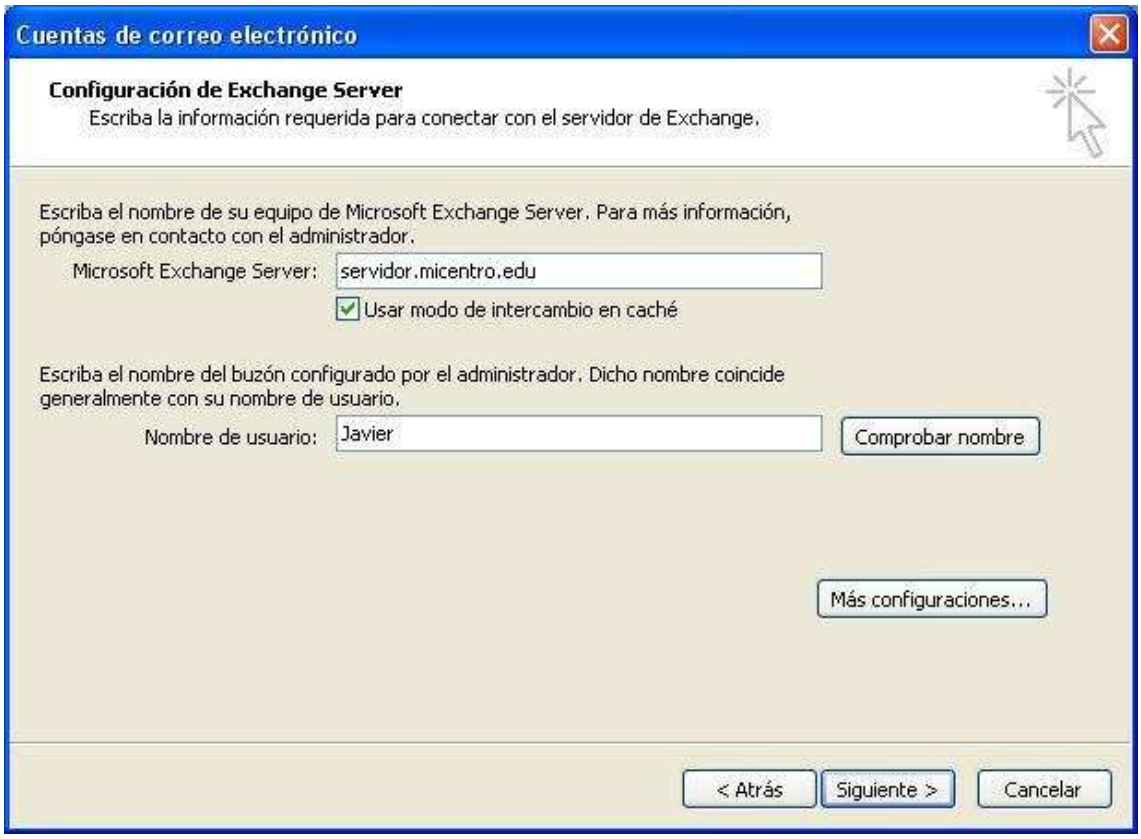


Imagen: ISA\entran32.JPG

El asistente de configuración nos presenta a continuación la siguiente ventana, en la que pulsaremos directamente sobre el botón "Sí".

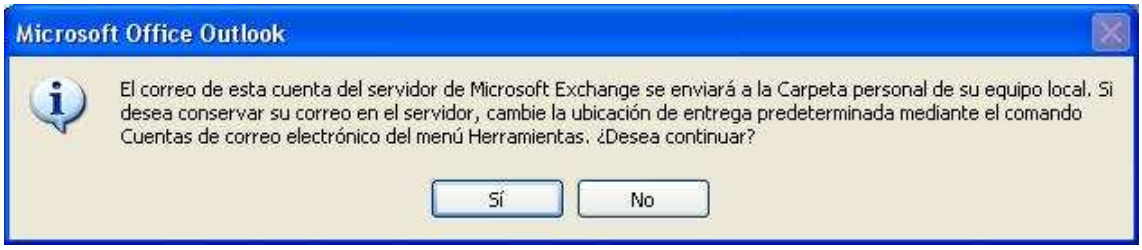


Imagen: ISA\entran33.JPG

Tras ello se nos presenta la siguiente ventana, en la cual deberemos introducir las credenciales del profesor "Javier" en el dominio "MiCentro.edu", y tras ello pulsar sobre el botón "Aceptar".

Imagen: ISA\entran34.JPG

Una vez completado el proceso de definición de la nueva cuenta, se nos mostrará la siguiente ventana en la que pulsaremos directamente sobre el botón "Finalizar".

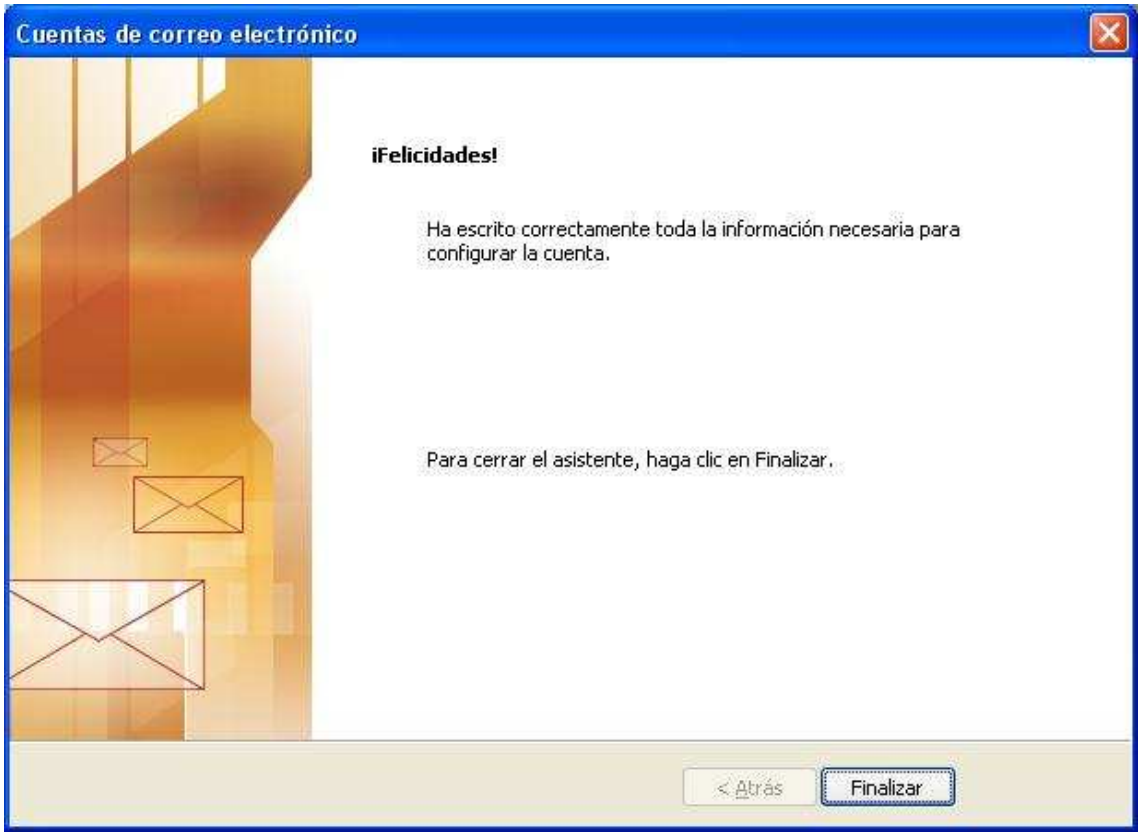


Imagen: ISA\entran35.JPG

A partir de este instante, el profesor "Javier" podrá descargar el contenido del buzón de su

cuenta de correo electrónico "javier@micentro.edu" desde Internet; por ejemplo si el profesor "Joaquin" le hubiera enviado desde su cuenta de correo "joaquin@micentro.edu" un correo electrónico al profesor "Javier" a su cuenta de correo "javier@micentro.edu", el profesor "Javier" podrá descargar dicho correo desde la cuenta que acaba de ser configurada anteriormente para dicho usuario en el equipo anfitrión.

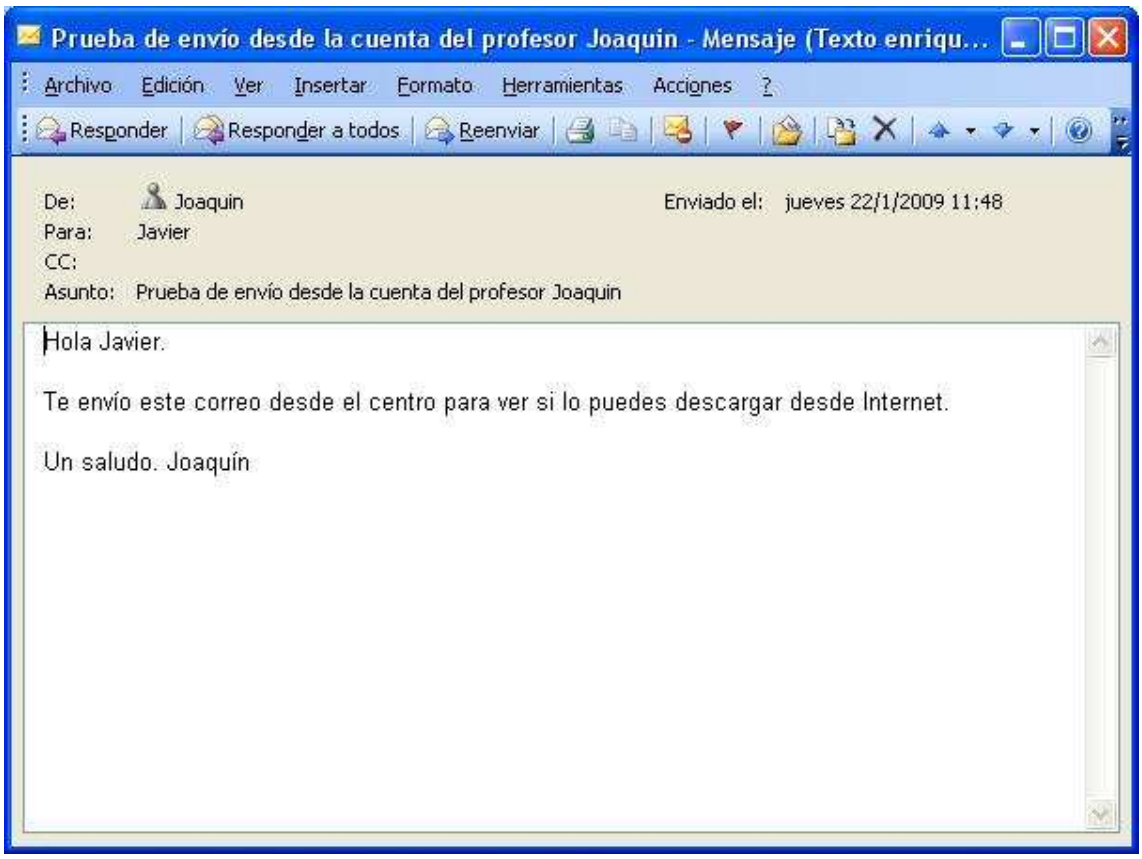


Imagen: ISA\entran36.JPG

NOTA: Igualmente, si el profesor "Javier" le envía desde Internet un correo al profesor "Joaquín", desde la cuenta "javier@micentro.edu" a la cuenta "joaquin@micentro.edu", el profesor "Joaquín podrá descargarlo desde un equipo cliente del centro, o desde Internet.

Una vez configurado el acceso al servidor de correo "Microsoft Exchange 2003", también podríamos configurar "ISA Server 2004" para habilitar el acceso desde Internet a los sitios web del servidor IIS.

En nuestro caso crearemos una regla de publicación de servidor web para permitir el acceso desde Internet al sitio web "Sitio Web de MiCentro" de nuestro equipo "SERVIDOR", pero antes de comenzar con la configuración indicada, queremos recordar que al comienzo de este apartado ya explicamos que por el hecho de estar instalado el servidor "ISA Server 2004" en el mismo equipo donde se encuentran los sitios web a publicar, no podremos configurar la escucha de los mismos en el puerto 80 del "ISA Server 2004", pues dicho puerto está siendo utilizado por los sitios web reseñados.

Así pues para habilitar el acceso al sitio web "Sitio Web de MiCentro" desde Internet nos

situaremos sobre "Directivas de firewall (SERVIDOR)" de la matriz "SERVIDOR", y pulsaremos sobre ella con el botón derecho del ratón para elegir la opción "Nuevo", y luego "Regla de publicación de servidor web", en los desplegables correspondientes.

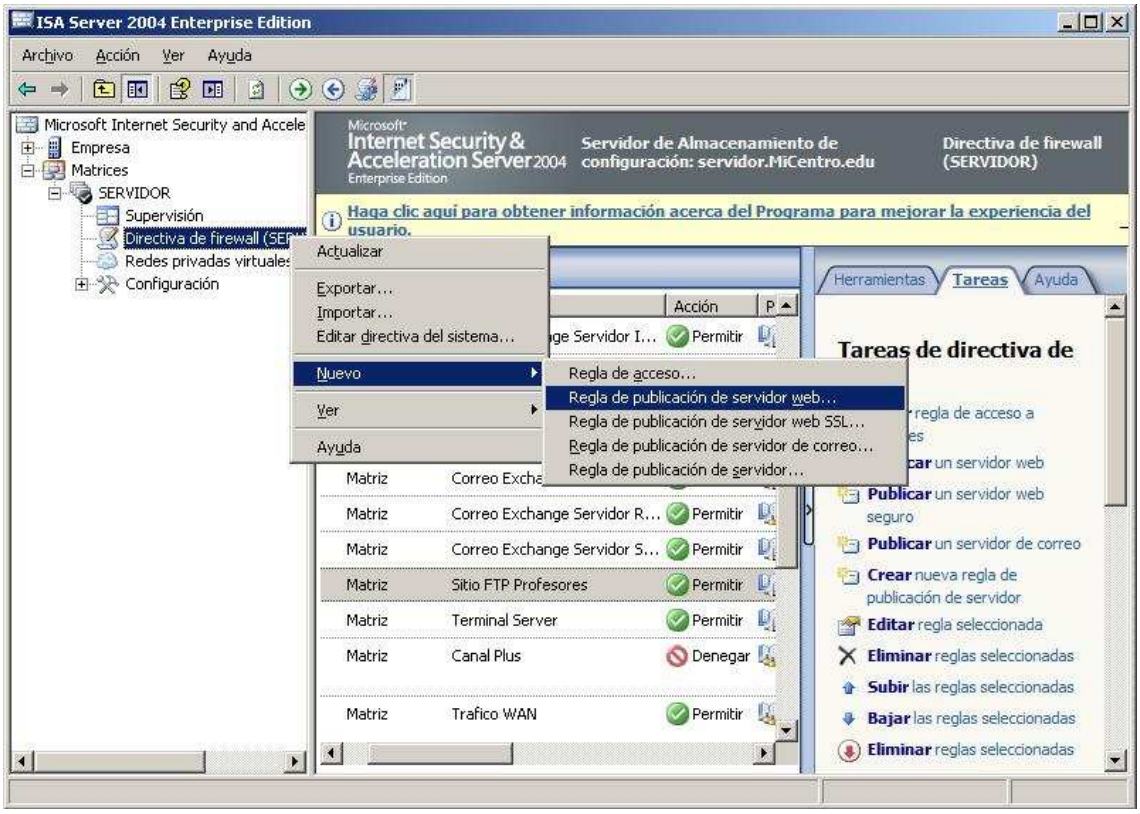


Imagen: ISA\entran37.JPG

En la primera ventana del asistente de publicación de servidor web indicaremos "Sitio Web de MiCentro" como nombre de la regla de publicación, y posteriormente pulsaremos sobre el botón "Siguiente".

Imagen: ISA\entran38.JPG

En la siguiente ventana mostrada confirmaremos que este seleccionado el radio botón "Permitir", y tras ello pulsaremos sobre el botón "Siguiente".

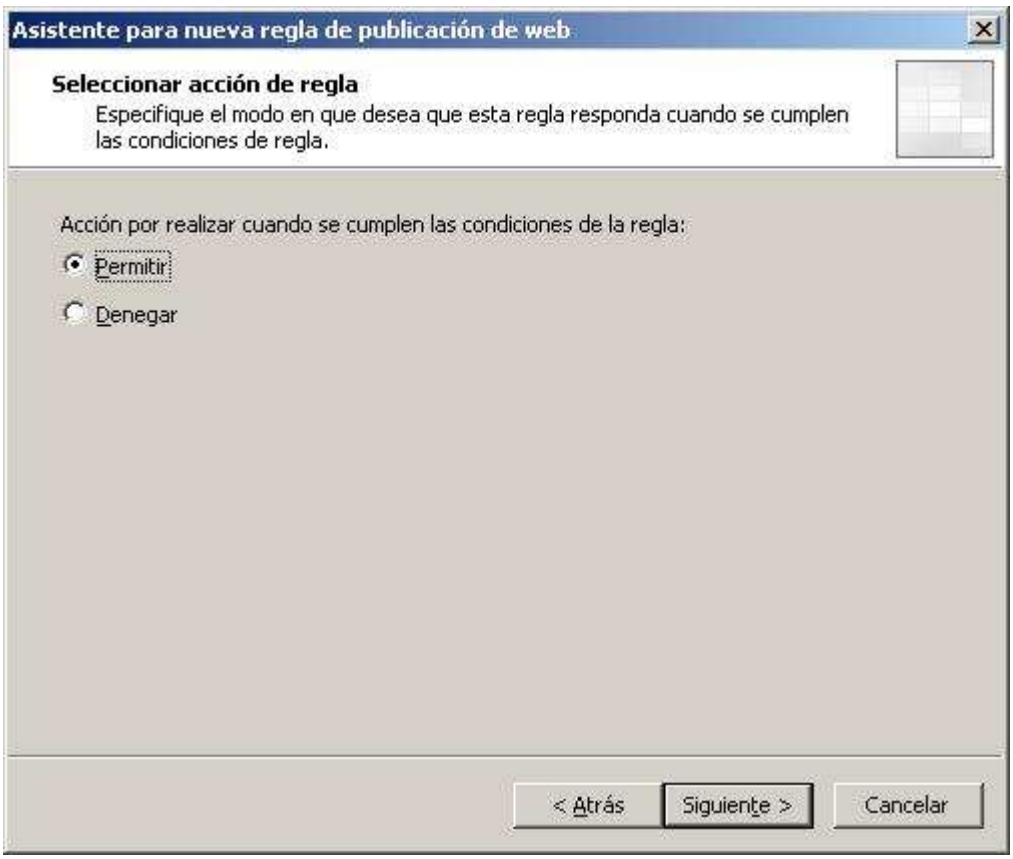


Imagen: ISA\entran39.JPG

A continuación especificaremos nombre del sitio web "Sitio Web de MiCentro" que deseamos publicar, tecleando su URL de acceso, es decir tecleando "www.micentro.edu" en la caja de texto "Dirección IP o nombre de equipo", y posteriormente pulsaremos sobre el botón "Siguiente".

Imagen: ISA\entran40.JPG

En la siguiente ventana especificaremos el nombre público del sitio web que vamos a publicar, tecleando en nuestro caso "www.micentro.edu" en la caja de texto "Nombre público", y pulsando tras ello sobre el botón "Siguiente".

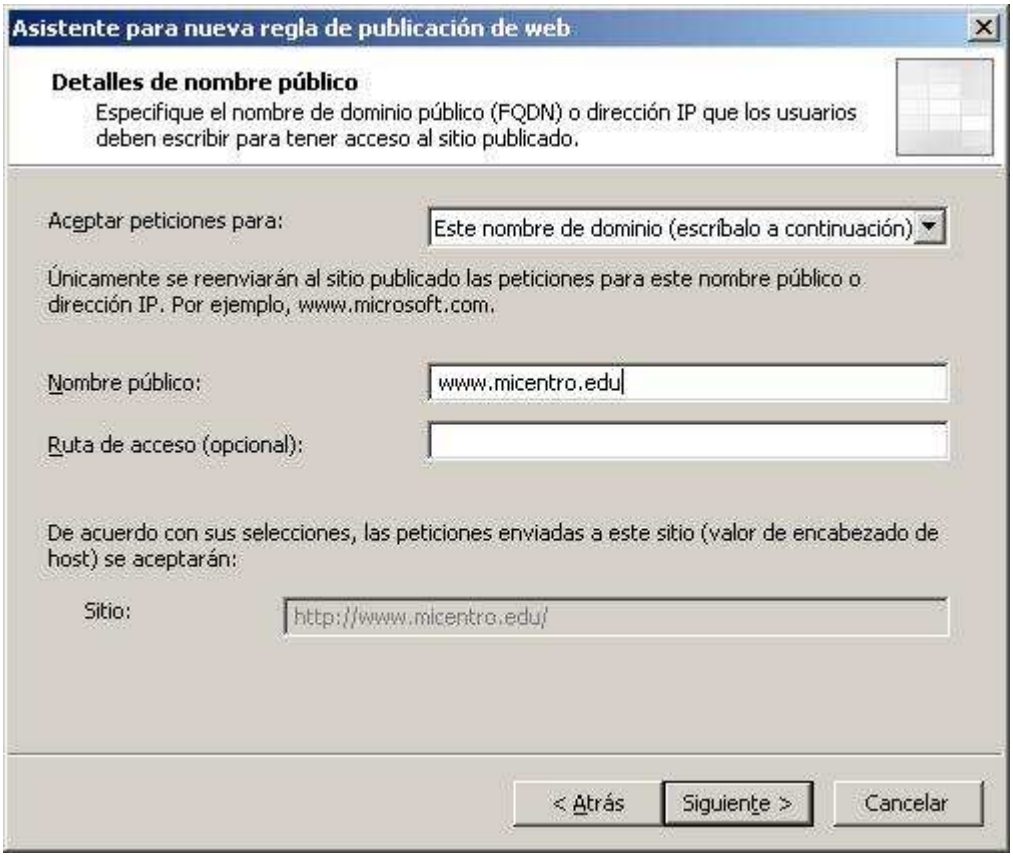


Imagen: ISA\entran41.JPG

NOTA: El nombre del sitio web y su nombre público NO tienen porqué coincidir, aunque en nuestro caso los hemos hecho coincidir por parecernos más coherente.

En la siguiente ventana mostrada deberemos especificar el puerto de escucha por el cual el servidor "ISA Server 2004" atenderá peticiones de acceso a este sitio web, pulsando en la misma sobre el botón "Nueva" para definir el nuevo puerto.

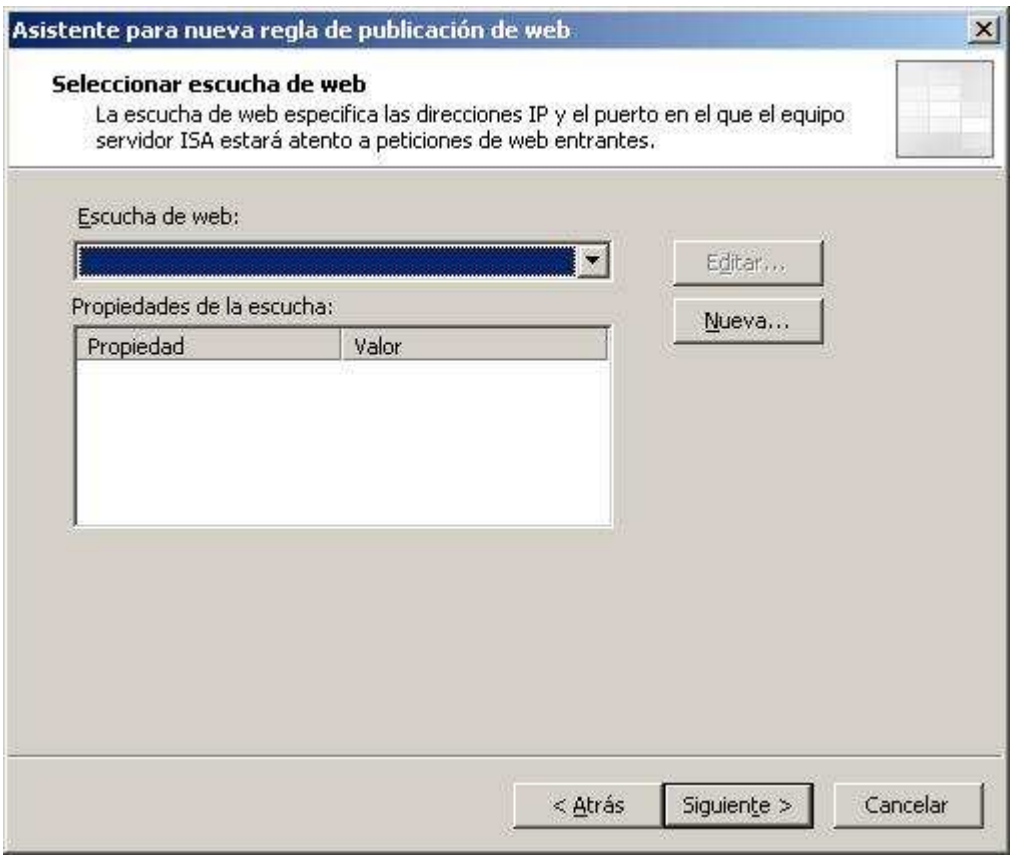


Imagen: ISA\entran42.JPG

Como resultado de la acción anterior pasa a ser mostrada la primera ventana del asistente de agregación de nueva escucha web, en la cual indicaremos en primer lugar "Escucha Web MiCentro" como nombre para la escucha que estamos creando

Imagen: ISA\entran43.JPG

En la siguiente ventana indicaremos la red desde la que deseamos permitir dicho tipo de conexión, activando en nuestro caso la casilla "Externa", y pulsando posteriormente sobre el botón "Siguiente".

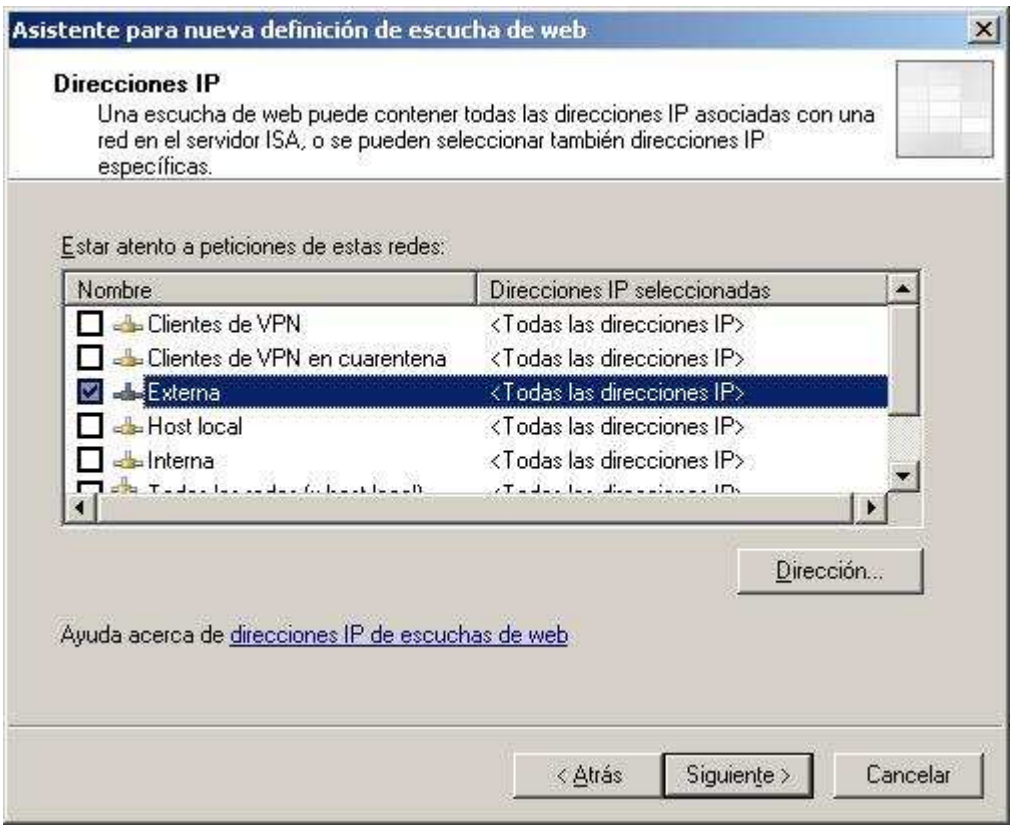


Imagen: ISA\entran44.JPG

En la siguiente ventana deberemos especificar los puertos por los que escuchará el "ISA Server 2004" las peticiones de acceso a este sitio web, debiendo dejar activada la casilla "Habilitar HTTP", y cambiando el valor de dicho puerto a uno distinto del puerto "80", por los motivos antes comentados; en este caso hemos elegido el puerto "880", aunque podríamos haber elegido otro puerto cualquiera que estuviera libre; además activaremos la casilla "Habilitar SSL", y tras ello indicaremos como puerto para SSL un puerto que NO esté siendo utilizado por el servidor IIS, por ejemplo "8443"; tras completar las operaciones anteriores, pulsaremos sobre el botón "Seleccionar" para escoger en la nueva ventana mostrada, el certificado "www.micentro.edu", de modo que cuando la ventana indicada presente el aspecto mostrado en la imagen inferior, pulsaremos sobre el botón "Siguiente" para continuar.

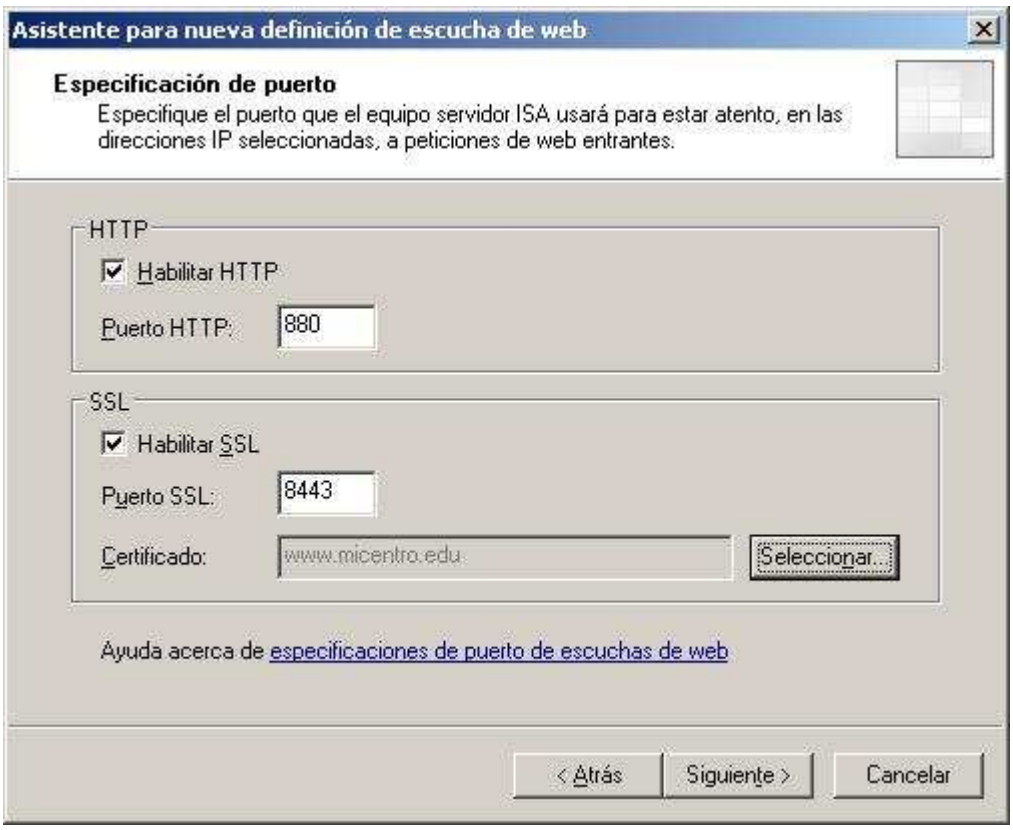


Imagen: ISA\entran45.JPG

En la siguiente ventana pulsaremos directamente sobre el botón "Finalizar" para terminar con la definición del puerto de escucha correspondiente.

Imagen: ISA\entran46.JPG

De vuelta a la ventana de selección de escucha web, el aspecto que debe presentar la misma es el que podemos ver en la siguiente imagen, momento en el cual pulsaremos sobre el botón "Siguiente" para continuar con la creación de la regla de publicación del servidor web.

Imagen: ISA\entran47.JPG

A continuación el asistente de creación de nueva regla de publicación de servidor web nos presenta la siguiente ventana, en la que podremos seleccionar los usuarios a los que se les aplicará esta regla, si bien en nuestro caso aceptaremos la opción propuesta por el asistente, pulsando en ella directamente sobre el botón "Siguiente".

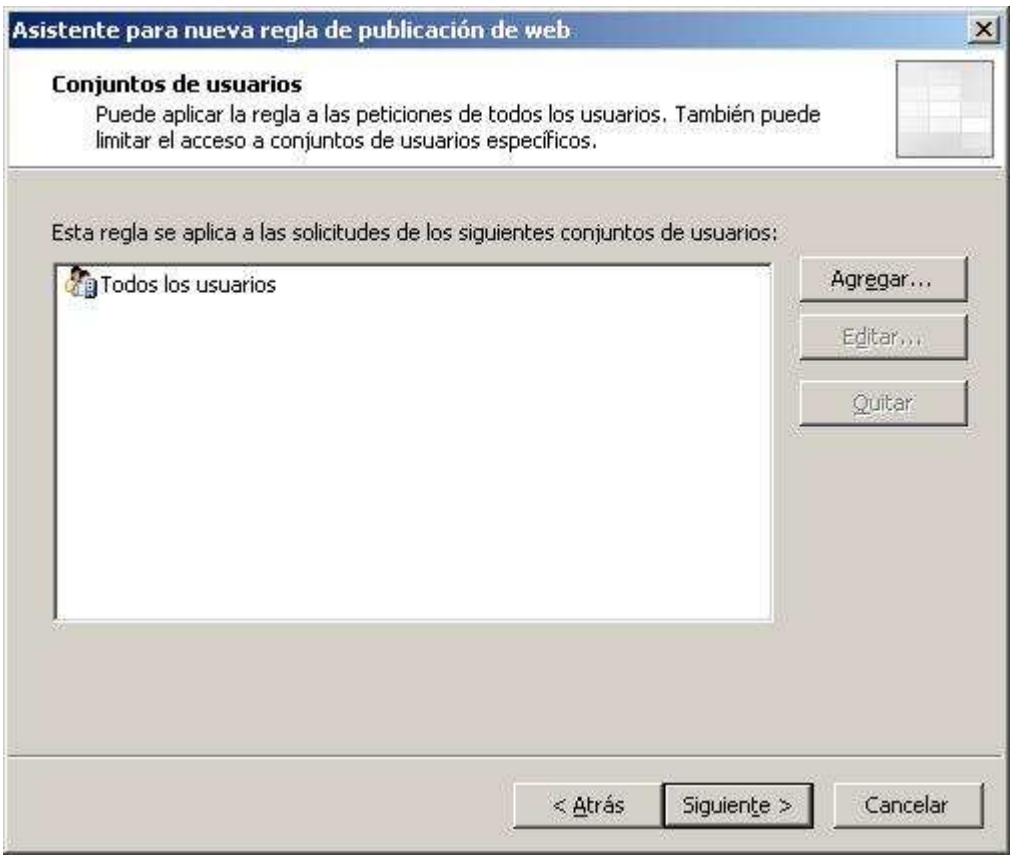


Imagen: ISA\entran48.JPG

En la última ventana del asistente pulsaremos directamente sobre el botón "Finalizar" para completar el proceso de creación de la regla de publicación del servidor web "www.micentro.edu".

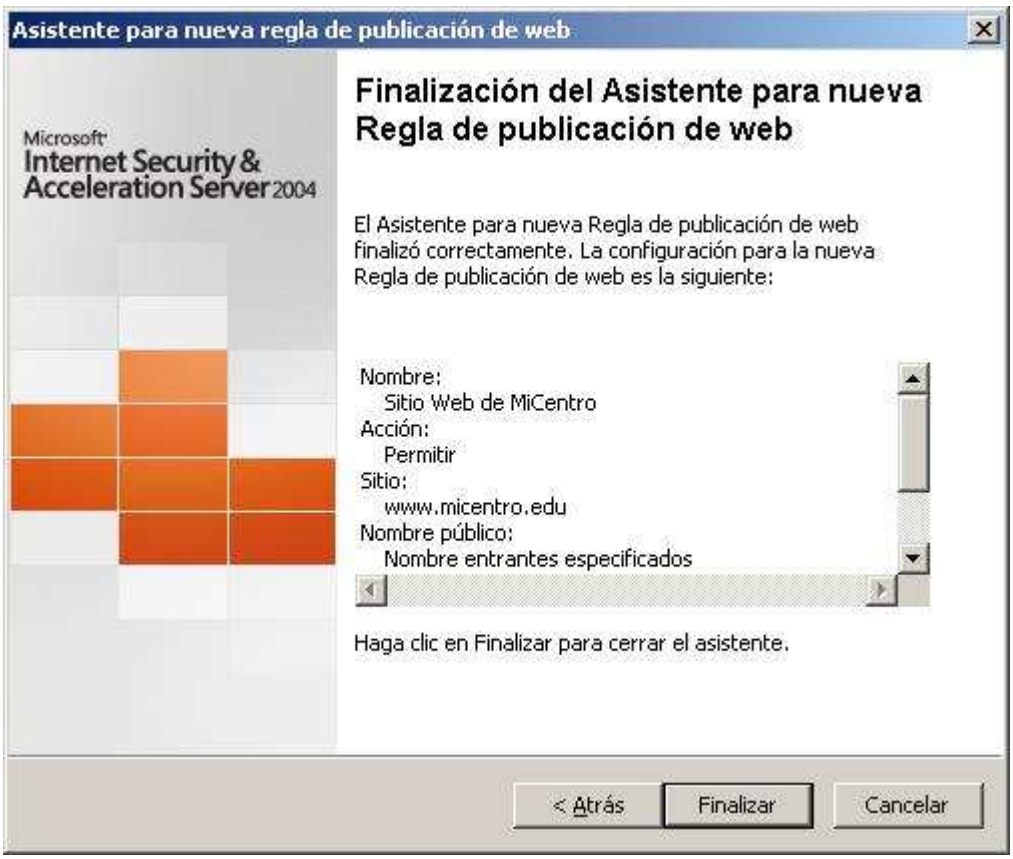


Imagen: ISA\entran49.JPG

Tras ello haremos doble clic sobre la nueva regla de publicación de servidores "Sitio Web de MiCentro" que acaba de ser creada, pasando a ser mostrada la siguiente ventana en la que nos ubicaremos sobre la pestaña "Protocolo de puente", activando a continuación en ella la casilla "Redirigir peticiones al puerto SSL", y asociando a la misma el puerto en el cual escucha el sitio web indicado las páginas seguras, "444" en nuestro caso, de modo que cuando dicha ventana presente el aspecto mostrado en la imagen inferior, pulsaremos sobre el botón "Aceptar".

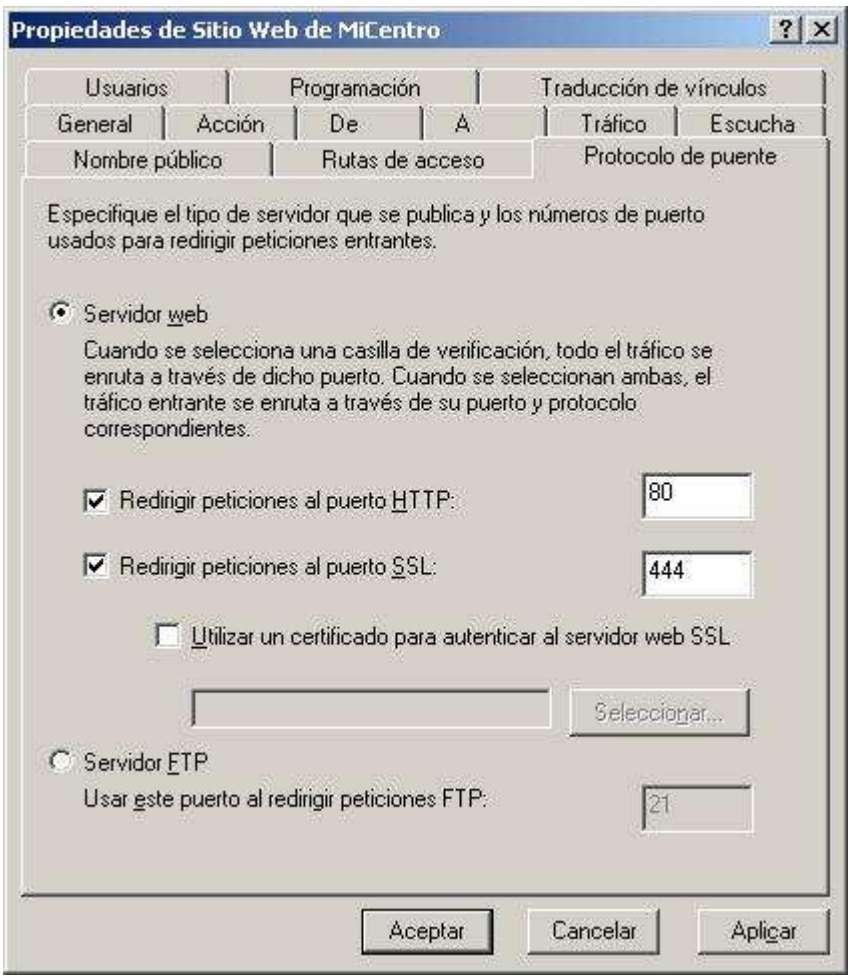


Imagen: ISA\entran50.JPG

Tras completar la acción anterior, hemos de recordar pulsar sobre el botón "Aplicar" en la ventana de administración de "ISA Server 2004" para que la nueva regla creada pase a ser efectiva.

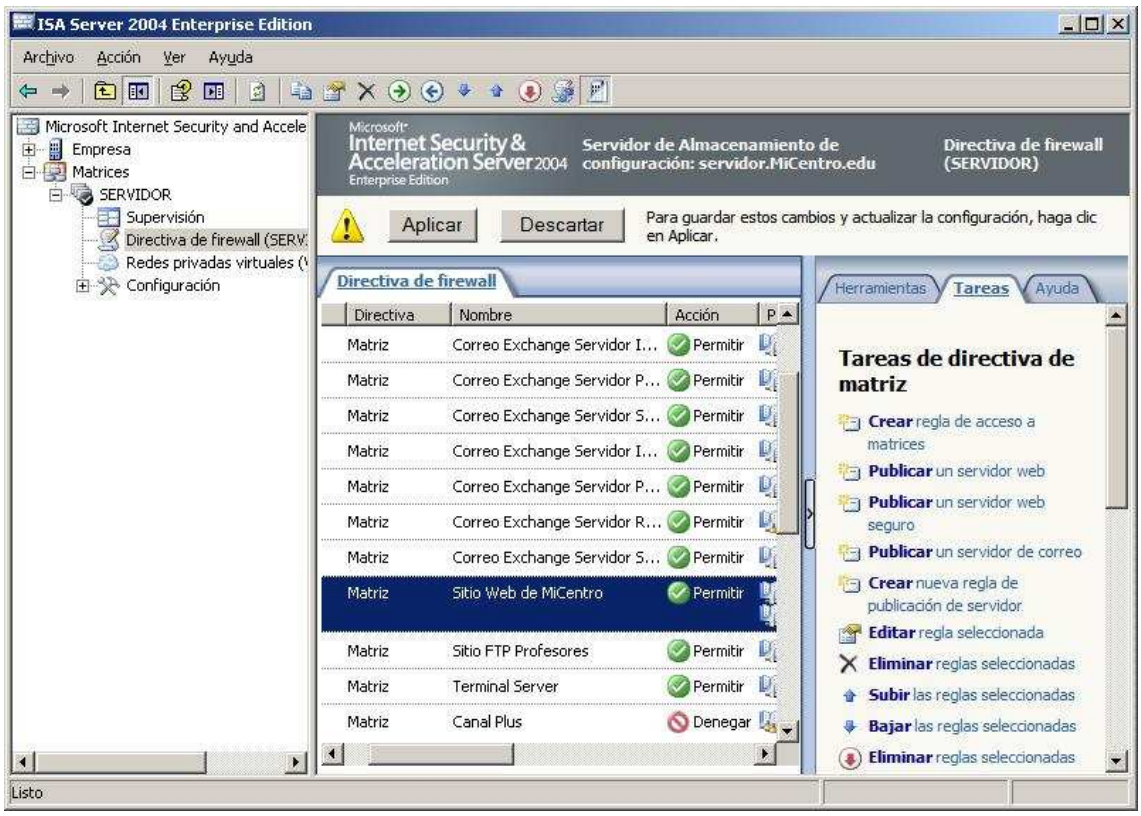


Imagen: ISA\entran51.JPG

A partir de este momento podemos acceder al sirio web "www.micentro.edu" desde Internet mediante el protocolo HTTP por el puerto "880", y mediante el protocolo HTTPS por el puerto "8443".

Antes de probar el acceso al sitio web "Sitio Web de MiCentro", hemos de modificar de nuevo el fichero "hosts" ubicado en la ruta "C:\Windows\System32\drivers\etc" del equipo ANFITRION, añadiendo una nueva entrada "192.168.0.220 www.micentro.edu", tal y como vemos en la imagen inferior, y guardando tras ello los cambios realizados en dicho fichero.

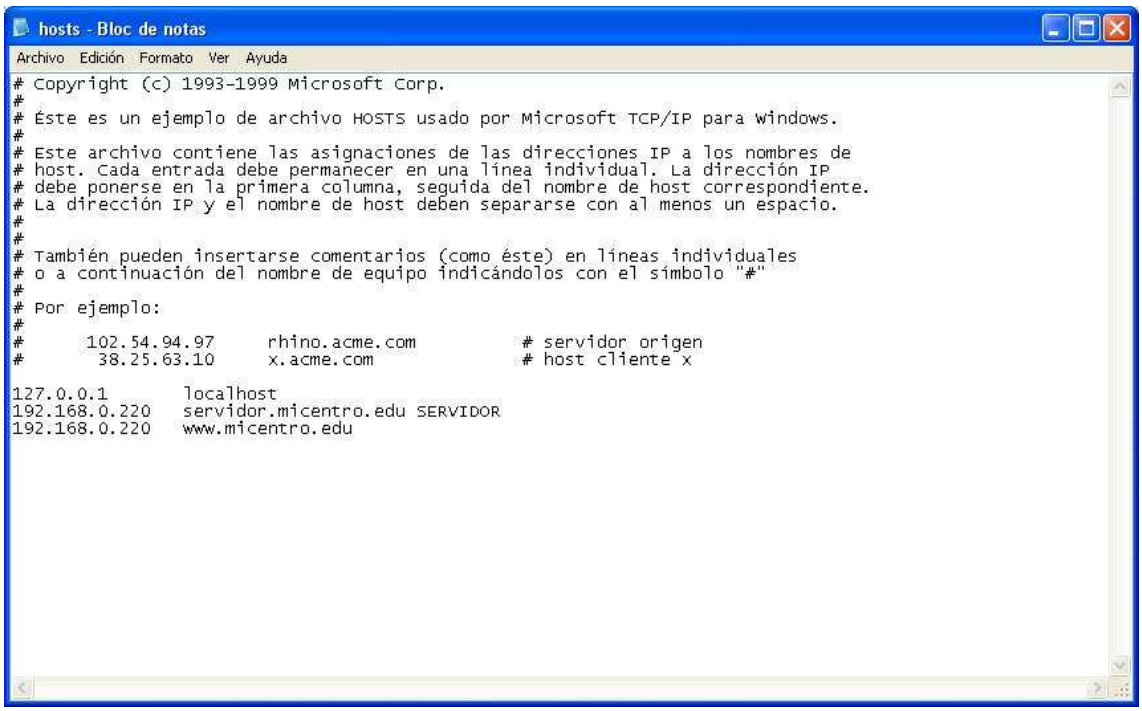


Imagen: ISA\entran52.JPG

Ahora sí que desde el navegador del equipo anfitrión podríamos teclear "http://www.micentro.edu:880", comprobando que llegaríamos a visualizar la página web principal de nuestro centro desde dicho equipo anfitrión.

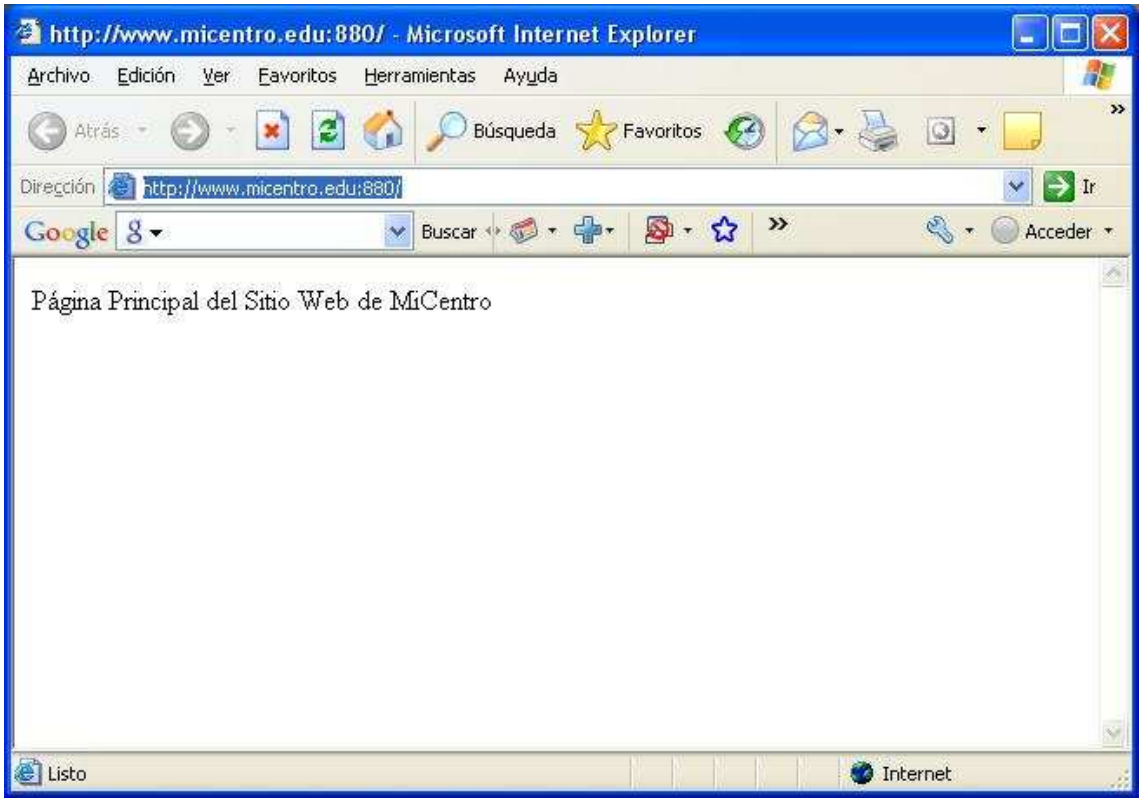


Imagen: ISA\entran53.JPG

Igualmente si desde el equipo anfitrión intentamos el acceso a una página web segura del sitio web "Sitio Web de MiCentro" por le puerto "8443", por ejemplo a la página web segura "https://www.micentro.edu:8443/Departamentos/Matematicas/javier/seguro/", conseguiríamos acceder a la misma pudiendo ver su contenido desde el equipo anfitrión.

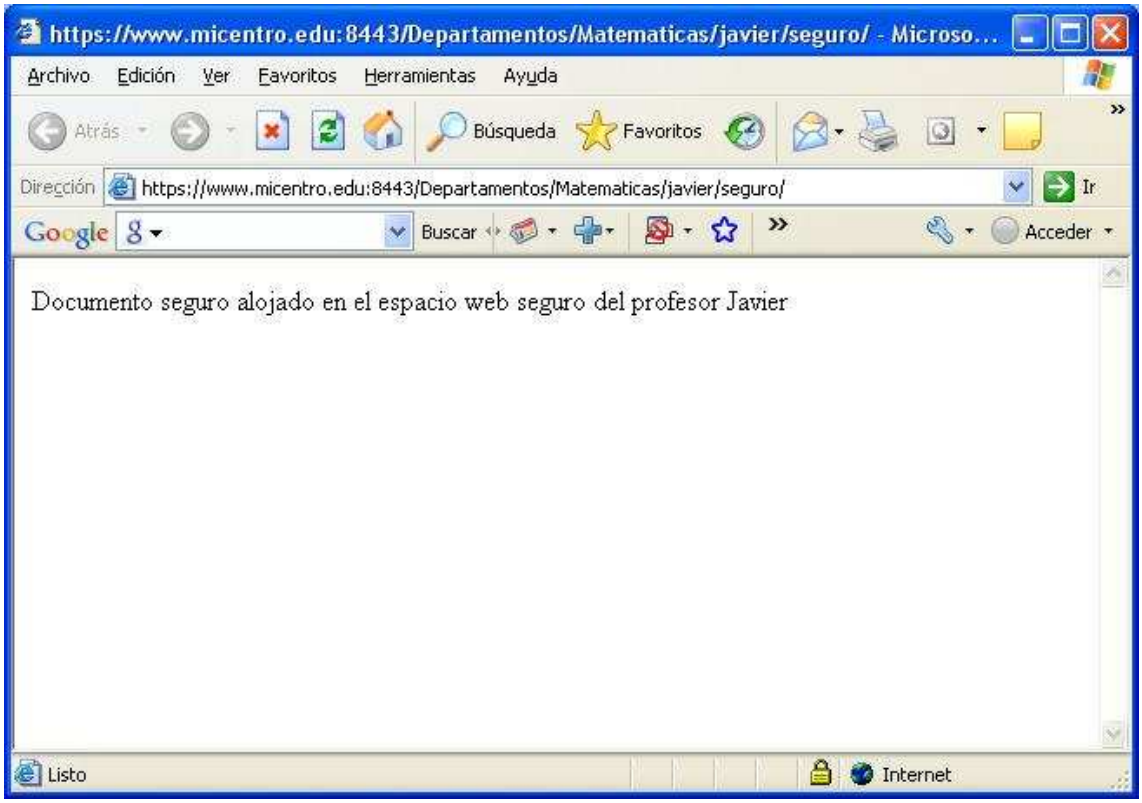


Imagen: ISA\entran54.JPG

NOTA: Previamente a mostrarse la página web mostrada en la imagen superior, se nos mostraría la siguiente advertencia de seguridad, que nos indica que el certificado presentado por el servidor no está emitido por una entidad certificadora de confianza, lo cual es lógico pues el equipo anfitrión no está integrado en el dominio "MiCentro.edu" y NO reconoce como válida a la entidad certificadora del equipo "SERVIDOR"; en la ventana de la imagen inferior pulsaremos sobre el botón "Sí" para continuar con la carga de la página web solicitada.

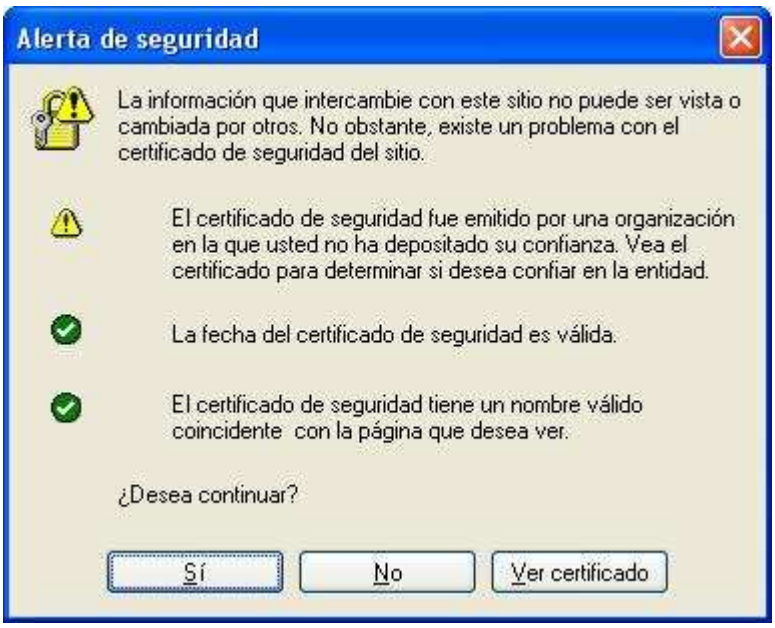


Imagen: ISA\entran55.JPG

Siguiendo el mismo proceso que hemos llevado a cabo anteriormente para crear múltiples reglas de publicación para algunos de los servicios prestados por nuestro equipo "SERVIDOR", podríamos definir nuevas reglas para otros servicios a los que quisiéramos acceder desde Internet, si bien en nuestro caso consideramos que con los ejemplos anteriores es suficiente.

Proxy Caché

En este apartado analizaremos las posibilidades que nos ofrece "ISA Server 2004" para ser utilizado como proxy-caché en el equipo "SERVIDOR".

La caché del servidor "ISA Server 2004" nos dotará de una doble función:

- Caché de reenvío (Forward Caching).- Proporcionará las páginas web que se encuentren almacenadas en su caché a los equipos internos de la red de nuestro centro.
- Caché inversa (Reverse Proxy).- Proporcionará las páginas web de los servidores internos de nuestra red que se encuentren almacenadas en la caché a los equipos externos que deseen acceder a los mismos.

NOTA: La caché del servidor proxy mejora sustancialmente el rendimiento de acceso al equipo "SERVIDOR", liberándolo además de mucha carga de CPU, al margen de la mejora en la velocidad de respuesta a las demandas de nuestros usuarios.

Si deseamos configurar los parámetros precisos para que el servidor proxy-caché funcione como deseemos, lanzaremos el administrador de "ISA Server 2004", para desplegar el contenido de la entrada "Configuración" de la matriz "SERVIDOR", situándonos a continuación

sobre la entrada "Caché", la cual está representada con un icono con una flecha roja apuntado hacia abajo, lo cual significa que actualmente el "ISA Server 2004" no está realizando la función de proxy-caché.

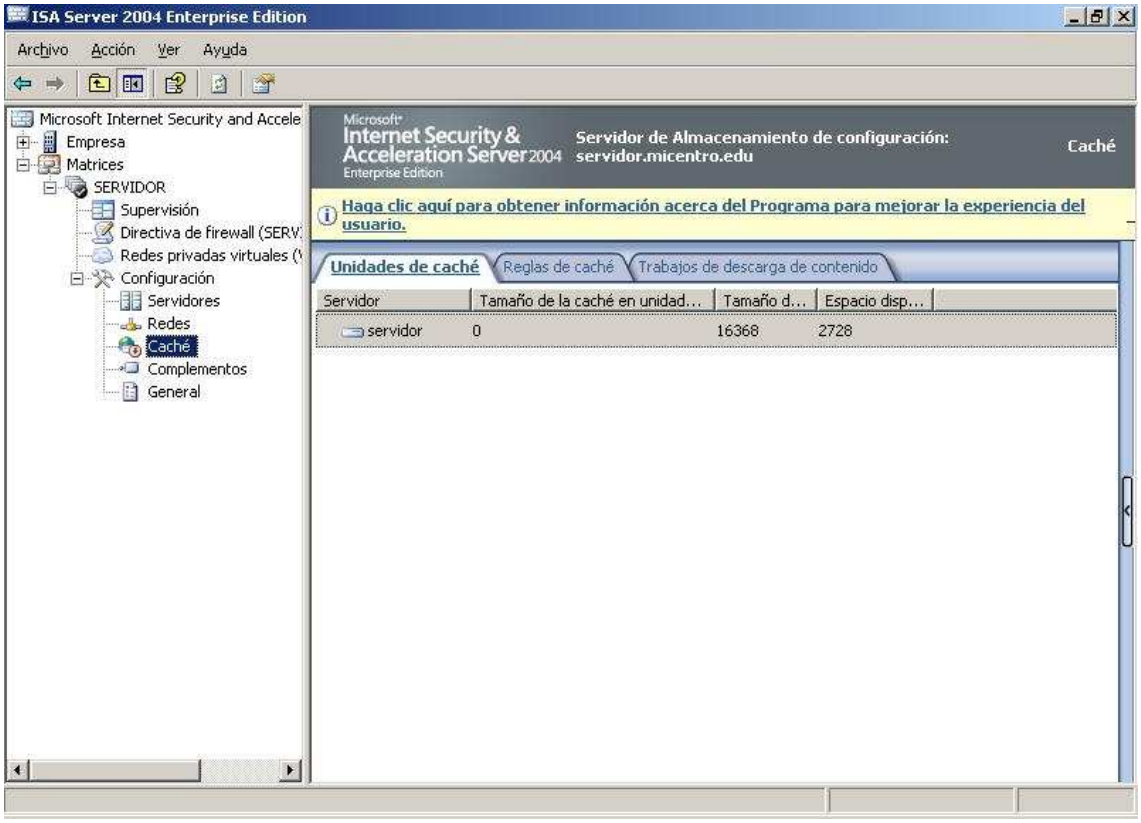


Imagen: ISA\proxy01.JPG

Si deseamos activar la caché nos situaremos sobre la pestaña "Unidades de caché", pulsando a continuación con el botón derecho del ratón sobre la entrada "servidor", para elegir la opción "Propiedades" en el desplegable correspondiente.

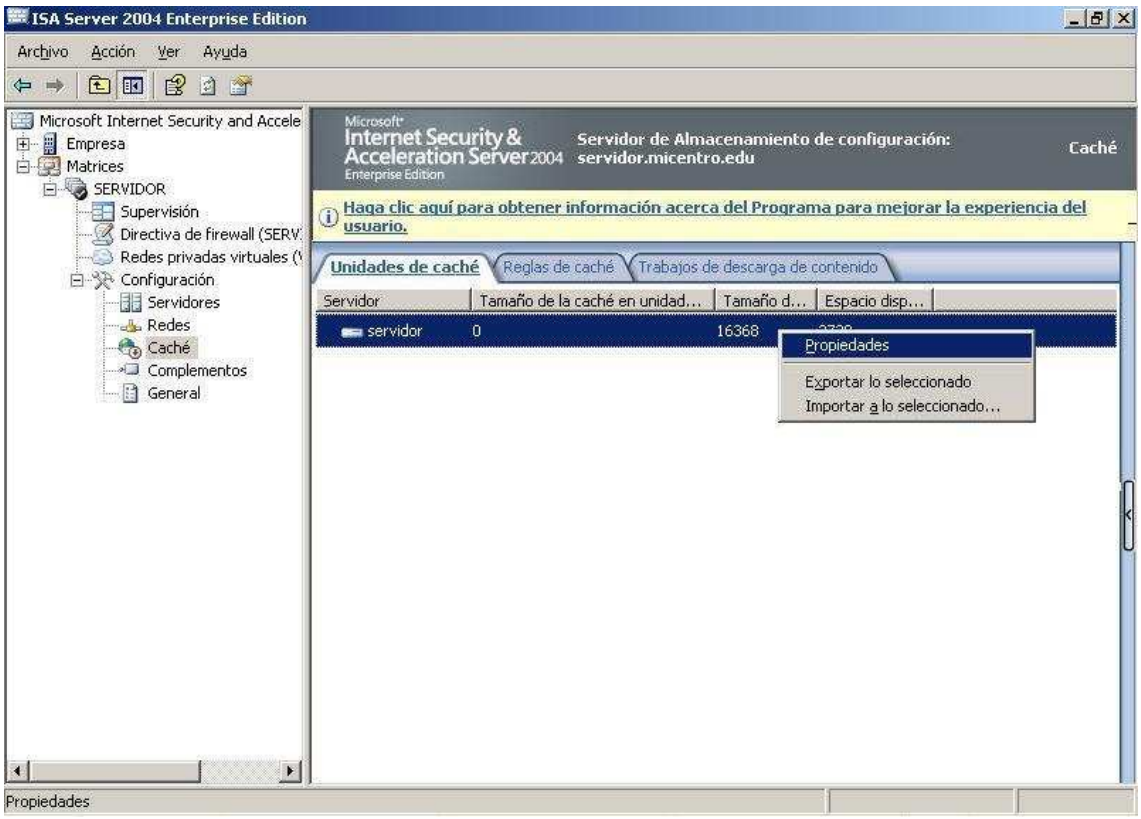


Imagen: ISA\proxy02.JPG

En la nueva ventana mostrada como resultado de la acción anterior nos situaremos sobre la unidad donde deseamos almacenar los elementos a cachear, en nuestro caso en la unidad "E:", y tras ello estableceremos en la caja de texto correspondiente el tamaño máximo de la caché, 1 Gb. (1.024 Mb.) en este caso, y tras ello pulsaremos sobre el botón "Establecer", de modo que cuando dicha ventana presente el aspecto mostrado en la imagen inferior, pulsaremos en ella sobre el botón "Aceptar".

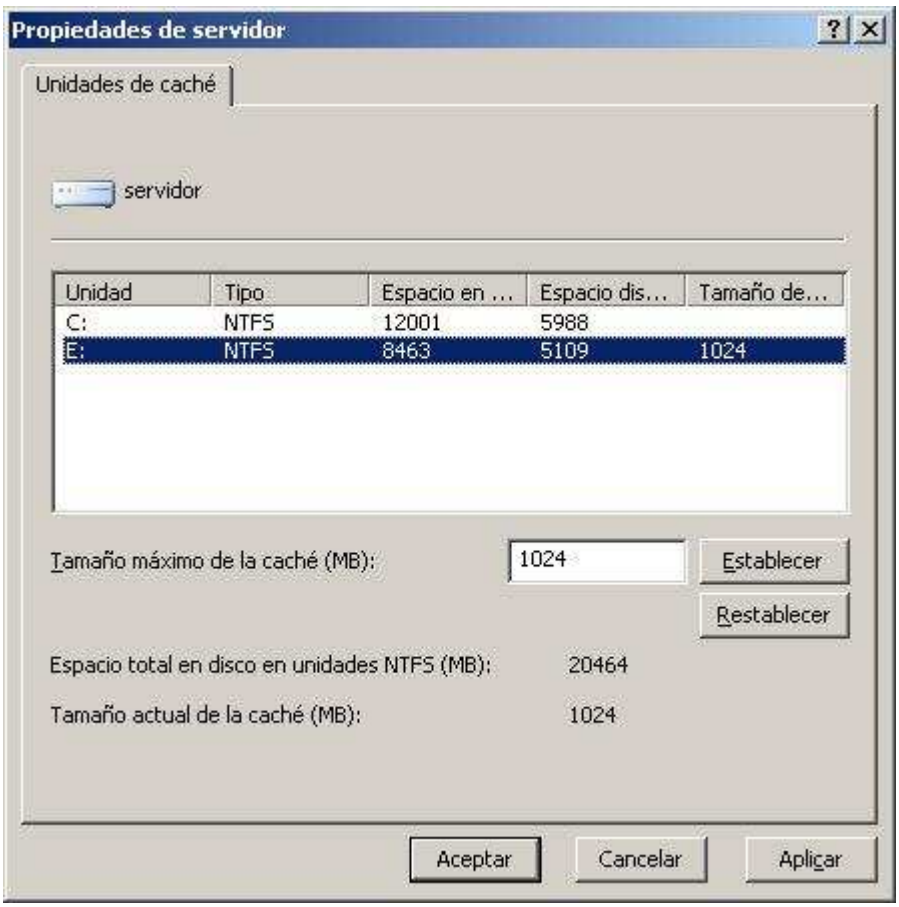


Imagen: ISA\proxy03.JPG

Tras ello pulsaremos en la ventana de administración del "ISA Server 2004" sobre el botón "Aplicar" para que los cambios se hagan efectivos.

Como resultado de la operación anterior se nos presenta la siguiente ventana, en la que activaremos el radio botón "Guardar los cambios y reiniciar los servicios", y tras ello pulsaremos sobre el botón "Aceptar".

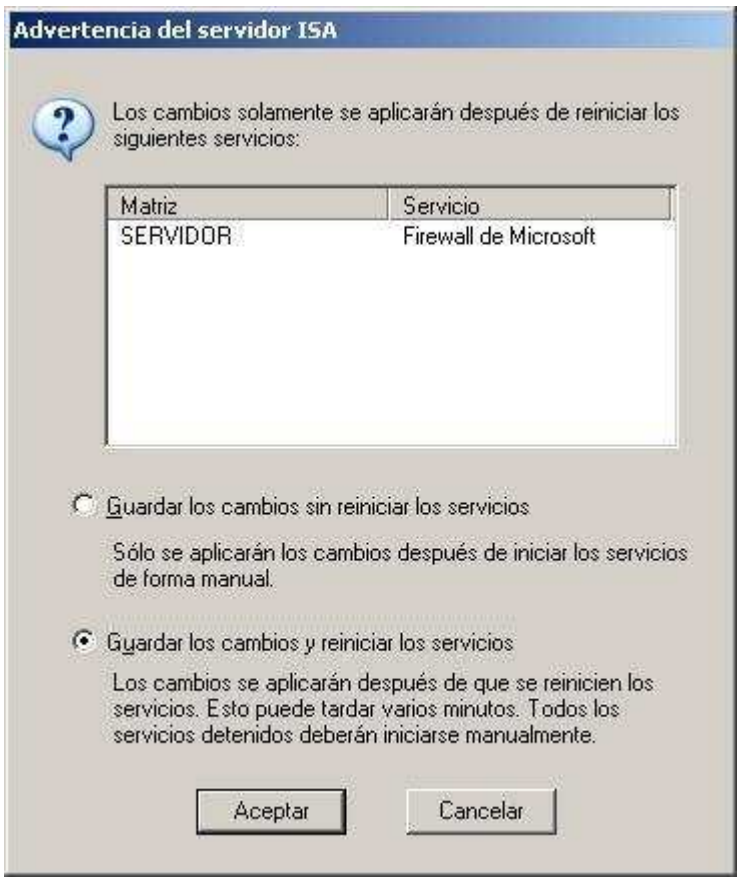


Imagen: ISA\proxy04.JPG

De vuelta a la ventana de administración del "ISA Server 2004" observaremos que la entrada "Caché" ya no tiene asociada la fecha roja apuntando hacia abajo, luego en este instante el "ISA Server 2004" instalado en el equipo "SERVIDOR" está realizando labor de cacheo de las páginas web visitadas.

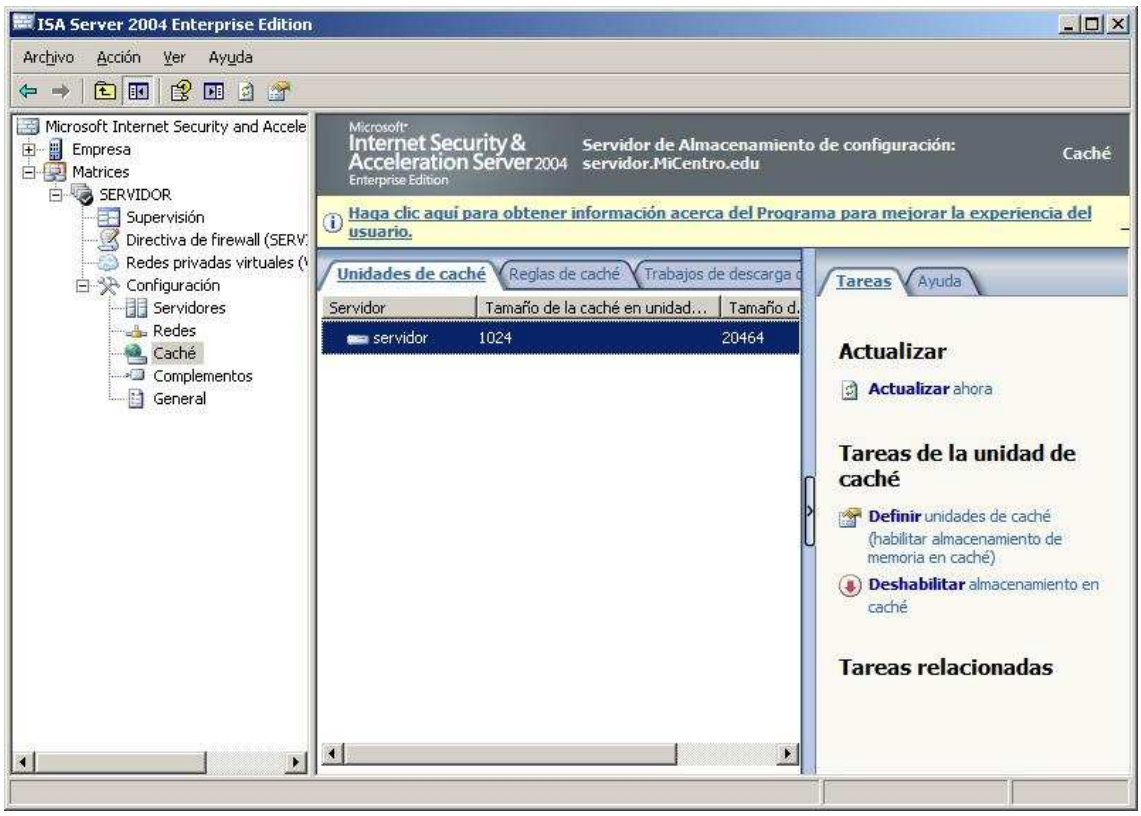


Imagen: ISA\proxy05.JPG

Una vez que tenemos activa la caché del "ISA Server 2004", podremos programar la descarga de determinados contenidos en la misma.

Supongamos por ejemplo que el profesorado de nuestro centro lo primero que hace cuando llega al mismo a las 9 horas de la mañana es acceder al contenido del portal educativo del ISFTIC, yendo a la URL "http://www.isftic.mepsyd.es/", en dicha circunstancia podría resultar interesante que a esa hora todos los contenidos de dicho portal estuvieran cacheados por el "ISA Server 2004", de modo que el acceso a los mismos fuera más rápido y además se liberase el ancho de banda de conexión a Internet de nuestro centro, pues bien, en dicho escenario la descarga programada de la caché es una solución idónea.

Para configurar la descarga programada de la caché del "ISA Server 2004", deberemos situarnos sobre la entrada "Caché" del apartado "Configuración" de la matriz "SERVIDOR", seleccionando a continuación la pestaña "Trabajos de descarga de contenido", para posteriormente en el marco de la derecha, colocarnos sobre la pestaña "Tareas", para finalmente pinchar sobre el enlace "Programar un trabajo de descarga de contenido".

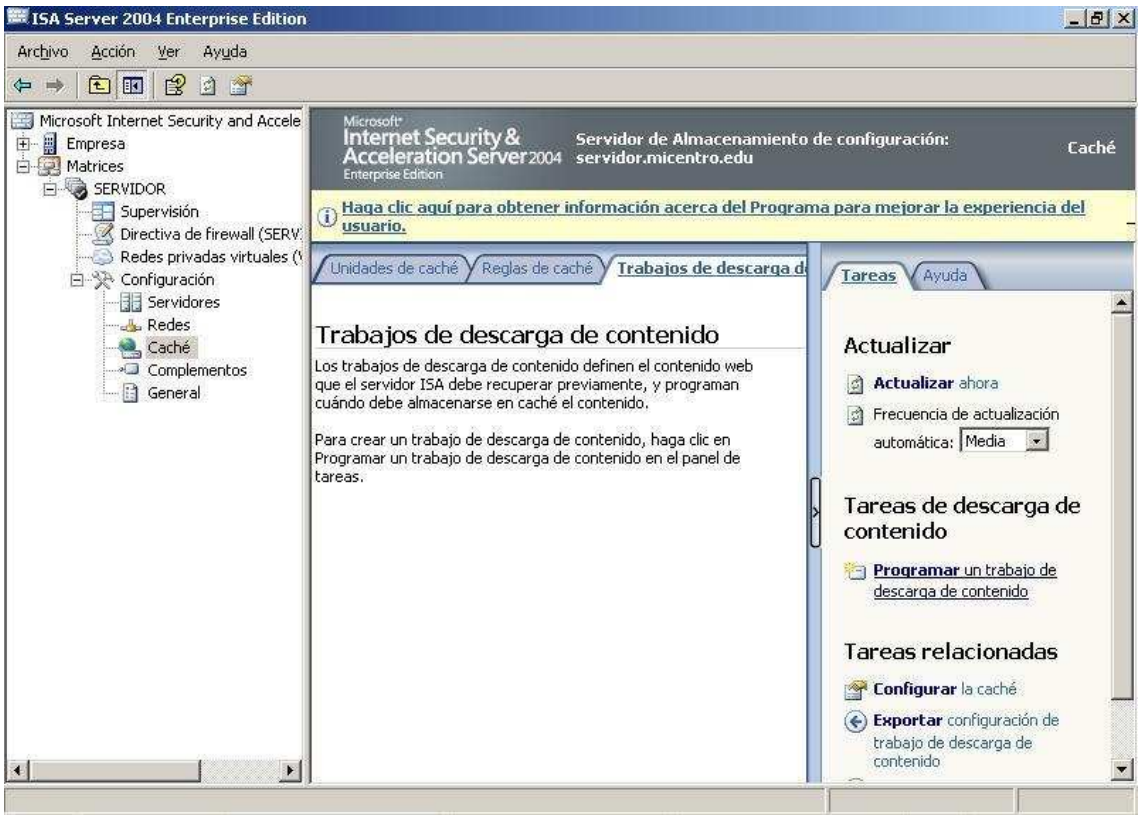


Imagen: ISA\proxy06.JPG

Como resultado de la acción anterior pasa a ser mostrada la siguiente ventana, en la que se nos informa de la necesidad de configurar ciertos parámetros para poder definir dichos trabajos; pulsaremos en ella sobre el botón "Sí" para continuar.

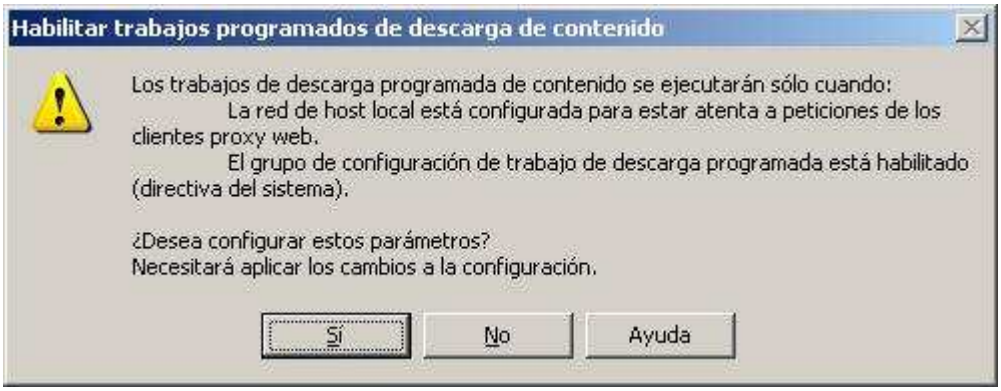


Imagen: ISA\proxy07.JPG

Como siempre, deberemos recordar pulsar sobre el botón "Aplicar" para que las configuraciones anteriores pasen a ser efectivas.

Tras ello, pulsaremos de nuevo sobre el enlace "Programar un trabajo de descarga de contenido", pasando a ser mostrada en esta ocasión la siguiente ventana del asistente de

creación de trabajo de descarga de contenido, en cuya primera ventana teclearemos "IFSTIC" en la caja de texto correspondiente como nombre para la descarga programada.

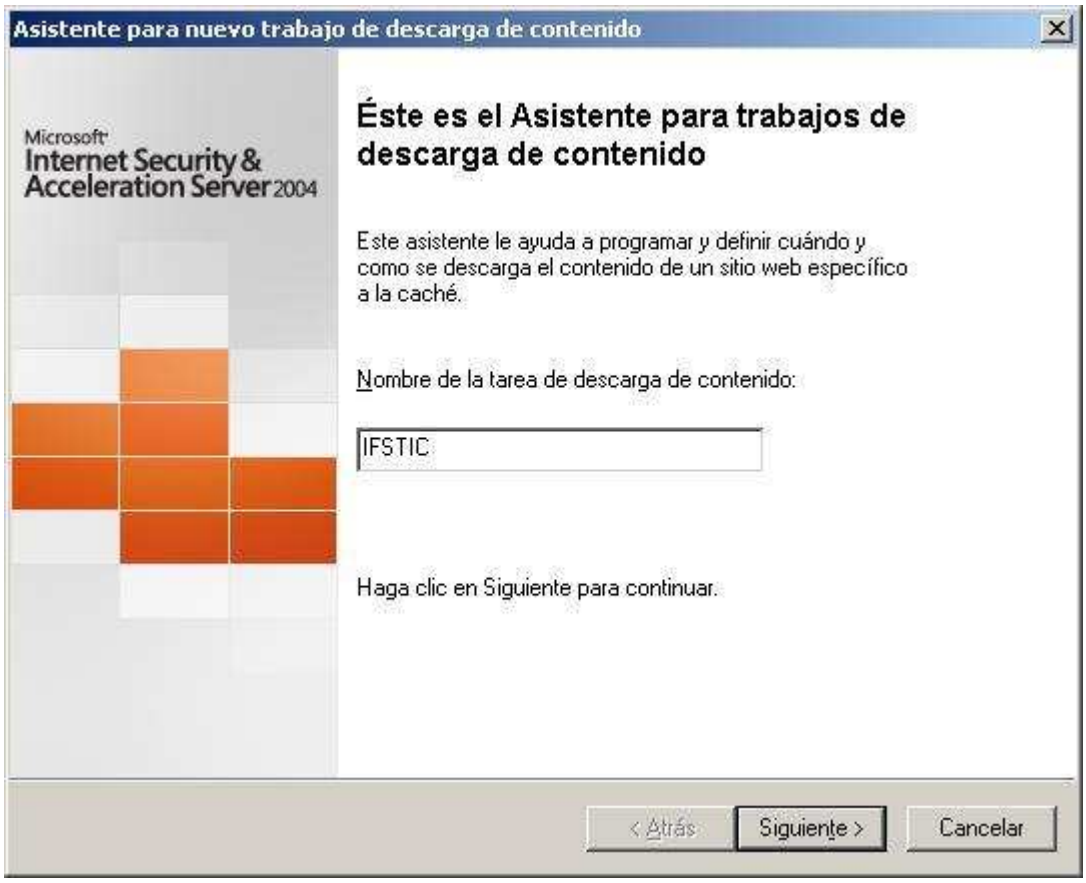


Imagen: ISA\proxy08.JPG

En la siguiente ventana el asistente nos pregunta por la frecuencia con la cual deberá realizarse el trabajo en cuestión, eligiendo en nuestro caso una frecuencia diaria mediante la selección del radio botón "Diariamente", y pulsando posteriormente sobre el botón "Siguiente".

Imagen: ISA\proxy09.JPG

A continuación se nos presentará la siguiente ventana, en la que deberemos especificar la fecha desde la que queremos que comience a aplicarse la descarga y la hora a la que se efectuará la misma, dando por válida la fecha que el sistema nos ofrece por defecto, e indicando como hora de comienzo de la descarga las 8 horas de la mañana, para que dichos contenidos estén almacenados en la caché a la hora en la que el profesorado llega al centro, es decir a las 9 de la mañana.

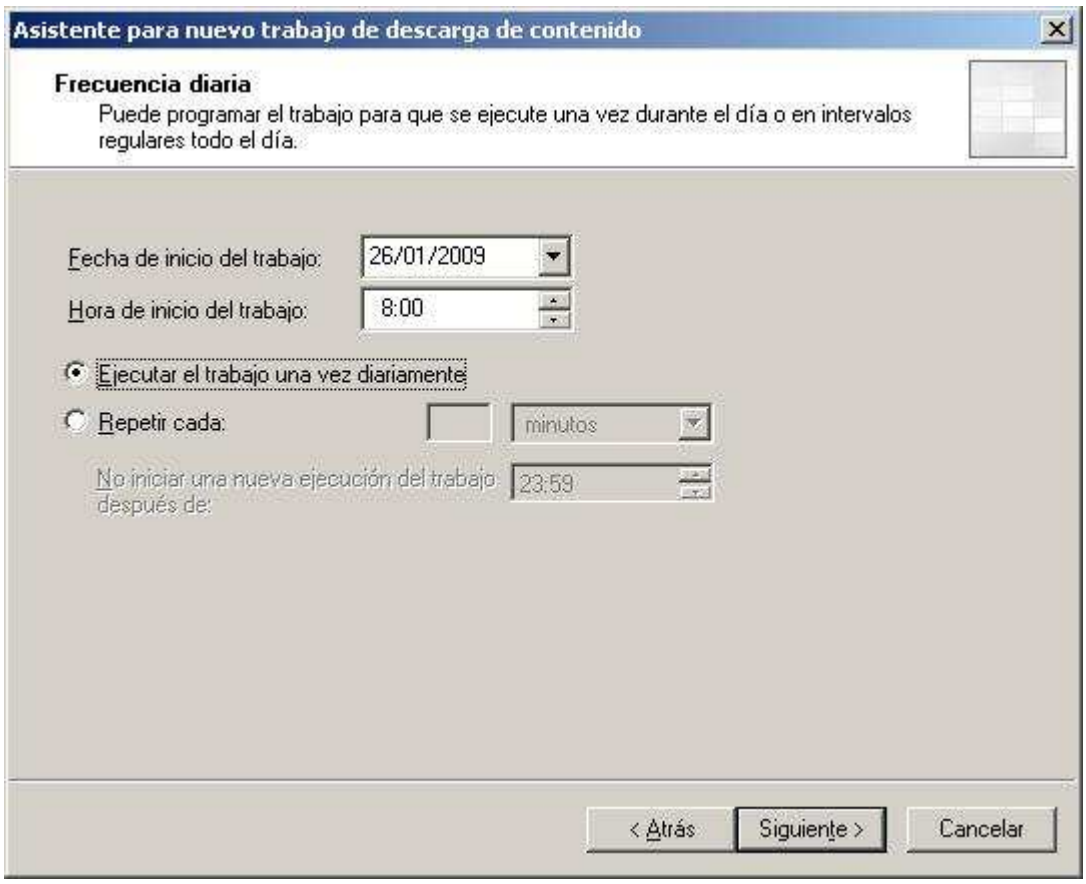


Imagen: ISA\proxy10.JPG

En la siguiente ventana especificaremos la URL que deseamos descargar, en nuestro caso "http://www.isftic.mepsyd.es", y además activaremos la casilla "No seguir el vínculo fuera del nombre de dominio de direcciones URL especificado", para evitar que se cacheen páginas externas con las que enlace el portal del "ISFTIC".

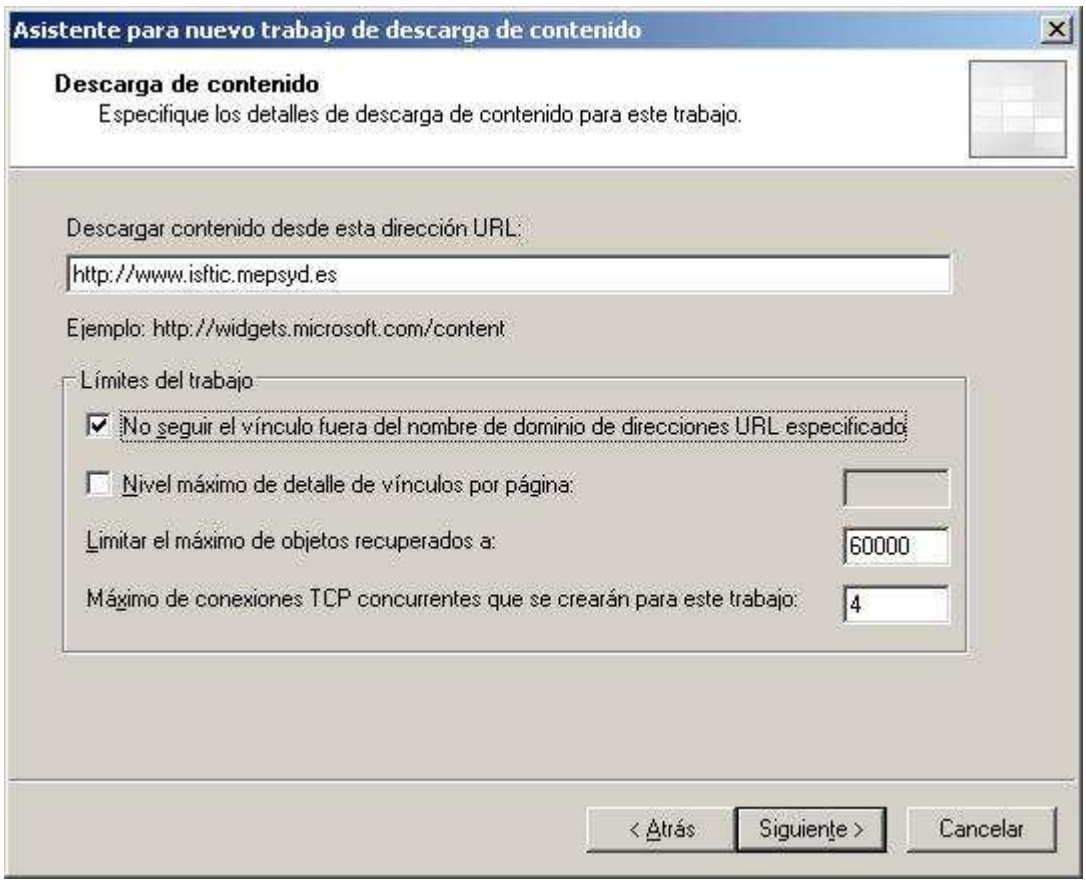


Imagen: ISA\proxy11.JPG

En la siguiente ventana mostrada por el asistente deberemos indicar las condiciones y vigencia del cacheo realizado, si bien en nuestro caso dejaremos asociados los valores que por defecto nos ofrece el asistente, y pulsaremos directamente en ella sobre el botón "Siguiente".

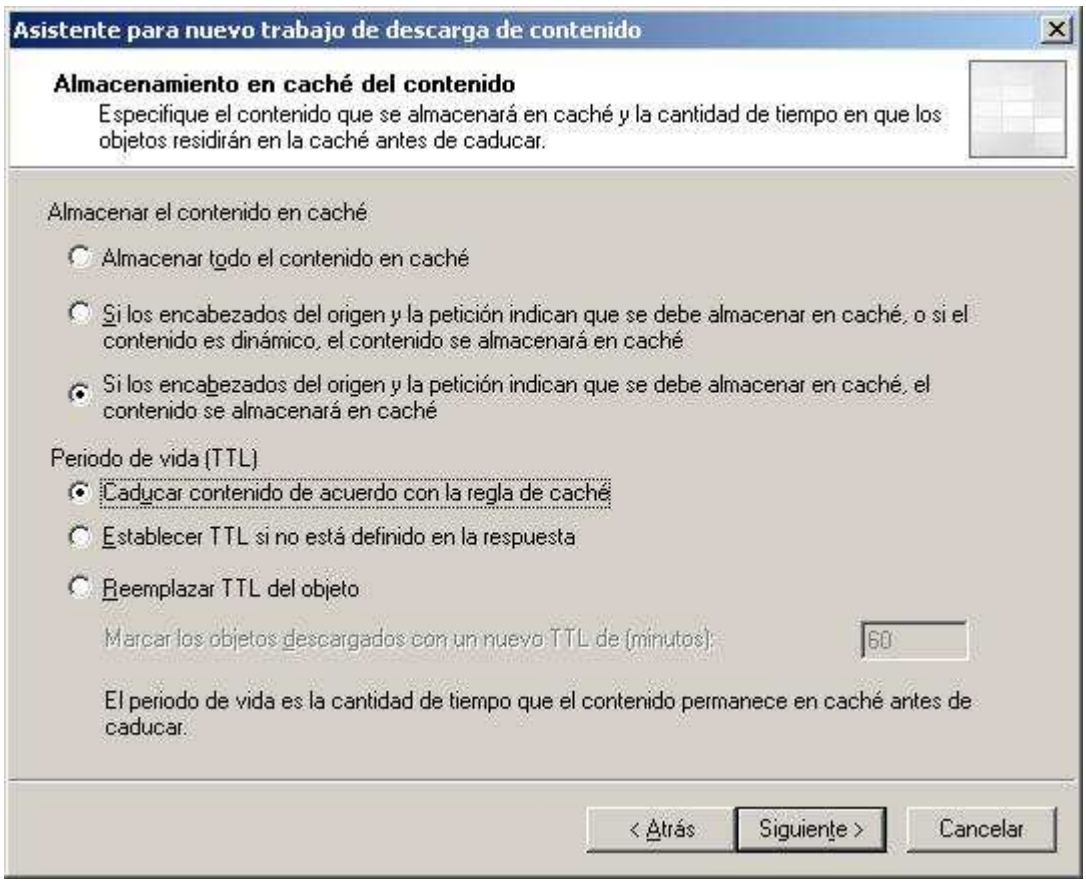


Imagen: ISA\proxy12.JPG

En la última ventana del asistente pulsaremos directamente sobre el botón "Finalizar" para dar por válidas las configuraciones realizadas.

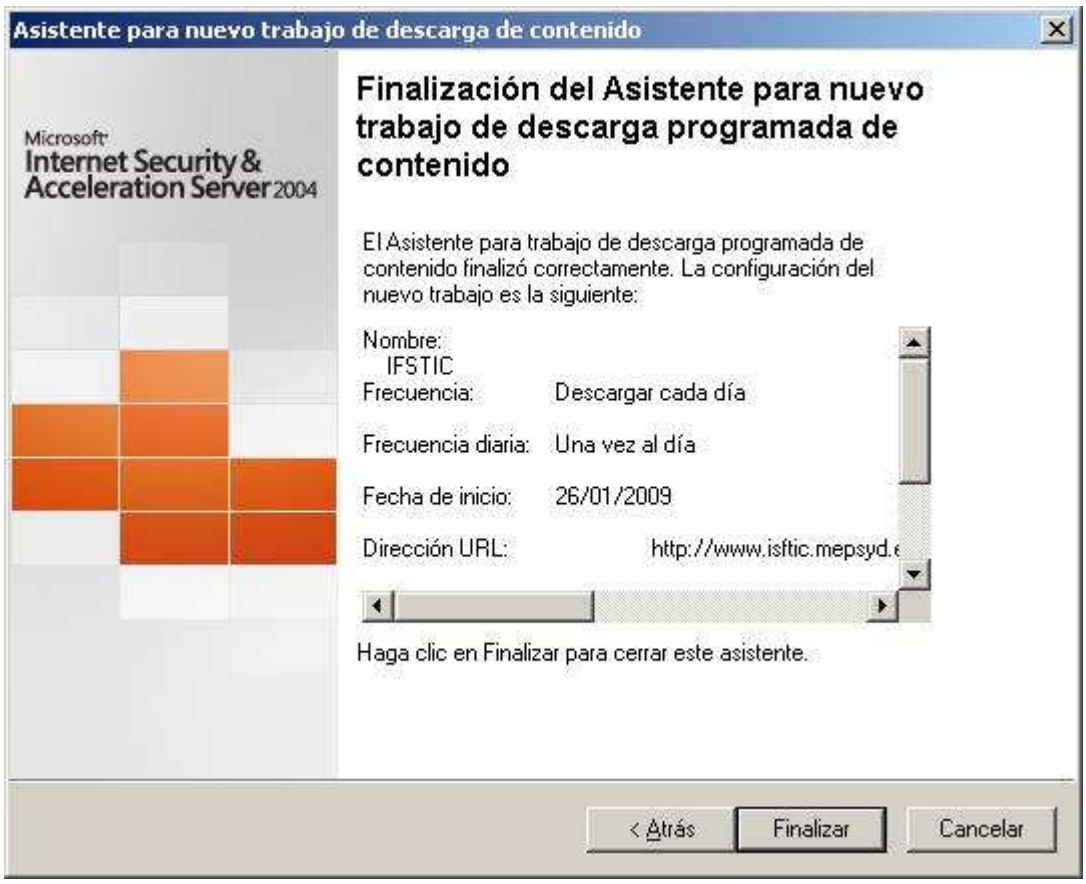


Imagen: ISA\proxy13.JPG

Una vez configurado el trabajo de descarga anterior, podremos comprobar la existencia del mismo en el apartado "Trabajos de descarga", tal y como vemos en la imagen inferior.

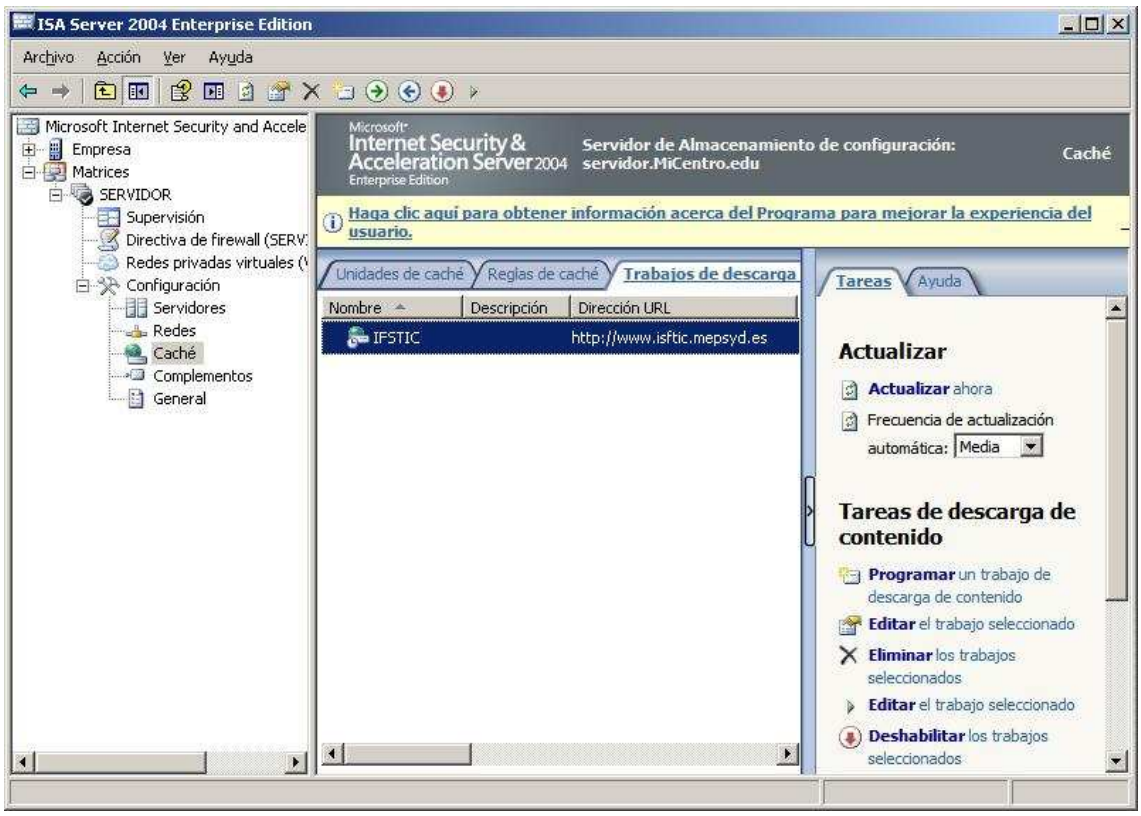


Imagen: ISA\proxy14.JPG

Otra de las funcionalidades muy útiles del proxy-caché del "ISA Server 2004" es la descarga de los contenidos de la caché más visitados cuando su vigencia esté a punto de caducar.

"ISA Server 2004" utiliza para ello su función de caché activa, que modo automático accede a las páginas web más visitadas para actualizar los contenidos de la caché, de forma que siempre tengamos chacheadas la versión más actual de dichas páginas web.

Podremos comprobar la configuración de la caché activa ubicándonos sobre la entrada "Caché" del apartado "Configuración" de la matriz "SERVIDOR", concretamente en la zona derecha de la ventana mostrada, donde podremos confirmar que actualmente la actualización de los contenidos de la caché está configurada a "Media", tal y como se ve en la imagen inferior.

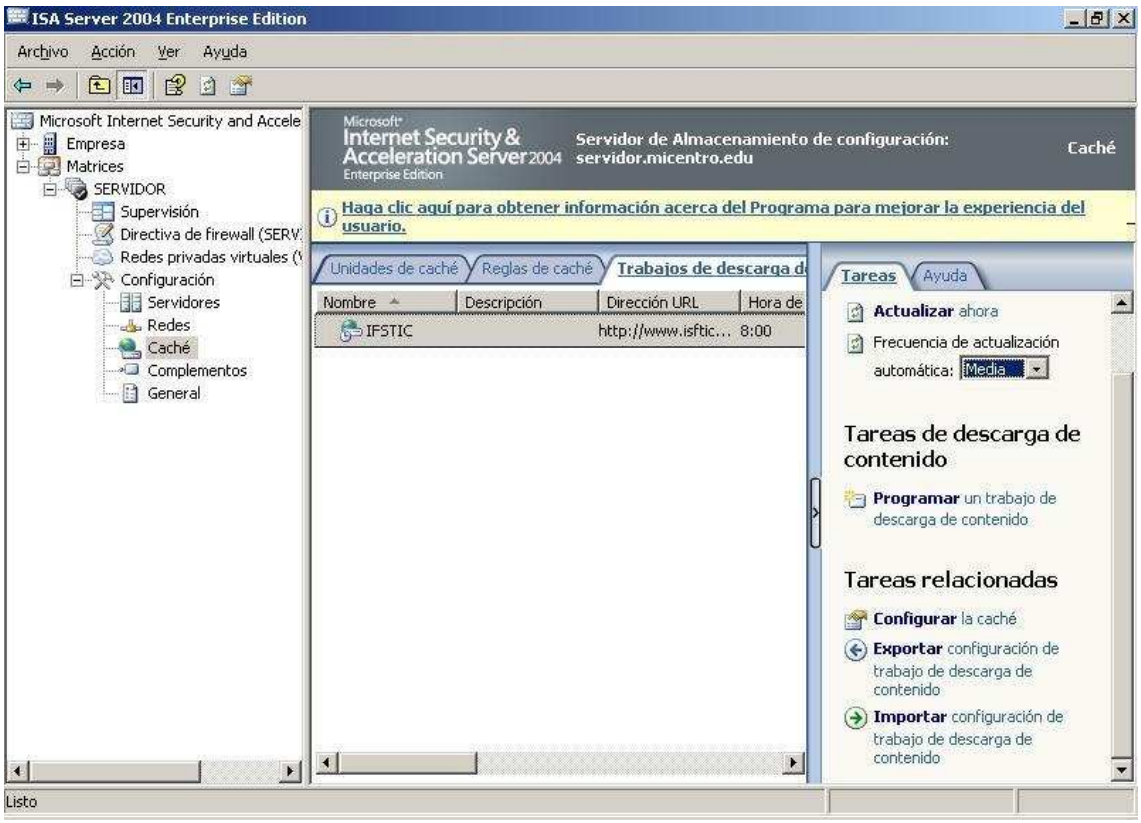


Imagen: ISA\proxy15.JPG

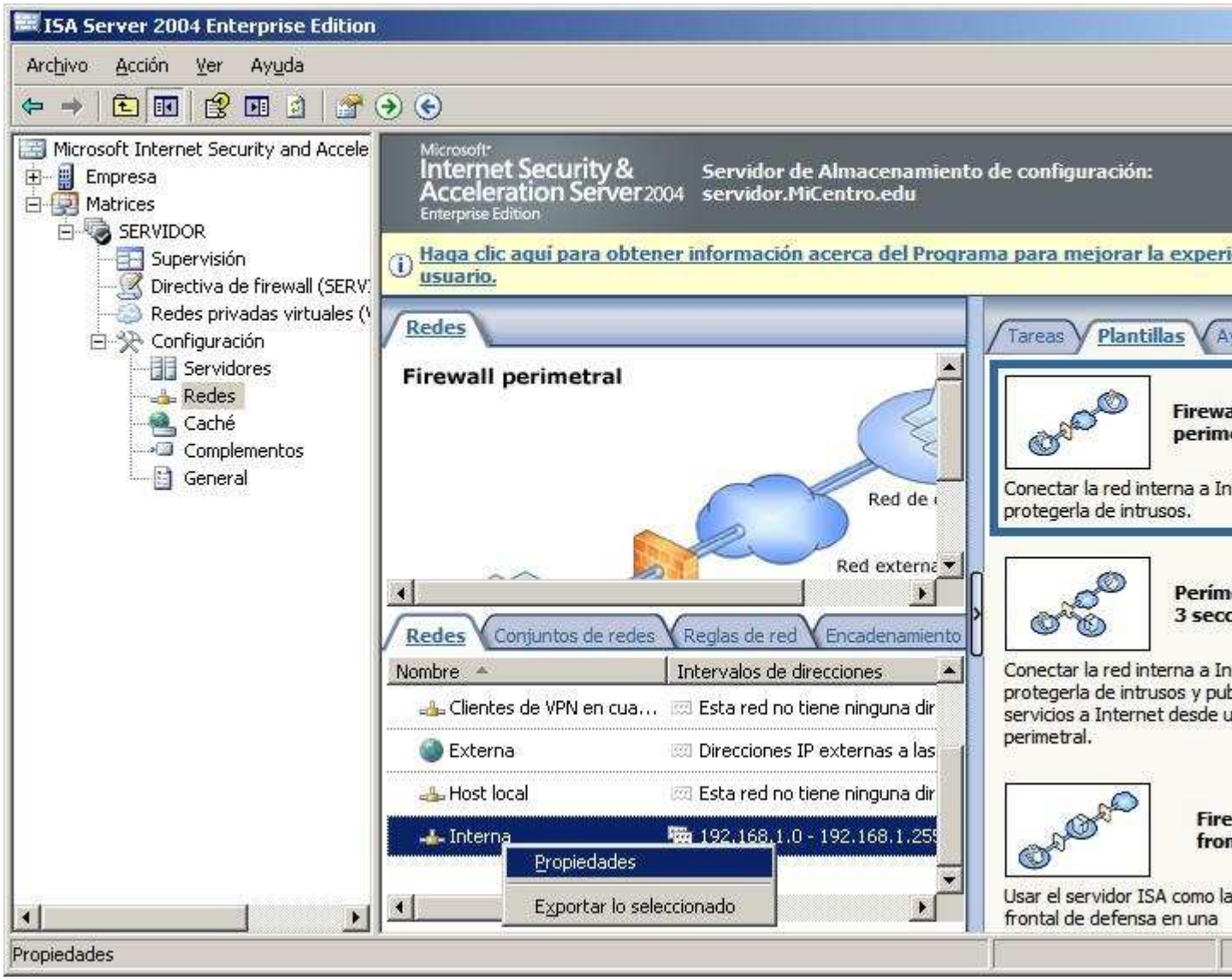
Podremos variar la configuración correspondiente a la frecuencia de actualización, aumentándola, disminuyéndola o incluso anulándola, pulsando en el desplegable correspondiente y eligiendo la opción deseada.

VPN

Finalmente en este apartado analizaremos la posibilidad de utilizar "ISA Server 2004" como servidor de VPN (red privada virtual), de modo que nuestro equipo "SERVIDOR" acepte conexiones de clientes externos desde Internet.

Antes de comenzar con la configuración propia del servidor VPN, hemos de cambiar el rango de direccionamiento de la red "Interna" del servidor "ISA Server 2004", reservando algunas de dichas direcciones para poder asociárselas a los clientes que acceden mediante VPN a la red interna de nuestro centro.

Para ello nos situaremos sobre la entrada "Redes" del apartado "Configuración" de la matriz "SERVIDOR", y tras ello pulsaremos con el botón derecho del ratón sobre la red "Interna" para seleccionar la opción "Propiedades" en el desplegable correspondiente.

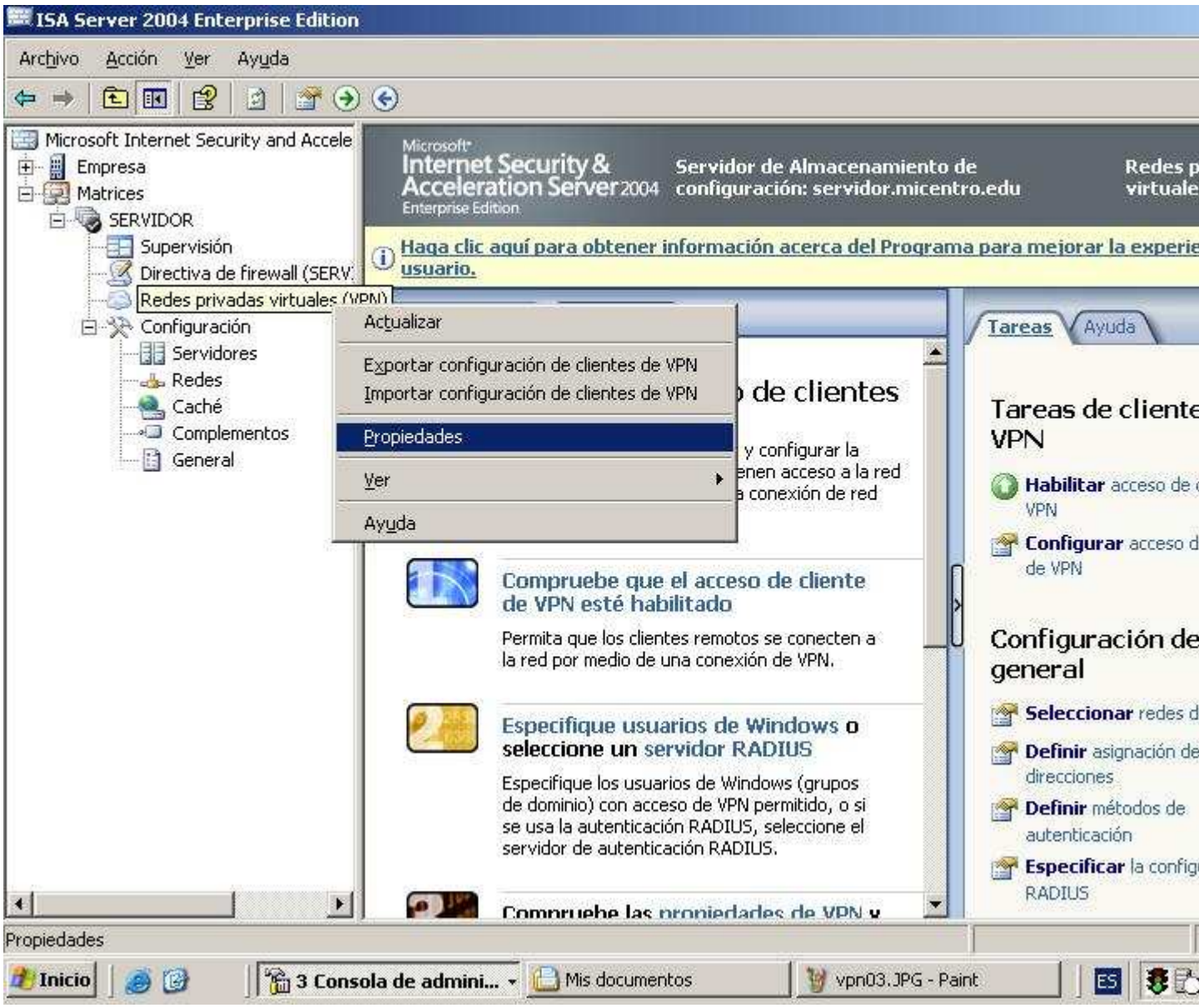


En la nueva ventana mostrada como resultado de la acción anterior nos situaremos sobre la pestaña "Direcciones", para seleccionar a continuación la red definida ("192.168.1.0" a "192.168.1.255"), tras lo cual pulsaremos sobre el botón "Editar" para modificar dicha red, indicando como rango final "192.168.1.229" en vez "192.168.1.255"; tras ello pulsaremos sobre el botón "Agregar intervalo" para añadir el intervalo "192.168.1.241" a "192.168.1.255", de modo que cuando la ventana reseñada presente finalmente el aspecto mostrado en la imagen inferior, pulsaremos sobre el botón "Aceptar".

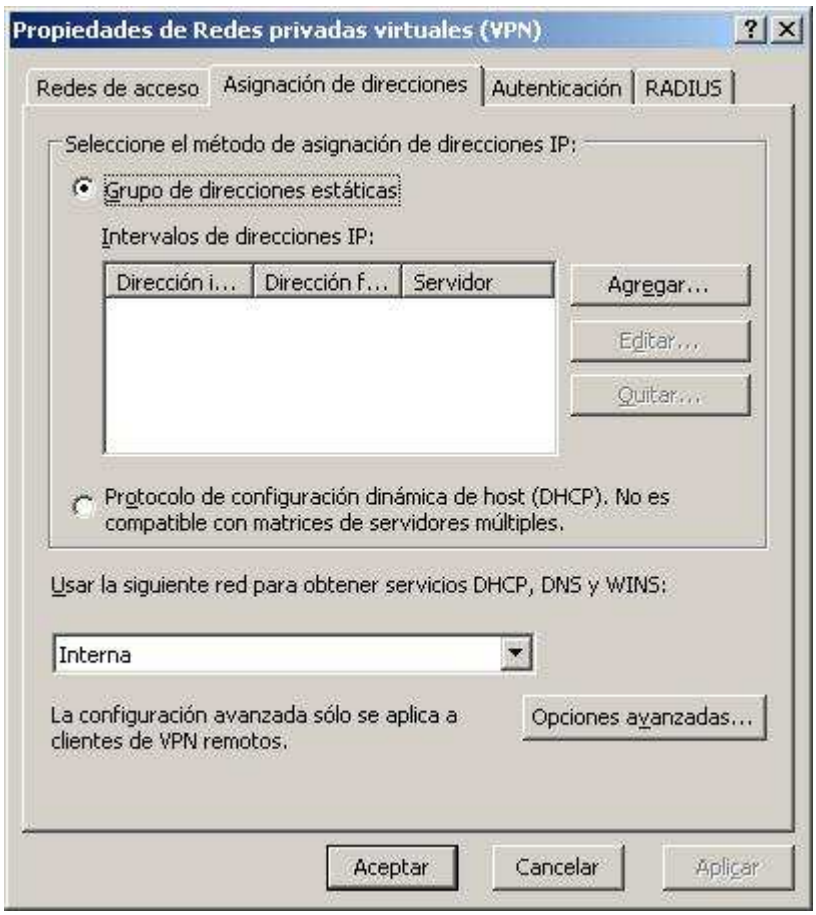
NOTA: Con la operación anterior hemos liberado 11 direcciones IP del rango de la red "Interna" para que puedan ser utilizadas por los clientes de VPN; las direcciones que hemos excluido serán las que utilicemos para asociar los clientes VPN, de modo que NO deberán ser asociadas a los equipos clientes internos de nuestra red.

Como siempre deberemos recordar pulsar sobre el botón "Aplicar" para que las modificaciones anteriores pasen a tener efecto.

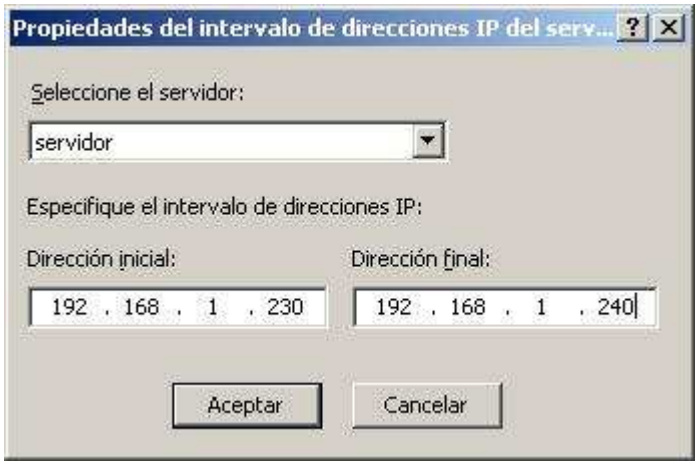
El siguiente paso que debemos llevar a cabo para que el servidor "ISA Server 2004" efectúe la labor de servidor VPN, es ubicarnos sobre la entrada "Redes Privadas Virtuales (VPN)" de la matriz "SERVIDOR", y a continuación pulsar sobre ella con el botón derecho del ratón para elegir la opción "Propiedades" en el desplegable correspondiente.



Como resultado de la acción anterior pasa a ser mostrada la siguiente ventana en la que nos ubicaremos sobre la pestaña "Asignación de direcciones", y tras ello pulsaremos sobre el botón "Agregar" asociado al radio botón "Grupo de direcciones estáticas".

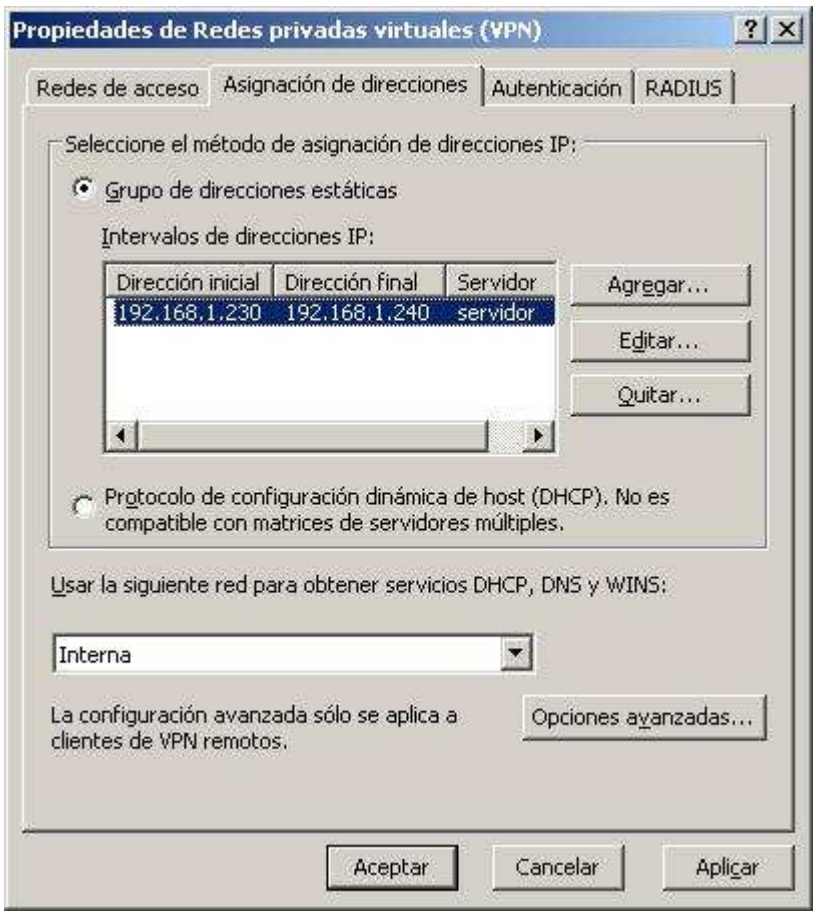


A continuación se nos presenta la siguiente ventana, en la que seleccionaremos en el desplegable "Seleccione el servidor", la única opción disponible, "servidor", y posteriormente indicaremos el rango de direccionamiento IP que vamos a asociar a nuestros clientes VPN, en nuestro caso de "192.168.1.230" a "192.168.1.240" inclusive, para finalmente pulsar sobre el botón "Aceptar".



NOTA: En el rango de direccionamiento de la VPN hemos de especificar una dirección IP más del número máximo de clientes de VPN que se pueden conectar simultáneamente, luego dado que hemos reservado 11 direcciones IP para las conexiones VPN, podremos tener un máximo de 10 conexiones VPN simultáneas.

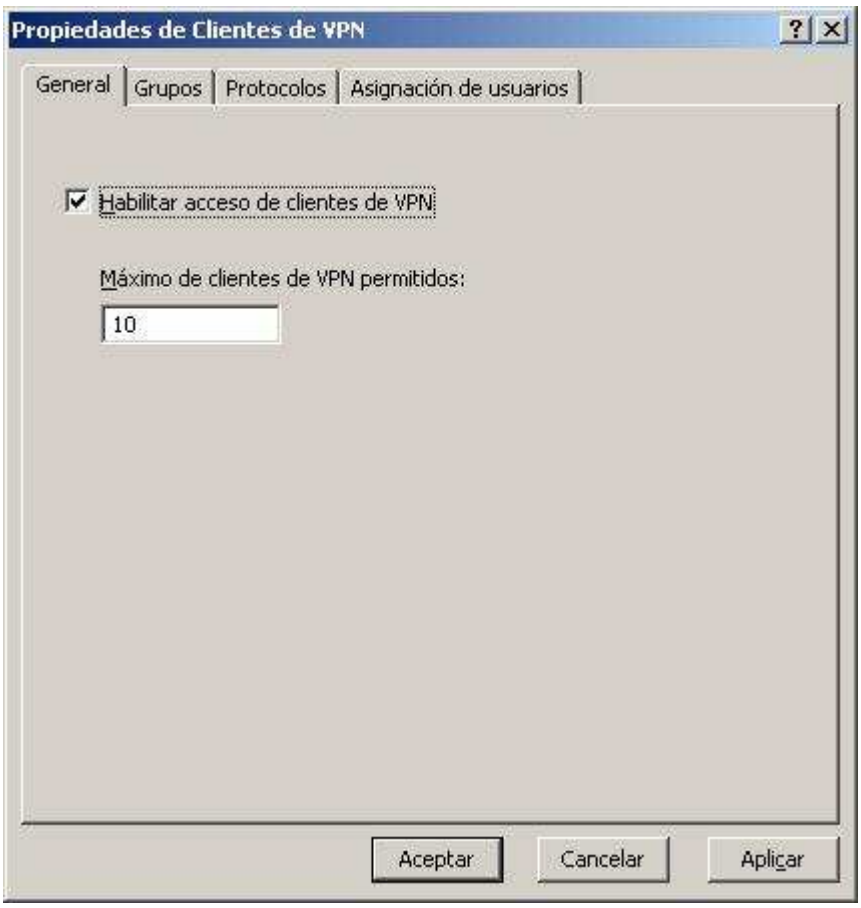
De vuelta a la ventana de las propiedades de VPN, ya aparecerá especificado el rango de direcciones IP a servir a los clientes de VPN, tal y como se muestra en la imagen inferior; en dicha ventana pulsaremos sobre el botón "Aceptar" para continuar.



De nuevo hemos de recordar pulsar sobre el botón "Aplicar" en la ventana del administrador de "ISA Server 2004" para que los cambios pasen a ser efectivos.

Una vez realizada la configuración anterior, a continuación hemos de indicar el número de conexiones simultáneas de clientes VPN permitidas, para lo cual nos ubicaremos sobre la entrada "Redes Privadas Virtuales (VPN)" de la matriz "SERVIDOR", y a continuación en el marco situado a la derecha pincharemos sobre el enlace "Configurar acceso de cliente de VPN" de la pestaña "Tareas".

En la nueva ventana mostrada como resultado de la acción anterior nos situaremos sobre la pestaña "General", activando la casilla "Habilitar acceso a clientes de VPN" e indicando posteriormente el valor "10" como el número máximo de clientes VPN simultáneos permitidos.

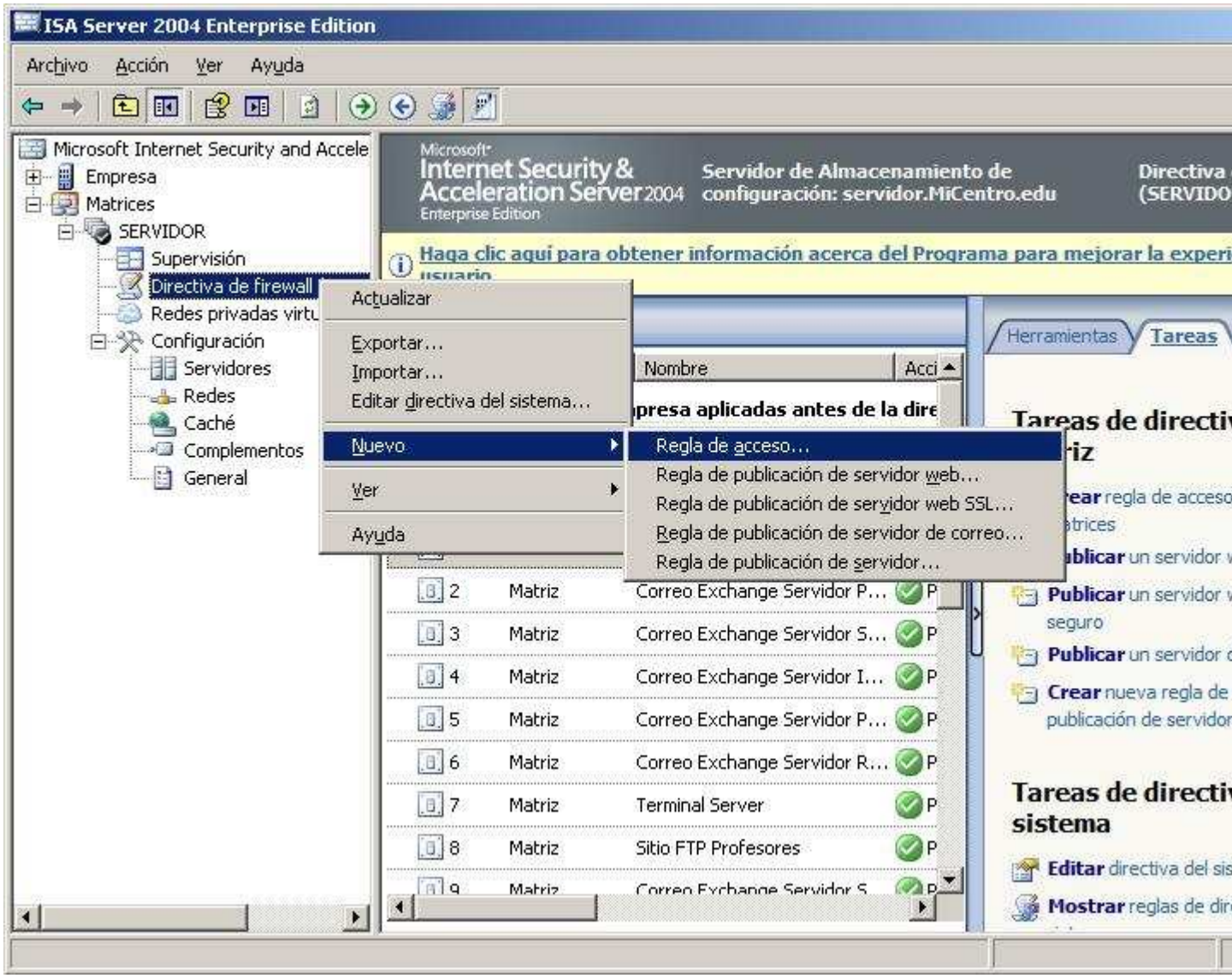


A continuación nos situaremos sobre la pestaña "Grupos" en la ventana de la imagen superior, para habilitar el acceso a través de la VPN a la red de nuestro centro a los usuarios deseados; en nuestro caso dotaremos de dicho acceso a los profesores de nuestro centro, luego en la ventana de la imagen inferior, pulsaremos sobre el botón "Agregar" para incluir al grupo "Profesores" entre los grupos que tienen acceso a la red del centro mediante una conexión VPN,

Cuando pulsemos sobre el botón "Aceptar" en la ventana de la imagen superior, se nos presentará la siguiente ventana de advertencia en la cual pulsaremos directamente sobre el botón "Aceptar" para proceder a su cierre.

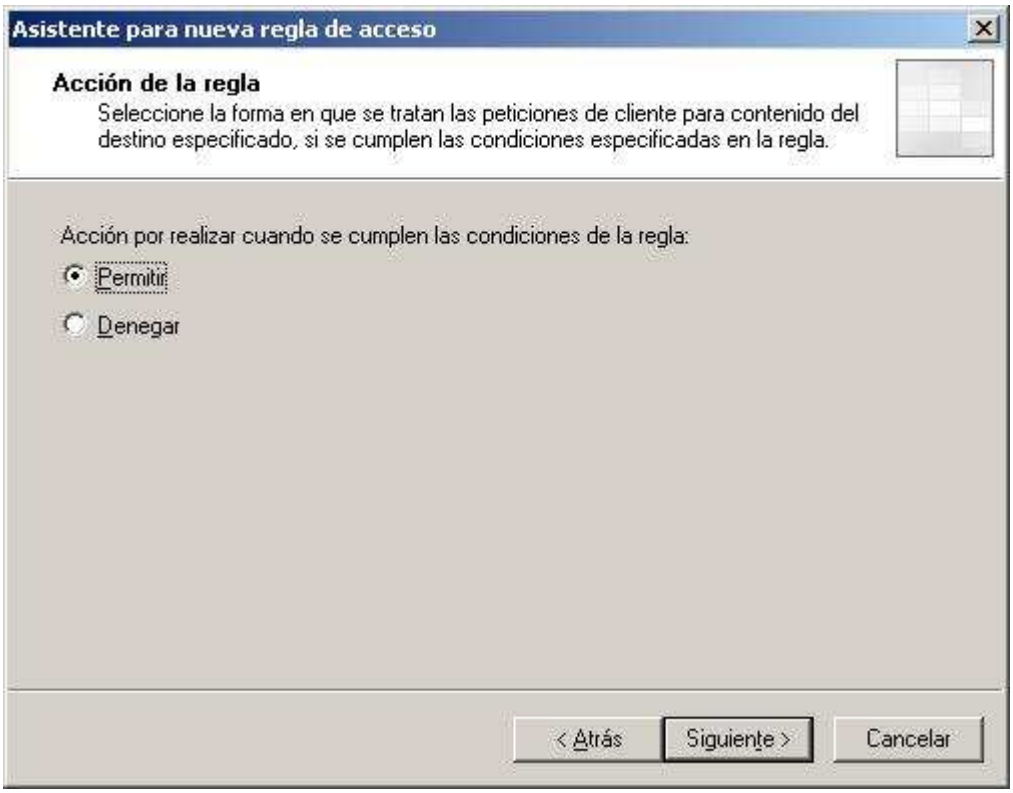
Deberemos recordar pulsar sobre el botón "Aplicar" en la ventana de administración de "ISA Server 2004" para que los cambios se hagan efectivos.

El último paso que debemos llevar a cabo para configurar la conexión VPN consiste en habilitar una regla de acceso para las conexiones de los clientes VPN, para lo cual en primer lugar pulsaremos con el botón derecho del ratón sobre la entrada "Directiva de firewall (SERVIDOR)" de la matriz "SERVIDOR", para elegir "Nuevo", y luego "Regla de acceso", en los desplegables correspondientes.

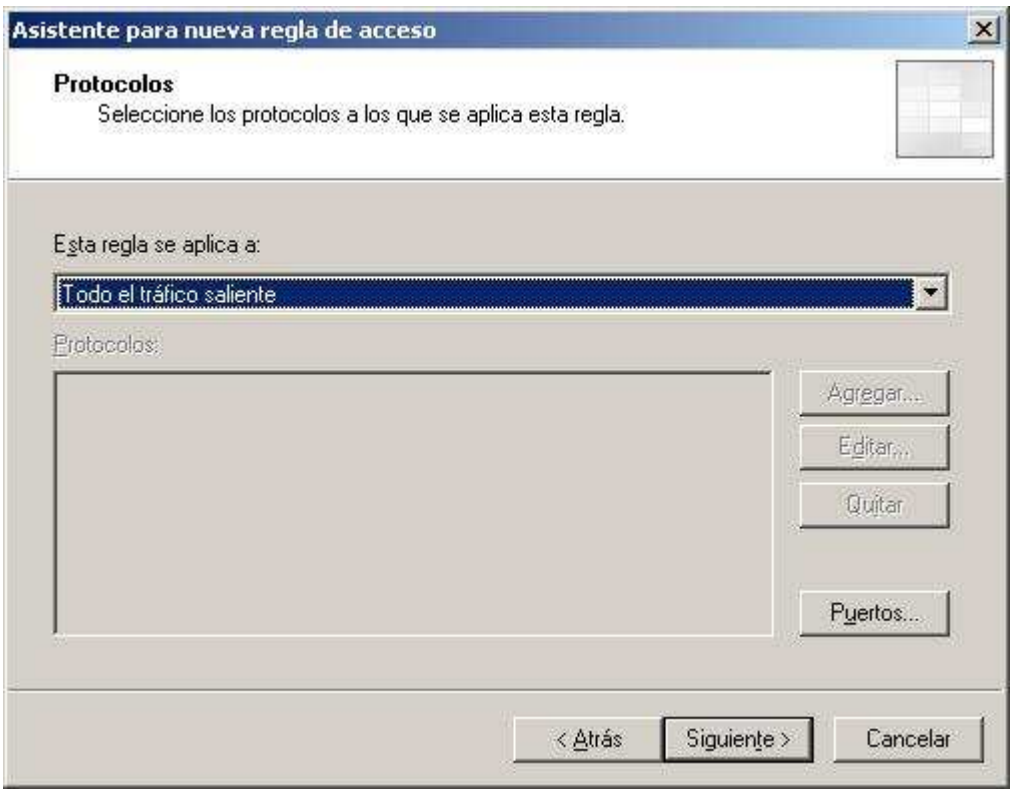


Como resultado de la acción anterior pasa a ser mostrada la siguiente ventana, en la cual indicaremos "Conexion VPN" como nombre para la nueva regla que vamos a crear, y tras ello pulsaremos sobre el botón "Siguiente".

En la siguiente ventana del asistente de creación de nueva regla seleccionaremos el radio botón "Permitir", para indicar que la regla que estamos creando es de permiso, y tras ello pulsaremos sobre el botón "Siguiente".

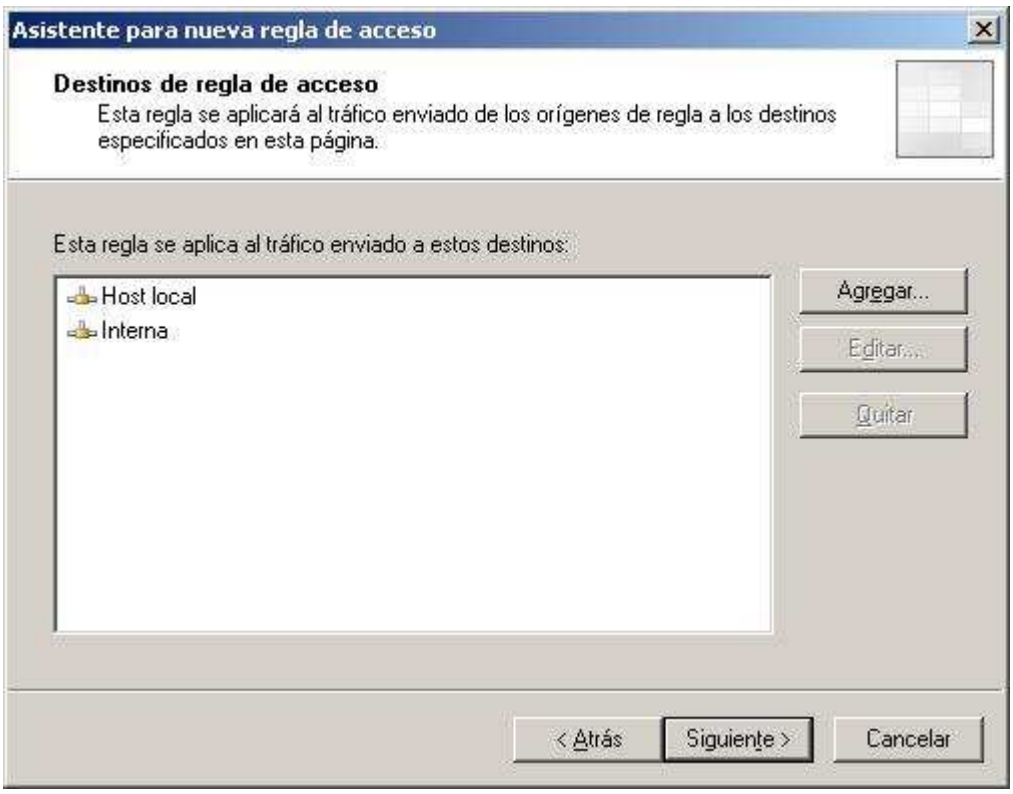


En la nueva ventana mostrada seleccionaremos la opción "Todo el tráfico saliente" en el desplegable correspondiente, y tras ello pulsaremos sobre el botón "Siguiente".



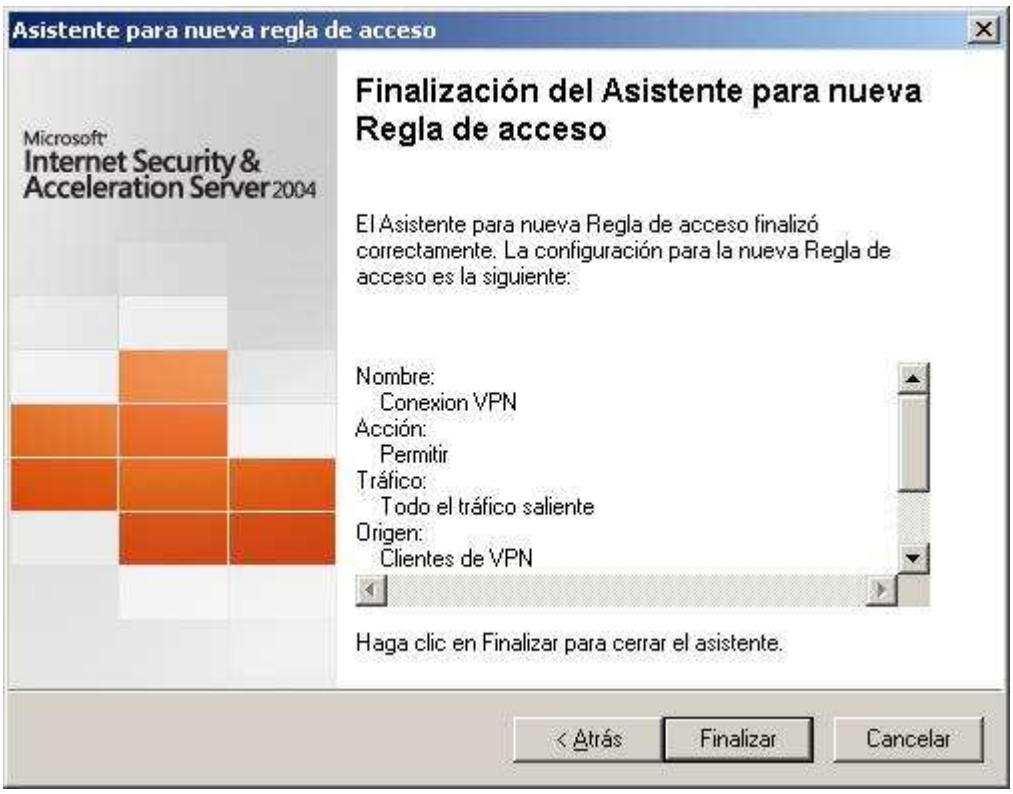
A continuación se nos presenta la siguiente ventana, en la cual pulsaremos sobre el botón "Agregar" para seleccionar "Clientes de VPN" en el apartado de "Redes", de modo que finalmente la ventana indicada deberá quedar tal y como se muestra en la imagen inferior.

Tras ello deberemos indicar los destinos a los cuales será aplicada esta regla, así pues pulsaremos en la ventana de la imagen inferior sobre el botón "Agregar", para incluir las redes "Host local" e "Interna", y tras ello pulsaremos sobre el botón "Siguiente".



La siguiente ventana nos permite especificar los usuarios a los cuales será aplicada esta regla, si bien en nuestro caso daremos por válida la opción "Todos los usuarios", ofertada por defecto por el asistente, y pulsaremos directamente en ella sobre el botón "Siguiente".

Completaremos el proceso de creación de nueva regla pulsando sobre el botón "Finalizar" en la siguiente ventana.



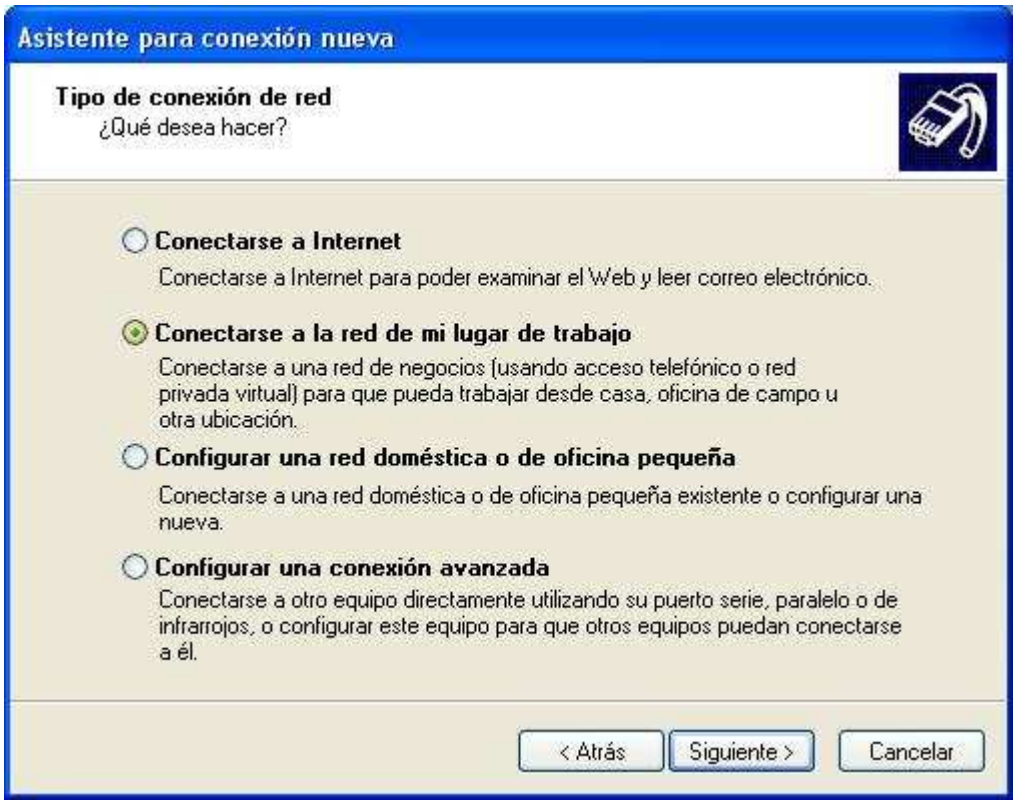
Finalmente hemos de recordar pulsar sobre el botón "Aplicar" en la ventana de administración de "ISA Server 2004" para que la regla pase a ser aplicada de modo efectivo.

En este instante ya hemos configurado el servidor "ISA Server 2004" para que realice la función de servidor VPN, estando en disposición de poder probar el correcto funcionamiento del servidor VPN que hemos configurado anteriormente.

Si estamos trabajando con máquinas virtuales, podremos probar fácilmente el correcto funcionamiento del servidor VPN definiendo en el equipo anfitrión una conexión de cliente de VPN.

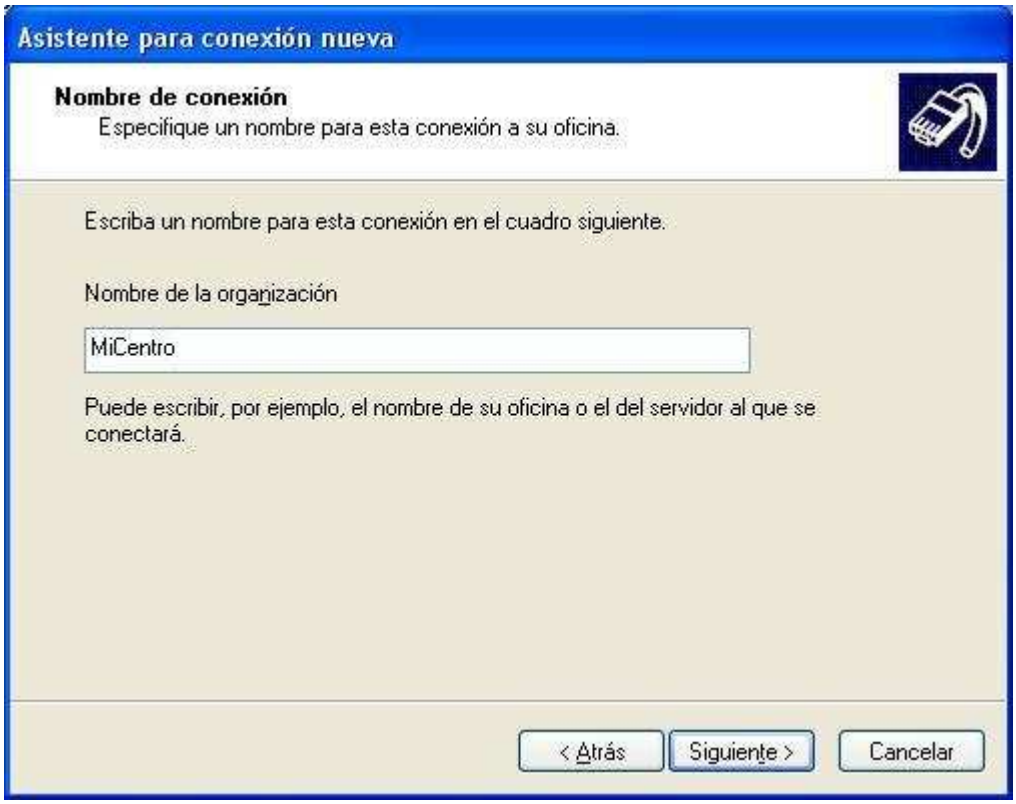
Por ejemplo si el equipo anfitrión tiene instalado el sistema operativo "Windows XP", desde el botón de "Inicio" ejecutaremos "Todos los programas -> Accesorios -> Comunicaciones -> Asistente para conexión nueva", pasando a ser mostrada como resultado de dicha acción la siguiente ventana de inicio del asistente, en la cual pulsaremos directamente sobre el botón "Siguiente":

En la nueva ventana mostrada indicaremos el tipo de conexión que deseamos realizar, en nuestro caso como deseamos conectarnos a la red de nuestro centro, seleccionamos el radio botón "Conectarse a la red de mi lugar de trabajo", y a continuación pulsaremos sobre el botón "Siguiente".

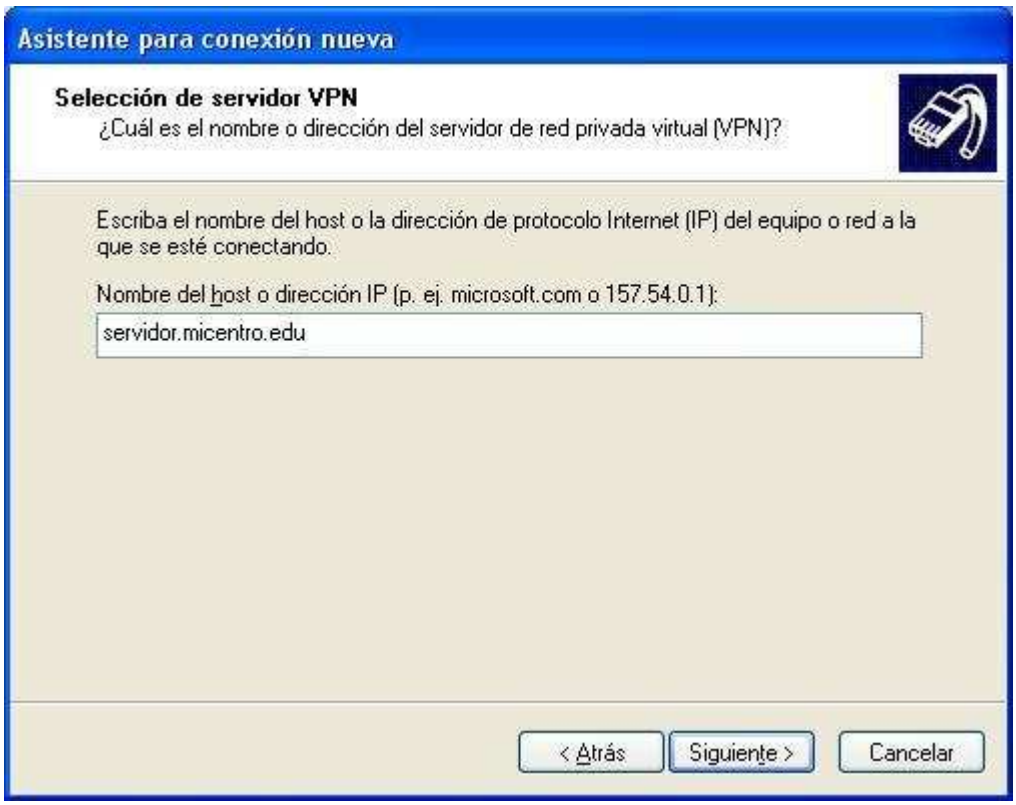


En la siguiente ventana indicaremos con que dispositivo vamos a realizar la conexión, si mediante un modem y línea RTB o RDSI o bien mediante la propia conexión a Internet del equipo; en nuestro caso seleccionaremos el radio botón "Conexión de red privada virtual", y tras ello pulsaremos sobre el botón "Siguiente".

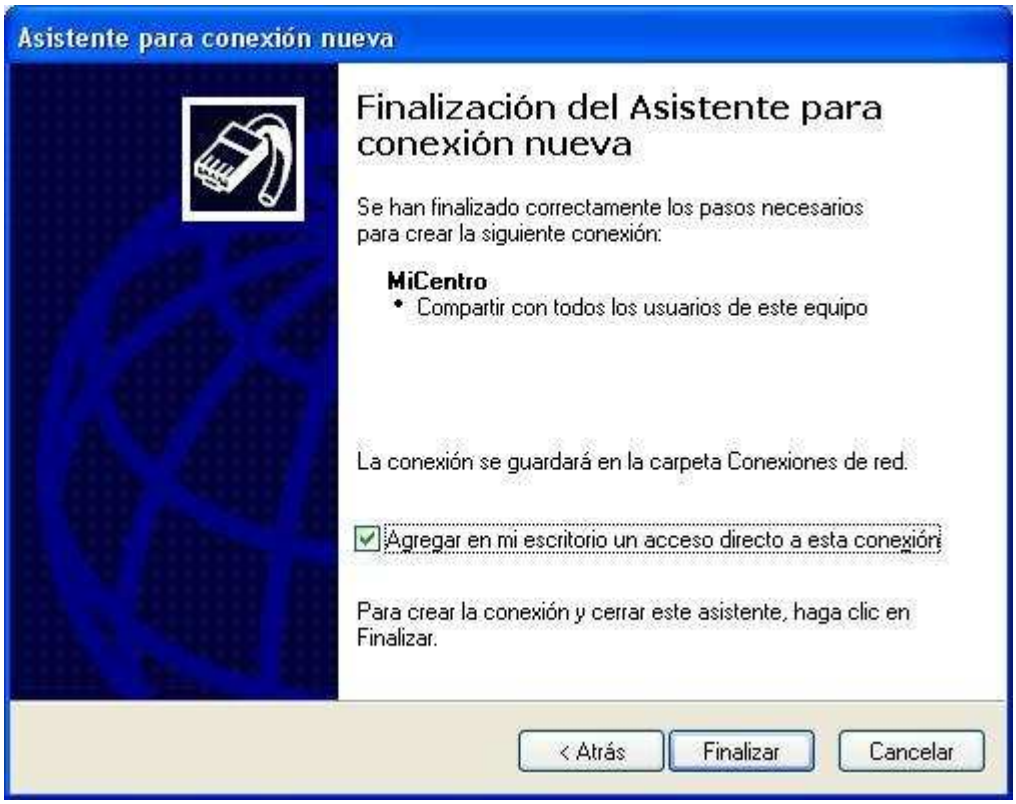
A continuación especificaremos el nombre que deseamos darle a la nueva conexión que estamos creando; en nuestro caso elegiremos como nombre para la conexión "MiCentro", y tras ello pulsaremos sobre el botón "Siguiente".



En la siguiente ventana especificamos la dirección IP o el nombre de equipo al equipo al cual deseamos conectarnos mediante la conexión VPN, en nuestro caso teclearemos la cadena "servidor.micentro.edu" en la caja de texto correspondiente, y tras ello pulsaremos sobre el botón "Siguiente".



Para completar el asistente de nueva conexión activaremos en la última ventana del mismo la casilla "Agregar en mi escritorio un acceso directo a esta conexión", y posteriormente pulsaremos sobre el botón "Finalizar".



Una vez completado este proceso, si hacemos doble clic sobre el icono "MiCentro" de acceso directo a la VPN ubicado en el Escritorio del equipo anfitrión, se mostrará la siguiente ventana, en la cual introduciremos las credenciales de un usuario del dominio "MiCentro.edu" que disponga de acceso VPN al "SERVIDOR", en nuestro caso las credenciales del profesor "Javier", y tras ello pulsaremos sobre el botón "Conectar".

Al cabo de un instante observaremos que nuestro equipo anfitrión se ha conectado al servidor mediante VPN, pues se mostrará el correspondiente icono de conexión de red en la parte inferior derecha de la ventana de dicho equipo anfitrión; si además nos ubicamos con el ratón sobre dicho icono, se mostrarán los parámetros básicos de la conexión VPN establecida con el equipo "SERVIDOR".

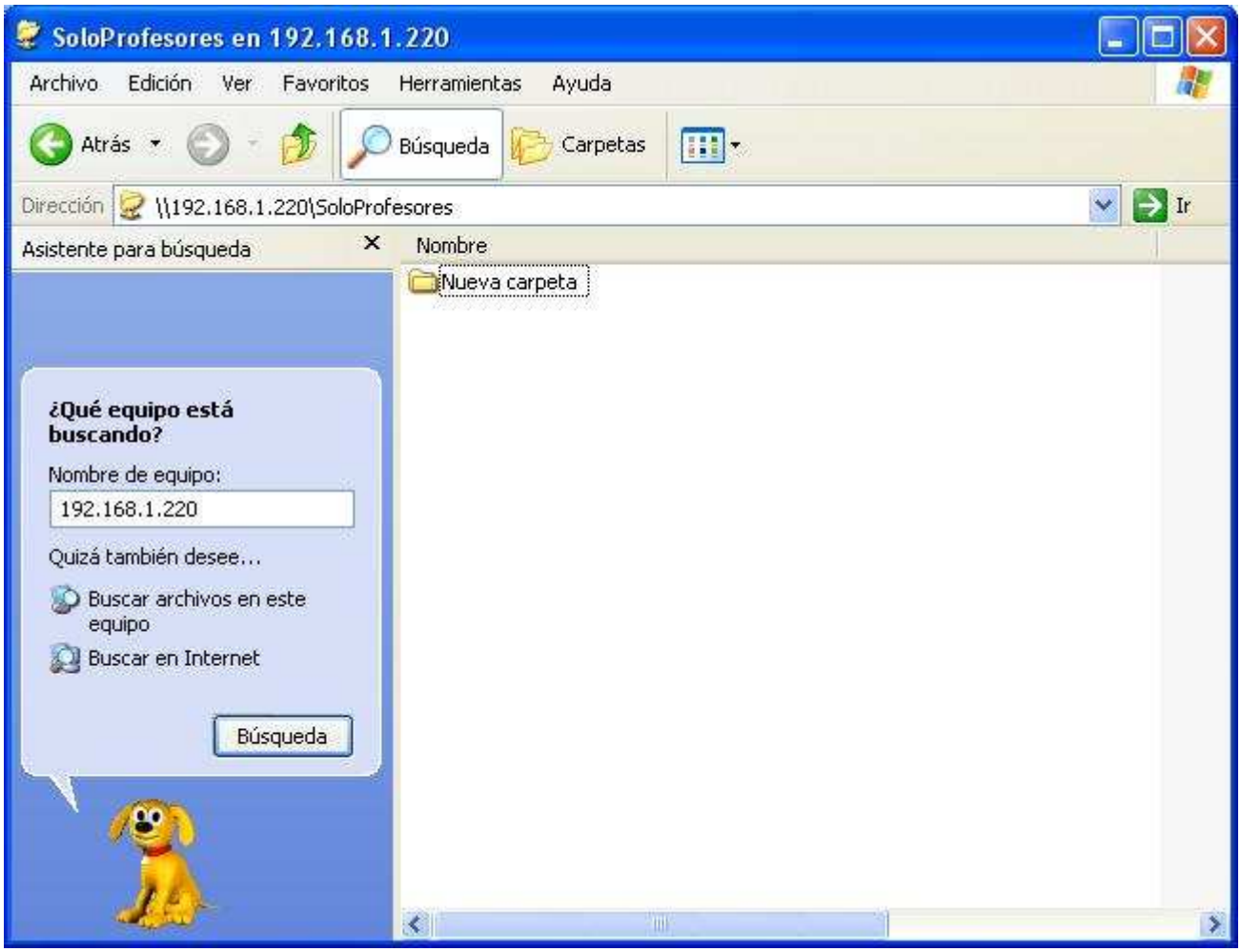
A partir de este instante el profesor "Javier" está conectado a la red de su centro, de forma que aunque esté ubicado físicamente sobre el equipo anfitrión, equipo externo al centro, dispone de las mismas posibilidades que si estuviera ubicado en un equipo cliente de la red de su centro.

Por ejemplo si el profesor "Javier" desea acceder a la carpeta compartida "SoloProfesores" del equipo "SERVIDOR", desde el equipo anfitrión lanzará "Mi PC", y en la ventana mostrada seleccionará la opción "Herramientas", y luego "Conectar a unidad de red" en el desplegable correspondiente, tras lo cual se le presentará la siguiente ventana en la que tecleará en la caja de texto correspondiente la ruta a dicho recurso compartido, es decir "\\192.168.1.220\SoloProfesores", de igual modo que haría si estuviera ubicado en un equipo cliente de la red de su centro.

NOTA: Debemos reparar en que la conexión se establece contra la dirección IP del interfaz de red "Conexión LAN" del equipo "SERVIDOR", es decir, se establece a la dirección IP "192.168.1.220" de dicho equipo, pues a todos los efectos desde la conexión VPN establecida, el equipo anfitrión estaría ubicado en la red interna del centro, como cualquier otro equipo cliente.

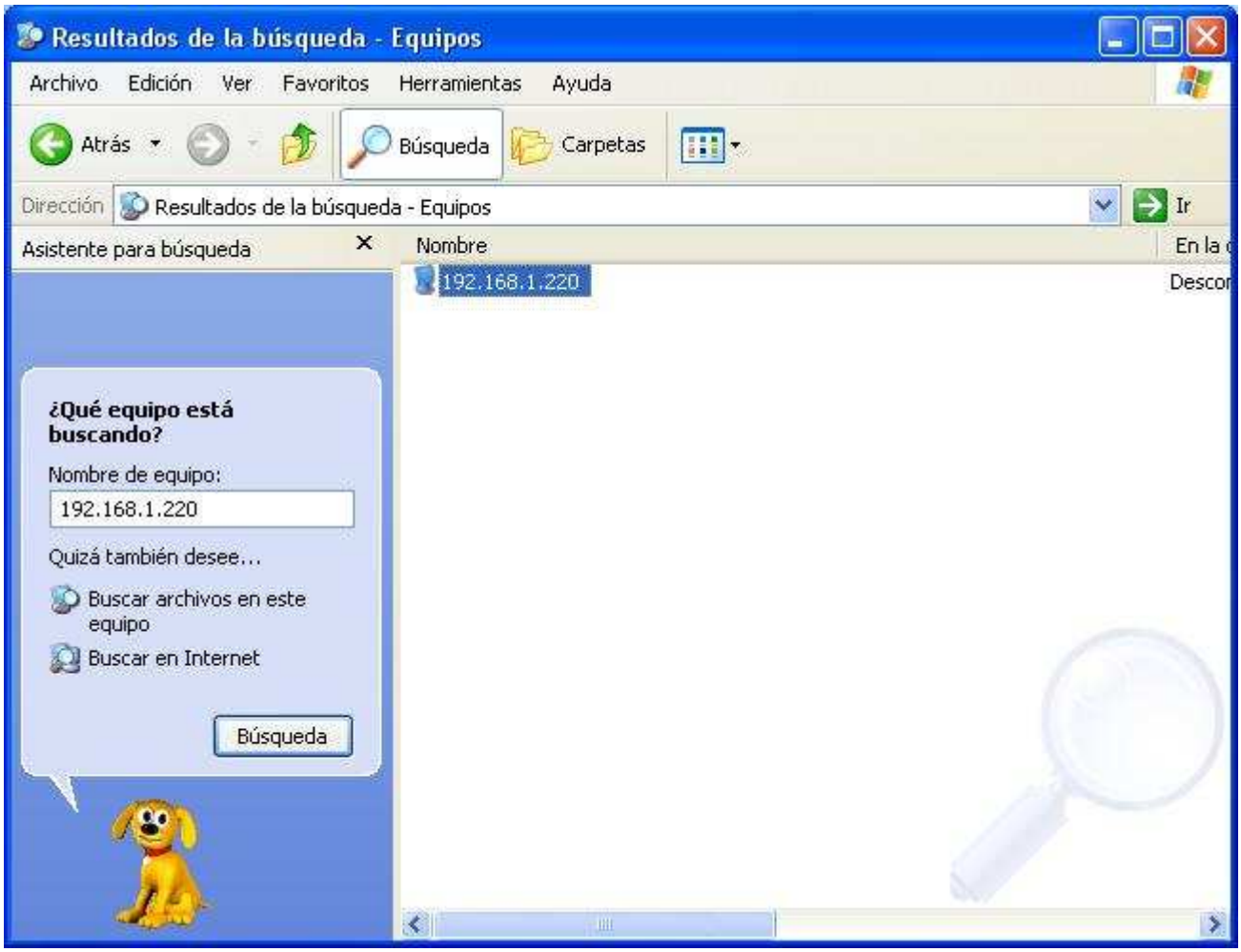
Tras pulsar sobre el botón "Finalizar" en la ventana de la imagen anterior, se nos presenta la siguiente ventana, en la que especificaremos los datos del usuario que desea acceder al recurso compartido en cuestión, en nuestro caso teclearemos las credenciales en el dominio "MiCentro.edu" del profesor "Javier".

Tras ello accederemos a la carpeta compartida "SoloProfesores" ubicada en el equipo "SERVIDOR", tal y como vemos en la imagen inferior, pudiendo hacer sobre ella lo mismo que si estuviésemos ubicados en un equipo cliente del dominio, por ejemplo crear un carpeta colgando de dicha carpeta compartida, tal y como vemos en la imagen inferior.



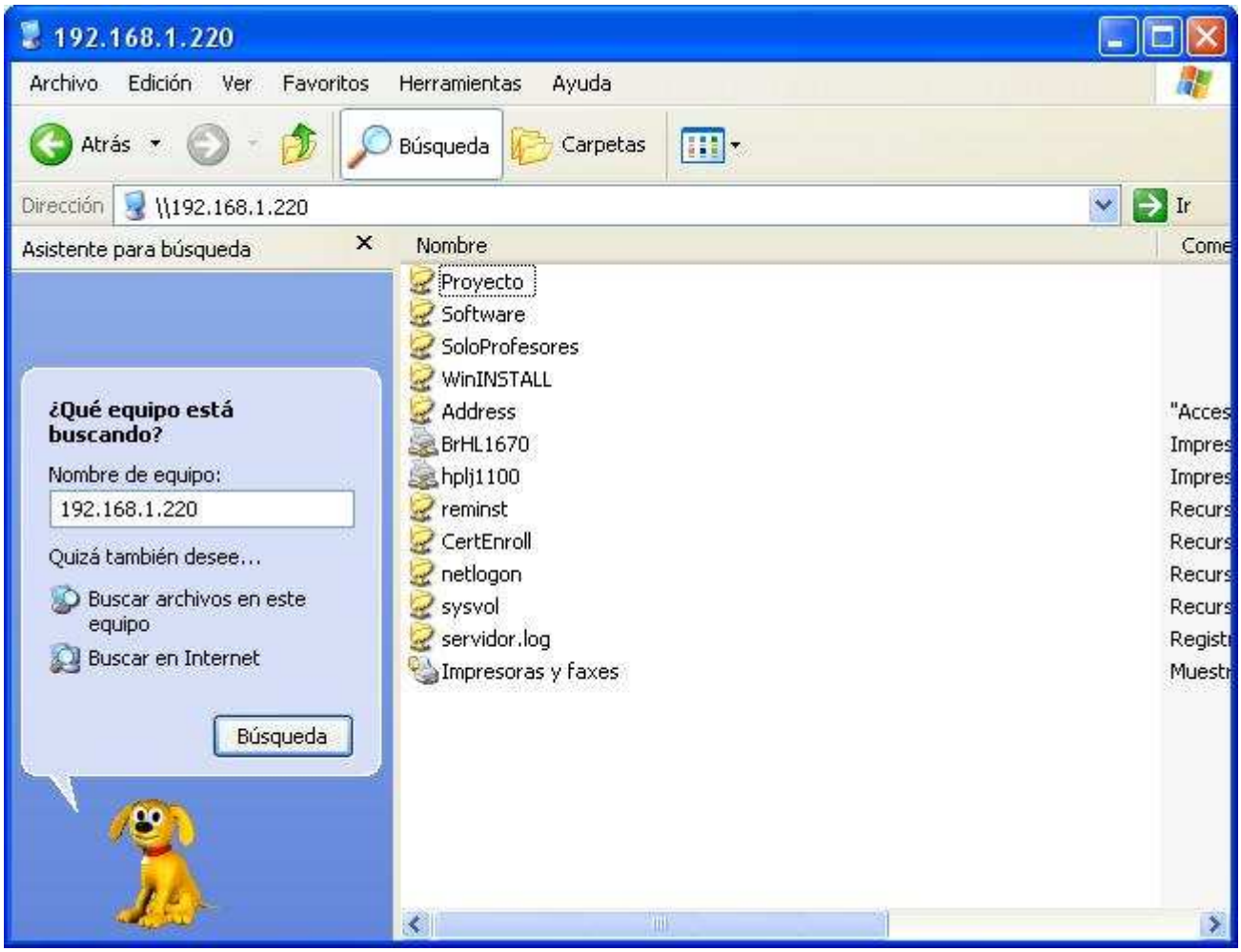
NOTA: Desde el equipo anfitrión desde el cual establecemos la conexión VPN, podremos realizar cualquier operación que pudiéramos realizar desde un equipo cliente que estuviera ubicado en la red de nuestro centro, como por ejemplo imprimir en una impresora de la red del centro, acceder a cualquier carpeta compartida, visualizar el contenido de un servidor web interno, etc.

Una vez establecida la conexión VPN desde el equipo anfitrión, si desconociéramos los recursos a los que podemos acceder, podríamos ejecutar la opción "Buscar" del "Menú Inicio" para seleccionar la opción "Equipos o personas", y posteriormente elegir "Un equipo en la red", pasando a ser mostrada las siguiente ventana en la que especificaríamos la dirección IP INTERNA del equipo a buscar (en este caso "192.168.1.220", la dirección IP interna del equipo "SERVIDOR"), para finalmente pulsar en dicha ventana sobre el botón "Búsqueda" para encontrar al equipo correspondiente.



NOTA: Podríamos haber buscado cualquier otro equipo de la red interna de nuestro centro, NO tenemos porque acceder exclusivamente a los recursos que nos ofrece el equipo "SERVIDOR".

Si en la ventana de la imagen superior hacemos doble clic sobre el equipo "192.168.1.220", el equipo "SERVIDOR", podremos visualizar todos aquellos recursos que ofrece el equipo al cual nos hemos conectado mediante el cliente de VPN.



Si deseamos cerrar la conexión VPN establecida, en el equipo anfitrión pulsaremos con el botón derecho del ratón sobre el icono correspondiente a la conexión VPN, para elegir la opción "Desconectar" en el desplegable correspondiente, tal y como vemos en la imagen inferior.

NOTA: Si habilitamos el servidor VPN en el equipo "SERVIDOR", tal y como hemos hecho en este apartado, deberemos replantearnos la creación de reglas de publicación de servidor, pues es posible que algunas de ellas NO sean necesarias, al poder habilitar el acceso externo a los recursos y servicios configurados en dichas reglas, a través de la conexión VPN.