Vicente J. Rico Cuba-k idatzia
Asteazkena, 2007(e)ko iraila(r)en 19-(e)an 13:11etan

There are no translations available.
Actualmente, la seguridad informática es uno de los temas que más preocupan a los usuarios de ordenadores...

CORTAFUEGOS GRATUITOS

Actualmente, la seguridad informática es uno de los temas que más preocupan a los usuarios de ordenadores. Cuando conectamos nuestro ordenador a Internet nos enfrentamos a la posibilidad de que otro internauta acceda a nuestros datos almacenados como vídeos, fotografías, archivos, etc. o lo que es peor a los datos de cuentas bancarias y contraseñas de acceso a correo y otros servicios; eso si no es uno de los que se divierten eliminando archivos o bien estropeando el ordenador.

En ocasiones incluso nos instalan rutinas para tener acceso a los programas de nuestra máquina, ejecutando de forma invisible cualquier aplicación que desee o incluso controlando o configurando opciones de nuestro sistema operativo.

Una de las primeras decisiones que un usuario debe tomar es la de adoptar medidas según el grado de protección que necesite. No es lo mismo un puesto independiente, que un ordenador conectado en red con otros dentro de una oficina en donde existen múltiples empleados, o que un equipo personal conectado a Internet. Generalmente el nivel de seguridad debe incrementarse con el aumento de la complejidad del sistema.

Por defecto nuestro sistema operativo, y en concreto Windows, ofrece una serie de servicios a los demás usuarios de la red. Estos servicios son ofrecidos por algún programa en ejecución mediante puertos de comunicación, por lo que cualquier internauta puede acceder a ellos sabiendo la dirección IP de nuestro ordenador y el número del puerto. A esto deberíamos añadir los errores (bugs) de seguridad que detectan en el sistema operativo y deben ser actualizados mediante parches (service packs).

Pero, ¿cómo puede saber alguien nuestra dirección IP?. La verdad es que no la conocen sino que realizan barridos o escaneos entre diferentes rangos hasta encuentran algún ordenador que ofrece un servicio y no está protegido.

Los puertos están clasificados en puertos IANA, puertos registrados y puertos dinámicos. Los puertos IANA (estandarizados por la organización Internet Assigned Numbers Authority) son los

1024 primeros y fueron asignados para estandarizar la comunicación entre ordenadores. Los puertos registrados están comprendidos entre el 1024 y el 49151 y tienen programas asignados, aunque no están estandarizados. El resto son puertos dinámicos y se encuentran entre el 49152 y el 65535 sin ningún programa concreto definido.

Para conocer los puertos abiertos de nuestro ordenador, es decir, los servicios que ofrecemos, podemos abrir una consola de intérprete de comandos de Windows y teclear el comando "netstat -a". Podremos comprobar que existen múltiples puertos en estado "LISTENING", es decir, escuchando o esperando una conexión.

Un cortafuegos o firewall es un programa que controla todos los programas y servicios que se están ejecutando en nuestro ordenador vigilando toda comunicación entrante o saliente que se produzca. En ocasiones incluso controlan opciones de los propios programas, principalmente de navegadores, como ventanas emergentes, envío de contraseñas, banners de publicidad, cookies, etc. El usuario puede realizar un control desde este tipo de aplicaciones permitiendo o denegando accesos o simplemente monitorizándolos.

Al monitorizar la comunicación creada entre nuestro ordenador y el resto de máquinas de Internet, comprobaremos que existe una gran cantidad de paquetes transmitiéndose creando un tráfico continuo. Estos paquetes con información y comandos tienen un origen identificado por un programa que se ejecuta en una máquina conocida por su dirección IP que utiliza un puerto de comunicación por el que envía y recibe los datos, y un destino identificado por una dirección IP con un puerto. Los paquetes contienen toda la información necesaria de emisor y receptor por lo que el cortafuegos, al controlarlos, puede discriminar la comunicación que estime peligrosa.

La manera de actuar de un cortafuegos es filtrando el tráfico generado entre nuestro ordenador y el resto, pero eso sí, ya sea los de la propia red local o bien los de Internet. Para poder realizar el filtrado necesita una serie de criterios y reglas establecidas en su configuración. Esto significa que un cortafuegos realizará correctamente su función si dispone de reglas bien descritas que le permitan aceptar la información deseada y no peligrosa.

Aunque los programas más utilizados para acceder a Internet son los navegadores y los clientes de correo electrónico, en general, casi todos las aplicaciones hoy en día realizan comprobaciones con servidores en Internet para registrarse o realizar actualizaciones, pero además otras muchas se ejecutan de manera transparente ofreciendo servicios de páginas

web (http), de transferencia de archivos (ftp), o bien recursos compartidos como carpetas o impresoras a través del protocolo Netbios u otras funciones específicas.

Al conectarnos a Internet se genera tráfico desde y hacia los puertos que tenemos abiertos, por lo que en principio somos candidatos para recibir un ataque, pudiendo un intruso penetrar en nuestro ordenador. Los cortafuegos que podemos instalar reciben el calificativo de personales. La función de un cortafuegos personal consistirá en protegernos de los ataques procedentes del exterior (desde Internet) o desde nuestra red local.

En ocasiones debemos llevar cuidado incluso de programas que al activarlos intentan acceder a Internet sin un propósito conocido por nuestra parte, pues podrían ser programas de tipo troyano o spyware que conecten con un intruso. Suelen disfrazarse de aplicaciones inocuas pero al aceptarlos posibilitamos que un extraño pueda realizar funciones de control a distancia de nuestro ordenador. Los spyware, que vienen incluidos a veces en ciertos programas freeware, registran la información que se transmite al navegar pudiendo extraer los datos de cuentas bancarias u otra información relevante. Los cortafuegos nos pueden avisar cuando un programa de este tipo intenta realizar registros de la información evitándonos violaciones de nuestra intimidad.

Lo que es seguro es que cuanto más tiempo pasemos conectados a Internet mayor será el número de ataques que sufriremos y por lo tanto, mayor el riesgo de intrusión.

Los cortafuegos disponen de múltiples opciones que nos permiten configurar las funciones que van a realizar. La mayoría de cortafuegos personales permiten configurar algunas de las siguientes opciones:

Opciones básicas:

- **Posibilidad de detectar los ataques de ordenadores remotos desde Internet.** Debe detectar los escaneos de puertos abiertos para evitar accesos indebidos.

- **Asistentes para crear reglas de comportamiento de las aplicaciones y del sistema**. La posibilidad de detectar y aplicar reglas para las aplicaciones y el sistema permite a los

usuarios sin conocimientos en redes que puedan empezar a usar
el cortafuegos
configurándolo según se produzcan alertas partiendo de una instalación básica inicial.

- **Niveles de acceso predefinidos para las aplicaciones y el sistema**. Si un cortafuegos tiene esta opción, significa que cuando detecta una comunicación, revisará la base de datos de preconfiguración y sugerirá un juego de reglas creadas por los diseñadores que son óptimas para esta aplicación, o bien mostrarán un nivel de peligrosidad. Esta técnica permite crear las reglas de forma cómoda sin ningún conocimiento especial de puertos o protocolos.

- **Los mensajes de las alarmas.** Los mensajes automáticos que nos advierten sobre los ataques que sufre el ordenador o cualquier otra actividad peligrosa.

- **Bloquear el tráfico de Internet.** Esta opción nos da la posibilidad de permitir o denegar con un clic todo el tráfico de Internet ignorando todas las reglas
del cortafuegos
.

- **Bloquear direcciones web.** Nos puede interesar bloquear algunos sitios web debido a su contenido, basado en datos tales como el nombre del sitio web, el nombre del dominio o palabras claves en las páginas web. Esto es muy útil para impedir la navegación en ciertas páginas a empleados en un trabajo o a niños.

- **Mostrar las conexiones activas y los puertos abiertos**. Esta opción nos informa del estado de la red mostrando las conexiones activas entre programas y los puertos abiertos que están esperando una conexión.

- **Mostrar un historial de conexiones**. Normalmente se dispone de una utilidad especial que muestra un historial de las conexiones y eventos producidos y registrados. El usuario puede seleccionar la información mediante filtros para consultar cualquier conexión o evento que se haya producido. Por ejemplo, las conexiones realizadas por el cliente de correo electrónico entre unas fechas determinadas.

Opciones para usuarios avanzados:

- **Filtrado de paquetes de la aplicación**. Permite al cortafuegos supervisar el comportamiento de las aplicaciones. Esta clase de filtrado debe permitir especificar las actividades individuales de una aplicación. Por ejemplo, "Permitir a OutLook Express la comunicación de salida usando el protocolo TCP al puerto remoto 25 y 110 del host servidor.correo.com y prohibir cualquier otra comunicación de la aplicación .

- **Control de protocolo ICMP (Stealth de hackers).** Normalmente, cuando recibimos una petición de conexión de otro ordenador a un puerto cerrado, enviamos una respuesta de vuelta. El modo Stealth permite que el ordenador no responda, pareciendo que no estemos conectados a Internet.

- **Renombrar ficheros adjuntos de correos electrónicos (gusanos).** Posibilidad para neutralizar (renombrar) los ficheros adjuntos peligrosos en un correo electrónico entrante.

- **Bloquear el historial del navegador Web (referrer)**. Cuando navegamos por Internet el historial puede revelar la información sobre sitios previamente visitados. Los operadores de un sitio Web pueden utilizar esta información privada para propósitos de comercialización. Esta información se llama "referrer" y algunos cortafuegos pueden bloquearla.

- **Bloquear ventanas emergentes** / **banners.** Posibilidad de bloquear las ventanas emergentes y banners publicitarios que incomodan mientras se está navegando por Internet.

- **Bloquear archivos ejecutables al navegar y en el correo electrónico.** Esta opción nos permite bloquear archivos ejecutables potencialmente peligrosos (ActiveX, EXE s, etc) de páginas web y de mensajes del correo electrónico.

- **Bloquear las cookies al navegar y en el correo electrónico**. La posibilidad de permitir o bloquear las cookies es importante, ya que son un pedazo pequeño de información transferido por el servidor a un navegador y almacenado en el ordenador del usuario. El navegador guarda esta información y a veces la transfiere al servidor.

- **Bloquear scripts activos al navegar y en el correo electrónico.** Esta opción da la posibilidad de bloquear los scripts potencialmente peligrosos (de Java, de Visual Basic, etc.) de páginas web y de mensajes del correo electrónico.

- **Grupo de direcciones de confianza (Trust address group/zone).** Mediante una ventana de configuración podremos seleccionar un rango de red o redes a los que permitir toda actividad sin crear reglas especiales para ellos. Esto es muy útil para utilizar el cortafuegos exclusivamente para la comunicación con Internet y permitir que todos los servicios ofrecidos por el ordenador sean accesibles desde cualquier puesto de la red local.

- **Opciones de seguridad para protección de contraseñas.** Esta opción nos permitirá proteger las contraseñas proporcionadas en los programas.

Algunas características adicionales de los cortafuegos personales:

- **Posibilidad de actualización automática.** Esta utilidad permite actualizar el cortafuegos sin interacción del usuario para una protección óptima contra los nuevos y diferentes ataques. Otros cortafuegos disponen de un botón para comprobar si existen actualizaciones y en caso afirmativo descargarlas e instalarlas.

- **Posibilidad de cambiar entre configuraciones diferentes.** Los Cortafuegos que disponen de esta opción puede crear configuraciones diferentes para casa, trabajo, etc. incluso con el mismo perfil de Windows.

- **Traza visual de un ataque.** Mediante esta opción podremos rastrear el ordenador origen que nos ataca una vez detectado un intento de acceso no permitido.

- **Ejecutarse como un servicio.** Posibilidad de configurarse para funcionar completamente oculto al usuario.

- **Acelerar el tiempo de respuesta.** Almacena todos los nombres de DNS resueltos en una base de datos especial (caché) para reducir significativamente los tiempos de respuesta.

- **Administración y registro remoto.** Sirve para poder configurar el cortafuegos de forma remota, pudiendo consultar el registro de eventos.

Windows XP dispone de un cortafuegos personal muy simple. Para configurarlo debemos acceder a Mis sitios de red , luego la opción de Ver conexiones de red y en las propiedades de la conexión que deseemos proteger (accesible con el botón derecho del ratón) pulsaremos en la pestaña de opciones avanzadas. Aquí podremos activar o desactivar el Firewall diseñado por Microsoft que por defecto bloquea todo menos las excepciones introducidas en la pestaña correspondiente. Las opciones que ofrece son:

- Permiso de comunicación a un programa.
- Permiso de acceso a nuestro ordenador a un puerto a todos los ordenadores o sólo a los de mi red local.
- Mostrar un mensaje cuando se bloquee a un programa.
- Registro de paquetes perdidos y conexiones correctas.
- Control del protocolo de mensajes ICMP.



ZONE ALARM

ZoneAlarm es un cortafuegos personal orientado especialmente al usuario doméstico sin demasiados conocimientos de seguridad ni de redes. Su interfaz de configuración es extremadamente sencillo y no requiere demasiada experiencia para su correcta configuración.

Podemos descargarlo desde la página oficial del programa http://www.zonelabs.com . Existe

una versión en castellano, la 4.5.594 y otra versión más actual, de momento sólo en inglés, la 5.5.062.

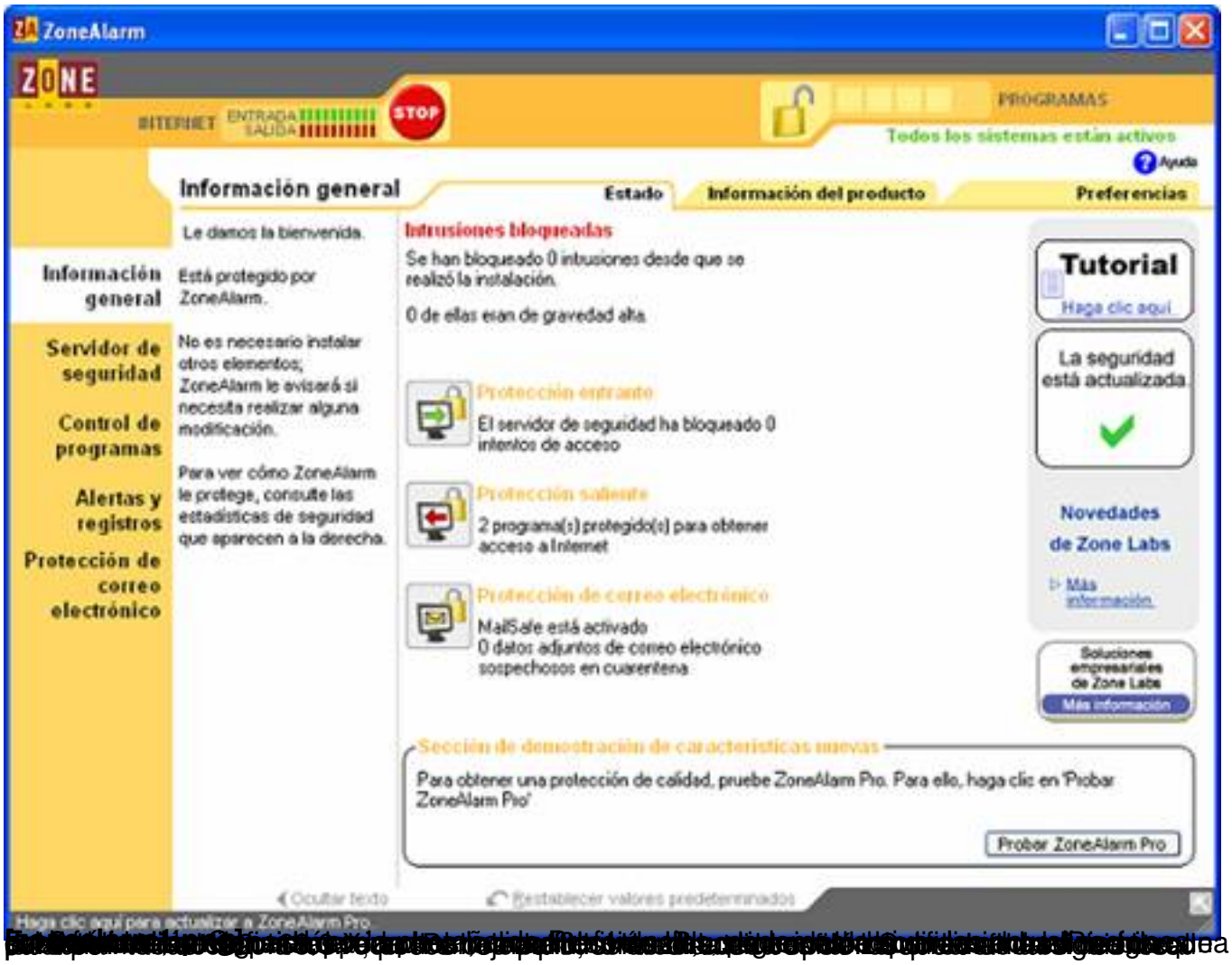
En la instalación debemos indicar el tipo de conexión (módem, cable, ADSL,), el nivel de conocimientos en seguridad (principiante, usuario avanzado,) , número de ordenadores conectados y tipo de ordenador (PC, red, portátil,), aunque no afecta al resultado de la instalación.

Una vez iniciado seleccionaremos ZoneAlarm, pues existe otra versión más completa no gratuita que es ZoneAlarm PRO. Aparecerá a continuación un asistente para configurar las siguientes opciones:

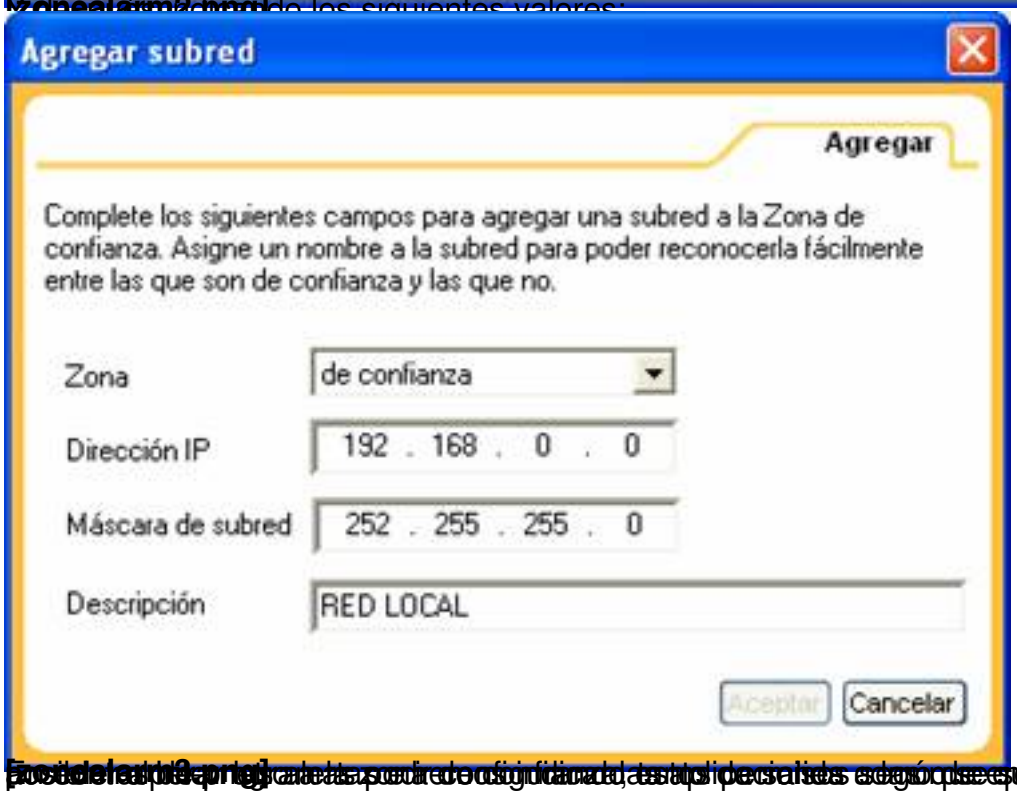
- Funcionamiento en modo servicio o mostrando alertas.
- Posibilidad de aplicar reglas preconfiguradas para ciertos programas conocidos como el navegador, el cliente de correo electrónico o los servicios básicos.
- Posibilidad de cifrar las contraseñas.

A partir de este momento el cortafuegos mostrará un interfaz para completar la configuración:

Vicente J. Rico Cuba-k idatzia
Asteazkena, 2007(e)ko iraila(r)en 19-(e)an 13:11etan




ZoneAlarm
ZONE LABS
INTERNET
ENTRADA
SALIDA
STOP
PROGRAMAS
Todos los sistemas están activos
Ayuda
Servidor de seguridad
Principal
Zonas
Información general
Servidor de seguridad
Control de programas
Alertas y registros
Protección de correo electrónico
Utilice esta ficha para agregar equipos y redes a la Zona de confianza.
Ejemplo: ponga el equipo o la red que desea compartir en la Zona de confianza.
Todos los orígenes de tráfico no mencionados aquí se incluyen, de forma predeterminada, en la Zona de Internet.
Nombre
Dirección IP/Sitio
Tipo de ent...
Zona
Intel(R) PRO/100...
0.0.0.0/0.0.0.0
Subred d...
Internet
Detalles de la entrada
Nombre Intel(R) PRO/100 VE Network Co...
Zona Internet
Tipo de entr... Subred de adaptador
Dirección IP... 0.0.0.0/0.0.0.0
Agregar >>
Editar
Host/Sitio
Dirección IP
Intervalo IP
Subred
Ocultar texto
Haga clic aquí para actualizar a ZoneAlarm Pro.


Agregar subred
Agregar
Complete los siguientes campos para agregar una subred a la Zona de confianza. Asigne un nombre a la subred para poder reconocerla fácilmente entre las que son de confianza y las que no.
Zona
de confianza
Dirección IP
192 . 168 . 0 . 0
Máscara de subred
252 . 255 . 255 . 0
Descripción
RED LOCAL
Aceptar
Cancelar



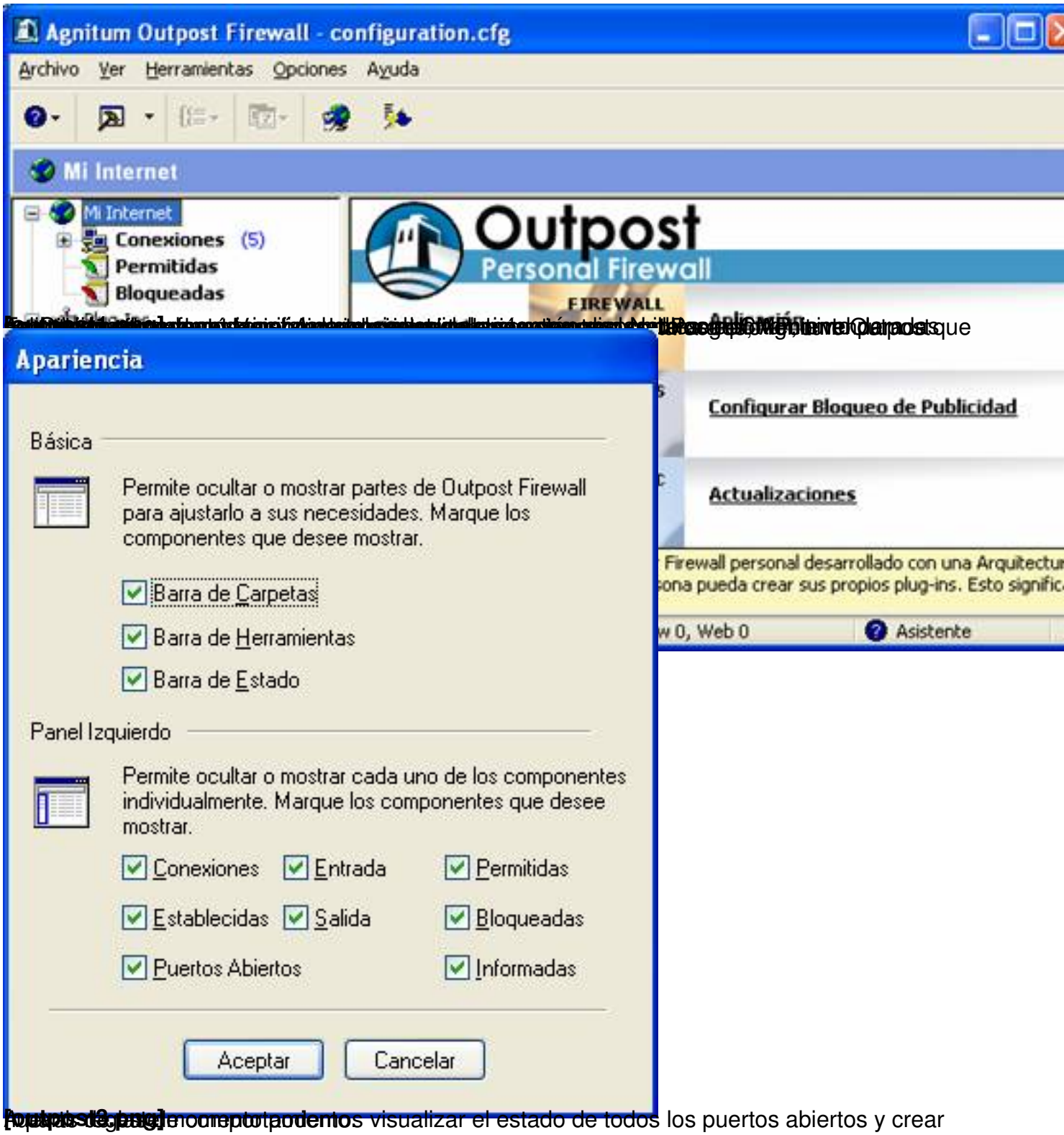


AGNITUM OUTPOST

Es un cortafuegos personal muy completo, orientado a un público más profesional. Funciona igualmente bloqueando puertos de entrada y salida, así como programas, incorporando además una serie de plug-ins para realizar funciones de bloquear publicidad, contenido de páginas web, caché DNS, contenido activo (controles ActiveX, JavaScript, applets de Java, cookies, etc.), control de archivos adjuntos en el correo electrónico y detección ataques.

Podemos descargarlo desde la página oficial del programa http://www.agnitum.com . La versión 1.0 dispone de una instalación en inglés que solicita el lenguaje de funcionamiento del programa, donde seleccionaremos spanish para utilizarla en español.

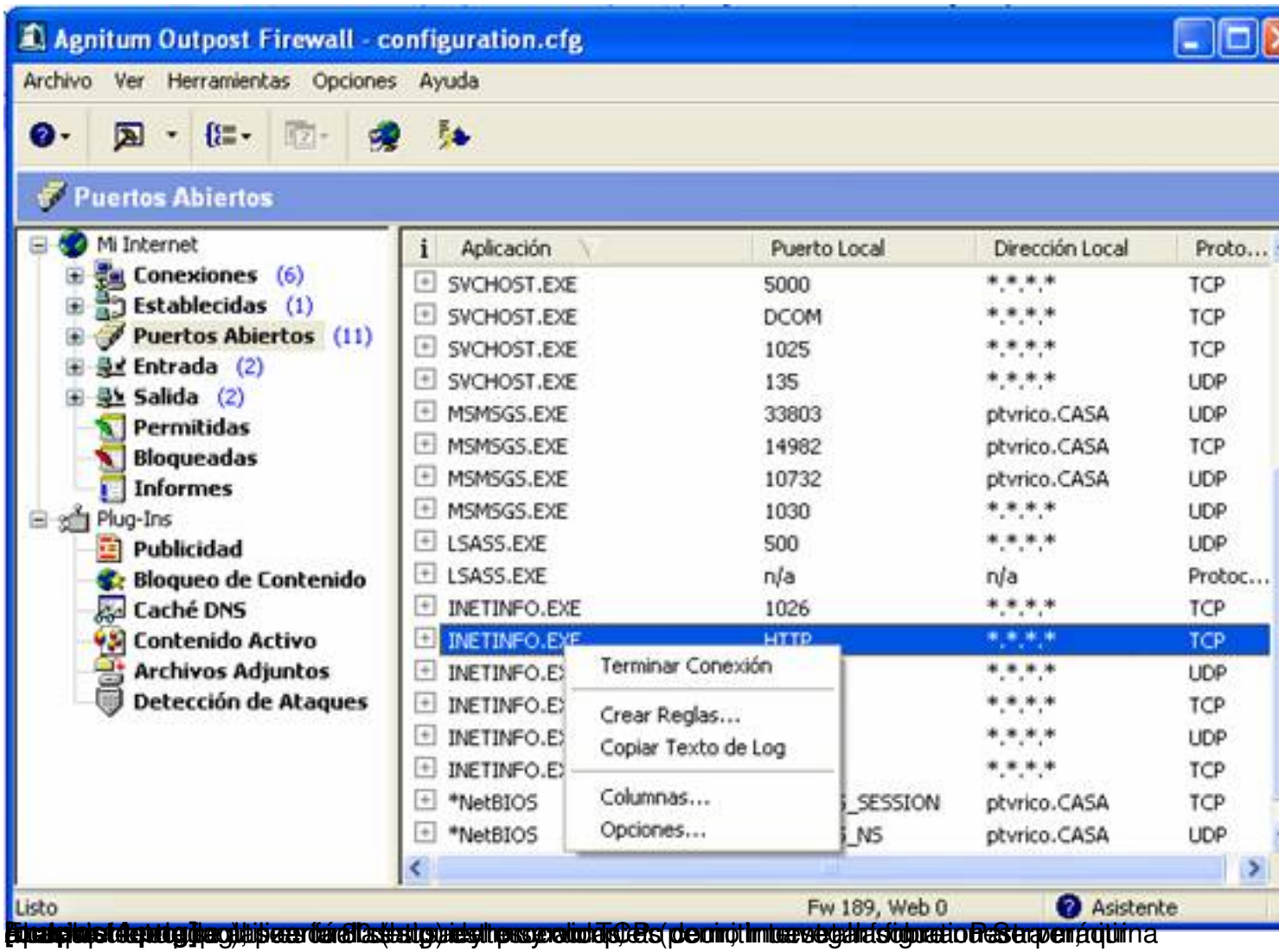
Dispone de una interfaz muy actual y amigable como muestra la imagen siguiente:



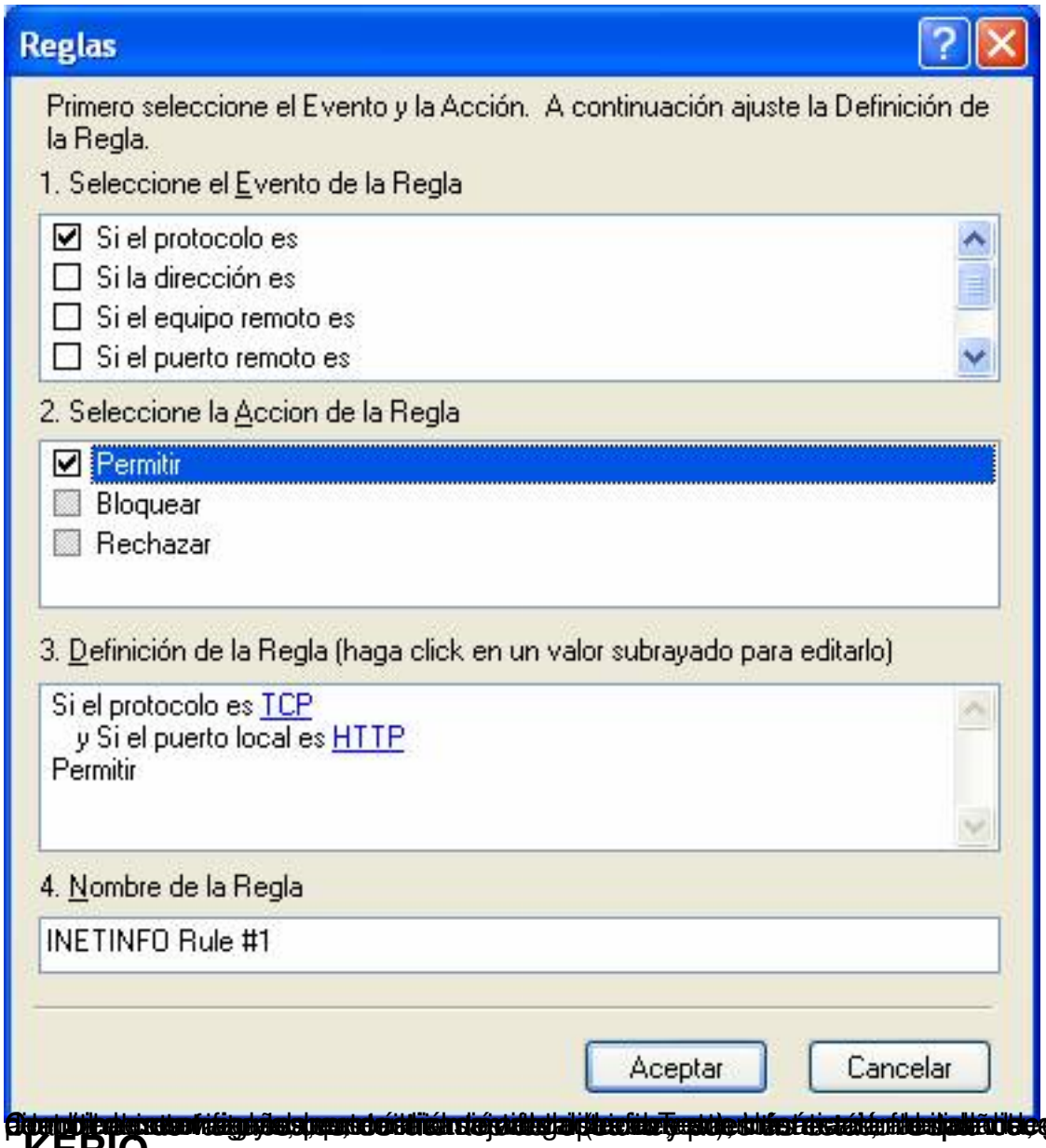
que

visualizar el estado de todos los puertos abiertos y crear

Vicente J. Rico Cuba-k idatzia
Asteazkena, 2007(e)ko iraila(r)en 19-(e)an 13:11etan



[illegible]



KERIO

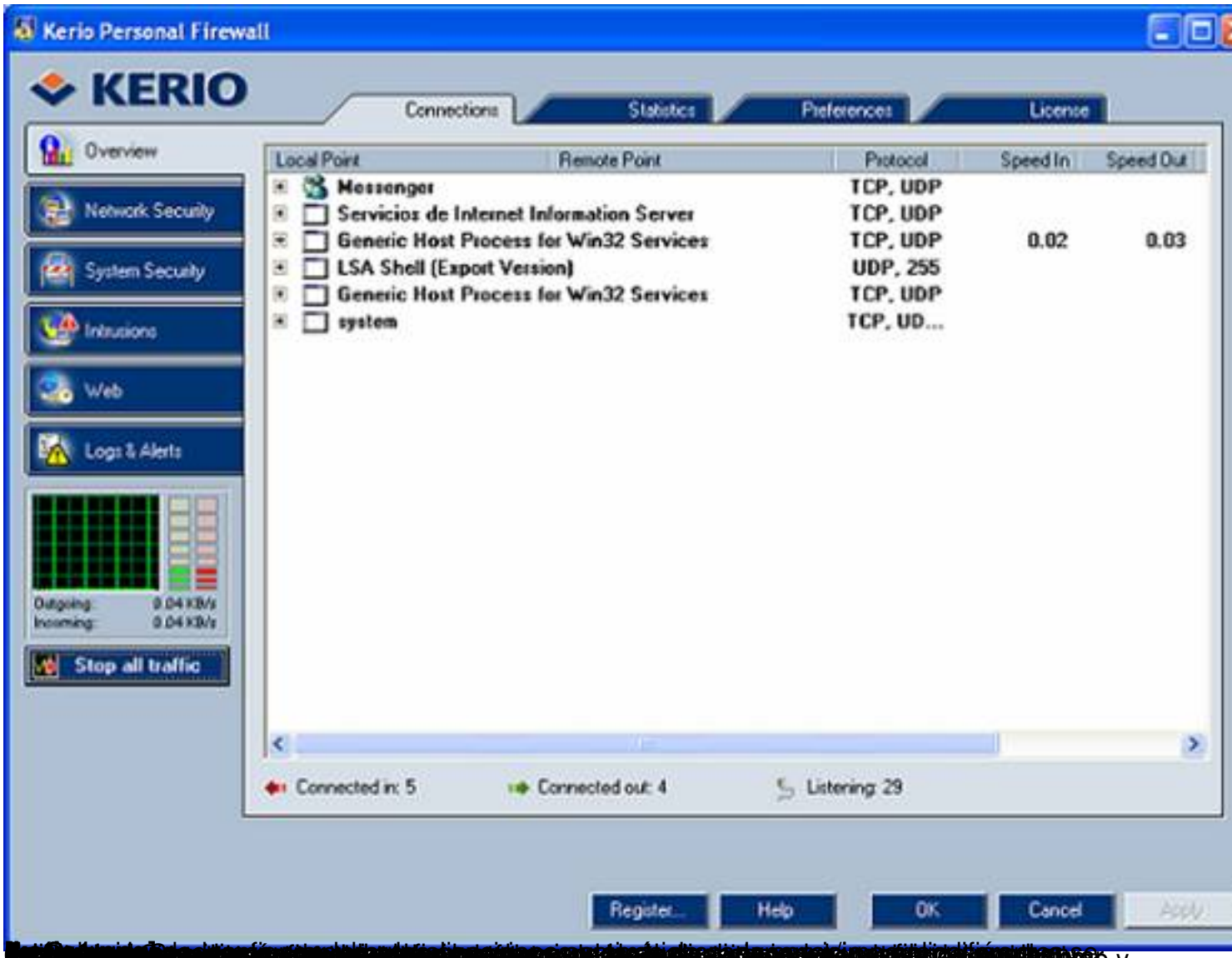
Kerio Personal Firewall es un cortafuegos gratuito sólo para uso personal, es decir, que para ser usado en empresas es necesario adquirir una licencia de pago. Después de la instalación funcionará como la versión completa durante 30 días, y después como versión libre donde no se da soporte para capacidades de filtro de contenidos (scripts, cookies, archivos adjuntos, etc.), bloqueo de ventanas emergentes, y otras características.

Podemos descargarlo desde la página oficial http://www.kerio.com/kpf_download.html aunque no está disponible en español.

En su instalación se puede elegir entre modo simple o modo avanzado, necesitando en este último de conocimientos de redes.

Kerio Personal Firewall versión 4 dispone de reglas que pueden configurarse manualmente o descargarse preconfiguradas. Una característica interesante es su capacidad de monitorizar la integridad de aplicaciones y archivos, lo que permite detectar infecciones de virus. También incorpora capacidades de detección de intrusos o ataques.

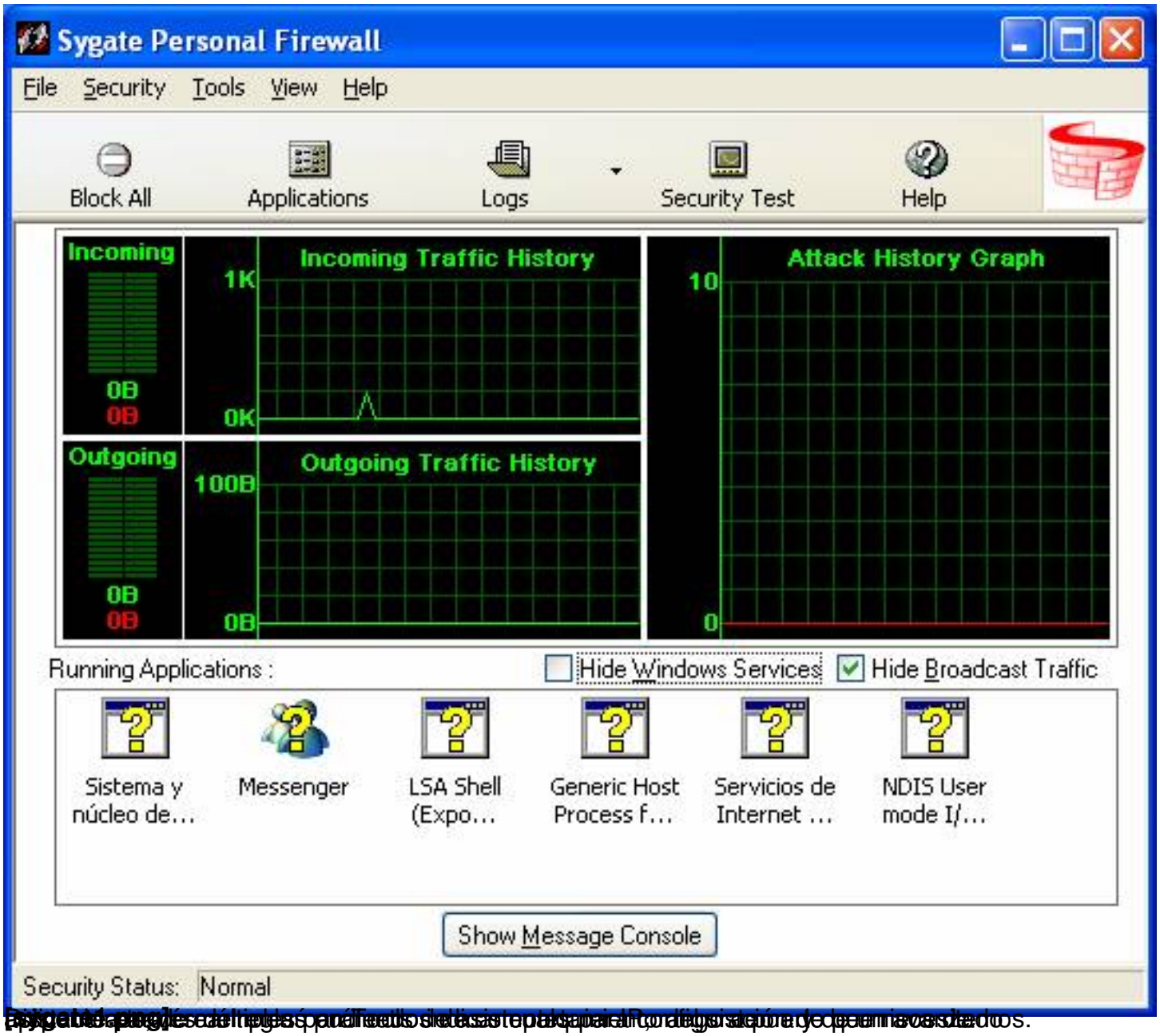
En el primer reinicio con Kerio instalado nos detectará la tarjeta de red (interfaz de conexión) por la que accedemos a Internet y se preconfigurará. Al entrar al programa nos mostrará la pantalla siguiente:

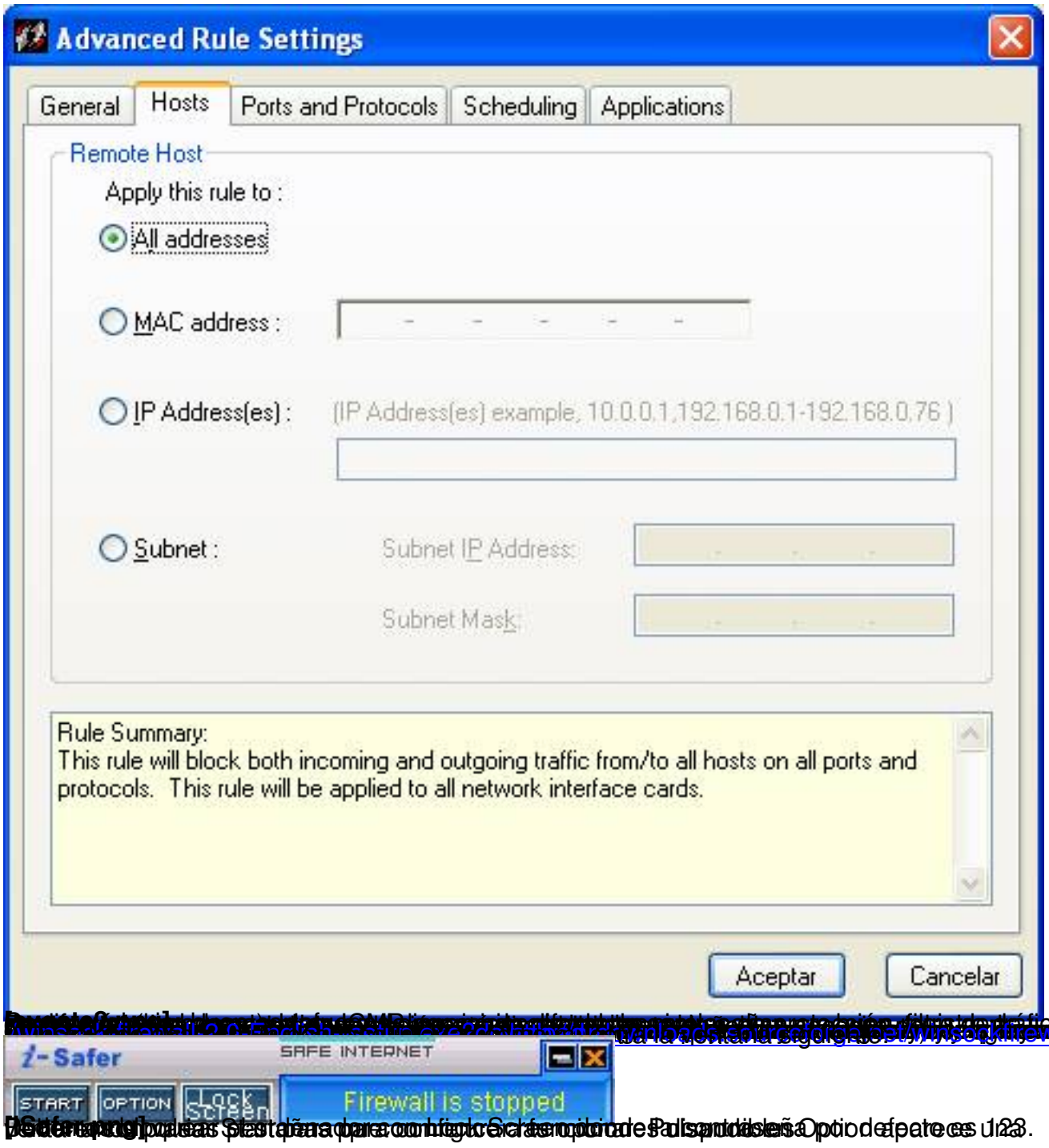


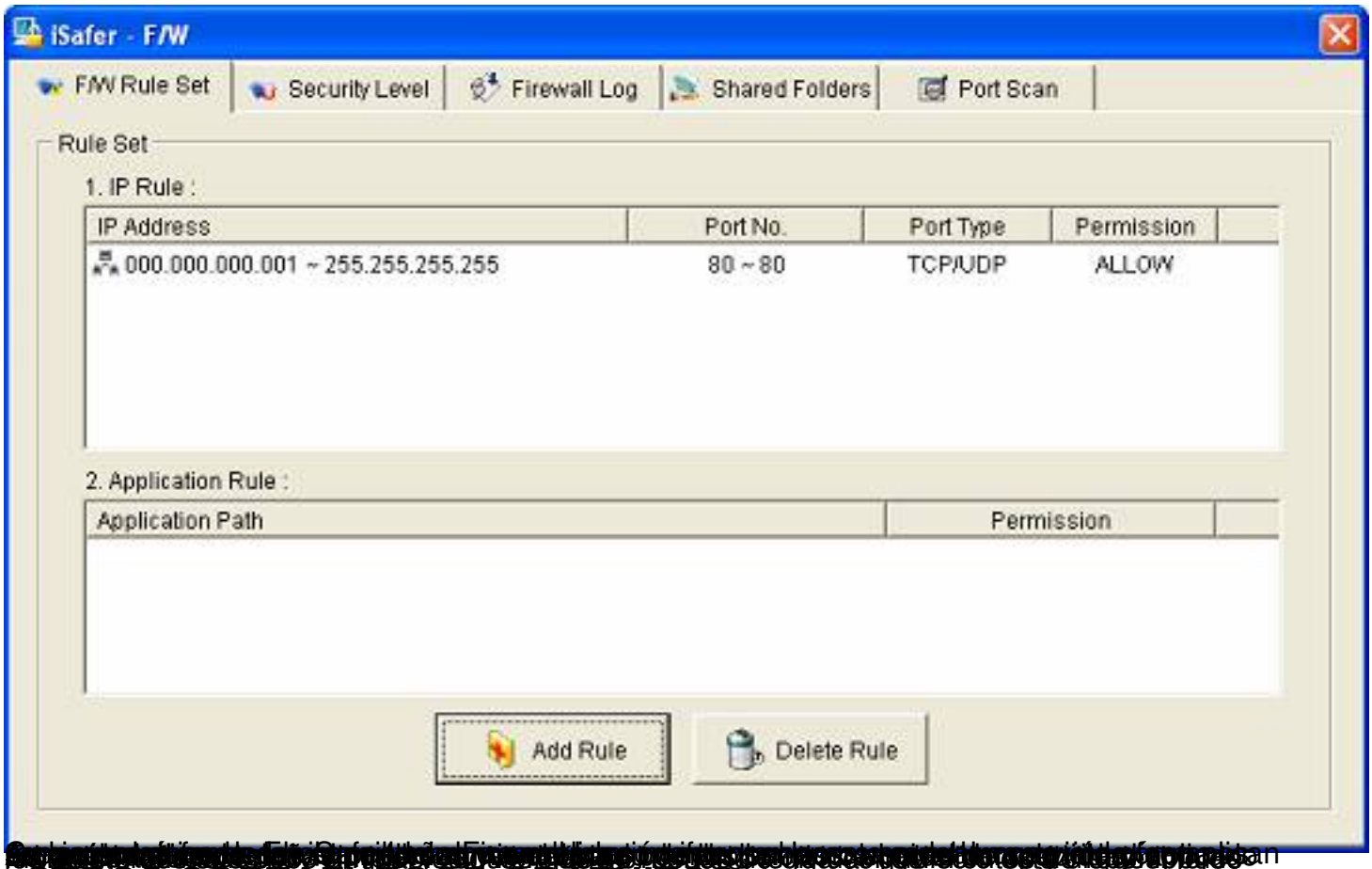
SYGATE

Sygate Personal Firewall es gratuito sólo para uso personal y su versión 5 ofrece un interfaz amigable protegiendo el ordenador frente a hackers y programas de tipo troyano, además de incluir características de niveles de protección, registro de eventos, control de privacidad, etc.

Como se puede observar en la siguiente imagen, el interfaz de entrada es muy atractivo y muestra estadísticas de tráfico de red y ataques en tiempo real.


Sygate Personal Firewall
File Security Tools View Help
Block All
Applications
Logs
Security Test
Help
Incoming
0B
0B
Incoming Traffic History
1K
0K
Attack History Graph
10
0
Outgoing
0B
0B
Outgoing Traffic History
100B
0B
Running Applications :
Hide Windows Services
Hide Broadcast Traffic
Sistema y núcleo de...
Messenger
LSA Shell (Expo...
Generic Host Process f...
Servicios de Internet ...
NDIS User mode I/...
Show Message Console
Security Status: Normal


Advanced Rule Settings
General
Hosts
Ports and Protocols
Scheduling
Applications
Remote Host
Apply this rule to :
All addresses
MAC address :
IP Address(es) :
(IP Address(es) example, 10.0.0.1,192.168.0.1-192.168.0.76)
Subnet :
Subnet IP Address:
Subnet Mask:
Rule Summary:
This rule will block both incoming and outgoing traffic from/to all hosts on all ports and protocols. This rule will be applied to all network interface cards.
Aceptar
Cancelar
i-Safer
SAFE INTERNET
START
OPTION
Lock Screen
Firewall is stopped



OTROS CORTAFUEGOS GRATUITOS

Existen otros cortafuegos gratuitos como:

Filseclab

Es un cortafuegos que permite controlar la conexión a Internet en tiempo real, asignando a las aplicaciones permiso de acceso y controlando los intentos de ataque desde el exterior. Además muestra detalles del tráfico producido y de la conexión del ordenador mediante un atractivo diseño.

Puede descargarse su versión en inglés en http://www.filseclab.com .

Dispone de tres niveles de seguridad, control de eventos a través de ficheros log, un asistente

para crear las reglas y filtros para las aplicaciones y el sistema que controlan el funcionamiento del programa. Además incorpora filtros para la navegación por determinadas páginas web.

Jetico

Jetico Personal Firewall realiza las funciones básicas de protección de intrusiones y control de aplicaciones y servicios que intentan acceder a la conexión. Se pueden establecer diferentes niveles de seguridad y monitorizar el tráfico de paquetes producido.

Puede descargarse su versión en inglés en http://www.jetico.com .

Existen perfiles preconfigurados de seguridad que posteriormente pueden modificarse mediante reglas de filtrado según las necesidades.

WyvernWorks

Es un cortafuegos sencillo de usar pudiendo monitorizar todos los accesos a la conexión permitiendo o denegando permiso a cada aplicación que lo solicite.

Puede descargarse su versión en inglés en http://www.wyvernworks.com/firewall.html .

WyvernWorks Firewall dispone de un gran número de funciones integradas en un interfaz actual y de fácil manejo.

CONCLUSIONES

Aunque la instalación de programas como antivirus o cortafuegos no garantiza una total seguridad, es recomendable protegernos para que la mayoría de intrusos encuentren

suficientes problemas al intentar atacarnos y desistan de sus intenciones.

Además, deberíamos tomar una serie de medidas de seguridad básicas para evitar en lo posible riesgos innecesarios, como:

- mantener actualizado nuestro sistema operativo, navegador y cliente de correo electrónico cómo mínimo
- no guardar o recordar las contraseñas
- asegurarnos antes de instalar nuevo software
- etc.

Debemos tener en cuenta que todos los fabricantes aquí mencionados actualizan continuamente sus productos y pueden añadir funciones que en las versiones probadas no estén disponibles, por lo que es aconsejable leer las indicaciones que nos informan de las características incorporadas en las nuevas versiones que aparezcan.

* Los productos o marcas mencionados en este artículo están registrados por sus respectivas compañías.