

Protección esencial.

La instalación de un cortafuegos es, junto con la del antivirus, una de las columnas esenciales para la seguridad en nuestros sistemas. Este hecho básico aún es ignorado por un número relevante de usuarios.

Dentro del panorama de este tipo de software, **Zone Alarm** destaca por su buenos resultados, requiriendo una experiencia por parte del usuario prácticamente nula para su uso. Pero en el caso del cortafuegos Outpost Firewall de la casa **Agnitum**, vamos a dar un paso adelante, eligiendo un programa eficaz y muy configurable, cuyo uso será aleccionador en cuanto a la comprensión de los mecanismos y configuraciones comunes a estos programas, con la importante ventaja de disponer de versión en nuestro idioma. Existe una guía oficial del programa, en inglés, <http://www.outpostfirewall.com/guide/>

Instalación.

Descargamos el programa de la Web de **Agnitum**. Elegimos para la prueba la versión Pro, que dispone de un periodo de prueba de 30 días, aunque disponemos también de una versión Free con menos opciones. La casa Agnitum es desarrolladora de otros programas de seguridad muy conocidos como lo son el Tauscan y el Jammer. Una vez descargado el ejecutable, procedemos a la instalación, de la que únicamente reseñaremos la posibilidad de elección del módulo de lenguaje y la advertencia que hace el programa de no mantenerlo instalado junto con otros cortafuegos por posible incompatibilidad, si durante la instalación detecta alguno. También es conveniente la actualización inmediata, que viene configurada automáticamente aunque en nuestro caso comprobamos que nada más instalar el programa había actualizaciones pendientes, que instalamos manualmente. Podemos hacerla mediante el icono de la barra de tareas superior.



El programa.

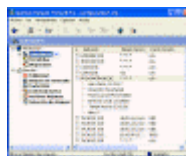
La interfaz del programa es agradable y lo primero que notamos es lo gratificante que resulta encontrarlo en nuestro idioma. La ventana principal del programa es cómoda y nos permite acceder a todas las opciones de configuración desde allí, bien utilizando los menús de la parte superior, bien accediendo a las mismas a través de la celda principal derecha, que más adelante veremos una a una. Hay que señalar que el programa está

configurado por defecto para aportar una protección correcta, como veremos, y que posteriormente podemos mejorar según nuestras necesidades y preferencias.

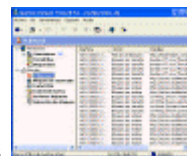


Ventana principal

En la celda principal izquierda se despliega un árbol informativo, que nos brinda el acceso a todas las circunstancias y eventos que en tiempo real controla el firewall, como las conexiones establecidas, o los bloqueos realizados por el programa. Esto admite ser configurado, mediante el comando "Ver --- apariencia" del menú superior. Es interesante, por ejemplo, añadir mediante la selección de la casilla "Puertos Abiertos" la opción de ver los puertos que tenemos abiertos y las aplicaciones que los están utilizando, el tiempo de conexión etc. Desde este árbol podemos igualmente cambiar las reglas aplicadas o las distintas configuraciones de las opciones y plug-ins, seleccionando y pulsando el botón derecho para acceder al menú emergente correspondiente.



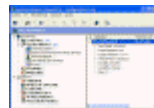
Despliegue conexiones



Despliegue bloqueos



Ver puertos abiertos



Despliegue puertos abiertos.

Configuración.

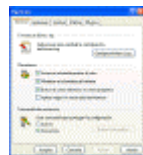
Desde el menú superior "Opciones" o directamente desde la celda principal derecha "Firewall --- Aplicación ó Sistema" establecemos los parámetros principales de funcionamiento del programa.

Pestaña "General" Configura tres opciones generales del programa:

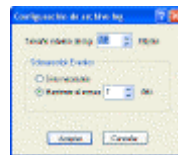
El tamaño y permanencia del archivo "Log", una posibilidad necesaria y que no todos los cortafuegos incorporan.

Las opciones de inicio y la posibilidad de establecer una contraseña para proteger la configuración que establezcamos en el programa.

Podemos mantener sin mayores problemas la configuración por defecto.



Pestaña "general"



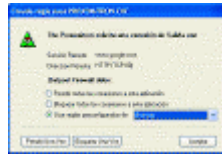
Configurar Log

Pestaña "Aplicación" Aquí accedemos a una ventana donde se reflejan todas aquellas aplicaciones de nuestro sistema que mantengan una relación con el firewall, relación que puede ser de permiso, de bloqueo o de comportamiento establecido conforme a la regla asociada para ella.

Seleccionando la aplicación y mediante el botón "Modificar" podemos cambiar el estado de la mismas, o agregar o quitar aplicaciones mediante los botones respectivos. No es necesario agregar previamente las aplicaciones, ya que el asistente del cortafuegos nos preguntará en el momento que algún programa requiera que se establezca una regla respecto al mismo, pero acudiremos a esta ventana para cambiar esa condición o para establecer los permisos que queramos, pudiendo protegerlos de otros usuarios si utilizamos la contraseña. Seleccionando la aplicación, podemos modificar sus reglas mediante el botón "Modificar" que da paso a una ventana de estado donde se reflejan las reglas establecidas para la aplicación, las cuales podemos modificar.

También podemos eliminar una aplicación del listado del firewall con el comando "Eliminar", lo que puede ser conveniente con aplicaciones que hemos desinstalado. En el caso de que eliminamos una aplicación de la relación del firewall y posteriormente la volvamos a utilizar, el asistente nos

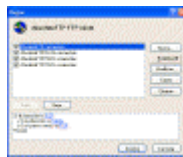
consultará para crear una regla hacia la misma, con el añadido de que entre las opciones incluirá la antigua regla asociada a dicha aplicación.



Asistente para reglas



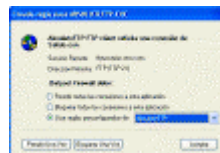
Pestaña Aplicación



Acceso a reglas aplicaciones



Configurando reglas



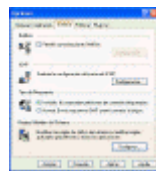
Reasignación de regla

Pestaña "Sistema" Este es un lugar importante dentro de la configuración del cortafuegos.

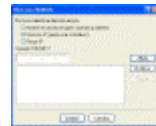
Permitir comunicaciones Netbios. En primer lugar, nos encontramos con una casilla que permite seleccionar el tratamiento a las comunicaciones Netbios. Convenientemente desactivada por defecto, podemos no obstante activarla si necesitamos compartir recursos y autorizar a un dominio, IP concreta o rango de las mismas.

Cambiar la configuración del protocolo ICMP. ¿Y esto qué es? Bueno, en pocas palabras este protocolo maneja los mensajes de error entre la fuente IP de origen y la de destino informando si un paquete enviado alcanza el destino, si su encabezamiento es correcto etc. Sobre este protocolo funciona el servicio de PING. Este protocolo y la herramienta ping es útil a los administradores de redes, pero también posibilita ciertos tipos de ataques, por lo que en principio no necesitamos activar ninguna opción, cosa que confirmamos con algunas pruebas, en todo caso marcaremos las dos primeras casillas en el apartado "Salida".

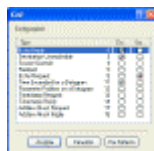
Tipo de respuesta. Es importante que mantengamos activada la casilla "Invisible: no responder a peticiones de conexión bloqueadas". Es el famoso modo "Stealth". Es mucho más seguro no existir aparentemente que estar cerrado pero que sepan donde estás.



Pestaña Sistema



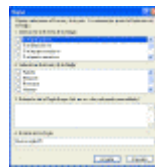
Netbios



Protocolo ICPM



Reglas generales



Creando regla

Realizamos seguidamente los otros test de la página, más avanzados, obteniendo resultados Stealth, excepto para el puerto 135 abierto por su utilización por el Generic Host Process de Windows, al que hemos permitido la conexión en principio, pues la requieren ciertos servicios de W XP mediante el SVCHOST.EXE . Debemos crear más tarde una regla para bloquear dicho puerto, o buscar la posibilidad de cerrarlo. Más adelante haremos otras pruebas más a fondo y crearemos reglas a medida, pero en principio comprobamos que la protección que ofrece la configuración por defecto es correcta.

Pestaña "Política" Esta pestaña permite asignar un nivel de permisividad al firewall, y no nos parece más relevante que por la posibilidad de desactivar el firewall desde aquí, o bloquear todas las conexiones de una vez. El nivel "Asistente" nos da la comodidad de ir asignando permisos a medida que surja la necesidad, el nivel restrictivo solo atenderá aquellas

peticiones con regla preestablecida por nosotros. El nivel permisivo, como si no existiera.

Los sitios de confianza se agregan desde esta pestaña, asimismo, para dar ese tratamiento a aquellos que seleccionemos como seguros.



Política

Pestaña "Plug-ins" Y llegamos a los "Plug-ins" una parte muy interesante de este firewall. Veámoslos uno a uno:

Publicidad. Este Plug-in posibilita dos tipos de acciones sobre la publicidad Web:

Bloquear imágenes por cadenas de html. Sencillo, seleccionamos una cadena de texto de cualquier imagen y la añadimos al listado, el programa la bloqueará antes de que el navegador la presente. Este filtro se ha mostrado efectivo frente a algunas imágenes que han superado el filtro por tamaño.

Bloquear imágenes por tamaño. En este filtro se especifican los distintos tamaños de imágenes que serán bloqueadas por el cortafuegos antes de ser mostradas por el navegador. Dichas medidas son Standard, pero el filtro puede fallar por ligeras variaciones.

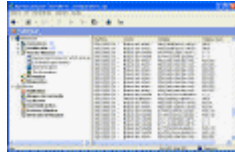
Lo ideal es ir añadiendo dimensiones o cadenas de texto de las imágenes y ventanas de sitios que vayamos a visitar a menudo, así como de empresas publicitarias que no estén incluidas en el listado por defecto, y de esa manera combinar el cortafuegos con el uso del [Proxomitron](#). Una dimensión muy aconsejable de añadir es la de 1 X 1 píxel, en prevención de contenido [Web-Bug](#) y gifs invisibles en las páginas visitadas.

En la captura se puede apreciar la cantidad de bloqueos que realiza el programa, incluidos un par de ellos de gifs de 1X1 píxel, bloqueados a los pocos minutos de navegar con esas medidas añadidas a la lista. Todo eso es basura que no nos llega.



Bloqueo por texto

Bloqueo por tamaño



Log bloqueo publicidad



Bloqueo de contenido



Caché DNS

Bloqueo de contenido. Es otra interesante herramienta, que bloquea de manera efectiva cualquier palabra o combinación de ellas que incluyamos en el listado. Útil no sólo para filtrar un contenido inadecuado, sino para el bloqueo de página enteras, dependiendo de la pestaña en la que incluyamos la orden.

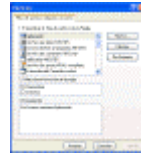
Caché DNS. Al solicitar una página a nuestro navegador, este ha de buscar esa dirección en ocasiones en diferentes bases de datos, lo que puede ralentizar el proceso. Activar esta opción puede acelerar la manera de resolver dichas peticiones, ya que se almacena una tabla personalizada de direcciones habituales para acceder a ellas más rápidamente. Es posible configurar parámetros como el número de registros guardados, los días de permanencia y añadir o quitar direcciones.

Contenido activo. Otro plug-in interesante. Aquí podemos establecer el tratamiento que el firewall dará al contenido activo de las páginas que visitemos. En primer lugar, se establecen las pautas con carácter general. Si somos muy restrictivos, podemos impedir contenido potencialmente nocivo así como cookies y aplicaciones e java, o ventanas emergentes. Si seleccionamos la opción "Preguntar" la navegación puede hacerse un tanto pesada ya que el cortafuegos nos preguntará prácticamente en cada página

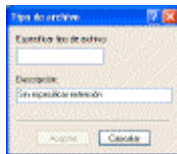
que abramos, pero podemos establecer de esa forma la regla para las página que visite mos asiduamente, bloqueando el contenido de forma genérica a otro tipo de páginas menos habitual.



Contenido activo



Adjuntos



Agregar tipo de archivo



Detección de ataques



Log ataques

Archivos adjuntos. Plug-in para el filtrado de los mensajes de correo. Por archivos adjuntos no sólo se entiende los ficheros que acompañan a los mensajes, sino el contenido embebido en los mismos, en forma de código html, scripts etc. La operativa para la modificación o creación de reglas es la misma que la descrita para las aplicaciones. A nosotros no nos ha funcionado con total eficacia con el Outlook y cuentas Hotmail, ... lo miraremos más a fondo. El plug-in se integra mejor el el gestor de correo The Bat, pero tampoco alcanza una efectividad plena.

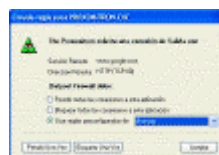
Detección de ataques. Por último, este plug-in establece la actuación del firewall frente a los ataques externos. La posición intermedia del nivel de alarma es la adecuada, y los bloqueos podemos establecerlos a nuestra elección, siendo a nuestro entender conveniente activarlos, en especial el bloqueo DOS, aunque hay algunas informaciones que desaconsejan su utilización (Ver enlaces, [comparativas](#)).

En la captura podemos ver el listado en tiempo real al cual podemos acceder en cualquier momento, en el que hemos resaltado un escaneo de

puerto y un intento de conexión por parte de la misma IP. El programa así configurado registra los eventos, disponemos de la información fácilmente y no agobia con insistentes alertas.

Funcionamiento

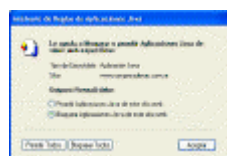
Una vez revisadas las distintas opciones que trae el programa, de las cuales hemos modificado las que nos haya parecido necesario, según lo visto, no hay más que ponerse a funcionar. El programa irá solicitando nuestra intervención a medida que surja la necesidad de aplicar una regla a una aplicación o a un evento en una Web. Sólo habrá que elegir la opción adecuada al nivel de seguridad elegido para esa Web o el permiso o denegación de conexión a las aplicaciones, que puede ser permanente o momentáneo.



Asistente aplicaciones



Asistente Cookies



Asistente Java

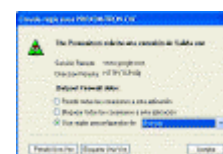


Reglas preconfiguradas

Las reglas establecidas para las aplicaciones pueden ser fácilmente cambiadas, simplemente seleccionándolas y accediendo al menú de reglas con el botón derecho. allí encontramos también los tipos de reglas predeterminadas.

Funcionamiento

Una vez revisadas las distintas opciones que trae el

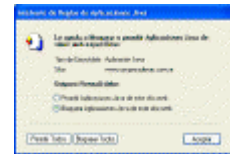


programa, de las cuales hemos modificado las que nos haya parecido necesario, según lo visto, no hay más que ponerse a funcionar. El programa irá solicitando nuestra intervención a medida que surja la necesidad de aplicar una regla a una aplicación o a un evento en una Web. Sólo habrá que elegir la opción adecuada al nivel de seguridad elegido para esa Web o el permiso o denegación de conexión a las aplicaciones, que puede ser permanente o momentáneo.

Asistente aplicaciones



Asistente Cookies



Asistente Java



Reglas preconfiguradas

Las reglas establecidas para las aplicaciones pueden ser fácilmente cambiadas, simplemente seleccionándolas y accediendo al menú de reglas con el botón derecho. allí encontramos también los tipos de reglas predeterminadas.

Opinión sobre el programa.

El programa tiene, aparte de su efectividad innegable como cortafuegos, otras características positivas:

Incluye opciones de configuración para Netbios y limitación del tamaño del archivo "Log".

Una interfaz práctica y muy clara, es difícil perderse o no tener una idea clara del funcionamiento a las primeras de cambio.

El idioma, un punto importante.

Es lo suficientemente sencillo en el uso y configuraciones, pero no es un programa simple o escaso de medios, al contrario.

Es discreto en el espacio ocupado/recursos consumidos. La carga del programa al inicio pasa totalmente desapercibida al usuario, al contrario que en otros programas como el Zone.

El programa resulta agradable, esto se agradece en un programa de uso cotidiano como es un cortafuegos.

Supero correctamente diferentes test online, concretamente los de Sygate, PC Flanks, Symantec y Steve Gibson, apareciendo en modo Stealth todos los puertos excepto el 135.

Ya probamos el programa cuando apareció su primera versión y nos dio algunos problemas con ciertas aplicaciones, en esta segunda ocasión, varias versiones después, dichos problemas no han surgido.