MINISTERIO
DE EDUCACIÓN
Y CIENCIA

SECRETARÍA GENERAL
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL

DIRECCIÓN GENERAL
DE EDUCACIÓN,
FORMACIÓN PROFESIONAL
E INNOVACIÓN EDUCATIVA

CENTRO NACIONAL
DE INFORMACIÓN Y
COMUNICACIÓN EDUCATIVA

Internet aula abierta

Seguridad

C/ TORRELAGUNA, 58
28027 - MADRID

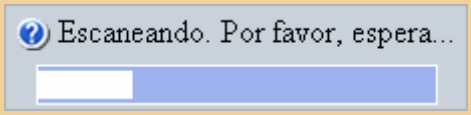
ÍNDICE GENERAL

Comprobando la seguridad

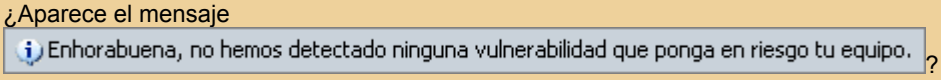
En esta ocasión vamos a empezar realizando una práctica que te permitirá comprobar el grado de seguridad de tu equipo.

Práctica

Conéctate a la dirección www.upseros.net/portscan/portscan.php

Mientras se realizan las pruebas aparecerá el mensaje 

Comprueba los resultados.

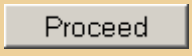
¿Aparece el mensaje


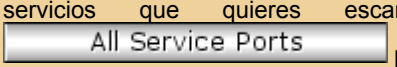
?

Si has logrado que el listado de puertos esté lleno de semáforos en rojo y el colofón de la información es el mensaje anterior quiere decir que tu equipo está protegido contra las intrusiones desde el exterior y es probable que hayas puesto en práctica la mayoría de las medidas que se van a comentar en este módulo. En caso contrario necesitarás mejorar la seguridad de tu sistema, para lo cual tendrás que modificar algunas conductas en tu navegación por la red y dotarte de algunas herramientas que te ayuden a protegerte de accesos indeseados.

Práctica

Si quieres corroborar los resultados anteriores puedes conectarte a grc.com/default.htm, localiza el enlace **ShieldsUP!** y pulsa sobre él

Pulsa ahora el botón 

que te llevará a una nueva página en la que podrás escoger los servicios que quieres escanear. Lo más recomendable es que selecciones 

para hacer un test completo.

En esta ocasión el objetivo es que la matriz que representa los 1056 primeros puertos no presente ningún cuadradito rojo

Normas básicas de seguridad

La utilización de herramientas tecnológicas exige, al igual que ocurre con cualquier otro tipo de herramientas, comportarse de forma prudente para evitar consecuencias negativas. Antes de continuar querría subrayar que la prudencia no tiene nada que ver con la paranoia: es una actitud vigilante pero tranquila que salvaguarda nuestra seguridad y nuestros intereses.

Adoptando pues esta actitud básica podemos decir que existen conductas de protección de la seguridad de tipo activo y de tipo pasivo. Sería algo similar a lo que ocurre cuando nos ponemos al volante de un coche: abrocharse el cinturón supone dotarnos de una protección pasiva, mientras que mantener una velocidad adecuada o regular las paradas para que el cansancio no nos provoque sueño entraría dentro de conductas activas que, en ambos casos redundan en un aumento de la seguridad.

Dentro de las conductas que hemos denominado pasivas podríamos destacar las siguientes:

- Configurar nuestro sistema operativo para que obtenga e instale de forma automática las actualizaciones y parches de seguridad que sean necesarios.
- Obtener e instalar un antivirus que disponga de actualización automática y configurarlo de forma que revise, también de forma automática, el correo, los archivos descargados y, en general, cualquier archivo que podamos abrir en nuestro ordenador.
- Proteger nuestro equipo del acceso no autorizado del exterior, así como evitar la salida inadvertida de datos desde el mismo, instalando y configurando un cortafuegos, especialmente si disponemos de una conexión a constante a Internet.
- Apagar aquellos equipos que tengan posibilidad de acceder de forma constante a internet cuando no se utilicen.
- Si eres usuario de Windows es probable que la utilización de contraseñas para acceder al sistema te resulte un procedimiento poco habitual y que lo consideres incómodo. No estaría de más que te plantearas, si dispones de algún sistema que permita un control real de usuarios (Windows 2000, XP), la creación de un perfil de usuario con permisos limitados dejando los permisos de administrador sólo para aquellos momentos en los que tuvieras que instalar algún programa. Lógicamente la misma recomendación es válida para sistemas Linux, aunque en este caso lo habitual es aacc(Si no lo haces así es posible que algún código malicioso se aproveche de tu acceso libre con permisos absolutos para instalar virus, gusanos, troyanos y otros especímenes)

Veamos ahora algunas cuestiones en las que deberían convertirse en pautas activas de conducta cuando utilices Internet:

- Actualiza regularmente el software de tu ordenador a las versiones más recientes.
- Realiza copias de seguridad de tus datos cada cierto tiempo. Reinstalar un sistema operativo con todas sus aplicaciones puede ser muy pesado, pero es algo casi mecánico,...rehacer dos años de trabajo suele ser imposible.
- Si accedes a Internet mediante un módem revisa de vez en cuando el Acceso Telefónico a Redes para ver la conexión. Ten cuidado con algunas páginas, sobre todo las de juegos, contenido para adultos y algunas de descargas gratuitas, que te piden que instales programas para optimizar el acceso: en la mayoría de los casos se trata de un Acceso Telefónico a Redes que conecta con un número de teléfono de pago incrementado, lo que se conoce con el nombre de dialer. Recuerda que puedes solicitar a Telefónica que anule el acceso a los números de tarificación especial con lo que, al menos, evitarás el perjuicio que te puede suponer mantener sin saberlo una llamada internacional durante varias horas o días.
- Si tienes que introducir información sensible, como por ejemplo el número de tu tarjeta de crédito, en una página web, no lo hagas nunca si no se trata de una conexión segura: en el campo de protocolo de la dirección pondrá **https:** en lugar de **http:** y en tu barra de estado aparecerá el símbolo 
- No te fíes de los enlaces de las páginas, especialmente cuando accedas a páginas de servicios bancarios o de comercio electrónico. Comprueba que te conducen donde realmente quieras ir.
- Configura tu cliente de correo para recibir y enviar en modo texto. Tal vez quede algo más soso, pero evitarás una fuente de problemas de seguridad y de privacidad.
- Comprueba la extensión de los archivos que recibes por correo electrónico. No los abras nunca si se trata de ejecutables.
- Tus amigos, esos que no saben decir en inglés más que yes, no se han apuntado a una academia milagrosa y por eso te escriben ya en la lengua de Shakespeare: o bien tienen un virus en su ordenador o bien alguien ha usurpado su dirección, pero lo que es seguro es que el archivo adjunto que te envían es un código malicioso.
- Ni los bancos, ni ninguna otro servicio web que necesite identificación, se va a poner en contacto contigo por correo electrónico para solicitar que confirmes tu nombre de usuario y tu contraseña desde un formulario en el propio mensaje de correo o desde una página a la que se te enlaza desde el mismo: se trata de una práctica para apoderarse de esos datos.
- Cuando envíes archivos adjuntos coméntalo en el cuerpo del mensaje y haz un breve resumen de su contenido. No envíes nunca archivos ejecutables.
- Lee despacio y con todo detalle todas las ventanas que se muestran durante la instalación de cualquier aplicación que descargues de Internet, incluso la licencia o el contrato del usuario final. De esta forma te asegurarás de que no incluyen ningún software sospechoso.
- Analiza periódicamente tu equipo con algún programa antiespía.
- No propagues bulos. Cuando te llega un mensaje avisando de un peligro muy grave cuando se hace tal o cual cosa suele ser un bulo difundido por un amigo que te quiere bien pero no se ha preocupado de comprobar la veracidad del contenido. Muchas veces basta con hacer una lectura

medianamente atenta y una simple búsqueda en Google para comprobar que el mensaje no es más que un bulo infundado.

- No estaría de más que, de vez en cuando pasaras por alguna de las páginas que disponen de secciones divulgativas sobre seguridad para mantener tu información actualizada: Asociación de Usuarios de Internet, Hispasec, Alerta antivirus pueden ser unos buenos puntos de referencia.
- Utiliza el sentido común: no hagas en la red aquello que no harías en la vida real.
- Una última cuestión de no poca importancia: sigue el espíritu básico de la red y ayuda a los demás dando a conocer las normas de seguridad.

Antivirus on-line y otras utilidades

Si no dispones aún de un antivirus actualizado tienes la posibilidad de aplicar algunas utilidades que se ofrecen de forma gratuita en la red, mediante las cuales podrás informarte de las últimas amenazas, realizar un análisis de tu equipo y descargar utilidades de desinfección en caso de que localices algún código maligno. Las tres que se muestran a continuación son ofrecidas gratuitamente por Panda Software

Chequeo on-line	Utilidades de reparación	Virusómetro
Pulsa sobre la imagen para acceder al chequeo on-line de virus. Necesitarás una conexión activa para poder utilizarlo.	Pulsa sobre los enlaces que aparecen abajo para acceder a las utilidades de reparación. Si tu conexión no está activa, sólo verás este párrafo	Pulsa sobre la imagen para acceder al Virusómetro con las alertas de virus. Si tu conexión no está activa, sólo verás este párrafo

Cortafuegos

Con la denominación cortafuegos (firewall) nos referimos a los programas que se encargan de monitorizar las transferencias de información que se producen desde y hacia nuestro ordenador. En muchos casos estas transferencias de información corresponden a procesos que hemos iniciado voluntariamente y sus correspondientes respuestas, tales como peticiones de páginas web, envíos o recepciones de correo, exploración de las máquinas de nuestra red, consultas automáticas de actualizaciones de programas, etc. Pero también puede haber ocasiones en las que dichas transferencias se producen sin nuestra autorización y con finalidades que nada tienen que ver con nuestros intereses pudiendo, incluso, resultar particularmente perjudiciales.

Antes de continuar vamos a formular un par de advertencias:

- La red está plagada de aplicaciones y funcionalidades útiles e interesantes aunque, como en cualquier otro ámbito de las interacciones humanas, existen personas o grupos malintencionados que diseñan aplicaciones perjudiciales.
- Ser prudente y mantener una adecuada preocupación por la seguridad es muy positivo; la actitud paranoica que nos lleve a sentir una constante amenaza será, como en cualquier otro ámbito, una patología que no reportará ningún beneficio.

Se hace imprescindible llevar un control de las comunicaciones que se producen a través de nuestra máquina para evitar que programas malintencionados nos espíen, utilicen nuestro ordenador para enmascararse o, simplemente se difundan desde nuestro equipo a través de las redes a las que estemos conectados. Lógicamente, cuanto más amplia sea nuestra conectividad, más importante es contar con alguna utilidad que controle el intercambio de información.

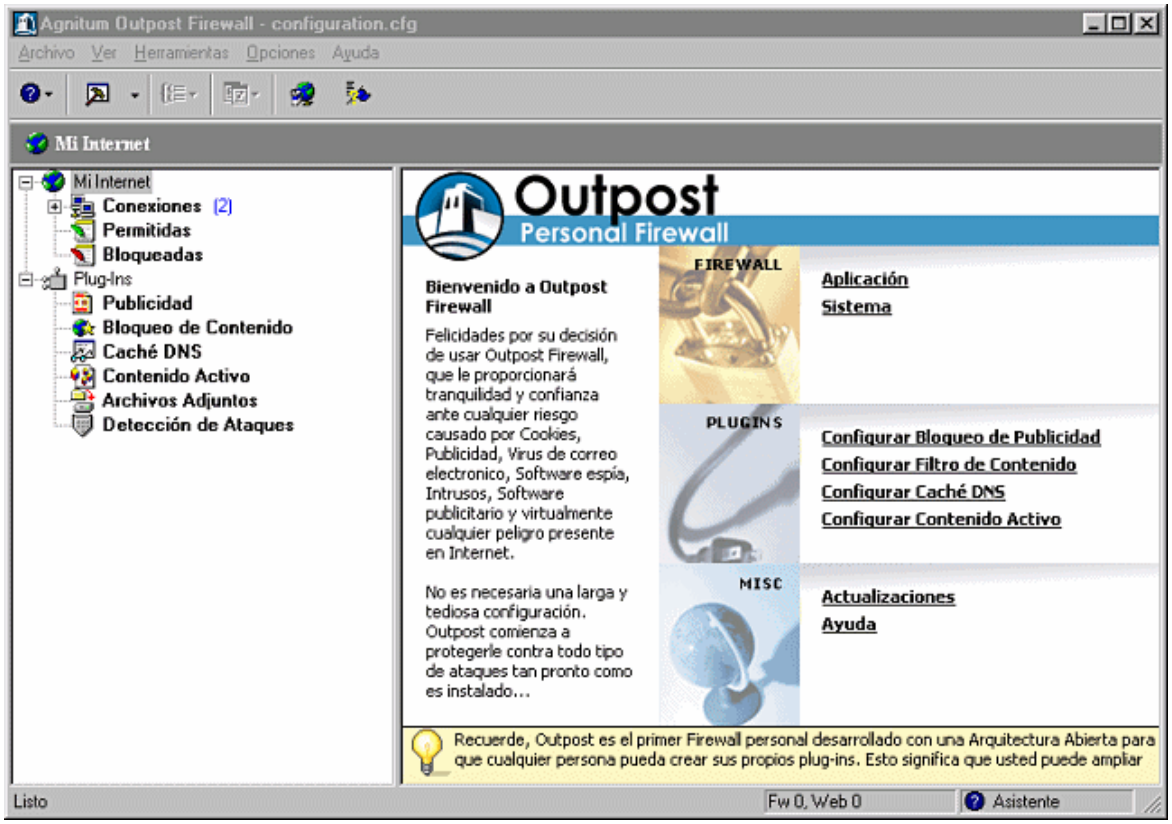
Existen programas comerciales que ofrecen multitud de prestaciones, pero también existen versiones freeware que aportan una funcionalidad bastante completa. En este epígrafe describiremos la utilización de un programa para entorno Windows que dispone de una versión totalmente gratuita: Agnitum Outpost Firewall free. Si quieres buscar y probar algún software diferente puedes consultar en Softonic la sección dedicada a cortafuegos para Windows o Linux

Descarga e instalación de Agnitum Outpost Firewall

Posiblemente lo primero que haya que aclarar, teniendo el cuenta el nombre del programa, es que se encuentra en castellano. Para descargarlo hay que visitar la página de la empresa creadora, Agnitum, para localizar la versión free.

Es posible que cuando inicies la instalación pienses que has descargado una versión errónea porque todo el proceso aparece en inglés. No te preocupes puesto que el cambio al castellano se produce de forma automática al iniciar el programa ya que éste detectará la configuración del sistema y adaptará el idioma de presentación. Lo que sí te ocurrirá es que cuando intentes consultar la ayuda ésta aparecerá en inglés, aunque puedes corregir esta situación si descargas el archivo comprimido en formato .zip o bien formato .rar que se encuentran en www.outpost-es.com/download/manual.html.

Como la versión con la que trabajamos es la que se distribuye gratuitamente, lo primero que hará el programa cuando se inicie es informarnos de que existe una actualización y sugerirnos la posibilidad de utilizar la conexión a Internet para descargarla. Ten en cuenta que no se trata de una actualización de la versión free, sino de una demostración de la versión comercial que tiene un periodo de prueba de treinta días.



Verás que en la barra del sistema ha aparecido un icono 

que nos indica que el programa está activo y nos informa del modo en que está funcionando. Por defecto, el modo de funcionamiento es el asistente de reglas, aunque también existen otros modos de trabajo que puedes especificar mediante la opción de menú **Opciones ➡ Política**

Icono	Modo	Descripción
	Desactivado	Permite todas las conexiones sin ninguna restricción.

Icono	Modo	Descripción
	Permisivo	Permite todas las conexiones que no hayan sido específicamente bloqueadas mediante reglas.
	Asistente	Lanza el Asistente de Reglas para crear nuevas reglas para cualquier tipo de conexión que no esté cubierta por alguna de las reglas actuales.
	Restrictivo	Bloquea todas las comunicaciones que no hayan sido específicamente permitidas mediante reglas.
	Bloqueado	Bloquea todas las comunicaciones, tanto de Entrada como de Salida.

Para modificar el modo en el que actúa el programa también puedes hacerlo pulsando con el botón derecho sobre el icono de la barra de sistema y eligiendo igualmente la sección **Política** para marcar el modo que se quiere utilizar.

Si nunca antes habías utilizado un cortafuegos, es probable que te sientas algo desconcertado cuando te conectas a Internet y el programa empieza a preguntarte qué debe hacer en determinadas situaciones. Para evitarlo veamos cuál es el esquema básico de funcionamiento del cortafuegos:

1. Una aplicación intenta acceder a Internet
2. Outpost Firewall comprueba si se encuentra dentro de las aplicaciones reconocidas.
    A. Es una aplicación conocida y tiene adjudicadas unas reglas predefinidas ➡ El programa aplica las reglas y permite o bloquea la conexión en función de lo establecido en ellas.
    B. Es una aplicación desconocida o las condiciones de las reglas definidas no contemplan la situación actual ➡ El programa nos pide que le indiquemos una regla:
        1. Permitiendo o bloqueando de forma continua esa aplicación
        2. Permitiendo o bloqueando el acceso en esta ocasión
        3. Utilizando alguna de las correspondiente a las aplicaciones conocidas
        4. Estableciendo las condiciones y las acciones que se realizarán cuando se repitan las actuales condiciones.
    C. El programa aplica la regla y la almacena para ocasiones sucesivas, clasificando la aplicación como permitida, bloqueada o con reglas.

En función de lo que hagamos en los pasos anteriores, las aplicaciones quedarán clasificadas en:

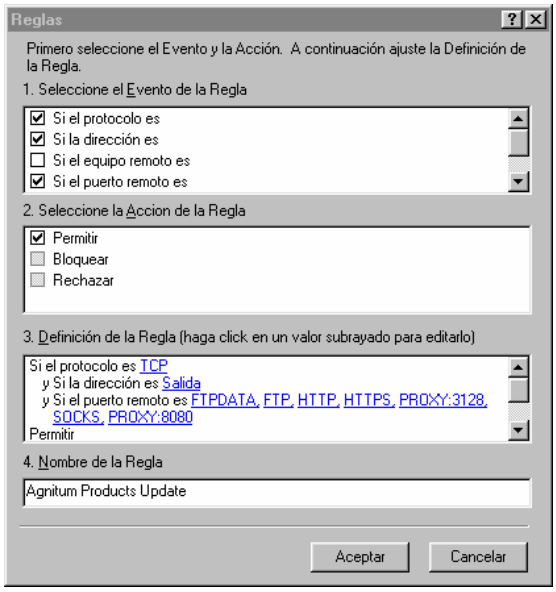
Bloqueadas:
Todas las conexiones a Internet de este grupo se encuentran bloqueadas. El programa recomienda incluir en este grupo las aplicaciones que no necesitan conexión a Internet, como editores de texto, calculadoras, etc, pero no olvides que si lo haces así y encuentras un documento de texto que incluye un enlace a una dirección en Internet, no podrás acceder directamente a la misma desde el propio procesador de texto.

Aplicaciones con Reglas
Todas las conexiones a Internet de este grupo se encuentran restringidas según la regla creada para cada aplicación en particular y sólo serán permitidas las conexiones específicamente admitidas. La mayoría de las aplicaciones estarán contenidas en este grupo.

Aplicaciones permitidas
Todas las conexiones a Internet de este grupo se encuentran permitidas. Si quieres mantener un nivel de protección adecuado sería conveniente que este grupo estuviera vacío, aunque eso suponga una cierta molestia porque, de cuando en cuando, aparecerá una pregunta del asistente para averiguar qué se debe hacer en una circunstancia no habitual.

Para llega a la clasificación que hemos visto habrá bastantes casos sencillos, ya que cuando nos pregunte la primera vez qué debe hacer cuando nuestro navegador intente acceder a Internet bastará con decirle que utilice las reglas preconfiguradas para el browser (navegador). Posiblemente la situación más compleja se producirá cuando nos encontremos con el punto 2.B.4 del proceso, bien sea porque se trata de una aplicación desconocida o porque se produce una circunstancia que no está contemplada en las reglas generales.

En estos casos, cuando se lance el asistente ya vendrán recogidos los datos que caracterizan la situación: protocolo, dirección de la comunicación, URL del equipo remoto, puerto, etc, debiendo especificar la acción que deseamos que se realice. En la imagen que se muestra como ejemplo vemos las condiciones y la acción que se aplica para la configuración de las actualizaciones del propio cortafuegos.



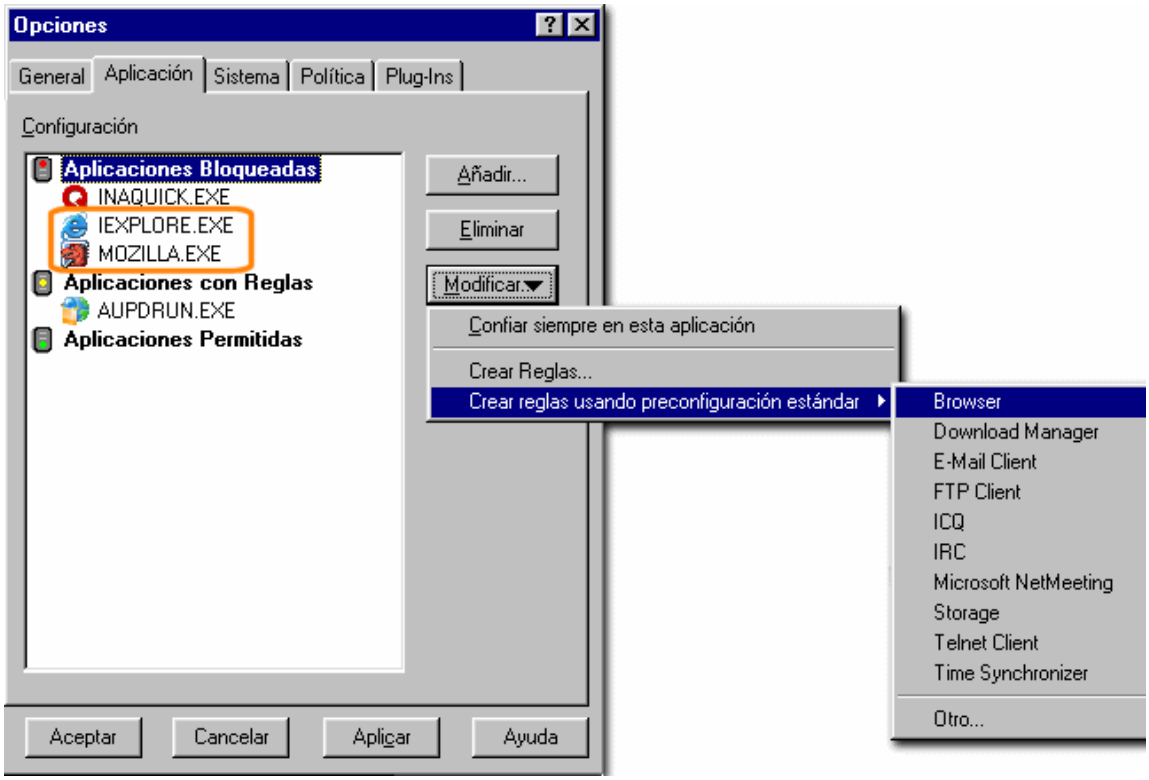
Como puede observarse, en la zona inferior aparece el resumen de todas ellas, pudiendo modificarse con un doble clic.

Si no tienes muy claro lo que hay que hacer, lo mejor es optar por decisiones que no sean definitivas y que te permitan ir observando lo que ocurre hasta que llegues a una conclusión sobre si la regla que debes adoptar es en la línea de permitir o denegar la conexión. Dentro de esta política de aprendizaje podrías optar por Permitir una vez o Bloquear una vez. Parece lógico que, si pretendes mantener tu seguridad mientras te dedicas a observar, lo más prudente es que optes por la opción de Bloquear el acceso en esta ocasión: si ves que el bloqueo no produce ningún efecto negativo ya tienes un elemento que te aproxima hacia uno de los criterios, mientras que si ves lo contrario y el programa vuelve a solicitarte permiso tal vez se deba a que la opción adecuada es conceder ese permiso.

Mientras no tengas claro si debes conceder permiso a una aplicación es preferible que sigas haciendo pruebas bloqueando el acceso cada vez que se produzca una petición. Ten en cuenta que, una vez establecida una regla, se aplicará automáticamente sin volver a consultarte.

No puedo acceder a Internet

Todos podemos equivocarnos y pulsar la opción inadecuada. A veces no nos daremos ni cuenta del error, pero en otros casos la situación se hará evidente de forma inmediata. Uno de los problemas más frecuentes cuando se utiliza un programa cortafuegos es que indiquemos erróneamente el bloqueo permanente de una aplicación y si ésta es nuestro navegador...



Parece que el usuario que realizó la configuración que se muestra en la imagen previa no estaba muy dispuesto a navegar por Internet, ya que Mozilla y Explorer se encontraban dentro de las aplicaciones bloqueadas, pero como ves también en la ilustración habría una solución, ya que marcando cada una de ellas podríamos indicarle al cortafuegos que les aplicara las reglas predeterminadas para los navegadores.

Para poder realizar esta modificación acudiríamos al menú **Opciones ➡ Aplicación...** y se nos mostraría la pantalla con las aplicaciones incluidas en cada categoría. Tras realizar el cambio sugerido comprobaríamos que los dos navegadores han cambiado su ubicación pasando a la categoría de Aplicaciones con reglas.

No puedo acceder a los equipos de la red (o los otros equipos no pueden acceder al mío)

Uno de los protocolos que pueden suponer un mayor riesgo en la comunicación de nuestro ordenador con otros equipos es el denominado Netbios (Network Basic Input/Output System). Se trata de un protocolo diseñado para compartir impresoras y archivos dentro de una red de área local, pero supone un importantísimo agujero de seguridad ya que podría darse el caso de que alguien lo utilizara para acceder desde Internet a nuestro equipo, utilizando todos los permisos que hayamos establecido para las carpetas compartidas.

Outpost Firewall bloquea por defecto el puerto 139 que es el utilizado por el protocolo Netbios, por lo que si existen en la red local equipos con versiones de Windows que utilicen este protocolo dejaremos de ser capaces de acceder a los mismos, así como a los recursos compartidos de nuestro equipo desde ellos. Si necesitamos activar el protocolo Netbios porque se utiliza en nuestra red tendremos que utilizar la opción de menú **Opciones ➡ Sistema...**, marcar ☑ Permitir comunicaciones NetBios y pulsar el botón Configuracion...

En la pantalla de configuración podremos optar por utilizar ◉ Nombre de dominio (requiere conexión a internet) pero está claro que esto no es una opción nada recomendable.

Sin embargo sí podemos utilizar ◉ Dirección IP (puede usar comodines) que nos permite indicarle al programa una dirección concreta (ej.: 192.168.1.4) o bien utilizar comodines para permitir el acceso a todas las direcciones de un subdominio (ej.: 192.168.1.* que permitiría el acceso a cualquier ordenador que tuviera una dirección IP comprendida entre la 192.168.1.0 y la 192.168.1.255).

También tenemos la opción de restringir el rango de direcciones a una cantidad más limitada utilizando ◉ Rango IP que nos permite especificar los extremos del intervalo de direcciones permitidas (ej.: 192.168.1.1 - 192.168.1.10 que permitiría el acceso únicamente a los equipos que tuvieran alguna de las diez direcciones comprendidas en ese intervalo)

Plugins

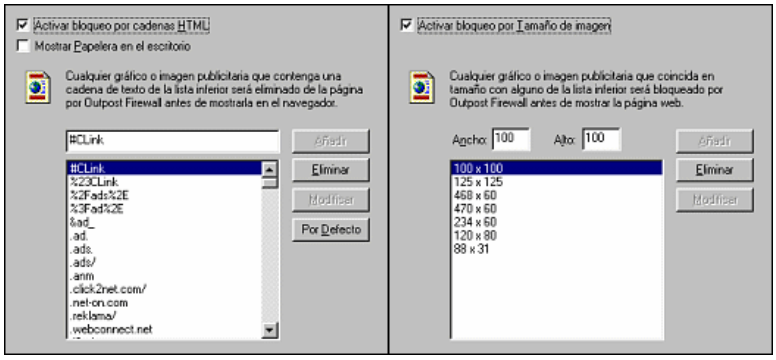
El término plug-in se utiliza para referirse a componentes ajenos al núcleo de un programa que tienen la capacidad de integrarse con el mismo para aportar nuevas funcionalidades. Outpost Firewall está concebido para incorporar plugins y cuando lo instalamos ya incluye unos cuantos que se inician de forma automática con el programa.

El acceso a la pestaña desde la que se controlan y configuran estos añadidos se realiza desde la opción de menú **Opciones ➡ Configurar Plug-Ins...**

Uno de los que puede tener una beneficiosa repercusión cuando no disponemos de una conexión de banda ancha es el que se encarga de gestionar la **publicidad**. Su trabajo consiste en

localizar las imágenes que tienen en su nombre o en la URL de la que proceden algunas cadenas que se corresponden con los nombres de sitios que distribuyen publicidad. También realiza un bloqueo ateniéndose al tamaño habitual de los banners publicitarios que se presentan en las páginas web.

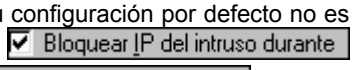
Aunque para quienes disponen de conexión de banda ancha no aporta una gran mejora sí puede suponerlo para quienes utilizan una conexión RTC con módem, ya que una vez que el programa determina que una imagen es publicidad no se produce su descarga del servidor con la consiguiente aceleración en la navegación.



El filtro de publicidad puede combinarse el filtro de **bloqueo de contenidos** como un recurso para lograr una navegación en la que se minimice el impacto de contenidos no deseados, tales como enlaces a páginas de juego o con contenidos de los que eufemísticamente se denominan "para adultos".

Cuando se intente acceder a un sitio web cuya dirección se haya incluido entre las bloqueadas o que contenga palabras que se hayan establecido como filtro, aparecerá un mensaje indicando la situación: "The web page being accessed was blocked due to undesirable content. Please see the Outpost Content Filtering Plug-In Log for details." (*"El sitio de Internet al que se está accediendo ha sido bloqueado debido a su contenido indeseado. Por favor, vea el registro del complemento Bloqueo de Contenido para más detalles."*)

De todas maneras, aunque el filtro de contenidos se inicia automáticamente cuando arranca el programa, no está configurado, apareciendo en blanco el listado de palabras y de sitios web que se utilizarán como criterio de filtrado. Esto tiene la ventaja de resultar muy respetuoso con los criterios del usuario, pero presenta el inconveniente de que es necesario configurarlo manualmente, agregando las palabras o los sitios web uno a uno ya que no hay posibilidad de incorporarlos desde un archivo externo.

También merece una mención el filtro de **detección de ataques,** ya que su configuración por defecto no es muy estricta y sería conveniente modificarla en el sentido de activar 

indicando el tiempo que durará el bloqueo y activar también 

Práctica

Descarga la versión free de Agnitum Outpost Firewall e instálalo.

Realiza una búsqueda en Google de páginas que te muestren información sobre Dante.

Configura el plug-in de bloqueo contenido para que impida la visualización de páginas en las que aparezca la palabra Dante.

Intenta visitar alguno de los enlaces que has obtenido como resultado de la búsqueda que has realizado.

Elimina la palabra Dante del listado de sitios bloqueados.

Conéctate a la edición digital de un diario o a alguno de los principales portales (terra, ya.com, wanadoo, tiscali, etc). Comprueba qué ocurre con algunos anuncios dependiendo de que el estado de plug-in de publicidad sea iniciado o detenido.

Spyware

¿Qué es?

Si has llegado hasta aquí directamente desde la sección de ftp, es posible que sientas una cierta inquietud, ya que te hemos derivado a una sección denominada "seguridad" y es probable que pienses que te acecha algún peligro.

Si tu llegada corresponde a una lectura más lineal, te recordamos que en el capítulo de ftp habíamos comentado la posibilidad de descargar una buena cantidad de programas de forma gratuita y que, algunos de ellos, a los que enmarcábamos dentro de la categoría denominada adware ofrecían las prestaciones de los versiones comerciales a base de reservar una parte de la pantalla para la presentación de anuncios publicitarios.

Aparentemente, el único compromiso que adquiere el usuario de uno de estos programas es permitir la aparición en su pantalla de publicidad cuya visita no es obligatoria. Pero, en muchos casos la realidad no es tan inocente como aparenta y, además de ese pequeño banner publicitario, se instala en el ordenador un programa que se encarga de monitorizar las páginas de Internet que se visitan y enviar esa información a empresas especializadas en el análisis de datos, siempre sin conocimiento por parte del usuario de que este hecho se está produciendo. Dichas empresas se encargan de ir afinando los perfiles de cada usuario para vender esos datos a las grandes corporaciones publicitarias y posibilitar la segmentación de la publicidad, de forma que los mensajes que nos vayan llegando se adecuen cada vez más al perfil que traslucimos a través de la navegación por la red.

Este tipo de programas espía se denominan en terminología anglosajona spyware y su introducción por esta vía es muy poco frecuente entre los programas de software libre ya que, al ser obligatoria la distribución junto con el código del programa, cualquier programador podría descubrirlos y modificarlos.

Otra forma de que se introduzcan espías en nuestro navegador es a través de la visita a páginas que incluyen en su código las instrucciones para almacenar en nuestro ordenador una "*cookie*". Estas "galletitas" son pequeños fragmentos de código, entre cuyas funciones puede estar la de determinar los intervalos entre una y otra visita, el número de veces que se visita la página, etc.

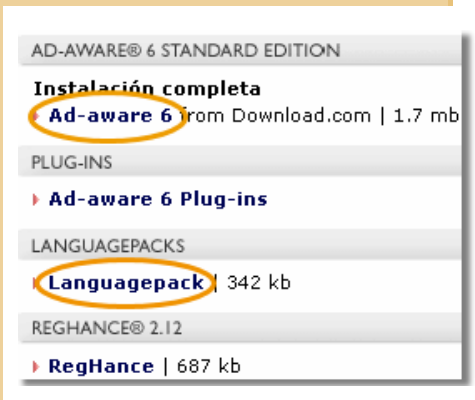
¿Como defenderse?

Si quieres defenderte de estos espías puedes utilizar algunos programas disponibles para descargar gratuitamente desde la red. Veremos el funcionamiento de As-aware.

No podemos incluir el programa en el CD porque la licencia prohíbe expresamente la distribución de los productos que se pueden descargar de la web

Práctica

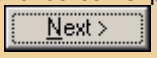
Conéctate a www.lavasoftusa.com. La web aparece en inglés pero puedes seleccionar el español utilizando las banderas que aparecen en la parte superior izquierda.



Selecciona el enlace Ad-aware (las versiones plus y profesional no son freeware)

Verás que aparecen varios componentes. Te recomendamos que descargues sólo aquellos que están marcados. El enlace de descarga te llevará a **c|net** que es uno de los más importantes sitios de descargas de programas y bastará con pulsar

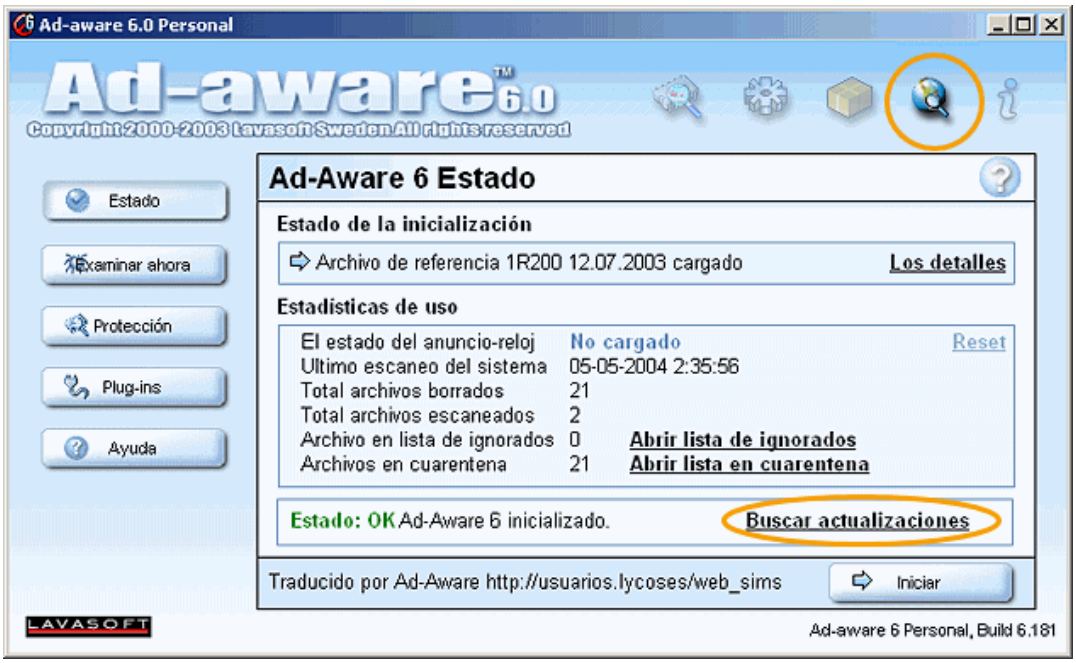
para que se inicie la descarga.

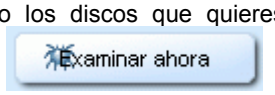
Instala, empezando por el programa propiamente dicho y, cuando hayas completado la instalación del mismo, continúa con el pack de lenguaje. En ambos casos la instalación puede reducirse a las pulsación del botón 

hasta que aparezca el botón 

, salvo un momento en la instalación del pack de lenguaje en el que sería conveniente desmarcar las traducciones suplementarias para no desperdiciar espacio en disco.

La ejecución del programa es muy intuitiva. Lo primero que deberías hacer cada vez que vayas a utilizarlo sería actualizar el archivo que contiene las referencias de los programas y sitios espías, para lo cual puedes utilizar cualquiera de las dos opciones que aparecen marcadas en la imagen.

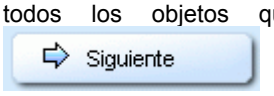


Puedes utilizar el botón  para modificar las preferencias, aunque encontrarás que algunas opciones están marcadas en gris puesto que sólo es posible habilitarlas cuando se utiliza alguna de las versiones comerciales. Una vez que hayas establecido los discos que quieres revisar y cualquier otro tipo de preferencia, puedes iniciar la revisión pulsando 

Cuando se complete el proceso aparecerá una pantalla resumen en la que se nos informa de los espías localizados.

Pulsando 

nos mostrará todas las referencias encontradas. Verás que la mayoría de ellas serán lo que el programa denomina "Tracking cookies", por lo que la forma más cómoda de seleccionarlas será pulsando con el botón derecho sobre cualquiera de ellas y eligiendo la opción correspondiente del menú que se despliega.

Cuando aparezcan otro tipo de espías, los que denomina "Archivo", puedes utilizar la primera opción del menú para ver la información disponible. Una vez que tengas marcados todos los objetos que deseas eliminar pulsa en 

y confirma la eliminación de los mismos.

Ten en cuenta que algunos programas pueden dejar de funcionar si se elimina el archivo espía que instalan. Por eso, si no tienes muy claro si te conviene eliminarlos o no, puedes

utilizar el botón 

de forma que la eliminación no sea absoluta. De todas maneras, si no has modificado la opción que el programa trae por defecto, siempre se creará un archivo de cuarentena de forma automática por lo que, si ves que algún programa deja de funcionar, puedes utilizar el icono  y restaurar los espías aunque, habiendo muchos programas con licencia GNU/GPL o freeware que pueden hacer funciones similares, te recomendamos que busques otro programa que pueda realizar las mismas funciones y abandones el que instaló un espía.

Práctica

Ejecuta Ad-aware para limpiar tu sistema de indeseables espías.

No olvides ejecutar la actualización del archivo de referencias antes de iniciar el proceso.