

## **ENLACES DE SEGURIDAD**

### **Tutorial ZONE ALARM.**

Uno de los cortafuegos o firewall con mayor difusión. La política de Zonelabs de gratuidad para el usuario particular y su eficacia, hacen de él una de las protecciones preferidas por muchos internautas.

#### **Características generales:**

Cortafuegos con capacidad de control del tráfico entrante y saliente, fácilmente configurable mediante su sistema de selección de niveles de seguridad para red local e Internet.

Posibilidad de control de los programas a los que permitimos el acceso a Internet, bien configurándolos permanentemente, bien mediante petición de autorización cada vez que un programa vaya a conectarse. Esto es ciertamente interesante, ya que siempre estaremos informados de las conexiones que establecen los programas, algo muy útil contra Troyanos, Spywares y algunos virus con componente troyano.

#### **Instalación:**

Podemos descargar la última versión del cortafuegos gratuita de su página oficial:

<http://www.zonelabs.com/>

Una vez descargado el archivo ejecutable, comenzaremos la instalación eligiendo el directorio deseado. Si queremos ver el proceso de instalación paso a paso, -----

> [Instalación](#)

### **El panel principal.**

Desde este panel realizaremos la configuración del firewall De una manera muy sencilla.

El panel principal cuenta con los siguientes elementos:



**Monitor de tráfico.** Nos indica gráficamente el tráfico de entrada y salida, mediante unas barras dinámicas , verde para la recepción, rojo para la transmisión. Esta información también se reproduce en la zona de inicio de barra de tareas.

### **Candado de bloqueo.**

El icono del candado permite bloquear o desbloquear el acceso de los programas a la red, según pulsemos sobre él adquirirá la condición de abierto o cerrado.

### **Botón de Stop.**

Permite cortar instantáneamente todo el tráfico con Internet. Es una medida extra de seguridad.

**Zona de representación de programas conectados.**

Aquí se representan mediante su icono correspondiente los programas que están conectados a la red.

**Acceso directo de ayuda.**

Nos direcciona a la página de ayuda de Zone Alarm en inglés.

**Botones de funciones:**

**ALERTS, LOCK, SECURITY, PROGRAMS y CONFIGURE**



los cuales a continuación detallaremos.

Bien, ya hemos efectuado la toma de contacto con el programa. Ahora veamos sus posibilidades de configuración.

**FUNCIONES:**

**Security.**

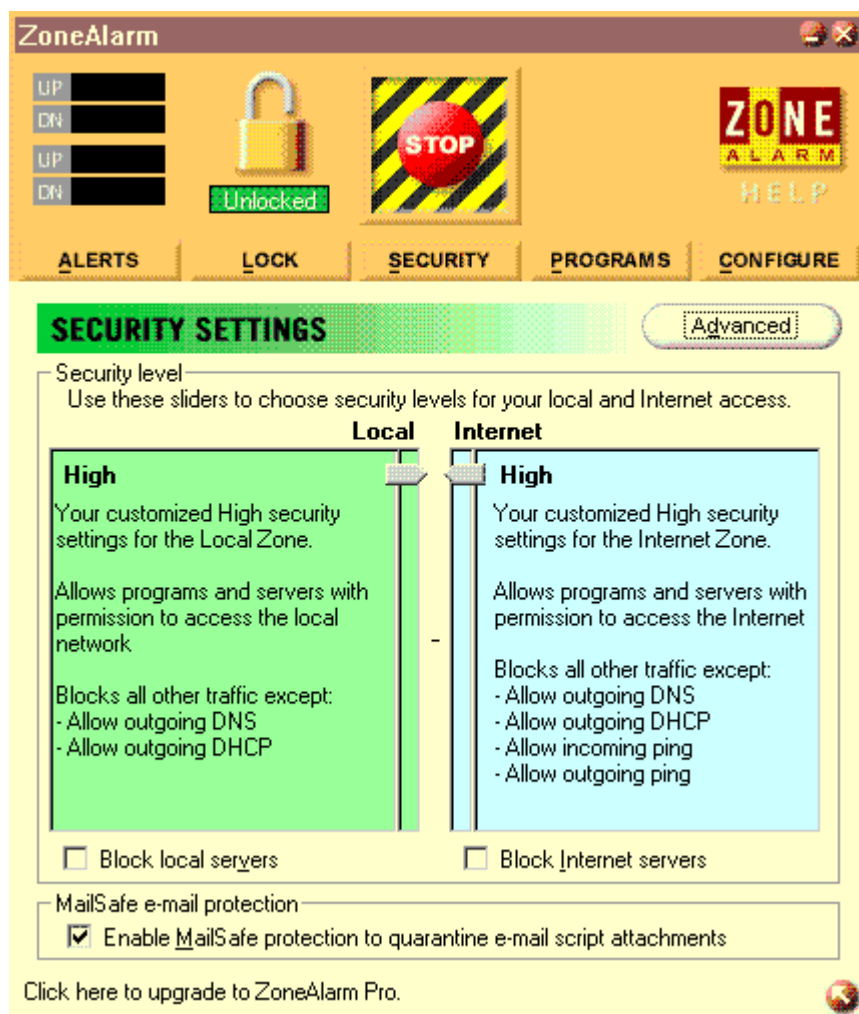
La primera configuración que realizaremos será seleccionar el nivel de seguridad del firewall. Tenemos posibilidad de asignar un nivel de seguridad distinto a cada una de las zonas que incorpora el firewall: La zona de Internet y la zona de red de área local (LAN)

Los niveles que vienen predeterminados son nivel "Medium" en la zona local y nivel "High" en la Zona de Internet.

Estos valores, que serían adecuados en la mayoría de los casos, no son los que vamos a elegir. Se ha dado el caso, en algunas versiones del cortafuegos, que el programa en ciertos casos muy concretos reconoce como locales algunas conexiones desde Internet, por lo que les aplica menor grado de seguridad. ver <http://www.securityfocus.com/archive/1/225205>

**ENLACES DE SEGURIDAD** recomienda mantener el nivel de las dos zonas en High (Alto). Usuarios conectados mediante LAN (Cable modem) deben tener especial interés en incrementar el nivel de la zona local a High.

En la zona de Internet el nivel de seguridad lo mantendremos siempre en High.



**Descripción de los niveles de seguridad. Estas características son aplicables a las dos zonas:**

**Alto.** Servicios de Windows bloqueados (Netbios), al igual que archivos e impresora. En este nivel, el cortafuegos abre automáticamente los puertos si el programa solicitante está previamente autorizado. El ordenador está en modo stealth (Sigilo) en el cual los puertos que no estén en utilización por programas autorizados se encuentran bloqueados y no son detectables en la zona de Internet. Nivel altamente recomendado.

**Medio.** Ordenador visible a la zona de Internet. Servicios de Windows bloqueados. Realización de la función de bloqueo automático. Nivel no recomendado.

**Bajo.** Ordenador en modo visible, NetBios no bloqueado... para que seguir, este nivel se desaconseja enérgicamente.

Las opciones avanzadas permiten mantener el nivel de seguridad en la zona local en "Alto", permitiendo agregar otros ordenadores y elevar el alcance de la zona local.

Es muy conveniente para los usuarios de cable módem dejar los subnets del cable deshabilitados.

La activación de la casilla "block local/Internet servers" situada debajo de cada zona impide la actuación de los programas como servidores para las zonas respectivas, impidiendo a las aplicaciones escuchar los puertos. Tendremos esto en cuenta, ya que si queremos ejecutar un servidor para Internet esta casilla deberá estar desactivada. Los programas como ICQ o Netmeeting requieren esta desactivación.

**"Mailsafe E-mail Protection."**

Al seleccionar esta casilla activaremos la capacidad del cortafuegos de interceptar scripts de Visual Basic, potencialmente peligrosos, en los correos recibidos, aislándolos antes de su ejecución.

Esta función se aplica a gestores de correo que utilicen protocolo POP3 e IMAP.

**Alerts.**

## **Internets alerts (Alarmas)**

Al expandir esta ventana obtenemos información sobre las alertas que ha reflejado el firewall, así como del tráfico de internet en nuestro ordenador. Esto último se refleja en la casilla "Today's summary".

En la casilla "Current Alerts" (Alertas actuales) visualizamos la última alerta, pulsando en la flecha correspondiente vemos la anterior y así sucesivamente.

Estas alertas nos informan de un intento de conexión por parte de un programa alojado en nuestro ordenador o de un intento de conexión exterior.

La información que refleja la alerta es la siguiente:

Fecha y hora.

Dirección IP de la fuente y puerto de acceso.

Dirección IP del destino y puerto de acceso.

Indicación del tipo de transporte TCP, UDP, ICMP, o IGMP

La opción "More Info" (Más información) posibilita ampliar la información sobre las causas de la alerta y sus riesgos, diseccionándonos a una página específica para ello de zoneLabs, (en inglés) donde incluso podemos efectuar un seguimiento mediante Whois o traceroute de la dirección IP entrante bloqueada.

Zone Labs AlertAnalyzer - Microsoft Internet Explorer

http://www.zonelabs.com/alerts/alertresult?record=ZLN14011779771055-1005/02#5386380ev3c

Zone Labs AlertAnalyzer™

Enter Host/URL:

**WHO'S PINGING YOU?**

cc:1000028-e2.3

**ZoneAlarm has blocked access to port 0 on your computer**

The ZoneAlarm firewall has successfully stopped local network or Internet traffic from reaching your computer. No breach in your security has occurred. **Your computer is safe.**

[What happened?](#)   [Should I be concerned?](#)   [What should I do?](#)   [Alert Summary](#)   [Technical Discussion](#)   [Related Links](#)

**What Happened?**

ZoneAlarm blocked data sent over the Internet to port 0 on your machine from port 0 on a remote computer whose IP address is 10.34.0.1. This communication attempt may have been a port scan, or simply one of the millions of unsolicited commercial or network control messages that are routinely sent out over the Internet. Such unsolicited messages are often called *Internet background noise*.

Zone Labs AlertAnalyzer - Microsoft Internet Explorer

http://www.zonelabs.com/alerts/alertresult?record=ZLN14011779771055-1005/02#5386380ev3c

**Should I be concerned?**

Because ZoneAlarm is hiding all the ports on your computer, the remote computer's attempt to communicate with your computer was unsuccessful. Your computer is safe.

**What should I do?**

There is no need to make any changes to your settings in ZoneAlarm unless the alerts are interfering with your ability to use the Internet or your network-aware software. If you are having problems, see the paragraphs below for a discussion of some of the more common reasons for alerts, and how you can minimize them.

**Alert Summary**

From	To
IP Address: 10.34.0.1	IP Address: 224.0.0.xxxx
Host Name: <a href="#">Who is this?</a> ZoneAlarm Pro feature	Host Name: <a href="#">Who is this?</a> ZoneAlarm Pro feature
Port: 0	Port: 0
Program:	File Name:

**Technical Discussion**

The rest of this page discusses some possible causes of this alert.

The connection attempt that caused this alert was probably harmless. The most likely scenarios are:

- The communication may have been a legitimate attempt by your ISP, a news server, a mail server, or other service provider to authenticate your IP address for the purpose of providing services you requested. ZoneAlarm usually allows authentication to take place, but this attempt may have come from a different computer than the one you originally contacted for services, possibly due to load balancing requirements in the provider organization.
- You may have set up a web site or some other service such as an e-mail, FTP, news server, or hosted game to provide services that require an Internet connection, without giving your web application server permission in ZoneAlarm. To give your application server permission, find the program that contains your web application in the Programs panel. On the box where this program is located, grant your web application the correct permission to act as a server. This will allow your web site to accept connection requests from the local network or the Internet, depending on which option you select.

**La página incluye una serie de explicaciones de las alertas más frecuentes y sus posibles causas, indicándonos si nuestro sistema permanece seguro o por el contrario existe alguna acción contra nuestra vulnerabilidad.**

### **"Alert settings"**

**En esta casilla podemos seleccionar un par de funciones relativas a los avisos de alerta que nos da el firewall.**

**Una opción que puede resultar interesante es la posibilidad de guardar en un fichero de texto la relación de las alarmas sucedidas, lo que posibilita su consulta y comparación posterior. Para ello activaremos la casilla "Log alerts to a text file".**



**Para que las alertas sean mostradas en una ventana independiente en el momento en que se produzcan, activaremos la casilla "Show the alert popup window".**

**Este sería el aviso de un bloqueo entrante:**

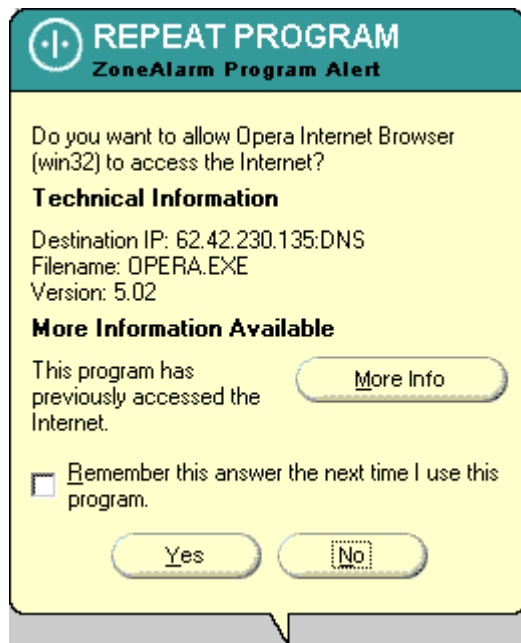


**Recordemos que no todos los bloqueos entrantes corresponden a ataques maliciosos, esto se oye con frecuencia en foros y consultas, puesto que es posible tener varias alertas de bloqueos entrantes el mismo día. Muchas veces las mismas empresas suministradoras de la conexión efectúan comprobaciones mediante el empleo de "Pings" los cuales no afectan a la integridad de nuestro sistema. Esta circunstancia es de fácil comprobación mediante el empleo de la opción "More Info" de la misma ventana de aviso, desde la que accederemos a la página de Whois de Zone Labs, como hemos visto anteriormente.**

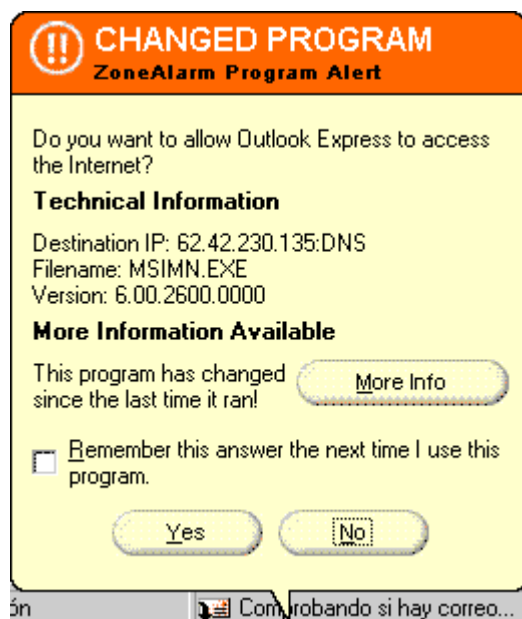
**Si los avisos supusieran un incordio, es posible impedir el aviso marcando la casilla "Don't show this dialog again" o deshabilitar la aparición de las ventanas emergentes desde la ventana "Alerts" desmarcando la casilla "Show the alert in popup window".**

**Esta es la ventana que solicita el permiso de conexión de un programa a la red. Si vamos a permitir el acceso del programa habitualmente, caso por ejemplo de los navegadores, podemos autorizar el acceso evitando ser consultados, para ello marcaremos la casilla "Remember This answer the next time I use this program". Esto también podemos hacerlo desde la ventana "programs", como más adelante**

veremos. De esta manera, es sencillo configurar el cortafuegos seleccionando casi por sí sólo los programas que tendrán libre acceso o por el contrario necesitarán de nuestra autorización para conectarse, o incluso los que estarán bloqueados .



En esta ventana en cambio, Zone Alarm nos da el aviso de un programa en el cual ha detectado un cambio desde la última vez que se ejecutó, el cual intenta conectarse a Internet. Si el programa no ha sido actualizado por nosotros significa que dicho cambio pudiera ser de origen malicioso. Esto es de gran utilidad en la detección de virus y troyanos.



## **LOCK (Bloqueo)**

**Este apartado se ocupa de configurar las posibilidades de bloqueo del cortafuegos.**

### **"Lock status"**

**Esta casilla refleja las condiciones de bloqueo de conexión en que se encuentra el cortafuegos. Su condición de abierto o cerrado varía según accionemos el icono del candado, abriéndolo o cerrándolo.**

### **"Automatic lock" (Bloqueo automático)**

**Seleccionando "enable" posibilitamos que el firewall bloquee la conexión cuando se active el protector de pantalla o tras cierto tiempo de inactividad.**

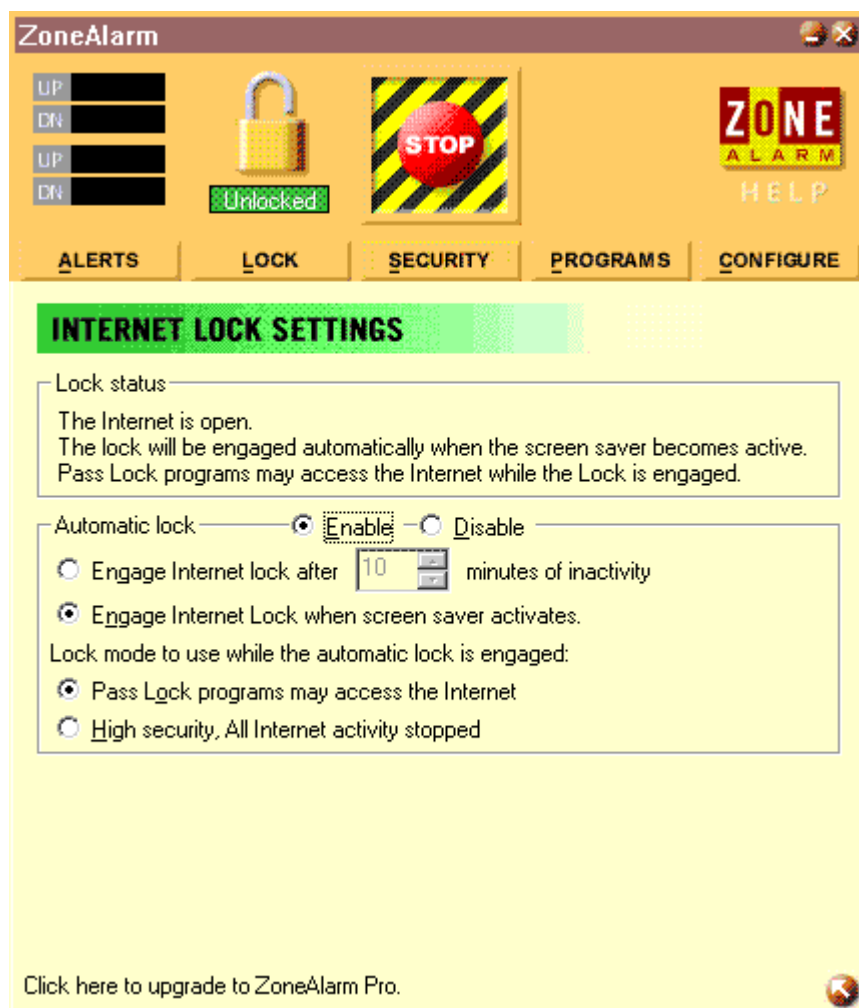
**Para seleccionar cualquiera de estas dos opciones, o ambas, activaremos las casillas:**

**"Engage internet lock after (aquí introduciremos los minutos de inactividad requeridos para activar el bloqueo) minutes of inactivity"**

**"Engage internet lock when screen saver activateds" para el protector de pantalla.**

**También podemos autorizar a un programa a acceder a la conexión pasando el bloqueo. Esto es útil para aplicaciones que necesitan conectar con periodicidad o permanentemente, como los gestores de correo. Para ello seleccionaremos la opción "Pass lock programs may access to internet".**

**Seleccionando, por contra, "Hig security, all internet activity stopped" detendremos toda la actividad en internet a todos los programas cuando el bloqueo automático se active.**



## Programs.

Cuando un programa se conecta a Internet por vez primera, estando activado el cortafuegos, será añadido en la relación de esta ventana, desde donde podremos elegir su nivel de autorización de acceso. Por defecto, todos los programas solicitan autorización para conectarse. Marcando la opción "Remember the answer each I use this program" podemos autorizar a ese programa en concreto a que acceda directamente sin previa consulta. Esto puede resultar práctico con algunos programas de frecuente utilización. Siempre tendremos la posibilidad de variar esto último en la ventana "Programs".

**V - La marca de comprobación verde** permite a un programa conectar siempre.

**X - El X rojo** Deniega el acceso a internet hasta que sea asignada la marca de comprobación o el signo de interrogación.

**? - El signo de interrogación.** Configuración por defecto. Alerta y solicita autorización cuando un programa intenta acceder a Internet.

Los programas no pueden tener mayores derechos de acceso a la zona Internet que a la zona local.

Para quitar un programa de la lista, iremos a la entrada del programa y seleccionaremos la opción de eliminar. Esto no impide que el cortafuegos vigile la aplicación, que será detectada la siguiente vez que intente acceder a la red.

También podemos cambiar los derechos de acceso a Internet de un programa usando el menú del botón derecho del ratón.

**"Allow conect"**

En esta columna podemos ver el estado de autorización de cada programa, en ambas zonas

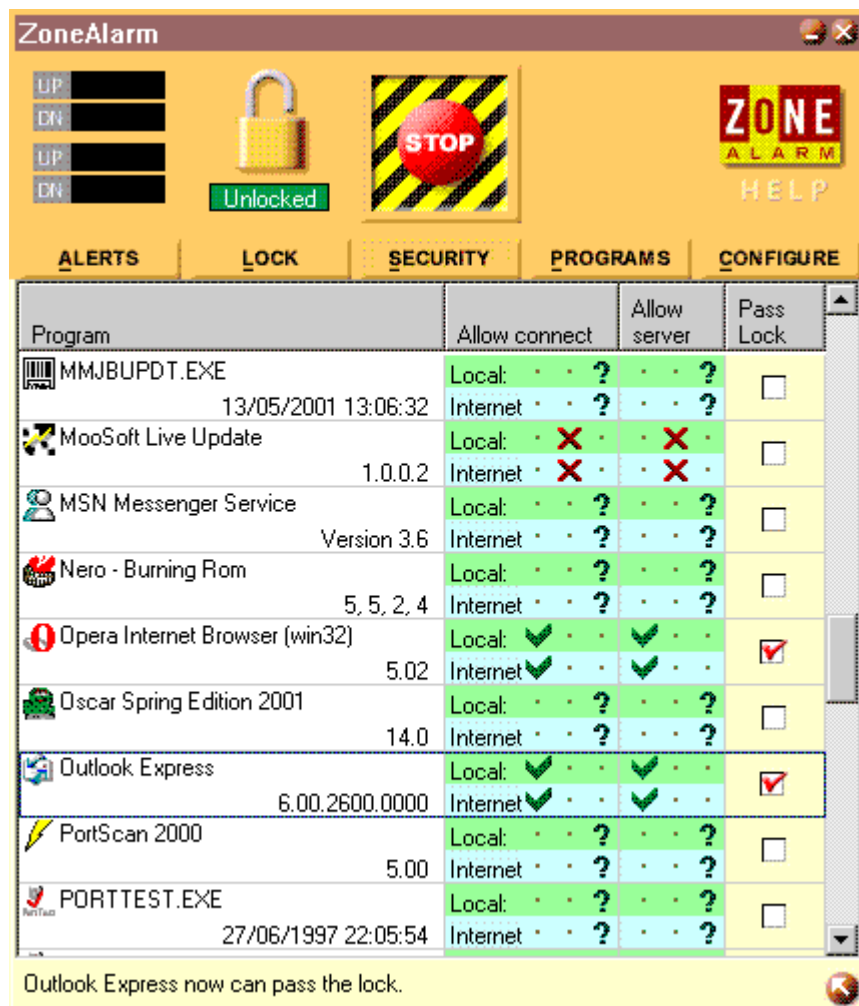
**"Allow server"**

Aquí podemos seleccionar si autorizamos o no a que un programa servidor de Internet pueda admitir peticiones del exterior. Si no marcamos nada tampoco tendrá acceso. Seleccionando los programas que puedan efectuar este tipo de

comunicación damos un paso importante en nuestra seguridad. Los programas troyanos son aplicaciones que responden a peticiones remotas, cualquier intento de respuesta no autorizada provocará el consiguiente aviso de alerta.

### "Pass Lock"

Marcando esta casilla autorizamos al programa a conectarse aunque hayamos activado la función "Lock" (Ver apartado con el mismo nombre).



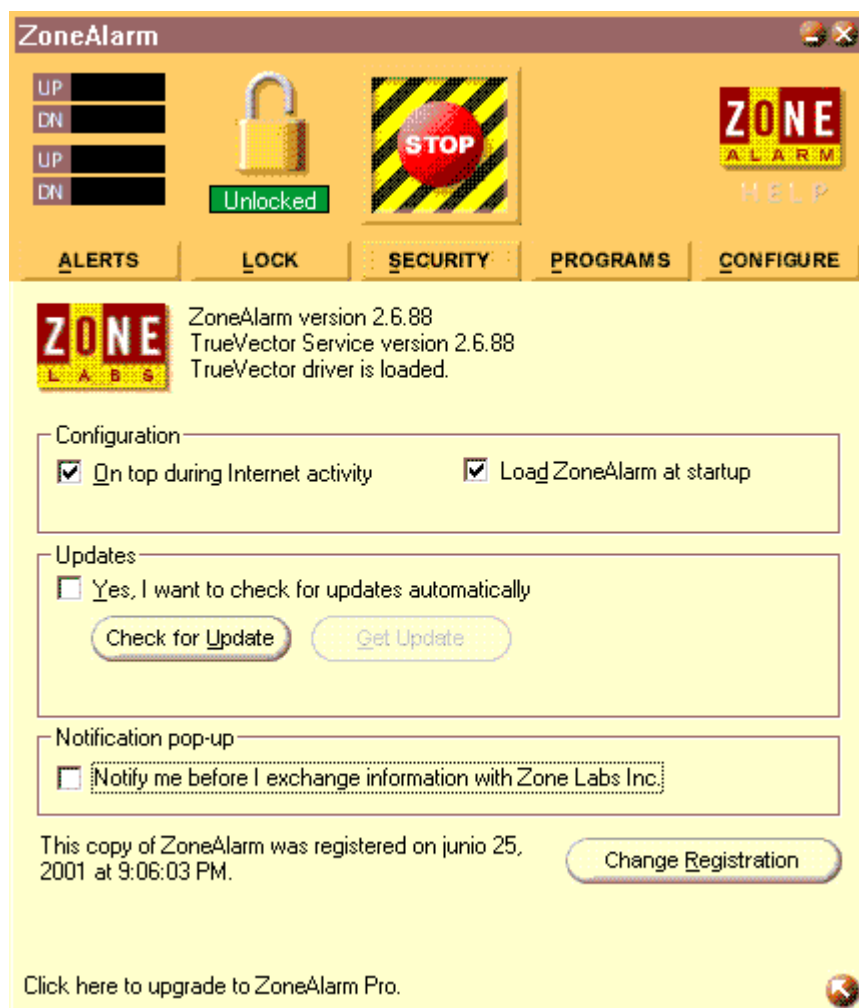
### "Configure".

## **Casilla "Configuración".**

**Aquí podemos seleccionar que el cortafuegos nos informe de cualquier actividad de nuestro ordenador en Internet, mediante los correspondientes mensajes de alerta. Para ello marcaremos " on top during internet activity ".**

**La opción "Load ZoneAlarm at startup", la cual viene seleccionada por defecto, provoca que el cortafuegos se inicie al arrancar el sistema, lo cual se recomienda. Al desactivarla, tendremos que ejecutar ZoneAlarm manualmente cada vez que necesitemos sus funciones.**

**Las opciones "updates " y "notificación pop-up" permiten recibir automáticamente información sobre nuevas versiones y productos de Zone Labs Inc. y no es necesaria su activación para el funcionamiento eficaz del programa.**



### **Conclusión:**

**Zone Alarm es un buen cortafuegos, de eficacia probada y garantizada, manejo sencillo y un nivel de posibilidades de configuración correcto. además, es gratuito. En definitiva, un compañero de navegación muy aconsejable.**