Materials de Formació

Manual del Zonealarm 2.6

Antoni Morante Milla

Juliol de 2001

GOVERN DE LES ILLES BALEARS
Conselleria d'Educació i Cultura
Direcció General d'Ordenació i Innovació

Manual del Zonealarm 2.6

Servei de Formació Permanent del Professorat
Direcció General d'Ordenació i Innovació
Conselleria d'Educació i Cultura

Juliol de 2001

1. SEGURETAT I ORDINADORS

Els mitjans de comunicació informen cada cop més freqüentment de problemes relacionats amb atacs a ordinadors, individuals o d'empreses, fent ús de les possibilitats que dóna Internet: virus a través del correu electrònic, atacs a llocs comercials, robatori de dades confidencials de servidors d'Internet, intents de sabotatge de llocs oficials, etc. El problema és especialment greu per als ordinadors que es connecten a Internet a través d'una línia d'alta velocitat (XDSI, ADSL, etc.) i que romanen molt de temps connectats (per exemple, els servidors web, però també les estacions de treball individual connectades a través d'una xarxa local corporativa o amb una tarifa plana). Quan més temps passi connectat a Internet l'ordinador, major és el risc que algú vulgui "colar-se" amb males intencions.

És evident que la primera regla bàsica per augmentar -que no garantir- la seguretat d'aquests equipaments és disposar almanco d'un antivirus (millor si és més d'un) degudament actualitzat, tot i que això no basta, i en el cas d'ordinadors que passen moltes hores connectats a Internet, o que ofereixen serveis accessibles des de l'exterior (servidors Web o FTP) o fan servir programari de connexió remota (Telnet, Laplink, etc.) cal instal·lar una protecció específica, anomenada *tallafocs.*

2. TALLAFOCS

En els edificis, un tallafocs és una barrera per evitar que el foc s'escampi. Els punts febles d'aquesta barrera són les portes, perquè és necessari que la gent pugui entrar i sortir. En termes informàtics, un *tallafocs* és una barrera entre un ordinador i el món exterior. També és més vulnerable en les seves portes, anomenades *ports*, perquè sense aquests *ports* l'ordinador no pot establir cap connexió a Internet (els serveis WWW, correu electrònic, FTP, etc., utilitzen diversos ports de connexió per a la transferència de dades).

El *tallafocs* protegeix els ports de l'ordinador que es connecta a Internet i bloqueja tot el tràfic que entra i surt en funció de les instruccions donades per l'usuari.

Funcions més habituals d'un tallafocs

- Protegir el sistema de l'accés no autoritzat a través d'Internet.
- Advertir dels intents d'intrusió i mantenir un arxiu d'enregistrament (*log*) per a seguir les seves pistes.
- Protecció parcial per als virus que arriben a través del correu electrònic. En matèria de virus, el tallafocs s'ha de combinar amb un bon antivirus (o més d'un) degudament actualitzat.
- Bloqueig dels continguts potencialment perillosos d'Internet: applets de Java, controls ActiveX, cookies, etc.
- Bloqueig del tràfic d'Internet mentre no treballam amb l'ordinador o mentre no utilitzam Internet (es pot activar aquesta opció automàticament amb el protector de pantalla o després d'un període d'inactivitat).
- Decidir quins programes es poden connectar a Internet i quins no, per evitar l'actuació dels anomenats *troians*[1]. Per exemple, pot fer que només es pugui connectar a Internet el programa de correu electrònic i el navegador web, però no el programa d'FTP o el deTelnet.

Quin tallafocs hem d'instal·lar?

Això dependrà de les necessitats de seguretat, perquè no és el mateix un tallafocs per al PC d'un usuari individual que per a la intranet d'un banc. Per a un usuari individual o per a protegir una xarxa d'àrea local d'un centre educatiu hi ha diverses opcions d'entre els anomenats *tallafocs personals* (Mcafee Personal Firewall, BlackICE Defender, Norton Personal Firewall, Zonealarm,...) que van desde la gratuïtat total fins a les 10.000 ptes. aproximadament. Sens dubte d'entre tots aquests el més adequat és el **Zonealarm**, ja que combina bones prestacions amb la característica de ser gratuït per a usuaris individuals i organitzacions sense ànim de lucre.

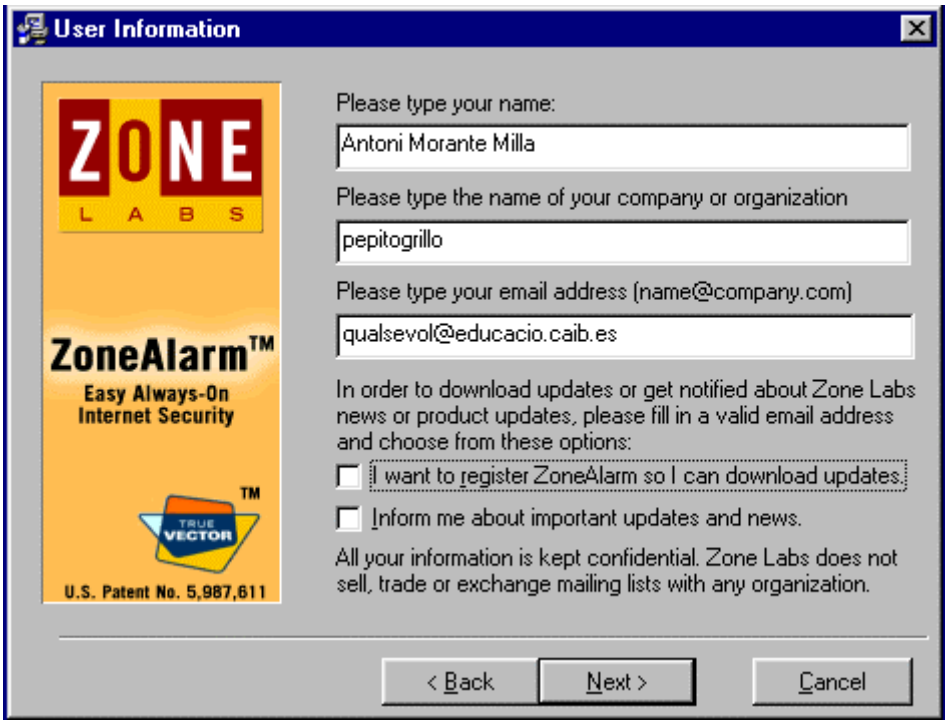
1 Un troià és un programa que s'introdueix inadvertidament a l'ordinador de l'usuari amb l'objectiu d'executar programes remotament sense coneixement del propietari de l'ordinador, instal·lar virus, robar informació confidencial, enviar correu electrònic massivament, etc. Per a més informació sobre aquests programes maliciosos, podeu consultar l'adreça: http://www.textolandia.org.ar/txt/newbie/queesuntroyano.html

El tallafocs “Zonealarm”

Instal·lació

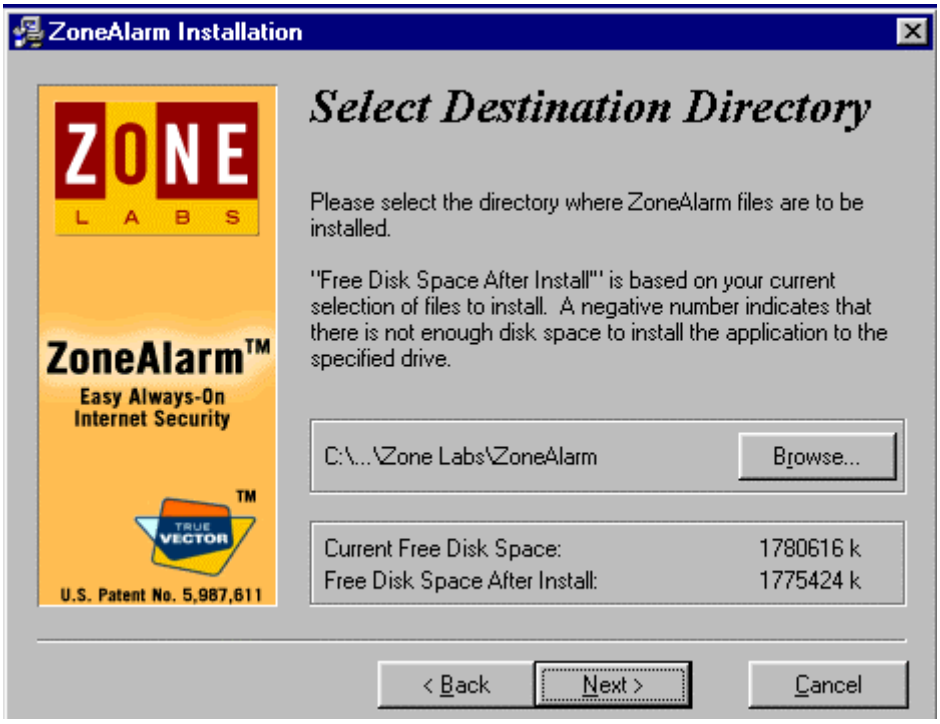
Per a instal·lar el **Zonealarm** heu de descarregar l’arxiu **Zonalm6.exe**, que trobareu a la secció de **Programari** del CD-ROM de materials de formació o a la web del fabricant (http://www.zonelabs.com) i guardar-lo a qualsevol carpeta del vostre disc dur (per exemple, a **l’Escriptori**).

A continuació heu de fer doble clic a sobre d’aquest arxiu i s’iniciarà el procés d’instal·lació. Podeu passar les dues primeres pantalles de presentació del programa fent clic a **Next** i després un altre cop a **Next**. A la tercera pantalla el programa us sol·licitarà el vostre nom i llinatges, l’organització a què pertanyeu i l’adreça de correu electrònic:



També us ofereix la possibilitat de deixar marcades les caselles “**I want to register ZoneAlarm so I can download updates**” i “**Inform me about important updates and news**” per a rebre actualitzacions automàticament i informació sobre novetats del programari. Podeu desmarcar-les si voleu.

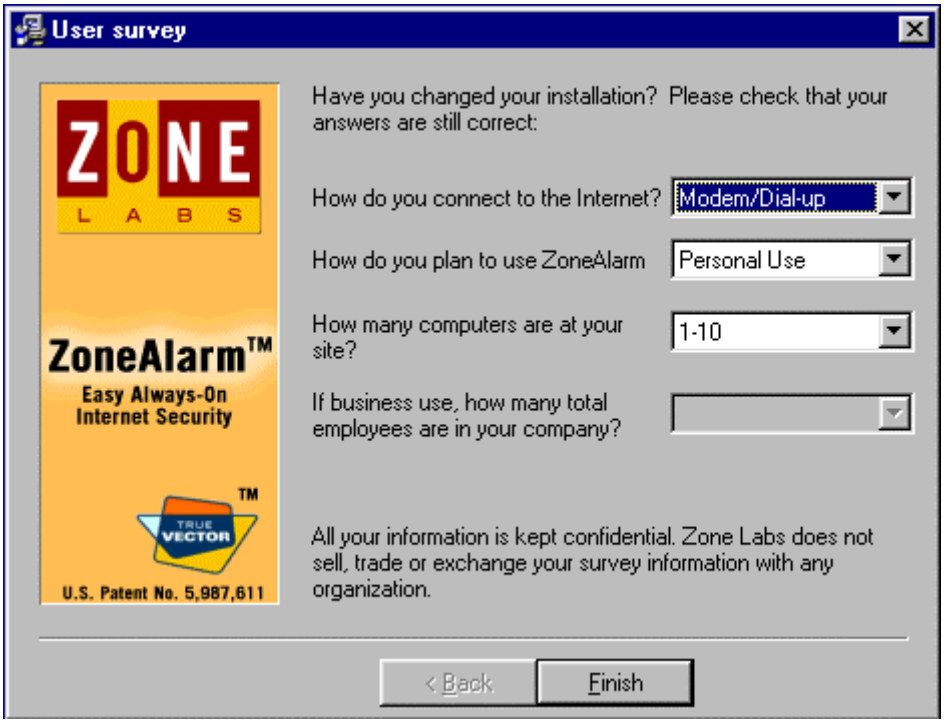
A continuació heu de fer clic a **Next** i apareixerà una finestra amb el contracte de llicència (**License Agreement**), que podeu llegir si us interessa especialment. A aquesta finestra heu de fer clic al botó **Accept** per passar a la finestra següent, on podreu canviar la carpeta on s’instal·larà el programa al vostre ordinador o deixar la que us proposa el programa:



Després feis clic a **Next** i a la finestra que apareix podeu deixar marcada la casella que farà que el programa detecti automàticament el navegador per defecte que utilitzau amb Internet i permeti que es connecti:

Convé que deixeu marcada aquesta casella i feis clic a **Next** per passar a la finestra **Ready to Install!** on podreu fer clic a **Next** per a començar la instal·lació.

A continuació apareixerà la finestra **User survey** on haureu de seleccionar les opcions corresponents al mètode que feis servir per connectar-vos a Internet amb ordinador (modem, ADSL, XDSI, etc.), quin ús pensau donar a **Zonealarm** (personal -**Personal use-** o per al centre educatiu -**Educational use**-) i el nombre d'ordinadors que hi ha al lloc on s'instal·la el programari:



Seleccionau les opcions adients i feis clic a **Finish** per a finalitzar el procés d'instal·lació. A continuació el programa us informarà que la instal·lació s'ha completat i si el voleu iniciar en aquest moment. Podeu fer clic a **Yes** i apareixerà un petit tutorial en anglès que podeu saltar-vos fent clic a **Cancel**.

A la finestra **Zonealarm tips** (consells de Zonealarm) que apareix a continuació, podeu fer clic a **OK** (si no voleu que torni a aparèixer aquesta finestra ho podeu indicar marcant la casella corresponent) i el programa quedarà instal·lat i observareu que apareix la seva icona a la barra de tasques de l'Escriptori:

i que apareix també la barra d'eines del programa, on podreu definir les seves característiques de funcionament:

Podeu activar aquesta barra d'eines en qualsevol moment fent doble clic a la icona de la barra de tasques de l'Escriptori o fent clic amb el botó dret a un lloc lliure de la barra de tasques, i a continuació, clic a **Barras de herramientas** i **ZoneAlarm Desk Band**:

A partir d'ara, el programa es posarà en marxa automàticament en arrencar l'ordinador i vigilarà qualsevol activitat relacionada amb la vostra connexió a internet, proporcionant un elevat nivell de seguretat que farà, entre d'altres coses, que el vostre ordinador sigui "invisible" per als "hackers" i intrusos. Podreu configurar molt fàcilment els nivells de seguretat que volgueu i haureu de donar permisos als programes instal·lats al vostre ordinador per a què puguin connectar-se a Internet. Això us garanteix que un programa maliciós (un *troià*) no capturi furtivament les vostres dades (per exemple contrasenyes o nombre de targeta de crèdit) i les enviï a un altre ordinador.

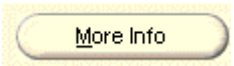
Configuració i característiques de funcionament

ZoneAlarm disposa de cinc eines de configuració: el panell d'avisos (**Alerts**), el panell de bloqueig (**Lock**), el panell de seguretat (**Security**) el panell de programes (**Programs**) o el panell de configuració (**Configure**). Cadascun d'ells es pot desplegar fent clic al botó corresponent de la barra d'eines del programa.

El panell d'avisos

Permet definir com volem que el programa ens avisi de la seva activitat coma tallafocs i de les incidències que es produeixin. Es recomana marcar l'opció de gravar els avisos en un fitxer de text **(Log alerts to a text file**) que podrem revisar posteriorment, però no la que fa que s'obri una finestra avisant cada cop que es produeix un avís (**Show the alert pop up window**), degut al relativament elevat nombre de falses alarmes que es produeixen, fet que pot fer la nostra activitat amb internet bastant incòmode.

Podeu obtenir més informació sobre un avís concret amb el botó:

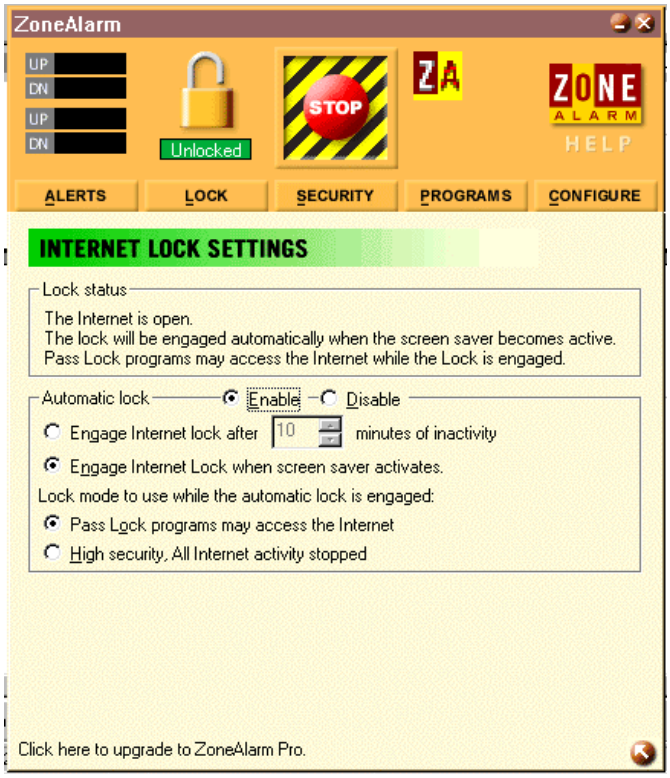


i podeu anar visualitzant cadascun dels avisos que s'han produït amb els botons:

L'arxiu de registre pot ser suprimit quan sigui massa gran (es pot veure el tamany al costat del nom) amb el botó **Delete Log**.

Podeu tornar la barra d'eines a les seves mides originals amb el botó  i minimitzar o tancar la barra d'eines amb els botons de la part superior: 

El panell de bloqueig



Es poden desplegar les seves opcions amb el botó **LOCK** i permet a l'usuari aturar de manera automàtica el tràfic amb Internet, marcant la casella **Enable**. Es pot optar per aturar el tràfic després d'un període d'inactivitat (**Engage Internet lock after .... minutes of inactivity**) o quan s'activa el protector de pantalla (**Engage Internet lock when screen saver activates**).

L'usuari pot activar també la casella **Pass Lock programs may access the Internet**, que permet a determinats programes autoritzats per l'usuari (per exemple, el client de correu electrònic) botar-se el bloqueig. Si s'activa la casella **High security, All Internet activity stopped**, cap programa podrà connectar-se a Internet.

El bloqueig pot ser també activat immediatament de forma manual fent clic a la icona: 

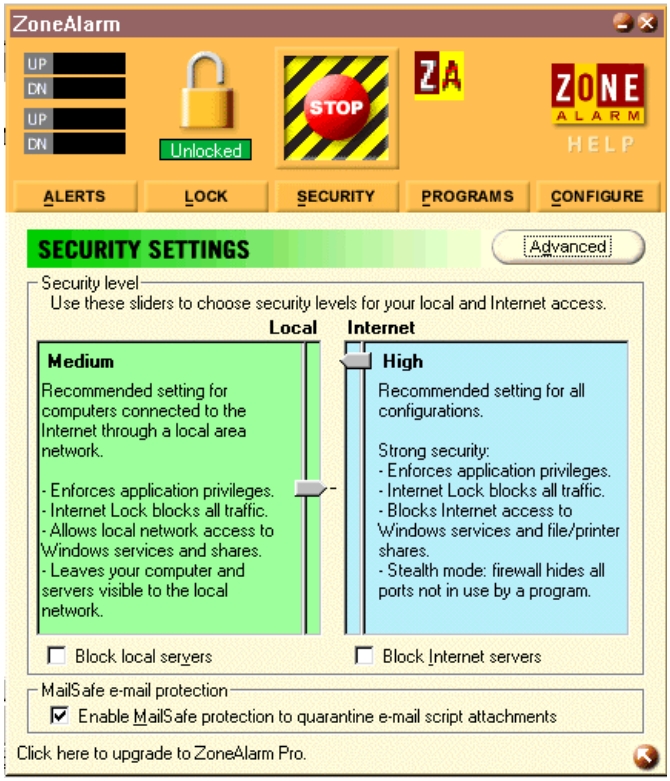
, que aleshores es transformarà en aquesta: 

.

En cas d'emergència (per exemple, si pensau que un programa pot estar fent servir Internet incorrectament) es pot aturar completament tot el tràfic amb Internet, inclosos els programes autoritzats a botar-se el bloqueig, amb la icona: 

. Per a desactivar l'aturada caldrà pitjar de nou a sobre de la mateixa icona.

El **Panell de seguretat**

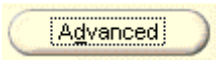


Permet veure i definir els permisos de seguretat de les zones **Local** (ordinadors connectats al nostre mitjançant una xarxa d'àrea local o considerats segurs per l'usuari) i d'**Internet** (qualsevol ordinador no inclòs a la zona **Local**), així com activar l'opció **MailSafe**, que intercepta missatges de correu electrònic amb *scripts* (petits programes) en Visual Basic que poden ser virus com el "Love Letter " o el "Funny joke", i requereix autorització explícita de l'usuari abans que aquests *scripts* puguin ser executats. **ZoneAlarm MailSafe** no esborra els virus, sinó que protegeix el PC identificant i donant l'opció de cancel·lar l'escriptura abans que s'executi. Aquesta casella, que es troba a la part inferior de la finestra, s'hauria de mantenir sempre activada. Es recomana mantenir les opcions de seguretat per defecte del programa, que poden veure's a la imatge de la dreta.

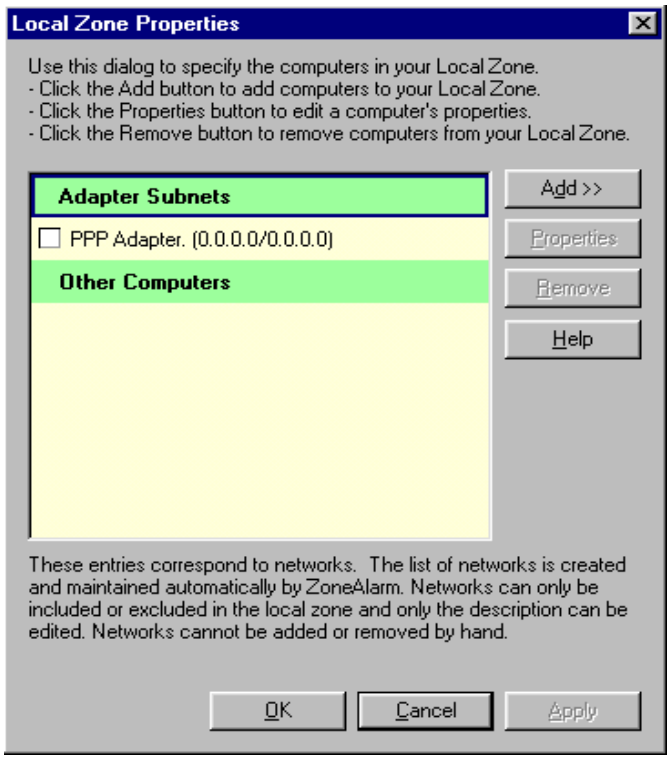
A més, no oblideu que sempre s'ha de fer servir un antivirus actualitzat i tractar el correu electrònic rebut amb molta precaució.

El nivell de seguretat de la zona **Internet** ha de ser sempre **igual o més alt** que el nivell seleccionat per a la zona **Local**. Si manteniu alt **(High)** el nivell de seguretat per a la zona d'**Internet**, **ZoneAlarm** ocultarà tots els ports que no s'utilitzin en cada moment de manera que el vostre ordinador no respondrà a les peticions que es facin sobre aquests ports, i monitoritzarà les peticions i registrarà la seva procedència.

Les caselles de la part inferior de la pantalla permeten a l'usuari impedir que qualsevol programa de la zona **Local** -**Block local servers**- o de la zona **Internet** -**Block Internet servers**- actuï com a servidor i per exemple enviï informació confidencial a un "hacker". Això pot provocar problemes amb algunes aplicacions de xat o de compartició de fitxers com **Napster**. No obstant això, es recomana marcar aquestes caselles.

El botó **Advanced**: 

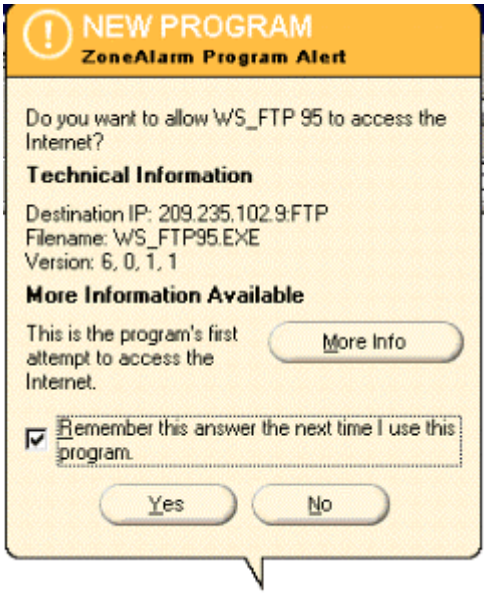
permet definir les propietats de la zona **Local**, designant computadors o subxarxes que s'inclouran en aquesta zona. Per a afegir una subxarxa local, marcau la casella que hi ha a l'esquerra de l'adaptador de xarxa Ethernet o del mòdem connectat a l'esmentada xarxa, però no afegiu xarxes connectades via mòdem ADSL o cable mòdem. També es poden afegir a la nostra zona local ordinadors remots connectats a Internet fent clic en el botó **Add>>** i seleccionant una direcció o conjunt de direccions IP, o un domini (com per exemple http://www.zonelabs.com).



Si l'ordinador està inclòs en una subxarxa d'una xarxa corporativa més gran, **ZoneAlarm** no reconeixerà les subxarxes que no s'hagin seleccionat com a parts de la zona **Local**. Això pot ser un problema si hi ha recursos que es troben en una subxarxa distinta, per exemple impressores de xarxa, que caldrà afegir a la zona **Local**.

El Panell de Programes

El panell de programes es desplega fent clic a **PROGRAMS** de la barra d'eines i mostra el llistat dels programes que ZoneAlarm ha detectat que intenten connectar-se a Internet. Cada aplicació té una sèrie d'autoritzacions per a la connexió local o a Internet, per actuar com a servidor i per saltar-se el bloqueig. **ZoneAlarm** avisarà a l'usuari quan detecti **per primer cop** que una aplicació vol connectar-se a la xarxa:



Si marcau **Sí (Yes)** permetreu que el programa es connecti a Internet. Si marcau l'opció **"Remember the answer each time I use this program"** i feis clic a **Yes,** el tallafocs **ZoneAlarm** no us tornarà a demanar autorització en el futur, quan aquest programa intenti connectar-se a Internet. Sempre es poden corregir aquests permisos en el **Panell de Programes**:

Davall de la columna **Program** trobareu el nom del programa i la seva versió. Si posau el cursor a sobre del nom del programa podreu veure detalls com: nom i ubicació del fitxer utilitzat per a la connexió a Internet, data de creació, tamany de l'arxiu, etc.

La columna **Allow Connect** mostra les opcions de connexió de cada programa, tant a la zona local com a Internet. Aquestes opcions poden ser modificades per l'usuari en qualsevol moment:

- **La icona verda** permet que el programa es connecti sempre amb Internet i amb la zona local.
- **La X vermella** impossibilita l'accés del programa a Internet fins que l'usuari la canviï a o a .
- **El signe d'interrogació** és l'opció per defecte i significa que ZoneAlarm demanarà permís a l'usuari cada cop que el programa en qüestió intenti connectar-se a Internet.

La columna **Allow Server** permet fer que un programa instal·lat en l'ordinador actuï com a servidor. Pot ser necessari permetre que alguns programes tenguin aquesta possibilitat (per exemple **ICQ**, **Netmeeting** o aplicacions tipus **Napster**, que han de possibilitar que altres usuaris accedeixin als arxius del nostre ordinador), però s'ha de tenir en compte que aquest és també el mode de funcionament dels anomenats **troians**, que són programes que s'instal·len furtivament en l'ordinador d'un usuari i permeten que els "hackers" el controlin remotament.

Si es marca la casella de la columna **Pass Lock**, es permetrà que el programa en qüestió es boti el **bloqueig automàtic**. Pot interessar activar aquesta opció per exemple per al programa de correu electrònic, per rebre el correu nou que vagi arribant mentre l'accés a Internet està bloquejat. Aquesta opció quedarà deshabilitada si pitjam el bloqueig manual d'emergència.

Per a eliminar programes d'aquest llistat és suficient fer clic a sobre del seu nom amb el botó dret del ratolí i al menú emergent triar **Remove "nom del programa"**

El **Panell de configuració** s'activa fent clic al botó **CONFIGURE** de la barra d'eines i permet registrar el programa, cercar actualitzacions automàticament, activar l'opció recomanada de carregar **ZoneAlarm** quan s'encén l'ordinador (**Load ZoneAlarm at startup**), etc.