Zone Alarm

MCours.com

1 Préambule

Ce document présente l'installation et la configuration du firewall ZoneAlarm sur un poste Windows 9X. La dernière version de ce document est téléchargeable à l'URL http://funix.free.fr. Ce document peut être reproduit et distribué librement dès lors qu'il n'est pas modifié et qu'il soit toujours fait mention de son origine et de son auteur, si vous avez l'intention de le modifier ou d'y apporter des rajouts, contactez l'auteur pour en faire profiter tout le monde. Ce document ne peut pas être utilisé dans un but commercial sans le consentement de son auteur. Ce document vous est fourni "dans l'état" sans aucune garantie de toute sorte, l'auteur ne saurait être tenu responsable des quelconques misères qui pourraient vous arriver lors des manipulations décrites dans ce document.

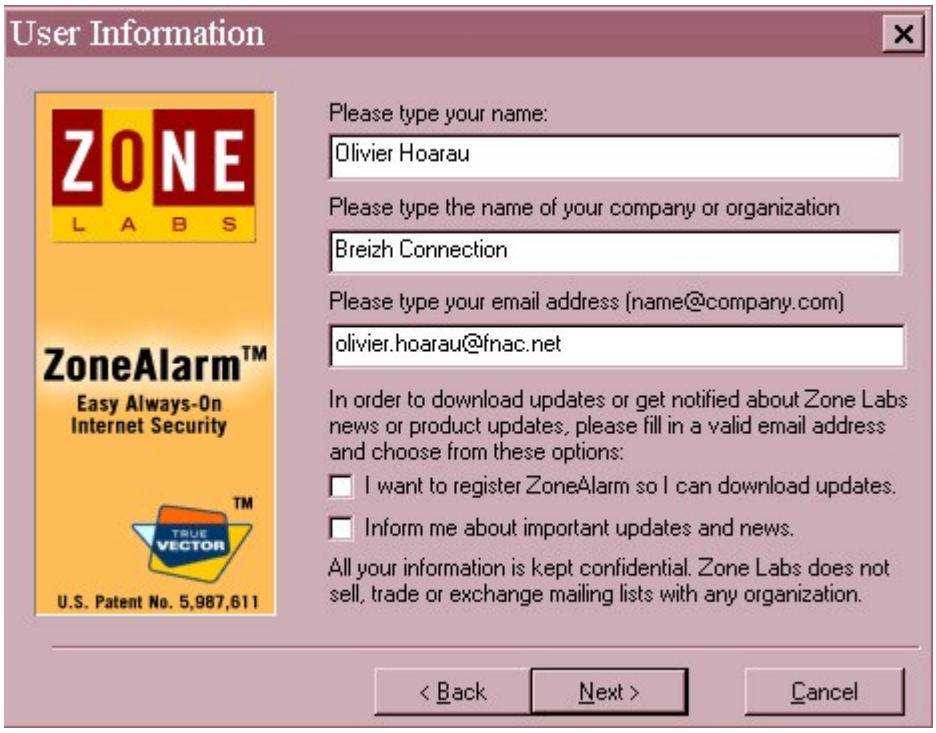
2 Présentation

ZoneAlarm est un Firewall fonctionnant sous windows, c'est à dire qu'il vous avertit des tentatives d'intrusion sur votre poste quand vous êtes connectés à internet mais peux aussi suivant sa configuration les bloquer automatiquement. **ZoneAlarm** est un freeware pour une utilisateur perso, par contre pour une utilisation dans le cadre du boulot au bout de 60 jours il faudra s'acquitter du prix d'une licence. Vous pouvez le

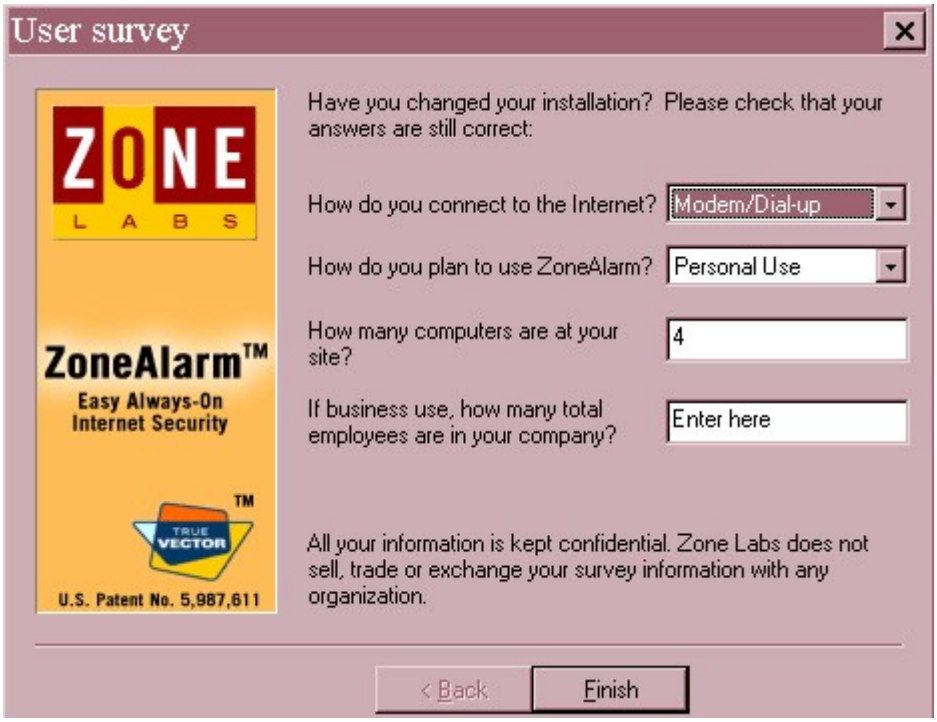
récupérer à l'URL www.zonelabs.com.
Pour la suite de la page, on appelera **idefix** (192.168.13.10) le poste où est installé **ZoneAlarm** et **obelix** (192.168.13.11) un autre poste de votre réseau local.

3 Installation

Pour installer **ZoneAlarm**, il faut exécuter l'archive récupérée sur le site **zone-alarme21.exe**, une fenêtre de bienvenue (**Welcome**) doit apparaître, cliquez sur **Next**, une autre fenêtre **Important Information !** apparaît avec pas mal d'infos sur **ZoneAlarm**, il est intéressant de prendre le temps de les lire, vous pouvez noter aussi le numéro précis de la version à savoir la 2.1.25. Quand vous avez tout lu, cliquez sur **Next**. La fenêtre **User Information** apparaît, vous devez y saisir des infos sur vous, vous pouvez éventuellement cocher la case **I want to register ZoneAlarm so I can download update** pour pouvoir récupérer les mises à jour de **ZoneAlarm** sur le site de **zonelabs** (ou plutôt être mis au courant des mises à jour). Si vous voulez recevoir des news sur **ZoneAlarm** cliquez la case correspondante.



Ensuite apparaît la fenêtre de licence **License Agreement**, vous pouvez y lire notamment, que c'est gratuit pour une utilisation perso, ou alors pour les organisations à but non lucratifs, cela exclue néanmoins toutes les organisations gouvernementales et tout le secteur éducatif. Dans le cadre d'une utilisation perso, on a le droit de l'installer que sur un seul ordinateur. Pour les organisations à but lucratif, les organisations gouvernementales, le milieu éducatif, le produit est gratuit pendant 60 jours, passé ce délai il faudra payer la licence. Cliquez sur **Accept** quand vous avez lu ou pas les termes de la licence.
Vous devez à présent sélectionner le répertoire de destination de **ZoneAlarm**, qui est par défaut **c:\Program Files\Zone Labs\ZoneAlarm**, changez en cliquant sur **Browse** si ça ne vous convient pas. Cliquez sur **Next** ensuite.
La fenêtre **Ready to Install** (prêt à être installé) apparaît, vous pouvez cliquer pour terminer sur **Next**. Suit l'installation des fichiers proprement dite sur votre disque dur.
La fenêtre **User survey** apparaît, elle permet de définir votre type de connexion.



Dans le champ **How do you connect to the Internet** vous devez indiquer comment vous vous connectez à Internet, vous avez le choix avec:

- **Modem/Dial-up** connexion avec modem (ligne téléphonique classique)
- **DSL** (ADSL)
- **ISDN** (Numéris)
- **Cable modem** (comme son nom l'indique)
- **T1/LAN** (ligne spécialisée numérique et réseau local)
- **Other** (autre)

Je ne pense pas que ce soit capital pour le bon fonctionnement de **ZoneAlarm**. De même que les champs suivants:

- **How do you plan to use ZoneAlarm?** C'est à dire Vous vous servez de **ZoneAlarm** pour... avec le choix: utilisation perso (**Personal Use**) ou pour le boulot (**Business Use**), j'ai choisi **Personal Use**
- **How many computers are at your site ?** Nombre de postes sur votre réseau perso.
- **If business use, how many total employees are in your company ?** Pour une utilisation perso, vous pouvez ignorer cela sans remord.

La fenêtre **Installation Completed !** (installation terminée) apparaît, on peut y relever que **ZoneAlarm** va se lancer automatiquement au prochain lancement de Windows. Une petite fenêtre apparaît disant qu'il faut rebootez la machine, cliquez sur OK.

4 Configuration de ZoneAlarm

4.1 Présentation

ZoneAlarm divise le monde en deux zones, la zone locale et la zone Internet. La zone locale est constituée de machines "amis", par contre la zone internet est consistuée de machines dont il faut se méfier. Concrètement la zone locale est votre réseau local, vous pouvez cependant

rajouter des machines se trouvant sur internet.
La première fois que **ZoneAlarm** est lancé, une fenêtre **ZoneAlarm** tips (astuces de **ZoneAlarm**) apparaît, si vous voulez que ça soit ainsi à chaque lancement de windows ne faites rien dans le cas contraire cochez la case **Don't show this message again**, noter bien que toutes ces astuces sont aussi accessibles dans la doc fournie avec **ZoneAlarm**.

Notez en bas à droite dans la barre de tâche une nouvelle icône 

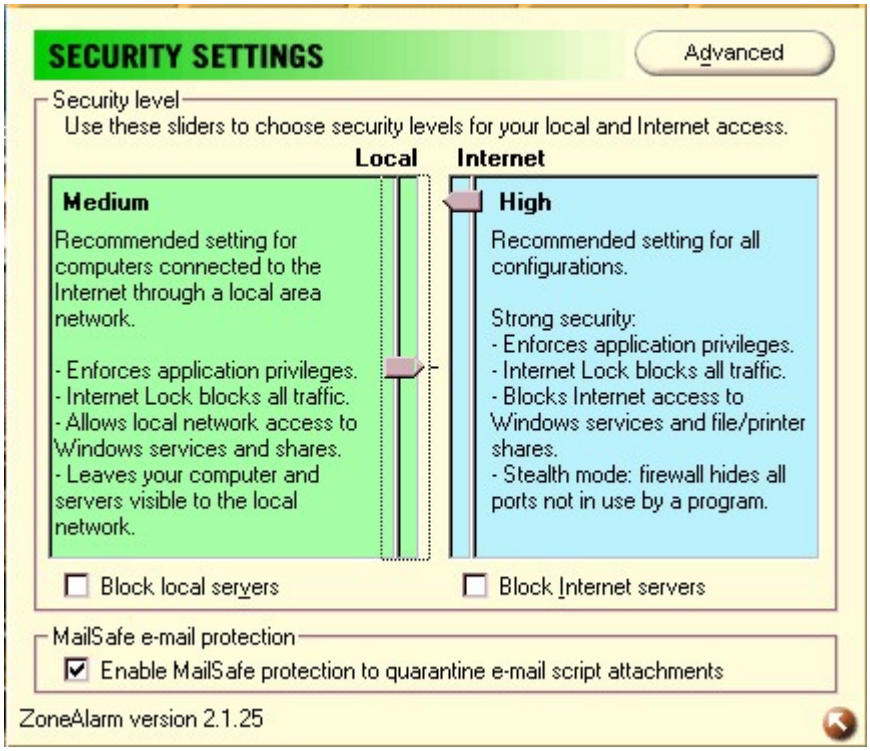
(sur le screenshot deuxième icône en partant de la droite). Pour faire apparaître la fenêtre de propriétés, cliquez avec le bouton droit de la souris sur cette icône, un menu apparaît, choisissez **Restore ZoneAlarm Control Center**.

De gauche à droite:

- les champs **UP** et **DN** sont des indicateurs de trafic de données sur internet (**UP** pour le trafic de votre poste vers internet (montant), et **DW** pour down pour le trafic venant d'internet vers votre poste(descendant)), si vous n'êtes pas connecté à Internet les champs sont tels que sur ce screenshot.
Les **UP** et **DN** du haut correspondent au trafic internet et ceux du bas au trafic réseau local.
- le cadenas en position ouverte (**Unlocked** dévérouillé) indique que **ZoneAlarm** ne bloque pas le trafic.
- Le gros bouton **Stop** vous permet de stopper immédiatement tout trafic de et vers internet.
- Le bouton **ZoneAlarm Help** vous permet d'accèder à l'aide en ligne au format HTML où vous retrouverez toutes les astuces qui s'affiche au démarrage.
Vous retrouvez ensuite en bas de la fenêtre cinq boutons **Alerts**, **Lock**, **Security**, **Programs** et **Configure** qui servent à la configuration proprement dite de **ZoneAlarm**.

4.2 SECURITY

Première étape dans la configuration, si votre poste **ZoneAlarm idefix** est sur un réseau local, vous devez indiquer que les autres postes du réseau ne sont pas hostiles mais peuvent accéder en toute liberté au poste **ZoneAlarm**, en effet si **obelix** est un serveur samba (serveur de fichiers), par défaut vous ne pourrez plus d'**idefix** accéder aux fichiers présent sur **obelix**. Pour cela cliquer sur **SECURITY**.



Noter que dans cette fenêtre vous pouvez fixer les niveaux de sécurité en local (poste **ZoneAlarm** et réseau local) et sur internet, par défaut le niveau de sécurité en local est fixé à **medium** (moyen) et celui sur Internet à **High** (élevé). Pour changer ce niveau hausser ou baisser le scrollbar correspondant, néanmoins vous pouvez les niveaux par défaut qui sont pas trop mal.
Pour info:
Le niveau élevé (**High**) correspond à:

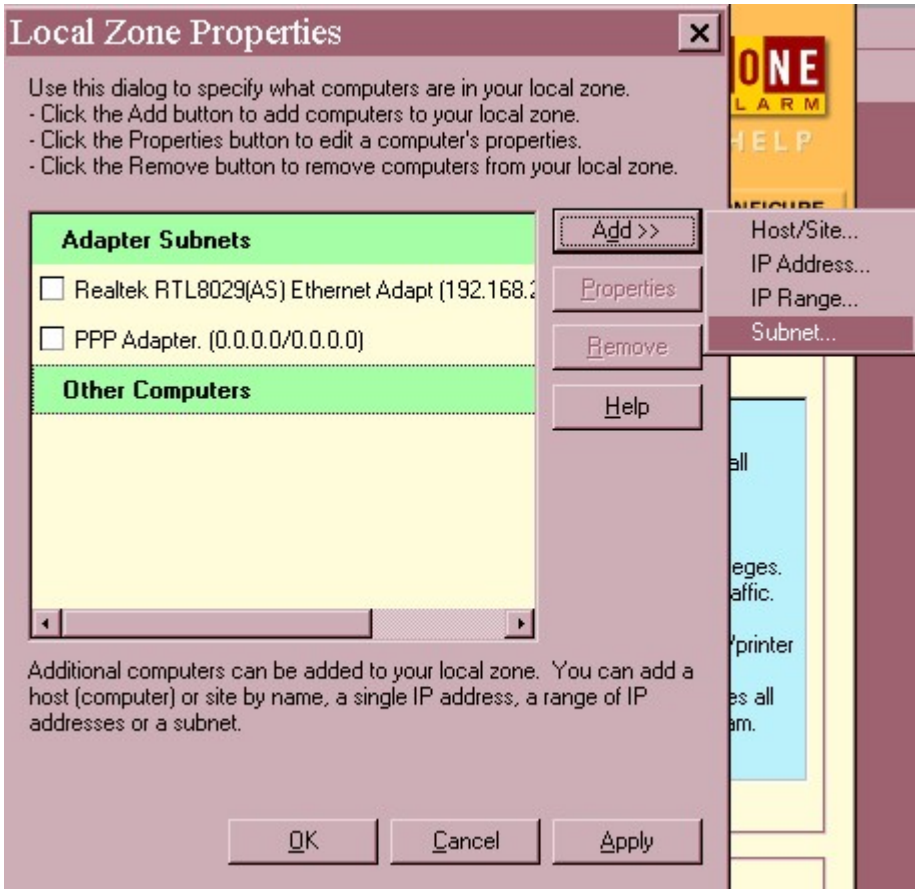
- renforce les privilèges applicatifs
- le verrou internet bloque tout le trafic
- les services windows (partage de répertoire, d'imprimantes, ...) ne peuvent accèder à internet
- les ports non utilisés de la machine **ZoneAlarm** sont masqués et ne sont pas vus sur internet (mode furtif)

Le niveau moyen (**Medium**) correspond à:

- renforce les privilèges applicatifs
- le verrou internet bloque tout le trafic
- les services windows sont autorisés à accèder au réseau local
- votre ordinateur et les serveurs qui y tournent sont visibles et accessibles aux autres ordinateurs de votre réseau

Sur cette fenêtre vous pouvez bloquer l'accès aux serveur locaux (de votre réseau local), ça ne présente aucun intérêt, laissez la case décochée. Vous pouvez aussi bloquer l'accès aux serveurs se trouvant sur internet, ça présente encore moins d'intérêt car vous ne pourrez plus surfer ! Par contre vous pouvez laisser coché la case **Enable MailSafe** protection qui permet un contrôle des pièces attachées des emails que vous récupérez, pour info **ZoneAlarm** intercepte tous les attachements de type VBS (Visual Basic Script) type I Love You, **ZoneAlarm** ne va pas les supprimer mais vous avertir afin que vous preniez les mesures

nécessaires.
Maintenant pour que **ZoneAlarm** ne prenne pas les postes de votre réseau local pour des "hostiles", cliquez sur **Advanced**.



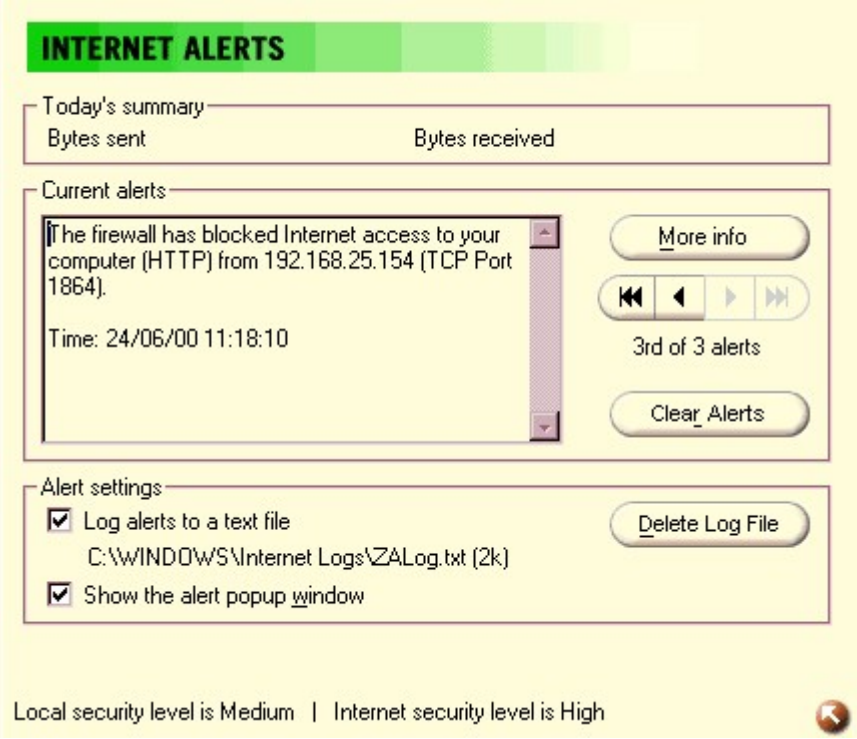
Dans cette fenêtre vous voyez vos interfaces, ici ma carte réseau **Realtek** qui permet d'accéder au réseau local et l'interface **PPP** (modem) qui permet d'accèder au net. Pour que **ZoneAlarm** ne contrôle pas le trafic de ou vers le réseau local, cochez la case devant le nom de votre carte réseau. Dans tous les cas laisser décocher la case devant l'interface PPP, sinon **ZoneAlarm** ne contrôlera pas le trafic de/vers Internet!
Vous pouvez ne pas contrôler le trafic de/vers certaines machines qu'elles soient sur internet ou sur votre réseau local, ces machines autorisées pourront accèder à votre poste sans que **ZoneAlarm** les bloque ou vous avertisse. Pour cela cliquer sur **Add**, vous avez le choix entre:

- **Host/Site**, il faut mettre le nom d'une machine se trouvant sur internet (ou sur le réseau local),
- **IP Address**, il faut mettre l'adresse IP de la machine,
- **IP Range**, fourchette d'adresse IP
- **Subnet**, sous réseau

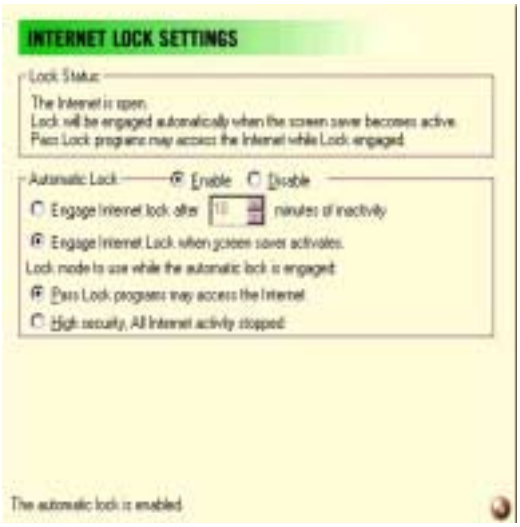
Dans le cas présent, j'ai coché la case devant mon interface réseau pour que **ZoneAlarm** ne bloque pas les accès de/vers mon réseau local.

4.3 ALERTS

La fenêtre **ALERTS** permet de visualiser les alertes de **ZoneAlarm**.



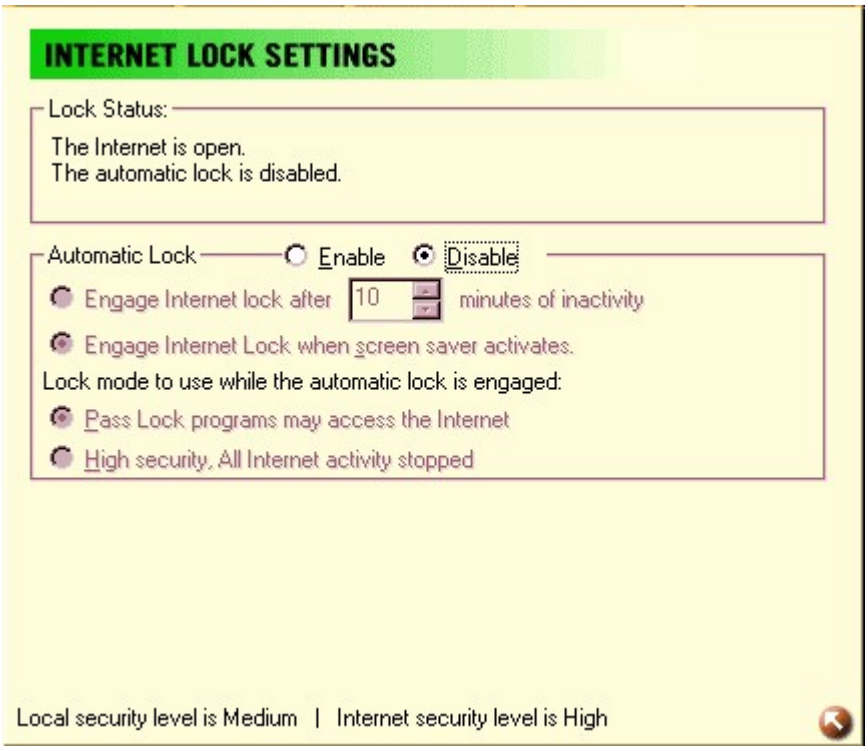
Sur ce screenshot on peut voir que **ZoneAlarm** a bloqué un accès venant de la machine 192.168.25.154 qui tentait d'accèder au port TCP 1864 à 11h18 le 24.6.00. Par défaut ces alertes ne sont pas archivées, je vous conseille de le faire en cochant la case **Log alerts to a text file**, le fichier en question se nomme **ZALog.txt** et se trouve sous **c:\windows\Internet Logs**. A noter qu'on voit aussi la taille du dit-fichier, ici 2k, s'il devient trop énorme vous avez la possiblité de le supprimer en cliquant sur **Delete Log File**.
La case cochée **Show the alert popup window** permet qu'une fenêtre popup apparaît à chaque fois qu'il y a une alerte, cette fenêtre décrit la nature du problème. En voici un exemple:



4.4 LOCK

La fenêtre **LOCK** permet de mettre en place un verrou automatique. Le verrou en question est le cadenas qu'on voit sur la fenêtre principal de **ZoneAlarm** qui est désactivé par défaut. Ce

verrou est utile quand vous vous êtes absenté de votre poste que celui-ci soit resté connecté sur internet ou non, il permet de stopper les accès. Cependant vous pouvez autoriser certaines applications à se connecter même en votre absence.



Par défaut le verrou automatique est désactivé (**Disable**), en l'activant (conseillé) en cliquant sur **Enable** vous pourrez:

L'activer automatiquement:
- au bout d'un certain temps d'inactivité
- quand l'économiseur d'écran se déclenche

Quand le verrou est actif (fermé):
- seuls les programmes autorisés pourront accèder à internet
- aucun trafic entrant et sortant n'est autorisé

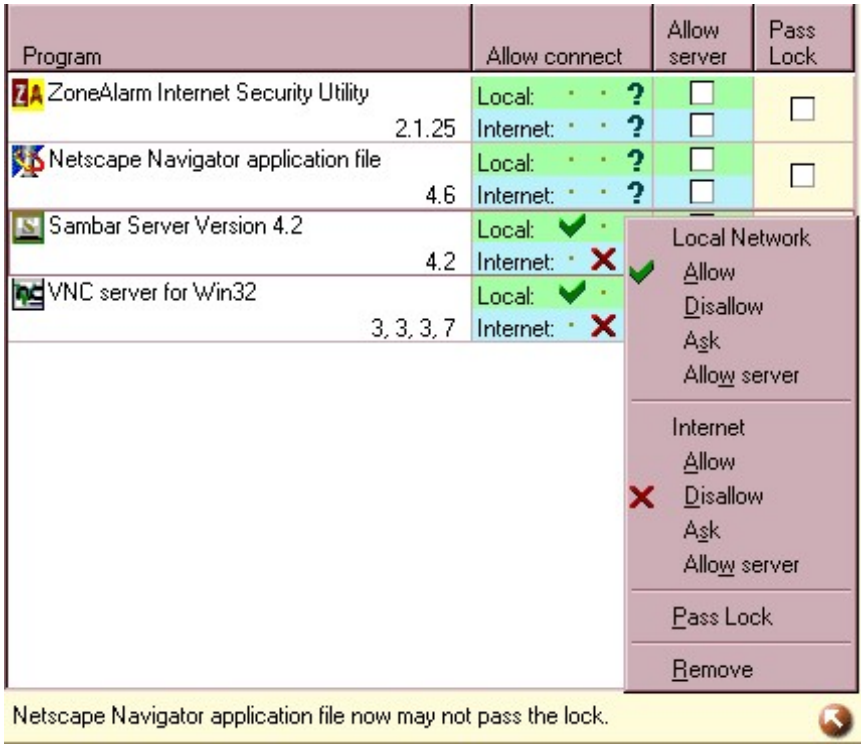
Pour autoriser les programmes à accéder à Internet même quand le verrou est actif, vous avez le bouton **PROGRAMS**.
Noter que pour activer immédiatement le verrou, il suffit de cliquer dessus le cadenas sur la fenêtre principale de **ZoneAlarm**, la fenêtre prendra cette allure:

Le nombre en dessous du verrou est le temps (en minute) depuis lequel le verrou est en place. Pour désactiver le verrou, cliquer à nouveau sur le cadenas.

4.5 PROGRAMS

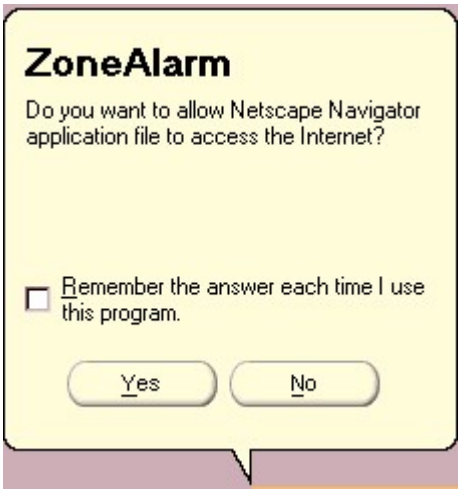
MCours.com

La fenêtre **PROGRAMS** permet de fixer les droits d'accès de/vers votre réseau local ou internet pour un certain nombre d'applications.



Apparaissent dans cette liste tous les programmes qui ont eu des accès de/vers votre réseau local et/ou internet. Pour chacun des programmes, vous avez les champs suivantes:
Allow connect : pour autoriser une simple connexion du programme de/vers le réseau local (Local) et/ou Internet

- **?** à chaque fois que le programme va chercher à se connecter, **ZoneAlarm** avertit l'utilisateur qui autorise ou non le programme à le faire (**Ask**). Ainsi dans le screenshot, à chaque fois qu'on cherche à accéder à internet avec **Netscape**, **ZoneAlarm** demande à l'utilisateur s'il veut autoriser **Netscape** à le faire ou non.



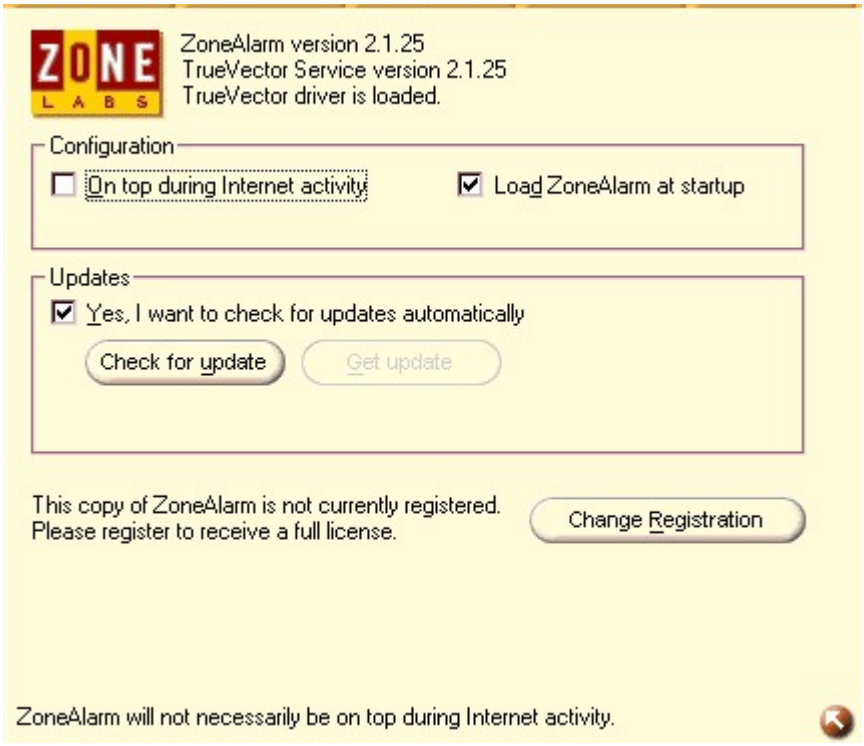
Noter qu'on peut faire en sorte de mémoriser cette décision dans ce cas, pour le programme en question on ne vous posera plus la question.
- une croix, le programme n'a pas le droit d'accéder au réseau local et/ou à internet
- un signe coché, le programme a le droit d'accéder au réseau local et/ou internet, **ZoneAlarm** ne demande pas l'autorisation à l'utilisateur.
Exemple sur le screenshot pour **Sambar Server**, il est autorisé sur le réseau local mais refusé sur Internet (trafic descendant et montant).

NOTE : Si vous avez coché la case **Remember the answer each time I use this program** dans la fenêtre popup **ZoneAlarm** au lancement d'un programme voulant accèder à Internet, cela mettra automatiquement le signe coché pour le programme en question dans la fenêtre **PROGRAMS**. Si le programme ne vous dit rien du tout, je vous conseille de mettre **No** dans cette même fenêtre popup, sait-on jamais.

Allow server : certains programmes doivent se comporter comme un serveur, c'est le cas de **Napster** par exemple, vous devez donc cocher la case correspondante.
Pass Lock : quand le verrou est actif vous pouvez autoriser certains programmes à se connecter ou pas.
Vous pouvez changer les droits des programmes en cliquant sur les champs de propriétés avec le bouton droit de la souris, le menu représenté dans le screenshot plus haut apparaîtra.

4.6 CONFIGURE

La fenêtre **CONFIGURE** permet de configurer certains paramètres.



Dans cette page vous pouvez définir si les fenêtres **ZoneAlarm** doivent être devant toutes les autres ou pas, c'est à dire que dès que vous êtes connecté à internet la fenêtre principale de **ZoneAlarm** masquera en permanence vos autres pages, c'est très génant je vous conseille donc de décocher prestement cette case. Vous pouvez définir que **ZoneAlarm** soit lancé au démarrage (startup) de windows. Les autres champs correspondent à l'update de **ZoneAlarm** et à l'enregistrement de la licence.

NOTE : Comme **ZoneAlarm** a tendance à ralentir légèrement windows, je vous conseille de ne pas le lancer au démarrage (on décoche la case correspondant) mais de le lancer juste avant une connexion (**Menu Démarrer ->Programmes->Zone Labs->ZoneAlarm**) puis de le stopper à la fin de la connexion (bouton droit de la souris sur l'icône **ZoneAlarm** puis **Shutdown ZoneAlarm**).

5 Utilisation normale

Pour terminer voilà un screenshot de **ZoneAlarm** en fonctionnement normal:

On peut voir le trafic entrant et sortant de/vers internet (rouge montant, vert descendant), et les programmes accèdant à internet sont à droite du bouton **Stop**, ici on n'a que **Netscape**.