Micro-ordinateurs,
informations, idées, trucs et astuces

Utiliser Zone Alarm,

Version 5

Auteur : ***François CHAUSSON***
Date : ***8 octobre 2008***
Référence : ***utiliser Zone Alarm.doc***

Préambule

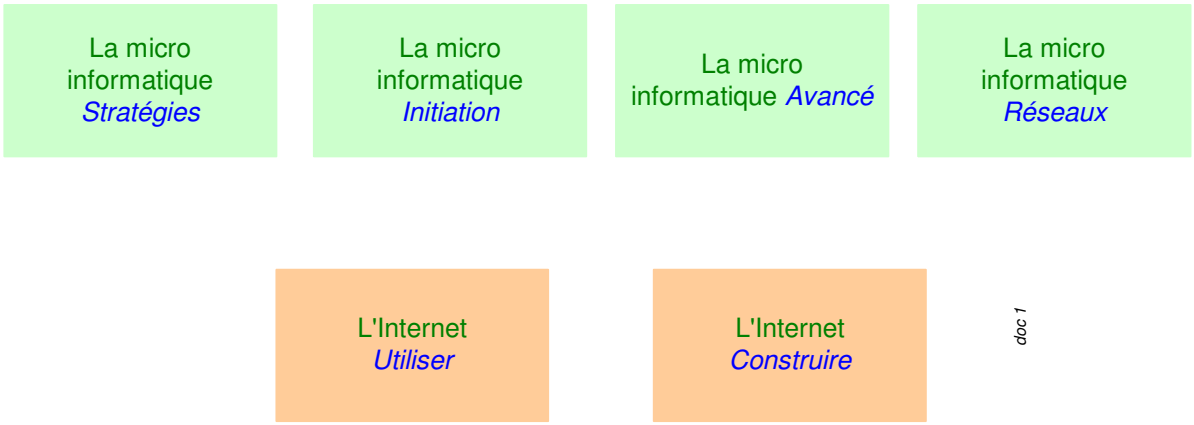
Voici quelques informations utiles réunies ici initialement pour un usage personnel en espérant qu'elles puissent aider d'autres utilisateurs de micro-informatique.

Ces informations sont présentées sans démarche pédagogique ; si un niveau de détail était nécessaire sur un sujet particulier, ne pas hésiter à me demander.

Ce document

Il fait partie de l'ensemble documentaire ***Micro-ordinateurs, informations, idées, trucs et astuces*** qui couvre ces sujets :

1. *La micro-informatique*, en 2 tomes
2. *L'Internet*, en 2 tomes



3. *Des Trucs HTML et Javascript*
4. *Des notices d'utilisation de divers logiciels*[1]

Tout commentaire à propos de ce document pourrait être adressé à :
pcinfosmicro@francois.chausson.name

Ce document est régulièrement mis à jour sur : http://fcfamille.free.fr/[2]

[1] ZoneAlarm, AVG, …
[2] Site à accès contrôlé

Table des matières

Zone Alarm

Un Firewall contrôle les accès, entrants comme sortants, conformément aux descriptions saisies par son utilisateur.

Alternative

Utiliser le pare-feu Windows XP[3].

Remarques :

- Celui-ci ne contrôle que les flux entrants.

Installation

Chargement

Télécharger d'abord depuis un site comme :

- www.tucows.com
- www.download.com
- …

Versions

Ce versions portent des noms différents[4]

- gratuite : *zlsSetup_60_667_000.exe*
- payante : *zapSetup_60_667_000.exe*

Le choix : prendre la version gratuite tant qu'une fonction de la version payante n'est pas nécessaire.

Installation

Cliquer sur le fichier reçu[5] et suivre ensuite les instructions données par le logiciel.

Seule une toute petite icône en bas à droite est créée[6].

Post–installation

Rien n'est prévu pour relancer ZA dans ce qui est installé ; pourtant, comme il peut arriver de l'arrêter, il faut aussi pouvoir le relancer rapidement.

Il faut donc créer une icône sur le bureau ; voir en annexe.

[3] voir « Firewall Windows », p.13
[4] montrés ici pour la version 6.0 667
[5] Auto-exécutable
[6] Rien sur le Bureau

Utilisation

Zone Alarm est actif par défaut immédiatement après installation ; aucune action n'est nécessaire à un lancement éventuel puisque c'est déjà fait.

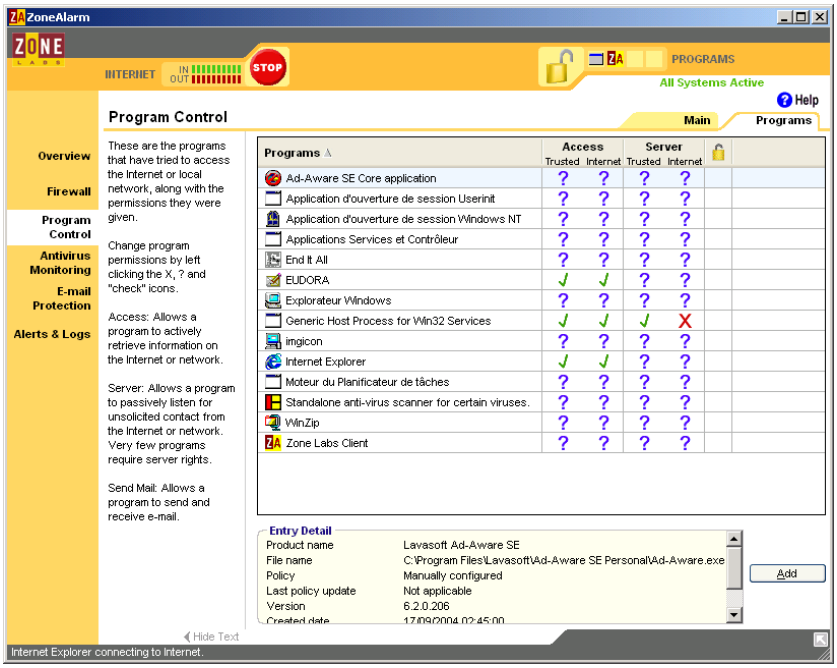
Par contre, des actions de paramétrage permettent d'adapter ce fonctionnement aux besoins de l'utilisateur.

Paramétrages

Le panneau de contrôle

Le *Control center*[7] de ZA présente :

- les paramètres existants
- un historique des tentatives d'accès.



Les onglets

- *Firewall*:
  La carte Ethernet[8] apparaît là, en zone Internet
- *Program control*
  La liste de tous les programmes qui ont sollicité une autorisation[9]
- *Alerte and logs*
  Un historique des tentatives d'accès

Des concepts

- Les *Zones*:
  Trusted: c'est au dedans, le réseau local, de confiance[10]

[7] Appelé par un clic droit sur la petite icône *ZA* en bas à droite
[8] Si une carte est installée, voire même plusieurs (WiFi ? …)
[9] voir plus bas

Internet: c'est au dehors, l'Internet, aucune confiance

- Les comportements

  Access: toute action positive d'un programme installé dans le PC pour « parler » vers l'extérieur

  Server: une posture d'attente d'un programme pour « écouter »[11] un événement arrivant de l'extérieur

Les signes

- La coche verte: autorisation permanente
- Le point d'interrogation bleu: demande à chaque fois
- La croix rouge: interdiction permanente

Les accès légitimes

- Les fonctions évidentes:
  - *Internet explorer*
  - La messagerie: Outlook, Eudora
  - …
- Des fonctions système:
  - *Applications services et controler*
  - *Generic host process*
  - Voir aussi dans le Help ZA

Les recommandations de spécification

Dans l'onglet *Program control* :

- *Access/trusted* :
  mettre en point d'interrogation
- *Access/Internet* :
  mettre en coche verte pour les accès légitimes
  mettre en point d'interrogation pour les autres
- *Server/Trusted* :
  mettre en point d'interrogation
- *Server/Internet :*
  mettre en croix rouge[12]

Recommandations de ZoneAlarm

Generally you should not grant 'server' rights to any program unless they need to "listen" for a internet connection to function properly.

Exercise caution when granting permission for programs to act as a server, as Trojan horses and other types of malware often need server rights in order to do mischief. Permission to act as a server should be reserved for programs you know and trust, and that need server permission to operate properly.

---

[10] Le réseau local peut ne pas exister, être composé d'une seule carte (Ethernet pour la Freebox, WiFi, …), de plusieurs cartes, …

[11] éventuellement répondre (comme un serveur)

[12] sauf rare exception : chat, …

The exception is you should grant server rights to Generic Host Process but only in the Trusted zone not the Internet zone. Application Layer Gateway Service generally should not need server rights although some FTP clients might require ALGS to have server rights.

Note that you probably have several programs that will ask for server rights even thought it is not required for them to function properly. Media players are famous for this. So when in doubt, deny server rights until and unless your program will not function without it. You can always allow later.

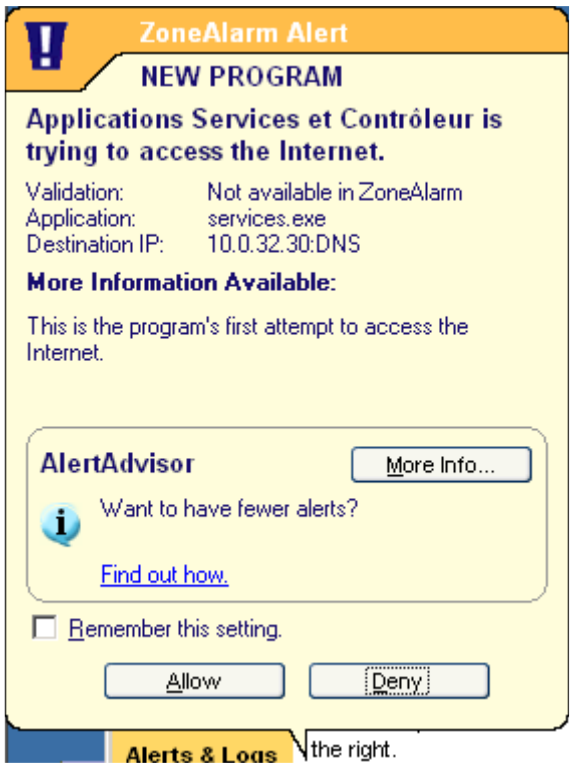
Au premier lancement

ZA découvre un réseau local, une carte Ethernet, un réseau WiFi et demande le niveau d'autorisation / cantonnement à lui attribuer :

En cours d'activité

Solliciter une autorisation

Quand un programme fait une tentative d'accès qui n'est pas autorisée, ZA pose la question d'accorder ou pas une autorisation nouvelle:



Cocher la boite *Remember this setting* permet de donner l'autorisation de manière définitive ; à l'inverse, ne pas la cocher permet de ne donner qu'une autorisation pour cette fois là.

Task List programs

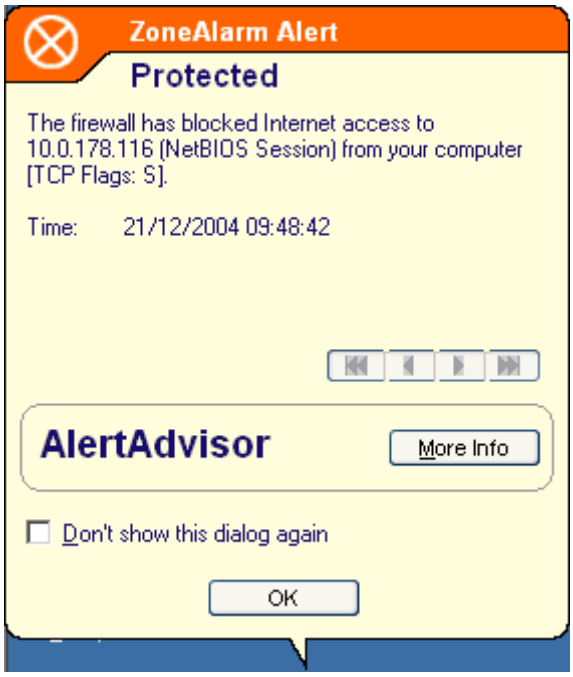
Pour vérifier la fonction exacte d'un programme, consulter :

- http://www.answersthatwork.com/Tasklist_pages/tasklist.htm

http://forum.zonelabs.org/zonelabs/board/message?board.id=AllowAccess&message.id=58#M58

Avertir d'une tentative d'intrusion

Quand une tentative d'intrusion se présente, ZA avertit l'utilisateur[13] :

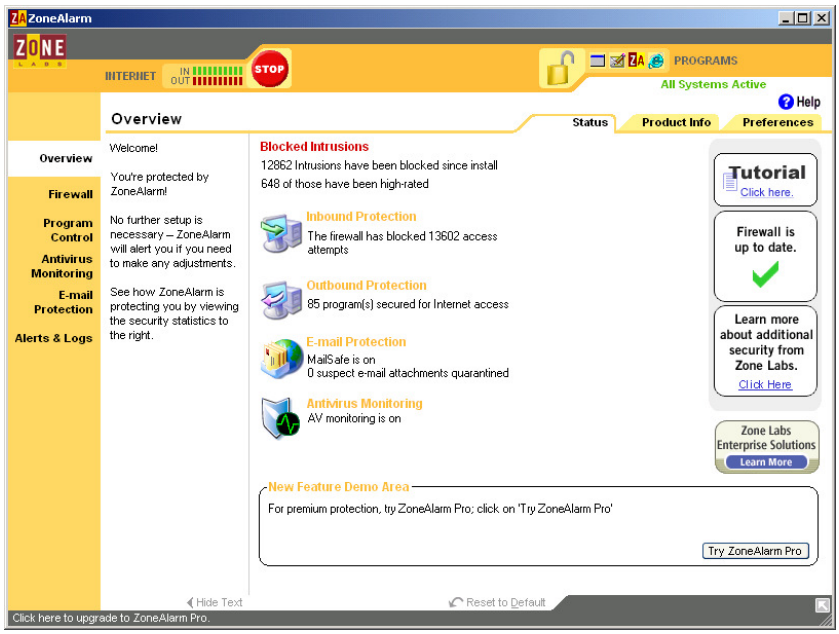


Mise à jour

L'état de la situation

L'état de la situation peut être vu sur le *Control center*, à l'onglet *Overview* :

[13] sauf s'il a auparavant déjà coché la case *Don't show …*



Un bouton sur la droite indique qu'ici « Firewall is up to date ».

Lancer la mise à jour

Quand l'état, vu sur le bouton, dit « aaaaa » :

-

Granularité de la mise à jour

Attention car une mise à jour de ZA n'est jamais livrée en incrémental ; c'est toujours une version opérationnelle complète qui arrive, volumineuse donc[14].

[14] et « lourde » si on est en accès RTC

Incidents

Pas d'accès sur le réseau local

Question

Voici un rebus:
- mon routeur WiFi: 192.168.1.1
- mon PC: 192.168.1.10 (adresse fixe, vérifié par Ipconfig)
- le PC de ma femme: 192.168.1.5 (adresse fixe, vérifié par Ipconfig)
- chaque PC ping le routeur
- les 2 PC accèdent bien à Internet (Freebox) donc le WiFi fonctionne
- mais:
    - quand je fais un Ping du PC 1.5 vers le PC 1.10: OK
    - par contre, en sens inverse: KO
    - malgré mon Domaine toujours commun aux deux PC, je ne voit plus dans l'Explorateur les répertoires partagés de l'autre PC

Ca eut fonctionné mais ça ne fonctionne plus.

Réponse

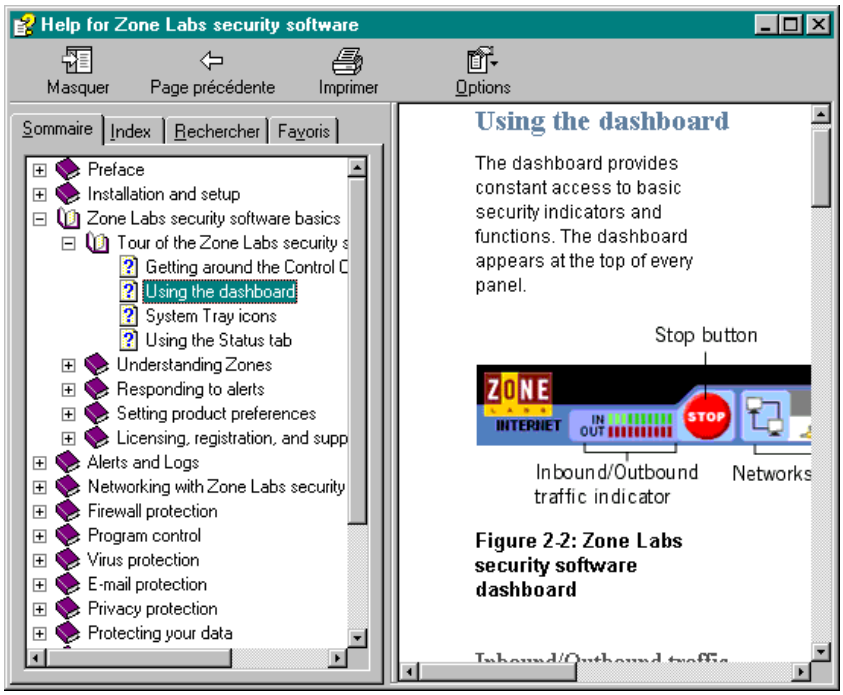
Vérifies que sur le 1.6 le firewall intégré ou ajouté, ne bloque pas le protocole ECHO (ping) et qu'il ne bloque pas les ports 137 138 139 et 445 (partage et RPC)

Annexes

En savoir plus

Sur le *Control center* :

- Clic sur le bouton *Help*



Kaspersky et la protection contre les attaques réseau

Voir ce chapitre dans le document « utiliser Kaspersky 5.doc ».

Créer une icône

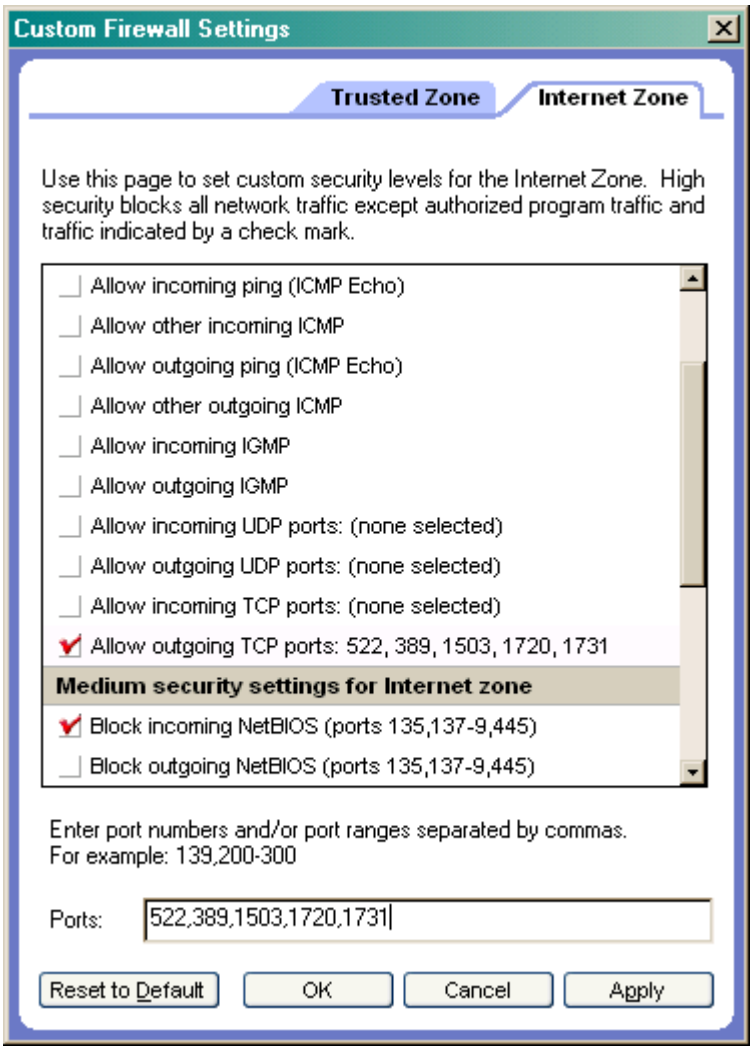
Pour ça :

- Aller dans *C:\Program Files\Zone Labs\ZoneAlarm*
- Clic droit sur *zonealarm.exe*
- Dans le menu contextuel, sélectionner *Créer un raccourci*
- Faire Drag/Drop du raccourci qui est apparu dans Explorateur vers le bureau
- Au besoin, renommer le raccourci[15]

Ouvrir les Ports dans Zone Alarm[16]

- Dans l'onglet *Firewall/Main*
- Clic sur *Custom*
- dans la fenêtre, spécifier les Ports à autoriser

[15] faire F2
[16] uniquement possible avec la version payante de ZA



Désinstaller ZA

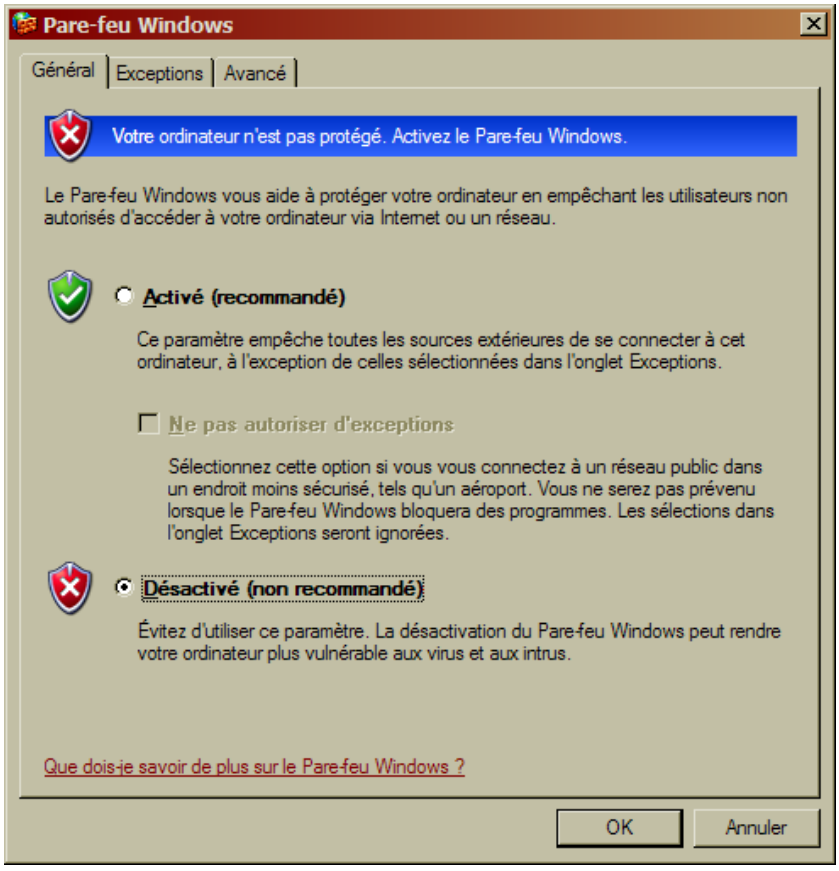
- trouvé dans : http://forum.zonelabs.org/zonelabs/board/message?board.id=gen&message.id=24018#M24018
-

Try resetting the ZoneAlarm database and reconfiguring the entire firewall and see if it still happen's.
Reset the database this way
1. Shut down the client from the system tray(Rightclick ZA icon choose shutdown)
2. access the c:\windows\internet logs folder
3. Delete the backup.rdb and iamdb.rdb files.
4. Restart ZA
Something may have triggered the database to corrupt itself

Firewall Windows XP

Pour l'activer :

- dans *Panneau de configuration*
- dans *Centre de sécurité*
- clic sur le lien *Pare feu Windows*



Pour utiliser le pare feu Windows seul :

- clic sur *Activé*

A l'inverse, pour utiliser le pare feu ZA seul :

- cocher *Désactiver*

ZA settings

Conserver ses options

- http://forum.zonelabs.org/zonelabs/board/message?board.id=inst&message.id=39388#M39388

If you wish to keep your settings, create a Backup from Overview - > Preferences before starting, and then Restore afterwards (available in ZoneAlarm Premium products only).

Click on Start -> Programs -> Zone Labs. RIGHT-click on Uninstall Zone Labs Security, then select Properties.
Under Target you will see the following line (the actual drive may be different on your system):
"C:\Program Files\Zone Labs\ZoneAlarm\zauninstexe"
Change it to:
"C:\Program Files\Zone Labs\ZoneAlarm\zauninst.exe" /clean (add a space and then the /clean)

Click OK to save the new command line. Click on Start -> Programs -> Zone Labs -> Uninstall Zone Labs Security.
Click OK to run the uninstaller, and OK any security alerts that pop up. say "Yes when being prompted for the removal of all files and allow TrueVector to shut down. Reboot.
After rebooting, check for the following folders, and delete them if you find them: C:\WINDOWS\Internet Logs, C:\Program Files\Zone Labs and C:\WINDOWS\system32\ZoneLabs.
For Windows **XP: clean your C:\WINDOWS\Prefetch folder.** Clean the history in Internet Explorer or your current browser, clean the cookies.
Then empty your recycle bin. ZoneAlarm should be gone.
Reboot. Install the latest version if you are reinstalling.
For clean reinstall: Turn off your Anti Virus program and all other running programs, it's strongly recommended that you exit all Windows programs before running the Setup Program of ZoneAlarm.
Double click the ZoneAlarm file icon on your PC to begin the installation wizard. Select a 'clean' install when asked

Nettoyage total avant de réinstaller

Prendre la même procédure en entrant en cours de route

ZA et VNC

Message

Is there any way to enable the control of ZoneAlarm through VNC? I need to be able to control ZoneAlarm from remote locations to help family and friends, but ZA does not respond to anything other than the local inputs.

Message

See if these two documents helps.
http://www.nohold.net/noHoldCust25/Prod_1/Articles55646/RemoteAccess_version6.htm
http://www.nohold.net/noHoldCust25/Prod_1/Articles55646/VNC.html

Premier lien

Troubleshooting VNC/pcAnywhere with ZoneAlarm 6
Solution:
ZoneAlarm Pro and Suite version 6 include a new integrated AntiSpyware. The AntiSpyware picks up some programs (such as VNC, pcAnywhere and CarbonCopy) as a RAT (Remote Access Tool). Usually these types of files are quarantined by default, so you may be able to restore any missing files from the Quarantine tab in the ZoneAlarm Antivirus/AntiSpyware panel.
To set programs to OK, go to AntiSpyware advanced settings and set it to NOT automatically treat infections. Run the AntiSpyware Scan. Once it completes, locate the entries you wish to allow and select "Always Ignore". Afterward you can set it back to automatically treat.

Deuxième lien

VNC is not working properly with ZoneAlarm running.
Solution:
In order for VNC and ZoneAlarm to work together, please follow these instructions:

1. On the Server (client) machine, configure VNC with a password.
2. On the Server (client) machine, run WinVNC. The menu shortcut is "Run WinVNC (App mode)" and set the following settings in ZoneAlarm:
    - If you know the IP or subnet will always be the same from the Viewer, add that IP or subnet to your Trusted zone in Firewall -> Zones -> Add. As long as Trusted Zone security is set to or Medium, the IP should be available.
    - Then in the Program Panel: Allow Connect in Trusted Zone only, and Allow Server in Trusted Zone only (be sure to NOT block servers in Local Zone)
    - If you do not know the IP of the Viewer, or it will change, then in ZoneAlarm's Program Panel: Allow Connect in Trusted and Internet Zones, Allow Server in Trusted and Internet Zones.
    - On free ZoneAlarm you may need to set Internet to Medium setting or the connection will be blocked. In ZoneAlarm Plus/Pro/Suite you can open the specific ports required by your VNC version.
3. From the Viewer (remote) machine, run VNCViewer to connect to the Server (client) machine. The menu shortcut is "Run VNCViewer". Do not run "VNCViewer (Listen mode)".
4. When prompted by VNCViewer on Viewer (remote) machine, enter name or IP address of the Server (client) machine, followed by password when prompted. You should be able to connect.

    Since the Server machine has allowed connections and server rights, the main security measure available is VNC's password. Therefore, we recommend disallowing connections and disallowing server when not required.

When configured in this manner, VNC can run with ZoneAlarm -- usually even at High security

ZA Release history

ZA general release history

http://forum.zonelabs.org/zonelabs/board/message?board.id=inst&message.id=39388#M39388

ZA Pro release history

http://download.zonelabs.com/bin/free/information/zap/releaseHistory.html

Last ZA version for Millenium

Last ZA version for W98

The last version that is compatible with windows 98 is 6.1.744.001 which can be downloaded HERE

Internet Connection sharing

« Only the pais versions of the ZA will support sharing. »

Bibliographie « Utiliser … »

Ces différents documents constituent l'ensemble documentaire ***Utiliser ….***

La liste complète est disponible sur http://fceduc.free.fr/documentation.php.

