

CONNAITRE LES SIGNIFICATIONS DES ALERTES DU FIREWALL DE SECURITOO V2

Cette fiche pratique vous indique la signification des alertes du Firewall de Securitoo.

Signification des alertes.

Etape 1 : Cliquez avec le bouton droit de la souris sur l'icône de Securitoo, située en bas à droite à coté de l'heure. Puis cliquez sur "Ouvrir Securitoo AntiVirus Firewall".

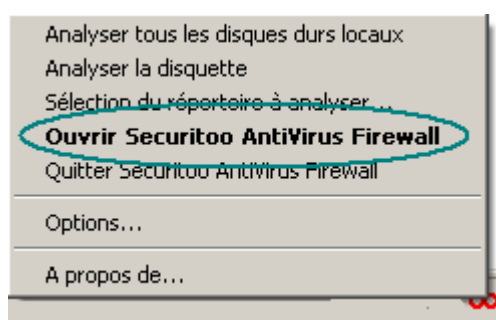


Figure 1 : Ouvrir Securitoo

Etape 2 : La fenêtre suivante apparaît. Cliquez sur le bouton **Firewall**.



Figure 2 : Firewall

Etape 3 : La fenêtre ci-dessous s'affiche. Cliquez sur "Paramètres avancés..."



Figure 3 : Paramètres avancés

Etape 4 : Une fenêtre comme celle ci-dessous s'affiche. Allez dans l'onglet "Alertes".

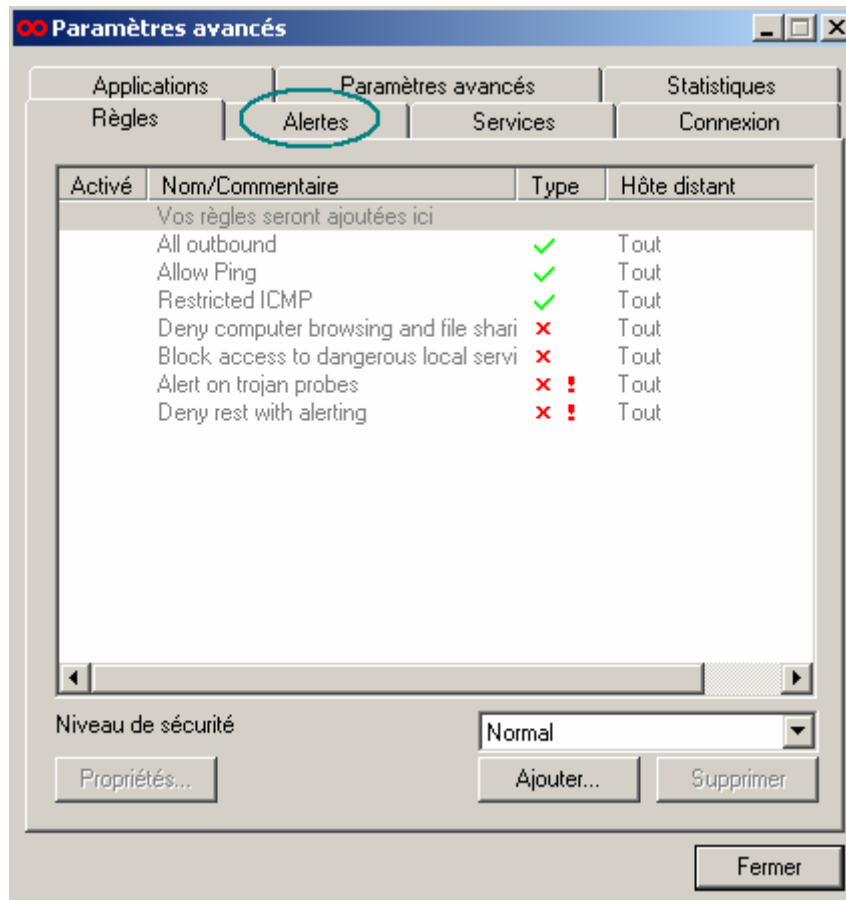


Figure 4 : Alertes

Etape 5 : Une fenêtre comme celle ci-dessous s'affiche, en bas à gauche vous pouvez cocher deux cases. La 1ère case à cocher "Affichage de l'alerte" (1), vous permet d'afficher toutes les alertes venant du Firewall. Pour savoir à quoi correspond une alerte il faut double cliquer sur l'une d'entre-elles (2). *(Ici l'image est un exemple).*

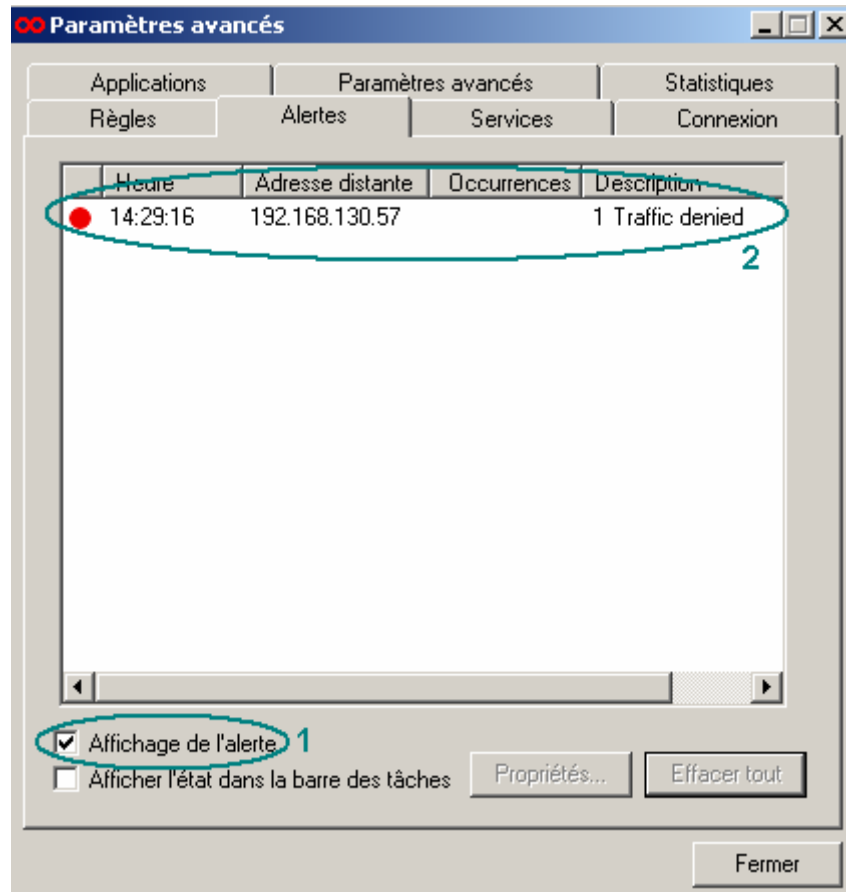


Figure 5 : Affichage des alertes

Vous pouvez avoir une fenêtre (une alerte) comme celle-ci dessous (cette fenêtre est un exemple):

Général	
Commentaire sur l'alerte	Traffic denied
Adresse local	192.168.130.195
Action	Refuser
Direction	Entrant
Adresse distante	192.168.128.182
Tampon horodateur	05/02/05 14:41:28
Nom DNS	

Service	
Protocole	udp
Port local	1193
Port	62838
Services	UDP in

Figure 6 : Alertes

Le 1er rond en haut à gauche (1) indique quelle adresse à voulu entrer sur votre machine.

Le 1er rond en haut à droite (2) indique le type de l'attaque, ici "Entrant", donc d'Internet vers votre PC.

Le 2eme rond en bas à gauche (3) indique le protocole qu'utilise l'attaque potentielle, ici UDP.

Le 2eme rond en bas à droite (4) indique par quel port l'attaque potentielle est arrivée sur votre machine.