

FireStarter : simple et efficace.

Voici une petite présentation de ce très bon firewall libre, aussi simple qu'efficace, et toujours utile.

Pensons à la sécurité avec ce très bon frontend pour iptable, le pare feu du noyau GNU/Linux. Un pare feu permet de protéger son ordinateur du réseau, pour que personne ne puisse « entrer » dans votre pc à votre insu. Il est vraiment très simple à utiliser et à configurer, mais il est aussi vraiment efficace. Il permet une vue en temps réel du trafic, le partage de connexions, permet de gérer le trafic entrant et sortant, gère les réseaux avec DHCP (Dynamic Host Configuration Protocol), et on peut aussi créer des listes noires.

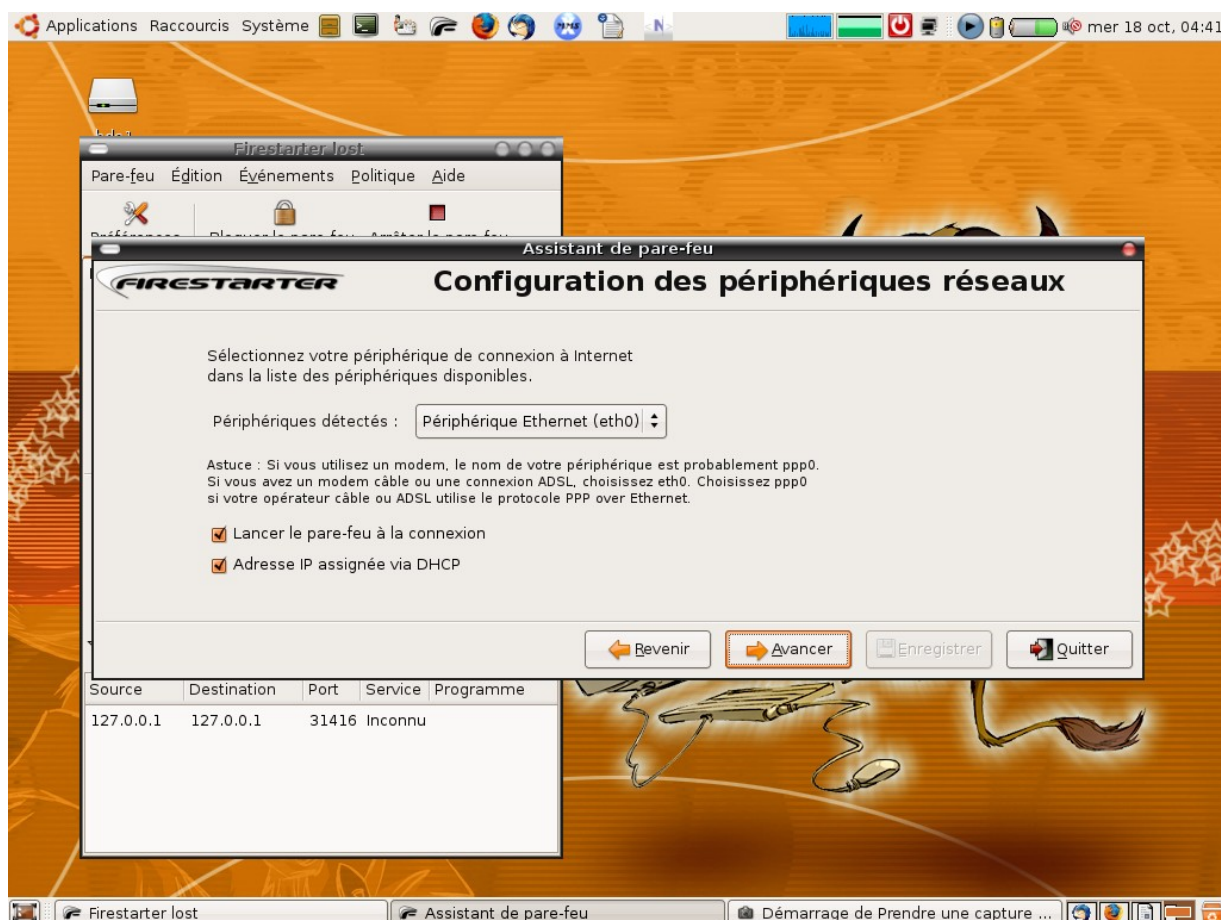
Il est dédié à l'environnement graphique Gnome.

Site officiel : <http://www.fs-security.com>

Pour l'installer, il suffit de passer par le gestionnaire de paquets de votre distribution (RpmDrake pour Mandriva, Synaptic pour Ubuntu).

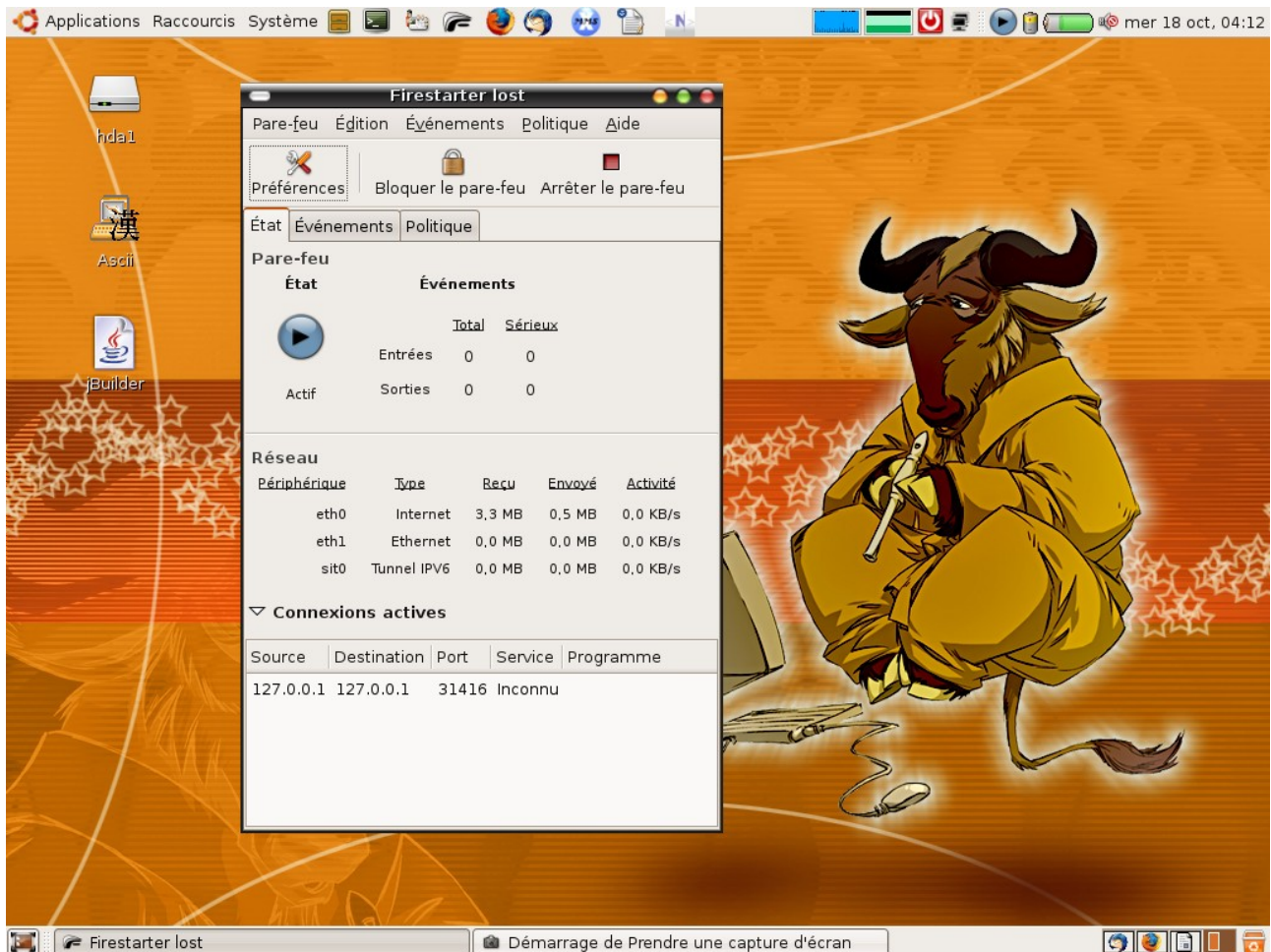
Sinon, rendez-vous sur cette page : <http://www.fs-security.com/download.php> pour télécharger les sources.

Lorsqu'il est lancé pour la première fois, l'assistant vous pose un certain nombre de questions pour le configurer.



Quelle carte réseaux doit-il surveiller, doit-il utiliser un DHCP, accepte-il le partage de connections. Ensuite, il démarre.

Quand il tourne, on voit son statut ainsi que les connections actives (leur type, sur quel carte réseau, l'IP de destination et les ports).



Il y a plusieurs menus :

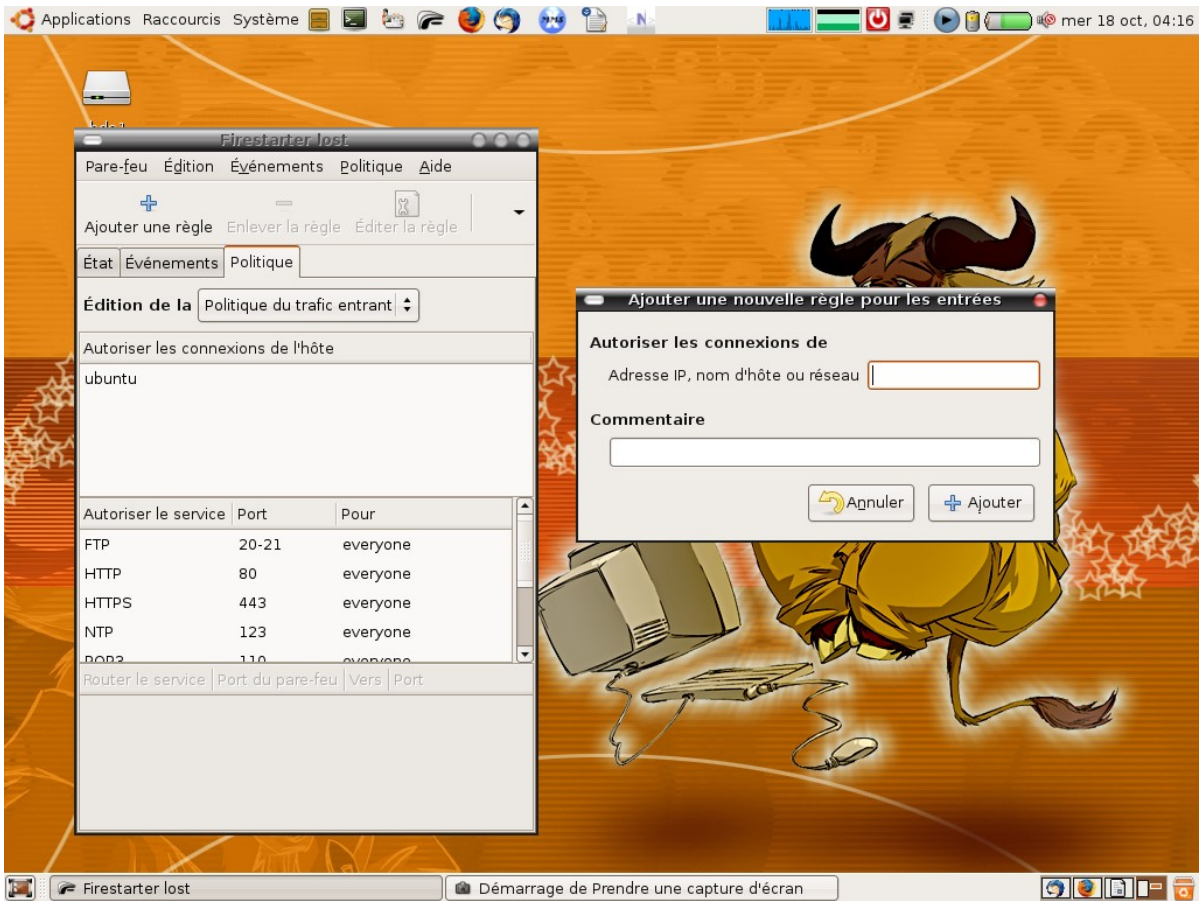
Pare-Feu : pour lancer l'assistant, démarrer ou bloquer FireStarter.

Editions : pour modifier les préférences.

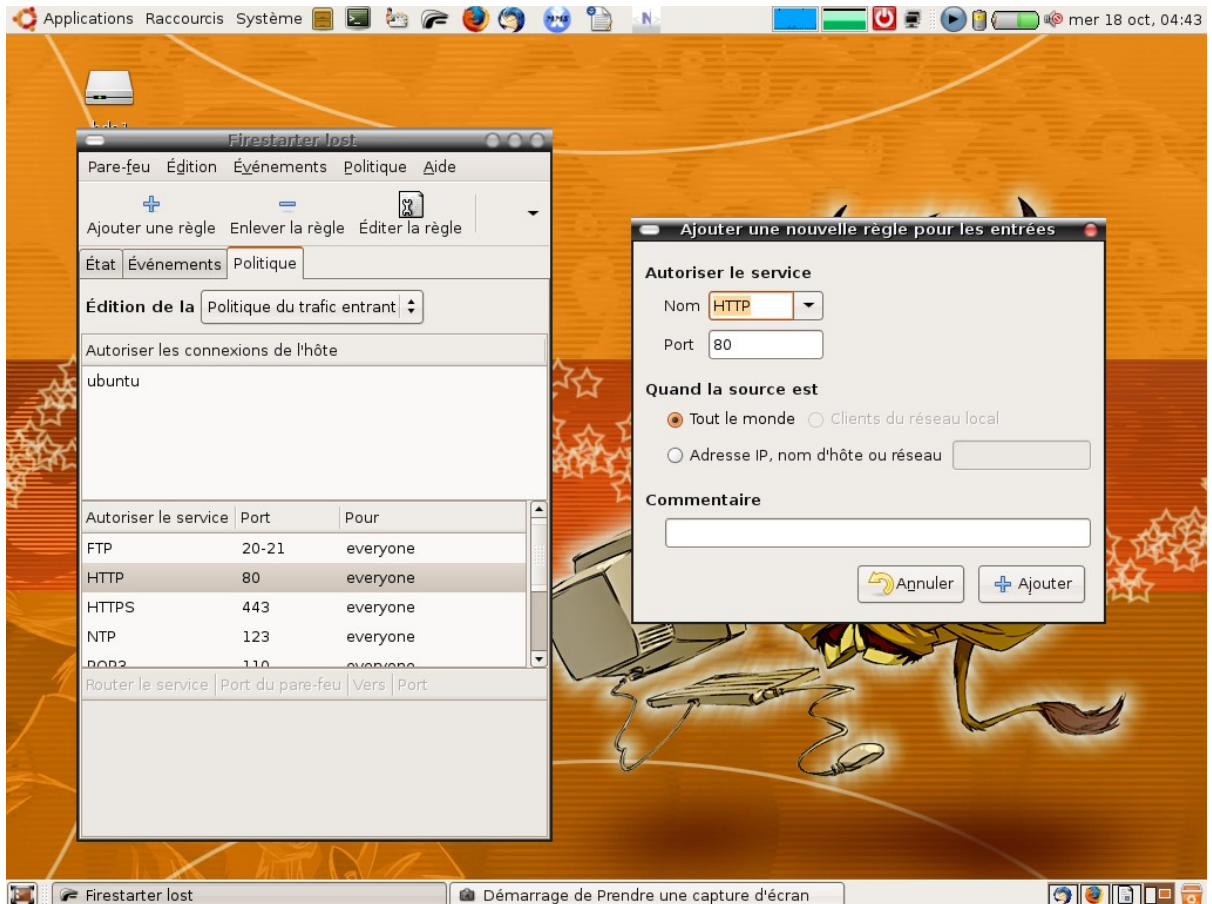
Événements : pour choisir ce que l'on affiche dans la fenêtre d'événements.

Politique : permet d'ajouter, enlever ou encore modifier des règles.

L'ajout de règles est simple, et on peut configurer diverses choses, comme vous le voyez sur la capture ci-dessous :



Voilà ce que l'on peut configurer dans les règles d'autorisation :



Dans les Préférences, on peut configurer plusieurs choses, notamment le partage de connexions, le DHCP, le filtrage par type de service, blocage du broadcast, le rejet des paquets silencieusement ou alors, avec erreur.

