Contrôle parental sous PrimTux

Mettre un PC à disposition des enfants présente de gros risques lorsque la machine est reliée à Internet. Comment dès lors leur permettre de bénéficier des atouts du Net en matière éducative, tout en les préservant de ses dangers ?

Linux peut être la solution, ce système d'exploitation proposant une multitude de distributions dont certaines sont spécialisées dans des domaines précis. Ainsi par exemple PrimTux est une distribution qui s'adresse aux enfants de la maternelle au début de collège aussi bien qu'aux adultes. Elle intègre de base des outils de contrôle parental. Dans ses versions jusqu'à la version 3, la sécurité Internet est assurée par Tinyproxy et dansguardian, et dans sa version 4 par CTParental.

Voici comment paramétrer efficacement ces outils si vous décidez d'adopter la solution clé en main PrimTux.

PrimTux2 et PrimTux3

Personnaliser le contrôle parental

Sur les versions antérieures à la version 4, PrimTux s'appuie sur Tinyproxy et Dansguardian pour assurer la protection sur Internet par l'utilisation des blacklists de l'université de Toulouse.

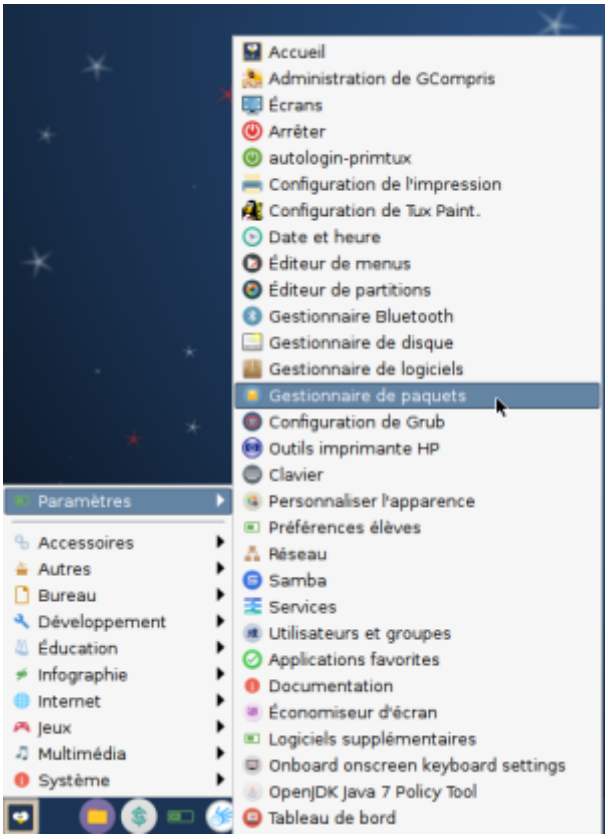
Il est possible de personnaliser ce contrôle parental avec Webstrict installable en logiciel complémentaire. Cet outil fonctionne selon le principe de liste noire et liste blanche:

- la liste noire permet d'interdire l'accès aux sites indiqués;
- la liste blanche permet d'autoriser l'accès aux sites indiqués.

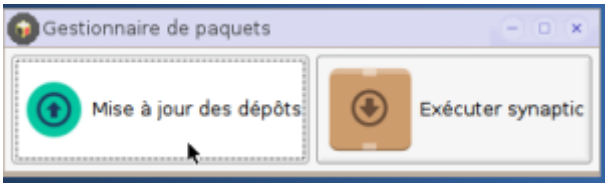
Installation de Webstrict

Tout d'abord vous devez vérifier que vous avez installé Webstrict. Si c'est le cas, son raccourci devrait apparaître dans les sous-menus paramètres et système. Dans le cas contraire installez-le.

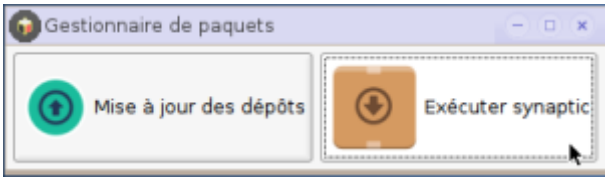
Installation par le gestionnaire de paquets Synaptic



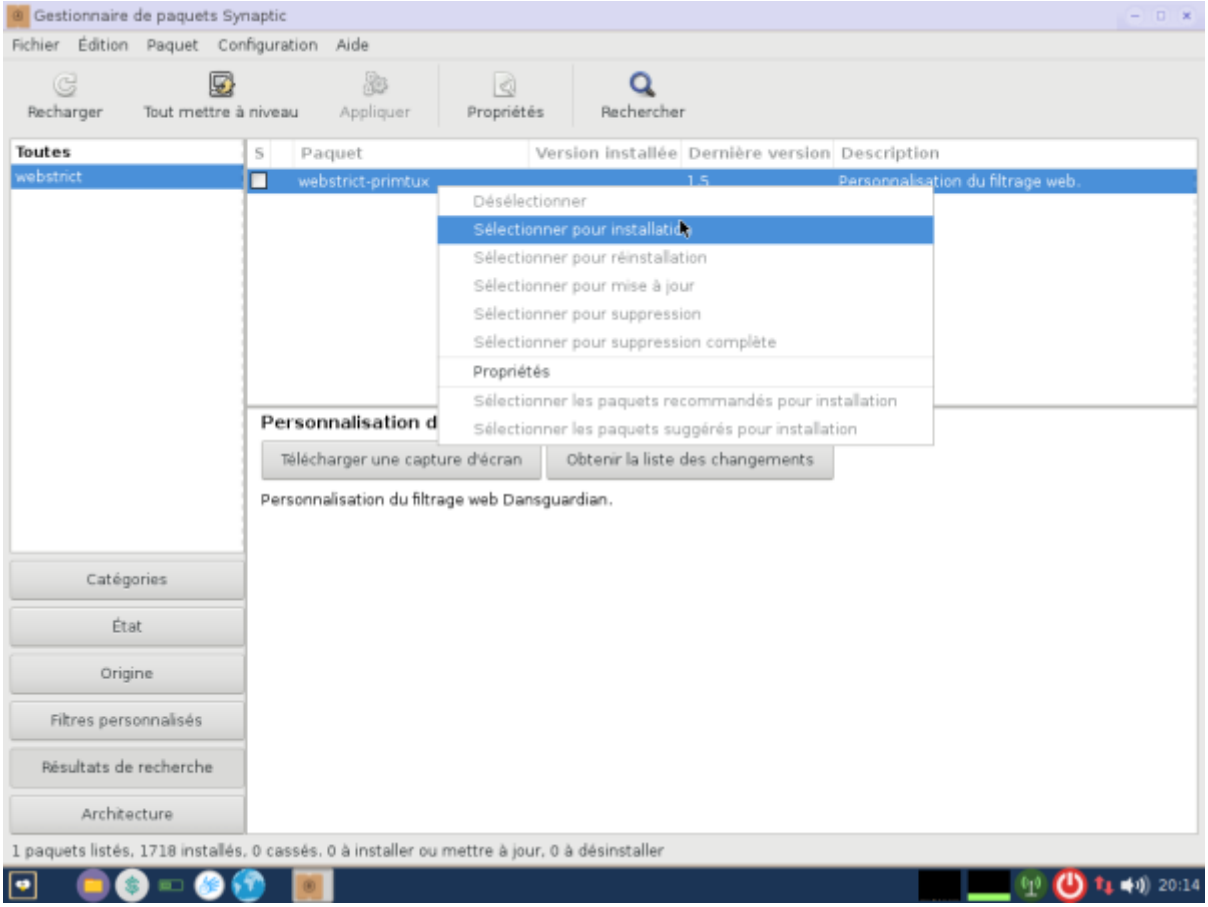
Vous devez d'abord mettre à jour la liste des paquets :



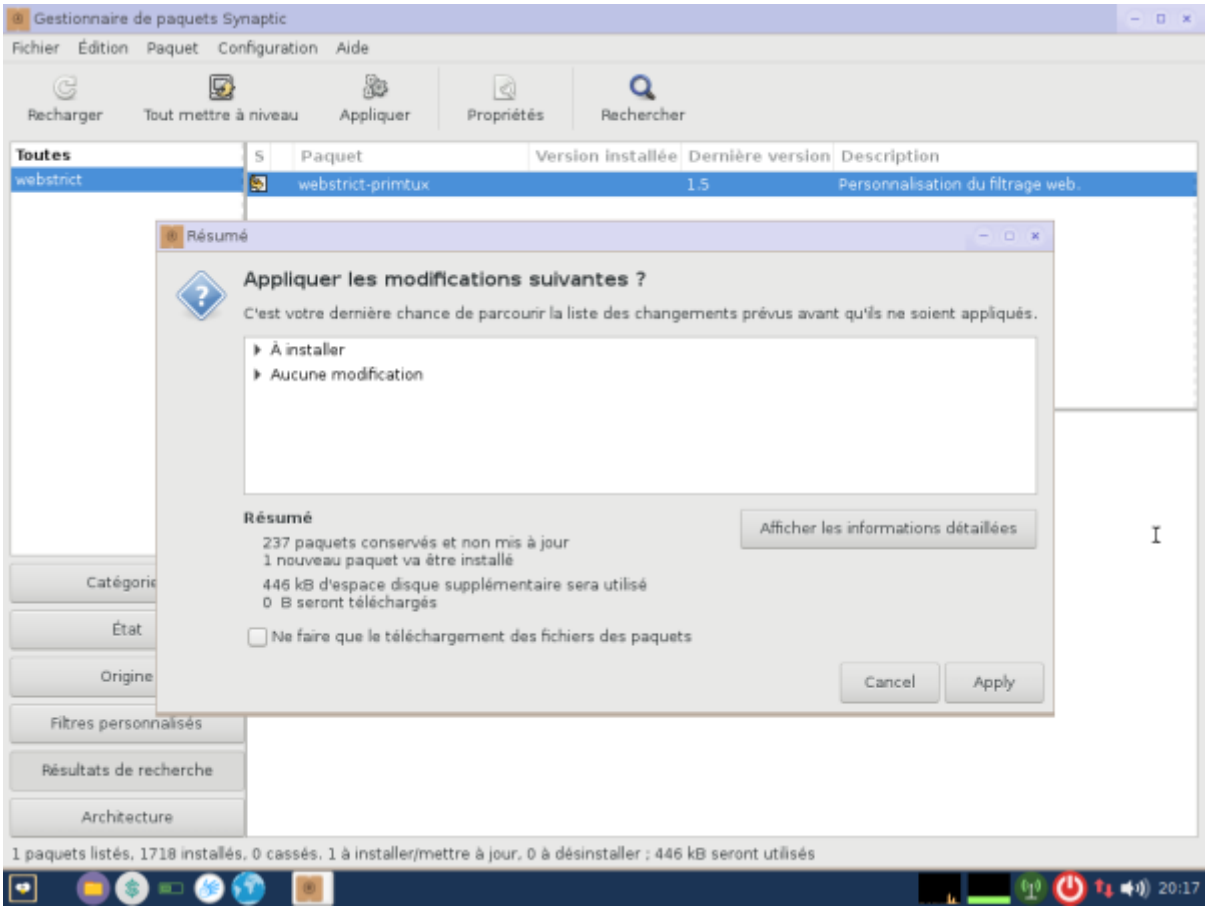
Vous pouvez ensuite démarrer Synaptic :



Cliquez sur le bouton “Rechercher” et saisissez “Webstrict” dans le champ de recherche qui apparaît. Cliquez alors sur la ligne “Webstrict-Primtux” avec le bouton droit, puis choisissez “Sélectionner pour installation”.



Confirmez les installations dans la fenêtre qui suit.



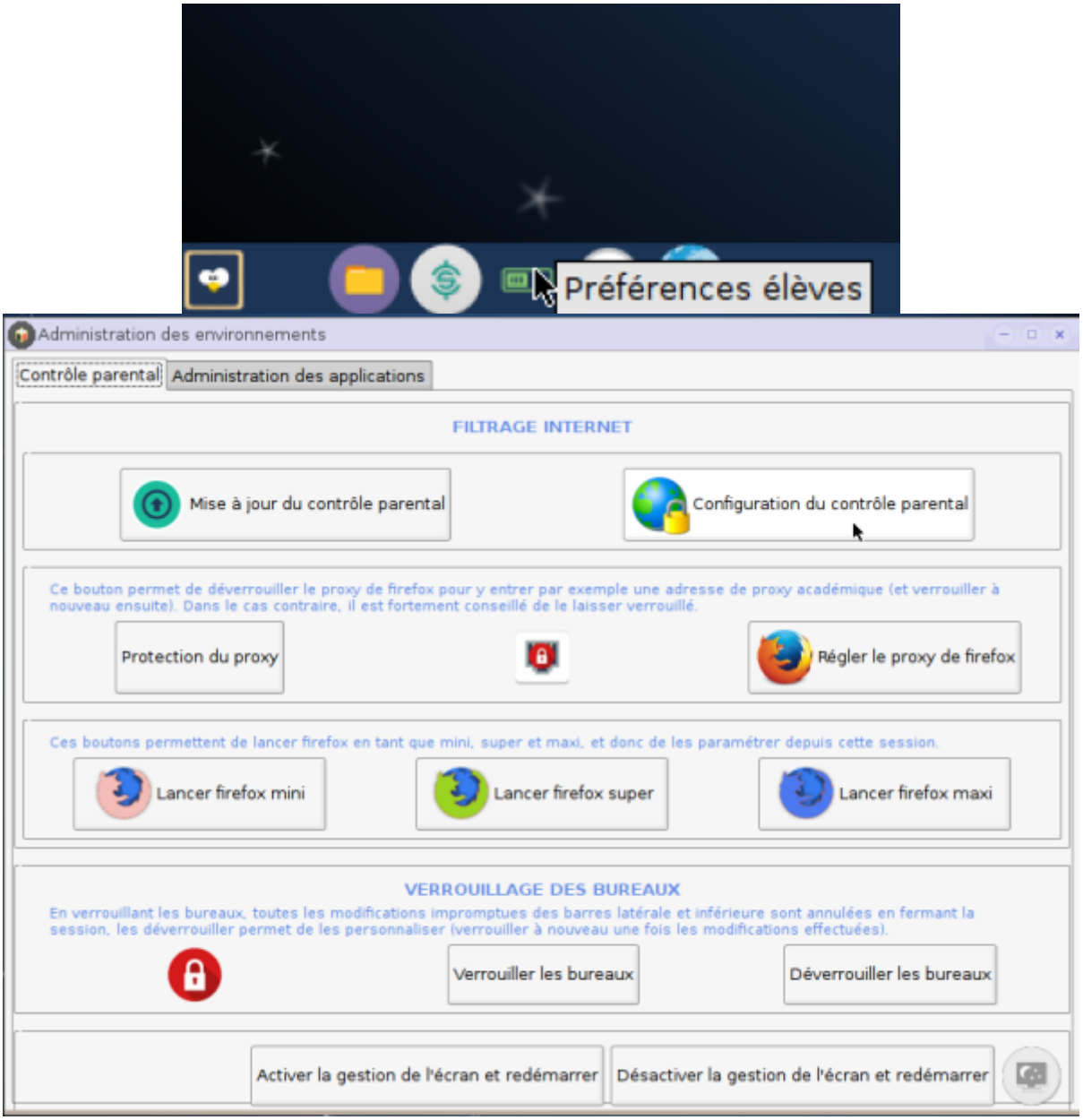
Enfin cliquez sur le bouton “Appliquer”.

Installation en ligne de commande

Ouvrez un terminal et saisissez les commandes suivantes :

```
sudo apt-get update
sudo apt-get install webstrict-primtux
```

Webstrict est maintenant accessible depuis le panneau des préférences élèves:



Paramétrage de Webstrict

En listes noires vous avez la possibilité d'interdire les accès selon divers critères :

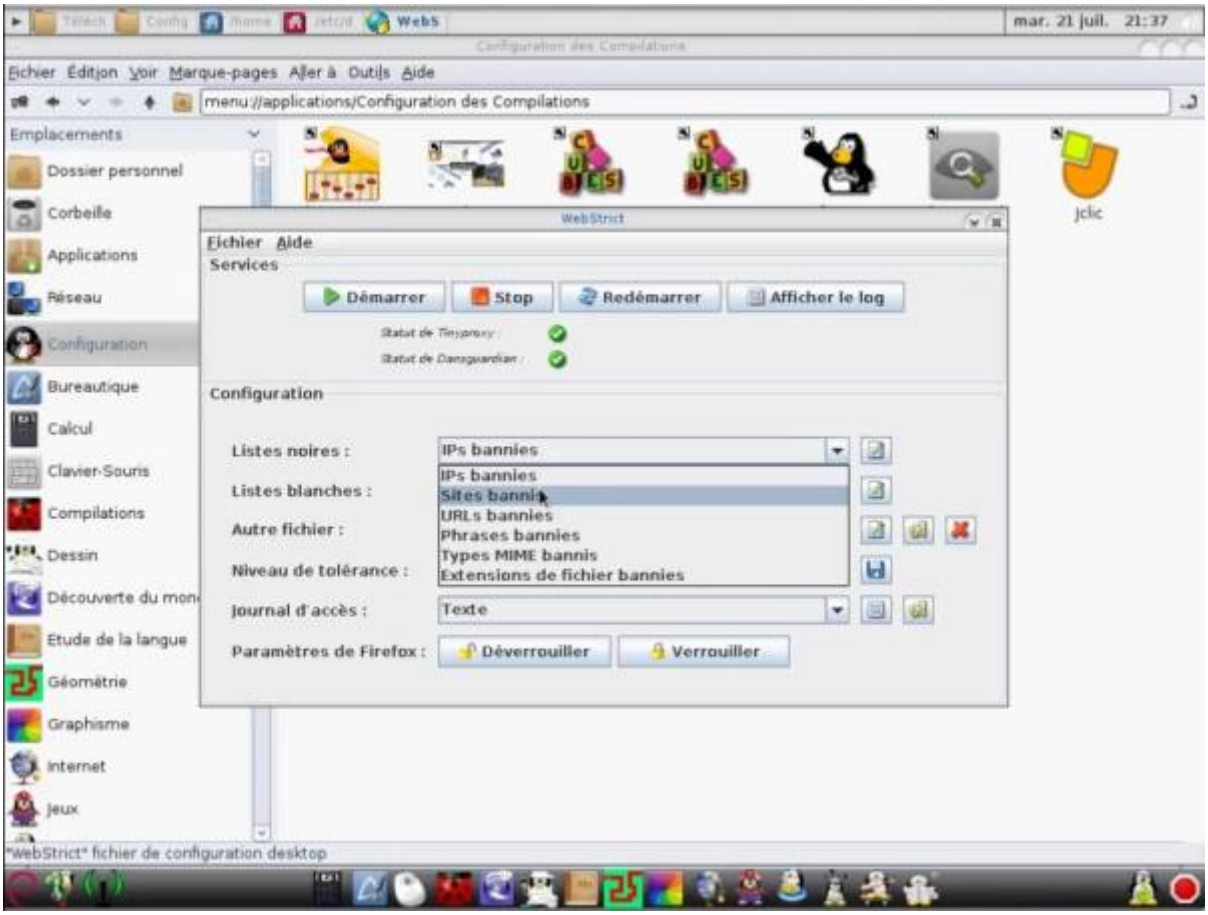
- IPs bannies permet de filtrer selon les numéros d'IP ;
- Sites bannis permet de filtrer par noms de domaine (utile pour interdire un site dans sa totalité) ;

- URLs bannies permet de filtrer des adresses précises (utile pour n'interdire que certaines pages d'un site) ;
- Phrases bannies permet d'interdire des pages si elles contiennent certains termes ;
- Types MIME bannis permet de filtrer selon le type de médias (utile pour interdire de visualiser certains types de médias) ;
- Extensions de fichiers bannies permet de filtrer selon l'extension d'un fichier (utile pour interdire le téléchargement d'un type précis de fichiers).

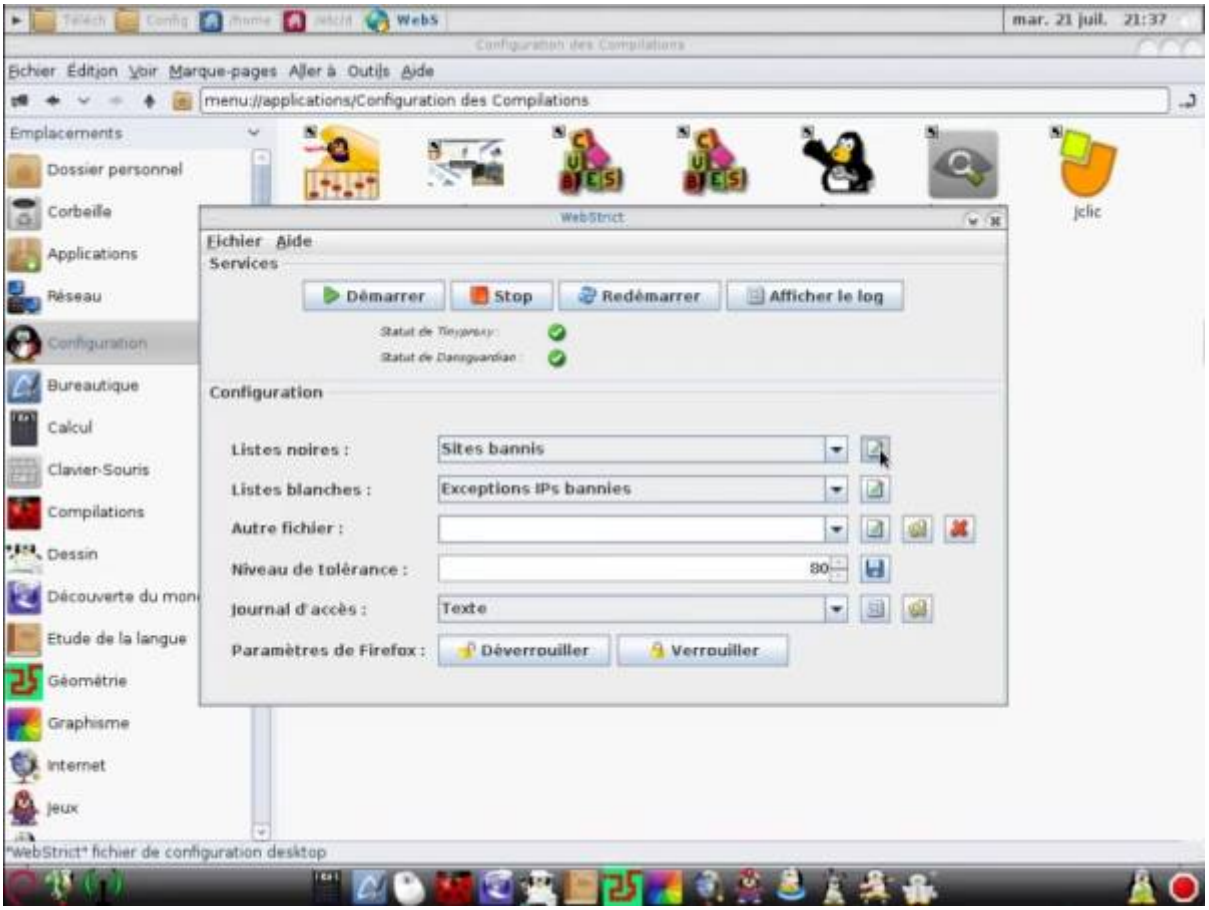
Pour chaque option, le principe est le même : après avoir sélectionné l'option choisie, on clique sur le bouton d'édition à droite du champ. Un éditeur de texte affiche le fichier des filtres qui contient des explications et des exemples en commentaires, mais en langue anglaise. En cliquant sur le bouton “Nouveau”, il est possible d'entrer une nouvelle valeur.

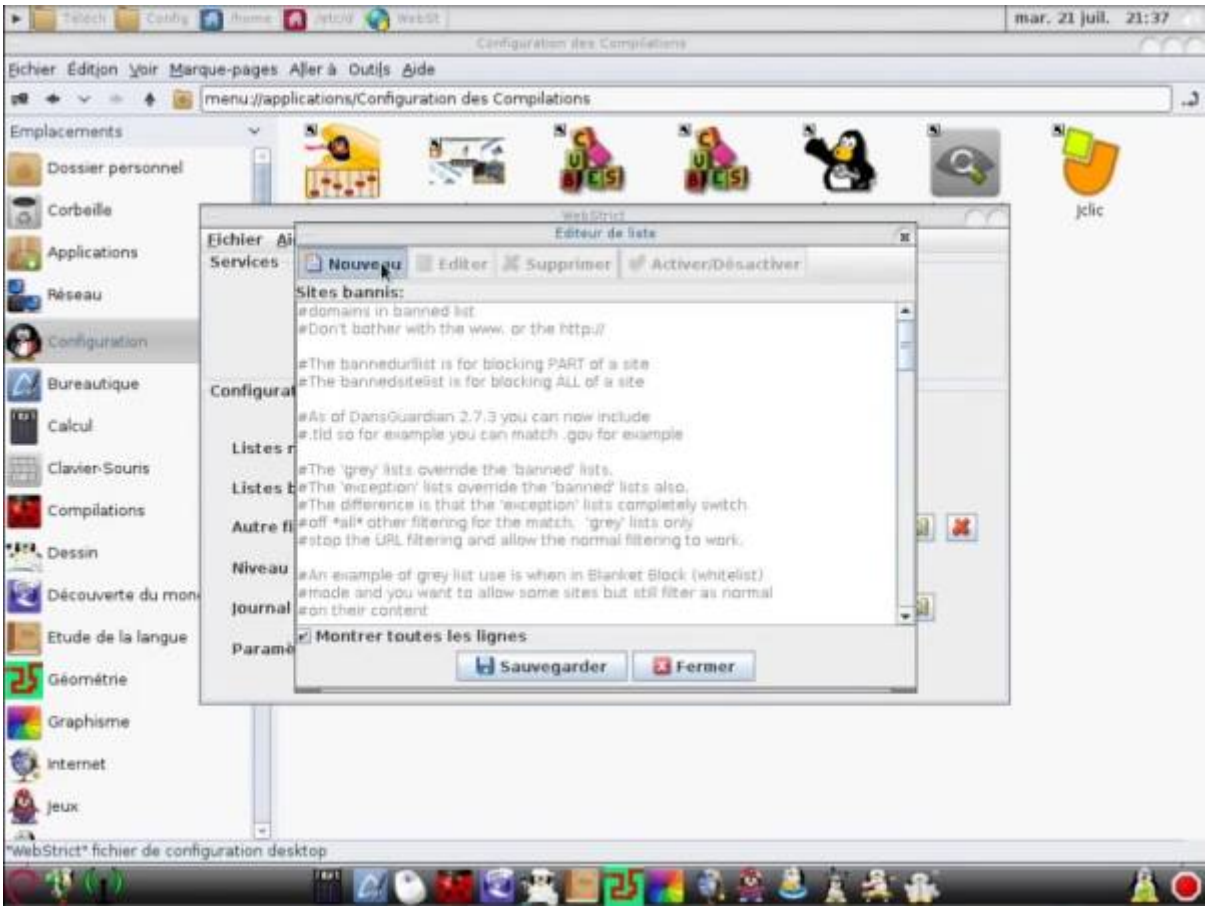
Nous allons illustrer par un exemple concret afin de mieux comprendre comment mettre en place un filtre.

Imaginons par exemple que nous désirions interdire l'accès au site de vente en ligne Amazon. Dans le champ listes noires, nous choisissons “Sites bannis” dans la fenêtre déroulante.



Nous cliquons sur l'icône d'édition, puis sur “Nouveau”:

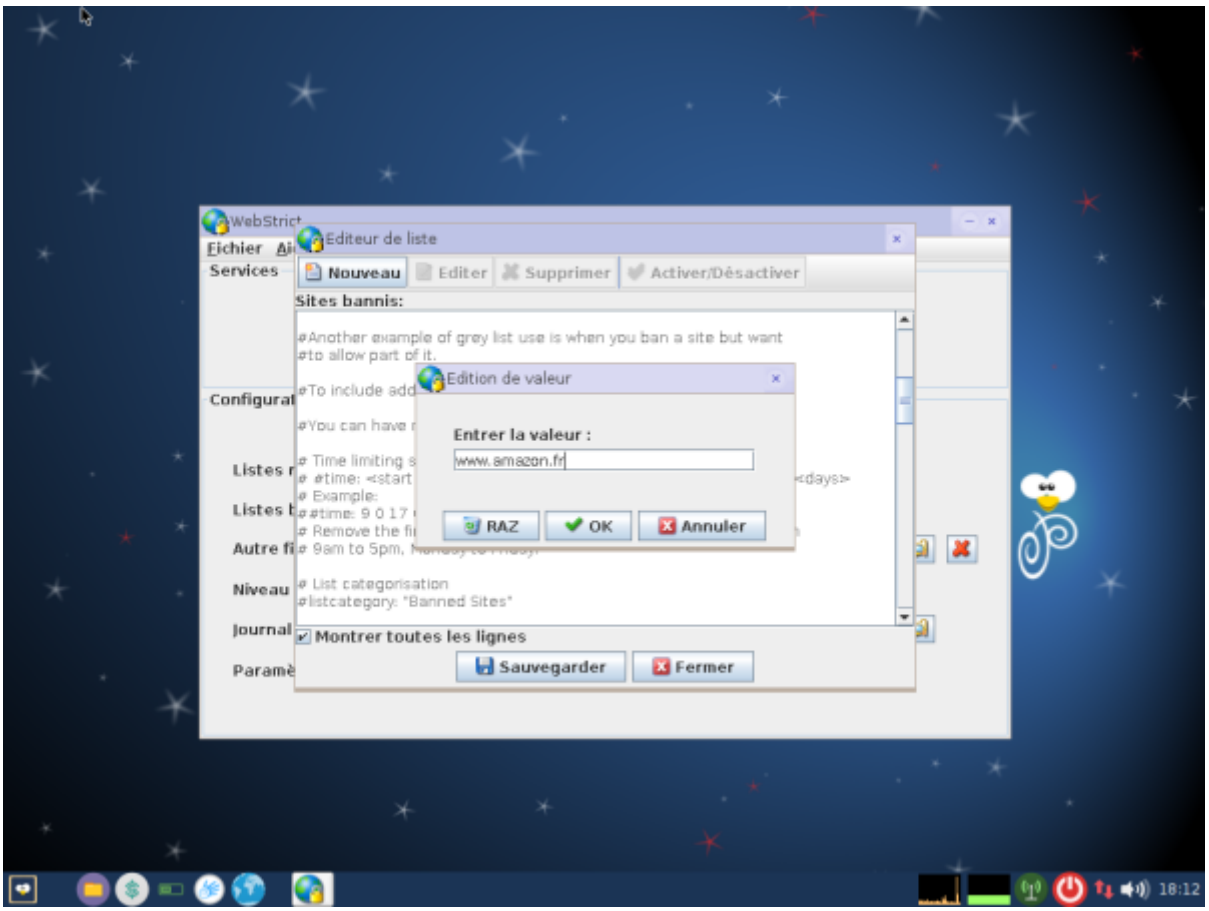


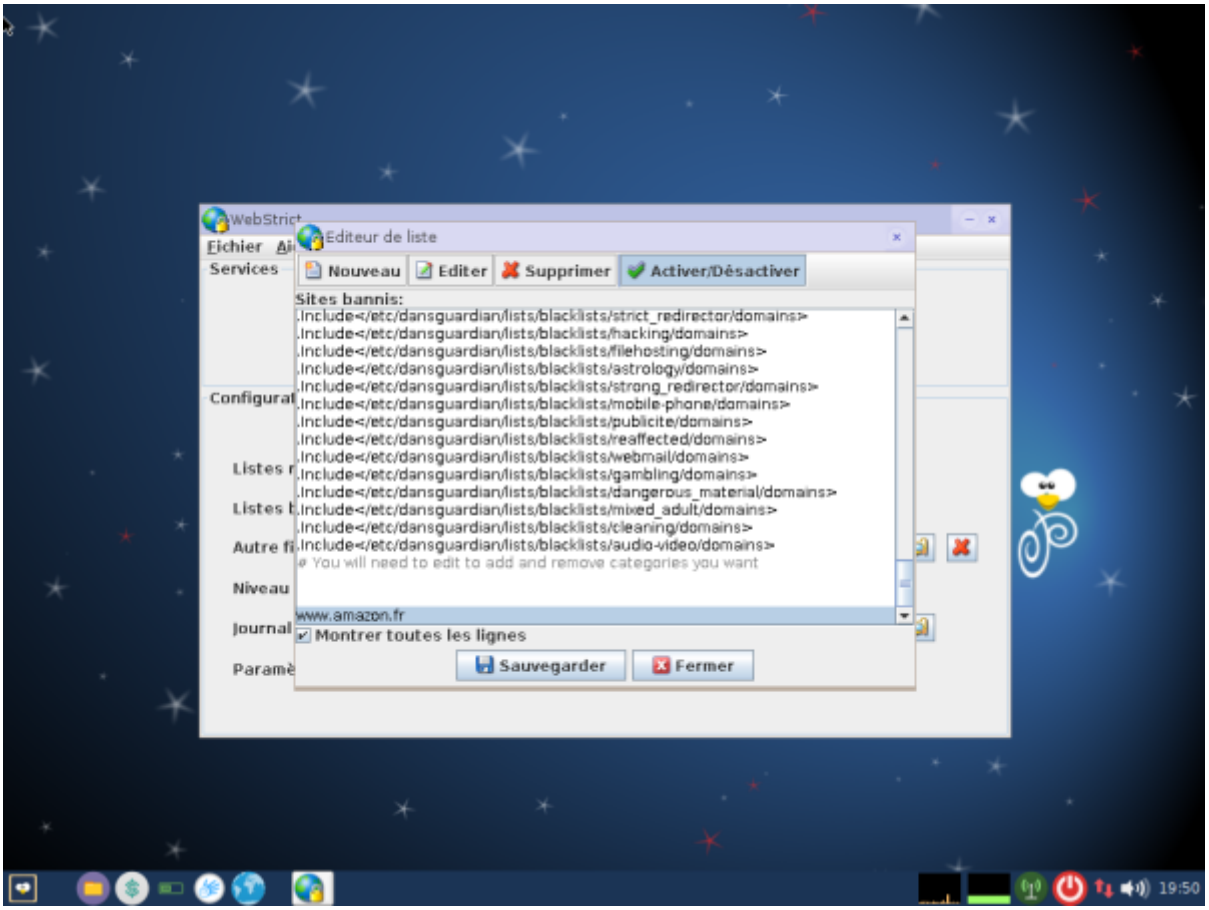


Nous entrons l'adresse du site sans http://:

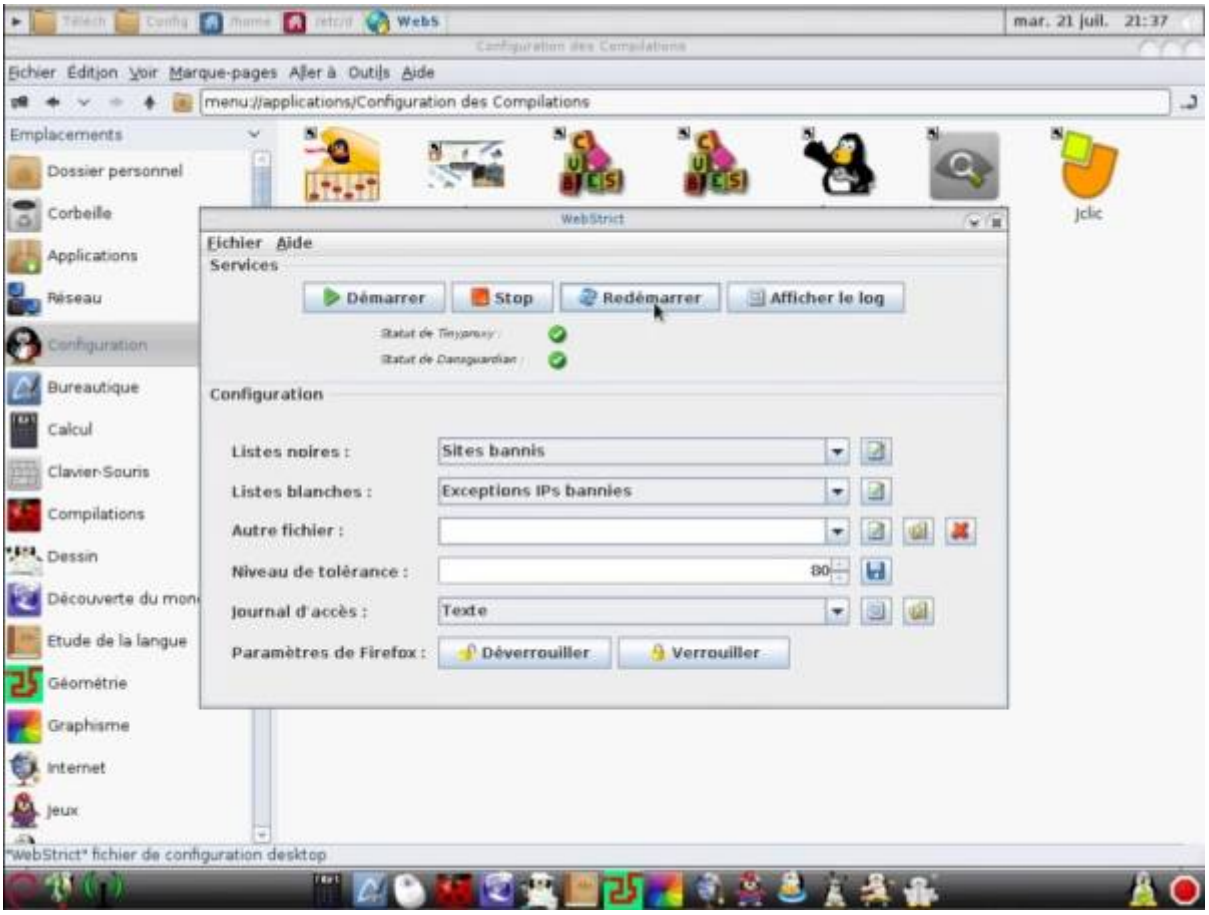
www.amazon.fr

puis nous sauvegardons :





Nous redémarrons le filtrage :

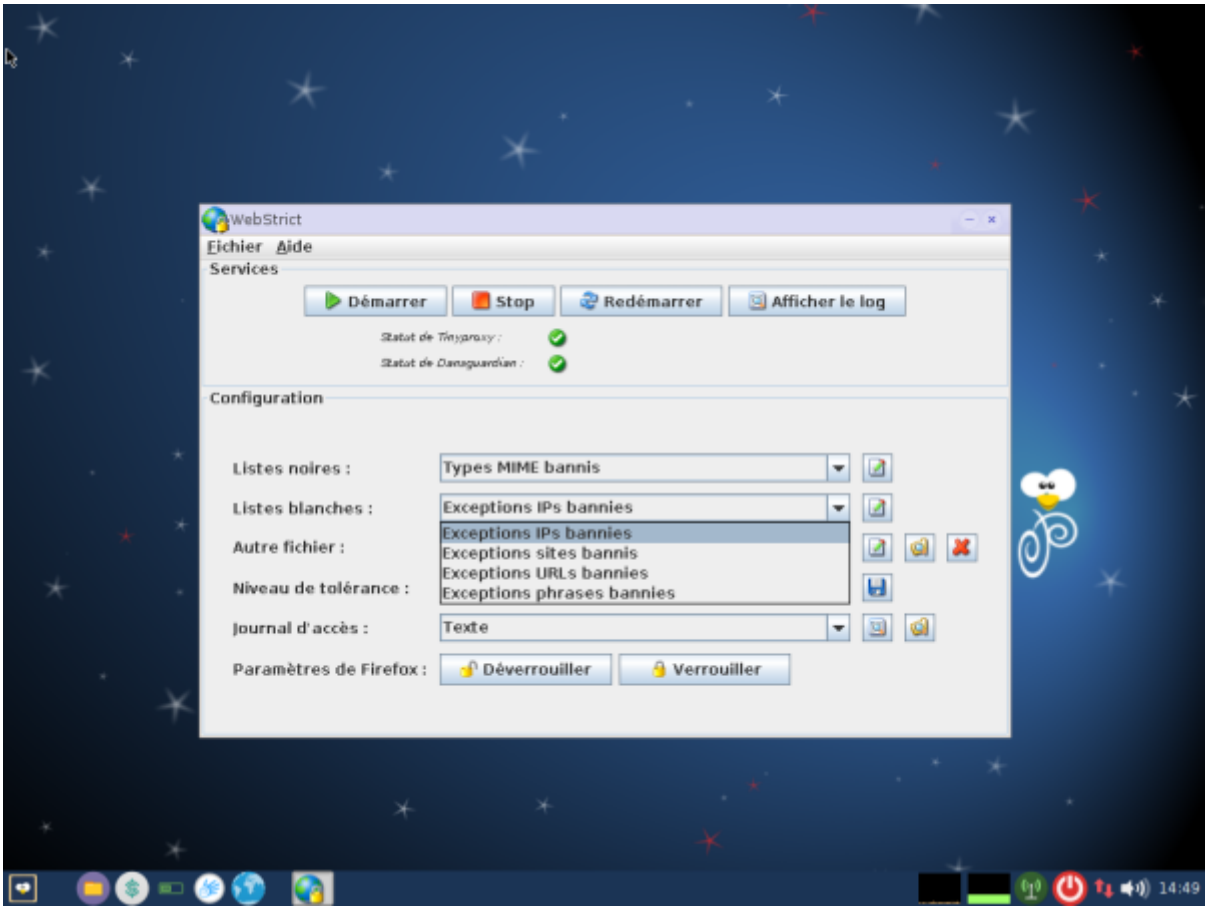


Nous pouvons tester :

Les listes blanches permettent d'ajouter des exceptions aux accès interdits. Pour une sécurité maximale, on peut ainsi tout interdire, excepté ce qui est indiqué en listes blanches. Ces exceptions peuvent être ajoutées selon les critères suivants :

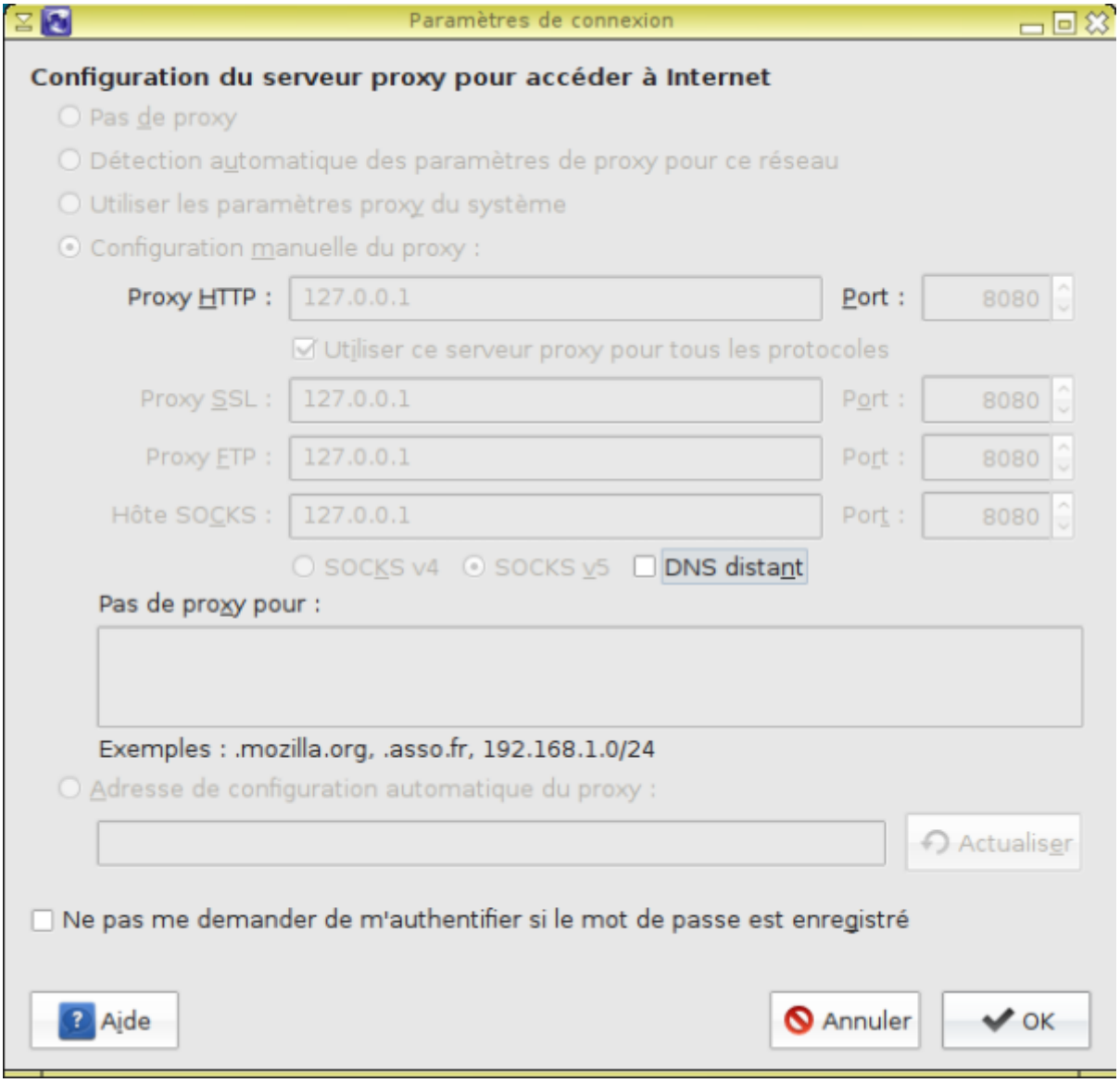
- Exceptions IPs bannies ;
- Exceptions sites bannis ;
- Exceptions URLs bannies ;
- Exceptions phrases bannies.

La méthode est identique à celle des listes noires : on sélectionne le critère dans la liste déroulante, et on clique sur le bouton d'édition à droite du champ pour ajouter des valeurs au fichier.



Modifier les paramètres de proxy de Firefox / Désactiver le contrôle parental

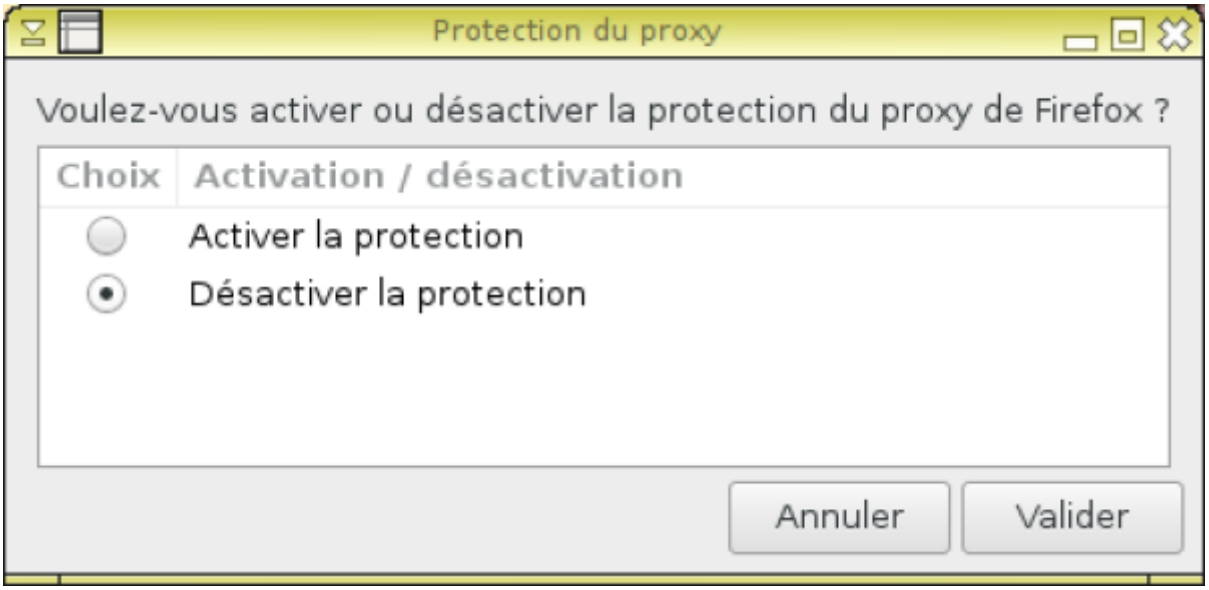
Afin de protéger les enfants des dangers de l'Internet, dès la première utilisation de Primtux, même en live, le paramétrage d'un proxy a été mis en place par défaut. Ceci est nécessaire pour que l'accès à Internet se fasse à travers DansGuardian et Webstrict qui assurent la protection. Pour la renforcer encore, une sécurité supplémentaire a été mise en place en interdisant les modifications directes des paramètres du navigateur. C'est l'outil proxy-protect qui se charge de cela.



Si vous souhaitez modifier ces paramètres, soit pour enlever le proxy, soit pour passer par un serveur académique par exemple, il vous faut tout d'abord en débloquer la modification. Voici comment faire :

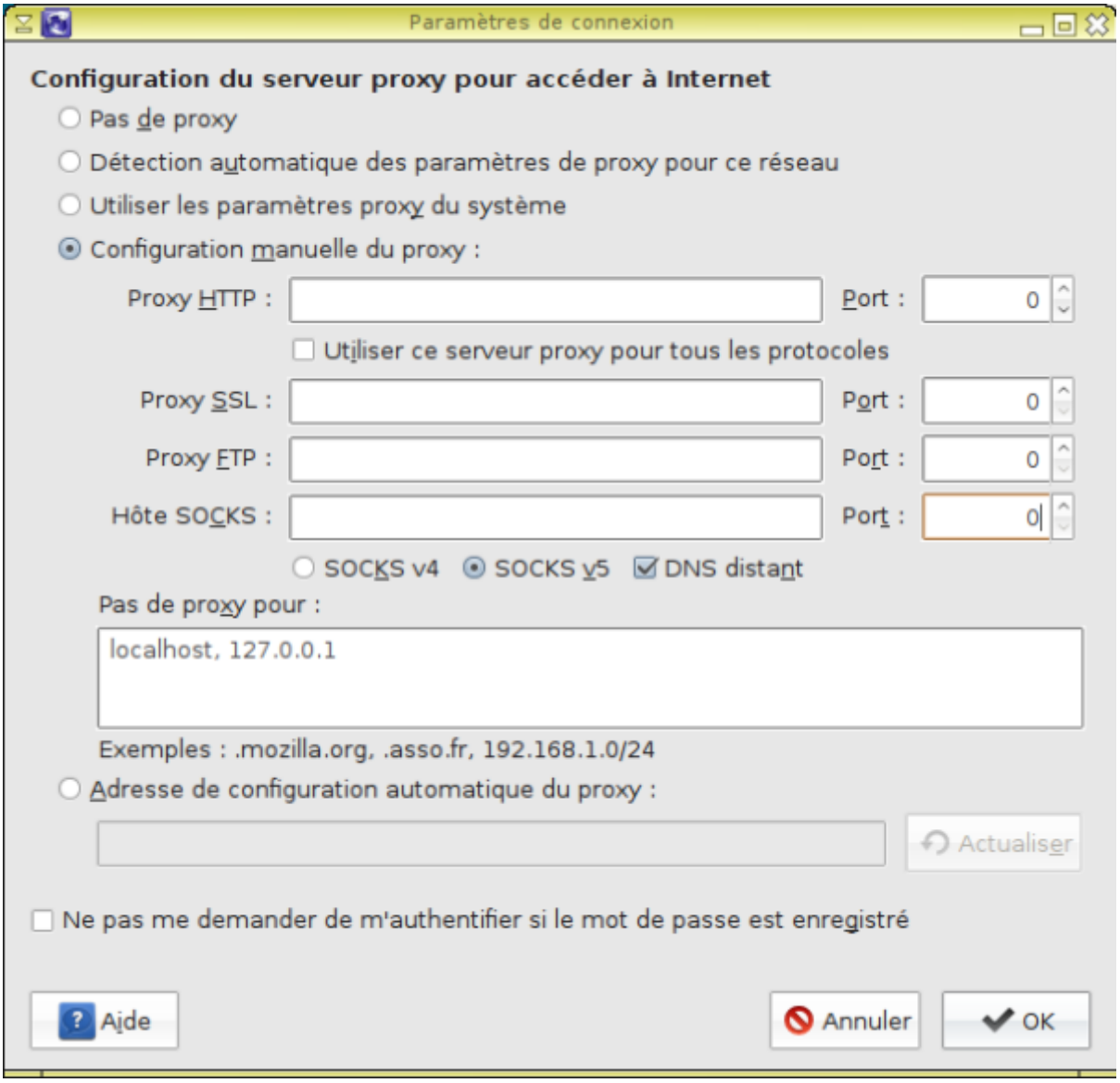
Cliquer sur l'icône du menu principal, sous-menu Internet ou Système, et lancer “Proxy protect pour Firefox”

Choisir l'option “Désactiver la protection”, puis valider.

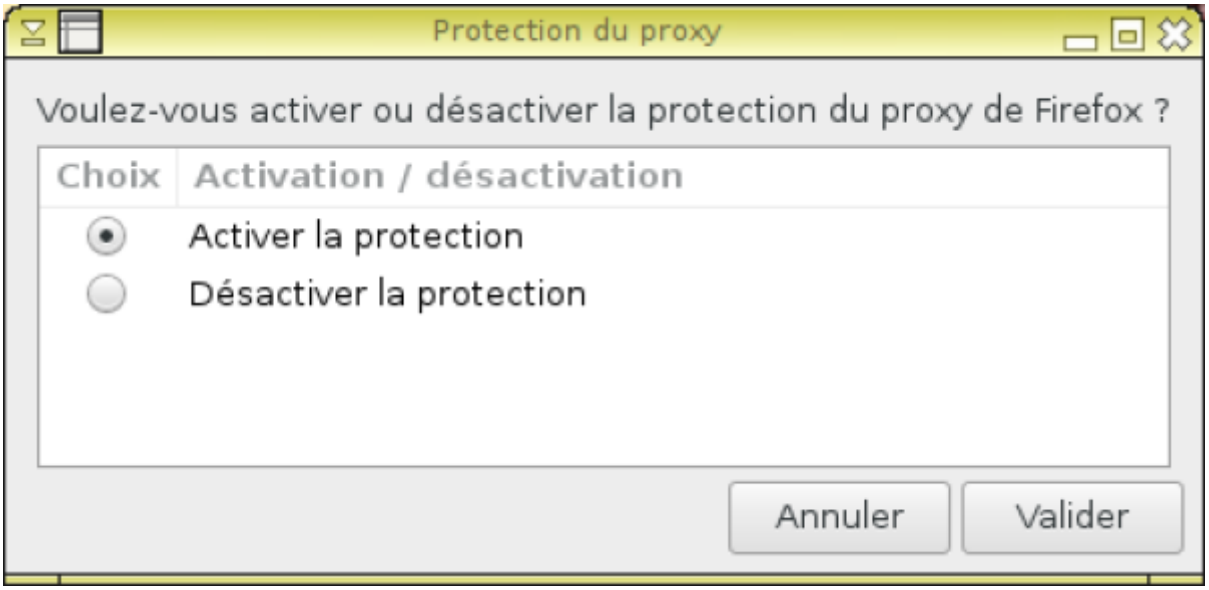


Si Firefox était en cours de fonctionnement, il faudra le redémarrer pour que cela soit pris en compte. Dans les préférences du navigateur, les paramètres réseau peuvent maintenant être modifiés librement. Pour désactiver, le contrôle parental:

⇒ Paramètres, choisir: “Pas de Proxy” ou entrer celui désiré.



Une fois vos modifications opérées, si vous souhaitez empêcher qu'elles puissent être changées, il vous suffit de relancer Proxy protect pour Firefox en choisissant cette fois “Activer la protection”. Ceci prendra effet au prochain démarrage du navigateur.



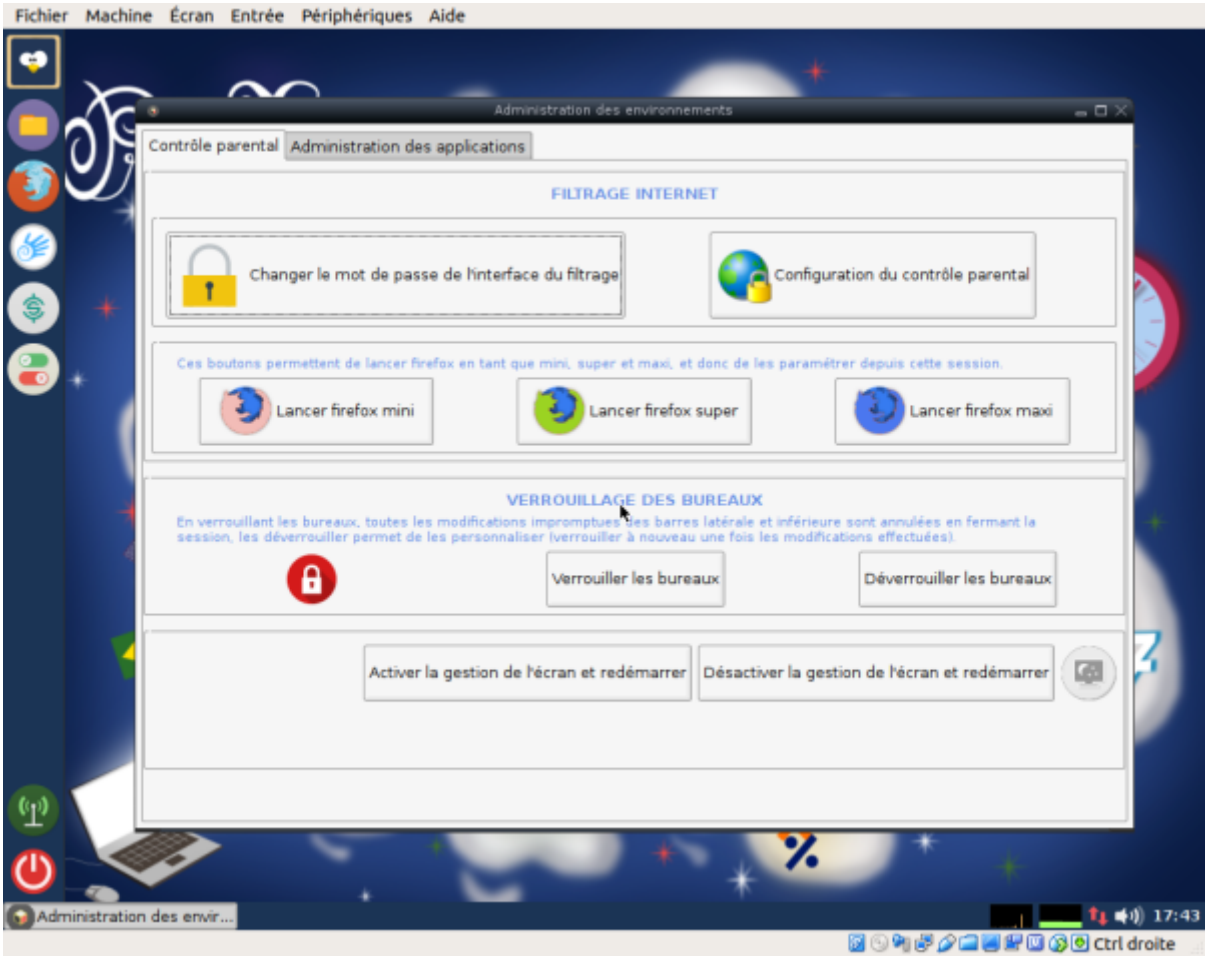
PrimTux 4

Ctparental est le nouveau filtrage utilisé par PrimTux. Contrairement à l'ancien système, il est maintenu, filtre le https, filtre tous les navigateurs sans nécessité de rentrer un proxy et permet d'affecter des horaires et des temps de connexion à ne pas dépasser quand on surfe sur internet.

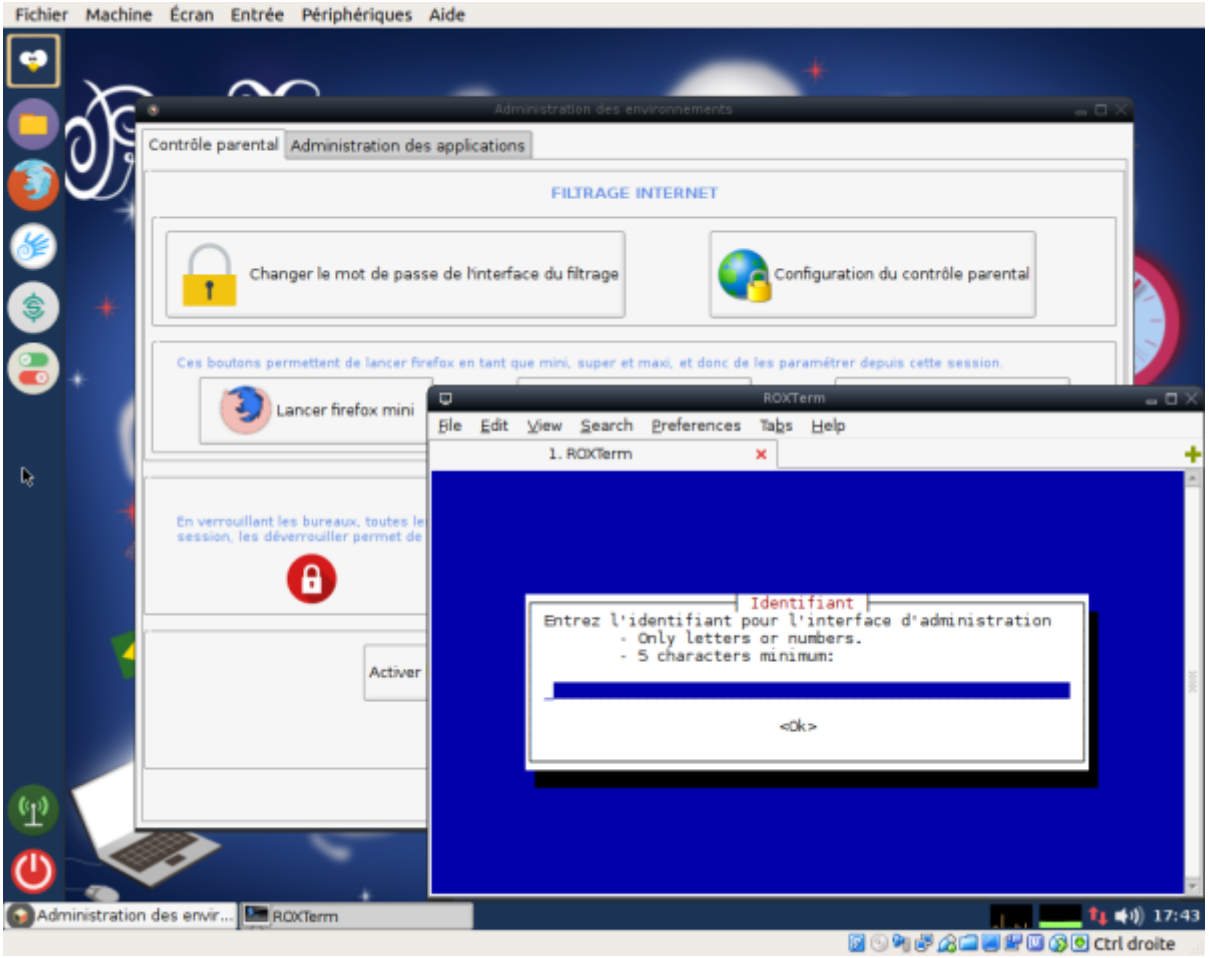
Le nom d'utilisateur et le mot de passe du filtrage sont indépendants et différents du système dans son ensemble. Il s'agit par défaut de: Nom d'utilisateur: **administrateur** / mot de passe: **PrimTux2015**

Changer le nom d'utilisateur et le mot de passe du filtrage

Si vous souhaitez les changer, il faudra passer par l'interface d'administration: dernier bouton de la barre des taches (avec les curseurs verts et rouges), puis cliquer sur “Changer le mot de passe de l'interface de filtrage”. Dans la fenêtre du terminal qui s'ouvre, il faut entrer le mot de passe système (tuxprof).

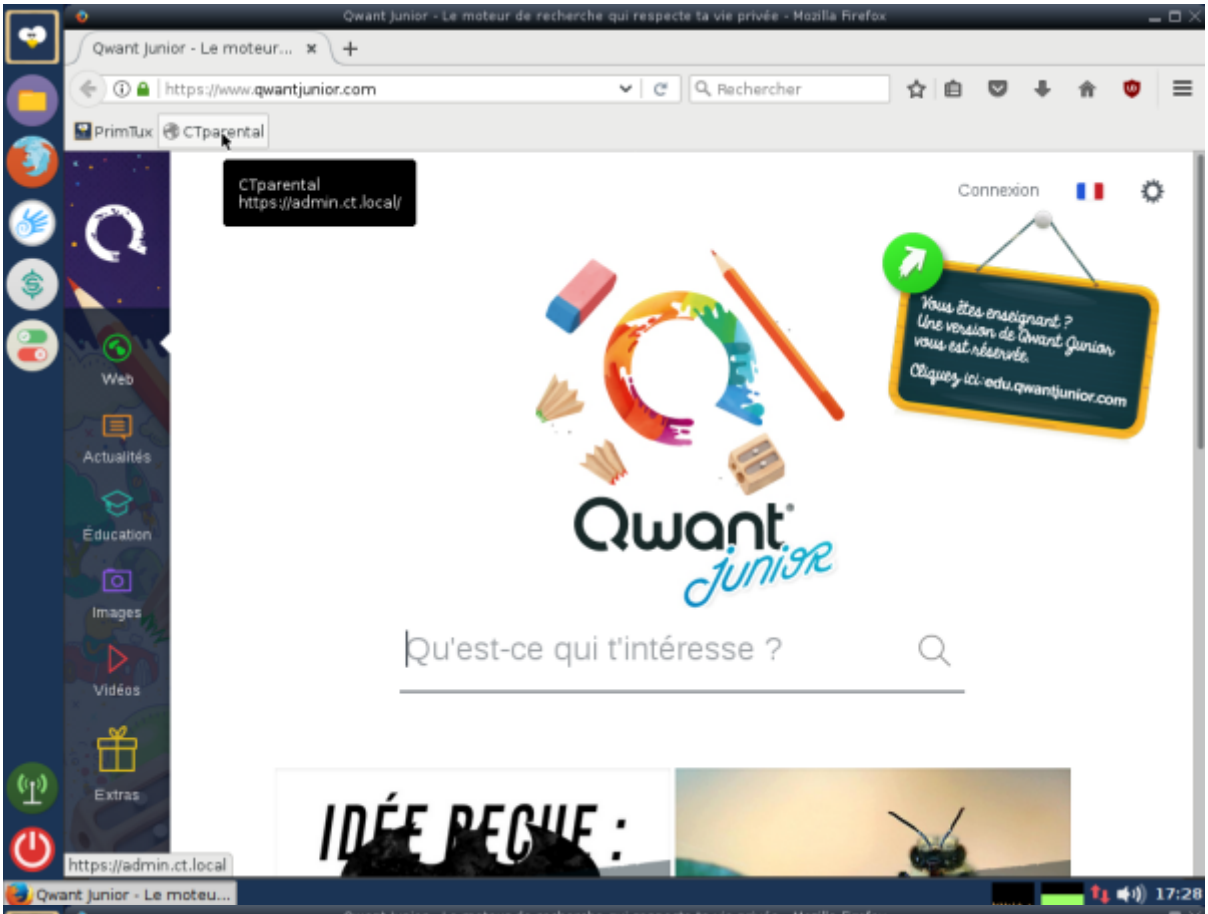


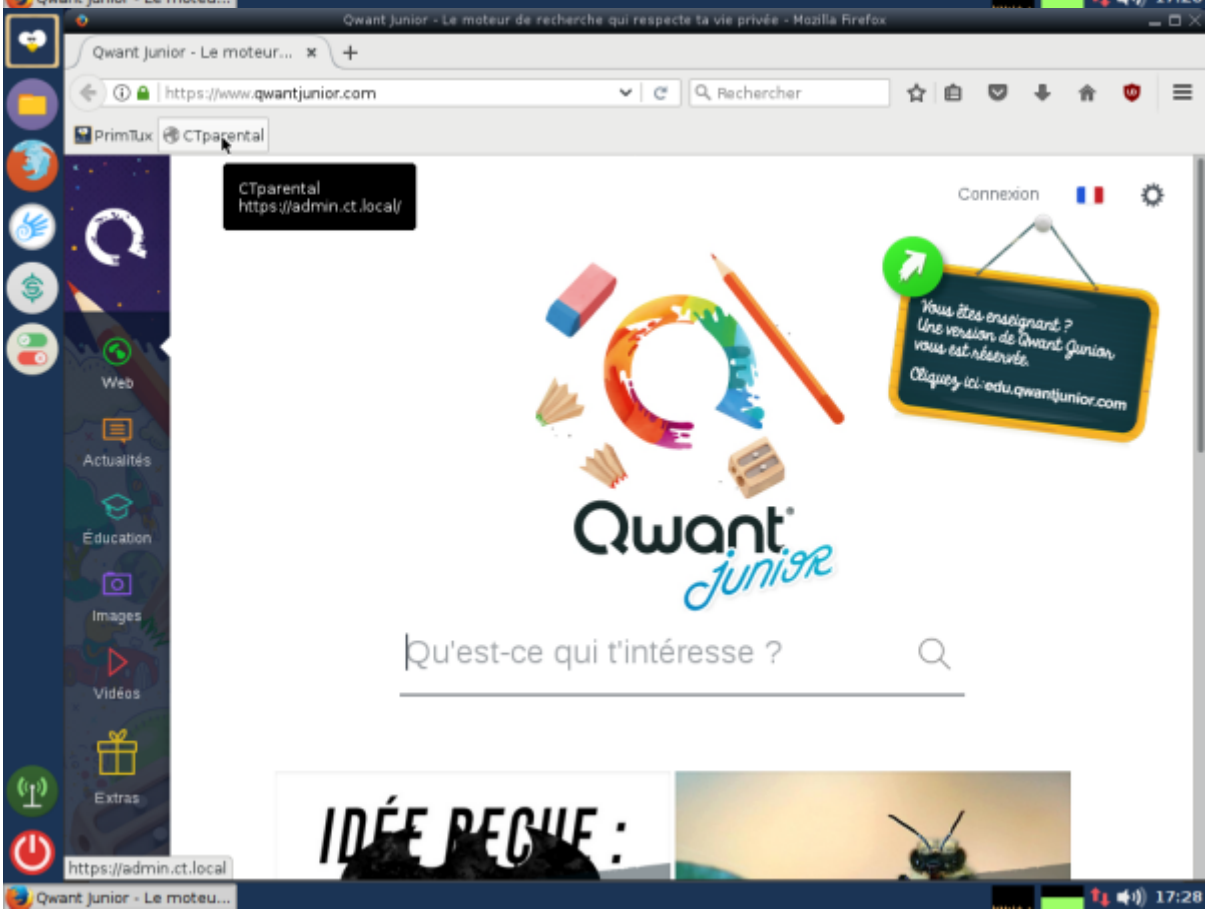
Il faudra ensuite entrer un nouveau nom d'utilisateur, puis son mot de passe. Attention, ce mot de passe doit comporter au moins 8 caractères, un chiffre et une majuscule.



Connexion à l'interface de filtrage

Ouvrir firefox, cliquer sur “CTParental” et entrer administrateur / PrimTux2015 (sauf si changés selon la procédure expliquée ci-dessus).

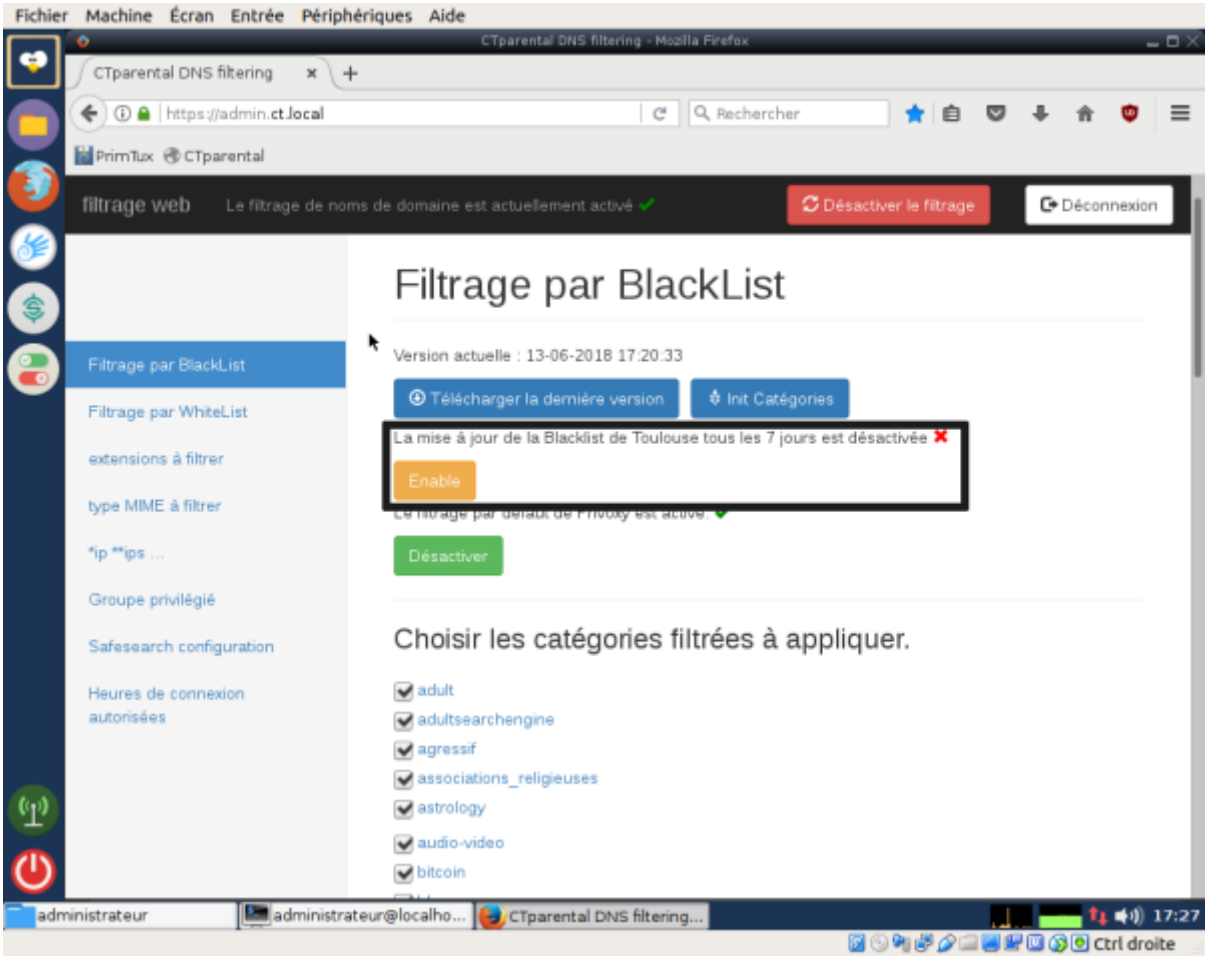




Mise à jour des listes de filtrage

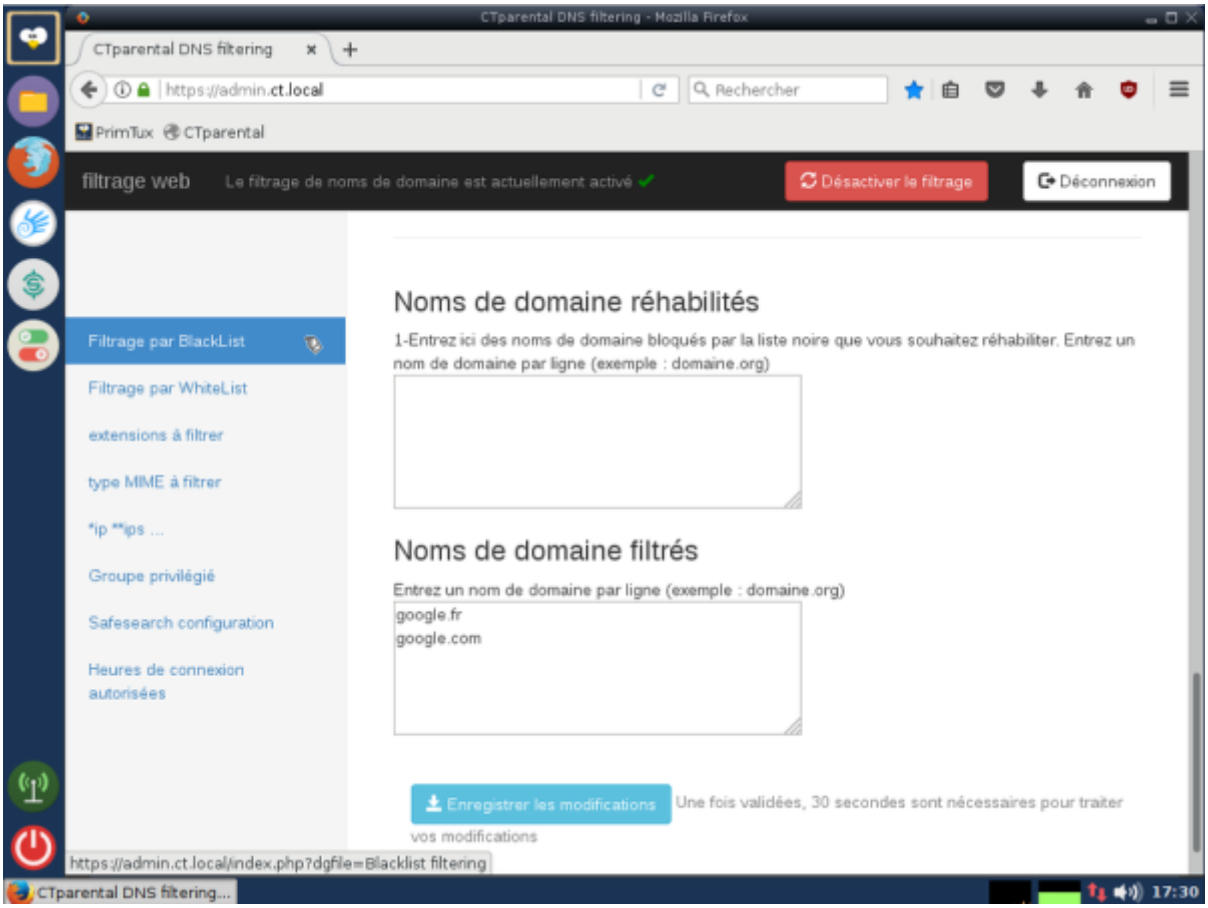
Cliquez sur “Enable” pour activer cette mise à jour de manière hebdomadaire, sur “Télécharger la

dernière version” pour mettre les listes à jour immédiatement. Vous pouvez aussi choisir les catégories à filtrer (tout est filtré par défaut dans PrimTux). On n'oublie pas de cliquer sur “Enregistrer les modifications” (bouton situé tout en bas de la page).



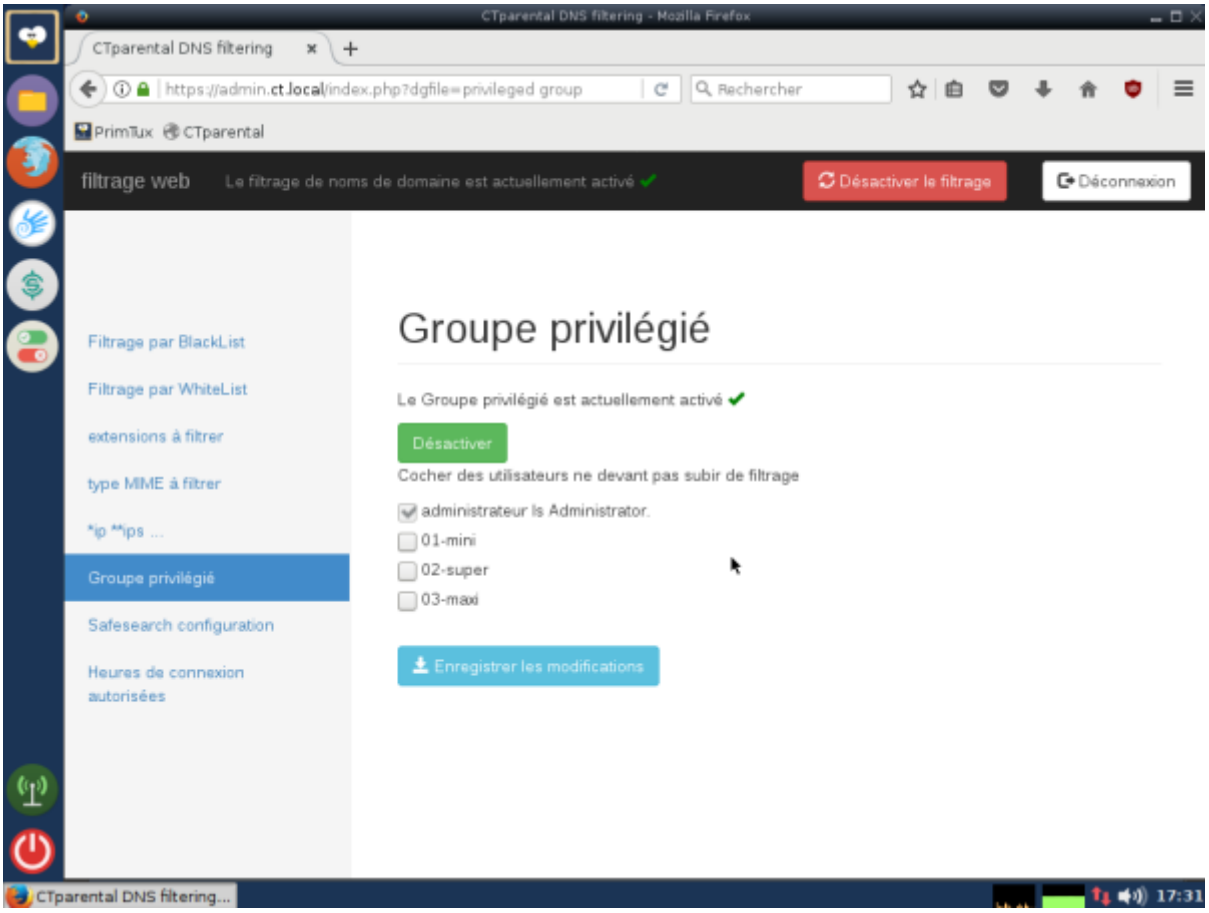
Ajout de sites dans la liste blanche et noire

Il faut aller tout en bas de cette page pour les ajouter dans les cadres adéquats. On n'oublie pas de cliquer sur “Enregistrer les modifications”.



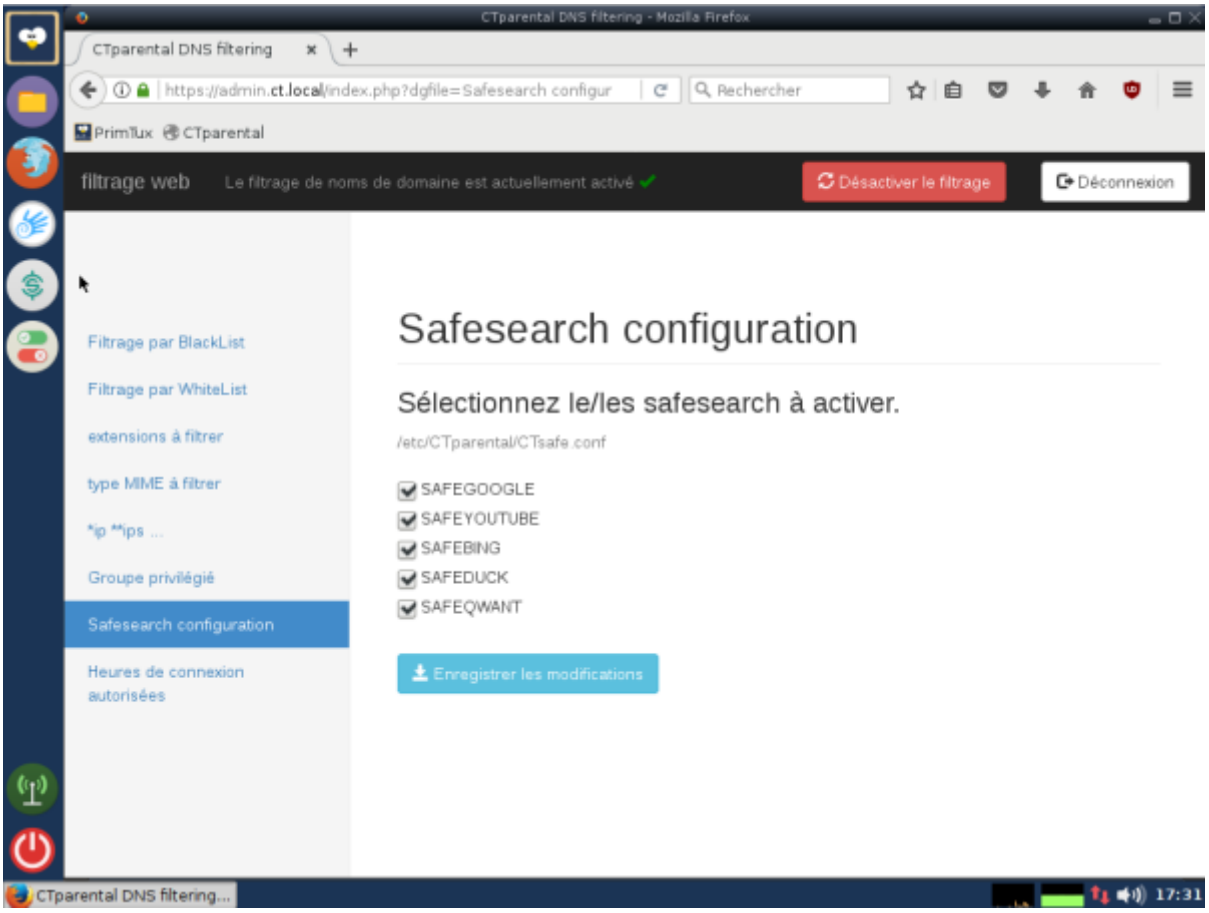
Utilisateurs privilégiés

Les utilisateurs cochés ne sont pas filtrés.



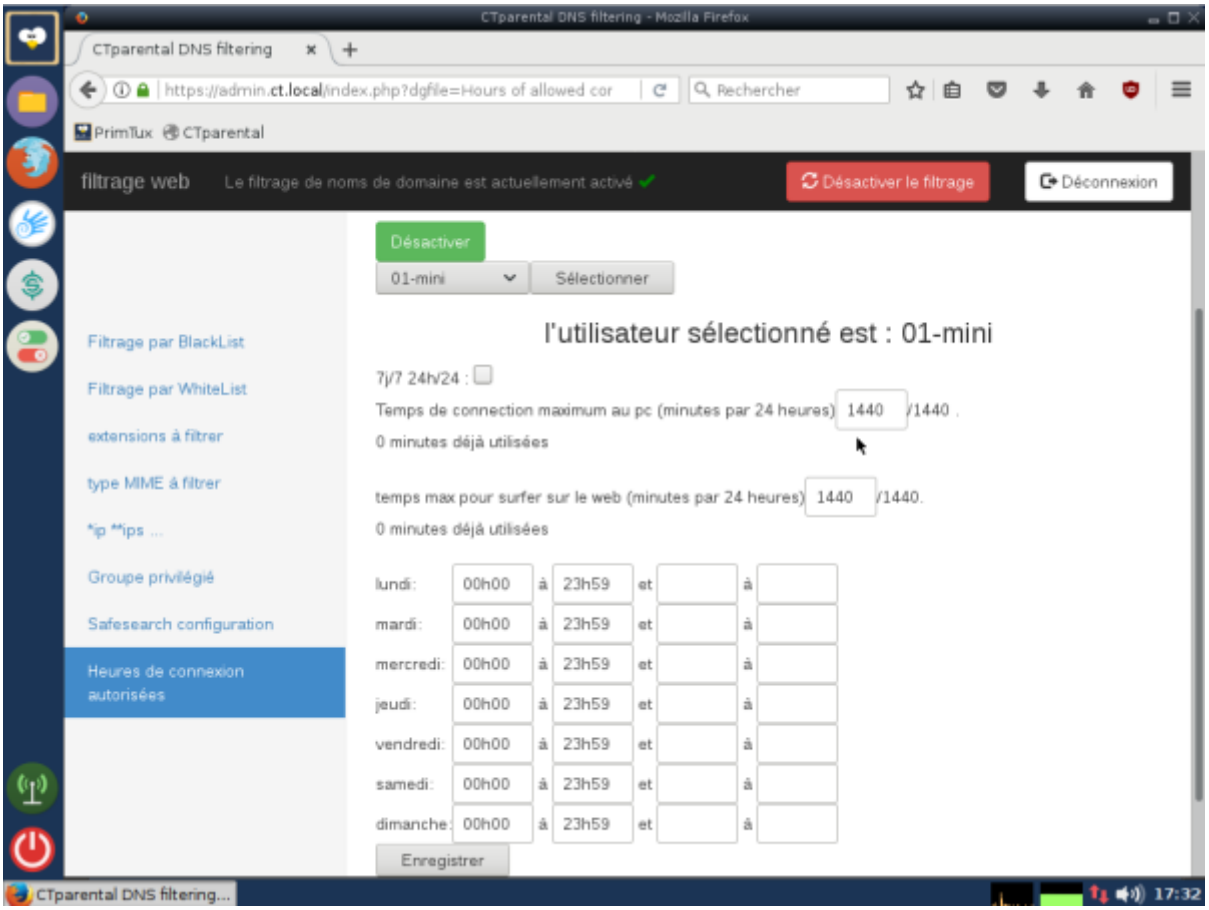
Bloquer les résultats explicites

Activer la safesearch permet de bloquer les résultats indésirables sur les sites mentionnés:



Limiter les horaires et temps de connexion d'un utilisateur

Décocher 7j/7 24h/24, puis choisir l'utilisateur concerné et entrer les limites souhaitées. Ne pas oublier d'enregistrer.



From:
https://www.wikiwiki.primtux.fr/ - **PrimTux - Wiki**

Permanent link:
https://www.wikiwiki.primtux.fr/doku.php/controle_parental_ccm

Last update: **2022/10/04 17:49**