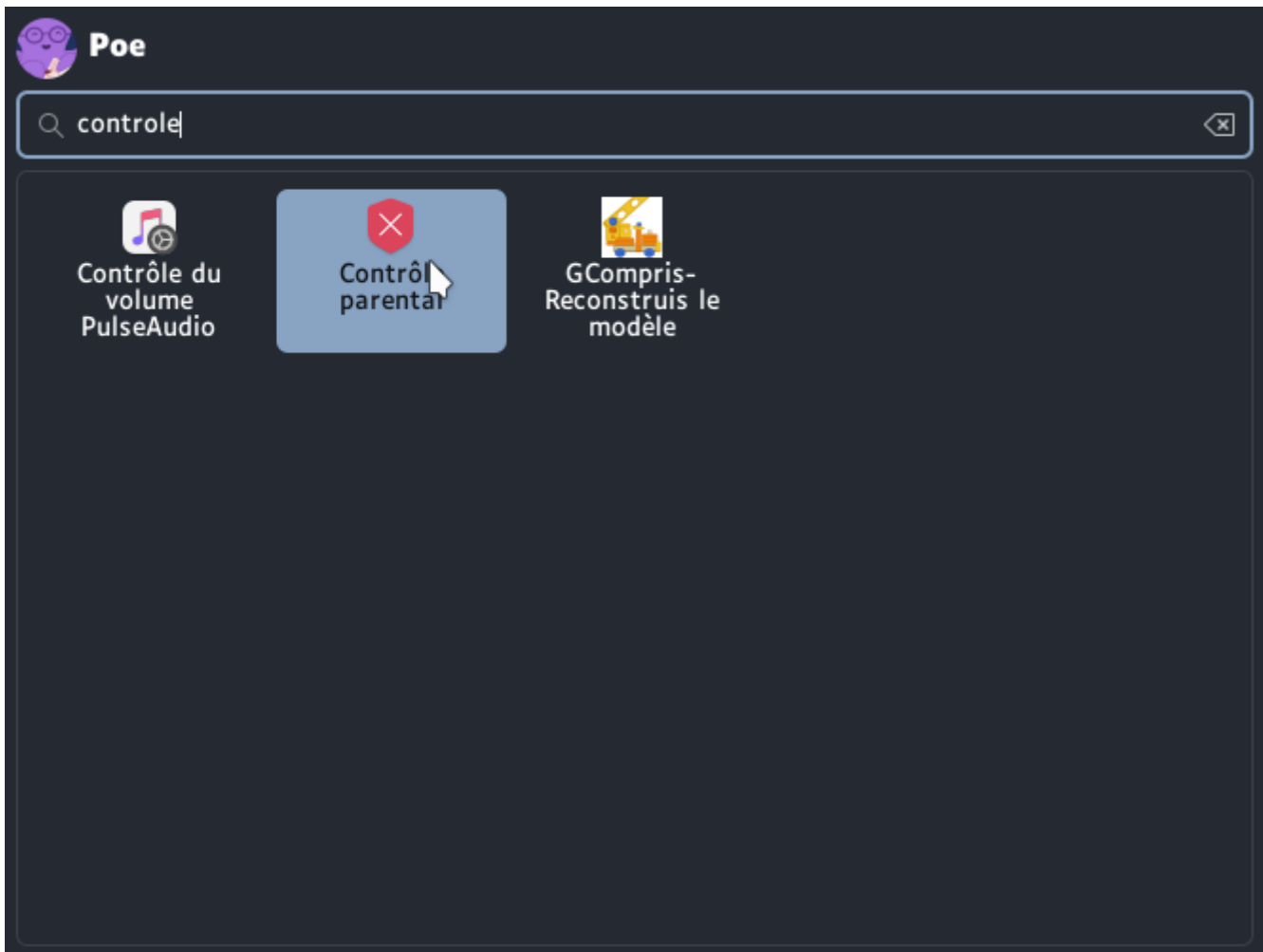


Réglages divers

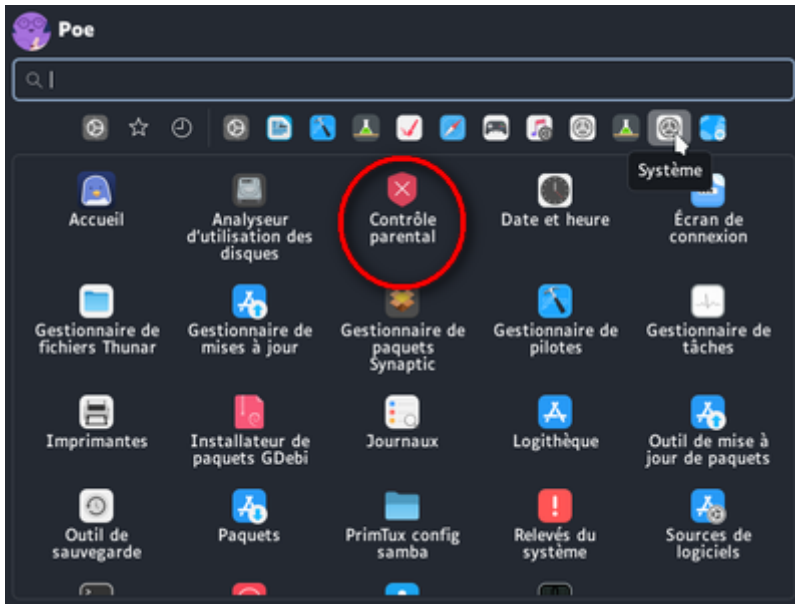
- [Configuration du contrôle parental](#)
- [Ré-initialiser un compte élève](#)
- [Connexion automatique à une session](#)
- [Blocage d'Internet pour les sessions élèves](#)

Configuration du contrôle parental

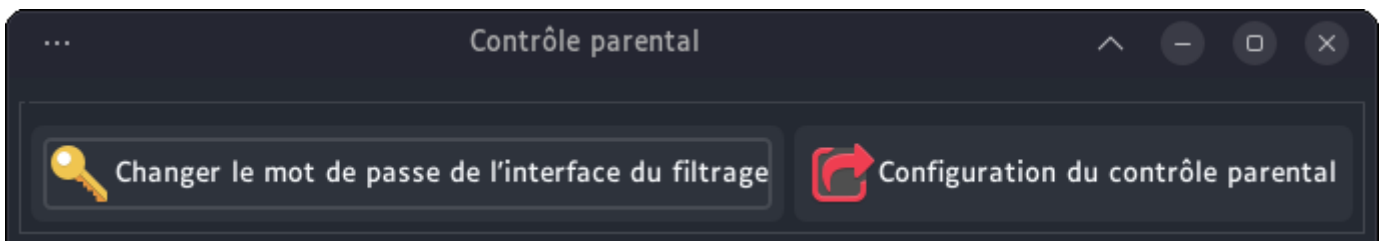
Pour modifier les règles de contrôle parental, il faut aller dans le menu principal, et saisir « contrôle » dans la barre de recherche. Dans les icônes qui apparaissent, on clique sur « Contrôle parental » :



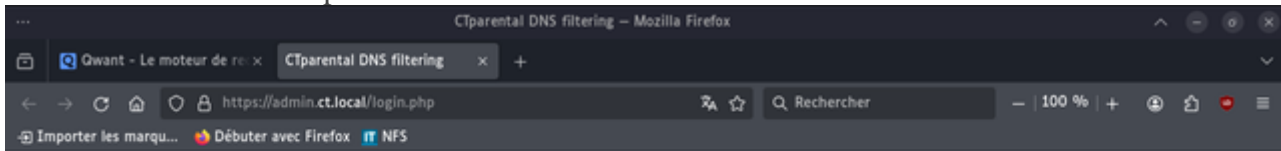
On peut également y accéder depuis ce même menu dans la catégorie "Système" (seconde roue dentée) :



Une boîte de dialogue permet de choisir entre changer le mot de passe et modifier la configuration :



Il est demandé le nom d'utilisateur et le mot de passe. Ce sont les identifiants qui ont été saisis lors de l'installation du contrôle parental :



Interface d'administration de CTparental

Identifiant :

Mot de passe :

Plusieurs pages permettant différents réglages sont à disposition.

Page filtrage par blacklist

Dans cette page on sélectionne les sites qui seront autorisés ou interdits, par mots clés ou bien par nom de domaine. Pour le filtrage par mots clés, toutes les cases cochées interdiront les sites liés à ces mots clés, toutes les cases non cochées les autoriseront :

CTparental DNS filtering – Mozilla Firefox

Qwant - Le moteur de re... CTparental DNS filtering x +

https://admin.ct.local/index.php

Rechercher

100 %

Importeur les marqu... Débuter avec Firefox NFS

filtrage web Le filtrage de noms de domaine est actuellement activé ✓

Désactiver le filtrage Déconnexion

Filtrage par BlackList

Version actuelle : 16-04-2024 17:45:18

Télécharger la dernière version Init Catégories

La mise à jour de la blacklist de Toulouse tous les 7 jours est activée ✓

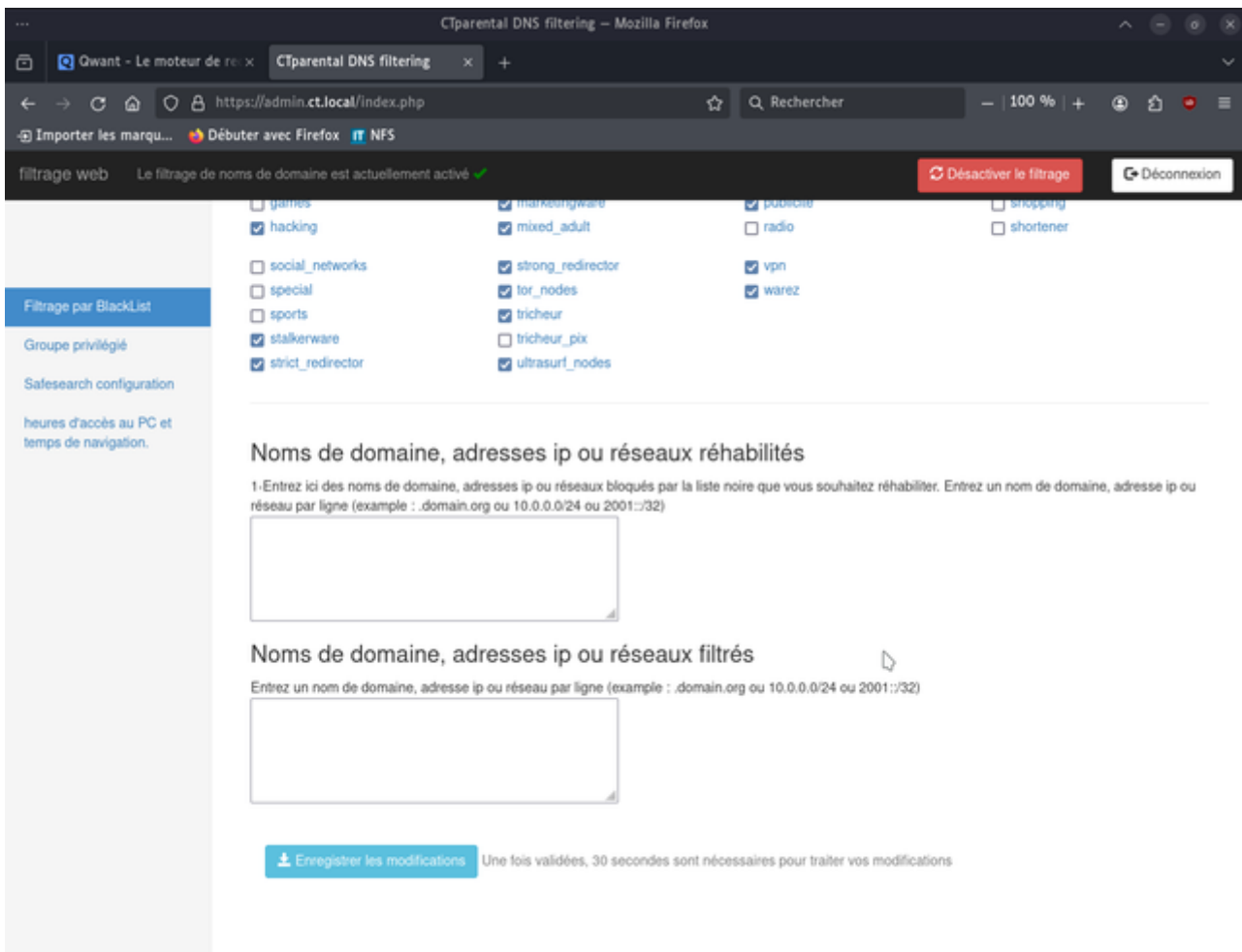
Désactiver

Basculer en Whitelist

Choisir les catégories filtrées à appliquer.

<input checked="" type="checkbox"/> adult	<input type="checkbox"/> audio-video	<input checked="" type="checkbox"/> ct_doh_dot_doq	<input type="checkbox"/> dialer
<input checked="" type="checkbox"/> adultsearchengine	<input checked="" type="checkbox"/> bitcoin	<input checked="" type="checkbox"/> ctparental	<input checked="" type="checkbox"/> doh
<input checked="" type="checkbox"/> agressif	<input type="checkbox"/> blog	<input checked="" type="checkbox"/> dangerous_material	<input checked="" type="checkbox"/> drogue
<input type="checkbox"/> associations_religieuses	<input type="checkbox"/> celebrity	<input checked="" type="checkbox"/> dating	<input type="checkbox"/> exceptions_liste_bu
<input type="checkbox"/> astrology	<input checked="" type="checkbox"/> cryptojacking	<input checked="" type="checkbox"/> ddos	<input type="checkbox"/> filehosting
<input type="checkbox"/> financial	<input type="checkbox"/> lingerie	<input type="checkbox"/> mobile-phone	<input type="checkbox"/> reaffected
<input type="checkbox"/> forums	<input checked="" type="checkbox"/> malware	<input checked="" type="checkbox"/> phishing	<input checked="" type="checkbox"/> redirector
<input checked="" type="checkbox"/> gambling	<input type="checkbox"/> manga	<input type="checkbox"/> press	<input checked="" type="checkbox"/> sect
<input type="checkbox"/> games	<input checked="" type="checkbox"/> marketingware	<input checked="" type="checkbox"/> publicite	<input type="checkbox"/> shopping
<input checked="" type="checkbox"/> hacking	<input checked="" type="checkbox"/> mixed_adult	<input type="checkbox"/> radio	<input type="checkbox"/> shortener
<input type="checkbox"/> social_networks	<input checked="" type="checkbox"/> strong_redirector	<input checked="" type="checkbox"/> vpn	
<input type="checkbox"/> special	<input checked="" type="checkbox"/> tor_nodes	<input checked="" type="checkbox"/> warez	
<input type="checkbox"/> sports	<input checked="" type="checkbox"/> tricheur		
<input checked="" type="checkbox"/> stalkerware	<input type="checkbox"/> tricheur_pix		
<input checked="" type="checkbox"/> strict_redirector	<input checked="" type="checkbox"/> ultrasurf_nodes		

Plus bas sur la page, des zones de saisie permettent d'indiquer précisément des noms de domaine que l'on veut réhabiliter (dont on veut autoriser l'accès), ou interdire explicitement :



Si par exemple on veut interdire l'accès au moteur de recherche google, il faudra saisir dans la zone "Noms de domaine, adresses ip ou réseaux filtrés, les divers noms de domaine ou ip de ce moteur de recherche, notamment

google. fr

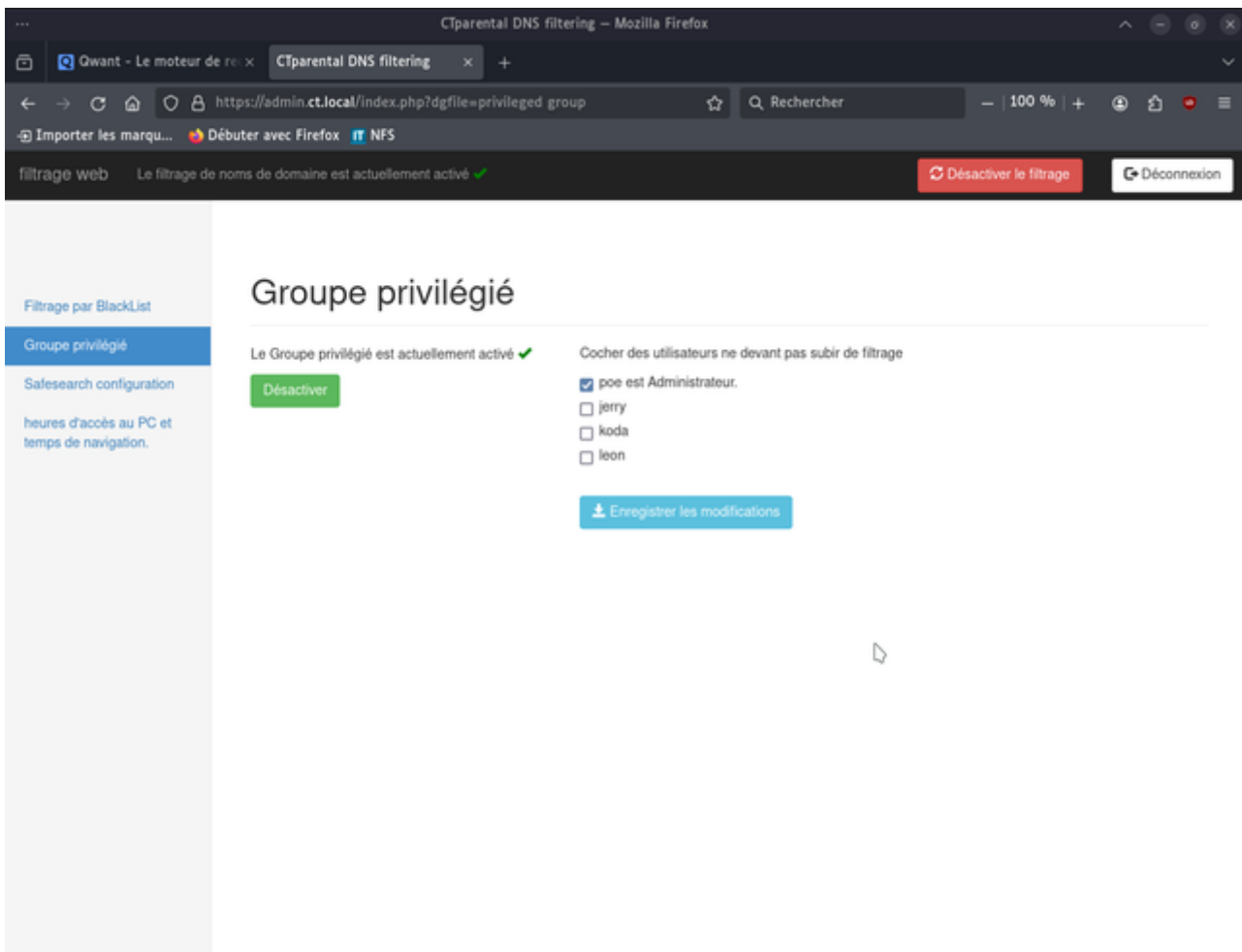
www. google. fr

google. com

www. google. com

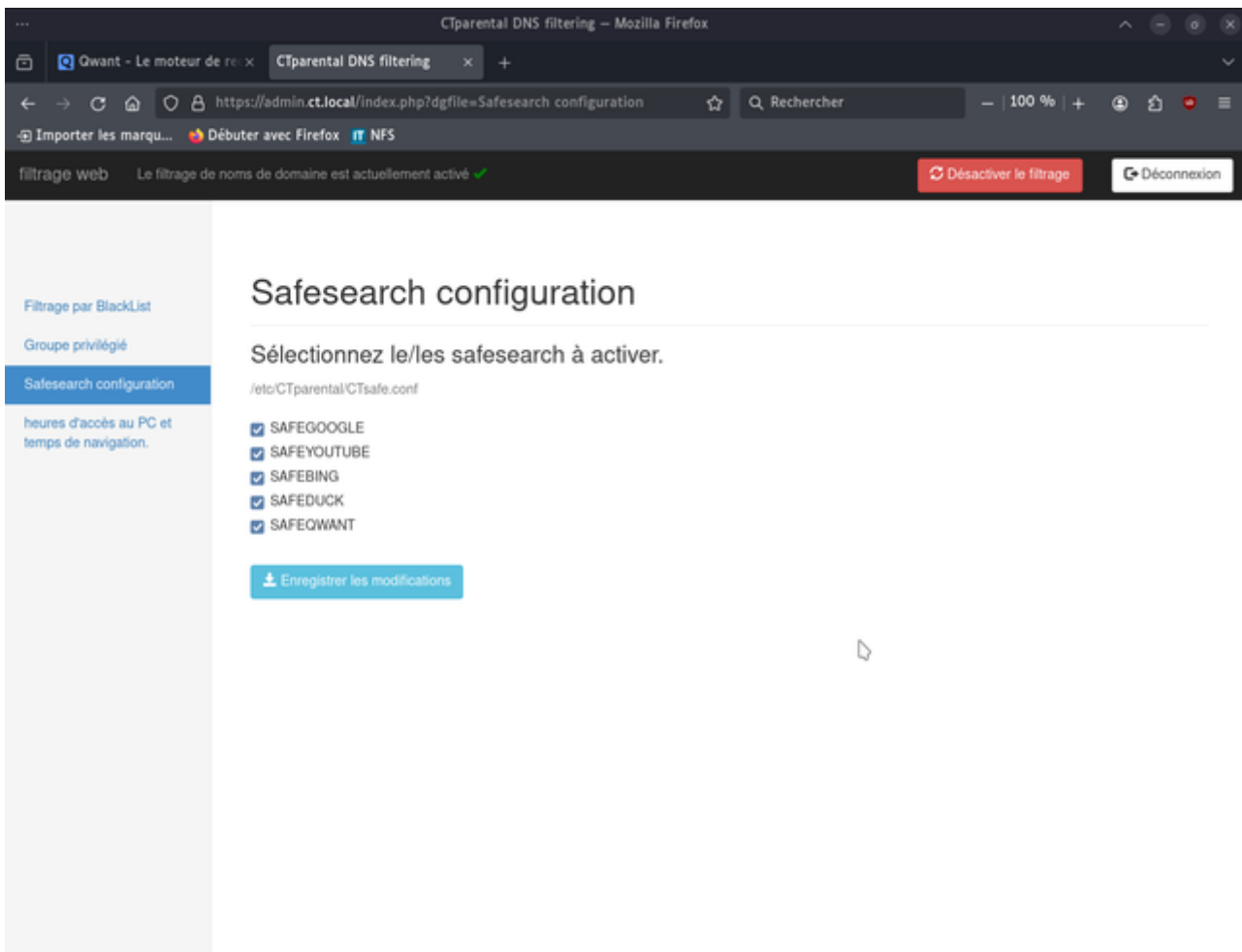
Page groupe privilégié

Dans cette page, on pourra sélectionner les sessions pour lesquelles le contrôle parental s'exercera le contrôle parental. Pour que le filtrage ne soit pas actif, il faut cocher les cases des sessions correspondantes. Ici, le filtrage est actif pour toutes les sessions sauf la session Poe (administrateur) :



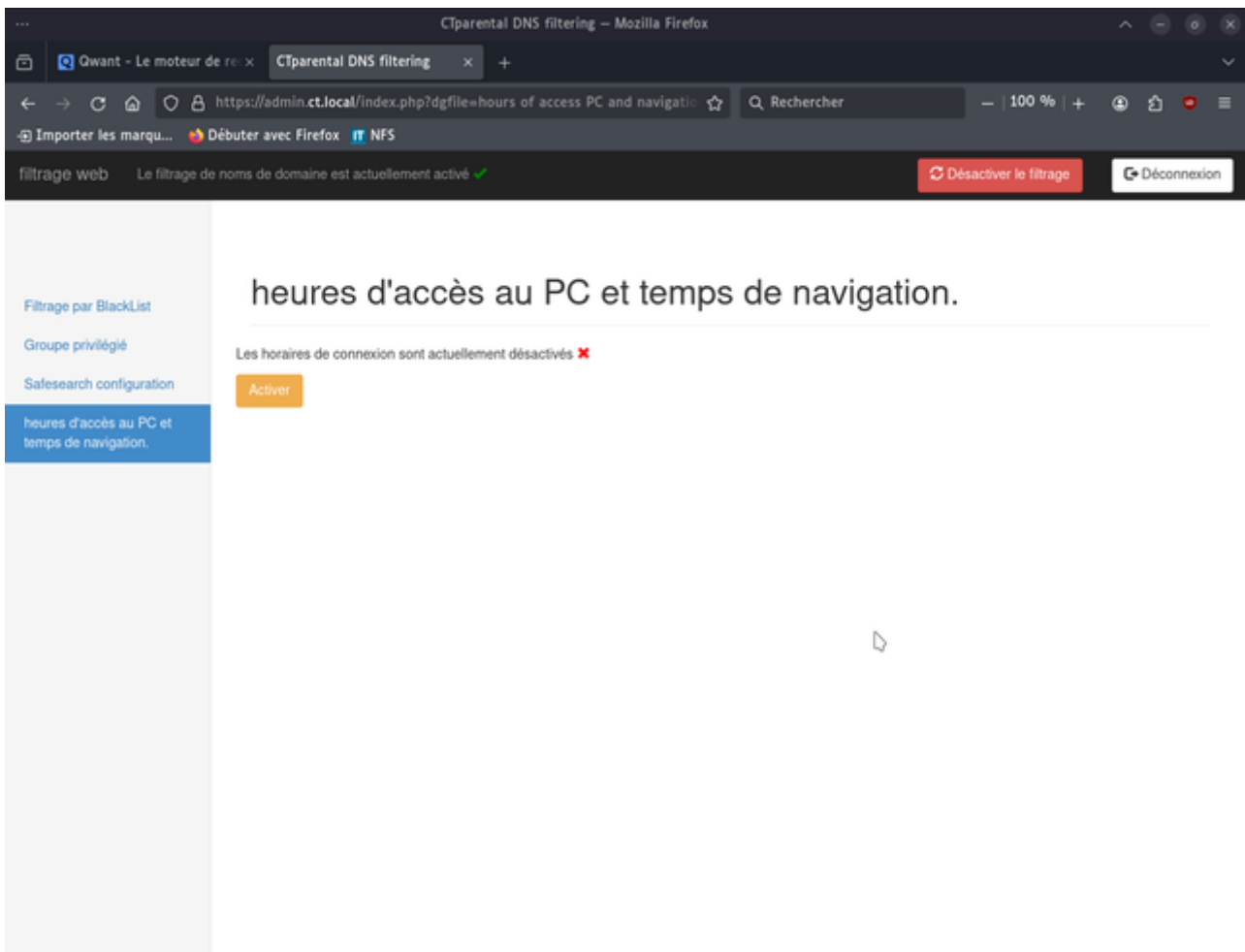
Page safesearch configuration

Cette page permet d'activer/désactiver l'option Safesearch de plusieurs moteurs de recherche (Google, YouTube, Bing, DuckDuckgo et Qwant) sans rien avoir à faire sur les pages de paramètres de ces derniers.



Page heures d'accès au PC et temps de navigation

Dans cette page il sera possible de définir des jours, heures, périodes et limites d'accès à Internet. On commence par activer les horaires de connexion :



puis un utilisateur auquel s'appliquera les restrictions :

CTparental DNS filtering – Mozilla Firefox

Qwant - Le moteur de recherche

CTparental DNS filtering

https://admin.ct.local/index.php?dgfile=hours of access PC and navigation

Rechercher

100 %

Importeur les marques

Débuter avec Firefox

NFS

filtrage web

Le filtrage de noms de domaine est actuellement activé ✓

Désactiver le filtrage

Déconnexion

heures d'accès au PC et temps de navigation.

Les horaires de connexion sont actuellement activés ✓

Désactiver

Sélectionner

poe

jerry

koda

leon

Veuillez sélectionner un utilisateur.

CTparental DNS filtering – Mozilla Firefox

Qwant - Le moteur de recherche

CTparental DNS filtering

https://admin.ct.local/index.php?dgfile=hours of access PC and navigation

Rechercher

100 %

Importeur les marques

Débuter avec Firefox

NFS

filtrage web

Le filtrage de noms de domaine est actuellement activé ✓

Désactiver le filtrage

Déconnexion

heures d'accès au PC et temps de navigation.

Les horaires de connexion sont actuellement activés ✓

Désactiver

jerry

Sélectionner

l'utilisateur sélectionné est : jerry

Attention !

Lorsque l'option **7j/7 24h/24** est décochée pour un utilisateur, il verra sa session se fermer automatiquement au moment où vous enregistrerez la modification et il perdra toutes les données non enregistrées. Alors avant tout changement de configuration, veuillez à bien fermer les sessions ouvertes des comptes concernés pour éviter d'éventuels problèmes.

Aussi, sur le poste, **conservez un compte avec des droits d'administration sans limitation d'heure d'accès** (option **7j/7 24h/24** cochée pour ce compte) afin de garder un compte pour administrer le PC en dehors des horaires d'accès définies, surtout sur les distributions sans compte **root**, comme Ubuntu.

7j/7 24h/24 : Enregistrer

En décochant l'option 7j/7 24h/24 on fait apparaître un formulaire permettant de définir finement des horaires des limites de temps :

CTparental DNS filtering – Mozilla Firefox

https://admin.ct.local/index.php?dgfile=hours of access PC and navi

Rechercher

100 %

Importeur les marqu... Débuter avec Firefox NFS

filtrage web Le filtrage de noms de domaine est actuellement activé

Désactiver le filtrage Déconnexion

jerry Sélectionner

l'utilisateur sélectionné est : jerry

Attention !

Lorsque l'option **7j/7 24h/24** est décochée pour un utilisateur, il verra sa session se fermer automatiquement au moment où vous enregistrerez la modification et il perdra toutes les données non enregistrées. Alors avant tout changement de configuration, veuillez à bien fermer les sessions ouvertes des comptes concernés pour éviter d'éventuels problèmes.

Aussi, sur le poste, **conservez un compte avec des droits d'administration sans limitation d'heure d'accès** (option **7j/7 24h/24** cochée pour ce compte) afin de garder un compte pour administrer le PC en dehors des horaires d'accès définies, surtout sur les distributions sans compte **root** comme Ubuntu.

7j/7 24h/24 :

temps d'accès maximum au pc (minutes par 24 heures) /1440 .
0 minutes déjà utilisées

temps max pour surfer sur le web (minutes par 24 heures) /1440 .
0 minutes déjà utilisées

bloquer l'accès complet au PC en dehors des heures ci-dessous.

lundi:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>
mardi:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>
mercredi:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>
jeudi:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>
vendredi:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>
samedi:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>
dimanche:	<input type="text" value="00h00"/>	à	<input type="text" value="23h59"/>	et	<input type="text"/>	à	<input type="text"/>

Enregistrer

Ré-initialiser un compte élève

Si on a besoin de ré-initialiser un compte élève : jerry, koda ou leon, ceci est possible à partir du compte Poe.

On perdra toutes les données de ces comptes !!! Il faudra donc éventuellement les sauvegarder avant.

Voici les commandes à taper si on veut réinitialiser le compte élève "jerry" (mais il suffira de remplacer "jerry" par "koda" ou "leon" selon le besoin).

Tout d'abord, il faudra tuer tous les process liés au compte "jerry" à supprimer. Si aucune session de ce compte n'a été ouverte depuis le démarrage de l'ordinateur, ça ne sera pas la peine. Sinon, il faudra saisir cette commande :

```
sudo pkill -u jerry
```

Ensuite on supprime le compte (et ses dossiers, documents) avec :

```
sudo userdel -r jerry
```

On réinstalle le fichier de profil associé avec :

```
sudo apt reinstall profil-jerry-primtux
```

Puis on recrée le compte "jerry" avec un mot de passe vide :

```
sudo useradd --password '' -m -k /etc/skel-jerry jerry -c "Jerry"
```

Remarques :

- On indique un mot de passe vide car il s'agit d'une session pour les élèves.
- Il serait possible de réinitialiser le compte Poe de cette façon à condition d'avoir un autre compte administrateur. Mais à éviter ou à vos risques et périls...

Connexion automatique à une session

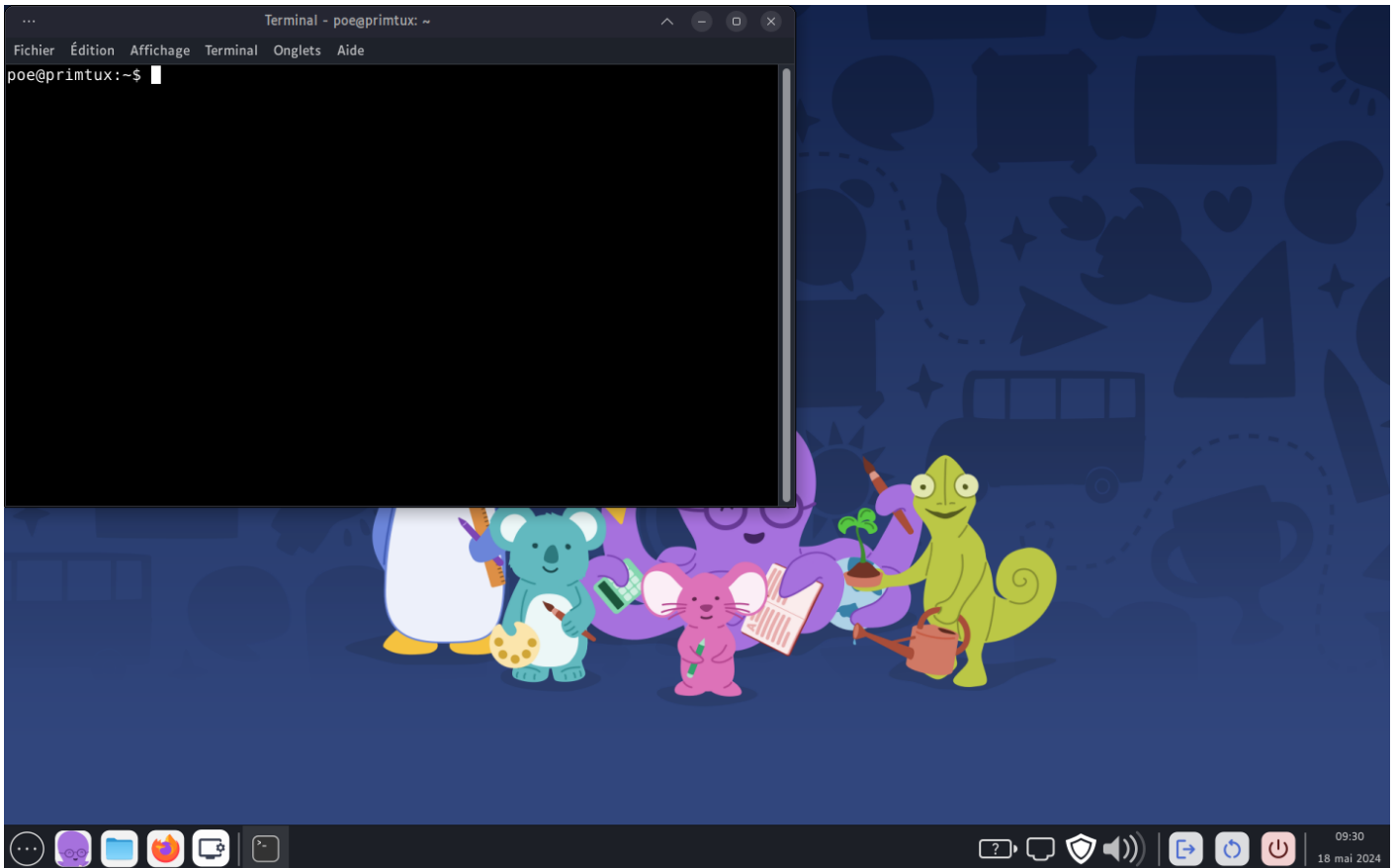
Si vous avez dans votre classe des élèves ne relevant que d'un seul cycle, vous pourriez souhaiter qu'au lancement PrimTux démarre directement sur la session correspondant à ce cycle. L'équipe PrimTux propose un utilitaire permettant de faire cela simplement.

Installation de l'utilitaire

Saisir "terminal" dans la barre de recherche du menu principal, puis cliquer sur l'icône du terminal qui apparaît :



Une fenêtre de terminal s'ouvre :



Y saisir la commande suivante, et appuyer sur la touche Entrée :

```
sudo apt update
```

Cette commande permet de mettre à jour la liste des logiciels disponibles.

Saisir maintenant la commande suivante qui installera le logiciel autologin, puis appuyer sur la touche Entrée :

```
sudo apt install autologin-primitux8
```

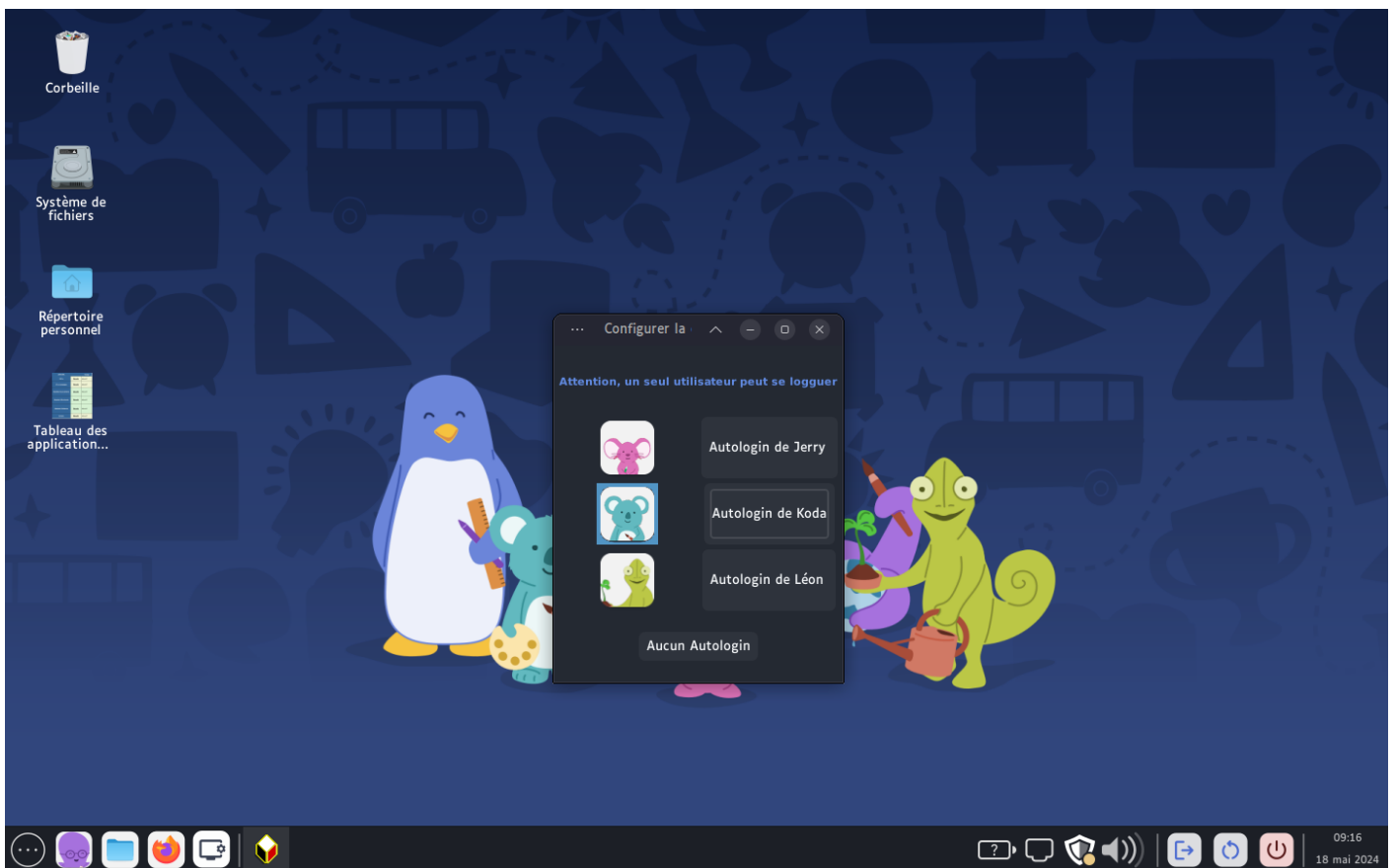
L'application est maintenant installée.

Lancer l'application autologin

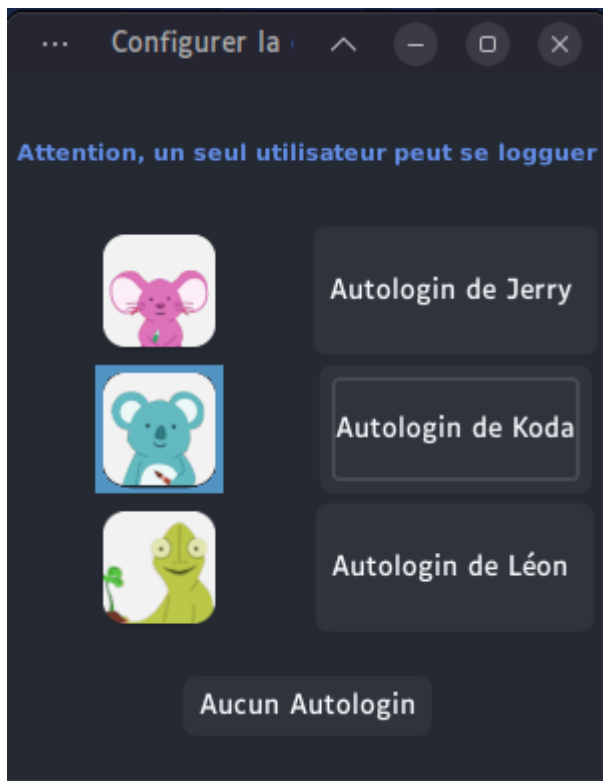
Saisir "auto" dans la barre de recherche du menu principal, puis cliquer sur l'icône autologin-primitux qui apparaît :



Une fenêtre avec le choix des sessions va s'ouvrir :



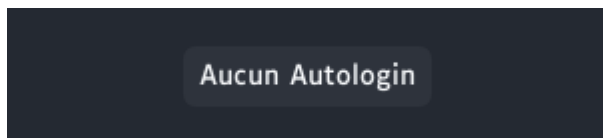
Dans cette fenêtre, cliquer sur la session souhaitée. Par exemple, ici Koda :



Redémarrer l'ordinateur qui s'ouvrira désormais directement sur la session choisie.

Pour ouvrir automatiquement PrimTux sur une autre session, refaire la même démarche pour ouvrir l'application autologin-primtux et choisir la session désirée.

Pour revenir à l'ouverture sur les 4 sessions, choisir "Aucun autologin" :



Blocage d'Internet pour les sessions élèves

Il peut arriver qu'on ne veuille pas que les élèves en maternelle (utilisateur "Jerry") aient accès à Internet tout en gardant cette possibilité pour le compte Poe de l'enseignant·e et les autres élèves (utilisateurs "Koda et "Leon").

La solution repose sur nftables qui est assez peu utilisé face à son prédécesseur iptables.

Voir cette page pour plus d'info sur nftables : <https://fr.wikipedia.org/wiki/Nftables>

EN COURS DE TEST : RETOURS APPRÉCIÉS !!!

On va d'abord trouver l'UID de l'utilisateur Jerry avec la commande :

```
id -u jerry
```

Ça nous retourne un nombre. Pour Jerry, l'UID est :

```
1001
```

On peut dès lors éditer le fichier de configuration de nftables avec la commande :

```
sudo nano /etc/nftables.conf
```

Voici le contenu initial :

```
# /usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority filter;
    }
    chain forward {
        type filter hook forward priority filter;
    }
    chain output {
```

```
        type filter hook output priority filter;
    }
}
```

On va alors ajouter dans la partie "chain output", les règles pour l'utilisateur ayant l'UID 1001 qui est Jerry :

```
#!/usr/sbin/nft -f

# Paramètres à adapter selon l'UID de Jerry et votre réseau LAN
# Il suffit d'initialiser les variables nécessaires uniquement dans cette partie
define UTILISATEUR = 1001
# Pour plusieurs utilisateurs UID 1001 (Jerry), 1002 (Koda) et 1003 (Léon)
# et remplacer $UTILISATEUR par $UTILISATEURS défini ci-dessous
#define UTILISATEURS = { 1001, 1002, 1003 }
define LAN = 192.168.1.0/24

# Suppression des règles existantes (remise à zéro)
flush ruleset

# Règles à appliquer
table inet filter {
    chain input {
        type filter hook input priority filter;
    }

    chain forward {
        type filter hook forward priority filter;
    }

    chain output {
        type filter hook output priority 0;
        # les règles "accept" doivent précéder les règles "drop" !!!
        # Loopback / localhost
        meta skuid $UTILISATEUR oif lo accept
        # LAN IPv4
        meta skuid $UTILISATEUR ip daddr $LAN accept
        # LAN IPv6
        meta skuid $UTILISATEUR ip6 daddr { fe80::/10, fc00::/7 } accept
        # Blocage total Internet avec message indiquant que la connexion est refusée
```

```
meta skuid $UTILISATEUR reject with icmpx type admin-prohibited
# ou Blocage total sans message avec Timeout
#meta skuid $UTILISATEUR drop

}
}
```

On applique la config avec cette commande :

```
sudo nft -f /etc/nftables.conf
```

Pour rendre cette règle pérenne au démarrage, taper les commandes :

```
sudo systemctl enable nftables
sudo systemctl restart nftables
```

Pour vérifier les règles, taper :

```
sudo nft list ruleset
```