



Publié sur **COAGUL** (<https://coagul.org/drupal>)

[Accueil](#) > [Rubriques](#) > [Publications](#) > [Réseaux](#) > PDF imprimable

Contrôle parental avec DansGuardian et TinyProxy

jeu, 22/02/2007 - 21:34 — Tony

[Réseaux](#) ^[1]

Ce document me sert de mémo pour installer DansGuardian et TinyProxy dans le but de mettre en place un contrôle parental pour l'accès Web.

Cela est particulièrement utile (voire indispensable) si vous avez des jeunes enfants désirant utiliser régulièrement un accès Web.

But de ce document

Ce document me sert de mémo pour installer DansGuardian et TinyProxy dans le but de mettre en place un contrôle parental pour l'accès web.

Cela est particulièrement utile (voire indispensable) si vous avez des jeunes enfants désirant utiliser régulièrement un accès web.

Cette installation a été effectuée sur Debian Testing mais elle doit fonctionner sans problème sur d'autres distributions.

Différences entre DansGuardian et SquidGuard

Pour filtrer les URL, SquidGuard utilise une base de données des sites interdits. Pour fonctionner correctement, il est donc nécessaire de maintenir cette base de données à jour en permanence.

De son côté, DansGuardian analyse le contenu des pages pour savoir si elle doit être bloquée ou pas. Il est possible également d'ajouter une liste de sites ou de mots interdits et il est même possible d'utiliser les listes noires de SquidGuard comme nous le verrons à la fin de ce document.

Si vous souhaitez installer SquidGuard, vous pouvez lire cet article :

- http://www.coagul.org/article.php3?id_article=184 ^[2]

Installation de TinyProxy

Pour faire fonctionner DansGuardian, il faut commencer par installer un serveur proxy. Il est possible d'installer par exemple « **Squid** », mais nous allons dans ce document utiliser « **TinyProxy** » qui est plus léger mais suffisant pour notre besoin :

```
# aptitude install tinyproxy
```

Remarque : Par défaut, « **TinyProxy** » utilise le port 8888. Pour le changer, il faut éditer son fichier de configuration « **/etc/tinyproxy/tinyproxy.conf** ».

Configuration de TinyProxy

La configuration de TinyProxy s'effectue dans le fichier « **/etc/tinyproxy/tinyproxy.conf** ».

Par exemple, pour changer le port en écoute, il faut modifier cette ligne :

Port 8888

Pour des raisons de sécurité et pour faciliter le filtrage avec « **iptables** » je conseille de créer un compte utilisateur spécifique pour le démon de TinyProxy :

```
# useradd -s /bin/false tiny
```

Ensuite, il faut éditer le fichier de configuration « **/etc/tinyproxy/tinyproxy.conf** » et modifier ces lignes :

```
User tiny
Group tiny
```

Pour finir, il faut démarrer ou redémarrer TinyProxy :

```
# /etc/init.d/tinyproxy restart
```

Et vérifier que le démon tourne bien sous le compte « tiny » :

```
# ps aux | grep tiny
tiny 7706 0.0 0.1 2216 560 ? S 13:17 0:00 /usr/sbin/tinyproxy
```

Test de TinyProxy

Pour tester TinyProxy, il suffit de configurer un navigateur web pour qu'il l'utilise. Par exemple, pour Firefox, il faut faire :

- Menu « Éditions / Préférences » onglet « Avancé », bouton « Paramètres ».
 - Mettre « **localhost** » dans le champ « Proxy HTTP »
 - Mettre « **8888** » dans le champ « Port »
 - Cocher « Utiliser ce serveur proxy pour tous les protocoles »
- Si après ce réglage, l'accès web fonctionne toujours c'est que le proxy est opérationnel.

Et normalement en arrêtant le proxy, cela doit bloquer l'accès web :

```
# /etc/init.d/tinyproxy stop
```

Ensuite, il faut le démarrer pour refaire fonctionner l'accès web :

```
# /etc/init.d/tinyproxy start
```

Installation de DansGuardian

```
# aptitude install dansguardian
```

L'installation de « DansGuardian entraîne l'installation de l'antivirus « **Clamav** ». Dans ce document, nous n'activerons pas cet antivirus car il n'est pas indispensable sous Linux et consomme pas mal de ressources.

Configuration de DansGuardian

DansGuardian utilise plusieurs fichiers de configuration enregistrés dans « **/etc/dansguardian** ».

Configuration de « **/etc/dansguardian/dansguardian.conf** »

Pour activer la configuration, il faut commenter ou supprimer cette ligne en début de fichier :

```
#UNCONFIGURED
```

Cette ligne permet d'indiquer le port utilisé par le proxy :

```
proxyport = 8888
```

Cette ligne permet d'avoir les messages en français en cas de blocage des sites :

```
language = 'french'
```

Cette ligne permet de désactiver l'antivirus :

```
virusscan = off
```

Configuration de « /etc/dansguardian/dansguardianf1.conf »

La ligne suivante permet de paramétrer le filtrage en fonction de l'âge des personnes concernées :

```
naughtynesslimit = 80
```

La valeur par défaut de « 50 » donne un filtrage très dur et peu de sites sont accessibles. Plus cette valeur est élevée et plus le filtrage est faible. Personnellement, j'ai fait quelques tests et j'ai passé cette valeur à « 80 ».

Cette ligne permet de désactiver l'antivirus :

```
virusscan = off
```

Configuration du fichier « /etc/dansguardian/bannedextensionlist »

Ce fichier permet de définir des types de fichiers qui seront interdits de télécharger. Par défaut, la liste est très restrictive. Il faut donc commenter les types de fichiers autorisés :

```
#.gz # Gzipped file
#.tar # Tape ARchive file
#.tgz # Unix compressed file
#.bz2 # Unix compressed file
```

Configuration du fichier « /etc/dansguardian/bannedmimetyplist »

Là encore il s'agit de restreindre des types de fichiers.

```
#application/gzip
#application/x-gzip
#application/zip
```

Configuration du fichier « /etc/dansguardian/bannedregexpurllist »

L'ajout de cette ligne à la fin du fichier permet de bloquer la plupart des sites français de rencontres en ligne :

```
(webcam|tchat|t'chat|rencontre|meetic|amour)
```

Configuration du fichier /etc/dansguardian/phraselists/pornography/weighted_french »

Il est possible d'ajouter des mots ou des listes de mots dans ce fichier, avec des coefficients positifs (mauvais mot) ou négatifs (bons mots) :

```
< tchat ><20>
< t'chat ><20>
< partouze ><70>
```

Prise en compte des modifications dans la configuration de DansGuardian

Pour prendre en compte les modifications, il faut exécuter cette commande :

```
# /etc/init.d/dansguardian restart
```

Remarque : Un simple « **reload** » ne semble pas être suffisant.

Configuration du navigateur

Pour tester « **DansGuardian** », il suffit de configurer un navigateur web pour qu'il l'utilise. Par exemple, pour Firefox, il faut faire

:

- Menu « Éditions / Préférences » onglet « Avancé », bouton « Paramètres ».
- Mettre « **localhost** » dans le champ « Proxy HTTP »
- Mettre « **8080** » dans le champ « Port » (et non plus « 8888 » qui est le port utilisé par le proxy mais pas par DansGuardian)
- Cocher « Utiliser ce serveur proxy pour tous les protocoles »

Test de filtrage

Dans Firefox ,allez sur www.google.fr ^[3] et faites une recherche sur le mot « chatte ». Normalement la page résultante de cette recherche devrait être bloquée et une page d'avertissements s'affiche à la place.

Pour modifier cette page, il suffit de modifier le fichier html suivant :

```
/etc/dansguardian/languages/french/template.html
```

Ensuite, faites une recherche dans « google » sur le mot « chat ». La page résultante n'est pas bloquée mais offre des liens vers des sites de rencontres. Si vous suivez les liens donnés, vous constaterez que certains sont immédiatement bloqués car ils contiennent un contenu sensible. Pour d'autres sites, vous accédez à la page d'accueil ne contenant rien de compromettant.

Configuration d'iptables pour forcer les navigateurs à passer par le proxy

Avec cette configuration, il suffit de supprimer la configuration du proxy dans le navigateur pour accéder à tout le web sans filtrage. Pour remédier à ce problème, il faut configurer iptables pour bloquer l'accès direct au web à tous les utilisateurs (sauf root et tiny). Pour cela il suffit d'ajouter ces lignes à la configuration de votre parefeu ou dans un script qui se lancera automatiquement au démarrage :

```
# iptables -A OUTPUT -o eth0 -p tcp --dport http -j REJECT --reject-with tcp-reset
# iptables -I OUTPUT -o eth0 -p tcp --dport http -m owner --uid-owner root -j ACCEPT
# iptables -I OUTPUT -o eth0 -p tcp --dport http -m owner --uid-owner tiny -j ACCEPT
```

Pour plus d'informations sur la configuration d'iptables et la mise en place d'un parefeu, vous pouvez lire cet article :

- http://www.coagul.org/article.php3?id_article=485 ^[4]

ATTENTION : Avec cette configuration, aucun programme ne pourra avoir un accès http sans passer par le proxy. Par exemple, il faudra configurer Thunderbird pour pouvoir recevoir les fils RSS.

Utilisation des listes noires de SquidGuard

Vous trouverez sur ce site, des listes noires régulièrement actualisées pour SquidGuard :

- <http://cri.univ-tlse1.fr/documentations/cache/squidguard.html> ^[5]

Le script suivant que vous pouvez placer dans la crontab de root, permet de récupérer et décompresser automatiquement la liste noire « **adult** » :

```
#!/bin/bash
mkdir /etc/dansguardian/blacklists
cd /etc/dansguardian/blacklists
wget ftp://ftp.univ-tlse1.fr/pub/reseau/cache/squidguard_contrib/adult.tar.gz
tar -xvzf adult.tar.gz
```

Ensuite, il suffit de décommenter la ligne suivante du fichier « **/etc/dansguardian/bannedsitelist** » :

```
.Include
```

Et de redémarrer DansGuardian :

```
# /etc/init.d/dansguardian restart
```

Pour tester que la liste est bien opérationnelle, il faut tester l'un des sites proposés dans le fichier « domain » et regarder les logs :

```
2007.2.17 11:49:44 - 127.0.0.1 http://votresite.com *DENIED* Site interdit: votresite.com GET 0
```

Liens pour avoir plus d'informations

Cet article est fortement inspiré des informations provenant de ce mail et de cet article :

- <http://lists.debian.org/debian-user-french/2006/04/msg01654.html> ^[6]
- <http://easy.open.and.free.fr/TinyDansguard/> ^[7]

Historique des modifications

Version	Date	Commentaire
0.4	17/02/07	Création par Tony GALMICHE
0.41	14/08/07	Petite correction

Licence Creative Commons by-sa 3.

URL source: <https://coagul.org/drupal/publication/contr%C3%B4le-parental-dansguardian-et-tinyproxy>

Liens:

- [1] <https://coagul.org/drupal/rubrique/reseaux>
- [2] http://www.coagul.org/article.php3?id_article=184
- [3] <http://www.google.fr/>
- [4] http://www.coagul.org/article.php3?id_article=485
- [5] <http://cri.univ-tlse1.fr/documentations/cache/squidguard.html>
- [6] <http://lists.debian.org/debian-user-french/2006/04/msg01654.html>
- [7] <http://easy.open.and.free.fr/TinyDansguard/>