

MANUEL D'INSTALLATION D'UN PROXY

Squid, SquidGuard, Dansguardian

Dans ce guide on va détailler l'installation et la configuration d'une solution proxy antivirale en utilisant les outils ; squid, dansGuardian, squidguard et un antivirus Clamav sur un système d'exploitation linux debian lenny.





الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

Gestion de Gestion des versions de guide

Version	Date	Modification apportée
1.0	28/07/2010	Première version

PLAN

1. présentation	3
2. Paramétrage du gestionnaire de package	4
3. Installation.....	5
a. Installation de Webmin.....	5
b. Installation de Squid.....	5
c. Installation de SquidGuard	5
d. Installation de DansGuardian	6
4. Configuration via webmin	7
a. Squid.....	7
b. SquidGuard	15
c. DansGuardian	20
d. Mise à jour de Dansguardian.....	23
e. Configuration du client	24
5. Test de fonctionnement.....	24

1. PRESENTATION

Un serveur proxy est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les proxy sont notamment utilisés pour assurer les fonctions suivantes :

- mémoire cache
- la journalisation des requêtes (« logging »)
- la sécurité du réseau local
- le filtrage et l'anonymat

Notre serveur proxy va être composé de squid, squidguard et dansguardian

❖ Squid est un serveur proxy cache open source qui supporte les protocoles http, https, FTP et SSL. Il assure les fonctions de :

- Cache : pour optimiser la bande passante
- Contrôle des accès
- Reverse proxy

❖ SquidGuard est un redirecteur de requêtes web qui utilise la librairie Berkeley Database. Il propose un filtrage puissant d'accès au web, en fonction de:

- Groupes d'utilisateurs, définis de diverses manières.
- Listes de domaines et d'URI qui serviront à définir soit des cibles autorisées, soit des cibles interdites,
- Black listes de domaines et d'URI
- Plages horaires

❖ DansGuardian est un système de contrôle de contenu. Il utilise plusieurs méthodes paramétrables pour déterminer si une page web doit être bloquée.

- Il utilise ; un système de pondération qui détecte des mots interdits dans une page, et lui assigne un score en fonction de la gravité et du nombre de mots détectés. DansGuardian bloque alors les pages dont le score dépasse un certain seuil.

- Il peut également se fier à des listes noires d'URL telles que celle proposée par le site URLBlacklist.com, ou au code PICS d'une page web lorsqu'il est renseigné.

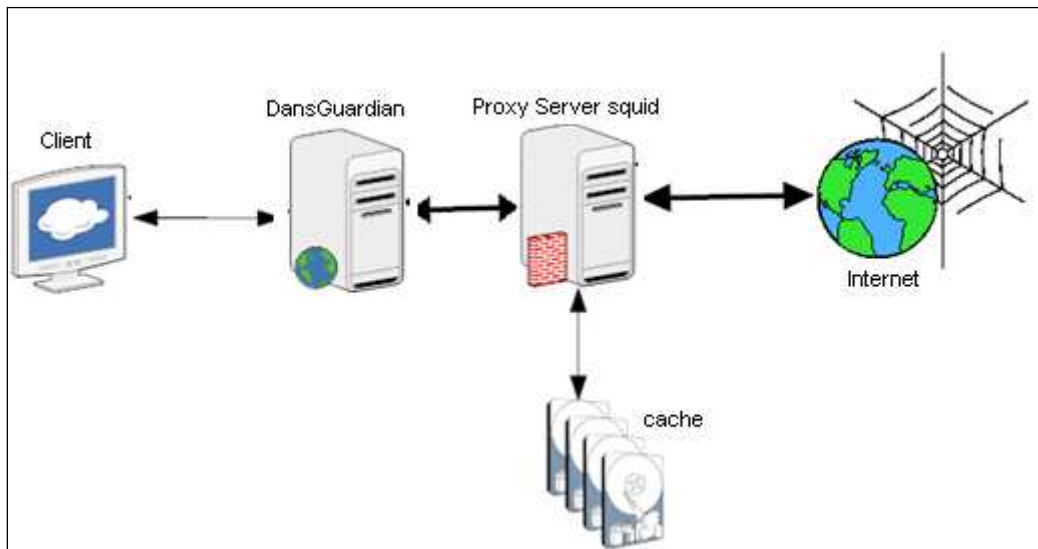


Fig1. Schéma de fonctionnement d'un proxy

2. PARAMETRAGE DU GESTIONNAIRE DE PACKAGE

- Changer le fichier `/etc/apt/sources.list` comme suit :

```
deb http://ftp.us.debian.org/debian lenny main
deb-src http://ftp.us.debian.org/debian lenny main
deb http://security.debian.org/ lenny/updates main
deb-src http://security.debian.org/ lenny/updates main
deb http://volatile.debian.org/debian-volatile lenny/volatile main
deb-src http://volatile.debian.org/debian-volatile lenny/volatile main
```

- Mettez à jour la liste des fichiers disponibles dans les dépôts APT présents dans le fichier de configuration `/etc/apt/sources.list`. puis mettez à jour tous les paquets installés vers les dernières versions

```
Apt-get update
```

```
Apt-get upgrade
```

3. INSTALLATION

a. Installation de Webmin

- Webmin est une interface web, qui permet d'administrer à distance notre serveur proxy (squid, squidguard et dansguardian).
- Télécharger webmin à partir de ce lien : <http://prdownloads.sourceforge.net/webadmin/webmin-1.480.tar.gz>
- Décompresser le :

```
Tar xzvf webmin-1.480.tar.gz
```

```
Cd webmin-1.480
```

- Installez-le :

```
./setup.sh
```

- Connexion à l'interface de webmin : https://adresse_de_host:10000

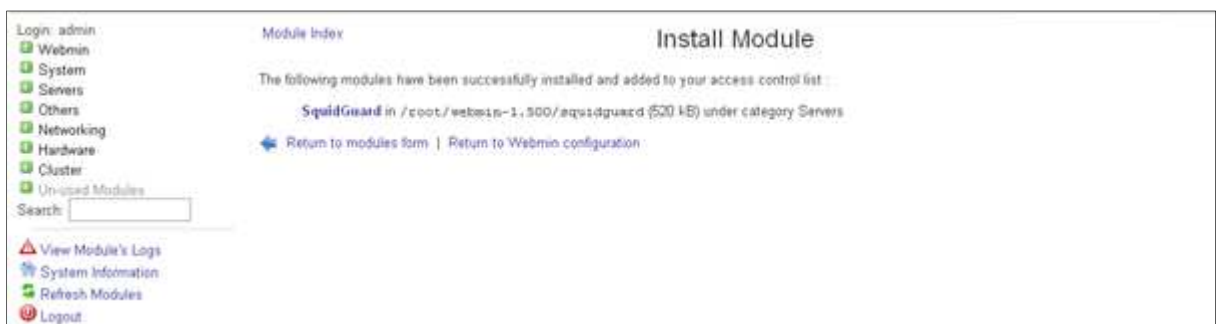
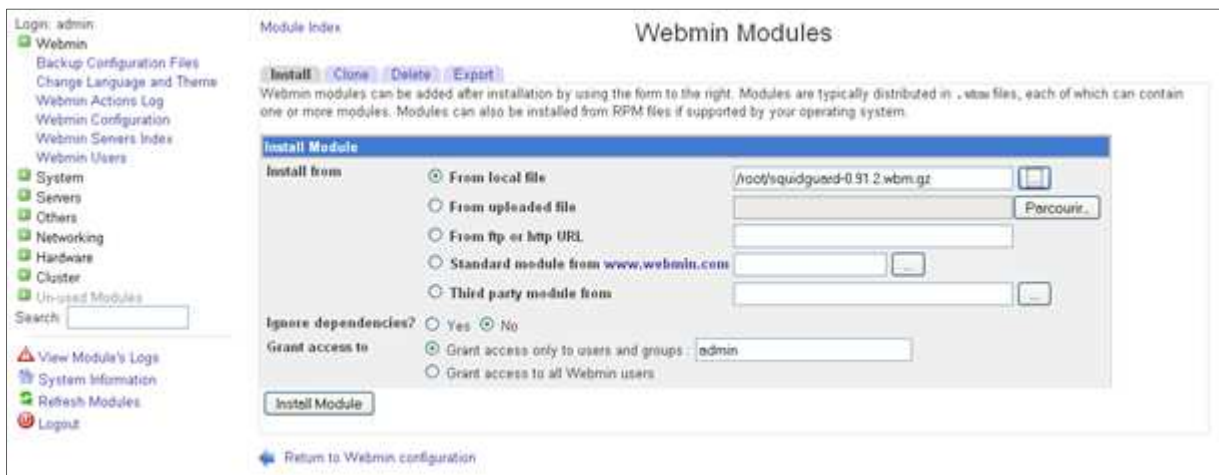
b. Installation de Squid

```
apt-get install squid
```

c. Installation de SquidGuard

```
apt-get install squidguard
```

- Téléchargez maintenant son module de webmin à partir de ce lien : <http://www.niemueller.de/webmin/modules/squidguard/squidguard-0.91.2.wbm.gz>
- Installez-le via webmin comme suit :



d. Installation de DansGuardian

```
apt-get install dansguardian
```

- Téléchargez maintenant son module de webmin à partir de ce lien : <http://sourceforge.net/projects/dgwebminmodule/files/dgwebmin-devel/0.7.0beta1b/dgwebmin-0.7.0beta1b.wbm/downloadn>
- Et faites de même que l'ajout du module de squidguard via webmin.

4. CONFIGURATION VIA WEBMIN

a. Squid

- **Configuration squid :**



















- En haut de la page de « serveur proxy squid », cliquez sur « configuration du module ».

Aide :
Configuration du module

Serveur proxy Squid

Squid version 2.7

Appliquer les changements
 Arrêter Squid
 Rechercher la documentation..

 Ports et options de réseau	 Ajouter un cache	 Utilisation de la mémoire	 Fichiers logs
 Options du cache	 Programmes utiles	 Listes d'accès	 Administraiton de la mémoire-cache
 Authentification du proxy	 Authentication Programs	 Delay Pools	 Header Access Control
 Refresh Rules	 Options diverses	 Port Redirection Setup	 Suivie du cache
 Cache Manager Passwords	 Vider et ré-initialiser la mémoire-cache		

Apply Configuration

Click this button to activate the current Squid configuration.

Stop Squid

Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests.

- Changez les commandes de démarrage, d'arrêt et de redémarrage comme suit, puis sauvegardez :

Configuration

Pour le module Serveur Proxy Squid

Options configurables pour Serveur Proxy Squid

Configurable options

Generate all calamaris reports? Yes No

Calamaris output format HTML Text

Extra Calamaris command-line parameters

Nb maximum de lignes de log à passer à calamaris Non limité 50000

Encryption method for proxy passwords crypt md5base64

Sort proxy users Yes No

Show stop/start/apply buttons On main page In headings Both

Create proxy users when creating system users Yes No

Update proxy users when updating system users Yes No

Delete proxy users when deleting system users Yes No

System configuration

Chemin du fichier de configuration de squid

Commande de démarrage de squid Automatique /etc/init.d/squid start

Commande d'arrêt de squid Automatique /etc/init.d/squid stop

Command to apply changes Automatic /etc/init.d/squid restart

Exécutable de squid

Chemin du fichier de numéro de processus

Répertoire cache de squid

Chemin de l'exécutable 'cachemgr.cgi'

Répertoire d'audit de squid

Chemin vers le programme d'analyse de log calamaris Non installé calamaris

Path to squidclient program Not installed squidclient

Arguments de la commande calamaris

- **Port et adresse d'écoute :**

- Sous la catégorie serveur, cliquez sur serveur proxy squid, puis sur « port et options de réseau » et configurer le port et l'adresse de proxy.

Index du module
Aide..
Ports et réseau
Appliquer les changements
Arreter Squid

Options des ports et de réseau

Adresse proxy et port Default (usually 3128) Listed below..

Port	Adresse de nom d'hôte/IP	Options for port
3128	<input type="radio"/> All <input checked="" type="radio"/> 192.168.12.145	<input type="text"/>
<input type="text"/>	<input checked="" type="radio"/> All <input type="radio"/>	<input type="text"/>

SSL addresses and ports Default (usually 3128) Listed below..

Port	Adresse de nom d'hôte/IP	Options for port
<input type="text"/>	<input checked="" type="radio"/> All <input type="radio"/>	<input type="text"/>

Port ICP Défaut

Adresse UDP sortante Tous

Adresse TCP sortante Tous

Adresse UDP entrante Tous

Groupe multicast

Mémoire de la réception pour TCP OS par défaut

Validate hostnames in URLs? Oui Non

Do unclean SSL shutdowns? Marche Arrêt

Allow underscore in hostnames? Oui Non

[Retourner à index de squid](#)

- **Utilisation de la mémoire :**

- Fixer l'utilisation de la mémoire (à 8 MB)

Index du module
Aide..
Utilisation de la mémoire
Appliquer les changements
Arreter Squid

Options d'utilisation de la mémoire et des disques


Limite d'utilisation de la mémoire <input type="radio"/> Défaut <input checked="" type="radio"/> 8 <input type="text" value=""/> MBs	FQDN cache size <input checked="" type="radio"/> Défaut <input type="text" value=""/>		
Disque: niveau haut de remplissage <input checked="" type="radio"/> Défaut <input type="text" value=""/> %	Disque: niveau bas de remplissage <input checked="" type="radio"/> Défaut <input type="text" value=""/> %		
La taille maximal d'objet <input checked="" type="radio"/> Défaut <input type="text" value=""/> kB	La taille maximal de la mémoire pour les adresses IP <input checked="" type="radio"/> Défaut <input type="text" value=""/> entrées		
cache IP: niveau haut de remplissage <input checked="" type="radio"/> Défaut <input type="text" value=""/> %	cache IP: niveau bas de remplissage <input checked="" type="radio"/> Défaut <input type="text" value=""/> %		
Algorithme de remplacement sur disque <input type="text" value="Défaut"/>	Algorithme de remplacement dans la mémoire <input type="text" value="Défaut"/>		


[Retourner à l'index de squid](#)


- **Ajouter l'authentification :**


- Ouvrez l'onglet « Authentication Programs »


Aide..
Configuration du module
Serveur proxy Squid
Squid version 2.7
Appliquer les changements
Arreter Squid
Rechercher la documentation..



Ports et options de réseau



Ajouter un cache



Utilisation de la mémoire



Fichiers logs



Options du cache



Programmes utiles



Listes d'accès



Administratoin de la mémoire-cache



Authentication Programs



Delay Pools



Header Access Control



Refresh Rules


Options diverses


Port Redirection Setup


Suivie du cache


Cache Manager Passwords


Vider et ré-initialiser la mémoire-cache

Click this button to activate the current Squid configuration.
 Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests.

- Indiquer le programme d'authentification que vous allez utiliser. Sauvegarder et retourner à la page d'index.

Index du module
Aide..

Programmes d'authentification

Appliquer les changements
Arreter Squid

External authentication program options

Basic authentication program Aucun Webmin default ...

Nombre de programme d'authentification Défaut

Authentication cache time Défaut heures

Authentication realm Défaut

Digest authentication program Aucun ...

Nombre de programme d'authentification Défaut

Authentication realm Défaut

NTLM authentication program Aucun ...

Nombre de programme d'authentification Défaut

Number of times an NTLM challenge can be re-used Défaut

Lifetime of NTLM challenges Défaut heures

Authenticate IP TTL is required to be > 0 if you are using a "max_user_ip" ACL. Enter the time you wish Squid to remember the User/IP relationship. The user may only logon from the remembered IP until this amount of time has passed, even if they have closed their browser.

Authenticate IP cache time Défaut heures

[Retourner à index de squid](#)



















- Il vous apparait un nouveau onglet nommé « Authentication du proxy », cliquer dedans et ajouter un nouveau utilisateur du proxy, puis cliquez sur créer.

Aide..
Configuration du module

Serveur proxy Squid

Squid version 2.7

Appliquer les changements
Arreter Squid
Rechercher la documentation..

 Ports et options de réseau	 Ajouter un cache	 Utilisation de la mémoire	 Fichiers logs
 Options du cache	 Programmes utiles	 Listes d'accès	 Administraiton de la mémoire-cache
 Authentication du proxy	 Authentication Programs	 Delay Pools	 Header Access Control
 Refresh Rules	 Options diverses	 Port Redirection Setup	 Suivie du cache
 Cache Manager Passwords	 Vider et ré-initialiser la mémoire-cache		

Click this button to activate the current Squid configuration.

Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests.

Détails d'un utilisateurs proxy

Nom de connexion

Mot de passe

Enabled? Oui Non

[← Retourner à liste des utilisateurs](#) | [Retourner à l'index de squid](#)


- **Mise en place des ACLs :**


Aide...
Configuration du module


Serveur proxy Squid


Squid version 2.7


Appliquer les changements
Arreter Squid
Rechercher la documentation...



 Ports et options de réseau



 Ajouter un cache



 Utilisation de la mémoire



 Fichiers logs



 Options du cache



 Programmes utiles



Listes d'accès



 Administraiton de la mémoire-cache



 Authentification du proxy



 Authentication Programs



 Delay Pools



 Header Access Control



 Refresh Rules


 Options diverses


 Port Redirection Setup


 Suivre du cache


 Cache Manager Passwords


 Vider et ré-initialiser la mémoire-cache

Apply Configuration

Click this button to activate the current Squid configuration.

Stop Squid

Click this button to stop the running Squid proxy server. Once stopped, clients using it will be unable to make web or FTP requests.

- ❖ Ajouter une première ACL pour l'authentification des utilisateurs :

- Créer une nouvelle ACL de type « Authentification extérieur » en lui donnant un nom signifiant.

Index du module Aide.. Control d'accès Appliquer les changements Arrêter Squid

[Listes des contrôles d'accès](#)
[Restrictions du proxy](#)
[Restriction ICP](#)
[External ACL programs](#)
[Reply proxy restrictions](#)

Nom	Type	Correspond..
all	Adresse cliente	all
manager	Protocol URL	cache_object
localhost	Adresse cliente	127.0.0.1/32
to_localhost	Adresse du serveur WEB	127.0.0.0/8
localnet	Adresse cliente	10.0.0.0/8
localnet	Adresse cliente	172.16.0.0/12
localnet	Adresse cliente	192.168.0.0/16
SSL_ports	Port URL	443
SSL_ports	Port URL	563
SSL_ports	Adresse Ethernet	
Safe_ports	Adresse IP du proxy	
Safe_ports	Adresse cliente	
Safe_ports	Adresse du serveur WEB	
Safe_ports	Authentification extérieur	
Safe_ports	Communauté SNMP	
Safe_ports	Date et Heure	5-65535
Safe_ports	External Program	
Safe_ports	Hôte client	
Safe_ports	L'expression rationnelle pour URL	
Safe_ports	L'expression rationnelle pour client	
Safe_ports	L'expression rationnelle pour l'authentification extérieur	
Safe_ports	L'expression rationnelle pour le chemin de URL	
Safe_ports	L'expression rationnelle pour navigateur	
Safe_ports	L'expression rationnelle pour serveur Web	
purge	Le nombre du system autonome de destination	URGE
CONNECT	Le nombre du system autonome source	NNECT
shoutcast	Méthode de résolution	TTP09-First-Line ^CYs[0-9]
apache	Max User IP	ver ^Apache
apache	Nom d'hôte du serveur WEB	
	Adresse Ethernet	

Créer une nouvelle ACL

[Retourner à l'index de squid](#)

Index du module Créer ACL Appliquer les changements Arrêter Squid

Authentification extérieur ACL

Nom ACL:

Utilisateurs externes autorisés: All users Only those listed..

Failure URL:

Store ACL values in file: Configuration de Squid Separate file ...

Just use existing contents of file?

[Retourner à Liste ACL](#) | [Retourner à l'index de squid](#)

- Puis passer à l'onglet « Restrictions du proxy » et cliquer sur « ajouter une restriction au proxy ».
- Sélectionner le nom de votre ACL, et choisissez l'action «Autorisé». Sauvegardez

Index du module Appliquer les changements
Arreter Squid

Créer une restriction du proxy

Restriction du proxy

Action Autorisé Interdit

Conforme ACLs	Non conforme ACLs
localhost	all
to_localhost	manager
localnet	localhost
SSL_ports	to_localhost
Safe_ports	localnet
purge	SSL_ports
CONNECT	Safe_ports
shoutcast	purge
apache	CONNECT
authentication	shoutcast

[Retourner à Liste ACL](#) | [Retourner à l'index de squid](#)

- Retournez à la liste des ACLs, et faire remonter la restriction que vous venez de créer juste au-dessus de la restriction « interdit all ». Parce que squid prends en compte l'ordre des ACLs.

Index du module Appliquer les changements
Arreter Squid

Control d'accès

Aide..

Listes des contrôles d'accès **Restrictions du proxy** Restriction ICP External ACL programs Reply proxy restrictions

Ajouter une restriction au proxy

Action	ACL	Déplacer
<input type="checkbox"/> Autoriser	manager localhost	↓
<input type="checkbox"/> Interdit	manager	↓↑
<input type="checkbox"/> Autoriser	purge localhost	↓↑
<input type="checkbox"/> Interdit	purge	↓↑
<input type="checkbox"/> Interdit	!Safe_ports	↓↑
<input type="checkbox"/> Interdit	CONNECT !SSL_ports	↓↑
<input type="checkbox"/> Autoriser	localhost	↓↑
<input type="checkbox"/> Autoriser	authentication	↓↑
<input type="checkbox"/> Interdit	all	↑

Ajouter une restriction au proxy

[Retourner à l'index de squid](#)

- ❖ Ajouter une deuxième ACL pour l'accès d'adresse client :

Index du module Aide.. Appliquer les changements
Arreter Squid

Control d'accès

[Listes des contrôles d'accès](#)
[Restrictions du proxy](#)
[Restriction ICP](#)
[External ACL programs](#)
[Reply proxy restrictions](#)

Nom	Type	Correspond..
all	Adresse cliente	all
manager	Protocol URL	cache_object
localhost	Adresse cliente	127.0.0.1/32
to_localhost	Adresse du serveur WEB	127.0.0.0/8
localnet	Adresse cliente	10.0.0.0/8
localnet	Adresse cliente	172.16.0.0/12
localnet	Adresse cliente	192.168.0.0/16
SSL_ports	Port URL	443
SSL_ports	Port URL	563
SSL_ports	Port URL	873
Safe_ports	Adresse Ethernet	
Safe_ports	Adresse IP du proxy	
Safe_ports	Adresse cliente	
Safe_ports	Adresse du serveur WEB	
Safe_ports	Authentification extérieur	
Safe_ports	Communauté SNMP	25-65535
Safe_ports	Date et Heure	
Safe_ports	External Program	
Safe_ports	Hôte client	
Safe_ports	L'expression rationelle pour URL	
Safe_ports	L'expression rationelle pour client	
Safe_ports	L'expression rationelle pour l'authentification extérieur	
Safe_ports	L'expression rationelle pour le chemin de URL	
Safe_ports	L'expression rationelle pour navigateur	
Safe_ports	L'expression rationelle pour serveur Web	
purge	Le nombre du system autonome de destination	URGENT
CONNECT	Le nombre du system autonome source	CONNECT
shoutcast	Méthode de résolution	HTTP09-First-Line ^ICY\s[0-9]
apache	Max User IP	server ^Apache
authentification	Nom d'hôte du serveur WEB	REQUIRED

Créer une nouvelle ACL

[Retourner à l'index de squid](#)

- Créer une nouvelle ACL de type « Adresse cliente » en lui donnant un nom significatif.

Index du module Appliquer les changements
Arreter Squid

Créer ACL

Adresse cliente ACL

Nom ACL

de l'IP à l'IP Masque de réseau

Failure URL

Store ACL values in file Configuration de Squid Separate file ...

Just use existing contents of file?

[Retourner à Liste ACL](#) | [Retourner à l'index de squid](#)

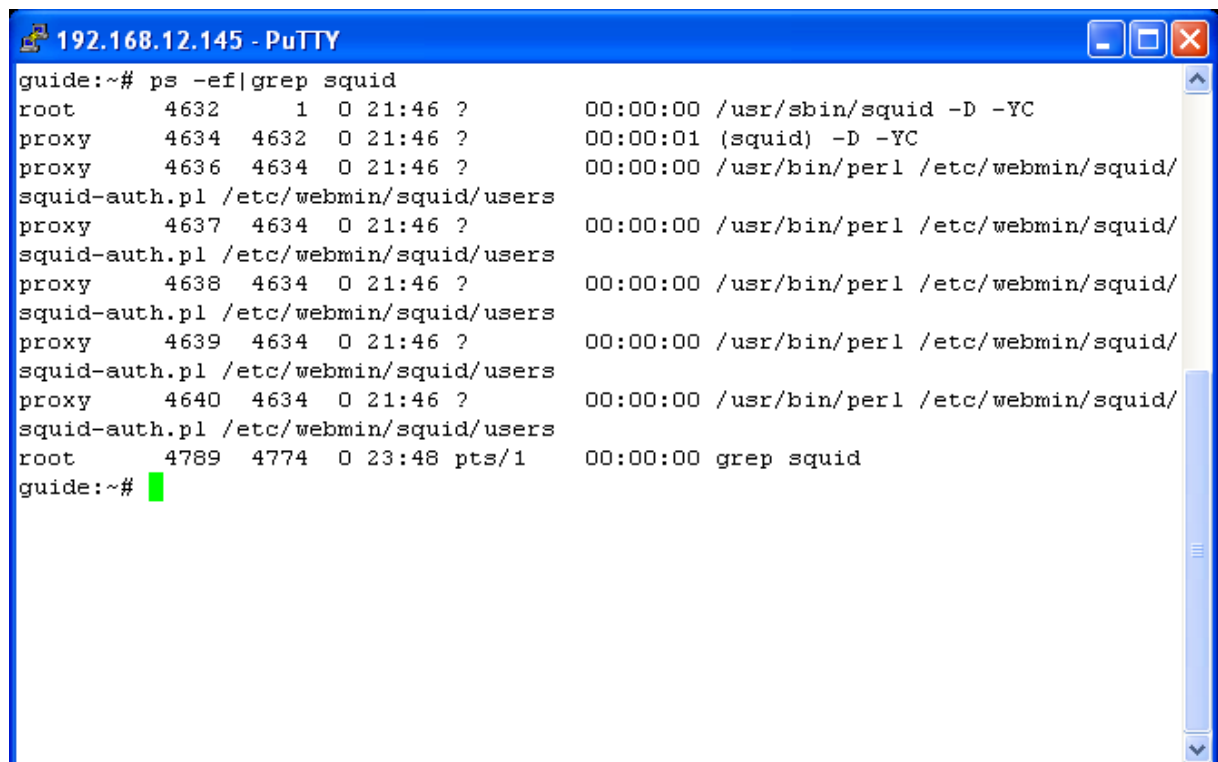
- De même que l'ACL précédente, ajoutez une restriction à cette ACL en lui donnant l'action «Autorisé».
- Et faire remonter la restriction que vous venez de créerz juste au-dessus de la restriction « interdit all ».

- **Test de fonctionnement de squid :**

- Dans l'interface principale de squid, cliquez sur « Appliquez les changements » en haut de la page.
- Ensuite, vérifiez le bon fonctionnement de Squid en utilisant le Shell.

```
guide:~# /etc/init.d/squid status  
squid is running.
```

Ou



```
192.168.12.145 - PuTTY  
guide:~# ps -ef|grep squid  
root      4632      1  0 21:46 ?        00:00:00 /usr/sbin/squid -D -YC  
proxy    4634    4632  0 21:46 ?        00:00:01 (squid) -D -YC  
proxy    4636    4634  0 21:46 ?        00:00:00 /usr/bin/perl /etc/webmin/squid/  
squid-auth.pl /etc/webmin/squid/users  
proxy    4637    4634  0 21:46 ?        00:00:00 /usr/bin/perl /etc/webmin/squid/  
squid-auth.pl /etc/webmin/squid/users  
proxy    4638    4634  0 21:46 ?        00:00:00 /usr/bin/perl /etc/webmin/squid/  
squid-auth.pl /etc/webmin/squid/users  
proxy    4639    4634  0 21:46 ?        00:00:00 /usr/bin/perl /etc/webmin/squid/  
squid-auth.pl /etc/webmin/squid/users  
proxy    4640    4634  0 21:46 ?        00:00:00 /usr/bin/perl /etc/webmin/squid/  
squid-auth.pl /etc/webmin/squid/users  
root      4789    4774  0 23:48 pts/1    00:00:00 grep squid  
guide:~# █
```

- Vérifier que le port d'écoute est correct.

```
guide:~# netstat -avp | grep LISTEN █
```

```
tcp        0      0 192.168.12.145:3128  *:*          LISTEN  
4634/ (squid)
```

b. SquidGuard

- Ouvrez l'onglet «serveurs» de l'interface webmin et cliquer sur l'icône «squidguard». Vous êtes invités à créer les chemins de: fichier de configuration, répertoires de la base et des journaux.

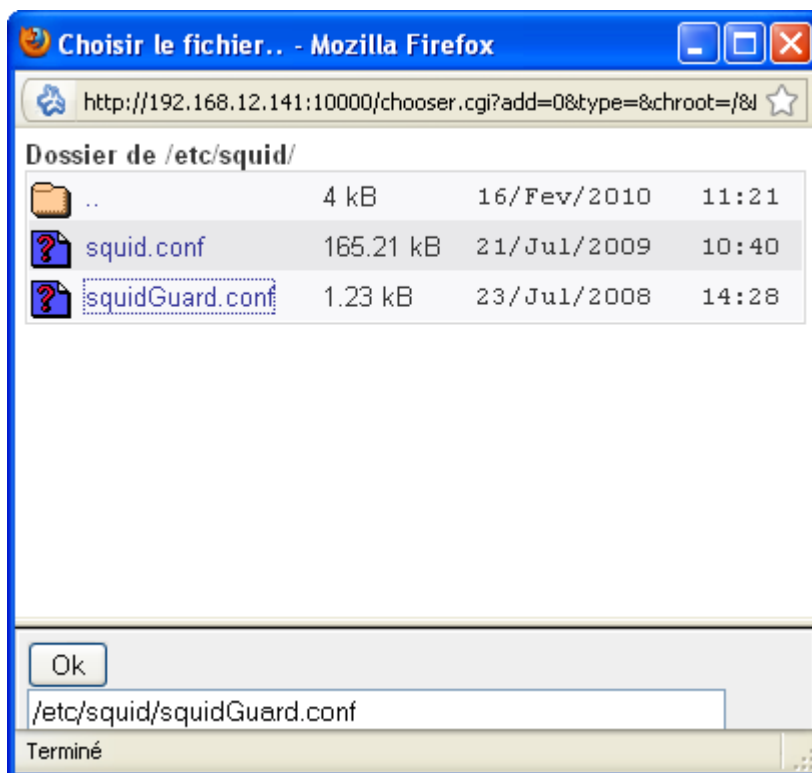
Aide.
Configuration du module

SquidGuard

Written by
Tim Niemueller
[Home://page](#)

Fichier de configuration non défini

Ce module doit connaître l'emplacement du fichier de configuration de SquidGuard. Veuillez saisir le chemin d'accès absolu (!).



Aide.
Configuration du module

SquidGuard

Written by
Tim Niemueller
[Home://page](#)

Fichier de configuration non défini

Ce module doit connaître l'emplacement du fichier de configuration de SquidGuard. Veuillez saisir le chemin d'accès absolu (!).

Aide.. Configuration du module


SquidGuard

Written by
Tim Niemueller
[Home://page](#)

UID/GID not set

The SquidGuard Webmin Modules must now, as which user and group the Squid daemon runs as.

User: ...

Group: 

- A ce stade, Squidguard est configuré mais n'est pas encore opérationnel tant que Squid n'est pas encore informé de sa présence. Alors cette fenêtre vous invite à configurer squid.

Aide.. Configuration du module

SquidGuard

Written by
Tim Niemueller
[Home://page](#)

Squid n'est pas configuré

Il semble que Squid ne soit pas configuré pour utiliser SquidGuard comme redirecteur. C'est pourtant indispensable au fonctionnement de SquidGuard. Cliquer sur 'Configurer Squid' pour apporter les modifications nécess au fichier de configuration de Squid.


[Configurer Squid](#)

- Vous devriez avoir ceci dans la fenêtre Squidguard de Webmin


Aide.. Configuration du module

SquidGuard


Written by
Tim Niemueller
[Home://page](#)




Chemins d'accès




Plages horaires




Clients




Destinations



Règles de réécriture



Listes de contrôle d'accès



Listes noires

[v 0.91.2]

- **Ajout des clients :**

- Vous pouvez ajouter vos clients en cliquant sur l'icône « client », faites saisir le nom du groupe client et cliquez sur « Ajouter des nouveaux clients ».

Index du module Written by
Tim Niemueller
[Home://page](#)

Clients

Liste des clients

Identifiant des nouveaux clients :

[← Retourner à l'index du module](#)

Index du module Written by
Tim Niemueller
[Home://page](#)

Clients

Liste des clients



mes_client

Identifiant des nouveaux clients :


[← Retourner à l'index du module](#)

- Editez le groupe de clients que vous venez de créer, comme ci-dessous il vous permet de créer les utilisateurs selon l'adresse de leur machine, leur plage d'adresse, leur nom... pour cet exemple j'ai ajouté une adresse hôte.

Index du module Written by
Tim Niemueller
[Home://page](#)

Edition des clients

Hôtes définis pour les clients 'mes_client'



192.168.6.182

Plage horaire:

[← Retourner à la liste des clients](#)

- **Ajout de destination :**

Index du module Written by
Tim Niemueller
[Home://page](#)

Destinations

Liste des destinations (Serveurs Web)



good



local

Identifiant des destinations:

[Retourner à l'index du module](#)

- Le groupe « good » pour le réseau externe et le groupe « local » pour le réseau interne. Vous pouvez donc éditez un groupe et ajouter un nom de domaine ou **un** URL.

Index du module Written by
Tim Niemueller
[Home://page](#)

Editer les destinations

Domaines pour les destinations 'good'

Aucun domaine pour ces destinations.
[[Ajouter un domaine](#)]

URLs pour les destinations 'good'

Aucune URL pour ces destinations.
[[Ajouter une URL](#)]

Expressions régulières pour les destinations 'good'

Aucune expressions régulières pour ces destinations.
[[Ajouter une expression régulière](#)]

Plage horaire:

[[Effacer ces destinations](#)]

[Retourner à list of destination groups](#)

- **Listes de contrôle d'accès :**

Squidguard redirige les URLs interdits vers un URL local. Généralement, il s'agit d'un script CGI.

- Si cet URL de redirection n'est pas indiqué, Squidguard ne sache pas où rediriger les requêtes interdites, alors il les laissera passer.
- Il est donc impératif d'installer un tel script ou une page d'avertissement quelconque vers laquelle rediriger les URLs interdits en spécifiant son chemin dans l'ACL « default ».
- Cliquez sur « Listes de contrôle d'accès », spécifiez les clients puis cliquez sur « Ajouter une règle ».

- Dans cet exemple, j'ai ajouté une règle qui redirige toutes connexions, où la destination n'est pas configurée dans la liste des URLs « good », vers une page interne.

Index du module Editer une règle Written by
Tim Niemueller
[Home://page](#)

Editer une règle

Clients	mes_client	Destinations	IPs	Règles de réécriture	Listes noires
Timespace	None		!IPs		
Mode			good		
Plages horaires	workhours		!good		
			local		
			!local		

Rediriger vers l'URL : Défaut http://192.168.12.145/access.html

[Retourner à list ACLs](#)

c. DansGuardian

- Sous la catégorie serveur, cliquez sur « DansGuardian filtrage de contenu web », cliquez sur configuration du module pour vérifier les chemins du répertoire de configuration, du log et du binaire. Puis sauvegardez.

Aide..
DansGuardian
Démarrer DG

Configuration du module
Version ? (Version du Module 0.7.0beta1b)
Rechercher la documentation..

DansGuardian - le filtrage de contenu web pour tous

Attention - dansguardian ne trouve pas de fichier binaire, vous avez peut-être besoin de mettre à jour votre **Configuration du module** (en particulier les chemins.)
(Chemin d'accès au fichier: /sbin/dansguardian)

Attention - la version de dansguardian vous avez n'est pas supporté par ce module Webmin version
Version du Module 0.7.0beta1b DG soutient version 2.9/2.10
actuellement installés DG version ?

Attention - courir en tant que root (superles risques de nouveaux fichiers ne sont pas lisibles par la production dansguardian)

Configuration

Pour le module DansGuardian Filtrage De Contenu Web

Options configurables pour DansGuardian Filtrage De Contenu Web

Full chemin de la DG de configuration (etc) répertoire	<input type="text" value="/etc/dansguardian"/> ...
Full chemin de la DG pid file	<input type="text" value="/var/run/dansguardian.pid"/> ...
Full chemin de la DG binaire	<input type="text" value="/usr/sbin/dansguardian"/> ...
Full chemin de la DG log	<input type="text" value="/var/log/dansguardian"/> ...
Full chemin de la DG messages fichier (ou littéralement 'followDansGuardian')	<input type="text" value="followDansGuardian"/> ...
Format de la DG logfile	<input checked="" type="radio"/> followDansGuardian <input type="radio"/> vigueur DG indigène <input type="radio"/> vigueur CSV <input type="radio"/> vigueur Squid indigène (aucun journal d'analyse) <input type="radio"/> vigueur onglet délimité
Command à redémarrer DG (si permis)	<input type="radio"/> Module built-in -ou- System <input checked="" type="radio"/> <input type="text" value="/etc/init.d/dansguardian"/>
Auto redémarrer DG en tant que de besoin (si permis)	<input checked="" type="radio"/> explicite redémarrage manuel seulement <input type="radio"/> redémarrer automatiquement
Command pour commencer DG (si permis)	<input type="radio"/> Module built-in -ou- System <input checked="" type="radio"/> <input type="text" value="/etc/init.d/dansguardian"/>
Command d'arrêter DG (si permis)	<input type="radio"/> Module built-in -ou- System <input checked="" type="radio"/> <input type="text" value="/etc/init.d/dansguardian"/>
Auto recharger DG groupes en tant que de besoin (si permis)	<input type="radio"/> rechargement manuel explicite que <input checked="" type="radio"/> recharge automatiquement
Include "fixe" des listes (blacklists/phraselists/etc.) dans les écrans	<input checked="" type="radio"/> exclure "fixes" de l'affichage des listes <input type="radio"/> écran "fixe" listes trop

- Editez le fichier «/etc/dansguardian/dansguardian.conf» et commentez ou supprimez la ligne « UNCONFIGURED ».

```

192.168.12.145 - PuTTY
# DansGuardian config file for version 2.9.9.4

# **NOTE** as of version 2.7.5 most of the list files are now in dansguardianf1.conf

UNCONFIGURED - Please remove this line after configuration

# Web Access Denied Reporting (does not affect logging)
#
# -1 = log, but do not block - Stealth mode
# 0 = just say 'Access Denied'
# 1 = report why but not what denied phrase
# 2 = report fully
# 3 = use HTML template file (accessdeniedaddress ignored) - recommended
#
reportinglevel = 3

# Language dir where languages are stored for internationalisation.
# The HTML template within this dir is only used when reportinglevel
# is set to 3. When used, DansGuardian will display the HTML file instead of
# using the perl cgi script. This option is faster, cleaner
# and easier to customise the access denied page.
# The language file is used no matter what setting however.
"dansguardian.conf" 612 lines, 22504 characters
  
```

- Retournez vers la page principale de DansGuardian d'index et cliquez sur « Voir et modifier la configuration ».

- Faire vérifier le port d'écoute de DansGuardian, ainsi que l'IP et le port du proxy squid. Puis cliquez sur le bouton « mise à jour ».

Aide.. Configuration du module

DansGuardian
Version 2.9.9.4 (Version du Module 0.7.0beta1b)

Démarrer DG
Rechercher la documentation..

DansGuardian - le filtrage de contenu web pour tous

Attention - courir en tant que root (superles risques de nouveaux fichiers ne sont pas lisibles par la production dansguardian)



STATUS
Afficher le statut de DansGuardian



ANALYZE
Consulter les logs de DG



SEARCH
Recherche de mots pour mots (ou de domaine ou URL)



SYSCONF
Voir/Modifier la configuration



PLUGINS
Voir/Modifier la Plugin configuration



SYSLISTS
Voir/Modifier les fichiers



XLATE
Voir/Modifier les messages système (traduction)



ASSIGN
Voir/Modifier groupe de filtrage Assignments



CONFS
Voir/Modifier Un filtre du Groupe de la Base de Config



LISTS
Voir/Modifier Un filtre du Groupe Lists)



MULTI
Voir Comment Listes et Configs Pour filtres multiples groupes sont constitués



SETUP
Set Up Listes & Configs Pour les filtres multiples Groupes

Index du module Aide.. Configuration du module

DansGuardian
Version 2.9.9.4 (Version du Module 0.7.0beta1b)

Démarrer DG
Rechercher la documentation..

Voir/Modifier la configuration

Étant donné le nom d'une option, passez à l'onglet qui se retrouve sur la

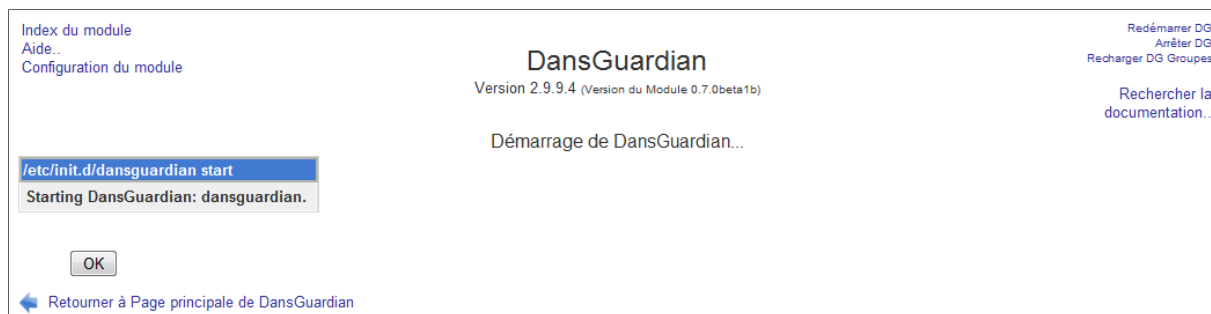
- select option -

(Cliquez sur le nom d'une option de configuration pour afficher une page d'aide.)

Network Paramètres

Nom	L'échelle Du Système Valeur	Définir?	Défaut
Adresse IP d'écoute (filterip)	<input type="text"/>	⇐ <input checked="" type="checkbox"/>	
Port d'écoute (filterport)	<input type="text" value="8080"/>	⇐ <input checked="" type="checkbox"/>	
Proxy IP (proxypip)	<input type="text" value="127.0.0.1"/>	⇐ <input checked="" type="checkbox"/>	
Port du Proxy (proxypport)	<input type="text" value="3128"/>	⇐ <input checked="" type="checkbox"/>	
Ajoute X-Forwarded-For: clientip à la requête HTTP (forwardedfor)	<input type="checkbox"/>	⇐ <input checked="" type="checkbox"/>	<input type="checkbox"/>
Utilisez x transmis pour (usexforwardedfor)	<input type="checkbox"/>	⇐ <input checked="" type="checkbox"/>	<input type="checkbox"/>
Maximum Allowed IP (maxips)	<input type="text" value="0"/>	⇐ <input checked="" type="checkbox"/>	

- Redémarrer Squid, ensuite Démarrer DansGuardian.



d. Mise à jour de Dansguardian

Certains sites non autorisés auront tendance à disparaître de la toile avec l'apparition de nouveaux. De même, des phrases interdites pourraient devenir obsolète avec l'apparition de nouvelles inconnues dans la base de connaissance de Dansguardian.

Il est donc utile de maintenir la blacklist et la phraselist à jour. Vous pouvez vous rendre sur le site <http://URLBlacklist.com> pour télécharger la dernière mise à jour de la blacklist.

Enregistrez-la dans votre répertoire personnel et ensuite décompressez-la dans le répertoire `/etc/dansguardian` par :

```
# tar -xzf bigblacklist.tar.gz
```

De même pour la mise à jour de phraselist <http://contentfilter.futuragts.com/phraselists/>

Maintenant vous pouvez configurer la blacklist de votre dansguardian :

- L'autorisation d'accès à vos sites se trouve dans le fichier `/etc/dansguardian/exceptionsitelist`
- A l'inverse, `/etc/dansguardian/banneditelist` gère les sites non autorisés (vous pouvez tester avec `badboys.com` qui est l'exemple par défaut de ce fichier et dansguardian vous en refusera l'accès).
- Bloquer tout sites contenant une phrase se trouvant dans le fichier `/etc/dansguardian/bannedphraselist`.
- Autoriser des phrases dans le contenu d'un site dans le fichier `/etc/dansguardian/exception phraselist`.

N.B : le site URLBlacklist.com est un site payant qui ne permet qu'un et un seul téléchargement gratuit de la blacklist. Il vous faudra ensuite, pour maintenir votre blacklist à jour, soit souscrire à un abonnement, soit trouver un site qui fournisse ce service gratuitement.

e. Configuration du client

Configurez le client pour qu'il utilise le service proxy sur les requêtes HTTP. Donc sous l'onglet outils du navigateur cliquez sur « options internet/connexions/paramètres réseau. Puis cochez le serveur proxy et faites entrer l'adresse et le port de l'écoute de Dansguardian.

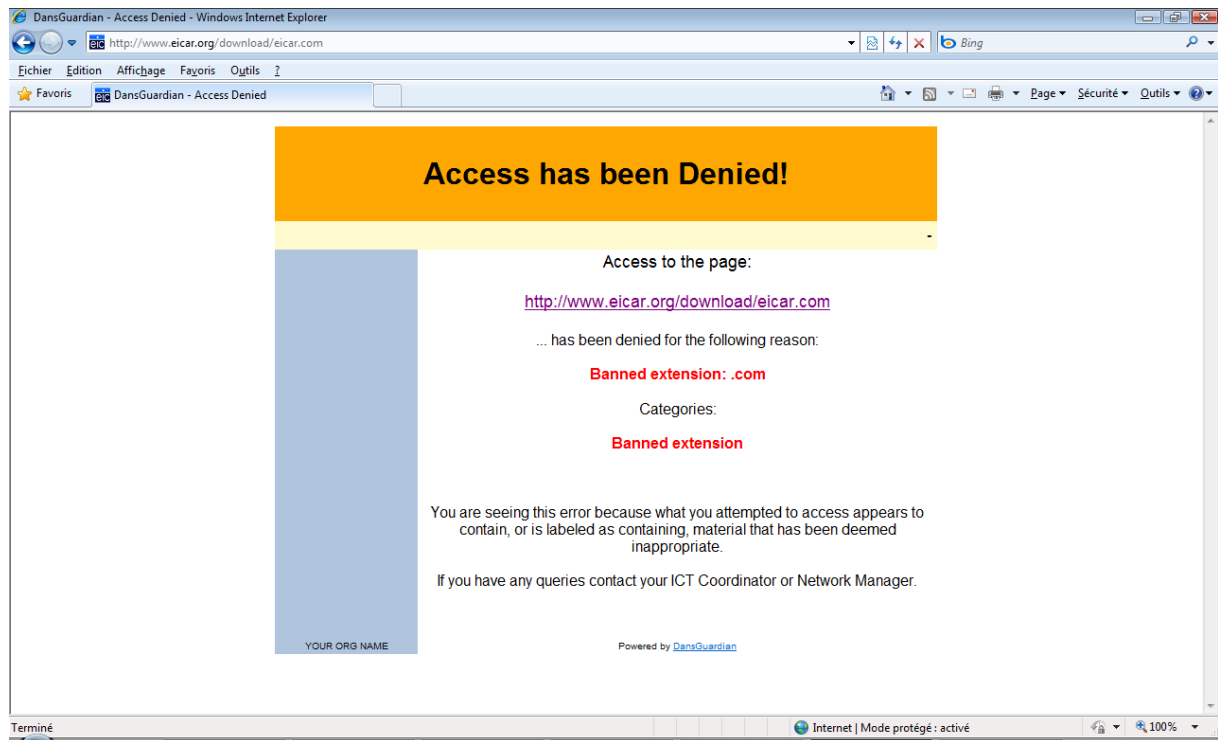


5. TEST DE FONCTIONNEMENT

Ouvrez maintenant votre navigateur et rendez-vous sur ce site, qui implémente plusieurs types de fichiers contenant le "virus de test" EICAR, afin de tester le filtre Dansguardian:

<http://www.eicar.org/download/eicar.com>

Cette page doit être refusée !



N.B :

- 1) Il se peut que DansGuardian génère des faux-positifs en refusant l'accès à des pages telles que google. L'autorisation d'accès à vos sites se trouve dans le fichier /etc/dansguardian/exceptionsitelist. A l'inverse, /etc/dansguardian/bannedsitelist gère les sites non autorisés.
 - 2) N'oubliez pas de relancer DansGuardian à chaque modification des listes.
-