Version : **2021.01**

Dernière mise-à-jour : 2021/03/05 08:50

LRF409 - Serveur Proxy

Contenu du module

Présentation

Squid est un serveur mandataire (proxy cache) sous Linux. Squid permet d'accélérer l'accès à Internet en stockant des fichiers reçus des sites visités en mémoire cache. Notez, cependant que Squid n'est pas un serveur proxy pour les protocoles POP, SMTP et NNTP car il ne peut traiter que les protocoles HTTP et FTP et d'une manière limitée les protocoles TLS, SSL, Internet Gopher et HTTPS.

Il est utile de noter ici qu'un serveur proxy utilise beaucoup d'espace disque pour le cache et pour ses logs. Dans la mesure du possible donc, il faut prévoir une partition à part, d'une taille importante pour le cache et éventuellement une autre partition pour les fichiers logs.

Installation

Utilisez yum :

```
# yum install squid [Entrée]
```

```
[root@centos6 ~]# yum install squid
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package squid.i686 7:3.1.10-1.el6_2.4 set to be updated
--> Processing Dependency: perl(DBI) for package: 7:squid-3.1.10-1.el6_2.4.i686
--> Running transaction check
---> Package perl-DBI.i686 0:1.609-4.el6 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                 Arch                                 Version
Repository                              Size
================================================================================
================================================================================
Installing:
 squid                                   i686                                 7:3.1.10-1.el6_2.4
updates                                1.7 M
```

```
Installing for dependencies:
 perl-DBI                                  i686                                  1.609-4.el6
base                                     705 k

Transaction Summary
================================================================================================================================
================================================================
Install       2 Package(s)
Upgrade       0 Package(s)

Total download size: 2.4 M
Installed size: 7.3 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): perl-DBI-1.609-4.el6.i686.rpm
| 705 kB     00:00
(2/2): squid-3.1.10-1.el6_2.4.i686.rpm
| 1.7 MB     00:01
--------------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------
Total
1.2 MB/s | 2.4 MB     00:01
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : perl-DBI-1.609-4.el6.i686
1/2
  Installing     : 7:squid-3.1.10-1.el6_2.4.i686
2/2

Installed:
  squid.i686 7:3.1.10-1.el6_2.4
```

```
Dependency Installed:
  perl-DBI.i686 0:1.609-4.el6

Complete!
```

Configurez ensuite le service squid pour un démarrage automatique à chaque démarrage du système :

```
[root@centos6 ~]# chkconfig --level 345 squid on
[root@centos6 ~]# chkconfig --list squid
squid           0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Options de la commande squid

Les options de cette commande sont :

```
[root@centos6 squidguard]# squid -h
Usage: squid [-cdhvzCFNRVYX] [-s | -l facility] [-f config-file] [-[au] port] [-k signal]
       -a port   Specify HTTP port number (default: 3128).
       -d level  Write debugging to stderr also.
       -f file   Use given config-file instead of
                 /etc/squid/squid.conf
       -h        Print help message.
       -k reconfigure|rotate|shutdown|interrupt|kill|debug|check|parse
                 Parse configuration file, then send signal to
                 running copy (except -k parse) and exit.
       -s | -l facility
                 Enable logging to syslog.
       -u port   Specify ICP port number (default: 3130), disable with 0.
       -v        Print version.
       -z        Create swap directories
       -C        Do not catch fatal signals.
       -D        OBSOLETE. Scheduled for removal.
       -F        Don't serve any requests until store is rebuilt.
```

```
       -N        No daemon mode.
       -R        Do not set REUSEADDR on port.
       -S        Double-check swap during rebuild.
       -X        Force full debugging.
       -Y        Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.
```

Configuration

Créez un fichier squid.conf sans commentaires :

```
[root@centos6 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/squid/squid.conf > squid.conf
```

Ouvrez le fichier **/tmp/squid.conf** avec l'éditeur de votre choix. Ajoutez les directives ci-dessous.

Cette directive stipule la taille en Mo, ici 124 MB, du cache en mémoire :

```
cache_mem 124 MB
```

Cette directive spécifie l'endroit et la taille, ici 3 641 Mo, du cache sur disque :

```
cache_dir ufs /var/spool/squid 3641 16 256
```

Cette directive correspond à la règle nécessaire pour que les machines du réseau local puissent se connecter à Squid :

```
acl mynetwork src 10.0.2.0/24
```

Cette directive spécifie l'emplacement du fichier log qui contiendra une entrée pour chaque requête d'un client :

```
cache_access_log /var/log/squid/access.log
```

Cette directive spécifie l'emplacement du fichier log général :

```
cache_log /var/log/squid/cache.log
```

Cette directive accorde l'accès au proxy à partir de votre réseau :

```
http_access allow mynetwork
```

Cette directive définit le nom d'hôte du serveur squid :

```
visible_hostname proxy.fenestros.loc
```

Sauvegardez votre fichier et déplacez-le à /etc/squid :

```
[root@centos6 tmp]# mv /tmp/squid.conf /etc/squid/
mv : voulez-vous écraser « /etc/squid/squid.conf » ? o
```

Vous devez maintenant vérifier le syntaxe de votre fichier de configuration à l'aide de la commande :

```
[root@centos6 tmp]# squid -k parse
2012/06/01 09:00:41| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2012/06/01 09:00:41| Initializing https proxy context
```

En cas d'erreur, consultez la ligne indiquée et corrigez l'erreur.

Voici le fichier édité :

squid.conf

```
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
```

```
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
http_access allow localhost
http_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
coredump_dir /var/spool/squid
refresh_pattern ^ftp:       1440    20%    10080
refresh_pattern ^gopher:    1440    0%    1440
refresh_pattern -i (/cgi-bin/|?) 0  0%    0
refresh_pattern .       0    20%    4320
cache_mem 124 MB
cache_dir ufs /var/spool/squid 3641 16 256
acl mynetwork src 10.0.2.0/24
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
http_access allow mynetwork
```

```
visible_hostname proxy.fenestros.loc
```

Si squid doit passer par le proxy de votre société, ajoutez la ligne suivante à votre fichier de configuration squid.conf en modifiant les variables :

cache_peer $PROXY_HOST parent $PROXY_PORT 0 no-query default proxy-only login=$PROXY_USER:$PROXY_PASSWORD

Important - Attention à l'ordre des directives dans le fichier ci-dessus. En cas de règles contradictoires, c'est la première règle troiuvée qui est appliquée.

Sous CentOS 6, SELinux est en mode **enforcing** :

```
[root@centos6 tmp]# getenforce
Enforcing
```

Afin de poursuivre, il faut changer le mode de SELinux en **permissive** :

```
[root@centos6 tmp]# setenforce permissive
[root@centos6 tmp]# getenforce
Permissive
```

Démarrez le service squid :

```
[root@centos6 tmp]# service squid start
init_cache_dir /var/spool/squid... Démarrage de squid : .  [  OK  ]
```

Si vous obtenez une sortie similaire à celle ci-dessous, vous avez oubliez de passer SELinux en mode **permissive** :

```
[root@centos6 tmp]# service squid start
Démarrage de squid :                                       [ÉCHOUÉ]
2012/11/09 14:46:33| Processing Configuration File: /etc/squid/squid.conf (depth 0)
FATAL: Unable to open configuration file: /etc/squid/squid.conf: (13) Permission denied
Squid Cache (Version 3.1.10): Terminated abnormally.
CPU Usage: 0.011 seconds = 0.007 user + 0.004 sys
Maximum Resident Size: 18928 KB
Page faults with physical i/o: 0
```

L'Extension squidGuard

squidGuard est une **extension** pour le serveur proxy **Squid**. **squidGuard** est un **redirecteur** qui permet de filtrer l'accès à des sites suivant des règles en affichant à leur place une ou plusieurs pages html définies par root.

squidGuard se trouve dans les dépôts **rpm-forge**.Installez donc ce dépôt ainsi :

```
[root@centos6 tmp]# rpm -Uhv
http://apt.sw.be/redhat/el6/en/i386/rpmforge/RPMS/rpmforge-release-0.5.2-2.el6.rf.i686.rpm
```

Installez ensuite squidGuard et ses **blacklists** :

```
[root@centos6 tmp]# yum install squidguard squidguard-blacklists
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package squidguard.i686 0:1.3-2.el6.rf set to be updated
```

```
---> Package squidguard-blacklists.noarch 1:1.3-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                        Arch                              Version
Repository                              Size
================================================================================================================
================================================
Installing:
 squidguard                                     i686                              1.3-2.el6.rf
rpmforge                                90 k
 squidguard-blacklists                          noarch                            1:1.3-1.el6.rf
rpmforge                                19 M

Transaction Summary
================================================================================================================
================================================
Install       2 Package(s)
Upgrade       0 Package(s)

Total download size: 19 M
Installed size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): squidguard-1.3-2.el6.rf.i686.rpm
|  90 kB     00:00
(2/2): squidguard-blacklists-1.3-1.el6.rf.noarch.rpm
|  19 MB     00:14
----------------------------------------------------------------------------------------------------------------
------------------------------------------------
Total
```

```
1.3 MB/s |  19 MB     00:14
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : squidguard-1.3-2.el6.rf.i686
1/2
  Installing     : 1:squidguard-blacklists-1.3-1.el6.rf.noarch
2/2

Installed:
  squidguard.i686 0:1.3-2.el6.rf                                                squidguard-blacklists.noarch
1:1.3-1.el6.rf

Complete!
```

Vous devez maintenant indiquer à **squid** que vous allez utiliser squidGuard.

Ajoutez les lignes suivantes au fichier **/etc/squid/squid.conf** :

```
redirect_program /usr/bin/squidGuard -c /etc/squid/squidguard.conf
redirect_children 4
```

Consultez le fichier **/etc/squid/squidguard.conf**.

```
[root@centos6 tmp]# cat /etc/squid/squidguard.conf
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard
logdir /var/log/squidguard

#
```

```
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {
    weekly mtwhf 08:00 - 16:30
    date *-*-01  08:00 - 16:30
}

#
# REWRITE RULES:
#

rew dmz {
    s@://admin/@://admin.foo.bar.de/@i
    s@://foo.bar.de/@://www.foo.bar.de/@i
}

#
# SOURCE ADDRESSES:
#

src admin {
    ip        1.2.3.4 1.2.3.5
    user        root foo bar
    within         workhours
}

src foo-clients {
    ip        172.16.2.32-172.16.2.100 172.16.2.100 172.16.2.200
}

src bar-clients {
    ip        172.16.4.0/26
```

```
}

#
# DESTINATION CLASSES:
#

dest good {
}

dest local {
}

dest adult {
    domainlist    dest/adult/domains
    urllist        dest/adult/urls
    expressionlist    dest/adult/expressions
    redirect
http://admin.foo.bar.de/cgi/blocked?clientaddr=%a+clientname=%n+clientuser=%i+clientgroup=%s+targetgroup=%t+url=%
u
}


acl {
    admin {
        pass     any
    }

    foo-clients within workhours {
        pass     good !in-addr !adult any
    } else {
        pass any
    }

    bar-clients {
```

```
        pass    local none
    }

    default {
        pass     local none
        rewrite     dmz
        redirect
http://admin.foo.bar.de/cgi/blocked?clientaddr=%a+clientname=%n+clientuser=%i+clientgroup=%s+targetgroup=%t+url=%
u
    }
}
```

Remplacez ce fichier par le suivant :

squidguard.conf

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard
logdir /var/log/squidguard

time workhours {
        weekly s 09:30-12:00 13:00-19:00
        weekly m 09:00-12:00 13:00-19:00
        weekly t 09:00-11:00 12:00-19:00
        weekly w 09:00-12:00 12:00-18:00
        weekly h 09:00-13:00 13:00-18:00
        weekly f 09:00-12:00 13:30-18:00
        weekly a 08:20-13:00 13:30-19:00
}

#
```

```
# SOURCE ADDRESSES:
#

src privilegedsource {
        iplist  privilegedsource/ips
}

src bannedsource {
        iplist  bannedsource/ips
}

src lansource {
        iplist lansource/lan
}

#
# DESTINATION CLASSES:
#

dest porn {
        domainlist porn/domains
        urllist porn/urls
}

dest adult {
        domainlist adult/domains
        urllist adult/urls
        expressionlist  adult/expressions
}

dest audio-video {
        domainlist audio-video/domains
        urllist audio-video/urls
}
```

```
dest forums {
        domainlist forums/domains
        urllist forums/urls
        expressionlist  forums/expressions
}

dest hacking {
        domainlist hacking/domains
        urllist hacking/urls
}

dest redirector {
        domainlist redirector/domains
        urllist redirector/urls
}

dest warez {
        domainlist warez/domains
         urllist warez/urls
}

dest ads {
         domainlist ads/domains
         urllist ads/urls
}

dest aggressive {
        domainlist aggressive/domains
        urllist aggressive/urls
}

dest drugs {
         domainlist drugs/domains
```

```
         urllist drugs/urls
}

dest gambling {
         domainlist gambling/domains
         urllist gambling/urls
}

dest violence {
        domainlist violence/domains
        urllist violence/urls
        expressionlist  violence/expressions
}

#
# ACLs
#
acl {
        privilegedsource {
                pass !ads all
                redirect http://localhost/access-denied.html?url=%u

        }

        bannedsource {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }

        lansource {
                pass !porn !adult !audio-video !forums !hacking !redirector !warez !ads !aggressive !drugs
!gambling !violence all
                redirect http://localhost/access-denied.html?url=%u
```

```
        }


        default {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }
}
```

Ce fichier contient des sections dont :

Nom de la Section	***Qui déclare***
CONFIGURATION DIRECTORIES	Les **Chemins** des fichiers db et des logs
TIME RULES	Les **Plages Horaires** de connexion
SOURCE ADDRESES	Les **Clients** se connectant au proxy
DESTINATION RULES	Les règles gouvernant les **URLs** de Destination
ACL	Les Règles de Contrôle d'Accès (ACL)

Le fichier de configuration de squidGuard contient des directives de chargement des bases de données. Ces directives contiennent uniquement les noms des fichiers sans extension, par exemple, **domains**.

squidGuard utilise des bases de données de type **Berkeley**.

Ces fichiers sont stockés dans **/var/lib/squidguard/** et sont au format db ou au format texte.

squidGuard utilise une base de données divisée en catégories telles **local**, **clients** etc.

Chaque catégorie peut être composée de listes de **domaines**, d'**URL**s ou d'**expressions régulières**.

```
[root@centos6 tmp]# ls /var/lib/squidguard/
ads  adult  aggressive  audio-video  drugs  forums  gambling  hacking  local  mail  proxy  violence  warez
```

Lors de son lancement squidGuard essaie dans un premier temps de localiser le fichier **.db**. S'il ne parvient pas, il charge la version texte de la liste et construit les **B-arbres** en mémoire.

Cette construction de B-arbres peut ralentir le démarrage de **Squid** sensiblement.

Afin de palier à cet éventuel problème, les fichiers texte peuvent être transformés en base de données pré-construites à l'aide de la commande :

```
squidGuard -C chemin_et_nom_du_fichier_texte [Entrée]
```

Installez maintenant la mise à jour de la liste **blacklist**.

Premièrement téléchargez la liste suivante :

```
[root@centos6 tmp]# wget http://www.shallalist.de/Downloads/shallalist.tar.gz
--2012-06-01 09:20:46--  http://www.shallalist.de/Downloads/shallalist.tar.gz
Résolution de www.shallalist.de... 78.47.242.85
Connexion vers www.shallalist.de|78.47.242.85|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 9907814 (9,4M) [application/x-tar]
Sauvegarde en : «shallalist.tar.gz»

100%[=======================================================================================================
==================>] 9 907 814    804K/s   ds 11s

2012-06-01 09:20:57 (873 KB/s) - «shallalist.tar.gz» sauvegardé [9907814/9907814]
```

Désarchivez blacklists.tar.gz :

```
[root@centos6 tmp]# tar xvf shallalist.tar.gz
BL/
BL/porn/
```

```
BL/porn/domains
BL/porn/urls
BL/gamble/
BL/gamble/domains
BL/gamble/urls
BL/chat/
BL/chat/domains
BL/chat/urls
BL/automobile/
BL/automobile/cars/
BL/automobile/cars/domains
BL/automobile/cars/urls
BL/automobile/bikes/
BL/automobile/bikes/domains
BL/automobile/bikes/urls
BL/automobile/boats/
BL/automobile/boats/domains
BL/automobile/boats/urls
BL/automobile/planes/
...
```

Créez ensuite les répertoires et fichiers pour les ACL des adresses IP :

```
[root@centos6 tmp]# cd /var/lib/squidguard
[root@centos6 squidguard]# mkdir privilegedsource bannedsource lansource
[root@centos6 squidguard]# touch privilegedsource/ips bannedsource/ips lansource/lan
```

Éditez le fichier **/var/lib/squidguard/lansource/lan** :

lan

```
127.0.0.0/8
10.0.2.0/24
```

De cette façon, vous autorisez votre propre machine ainsi que les machines de votre réseau à utiliser le serveur proxy.

Copiez les fichiers du répertoire **/tmp/BL** vers **/var/lib/squidguard/** :

```
[root@centos6 squidguard]# cp -pfR /tmp/BL/* /var/lib/squidguard/
cp : voulez-vous écraser « /var/lib/squidguard/aggressive/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/aggressive/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/drugs/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/drugs/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/hacking/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/hacking/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/violence/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/violence/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/warez/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/warez/urls » ? o
```

Pré-générez maintenant les B-arbres des listes et mettez-les à jour :

```
[root@centos6 squidguard]# squidGuard -C all
Processing file and database /var/lib/squidguard/porn/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/porn/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/adult/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/adult/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/audio-video/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/audio-video/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/forums/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/forums/urls
```

```
Processing file and database /var/lib/squidguard/hacking/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/hacking/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/redirector/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/redirector/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/warez/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/warez/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/ads/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/ads/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/aggressive/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/aggressive/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/drugs/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/drugs/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/gambling/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/gambling/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/violence/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/violence/urls
    [==================================================] 100 % done
```

La commande suivante permet de mettre à jour les listes :

```
[root@centos6 squidguard]# squidGuard -u
```

Assurez-vous que /var/lib/squidguard appartient à l'utilisateur **squid** du groupe **squid**:

```
[root@centos6 squidguard]# chown -R squid:squid /var/lib/squidguard
```

Pour que **squid** prenne en compte la modification des listes, il faut utiliser la commande :

```
[root@centos6 squidguard]# squid -k reconfigure
```

Étudiez le contenu de /var/lib/squidguard/. Vous y trouverez d'autres répertoires contenant des listes selon des catégories. Notez que les fichiers à extension **.diff** sont des fichiers de **modification** de listes. Ces fichiers de modifications contiennent des instructions du type :

```
+nouvelle_entrée_à_ajouter
-ancienne_entrée_à_retirer
```

Consultez maintenant le fichier **/var/log/squidguard/squidGuard.log** et vérifiez que les fichiers ont été mis à jour correctement :

```
[root@centos6 squidguard]# cat /var/log/squidguard/squidGuard.log
2012-06-01 09:26:24 [7426] New setting: dbhome: /var/lib/squidguard
2012-06-01 09:26:24 [7426] New setting: logdir: /var/log/squidguard
2012-06-01 09:26:24 [7426] init iplist /var/lib/squidguard/privilegedsource/ips
2012-06-01 09:26:24 [7426] sourceblock privilegedsource missing active content, set inactive
2012-06-01 09:26:24 [7426] init iplist /var/lib/squidguard/bannedsource/ips
2012-06-01 09:26:24 [7426] sourceblock bannedsource missing active content, set inactive
2012-06-01 09:26:24 [7426] init iplist /var/lib/squidguard/lansource/lan
2012-06-01 09:26:24 [7426] init domainlist /var/lib/squidguard/porn/domains
2012-06-01 09:28:09 [7426] create new dbfile /var/lib/squidguard/porn/domains.db
2012-06-01 09:28:09 [7426] init urllist /var/lib/squidguard/porn/urls
2012-06-01 09:28:15 [7426] create new dbfile /var/lib/squidguard/porn/urls.db
2012-06-01 09:28:15 [7426] init domainlist /var/lib/squidguard/adult/domains
2012-06-01 09:30:28 [7426] create new dbfile /var/lib/squidguard/adult/domains.db
2012-06-01 09:30:28 [7426] init urllist /var/lib/squidguard/adult/urls
```

```
2012-06-01 09:30:41 [7426] create new dbfile /var/lib/squidguard/adult/urls.db
2012-06-01 09:30:41 [7426] init expressionlist /var/lib/squidguard/adult/expressions
2012-06-01 09:30:41 [7426] init domainlist /var/lib/squidguard/audio-video/domains
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/audio-video/domains.db
2012-06-01 09:30:42 [7426] init urllist /var/lib/squidguard/audio-video/urls
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/audio-video/urls.db
2012-06-01 09:30:42 [7426] init domainlist /var/lib/squidguard/forums/domains
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/forums/domains.db
2012-06-01 09:30:42 [7426] init urllist /var/lib/squidguard/forums/urls
2012-06-01 09:30:42 [7426] urllist empty, removed from memory
2012-06-01 09:30:42 [7426] init expressionlist /var/lib/squidguard/forums/expressions
2012-06-01 09:30:42 [7426] init domainlist /var/lib/squidguard/hacking/domains
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/hacking/domains.db
2012-06-01 09:30:42 [7426] init urllist /var/lib/squidguard/hacking/urls
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/hacking/urls.db
2012-06-01 09:30:42 [7426] init domainlist /var/lib/squidguard/redirector/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/redirector/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/redirector/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/redirector/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/warez/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/warez/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/warez/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/warez/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/ads/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/ads/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/ads/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/ads/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/aggressive/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/aggressive/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/aggressive/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/aggressive/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/drugs/domains
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/drugs/domains.db
2012-06-01 09:30:55 [7426] init urllist /var/lib/squidguard/drugs/urls
```

```
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/drugs/urls.db
2012-06-01 09:30:55 [7426] init domainlist /var/lib/squidguard/gambling/domains
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/gambling/domains.db
2012-06-01 09:30:55 [7426] init urllist /var/lib/squidguard/gambling/urls
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/gambling/urls.db
2012-06-01 09:30:55 [7426] init domainlist /var/lib/squidguard/violence/domains
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/violence/domains.db
2012-06-01 09:30:55 [7426] init urllist /var/lib/squidguard/violence/urls
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/violence/urls.db
2012-06-01 09:30:55 [7426] init expressionlist /var/lib/squidguard/violence/expressions
2012-06-01 09:30:55 [7426] squidGuard 1.3 started (1338535584.022)
2012-06-01 09:30:55 [7426] db update done
2012-06-01 09:30:55 [7426] squidGuard stopped (1338535855.695)
2012-06-01 09:37:59 [7519] New setting: dbhome: /var/lib/squidguard
2012-06-01 09:37:59 [7519] New setting: logdir: /var/log/squidguard
2012-06-01 09:37:59 [7519] init iplist /var/lib/squidguard/privilegedsource/ips
2012-06-01 09:37:59 [7519] sourceblock privilegedsource missing active content, set inactive
2012-06-01 09:37:59 [7519] init iplist /var/lib/squidguard/bannedsource/ips
2012-06-01 09:37:59 [7519] sourceblock bannedsource missing active content, set inactive
2012-06-01 09:37:59 [7519] init iplist /var/lib/squidguard/lansource/lan
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/porn/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/porn/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/porn/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/porn/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/adult/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/adult/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/adult/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/adult/urls.db
2012-06-01 09:37:59 [7519] init expressionlist /var/lib/squidguard/adult/expressions
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/audio-video/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/audio-video/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/audio-video/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/audio-video/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/forums/domains
```

```
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/forums/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/forums/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/forums/urls.db
2012-06-01 09:37:59 [7519] init expressionlist /var/lib/squidguard/forums/expressions
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/hacking/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/hacking/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/hacking/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/hacking/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/redirector/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/redirector/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/redirector/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/redirector/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/warez/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/warez/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/warez/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/warez/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/ads/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/ads/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/ads/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/ads/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/aggressive/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/aggressive/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/aggressive/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/aggressive/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/drugs/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/drugs/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/drugs/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/drugs/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/gambling/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/gambling/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/gambling/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/gambling/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/violence/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/violence/domains.db
```

```
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/violence/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/violence/urls.db
2012-06-01 09:37:59 [7519] init expressionlist /var/lib/squidguard/violence/expressions
2012-06-01 09:37:59 [7519] squidGuard 1.3 started (1338536279.458)
2012-06-01 09:37:59 [7519] db update done
2012-06-01 09:37:59 [7519] squidGuard stopped (1338536279.467)
```

Redémarrez le service squid pour que toutes vos modifications soient prises en compte :

```
[root@centos6 squidguard]# service squid restart
Arrêt de squid : .................                          [  OK  ]
Démarrage de squid : .                                     [  OK  ]
```

Créez maintenant la page **/var/www/html/access-denied.html** :

access-denied.html

```
<html>
<head>
<title>Acc&egrave;s Interdit</title>
</head>
<body>
<br>
<br>
<br>
<center>ACCES INTERDIT !!</center>
</body>
</html>
```

Puisque le serveur apache va servir la page **access-denied.html**, il convient de démarrer le service **httpd**.

Modifiez le propriétaire et le groupe du fichier **/var/www/html/access-denied.html** :

```
[root@centos6 squidguard]# chown apache:apache /var/www/html/access-denied.html
```

Options de la commande squidguard

Les options de cette commande sont :

```
[root@centos6 squidguard]# squidguard --help
squidguard: invalid option -- '-'
Usage: squidGuard [-u] [-C block] [-t time] [-c file] [-v] [-d]
Options:
  -v          : show version number
  -d          : all errors to stderr
  -c file     : load alternate configfile
  -t time     : specify startup time in the format: yyyy-mm-ddTHH:MM:SS
  -u          : update .db files from .diff files
  -C file|all : create new .db files from urls/domain files
                specified in "file".
```

T.P. #1

Configurez votre navigateur afin d'utiliser le proxy 127.0.0.1 port 3128.

Créer une whitelist

Trouver le site de google.de dans les fichiers de squidGuard est une tâche fastidieuse, d'autant plus qu'il est fort probable que d'autres sites peuvent

se trouver dans une des bases par erreur.

La façon la plus simple de remédier à ceci est de créer votre propre base de données de sites où vous accordez l'accès et de faire analyser cette base avant les autres.

Ouvrez donc le fichier **squidguard.conf** et ajoutez la section suivante :

DESTINATION CLASSES:

```
dest ok { domainlist ok/domains
          urllist ok/urls
}
```

Modifiez ensuite l'**ACL lansource** comme indiqué ci-après :

```
lansource {pass ok !porn !adult !audio-video ! ..... }
```

Votre fichier de configuration ressemblera à :

squidguard.conf

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard
logdir /var/log/squidguard

time workhours {
        weekly s 09:30-12:00 13:00-19:00
        weekly m 09:00-12:00 13:00-19:00
        weekly t 09:00-11:00 12:00-19:00
        weekly w 09:00-12:00 12:00-18:00
        weekly h 09:00-13:00 13:00-18:00
```

```
        weekly f 09:00-12:00 13:30-18:00
        weekly a 08:20-13:00 13:30-19:00
}

#
# SOURCE ADDRESSES:
#

src privilegedsource {
        iplist  privilegedsource/ips
}

src bannedsource {
        iplist  bannedsource/ips
}

src lansource {
        iplist lansource/lan
}

#
# DESTINATION CLASSES:
#

dest porn {
        domainlist porn/domains
        urllist porn/urls
}

dest adult {
        domainlist adult/domains
        urllist adult/urls
        expressionlist  adult/expressions
}
```

```
dest audio-video {
        domainlist audio-video/domains
        urllist audio-video/urls
}

dest forums {
        domainlist forums/domains
        urllist forums/urls
        expressionlist  forums/expressions
}

dest hacking {
        domainlist hacking/domains
        urllist hacking/urls
}

dest redirector {
        domainlist redirector/domains
        urllist redirector/urls
}

dest warez {
        domainlist warez/domains
         urllist warez/urls
}

dest ads {
         domainlist ads/domains
         urllist ads/urls
}

dest aggressive {
        domainlist aggressive/domains
```

```
        urllist aggressive/urls
}

dest drugs {
         domainlist drugs/domains
         urllist drugs/urls
}

dest gambling {
         domainlist gambling/domains
         urllist gambling/urls
}

dest violence {
        domainlist violence/domains
        urllist violence/urls
        expressionlist  violence/expressions
}

dest ok { domainlist ok/domains
          urllist ok/urls
}

#
# ACLs
#
acl {
        privilegedsource {
                pass !ads all
                redirect http://localhost/access-denied.html?url=%u

        }

        bannedsource {
```

```
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }

        lansource {
                pass ok !porn !adult !audio-video !forums !hacking !redirector !warez !ads !aggressive
!drugs !gambling !violence all
                redirect http://localhost/access-denied.html?url=%u
        }


        default {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }
}
```

Créez maintenant le répertoire **ok** :

```
[root@centos6 squidguard]# mkdir /var/lib/squidguard/ok
```

Et ensuite les fichiers domains et urls :

```
[root@centos6 squidguard]# touch /var/lib/squidguard/ok/domains
[root@centos6 squidguard]# touch /var/lib/squidguard/ok/urls
```

Editez ensuite le fichier **domains** en y insérant les adresses IP du site auquel vous voulez avoir accès :

domains

```
XXX.XXX.XXX.XXX
```

Editez ensuite le fichier **urls** en y insérant l'URL du site auquel vous voulez avoir accès :

urls

```
www.site.ext
site.ext
```

Pré-générez maintenant les B-arbres des listes et mettez-les à jour :

```
[root@centos6 squidguard]# squidGuard -C ok/domains
Processing file and database /var/lib/squidguard/ok/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/ok/urls
    [==================================================] 100 % done
[root@centos6 squidguard]# squidGuard -u
Processing file and database /var/lib/squidguard/ok/urls
    [==================================================] 100 % done
[root@centos6 squidguard]# squid -k reconfigure
```

Assurez-vous que les repertoires et les fichiers que vous venez de créer appartiennent à l'utilisateur **squid** du groupe **squid** :

```
[root@centos6 squidguard]# chown -R squid:squid /var/lib/squidguard/
```

Ensuite redémarrez squid :

```
[root@centos6 squidguard]# service squid restart
Arrêt de squid : ..............                            [  OK  ]
Démarrage de squid : .                                     [  OK  ]
```

Dansguardian

Squid ne peut pas contrôler le *contenu* des pages web. Pour faire ceci, il faut utiliser un logiciel de filtrage du contenu tel **Dansguardian** :

```
[root@centos6 squidguard]# yum install dansguardian
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package dansguardian.i686 0:2.10.1.1-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                Arch                           Version
Repository                           Size
================================================================================
================================================================================
Installing:
 dansguardian                           i686                           2.10.1.1-1.el6.rf
rpmforge                             454 k

Transaction Summary
================================================================================
================================================================================
Install       1 Package(s)
```

```
Upgrade       0 Package(s)

Total download size: 454 k
Installed size: 1.4 M
Is this ok [y/N]: y
Downloading Packages:
dansguardian-2.10.1.1-1.el6.rf.i686.rpm
| 454 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : dansguardian-2.10.1.1-1.el6.rf.i686
1/1

Installed:
  dansguardian.i686 0:2.10.1.1-1.el6.rf

Complete!
[root@centos6 squidguard]# chkconfig --level 345 dansguardian on
[root@centos6 squidguard]# chkconfig --list dansguardian
dansguardian    0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Dansguardian se configure grâce au fichier **/etc/dansguardian/dansguardian.conf**.

Notez que Dansguardian est un logiciel *complémentaire* à squid. En effet, Dansguardian n'est pas un proxy mais seulement un filtre.

Démarrez votre service dansguardian :

```
[root@centos6 squidguard]# service dansguardian start
Démarrage de Web Content Filter (dansguardian) :           [  OK  ]
```

Configurez votre navigateur afin d'utiliser le proxy 127.0.0.1 port 8080. Testez maintenant votre accès à Internet.