

0.1 Partage de connexion : proxy Squid

Squid est un serveur Proxy/cache qui supporte les protocoles HTTP, FTP et SSL. Un proxy est un mandataire. Lorsque votre passerelle fait proxy, cela signifie que ses clients ne se connectent pas directement à Internet, mais demande au proxy de télécharger pour eux les pages dont ils ont besoin. Ce didacticiel n'a pas vraiment pour but l'installation d'un proxy transparent, mais plutôt la configuration d'un proxy avec blacklist et restriction d'accès par ip. Pour être efficace, en plus de Squid vous devez également installer Squidguard comme indiqué ICI¹.

0.1.1 1. Installation de Squid

0.1.2 1.1 Depuis les sources

Téléchargez la dernière version stable de Squid ICI², puis installez-la par :

```
$ tar jxvf squid-xxx.tar.bz2
$ cd squid-xxx/
$ ./configure --prefix=/usr --sysconfdir=/etc/squid --enable-carp --enable-icmp --
  enable-useragent-log --enable-referer-log --enable-snmp --enable-arp-acl --
  enable-htcp --enable-cache-digests
```

Bien que le sujet ne soit ni la mise en place d'un proxy transparent ni l'installation d'un proxy ssl, je vous donne les options qu'il suffit de rajouter au configure, pour le proxy transparent :

```
--enable-ipf-transparent (si vous utilisez ipchains)
--enable-pf-transparent (si vous utilisez PF)
--enable-linux-netfilter (si vous utilisez netfilter/iptables)
```

Pour le support ssl :

```
--enable-ssl
```

La compilation et l'installation se résume toujours à :

```
$ make
$ su
<password>
# make install
# mkdir /var/log/squid
# mkdir /var/spool/squid
```

0.1.3 1.2 Depuis les paquetages

- **Debian**
apt-get install squid
- **Mandriva**
urpmi squid
- **Gentoo**
emerge squid

¹<http://www.trustonme.net/didactels/295.html>

²<http://www.squid-cache.org>

0.1.4 2. Lancement sécurisé

Dans cette partie j'indique comment lancer Squid par un utilisateur différent de root, par mesure de sécurité. Pour cela, en tant que root, créez les groupe et utilisateur "proxy" s'ils n'existent pas, par :

```
# groupadd proxy
# useradd -g proxy -d /etc/squid -s /bin/bash proxy
# passwd proxy
```

Il ne vous reste plus qu'à attribuer les bonnes permissions aux répertoires :

```
# chown -R proxy.proxy /etc/squid /var/log/squid /var/spool/squid /usr/lib/squid
/usr/sbin/squid
# chmod 665 /var/run
```

0.1.5 3. Configuration

Le fichier de configuration de Squid est /etc/squid/squid.conf . Avant de le modifier faites-en une sauvegarde par :

```
# cp /etc/squid/squid.conf /etc/squid/squid.conf.default
```

Je fournis un exemple de fichier squid.conf, correspondant au réseau suivant :

- Adresses de type : 192.168.0.x
- Adresse du serveur proxy : 192.168.0.1
- Nom du serveur proxy : serveur
- Port d'écoute de Squid : 3128.
- Stations autorisées à utiliser Internet : 192.168.0.50 et de 192.168.0.100 à 192.168.0.125

Le fichier squid.conf :

```
##### /etc/squid/squid.conf #####
# comme Squid est lancé par un utilisateur différent de
  root
# alors http_port ne peut être inférieur à 1024
http_port 192.168.0.1 :3128
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
cache_mem 10 MB
cache_dir ufs /var/spool/squid 100 16 256
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
pid_filename /var/run/squid.pid
# Pour que le proxy soit serveur DNS :
# dns_nameservers dns_fai ou/et dns_passerelle
# redirect_program /usr/bin/squidGuard -c etc/squid/squidGuard.conf
refresh_pattern ftp : 1440 20% 10080
refresh_pattern gopher : 1440 0% 1440
refresh_pattern . 0 20% 4320
```

```
# ACL : les acl permettent de spécifier les autorisations
# d'accès sur certains ports, et pour les ip des stations
# Attention l'ordre donné ici est important !
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl manager proto cache_object
acl serveur src 192.168.0.1
acl poste src 192.168.0.50
acl multipostes src 192.168.0.100-192.168.0.125
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 20 # ftp-data
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # ssl
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 Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT
acl purge method PURGE
acl CONNECT method CONNECT
# On accepte tout ce qui vient du serveur
http_access allow serveur
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
# On rejette tous les ports différents de ceux déclarer
# dans les acl
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
# On accepte les requetes des stations suivantes sur le
# proxy :
http_access allow poste
http_access allow multipostes
# On accepte le local
http_access allow localhost
```

```
# On rejette tout le reste
http_access deny all
http_reply_access allow all
icp_access allow all
# On renseigne l'utilisateur et le groupe qui initialise
  Squid :
cache_effective_user proxy
cache_effective_group proxy
# On renseigner le nom de machine qui fait serveur
visible_hostname serveur
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
#### END /etc/squid/squid.conf ####
```

Maintenant que Squid est configuré, activez le répertoire de swap de Squid par :

```
# /usr/sbin/squid -z
```

Attribuez le répertoire `/var/spool/squid` à l'utilisateur `squid` :

```
chown -R proxy.proxy /var/spool/squid
```

Vous pouvez tester le bon fonctionnement par :

```
/usr/sbin/squid
```

0.1.6 4. Lancement automatique de Squid

Pour que Squid soit lancé au démarrage, je fournis un script à placer dans le répertoire d'initialisation de votre distribution. Il suffit ensuite de faire un lien vers celui-ci dans les différents runlevels. Reportez-vous aux didacticiels sur votre distribution pour savoir comment faire. Ce Script de démarrage ne concerne que ceux qui ont installé Squid depuis les sources, pour les autres, les paquets ont déjà installé tout le nécessaire. Vérifiez simplement que le script est bien exécuté dans les bons runlevels.

```
#!/bin/bash
# script init squid
case $1 in
start)
echo "Starting Squid"
/usr/sbin/squid
sleep 2
;;
stop)
echo "Stopping Squid"
sleep 2
kill `cat /var/run/squid.pid`
```

```
;;
restart)
echo "Restarting Squid"
kill `cat /var/run/squid.pid`
sleep 4
/usr/sbin/squid
;;
status)
if [ -f /var/run/squid.pid ]
then
PID=`cat /var/run/squid.pid`
echo "Squid running - process $PID "
else
echo "Squid not Running"
fi
;;
*)
echo "Usage : squid (start|stop|restart|status) "
;;
esac
# end
```

N'oubliez pas d'attribuer le script d'initialisation de squid à l'utilisateur proxy ! Exemple pour les utilisateur de debian :

```
# chown proxy.proxy /etc/init.d/squid
```