# Proxy HTTP

## Généralités

Un proxy est un **intermédiaire/agent intermédiaire entre un hôte/des hôtes et d'autres ressources**, principalement Internet. Il **recueille les demandes des clients et les transfère sur Internet**.

**Avantages d'un proxy Web**

* Il peut être utilisé pour **accélérer Internet** car un proxy peut créer un cache de sites Web fréquemment utilisés, ce qui facilite et accélère le chargement après ;
* Il peut être utilisé pour **bloquer/autoriser les sites Web au besoin** ;
* Il peut également être utilisé pour **contourner un autre proxy Web**.   
  Par exemple, dans de nombreuses organisations, les sites Web de réseautage social comme **Facebook**, **Twitter**, **Youtube**, ... ne sont pas autorisés.   
  Ainsi, un proxy Web peut être utilisé pour **contourner ces restrictions** et **fournir un accès à des sites Web** restreints.

### squid

squid est un **serveur mandataire** (proxy) et un **mandataire inverse** capable d'utiliser les protocoles **FTP**, **HTTP** et **HTTPS**. Contrairement aux serveurs proxy classiques, un serveur squid gère toutes les requêtes en **un seul processus** **d'entrée/sortie**, non bloquant.

squid **garde les metadonnées** et plus particulièrement les **données les plus fréquemment utilisées en mémoire**.  
 Il **conserve aussi en mémoire les requêtes DNS**, ainsi que les **requêtes ayant échoué**.   
Les requêtes DNS sont non bloquantes.

Les données mémorisées peuvent être rangées en hiérarchies ou en mailles pour utiliser moins de bande passante.

En outre, squid peut accélérer un serveur Web en mettant des **ressources en cache**.   
Le proxy Squid permet à un serveur de **mettre en cache les pages Web fréquemment visitées**.   
Lorsque l'utilisateur demande une page Web ou un fichier, la demande va directement au serveur proxy - un **appareil intermédiaire entre l'appareil de l'utilisateur et Internet**.   
Le serveur proxy **extrait les ressources et les transmet à l'utilisateur**.

## Installation de squid

Pour installer squid …   
**>> sudo apt install squid**

Pour vérifier si le service est démarré …  
**>> sudo squid --version**ou **>> ps aux | grep squid**

## Configuration du proxy

La configuration de squid se fait en éditant le fichier **/etc/squid/squid.conf**.

Pour visualiser le fichier de configuration …  
**>> cat /etc/squid/squid.conf**

Toutefois ce fichier est très verbeux. Il est préférable de l’épurer.  
Les commandes suivantes (pour la modification du fichier squid.conf) se font en tant que root.  
Pour épurer le fichier de configuration …

**>> sudo -i  
>> sudo mv /etc/squid/squid.conf /etc/squid/squid.conf.original   
>> sudo cat /etc/squid/squid.conf.original | sudo egrep -v -e '^[[:blank:]]\*#|^$' | sudo tee --append /etc/squid/squid.conf**ou   
**>> egrep -v -e '^[[:blank:]]\*#|^$' squid.conf**

**>> exit**

## Modification des directives (de base)

Pour éditer le fichier de configuration …   
**>> sudo nano /etc/squid/squid.conf**

### Nom du proxy

squid a besoin de connaître le **nom de l’hôte afin d’afficher ce nom pour les messages d’erreur**.  
On ajoute la directive suivante en début de fichier …  
**visible\_hostname ProxyWebMaisonneuve**

Afin de tenir compte de la modification, il faut **recharger le fichier de configuration** ...  
**>>** **sudo systemctl reload squid.service**

**Remarque** …  
La commande **sudo systemctl restart squid.service** est aussi possible.  
Cette **demande peut toutefois prendre un certain temps**.

### Choix du port

Par défaut, le **serveur proxy sera en écoute sur le port 3128**.  
Pour choisir un autre port, on remplace la directive **http\_port 3128** par le nouveau port …  
**http\_port 3177**

Afin de tenir compte de la modification, il faut recharger le fichier de configuration …  
**>> sudo systemctl relaod squid.service**

### Choix de l'interface

Par défaut le **serveur proxy sera en écoute sur toutes les interfaces**.   
Pour des raisons de sécurité, il faut qu’il soit **en écoute que sur le réseau** local.

Par exemple, si l’interface réseau reliée au réseau local possède l'adresse IP 192.168.1.100 …   
**http\_port 192.168.1.100:3177**

Afin de tenir compte de la modification, il faut recharger le fichier de configuration …  
**>> sudo systemctl reload squid.service**

## Configuration du client

Il faut configurer le client afin qu’il utilise le serveur proxy.

|  |  |
| --- | --- |
| **Client Windows** | |
| Après avoir accédé aux paramètres de configuration de Windows, on recherche le mot-clé … proxy  La rubrique Réseau et internet devrait apparaître  Dans la configuration manuelle du proxy …   * Utiliser un serveur proxy Activé * Adresse Adresse IP du proxy * Port Port du proxy |  |

|  |  |
| --- | --- |
| **Client Linux** | |
| Il n'y a pas de solution unique pour les clients Linux  Chaque programme utilise sa propre façon de se connecter à un serveur proxy | Toutefois, beaucoup de logiciels Linux/Unix qui utilisent le réseau respectent les **variables d'environnement http\_proxy et ftp\_proxy**.  En fonction de la configuration de sa distribution, le **fichier /etc/environment** (s’il existe) sera lue par défaut par les shells de connexion.  On peut ajouter à ce fichier une ligne indiquant … **http\_proxy=192.168.1.100:1011**  Les modifications dans ce fichier ne seront **effectives seulement lors du démarrage** **d’un processus shell** - et seulement dans ce processus shell.  Il faudra **fermer la session actuelle et ouvrir une nouvelle session**.  **Syntaxe générale** … **http\_proxy="http://<Nom utilisateur:<Mot de passe>@<Serveur proxy>:<port>/" https\_proxy="https:// Nom utilisateur:<Mot de passe>@<Serveur proxy>:<port>/" ftp\_proxy="ftp:// Nom utilisateur:<Mot de passe>@<Serveur proxy>:<port>/"**  Il est aussi possible d’ajouter à la **configuration du serveur DHCP pour indiquer squid** **comme passerelle par défaut**. De cette manière, on n’aura pas besoin de configurer les fureteurs (*browser*) individuels pour travailler avec le proxy. |

## Définition des droits d'accès

Les restrictions indiquent **quoi faire lorsque ces conditions sont vérifiées**.   
On autorise ou on interdit **en fonction d'une ACL ou d'un groupe d'ACLs**, le sens de « restriction » est donc à prendre avec un peu de recul, une restriction pouvant être une autorisation.   
**Tout comme les règles d’un pare-feu**, la **première restriction vérifiée est la bonne**, d'où **l'importance** de **l'ordre dans lequel elles sont placées**.

Sans faire une analyse détaillée, il est possible de constater que dans la configuration **par défaut**, **seul localhost peut** **utiliser le proxy** (*Allow* localhost). Si cette condition n'est pas respectée, la **règle suivante étant deny all**, **personne** ne passe. Il nous faut donc faire **intervenir la notion de réseau local**.

Bien entendu, l'idée de faire **plutôt Allow all est une mauvaise idée**. Si le **proxy possède un pied sur Internet** (s'il est installé sur la passerelle), on risque un proxy ouvert, avec tous les usages pervertis que l'on peut en faire.

### Autorisation du réseau local

Par défaut, personne n'est autorisé à se connecter au serveur proxy, sauf l’hôte lui-même.   
Afin de modifier cet état, il faut créer une liste d'autorisations.

Il existe, dans le fichier de configuration par défaut (/etc/squid/squid.conf), un ensemble de réseau prédéfinis …  
**acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)  
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)  
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)  
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines  
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)  
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)  
acl localnet src fc00::/7 # RFC 4193 local private network range  
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines**

Après avoir vérifié si le réseau local fait partie de cette liste, il faut l'autoriser à utiliser le proxy.  
On doit modifier la ligne suivante …  
**http\_access allow localhost**   
pour  
**http\_access allow localnet**

Afin de tenir compte de la modification, il faut recharger le fichier de configuration …  
**>> sudo systemctl reload squid.service**

**Remarque** …  
Il existe également un ensemble de ports déjà défini dans le fichier de configuration principal de squid …  
**acl SSL\_ports port 443 # https  
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**

### Résumé d’une règle ACL.

Pour les ACL (*Access Control List*) suivants …  
**acl localnet src 192.168.1.0/24  
http\_access allow localnet**

**acl localnet src 127.0.0.1/32**

* **acl**  
  Déclaration d’un nouvel ACL ;
* **localnet**  
  Nom de l’ACL ;
* **src**Indication de l’adresse IP locale  
  ou  
  **srcdomain**   
  indication du domaine local  
  ou  
  **dst**  
  Indication de l’adresse IP publique   
  et   
  **dstdomain**  
  Indication du domaine public ;
* **127.0.0.1/32**  
  Déclaration de l'adresse IP sur laquelle l'acl doit être appliqué.

**http\_access allow localnet**

* **http\_access**Lancement d’une action basée sur le mot suivant ;
* **allow|deny**Autorisation ou refus de l'accès ;
* **localnet**  
  Nom de l’ACL comme déclaré ci-dessus.

|  |  |
| --- | --- |
| **Blocage de sites Web** | |
| Mise en place  d’une ACL simple | La **mise en place d’une ACl se fait toujours en deux étapes** …   * Création de l’ACL ; * Activation de l’ACL.   Pour ce faire on doit modifier le fichier **/etc/squid/squid.conf**.  **ACL pour interdire Facebook**  **Création de l’ACL** Il s’agit de la définition de l’ACL … **acl facebook dstdomain .facebook.com**  **Activation de l’ACL** Il faut par la suite indiquer à qui cette restriction s'impose … **http\_access deny localnet facebook**  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service**  **Remarques** … Il est aussi possible de formuler l’ACL de la manière suivante … **acl blacksite .facebook.com**  Le **point (.facebook) spécifie de bloquer tous les sous-sites** du site principal. |
| Mise en place  d’une ACL multiple | **ACL pour interdire Facebook et Twitter**  Ajout d’un fichier texte **/etc/squid/blocked.acl** … **>> sudo nano /etc/squid/blocked.acl** Le contenu du fichier est … **.facebook.com .twitter.com .youtube.com**  On ajoute les lignes suivantes juste au-dessus de la liste d’ACL … **acl blocked\_websites dstdomain “/etc/squid/blocked.acl” http\_access deny blocked\_websites**  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service** |

Afin de **vérifier la syntaxe du fichier de configuration** /etc/squid/squid.conf, on peut exécuter …  
**>>**

## Journalisation des accès

Il est possible de vérifier les journaux du serveur, pour voir si une demande a été reçue par un serveur proxy ou non …  
**>> sudo tail -f /var/log/squid/access.log**

On devrait y retrouver toutes les demandes reçues du client au serveur …  
**…  
1616876765.780 1200366 192.168.1.104 TCP\_TUNNEL/200 472883 CONNECT www.cmaisonneuve.qc.ca:443 - HIER\_DIRECT/151.101.126.133 -  
…**

## Commandes du service Squid

Pour **vérifier l'état** de squid …  
**>> sudo systemctl status squid**La réponse de la commande indique si le service est en cours d'exécution ou non.

Pour **démarrer le service** …  
**>> sudo systemctl start squid**

Pour **redémarrer le service** …  
**>> sudo systemctl restart squid**

Pour **recharger le fichier de configuration du service** …  
**>> sudo systemctl relaod squid**Cette commande est plus rapide que de redémarrer squid.

Pour configurer le service **squid pour qu'il se lance lorsque le système démarre** …  
**>> sudo systemctl enable squid**

Pour **arrêter le service** …  
**>> sudo systemctl stop squid**

Pour **empêcher squid de se lancer au démarrage** …  
**>> sudo systemctl disable squid**

|  |  |
| --- | --- |
| **Authentification des utilisateurs** | |
| Introduction | Il existe différents types d'authentification des utilisateurs avec squid.  La plus simple est la méthode d'authentification utilise des fichiers de type **.htpasswd** dans lesquels les mots de passe ne sont pas en clair mais condensés (hash) dans un fichier séparé.  Pour mettre en place une authentification, il est nécessaire que le proxy ne soit pas transparent (une demande d'authentification alors que le serveur est censé être invisible est un peu contre-productive).  Il faut utiliser un module appelé 'ncsa\_auth' pour l'authentification squid.  Ce dernier se trouve dans le répertoire /usr/lib/squid/ncsa\_auth (pour les systèmes 32 bits) et /usr/lib64/squid (pour les systèmes 64 bits). |
| Fichier des utilisateurs | Il faut, dans un premier temps, créer un fichier dans lequel les utilisateurs et leurs mots de passe (hashés) se retrouveront …  **>> sudo touch /etc/squid/utilisateurs.bd  >> sudo chmod 777 /etc/squid/utilisateurs.bd**  **>> sudo htpasswd -c /etc/squid/utilisateurs.bd <utilisateur> >> htpasswd -c /etc/squid/utilisateurs.bd tux**  La **commande demande alors un mot de passe** (et une confirmation) pour cet utilisateur.  **Remarque** … Si la commande htpasswd n'est pas disponible, il faut installer le paquet **apache2-utils**.  Afin de vérifier le bon fonctionnement de la commande, on peut **consulter le fichier /etc/squid/utilisateurs.bd** … **>> cat /etc/squid/utilisateurs.bd tux:$apr1$PcDKJNPA$9Z.BsczHlOpLzD5HjPSHb.**  Les **mots de passe sont sous format de condensés**. |
| Tester de la base de données de mots de passe | Pour vérifier la validité <Nom utilisateur> <Mot de passe> …  **>> /usr/lib/squid3/basic\_ncsa\_auth /etc/squid/passwords**  Après avoir entré la commande, la console propose une invite sans aucun texte. On entre alors <Nom utilisateur> <Mot de passe> et on confirmeavec Retour. Le système devrait répondre par OK. |
| Modification du fichier /etc/squid/squid.conf | Par la suite, il faut apporter des modifications dans le fichier de configuration principal de squid … **auth\_param basic program /usr/lib64/squid/ncsa\_auth /etc/squid/utilisateurs.db auth\_param basic Squid Basic Authentication auth\_param basic credentialsttl 5 hours auth\_param basic children 5 acl password proxy\_auth REQUIRED**  **/etc/squid/utilisateurs.db** est le fichier contenant les informations utilisateur.  La directive auth\_param basic credentialsttl 5 hours indique que <Nom utilisateur> <Mot de passe> sera à nouveau demandé. La directive auth\_param basic children 5 est le nombre de processus d'aide à l'authentification de base utilisés par Squid.  Ensuite, il faut **créer une ACL nommé auth\_users pour l'authentification** … **acl auth\_users proxy\_auth REQUIRED**  Il faut enfin activer l'ACL … **http\_access allow auth\_users http\_access deny all**  **Remarque** … Ces ajouts (nouvelles ACLs) **doivent être saisis au-dessus de tous les autres ACL**, sinon elles pourraient ne pas fonctionner.  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service** |
| Autre exemple | Il est aussi possible d’ajouter des directives proxy\_auth à la configuration de squid en **indiquant les noms d'utilisateurs**. Dans cet exemple, les utilisateurs nommés **tux**, **squidly**, **kermit** et **grangallop** sont autorisés d'utiliser le proxy à tout moment.  Les autres utilisateurs ne peuvent le faire que pendant la journée.  **acl identification proxy\_auth REQUIRED acl utilisateurs proxy\_auth tux squidly kermit grangallo acl daytime time 08:00-17:00 http\_access allow identification daytime http\_access allow utilisateurs http\_access deny all** |

|  |  |
| --- | --- |
| **Autres directives** | |
| Limitation du nombre de connexions Web simultanées | On peut utiliser l’**ACL** **appelée** **maxconn**.  Elle permet de **limiter le nombre maximum** **de connexions à partir d'une seule adresse IP client**.  Dans le fichier /etc/squid/squid.conf, on ajoute une ACL … **acl allowedIPs 192.168.1.0/24 acl limitusercon maxconn 3 http\_access deny allowedIPs limitusercon**  Les directives sont …   * **acl allowedIPs 192.168.1.0/24** Étendues d'adresses IP ; * **acl limitusercon maxconn 3**  Définition de 3 accès Web simultanés à partir de la même adresse IP client ; * **http\_access deny allowedIPs limitusercon** Activation de l’ACL.   Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service** |
| Définition d’une période d’utilisation | On peut, pour certaines occasions, avoir bes**oin d'accéder à un site Web bloqué ou encore avoir besoin de bloquer certains sites Web** pendant un **certain temps**.  Pour définir un temps d'utilisation en créant une **acl jour** *…* **acl jour time 08:00-17:30**  Il faut par la suite indiquer à qui cette restriction s'impose … **http\_access allow localnet jour**  La période de temps (une journée) est définie de 8h00 à 17h30.  En dehors de cette étendue, le proxy refusera la connexion.  Il est aussi possible de **spécifier des jours de la semaine** … **acl jour time MTW 10:30-11:30** Cette directive défini l’ACL jour comme étant les **lundis**, **mardis** et **mercredis** **entre** **10h30 et 11h30**.  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service**  **Autres exemples**  **acl horaires\_travail time M-F 08:00-17:00 acl horaires\_travail time MTWHF 08:00-17:00 acl Exception1 time W 11:30-11:50**  M-F correspond à Monday-Friday (de lundi à vendredi) |

|  |  |
| --- | --- |
| Activation du cache pour accélérer la navigation | En activant le cache sur le serveur, il est possible d’accélérer la vitesse de navigation pour les pages fréquemment visitées. En ajoutant une seule ligne dans le fichier de configuration, on peut activer le cache.  Pour activer le cache, on ajoute la directive suivante … cache\_dir ufs /var/cache/squid 2000 16 256 où …   * ufs  est le format de stockage squid ; * /var/cache/squid  est le chemin du fichier de stockage du cache ; * 2000  est la taille en Mo peut être utilisée pour le cache ; * 16 est le nombre de sous-répertoires de premier niveau  et  256 est le nombre de sous sous-répertoires de second niveau.   Message(s) d’erreur … Il est possible que squid retourne un ou des messages d’erreur indiquant un problème d’accès à des répertoires. il suffit de modifier les permissions d’accès … >> sudo chown -R proxy:proxy <répertoire> >> sudo chmod -R 775 <répertoire>  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … >> sudo systemctl reload squid.service |
| Exclusion de l'adresse IP dans les requêtes HTTP | Il est possible de **ne pas inclure l'adresse IP** ou le **nom du système dans les requêtes** **HTTP**. il faut modifier la directive forwarded\_for … **forwarded\_for off**  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service** |
| Messages d'erreur en français | Afin que squid **retourne ses messages d’erreurs en français** … **error\_directory /usr/share/squid/errors/French**  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … **>> sudo systemctl reload squid.service** |

|  |  |
| --- | --- |
| Blocage des fichiers musicaux | Il est possible de déclarer des ACL afin de bloquer différents types d’extensions et ainsi alléger le cache et la rapidité de navigation ou tout simplement pour restreindre les utilisateurs.  Pour se faire, on ajoute les directives suivantes … # Bloquer les fichiers AVI : acl extension\_avi url\_regex -i \.avi$ http\_access deny extension\_avi  Lorsque l’on met cette option dans une ACL, cela permet de rechercher une chaîne de caractères contenu dans l'URL. Il est important de noter que l’url\_regex est sensible à la casse (majuscules/minuscules).  On peut ajouter une directive afin de bloquer le téléchargement ou l’écoute de fichiers musicaux. La technique est la même pour d’autres fichiers tels que les exécutables.  Il faut créer, dans un premier temps, un nouveau fichier nommé fichier /etc/squid/blocks.files.acl. Son contenu ressemble à ceci … \.exe(\?.\*)?$ \.avi(\?.\*)?$ \.bat(\?.\*)?$ \.tar(\?.\*)?$ \.mpg(\?.\*)?$ \.mp3(\?.\*)?$ \.mp4(\?.\*)?$  Il faut par la suite ajouter les directives suivantes … acl blockfiles urlpath\_regex -i "/etc/squid/blocks.files.acl"  Il est possible d‘afficher un message d'erreur personnalisé lorsqu'un fichier est bloqué. Pour ce faire, on doit créer un fichier HTML de message d'erreur personnalisé nommé ERR\_BLOCKED\_FILES dans le répertoire /etc/squid/error/ ou /usr/share/squid/errors/French.  # Bloquer les extensions de fichiers musicaux all blocked extension error\_directory /usr/share/squid/errors/French deny\_info ERR\_BLOCKED\_FILES blockfiles  Enfin, on active la directive … http\_access deny blockfiles  Afin de tenir compte de la modification, il faut recharger le fichier de configuration … >> sudo systemctl reload squid.service |

|  |  |
| --- | --- |
| Exemple de fichier HTML | <HTML>  <HEAD>  <TITLE> ERREUR: contenu de fichier bloqué </TITLE> </HEAD> <CORPS> <H1> Le fichier est bloqué en raison d'une nouvelle politique de sécurité </H1> <p> Veuillez contacter le service d'assistance pour plus d'informations: </p> <ul>  <li> Téléphone: 555-1243 (poste 5678) </li>  <li> E-mail: aide@tux.info </li> </BODY> </HTML> |
| Blocage des torrents | Le **filtrage des torrents est un problème difficile** qui ne peut pas être résolu facilement.  On peut d'abord **refuser le téléchargement de fichiers .torrent**.  **# Bloquer les fichiers torrent acl TorrentFiles rep\_mime\_type -i application de type mime / x-bittorrent http\_reply\_access deny TorrentFiles deny\_info TCP\_RESET TorrentFiles**  Cela empêche le téléchargement de fichiers .torrent par les utilisateurs à l’aide des fureteurs.  Il est aussi possible de **limiter le nombre maximal de connexions simultanées**. **Bittorrent** connecte des **centaines de connexions pour une meilleure vitesse**, donc limiter le nombre maximum de connexions peut **limiter sa vitesse de téléchargement**.  **acl allowedIPs 192.168.1.0/24 acl limitusercon maxconn 3 http\_access deny allowedIPs limitusercon** |

# Annexe 01 Gestion de squid avec Webmin

## Installation de webmin

Dans un premier temps, il faut installer l’utilitaire Webmin.

Pour se faire, on ajoute, dans un premier temps, le référentiel de webmin …  
**>> sudo nano /etc/apt/sources-list  
deb https://download.webmin.com/download/repository sarge contrib**

On lance, par la suite, la commande d’installation suivante …  
**>> sudo apt update && sudo apt upgrade -y && sudo apt install webmin -y**

## Procédure d’installation de squid (à l’aide de webmin)

Pour commencer la procédure d'installation, on accède a webmin à l’aide d’un fureteur (*browser*) à l’adresse **https://<Adresse IP>:10000**.   
La page de connexion de webmin devrait apparaître.

Le nom d’usager, par défaut, est … **root**.  
Le mot de passe est celui de root sur le système.

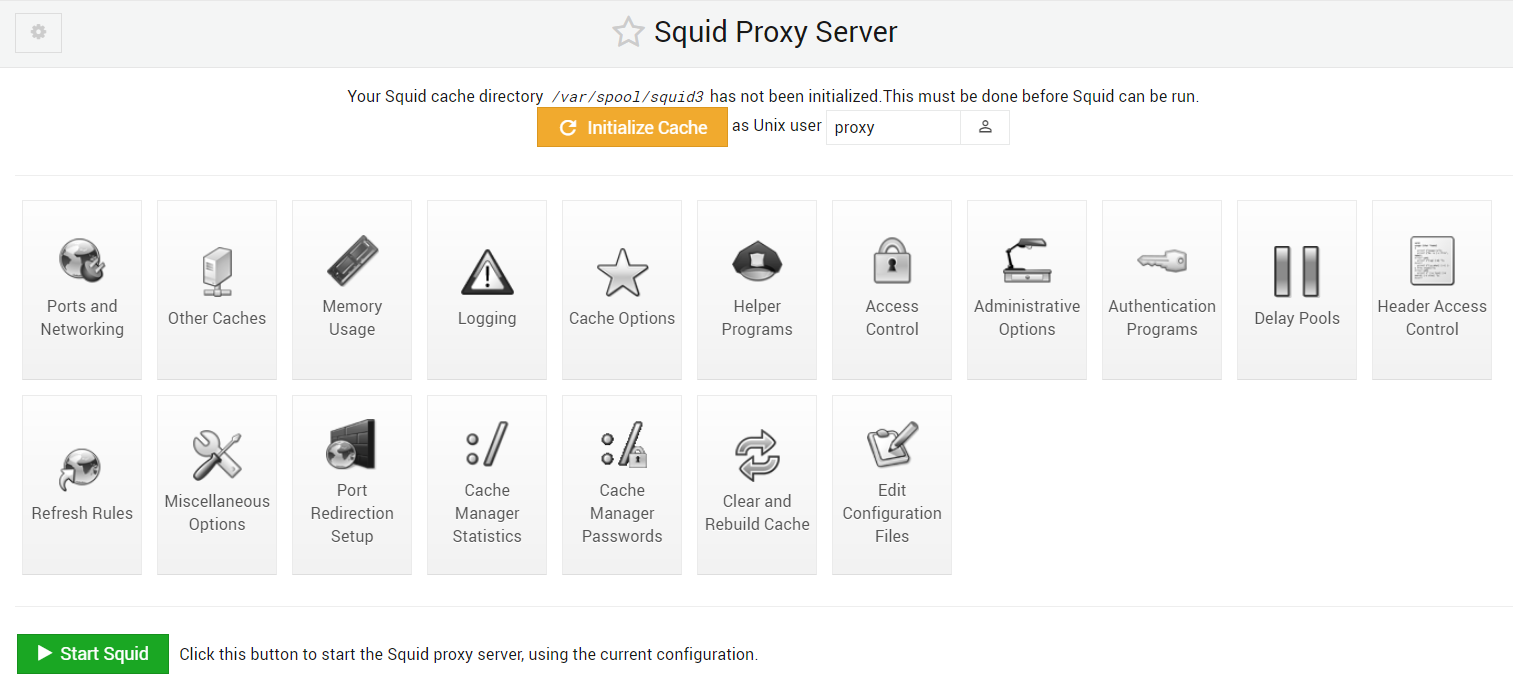
Dans le tableau de bord, le volet de gauche contient une liste de modules déjà installés.  
On sélectionne la rubrique **Modules non utilisés** (**Un-used modules**) et on sélectionne celui de **Squid Proxy Server**.

Un message d’erreur peut apparaître …  
**The Squid config file** **/etc/squid3/squid.conf does not exist. If you have Squid installed, adjust your module configuration to use the correct paths.**

On clique alors sur le lien **module configuration** afin d’accéder à ce module.

Il suffit à cette étape de modifier le chemin du fichier de configuration de squid.  
On remplace …  
**/etc/squid3/squid.conf**par  
**/etc/squid/squid.conf**

Il faut sauvegarder la modification avant de passer au module de gestion de squid …



# Annexe 02 Installation de squid Exemple de script

Ce script bash permet d’installer facilement un proxy squid avec authentification par **<nom utilisateur>/<mot de passe>** sur un serveur debian Linux en une ligne de commande.

Pour l’utiliser rien de plus facile : il faut un serveur debian, puis télécharger le fichier et l’exécuter …  
**>> sudo wget --no-check-certificate https://www.christophe-casalegno.com/tools/squid.sh  
>> sudo chmod +x squid.sh  
>> sudo ./squid.sh**

**Lien Web** …  
https://www.christophe-casalegno.com/installation-dun-proxy-squid-avec-authentification-sur-linux-debian/

# Références

**Site officiel squid**<http://www.squid-cache.org/>

**Livre numérique**<https://www.editions-eni.fr/open/mediabook.aspx?idR=b1c34624b2b9ba1b1454580aa99289ca>

**Page de démarrage pour un portail captif**<https://wiki.squid-cache.org/ConfigExamples/Portal/Splash>