

## Référentiel

B2.2 - Installer, tester et déployer une solution d'infrastructure réseau.

Installer et configurer des éléments nécessaires pour assurer la qualité de service.



## Définition

(Source : <https://fr.wikipedia.org/wiki/Proxy/>)

Un proxy (ou serveur mandataire) est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement Internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.

Les serveurs mandataires sont notamment utilisés pour assurer les fonctions suivantes :

- accélération de la navigation : mémoire cache, compression de données ;
- historique (logs) : journalisation des requêtes ;
- la sécurité du réseau local ;
- le filtrage : restrictions de sites, blocage des publicités ou des contenus lourds (Java, Flash) ;
- l'anonymat ;
- la répartition de charge ;

## Le service SQUID

### Avant propos

Le paquet à installer est **squid** via la commande **apt install squid**

Le fichier de configuration est **/etc/squid/squid.conf**

Réalisez une sauvegarde de ce fichier (**cp /etc/squid/squid.conf /etc/squid/squid.conf.svg**)

Ce fichier est essentiellement composé d'**acl** (access control list) et de directives **http\_access** (allow ou deny).

*Exemple : Autoriser le réseau 172.16.0.0/16 à accéder à Internet*

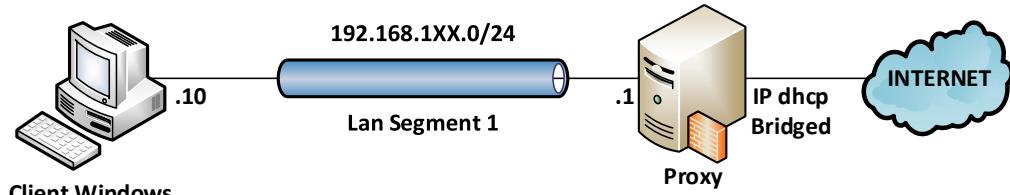
```
acl Lan172 src 172.16.0.0/16
...
http_access allow Lan172
http_access deny all
```

Pour relancer squid : **service squid restart** (ou **systemctl restart squid.service**)

Pour visualiser les erreurs de configuration : **squid** (ou **squid /etc/squid/squid.conf**)

Pour visualiser le fichier de log de squid : **tail -f /var/log/squid/access.log**

### Schéma réseau



### Contrainte supplémentaire :

Sur le poste client, il ne faudra pas définir de passerelle par défaut.

Configurez le navigateur du poste client afin qu'il utilise votre proxy.

Le port de squid sera **3128**.

### Exercice 1 – Recherche sur les principales variables de configuration du proxy

**http\_port** `http_port` : Cette variable définit le port sur lequel Squid écoutera les requêtes HTTP. Par exemple, si vous avez `http_port 3128`, cela signifie que Squid écoutera sur le port 3128.

**cache\_mem** Cette variable spécifie la quantité de mémoire vive (RAM) que Squid devrait utiliser pour stocker en cache des objets. Par exemple, `cache_mem 256 MB` allouera 256 mégaoctets de mémoire vive au cache de Squid.

**cache\_dir** Cette variable spécifie le répertoire où les objets mis en cache seront stockés sur le disque. Elle est définie avec plusieurs paramètres, notamment la taille, le type et le chemin du répertoire. Par exemple, `cache_dir ufs /var/spool/squid 100 16 256` signifie que Squid utilisera le système de fichiers UFS pour stocker le cache dans le répertoire `/var/spool/squid`, avec une limite de 100 mégaoctets et 16 niveaux de sous-répertoires.

**cache\_access\_log** Cette variable spécifie le chemin du fichier journal d'accès, où Squid enregistre les détails des requêtes HTTP traitées. Par exemple, `cache_access_log /var/log/squid/access.log` indique que les informations d'accès seront enregistrées dans le fichier `/var/log/squid/access.log`.

**cache\_log** Cette variable spécifie le chemin du fichier journal système où Squid enregistre les informations générales sur son fonctionnement. Par exemple, `cache_log /var/log/squid/cache.log` indique que les informations du cache seront enregistrées dans le fichier `/var/log/squid/cache.log`.

### Exercice 2 – Configuration de squid

Voici la liste des règles à mettre en place :

1. Autorisez votre réseau à accéder à Internet
2. Autorisez une seule machine de votre réseau à accéder à Internet.
3. Affectez une plage horaire d'accès à Internet à votre réseau (par exemple de 8h00 à 18h00).
4. Interdisez les sites contenant le mot **jeu** dans leur url.
5. Interdisez l'accès au domaine **facebook.com**.
6. Interdisez l'accès à une liste de domaines (**facebook.com, lequipe.fr et lemonde.fr**).

Pour tester votre configuration, il vous faudra ajouter les lignes suivantes :

```
cache_peer 192.168.1.21 parent 3128 0 no-query default login=VotreLogin:VotreMotDePasse
never_direct allow all
```

### Exercice 3 – L'authentification sur squid

Il existe des modules pour squid qui permettent d'utiliser les types d'authentification les plus courants :

- **ldap\_auth** : pour s'authentifier via un annuaire LDAP
- **smb\_auth** : pour une authentification de type contrôleur de domaine Windows
- **ncsa\_auth** : pour une authentification simple depuis un fichier d'utilisateurs

Nous mettrons en place le dernier module afin de donner une première approche des possibilités.

Installez le paquet **apache2-utils** afin de pouvoir utiliser la commande **htpasswd**.

Ceci étant fait, effectuez dans cet ordre :

- créer un nouveau fichier par la commande :  
`touch /etc/squid/squid_users`
- créez 3 utilisateurs différents par la commande :  
`htpasswd -b /etc/squid/squid_users riri neveu1`  
`htpasswd -b /etc/squid/squid_users fifi neveu2`  
`htpasswd -b /etc/squid/squid_users loulou neveu3`

Observez le résultat obtenu dans le fichier **squid\_users**. Que s'est-il passé ?

Modifiez ensuite le fichier de configuration de squid afin de rendre possible l'authentification. Pour vous aider, identifiez les éléments dont vous avez besoin dans le fichier de configuration fourni sur le site suivant :

<https://caleca.developpez.com/tutoriels/squid-squidguard/#LIV>

## Exercice 4 – L’authentification LDAP sur squid

En lieu et place de l’authentification simple, utilisez l’authentification via un annuaire LDAP. Vous pouvez vous inspirer du site suivant :

<https://workaround.org/squid-ldap/>

## Exercice 5 – Lecture d’un fichier de configuration

Soit le fichier de configuration `/etc/squid/squid.conf` :

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/squid_users
auth_param basic children 5
auth_param basic realm squid proxy-caching web server
auth_param basic credentialsttl 2 hours
acl lan src 192.168.1.0/24
acl poste src 192.168.1.11
acl mot_url url_regex jeu
acl domaines_1 dstdomain .facebook.com
acl domaines_2 dstdomain .infoSIO.fr
acl horaires time MTWHF 08:00-17:00
acl utilisateurs proxy_auth REQUIRED
http_access allow domaines_2
http_access deny domaines_1
http_access allow poste
http_access deny mot_url
http_access allow lan horaires utilisateurs
http_access deny all
```

Que contient le fichier `/etc/squid/squid_users` ? \_\_\_\_\_

Un utilisateur ouvrant un navigateur sur le poste 192.168.1.10, peut-il :

- Accéder au site [www.facebook.com](http://www.facebook.com) le lundi à 8h10?  Oui  Non
- Accéder au site [www.jeu.fr](http://www.jeu.fr) le mardi à 13h ?  Oui  Non
- Accéder au site [www.google.fr](http://www.google.fr) le samedi à 22h ?  Oui  Non

Devra-t-il s’authentifier pour accéder au site [www.microsoft.com](http://www.microsoft.com) ? \_\_\_\_\_

Même question depuis le poste 192.168.1.11 :

- Accéder au site [www.facebook.com](http://www.facebook.com) le lundi à 8h10?  Oui  Non
- Accéder au site [www.jeu.fr](http://www.jeu.fr) le mardi à 13h ?  Oui  Non
- Accéder au site [www.google.fr](http://www.google.fr) le samedi à 22h ?  Oui  Non

Devra-t-il s’authentifier pour accéder au site [www.microsoft.com](http://www.microsoft.com) ? \_\_\_\_\_