TP Mise en oeuvre du proxy Squid sous Linux Debian

Plan de l'atelier

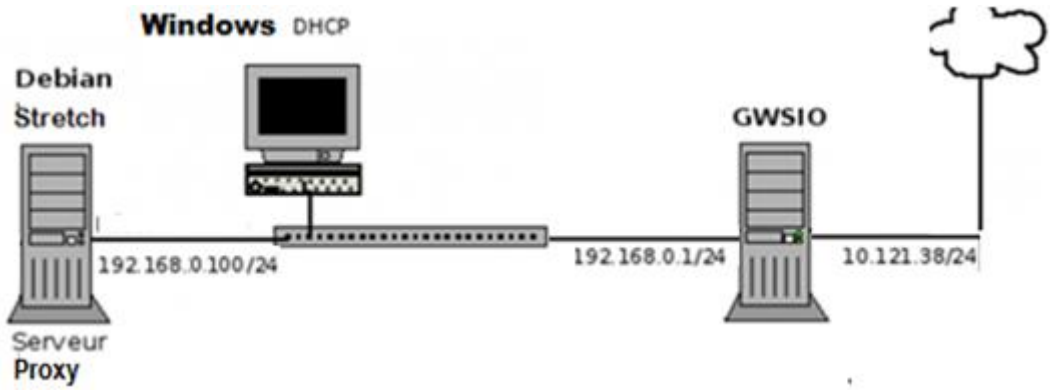
1. Installer squid (squid3) sur une Debian Stretch
2. Mettre en place une configuration de base (écoute sur le port 8080, accès limité au réseau local)
3. Tester avec un client web et examiner les logs (cache.log,access.log)
4. Mettre en place le filtrage pour interdire des mots clés (tf1, ,,,)
5. Autoriser les mots-clé pour une adresse donnée
6. Mettre en place une authentification (ncsa, msnt, ntml)
7. Mettre en place le proxy transparent

Préliminaires

Remarque : adapter au réseau 192.168.0.0/24 la répartition du **dernier octet** entre les membres d'un même plot. Plages : 100-109, 110-119, 120-129 par ex. pour 3 utilisateurs (10 adresses chacun).

- le réseau est en **192.168.0.0/24**
- le serveur *Debian 9* **srvproxy** (adresse fixe: 192.168.0.**100** dans etc/network/interfaces)
- le client *Windows Xp* **pcwin** en client dhcp

Schéma



Créer ce réseau avec la configuration des interfaces et le nommage des postes (reboot ensuite) :

```
root@stretch64:~# sed -i 's/stretch64/srvproxy/g' /etc/host{s,name}
```

1. Installer squid (squid3)

- Paquetage à installer et lancement du service

  apt-get install squid3
  /etc/init.d/squid start

- Configurer le navigateur du poste **pcwin** et vérifier l'impossibilité d'atteindre internet via **srvproxy**.

2. Mettre en place une configuration de base (écoute sur le port 8080, accès limité au réseau local)

Les fichiers de configuration sont situés dans */etc/squid*

Modifier le fichier /etc/squid/squid.conf (faire une sauvegarde de la version initiale en squid.conf.anc par exemple)

```
http_port 8080                      # on écoute sur le port 8080
acl  localnet src 192.168.0.0/24    # à ajouter à la fin de la partie de déclaration des ACL
http_access allow localnet          # à insérer avant la règle finale http_access deny all
```

Remarque : avec vim, rechercher une chaine : /chaine le suivant avec n

3. Tester avec le client web et examiner les logs

Relancer le service et retester avec le client **pcwin**.
Visualiser les journaux :

tail -f /var/log/squid/cache.log
tail -f /var/log/squid/access.log

4. Mettre en place le filtrage pour interdire des mots clés (tf1, „„)

Interdire le mot tf1 dans l'url.
Interdire le site lemonde.fr

Modifier le fichier de configuration et relancer le service. Tester.

5. Autoriser les mots-clé pour une adresse ip donnée

Autoriser l'accès à tf1.fr uniquement à la machine d'adresse ip : 192.168.0.105

Modifier le fichier de configuration et relancer le service. Tester.

6. Mettre en place une authentification (ncsa, msnt, ntml)

- Télécharger le paquet htpasswd pour générer un nom avec un mot de passe.

aptitude install apache2-utils

- Création du fichier des mots de passe

htpasswd -c /etc/squid/users etudiant (saisie d'un mdp)

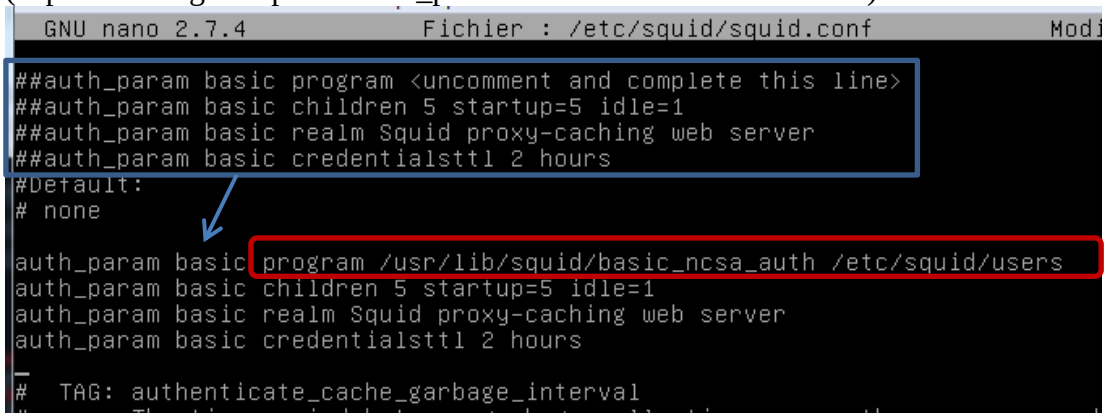
Vérification : *more /etc/squid/users*

- Modifier le fichier /etc/squid/squid.conf

Retrouver l'emplacement du programme de contrôle d'accès pour le mettre dans squid.conf :
*find / -name "*ncsa*"*

Rajouter les lignes suivantes dans squid.conf :

(copier les 4 lignes option «auth_param basic» en modifiant la 1ère)



Déclarer une acl : *acl mdp proxy_auth REQUIRED*

Et rajouter une ligne : *http_access …*

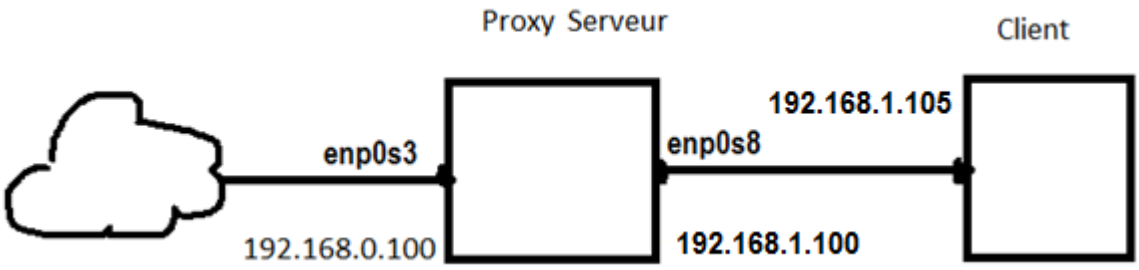
Relancer le service et tester.

7. Mettre en place le proxy transparent

Le proxy transparent évite aux clients de configurer spécifiquement leur navigateur. Le principe est le suivant : on redirige les requêtes arrivant sur le port 80 du proxy pour les transférer sur le port d'écoute du proxy (par exemple 3128 ou 8080) et forcer le passage à travers le proxy. La redirection des ports se fait avec iptables/netfilter.

Le proxy transparent présente donc aussi l'intérêt de forcer le client à utiliser le proxy : on peut donc mettre en place des règles de filtrage et d'autre part les clients laissent obligatoirement des traces dans les logs.

Remarque : le proxy transparent fait mauvais ménage avec les systèmes d'authentification : on devra choisir l'un ou l'autre.

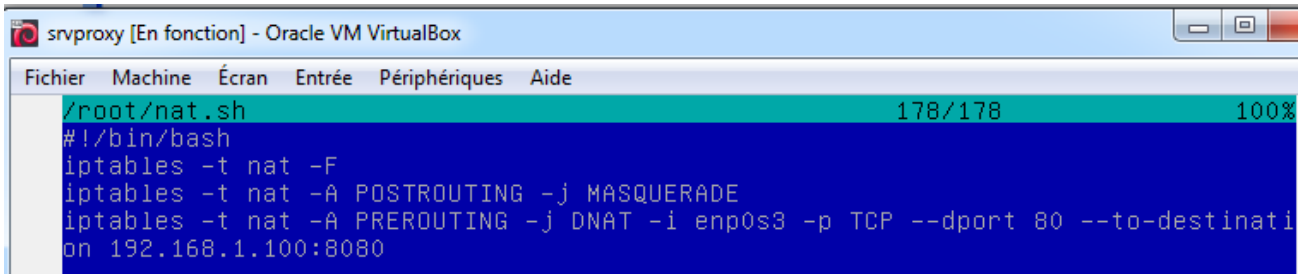


- Mettre en place la configuration ci-dessus (paramétrage des interfaces)
- Activer le routage :

```
root@srvproxy:~# echo "1" > /proc/sys/net/ipv4/ip_forward
```

  Tester
- Modifier le fichier */etc/squid/squid.conf* pour désactiver l'authentification.
- Adapter les adresses dans le fichier de configuration (localnet, poste105)
- Relancer le service. Tester sur le client.
- Modifier le port dans */etc/squid/squid.conf* : *http_port 8080 transparent*
- Relancer le service
- Mettre en place les règles iptables :

  ✓ Création du fichier /root/nat.sh :



  ✓ Le rendre exécutable :
  chmod +x /root/nat.sh
  ✓ Lancer **nat.sh** avec : ./nat.sh

- Tester sur le client en reparamettrant son navigateur, option : Pas de proxy
  Indiquer comme serveur dns : 192.168.0.1

  Examiner les logs (cache.log, access.log)