

Installation d'un serveur proxy

Dans le cadre de la mise aux normes de nos infrastructures il est demandé a l'équipe DSI de mettre en place un serveur proxy web pour l'ensemble de l'entreprise.

Auteur

Roblot Jean-Philippe - jroblot.simplon@proton.me

Version

21/02/2024 - V1R0

Releases

Ubuntu server LTS22.04 Squid 5.7

Powered by <https://shields.io>

Contexte

En tant que administrateur Système, il vous est demander de vous documenter et de mettre en place un proxy web sur l'infrastructure de votre entreprise afin de respecter la législation.

Afin de réaliser cela il vous est indiqué le souhait d'utiliser des technologies Opensource.En tant que administrateur Système, installation d'un proxy web dans l'infrastructure.

Matériel

Réseau Privé Hôte @ip 192.168.56.0/24

Machine serveur

- Ubuntu Server LTS 22.04
- vCPU : 1 core
- vRAM 4Go
- vHDD : 25Go
- NIC 1 : @ip 192.168.1.203/24 par pont
- NIC 2 : @ip 2 : 192.168.1.202/24 en réseau interne

Machine client

- Laptop Ubuntu Desktop LTS 22.04
- CPU : 1 core
- RAM 4Go
- SSD : 25Go
- @ip 192.168.1.204

Questions

1. Qu'est-ce que Squid et quel est son rôle dans une infrastructure réseau ?

C'est un proxy web qui permet de filtrer le trafic réseau et de garder en cache les pages web visitées afin de rendre la navigation plus rapide.

Il stocke également les logs du trafic réseau.

2. Quels sont les avantages de l'utilisation de Squid en tant que serveur proxy cache ?

Rendre la navigation plus rapide pour les pages déjà visitées.

3. Comment installer et configurer Squid sur un système Linux ?

```
sudo apt install squid  
sudo nano /etc/squid/squid.conf
```

4. Quelles sont les différentes méthodes de configuration de Squid pour le filtrage du contenu web ?

- Filtrage par domaine: Vous pouvez bloquer l'accès à certains noms de domaine en utilisant les ACL (Access Control Lists) dans le fichier de configuration de Squid.
- Filtrage par extension de fichier: Squid permet également de bloquer certaines extensions de fichiers.
- Authentification des utilisateurs: Vous pouvez demander aux utilisateurs de s'authentifier pour pouvoir accéder au proxy.
- Utilisation de SquidGuard: SquidGuard est un plugin pour Squid qui permet d'effectuer du filtrage de sites Web basé sur des catégories, via une blacklist. Il permet également de mettre en place des règles en fonction de plages horaires, de groupes d'utilisateurs, etc.

5. Comment configurer Squid pour fonctionner en mode transparent ?

6. Quels sont les mécanismes de contrôle d'accès disponibles dans Squid et comment les configurer ?

Il y a deux choses principales à paramétrer :

- Les ACL (Access Control List) qui sont des critères de contrôle d'accès qui seront ensuite utilisés par la directive `http_access`
- Les `HTTP_ACCESS`, suivies de `allow` ou `deny` pour autoriser ou interdire l'accès au proxy-cache

7. Quels sont les outils de surveillance et de gestion disponibles pour superviser les performances de Squid ?

- ManageEngine OpManager: C'est un outil proactif de surveillance des serveurs qui aide les organisations à surveiller et à gérer leurs serveurs de manière transparente. Il fournit un tableau de bord unique pour chaque serveur et permet aux administrateurs informatiques d'afficher l'utilisation du processeur, de la mémoire et du disque pour chaque occurrence de machine virtuelle invitée sur le serveur.
- Site24x7: Il offre une planification de la maintenance et des rapports personnalisables.
- Moniteur de serveur et d'application: Il offre une interface Web intégrée unique et une cartographie intelligente des dépendances infra des applications.
- Meilleure pile: Il offre une interface intégrée unique, des tableaux de bord, livetail et des alertes exploitables illimitées

8. Comment gérer les journaux d'accès et les journaux d'erreurs de Squid et comment interpréter les informations qu'ils contiennent ?

- Journaux d'accès : Ces journaux enregistrent toutes les requêtes traitées par Squid. Chaque ligne du journal d'accès correspond à une requête unique et contient des informations telles que l'heure de la requête, la durée de la transaction, l'adresse IP du client, le code d'état HTTP, la taille de la réponse, le type de requête (GET, POST, etc.), l'URL demandée, et plus encore.
- Journaux d'erreurs : Ces journaux enregistrent les messages d'erreur générés par Squid. Ils sont utiles pour le dépannage et contiennent des informations sur les problèmes rencontrés par Squid lors de l'exécution.
- Pour afficher les dernières entrées dans le journal d'accès :

```
tail /var/log/squid/access.log
```

- Pour afficher les dernières entrées dans le journal d'erreurs :

```
tail /var/log/squid/cache.log
```

- Pour vider un journal :

```
> /var/log/squid/access.log
```

Activités

1. Installation d'un serveur Linux, Ubuntu Server LTS 22.04 et Squid

```
sudo apt update && sudo apt upgrade
```

```
sudo apt install squid
```

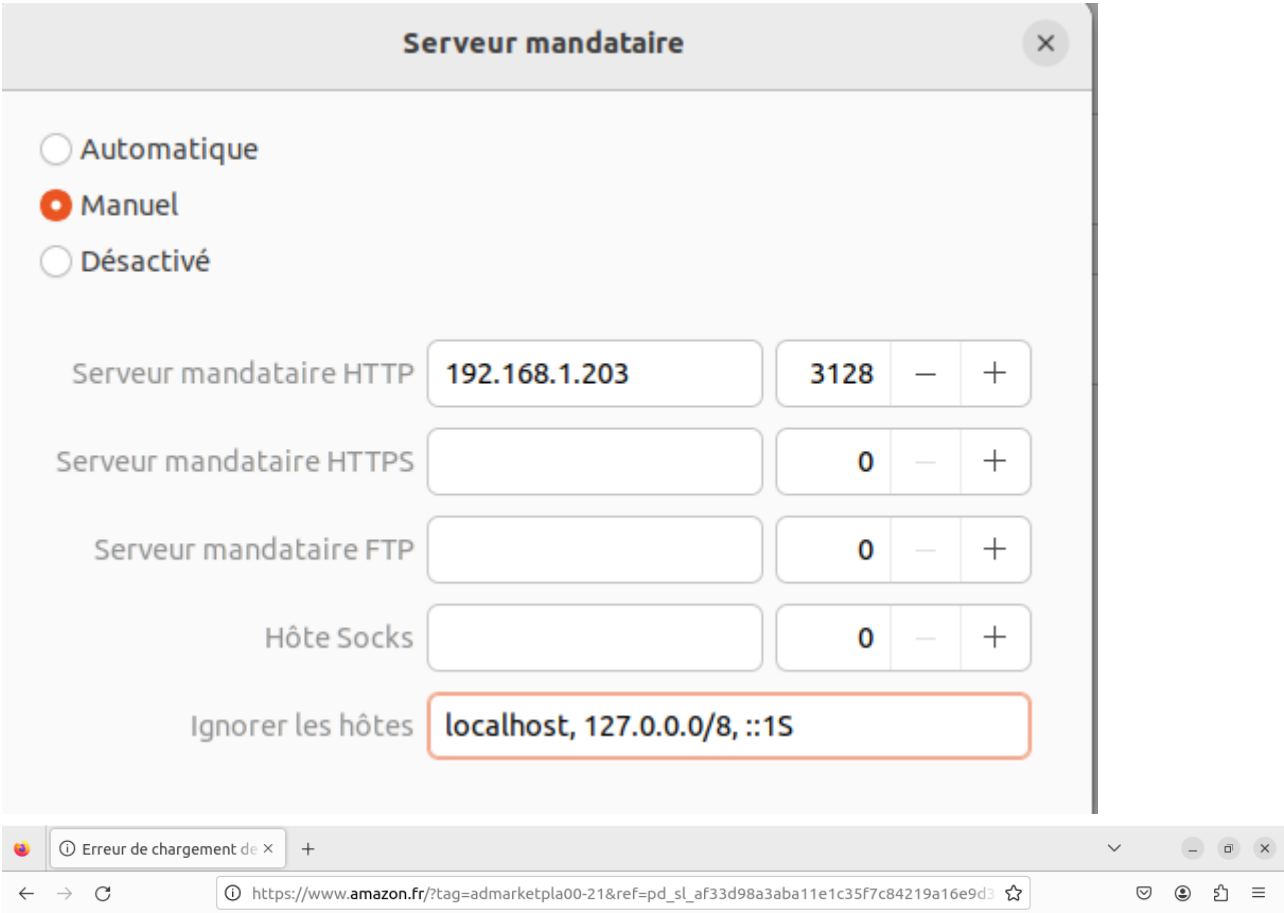
```
sysadmin@linuxroxx:~$ systemctl status squid.service
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-02-21 10:13:04 UTC; 11min ago
     Docs: man:squid(8)
   Process: 15470 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
    Main PID: 15473 (squid)
      Tasks: 4 (limit: 4558)
     Memory: 16.0M
        CPU: 316ms
   CGroup: /system.slice/squid.service
           └─15473 /usr/sbin/squid --foreground -sYC
             └─15475 "(squid-1)" --kid squid-1 --foreground -sYC
               └─15476 "(logfile-daemon)" /var/log/squid/access.log
                 └─15477 "(pinger)"
```

```
sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.bak # Sauvegarde du
fichier de configuration d'origine avant modif
```

```
sudo grep -vE '^#|^$' /etc/squid/squid.conf | sudo tee
/etc/squid/squid.conf > /dev/null # Retire les ligne commentées du fichier
de conf (plus de 9k lignes) par défaut)
```

```
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
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
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf
http_access allow localhost
http_access deny all
http_port 3128
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 \/(Packages|Sources)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern \/(Release(|\.gpg)$ 0 0% 0 refresh-ims
refresh_pattern \/(InRelease$ 0 0% 0 refresh-ims
refresh_pattern \/(Translation-.*)(|\.bz2|\.gz|\.xz)$ 0 0% 0 refresh-ims
refresh_pattern . 0 20% 4320
```

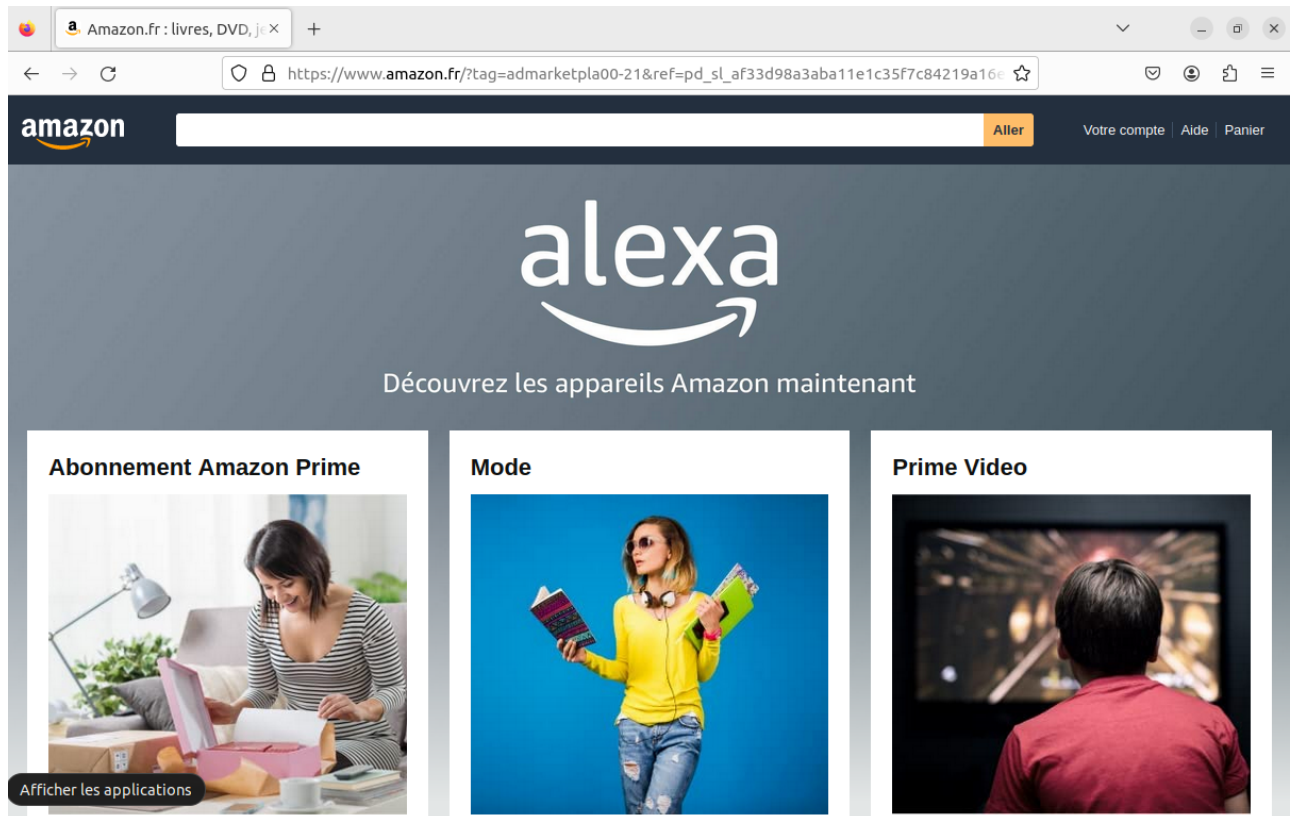
2. A ce stade, notre proxy bloque tout le trafic internet par défaut, et n'est pas en mode transparent. Ainsi, il nous faudra configurer le proxy côté client :



3. Autoriser l'accès au web pour notre réseau local

```
acl lan src 192.168.1.0/24
```

```
http_access allow lan
http_access deny all
```



4. Empêcher l'accès à certains domaines

```
acl youtubeblock dstdomain .youtube.com
acl leboncoinblock dstdomain .leboncoin.fr

http_access allow !youtubeblock !leboncoinblock
```



La connexion a été refusée par le serveur proxy

Une erreur est survenue pendant une connexion à www.leboncoin.fr.

- Vérifiez que les paramètres du proxy sont corrects ;
- Contactez votre administrateur réseau pour vous assurer que le serveur proxy fonctionne.

Réessayer

- Affichage des log

```
sudo cat /var/log/squid/access.log
```

```
1708613597.903 46 192.168.1.204 TCP_TUNNEL/200 39 CONNECT images-eu.ssl-images-amazon.com:443 - HIER_DIRECT/18.155.121.123 -  
1708613597.971 0 192.168.1.204 NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -  
1708613601.652 deny 0 192.168.1.204 TCP_DENIED/403 4012 CONNECT www.leboncoin.fr:443 - HIER_NONE/- text/html  
1708613603.502 2146 192.168.1.204 TCP_TUNNEL/200 5714 CONNECT lm.serving-sys.com:443 - HIER_DIRECT/52.28.91.150 line question...
```

TCP_TUNNEL pour Amazon qui est autorisé

TCP_DENIED pour Leboncoin est bloqué

- Nous allons maintenant passer notre proxy en mode transparent, ce qui offre l'avantage de rediriger automatiquement le trafic vers ce dernier sans avoir à paramétrer le poste client.

```
http_port 3128  
http_port 3129 intercept
```