
Installation du serveur Proxy Squid sous Windows.

Installation du serveur Proxy Squid sous Windows :

Un **serveur proxy** (appelé aussi «*serveur mandataire*») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un [réseau local](#) (utilisant parfois des [protocoles](#) autres que le [protocole TCP/IP](#)) et internet.

Squid a été porté sur la plateforme Windows afin d'être compatible avec l'OS et ainsi permettre aux professionnels de l'IT de l'intégrer sur une machine disposant de Windows comme un serveur par exempl

Étape 1 : Télécharger Squid pour Windows

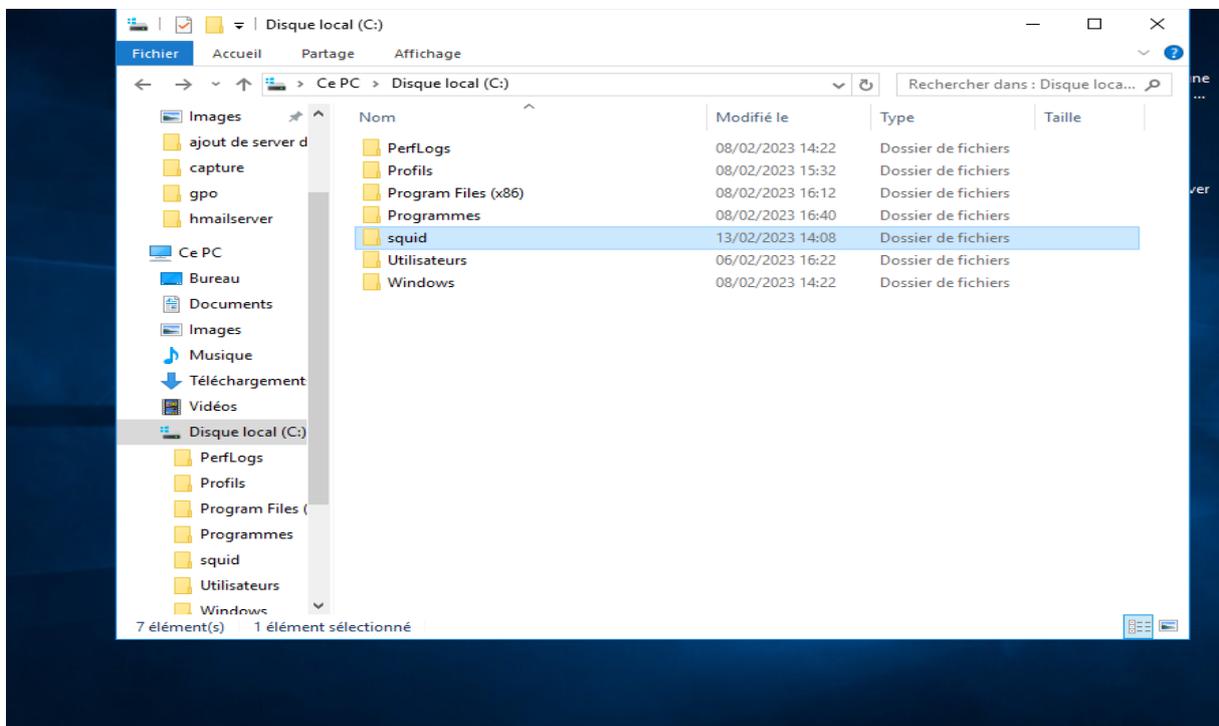
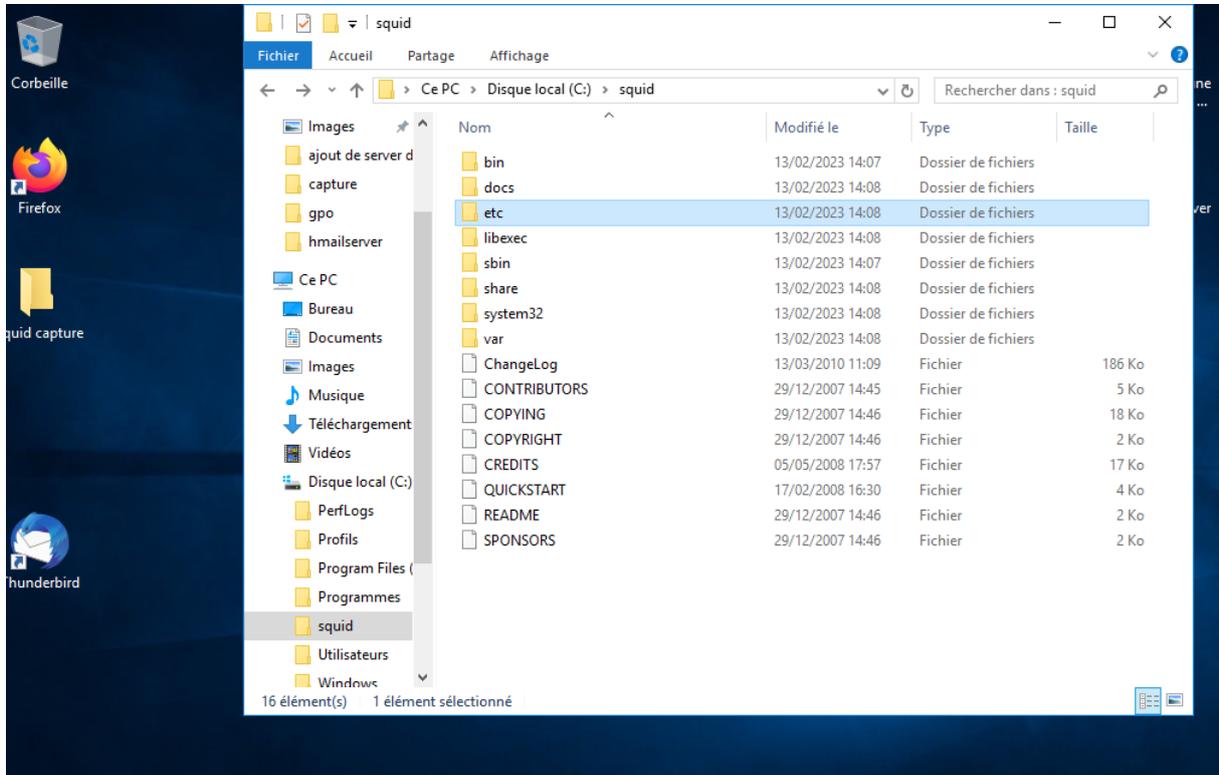
La première étape consiste à télécharger Squid pour Windows. Vous pouvez télécharger la dernière version de Squid pour Windows (**la version 2.7 STABLE8**) à partir du site officiel de Squid :

[http://squid.acmeconsulting.it/download ... DELAYP.zip](http://squid.acmeconsulting.it/download... DELAYP.zip)

On se retrouve avec un ZIP à dézipper sur notre serveur. Dans ce ZIP, un seul dossier (squid) que nous extrayons à la racine de notre lecteur C :
(Il faut faire bien attention de le mettre sur le C : sinon il faudra s'amuser à modifier la config de SQUID.)

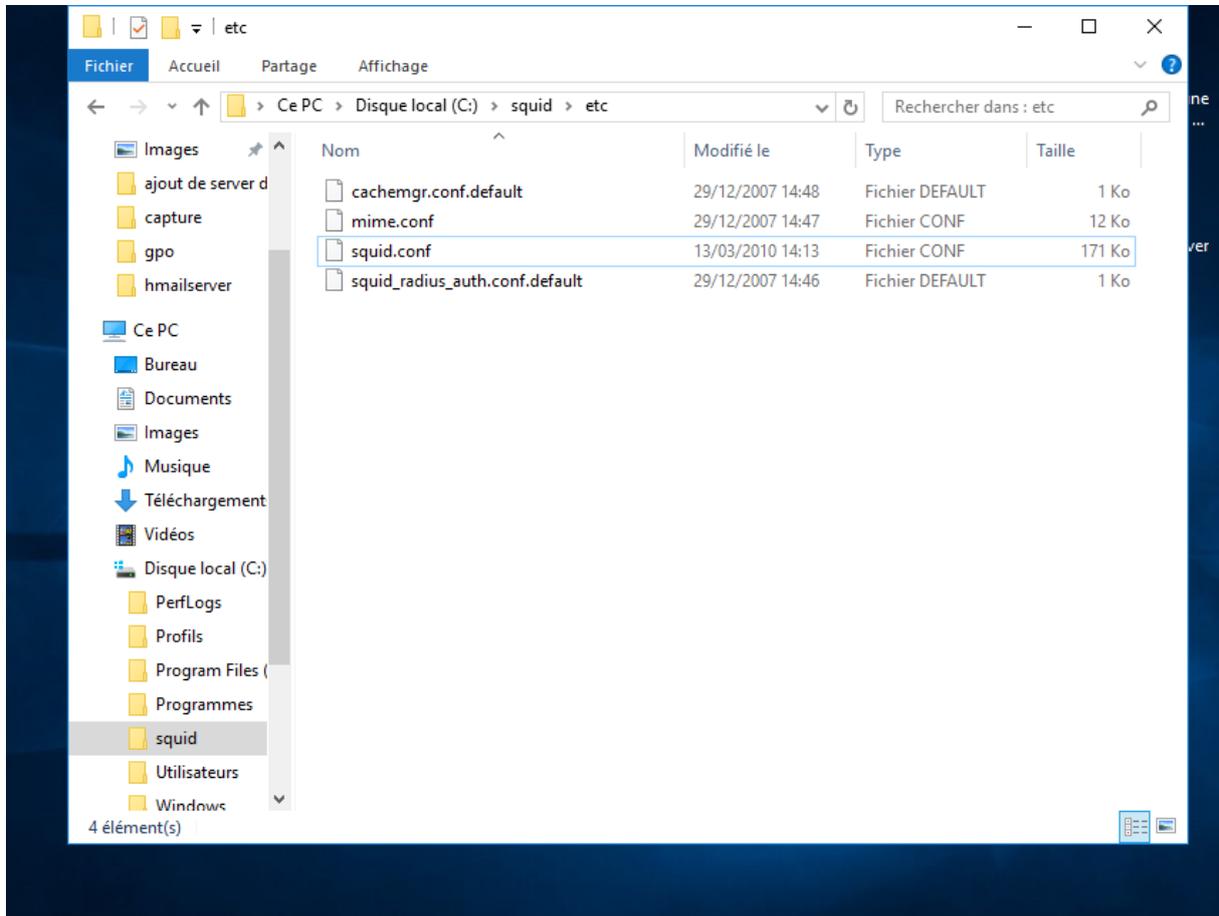
Installation de squid :

Une fois le dossier décompressé et placé à la racine de notre lecteur C : il faut se rendre dans : squid -> etc -> et renommer les fichiers :

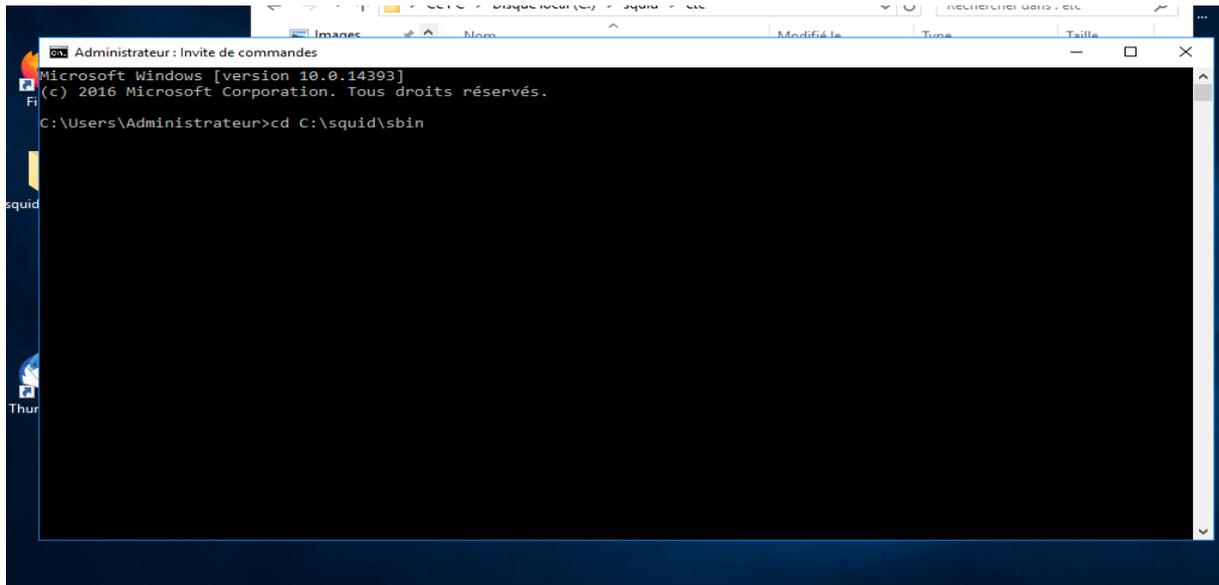


On modifie le fichier de configuration :

- « **mime.conf.default** » en « **mime.conf** »
- « **squid.conf.default** » en « **squid.conf** »

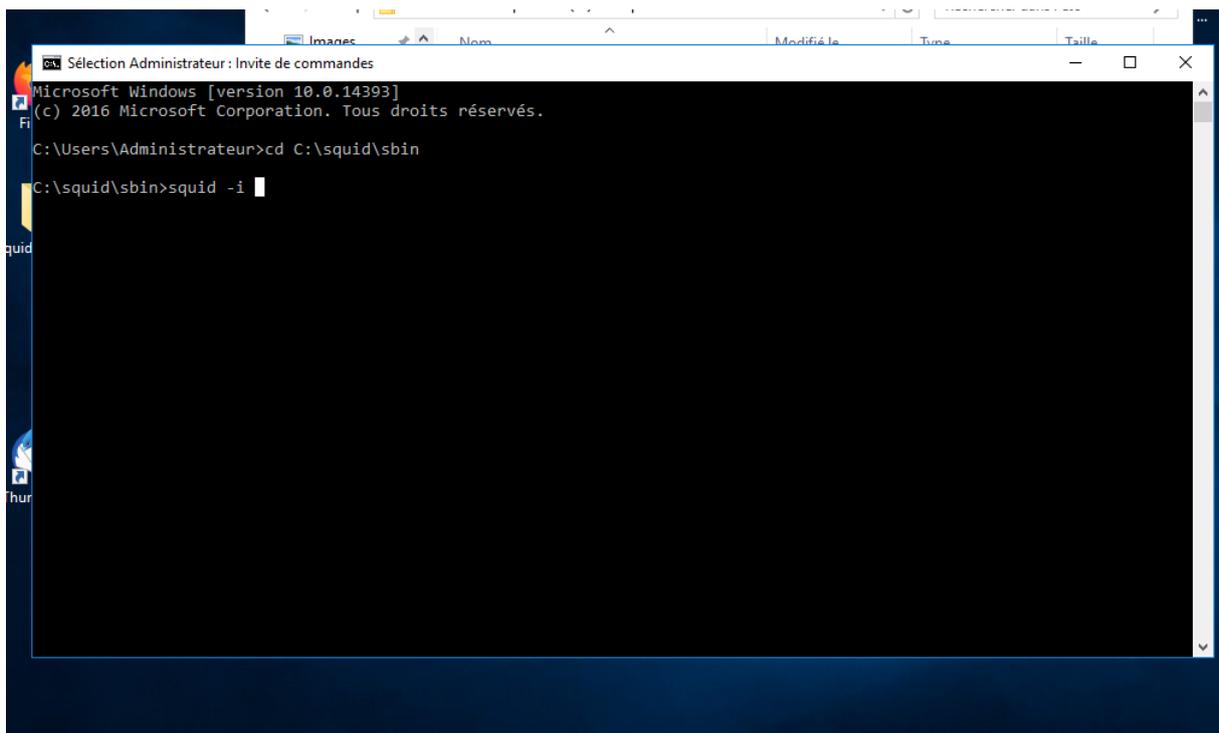


On ouvre une fenêtre de commande (*Windows + R, puis on tape cmd et valider*).
On tape **cd C:\squid\sbin** pour se placer dans le dossier « sbin » de l'installation de SQUID.



On tape « **squid -i** » pour créer le service squid.

(En effet SQUID s'installe sur Windows en tant que service afin de pouvoir le démarrer dès le lancement de Windows comme n'importe quel autre service.)



Voici ce qu'il s'affichera dans la fenêtre de commande si tout se passe bien :

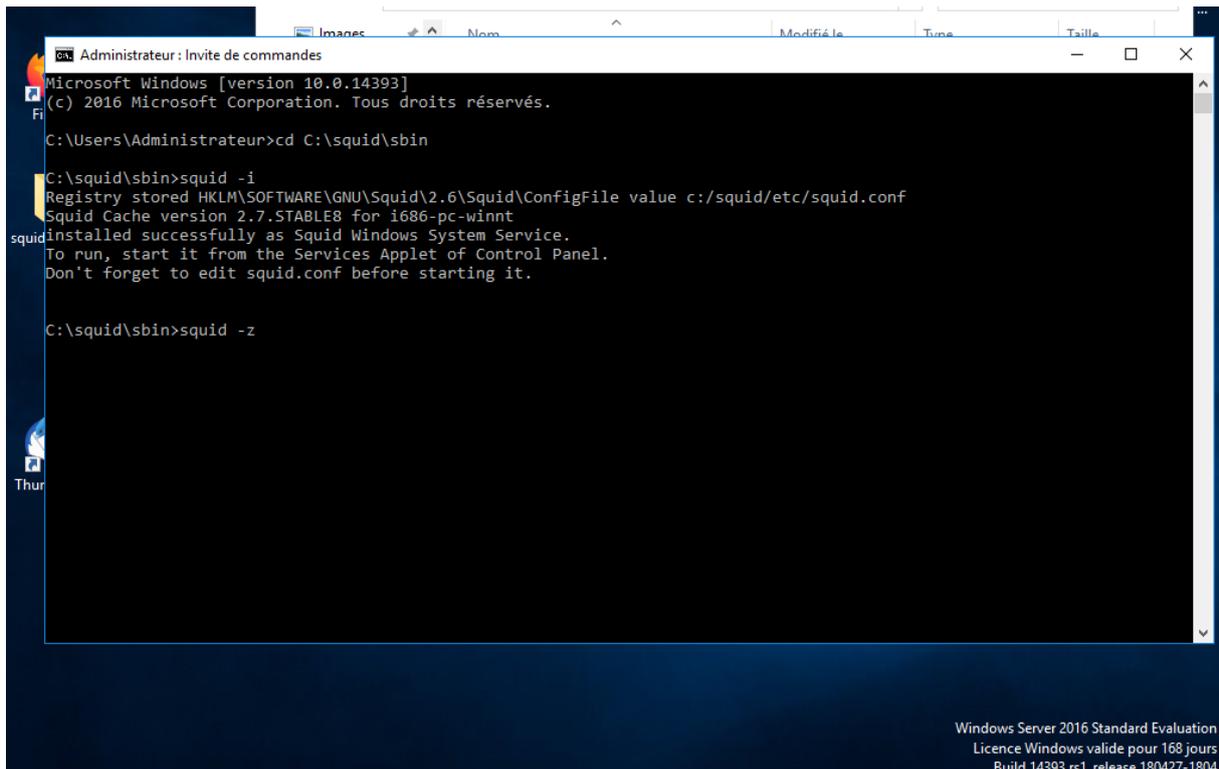
```
C:\squid\sbin>squid -i
Registry stored HKLM\SOFTWARE\GNU\Squid\2.6\Squid\ConfigFile value c:/squid/etc/
squid.conf
Squid Cache version 2.7.STABLE8 for i686-pc-winnt
installed successfully as Squid Windows System Service.
```

To run, start it from the Services Applet of Control Panel.
Don't forget to edit squid.conf before starting it.

Toujours dans la même fenêtre de commande, on tape « **squid -z** » afin de créer le dossier de cache :

Voici ce qui s'affichera dans la fenêtre de commande :

2013/04/08 15 :55 :48 | Creating Swap Directories



```
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>cd C:\squid\sbin

C:\squid\sbin>squid -i
Registry stored HKLM\SOFTWARE\GNU\Squid\2.6\Squid\ConfigFile value c:/squid/etc/squid.conf
Squid Cache version 2.7.STABLE8 for i686-pc-winnt
squid installed successfully as Squid Windows System Service.
To run, start it from the Services Applet of Control Panel.
Don't forget to edit squid.conf before starting it.

C:\squid\sbin>squid -z
```

Windows Server 2016 Standard Evaluation
Licence Windows valide pour 168 jours
Build 14393.rs1 release.180427-1804

Le serveur est maintenant équipé de SQUID, il ne reste plus qu'à le paramétrer

Configuration de squid :

◇ Afin de réaliser cela, il est possible d'accéder au menu de configuration en utilisant la barre des tâches ou en effectuant des modifications sur le fichier de configuration "squid.conf" qui se trouve à la racine du disque C dans le répertoire C:\squid\etc.

◇ Dans notre cas, on utilise un éditeur de texte comme Bloc-Notes pour ouvrir le fichier.

```
#
#Default:
# none

# TAG: httpd_suppress_version_string on|off
#     Suppress Squid version string info in HTTP headers and HTML error pages.
#
#Default:
# httpd_suppress_version_string off

# TAG: visible_hostname
#     If you want to present a special hostname in error messages, etc,
#     define this. Otherwise, the return value of gethostname()
#     will be used. If you have multiple caches in a cluster and
#     get errors about IP-forwarding you must set them to have individual
#     names with this setting.
#
#Default:
visible_hostname WIN-EIB711QND01

# TAG: unique_hostname
#     If you want to have multiple machines with the same
#     'visible_hostname' you must give each machine a different
```

◇ On retrouve le bloc:

```
# TAG: visible_hostname
# If you want to present a special hostname in error messages, etc,
# define this. Otherwise, the return value of gethostname()
# will be used. If you have multiple caches in a cluster and
# get errors about IP-forwarding you must set them to have individual
# names with this setting.
#
#Default:
# none
```

◇ On décommente la dernière ligne (**#none**) et on la remplace par :

visible_hostname WIN-EIB711QND01

```

71
72 # And finally deny all other access to this proxy
73 http_access deny all
74
75 # Squid normally listens to port 3128
76 http_port 3128
77 http_port 8080
78
79 # Uncomment the line below to enable disk caching - path
80 #cache_dir aufs /cygdrive/d/squid/cache 3000 16 256
81

```

◇ On retrouve le bloc:

```

# Squid normally listens to port 3128
http_port 3128

```

On peut modifier le port d'écoute de SQUID (en 8080 par exemple), mais on peut le laisser par défaut.

```

# ACLs all, manager, localhost, and to_localhost are predefined.
#
#
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network
#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
#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
acl CONNECT method CONNECT

# TAG: proxy_protocol_access
# Determine which client proxies can be trusted to provide correct
# information regarding real client IP address using PROXY protocol.
#

```

◇ Dans ce bloc :

On peut trouver dans cette configuration les trois plages d'adresses IP locales (A, B et C) conformes à la RFC1918 pour autoriser la navigation à partir de réseaux internes. Si notre réseau est inclus dans l'une de ces plages, aucune modification n'est nécessaire. Cependant, si notre réseau n'appartient pas à l'une de ces plages, il faudra ajouter une ligne pour notre adresse IP interne juste en dessous de la dernière ligne, comme cela :

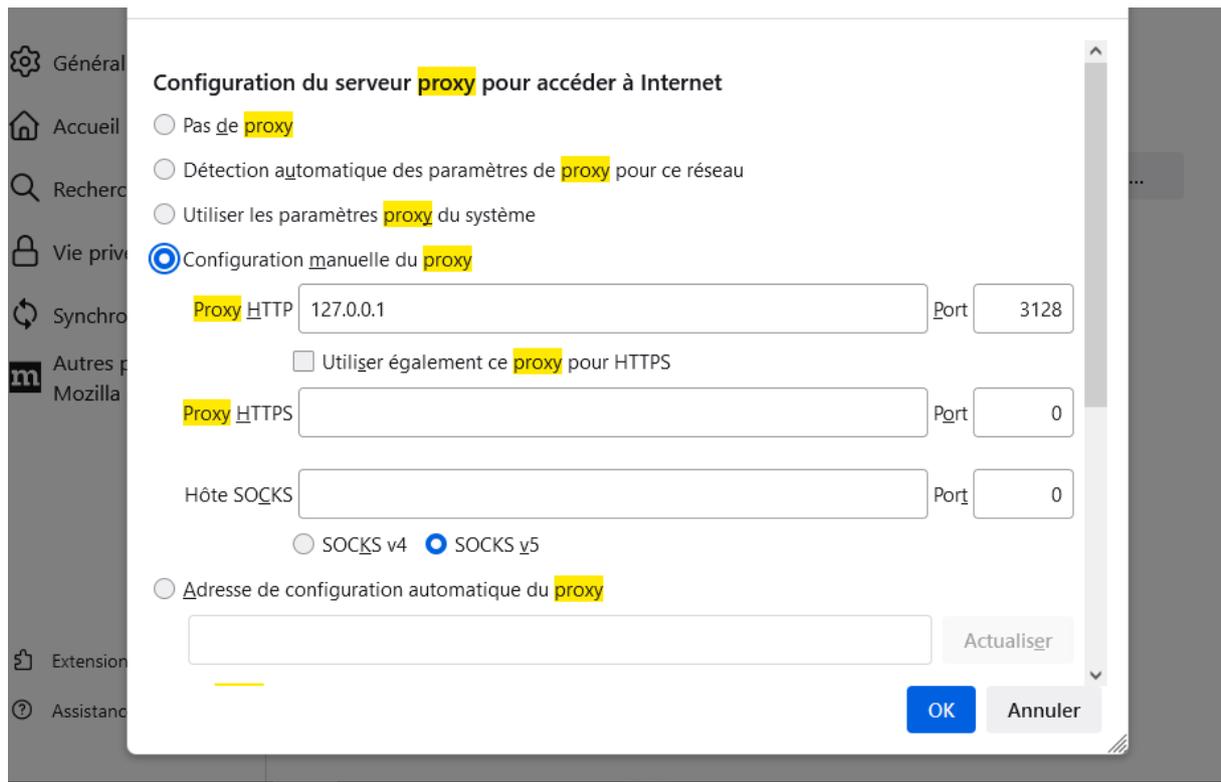
```
acl localnet src xxx.xxx.xxx.xxx/xx
```

◇ La configuration minimale du proxy est désormais achevée et il est possible d'enregistrer le fichier de configuration.

◇ Cependant, pour que les changements prennent effet, il est nécessaire de redémarrer le service squid. Cette opération doit être effectuée chaque fois que des modifications sont apportées au fichier **squid.conf**. Pour ce faire, il suffit d'accéder à la console de gestion des services Windows en appuyant sur les touches **Windows + R**, puis en tapant "**services.msc**" et en validant. Une fois dans la console, il faut localiser le service "**squid**", cliquer dessus avec le bouton droit de la souris, puis sélectionner "**Redémarrer**".

Test de l'accès au proxy :

◇ Pour utiliser le proxy avec Chrome ou tout autre navigateur, il est nécessaire de configurer les options de proxy. Pour cela, dans Chrome, il faut se rendre dans les **Paramètres**, puis dans les **Paramètres réseau**. Dans la section "**Serveur proxy**", **cocher les deux cases**, Dans "**Adresse**" mettez l'adresse IP locale du serveur sur lequel SQUID est installé . Enfin, dans la zone "**Port**", saisir le chiffre **3128**

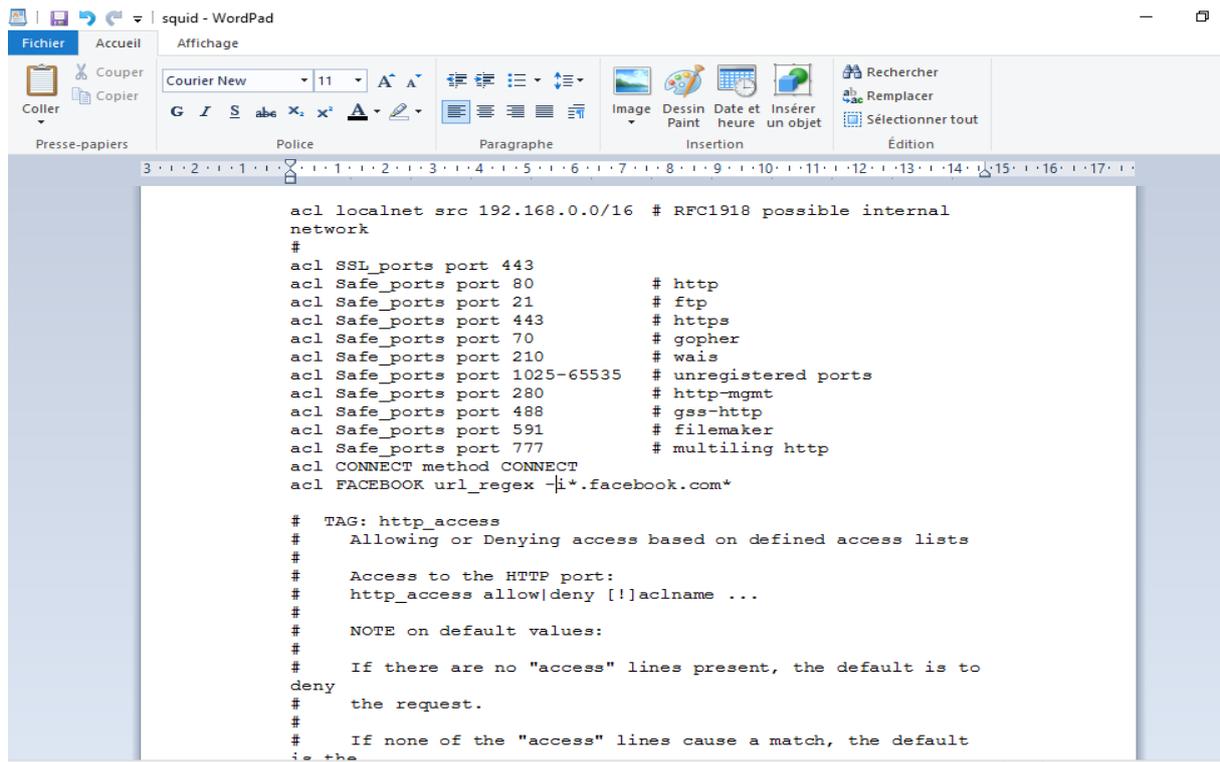


Blacklistage :

Le proxy est désormais configuré par défaut, sans aucune règle de restriction, ce qui signifie que l'accès à Internet est entièrement libre.

Cependant, nous allons maintenant ajouter quelques règles (également appelées ACL, pour "Listes de Contrôle d'Accès" en français) pour bloquer l'accès à certains sites web.

Nous allons commencer par interdire l'accès à Facebook.

A screenshot of a Windows WordPad application window titled "squid - WordPad". The window shows the text content of the "squid.conf" file. The text includes several ACL definitions for local networks and safe ports, followed by a "CONNECT" method ACL and a "TAG: http_access" section with explanatory comments.

```
acl localnet src 192.168.0.0/16 # RFC1918 possible internal
network
#
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
acl CONNECT method CONNECT
acl FACEBOOK url_regex -i *.facebook.com*

# TAG: http_access
#   Allowing or Denying access based on defined access lists
#
#   Access to the HTTP port:
#   http_access allow|deny [!]aclname ...
#
#   NOTE on default values:
#
#   If there are no "access" lines present, the default is to
deny
#   the request.
#
#   If none of the "access" lines cause a match, the default
is the
```

On ouvre le fichier « **squid.conf** » avec un éditeur de texte. On repère la ligne :

acl CONNECT method CONNECT

Juste après cette ligne, il est possible d'ajouter toutes les ACL que l'on souhaite. Dans mon cas, j'ajoute mon ACL (Facebook)

acl FACEBOOK url_regex -i *.facebook.com*

Maintenant que l'ACL pour Facebook est créée, il est nécessaire de dire au proxy de refuser l'accès à cette ACL, donc à Facebook.

```

# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
#
# We strongly recommend the following be uncommented to
protect innocent
# web applications running on the proxy server who think the
only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
CLIENTS
http_access deny FACEBOOK

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP
networks

```

Je repère la ligne :

INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

Il est possible d'ajouter nos propres règles d'accès juste après cette ligne. Dans le cadre de cet exemple, on peut ajouter la règle suivante :

http_access deny FACEBOOK , qui interdit l'accès à Facebook.

Voilà la règle de blocage de Facebook est désormais prête. Il convient maintenant d'enregistrer le fichier squid.conf.

Comme d'habitude, pour tout changement de configuration, il est nécessaire de redémarrer le service SQUID.



Ce site est inaccessible

127.0.0.1 n'autorise pas la connexion.

Essayez les suggestions ci-dessous :

- Vérifier la connexion
- Vérifier le proxy et le pare-feu

ERR_CONNECTION_REFUSED

Actualiser

DÉTAILS

Pour vérifier que tout est bien paramétré, il faut ouvrir une page Google depuis un ordinateur client du Proxy et rechercher "Facebook", puis ouvrir le lien.

Si tout est configuré correctement, vous devriez recevoir une page d'erreur du proxy vous informant que vous n'êtes pas autorisé à accéder à cette page

Blacklistage avec liste dans un fichier txt :

Nous créons un fichier texte intitulé "Médias_Sociaux .txt" dans le même dossier que le fichier squid.conf, soit C:\Squid\etc\squid.

puis nous y ajoutons les sites que nous souhaitons bloquer tels que :

. facebook.com

. wordpress.com

. hotmail.com

. free.fr

Une fois enregistré et fermé, nous retournons dans squid.conf

On repère la ligne : **acl CONNECT method CONNECT**

Et je rajoute la blacklist :

acl Medias_Sociaux url_regex -i « C:\squid\etc\Medias_Sociaux.txt »

Ensuite, on repère la ligne :

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

Puis on rajoute la nouvelle règle :

```
http_access deny Medias_Sociaux
```

Enfin, nous enregistrons et relançons Squid. Si tout est correctement configuré, tous les sites mentionnés dans le fichier texte Medias_Sociaux.txt seront bloqués.