

INSTALLER ET CONFIGURER UN PROXY CACHE SQUID

Table des matières

1. Le proxy-cache :	2
2. Installer le proxy-cache Squid :	3
3. Créer les règles du proxy-cache :	8
4. Test depuis un navigateur d'un poste client :	12

1. Le proxy-cache :

Le **proxy-cache** est très répandu dans le monde de l'entreprise, ce serveur se place sur le réseau des clients et joue le rôle d'intermédiaire avec les sites Internet distants.

Lors de la consultation d'une page internet par un client qui passe par le proxy-cache, les fichiers seront téléchargés par le client et seront stockés sur le proxy-cache.

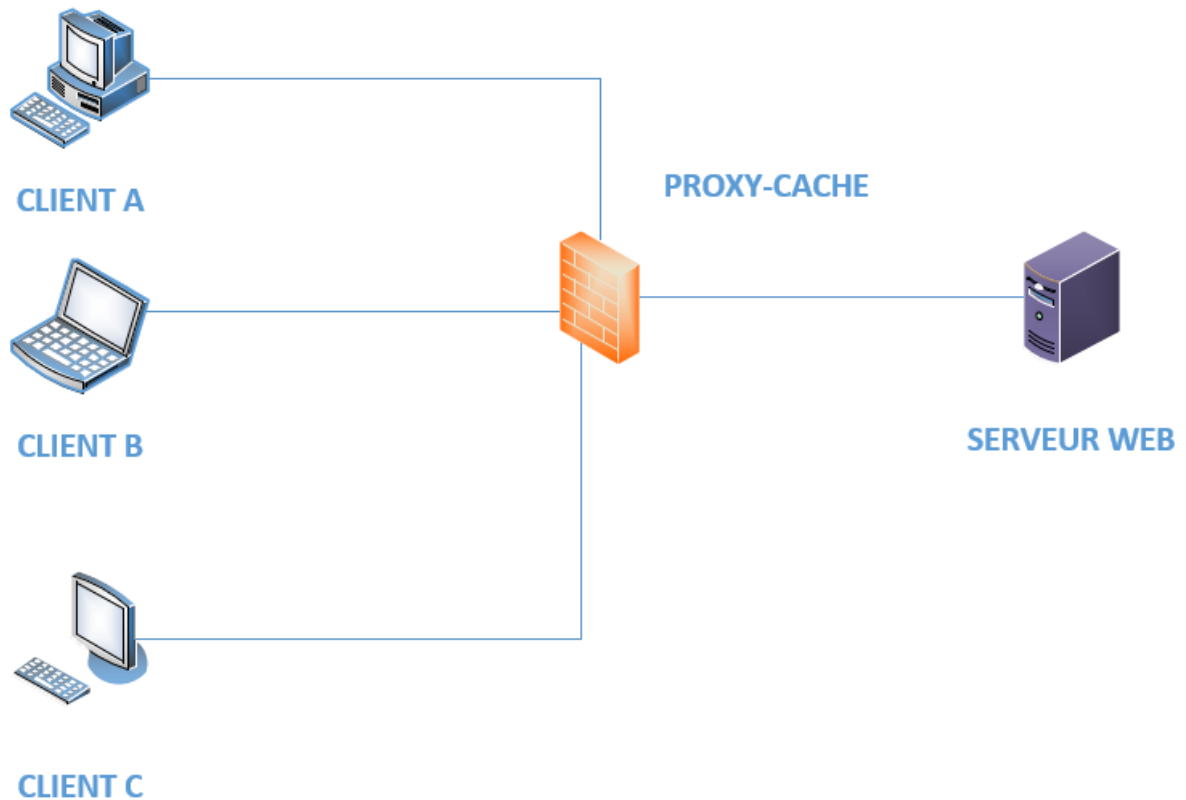
Dans le cas où un deuxième client consulte ces mêmes fichiers, ils seront disponibles dans le cache du proxy permettant ainsi **un accès plus rapide aux utilisateurs et un gain de bande passante** au niveau de la connexion Internet.

Une autre fonctionnalité d'un serveur proxy-cache est qu'il permet **d'autoriser ou interdire l'accès à certaines ressources en ligne** (site web, ports, services, etc.) afin de mettre en place une politique de sécurité globale pour le LAN.

Les différents façons d'utiliser un proxy-cache :

- **Utilisation optionnelle** : accès direct à Internet (mise en place pour améliorer les performances).
- **Utilisation obligatoire et explicite** : pour accéder à Internet, l'utilisateur doit passer à travers le proxy-cache (configuration manuelle du navigateur client).
- **Utilisation obligatoire et implicite** : pour accéder à Internet, l'utilisateur doit passer à travers le proxy-cache mais les utilisateurs n'ont pas besoin de configurer leurs navigateurs, la connexion à travers le proxy-cache est transparente.

L'utilisation d'un proxy-cache est soumis à la législation du pays qui impose notamment en France d'informer les utilisateurs de la collecte et l'utilisation de leurs données.



2. Installer le proxy-cache Squid :

Installez le package squid à l'aide de la commande suivante : ***apt-get install squid***.

```

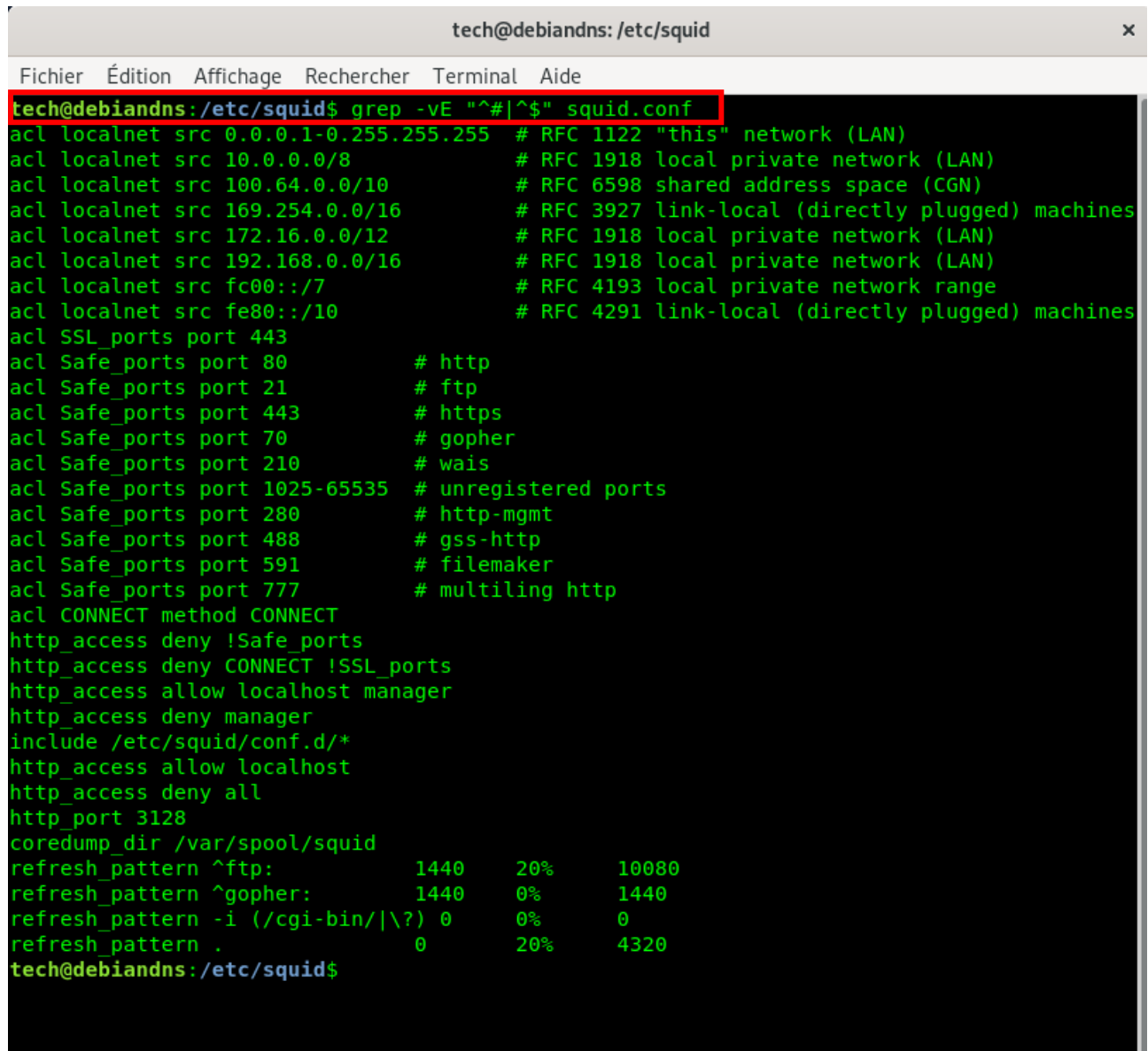
tech@debiandns: ~
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
tech@debiandns:~$ sudo apt-get install squid
[sudo] Mot de passe de tech :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-4.19.0-14-amd64
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
  libdbi-perl libcap3 squid-common squid-langpack
Paquets suggérés :
  libclone-perl libmldbm-perl libnet-daemon-perl
  libsql-statement-perl squidclient squid-cgi squid-purge
  resolvconf smbclient ufw winbind
Les NOUVEAUX paquets suivants seront installés :
  libdbi-perl libcap3 squid squid-common squid-langpack
0 mis à jour, 5 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 3 915 ko dans les archives.
Après cette opération, 15,4 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n]

```

La configuration du proxy-cache squid se fait directement à partir du fichier de configuration qui se trouve à l'emplacement `/etc/squid/squid.conf`.

Les lignes commençant par un `#` sont des commentaires, par défaut sur Debian ce fichier est abondamment commenté.

Tapez la commande `grep -vE « ^#|^$ » /etc/squid/squid.conf` pour ne pas afficher les lignes de commentaires.



```
tech@debiandns: /etc/squid
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
tech@debiandns:/etc/squid$ grep -vE "^#|^$" squid.conf
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8           # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10        # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16       # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12        # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16       # RFC 1918 local private network (LAN)
acl localnet src fc00::/7            # RFC 4193 local private network range
acl localnet src fe80::/10           # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80                # http
acl Safe_ports port 21                # ftp
acl Safe_ports port 443               # https
acl Safe_ports port 70                # gopher
acl Safe_ports port 210               # wais
acl Safe_ports port 1025-65535        # unregistered ports
acl Safe_ports port 280               # http-mgmt
acl Safe_ports port 488               # gss-http
acl Safe_ports port 591               # filemaker
acl Safe_ports port 777               # multiling http
acl CONNECT method CONNECT
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*
http_access allow localhost
http_access deny all
http_port 3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp:                1440    20%    10080
refresh_pattern ^gopher:             1440    0%     1440
refresh_pattern -i (/cgi-bin/|\?)    0        0%     0
refresh_pattern .                     0        20%    4320
tech@debiandns:/etc/squid$
```

Chacune des lignes commencent par une directive :

- **http_port** : indique l'adresse et le port sur lesquels écoute Squid, par défaut il écoute toute les interfaces sur le port 3128 (plusieurs directives `http_port` sont configurables).
- **coredump_dir** : indique le répertoire dans lequel Squid peut écrire des fichiers core (fichiers d'erreurs).
- **refresh_pattern** : ces directives précisent les règles qui établissent qu'un fichier est « frais » ou « périmé » (s'il est périmé, il est supprimé du cache).

Les directives les plus importantes sont **acl** et **http_access**, les listes d'accès sont des critères de contrôle d'accès qui sont utilisées par la directive **http_access** pour autoriser ou interdire une connexion http/https en fonction des critères de la liste d'accès.

La directive **acl** est composée :

- le 2^{ème} champ représente le nom de l'ACL, plusieurs directives avec le même nom vont cumuler les critères de chaque directive.
- le 3^{ème} champ indique le type d'ACL, les plus importants sont **src** (source) , **dst** (destination), **port** et **time**.
- le 4^{ème} champ indique la valeur, en fonction du type ce champ sera l'adresse d'un réseau, d'un port, etc.

L'ACL **Safe_ports** définie par défaut regroupe un ensemble de ports TCP courants et considérés comme sûrs auxquels vous pourrez donner accès aux utilisateurs.

La directive **http_access** permet d'autoriser (**allow**) ou interdire (**deny**) l'accès au proxy-cache en fonction de l'ACL associée (! devant une ACL indique le contraire de l'ACL).

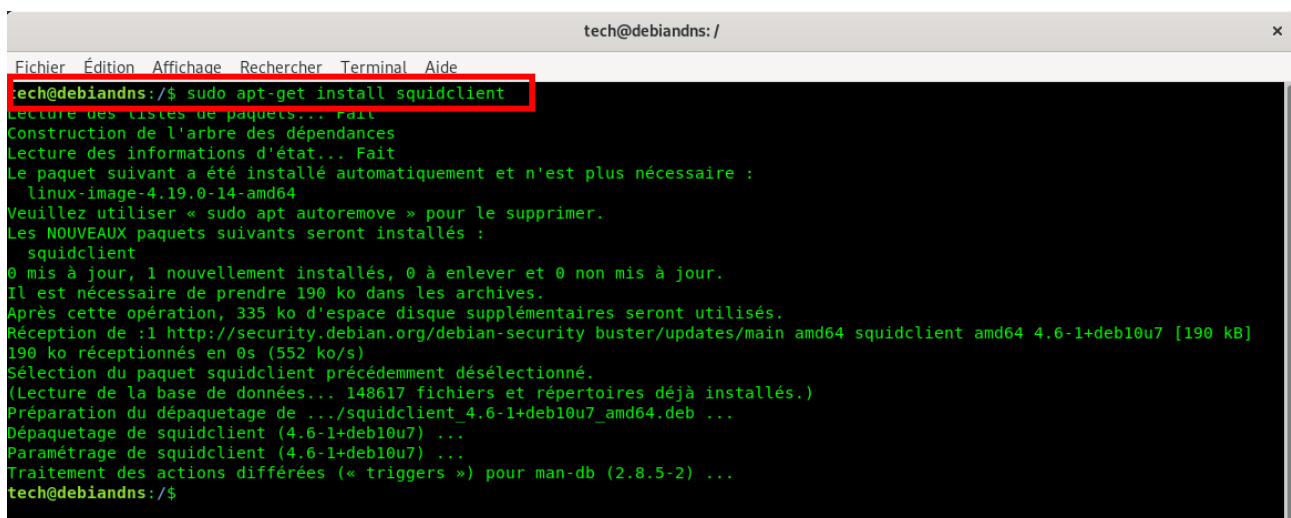
http_access deny !Safe_ports : cette directive interdit l'accès à tous les ports sauf les ports définis dans l'ACL **Safe_ports**.

Les directives http_access sont lues dans l'ordre (séquentiel) et exécutées dès qu'une règle correspond à la directive.

Il est recommandé de terminer toujours par **http_access deny all** afin d'interdire l'accès si aucune règle ne correspond à une directive.

http_access allow localhost manager : cette directive n'autorise l'accès au service de manager qu'à partir du poste localement.

Squid dispose d'un Cache Manager qui est une interface web de gestion du cache accessible en lignes de commandes avec l'outil **squidclient**.



```
tech@debiandns: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
tech@debiandns:/$ sudo apt-get install squidclient
Lecture des listes de paquets... fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-4.19.0-14-amd64
Veuillez utiliser « sudo apt autoremove » pour le supprimer.
Les NOUVEAUX paquets suivants seront installés :
  squidclient
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 190 ko dans les archives.
Après cette opération, 335 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://security.debian.org/debian-security buster/updates/main amd64 squidclient amd64 4.6-1+deb10u7 [190 kB]
190 ko réceptionnés en 0s (552 ko/s)
Sélection du paquet squidclient précédemment désélectionné.
(Lecture de la base de données... 148617 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ../squidclient_4.6-1+deb10u7_amd64.deb ...
Dépaquetage de squidclient (4.6-1+deb10u7) ...
Paramétrage de squidclient (4.6-1+deb10u7) ...
Traitement des actions différées (« triggers ») pour man-db (2.8.5-2) ...
tech@debiandns:/$
```

Fichier Édition Affichage Rechercher Terminal Aide

```
Dépaquetage de squidclient (4.6-1+deb10u7) ...  
Paramétrage de squidclient (4.6-1+deb10u7) ...  
Traitement des actions différées (« triggers ») pour man-db (2.8.5-2) ...  
tech@debiandns:/$ squidclient mgr:info
```

```
HTTP/1.1 200 OK  
Server: squid/4.6  
Mime-Version: 1.0  
Date: Tue, 09 Aug 2022 09:36:16 GMT  
Content-Type: text/plain;charset=utf-8  
Expires: Tue, 09 Aug 2022 09:36:16 GMT  
Last-Modified: Tue, 09 Aug 2022 09:36:16 GMT  
X-Cache: MISS from debiandns.mondomaine.lan  
X-Cache-Lookup: MISS from debiandns.mondomaine.lan:3128  
Via: 1.1 debiandns.mondomaine.lan (squid/4.6)  
Connection: close
```

```
Squid Object Cache: Version 4.6  
Build Info: Debian linux  
Service Name: squid  
Start Time: Tue, 09 Aug 2022 09:28:06 GMT  
Current Time: Tue, 09 Aug 2022 09:36:16 GMT  
Connection information for squid:
```

```
Number of clients accessing cache: 1  
Number of HTTP requests received: 0  
Number of ICP messages received: 0  
Number of ICP messages sent: 0  
Number of queued ICP replies: 0  
Number of HTCP messages received: 0  
Number of HTCP messages sent: 0  
Request failure ratio: 0.00  
Average HTTP requests per minute since start: 0.0  
Average ICP messages per minute since start: 0.0  
Select loop called: 1140 times, 430.276 ms avg
```

```
Cache information for squid:
```

```
Hits as % of all requests: 5min: 0.0%, 60min: 0.0%  
Hits as % of bytes sent: 5min: -0.0%, 60min: -0.0%  
Memory hits as % of hit requests: 5min: 0.0%, 60min: 0.0%  
Disk hits as % of hit requests: 5min: 0.0%, 60min: 0.0%  
Storage Swap size: 0 KB  
Storage Swap capacity: 0.0% used, 0.0% free  
Storage Mem size: 216 KB  
Storage Mem capacity: 0.1% used, 99.9% free  
Mean Object Size: 0.00 KB
```

Fichier Édition Affichage Rechercher Terminal Aide

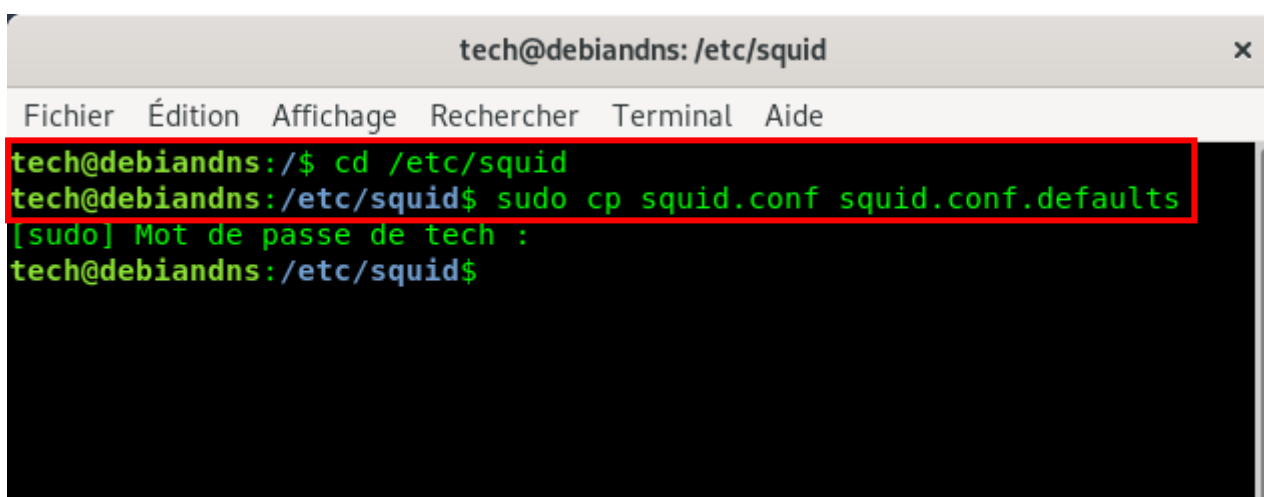
```
Hits as % of bytes sent:      5min: -0.0%, 60min: -0.0%
Memory hits as % of hit requests:      5min: 0.0%, 60min: 0.0%
Disk hits as % of hit requests: 5min: 0.0%, 60min: 0.0%
Storage Swap size:          0 KB
Storage Swap capacity:      0.0% used, 0.0% free
Storage Mem size:           216 KB
Storage Mem capacity:       0.1% used, 99.9% free
Mean Object Size:           0.00 KB
Requests given to unlinkd:      0
Median Service Times (seconds) 5 min   60 min:
HTTP Requests (All):          0.00000 0.00000
Cache Misses:                  0.00000 0.00000
Cache Hits:                     0.00000 0.00000
Near Hits:                       0.00000 0.00000
Not-Modified Replies:         0.00000 0.00000
DNS Lookups:                    0.00000 0.00000
ICP Queries:                    0.00000 0.00000
Resource usage for squid:
UP Time:                        490.515 seconds
CPU Time:                        0.049 seconds
CPU Usage:                        0.01%
CPU Usage, 5 minute avg:          0.01%
CPU Usage, 60 minute avg:         0.01%
Maximum Resident Size: 94240 KB
Page faults with physical i/o: 0
Memory accounted for:
Total accounted:                  534 KB
memPoolAlloc calls:               3081
memPoolFree calls:                3086
File descriptor usage for squid:
Maximum number of file descriptors: 1024
Largest file desc currently in use: 14
Number of file desc currently in use: 7
Files queued for open:            0
Available number of file descriptors: 1017
Reserved number of file descriptors: 100
Store Disk files open:            0
Internal Data Structures:
  52 StoreEntries
  52 StoreEntries with MemObjects
  0 Hot Object Cache Items
  0 on-disk objects
tech@debiandns:/$ █
```

3. Créer les règles du proxy-cache :

Dans le cadre du test du fonctionnement du proxy-cache squid, vous allez créer une politique de sécurité pour le réseau LAN :

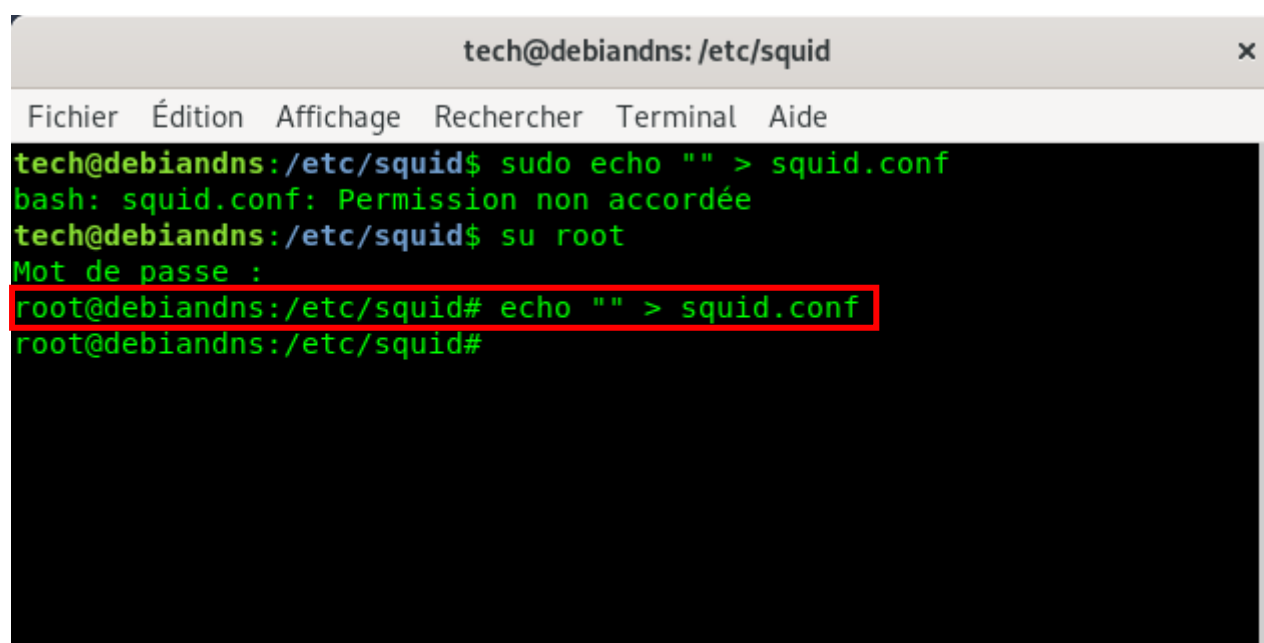
- Les utilisateurs ne peuvent se connecter qu'aux services HTTP et HTTPS sur les ports par défaut.
- Les utilisateurs peuvent consulter Facebook uniquement entre 12h et 14h.

Sauvegardez la configuration par défaut du fichier **squid.conf** en cas de dysfonctionnement.



```
tech@debiandns: /etc/squid
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
tech@debiandns:/$ cd /etc/squid
tech@debiandns:/etc/squid$ sudo cp squid.conf squid.conf.defaults
[sudo] Mot de passe de tech :
tech@debiandns:/etc/squid$
```

Videz en tant que root le fichier **squid.conf** qui comporte trop de lignes commentées à l'aide de la commande **echo "" > squid.conf**.



```
tech@debiandns: /etc/squid
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
tech@debiandns:/etc/squid$ sudo echo "" > squid.conf
bash: squid.conf: Permission non accordée
tech@debiandns:/etc/squid$ su root
Mot de passe :
root@debiandns:/etc/squid# echo "" > squid.conf
root@debiandns:/etc/squid#
```

Editez le contenu du fichier squid.conf pour établir les directives.


```
tech@debiandns: /etc/squid
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 3.2      squid.conf      Modifié
http port 192.168.0.10:3128
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 (Release|Packages(.gz)*)$      0      20%      2880
refresh_pattern .      0      20% 4320

```

^G Aide ^O Écrire ^W Chercher ^K Couper ^J Justifier
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^T Orthograp.

Toutes les directives ci-dessus sont des directives par défaut hormis la directive **http_port** qui écoute sur l'interface interne du serveur (LAN) si celui possède deux interfaces réseaux (LAN et WAN).

Cette directive oblige les utilisateurs du LAN de passer par le proxy-cache pour l'accès au WAN.

Les directives ACL sont aussi les directives par défaut relatives aux ports 80 et 443.

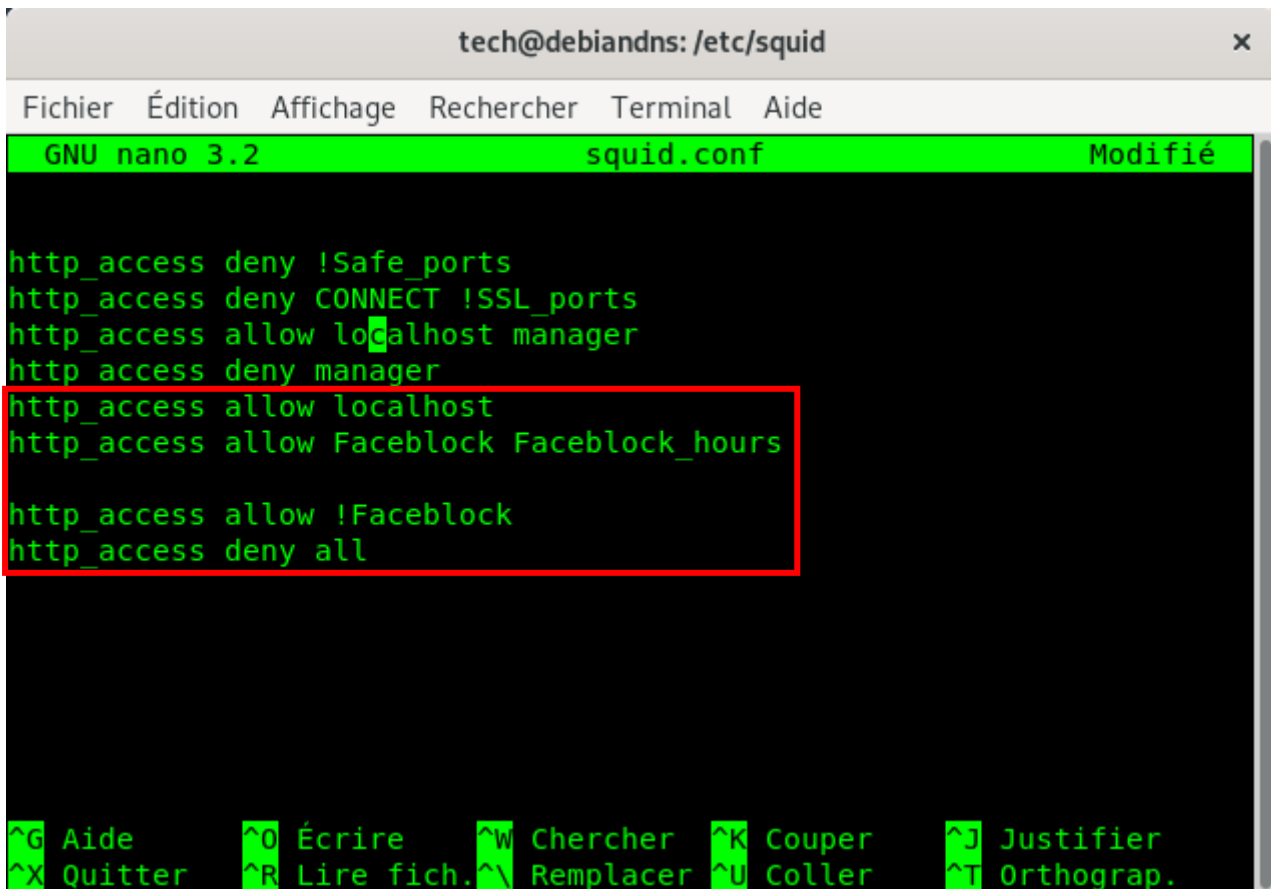
```
tech@debiandns: /etc/squid
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 3.2 squid.conf Modifié
http_port 192.168.0.10:3128
coredump_dir /var/spool/squid
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern (Release|Packages|.gz)*$ 0 20% 2880
refresh_pattern . 0 20% 4320
acl SSL_ports port 443
acl Safe_ports port 80 # http
acl Safe_ports port 443 # https
acl CONNECT method CONNECT
acl Facebook dstdomain .facebook.com
acl Facebook_hours time M T W T F 12:00-14:00
^G Aide ^O Écrire ^W Chercher ^K Couper ^J Justifier
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^T Orthograp.
```

Ajoutez les directives permettant de filtrer l'accès au domaine de destination facebook.com, le type **dstdomain** filtre le nom du domaine de destination.

Le type **time** permet d'indiquer des jours et des créneaux horaires pour la directive.

Maintenant les ACL sont définies, vous pouvez les utiliser au sein des directives d'autorisations et de restrictions.

Commencez par établir les directives d'autorisation et terminez par les directives d'interdiction.



The screenshot shows a terminal window titled 'tech@debiandns: /etc/squid' with a nano editor open to 'squid.conf'. The editor's status bar shows 'GNU nano 3.2' and 'Modifié'. The configuration file content is as follows:

```
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access allow Facebook Facebook_hours
http_access allow !Facebook
http_access deny all
```

At the bottom of the editor, a list of keyboard shortcuts is visible:

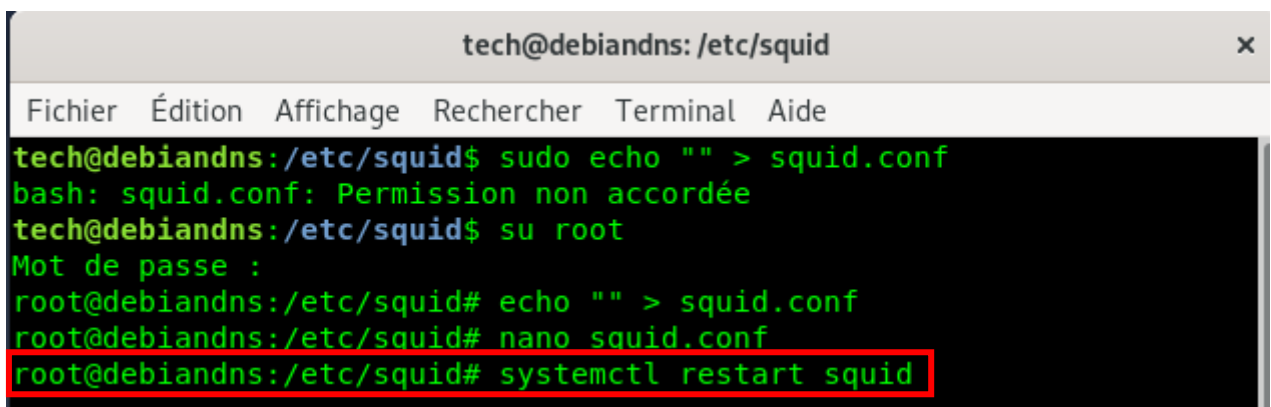
```
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^T Orthograp.
```

La directive `http_access allow Facebook Facebook_hours` contient deux ACL, les deux ACL doivent être vraies en même temps pour que la directive s'applique (ET logique).

La règle suivante `http_access allow !Facebook` autorise l'accès à tous les domaines sauf à l'ACL Facebook (Facebook.com).

Tous les autres accès sont interdits par la dernière directive.

Enregistrez le fichier, puis redémarrez les services de squid.



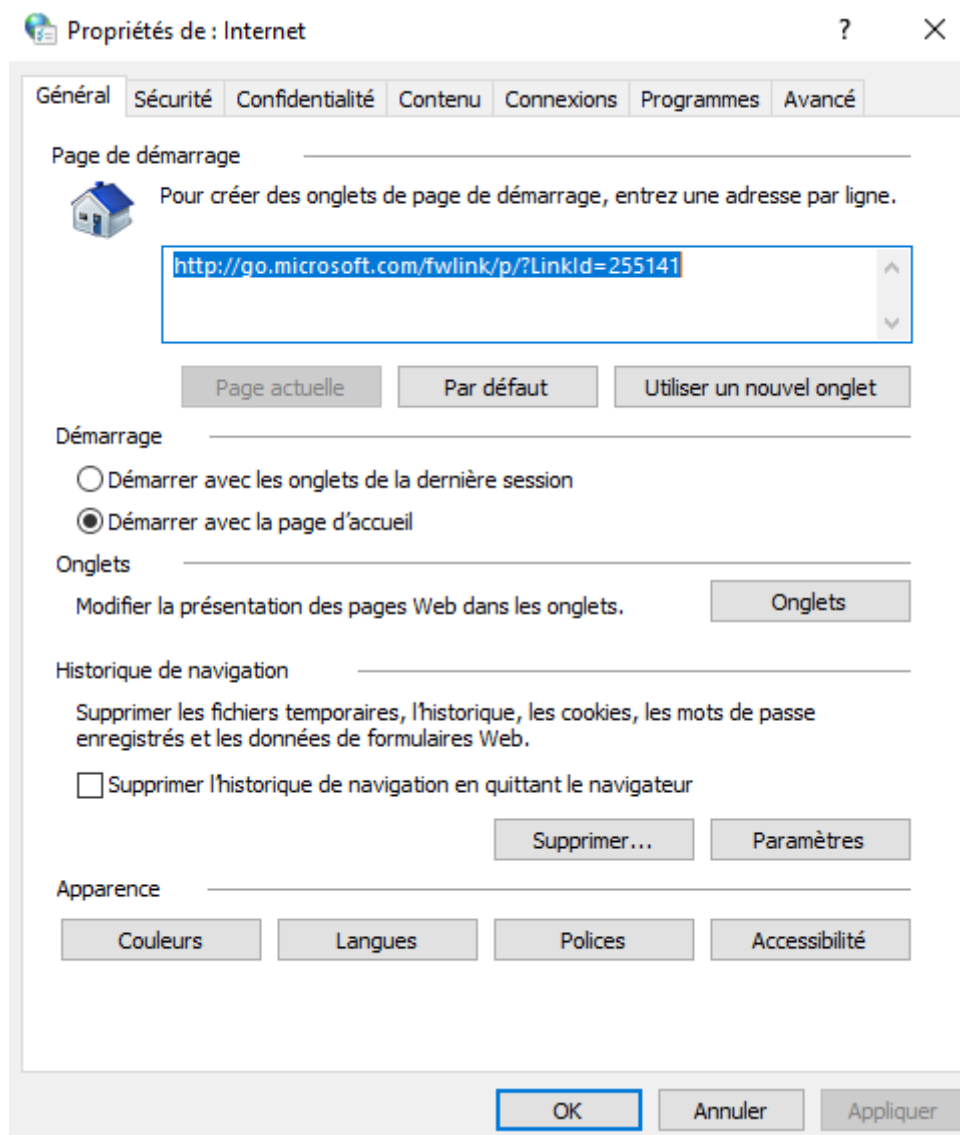
The screenshot shows a terminal window titled 'tech@debiandns: /etc/squid' with the following commands and output:

```
tech@debiandns:/etc/squid$ sudo echo "" > squid.conf
bash: squid.conf: Permission non accordée
tech@debiandns:/etc/squid$ su root
Mot de passe :
root@debiandns:/etc/squid# echo "" > squid.conf
root@debiandns:/etc/squid# nano squid.conf
root@debiandns:/etc/squid# systemctl restart squid
```

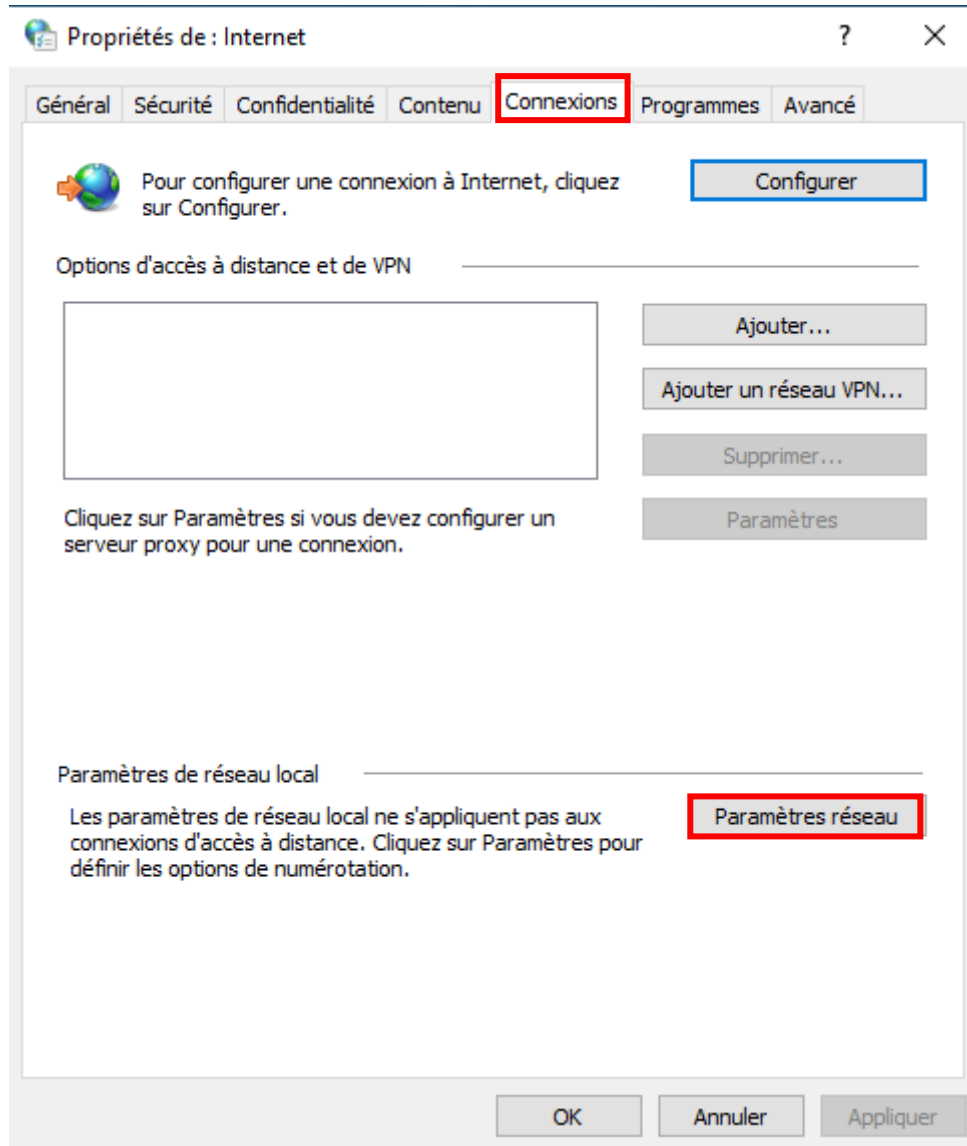
4. Test depuis un navigateur d'un poste client :

Vous devez configurer le navigateur internet du poste d'un client pour le forcer à passer par le proxy-cache pour la consultation de pages web.

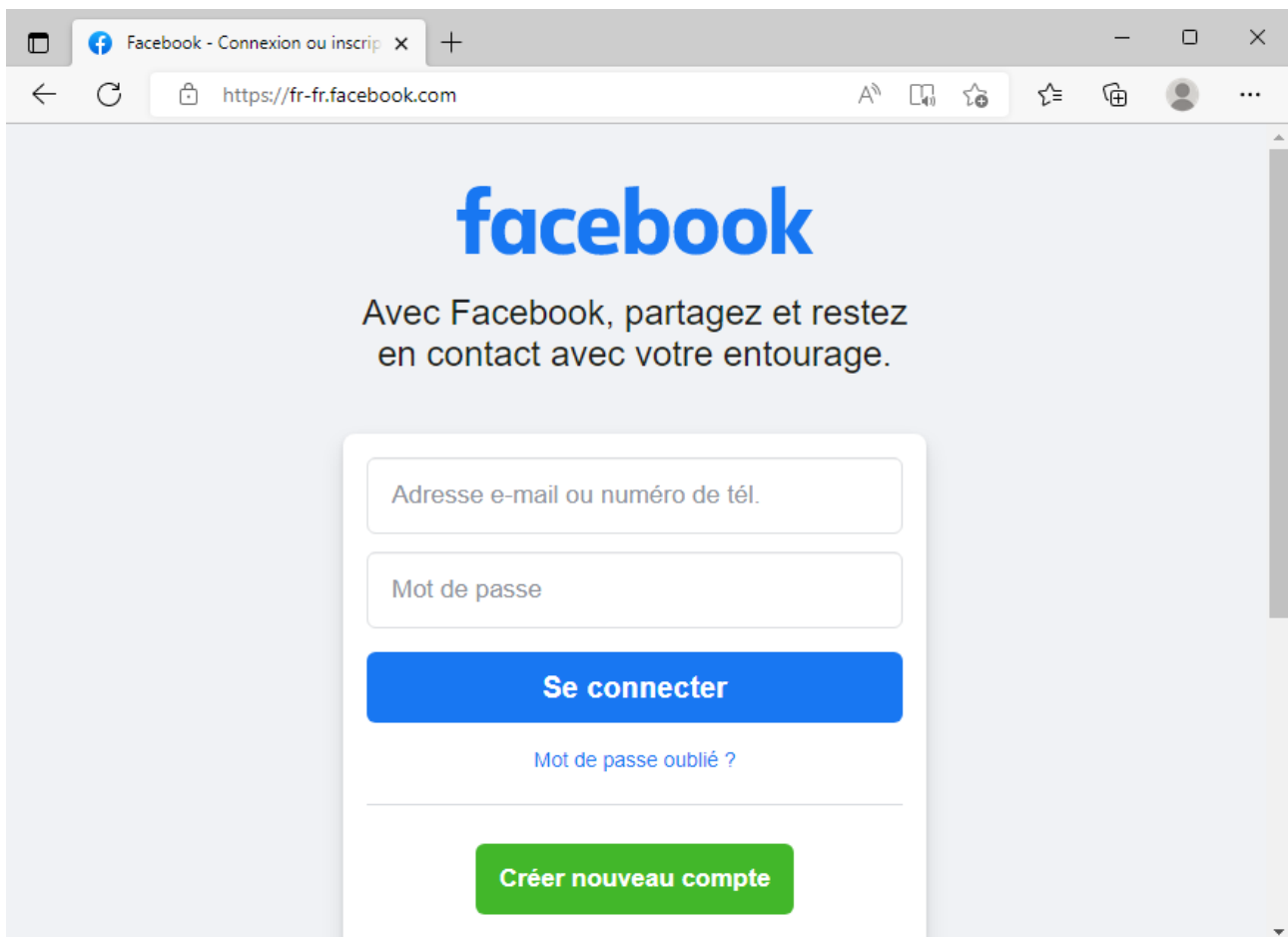
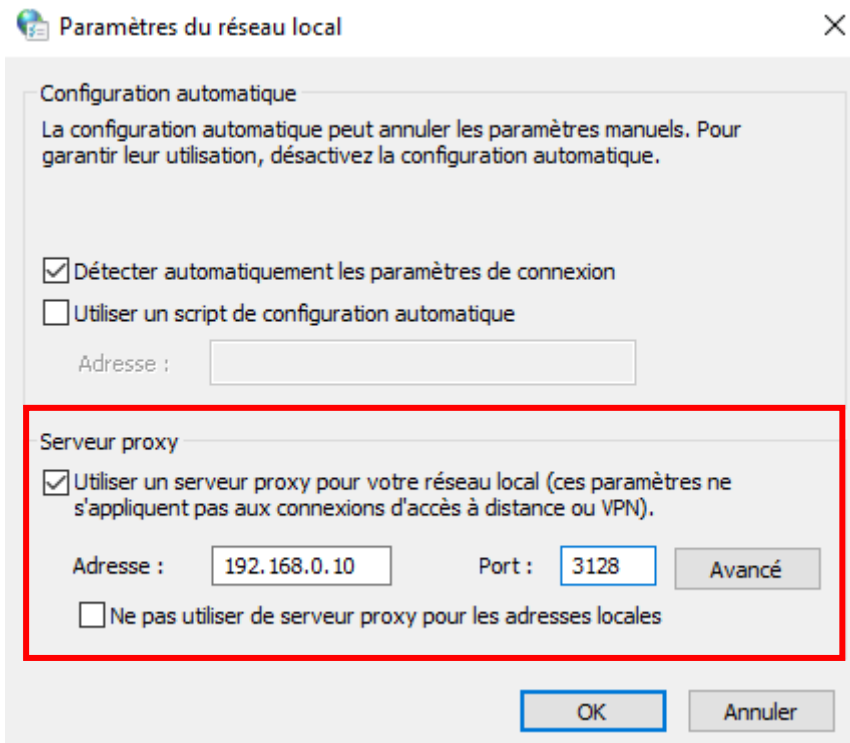
Accédez aux **propriétés Internet** pour un client sur Windows.



Affichez l'onglet Connexions, puis les paramètres réseau.



Spécifiez l'adresse IP du proxy-cache ainsi que le port par défaut 3128 pour le proxy-cache squid.



Testez le bon fonctionnement des directives du proxy-cache.

Le site Facebook est accessible uniquement du Lundi au vendredi de 12h à 14h.

