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.

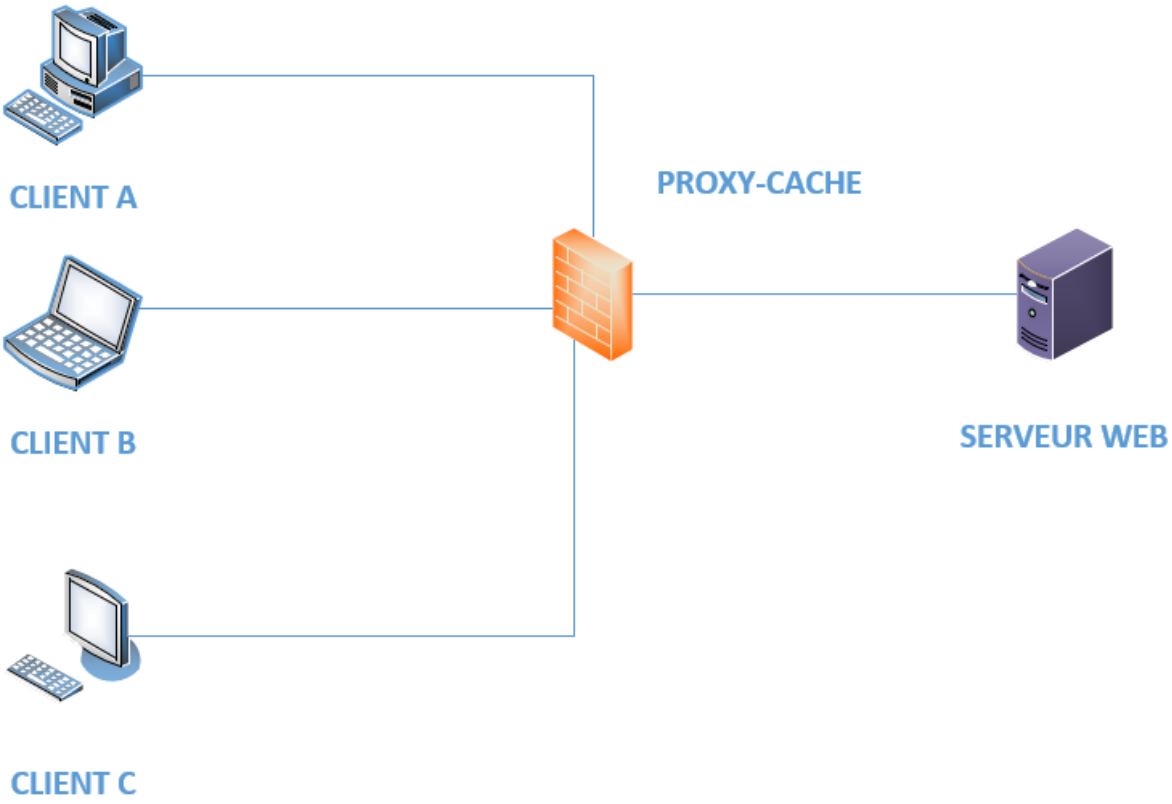
Dans le cas où un deuxième client consulte ces mêmes fichiers, ils seront disponibles dans le cache du proxy permettant ainsi **un accès plus rapide aux utilisateurs et un gain de bande passante** au niveau de la connexion Internet.

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 :

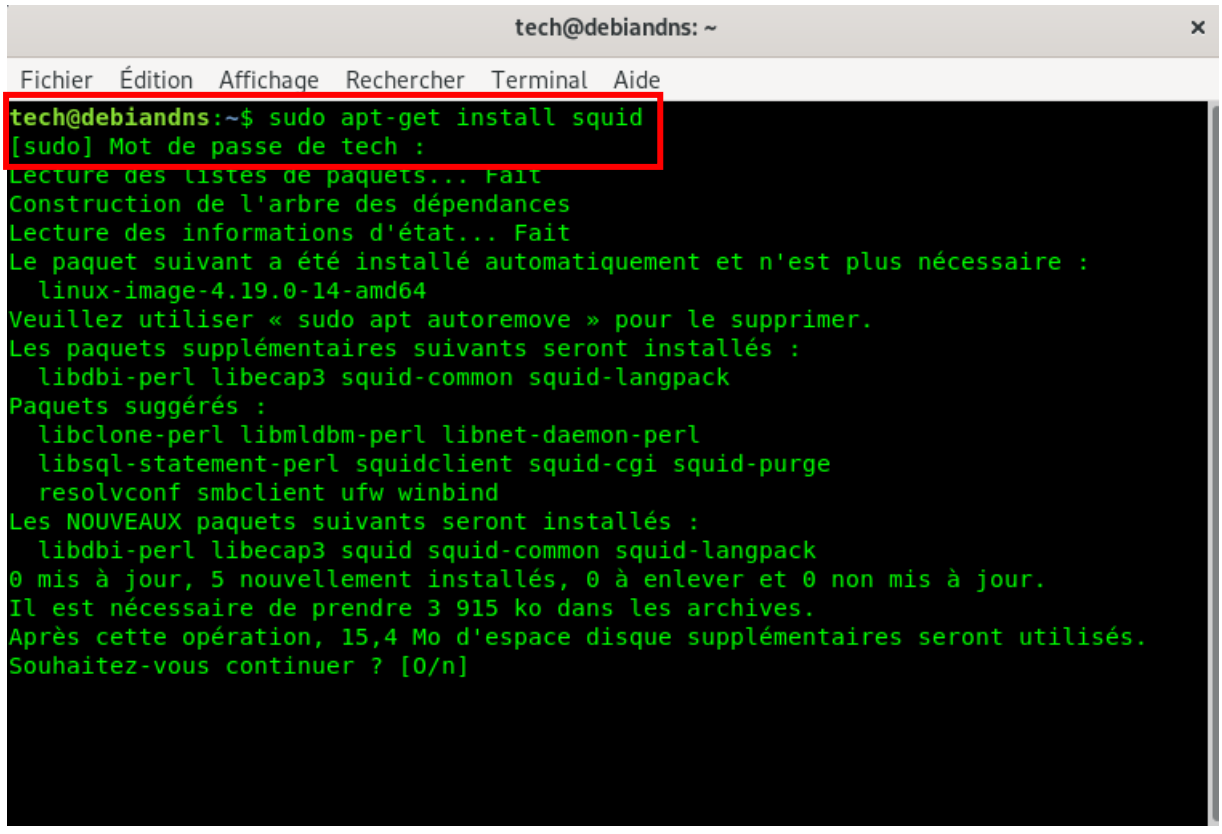
- **Utilisation optionnelle** : accès direct à Internet (mise en place pour améliorer les performances).
- **Utilisation obligatoire et explicite** : pour accéder à Internet, l'utilisateur doit passer à travers le proxy-cache (configuration manuelle du navigateur client).
- **Utilisation obligatoire 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 :

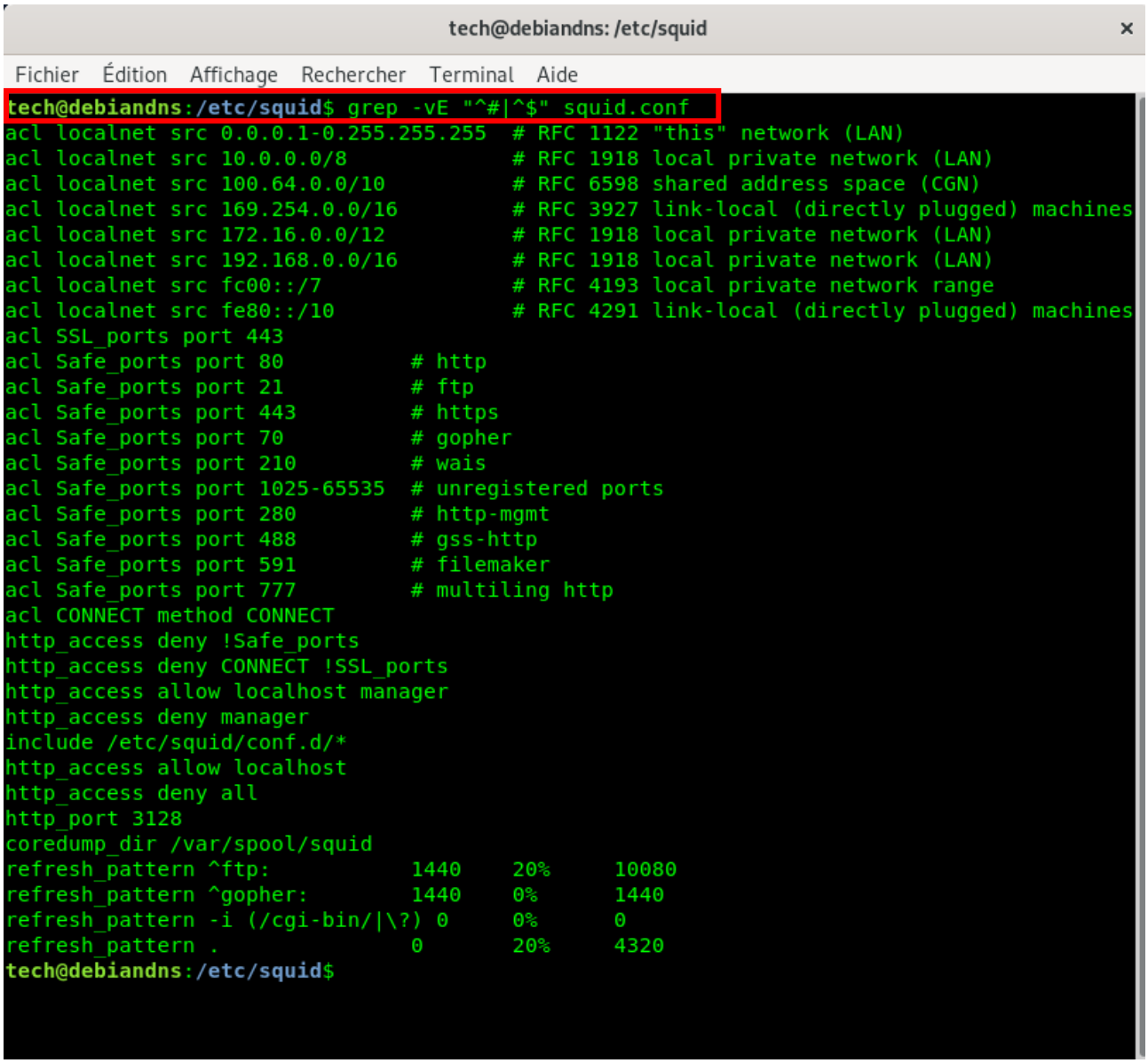
Installez le package squid à l'aide de la commande suivante : ***apt-get install squid***.



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.



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 2ème champ représente le nom de l'ACL, plusieurs directives avec le même nom vont cumuler les critères de chaque directive.
- le 3ème champ indique le type d'ACL, les plus importants sont src (source) , dst (destination), port et time.
- le 4ème 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).

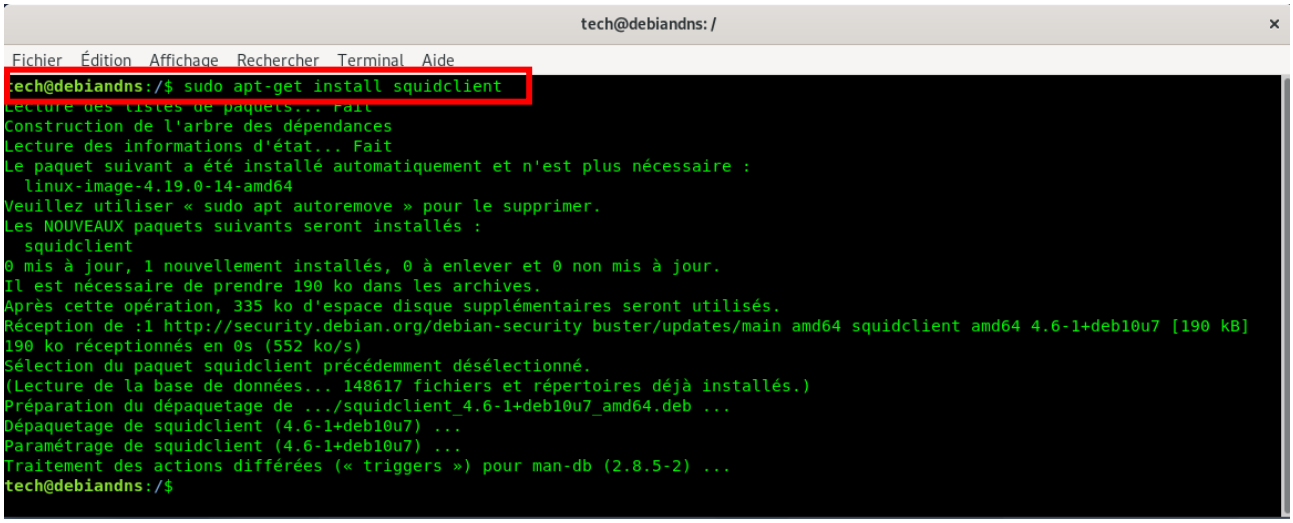
http_access deny !Safe_ports : cette directive interdit l'accès à tous les ports sauf les ports définis dans l'ACL **Safe_ports**.

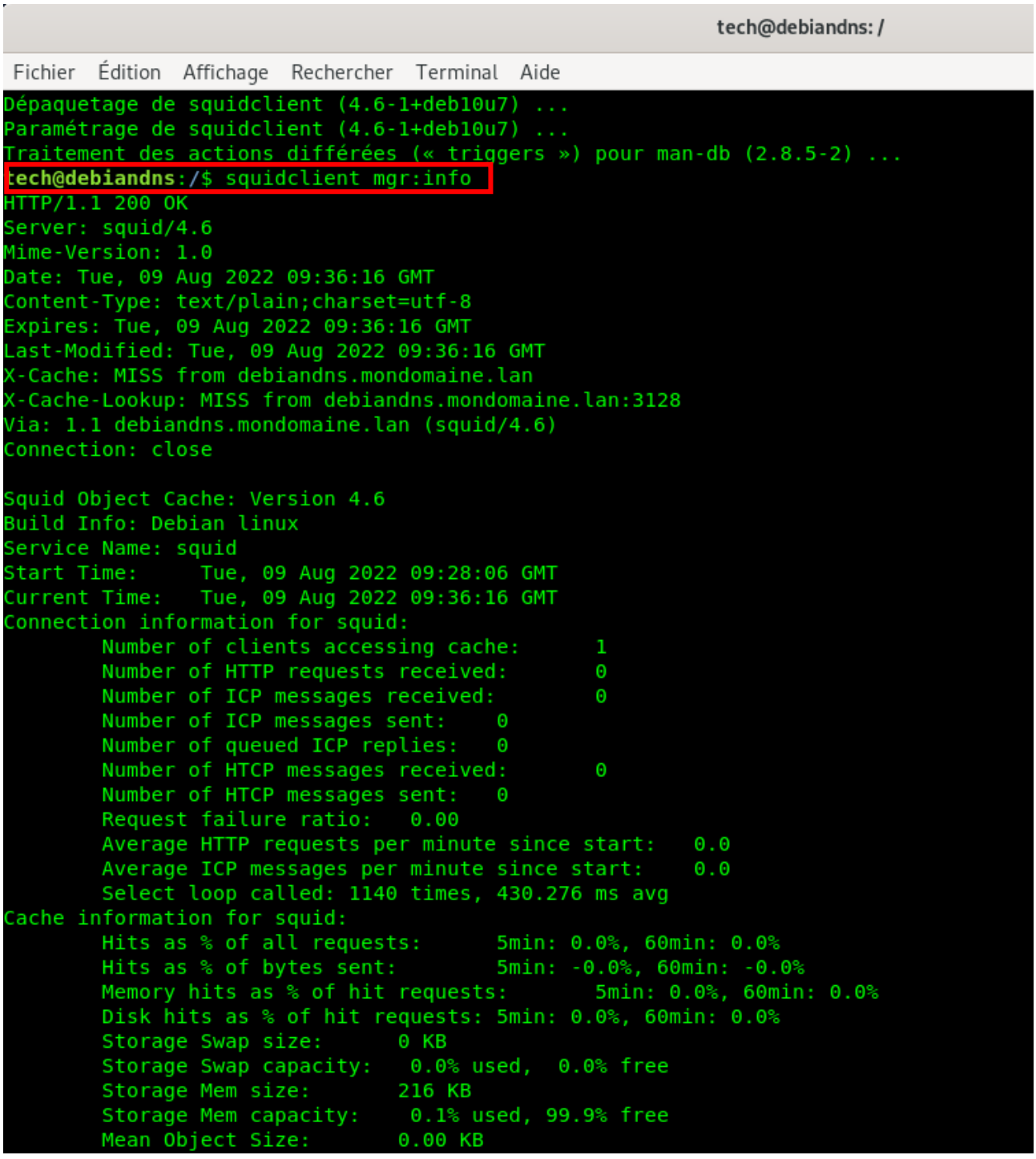
Les directives http_access sont lues dans l'ordre (séquentiel) et exécutées dès qu'une règle correspond à la directive.

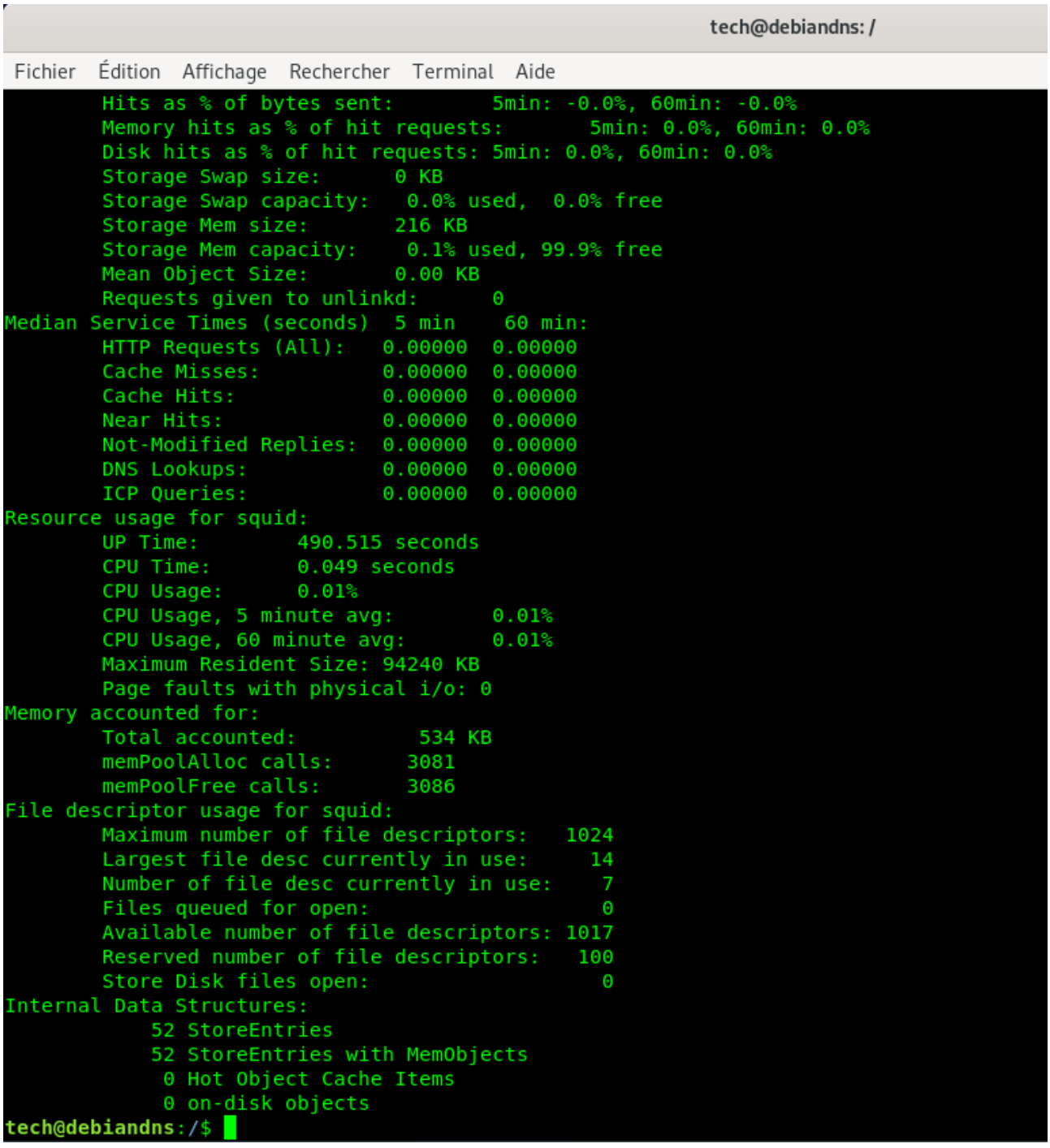
Il est recommandé de terminer toujours par **http_access deny all** afin d'interdire l'accès si aucune règle ne correspond à une directive.

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
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

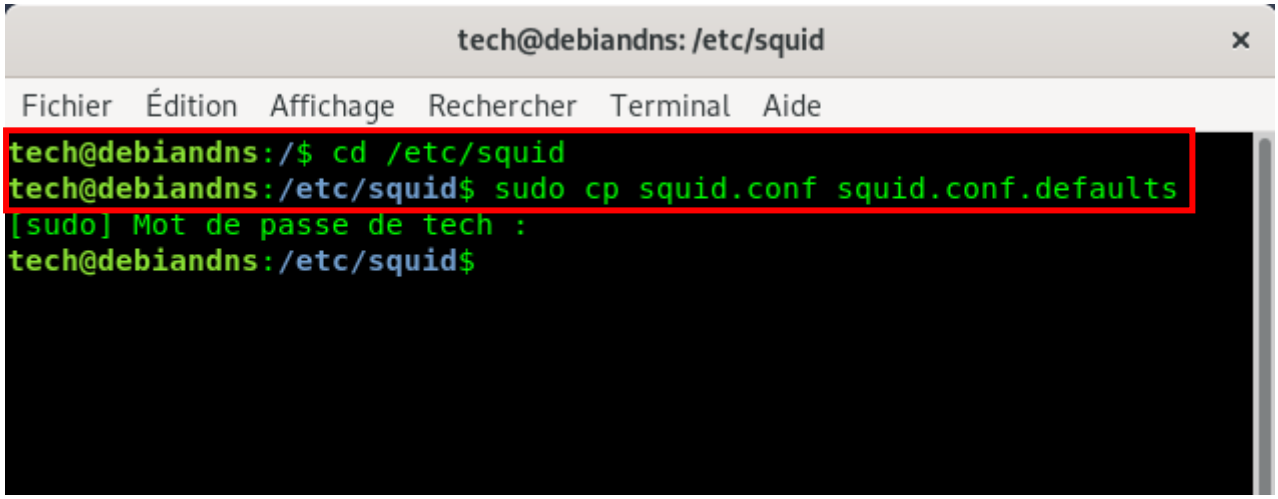

tech@debiandns: /
Fichier Édition Affichage Rechercher Terminal Aide
Hits as % of bytes sent: 5min: -0.0%, 60min: -0.0%
Memory hits as % of hit requests: 5min: 0.0%, 60min: 0.0%
Disk hits as % of hit requests: 5min: 0.0%, 60min: 0.0%
Storage Swap size: 0 KB
Storage Swap capacity: 0.0% used, 0.0% free
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 :

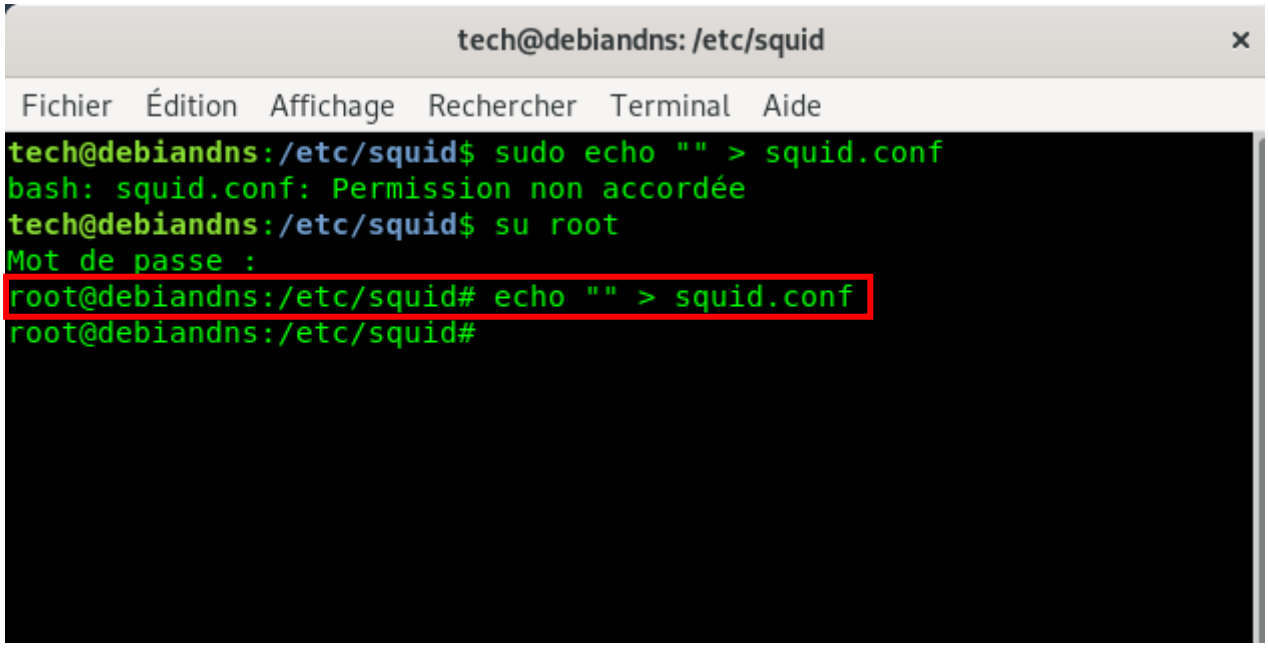
Dans le cadre du test du fonctionnement du proxy-cache squid, vous allez créer une politique de sécurité pour le réseau LAN :

- 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.

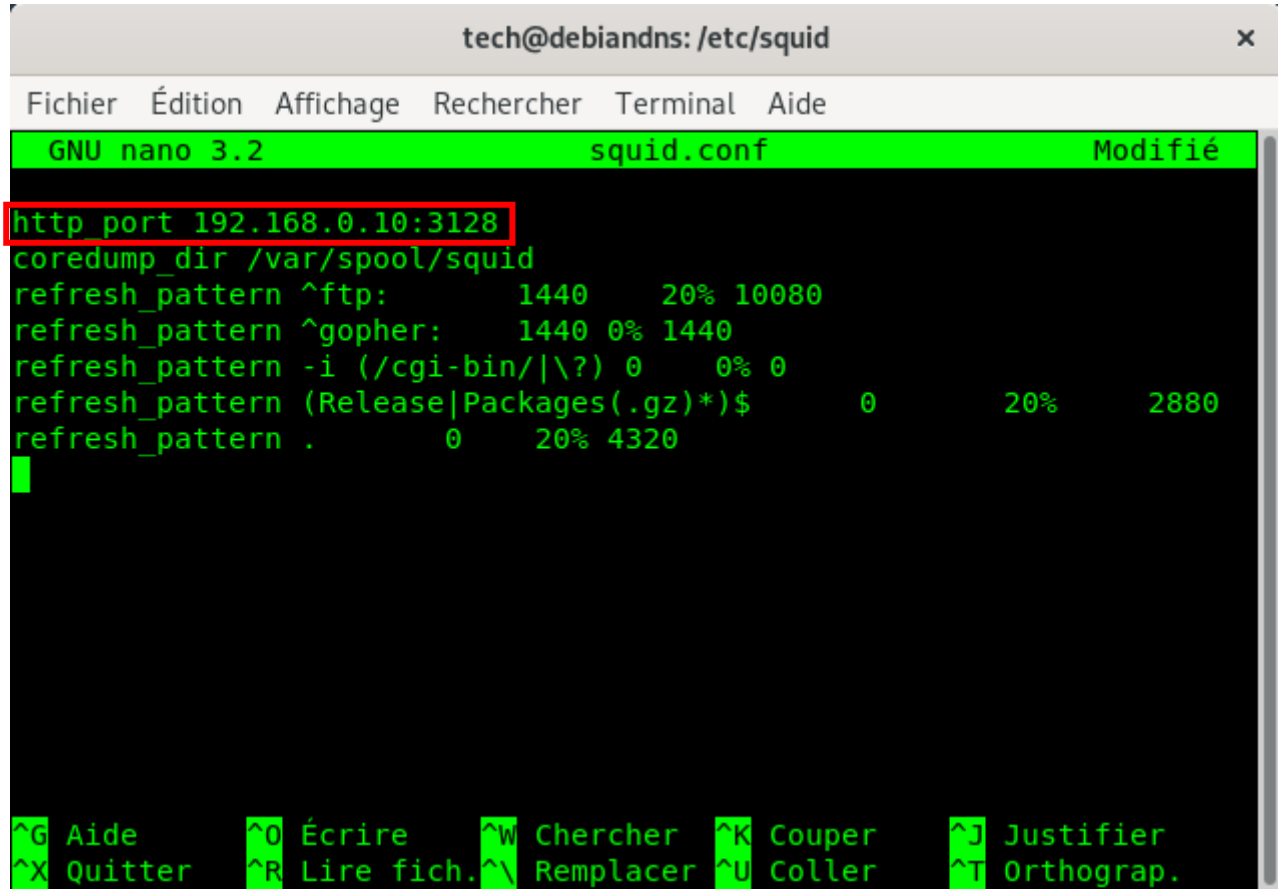
Sauvegardez la configuration par défaut du fichier **squid.conf** en cas de dysfonctionnement.



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



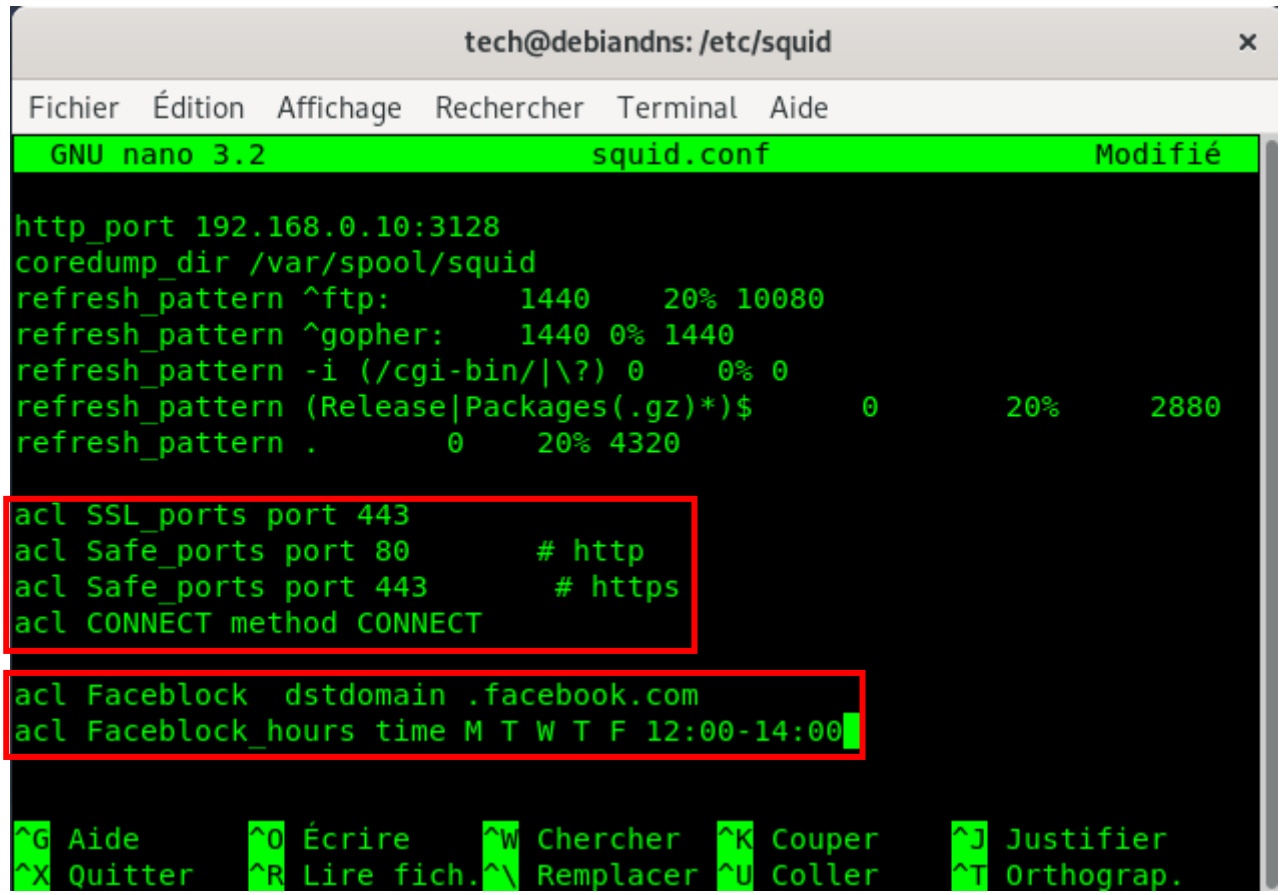
Editez le contenu du fichier squid.conf pour établir les directives.



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.

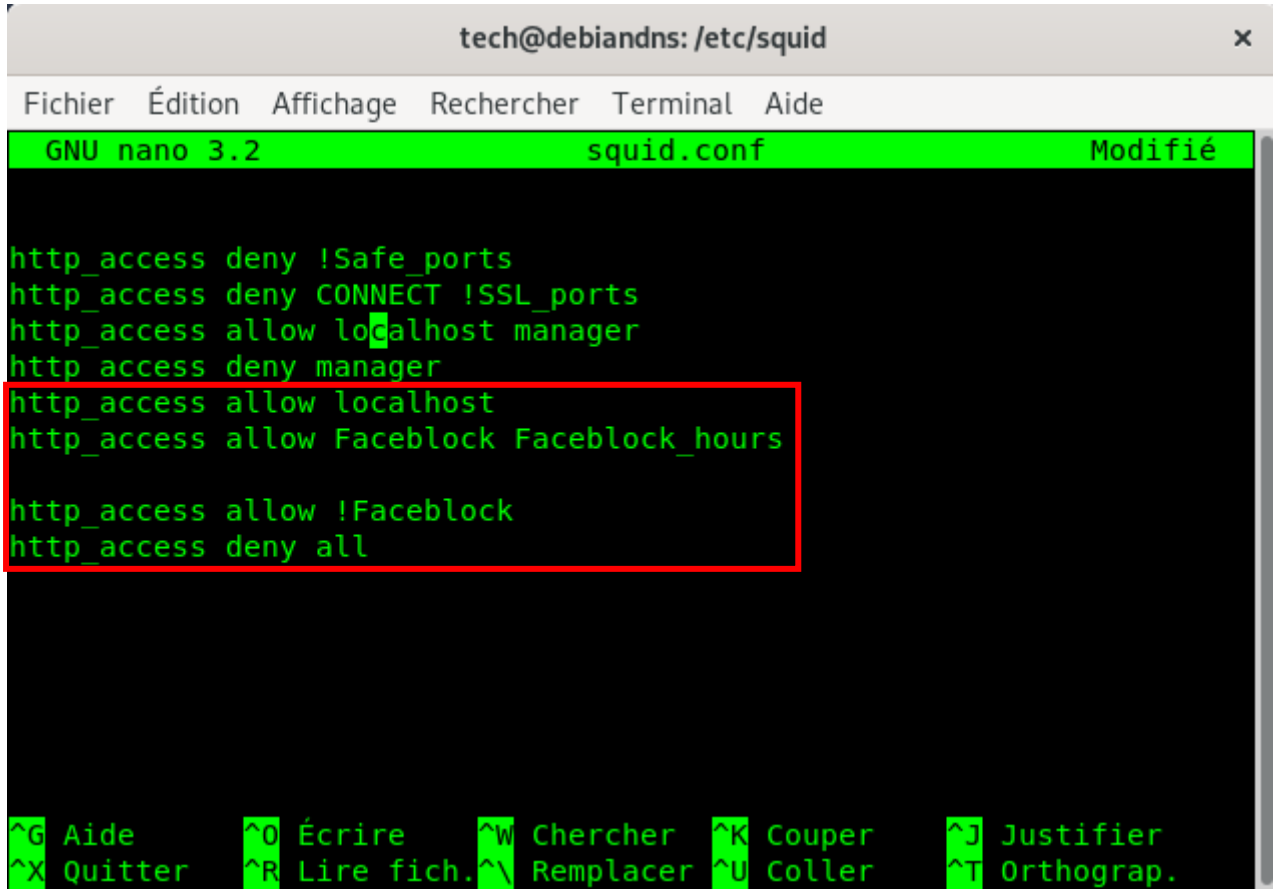


Ajoutez les directives permettant de filtrer l'accès au domaine de destination faceboook.com, le type **dstdomain** filtre le nom du domaine de destination.

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.

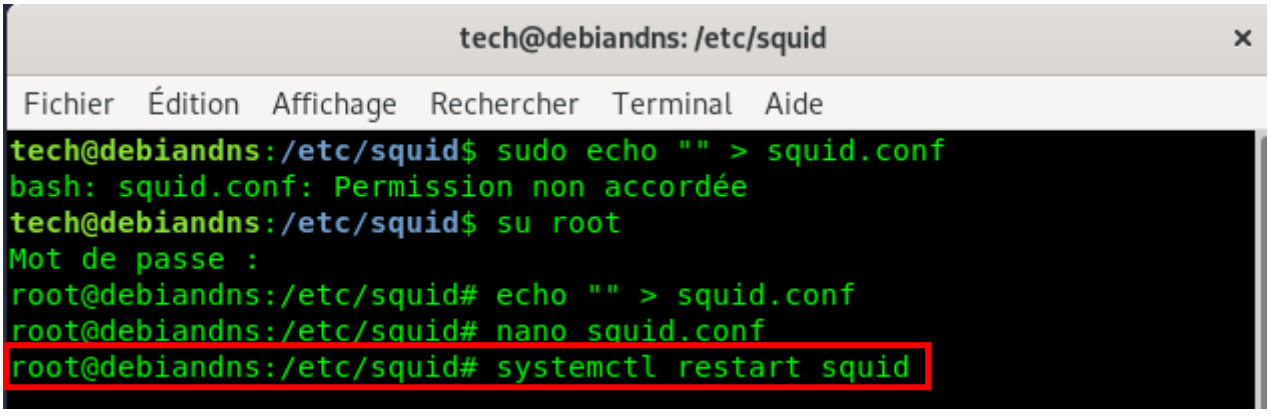


La directive http_access allow Faceblock Faceblock_hours contient deux ACL, les deux ACL doivent être vraies en même temps pour que la directive s'applique (ET logique).

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

Tous les autres accès sont interdits par la dernière directive.

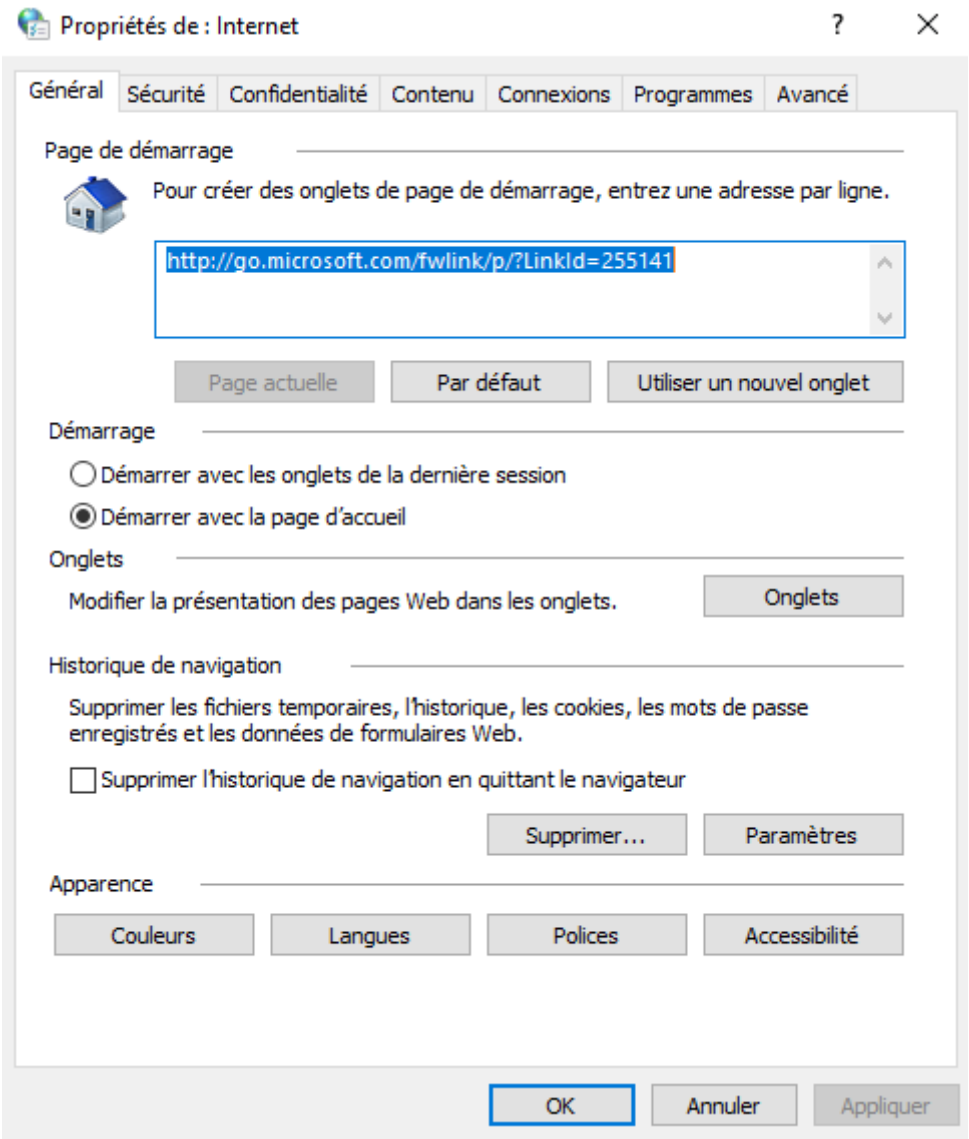
Enregistrez le fichier, puis redémarrez les services de squid.



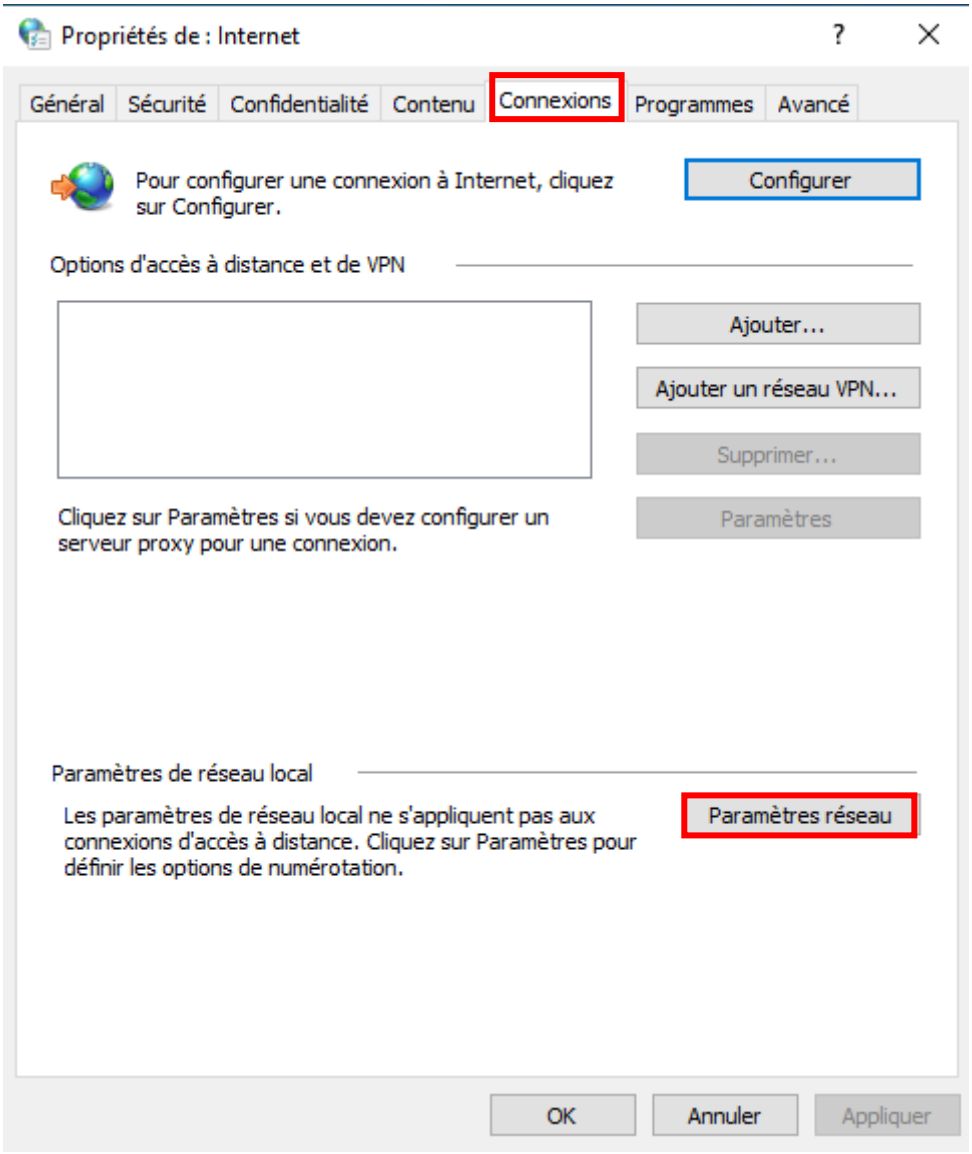
4.Test depuis un navigateur d'un poste client :

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.

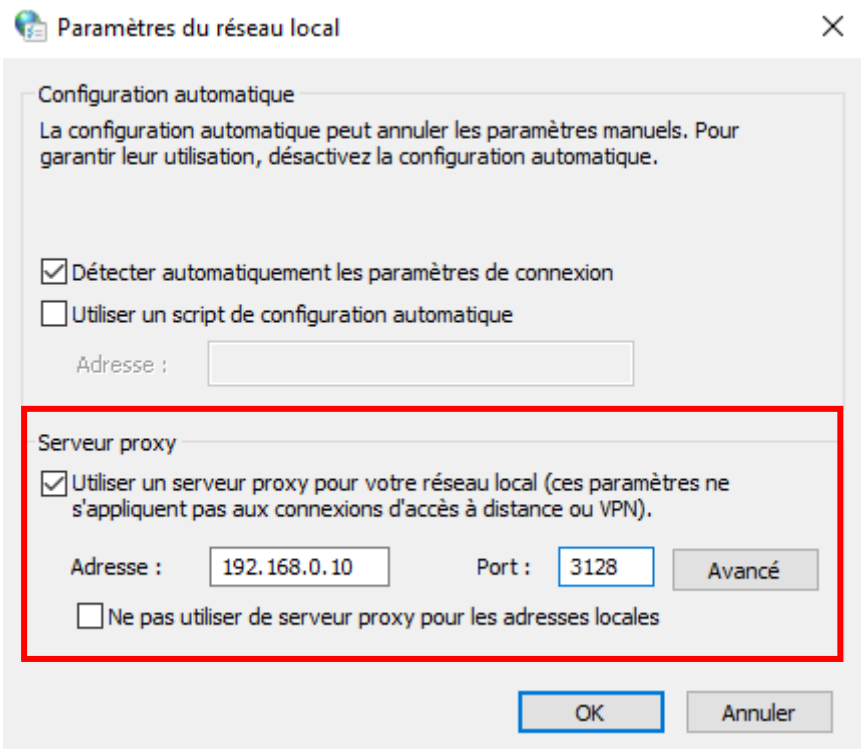
Accédez aux ***propriétés Internet*** pour un client sur Windows.

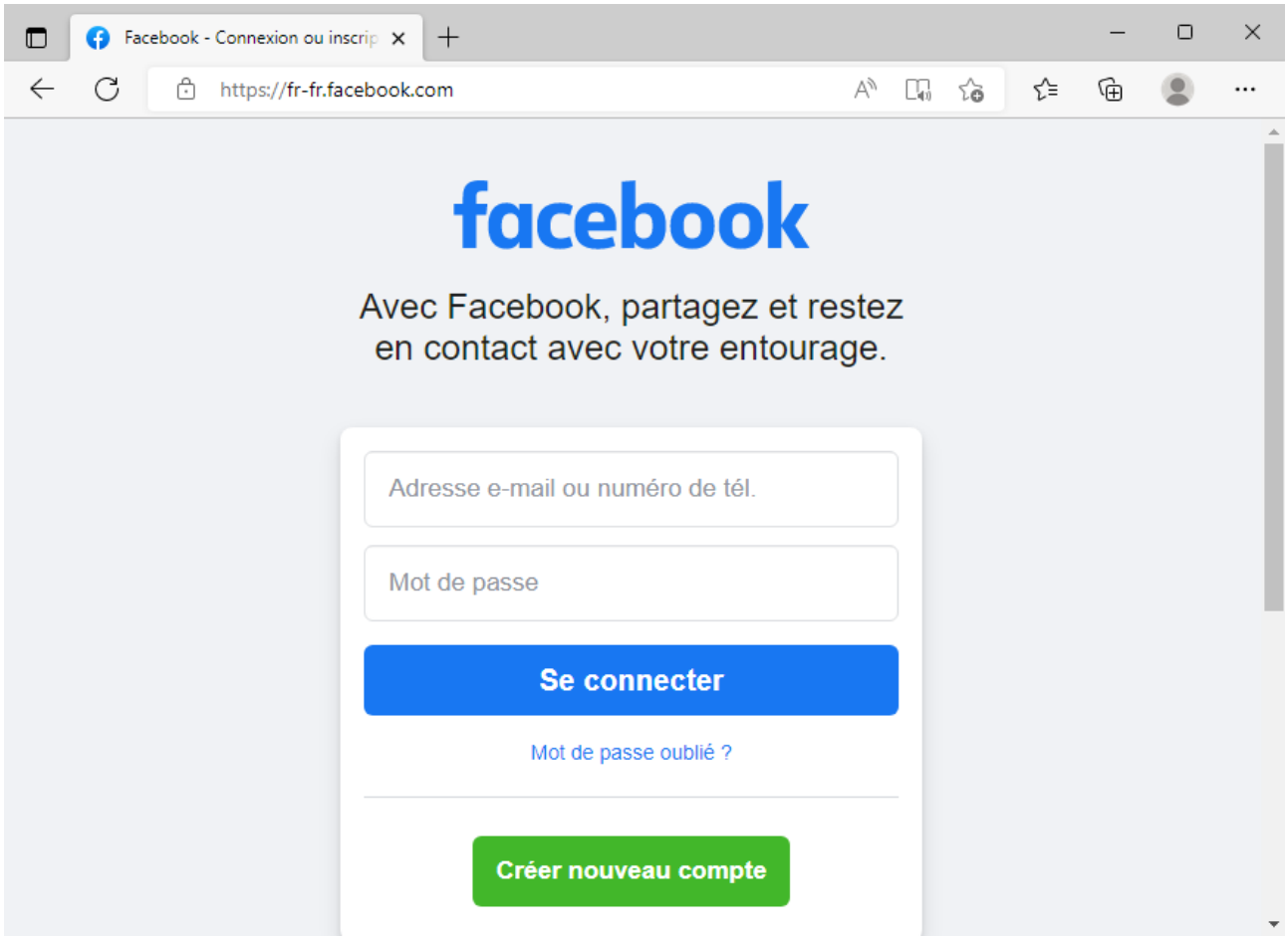


Affichez l'onglet Connexions, puis les paramètres réseau.



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.