# Mise en place d'un serveur Proxy Squid

## Qu'est ce qu'un Proxy

Un proxy, ou serveur mandataire, est un serveur qui agit comme intermédiaire pour les requêtes des clients cherchant à accéder à d'autres serveurs. En d'autres termes, un proxy reçoit les requêtes des clients (par exemple, des navigateurs web), les transmet aux serveurs appropriés, puis renvoie les réponses de ces serveurs aux clients. Cela peut offrir plusieurs avantages, notamment l'amélioration de la sécurité, le filtrage des contenus, l'accélération des accès grâce à la mise en cache, et l'anonymisation des requêtes pour protéger la vie privée des utilisateurs.

## Le choix du pare feu Squid

Le pare-feu UFW, pour "Uncomplicated Firewall", est une interface utilisateur simplifiée destinée à la gestion des iptables sur les systèmes basés sur Linux. UFW a été développé pour faciliter la configuration d'iptables, qui est puissant mais peut s'avérer complexe pour les utilisateurs peu expérimentés. Grâce à UFW, les administrateurs système et les utilisateurs peuvent configurer des règles de pare-feu de manière plus intuitive sans avoir à plonger dans les détails syntaxiques complexes d'iptables.

**Fonctionnalités principales d'UFW**

- **Simplicité d'utilisation :** UFW fournit une interface de ligne de commande simple pour la gestion des règles de pare-feu, rendant les tâches de sécurité réseau moins intimidantes pour les nouveaux utilisateurs.
- **Gestion de règles basées sur des politiques :** Permet aux administrateurs de définir facilement des règles qui contrôlent le trafic entrant, sortant et interne sur la base de ports spécifiques, d'applications, et de protocoles.
- **Support des profils d'application :** UFW permet la définition de profils pour des applications spécifiques, facilitant la configuration du pare-feu pour des services et des logiciels courants.

- **Logging :** Offre des capacités de journalisation pour surveiller et analyser les tentatives d'accès et les activités suspectes.
- **Intégration avec iptables :** Bien qu'UFW soit conçu pour être plus simple que la manipulation directe d'iptables, il se base sur iptables pour le filtrage du trafic, garantissant ainsi robustesse et fiabilité.

# Comment utiliser Proxy

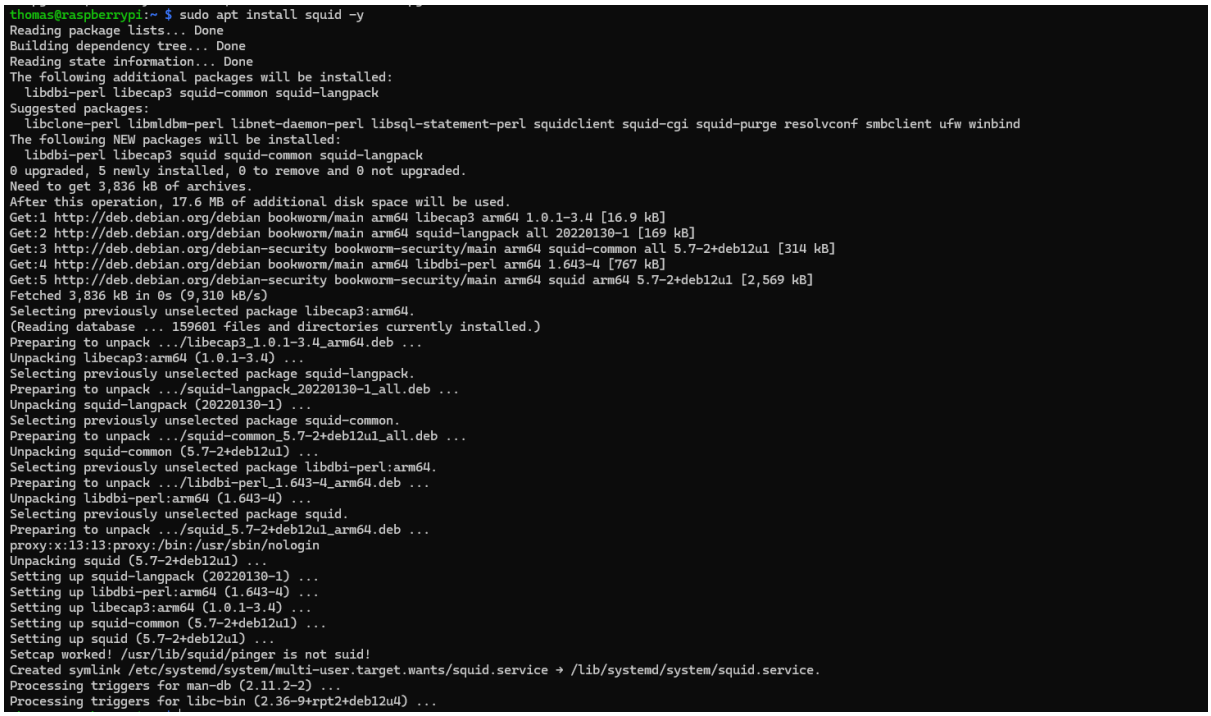
L'utilisation d'un proxy Squid dans votre réseau peut être configurée de manière à ce que les clients redirigent leurs requêtes web à travers le serveur proxy. Voici quelques étapes pour configurer et utiliser un proxy Squid :

**Configurer les Clients :** Sur les ordinateurs clients, configurez les paramètres de proxy dans le navigateur ou le système d'exploitation pour pointer vers l'adresse IP et le port du serveur Squid (par exemple, 192.168.1.100:3128).

**Configurer les Politiques de Contrôle d'Accès :** Dans le fichier de configuration de Squid (/etc/squid/squid.conf), vous pouvez définir des règles d'accès pour contrôler quels utilisateurs ou appareils peuvent utiliser le proxy.

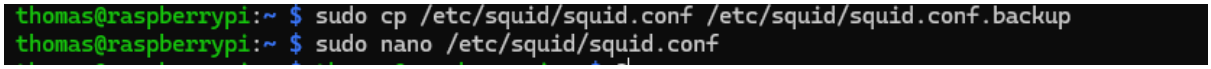
# Installation de Squid

- sudo apt install squid -y




# Configuration de Squid

- sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.backup
- sudo nano /etc/squid/squid.conf
- Il faut modifier le fichier pour parametrer le proxy



```
  GNU nano 7.2
#       WELCOME TO SQUID 5.7
#       ----------------------------
#
#       This is the documentation for the Squid configuration file.
#       This documentation can also be found online at:
#               http://www.squid-cache.org/Doc/config/
#
#       You may wish to look at the Squid home page and wiki for the
#       FAQ and other documentation:
#               http://www.squid-cache.org/
#               http://wiki.squid-cache.org/SquidFaq
#               http://wiki.squid-cache.org/ConfigExamples
#
#       This documentation shows what the defaults for various directives
#       happen to be.  If you don't need to change the default, you should
#       leave the line out of your squid.conf in most cases.
#
#       In some cases "none" refers to no default setting at all,
#       while in other cases it refers to the value of the option
#       - the comments for that keyword indicate if this is the case.
#

#  Configuration options can be included using the "include" directive.
#  Include takes a list of files to include. Quoting and wildcards are
#  supported.
#
#  For example,
#
#  include /path/to/included/file/squid.acl.config
#
#  Includes can be nested up to a hard-coded depth of 16 levels.
#  This arbitrary restriction is to prevent recursive include references
#  from causing Squid entering an infinite loop whilst trying to load
#  configuration files.
#
#  Values with byte units
#
#       Squid accepts size units on some size related directives. All
#       such directives are documented with a default value displaying
#       a unit.
#
#       Units accepted by Squid are:
#               bytes - byte
#               KB - Kilobyte (1024 bytes)
#               MB - Megabyte
#               GB - Gigabyte
#
```

.

- Choix du port utilisé

```
# Squid normally listens to port 3128
http_port 8888

#  TAG: https_port
#       Usage:  [ip:]port [mode] tls-cert=certificate.pem [options]
#
#       The socket address where Squid will listen for client requests made
#       over TLS or SSL connections. Commonly referred to as HTTPS.
#
#       This is most useful for situations where you are running squid in
#       accelerator mode and you want to do the TLS work at the accelerator
#       level.
#
#       You may specify multiple socket addresses on multiple lines,
#       each with their own certificate and/or options.
#
#       The tls-cert= option is mandatory on HTTPS ports.
#
#       See http_port for a list of modes and options.
#Default:
# none
```

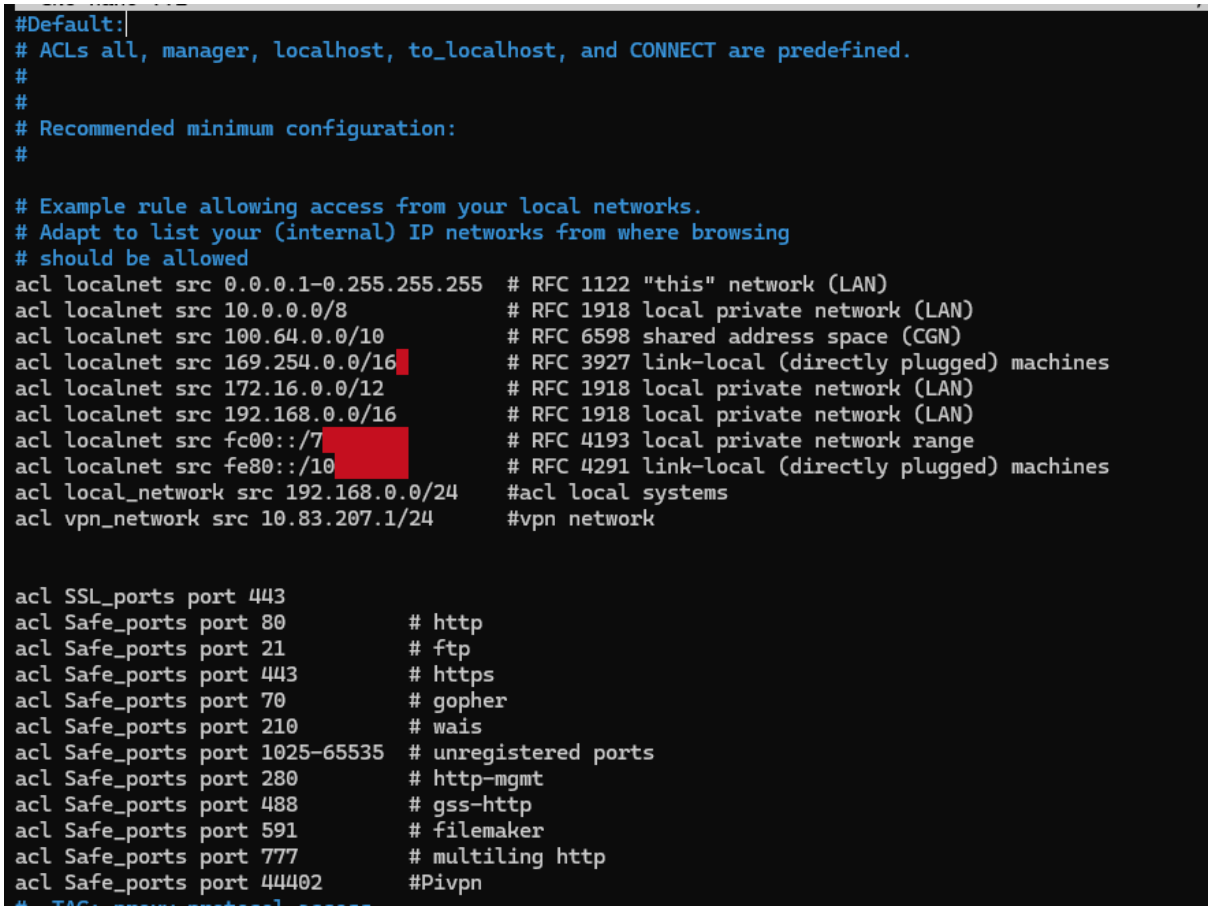

```
# Squid normally listens to port 3128
http_port 8888

#  TAG: https_port
#       Usage:  [ip:]port [mode] tls-cert=certificate.pem [options]
#
#       The socket address where Squid will listen for client requests made
#       over TLS or SSL connections. Commonly referred to as HTTPS.
#
#       This is most useful for situations where you are running squid in
#       accelerator mode and you want to do the TLS work at the accelerator
#       level.
#
#       You may specify multiple socket addresses on multiple lines,
#       each with their own certificate and/or options.
#
#       The tls-cert= option is mandatory on HTTPS ports.
#
#       See http_port for a list of modes and options.
#Default:
# none
```


- Etablissement des règles ACL
- On commence à les chercher

```
#       the cache_dir with most availabl
#
#       When a mix of cache_dir sizes ar
#       have a naturally lower I/O loadi
Search [tag acl:]: TAG: acl
^G Help
^C Cancel
```

- On indique les reseaux voulu
- Et les port qu'on veut inclure



```
#Default:
# ACLs all, manager, localhost, to_localhost, and CONNECT 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 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 local_network src 192.168.0.0/24    #acl local systems
acl vpn_network src 10.83.207.1/24      #vpn 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 Safe_ports port 44402       #Pivpn
```

- On indique les règles de permission ou de refus

```
#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

#Permettre l'accès localhost et mon lan à internet
http_access allow localhost
http_access allow local_network
http_access allow vpn_network


#Après bloquer le reste#

http_access deny all
```

- Modification de la mémoire cache

```
#Default:
 cache_mem 256 MB
```

```
#Default:
 cache_mem 512 MB
```

```
# Squid normally listens to port 3128
http_port 3128
```

```
# Squid normally listens to port 3128
http_port 8888
```

- On ajoute le serveur DNS

```
#
# Spécifier la liste des serveurs DNS à utiliser :
dns_nameservers 10.0.0.1 192.172.0.4
#Default:
```

```
thomas@raspberrypi:~ $ sudo /usr/sbin/squid -k check
thomas@raspberrypi:~ $ sudo /usr/sbin/squid -k pars
2024/03/23 01:20:03| Startup: Initializing Authentication Schemes ...
2024/03/23 01:20:03| Startup: Initialized Authentication Scheme 'basic'
2024/03/23 01:20:03| Startup: Initialized Authentication Scheme 'digest'
2024/03/23 01:20:03| Startup: Initialized Authentication Scheme 'negotiate'
2024/03/23 01:20:03| Startup: Initialized Authentication Scheme 'ntlm'
2024/03/23 01:20:03| Startup: Initialized Authentication.
2024/03/23 01:20:03| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2024/03/23 01:20:03| Processing: acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
2024/03/23 01:20:03| Processing: acl localnet src 10.0.0.0/8           # RFC 1918 local private network (LAN)
2024/03/23 01:20:03| Processing: acl localnet src 100.64.0.0/10        # RFC 6598 shared address space (CGN)
2024/03/23 01:20:03| Processing: acl localnet src 169.254.0.0/16       # RFC 3927 link-local (directly plugged) machines
2024/03/23 01:20:03| Processing: acl localnet src 172.16.0.0/12        # RFC 1918 local private network (LAN)
2024/03/23 01:20:03| Processing: acl localnet src 192.168.0.0/16              # RFC 1918 local private network (LAN)
2024/03/23 01:20:03| Processing: acl localnet src fc00::/7             # RFC 4193 local private network range
2024/03/23 01:20:03| Processing: acl localnet src fe80::/10            # RFC 4291 link-local (directly plugged) machines
2024/03/23 01:20:03| Processing: acl local_network src 192.168.0.0/24    #acl local systems
2024/03/23 01:20:03| Processing: acl vpn_network src 10.83.207.1               #vpn network
2024/03/23 01:20:03| Processing: acl SSL_ports port 443
2024/03/23 01:20:03| Processing: acl Safe_ports port 80         # http
2024/03/23 01:20:03| Processing: acl Safe_ports port 21         # ftp
2024/03/23 01:20:03| Processing: acl Safe_ports port 443                # https
2024/03/23 01:20:03| Processing: acl Safe_ports port 70         # gopher
2024/03/23 01:20:03| Processing: acl Safe_ports port 210                # wais
2024/03/23 01:20:03| Processing: acl Safe_ports port 1025-65535 # unregistered ports
2024/03/23 01:20:03| Processing: acl Safe_ports port 280                # http-mgmt
2024/03/23 01:20:03| Processing: acl Safe_ports port 488                # gss-http
2024/03/23 01:20:03| Processing: acl Safe_ports port 591                # filemaker
2024/03/23 01:20:03| Processing: acl Safe_ports port 777                # multiling http
2024/03/23 01:20:03| Processing: acl Safe_ports port 44402      #Pivpn
2024/03/23 01:20:03| Processing: http_access deny !Safe_ports
2024/03/23 01:20:03| Processing: http_access deny CONNECT !SSL_ports
2024/03/23 01:20:03| Processing: http_access allow localhost manager
2024/03/23 01:20:03| Processing: http_access deny manager
2024/03/23 01:20:03| Processing: http_access allow localhost
2024/03/23 01:20:03| Processing: http_access allow local_network
2024/03/23 01:20:03| Processing: http_access allow vpn_network
2024/03/23 01:20:03| Processing: http_access deny all
2024/03/23 01:20:03| Processing: include /etc/squid/conf.d/*.conf
2024/03/23 01:20:03| Processing Configuration File: /etc/squid/conf.d/debian.conf (depth 1)
2024/03/23 01:20:03| Processing: logfile_rotate 0
2024/03/23 01:20:03| Processing: http_access allow localhost
```

```
thomas@raspberrypi:~ $ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-03-22 23:07:21 CET; 1s ago
       Docs: man:squid(8)
    Process: 2462 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
   Main PID: 2465 (squid)
      Tasks: 5 (limit: 9248)
        CPU: 199ms
     CGroup: /system.slice/squid.service
             ├─2465 /usr/sbin/squid --foreground -sYC
             ├─2467 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─2468 "(logfile-daemon)" /var/log/squid/access.log
             ├─2469 "(unlinkd)"
             └─2470 "(pinger)"

Mar 22 23:07:21 raspberrypi squid[2467]:         0 Objects expired.
Mar 22 23:07:21 raspberrypi squid[2467]:         0 Objects cancelled.
Mar 22 23:07:21 raspberrypi squid[2467]:         0 Duplicate URLs purged.
Mar 22 23:07:21 raspberrypi squid[2467]:         0 Swapfile clashes avoided.
Mar 22 23:07:21 raspberrypi squid[2467]:   Took 0.04 seconds (  0.00 objects/sec).
Mar 22 23:07:21 raspberrypi squid[2467]: Beginning Validation Procedure
Mar 22 23:07:21 raspberrypi squid[2467]:   Completed Validation Procedure
Mar 22 23:07:21 raspberrypi squid[2467]:   Validated 0 Entries
Mar 22 23:07:21 raspberrypi squid[2467]:   store_swap_size = 0.00 KB
Mar 22 23:07:22 raspberrypi squid[2467]: storeLateRelease: released 0 objects
```

Pour consulter les logs

- sudo tail /var/log/squid/access.log

https://www.youtube.com/watch?v=qcXO93wgSQk