

Mise en place d'un proxy filtrant transparent avec Squid

- [Préparation du système et du réseau](#)
 - [Ligne de commande](#)
 - [Capture d'écran](#)
- [Activation du routage](#)
 - [Ligne de commande](#)
 - [Capture d'écran](#)
- [Config du Pare-feu \(nftables\)](#)
 - [Lignes de commande](#)
 - [Capture d'écran](#)
- [Mise en place du filtrage automatisé \(liste noires\)](#)
 - [Création du script de mise à jour](#)
 - [Ligne de commande](#)
 - [Capture d'écran](#)
- [Planification avec cron](#)
 - [Ligne de commande](#)
- [Config de Squid](#)
 - [Lignes de commandes](#)
 - [Capture d'écran](#)
- [Configuration des postes clients](#)
 - [Sur un poste Linux](#)
 - [Lignes de commande](#)
 - [Sur un poste Windows](#)

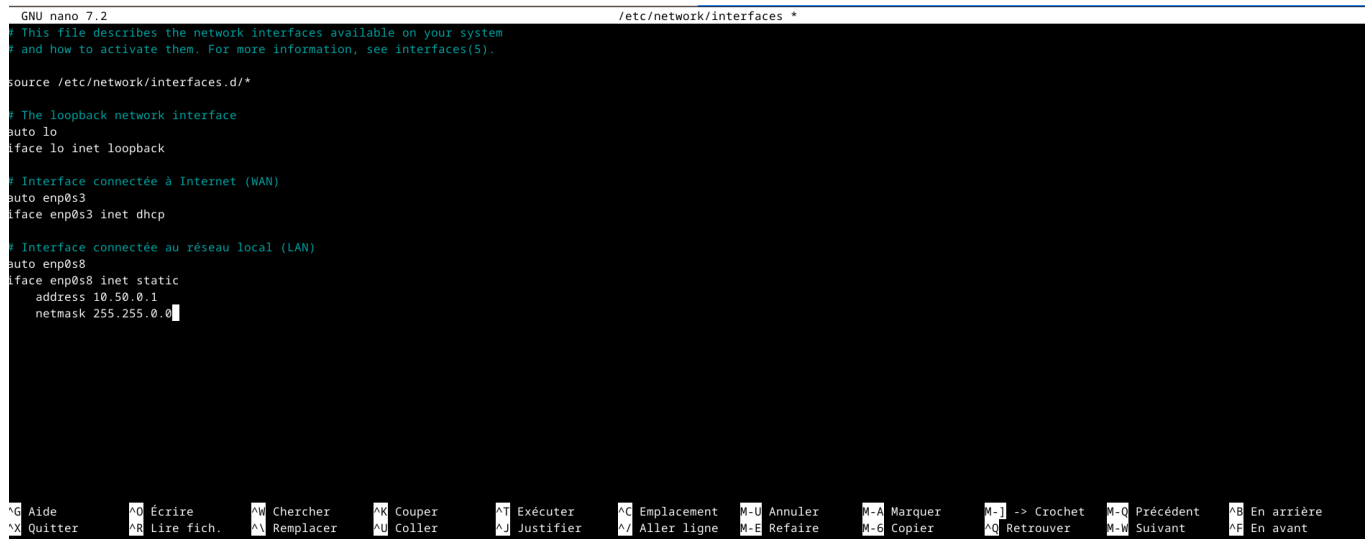
Préparation du système et du réseau

Ligne de commande

```
# Mise à jour des paquets et installation de Squid et nftables
sudo apt update && sudo apt install squid nftables
#Modifier le fichier de config des interfaces réseau
sudo nano /etc/network/interfaces
#config comme ca
auto lo iface lo inet loopback
# Interface connectée à Internet (WAN) auto enp0s3 iface enp0s3 inet dhcp #
Interface connectée au réseau local (LAN) auto enp0s8 iface enp0s8 inet static
address 10.50.0.1 netmask 255.255.0.0
```

```
#appliquer les changements
sudo systemctl restart networking.service
```

Capture d'écran

A screenshot of a terminal window with a black background and white text. The title bar at the top shows 'GNU nano 7.2' on the left and '/etc/network/interfaces *' on the right. The terminal content shows the configuration of network interfaces. It starts with a comment about the file's purpose, followed by 'source /etc/network/interfaces.d/*'. Then, it defines the loopback interface 'lo' with 'auto lo' and 'iface lo inet loopback'. Next, it defines the WAN interface 'enp0s3' with 'auto enp0s3' and 'iface enp0s3 inet dhcp'. Finally, it defines the LAN interface 'enp0s8' with 'auto enp0s8', 'iface enp0s8 inet static', 'address 10.50.0.1', and 'netmask 255.255.0.0'. At the bottom of the terminal, there is a horizontal bar containing various keyboard shortcuts for nano, such as 'Aide', 'Quitter', 'Écrire', 'Lire fich.', 'Chercher', 'Remplacer', 'Couper', 'Coller', 'Exécuter', 'Justifier', 'Emplacement', 'Aller ligne', 'Annuler', 'Refaire', 'Marquer', 'Copier', 'Retrouver', 'Précédent', 'Suivant', 'En arrière', and 'En avant'.

Activation du routage

Ligne de commande

```
# mod un files de configuration
sudo pluma /etc/sysctl.conf
#Décommenter la ligne
net.ipv4.ip_forward=1
#appliquer la modification sans redémarré
sudo sysctl -p
```

Capture d'écran

sysctl.conf (/etc) - Pluma

Fichier Édition Affichage Recherche Outils Documents Aide

Ouvrir Enregistrer Annuler

sysctl.conf

```
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

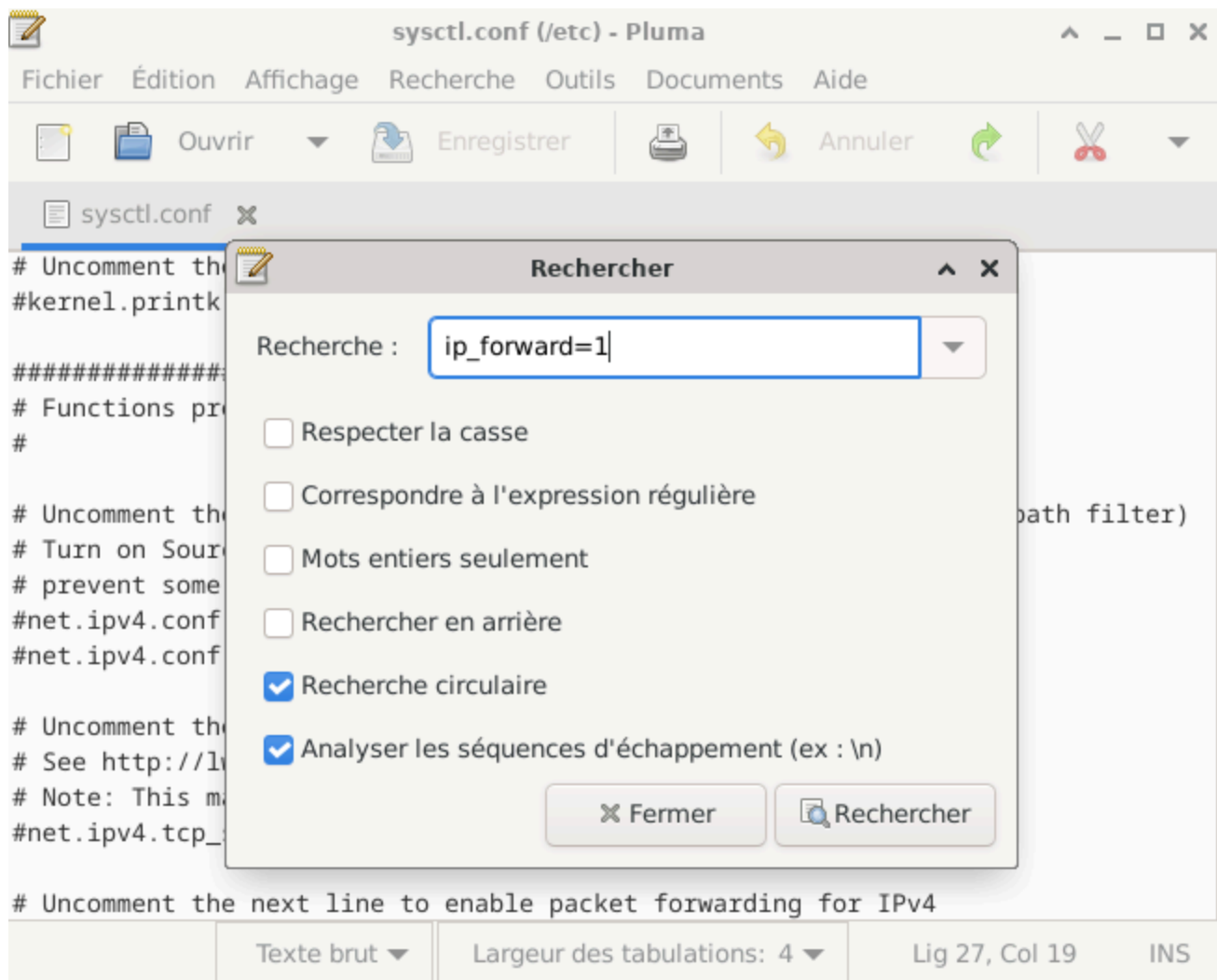
#kernel.domainname = example.com

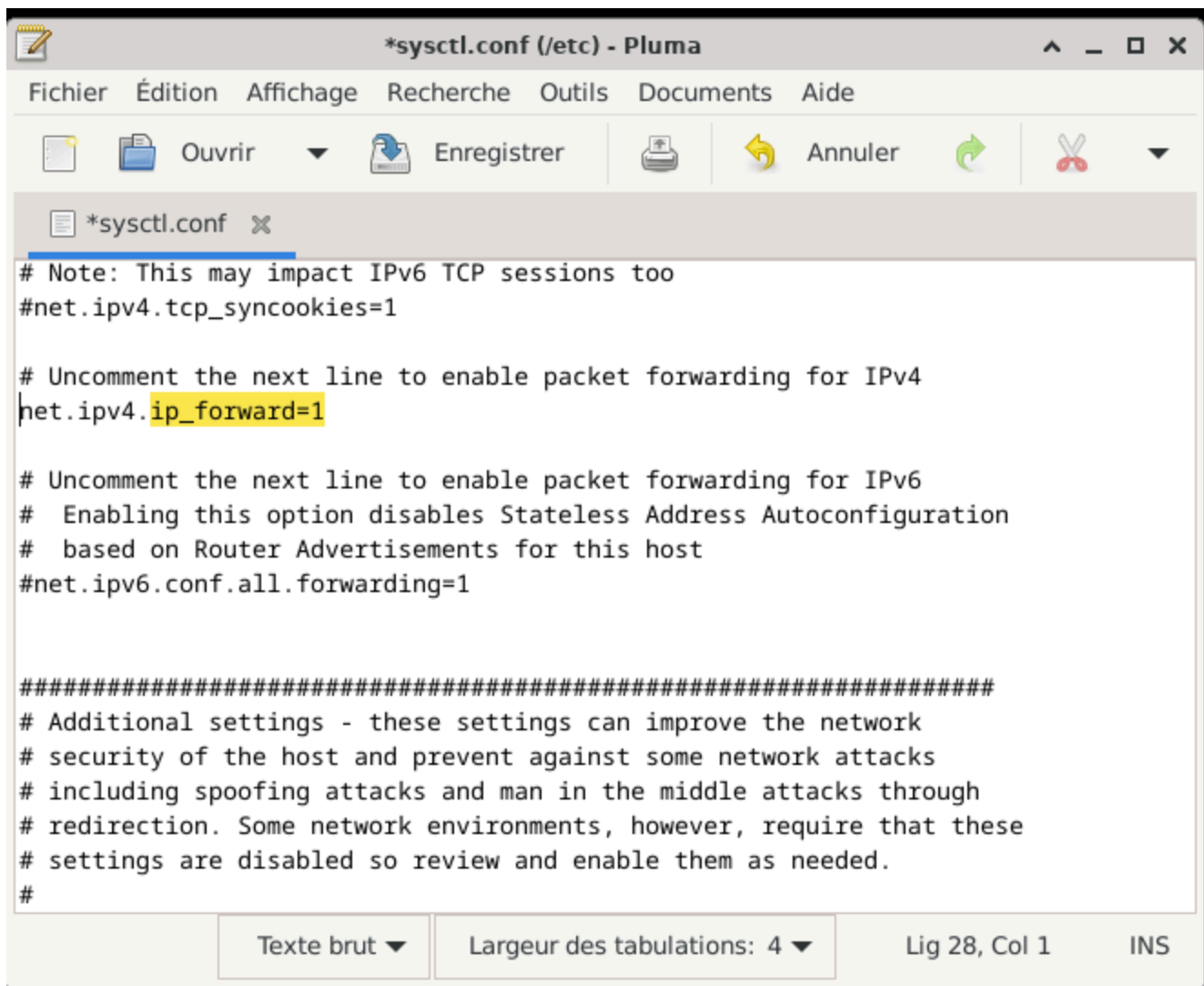
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
|
```

Texte brut ▼ Largeur des tabulations: 4 ▼ Lig 21, Col 1 INS





```
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
```

Config du Pare-feu (nftables)

Lignes de commande

```
#rentrer dans le fichier de config du pare-feu
sudo nano /etc/nftables.conf
#Remplacer son contenu par
#!/usr/sbin/nft -f flush ruleset table inet filter { chain input { type filter
hook input priority 0; policy drop; # Accepter le trafic de la boucle locale
iifname "lo" accept # Accepter les requêtes DHCP et DNS venant du LAN iifname
"enp0s8" udp dport {67, 53} accept iifname "enp0s8" tcp dport 53 accept #
Accepter le trafic déjà établi ct state { established, related } accept }
chain forward { type filter hook forward priority 0; policy accept; #
Autoriser le trafic du LAN vers le WAN à condition qu'il soit "natté" iif
"enp0s8" oif "enp0s3" accept # Accepter le trafic déjà établi ct state {
established, related } accept } chain output { type filter hook output
priority 0; policy accept; } } table nat { chain prerouting { type nat hook
prerouting priority -100; # Rediriger le trafic HTTP (port 80) vers le port de
Squid 3129 iifname "enp0s8" tcp dport 80 redirect to :3129 # Rediriger le
```

```
trafic HTTPS (port 443) vers le port de Squid 3130 iifname "enp0s8" tcp dport
443 redirect to :3130 } chain postrouting { type nat hook postrouting priority
100; # Masquer le trafic sortant du LAN derrière l'IP du WAN oifname "enp0s3"
masquerade } }
```

```
#Activer le service
```

```
sudo systemctl enable nftables.service
```

```
#Appliquer les nouvelles règles
```

```
sudo systemctl restart nftables.service
```

Capture d'écran

```

GNU nano 2.2 /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;

        # Accepter le trafic de la boucle locale
        iifname "lo" accept

        # Accepter les requêtes DHCP et DNS venant du LAN
        iifname "enp0s8" udp dport {67, 53} accept
        iifname "enp0s8" tcp dport 53 accept

        # Accepter le trafic déjà établi
        ct state { established, related } accept
    }

    chain forward {
        type filter hook forward priority 0; policy accept;
        # Autoriser le trafic du LAN vers le WAN à condition qu'il soit "natté"
        iif "enp0s8" oif "enp0s3" accept
        # Accepter le trafic déjà établi
        ct state { established, related } accept
    }
}

table nat {
    chain prerouting {
        type nat hook prerouting priority -100;

        # Rediriger le trafic HTTP (port 80) vers le port de Squid 3129
        iifname "enp0s8" tcp dport 80 redirect to :3129

        # Rediriger le trafic HTTPS (port 443) vers le port de Squid 3130
        iifname "enp0s8" tcp dport 443 redirect to :3130
    }

    chain postrouting {
        type nat hook postrouting priority 100;
        # Masquer le trafic sortant du LAN derrière l'IP du WAN
        oifname "enp0s3" masquerade
    }
}

```

Mise en place du filtrage automatisé (liste noires)

Création du script de mise à jour

Ligne de commande

```

#création du répertoire où sera mis les blacklists
sudo mkdir /etc/squid/blacklist
#permissions

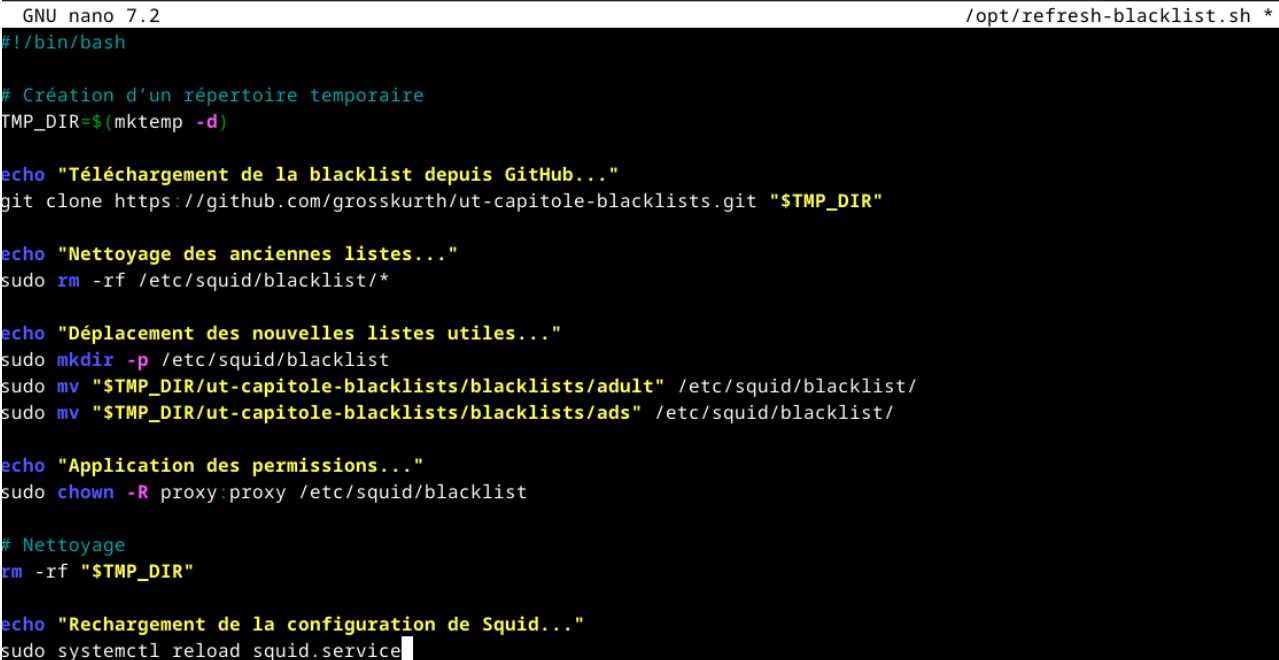
```

```
sudo chown -R proxy:proxy /etc/squid/blacklist
#création du script
sudo nano /opt/refresh-blacklist.sh

#!/bin/bash # Création d'un répertoire temporaire TMP_DIR=$(mktemp -d) echo
"Téléchargement de la blacklist depuis GitHub..." git clone
https://github.com/grosskurth/ut-capitole-blacklists.git "$TMP_DIR" echo
"Nettoyage des anciennes listes..." sudo rm -rf /etc/squid/blacklist/* echo
"Déplacement des nouvelles listes utiles..." sudo mkdir -p
/etc/squid/blacklist sudo mv "$TMP_DIR/ut-capitole-
blacklists/blacklists/adult" /etc/squid/blacklist/ sudo mv "$TMP_DIR/ut-
capitole-blacklists/blacklists/ads" /etc/squid/blacklist/ echo "Application
des permissions..." sudo chown -R proxy:proxy /etc/squid/blacklist # Nettoyage
rm -rf "$TMP_DIR" echo "Rechargement de la configuration de Squid..." sudo
systemctl reload squid.service

#installation de git
sudo apt install git -y
#rendre le script exécutable
sudo chmod +x /opt/refresh-blacklist.sh
```

Capture d'écran



The screenshot shows a terminal window with the title bar "GNU nano 7.2" and the file path "/opt/refresh-blacklist.sh *". The script content is displayed in a monospaced font with syntax highlighting. The script performs the following actions: creates a temporary directory, clones a GitHub repository, removes old blacklists, moves new ones to /etc/squid/blacklist, sets permissions, cleans up the temporary directory, and reloads the squid.service.

```
GNU nano 7.2 /opt/refresh-blacklist.sh *
#!/bin/bash

# Création d'un répertoire temporaire
TMP_DIR=$(mktemp -d)

echo "Téléchargement de la blacklist depuis GitHub..."
git clone https://github.com/grosskurth/ut-capitole-blacklists.git "$TMP_DIR"

echo "Nettoyage des anciennes listes..."
sudo rm -rf /etc/squid/blacklist/*

echo "Déplacement des nouvelles listes utiles..."
sudo mkdir -p /etc/squid/blacklist
sudo mv "$TMP_DIR/ut-capitole-blacklists/blacklists/adult" /etc/squid/blacklist/
sudo mv "$TMP_DIR/ut-capitole-blacklists/blacklists/ads" /etc/squid/blacklist/

echo "Application des permissions..."
sudo chown -R proxy:proxy /etc/squid/blacklist

# Nettoyage
rm -rf "$TMP_DIR"

echo "Rechargement de la configuration de Squid..."
sudo systemctl reload squid.service
```

Planification avec cron

Ligne de commande


```
#ouvrir l'éditeur cron
sudo crontab -e
#ajouter cette ligne pour exécuter le fichier tout les jours à 2h du matin
0 2 * * * /opt/refresh-blacklist.sh
```

Config de Squid

Lignes de commandes

```
#installer squid
sudo apt install squid-openssl
#créer un répertoire
sudo mkdir -p /etc/squid/cert/
#aller dans ce répertoire
cd /etc/squid/cert/
#création de l'autorité de certification (CA de Squid)
sudo openssl req -new -newkey rsa:4096 -sha256 -days 3650 -nodes -x509 -keyout
squid_proxyCA.pem -out squid_proxyCA.pem
#permissions
sudo chown -R proxy:proxy /etc/squid/cert/
sudo chmod 0400 /etc/squid/cert/squid_proxyCA.pem
#vérifier le chemin
which security_file_certgen
#s'il y a une erreur
sudo /usr/lib/squid/security_file_certgen -c -s /var/spool/squid/ssl_db -M 4MB
sudo chown -R proxy:proxy /var/spool/squid/ssl_db
#Rédaction du fichier squid.conf
sudo mv /etc/squid/squid.conf /etc/squid/squid.conf.bak
sudo touch /etc/squid/squid.conf
sudo nano /etc/squid/squid.conf
# -- PORTS D'ECOUTE -- # Port HTTP transparent http_port 3129 transparent #
Port HTTPS transparent avec interception SSL https_port 3130 intercept ssl-
bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB
cert=/etc/squid/cert/squid_proxyCA.pem key=/etc/squid/cert/squid_proxyCA.pem #
-- CONFIGURATION DE L'INTERCEPTION SSL (SSL-BUMP) -- # Programme helper pour
générer les certificats sslcrtd_program /usr/lib/squid/security_file_certgen -
s /var/spool/squid/ssl_db -M 4MB # Configuration du "bumping" ssl_bump peek
all ssl_bump bump all # -- LISTES DE CONTROLE D'ACCES (ACL) -- # ACL pour les
ports sécurisés acl Safe_ports port 80 # http acl Safe_ports port 443 # https
acl CONNECT method CONNECT # ACL pour nos listes noires acl adult dstdomain
"/etc/squid/blacklist/adult/domains" acl adult url_regex
"/etc/squid/blacklist/adult/urls" acl ads dstdomain "/etc/squid/blacklist/ads"
# -- REGLES D'ACCES -- # Les règles sont lues dans l'ordre. La première qui
correspond est appliquée. http_access deny !Safe_ports http_access deny
```

```
CONNECT !Safe_ports # Autoriser l'administration locale (non utilisé ici, mais
bonne pratique) http_access allow localhost manager http_access deny manager #
Blocage basé sur nos listes noires http_access deny adult http_access deny ads
# Autoriser tout le reste http_access allow localhost http_access allow all #
-- AUTRES PARAMETRES -- coredump_dir /var/spool/squid refresh_pattern . 0 20%
4320
```

changer l'extension du fichier certificat convertir le certificat .pem en .crt et le placer au bon endroit

```
sudo openssl x509 -inform PEM -in /etc/squid/cert/squid_proxyCA.pem -out
/usr/local/share/ca-certificates/squid_proxyCA.crt
```

#Mettre à jour le magasin de certificat du serveur

```
sudo update-ca-certificates
```

#redémarrer squid

```
sudo systemctl restart squid.service
```

Capture d'écran

```
GNU nano 7.2 /etc/squid/squid.conf *
# -- PORTS D'ECOUTE --
# Port HTTP transparent
http_port 3129 transparent
# Port HTTPS transparent avec interception SSL
https_port 3130 intercept ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/cert/squid_proxyCA.pem key=/etc/squid/cert/squid_proxyCA.pem

# -- CONFIGURATION DE L'INTERCEPTION SSL (SSL-BUMP) --
# Programme helper pour générer les certificats
sslcrtld_program /usr/lib/squid/security_file_certgen -s /var/spool/squid/ssl_db -M 4MB
# Configuration du "bumping"
ssl_bump peek all
ssl_bump bump all

# -- LISTES DE CONTROLE D'ACCES (ACL) --
# ACL pour les ports sécurisés
acl Safe_ports port 80      # http
acl Safe_ports port 443    # https
acl CONNECT method CONNECT

# ACL pour nos listes noires
acl adult dstdomain "/etc/squid/blacklist/adult/domains"
acl adult url_regex "/etc/squid/blacklist/adult/urls"
acl ads dstdomain "/etc/squid/blacklist/ads"

# -- REGLES D'ACCES --
# Les règles sont lues dans l'ordre. La première qui correspond est appliquée.
http_access deny !Safe_ports
http_access deny CONNECT !Safe_ports

^G Aide      ^O Écrire    ^W Chercher  ^X Couper    ^T Exécuter  ^C Emplacement ^U Annuler   ^M-A Marquer   ^=] -> Crochet ^M-Q Précédent  ^B En arrière
^X Quitter   ^R Lire fich. ^N Remplacer  ^J Coller    ^_ Justifier  ^G Aller ligne ^M-E Refaire  ^M-G Copier  ^Q Retrouver ^M-W Suivant  ^_ En avant
```

Configuration des postes clients

Sur un poste Linux

Lignes de commande

#Récupérer le fichier du certiificat

Le fichier à distribuer est ``/usr/local/share/ca-certificates/squid_proxyCA.crt``. Vous pouvez utiliser une clé USB, un partage réseau ou ``scp``

#copier le fichier dans le répertoire du client `/usr/local/share/ca-certificates/`

```
# Sur le client exécuté cette commande de mise à jour  
sudo update-ca-certificates
```

Sur un poste Windows

Récupérer le fichier .crt

Installer le certificat en double cliant dessus

choisissez machine Locale

Important : Sélectionnez « Placer tous les certificats dans le magasin suivant » et choisissez le magasin « **Autorités de certification racines de confiance** »

valider l'assistant