Squid Proxy

Compte rendu – Configuration du Proxy Squid avec SSL-Bump, Blocage HTTP/HTTPS, et Filtrage par mots-clés

---

1. Installation de Squid sur Ubuntu 24.04

- Installation du package Squid :

```
sudo apt update
sudo apt install squid
```

- Version installée confirmée : Squid 6.10

---

2. Génération du certificat CA pour SSL-Bump

- Création du certificat CA pour Squid :

```
openssl req -new -newkey rsa:4096 -days 3650 -nodes -x509 \
  -keyout /etc/squid/squid-ca-key.pem \
  -out /etc/squid/squid-ca-cert.pem \
  -subj "/C=FR/ST=France/L=Paris/O=Squid/CN=Squid-Proxy-CA"
```

- Combinaison de la clé et du certificat en un seul fichier PEM utilisé par Squid :

```
cat /etc/squid/squid-ca-key.pem /etc/squid/squid-ca-cert.pem >
/etc/squid/squid.pem
chmod 400 /etc/squid/squid.pem
```

---

3. Initialisation de la base de certificats dynamiques (ssl_db)

Correction du problème de génération des certificats dynamiques avec l'option obligatoire `-d` (Squid 6+) :

```
sudo /usr/lib/squid/security_file_certgen -c -d -s /var/lib/ssl_db -M 4MB
sudo chown -R proxy:proxy /var/lib/ssl_db
sudo chmod -R 700 /var/lib/ssl_db
```

---

4. Configuration complète du fichier `/etc/squid/squid.conf`

Voici le fichier `squid.conf` complet :

```
# Proxy avec SSL-Bump et blocage

# Ports HTTP et HTTPS avec SSL-Bump activé
http_port 172.17.100.7:3128
https_port 172.17.100.7:3129 intercept ssl-bump cert=/etc/squid/squid.pem
generate-host-certificates=on dynamic_cert_mem_cache_size=4MB

# SSL BUMP CONFIG
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump all

# ACLs DEFINIES

# Réseaux locaux autorisés
acl localnet src 192.168.0.0/16
acl localnet src 10.0.0.0/8
acl localnet src 172.17.0.0/12

# Autorisation des ports sécurisés
acl SSL_ports port 443
acl Safe_ports port 21
acl Safe_ports port 443
acl Safe_ports port 70
acl Safe_ports port 210
acl Safe_ports port 1025-65535
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
```

```
# Tunneling HTTPS (CONNECT)
acl CONNECT method CONNECT

# Liste noire des sites bloqués (HTTP)
acl blacklist url_regex -i (^|\.)facebook\.com (^|\.)jeux\.fr
(^|\.)crazygames\.fr (^|\.)httpforever.com

# Blocage HTTPS via SNI
acl blocked_https ssl::server_name "/etc/squid/blacklist.txt"

# Filtrage par mots-clés (HTTP et HTTPS)
acl blocked_words url_regex -i "/etc/squid/blocked_words.txt"

# RÈGLES D'ACCÈS

http_access deny !Safe_ports
http_access deny CONNECT blacklist
http_access deny blocked_https
http_access deny blocked_words
http_access allow CONNECT SSL_ports
http_access allow localhost
http_access allow localnet
http_access deny all

# PERSONNALISATION DES ERREURS
deny_info ERR_BLOCKED_SITE blacklist
deny_info ERR_BLOCKED_SITE blocked_words
deny_info ERR_BLOCKED_SITE blocked_https
error_directory /usr/share/squid/errors/fr

# GESTION SSL et CERTIFICATS
sslproxy_cert_error allow all
tls_outgoing_options cert=/etc/squid/squid.pem key=/etc/squid/squid.pem
sslcrtd_program /usr/lib/squid/security_file_certgen -s /var/lib/ssl_db -M 4MB
sslcrtd_children 8 startup=1 idle=1

# LOGS & DIVERS
access_log /var/log/squid/access.log squid
coredump_dir /var/spool/squid
```

---

5. Fichier pour bloquer les domaines HTTPS via SNI

Chemin : `/etc/squid/blacklist.txt`

Contenu :

```
.facebook.com
.jeux.fr
.crazygames.fr
.httpforever.com
```

---

6. Fichier pour bloquer par mots-clés

Chemin : `/etc/squid/blocked_words.txt`

Contenu :

```
porno
gambling
casino
drugs
bitcoin
```

---

7. Personnalisation de la page de blocage Squid

Page modifiée : `/usr/share/squid/errors/fr/ERR_BLOCKED_SITE`

Contenu personnalisé :

```
<html>
<head>
    <title>Accès Bloqué</title>
    <style>
        body { font-family: Arial, sans-serif; text-align: center; background-
color: #f8d7da; color: #721c24; padding: 50px; }
        h1 { font-size: 2em; }
        p { font-size: 1.2em; }
    </style>
</head>
<body>
```

```
    <h1>⛔ Accès Bloqué ⛔</h1>
    <p>Ce site a été bloqué par la politique de filtrage de votre réseau.</p>
    <p>Si vous pensez que ceci est une erreur, veuillez contacter
l'administrateur.</p>
</body>
</html>
```

---

8. Sécurisation des paramètres proxy Windows et Firefox

Windows (via Registre) :

- Chemin :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings
```

- Valeurs ajoutées :

```
ProxySettingsPerUser = 0 (DWORD)
DisableProxySettingsUI = 1 (DWORD)
```

Firefox (via Registre) :

- Chemin :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mozilla\Firefox
```

- Valeurs ajoutées :

```
Mode = fixed (REG_SZ)
Proxy = http://172.17.100.7:3128 (REG_SZ)
Locked = 1 (DWORD)
```

---

9. Tests fonctionnels validés

- Blocage HTTP :
  `curl -x http://172.17.100.7:3128 http://facebook.com` → Page de blocage Squid.
- Blocage HTTPS :
  `curl -x http://172.17.100.7:3128 -k https://facebook.com` → Connexion refusée proprement.
- Blocage par mots-clés (HTTP) :
  `curl -x http://172.17.100.7:3128 http://example.com/casino` → Bloqué avec page de blocage.
- Logs Squid confirmant les blocages :

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

Conclusion

Le proxy Squid avec SSL-Bump est configuré et fonctionne parfaitement avec :

- Blocage HTTP/HTTPS par domaines (regex et SNI)
- Blocage par mots-clés
- Page de blocage personnalisée
- Verrouillage des paramètres proxy sous Windows et Firefox

L'ensemble du système est sécurisé et opérationnel.