PROCÉDURE SSL BUMP

Proxy Squid Explicite + Certificat CA via GPO

SRV-WEB-01 (10.11.3.2:3127) — Mode Proxy Manuel — Infrastructure SISR 2026

Auteur	CHADHOULI EL-Anrif
Machine proxy	SRV-WEB-01 — 10.11.3.2 (Debian 12, DMZ)
Date	Mars 2026
Mode proxy	Manuel (Explicite) — port 3127
Mode SSL	SSL Bump sur connexions CONNECT
Prérequis	Squid 5.7.x installé, openssl disponible, GPO AD opérationnelles

1. Contexte Technique et Choix d'Architecture

1.1 Deux modes de proxy possibles

Avant de configurer Squid avec SSL Bump, il est essentiel de comprendre la différence entre les deux modes de déploiement possibles, car ce choix impacte toute la configuration réseau :

Critère	Mode Transparent (Intercept)	Mode Manuel (Explicite) ← CHOISI
Port d'écoute	3128 intercept + 3129 intercept	3127 (un seul port) ☑
Configuration client	Aucune (transparent)	Proxy configuré dans le navigateur ou via GPO
Redirection pfSense	NAT Port Forward 443→3129 obligatoire	Règles firewall simples, pas de NAT
Compatibilité VPN IPsec	Problèmes de routage asymétrique	Compatible sans conflit ☑
Robustesse SNI / SSL	409 Conflict fréquents, 503 timeouts	SNI correctement géré via CONNECT ☑

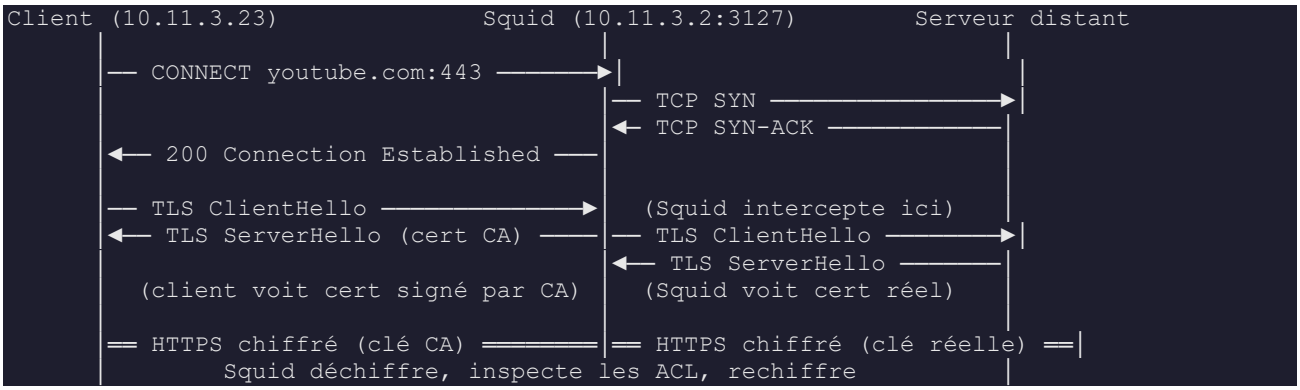
1.2 Pourquoi le mode Transparent a été abandonné

Le mode intercept (transparent) a été testé et abandonné pour trois raisons techniques majeures :

- Routage asymétrique :
- Conflit NAT/IPsec :
- Erreurs 409 Host Forgery :

CHOIX D'ARCHITECTURE : Le mode Manuel (Explicite) sur le port 3127 a été retenu. Le client envoie une requête CONNECT explicite à Squid, qui contacte le serveur distant avec sa propre IP (10.11.3.2). pfSense NAT normalement. Aucun conflit de routage. Le SSL Bump s'applique sur les tunnels CONNECT, ce qui est son usage nominal.

1.3 Ce que fait le SSL Bump en mode explicite



IMPORTANT : Le SSL Bump est une interception de trafic chiffré. Il est légal uniquement sur votre propre infrastructure, avec information préalable des utilisateurs. Ne jamais l'utiliser sur un réseau tiers.

2. Générer le Certificat CA sur SRV-WEB-01

> **INFO :** Les sections 2.1 et 2.2 ont déjà été réalisées lors de la première tentative. Les fichiers squid_CA.crt et squid_CA.key sont déjà présents et valides. Les captures correspondantes sont conservées.

2.1 Connexion et génération de la clé + certificat

Se connecter en SSH sur SRV-WEB-01 (10.11.3.2) et générer un certificat CA auto-signé dédié au proxy :

```
# Sur SRV-WEB-01 — en root
ssh root@10.11.3.2

# Créer le dossier pour les certificats Squid
mkdir -p /etc/squid/ssl_cert
cd /etc/squid/ssl_cert

# Générer la clé privée RSA 2048 bits
openssl genrsa -out squid_CA.key 2048

# Générer le certificat CA auto-signé (valable 10 ans)
openssl req -new -x509 -days 3650 -key squid_CA.key \
  -out squid_CA.crt \
  -subj '/C=FR/ST=Grand-Est/L=Metz/O=SISR2026/OU=Proxy/CN=SRV-WEB-01-ProxyCA'

# Vérifier le certificat généré
openssl x509 -in squid_CA.crt -text -noout | head -20
```

SRV-WEB-01 — ls -la /etc/squid/ssl_cert/ montrant squid_CA.key et squid_CA.crt + openssl x509 avec CN=SRV-WEB-01-ProxyCA, validité 10 ans

```
root@SRV-WEB-01:~# ls -l /etc/squid/ssl_cert
total 8
-rw-r--r-- 1 proxy proxy 1363 25 mars  16:15 squid_CA.crt
-rwx------ 1 proxy proxy 1704 25 mars  16:15 squid_CA.key
```

```
root@SRV-WEB-01:~# openssl x509 -in /etc/squid/ssl_cert/squid_CA.crt -text -noout | head -20
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:0a:5d:01:17:57:60:16:aa:08:5b:a7:6c:53:c4:d7:45:ad:d2:c6
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = FR, ST = Grand-Est, L = Metz, O = SISR2026, OU = Proxy, CN = SRV-WEB-01-ProxyCA
        Validity
            Not Before: Mar 25 15:15:54 2026 GMT
            Not After : Mar 22 15:15:54 2036 GMT
        Subject: C = FR, ST = Grand-Est, L = Metz, O = SISR2026, OU = Proxy, CN = SRV-WEB-01-ProxyCA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:94:a0:a8:82:c9:76:2d:b8:ac:3b:94:d1:22:33:
                    01:2b:80:f0:f8:44:6a:19:d1:87:6b:2e:eb:90:a5:
                    25:24:a2:fb:d5:d0:83:33:cf:b5:58:23:54:27:ab:
                    76:30:bd:7b:23:23:fb:e7:70:db:25:5b:fc:62:d9:
                    87:ae:cf:75:ee:11:91:95:e0:98:96:10:d9:99:4b:
```

2.2 Répertoire du cache SSL Squid

```
# Créer et initialiser le répertoire de cache SSL
mkdir -p /var/lib/squid/ssl_db
/usr/lib/squid/security_file_certgen -c -s /var/lib/squid/ssl_db -M 4MB

# Droits pour l'utilisateur proxy
chown -R proxy:proxy /var/lib/squid/ssl_db
chown -R proxy:proxy /etc/squid/ssl_cert
chmod 700 /etc/squid/ssl_cert/squid_CA.key
```

SRV-WEB-01 — ls -la /var/lib/squid/ssl_db/ base initialisée + /etc/squid/ssl_cert/ avec droits proxy:proxy

```
root@SRV-WEB-01:~# ls -la /var/spool/squid/ssl_db
total 16
drwxr-xr-x 3 proxy proxy 4096 25 mars  16:59 .
drwxr-xr-x 3 proxy proxy 4096 25 mars  16:59 ..
drwxr-xr-x 2 proxy proxy 4096 25 mars  16:59 certs
-rw-r--r-- 1 proxy proxy    0 25 mars  16:59 index.txt
-rw-r--r-- 1 proxy proxy    1 25 mars  16:59 size
```

```
root@SRV-WEB-01:~# chown -R proxy:proxy /var/spool/squid/ssl_db
chown -R proxy:proxy /etc/squid/ssl_cert
chmod 700 /etc/squid/ssl_cert/squid_CA.key
```

3. Configurer Squid en Mode Proxy Explicite avec SSL Bump

3.1 Nouveau squid.conf — Mode Explicite

Remplacer entièrement le squid.conf existant. En mode explicite, un seul port suffit (3127). Aucun mot-clé 'intercept', aucune règle iptables NAT nécessaire :

```
nano /etc/squid/squid.conf
```

Contenu complet du nouveau fichier :

```
GNU nano 7.2                                                    /etc/squid/squid.conf
# ========================================================
# CONFIGURATION SQUID : MODE MANUEL (GPO) + SSL BUMP
# ========================================================

# --- RÉSEAUX AUTORISÉS ---
acl networklan src 10.11.3.16/28
acl site2_lan src 10.11.4.0/24
acl localhost src 127.0.0.1/32

# --- FILTRAGE TOULOUSE ---
acl cat_porn dstdomain /etc/squid/blacklists/porn/domains
acl cat_social_networks dstdomain /etc/squid/blacklists/social_networks/domains
acl sites_interdits dstdomain /etc/squid/sites_bloques.txt
acl test_manuel dstdomain .facebook.com .pornhub.com .youtube.com .netflix.com .crunchyroll.com
# --- PORT MANUEL AVEC SSL BUMP ---
# AUCUN mot "intercept" ici. C'est le port 3127 qu'on attaque.
http_port 3127 ssl-bump generate-host-certificates=on dynamic_cert_mem_cache_size=4MB cert=/etc/squid/squid-ca.crt key=/etc/squid/squid-ca.key

# --- MOTEUR SSL BUMP ---
sslcrtd_program /usr/lib/squid/security_file_certgen -s /var/lib/squid/ssl_db -M 4MB
sslcrtd_children 5
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump all

# --- RÈGLES D'ACCÈS ---
http_access deny test_manuel
http_access deny cat_porn
http_access deny cat_social_networks
http_access deny sites_interdits

http_access allow networklan
http_access allow site2_lan
http_access allow localhost
# --- LOGS ---
access_log daemon:/var/log/squid/access.log squid
coredump_dir /var/spool/squid
refresh_pattern .               0       20%     4320
```

3.2 Supprimer les règles iptables TPROXY résiduelles

> ⚠ **ATTENTION :** Si des règles iptables TPROXY ou REDIRECT ont été créées lors des tentatives précédentes, elles doivent être supprimées. En mode explicite, aucune règle iptables n'est nécessaire sur Debian.

```
# Nettoyer toutes les règles résiduelles
iptables -t nat    -F
iptables -t mangle -F
ip rule del fwmark 0x1 lookup 100 2>/dev/null
ip route flush table 100 2>/dev/null

# Vérifier que les tables sont propres (doit retourner 0 règles)
iptables -t nat    -L PREROUTING -n -v
iptables -t mangle -L PREROUTING -n -v

# ip_forward toujours actif (nécessaire pour le routage DMZ)
sysctl net.ipv4.ip_forward
# → doit retourner net.ipv4.ip_forward = 1
```

3.3 Vérifier la syntaxe et redémarrer Squid

```
# Tester la syntaxe — doit retourner sans erreur
squid -k parse

# Redémarrer Squid
systemctl restart squid
systemctl status squid

# Vérifier le port d'écoute (un seul port : 3127)
ss -tlnp | grep squid
# → doit montrer LISTEN sur 10.11.3.2:3127 uniquement
```

4. Configuration pfSense — Règles Pare-feu LAN

En mode proxy explicite, il n'y a plus de NAT Port Forward. On remplace par trois règles firewall LAN simples qui forcent le passage par le proxy tout en autorisant le DNS.

4.1 Récapitulatif des 3 règles à créer

#	Source	Destination	Port	Action
1	LAN 10.11.3.16/28	SRV-AD-01 10.11.3.18	UDP 53	☑ PASS — DNS autorisé
2	LAN 10.11.3.16/28	SRV-WEB-01 10.11.3.2	TCP 3127	☑ PASS — Accès au proxy
3	LAN 10.11.3.16/28	any	TCP 80, 443	✗ BLOCK — Forcer le proxy

⚠ **ATTENTION :** L'ordre des règles est CRITIQUE dans pfSense. La règle Pass TCP 3127 doit être AVANT la règle Block 80/443. pfSense lit les règles de haut en bas et s'arrête à la première qui correspond.

4.2 Règle 1 — Autoriser DNS (UDP 53)

Sans cette règle, les postes clients ne peuvent plus résoudre les noms de domaine une fois le trafic 80/443 bloqué.

1. pfSense → Firewall → Rules → onglet LAN → Add ↑
2. Renseigner :

Champ	Valeur
Action	Pass
Interface	LAN
Protocol	UDP
Source	10.11.3.16/28 (LAN Site A)
Destination	10.11.3.18 (SRV-AD-01)
Destination Port	DNS (53)
Description	LAN → DNS SRV-AD-01 (obligatoire)

3. Sauvegarder

4.3 Règle 2 — Autoriser TCP vers le proxy (port 3127)

Cette règle autorise les clients à contacter Squid sur le port 3127.

4. Firewall → Rules → onglet LAN → Add ↑ (en dessous de la règle DNS)
5. Renseigner :

Champ	Valeur

Action	Pass
Interface	LAN
Protocol	TCP
Source	10.11.3.16/28 (LAN Site A)
Destination	10.11.3.2 (SRV-WEB-01 — Squid)
Destination Port	3127
Description	LAN → Proxy Squid DMZ (TCP 3127)

6. Sauvegarder

4.4 Règle 3 — Bloquer la navigation directe (ports 80 et 443)

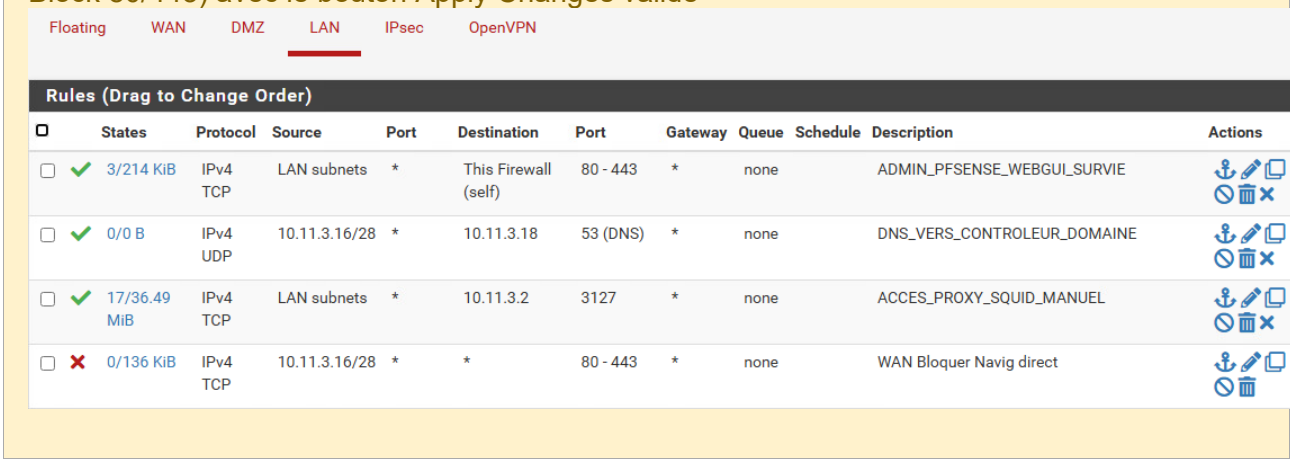
Règle critique : empêche les clients de contourner le proxy en accédant directement à Internet.

7. Firewall → Rules → onglet LAN → Add ↓ (en DESSOUS des deux règles Pass)
8. Renseigner :

Champ	Valeur
Action	Block
Interface	LAN
Protocol	TCP
Source	10.11.3.16/28
Destination	any
Destination Port Range	HTTP (80) → HTTPS (443)
Description	LAN → WAN bloquer navigation directe (forcer proxy)

9. Sauvegarder → Apply Changes

pfSense — Firewall > Rules > LAN : les 3 règles dans le bon ordre (Pass DNS, Pass 3127, Block 80/443) avec le bouton Apply Changes validé



INFO : Supprimer ou désactiver l'ancienne règle NAT Port Forward (443→3129) si elle existe encore dans Firewall → NAT → Port Forward. Elle n'est plus nécessaire et peut provoquer des conflits.

5. Déploiement via GPO Active Directory

Deux GPO sont nécessaires : la première déploie le certificat CA (déjà réalisée), la seconde configure automatiquement le proxy sur tous les postes Windows.

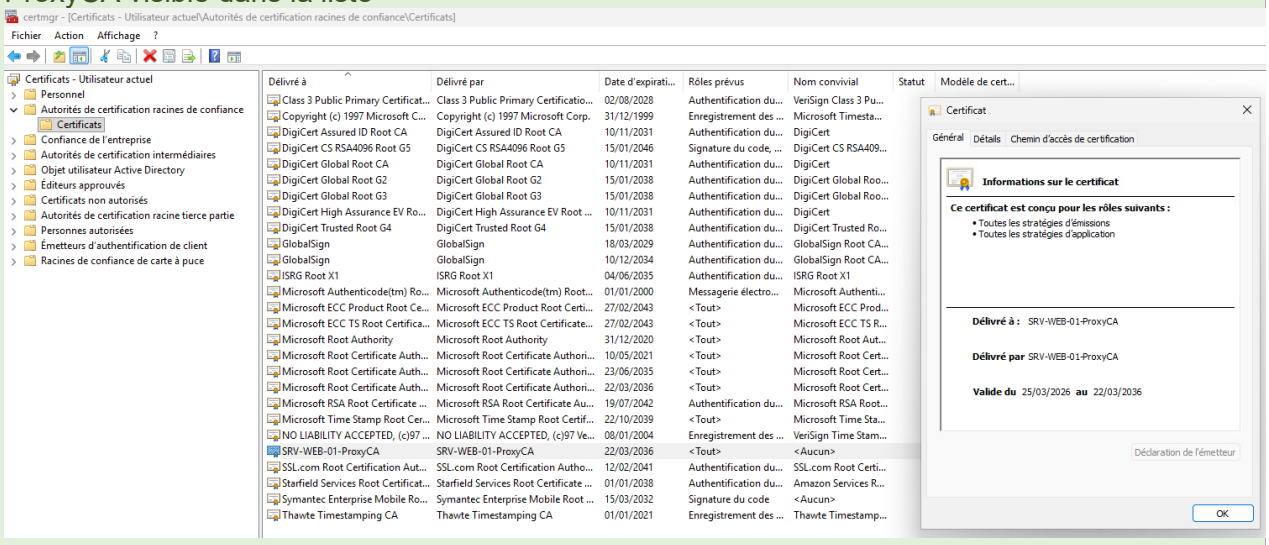
5.1 GPO_CERTIFICAT_PROXY — Déploiement du certificat CA

INFO : Cette GPO a déjà été créée et liée aux OUs lors de la procédure précédente. Les captures correspondantes sont conservées. Vérifier simplement qu'elle est toujours active.

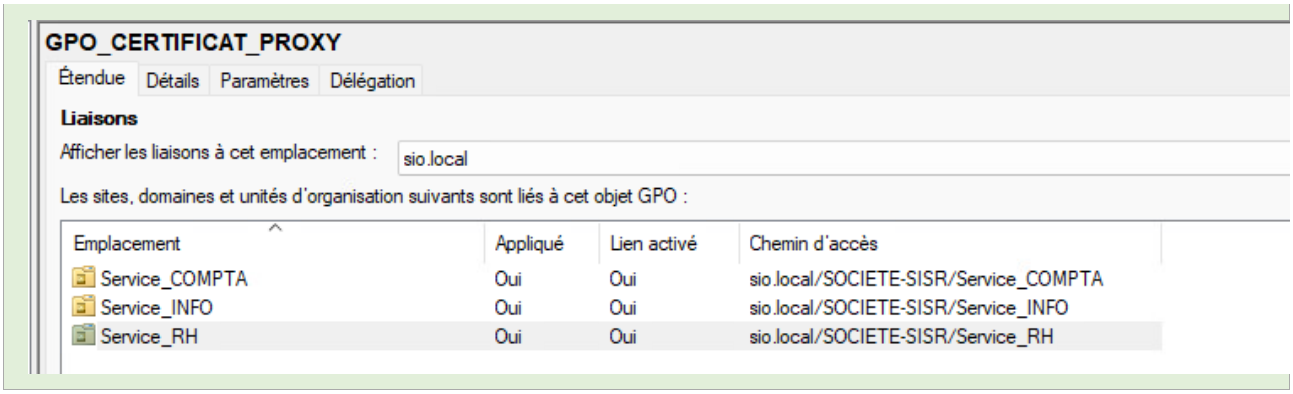
Vérifier que GPO_CERTIFICAT_PROXY est bien liée et active :

```
# Sur SRV-AD-01 — PowerShell
Get-GPO -Name 'GPO_CERTIFICAT_PROXY' | Select-Object DisplayName, GpoStatus
# → GpoStatus doit être 'AllSettingsEnabled'
```

: Éditeur GPO — Autorités de certification racines de confiance : certificat SRV-WEB-01-ProxyCA visible dans la liste



: Console GPMC — GPO_CERTIFICAT_PROXY liée aux OUs Service_RH, Service_INFO, Service_COMPTA



5.2 GPO_PROXY_SETTINGS — Configurer le proxy dans Windows

Cette nouvelle GPO configure automatiquement l'adresse du proxy (10.11.3.2:3127) dans les paramètres Internet de tous les postes Windows du domaine, sans intervention manuelle.

Créer la GPO

10. Sur SRV-AD-01, ouvrir gpmc.msc
11. Clic droit sur Service_INFO → Créer un objet GPO → nommer : GPO_PROXY_SETTINGS
12. Clic droit sur GPO_PROXY_SETTINGS → Modifier

Méthode 1 — Via Préférences Registre (recommandée, fonctionne sur tous les navigateurs)

Cette méthode écrit directement dans les clés de registre Windows qui contrôlent le proxy système :

13. Dans l'éditeur GPO, naviguer vers :

```
Configuration utilisateur → Préférences → Paramètres Windows → Registre
```

14. Clic droit → Nouveau → Élément registre → créer les 3 clés suivantes :

Clé de registre	Valeur	Données
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	ProxyEnable	1 (DWORD)
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	ProxyServer	10.11.3.2:3127 (REG_SZ)
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	ProxyOverride	10.*;192.168.*;localhost (REG_SZ)

INFO : ProxyOverride liste les adresses qui contournent le proxy (réseau local). Adapter si nécessaire. Les navigateurs modernes (Edge, Chrome, IE) lisent ces clés de registre automatiquement. Firefox nécessite une configuration séparée.

Méthode 2 — Via Maintenance Internet Explorer (pour IE/Edge Legacy)

15. Dans l'éditeur GPO, naviguer vers :

```
Configuration utilisateur → Paramètres Windows → Maintenance Internet Explorer →
Connexion → Paramètres proxy
```

16. Cocher Activer les paramètres du proxy
17. Serveur proxy : 10.11.3.2 | Port : 3127
18. Exceptions (ne pas utiliser le proxy pour) : 10.*;192.168.*;localhost
19. Cliquer OK

Lier GPO_PROXY_SETTINGS aux OUs

20. Dans GPMC, faire un clic droit sur Service_RH → Lier un objet GPO existant → GPO_PROXY_SETTINGS
21. Répéter pour Service_INFO et Service_COMPTA

6. Test et Validation

6.1 Appliquer les GPO sur CL-WIN11-01

```
# Sur CL-WIN11-01
gpupdate /force
# Redémarrer le poste pour appliquer les nouvelles GPO
```

6.2 Vérifier le certificat et la configuration proxy

```
# Sur CL-WIN11-01 — PowerShell

# Vérifier le certificat CA dans le magasin
Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like '*ProxyCA*'}

# Vérifier la configuration proxy dans le registre
Get-ItemProperty 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings' |
  Select-Object ProxyEnable, ProxyServer, ProxyOverride
# ProxyEnable = 1, ProxyServer = 10.11.3.2:3127
```

CL-WIN11-01 — Get-ChildItem Cert:\LocalMachine\Root : certificat SRV-WEB-01-ProxyCA présent

```
PS C:\Users\Administrateur> Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like '*ProxyCA*' -or $_.Subject -like '*SISR*


   PSParentPath : Microsoft.PowerShell.Security\Certificate::LocalMachine\Root

Thumbprint                                Subject
----------                                -------
97FCAB84282CE0F99A0AFFB261A6CA59A5C83AB4  CN=SRV-WEB-01-ProxyCA, OU=Proxy, O=SISR2026, L=Metz, S=Grand-Est, C=FR
```

6.3 Tester la navigation HTTPS

Depuis CL-WIN11-01, ouvrir Edge ou Firefox et naviguer vers un site HTTPS. Le proxy doit être utilisé automatiquement sans configuration manuelle dans le navigateur :

22. Accéder à https://www.debian.org
23. Cliquer sur le cadenas dans la barre d'adresse
24. Vérifier le certificat : l'émetteur doit être SRV-WEB-01-ProxyCA

6.4 Tester le forçage du proxy

Vérifier que la navigation directe (sans passer par le proxy) est impossible grâce à la règle pfSense Block 80/443 :

25. Dans le registre Windows, mettre temporairement ProxyEnable = 0 pour simuler un contournement
26. Tenter d'accéder à https://www.google.com → la connexion doit échouer (règle Block 80/443 active)
27. Remettre ProxyEnable = 1

```
# Test en PowerShell (sans passer par le proxy)
Invoke-WebRequest -Uri 'https://www.google.com' -Proxy '' -TimeoutSec 10
# → doit retourner une erreur (connexion refusée par pfSense)
```

6.5 Vérifier l'interception dans les logs Squid

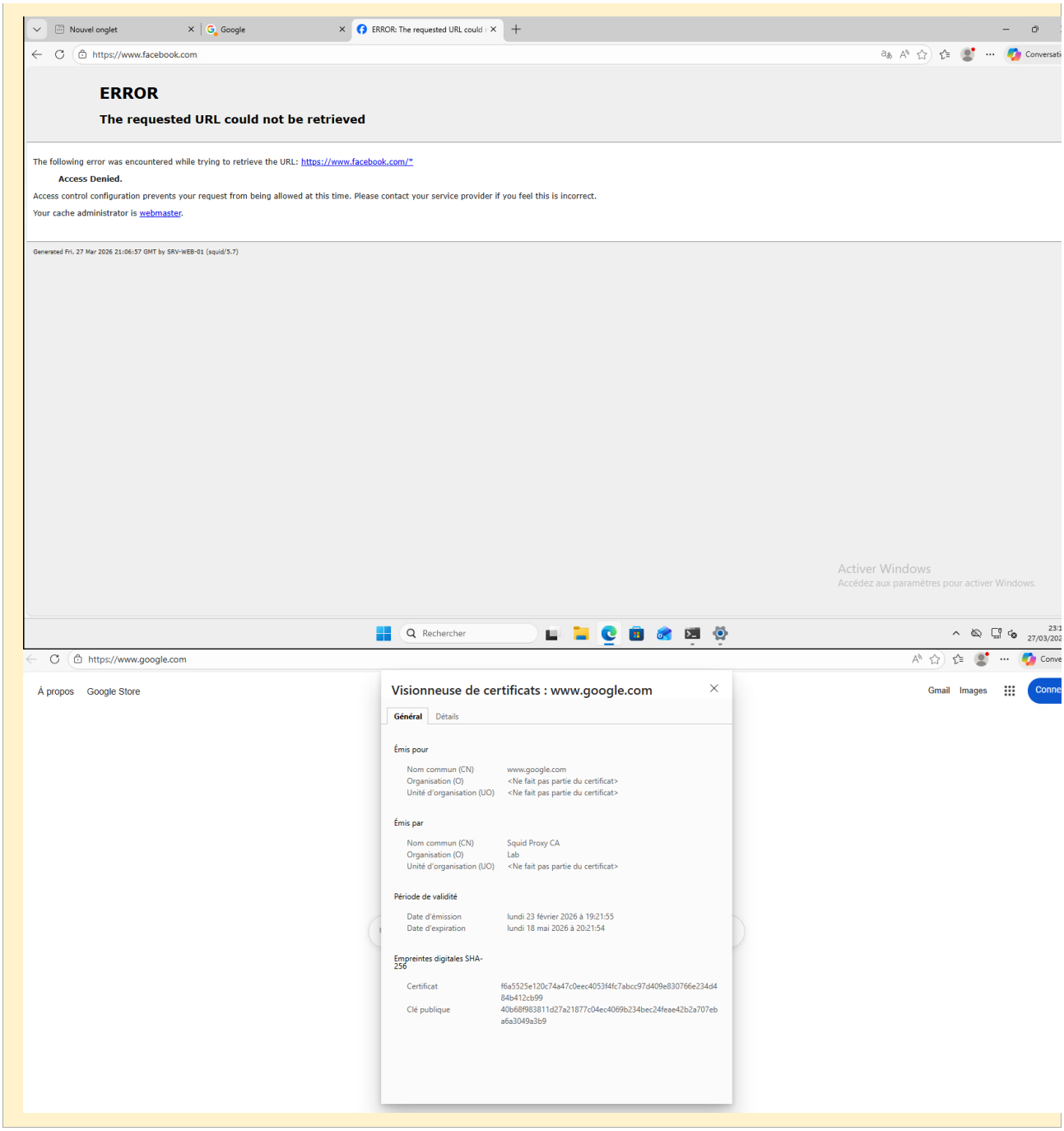
```
# Sur SRV-WEB-01
tail -f /var/log/squid/access.log

# En mode proxy explicite + SSL Bump, on doit voir :
# CONNECT ... 200  → tunnel CONNECT établi
# TCP_MISS/200 https://... → Squid déchiffre et accède à l'URL complète
# TCP_DENIED/403 → sites bloqués par ACL
```

6.6 Tester le blocage HTTPS

```
# Dans le navigateur sur CL-WIN11-01 :
https://www.youtube.com   → doit être BLOQUÉ (TCP_DENIED/403)
https://www.facebook.com  → doit être BLOQUÉ
https://www.google.com    → doit être AUTORISÉ (TCP_MISS/200)
```

Firefox/Edge CL-WIN11-01 — Message 'connexion refusée' pour facebook.com et connexion établi pour google.com


Nouvel onglet
Google
ERROR: The requested URL could
https://www.facebook.com
ERROR
The requested URL could not be retrieved
The following error was encountered while trying to retrieve the URL: https://www.facebook.com/*
Access Denied.
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.
Your cache administrator is webmaster.
Generated Fri, 27 Mar 2026 21:06:57 GMT by SRV-WEB-01 (squid/5.7)
Activer Windows
Accédez aux paramètres pour activer Windows.
Rechercher
https://www.google.com
À propos
Google Store
Gmail
Images
Visionneuse de certificats : www.google.com
Général
Détails
Émis pour
Nom commun (CN) www.google.com
Organisation (O) <Ne fait pas partie du certificat>
Unité d'organisation (UO) <Ne fait pas partie du certificat>
Émis par
Nom commun (CN) Squid Proxy CA
Organisation (O) Lab
Unité d'organisation (UO) <Ne fait pas partie du certificat>
Période de validité
Date d'émission lundi 23 février 2026 à 19:21:55
Date d'expiration lundi 18 mai 2026 à 20:21:54
Empreintes digitales SHA-256
Certificat f6a5525e120c74a47c0eec4053f4fc7abcc97d409e830766e234d484b412cb99
Clé publique 40b68f983811d27a21877c04ec4069b234bec24feae42b2a707eba6a3049a3b9