BTS SIO — Option SISR — Fiche de Réalisation Professionnelle

Renouvellement du Certificat SSL Bump du Proxy Squid via la PKI d'entreprise Microsoft (AD CS)

Interception HTTPS — Certificat signé par SRV-AD-01 (AD CS) — Déploiement sur SRV-WEB-01 (Squid/Debian)

PKI : 10.11.3.18 (sio.local) | Proxy : 10.11.3.2 (Debian 12.5) | Client : 10.11.3.23 (Win11)

Champ	Valeur
Candidat	BTS SIO option SISR — Session 2026
Entreprise	SOS Futur
Objet	Renouvellement certificat SSL Bump Squid via AD CS (PKI interne)
Serveur Proxy	SRV-WEB-01 — Debian 12.5 — 10.11.3.2 — Squid 5.7.x
PKI	SRV-AD-01 — Windows Server 2025 — 10.11.3.18 — AD CS
Date	Mai 2026

I. CONTEXTE MÉTIER ET PKI — SSL Bump & Autorité de Certification d'Entreprise

Le mécanisme SSL Bump (ou HTTPS Inspection) permet au proxy Squid d'intercepter le trafic TLS des clients pour appliquer les politiques de filtrage web (antivirus, catégories bloquées, journalisation). Pour que cette interception soit transparente côté client, Squid doit présenter, à la volée, un certificat recréé au nom du site réel, signé par une autorité de certification reconnue par le navigateur du poste client.

Critère	Certificat auto-signé local	Certificat signé par AD CS (PKI interne)
Confiance client	**Alerte de sécurité dans tous les navigateurs**	**Confiance native via GPO (certificat racine déployé automatiquement)**
Déploiement	Import manuel sur chaque poste	Automatique via GPO — Computer Configuration > Trusted Root CAs
Révocation (CRL/OCSP)	**Absente — impossible à révoquer**	**CRL publiée par AD CS, révocation centralisée**
Traçabilité	**Aucune — certificat hors contrôle**	**Enregistré dans la base AD CS, audit possible**
Renouvellement	Manuel, sans processus formalisé	Via certsrv ou certreq — procédure reproductible
Conformité ANSSI	**Non conforme**	**Conforme aux recommandations PKI interne**

Flux d'interception SSL Bump — Architecture

① CL-WIN11-01 envoie une requête HTTPS vers https://www.google.fr au Proxy Squid (10.11.3.2:3127).
② Squid intercepte la connexion TLS et établit sa propre connexion vers google.fr (serveur réel).
③ Squid génère à la volée un certificat au nom de google.fr, signé par son certificat SSL Bump.

④ Le certificat SSL Bump est lui-même signé par la PKI interne (AD CS — SRV-AD-01).
⑤ Le client fait confiance au certificat google.fr car la chaîne remonte à la PKI interne (déployée via GPO).
⑥ Squid peut ainsi inspecter, filtrer et journaliser le contenu HTTPS en clair.

II. GÉNÉRATION DE LA DEMANDE DE SIGNATURE (CSR) SOUS DEBIAN

Toutes les commandes de cette section sont exécutées sur SRV-WEB-01 (Debian 12.5) en tant que root ou via sudo. Le répertoire de travail est /etc/squid/ssl_cert/.

Étape 1 — Préparation du répertoire et vérification de l'environnement

Navigation : SRV-WEB-01 — Terminal SSH (root)

```
# Création du répertoire sécurisé pour les certificats Squid
mkdir -p /etc/squid/ssl_cert
chmod 700 /etc/squid/ssl_cert
chown proxy:proxy /etc/squid/ssl_cert

# Vérification de la version OpenSSL disponible
openssl version
# Résultat attendu : OpenSSL 3.x.x (Debian 12)
```

Étape 2 — Génération de la nouvelle clé privée RSA 4096 bits

La clé privée est générée localement sur SRV-WEB-01. Elle ne doit jamais quitter le serveur et ne sera pas transmise à la PKI. Seul le CSR (demande de signature) sera envoyé à AD CS.

```
# Génération de la clé privée RSA 4096 bits (sans passphrase pour le service
Squid)
openssl genrsa -out /etc/squid/ssl_cert/squid-bump.key 4096

# Restriction des droits sur la clé privée (lecture seule pour proxy)
chmod 640 /etc/squid/ssl_cert/squid-bump.key
chown root:proxy /etc/squid/ssl_cert/squid-bump.key

# Vérification de la clé générée
openssl rsa -in /etc/squid/ssl_cert/squid-bump.key -check
# Résultat attendu : RSA key ok
```

⚠ EXPLICATION TECHNIQUE : L'absence de passphrase est intentionnelle : Squid doit charger la clé automatiquement au démarrage du service, sans intervention humaine. La sécurité repose sur les permissions filesystem (chmod 640) et l'isolation du serveur.

Étape 3 — Création du fichier de configuration OpenSSL pour le CSR

Un fichier de configuration dédié définit les extensions X.509 requises pour un certificat d'autorité de certification subordonnée (CA:TRUE, KeyCertSign, CRLSign) — indispensable pour que Squid puisse signer les certificats à la volée.

```
# Création du fichier de configuration CSR
cat > /tmp/squid-bump.cnf << 'EOF'
[req]
default_bits       = 4096
prompt             = no
default_md         = sha256
distinguished_name = dn
req_extensions     = v3_req

[dn]
C  = FR
ST = Grand Est
L  = Metz
O  = Sio Sisr
OU = Informatique
CN = SRV-WEB-01 Squid SSL Bump CA

[v3_req]
subjectAltName     = @alt_names
basicConstraints   = CA:TRUE
keyUsage           = keyCertSign, cRLSign, digitalSignature

[alt_names]
DNS.1 = srv-web-01.sio.local
IP.1  = 10.11.3.2
EOF
```

Étape 4 — Génération du CSR (Certificate Signing Request)

```
# Génération du CSR avec la clé privée et le fichier de configuration
openssl req -new \
  -key /etc/squid/ssl_cert/squid-bump.key \
  -config /tmp/squid-bump.cnf \
  -out /tmp/squid-bump.csr

# Vérification du contenu du CSR
openssl req -in /tmp/squid-bump.csr -text -noout | head -40

# Champs à vérifier dans la sortie :
# Subject: C=FR, ST=Grand Est, O=SOS Futur, CN=SRV-WEB-01 Squid SSL Bump CA
# X509v3 Basic Constraints: CA:TRUE
# X509v3 Key Usage: Certificate Sign, CRL Sign
```

☑ **Le fichier /tmp/squid-bump.csr est généré. La sortie openssl req -text confirme Subject et extensions CA:TRUE.**

CAPTURE D'ÉCRAN N°1 — Terminal SRV-WEB-01 — Sortie de 'openssl req -in /tmp/squid-bump.csr -text -noout' affichant le Subject, les extensions X509v3 (CA:TRUE, KeyUsage) et la signature du CSR.

```
root@SRV-WEB-01:~# openssl req -in /tmp/squid-bump.csr -text -noout | head -40
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = FR, ST = Grand Est, L = Metz, O = Sio Sisr, OU = Informatique, CN = SRV-WEB-01 Squid SSL Bump CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:aa:b8:6c:f0:0e:e9:28:9c:f1:ac:76:14:66:c9:
                    b7:54:90:89:f7:9d:ff:da:8e:fb:59:cb:b7:ce:fd:
                    cb:d0:ad:50:38:a7:16:8e:c8:cd:56:e3:01:74:0c:
                    93:fe:c3:7d:98:96:72:79:54:06:25:85:a5:0c:10:
                    53:4e:08:ee:02:a1:8a:c3:44:c3:13:a8:72:57:6e:
                    8c:6c:dc:ee:a6:c2:d1:6d:2b:d6:18:15:52:51:ed:
                    9c:41:b7:10:89:01:9c:9d:45:58:2f:41:cd:8d:d6:
                    69:5a:1b:e2:1c:df:8d:b8:23:f5:a7:6d:50:77:b2:
                    2a:dd:9e:3b:5e:fb:2f:5f:7d:1f:08:ef:fc:71:7d:
                    a1:db:e3:43:81:80:07:61:fa:df:0e:b9:ee:2f:f2:
                    ae:7b:90:d0:88:eb:93:5f:bb:e5:fc:ee:1b:da:d5:
                    2d:4e:7b:61:e6:a4:26:89:5b:f5:1c:72:66:da:72:
                    5a:f1:b7:b4:74:16:f1:ba:df:65:de:05:78:47:dd:
                    33:dd:94:ad:6d:de:38:da:b7:fe:c3:5d:82:89:b8:
                    5b:75:f5:63:b3:c7:44:9e:56:8b:cb:6c:61:23:22:
                    50:58:c5:fe:d0:79:52:9e:22:b9:4d:5d:c8:d9:4f:
                    1f:ce:14:c2:da:64:e4:98:d1:3c:fe:c2:59:86:a0:
                    92:c2:6e:fc:93:47:9c:54:41:28:49:eb:28:ef:69:
                    d9:aa:0b:1e:3c:47:96:b5:55:91:4c:31:27:62:07:
                    b5:d7:7d:c6:3f:d2:84:eb:0b:8b:c9:ab:3f:d9:d4:
                    cc:fd:18:85:1f:c1:3a:1a:2e:75:f9:ca:50:b7:ac:
                    6e:a8:32:05:64:4a:84:89:d3:3e:96:55:91:a8:09:
                    67:b8:37:c7:bb:9f:97:9b:6e:e5:0d:8c:25:0f:72:
                    69:66:86:93:ca:b5:a1:40:f3:9f:58:56:b8:f0:6f:
                    19:08:d6:17:5f:a8:0e:c2:ac:a3:a2:8c:ce:0e:25:
                    5f:f0:61:97:65:57:c7:65:2b:1b:ba:57:a1:63:d6:
                    ac:a8:4b:dc:ab:83:64:88:27:5f:4b:e6:ea:2f:b7:
                    af:31:cd:54:d6:07:9c:05:70:37:08:c8:50:1c:34:
                    0f:05:4a:04:3e:82:9f:f1:95:7c:2b:a5:7c:ac:05:
                    56:f3:18:9f:ed:29:7d:c8:7a:c2:51:5d:bf:e6:58:
                    3f:e0:e9:2b:3e:f3:2b:69:ae:a0:03:fd:bc:e6:6d:
                    6b:e0:e6:62:ea:e0:2e:9e:be:fb:ef:0d:2b:94:d8:
```

III. SIGNATURE PAR LA PKI WINDOWS — AD CS (certsrv)

La signature du CSR par la PKI Microsoft garantit que le certificat délivré à Squid sera reconnu par tous les postes du domaine sio.local via la chaîne de confiance déployée par GPO. L'opération est réalisée depuis n'importe quel poste du domaine ou depuis SRV-AD-01 directement.

Étape 5 — Transfert du CSR vers un poste Windows du domaine

Navigation : SRV-WEB-01 — Terminal SSH ou SCP

```
# Afficher le contenu du CSR pour copie-coller dans certsrv
cat /tmp/squid-bump.csr

# Ou transférer via SCP vers SRV-AD-01
scp /tmp/squid-bump.csr admin@10.11.3.18:C:/Temp/squid-bump.csr
```

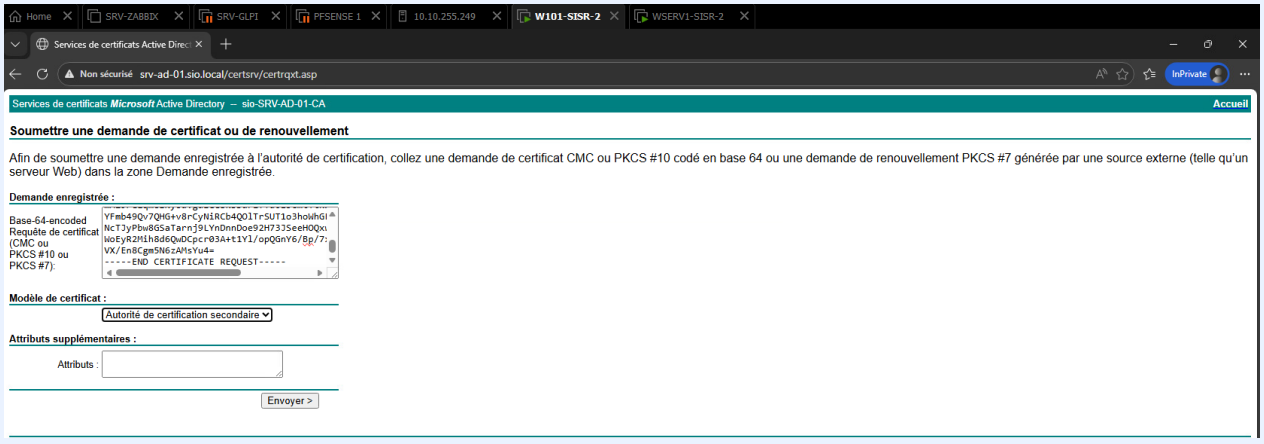
Étape 6 — Soumission du CSR via l'interface Web de la PKI (certsrv)

Navigation : Navigateur Web (depuis poste du domaine) — http://10.11.3.18/certsrv

1. Ouvrir un navigateur et accéder à http://10.11.3.18/certsrv (interface Web AD CS).
2. Se connecter avec un compte du domaine ayant les droits d'enrôlement (ex : Administrator ou compte PKI-Admin).
3. Cliquer sur « Request a certificate ».
4. Cliquer sur « Advanced certificate request ».
5. Cliquer sur « Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file ».
6. Dans le champ « Saved Request », coller l'intégralité du contenu du fichier squid-bump.csr (de -----BEGIN CERTIFICATE REQUEST----- à -----END CERTIFICATE REQUEST-----).
7. Dans la liste déroulante « Certificate Template », sélectionner le modèle Subordinate Certification Authority (ou SubCA selon le nom configuré dans AD CS).
8. Cliquer sur « Submit ».

⚠ **PRÉREQUIS MODÈLE AD CS :** Si le modèle 'Subordinate Certification Authority' n'est pas visible dans la liste, il doit être publié dans AD CS : certsrv > Certificate Templates > Manage > Duplicate du modèle SubCA, puis l'activer dans Certificate Templates > New > Certificate Template to Issue.

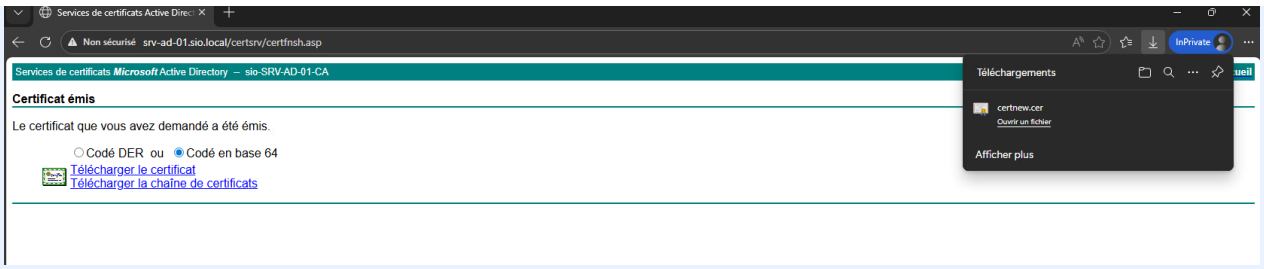
CAPTURE D'ÉCRAN N°2 — Interface certsrv (http://10.11.3.18/certsrv) — Formulaire 'Advanced Certificate Request' avec le contenu du CSR collé dans le champ 'Saved Request' et le modèle 'Subordinate Certification Authority' sélectionné.



Étape 7 — Téléchargement du certificat signé

9. Après soumission, si la PKI est configurée en émission automatique, la page affiche 'Certificate Issued'.
10. Cliquer sur « Download certificate » — choisir le format Base 64 encoded (.cer).
11. Enregistrer le fichier sous le nom squid-bump.cer.
12. Si la PKI requiert une approbation manuelle, se connecter à la console certsrv sur SRV-AD-01, approuver la demande en attente dans Pending Requests, puis télécharger le certificat.

CAPTURE D'ÉCRAN N°3 — Interface certsrv — Page 'Certificate Issued' avec le lien de téléchargement du certificat signé au format Base 64. Preuve que la PKI interne a bien signé la demande Squid.




```
root@SRV-WEB-01:~# ls -l /etc/squid/ssl_cert/
total 16
-rw-r----- 1 root  proxy 3272  8 mai   16:55 squid-bump.key
-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
-rw-r--r-- 1 root  root  2343  8 mai   18:07 squid.crt
root@SRV-WEB-01:~#
```

IV. DÉPLOIEMENT DU CERTIFICAT SUR SRV-WEB-01 (SQUID/DEBIAN)

Étape 8 — Transfert du certificat signé vers SRV-WEB-01

Navigation : SRV-AD-01 ou poste Windows — PowerShell / SCP

```
# Depuis SRV-AD-01 (PowerShell) — envoi vers SRV-WEB-01
scp C:\Temp\squid-bump.cer admin@10.11.3.2:/tmp/squid-bump.cer

# Vérifier la réception sur SRV-WEB-01
ls -lh /tmp/squid-bump.cer
# Résultat attendu : -rw-r--r-- 1 root root ~2.5K /tmp/squid-bump.cer
```

Étape 9 — Conversion du certificat et vérification de la chaîne

Navigation : SRV-WEB-01 — Terminal SSH (root)

```
# Conversion du .cer (DER ou Base64) en .pem si nécessaire
openssl x509 -inform DER -in /tmp/squid-bump.cer \
  -out /tmp/squid-bump.pem 2>/dev/null || \
openssl x509 -inform PEM -in /tmp/squid-bump.cer \
  -out /tmp/squid-bump.pem

# Vérification du certificat signé
openssl x509 -in /tmp/squid-bump.pem -text -noout | grep -E
'Subject:|Issuer:|Not After|CA:'
```

```
# Résultat attendu :
# Subject: CN=SRV-WEB-01 Squid SSL Bump CA, O=SOS Futur, ...
# Issuer:  CN=sio-SRV-AD-01-CA, DC=sio, DC=local
# Not After: [date dans ~2 ans]
# CA:TRUE
```

☑ **Issuer: CN=sio-SRV-AD-01-CA — Le certificat est bien signé par la PKI interne AD CS.**

Étape 10 — Déploiement des fichiers dans le répertoire Squid

```
# Copie du certificat signé dans le répertoire Squid
cp /tmp/squid-bump.pem /etc/squid/ssl_cert/squid-bump.crt

# Création du fichier combiné PEM (certificat + clé privée) requis par Squid
cat /etc/squid/ssl_cert/squid-bump.crt \
    /etc/squid/ssl_cert/squid-bump.key \
  > /etc/squid/ssl_cert/squid-bump-combined.pem

# Application des permissions sécurisées
chmod 640 /etc/squid/ssl_cert/squid-bump-combined.pem
chown root:proxy /etc/squid/ssl_cert/squid-bump-combined.pem

# Vérification cohérence clé privée / certificat (les deux hash doivent être
identiques)
openssl x509 -noout -modulus -in /etc/squid/ssl_cert/squid-bump.crt | openssl
md5
openssl rsa  -noout -modulus -in /etc/squid/ssl_cert/squid-bump.key  | openssl
md5
# Les deux lignes doivent afficher le même hash MD5
```

☑ **Les deux hash MD5 (clé + certificat) sont identiques — la paire clé/certificat est cohérente.**

Étape 11 — Mise à jour de la configuration Squid et redémarrage du service

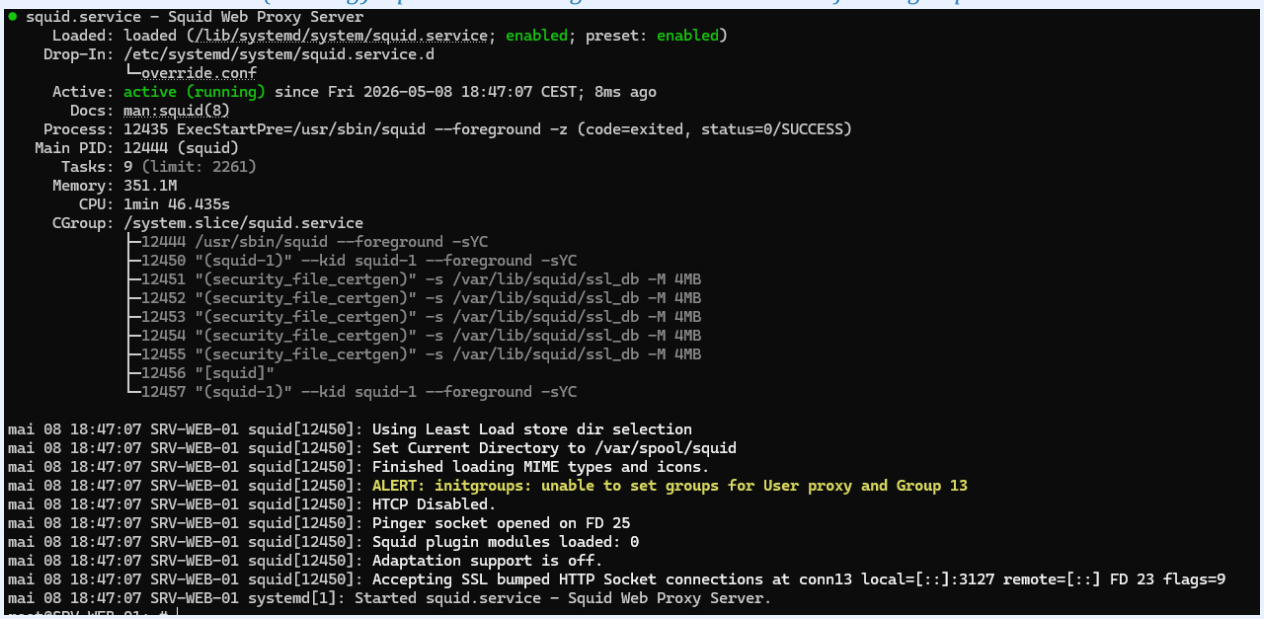
Vérifier que squid.conf référence bien le nouveau fichier de certificat combiné :

```
# Vérification de la directive ssl-bump dans squid.conf
grep -n 'ssl_bump\|tls-cert\|generate-host-certificates' /etc/squid/squid.conf

# Lignes attendues (exemple) :
# http_port 3127 ssl-bump \
#   tls-cert=/etc/squid/ssl_cert/squid-bump-combined.pem \
#   generate-host-certificates=on \
#   dynamic_cert_mem_cache_size=20MB

# Mettre à jour le chemin si nécessaire :
# sed -i 's|tls-cert=.*|tls-cert=/etc/squid/ssl_cert/squid-bump-combined.pem|'
\
```

```
#    /etc/squid/squid.conf

# Reconstruction du cache de certificats SSL Squid
/usr/lib/squid/security_file_certgen -c -s /var/spool/squid/ssl_db -M 20MB

# Test de la configuration avant redémarrage
squid -k parse
# Résultat attendu : 0 errors — Configuration valide

# Redémarrage du service Squid
systemctl restart squid

# Vérification du statut du service
systemctl status squid | grep -E 'Active|Loaded'
# Résultat attendu : Active: active (running)
```

☑ systemctl status squid → Active: active (running) — Squid redémarré avec le nouveau certificat PKI.

📂 CAPTURE D'ÉCRAN N°4 — Terminal SRV-WEB-01 — Sortie de 'systemctl status squid' affichant 'Active: active (running)' après redémarrage avec le nouveau certificat signé par AD CS.



V. TESTS ET VALIDATION — Preuve du SSL Bump fonctionnel depuis CL-WIN11-01

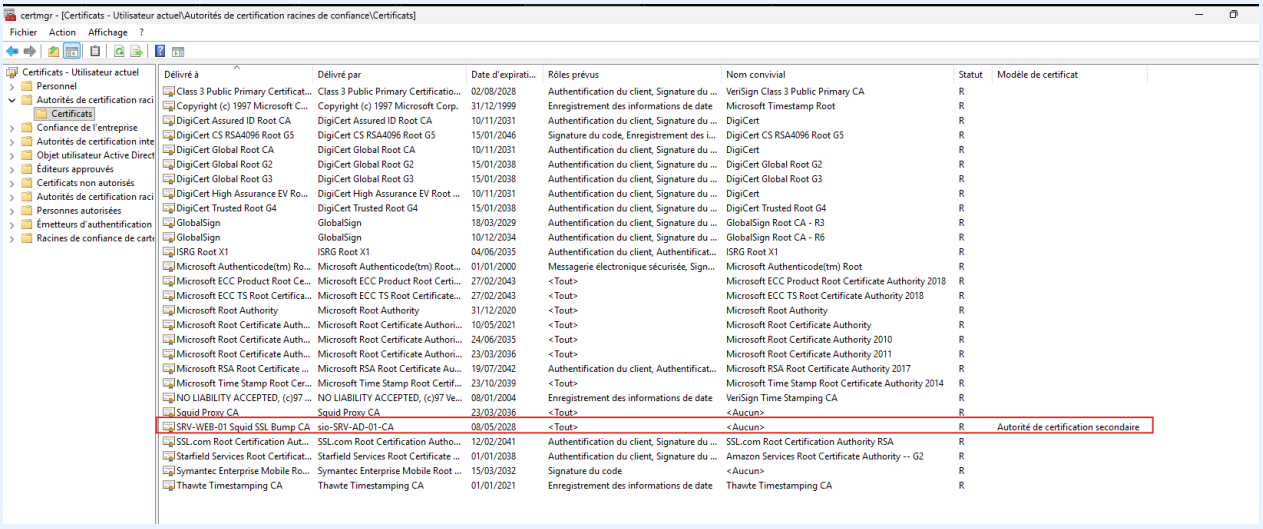
La validation doit prouver deux choses : que la navigation HTTPS fonctionne sans alerte de sécurité, et que le certificat présenté au navigateur est bien signé par la PKI interne sio.local — preuve irréfutable que l'interception SSL Bump est opérationnelle avec le nouveau certificat.

Étape 12 — Vérification que le certificat racine PKI est bien présent sur CL-WIN11-01

Navigation : CL-WIN11-01 — Gestionnaire de certificats (certmgr.msc)

13. Ouvrir certmgr.msc (Win+R → certmgr.msc).
14. Naviguer dans Trusted Root Certification Authorities > Certificates.
15. Vérifier la présence du certificat racine de la PKI interne (CN = sio-SRV-AD-01-CA ou similaire).
16. Si absent : forcer l'application de la GPO avec gpupdate /force en PowerShell Administrateur.

CAPTURE D'ÉCRAN N°5 — CL-WIN11-01 — certmgr.msc — Dossier 'Trusted Root Certification Authorities' affichant le certificat racine 'sio-SRV-AD-01-CA'. Preuve que la chaîne de confiance PKI est déployée.



Étape 13 — Navigation HTTPS et vérification du chemin de certification

Navigation : CL-WIN11-01 — Navigateur Web (Microsoft Edge ou Google Chrome) — Proxy configuré sur 10.11.3.2:3127

17. Ouvrir Microsoft Edge ou Chrome.
18. Accéder à https://www.google.fr.
19. Vérifier l'absence d'alerte de sécurité (pas de page rouge 'Votre connexion n'est pas privée').
20. Cliquer sur le cadenas (🔒) dans la barre d'adresse.
21. Cliquer sur 'La connexion est sécurisée' puis sur 'Informations sur le certificat' (ou l'icône certificat).
22. Dans l'onglet Chemin de certification (Certification Path), vérifier la chaîne :

Niveau	Certificat attendu	Rôle
Racine (niveau 1)	**sio-SRV-AD-01-CA**	Autorité de Certification racine AD CS (PKI interne SOS Futur)
Intermédiaire (niveau 2)	**SRV-WEB-01 Squid SSL Bump CA**	Certificat SSL Bump signé par AD CS — déployé sur Squid
Feuille (niveau 3)	www.google.fr	Certificat généré à la volée par Squid pour le site réel

☑ **Navigation HTTPS sur google.fr sans alerte — Cadenas vert/sécurisé affiché dans la barre d'adresse.**

☑ **Chemin de certification : sio-SRV-AD-01-CA → SRV-WEB-01 Squid SSL Bump CA → www.google.fr — SSL Bump opérationnel avec certificat PKI interne.**

Étape 14 — Vérification dans les logs Squid — Confirmation de l'interception HTTPS

Navigation : SRV-WEB-01 — Terminal SSH (root)

```
# Vérification en temps réel des logs d'accès Squid
tail -f /var/log/squid/access.log | grep 'CONNECT\|200'

# Lignes attendues lors de la navigation sur google.fr :
# 1715000000.000  200 TCP_TUNNEL/200 0 CONNECT www.google.fr:443 ...
# (ou TCP_MISS pour les requêtes interceptées et filtrées)

# Vérification du certificat actif dans Squid
openssl s_client -connect 10.11.3.2:3127 \
  -proxy 10.11.3.2:3127 -servername www.google.fr 2>/dev/null \
  | openssl x509 -noout -issuer -subject 2>/dev/null
# Résultat attendu :
# subject=CN=www.google.fr
# issuer=CN=SRV-WEB-01 Squid SSL Bump CA, O=SOS Futur
```

VI. BILAN ET ARGUMENTAIRE POUR L'ORAL

Étape	Action	Résultat	Statut
CSR Debian	openssl req — clé 4096 + extensions CA:TRUE	squid-bump.csr généré	☑
Signature PKI	certsrv — modèle SubCA — Issuer: sio-SRV-AD-01-CA	squid-bump.cer signé	☑
Déploiement	Hash MD5 cohérent — squid.conf mis à jour	Squid active (running)	☑
Validation	Cadenas navigateur — Chemin PKI interne affiché	SSL Bump opérationnel	☑
Logs Squid	access.log — CONNECT/TCP_MISS vers HTTPS	Interception confirmée	☑

Conclusion technique

- Cette procédure démontre la maîtrise de l'intégration Linux/Windows : génération OpenSSL sur

Debian, soumission à une PKI Windows AD CS, et déploiement sur Squid — compétence transversale clé du profil SISR.

- L'utilisation de la PKI interne AD CS élimine le principal frein à l'adoption du SSL Bump en entreprise : les alertes de sécurité navigateur. Le déploiement automatique du certificat racine via GPO rend l'inspection HTTPS totalement transparente pour les utilisateurs du domaine sio.local.

- La chaîne de confiance visible dans le chemin de certification (sio-SRV-AD-01-CA → Squid CA → site) constitue une preuve formelle et auditable du fonctionnement du mécanisme.

- Pour une mise en production robuste : automatiser le renouvellement du certificat Squid via certreq et une tâche cron, et surveiller la date d'expiration via Zabbix (item cert.expiry).