

Incident 8 ★ ★ ★ — Proxy : Certificat SSL supprimé sur PC-CLIENT-1

1. Contexte

Le certificat SSL `CN=Proxy-SIO` est déployé sur les postes clients via GPO pour permettre le SSL Bumping de Squid. Si ce certificat est supprimé, Edge affiche des erreurs de certificat non reconnu pour tous les sites HTTPS.

Paramètre	Valeur
Certificat	CN=Proxy-SIO
Magasin	Autorités de certification racines de confiance
Déployé via	GPO Proxy Squid

2. Situation initiale — Infrastructure fonctionnelle

2.1 Certificat présent sur PC-CLIENT-1

Depuis PC-CLIENT-1, ouvrir un CMD et taper `certutil -store Root | findstr "Proxy-SIO"`

Résultat attendu : CN=Proxy-SIO affiché.

3. Simulation de l'incident

3.1 Suppression du certificat

Depuis PC-CLIENT-1, ouvrir un CMD en administrateur et taper `certutil -delstore Root "Proxy-SIO"`

4. Constat de l'incident

4.1 Erreur certificat dans Edge

Depuis PC-CLIENT-1, tenter de naviguer sur n'importe quel site HTTPS.

Résultat attendu : Edge affiche une erreur de certificat non reconnu — NET: :ERR_CERT_AUTHORITY_INVALID

4.2 Vérification du certificat

Depuis PC-CLIENT-1, ouvrir un CMD et taper `certutil -store Root | findstr "Proxy-SIO"`

Constat : Aucun résultat — le certificat est absent.

5. Diagnostic

5.1 Vérification de la connectivité réseau

Depuis PC-CLIENT-1, ouvrir un CMD et taper `ping 10.11.89.2`

Constat : Ubuntu3-DMZ répond — problème de certificat et non réseau.

5.2 Vérification du service Squid

Depuis la console Ubuntu3-DMZ, taper `sudo systemctl status squid`

Constat : Squid actif — problème côté client uniquement.

6. Résolution

6.1 Réinstallation du certificat via GPO

Depuis PC-CLIENT-1, ouvrir un CMD et taper `gpupdate /force`

Le certificat doit être redéployé automatiquement via la GPO Proxy Squid.

6.2 Si le certificat n'est pas redéployé automatiquement

Installer le certificat manuellement :

1. Télécharger le certificat depuis `http://10.11.89.2/squid-ca.crt`
2. Depuis PC-CLIENT-1, ouvrir un CMD en administrateur et taper `certutil -addstore -f Root "C:\Users\Administrateur\Downloads\squid-ca.crt"`

7. Validation

7.1 Certificat présent

Depuis PC-CLIENT-1, ouvrir un CMD et taper `certutil -store Root | findstr "Proxy-SIO"`

Résultat attendu : CN=Proxy-SIO affiché.

8. Tableau de synthèse

Étape	Action	Résultat
Constat	Erreur certificat dans Edge	Certificat absent
Diagnostic 1	Ping 10.11.89.2	Réseau OK
Diagnostic 2	systemctl status squid	Squid actif
Diagnostic 3	certutil -store Root	Certificat absent
Résolution 1	gpupdate /force	Certificat redéployé via GPO
Résolution 2	Installation manuelle si nécessaire	Certificat installé
Validation	certutil -store Root Proxy-SIO	Incident résolu 