Incident 10 ⭐⭐⭐⭐⭐ — Proxy : Corruption totale (passerelle + Squid + GPO + règle pfSense + mauvais port)

1. Contexte

Cet incident simule une panne catastrophique combinant 5 problèmes simultanés sur l'ensemble des composants du proxy.

> **Note de sécurité :** Pour éviter tout risque sur pfSense1, on désactive la règle de blocage au lieu de la supprimer — c'est réversible en un clic. De même on change le port proxy dans la GPO (3128 → 3129) plutôt que de toucher la config réseau de pfSense1 ce qui serait trop risqué.

Problème	Cause simulée
Mauvaise passerelle Ubuntu3-DMZ	10.11.89.1 → 10.11.89.99
Service Squid arrêté	systemctl stop squid
GPO Proxy Squid supprimée	Suppression dans GPMC
Règle pfSense désactivée	Règle blocage HTTPS désactivée
Mauvais port dans GPO recréée	3128 → 3129

---

2. Situation initiale — Infrastructure fonctionnelle

2.1 Passerelle correcte

Depuis la console Ubuntu3-DMZ, taper `ip route`

> **Résultat attendu :** `default via 10.11.89.1`

2.2 Squid actif

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

> **Résultat attendu :** active (running)

2.3 GPO présente

Depuis WSERV1, ouvrir `gpmc.msc`

> **Résultat attendu :** GPO **Proxy Squid** liée à l'OU SIO.

2.4 Règle pfSense active

Depuis pfSense1 → **Pare-feu** → **Règles** → **LAN**

> **Résultat attendu :** Règle blocage HTTPS active.

2.5 Proxy correct dans Edge

Depuis PC-CLIENT-1, ouvrir `edge://policy`

> **Résultat attendu :** ProxyServer `10.11.89.2:3128`

---

3. Simulation de l'incident

3.1 Mauvaise passerelle

Depuis la console Ubuntu3-DMZ, taper `sudo nano /etc/netplan/01-netcfg.yaml`

Remplacer `10.11.89.1` par `10.11.89.99` puis `sudo netplan apply`

3.2 Arrêt Squid

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

3.3 Suppression GPO

Depuis WSERV1, `gpmc.msc` → supprimer **Proxy Squid**

3.4 Désactivation règle pfSense

Depuis pfSense1 → **Pare-feu** → **Règles** → **LAN** →
désactiver règle **Bloquer HTTPS direct** →
Appliquer les changements

3.5 Recréation GPO avec mauvais port

Depuis WSERV1, recréer la GPO **Proxy Squid** mais avec
le port `3129` au lieu de `3128`

Depuis PC-CLIENT-1, taper `gpupdate /force`

---

4. Constat de l'incident

4.1 Situation sur PC-CLIENT-1

Depuis PC-CLIENT-1, ouvrir `edge://policy`

> **Constat :** ProxyServer affiche `10.11.89.2:3129` — mauvais port. Navigation impossible malgré la GPO présente.

---

5. Diagnostic

5.1 Vérification proxy dans Edge

Depuis PC-CLIENT-1, ouvrir `edge://policy`

> **Constat :** Port `3129` incorrect. Premier problème identifié.

5.2 Vérification connectivité

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

> **Constat :** Ubuntu3-DMZ répond — réseau OK.

5.3 Vérification service Squid

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

> **Constat :** Squid arrêté. Deuxième problème identifié.

5.4 Vérification passerelle

Depuis la console Ubuntu3-DMZ, taper `ip route`

> **Constat :** `default via 10.11.89.99` — passerelle incorrecte. Troisième problème identifié.

5.5 Vérification règles pfSense

Depuis pfSense1 → **Pare-feu** → **Règles** → **LAN**

> **Constat :** Règle blocage HTTPS désactivée.
> Quatrième problème identifié.

5.6 Vérification port GPO

Depuis WSERV1, `gpmc.msc` → modifier GPO **Proxy Squid**

> **Constat :** Port configuré à `3129` au lieu de `3128`.
> Cinquième problème identifié.

---

6. Résolution

Ordre de résolution : Passerelle → Squid → pfSense → GPO port

6.1 Correction passerelle

Depuis la console Ubuntu3-DMZ, taper `sudo nano /etc/netplan/01-netcfg.yaml`

Remplacer `10.11.89.99` par `10.11.89.1` puis `sudo netplan apply`

6.2 Redémarrage Squid

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

6.3 Réactivation règle pfSense

Depuis pfSense1 → **Pare-feu** → **Règles** → **LAN** →
réactiver règle **Bloquer HTTPS direct** →
Appliquer les changements

6.4 Correction port GPO

Depuis WSERV1, `gpmc.msc` → modifier GPO **Proxy Squid** :

1. Corriger **Adresse serveur proxy** → `10.11.89.2:3128`
2. Corriger **Paramètres proxy** → `{"mode":"fixed_servers","server":"10.11.89.2:3128"}`
3. Cliquer sur **OK**

6.5 Forcer mise à jour GPO

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

---

7. Validation

7.1 Proxy correct dans Edge

Depuis PC-CLIENT-1, ouvrir `edge://policy`

> **Résultat attendu :** ProxyServer `10.11.89.2:3128`.

7.2 Logs Squid actifs

Depuis la console Ubuntu3-DMZ, taper `sudo tail -f /var/log/squid/access.log`

> **Résultat attendu :** Requêtes TCP_DENIED visibles.

7.3 Squid actif + passerelle correcte

Depuis la console Ubuntu3-DMZ :

`sudo systemctl status squid` → active (running)

`ip route` → `default via 10.11.89.1`

---

8. Tableau de synthèse

Étape	Action	Résultat
Constat	Navigation impossible + port 3129	Panne catastrophique
Diagnostic 1	edge://policy	Port 3129 incorrect
Diagnostic 2	Ping 10.11.89.2	Réseau OK
Diagnostic 3	systemctl status squid	Squid arrêté
Diagnostic 4	ip route	Passerelle incorrecte
Diagnostic 5	Règles LAN pfSense1	Règle blocage désactivée
Diagnostic 6	GPO Proxy Squid	Port 3129 dans GPO
Résolution 1	Correction passerelle → 10.11.89.1	Routage restauré
Résolution 2	systemctl start squid	Squid redémarré
Résolution 3	Réactivation règle pfSense	Blocage direct restauré
Résolution 4	Correction port GPO → 3128	GPO corrigée
Résolution 5	gpupdate /force	GPO appliquée

Étape	Action	Résultat
Validation	Proxy OK + Squid actif + pfSense OK	Incident résolu ✅