Incident 1 ⭐ — Proxy : Service Squid arrêté

1. Contexte

Squid est le service proxy filtrant installé sur Ubuntu3-DMZ.
Si ce service est arrêté, tous les clients perdent l'accès internet car pfSense1 bloque tout trafic HTTP/HTTPS direct et force le passage par le proxy.

Paramètre	Valeur
VM concernée	Ubuntu3-DMZ
IP	10.11.89.2/28
Passerelle	10.11.89.1 (pfSense1 em2)
Port proxy	3128
Service	squid

---

2. Situation initiale — Infrastructure fonctionnelle

2.1 Service Squid actif

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

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

2.2 Proxy configuré dans Edge sur PC-CLIENT-1

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

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

2.3 Logs Squid actifs

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

> **Résultat attendu :** Requêtes TCP_DENIED visibles depuis `10.11.89.244` (PC-CLIENT-1).

---

3. Simulation de l'incident

3.1 Arrêt du service Squid

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

---

4. Constat de l'incident

4.1 Navigation impossible sur PC-CLIENT-1

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

> **Résultat attendu :** Erreur de connexion — le proxy ne répond plus, aucun site n'est accessible.

---

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 — le problème n'est pas réseau mais applicatif.

5.2 Vérification du service Squid

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

> **Constat :** Le service Squid est arrêté — c'est la cause de l'incident.

---

6. Résolution

6.1 Redémarrage du service Squid

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

Vérifier que le service est bien redémarré : `sudo systemctl status squid`

6.2 Vérifier le démarrage automatique

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

> **Résultat attendu :** enabled

---

7. Validation

7.1 Logs Squid actifs de nouveau

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

> **Résultat attendu :** Requêtes TCP_DENIED visibles —
> Squid filtre de nouveau le trafic.

---

8. Tableau de synthèse

Étape	Action	Résultat
Constat	Navigation impossible sur PC-CLIENT-1	Proxy inaccessible
Diagnostic 1	Ping 10.11.89.2	Réseau OK
Diagnostic 2	systemctl status squid	Service arrêté
Résolution 1	systemctl start squid	Service redémarré
Résolution 2	Vérification is-enabled	Démarrage auto OK
Validation	Logs Squid actifs	Incident résolu ✅