Incident 3 ⭐ ⭐ — Proxy : Mauvais DNS sur Ubuntu3-DMZ

1. Contexte

Squid utilise le DNS configuré sur Ubuntu3-DMZ pour résoudre les noms de domaine des requêtes des clients. Si le DNS est incorrect, Squid ne peut plus résoudre les noms et toutes les requêtes échouent — même si le service tourne.

Paramètre	Valeur normale
DNS correct	10.11.89.242 (WSERV1)
DNS incorrect simulé	10.11.89.99
Fichier de config réseau	`/etc/netplan/01-netcfg.yaml`

---

2. Situation initiale — Infrastructure fonctionnelle

2.1 DNS correct sur Ubuntu3-DMZ

Depuis la console Ubuntu3-DMZ, taper `cat /etc/resolv.conf`

> **Résultat attendu :** nameserver `10.11.89.242`

2.2 Service Squid actif

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

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

---

3. Simulation de l'incident

3.1 Modification du DNS

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

1. Localiser le champ `nameservers addresses`

2. Remplacer `10.11.89.242` par `10.11.89.99`
3. Enregistrer avec Ctrl+O puis Entrée, quitter avec Ctrl+X

Appliquer les changements : `sudo netplan apply`

---

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 — Squid ne peut plus résoudre les noms de domaine.

---

5. Diagnostic

5.1 Vérification de la connectivité vers le proxy

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 DNS.

5.2 Vérification du service Squid

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

> **Constat :** Squid tourne — le problème n'est pas le service mais la résolution DNS.

5.3 Vérification du DNS

Depuis la console Ubuntu3-DMZ, taper `cat /etc/resolv.conf`

> **Constat :** nameserver `10.11.89.99` — DNS incorrect.
> C'est la cause de l'incident.

---

6. Résolution

6.1 Correction du DNS

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

1. Remplacer `10.11.89.99` par `10.11.89.242`
2. Enregistrer avec Ctrl+O puis Entrée, quitter avec Ctrl+X

Appliquer les changements : `sudo netplan apply`

---

7. Validation

7.1 DNS correct

Depuis la console Ubuntu3-DMZ, taper `cat /etc/resolv.conf`

> **Résultat attendu :** nameserver `10.11.89.242`

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 —
> Squid filtre de nouveau le trafic.

---

8. Tableau de synthèse

Étape	Action	Résultat
Constat	Navigation impossible	Squid ne résout plus les noms
Diagnostic 1	Ping 10.11.89.2	Réseau OK
Diagnostic 2	systemctl status squid	Squid actif
Diagnostic 3	cat /etc/resolv.conf	DNS incorrect
Résolution	Correction DNS → 10.11.89.242	DNS restauré
Validation	Logs Squid actifs	Incident résolu ✅