Incident 5 ⭐ ⭐ ⭐ — Proxy : Mauvaise passerelle sur Ubuntu3-DMZ

1. Contexte

Ubuntu3-DMZ communique avec internet via la passerelle `10.11.89.1` (interface DMZ de pfSense1). Si la passerelle est incorrecte, Squid ne peut plus relayer les requêtes vers internet et tous les clients perdent l'accès.

Paramètre	Valeur normale
IP Ubuntu3-DMZ	10.11.89.2/28
Passerelle correcte	10.11.89.1
Passerelle incorrecte simulée	10.11.89.99

---

2. Situation initiale — Infrastructure fonctionnelle

2.1 Passerelle correcte sur Ubuntu3-DMZ

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

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

2.2 Logs Squid actifs

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

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

---

3. Simulation de l'incident

3.1 Modification de la passerelle

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

1. Localiser le champ `gateway4`

2. Remplacer `10.11.89.1` par `10.11.89.99`
3. Enregistrer avec Ctrl+O puis Entrée, quitter avec Ctrl+X

Appliquer : `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 relayer les requêtes.

---

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 la connectivité vers le proxy mais le routage depuis le proxy.

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.

5.3 Vérification de la passerelle

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

> **Constat :** `default via 10.11.89.99` — passerelle incorrecte. C'est la cause de l'incident.

---

6. Résolution

6.1 Correction de la passerelle

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

1. Remplacer `10.11.89.99` par `10.11.89.1`
2. Enregistrer avec Ctrl+O puis Entrée, quitter avec Ctrl+X

Appliquer : `sudo netplan apply`

---

7. Validation

7.1 Passerelle correcte

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

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

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.

---

8. Tableau de synthèse

Étape	Action	Résultat
Constat	Navigation impossible	Proxy ne relaie plus
Diagnostic 1	Ping 10.11.89.2	Ubuntu3-DMZ joignable
Diagnostic 2	systemctl status squid	Squid actif
Diagnostic 3	ip route	Passerelle incorrecte
Résolution	Correction passerelle → 10.11.89.1	Routage restauré
Validation	Logs Squid actifs	Incident résolu ✅