Incident 7 ⭐ ⭐ ⭐ — Proxy : Règle pfSense désactivée

1. Contexte

pfSense1 dispose d'une règle qui bloque tout trafic HTTP/HTTPS direct depuis les clients pour forcer le passage par le proxy Squid. Si cette règle est désactivée, les clients peuvent accéder directement à internet sans passer par le proxy — le filtrage ne fonctionne plus.

> **Note de sécurité :** On désactive la règle et non on la supprime — c'est réversible en un clic et évite tout risque de casser la configuration pfSense1.

Paramètre	Valeur
Pare-feu	pfSense1
Interface	LAN
Règle concernée	Bloquer HTTPS direct (port 443)

---

2. Situation initiale — Infrastructure fonctionnelle

2.1 Règles pfSense1 actives

Depuis PC-CLIENT-1, naviguer sur `https://10.11.89.241` puis aller dans **Pare-feu → Règles → LAN**

> **Résultat attendu :** Les règles de blocage HTTP/HTTPS direct sont actives.

2.2 Navigation bloquée sans proxy

Depuis PC-CLIENT-1 avec proxy désactivé manuellement dans Edge, tenter de naviguer.

> **Résultat attendu :** Accès bloqué par pfSense1.

---

3. Simulation de l'incident

3.1 Désactivation de la règle de blocage HTTPS

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

1. Localiser la règle **Bloquer HTTPS direct** (port 443)
2. Cliquer sur l'icône de désactivation
3. Cliquer sur **Appliquer les changements**

---

4. Constat de l'incident

4.1 Accès internet sans proxy possible

Depuis PC-CLIENT-1 avec proxy désactivé manuellement dans Edge,
tenter de naviguer sur `https://www.google.com`

> **Constat :** Google s'affiche — les clients contournent
> le proxy et accèdent directement à internet.
> Le filtrage ne fonctionne plus.

---

5. Diagnostic

5.1 Vérification du service Squid

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

> **Constat :** Squid est actif — le problème ne vient pas
> de Squid mais de pfSense1.

5.2 Vérification des règles pfSense1

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

> **Constat :** La règle de blocage HTTPS direct est désactivée
> — c'est la cause de l'incident.

---

6. Résolution

6.1 Réactivation de la règle de blocage HTTPS

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

1. Localiser la règle **Bloquer HTTPS direct**
2. Cliquer sur l'icône d'activation
3. Cliquer sur **Appliquer les changements**

---

7. Validation

7.1 Accès direct bloqué de nouveau

Depuis PC-CLIENT-1 avec proxy désactivé manuellement dans Edge, tenter de naviguer sur `https://www.google.com`

> **Résultat attendu :** Accès bloqué par pfSense1.

---

8. Tableau de synthèse

Étape	Action	Résultat
Constat	Accès internet sans proxy possible	Règle pfSense désactivée
Diagnostic 1	systemctl status squid	Squid actif
Diagnostic 2	Règles LAN pfSense1	Règle HTTPS désactivée
Résolution	Réactivation règle blocage HTTPS	Filtrage restauré
Validation	Accès direct bloqué	Incident résolu ✅