**Accès autorisé uniquement à l'interface WAN publique (pas de LAN ni de scan réseau),**

**Conformité impérative (aucune prise d’initiative non validée),**

**Capacité d’agir via console Infomaniak *et terminal root Ubuntu* uniquement**.

**Mémo technique – Supervision pfSense par SNMP (sans accès LAN)**

**Auteur :** [Benoît, Auditeur externe – Projet Monitoring Jitsi/Infomaniak]  
**Date :** 16 juillet 2025  
**Objet :** Justification et sécurisation d’une requête d’ouverture SNMP UDP/161 pour supervision externe  
**Infrastructure :** pfSense en frontal Infomaniak, Grafana/Prometheus/Telegraf en surveillance distante.

**1.Objectif**

Permettre à **Telegraf** (installé sur l’instance Ubuntu publique 37.156.46.238) de superviser l’état du routeur pfSense via le protocole **SNMP** (port UDP 161).

Cette supervision est cruciale pour assurer la **visibilité du cœur réseau** (passerelle/sécurité), dans un contexte **RGPD, ISO 27001, et NIS2**.

**2. Contraintes imposées**

* **Accès LAN proscrit** : aucune interaction directe avec les IP locales 192.168.x.x, 191.x.x.x, etc.
* **Aucun outil de scan autorisé** : nmap, netstat, arp, etc. → interdits.
* **Console Infomaniak** = seule interface autorisée pour les actions réseau.
* **Scripts** & configurations uniquement sur la VM Ubuntu publique.

**3. État constaté**

* UDP/161 semble théoriquement ouvert côté Infomaniak (console cloud) → **non bloqué en amont**.
* Pourtant, Telegraf retourne :  
  read udp ... recvfrom: connection refused   
  ➤ preuve que **pfSense refuse** les requêtes SNMP sur son interface WAN (probablement non activé, ou mal configuré côté daemon/service).

**4. Action recommandée (strictement WAN & réversible)**

1. **Activer SNMP sur pfSense** *(interface WAN uniquement)*  
   ➤ via l’interface WebAdmin pfSense ou fichier XML de config (si console cloud autorise son injection).
2. **Définir une communauté SNMP restreinte** :
   * Exemple **: prom-readonly**
   * Niveau : **lecture seule**
3. **Créer une règle firewall WAN dans pfSense** :
   * Protocole : UDP
   * Port destination : 161
   * Source : **37.156.46.238**
   * Action : ***Pass***
   * Schedule : *(optionnel : fenêtre horaire de supervision)*
4. **Option sécurisée supplémentaire (si autorisée)**  
   ➤ Bind SNMP uniquement à WAN (désactiver LAN/loopback)

**5. Risque si aucune ouverture**

* **Perte de visibilité complète sur pfSense** (bande passante, latence, CPU, logs, reboot),
* **Monitoring partiel** dans Grafana (limité aux métriques OS/containers),
* **Non-conformité partielle RGPD/NIS2** sur traçabilité du pare-feu frontal.

**6. ✅ Reversibilité**

Toutes les modifications sont :

* Documentables,
* Réversibles à tout moment,
* Activables pour audit puis désactivables à l’issue.