Memo technique - Supervision pfSense via SNMP (interface WAN uniquement)

Auteur : Benoit

Date : 16 juillet 2025

Contexte : Projet Monitoring Jitsi/Infomaniak

Instance publique : 37.156.46.238

Objectif

Activer un canal de supervision SNMP pour observer les metriques reseau de pfSense sans acces LAN ni outils d'analyse interdits (nmap, netstat, etc.).

Contraintes de securite

- Acces LAN interdit
- Acces SNMP uniquement par l'interface WAN
- Acces console uniquement via interface Infomaniak
- Toute configuration doit etre reversible

Etat actuel

- Port UDP/161 semble autorise depuis l'exterieur (console Infomaniak OK)
- Mais telegraf retourne connection refused => pfSense refuse le dialogue SNMP

Action recommandee

1. Activer SNMP sur pfSense (interface WAN uniquement)
2. Definir une communaute securisee : prom-readonly
3. Creer une regle firewall sur pfSense :
   - Source : 37.156.46.238
   - Destination : Port UDP 161
   - Interface : WAN

4. (Option) Restreindre SNMP a l'interface WAN uniquement

Risques si inaction

- Grafana/Prometheus perd toute visibilite sur pfSense

- Aucune tracabilite reseau possible (logs, metriques, uptime, etc.)

- Non-conformite partielle RGPD / ISO 27001 / NIS2

Reversibilite

Chaque action peut etre desactivee sans impact :

- SNMP desactivable

- Regle firewall WAN supprimable

- Community SNMP reinitialisable