Table of Contents

ePDG Monitoring

Integrated VoWiFi Gateway Monitoring System (ePDG)

Review of the decision

The VAS Experts ePDG Monitoring system provides full operational control of the **fast-epdg** component, the VoWiFi (Voice over WiFi) gateway operating according to 3GPP TS 29.273 and TS 24.302. The gateway provides secure transmission of voice and packet traffic through untrusted Wi-Fi channels with IPSec / IKEv2 tunneling and integration with the EPC core through SWu, SWm, SWx, S2b, S6b interfaces.

The solution provides a single monitoring platform for the mobile operator's operational services — from the IPSec SA (L3 security) level to the KPI of VoWiFi subscriber experience.

Key advantages

- **Real-time monitoring** — update metrics every 10-15 seconds, directly display the status of IKE SA / Child SA and GTP tunnels in NOC dashboards without delayed aggregation (hereinafter NOC — Network Operation Center, network management center).
- **Proactive detection of anomalies** — 20+ alarms with automatic escalation in importance. PGW/AAA inaccessibility, increased IKEv2 delays, and an increase in EAP-AKA errors are detected before subscribers notice problems with calls.
- **Open integration interfaces** — Prometheus, SNMP v2c, Alertmanager webhooks, Grafana support. Integration into the existing NMS/OSS infrastructure without vendor binding.
- **Minimum external dependencies at the plugin level** — built-in `/metrics` endpoint in fast-epdg, without Java, without JMX, without external agents.
- **Coverage of the entire SWu → S2b** stack — IKEv2 (SWu), Diameter SWm/SWx/S6b, GTPv2-C (S2b) and GTP-U data plane — all in one place. The 33 metrics cover control plane and data plane.

Four-level monitoring architecture

Level	Component	Technology
Collection	Built-in `/metrics` endpoint fast-epdg	Prometheus text format over HTTP
Storage	Prometheus TSDB	Local storage, 15-day storage by default
Visualization	Grafana + JSON support	Autodownload 4 dashboards
Alerting	Alertmanager + SNMP Trap Sender	PromQL rules → webhook → SNMP v2c trap

Quantitative review by category

Category	Number of metrics	Survey interval	Key indicators
Config	2	10 sec	Configuration status, reload counter
Network	1	10 sec	Node connection status (PGW/AAA/HSS)

Category	Number of metrics	Survey interval	Key indicators
IKEv2 (SWu)	3	10 sec	Reports by type (IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA), delay diagram, errors
GTPv2-C (S2b)	4	10 sec	Messages (Create/Modify/Delete Session), delays, errors, relays
GTP-U data plane	3	10 sec	Packets/bytes, tunneling errors
Diameter (SWm/SWx/S6b)	5	10 sec	Command code messages (DER/DEA, MAR/MAA, AAR/AAA), delays, errors, watchdog, connection status
Service KPI	4	10 sec	Percentage of successful attempts, duration histogram, service availability, uptime
Session State	4	10 sec	IKE SA, Child SA, GTP sessions, all users
Application	3	10 sec	Number of streams, memory, log messages by levels
System	4	10 sec	CPU recycling, memory, memory disposal, open FD
Total	**33 metrics**		

Alarm categories

Criticism	Alarma	Description	Reaction
Critical	`ePDG_Service_Down`, `ePDG_High_Attach_Failure_Rate`, `ePDG_PGW_Unreachable`, `ePDG_AAA_Unreachable`, `ePDG_Diameter_Watchdog_Timeout`	Component is unavailable, widespread connection failures, nodes are unavailable	Immediate escalation: Email + SNMP Trap + Webhook. Repeat every hour
Warning	`ePDG_High_IKEv2_Latency`, `ePDG_High_GTP_Latency`, `ePDG_High_IKEv2_Error_Rate`, `ePDG_High_GTP_Error_Rate`, `ePDG_High_Memory_Usage`, `ePDG_High_CPU_Usage`, `ePDG_Low_Disk_Space`, `ePDG_High_Error_Log_Rate`	Performance degradation, resource anomalies	Email. Resend every 4 hours. Suppressed if a “Critical” status is present on the same component