VAS Experts ITG

Stingray PCEF (Policy and Charging Enforcement Function)

About VAS Experts

VAS Experts is a telecom software developer. Since 2013, we have completed **over 2000 installations** worldwide.

Our team has **over 25 years work experience** in telecommunication software development and wide knowledge in technologies.

20M+
users

More than
35 Tbps

Latest Installations:

- Middle East
- Europe
- CIS
- Africa
- South America
- Asia-Pacific

Our products

Stingray Service Gateway (SSG) — multifunctional platform for traffic management

For Internet Service Providers:

DPI

QoS-based traffic management, filtering by black and white lists

BNG/BRAS

Scalable and Cost-Effective Software Gateway

AntiDDoS

Protecting the operator's network from cyberattacks

QoE analytics

Traffic Monitoring and Analysis System

CG-NAT

Providing transparent network address and protocol translation

VEOS

Operating system

Our products

Stingray Service Gateway (SSG) — multifunctional platform for traffic management

For mobile operators:

PGW

An intelligent gateway that provides traffic control within the EPC architecture

PCEF

Flexible pricing based on various conditions in accordance with PCRF requirements

EPDG

Solution for launching Wi-Fi Calling (VoWiFi)

Stingray PCEF – Purpose

Policy and Charging Enforcement Function is an integral and important part of the EPC (Evolved Packet Core) architecture in 4G/LTE and 5G networks. It facilitates interaction with the telecom operator’s PCRF and OCS via their standard interfaces and enforces specified policies based on DPI (UPF) capabilities.

Designed in accordance with the TDF (Traffic Detection Function) concept within the 3GPP framework.

- Receives policies for the subscriber
- Receives traffic quotas for the subscriber, updating them when exhausted
- Notifies operator systems about events in the subscriber's traffic
- Enriches subscriber data from other systems via API when certain policies are triggered
- Adapts operator policies for execution on DPI, and monitors their enforcement

Advantages of VAS Experts PCEF

- At the core of the solution is **single high-performance, in-house-developed DPI engine**, operating as the user plane in the roles of DPI, BNG, CG-NAT and mobile UPF/PGW-U. The control plane (PCEF, PGW-C/SMF, ePDG) is modular and integrates via standard 3GPP interfaces. This allows the solution to be developed and scaled without replacing hardware.
- Ensures high quality of service through fast rollout of new tariff plans, data usage control, and policy compliance.
- Supports all modern interfaces and has been tested with billing systems ensuring simple integration.
- In-house development with customization capability.

Standards compliance

Mechanism		Specification
PCEF (Gi/SGi, TDF)	PCC-architecture, QCI / ARP, TDF / ADC	TS 23.203 (sec. 6.1.7.2)
	Gx — CCR/CCA, RAR, Charging-Rule-Install, QoSInformation, Flow-Information, detection of applications	TS 29.212 (sec. 5.3, 5.6, 4.5)
	Gy — online charging, Granted/UsedService-Unit, Reporting-Reason	TS 32.299; RFC 4006
	Subscriber ↔ IP binding — RADIUS Accounting on Gi/SGi	TS 29.061 sec. 16
	Basic Diameter (peers, fault tolerance, Termination-Cause)	RFC 6733
	Offline charging (Gz, CDR ASN.1 BER/XER/JER + SFTP)	TS 32.240 (sec. 4.1.1, 4.3.1, 4.4.1, 4.5.1)
PGW/SMF+UPF	Plane separation (CUPS); PFCP (N4 / Sx); S5/S8	TS 23.214; TS 29.244
	Dedicated bearers; GTP-C Create/Update/ Delete Bearer	TS 23.401 sec. 5.4; TS 29.274 sec. 7.2.3–7.2.4
	Rx (IMS media → QoS), media → QCI	TS 29.214; TS 29.213 sec. 6.3

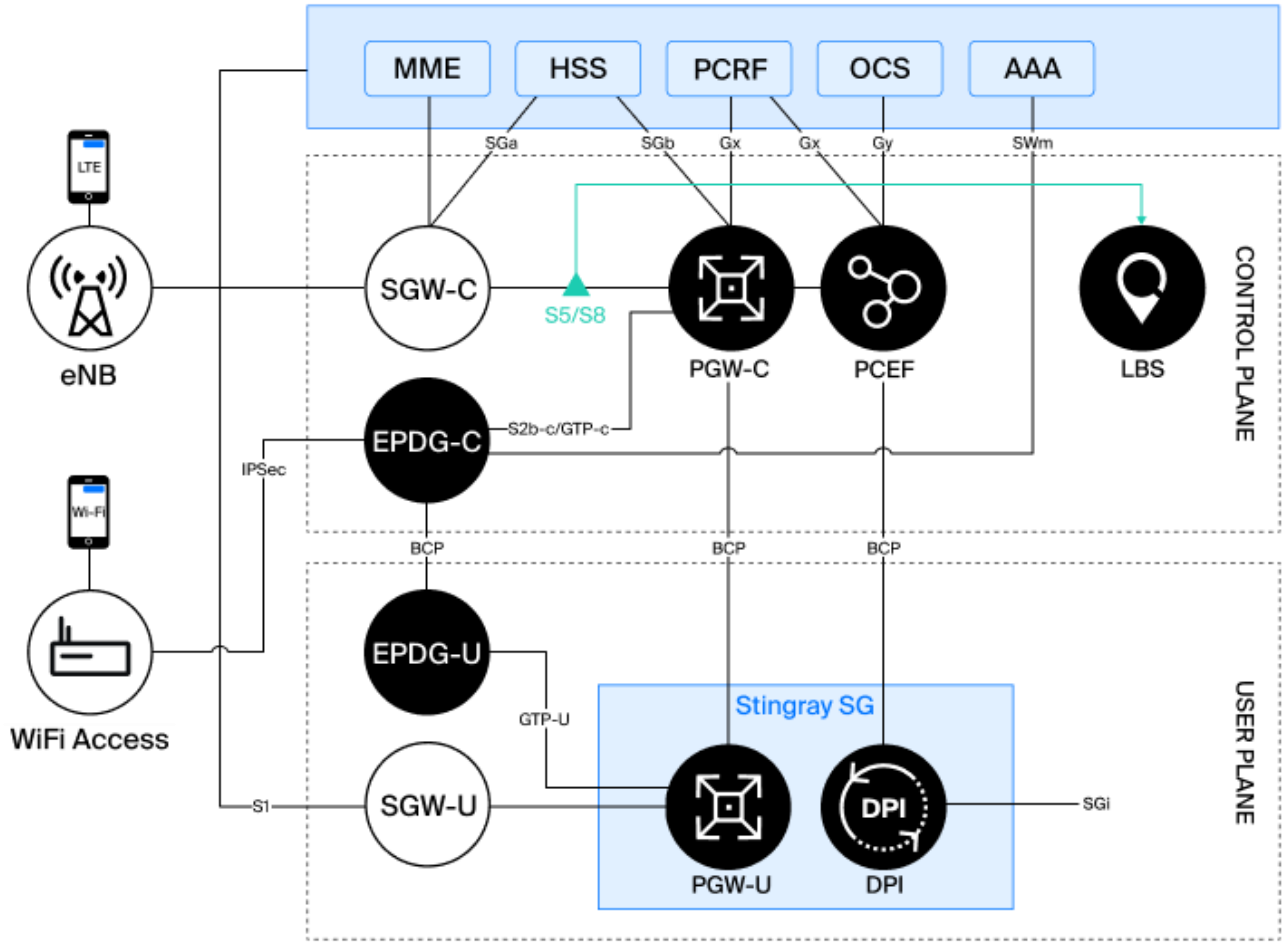
Standards compliance is a basic requirement for software.

In Stingray PCEF the correct behavior of adjacent nodes (PCRF, OCS, HSS, gateway) is accepted and processed; if the protocol is violated, the platform returns the error code defined by the standard.

Solution Architecture

CUPS – Control and User Plane Separation – a concept, whereby the control and user planes in communication network are separated.

Network management and data transfer take place on different physical and logical elements.

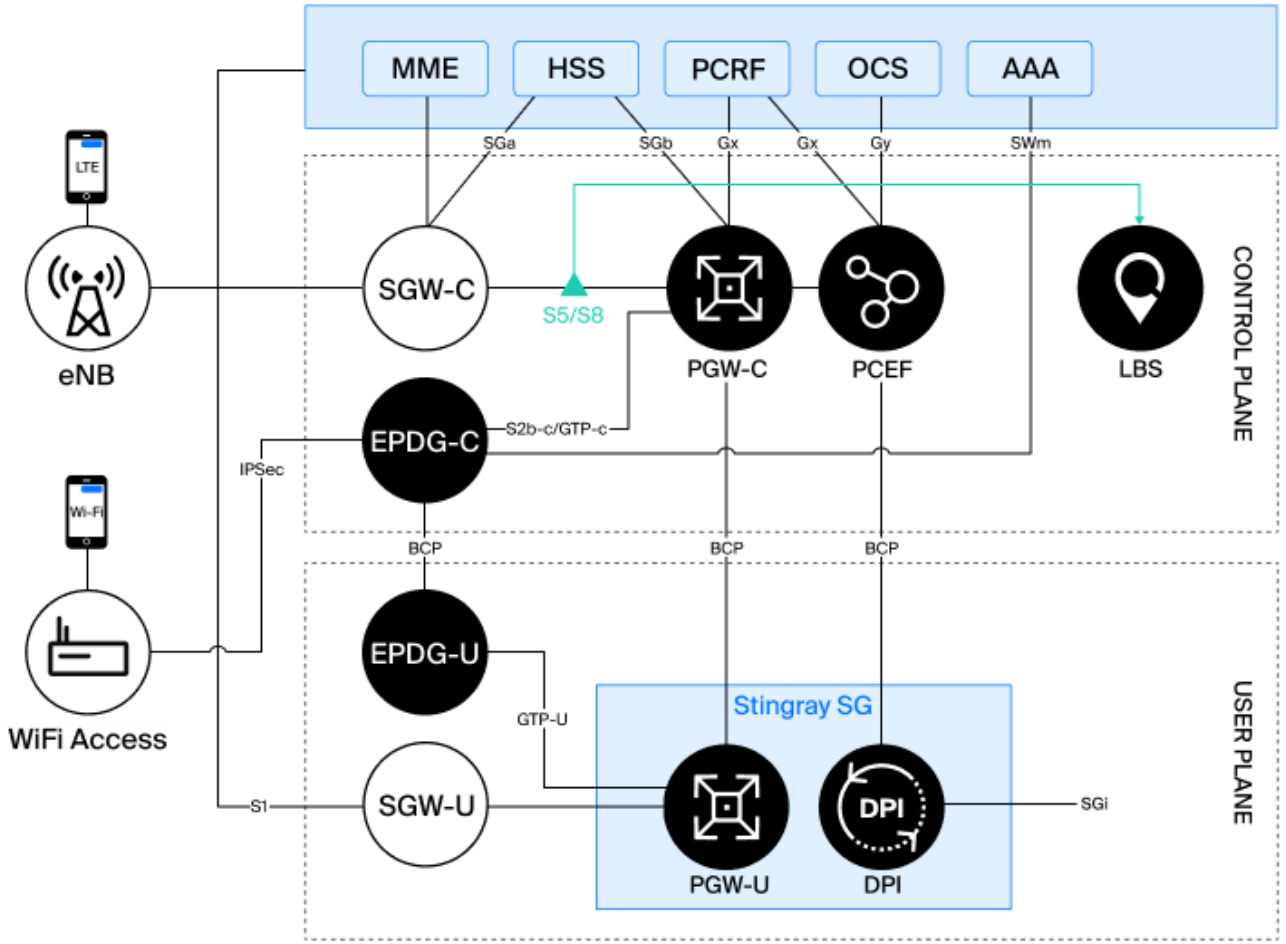


Benefits:

+ flexibility and load management
+ scalability
+ performance

Solution Architecture

- **Control Plane –** handles all the logic: where traffic comes from and goes, and which scenarios and rules are applied
- **User Plane –** is responsible for processing all traffic at maximum speed with minimal latency
- **Result of separation –** high load does not break the system's logic, and complex logic does not degrade system performance

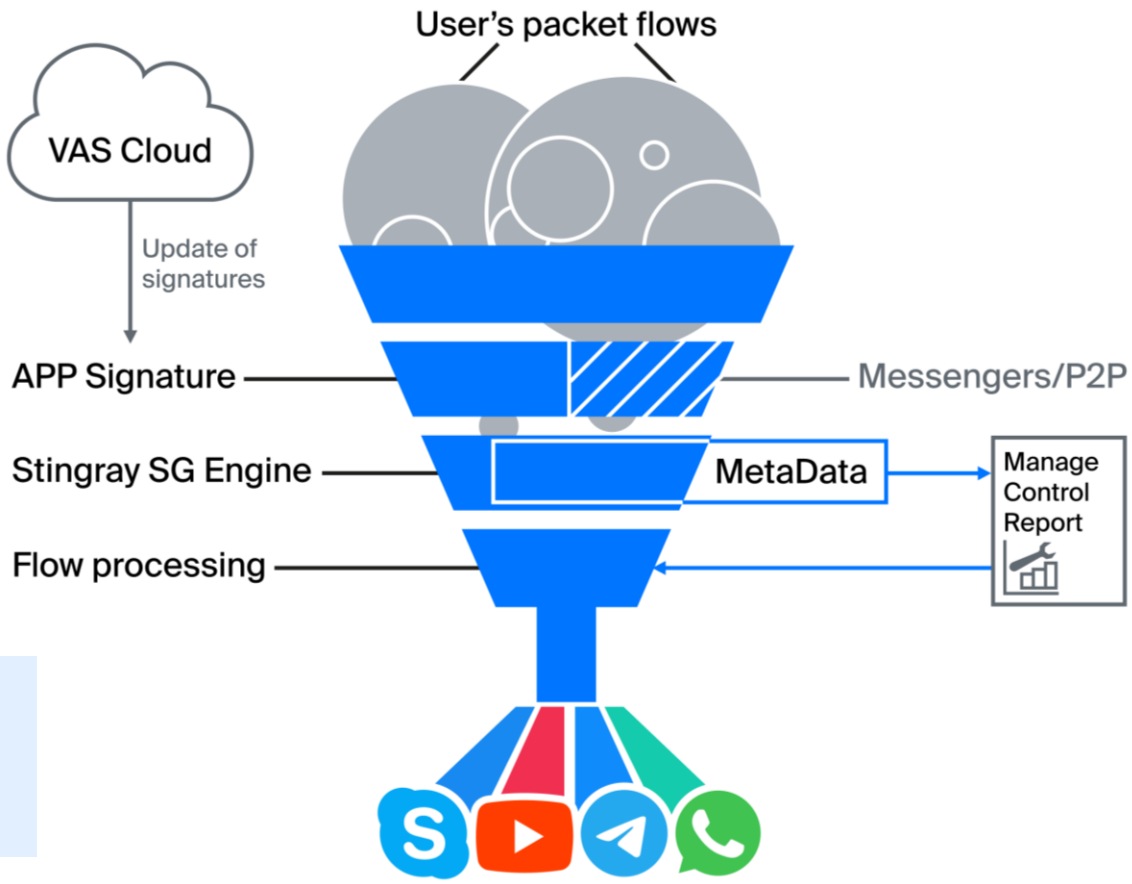


DPI-engine at the core of PCEF

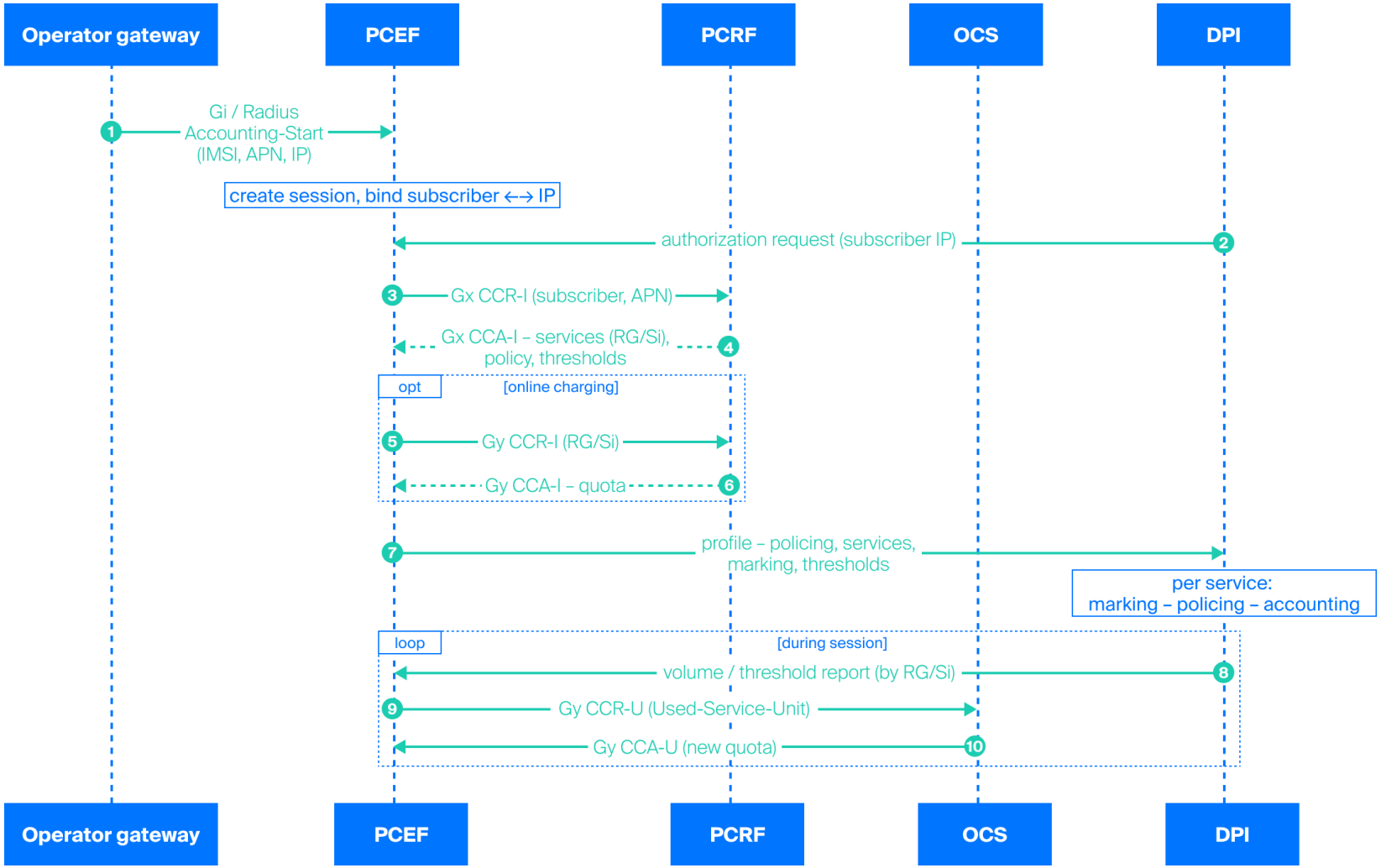
Benefits:

- DPI-classification of traffic (including encrypted traffic – HTTPS/QUIC).
- An updatable database of 6200+ signatures with the ability to add custom signatures
- Export of User Detail Records to link subscriber actions with network statistics
- Hierarchical policing – QoS per channel, subscriber, rating group, or session
- Web filtering by lists and other VAS services

A proven solution from VAS Experts:
DPI-engine is embedded in the architecture of hundreds of telecom operators worldwide



Call Flow for Subscriber Authorization



Use Cases

1. Subscriber and Policy Management

- Throttling/Unthrottling (speed limiting/unlimiting in real time)
- Suspending/resuming the service
- Prioritization of policies when they overlap
- Subscriber lookup and session profiling
- Subscriber Services Management (including NAT)

2. Monetization and zero-rating

- Zero-rating for specific services and applications
- Free access to a service (e.g.,video streaming) upon booster activation
- Differentiated speed-profiles by package
- Fair Usage Policy (FUP) with automatic restoration
- Excluding local CDN traffic from the quota
- Policy bypass for local cache/selected destinations

3. DPI and Traffic Management

- Precise application classification (including encrypted traffic)
- Prioritization by application, traffic shaping
- Reporting by subscriber and application
- DPI mechanisms for bypass/shunting
- Redirecting traffic to a test DPI environment
- Load balancer at L2

4. Regulatory Compliance

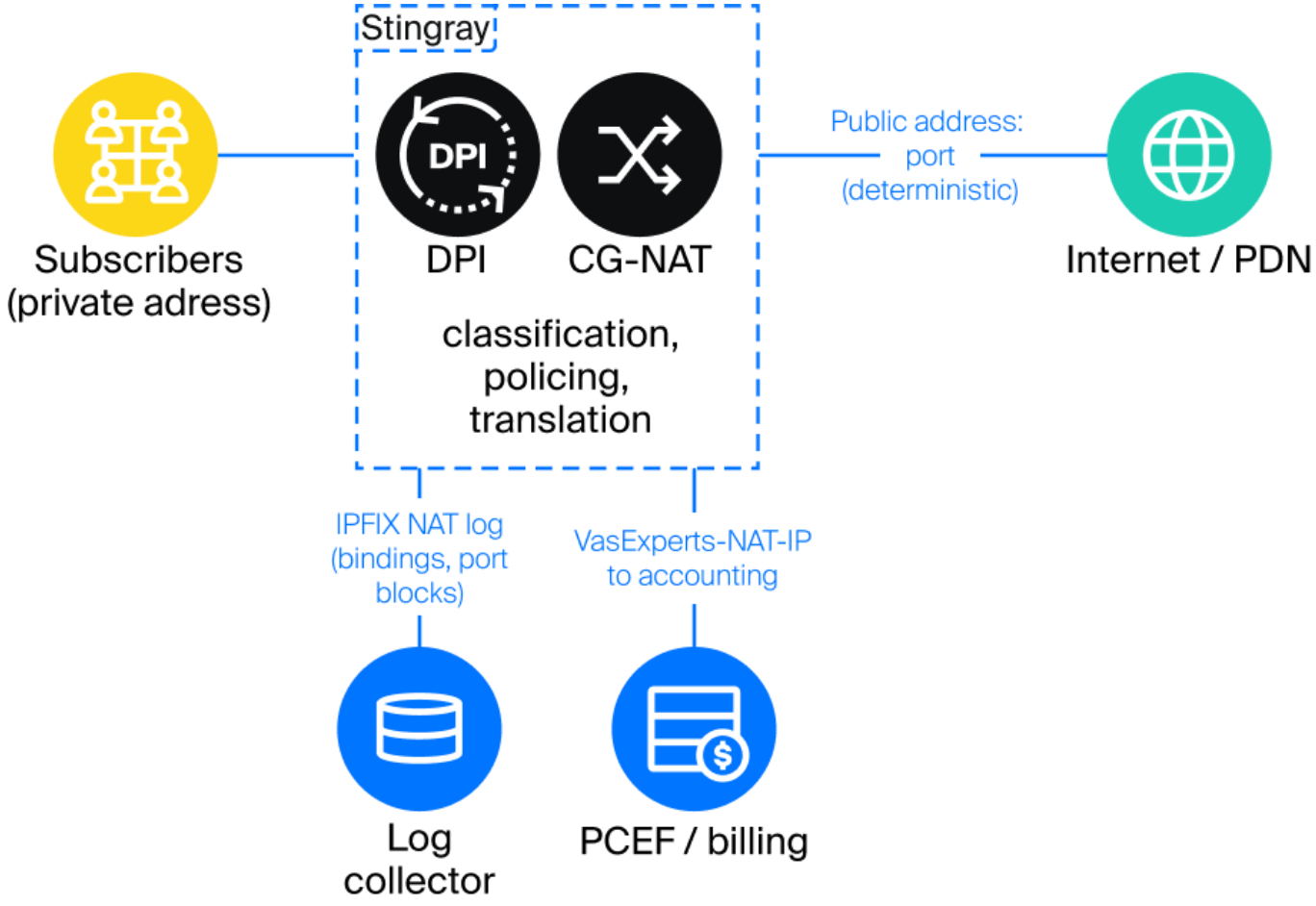
- Blocking by domain/URL/category
- Working with blacklists and whitelists
- Integration with external threat feeds
- Integration with IWF-type registries
- DNS redirect
- Advanced methods for blocking encrypted traffic
- Lawful interception compatibility

5. Built-in CG-NAT

CG-NAT is integrated with DPI. NAT profiles are assigned based on rules from PCRF or by default.

CG-NAT capabilities:

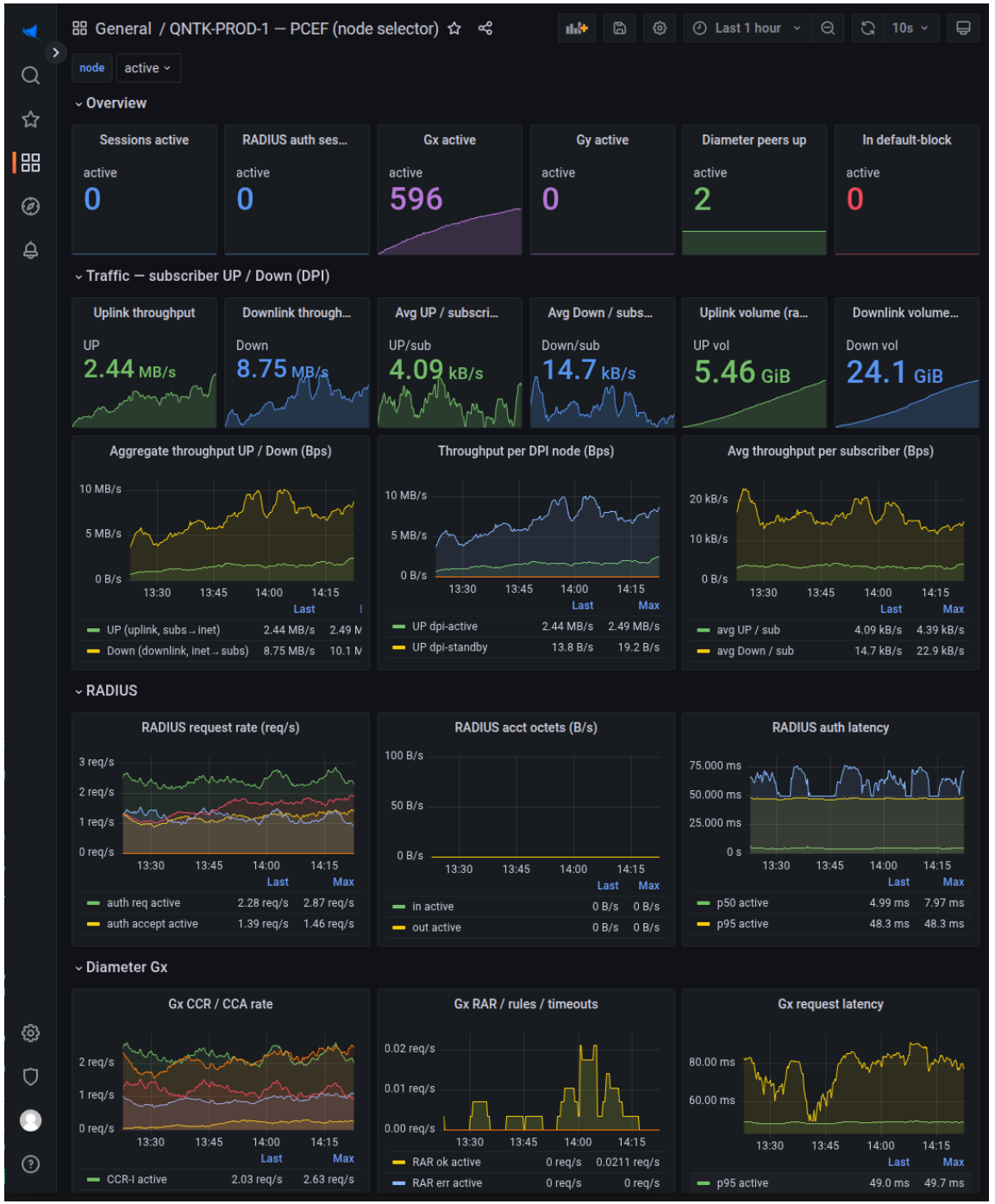
- Managing public IP address pools
- Port allocation per subscriber
- Session limits per private IP address
- Hairpinning – local traffic without translation
- Fast port reuse
- Resilience to DDoS- and BotNet-attacks
- Usage statistics and NAT-logs export



VAS Experts

Monitoring and Operations

- Real-time monitoring and reporting across 60+ metrics in Prometheus and Grafana
  - accounting and signaling (authorization, session start, renewal and termination, volumes
  - Gx/Gy exchange (requests and responses, successes and errors, installed rules, granted and used quotas)
  - active sessions
  - latency distributions, queue depth
  - worker thread metrics and protective counters
  - load distribution across nodes, number and status of sessions, capacity, etc.
- Health checks
- End-to-end tracing by subscriber
- Impact assessment on active sessions, diagnostic and troubleshooting tools, ensuring quality and reliability of service



Sizing the PCEF/PGW Solution

UP and CP sizing is based on independent axes:

User Plane – by bandwidth (DPI/UPF nodes),

Control Plane – by the number of subscriber sessions (Control Plane nodes).

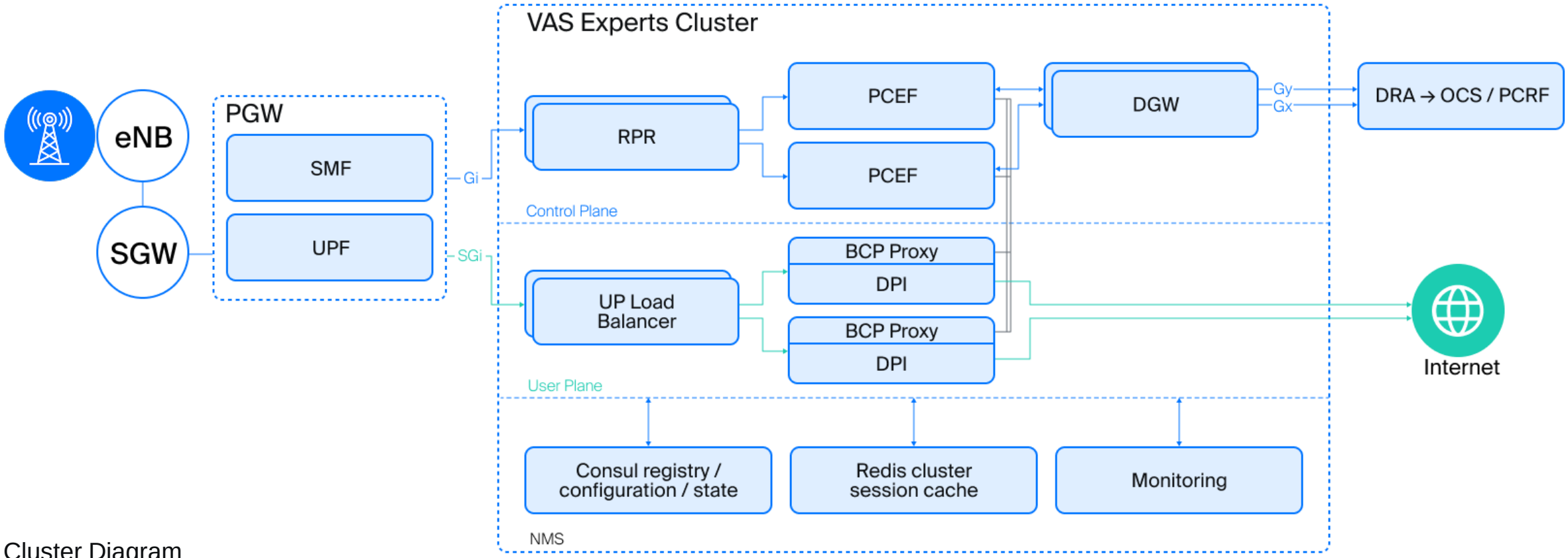
Calculation **for 1 million sessions** with N+1 redundancy: 8 transactions per session per hour and 100 Gbps.

Control Plane		
PCEF	1+1 nodes	RPS: 2 444 (transactions per second)
SMF/PGW-C	2+1 nodes	
Redis Session Database	3 nodes	minimum 3 DB nodes in cluster mode – sufficient for up to 10 million sessions
User Plane		
DPI	1+1 nodes	100 Gbps per node, may be split across several nodes depending on hardware capabilities
Load Balancer	1+1 nodes	20 Gbps per node, only outbound traffic is balanced

Proven Performance

Metric	Value	Conditions
Control Plane throughput	**~120 000 RADIUS-requests/sec** per server (64 cores)	CPU: Linear scaling across cores
Memory per session	**Cashe: 4 KB** (PCEF) + 4 KB (Redis)	RAM: 1 million sessions ≈ 4,2 GB; 128 GB ≈ 32 million sessions
Processing latency	Session authorization cycle: **1.5–3.0 ms**	Asynchronous model: network delays **do not reduce** throughput

PCEF / DPI Cluster Diagram



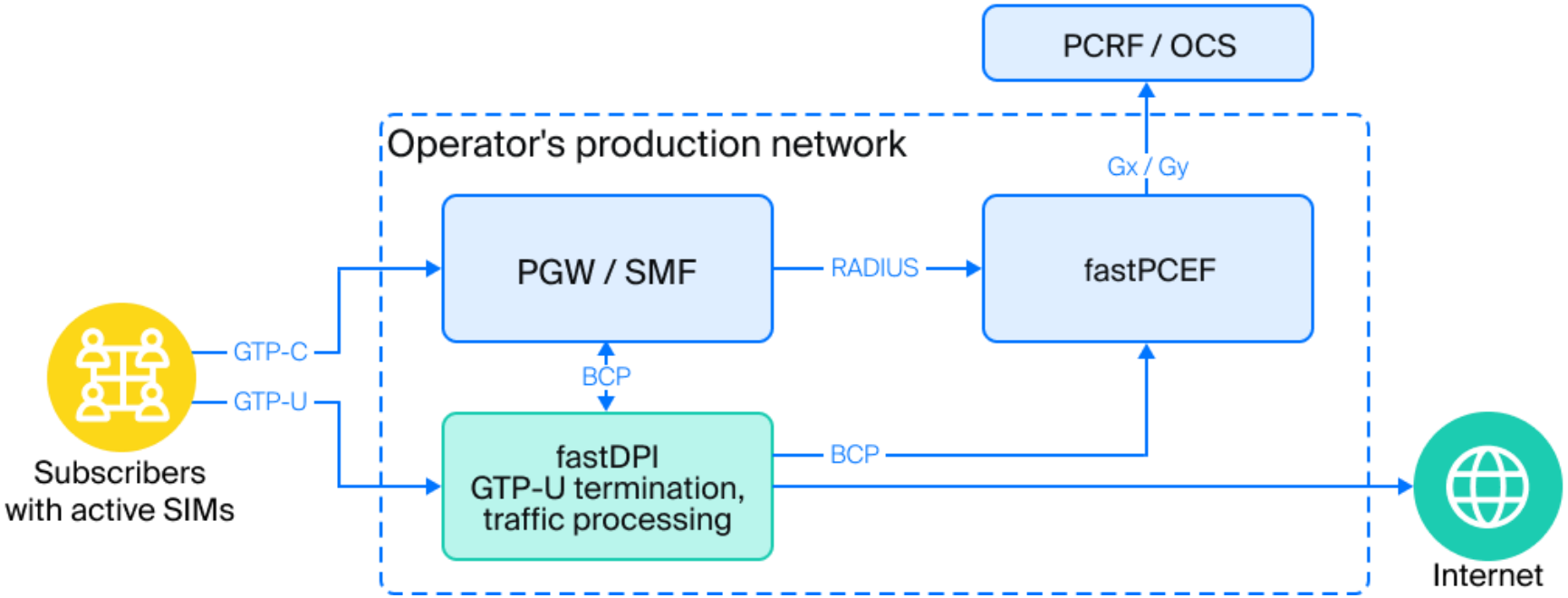
Cluster Diagram

Control Plane Scaling

Performance scales via a horizontally scalable, fault-tolerant cluster serving 100 million subscribers.

Subscriber Sessions	RPS	PCEF Servers (N+1)	Redis DB Servers	CP Total	NIC
1M	2 444	2	3	5	1 Gbps
1M	24 444	2	3	5	1 Gbps
100M	244 444	8	9	17	10 Gbps

Production Deployment

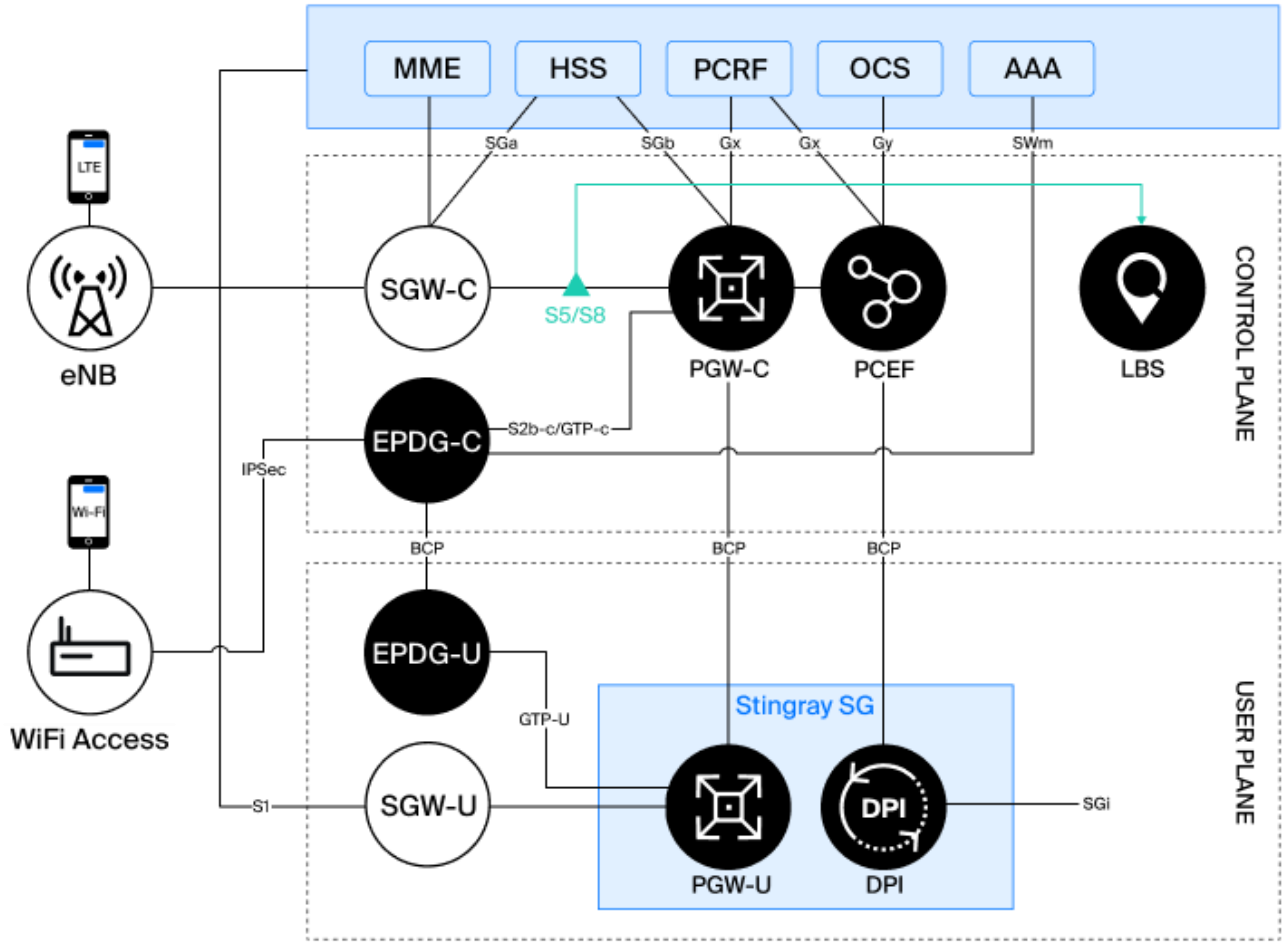


- VAS Experts products operate in a real operator network, serving real subscribers with real traffic
- Deployment uses only tested packages, with verification and rollback capability
- Charging via Gx / Gy with one of the leading commercial billing systems in region
- Software updates are seamless, with no interruption of subscriber sessions

Demo and Proof of Concept

Test traffic management and charging policies on your own scenarios

- Combinations of applied policies and launching complex tariffs
- Quota exhaustion
- Charging exceptions
- Roaming
- CG-NAT



Follow The Experts

sales@vas.expert

vasexperts.com