VAS Experts ITG

Stingray Service Gateway

Web and apps filtering

Traffic policing and QoS

Lawful Interception

Deep Data Analytics

Content

About VAS Experts

VAS Experts is a telecom software developer. Since 2013, we have carried out more than **2000 installations** in CIS, Europe, Africa, Latin America, Asia, and even Oceania that are using our Stingray Service Gateway.

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:

- Lebanon
- India
- Iraq
- Peru
- Congo
- Brazil

Our products

For telecom operators:

DPI

Multifunctional platform for traffic management

QoE analytics

Traffic Monitoring and Analysis System

Load Balancer

Traffic balancer

BRAS

Scalable and Cost-Effective Software Gateway

CG-NAT

Providing transparent network address and protocol translation

VEOS

Operating system

For mobile operators:

LBS

Module for detection of subscriber's location

EPDG

Solution for launching Wi-Fi Calling (VoWiFi)

PCEF

Flexible tariff plans and QoS policies
Integration by Diameter protocol

Own DPI Engine

History

2013 — DPI

2016 — CG-NAT

2017 — L3 BNG DualStack IPv4/IPv6

2018 — Lawful Interception

2019 — L2 BNG DualStack IPv4/IPv6

2020 — Mobile Networks Support, LBS

2021 — Border Router

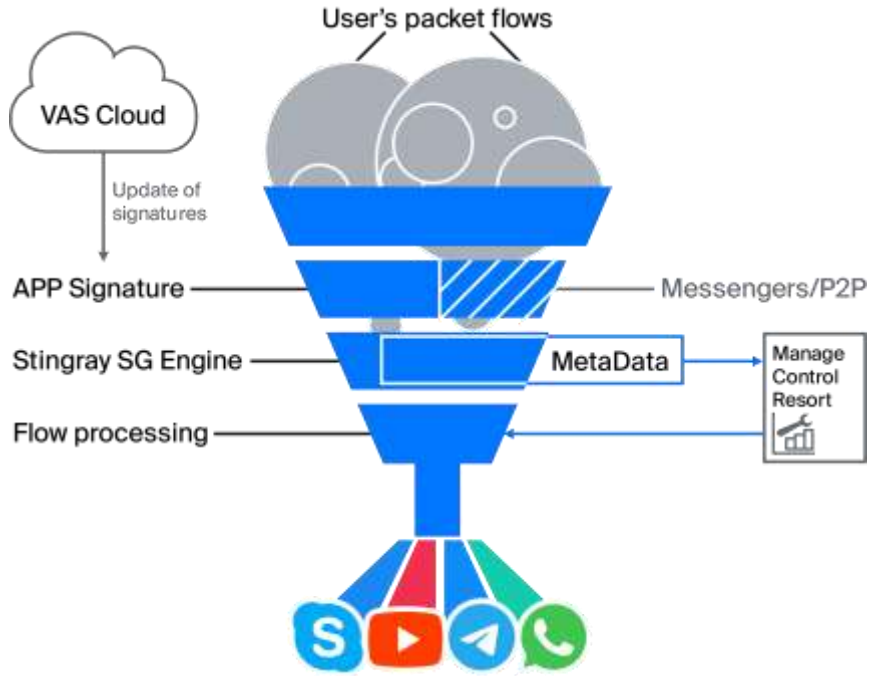
2022 — VAS Cloud Services

2023 — VEOS, On-Stick, EPDG

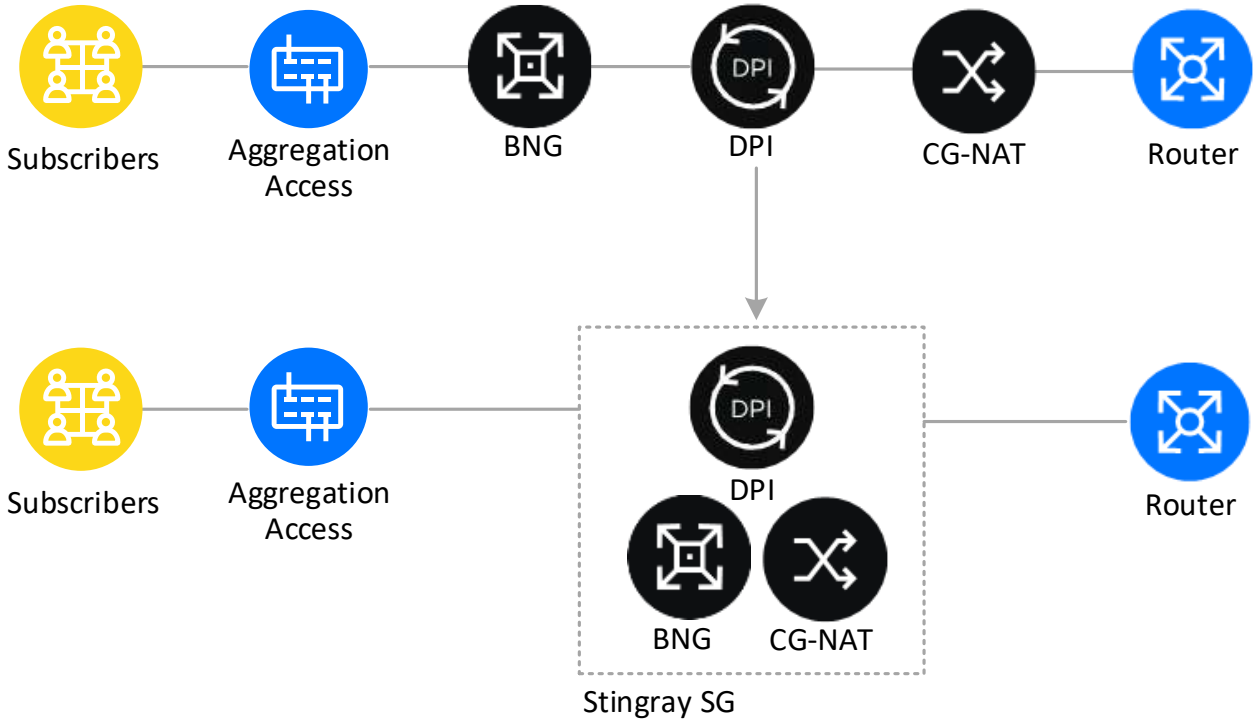
2024 — PCEF, Diameter

Stingray SG can compete with:

Sandvine	Cisco SCE	Cisco ASR	MikroTik
Allot	A10 Network	Juniper MX	Huawei NE



Multi-functionality



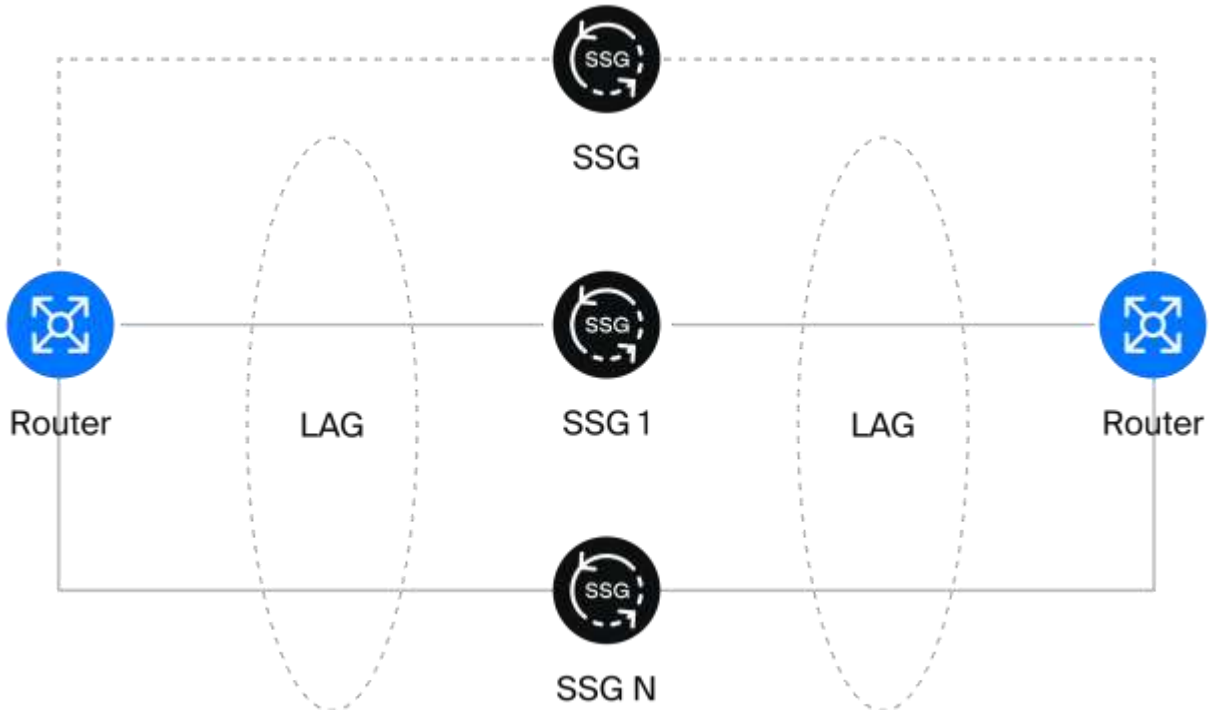
Installed on a regular **x86 server**, the multifunctional SSG platform replaces a set of disparate network equipment.

This simplifies administration, maintenance, and scaling processes.

Platform Performance

FEATURE	SSG-6	SSG-40	SSG-80	SSG-120	SSG-240	SSG-360
Performance, Gbps	6G	40G	80G	120G	240G	360G
Number of subscribers (2Mbps per subscriber)	2,5K	20K	35K	50K	100K	150K
Maximum number of session	8M	64M	160M	256M	512M	768M
Number of new sessions	250K	2000K	3000K	5000K	10000K	15000K
Ports, GbE	2x10G	6x10G 4x25G 4x40G 2x100G	12x10G 6x25G 6x40G 4x100G	20x10G 8x25G 8x40G 4x100G	16x25G 14x40G 8x100G	28x25G 20x40G 12x100G
Latency (average value), microseconds	30					
Platform	1U-2U, 19”, AC/DC 2xPSU, N+1 Fan					

Redundancy



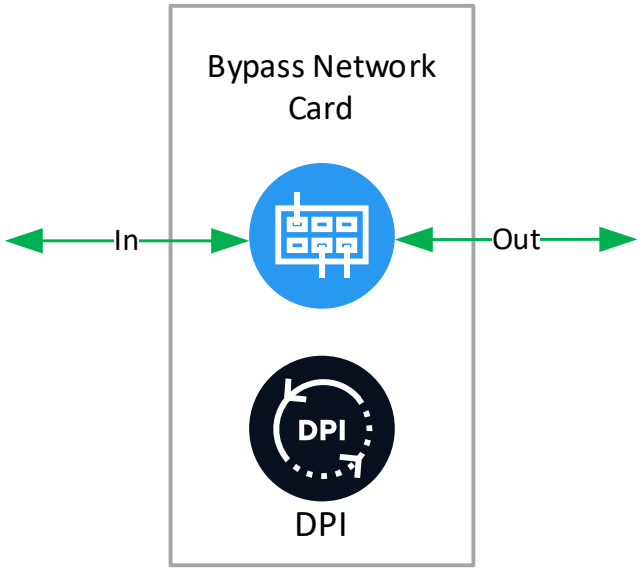
- DPI works as a L2 Bridge. In this scenario, it is possible to combine multiple devices into a LAG and to balance sessions between them.
- The main idea is to place traffic from one subscriber in the one DPI server. It is possible to organize a balance by LACP hashing algorithms or by creating DPI cluster with Network Packet Broker.
- Supported modes: Active-Active and Active-Standby
- Special price for reserve license.

Bypass Support

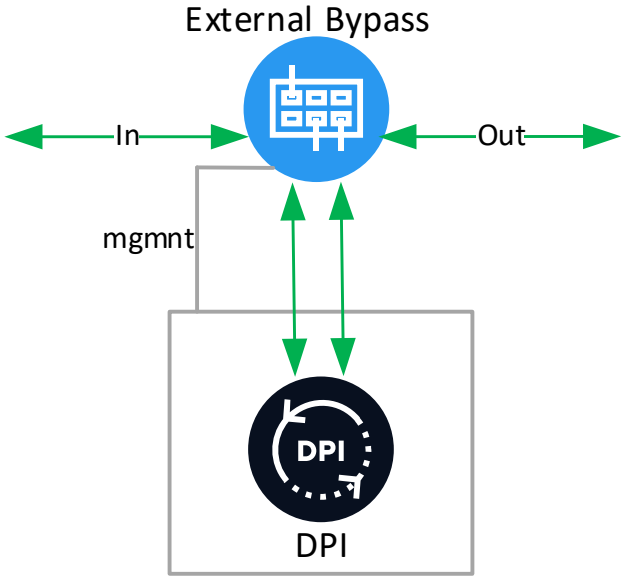
Bypass allows to ensure the network operability in case of installation of the system in-line in the following situations:

- Equipment malfunction
- Software errors
- Preventive maintenance
- Power cut

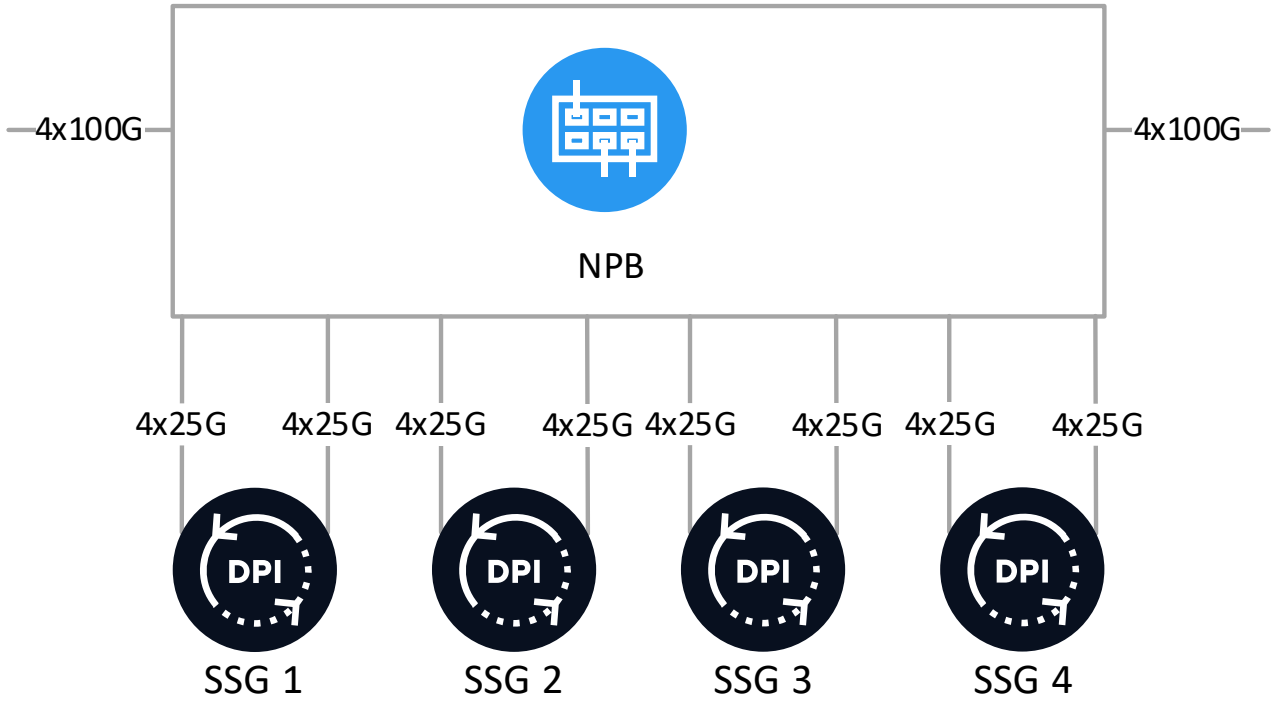
Cards with internal bypass



External bypass



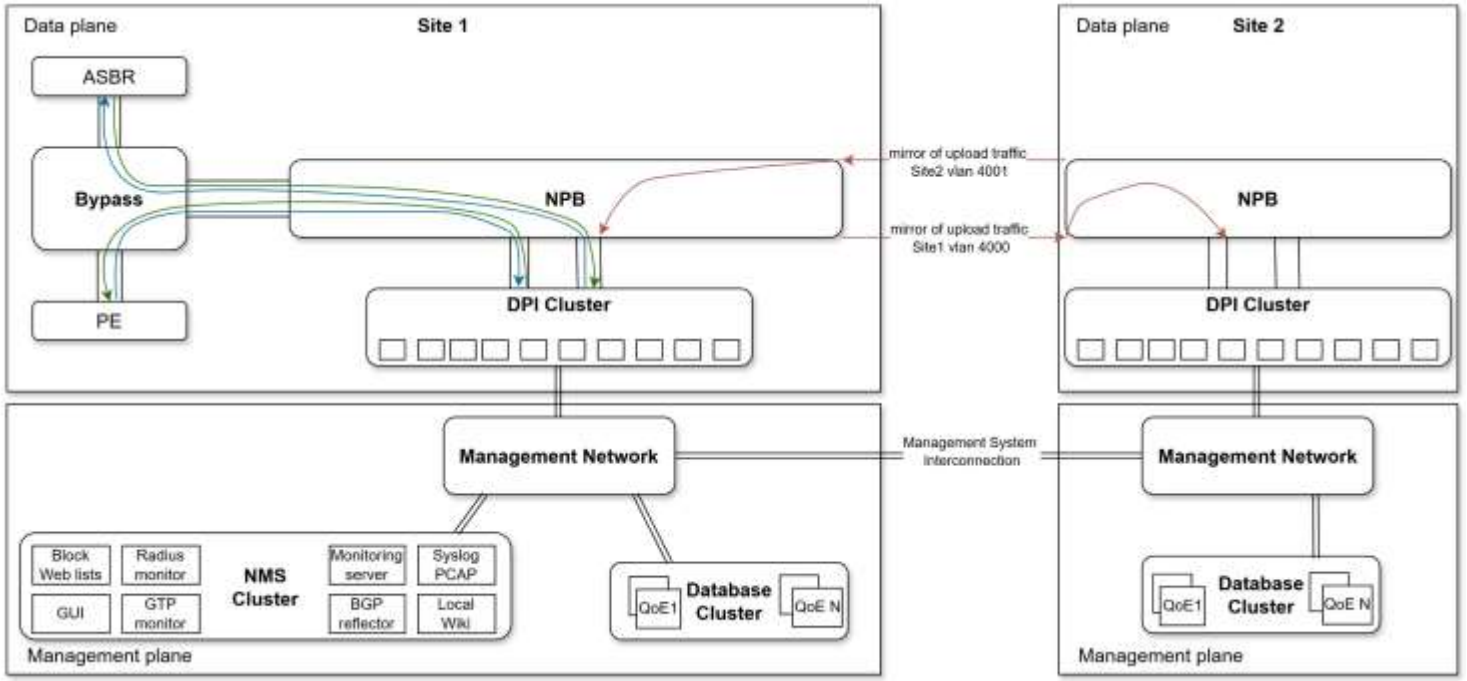
Cluster Performance



Up to **4.6 Tbps per cluster** with Network Packet Broker

The system is configured for redundancy using an N+X scheme, where X represents the number of additional nodes; N+N is also available with full redundancy of all components.

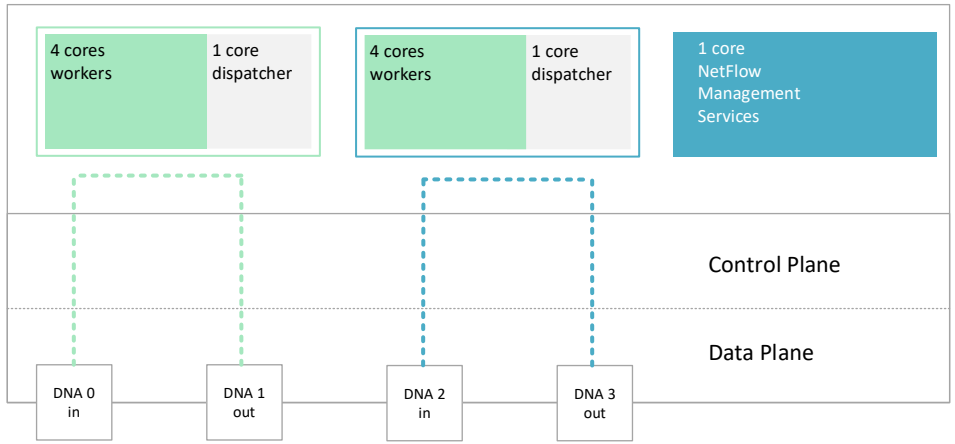
Cluster Architecture



Asymmetric traffic between sites:

Processing of asymmetric traffic between sites is carried out by delivering a copy of outgoing traffic from one site to another. The original traffic remains at the original site and the route of traffic does not change. A copy of the traffic is transmitted in a specific VLAN via direct links between NPBs in order to minimize latency. A copy of the traffic is balanced across the DPI cluster device. DPI takes this traffic into account when detecting the signature, but does not take it into account when it is uploading the statistics. After processing, this traffic is discarded based on a specific VLAN. The usage of this method increases the percentage of recognition in an asymmetrical traffic.

Platform Architecture



Performance up to **240 Gbps** per platform

Control Plane

- VEOS is a proprietary operating system with support for VAS Experts

Data Plane

- DPDK – Direct NIC Access technology

Hardware Factors

- Available platforms
- x86 servers
- High performance
- Soft limit
- Scalability
- Hands-On Upgrade
- Continuous growth

Main Features

Web filtering by URL/SNI/CN/IP/IP:port	Supported HTTP/HTTPS/QUIC protocols
Traffic blocking by IP/ASN/Signatures	Automatic updating and loading of huge lists. Creating custom signatures based on SNI, IP, CIDR
Traffic policing by IP/ASN/Signatures	Per session policing, per user policing, per channel policing
Congestion control and Traffic coloring	Priority management and traffic markup based on protocols and directions
Advanced Traffic Detection	Signatures customization and Regular updates guarantee high traffic recognition
Group policies: per subscriber, per channel	Subscriber and channel mapping using RADIUS, GTP-C and BGP
Statistics gathering and reports	Detailed statistics on IP, ASN, DNS, Signatures and automatic mail reports

DPI Protocols / Signatures

SGG applies various approaches to form a stable signature

- Sample analysis (Pattern analysis)
- Numerical analysis
- Behavioral analysis
- Heuristic analysis
- Protocol/stateful analysis

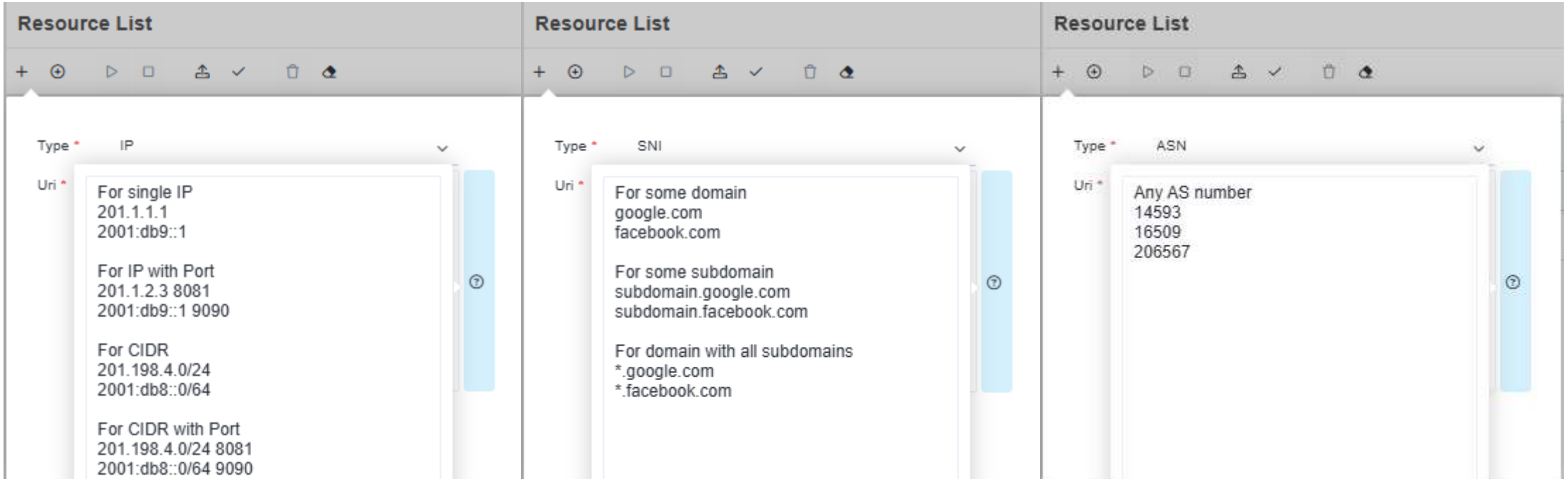
SSG contains 3 types of signatures:

- Built-in signatures, which are a part of the DPI engine and are updated along with the SSG software
- Dynamic signatures loaded into the core during the operation of SSG
- Custom User signatures created by an end user in the GUI and loaded into the core during the operation of SSG

Custom User Protocols / Signatures

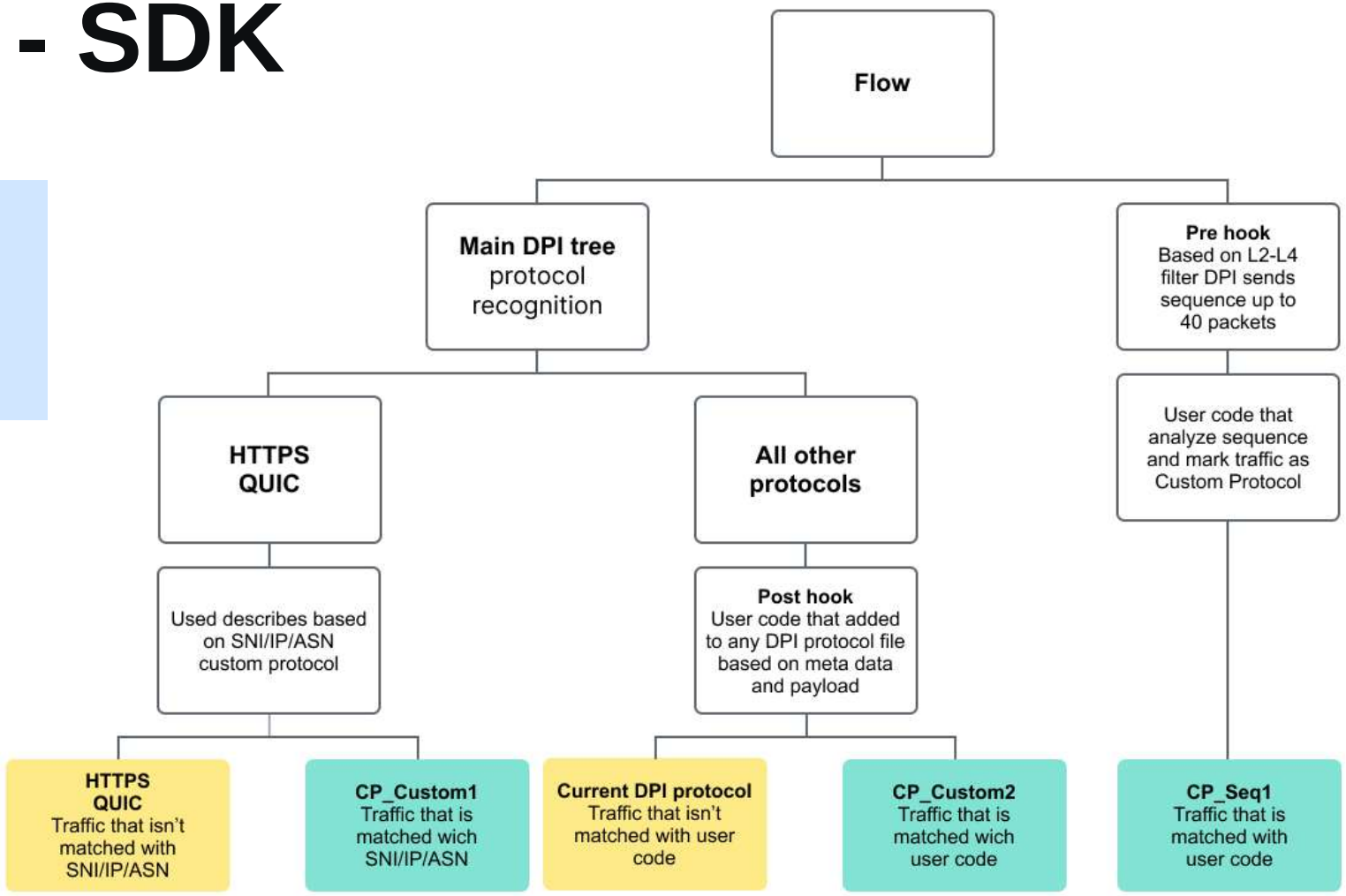
The user protocol mechanism allows for defining a new protocol based on the following criteria:

IP; IP + port; CIDR; CIDR + port; AS number; TLS Server Name Indication (SNI), In the absence of SNI, the Common Name is checked.



DPI Toolkit - SDK

DPI supports protocol customization with adding an extra code to the recognition protocol tree.

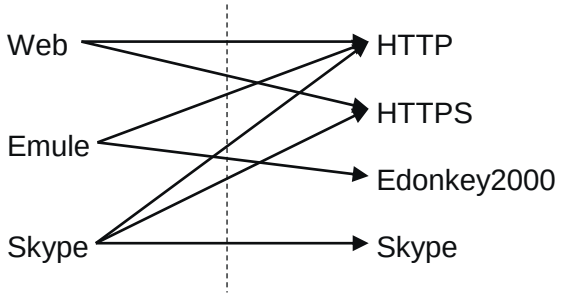


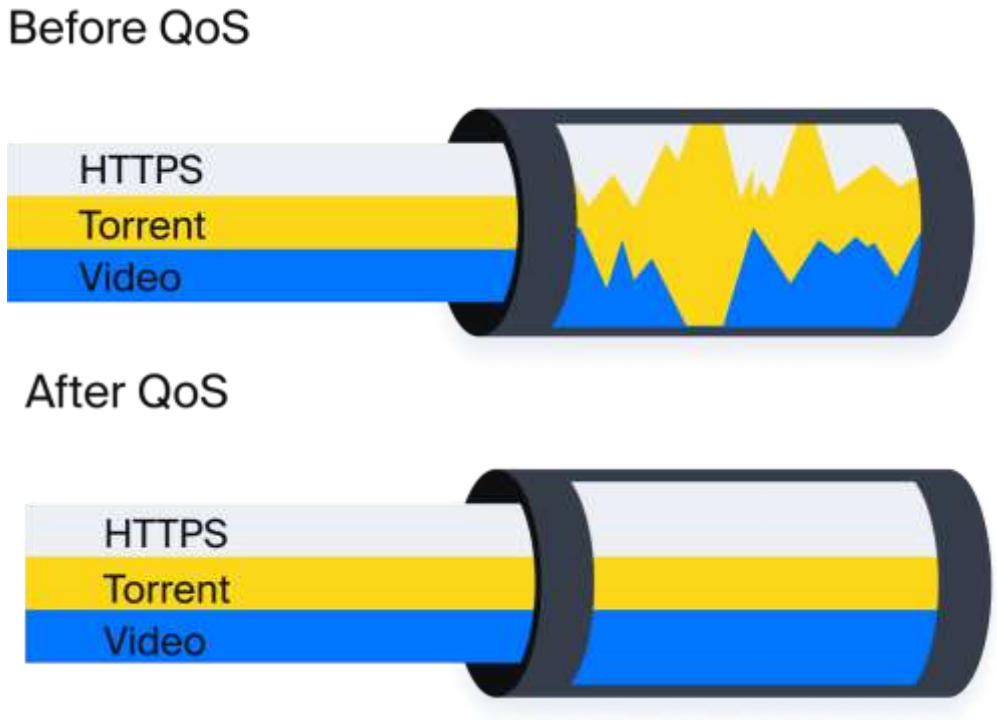
Traffic Prioritization

By direction

- Registered AS
- Customized AS

By protocol / application





Policing levels

Per Session

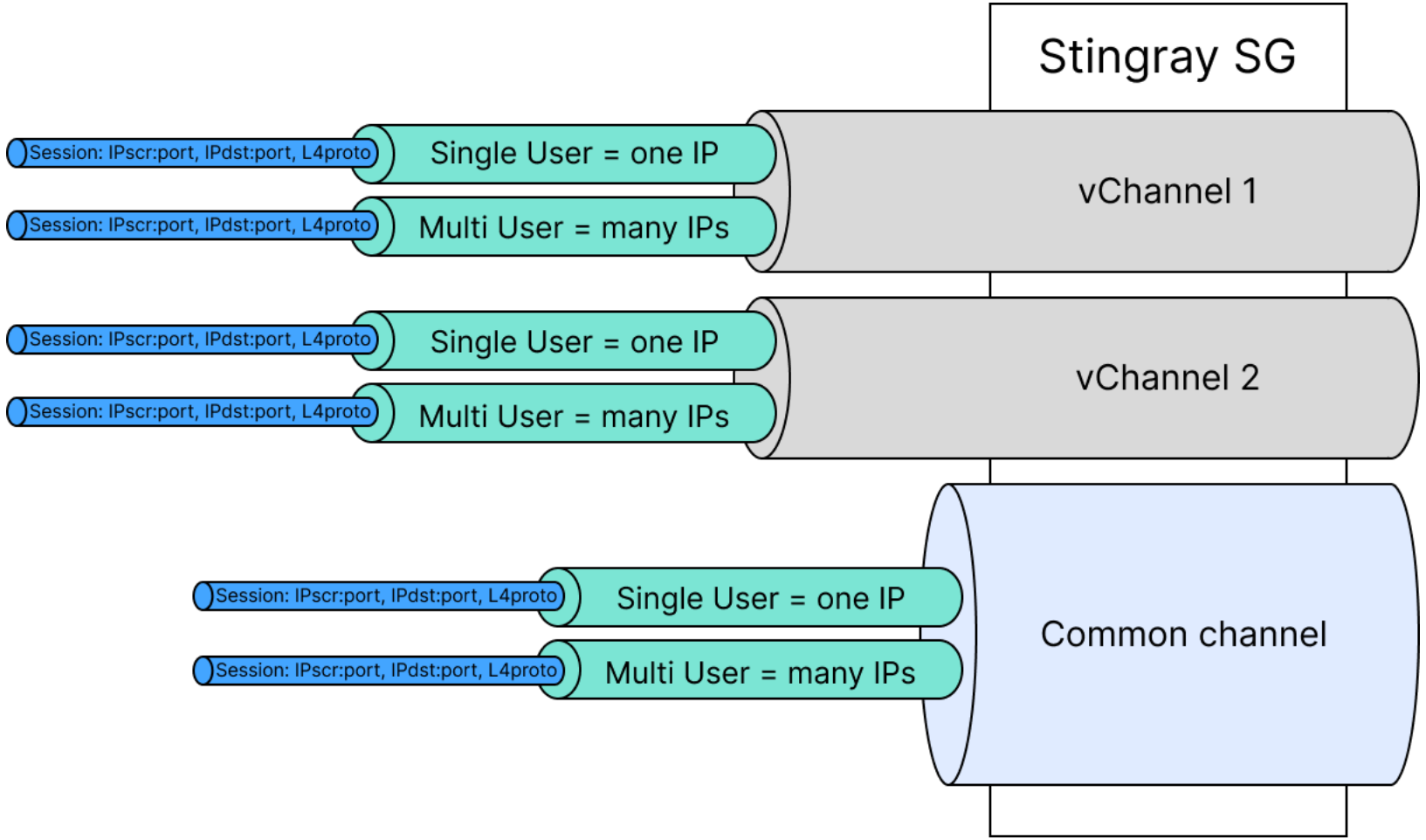
Per session control

Per Subscriber

Prioritized speed limit per subscriber

Per Channel

Channel rate control for congestion management



Flexible Tariff Plans – Policing per IP/Login

Task

1) Outbound Torrent Limit
2) Maximum speed on local resources
3) Increase speed to:
   - Messengers and SIP
   - Web resourses: HTTP, HTTPS, QIUC
   - Game services

Use cases:

1. Time schedule tariff plans
2. High speed to local recourses
3. Increasing subscribers QoE
4. Throughput is shared between IPv4/IPv6 connections

Classes (cs):

cs0 dns, icmp (e.g. World of tanks)
cs1 http, https, quic
cs2 viber, whatsapp, skype, sip
cs3 default
cs4 reseved
cs5 AS local IP, peering
cs6 tcp_unknown, udp_unknown
cs7 Bittorrent

htb_inbound_root=rate 50mbit	**htb_root=rate 50mbit**
htb_inbound_class0=rate 20mbit ceil 50mbit	htb_class0=rate 20mbit ceil 50mbit
htb_inbound_class1=rate 1mbit ceil 50mbit	htb_class1=rate 1mbit ceil 50mbit
htb_inbound_class2=rate 1mbit ceil 50mbit	htb_class2=rate 1mbit ceil 50mbit
htb_inbound_class3=rate 8bit ceil 50mbit	htb_class3=rate 8bit ceil 50mbit
htb_inbound_class4=rate 8bit ceil 1mbit	htb_class4=rate 8bit ceil 1mbit
htb_inbound_class5=rate 100mbit static	***htb_class5=rate 100mbit static***
htb_inbound_class6=rate 8bit ceil 50mbit	htb_class6=rate 8bit ceil 5mbit
htb_inbound_class7=rate 8bit ceil 50mbit	htb_class7=rate 8bit ceil 5mbit

Filtering By Blocklist and Categories

Description	Characteristic
✓	Using your own operator list
✓	Using centralized private operator’s list for a cluster of servers
In-line, asymmetric, mirroring	Connection Diagrams Support
✓	Ability to control filtering by specific users and subnets for the organization of filtering services for downstream operators
✓	
✓	Web Filtering HTTP by URL
✓	Web Filtering HTTPS/QUIC by SNI, CN, IP:port
✓	Redirect support for HTTP to info page
✓	Ability to collect statistics on blocked pages
	Ability to monitor loading lists and filtering work
Up to 4 billion URL	Maximum list size

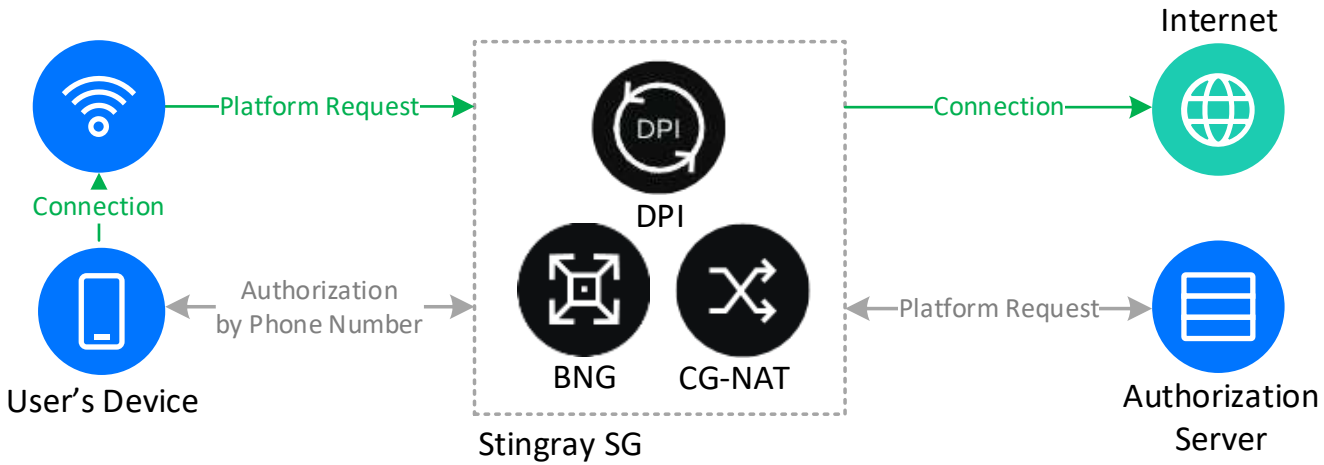
Filtration allows you to block a specific URL for the HTTP protocol from a page.

Blocklisting by category is supported and it is possible to use a combination of categories. Categorized lists are loaded automatically from VAS Cloud.

Filtration for SSL resources are supported SNI looks like *.domain.com and regular expressions that provide flexible filtering.

Allow List and Redirect to Captive Portal

The Allow List makes it possible to limit the sites and pages available to the subscriber and to redirect the subscriber to the specified page when trying to go outside this list.



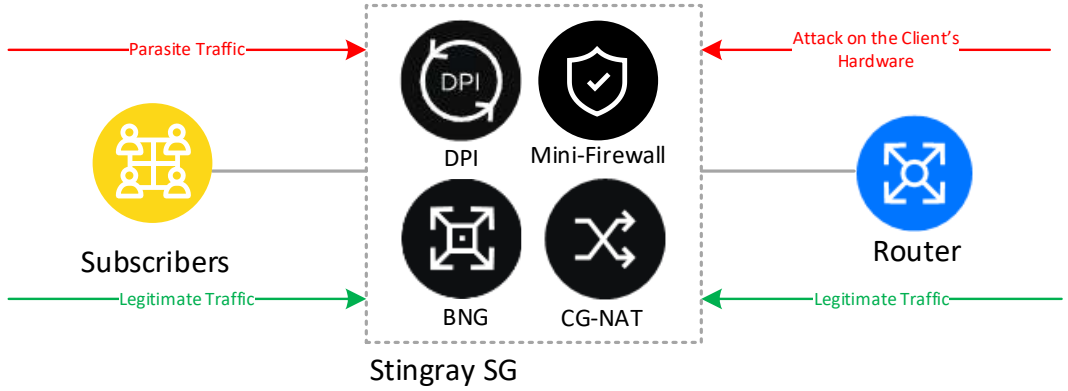
Use cases:

1. Subscriber blocking in case of low balance, with the possibility of payment via authorized payment systems.
2. Organization of user identification in Public Wi-Fi HotSpot, provision of certain user actions in a Wi-Fi network to provide access.

Mini Firewall

The tasks are:

- Preventing hacking of user devices by system ports
- Blocking malicious activity from the subscriber — SPAM, BotNet



Recommendations:

- Utilize statistics from QoE module in user accounts
- Announcement to the client warning him of his problem and offering an antivirus service

Marketing and notifications

Notification capabilities:

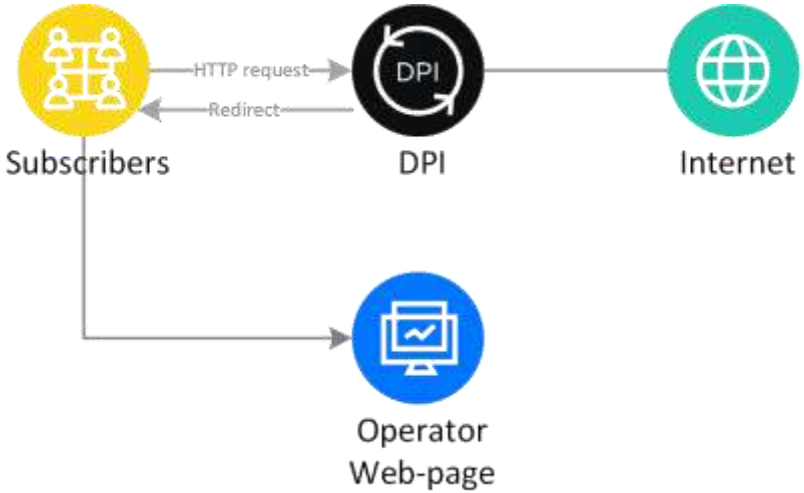
Automatic segmentation of subscriber base according to the certain criteria

Customization of notifications in a certain period of time and day of the week

Possibility to run several campaigns simultaneously

Application:

1. Conducting user surveys
2. Warning about network works and communication outages
3. Informing about new services and promotions for subscribers



DDOS Attacks Protection

1. Protection against TCP SYN Flood

- Detects an attack on exceeding a specified threshold of requests not confirmed by the client SYN
- Independently, instead of the protected site, responds to SYN requests
- Organizes a TCP session with the protected site after confirmation of the request by the client

Depending on the settings, Stingray SG may be activated manually, automatically or to be in constant protection mode against this type of attack.

DDOS Attacks Protection

2. Fragmented UDP Flood Protection

This type of attack is carried out by fragmented UDP packets, usually of a short size. The attacked platform is forced to spend a lot of resources for assembling and analyzing them.

For protection, protocols that are irrelevant for the protected site are dropped or hard-limited by the bandwidth.

3. Protection (LOIC, etc.) based on Turing test (Human Detection)

When the limit value of requests is exceeded, protection is activated and the user must enter information from the CAPTCHA to confirm that he is not a part of the botnet.

After that access to the site will be allowed. This test determines who the user of the system is — a person or a computer.

Metadata Extraction

SSG can recognize all traffic and generate statistics by IPFIX (Netflow v10)

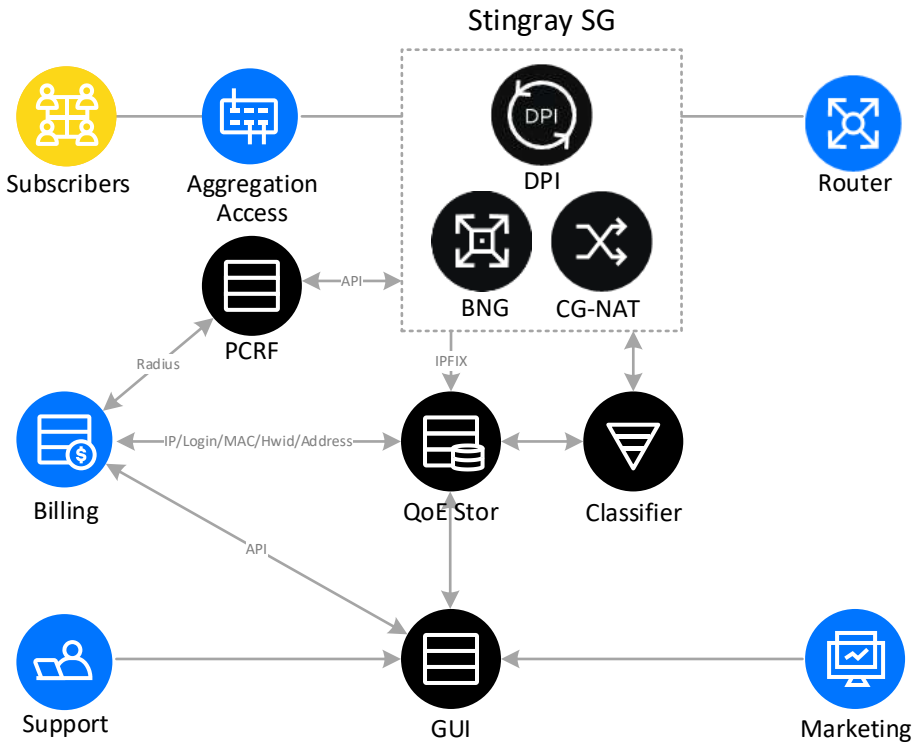
- FullFlow — IPFIX flow contains information about connections pass though DPI, full session statistics and enriched DPI information (subscriber ID: login/MSISD/IMSI, IP port, DPI protocol, traffic volume, QoE metrics)
- Clickstream — IPFIX flow contains information about subscriber's visits to web-pages (HTTP, HTTPS, QUIC)
- Metadata — IPFIX flow contains fields specified for protocols SIP, XMPP, MAIL (POP, IMAP, SMTP), FTP
- Extended (Raw) metadata — IPFIX flow contains raw truncated IP packets for some protocols like STUN sequences and VoIP control protocol sessions. DPI sends raw data to LI-subsystem to postprocess data if needed.
- DNS — IPFIX flow contains all domain name service requests
- RADIUS — IPFIX flow contains all RADIUS attributes
- GTP — IPFIX flow contains all GTP-C attributes using for LBS solution

Quality Of Experience Module

QoE is a software product responsible for statistic gathering and viewing subscribers' perception of services.

The statistics are transferred to special metrics which allow to define users' experience. It provides the operator with information about what kind of problems does he or she encounter.

The data obtained allows the operator to take action and to improve the services quality. The result is increasing customer loyalty.



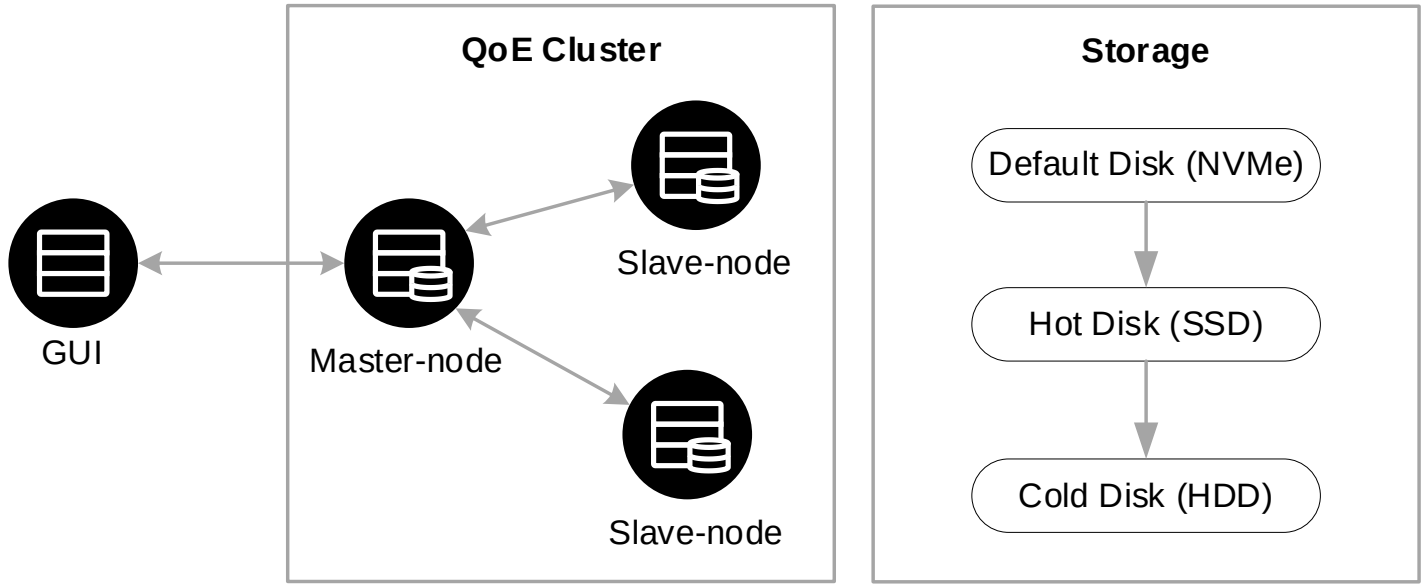
QoE Architecture

QoE Stor is based on the ClickHouse database with the ability to create a cluster of multiple nodes:

A master node is assigned in the cluster, which accepts a request from the GUI and sends requests to the slave node.

Each slave node creates a report based on its own data and transmits it to the master node.

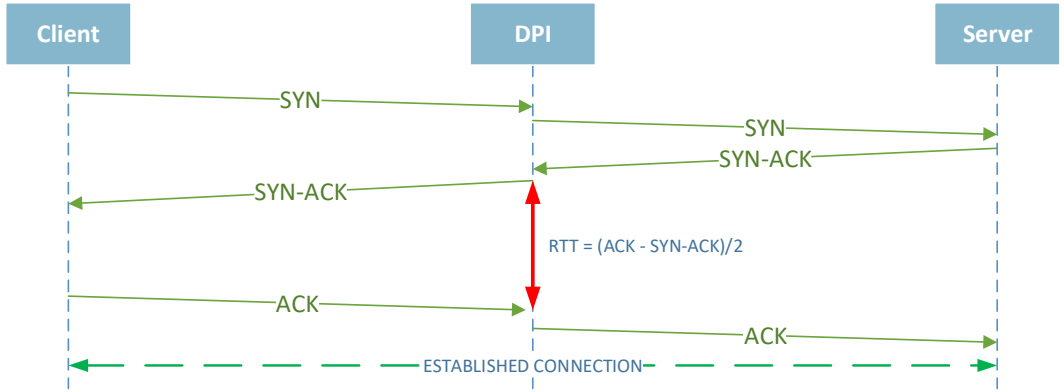
The master node aggregates the received responses from the slave node and makes the resulting representation for visualization in the GUI.



This hierarchy allows for linear scaling of the cluster when adding new nodes without the need to increase the performance of the master node.

QoE Metrics

1. Round-trip-time (RTT)
2. Indicators of retries number
3. The number of sessions, devices, agents, IP-addresses per subscriber
4. Traffic distribution by application and transport protocols
5. Traffic distribution by autonomous system (AS) numbers
6. Clickstream for each subscriber (URL, Hostname, IP)



How To Use QoE Metrics?

Sales and Marketing

- Upselling new service, Wi-Fi equipment, traffic plans
- Work with outflow and analysis of the causes of outflow in the past
- Target advertising with using subscriber profiling
- Antivirus for sale

Technical and Support departments

- Deep troubleshooting and monitoring with using Round Trip Time and TCP retransmitting
- Identification of problems with client terminal equipment, Wi-Fi router, access switch and aggregation
- Search for optimal peering points and connections to higher providers

How To Use QoE Metrics?

Retention of subscriber base

- Identifying degradation in subscriber service quality and responding promptly
- Working with potential churn and analyzing the reasons for past churn
- Automating surveys after a master visit to a subscriber

Increasing loyalty

- Conducting marketing campaigns on new tariffs, services, and offers, taking into account the interests of subscribers
- Providing information on channel utilization and quality via the subscriber's personal cabinet
- Notifications about BotNet activity in the network (relevant for IoT)
- Notification of a virus activity

QoE Analytics Reports

Built-in reports

- Available to get report from each dataset: NetFlow; Raw Full NetFlow; Clickstream; Raw Clickstream; DNS Flow; Raw DNS Flow
- Filters in reports enable users to refine data based on specific criteria, making it easier to locate necessary information within large datasets
- Large Report Manager allows users to initiate report generation in the background and queue multiple reports for execution

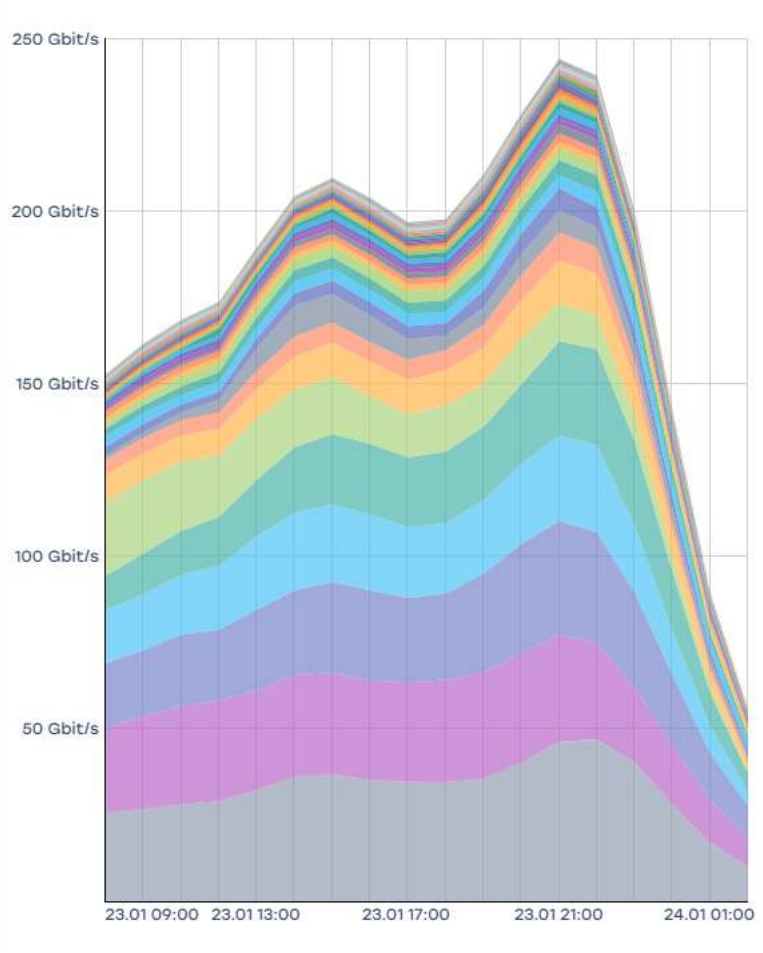
Email Reports

- Supported all Built-in reports with enabling filters.
- Flexible email report management: period, email subject
- Supported different formats: Excel, CSV, PDF, PNG
- Track distribution status: Waiting, Caching, Checking, Notification

Graphical User Interface

1. Restricting access by role
2. Logging user actions
3. Managing multiple SSG functions: monitoring and configuration
4. Service management
5. Creating tariff plans
6. Creating NAT pools
7. Working with QoE analytics
8. API integration

Protocol	Group	Traffic	Traffic
Filter			
tiktok 49264	Video, pictures	34,656,205,61	2,301,284,873
youtube 49227	Video, pictures	27,543,142,911	1,332,700,996
https 443	Web browsing	25,099,189,954	2,716,677,923
http 80	Web browsing	20,122,865,28	990,400,701
netflix 49263	Video, pictures	19,230,789,792	1,008,864,482
fortnite epic 49280	Gaming	13,919,355,017	467,373,401
instagram 49266	Social networks	9,466,406,097	216,686,005
facebook_video 49242	Video, pictures	5,618,589,875	188,273,560
twitch 49265	Video, pictures	5,134,396,807	335,608,801
udp unknown 65041	Unknown	3,966,260,605	1,836,133,549
telegram 49224	Instant messengers	3,514,382,562	246,259,307
quic 49218	Web browsing	3,368,569,530	286,677,905
bittorrent 49165	P2P	2,999,358,513	821,370,224
google_play 54313	Application servers	1,856,532,022	154,022,306
whatsapp 49223	Instant messengers	1,769,536,134	254,226,257
5,836			



Mapping from RADIUS and GTP

DPI supports binding IP-Login from RADIUS, ports: 1813,1814,1815 etc.

1. Login = User-Name or Calling-Station-ID
2. Login prefixes based on NAS-IP-Address
3. IP = Framed-IPv4-Address, Framed-IPv6-Address, Delegated-IPv6-Prefix

DPI supports binding IP-Login from mirror of GTP-C traffic.

GTPv1 and GTPv2 from S11/S8/S5 interfaces is supported.

Bind rules:

1. Login = IMSI or MSISDN
2. IP = Framed-IPv4-Address, Framed-IPv6-Address, Delegated-IPv6-Prefix

Mapping from BGP

DPI supports binding IP prefix to Channels/Subscribers from BGP signaling.

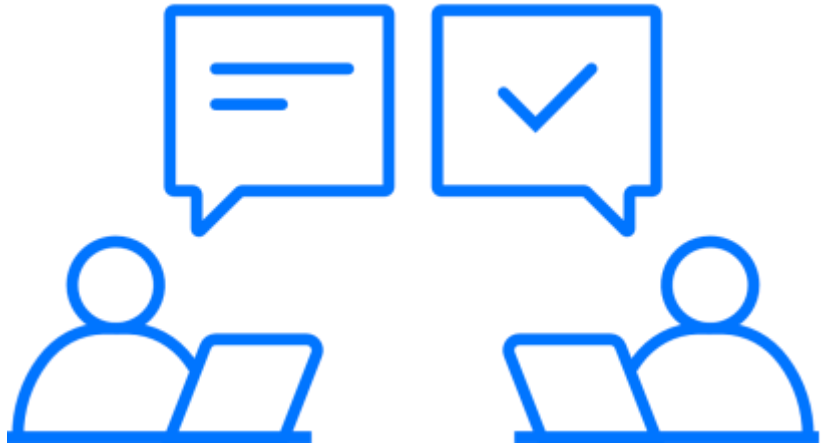
Using BGP signaling, the customer have to setup the Router(s) a new session with BGP-reflector which is a part of solution. The BGP-reflector only receive messages and not to send any routing information for the peer.

Bind rules:

1. define channel base on BGP community or BGP AS-path
2. define user base on BGP community or BGP AS-path

Support at every stage

1. Providing a test version for verifying functionality
2. Offering implementation support and consulting at every stage
3. Providing three levels of support: Next Business Day, 8x5, and 24x7
4. Allowing 24x7 call registration via email and phone



Follow The Experts

sales@vas.expert

vasexperts.com