VAS Experts ITG

СКАТ — платформа для операторов связи

- Анализ
- Контроль
- Управление

Содержание

DPI платформа

Собственный движок

Мультифункциональность

Производительность

Резервирование

Производительность кластера

Архитектура кластера

Архитектура платформы

Основные функции

Протоколы / Сигнатуры

Опции

Поддержка Bypass

Приоритизация трафика

Уровни полисинга

Гибкие тарифные планы

Фильтрация по черному списку

Белые списки и Captive Portal

Mini-Firewall

Маркетинг и уведомления

Решение AntiDDoS на базе QoE

Защита от SYN Flood DDOS-атак

Извлечение метаданных

Quality of Experience

Модуль QoE

Архитектура

Метрики

Отчеты

Графический интерфейс

Сопоставление из RADIUS и GTP

Сопоставление из BGP

Общая информация

О компании

Наши продукты

Поддержка

Контакты

О компании VAS Experts

VAS Experts — разработчик программного обеспечения для контроля и анализа трафика. С 2013 года мы выполнили **более 2000 инсталляций** в России и по всему миру.

Наша команда имеет **более чем 25-летний** опыт разработки программного обеспечения и обширные знания в области телеком-технологий.

20M+

абонентов

Более

35 Тбит/с

Последние инсталляции:

- Россия и СНГ
- Европа
- Ближний Восток
- Латинская Америка
- Африка
- Юго-Восточная Азия

MTS Sarkor YOTA COM GhoFi connecting people Norte CableColor SKYTiC telecom

Наши продукты

Система контроля и анализа трафика (СКАТ) — мультифункциональная платформа для управления трафиком

Для интернет-провайдеров:

DPI

Управление трафиком на основе QoS, фильтрация по белым и черным спискам

BRAS

Гибкое и масштабируемое программное решение

AntiDDoS

Защита сети оператора от злоумышленников

Модуль аналитики QoE

Сбор статистики, оценка здоровья сети и качества услуг

CG-NAT

Прозрачная трансляция сетевых адресов на стандартном x86-сервере

VEOS

Операционная система

Наши продукты

Система контроля и анализа трафика (СКАТ) — мультифункциональная платформа для управления трафиком

Для мобильных операторов:

PGW

Интеллектуальный шлюз, обеспечивающий контроль трафика в рамках архитектуры EPC

PCEF

Гибкая тарификация на основе различных условий в соответствии с требованиями PCRF

EPDG

Решение для запуска Wi-Fi Calling (VoWiFi)

Собственный DPI движок

История развития

2013 — DPI

2016 — CG-NAT

2017 — L3 BRAS Dual Stack IPv4/IPv6

2018 — COPM

2019 — L2 BRAS Dual Stack IPv4/IPv6

2020 — Поддержка мобильных сетей

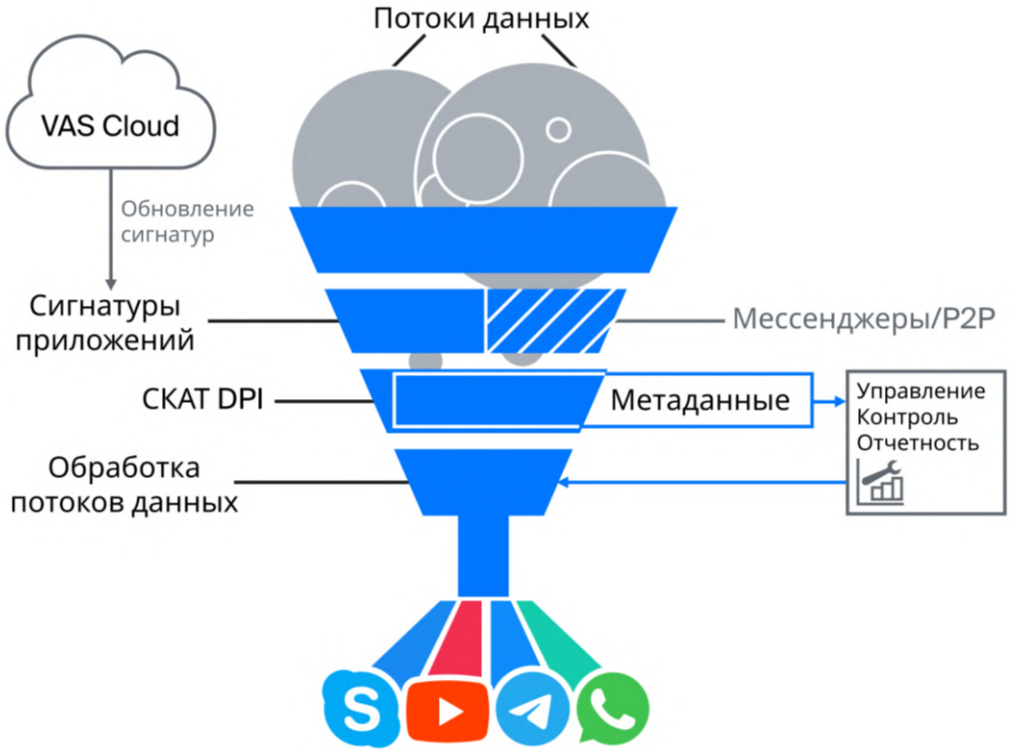
2021 — Border Router

2022 — VAS Services, LBS

2023 — VEOS, On-Stick, EPDG

2024 — PCEF, Diameter

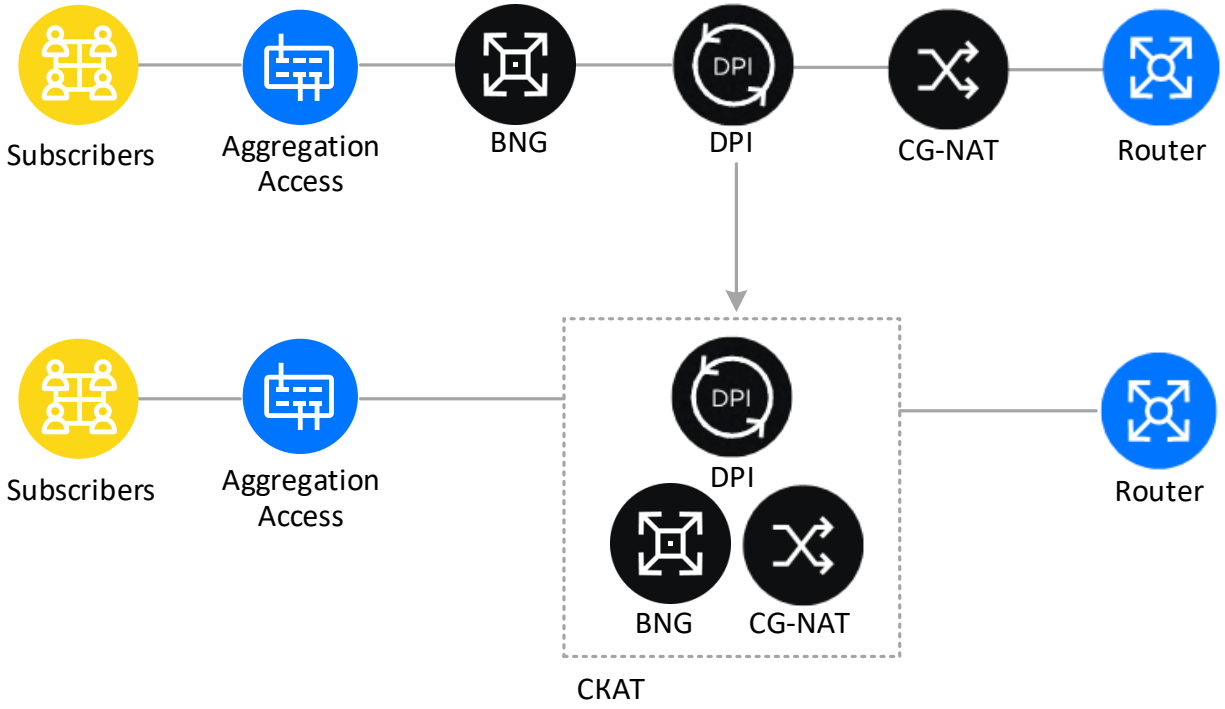
2025 — PGW, AntiDDoS



Замена решений

Sandvine	Cisco SCE	Cisco ASR	MikroTik	Ericsson SE
Allot	A10 Network	Juniper MX	Huawei NE	Nokia SR

Мультифункциональность



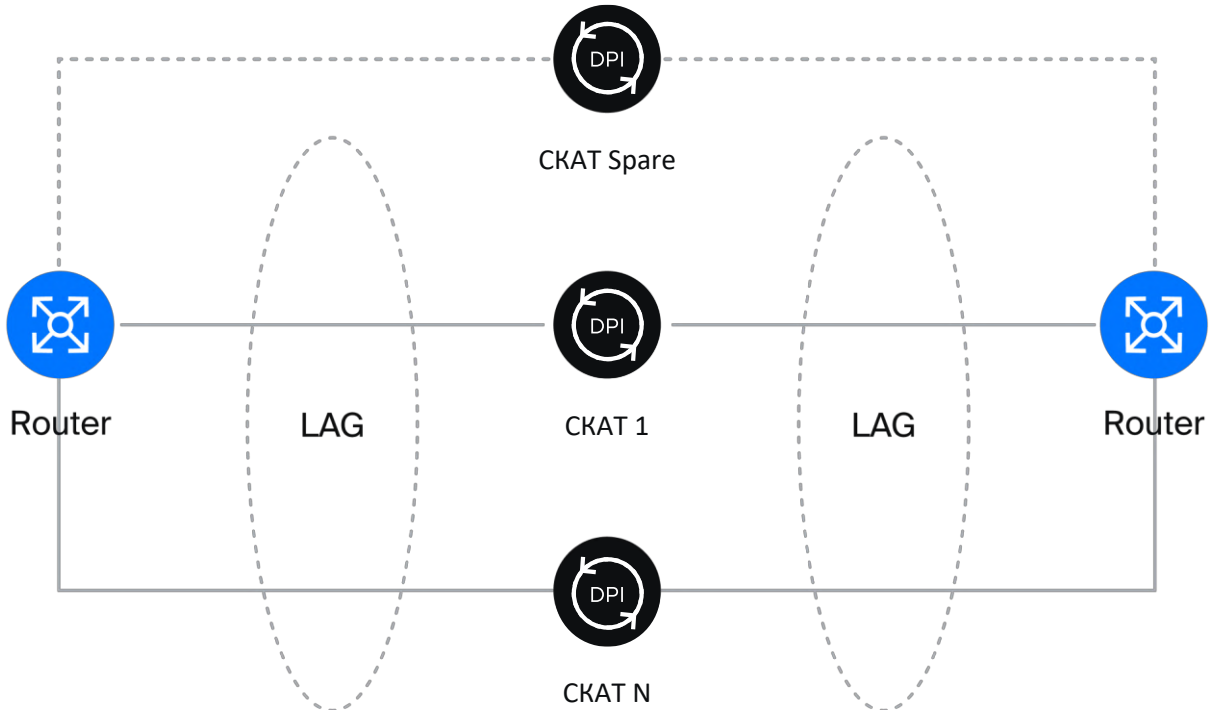
Многофункциональная платформа СКАТ DPI, установленная на обычном **x86-сервере,** заменяет целый набор сетевого оборудования.

Это упрощает процессы администрирования, обслуживания и масштабирования.

Производительность

ОПЦИЯ	СКАТ-40	СКАТ-100	СКАТ-200	СКАТ-400	СКАТ-800
Производительность	20	50	100	200	400
Количество абонентов (2Mbps per subscriber)	20K	50K	100K	200K	300K
Количество сессий	20M	60M	120M	240M	360M
Порты, GbE	4x10 2x25 2x40	10x10 4x25 4x40 2x100	20x10 8x25 8x40 4x100	16x25 8x100	10x100
Задержка (среднее), µс	**30**				
Платформа	1U-2U, 19”, AC/DC 2xPSU, N+1 Fan				

Резервирование



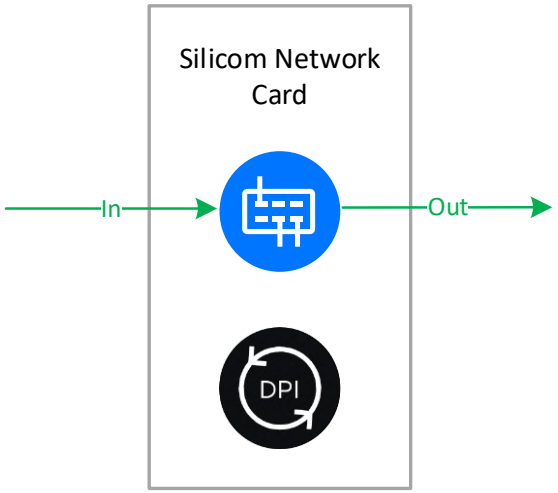
- Для режима L2 Bridge используется объединение нескольких устройств в LAG и балансировка сессий между ними
- Основная идея — разместить трафик от одного абонента на одном DPI-сервере. Балансировку можно организовать с помощью алгоритмов хеширования LACP или путем создания DPI-кластера с Network Packet Broker.
- Поддерживаемые режимы: Active-Active и Active-Standby
- Специальная цена на резервную лицензию

Поддержка Bypass

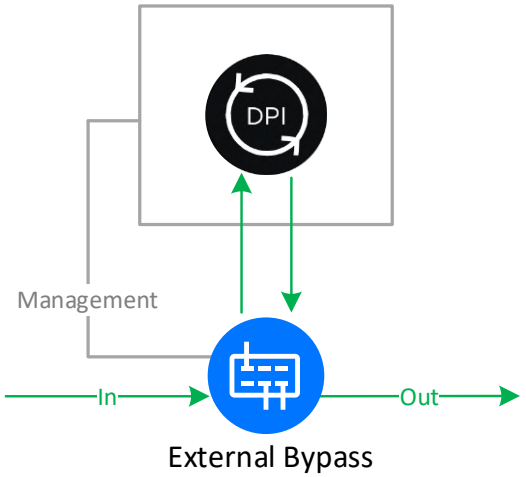
Опция Bypass позволяет гарантировать работоспособность при установке «в разрыв» и асимметрично в случаях:

- Неисправности оборудования
- Ошибки ПО
- Отключения питания
- Проведения ремонтных работ

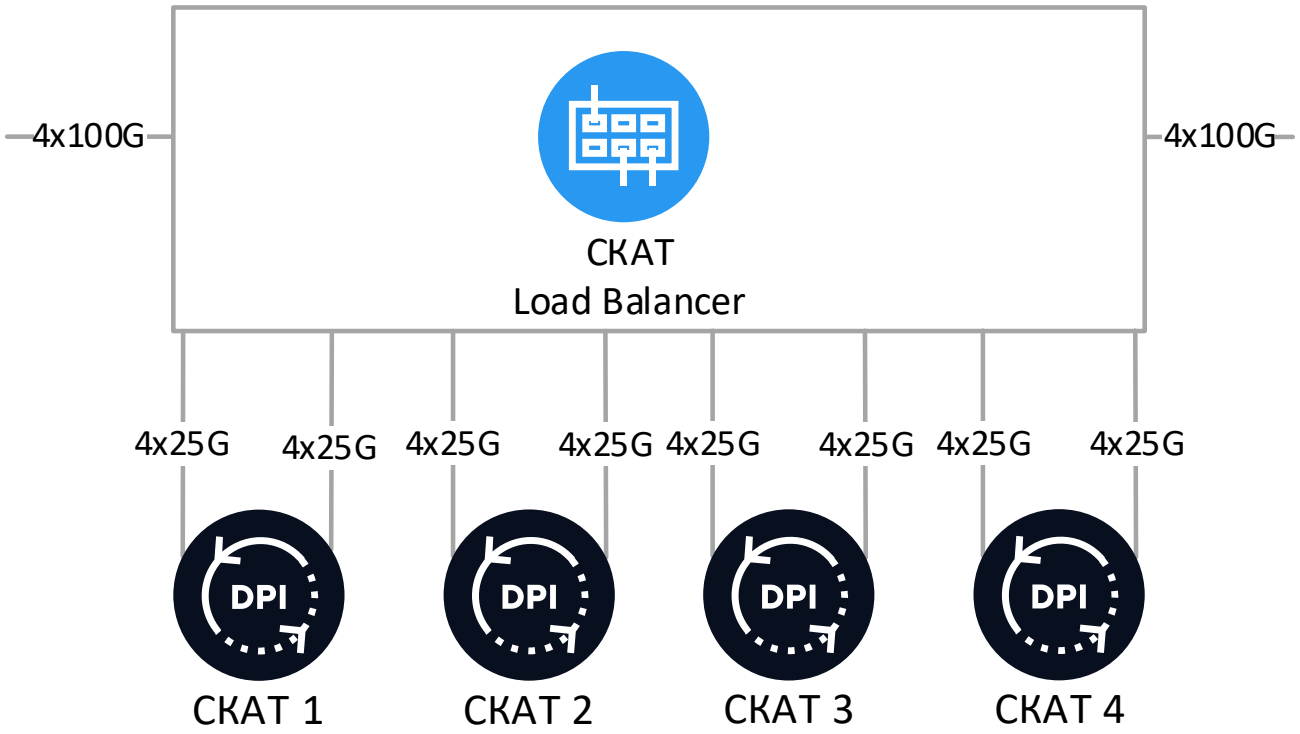
Встроенный bypass в карту Silicom



Внешний bypass любого производителя, управляемый СКАТ



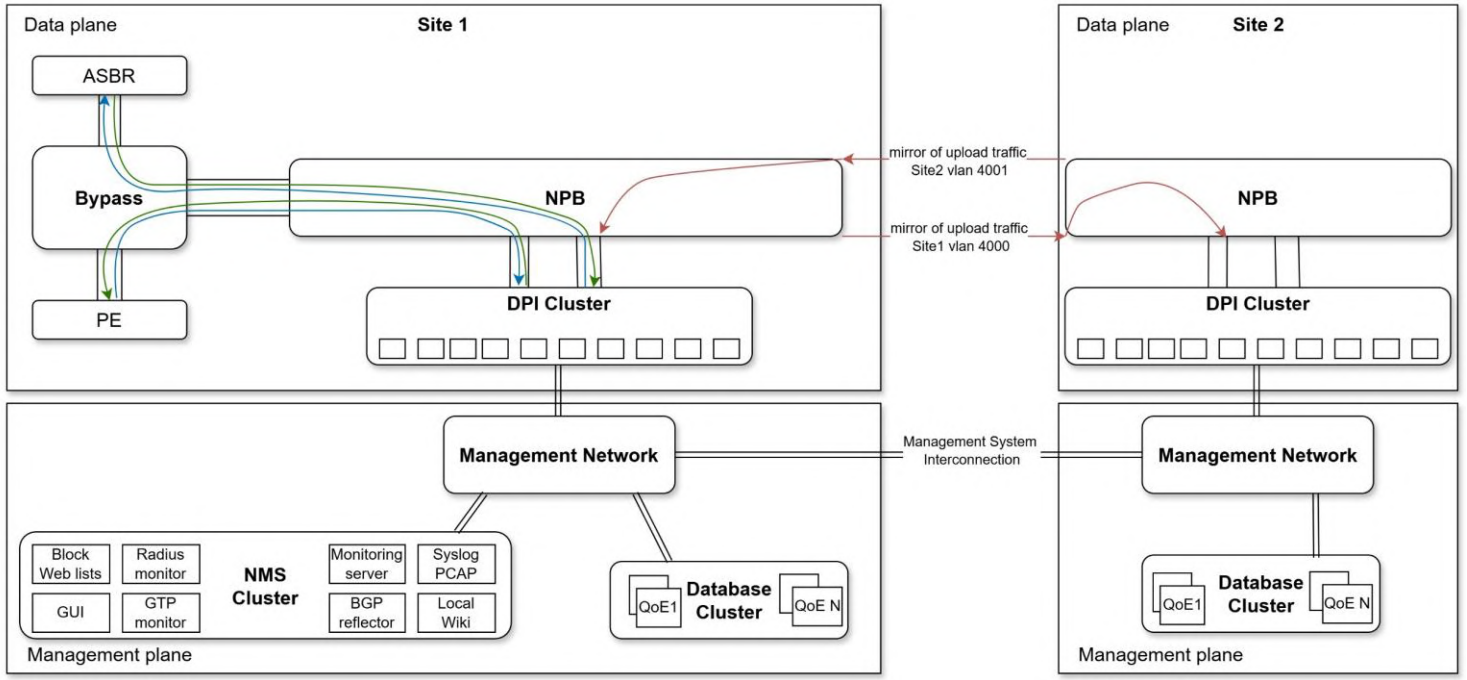
Производительность кластера



Обработка до **4,6 Тбит/с на один кластер** с использованием сторонних Network Packet Broker

Система сконфигурирована для резервирования по схеме N+X, где X — количество дополнительных узлов; также доступна схема N+N с полным резервированием всех компонентов.

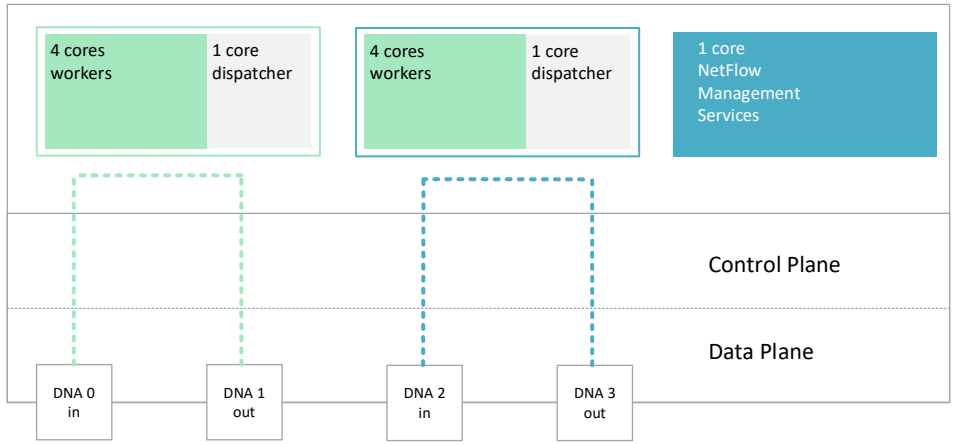
Архитектура кластера



Асимметричный трафик между сайтами:

Обработка асимметричного трафика между сайтами осуществляется путём передачи копии исходящего трафика с одного сайта на другой. Исходный трафик остаётся на исходном сайте, и маршрут трафика не меняется. Копия трафика передаётся в определённой VLAN по прямым каналам между NPB для минимизации задержки. Копия трафика балансируется по кластерному устройству DPI. DPI учитывает этот трафик при обнаружении сигнатуры, но не учитывает его при загрузке статистики. После обработки этот трафик отбрасывается в зависимости от конкретной VLAN. Использование этого метода увеличивает процент распознавания асимметричного трафика.

Архитектура платформы



Используется распределение нагрузки по ядрам процессора, что позволяет достигнуть вертикального масштабирования **до 400 Гбит/с full duplex** на один сервер

Control Plane

- VEOS – собственная операционная система с поддержкой от VAS Experts

Data Plane

- DPDK – Direct NIC Access technology

Факторы

- Доступные платформы
- x86 серверы
- Высокая производительность
- Мягкий лимит
- Масштабируемость
- Апгрейд своими руками
- Непрерывный рост

Основные функции

Фильтрация по URL/SNI/CN/IP/IP:port	Поддержка протоколов HTTP/HTTPS/QUIC
Блокировка трафика по IP/ASN/Сигнатурам	Автоматическое обновление и загрузка объемных списков. Создание собственных сигнатур на основе SNI, IP, CIDR.
Полисинг трафика по IP/ASN/Сигнатурам	Полисинг по сессиям, абонентам, каналам
Контроль загрузки канала и разметка трафика	Управление приоритетами и разметка трафика на основе протоколов и направлений
Продвинутое распознавание трафика	Настройка сигнатур и регулярные обновления гарантируют высокую точность распознавания трафика
Групповые политики: на абонента, на канал	Сопоставление абонентов и каналов с использованием RADIUS, GTP-C и BGP
Сбор статистики и отчеты	Подробная статистика по IP, ASN, DNS, сигнатурам и автоматическим e-mail отчетам

Протоколы и сигнатуры

СКАТ DPI применяет различные подходы для формирования стабильной сигнатуры

- Анализ образца (анализ паттернов)
- Численный анализ
- Поведенческий анализ
- Эвристический анализ
- Анализ протокола/состояния

СКАТ DPI содержит 3 типа сигнатур:

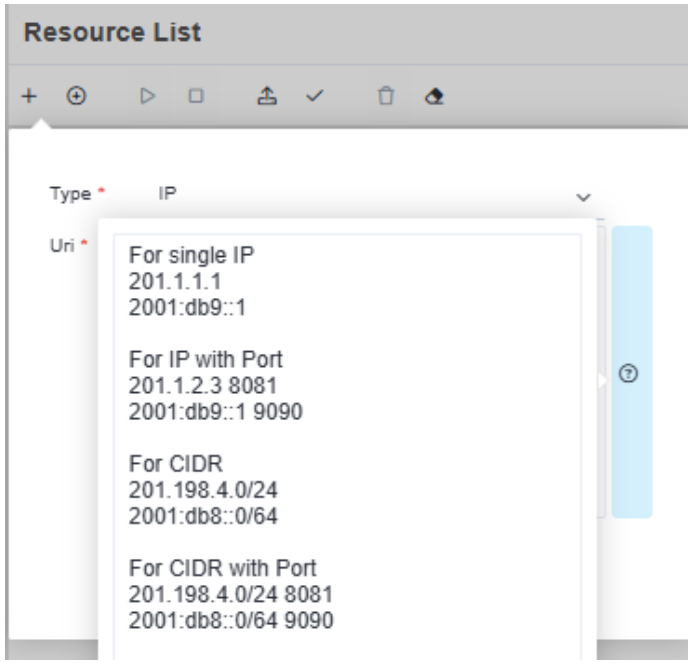
- **Встроенные сигнатуры,** которые являются частью движка DPI и обновляются вместе с программным обеспечением СКАТ
- **Динамические сигнатуры,** загружаемые в ядро во время работы СКАТ
- **Кастомные сигнатуры,** созданные пользователем в графическом интерфейсе и загруженные в ядро во время работы СКАТ

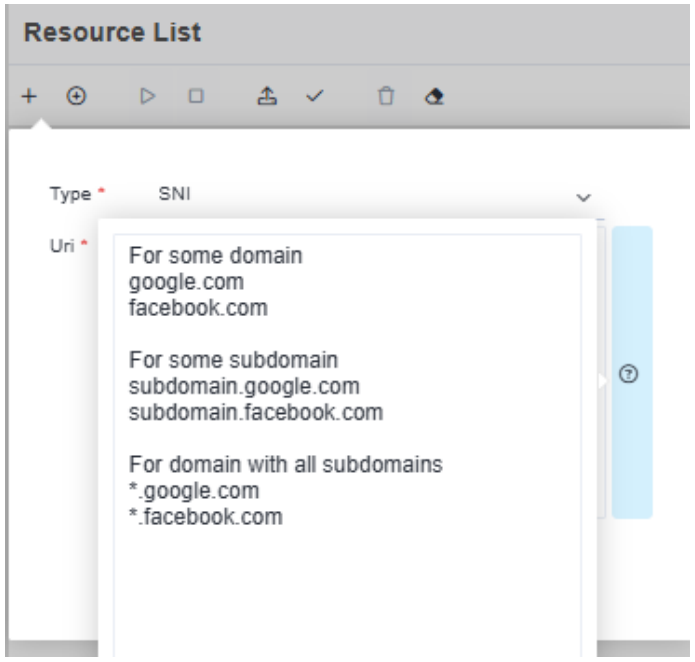
Кастомные протоколы и сигнатуры

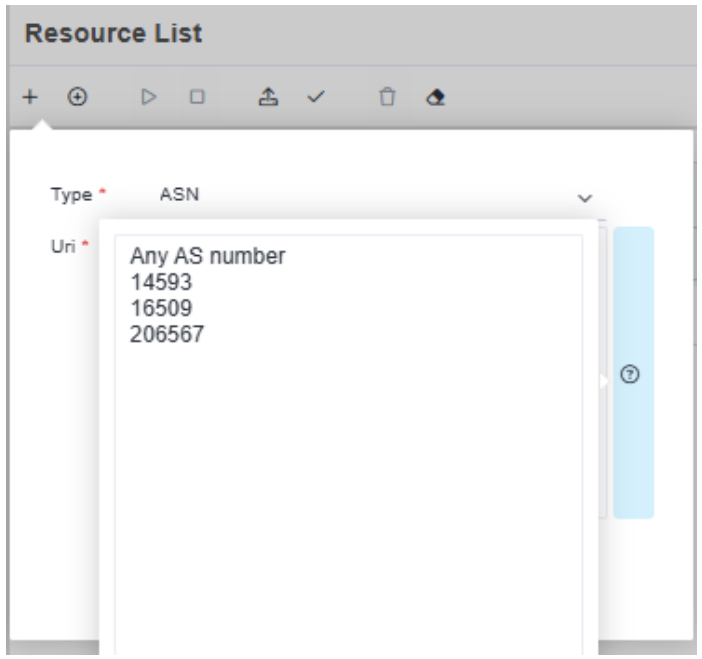
Механизм создания кастомного протокола определяет новый протокол на основе следующих критериев:

IP; IP + порт; CIDR; CIDR + порт; Номер AS; TLS Server Name Indication (SNI).

При отсутствии SNI проверяется Common Name.

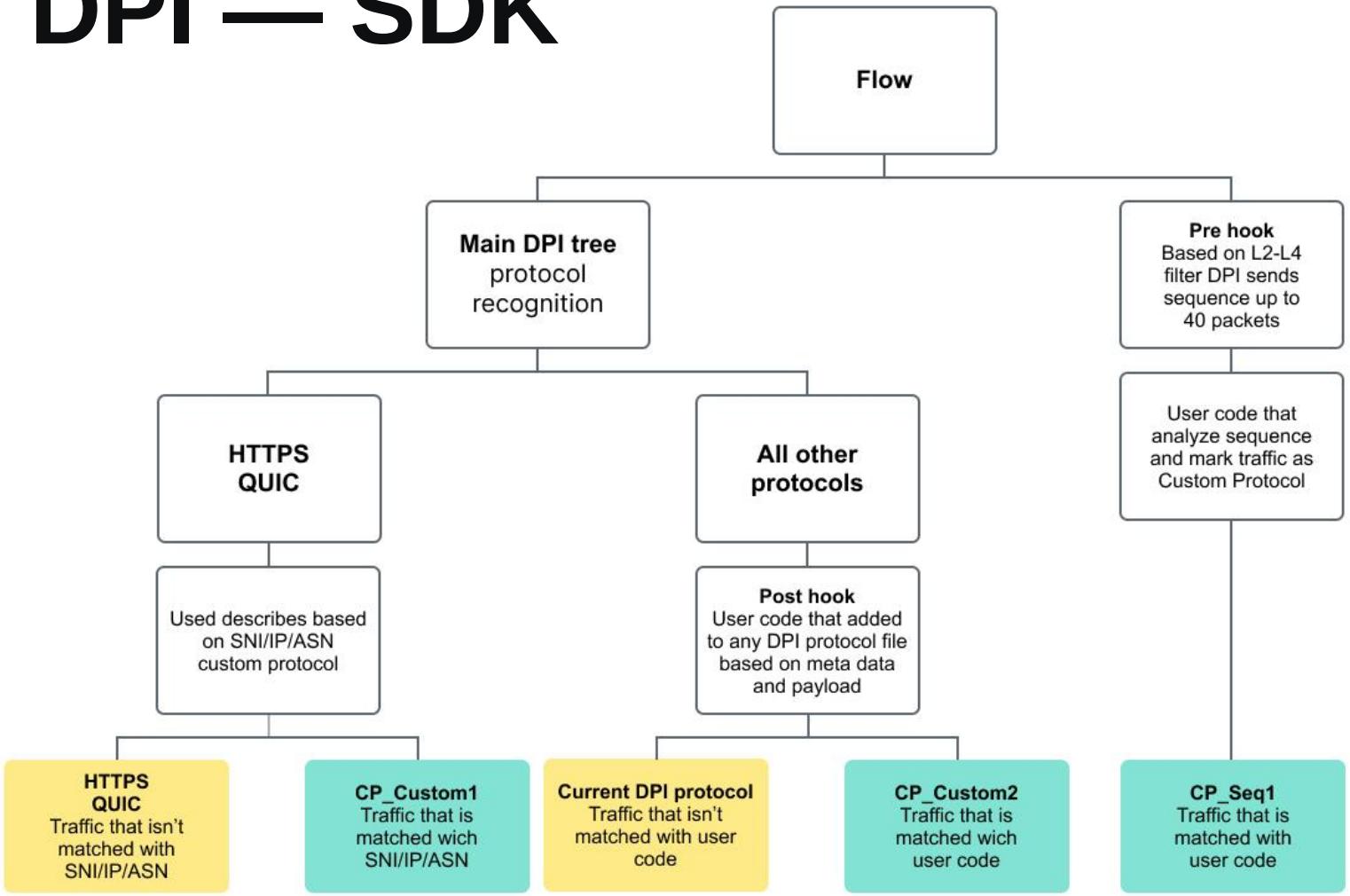






Инструменты DPI — SDK

DPI поддерживает кастомизацию протокола путем добавления дополнительного кода в дерево распознавания протокола.

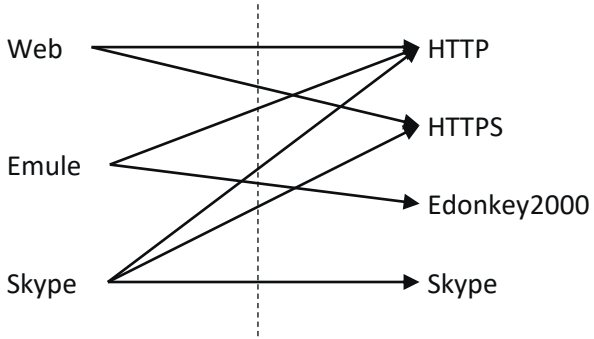


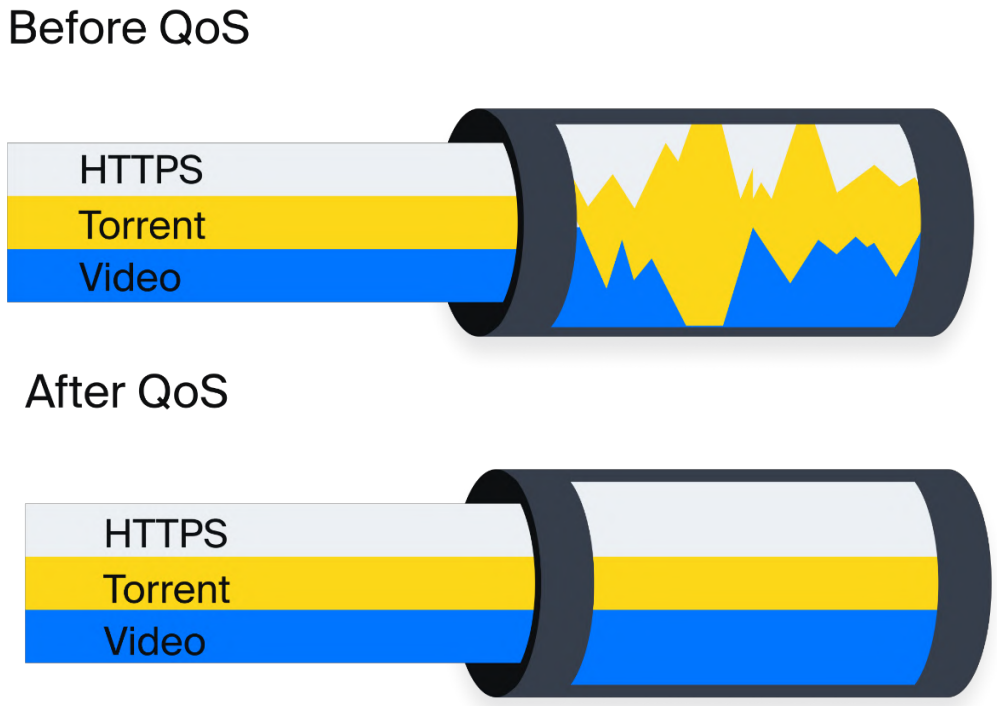
Приоритизация

По направлению

- Registered AS
- Customized AS

По протоколу / приложению





Уровни полисинга

Per Session

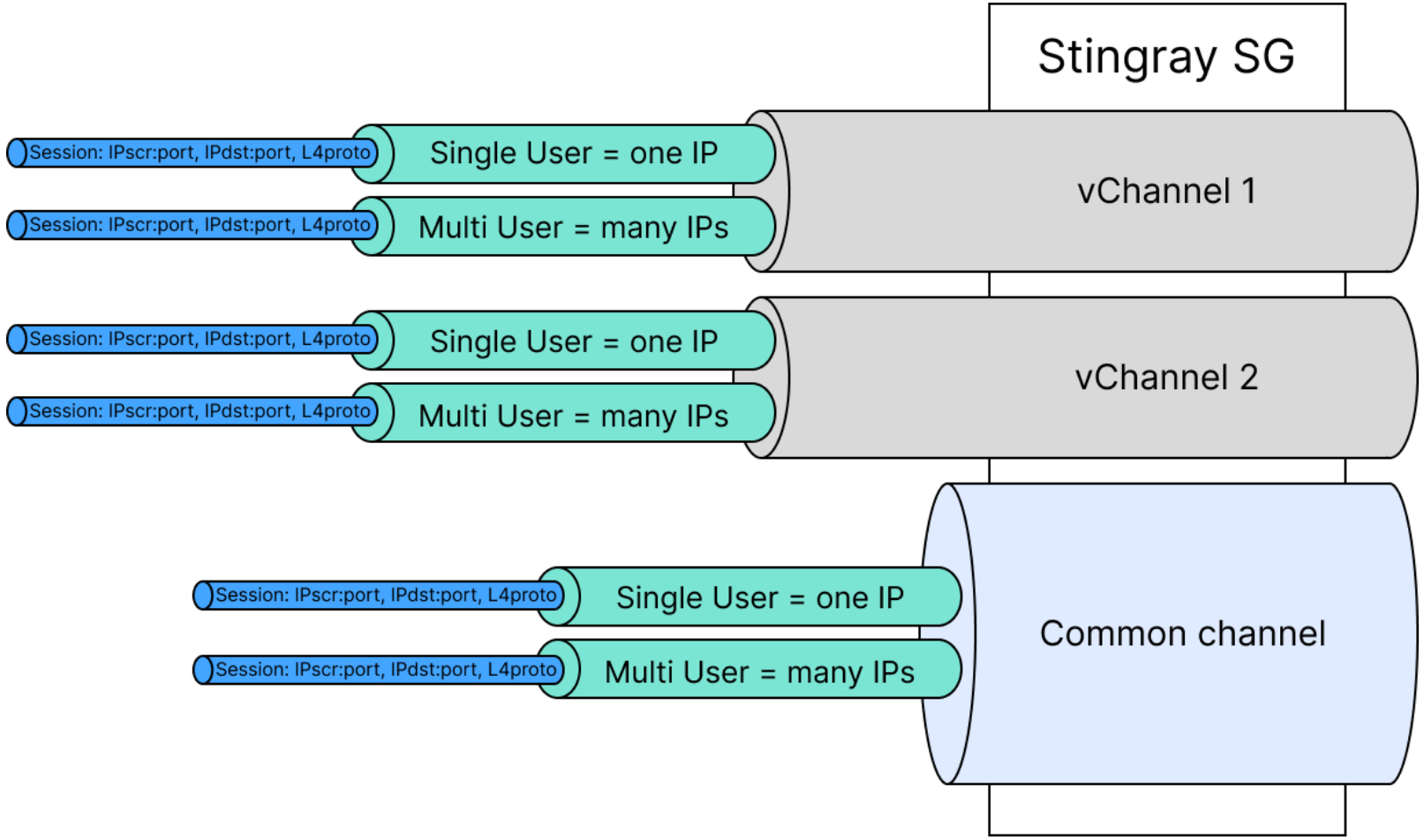
Контроль каждой сессии

Per Subscriber

Ограничение скорости на абонента с учетом приоритетов

Per Channel

Контроль скорости каналов для управления перегрузками



Гибкие тарифные планы

Задача

1. Ограничение по исходящему торренту
2. Максимальная скорость на локальные ресурсы
3. Приоритизация для:
   - Мессенджеров и SIP
   - HTTP, HTTPS, QIUC
   - Игровой сервис World of tanks

Сценарии применения:

1. Расписание для тарифных планов
2. Высокая скорость для локальных ресурсов
3. Повышение качества обслуживания (QoE)
4. Распределение пропускной способности между соединениями IPv4/IPv6

Classes (cs):

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

htb_inbound_root=rate 50mbit
htb_inbound_class0=rate 20mbit ceil 50mbit
htb_inbound_class1=rate 1mbit ceil 50mbit
htb_inbound_class2=rate 8bit ceil 50mbit
htb_inbound_class3=rate 8bit ceil 50mbit
htb_inbound_class4=rate 8bit ceil 1mbit
htb_inbound_class5=rate 100mbit static
htb_inbound_class6=rate 8bit ceil 50mbit
htb_inbound_class7=rate 8bit ceil 50mbit

htb_root=rate 50mbit
htb_class0=rate 20mbit ceil 50mbit
htb_class1=rate 1mbit ceil 50mbit
htb_class2=rate 8bit ceil 50mbit
htb_class3=rate 8bit ceil 50mbit
htb_class4=rate 8bit ceil 1mbit
htb_class5=rate 100mbit static
htb_class6=rate 8bit ceil 5mbit
htb_class7=rate 8bit ceil 5mbit

Фильтрация по черному списку

Описание	Характеристика
✓	Фильтрация по собственному списку оператора
✓	Использование централизованного списка для кластера серверов
В разрыв, зеркало асимметрично	Поддержка схем подключения
✓	Возможность управления фильтрацией по определенным пользователям и подсетям для организации сервисов фильтрации
✓	Блокировка трафика HTTP/HTTPS/QUIC
✓	Блокировка HTTPS/QUIC-трафика по SNI и Common Name
✓	Переадресация HTTP-запроса на страницу оператора для заблокированного URL
✓	Возможность собирать статистику по заблокированным страницам
✓	Возможность мониторинга загрузки списков и фильтрации
До 4 млрд URL	Максимальный размер списка

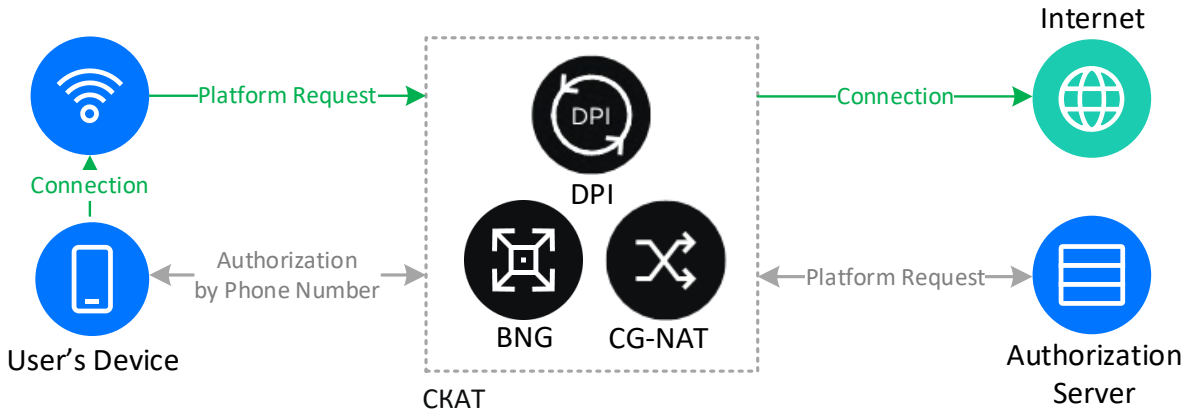
Фильтрация позволяет заблокировать определенный URL-адрес для протокола HTTP на странице.

Поддерживается блокировка по категориям, а также возможно использование комбинации категорий. Категоризированные списки автоматически загружаются из VAS Cloud.

Поддерживается фильтрация по SSL-ресурсам. SNI выглядит как *.domain.com, а регулярные выражения обеспечивают гибкую фильтрацию.

Белые списки и Captive portal

Опция «Белый список» позволяет ограничить список сайтов и ресурсов, доступных для абонента, и настроить редирект на определенную страницу при попытке перейти к другим ресурсам.



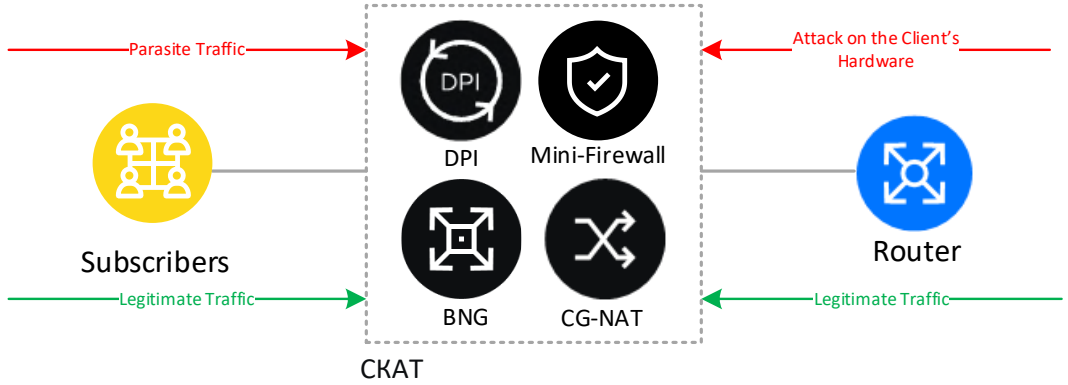
Применение:

1. Блокировка доступа при нулевом балансе с возможностью перейти к пополнению счета через авторизованные платежные системы.
2. Идентификация абонента в публичных сетях WiFi, разрешение определенных действий в сети WiFi для обеспечения доступа.

Mini Firewall

Задачи:

- Предотвратить взлом устройств пользователя по системным портам
- Заблокировать вредоносную активность от абонента – SPAM, BotNet



Рекомендации:

- Использовать статистику из модуля QoE в Личном Кабинете абонента
- Провести уведомление через СКАТ DPI о факте заражения и предложить решение, помощь по защите от вирусов

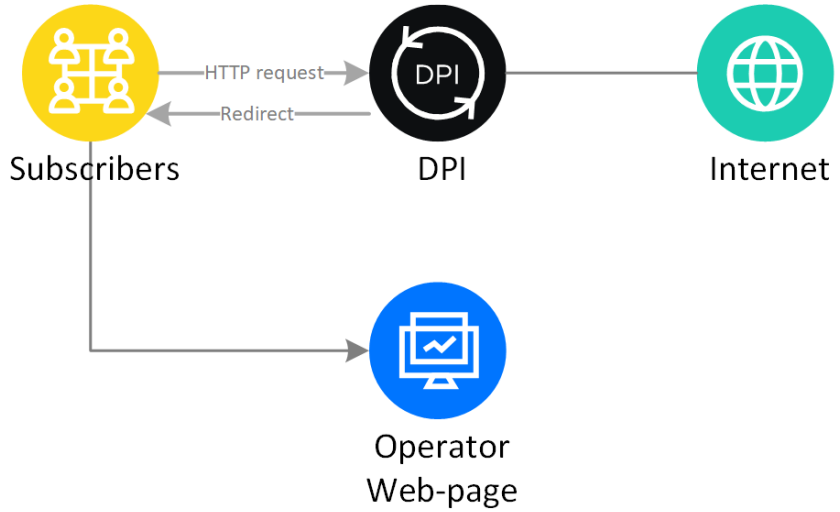
Маркетинг и уведомления

Возможности нотификации:

- Автоматическое сегментирование базы абонентов в соответствии с определенными критериями
- Настройка уведомлений в определенный период времени и день недели
- Возможность проведения нескольких кампаний одновременно

Применение:

1. Проведение опросов пользователей
2. Предупреждение о работах на сетях и перебоях связи
3. Информирование о новых услугах и акциях для абонентов

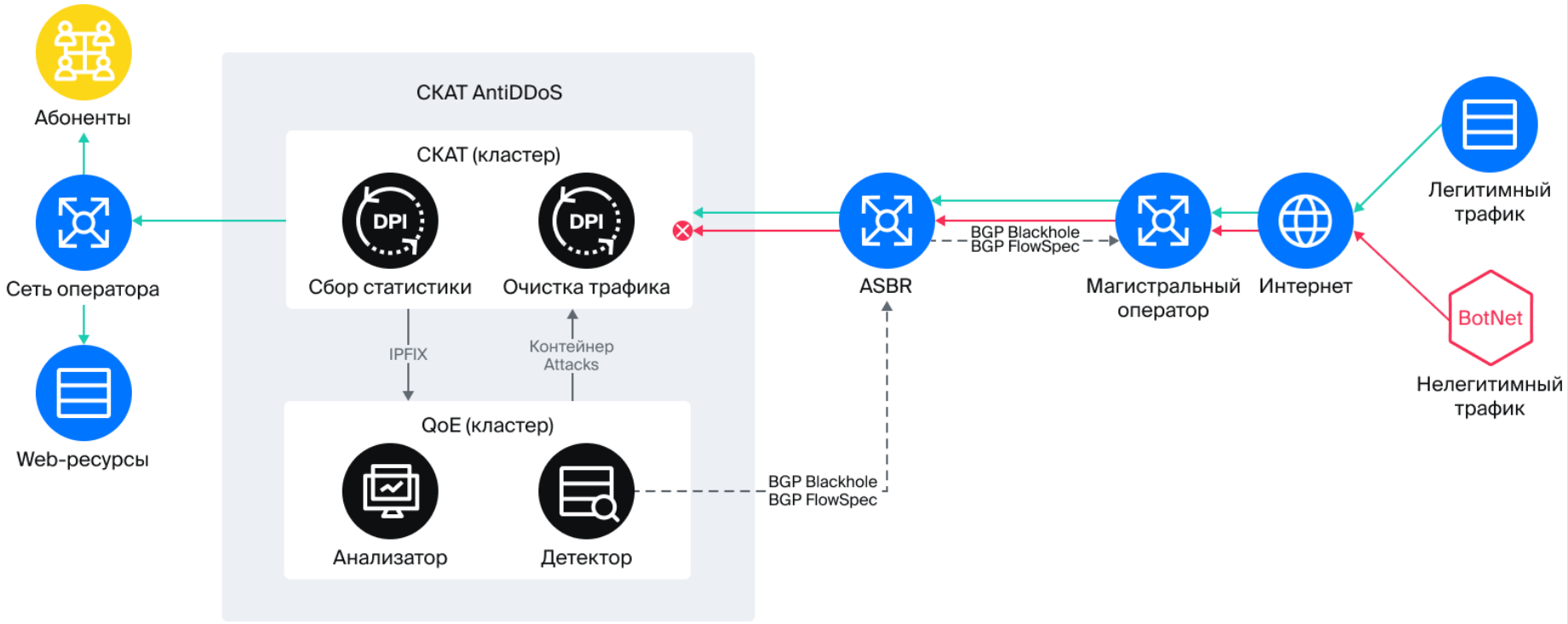


Выгрузка статистики и метаданных

СКАТ DPI обеспечивает распознавание > 95% трафика и выгрузку статистики по IPFIX (Netflow v10).

- FullFlow — поток IPFIX содержит информацию о соединениях, проходящих через DPI, полную статистику сессий и расширенную информацию DPI (идентификатор абонента: логин/MSISD/IMSI, порт IP, протокол DPI, объем трафика, метрики QoE).
- Clickstream — поток IPFIX содержит информацию о посещенных абонентом web-страниц (HTTP, HTTPS, QUIC)
- Metadata — поток IPFIX содержит данные полей, заданные для протоколов SIP, XMPP, MAIL (POP, IMAP, SMTP), FTP
- Extended (Raw) metadata — поток IPFIX содержит необработанные усеченные IP-пакеты для некоторых протоколов, таких как последовательности STUN и сеансы протокола управления VoIP. DPI отправляет необработанные данные в систему СОРМ для последующей обработки данных при необходимости.
- DNS — поток IPFIX содержит все запросы служб доменных имен
- RADIUS — поток IPFIX содержит все атрибуты RADIUS
- GTP — поток IPFIX содержит все атрибуты GTP-C, используемые для решения LBS

Решение AntiDDoS на базе QoE



Анализ

Детектирование

Очистка

Blackhole

FlowSpec

Защита от SYN Flood DDOS-атак

- Обнаруживает атаку при превышении указанного порога запросов, неподтвержденных клиентом SYN.
- Самостоятельно, вместо защищенного сайта, отвечает на запросы SYN.
- Организует сеанс TCP с защищенным сайтом после подтверждения запроса клиентом.

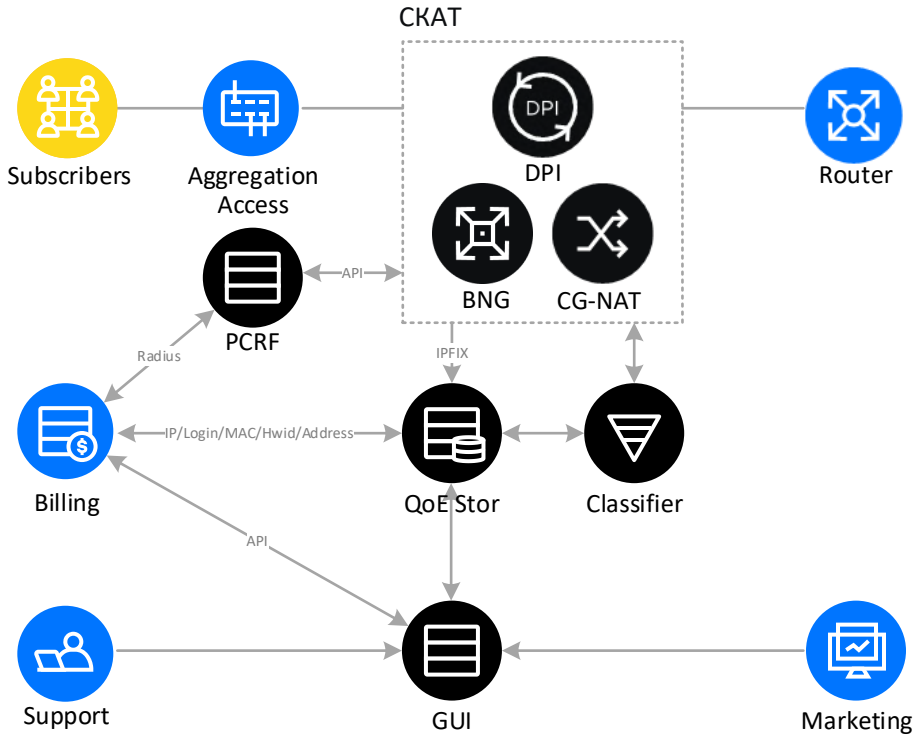
СКАТ DPI позволяет применять защиту в ручном режиме или автоматически активировать защиту при превышении порогов.

Модуль Quality Of Experience

Модуль Quality of Experience (QoE) — это программный продукт для сбора статистики и оценки качества восприятия услуг.

Собранная модулем статистика накладывается на особые метрики для определения пользовательского опыта и отвечает на вопрос, насколько качественные услуги связи и доступа в Интернет получает конечный пользователь.

Полученные данные позволяют оператору предпринять необходимые действия для улучшения качества услуг и, как следствие, для повышения лояльности абонентов.



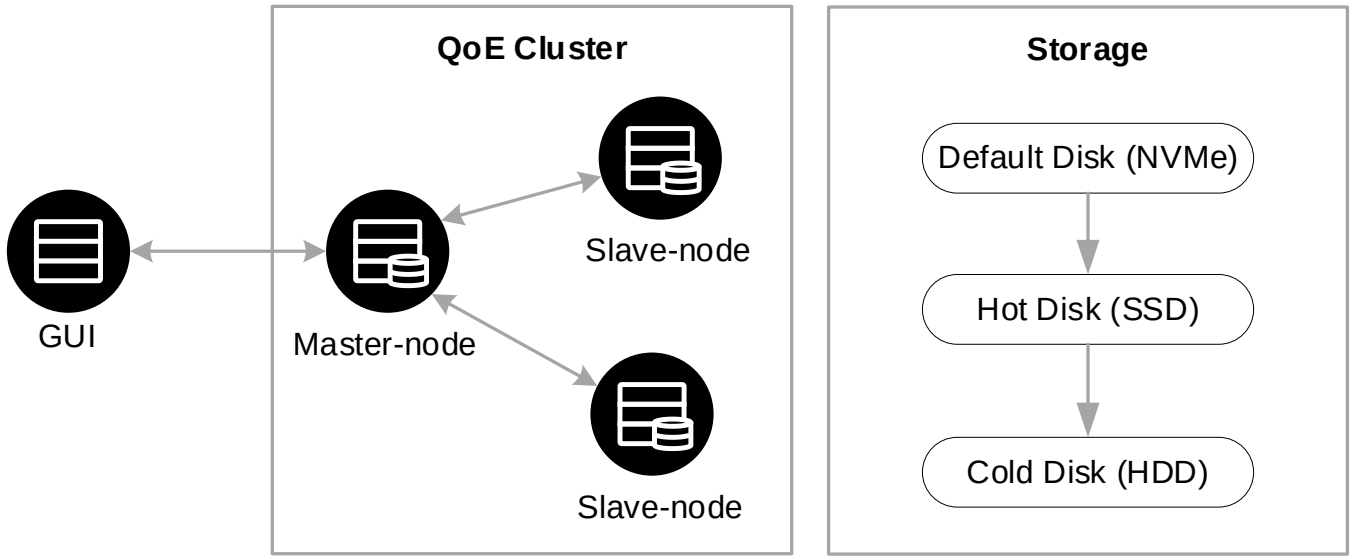
Архитектура QoE

QoE Stor основан на базе данных ClickHouse с возможностью создания кластера из нескольких узлов:

В кластере назначается главный узел, который принимает запросы от графического интерфейса и отправляет запросы на подчинённый узел.

Каждый подчинённый узел формирует отчёт на основе собственных данных и передаёт его главному узлу.

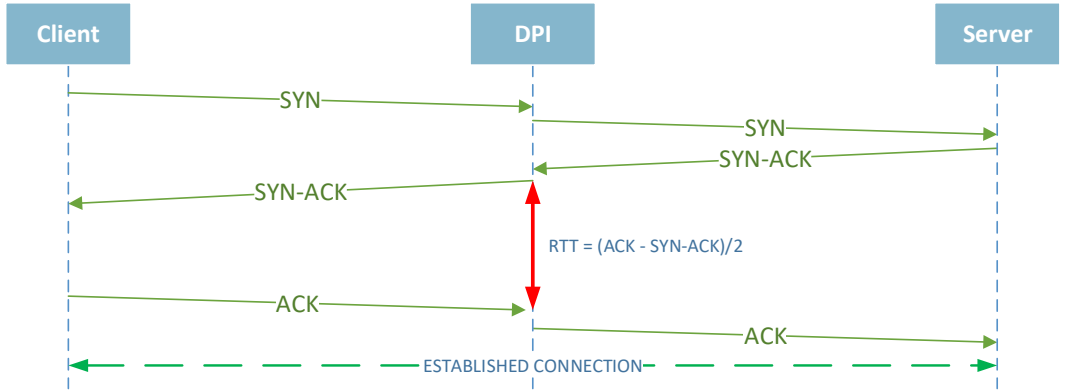
Главный узел агрегирует полученные ответы от подчинённого узла и формирует результирующее представление для визуализации в графическом интерфейсе.



Такая иерархия позволяет линейно масштабировать кластер при добавлении новых узлов без необходимости увеличения производительности главного узла.

Метрики QoE

1. Показатели круговой задержки (RTT)
2. Показатели количества перезапросов
3. Количество сессий, устройств, агентов, IP-адресов на абонента
4. Распределение трафика по прикладным и транспортным протоколам
5. Распределение трафика по направлениям и AS
6. Кликстрим для каждого абонента



Как использовать QoE-метрики?

Повышение продаж

- Продажа новых сервисов, Wi-Fi оборудования, тарифных планов
- Борьба с оттоком и анализ причин, повышение лояльности
- Таргетированная реклама с использованием профилей абонентов
- Продажа антивируса

Проактивная поддержка

- Мониторинг качества аплинков на основе задержек и изменений потребляемого трафика
- Поиск проблем с клиентским оборудованием, Wi-Fi, свитчами доступа и агрегации
- Определение оптимальных точек пиринга и связности через Uplink

Как использовать QoE-метрики?

Удержание базы абонентов

- Определение деградации качества услуг у абонента и оперативное реагирование
- Работа с возможным оттоком и анализ причин оттока в прошлом
- Автоматизация опроса после выезда мастера к абоненту

Повышение лояльности

- Проведение маркетинговых кампаний по новым тарифам, услугам и предложениям с учетом интересов абонентов
- Услуга по предоставлению информации о загруженности и качестве канала через личный кабинет абонента
- Уведомления об активности BotNet в сети (актуально для IoT)
- Уведомление о вирусной активности

Отчеты QoE

Встроенные отчеты

- Доступны отчёты по датасетам: NetFlow; Raw Full NetFlow; Clickstream; Raw Clickstream; DNS Flow; Raw DNS Flow
- Фильтры в отчётах позволяют пользователям уточнять данные по определённым критериям, упрощая поиск необходимой информации в больших датасетах
- Менеджер больших отчётов позволяет пользователям инициировать создание отчётов в фоновом режиме и ставить несколько отчётов в очередь на выполнение

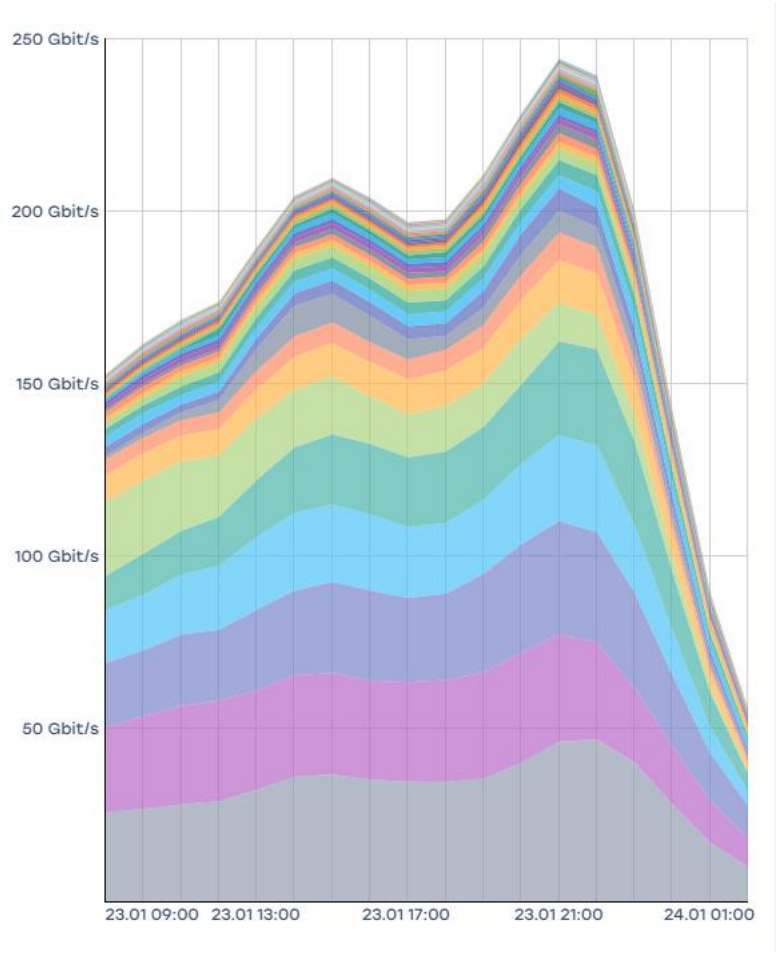
Email-отчеты

- Поддержка всех встроенных отчётов с возможностью включения фильтров
- Гибкое управление отчётами по электронной почте: период, тема письма
- Поддерживаются различные форматы: Excel, CSV, PDF, PNG
- Отслеживание статуса: «Ожидание», «Кэширование», «Проверка», «Уведомление»

Графический интерфейс

1. Ограничение доступа по ролям
2. Логирование действий пользователя
3. Управление несколькими DPI: мониторинг и конфигурация
4. Управление сервисами
5. Создание тарифных планов
6. Создание NAT-пулов
7. Работа с QoE-аналитикой
8. Интеграция по API

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			



Сопоставление из RADIUS и GTP

DPI поддерживает привязку IP-логина из RADIUS, порты: 1813, 1814, 1815 и т.д.

1. Login = User-Name или Calling-Station-ID
2. Префиксы Login на основе NAS-IP-Address
3. IP = Framed-IPv4-Address, Framed-IPv6-Address, Delegated-IPv6-Prefix

DPI поддерживает привязку IP-логина из зеркала трафика GTP-C.

Поддерживаются GTPv1 и GTPv2 с интерфейсов S11/S8/S5.

Правила привязки:

1. Логин = IMSI или MSISDN
2. IP = Framed-IPv4-Address, Framed-IPv6-Address, Delegated-IPv6-Prefix

Сопоставление из BGP

DPI поддерживает привязку IP-префикса к каналам/абонентам через сигнализацию BGP.

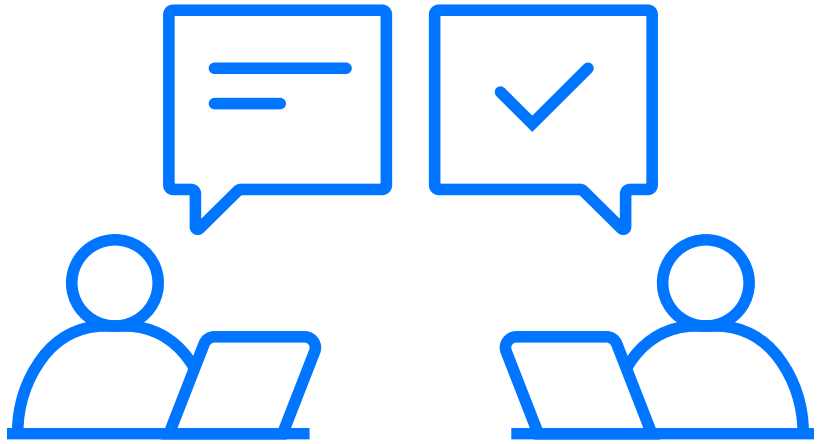
При использовании сигнализации BGP клиенту необходимо настроить на маршрутизаторе(ах) новый сеанс с BGP-рефлектором, который входит в состав решения. BGP-рефлектор только принимает сообщения и не отправляет никакой маршрутной информации для однорангового узла.

Правила привязки:

1. Канал определяется на основе BGP community или BGP AS-path
2. Пользователь определяется на основе BGP community или BGP AS-path

Поддержка на каждом этапе

1. Предоставление тестовой версии для проверки функциональности
2. Поддержка внедрения и консультирование на каждом этапе
3. Три уровня поддержки: Next Business Day, 8x5 и 24x7
4. Регистрация обращения 24x7 по e-mail и телефону



Контакты

dpi@vas.expert

vasexperts.ru