Программное обеспечение «Платформа балансировки сетевого трафика flxGATE (Флексигейт)»

ОПИСАНИЕ ТЕХНИЧЕСКОЙ АРХИТЕКТУРЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2026

Аннотация

В документе приведено описание архитектуры платформы балансировки сетевого трафика **flxGATE (Флексигейт)**.

Содержание

Введение

flxGATE (Флексигейт) – это платформа балансировки сетевого трафика, предназначенная для управления потоком трафика в сети передачи данных с использованием гибкой логики и настраиваемым набором правил. Программная платформа балансировки сетевого трафика работает на уровнях L4-L7 модели OSI/ISO (сетевой модели стека сетевых протоколов).

flxGATE (Флексигейт) позволяет:

1. Реализовать техническую оптимизацию, масштабируемость и обеспечить высокую доступность вычислительной инфраструктуры.
2. Сократить затраты на стоимость вычислительной инфраструктуры и процессы ее эксплуатации за счет:
   - оптимизации использования ресурсов и их максимальной утилизации,
   - снижения операционных расходов через автоматизацию и упрощение процессов конфигурирования сервисов,
   - предотвращения потерь от простоев сервисов/минимизация времени недоступности сервисов,
   - обеспечения стабильности сервисов для пользователей,
   - автоматизации операций восстановления сервисов при обнаружении проблем.
3. Улучшить безопасность, мониторинг и наблюдаемость инфраструктуры за счет:
   - изоляции внутренних сервисов от внешних угроз,
   - удобного управления SSL/TLS терминацией и единой политикой обслуживания сертификатов безопасности,
   - централизованного сбора метрик производительности,
   - логирования всех запросов/ответов.

Платформа балансировки сетевого трафика **flxGATE (Флексигейт)**:

1. Обеспечивает балансировку нагрузки на инфраструктуру на уровнях L4 (транспортный уровень) и L7 (уровень приложений) с поддержкой протоколов TCP, UDP, QUIC, и расширенным набором алгоритмов балансировки (Round Robin, WRR, Least Connections, WLC, IP Hash, Source IP Hash).
2. Позволяет реализовывать функции проверки состояния (health check) серверов/сервисов с автоматическим исключением неработающих серверов/сервисов и с восстановлением их обслуживания при восстановлении работоспособности.
3. Обеспечивает поддержку протоколов L7 (уровня приложений): HTTP/1.1, HTTP/2, HTTP/3, HTTPS, gRPC.
4. Обеспечивает высокую доступность подсистемы управления платформы.
5. Реализует:

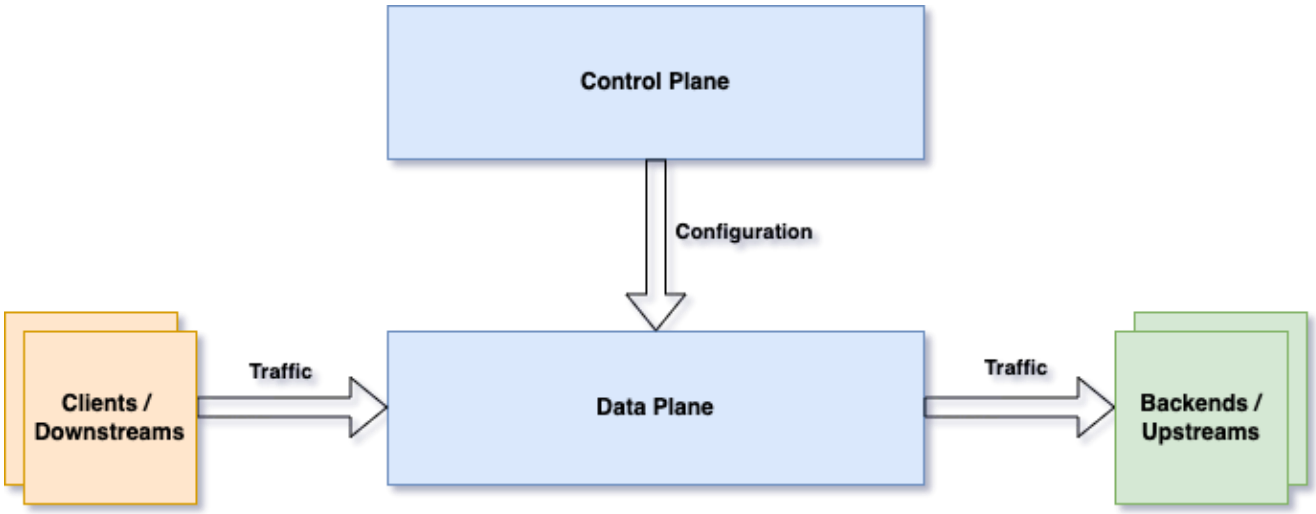
- гибкую логику управления сетевым трафиком с использованием большого набора средств настройки правил маршрутизации;
- сбор метрик производительности и статистики по обрабатываемому трафику;
- логирование событий с возможностью передачи во внешние системы.

1 Общая архитектура решения

Архитектурно решение flxGATE состоит из двух слоев

- **Data Plane** - слой обработки трафика
- **Control Plane** - слой управления узлами обработки трафика

1.1 Схема решения



1.2 Функциональность

1.2.1 Control Plane

Обеспечивает централизованное управление конфигурацией узлов обработки трафика.
Основные функции:

- **Управление конфигурацией**: предоставление REST API для создания, изменения и удаления конфигурационных объектов (узлы, слушатели, кластеры, маршруты, секреты)
- **Доставка конфигурации**: распространение изменений конфигурации до узлов Data Plane в режиме реального времени
- **Хранение состояния**: централизованное хранение конфигурационных данных в распределенном хранилище
- **Мониторинг изменений**: отслеживание изменений в хранилище и автоматическая синхронизация с узлами обработки трафика
- **Управление узлами**: контроль жизненного цикла узлов, блокировка конфигурации для безопасного обновления

1.2.2 Data Plane

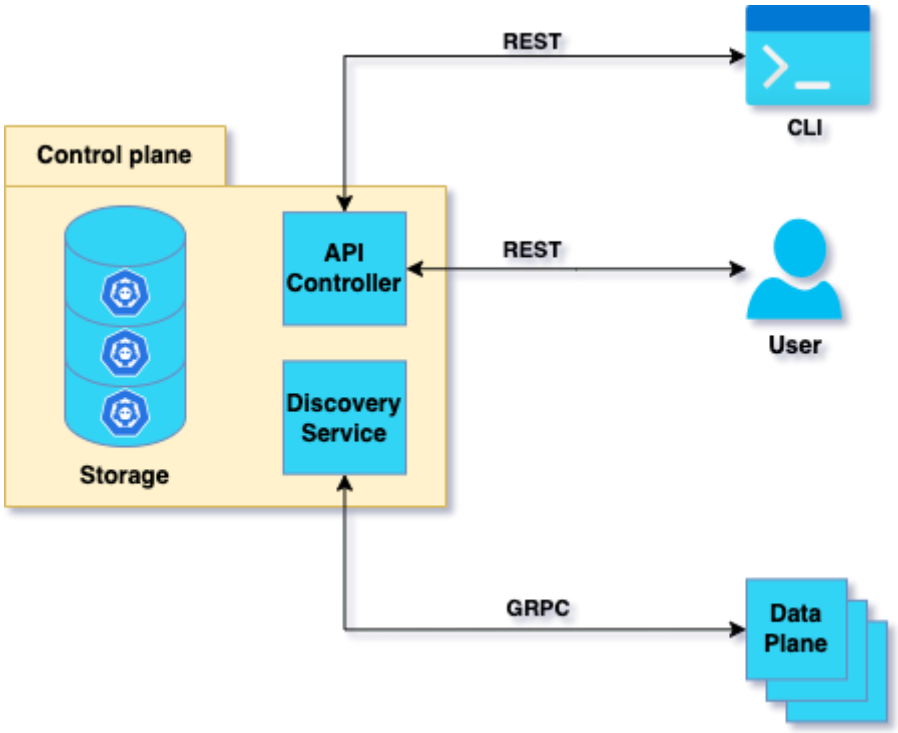
Отвечает за обработку сетевого трафика на основе конфигурации, полученной от Control Plane.
Основные функции:

- **Обработка трафика**: прием, маршрутизация и балансировка входящего сетевого трафика
- **Динамическая конфигурация**: получение и применение обновлений конфигурации от Control Plane без перезапуска
- **Балансировка нагрузки**: распределение запросов между бэкенд-серверами с использованием различных алгоритмов (round-robin, least-request и др.)
- **Маршрутизация**: определение путей прохождения трафика на основе правил маршрутизации
- **Фильтрация трафика**: применение сетевых и HTTP фильтров для обработки, модификации и контроля трафика
- **Обеспечение безопасности**: поддержка TLS/SSL терминации, управление сертификатами и секретами
- **Мониторинг и наблюдаемость**: сбор метрик, логов доступа и статистики производительности
- **Управление маршрутизацией**: поддержка протоколов маршрутизации BGP, OSPF, VRRP, динамическое изменение маршрутов

2 Control Plane

Подсистема управления узлами обработки трафика

2.1 Компоненты



2.1.1 API Controller

Реализует интефейс управления конфигурацией узлов Data Plane по протоколу REST.

Позволяет управлять основными сущностями конфигурации Data Plane: node, endpoint, clusters, listeners и т.д.

2.1.2 Discovery Service

Обеспечивает распространение изменений конфигурации до узлов Data Plane в режиме реального времени по протоколу GRPC.

2.1.3 Storage

Обеспечивает централизованное хранение конфигурационной информации.

Может быть развернуто в виде распределенного хранилища.

2.1.4 CLI

Обеспечивает возможность интерактивного управления узлами управления и обработки трафика.

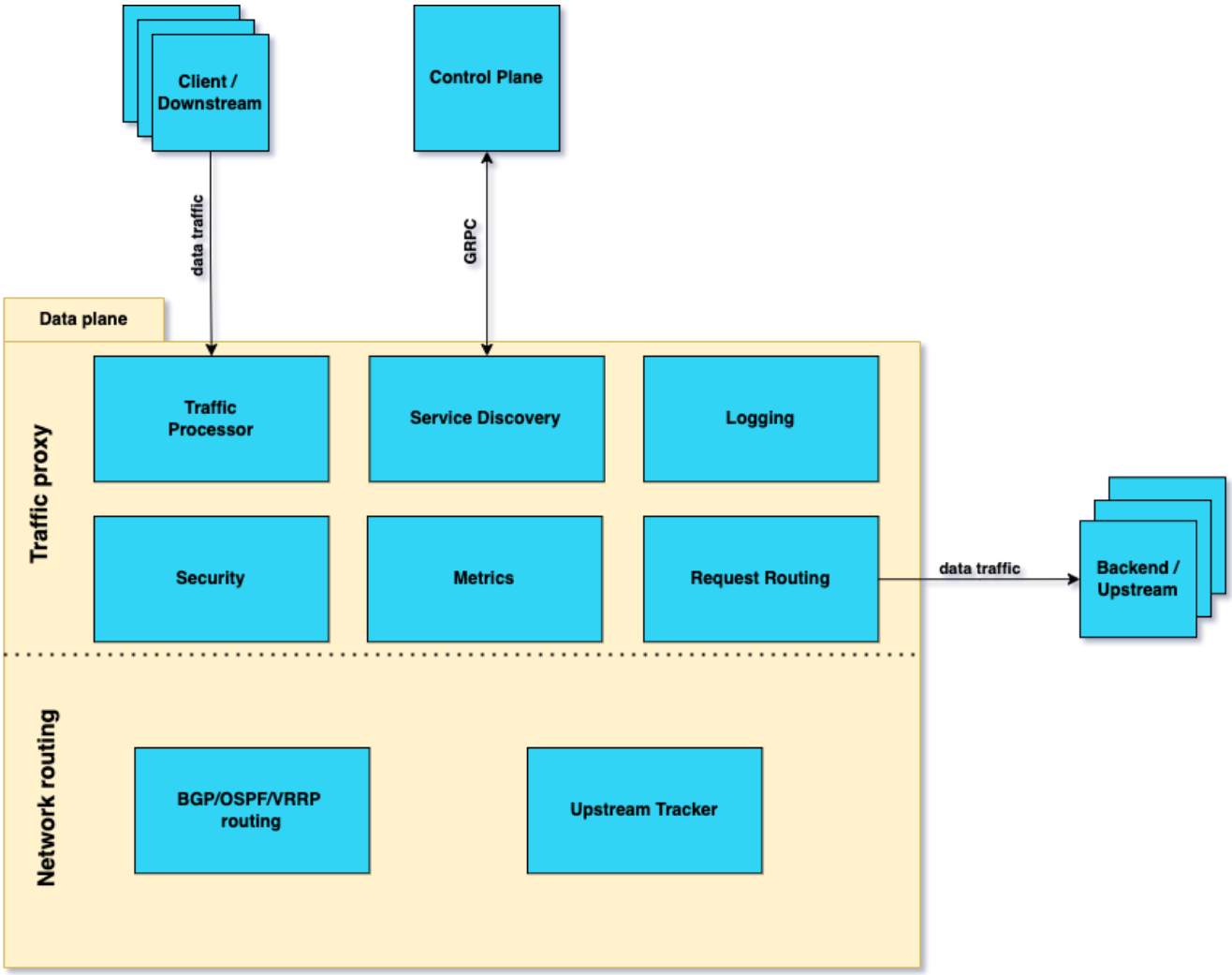
3 Data Plane

Подсистема обработки и управления трафиком

3.1 Компонентая схема

Состоит из двух основных подсистем:

- **Traffic proxy**: система обработки трафика
- **Network routing**: система управления сетевой маршрутизацией



3.1.1 Traffic Proxy

Реализует логику обработки трафика в соответствии с заданной конфигурацией.

Предоставляет функции обработки и маршрутизации трафика, сбора метрик, динамического конфигурирования, журналирования и безопасности.

3.1.1.1 Traffic Processor

Реализует функцию обработки и фильтрации поступающих запросов/пакетов.

3.1.1.2 Service Discovery

Реализует интерфейс взаимодействия с Control Plane для получения актуальной информации о конфигурации.

3.1.1.3 Logging

Реализует функционал журналирования: access-логи, трассировка.

3.1.1.4 Security

Реализует функции безопасности: работа с TLS/SSL, аутентификация/авторизация, хранение и использование чувствительной информации.

3.1.1.5 Metrics

Реализует сбор внутренних метрик с целью их дальнейшей передачи через систему мониторинга (Prometheus)

3.1.1.6 Request Routing

Реализует правила и действия для маршрутизации проходящего через Data Plane запроса.

3.1.2 Network routing

Реализует логику изменения маршрутизации на узле обработки трафика.

3.1.2.1 BGP/OSPF/VRRP routing

Предоставляет функции работы с протоколами маршрутизации BGP/OSPF/VRRP.

3.1.2.2 Upstream Tracker

Реализует логику проверки изменения маршрутизации в зависимости от состояния серверов, на которые балансируется трафик.

Термины, сокращения и определения

Термин	Определение
API	Application Programming Interface. Программный интерфейс
CA	Certification Authority. Центр сертификации, удостоверяющий центр
CLI	Command Line Interface. Интерфейс командной строки
CRL	Certificate Revocation List. Список отзыва сертификатов
DHCP	Dynamic Host Configuration Protocol. Протокол динамического конфигурирования узлов
DNS	Domain Name System. Система доменных имен
flxGATE	Платформа управления сетевым трафиком
HA	High Availability. Высокая доступность
HTTP	HyperText Transfer Protocol. Протокол передачи гипертекста
ICMP	Internet Control Message Protocol. Протокол межсетевых управляющих сообщений. Передает сообщения об ошибках и других исключительных ситуациях, которые возникают при передаче данных
ID	Идентификатор
IP	Интернет-протокол
IPMI	Intelligent Platform Management Interface. Интеллектуальный интерфейс управления платформой
ISO-образ	Архивный файл, который содержит идентичную копию (образ) данных
JSON	JavaScript Object Notation. Текстовый формат обмена данными, основанный на JavaScript
LDAP	Lightweight Directory Access Protocol. Протокол быстрого доступа к каталогам
LLDP	Link Layer Discovery Protocol. Протокол канального уровня, который позволяет сетевым устройствам анонсировать в сеть информацию о себе и о своих возможностях, а также собирать информацию о соседних устройствах
MAC-адрес	Media Access Control Address. Уникальный идентификатор. Присваивается каждому сетевому оборудованию
MTU	Maximum Transmission Unit. Максимальная единица передачи
NFS	Network File System. Сетевая файловая система
NIC	Network Interface Card. Сетевая интерфейсная карта
OpenLDAP	OpenLDAP. Протокол облегченного доступа к каталогам с открытым исходным кодом
QoS	Quality of Service. Набор технологических решений для оптимизации сетевого трафика с помощью назначаемых приоритетов передачи информации

Термин	Определение
RBAC	Role-Based Access Control. Управление доступом на основе ролей
REST API	Способ доступа к веб-сервисам без какой-либо обработки
SCTP	Stream Control Transmission Protocol. Протокол транспортного уровня в компьютерных сетях
SDN	Software-Defined Networking. Программно-определяемые сети
SFTP	Secure File Transfer Protocol. Протокол безопасной передачи файлов через сеть
SR-IOV	Single Root Input/Output Virtualization. Виртуализация ввода-вывода. Применяется для виртуализации ресурсов ввода-вывода для отдельных серверов
SSH	Secure Shell. Безопасная оболочка – сетевой протокол прикладного уровня. Позволяет удаленно управлять операционной системой и туннелировать TCP-соединения
SSL	Secure Sockets Layer. Протокол безопасности, который создает зашифрованное соединение между веб-сервером и веб-браузером
TCP	Transmission Control Protocol. Протокол управления передачей данных
TLS	Transport Layer Security. Криптографический протокол обеспечения безопасной передачи данных
UDP	User Datagram Protocol. Сетевой протокол транспортного уровня. Использует IP для передачи данных от одного устройства к другому. Данные (датаграммы), которые вносятся в пакет UDP, включают порты назначения, источник, контрольную сумму и длину пакета
URI	Uniform Resource Identifier. Унифицированный идентификатор ресурса
UUID	Универсально уникальный идентификатор. 128-битная метка, используемая для идентификации информации
vCPU	Virtual Central Processing Unit. Виртуализированный вариант физического CPU – центральные блоки управления в виртуальных машинах и облачных средах
VF	Virtual Function. Виртуальная функция
VIP	Virtual IP address. Виртуальный IP-адрес – компонент сетевой и интернет-инфраструктуры, который обеспечивает балансировку нагрузки, высокую доступность и эффективное распределение ресурсов в вычислительной среде. Это уникальная числовая метка, присвоенная виртуальной машине или службе, а не физическому устройству
VLAN	Virtual Local Area Network. Виртуальная локальная сеть
VNC	Virtual Network Computing. Метод удаленного доступа к рабочему столу компьютера по сети
vNIC	Virtual Network Interface Card. Виртуальный сетевой интерфейс, основанный на физических сетевых картах узла
VoIP	Voice over Internet Protocol. Технология передачи голосовых сообщений в локальных сетях или в сети Интернет с использованием протокола IP

Термин	Определение
VRRP	Virtual Router Redundancy Protocol. Сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, которые выполняют роль шлюза по умолчанию
VXLAN	Virtual Extensible LAN. Технология сетевой виртуализации для решения проблем масштабируемости в больших системах облачных вычислений
YAML	Yet Another Markup Language. Формат сериализации данных. Используется при управлении конфигурацией, а также для хранения данных в структурированном формате
ОЗУ	Оперативная память
ОС	Операционная система
ПО	Программное обеспечение
ЦПУ	Центральный процессор