Skillbox

API Gateway

Андрей Гордиенков

Solution Architect

ABAX

Skillbox

Специфика API Gateway

Андрей Гордиенков

Solution Architect

ABAX

В прошлом модуле

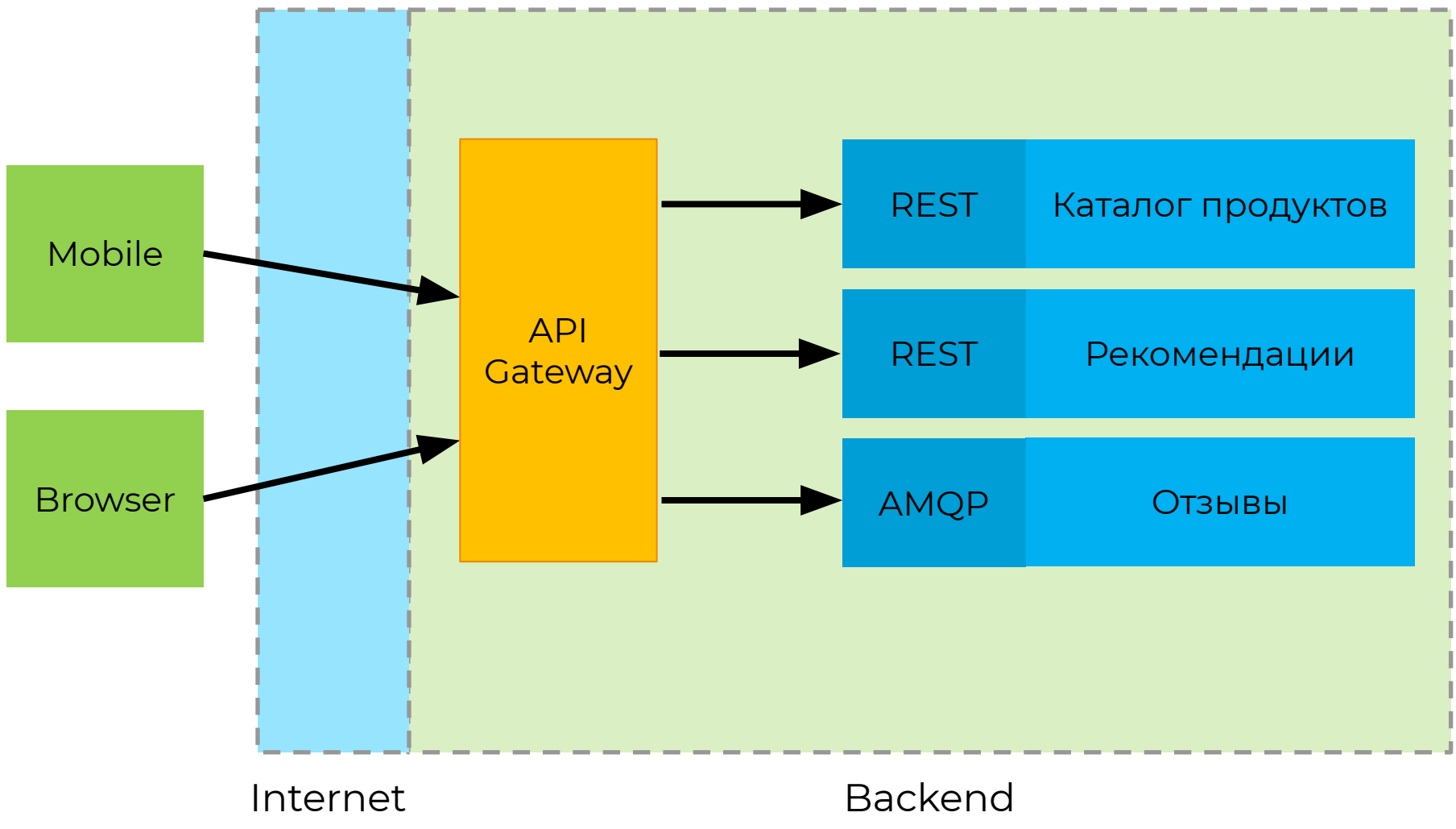
- Шаблон API Gateway
- Представители на рынке

В этом модуле узнаем

Функциональные части API Gateway.

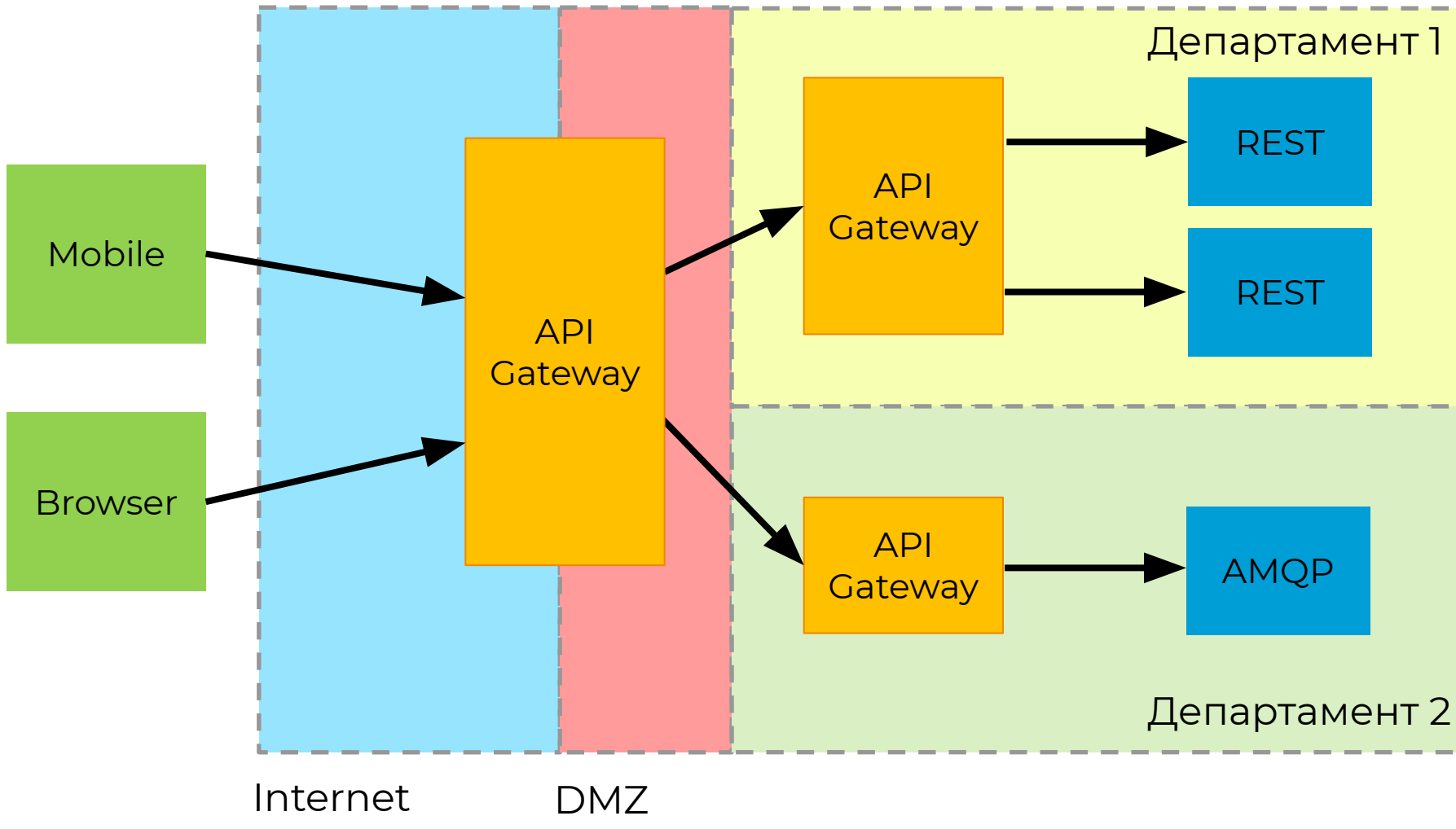
API Gateway

Средний и малый бизнес

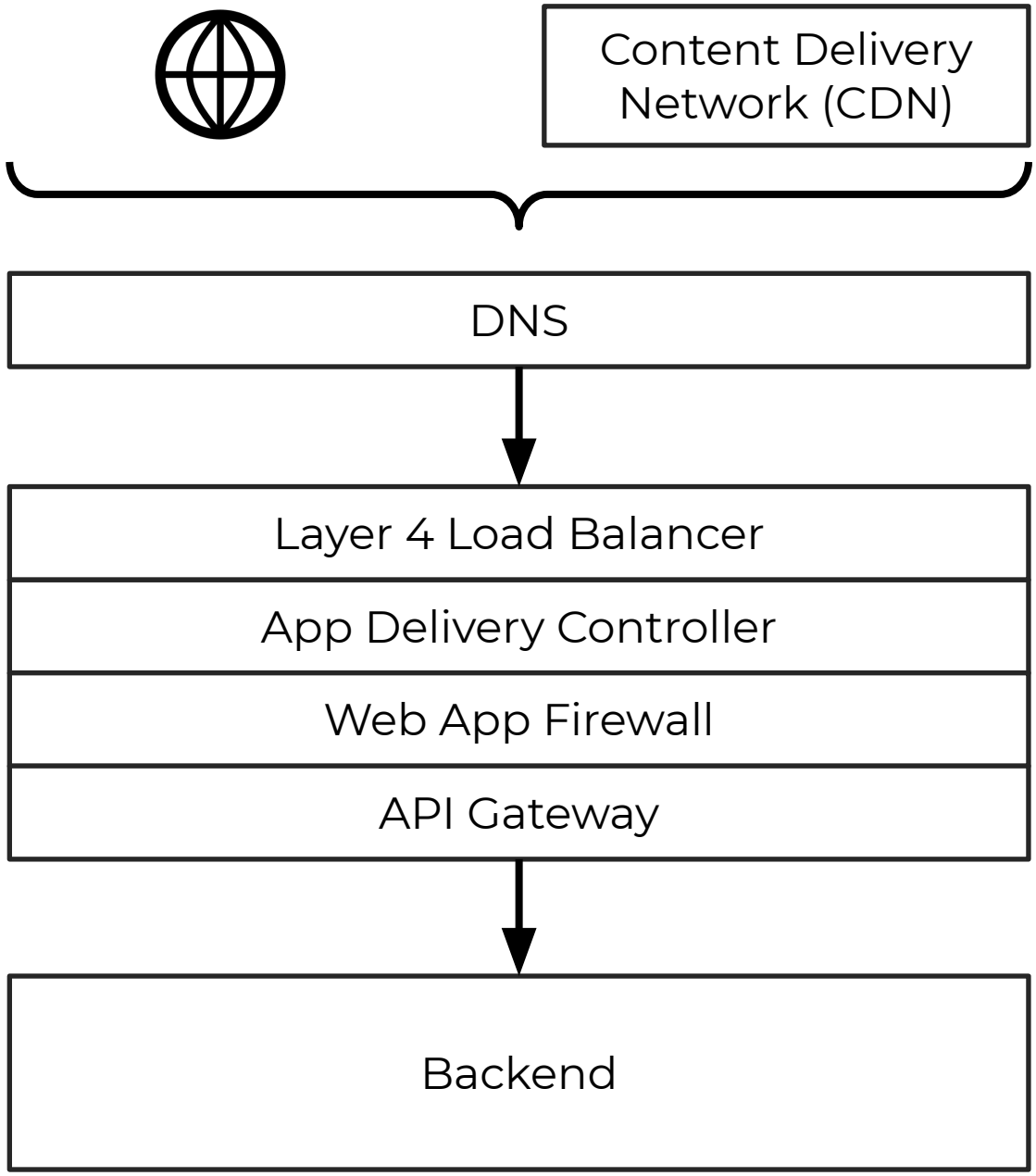


API Gateway

Крупный бизнес



Edge Stack


Content Delivery Network (CDN)
DNS
Layer 4 Load Balancer
App Delivery Controller
Web App Firewall
API Gateway
Backend
Внешние поставщики услуг
Edge Stack
Приложения и сервисы

Функциональность

- **Слабая связанность:** адаптер / фасад между фронтендом и бэкендом
- **Простота:** агрегирование / трансляция сообщений сервисов бэкэнда
- **Защита API:** обнаружение и устранение угроз
- **Утилизация API:** наблюдаемость
- **Управление API:** управление жизненным циклом
- **Монетизация API:** управление счетами, выставление счетов и оплата

Векторы атак

Основные классы опасности в зоне ответственности API Gateway:

- **Spoofing** — представление другим пользователем
- **Tampering** — изменение данных, сообщений или настроек, к которым нет доступа
- **Repudiation** — отрицание действия
- **Information disclosure** — раскрытие приватной информации
- **Denial of service** — предотвращение доступа к данным и сервисам другим пользователям
- **Elevation of privilege** — получение доступа к функциональности, к которой нет доступа

STRIDE — общее название типовых векторов атак.
Не забываем про OWASP топ-10.

Skillbox

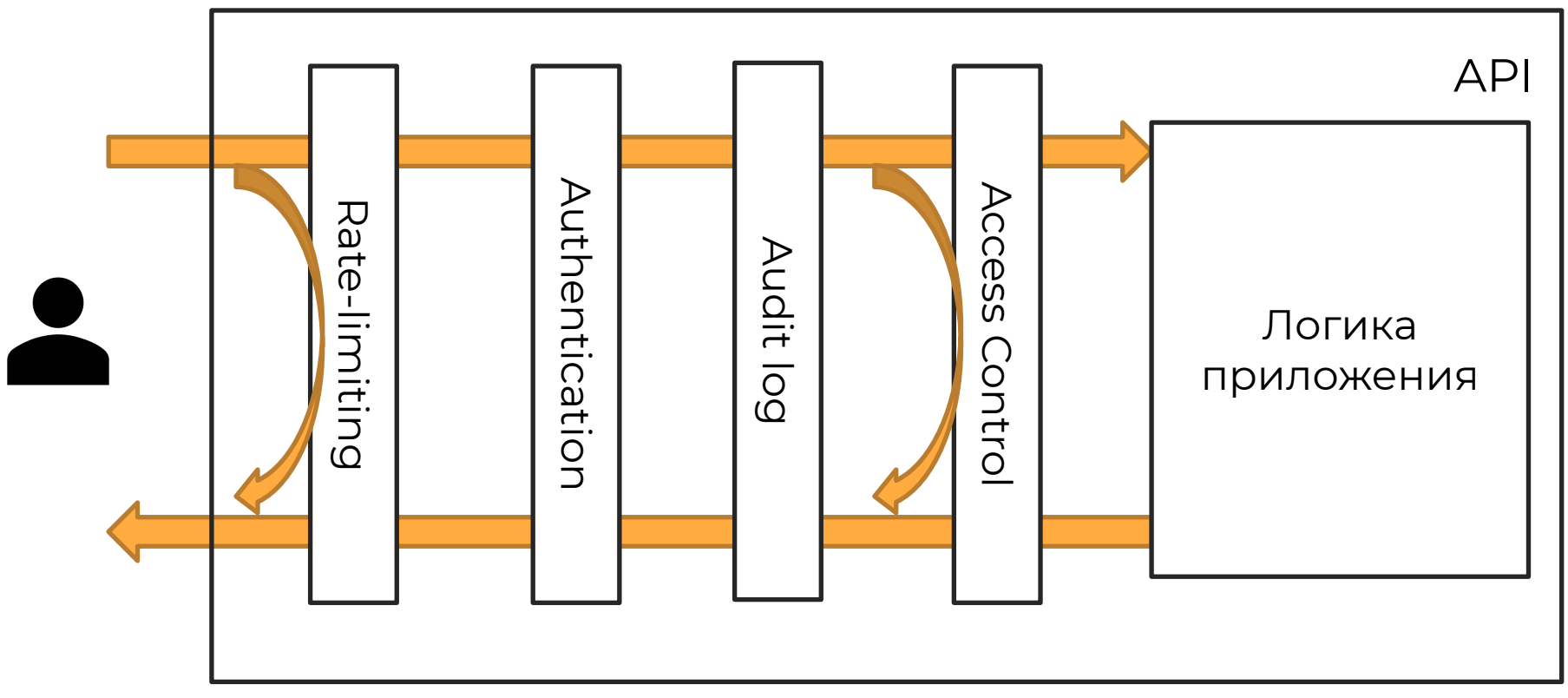
Защита API

- Шифрование
- Авторизация
- Контроль доступа
- Аудит
- Ограничение пропускной способности

Skillbox

Защита API

Расположение слоёв защиты



Rate limiting

- Защита от DoS-атак
- Честное использование услуг
- Способ монетизации

Ключевой фактор — работа компонента должна в теории потреблять меньше ресурсов, чем тратит пользователь.

Квоты устанавливаются для каждого типа ресурсов или услуг.

Throttling реализуется с помощью очереди или кодов ответа, чтобы клиент притормозил, а иначе отказ принятия запросов.

Skillbox

Авторизация

Аутентификация и авторизация — способы сохранить приватность и целостность информационных активов.

Архитектура системы может физически не позволить читать сообщения других пользователей.

Role-based access control (RBAC) — доступ на основе роли.

Attribute-based access control (ABAC) — доступ на основе атрибутов.

Skillbox

Аутентификация

Каждый фактор аутентификации может быть скомпрометирован:

- слабые пароли
- социальный инжиниринг
- ненадёжность биометрии

Для хорошей защиты требуется 2 и более факторов аутентификации:

- пароль
- секретный меняющийся код
- подтверждение, если новое устройство или новая локация пользователя

При этом 2 пароля к одному аккаунту — это всё ещё один фактор.

Skillbox

Аудит

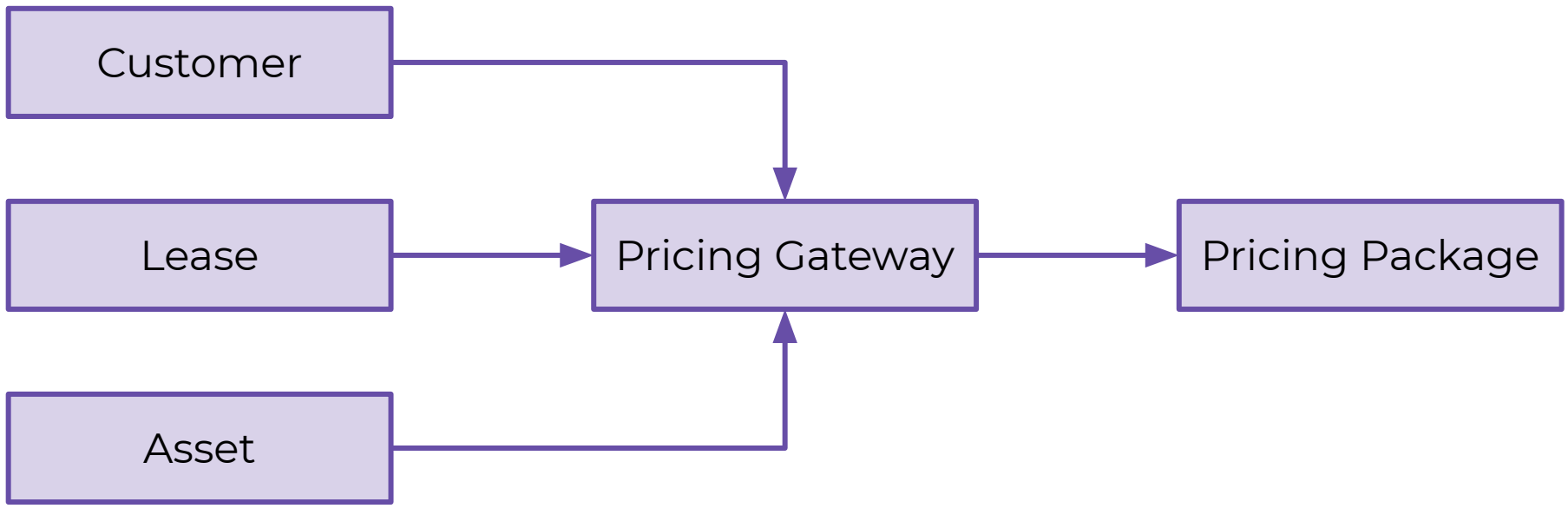
Audit Logging — детальное логирование действий пользователя для дальнейшего анализа и принятия решений.

Хороший аудит позволяет ответить на вопросы:

- кто выполнил действие и какой клиент был использован?
- когда был получен запрос?
- какого рода был запрос, например, операция чтения или изменения?
- к какому ресурсу осуществлялся доступ?
- был ли запрос успешным? Если нет, то почему?
- какие ещё запросы были сделаны примерно в то же время?

Агрегация данных

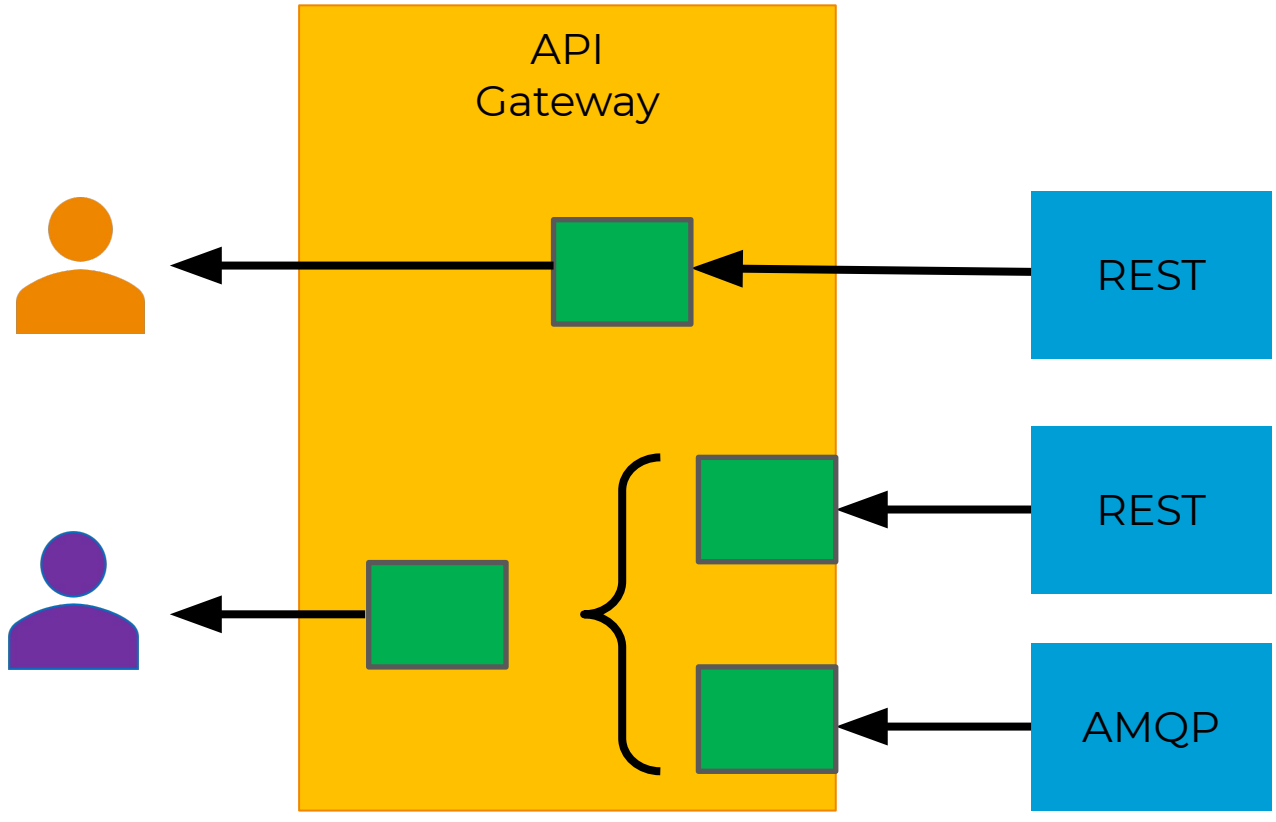
Необходимое гранулирование данных для клиента



Skillbox

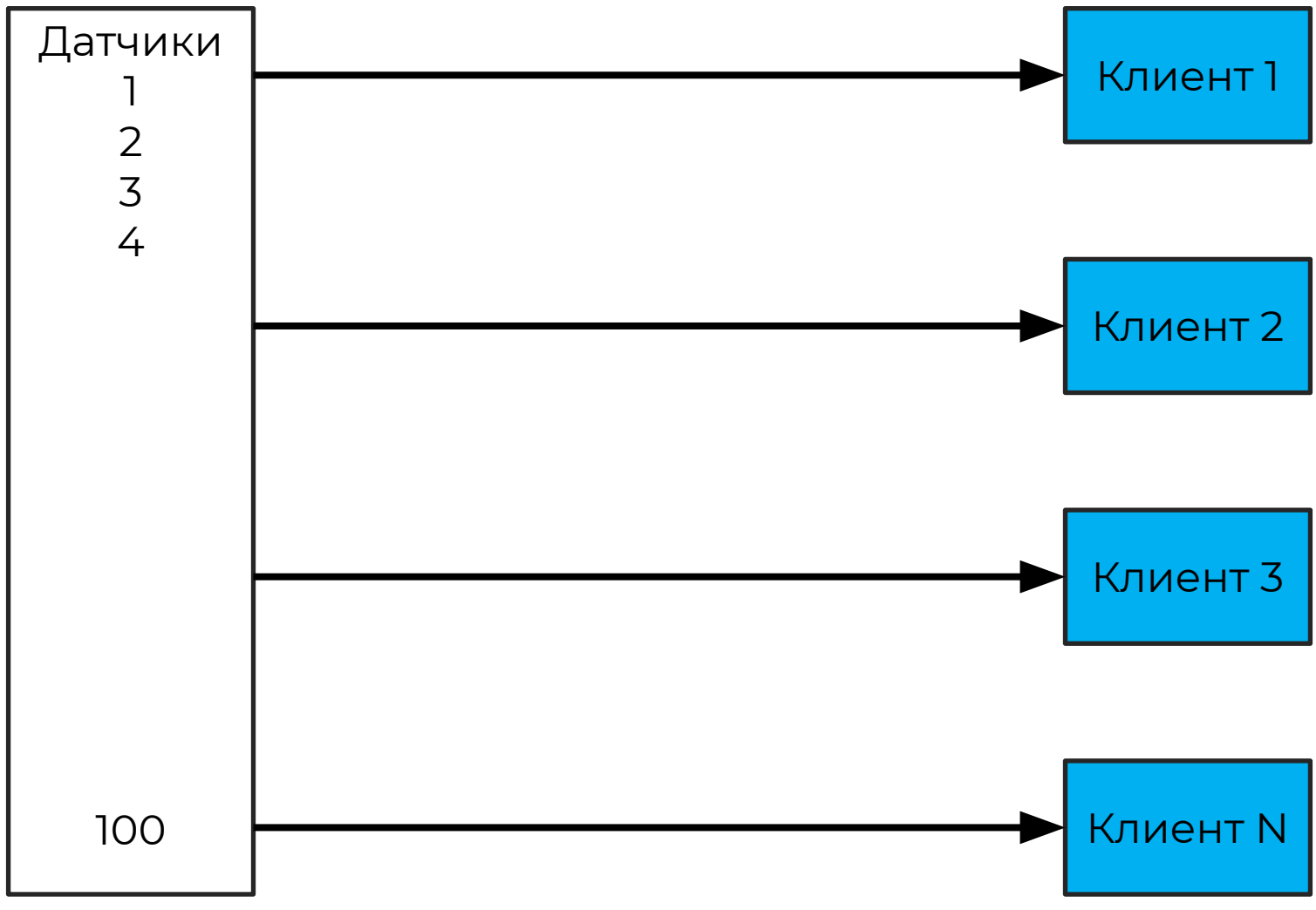
Агрегация данных

Трансформация и объединение ответов внутренних сервисов для пользователя.



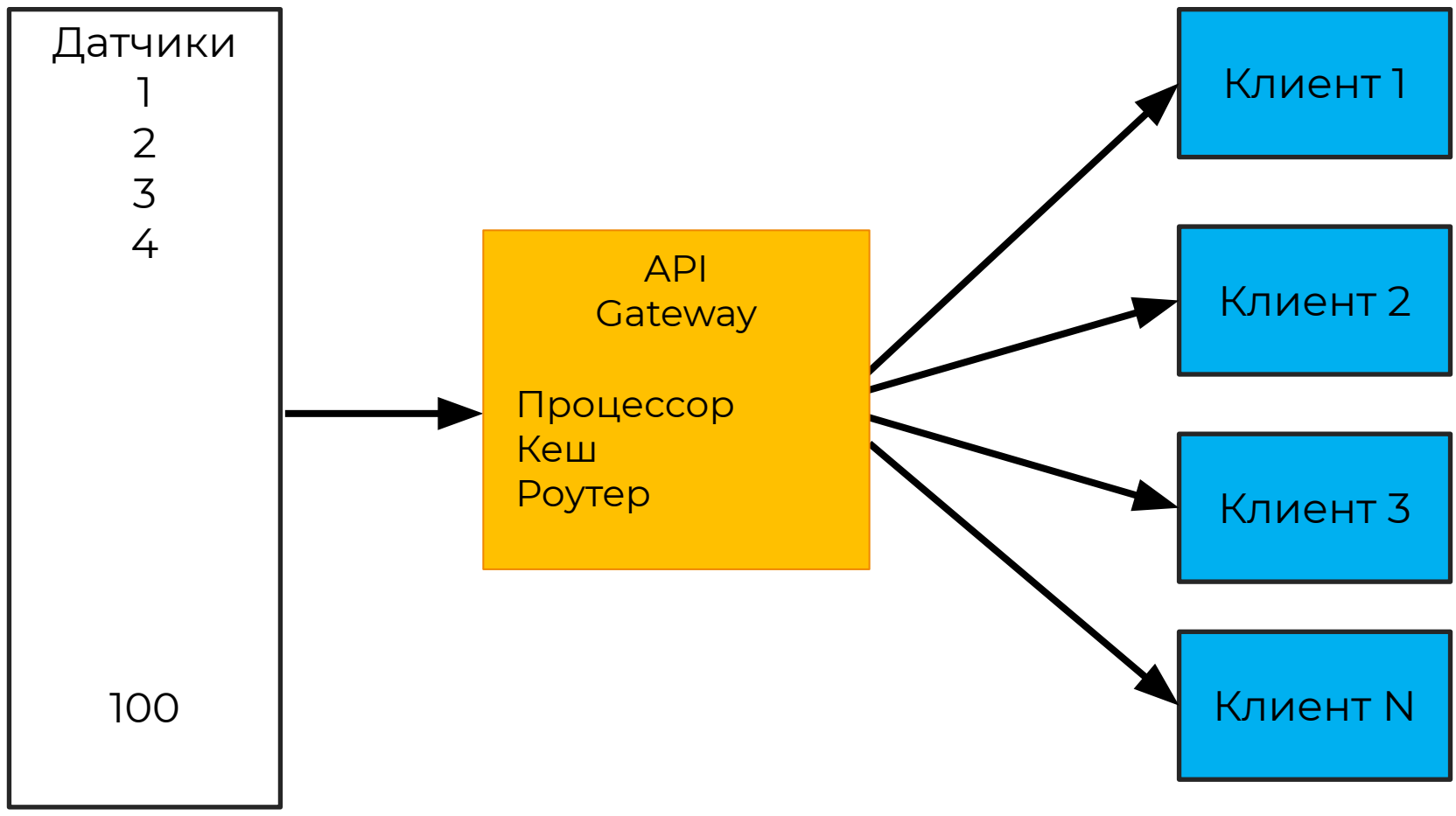
Агрегация данных

Рассылать все данные всем — дорого во всех смыслах.

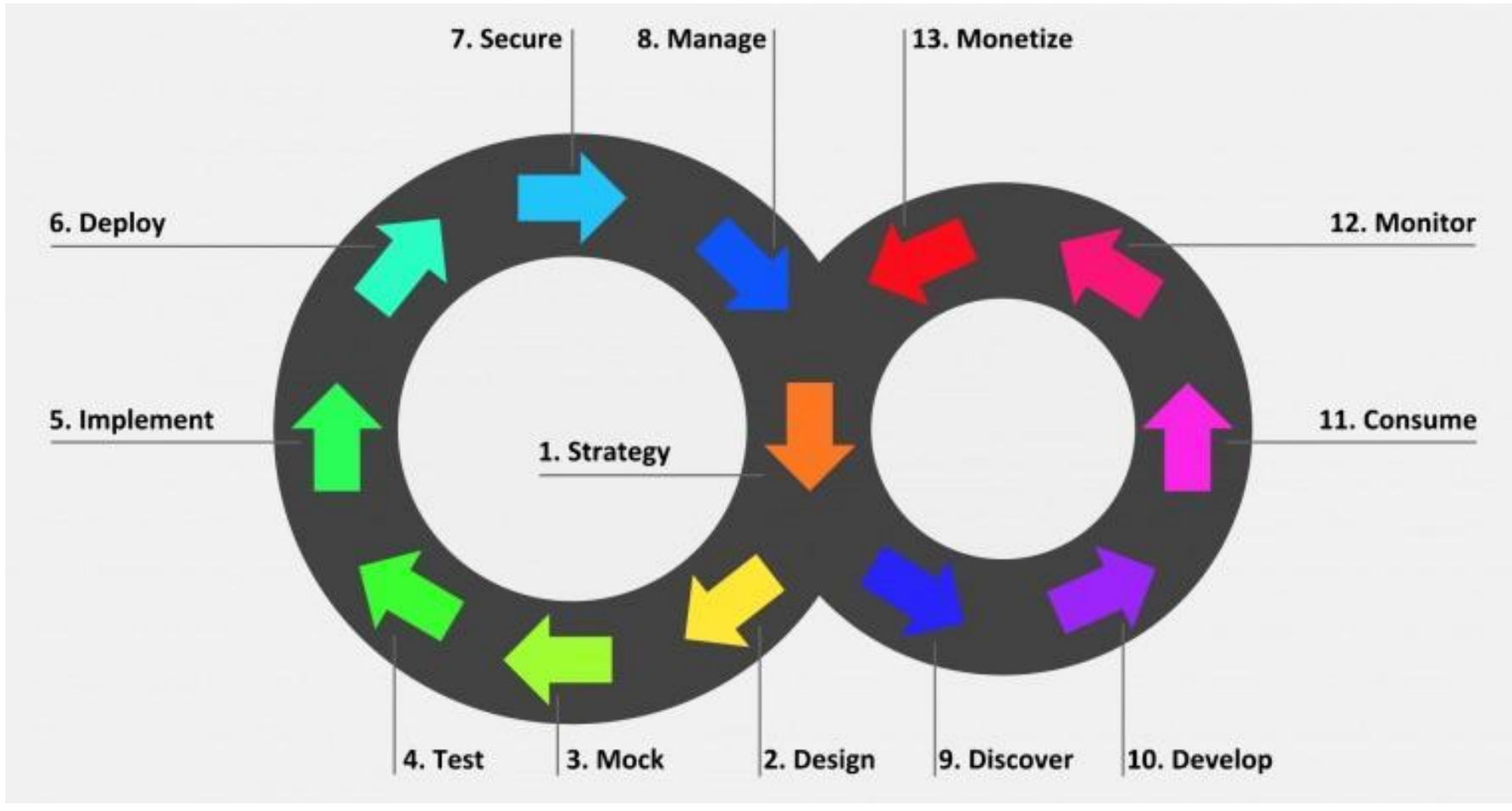


Агрегация данных

Не допускайте проникновения бизнес-логики в API Gateway.



Управление API

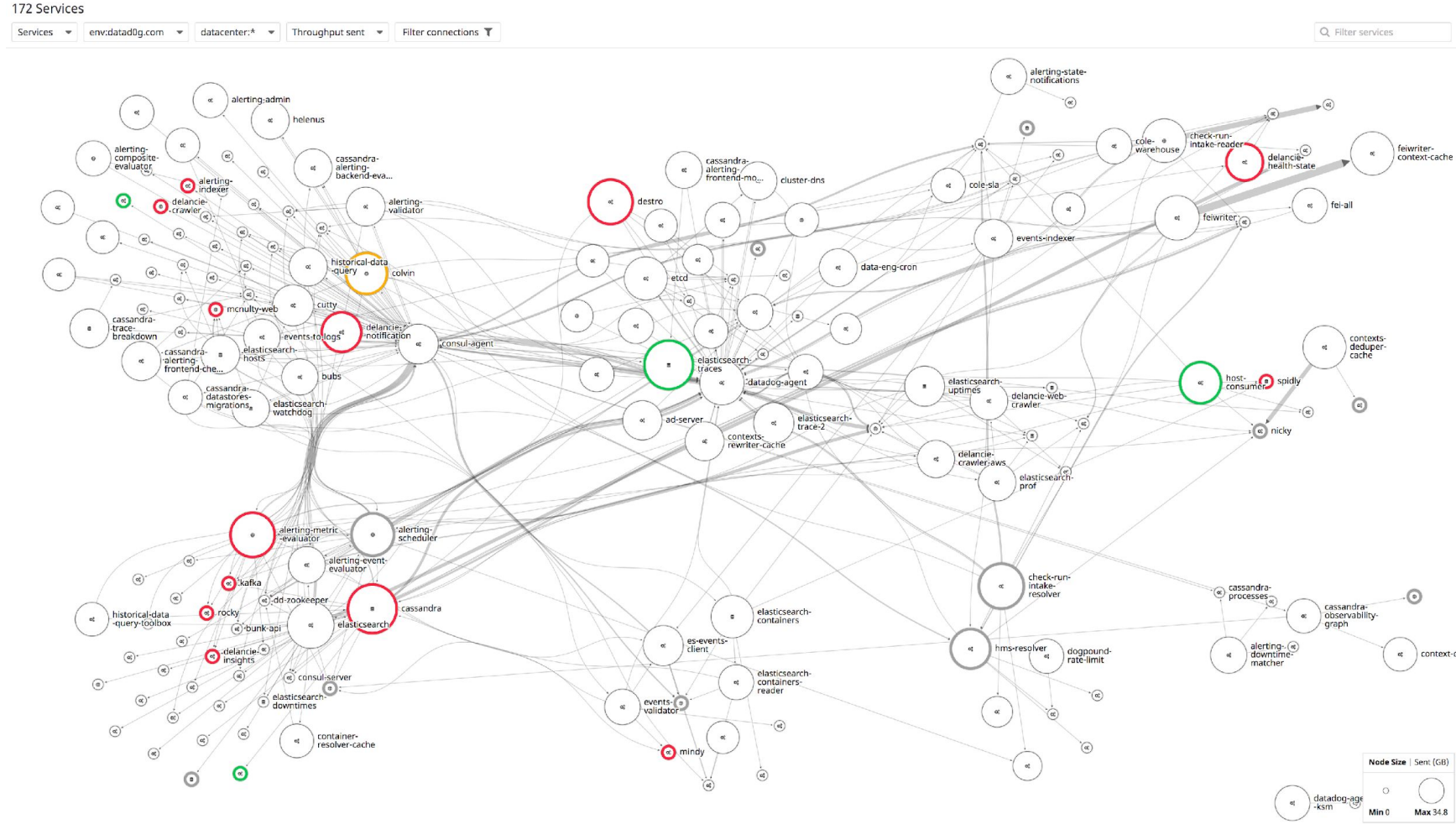


Подход 3Scale и RedHat к жизненному циклу API

Skillbox

Управление и утилизация API

Специализированные сервисы могут помочь, но...



Skillbox

Управление и утилизация API

Портал разработчика

- Доступ
- Лимиты
- Документация
- Тестирование

Понимание использования API

- Бизнес-цели и KPI
- SLI — Service Level Indicators
- Технические метрики

Следует внимательно отнестись к процессу сбора метрик, анализу и интерпретации результатов. Только комплексный анализ даст правильную картину.

Выводы

- API Gateway — сложный симбиоз технических решений для целого спектра задач от бизнес-ориентированных до технических
- Необходима работа разных команд/специалистов для построения полновесного API Gateway
- Всё сразу реализовывать не стоит

Что дальше?

- Типы API Gateway
- Как выбрать подходящий продукт
- Антипаттерны

Skillbox

Спасибо за внимание!