NGENIX

Спокойствие как сервис,
и как в этом участвует DNS

Константин Чумаченко, CEO

TLDCON, Jūrmala, 12-13 сентября 2018 https://tldcon.ru

Веб и облака для веба

NGENIX

Управлять серверами и ПО сегодня – удел избранных. Большинство необходимых функций для работы веб-сайтов и веб-приложений доступно из облака.

CDN – древнейшая облачная технология после **DNS**, со многими взаимозависимостями.

Как шла их совместная эволюция?

Как менялся контент (и CDN)

NGENIX

Первое поколение (...-2005)

Файлы, изображения, Flash и прочие статические rich media.

Второе поколение (2005-2015)

+ потоковое видео и динамические веб-приложения.

Третье поколение (2015 – ...)

+ безопасность.

1-е поколение (до 2005)

NGENIX

Файлы, изображения, Flash и прочие статические rich media.

Типовые боли и страхи:

«У нас всплеск посещаемости, сайт упал!»

«Картинки долго грузятся!»

Балансировка

NGENIX

Как выбрать из 10K+ серверов CDN оптимальный для ответа пользователю, если:

- Дистанция в интернете ≠ географии (геобазы IP-адресов не работают).
- Пользователь и сервера CDN находятся в разных сетях и ничего не знают друг о друге до момента обращения пользователя к сайту.
- Нельзя направлять запрос к серверу, который не может ответить.
- Система балансировки должна управлять нагрузкой на сеть и сервера CDN.
- Система балансировки должна сама масштабироваться с ростом нагрузки.

DNS-балансировка

NGENIX

CNAME foo.example.com TTL example.cdn.ngenix.net

Пользователь | **Рек. DNS-резолвер** | **Авт. DNS-сервер зоны example.com** | **Авт. DNS-сервер зоны ngenix.net** | **Серверы облака**

A.B.C.1 A.B.C.2 A.B.C.N

Где foo.example.com?

Где foo.example.com?

example.cdn.ngenix.net

Где example.cdn.ngenix.net?

A.B.C.1

A.B.C.1

2-е поколение (2005-2015)

NGENIX

+ потоковое видео (OTT).
+ динамические веб-приложения (E-Com).

Типовые боли и страхи:

«А правда, что +1 сек. latency = -7% конверсии?»

«Как насчет стриминга в формате $&%@ на мобильные устройства?»

«Что делать с пиковым OTT-трафиком?»

А что DNS?

NGENIX

Проблемы с DNS-балансировкой:

- Низкая точность. IP резолвера ≠ IP пользователя. Многие пользователи используют DNS-резолверы Google, Yandex и пр.
- Недостаточная избирательность. (До домена, без учета типа контента, нет механизма перебалансировки).
- Сложности с инвалидацией DNS-кэшей в резолверах и браузерах.

EDNS Client-Subnet

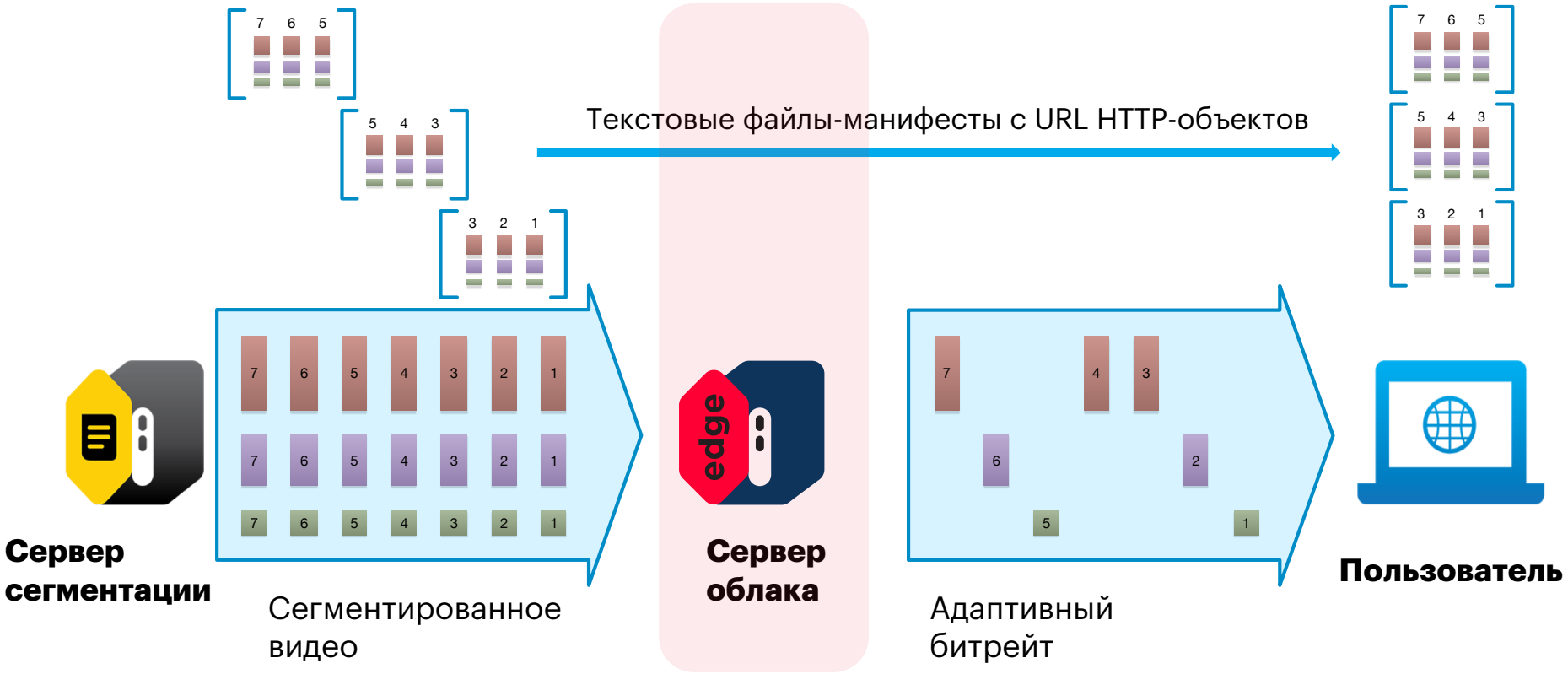
NGENIX

EDNS0 (RFC 7871) позволяет резолверу сообщить авт. DNS-серверу сеть источника запроса (т.е. пользователя) в OPT record.

- Улучшает таргетирование для 7-10% пользователей.
- Должно поддерживаться всей цепочкой DNS-резолверов (stub, caching).
- Privacy? What Privacy?

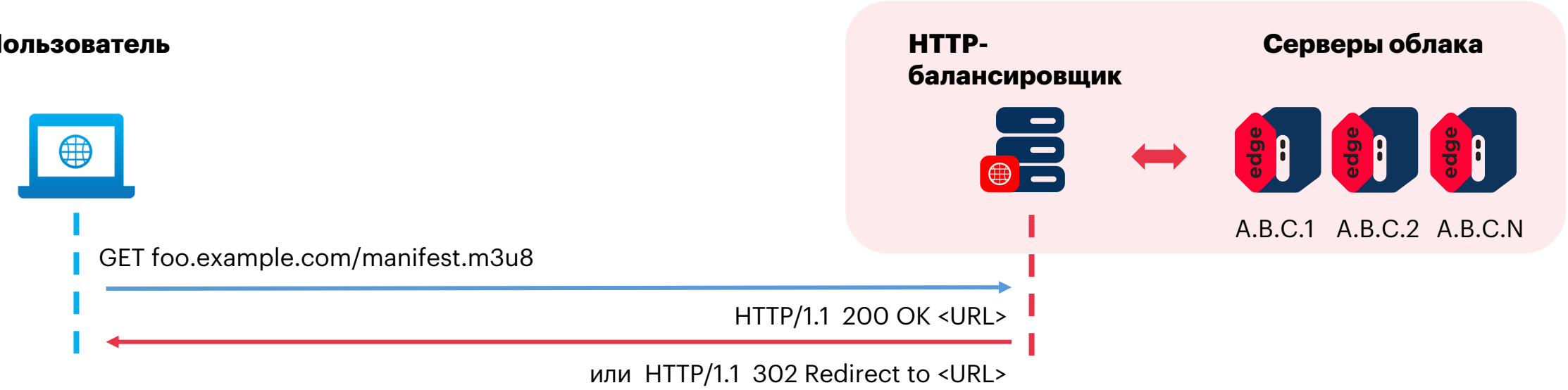
HTTP-стриминг

NGENIX



HTTP-балансировка

NGENIX



DNS используется до и после HTTP (балансировка балансировщиков)

3-е поколение (2015-...)

NGENIX

Те же + **безопасность.**

Типовые боли и страхи:

«Меня взломали?»

«Кто из вас не бот?!»

«Я под атакой!!!»

Повестка

NGENIX

Авт. DNS-серверам в облаке тоже нужна защита.

- DDoS на уровнях L3 и L7 ← Dyn / Mirai
- Перехват запросов (BGP hijacking, port 53 и пр.) ← AWS / MyEtherWallet.
- Нарушение приватности (pervasive monitoring и пр.) ← RFC7627. S.Bortzmeyer. DNS Privacy Considerations.

Что будет актуально?

NGENIX

Сегодня:

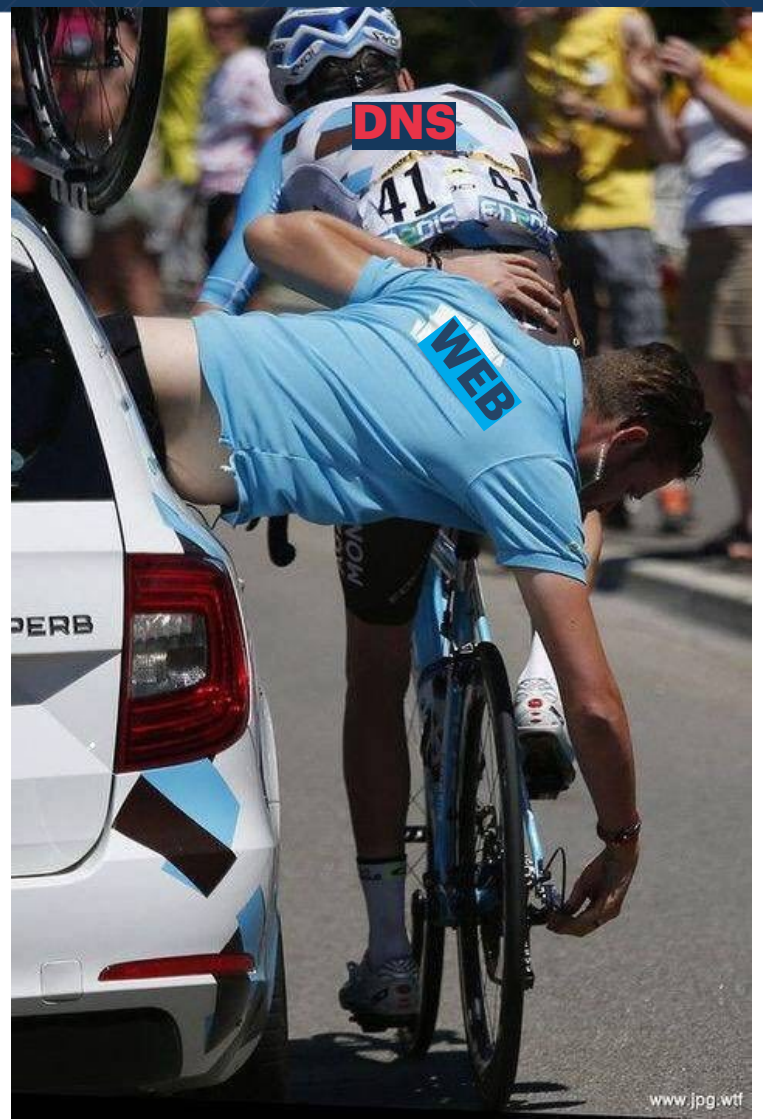
- Анализ и фильтрация входящего трафика (L3 и L7).
- Защита интерфейсов и API (HTTPS, REST security, 2FA и пр. гигиена).
- BGP security & best practices (фильтры).
- DNSSEC для валидации данных зон.

В перспективе:

- Разработки DPRIVE WG – в контексте обмена резолверов с авт. DNS-серверами:
  - DNS-over-TLS (RFC7858)
  - DoH (I-D.ietf-doh-dns-over-https)

Поможет ли веб DNS?

NGENIX



Спасибо. Вопросы?

NGENIX

Константин Чумаченко

k.chumachenko@ngenix.net