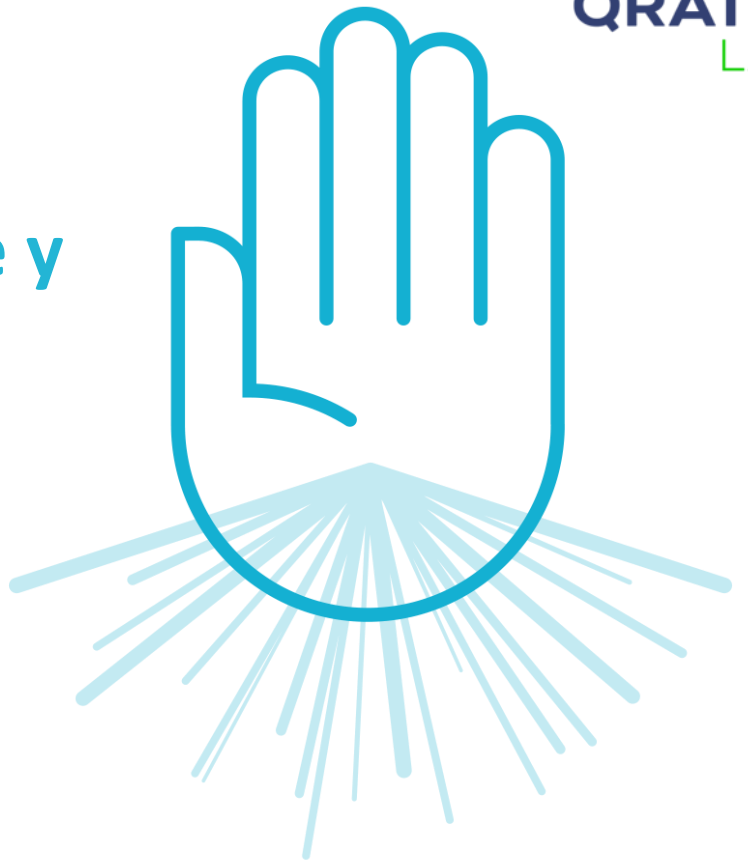
QRATOR LABS

Шифрование на службе у злодеев: DDoS-атаки на TLS-сервисы



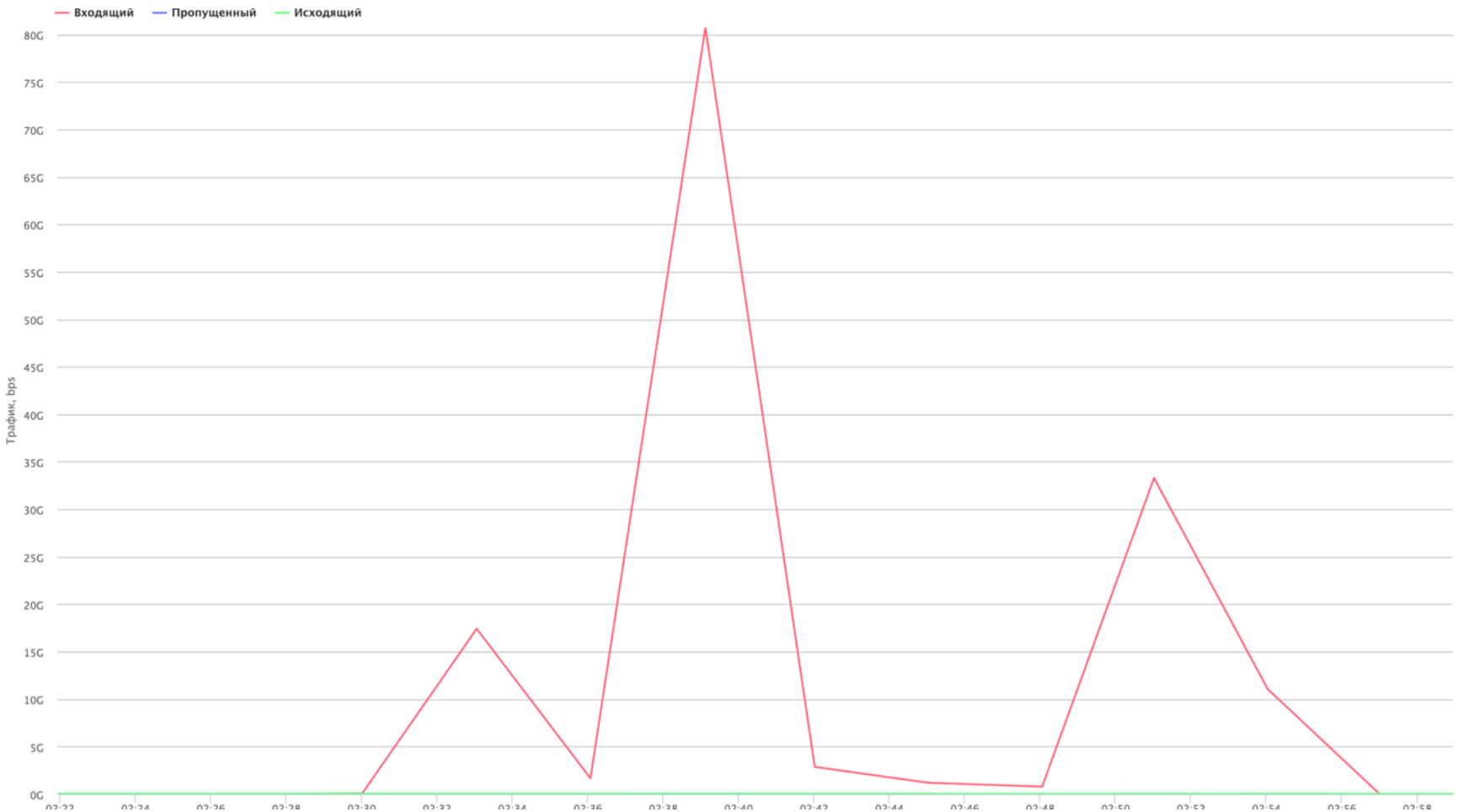
Максим Белоенко
Qrator Labs

Типы атак

QRATORLABS

- **L2** - «Забивание» канала: ICMP Flood, * Amp…
- **L3** - Нарушение функционирования сетевой инфраструктуры
- **L4** - Эксплуатация слабых мест TCP-драйвера
- **…**
- **L7** - Деградация Web-приложения

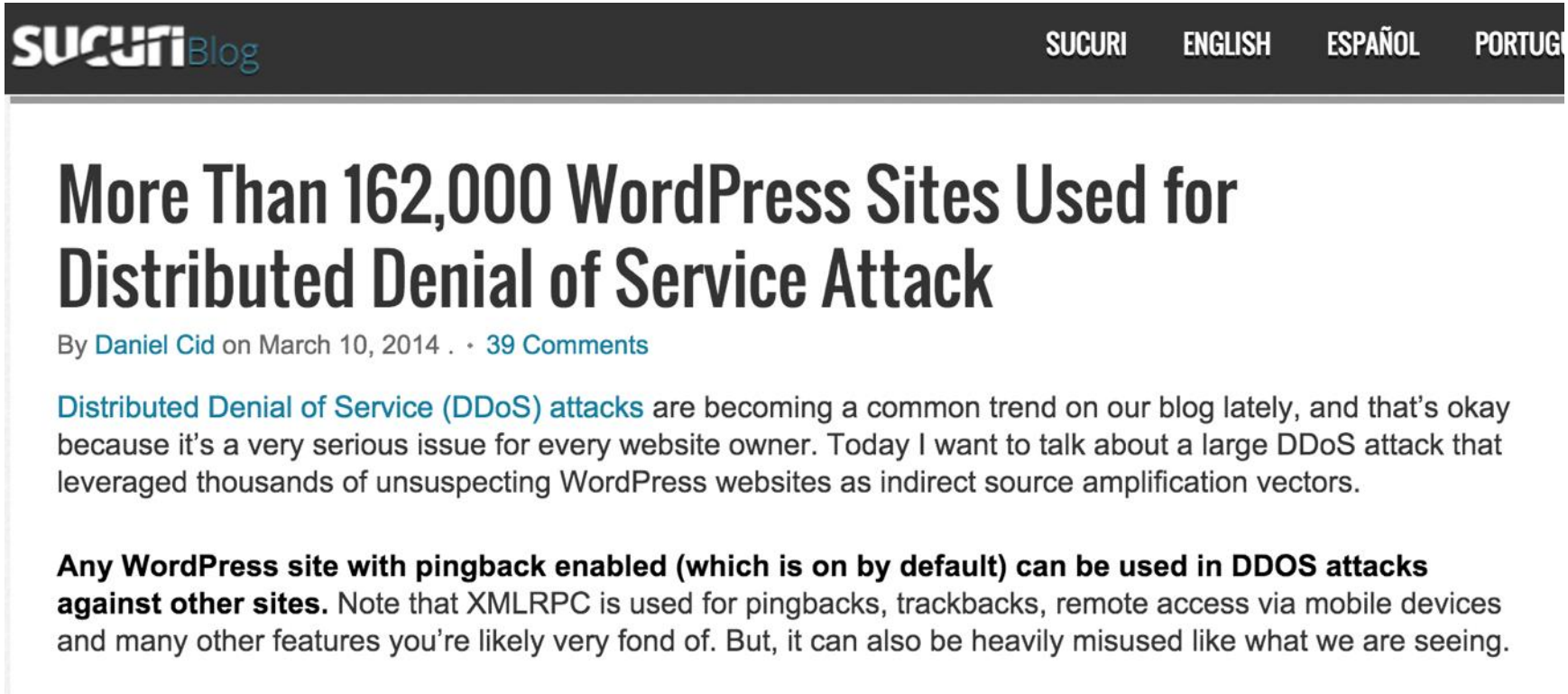
Атаки на канал



Прикладные атаки

QRATORLABS

- **L7** -атака типа WordPress Pingback
- 7 Gbps от 3500 ботов.



SUCURI Blog SUCURI ENGLISH ESPAÑOL PORTUG

More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack

By Daniel Cid on March 10, 2014 . • 39 Comments

Distributed Denial of Service (DDoS) attacks are becoming a common trend on our blog lately, and that's okay because it's a very serious issue for every website owner. Today I want to talk about a large DDoS attack that leveraged thousands of unsuspecting WordPress websites as indirect source amplification vectors.

Any WordPress site with pingback enabled (which is on by default) can be used in DDOS attacks against other sites. Note that XMLRPC is used for pingbacks, trackbacks, remote access via mobile devices and many other features you're likely very fond of. But, it can also be heavily misused like what we are seeing.

QRATORLABS

Чтобы защититься в 2016 году:

Аренда каналов (от 100 гбит/с)

или

Использование «облачного» решения

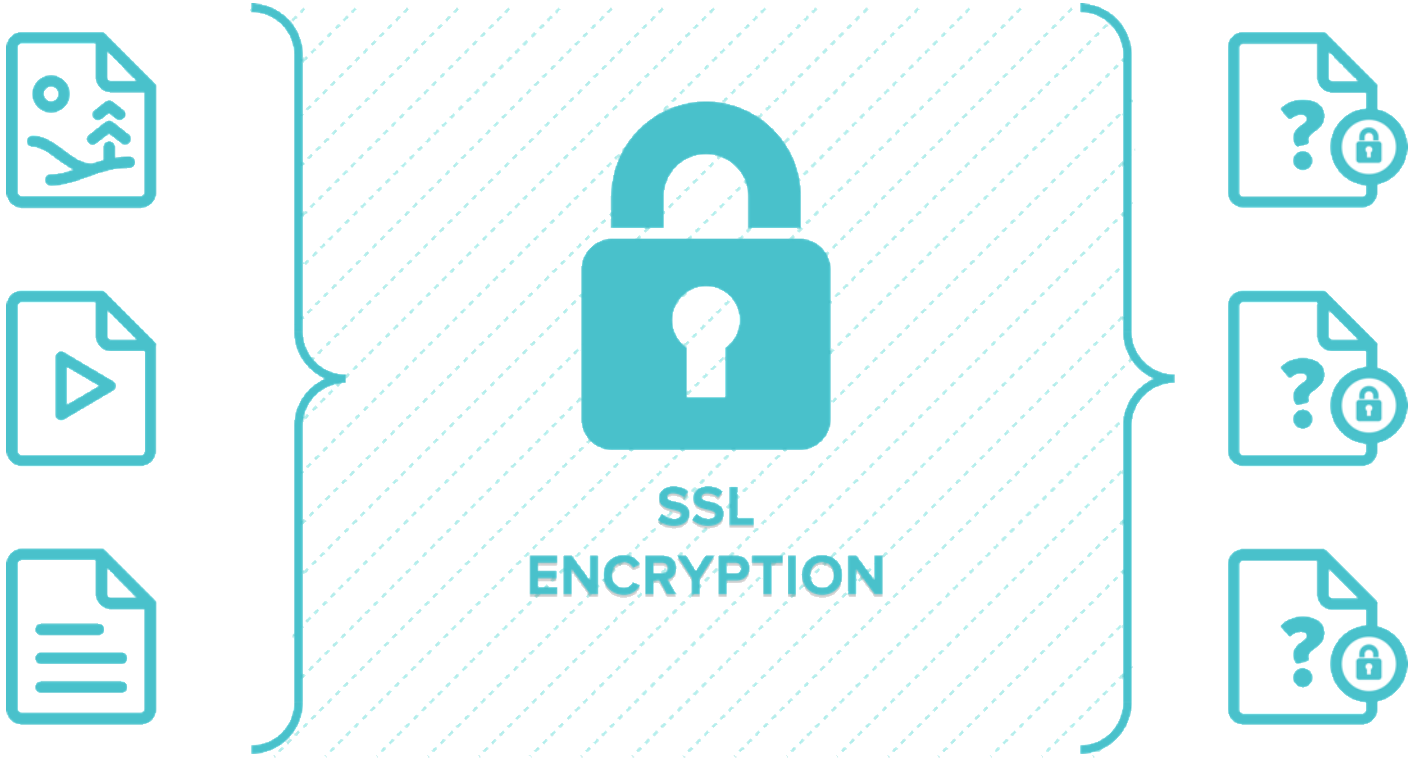
Типы атак

QRATORLABS

- **L2** - «Забивание» канала: ICMP Flood, * Amp…
- **L3** - Нарушение функционирования сетевой инфраструктуры
- **L4** - Эксплуатация слабых мест TCP-драйвера
- **L5, L6 -** SSL/TLS
- **L7** - Деградация Web-приложения

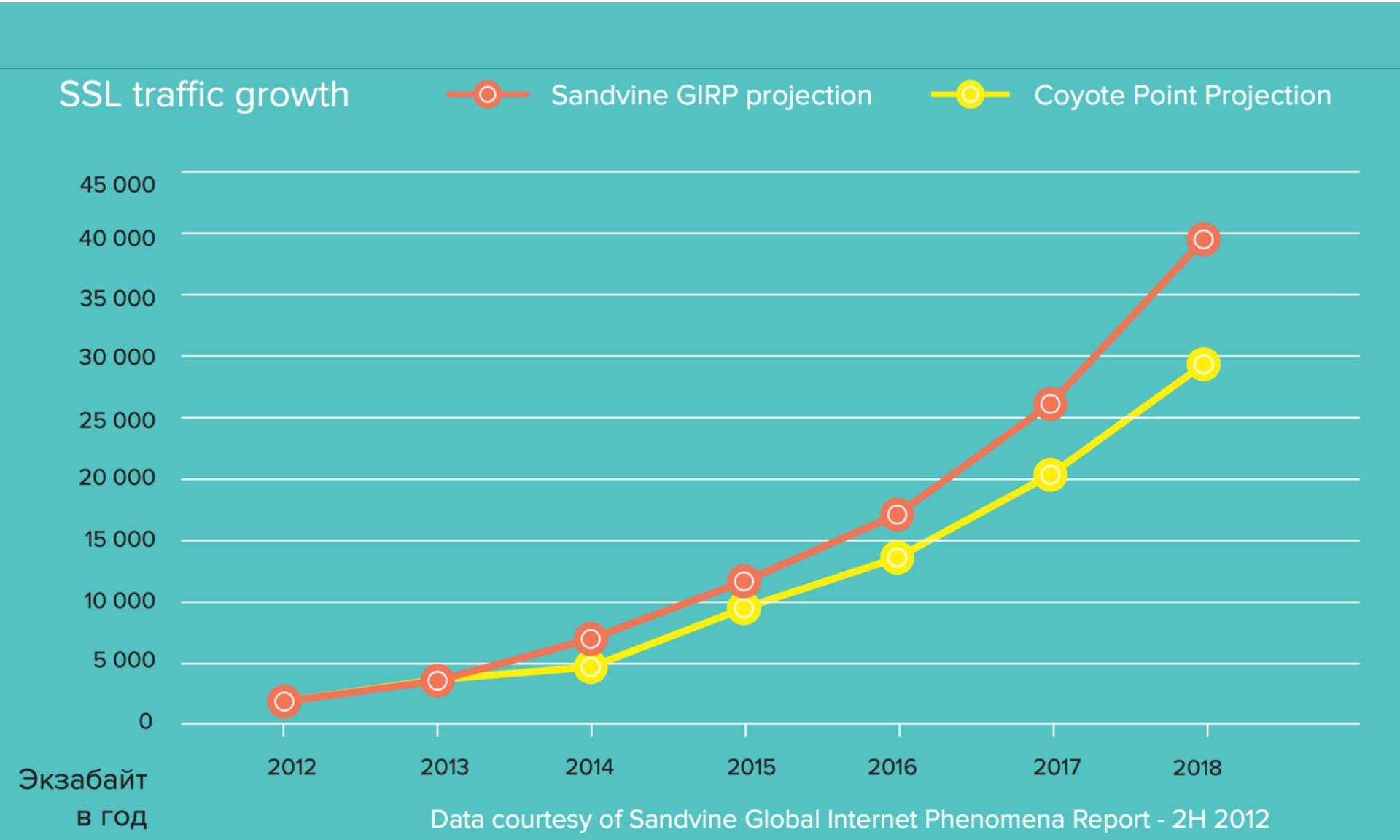
Защита SSL: трудности

QRATORLABS



SSL-трафик в мире

QRATORLABS



QRATORLABS

Что делать?

Что делать?

QRATORLABS

Раскрытие
RSA ключей
шифрования

Раскрытие
Сессионных ключей
(Keyless SSL)

Трансляция логов
(без раскрытия ключей)

Защита с раскрытием RSA ключей

QRATORLABS

- ➕ простота реализации

- ➖ требования аудита безопасности
- ➖ требования регуляторов
- ➖ защита перс. данных.
- ➖ невозможность анализа mirrored-трафика

Раскрытие сессионных ключей (Keyless ssl)

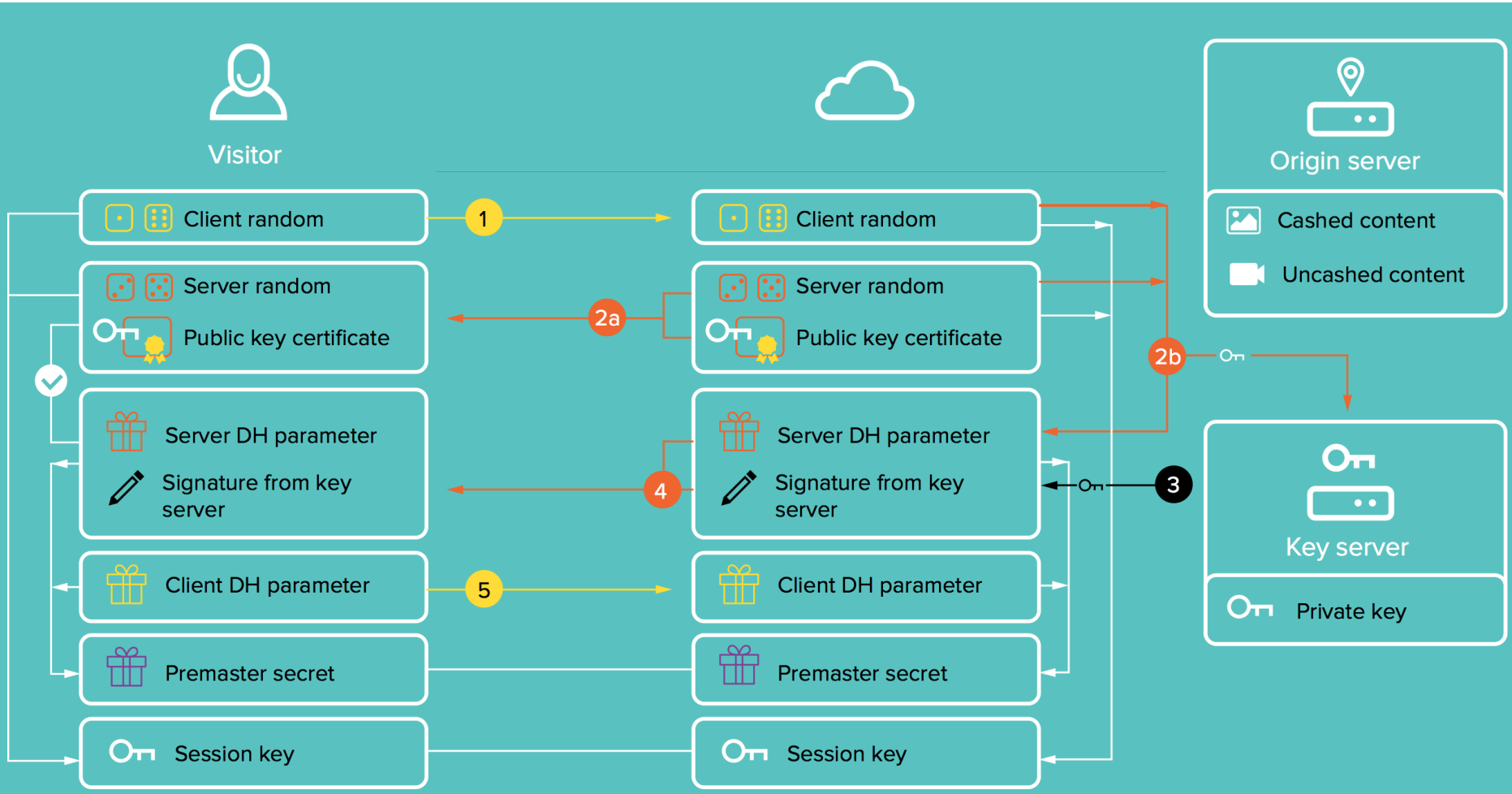
QRATORLABS

- ➕ Возможность анализа mirrored трафика

- ➖ требования аудита безопасности
- ➖ требования регуляторов: серая зона
- ➖ защита перс. данных.
- ➖ **сложность реализации**

Раскрытие сессионных ключей (Keyless ssl)

QRATORLABS



Трансляция логов в realtime

QRATORLABS

- ➕ возможность анализа mirrored трафика
- ➕ требования аудита безопасности
- ➕ требования регуляторов
- ➕ защита перс. данных.

- ➖ сложно в настройке (требует установки специфического ПО)

Трансляция логов в realtime

QRATORLABS