Защита. Скорость. Контроль.

Бекнур Нурсултанов

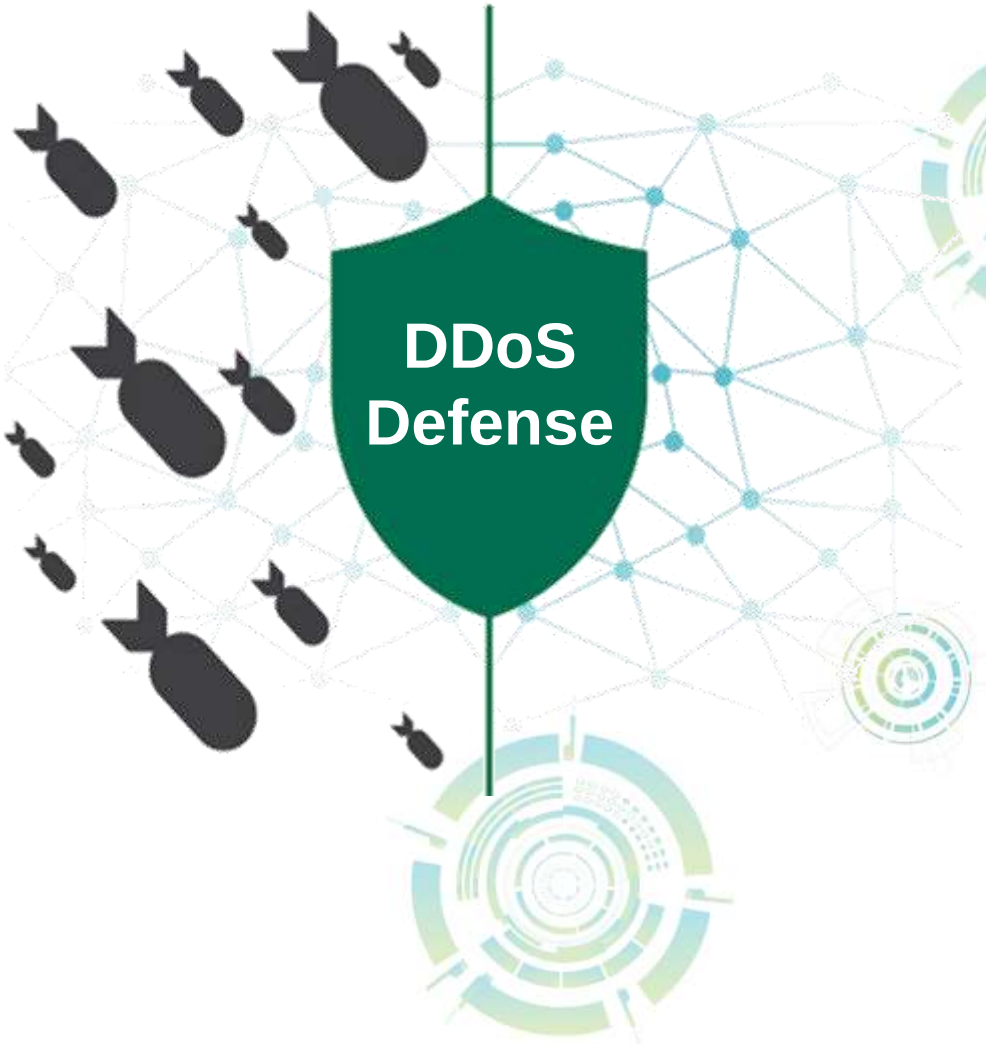
Начальник управления защиты ресурсов ЦОД

+7 778 666 99 08
NursultanovB@kazteleport.kz

Дмитрий Никонов

Руководитель направления защиты от DDoS на уровне веб-приложений

8 (499) 322-04-87
d.nikonov@ddos-guard.net



Halyk Kazteleport

25+

Лет на рынке

160+

Сертифицированных профессионалов с высоким уровнем компетенции

200+

Довольных клиентов

300+

Проверенных партнеров и вендоров

24/7/365

Мы всегда рядом!

Комплексные решения по кибербезопасности

Email Gateway

Основные возможности

- Многоуровневая защита от спама
- Антивирус
- Защита от фишинга
- Проверка аутентичности отправителя
- Интеграция с локальной песочницей Sandbox

WAF

Основные возможности

- Защита от веб-угроз OWASP TOP-10
- Производительность
- Rate-limiting и блокировка аномалий
- Защита API и микросервисов
- Поддержка CAPTCHA, JS-валидации и геофильтров

Next-Generation Firewall

Преимущества

- Отказоустойчивость (оборудование размещено в двух ЦОДах)
- Используется технология Virtual Domains – каждому клиенту предоставляется собственный изолированный виртуальный Firewall на базе аппаратного Fortigate

SOC/ОЦИБ

Преимущества

- Ежемесячные отчеты
- Доработка конфигурации
- Настройка правил корреляции
- Оповещение по почте и телеграм-канал

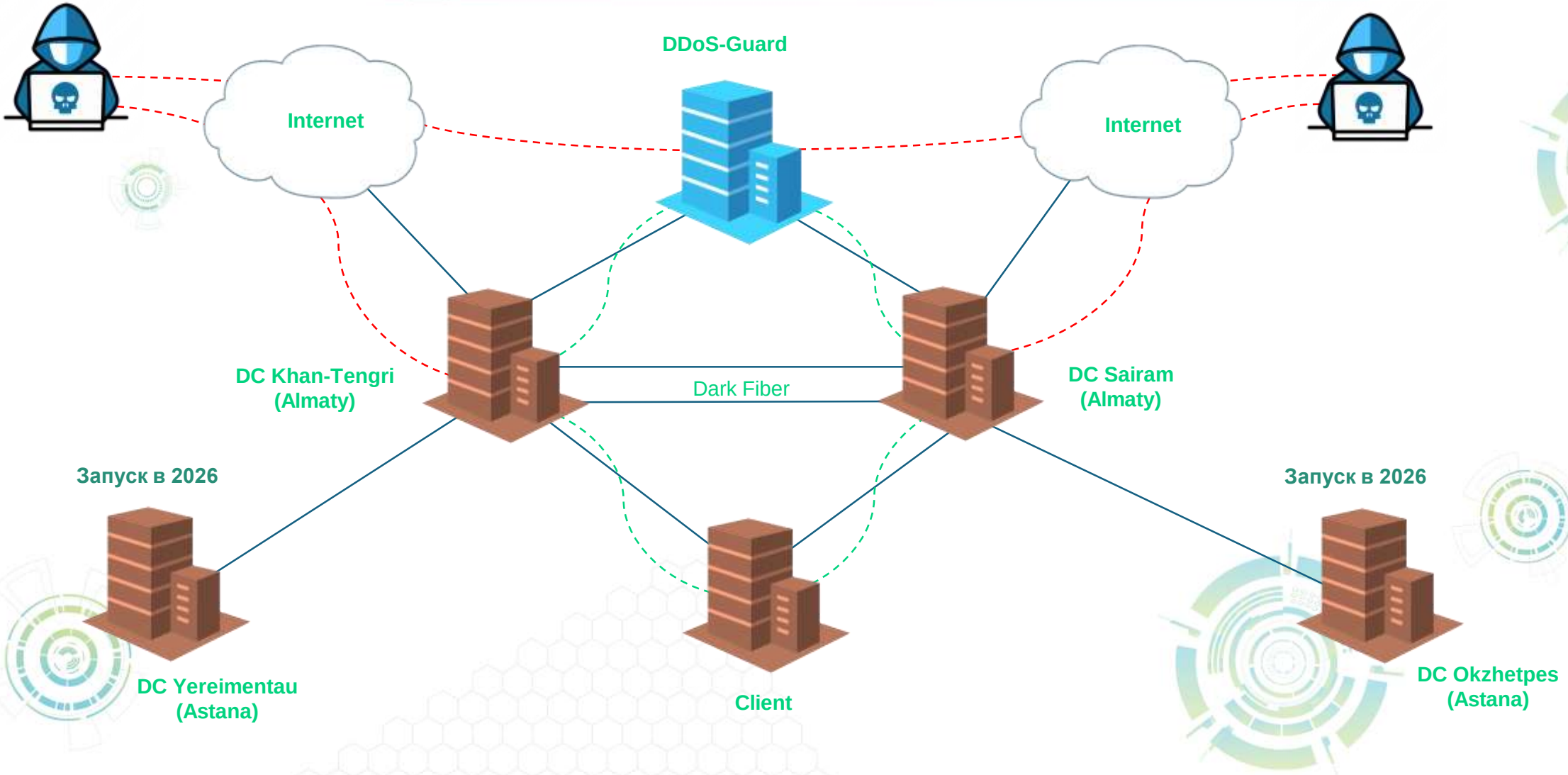
DDoS-Protection

Геораспределенная защита от DDoS-атак

Узлы фильтрации расположены в ключевых точках концентрации трафика. В текущее время активны точки, находящиеся в Нидерландах, России, Казахстане, Китае, а также в Северной и Латинской Америке.

Использование CDN позволяет значительно снизить время доставки трафика посетителям сайтов из различных регионов вне зависимости от физического расположения веб-сервера.

Локальный узел в Казахстане

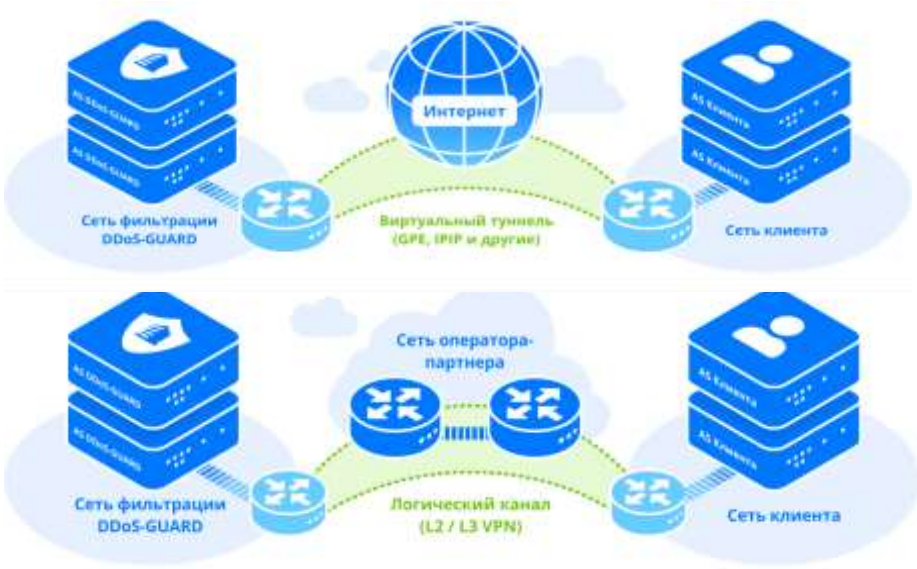


Защита сети

Предлагаем вам современные технологии по защите, оптимизации и доставке контента

Сеть DDoS-Guard работает как единая интеллектуальная система — фильтрующие узлы обмениваются данными, обеспечивая быструю и точную очистку трафика.

Надёжное подключение: собственная и партнёрская сеть с минимальными задержками



Уровень L3-4

- Фильтрация в постоянном режиме (Always On)
- Симметрия — фильтрация на основе анализа входящего и исходящего трафика защищаемых префиксов
- Асимметрия — фильтрация на основе анализа только входящего трафика защищаемых префиксов

Уровень L7

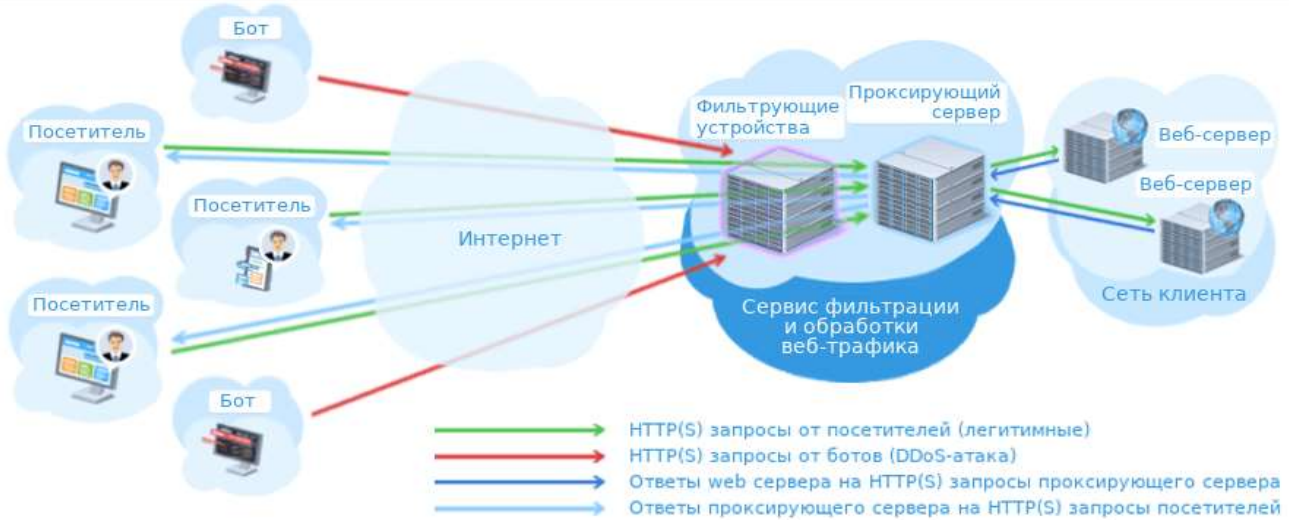
- Защита от всех HTTP(S) DDoS-атак (L7 OSI)
- Защита неограниченного количества веб-сайтов сети без смены А-записей
- Дашборд управления и мониторинга веб-трафика

Защита и ускорение сайтов

Оптимизируйте работу вашего сайта и обеспечьте его максимальную доступность

Как это работает?

- Очищаем входящий трафик от аномальных запросов на защищённом IP-адресе и передаём на конечный веб-сервер
- Включаем опцию кеширования и CDN, что снижает нагрузку на ваш сервер
- Благодаря этому, ваш сайт загружается быстрее и остаётся в безопасности от DDoS-атак



Преимущества защиты и ускорения

- Скрытие IP-адреса и расположения сервера
- Ускоренная доставка контента посетителям сайта
- Защита на основе ИИ на уровнях L3–L4, L7 OSI
- Балансировка запросов через распределение трафика между серверами
- Бесплатный DNS-хостинг с доступом к управлению
- Балансировка запросов через распределение трафика между серверами
- Оптимизация контента с помощью Gzip, Brotli и эвристической рекомпрессии
- Уникальные модули защиты и фильтрации

Кейс банка второго уровня: стабильная работа онлайн-банкинга при высокой нагрузке

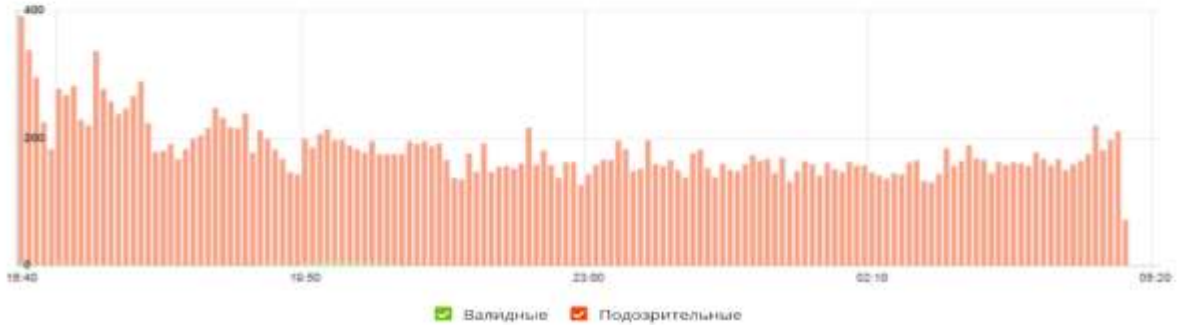
Halyk Kazteleport

ID атаки: 43244550-6af2-4578-8dc6-0ac858797331

12 часов 49 минут

1 291	8 096 971	50 338	4 568

Запросы во время атаки (RPS)



Страна	Запросы
Германия	4 143 052
Нидерланды	573 997
Великобритания	287 480
Польша	272 009
Канада	257 405
Австрия	206 034

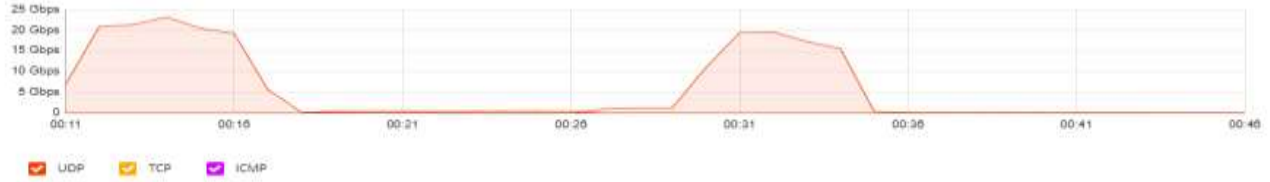
Страна	IP	Запросы
Испания	2.138.41.173	54 107
Бразилия	186.249.182.178	50 287
Германия	91.184.248.29	49 525
США	20.80.234.218	48 535
Финляндия	65.109.176.102	47 829
Турция	31.210.50.6	45 912
Индия	103.99.37.223	44 989
ОАЭ	80.227.63.66	44 736
Иран	37.202.237.251	43 877
Иран	95.215.59.249	43 578

Тип вредоносного трафика

BPS PPS

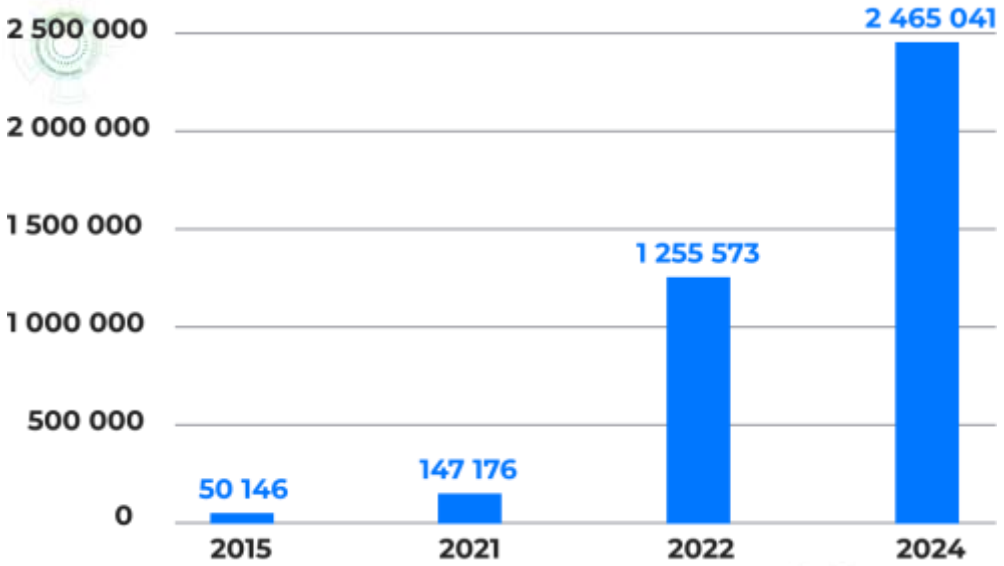
Протоколы

BPS PPS



ASN	Оператор	Запросы
14061	DIGITALOCEAN-ASN	3 161 017
60729	Stiftung Erneuerbare Frei...	970 281
3214	xTom GmbH	256 733
210558	1337 Services GmbH	235 284
Неизвестно		208 728
208323	Foundation for Applied Pr...	199 564
8075	MICROSOFT-CORP-MSN-A...	193 678
198093	Foreningen for digitala fri...	182 818
62212	SmartApe OU	117 535
200195	Verasel, Inc.	112 296

Как менялось число DDoS-атак за последние 10 лет



Пиковая мощность

2015 — 242 Гигабит в секунду

2024 — 2,46 Терабит в секунду*

x10

*по собственным данным DDoS-Guard

Вариативность DDoS-атак сегодня

DST PORT	PROTO	DST ADDR	MIN	MAX	AVERAGE	~95TH
80/http	UDP	[redacted].253.0	46.79Mbps	679.50Gbps	58.98Gbps	511.34Gbps
80/http	UDP	[redacted].254.0	140.38Mbps	659.29Gbps	58.86Gbps	504.60Gbps
443/https	UDP	[redacted].253.0	48.10Mbps	735.85Gbps	57.62Gbps	474.81Gbps
443/https	UDP	[redacted].254.0	144.31Mbps	748.87Gbps	56.72Gbps	469.06Gbps

По определенному протоколу/порту (напр. UDP 53)

Либо максимально разбросанно (TCP/GRE/ICMP/etc)

На определенный хост или максимально размазанно

PROTO	MIN	MAX	AVERAGE	~95TH
GRE	197.13Mbps	816.81Gbps	316.59Gbps	743.30Gbps
UDP	5.70Mbps	52.03Gbps	19.79Gbps	45.67Gbps
ICMP	5.70Mbps	108.33Mbps	9.22Mbps	46.01Mbps
TCP	2.62Mbps	16.64Mbps	376.38Kbps	2.62Mbps

Атакующие ASN

8151 4788 9829

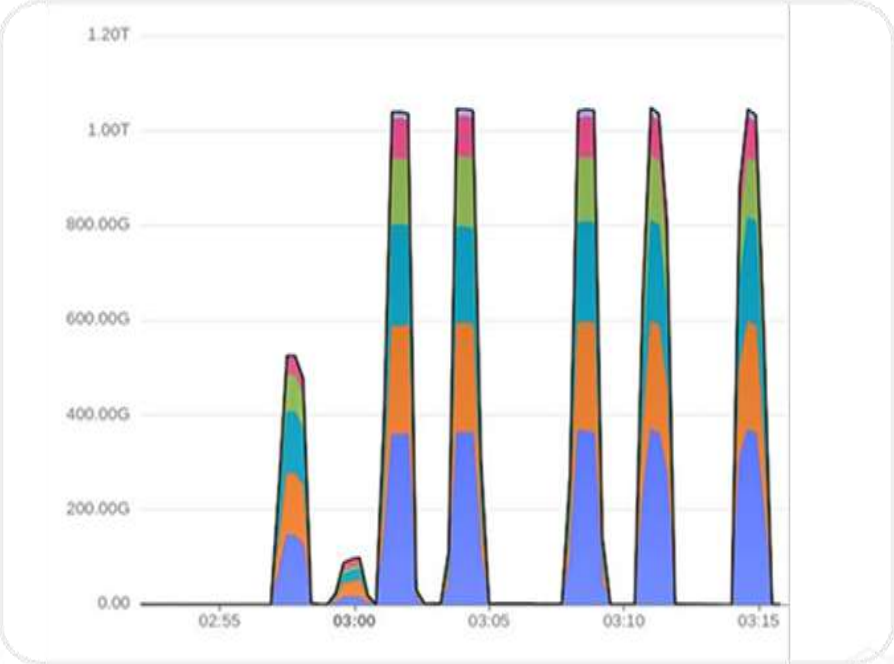
25019 263033

12479 7713

45.10.243.0/24
217.114.42.0/24
91.215.43.0/24
95.129.235.0/24
185.129.101.0/24
и так далее...

Вариативность DDoS-атак сегодня

Кратковременные,
но очень мощные всплески



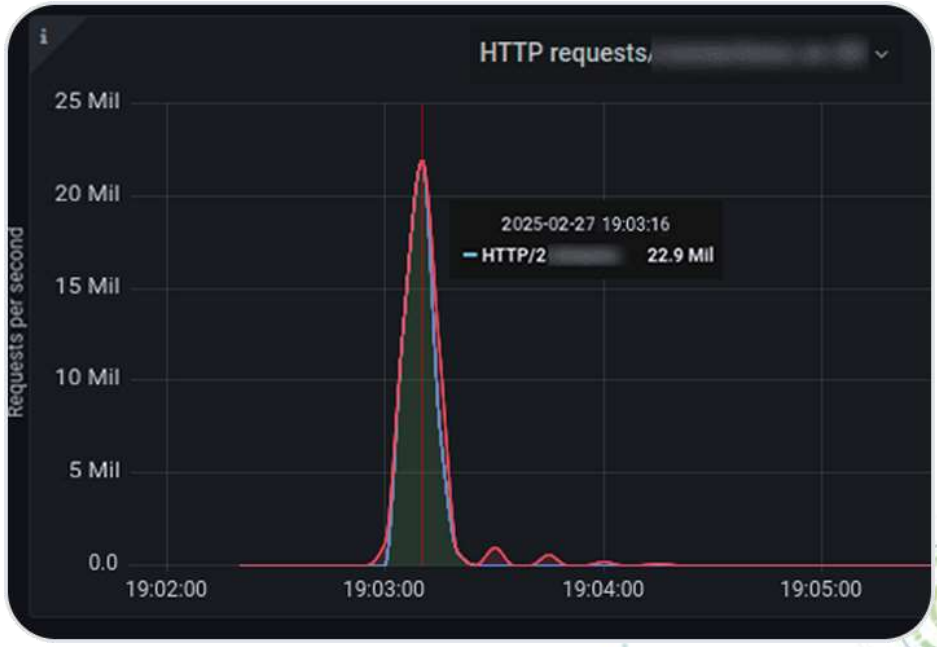
Небольшие по мощности,
но очень продолжительные

Импульсные и мощные L7-атаки

Среднее количество L7-атак в сутки в **6 раз превышает** число DDoS-атак на уровне L3-4.

В 2025 году мы зафиксировали одну из крупнейших L7-атак, ее пиковая мощность достигла **почти 23 млн RPS** (запросов в секунду), а длительность составила **менее 10 секунд.**

В рамках одной DDoS-атаки может участвовать более 2 млн уникальных IP-адресов. Они и питают ботнеты



Топ-5 стран–источников атак

Индонезия	Бразилия
США	США
Россия	Китай
Бразилия	Индия
Германия	Аргентина
по версии DDoS-Guard (октябрь 2025)	**по версии Spamhaus (октябрь 2025)**

https://www.spamhaus.com/threat-map/#botnet

example.com

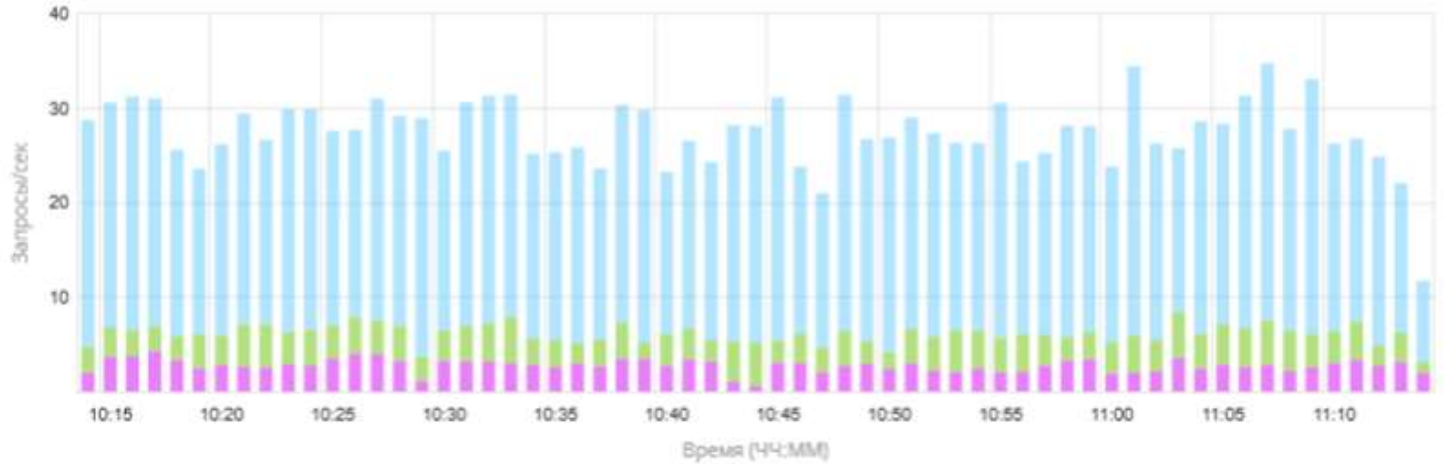
- ОБЩИЕ
- DNS
- SSL
- КАСТОМНЫЕ СТРАНИЦЫ
- ГЕОБЛОКИРОВКА
- БАЛАНСИРОВКА НАГРУЗКИ
- Ч/Б СПИСКИ
- ТРИГГЕРЫ
- BOT MITIGATION
- ПРАВИЛА ЗАЩИТЫ
- СЕГМЕНТАЦИЯ ДОМЕНА
- ЛИМИТ ЗАПРОСОВ

Bot Mitigation: **Блокировка** Изменить

22 373	10 071	12 302	77 834
Всего запросов от ботов	Вредоносные боты	Легитимные боты	Пользователи

Аналитика трафика

За последний 1 час



Вредоносные боты 10.05%

Легитимные боты 12.28%

Пользователи 77.67%

Вредоносные боты Легитимные боты Пользователи

Топ заблокированных IP

Топ заблокированных стран

Топ заблокированных AS

Кейс: защита от DDoS-атак + CDN для медиаплафортмы

Заказчик — высоконагруженная медиаплощадка с многотысячной ежедневной посещаемостью, развитой системой хранения и передачи контента.

Проблемы:

- **Высокая задержка TTFB** (Time to First Byte), что негативно сказывалось на пользовательском опыте
- **Отсутствие гибкости в настройке защиты** от DDoS-атак и парсинга, что делало их ресурс уязвимым для злоумышленников
- **Необходимость в балансировке нагрузки** между кластерами серверов и возможности дополнительной оптимизации трафика

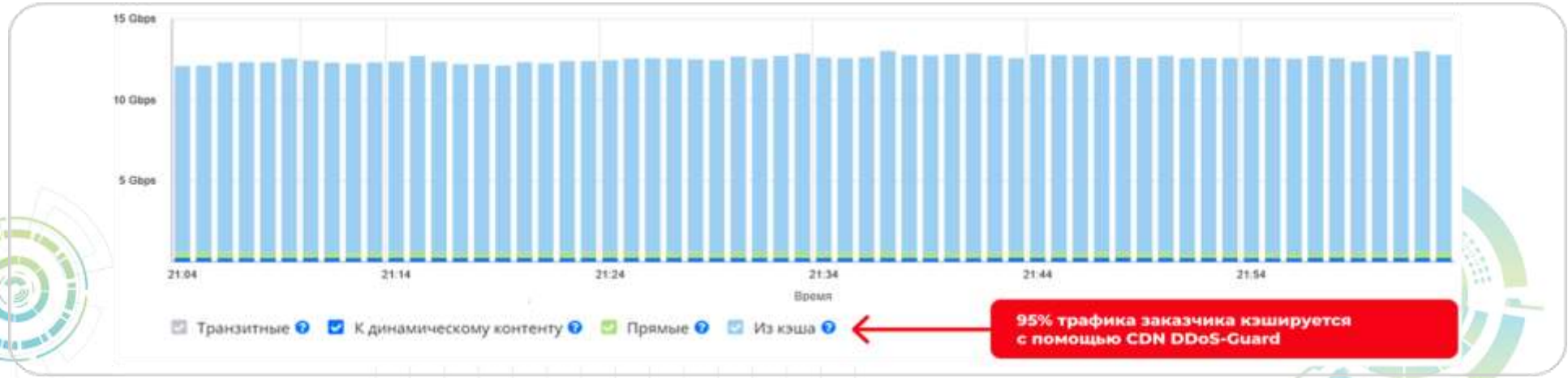
Кейс: защита от DDoS-атак + CDN для медиаплафортмы

Решение:

- **Перманентная фильтрация на уровнях L3/L4/L7.** Стабильное соединение и быстрый DNS resolve, что сразу улучшило показатели TTFB заказчика
- **Rate Limiter** — функционал, который поддерживает 18 параметров HTTP(S)-запроса с гибкими настройками для каждого параметра
- **Разграничение домена на сегменты по типу контента** для более точного срабатывания алгоритмов защиты
- Запросы обрабатываются на ближайшей ноде, а CDN отдает кэшированный контент **за 1-3 мс**

Результаты

- **Защита от DDoS-атак:** трафик с региональных серверов защищен, система анализирует реальные IP-адреса пользователей, гибкие инструменты позволяют самостоятельно управлять фильтрацией в дополнение к базовым настройкам
- **Скорость работы медиаплатформы повысилась на 40%** благодаря CDN, снижению TTFB и быстрому DNS resolve
- **Модуль балансировки помогает поддерживать доступность сервиса** для пользователей даже в периоды повышенной посещаемости



Спасибо за внимание!

г. Алматы, пр. Абая 109В

Единый контакт-центр: 5151

sales@kazteleport.kz