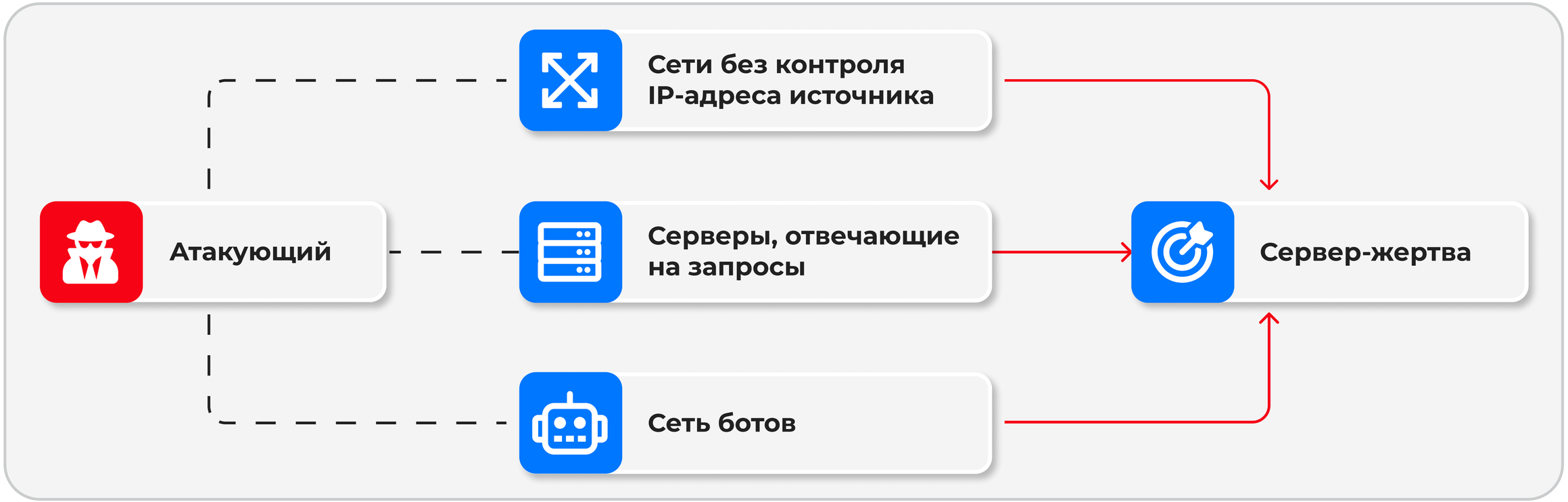
Защита сетей оператора связи: DDoS-атаки, контент и не только. Стратегии партнерства с государственным сектором в эпоху цифровых угроз

Дмитрий Шмидт

Главный инженер информационной безопасности и защиты сети **DDoS-Guard**

Что такое DDoS-атака

— вид кибератаки, при которой злоумышленники создают огромное количество запросов или трафика, чтобы перегрузить целевой ресурс и ограничить к нему доступ для легитимных пользователей.

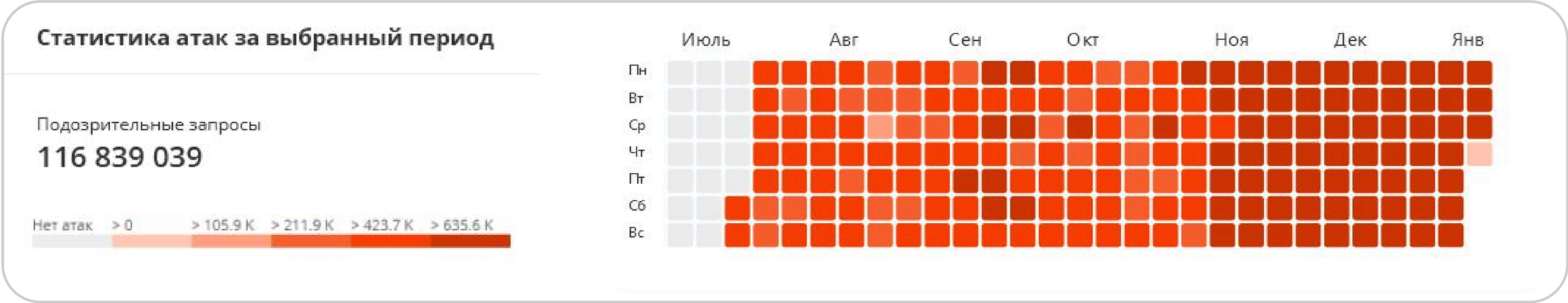


Тренд: «коммерческие» атаки

Хактивизм постепенно теряет актуальность.

DDoS используют как один из наиболее доступных инструментов, чтобы вывести соперника по рынку из игры.

Например, известного хостинг-провайдера, работающего в России и за рубежом, **каждый день атакуют** по заказу его конкурентов.



Тренд: активное развитие ботнетов

По данным DDoS-Guard за 2024 год
в рамках одной атаки может участвовать более 900 000 уникальных IP-адресов.

Основу ботнетов составляет IoT: камеры видеонаблюдения, маршрутизаторы Mikrotik, TP-Link, Zyxel, «умная» техника.

Число уникальных IP в одной DDoS-атаке сопоставимо с количеством IP, которое используется целой страной (Исландия, Кипр, Оман и другие).

ip2location.com: The Percentage of IP Address Ownership by Country in 2024

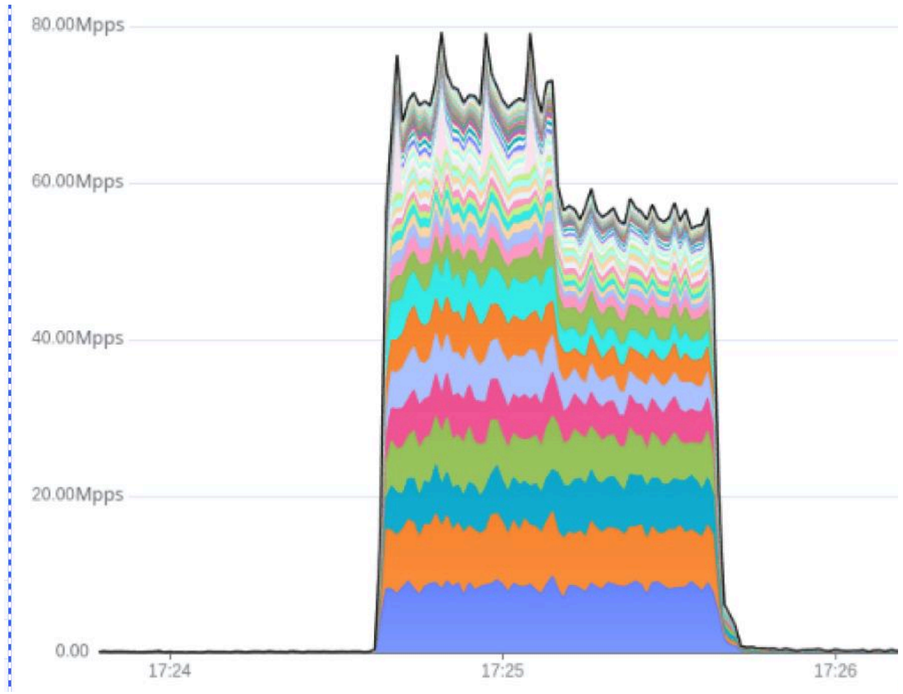
Country Code	Country Name	Total IPs	2024 Ranking
RU	RUSSIA	45,315,781	14
OM	OMAN	1,076,381	93
SC	SEYCHELLES	1,033,497	94 ↑
CY	CYPRUS	1,023,990	95 ↓
IS	ICELAND	913,781	96 ↓

Тренд: мультивекторность и импульсность атак

Актуальны атаки по BGP и GRE с прицелом на бордеры, что влечет за собой падение всего остального по принципу домино

L3-атаки растут в объеме и разрушительности (всплески по 600-800 Гбит/с — уже норма)

	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

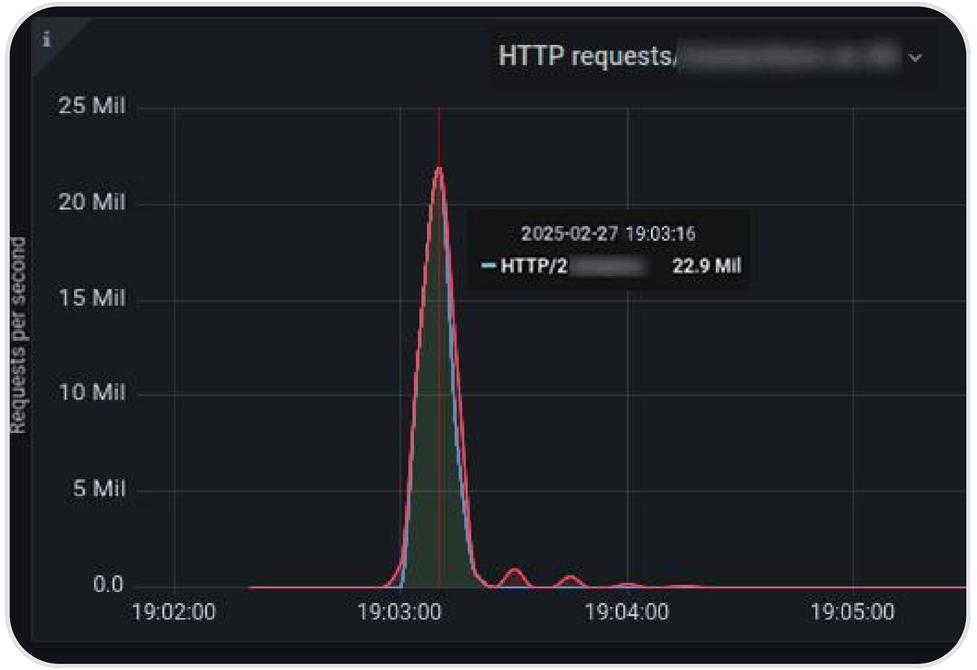


Пример: одна из весьма ярких, но коротких атак: 800 Гбит/с и почти 80 млн пакетов в секунду

Тренд: импульсные и мощные L7-атаки

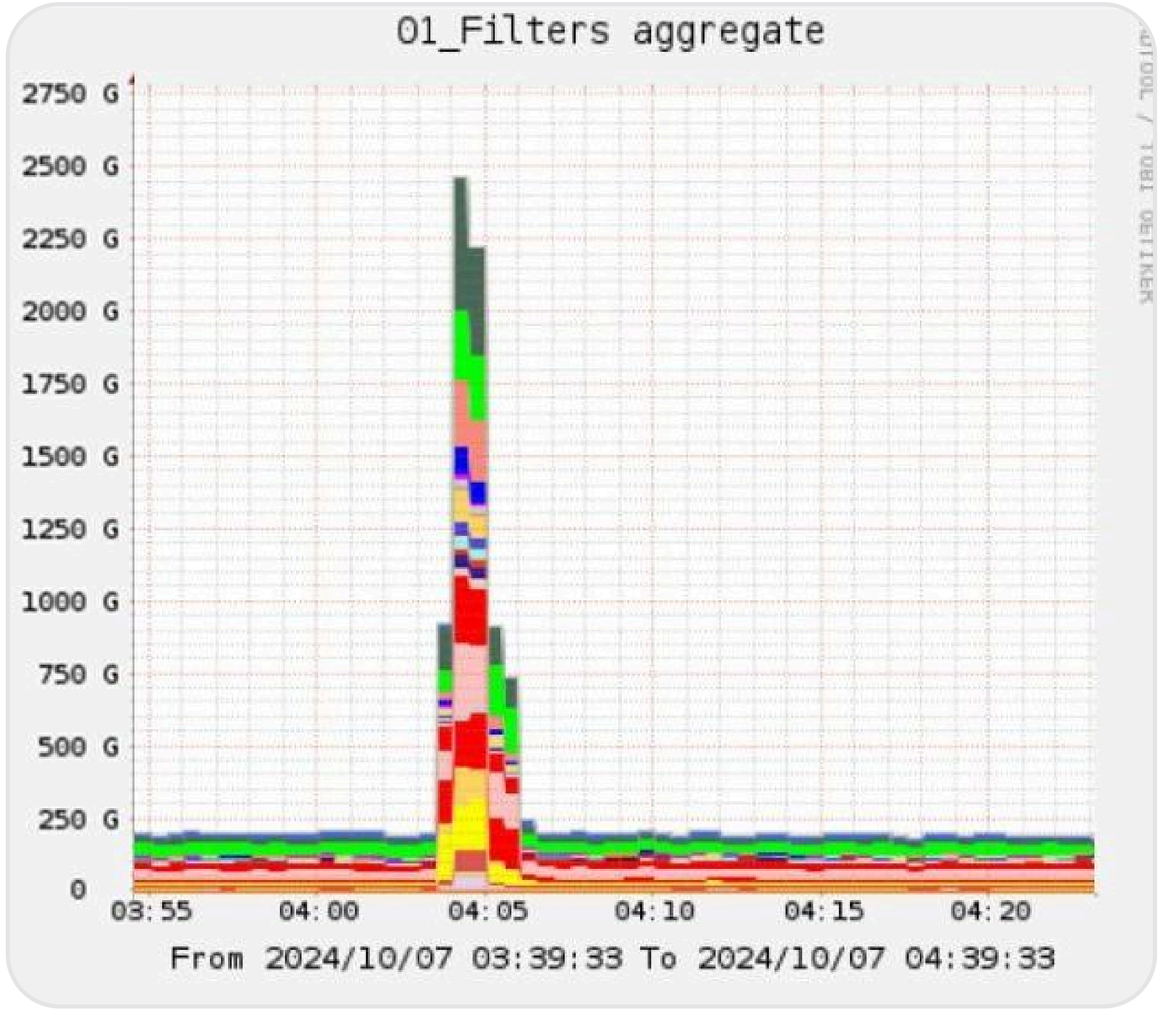
Среднее количество L7-атак в сутки **в 5 раз превышает** число DDoS-атак на уровне L3-4.

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



Особенности атак на операторов и медиаплатформы

- **Прирост числа атак более чем на 60%** в сегменте телекома за последний год
- **Предварительная разведка** периметра жертвы на предмет открытых портов
- **Ковровые атаки** с добавлением спуфинга с российских IP
- **Замена SRC IP и DST IP** в зависимости от метода атакующего
- **DDoS в комбинации с хакерскими манипуляциями**



В октябре 2024 года сеть DDoS-Guard пережила крупнейшую в своей истории атаку в 2,46 Тбит/с.

Пример DDoS-атаки на оператора без защиты

21 марта 2025 года провайдер домашнего интернета Lovit подвергся массированной DDoS-атаке. На пике мощность атаки составила до 219,06 Гбит/с, скорость — до 22,39 млн пакетов в секунду.

> По заявлению Роскомнадзора, «инфраструктура провайдера оказалась не готова к такому потоку вредоносного трафика, что привело к серьезным сбоям в работе сервисов. Компания не предприняла своевременных шагов для минимизации рисков подобных атак.
>
> Это свидетельствует о недостаточном уровне подготовки и планирования в сфере кибербезопасности».

В такой ситуации сегодня может оказаться любая компания

Важно, будет ли она к этому готова!

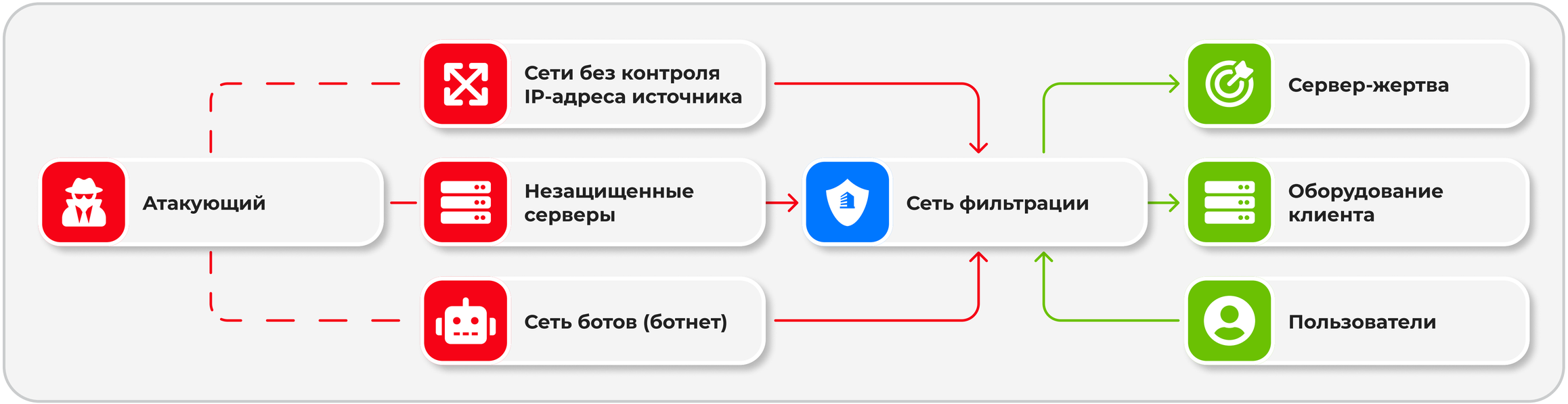
Как подготовиться к угрозам

Что необходимо сделать самостоятельно:

- **Получить четкое понимание архитектуры своего проекта** и «нормального» трафика
- **Исследовать свой периметр через публичные сервисы** (Shodan, Censys, Zoomey и др.)
- **Применить технологии полисинга на оборудовании** (Control Plane (CoPP), ACL и др.)
- **Составить план действий при DDoS-атаке** Disaster Recovery Plan (DRP)

Механизм оптимальной защиты

— защита работает в режиме Always-On, что эффективно нейтрализует известные виды DDoS-атак с первого аномального пакета или потока, **без блокировки по IP-адресу.**



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.

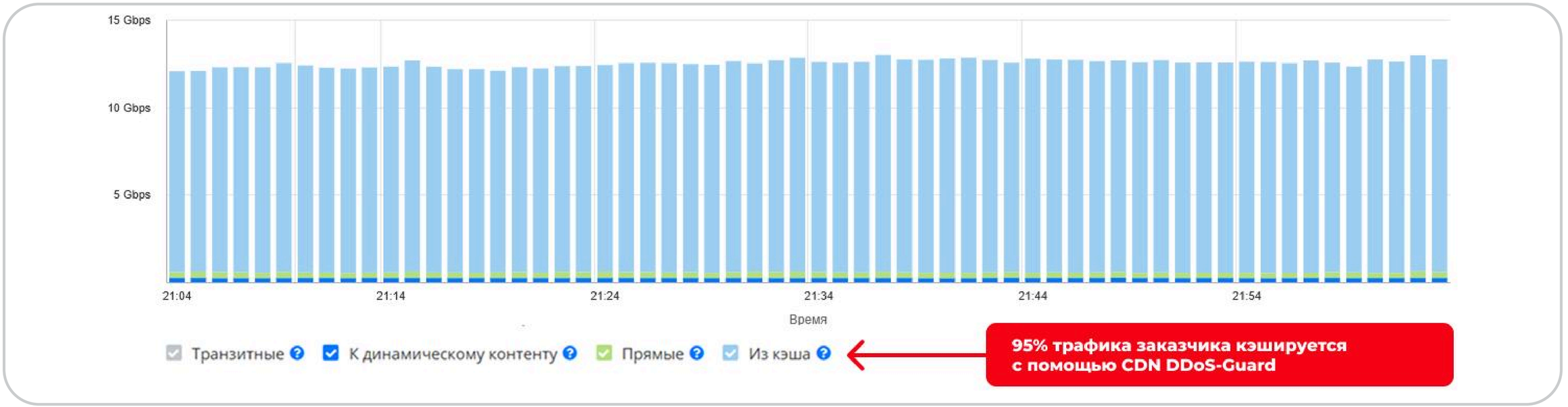
Кейс: защита от DDoS-атак + CDN для медиаплафортмы

Решение:

- **Миграция на инфраструктуру DDoS-Guard** с минимальным окном простоя;
- **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, снижениюTTFB и быстрому DNS resolve.
- **Модуль балансировки помогает поддерживать доступность сервиса** для пользователей даже в периоды повышенной посещаемости.



Работа оператора с государственным сектором через госзакупки

Кейс: к нашему партнеру обратилась крупная государственная компания с просьбой предоставить коммерческое предложение на доступ в интернет с защитой от DDoS-атак в городе Москва.

Боль заказчика: риск простоев через из-за аварийных работ на канале действующего оператора связи.

Решение: резервированное подключение на нескольких узлах. Благодаря наличию у DDoS-Guard 3-х узлов очистки трафика в Москве, в случае падения одного из них, трафик моментально переходит на другой, исключая простой защищаемого сервиса.

Сценарии взаимодействия «DDoS-Guard-партнер-заказчик»

DDoS-Guard — исполнитель, предоставляющий каналы связи с защитой от DDoS-атак

Оператор связи выступает в роли субподрядчика

Оператор связи участвует в закупке от своего имени с полным соответствием ТЗ

DDoS-Guard субподрядчик по защите от DDoS-атак

Заказчик получает комплексное решение

DDoS-Guard

Надежная защита от DDoS-атак

Предоставляем услуги по защите от DDoS-атак и доставке контента с 2011 года. Для обработки и фильтрации трафика самостоятельно разрабатываем ПО и создаем сервисы, основанные на алгоритмах машинного обучения.

Фирменное ПО «DDoS-Guard Protection» зарегистрировано в Едином реестре российских программ для электронных вычислительных машин и баз данных

За 2024 год сеть фильтрации DDoS-Guard нейтрализовала 2,5 млн атак

Контакты

ddos-guard.ru

d.shmidt@ddos-guard.net

@ddos_guard