Пример архитектуры системы защиты географически распределенной системы от DDoS-атак

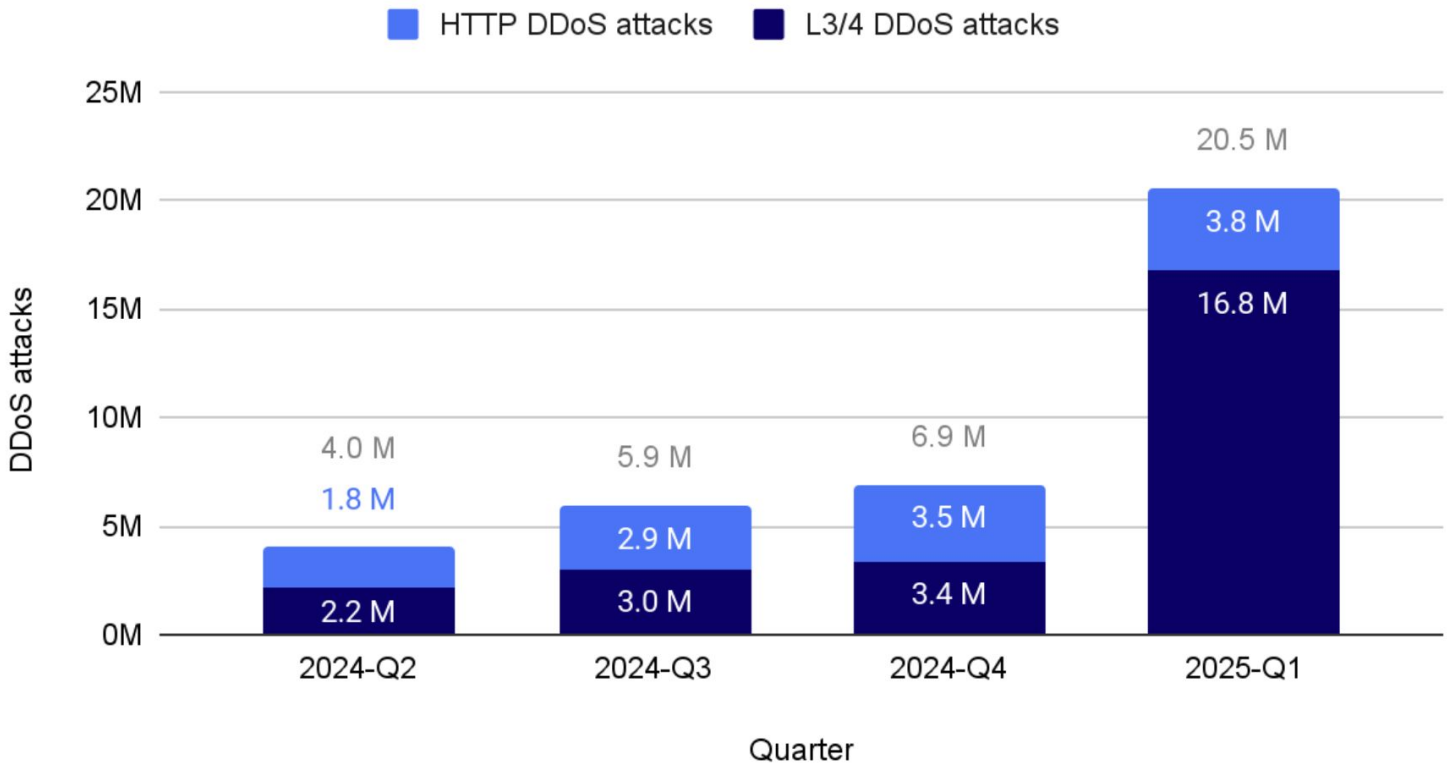
Сергей Черкашин
TeamLead команды AntiDDoS

Сергей Черкашин

TeamLead команды AntiDDoS

- 6 лет в WB
- Руководитель команды по эксплуатации систем защиты от DDoS-атак

DDoS attacks by quarter

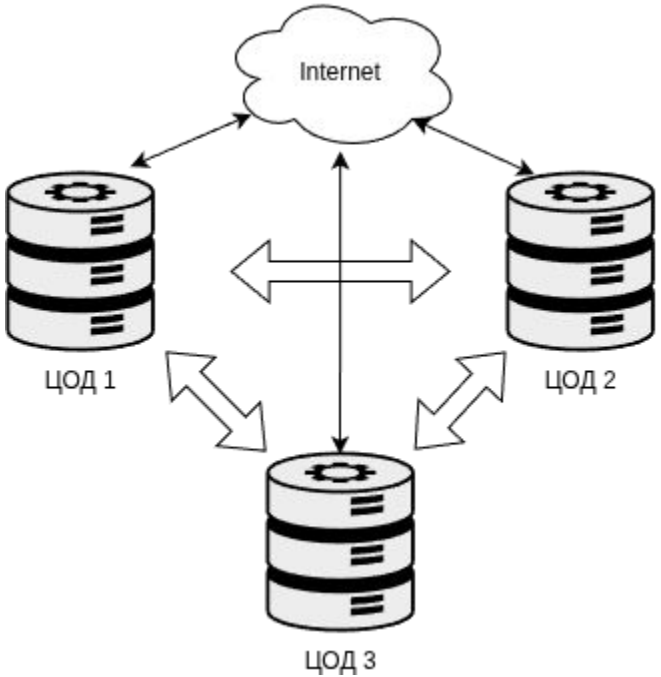


Пример архитектуры системы защиты географически распределенной системы от DDoS-атак

Инфраструктура

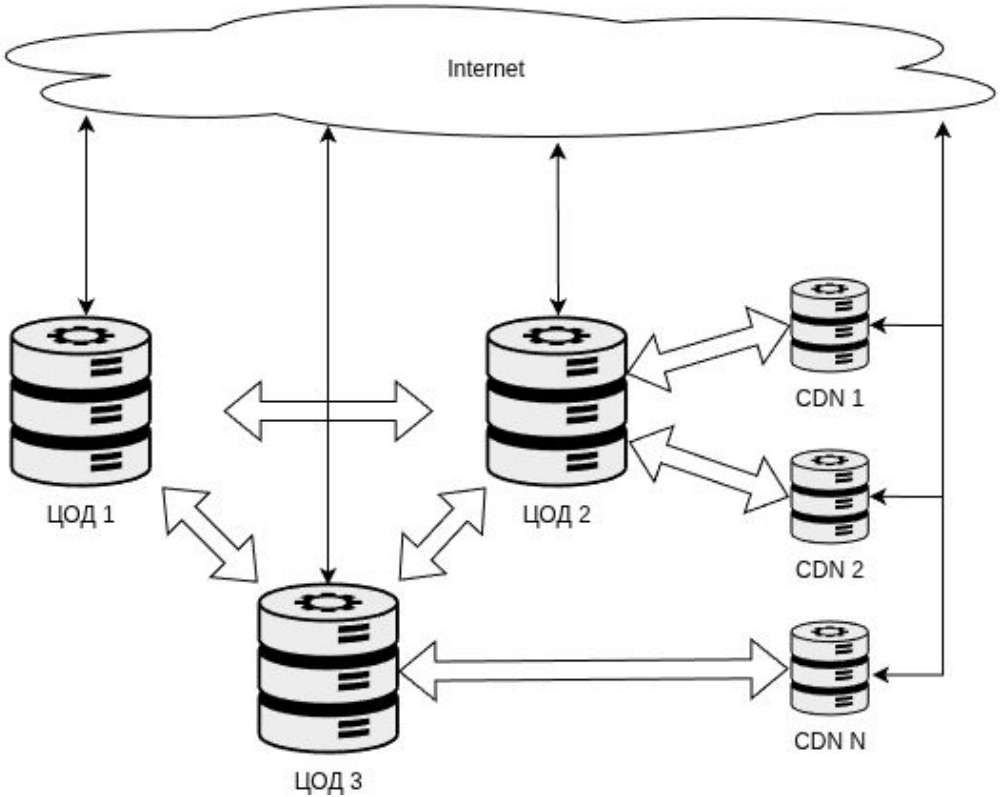
- Несколько ЦОД
- Географическое распределение трафика
- Anycast

Инфраструктура



Пример архитектуры системы защиты географически распределенной системы от DDoS-атак

Инфраструктура



Пример архитектуры системы защиты географически распределенной системы от DDoS-атак

Компоненты системы защиты

- Data collector + storage
- Sensor
- Analyzer
- Decider
- Defender

Defender

Любой инструмент, который позволит отсечь атаку:

- Blackhole пакетов по конкретному признаку на стороне провайдера, через flowspec (L3/L4)
- Blackhole пакетов по конкретному признаку на входе в ДЦ (L3/L4)
- Отказ в обработке “плохих” HTTP-запросов. Кэш. Рейтлимиты. (L7)
- Вывод CDN из анонса (L3)

Decider

Сервис принятия решений:

- Выбирает, какой способ отражения атаки применить.
- На какое время включить этот способ.
- Выполняет дополнительные действия: шлёт алерты, отчёты.

Analyzer

Чтобы кого-то забанить, нужно сначала понять, кого именно банить.

Сунь-Цзы. “Искусство войны”

Sensor

Сервис обнаружения атак.

- Генератор событий
- Узкоспециализированный
- Легковесный

Data storage

- NetFlow
- sFlow
- iMon
- Access log
- L3 metrics
- L7 metrics
- ...

Сценарий №1:
UDP Flood на CDN

Вводные данные

- Зона: CDN
- Канал подключения: 10 Гбит/с
- Оборудование: 2 сервера по 10 ядер
- Канал у основного ДЦ: 500 Гбит/с.

Сценарий реагирования

1. Сенсор обнаруживает переполнение канала
2. Decider:
   - решает ничего не анализировать
   - дает команду вывести CDN из анонса
   - отправляет алерт
3. Defender снимает анонс маршрута

Сценарий №2:
HTTP Flood на CDN

Вводные данные

- Зона: CDN
- Канал подключения: 10 Гбит/с
- Оборудование: 2 сервера по 10 ядер
- Канал у основного ДЦ: 500 Гбит/с.
- Нет Access Log

Сценарий реагирования

1. Сенсор обнаруживает HTTP Flood
2. Сенсор не обнаруживает переполнение канала
3. Decider решает ничего не делать. Отправляет алерт на всякий случай.

Сценарий №3:
HTTP Flood на основной ЦОД

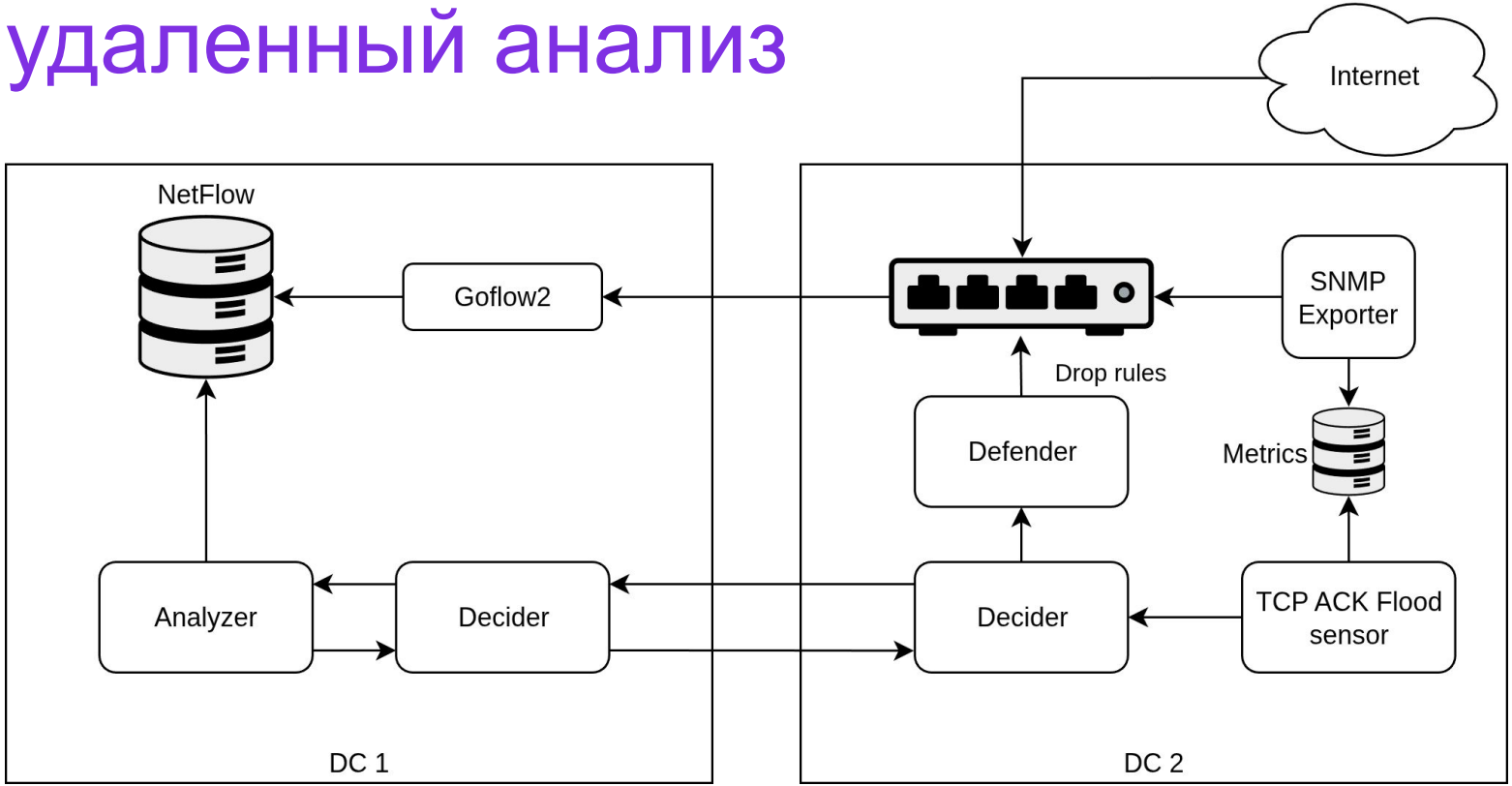
Вводные данные

- Зона: крупный ДЦ
- Канал подключения: 500 Гбит/с
- Оборудование: 2 сервера по 10 ядер
- Канал у основного ДЦ: 30 серверов по 96 ядер
- Есть Access Log

Сценарий реагирования

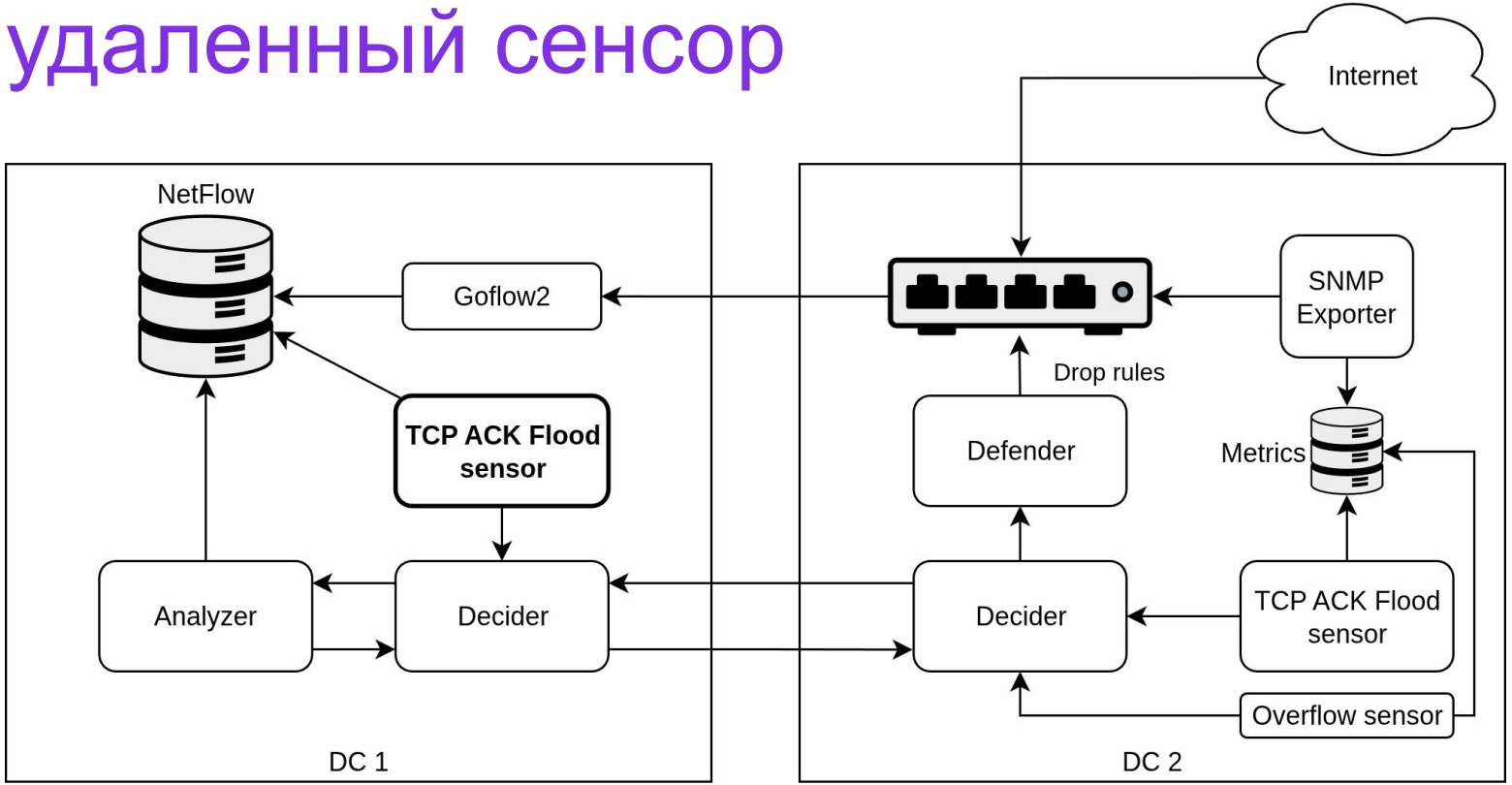
1. Сенсор обнаруживает HTTP Flood
2. Decider запускает Analyzer
3. Analyzer обнаруживает паттерн атаки (например, конкретный User Agent)
4. Decider передает эти данные конкретному Defender-у
5. Defender формирует конфиг Nginx, чтобы тот отвечал 451 Response code на все запросы от этого User Agent

Сценарий №4:
удаленный анализ



Пример архитектуры системы защиты географически распределенной системы от DDoS-атак

Сценарий №4.1:
удаленный сенсор



Пример архитектуры системы защиты географически распределенной системы от DDoS-атак

Спасибо за внимание!

Сергей Черкашин
TeamLead команды AntiDDoS