VAS Experts ITG

Разработка программного обеспечения
для анализа и управления сетевым трафиком
мобильных операторов и интернет-провайдеров

СКАТ AntiDDoS — решение для защиты интернет-провайдеров от DDoS-атак и BotNet-активности

Решение использует DPI, IPFIX Fullflow, технологии QoE и алгоритмы машинного обучения для выявления атак, анализа сетевого трафика и автоматического применения механизмов защиты.

Характеристики решения

< 1 минуты	**100+**	**До 5 Тбит/с**
Время реакции	Одновременных атак	Емкость фильтрации

До 600 млн пакетов/сек

Производительность обработки трафика

Принцип работы

1

Анализ трафика

СКАТ DPI передаёт IPFIX Fullflow в модуль QoE для детального анализа

2

Детектирование угроз

QoE формирует эталон «здорового» трафика и выявляет отклонения от нормы

3

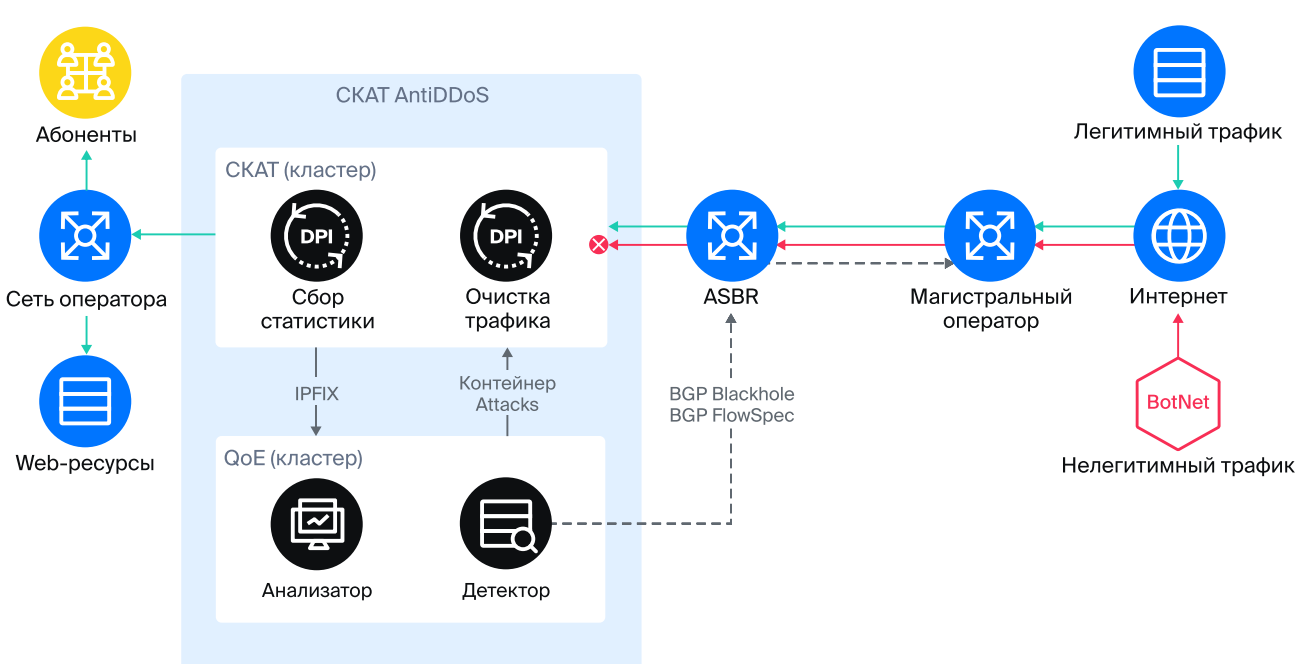
Определение атакующих IP

Детектор классифицирует угрозы и определяет IP-адреса злоумышленников с помощью алгоритмов машинного обучения

4

Фильтрация и блокировка

СКАТ DPI либо полностью блокирует этот трафик, либо ограничивает пропускную способность для него



Защита от распространенных форм атак

Flood, SYN Flood

Перенаправление трафика на СКАТ для фильтрации или blackhole атакуемых адресов

Amplification attacks (DNS, NTP, UDP Flood и др.)

Blackhole атакуемых адресов или применение flowspec на аплинк-канале

BotNet attacks

Blackhole атакуемых адресов, flowspec на аплинк-канале, создание списка адресов BotNet-сети и их блокировка на СКАТ

Взлом элементов сети оператора

Риск взлома определяется по сканированию сети адресов оператора. Детектирование таких сессий и их блокировка по внешнему адресу

Инструмент нейтрализации рисков DDoS и BotNet для операторов

- ⚠ Перегрузка вышестоящего канала
- ⚠ Невозможность оказывать услуги
- ⚠ Жалобы абонентов и отток базы
- ⚠ Финансовые и репутационные потери
- ⚠ Повышенная нагрузка на оборудование
- ⚠ Попадание IP-адресов в черные списки

Преимущества СКАТ AntiDDoS

Распределенная архитектура

Обеспечивает высокую отказоустойчивость

Гибкая настройка

Поддержка различных сценариев блокировки и защиты

Нейросетевые алгоритмы и DPI

Обеспечивают глубокую аналитику трафика

Адаптивная защита

Автообновление правил и реагирование на изменения сетевой активности

Аналитика атак

Модуль QoE представляет статистику:

- По IP-адресам источников и целей
- Геолокации атакующего
- Количеству сессий
- По протоколам

Запросите демо и начните бесплатное тестирование продуктов VAS Experts!

dpi@vas.expert
+7 (812) 313-88-54