Table of Contents

Описание инструментов и архитектуры

VAS Experts предлагает решение для борьбы с DDOS атаками на операторов связи и их инфраструктуру, которые приводят к тому, что оператор связи не может обслуживать своих абонентов. Как следствие массовый отток абонентов, финансовый и репутационные потери.

VAS Experts предлагает несколько вариантов защиты от DDOS атак:

1. Использование только CKAT с функцией автозащиты от SYN Flood, UDP Flood и HTTP Flood. Требуется CKAT с опцией Автозащита от DDoS атак (опция **ddos**).
2. Использование связки CKAT и QoE для детектирования любых типов DDoS атак с возможностью полной блокировки входящего трафика (**blackhole**) и очистки на CKAT. Требуется CKAT с опцией Сбор и выгрузка статистики по протоколам и направлениям в формате IPFIX (опция **ipfix**) и QoE с опцией Обнаружение и очистка трафика (**blackhole and flowspec**) от BotNet и DDoS-атак (опция **antiddos**). Для очистки трафика возможно использовать текущие CKAT (доступно в версиях: BASE, BRAS с опцией mark и channels, COMPLETE), так же возможно поставить выделенный сервер CKAT версии BASE для обработки части трафика.

Лицензирование опции AntiDDoS в рамках CKAT и QoE описано здесь.

Требования:

- QoE и GUI последней версии. Лицензия QoE — любая, AntiDDoS приобретается отдельной опцией
- CKAT лицензии BASE / COMPLETE / BRAS с доп.опциями mark и channels
- Сервер — либо отдельный сервер, либо существующий с установленным QoE
  Обязателен отдельный от CKAT сервер
- На 1гб/с пикового входящего трафика требуется 8,4 ГБ для хранения статистики

Наиболее распространённые формы атак на операторов связи

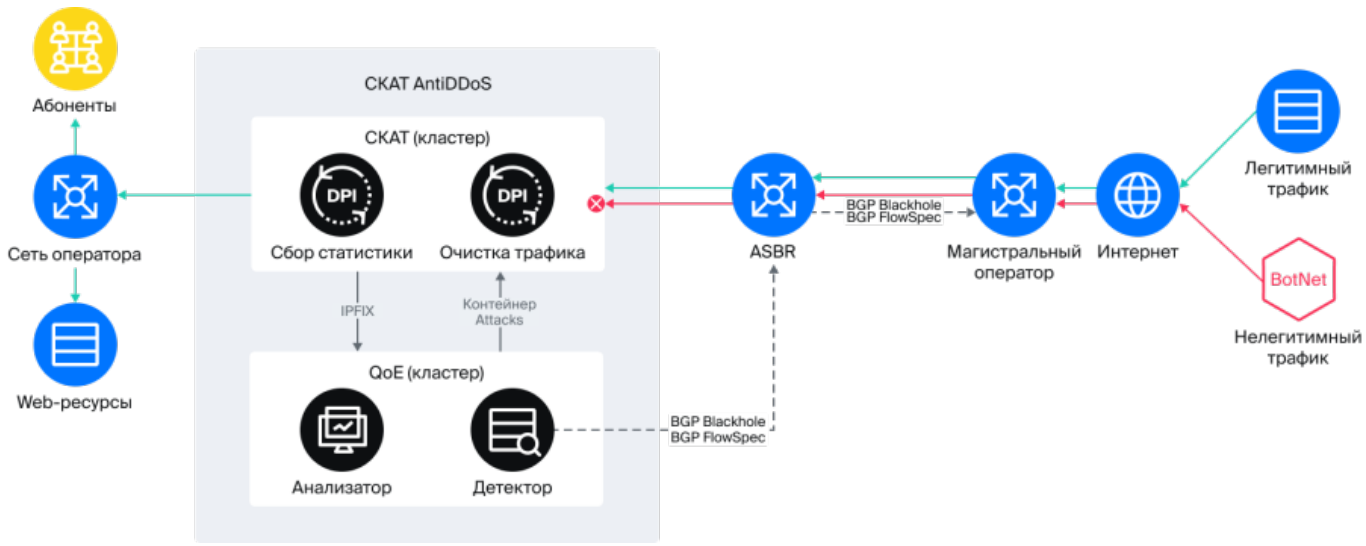
1. Переполнение входных каналов
   - Amplification attacks (DNS, NTP, UDP flood и другие)
     Защита: blackhole атакуемых адресов или применение flowspec на аплинк канале, другие способы защиты неэффективны.
   - BotNet attacks — каждый бот создает относительно небольшой похожий на легитимный трафик, но суммарно трафик превышает возможности входящих каналов оператора, подмена исходящего адреса не осуществляется (см. также п.2)
     Осложнение: в качестве целевого IP для атаки часто фигурирует не один адрес, а до тысячи адресов

Защита: blackhole атакуемых адресов, flowspec на аплинк канале (для некоторых типов трафика), создание списка адресов BotNet сети и их блокировка на CKAT (для некоторых типов трафика)

2. Атака высоким PPS:
   - Flood, SYN flood, обычно с подменой source IP
     Защита: Использовать механизмы защиты от подмены source IP: IP source guard и Фильтрация трафика. Включить перенаправление трафика на CKAT для фильтрации или включить blackhole атакуемых адресов
3. Взлом элементов сети оператора: определяется по наличию SSH и прочих сессий со служебных адресов оператора, которые предварительно конфигурируются и адреса не входят в белый список
   Защита: детектирование таких сессий и их блокировка по внешнему адресу

Архитектура решения AntiDDoS на базе CKAT и QoE

FastMitigator — интеллектуальная система защиты от сетевых атак. Это распределенный модуль анализа трафика, обеспечивающий обнаружение и блокировку широкого спектра киберугроз в режиме реального времени.



Принцип работы

1. Глубокий анализ трафика (DPI) и выгрузка статистики
   - Весь трафик проходит через DPI (CKAT), работающий in-line или на зеркале трафика.
   - В систему QoE отправляется Full NetFlow в формате IPFIX для детального анализа.
2. Анализ статистики и формирование эталона
   - Анализатор обрабатывает Full NetFlow и создаёт "нормальный профиль" — эталон "здорового" трафика (без атак и ботнет-активности).
   - Профиль хранится в распределённых таблицах QoE для быстрого доступа.
3. Выявление аномалий
   - Детектор на основе нейросетей и алгоритмов машинного обучения обнаруживает отклонения, классифицирует угрозы и определяет их источники.
4. Очистка трафика по динамическим правилам
   - При обнаружении атаки в QoE формируется контейнер Attacks, содержащий:

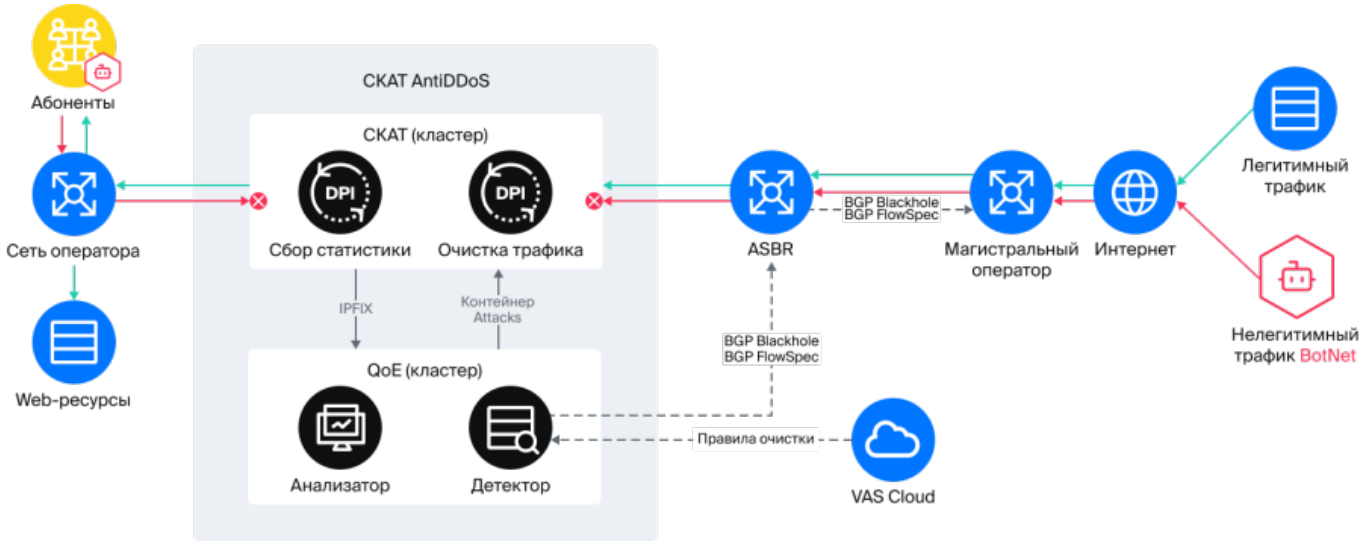
        - IP-адреса атакующих хостов
        - Порты, используемые для атак
    - Контейнер передаётся на CKAT DPI, где создаются специальные протоколы Attacks (или группы протоколов) для каждого типа угрозы. Рекомендуется использовать выделенный CKAT в режиме in-line, который постоянно пропускает весь трафик или получает только часть трафика для очистки.
    - На DPI заранее настраиваются профили защиты (например, через "18. Сессионный полисинг"), где для протоколов Attack применяются в случае если емкость каналом оператора не исчерпана:
        - Drop (полная блокировка)
        - Полисинг (ограничение пропускной способности)
    - Контейнер Attacks обновляется в реальном времени: если атака прекращается, IP хостов исключаются из списка.
5. Защита средствами BGP через blackhole и flowspec
    - В случаях, когда емкость каналов оператора исчерпана, контейнер Attacks может быть передан специальному скрипту, который автоматически добавляет IP абонентов в blackhole, что обеспечивает максимальный уровень защиты инфраструктуры оператора. Входящий трафик на данных абонентов отбрасывается на Uplink канале.
    - Для того чтобы абоненты, на заблокированных публичных IP-адресах, продолжили получать доступ в интернет необходимо временно подменить их IP-адрес — включить услугу CG-NAT на CKAT (использовать ранее на анонсированный публичный пул адресов). Тем самым нет необходимости менять IP-адрес на устройстве абонента в момент атаки, доступ в интернет абонент временно будет получать на другом публичном IP-адресе, а при завершении атаки возвращается исходный IP-адрес — отключить услугу CG-NAT на CKAT.

Преимущества FastMitigator

1. Распределенная архитектура — высокая отказоустойчивость
2. Адаптивная защита — автоматическое обновление правил
3. Глубокая аналитика — нейросетевые алгоритмы + DPI
4. Гибкость — поддержка разных сценариев блокировки

Organic AntiDDoS System

Развитие решения защиты от DDoS нацелено на очистку трафика еще до его попадания в сеть интернет. Установка комплексов CKAT AntiDDoS у множества операторов связи позволит остановить трафик BotNet еще внутри сети оператора. Централизованное управление через VAS Cloud даст возможность реагировать на любые атаки молниеносно и оставить нетронутым даже транспортные каналы между операторами связи, IX и Дата центрами. В случае детектирования атаки на любой ресурс, где стоит CKAT возможно передать параметры для очистки на оператора от которого исходит нелегитимный трафик.


Абоненты
Сеть оператора
Web-ресурсы
СКАТ AntiDDoS
СКАТ (кластер)
DPI
Сбор статистики
DPI
Очистка трафика
IPFIX
Контейнер Attacks
QoE (кластер)
Анализатор
Детектор
ASBR
BGP Blackhole
BGP FlowSpec
Магистральный оператор
Интернет
Легитимный трафик
Нелегитимный трафик BotNet
BGP Blackhole
BGP FlowSpec
Правила очистки
VAS Cloud