iHome
телекоммуникации

Kaspersky DDoS Protection защищает клиентов iHome от DDoS-атак

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky DDoS Protection защищает клиентов iHome от DDoS-атак

ООО «Айхоум» – один из крупнейших магистральных операторов связи в России.

Отрасль: телекоммуникации и связь

Клиент:
ООО «Айхоум»

- Основано в 2010 году
- Москва, Россия
- Протяженность сети – 15 000 км
- 8 стран, 40 городов
- Емкость сети – 5 Тб/с

За 20 лет работы компания, начинавшая как городская сеть обмена трафиком домовых сетей, стремительно выросла в одного из лидеров отрасли связи по объёмам выручки и абсолютного чемпиона по темпам прироста.

Ключевые факторы – фокус на основном бизнесе и постоянное внедрение комплементарных услуг. Услуга защиты от DDoS-атак существует в портфеле компании с 2011 года.

Проблематика

- 2015 год: атака на АО «Транстелеком» затронула около 8% Рунета на 12 часов
- 2016 год: атака на АО «Ростелеком» оставила без связи всю страну к востоку от Урала
- 2017 год: атака на АО «Тинькофф» вывела из строя сеть RETN на 6 часов

В последние годы ресурсы для инициирования DDoS-атаки становятся все более доступны, поэтому масштаб и частота атак быстро растет.

При этом для оператора связи любая атака на конкретного клиента может повлечь негативные последствия для сетевого оборудования, а значит, и негативно отразится на всех клиентах данного сегмента сети.

Перед iHome стояла задача обновить существующее решение, с новыми требования экономической эффективности. При этом решение должно обеспечить как гранулярную защиту выделенных ресурсов заказчиков, так и защиту всей сети оператора без использования таких грубых инструментов, как BGP blackhole.

Решение

Продукты:

- KDP CloudLink
- KDP Local Scrubbing Center

Эффективная защита предполагает детектирование атаки DDoS по периметру сети, с перенаправлением трафика на фильтрующее оборудование, что требует нескольких бесшовно интегрированных сетевых устройств, создающих экосистему, которая включает в себя:

- анализ трафика, обнаружение атак;
- управление маршрутизацией трафика атаки;
- фильтрацию и подавление трафика атаки.

Одновременно с этим на сетевое оборудование оператора, затронутое трафиком атаки, могут направляться правила (по протоколу BGP FlowSpec) для фильтрации volumetric-атак, которые могут привести к выводу его из строя.

Такая схема – с перенаправлением только одного «плеча» трафика – экономически эффективна на больших высокоскоростных сетях с множественным пиринг-партнеров, таких как сеть iHome, за счет архитектурного разделения компонентов DDoS-решения и наращивания отдельных компонентов в нужных точках.

«Для бизнеса непрерывная работа с затратами и при этом обеспечение нового качества услуг – сложная задача. Гибкость решения «Лаборатории Касперского» позволила не только решить наши инфраструктурные задачи, но найти новые точки роста выручки»

Андрей Горбунов,
генеральный директор
iHome

Результат

«Лаборатория Касперского» совместно с партнером ООО «Модель защиты» успешно внедрили решение в инфраструктуру iHome и провели интеграцию с привычными инструментами NOC iHome (Zabbix и Grafana) через API.

Поставленное решение включает в себя «ISP Partners Portal», который позволяет реализовывать и управлять услугами для своих клиентов и получать данные для биллинга услуг в адаптированном формате. Представленная ценовая модель позволяет iHome вести достаточно независимую ценовую политику, реализуя кобрендинговое решение с собственным SLA.

В рамках Kaspersky Hybrid Protection Cloud также реализована возможность bypass- и burst-фильтрующего оборудования на сети iHome с центрами очистки «Лаборатории Касперского», что позволяет переносить часть нагрузки с оборудования iHome и еще более гибко планировать расширение.