Kaspersky® DDoS Protection

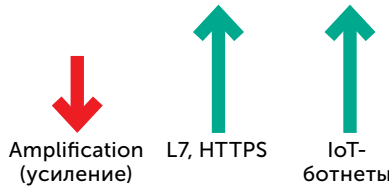
Если ваша компания когда-либо становилась жертвой DDoS-атаки, то вы не понаслышке знаете, что такая атака может привести к серьезным финансовым и репутационным последствиям. А если вам повезло и вы пока не сталкивались с DDoS-атаками, то лучше начать готовиться к ним сейчас, потому что однажды везение может закончиться.

Kaspersky DDoS Protection — это специализированное решение для защиты от DDoS-атак, позволяющее обеспечить непрерывность бизнес-процессов и бесперебойную работу ваших критических онлайн-ресурсов и инфраструктуры.

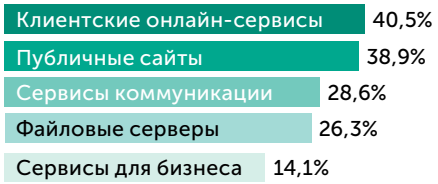
Преимущества решения «Лаборатории Касперского»

- Эффективное всестороннее противодействие DDoS-атакам
- Полный охват и успешная работа с атаками большого объема
- Уникальный сенсор для мониторинга трафика в режиме реального времени
- Оперативная круглосуточная защита и поддержка Экспертной группы KDP
- Отказоустойчивая инфраструктура центров очистки расположенных в основных точках обмена интернет-трафика

Ландшафт атак



Цели атак



Быстрое и точное распознавание атак

Сенсор «Лаборатории Касперского», установленный в облаке KDP либо на площадке заказчика, собирает данные о трафике, строит профили типичного поведения пользователей и различные модели трафика. После этого решение постоянно следит за поведением трафика в режиме реального времени. Любая аномалия, которая может указывать на возможную атаку, немедленно распознается.

Одновременно с этим наши эксперты постоянно отслеживают ситуацию с DDoS-угрозами, чтобы вовремя предотвратить возможные запланированные атаки.

Гибкое реагирование на DDoS-угрозы

Как только распознается возможный сценарий атаки, Группа экспертов KDP получает уведомление и принимает меры по отражению атаки. В рамках KDP Connect или Connect+ отражение DDoS-атак происходит в автоматическом режиме. Параллельно эксперты немедленно проводят детальное исследование атаки и вносят коррективы, учитывая мощность DDoS-атаки, ее тип и сложность.

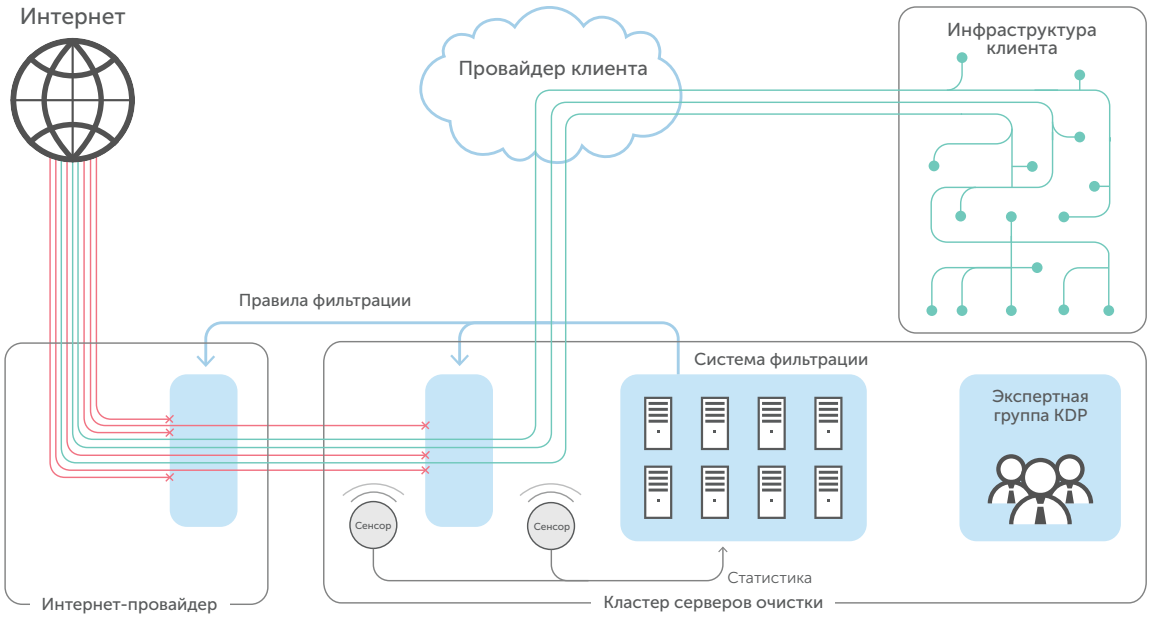
KDP Control позволяет вам самостоятельно определить, когда следует перенаправить трафик на центры очистки для отражения DDoS-атаки.

Вы под атакой? Работайте в обычном режиме!

Как только начинается атака, весь ваш трафик перенаправляется на наши центры очистки. При этом:

- Доступ к вашей инфраструктуры не блокируется большим объемом мусорного трафика.
- Система KDP распознает и удаляет весь «мусорный» трафик.
- Легитимный трафик возвращается к вам сразу после очистки.

Весь процесс отражения атаки происходит незаметно для ваших сотрудников и клиентов и не затрагивает ваши бизнес-процессы.



Отражение DDoS-угроз любого типа и масштаба

Kaspersky DDoS Protection – это эффективное решение для противодействия всем видам DDoS-атак, включая атаки большого объема **(amplification, direct flood), TCP short-packet, TCP connect, L7 (HTTP) и SSL (HTTPS)**. Каждый вид атак направлен на различные элементы IT-инфраструктуры жертвы – интернет-каналы, сетевое оборудование, приложения и др. Одновременное применение различных видов атак может привести к увеличению причиняемого ущерба. Обширный опыт и уникальный подход «Лаборатории Касперского», в котором сочетаются постоянный мониторинг трафика и статистический анализ, а также оперативная и профессиональная работа Группы экспертов KDP позволяют обеспечить вас защитой от всех видов DDoS-атак, включая комбинированные.

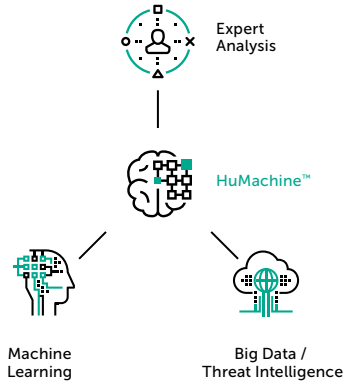
Выберите свой вариант противодействия DDoS-атакам

«Лаборатория Касперского» предлагает три версии решения, которые вы можете выбрать в зависимости от ваших целей, ресурсов и сетевой инфраструктуры:

- **KDP Connect** – перенаправление трафика изменением DNS-записи в режиме Always On, доставка очищенного трафика осуществляется через прокси-сервер, GRE-туннели или через выделенную линию.
- **KDP Connect +** – перенаправление трафика средствами протокола BGP в режиме Always On, доставка очищенного трафика осуществляется через GRE-туннели или выделенную линию.
- **KDP Control** – перенаправление трафика средствами протокола BGP в режиме On Demand, доставка очищенного трафика осуществляется через GRE-туннели или выделенную линию.

Группа экспертов KDP

Группа экспертов KDP (Emergency Response Team), состоящая из специалистов высочайшего класса, круглосуточно отслеживает аномалии в трафике – это позволяет как можно раньше обнаружить начинающуюся атаку и необходимым образом настроить фильтры. Опыт и знания экспертов очень важны, поскольку киберпреступники способны оперативно менять характеристики проводимых DDoS-атак, чтобы причинить максимальный ущерб. Постоянный экспертный мониторинг позволяет оперативно реагировать на опасные изменения в характеристиках происходящей атаки.



www.kaspersky.ru

#ИстиннаяБезопасность