

kaspersky активируй
будущее

Kaspersky DDoS Protection





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.

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 Kaspersky DDoS Protection:

- Защита от всех видов DDoS-атак на уровнях L3, L4 и L7
- Уникальный Сенсор для мониторинга трафика в режиме реального времени
- Оперативная круглосуточная работа Службы технической поддержки
- Отказоустойчивая инфраструктура Центров очистки, расположенных в основных точках обмена интернет-трафиком
- Защита от ботов, возможность интеграции по API

Быстрое и точное распознавание атак

Сенсор Kaspersky DDoS Protection, который установлен в облаке KDP или на площадке клиента, собирает статистику о трафике, строит профили типичного поведения пользователей и различные модели трафика. Благодаря сбору статистики в режиме реального времени любая аномалия, указывающая на возможную атаку, немедленно обнаруживается системой.

Одновременно с этим наши эксперты постоянно следят за ландшафтом угроз, изучают новые методы кибератак и совершенствуют средства защиты от них.

Гибкое реагирование на DDoS-угрозы

При обнаружении возможной атаки команда экспертов Kaspersky DDoS Protection получает уведомление и принимает меры по отражению атаки. Параллельно эксперты немедленно проводят детальное исследование атаки и вносят коррективы, учитывая мощность DDoS-атаки, ее тип и сложность.

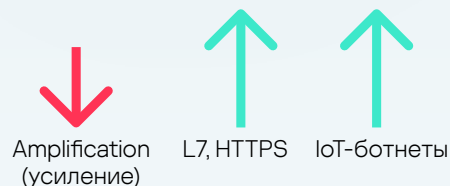
Вы под атакой? Работайте в обычном режиме!

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

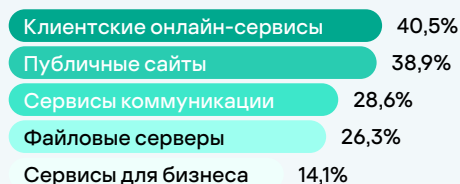
- доступ к вашей инфраструктуре не блокируется большим объемом нелегитимного трафика;
- система Kaspersky DDoS Protection распознает и удаляет весь нелегитимный трафик;
- легитимный трафик возвращается к вам сразу после фильтрации.

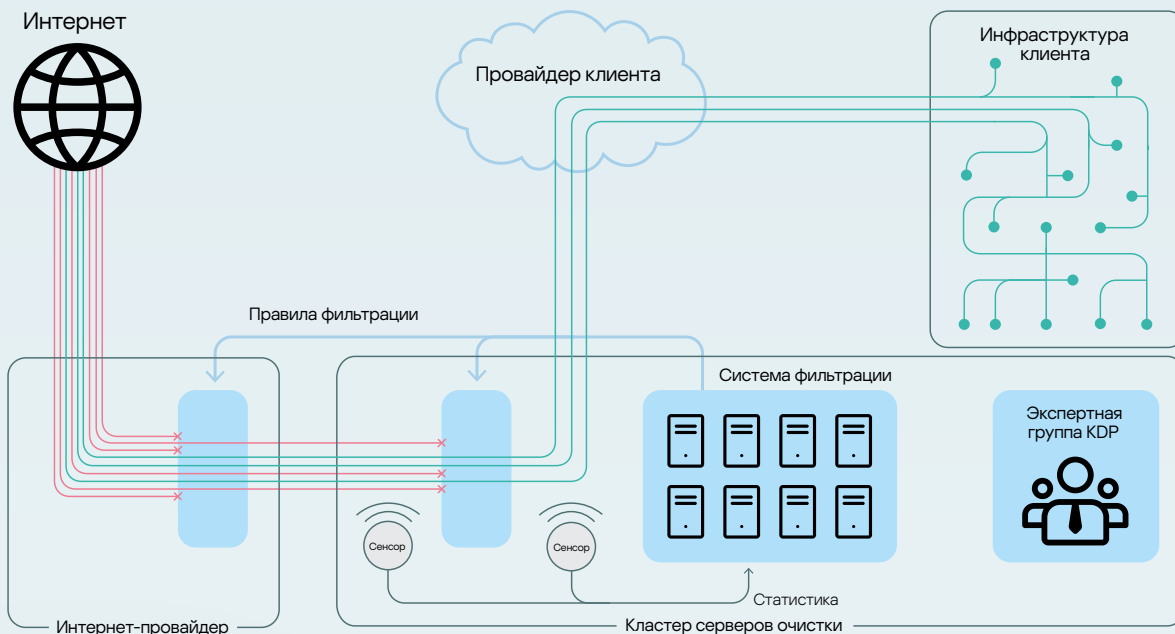
Весь процесс отражения атаки происходит незаметно для ваших сотрудников и не затрагивает ваши бизнес-процессы.

Ландшафт атак



Цели атак





Kaspersky DDoS Protection предоставляет средства и меры защиты для защиты от всех известных типов атак:

- TCP SYN+ACK
- TCP FIN
- TCP RESET
- TCP ACK
- TCP ACK+PSH
- TCP Fragment
- UDP
- Slowloris
- Spoofing
- ICMP
- IGMP
- HTTP Flood
- Brute Force
- Connection Flood
- DNS Flood
- NXDomain
- Mixed
- Ping of Death
- Smurf
- Reflected ICMP & UDP
- Другие атаки

Отражение DDoS-угроз любого типа и масштаба

Kaspersky DDoS Protection – это эффективное решение для противодействия всем видам DDoS-атак, включая атаки большого объема, атаки на уровне L7, TCP short packet, TCP connect и SSL. Каждый вид атак направлен на различные элементы IT-инфраструктуры жертвы – интернет-каналы, сетевое оборудование, приложения и др. Одновременное применение нескольких типов атак может привести к увеличению причиняемого ущерба. Обширный опыт и уникальный подход команды Kaspersky DDoS Protection позволяют обеспечить вас защитой от всех видов DDoS-атак, включая смешанные.

Команда специалистов

Служба технической поддержки, состоящая из специалистов высокого класса, круглосуточно отслеживает аномалии в трафике – это позволяет постоянно применять обновления фильтрующих правил и оперативно реагировать на запросы пользователей. Опыт и знания экспертов важны, поскольку киберпреступники способны оперативно менять характеристики проводимых DDoS-атак, чтобы причинить максимальный ущерб. Постоянный мониторинг трафика позволяет оперативно реагировать на опасные изменения в характеристиках происходящей атаки.

