



Противодействие DDoS-атакам для непрерывной работы вашего бизнеса

- Гибкий подход к построению системы защиты
- Уникальные технологии фильтрации трафика
- Обнаружение атак на ранних стадиях
- Собственная сеть центров очистки трафика
- Детальный анализ и подробные отчеты
- Круглосуточная экспертная поддержка



**Kaspersky
DDoS
Protection**

kaspersky

www.kaspersky.ru/enterprise

Надежная защита онлайн-ресурсов от DDoS-атак

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

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.

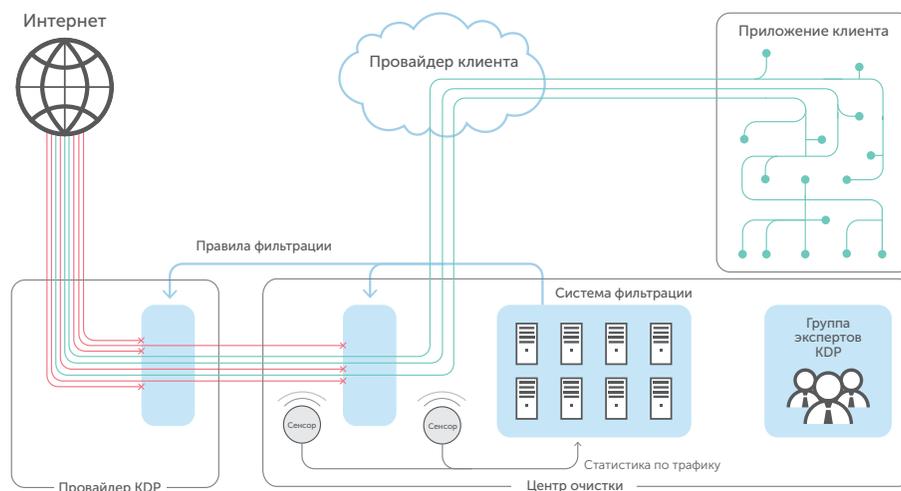
Быстрое и точное распознавание атак

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.

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

© АО «Лаборатория Касперского», 2020.
Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью соответствующих владельцев.

Как приобрести:

По вопросам покупки и любым другим вопросам относительно Kaspersky DDoS Protection проконсультируйтесь с партнером «Лаборатории Касперского». Контактная информация и адреса партнеров представлены на странице: kaspersky.ru/how-to-buy