
Kaspersky®
DDoS Prevention
Защита вашей компании
от финансового
и репутационного
ущерба
• 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.ru/ddos-prevention
KASPERSKY lab

Затраты на проведение DDoS-атак снижаются, особенно с учетом распространения уязвимых устройств и рабочих станций и обилия недостатков конфигурации на уровне приложения. При этом атаки становятся сложнее и масштабнее: за считанные минуты они могут вывести из строя веб-ресурсы предприятия, вызвать перегрузку сети, остановить ключевые внутренние бизнес-процессы и полностью парализовать онлайн-операции.

Kaspersky DDoS Prevention

Чтобы избежать репутационных и финансовых потерь в результате атак, используйте решение Kaspersky DDoS Prevention. Оно поможет вам сохранить непрерывность бизнес-процессов и надежно защитить свои ресурсы от DDoS-атак современного типа.

Гибкий подход к защите

Вы можете выбрать один из вариантов решения, в зависимости от степени риска и потребностей вашего бизнеса.

Control — защита по требованию, перенаправление трафика по протоколу BGP и доставка очищенного трафика с помощью GRE/MPLS, требуется установка сенсора*.

Connect — перенаправление трафика по протоколу DNS и доставка очищенного трафика с помощью Proxy или GRE-туннелей.

Connect+ — перенаправление трафика по протоколу BGP и доставка очищенного трафика с помощью GRE/MPLS.

Connect и Connect+ используют облачные технологии и обеспечивают постоянную фильтрацию трафика. При этом установка сенсора не требуется — эта функция будет выполняться в наших центрах очистки. Кроме того, Connect и Connect+ экономят ваши ресурсы, так как полностью управляются специалистами «Лаборатории Касперского».

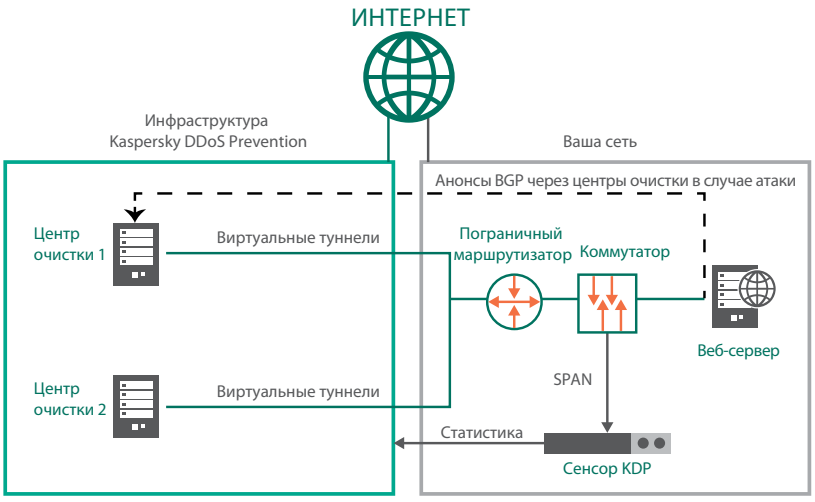

Схема Kaspersky DDoS Prevention Control

Раннее обнаружение атак

Благодаря DDoS-аналитике «Лаборатории Касперского» (Kaspersky DDoS Intelligence) многие DDoS-атаки обнаруживаются на ранней стадии и не успевают причинить вред. С помощью Kaspersky DDoS Intelligence решение ведет мониторинг поведения ботнетов, что помогает заблаговременно узнавать о подготовке к проведению атаки.

Распределенные центры очистки

Ключевой элемент Kaspersky DDoS Prevention — центры очистки, подключенные к крупнейшим интернет-магистралям. В каждом регионе «Лаборатория Касперского» одновременно использует несколько центров, чтобы иметь возможность разделить или перенаправить трафик, нуждающийся в очистке.

КАК ПРИОБРЕСТИ:
По вопросам покупки и любым другим вопросам относительно Kaspersky DDoS Prevention проконсультируйтесь с партнером «Лаборатории Касперского». Контактная информация и адреса партнеров представлены на странице: kaspersky.ru/find_partner_office

* Сенсор – программный компонент, осуществляющий сбор статистики по трафику защищаемых ресурсов.