

Kaspersky DDoS Prevention

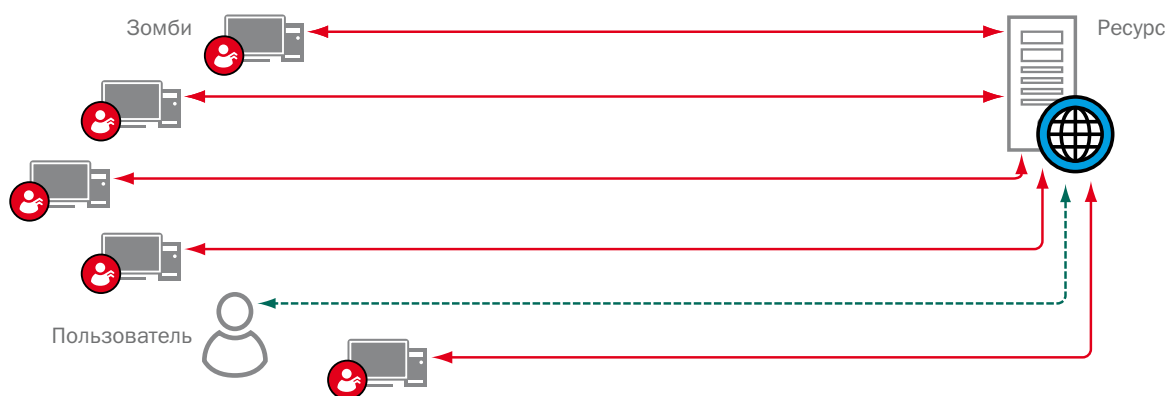


Активное развитие сферы услуг и систем дистанционного обслуживания клиентов через интернет заставляет владельцев задумываться об обеспечении высокой доступности их ресурсов. Для этого предпринимается много усилий, в том числе — построение всевозможных схем резервирования и обеспечения катастрофостойчивости.

Но все эти усилия могут оказаться бесполезными перед угрозой, от которой просто невозможно застраховаться — перед DDoS-атаками.

DDoS-атака (англ. Distributed Denial of Service — «распределённая атака типа «отказ в обслуживании») — атака на вычислительную систему, выполняемая одновременно с большого числа компьютеров, с целью довести атакуемую систему до отказа, т.е. цель атаки — создание таких условий, при которых легитимные пользователи системы или совсем не могут получить доступ к предоставляемым системой ресурсам (сервисам), или этот доступ для них затруднён.

Схема осуществления DDoS атаки



Все DDoS атаки можно разделить на два типа:

- канал связи атакуемой сети переполняется большим количеством «мусорного» трафика;
- на сервер, где размещен атакуемый ресурс, отправляется большое количество «мусорных» запросов, что перегружает вычислительные мощности сервера и он теряет возможность обрабатывать легитимные запросы.

Опасность DDoS-атак заключается и в том, что, будучи направлены только на один из ресурсов, они могут оказать влияние на другие ресурсы и систе-

мы, размещенные в тех же сегментах сети, что и атакуемый ресурс. Кроме того, в последнее время все чаще объектами атак становятся не просто интернет-порталы, но и иные доступные в интернете сервисы и приложения. В результате атака, направленная, например, на серверы электронной почты, может помешать нормальному функционированию бизнес-процессов всей организации, а при перегрузке каналов связи из-за атаки на интернет-портал может затруднить связь с дополнительными офисами и филиалами, парализовать работу сети терминалов и т.п.

Kaspersky DDoS Prevention

В зависимости от сферы бизнеса, в которой работает та или иная компания, простой сервисов в результате DDoS-атаки может повлечь за собой:

- падение продаж
- убытки от простоя демонстрации рекламы и т.п.
- недовольство клиентов и контрагентов
- срыв бизнес-процессов
- сокрытие других, осуществляемых параллельно атак
- прямой ущерб от воздействия на системы электронных торгов и т.п.

К сожалению, в силу ряда причин организация DDoS-атак становится все доступнее. Минимальная стоимость 1 дня атаки составляет 3–5 тысяч рублей. Это способствует тому, что DDoS становится распространенным оружием конкурентной борьбы. По статистике «Лаборатории Касперского», мишенью DDoS-атак становятся компании, занимающиеся самым разным бизнесом.

Распространенные средства защиты, увы, не способны в полной мере противодействовать DDoS-атакам:

- межсетевые экраны и системы IDS/IPS: находятся непосредственно перед защищаемым ресурсом и бессильны против переполнения канала связи;
- маршрутизация в «черные дыры», применяемая провайдерами, заключается в блокировке атакующего трафика. Однако таким образом блокируются и легальные запросы, то есть злоумышленники достигают своей цели — ресурс становится недоступным для пользователей;

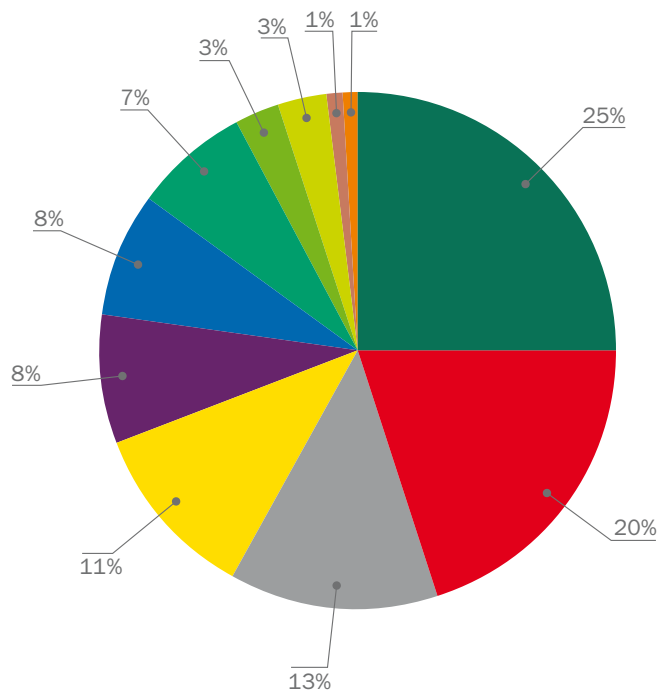
Распределение атакованных сайтов по категориям интернет-деятельности
(из «Обзора DDoS-атак», второй квартал 2011 г.)



- оптимизация настроек ресурса помогает только от маломощных атак;
- многократное резервирование ресурсов — крайне дорогой, а значит, недоступный для большинства организаций способ.

Последнее время вопросам защиты от DDoS-атак уделяется внимание в отраслевых стандартах и сборниках лучших практик в области обеспечения информационной безопасности:

Документ	Разделы, в которых затронуты вопросы защиты от DDoS
FFIEC	<ul style="list-style-type: none"> • Availability security objectives
Gramm-Leach Bliley	<ul style="list-style-type: none"> • Protect Security and Confidentiality of Customer's Non-Public Personal Information • Protect Against Anticipated Threats and Hazards to Information Security • Establish Disaster Recovery and Business Continuity Program
Sarbanes Oxley	<ul style="list-style-type: none"> • Secure Information Infrastructure • Safeguard Information Assets
USA Patriot Act	<ul style="list-style-type: none"> • Implement Risk Based Systems and Monitoring
Basel II	<ul style="list-style-type: none"> • Monitoring of Risks • Business Continuity Plans • Implementation of Risk Mitigation



Kaspersky DDoS Prevention

Сервис Kaspersky DDoS Prevention представляет собой мощную систему распределенной фильтрации трафика, состоящую из географически распределенных высокопроизводительных центров очистки трафика, подключенных к интернету по высокоскоростным каналам связи. Такое решение позволяет выдержать DDoS-атаку практически любой мощности.

Для выявления паразитного трафика во время атаки в системе Kaspersky DDoS Prevention, среди прочих, применяется следующий ряд критериев фильтрации трафика:

- **статистический:** основан на анализе отклонения статистических параметров трафика от средних значений;
- **статический:** основан на черных и белых списках, в том числе формируемых пользовательскими приложениями через API;
- **поведенческий:** основан на анализе соблюдения или несоблюдения спецификаций прикладных протоколов;
- **сигнатурный:** основан на анализе индивидуальных особенностей поведения ботов и т.п.

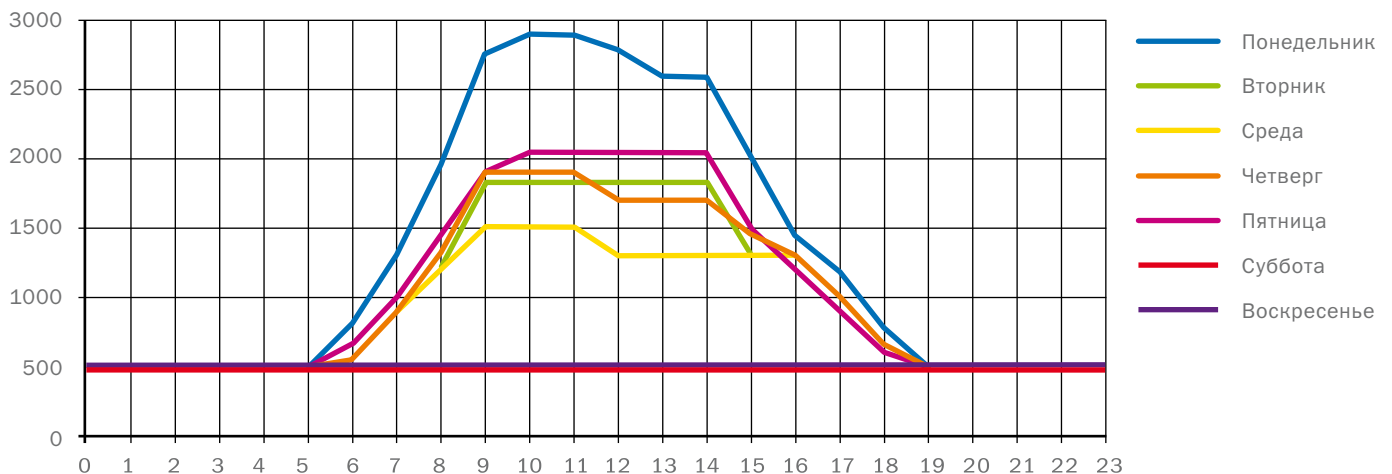
Система включает в себя набор программных компонентов, необходимые технические средства, а также персонал, который обслуживает систему, осуществляет взаимодействие с клиентами и занимается анализом, способствующим качественному управлению системой. В состав системы Kaspersky DDoS Prevention входят следующие компоненты:

- сенсор;
- центр очистки трафика;
- подсистема управления;
- портал.

Сенсор

Назначение сенсора — собирать информацию о трафике, направленном на ресурс клиента, и предоставлять ее системе Kaspersky DDoS Prevention для анализа и своевременного выявления аномалий. На основании данных, полученных от сенсора, в системе Kaspersky DDoS Prevention строятся статистические профили трафика, которые позволяют своевременно выявлять отклонение параметров трафика ресурса и создавать критерии для статистических методов фильтрации.

Пример статистического профиля фильтрации



Центр очистки трафика

Назначение центра очистки — очистка перенаправленного трафика от паразитной составляющей.

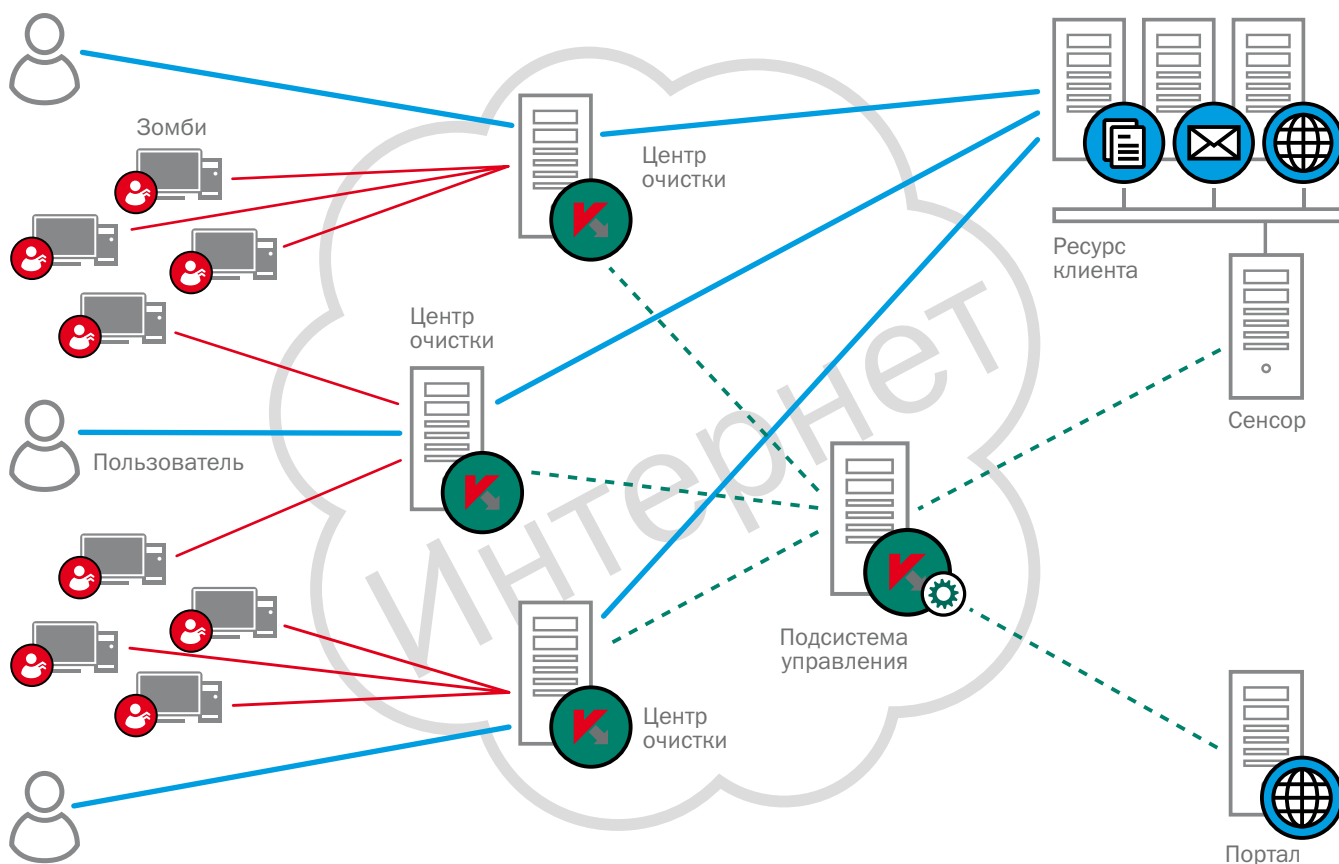
Центр очистки представляет собой программный компонент системы, развернутый на нескольких серверах, выполняющих роль:

- **фильтрующего маршрутизатора**, фильтрующего маршрутизатора, принимающего решение по пропуску того или иного трафика на основании профиля фильтрации, переданного с подсистемы управления;

- **прокси-сервера**, обеспечивающего перенаправление очищенного трафика на ресурс клиента

Один центр очистки может обслуживать несколько сетевых ресурсов одного или нескольких клиентов.

Архитектура системы Kaspersky DDoS Prevention



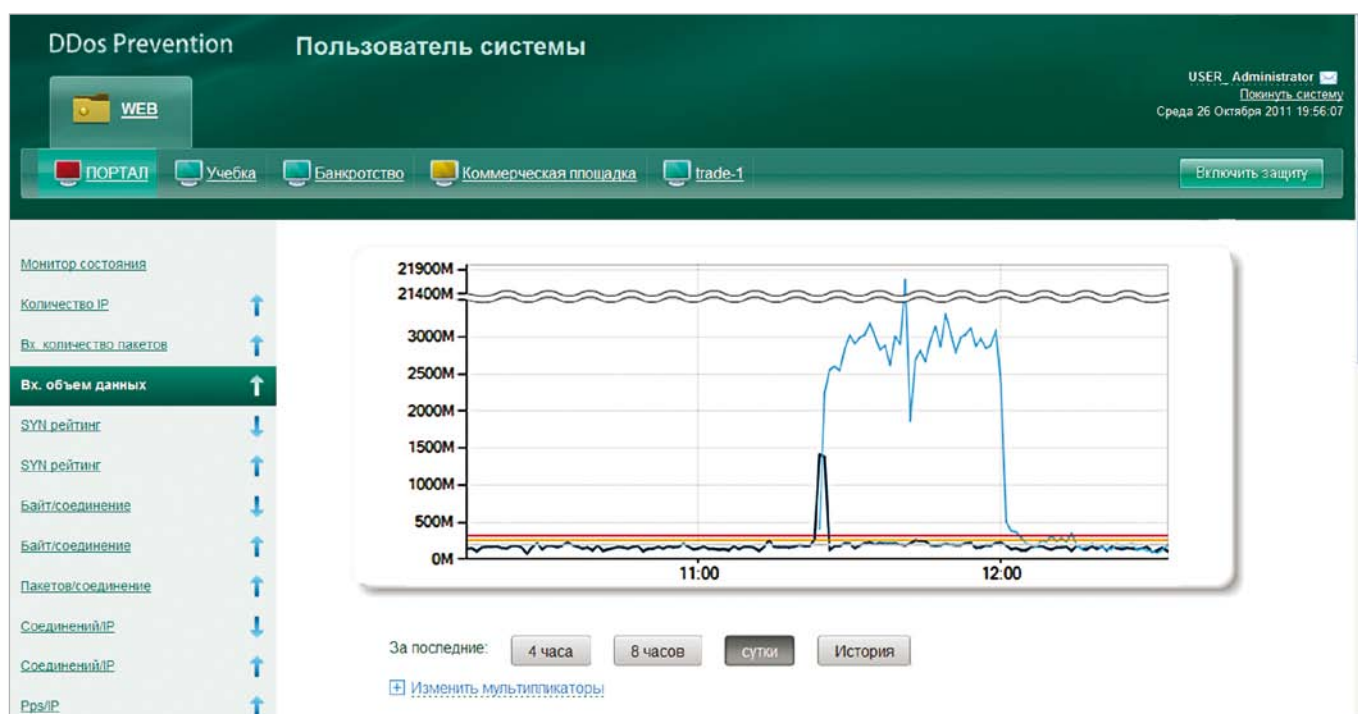
Подсистема управления

Подсистема управления обеспечивает координацию работы всех компонентов системы и равномерное распределение нагрузки на компоненты системы.

Портал

Портал представляет собой WEB-портал, при помощи которого Клиент системы Kaspersky DDoS prevention может контролировать параметры работы системы, анализировать параметры трафика ресурса и возникающие аномалии.

Интерфейс системы Kaspersky DDoS Prevention



Конкурентные преимущества Kaspersky DDoS Prevention

- Система защиты Kaspersky DDoS Prevention — это эффективная распределенная система фильтрации трафика готовая принять на себя мощь практически любых DDoS-атак.
- Надежность работы сервиса обеспечивается за счет территориального распределения компонентов системы, что исключает их одновременный выход из строя вследствие различных причин. Система Kaspersky DDoS Prevention не зависит от какого-либо конкретного провайдера, что также повышает ее надежность и отказоустойчивость.
- Система Kaspersky DDoS Prevention в режиме 24x7 поддерживается командой профессионалов, которые уже 5 лет занимаются вопросами защиты от DDoS-атак, изучают методы и способы, применяемые злоумышленниками для нападения на интернет-ресурсы.
- На компонентах системы Kaspersky DDoS Prevention применяется комплекс статистических, сигнатурных, поведенческих и иных методов очистки трафика, что позволяет защищать ресурсы и от сложных интеллектуальных атак, которые уже преодолели другие средства защиты, в том числе от атак типа low rate.
- В систему Kaspersky DDoS Prevention включена функция детектирования атак при помощи сенсоров, размещенных непосредственно около защищаемого ресурса, что позволяет незамедлительно реагировать на любые отклонения трафика.
- Работа системы Kaspersky DDoS Prevention основана на индивидуальном подходе к защите каждого ресурса или сетевого сервиса. Для каждого защищаемого объекта в системе создаются индивидуальные профили фильтрации трафика.
- Система Kaspersky DDoS Prevention разработана ведущей антивирусной компанией, аналитики которой постоянно изучают самые последние версии вредоносного ПО. В структуру «Лаборатории Касперского» входит специальное подразделение, которое занимается исключительно изучением зомби-сетей и борьбой с ними, поэтому мы обладаем самой свежей информацией о тех методах, которые используют злоумышленники, и можем эффективно противостоять им.
- Сервисом Kaspersky DDoS Prevention можно воспользоваться заранее, подключившись к нему для предотвращения возможных атак, а также после того, как атака уже началась.
- По желанию клиента специалисты «Лаборатории Касперского» после отражения атаки на ресурс могут подготовить для заказчика полный пакет документов для передачи в правоохранительные органы.
- Система Kaspersky DDoS Prevention — гибкое решение, ее работа основана не только на фиксированном наборе параметров, но и на наборе правил, которые могут вручную добавляться аналитиками системы прямо в ходе отражения атаки.
- Обновление функционала Kaspersky DDoS Prevention может происходить непосредственно в ходе отражения атаки.
- Многоуровневая смешанная фильтрация с использованием поведенческого и статистического анализа позволяет отражать атаки, которые проходят через многие другие системы защиты.
- В ходе мероприятий по защите администраторы системы Kaspersky DDoS Prevention дают клиенту рекомендации по администрированию защищаемых веб-сайтов и прочих ресурсов.
- Сама атака может быть настолько мощной, что вполне способна перегрузить канал, ведущий к конкретному (небольшому) провайдеру услуг. Центры очистки Kaspersky DDoS Prevention подключены к интернету через нескольких провайдеров по высокоскоростным каналам связи, что серьезно затрудняет возможность их перегрузки.
- Провайдер, использующий в своей сети средства защиты от DDoS, может защитить только своих клиентов. Система Kaspersky DDoS Prevention может защитить ресурс, расположенный в любом месте сети.
- Система Kaspersky DDoS Prevention используется многими компаниями для защиты своих сетевых инфраструктур, что позволяет специалистам «Лаборатории Касперского» постоянно изучать новые механизмы и особенности работы бот-сетей.

О «Лаборатории Касперского»

«Лаборатория Касперского» — крупнейший в Европе производитель систем защиты от вредоносного и нежелательного ПО, хакерских атак и спама. Компания входит в четверку ведущих мировых производителей программных решений для обеспечения информационной безопасности. По итогам 2010 года, выручка компании выросла на 38%, превысив 500 млн долларов США. В «Лаборатории Касперского» работают более 2300 высококвалифицированных специалистов. Продукты компании надежно защищают компьютеры и мобильные устройства более 300 млн пользователей во всем мире, технологии используются в продуктах крупнейших мировых поставщиков программных и аппаратных решений. Более подробную информацию можно получить на сайте www.kaspersky.ru.

Kaspersky DDoS Prevention

© ЗАО «Лаборатория Касперского», 2011.
Зарегистрированные товарные знаки и знаки обслуживания
являются собственностью их правообладателей