# KASPERSKY DDOS PREVENTION

**Узнайте, как «Лаборатория Касперского» защищает бизнес от DDoS-атак**

www.kaspersky.ru/DDoS-prevention

# КИБЕРПРЕСТУПНИКИ ЦЕЛЕНАПРАВЛЕННО АТАКУЮТ БИЗНЕС

Если ваш бизнес уже подвергался атаке, приводящей к отказу в обслуживании (DDoS), то вы знаете, каким масштабным может быть ущерб от нее. Но даже если до сих пор ваша компания не привлекала внимания киберпреступников, это еще не означает, что проблема DDoS-атак никогда вас не коснется.

## ОБЪЕМЫ И СЛОЖНОСТЬ АТАК РАСТУТ

К сожалению, за последние годы затраты на организацию DDoS-атак существенно снизились, а объем таких атак значительно возрос. Вместе с тем, атаки стали более сложными и достаточно масштабными, чтобы в течение нескольких секунд вызвать перегрузку сети атакуемой организации, остановить ее ключевые внутренние бизнес-процессы и полностью парализовать онлайн-операции.

Нарушение работы онлайн-сервисов компании, деятельность которой напрямую связана с функционированием веб-сайта или внутренней IT-инфраструктуры, совершенно недопустимо. Устранение последствий успешной DDoS-атаки может обойтись пострадавшему бизнесу очень недешево. Поэтому коммерческим предприятиям и государственным организациям необходимо быть в курсе возможных угроз и принимать упреждающие меры для защиты от DDoS-атак.

## ПРЕДУПРЕЖДЕН – ЗНАЧИТ ВООРУЖЕН

У каждой компании должна быть эффективная стратегия защиты, чтобы применить ее в случае обнаружения DDoS-атаки. Тогда организация сможет незамедлительно заняться устранением ее последствий, чтобы:

- минимизировать ущерб от простоя инфраструктуры и остановки бизнес-процессов;
- обеспечить клиентам скорейший доступ к онлайн-сервисам;
- не допустить падения продуктивности работы сотрудников.

# ▶ МЕТОДЫ ПРОВЕДЕНИЯ DDOS-АТАК

Киберпреступники используют различные методы проведения DDoS-атак, чтобы парализовать работу IT-инфраструктуры компании-жертвы.

## ОБЪЕМНЫЕ АТАКИ

Атаки данного типа становятся все более частыми. Такая атака полностью парализует выполнение всех онлайн-операций (или значительно увеличивает необходимое для этого время) за счет создания такого объема трафика, который значительно превышает пропускную способность канала организации.

## АТАКИ НА ПРИЛОЖЕНИЯ

Цель атак на приложения – с помощью сложных запросов, выполнение которых требует значительных вычислительных ресурсов, вывести из строя ключевые приложения, от работоспособности которых зависят онлайн-операции компании-жертвы.

## ДРУГИЕ ИНФРАСТРУКТУРНЫЕ АТАКИ

Цель таких атак – вызвать перегрузку сетевого оборудования и/или серверных ОС, чтобы временно вывести их из строя.

## ГИБРИДНЫЕ АТАКИ

Киберпреступники также могут проводить сложные атаки, сочетающие в себе элементы объемных атак и атак на приложения и инфраструктуру.

# КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ОТ DDOS-АТАК И УСТРАНЕНИЯ ИХ ПОСЛЕДСТВИЙ

Kaspersky DDoS Prevention обеспечивает надежную интегрированную защиту от DDoS-атак. Решение включает все необходимое для безопасности вашего бизнеса. Система Kaspersky DDoS Prevention (KDP) осуществляет непрерывный анализ всего онлайн-трафика, уведомляет вас о возможной атаке, а затем принимает перенаправленный трафик, очищает его и доставляет на ваши ресурсы. Это позволяет эффективно защитить ваш бизнес от всех типов DDoS-атак.

## KASPERSKY DDOS PREVENTION ВКЛЮЧАЕТ:

- приложение-сенсор «Лаборатории Касперского», которое работает в составе вашей IT-инфраструктуры;
- глобальную сеть центров очистки трафика;
- поддержку центра управления KDP и консультации экспертов по защите от DDoS-атак;
- детальный анализ и отчеты по имевшим место атакам;
- личный кабинет клиента на портале Kaspersky DDoS Prevention.

# КАК РАБОТАЕТ KASPERSKY DDOS PREVENTION

Приложение-сенсор устанавливается максимально близко к защищаемому ресурсу и круглосуточно собирает данные о вашем трафике, включая:

- количество отправленных и полученных байтов;
- количество отправленных и полученных пакетов;
- статистику по действиям посетителей веб-сайта;
- другие статистические данные по трафику (всего более двух десятков параметров).

Вся собранная информация отправляется на облачные серверы «Лаборатории Касперского», где она подвергается анализу. В результате формируются профили типичного поведения пользователей и типичного трафика; выявляются закономерности изменения трафика в зависимости от времени суток, дня недели, наличия специальных мероприятий; устанавливаются пороговые значения отклонений измеряемых параметров трафика для уровней «Внимание» и «Тревога». Используя сформированные профили, наши облачные серверы с высокой точностью оценивают состояние вашего трафика в режиме реального времени и оперативно выявляют аномалии, которые могут свидетельствовать о начале DDoS-атаки на защищаемый ресурс.

Кроме того, наши специалисты постоянно отслеживают ландшафт DDoS-угроз, чтобы идентифицировать новые виды атак. Такие экспертные исследования гарантируют, что клиенты «Лаборатории Касперского» смогут воспользоваться всеми преимуществами быстрого реагирования на DDoS-атаки.

## МЫ ПРОВОДИМ ДОПОЛНИТЕЛЬНУЮ ПРОВЕРКУ, ЧТОБЫ ИЗБЕЖАТЬ ЛОЖНЫХ СРАБАТЫВАНИЙ, А ЗАТЕМ ОЧИЩАЕМ ВАШ ТРАФИК

При появлении в трафике защищаемых ресурсов аномальной активности наши эксперты собирают о ней исчерпывающую информацию, принимают решение о целесообразности перехода в режим фильтрации и связываются с заказчиком для выдачи соответствующих рекомендаций.

При переводе трафика защищаемых ресурсов заказчика на центры очистки (переходе в режим фильтрации):

- ваша инфраструктура не перегружена мусорным трафиком;
- процесс очистки устраняет весь мусорный трафик;
- легальный трафик доставляется на ваши ресурсы.

Обнаружение атаки и переход в режим фильтрации проходят абсолютно незаметно для ваших сотрудников и клиентов.

# НАСТРОЙКА ЗАЩИТЫ: БЫСТРО И ПРОСТО

Выбирая Kaspersky DDoS Prevention, вы получаете круглосуточный сервис, включающий мониторинг защищаемых ресурсов, сопровождение и поддержку специалистов по отражению DDoS-атак, а также возможность быстро и просто обеспечить перевод ваших ресурсов в режим защиты и обратно (в обычный режим работы). «Лаборатория Касперского» и ее партнеры помогут настроить систему защиты в соответствии с нуждами вашего бизнеса.

Если вам требуется решение «под ключ», готовое к немедленной эксплуатации, то «Лаборатория Касперского» и ее партнеры возьмут на себя настройку системы, в том числе:

- установят приложение-сенсор и необходимое аппаратное обеспечение в вашей инфраструктуре;
- настроят перенаправление трафика на центры очистки;
- настроят возврат «чистого» трафика на ваши ресурсы.

От вас потребуется лишь обеспечить отдельный интернет-канал для сенсора, чтобы Kaspersky DDoS Prevention продолжал сбор данных, если ваш основной интернет-канал станет недоступен в результате атаки.

## ПРИЛОЖЕНИЕ-СЕНСОР: МОНИТОРИНГ 24X7

Сенсор поставляется в комплекте со стандартной ОС Ubuntu Linux. Поскольку сенсор работает в ОС Ubuntu Linux, на стандартном сервере x86 или на виртуальной машине*, вам не потребуется устанавливать какое-либо специализированное оборудование.

Сенсор подключен к SPAN-порту (Switched Port Analyzer, анализатор коммутируемых портов), что позволяет ему осуществлять мониторинг входящего и исходящего трафика в полном объеме.

Как только сенсор подключается к вашей инфраструктуре, он сразу же начинает собирать данные о входящем и исходящем трафике. Приложение анализирует заголовки каждого пакета и отправляет собранную информацию на облачные серверы «Лаборатории Касперского», где формируются статистические профили трафика, типичного для вашего ресурса.

В целях соблюдения конфиденциальности информации сенсор и система Kaspersky DDoS Prevention не обрабатывают содержимое трафика, а лишь собирают данные о нем.

* Параметры виртуальной машины должны соответствовать или превышать минимальные требования, указанные «Лабораторией Касперского».

## ПЕРЕНАПРАВЛЕНИЕ ТРАФИКА

В обычных условиях облачные серверы Kaspersky DDoS Prevention отслеживают наличие любых признаков DDoS-атаки на защищаемый ресурс, а ваш трафик направляется напрямую в корпоративную сеть. Трафик перенаправляется в нашу глобальную сеть центров очистки только в том случае, если после обнаружения атаки вы самостоятельно предпримете необходимые действия по его перенаправлению.

Kaspersky DDoS Prevention позволяет выбрать один из следующих способов перенаправления:

- протокол динамической маршрутизации BGP (Border Gateway Protocol);
- изменение DNS-записи.

## ВИРТУАЛЬНЫЕ ТУННЕЛИ (GENERIC ROUTING ENCAPSULATION, GRE)

Вне зависимости от того, какой метод перенаправления трафика является оптимальным для вашего бизнеса, для коммуникации между вашим пограничным шлюзом (или маршрутизатором) и центром очистки Kaspersky DDoS Prevention используется виртуальный GRE-туннель.

В том случае, если бизнес подвергся DDoS-атаке, весь трафик может быть перенаправлен на один из наших центров очистки. Очищенный трафик затем доставляется обратно на ваши ресурсы через виртуальные GRE-туннели.

# ▶ ВЫБОР МЕЖДУ BGP И DNS

Как настраивать перенаправление трафика – через BGP или через DNS? Это зависит от особенностей вашей корпоративной IT-инфраструктуры.

- Для использования BGP необходимо, чтобы:
  - ресурсы, которые вы хотите защитить, находились в провайдеро-независимой сети IP-адресов;
  - вы имели автономную систему (AS).

  Как правило, большинство крупных и средних компаний отвечают этим условиям.

- Для использования DNS необходимо, чтобы:
  - ресурсы, которые вы хотите защитить, располагались внутри доменной зоны, находящейся под вашим управлением;
  - значение параметра Time to Live (TTL, «время жизни») для DNS-записей составляло 5 мин.

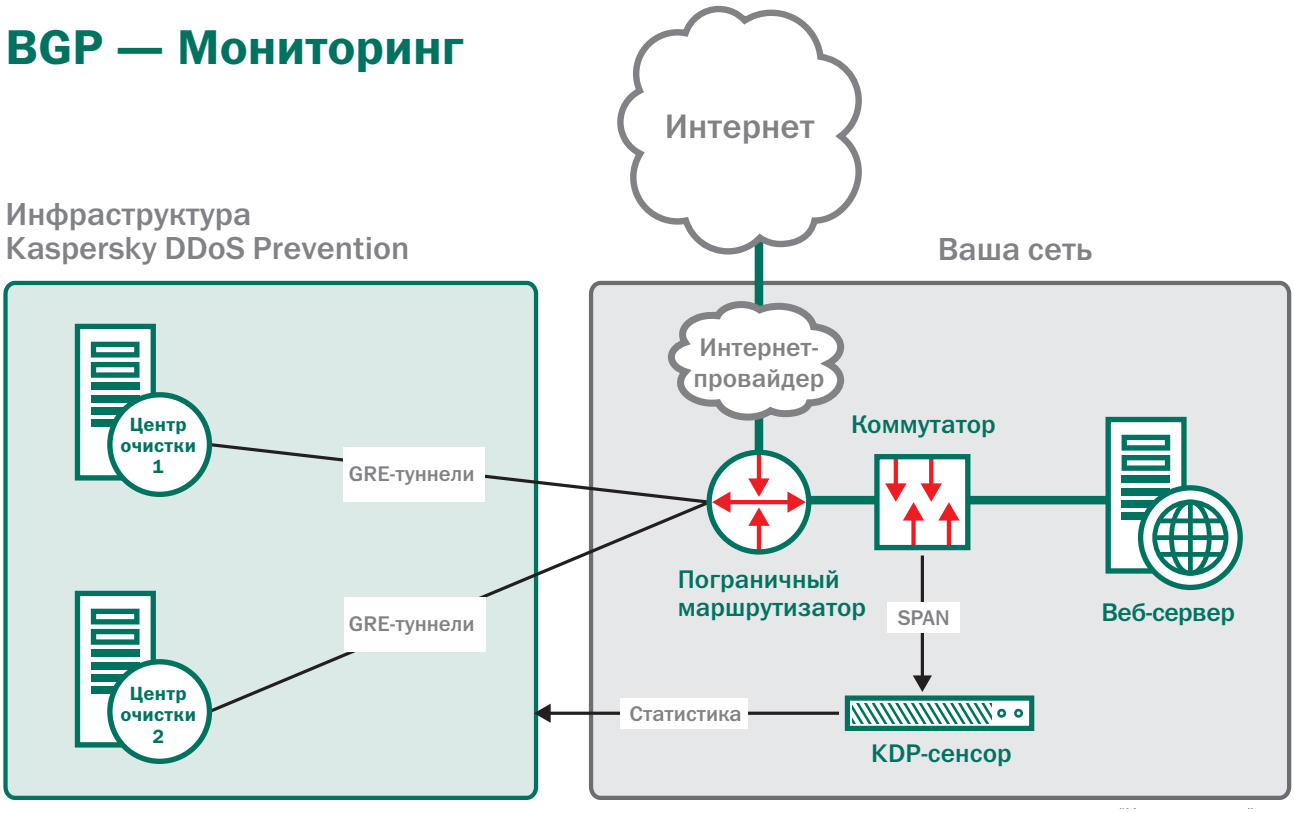
В целом в случае атаки перенаправление трафика посредством BGP происходит быстрее, поэтому для большинства компаний BGP является предпочтительным методом.

# КАК РАБОТАЕТ ПЕРЕНАПРАВЛЕНИЕ ПОСРЕДСТВОМ BGP

## МОНИТОРИНГ

В режиме мониторинга весь трафик направляется напрямую на ваши корпоративные ресурсы. Ваши маршрутизаторы и наши BGP-маршрутизаторы регулярно обмениваются информацией о статусе соединения, поддерживая виртуальные GRE-туннели в рабочем (активном) состоянии. Благодаря этому центры очистки Kaspersky DDoS Prevention могут принять перенаправленный трафик, как только возникнет такая необходимость.

### BGP — Мониторинг

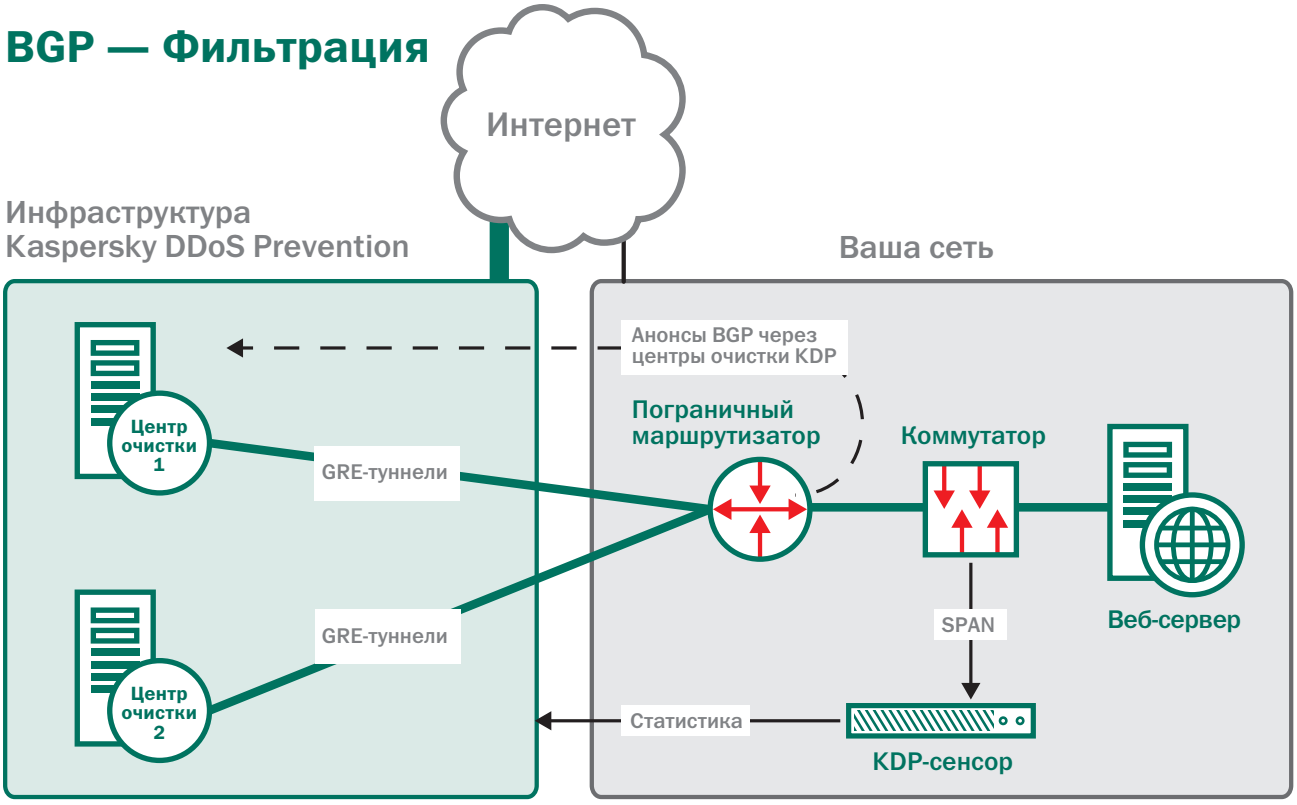



## ВО ВРЕМЯ АТАКИ

Когда сенсор «Лаборатории Касперского» детектирует аномалию в трафике, а специалисты «Лаборатории Касперского» подтверждают факт атаки, вы можете перенаправить весь свой трафик на центры очистки Kaspersky DDoS Prevention.

Во время атаки сенсор «Лаборатории Касперского» продолжает собирать информацию и отправлять ее для анализа на облачные серверы системы Kaspersky DDoS Prevention.

## BGP — Фильтрация




## ПОСЛЕ АТАКИ

После завершения атаки трафик снова направляется напрямую на ваши корпоративные ресурсы. Сенсор продолжает собирать данные о трафике и передавать их на наши облачные серверы для постоянного уточнения профилей, характерных для вашего обычного трафика.

Виртуальные туннели продолжают работать; происходит обмен данными о статусе соединения между вашими маршрутизаторами и маршрутизаторами «Лаборатории Касперского». Это позволяет обеспечить немедленное реагирование системы Kaspersky DDoS Prevention в том случае, если начнется новая атака и вы снова примете решение перенаправить трафик на наши центры очистки.

Кроме того, по завершении атаки эксперты «Лаборатории Касперского» предоставят вам ее детальный анализ с подробным описанием:

- что произошло во время атаки;
- сколько времени длилась атака;
- как решение Kaspersky DDoS Prevention справилось с атакой.

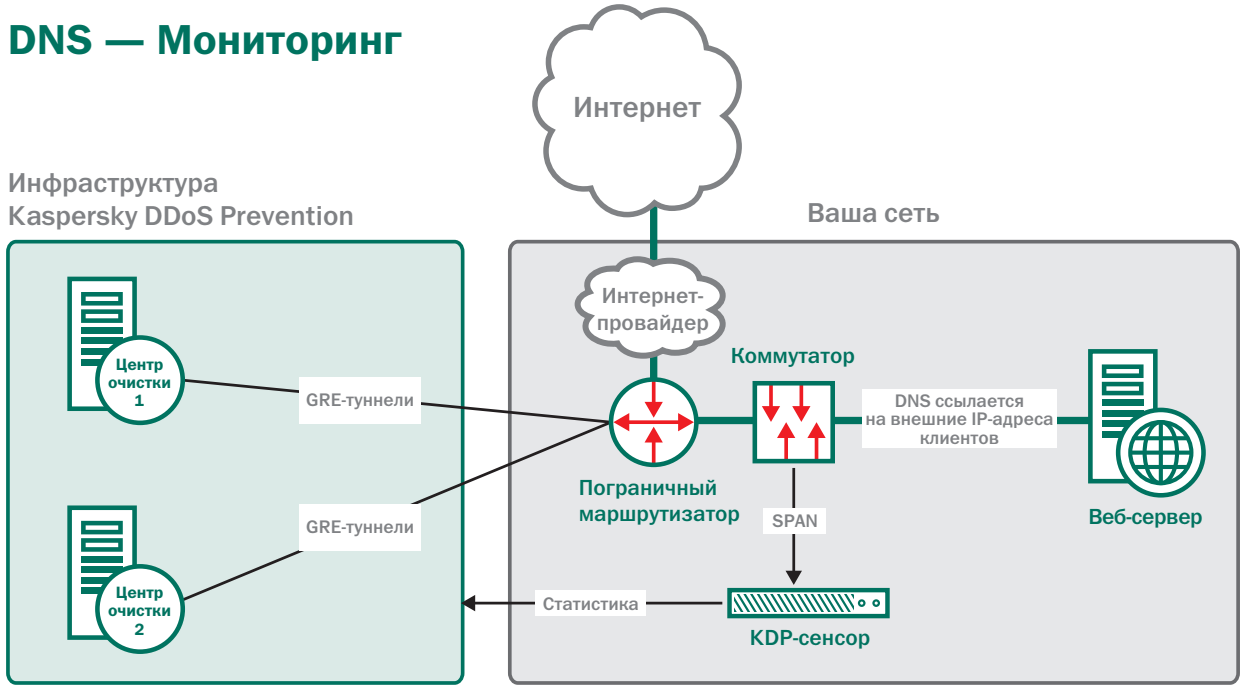
# КАК РАБОТАЕТ ПЕРЕНАПРАВЛЕНИЕ ПОСРЕДСТВОМ DNS

## МОНИТОРИНГ

Во время первоначальной настройки «Лаборатория Касперского» выделяет один из пулов IP-адресов системы Kaspersky DDoS Prevention под ваши корпоративные ресурсы. Эти адреса будут использоваться в случае атаки.

В режиме мониторинга весь трафик направляется напрямую на ваши корпоративные ресурсы по их обычным IP-адресам. Ваши маршрутизаторы и маршрутизаторы «Лаборатории Касперского» регулярно обмениваются информацией о статусе соединения, поддерживая виртуальные GRE-туннели в рабочем (активном) состоянии.

Благодаря этому центры очистки Kaspersky DDoS Prevention могут принять перенаправленный трафик, как только возникнет такая необходимость.

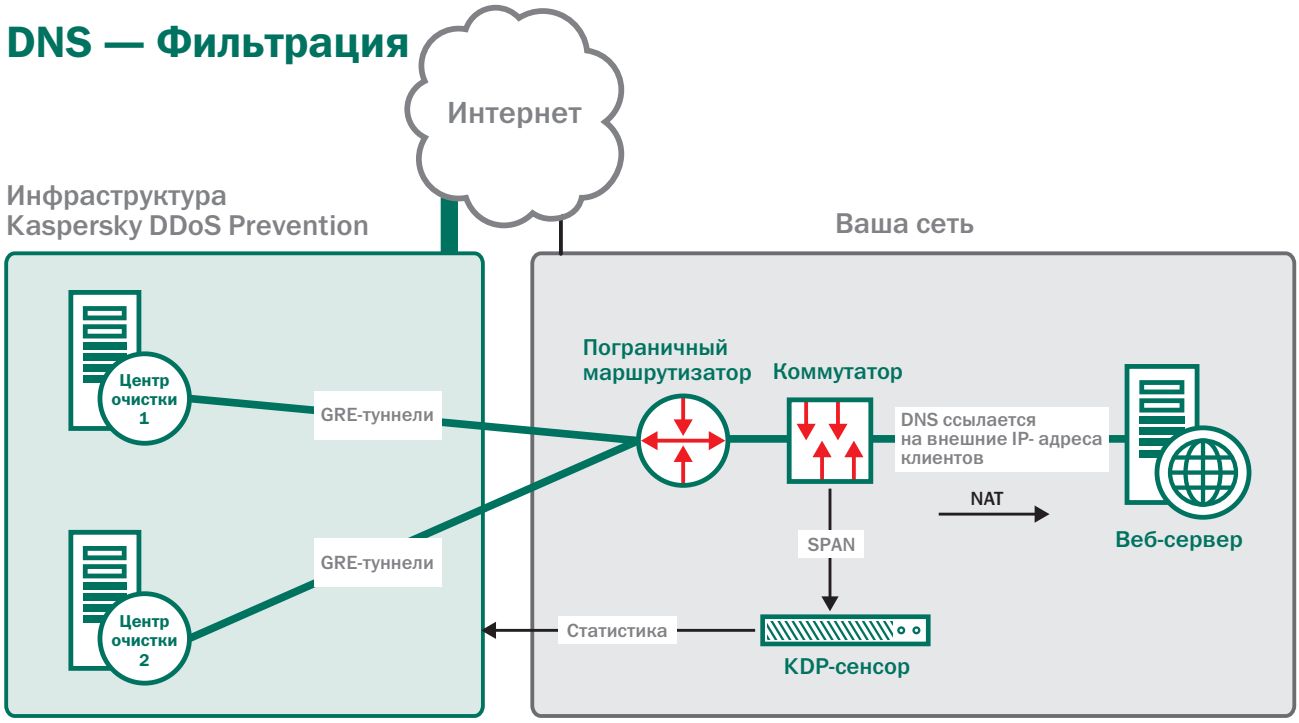



## ВО ВРЕМЯ АТАКИ

Когда сенсор «Лаборатории Касперского» детектирует аномалию в трафике, а специалисты «Лаборатории Касперского» подтверждают факт атаки, вы просто меняете IP-адрес своего ресурса в DNS-записи. В результате ваши корпоративные ресурсы используют IP-адрес системы Kaspersky DDoS Prevention, выделенный для вас во время первоначальной настройки. В то же время, поскольку злоумышленники могут атаковать непосредственно IP-адрес, интернет-провайдер должен заблокировать весь трафик, идущий на ваш обычный IP-адрес, за исключением коммуникаций с инфраструктурой системы Kaspersky DDoS Prevention.

После того как вы меняете свой IP-адрес, весь трафик перенаправляется на центры очистки «Лаборатории Касперского». Затем «чистый» трафик доставляется обратно на ваши ресурсы из центров очистки через виртуальные GRE-туннели.

## DNS — Фильтрация




## ПОСЛЕ АТАКИ

После завершения атаки вы можете разблокировать свои обычные IP-адреса и изменить DNS-запись, чтобы трафик снова шел непосредственно на ваши корпоративные ресурсы.

Сенсор «Лаборатории Касперского» продолжает собирать данные о трафике и передавать их на облачные серверы Kaspersky DDoS Prevention. Это позволяет нам постоянно уточнять профили, характерные для вашего обычного трафика.

Также продолжается работа виртуальных туннелей и обмен информацией о статусе соединения между вашими маршрутизаторами и маршрутизаторами «Лаборатории Касперского». Это позволяет обеспечить немедленное реагирование системы Kaspersky DDoS Prevention в том случае, если начнется новая атака и вы снова примете решение перенаправить трафик на наши центры очистки.

Кроме того, по завершении атаки эксперты «Лаборатории Касперского» предоставят вам ее детальный анализ с подробным описанием:

- что произошло во время атаки;
- сколько времени длилась атака;
- как решение Kaspersky DDoS Prevention справилось с атакой.

# ИССЛЕДОВАНИЕ УГРОЗ ДЛЯ ЕЩЕ БОЛЕЕ ЭФФЕКТИВНОЙ ЗАЩИТЫ

Система Kaspersky DDoS Prevention включает уникальный компонент, с которым не могут конкурировать защитные решения других производителей.

«Лаборатория Касперского» обладает широчайшей экспертизой как в области DDoS-атак, так и в сфере вредоносного ПО. Ни один другой разработчик защитных решений не может похвастаться таким квалифицированным штатом и настолько крупными подразделениями, занимающимися исследованиями в области IT-безопасности, а также соответствующей инфраструктурой.

Наши эксперты постоянно анализируют ландшафт угроз, чтобы быть в курсе актуальных тенденций в этой области и предоставлять клиентам «Лаборатории Касперского» максимально эффективную защиту. При этом DDoS-угрозам уделяется особое внимание. Это позволяет обеспечить раннее обнаружение DDoS-атак и предоставить вашему бизнесу все преимущества оперативной защиты.

Благодаря уникальному сочетанию постоянного мониторинга трафика и статистической обработки собранных данных с поведенческим анализом и экспертными исследованиями DDoS-атак наши клиенты получают наиболее эффективное решение для защиты от данного вида угроз.

Twitter.com/
Kaspersky_ru

www.facebook.com/
KasperskyLabRussia

www.youtube.com/user/
KasperskyChannelRU

ЗАО «Лаборатория Касперского»,
Россия, Москва www.kaspersky.ru

Всё о безопасности в
интернете: www.securelist.ru

Узнать больше о Kaspersky DDoS Prevention:
www.kaspersky.ru/DDoS-prevention



KASPERSKY lab