kaspersky

Обзор Kaspersky DDoS Protection

kaspersky

Оглавление

kaspersky

Что такое Kaspersky DDoS Protection

Kaspersky DDoS Protection – специализированная система, покрывающая все возможные решения по внедрению защиты от DDoS-атак, а также решения по защите от несанкционированной автоматизированной активности (защита от ботов), взлома веб-ресурса (WAF) и ускорению работы веб-сайтов (CDN).

Решение Kaspersky DDoS Protection состоит из трех основных компонентов:

- Инфраструктура обнаружения атак, которая собирает статистические данные и анализирует поведение трафика.
- Инфраструктура фильтрации атак, которая представлена Центрами очистки и справляется с атаками любого типа и объема.
- Служба технической поддержки, которая обеспечивает круглосуточный мониторинг и выполнение соглашения SLA, а также от которой зависит качество обнаружения и противодействия новым угрозам.

Инфраструктурные составляющие решения могут быть вынесены за пределы облачной инфраструктуры Kaspersky DDoS Protection на площадку клиента.

Такое устройство позволяет Kaspersky DDoS Protection отвечать любым требованиям по развертыванию решения и максимально гибко подходить к защите инфраструктуры Клиента.

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

kaspersky

Устройство Центров очистки

Каждый Центр очистки может быть разделен на несколько компонентов:

- Сетевое оборудование, осуществляющее коммутацию компонентов Центров очистки и маршрутизацию трафика в интернет. В Kaspersky DDoS Protection используется вендорское оборудование операторского класса. Все остальные компоненты системы – собственная разработка.
- Фильтрующие сервера, на которых происходит анализ и блокировка вредоносного трафика.
- Проксирующие сервера, которые используются для анализа и блокировки вредоносного трафика по протоколу HTTPS.
- Сервера, которые используются для сбора статистики о трафике и обнаружения атак.
- API и веб-сервера, которые позволяют управлять конфигурациями и отображать статистическую информацию о трафике.

Все компоненты Центров очистки могут быть линейно масштабированы при росте нагрузки.

Отказоустойчивость

Отказоустойчивость облачной инфраструктуры Kaspersky DDoS Protection обеспечивается благодаря архитектуре решения, представленной двумя независимыми Центрами очистки: основным и резервным. Центры очистки соединены между собой в отказоустойчивый кластер.

Под независимостью Центров очистки подразумевается отсутствие любой общей инфраструктуры: в России Центры очистки находятся на севере и юге Москвы, в Европе они расположены в разных городах – Франкфурте и Амстердаме.

Связность с интернетом дублируется тремя и более Tier-1 операторами, при этом маршруты от клиента к Центрам очистки не пересекаются с маршрутами от Центров очистки к клиенту. Каждый инфраструктурный элемент в свою очередь способен обработать 100% трафика второго Центра очистки из кластера.

Локальные и клиентские Центры очистки

На площадке клиента могут быть развернуты локальные Центры очистки. Такие Центры очистки не обладают большой емкостью из экономических соображений, поэтому если мощность атаки превышает их пропускную способность, трафик перенаправляется на сетевую инфраструктуру Kaspersky DDoS Protection, чтобы не допустить перегрузки сети клиента и локальных Центров очистки.

Установка Центра очистки в инфраструктуре клиента целесообразна при выполнении нескольких условий:

- Клиент маршрутизирует трафик в интернет по протоколу BGP и может управлять маршрутными таблицами.
- Клиент имеет возможность применять FlowSpec-правила по протоколу BGP на сети вышестоящего провайдера.

- Наличие круглосуточной дежурной смены или передача управления сетью в Kaspersky DDoS Protection для оперативного реагирования.

Технологии обнаружения DDoS-атак

Инструменты обнаружения атак

Умное обнаружение атак

Специалисты Kaspersky DDoS Protection собирают и анализируют данные о трафике из многих источников, благодаря чему удается прорабатывать превентивные меры безопасности и обеспечивать минимальное количество ложных срабатываний системы.

Сенсор

Основное назначение Сенсора – получение информации о трафике и преобразование ее в статистические данные.

Также Сенсором выполняется глубокая проверка пакетов для обнаружения сложных HTTP-атак, анализ системного журнала сервера без раскрытия закрытого ключа для обнаружения атак на основе HTTPS и анализ трафика для обнаружения атак на уровне L7, запущенных ботнетами.

Способы обнаружения атак

Система Kaspersky DDoS Protection анализирует более 200 параметров трафика для обнаружения атак.

Обнаружение объемных атак

Чтобы обнаружить объемную атаку, Kaspersky DDoS Protection полагается на статистику трафика, которая показывает аномалии для таких параметров, как входящий UDP-трафик в пакетах в секунду, количество IP-адресов в секунду и т.д.

Обнаружение атак SYN flood

Атаки SYN flood в основном выявляются с помощью анализа статистики по таким параметрам, как входящий TCP-трафик в пакетах в секунду, рейтинг SYN, входящий трафик в пакетах и т.д.

Обнаружение атак HTTP/HTTPS

Обнаружение HTTP-атак требует комплексного подхода. Простые атаки, такие как HTTP flood, могут быть легко обнаружены с помощью анализа статистики по таким параметрам, как входящий трафик в пакетах, количество HTTP запросов в секунду, количество IP-адресов в секунду и т.д.

Сложные атаки, имитирующие поведение пользователей, требуют более продвинутых инструментов. Для успешного отражения таких атак Kaspersky DDoS Protection использует технологию Deep Packet Inspection, поведенческий анализ и умное обнаружение атак.

kaspersky

Технологии фильтрации DDoS-атак

Решение для защиты от DDoS-атак полностью прозрачно для конечных пользователей и служб. В целях фильтрации Kaspersky DDoS Protection использует только фоновые инструменты, которые не мешают пользователю. Kaspersky DDoS Protection имеет инструменты многоуровневой фильтрации, расположенные на пути от магистрали провайдера до Центра очистки.

FlowSpec

Kaspersky DDoS Protection использует подход, при котором все атаки на основе UDP нейтрализуются внутри облака провайдера. Благодаря технологическому партнерству с Tier-1 провайдерами, Kaspersky DDoS Protection имеет уникальную возможность отбрасывать весь вредоносный UDP-трафик на границе сети провайдера автоматически, генерируя FlowSpec-правила блокировки по протоколу BGP, и, тем самым, сохранять свои собственные канальные ресурсы, а также ресурсы клиента.

Такой подход позволяет заявлять, что объем UDP-атак, отражаемых Kaspersky DDoS Protection, равен свободным емкостям подключённых сетей провайдеров. На текущий момент это более 10 Тб/с.

Фильтрация трафика без раскрытия сертификата

Kaspersky DDoS Protection обеспечивает защиту SSL/TLS без раскрытия закрытого ключа шифрования.

Для повышения уровня обнаружения аномалий для протокола HTTPS клиент передает расшифрованную версию трафика SSL/TLS или Syslog с веб-сервера защищаемого ресурса на Сенсор.

Защита DNS-серверов

Kaspersky DDoS Protection предоставляет функцию защиты DNS-сервера. Защита реализована в виде отдельного модуля со следующими функциональными возможностями:

- проверка полезной нагрузки на уровне L7;
- кэширование ответов защищаемого сервера;
- редактирование списков разрешенных и запрещенных IP-адресов и доменных имен;
- установка предельного значения для среднего количества запросов, которые могут быть направлены к серверу за секунду.

kaspersky

Организационная структура

Команда Kaspersky DDoS Protection включает в себя три группы специалистов.

Группа аварийного реагирования

Одним из ключевых преимуществ Kaspersky DDoS Protection является наличие дежурной смены, состоящей из специалистов высокой квалификации. Эта группа следит за процессом фильтрации трафика, контролирует применение правил фильтрации и реагирует на стратегию киберпреступника.

Группа исследования DDoS

Группа исследования DDoS анализирует тренды в сфере киберпреступности и регулярно обновляет базы данных ботнетов. Это позволяет получать актуальные данные о текущей ситуации в мире цифровой преступности и прогнозировать развитие DDoS-угроз в будущем.

Группа внедрения и поддержки решения

Системные инженеры, которые внедряют и поддерживают решение Kaspersky DDoS Protection для клиентов.

kaspersky

Взаимодействие с Kaspersky DDoS Protection

Клиентский портал

Kaspersky DDoS Protection предоставляет заказчикам доступ к Клиентскому порталу, где конечный пользователь имеет следующие возможности:

- проверка состояния защиты;
- отслеживание аномалий и DDoS-атак;
- оценка параметров аномалий и атак;
- изменение списков разрешенных и запрещенных IP-адресов.

API

API позволяет автоматизировать операции мониторинга, обнаружения и управления фильтрацией трафика.

Отчеты о DDoS-атаках

После каждой DDoS-атаки клиент получает отчет, который включает в себя хронологию атаки, детальное описание атаки, объяснение параметров атаки, ее оценку и заключение.

Служба технической поддержки

Служба технической поддержки Kaspersky DDoS Protection доступна круглосуточно по электронной почте и телефону. Для проверки статуса заявок можно использовать Telegram-бота.

kaspersky

Подходы к внедрению решения

Все существующие решения по защите от DDoS-атак, независимо от их функциональной наполненности, можно поделить на четыре варианта внедрения. Kaspersky DDoS Protection поддерживает все эти подходы:

- **Device-based Mitigation** – атакующий трафик целиком попадает в сеть клиента, где он фильтруется на локальном устройстве. Основной минус такого подхода – ограниченность емкости сети клиента и устройств, фильтрующих атакующий трафик. Такой вариант подходит клиентам с корпоративными сетями, сравнимыми с сетями операторов связи.
- **Cloud-based Protection** – сеть клиента располагается за пределами сети провайдера защиты, принимающей на себя все последствия атак и пропускающей к сети клиента только легитимный трафик. Это накладывает особые требования на сети провайдеров защиты – они должны обладать достаточным запасом емкости, чтобы выдерживать множество одновременных атак на всех клиентов под защитой. Также необходимо доверять провайдеру защиты, его процессам обеспечения безопасности и используемому ПО, поскольку при защите в облаке зачастую требуется передача сертификатов безопасности доменов на его сторону.
- **Cloud-based Protection & Local Detection** – вариант внедрения, который аналогичен варианту **Cloud-based Protection**, но включает в себя использование локального Сенсора на стороне клиента, который собирает статистические данные о трафике и направляет их провайдеру защиты. Использование Сенсора позволяет расширить уровень доверия к провайдеру защиты, поскольку не требует передачи сертификатов за пределы площадки клиента.
- **Hybrid Protection** – устройство защиты на стороне клиента работает в связке с комплексом вышестоящего провайдера, который включается в работу для отражения объемных атак, чтобы не допустить перегрузки сети клиента. Основной недостаток такого решения – зависимость от вендора решения. Но этот подход особенно эффективен при необходимости защиты на уровне L7 без передачи ключей шифрования на сторону провайдера защиты.

kaspersky

www.kaspersky.com/
www.securelist.com