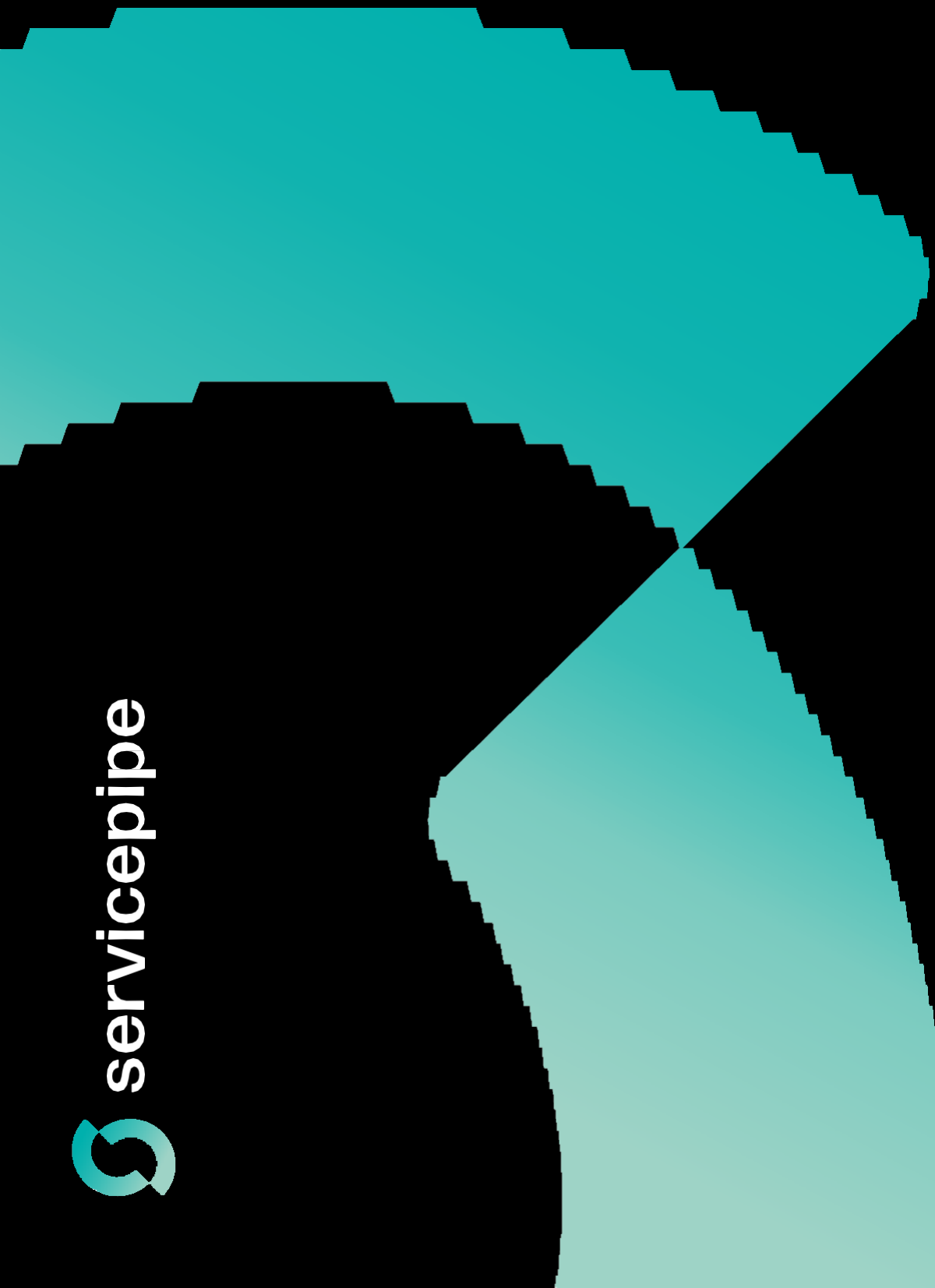
Web DDoS & Bot protection

Защита веб-сайтов и API мобильных приложений
от продвинутых ботов и DDoS-атак



servicepipe

О Servicepipe

Servicepipe работает на рынке защиты интернет-ресурсов более 6 лет. На этапе становления компания фокусировалась на предоставлении услуг защиты провайдерам связи и дата-центрам. Эти сервисы строились на базе оборудования ведущих производителей Arbor Networks и F5 Networks, а в дальнейшем их число пополнили продукты российских компаний БИФИТ Митигатор, и Inoventica.

Работа с решениями разных производителей дала опыт интеграции и создания комплексных сервисов, знание сильных и слабых сторон имеющихся на рынке средств защиты, их возможностей и ограничений. Мы осознали, что идеальных продуктов нет, по крайней мере пока, поэтому приняли решение начать разработку собственных продуктов и сервисов на их базе.

Сейчас в команде Servicepipe более 50 специалистов в области построения и эксплуатации сетей передачи данных, разработки высоконагруженных решений, Data science, DevOps и front-end разработчиков.

Мы разрабатываем решения, обеспечивающие доступность и безопасность онлайн-ресурсов и оказываем услуги на базе собственной распределённой инфраструктуры. Услуги Servicepipe помогают очистить трафик клиентов и защитить их интернет-активы от внешних угроз различного типа – DDoS-атак, нежелательных ботов, попыток взлома и целевых атак.

Услуги предоставляются как в виде полностью облачных сервисов, так и по гибридной схеме, с установкой компонент решения внутри ИТ-инфраструктуры клиентов.

Помимо этого, Servicepipe проводит аудиты защищенности, нагрузочное и стресс-тестирование, которые помогают заранее выявить актуальные уязвимости в сетевом периметре и приложениях, проверить работу имеющихся средств защиты, а также проверить и подготовить приложения к условиям высоких нагрузок.

Нашим продуктам доверяют

РБК

точка
банк для предпринимателей

2GIS

Почта Банк

PONY EXPRESS

RUNNet

самокат

ЕАПТЕКА

X5

okko

tutu

ДОМ РФ

Источник внешних угроз

Бот – это программа или алгоритм, которая автоматически выполняет заданные при её создании действия. Такие алгоритмы нужны для выполнения рутинной работы или тогда, когда требуется мгновенная реакция на внешние условия, которую не сможет обеспечить живой человек.

Хорошие боты широко применяются для разных задач. Без них невозможно обеспечить работу ключевых систем в Интернет, например обновление поисковой выдачи, а также автоматизировать большинство бизнес-процессов. Но автоматизацию широко применяют и злоумышленники, которые объединяют ботов в подконтрольные сети —ботнеты.

Ботнеты состоят из плохих ботов, работающих на различных взломанных устройствах подключенных к Интернет. Проблема ботнетов постоянно усугубляется растущим количеством недорогих устройств Интернета вещей (IoT – Internet of things). Значительная часть таких устройств имеет слабую защиту и уязвима к неавторизованному доступу, что сильно упрощает злоумышленникам задачу создания масштабных ботнетов, состоящих из десятков, сотен тысяч и миллионов элементов. Их целями могут быть как отдельные веб-приложения или API, так и вся ИТ-инфраструктура компаний, крупных операторов связи и дата-центров.

Самые распространенные примеры вредоносных действий ботов это:

- DoS- и DDoS-атаки;
- Подбор и кража логинов / паролей;
- Сбор контактной информации для спам-рассылок;
- Неавторизованное копирование информации или контента;
- Сканирование и эксплуатация уязвимостей

Привычные способы защиты

CAPTCHA

Самые распространенный способ борьбы с ботами в веб-приложениях – установка CAPTCHA (Completely Automated Public Turning test to tell Computer and Humans Apart), набора символов или картинок, сформированных специальным способом, которые может распознать только человек. CATPCHA является одной из форм теста Тьюринга и используется для различия машины и человека.

К сожалению, этот способ помогает в борьбе только с простыми ботами и при этом имеет ряд существенных недостатков. Многие предпочитают не выполнять задания CAPTCHA, угадывая трудноразличимый набор букв и цифр, пешеходные переходы, автомобили или светофоры на картинках и уходят на веб-сайты конкурентов. По данным исследований CAPTCHA снижает конверсию в целевые действия на в среднем на 15%.

Кроме этого, CAPTCHA невозможно использовать при защите API мобильных приложений, поскольку CAPTCHA работает только для браузеров, а мобильные приложения не могут ее отобразить.

Репутационные базы и лимиты с привязкой к IP-адресам

Другой способ борьбы с ботами – установка ограничений частоты выполнения действий, ведение черных списков, а также баз репутации, в которых используется привязка к IP-адресам источников трафика. Однако, сегодня большинство людей для работы с веб-сайтами используют мобильные устройства, доступ в Интернет для которых предоставляют сотовые операторы или Wi-Fi сети. Здесь за одним IP-адресом могут находиться десятки пассажиров вагона метрополитена, сотни пользователей Wi-Fi сети аэропорта или тысячи абонентов оператора сотовой связи. Любые блокировки и ограничения с привязкой к IP-адресам неизбежно приведут к блокировкам реальных пользователей, потере аудитории и, как следствие, прямым убыткам. Кроме этого, ложные блокировки ухудшают клиентский опыт и лояльность, последствием которых будут косвенные финансовые потери, часто превышающие прямые убытки.

Поведенческий анализ

Особую сложность для блокировки представляют запросы продвинутых ботов. Их алгоритмы способны взаимодействовать с приложением как человек, выполняя переходы между страницами и отправляя/получая данные через достаточное для прочтения живым человеком время. Во многих случаях они способны проходить некоторые типы CAPTCHA.

Цель действий таких ботов – это атаки на бизнес-логику приложений и нормальное течение бизнес-процессов. Самые простые примеры такого рода атак, это создание потоков:

- Ложных заявок в формы сайта;
- Фейковых заказов на доставку товаров;
- Предзаказов товаров в корзине, которые не будут выкуплены;
- Паразитной нагрузки на колл-центр запросами обратных звонков;
- Запросов смс-кодов для авторизации.

Поведенческий анализ (Behavioral analysis), который все чаще применяют в решениях для защиты от продвинутых угроз, анализирует последовательность действий пользователей и сравнивает её с заданной легитимной моделью поведения. Это означает, что для анализа и сравнения такая защита должна пропустить некоторое количество запросов.

Запросы продвинутого бота, последовательность действий которого мало отличима от настоящего пользователя, будут выявлены не сразу. Даже в случае успешной блокировки у бота будет возможность выполнить значительное количество целевых действий. В подобных случаях поведенческий анализ будет малоэффективен, так как злоумышленники смогут достичь поставленных целей.

WAF

Решения класса WAF (Web Application Firewall или межсетевой экран уровня приложения) – это специализированное средство защиты от внешних угроз для веб-приложений.

Такие решения предназначены для предотвращения попыток использования уязвимостей или недоработок в коде, в результате использования которых, например, можно получить несанкционированный доступ к закрытым данным.

В основе своей работы WAF опирается на статически заданные шаблоны «плохих» запросов (сигнатуры) и дополнительно может использовать указанные выше методы обнаружения вредоносных запросов – опциональную CAPTCHA, рейт-лимиты, репутационные базы IP-адресов и поведенческий анализ.

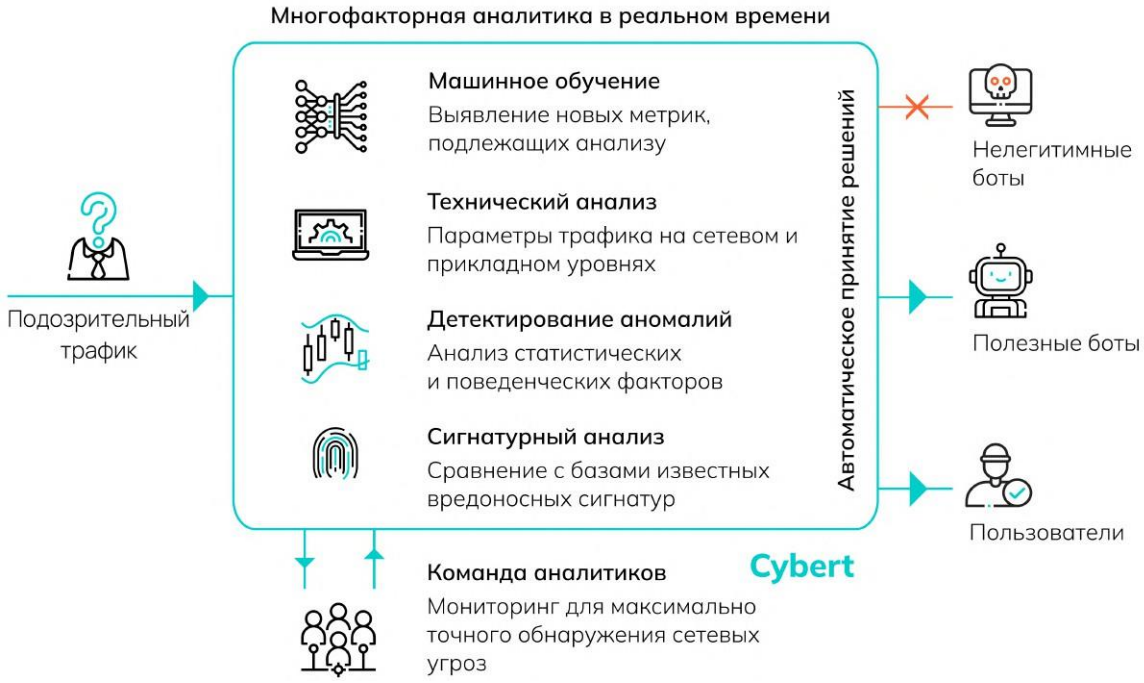
Для фильтрации запросов, которые могут представлять угрозу, содержимое запросов «на лету» анализируется на предмет совпадения с базой известных вредоносных сигнатур. Такой анализ позволяет выявить даже единичные атакующие запросы, но требует больших вычислительных ресурсов. Именно по причине не самой высокой производительности при высоких нагрузках, WAF не рекомендуется устанавливать в качестве основного средства защиты, в противном случае стоимость инсталляции с должным уровнем запаса производительности будет очень велика.

Описание технологии Servicepipe Cybert

В технологии определения ботов Servicepipe в отличие от других решений, которые присутствуют на рынке, используется совокупность факторов, которые можно описать следующими категориями:

- Технический анализ;
- Статистический и поведенческий анализ;
- Сигнатурный анализ.

При этом статистические факторы не являются основными, а сигнатурные – генерируются автоматически и «на лету», т. е. не являются статической частью конфигурации защиты. Кроме этого, для анализа совокупности данных применяется машинное обучение, а для улучшения точности применяется дополнительный контроль выделенной команды опытных аналитиков.



Процесс принятия решения можно представить следующим образом:

1. Трафик, поступающий на ресурс, постоянно анализируется на предмет обнаружения всевозможных статистических аномалий;
2. При получении очередного запроса проводится базовый технический анализ пославшего его клиента/пользователя;
3. Если запрос от данного клиента является не первым в наблюдаемом интервале времени, то вычисляются поведенческие факторы клиента/пользователя;
4. Запрос сопоставляется с сигнатурами, актуальными для ресурса в данный момент, при этом может учитываться как совпадение, так и «близость»;
5. Полученная информация комбинируется в вектор факторов, на основе которого и вычисляется легитимность запроса.

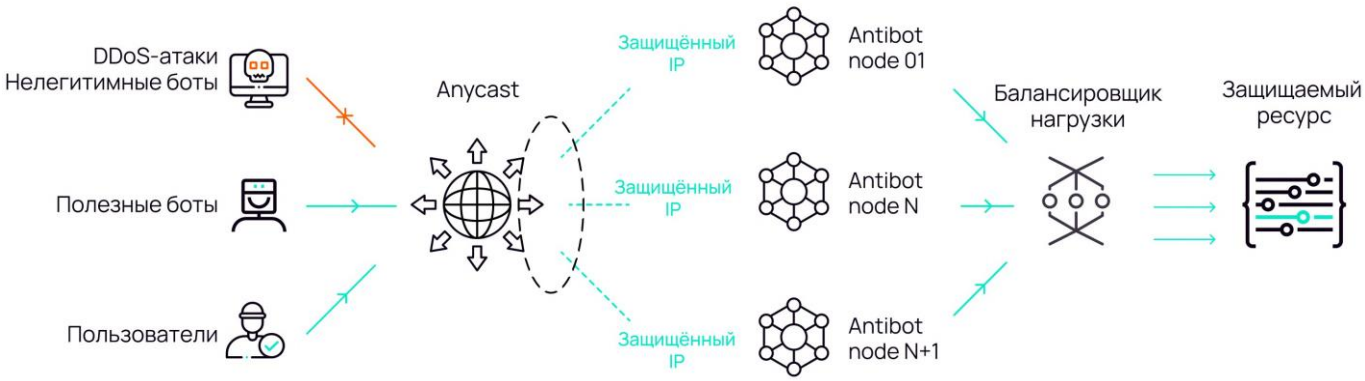
Процесс принятия решения оптимизирован под высокие нагрузки – применяется многоуровневое кеширование, а принятие негативного решения происходит как можно раньше для фильтрации основной части паразитной нагрузки массовой атаки.

Сомнительный пользователь может быть дополнительно проверен с помощью JavaScript-сценария, который протестирует стек JS браузера и соответствие другим характеристикам.

Способы интеграции

Cloud protection

Стандартным методом интеграции является подключение к платформе Servicepipe через проксирование трафика защищаемого приложения.



1. Выделенный для подключения защищенный IP-адрес постоянно анонсируется по Anycast в сеть Интернет одновременно со всех центров очистки. Таким образом, пользователь обслуживается на ближайшем к нему оборудовании;
2. В центре очистки каждый запрос распределяется на одну из нод фильтрации (реальный сервер). Сервер принимает соединение, получает запрос, проводит анализ и принимает решение;
3. В случае принятия решении о легитимности запроса сервер соединяется с клиентским сервером и отправляет (проксирует) запрос.

Соединение с клиентским сервером происходит через Интернет или по выделенному каналу. Реальные IP-адреса пользователей передаются с помощью proxy-protocol.

Это рекомендуемый метод подключения, при котором реакция на атаки происходит автоматически и позволяет мгновенно реагировать на поступающие нежелательные запросы.

Данный способ подключения позволяет защитить веб-приложение от:

- Сетевых DDoS-атак;
  - TCP / SYN / ACK / RST flood
  - UDP amplification
- Прикладных DDoS-атак;
  - HTTP(s) flood атак
  - Big & slow Layer 7 атак
- Нежелательных ботов и угроз из списка OWASP Automated Threats, включая низкочастотные и распределенные атаки на бизнес-логику с помощью продвинутых ботов, например:
  - Credential stuffing / cracking
  - CAPTCHA defeat
  - Scaping
  - Denial of inventory
  - Scalping
  - Card cracking / Carding
  - Vulnerability scanning и т.д.
- Целевых атак, включая угрозы OWASP Top 10, с помощью дополнительных средства WAF, развернутого на распределенной инфраструктуре Servicepipe:

Поддерживается все современные стандарты работы https, включая http/2 и websocket.

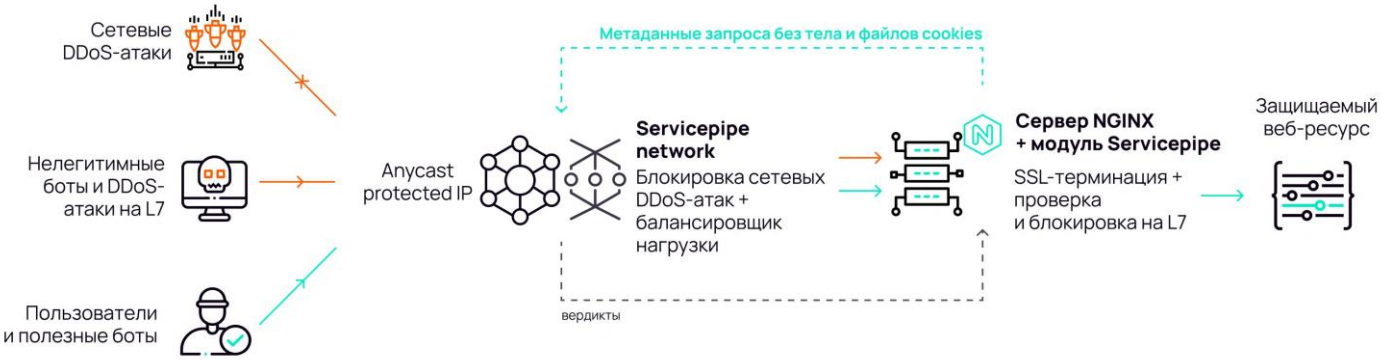
Дополнительно возможна оптимизация скорости работы приложения, распределенное кеширование и доставка статического контента приложений средствами CDN.

NGINX module

Продукт Servicepipe Bot Mitigation может быть развернут по гибридной схеме с использованием вычислительных мощностей клиента и предоставлен в виде модуля для веб-сервера NGINX.

Такой способ интеграции необходим, когда требуется исключить передачу SSL-сертификата для работы алгоритмов определения нежелательных ботов и встроить полноценную защиту в существующую ИТ-инфраструктуру.

В отличие от других решений, построенных на анализе журналов записей (логов) веб-сервера, на котором работает приложение, схема позволяет блокировать любые, даже единичные ботовые запросы до момента их обработки. Это исключает риск того, что приложение будет выведено из строя внезапной объемной атакой или запросы продвинутых ботов будут пропущены и достигнут своих целей.



1. Аналогично стандартной схеме, защищенный IP-адрес постоянно аносируется по Anycast в сеть Интернет одновременно со всех нод фильтрации, пользователь обслуживается на ближайшем к нему центре очистки;
2. В центре очистки производится технический анализ каждого поступающего соединения и фильтрация сетевых DDoS-атак;
3. В случае принятия решении о легитимности соединения сервер соединяется с клиентским сервером и отправляет (проксирует) трафик;
4. Сервер клиента с установленным SSL-сертификатом, принимает соединение и устанавливает https-сессию. Развёрнутый на нем модуль получает необходимые для анализа на прикладном уровне дополнительные данные о запросе и, в случае необходимости, направляет их на проверку в сеть Servicepipe. Получив решение, модуль выдает серверу директиву пропустить или заблокировать данный запрос.

Соединение с клиентским сервером происходит через Интернет или по выделенному каналу. Реальные IP-адреса пользователей передаются с помощью proxy-protocol.

Способ подключения позволяет защитить веб-приложение от:

- Сетевых DDoS-атак;
  - TCP / SYN / ACK / RST flood;
  - UDP amplification;
- Прикладных DDoS-атак;
  - HTTP(s) flood;
  - Big & slow Layer 7 атак;
- Нежелательных ботов и угроз из списка OWASP Automated Threats, включая низкочастотные и распределенные атаки на бизнес-логику с помощью продвинутых ботов.

Модуль может быть развернут без проксирования трафика через сеть Servicepipe. Это позволит сохранить под своим контролем и управлением сетевые маршруты, по которым к защищаемому ресурсу обращаются пользователи, однако, для отражения DDoS-атак потребует серьезного запаса емкости каналов доступа в Интернет и вычислительных ресурсов.

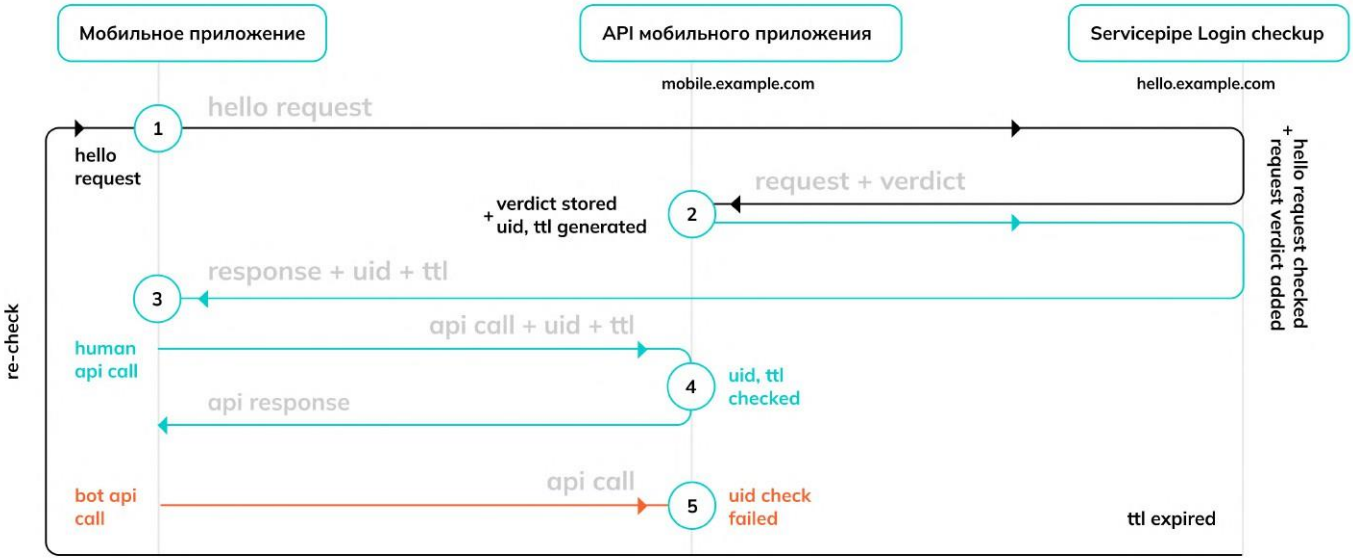
Login protection для API мобильных приложений

В том случае если первые два способа интеграции по каким-то причинам невозможны или требуется исключительно защита механизмов авторизации может быть реализована интеграция по схеме Login protect.

Механизм защиты реализуется с помощью проксирования части вызовов к API мобильного приложения через платформу Servicepipe, их проверки и обработки результатов проверки на backend мобильного приложения. Мобильное приложение работает с двумя IP-адресами или доменными именами - API мобильного приложения (mobile.example.com) и платформой проверки Servicepipe (hello.example.com).

Для работы интеграции требуется:

- механизм hello-request – при запуске мобильного приложения оно должно обратиться к API через систему проверки;
- механизм записи полученного по итогам проверки результата (request verdict), формирования уникального идентификатора/token (uid), времени действия (ttl) и проверки их валидности;



1. Мобильное приложение при запуске обращается к платформе Servicepipe (hello.example.com), где проводится необходимые проверки запроса и обогащение его информацией о легитимности (verdict). Запрос с добавленным заголовке verdict проксируется на API (mobile.example.com);
2. Полученный hello-запрос с доп. информацией (verdict) запоминается на backend, ему присваивается уникальный uid/token, а также задается параметр времени действия ttl.
3. В ответе на hello запрос в мобильное приложение возвращается token +ttl;
4. Все последующие запросы приложения к API осуществляются с добавленным ранее token. На стороне API (mobile.example.com) проверяется ttl, а по token определяется проверялась ли ранее данная https-сессия, а также результат проведенной ранее проверки данной сессии.
5. При отсутствии uid/token в запросе, истекшего ttl или в том случае, если результат ранее проведённой проверки говорит о нелегитимности сессии, запрос может быть заблокирован или обработан иным образом в рамках необходимой бизнес-логики.

Схема позволяет реализовать защиту от нежелательных ботов и угроз из списка OWASP Automated Threats, включая низкочастотные и распределенные атаки на бизнес-логику с помощью продвинутых ботов.

Login protection для веб-сайтов

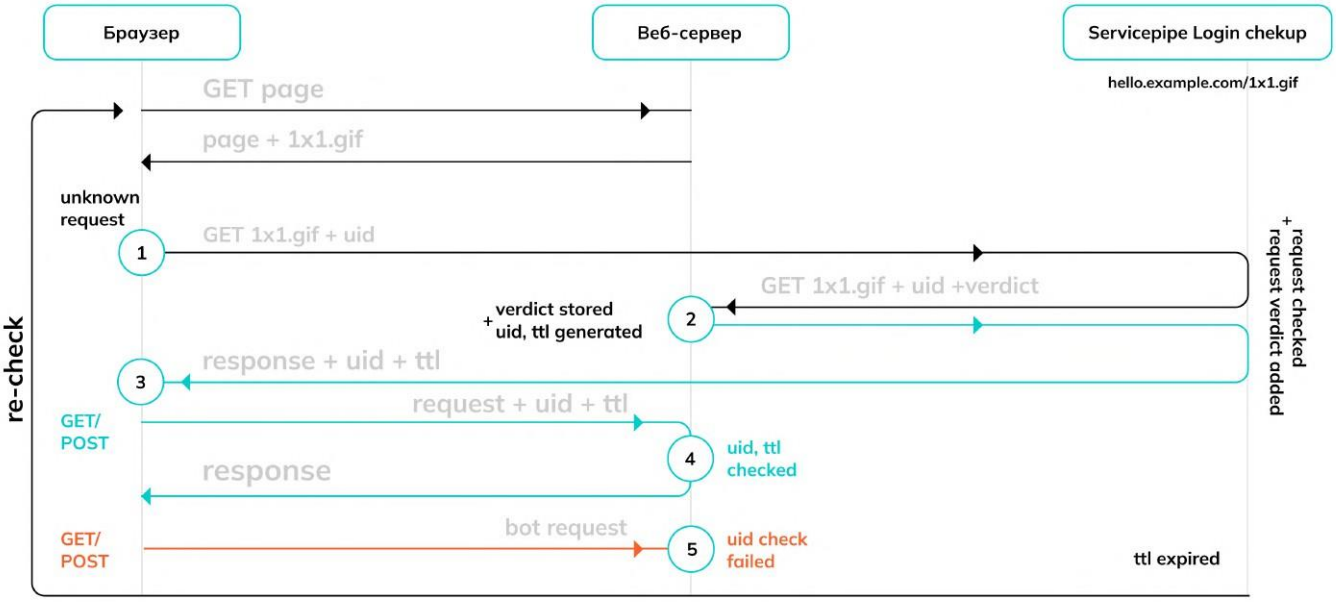
Для защиты отдельных страниц веб-сайтов может быть использована схема во многом аналогичная Login protect для API мобильных приложений.

Механизм защиты реализуется также с помощью проксирования запросов через платформу Servicepipe, их проверки и обработки результатов проверки на backend.

Для работы интеграции требуется:

Размещенный на нужных веб-страницах элемент, направляющий GET-запросы на платформу проверки Servicepipe (может использоваться js или любой существующий элемент страницы);

Механизм записи полученного по итогам проверки результата (request verdict), формирования уникального идентификатора/token (uid), времени действия (ttl) и проверки их валидности;



1. Браузер при загрузке страницы получает элемент и затем обращается к платформе Servicepipe (hello.example.com), где проводится необходимые проверки запроса и обогащение его информацией о легитимности (verdict). Запрос с добавленным заголовке verdict проксируется на веб-сервер;
2. Полученный запрос с доп. информацией (verdict) запоминается на backend, ему присваивается уникальный uid/token, а также задается параметр времени действия ttl.
3. В ответе на начальный запрос в браузер возвращается token + ttl;
4. Все последующие запросы осуществляются с добавленным ранее token. На стороне веб-сервера/ backend проверяется ttl, а по token определяется проверялась ли ранее данная https-сессия, а также результат проведенной ранее проверки данной сессии.
5. При отсутствии uid/token в запросе, истекшего ttl, а также если результат ранее проведённой проверки говорит о нелегитимности сессии запрос может быть заблокирован, перенаправлен на другую страницу или обработан любым иным образом в рамках необходимой бизнес-логики.

Обзор платформы

Возможности:

- Защита веб-приложений от любых DDoS-атак без блокировки источников по IP-адресам;
- Балансировка нагрузки;
- Пользовательские белые и черные списки;
- Поддержка IPv6, Websocket, HTTP 2.0;
- Защита HTTPS без раскрытия SSL и передачи логов с веб-сервера;

Дополнительно:

- Защита от нежелательных ботов – парсинга, подбора логинов/паролей и других угроз из списка OWASP Automated Threats;
- Защита от попыток взлома средствами Web Application Firewall;
- Кэширование и ускорение статики средствами CDN;
- SSL offload с получением, хранением и автопродлением сертификатов;
- Прямое подключение к платформе с помощью L2 или выделенных ОВ.

Характеристики:

- Собственная геораспределенная инфраструктура расположена в дата-центрах уровня не менее Tier3;
- Не мнее двух независимых апстримов с поддержкой flowspec на каждом узле;
- Полное резервирование компонентов, отсутствие единой точки отказа;

Преимущества:

Комплексная защита от любых автоматизированных угроз без потери пользователей;

Многофакторные методы анализа, современные математические модели и Machine learning с высокой точностью выявляют и мгновенно блокируют запросы ботов;

Подключение plug&play за 15 минут, не требует сложных настроек, периода обучения и накопления статистики;

Полноценная работа без изменений в коде и CAPTCHA (может быть включена опционально) не видна пользователям и не вмешивается в клиентский опыт;

Блокировки ботов без влияния на SEO за счет непрерывной поддержки обновляемого глобального белого списка хороших роботов (поиск, соц. сети и пр.);

API для управления и интеграции, гибкость настроек и режимов работы, поддержка PCI DSS Compliance;

Отказоустойчивая архитектура каждого центра очистки и платформы в целом обеспечивает высокую доступность защищаемых приложений;

Фильтрация паразитной нагрузки на приложение и ИТ-инфраструктуру оптимизирует TCO и повышает эффективность использования имеющихся ИТ-ресурсов.

Пример использования

Финтех, топ-50 банк РФ

Банк выстраивает свою работу вокруг онлайн-сервисов. Большинство вопросов клиент может решить через личный кабинет, не приезжая в офис. Авторизация пользователей в веб-приложении реализована по номеру мобильного телефона и вводу полученного на номер смс-кода.

В ноябре 2021 года банк столкнулся с резким ростом затрат на отправку авторизационных смс. Количество дополнительно отправленных сообщений достигало 30 000, а потери исчислялись сотнями тысяч рублей в сутки. Среди получателей были номера людей, не являющихся клиентами банка, а также абоненты зарубежных операторов связи. Часть людей, получивших сообщения, являлись клиентами банка, что вызвало их обеспокоенность и рост количества обращений в поддержку банка.

ИТ-специалисты банка выявили причину - ботовые запросы в отдельные методы приложения и API, отвечающие за отправку сообщений. Блокировка выявленных на первом этапе источников по IP-адресам и user-agent запросов не заброкировала атаку – злоумышленники адаптировали алгоритмы и паразитная активность вернулась вновь.

Для отражения атаки банк обратился к существующему поставщику сервисов защиты и оптимизации работы веб-приложений. Предложенный провайдером продукт тоже не смог отразить атаку, поскольку его работа была основана на статически заданных порогах срабатывания по количеству запросов в секунду, паразитные запросы успешно блокировались только в ночное время, при минимальном количестве пользовательского трафика. В дневное время запросы реальных клиентов блокировались вместе с ботами, что приводило к росту недовольства, жалобам и повышенной нагрузке на клиентскую поддержку. Банк принял решение протестировать продукт Servicepipe Bot Protection (антибот Cybert).

ИТ-специалисты банка приняли решение о всестороннем и поэтапном тестировании. На первом этапе работа сервиса была проверена без клиентского трафика. После этого – сервис был подключен в ночное время. Собранные за два ночных включения данные позволили аналитикам Servicepipe обучить платформу профилю трафика мобильного приложения банка. Кроме этого, для трафика, поступающего в личный кабинет с браузера, в конфигурации сервиса была активирована опциональная CAPTCHA, дающая возможность реальным клиентам, столкнувшимся с блокировкой, пройти тест и продолжить работу.

Сразу после полноценного включения атака была успешно отражена, при этом количество обращений в поддержку осталось в пределах стандартных значений.

За первые 5 дней проведения пилота было выявлено:

- 19,5 миллионов ботовых запросов, доля которых составила более 23% от общего количества трафика;
- 9,5 миллионов ботовых запросов были направлены на получение авторизационных смс в процессе регистрации нового пользователя;
- Целью 4,5 млн. запросов являлись попытки авторизации в личном кабинете, что может свидетельствовать об атаке типа credential stuffing;
- 15% ботовых запросов были сформированы продвинутыми ботами, поддерживающих стек браузера с моделью поведения близкой к реальному пользователю;
- Доля успешных прохождений опциональной CAPTCHA составила менее 0,003%;
- Снижение утилизации CPU/RAM/Disk в среднем составило 14%;

По итогам пилотный проект был признан успешным, а банк пополнил число клиентов Servicepipe. Планируем расширить сотрудничество, количество защищаемых приложений и используемых банком продукт