Приложение № 1.5.
к Договору

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ
«SberCloud Anti-DDoS», «SberCloud Anti-DDoS+WAF»

1. НАИМЕНОВАНИЕ УСЛУГ

1.1. Наименование Услуг: ***«SberCloud Anti-DDoS», «SberCloud Anti-DDoS+WAF»***.

1.2. Настоящий документ содержит описание состава и базовой функциональности Услуг, возможных сопутствующих и дополнительных опций Услуг, техническое описание Услуг, ограничений по предоставлению Услуг, описание порядка подключения, изменения и отключения Услуг и условий по предоставлению Услуг.

2. ИНФОРМАЦИЯ ОБ УСЛУГАХ

2.1. **Краткое описание Услуг**

2.1.1. ***«SberCloud Anti-DDoS»*** – услуга фильтрации трафика от DDoS-атак в целях обеспечения стабильности и бесперебойности работы размещаемых у Исполнителя сервисов[1] Заказчика, доступных по протоколам HTTP или HTTPS.

2.1.2. ***«SberCloud Anti-DDoS+WAF»*** – услуга фильтрации трафика от DDoS-атак в целях обеспечения стабильности и бесперебойности работы размещаемых у Исполнителя сервисов Заказчика, доступных по протоколам HTTP или HTTPS, расширенная опцией защиты указанных сервисов от полного спектра современных атак, направленных на эксплуатацию уязвимостей WEB-приложений (функцией WEB Application Firewall, WAF).

2.1.3. Услуги предоставляются в сотрудничестве с ООО «Эйч-эль-эль» (Qrator Labs, далее – Партнер).

2.1.4. Услуги предоставляются на базе облачного решения Партнера по защите от DDoS-атак и атак, направленных на эксплуатацию уязвимостей WEB-приложений (далее – облако Партнера).

2.2. **Базовая функциональность Услуг**

2.2.1. Базовая функциональность Услуги ***«SberCloud Anti-DDoS»*** включает:

- **Противодействие атакам класса «отказ в обслуживании» (Distributed denial of service), включая:**
  - DDoS-атаки, направленные на исчерпание канальной емкости;
  - DDoS-атаки на сетевую инфраструктуру;
  - DDoS-атаки транспортного уровня;
  - DDoS-атаки, основанные на протоколах SSL/TLS;
  - DDoS-атаки уровня приложений.

2.2.2. Базовая функциональность Услуги ***«SberCloud Anti-DDoS+WAF»*** включает:

- **Противодействие атакам класса «отказ в обслуживании» (Distributed denial of service), включая:**
  - DDoS-атаки, направленные на исчерпание канальной емкости;
  - DDoS-атаки на сетевую инфраструктуру;
  - DDoS-атаки транспортного уровня;

[1] Здесь и далее по тексту настоящего документа под сервисами Заказчика подразумеваются любые сервисы, доступные по протоколу HTTP или HTTPS, в том числе, но не ограничиваясь WEB-сайтами, Интернет-магазинами и прочими WEB-сервисами Заказчика.

- DDoS-атаки, основанные на протоколах SSL/TLS;
- DDoS-атаки уровня приложений.

– **Выявление и блокирование современных атак на сервисы Заказчика, в том числе, но не ограничиваясь противодействием следующим угрозам безопасности уровня приложений:**
  - Injection;
  - Broken Authentication;
  - Sensitive data exposure;
  - XML External Entities (XXE);
  - Broken Access control;
  - Security misconfigurations;
  - Cross-Site Scripting (XSS);
  - Insecure Deserialization;
  - Using Components with Known Vulnerabilities;
  - Insufficient Logging and Monitoring.

2.3. **Состав Услуг**

2.3.1. В составе Услуги ***«SberCloud Anti-DDoS»*** осуществляется[2]:

- подключение к Услуге[3];
- фильтрация HTTP-трафика от DDoS-атак на всех уровнях;
- фильтрация HTTPS-трафика от DDoS-атак на всех уровнях при условии предоставления (раскрытия) Заказчиком закрытых ключей шифрования SSL для их загрузки в облако Партнера;
- перевод сервиса (сайта) Заказчика на использование протокола HTTPS[4] с использованием бесплатных закрытых ключей шифрования SSL от Let’s Encrypt, загружаемых в облако Партнера;
- передача «очищенного» трафика от облака Партнера до размещаемого у Исполнителя сервиса Заказчика с использованием выделенного оптического канала связи;
- балансировка трафика сервиса Заказчика между узлами облака Партнера, а далее – распределение трафика между сервисами Заказчика, функционирующими в инфраструктуре облачной платформе SberCloud , по определенному алгоритму;
- мониторинг производительности защищаемого сервиса (сайта) Заказчика с оповещением по электронной почте о возникающих проблемах в его работе;
- предоставление доступа к системе мониторинга трафика в режиме реального времени посредством Личного кабинета);
- сбор и отображение подробной статистики по трафику сервиса Заказчика в Личном кабинете Заказчика;
- предоставление ежемесячных подробных отчетов об инцидентах в формате PDF;
- техническая поддержка 24*7*365.

2.3.2. В составе Услуги ***«SberCloud Anti-DDoS+WAF»*** осуществляется (без самостоятельной тарификации):

---

[2] Входит во все тарифные планы Услуги (без самостоятельной тарификации).

[3] Для подключения к Услуге Заказчику необходимо самостоятельно изменить А-запись, соответствующую доменному имени защищаемого сервиса, в своей DNS-зоне, чтобы она указывала на выделенный этому сервису IP-адрес в облаке Партнера (Qrator-IP), настроить firewall для запрета хождения трафика на IP адрес защищаемого ресурса с любых внешних адресов кроме узлов Qrator Labs, настроить сертификаты для очистки шифрованного трафика.

[4] В случае если ранее для доступа к защищаемому сервису (сайту) Заказчика использовался протокол HTTP.

- подключение к Услуге[5];
- фильтрация HTTP-трафика от DDoS-атак на всех уровнях;
- фильтрация HTTPS-трафика от DDoS-атак на всех уровнях при условии предоставления (раскрытия) Заказчиком закрытых ключей шифрования SSL для их загрузки в облако Партнера;
- перевод сервиса (сайта) Заказчика на использование протокола HTTPS[6] с использованием бесплатных закрытых ключей шифрования SSL от Let's Encrypt, загружаемых в облако Партнера;
- передача «очищенного» трафика от облака Партнера до размещаемого у Исполнителя сервиса Заказчика с использованием выделенного оптического канала связи;
- балансировка трафика сервиса Заказчика между узлами облака Партнера, а далее – распределение трафика между сервисами Заказчика, функционирующими в инфраструктуре облачной платформе SberCloud, по определенному алгоритму;
- мониторинг производительности защищаемого сервиса (сайта) Заказчика с оповещением по электронной почте о возникающих проблемах в его работе;
- активное сканирование сайта Заказчика на наличие уязвимостей уровня приложений, которые могут привести к его «взлому»;
- предоставление отчетов об обнаруженных уязвимостях уровня приложений сайта Заказчика с рекомендациями по их устранению;
- предоставление услуги «Virtual Patching» в отношении сайта Заказчика с автоматическим отслеживанием состояния уязвимости до момента ее устранения и контролем качества устранения уязвимостей;
- защита сайта Заказчика от атак-перебора (брутфорс паролей и т.д., включается по запросу Заказчика);
- осуществление активной проверки угроз из трафика на сайты Заказчика;
- формирование периодических отчетов;
- сбор и отображение подробной статистики по трафику сервиса Заказчика в Личном кабинете Заказчика;
- предоставление доступа к системе мониторинга трафика в режиме реального времени (посредством личного кабинета);
- техническая поддержка 24*7*365.

2.4. **Техническое описание Услуг**

2.4.1. Техническое описание Услуг ***«SberCloud Anti-DDoS»*** и ***«SberCloud Anti-DDoS+WAF»***

Услуги ***«SberCloud Anti-DDoS»*** и ***«SberCloud Anti-DDoS+WAF»*** предоставляются на базе отдельной инфраструктуры облачной платформы Партнера, включающей более 10 центров обработки данных (ЦОД) по всему миру, в том числе 3 ЦОД в России (облаке Партнера).

Сеть облака Партнера спроектирована и построена в расчете на работу под постоянным воздействием большого числа DDoS-атак. Узлы фильтрации облака Партнера подключены к каналам крупнейших магистральных Интернет-провайдеров США, России, Западной и Восточной Европы, Юго-восточной Азии. Таким образом, в отличие от сетей операторов хостинга (особенно, виртуального), сеть облака Партнера спроектирована в расчете на экстремальные нагрузки, и атака на один из ресурсов, защищаемых

[5] Для подключения к Услуге Заказчику необходимо самостоятельно изменить А-запись, соответствующую доменному имени защищаемого сервиса, в своей DNS-зоне, чтобы она указывала на выделенный этому сервису IP-адрес в облаке Партнера (Qrator-IP), настроить firewall для запрета хождения трафика на IP адрес защищаемого ресурса с любых внешних адресов кроме узлов Qrator Labs, настроить сертификаты для очистки шифрованного трафика.

[6] В случае если ранее для доступа к защищаемому сервису (сайту) Заказчика использовался протокол HTTP.

облаком Партнера, никак не влияет на работоспособность других защищаемых ресурсов (сайтов, WEB-приложений).

Технические характеристики облака Партнера:

- Более 1000 Гбит/с пассивной полосы пропускания - детерминированная обработка IP-пакетов без установления TCP-соединения;
- Более 500 Гбит/с активной полосы пропускания - каждое входящее TCP-соединение обрабатывается и анализируется;
- <5% ложных срабатываний в процессе отражения DDoS-атаки;
- время обучения сети от момента подключения нового Заказчика - менее 2 часов:
  1) в 33% случаев - до 4 минут;
  2) в 60% случаев - от 5 минут до 1 часа;
- время старта фильтрации атаки на «обученном» трафике – в 80% случаев до 2 минут от начала атаки;
- добавленное время задержки при проксировании трафика - от 0 до 100 мс. В случае проксирования HTTP-трафика в силу использования persistent HTTP-соединений с защищаемым сервисом возможен прирост скорости работы защищаемого сервиса;
- опциональная балансировка очищенного трафика между экземплярами сервиса Заказчика на основе алгоритмов: primary-backup, round-robin, iphash, а также в фиксированных пропорциях.
- количество защищаемых сервисов Заказчика - неограниченно.

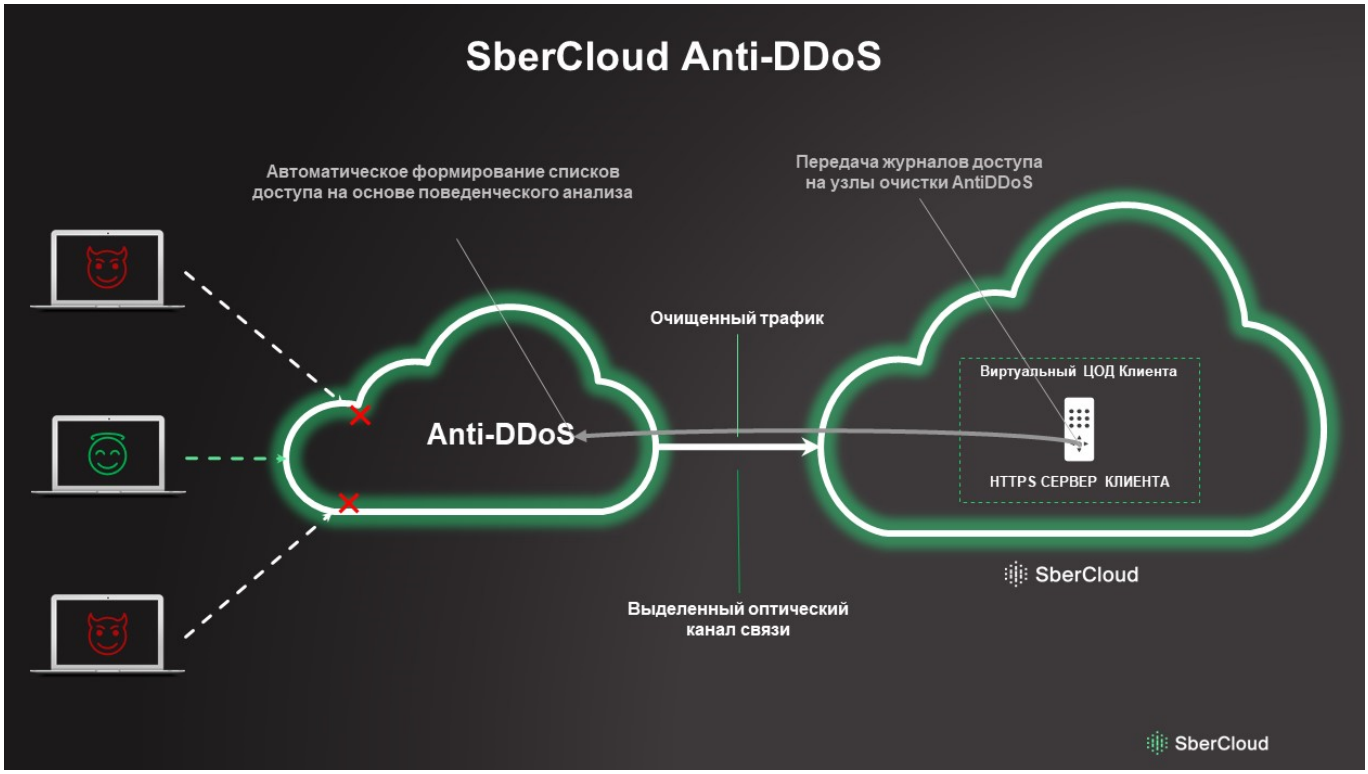
Технически Заказчик подключается следующим образом. Заказчик вносит изменения в записи DNS, направляющие пользовательский трафик на предоставленный Заказчику IP-адрес узлов фильтрации Партнера (Qrator-IP), выполняет настройки, запрещающие хождение трафика на IP адрес защищаемого ресурса с любых внешних адресов кроме узлов Qrator Labs, настраивает сертификаты.

После подключения трафик Заказчика постоянно, вне зависимости от наличия атаки, поступает в сеть облака Партнера и анализируется им. «Чистый» трафик перенаправляется на защищаемый сервис (сайт) Заказчика, размещаемый в инфраструктуре облачной платформы SberCloud». Такая схема работы позволяет узлам фильтрации Партнера сформировать профиль трафика, который является нормой для каждого сервиса (сайта) Заказчика в отдельности, и в случае любых отклонений реагировать на это.

Все узлы фильтрации сети инфраструктуры облачной платформы Партнера работают независимо друг от друга и, в случае выхода из строя одного из них, трафик защищаемого сервиса Заказчика не потеряется, а автоматически будет перемаршрутизирован на другой ближайший узел фильтрации Партнера.

Передача «очищенного» трафика от облака Партнера до инфраструктуры облачной платформы SberCloud осуществляется с использованием выделенного оптического канала связи, организуемого и поддерживаемого силами Исполнителя и Партнера. Указанный канал изолирован от сети Интернет и построен на базе резервированных, оптических линий связи.

Общая архитектура решения Услуги ***«SberCloud Anti-DDoS»*** приведена ниже.



В рамках Услуги ***«SberCloud Anti-DDoS+WAF»*** облако Партнера обеспечивает как противодействие DDoS-атакам, так и защиту от хакерских атак, направленных на эксплуатации уязвимостей сервисов (сайтов) Заказчика (сервис Web Application Firewall, далее – WAF).

В рамках предоставляемого в составе услуги ***«SberCloud Anti-DDoS+WAF»*** сервиса WAF осуществляются:

- блокирование большей части атак на веб-приложения при работе с большим потоком трафика;
- выявление существующих ошибок безопасности веб-приложений;
- защита приложений сайта от попыток эксплуатации неисправленных уязвимостей путем обнаружений и блокировки попыток атак и вторжений в режиме on-line, что позволяет не приостанавливать работу сайта (не предоставляется на этапе тестовой эксплуатации);
- автоматическое отслеживание состояния уязвимости до момента ее устранения;
- контроль устранения уязвимостей.

Для обеспечения возможности работы WAF в составе услуги ***«SberCloud Anti-DDoS+WAF»*** необходима передача и загрузка в облако Партнера закрытых ключей шифрования SSL, используемых Заказчиком для организации защищенного доступа к их сайтам с использованием протокола HTTPS.

3. ОГРАНИЧЕНИЯ ПО ПРЕДОСТАВЛЕНИЮ УСЛУГ

3.1. Услуги ***«SberCloud Anti-DDoS»*** и ***«SberCloud Anti-DDoS+WAF»*** доступны только для сервисов Заказчика, функционирующих в инфраструктуре облачной платформы SberCloud.

4. УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ

4.1. Технические аспекты работы системы фильтрации трафика, за несоблюдение которых Исполнитель не отвечает и при несоблюдении которых Исполнитель не может гарантировать обеспечение заявленного уровня качества услуг по фильтрации трафика:

4.1.1. Для целей фильтрации трафика предполагается, что данные из сети «Интернет» передаются не непосредственно на IP-адрес сервера (или виртуальной машины) Заказчика, а на адрес, имеющий FQDN сервера (или виртуальной машины) Заказчика.

4.1.2. В случае, если сервер (или виртуальная машина) Заказчика, для обеспечения стабильности и бесперебойности работы которого подключены услуги по фильтрации трафика, будет способен принимать входящий трафик от любых серверов в сети «Интернет», Исполнитель не может гарантировать оказание услуги по фильтрации трафика в запрашиваемом объеме до момента полного обновления DNS-записей об адресах серверов защищаемых Доменов во всей сети «Интернет».

4.1.3. Для исключения ситуации обработки сервером Заказчика вредоносного входящего трафика на сервере или в «Организации» (тенанте) Заказчика должен быть включен или развернут Брандмауэр (Firewall), блокирующий любой входящий трафик, кроме входящего трафика с конкретного сервера Исполнителя.[7]

4.1.4. Для снижения количества вредоносного трафика, блокируемого Брандмауэром (межсетевым экраном) Заказчика, а соответственно, для снижения нагрузки на сервер (или виртуальную машину) Заказчика, Заказчик обязан предпринять меры по сокрытию (неразглашению) фактических IP-адресов серверов и виртуальных машин, для которых осуществляется фильтрация трафика.

4.1.5. Услуги по фильтрации трафика заключаются в объявлении сервером (или виртуальной машиной) Заказчика фильтрующего облака Партнера путем внесения соответствующих записей в описание DNS-зоны, к которой принадлежит сервер (или виртуальная машина) Заказчика; на фильтрующем облаке Партнера происходит последовательное выполнение следующих операций с данными, передаваемыми на сервер с FQDN сервера Заказчика:

4.1.6. прием передаваемых на FQDN сервера (или виртуальной машины) Заказчика, на котором функционируют его защищаемый сервис, запросов (прием входящего трафика);

4.1.7. анализ структуры запросов (анализ входящего трафика) на предмет наличия последовательностей данных, способных повлечь некорректное функционирование защищаемого сервиса Заказчика;

4.1.8. отсечение запросов, содержащих последовательности данных, нарушающие корректное функционирование защищаемого сервиса Заказчика (очистка входящего трафика от вредоносной составляющей);

4.1.9. перенаправление на реальный IP-адрес сервера (или виртуальной машины) Заказчика, на котором функционирует его защищаемый сервис, очищенного от вредоносной составляющей входящего трафика.

5. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

5.1. **Возможные виды подключения / изменения / удаления Услуг:**

5.1.1. Подключение Услуги посредством подписания Заказа.

5.2. **Возможный порядок расчётов по услуге**

5.2.1. Постоплата (на основании отдельно заключенного письменного бланка Заказа).

5.3. **Возможные способы оплаты / порядок пополнения баланса:**

5.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта.

[7] В случае защиты виртуальной машины, размещаемой в «Организации» (тенанте) Заказчика на базе инфраструктуры облачной платформы SberCloud, в качестве соответствующего межсетевого экрана может быть использован и соответствующим образом настроен VMWare NSX Edge.