

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ «ЗАЩИТА ОТ DDOS-АТАК (QRATOR)», «ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (QRATOR)»

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГ

- 1.1. **Услуга «Защита от DDoS-атак (Qrator)»** – услуга по защите от атак отказа в обслуживании или DDoS-атак сервисов¹ Заказчика, доступных по протоколам HTTP, HTTPS или иным прикладным протоколам, подверженным DDoS-атакам.
- 1.2. **Услуга «Защита веб-приложений (Qrator)»** – услуга по фильтрации веб-трафика для защиты от атак, направленных на эксплуатацию уязвимостей WEB-приложений (функция Web Application Firewall, WAF). Услуга Защита веб-приложений предоставляется Заказчикам только совместно с услугой Защита от DDoS-атак
- 1.3. Услуги предоставляются в сотрудничестве с ООО «Эйч-эль-эль» (Qrator Labs, далее – Партнер).
- 1.4. Услуги предоставляются на базе облачного решения Партнера по защите от DDoS-атак и атак, направленных на эксплуатацию уязвимостей WEB-приложений, реализованного с помощью отдельной инфраструктуры облачной платформы Партнера, включающей более десяти центров обработки данных (ЦОД) по всему миру, в том числе три ЦОД в России (далее – облако 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 облаком Партнера, никак не влияет на работоспособность других защищаемых ресурсов (сайтов, WEB-приложений). В рамках Услуги «Защита веб-приложений» облако Партнера обеспечивает, как противодействие DDoS-атакам, так и защиту от хакерских атак, направленных на эксплуатации уязвимостей сервисов (сайтов) Заказчика.
- 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:
- прием передаваемых на FQDN сервера (или виртуальной машины) Заказчика, на котором функционируют его защищаемый сервис, запросов (прием входящего трафика);
 - анализ структуры запросов (анализ входящего трафика) на предмет наличия последовательностей данных, способных повлечь некорректное функционирование защищаемого сервиса Заказчика;
 - отсеечение запросов, содержащих последовательности данных, нарушающие корректное функционирование защищаемого сервиса Заказчика (очистка входящего трафика от вредоносной составляющей);
 - перенаправление входящего трафика очищенного от вредоносной составляющей (легитимного трафика) на реальный IP-адрес сервера (или виртуальной машины) Заказчика, на котором функционирует его защищаемый сервис.
- 1.6. После подключения Услуги трафик Заказчика постоянно, вне зависимости от наличия атаки, поступает в сеть облака Партнера и анализируется им. Легитимный («очищенный») трафик перенаправляется на защищаемый сервис (сайт) Заказчика, размещаемый в инфраструктуре облачной платформы Исполнителя. 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.
- 1.7. Передача легитимного («очищенного») трафика от облака Партнера до инфраструктуры облачной платформы Исполнителя 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.

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

- 1.8. Для обеспечения возможности работы WAF в составе услуги Защита веб-приложений необходима передача и загрузка в облако Партнера закрытых ключей шифрования SSL/TLS, используемых Заказчиком для организации защищенного доступа к их сайтам с использованием протокола HTTPS.
- 1.9. Общая архитектура решения Услуги приведена ниже на Рис.1:

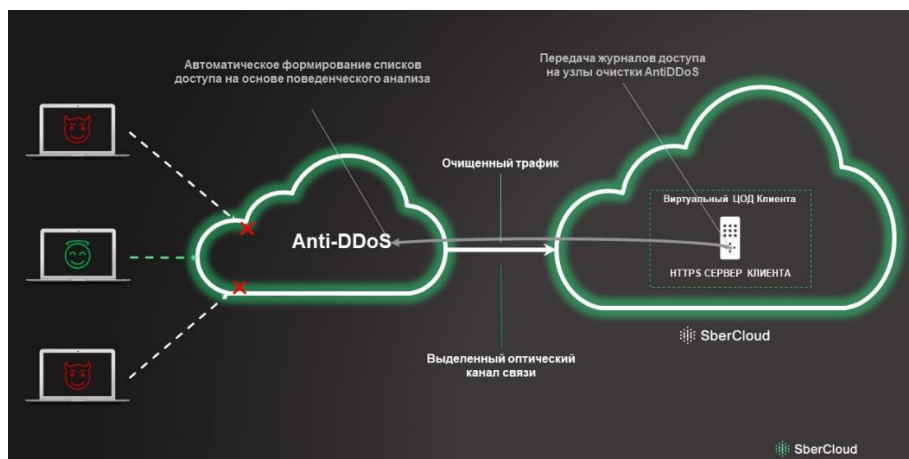


Рис.1. Общая архитектура решения Услуги

- 1.10. В составе Услуги «Защита от DDoS-атак (Qrator)» осуществляется²:
- подключение к услуге;
 - фильтрация трафика от DDoS-атак на всех уровнях;
 - фильтрация HTTPS-трафика от DDoS-атак на прикладном уровне при условии предоставления (раскрытия) Заказчиком закрытых ключей шифрования SSL/TLS для их загрузки в облако Партнера;
 - перевод сервиса (сайта) Заказчика на использование протокола HTTPS³ с использованием бесплатных закрытых ключей шифрования SSL/TLS 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 платформы Исполнителя, 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.
- 1.11. Для подключения услуги «Защита от DDoS-атак (Qrator)» Заказчик должен выбрать тарифный план на основании предполагаемой полосы вредоносного трафика, гарантированной доступности защищаемых сервисов и необходимой дополнительной функциональности:

Наименование тарифного плана	Professional	Business	Corporate
Полоса фильтрации вредоносного (нежелательного) трафика	10 Гбит/сек	50 Гбит/сек	500 Гбит/сек
Полоса легитимного трафика в тарифе	10 Мбит/с		
Гарантированная доступность информационного ресурсов	97%	99%	99,50%
Тарифицируемый трафик	легитимный		
Фильтрация HTTPS с использованием приватных ключей Клиента	включено в тариф		
Предоставление сертификатов Let's Encrypt	включено в тариф		

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

³ В случае если ранее для доступа к защищаемому сервису (сайту) Заказчика использовался протокол HTTP.

Активная проверка доступности площадок клиента	не предусмотрено	включено в тариф
Фильтрация HTTPS без использования частных ключей	не предусмотрено	включено в тариф
Доступ к API	не предусмотрено	включено в тариф
Прямое подключение в существующий стык с инфраструктурой Исполнителя QDC (Qrator Direct Connection)	не предусмотрено	включено в тариф
Базовая балансировка очищенного трафика между IP-адресами (не более двух апстримов по алгоритму Round-robin)	включено в тариф	
Балансировка очищенного трафика между IP-адресами Заказчика QLB (Qrator Load Balancing)	не предусмотрено	лицензируется дополнительно
Услуга защиты Websockets (проксирование TCP соединений)	лицензируется дополнительно	включено в тариф
Подключение к инфраструктуре Исполнителя посредством анонса сетевых префиксов Заказчика по протоколу BGP	не предусмотрено	лицензируется дополнительно
Предоставление выделенного порта на оборудовании Исполнителя для организации ВОЛС QDP (Qrator Dedicated Port)	не предусмотрено	лицензируется дополнительно
Фильтрация трафика по геоэонам	не предусмотрено	лицензируется дополнительно

1.12. В составе Услуги «Защита веб-приложений (Qrator)» осуществляется (без самостоятельной тарификации):

- 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.

1.13. Для подключения Услуги «Защита веб-приложений (Qrator)» Заказчик должен выбрать тарифный план на основании необходимой ему функциональности:

Наименование тарифного плана	Elementary WAF	Advisory WAF
Блокирование атак	Блокируются отдельные вредоносные запросы и ответы	
Возможные способы обнаружения атак	<p>Атаки выявляются следующими способами:</p> <ul style="list-style-type: none"> • Выявление атак на уровне параметров HTTP протокола внутри запросов и ответов. • Выявление признаков атак внутри вложенных данных передаваемых в запросах. • Выявление переборных атак (включается по запросу, единые настройки для всего приложения). 	<p>Атаки выявляются следующими способами:</p> <ul style="list-style-type: none"> • Выявление атак на уровне параметров HTTP протокола. • Выявление признаков атак внутри вложенных данных, передаваемых как в запросах, так и в ответах. • Выявление признаков атак на уровне отдельных логических действий в приложении с возможностью (включается по запросу, настраивается в рамках дополнительных услуги по обнаружению и блокированию сетевых атак). • Выявление атак на уровне отдельных сессий пользователей и контроль авторизации для ресурсов с низкой и средней нагрузкой (включается по запросу, настраивается в рамках дополнительных услуги по обнаружению и блокированию сетевых атак). • Выявление переборных атак на уровне отдельных логических действий (включается по запросу, настраивается в рамках дополнительных услуги по

		<p>обнаружению и блокированию сетевых атак).</p> <ul style="list-style-type: none"> Выявление бот-активности (включается по запросу, настраивается в рамках дополнительных услуги по обнаружению и блокированию сетевых атак).
Хранение данных	<p>Сохраняются события безопасности, а также вредоносные запросы и ответы.</p>	<p>Сохраняются следующие данные:</p> <ul style="list-style-type: none"> события безопасности, вредоносные запросы и ответы, легитимные запросы и ответы в рамках приобретенного объема хранилища, важные логические действия (ограничено приобретенным объемом хранилища, включается по запросу, настраивается в рамках дополнительных услуги по обнаружению и блокированию сетевых атак).
Доступ к интерфейсу управления SolidWall WAF	<p>Доступ к личному кабинету с базовым функционалом. Поддерживаются следующие функции:</p> <ul style="list-style-type: none"> Дашборды мониторинга. Отображение событий безопасности с поддержкой группировкой. Отображение журнала заблокированных транзакций. 	<p>Доступ к личному кабинету с расширенным функционалом. Поддерживаются следующие функции:</p> <ul style="list-style-type: none"> Дашборды мониторинга. Отображение событий безопасности с поддержкой группировкой. Отображение журнала заблокированных транзакций. Возможность включения/ выключения защиты и подавления ложных срабатываний.
Предоставление возможности интеграции SolidWall WAF с внешними системами	<p>Не предусмотрено тарифом.</p>	<p>Предоставляется возможность интеграции с использованием механизмов SYSLOG или REST API (включается по запросу).</p>
Предоставление автоматизированных отчетов	<p>Предоставляются следующие виды отчетов:</p> <ul style="list-style-type: none"> Регулярные автоматизированные отчеты (настраиваются по запросу). Однократные автоматизированные отчеты (предоставляются по запросу). 	<p>Предоставляются следующие виды отчетов:</p> <ul style="list-style-type: none"> Регулярные автоматизированные отчеты (настраиваются по запросу). Однократные автоматизированные отчеты (предоставляются по запросу).
Консультирование Клиентов по вопросам использования Услуг WAF	<p>Консультирование Клиентов по следующим вопросам:</p> <ul style="list-style-type: none"> использование базового функционала личного кабинета, разъяснения по заблокированным запросам. 	<p>Консультирование Клиентов по следующим вопросам:</p> <ul style="list-style-type: none"> использование базового функционала личного кабинета, разъяснения по заблокированным запросам, интеграция с внешними системами с использованием механизмов SYSLOG или REST API.
Услуги базовой технической поддержки, оказываемые при подключении новых Клиентов	<p>При подключении осуществляются следующие настройки (выполняются с применением машинного обучения):</p> <ul style="list-style-type: none"> Настройка параметров протокола; Подавление ложных срабатываний; Фильтрация статических ресурсов; Глобальная настройка модуля противодействия переборным атакам (по запросу). 	<p>При подключении осуществляются следующие настройки (выполняются с применением машинного обучения):</p> <ul style="list-style-type: none"> Настройка параметров протокола Подавление ложных срабатываний; Фильтрация статических ресурсов; Глобальная настройка модуля противодействия переборным атакам (по запросу); Автоматизированная разметка логических действий (в целях подавления ложных срабатываний); Глобальная настройка модуля контроля сессий и защиты от атак на авторизацию (по запросу и если не превышена допустимая нагрузка).
Услуги базовой технической поддержки, оказываемые в процессе эксплуатации SolidWall WAF	<ul style="list-style-type: none"> поддержание работоспособности и устранение ошибок в работе SolidWall WAF в инфраструктуре Заказчика; обновление версий SolidWall WAF в инфраструктуре Заказчика; предоставление Заказчику доступа к интерфейсу управления SolidWall WAF для осуществления им самостоятельной настройки, а также контроля работоспособности SolidWall WAF; 	

	<ul style="list-style-type: none"> • предоставление Заказчику возможности интеграции SolidWall WAF с внешними информационными системами для осуществления им самостоятельной настройки, а также контроля работоспособности SolidWall WAF; • Консультирование Заказчика по вопросам и администрирования «SolidWall WAF».
--	---

1.14. 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:
- в 33% случаев - до 4 минут;
- 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.

1.15. 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 межсетевой экран (firewall) для запрета хождения трафика на IP адрес защищаемого ресурса с любых внешних адресов кроме узлов Qrator Labs;
- настроить сертификаты для очистки зашифрованного трафика.

1.16. Услуги доступны только для сервисов Заказчика, функционирующих в инфраструктуре облачной платформы Исполнителя.

2. МЕТРИКИ УСЛУГИ

2.1. Базовая функциональность и метрики Услуг представлены в Таблице 1.

Табл. 1. Параметры предоставляемых Услуг

Наименование Услуги	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Защита от DDoS-атак (Qrator)	Тариф	Абонентская плата по тарифу	Professional, Business, Corporate
	Защищаемый домен	Дополнительный Qrator-IP	от 1 и более
	Легитимный трафик	Легитимный трафик сверх включенного в тариф	от 1 Мбит/с
		Предоплаченная полоса сверх тарифа	10, 50, 100, 200, 300, 400, 500 Мбит/с
		Защита от ботов	от 1 Мбит/с
		Предоплаченная полоса защиты от ботов	10, 50, 100, 200, 300, 400, 500 Мбит/с
	Опции подключения	Фильтрация HTTPS без использования приватных ключей	Только на тарифах Business, Corporate
		Защита WebSocket (проксирование TCP соединений)	На всех тарифах
		Подключение по протоколу BGP	Только на тарифе Corporate
		Прямое подключение в существующий стык с инфраструктурой Исполнителя QDC (Qrator Direct Connection)	

		Выделенный порт на оборудовании	
	Дополнительные опции	Фильтрация трафика по геоэонам	Только на тарифе Corporate
		Активная проверка доступности площадок заказчика	Только на тарифах Business, Corporate
		Доступ к API	
	Балансировка очищенного трафика между IP-адресами	Не более двух апстримов по алгоритму Round-robin	На всех тарифах
		Qrator Load Balancing	Только на тарифах Business, Corporate
Защита веб-приложений (Qrator)	Отказоустойчивый DNS	Отказоустойчивый DNS	DNS10, DNS10+, DNS100, DNS100+
	Тариф	Абонентская плата по тарифу	Elementary, Advisory
	Защищаемый домен	Дополнительный домен/веб-приложение	от 1 и более
	Легитимный трафик	Легитимный трафик сверх включенного в тариф	от 1 Мбит/с
		Предоплаченная полоса сверх тарифа	10, 50, 100, 200, 300, 400, 500 Мбит/с

3. ТАРИФИКАЦИЯ УСЛУГИ

- 3.1. Для данной Услуги используется статическая тарификация (Allocation). Величина ежемесячного платежа за пользование Услугой определяется в соответствии с параметрами запрошенной услуги.

4. ОГРАНИЧЕНИЯ

- 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:
- 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;
 - 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;
 - для исключения ситуации обработки сервером Заказчика вредоносного входящего трафика на сервере или в «Организации» (тенанте) Заказчика должен быть включен или развернут межсетевой экран (firewall), блокирующий любой входящий трафик, кроме входящего трафика с конкретного сервера Исполнителя;⁴
 - для снижения количества вредоносного трафика, блокируемого межсетевым экраном (firewall) 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.

5. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГАМ

- 5.1. Возможные виды подключения / изменения / отключения Услуг:
- 5.1.1. посредством подписания Заказа.
- 5.2. Возможный порядок расчётов по Услугам:
- 5.2.1. постоплата.

⁴ В случае защиты виртуальной машины, размещаемой в «Организации» (тенанте) Заказчика на базе инфраструктуры облачной платформы Исполнителя, в качестве соответствующего межсетевого экрана (firewall) может быть использован и соответствующим образом настроен VMWare NSX Edge.

- 5.3. **Возможные способы оплаты / порядок пополнения баланса:**
- 5.3.1. оплата в безналичном порядке на основании выставленного Исполнителем счёта.