

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 (Qrator)» предоставляется Заказчиком только совместно с услугой «Защита от DDoS-атак (Qrator)».
- 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 атака² 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 эксплуатацию уязвимостей сервисов 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 «Защита веб-приложений (Qrator)» трафик Заказчика постоянно, вне зависимости от наличия атаки, поступает в сеть облака Партнера и анализируется им. Легитимный («очищенный») трафик перенаправляется на защищаемый сервис Заказчика, размещаемый в Инфраструктуре. Такая схема работы позволяет узлам фильтрации Партнера сформировать профиль трафика, который является нормой для каждого сервиса Заказчика в отдельности, и в случае любых отклонений реагировать на это.
- 1.7. Передача легитимного (очищенного) трафика от Облака Партнера до Инфраструктуры 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.
- 1.8. Для обеспечения возможности работы WAF в составе услуги «Защита веб-приложений (Qrator)» необходима передача и загрузка в Облако Партнера закрытых ключей шифрования SSL/TLS, используемых Заказчиком для организации защищенного доступа к сервисам заказчика с использованием протокола HTTPS.
- 1.9. Общая архитектура решения Услуги приведена ниже на Рис.1:

¹ Здесь и далее по тексту 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, доменными именами, Интернет-магазинами и прочими WEB-сервисами Заказчика.

² Здесь и далее по тексту документа под «атаками» подразумевается любая из атак, указанных в п.1.1. и/или п. 1.2. Приложения № 1.CRS.2.1., если контекст не содержит иного прямо указанного значения.

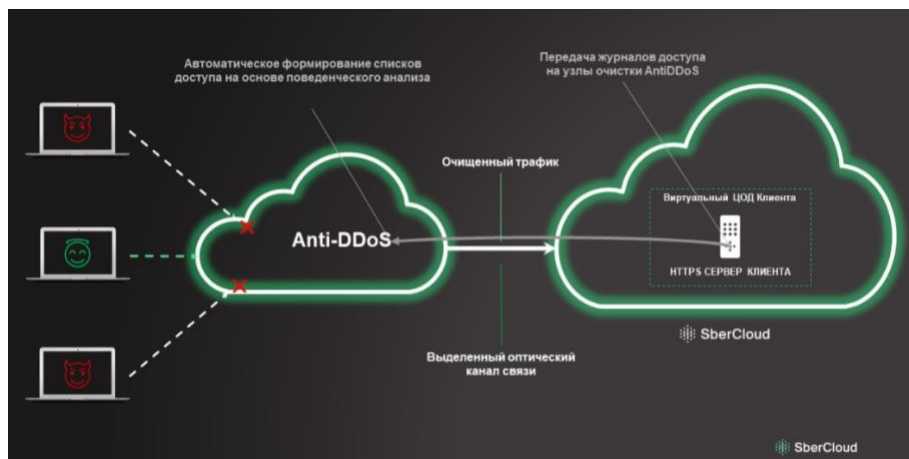


Рис.1. Общая архитектура решения Услуги

1.10. В составе Услуги «Защита от DDoS-атак (Qrator)» осуществляется³:

- 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 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, по определенному алгоритму;
- мониторинг производительности защищаемого сервиса 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;
- предоставление ежемесячных подробных отчетов об инцидентах в формате PDF.

1.10.1. 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:

Табл.1. Тарифные планы Услуги «Защита от DDoS-атак (Qrator)»

Наименование тарифного плана	Professional (Pro)	Business (Bsns)	Corporate (Corp)
Включена полоса фильтрации вредоносного (нежелательного) трафика, до:	10 Гбит/сек	50 Гбит/сек	500 Гбит/сек
Включено трафика в тарифный план	10 Мбит/с		
Гарантированная доступность сервисов в месяц, не менее	97%	99%	99,5%
Тарифицируемый трафик	легитимный		
Оплата полосы трафика сверх включенного в тарифный план, за каждый Мбит/с	тарифицируется дополнительно		
Фильтрация HTTPS с использованием приватных ключей Клиента	включено		
Предоставление сертификатов Let's Encrypt	включено		

³ Входит во все тарифные планы Услуги (без самостоятельной тарификации).

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

Активная проверка доступности площадок клиента	Не предусмотрено	включено	
Фильтрация HTTPS без использования приватных ключей	Не предусмотрено	включено	
Доступ к API	Не предусмотрено	включено	
Прямое подключение в существующий стык с инфраструктурой Исполнителя QDC (Qrator Direct Connection)	Не предусмотрено		включено
Дополнительные услуги	Professional (Pro)	Business (Bsns)	Corporate (Corp)
Предоставление IP-адресов (сверх 1 IP-адреса, включенного в тарифный план), ежемесячно	тарифицируется дополнительно	тарифицируется дополнительно	тарифицируется дополнительно
Базовая балансировка очищенного трафика между IP-адресами (Не более двух апстримов по алгоритму Round-robin)	включено		
Балансировка очищенного трафика между IP-адресами Заказчика QLB (Qrator Load Balancing), ежемесячно	Не предусмотрено	тарифицируется дополнительно	
Услуга защиты Websockets (проксирование TCP соединений), ежемесячно	тарифицируется дополнительно	включено	
Подключение к инфраструктуре Исполнителя посредством анонса сетевых префиксов Заказчика по протоколу BGP, ежемесячно	Не предусмотрено		тарифицируется дополнительно
Предоставление выделенного порта на оборудовании Исполнителя для организации ВОЛС QDP (Qrator Dedicated Port), ежемесячно	Не предусмотрено		тарифицируется дополнительно
Фильтрация трафика по геоэонам, ежемесячно	Не предусмотрено		тарифицируется дополнительно
Отказоустойчивый DNS10, ежемесячно	тарифицируется дополнительно		
Отказоустойчивый DNS10+, ежемесячно	тарифицируется дополнительно		
Отказоустойчивый DNS100, ежемесячно	тарифицируется дополнительно		
Отказоустойчивый DNS100+	тарифицируется дополнительно		
Защита от ботов, ежемесячно, за каждый Мбит/сек (руб.)	тарифицируется дополнительно		
Кэширование контента CDN 100, стоимость за 1Тбайт (до 100 Тбайт включительно)	тарифицируется дополнительно		
Кэширование контента CDN 100+, стоимость за 1Тбайт (свыше 100 Тбайт)	тарифицируется дополнительно		
10 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно		
50 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно		
100 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно		
200 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно		

300 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно
400 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно
500 Мбит/с предоплаченная полоса трафика сверх включенного в тарифный план	тарифицируется дополнительно

- 1.11. В составе Услуги «Защита веб-приложений (Qrator)» осуществляется без самостоятельной тарификации:
- активное сканирование сервиса Заказчика на наличие уязвимостей уровня приложений, которые могут привести к его взлому;
 - предоставление отчетов об обнаруженных уязвимостях уровня приложений сервиса Заказчика с рекомендациями по их устранению;
 - предоставление услуги «Virtual Patching» в отношении сервиса Заказчика с автоматическим отслеживанием состояния уязвимости до момента ее устранения и контролем качества устранения уязвимостей;
 - защита сервиса Заказчика от атак-перебора (брутфорс паролей и т.д.) - включается по запросу Заказчика;
 - осуществление активной проверки угроз из трафика на сервисы Заказчика;
 - формирование периодических отчетов.
- 1.12. Для подключения Услуги «Защита веб-приложений (Qrator)» Заказчик должен выбрать тарифный план на основании необходимой ему функциональности:

Табл. 2. Тарифные планы Услуги «Защита веб-приложений (Qrator)»

ОБНАРУЖЕНИЕ И ЗАЩИТА ОТ ХАКЕРСКИХ АТАК. WEB APPLICATION FIREWALL (WAF) ТЕХНОЛОГИЯ SOLIDWALL		
Наименование тарифного плана	Elementary Partner WAF	Advisory Partner WAF
Включено трафика в АП	3 Мбит/с	
Оплата полосы (трафика) сверх включенного в тарифный план (за 1 Мбит/с)	тарифицируется отдельно	
Включенное количество защищаемых сервисов	1 шт.	
Дополнительные услуги		
Защита 1 дополнительного сервиса, ежемесячно	тарифицируется отдельно	тарифицируется отдельно
Дополнительное пространство для хранения, за 1 ТБ ежемесячно	тарифицируется отдельно	
Стоимость дополнительных услуг по обнаружению и блокированию сетевых атак (Professional Services WAF), ежемесячно (24ч)	тарифицируется отдельно	
Услуги расширенной технической поддержки, оказываемые при подключении новых сервисов Заказчика (Professional Services WAF)	тарифицируется отдельно	

- 1.13. **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.

1.14. 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), для отключения необходимо выполнить обратное действие;
- настроить межсетевой экран (firewall) для запрета хождения трафика на IP-адрес защищаемого ресурса с любых внешних адресов, кроме узлов Партнера;
- настроить сертификаты для очистки шифрованного трафика.

1.15. Услуги доступны как для сервисов Заказчика, функционирующих в Облаке Cloud, так и в сторонней инфраструктуре.

1.16. Пользуясь Услугами, Заказчик подтверждает, что доменные имена, для которых подключаются Услуги, принадлежат ему на законном основании, либо он действует от имени и по поручению законных владельцев этих доменных имен.

2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

2.1. Функциональность и метрики Услуг представлены в Таблицах 3 и 4.

Табл. 3. 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 сервис	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
	Отказоустойчивый DNS	Отказоустойчивый DNS	DNS10, DNS10+, DNS100, DNS100+
Защита веб-приложений (Qrator)	Тариф	Абонентская плата по тарифу	Elementary, Advisory
	Защищаемый сервис	Дополнительный сервис	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

Табл. 4. Параметры услуги «Защита веб-приложений (Qrator)»

Наименование услуг	Elementary Partner WAF	Advisory Partner WAF
Описание услуг по обнаружению и блокированию сетевых атак, включенных в тарифный план		
Блокирование атак	Блокируются отдельные вредоносные запросы и ответы	
Возможные способы обнаружения атак	Атаки выявляются следующими способами: 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)	Атаки выявляются следующими способами: 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 обнаружению и блокированию сетевых атак). Выявление бот-активности (включается по запросу, настраивается в рамках дополнительных услуги по обнаружению и блокированию сетевых атак)
Хранение данных	Сохраняются события безопасности, а также вредоносные запросы и ответы	Сохраняются следующие данные: 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	Доступ к личному кабинету с базовым функционалом. Поддерживаются следующие функции: Дашборды мониторинга Отображение событий безопасности с поддержкой группировкой Отображение журнала заблокированных транзакций	Доступ к личному кабинету с расширенным функционалом. Поддерживаются следующие функции: 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	Не предусмотрено в тарифе	Предоставляется возможность интеграции с использованием механизмов SYSLOG или REST API (включается по запросу)
Предоставление автоматизированных отчетов	Предоставляются следующие виды отчетов: Регулярные автоматизированные отчеты (настраиваются по запросу) Однократные автоматизированные отчеты (предоставляются по запросу)	Предоставляются следующие виды отчетов: Регулярные автоматизированные отчеты (настраиваются по запросу) Однократные автоматизированные отчеты (предоставляются по запросу)
Консультирование Клиентов по вопросам использования Услуг WAF	Консультирование Клиентов по следующим вопросам: использование базового функционала личного кабинета разъяснения по заблокированным запросам.	Консультирование Клиентов по следующим вопросам: 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	При подключении осуществляются следующие настройки (выполняются с применением машинного обучения): Настройка параметров протокола Подавление ложных срабатываний Фильтрация статических ресурсов Глобальная настройка модуля противодействия переборным атакам (по запросу)	При подключении осуществляются следующие настройки (выполняются с применением машинного обучения): 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	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; 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»
Дополнительные услуги по обнаружению и блокированию сетевых атак (Professional Services WAF)	
Услуги расширенной технической поддержки, оказываемые при подключении новых сервисов Заказчика	Тонкая ручная настройка механизмов защиты под особенности приложений Клиента, в том числе, корректировка результатов машинного обучения. Проактивное реагирование на критичные события информационной безопасности на основе согласованных с Заказчиком сценариев. Периодический анализ (аудит) событий информационной безопасности с целью сбора статистики и анализа менее критичных событий. Техническое расследование инцидентов информационной безопасности. Разработка аналитических отчетов. Изменение функциональности SolidWall WAF (формы отчетности, изменение сценариев работы с пользовательским интерфейсом). Интеграция со сторонними средствами Заказчика (SIEM, «тикетные» системы, СМС-информирование и т.п). Анализ защищенности сервисов Заказчика (тестирование на проникновение, анализ исходного кода). Консультирование Заказчика по общим вопросам защиты веб-приложений, в том числе – по практикам безопасного кодирования

3. ТАРИФИКАЦИЯ УСЛУГИ

3.1. Статическая тарификация (Allocation).

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 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.

5.3. Возможные способы оплаты / порядок пополнения Баланса:

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

⁴ В случае защиты виртуальной машины, размещаемой в тенанте Заказчика на базе Инфраструктуры, в качестве соответствующего межсетевого экрана (firewall) может быть использован и соответствующим образом настроен Edge Gateway.