

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

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГ

- 1.1. Услуга «Защита от DDoS-атак (StormWall)» – 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 (StormWall)» – услуга по фильтрации веб-трафика для защиты от атак, направленных на эксплуатацию уязвимостей WEB-приложений (функция Web Application Firewall, WAF). Услуга «Защита веб-приложений (StormWall)» предоставляется Заказчикам только совместно с услугой «Защита от DDoS-атак (StormWall)».
- 1.3. Услуги предоставляются в сотрудничестве с ООО «СТОРИ ЛАБС» (бренд StormWall, далее – Партнер) и на базе его облачного решения² по защите от DDoS-атак и атак, направленных на эксплуатацию уязвимостей WEB-приложений.

2. ОПИСАНИЕ УСЛУГИ «ЗАЩИТА ОТ DDOS-АТАК (STORMWALL)»

- 2.1. Общие характеристики Услуги:
 - 2.1.1. предоставляется посредством изменения DNS-записей интернет-сервисов Заказчика с целью направления всех запросов на оборудование Исполнителя.
 - 2.1.2. при срабатывании защиты реализована отправка E-Mail-уведомлений о начавшейся и прекратившейся атаке.
 - 2.1.3. Услуга обеспечивает:
 - сквозную передачу на оборудование Заказчика IP-адресов источников запросов;
 - возможность прохождения протокола WebSocket с настройкой соответствующих портов;
 - беспрепятственную работу легальных поисковых ботов и не оказывает влияния на показания Яндекс- и Google-метрик в части источников перехода даже в режиме фильтрации атаки. При этом полностью исключено влияние защиты на такие показатели, как число внутренних переходов, число отказов и продолжительность сессии;
 - не менее 5 точек очистки трафика по миру в США, Европе, Российской Федерации, Центральной Азии и в Китае.
 - 2.1.4. включение режима блокировки атаки и очистки трафика осуществляется автоматически при обнаружении системой мониторинга Исполнителя атаки, направленной на Интернет-ресурсы Заказчика, а также при поступившей заявке от Заказчика.
 - 2.1.5. поддерживает автоматическую установку бесплатных Let's Encrypt SSL сертификатов, предоставляемых Исполнителем.
- 2.2. Технические характеристики Услуги:
 - 2.2.1. Защита от следующих типов атак:
 - TCP-флуд (включая SYN ACK reflecton flood, TCP ACK flood, TCP fragmented attack);
 - SYN-флуд (включая Spoofed SYN flood);
 - UDP-флуд (включая DNS/NTP/SSDP amplification, UDP fragment flood);
 - HTTP/S-флуд (POST/GET bot attack, SlowLoris);
 - ICMP-флуд (включая Smurf attack, Ping of Death);
 - Флуд другими протоколами (GRE flood etc.); - Заполнение полосы пропускания (volumetric flood).
 - 2.2.2. Услуга обеспечивает:
 - фильтрацию как HTTP, так и HTTPS трафика с раскрытием приватных ключей SSL;
 - поддержку протокола HTTP/2 без переключения клиентов с поддержкой протокола HTTP/2 на более старые версии протокола;
 - балансировку нагрузки между пулом основных и резервных бэкендов;
 - кэширование для необходимых расширений файлов;
 - 2.2.3. Защита на уровне оборудования Исполнителя;
 - обеспечивается защита от атак, имеет техническую возможность подавления (грубой очистки) атаки емкостью не менее 3,5 Тбит/сек;

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 Т.е. без необходимости установки программного обеспечения на серверы Заказчика.

- обеспечивается тонкая пакетная фильтрация трафика со скоростью не менее 1,6 Тбит/с.

3. ПОРЯДОК ДОСТУПА К УСЛУГЕ «ЗАЩИТА ОТ DDOS-АТАК (STORMWALL)»

- 3.1. Заказчику предоставляется личный кабинет и API для управления услугой с возможностью изменения защиты (в том числе ее отключения), порогов ее срабатывания, бэкендов, параметров проверки доступности бэкендов, сертификатов и приватных ключей, черных и белых списков, исключения по типам файлов, исключения по локациям.
- 3.2. Личный кабинет Услуги предоставляет Заказчику следующие функциональные возможности:
- 3.2.1. управление порогами (лимитами) для обнаружения атак:
- По количеству запросов в секунду;
 - По % соотношению запросов, завершенных с ошибками на подзащитном сервисе;
 - По скорости увеличения входящего трафика;
 - Возможность настройки индивидуальных порогов для блокировки IP-адресов по количеству заблокированных запросов и запросов в определенные области web-приложения (Location);
 - Возможность настройки максимальной продолжительности атаки, а также управление условиями завершения (обратного перехода из режима активной фильтрации в режим обнаружения).
- 3.2.2. В личном кабинете Услуги присутствуют следующие возможности:
- Выбор определенного домена/поддомена и персональная настройка для каждого сайта - Возможность построения различных графиков:
 - o запросов к сайту с возможностью выбора типа отображаемых запросов: общее количество запросов, разрешенные запросы, из кэша, в белом списке, всего заблокированных запросов, ошибки;
 - o объема трафика с возможностью просмотра информации за диапазон в 5 минут; o Графики времени ответа и кодов ответа с возможностью просмотра информации за диапазон в 5 минут с шагом 0-50 ms, 51-100 ms, 201-600 ms, 601-1000 ms, 1001-4000 ms;
 - o График кодов ответа с возможностью просмотра информации за диапазон в 5 минут;
 - Возможность масштабирования графиков за период 5 минут, 15 минут, 1 час, 3 часа, 6 часов, 24 часа, 3 дня, неделя, месяц;
 - Тепловая карта запросов;
 - Информация о городах и странах, откуда были запросы. Отображение в виде списка и в виде круговой (секторной) диаграммы;
 - Список и круговая (секторная) диаграмма основной локацией запросов с отображением процента;
 - Возможность скачать лог запросов;
 - Возможность управления функциями black и whitelist для определенного домена/поддомена, а именно просмотр и добавления/удаления IP адресов;
 - Возможность просмотра истории атак для определенного домена/поддомена с выбором конкретных дат и формированием PDF-отчета в реальном времени. По каждой атаке должна быть возможность просмотреть подробную информацию по цели атаки, по уровню атаки, по времени начала и конца атаки, мощность атаки, протокол и значение на момент атаки в rps / bps / cps с подробным графиком. В деталях трафика должна быть информация по запросам на сайт, объему трафика, времени ответа, кода ответа и тепловая карта с указанием топ локаций;
 - Возможность просмотра заблокированных IP адресов и истории блокировок за определенный период с указанием времени и причины блокировки;
 - Возможность смены IP backend адреса сервера/хостинга;
 - Возможность добавления субаккаунтов с настройками прав управления под каждый аккаунт отдельно;
 - Возможность смены имени домена/поддомена без дополнительных плат или обращений; - Возможность ручной настройки редиректов с одного домена на другой.
 - Возможность добавления Websocket
 - Возможность добавление e-mail адресов для получения рассылок об атаках
 - Возможность активации проактивной защиты для проверки новых клиентов по методам location, keepalive соединения, использованию User Agent и лимитам RPS
- 3.2.3. В личном кабинете обеспечивается возможность ознакомления со списком атак за указанный временной интервал. По каждой атаке существует возможность просмотреть подробную информацию по цели атаки, по уровню атаки, по времени начала и конца атаки, мощность атаки, протокол и значение на момент атаки в rps / bps / cps с подробным графиком. В деталях трафика предоставляется информация по запросам на сайт, объему трафика, времени ответа, кода ответа и тепловая карта с указанием топ локаций.
- 3.2.4. Используемые режимы Услуги:
- Полностью выключена в этом режиме защита полностью выключена. Ни при каких обстоятельствах защита не будет переключена ни каким из автоматов
 - Выключена/авто для запросов с обычных IP защита выключена. Но если IP находится в грейлисте, то уровень защиты автоматически повысится до редиректа. Если IP находится в дарклисте, то защита будет повышена до максимальной(капча). Если IP находится в блэклисте, то соединение закроется с 418 статусом.
 - Редирект/авто для запросов с обычных IP применяется редирект. Но если IP находится в грейлисте, то уровень защиты автоматически повысится до JS валидации. Если IP находится в дарклисте, то защита будет повышена до максимальной(капча). Если IP находится в блэклисте, то соединение закроется с 418 статусом.

- JS/авто для запросов с обычных IP применяется JS валидация. Для IP грейлиста/дарклиста применяется JSA. Если IP находится в блэклисте, то соединение закрывается с 418 статусом.
- JSA/авто для запросов с обычных IP применяется JSA валидация. Для IP грейлиста/дарклиста применяется капча. Если IP находится в блэклисте, то соединение закрывается с 418 статусом.
- Капча/авто для всех запросов применяется капча
- Редирект (Redirect) для всех запросов применяется редирект.
- JS для всех запросов применяется JS валидация.
- JSA для всех запросов применяется JS валидация.

3.3. Заказчику предоставляется доступ ко всем запросам, проходящим через систему Anti-DDoS, в режиме реального времени через личный кабинет и через API, с возможностью поиска и выборки запросов, построения графиков по заданной выборке, с интервалом хранения запросов не меньше 1 недели.

4. ОПИСАНИЕ УСЛУГИ «ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ (STORMWALL)»

4.1. Общие характеристики Услуги:

- 4.1.1. поддерживает режимы блокировки («в разрыв») обратный прокси-сервер (reverse proxy);
- 4.1.2. предоставляет режим блокировки («в разрыв») допускает возможность частичного или полного отключения блокировки на время настройки Услуги или регламентных работ;
- 4.1.3. имеет возможность терминирования защищенного SSL/TLS – трафика (SSL/TLS-offload), в том числе с размещением нескольких поддерживающих HTTPS WEB приложений (сайтов) на одном IP адресе, а затем упаковки обратно в SSL/TLS соединение;
- 4.1.4. Может автоматически определять статический контент в трафике приложений, а также отдельный режим его обработки для обеспечения оптимальной производительности и повышения эффективности анализа данных в подсистеме управления и мониторинга;
- 4.1.5. Может обрабатывать массовые однотипные блокируемые запросы в специальном режиме непосредственно в подсистеме захвата трафика, без передачи в подсистему анализа трафика, для обеспечения оптимальной производительности при защите от бот-активности и DDoS атак;
- 4.1.6. обеспечивает возможность контроля использования защищаемого приложения легитимными пользователями;
- 4.1.7. поддерживает схемы работы «разрешено все, что не запрещено явно», «запрещено все, что не разрешено явно», а также комбинации обеих схем, в зависимости от рассматриваемой модели угроз и критичности защищаемых приложений;
- 4.1.8. обеспечивает своевременное обнаружение факторов компрометации и возможность последующего расследования инцидентов;
- 4.1.9. Возможность разделения запросов к статическому и динамическому контенту для экономии системных ресурсов, а также ресурсов, требуемых аналитику для разбора событий (запросы к статическим ресурсам не должны отображаться в консоли мониторинга);
- 4.1.10. предоставляет возможность управления правилами принятия решений (создание, удаление, перегруппировка) с помощью графического конфигуратора через интерфейс управления.
- 4.1.11. Для всех запросов применяется капча.
- 4.1.12. поддерживает гибкие механизмы автоматического обучения для снижения затрат времени и ресурсов на настройку при внедрении и обслуживании в условиях частых изменений функционала защищаемых приложений, а также в условиях активного цикла разработки (см. подробнее ниже).

4.2. Технические характеристики Услуги:

4.2.1. Поддержка следующих ключевых возможностей:

- поддерживает протокол WebSocket, приложения, использующие NTLM-аутентификацию;
- Работа с использованием сигнатурных методов обнаружения аномалий³;

4.2.2. Защита от следующих видов атак:

- основных видов атак на веб-приложения из перечня OWASP Top 10;
- на протокол HTTP, включая атаки на переполнение буфера; синтаксических в т.ч. различных атак класса injection (внедрение команд в передаваемые данные SQL Injection, Code Injection, OS Command Injection, LDAP Injection, Path Traversal и др.); - «методом грубой силы», в т.ч. переборных атак и атак класса «умный DoS»;
- логических на приложения, в том числе от атак на механизмы аутентификации и контроля сессий и атак на бизнес-логику;
- «внутри» передаваемых данных с произвольным уровнем вложенности (атаки на бэкэнд, механизмы сериализации/десериализации и т.п.);
- на клиенты веб-приложений (CSRF, XSS);
- 0-day и 1-day атак;
- нежелательной активности с применением средств автоматизации (защита от ботов).

4.2.3. Возможность гибкой настройки различных типов моделей для каждого из защищаемых приложений, в том числе:

- определения и фильтрации статического контента;

³ В том числе наличие базового набора встроенных сигнатур в комплекте поставки для защиты от угроз OWASP top 10; поддержка распространенного открытого формата веб-сигнатур ModSecurity;

- валидации протокола HTTP, включая контроль заголовков, cookie и др.;
- рекурсивной модели синтаксического анализа запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности данных (в частности, XML, JSON, BASE64, GZIP, SOAP);
- источников – определение характеристик источника на основе параметров запроса;
- определения логических действий (бизнес-действий) в приложении, параметров логических действий и их значений, последовательностей действий, проверки успешности действий;
- идентификации, аутентификации и контроля сессий в приложении;
- защиты от переборных атак и атак типа «умный DoS» на уровне отдельных логических действий и произвольных параметров действия;
- Наличие готовых моделей валидации протокола HTTP и синтаксического анализа запросов для типового веб-приложения в комплекте поставки;
- Возможность ручной тонкой настройки моделей отдельно для каждого из логических действий и параметров, в частности настройка сигнатурного анализа, моделей параметров, конфигураций модуля защиты от переборных атак;

4.2.4. Возможность обнаружения следующих видов аномалий:

- аномалий или значимых данных как в HTTP-запросах, так и в HTTP-ответах; в работе приложения на основе настроенных позитивных моделей приложения (совпадение с моделью или наоборот – отклонение от нее);
- работы приложения на основе сопоставления значений параметров HTTP запросов/ответов с сигнатурами атак;
- аномалий и значимых параметров непосредственно внутри вложенных данных, передаваемых по протоколу HTTP без ограничений на количество уровней вложенности; в процессе работы механизмов идентификации, аутентификации, авторизации пользователей и контроля пользовательских сессий;
- аномалий, свидетельствующих о возможных попытках атак, осуществляемых «методом грубой силы» (bruteforce);
- нарушение бизнес-логики приложения или контроля выполнения бизнес-логики путем использования соответствующей позитивной модели работы приложения;

4.2.5. Механизмы подавления ложных срабатываний, доступные Заказчику: предварительного ("раннего") подавления, чтобы исключить возможность их влияния на сформированные правила принятия решений, а также чтобы предотвратить их попадание в интерфейс мониторинга;

- упрощенного ("быстрого") подавления Исполнителем непосредственно при просмотре описания выявленной аномалии;
- возможность тонкой настройки различных механизмов определения аномалий в привязке к отдельным параметрам запроса/ответа или логическим действиям в приложении.

4.2.6. Возможности работы с HTTP-транзакциями:

- Наличие настраиваемого модуля принятия решений, позволяющего выделять значимые события информационной безопасности и принимать решения относительно дальнейших действий в отношении HTTP-транзакций (запрос/ответ);
- Управление правилами принятия решений на основе данных об источнике (ip-адрес, пользователь, id сессии) и цели HTTP-транзакции (приложение, логическое (бизнес)-действие), а также обнаруженных в ней аномалиях или значимых данных;
- Поддержка следующих возможных решений: блокировать HTTP-транзакцию, пропустить HTTP транзакцию, пометить HTTP-транзакцию, модифицировать ответ;

4.2.7. Услуга обладает следующими возможностями автоматического обучения:

- определение и описание статического контента на основе анализа статистики запросов к защищаемым приложениям;
- построение рекурсивной модели синтаксического анализа данных запросов и ответов с поддержкой различных видов сжатия, кодирования и способов передачи данных с произвольным уровнем вложенности (в частности, XML, JSON, BASE64, GZIP, SOAP);
- выявление сигнатурных правил с высоким уровнем ложных срабатываний (автоматическое подавление ложных срабатываний);
- построение модели маршрутизации запросов для веб-приложения;
- построение моделей логических действий в приложении и моделей параметров этих действий, а также последовательностей (цепочек) логических действий;
- Оценка отклонения параметров логических действий в веб-приложении от статистической нормы;

4.2.8. Возможности по выполнению автоматического обучения:

- непрерывное обучение в процессе функционирования;
- периодический запуск заданий по обучению по установленному расписанию;
- ручной однократный запуск заданий по обучению;
- инкрементное (только для изменений, произошедших с момента предыдущего обучения), а также частичная ручная корректировка результатов обучения для отдельных статических ресурсов, ложных срабатываний, логических действий и т.п. без необходимости проводить обучение заново.

4.2.9. Результаты автоматического обучения полностью интерпретируемы и корректируемы Исполнителем.

5. СОСТАВ, УСЛОВИЯ И ПОРЯДОК ОКАЗАНИЯ УСЛУГИ

- 5.1. Услуги доступны для заказа как для сервисов Заказчика, функционирующих как в Облаке Cloud.ru, так и в сторонней инфраструктуре Заказчика.
- 5.2. 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.
- 5.3. Для подключения Услуг «Защита от DDoS-атак (StormWall)» и «Защита Веб-приложений (StormWall)»:
- 5.3.1. Заказчик выбирает тарифный план на основании предполагаемой полосы легитимного трафика, гарантированной доступности защищаемых сервисов и необходимой дополнительной функциональности из Таблицы № 1;
- 5.3.2. Исходя из выбранных параметров Услуг (см. п. 5.1.1.), заполняет форму Заказа Услуги, представленную в приложении № 1.CRS.3.A. и направляет её Исполнителю на адрес электронной почты уполномоченного лица;
- 5.3.3. В течение 3 (трех) рабочих дней Исполнитель обязуется согласовать предоставление Услуг Заказчику либо предоставить мотивированный отказ, при этом Стороны признают, что т.к. Услуга является партнёрской, отказ в её предоставлении может быть связан с действиями партнёра; В случае согласования предоставления Услуги, Исполнитель передает уполномоченному лицу Заказчика логина и пароль от личного кабинета Услуги, размещенной на сайте партнера.

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

Наименование тарифа	Набор опций, входящих в абонентскую плату по тарифу	Тариф/доп. опции	Диапазон на выбор, включенного в тариф легитимного трафика (после очистки, без учета трафика атак)
Защита сайта - Business ONE	Защита от атак на уровнях L3-L7 модели OSI Число доменов 2-го уровня - 1-4 100 поддоменов на домен Бесплатный SSL (Let's encrypt) Размер Black/White листов - 1000 Время реакции на запрос - до 30 мин Месячный SLA - 99,2% Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Поддержка HTTPS и HTTP/2 - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			2500 Мбит/с
			3000 Мбит/с
			3500 Мбит/с
			4000 Мбит/с
			4500 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
		GeoIP (проверки, блокировки)	-
		Фильтры по заголовкам и локациям	
		Кэширование	
		Защищенный DNS	
		Поддержка Websocket	
		Балансировка нагрузки	
		Серые списки	
		API на управление	

		Дополнительный домен	
		Дополнительный IP-адрес	
		Дополнительный Websocket	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
Защита сайта – Business 100	Защита от атак на уровнях L3-L7 модели OSI Число доменов 2-го уровня - 100 100 поддоменов на домен Бесплатный SSL (Let's encrypt) Размер Black/White листов - 1000 Время реакции на запрос - до 30 мин Месячный SLA - 99,2% Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Поддержка HTTPS и HTTP/2 - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			2500 Мбит/с
			3000 Мбит/с
			3500 Мбит/с
			4000 Мбит/с
			4500 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
		GeoIP (проверки, блокировки)	
		Фильтры по заголовкам и локациям	
		Кэширование	
		Защищенный DNS	
		Поддержка Websocket	
		Балансировка нагрузки	
		Серые списки	
		API на управление	
		Дополнительный домен	
		Дополнительный IP-адрес	
		Дополнительный Websocket	
		Дополнительные 100 доменов	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
Защита сайта – Enterprise ONE	Защита от атак на уровнях L3-L7 модели OSI Число доменов 2-го уровня - 1-4 100 поддоменов на домен Бесплатный SSL (Let's encrypt) Размер Black/White листов - 5000	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с

	Время реакции на запрос - до 15 мин Месячный SLA - 99,5% Enterprise опции: - Ролевая модель доступа к личному кабинету и логирование действий пользователей - Проактивный мониторинг (мы самостоятельно связываемся при недоступности) - Поддержка в Telegram - Персонализация страниц ошибок - Защита L7 без раскрытия SSL (анализ логов по UDP) - Возможность подключения на площадке - Возможность подключения по BGP Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Поддержка HTTPS и HTTP/2 - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)		1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			2500 Мбит/с
			3000 Мбит/с
			3500 Мбит/с
			4000 Мбит/с
			4500 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
		GeoIP (проверки, блокировки)	-
		Фильтры по заголовкам и локациям	
		Кэширование	
		Защищенный DNS	
		Поддержка Websocket	
		Балансировка нагрузки	
		Серые списки	
		API на управление	
		ГОСТ сертификаты	
		Управление антиботом (JA3/JA4 и Цепочки)	
		Доступ к логам запросов (Graylog)	
		Дополнительный домен	
		Дополнительный IP-адрес	
		Дополнительный Websocket	
		Выделенный IP-адрес	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
		Расширенное логирование 200 Гигабайт	
		Дополнительные ресурсы к логированию 1 Гигабайт	
Защита сайта – Enterprise 100	Защита от атак на уровнях L3-L7 модели OSI Число доменов 2-го уровня - 100 100 поддоменов на домен Бесплатный SSL (Let's encrypt) Размер Black/White листов - 5000 Время реакции на запрос - до 15 мин Месячный SLA - 99,5% Enterprise опции: - Ролевая модель доступа к личному кабинету и логирование действий пользователей - Проактивный	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			2500 Мбит/с
			3000 Мбит/с
			3500 Мбит/с

	мониторинг (мы самостоятельно связываемся при недоступности) - Поддержка в Telegram - Персонализация страниц ошибок - Защита L7 без раскрытия SSL (анализ логов по UDP) - Возможность подключения на площадке - Возможность подключения по BGP Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Поддержка HTTPS и HTTP/2 - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)		4000 Мбит/с
			4500 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
		GeoIP (проверки, блокировки)	-
		Фильтры по заголовкам и локациям	
		Кэширование	
		Защищенный DNS	
		Поддержка Websocket	
		Балансировка нагрузки	
		Серые списки	
		API на управление	
		ГОСТ сертификаты	
		Управление антиботом (JA3/JA4 и Цепочки)	
		Доступ к логам запросов (Graylog)	
		Дополнительный домен	
		Дополнительный IP-адрес	
		Дополнительный Websocket	
		Дополнительные 100 доменов	
		Выделенный IP-адрес	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
		Расширенное логирование 200 Гигабайт	
		Дополнительные ресурсы к логированию 1 Гигабайт	
Защита сайта – Private ONE	Защита от атак на уровнях L3-L7 модели OSI Число доменов 2-го уровня - 1-4 100 поддоменов на домен Бесплатный SSL (Let's encrypt) Размер Black/White листов - 5000 Время реакции на запрос - до 15 мин Месячный SLA - 99,9% Private опции: - опции Enterprise ONE - Выделенный TAM (Technical Account Manager), который в курсе всех нюансов клиента и предоставляет персонализированные консультации (8x5) - Круглосуточный мониторинг и техническая поддержка с приоритетным обслуживанием. Запросы	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			2500 Мбит/с
			3000 Мбит/с
			3500 Мбит/с
			4000 Мбит/с
			4500 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с

	обрабатываются в первую очередь, время реакции — до 15 минут - Еженедельные звонки для обсуждения текущего состояния защиты - Обучение работе с Личным кабинетом StormWall - Полный доступ к настройкам в Личный кабинет - Глубокая аналитика и персонализированные отчёты, в т.ч. актуальные уведомления о текущем статусе угрозы, принятых мерах и ожидаемом времени нейтрализации Общее: - Максимальная полоса очистки — до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Поддержка HTTPS и HTTP/2 - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)		8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
		Дополнительный домен	
		Дополнительный IP-адрес	
		Дополнительный Websocket	
		Выделенный IP-адрес	
		Расширение белых списков (до 5000)	
		Расширение черных списков (до 5000)	
		Расширенное логирование 200 Гигабайт	
		Дополнительные ресурсы к логированию 1 Гигабайт	
		Разовая стоимость инсталляции	
		Цена за месяц (1-летний контракт)	
		Цена за месяц (2-летний контракт)	
		Цена за месяц (3-летний контракт)	
Защита сайта – Private 100	"Защита от атак на уровнях L3-L7 модели OSI Число доменов 2-го уровня - 100 100 поддоменов на домен Бесплатный SSL (Let's encrypt) Размер Black/White листов - 5000 Время реакции на запрос - до 15 мин Месячный SLA - 99,9% Private опции: - опции Enterprise 100 - Выделенный TAM (Technical Account Manager), который в курсе всех нюансов клиента и предоставляет персонализированные консультации (8x5) - Круглосуточный мониторинг и техническая поддержка с приоритетным обслуживанием. Запросы обрабатываются в первую очередь, время реакции — до 15 минут - Еженедельные звонки для обсуждения текущего состояния защиты - Обучение работе с Личным кабинетом StormWall - Полный доступ к	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			2500 Мбит/с
			3000 Мбит/с
			3500 Мбит/с
			4000 Мбит/с
			4500 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
		Дополнительный домен	
		Дополнительный IP-адрес	
		Дополнительный Websocket	

	настройкам в Личный кабинет - Глубокая аналитика и персонализированные отчёты, в т.ч. актуальные уведомления о текущем статусе угрозы, принятых мерах и ожидаемом времени нейтрализации Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Поддержка HTTPS и HTTP/2 - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)"	Дополнительные 100 доменов	
		Выделенный IP-адрес	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
		Расширенное логирование 200 Гигабайт	
		Дополнительные ресурсы к логированию 1 Гигабайт	
		Разовая стоимость инсталляции	
		Цена за месяц (1-летний контракт)	
		Цена за месяц (2-летний контракт)	
Защита сети – Standard	Защита от атак на уровнях L3-L5 модели OSI 1 ASN (докупать нельзя) 1 туннель/подключение 100 собственных префиксов Защита от атак до 600 Гбит/с Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS Время реакции на запрос - до 60 мин Месячный SLA 99.2% Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Цена за месяц (3-летний контракт)	
		Тариф	200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			600 Мбит/с
			700 Мбит/с
			800 Мбит/с
			900 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			3000 Мбит/с
			4000 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
			15000 Мбит/с
			20000 Мбит/с
			30000 Мбит/с
			40000 Мбит/с
			50000 Мбит/с
			60000 Мбит/с
			70000 Мбит/с
			100000 Мбит/с
		Дополнительно 1000 префиксов	-

		Дополнительно 1 туннель	
		DDoS сенсор	
		Физическое подключение (единоразово)	
		Поддержка в Telegram	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
Защита сети – Business	Защита от атак на уровнях L3-L5 модели OSI 1 ASN (прямая BGP сессия, можно докупить) 1 туннель/подключение 1000 собственных префиксов Защита от атак - без ограничения по ёмкости Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS Время реакции на запрос - до 30 мин Месячный SLA 99.5% Business опции: - Индивидуальные профили защиты Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Тариф	200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
		Дополнительно 1000 префиксов	
		Дополнительно 1 AS	
		Дополнительно 1 туннель	
		DDoS сенсор	
		Физическое подключение (единоразово)	
		Поддержка в Telegram	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
Защита сети – Enterprise	Защита от атак на уровнях L3-L5 модели OSI 1 ASN (прямая BGP сессия, можно докупить) До 10 туннелей/подключений 1000 собственных/транзитных префиксов Защита от атак - без ограничения по ёмкости Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS Время реакции на запрос - до 15 мин Месячный SLA 99.9% Enterprise опции: - Индивидуальные профили защиты - DDoS-сенсор - Поддержка в чате Telegram	Тариф	600 Мбит/с
			700 Мбит/с
			800 Мбит/с
			900 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			3000 Мбит/с
			4000 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с

	Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)		15000 Мбит/с
			20000 Мбит/с
			30000 Мбит/с
			40000 Мбит/с
			50000 Мбит/с
			60000 Мбит/с
			70000 Мбит/с
			100000 Мбит/с
		Дополнительно 1000 префиксов	-
		Дополнительно 1 AS	
		Дополнительно 1 туннель	
		Физическое подключение (единоразово)	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
Защита сети – Private	Защита от атак на уровнях L3-L5 модели OSI 1 ASN (прямая BGP сессия, можно докупить) До 10 туннелей/подключений 1000 собственных/транзитных префиксов Защита от атак - без ограничения по ёмкости Типы подключения: Физическое подключение на MMTC-9, GRE-туннель, MPLS Время реакции на запрос - до 15 мин Месячный SLA 99.9% Enterprise опции: - Индивидуальные профили защиты - DDoS-сенсор - Поддержка в чате Telegram Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Тариф	600 Мбит/с
			700 Мбит/с
			800 Мбит/с
			900 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			3000 Мбит/с
			4000 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
			15000 Мбит/с
			20000 Мбит/с
			30000 Мбит/с
			40000 Мбит/с
			50000 Мбит/с
			60000 Мбит/с
			70000 Мбит/с
		Дополнительно 1000 префиксов	-
		Дополнительно 1 AS	
		Дополнительно 1 туннель	
		Физическое подключение (единоразово)	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
		Разовая стоимость инсталляции	
		Цена за месяц (1-летний контракт)	
		Цена за месяц (2-летний контракт)	

		Цена за месяц (3-летний контракт)	
Защита сервисов – Standard	Защита от атак на уровнях L3-L5 модели OSI 1 туннель/подключение 100 собственных префиксов Защита от атак до 600 Гбит/с Типы подключения: GRE-туннель, L4 прокси Время реакции на запрос - до 60 мин Месячный SLA 99.2% Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			600 Мбит/с
			700 Мбит/с
			800 Мбит/с
			900 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			3000 Мбит/с
			4000 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
			15000 Мбит/с
			20000 Мбит/с
			30000 Мбит/с
			40000 Мбит/с
			50000 Мбит/с
			60000 Мбит/с
			70000 Мбит/с
			100000 Мбит/с
Защита сервисов – Business	Защита от атак на уровнях L3-L5 модели OSI 1 туннель/подключение 1000 собственных префиксов Защита от атак - без ограничения по ёмкости Типы подключения: GRE-туннель, L4 прокси Время реакции на запрос - до 30 мин Месячный SLA 99.5% Business опции: - Индивидуальные профили защиты	Тариф	50 Мбит/с
			100 Мбит/с
			200 Мбит/с
			300 Мбит/с
			400 Мбит/с
			500 Мбит/с
			-
			-

	Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Расширение черных списков (по 1000)	
Защита сервисов – Enterprise	Защита от атак на уровнях L3-L5 модели OSI До 10 туннелей/подключений 1000 собственных/транзитных префиксов Защита от атак - без ограничения по ёмкости Типы подключения: GRE-туннель, L4 прокси Время реакции на запрос - до 15 мин Месячный SLA 99.9% Enterprise опции: - Индивидуальные профили защиты - Поддержка в чате Telegram Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет-систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)	Тариф	600 Мбит/с
			700 Мбит/с
			800 Мбит/с
			900 Мбит/с
			1000 Мбит/с
			1500 Мбит/с
			2000 Мбит/с
			3000 Мбит/с
			4000 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
			15000 Мбит/с
			20000 Мбит/с
			30000 Мбит/с
			40000 Мбит/с
			50000 Мбит/с
			60000 Мбит/с
			70000 Мбит/с
			100000 Мбит/с
		Дополнительно 1 туннель	-
		Дополнительный IP-адрес (для того же туннеля)	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
Защита сервисов – Private	Защита от атак на уровнях L3-L5 модели OSI До 10 туннелей/подключений 1000 собственных/транзитных префиксов Защита от атак - без	Тариф	600 Мбит/с
			700 Мбит/с
			800 Мбит/с
			900 Мбит/с
			1000 Мбит/с

	ограничения по ёмкости Типы подключения: GRE- туннель, L4 прокси Время реакции на запрос - до 15 мин Месячный SLA 99.9% Enterprise опции: - Индивидуальные профили защиты - Поддержка в чате Telegram Общее: - Максимальная полоса очистки – до 5 Тбит/с - Режим технической поддержки – 24/7 по почте, через тикет- систему и по телефону - Личный кабинет (аналитика, отчеты, настройки защиты) - Возможность заключения договора / безналичной оплаты - Настройка уведомлений (Telegram, email, webhook)		1500 Мбит/с
			2000 Мбит/с
			3000 Мбит/с
			4000 Мбит/с
			5000 Мбит/с
			6000 Мбит/с
			7000 Мбит/с
			8000 Мбит/с
			9000 Мбит/с
			10000 Мбит/с
			15000 Мбит/с
			20000 Мбит/с
			30000 Мбит/с
			40000 Мбит/с
			50000 Мбит/с
			60000 Мбит/с
			70000 Мбит/с
		Дополнительно 1 туннель	-
		Дополнительный IP-адрес (для того же туннеля)	
		Расширение белых списков (по 1000)	
		Расширение черных списков (по 1000)	
		Разовая стоимость инсталляции	
		Цена за месяц (1-летний контракт)	
		Цена за месяц (2-летний контракт)	
		Цена за месяц (3-летний контракт)	
WAF - T1	-	Тариф	100 RPS
			300 RPS
			500 RPS
			700 RPS
			1000 RPS
			1500 RPS
			2000 RPS
			3000 RPS
			5000 RPS
			7000 RPS
			10000 RPS
		Дополнительное веб приложение	-
WAF - T2	-	Тариф	100 RPS
			300 RPS
			500 RPS
			700 RPS
			1000 RPS
			1500 RPS
			2000 RPS
			3000 RPS

			5000 RPS
			7000 RPS
			10000 RPS
		Дополнительное веб приложение	-
WAF - T3	-	Тариф	100 RPS
			300 RPS
			500 RPS
			700 RPS
			1000 RPS
			1500 RPS
			2000 RPS
			3000 RPS
			5000 RPS
			7000 RPS
			10000 RPS
		Дополнительное веб приложение	
Cloud Application Firewall (uC-WAF)	-	Тариф	100 RPS
			300 RPS
			500 RPS
			750 RPS
			1000 RPS
			2000 RPS
			3000 RPS
			4000 RPS
			5000 RPS
			10000 RPS

6. ТАРИФИКАЦИЯ УСЛУГИ

- 6.1. Расчетным периодом является календарный месяц.
- 6.2. Оплата за Услуги состоит из фиксированной оплаты по тарифу и переменной частей (за превышение легитимной пропускной способности и/или количество запросов в секунду (RPS)).
- 6.3. Размер фиксированной платы, определяется на основании выбранного тарифа.
- 6.4. Сумма оплаты за превышение легитимной пропускной способности и/или количество запросов в секунду (RPS) рассчитывается по следующей формуле:

Если $Y > R$

$$P = (T + F * (Y - R))$$

P - Ежемесячный платеж за Услугу.

T - Цена за 1 месяц пользования по тарифу.

F - Цена за 1 Мбит/с превышения и/или цена за 1 RPS превышения, указанная в Спецификации в Приложении № 1 к Договору.

R - Легитимная пропускная способность, включенная в подписку.

Y - Фактически использованная легитимная пропускная способность по 95 перцентилю за расчетный период. Легитимная полоса пропускания, включенная в подписку, может быть превышена на 36 часов за каждый расчетный период (5% времени в месяц). Используемая полоса пропускания измеряется делением количества переданных данных на 5 минутный интервал. По окончании расчетного периода 5% от максимальных значений удаляются. Затем из оставшихся 95% выбирается максимальное число, которое используется для расчета.

7. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГАМ

- 7.1. Возможные виды подключения / изменения / отключения Услуг:
 - 7.1.1. Посредством подписания Заказа⁴.
- 7.2. Возможный порядок расчётов по Услугам:
 - 7.2.1. Постоплата.
- 7.3. Возможные способы оплаты / порядок пополнения Баланса:
 - 7.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта.

⁴ С учётом особенностей, изложенных в разделе 6 настоящего Приложения.