Система защиты от DoS/DDoS атак CyberFlow

руководство пользователя

Москва, 2023

Содержание

1. Назначение программы

CyberFlow – это программно-аппаратный комплекс на основе искусственного интеллекта, направленный на обеспечение защиты интернет-ресурсов от кибератак.

Система постоянно просматривает все потоки данных, идущие к серверу, отслеживает аномалии и автоматически определяет тип идущей атаки. По результатам анализа происходит динамическая подстройка параметров защиты с использованием BGP FlowSpec и API нашей системы. На аппаратных фильтрах блокируется основная часть TCP/UDP-флуда. Благодаря использованию аппаратных фильтров, удаётся добиться огромной скорости обработки пакетов. На фильтрах точной очистки блокируются самые изощрённые атаки, в том числе, с использованием ботов. Сеть фильтрации построена таким образом, чтобы равномерно распределять нагрузку на несколько аппаратных фильтров.

Система CyberFlow имеет личный кабинет, в котором пользователь системы может отслеживать: статистику трафика, время и коды ответа бэкенда, статистику заблокированных IP-адресов, список атак и прочее. Все управление на уровне пользователя системой осуществляется в личном кабинете.

2. Условия эксплуатации

CyberFlow является закрытой системой. Весь исходный код системы защиты расположен на серверах компании ООО «СайберФёст». Компания или физическое лицо, которая хочет подключить систему защиты от DoS/DDoS атак CyberFlow, должна заключить договор с компанией ООО «СайберФёст».

Защита ресурсов обеспечивается посредством изменения DNS-записей интернет-сервисов с целью направления всех запросов на аппаратно-программный комплекс защиты от DDoS-атак CyberFlow либо путем прозрачной фильтрации трафика при его маршрутизации посредством протокола BGP.

Заказчику предоставляется доступ к личному кабинету, в котором отображаются все его услуги, находящиеся под защитой, также создается чат для оперативного реагирования.

3. Требования к рабочему месту пользователя

Для входа в личный кабинет потребуется устройство с возможностью доступа в Интернет, которое поддерживает веб-браузер: Спутник, Яндекс Браузер, Google Chrome, Microsoft Edge, Mozilla Firefox или Opera.

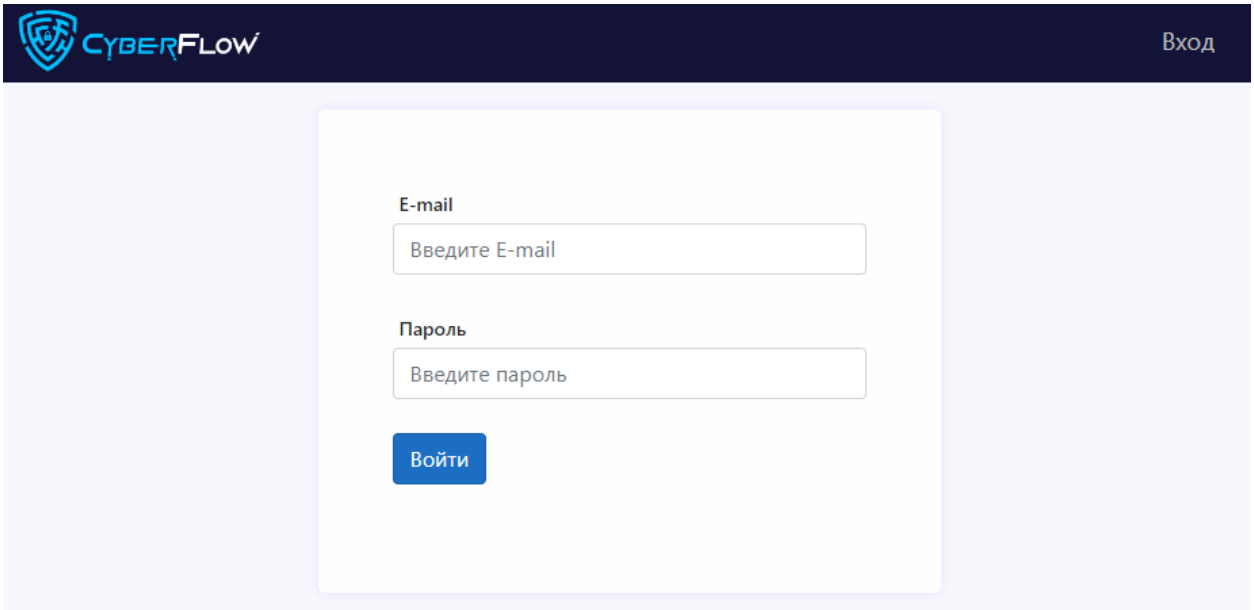
Для корректной работы данных браузеров, ваше устройство должно подходить под их системные требования. Скорость интернет-соединения на данном устройстве не должно быть ниже 10 MB/сек.

4. Вход в личный кабинет

4.1. Для входа в личный кабинет в адресной строке браузера введем https://lk.cyberfirst.ru

добавить скриншот

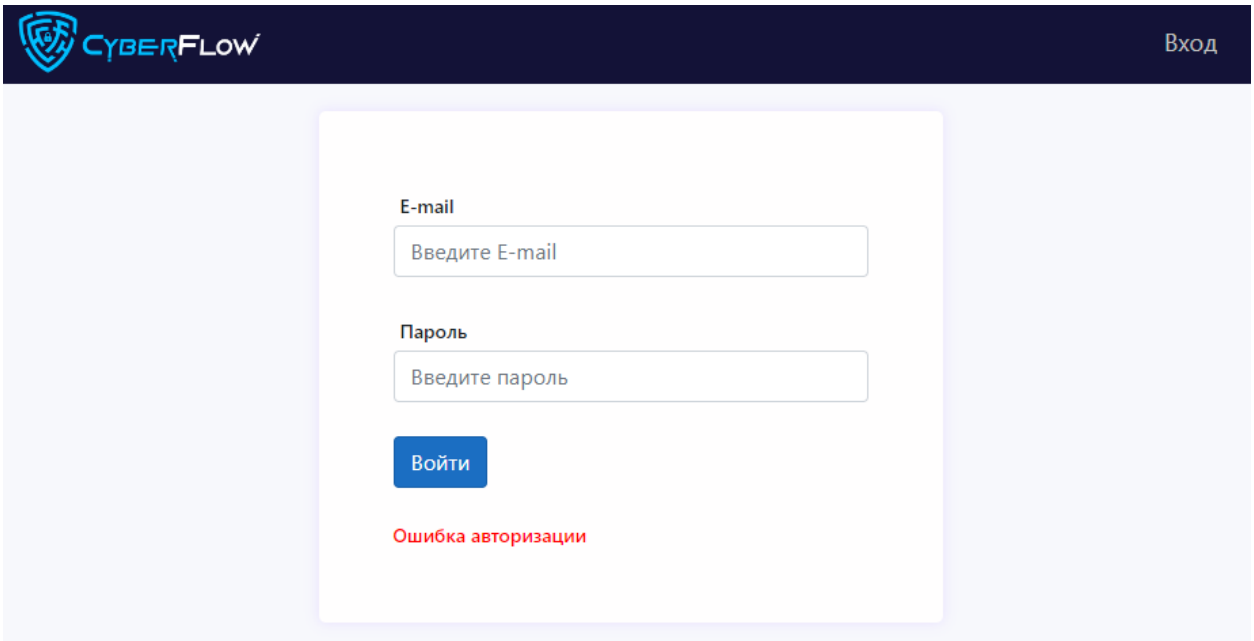
4.2. В открывшемся окне введем электронный адрес вашей учетной записи и пароль.



Если данные введены корректно, то откроется личный кабинет, где отобразиться ваши услуги.

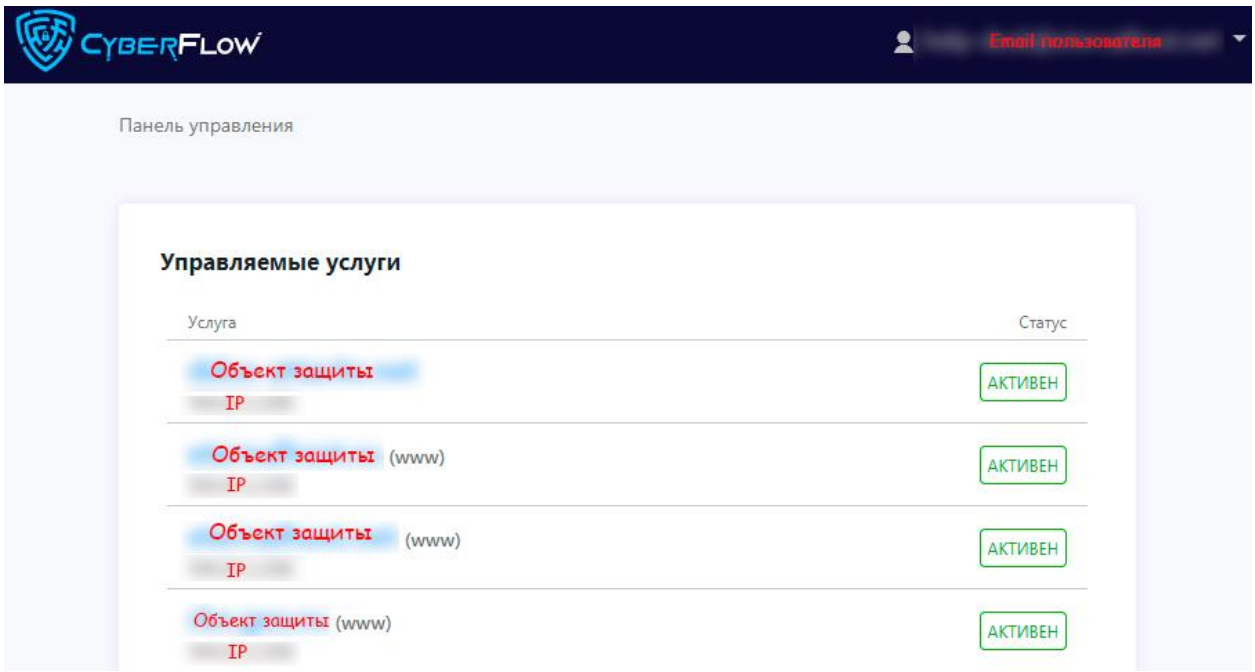
5. Восстановление доступов к личному кабинету

Если при попытке входа в личный кабинет появилась ошибка авторизации, обратитесь в техническую поддержку: support@cyberflow.ru

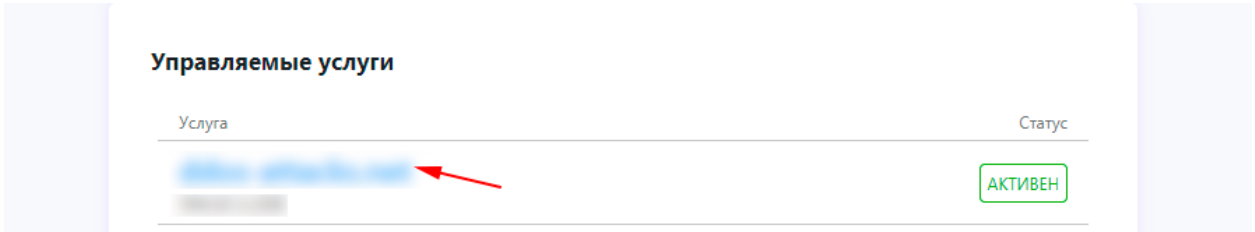


6. Выбор управляемой услуги

После удачного входа в личный кабинет, вы увидите список услуг, прикрепленных к вашему аккаунту.



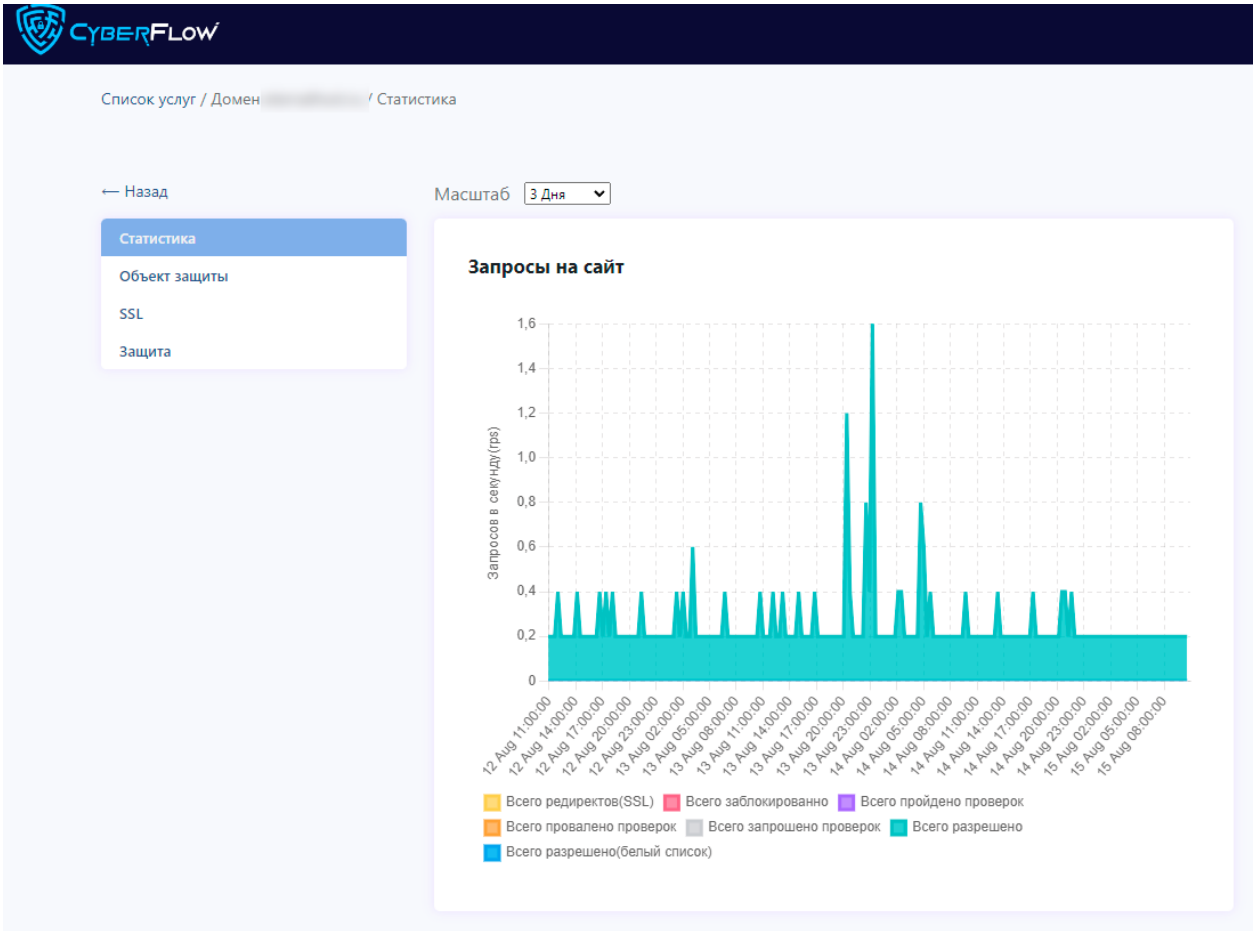
В качестве объекта защиты у вас будут отображаться домены, IP-адреса или подсети. Если напротив объекта защиты стоит статус «Активен», то можно получить информацию по данной услуге. Для этого нужно нажать на активную ссылку объекта защиты.



Если напротив объекта защиты стоит статус «Не активен», то обратитесь в техническую поддержку по электронной почте support@cyberflow.ru, для уточнения причин отключения услуги.

7. Выбор нужных данных для управляемой услуги

После переходы к выбранной управляемой услуге, откроется панель управления данной услугой. В меню, расположенном в левом столбце или сверху, можно выбрать нужный раздел по данной услуге. Расположение меню зависит от разрешения окна вашего браузера.



Расположение меню в левом столбце

Верхнее расположение меню при низком разрешение браузера

В меню можно выбрать нужный раздел для отображения:

- Статистика (п.8, стр.11)
- Объект защиты (п.9, стр.16)
- SSL (п.10, стр.17)
- Защита (п.11, стр.19)

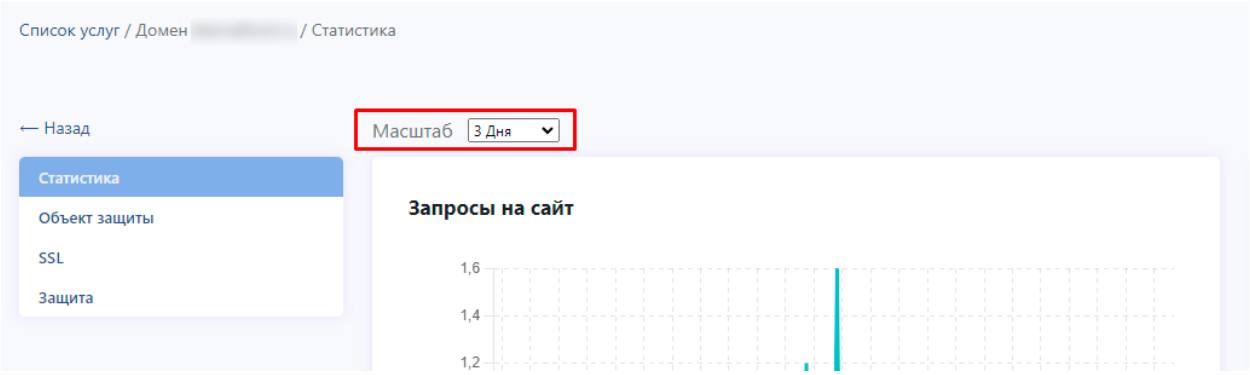
8. Отображение статистики

В разделе «Статистика» выводятся данные о работе системы защиты CyberFlow. Данные выводятся в виде графиков. Графики разбиты на типы:

- Запросы на сайт
- Объем трафика
- Время ответа бэкенда
- Коды ответа бэкенда
- Блокировки IP
- Топ блокировок IP по странам

8.1. Выбор масштаба статистики

В разделе статистика вверху можно выставить параметр «Масштаб». Масштаб – это параметр, который позволяет отобразить статистику за выбранный период.



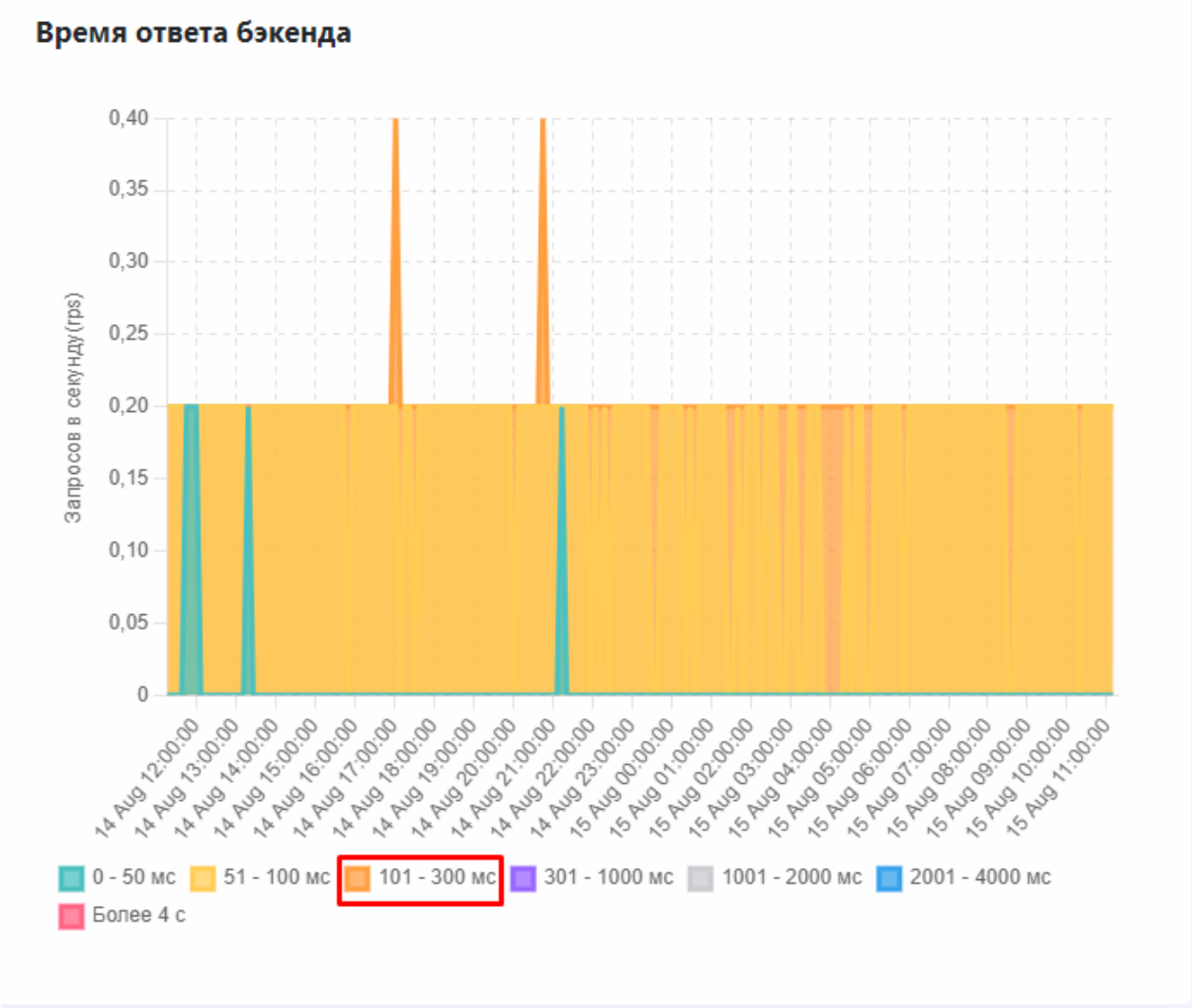
Можно установить следующие значения для масштаба:

- 5 минут
- 15 минут
- Час
- 3 часа
- 6 часов
- 24 часа
- 3 дня
- 7 дней
- 30 дней

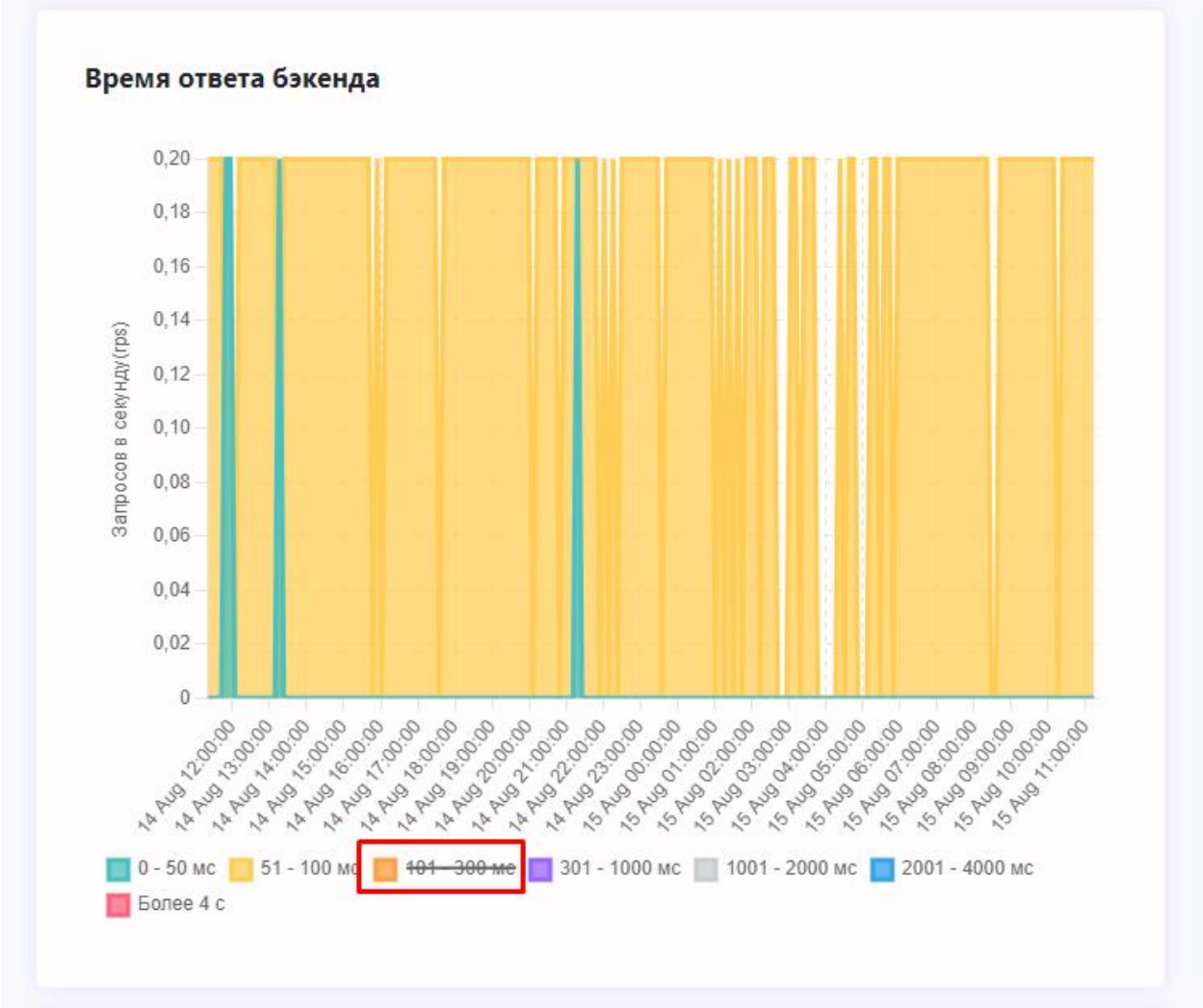
8.2. Отключение данных в графике

В разделе статистика для каждого графика можно отключать конкретные параметры для отображения. Для этого нужно нажать на параметр под графиком, который мы хотим убрать для отображения.

К примеру, отключим параметр «100 – 300 мс» на графике Время ответа бэкенда. Для это один раз нажмем курсором мыши на данный параметр.



Данный параметр станет зачеркнут, его данные пропадут с графика, если у данного параметра были максимальные значения, то график будет перестроен в соответствии с новыми максимальными значениями.

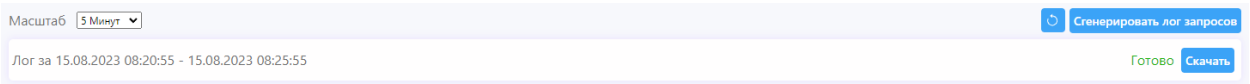


Если нужно снова включить данный параметр, то нужно снова нажать на него курсором мыши или обновить страницу браузера.

8.3. Генерация и выгрузка лога запросов

В разделе статистика можно сгенерировать лог запросов. Для этого в верхнем меню нажмите «Сгенерировать лог запроса».

Лог запроса будет сгенерирован в соответствии с установленным параметром Масштаб. По завершению создания лога появится надпись «Лог за…» (где будет указан параметр согласно выбранному Масштабу), появится зеленый индикатор «Готов» и активная кнопка «Скачать».



Для выгрузки лога нажмем кнопку «Скачать». После нажатия на ваш компьютер будет скачан файл в формате CSV. Открыть его можно с помощью Microsoft Excel или программ с аналогичным функционалом.

9. Объект защиты

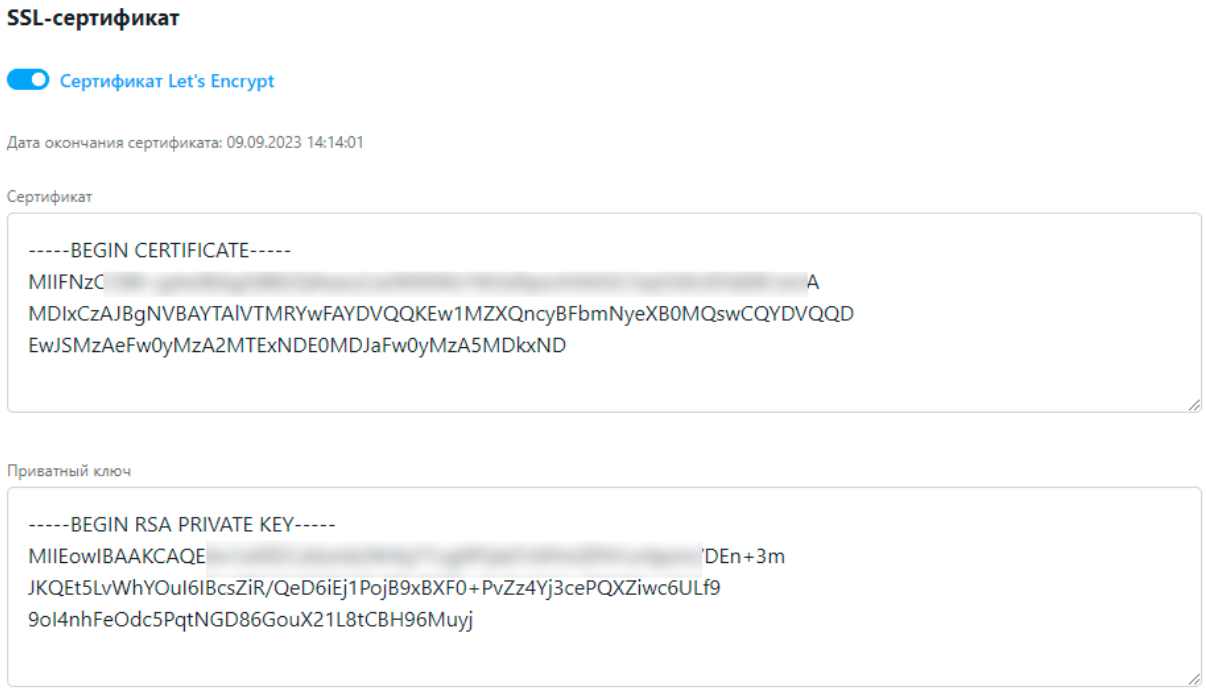
В разделе «Объект защиты» выставляется значение для защищаемого ресурса. Как правило, это backend-сервер.

10. Подключение SSL-сертификата

В разделе «SSL» можно выполнить подключение SSL-сертификата и настроить редирект.

Для подключение бесплатного Let's Encrypt сертификата включите данный параметр. Let's Encrypt сертификат будет сгенерирован автоматически.

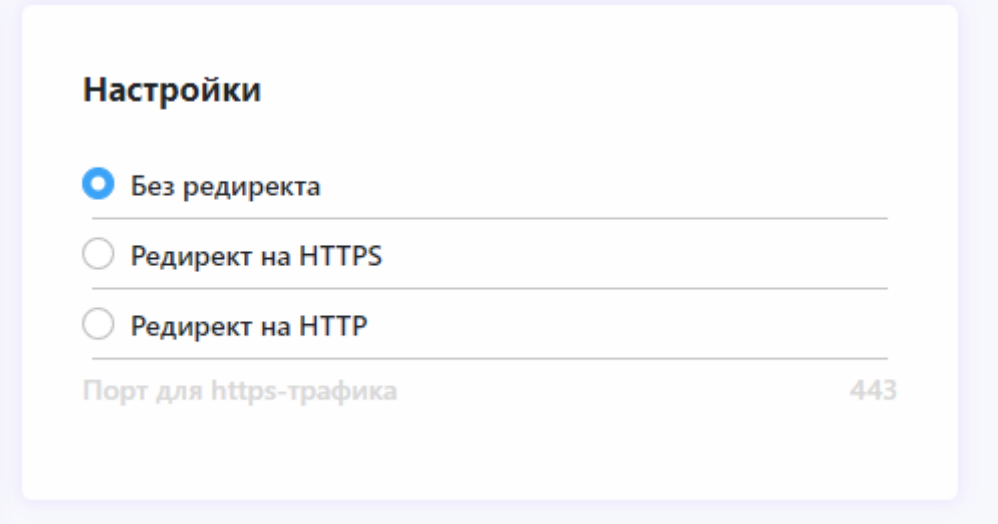
Если у вас есть существующие сертификат, то отключите параметр «Сертификат Let's Encrypt» и в разделы Сертификат и Приватный ключ внесите данные своего сертификата.



Для настройки редиректа в столбце «Настройки» выберите нужный вам параметр:

- Без редиректа

- Редирект на HTTPS
- Редирект на HTTP

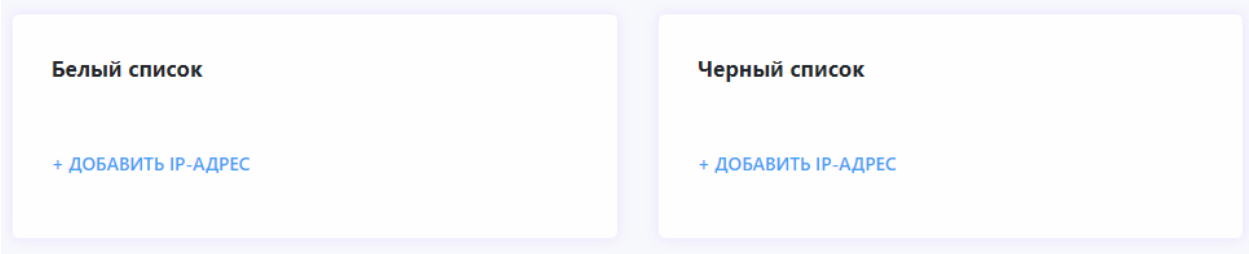


По умолчанию для https трафика используется 443 порт.

11. Пользовательская настройка фильтров

В разделе «Защита» пользователь может настроить белые и черные списки, выставить настройки защиты и Location filters.

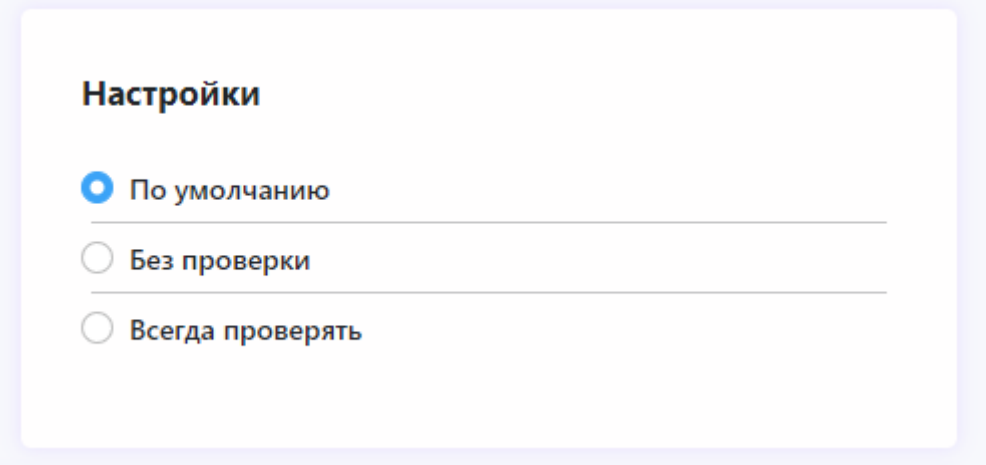
Для добавления IP-адреса в белый или черный список нажмите «ДОБАВИТЬ IP-АДРЕС» в нужном столбце.



Белый список – это доверенные адреса, которые не проходят фильтрацию.

Черный список – это запрещенные адреса, которые не имеют доступы к сервису не зависимо от того какой трафик с них идет.

В столбце «Настройки» можно выставить параметры по умолчанию для Location.



Выбрать можно из параметров:

- По умолчанию
- Без проверки
- Всегда проверять

В столбце «Location filters» можно создать дополнительные фильтры, в которых указываются действия, методы и таймер фильтации.