



Стандартное подключение в режиме проксирования

По всем возникающим техническим вопросам вы можете обратиться в техническую поддержку:

- Посредством сообщения на support@curator.pro
- Через личный кабинет в разделе Заявки/Tickets

Информация, необходимая для регистрации и подключения:

1. Учетные данные для входа в ЛК CURATOR
2. Имя сайта/ваш домен
3. TLS-сертификаты для ваших доменов для подключения к сети CURATOR. В случае отсутствия TLS-сертификата, возможен его выпуск в личном кабинете CURATOR.

Добавление домена:

1. Войдите в личный кабинет CURATOR, используя данные из письма в вашей электронной почте
2. В левой панели выберите Домены — справа сверху нажмите “ДОБАВИТЬ ДОМЕН”
3. В открывшемся диалоговом окне введите название домена, это текстовое поле (например: Тестовый сайт). Это название будет отображаться в списке ваших доменов.

Если ваш ресурс находится под атакой, то отметьте это флажком. В ином случае флажок устанавливать не нужно.

4. Укажите IP-адрес вашего ресурса или укажите доменное имя (например: test.ru) и воспользуйтесь функцией DNS поиск. После заполнения поля нажмите Создать.
5. Ваш домен будет включен службой технической поддержки CURATOR в течение одного часа и его статус будет изменен с “Модерируется” на “Онлайн”. Обычно ответ об активации приходит в течение 30 минут на указанный при регистрации email. Также для вас выпустят защищенный CURATOR IP.

До активации домен будет находиться в статусе «Модерируется», но вы можете продолжить настройку по этой инструкции не дожидаясь окончания модерации.

6. Сеть CURATOR будет пропускать очищенный трафик только по тем портам и протоколам, для которых создана настройка в личном кабинете. Такая настройка будет иметь название "Сервис". Во время создания вашего домена мы автоматически настроили сервис для порта 80, то есть HTTP-трафика.

Для настройки фильтрации HTTPS-трафика по порту 443 необходимо создать дополнительный сервис

- 1.1. Первым шагом добавьте файлы TLS-сертификата и закрытого ключа для вашего доменного имени в пункте левого меню «Хранилище сертификатов» или по [ссылке](#). Нажмите «Добавить сертификат» и выберите нужные файлы. После обработки этих файлов личным кабинетом нажмите кнопку «Добавить сертификат» в самом низу страницы.
- 1.2. Затем установите сертификат из хранилища для домена. Это можно сделать в текущем окне по кнопке «Установить сертификат» или перейдя в настройки вашего домена, в которые можно попасть из левого меню по кнопке «Домены». Также можно воспользоваться этой [ссылкой](#). Далее уже в правом меню откройте пункт «TLS». Для установки сертификата потребуется указать доменные имена для которых он будет использоваться или установить флажок «Использовать данный сертификат по умолчанию для любого доменного имени». Один из ваших сертификатов обязательно должен быть установлен по умолчанию.
- 1.3. Перейдите в раздел «Сервисы» в правом меню и добавьте сервис для работы по протоколу HTTPS:
 - 1.3.1. Нажмите на кнопку «Добавить», выберите тип HTTP и укажите порт 443. Установите флажок «Использовать TLS»;
 - 1.3.2. Нажмите «Настройка апстримов» и добавьте апстрим в группу основных апстримов нажав на кнопку «Добавить апстрим» в колонке «Основной»;
 - 1.3.3. Воспользуйтесь кнопкой с волшебной палочкой или вручную укажите IP-адрес и порт. Поле «Название» опционально;
 - 1.3.4. Нажмите последовательно «Добавить» в окне добавления основного апстрима, «Сохранить» в окне апстримов, «Добавить» на виджете добавления сервиса и «Сохранить» на экране всех сервисов.

Вы можете найти документацию для других типов сервисов по ссылкам: [websocket](#), [tcp-proxy](#), [tcp](#).

Мы рекомендуем вам провести тестирование, прежде чем вы начнете отправлять все запросы пользователей через облако CURATOR, чтобы убедиться, что ресурс работает корректно с подключенной защитой. Для этого попробуйте выполнить запросы к веб-сайту со своего устройства, используя выданный вам CURATOR IP. Это можно сделать из терминала с помощью утилиты cURL или вручную отредактировав файл hosts. Подробную информацию можно найти по [ссылке](#).

Перенаправьте трафик на облако CURATOR, изменив DNS для вашей доменной зоны таким образом, чтобы А-запись домена содержала CURATOR IP. Обратите внимание, что менять записи DNS необходимо на стороне используемых вами серверов имен.

Как правило, записи должны иметь следующий вид:

@ IN A <CURATOR IP>

WWW IN A <CURATOR IP>

Если требуется поставить под защиту несколько доменных имен, расположенных на одном сервере, то вам необходимо повторить процедуру для каждого доменного имени.

После изменения DNS запросы на ваш веб-сайт начнут поступать с IP-адресов системы фильтрации трафика CURATOR. Список адресов вы можете найти по [ссылке](#).

Чтобы предотвратить прямые атаки, нацеленные на IP-адрес апстрима (в обход CURATOR), мы рекомендуем ограничить доступ к серверу, заблокировав запросы для всех, кроме списка IP-адресов узлов CURATOR. Инструкции по настройке брандмауэра можно найти по ссылке выше.

После того, как трафик начнет проходить через сеть фильтрации CURATOR, реальные IP-адреса пользователей будут сохранены в HTTP-заголовке X-Forwarded-For. Вы можете найти инструкцию по извлечению данных из этого HTTP-заголовка по [ссылке](#).

Если у вас есть какие-либо отзывы или вопросы по поводу сервиса, не стесняйтесь обращаться к нам через систему заявок в вашем личном кабинете или по электронной почте: support@curator.pro.