

Документация Curator

Архитектура сети, подключение сервисов и работа в личном кабинете Curator

Содержание

01	Обзор	5
1.1	Архитектура сети Curator	6
	ТЕХНОЛОГИИ	
1.2	Обзор технологий	8
1.3	Защита от ботов	9
1.4	Работа с CDN	10
1.5	Перенаправление с установкой cookie	12
1.6	Обратный HTTP-прокси	17
1.7	Обратный TCP-прокси	22
1.8	Обратный WebSocket-прокси	25
1.9	Балансировка нагрузки	27
1.10	Ingress-фильтрация	31
1.11	HTTP-перенаправления	35
1.12	Защищённый DNS	38
02	Подключение к Curator	40
2.1	Обзор способов подключения	41
2.2	Защита от ботов	42
2.3	Обратный HTTP-прокси	46
2.4	Ingress-фильтрация	49
2.5	Обратный TCP-прокси	51
2.6	Обратный WebSocket-прокси	54
2.7	Туннели	56
2.8	Curator.CDN	60
2.9	Передача лог-файлов	64
2.10	BGP	77
2.11	Защищённый DNS	79

03	Личный кабинет	81
3.1	Обзор интерфейса	82
	СПИСКИ РЕСУРСОВ	
3.2	Домены	87
3.3	Сервисы	90
3.4	Префиксы	93
	CURATOR	
3.5	Статистика	96
3.6	Сервисы	101
3.7	IP-адреса	109
3.8	Порты и протоколы	111
3.9	TLS	117
3.10	Списки IP	120
3.11	Туннели	123
3.12	Настройки фильтров	127
3.13	HTTP-перенаправления	132
3.14	Страницы ошибок	136
3.15	Уведомления	139
	BOT PROTECTION	
3.16	Сводка	141
3.17	Локации	145
3.18	Посетители	151
3.19	Подписи	157
	CDN	
3.20	CDN	162
3.21	Настройки	166
3.22	Утилиты	175
3.23	Хранилище сертификатов	177
	ПРАВА ДОСТУПА	
3.24	API токены	186
3.25	Пользователи	189
3.26	Группы	194
3.27	Уведомления	200

3.28	Мой профиль	201
3.29	SSO	204
04	Справка и поддержка	211
4.1	Дополнительные HTTP-заголовки	212

CURATOR

01

Обзор

Архитектура сети Curator

Технологии

Архитектура сети Curator

Распределённая сеть Curator спроектирована так, чтобы клиенты, трафик к которым через неё проходит, могли рассчитывать на высокий SLA даже под большими нагрузками.

Сеть состоит из нескольких *центров очистки трафика*, входящих в одну автономную систему (AS, autonomous system). Каждый центр очистки трафика может работать независимо от остальных: поступивший пользовательский трафик анализируется и, если он признан легитимным, направляется в сеть клиента.

Для направления трафика в ближайший центр очистки трафика используется технология BGP Anycast. Это означает, что любой центр очистки трафика может ответить на запрос пользователя, направленный к одному и тому же IP-адресу из сети Curator.

Также благодаря использованию BGP Anycast маршрутизаторы, через которые проходит пользовательский трафик в интернете, предпочитают маршрут до топологически ближайшего к пользователю доступного центра очистки трафика. Именно с ним для пользователя будет возможен максимально быстрый обмен трафиком.

Каждый центр очистки трафика имеет прямую связь с магистральными провайдерами Tier-1. Благодаря этому сеть Curator остаётся доступной даже при авариях у отдельных провайдеров.



ПРИМЕЧАНИЕ

На сегодняшний день в сеть Curator входит 21 центров очистки трафика в Северной Америке, Европе, странах Ближнего Востока, Азии, России и СНГ. Суммарная пропускная способность сети — более 6000 Гбит/с.

Средняя доступность приложений клиентов Curator в 2021 году составила 99,9875%. Если доступность в течение какого-либо месяца составляет меньше, чем SLA, обещанный в тарифе, то клиент не оплачивает данный месяц.

Приём трафика от пользователя

В рамках первоначальной подготовки к работе клиент при помощи специалистов технической поддержки Curator обеспечивает необходимые настройки, чтобы весь трафик от пользователей шёл в сеть клиента не напрямую, а через центры очистки трафика.

Конкретные шаги, необходимые для настройки приёма трафика, зависят от выбранного способа подключения и описаны в соответствующей документации.

Анализ трафика

Цель Curator — отправить в сеть клиента только *легитимный* пользовательский трафик, то есть трафик, не являющийся частью атак. Для этого на центрах очистки трафика Curator производится анализ трафика на всех уровнях сетевой модели OSI/ISO.

Чтобы определять атаки, Curator применяет поведенческие, эвристические и сигнатурные алгоритмы. Также Curator автоматически настраивает методы фильтрации, используя для обучения структуру трафика без DDoS-атак. Это позволяет с высокой точностью определять даже атаки уровня приложений (L7 по модели OSI/ISO), которые похожи на действия обычных пользователей, а также позволяет отличать DDoS-атаки от повышенного интереса посетителей к сайту.



ПРИМЕЧАНИЕ

Количество ложных срабатываний при атаке не превышает 5%.

Статистика об обнаруженных атаках доступна клиенту в личном кабинете. Также информацию об атаках можно получать через [API](#), что позволяет интегрировать Curator с системой мониторинга, Security operation center (SOC) или Security information and event management (SIEM), чтобы получать оповещения в удобном для клиента формате.

Клиент может настроить чёрные и белые списки, которые будут влиять на обработку трафика. Это может быть сделано как в личном кабинете, так и через API.

Отправка трафика клиенту

Для связи с оборудованием клиента могут использоваться различные технологии в зависимости от того, какими техническими возможностями клиент располагает и какой набор услуг ему необходим.

Подробнее о разных способах организации канала между Curator и клиентом читайте в разделе [Подключение](#).

Для многих из услуг, предоставляемых Curator, возможны балансировка или резервирование соединений с сетью клиента. При этом каждый центр очистки трафика может независимо от других отслеживать состояние каждого апстрима клиента, чтобы динамически изменять список используемых соединений. Например, если туннель до одного из апстримов станет недоступным из определённого региона, центр очистки трафика в этом регионе может автоматически переключиться на использование туннеля до другого апстрима, чтобы сохранить доступность ресурса для пользователей.

Обзор технологий

- Защита от ботов
- Технологии: Работа с CDN
- Перенаправление с установкой cookie
- Обратный HTTP-прокси
- Технологии: Обратный TCP-прокси
- Технологии: Обратный WebSocket-прокси
- Балансировка нагрузки
- Технологии: Ingress-фильтрация
- Технологии: Защищённый DNS-сервер

Защита от ботов

Угрозу для многих сайтов представляют *боты*. Под этим термином подразумевается множество разновидностей инструментов, с помощью которых конкуренты и злоумышленники совершают автоматические запросы. Боты могут быть как небольшими скриптами, так и сложными программными комплексами, которые применяют различные методы маскировки под браузеры обычных пользователей. Несмотря на то, что боты редко создают высокую нагрузку на сайт, они могут совершать несанкционированные действия, угрожать безопасности пользовательских данных и нарушать корректную работу сайта.

Основные угрозы, которые могут создавать боты:

- **Парсинг данных.**

Как владелец сайта, вы можете не хотеть, чтобы боты ваших конкурентов автоматически скачивали и обрабатывали информацию, размещённую у вас. Поэтому такие боты могут не угрожать работоспособности сайта, но представлять угрозу для вашего бизнеса.

Автоматический обход страниц и извлечение данных из них называется *парсингом*. Решение от Curator затрудняет парсинг, проверяя цифровые отпечатки (digital fingerprints) пользователей с помощью кода на JavaScript. По умолчанию защита работает прозрачно для легитимных пользователей, создавая минимальные задержки в работе и не прибегая к «капчам» и другим решениям, которые бы ухудшили восприятие сайта.

Для борьбы с парсингом данных используются:

- [обратный HTTP-прокси](#),
- [перенаправление с установкой cookie](#).

- **Брутфорс.**

Часто боты создаются, чтобы узнать некоторую информацию методом перебора. Например, боты могут осуществлять большое количество попыток авторизации, пробуя разные пароли. Таким же способом же могут быть подобраны секретные ссылки, промокоды и прочие параметры, которые вы не хотели бы делать публичными. Такая деятельность называется *брутфорсом*.

Curator распознаёт брутфорс и точно блокирует трафик с тех публичных IP-адресов, откуда приходят такие запросы. Это позволяет ограничивать деятельность ботов с минимальным ущербом для легитимных пользователей.

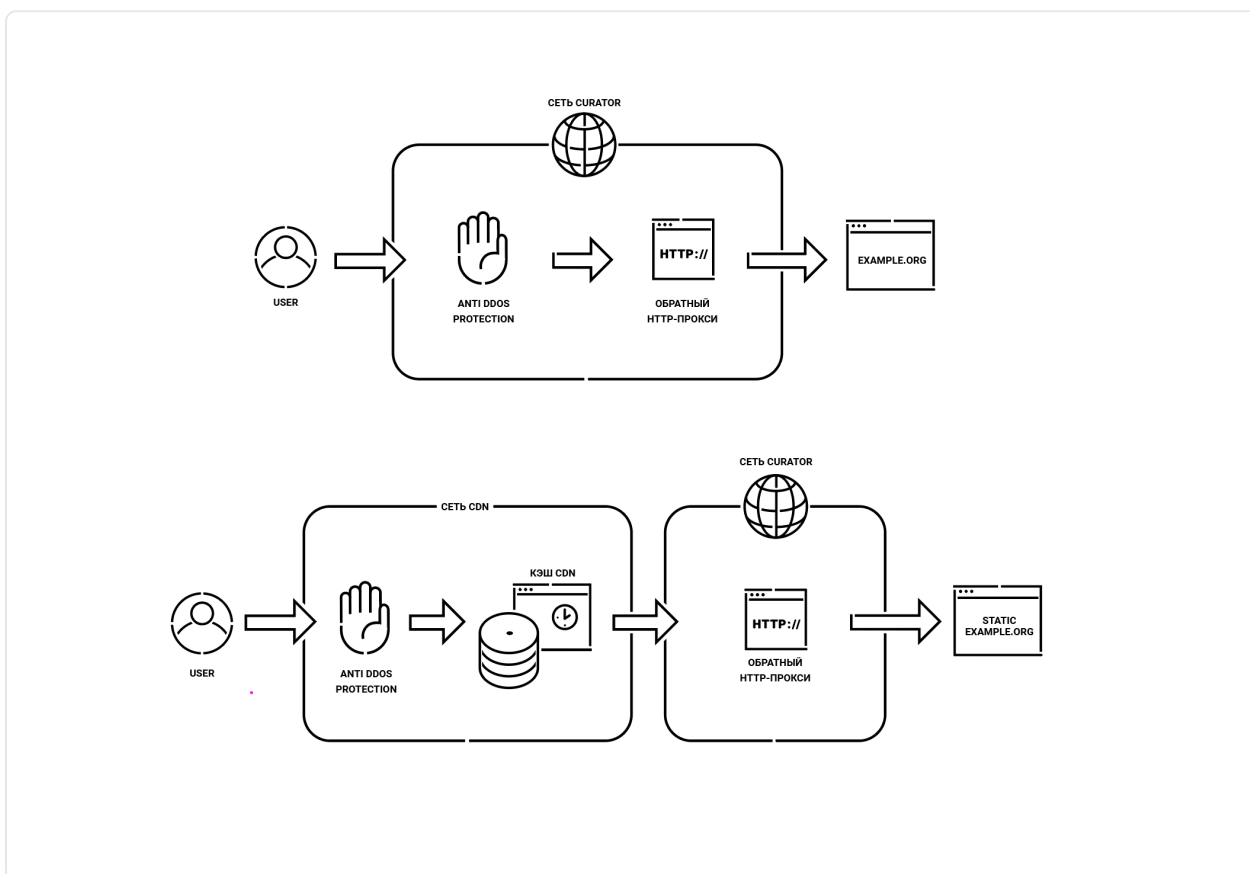
Для борьбы с брутфорсом используется [обратный HTTP-прокси](#).

Чтобы подключить защиту от ботов на своём аккаунте, обратитесь к специалистам поддержки Curator. После подключения услуги вы сможете настраивать политику защиты от ботов в личном кабинете. Подробнее о процессе настройки читайте в разделе [Подключение: Защита от ботов](#).

Технологии: Работа с CDN

Многие сайты используют сторонние сервисы CDN (Content Delivery Network, сеть доставки контента), которые хранят статический контент на множестве географически распределенных серверов. Когда пользователь запрашивает контент, запрос обрабатывается ближайшим к пользователю сервером CDN. Такой подход особенно активно применяется на сайтах, оперирующих большим объёмом трафика — например, предоставляющих мультимедийный контент. CDN позволяет не только ускорить работу сайта для пользователя, но и уменьшить нагрузку на сервер, который служит источником контента.

Частой практикой является разместить весь статический контент сайта на отдельном домене, который будет обслуживаться с использованием CDN, в то время как основной домен сайта будет работать без него.



Если сервер, который служит источником контента, находится под защитой Curator (т. е. является апстримом), то необходима дополнительная настройка защиты для пропуска трафика из сети CDN. CDN находится не просто за пределами сети клиента, но и за пределами [сети Curator](#). Поэтому запросы от CDN к этому апстриму проходят такой же путь, как и запросы от абстрактного пользователя. Однако их количество и характер могут заметно отличаться. При некорректной настройке такие запросы могут вызвать ложное срабатывание защиты от DDoS-атак в сети Curator. Это скажется сразу на всех пользователях, которые получают контент через CDN.

Curator предлагает клиентам собственную услугу Curator.CDN, а также возможность интеграции со многими популярными провайдерами услуг CDN. Вне зависимости от конкретного провайдера, общий принцип интеграции заключается в том, чтобы корректно идентифицировать запросы из сети CDN и всегда считать их легитимными.

Конкретный способ определения запросов зависит от того, CDN какого провайдера вы используете. Для некоторых провайдеров используется проверка подписей запросов согласно протоколу G2O, а для некоторых — проверка IP-адреса согласно белому списку. Различаются также способы настройки остальных параметров CDN: для Curator.CDN настройки доступны прямо из [специального раздела личного кабинета](#) или выполняются специалистами технической поддержки Curator, тогда как для других провайдеров настройку необходимо выполнять на их сайтах отдельно от настройки Curator.

Работа с Ngenix, Akamai и G-Core

Для клиентов, использующих CDN от [Ngenix](#), [Akamai](#) или [G-Core](#), Curator автоматически добавляет IP-адреса соответствующих сетей в исключения при защите от атак. Таким образом, весь трафик, пропущенный CDN, гарантированно доходит до апстрима.

Все настройки выполняются на сайте соответствующего CDN. В качестве апстрима для CDN следует указать Curator IP.

Работа по протоколу G2O

Многие провайдеры CDN поддерживают протокол авторизации запросов G2O. В рамках этого протокола к каждому запросу добавляется два HTTP-заголовка. В одном из них содержатся определённые дополнительные данные о запросе, включая его ID, сгенерированный случайным образом. Во втором заголовке содержится подпись, сделанная на основе этих данных. Для подписи используется ключ, одна из частей которого известна сети Curator и используется для проверки. Таким образом, сеть Curator может убедиться, что запрос был отправлен именно с CDN.

Все настройки выполняются на сайте соответствующего CDN. В качестве апстрима для CDN следует указать Curator IP.

Перенаправление с установкой cookie

Перенаправление с установкой cookie — способ проверки пользователя сайта или мобильного приложения, используемый в основном для [защиты от ботов](#).

При первом посещении сайта приложение пользователя (например, браузер или мобильное приложение) получает в качестве ответа статус [401 Unauthorized](#) и страницу с кодом на JavaScript, который собирает данные о цифровом отпечатке окружения пользователя и отправляет их на сервер Curator. Если этот сервер определяет окружение как легитимный браузер, то он назначает пользователю трекиговую cookie. После этого пользователь некоторое время может просматривать сайт без дополнительных проверок, при этом каждый раз Curator автоматически продлевает срок действия cookie. Если же сервер Curator определяет пользователя как бота, то он не устанавливает cookie, а вместо содержимого страниц возвращает ошибку [403 Forbidden](#).

Для разных адресов вы можете настроить, как Curator будет реагировать на пользователя без трекиговой cookie: либо отвечать статусом [401 Unauthorized](#) с кодом для проверки окружения, либо отвечать статусом [403 Forbidden](#).

Преимуществом решения на основе анализа цифрового отпечатка является то, что активность бота пресекается мгновенно, не позволяя ему выполнить даже первый запрос. Это отличает такой подход от блокировки после анализа активности, который возможен лишь после нескольких запросов.



ВАЖНО

Ресурсы, работающие по протоколу HTTPS, могут быть защищены с помощью этого механизма только при определённых условиях:

1. Принудительное включение протокола HTTPS должно выполняться с помощью [перенаправлений на стороне обратного HTTP-прокси](#).

Cookies, установленные по протоколу HTTP, недоступны при работе по протоколу HTTPS, и наоборот. Поэтому для корректной работы защиты от ботов необходимо, чтобы перенаправление с использованием правильного протокола выполнялось раньше, чем анализ цифрового отпечатка и установка cookie.

2. Должно быть настроено проксирование HTTPS с раскрытием ключей.

В противном случае обратный HTTP-прокси Curator не будет иметь возможности проверять или устанавливать заголовки HTTP, что необходимо для работы с cookie.

Использование капчи

В дополнение к стандартной неинтерактивной проверке, в некоторых случаях сервер Curator может также проверять легитимность пользователя с помощью капчи. Эта проверка выключена по умолчанию, но может быть включена по обращению в техническую поддержку.

Капча будет показана не всем пользователям, а только тем, в отношении которых сервер Curator не смог принять однозначного решения после анализа цифрового отпечатка.

Использование капчи позволяет дополнительно снизить количество ложноположительных срабатываний проверки в целом. При успешном вводе символов с капчи пользователь считается легитимным и получает трекинг-cookie так же, как те пользователи, цифровой отпечаток которых оказался однозначно легитимным без показа капчи.

Настройка ответа 403 Forbidden

Если не прошедший проверку пользователь делает запрос к URL, для которого в разделе [Bot protection](#) → [Локации](#) установлено правило «Принять Только с Куки», то сервер Curator отправляет ему ответ с кодом 403 Forbidden. По умолчанию в качестве тела ответа отправляется простая HTML-страница, дублирующая код ответа.

Вы можете настроить ответ несколькими способами.

- **Предоставьте пользователю дополнительную информацию на странице 403 Forbidden**

Curator возвращает HTML-страницу для статуса 403 Forbidden, когда в заголовке `Accept` запроса присутствует тип `text/html` или этот заголовок отсутствует. Эту страницу увидят прежде всего легитимные пользователи, в отношении которых произошло ложноположительное срабатывание проверки.

В зависимости от специфики вашего веб-сайта, вы можете прямо на странице ответа порекомендовать таким пользователям включить JavaScript, связаться с вами или перейти в другой раздел веб-сайта.

Чтобы сервер Curator использовал ваш вариант страницы, загрузите файл `403.html` в раздел [Страницы ошибок](#) личного кабинета.

- **Предусмотрите вариант ответа в формате JSON**

Curator может возвращать JSON-ответ для статуса 403 Forbidden, когда в заголовке `Accept` запроса присутствует тип `application/json` и отсутствует тип `text/html`. Такое поведение особенно удобно для одностраничных или мобильных приложений, которые могут самостоятельно показать пользователю то или иное сообщение в зависимости от ответа сервера.

Ответ может содержать идентификатор, позволяющий отличить ответ сервера Curator от ответа апстрима, а также дополнительную информацию, такую как время получения запроса или строку из заголовка `Referer`.

Чтобы включить это поведение и согласовать содержимое JSON-ответа, обратитесь к специалистам технической поддержки Curator.

- **Используйте HTTP-заголовки при проверке ответа**

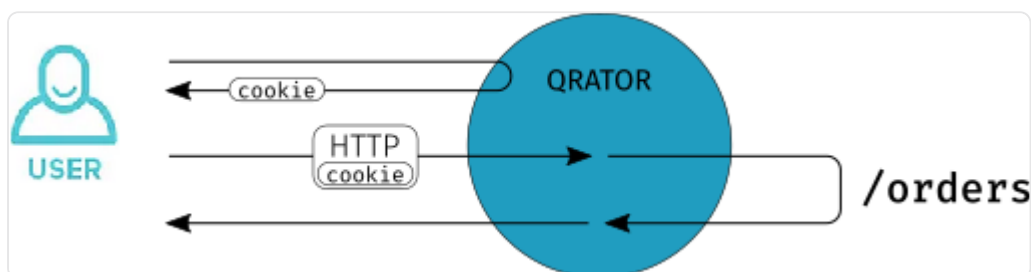
HTTP-заголовки — ещё один способ сообщить одностороннему или мобильному приложению, какой сервер отправил ответ на их запрос: апстрим или сервер Curator. Чаще всего для этого достаточно всего одного заголовка, который будет указан в ответе 403 Forbidden сервера Curator, но заведомо будет отсутствовать в ответе апстрима.

Чтобы включить добавление HTTP-заголовков и согласовать их названия, обратитесь к специалистам технической поддержки Curator.

Примеры интеграции

Защита веб-сайта с использованием cookie

Предположим, что все страницы вашего сайта предназначены для просмотра в браузере. В этом случае вы можете настроить защиту от Curator так, чтобы и проверка, и выдача трекинговой cookie могли происходить на любой странице.



Пользователь начинает просмотр сайта с любой страницы, и при первом посещении Curator выполняет проверку и устанавливает cookie. Если срок действия cookie истечёт, то при очередном обращении к сайту проверка будет выполнена повторно. В то же время боты не смогут пройти проверку и будут получать ошибку `401 Unauthorized` на любой странице.

Такой подход работает максимально прозрачно для пользователей, но для него требуется, чтобы они всегда использовали браузеры с поддержкой JavaScript.

Защита мобильных API с использованием cookie

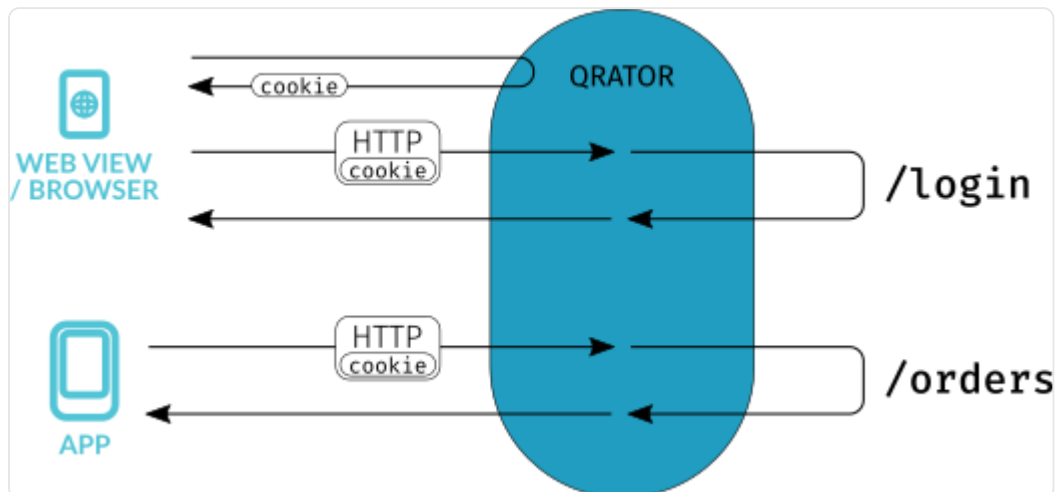
Предположим, что у вас есть приложение, которое делает запросы к вашему API-шлюзу (API gateway) и может обрабатывать полученные от него данные, но не сможет обработать страницу HTML с кодом на JavaScript. Это частая ситуация, например, для мобильных приложений.

В такой ситуации рекомендуется настроить установку и проверку трекинговой cookie на разных страницах:

1. Добавьте в карту приложения URL, предназначенный для посещения из браузерного окружения.
2. Для этой страницы в личном кабинете Curator включите проверку отпечатка с последующей выдачей трекинговой cookie.
3. Добавьте в клиентский код приложения обращение к этому URL через браузер. Например, приложение может показывать HTML-страницу с сервера в компоненте WebView в качестве экрана

загрузки, а затем извлекать из хранилища WebView полученную cookie. Если вы используете **капчу**, убедитесь, что у пользователя будет возможность ввести символы в поле ввода.

4. Приложение должно использовать полученную cookie в последующих запросах к API-шлюзу. Когда срок действия cookie истечёт, необходимо повторно направить пользователя на страницу проверки.



Защита мобильных API с использованием хэша

Для работы некоторых мобильных приложений может оказаться неприемлемым **способ защиты с использованием cookie**, поскольку он требует обязательного получения трекинговой cookie через веб-страницу.

Для таких приложений можно использовать проверку хэша, для вычисления которого используются HTTP-заголовки запроса и секретный ключ, известный только вам и Curator:

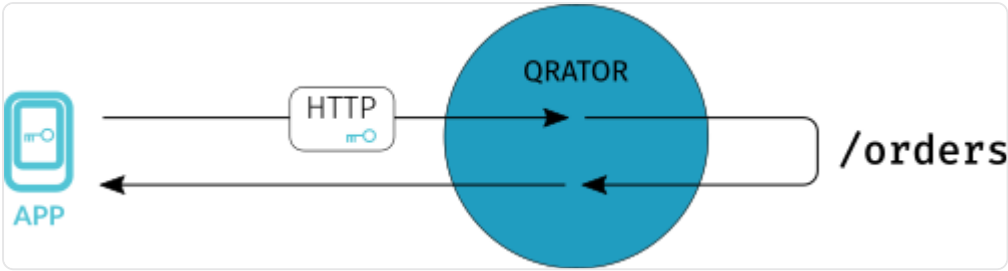
1. В разделе **Bot protection** → **Локации** установите правило «Принять Только с Куки» для всех страниц, которые должны быть под защитой.

При такой настройке сервер Curator будет считать легитимными посетителей либо с корректной cookie, либо с корректным хэшем в HTTP-заголовках.

2. В разделе **Bot protection** → **Подписи** добавьте новую подпись и включите проверку подписей.
3. На этапе сборки приложения добавьте в него секретный ключ и соль подписи в обфусцированном виде.

Перед каждым запросом к API-шлюзу используйте эти данные, чтобы вычислить хэш заголовков, и добавляйте заголовок с этим хэшем к запросу.

Боты, не владеющие ключом, не смогут добавлять к запросам корректный хэш. Curator не будет направлять такие запросы API-шлюзу.



Обратный HTTP-прокси

В основе значительной части услуг, оказываемых Curator, лежит технология *обратного прокси* (reverse proxy). Это означает, что запросы, предназначенные для вашего сервера, сначала поступают на обратный прокси, а уже он перенаправляет их на ваш сервер, выступая в роли клиента. Аналогично происходит с ответами: сервер посылает их не пользователю напрямую, а обратному прокси, а он перенаправляет их пользователю.

Сервер, к которому обращается обратный прокси, называется *апстримом*.

Такая архитектура позволяет Curator решать следующие задачи:

- определять и останавливать DDoS-атаки;
- блокировать известные вредоносные запросы;
- блокировать [запросы от ботов](#);
- выполнять [балансировку](#), а именно распределять нагрузку между несколькими апстримами, которые обеспечивают работу одного и того же сервиса;
- устанавливать [постоянные соединения](#) с апстримами для экономии ресурсов.

Обратный HTTP-прокси работает как с входящим незашифрованным трафиком по [протоколу HTTP](#), так и с зашифрованным по [протоколу HTTPS](#). Соединение с апстримами также может осуществляться как с использованием HTTP, так и HTTPS.

См. также: [как подключить обратный HTTP-прокси](#).

Проксирование HTTP

Если сайт использует HTTP, то для того, чтобы обратный прокси начал обрабатывать трафик, достаточно сменить A-записи зоны DNS для нужного домена.

Устройство пользователя обращается к DNS-серверу и получает IP-адрес обратного прокси. После этого непосредственное взаимодействие пользователя идёт только с серверами Curator. Запросы, которые не являются частью DDoS-атак, пересылаются на апстрим, при этом к ним добавляется заголовок `X-Forwarded-For`, в который дописывается реальный IP-адрес пользователя, а также другие [дополнительные HTTP-заголовки](#).

Исключение составляют следующие ситуации:

- Если вы добавили IP-адреса в [чёрный список](#), то запросы от пользователей с таких адресов не будут пересылаться на апстрим. Управлять чёрным списком можно из личного кабинета Curator.
- Если вы настроили [HTTP-перенаправления](#), то на соответствующие запросы обратный прокси Curator будет возвращать ответ самостоятельно, не пересылая запрос на апстрим.

Проксирование HTTPS

Для HTTPS-сайтов технология работает по [тем же принципам](#), что и для HTTP-сайтов: каждый запрос от пользователя анализируется, и если он пришёл от легитимного пользователя, то обратный прокси пересылает запрос на апстрим.

Но поскольку трафик HTTPS зашифрован, перед обработкой запроса обратный прокси должен расшифровать его. Для этого необходимы TLS-сертификат и связанные с ним цепочка доверия и приватный ключ. Эти данные помещаются в *хранилище сертификатов* и используются для [установления зашифрованных соединений](#) между пользователями и обратным прокси. При этом для соединений между обратным прокси и апстримом можно настроить использование как [протокола HTTPS](#), так и протокола HTTP.

Добавить данные в хранилище сертификатов можно двумя способами:

- [Настроив автоматический выпуск и обновление сертификатов.](#)
- [Загрузив файлы вручную через личный кабинет или API.](#)

Автоматический выпуск сертификатов

Для автоматического выпуска сертификатов Curator использует бесплатный сервис [Let's Encrypt](#). Вы можете заказать выпуск такого сертификата [через личный кабинет](#), указав список доменных имён, для которых должен быть выпущен сертификат.



ПРИМЕЧАНИЕ

Выпуск сертификатов, действующих для неограниченного числа поддоменов (wildcard), не поддерживается.

Каждый сертификат Let's Encrypt действителен в течение 90 дней после выпуска. За несколько дней до окончания этого срока Curator автоматически отправляет запрос на перевыпуск сертификата и устанавливает его вместо устаревающего. В случае невозможности автоматического продления Curator уведомит вас об этом.

Чтобы подтвердить владение доменом для Let's Encrypt, обратный прокси возвращает особый токен по определённому URL ([HTTP-01 challenge](#)). Обратите внимание, что сервис Let's Encrypt сможет проверить наличие этого токена только тогда, когда А-записи в зоне DNS уже указывают на IP-адрес обратного прокси. Автоматический выпуск сертификата до изменения записей DNS невозможен. Таким образом, после изменения записей DNS и до выпуска сертификата ваш ресурс будет недоступен пользователям по протоколу HTTPS. Если вам необходимо, чтобы он стал доступен сразу после изменения записей DNS и обновления кешей, рекомендуется заранее получить и [загрузить сертификат в хранилище в ручном режиме](#).

Ручное добавление файлов в хранилище сертификатов

Вы можете вручную добавить сертификат и связанные с ним файлы в хранилище сертификатов, предварительно выпустив сертификат любым способом. Например, вы можете добавить тот же сертификат, который использовался для домена до подключения к Curator.

К каждому сертификату должны прилагаться цепочка доверия и приватный ключ.

Данные можно добавить как [через личный кабинет](#), так и через API-методы `certrequest_upload`, `certrequest_install` и `sni_link_add`. Поддерживаются сертификаты X.509 в формате PEM. В качестве контейнерных форматов поддерживаются `pem`, `cer`, `crt`, `der`, `p7b`, `p7c`, `p12`.

Проксирование HTTP/2

По умолчанию обратный прокси Curator работает только по протоколу HTTP/1.1, но по вашей заявке специалисты технической поддержки могут включить поддержку протокола [HTTP/2](#) для соединения с пользователями. Эта версия протокола в некоторых случаях может значительно ускорить загрузку ресурсов для пользователей, браузеры которых также поддерживают HTTP/2. Использование HTTP/2 возможно только при [использовании HTTPS](#).

Одно из ключевых различий между HTTP/1.1 и HTTP/2 проявляется в возможности загрузки нескольких ресурсов одновременно. При использовании HTTP/1.1, чтобы запросить новый ресурс, необходимо либо дождаться, пока завершится загрузка предыдущего, либо создать новую TCP-сессию. Создание каждой новой TCP-сессии влечёт определённые издержки, а общее количество таких сессий в браузере обычно ограничено. При использовании HTTP/2 браузер может отправлять новые запросы в рамках уже созданной TCP-сессии — такой подход называется *мультиплексированием*.

Соединение между обратным прокси Curator и апстримом в любом случае происходит по протоколу HTTP/1.1, но благодаря большому пулу соединений обратный прокси способен отправлять запросы параллельно, см. раздел [Постоянные соединения с апстримом](#) ниже.



Установка зашифрованного соединения

При работе с HTTPS-трафиком обратный прокси:

- Поддерживает следующие алгоритмы шифрования (cipher suites) для соединений с пользователями:

Версии TLS	Алгоритмы шифрования
------------	----------------------

TLS 1.0, 1.1, 1.2	ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 AES128-GCM-SHA256 AES128-SHA256 AES128-SHA DES-CBC3-SHA
TLS 1.3	TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256

**ПРИМЕЧАНИЕ**

Техническая поддержка Curator может изменить список разрешённых алгоритмов по вашему запросу.

- Поддерживает все возможные алгоритмы и все версии TLS для соединений с апстримом. Подлинность апстрима не проверяется.

**ВАЖНО**

Устаревший протокол SSL не поддерживается ни для соединений с пользователями, ни для соединений с апстримом.

Оптимизация скорости

Обратный HTTP-прокси Curator позволяет оптимизировать работу с соединениями за счёт нескольких технологий:

- [Постоянные соединения с апстримом](#)
- [TLS offloading](#)

Постоянные соединения с апстримом

При обработке HTTP-запроса посетителя сайта существенное время тратится на установление транспортной TCP-сессии. Если используется протокол HTTPS, то после создания каждой новой TCP-сессии выполняется *TLS-рукопожатие* (TLS handshake) и генерация сессионного ключа, что также занимает существенное время.

Обратный прокси может устанавливать TCP-сессии и выполнять TLS-рукопожатия заранее, формируя динамический пул сессий, готовых к мгновенной передаче полезных данных. Для обработки каждого запроса обратный прокси использует сессию из этого пула. Одна сессия может быть последовательно использована для обработки многих запросов.

Когда соединение с пользователем выполняется [по протоколу HTTP/2](#) и пользователь запрашивает несколько ресурсов в рамках одного соединения, обратный прокси Curator направляет эти запросы к апстриму через разные соединения из пула. Таким образом удаётся эффективно использовать возможности HTTP/2 со стороны пользователя без необходимости настраивать полноценную поддержку HTTP/2 со стороны апстрима.

TLS offloading

Использование протокола HTTPS предполагает шифрование всего трафика сессионным ключом, что может приводить к более медленной обработке каждого запроса, чем по протоколу HTTP. Особенно заметно это становится на сайтах с высокой посещаемостью.

Обратный прокси может работать в режиме *TLS offloading*. Это означает, что соединение с апстримом может использовать протокол HTTP, даже если пользователь обращается к ресурсу по протоколу HTTPS. Всю нагрузку, связанную с TLS, обратный прокси берёт на себя, а апстрим расходует на обработку каждого запроса меньше ресурсов. Такая конфигурация зачастую обеспечивает более быструю работу ресурса.

Технологии: Обратный TCP-прокси

Обратный TCP-прокси перенаправляет трафик от пользователя на апстрим клиента и наоборот.

Обратный TCP-прокси схож по принципу действия с обратным HTTP-прокси, но работает на транспортном уровне сетевой модели OSI/ISO и анализирует TCP-трафик. Вредоносный TCP-трафик отсекается и не попадает на апстрим. Таким образом обратный TCP-прокси от Curator защищает сайты от DDoS-атак на транспортном уровне (L4).

TCP-прокси также может использоваться и для защиты от DDoS-атак на уровне приложения (L7), выступая в качестве альтернативы обратному HTTP-прокси. Для этого необходимо настроить [автоматическую отправку логов](#) с вашего сервера на сервер Curator.



ВАЖНО

Обратите внимание, что это не эквивалентно полной обработке трафика на уровне приложения (TCP-прокси не работает на этом уровне), поэтому с помощью такого прокси нельзя организовать работу Web Application Filter или защиты от ботов. Эти продукты работают строго на уровне приложения и требуют использования обратного HTTP-прокси.

Поэтому обратный TCP-прокси подходит для обработки трафика во многих ситуациях, в которых [обратный HTTP-прокси](#) или [туннель](#) не могут быть использованы, например:

- когда серверу необходимо видеть заголовки TCP-сегментов пользователя;
- когда необходимо защитить от DDoS-атак ресурс, работающий по протоколам, отличным от HTTP и HTTPS;
- когда необходимо установить соединение типа «точка—точка» с сервером под управлением Windows.

Обратный TCP-прокси Curator поддерживает работу как в [режиме Proxy Protocol](#) для апстримов, поддерживающих этот протокол, так и в [режиме Raw TCP Proxy](#) для любых апстримов.

Режим Proxy Protocol

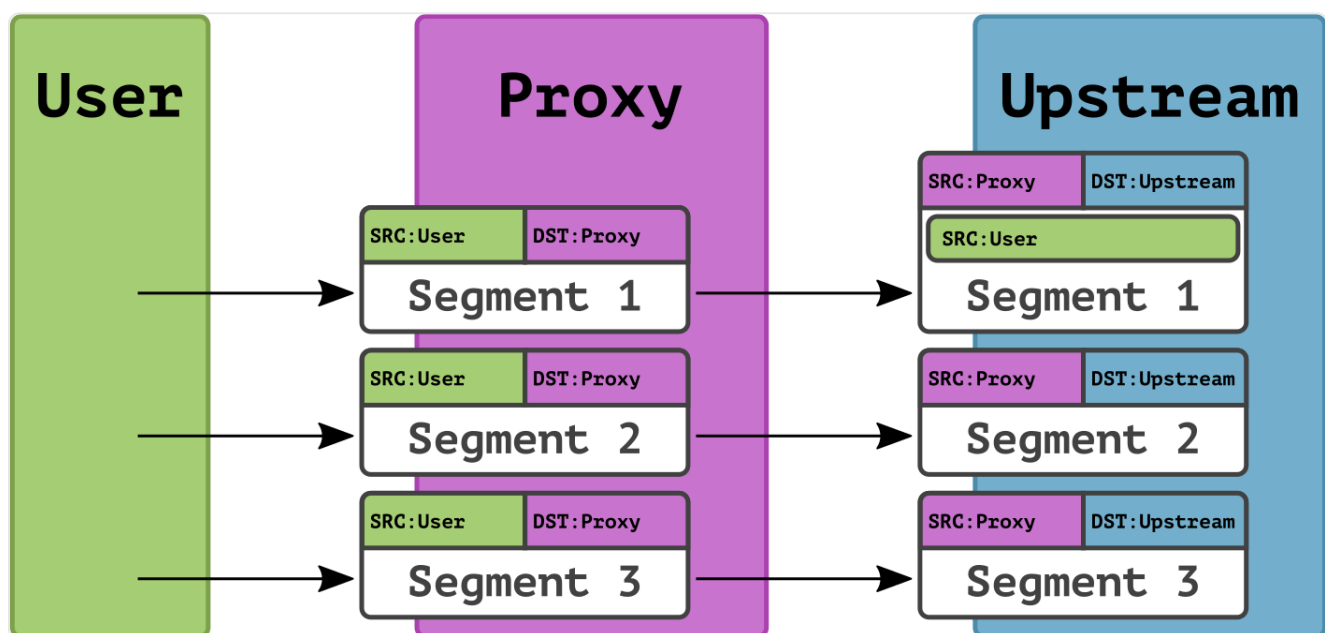
Если программное обеспечение вашего апстрима поддерживает [Proxy Protocol](#), то обратный TCP-прокси может направлять ему как содержимое пользовательских TCP-сегментов, так и информацию об IP-адресах, с которых они пришли. Апстрим должен направлять ответный трафик также с использованием Proxy Protocol через сеть Curator, откуда они будут перенаправлены пользователю.

**ПРИМЕР**

Поддержка Proxy Protocol встроена в торговую платформу для финансовых брокеров MetaTrader, поэтому обратный TCP-прокси может защищать торговые шлюзы на этой платформе от DDoS-атак. В данном случае вместо того, чтобы принимать TCP-трафик от пользователей напрямую, шлюз MetaTrader в сети брокера принимает его только от обратного TCP-прокси в сети Curator. Нелегитимный трафик от пользователей не передаётся в сеть брокера и не угрожает работоспособности шлюза.

В рамках Proxy Protocol в начале каждого TCP-соединения апстрим получает заголовок с информацией об IP-адресах отправителя и получателя исходного сегмента. Все остальные данные он может получить непосредственно из пересланного сегмента. Это означает, что после правильной обработки заголовка программное обеспечение на стороне апстрима может реализовать все те же функции, что и при получении TCP-трафика напрямую без обратного прокси: например, логировать IP-адрес отправителя или выполнять другие действия.

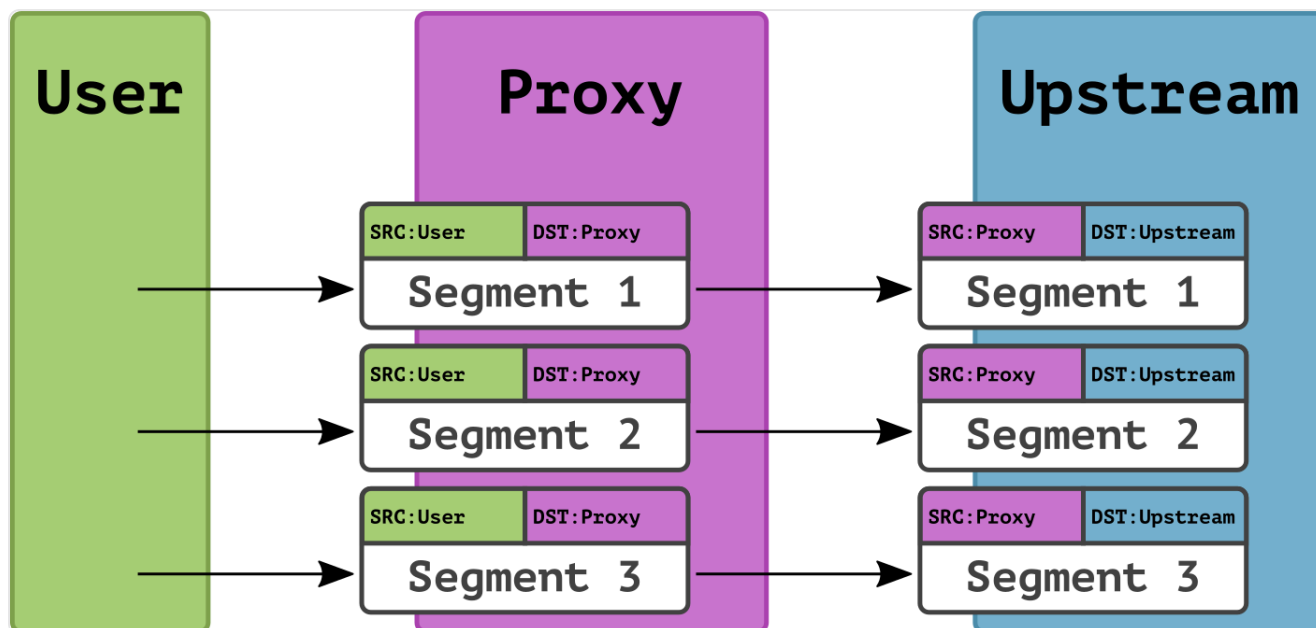
На рисунке апстрим подставляет полученный отдельно заголовок к каждому сегменту, полученному в рамках этого соединения, воссоздавая таким образом всю информацию, отправленную пользователем:



О том, как подключить обратный TCP-прокси в режиме Proxy Protocol, читайте в [соответствующем разделе](#).

Режим Raw TCP Proxy

Для защиты апстримов, не поддерживающих Proxy Protocol, используйте обратный TCP-прокси в режиме Raw TCP Proxy. В таком режиме, получив TCP-сегмент от пользователя, обратный TCP-прокси просто проксирует этот сегмент, выступая для апстрима в качестве отправителя сегмента. Дополнительная информация об исходном отправителе не передается на апстрим



При использовании Raw TCP Proxy апстрим не может получить информацию об IP-адресе пользователя, если это не предусмотрено протоколом более высокого уровня. Поэтому такой режим используется в основном для протоколов, которые предусматривают способ авторизации, не полагающийся на IP-адрес отправителя. Например, с помощью Raw TCP Proxy вы можете защититься от DDoS-атак, направленных на находящийся за апстримом сервер SSH.

Основным преимуществом Raw TCP Proxy по сравнению с использованием Proxy Protocol является отсутствие необходимости в дополнительной настройке на стороне апстрима. Апстрим принимает легитимные TCP-сегменты из сети Curator так же, как принимал бы их напрямую от пользователей.

Raw TCP Proxy от Curator защищает ресурсы от DDoS-атак не выше транспортного уровня (L4).

О том, как подключить Raw TCP proxy, читайте в [соответствующем разделе](#).

Технологии: Обратный WebSocket-прокси

Многие современные веб-приложения используют для передачи данных не только привычные протоколы HTTP и HTTPS, но и протокол WebSocket ([RFC 6455](#)). Например, через HTTPS может работать фронтенд веб-приложения, а через WebSocket — подгружаться видеопоток. Зачастую апстримы WebSocket располагаются на тех же IP-адресах или в тех же сетях, что и HTTP-апстримы, таким образом, незащищённый WebSocket-трафик может упростить для злоумышленника проведение атаки на вашу сеть даже при полной защищённости HTTP-трафика.

Поэтому клиентам, разрабатывающим такие мультипротокольные веб-приложения, следует обеспечить прохождение всего трафика приложения через сеть Curator. Для этого нужно использовать комбинацию из [обратного HTTP-прокси](#) и *обратного WebSocket-прокси*.

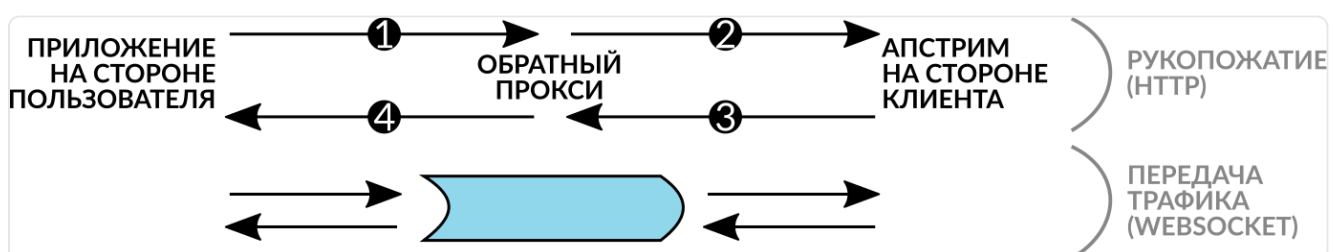
О том, как начать использовать обратный WebSocket-прокси от Curator, читайте в статье [Подключение: Обратный WebSocket-прокси](#).

Принцип работы

Частью протокола WebSocket является рукопожатие (handshake), которое должны выполнить пользователь и апстрим, прежде чем начать пересылку данных. Для самого рукопожатия используется протокол HTTP. После завершения рукопожатия обе стороны могут отправлять друг другу трафик по протоколу WebSocket до тех пор, пока соединение не будет закрыто одной из сторон.

Обратный WebSocket-прокси проксирует запрос пользователя и ответ сервера, при этом в запрос добавляются дополнительные HTTP-заголовки. После этого обратный прокси принимает и проксирует WebSocket-трафик в обе стороны через соединения, созданные во время рукопожатия.

Ответственность за разбор и обработку данных, передаваемых после рукопожатия, лежит на приложении. Обратный прокси не анализирует и не изменяет WebSocket-трафик, что позволяет использовать его вне зависимости от формата пересылаемых данных.



Ниже подробнее описана процедура рукопожатия с участием обратного WebSocket-прокси.

1. Пользователь отправляет запрос HTTP [101 Switching Protocols](#).

Получив этот запрос, обратный прокси проверяет, не превышает ли количество запросов с IP-адреса пользователя [заданный клиентом лимит](#). Если лимит ещё не превышен, то обратный

прокси выбирает апстрим для данного пользователя, исходя из его IP-адреса, см. раздел [Балансировка](#).

2. На выбранный апстрим проксируется запрос HTTP `101 Switching Protocols` с заголовками, которые указал пользователь в своём запросе, а также [дополнительными HTTP-заголовками](#).

**ВАЖНО**

По умолчанию обратный прокси настроен так, что перед передачей запроса на апстрим из него удаляются заголовки, содержащие знак подчёркивания `_`. Если вам необходимо, чтобы такие заголовки оставались в запросе, обратитесь в техническую поддержку Curator для изменения этой настройки.

3. Обратный прокси ожидает ответ от апстрима в течение 5 секунд. Если апстрим не отвечает, то обратный прокси возвращается к шагу 2 и предпринимает попытки обратиться к другим апстримам клиента. Подробнее об этом написано в разделе [Балансировка](#).
 - Если ответ ни от одного апстрима не приходит, обратный прокси возвращает пользователю ответ со статусом HTTP `400 Bad Request`, и попытка начать работу по протоколу WebSocket прекращается.
 - Если апстрим отвечает сообщением об ошибке с любым статусом, то соединения сбрасываются, и попытка начать работу по протоколу WebSocket прекращается.
 - Если апстрим отвечает рукопожатием со статусом HTTP `101 Switching Protocols` и корректными заголовками, обратный прокси проксирует этот ответ пользователю без изменений. В этом случае соединение между обратным прокси и апстримом считается успешно установленным.
4. Пользователь проверяет статус и заголовки полученного ответа. На этом рукопожатие завершается, и WebSocket-соединение между пользователем и обратным прокси считается успешно установленным. Протокол HTTP в рамках этого соединения больше не используется.

Вся дальнейшая передача информации от пользователя к апстриму и обратно происходит через обратный прокси в рамках уже установленной пары соединений.

Обратный прокси не анализирует пересылаемые данные и не изменяет их содержимое при пересылке, что позволяет корректно работать вне зависимости от формата пересылаемых данных.

Когда одна из сторон закрывает соединение с обратным прокси, обратный прокси автоматически закрывает соединение с другой стороной.

Балансировка нагрузки

Если ваш ресурс обслуживается несколькими серверами, то вы можете настроить в личном кабинете несколько *апстримов*, соответствующих этим серверам. В этом случае обратный прокси Curator может использоваться не только для защиты от нелегитимного трафика, но и для балансировки легитимного трафика между апстримами.

Балансировка осуществляется независимо на каждом из центров очистки трафика Curator, которые расположены в разных регионах мира.

Настроить балансировку нагрузки можно [в разделе «Сервисы» личного кабинета](#).

Переключение между списками апстримов

В личном кабинете вы можете задать один или два списка апстримов (по умолчанию включён только один список). Первый список считается основным, а второй — запасным.

По умолчанию каждый центр очистки трафика балансирует все запросы только между апстримами из основного списка, при этом недоступные апстримы временно выводятся из обращения по результатам активных или пассивных проверок. Автоматическое переключение на запасной список и обратно осуществляется исходя из [доступности апстримов](#):

- Если все апстримы из основного списка стали недоступны для центра очистки трафика, то он переключается на использование запасного списка вместо основного.
- Как только в результате проверок обнаруживается, что хотя бы один апстрим из основного списка снова стал доступен, центр очистки трафика переключается обратно на использование основного списка.

Алгоритмы выбора апстрима

Curator поддерживает два алгоритма выбора апстрима: [Round robin](#) и [IP hash](#). В личном кабинете вы можете указать, какой из этих алгоритмов следует использовать. Выбранный алгоритм будет использоваться как для балансировки между апстримами основного списка, так и для балансировки между апстримами запасного списка.

На работу каждого алгоритма можно повлиять, указав для апстрима целочисленный вес. В зависимости от используемого алгоритма вес апстрима интерпретируется по-разному. Апстримы с нулевым весом считаются отключёнными и не участвуют в балансировке, трафик на них не поступает. Если веса не указаны, то считается, что вес каждого апстрима равен единице.

Round robin

Алгоритм *Round robin* работает со списком апстримов как с очередью в том порядке, в котором вы расположили их в личном кабинете. По умолчанию каждый апстрим используется для обработки одного запроса, прежде чем очередь переходит к следующему апстриму. Таким образом, алгоритм обеспечивает равномерное распределение запросов между всеми апстримами из соответствующего списка.

Вес апстрима определяет, какая доля запросов будет направлена на этот апстрим.

**ПРИМЕР**

Если вы используете алгоритм Round robin для двух апстримов с весами **1** и **2**, то из каждых трёх запросов первый будет обработан первым апстримом, а второй и третий — вторым.

IP hash

Алгоритм *IP hash* выбирает апстрим в зависимости от IP-адреса запроса, при этом повторные запросы с того же IP-адреса передаются тому же апстриму. Этот алгоритм выгоден, если желательно, чтобы все запросы одного пользователя обрабатывались одним и тем же апстримом — например, для более эффективного использования кеша на каждом сервере.

Вес апстрима определяет вероятность, с которой этот апстрим будет выбран и закреплен за пользователем.

**ПРИМЕР**

Если вы используете алгоритм IP hash для двух апстримов с весами **1** и **2**, то из 3 000 первых запросов пользователей с уникальными IP-адресами в среднем около 1 000 будут направлены на первый апстрим и около 2 000 на второй. Распределение дальнейших запросов этих пользователей зависит от самих пользователей и может сильно отличаться от первоначального.

Проверка доступности апстримов

Одним из преимуществ использования нескольких апстримов является возможность повысить отказоустойчивость ресурса в целом. Если один из апстримов становится недоступен или перестаёт своевременно обрабатывать запросы, доступность ресурса могут обеспечить остальные.

Доступность апстримов отслеживается отдельно из каждого центра очистки трафика Curator.

Доступны два метода проверки доступности апстримов:

- **пассивная проверка** происходит во время совершения обычных запросов;
- **активная проверка** совершается регулярно специальным запросом.

Пассивная проверка

При пассивной проверке центр очистки трафика не делает специальных диагностических запросов к апстримам, а анализирует ошибки при обработке запросов пользователей.

Для анализа используются только безопасные типы запросов (см. [Обработка ошибок](#)). Если более трети таких запросов к апстриму, сделанных в течение трёх секунд, завершилось с ошибками, то центр очистки трафика перестаёт делать запросы к данному апстриму по обычному алгоритму. Вместо этого на апстрим направляется не более одного запроса в три минуты, и если обработка очередного запроса завершается успешно, то апстрим вновь считается доступным.

Обратите внимание, что некоторые типы запросов не повторяются после неудачной отправки, см. [Обработка ошибок](#). Поэтому при пассивной проверке доступности пользователи могут видеть ошибки чаще, чем при активной проверке.

Активная проверка

Чтобы реагировать на недоступность апстримов раньше, чем она проявится в многократных ошибках при обработке запросов от реальных пользователей, вы можете использовать активную проверку. При активной проверке центр очистки трафика регулярно делает диагностические запросы к определённому URL на каждом апстриме. Решение о том, использовать ли апстрим, принимается на основе результатов таких запросов.

Все параметры активной проверки настраиваются индивидуально по обращению в техническую поддержку:

- Какой запрос центр очистки трафика будет делать к апстриму.

Настраиваются протокол (HTTP или HTTPS), URL и метод HTTP. При необходимости вы также можете указать параметры запроса — например, специальный токен, чтобы апстрим мог отличать диагностические запросы от запросов пользователей.

- Как часто необходимо совершать проверку.

Чем меньше интервал между запросами, тем оперативнее центр очистки трафика сможет узнавать о проблемах, но слишком частые запросы иногда могут сказаться на загрузке апстрима. Оптимальный интервал зависит от производительности ваших апстримов.

- Какие результаты проверок считаются успешными.

В зависимости от особенностей вашего ресурса, успешными можно считать либо ответы со всеми статусами, кроме ошибок сервера ([HTTP 5xx](#)), либо только ответы со статусом [HTTP 200](#) .

Кроме того, вы можете указать, сколько раз подряд проверка должна закончиться ошибкой, прежде чем центр очистки трафика посчитает апстрим недоступным и временно перестанет отправлять на него запросы пользователей. Аналогично настраивается, при каких условиях апстрим вновь считается доступным.

Обработка ошибок

После каждого запроса к апстриму центр очистки трафика Curator анализирует, завершился ли запрос успешно или произошла ошибка. Ошибки отображаются в разделе «Статистика» личного кабинета, а также влияют на дальнейшее поведение этого центра очистки трафика.

Ошибкой считается любая из следующих ситуаций:

- Соединение с апстримом потеряно, и центру очистки трафика не удаётся восстановить соединение в течение 15 секунд.
- Апстрим не ответил на запрос в течение 60 секунд или прислал неполный (некорректный) ответ.
- Апстрим вернул ответ со статусом `502 Bad Gateway` или `504 Gateway Timeout`.

Порядок обработки ошибок отличается для *небезопасных* (unsafe) и *безопасных* (safe) типов запросов (см. RFC 7231):

- Небезопасными считаются запросы POST, PUT, PATCH, DELETE, CONNECT.

Такие запросы не направляются повторно ни тому же, ни другому апстриму, поскольку это может нарушить логику работы приложения. Пользователь всегда получает первый ответ апстрима либо, если от апстрима не удалось получить ответ, ответ со статусом `502 Bad Gateway` или `504 Gateway Timeout` в зависимости от причины проблемы.

- Безопасными считаются запросы GET, HEAD, OPTIONS, TRACE.

Прежде чем возвращать ошибку пользователю, центр очистки трафика последовательно направляет запрос другим апстримам из списка и дожидается ответов от них. Если какой-либо апстрим обработает запрос без ошибок, его ответ будет возвращён пользователю. Если центр очистки трафика переберёт все апстримы, не получив успешного ответа, то он вернёт пользователю ответ со статусом ошибки от последнего апстрима. При этом, если от последнего апстрима не удалось получить ответ, то центр очистки трафика сам сформирует пользователю ответ со статусом `502 Bad Gateway` или `504 Gateway Timeout` в зависимости от причины проблемы.

Если пользователь разорвёт соединение, не дождавшись ответа (например, по таймауту), то попытки обработать запрос прекращаются.

Каждая ошибка отражается в личном кабинете в разделах «Аналитика» и «Сводка». Чтобы оперативно узнавать о проблемах с доступностью ресурса, обратитесь к специалистам технической поддержки Curator, и они настроят подходящие вам автоматические уведомления, которые будут срабатывать после определённого количества ошибок.

Технологии: Ingress-фильтрация

Защита транзитных сетей, через которые проходит трафик сразу к нескольким конечным сетям, отличается от защиты самих конечных сетей.

- Пропускная способность транзитной сети может страдать как от DDoS-атак, направленных непосредственно на неё, так и от атак, направленных на любую из конечных сетей.

При этом у владельцев транзитной сети есть необходимость максимально сохранить доступность ресурсов во всех конечных сетях, даже во время атак на часть из них.

- Защита транзитной сети должна полагаться только на анализ трафика на сетевом и транспортном уровнях, поскольку в конечных сетях могут использоваться разные протоколы более высокого уровня.

Curator предоставляет технологию Ingress-фильтрации для защиты транзитных сетей. Она позволяет эффективно реагировать на атаки, либо сохраняя полную доступность ресурсов каждой конечной сети, либо ограничивая доступность только конкретных сетей под атакой.

Для использования Ingress-фильтрации владелец транзитной сети указывает *префиксы*, соответствующие защищаемым подсетям, и производит настройку в личном кабинете Curator, см. раздел [Подключение: Ingress-фильтрация](#). Этот процесс происходит прозрачно для конечных сетей, на их стороне не требуется выполнять никаких настроек.

Отличия от защиты конечных сетей

Ключевым различием между защитой от DDoS-атак для конечных и для транзитных сетей является то, что обнаружение угроз для транзитной сети происходит только на сетевом и транспортном уровнях (L3, L4 по модели OSI) и не требует анализа исходящего трафика.

Во многих случаях это позволяет сэкономить ресурсы и не производить анализ трафика, источник которого известен и легитимен. В частности, при обслуживании стриминговых и других мультимедийных сервисов, где исходящий трафик сети может в десятки раз превышать входящий, зачастую имеет смысл пропускать входящий и исходящий трафик через разные сети и подключать Ingress-фильтрацию только для той сети, через которую проходит входящий трафик.



Учёт трафика

Сеть Curator учитывает и фильтрует входящий трафик для наборов префиксов, настроенных клиентом. Весь трафик в рамках одного набора префиксов делится на три категории, трафик в которых считается независимо.

- TCP-сегменты SYN и ACK, с помощью которых устанавливаются новые сессии, учитываются как *TCP Unverified*. В эту же категорию попадают некорректные сегменты и сегменты в рамках неизвестных сессий.
- TCP-сегменты, отправляемые в рамках уже установленных сессий, учитываются как *TCP Verified*.
- Любые другие сегменты, включая трафик по протоколам UDP и ICMP, учитываются как *Other*.

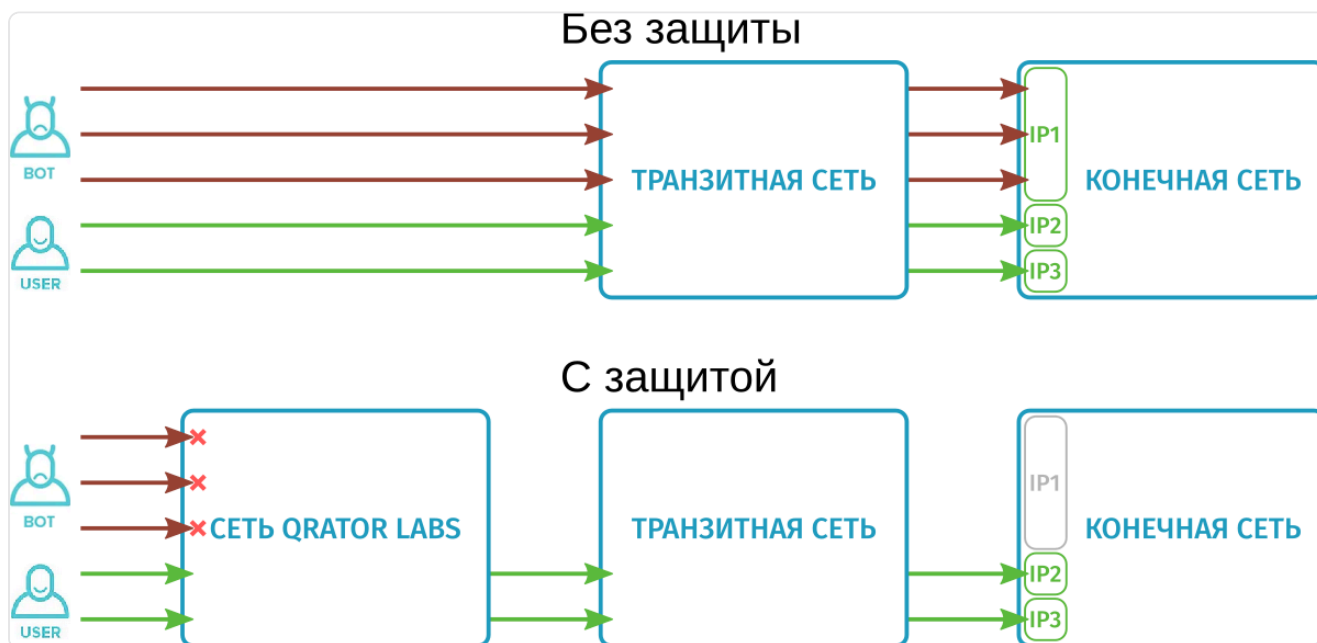
При настройке [политик фильтрации](#) вы можете установить произвольные лимиты на каждую из этих категорий трафика отдельно, а также установить лимит на общий объём трафика.

Также сеть Curator ведет статистику распределения трафика по IP-адресам конечной сети. Это не связано с какими-либо лимитами само по себе, но играет роль при [блокировке нагруженных IP-адресов](#).

Счётчик сегментов каждой категории и общий счётчик трафика сбрасываются один раз в несколько секунд (точный размер интервала может варьироваться в зависимости от нагрузки). Если до истечения этого периода какой-либо из счётчиков превысил соответствующий лимит или приближается к нему, то чтобы защитить транзитную сеть, сеть Curator [блокирует нагруженные IP-адреса](#) или применяет механизм [SYN cookies](#).

Блокировка нагруженных IP-адресов

Данный способ борьбы с атакой применяется, когда достигнут лимит трафика *TCP Verified*, *Other* или общий лимит на трафик (см. [Учёт трафика](#)).

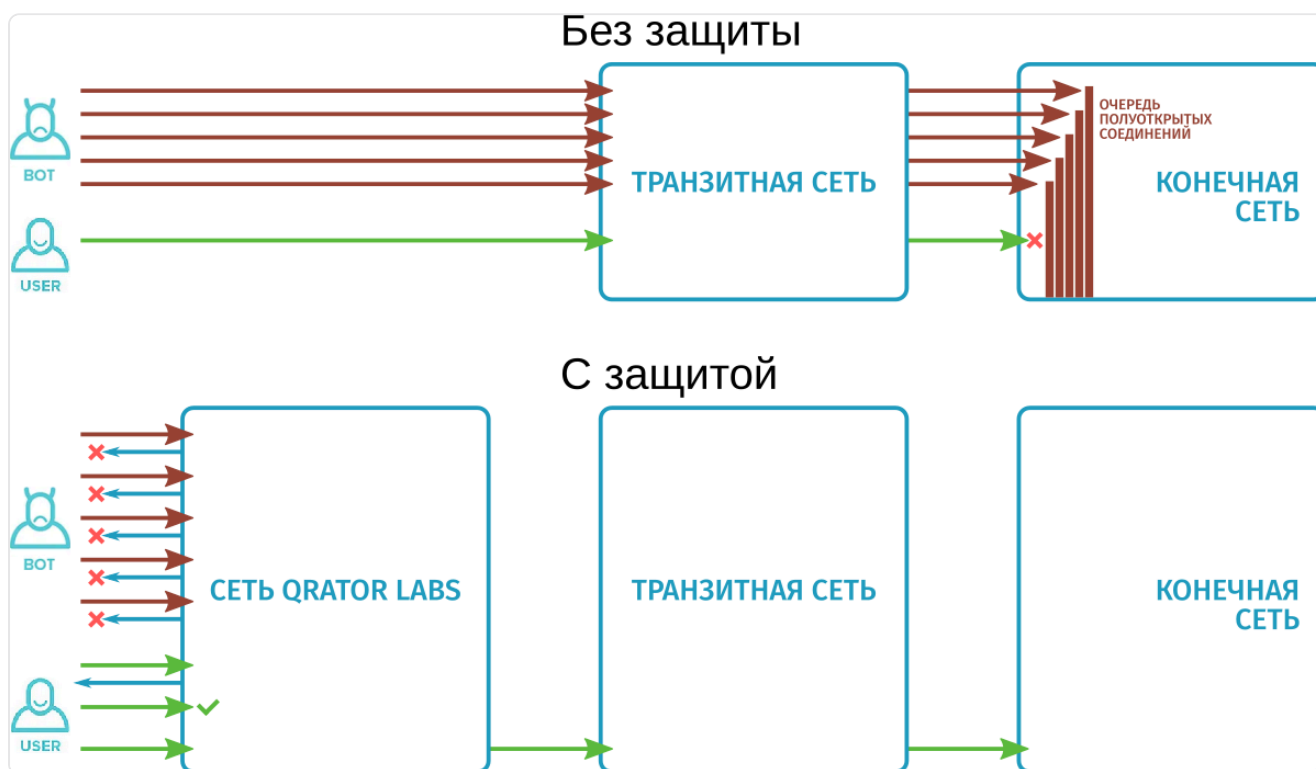


Используя статистику распределения трафика по IP-адресам в конечной сети, сеть Curator вносит в чёрный список те IP-адреса, на которые было направлено больше всего трафика за последние несколько секунд. Количество временно вносимых в чёрный список адресов рассчитывается таким образом, чтобы после прекращения доставки трафика к этим адресам оставшийся объём трафика вновь оказался не выше лимита.

Это решение позволяет снизить нагрузку на транзитную сеть во время атаки, временно заблокировав минимально возможное число IP-адресов в конечных сетях.

SYN cookies

Механизм SYN cookies применяется, когда на сервер совершается атака типа SYN flood, из-за чего оказывается достигнут лимит трафика *TCP Unverified* (см. [Учёт трафика](#)).



В рамках атаки SYN flood злоумышленник присылает на сервер множество TCP-сегментов, указывая в качестве источника посторонний IP-адрес. Сервер, пытаясь продолжить рукопожатие (TCP handshake) с этим адресом, никогда не получает ответа. Из-за этого данные о полуоткрытом соединении (half-opened connection) могут надолго остаться в очереди, что приведёт к её переполнению и невозможности устанавливать сессии с легитимными пользователями.

Задача Ingress-фильтрации в момент такой атаки — доставлять в транзитную сеть TCP-сегменты только от легитимных пользователей с настоящими IP-адресами. На TCP-сегменты от не проверенных ранее IP-адресов сеть Curator отвечает самостоятельно, пытаясь таким образом продолжить рукопожатие. Этот ответный TCP-сегмент подбирается таким образом, чтобы по следующему сегменту от пользователя в рамках этого рукопожатия можно было однозначно установить, получил ли он

сегмент из сети Curator. Прошедшие такую проверку IP-адреса добавляются в белый список. Более полно алгоритм SYN cookies описан в [RFC 6013](#).

Данный процесс не использует очередь полуоткрытых соединений, поэтому количество трафика от злоумышленника не влияет на возможность легитимному пользователю получить ответный TCP-сегмент и завершить рукопожатие.

После успешного завершения проверки сеть Curator сразу сбрасывает сессию. Большинство современных приложений устойчивы к сбросу TCP-сессий и предпринимают повторные попытки соединения автоматически. Поскольку IP-адрес пользователя уже находится в белом списке, все новые сегменты отправляются в транзитную сеть без ограничений.

Политики фильтрации

В личном кабинете Curator клиент может определить одну или несколько *политик* Ingress-фильтрации. Созданную политику клиент может установить для любого набора префиксов в пределах своей сети либо для всей своей сети.

Возможна установка нескольких политик для одного и того же префикса. В этом случае, как только будет достигнут какой-то из лимитов в одной из политик, на IP-адреса из префикса могут быть наложены ограничения, даже если лимиты в других политиках ещё не достигнуты.

Каждая политика представляет собой набор из лимитов для [учёта трафика](#). В политику могут входить отдельные лимиты для категорий трафика *TCP Verified*, *TCP Unverified*, *Other*, а также общий счётчик *Total* для всего трафика. Некоторые из лимитов клиент может оставить неустановленными.

Лимиты могут быть установлены как в битах в секунду, так и в пакетах в секунду. Лимиты в битах в секунду помогают защититься от атак, нацеленных на заполнение полосы трафика, в то время как лимиты в пакетах в секунду помогают защититься от тех атак, которые занимают сетевое оборудование обработкой множества мелких сегментов — например, от атаки TCP SYN flood.

Технологии: HTTP-перенаправления

Клиентам, использующим [обратный HTTP-прокси](#) Curator, доступна возможность настроить некоторые виды HTTP-перенаправлений на стороне обратного HTTP-прокси. При использовании этой услуги запросы, требующие перенаправления, будут обрабатываться непосредственно обратным HTTP-прокси без обращения к апстриму.

Одно из популярных применений HTTP-перенаправлений — принудительное включение протокола HTTPS для всех пользовательских запросов (см. [пример конфигурации](#) в конце статьи). В этом случае обработку HTTP-запросов в сети клиента можно отключить полностью, поскольку до апстрима будут доходить только запросы, сделанные по HTTPS. Такая конфигурация снижает количество запросов, отправляемых на апстрим.



ВАЖНО

Если вы планируете включить для домена защиту от ботов (см. [Перенаправление с установкой cookie](#)), то важно, чтобы перенаправления с HTTP на HTTPS выполнял не сам апстрим, а обратный прокси Curator. В противном случае защита от ботов будет работать некорректно.

Принцип работы

В настройках домена в личном кабинете Curator находится раздел «[HTTP-перенаправления](#)» со списком правил. Создавая и редактируя эти правила, вы можете управлять поведением обратного HTTP-прокси. Правила могут быть добавлены в любом порядке.

При поступлении входящего запроса обратный прокси ищет во всём списке правил наиболее специфичное правило, которое может быть применено к запросу. Это позволяет настраивать сложные комбинации правил перенаправления, см. [Примеры](#).

Запрос	Перенаправление	
http:// ANY	301 https:// \$hostname \$path ? \$args	Редактировать Удалить
http://example.com	301 https://www.example.com \$path ? \$args	Редактировать Удалить
https://example.com	301 https://www.example.com \$path ? \$args	Редактировать Удалить
http://old.example.com	Выключено	Редактировать Удалить

У каждого правила есть условия, при которых оно должно срабатывать («Запрос»):

- протокол, который использовал пользователь в исходном запросе — HTTP или HTTPS,
- хост, к которому сделан запрос — конкретная строка либо значение «ANY», соответствующее любому хосту.

Если обратный HTTP-прокси нашёл в списке правило, подходящее для текущего запроса, он выполняет описанные в нём действия («Перенаправление»).

- Пользователю может быть отправлен код HTTP-ответа, выбранный вами из списка:
 - 301 Moved Permanently
 - 302 Found
 - 307 Temporary Redirect
 - 308 Permanent Redirect
- При составлении URL, на который будет совершено перенаправление, будут использованы хост и путь, введённые вами либо скопированные из исходного запроса.
- GET-аргументы могут быть скопированы из исходного запроса либо удалены.
- Перенаправление для конкретного правила может быть выключено полностью. В этом случае запросы, соответствующие условиям этого правила, будут переданы в вашу сеть.

Примеры

Принудительное включение протокола HTTPS

Запрос	Перенаправление
http:// ANY	301 https:// \$hostname \$path ? \$args

В этой конфигурации обратный HTTP-прокси заменяет протокол у всех поступающих запросов с HTTP на HTTPS. Рекомендуется использовать код состояния 301 Moved Permanently, чтобы браузер пользователя мог кешировать ответ на своей стороне и не выполнять обращения по протоколу HTTP в следующий раз.

Создание исключений из правила

Запрос	Перенаправление
<code>http://ANY</code>	301 <code>https://\$hostname \$path ? \$args</code>
<code>http://old.example.com</code>	<i>Выключено</i>

Этот пример аналогичен [примеру с принудительным перенаправлением на HTTPS](#), но к нему добавлено второе правило, которое говорит, что для запросов к хосту `old.example.com` перенаправление выполняться не должно. Обратный HTTP-прокси при сопоставлении запроса с правилами отдаёт предпочтение более точному совпадению, поэтому первое правило перестает срабатывать для запросов к `old.example.com`.

Такая конфигурация может быть полезна, если среди сайтов, обслуживаемых вашим апстримом, есть один или несколько, которые не поддерживают работу по защищённому протоколу HTTPS, но вы хотите принудительно включать этот протокол для всех остальных сайтов.

Перенаправление на новый хост

Запрос	Перенаправление
<code>https://ANY</code>	301 <code>https://www.example.com/</code>
<code>https://www.example.com</code>	<i>Выключено</i>

Предположим, что содержимое вашего сайта находилось на хостах `wiki.example.com`, `app.example.com` и других поддоменах `*.example.com`, обслуживаемых одним апстримом, но после изменения структуры возникла необходимость перенаправлять всех посетителей с этих хостов на главную страницу сайта на новом основном хосте `www.example.com`.

В такой ситуации вы можете создать два правила, как описано выше. Под первое условие в первом правиле попадают все HTTPS-запросы, но второе правило создаёт исключение из первого для основного хоста, не допуская таким образом циклических перенаправлений.

Технологии: Защищённый DNS-сервер

Обеспечение доступности DNS-сервера является важной частью защиты веб-сервиса. Если злоумышленник сделает недоступным DNS-сервер, для большинства пользователей это может означать недоступность сайта или неработоспособность приложения, обращающегося к вашему домену. Кроме того, информация о недоступности DNS-сервера обычно на некоторое время сохраняется в кеше на устройстве пользователя или на используемом им рекурсивном DNS-сервере, таком как Google Public DNS или рекурсивный DNS-сервер интернет-провайдера. Из-за этого пользователи могут продолжать испытывать проблемы с доступом к вашему сайту даже после того, как атака на DNS-сервер прекращена.

Чтобы защититься от атак на DNS-сервер, можно использовать *защищённый DNS-сервер* от Curator. Ниже приведены [общий принцип работы](#) данной услуги и описания двух возможных режимов работы: [режима вторичного DNS-сервера](#) и [режима проксирующего DNS-сервера](#).

Инструкция по подключению услуги находится в статье [Подключение: Защищённый DNS-сервер](#).

Принцип работы

Атака на DNS-сервер обычно представляет собой большое количество одновременных запросов к нему. Злоумышленник рассчитывает, что поскольку расходы на обработку DNS-запроса превышают расходы на его создание, атакуемый DNS-сервер либо существенно замедлится, либо полностью перестанет обрабатывать запросы от легитимных пользователей. DNS-серверы Curator могут сохранять работоспособность во время атак благодаря большой пропускной способности сети Curator, в которой они расположены.

При первичной настройке услуги клиент указывает DNS-сервер Curator в качестве авторитативного сервера своей DNS-зоны (см. [Подключение: Защищённый DNS-сервер](#)). Таким образом, пользователь делает запросы не к DNS-серверу клиента, а к одному из DNS-серверов Curator. Эти серверы транслируют данные, полученные от DNS-сервера клиента одним из двух способов:

- путём передачи DNS-зоны (см. [Режим вторичного DNS-сервера](#))
- путём проксирования DNS-ответов (см. [Режим проксирующего DNS-сервера](#))



ВАЖНО

Вне зависимости от выбранного режима работы рекомендуется выполнить переключение на защищённый DNS-сервер Curator заранее, не дожидаясь возможной атаки.

Смена DNS-сервера, начатая во время атаки, зачастую не может быстро минимизировать ущерб, поскольку и пользователи, и рекурсивные DNS-серверы продолжают попытки обращаться к прежнему DNS-серверу до истечения времени жизни кеша.

Режим вторичного DNS-сервера

Данный режим предполагает использование стандартного механизма передачи зоны (zone transfer), при котором DNS-сервер клиента является первичным (primary), а DNS-сервер Curator — вторичным (secondary). Механизмы взаимодействия между первичным и вторичным DNS-серверами описаны в RFC 1996 и RFC 5936.

DNS-сервер Curator запрашивает у первичного сервера полную информацию о зоне, включая запись SOA (start of authority), и отвечает на запросы пользователей в соответствии с полученной информацией.

По умолчанию повторное обращение к первичному серверу происходит по истечении периода, указанного в поле refresh записи SOA. Также первичный сервер может отправить DNS-серверу Curator запрос notify, в этом случае DNS-сервер Curator запрашивает полную информацию о зоне от DNS-сервера клиента немедленно.

Если сервер клиента оказывается недоступен, то DNS-сервер Curator продолжает использовать данные, полученные при последнем успешном обновлении.

Режим проксирующего DNS-сервера

В этом режиме DNS-серверы клиента и Curator не вступают в отношения первичного и вторичного сервера и взаимодействуют без авторизации. Получив новый запрос от пользователя, проксирующий сервер в неизменном виде перенаправляет его к серверу клиента. Если сервер клиента отвечает на запрос, то этот ответ перенаправляется пользователю, а также сохраняется в кеш.

По умолчанию срок действия кеша для негативного ответа (ответа об отсутствии искомой записи) считается равным 600 секундам (10 минутам), а для положительного ответа определяется параметром TTL в ответе сервера клиента. В течение этого времени все пользователи, которые делают в точности такой же запрос к DNS-серверу Curator, получают ответ из кеша. После истечения TTL запросы снова перенаправляются к серверу клиента, чтобы обновить кеш. Если при очередном обновлении сервер клиента оказывается недоступен, то DNS-сервер Curator продолжает использовать данные из кеша.

Таким образом, в обычное время проксирующий DNS-сервер Curator снижает нагрузку на DNS-сервер клиента благодаря использованию кеша, а в непредвиденных ситуациях не позволяет временной недоступности DNS-сервера клиента повлечь распространение негативного кеша по другим DNS-серверам.

Возможность принудительного обновления кеша до истечения TTL при использовании данного режима отсутствует.

02

Подключение к Curator

Обзор способов подключения

Защита от ботов

Обратный HTTP-прокси

Ingress-фильтрация

Обратный TCP-прокси

Обратный WebSocket-прокси

Туннели

Curator.CDN

Передача лог-файлов

BGP

Защищённый DNS

Обзор способов подключения

- Подключение: Защита от ботов
- Обратный HTTP-прокси
- Подключение: Ingress-фильтрация
- Подключение: Обратный TCP-прокси
- Подключение: Обратный WebSocket-прокси
- Подключение: Туннели
- Подключение: Curator.CDN
- Передача лог-файлов
- Подключение: BGP
- Подключение: Защищённый DNS-сервер

2.2 ПОДКЛЮЧЕНИЕ К CURATOR

Подключение: Защита от ботов

В этой статье описывается рекомендуемый порядок первичной настройки услуги [защиты от ботов](#) от Curator.

1. Настройте правила обработки запросов
2. Добавьте исключения для доверенных посетителей
3. Протестируйте защиту от ботов
4. Поэтапно включите защиту для всех пользователей



ЧЕК-ЛИСТ ДЛЯ ПОДКЛЮЧЕНИЯ ЗАЩИТЫ ОТ БОТОВ

В результате настройки у вас должны быть выполнены следующие условия:

- в разделе [Bot protection](#) → [Локации](#):
 - заданы правила обработки запросов,
- в разделе [Bot protection](#) → [Посетители](#):
 - активирована опция **Включено**,
 - настройка **А/В Распределение проверок** установлена в 100%.

1. Задайте правила обработки запросов

В разделе **Bot protection** → **Локации** [задайте правила обработки запросов](#), исходя из структуры вашего ресурса. Правила описывают, как следует обрабатывать каждый запрос в зависимости от его HTTP-метода, хоста и пути. Один из возможных наборов правил описан в [примере конфигурации](#).

2. Добавьте исключения для доверенных посетителей

С помощью настроек в разделе **Bot protection** → **Посетители** опишите признаки пользователей, которых следует считать легитимными без проверки.

К таким пользователям вы можете отнести:

- пользователей с определённым HTTP-заголовком,
- пользователей из определённых стран,
- пользователей из определённых подсетей.

Также в разделе **Bot protection** → **Посетители** активируйте опцию «Включено».

3. Протестируйте защиту от ботов



ПРИМЕЧАНИЕ

Перед тестированием убедитесь, что в разделе [Bot protection](#) → [Посетители](#) активирована опция **Включено**, а в [список для принудительной проверки](#) внесены IP-адреса, с которых вы собираетесь выполнять запросы в рамках тестирования.

Протестируйте защиту от ботов с ограниченного количества устройств, чтобы выявить возможные ошибки в правилах, не включая её для всех пользователей. Для этого [включите принудительные проверки для одного или нескольких IP-адресов](#) и выполните запросы с этих IP-адресов. Проверьте, что защита блокирует запросы от ботов, но не блокирует запросы от настоящих пользователей.

Для тестирования рекомендуется использовать браузеры (например, Google Chrome) и консольные утилиты (например, curl).

Ниже приведены несколько возможных наборов сценариев для тестирования доступа к ресурсу.

Пример: доступ к веб-страницам

Этот набор сценариев предназначен для веб-страниц, которые должны быть доступны браузерам, но не ботам.

- С помощью браузера посетите страницу. Страница должна открыться корректно, а браузер должен получить cookie с названием `qrator_jsid`.
- С помощью консольной утилиты обратитесь к странице несколько раз. Каждый раз утилита должна получать ответ со статусом 401 Unauthorized. Данные обо всех запросах, кроме первого, должны появиться в разделе [Bot protection](#) → [Сводка](#).
- С помощью консольной утилиты обратитесь к странице, предоставив в запросе заголовки, для которых настроены [исключения по заголовку](#). Утилита должна получить содержимое от апстрима без ошибок.

Если защита работает некорректно:

- убедитесь, что в [правилах обработки запросов](#) для соответствующих условий заданы правила с действием **Принять и Выдать Проверку**;
- убедитесь, что IP-адрес, с которого выполняется тестирование, добавлен в [список для принудительных проверок](#) и не добавлен в списки [исключений IP](#) и [подсетей](#);
- если настройки защиты от ботов изменены недавно, то подождите несколько минут для их применения.

Пример: доступ к защищённым API-эндпоинтам

Этот набор сценариев предназначен для API-эндпоинтов, обращение к которым должно быть доступно только пользователям, ранее получившим трекингую cookie на одной из веб-страниц.

- С помощью браузера посетите любую страницу, для которой действует правило с действием **Принять и Выдать Проверку**. Браузер должен получить cookie с названием `qrator_jsid`. После этого обратитесь к API-эндпоинту, для которого действует правило **Принять Только с Куки**. Запрос к API-эндпоинту должен выполняться успешно.
- После предыдущего теста удалите cookie с названием `qrator_jsid` в браузере и обратитесь к API-эндпоинту повторно. Браузер должен получить ответ 403 Forbidden. Данные об этом запросе должны появиться в разделе [Bot protection → Сводка](#).
- С помощью консольной утилиты обратитесь к API-эндпоинту. Утилита должна получить ответ со статусом 403 Forbidden. Данные об этом запросе должны появиться в разделе [Bot protection → Сводка](#).
- С помощью консольной утилиты обратитесь к API-эндпоинту, предоставив в запросе заголовки, для которых настроены [исключения по заголовку](#). Утилита должна получить содержимое от апстрима без ошибок.

Если защита работает некорректно:

- убедитесь, что в [правилах обработки запросов](#) веб-страница подпадает под условия для действия **Принять и Выдать Проверку**, а API-эндпоинты подпадают под условия для действия **Принять Только с Куки**;
- убедитесь, что IP-адрес, с которого выполняется тестирование, добавлен в [список для принудительных проверок](#) и не добавлен в списки [исключений IP и подсетей](#);
- если настройки защиты от ботов изменены недавно, то подождите несколько минут для их применения.

Пример: доступ к незащищённым API-эндпоинтам

Этот сценарий предназначен для API-эндпоинтов, обращение к которым должно быть доступно любым пользователям, включая ботов.

- С помощью консольной утилиты обратитесь к API-эндпоинту. Утилита должна получить содержимое от апстрима без ошибок.

Если защита работает некорректно:

- убедитесь, что в [правилах обработки запросов](#) для соответствующих условий заданы правила с действием **Не реагировать**;
- убедитесь, что IP-адрес, с которого выполняется тестирование, добавлен в [список для принудительных проверок](#) и не добавлен в списки [исключений IP и подсетей](#);
- если настройки защиты от ботов изменены недавно, то подождите несколько минут для их применения.

4. Поэтапно включите защиту для всех пользователей

Включение защиты от ботов для сайта рекомендуется производить в несколько этапов, постепенно повышая процент пользователей, трафик от которых будет проверяться. Такой подход позволяет минимизировать ущерб от возможных ошибок в конфигурации.

Для поэтапного включения защиты используйте настройку [A/B Распределение проверок](#). Например, вы можете начать с включения защиты от ботов для 5% пользователей и повышать это значение ещё на 5% каждые несколько минут. Обратите внимание, что сохранение каждого изменения настроек может занимать 5–7 минут.

После каждого изменения настроек отслеживайте изменения на графиках **Трафик** и **Bot protection** в разделе [Статистика](#). Чаще всего равномерному повышению доли проверяемого трафика соответствует равномерное повышение количества выявленных ботов и равномерное снижение легитимного трафика. Однако возможны отклонения от этого паттерна — как из-за случайного попадания под проверку больших сетей ботов, так и из-за ошибочных блокировок легитимных пользователей.

Если вы наблюдаете резкие изменения на графиках, проанализируйте более подробные данные в разделе [Bot protection](#) → [Сводка](#), чтобы установить их причину. При ложноположительных срабатываниях рекомендуется временно отключить защиту от ботов, вернув настройку **A/B Распределение проверок** в значение 0%, исправить настройки в разделе [Bot protection](#) → [Посетители](#) и приступить к поэтапному включению заново.

Если ложноположительных срабатываний не обнаружено, продолжайте постепенно повышать значение **A/B Распределение проверок** вплоть до 100%.

2.3 ПОДКЛЮЧЕНИЕ К CURATOR

Обратный HTTP-прокси

Чтобы обратный HTTP-прокси Curator мог защищать серверы, обслуживающие ваш ресурс, нужно, чтобы весь входящий трафик, предназначенный для ресурса, всегда направлялся на обратный прокси.

Для этого нужно:

1. Настроить DNS так, чтобы трафик к серверам проходил через обратный прокси.
2. Изменить IP-адреса серверов в случае, если серверы уже находятся под атакой.

Если оставить тот же IP-адрес, который использовался ранее, то злоумышленник сможет направить трафик на сервер напрямую, минуя обратный прокси Curator.

3. Настроить фаервол (firewall) на серверах так, чтобы был разрешен трафик только из доверенных сетей.

Если сервер не будет сбрасывать (drop) соединения из неизвестных сетей, то у злоумышленника останется возможность обнаружить его путём перебора IP-адресов. Это позволит направить трафик на сервер напрямую, минуя обратный прокси Curator.

4. Для того, чтобы сохранить информацию о реальных IP-адресах пользователей ресурса, необходимо настроить [обработку заголовка X-Forwarded-For](#)

Настройка DNS

В настройках DNS-зоны измените А-запись для вашего домена на IP-адрес обратного прокси, который отображается как *Curator IP* в личном кабинете. Обратите внимание, что изменения становятся видны другим DNS-серверам и пользователям не сразу. Точное время, которое займёт обновление А-записи, зависит от её значения TTL.

Сеть Curator готова обрабатывать трафик и осуществлять защиту сразу, как только трафик начнёт поступать на обратный прокси.

Смена актуального IP-адреса

**ВАЖНО**

Этой инструкцией следует воспользоваться, если вы уже находитесь под DDoS-атакой.

Иногда злоумышленник располагает архивом старых записей DNS для вашего домена. Поэтому даже после того, как вы смените А-запись на Curator IP, злоумышленник может направить трафик на

настоящий IP-адрес сервера, минуя обратный прокси.

Чтобы защититься от такого вектора атаки, смените IP-адрес апстрима:

1. Убедитесь, что A-запись зоны DNS для нужного домена указывает на Curator IP.
2. Получите у вашего провайдера новый IP-адрес, никогда ранее не использовавшийся для вашего сайта. Не публикуйте новый IP-адрес нигде и не используйте его в записях DNS. Если есть возможность, лучше получить IP-адрес не из той же сети, что предыдущий.
3. В личном кабинете Curator добавьте новый IP-адрес в качестве адреса апстрима. Прежний апстрим, IP-адрес которого может быть известен злоумышленнику, удалите.
4. Прекратите обработку запросов на прежнем IP-адресе.

Curator начнёт использовать обновлённый список апстримов, как только вы сохраните его в личном кабинете.

Настройка файервола

Если IP-адреса для апстримов берутся из одного диапазона, то злоумышленник может попытаться найти актуальный IP-адрес сервера методом перебора адресов в той же сети, к которой принадлежал прежний IP-адрес. Такое бывает, если вы используете адреса из одной и той же собственной сети или от одного и того же провайдера.

Для защиты от обнаружения настройте правила файервола так, чтобы сервер отвечал на запросы только из сетей Curator и из ваших доверенных сетей, а все остальные соединения сбрасывал (drop). Если ни один из серверов не будет отвечать на попытки соединения от злоумышленника, то злоумышленник не сможет узнать, на какой адрес направлять атаку.

Обеспечьте, чтобы в списке разрешённых подсетей, запросы из которых будут обрабатываться, присутствовала подсеть Curator: `185.94.108.0/24`.

Также к этому списку можно добавить доверенную офисную сеть и IP-адреса некоторых сотрудников, если они планируют делать запросы в обход обратного прокси. Соединения от всех остальных адресов необходимо запретить на уровне межсетевого экрана.

В зависимости от операционной системы на апстриме вы можете использовать либо только правила `iptables` для plain HTTP, либо комбинировать их с правилами для `iptables` с поддержкой модулей `conntrack` и `ipset`. Мы рекомендуем использовать как `conntrack`, так и `ipset`, поскольку он делает набор правил `iptables` меньше (тем самым упрощая его обслуживание) и быстрее (меньше правил означает меньшее количество запросов на входящем пакете).

Вы можете убедиться, что настройка для портов 80 и 443 выполнена корректно, в разделе [Утилиты](#) → [Уязвимости](#).

Ниже приведены примеры скриптов, выполняющих такую конфигурацию для `iptables`.

**ПРИМЕРЫ МОГУТ НЕ ПОДОЙТИ К ВАШЕЙ КОНФИГУРАЦИИ**

Приведённые ниже примеры скриптов могут не сработать или иметь нежелательный эффект на вашем сервере. Это зависит от того, какая конфигурация `iptables` используется на данный момент. Будьте внимательны и не используйте скрипты из примеров, если вы не уверены, что они подходят для вашего случая.

Пример конфигурации `iptables` для plain HTTP

```
#!/bin/sh

CURATOR_NODE="
185.94.108.0/24
"

ADMIN_IPS="
127.0.0.1
"

iptables -N trusted_nodes
for IP in $CURATOR_NODE $ADMIN_IPS; do
    iptables -A trusted_nodes -s $IP -j RETURN
done

iptables -A trusted_nodes -j DROP
iptables -A INPUT -p tcp -m multiport --dports 80,443 -j trusted_nodes
```

Пример конфигурации для `iptables` с поддержкой `conntrack` и `ipset`

```
#!/bin/sh

CURATOR_NODE="
185.94.108.0/24
"

ADMIN_IPS="
127.0.0.1
"

ipset -N trusted_nodes hash:net
for IP in $CURATOR_NODE $ADMIN_IPS; do
    ipset -A trusted_nodes $IP
done

iptables -N curator
iptables -A curator -m set --match-set trusted_nodes src -j ACCEPT
iptables -A curator -j DROP

iptables -I INPUT --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 --state NEW -j curator
```

2.4 ПОДКЛЮЧЕНИЕ К CURATOR

Подключение: Ingress-фильтрация

Чтобы воспользоваться [услугой Ingress-фильтрации](#) от Curator, необходимо быть локальным интернет-регистратором (local Internet registry, LIR) и располагать собственной автономной системой (autonomous system, AS). Подключение услуги возможно для префиксов сетей не менее класса C (/24).

Для начала использования Ingress-фильтрации:

- [Добавьте префиксы.](#)
- [Настройте канал до Curator.](#)
- [Настройте политики фильтрации.](#)

Добавление префиксов

Добавление префиксов происходит в два этапа.

Сначала опишите всё адресное пространство транзитной сети, которую вы хотите защитить, и подтвердите право на управление им. Для этого зайдите в раздел «Префиксы» на вкладке «Curator» личного кабинета и укажите один или несколько префиксов сетей. Часто имеет смысл указывать непосредственно те сети, которыми вы управляете, и не делить их на более мелкие подсети. Для каждого префикса введите номер вашей AS, которая является источником (origin) этого префикса. Префикс должен принадлежать этой AS согласно базе данных интернет-регистратора. Для подтверждения операции добавления префикса Curator направит письмо со ссылкой на адрес, указанный как `tech-c` для соответствующей AS.

Затем добавьте подтверждённые сети или их подсети в раздел «Префиксы» на вкладке «Ingress» личного кабинета. На этом этапе вы можете использовать сколь угодно маленькие подсети ваших сетей, для которых вам впоследствии будет удобно настраивать политики фильтрации.

Настройка канала до Curator

Канал связи между вашей автономной системой и сетью Curator может быть установлен разными способами, включая туннели, физические стыки или кроссировки в центрах обработки данных. Доступность конкретных способов подключения зависит от конкретных провайдеров и центров обработки данных, с которыми соединена ваша транзитная сеть.

Рекомендуемым способом подключения является прямое подключение от вашей транзитной сети к сети Curator, используя для этого выделенный канал провайдера или кроссировку в центре обработки данных. Проконсультируйтесь со специалистами технической поддержки, чтобы выбрать наилучший способ подключения для защиты вашей сети.

Обратите внимание, что Ingress-фильтрация работает со входящим трафиком, и направлять через сеть Curator исходящий трафик не требуется, см. [Отличия от защиты конечных сетей](#). В большинстве случаев рекомендуется направлять входящий трафик через сеть Curator, чтобы использовать преимущества Ingress-фильтрации, а исходящий трафик в обход сети Curator, чтобы обеспечить для него максимальную скорость.

Настройка политик фильтрации

[Политики фильтрации](#) представляют собой наборы лимитов, применяемых к входящему трафику. Политики фильтрации настраиваются на вкладке «Ingress» личного кабинета и находятся в отношении «многие ко многим» с указанными вами префиксами. Это позволяет гибко настроить фильтрацию для ваших нужд.



ПРИМЕЧАНИЕ

Один из возможных подходов к настройке политик фильтрации состоит в том, чтобы разработать несколько политик фильтрации, подходящих для конечных сетей с разными объёмами трафика, и назначить нужные политики на префиксы каждой сети.

При настройке лимитов рекомендуется взять за основу те объёмы легитимного трафика, которые проходят через вашу сеть в обычное время. Оптимальный способ выразить эти объёмы в виде набора политик зависит от характера сервисов в конечных сетях, постоянности или сезонности их трафика, модели угроз. Вы можете проконсультироваться со специалистами технической поддержки Curator, чтобы подобрать оптимальные политики Ingress-фильтрации, подходящие для вашей транзитной сети.

2.5 ПОДКЛЮЧЕНИЕ К CURATOR

Подключение: Обратный TCP-прокси

Данная статья описывает подключение к обратному TCP-прокси Curator в режиме [Proxy Protocol](#) или [Raw TCP Proxy](#).

Подробнее о принципах работы и различиях между этими режимами читайте в статье [Технологии: Обратный TCP-прокси](#).

Подключение в режиме Proxy Protocol

Подключение к Curator с помощью Proxy Protocol позволяет защитить от DDoS-атак трафик на уровне TCP-сегментов с сохранением информации об отправителе.

Требуемое ПО

TCP-сегмент с заголовком Proxy Protocol отличается от обычного TCP-сегмента и требует дополнительной обработки принимающей стороной. Обработкой может заниматься любое программное обеспечение за апстримом, умеющее работать с этим протоколом. Например, оно может быть установлено на маршрутизаторы или отдельные серверы.

Некоторые специализированные программные пакеты имеют встроенную поддержку Proxy Protocol. Так, почтовый сервер Dovecot или торговая платформа MetaTrader могут принимать сегмент по этому протоколу без дополнительных инструментов.

Актуальный список ПО, поддерживающего Proxy Protocol, можно найти [на сайте HAProxy](#).

Обратите внимание, что существуют две версии протокола. Proxy Protocol v1 использует текстовый формат заголовка, тогда как Proxy Protocol v2 использует бинарный формат. Накладные расходы на передачу и обработку данных при использовании бинарной версии протокола ниже в сравнении с текстовой версией. В некоторых версиях программного обеспечения поддерживается только один из вариантов протокола. Например, поддержка Proxy Protocol v1 есть в NGINX 1.5.12 и выше, но поддержка Proxy Protocol v2 есть только в NGINX 1.13.11 и выше.

Некоторое программное обеспечение, например, торговая платформа MetaTrader 5, поддерживает Proxy Protocol без дополнительной настройки.

О том, как включить использование Proxy Protocol в том или ином программном обеспечении, читайте в соответствующей документации, например:

- [Параметр accept-proxy в HAProxy](#)
- [Настройка Proxy Protocol в NGINX](#)

Переключение между апстримами

По умолчанию, если настроен всего один апстрим, обратный TCP-прокси пытается отправлять все TCP-сегменты от пользователей на этот апстрим, а если соединение с апстримом не удаётся установить в течение 5 секунд, то сообщает пользователю об ошибке.

Если вы настроили два или более апстрима, то в случае ошибки при подключении к одному из них, обратный TCP-прокси будет обращаться к следующему апстриму по списку. Обратите внимание, что один и тот же порядок проверки апстримов будет использоваться для каждого запроса. Это означает, что при долговременном выходе из строя основного апстрима запросы всех пользователей станут обрабатываться с задержкой не менее 5 секунд. Поэтому если вы знаете, что один из ваших апстримов сейчас недоступен, обратитесь в техническую поддержку, чтобы временно убрать его из списка используемых апстримов или изменить их порядок.

Также по вашему обращению техническая поддержка Curator может настроить активную проверку апстримов, чтобы автоматически включать и отключать каждый апстрим в зависимости от его доступности. Активная проверка выполняется каждым узлом сети Curator по отдельности и работает следующим образом:

1. В рамках каждой проверки обратный TCP-прокси выполняет специальный диагностический запрос о состоянии каждого апстрима. Этот запрос делается к специальному healthcheck-сервису, который может находиться как на самом апстриме, так и по любому другому указанному вами URL. Запрос выполняется по протоколу HTTP или HTTPS к определённому URL на апстриме. При необходимости вы можете указать HTTP-метод (по умолчанию GET), HTTP-заголовки (в том числе `Host`) и тело запроса, которые будут отправляться.
2. Если с апстримом не удалось установить соединение в течение определённого времени (по умолчанию 5 секунд) или он вернул ответ с определённым статусом (по умолчанию любой статус HTTP 5xx), это считается ошибкой. При необходимости обратный TCP-прокси может также проверять содержимое тела запроса, а также сертификат апстрима при соединении по HTTPS.
3. По умолчанию обратный TCP-прокси настроен так, что после произошедшей ошибки он сразу же выводит апстрим из обращения. Это означает, что пользовательский трафик временно не будет на него направляться.

Для защиты от ложных срабатываний можно настроить обратный TCP-прокси так, чтобы в рамках одной проверки он выполнял несколько диагностических запросов друг за другом сразу или с небольшой задержкой. Обратный TCP-прокси будет считать количество успешных и неуспешных попыток и закончит проверку, как только накопится определённое количество успешных попыток или определённое количество неуспешных попыток. В зависимости от того, какое событие наступит раньше, апстрим будет признан активным или неактивным.

Полная проверка всех апстримов, включая выведенные из обращения, выполняется каждые несколько секунд. По умолчанию интервал равен 15 секундам, но его можно изменить в зависимости от ваших нужд.

Порядок настройки подключения

1. В разделе [Сервисы](#) личного кабинета Curator настройте сервис типа «*TCP Proxy*». Укажите для него IP-адреса и порты ваших апстримов, принимающих трафик по протоколу Proxy Protocol.

2. В случае настройки нескольких апстримов выберите необходимые параметры [переключения между ними](#).
3. Если необходимо, сообщите специалистам технической поддержки Curator версию протокола, которую поддерживает ПО на вашей стороне. По умолчанию будет использована версия Proxy Protocol v2.
4. Если вам необходима защита от DDoS-атак на уровне приложений (application layer модели OSI/ISO), то обеспечьте оперативную [передачу логов сервера для анализа на серверы Curator](#). Если этого не сделать, обратный TCP-прокси не сможет выполнять защиту от атак на уровне приложения (L7).
5. Согласуйте с технической поддержкой время включения обратного TCP-прокси. Обратите внимание, что если апстрим по этому IP-адресу сейчас работает через обратный HTTP-прокси, то при переключении возможна временная недоступность сайта в течение около 10 минут.
6. В заданное время включите поддержку Proxy Protocol на своей стороне.

Подключение в режиме Raw TCP Proxy

Режим Raw TCP Proxy подходит для случаев, когда включение поддержки Proxy Protocol на апстриме затруднено или невозможно, при этом информация об отправителе TCP-сегментов не критична для работы апстрима.

Дополнительной настройки на стороне апстримов не требуется.

2.6 ПОДКЛЮЧЕНИЕ К CURATOR

Подключение: Обратный WebSocket-прокси

Обратный WebSocket-прокси позволяет пропускать весь WebSocket-трафик между пользователем и апстримом через сеть Curator. Подробнее читайте в статье [Технологии: Обратный WebSocket-прокси](#).

Ниже описан необходимый [порядок настройки подключения](#) обратного WebSocket-прокси, а также информация по настройке [лимитов](#) и [балансировки](#) для этой услуги.

Порядок настройки

1. Сконфигурируйте клиентскую часть своего приложения так, чтобы WebSocket-трафик направлялся на специально выделенный для этого порт.

Curator использует один и тот же IP-адрес как для получения трафика по протоколам HTTP и HTTPS, так и для получения трафика по протоколу WebSocket. Для корректного анализа и защиты необходимо, чтобы эти два вида трафика приходили на этот IP-адрес на разные порты.

**ПРИМЕЧАНИЕ**

Например, вы можете настроить своё приложение так, чтобы оно использовало порт 8080 для передачи WebSocket-трафика, оставив при этом обработку HTTP- и HTTPS-трафика на стандартных портах 80 и 443.

Обратный WebSocket-прокси в ответ на любой HTTP-запрос, отличный от HTTP [101 Switching Protocols](#), возвращает ответ с кодом ошибки HTTP [400 Bad Request](#).

2. В разделе [Сервисы](#) личного кабинета Curator настройте сервис типа «*WebSocket*». Укажите для него IP-адреса и порты ваших апстримов, обрабатывающих WebSocket-трафик. Они могут не совпадать с IP-адресами и портами апстримов для [обратного HTTP-прокси](#).

При использовании нескольких апстримов одновременно будет задействована балансировка, см. раздел [Балансировка](#).

3. Если необходимо, сообщите специалистам технической поддержки Curator лимиты на количество одновременных подключений с одного IP-адреса. Подробнее об этом написано в разделе [Лимиты](#).
4. Настройте фаервол (firewall) на апстримах так, чтобы был разрешен трафик только из доверенных сетей.

Рекомендации по настройке фаервола даны в [соответствующем разделе статьи «Подключение: Обратный HTTP-прокси»](#). Обратите внимание, что в приведённых в нём скриптах необходимо заменить порты 80 и 443 на порты, на которых ваш апстрим принимает запросы по протоколу WebSocket.

Лимиты

Чтобы затруднить проведение DDoS-атак на апстримы вашего приложения, Curator ограничивает количество WebSocket-соединений, которые пользователи могут инициировать с одного IP-адреса. При исчерпании лимитов WebSockets-прокси будет отклонять новые попытки установить соединения до тех пор, пока какое-либо из ранее установленных соединений не будет закрыто.

Лимиты, используемые по умолчанию, подходят для большинства клиентов, но могут быть изменены при необходимости. Так, если ваше приложение должно обращаться одновременно ко многим WebSocket-ресурсам для одного пользователя, сообщите об этом специалистам технической поддержки, и они увеличат лимит соответствующим образом. Это позволит избежать ошибочных блокировок легитимного трафика.

Если вы планируете часто делать запросы к ресурсу с некоторых заранее известных IP-адресов, сообщите эти IP-адреса технической поддержки для добавления в белый список. На запросы из этого списка будут действовать увеличенные лимиты.



ПРИМЕЧАНИЕ

Часто клиенты добавляют в белый список сети своих офисов, например, чтобы частое тестирование ресурса со стороны клиента не распознавалось обратным прокси как превышение лимита.

Балансировка

При работе с несколькими апстримами обратный WebSocket-прокси распределяет пользователей между ними, используя алгоритм *IP hash*. Этот алгоритм выбирает апстрим в зависимости от IP-адреса запроса, при этом повторные соединения с того же IP-адреса устанавливаются с тем же апстримом. На практике это означает, что все соединения, инициируемые одним пользователем, с высокой вероятностью будут проксированы до одного и того же апстрима — что выгодно, в частности, для более эффективного использования кэша на каждом сервере.

Если при попытке установить соединение апстрим не отвечает на запрос в течение 5 секунд, то обратный прокси пытается установить соединение со следующим апстримом по списку. Порядок апстримов в списке может быть изменён по обращению в техническую поддержку.

Ответ со статусом HTTP `400 Bad Request`, сигнализирующий о невозможности установить соединение, будет отправлен пользователю только после того, как неудачей завершатся попытки установить соединение с каждым апстримом по очереди.

2.7 ПОДКЛЮЧЕНИЕ К CURATOR

Подключение: Туннели

Туннелирование — это один из способов организовать связь между сетью Curator и вашей сетью. Эта технология позволяет создать виртуальное соединение — *туннель* — поверх интернета и пропускать через него трафик так, как будто эти сети связаны напрямую друг с другом. Через туннель можно организовать работу других технологий и услуг Curator, например, [обратного HTTP-прокси](#) или [подключения через BGP](#).

Curator поддерживает настройку туннелей типа «точка-точка» с помощью протоколов IPsec или GRE.

Если вам необходима защита от DDoS-атак на уровне приложений (application layer модели OSI/ISO), то обеспечьте оперативную [передачу логов сервера](#) для анализа на серверы Curator в автоматическом режиме. Если этого не сделать, сеть Curator не сможет выполнять защиту от атак на уровне приложения (L7). Подробности о вариантах передачи логов уточняйте у специалистов технической поддержки.

Чтобы начать использовать туннелирование, выполните три шага:

1. Создайте туннель в личном кабинете (см. раздел «[Туннели](#)»).
2. Сообщите технической поддержке желаемую [конфигурацию на стороне Curator](#).
3. Выполните [настройку своего эндпоинта](#).

Принцип работы туннелей

Туннель создаётся между двумя эндпоинтами, подключёнными к интернету. Один из них находится в сети Curator, другой в вашей сети.

Эндпоинт — это сущность, которая маршрутизирует входящий и исходящий туннельный трафик на одном из концов туннеля. Например, в качестве эндпоинта могут выступать: маршрутизатор, фаервол, виртуальная машина с Linux в роли маршрутизатора, непосредственно сервер, на котором размещены ваши ресурсы, и так далее.

**ПРИМЕЧАНИЕ**

Эндпоинт для туннеля создаётся в каждом из центров очистки трафика в сети Curator. Все они имеют используют одинаковую конфигурацию и одинаковые адреса, благодаря чему становятся взаимозаменяемыми. С точки зрения клиента, все эндпоинты в сети Curator можно рассматривать как один эндпоинт с высокой отказоустойчивостью.

При настройке туннеля используются две пары IP-адресов: *внешние* и *внутренние*.

- Внутренние адреса — это адреса, назначенные эндпоинтам внутри виртуальной сети. Например, приложение на вашем сервере может отправлять IP-пакеты на внутренний адрес в сети Curator так,

как будто этот адрес есть в одной сети с сервером.

Если эндпоинт на вашей стороне не поддерживает использование внутренних IP-адресов при настройке туннелей типа «точка-точка», можно указать имя сетевого интерфейса, см. [Настройка на стороне клиента](#).

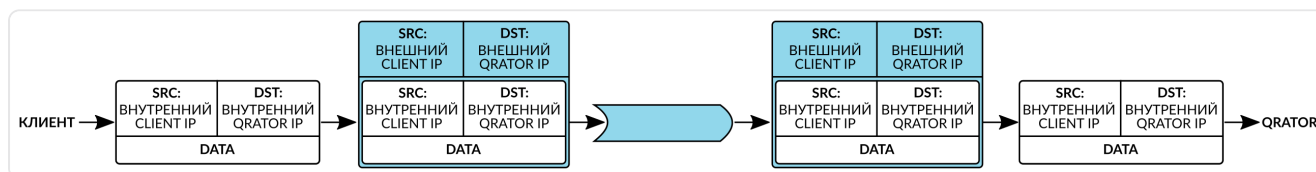
Внутренние адреса генерируются автоматически при [добавлении туннеля в личном кабинете](#).

- Внешние адреса — это реально существующие адреса, по которым эндпоинты доступны в интернете. Так, ваш эндпоинт упаковывает IP-пакет, отправляемый на внутренний IP-адрес Curator, в другой пакет, отправляемый на внешний IP-адрес Curator.

В качестве внешнего Curator IP используется IP-адрес, соответствующий домену, для которого настраивается туннель. Внешний IP-адрес клиента указывает сам клиент.

Все промежуточные узлы, через которые проходит пакет во внешней сети, проверяют только внешние IP-адреса и маршрутизируют пакет согласно протоколам маршрутизации. Когда пакет приходит на внешний IP-адрес туннеля на стороне Curator, эндпоинт отбрасывает внешние заголовки и далее работает с пакетом, который был отправлен приложением изначально.

Таким образом, с точки зрения приложения на стороне клиента осуществляется прямая передача пакета в сеть Curator без изменений вне зависимости от того, какой именно маршрут до Curator был использован на самом деле.



Пакеты в обратную сторону пересылаются аналогичным образом.

Настройка на стороне Curator

Трансляция портов

Чтобы защитить клиента от нежелательного трафика, сеть Curator пропускает через туннель пакеты только к тем портам, которые клиент явно обозначил как *открытые*. Например, для веб-сервисов обычно требуется держать открытыми только порты 80 и 443.

По умолчанию никакие порты не считаются открытыми. Чтобы открыть порт, в личном кабинете [создайте сервис типа «TCP»](#).

Резервирование туннелей

Сеть Curator состоит из множества центров очистки трафика в разных регионах, но по умолчанию все они используют один и тот же туннель для связи с вашим эндпоинтом. Этот туннель помечен как *активный туннель* в [разделе «Туннели» личного кабинета](#). Вы можете самостоятельно выбрать, какой из туннелей назначить активным. Curator не будет пытаться отправлять трафик в неактивные туннели.

Чтобы обеспечить резервирование на случай отказа, а также максимально полно использовать преимущества распределённой сети Curator, рекомендуется настроить несколько туннелей до разных точек и включить автоматическое переключение между ними.

Автоматическое переключение работает следующим образом:

1. Раз в 120 секунд каждый центр очистки трафика делает диагностический запрос на внутренний адрес туннеля на стороне клиента для проверки доступности каждого туннеля. Запрос может осуществляться по протоколам ICMP, HTTP или HTTPS. Параметры запроса и время ожидания ответа (в миллисекундах) настраиваются в личном кабинете.
2. Если центр очистки трафика несколько раз подряд не смог получить ответ, то туннель считается временно недоступным, и трафик направляется в следующий доступный туннель согласно списку из личного кабинета. Статусы доступности туннелей отслеживаются каждым центром очистки трафика независимо от других центров.
3. Когда проверка вновь выполняется успешно, центр очистки трафика считает туннель доступным.

Таким образом, даже если из каждого региона стабильно доступен только один туннель, сеть Curator продолжит доставлять трафик от любого пользователя до вашей сети.

Изменение внутреннего IP-адреса

Curator назначает всем туннелям одного клиента одинаковые внутренние IP-адреса. Благодаря этому вы можете использовать одинаковую конфигурацию на всех эндпоинтах на вашей стороне. Между несколькими доступными туннелями с одинаковым внутренним IP-адресом будет выполняться балансировка трафика.



ПРИМЕЧАНИЕ

Техническая поддержка Curator может изменить внутренний IP-адрес туннелей по вашему запросу.

Настройка на стороне клиента

Эндпоинтом, находящимся на вашем конце туннеля, может быть как непосредственно апстрим, так и роутер, обслуживающий несколько ваших серверов.

В общем случае настройка сводится к следующим шагам:

1. Создайте в системе новый туннель, используя IP-адреса, которые были сгенерированы в личном кабинете Curator. Система начнёт принимать входящие пакеты из этого туннеля автоматически.
2. Настройте эндпоинт так, чтобы для пакета, полученного через туннель, ответный пакет также направлялся в туннель. Для этого можно настроить отдельную таблицу маршрутизации (например, с помощью VRF), настроить маршрутизацию с помощью политик (PBR) или воспользоваться комбинацией этих методов.

Если нет возможности настроить внутренние IP-адреса для туннеля — используйте имя туннельного интерфейса при настройке маршрутизации трафика в туннель. Это возможно, т. к. настраиваются туннели типа «точка-точка».

Обратите внимание, что без правильной настройки VRF или PBR ваш эндпоинт не сможет отправлять исходящие пакеты через туннель и будет получать только входящий трафик, что приведёт к некорректной работе ресурса. Специалисты технической поддержки Curator помогут вам выполнить правильную настройку.

Операционная система Windows не поддерживает настройку VRF и PBR. Если ваш сервер работает под управлением Windows, рекомендуется подключить его к интернету не напрямую, а через прокси-сервер под управлением Linux или роутер.

Чтобы избежать фрагментации пакетов при маршрутизации, рекомендуется настроить MTU (maximum transmission unit) и MSS (maximum segment size) с учетом выбранного туннельного протокола:

- Для туннелей IP/IP установите MTU не более 1480 байт, MSS не более 1440 байт.
- Для туннелей GRE установите MTU не более 1476 байт, MSS не более 1436 байт.

Если внутри туннеля будет проходить трафик, также представляющий собой один или несколько туннелей, то значения MTU и MSS должны быть скорректированы соответствующим образом.

Подключение: Curator.CDN

Прямо в личном кабинете Curator клиенты могут подключить и настроить услугу Curator.CDN.

Домен и сертификат

Для использования Curator.CDN вам необходимо настроить сайт таким образом, чтобы для статического контента использовался отдельный домен. Curator.CDN будет обрабатывать запросы пользователей к этому домену, при необходимости обращаясь к вашему апстриму и обновляя контент оттуда.

Curator.CDN автоматически создаёт для каждого сайта домен, который может быть использован для этих целей. Однако часто клиентам нужно, чтобы статический контент располагался на их собственном домене — например, определённом поддомене основного домена. В таком случае необходимо завести запись CNAME в соответствующей DNS-зоне.

При обращении к домену по протоколу HTTPS будет использован сертификат, указанный клиентом. Вы можете использовать любой сертификат, предварительно загруженный в *хранилище сертификатов* в личном кабинете.

См. руководство по использованию личного кабинета: [Добавить HTTP-хост](#), [Добавить HTTPS-хост](#).

Настройки заголовков

Хотя CDN не модифицирует тело контента, который кеширует (за исключением опциональной обработки изображений, см. ниже), зачастую возникает необходимость в том, чтобы CDN добавил тот или иной HTTP-заголовок к запросу пользователя или ответу апстрима. Curator.CDN может добавлять произвольные заголовки, описанные в личном кабинете.

Также Curator.CDN может указывать исходный IP-адрес пользователя в специальном заголовке, название которого вы можете настроить в личном кабинете.

См. руководство по использованию личного кабинета: [Изменить настройки HTTP-заголовков](#).

Списки запрещённых и разрешённых URL

Клиент может настроить список запрещённых URL, на запросы которых CDN будет отвечать с кодом ошибки, не запрашивая контент из с апстрима. Конкретный код ошибки настраивается клиентом индивидуально для каждого URL.

При необходимости клиент может также задать список разрешённых URL. В этом случае CDN будет запрашивать контент только для URL из этого списка, а на все остальные отвечать кодом ошибки. Код ошибки по умолчанию — `404 Not Found`, но он может быть переопределён для отдельных страниц с помощью списка запрещённых URL.

См. руководство по использованию личного кабинета: [Настроить политики для URL запросов](#).

Настройки кеширования

Эффективное кеширование является основной задачей CDN, и важно, чтобы оно выполнялось корректно, с учётом структуры размещения контента на сайте. Поэтому в личном кабинете клиент может настроить то, как CDN будет работать с HTTP-заголовком `Cache-Control`, а также включить или отключить кеширование ошибок определённых типов. Также клиент может включить игнорирование всех GET-параметров запроса. Например, это удобно, если вы полагаетесь на случайно сгенерированные GET-параметры для принудительного обновления закешированного контента браузером, но не хотите, чтобы это приводило к лишним запросам от CDN к апстриму.

В некоторых случаях после обновления контента на апстриме или значительных изменений настроек кеширования может быть полезно удалить некоторые файлы из кеша. Это может быть сделано через личный кабинет.

Вы можете попросить специалистов технической поддержки Curator принудительно закешировать и обновить часть контента в CDN (выполнить так называемый «прогрев» CDN), не дожидаясь момента, когда этот контент впервые запросят пользователи. Это бывает нужно, если на сервере-источнике обновляется значительная часть контента. Без выполнения предварительного кеширования загрузка нового контента для первых пользователей может производиться дольше обычного, т. к. в CDN еще не будет закешированного контента и кеши будут наполняться постепенно.

См. руководство по использованию личного кабинета: [Изменить настройки кеширования](#).

Обработка изображений

Для изображений JPEG, PNG, TIFF, WebP и AVIF (типы определяются по заголовку `Content-Type`) Curator.CDN может выполнять простые операции в соответствии с GET-параметрами в запросе пользователя.

- `crop` — обрезать изображение.

Значение GET-параметра должно иметь формат `x{число},y{число},w{число},h{число}`. Операция возвращает содержимое прямоугольника, начинающегося в точке `(x,y)` от верхнего левого угла и имеющего размер `w×h`.

Пример ниже указывает, что Curator.CDN должен загрузить изображение `image.png` из апстрима и вернуть его фрагмент размером 500×200 пикселей, отступив 10 пикселей слева и 15 пикселей сверху.

```
https://cdn.example.com/image.png?crop=x10,y15,w500,h200
```

- **resize** — масштабировать изображение.

Значение GET-параметра должно иметь формат **w{ЧИСЛО}** для масштабирования к указанной ширине или **h{ЧИСЛО}** для масштабирования к указанной высоте. Пропорции изображения при масштабировании сохраняются.

Если **resize** используется вместе с **crop**, то масштабирование применяется к результату операции **crop**.

Пример ниже указывает, что Curator.CDN должен загрузить изображение **image.png** из апстрима и вернуть его копию, уменьшенную или увеличенную до ширины 300 пикселей.

```
https://cdn.example.com/image.png?resize=w300
```

- **format** — конвертировать изображение в нужный формат.

Значение GET-параметра может быть одной из строк: **jpeg**, **png**, **webp**, **avif**. Опциональный параметр **q{ЧИСЛО}** (допустимы значения от 1 до 100) указывает конвертеру, насколько близким к оригиналу следует сохранять качество изображения. Реальное качество может отличаться в зависимости от выбранного формата.

Пример ниже указывает, что Curator.CDN должен загрузить изображение **image.png** из апстрима и вернуть его копию в формате JPEG с уровнем качества 75.

```
https://cdn.example.com/image.png?format=jpeg,q75
```

Обратите внимание, что при невалидных или отсутствующих параметрах для операции Curator.CDN вернёт оригинал изображения без изменений.

При использовании операций **crop** или **resize** без операции **format** Curator.CDN вернёт изображение в формате JPEG либо WebP (если включено [Преобразование изображений в WebP](#)).

Преобразование изображений в WebP

Для ускорения работы сайта можно использовать режим автоконвертации изображений в формат **WebP**. Формат WebP обеспечивает более компактный размер файла при сравнимом качестве изображения.

Когда режим автоконвертации включён, Curator.CDN определяет по заголовку **Accept** в запросе, поддерживает ли браузер пользователя формат WebP. Если формат поддерживается, то вместо каждого изображения пользователю отправляется версия этого изображения в формате WebP. Исходные версии изображений остаются в кеше Curator.CDN. Если версия браузера пользователя не поддерживает WebP, то Curator.CDN отправляет исходную версию изображения без изменений.

См. руководство по использованию личного кабинета: [Настроить конвертацию изображений в WebP](#).

Настройки транспорта

По умолчанию Curator.CDN отдаёт статический контент только по протоколу HTTP/1.1. Вы можете включить поддержку [HTTP/2](#), чтобы обеспечить более эффективную передачу трафика за счёт сжатия заголовков, мультиплексирования запросов и некоторых других техник.

Как для HTTP/1.1, так и для HTTP/2 вы можете выбрать используемый формат потокового сжатия трафика. Curator.CDN поддерживает форматы сжатия `gzip`, `deflate`, `br`, а также передачу без сжатия. Переключение между ними осуществляется в личном кабинете.

См. руководство по использованию личного кабинета: [Изменить настройки транспорта](#).

2.9 ПОДКЛЮЧЕНИЕ К CURATOR

Передача лог-файлов

Отправка логов веб-серверов на серверы Curator позволяет анализировать и очищать HTTP-трафик, идущий к этим веб-серверам на уровне приложений (L7 по модели OSI/ISO) в тех ситуациях, когда техническая возможность анализировать сам HTTP-трафик отсутствует.

В частности, рекомендуется настроить отправку логов, если вы используете [обратный TCP-прокси Curator](#). Этот прокси анализирует трафик на транспортном уровне (L4), но с помощью анализа логов может также осуществлять защиту от некоторых атак уровня приложений (L7).

Чтобы передавать логи в сеть Curator:

1. Определите IP-адреса и порты для передачи логов.
2. Задайте формат логов.
3. Настройте сбор и отправку логов.

**ВАЖНО**

Для анализа требуются логи именно того веб-сервера в вашей сети, который принимает внешние запросы первым, вне зависимости от того, куда он маршрутизирует или проксирует их позже. При этом необходимы только логи доступа (access logs). Логи ошибок передавать не требуется.

1. Определите IP-адреса и порты для передачи логов

Этот шаг выполняется вами совместно со специалистами технической поддержки Curator. С вашей стороны необходимо зафиксировать, с какого IP-адреса будет происходить отправка логов. Со стороны Curator будут назначены IP-адрес и порт приёмника логов (log receiver). Назначенный IP-адрес может отличаться от Curator IP, указанного в личном кабинете.

2. Задайте формат логов

Настройте сервер так, чтобы логи доступа (access logs) записывались в определённом формате, из которого обратный TCP-прокси Curator сможет извлечь всю необходимую для анализа информацию. Требования к формату логов могут меняться в будущем, в этом случае специалисты технической поддержки Curator заблаговременно сообщат вам об изменениях.

Ниже представлены актуальные форматы логов для популярных веб-серверов.

NGINX

Укажите следующую строку в опции **log_format**.

```
'2xXXXXXX|:,$bytes_sent|:,$http_accept|:,$http_accept_encoding|:,$http_accept_language|:,$http_cookie|:,$http_host|:,$http_referer|:,$http_user_agent|:,$http_x_forwarded_for|:,$remote_addr|:,$request|:,$request_time|:,$status|:,$time_local|:,$upstream_response_time|:,$http_x_requested_with|:,$http_authorization|:,$remote_port|:,$-|:,$msec|:,$-|'
```

Apache

Укажите следующую строку в опции **CustomLog**.

```
'5xXXXXXX|:,$%O|:,$%{Accept}i|:,$%{Accept-Encoding}i|:,$%{Accept-Language}i|:,$%{Cookie}i|:,$%{Host}i|:,$%{Referer}i|:,$%{User-Agent}i|:,$%{X-Forwarded-For}i|:,$%a|:,$%r|:,$%{ms}T|:,$%s|:,$%t|:,$%D|:,$%{X-Requested-With}i|:,$%{Authorization}i|:,$%{remote}p|:,$%{sec}t.%{msec_frac}t|:,$-|:,$-|'
```

F5 BIG-IP

Укажите следующую строку при настройке логирования согласно руководству **Configuring Request Logging**.

```
'3xXXXXXX|:,$RESPONSE_SIZE|:,$Accept|:,$%{Accept-Encoding}|:,$%{Accept-Language}|:,$Cookie|:,$Host|:,$Referer|:,$%{User-Agent}|:,$%{X-Forwarded-For}|:,$CLIENT_IP|:,$CLIENT_PORT|:,$HTTP_REQUEST|:,$RESPONSE_MSECS|:,$HTTP_STATCODE|:,$DATE_YYYY/$DATE_MM/$DATE_DD_$TIME_HH24:$TIME_MM:$TIME_SS|:,$HTTP_KEEPALIVE|:,$SERVER_IP|:,$SERVER_PORT|:,$BIGIP_CACHED|:,$%{X-Requested-With}|:,$%{Authorization}|:,$CLIENT_PORT|:,$TIME_MSECS|:,$-|:,$-|'
```

HAProxy

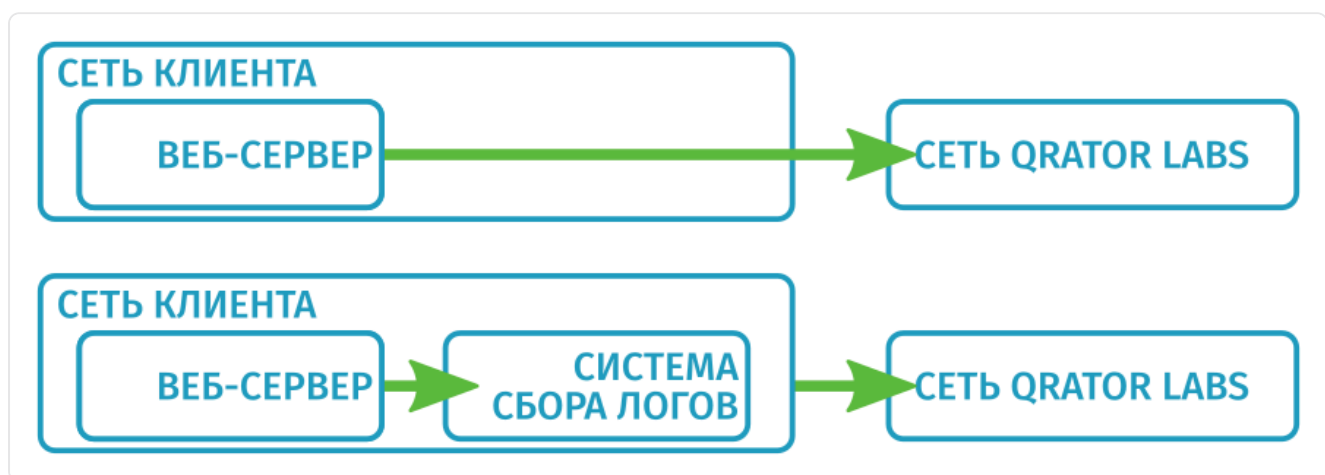
Вставьте следующий фрагмент в конфигурационный файл HAProxy.

```
capture request header Accept len 4096
capture request header Accept-Encoding len 4096
capture request header Accept-Language len 4096
capture request header Cookie len 16384
capture request header Host len 4096
capture request header Referer len 4096
capture request header User-Agent len 4096
capture request header X-Forwarded-For len 4096
capture request header X-Requested-With len 4096
capture request header Authorization len 4096
log-format "4xXXXXXX|:,$%B|:,$%[capture.req.hdr(0)]|:,$%[capture.req.hdr(1)]|:,$%[capture.req.hdr(2)]|:,$%[capture.req.hdr(3)]|:,$%[capture.req.hdr(4)]|:,$%[capture.req.hdr(5)]|:,$%[capture.req.hdr(6)]|:,$%[capture.req.hdr(7)]|:,$%ci|:,$%r|:,$%Ta|:,$%ST|:,$%Tl|:,$%Tr|:,$%[capture.req.hdr(8)]|:,$%[capture.req.hdr(9)]|:,$%cp|:,$%Ts.%ms|:,$-|:,$-|"
```

3. Настройте сбор и отправку логов

В зависимости от используемого веб-сервера, вам могут быть доступны разные способы отправки логов в сеть Curator. Наиболее простым способом является [отправка логов напрямую](#) из веб-сервера, если он поддерживает такую конфигурацию. Более универсальным решением является [использование системы сбора логов](#) для любого веб-сервера.

Обратите внимание, что приёмник логов на стороне Curator принимает логи по протоколу syslog поверх транспортного протокола TCP. Некоторые веб-серверы поддерживают протокол syslog только поверх UDP или через Unix-сокеты. В таком случае рекомендуется собирать их с помощью систему сбора логов, которая будет перенаправлять логи в сеть Curator.



Отправка логов напрямую

Если веб-сервер, обрабатывающий запросы пользователей, способен отправлять логи в сеть Curator по протоколу syslog самостоятельно, то вам достаточно произвести соответствующие настройки этого веб-сервера. Например, инструкцию по отправке логов напрямую из F5 BIG-IP можно найти [здесь](#): [Configuring the BIG-IP system to log to a remote syslog server](#).

Чтобы использовать для отправки логов защищённый протокол TLS, даже если сам веб-сервер не поддерживает этот протокол, можно воспользоваться дополнительной программой stunnel, как описано в этой инструкции: [SSL Encrypting Syslog with Stunnel](#).

Использование систем сбора логов

Система сбора логов — это программное обеспечение, которое может выполнять роль промежуточного узла между вашим веб-сервером и приёмником логов Curator. Примерами таких систем для Unix-подобных операционных систем являются [rsyslog](#) и [syslog-ng](#), для Windows — [Snare](#). При выборе системы сбора логов обратите внимание, что сеть Curator принимает логи по протоколу syslog поверх транспортного протокола TCP, а не UDP.

**ПРИМЕЧАНИЕ**

Популярные системы сбора логов также поддерживают шифрование отправляемых логов с использованием протокола TLS, например:

- [Документация по использованию TLS для syslog-ng](#)
- [Документация по использованию TLS для rsyslog](#)

Взаимодействие между веб-сервером и системой сбора логов может быть настроено разными способами, включая чтение логов из текстового файла, через Unix-сокеты или по протоколам TCP или UDP. Выбор способа зависит от того, находятся ли веб-сервер и система сбора логов на одном сервере или на разных серверах.

Также обычно требуется выполнить настройку самого веб-сервера, чтобы отправлять логи в нужный файл, сокет или на нужный адрес. Подробнее читайте в документации используемого веб-сервера, например:

- [Документация по записи в syslog для NGINX](#)
- [Документация по записи в syslog для lighttpd](#)

**ВАЖНО**

При использовании системы сбора логов rsyslog необходимо дополнительно сконфигурировать очереди записей, а также правила их игнорирования (discard). Подробнее можно прочитать по ссылке: [Action Queue cfg discarding local messages](#).

Примеры конфигурации rsyslog

Ниже приведены примеры конфигурационных файлов rsyslog для HAProxy и NGINX. Нужный конфигурационный файл следует поместить в директорию `/etc/rsyslog.d/`, после чего следует перезапустить rsyslog. Для использования транспортного протокола TLS требуется также подставить в конфигурационный файл путь к [сертификату Curator](#).

HAProxy без TLS

```

$AddUnixListenSocket /var/lib/haproxy/dev/log
if ($programname startswith 'haproxy') then {
    if ($msg contains '4xxxxxxx') then {
        $template codename-fwd, "<%PRI%>1 %timegenerated:::date-rfc3339% codename
%syslogtag:1:32% - - %msg:::drop-last-1f%\n"
        action(type="omfwd"
            Target="<IP-адрес приёмника логов>"
            Port="<порт приёмника логов>"
            protocol="tcp"
            queue.filename="codename-fwd-q1"
            queue.discardSeverity="4"
            queue.discardMark="25000"
            queue.size="30000"
            queue.highWatermark="10000"
            queue.lowWatermark="0"
            queue.timeoutEnqueue="500"
            queue.maxDiskSpace="20m"
            queue.timeoutWorkerthreadShutdown="-1"
            queue.saveOnShutdown="on"
            queue.type="LinkedList"
            Action.ResumeRetryCount="-1"
            template="codename-fwd"
        )
    }
}

```

HAProxy с TLS

```
$AddUnixListenSocket /var/lib/haproxy/dev/log
global(
    DefaultNetstreamDriverCAFile="<путь к файлу сертификата приёмника>"
)
if ($programname startswith 'haproxy') then {
    if ($msg contains '4xAAAAAA') then {
        $template codename-fwd,"<%PRI%>1 %timegenerated:::date-rfc3339% codename
%syslogtag:1:32% - - %msg:::drop-last-1f%\n"
        action(type="omfwd"
            Target="<IP-адрес приёмника логов>"
            Port="<порт приёмника логов>"
            protocol="tcp"
            queue.filename="codename-fwd-q1"
            queue.discardSeverity="4"
            queue.discardMark="25000"
            queue.size="30000"
            queue.highWatermark="10000"
            queue.lowWatermark="0"
            queue.timeoutEnqueue="500"
            queue.maxDiskSpace="20m"
            queue.timeoutWorkerthreadShutdown="-1"
            queue.saveOnShutdown="on"
            queue.type="LinkedList"
            Action.ResumeRetryCount="-1"
            template="codename-fwd"
        )
    }
}
```

NGINX без TLS

```
input(type="imuxsock"
      Socket="/var/log/nginx/nginx.sock")

template(name="codename-fwd" type="string"
         string="<%PRI%>1 %timegenerated:::date-rfc3339% codename %syslogtag:1:32% - -
%msg:::drop-last-lf%\n"
)
if ($programname startswith 'nginx') then {
  if ($msg contains '2FFFFFFF') then {
    action(type="omfwd"
          Target="<IP-адрес приёмника логов>"
          Port="<порт приёмника логов>"
          protocol="tcp"
          StreamDriver="gtls"
          StreamDriverMode="1"
          StreamDriverAuthMode="anon"
          queue.filename="codename-fwd-q1"
          queue.discardSeverity="4"
          queue.discardMark="30000"
          queue.size="30000"
          queue.highWatermark="10000"
          queue.lowWatermark="0"
          queue.timeoutEnqueue="500"
          queue.maxDiskSpace="20m"
          queue.timeoutWorkerthreadShutdown="-1"
          queue.saveOnShutdown="on"
          queue.type="LinkedList"
          Action.ResumeRetryCount="-1"
          template="codename-fwd"
    )
    & stop
  }
}
```

NGINX с TLS

```

input(type="imuxsock"
      Socket="/var/log/nginx/nginx.sock")

template(name="codename-fwd" type="string"
         string="<%PRI%>1 %timegenerated:::date-rfc3339% codename %syslogtag:1:32% - -
%msg:::drop-last-lf%\n"
         )
global(
  DefaultNetstreamDriverCAFile="<путь к файлу сертификата приёмника>"
)
if ($programname startswith 'nginx') then {
  if ($msg contains '2FFFFFFF') then {
    action(type="omfwd"
          Target="<IP-адрес приёмника логов>"
          Port="<порт приёмника логов>"
          protocol="tcp"
          StreamDriver="gtls"
          StreamDriverMode="1"
          StreamDriverAuthMode="anon"
          queue.filename="codename-fwd-q1"
          queue.discardSeverity="4"
          queue.discardMark="30000"
          queue.size="30000"
          queue.highWatermark="10000"
          queue.lowWatermark="0"
          queue.timeoutEnqueue="500"
          queue.maxDiskSpace="20m"
          queue.timeoutWorkerthreadShutdown="-1"
          queue.saveOnShutdown="on"
          queue.type="LinkedList"
          Action.ResumeRetryCount="-1"
          template="codename-fwd"
        )
    & stop
  }
}

```

Сертификаты Curator

Чтобы отправлять данные по транспортному протоколу TLS, необходимо использовать сертификат приёмника логов Curator.

Разные приёмники на стороне Curator используют разные сертификаты. Чтобы узнать, на какой именно приёмник вам нужно передавать логи, свяжитесь со специалистами технической поддержки Curator. Также вы можете проверять подлинность CA (certificate authority), которым подписаны данные сертификаты.

Сохраните нужный сертификат в файл, например, `/etc/rsyslog.d/codename-syslog-ca.crt`, и укажите этот в путь в конфигурации системы сбора логов. Файлы конфигурации для rsyslog вы можете найти в разделе [Примеры конфигурации rsyslog](#).

✓ Сертификат для 178.248.239.29

```
-----BEGIN CERTIFICATE-----
MIIFoDCCA4igAwIBAgIU5m2ENhIrqiVbcdGikZvsaic1ChcwDQYJKoZIhvcNAQEL
BQAwUTEZMBcGA1UEAwQUXJhdG9yIFN5c2xvZyBDQTEUMBGA1UECgwLUXJhdG9y
IEExhYnMxHjAcBgkqhkiG9w0BCQEWZD21haWwAcXJhdG9yLm5ldDAeFw0yNjA3MDgy
MDQzNDJhFw0zMTA3MDcyMDQzNDJhME8xFDASBgNVBAoMCFYXRvcjBMWjZMRcw
FQYDVQQDDA4xNzguMjQ4LjIzOS4yOTEmBwGCSqGSIb3DQEJARYPbWpEbXcmF0
b3IubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAusYLR0DkJPkf
OhZzaLupR+y01L5SxDka8tW89Mf8mYkpmLPVd42B/8Zw4aqR+YYmsvob8sJYlhv6
zPl1dRocPZ3qXkbvVRj+IrWwZKRvVIiN7RS/Ducw+PcDxWA+3Gq7YF02z8nxcn2
YqfIUCsitjQAFxx/UNpCvk3w1gQUSsDh2rPvZZNy1DlmpKy0ArKA8r3qaLqY55vk
qq37cHDSf+ycZxQ4cj8Yxj+yltX7IX7n0cE/s2esb/fzeqB0fVxugZe3Cqumkq+
oI3m0NJsT/F35hu4eFlqK/YRvmwsFqgFBozZ2FuyxStWocYdKyYYIe30X1NQSS2y
1f1FRPwae6MAydn0tHmBRCWdrFK38y7AdmztCFN68qF9iKG5Wh0k3sAg39Korlt/
86Ki3Eeggm14IkKPxi7b0W+fCVIJCN7y2eMMU1ZVDabJk1Bq0nwZ1f+UEmYXBJ7L
Ys5rr71hpTcjYe2QfjZH6fTIRbMwLw5tLY31OR1iy9ybDZmirbQVfEXSdokDBZjm
W5UhrnWip00XFek74WffnbGa0mbDUL4iFvfzR1q00/YTB5LK3RzXZesl0kSk3InK
eXhCSTjeGLisxiSsGRLZqcJhA4tHywr0pOIZvMeZHoejsTgvvAxhaCSX0Nbwj88u
Qbrkl4FqzLJdtaAt3KhCtPfwaZi9QDMCAwEAAANyMHAwHQYDVIR00BBYEFPE0qob
GzPswrrg22lwhjsAtqiHMB8GA1UdIwQYMBaAFGyR/xVNshdETvLwhPdkBYlAEBAO
MAKGA1UdEwQCMAAwDgYDVDR0PAQH/BAQDAgXgMBMGA1UdJQQMMAoGCCsGAQUFBwMB
MA0GCSqGSIb3DQEBGwUAAICAQBSKcJW8WrHFFzQ5KFxiyDmxQGFUdGGsq3l4VLE
qIReEW2uLnFaCxbCzaW40IQ6VqBg5z0T4b1MxA+P7s3VVka6c13epUa6yt0Pl+U
N+0uIdmhpzchEUTNf8VCBHYWhZGJMra3Bpa7i2PnFAu1eC9kCa0vIvdxajcVn2EA
sSt/P+VBcS9zduY1+woeflwyT896EZ0/Td+WDqG6I81U1z5684tBZKXao9rffioV
WdKUFXd0f1ECilZdj5ADFY7Znu6o0gk3X59Lo43Yp37tfJiIniKSxc1N2LPghU8z
rkxUHa3MK/6nbk/anF6PwAIE2Rm5oCaoK5xNuQU87u903mEIKQS3Ps/x1Qdu+JJZ
/nD7lIM9QFABjpoFcBWR/209c4x275CL8L9yzLxsqJQKX+zpAguXrNUnIVPvTI5v
9YsuCrrcdwK90lgrRXFerF14jgAdKIDYk2p0cBHfPyN1m5GQKotp2JwHwCR+sN5G
5v1VVomK5Yde7HXyM7XKBBCdyTqjMcdJVQ0+QAx3mwTy23S4ckuwGk5NI5W30LE
/xZhpj0lMtRAoNogDIYu4z31+YNJe1M0Xu5A/f/Tt2MIhVlaPiOVb43vaEu4mFaT
vm12e9/qPuX3CyBbwLGJBy3DmP5iaCxuBCnNKmawce0sRuFmGgotFlwy2uzP3nKr
G0+f3g==
-----END CERTIFICATE-----
```

✓ Сертификат для 178.248.239.30

-----BEGIN CERTIFICATE-----

```
MIIFoDCCA4igAwIBAgIUH3a0xgrPp8ReTBS0xgwMiDo+RzYwDQYJKoZIhvcNAQEL
BQAwUTEZMBcGA1UEAwQUXJhdG9yIFN5c2xvZyBDQTEUMBIGA1UECgwLUXJhdG9y
IEExhYnMxHjAcBgkqhkiG9w0BCQEWDD21haWwAcXJhdG9yLm5ldAeFw0yNjA3MDgy
MDQzNDRAfW0zMTA3MDcyMDQzNDRAfW0zMTA3MDcyMDQzNDRAfW0zMTA3MDcyMDQz
FQYDVQDDA4xNzguMjQ4LjIzOS4zMDEeMBwGCsqGSIb3DQEQJARYPbWFPbEBxcMF0
b3IubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAusYLR0DkJPkf
OhZzaLupR+y01L5SxDka8tW89Mf8mYkpmLPVd42B/8Zw4aqR+YYmsvob8sJYlhv6
zPl1dRocPZ3qXkbvVRj+IrWwZKRvViIN7RS/Ducw+PcDxWA+3Gq7YF02z8nxcn2
YqfIUcsitjQAFxx/UNpCvk3w1gQUSsDh2rPvZZNy1DlmpKy0ArKA8r3qaLqY55vk
qq37cHDSf+ycZxQ4cj8Yxj+yltX7IX7n0cE/s2esb/fzeqB0fVxugZe3Cqumkq+
oI3m0NJsT/F35hu4eFlqK/yRvmwsFqgFBozZ2FuyxStWocYdKyYYIe30X1NQSS2y
1f1FRPwae6MAydn0tHmBRCWdrFK38y7AdmztcFN68qF9iKG5WhOk3sAg39Korlt/
86Ki3Eegml4IkKPx17b0W+fCVIJCn7y2eMMULZVDabJk1Bq0nwZ1f+UEmYXBJ7L
Ys5rr71hpTcjYe2QFjZH6FtIRbMwLW5tLY310R1iy9ybDZmirbQVfEXSdokDBZjm
W5UhrnWip00XFek74WffnbGa0mbDUL4iFvfzR1q00/YTB5LK3RzXZesl0kSk3InK
eXhCSTjeGLisxiSSGRlZqcJhA4tHywr0poIZvMeZHoejsTgvvAxhaCSX0NbWj88u
Qbrkl4FqzLJdtaAt3KhCtPfwazi9QDMCAwEAAANyMHAwHQYDVIR00BBYEFpWE0qob
GzPswrrg22lwhjsAtqiHMB8GA1UdIwQYMBaAFGyR/xVNsHdETvLwhPDkBYIAEBAO
MAKGA1UdEwQCMAAwDgYDVROPAQH/BAQDAgXgMBMGA1UdJQQMMAoGCCsGAQUFBwMB
MA0GCSqGSIb3DQEBwUAAICAQBpf//Kfr6Ya1sNV0aQWB9a3M0lqZ2hmpf0SPi3
AddwWpmXLa50DRpDR6TeV88TPyhyj9AWaA7KXZCdK1a798o4FNYwZRieNN4Q0ugk
gUekvTy9fSjKgAhMSeX0LgVMi5DaKC71mdGDAD1SfBp2irC6ZT6tP0mQHCJ/iqJg
HMD1KG2+mtwWnhAHLGYLm/yUUhdzToDDUjS2kwVJuFB9uIFP1xZiQz6mZUdrI4ZA
ao2Umdm8u5NJ4Xfy52JrcsPsAK4nptpys8YmoQd2FBfYLS8kkz1S9tziCDejB/3d
CeBAK6RPpzHeVG3c7l3yUAgmLpgmn5diXw6Fyxq7pbTqknI3d6h0TrnAYJGgdfvb
l8N8TBoGjr7Uw4yFbefp4pEcyFD+UalakRoSk4Eb0c6DhsYpGRSST/4wbabbdudo
PbeMMS0vtihpahz7lWKpGZ0VdDdXUCi/voSQL2mg//R90AS3kCKFYAlV01yaxL6
vv9Cc7uT2Hbv7zMWhdJZS0M3fsUh9/Vd4ygy+D3NoUsmptpsQJy/ffFgaLZWw6e
Gu8C17PfYn6vFD9vP90YYKY8LoghbeMQpXPUx0BGYzzQoLBtusIUVUblRcQDfYvC
QnL8tT739AFEE5oRtjGzaETpKJEQt0xltI3LFh1wvm1CMQo//s0Gx2lXDFBt1gXS
XivWYw==
```

-----END CERTIFICATE-----

✓ Сертификат для 185.94.108.254

-----BEGIN CERTIFICATE-----

```
MIIFoDCCA4igAwIBAgIUcPorCucj1+yBchknNH0qa76Ax5EwDQYJKoZIhvcNAQEL
BQAwUTEZMBcGA1UEAwQUXJhdG9yIFN5c2xvZyBDQTEUMBIGA1UECgwLUXJhdG9y
IEExhYnMxHjAcBgkqhkiG9w0BCQEWOD21haWxAcXJhdG9yLm5ldAeFw0yNjA3MDgy
MDQzNDVaFw0zMTA3MDcyMDQzNDVaME8xFDASBgNVBAoMC1FyYXRvcjBMWjZMRcw
FQYDVQDDA4xODUuOTQuMTA4LjI1NDEeMBwGCsqGSIb3DQEJARYPbWpEYXcmF0
b3IubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAusYLR0DkJPkf
OhZzaLupR+y01L5SxDka8tW89Mf8mYkpmLPVd42B/8Zw4aqR+YYmsvob8sJYlhv6
zPl1dRocPZ3qXkbvVRj+IrWwZKRvViN7RS/Ducw+PcDxWA+3Gq7YF02z8nxcn2
YqfIUcsitjQAFxx/UNpCvk3w1gQUSsDh2rPvZZNy1DlmpKy0ArKA8r3qaLqY55vk
qq37cHDSf+ycZxQ4cj8Yxj+yltX7XIx7n0cE/s2esb/fzeqB0fVxugZe3Cqumkq+
oI3m0NJsT/F35hu4eFlqK/yRvmwsFqgFBozZ2FuyxStWocYdKyYYIe30X1NQSS2y
1f1FRPwae6MAydn0tHmBRCWdrFK38y7AdmztcFN68qF9iKG5WhOk3sAg39Korlt/
86Ki3Eegml4IkKPx17b0w+fCVIJCn7y2eMMULZVDabJk1Bq0nwZ1f+UEmYXBJ7L
Ys5rr71hpTcjYe2QFjZH6FtIRbMwLw5tLY310R1iy9ybdZmirbQVfEXSdokDBZjm
W5UhrnWip00XFek74WffnbGa0mbDUL4iFvfzR1q00/YTB5LK3RzXZesl0kSk3InK
eXhCSTjeGLisxiSSGRlZqcJhA4tHywr0poIZvMeZHoejsTgvvAxhaCSX0NbWj88u
Qbrkl4FqzLJdtaAt3KhCtPfwazi9QDMCAwEAAANyMHAwHQYDVR00BBYEFpWE0qob
GzPswrrg22lwhjsAtqiHMB8GA1UdIwQYMBaAFGyR/xVNshdETvLwhPDkBYlAEBAo
MAKGA1UdEwQCMAAwDgYDVR0PAQH/BAQDAgXgMBMGA1UdJQQMMAoGCCsGAQUFBwMB
MA0GCSqGSIb3DQEBwUAA4ICAQB9LYRBwR2uLybwHEiHJ5vNPAv65ZUxZKIaqN5T
VYSfr3R3zpZRzcUYLSicCe6YoTZqavaIAxsmqxDEsK/C9JLOTdw3WdLhbOCxiqzT
7rmx/X300GuM9BdGmg1vti9s7J67Mj+U9q+t9qrQnPmDPQYom9sWnTZ7ft6lwiGy
+QXJAW+I9XrxScU0K0BemdCYTCFHPBEJanYTtBbA+0jtCRw8WZ0cRtmJYiuni1IT
dk/mAHvKppGr0d8vxsXT98TpWqLyyYpdQC7eprIwfbsl+cix6LzN7kw5BoMNd+N
2Y5J9EJNSnDSh1FTkuU2tg4Kzem+15rZzAUBOrY+8pQDjlepMqY9e6IC9kthKmf4
Okm5pFX40LkqK2nTLpqF4H9Ias6Io16R0pJ8Gd437MnnE3X+ZqNpnu9fCiajUwjF
4hBCPHBVLHK0fC81s1vZkzggcXq0zY4SVMoFaEbcjRt1UrdRLBik9PldpvJLxAdQ
/LlGEjF9E0Tr6Rrb5qGovKmQGnyujrTMoWeV7AegODFvXv00SZk3oukmJnLn4BF4E
Kbbqa5tmwJlB+FtUGdRadH8Jk8ur1CwF3TL62uAjbwfdq7yU6dp6g/Vl7tEq7d1C
So1MjcfWnUkFu9f8pcgD6SKNxNRRwlnyQUNfKoat/n4MwnYuN2hJT+jcj4ILf6M
EgK5VA==
```

-----END CERTIFICATE-----

✓ Сертификат для 100.64.1.254

-----BEGIN CERTIFICATE-----

MIIFnjCCA4agAwIBAgIUeJgBKIAHq2QIM+1t40i+dtltjSwWDQYJKoZIhvcNAQEL
BQAwUTEZMBcGA1UEAwQUXJhdG9yIFN5c2xvZyBDQTEUMBGA1UECgwLUXJhdG9y
IEExhYnMxHjAcBgkqhkiG9w0BCQEWOD21haWwAcXJhdG9yLm5ldAeFw0yNjA3MDgy
MDQzMzZaFw0zMTA3MDcyMDQzMzZaME0xFDASBgNVBAoMC1FyYXRvcjBMWjZMRUw
EwYDVQQDDAwwMDAuNjQuMS4yNTQxHjAcBgkqhkiG9w0BCQEWOD21haWwAcXJhdG9y
Lm5ldDCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAggIBALrGC6zg5CT5HzoW
c2i7qUfsjtS+UsQ5GvLVvPTH/JmJKZiz1XeNgf/GcOGqkfmgJrL6G/LCWJYb+sz5
dXUAHD2d615G71UY/iK1lsykb1SIje0Uvw7nMPj3A8VgPtXqu2BTts/J8XLZ9mKn
yFarIrY0ABccf1DaQr5N8NYEFerA4dqz72WTctQ5ZqSsjgK5APK96mi6m0eb5Kqt
+3Bw7H/snGcu0HI/GMY/spbV+1yMe5znBP7NnrG/383qgdH1cboGxtwqrpKvqCN
5tDSbE/xd+YbuHhZaiv8kb5sLBaoBQAM2dhbssUrVqHGHSsmGCHtz19TUEktstX9
RUT8GnujAMnZ6LR5gUQlnaxSt/MuWHZs7XBTEvKhfYihuVoTpN7AIN/SqK5bf/Oi
otxHoIjpeCJCj8Yu2z1vnw1SCQje8tnjDFJwVQ2myZNQatJ8GdX/1BJmFwSey2LO
a6+9YaU3I2HtkBY2R+hbSEWzMJVubS2N9TkdYsvcmw2Z0q20FXxFOaJAwWY5luV
Ia51oqtTfXxp0+F352xmjpwmw1C+Ihb380dajjv2EweSyt0c12XrJdJEpNyJyn14
XEK43hi4rMYkrBkZWanCYQLR8sK9KaCgbzHmR6Ho7E4L7wMYWgk19DW1o/PLK66
5JeBasyyXbwGLdyoQrT38GmYvUAzAgMBAAGjcjBwMB0GA1UdDgQWBbT1hNKqGxsZ
7Fq64NtpcIY7ALaohzAFBgNVHSMEGDAWgBRskf8VTbB3RE7y8ITw5AWJQBAQKDAJ
BgNVHRMEAjAAMA4GA1UdDwEB/wQEAwIF4DATBgNVHSUEDDAKBggrBgEFBQcDATAN
BgkqhkiG9w0BAQsFAAOCAGeAk77DkGwJld0cCF2KJysst2ycm0s4Et0cunM4D96s
pMkbBV5s13shGM6Hq+RQy9rknrQuM4RoP2/ZctIc+Eny8YwMyHkcp7Uog43wDlEO
niYUde9HMgT6XjsgKKmFw2p8si60zIOKQktbMZUn40RBBLwStPwVam/X4IZeKfT0
J5I/0ka6V2bIJGeUxL7PjxtAoTuH+vvsh7EE9ZdNNNTy43B1C4czCoEir55v+S98
GJpUnKV557aQ3GjXiqpZJmM+Z8RmmamLgNhtSrplHf6sNKLMITgPZCZP9gEjjcqq
cHpGXFnpPC21aUdj6ArD8KpRqGGAPWN5adZpkDWV43o3GxY63vrBZUbvLKyt75Q
CN0MIS6cEihouww0U9Q3qab+BrEdsr6oUBplazfMWRZwz6vBuKzh5ncWDvb1NpJ
rIHwGkN9yR2Z2JWHZS5Xh1y9uKBbXtdy0BFECyck/CwmyhwSkeKnnFYGuwIiH/t
pw9qBwbVUQXX1NPAKYndT6k9Js98h+QY0J3JvwqzsIZQGyHM860mG6CXLBqZSGyo
TDhNhCSvcvU11rKFwx7/+aqKVIloqR0Rk3MzHDVQJ6ZloqogLYcSBT7WH2hNnfu8
XLBbS6htklXPcDiACuZe53sStwWkOxZQf0iMJgUk8R8dPZNkoUuvLgnlj2UN9m5Q
sbM=

-----END CERTIFICATE-----

✓ Сертификат для СА

-----BEGIN CERTIFICATE-----

```

MIENDCCA52gAwIBAgICBHYwDQYJKoZIhvcNAQELBQAwwYQxCzAJBgNVBAYTA1JVMQ8wDQYDVQQQIEwZbn3Njb3cxZDZANBgNVBACTBk1vc2NvdzEMMAoGA1UEChMDSExMMQ8wDQYDVQQLEwZRCmF0b3IxFDASBgNVBAMTC1FyYXRvcjB0b2RlMR4wHAYJKoZIhvcNAQkBFg9tYWlsQHfYyXRvcj5uZXQwHhcNMjEwNzEyMTUyMjM5WmcNMzEwNzEwMTUyMjM5WjBRMRkwFwYDVQQDDDBBRcmF0b3Igu3lzbG9nIENBMRQwEgYDVQQKDATRcmF0b3IguTGFIczEeMBwGCSqGSIb3DQEJARYPbWpEbXcmF0b3IubmV0MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAmQmcErDsVsHgZ3+C+Q1EEVlMN2HgbnBB1Vwu5d0Cp9Em2T5+L2XrvGb6fd1XEEgDi4qi0d6DtCP015NaUCr4su7RVpxw/flzuHcq7DyS0kyjEA0dkaZ3L20n1Lx5j jmnC8i+5vdaDhC94NfwdQdkHnTT047Pkb80RkaJTVACZAIa8ab86L02PmL54Y0iTSX+/IUo05SILElZewVJ8fkjnOwmGPiPX0dkP9YAV/6qfoQfa9PVUkPeV9UHNUpw2laN09hAog4UybeIzTV0bwweiCnlj5TW16zn0JcftViiNn9HUw3EWmbi8YUhv86yTiLjMXHDafhFzQqTDKkg5J4dn7ye0AqzqXUo090jrBC4+fX5RgImJoXMeFS2exSB5f8PxDPBS95LQVuSZzXesuDUzQVJD9T0JT57u/27EB1TwQqMLgqo39RE8iaroduibUjFKAzBn3xXA0Mx5EbPK0aliymq82PDBwB69JDM/i0xSeRia5r7C/mAjVfcdQxQVz97IfJXek0FChUjHkddgWpHuYqYQreq5sZX218te+86yh5RjRmgN52gb9c4KppJEE04fAXJYhMARuMhuswyCzWLPP8SHIO/QeHD4ifw+FyT8jh/qiFhcIcY48wC2/4IOsfP50WTUfzfjuZF+g6SSGXhDdKidAWUZ2mBa/UsZZsMvsECAwEAAANjMGEWHQYDVR00BBYEFgyR/xVNsHdETvLwhPDkBY1AEBAoMB8GA1UdIwQYMBaAFAbuy5jX1iZn8znnG0wGytbFKt/XMA8GA1UdEwEB/wQFMAMBAf8wDgYDVR0PAAQH/BAQDAgGGMA0GCSqGSIb3DQEBCwUAA4GBAI5bpB870oTPMLGE4ZsTSa2LmjYPLz9i0Z0ubzUAZwz7B81RxSdFDz90Y2QNmU0x7Pztzz13IW5XsmtRqOf3Q7jRUWSzBi/JFTEqWALVcGrFixZA9QOPJ/n0o1FC8hlxmwxA6yoXRnW3ntngAJiziHrrtNKKjILT0Jv4zbk25Jtm

```

-----END CERTIFICATE-----

Подключение: BGP

Если ваша организация располагает собственной автономной системой (Autonomous System, AS), вы можете подключиться к сети Curator по протоколу BGP и анонсировать свои префиксы. Таким образом, автономная система Curator будет выступать как транзитная AS, через которую будет проходить весь связанный с анонсированными префиксами трафик.

Сеть Curator подключена к нескольким провайдерам Tier 1 и анонсирует ваши префиксы каждому из них. Каждый провайдер будет выбирать маршрут, проходящий через ближайший к нему роутер Curator, благодаря чему трафик из любой части мира будет приходить к вам с минимумом дополнительных задержек. При этом трафик, который Curator распознает как атаку, не будет отправляться в вашу сеть.

Для подключения к Curator по протоколу BGP:

1. Добавьте префиксы.
2. Настройте канал до Curator.
3. Настройте BGP-пиринг с Curator.
4. Опишите карту сервисов.
5. Анонсируйте префиксы.

Добавление префиксов

Заранее укажите в разделе «Префиксы» личного кабинета каждый префикс, который вы собираетесь анонсировать, и соответствующий номер вашей AS, которая будет источником (origin) для этого префикса. Префикс должен принадлежать этой AS согласно базе данных интернет-регистратора.

Для подтверждения операции добавления префикса Curator направит письмо со ссылкой на адрес, указанный как `tech-c` для соответствующей AS.

Настройка канала до Curator

Для BGP-сессии необходим канал связи типа «точка-точка» между вашей сетью и сетью Curator. Чаще всего для этого удобно использовать виртуальные туннели, такие как GRE, IPsec или MPLS L2 VPN. В отдельных случаях доступны другие способы, например, выделенные каналы связи или физическая коммутация в рамках одного дата-центра.

BGP-пиринг организуется поверх такого канала. Таким образом, выбранные префиксы из вашей AS будут анонсированы только в сеть Curator.

Это важно, поскольку нужно обеспечить прохождение через Curator всего входящего трафика, связанного с анонсированными префиксами. Обратите внимание, что если вы будете анонсировать

префиксы провайдерам напрямую, то атакующий сможет направить DDoS-атаку через другой маршрут в обход сети Curator.

Даже если провайдер анонсирует маршрут до суперсети (less specific route), а Curator — маршрут до подсети (more specific route), риск случайного или целенаправленного прохода трафика в подсеть через провайдера в обход сети Curator сохраняется.

Для обеспечения отказоустойчивости и надежности рекомендуется создать два или более канала до Curator. Например, это могут быть два разных GRE-туннеля через разных провайдеров. Со своей стороны Curator также уделяет большое внимание резервированию, поэтому даже в случае, если отключится или выйдет из строя часть оборудования, AS в целом останется доступной и сможет обеспечивать доступность и защиту вашего сайта по другому каналу.

Настройка BGP-пиринга с Curator

После создания канала типа «точка-точка» между вашей сетью и сетью Curator настройте ваше оборудование так, чтобы организовать BGP-сессию поверх этого канала.

Пошаговые инструкции, включая примеры конфигурации для популярных производителей оборудования, вы можете получить у службы поддержки Curator.

Описание карты сервисов

При анализе трафика, проходящего по BGP, центры очистки трафика ориентируются на сведения, предоставленные клиентом в разделах «IP-адреса» и «Порты и протоколы» личного кабинета. Эти сведения вместе называются *картой сервисов* и описывают направления и объём легитимного трафика, ожидаемого клиентом.

Для начала описания трафика создайте один или несколько сервисов в разделе «Сервисы». Затем для каждого сервиса задайте список IP-адресов (раздел «IP-адреса»), портов и протоколов (раздел «Порты и протоколы»). Весь входящий и исходящий трафик, не соответствующий описанному в карте сервисов, будет отбрасываться.

Анонс префиксов

Непосредственное начало анонса ваших префиксов происходит в рамках протокола BGP и не требует действий в личном кабинете. Сеть Curator начнёт анонсировать ваши префиксы, как только ваше оборудование начнёт анонсировать их в автономную систему Curator. Если вы приостановите анонс какого-либо префикса, то Curator сразу приостановит его анонс, а также перестанет пропускать трафик к этому префиксу.

Обратите внимание, что Curator при анонсе префиксов не обрабатывает атрибут BGP `community`.

2.11 ПОДКЛЮЧЕНИЕ К CURATOR

Подключение: Защищённый DNS-сервер

Данная статья описывает порядок подключения услуги [Защищённый DNS-сервер](#).

Услуга подключается в три шага:

1. Настройте взаимодействие между вашим DNS-сервером и DNS-сервером Curator.
2. Убедитесь, что DNS-сервер Curator отвечает на запросы о вашей зоне.
3. Укажите DNS-сервер Curator в качестве авторитарного для вашей зоны.

**СОВЕТ**

Прежде чем приступить к подключению, рекомендуется настроить для вашего DNS-сервера новый IP-адрес, ранее не использовавшийся и не публиковавшийся. При этом доступ к серверу по прежнему IP-адресу можно отключить на [шаге 3](#).

1. Настройка взаимодействия между DNS-серверами

Настройка взаимодействия в режиме вторичного DNS-сервера

Перед подключением услуги в [режиме вторичного DNS-сервера](#) убедитесь, что используемый вами DNS-сервер позволяет настраивать передачу зоны (zone transfer) на вторичные авторитативные DNS-серверы. Если вы используете DNS-сервер доменного регистратора или хостинга, убедитесь, что такая возможность есть в его панели управления (например: [инструкция для GoDaddy](#)).

В access control list (ACL) вашего DNS-сервера разрешите передачу зоны серверу `ns.curator.pro`. Это позволит DNS-серверу Curator выполнять роль вторичного DNS-сервера.

Сообщите специалистам технической поддержки Curator IP-адрес вашего первичного DNS-сервера. Специалисты выполнят соответствующую настройку вторичного DNS-сервера, после чего вторичный DNS-сервер сделает запрос на передачу зоны от первичного DNS-сервера.

Настройка взаимодействия в режиме проксирующего DNS-сервера

Чтобы подключить услугу в [режиме проксирующего DNS-сервера](#), сообщите специалистам технической поддержки Curator IP-адрес вашего DNS-сервера, а также перечень доменов, информацию о которых необходимо проксировать. Специалисты технической поддержки выполнят соответствующую настройку DNS-сервера Curator, после чего сервер сможет перенаправлять на ваш сервер запросы об указанных доменах.

2. Проверка конфигурации

Прежде чем переключиться на DNS-сервер Curator, проверьте новую конфигурацию. Для этого сделайте к этому серверу один или несколько запросов о ваших доменах. Если сервер не находит искомую запись или возвращает неверную информацию, сообщите об этом специалистам технической поддержки для выяснения причин проблемы.

Для проверки можно использовать утилиту `nslookup`, указывая DNS-сервер последним аргументом. Например, команда для получения IP-адреса домена www.example.com от DNS-сервера Curator будет выглядеть так:

```
nslookup www.example.com ns.curator.pro
```

3. Переключение на DNS-сервер Curator

В панели управления доменного регистратора укажите DNS-сервер Curator в качестве авторитативного сервера для вашей зоны, а ваш DNS-сервер удалите из списка.

В зависимости от настроек TTL на стороне доменного регистратора, обновление информации о NS-записях может занять до 72 часов.



СОВЕТ

Если вы использовали новый IP-адрес, отличный от указанного в NS-записях ранее, то после обновления записей рекомендуется запретить обращение к прежнему адресу в настройка файервола на вашей стороне. Таким образом, не зная новый IP-адрес, злоумышленник не сможет направить атаку на первичный сервер и тем самым затруднить своевременное обновление данных на DNS-сервере Curator. Такая техника сокрытия DNS-сервера известна как *hidden primary*.

03

Личный кабинет

Обзор интерфейса

Списки ресурсов

Curator

Bot protection

CDN

Утилиты

Хранилище сертификатов

Права доступа

Уведомления

Мой профиль

SSO

3.1 ЛИЧНЫЙ КАБИНЕТ

Обзор интерфейса личного кабинета

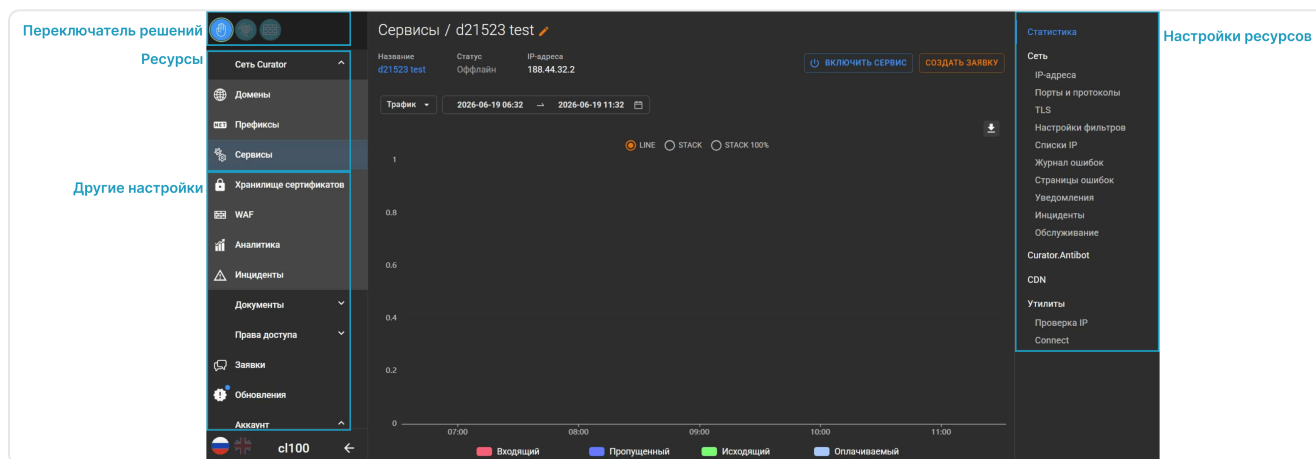
В личном кабинете Curator клиенты могут настраивать используемые услуги, а также отслеживать информацию об их работе.

На этой странице приведён полный список разделов личного кабинета, разделённый на несколько частей:

- Управление списком [ресурсов](#).
- Управление [настройками ресурсов](#).
- Управление [настройками Ingress](#).
- Управление [другими настройками](#).

[Ресурсы](#), [Настройки Ingress](#) и [Другие настройки](#) отображаются в *основном меню* личного кабинета, расположенном в левой части интерфейса. Список видимых элементов в основном меню варьируется в зависимости от режима, выбранного в *переключателе*: **Curator**, **Ingress**, **WAF** или **CDN**.

[Настройки ресурсов](#) отображаются в *дополнительном меню* личного кабинета, расположенном в правой части интерфейса. Это меню отображается только после выбора конкретного ресурса в разделе [Домены](#) или [Сервисы](#).



Доступность некоторых режимов и разделов личного кабинета может зависеть от того, какие услуги включены для клиента. При возникновении вопросов обратитесь в службу поддержки Curator.

Также некоторые разделы или отдельные настройки в них могут быть недоступны, если учётная запись пользователя не входит в группы с определёнными правами доступа. Подробнее см. в описании раздела [Группы](#).

Ресурсы

Ключевым понятием для настройки большинства услуг Curator является *ресурс*. Ресурсом может быть, например, веб-сайт или API-шлюз, доступ к которому необходимо защитить от атак. Для разных услуг Curator настраиваются разные виды ресурсов: *домены* или *сервисы*.

Для начала работы с какой-либо услугой добавьте новый ресурс в список, используя разделы, перечисленные в таблице ниже. После этого перейдите к [настройкам ресурса](#).

Раздел	Описание
Домены	Настройки <i>доменов</i> для работы таких услуг как обратный HTTP-прокси и интеграция с CDN . Для каждого домена независимо выполняется балансировка нагрузки между указанными апстримами.
Префиксы	Настройки подключения к Curator по протоколу BGP , которые необходимо выполнить перед добавлением сервисов в разделе Сервисы .
Сервисы	Настройка <i>карты сервисов</i> для работы по протоколу BGP . Каждый сервис описывает тип и объём легитимного трафика для определённых IP-адресов, что позволяет сети Curator отбрасывать трафик, использующие непредусмотренные сервисом порты и протоколы.



ПРИМЕЧАНИЕ

Не следует путать раздел [Префиксы](#), относящийся к настройке работы по протоколу BGP, с разделом [Ingress](#) → [Префиксы](#), относящимся к [настройкам Ingress](#).

Настройки ресурсов

Большинство разделов личного кабинета содержат настройки, применяемые к конкретному [ресурсу](#).

Чтобы перейти к настройкам ресурса, сначала зайдите в раздел [Домены](#) или [Сервисы](#) и выберите нужный ресурс в списке. После этого в дополнительном меню отобразится список разделов, относящихся к данному ресурсу.

Набор доступных разделов различается для доменов и сервисов.

Раздел	Описание	Для доменов	Для сервисов
Статистика	Статистика запросов, ошибок и применённых блокировок трафика.	✓	✓
Сервисы	Настройка апстримов и балансировки для обратного HTTP-прокси , обратного WebSocket-прокси и обратного TCP-прокси .	✓	
IP-адреса	IP-адреса, на которые сеть Curator перенаправляет очищенный трафик при работе по протоколу BGP .		✓

Порты и протоколы	Тип и объём легитимного трафика, который ожидается для IP-адресов сервиса.		✓
TLS	Настройки, в соответствии с которыми для домена или сервиса используется протокол HTTPS .	✓	✓
Списки IP	Чёрный и белый списки, учитываемые при определении легитимности трафика.	✓	✓
Туннели	Настройки, связанные с подключением к Curator через туннели .	✓	
Настройки фильтров	Настройка фильтрации запросов по HTTP-заголовкам, странам-источникам запросов и другим свойствам.	✓	✓
HTTP-перенаправления	Настройка HTTP-перенаправлений , работающих на стороне обратного HTTP-прокси.	✓	
Страницы ошибок	Настройка страниц, которые будут показаны пользователю при проблемах доступа к ресурсу.	✓	✓
Уведомления	Настройка уведомлений о превышении заданных порогов трафика.	✓	✓
Инциденты	Отчёты об обнаруженных атаках и прочих инцидентах.	✓	✓
Bot protection → Сводка, Bot protection → Локации, Bot protection → Посетители, Bot protection → Подписи	Статистика и настройки, связанные с защитой от ботов .	✓	✓
CDN, Curator.CDN → Настройки	Статистика и настройки, связанные с работой услуги Curator.CDN.	✓	
Утилиты	Вспомогательные утилиты для проверки состояния услуг.	✓	✓

Настройки Ingress

В перечисленных ниже разделах осуществляется настройка [услуги Ingress-фильтрации](#). Эта услуга предназначена для администраторов транзитных сетей, которым необходимо очистить входящий трафик до конечных сетей. Для настройки услуги определите список *префиксов* конечных сетей и список *политик*, применяемых к этим префиксам.

По умолчанию разделы личного кабинета, связанные с настройкой Ingress-фильтрации, скрыты. Чтобы увидеть их, воспользуйтесь переключателем над основным меню (см. [описание интерфейса](#)).

Раздел	Описание
Ingress	Этот раздел отображает как список префиксов из раздела Ingress → Префиксы , так и список политик из раздела Ingress → Политики . Также в этом разделе вы можете добавить новый префикс или новую политику.
Ingress → Префиксы	Список префиксов конечных сетей, транзитный трафик к которым необходимо защищать.
Ingress → Политики	Список политик фильтрации трафика, применяемых к трафику конкретных префиксов.

Другие настройки

Часть разделов личного кабинета не связана с управлением конкретными услугами.

Все перечисленные ниже разделы доступны через основное меню личного кабинета.

Раздел	Описание
Хранилище сертификатов	Управление TLS-сертификатами, которые могут использоваться для обратного HTTP-прокси и интеграции с CDN .
WAF	Настройка Web Application Firewall.
Аналитика	Отчёты о трафике.
Инциденты	Отчёты об обнаруженных атаках и прочих инцидентах.
Отчёты	Отчёты о трафике.
Финансы	Отчёты о финансах.
Компания	Управление банковскими реквизитами и другими данными, необходимыми для взаимодействия с Curator.
API токены	Управление токенами, с помощью которых возможна работа с Curator API.
Пользователи, Группы	Управление пользователями, имеющими доступ к вашему личному кабинету, и выдача прав доступа для групп пользователей.
Заявки	Взаимодействие со специалистами технической поддержки Curator.
Обновления	Информация об изменениях личного кабинета и услуг Curator.

Уведомления	Настройки получения уведомлений на электронную почту.
Мой профиль	Управление вашим профилем в личном кабинете.

**ПРИМЕЧАНИЕ**

Раздел [Инциденты](#) доступен как в основном меню, так и среди [настроек ресурсов](#) в дополнительном меню. В зависимости от того, через какое меню открыт раздел, в нём будут отображены либо данные обо всех инцидентах, либо данные об инцидентах по конкретному ресурсу.

Личный кабинет: Домены



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

Настройка многих услуг Curator предполагает работу с конкретным *доменом*. Вы можете [видеть список доменов](#), подключённых к вашему аккаунту, в разделе «Домены» личного кабинета. Здесь же вы можете [добавлять новые домены](#).

Для каждого добавленного домена в личном кабинете становятся доступны разделы со статистикой и настройками конкретных услуг, см. [Обзор интерфейса личного кабинета](#).

Посмотреть список доменов

Домены, доступные вашему аккаунту, отображаются в виде таблицы со следующими полями:

- **ID** — уникальный идентификатор домена в системе Curator (например, [d12345](#)), а также само доменное имя (например, [example.com](#)).

Нажмите на ID домена, чтобы перейти к его статистике и настройкам.

- **Curator IP** — IP-адрес в сети Curator, назначенный для использования с данным доменом. Отображается только для доменов, прошедших модерацию (см. [Добавить домен](#)).
- **Статус** — текущее состояние сервиса.
 - **Модерируется** — домен проверяется сотрудниками Curator перед включением в работу (см. [Добавить домен](#)).
 - **Онлайн** — домен обслуживается.
 - **Оффлайн** — домен отключён.
 - **Обновляется** — происходит применение изменённой конфигурации услуг.
 - **Ошибка** — произошла непредвиденная ошибка, домен может быть недоступен.
- **Апстримы** — перечень апстримов, между которыми распределяется трафик домена. Настраивается в разделе [Апстримы](#).
- **Трафик** — скорость трафика между пользователями и сетью Curator для данного домена. Каждое значение рассчитывается как средняя скорость в секунду на основе информации за последнюю минуту.

-  — входящий трафик.
-  — исходящий трафик.

Рядом с заголовками столбцов таблицы присутствуют поля фильтров, с помощью которых вы можете быстро найти домены, удовлетворяющие определённым условиям.

По умолчанию таблица отображает не более 20 доменов одновременно. Если для вашего аккаунта доступно больше доменов, то для перехода к другим частям списка используйте кнопки < и > под таблицей. Также вы можете выбрать количество доменов, отображаемых за один раз, с помощью поля **Строк на страницу**.

Добавить домен

1. Откройте раздел «Домены» и нажмите кнопку **Добавить домен**.
2. В появившемся диалоге введите название домена (например, `example.com`). Нажмите кнопку **Далее**.
3. Укажите апстримы, на которые будет перенаправляться трафик для домена. Это можно сделать двумя способами:

- **Ручной ввод IP-адресов**

Введите один или несколько IP-адресов в поле **Апстримы**.

- **Определение IP-адресов с помощью DNS**

Нажмите ссылку **DNS поиск**. В появившемся диалоге введите **Имя хоста**, по которому сейчас доступен необходимый апстрим, и нажмите кнопку **Найти**. В диалог автоматически загрузится список адресов из А-записи домена. При необходимости снимите галочки с адресов, которые не должны быть апстримами в новой конфигурации. После этого нажмите кнопку **Импортирование**.



ВАЖНО

При подключении домена не рекомендуется использовать апстримы, которые ранее были публично связаны с доменом, так как это может позволить злоумышленнику провести атаку в обход защиты Curator. Подробнее см. [Смена актуального IP-адреса](#).

4. Нажмите кнопку **Создать**.

Домен будет добавлен в общий список доменов, и ему будет назначен статус **Модерируется**. В течение нескольких часов специалисты Curator проверят заявку и назначат домену статус **Онлайн** либо свяжутся с вами для уточнения деталей.

После успешного подключения домену будет назначен Curator IP, который вы сможете использовать для настройки услуг — например, для [Подключения обратного HTTP-прокси](#).

Удалить домен

Чтобы удалить домен, обратитесь в техническую поддержку Curator.

Пример конфигурации

ID	Qrator IP	Статус	Апстримы	Трафик
×	×	Все ▼	×	
d123domain1.example.com	178.248.233.165	Онлайн	203.0.113.1 203.0.113.2 203.0.113.3	879.867 bps 122.133 bps
d234domain2.example.com	185.65.148.91	Онлайн	203.0.113.6 203.0.113.7	32 bps
d345domain3.example.com		Модерируется	203.0.113.8 203.0.113.9	
Строк на страницу 20 1-3 из 3 < >				

Личный кабинет: Сервисы



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Сервисы» личного кабинета вы можете описать, какой трафик должен считаться легитимным при [подключении по протоколу BGP](#).

Каждый сервис включает в себя:

- один или несколько IP-адресов (раздел [«IP-адреса»](#)),
- один или несколько открытых портов, на которых разрешена работа тех или иных сетевых протоколов (раздел [«Порты и протоколы»](#)).

Перечень сервисов, настроенный в личном кабинете, называется *картой сервисов*. Карта сервисов должна полностью описывать ожидаемый легитимный трафик, который будет проходить через сеть Curator. Защита от DDoS будет автоматически настроена так, чтобы определять и предотвращать атаки на указанные протоколы. Кроме того, будет запрещён весь входящий и исходящий трафик к IP-адресам, портам и протоколам, не указанным в карте сервисов.

Перед добавлением сервисов необходимо [настроить соответствующие префиксы](#).

Для каждого добавленного сервиса в личном кабинете становятся доступны разделы со статистикой и настройками конкретных услуг, см. [Обзор интерфейса личного кабинета](#).

Посмотреть список сервисов

Сервисы, доступные вашему аккаунту, отображаются в виде таблицы со следующими полями:

- **ID** — уникальный идентификатор сервиса в системе Curator (например, [d12345](#)), а также его название (например, [Основной сайт](#)). Нажмите на ID сервиса, чтобы перейти к его статистике и настройкам.
- **IP-адреса** — список IP-адресов сервиса.
- **Статус** — текущее состояние сервиса.
 - **Онлайн** — сервис обслуживается.
 - **Офлайн** — сервис отключён.
 - **Обновляется** — происходит применение изменённой конфигурации услуг.

-  **Ошибка** — произошла непредвиденная ошибка, сервис может быть недоступен. Обратитесь в техническую поддержку Curator за подробностями.
- **Трафик** — скорость трафика между пользователями и сетью Curator для данного сервиса. Каждое значение рассчитывается как средняя скорость в секунду на основе информации за последнюю минуту.
 -  — входящий трафик.
 -  — исходящий трафик.

Рядом с заголовками столбцов таблицы присутствуют поля фильтров, с помощью которых вы можете быстро найти сервисы, удовлетворяющие определённым условиям.

По умолчанию таблица отображает не более 20 сервисов одновременно. Если для вашего аккаунта доступно больше сервисов, то для перехода к другим частям списка используйте кнопки **<** и **>** под таблицей. Также вы можете выбрать количество сервисов, отображаемых за один раз, с помощью поля **Строк на страницу**.

Добавить сервис

Чтобы добавить новый сервис в карту сервисов:

1. Откройте раздел **Сервисы** и нажмите кнопку **Добавить сервис**.
2. В появившемся диалоге введите произвольное название сервиса (например, «Основной сайт»).
3. Укажите IP-адреса, по которым должен быть доступен сервис. Каждый вводимый IP-адрес должен принадлежать к одному из подтверждённых префиксов в разделе [«Префиксы»](#).

Указать адреса можно двумя способами:

- **Ручной ввод IP-адресов**

Введите один или несколько IP-адресов в поле **IP адреса**.

- **Определение IP-адресов с помощью DNS**

Нажмите ссылку **DNS поиск**. В появившемся диалоге введите **Имя хоста**, по которому сейчас доступен необходимый апстрим, и нажмите кнопку **Найти**. В диалог автоматически загрузится список адресов из А-записи домена. При необходимости снимите галочки с адресов, которые не должны быть аптримами в новой конфигурации. После этого нажмите кнопку **Импортирование**.

4. Нажмите кнопку **Подтвердить**.

После создания сервиса рекомендуется настроить для него разрешённые порты и протоколы. Для этого кликните по ID созданного сервиса, выберите раздел [«Порты и протоколы»](#) и задайте необходимые настройки.

Когда все необходимые настройки заданы, [включите сервис](#).

Включить сервис

Чтобы включить сервис и разрешить прохождение соответствующего трафика:

1. В разделе **Сервисы** личного кабинета выберите нужный сервис.
2. В верхней части страницы нажмите кнопку **Включить сервис**.
3. В появившемся диалоге подтвердите операцию, нажав кнопку **Включить**.

Сервис на некоторое время перейдёт в состояние **Обновляется**, после чего перейдёт в состояние **Онлайн**.

Отключить сервис

Чтобы отключить сервис, обратитесь в техническую поддержку Curator.

Удалить сервис

Чтобы удалить сервис, обратитесь в техническую поддержку Curator.

Пример конфигурации

ID	IP-адреса	Статус	Трафик
		Все	
d123 Основной сайт	203.0.113.10		
d234 DNS-сервер	203.0.113.1		
Строк на страницу 20 1-3 из 3 < >			

Личный кабинет: Префиксы



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Префиксы» личного кабинета вы можете управлять списком префиксов, используемых для подключения к Curator по протоколу BGP. Настройки префиксов должны выполняться вместе с настройкой карты сервисов в разделе «Сервисы».

Посмотреть список префиксов

Чтобы посмотреть все префиксы, доступные вашему аккаунту:

1. Откройте раздел **Префиксы**.
2. При необходимости переключитесь на нужную вкладку: **Подтверждённые** или **Неподтверждённые** (см. [Добавить префикс](#)). По умолчанию выбрана вкладка **Все префиксы**.

Префиксы будут перечислены в таблице со следующими столбцами:

- **Префикс** — уникальный идентификатор префикса в системе Curator (например, [p123](#)), а также его маска подсети.
- **Номер АС** — номер автономной системы (Autonomous System, AS), которая является источником (origin) для этого префикса.
- **Статус** — состояние данного префикса в системе (см. описание в разделе [Добавить префикс](#)):
 - **Новый** — префикс добавлен в список, но соответствующая заявка ещё не отправлена на рассмотрение.
 - **Обрабатывается** — заявка находится на модерации.
 - **Проверен** — префикс одобрен и может быть анонсирован.
 - **Отказ** — заявка отклонена.

По умолчанию таблица отображает не более 30 префиксов за один раз. Если для аккаунта сконфигурировано больше префиксов, то для перехода к другим частям списка используйте кнопки < и > под таблицей. Также вы можете выбрать количество префиксов, отображаемых за один раз, с помощью поля **Строк на страницу**.

Добавить префикс

Чтобы добавить новый префикс и подтвердить владение им:

1. В разделе **Префиксы** личного кабинета нажмите кнопку **Добавить префикс**.
2. В поле **Префикс** укажите префикс подсети, который вы собираетесь анонсировать через сеть Curator. При вводе префикса используйте нотацию CIDR, например: `198.51.100.0/24`.
3. В поле **Номер АС** укажите номер автономной системы, которой принадлежит префикс. Это можно сделать двумя способами.

- **Ручной ввод**

Введите номер автономной системы в текстовое поле, например: `64500`.

- **Автоматический поиск**

Рядом с полем **Префикс** нажмите . Загрузится список из одной или нескольких автономных систем, к которым относится префикс. Поставьте чекбокс рядом с номером вашей автономной системы.

Если вы хотите вернуться к ручному вводу номера, нажмите ссылку **Ручной ввод**.

4. Нажмите кнопку **Добавить**.

В списке префиксов появится новая запись с введёнными данными. В столбце **Статус** будет отображён значок .



ВАЖНО

На следующем шаге будет инициирована проверка данных о префиксе, после чего введённые данные нельзя будет изменить. Поэтому убедитесь, что данные введены верно.

Если допущена ошибка, исправьте её. Для этого кликните на префикс в списке и на открывшейся странице нажмите кнопку **Редактировать**. В появившемся диалоге внесите необходимые изменения в полях **Префикс** и **Номер АС** и нажмите кнопку **Сохранить**.

5. Кликните на префикс в списке. На открывшейся странице нажмите кнопку **Отправить на модерацию**.
6. Curator направит письмо со ссылкой на адрес, указанный как `tech-c` для указанной автономной системы согласно базе данных интернет-регистратора. Перейдите по ссылке в этом письме, чтобы подтвердить владение префиксом.

После того, как владение префиксом успешно подтверждено, в столбце **Статус** для этого префикса будет отображаться значок .

Если владение префиксом не было подтверждено в отведённый срок и ссылка стала недействительной, для префикса будет отображаться значок . Вы можете инициировать повторную проверку владения, выполнив предыдущий шаг ещё раз.

После добавления префикса настройте сервисы, которые должны быть доступны в нём, в разделе «Сервисы».

Пример конфигурации

ВСЕ ПРЕФИКСЫ (3) ПОДТВЕРЖДЁННЫЕ (1) НЕПОДТВЕРЖДЁННЫЕ (2)			
Префикс	Номер АС	Статус	Анонс
p123 198.51.100.0/24	AS64500		
p456 203.0.113.0/24	AS64500		
p789 233.252.0.0/24	AS65536		
Строк на страницу 30 ▾ 1-3 из 3 < >			

В этом примере добавлены три префикса. Для всех трёх был инициирован процесс проверки владения, но только для префикса [203.0.113.0/24](#) он был успешно завершён. Теперь этот префикс можно анонсировать по протоколу BGP в сеть Curator.

Личный кабинет: Статистика



ПРИМЕЧАНИЕ

В конфигурации по умолчанию этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*.

Для каждого [домена](#) или [сервиса](#) доступен раздел «Статистика», в котором отображаются данные о входящем трафике. Вы можете переключаться между различными [категориями данных](#), [периодами](#) и [представлениями](#).

Построенный график можно скачать в виде изображения, нажав кнопку . Изображение будет скачано в том же размере, в котором оно было отображено в браузере на момент сохранения.

Выбор категории данных

В верхней части страницы находится выпадающий список, в котором вы можете выбрать категорию данных для отображения на графике. По умолчанию отображается категория «[Трафик](#)».

Категория содержит несколько наборов данных. Каждый набор данных показывается отдельным цветом на графике. Вы можете скрыть набор данных с графика, кликнув по его обозначению в легенде.

Доступны следующие категории:

- **Трафик**

Количество входящего и исходящего трафика, бит/с. Разными цветами обозначаются разные виды трафика:

- *Входящий* — весь трафик от пользователей.
- *Пропущенный* — трафик от пользователей, не являвшийся частью атак.
- *Исходящий* — трафик от апстрима к пользователям.
- *Оплачиваемый* — трафик, за который Curator выставляет счёт клиенту (только в [представлении «График»](#)).

- **Трафик (входящий)**

Количество трафика от пользователей, бит/с. Разными цветами обозначаются протоколы *TCP*, *UDP*, *ICMP*, а также *Other* (все остальные протоколы).

- **Пакеты**

Количество входящих и исходящих пакетов в секунду. Разными цветами обозначаются разные виды трафика:

- *Входящий* — весь трафик от пользователей.
- *Пропущенный* — трафик от пользователей, не являвшийся частью атак.
- *Исходящий* — трафик от апстрима к пользователям.

- **Пакеты (входящие)**

Количество пакетов от пользователей в секунду. Разными цветами обозначаются протоколы *TCP*, *UDP*, *ICMP*, а также *Other* (все остальные протоколы).

- **Запросы**

Общее количество запросов в секунду (статических и динамических), а также количество только динамических запросов.

- Статическими запросами считаются запросы типа GET с известными расширениями в именах запрашиваемых файлов (стили, изображения, видеофайлы и т.п.).
- Динамическими запросами считаются все запросы, кроме статических.

- **Время ответа**

Количество запросов в секунду, на которые апстрим ответил в течение указанного периода.

Разными цветами отображаются данные по разным периодам ответов: *Менее 200мс*, *200-500мс*, *500-700мс*, *700-1000мс*, *1-1.5с*, *1.5-2с*, *2-5с*, *Более 5с*.

- **Ошибки**

Количество запросов в секунду, на которые обратный HTTP-прокси Curator ответил тем или иным кодом ошибки. Отображаются данные по кодам ошибок HTTP 4xx и HTTP 5xx.

- **Чёрный список**

Количество заблокированных IP-адресов, с которых поступали запросы. Разными цветами обозначаются IP-адреса из автоматически обновляемых чёрных списков Curator и WAF, а также собственного чёрного списка клиента.

- **Bot protection**

Количество *Проверок* и *Блокировок* в секунду, совершённых в рамках [Перенаправления с установкой cookie](#).

Выбор периода

Вы можете изменить период, за который отображаются данные на графике, одним из двух способов.

- Жажмите левую кнопку мыши в начале интересующего вас участка графика и, не отпуская кнопку, потяните до конца участка. Масштаб графика автоматически поменяется так, чтобы включать данные только из выбранного участка. Такое увеличение масштаба можно производить последовательно несколько раз.

Чтобы вернуться к предыдущему масштабу, нажмите кнопку . Чтобы вернуться к масштабу, который использовался до увеличений, нажмите кнопку **Сбросить зум**.

- Выберите один из предустановленных периодов в выпадающем списке в верхней части страницы. Необходимые данные автоматически подгрузятся и отобразятся на графике. При этом масштаб графика (см предыдущий пункт) автоматически сбросится.

По умолчанию установлен период **5 часов**.

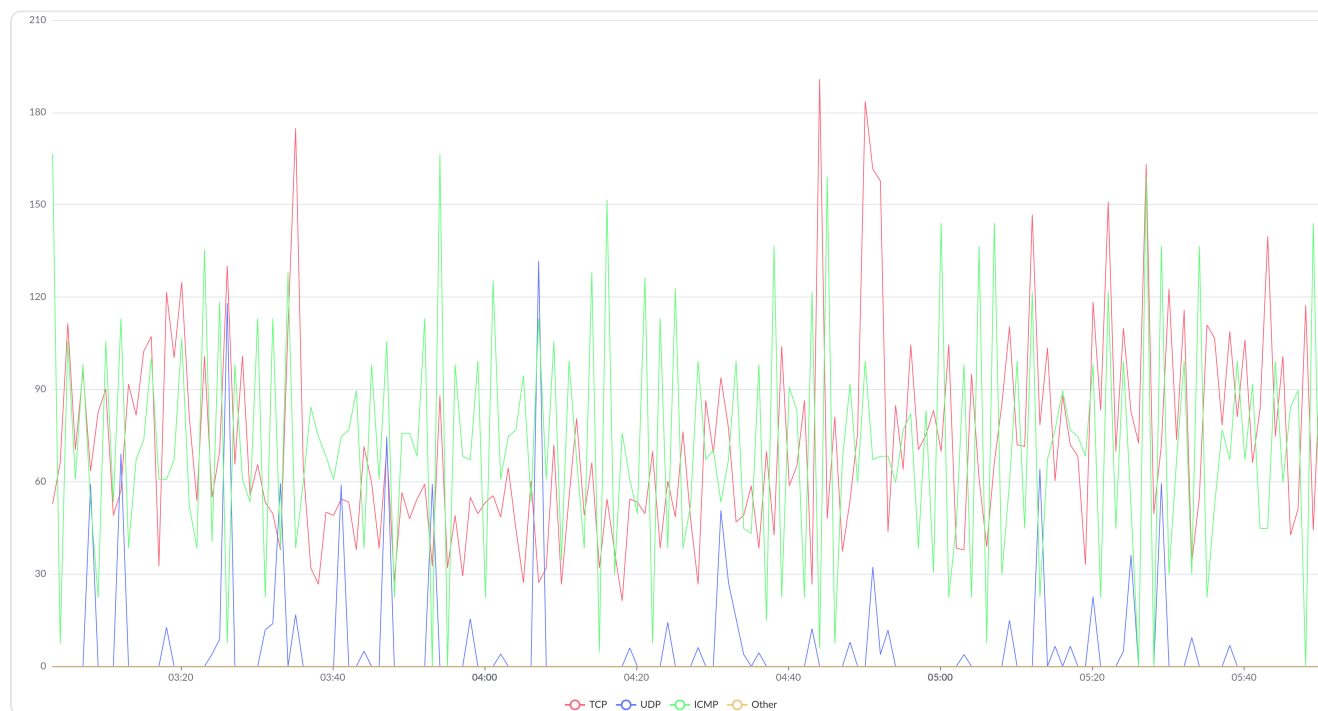
Выбор представления

Для всех **категорий данных**, кроме категории «Запросы», над графиком отображается переключатель представления. Воспользуйтесь им, чтобы представить данные в одном из следующих вариантов:

График (по умолчанию)

Разные значения показываются как независимые линии на графике.

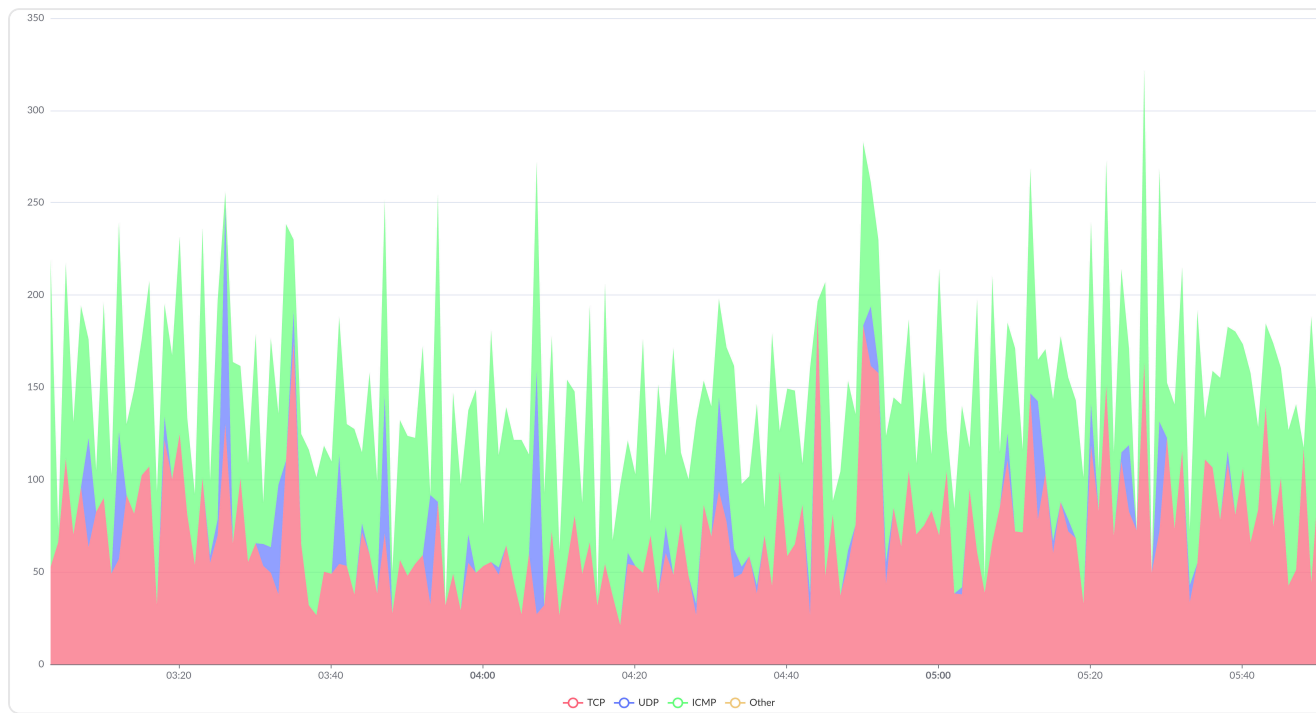
Этот тип представления используется, если опции **Stack** и **Stack 100%** отключены.



Столбчатая диаграмма

Объёмы разных видов трафика показываются разным цветом друг над другом, позволяя оценить вклад каждого из них в суммарное значение.

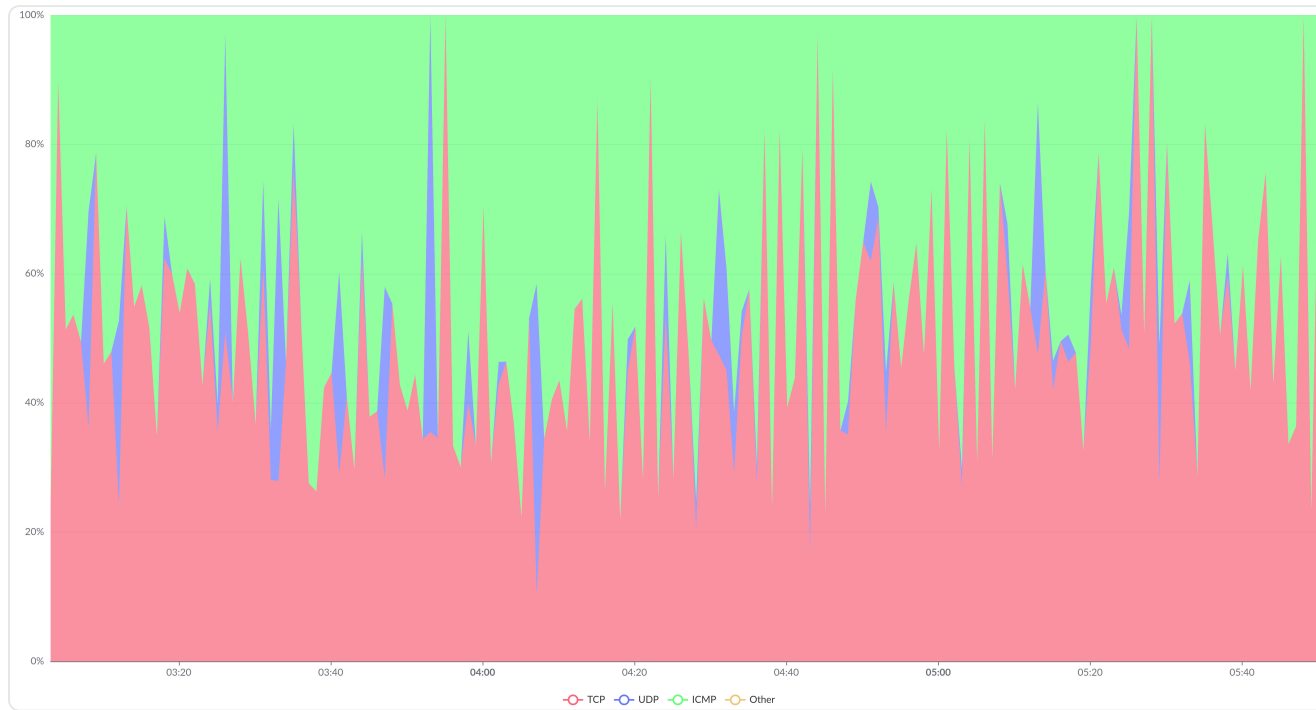
Чтобы выбрать этот тип представления, установите опцию **Stack**.



Столбчатая диаграмма с накоплением

Формируется аналогично обычной *Столбчатой диаграмме*, но суммарное значение в каждый момент времени принимается за 100% и отображается на всю высоту графика.

Чтобы выбрать этот тип представления, установите опцию **Stack 100%**.



Личный кабинет: Сервисы



ПРИМЕЧАНИЕ

Этот раздел личного кабинета:

- доступен только для доменов, см. [Обзор интерфейса личного кабинета](#);
- доступен для редактирования пользователям с *Технической ролью* и для просмотра пользователям с *Административной ролью*, см. [Пользователи](#).

В этом разделе личного кабинета вы можете управлять несколькими типами *сервисов* на вашем аккаунте Curator. Список сервисов определяет, как запросы пользователей будут маршрутизироваться к вашим апстримам.

Каждый сервис соответствует:

- одному порту на вашем Curator IP для соединения с пользователями,
- одному или нескольким IP-адресам и портам для соединения с апстримами.

Доступны следующие типы сервисов:

- **HTTP** — [обратный HTTP-прокси](#),
- **WebSocket** — [обратный WebSocket-прокси](#),
- **TCP Proxy** — обратный TCP-прокси в режиме [Proxy Protocol](#),
- **TCP** — [туннелирование](#).

Обратите внимание, что интерфейс «Сервисы» не рассчитан на одновременное редактирование данных с нескольких устройств или из нескольких вкладок. Если данные были изменены кем-то после того, как вы начали работу в разделе, Curator покажет сообщение о конфликте. В этом случае нажмите **Сохранить**, чтобы подтвердить ввод своих данных (с перезаписью всех изменений, сделанных другим пользователем), или **Отмена**, чтобы сбросить свои изменения и перезагрузить актуальные данные.

Посмотреть список сервисов

Чтобы посмотреть список сервисов, настроенных для домена:

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **Сеть** → **Сервисы**.

Апстримы, сконфигурированные для домена, будут отображены в виде таблицы.

☐								ДОБАВИТЬ
	Фильтр							
☐	HTTP	Порт: 80	Web Backend 1	Web Backend 2	Web Backend 3	🔒		✎ 🗑
☐	HTTP	Порт: 443	Web Backend 1	Web Backend 2	Web Backend 3	🔒 HTTP/2		✎ 🗑
☐	WEBSOCKET	Порт: 8080	Video Server 1	Video Server 2		🔒		✎ 🗑

Для каждого сервиса отображаются:

- Тип сервиса.
- Номер порта на Curator IP.
- Названия или адреса апстримов. Если для сервиса настроено более трёх апстримов, для просмотра полного списка нажмите .
- Обозначения дополнительных особенностей сервиса:
 -  — обратный HTTP-прокси без шифрования,
 -  — обратный HTTP-прокси с шифрованием,
 - **HTTP/2** — обратный HTTP-прокси с поддержкой протокола HTTP/2,
 -  — сервис с доступом только по белому списку.

Для быстрого поиска записей используйте поле фильтра над списком. В фильтр можно вводить:

- имя протокола, например, «HTTP» или «WebSocket»
- номер открытого порта, например, «80» или «53»
- название, IP-адрес или порт апстрима, например, «198.51.100.0».

Настроить сервис HTTP

Сервис типа «*HTTP*» определяет параметры работы [обратного HTTP-прокси](#). Прокси обрабатывает запросы пользователей к одному порту Curator IP и отправляет их на один из заданных апстримов в соответствии с выбранным [алгоритмом балансировки](#).

При настройке сервиса вы можете включить использование шифрования TLS как для обработки запросов пользователей, так и для соединения с апстримами. Обратите внимание, что чтобы включить TLS для обработки запросов пользователей, необходимо предварительно добавить хотя бы один сертификат в [Хранилище сертификатов](#) вашего аккаунта и установить его в разделе [TLS](#) настроек домена.

Чтобы добавить или изменить сервис типа «*HTTP*»:

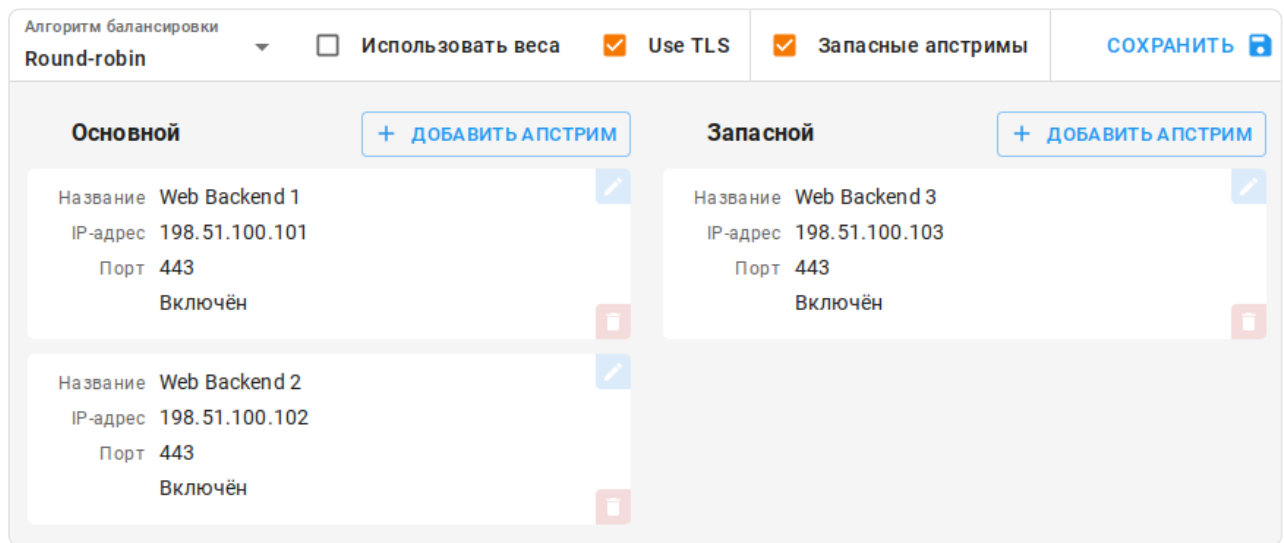
1. В разделе **Домены** личного кабинета выберите нужный домен.

2. Выберите пункт меню **Сервисы**.
3. Нажмите **Добавить** для настройки нового сервиса или нажмите  рядом с ранее добавленным сервисом, чтобы перейти к его редактированию.

При добавлении нового сервиса укажите тип «*HTTP*».

4. Укажите основные настройки для сервиса.
 - **Порт** — номер порта, к которому подключается пользователь.
 - **Использовать TLS** — обрабатывать запросы по протоколу HTTPS, а не HTTP. Эта настройка доступна, если для домена установлен хотя бы один TLS-сертификат.
 - **Использовать HTTP/2** — обрабатывать запросы, сделанные по протоколу HTTP/2. Эта настройка доступна, если для домена установлен хотя бы один TLS-сертификат, а также включена опция **Использовать TLS**.
 - **Ограниченный доступ** — сбрасывать соединения от IP-адресов, не входящих в [белый список](#).
5. Нажмите кнопку **Настройка апстримов**.

Откроется диалог для управления списком апстримов и настройками балансировки.



The screenshot shows a configuration window for upstreams. At the top, there are settings for the load balancing algorithm (Round-robin), checkboxes for 'Использовать веса' (disabled), 'Use TLS' (checked), and 'Запасные апстримы' (checked), along with a 'СОХРАНИТЬ' button. Below this, there are two columns: 'Основной' (Primary) and 'Запасной' (Backup). Each column has a '+ ДОБАВИТЬ АПСТРИМ' button. The 'Основной' column contains two entries: 'Web Backend 1' (IP: 198.51.100.101, Port: 443, Status: Включён) and 'Web Backend 2' (IP: 198.51.100.102, Port: 443, Status: Включён). The 'Запасной' column contains one entry: 'Web Backend 3' (IP: 198.51.100.103, Port: 443, Status: Включён). Each entry has edit and delete icons.

6. В верхней части диалога укажите основные настройки балансировки нагрузки.
 - **Алгоритм балансировки** — эта настройка влияет на то, как обратный HTTP-прокси будет [выбирать апстрим](#), на который отправить входящий запрос от пользователя.
 - *Round-robin*: обратный прокси будет стремиться обеспечить равномерное распределение нагрузки между включёнными апстримами. Разные запросы от одного пользователя могут попадать на разные апстримы.
 - *IP hash*: обратный прокси будет закреплять апстрим за пользователем, пока этот апстрим доступен.
 - **Использовать веса** — если эта опция включена, то вы можете указать вес для каждого апстрима, чтобы повлиять на распределение запросов. В зависимости от используемого

алгоритма вес апстрима интерпретируется по-разному. Более подробно влияние весов на работу алгоритмов балансировки описано в разделе [Алгоритмы выбора апстрима](#). Если опция отключена, то веса всех включённых апстримов считаются одинаковыми.

- **Use TLS** — использовать защищённый протокол HTTPS для соединений с апстримами.
- **Запасные апстримы** — если эта опция включена, то обратный HTTP-прокси будет переключаться с основного списка на запасной, когда апстримы из основного списка будут недоступны. Принцип переключения описан в разделе [Переключение между списками апстримов](#). Если опция отключена, то запасные апстримы не используются даже при недоступности основных.

7. Задайте апстримы для сервиса. Вы можете организовать независимые [основной или запасной список апстримов](#). Обратите внимание, что в основном списке всегда должен присутствовать хотя бы один апстрим — в противном случае изменения нельзя будет сохранить.

Чтобы добавить апстрим, нажмите **Добавить апстрим** рядом с соответствующим списком. В появившемся диалоге укажите IP-адрес, порт и, опционально, название апстрима. Для удобства можно заполнить форму данными от другого апстрима: нажмите  и в появившемся списке кликните по нужному IP-адресу (чтобы скопировать название и IP-адрес без порта) или порту (чтобы скопировать данные целиком). Если вы хотите временно исключить апстрим из алгоритма балансировки, снимите чекбокс **Включён**. Чтобы завершить редактирование и вернуться к предыдущему диалогу, нажмите **Добавить**.

Кроме того в настройках можно указать DNS-запись (перед этим необходимо написать в техническую поддержку, чтобы опция стала доступна).

Чтобы переместить апстрим из одного списка в другой или изменить его очерёдность в списке, перетащите мышью соответствующую карточку.

Чтобы отредактировать апстрим, нажмите кнопку



на его карточке, внесите необходимые изменения и нажмите **ОК**.

Чтобы удалить апстрим из списка, нажмите кнопку



на его карточке.

8. Нажмите кнопку **Сохранить** в диалоге настроек сервиса.

Если закрыть диалог, не нажав эту кнопку, то внесённые изменения будут потеряны.

9. Если необходимо, добавьте или отредактируйте другие сервисы перед сохранением изменений. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Настроить сервис WebSocket

Сервис типа «*WebSocket*» определяет параметры работы [обратного WebSocket-прокси](#). Прокси обрабатывает запросы пользователей к одному порту Curator IP и отправляет их на один из заданных апстримов в соответствии с алгоритмом *IP hash*.

При настройке сервиса вы можете включить использование шифрования TLS как для обработки запросов пользователей, так и для соединения с апстримами. Обратите внимание, что чтобы включить TLS для обработки запросов пользователей, необходимо предварительно загрузить хотя бы один сертификат в [Хранилище сертификатов](#) вашего аккаунта и установить его в разделе [TLS](#) настроек домена.

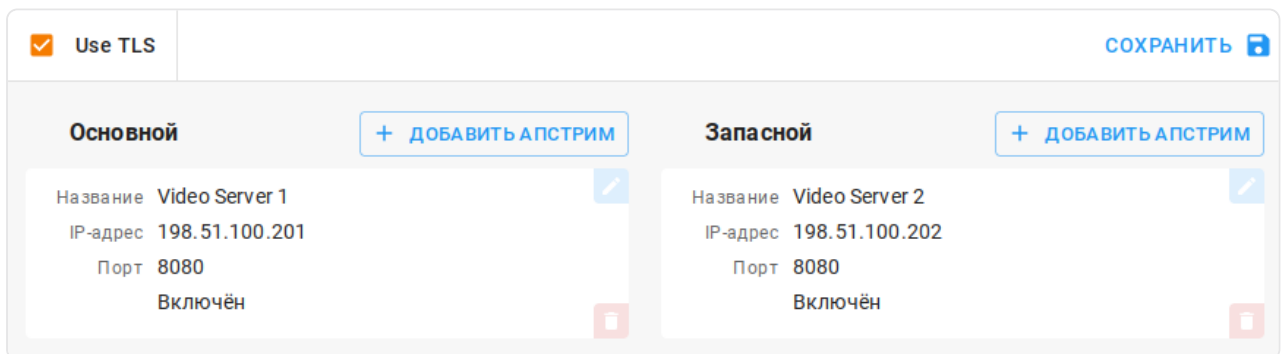
Чтобы добавить или изменить сервис типа «*WebSocket*»:

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **Сервисы**.
3. Нажмите **Добавить** для настройки нового сервиса или нажмите  рядом с ранее добавленным сервисом, чтобы перейти к его редактированию.

При добавлении нового сервиса укажите тип «*WebSocket*».

4. Укажите основные настройки для сервиса.
 - **Порт** — номер порта, к которому подключается пользователь.
 - **Использовать TLS** — обрабатывать запросы по протоколу HTTPS, а не HTTP. Эта настройка доступна, если для домена установлен хотя бы один TLS-сертификат.
 - **Ограниченный доступ** — сбрасывать соединения от IP-адресов, не входящих в [белый список](#).
5. Нажмите кнопку **Настройка апстримов**.

Откроется диалог для управления списком апстримов.



6. В верхней части диалога отметьте чекбокс **Use TLS**, если вам необходимо использовать защищённый протокол HTTPS для соединений с апстримами.
7. Задайте апстримы для сервиса. Вы можете организовать независимые [основной или запасной список апстримов](#). Обратите внимание, что в основном списке всегда должен присутствовать хотя бы один апстрим. В противном случае изменения нельзя будет сохранить.

Чтобы добавить апстрим, нажмите **Добавить апстрим** рядом с соответствующим списком. В появившемся диалоге укажите его IP-адрес, порт и, опционально, название. Для удобства можно

заполнить форму данными от другого апстрима: нажмите  и в появившемся списке кликните по нужному IP-адресу (чтобы скопировать название и IP-адрес без порта) или порту (чтобы скопировать данные целиком). Если вы хотите временно исключить апстрим из алгоритма балансировки, снимите чекбокс **Включён**. Чтобы завершить редактирование и вернуться к предыдущему диалогу, нажмите **Добавить**.

Чтобы переместить апстрим из одного списка в другой или изменить его очерёдность в списке, перетащите мышью соответствующую карточку.

Чтобы отредактировать апстрим, нажмите кнопку



на его карточке, внесите необходимые изменения и нажмите **ОК**.

Чтобы удалить апстрим из списка, нажмите кнопку



на его карточке.

8. Нажмите кнопку **Сохранить** в диалоге настроек сервиса.

Если закрыть диалог, не нажав эту кнопку, то внесённые изменения будут потеряны.

9. Если необходимо, добавьте или отредактируйте другие сервисы перед сохранением изменений. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Настроить сервис TCP Proxy

Сервис типа «*TCP Proxy*» определяет параметры работы [обратного TCP-прокси в режиме Proxy Protocol](#). Прокси обрабатывает запросы пользователей к одному порту Curator IP и отправляет их на один из заданных апстримов. Порядок выбора апстрима может быть настроен специалистами технической поддержки по вашему запросу, см. [Переключение между апстримами](#).

Чтобы добавить или изменить сервис типа «*TCP Proxy*»:

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **Сервисы**.
3. Нажмите **Добавить** для настройки нового сервиса или нажмите  рядом с ранее добавленным сервисом, чтобы перейти к его редактированию.

При добавлении нового сервиса укажите тип «*TCP Proxy*».

4. Укажите основные настройки для сервиса.
 - **Порт** — номер порта, к которому подключается пользователь.
 - **Ограниченный доступ** — сбрасывать соединения от IP-адресов, не входящих в [белый список](#).

5. Нажмите кнопку **Настройка апстримов**.

Откроется диалог для управления списком апстримов.

Основной	Запасной
Название Proxy Protocol Backend	Название Proxy Protocol Backend
IP-адрес 198.51.100.150	IP-адрес 198.51.100.151
Порт 3000	Порт 3000
Включён	Включён

6. Задайте апстримы для сервиса. Вы можете организовать независимые **основной** или **запасной список апстримов**. Обратите внимание, что в основном списке всегда должен присутствовать хотя бы один апстрим. В противном случае изменения нельзя будет сохранить.

Чтобы добавить апстрим, нажмите **Добавить апстрим** рядом с соответствующим списком. В появившемся диалоге укажите его IP-адрес, порт и, опционально, название. Для удобства можно заполнить форму данными от другого апстрима: нажмите  и в появившемся списке кликните по нужному IP-адресу (чтобы скопировать название и IP-адрес без порта) или порту (чтобы скопировать данные целиком). Если вы хотите временно исключить апстрим из алгоритма балансировки, снимите чекбокс **Включён**. Чтобы завершить редактирование и вернуться к предыдущему диалогу, нажмите **Добавить**.

Чтобы переместить апстрим из одного списка в другой или изменить его очерёдность в списке, перетащите мышью соответствующую карточку.

Чтобы отредактировать апстрим, нажмите кнопку



на его карточке, внесите необходимые изменения и нажмите **ОК**.

Чтобы удалить апстрим из списка, нажмите кнопку



на его карточке.

7. Нажмите кнопку **Сохранить** в диалоге настроек сервиса.

Если закрыть диалог, не нажав эту кнопку, то внесённые изменения будут потеряны.

8. Если необходимо, добавьте или отредактируйте другие сервисы перед сохранением изменений.

Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Настроить сервис TCP

Сервис типа «TCP» определяет трансляцию портов для работы **туннелирования**.

Чтобы добавить или изменить сервис типа «TCP»:

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **Сервисы**.
3. Нажмите **Добавить** для настройки нового сервиса или нажмите  рядом с ранее добавленным сервисом, чтобы перейти к его редактированию.

При добавлении нового сервиса укажите тип «TCP».

4. Укажите настройки для сервиса.
 - **Порт** — номер порта, к которому подключается пользователь.
 - **Апстрим** — IP-адрес и номер порта для подключения к апстриму.
 - **Ограниченный доступ** — сбрасывать соединения от IP-адресов, не входящих в [белый список](#).
5. Нажмите кнопку **Сохранить** в диалоге настроек сервиса.

Если закрыть диалог, не нажав эту кнопку, то внесённые изменения будут потеряны.

6. Если необходимо, добавьте или отредактируйте другие сервисы перед сохранением изменений.
Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить сервис

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **Сервисы**.
3. Найдите нужный сервис и кликните  рядом с ним.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Личный кабинет: IP-адреса



ПРИМЕЧАНИЕ

Этот раздел личного кабинета доступен только пользователям с *Административной* или *Технической ролью*. Редактировать настройки могут только пользователи с *Технической ролью*.

В разделе «IP-адреса» личного кабинета вы можете посмотреть или изменить список IP-адресов, на которые сеть Curator должна перенаправлять трафик данного сервиса.

Посмотреть сведения об IP-адресах

1. В разделе **Сервисы** личного кабинета выберите нужный сервис.
2. Выберите пункт меню **IP-адреса**.

На странице будет отображён список IP-адресов сервиса.

Нажмите над списком, чтобы отсортировать адреса по возрастанию или убыванию.

Нажмите напротив IP-адреса, чтобы перейти к информации об этом адресе на сайте [Qrator Radar](#).

Изменить список IP-адресов

1. В разделе **Сервисы** личного кабинета выберите нужный сервис.
2. Выберите пункт меню **IP-адреса**.
3. В правом верхнем углу нажмите кнопку **Редактировать**.
4. Укажите IP-адреса, по которым должен быть доступен сервис. Каждый вводимый IP-адрес должен принадлежать к одному из подтверждённых префиксов в разделе «[Префиксы](#)».

Указать адреса можно двумя способами:

- **Ручной ввод IP-адресов**

Введите один или несколько IP-адресов в поле **IP адреса**.

- **Определение IP-адресов с помощью DNS**

Нажмите ссылку **DNS поиск**. В появившемся диалоге введите **Имя хоста**, по которому сейчас доступен необходимый апстрим, и нажмите кнопку **Найти**. В диалог автоматически загрузится

список адресов из А-записи домена. При необходимости снимите галочки с адресов, которые не должны быть апстримами в новой конфигурации. После этого нажмите кнопку **Импортирование**.

5. Нажмите кнопку **Сохранить**.

Личный кабинет: Порты и протоколы



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Порты и протоколы» личного кабинета вы можете указать направления и объём легитимного трафика, который ожидается для IP-адресов текущего [сервиса](#).

Принцип работы

Данные в этом разделе вводятся в виде списка записей. Каждая запись (за исключением записи [IP service → ANY](#)) содержит информацию об одном разрешённом сетевом протоколе. В зависимости от протокола, запись может также содержать дополнительные настройки, определяющие порт, на котором разрешена работа этого протокола, и применяемый к нему лимит на объём трафика.

Весь входящий и исходящий трафик, не описанный ни в одной записи ни для одного из сервисов, будет считаться нелегитимным и отбрасываться при прохождении через центры очистки данных Curator. Подробнее о работе по протоколу BGP см. в статье [Подключение: BGP](#).

Доступны следующие типы записей:

- **Application → DNS**

Добавьте такую запись, если на указанном порту работает ваш DNS-сервер, трафик к которому вы защищаете с помощью услуги [Защищённый DNS](#) от Curator. Легитимным будет считаться входящий трафик к указанному порту от вторичных или кеширующих DNS-серверов Curator, а также ответный исходящий трафик. Обратите внимание, что добавления этой записи недостаточно для включения Защищённого DNS. Обратитесь в техническую поддержку Curator для корректной настройки услуги.



СОВЕТ

Если вы не собираетесь использовать Защищённый DNS от Curator, но хотите, чтобы трафик до вашего DNS-сервера считался легитимным, вместо этой записи просто добавьте запись [IP service → TCP](#) или [IP service → UDP](#) с указанием нужного порта (обычно 53).

- **Application → HTTP**

Добавьте такую запись, если на указанном порту работает веб-сервер по протоколу HTTP или HTTPS. Трафик будет анализироваться для выявления атак, специфичных для этих протоколов, как описано в разделе [Обратный HTTP-прокси](#).

Для данной записи доступна дополнительная настройка **Защищённое соединение до апстрима**. Если веб-сервер на указанном порту работает по протоколу HTTPS, включите эту настройку. В противном случае оставьте её выключенной.

- **IP service** → (протокол)

Добавьте запись с указанием конкретного протокола из раздела **IP service**, чтобы разрешить входящий и исходящий трафик с использованием выбранного протокола. Протокол трафика определяется по заголовкам в IP-пакетах. Доступны все протоколы, описанные в документе [Assigned Internet Protocol Numbers](#).

Чекбокс **Ограниченный доступ** позволяет запретить трафик от IP-адресов, не находящихся в [белом списке](#).

Для любого протокола, кроме TCP, доступна дополнительная настройка **Лимит скорости**. Указанный лимит применяется по отдельности к входящему и исходящему трафику на указанном порту каждого IP-адреса сервиса. Весь трафик, превышающий лимит, будет отбрасываться вне зависимости от присутствия IP-адреса пользователя в [белом списке](#).

Для протокола TCP настройка **Лимит скорости** недоступна, т. к. система фильтрации по умолчанию пропускает на апстрим только легитимные TCP соединения.

Для **IP service** → **TCP** доступны три режима работы с входящим трафиком:

- **Весь TCP-трафик** — открывается входящий и исходящий TCP-трафик по всем портам.
- **Указать порт** — открывается входящий TCP-трафик по указанному порту, а также исходящий трафик в рамках ответов на легитимные TCP-соединения.
- **Запретить** — в этом режиме ниже становится доступен чекбокс **Весь трафик** в секции **Исходящий трафик**: если он поставлен, то Curator будет пропускать только исходящий TCP-трафик по всем портам (но не входящий).

Для **IP service** → **UDP** доступны два режима работы с входящим трафиком:

- **Весь UDP-трафик** — открывается входящий и исходящий UDP-трафик по всем портам.
- **Указать порт** — открывается входящий UDP-трафик на один указанный порт.

Также для **IP service** → **UDP** доступна настройка **Блокировка Amplification атак**. Если она включена, то Curator будет считать нелегитимным входящий трафик на портах, уязвимых для популярных видов [Amplification DDoS-атак](#). В частности, будут закрыты порты 53 и 123, часто используемые злоумышленниками для Amplification-атак по протоколам DNS и NTP соответственно. Если вы ожидаете легитимный трафик на этих портах, то есть если на них работают ваши DNS-сервер и NTP-сервер, рекомендуем описать их через отдельный сервис, не отключая блокировку Amplification-атак для всего остального UDP-трафика.

- **IP service** → **ANY**

Добавьте такую запись, чтобы разрешить определённое количество входящего и исходящего трафика, не предусмотренного другими записями. Для данной записи доступна настройка **Лимит скорости**, указывающая, какое именно количество неопознанного трафика считается допустимым. Один и тот же лимит применяется по отдельности к входящему и исходящему неопознанному трафику.

Эта запись всегда применяется последней. Таким образом, в эту категорию попадает только трафик, который не был описан никакой другой записью.

**ВАЖНО**

При описании трафика, который должен быть разрешён для вашего сервиса, очень легко забыть о каком-то редко случающемся виде входящих или исходящих запросов и таким образом случайно заблокировать какие-то функции сервиса. Мы рекомендуем создать запись ANY, которая скомпенсирует такую ошибку.

Чаще всего имеет смысл создать запись ANY с небольшим лимитом, исходя из предположения, что в реальности количество трафика, не описанного другими записями, будет нулевым. После этого, ориентируясь на логи и [статистику сервиса](#), добавляйте новые записи при необходимости, описывая не предусмотренный ранее трафик.

- **Other options** → **Fragmented IP packets**

Добавьте такую запись, чтобы разрешить доставку фрагментированных IP-пакетов. Данная опция может быть необходимой, например, для работы некоторых протоколов SIP-телефонии.

Для данной записи доступна настройка **Лимит скорости**, указывающая, какое именно количество фрагментированных пакетов считается допустимым. Указанный лимит применяется по отдельности к входящему и исходящему трафику.

Посмотреть список записей

Чтобы посмотреть список записей:

1. В разделе **Сервисы** личного кабинета выберите нужный сервис.
2. Выберите пункт меню **Порты и протоколы**.

На странице будет отображён список записей, каждая из которых описывает определённый вид разрешённого трафика, см. [Принцип работы](#).

Для каждой записи отображаются:

- Направление разрешённого трафика:



- — Разрешён трафик, инициированный пользователем



- — Разрешён трафик, инициированный апстримом



- — Разрешены оба вида трафика
- Порт и протокол разрешённого трафика:
 - Для записей из категории **Application** отображаются название разрешённого протокола и номер порта.
 - Для записей из категорий **IP service** и **Other options** отображается название разрешённого протокола.
- Лимит скорости (только для записей, для которых эта настройка доступна)
- Тип соединения с апстримом (только для записей типа [Application → HTTP](#)):
 - — Разрешён незащищённый трафик по протоколу HTTP
 - — Разрешён защищённый трафик по протоколу HTTPS

Для быстрого поиска записей используйте поле фильтра над списком. В фильтр можно вводить:

- имя протокола, например, «TCP» или «DNS»
- номер открытого порта, например, «80» или «53», или строку «ANY»
- номер протокола IP, например, «47» для протокола GRE
- направление трафика, например, «input», «output»

Добавить запись

Чтобы добавить новую запись, описывающую легитимный трафик:

1. Перейдите к [списку портов и протоколов](#).
2. В верхней части страницы нажмите кнопку **Добавить**.
3. В выпадающих списках в появившемся диалоге последовательно выберите категорию и тип записи, которую вы хотите добавить. Подробнее о типах записей см. в разделе [Принцип работы](#).
4. В зависимости от выбранного типа записи, в диалоге могут стать доступными дополнительные настройки. В этом случае задайте необходимые значения этих настроек.
 - **Номер порта**

Укажите номер порта апстрима, на котором будет инициироваться соединение. Обратите внимание, что многие протоколы могут использовать для исходящего трафика порт, отличный от порта, на который поступил входящий трафик. В этом случае для некоторых протоколов

исходящий трафик, соответствующий легитимному входящему трафику, также становится легитимным. Подробнее об обработке разных протоколов см. [Принцип работы](#).

- **Лимит скорости**

Для большинства типов записей необходимо установить лимит скорости. Выберите единицу измерения для лимита в выпадающем списке: **Kbps**, **Mbps** или **Gbps** (опция **Gbps** недоступна для некоторых протоколов). После этого установите значение, введя его в текстовое поле или передвинув ползунок.

- **Защищённое соединение до апстрима**

Данная настройка доступна только для записи типа [Application](#) → [HTTP](#). Включение этой настройки означает, что должен быть разрешён трафик по протоколу HTTPS, а не HTTP.

5. Нажмите кнопку **Сохранить**.

6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменить лимит скорости

Для записей, в которых предусмотрено указание лимита скорости, вы можете изменить этот лимит в любой момент после создания записи.

1. Перейдите к [списку портов и протоколов](#).
2. Кликните по обозначению лимита скорости, который вы хотите изменить.
3. В появившемся диалоге установите необходимый лимит скорости.

Выберите единицу измерения для лимита в выпадающем списке: **Kbps**, **Mbps** или **Gbps** (опция **Gbps** недоступна для некоторых протоколов). После этого установите значение, введя его в текстовое поле или передвинув ползунок.

4. Нажмите кнопку **Сохранить**.

5. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить запись

Чтобы удалить одну запись:

1. Перейдите к [списку портов и протоколов](#).
2. Рядом с записью, которую вы хотите удалить, нажмите .
3. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Чтобы удалить несколько записей:

1. Перейдите к [списку портов и протоколов](#).

- Отметьте записи, которые вы хотите удалить.
- Нажмите ссылку **Удалить** над списком.
- Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Пример конфигурации

☐	↓	DNS	PORT: 53				
☐	↓	HTTP	PORT: 80	🔒	🔒		
☐	↓	HTTP	PORT: 443	🔒	🔒		
☐	↑	TCP					
☐	↕	UDP	PORT: ANY	📄 200 Kbps	✎	🛡️	
☐	↕	ICMP (1)		📄 200 Kbps	✎		

В данном примере клиент указал следующие порты и протоколы:

- Application → DNS на порту 53 для обеспечения работы услуги [Защищённый DNS](#)
- Application → HTTP на портах 80 (HTTP) и 443 (HTTPS) для обеспечения работы услуги [Обратный HTTP-прокси](#)
- IP service → TCP с запрещённым входящим трафиком и разрешённым исходящим
- IP service → UDP с лимитом скорости 200 Kbps и блокировкой Amplification-атак (не будет распространяться на сервис DNS, описанный выше)
- IP service → ICMP с лимитом скорости 200 Kbps

Личный кабинет: TLS



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

Если для ресурса установлен сертификат, к которому текущий пользователь не имеет доступа, то весь раздел «TLS» для данного ресурса становится доступным пользователю только на чтение.

Для каждого [домена](#) или [сервиса](#) доступен раздел «TLS». В нём вы можете смотреть и изменять настройки, в соответствии с которыми TLS-сертификаты используются при работе домена или сервиса.

Здесь вы можете [видеть установленные сертификаты](#), [просматривать информацию о сертификатах](#), а также [устанавливать](#) и [отключать сертификаты](#).

Обратите внимание, что в этом разделе личного кабинета можно только устанавливать сертификаты, добавленные в систему ранее, но не добавлять новые сертификаты. О разнице между установкой и добавлением сертификата, а также о том, как добавить сертификат, см. в разделе [Хранилище сертификатов](#).

Посмотреть установленные сертификаты

Чтобы посмотреть список сертификатов, настроенных для домена или сервиса:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **TLS**.

Сертификаты, установленные для выбранного домена или сервиса, будут отображены в виде таблицы со следующими столбцами:

- **ID** — уникальный числовой идентификатор сертификата в системе Curator. Идентификатор может повторяться в нескольких строках таблицы, если один и тот же сертификат [установлен для разных доменных имён](#).
- **Имя хоста** — информация о том, для какого хоста (доменного имени) должен использоваться этот сертификат. Может быть именем конкретного хоста или строкой «Хост по умолчанию».
- **Subject** — хосты, для которых действителен сертификат, а также ссылка для [просмотра информации о сертификате](#).

- **Not valid after** — конец периода действия сертификата. Если период действия уже закончился, то это поле выделяется цветом.

В столбцах **Имя хоста** и **Subject** в верхней строке есть поля-фильтры. Введя туда нужные значения, вы можете отфильтровать отображаемые в таблице сертификаты.

Посмотреть информацию о сертификате

Чтобы посмотреть информацию о сертификате:

1. Перейдите к [списку сертификатов](#) для домена или сервиса.
2. Найдите строку с нужным сертификатом и кликните в ней по ссылке **Смотреть подробнее**.

В появившемся диалоге будет доступна следующая информация:

- **ID** — уникальный числовой идентификатор сертификата в Хранилище сертификатов.
- **Тип** — происхождение сертификата: *Загруженный* или *Let's Encrypt*.
- **Имена доменов** — доменные имена, для которых действителен сертификат.
- **Not valid before, Not valid after** — начало и конец периода действия сертификата.

Сертификат может содержать одну или несколько цепочек. Если сертификат содержит несколько цепочек, между ними можно переключаться с помощью радиокнопок с названиями соответствующих алгоритмов шифрования. Для каждой цепочки доступна следующая информация:

- **Private key encryption** — криптографический алгоритм, используемый для приватного ключа.
 - **Private key size** — размер приватного ключа в битах.
 - **SHA-256 Fingerprint, SHA-1 Fingerprint** — отпечатки открытого ключа.
 - **Certificate chain** — вся цепочка в формате PEM. Полные данные можно скопировать кнопкой .
 - **Private key** — приватный ключ в формате PEM. Полные данные можно скопировать кнопкой .
- Поле не отображается, если [приватный ключ сертификата скрыт](#).

Установить сертификат для домена или сервиса

1. Убедитесь, что в [Хранилище сертификатов](#) присутствует необходимый сертификат. Если такого сертификата нет — [выпустите](#) или [загрузите](#) его.
2. Перейдите к [списку сертификатов](#) для домена или сервиса.
3. Нажмите кнопку **Установить сертификат**.
4. В появившемся диалоге найдите сертификат, который вы хотите установить.

Вы можете использовать кнопку , чтобы раскрыть более подробное описание конкретного сертификата. Описание включает в себя поля, аналогичные полям в диалоге [краткой информации](#) в Хранилище сертификатов.

В строчке, соответствующей нужному сертификату, нажмите кнопку **Установить**.

5. Укажите, для каких доменных имён должен использоваться этот сертификат.

- Если сертификат должен использоваться для одного или нескольких конкретных доменных имён, введите их в текстовое поле. После каждого доменного имени нажимайте клавишу **Enter** или **Пробел** или вводите запятую.
- Если сертификат должен использоваться в ситуациях, когда пользователь ещё не указал требуемое доменное имя или указал доменное имя, для которого не настроен никакой другой сертификат, отметьте опцию **Использовать данный сертификат по умолчанию для любого доменного имени**.

Нажмите кнопку **Установить**.



ВАЖНО

Обратите внимание, что если на домене или сервисе установлен хотя бы один сертификат для какого-либо доменного имени, то на этом домене или сервисе также обязательно должен быть установлен сертификат по умолчанию.

Внесённые изменения в конфигурации будут отображены в таблице, но не сохраняются автоматически.

6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Отключить сертификат для домена или сервиса

Чтобы отключить ранее установленный сертификат:

1. Перейдите к [списку сертификатов](#) для домена или сервиса.
2. Найдите сертификат, который вы хотите отключить, и в соответствующей строке таблицы нажмите  .

Внесённые изменения в конфигурации будут отображены в таблице, но не сохраняются автоматически.

3. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Сертификат более не будет использоваться при обслуживании этого домена или сервиса, но останется доступным в [Хранилище сертификатов](#). Чтобы удалить сертификат из системы полностью, воспользуйтесь инструкцией: [Личный кабинет: Хранилище сертификатов](#).

Личный кабинет: Списки IP



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В этом разделе вы можете управлять списками IP-адресов, влияющими на работу защиты от DDoS-атак для [домена](#) или [сервиса](#).

- Трафик с IP-адресов из *белого списка* считается легитимным, даже когда в нём есть признаки атак.
- Трафик с IP-адресов из *чёрного списка* считается нелегитимным, даже когда в нём нет признаков атак.

Посмотреть список

Чтобы посмотреть белый или чёрный список для домена или сервиса:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Сеть** → **Списки IP**.
3. Выберите одну из вкладок: **Белый список** или **Чёрный список**.

На странице будут показаны IP-адреса, добавленные в выбранный список, и введённые комментарии к каждому из них.

Чтобы проверить наличие одного или нескольких IP-адресов в списке, используйте фильтр над столбцом **IP-адрес**. В поле этого фильтра можно вводить как конкретный IP-адрес, так и подсеть в формате CIDR. Например, при вводе подсети `10.1.1.0/24` в таблице будут выведены все IP-адреса из списка, входящие в интервал от `10.1.1.1` до `10.1.1.254`.

Добавить IP-адрес в список

1. [Перейдите к нужному списку](#).
2. Нажмите кнопку **Добавить IP-адреса** (для чёрного списка — **Заблокировать IP-адреса**).
3. В появившемся диалоге заполните поля:
 - **IP-адреса** — один или несколько IP-адресов, которые необходимо добавить в список. Если вы добавляете несколько IP-адресов, вводите каждый на новой строке.

- **Комментарий** (необязательно) — текстовое примечание к IP-адресу. Это поле можно использовать, чтобы различать IP-адреса, внесённые в список по разным причинам.

Нажмите кнопку **Добавить**.



ПРИМЕЧАНИЕ

Если среди введённых IP-адресов есть такие, которые уже находятся в списке, старые комментарии к ним будут заменены новыми.

Изменить комментарий к IP-адресу в списке

Чтобы изменить комментарий к одному IP-адресу:

1. [Перейдите к нужному списку](#).
2. Найдите нужный IP-адрес и кликните по нему.
3. В появившемся диалоге отредактируйте текст комментария. Нажмите **Сохранить**.

Чтобы изменить комментарии к нескольким IP-адресам одновременно:

1. [Перейдите к нужному списку](#).
2. Поставьте чекбоксы возле нужных IP-адресов. Нажмите кнопку **Установить комментарий**.
3. В появившемся диалоге отредактируйте текст комментария. Нажмите **Сохранить**.

Удалить IP-адрес из списка

Чтобы удалить один IP-адрес:

1. [Перейдите к нужному списку](#).
2. Найдите нужный IP-адрес и кликните по иконке  в соответствующей строчке.

Чтобы удалить несколько IP-адресов одновременно:

1. [Перейдите к нужному списку](#).
2. Поставьте чекбоксы возле нужных IP-адресов. Нажмите кнопку **Удалить**.

Примеры конфигурации

Белый список

БЕЛЫЙ СПИСОК	ЧЕРНЫЙ СПИСОК														
Список доверенных IP-адресов, которым разрешен доступ вне зависимости от наличия в запросах признаков атак. Этот белый список наполняется клиентом ДОБАВИТЬ IP-АДРЕСА															
☐	<table><thead><tr><th>IP-адрес</th><th>Комментарий</th></tr></thead><tbody><tr><td colspan="2"> IP-адрес или подсеть </td></tr><tr><td>☐</td><td>203.0.113.1 компьютер в офисе</td></tr><tr><td>☐</td><td>203.0.113.2 компьютер в офисе</td></tr><tr><td>☐</td><td>203.0.113.3 компьютер в офисе</td></tr><tr><td>☐</td><td>233.252.0.70 личное устройство</td></tr><tr><td>☐</td><td>233.252.0.80 личное устройство</td></tr></tbody></table>	IP-адрес	Комментарий	IP-адрес или подсеть		☐	203.0.113.1 компьютер в офисе	☐	203.0.113.2 компьютер в офисе	☐	203.0.113.3 компьютер в офисе	☐	233.252.0.70 личное устройство	☐	233.252.0.80 личное устройство
IP-адрес	Комментарий														
IP-адрес или подсеть															
☐	203.0.113.1 компьютер в офисе														
☐	203.0.113.2 компьютер в офисе														
☐	203.0.113.3 компьютер в офисе														
☐	233.252.0.70 личное устройство														
☐	233.252.0.80 личное устройство														

Чёрный список

БЕЛЫЙ СПИСОК	ЧЕРНЫЙ СПИСОК								
	Чтобы заблокировать входящие запросы с IP-адресов, добавьте их в чёрный список. Этот чёрный список наполняется клиентом ЗАБЛОКИРОВАТЬ IP-АДРЕСА								
☐	<table><thead><tr><th>IP-адрес</th><th>Комментарий</th></tr></thead><tbody><tr><td colspan="2"> IP-адрес или подсеть </td></tr><tr><td>☐</td><td>198.51.100.100 известный бот #1</td></tr><tr><td>☐</td><td>198.51.100.200 известный бот #2</td></tr></tbody></table>	IP-адрес	Комментарий	IP-адрес или подсеть		☐	198.51.100.100 известный бот #1	☐	198.51.100.200 известный бот #2
IP-адрес	Комментарий								
IP-адрес или подсеть									
☐	198.51.100.100 известный бот #1								
☐	198.51.100.200 известный бот #2								

Личный кабинет: Туннели



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Туннели» личного кабинета вы можете управлять настройками, связанными [подключением к Curator через туннель](#).

Посмотреть список туннелей

Чтобы посмотреть список туннелей, настроенных для домена:

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **Туннели**.

Туннели будут отображены в виде таблицы со следующими столбцами:

- **Туннель**

Режим работы туннеля (*IPIP* или *GRE*) и его уникальный числовой идентификатор в Curator.

Если для домена [не включён автоматический выбор туннеля](#) и данный туннель является активным, то в этом столбце также отображается отметка «**Активный**».

- **Внешние IP-адреса**

Реально существующие адреса, по которым endpoints доступны в интернете.

- **Внутренние IP-адреса**

Адреса, назначенные endpoints внутри виртуальной сети.

Добавить туннель

1. Перейдите к [списку туннелей](#) и нажмите кнопку **Добавить туннель**.
2. В появившемся диалоге укажите:
 - **Режим** — режим работы туннеля: *IPIP* или *GRE*,

- **Внешний IP-адрес** — реальный адрес с вашей стороны, который будет отправлять и принимать пакеты.

Нажмите кнопку **Создать**.

Редактировать туннель

1. Перейдите к [списку туннелей](#).
2. Наведите курсор на строку с нужным туннелем и возле его идентификатора нажмите ссылку **Редактировать**.
3. В появившемся диалоге отредактируйте поля:
 - **Режим** — режим работы туннеля: *IPIP* или *GRE*,
 - **Внешний IP-адрес** — реальный адрес с вашей стороны, который будет отправлять и принимать пакеты.

Нажмите кнопку **Сохранить**.

Выбрать активный туннель

Выбор активного туннеля доступен только, если для домена [не включён автоматический выбор туннеля](#).

1. Перейдите к [списку туннелей](#).
2. Наведите курсор на строку с нужным туннелем и возле его идентификатора нажмите ссылку **Сделать активным**.
3. В появившемся диалоге нажмите **Подтвердить**.

Удалить туннель

1. Перейдите к [списку туннелей](#).
2. Наведите курсор на строку с нужным туннелем и возле его идентификатора нажмите ссылку **Удалить**.
3. В появившемся диалоге нажмите **Удалить**, чтобы подтвердить операцию.

Настроить автоматический выбор туннеля

По умолчанию Curator направляет трафик только в [активный туннель](#), но вы можете включить автоматическое переключение туннелей. В этом случае каждый [центр очистки данных](#) будет

производить периодические проверки работоспособности активного туннеля и, если проверка завершится неудачей, переключаться на следующий туннель из списка.

Чтобы включить автоматический выбор туннеля или изменить настройки проверки:

1. Перейдите к [списку туннелей](#).
2. Раскройте блок **Балансировка** и нажмите кнопку **Редактировать**.
3. Активируйте переключатель **Включена**.
4. Установите параметры проверки:
 - **Тип проверки** — способ, которым центр очистки данных будет отправлять запрос на IP-адрес туннеля: *Ping* или *HTTP*.
 - **Таймаут** — количество миллисекунд, в течение которых будет ожидаться ответ. Отсутствие ответа в течение этого периода считается ошибкой.
 - **Количество попыток** — сколько последних проверок используются для анализа работоспособности туннеля.
 - **Успешные попытки** — минимальное количество успешных попыток из числа последнего **Количества попыток**, при котором туннель считается работающим корректно.

При выборе типа проверки *HTTP* необходимо также задать дополнительные параметры:

- **Хостнейм** — значение для заголовка `Host`.
- **Путь** — путь, к которому будет делаться HTTP-запрос.
- **Использовать HTTPS** — если включено, то вместо HTTP будет использоваться протокол HTTPS.

5. Нажмите **Сохранить**.

Чтобы отключить автоматический выбор туннеля:

1. Перейдите к [списку туннелей](#).
2. Раскройте блок **Балансировка** и нажмите кнопку **Редактировать**.
3. Деактивируйте переключатель **Включена**.
4. Нажмите **Сохранить**.

Пример конфигурации

ⓘ Балансировка HTTP 172.16.133.165/healthcheck (example.com) Попытки: 2 из 3 Таймаут: 3000мс ▼				
+ ДОБАВИТЬ ТУННЕЛЬ				
Туннель	Внешние IP-адреса		Внутренние IP-адреса	
	Клиент	Qrator	Клиент	Qrator
IPIP (ID 800)	198.51.100.101	178.248.233.165	172.16.133.165	172.16.233.165
IPIP (ID 796)	198.51.100.102	178.248.233.165	172.16.133.165	172.16.233.165
GRE (ID 804)	198.51.100.103	178.248.233.165	172.16.133.165	172.16.233.165

В данном примере настроены три туннеля: два по протоколу IPIP и один по протоколу GRE. Они имеют разные внешние IP-адреса, но используют один и тот же внутренний IP-адрес 172.16.133.165, назначенный им Curator. Для взаимодействия с Curator им следует использовать внешний IP-адрес 178.248.233.165 («Curator IP») и внутренний IP-адрес 172.16.233.165.

Клиент предпочёл настроить [автоматический выбор туннеля](#), что отображено в блоке **Балансировка**. Чтобы проверить работоспособность каждого из туннелей, центр очистки данных Curator делает через них HTTP-запрос `example.com/healthcheck`, используя внутренний IP-адрес 172.16.133.165. Центр очистки данных ожидает получить успешный ответ в течение 3 секунд. Если две из трёх таких проверок подряд завершились неудачей, центр очистки данных переключается на другой туннель.

Личный кабинет: Настройки фильтров

В разделе «Настройки фильтров» личного кабинета Curator вы можете настроить фильтрацию запросов для текущего [домена](#) или [сервиса](#). Фильтрация может выполняться по [HTTP-заголовкам](#), по [странам-источникам запросов](#) или по [пользовательским правилам](#).

Фильтр по заголовкам

Фильтры по заголовкам позволяют автоматически формировать динамические чёрный и белый списки IP-адресов посетителей на основании HTTP-заголовков [User-Agent](#) и [Referer](#). Такие динамические списки определяют, как сеть Curator будет обрабатывать последующие запросы от тех же IP-адресов, даже если эти адреса не указаны вручную в разделе [Списки IP](#).

Каждое правило проверяется независимо от остальных. Если выполнено хотя бы одно из правил для белого списка, то запросы этого пользователя считаются легитимными. Если выполнено хотя бы одно из правил для чёрного списка, то все запросы после текущего считаются нелегитимными. Остальные случаи обрабатываются сетью Curator в обычном порядке.

Правила для белого списка имеют приоритет над правилами для чёрного списка.

Добавить правило

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Настройки фильтров**.
3. Рядом с названием секции **HTTP-заголовки** поставьте чекбокс, если он ещё не поставлен.
4. Нажмите ссылку **Добавить правило** рядом с нужным списком правил.
5. Заполните появившиеся поля:
 - **Заголовок** для проверки: [User-Agent](#) или [Referer](#).
 - Способ проверки:
 - **=** (знак «равно») — значение заголовка должно строго совпадать со строкой, введённой в текстовое поле.
 - **Содержит** — значение заголовка должно содержать строку, введённую в текстовое поле.
 - **Пуст** — заголовок должен отсутствовать.
 - Строка, используемая для проверки.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Удалить правило

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
 2. Выберите пункт меню **Настройки фильтров**.
 3. В секции **HTTP-заголовки** найдите правило, которое нужно удалить, и нажмите  рядом с этим правилом.
 4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.
- Изменения будут применены в течение нескольких минут.

Отключить фильтр по заголовкам

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
 2. Выберите пункт меню **Настройки фильтров**.
 3. Рядом с названием секции **HTTP-заголовки** снимите чекбокс.
 4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.
- Изменения будут применены в течение нескольких минут.

Фильтр по странам

С помощью этого фильтра вы можете ограничить доступ к ресурсу посетителям из определённых стран. Страна-источник запроса определяется по IP-адресу с помощью базы данных [MaxMind GeoIP](#).

Обратите внимание, что фильтр по странам игнорируется, когда IP-адрес пользователя находится в [белом или чёрном списке IP-адресов](#).

Включить фильтр по странам

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Настройки фильтров**.
3. Рядом с названием секции **Гео-фильтры** поставьте чекбокс, если он ещё не поставлен.
4. В выпадающем списке выберите подходящий режим ввода списка стран:
 - **Разрешить запросы** только из определённых стран.
 - **Отклонить запросы** из определённых стран.

В обоих случаях первый запрос от пользователя будет считаться легитимным, но после него IP-адрес будет внесён в чёрный список, если не соответствует условию. Если используется обратный HTTPS-прокси без раскрытия ключей, то IP-адрес будет внесён в чёрный список после [получения логов](#) первого запроса, что может вызвать дополнительную задержку.

5. Отредактируйте список стран. Страны в списке представлены кодами согласно стандарту ISO 3166, например, для России используется код «RU».

- Чтобы добавить страну в список, кликните по её названию в выпадающем списке. Для поиска нужной страны начните вводить в текстовое поле часть её названия или её код.
- Чтобы удалить страну из списка, кликните по крестику рядом с её кодом.

6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Отключить фильтр по странам

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.

2. Выберите пункт меню **Настройки фильтров**.

3. Рядом с названием секции **Гео-фильтры** снимите чекбокс.

4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Пользовательские правила

В секции **Пользовательские правила** можно настроить условия для внесения IP-адресов в чёрный или белый список на основе большого количества свойств запросов и ответов (см. список ниже). Также можно объединять эти условия в более сложные правила с помощью логических операций **AND**, **OR** и **NOT**.

Условия проверяются во время пересылки ответа апстрима пользователю. Если запрос и ответ соответствуют условиям, то к последующим запросам с того же IP-адреса будет применено действие, выбранное для правила.

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.

2. Выберите пункт меню **Настройки фильтров**.

3. Рядом с названием секции **Пользовательские правила** поставьте чекбокс, если он ещё не поставлен.

4. Задайте список правил.

Чтобы добавить правило, нажмите **Добавить правило** внизу страницы. Чтобы удалить правило, нажмите  рядом с правилом.

5. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Доступные действия для правил:

- **Whitelist** — отправить ответ на текущий запрос, проигнорировав другие фильтры и чёрный список.
- **Blacklist** — отправить ответ на текущий запрос, но добавить IP-адрес в чёрный список для будущих запросов.
- **RateLimit** — ограничить частоту запросов, соответствующих правилу, согласно алгоритму [Leaky bucket](#). При выборе этого действия можно указать значения **Rate** и **Burst** для алгоритма.

Доступные типы условий:

- группы для вложенных условий:
 - **AND** — условие выполняется, если выполнены все вложенные условия.
 - **OR** — условие выполняется, если выполнено хотя бы одно из вложенных условий.
 - **NOT** — условие выполняется, если не выполнено вложенное условие.
- проверки свойств запроса:
 - **Method** — HTTP-метод запроса.
 - **Path** — путь, к которому делается запрос.
 - **Query** — строка GET-аргументов из запроса.
 - **Request Uri** — полный URI запроса. Включает название протокола, **Host**, **Path** и **Query**.
 - **Host** — хост, к которому делается запрос.
 - **Header** — значение произвольного HTTP-заголовка из запроса. Имя заголовка вводится в первом поле.
 - **Cookie** — значение произвольной cookie из запроса. Имя cookie вводится в первом поле.
 - **User Agent** — значение HTTP-заголовка [User-Agent](#) из запроса.
 - **Referer** — значение HTTP-заголовка [Referer](#) из запроса.
 - **Content Length** — значение HTTP-заголовка [Content-Length](#) из запроса.
 - **Geo** — страна-источник запроса. В выпадающем списке можно выбрать несколько стран одновременно. Страна-источник запроса определяется по IP-адресу с помощью базы данных [MaxMind GeoIP](#).
- проверки свойств ответа:
 - **Status** — HTTP-код ответа.
 - **Duration** — время ожидания ответа от апстрима в миллисекундах.
 - **Response Header** — значение HTTP-заголовка из ответа. Поддерживаются только заголовки [Location](#) и [Content-Type](#). Нужный заголовок выбирается в первом поле.

Для разных свойств можно выбрать разные операции. Например, для всех строковых свойств доступны операции **!=** (проверка точного совпадения), **startsWith** (проверка совпадения префикса) и другие. Для числовых свойств доступны операции **>** (строго больше), **>=** (больше или равно) и другие. Для свойств, связанных с HTTP-заголовками и Cookies, доступны операции **exist** и **notExists**, проверяющие наличие заголовка.

Большинство операций требуют параметров: например, строки для сравнения. Все параметры обязательны для заполнения.

Пример конфигурации

The screenshot displays the Curator configuration interface with three main sections:

- HTTP-ЗАГОЛОВКИ (HTTP Headers):**
 - Запрещающие правила (Blocking rules):** A rule is configured where the **Referer** header **СОДЕРЖИТ** (contains) the value **https://example.com/**.
 - Whitelist правила (Whitelist rules):** A rule is configured where the **User-Agent** header **=** (equals) the value **CustomTestTool**.
- ГЕО-ФИЛЬТРЫ (Geo-filters):** The **Разрешить запросы** (Allow requests) filter is set to **только из RU** (only from RU).
- ПОЛЬЗОВАТЕЛЬСКИЕ ПРАВИЛА (User rules):**
 - A rule is **Включено** (Enabled).
 - The **RateLimit** action is configured with a **Rate, rps** (requests per second) of 1 and a **Burst** of 5.
 - The rule logic is defined by the following conditions:
 - AND** (logical AND):
 - USER-AGENT** **notExist** (does not exist).
 - OR** (logical OR):
 - PATH** **!=** (not equal) **/**.
 - DURATION** **>** (greater than) **1000** ms.

В данном примере:

- Клиент обнаружил большое количество автоматизированных запросов, которые содержали подстроку `https://example.com/` в заголовке `Referer`, и принял решение автоматически добавлять в чёрный список все IP-адреса, от которых приходят такие запросы.
- Клиент добавил правило для автоматического добавления в белый список всех IP-адресов, от которых приходят запросы со значением `CustomTestTool` в заголовке `User-Agent`. Например, если он настроит свои инструменты тестирования так, чтобы они использовали этот заголовок, то это предотвратит ложноположительные срабатывания защиты Curator при анализе тестовых запросов.
- Клиент работает только с пользователями из России, поэтому IP-адреса из любых других стран автоматически добавляются в чёрный список.
- Клиент принял решение вносить IP-адреса в чёрный список, если с них поступали запросы к главной странице без заголовка `User-Agent`, обработка которых заняла больше 1 секунды.

Личный кабинет: HTTP-перенаправления



ПРИМЕЧАНИЕ

Этот раздел Личного кабинета доступен только для пользователей с *Технической ролью*.

В этом разделе личного кабинета вы можете управлять правилами, согласно которым **обратный HTTP-прокси** будет перенаправлять часть HTTP-запросов пользователей.

Подробнее см. в разделе [Технологии: HTTP-перенаправления](#).

Посмотреть список правил

Чтобы посмотреть список правил, настроенных для домена:

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **HTTP-перенаправления**.

Правила отображаются в таблице со следующими столбцами:

- **Запрос** — шаблон URL-адресов, для которых применимо данное правило.

Если правило использует конкретный хост, то запрос в этом столбце отображается в формате `<протокол>://<хост>`, например: `http://example.com`.

Если правило должно срабатывать для любого хоста, то вместо хоста отображается значение «ANY», например: `http://ANY`.

- **Перенаправление** — код ответа HTTP, а также URL, на которое осуществляется перенаправление.

Код ответа и URL отображаются на одной строке через пробел, например: `301 http://example.com/`.

Если для некоторых компонентов запроса были включены опции **Передавать как есть** (см. [Добавить правило](#)), то строка будет отображаться со специальными переменными, значения которых будут подставляться при обработке каждого конкретного запроса:

- `$hostname` — хост из запроса пользователя,
- `$path` — путь из запроса пользователя,
- `$args` — GET-аргументы из запроса пользователя.

Например: `301 http://$hostname$path?$args`.

Если перенаправление в рамках данного правила исключено, то в этом столбце будет отображена надпись **Выключено**.

Добавить правило

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **HTTP-перенаправления**.
3. Нажмите кнопку **Добавить**.
4. В секции **Запрос** укажите параметры запросов, для которых будет срабатывать правило.
 - **Схема** — протокол запроса (*HTTP* или *HTTPS*).
 - **Хостнейм** — доменное имя, к которому сделан запрос. Если выбрана опция «FQDN», то в текстовом поле ниже необходимо ввести конкретное доменное имя, на соответствие которому будут проверяться запросы. Если выбрана опция «ANY», то правило не будет зависеть от доменного имени в запросе.
5. В секции **Перенаправление** укажите действия, которые обратный HTTP-прокси должен выполнить над запросом.
 - **Включено** — включить обработку запроса. Если эта опция выключена, то запросы будут отправляться на апстрим без изменений.
 - **Схема** — протокол запроса (*HTTP* или *HTTPS*).
 - **Код ответа** — с каким кодом HTTP-ответа будет выполнено перенаправление пользователя. Вы можете выбрать из следующих кодов:
 - 301 Moved Permanently
 - 302 Found
 - 307 Temporary Redirect
 - 308 Permanent Redirect
 - **Хостнейм** — доменное имя, которое будет использовано в URL для перенаправления.

Чтобы каждый раз использовалось доменное имя из оригинального запроса без изменений, установите опцию **Передавать как есть**.
 - **Путь** — путь, который будет использован в URL перенаправления.

Чтобы каждый раз использовался путь из оригинального запроса без изменений, установите опцию **Передавать как есть**.
 - **Параметры запроса** — использовать ли GET-параметры из оригинального запроса.

Чтобы каждый раз использовались GET-параметры из оригинального запроса без изменений, установите опцию **Передавать как есть**. Если опция не установлена, все GET-параметры будут удаляться из запроса.

6. Нажмите кнопку **Сохранить**.
7. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменить правило

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **HTTP-перенаправления**.
3. Рядом с правилом, которое вы хотите изменить, нажмите ссылку **Редактировать**.
4. Внесите необходимые изменения в правило.

Поля формы редактирования правила идентичны полям в [форме добавления правила](#).

5. Нажмите кнопку **Сохранить**.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить правило

1. В разделе **Домены** личного кабинета выберите нужный домен.
2. Выберите пункт меню **HTTP-перенаправления**.
3. Рядом с правилом, которое вы хотите изменить, нажмите ссылку **Удалить**.
4. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
5. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Пример конфигурации

Запрос	Перенаправление	
http:// ANY	301 https:// \$hostname \$path ? \$args	Редактировать Удалить
http://example.com	301 https://www.example.com \$path ? \$args	Редактировать Удалить
https://example.com	301 https://www.example.com \$path ? \$args	Редактировать Удалить
http://old.example.com	Выключено	Редактировать Удалить

В приведённом примере обратный HTTP-прокси используется для защиты сайта, использующего хост `example.com` и его поддомены. Предполагается, что все разделы сайта, кроме раздела на поддомене `old.example.com`, поддерживают работу по HTTPS.

Обратный HTTP-прокси будет выполнять правила следующим образом:

- При работе по протоколу HTTP:
 - В запросах к `example.com` протокол заменяется на HTTPS, а домен заменяется на `www.example.com` с сохранением пути и аргументов (правило 2).
 - Запросы к `old.example.com` отправляются на апстрим без изменений (правило 4).
 - В других запросах протокол заменяется на HTTPS с сохранением домена, пути и аргументов (правило 1).
- При работе по протоколу HTTPS:
 - В запросах к `example.com` домен заменяется на `www.example.com` с сохранением пути и аргументов (правило 3).
 - Другие запросы отправляются на апстрим без изменений (неявное правило по умолчанию).



ПРИМЕЧАНИЕ

Другие примеры конфигурации перенаправлений для типовых сценариев приведены в разделе [Примеры](#) статьи «Технологии: HTTP-перенаправления».

Личный кабинет: Страницы ошибок



ПРИМЕЧАНИЕ

В конфигурации по умолчанию этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Страницы ошибок» личного кабинета вы можете загрузить собственные страницы, которые обратный HTTP-прокси Curator будет отображать при возникновении ошибок 403 Forbidden, 502 Bad Gateway, 503 Service Unavailable или 504 Gateway Timeout. Все настройки действуют только для текущего домена или сервиса.

Принцип работы

Чтобы обратный HTTP-прокси использовал страницу в качестве страницы ошибки, её следует загрузить в виде файла с расширением `html`.

Для демонстрации одной и той же страницы ошибок для всех типов ошибок, используйте `index.html` в качестве имени файла. Если необходимо демонстрировать уникальные страницы для разных типов ошибок, используйте код ошибки в качестве имени файла, например: `502.html`.

Если требуется демонстрировать локализованные страницы ошибок пользователям, использующим разные языки, в названиях файлов необходимо указать язык, например: `502.en.html`. Язык будет определяться исходя из заголовка `Accept-Language` браузера пользователя, например: `en`, `ru`, `es`.

Если для отображения страниц необходимы дополнительные изображения или другие файлы, вы можете загрузить их в этом же разделе. В качестве путей к файлам в коде страниц ошибок необходимо использовать URL, начинающиеся с `/qerror/`, например: `/qerror/favicon.ico`, `/qerror/images/logo.png`. Ресурсы, расположенные на других URL, могут оказаться недоступны в момент возникновения ошибки.

Возможно использование ресурсов, исполняемых в браузере пользователя (скриптов JavaScript, элементов Flash или Silverlight). Использование ресурсов, исполняемых на сервере, в рамках страниц ошибок невозможно.

Обратите внимание, что загруженные страницы ошибок демонстрируются только в тех случаях, когда обратный HTTP-прокси формирует ошибку самостоятельно (см. [Перенаправление с установкой cookie](#), [Балансировка нагрузки](#)). Ошибки, сформированные на стороне защищаемого сервера, показываются без изменений.

**ПРИМЕР**

Предположим, что ни один из апстримов домена не ответил на запрос, и в соответствии с алгоритмом обработки ошибок необходимо сообщить пользователю об ошибке 504 Gateway Timeout. Также предположим, что в браузере пользователя выбран английский язык.

В этом случае обратный HTTP-прокси переберёт варианты в следующем порядке:

[504.en.html](#), [504.html](#), [index.en.html](#), [index.html](#), страница по умолчанию.

Пользователю будет показана первая найденная страница.

Посмотреть страницы ошибок

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Страницы ошибок**.
3. Нажмите на URL рядом с одним из кодов ошибок.

В новой вкладке браузера откроется страница, которую увидят пользователи при возникновении соответствующей ошибки.

Заменить страницы ошибок

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Страницы ошибок**.
3. Нажмите кнопку **Редактировать**.
4. В появившемся диалоге управления файлами создайте необходимую структуру файлов.

Все страницы должны находиться в корневой папке, и их имена должны соответствовать правилам, описанным в разделе [Принцип работы](#) выше. Если для отображения страниц необходимы дополнительные изображения или другие файлы, вы можете загрузить их в этом же диалоге.

В диалоге управления файлами доступны следующие кнопки:

- **Создать папку** — создать новую папку в текущей папке.
- **Загрузить файлы** — загрузить один или несколько файлов в текущую папку. Файлы для загрузки выбираются с помощью системного диалога.
- **Загрузить архив** — загрузить ZIP-архив и распаковать его в корневую папку. Архив для загрузки выбирается с помощью системного диалога. Поддерживаются только архивы формата ZIP.
- **Скачать всё** — скачать ZIP-архив с полным содержимым корневой папки.

-  **Удалить всё** — удалить всё содержимое корневой папки без возможности восстановления.

Кликните по имени любого файла, чтобы открыть его предпросмотр в новой вкладке, или нажмите кнопку  , чтобы скопировать ссылку для предпросмотра. Обратите внимание, что предпросмотр по этой ссылке доступен только после авторизации в личном кабинете.

Также рядом с каждым файлом доступно меню со следующими пунктами:

-  **Скачать** — скачать выбранный файл.
-  **Удалить** — удалить выбранный файл без возможности восстановления.

Все изменения, сделанные в этом диалоге, сохраняются автоматически и становятся видны пользователям через несколько минут. Чтобы закрыть диалог, нажмите **Применить**.

Пример конфигурации

							
Имя файла	Размер файла	Последнее изменение					
 images		2022-08-07 20:05 					
 502.html 	306.00 байт	2022-08-07 20:05 					
 503.html 	200.00 байт	2022-08-07 20:05 					
 504.html 	201.00 байт	2022-08-07 20:05 					
Начало							
ОТМЕНА		ПРИМЕНИТЬ					

В этом примере загружены три страницы ошибок. Также загружена папка `images` с изображениями, необходимыми для этих страниц.

Личный кабинет: Уведомления (настройка ресурса)



ПРИМЕЧАНИЕ

Эта страница описывает настройки порогов уведомлений для ресурса. О настройке получения уведомлений для конкретной учётной записи пользователя см. [Уведомления \(настройка учётной записи\)](#).

В конфигурации по умолчанию этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Уведомления» личного кабинета настраиваются пороги, при превышении которых клиент получает уведомление по электронной почте. Все настройки действуют только для текущего [домена](#) или [сервиса](#).

Поддерживаются уведомления о следующих показателях:

- **Входящий трафик** — общая полоса входящего трафика (до фильтрации).
- **Исходящий трафик** — общая полоса исходящего трафика.
- **Пропущенный трафик** — полоса входящего трафика, который был пропущен до клиента.
- **Заблокированные IP-адреса** — количество заблокированных IP-адресов, одновременно присутствующих в автоматических чёрных списках Curator.

Уведомление направляется в том случае, если среднее значение какого-то из показателей за последнюю минуту превысило заданный порог.

Включить уведомления или изменить порог уведомлений для показателя

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Уведомления**.
3. Нажмите кнопку **Редактировать**.
4. Найдите нужный вам показатель и отредактируйте числовое значение порога, введя его с клавиатуры или используя ползунок.
 - В категориях **Входящий**, **Исходящий** и **Пропущенный трафик** единицей измерения по умолчанию являются Мбит/с. Для ввода значений, превышающих 999 Мбит/с, необходимо

использовать единицу измерения Гбит/с. Для переключения между Мбит/с и Гбит/с кликните по обозначению единицы измерения.

- В категории **Заблокированные IP-адреса** единицей измерения является один IP-адрес.

5. Нажмите кнопку **Сохранить**.

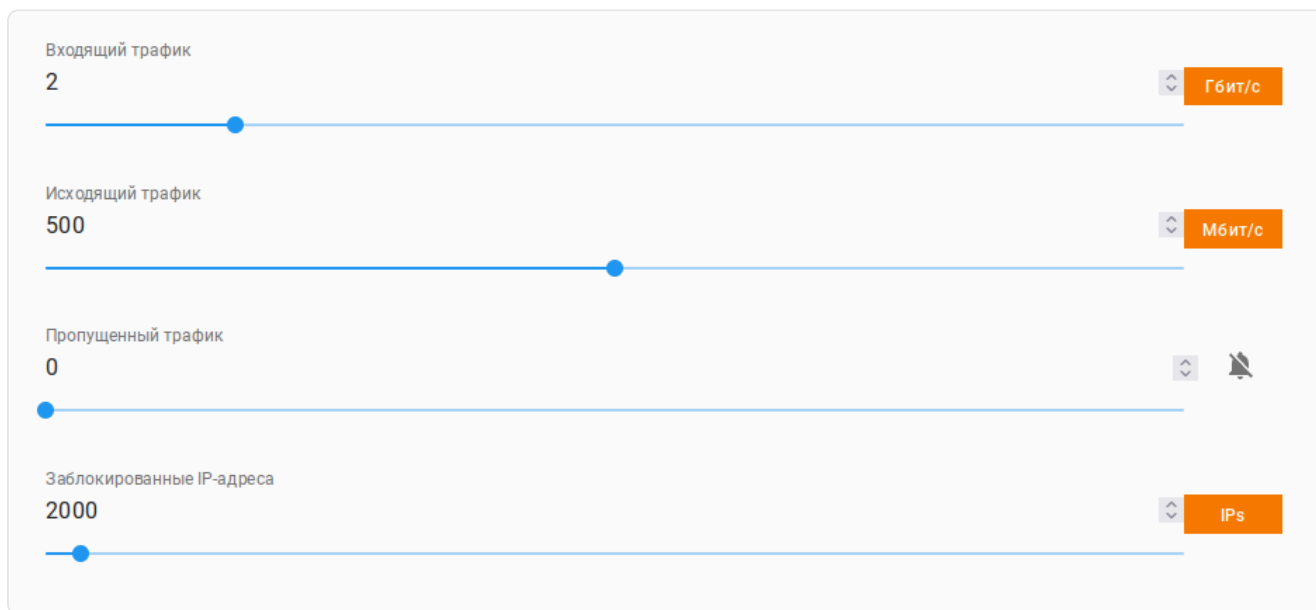
Отключить уведомления для категории

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Уведомления**.
3. Нажмите кнопку **Редактировать**.
4. Найдите нужный вам показатель и укажите для него значение порога 0.

Рядом с категорией должно появиться изображение .

5. Нажмите кнопку **Сохранить**.

Пример конфигурации



Категория	Значение	Единица измерения	Уведомление
Входящий трафик	2	Гбит/с	Нет
Исходящий трафик	500	Мбит/с	Нет
Пропущенный трафик	0		Да
Заблокированные IP-адреса	2000	IPs	Нет

В данном примере клиент будет получать уведомление в каждом из следующих случаев:

- средняя полоса трафика за последнюю минуту составила 2 Гбит/с,
- средняя полоса исходящего трафика за последнюю минуту составила 500 Мбит/с,
- средний размер автоматического чёрного списка за последнюю минуту составил 2000 IP-адресов.

Уведомления о полосе трафика, пропущенного до сети клиента, в данном примере отключены.

Личный кабинет: Bot protection → Сводка



ПРИМЕЧАНИЕ

В конфигурации по умолчанию этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*.

В разделе «Bot protection → Сводка» личного кабинета Curator отображаются данные о заблокированных запросах к текущему домену или сервису.

Раздел состоит из нескольких виджетов:

- график событий,
- виджет с ключевыми показателями,
- виджеты с данными о заблокированных запросах.

Вы можете загружать данные за разные периоды. По умолчанию данные на странице обновляются автоматически. Загруженные данные можно экспортировать в виде изображения или таблицы.

Просмотр данных

График событий

В верхней части страницы находится график, на котором отображаются события, связанные с защитой от ботов. Разные наборы данных на графике представляют разные типы событий. Вы можете скрыть набор данных с графика, кликнув по его обозначению в легенде.



ПРИМЕЧАНИЕ

События, соответствующие коду 401 Unauthorized, регистрируются только после того, как пользователь сделал следующий запрос. Например, событие **Проверка завершена неудачно** (401 Unauthorized) регистрируется одновременно с соответствующим событием **Заблокирован за провал проверки** (403 Forbidden). Из-за этого данные о событиях, соответствующих коду 401 Unauthorized, могут появляться на графике с небольшой задержкой.

Ниже приведён список типов событий, отображаемых на графике. В скобках указаны коды HTTP-ответов, отправляемых пользователям.

- **Игнорировал проверку** (401 Unauthorized)

Пользователь получил страницу с кодом проверки на JavaScript, но вместо его выполнения сделал другой запрос.

Это может говорить о том, что пользователь является ботом или использует браузер без возможности исполнения кода на JavaScript.

- **Проверка выявила бота** (401 Unauthorized)
Браузерный бот заблокирован (403 Forbidden)

Пользователь получил страницу с кодом проверки на JavaScript, прислал цифровой отпечаток окружения и был определён как бот.

- **Проверка завершена неудачно** (401 Unauthorized)
Заблокирован за провал проверки (403 Forbidden)

Пользователь получил страницу с кодом проверки на JavaScript, прислал цифровой отпечаток окружения и был определён как легитимный пользователь. Ему была выдана трекинговая cookie. После этого он обратился по адресу, требующему трекинговую cookie, но не предоставил её.

Причиной может быть неожиданный обрыв связи на стороне пользователя при получении трекинговой cookie после проверки. Чаще всего в такой ситуации пользователь может вернуться на страницу с проверкой и успешно пройти проверку заново.

- **Неверные куки/подпись** (403 Forbidden)

Пользователь обратился по адресу, требующему трекинговую cookie или подпись, но не предоставил их.

Это может говорить о том, что пользователь является ботом, либо о том, что пользователь не посещал страницу с проверкой. Если вы используете [защиту мобильных API с использованием хэша](#), то эта ошибка может также возникать, если ваше мобильное приложение отправляет запросы к API с отсутствующей или некорректной подписью заголовков.

Ключевые показатели

На этот виджет вынесена краткая информация о количестве запросов, обработанных за выбранный период.

- **Total blocked bot requests** — общее количество нелегитимных запросов.
- **Requests failed to validate** — количество нелегитимных запросов, при которых пользователь не выполнил код проверки на JavaScript, выданный ему перед посещением страницы (действие «Принять и Выдать Проверку» в [правилах обработки запросов](#)).
- **Requests failed to present a cookie** — количество нелегитимных запросов, при которых пользователь не предоставил трекинговую cookie на странице, которая требует её наличия (действие «Принять Только с Куки» в [правилах обработки запросов](#)).
- **Bad fingerprint requests** — количество нелегитимных запросов, при которых пользователь выполнил код проверки на JavaScript, выданный ему перед посещением страницы (действие «Принять и Выдать Проверку» в [правилах обработки запросов](#)), и был определён как бот.

Каждый показатель, кроме **Total blocked bot requests**, отображается как абсолютное значение и как доля от общего числа запросов. Обратите внимание, что некоторые запросы могут попадать более чем в одну категорию, поэтому сумма трёх значений может превышать значение **Total blocked bot requests** (100%).

Данные о заблокированных запросах

На эти виджеты вынесена информация о наиболее часто встречающихся значениях некоторых параметров запросов, заблокированных за выбранный период. Для каждого из значений указано количество запросов с таким значением.

- **Top 10 countries** — страны, из которых совершались запросы. Данные отображаются в виде столбчатой диаграммы. Чтобы увидеть количество запросов из страны, наведите курсор на соответствующий столбец. Страна-источник запроса определяется по IP-адресу с помощью базы данных [MaxMind GeoIP](#).
- **Top 10 IP addresses** — IP-адреса, с которых совершались запросы.
- **Top 10 URIs** — пути URI, к которым совершались запросы.
- **Top 10 referer** — значения HTTP-заголовка [Referer](#) из запросов.
- **Top 10 User agents** — значения HTTP-заголовка [User-Agent](#) из запросов.



СОВЕТ

Чтобы посмотреть более подробную информацию обо всех заблокированных запросах за выбранный период, воспользуйтесь [экспортом данных](#).

Выбор периода

Все виджеты в разделе отображают данные за определённый период (по умолчанию **1 день**). Вы можете изменить этот период одним из двух способов.

- Зажмите левую кнопку мыши в начале интересующего вас участка [графика событий](#) и, не отпуская кнопку, потяните до конца участка. Масштаб графика автоматически поменяется так, чтобы включать данные только из выбранного участка. Такое увеличение масштаба можно производить последовательно несколько раз.

При каждом обновлении графика все остальные виджеты в разделе автоматически обновляются и отображают данные за соответствующий период.

Чтобы вернуться к предыдущему периоду, нажмите кнопку . Чтобы вернуться к периоду по умолчанию, нажмите кнопку **Сбросить зум**.

- Выберите один из предустановленных периодов в выпадающем списке в верхней части страницы. Необходимые данные автоматически подгрузятся и отобразятся на графике и остальных виджетах.

Обновление данных

По умолчанию все данные в этом разделе личного кабинета автоматически обновляются без перезагрузки страницы каждые **2 минуты**. Чтобы изменить этот интервал, раскройте выпадающий список рядом с кнопкой ↻ в верхней части страницы и выберите нужный интервал. Чтобы отключить автообновление полностью, в выпадающем списке выберите опцию «Off».

Чтобы обновить данные принудительно, нажмите кнопку ↻.

Экспорт

Экспорт графика

Чтобы сохранить [график событий](#) за выбранный период, в верхней части страницы выберите пункт меню **Экспорт** → **Экспорт графика (.png)**. Изображение будет скачано в том же размере, в котором оно было отображено в браузере на момент сохранения.

Экспорт запросов

Чтобы скачать полные данные обо всех заблокированных запросах за выбранный период, в верхней части страницы выберите пункт меню **Экспорт** → **Экспорт запросов (.csv.gz)**.

Личный кабинет: Bot protection → Локации



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Bot protection → Локации» личного кабинета Curator вы можете включить, отключить и изменить правила обработки, применяемые к запросам на текущем [домене](#) или [сервисе](#).

Каждое правило состоит из условия, согласно которому запрос проверяется, и действия, которое выполняется при соблюдении условия. К одному запросу применяется не более одного правила.

Когда на сервер Curator поступает пользовательский запрос, сервер проверяет его на соответствие правилам в том порядке, в котором они сохранены в личном кабинете, начиная с самого верхнего. При первой успешной проверке выполняется действие, указанное в соответствующем правиле. Если проверки для всех правил закончились неудачно, то применяется неявное правило по умолчанию с действием **Не реагировать**.

Добавить группу хостов

Если ваш домен или сервис использует большое количество хостов, может быть удобно объединить некоторые из них в *группы хостов*. [Правила обработки запросов](#) могут ссылаться на группы хостов вместо отдельных хостов, что позволяет упростить структуру правил в целом.

Один хост может входить в несколько групп одновременно.



ПРИМЕР

Предположим, что часть контента вашего сайта расположена на поддоменах, указывающих на используемый язык: [ru.example.com](#), [en.example.com](#), [es.example.com](#) и т.д. В этом случае вы можете создать группу хостов с названием «Языковые версии сайта», включающую в себя эти поддомены, и ссылаться на неё в правилах.

Если впоследствии вы добавите на сайт поддержку нового языка и новый поддомен, к которому должны применяться такие же правила, просто добавьте поддомен в эту группу.

Чтобы добавить или изменить группу хостов:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection → Локации**.

3. В секции **Хостгруппы** нажмите ссылку **Добавить хостгруппу**.
4. В открывшемся диалоге заполните поля:
 - **Название** — уникальное название группы.
 - **Хостнеймы** — перечень хостов в группе, по одному хосту на строку.
5. Нажмите кнопку **Сохранить**.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.
Изменения будут применены в течение 5–7 минут.

Изменить группу хостов

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Локации**.
3. В секции **Хостгруппы** нажмите ссылку **Редактировать** рядом с названием группы, которую нужно изменить.
4. В открывшемся диалоге заполните поля:
 - **Название** — уникальное название группы.
 - **Хостнеймы** — перечень хостов в группе, по одному хосту на строку.
5. Нажмите кнопку **Сохранить**.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.
Изменения будут применены в течение 5–7 минут.

Удалить группу хостов

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Локации**.
3. Убедитесь, что группа хостов, которую нужно удалить, не используется в правилах обработки запросов.
При необходимости [измените](#) или [удалите](#) правила, ссылающиеся на эту группу хостов.
4. В секции **Хостгруппы** нажмите ссылку **Удалить** рядом с названием группы, которую нужно изменить.
5. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Добавить или изменить правило обработки запросов

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Локации**.
3. Найдите правило, которое нужно изменить, или место, в которое нужно добавить новое правило.
 - Чтобы изменить существующее правило, нажмите рядом с ним иконку .
 - Чтобы добавить новое правило, нажмите ссылку **Добавить правило** в нужном месте. Например, чтобы новое правило было самым приоритетным, нажмите ссылку над первым существующим правилом.

Откроется диалог с настройками правила.

4. В поле **Название** укажите название для правила. (Этот шаг можно пропустить.)
5. В секции **IF** опишите условие, при выполнении которого правило должно срабатывать. Условие состоит из трёх частей, проверяющих разные компоненты HTTP-запроса. Для каждой из частей независимо выбирается способ проверки.
 - **Host** — хост, к которому делается запрос. Например: `example.com`.

Возможные способы проверки хоста:

- **Host group** — хост должен принадлежать к **группе хостов**, выбранной из выпадающего списка.
- **Any value** — хост может быть любым значением.
- **Equal** — хост должен строго совпадать со строкой, введённой в текстовое поле.
- **Starts with** — хост должен начинаться со строки, введённой в текстовое поле.
- **Ends with** — хост должен заканчиваться строкой, введённой в текстовое поле.
- **Contains** — хост должен содержать строку, введённую в текстовое поле.
- **Method** — HTTP-метод запроса. Например: `GET`.

Возможные способы проверки метода:

- **Any value** — метод может быть любым значением.
- **Equal** — метод должен строго совпадать с методом, выбранным из выпадающего списка.
- **Path** — путь, к которому делается запрос. Например: `/`.

Возможные способы проверки пути:

- **Any value** — путь может быть любым значением.
- **Equal** — путь должен строго совпадать со строкой, введённой в текстовое поле.
- **Starts with** — путь должен начинаться со строки, введённой в текстовое поле.

- **Ends with** — путь должен заканчиваться строкой, введённой в текстовое поле.
- **Contains** — путь должен содержать строку, введённую в текстовое поле.

При выборе способов проверки **Equal**, **Starts with**, **Ends with** или **Contains** появляется дополнительное всплывающее окно с чекбоксом **One of**. Отметьте этот чекбокс, чтобы указать сразу несколько возможных значений, с которыми будет сравниваться компонент из запроса. Оставьте чекбокс неотмеченным и нажмите клавишу **Esc**, чтобы указать только одно значение.

6. В секции **THEN** выберите, что должно происходить при срабатывании правила.

- **Принять и Выдать Проверку** — пользователь получит содержимое сайта только при наличии корректной cookie. Если cookie отсутствует или неверна, пользователь получит страницу с кодом проверки на JavaScript. После успешного выполнения проверки пользователь получит cookie, а страница будет автоматически перезагружена.
- **Принять Только с Куки** — пользователь получит содержимое сайта только при наличии корректной cookie. Если cookie отсутствует или неверна, пользователь получит ответ со статусом 403 Forbidden.
- **Не реагировать** — пользователь получит содержимое сайта без дополнительных проверок.
- **CDN Origin** — пользователю будет выдана специальная cookie для CDN. Используйте эту опцию для локаций, на которых находится статический контент, кешируемый с помощью сторонних CDN-сервисов.

Обратите внимание, что действие **Принять и Выдать Проверку** предназначено только для обработки запросов GET и может работать некорректно с другими видами запросов. Остальные действия работают с любыми видами запросов.

7. Нажмите кнопку **Сохранить**.

8. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Изменить порядок правил

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Локации**.
3. Зажмите левую кнопку мыши на иконке  рядом с правилом, которое нужно переместить, и, не отпуская, потяните в нужное место списка.

При необходимости повторите это для других правил, которые нужно переместить.

4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Удалить правило

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Локации**.
3. Рядом с правилом, которое нужно удалить, нажмите иконку .
4. Подтвердите действие, нажав **Удалить правило** в появившемся диалоге.
5. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Пример конфигурации



The screenshot displays the 'Локации' (Locations) configuration page for Bot protection. At the top, a toggle switch is set to 'Включено' (On). Below this, there are sections for 'Хостгруппы' (Host groups) and 'Региональные версии' (Regional versions), each with a list of domains and links to 'Редактировать' (Edit) or 'Удалить' (Delete). The main section is 'Правила локаций' (Location rules), which contains four rules:

- Rule 1:** 'Эндпоинт для получения cookie перед работой с бэкендом' (Endpoint for getting cookie before working with backend).
 - IF: HOST GROUP 'Бэкенд для веб-приложения' (Backend for web application).
 - METHOD: GET.
 - PATH: /get-cookie.
 - ACTION: 'Принять и Выдать Проверку' (Accept and Issue Check).
- Rule 2:** 'Работа с бэкендом при наличии cookie' (Working with backend when cookie is present).
 - IF: HOST GROUP 'Бэкенд для веб-приложения' (Backend for web application).
 - METHOD: ANY VALUE.
 - PATH: ANY VALUE.
 - ACTION: 'Принять Только с Кукки' (Accept Only with Cookies).
- Rule 3:** 'Файлы, доступные всем' (Files accessible to all).
 - IF: REGIONAL VERSIONS 'Региональные версии' (Regional versions).
 - METHOD: GET.
 - PATH: /manifest.json, /robots.txt.
 - ACTION: 'Не реагировать' (Do not react).
- Rule 4:** 'Статический контент' (Static content).
 - IF: HOST 'static.example.com'.
 - METHOD: GET.
 - PATH: ANY VALUE.
 - ACTION: 'CDN origin'.

В данном примере клиент настроил защиту одностраничного веб-приложения. Веб-приложение работает на хостах из группы «Региональные версии», и взаимодействует с бэкендом, работающим на хостах из группы «Бэкенд веб-приложения».

Веб-интерфейс доступен пользователям только после прохождения проверки (правило 2). Исключение сделано для нескольких файлов, которые могут запрашиваться внешними сервисами и приложениями (правило 1).

Бэкенд доступен только после того, как браузер прошёл проверку для веб-интерфейса и получил трекингтовую cookie (правило 3).

Статический контент отдаётся со специальной cookie для внешних CDN-провайдеров (правило 4).

Личный кабинет: Bot protection → Посетители



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Bot protection → Посетители» личного кабинета Curator собраны настройки, влияющие на применимость правил обработки трафика в рамках защиты от ботов.

С помощью настроек в этом разделе вы можете:

- [включить](#) и [отключить](#) защиту от ботов,
- настроить принудительную проверку запросов [по IP-адресам](#),
- настроить исключения из проверки запросов [по заголовкам](#), [по странам](#) и [по IP-адресам](#),
- настроить частичное включение услуги с [A/B распределением](#) проверок.

Включить защиту от ботов

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection → Посетители**.
3. Отметьте опцию **Включено**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Отключить защиту от ботов

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection → Посетители**.
3. Отключите опцию **Включено**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Защита от ботов будет отключена в течение 5–7 минут.

Настроить принудительные проверки по IP-адресам

Данная настройка позволяет указать перечень IP-адресов, запросы с которых будут проверяться на соответствие правилам всегда, вне зависимости от настройки [А/В Распределение проверок](#). Это полезно для тестирования правил защиты с ограниченного количества устройств перед полным включением её для всех пользователей. Подробнее см. описание рекомендуемого порядка подключения услуги в статье [Подключение: Защита от ботов](#).

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Посетители**.
3. В секции **Форс Проверок для IP** нажмите ссылку **Редактировать**.
4. В появившемся диалоге введите список IP-адресов, для которых нужно включить принудительные проверки. Разделяйте IP-адреса переносами строк.
5. Нажмите кнопку **Сохранить**.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Добавить или изменить исключение по заголовку

Если данная настройка задана, то защита от ботов будет считать легитимными все запросы с определёнными HTTP-заголовками.



ПРИМЕР

Предположим, что вы используете собственного бота, чтобы делать запросы в рамках функционального или нагрузочного тестирования. Настройте бота таким образом, чтобы он добавлял к каждому запросу HTTP-заголовок с определённым именем и значением. Внесите эти имя и значение в исключения, как описано ниже. После этого бот сможет получать содержимое от апстрима без прохождения проверки.

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Посетители**.
3. В секции **Исключения по Заголовкам** добавьте новое исключение или выберите исключение, которое нужно изменить.
 - Чтобы добавить новое исключение, нажмите ссылку **Добавить исключение**.
 - Чтобы изменить существующее исключение, нажмите рядом с ним иконку .

4. В появившемся диалоге опишите условие, при выполнении которого пользователь будет считаться легитимным. Для этого введите название заголовка, способ его проверки и строку, используемую для проверки.

В появившемся диалоге заполните следующие поля:

- **Header name** — имя заголовка для проверки.
- Способ проверки:
 - **Contains** — значение заголовка должно содержать строку, введённую в текстовое поле.
 - **Ends with** — значение заголовка должно заканчиваться строкой, введённой в текстовое поле.
 - **Equal** — значение заголовка должно строго совпадать со строкой, введённой в текстовое поле.
 - **Starts with** — значение заголовка должно начинаться со строки, введённой в текстовое поле.

При выборе способа проверки появляется дополнительное всплывающее окно с чекбоксом **One of**. Отметьте этот чекбокс, чтобы указать сразу несколько возможных значений, с которыми будет сравниваться компонент из запроса. Оставьте чекбокс неотмеченным и нажмите клавишу **Esc**, чтобы указать только одно значение.

- Значение, используемое для проверки.

Если при выборе способа проверки был отмечен чекбокс **One of**, то вы можете ввести в текстовое поле несколько значений, разделяя их переносами строк.

**ВАЖНО**

Не добавляйте в исключения значения заголовков, которые создатели ботов могут найти в документации или других публичных источниках. Рекомендуется использовать сгенерированные случайные строки, известные только вашей команде.

5. Нажмите кнопку **Сохранить**.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.
- Изменения будут применены в течение 5–7 минут.

Удалить исключение по заголовку

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Посетители**.
3. В секции **Исключения по Заголовкам** нажмите иконку  рядом с исключением, которое нужно удалить.

4. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
5. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Настроить исключения стран

Если данная настройка задана, то защита от ботов будет считать легитимными все запросы из определённых стран. Страна-источник запроса определяется по IP-адресу с помощью базы данных [MaxMind GeoIP](#).

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Посетители**.
3. В секции **Исключения Стран** отредактируйте список стран. Страны в списке представлены кодами согласно стандарту [ISO 3166](#), например, для России используется код «RU».
 - Чтобы добавить страну в список, кликните по её коду в выпадающем списке. Для поиска нужной страны вы можете ввести одну или обе буквы кода в текстовое поле.
 - Чтобы удалить страну из списка, кликните по крестику рядом с её кодом.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Настроить исключения IP и подсетей

Если данная настройка задана, то защита от ботов будет считать легитимными все запросы с определённых IP-адресов. Например, таким образом вы можете разрешить работу автоматизированных инструментов из сетей вашей компании или её партнёров.

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Посетители**.
3. В секции **Исключения IP и Подсетей** нажмите ссылку **Редактировать**.
4. В появившемся диалоге введите список IP-адресов и подсетей в нотации CIDR, разделяя их переносами строк.
5. Нажмите кнопку **Сохранить**.
6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Настроить A/B распределение проверок

Данная настройка определяет, для какой доли пользователей будет активирована защита от ботов. Это полезно для поэтапного подключения услуги защиты от ботов, см. [соответствующий шаг в инструкции по подключению](#).



ПРИМЕЧАНИЕ

Запрос от пользователя будет проанализирован защитой от ботов, если:

- активирована опция «Включить» в разделе **Bot protection** → **Локации**,
- активирована опция «Включить» в разделе **Bot protection** → **Посетители**,
- выполняется любое из трёх условий:
 - **A/B распределение проверок** установлено в 100%,
 - **A/B распределение проверок** установлено в некоторое значение, и IP-адрес пользователя попал в выборку для проверки,
 - IP-адрес пользователя находится в [списке для принудительных проверок](#).

Чтобы изменить A/B распределение проверок:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Посетители**.
3. В секции **A/B Распределение проверок** передвиньте ползунок в нужное значение от 0% до 100%.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Пример конфигурации

Включено ? 

Исключения по Заголовкам ?

Форс Проверок для IP
203.0.113.61, 203.0.113.62, 203.0.113.63
[Редактировать](#)

TESTSECRET

EQUAL

g3xYPZKA6wNLhhXCgXsY6fITzN3h71gG
B3KX4KrvktKnKti3c15LkJgdEBnhosea
IzpsXv7Tg8wrpZnfikROTxW4lw4G4D21

[ДОБАВИТЬ ИСКЛЮЧЕНИЕ](#) +

Исключения Стран ?

JP ✕

PK ✕

Исключения IP и Подсетей ?

198.51.100.0/24, 233.252.0.0/24
[Редактировать](#)

А/В Распределение проверок ?

20% трафика будет проверено Антиботом

В данном примере защита от ботов будет применяться:

- к запросам от 20% посетителей,
- к запросам от IP-адресов 203.0.113.61, 203.0.113.62, 203.0.113.63.

Легитимными запросами без необходимости проверки будут считаться:

- запросы с одним из трёх указанных значений cookie `TestSecret`,
- запросы от IP-адресов из Японии и Пакистана,
- запросы от IP-адресов из подсетей 198.51.100.0/24, 233.252.0.0/24.

Личный кабинет: Bot protection → Подписи



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

В разделе «Bot protection → Подписи» личного кабинета Curator вы можете управлять подписями, предназначенными для проверки запросов мобильных приложений к API. Схема работы такой защиты описана в разделе [Защита мобильных API с использованием хэша](#).

Посмотреть список подписей

Чтобы посмотреть список подписей, настроенных для домена или сервиса:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection → Подписи**.

Подписи отображаются в таблице со следующими столбцами:

- **Статус** — статус подписи:
 -  — подпись включена, запросы с этой подписью разрешены.
 -  — подпись отключена, запросы с этой подписью запрещены.
- **Комментарий** — короткое описание подписи.
- **Отозванные версии** — устаревшие версии мобильного приложения, запросы от которых запрещены.

Включить проверку подписей

Чтобы разрешить запросы от пользователей, предоставляющих подпись вместо [трекинговой cookie](#):

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection → Подписи**.
3. В верхней части страницы активируйте опцию **Включено**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Отключить проверку подписей

Чтобы запретить запросы от пользователей, предоставляющих подпись вместо [трекинговой cookie](#):

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Подписи**.
3. В верхней части страницы деактивируйте опцию **Включено**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Добавить подпись

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Подписи**.
3. Нажмите кнопку **Добавить подпись**.
4. В открывшемся диалоге заполните поля:
 - **Включить** — если эта опция отключена, то запросы с этой подписью будут запрещены.
 - Настройки ключа подписи версий приложения:
 - **Заголовок с версией** — название заголовка, в котором мобильное приложение должно передавать информацию о своей версии.
 - **Секретный ключ** — ключ, используемый для вычисления значения salt.
 - **Salt метод** — метод вычисления значения salt:
 - **md5_lowercase** — MD5-хэш, представленный в виде строки в нижнем регистре.
 - **md5_uppercase** — MD5-хэш, представленный в виде строки в верхнем регистре.

В обоих случаях хэш вычисляется от строки, образованной конкатенацией **Секретного ключа** и значения **Заголовка с версией**.

- **Отозванные версии** — значения **Заголовка с версией**, использование которых запрещено.

Вы можете указать до 200 отозванных версий. Запрос с указанием любой из этих версий не будет считаться подписанными, и его обработка будет выполняться по обычному алгоритму, основанному на настроенных [локациях](#).

- Настройки механизма подписи:

- **Заголовок с Hash** — название заголовка, в котором мобильное приложение должно передавать подпись запроса.
- **Value метод** — метод формирования строки, от которой будет вычисляться хэш.
 - **salt_schema_host_uri_timestamp** — хэш от строки, включающей соль, полный URI и метку времени.
 - **salt_schema_host_path_timestamp** — хэш от строки, включающей соль, URI без строки GET-аргументов и метку времени.

К строке могут быть добавлены дополнительные значения, см. поле **Дополнительные заголовки** ниже.

- **Hash метод** — метод вычисления подписи:
 - **md5_lowercase** — MD5-хэш, представленный в виде строки в нижнем регистре.
 - **md5_uppercase** — MD5-хэш, представленный в виде строки в верхнем регистре.
- **Дополнительные заголовки** — названия заголовков, значения которых будут добавлены к строке, от которой будет вычисляться хэш.

Значения будут добавлены в том порядке, в котором указаны в этом поле.

○ Настройки интервала времени достоверности подписи:

- **Заголовок с Timestamp** — название заголовка, в котором мобильное приложение должно передавать время отправки запроса.
- **Формат времени** — поле влияет на формат передачи времени и способ его проверки:
 - **unix_msec** — заголовок должен содержать метку времени отправки запроса в миллисекундах.
 - **unix_sec** — заголовок должен содержать метку времени отправки запроса в секундах.
 - **any** — формат метки времени не проверяется.

При выборе форматов **unix_msec** и **unix_sec** обратный HTTP-прокси будет проверять полученную метку времени с текущим временем. Если они различаются более чем на заданный **Промежуток в секундах**, то запрос не будет считаться подписанным, и его обработка будет выполняться по обычному алгоритму, основанному на настроенных [локациях](#).

- **Промежуток в секундах** — допустимая разница между полученной меткой времени и текущим временем, см. описание поля **Формат времени**. Поле не отображается, если выбран формат времени **any**.

○ **Комментарий** (необязательно) — короткое описание подписи.

5. Нажмите кнопку **Добавить**.

6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

**ВАЖНО**

Добавлений подписей в список не означает автоматического включения проверки подписей у посетителей сайта. См. [Включить проверку подписей](#).

Изменить подпись

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.

2. Выберите пункт меню **Bot protection** → **Подписи**.

3. Найдите нужную подпись и кликните  рядом с ней.

4. В открывшемся диалоге отредактируйте нужные поля.

Поля формы редактирования подписи идентичны полям в [форме добавления подписи](#).

5. Нажмите кнопку **Сохранить**.

6. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Включить конкретные подписи

Чтобы включить одну или несколько подписей и разрешить запросы с их использованием:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.

2. Выберите пункт меню **Bot protection** → **Подписи**.

3. Поставьте чекбоксы возле нужных подписей. Нажмите кнопку **Включить**.

4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

**ВАЖНО**

Включение подписи в списке не означает автоматического включения проверки подписей у посетителей сайта. См. [Включить проверку подписей](#).

Отключить конкретные подписи

Чтобы отключить одну или несколько подписей и запретить запросы с их использованием:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Подписи**.
3. Поставьте чекбоксы возле нужных подписей. Нажмите кнопку **Отключить**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Удалить одну подпись

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Подписи**.
3. Найдите нужную подпись и кликните  рядом с ней.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Удалить несколько подписей

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Bot protection** → **Подписи**.
3. Поставьте чекбоксы возле нужных подписей. Нажмите кнопку **Удалить**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение 5–7 минут.

Личный кабинет: CDN



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*.

В разделе «CDN» личного кабинета Curator включается и настраивается [интеграция с CDN](#) для текущего домена или сервиса.

Включить интеграцию

Если для домена или сервиса ещё не включена интеграция с CDN, то в этом разделе доступны кнопки для настройки такой интеграции.

Необходимые настройки зависят от того, с каким именно провайдером CDN вам необходимо настроить интеграцию.

Включить Curator.CDN

1. Выберите нужный домен в разделе **Домены**.
2. Выберите пункт меню **CDN**.
3. Нажмите на ссылку **Curator.CDN**. В появившемся диалоге нажмите **Подключить Curator.CDN**.
4. В диалоге будет указан хост (доменное имя), который Curator.CDN выделит для обслуживания файлов для вашего домена или сервиса. Этот хост является основным и доступен вне зависимости от настроек. Дополнительно вы можете подключить произвольное количество других хостов.

Введите хосты в поле **Хостнеймы CDN**, разделяя их переносами строки. Нажмите **Далее**.



ПРИМЕЧАНИЕ

Вы сможете [изменить список хостов CDN](#) позже.

5. Перейдите в панель управления вашего регистратора доменных имён. Для каждого из хостов, по которым должен отвечать CDN, создайте запись CNAME, указывающую на основной хост, предоставленный Curator.CDN. Для вашего удобства пример записи CNAME будет показан на последнем шаге в диалоге настройки Curator.CDN.

При необходимости дождитесь обновления кеша DNS после внесённого изменения.

Включить интеграцию с Ngenix

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **CDN**.
3. Нажмите на ссылку **Ngenix**. В появившемся диалоге нажмите **Включить Ngenix**.

Включить интеграцию с Akamai

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **CDN**.
3. Нажмите на ссылку **Akamai**. В появившемся диалоге нажмите **Включить Akamai**.
4. Укажите параметры, необходимые для **взаимодействия с CDN по протоколу G2O**. Эти параметры необходимо получить на сайте Akamai.
 - **Data header** — название заголовка, содержащего данные о запросе.
 - **Sign header** — название заголовка, содержащего подпись запроса.
 - **Password** — ключ, используемый для верификации подписи.
 - **Algo** — криптографический алгоритм, используемый для подписания данных.

Нажмите **Сохранить**.



ПРИМЕЧАНИЕ

Нажмите **Настроить позже**, чтобы пропустить шаг. Вы сможете **изменить настройки G2O** позже.

Включить интеграцию по протоколу G2O

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **CDN**.
3. Нажмите на ссылку **G2O**.
4. Укажите параметры, необходимые для **взаимодействия с CDN по протоколу G2O**. Эти параметры необходимо получить на сайте используемого вами CDN.
 - **Data header** — название заголовка, содержащего данные о запросе.
 - **Sign header** — название заголовка, содержащего подпись запроса.
 - **Password** — ключ, используемый для верификации подписи.
 - **Algo** — криптографический алгоритм, используемый для подписания данных.

Нажмите **Сохранить**.

Включить интеграцию с G-Core

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **CDN**.
3. Нажмите на ссылку **G-Core**. В появившемся диалоге нажмите **Включить G-Core**.

Изменить настройки G2O

Если вы используете интеграцию с Akamai или другими CDN, [работающими по протоколу G2O](#), то в личном кабинете вам доступна возможность изменить настройки протокола.

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **CDN**.
3. Нажмите на ссылку **Редактировать** (или **Редактировать настройки G2O**).
4. В появившемся диалоге укажите параметры G2O. Эти параметры необходимо получить на сайте используемого вами CDN.
 - **Data header** — название заголовка, содержащего данные о запросе.
 - **Sign header** — название заголовка, содержащего подпись запроса.
 - **Password** — ключ, используемый для верификации подписи.
 - **Algo** — криптографический алгоритм, используемый для подписания данных.

Нажмите **Сохранить**.



ПРИМЕЧАНИЕ

При использовании CDN от Akamai вы можете полностью отключить взаимодействие по протоколу G2O, нажав кнопку **Сбросить G2O**. При этом IP-адреса Akamai останутся в белом списке Curator.

Пример конфигурации

Data header	X-G2O-Auth-Data
Sign header	X-G2O-Auth-Sign
Password	*****
Algo	sha256
СБРОСИТЬ G2O РЕДАКТИРОВАТЬ	

Выключить интеграцию

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.

2. Выберите пункт меню **CDN** → **Настройки**.
3. Нажмите кнопку **Выключить**.
4. В появившемся диалоге подтверждения нажмите кнопку **Выключить**.

Личный кабинет: Curator.CDN → Настройки



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

Эта страница описывает настройки, доступные при переключении личного кабинета в режиме **CDN** с помощью переключателя в левом верхнем углу.

Для удобства в режиме **Curator** (режим по умолчанию) также доступен раздел **Curator.CDN** в настройках домена, но некоторые настройки в нём могут быть недоступны.

Изменить настройки HTTP-заголовков

В этом разделе настраиваются различные параметры, связанные с обработкой HTTP-заголовков в запросах и ответах, получаемых и отправляемых сервером CDN.

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **Заголовки**.
3. Измените необходимые параметры.

- **Upstream headers, Client headers**

Наборы HTTP-заголовков, которые CDN добавляет в данные. **Upstream headers** определяет заголовки, добавляемые в каждый запрос от пользователя при пересылке его апстриму. **Client headers** определяет заголовки, добавляемые в каждый ответ пользователю.

Возле названия набора заголовков, который вы хотите отредактировать, нажмите ссылку **Редактировать**. Для каждого заголовка введите отдельно **Название** и **Значение**. Как название, так и значение должны быть непустыми строками. Чтобы добавить ещё один заголовок, нажмите **Добавить строку**. Чтобы удалить один из заголовков, нажмите **Удалить**. Чтобы применить изменения, нажмите **Сохранить**.

- **Access-Control-Allow-Origin**

Список регулярных выражений, определяющих допустимые значения заголовка **Origin** в запросах пользователя. Для любого значения **Origin**, удовлетворяющего одному из этих регулярных выражений, CDN будет добавлять в ответ такое же значение в заголовке **Access-Control-Allow-Origin**. Таким образом, браузеру будет разрешено использовать файлы, полученные с CDN, на сайтах, описанных в **Origin**.

Нажмите ссылку **Редактировать**. В каждой строчке введите валидное регулярное выражение. Если регулярное выражение валидно, рядом с ним отобразится иконка . Чтобы добавить ещё одно регулярное выражение, нажмите **Добавить строку**. Чтобы удалить одно из регулярных выражений, нажмите **Удалить**. Чтобы применить изменения, нажмите **Сохранить**.

**СОВЕТ**

Вы можете проверить работу введённого регулярного выражения, кликнув по иконке . В появившемся диалоге введите произвольную строку, чтобы проверить её на соответствие введённому ранее регулярному выражению. Если проверка успешна, рядом со строкой будет отображена иконка , в противном случае — иконка . Чтобы закрыть диалог проверки и вернуться к редактированию регулярного выражения, кликните вне диалога или нажмите клавишу **Esc**.

- Client IP header

Если задать этот параметр, то CDN будет передавать апстриму IP-адрес пользователя в HTTP-заголовке с указанным именем.

Нажмите ссылку **Редактировать**. В появившемся текстовом поле введите валидное имя HTTP-заголовка. Чтобы применить изменения, нажмите **Сохранить**.

Пример конфигурации

Upstream headers  Заголовки, которые будут передаваться в запросах от Qrator.CDN к апстриму		Client headers  Заголовки, которые будут передаваться в ответах от Qrator.CDN к клиенту	
Название	Значение	Название	Значение
X-Sent-Via-CDN	1	X-Cached-By-CDN	1
Access-Control-Allow-Origin  Если "Origin" заголовок клиента соответствует хотя бы одному из заданных регулярных выражений, то в ответ клиенту будет добавлен заголовок Access-Control-Allow-Origin, значение которого будет равно значению полученного от клиента заголовка "Origin"		Client IP header  Название заголовка, в котором будет передаваться реальный IP-адрес пользователя	
<code>/^http://example\.com(:80)?\$/</code>		X-Client-IP	
<code>/^https://example\.com(:443)?\$/</code>			

Посмотреть список хостов

- В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
- Выберите пункт меню **SNI/Хостнеймы**.

Хосты, настроенные для Curator.CDN, отображаются в виде таблицы со следующими столбцами:

- ID** (только для HTTPS) — уникальный числовой идентификатор сертификата в системе Curator. Кликните по идентификатору, чтобы посмотреть полную информацию о сертификате в [Хранилище сертификатов](#).
- Имя хоста** — доменное имя, по которому доступен Curator.CDN.

- **Subject** (только для HTTPS) — поле **Subject** установленного сертификата. Кликните по ссылке **Смотреть подробнее** в ячейке таблицы, чтобы увидеть краткую информацию о сертификате.
- **Не доступен после** (только для HTTPS) — конец периода действия сертификата. Если период действия уже закончился, это поле выделяется цветом.

Над таблицей присутствуют поля фильтров, с помощью которых вы можете находить сертификаты, содержащие нужные значения в полях **Имя хоста** и **Subject**.

Пример конфигурации

Установленные сертификаты				ДОБАВИТЬ
ID ↑↓	Имя хоста ↑↓	Subject ↑↓	Не доступен после ↑	
-	cdn1.example.com	Без сертификата	-	
89882	cdn2.example.com	CN=cdn2.example.com Смотреть подробнее	17 нояб. 2033 г., 19:31	
89883	cdn3.example.com	CN=cdn3.example.com Смотреть подробнее	17 нояб. 2033 г., 19:31	
90121	cdn4.example.com	CN=cdn4.example.com Смотреть подробнее	18 нояб. 2033 г., 21:34	
90121	cdn5.example.com	CN=cdn4.example.com Смотреть подробнее	18 нояб. 2033 г., 21:34	
Строк на страницу Все ▾ 1–5 of 5 < >				

Добавить HTTP-хост

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **SNI/Хостнеймы**.
3. Нажмите кнопку **Добавить**.
4. В появившемся диалоге нажмите **Установить** напротив пункта «Без сертификата».
5. В появившемся текстовом поле введите один или несколько хостов, на которых должен быть доступен сервис Curator.CDN.
6. Нажмите кнопку **Установить**.

В таблицу будет добавлено по одной строке для каждого из указанных хостов.

7. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

8. Перейдите в панель управления вашего регистратора доменных имён. Для каждого из добавленных хостов создайте запись CNAME, указывающую на основной хост, который был назначен вам при подключении услуги Curator.CDN. Вы можете уточнить адрес основного хоста у специалистов технической поддержки Curator.

При необходимости дождитесь обновления кеша DNS после внесённого изменения.

Добавить HTTPS-хост

1. Убедитесь, что действующий сертификат для добавляемого хоста загружен в раздел [Хранилище сертификатов](#).
2. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
3. Выберите пункт меню **SNI/Хостнеймы**.
4. Нажмите кнопку **Добавить**.
5. В появившемся диалоге найдите сертификат, действующий для хоста, который вы хотите добавить. При необходимости используйте фильтры **Имя хоста**, **Subject** и **Тип**, чтобы найти необходимый сертификат.

Нажмите **Установить** напротив нужного сертификата.

6. В появившемся текстовом поле введите или выберите из выпадающего списка один или несколько хостов, для которых следует использовать данный сертификат.
7. Нажмите кнопку **Установить**.

В таблицу будет добавлено по одной строке для каждого из указанных хостов.

8. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

9. Перейдите в панель управления вашего регистратора доменных имён. Для каждого из добавленных хостов создайте запись CNAME, указывающую на основной хост, который был назначен вам при подключении услуги Curator.CDN. Вы можете уточнить адрес основного хоста у специалистов технической поддержки Curator.

При необходимости дождитесь обновления кеша DNS после внесённого изменения.

Удалить хост

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **SNI/Хостнеймы**.
3. Найдите нужный хост и кликните  рядом с ним.

4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Настроить политики для URL запросов

По умолчанию Curator.CDN предполагает, что каждый запрос к нему следует перенаправлять к апстриму, но в некоторых случаях это может быть неоптимальным поведением.

Если вам известно, что для некоторых URL апстрим заведомо не сможет предоставить файл и поэтому на запросы к таким URL следует отвечать кодом 404 Not Found или другими кодами ошибок, рекомендуется описать это с помощью *правил для URL запросов*. Такая конфигурация позволит CDN в описанных случаях возвращать ответы с кодами ошибок сразу, не совершая запросов к апстриму.



ПРИМЕЧАНИЕ

CDN анализирует только путь (компонент path) из запрашиваемого URL. Например, если пользователь обратился к `/images/logo.png?v2`, то описанные в этом разделе правила будут проверяться для строки `/images/logo.png`.

Чтобы настроить правила:

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **Политики URL**.
3. Измените необходимые параметры.

- **Разрешённые URLs**

Список регулярных выражений, описывающих пути, которые пользователь может запрашивать с CDN. Если эта настройка задана, то для любых других URL будет возвращаться ошибка 404 Not Found (за исключением URL, описанных в списке **Запрещённые URLs**).

Нажмите ссылку **Редактировать**. В каждой строке введите валидное регулярное выражение. Если регулярное выражение валидно, рядом с ним отобразится иконка . Чтобы добавить ещё одно регулярное выражение, нажмите **Добавить строку**. Чтобы удалить одно из регулярных выражений, нажмите **Удалить**. Чтобы применить изменения, нажмите **Сохранить**.

- **Запрещённые URLs**

Список регулярных выражений, описывающих пути, для которых CDN должен возвращать тот или иной код ошибки.

Нажмите ссылку **Редактировать**. В каждой строке введите валидное регулярное выражение. Если регулярное выражение валидно, рядом с ним отобразится иконка . В поле **Код** введите код ошибки, который CDN должен использовать для запросов, соответствующих этому регулярному выражению. Чтобы добавить ещё одну пару регулярного выражения и кода

ошибки, нажмите **Добавить строку**. Чтобы удалить одну из пар, нажмите **Удалить**. Чтобы применить изменения, нажмите **Сохранить**.

**СОВЕТ**

Вы можете проверить работу введённого регулярного выражения, кликнув по иконке . В появившемся диалоге введите произвольную строку, чтобы проверить её на соответствие введённому ранее регулярному выражению. Если проверка успешна, рядом со строкой будет отображена иконка , в противном случае — иконка . Чтобы закрыть диалог проверки и вернуться к редактированию регулярного выражения, кликните вне диалога или нажмите клавишу **Esc**.

Пример конфигурации

Разрешённые URLs

Если запрашиваемый URL не соответствует хотя бы одному из заданных регулярных выражений, то клиент получит ответ со статусом 404. Настройка отключена, если не задано ни одного значения.

`/^/images/.*$/``/^/videos/.*$/``/^/files/.*$/`**Запрещённые URLs**

Если URL запрашиваемого ресурса соответствует одному из регулярных выражений, то клиент получит ответ с соответствующим HTTP-кодом

Изменить настройки кеширования

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **Кэш**.
3. Измените необходимые параметры.

- **Cache control**

Должен ли CDN учитывать время жизни закешированных файлов, предоставляемое апстримом в заголовках `Expires` и `Cache-Control`.

- **Client no cache**

Должен ли CDN добавлять заголовок `Cache-Control: no-cache` в ответах пользователю.

- **Cache errors**

Список кодов ошибок апстрима, которые CDN должен кешировать, а также время жизни кеша для каждого из них.

Нажмите ссылку **Редактировать**. В каждой строке введите **Код** ошибки и соответствующий **Таймаут** для её кеширования. Допустимые значения таймаута — от 60 000 до 300 000 мс. Чтобы применить изменения, нажмите **Сохранить**.

- **Cache errors (Client IP)**

Эта настройка работает аналогично обычной настройке **Cache errors**, но кеш, сохранённый в соответствии с этими правилами, будет использован только для запросов с того же IP-адреса, что и первоначальный запрос.

- **Игнорировать параметры запроса**

Игнорировать при кешировании все GET-параметры запроса. Например, это удобно, если вы полагаетесь на случайно сгенерированные GET-параметры для принудительного обновления закешированного контента браузером, но не хотите, чтобы это приводило к лишним запросам от CDN к апстриму.

- **Сброс кеша**

Здесь вы можете принудительно сбросить кеш CDN для одного или нескольких файлов.

Нажмите кнопку **Сбросить кеш**. В появившемся диалоговом окне введите пути ко всем файлам, которые вы хотите удалить из кеша. Каждый путь должен начинаться с `/`. После этого нажмите кнопку **Сбросить кеш** в диалоге. Указанные файлы будут удалены из кеша в течение нескольких минут.

Пример конфигурации

Cache control Если включен, запросы к апстриму регулируются заголовками expires, cache-control ☒ Включено Cache errors Если апстрим вернул ответ код ошибки, который соответствует одному из указанных, то ответ будет кеширован и повторный запрос к апстриму будет возможен только после заданного таймаута <table border="1"> <thead> <tr> <th>Код</th> <th>Таймаут, мс</th> </tr> </thead> <tbody> <tr> <td>500</td> <td>60000</td> </tr> <tr> <td>502</td> <td>120000</td> </tr> </tbody> </table> Игнорировать параметры запроса Игнорировать параметры запроса при вычислении ключа кеширования. ☒ Игнорировать	Код	Таймаут, мс	500	60000	502	120000	Client no cache Если включён, то в ответах клиенту будет отправлен заголовок "cache-control: no-cache" ☐ Включено Cache errors (Client IP) Если апстрим отвечает HTTP-кодом, который соответствует одному из указанных, то такой ответ будет кеширован и повторный запрос с данного IP-адреса клиента будет возможен после соответствующего таймаута <table border="1"> <thead> <tr> <th>Код</th> <th>Таймаут, мс</th> </tr> </thead> <tbody> <tr> <td>403</td> <td>60000</td> </tr> </tbody> </table> Сбросить кэш Ручное удаление файлов из кеша CDN СБРОСИТЬ КЭШ	Код	Таймаут, мс	403	60000
Код	Таймаут, мс										
500	60000										
502	120000										
Код	Таймаут, мс										
403	60000										

Изменить настройки транспорта

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **Транспорт**.
3. Измените необходимые параметры.

- **Поддержка HTTP/2**

Включить поддержку протокола HTTP/2. Если настройка не включена, CDN будет работать только по протоколу HTTP/1.1.

- **Алгоритмы сжатия**

Включить или отключить поддержку конкретного алгоритма сжатия данных. По умолчанию Curator.CDN поддерживает форматы сжатия `gzip`, `deflate` и `br`, но вы можете отключить поддержку любых из них, отключив соответствующие чекбоксы.

Пример конфигурации

Поддержка HTTP2 Установите эту опцию, чтобы включить в Qrator.CDN поддержку протокола HTTP2 ☒ HTTP2	Алгоритмы сжатия Настройте алгоритмы сжатия, которые будет использовать Qrator.CDN ☒ gzip ☒ deflate ☒ br
--	---

Настроить конвертацию изображений в WebP

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **WebP**.
3. Нажмите **Включено**, чтобы включить или выключить автоконвертацию изображений в формат WebP.

При необходимости измените желаемое значение параметра **Quality**. Более низкие значения параметра обеспечивают бóльшую эффективность сжатия, но бóльшие потери в качестве изображения.

4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Пример конфигурации

☒ Включено	Quality 80 <input type="range"/>
--	-------------------------------------

Настроить HTTP перенаправления

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **HTTP Перенаправления**.
3. Нажмите **Включено**, чтобы включить или выключить перенаправления.

При необходимости измените **HTTP-код**, который будет использоваться для перенаправлений. Доступны следующие коды:

- 301 Moved Permanently
- 302 Found

- 307 Temporary Redirect
- 308 Permanent Redirect

4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменения будут применены в течение нескольких минут.

Пример конфигурации

 Включено

HTTP-код перенаправления
301

Отключить услугу Curator.CDN

1. В режиме **CDN** перейдите в раздел **Домены** и кликните на нужный домен.
2. Выберите пункт меню **Отключить**.
3. Нажмите кнопку **Выключить**.
4. Подтвердите действие, нажав **Выключить** в появившемся диалоге.

Личный кабинет: Утилиты



ПРИМЕЧАНИЕ

В конфигурации по умолчанию этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*.

Утилиты «Проверка IP», «Трассировка» и «Уязвимости» в личном кабинете Curator могут быть полезны для диагностики проблем, возникающих у пользователей, а также для проверки корректности настройки файервола.

Проверить информацию об IP-адресе

С помощью утилиты «Проверка IP» вы можете узнать, как обратные прокси Curator расценивают входящий трафик с заданного IP-адреса. Утилита доступна для [доменов](#) и [сервисов](#). Если в вашем аккаунте настроены несколько доменов или сервисов, состояние одного и того же IP-адреса для них может различаться.

Чтобы воспользоваться утилитой:

1. Выберите нужный домен в разделе **Домены** или сервис в разделе **Сервисы**.
2. Выберите пункт меню **Проверка IP**. (При работе с доменом этот пункт находится в подменю **Утилиты**.)
3. В текстовом поле введите IP-адрес.
4. Нажмите кнопку **Поиск**.

Рядом с формой будет показан один из следующих статусов.

- Статусы, при которых трафик с IP-адреса пропускается без ограничений:
 - «IP-адрес не заблокирован»
 - «IP-адрес находится в "Белом списке"»
 - «IP-адрес является апстримом»
- Статусы, при которых трафик с IP-адреса ограничен:
 - «IP-адрес заблокирован через Curator API»
 - «IP-адрес заблокирован WAF»
 - «IP-адрес заблокирован системой фильтрации Curator»
 - «Заблокирован на основании HTTP кода (456) ответа сервера»

Посмотреть трассировку до IP-адреса

С помощью утилиты «Трассировка» вы можете посмотреть маршрут, которым отправляются пакеты от каждого из [центров очистки трафика Curator](#) до заданного IP. Эта утилита доступна только для [доменов](#).

Чтобы воспользоваться утилитой:

1. Выберите нужный домен в разделе **Домены**.
2. Выберите пункт меню **Утилиты** → **Трассировка**.
3. Выберите **IP-адрес** вашего апстрима из выпадающего списка.
4. Укажите **Порт**.
5. Нажмите кнопку **Выполнить**.

Проверить наличие уязвимых портов

В разделе «Уязвимости» отображаются результаты регулярных проверок [апстримов](#) на предмет наличия открытых портов 80 и 443.

Проверки выполняются проверки раз в 4 часа с IP-адреса, не входящего в подсети Curator. При правильной настройке фаервол должен сбросить (drop) запрос с такого адреса. Если же при проверке был получен любой ответ от сервера, это говорит об уязвимости вашей сети к атакам, которые направлены на апстрим напрямую, то есть не через сеть Curator.

Чтобы увидеть результаты проверки:

1. Выберите нужный домен в разделе **Домены**.
2. Выберите пункт меню **Утилиты** → **Уязвимости**.
3. В поле **Дата** выберите интересующие вас дату и время проверки. По умолчанию выбраны дата и время последней проверки.

Результаты проверки будут отображены в виде таблицы со следующими столбцами:

- IP-адрес апстрима,
- проверяемый порт,
- результат проверки: «Защищён» или «Уязвим».

Если хотя бы один из портов уязвим, измените конфигурацию вашего фаервола, чтобы устранить уязвимость. Для этого воспользуйтесь руководством [Настройка фаервола](#), а при необходимости обратитесь за помощью к специалистам Curator.

Личный кабинет: Хранилище сертификатов



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*. Редактировать настройки могут только пользователи группы *Technical*.

Хранилище сертификатов содержит TLS-сертификаты, доступные для вашего аккаунта, и позволяет устанавливать их на конкретные домены и сервисы.

Перед началом работы с сертификатами

Чтобы начать использовать TLS-шифрование на [домене](#) или [сервисе](#), необходимо выполнить два шага:

1. Добавление сертификата в Хранилище сертификатов

В разделе «Хранилище сертификатов» личного кабинета вы можете *добавить* сертификат в систему, [сгенерировав его с помощью сервиса Let's Encrypt или НУЦ](#), или [загрузив готовые файлы из другого источника](#). Эти же действия можно выполнить с помощью [методов Curator API](#). Добавленный сертификат не начинает использоваться автоматически, но становится доступным для установки на любой из доменов и сервисов аккаунта, см. следующий шаг.

2. Установка сертификата для домена или сервиса

Установка сертификата означает настройку соответствия между сертификатом и конкретным доменным именем, для которого будет использоваться этот сертификат. Установку можно выполнить [в разделе «Хранилище сертификатов»](#), [в разделе «TLS» для домена или сервиса](#), а также с помощью [методов Curator API](#).

При установке сертификата вы указываете, для каких доменных имён он будет использоваться. Также вы можете выбрать опцию «Хост по умолчанию». Сертификат, установленный с такой опцией, будет использован в случаях, когда пользователь делает запрос к доменному имени, для которого другой сертификат не назначен. Каждый домен или сервис, для которого установлены сертификаты, должен иметь один сертификат с опцией «Хост по умолчанию».

Посмотреть список сертификатов

Сертификаты, добавленные в Хранилище сертификатов, отображаются в таблице **Активные сертификаты**. Доступны следующие столбцы:

- **ID** — уникальный числовой идентификатор сертификата в системе Curator.

- **Истекает** — конец периода действия сертификата. Если период действия уже закончился, это поле выделяется цветом.
- **Тип** — происхождение сертификата: *Загруженный*, *НУЦ* или *Let's Encrypt*.
- **Subject** — доменные имена, для которых действителен сертификат, а также ссылка для [просмотра краткой информации о сертификате](#).

Если сертификат установлен на одном или нескольких ресурсах (доменах или сервисах), то для него будет показана дополнительная информация:

- **Ресурсы** — ссылки на раздел «TLS» для управления установленными сертификатами для доменов или сервисов. Ссылки в разных строчках ведут на настройки разных доменов или сервисов.
- **Имя хоста** — информация о том, для каких доменных имён используется этот сертификат. Каждая строчка может быть конкретным доменным именем или строкой «*default hostname*», см. [Перед началом работы с сертификатами](#).

Над таблицей присутствуют поля фильтров, с помощью которых вы можете находить сертификаты, содержащие нужные значения в полях **Subject**, **Имя хоста** и **Ресурсы**.

Посмотреть информацию о сертификате

Краткая информация

Чтобы посмотреть краткую информацию о сертификате:

1. Перейдите в раздел **Хранилище сертификатов**.
2. Найдите строку с нужным сертификатом и кликните в ней по ссылке **Показать детали сертификата**.

В появившемся диалоге будет доступна следующая информация:

- **ID** — уникальный числовой идентификатор сертификата в Хранилище сертификатов.
- **Тип** — происхождение сертификата: *Загруженный* или *Let's Encrypt*.
- **Имена доменов** — доменные имена, для которых действителен сертификат.
- **Not valid before, Not valid after** — начало и конец периода действия сертификата.

Сертификат может содержать одну или несколько цепочек. Если сертификат содержит несколько цепочек, между ними можно переключаться с помощью радиокнопок с названиями соответствующих алгоритмов шифрования. Для каждой цепочки доступна следующая информация:

- **Private key encryption** — криптографический алгоритм, используемый для приватного ключа.
 - **Private key size** — размер приватного ключа в битах.
 - **SHA-256 Fingerprint, SHA-1 Fingerprint** — отпечатки открытого ключа.
 - **Certificate chain** — вся цепочка в формате PEM. Полные данные можно скопировать кнопкой .
 - **Private key** — приватный ключ в формате PEM. Полные данные можно скопировать кнопкой .
- Поле не отображается, если [приватный ключ сертификата скрыт](#).

Полная информация

Чтобы посмотреть полную информацию о сертификате:

1. Перейдите в раздел **Хранилище сертификатов**.
2. Найдите строку с нужным сертификатом и кликните по ней.

В появившемся диалоге будет доступна следующая информация:

- **ID** — уникальный числовой идентификатор сертификата в Хранилище сертификатов.
- **Тип** — происхождение сертификата: *Загруженный*, *НУЦ* или *Let's Encrypt*.
- **Ресурс** — идентификатор и название домена или сервиса, для которого установлен сертификат. Отображается только для [установленных сертификатов](#).
- **Автообновление сертификата** — включено ли автообновление сертификата. Отображается только для сертификатов НУЦ и Let's Encrypt, [выпущенных через личный кабинет](#).
- **Имена доменов** — доменные имена, для которых действителен сертификат.
- **Not valid before, Not valid after** — начало и конец периода действия сертификата.

Сертификат может содержать одну или несколько цепочек. Если сертификат содержит несколько цепочек, между ними можно переключаться с помощью радиокнопок с названиями соответствующих алгоритмов шифрования. Для каждой цепочки доступна следующая информация:

- **Private key encryption** — криптографический алгоритм, используемый для приватного ключа.
 - **Private key size** — размер приватного ключа в битах.
 - **SHA-256 Fingerprint, SHA-1 Fingerprint** — отпечатки открытого ключа.
 - **Certificate chain** — вся цепочка в формате PEM. Полные данные можно скопировать кнопкой .
 - **Private key** — приватный ключ в формате PEM. Полные данные можно скопировать кнопкой .
- Поле не отображается, если [приватный ключ сертификата скрыт](#).

Если сертификат [установлен](#) для одного или нескольких доменов или сервисов, то они будут показаны на этой странице в виде списка. Рядом с каждым доменом или сервисом указывается информация о том, для каких доменных имён используется этот сертификат. Каждая строка может быть конкретным доменным именем или строкой «Хост по умолчанию». Кликните на название домена или сервиса, чтобы перейти к управлению всеми установленными для него сертификатами в разделе «TLS».

Выпустить сертификат НУЦ или Let's Encrypt

Curator позволяет выпустить новый сертификат для вашего доменного имени непосредственно из личного кабинета благодаря интеграции с сервисом НУЦ и [Let's Encrypt](#).

1. Убедитесь, что нужное доменное имя уже добавлено в настройках сервиса, для которого оно будет использовано. В противном случае Curator не сможет подтвердить управление доменным именем во время проверки НУЦ или Let's Encrypt.
 - Для [обратного HTTP-прокси](#): в А-записи зоны DNS для доменного имени укажите Curator IP, а само доменное имя [добавьте в список апстримов](#).

- Для [Curator.CDN](#): создайте CNAME-запись в DNS для доменного имени в соответствии с инструкциями при подключении, а само доменное имя [добавьте в список хостнеймов](#) как имя без сертификата.
- Для [подключения по BGP](#): настройте BGP-пиринг с сетью Curator и [включите сервис в личном кабинете](#).

2. Перейдите в раздел **Хранилище сертификатов** и нажмите кнопку **Добавить сертификат**.

На открывшейся странице выберите вкладку **Использовать НУЦ** или **Использовать Let's Encrypt**. Нажмите кнопку **Далее**.

3. Укажите информацию для прохождения проверки [HTTP-01 challenge](#) для НУЦ/Let's Encrypt:

- выберите домен или сервис на вашем аккаунте, на котором уже настроена работа обратного HTTP-прокси Curator или работа по BGP,
- введите одно или несколько доменных имён, для которых должен быть выпущен сертификат.

Обратный прокси на стороне Curator автоматически выполнит необходимые требования для прохождения проверки. Дополнительная настройка с вашей стороны для этого не требуется.

Нажмите кнопку **Создать сертификат**.

4. Дождитесь завершения проверки запроса сервером НУЦ/Let's Encrypt. Если процесс занимает долгое время, вы можете закрыть вкладку и вернуться к процессу позже, см. [Посмотреть или удалить незавершённые операции](#).

Если проверка завершится ошибкой, вы увидите сообщение с описанием ошибки. При необходимости свяжитесь с технической поддержкой Curator для выяснения причины проблемы.

5. Перед добавлением сертификата в Хранилище сертификатов вы увидите экран подтверждения, на котором сможете ознакомиться с детальной информацией о добавляемом сертификате.

Информация о цепочке:

- **Not valid before, Not valid after** — начало и конец периода действия сертификата.
- **Длина цепочки** — количество сертификатов в цепочке, не считая конечного сертификата.

Информация о каждом публичном ключе:

- **Subject** — сведения об области применимости сертификата.
- **Not valid before, Not valid after** — начало и конец периода действия ключа.
- **SHA-1, SHA-256** — отпечатки открытого ключа.

Чтобы завершить операцию, нажмите кнопку **Добавить в хранилище сертификатов**.

Обратите внимание, что добавление сертификата не означает его автоматическую установку и использование, см. подробности в разделе [Перед началом работы с сертификатами](#).

Загрузить сертификат

Воспользуйтесь этим способом добавления, если вы уже сгенерировали TLS-сертификат с помощью какого-либо сервиса или самостоятельно.

1. Перейдите в раздел **Хранилище сертификатов** и нажмите кнопку **Добавить сертификат**.

На открывшейся странице будет автоматически выбрана вкладка **Загрузить сертификат**.

2. Укажите файлы, которые вы хотите загрузить. Для этого кликните по значку  и выберите файлы в системном диалоге или просто перетащите их на страницу.

Список файлов, выбранных для загрузки, будет показан в специальном диалоге подтверждения. В этом диалоге вы можете:

- нажать ссылку **Удалить**, чтобы отменить загрузку конкретного файл, выбранного по ошибке,
- нажать ссылку **Удалить все**, чтобы очистить список файлов,
- нажать ссылку **+**, чтобы выбрать дополнительные файлы.

Убедитесь, что предоставляемый вами набор файлов содержит как публичные ключи или цепочки их публичных ключей, так и соответствующие им приватные ключи.

Поддерживаются сертификаты X.509 в формате PEM. В качестве контейнерных форматов поддерживаются `pem`, `cer`, `crt`, `der`, `p7b`, `p7c`, `p12`. Весь набор файлов или его часть может быть загружена в виде архива в одном из форматов: `tar`, `tar.gz`, `tar.bz2`, `zip`, `7z`.

3. Нажмите кнопку **Загрузить** и дождитесь завершения обработки файлов. Если процесс занимает долгое время, вы можете закрыть вкладку и вернуться к процессу позже, см. [Посмотреть или удалить незавершённые операции](#).
4. Если предоставленный набор файлов содержит несколько сертификатов или несколько возможных цепочек для одного сертификата, то вы увидите информацию обо всех доступных вариантах. (Если набор файлов содержит только один сертификат и одну цепочку, то этот шаг автоматически пропускается.)

Сертификаты / Сертификат (ID: 896250) УДАЛИТЬ (ID: 896250)

Выберите сертификат для установки

ПРЕДЫДУЩИЙ ● ● ● ● ДАЛЕЕ

Subject
CN=example.com

Not valid before
30 июля 2022 г., 8:52

Not valid after
30 июля 2023 г., 8:52

SHA-1
35:6F:70:BD:D2:0C:36:08:F2:96:89:F3:26:3A:43:2A:A2:78:8A:4C

SHA-256
F0:06:70:CC:BB:43:87:DE:FD:45:5D:6B:3D:51:26:40:F8:97:DF:56:08:3A:BE:A7:27:1C:DA:93:86:8C:53:B8

УСТАНОВИТЬ

Выберите нужный сертификат и цепочку с помощью ссылок **Предыдущий** и **Далее**.

Нажмите кнопку **Установить**, чтобы перейти к следующему шагу.

5. Перед добавлением сертификата в Хранилище сертификатов вы увидите экран подтверждения, на котором сможете ознакомиться с детальной информацией о добавляемом сертификате.

Информация о цепочке:

- **Not valid before, Not valid after** — начало и конец периода действия сертификата.
- **Длина цепочки** — количество сертификатов в цепочке, не считая конечного сертификата.
- **Self-signed** — является ли сертификат [самоподписанным](#).
- **Trusted CA** — содержит ли цепочка сертификат, подписанный доверенным удостоверяющим центром.

Информация о каждом публичном ключе:

- **Subject** — сведения об области применимости сертификата.
- **Not valid before, Not valid after** — начало и конец периода действия ключа.
- **SHA-1, SHA-256** — отпечатки открытого ключа.

Чтобы завершить операцию, нажмите кнопку **Добавить в хранилище сертификатов**.

Обратите внимание, что добавление сертификата не означает его автоматическую установку и использование, см. подробности в разделе [Перед началом работы с сертификатами](#).

**ПРИМЕЧАНИЕ**

Если загруженный набор файлов содержит несколько сертификатов, то после добавления вы можете закрыть диалог и вернуться к предыдущему шагу, чтобы добавить в Хранилище сертификатов ещё один сертификат из набора.

Посмотреть или удалить незавершённые операции

Существуют два вида незавершённых операций по добавлению сертификата:

- Заявки в обработке

Когда для заявки на добавление сертификата была запущена, но ещё не завершилась [проверка на сервере НУЦ/Let's Encrypt](#) или [обработка на сервере Curator](#), эта заявка отображается на вкладке **В обработке**. Если в вашем аккаунте нет заявок с таким статусом, вкладка не отображается.

- Обработанные заявки

Когда автоматическая проверка уже завершена, эта заявка отображается на вкладке **Обработаны**. Если в вашем аккаунте нет заявок с таким статусом, вкладка не отображается.

Чтобы перейти к незавершённой операции:

1. Перейдите в раздел **Хранилище сертификатов**. Откройте вкладку **В обработке** или **Обработаны**.
2. Кликните по нужной операции.

После этого вы сможете продолжить добавление сертификата с того же места, на котором запустилась [проверка на сервере НУЦ/Let's Encrypt](#) или [обработка на сервере Curator](#).

Чтобы отменить операцию:

1. Перейдите в раздел **Хранилище сертификатов**. Откройте вкладку **В обработке** или **Обработаны**.
2. Найдите операцию, которую вы хотите отменить, и кликните  рядом с ней.
3. В диалоге подтверждения нажмите **Удалить**.

Установить сертификат для домена или сервиса

Как описано в разделе [Перед началом работы с сертификатами](#), для установки необходим сертификат, уже добавленный в Хранилище сертификатов.

Чтобы установить сертификат:

1. Перейдите в раздел **Хранилище сертификатов**.
2. Найдите строку с нужным сертификатом и кликните на неё.

3. Нажмите кнопку **Установить сертификат**.
4. В появившемся диалоге выберите **Ресурс** — домен или сервис на вашем аккаунте, для которого вы хотите установить сертификат.

Нажмите **Далее**.

5. Укажите, для каких доменных имён должен использоваться этот сертификат.
 - Если сертификат должен использоваться для одного или нескольких конкретных доменных имён, введите их в текстовое поле. После каждого доменного имени нажимайте клавишу **Enter** или **Пробел** или вводите запятую.
 - Если сертификат должен использоваться в ситуациях, когда пользователь ещё не указал требуемое доменное имя или указал доменное имя, для которого не настроен никакой другой сертификат, отметьте опцию **Использовать данный сертификат по умолчанию для любого доменного имени**.

Нажмите кнопку **Установить**.



ВАЖНО

Обратите внимание, что если на домене или сервисе установлен хотя бы один сертификат для какого-либо доменного имени, то на этом домене или сервисе также обязательно должен быть установлен сертификат по умолчанию.

Включить или выключить автообновление

Для сертификатов НУЦ/Let's Encrypt, [выпущенных через личный кабинет](#), Curator может выполнять автоматическое обновление, см. [Автоматический выпуск сертификатов](#). По умолчанию эта функция включена для каждого такого сертификата.

Чтобы отключить эту функцию или включить её заново:

1. Перейдите в раздел **Хранилище сертификатов**.
2. Найдите строку с нужным сертификатом типа **Let's Encrypt** и кликните на неё.
3. Рядом с полем **Автообновление сертификата** нажмите кнопку **Выключить автообновление** или **Включить автообновление**. В появившемся диалоге подтвердите выбранное действие.

Спрятать приватный ключ сертификата

По умолчанию любой пользователь вашего аккаунта, входящий в группу с политикой «*Раздел 'Хранилище Сертификатов'*», может [посмотреть полную информацию о любом сертификате](#), в том числе его приватный ключ. В зависимости от состава вашей команды, это может быть нежелательно с

точки зрения безопасности, поэтому Curator позволяет навсегда спрятать содержимое приватного ключа конкретного сертификата из личного кабинета, не повлияв на работоспособность сертификата.

Чтобы спрятать содержимое приватного ключа из личного кабинета:

1. Перейдите в раздел **Хранилище сертификатов**.
2. Найдите строку с нужным сертификатом и кликните на неё.
3. Рядом с полем **Private key** нажмите кнопку **Защитить приватный ключ**. В появившемся диалоге подтвердите выбранное действие.

Удалить сертификат

1. Перейдите в раздел **Хранилище сертификатов**.
2. Найдите строку с сертификатом, который вы хотите удалить, и кликните на неё.
3. В верхней части открывшейся страницы нажмите кнопку **Удалить**.

Если сертификат установлен на доменах или сервисах, появится сообщение о том, что удаление сертификата невозможно. В этом случае перейдите к настройкам соответствующих доменов или сервисов и [отключите сертификат](#), после чего начните удаление заново.

4. В появившемся диалоге подтвердите действие, нажав кнопку **Удалить**.

Личный кабинет: API токены



ПРИМЕЧАНИЕ

В [конфигурации по умолчанию](#) этот раздел личного кабинета доступен только пользователям групп *Technical* и *Administrative*.

В разделе «API токены» личного кабинета вы можете добавлять и удалять токены для [авторизации в Curator API](#). Каждому токenu можно индивидуально назначить набор методов API, которые вы сможете вызывать при его использовании.

Посмотреть список токенов

В разделе **API токены** личного кабинета отображается таблица со всеми действующими токенами для текущего аккаунта.

Доступны следующие столбцы:

- **Токен** — строка, которую следует передавать в HTTP-заголовке для [авторизации в Curator API](#).

Строка отображается в сокращённом виде. Получить полное значение токена через интерфейс после его создания нельзя. Это возможно только в момент создания токена.

- **Комментарий** — комментарий к токenu, который был введён при его добавлении или редактировании. Может быть пустым.
- **Политики** — количество политик, добавленных для токена.

Иногда это число соответствует количеству методов API, которые могут быть вызваны с этим токеном, но в некоторых случаях реальное количество методов может быть больше (при использовании политик «*Любой клиентский метод*» или «*Любой ресурсный метод*»).

Добавить токен

1. В разделе **API токены** личного кабинета нажмите кнопку **Добавить токен API**. Откроется диалог добавления токена.
2. Введите **Комментарий** для токена. Это поле можно оставить пустым.

Рекомендуется описывать в комментарии, кто и для чего будет использовать данный токен. Это позволит проще находить нужный токен, чтобы [отредактировать](#) его позднее.

3. Добавьте одну или несколько политик. Набор политик определяет, какие методы API вы сможете вызывать с использованием данного токена.

Чтобы добавить политику, связанную с методами из раздела [Client methods](#) документации Curator API:

1. Нажмите **Добавить политику**. Откроется диалог добавления политики.
2. В выпадающем списке выберите название клиентского метода или политику *«Любой клиентский метод»*.
3. Нажмите **Сохранить**.

Чтобы добавить политику, связанную с методами из разделов [Domain methods](#) и [Service methods](#) документации Curator API:

1. Нажмите **Добавить политику**. Откроется диалог добавления политики.
2. В выпадающем списке выберите название ресурсного метода или политику *«Любой ресурсный метод»*.
3. Выберите один или несколько ресурсов (доменов или сервисов), для которых должна действовать политика, или отметьте чекбокс **Любой ресурс**.
4. Нажмите **Сохранить**.

Чтобы отменить добавление политики, нажмите  рядом с её названием.

5. Нажмите кнопку **Добавить**, чтобы завершить добавление токена.

Добавленный токен можно скопировать, кликнув на иконку копирования. Скопировать токен можно только один раз в процессе создания, далее он не будет отображаться в интерфейсе.

Редактировать токен

1. В разделе **API токены** личного кабинета нажмите  напротив токена, который вы хотите отредактировать.
2. Если необходимо, измените **Комментарий** для токена.
3. Если необходимо, измените список политик для токена.

Чтобы добавить политику, связанную с методами из раздела [Client methods](#) документации Curator API:

1. Нажмите **Добавить политику**. Откроется диалог добавления политики.
2. В выпадающем списке выберите название клиентского метода или политику *«Любой клиентский метод»*.
3. Нажмите **Сохранить**.

Чтобы добавить политику, связанную с методами из разделов [Domain methods](#) и [Service methods](#) документации Curator API:

1. Нажмите **Добавить политику**. Откроется диалог добавления политики.

2. В выпадающем списке выберите название ресурсного метода или политику *«Любой ресурсный метод»*.
3. Выберите один или несколько ресурсов (доменов или сервисов), для которых должна действовать политика, или отметьте чекбокс **Любой ресурс**.
4. Нажмите **Сохранить**.

Чтобы удалить политику, нажмите  рядом с её названием.

5. Нажмите **Редактировать**, чтобы сохранить изменения и закрыть диалог.

Удалить токен

1. В разделе **API токены** личного кабинета нажмите  напротив названия токена, который вы хотите удалить.
2. Подтвердите действие, нажав **Удалить** в появившемся диалоге.

Личный кабинет: Пользователи

Если вам необходимо обеспечить доступ в личный кабинет Curator сразу для нескольких сотрудников компании, вы можете завести несколько учётных записей пользователей. Учётные записи всех сотрудников привязываются к одному и тому же *аккаунту*, заведённому для компании. Управление учётными записями производится в разделе **Пользователи** личного кабинета.

Для разных пользователей можно настроить разные права доступа в личном кабинете, см. описание раздела **Группы**.



ПРИМЕЧАНИЕ

В *конфигурации по умолчанию* редактировать чужие учётные записи, а также добавлять и удалять учётные записи могут только пользователи группы *Access Manager*.

Сменить пароль или включить двухфакторную аутентификацию для учётной записи пользователя может только сам пользователь, см. раздел «**Мой профиль**».

Посмотреть список пользователей

В разделе **Пользователи** личного кабинета отображается таблица со всеми пользователями текущего аккаунта.

Доступны следующие столбцы:

- **Имя** — фамилия и имя пользователя.
- **Группы** — список *групп*, в которые входит учётная запись пользователя.
- **Контакты** — адрес электронной почты пользователя.

Посмотреть информацию о пользователе

В разделе **Пользователи** личного кабинета кликните по имени пользователя. На открывшейся странице будет отображена информация о пользователе.

Поля с информацией разделены на три группы.

- **Основная информация**
 - **Имя и Фамилия** пользователя.
 - **Группы** — список *групп*, в которые входит учётная запись пользователя.

- **Контакты**

- **Адрес эл. почты**, указанный при [создании учётной записи пользователя](#).
- **Skype** — аккаунт пользователя в Skype для оперативной связи (если указан).
- **Номер телефона, Добавочный номер, Мобильный телефон** — информация для оперативной связи по телефону (если указана).

- **Настройки языка**

- **Язык** — язык интерфейса личного кабинета для пользователя.

Изменить информацию о пользователе

1. В разделе **Пользователи** личного кабинета кликните по нужному пользователю.
2. В блоке **Информация о пользователе** нажмите .
3. Отредактируйте информацию о пользователе.
 - **Имя и Фамилия** пользователя.
 - **Skype** — аккаунт пользователя в Skype для оперативной связи (не обязательно).
 - **Номер телефона, Добавочный номер, Мобильный телефон** — информация для оперативной связи по телефону (не обязательно).
4. Нажмите кнопку **Сохранить**.

Изменить группы пользователя

1. В разделе **Пользователи** личного кабинета кликните по нужному пользователю.
2. В блоке **Информация о пользователе** нажмите .
3. Отредактируйте список в секции **Группы**.

Чтобы добавить группу в список, кликните по её названию в выпадающем списке. Для поиска нужной группы начните вводить в текстовое поле часть её названия.

Чтобы удалить группу из списка, кликните по крестику рядом с её названием.
4. Нажмите кнопку **Сохранить**.

**СОВЕТ**

Если вы изменили группы для учётной записи, под которой авторизованы, обновите страницу для полного применения изменений.

Изменить настройки языка пользователя

1. В разделе **Пользователи** личного кабинета кликните по нужному пользователю.
2. В блоке **Информация о пользователе** нажмите .
3. Задайте необходимые настройки.
 - **Язык** — язык интерфейса личного кабинета для пользователя.
 - **Язык отчётов** — язык [отчётов](#), которые пользователь будет получать на электронную почту. Чтобы пользователь не получал отчётов, выберите вариант **Не отправлять**.
4. Нажмите кнопку **Сохранить**.

Создать учётную запись пользователя

1. В разделе **Пользователи** личного кабинета нажмите кнопку **Создать пользователя**.
2. В появившемся диалоге введите информацию о пользователе.

Поля для ввода информации разделены на четыре группы.

- **Основная информация**
 - **Имя и Фамилия** пользователя.
- **Контакты**
 - **Адрес эл. почты** — будет использоваться для авторизации, а также для отправки [уведомлений](#) и [отчётов](#).
 - **Skype** — аккаунт пользователя в Skype для оперативной связи (не обязательно).
 - **Номер телефона, Добавочный номер, Мобильный телефон** — информация для оперативной связи по телефону (не обязательно).
- **Группы**
 - **Выбранные группы** — список [групп](#), в которые необходимо включить учётную запись пользователя.

Чтобы добавить группу в список, кликните по её названию в выпадающем списке. Для поиска нужной группы начните вводить в текстовое поле часть её названия.

Чтобы удалить группу из списка, кликните по крестику рядом с её названием.
- **Настройки языка**
 - **Язык** — язык интерфейса личного кабинета для пользователя.

3. Нажмите кнопку **Сохранить**.

На электронную почту пользователя будет отправлено приглашение со ссылкой для установки пароля.

Отключить двухфакторную аутентификацию

Если один из пользователей [включил двухфакторную аутентификацию](#) в личном кабинете, но впоследствии утратил доступ к приложению, генерирующему временные коды, то другой пользователь, для которого добавлена политика «Разделы 'Пользователи' и 'Группы'» с правом на изменения (см. [Политики](#)), может отключить двухфакторную аутентификацию для него.



ВАЖНО

Перед совершением операции убедитесь, используя доверенные средства связи, что просьба отключить двухфакторную авторизацию действительно исходит от самого пользователя.

1. В разделе **Пользователи** личного кабинета кликните по имени пользователя, для которого следует отключить двухфакторную авторизацию.
2. В блоке **Аккаунт защищён** нажмите кнопку **Отключить**.
3. Введите код и нажмите **Подтвердить**.

После этого пользователь сможет авторизоваться в личном кабинете с помощью только логина и пароля. При необходимости он сможет снова [включить двухфакторную авторизацию](#) самостоятельно.

Сбросить пароль пользователя

1. В разделе **Пользователи** личного кабинета кликните по имени пользователя, для которого следует сбросить пароль.
2. В блоке **Сброс пароля** нажмите кнопку **Сбросить пароль**.
3. В появившемся диалоге подтвердите операцию, нажав кнопку **Сбросить пароль**.

На электронную почту пользователя будет отправлено письмо со ссылкой для установки нового пароля.

Удалить пользователя

1. В разделе **Пользователи** личного кабинета кликните по имени пользователя, которого следует удалить.
2. В блоке **Удалить пользователя** нажмите кнопку **Удалить аккаунт**.

3. В появившемся диалоге подтвердите операцию, нажав кнопку **Удалить аккаунт**.

Личный кабинет: Группы

Группы являются необходимым компонентом системы прав доступа, используемой в личном кабинете Curator. Чтобы разрешить пользователю доступ к тому или иному разделу личного кабинета, необходимо добавить пользователя в группу, для которой настроены необходимые [политики](#). Пользователь может входить в несколько групп. Группы могут быть связаны между собой так, чтобы политики одной группы автоматически добавлялись к другой.

Управление группами производится в разделе «Группы» личного кабинета.



ПРИМЕЧАНИЕ

В конфигурации по умолчанию этот раздел личного кабинета доступен только пользователям группы *Access Manager*.



ВАЖНО

При настройке прав следите за тем, чтобы хотя бы у одного из пользователей оставалась возможность менять настройки в разделах «Пользователи» и «Группы». При необходимости обратитесь к специалистам технической поддержки Curator, чтобы восстановить доступ.

Введение

Термины

В основе системы прав доступа в личный кабинет лежат три понятия.

- *Пользователь* — лицо (обычно сотрудник компании-клиента Curator), использующее для входа в личный кабинет свои собственные адрес электронной почты и пароль. Для аккаунта компании может быть настроено несколько пользователей. Просматривать и управлять учётными записями пользователей можно в разделе [Пользователи](#). Редактировать свою собственную учётную запись каждый пользователь может в разделе [Мой профиль](#).
- *Политика* — право на доступ к определённому разделу личного кабинета или [ресурсу](#). Некоторые виды политик допускают более тонкую настройку прав: например, право на добавление новых ресурсов не означает автоматически права на их удаление.
- *Группа* — набор пользователей, объединённых с целью выдачи им общих прав доступа в личный кабинет. Группа реализует связь «многие ко многим» между пользователями и настроенными политиками. Возможно также [включение групп друг в друга](#).

**ПРИМЕР**

Один из возможных подходов к организации прав доступа — создать группы, соответствующие разным отделам компании: «Отдел технической поддержки», «Отдел продаж» и т.п. Также можно создать отдельную группу «Старшие специалисты поддержки» и включить её в «Отдел технической поддержки», чтобы переиспользовать настроенные политики.

Виды политик и их настройки

Названия доступных видов политик примерно соответствуют названиям разделов личного кабинета. Например, существуют политики «Раздел 'Префиксы'», «Раздел 'Финансы'» и т.п.

Для некоторых видов политик требуется указать идентификатор конкретного ресурса, к которому будет выдан доступ. Например, при добавлении политики «Указанный ресурс: Настройки туннелей» указывается идентификатор домена. Такая политика не влияет на доступ к остальным доменам. При необходимости можно добавить несколько одинаковых политик с разными идентификаторами ресурсов.

Также при добавлении любой политики указывается, какие именно операции смогут совершать пользователи группы в выбранном разделе. Существуют четыре вида операций: *Create*, *Read*, *Update*, *Delete* (часть операций может быть неприменима к конкретной политике). Например, если при создании политики «Раздел 'Хранилище Сертификатов'» выбрать только операции *Read* и *Update*, то пользователи группы смогут видеть и обновлять существующие TLS-сертификаты, но не смогут добавлять или удалять их. Точный смысл каждой операции может немного различаться от раздела к разделу.

Конфигурация по умолчанию

По умолчанию для каждого клиентов Curator создаётся конфигурация из четырёх групп, как описано в таблице ниже. Пользователь, который создаётся первым, по умолчанию входит во все четыре группы, в том числе в группу «Access Manager», что позволяет ему создавать новых пользователей и включать их в существующие или новые группы.

Группа	Права
Technical	Просматривать и изменять настройки в разделах «Домены» (все подразделы), «Сервисы» (все подразделы), «Префиксы», «Ingress», «Хранилище сертификатов», «WAF», «Аналитика», «Заявки», «API токены». Просматривать настройки в разделах «Отчёты», «Пользователи», «Группы».
Finance	Просматривать и изменять настройки в разделах «Финансы», «Компания», «Заявки». Просматривать настройки в разделах «Пользователи», «Группы».

Administrative	Просматривать и изменять настройки в разделах «Аналитика», «Финансы», «Компания», «Заявки». Просматривать настройки в разделах «Домены» (все подразделы), «Сервисы» (все подразделы), «Префиксы», «Ingress», «Хранилище сертификатов», «WAF», «Аналитика», «Отчёты», «API токены», «Пользователи», «Группы».
Access Manager	Просматривать и изменять настройки в разделах «Пользователи», «Группы».

Посмотреть список групп

В разделе **Группы** личного кабинета отображается таблица со всеми группами текущего аккаунта. Для каждой группы отображаются её **Название**, а также **Количество политик**, **Количество пользователей** и **Количество групп**.

Рядом с заголовком столбца **Название** присутствует поле фильтра, с помощью которого вы можете быстро найти группы, в названии которых присутствует определённая подстрока.

Добавить группу

1. В разделе **Группы** личного кабинета нажмите кнопку **Добавить группу**.

2. В появившемся диалоге введите название для новой группы.

Нажмите **Далее**.

3. Укажите политики, которые будут назначены для новой группы. Этот шаг можно пропустить, нажав **Далее**.

Для добавления каждой новой политики:

1. Нажмите **Добавить политику**. Откроется диалог добавления политики.
2. Выберите политику, которую нужно добавить в группу.
3. Укажите идентификатор ресурса, если выбранная политика требует его (см. [Виды политик и их настройки](#)).
4. Поставьте чекбоксы рядом с названиями операций, права на которые должны быть у пользователей группы.
5. Нажмите **Сохранить**, чтобы завершить настройку новой политики и закрыть диалог.

После добавления политики вы можете нажать , чтобы вернуться в диалог и отредактировать политику. Чтобы отменить добавление политики, нажмите  рядом с её названием.

Чтобы перейти к следующему шагу, нажмите кнопку **Далее**.

6. Укажите привязанные группы — группы, к пользователям которых должны применяться политики новой группы. Этот шаг можно пропустить, нажав **Далее**.

Для привязки групп нажмите **Добавить группу**. В появившемся диалоге выберите одну или более групп из выпадающего списка и нажмите **Сохранить**. Чтобы отменить добавление группы, нажмите  рядом с её названием.

Чтобы перейти к следующему шагу, нажмите кнопку **Далее**.

7. Укажите пользователей, которые будут включены в новую группу. Этот шаг можно пропустить, нажав **Создать**.

Для добавления пользователей нажмите кнопку **Добавить пользователей**. В появившемся диалоге выберите одного или более пользователей из выпадающего списка и нажмите **Сохранить**. Чтобы отменить добавление пользователя, нажмите  рядом с его именем.

Чтобы завершить создание группы, нажмите кнопку **Создать**.

Переименовать группу

1. В разделе **Группы** личного кабинета нажмите на название группы, которую вы хотите переименовать.
2. Рядом с заголовком страницы нажмите .
3. В появившемся диалоге введите новое название для группы и нажмите **Изменить**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Добавить политику

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В блоке **Политики** нажмите кнопку **Добавить**. Откроется диалог добавления политики.
3. Выберите политику, которую нужно добавить в группу.
4. Укажите идентификатор ресурса, если выбранная политика его требует (см. [Виды политик и их настройки](#)).
5. Поставьте чекбоксы рядом с названиями операций, права на которые должны быть у пользователей группы.
6. Нажмите **Сохранить**, чтобы завершить настройку новой политики и закрыть диалог.
7. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Изменить политику

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В блоке **Политики** нажмите  напротив названия политики, которую вы хотите удалить.

3. В появившемся диалоге поставьте или снимите чекбоксы напротив операций **Create, Read, Delete, Update**.
4. Нажмите **Сохранить**, чтобы завершить настройку политики и закрыть диалог.
5. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить политику

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В блоке **Политики** нажмите  напротив названия политики, которую вы хотите удалить.
3. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить несколько политик

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. Поставьте чекбоксы возле нужных политик. Нажмите кнопку **Удалить**.
3. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Включить группу в другие группы

Группу можно включить в одну или несколько других групп. Это означает, что все политики, настроенные для текущей группы, будут также настроены для групп, в которые она включена.

Чтобы включить группу в другие группы:

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В блоке **Входит в группы** нажмите кнопку **Добавить**.
3. В появившемся диалоге выберите одну или более групп из выпадающего списка и нажмите **Сохранить**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить группу из других групп

1. В разделе **Группы** личного кабинета нажмите на название дочерней группы.

2. В блоке **Входит в группы** нажмите  напротив одного из названий.
3. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Добавить пользователя в группу

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В блоке **Пользователи** нажмите кнопку **Добавить**.
3. В появившемся диалоге выберите одного или более пользователей из выпадающего списка и нажмите **Сохранить**.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить пользователя из группы

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В блоке **Пользователи** нажмите  напротив имени пользователя.
3. Подтвердите действие, нажав **Удалить** в появившемся диалоге.
4. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Удалить группу

1. В разделе **Группы** личного кабинета нажмите на название группы.
2. В правом верхнем углу экрана нажмите кнопку **Удалить группу**.
3. Подтвердите действие, нажав **Удалить** в появившемся диалоге.

Личный кабинет: Уведомления (настройка учётной записи)



ПРИМЕЧАНИЕ

Эта страница описывает настройки уведомлений для конкретной учётной записи пользователя. О настройке порогов уведомлений для ресурса см. [Уведомления \(настройка ресурса\)](#).

В разделе «Уведомления» личного кабинета можно включить или отключить определённые типы уведомлений от Curator для вашей учётной записи пользователя.

Поставьте или снимите нужные чекбоксы, чтобы изменить список получаемых уведомлений. Чтобы сохранить изменения, нажмите кнопку **Сохранить** в уведомлении в нижней части экрана.

Включённые уведомления будут отправляться на адрес электронной почты, указанный в [вашем профиле](#).

Обратите внимание, что следующие виды уведомлений отправляются при возникновении проблем, которые могут приводить к некорректной работе ваших ресурсов:

- «Отмена автообновления Let's Encrypt сертификата»,
- «Превышение порога трафика»,
- «Превышение установленного размера ЧС»,
- «Истечение срока действия сертификата».

Перед отключением этих видов уведомлений мы рекомендуем убедиться, что они включены хотя бы для одной другой учётной записи.

Личный кабинет: Мой профиль

В разделе «Мой профиль» личного кабинета вы можете управлять настройками учётной записи, под которой авторизованы в данный момент. Этот раздел доступен для любой учётной записи.

Посмотреть информацию о пользователе

Откройте раздел **Мой профиль**. На открывшейся странице будет отображена информация о пользователе.

Поля с информацией разделены на три группы.

- **Основная информация**
 - **Имя и Фамилия** пользователя.
 - **Группы** — список [групп](#), в которые входит учётная запись пользователя.
- **Контакты**
 - **Адрес эл. почты**, указанный при [создании учётной записи пользователя](#).
 - **Skype** — аккаунт пользователя в Skype для оперативной связи (если указан).
 - **Номер телефона, Добавочный номер, Мобильный телефон** — информация для оперативной связи по телефону (если указана).
- **Настройки языка**
 - **Язык** — язык интерфейса личного кабинета для пользователя.
 - **Язык отчётов** — язык генерации [отчётов](#) для пользователя (если получение отчётов включено).

Изменить информацию о пользователе

1. В разделе **Мой профиль** нажмите .
2. Отредактируйте информацию о пользователе.
 - **Имя и Фамилия** пользователя.
 - **Skype** — аккаунт пользователя в Skype для оперативной связи (не обязательно).
 - **Номер телефона, Добавочный номер, Мобильный телефон** — информация для оперативной связи по телефону (не обязательно).
3. Нажмите кнопку **Сохранить**.

Изменить настройки языка пользователя

1. В разделе **Мой профиль** нажмите .
2. Задайте необходимые настройки.
 - **Язык** — язык интерфейса личного кабинета.
 - **Язык отчётов** — язык **отчётов**, которые вы будете получать на электронную почту. Чтобы не получать отчётов, выберите вариант **Не отправлять**.
3. Нажмите кнопку **Сохранить**.

Включить двухфакторную аутентификацию

По умолчанию ваша учётная запись в личном кабинете Curator защищена паролем. Чтобы усилить защиту, вы можете включить *двухфакторную аутентификацию*. В этом случае, чтобы войти в личный кабинет, вы должны будете вводить не только электронную почту и пароль, но и одноразовый шестизначный код, сгенерированный на мобильном устройстве. Для генерации кодов можно использовать Google Authenticator на **iOS** или **Android** или другое приложение, работающее по протоколу TOTP.

Чтобы включить двухфакторную аутентификацию:

1. Перейдите в раздел **Мой профиль**.
2. В блоке **Защитите свой аккаунт** нажмите кнопку **Начать**.

После этого сгенерируются и отобразятся секретный ключ и QR-код.
3. Запустите приложение на мобильном устройстве. Добавьте в него учётную запись, введя секретный ключ или отсканировав QR-код из личного кабинета.
4. В личном кабинете нажмите кнопку **Далее**.
5. В поле **ПИН-код** введите код, сгенерированный мобильным приложением, и нажмите **Подтвердить**.

Отключить двухфакторную аутентификацию



ПРИМЕЧАНИЕ

Для отключения двухфакторной аутентификации необходимо иметь доступ к мобильному устройству с приложением, которое генерирует временные коды. Если это невозможно, отключить двухфакторную аутентификацию для вас может пользователь с полным доступом.

1. Перейдите в раздел **Мой профиль**.
2. В блоке **Аккаунт защищён** нажмите кнопку **Отключить**.
3. В поле **ПИН-код** введите код, сгенерированный мобильным приложением, и нажмите **Подтвердить**.

Сменить пароль



ПРИМЕЧАНИЕ

Для установки нового пароля необходимо ввести действующий пароль. Если вы забыли действующий пароль, [сбросить пароль для вас может пользователь с полным доступом](#).

1. Перейдите в раздел **Мой профиль**.
2. В блоке **Сменить пароль** нажмите кнопку .
3. В поле **Пароль** введите действующий пароль.
4. В поле **Новый пароль** введите новый пароль. В следующем поле повторите новый пароль.
5. Нажмите кнопку **Сохранить**.

Настройка SSO через OAuth 2.0 / OpenID Connect

Введение

CURATOR поддерживает аутентификацию пользователей через федерацию удостоверений с использованием протоколов OAuth 2.0 и [OpenID Connect](#) (OIDC).

Это стандартный механизм реализации единого входа (Single Sign-On, SSO) — технологии, которая позволяет пользователям получать доступ к нескольким системам без необходимости использовать отдельные логины и пароли для каждой из них.

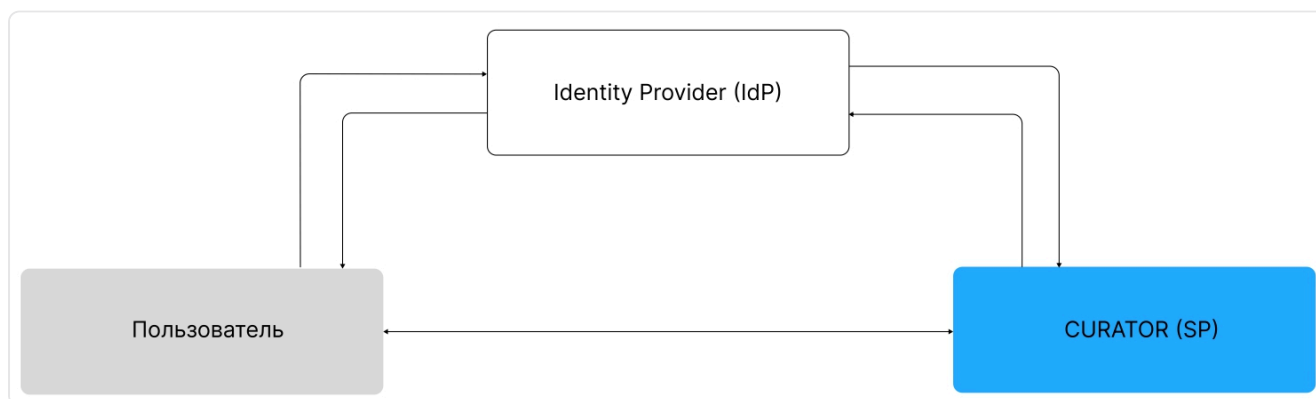
Такой подход называется федерацией удостоверений: информация об учетных данных пользователей хранится на стороне доверенного поставщика удостоверений — Identity Provider (IdP), а CURATOR выступает в роли Service Provider (SP) и делегирует аутентификацию внешней системе.

Если в вашей организации уже используется система централизованного управления пользователями и доступом, например Microsoft Active Directory, Keycloak или Google Workspace, вы можете использовать её для аутентификации сотрудников в личном кабинете CURATOR. В этом случае:

- не требуется создавать отдельные учетные записи для пользователей в CURATOR;
- управление доступами остается на стороне вашей инфраструктуры;
- пользователи входят в систему с использованием корпоративных учетных данных.

Схема работы SSO

Ниже приведена упрощённая схема аутентификации пользователя через SSO с использованием OpenID Connect.



Компоненты схемы

- **Пользователь** — сотрудник организации
- **CURATOR (SP)** — сервис, предоставляющий доступ
- **Identity Provider (IdP)** — система аутентификации

Поток аутентификации

1. Пользователь инициирует вход через SSO;
2. CURATOR перенаправляет пользователя в IdP;
3. Пользователь проходит аутентификацию;
4. IdP возвращает пользователя с токеном;
5. CURATOR проверяет токен и получает данные пользователя;
6. Применяется сопоставление групп;
7. Пользователь получает доступ.

Ключевые особенности

- Аутентификация полностью происходит на стороне IdP;
- CURATOR не получает доступ к паролю пользователя и обращается к IdP с IP адреса 185.65.149.86;
- Взаимодействие реализовано через redirect (через браузер);
- Доступ определяется на основе атрибутов, переданных IdP;
- Существующие группы будут перезаписаны на те, что в CURATOR передаст IdP;
- Доступ в личный кабинет для ранее созданных учетных записей будет сохранен.

Обзор

В личном кабинете CURATOR доступна настройка SSO через OpenID Connect.

После настройки:

- пользователи аутентифицируются через IdP;
- не создаются локальные учетные записи;
- доступ управляется через группы и политики.

Как работает OpenID Connect

OpenID Connect — это протокол, который добавляет аутентификацию поверх OAuth 2.0.

Предварительные требования

Перед началом настройки:

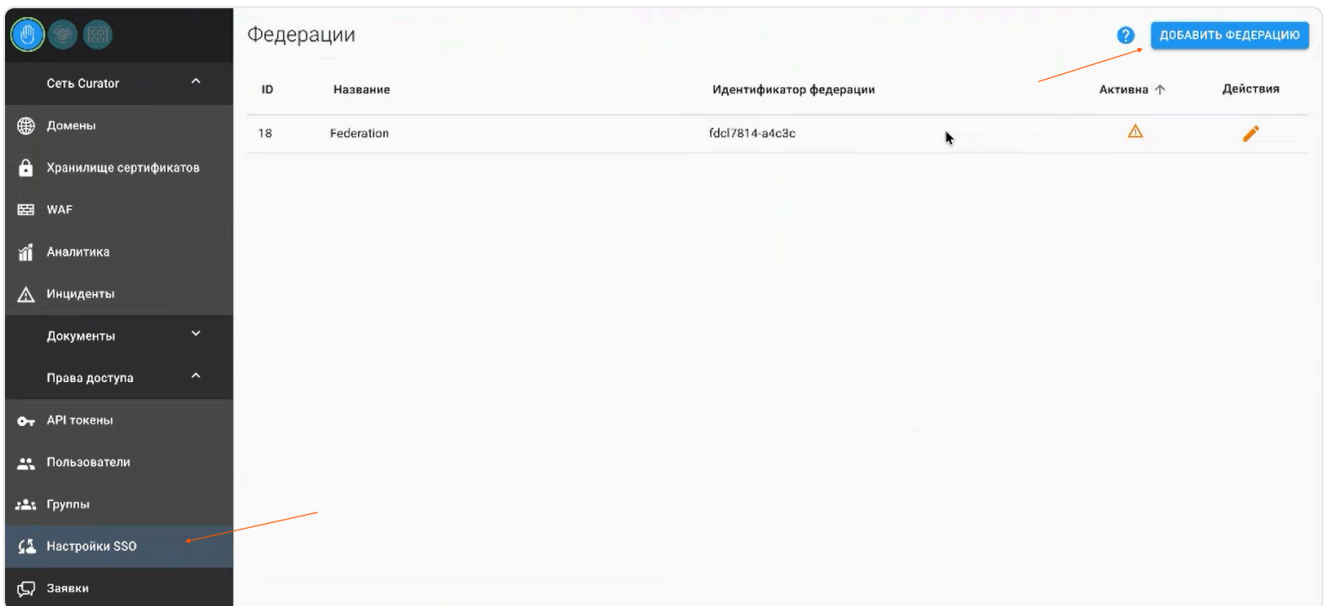
- настроен Identity Provider с поддержкой OIDC;
- доступны:
 - Client ID

- Client Secret
- OIDC endpoints или Discovery URL

Настройка SSO в CURATOR

1. Переход к настройкам SSO

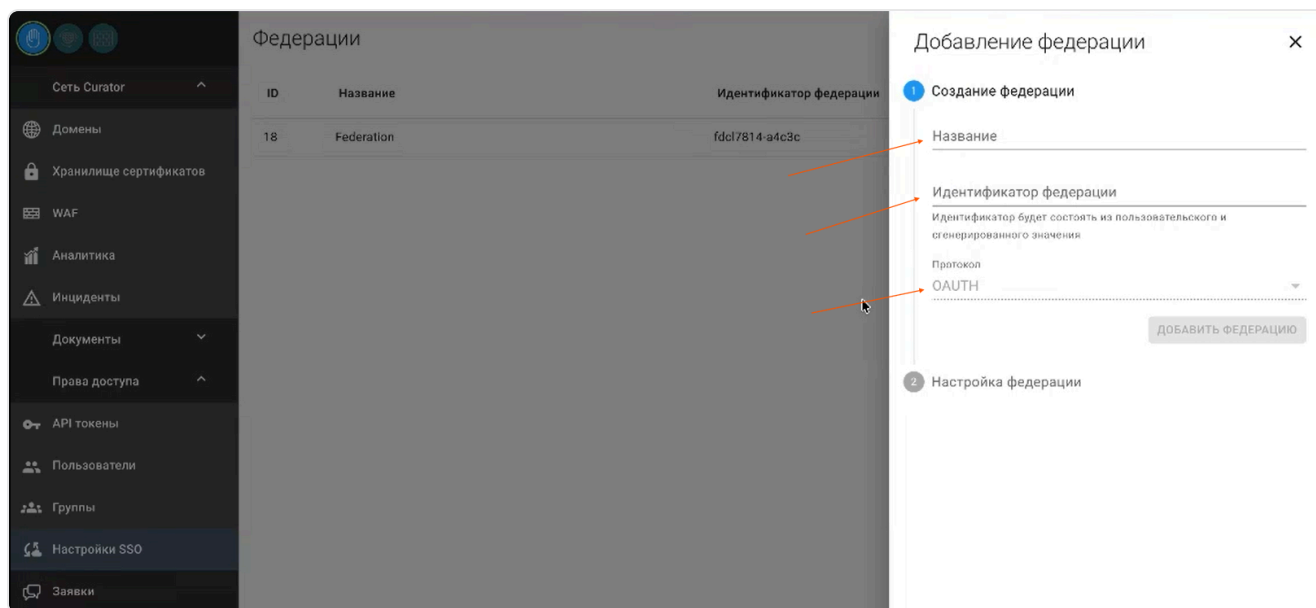
Перейдите в раздел **Настройки SSO** и нажмите **Добавить федерацию**.



2. Создание федерации

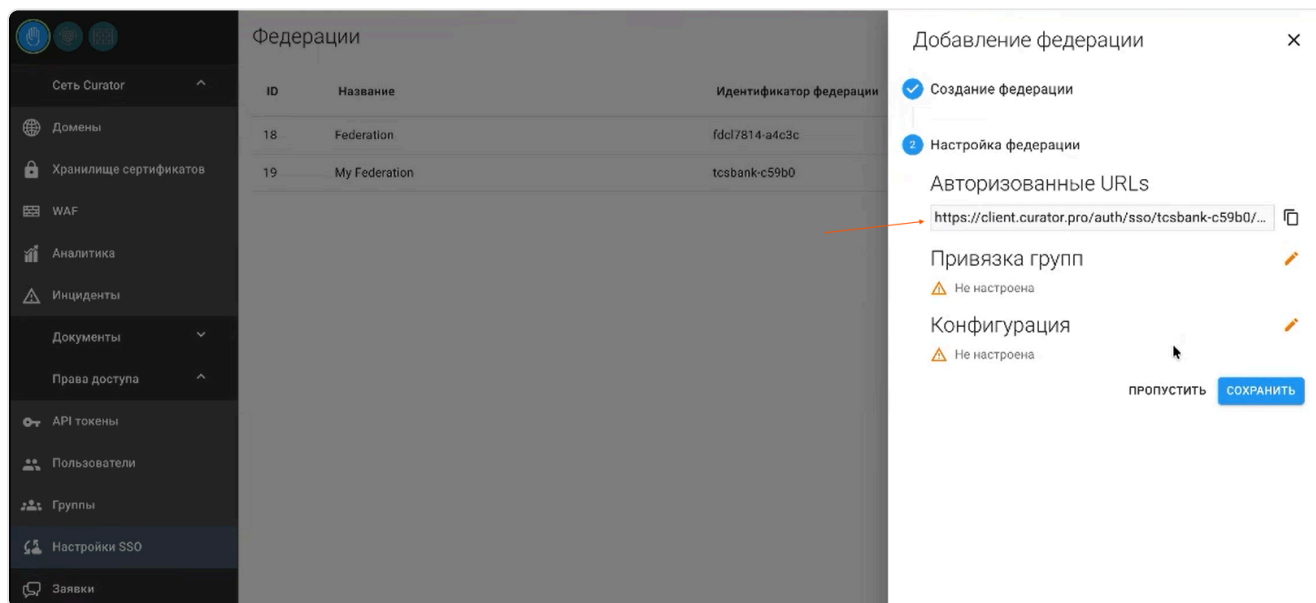
Укажите параметры:

- Название — произвольное;
- Идентификатор федерации (slug). Идентификатор будет дополнен случайным суффиксом;
- Протокол — OAuth.



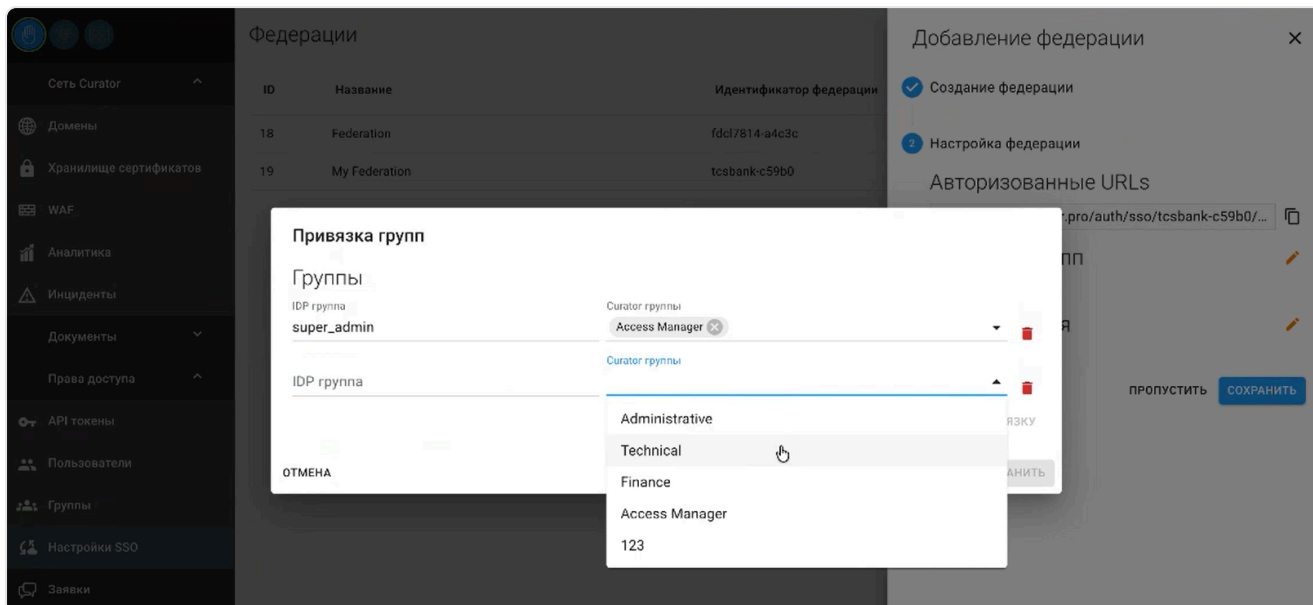
3. Получение Authorization URL

После создания федерации отобразится Authorization URL (Redirect URI). Этот URL необходимо указать в настройках вашего Identity Provider.



4. Настройка сопоставления групп

Перейдите в раздел **Привязка групп** и настройте соответствие групп IdP и групп CURATOR.

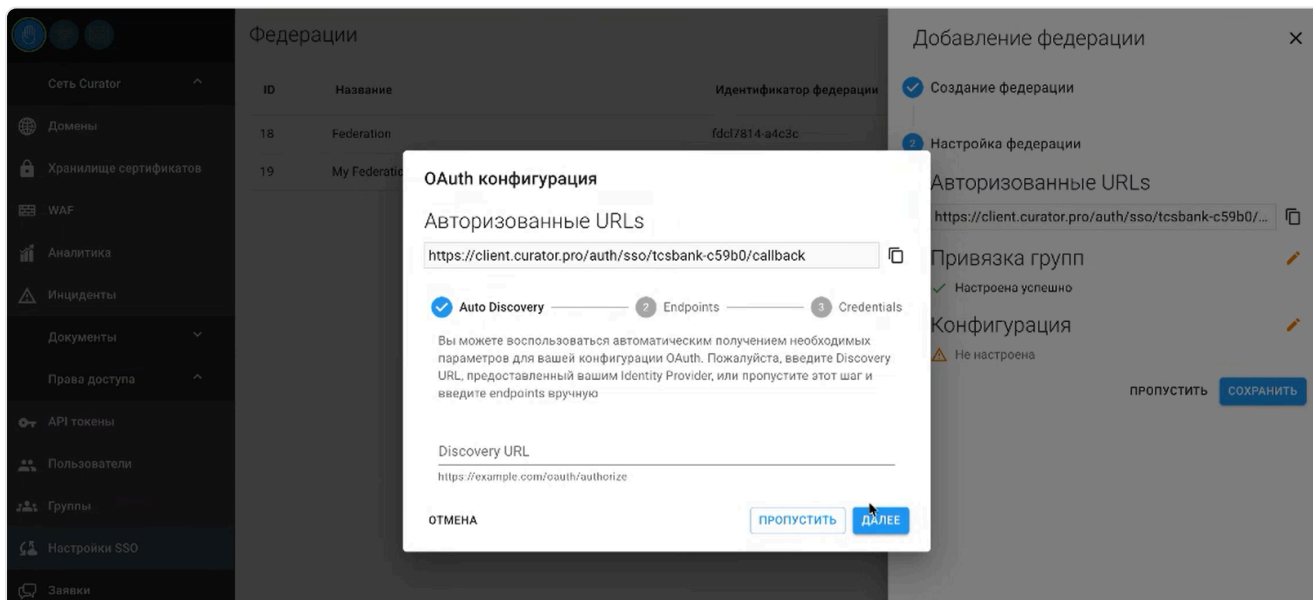


ВНИМАНИЕ! Без настройки привязки групп пользователи, входящие через SSO, не будут получать роли и группы. Этот шаг обязателен для корректной работы.

Убедитесь, что в маппинге присутствует группа, которая соответствует группе CURATOR с правами на управление пользователями (по умолчанию Access Manager). Иначе администраторы могут потерять доступ к управлению пользователями при следующем входе через SSO.

5. Настройка OAuth конфигурации

Перейдите в раздел **Конфигурация**.



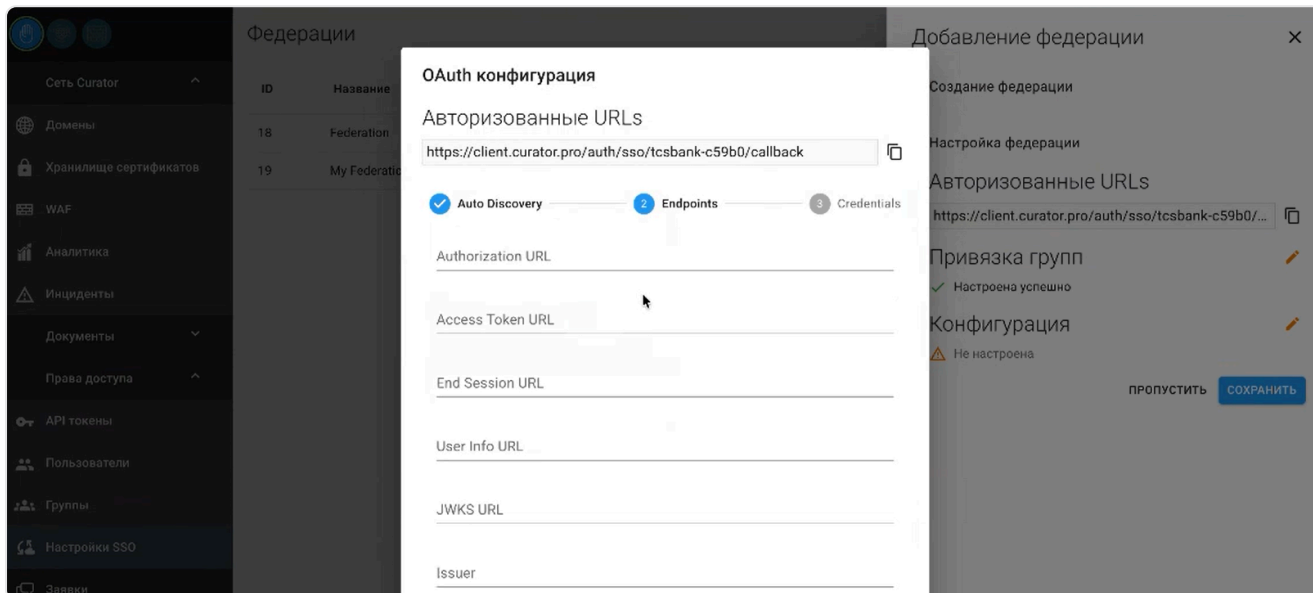
6. Указание Endpoints

Укажите endpoints вашего Identity Provider:

- Authorization Endpoint

- Token Endpoint
- UserInfo Endpoint
- JWKS Endpoint
- Logout Endpoint

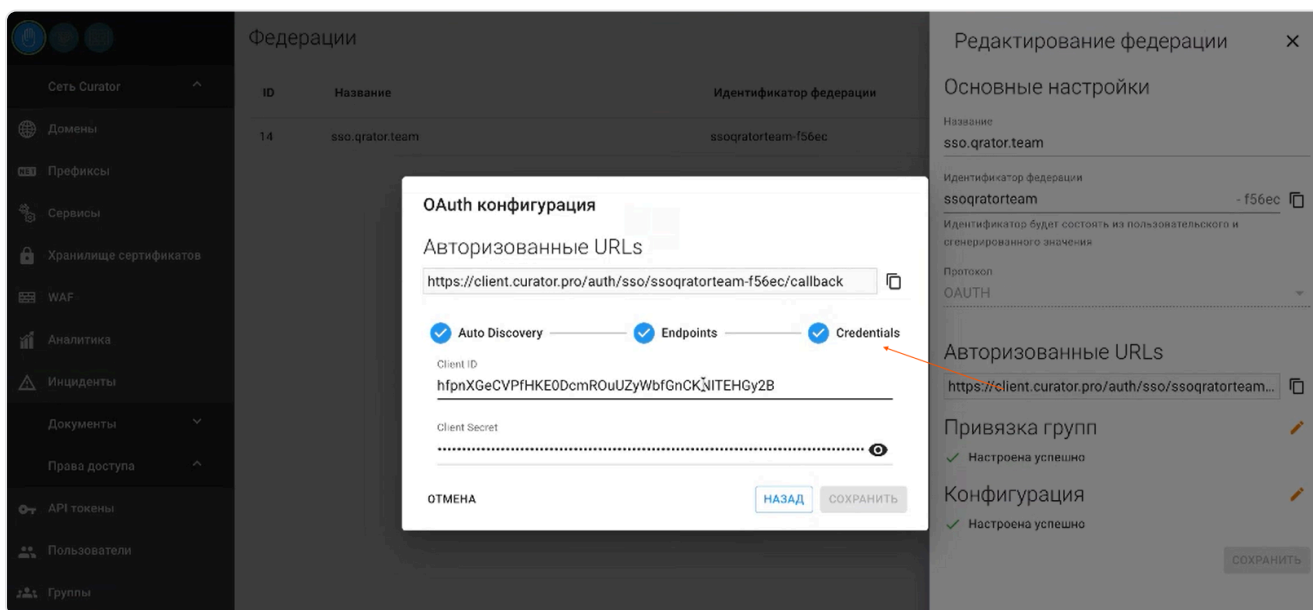
Или используйте Discovery URL (`.well-known/openid-configuration`), параметры подтянутся автоматически.



7. Указание учетных данных (Credentials)

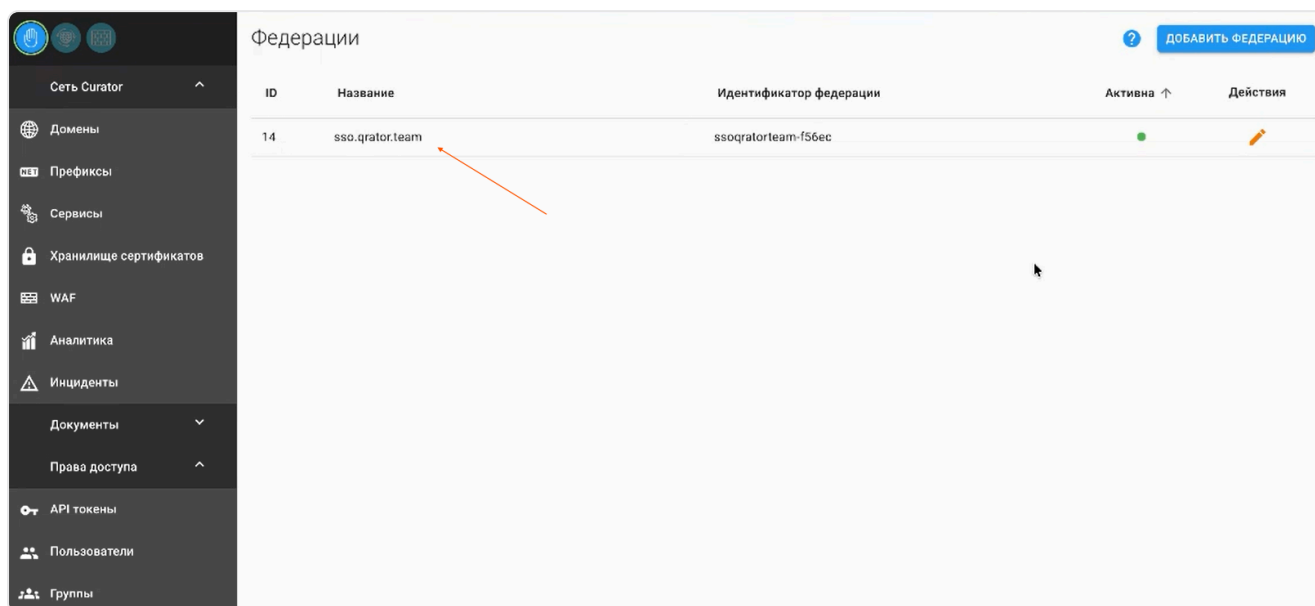
Введите параметры доступа:

- Client ID
- Client Secret



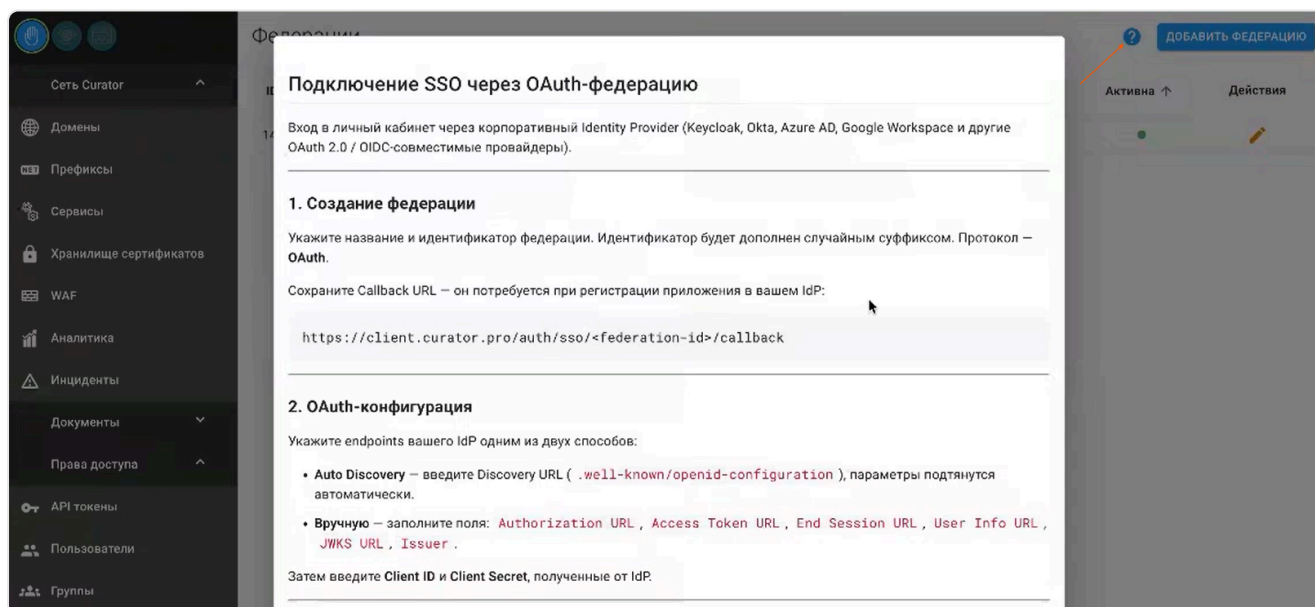
8. Завершение настройки

Сохраните конфигурацию. После этого федерация появится в списке и станет доступна для использования.



Дополнительная информация

В интерфейсе личного кабинета доступна встроенная инструкция по настройке SSO.



04

Справка и поддержка

Дополнительные HTTP-заголовки

4.1 СПРАВКА И ПОДДЕРЖКА

Дополнительные HTTP-заголовки

Обратный HTTP-прокси и обратный WebSocket-прокси добавляют к каждому HTTP-запросу, проксируемому от клиента, дополнительные заголовки.

Информация, содержащаяся в этих заголовках, может быть полезна для логирования запросов и последующей отладки возникающих проблем.

- **X-Forwarded-For**

Пример значения: `1.2.3.4, 5.6.7.8`

Содержит IP-адрес, с которого запрос пришёл на обратный прокси Curator, а также список всех предыдущих IP-адресов, добавленных в этот заголовок, если такие были.

Если в запросе, пришедшем на обратный прокси Curator, не было заголовка **X-Forwarded-For**, то он будет добавлен. Такой заголовок будет содержать только IP-адрес пользователя, от которого пришёл запрос.

Если в запросе, пришедшем на обратный прокси Curator, уже был заголовок **X-Forwarded-For**, то к существующему содержимому будет добавлен IP-адрес, от которого пришёл запрос. Таким образом, заголовок будет содержать и IP-адрес пользователя, и адреса всех прокси, через которые он дошёл до обратного прокси Curator. В качестве разделителя используются запятые и следующие за ними пробелы.

**ПРИМЕЧАНИЕ**

Если какое-то оборудование в вашей сети также модифицирует заголовок **X-Forwarded-For** перед передачей запроса серверу, то может оказаться затруднительно установить, с какого именно IP-адреса из перечисленных запрос пришёл в Curator. Если необходимо установить это точно, воспользуйтесь заголовком **X-Qrator-IP-Source**.

- **X-Q-DomId**

Пример значения: `11169`

Содержит числовой идентификатор домена, для которого выполняется проксирование. Он совпадает с идентификатором, указанным в списке доменов в личном кабинете, но в HTTP-заголовке указывается без буквы d.

- **X-Qrator-IP-Source**

Пример значения: `1.2.3.4`

Содержит IP-адрес пользователя, от которого пришёл запрос. Совпадает с последним IP-адресом из заголовка **X-Forwarded-For**.

- `X-Qrator-RequestID`

Пример значения: `f4b16a6bf0bcc8bebc394a2824d5d569`

Содержит уникальный идентификатор обработанного запроса. Если какая-то обнаруженная вами проблема связана с конкретными запросами, вы можете сообщить идентификаторы этих запросов специалистам технической поддержки для детального изучения.

- `X-Qrator-TCP-Info`

Пример значения: `51890, 69493, 10151`

Содержит информацию о TCP-сессии. Состоит из трёх чисел.

Первое число сообщает порт отправителя, с которого были отправлены TCP-сегменты в сеть Curator.

Второе и третье числа — это значения RTT и RTTVar, вычисленные согласно [RFC 2988](#).



Актуальная версия документации — docs.curator.pro