

Table of Contents

Table of Contents	1
Настройка политики безопасности	2
О политике безопасности	3
Настройка параметров безопасности WAF	4
Настройка исключений для WAF-правил	12
Работа с заголовком X-Request-Id	14
Фильтрация закодированного трафика	15
Обработка запросов с данными в формате JSON	16
Обработка запросов с данными в формате XML	19
Защита WebSocket-соединений	22
Профили ответа	24
Обработка дополнительных HTTP-заголовков	25

Version: 7.7.x

Product: WAF

Documentation: 

Политика безопасности в UserGate WAF задает параметры и уровень защиты веб-сервисов. Она позволяет продукту обнаруживать и блокировать различные угрозы, включая наиболее опасные атаки из списка OWASP Top 10, а также фильтровать запросы, содержащие данные в различных форматах. В зависимости от настроенных параметров политика безопасности может обеспечивать:

- защиту веб-сервисов организации от угроз с помощью экспертных WAF-правил;
- фильтрацию трафика, закодированного по стандарту Base64;
- защиту WebSocket-соединений;
- обработку дополнительных HTTP-заголовков;
- проверку и парсинг запросов с данными в формате JSON;
- проверку и парсинг запросов с данными в формате XML.

Настройка параметров безопасности WAF

Technology: WAF

Version: 7.7.x

Product: WAF

В UserGate WAF можно настроить политику безопасности, обеспечивающую защиту опубликованных веб-сервисов от атак. Механизмы защиты, разработанные экспертами UserGate, позволяют обнаруживать и блокировать различные угрозы, включая наиболее опасные атаки из списка OWASP Top 10. Настройка защиты выполняется в WAF-профилях — наборах WAF-правил и механизмов управления ими.

Структура WAF-профиля

WAF-профиль включает следующие элементы:

- **WAF-правило** — выражение на языке UserGate Policy Language (UPL), описывающее условия обнаружения угроз безопасности. Правило анализирует веб-трафик (запросы и ответы) и защищает веб-сервисы от атак и утечек конфиденциальных данных. При срабатывании правила выполняется назначенное действие (например, блокирование трафика). WAF-правила бывают системные (поставляются в пакете экспертизы) и пользовательские. В WAF-профиле системные WAF-правила сгруппированы по двум признакам: технологии (что именно защищает правило) и слои (от каких типов атак защищает правило).
- **Технология** — инструмент, который используется при разработке и эксплуатации защищаемого веб-сервиса (язык программирования, фреймворк, СУБД, веб-сервер и т. п.). Технологии формируют характерные признаки в трафике: структуру HTTP-запросов/ответов, наборы заголовков, параметры сессий и другие артефакты. Поэтому информация о технологиях позволяет настроить политику безопасности под конкретный веб-сервис и снизить количество ложных срабатываний. В UserGate WAF технологии служат признаком группировки WAF-правил: включение технологии в WAF-профиле делает доступными все связанные с ней WAF-правила, но не активирует их. Активация правил зависит от включенных слоев.
- **Слой** — конструкция, предназначенная для группировки WAF-правил по типам обнаруживаемых атак, их активации и настройки очередности проверки трафика WAF-правилами. Отключение всего слоя исключает из проверки все входящие в него WAF-правила. Слои бывают системные (создаются компанией UserGate) и персональные.

Таким образом, для защиты веб-сервиса в WAF-профиле необходимо включить соответствующие технологии и нужные слои, чтобы применялись WAF-правила, защищающие эти технологии от выбранных типов атак.

О системных WAF-правилах

UserGate WAF поставляется с набором системных WAF-правил, обеспечивающих защиту веб-сервисов от различных атак. Системные WAF-правила доступны для загрузки с серверов UserGate после активации лицензии и затем регулярно обновляются и дополняются командой экспертов UserGate, если настроено расписание автообновлений. Подробнее об автообновлении — в разделе [«Настройка общих параметров»](#).

Важно! Для получения регулярных обновлений системных WAF-правил необходима лицензия на модуль Security Updates.

Примечание При обновлении экспертизы новые и обновленные системные WAF-правила (как в WAF-профилях, так и в списке глобальных правил) переводятся в режим журналирования — в качестве их действия устанавливается No action. Журналирование включается автоматически, чтобы администратор мог проанализировать поведение новых версий правил перед включением блокировки. После обновления экспертизы следует проверить действия WAF-правил и при необходимости вернуть блокирующие действия.

Все системные WAF-правила отображаются в разделе **Политика безопасности → Глобальные правила**. Вы можете просматривать сведения о WAF-правилах (например, в каком слое они находятся, какое назначено действие при срабатывании или какой выбран профиль ответа), изменять их параметры, выполнять поиск и сортировку.

В WAF-профилях отображаются только те правила, которые соответствуют включенным технологиям и слоям.

Каждое WAF-правило защищает веб-сервисы от угроз определенного уровня. В системе выделено три уровня угроз. Уровень угрозы, от которой защищает правило, обозначается цветовым индикатором: зеленый (1) — низкий уровень, синий (2) — средний, желтый (3) — высокий. Это позволяет быстро оценить критичность правила и приоритет его применения при настройке защиты.

Системные WAF-правила группируются в системные слои, которые также формируются разработчиками решения. Критерием группировки WAF-правил в слои являются следующие типы атак:

- Abuse of Functionality;
- Authentication/Authorization Attacks;
- Buffer Overflow;
- Command Execution;
- Denial of Service;
- Detection Evasion;
- Directory Indexing;
- HTTP Parser Attack;
- HTTP Response Splitting;
- Information Leakage;
- LDAP Injection attempt;

- SQL-injection;
- Malicious File Upload;
- Microsoft OWA;
- Other Application Attacks;
- Path Traversal;
- Predictable Resource Location;
- Remote File Include;
- Server Side Code Injection;
- Session Hijacking;
- Trojan/Backdoor/Spyware;
- Vulnerability Scan;
- XPath Injection;
- Cross site scripting (XSS);
- XML External Entity (XXE).

Действия в системных WAF-правилах

При срабатывании системного WAF-правила к трафику применяется действие, назначенное этому правилу:

- No action — при срабатывании правила система фиксирует событие (если включено журналирование), но не предпринимает действий, блокирующих трафик. При этом в процессе обработки трафик может модифицироваться в соответствии с условиями правила, например в запрос могут быть добавлены заголовки.
- Pass — все правила, расположенные в слое под сработавшим правилом, пропускаются, и происходит переход к проверке WAF-правилами следующего слоя (при его наличии). Если следующего слоя нет, проверка завершается пропуском запроса или ответа.
- Deny — все правила, расположенные в слое под сработавшим правилом, пропускаются, и происходит переход к проверке WAF-правилами следующего слоя (при его наличии). Если следующего слоя нет, проверка завершается блокированием запроса или ответа.
- Force deny — является окончательным результатом обработки, и перехода к проверке WAF-правилами следующего слоя не происходит. Проверка завершается блокированием запроса или ответа.
- Force pass — является окончательным результатом обработки, и перехода к проверке WAF-правилами следующего слоя не происходит. Проверка завершается пропуском запроса или ответа.

Таким образом, приоритет force-действий выше, что следует учитывать, настраивая последовательность слоев.

Настройка и подключение WAF-профиля

В WAF-профиле настраиваются технологии, слои и WAF-правила, обеспечивающие защиту публикуемых веб-сервисов. Вы можете настроить несколько WAF-профилей и подключить их к разным правилам публикации, реализуя таким образом необходимые сценарии защиты одного или нескольких веб-сервисов.

Правило публикации с подключенным WAF-профилем проверяет веб-трафик выбранного веб-сервиса на наличие угроз. При срабатывании WAF-правила, для которого включено журналирование, UserGate WAF записывает информацию об обнаружении атаки или другого события ИБ. Эти данные доступны для просмотра и анализа в разделе **Атаки**. Подробнее — в разделе «[Просмотр обнаруженных атак](#)».

Общий сценарий настройки и подключения WAF-профиля следующий:

1. Проверьте, что лицензия UserGate WAF Security Updates активирована и скачаны пакеты экспертизы WAF. Подробнее о лицензии — в разделе «[Лицензирование UserGate WAF](#)».
2. Убедитесь, что для ваших веб-сервисов настроены серверы публикации и созданы правила публикации, настроенные на проверку трафика этих веб-сервисов. Подробнее — в разделе «[Публикация веб-сервисов](#)».
3. Создайте WAF-профиль, включите необходимые технологии и слои с WAF-правилами. Подробнее — в разделе «[Создание и настройка WAF-профиля](#)».
4. Если необходимо, настройте WAF-правила, чтобы выполнять только необходимые проверки трафика. Подробнее — в разделе «[Настройка системных WAF-правил](#)».
5. Подключите созданный WAF-профиль к правилу публикации, настроенному на проверку трафика соответствующего веб-сервиса. Подробнее — в разделе «[Подключение WAF-профиля к правилу публикации](#)».

В UserGate WAF предусмотрено быстрое создание настроенного WAF-профиля по шаблону:

- **Наблюдение** — подходит для отладки политики безопасности. По умолчанию включены все WAF-правила для всех технологий и слоев, для всех WAF-правил выбрано действие No Action, ведется журналирование срабатываний правил. Такой профиль позволяет отслеживать поведение всех WAF-правил без блокирования трафика, фиксировать ложные срабатывания и по результатам вносить изменения в политику безопасности. Сведения о срабатывании правил доступны на странице **Атаки**.
- **Базовая защита** — предназначен для защиты веб-сервисов от угроз высокого уровня. По умолчанию включены все WAF-правила,

выявляющие угрозы 3-го уровня, для этих правил выбрано блокирующее действие Deny, ведется журналирование срабатываний правил. Сведения о срабатывании правил доступны на странице **Атаки**.

- **Максимальная защита** — предназначен для выявления и блокирования всех видов угроз. По умолчанию включены все WAF-правила, для всех правил выбрано блокирующее действие Deny, ведется журналирование срабатываний правил. Сведения о срабатывании правил доступны на странице **Атаки**.
- **Пользовательский** — предназначен для самостоятельной настройки профиля «с нуля». По умолчанию включены технологии All systems и General Database, все слои выключены.

WAF-профиль, созданный по любому шаблону, остается доступным для внесения изменений. Например, в созданном по шаблону для наблюдения WAF-профиле вы можете настроить блокирование трафика любыми правилами.

В WAF-профиле можно использовать как системные слои, содержащие экспертизу UserGate, так и персональные слои с пользовательскими правилами. Подробнее — в разделе «[Создание персонального слоя и пользовательских WAF-правил](#)».

Созданные WAF-профили отображаются в разделе **Настройки → Политика безопасности → WAF-профили**. Профили можно редактировать, копировать и удалять.

Быстрое создание WAF-профиля

Чтобы создать WAF-профиль без дополнительной настройки:

1. В разделе **Политика безопасности → WAF-профили** нажмите **Добавить**.
2. В окне **WAF-профиль** выберите шаблон **Наблюдение**, **Базовая защита** или **Максимальная защита** и нажмите **Создать**.
3. В окне **WAF-профиль** на вкладке **Общие** при необходимости измените название профиля и описание.
3. Нажмите **Сохранить**.

Будет создан WAF-профиль с параметрами, предустановленными в выбранном шаблоне. Вы можете вносить дополнительные изменения в профиль или сразу перейти к его подключению к правилу публикации.

Создание и настройка WAF-профиля

Чтобы создать и настроить WAF-профиль:

1. В разделе **Политика безопасности → WAF-профили** нажмите **Добавить**.
2. В окне **WAF-профиль** выберите один из шаблонов и нажмите **Создать**.
3. В окне **WAF-профиль** на вкладке **Общие** укажите название профиля и при необходимости описание.
4. На вкладке **Технологии** включите технологии, которые используются при создании и эксплуатации веб-сервисов, которые будет защищать этот профиль.
5. При необходимости выполните оптимизацию профиля на основе рекомендаций по технологиям. Подробнее — в разделе «[Применение рекомендаций по технологиям в WAF-профиле](#)».
5. На вкладке **Слои** включите нужные системные слои. В счетчике активных правил отобразится общее количество включенных правил.

Примечание После сохранения WAF-профиля включенные слои автоматически поднимаются вверх в своих группах. Порядок в этом случае определяется так: первый в списке включенный слой поднимается на первое место, на второе место поднимается следующий по списку включенный слой, и т. д. В рамках одной группы вы можете перемещать слои по списку, чтобы таким образом настроить очередность проверки трафика системными WAF-правилами.

6. При необходимости добавьте персональный слой с пользовательскими правилами. Подробнее — в разделе «[Создание персонального слоя и пользовательских WAF-правил](#)».

Примечание Пользовательские слои и правила имеют более высокий приоритет, чем системные правила, включенные в WAF-профиле.

7. На вкладке **WAF-правила** при необходимости настройте WAF-правила. Например, вы можете выключить все правила, блокирующие угрозы 1-го (низкого) уровня. Подробнее — в разделе «[Настройка системных WAF-правил](#)».

8. Нажмите **Сохранить**.

Теперь созданный WAF-профиль можно подключить к правилу публикации.

Подключение WAF-профиля к правилу публикации

Чтобы подключить WAF-профиль к правилу публикации и начать проверку трафика в соответствии с настроенной политикой безопасности:

1. В разделе **Политика сервисов → Правила публикации** создайте или выберите правило публикации. Подробнее — в разделе «[Публикация веб-сервисов](#)».
2. На вкладке **Профили безопасности** установите флажок **Включить защиту веб-приложений (WAF)** и выберите из списка нужный WAF-профиль.

Примечание Если нужного профиля нет в списке, вы можете создать его, нажав в конце списка «Создать и выбрать новый объект».

3. Завершите настройку других параметров правила публикации и сохраните изменения.

Правило публикации настроено на защиту веб-сервиса, указанного в его параметрах.

Настройка WAF-профиля по рекомендованным технологиям

В WAF-профиле можно вручную управлять защищаемыми технологиями или использовать рекомендации по технологиям.

Даже если защищаемые технологии в WAF-профиле уже выбраны вручную, их состав необходимо периодически пересматривать. Со временем технологический стек веб-сервисов может измениться: одни WAF-правила становятся избыточными и замедляют проверку трафика, а для новых технологий существующих механизмов защиты может быть недостаточно.

Чтобы поддерживать WAF-профиль в соответствии с текущим технологическим стеком и исключать лишние проверки, в системе предусмотрена функция обнаружения технологий. С помощью специального пакета экспертизы UserGate WAF анализирует трафик, соответствующий условиям выбранных правил публикации, и определяет используемые технологии.

На основе обнаруженных технологий система формирует рекомендации по настройке WAF-профилей. Их применение помогает поддерживать актуальный список механизмов защиты, оптимизировать использование ресурсов и обеспечивать высокий уровень защиты веб-сервисов.

Для настройки WAF-профиля по рекомендованным технологиям необходимо:

- в правиле публикации включить функцию обнаружения технологий;
- в WAF-профиле применить рекомендации по технологиям.

Включение обнаружения технологий

Чтобы включить обнаружение технологий:

1. В разделе **Политика сервисов → Правила публикации** выберите правило публикации и нажмите **Редактировать**.

ПримечаниеЕсли правило публикации с нужными параметрами еще не создано, вы можете создать его по кнопке «Добавить» и выполнить в нем описанные ниже действия.

2. В окне **Настройка правила публикации** на вкладке **Общие** в блоке **Обнаружение технологий** установите флажок **Определять технологии защищаемого веб-сервиса**.

ПримечаниеДля работы этой функции необходим пакет экспертизы WAF Tech detector. Если пакет экспертизы не был скачан ранее, его можно скачать в блоке «Обнаружение технологий» по кнопке «Обновить».

3. Сохраните изменения.

4. При необходимости повторите шаги 1-3 для других правил публикации. Например, если для обработки трафика разных веб-сервисов, публикуемых с помощью одного сервера публикации, настроены разные правила публикации.

Результаты обнаружения технологий будут отображены в журнале технологий. Подробнее — в разделе «[Журнал технологий](#)».

ПримечаниеПри достижении порогового значения высокой нагрузки на CPU или оперативную память обнаружение технологий автоматически отключается. Это позволяет снизить нагрузку на систему и сохранить ее стабильную работу.

Применение рекомендаций по технологиям в WAF-профиле

Чтобы применить рекомендации по обнаруженным технологиям в WAF-профиле:

1. В разделе **Политика безопасности → WAF-профили** выберите WAF-профиль и нажмите **Редактировать**.

ПримечаниеЕсли WAF-профиль с нужными параметрами еще не создан, вы можете создать его по кнопке «Добавить» и выполнить в нем описанные ниже действия.

2. В окне **WAF-профиль** на вкладке **Технологии** в блоке **Выберите правила публикации** выберите из раскрывающегося списка одно или несколько правил публикации, которые настроены на обнаружение технологий тех же веб-сервисов, которые защищает выбранный WAF-профиль. Таблица со списком технологий обновится, для каждой обнаруженной технологии в столбце **Статус** отобразится запись **Обнаружена**, а также отобразятся рекомендации по включению или выключению технологий.

Внимание!Правила публикации, выбранные в WAF-профиле, применяются как временный фильтр. Поэтому после сохранения профиля выбранные правила не сохраняются.

3. В соответствии с рекомендациями выполните одно из действий:

- вручную включите или выключите технологии;
- нажмите кнопку **Применить рекомендации**, в окне **Подтверждение рекомендаций** проверьте рекомендованные изменения и нажмите **Подтвердить**, чтобы сразу применить все рекомендации по включению и выключению технологий.

Важно!Отсутствие технологии в результатах обнаружения не означает, что веб-сервис ее не использует. Технология может не обнаруживаться в анализируемом трафике, например, если соответствующие данные пока не передавались в запросах или ответах. Поэтому рекомендации по отключению необнаруженных технологий следует рассматривать с осторожностью. Перед отключением технологии убедитесь, что она действительно не используется веб-сервисом.

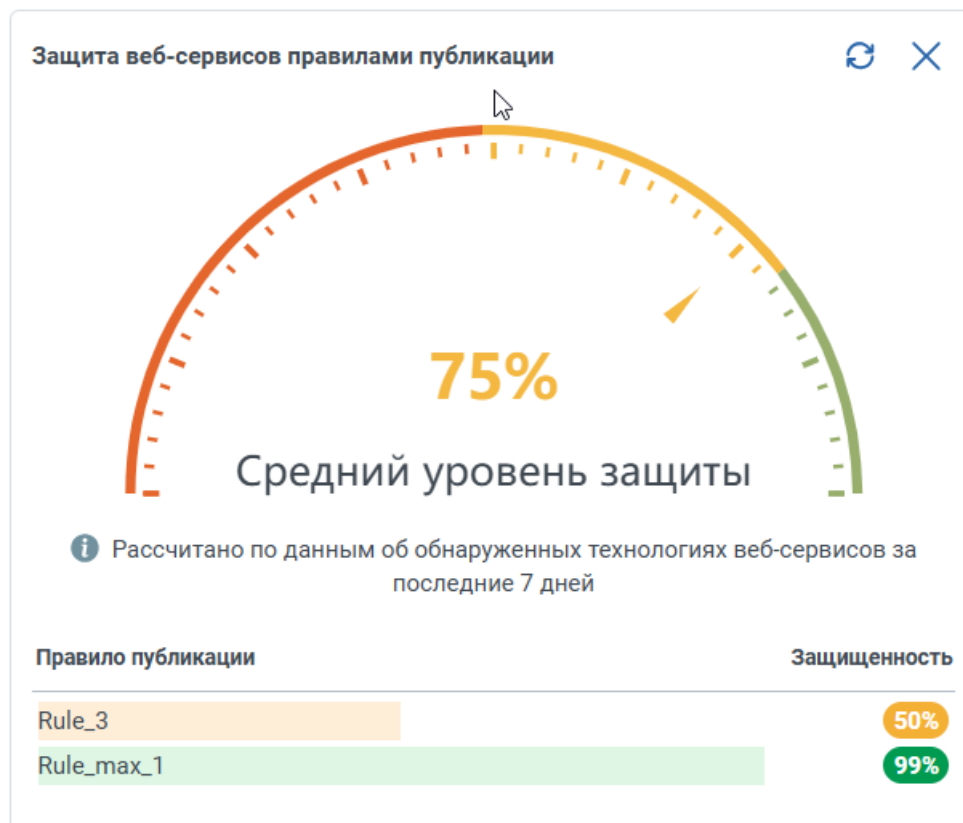
4. Сохраните изменения в WAF-профиле.

Управление уровнем защищенности веб-сервисов

Применение рекомендаций по обнаруженным технологиям позволяет контролировать уровень защищенности веб-серверов с помощью виджета **Защита веб-сервисов правилами публикации**. Виджет показывает, насколько конфигурация WAF-профиля соответствует технологиям веб-сервисов. Если уровень защищенности снижается, вы можете обновить WAF-профиль в соответствии с актуальными рекомендациями.

Чтобы добавить виджет на дашборд:

1. Перейдите на страницу **Дашборды**.
2. Перейдите на вкладку нужного дашборда, если их несколько, и нажмите **Добавить виджет**.
3. Выберите виджет **Защита веб-сервисов правилами публикации** и нажмите **Добавить**.



При расчете уровня защищенности учитываются правила публикации, для которых одновременно:

- включено обнаружение технологий, и технологии были обнаружены в трафике, обработанном этими правилами;

Примечание Информация об обнаруженных технологиях доступна на странице «Журналы и отчеты» в разделе «Журнал технологий».

- выбран WAF-профиль безопасности.

Эти же правила отображаются на виджете.

Остальные правила публикации с подключенными WAF-профилями также продолжают защищать соответствующие веб-сервисы. Однако если для правила не включено обнаружение технологий, оно не участвует в расчете уровня защищенности на виджете.

Уровень защищенности показывает, насколько WAF-профиль соответствует актуальному списку обнаруженных технологий веб-сервисов. Если в WAF-профиле применены все рекомендованные технологии, уровень защищенности составляет 99%. Значение 99% является максимальным для виджета.

Уровень защищенности веб-сервисов на виджете обозначается цветовыми индикаторами:

- **Красный** — низкий уровень защиты: в WAF-профиле включено менее 50% рекомендуемых технологий.
- **Желтый** — средний уровень защиты: в WAF-профиле включено менее 80% рекомендуемых технологий.
- **Зеленый** — высокий уровень защиты: в WAF-профиле включено более 80% рекомендуемых технологий.

Виджет отображает уровень защищенности веб-сервисов за последние 7 дней. Со временем уровень защищенности может снижаться, так как может изменяться набор технологий веб-сервиса. Например, при разработке или обновлении веб-сервиса могут появиться новые технологии, которые ранее не использовались. После того как новая технология будет обнаружена, она учитывается при оценке уровня защищенности. Если для этой технологии в подключенном WAF-профиле не приняты рекомендации по включению, уровень защищенности снижается.

Примечание Период в 7 дней также влияет на учет правил, в которых функцию обнаружения технологий сначала включили, а затем отключили. Такие правила продолжают участвовать в расчете уровня защищенности до окончания этого периода.

Таким образом, значение на виджете позволяет отслеживать изменения в составе технологий веб-сервисов и своевременно выявлять технологии, для которых защита еще не настроена. Чтобы повысить защищенность веб-сервисов, необходимо нажать на соответствующее правило публикации, чтобы перейти в окно свойств WAF-профиля, подключенного к этому правилу, и затем обновить профиль в соответствии с актуальными рекомендациями по обнаруженным технологиям.

Рассмотрим конфигурацию, на основе которой сформированы данные, отображаемые на виджете на рисунке выше:

- Созданы три правила Rule_max_1, Rule_max_2 и Rule_3, настроенные на публикацию трех разных веб-сервисов.
Внимание!Если два или более правила, в которых включено обнаружение технологий, настроены на публикацию одного веб-сервиса, в расчете уровня защищенности участвует только правило, которое первым обрабатывает трафик, соответствующий условиям публикации.
- Для правила публикации Rule_max_1 включено обнаружение технологий; в качестве профиля безопасности подключен WAF-профиль Profile_1, созданный по шаблону для максимальной защиты; в журнале технологий есть записи о технологиях, обнаруженных в трафике, обработанном этим правилом. Правило используется как для обнаружения технологий, так и для защиты первого веб-сервиса.
- Для правила публикации Rule_max_2 обнаружение технологий выключено, но подключен WAF-профиль Profile_2, также созданный по шаблону для максимальной защиты; в профиле применены рекомендации по технологиям в соответствии с правилом Rule_max_1. Правило используется для защиты второго веб-сервиса, но не участвует в обнаружении технологий и расчете уровня защищенности на виджете.
- Для правила публикации Rule_3 включено обнаружение технологий; подключен WAF-профиль Profile_3, созданный по шаблону для наблюдения; в журнале технологий есть записи о технологиях, обнаруженных в трафике, обработанном этим правилом; в профиле включены не все рекомендованные технологии. Правило используется для отслеживания срабатываний WAF-правил по рекомендованным технологиям без блокирования трафика.

На виджете отображается информация только о Rule_max_1 и Rule_3, поскольку для них включено обнаружение технологий и в журнале технологий есть соответствующие записи об обнаруженных технологиях.

Для правила Rule_max_1 уровень защищенности составляет 99%, так как в WAF-профиле Profile_1, созданному по шаблону для максимальной защиты, по умолчанию включены все технологии, в том числе и рекомендованные. Работу этого WAF-профиля можно оптимизировать, выключив лишние технологии в соответствии с рекомендациями. При этом уровень защищенности 99% сохранится. Но после отключения лишних технологий уровень защищенности может измениться, если в дальнейшем в веб-сервисе будет обнаружена новая технология, для которой защита в WAF-профиле не настроена.

Хотя правило Rule_3 не участвует в защите веб-сервиса, информация об уровне защищенности тоже отображается на виджете. Такой режим может использоваться для предварительной оценки работы WAF-профиля и наблюдения за срабатываниями WAF-правил. Для Rule_3 уровень защищенности ниже, поскольку в WAF-профиле Profile_3 применена только часть рекомендованных технологий.

Правила публикации с подключенными WAF-профилями, но без включенного обнаружения технологий, например Rule_max_2, не отображаются на виджете и не участвуют в расчете уровня защищенности.

Если необходимо отслеживать уровень защищенности веб-сервисов, рекомендуется включать обнаружение технологий в соответствующих правилах публикации и подключать к ним WAF-профили.

Работа с системными WAF-правилами

Поиск системных WAF-правил

Для быстрого поиска в списке WAF-правил предусмотрены быстрые фильтры по основным параметрам. Также вы можете формировать собственные поисковые запросы для выполнения более сложной фильтрации. Структура и логика поисковых запросов для фильтрации WAF-правил та же, что и в поисковых запросах для журналов. Подробнее о логических операторах в поисковых запросах — в разделе [«Поиск и фильтрация данных»](#).

Важно!При формировании поискового запроса рекомендуется для одного параметра WAF-правила указывать одно значение или несколько значений через оператор OR. В противном случае результаты поиска могут быть неверными. Примеры корректного запроса: technology = "PHP" или technology = "PHP" OR technology = "WordPress". Пример некорректного запроса: technology = "PHP" AND technology = "WordPress".

Для фильтрации WAF-правил по поисковому запросу используются следующие параметры.

Название параметра в веб-консоли	Параметр	Описание
Уровень угрозы	threatLevel	Уровень угрозы, от которой защищает WAF-правило: 1: низкий; 2: средний; 3: высокий
ID правила	ruleId	Идентификатор WAF-правила
Название	name	Название WAF-правила
Ссылка	reference	Ссылки на внешние ресурсы с описаниями уязвимостей
Время последнего обновления	lastUpdate	Время последнего обновления правила на серверах UserGate

Название параметра в веб-консоли	Параметр	Описание
Профиль ответа	responseProfile	Название профиля ответа
Системный слой	systemLayer	Системный слой, к которому относится WAF-правило
Пакет	package	Название пакета экспертизы, в который входит данное WAF-правило
Действие	action	Действие правила: No action, Pass, Deny, Force deny, Force pass
Состояние правила	enabled	Активация правила: true, false
Журналирование	loggingStatus	Включение или отключение журналирования событий, связанных с правилом: true, false
Технология	technology	Название технологии защиты
Исключения	exceptions	Название исключения, добавленного к правилу

Настройка системных WAF-правил

В веб-консоли UserGate WAF вы можете настраивать системные WAF-правила двумя способами:

- через настройку WAF-профиля;
- через список глобальных WAF-правил.

От выбранного способа зависит, как изменения будут влиять на работу WAF-профилей. Подробнее — ниже в разделах о каждом способе настройки.

Для изменения доступны следующие параметры системного WAF-правила:

- Включение или выключение WAF-правила.
- Исключения для WAF-правила. Подробнее об исключениях — в разделе « [Настройка исключений для WAF-правил](#) ».
- Журналирование событий, связанных с работой WAF-правила.

Примечание По умолчанию журналирование событий включено во всех системных WAF-правилах.

- Действие, которое будет выполнено при срабатывании WAF-правила.
- Профиль ответа, который вернется в ответ на клиентский запрос, если сработает WAF-правило с блокирующим действием. Подробнее о профилях ответа — в разделе « [Профили ответа](#) ».
- Отмена всех изменений и возвращение значений параметров правила к изначальным.

Настройка системного WAF-правила в WAF-профиле

При настройке системного WAF-правила в WAF-профиле параметры правила изменяются только в этом профиле и имеют более высокий приоритет, чем параметры в списке глобальных правил. Например, если в профиле Example для правила Rule1 действие No Action заменено на Pass, это значение сохранится, даже если в списке глобальных правил для правила Rule1 будет выбрано действие Force pass.

Чтобы изменить параметры системного WAF-правила в WAF-профиле:

1. В разделе **WAF-профили** создайте по кнопке **Добавить** или выберите из списка WAF-профиль.
2. В окне **WAF-профиль** на вкладке **WAF-правила** выберите WAF-правило и нажмите **Переопределить**.
3. В окне **Переопределение правил** измените нужные параметры.
4. Сохраните все изменения.

Примечание Вы также можете изменить параметры сразу нескольких WAF-правил. Для этого в окне «WAF-профиль» на вкладке «WAF-правила» нужно выбрать несколько WAF-правил, затем нажать «Переопределить», в окне «Переопределение правил» изменить нужные параметры и сохранить изменения.

Настройка системного WAF-правила в списке глобальных правил

При настройке системного WAF-правила через список глобальных правил параметры WAF-правила изменятся только в тех WAF-профилях, в которых не выполнялось переопределение параметров этого правила.

Чтобы изменить параметры системного WAF-правила через список глобальных правил:

1. В разделе **Глобальные правила** выберите системное WAF-правило и нажмите **Редактировать**.
2. В окне **Редактирование правил** измените нужные параметры.
3. Сохраните изменения.

Примечание Вы также можете изменить параметры сразу нескольких WAF-правил. Для этого в списке глобальных правил нужно выбрать несколько WAF-правил, затем нажать «Редактировать», в окне «Редактирование правил» изменить нужные параметры и сохранить изменения.

Восстановление значений по умолчанию

При настройке политики безопасности может понадобиться восстановить исходные состояния отдельных WAF-правил. В зависимости от того, значения параметров какого WAF-правила нужно вернуть к исходным, необходимо перейти в одно из следующих окон и нажать **Восстановить значения по умолчанию**:

- В окне **WAF-профиль** на вкладке **WAF-правила** — чтобы вернуть параметры правил в профиле к состоянию глобальных правил.
- В разделе **Глобальные правила** — чтобы восстановить исходное состояние выбранных правил в глобальном списке.

Создание персонального слоя и пользовательских WAF-правил

Чтобы более гибко управлять политикой безопасности, вы можете создавать персональные слои, содержащие пользовательские WAF-правила, написанные на языке UPL. Созданные персональные слои отображаются в разделе **Политика безопасности → Персональные слои**. Вы можете просматривать и редактировать их, выполнять поиск по названию слоя.

Чтобы создать персональный слой с пользовательским WAF-правилом:

1. В разделе **Персональные слои** нажмите **Добавить**.

Примечание Вы также можете создать персональный слой при создании или изменении WAF-профиля, нажав в окне свойств профиля на вкладке «Слои» кнопку «Добавить персональный слой».

2. В окне **Свойства персонального слоя** укажите название.

3. В области **Редактирование выражения** введите UPL-выражение, содержащее правила проверки трафика. Подробнее о синтаксисе UPL-выражений — в разделе [«UserGate Policy Language»](#).

Примечание Область представляет собой встроенный редактор с подсветкой ключевых слов и выражений и проверкой синтаксиса UPL.

4. Если необходимо, включите журналирование пользовательского правила. Для этого в области редактирования UPL-выражения добавьте свойство "rule_log(true)" или "rule_log(yes)".

5. Нажмите **Проверить выражение** и, если необходимо, внесите исправления.

6. Для активации правила добавьте свойство "enabled(true)".

7. Сохраните изменения.

Созданный персональный слой автоматически добавится во все WAF-профили и будет по умолчанию выключен. Чтобы UserGate WAF выполнял проверку веб-трафика с помощью пользовательских WAF-правил, при настройке WAF-профиля необходимо включить нужные персональные слои и затем подключить этот WAF-профиль к правилу публикации. Подробнее о настройке и подключении WAF-профилей — в разделе [«Настройка и подключение WAF-профиля»](#).

Настройка исключений для WAF-правил

Version: 7.7.x

Product: WAF

По умолчанию блокирующие WAF-правила применяются ко всем запросам и ответам, содержащим значения, соответствующие условиям WAF-правила. Вы можете настроить исключения, чтобы скорректировать работу WAF-правил.

Исключения помогут предотвратить ложные срабатывания и обеспечить гибкое управление обработкой трафика. Например, они позволяют игнорировать легитимный трафик от систем мониторинга, партнерских API и доверенных поисковых ботов (Googlebot, YandexBot), а также запросы с надежными реферерами или специфическими заголовками Accept от внутренних систем.

Исключения задаются условиями, при выполнении которых WAF-правило пропускает запрос или ответ без обработки. Если для WAF-правила есть исключение, оно проверяется в первую очередь. Если WAF-правило содержит несколько исключений, достаточно срабатывания любого исключения, чтобы прекратить обработку.

Для создания исключений используются UPL-условия и логические операторы, аналогичные операторам фильтрации данных. Подробнее о UPL-условиях и операторах — в разделах «[Условия](#)» и «[Поиск и фильтрация данных](#)».

Вы можете настраивать исключения по следующим условиям.

Условие	Описание
http.method	Проверка HTTP-метода
src.ip	Проверка IP-адреса
http.request.body.re2	Проверка тела HTTP-запроса
http.response.body.re2	Проверка тела HTTP-ответа
http.request.body, http.request.body.nocase	Проверка тела HTTP-запроса
http.response.body, http.response.body.nocase	Проверка тела HTTP-ответа
request.header.Host	Проверка HTTP-заголовка запроса Host
url.path	Проверка URL
request.header.User-Agent	Проверка заголовка useragent
request.header.Referer	Проверка запроса на доверенные рефереры
request.header.Accept	Проверка заголовка Accept
request.header.Cookie	Проверка заголовка запроса Cookie на значение
qparam	Проверка значения параметров запроса
upl.condition	Поле для произвольного исключения, написанного на языке UPL. Выражения записываются в поле значений через пробел, который работает как логическое «И»

Создание исключения

Чтобы создать исключение:

- В разделе **Настройки** → **Политика безопасности** → **Исключения** нажмите **Добавить**.
- В окне **Свойства исключения** укажите название исключения.
- Если необходимо вести запись сработавших исключений, установите флажок **Журналирование**.
- Выберите из списка условие, затем выберите доступный для него логический оператор и укажите одно или несколько значений.

Примечание Вы можете добавить несколько условий в одно исключение. В этом случае исключение сработает, если при проверке

запроса или ответа выполнены все указанные условия.

5. Сохраните изменения.

Исключение создано. Чтобы оно сработало, его следует применить к выбранным WAF-правилам.

Применение исключений

Созданные исключения можно применить к WAF-правилам двумя способами:

- **Через настройку WAF-профиля.** Исключения, добавленные в WAF-правила через настройку WAF-профиля, применяются только в рамках этого профиля. Таким образом, для одного WAF-правила, включенного в несколько WAF-профилей, можно применить собственный набор исключений в каждом из этих профилей. Если к WAF-правилу уже были применены исключения, их набор будет изменен только в выбранном WAF-профиле.
- **Через настройку WAF-правила, выбранного в общем списке WAF-правил.** Исключения, добавленные в WAF-правило через общий список WAF-правил, применяются только в тех WAF-профилях, использующих это WAF-правило, в которые не были добавлены исключения через настройку WAF-профиля.

Чтобы применить исключения через настройку WAF-профиля:

1. В разделе **Настройки → Политика безопасности → WAF-профили** выберите WAF-профиль.
2. В окне **WAF-профиль** нажмите название слоя с WAF-правилами, к которым требуется применить исключения.
3. В окне свойств слоя в секции **Правила** нажмите **Настройка правил**.
4. В окне **Настройка правил** выберите WAF-правило и нажмите **Переопределить**.
5. В окне **Переопределение правил** в секции **Исключения** в колонке **Доступны** выберите одно или несколько предварительно созданных исключений и нажмите значок плюса.
6. Сохраните изменения.

Примечание Вы также можете применить исключения сразу к нескольким WAF-правилам. Для этого в окне «Настройка правил» нужно выбрать несколько WAF-правил и затем нажать «Переопределить». В секции «Исключения» необходимо выбрать «Перезаписать», после чего станет доступным добавление исключений. После сохранения изменений добавленные исключения применятся ко всем выбранным WAF-правилам. Если в блок «Выбранные» не добавлено ни одно исключение, но выбрана перезапись исключений, все ранее добавленные исключения будут удалены из выбранных WAF-правил.

Чтобы применить исключения через настройку WAF-правила:

1. В разделе **Настройки → Политика безопасности → Правила** выберите WAF-правило и нажмите **Редактировать**.
2. В окне **Редактирование правил** в секции **Исключения** в колонке **Доступны** выберите одно или несколько предварительно созданных исключений и нажмите значок плюса.
3. Сохраните изменения.

Примечание Вы также можете применить исключения сразу к нескольким WAF-правилам. Для этого в списке нужно выбрать несколько WAF-правил и затем нажать «Редактировать». В секции «Исключения» необходимо выбрать «Перезаписать», после чего станет доступным добавление исключений. После сохранения изменений добавленные исключения применятся ко всем выбранным WAF-правилам. Если в блок «Выбранные» не добавлено ни одно исключение, но выбрана перезапись исключений, все ранее добавленные исключения будут удалены из выбранных WAF-правил.

Примененные исключения отобразятся в свойствах WAF-правила в общем списке WAF-правил в столбце **Исключения**.

Информация о сработавших исключениях доступна на странице атак: для WAF-правил со сработавшим исключением в столбце **Действие** отображается значение **No action**, а в столбце **Исключения** появляется соответствующий значок. При наведении на него курсора отображается название сработавшего исключения. Подробнее о просмотре информации о сработавших WAF-правилах — в разделе [«Просмотр обнаруженных атак»](#).

Работа с заголовком X-Request-Id

Product: WAF

Version: 7.7.x

X-Request-Id — вспомогательный опциональный заголовок HTTP, который содержит уникальный идентификатор запроса. Этот идентификатор позволяет трассировать отдельные HTTP-запросы при решении проблем в работе веб-сервисов.

Значение идентификатора запроса является случайным, не содержит никакой персональной информации о пользователе и генерируется для каждого отдельного HTTP-запроса, что исключает опасность нарушения приватности пользователя.

В UserGate WAF идентификатор запроса используется для корреляции HTTP-запросов и записей журнала веб-доступа и журнала срабатывания правил WAF в рамках одного соединения. Функциональность доступна в версии 7.4.0 и выше.

UserGate WAF проверяет входящие HTTP-запросы на наличие заголовка X-Request-Id и значения идентификатора запроса. Если заголовок X-Request-Id отсутствует, UserGate WAF добавляет его в запрос и генерирует уникальное значение идентификатора запроса. Если HTTP-запрос приходит в UserGate WAF с уже существующим заголовком X-Request-Id, то UserGate WAF заменяет его значение на собственное сгенерированное уникальное значение.

Далее запрос передается на анализ и дальнейшую обработку в соответствии с правилами и политиками безопасности в UserGate WAF. Значение идентификатора запроса сохраняется в записях журнала веб-доступа.

При срабатывании правила WAF клиенту возвращается ответ с идентификатором запроса в качестве значения заголовка X-Request-Id. В записях журнала срабатывания сохраняется значение идентификатора запроса.

В веб-интерфейсе администратора в разделе **Атаки**, а также в разделе **Журналы и отчеты** на вкладке **Журнал веб-доступа** есть колонка **Идентификатор запроса**, где отображается значение этого индикатора. Поддерживается функция фильтрации событий в журнале по идентификатору запроса.

Фильтрация закодированного трафика

Version: 7.7.x

Product: WAF

Двоичные данные могут передаваться в закодированном виде через каналы, предназначенные только для передачи текста. С помощью стандарта кодирования Base64 любой файл преобразуется в строку текста и передается по протоколам, поддерживающим только текстовый формат. Стандарт Base64 используется например для кодирования вложений электронной почты или для встраивания графических, видео- или аудиоданных в веб-разработку.

Некоторые атаки на веб-приложения также используют стандарт кодирования Base64 для обхода фильтров межсетевых экранов, в том числе используется многократное кодирование, затрудняющее анализ исходных данных. Например, в случае SQL-внедрения выполняется кодирование SQL-запроса в Base64, чтобы обойти сигнатурный анализ. Как правило, эти данные передаются в параметрах URL, cookies и заголовках HTTP-запросов.

В UserGate WAF вы можете использовать правила публикации для декодирования и фильтрации таких данных.

Поддерживается декодирование следующих элементов HTTP-запроса:

- путь из URL;
- значения Cookies;
- значения в заголовках HTTP-запросов;
- тело запроса/ тело ответа, если в заголовке content type указан MIME-тип application/x-www-form-urlencoded;
- параметры из тела POST-запроса или из URL GET-запроса.

Чтобы настроить фильтрацию закодированного трафика:

1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте правило. Подробнее о создании и настройке правила публикации — в разделе «[Публикация веб-сервисов](#)».
2. В окне **Настройка правила публикации** на вкладке **Профили безопасности** установите флажок **Включить защиту веб-приложений (WAF)** и выберите WAF-профиль, в соответствии с которым декодированные данные будут подвергаться сигнатурному анализу. После выбора WAF-профиля станет доступной вкладка **Base64**.
3. На вкладке **Base64** установите флажки для тех элементов клиентского запроса, которые следует декодировать.
4. Укажите количество итераций декодирования для многократно закодированных данных. Максимальное значение — 5.
5. Сохраните изменения.

При срабатывании правила публикации будет выполнена попытка декодирования выбранных элементов HTTP-запроса, а в записях журнала событий сохранится информация об изменении состояния декодированных параметров.

Version: 7.7.x

Product: WAF

Documentation: 

Веб-сервисы и API часто используют формат JSON для обмена данными. Если UserGate WAF будет обрабатывать HTTP-запрос с JSON-телом как обычный текст, не учитывая его структуру, это может привести к пропуску угроз. Для корректной проверки таких запросов в UserGate WAF предусмотрены разбор тела запроса и проверка соответствия данных структуре JSON. Эти параметры настраиваются в JSON-профилях.

JSON-профиль, подключенный к правилу публикации, обеспечивает:

- пропуск только легитимных запросов с данными в формате JSON;
- проверку соответствия данных заданным JSON-схемам и отклонение запросов с нестандартной структурой;
- контроль размера, сложности и глубины вложенности данных с помощью лимитов;
- разбор (парсинг) структуры JSON для последующей проверки тела запроса WAF-правилами;
- журналирование событий, связанных с проверкой данных в формате JSON.

О данных в формате JSON

JSON (JavaScript Object Notation) — текстовый формат для представления структурированных данных. В HTTP-запросах данные в формате JSON передаются в теле запросов POST, PUT или PATCH с заголовком Content-Type: application/json или аналогичным.

Пример HTTP-запроса с JSON.

```
POST /api/users HTTP/1.1
Host: example.com
Content-Type: application/json
Content-Length: 200
```

```
{
  "user": {
    "username": "Ivan",
    "email": ["ivan_1@example.com", "ivan_2@example.com"]
  },
  "settings": {
    "language": "ru",
    "notifications": {
      "email": true,
      "sms": false
    }
  }
}
```

JSON строится на двух основных конструкциях:

- **Объект** — набор пар «ключ: значение» в фигурных скобках {}.
- **Массив** — упорядоченный список значений в квадратных скобках [].

Внутри объектов и массивов допустимы различные типы значений (строка, число, булево значение, пустое значение, объект, массив), связанные поля могут группироваться во вложенные объекты, вложенность может достигать нескольких уровней.

Принцип проверки HTTP-запросов с телом в формате JSON

Если к правилу публикации подключен только JSON-профиль, проверка выполняется последовательно: сначала проверяется заголовок Content-Type или формат тела запроса, затем — заданные лимиты и соответствие JSON-схемам. Парсинг JSON и проверка тела запроса на соответствие JSON-схемам выполняются только в том случае, если в профиле настроен хотя бы один лимит или хотя бы одна JSON-схема. Само по себе указание заголовка Content-Type не запускает проверку структуры JSON.

1. Проверка заголовка Content-Type

Если в JSON-профиле указан заголовок Content-Type, UserGate WAF проверяет, соответствует ли ему заголовок запроса. Если заголовок запроса не соответствует заданному значению, запрос пропускается этим профилем и может быть проверен другими профилями или правилами публикации.

Если заголовок Content-Type не указан, UserGate WAF проверяет, соответствует ли тело запроса формату JSON:

- если тело не является JSON, запрос пропускается этим профилем;
- если тело является JSON, UserGate WAF переходит к проверке лимитов.

2. Проверка лимитов

Если в JSON-профиле настроены лимиты для тела запроса, UserGate WAF проверяет их соблюдение:

- если лимиты превышены и для профиля выбрано действие **Deny**, запрос отклоняется, дальнейшая проверка запроса в рамках текущего правила публикации прекращается;
- если лимиты превышены и для профиля выбрано действие **Pass**, запрос передается на проверку по JSON-схеме;
- если лимиты не превышены, запрос передается на проверку по JSON-схеме.

Если лимиты не настроены, этот этап пропускается, а запрос передается на проверку по JSON-схеме.

3. Проверка соответствия JSON-схеме

Если в JSON-профиле указаны JSON-схемы, UserGate WAF разбирает тело запроса, проверяет его структуру и сопоставляет ее с заданными схемами.

- если запрос не соответствует схемам и выбрано действие **Deny**, UserGate WAF отклоняет запрос, дальнейшая проверка запроса в рамках текущего правила публикации прекращается;
- если запрос не соответствует схемам и выбрано действие **Pass**, запрос пропускается и передается на проверку другими правилами публикации, если они предусмотрены в конфигурации политики безопасности;
- если запрос соответствует схемам, он пропускается и может быть проверен другими профилями или правилами публикации, если они предусмотрены в конфигурации политики безопасности.

Если в JSON-профиле не указаны JSON-схемы, запрос пропускается и передается на проверку другими правилами публикации, если они предусмотрены в конфигурации политики безопасности.

Порядок совместной проверки запроса JSON-профилем и WAF-профилем

Если к правилу публикации подключен только JSON-профиль, UserGate WAF будет фильтровать запросы в соответствии с настроенной конфигурацией JSON-профиля.

Чтобы после парсинга также выполнялась проверка JSON-тела запроса на наличие угроз, к правилу публикации помимо JSON-профиля также необходимо подключить и WAF-профиль.

Правило публикации, в котором одновременно подключены WAF-профиль (для проверки экспертными WAF-правилами) и JSON-профиль (для парсинга и проверки JSON), обрабатывает запрос в несколько этапов, порядок которых определяется параметрами JSON-профиля.

Порядок проверки зависит от того, какие параметры проверки указаны в JSON-профиле: значение заголовка **Content-Type**, лимиты на данные, JSON-схема. WAF-профиль при этом отвечает за проверку по экспертным правилам (заголовки, параметры, тело), а JSON-профиль — за парсинг, лимиты и проверку по схеме.

Рассмотрим проверку запроса на примере, когда к правилу публикации подключены WAF-профиль и JSON-профиль и в JSON-профиле указаны:

- значение заголовка **Content-Type**;
- лимиты на данные (например, максимальный размер тела);
- JSON-схема.

Тогда проверка запроса будет выполняться в следующем порядке:

1. Проверка соответствия заголовка **Content-Type** и лимитов (JSON-профиль).

Когда поступает запрос, система сначала сверяет значение заголовка **Content-Type** с тем, что указано в JSON-профиле.

- если **Content-Type** соответствует указанному в JSON-профиле, проверяются лимиты на тело запроса;
- если лимиты превышены и в JSON-профиле выбрано блокирующее действие **Deny**, запрос отклоняется, дальнейшая проверка не проводится.

2. Проверка заголовков (WAF-профиль).

Если лимиты не превышены, далее WAF-профилем проверяются заголовки, при условии что правило публикации настроено на проверку заголовков. Если эта проверка не блокирует запрос, управление возвращается JSON-профилю для продолжения проверки тела.

3. Проверка тела запроса (JSON-профиль, затем WAF-профиль).

JSON-профиль продолжает проверку тела: выполняет парсинг JSON, проверяет структуру, сопоставляет со схемой. Если после этой проверки запрос не заблокирован, проверка тела продолжается WAF-профилем по экспертным WAF-правилам.

Настройка и подключение JSON-профиля

Чтобы правило публикации участвовало в проверке запросов с данными в формате JSON, необходимо создать JSON-профиль и подключить его к правилу публикации.

Важно! Чтобы JSON-профиль выполнял проверку запросов, в нем необходимо указать хотя бы один лимит или добавить хотя бы одну JSON-схему.

Создание JSON-профиля

Чтобы создать JSON-профиль:

1. На странице **Настройки** в разделе **Политика безопасности** → **Профили безопасности** → **JSON-профили** нажмите **Добавить**.

2. В окне **Свойства JSON-профиля** на вкладке **Общие** выполните следующие действия:

- укажите название профиля и при необходимости описание;
- при необходимости выберите профиль ответа, который вернется клиенту, если запрос будет заблокирован профилем;
- выберите действие, которое будет выполняться в отношении трафика при ошибке парсинга или выходе за пределы лимитов;
- при необходимости включите журналирование событий.

3. На вкладке **Content-type** укажите одно или несколько значений заголовка Content-type. Для запросов с этим значением в заголовке будет выполняться проверка на соответствие формату JSON.

Примечание Если не выбрано ни одно значение, проверку на соответствие формату JSON будут проходить все входящие запросы.

4. На вкладке **Лимиты** укажите максимальное значение для одного или нескольких лимитов:

- размер тела формата JSON в байтах;
- глубина вложенности объектов;
- количество элементов «ключ: значение» в объекте;
- количество элементов (значений) в массиве;
- количество символов в значении типа «строка» (string);
- количество символов в имени ключа.

5. На вкладке **JSON-схемы** при необходимости добавьте хотя бы одну JSON-схему для проверки соответствия запросов необходимым требованиям. Подробнее о создании JSON-схем — в разделе «[JSON-схемы](#)»

Примечание UserGate WAF поддерживает спецификации JSON Schema Draft 03, Draft 04 и Draft 06.

6. Если вы добавили несколько схем, выберите, требуется ли проверять соответствие хотя бы одной JSON-схеме или всем добавленным.

7. Сохраните изменения.

Подключение JSON-профиля к правилу публикации

Чтобы подключить JSON-профиль к правилу публикации:

1. На странице **Настройки** в разделе **Политика сервисов → Правила публикации** создайте или выберите правило публикации. Подробнее — в разделе «[Публикация веб-сервисов](#)».

2. На вкладке **Профили безопасности** установите флажок **Включить проверку данных в формате JSON** и выберите из списка нужный JSON-профиль.

Примечание Если нужного профиля нет в списке, вы можете создать его, нажав в конце списка «Создать и выбрать новый объект».

3. Завершите настройку других параметров правила публикации и сохраните изменения.

Правило публикации настроено на проверку данных в формате JSON. Если в JSON-профиле включено журналирование, события, связанные с обработкой запросов с данными в формате JSON, отображаются на странице **Атаки**. Подробнее об этом — в разделе «[Просмотр обнаруженных атак](#)».

Обработка запросов с данными в формате XML

Version: 7.7.x

Product: WAF

Documentation: 

Веб-сервисы и API могут обмениваться данными в формате XML. Если UserGate WAF будет обрабатывать тело HTTP-запроса как обычный текст, не учитывая структуру XML, это может привести к пропуску угроз, включая XXE-атаки, XPath-инъекции и скрытые XSS-полезные нагрузки в элементах и атрибутах. Для корректной проверки таких запросов UserGate WAF выполняет разбор тела запроса и проверяет соответствие данных структуре XML. Эти параметры настраиваются в XML-профилях.

XML-профиль, подключенный к правилу публикации, обеспечивает:

- пропуск только легитимных запросов с данными в формате XML;
- проверку соответствия данных заданным XML-схемам (или XSD-схемам) и отклонение запросов с нестандартной структурой;
- контроль размера, сложности и глубины вложенности данных с помощью лимитов;
- разбор (парсинг) структуры XML для последующей проверки тела запроса WAF-правилами;
- журналирование событий, связанных с проверкой данных в формате XML.

О данных в формате XML

XML (Extensible Markup Language) — это расширяемый язык разметки для представления структурированных данных. В HTTP-запросах данные в формате XML обычно приходят в теле запроса с заголовком Content-Type: application/xml или более специфичным, например application/soap+xml или application/rss+xml.

Пример HTTP-запроса с XML

POST /api/users HTTP/1.1

Host: example.com

Content-Type: application/xml

Content-Length: 200

```
<?xml version="1.0" encoding="UTF-8"?>
<users>
  <user id="123">
    <name>Ivan</name>
    <role>admin</role>
  </user>
  <user id="200">
    <name>Anna</name>
    <role>user</role>
  </user>
</users>
```

Основными элементами структуры XML являются:

- **XML-декларация:** — указывает версию и кодировку (необязательный элемент). В примере: <?xml version="1.0" encoding="UTF-8"?>. UserGate WAF может использовать ее для проверки согласованности с заголовками.
- **Корневой элемент** — элемент, который охватывает весь документ. В примере это <users>. Корень в документе ровно один — двух корневых элементов быть не может.
- **Элемент** — пара открывающего и закрывающего тегов с содержимым (<name>Ivan</name>) либо самозакрывающийся тег без содержимого (<name/>).
- **Вложенность** — элементы образуют дерево: <name>, <role> вложены в <user> и являются его дочерними элементами. В свою очередь элементы <user> вложены в <users>.
- **Атрибут** — пара «ключ — значение» внутри открывающего тега, значение всегда в кавычках: <user id="123">.

Принцип проверки HTTP-запросов с телом в формате XML

Если к правилу публикации подключен только XML-профиль, проверка выполняется последовательно: сначала проверяется заголовок Content-Type или формат тела запроса, затем — заданные лимиты и соответствие XML-схемам. Парсинг XML и проверка тела запроса на соответствие XML-схемам выполняются только в том случае, если в профиле настроен хотя бы один лимит или хотя бы одна XML-схема. Само по себе указание заголовка Content-Type не запускает проверку структуры XML.

1. Проверка заголовка Content-Type

Если в XML-профиле указан заголовок Content-Type, UserGate WAF проверяет, соответствует ли ему заголовок запроса. Если заголовок запроса не соответствует заданному значению, запрос пропускается этим профилем и может быть проверен другими профилями или правилами публикации.

Если заголовок Content-Type не указан, UserGate WAF проверяет, соответствует ли тело запроса формату XML:

- если тело не является XML, запрос пропускается этим профилем;

- если тело является XML, UserGate WAF переходит к проверке лимитов.

2. Проверка лимитов

Если в XML-профиле настроены лимиты для тела запроса, UserGate WAF проверяет их соблюдение:

- если лимиты превышены и для профиля выбрано действие **Deny**, запрос отклоняется, дальнейшая проверка запроса в рамках текущего правила публикации прекращается;
- если лимиты превышены и для профиля выбрано действие **Pass**, запрос передается на проверку по XML-схеме;
- если лимиты не превышены, запрос передается на проверку по XML-схеме.

Если лимиты не настроены, этот этап пропускается, а запрос передается на проверку по XML-схеме.

3. Проверка соответствия XML-схеме

Если в XML-профиле указаны XML-схемы, UserGate WAF разбирает тело запроса, проверяет его структуру и сопоставляет ее с заданными схемами.

- если запрос не соответствует схемам и выбрано действие **Deny**, UserGate WAF отклоняет запрос, дальнейшая проверка запроса в рамках текущего правила публикации прекращается;
- если запрос не соответствует схемам и выбрано действие **Pass**, запрос пропускается и передается на проверку другими правилами публикации, если они предусмотрены в конфигурации политики безопасности;
- если запрос соответствует схемам, он пропускается и может быть проверен другими профилями или правилами публикации, если они предусмотрены в конфигурации политики безопасности.

Если в XML-профиле не указаны XML-схемы, запрос пропускается и передается на проверку другими правилами публикации, если они предусмотрены в конфигурации политики безопасности.

Порядок совместной проверки запроса XML-профилем и WAF-профилем

Если к правилу публикации подключен только XML-профиль, UserGate WAF будет фильтровать запросы в соответствии с настроенной конфигурацией XML-профиля.

Чтобы после парсинга также выполнялась проверка XML-тела запроса на наличие угроз, к правилу публикации помимо XML-профиля также необходимо подключить и WAF-профиль.

Правило публикации, в котором одновременно подключены WAF-профиль (для проверки экспертными WAF-правилами) и XML-профиль (для парсинга и проверки XML), обрабатывает запрос в несколько этапов, порядок которых определяется параметрами XML-профиля.

Порядок проверки зависит от того, какие параметры проверки указаны в XML-профиле: значение заголовка **Content-Type**, лимиты на данные, XML-схема. WAF-профиль при этом отвечает за проверку по экспертным правилам (заголовки, параметры, тело), а XML-профиль — за парсинг, лимиты и проверку по схеме.

Рассмотрим проверку запроса на примере, когда к правилу публикации подключены WAF-профиль и XML-профиль и в XML-профиле указаны:

- значение заголовка **Content-Type**;
- лимиты на данные (например, максимальный размер тела);
- XML-схема.

Тогда проверка запроса будет выполняться в следующем порядке:

1. Проверка соответствия заголовка **Content-Type** и лимитов (XML-профиль).

Когда поступает запрос, система сначала сверяет значение заголовка **Content-Type** с тем, что указано в XML-профиле.

- если **Content-Type** соответствует указанному в XML-профиле, проверяются лимиты на тело запроса;
- если лимиты превышены и в XML-профиле выбрано блокирующее действие **Deny**, запрос отклоняется сразу, с возвратом ответа, если в XML-профиле был указан профиль ответа. Дальнейшая проверка не проводится.

2. Проверка заголовков (WAF-профиль).

Если лимиты не превышены, далее WAF-профилем проверяются заголовки, при условии что правило публикации настроено на проверку заголовков. Если эта проверка не блокирует запрос, управление возвращается XML-профилю для продолжения проверки тела.

3. Проверка тела запроса (XML-профиль, затем WAF-профиль).

XML-профиль продолжает проверку тела: выполняет парсинг XML, проверяет структуру, сопоставляет со схемой. Если после этой проверки запрос не заблокирован, проверка тела продолжается WAF-профилем по экспертным WAF-правилам.

Таким образом, при наличии и WAF-профиля, и XML-профиля в одном правиле публикации запрос проходит последовательную цепочку: сначала условия и лимиты XML-профиля, затем (если не было блокировки) заголовки через WAF-профиль, затем тело через XML-профиль и, наконец, через WAF-профиль.

Настройка и подключение XML-профиля

Чтобы правило публикации участвовало в проверке запросов с данными в формате XML, необходимо создать XML-профиль и подключить его к правилу публикации.

Создание XML-профиля

Важно! Чтобы XML-профиль выполнял проверку запросов, в нем необходимо указать хотя бы один лимит или добавить хотя бы одну XML-схему.

Чтобы создать XML-профиль:

1. На странице **Настройки** в разделе **Политика безопасности → Профили безопасности → XML-профили** нажмите **Добавить**.
 2. В окне **Свойства XML-профиля** на вкладке **Общие** выполните следующие действия:
 - укажите название профиля и при необходимости описание;
 - при необходимости выберите профиль ответа, который вернется клиенту, если запрос будет заблокирован профилем;
 - выберите действие, которое будет выполняться в отношении трафика при ошибке парсинга или выходе за пределы лимитов;
 - при необходимости включите журналирование событий.
 3. На вкладке **Content-type** укажите одно или несколько значений заголовка Content-type. Для запросов с этим значением в заголовке будет выполняться проверка на соответствие формату XML.
- Примечание** Если не выбрано ни одно значение, проверку на соответствие формату XML будут проходить все входящие запросы.
4. На вкладке **Лимиты** укажите максимальное значение для одного или нескольких лимитов:
 - размер тела формата XML в байтах;
 - глубина вложенности элементов;
 - количество элементов «ключ: значение» в объекте;
 - количество атрибутов;
 - количество символов в имени ключа;
 - длина имени атрибута;
 - длина текстового значения;
 - длина значения атрибута.
 5. На вкладке **XML-схемы** при необходимости добавьте хотя бы одну XML-схему для проверки соответствия запросов необходимым требованиям. Подробнее о создании XML-схем — в разделе [«XML-схемы»](#)
 6. Если вы добавили несколько схем, выберите, требуется ли проверять соответствие хотя бы одной XML-схеме или всем добавленным.
 7. Сохраните изменения.

Подключение XML-профиля к правилу публикации

Чтобы подключить XML-профиль к правилу публикации:

1. На странице **Настройки** в разделе **Политика сервисов → Правила публикации** создайте или выберите правило публикации. Подробнее — в разделе [«Публикация веб-сервисов»](#).
2. На вкладке **Профили безопасности** установите флажок **Включить проверку данных в формате XML** и выберите из списка нужный XML-профиль.

Примечание Если нужного профиля нет в списке, вы можете создать его, нажав в конце списка «Создать и выбрать новый объект».

3. Завершите настройку других параметров правила публикации и сохраните изменения.

Правило публикации настроено на проверку данных в формате XML. Если в XML-профиле включено журналирование, события, связанные с обработкой запросов с данными в формате XML, отображаются на странице **Атаки**. Подробнее об этом — в разделе [«Просмотр обнаруженных атак»](#).

Version: 7.7.x

Product: WAF

UserGate WAF может контролировать безопасность установления соединений по протоколу WebSocket.

Протокол WebSocket обеспечивает двунаправленную связь между клиентом и сервером в реальном времени и позволяет поддерживать постоянное соединение, по которому данные могут передаваться в обе стороны без необходимости повторных запросов от клиента. Принцип работы протокола WebSocket следующий:

1. Установление соединения. Клиент отправляет HTTP-запрос на «рукопожатие» (handshake-запрос) серверу, предлагая установить WebSocket-соединение. Если сервер поддерживает протокол WebSocket, он возвращает подтверждающий ответ, и соединение переключается с HTTP на WebSocket.
2. Двунаправленный обмен данными. После успешного подключения клиент и сервер могут свободно отправлять данные друг другу в любое время без дополнительного подтверждения.
3. Закрытие соединения. Соединение может быть закрыто по инициативе клиента или сервера с отправкой кода закрытия и возможного описания причины.

В UserGate WAF правила установления WebSocket-соединений определяются WebSocket-профилем, который позволяет настроить:

- Блокирование любого WebSocket-трафика, который приходит в UserGate WAF.
- Проверку целостности handshake-запроса.
- Проверку наличия заголовка Origin — HTTP-заголовка, который браузеры автоматически добавляют в запрос при установке WebSocket-соединения. Заголовок Origin содержит URL источника, который иницирует соединение.
- Списки значений заголовков запроса (Origin, Sec-WebSocket-Extensions, Sec-WebSocket-Protocols), на основании которых UserGate WAF будет устанавливать WebSocket-соединение с доверенными источниками или игнорировать запросы, поступающие из нежелательных источников.
- Журналирование событий, связанных с установлением WebSocket-соединений. Подробнее — в разделе « [Журнал WebSocket](#) ».

Настройка WebSocket-профиля для блокирования всего WebSocket-трафика

Чтобы создать WebSocket-профиль, блокирующий весь WebSocket-трафик:

1. На странице **Настройки** в разделе **Политика безопасности** → **Профили безопасности** → **WebSocket-профили** нажмите **Добавить**.
2. В окне **Свойства WebSocket-профиля** на вкладке **Общие** установите флажок **Блокировать WebSocket-трафик**.
3. Если необходимо, включите журналирование событий
4. Сохраните изменения.

Чтобы начать блокирование трафика в соответствии с настроенным WebSocket-профилем, его нужно выбрать в качестве профиля безопасности в правиле публикации.

Настройка WebSocket-профиля для фильтрации WebSocket-соединений

Чтобы создать WebSocket-профиль, фильтрующий WebSocket-соединения:

1. На странице **Настройки** в разделе **Политика безопасности** → **Профили безопасности** → **WebSocket-профили** нажмите **Добавить**.
2. В окне **Свойства WebSocket-профиля** на вкладке **Общие** укажите название профиля.
3. Настройте один или несколько параметров фильтрации WebSocket-соединений:

- На вкладке **Общие** включите проверку целостности запроса, установив соответствующий флажок.
- На вкладке **Источники** установите флажок **Учитывать Origin**, нажмите **Создать и добавить новый объект** и создайте список URL источников, с которыми разрешается устанавливать WebSocket-соединение.

Примечание Вы также можете настроить WebSocket-профиль, игнорирующий источники, запрашивающие WebSocket-соединение. Для этого на вкладке «Источники» нужно сформировать список нежелательных источников либо добавить предустановленные списки и включить «Инвертировать».

- На вкладке **Расширения и протоколы** установите флажки **Учитывать Sec-WebSocket-Extensions** и **Учитывать Sec-WebSocket-Protocols** и добавьте списки разрешенных расширений и субпротоколов, которые указываются в заголовках Sec-WebSocket-Extensions и Sec-WebSocket-Protocols. WebSocket-соединения будут устанавливаться только по тем запросам, в заголовках которых указаны разрешенные значения.

Примечание Вы также можете настроить WebSocket-профиль на игнорирование WebSocket-соединений по запросам, в заголовках которых найдены расширения и субпротоколы из добавленных списков. Для этого на вкладке «Расширения и протоколы» нужно добавить списки нежелательных расширений и субпротоколов и включить «Инвертировать».

4. Если необходимо, на вкладке **Общие** включите журналирование событий.

5. Сохраните изменения.

Чтобы начать фильтрацию WebSocket-соединений в соответствии с настроенным WebSocket-профилем, его нужно выбрать в качестве профиля безопасности в правиле публикации.

Создание списков расширений и субпротоколов для WebSocket-соединений

Handshake-запрос может содержать в том числе следующие заголовки:

- Sec-WebSocket-Protocol — содержит набор субпротоколов, которые клиент будет использовать при передаче данных.
- Sec-WebSocket-Extensions — содержит дополнительные расширения WebSocket-протокола, которые поддерживает браузер. Например, может быть указан метод сжатия передаваемых данных.

Вы можете создавать списки расширений и субпротоколов и использовать их в WebSocket-профиле для фильтрации WebSocket-соединений.

Чтобы создать список расширений:

1. На странице **Настройки** в разделе **Библиотеки → WebSocket-расширения** нажмите **Добавить** и укажите название списка.
2. Выберите тип списка:
 - **Локальный**, если список будет поддерживаться вручную.
 - **Обновляемый**, если список будет загружаться из внешнего источника. В этом случае укажите URL источника и настройте расписание автоматических обновлений списка.
3. Сохраните список.

Чтобы создать список субпротоколов:

1. На странице **Настройки** в разделе **Библиотеки → WebSocket-протоколы** нажмите **Добавить** и укажите название списка.
2. Выберите тип списка:
 - **Локальный**, если список будет поддерживаться вручную.
 - **Обновляемый**, если список будет загружаться из внешнего источника. В этом случае укажите URL источника и настройте расписание автоматических обновлений списка.
3. Сохраните список.

О настройке расписания обновлений списков

Вы можете выбрать одно из предустановленных значений или указать время вручную в cron-формате: <минуты: 0-59> <часы: 0-23> <дни месяца: 1-31> <месяцы: 1-12> <дни недели: 0-6, где 0 — воскресенье>.

При ручном вводе также можно использовать следующие символы:

- Звездочка (*) — для выбора всех значений. Например, в поле для ввода часов символ означает, что резервное копирование должно выполняться каждый час.
- Дефис (-) — для указания диапазона значений.
- Запятая (,) — в качестве разделителя значений.
- Косая черта (/) — для указания шага между значениями. Например, «2-10/2» будет означать «2,4,6,8,10», а выражение «*/2» в поле «часы» будет означать «каждые два часа».

Подключение WebSocket-профиля к правилу публикации

Чтобы подключить WebSocket-профиль к правилу публикации:

1. На странице **Настройки** в разделе **Политика сервисов → Правила публикации** создайте или выберите из списка правило. Подробнее — в разделе «[Публикация веб-сервисов](#)».
2. В окне **Настройка правила публикации** на вкладке **Профили безопасности** установите флажок **Включить защиту WebSocket-соединений** и выберите нужный WebSocket-профиль.
3. Сохраните изменения.

Профили ответа

Technology: WAF

Version: 7.7.x

Product: WAF

В соответствии с политикой безопасности подозрительные запросы к защищаемым веб-серверам могут блокироваться. С помощью профилей ответа вы можете настроить, какой ответ будет возвращен клиенту, если сработал один из профилей безопасности: например, сработало блокирующее WAF-правило или запрос с данными в формате JSON не прошел проверку в JSON-профиле. Поддерживаются следующие виды ответов на заблокированный запрос:

- страница блокировки с указанием кода состояния HTTP;
- сообщение о разрыве соединения;
- переадресация на другой ресурс.

Чтобы создать профиль ответа:

1. На странице **Настройки** в разделе **Политика безопасности** → **Профили ответа** нажмите **Добавить**.

2. В окне **Свойства профилей ответа** укажите название профиля.

3. Выберите нужный тип политики и настройте для него необходимые параметры:

- **TCP RST**. Выберите этот тип политики, чтобы при блокировании выполнялся разрыв соединения.
- **Переадресация**. Укажите ссылку для перенаправления запроса, трехзначный код состояния HTTP и, если необходимо, добавьте текст ответа.

ПримечаниеТрехзначный код состояния HTTP для переадресации должен начинаться с цифры 3. Например, 302. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду.

- **Шаблон страницы**. В списке **Страница блокировки** выберите шаблон страницы из списка (либо оставьте выбранный по умолчанию), укажите трехзначный код состояния HTTP и, если необходимо, добавьте текст ответа. Подробнее о создании шаблона страницы — в разделе [«Шаблоны страниц»](#).

ПримечаниеТрехзначный код состояния HTTP для блокировки должен начинаться с цифр 1, 2, 4 или 5. Например, 403. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду.

4. Сохраните изменения.

Чтобы добавить созданный профиль ответа в WAF-правило:

1. На странице **Настройки** в разделе **Политика безопасности** → **Глобальные правила** выберите правило, которому назначено действие Deny или Force deny, и нажмите **Редактировать**.

2. В окне **Редактирование правил** в списке **Профили ответа** выберите нужный профиль

3. Сохраните изменения.

ПримечаниеВы также можете добавить профиль ответа в WAF-правило при создании или изменении WAF-профиля. Подробнее о настройке WAF-профилей — в разделе [«Настройка параметров безопасности WAF»](#).

Чтобы добавить созданный профиль ответа в JSON-профиль:

1. На странице **Настройки** в разделе **Политика безопасности** → **Профили безопасности** → **JSON-профили** выберите JSON-профиль с действием Deny и нажмите **Редактировать**.

2. В окне **Свойства JSON-профиля** в списке **Профили ответа** выберите нужный профиль

3. Сохраните изменения.

Чтобы добавить созданный профиль ответа в XML-профиль:

1. На странице **Настройки** в разделе **Политика безопасности** → **Профили безопасности** → **XML-профили** выберите XML-профиль с действием Deny и нажмите **Редактировать**.

2. В окне **Свойства XML-профиля** в списке **Профили ответа** выберите нужный профиль

3. Сохраните изменения.

Обработка дополнительных HTTP-заголовков

Product: WAF

Technology: WAF

Version: 7.7.x

При передаче запроса промежуточные узлы (такие, как сервер reverse-прокси или балансировщик нагрузки) меняют значения в стандартных заголовках запроса, обеспечивая таким образом безопасность внутренних веб-сервисов или правильную маршрутизацию. Но внутреннему веб-сервису для корректной обработки запроса требуется исходная информация, переданная клиентом. Например, для определения геолокации клиента или сбора статистики. Чтобы обеспечить корректную работу внутренних веб-сервисов, серверы reverse-прокси или другие устройства могут передавать исходные данные запроса в дополнительных HTTP-заголовках.

В UserGate WAF вы можете использовать правила публикации для обработки следующих дополнительных HTTP-заголовков:

- X-Forwarded-Host: содержит значение заголовка Host из исходного запроса. Это значение требуется внутреннему веб-сервису для уточнения, какой контент следует вернуть клиенту, а также при журналировании и балансировке нагрузки.
- X-Forwarded-Proto: содержит сведения о протоколе исходного запроса, которые позволяют на стороне внутреннего веб-сервиса выполнять переадресацию на безопасный ресурс либо генерировать корректные ссылки.
- X-Forwarded-Port: передает исходный порт подключения клиента, который необходим для генерации корректных ссылок на стороне внутреннего веб-сервиса.

Чтобы настроить обработку дополнительных HTTP-заголовков:

1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте правило. Подробнее об этом — в разделе [«Публикация веб-сервисов»](#).
2. В окне **Настройка правила публикации** на вкладке **Обработка заголовков** установите флажки для тех заголовков, которые будут добавлены в исходный запрос. Если заголовки уже содержатся в запросе, их значения будут переписаны.
3. Сохраните изменения.

