

Table of Contents

Table of Contents	1
Настройка публикации веб-сервисов	2
Публикация веб-сервисов	3
Настройка определения реального IP-адреса	8
Балансировка нагрузки	10

Product: WAF

Version: 7.7.x

UserGate WAF поддерживает публикацию веб-сервисов. Доступ к веб-сервисам и безопасность соединений с ними контролируются настраиваемыми правилами публикации.

Режим публикации предоставляет следующие возможности:

- **Балансировка нагрузки.** Если обработку запросов к веб-сервису выполняют несколько веб-серверов, UserGate WAF может равномерно распределять запросы между ними и тем самым предотвращать перегрузку отдельных веб-серверов.
- **Подмена путей.** UserGate WAF может выполнять подмену путей и доменных имен в запросах, помогая таким образом разделить трафик для разных веб-сервисов.
- **Управление доступом к веб-серверам.** UserGate WAF может блокировать попытки доступа по идентификационной строке клиентского приложения (useragent) и нежелательным адресам.
- **Поддержка SSL-подключения.** UserGate WAF может выполнять шифрование и расшифрование запросов и ответов, что позволяет снизить нагрузку на веб-серверы и повысить их производительность.
- **Сигнатурный анализ трафика.** Правила публикации с подключенными WAF-профилями безопасности защищают веб-сервисы от атак и других угроз безопасности. Подробнее — в разделе «[Настройка параметров безопасности WAF](#)».
- **Фильтрация WebSocket-трафика.** UserGate WAF поддерживает обмен трафиком по протоколу WebSocket и обеспечивает безопасность установления WebSocket-соединений. Подробнее — в разделе «[Защита WebSocket-соединений](#)».
- **Проверка и парсинг данных в формате JSON.** Правила публикации с подключенными JSON-профилями безопасности проверяют запросы с данными в формате JSON на их корректность и соответствие заданной структуре. Подробнее об этом — в разделе «[Обработка запросов с данными в формате JSON](#)».
- **Проверка и парсинг данных в формате XML.** Правила публикации с подключенными XML-профилями безопасности проверяют запросы с данными в формате XML на их корректность и соответствие заданной структуре. Подробнее об этом — в разделе «[Обработка запросов с данными в формате XML](#)».
- **Определение реального IP-адреса источника запроса.** UserGate WAF может анализировать заголовки HTTP-запросов, чтобы определить реальный IP-адрес. Подробнее — в разделе «[Настройка функции определения реального IP-адреса](#)».
- **Фильтрация трафика,** закодированного по стандарту Base64. Подробнее — в разделе «[Фильтрация закодированного трафика](#)».

Чтобы опубликовать веб-сервис:

1. Создайте один или несколько серверов публикации.
2. Если для доступа к веб-сервису используются несколько серверов, создайте для них правило балансировки.
3. Создайте правила публикации, которые будут определять условия публикации веб-сервисов выбранным сервером или балансировщиком.

Важно! Правила публикации применяются сверху вниз в списке правил. Срабатывает только первое правило публикации, для которого совпали все условия, указанные в параметрах правила.

4. В разделе **Настройки → Сеть → Зоны** в параметрах контроля доступа той зоны, в которой необходимо разрешить доступ к внутренним ресурсам, разрешите сервис **Reverse-прокси**.

Создание сервера публикации

Чтобы создать сервер публикации:

1. В разделе **Политика сервисов → Серверы публикации** нажмите **Добавить**.
2. В окне **Настройка сервера публикации** укажите название, IP-адрес или FQDN и TCP-порт сервера публикации.
3. Если необходимо, настройте остальные параметры:
 - Установите флажок **HTTPS до сервера**, чтобы выполнять передачу трафика по защищенному соединению от UserGate WAF до сервера публикации. Если этот флажок установлен, убедитесь, что на шаге 2 вы указали порт для защищенного соединения.
 - Установите флажок **Проверять SSL-сертификат**, чтобы включить проверку подлинности SSL-сертификата, установленного на сервере публикации. Доступно, если установлен флажок **HTTPS до сервера**.
 - Установите флажок **Не изменять IP-адрес источника**, чтобы сохранять оригинальный IP-адрес источника в запросах. Если флажок снят, IP-адрес источника заменяется на IP-адрес UserGate WAF.

Важно! Если установлен флажок «Не изменять IP-адрес источника», для корректной работы необходимо настроить маршрутизацию таким образом, чтобы сервер публикации отвечал через тот же сетевой интерфейс UserGate WAF, с которого приходят запросы клиентов. Для этого на сервере публикации в качестве шлюза по умолчанию можно указать UserGate WAF или можно настроить статические маршруты через UserGate WAF для «белых» IP-адресов источников.

4. Сохраните изменения.

Балансировка нагрузки на серверы публикации

Если для доступа к веб-сервису развернуто несколько серверов публикации, вы можете распределять клиентские запросы между ними с помощью правил балансировки нагрузки.

Чтобы создать правило балансировки серверов публикации:

1. В разделе **Политика сервисов → Серверы публикации** создайте серверы публикации веб-сервисов. Убедитесь, что в окне **Настройка сервера публикации** для каждого сервера, который участвует в балансировке, в поле **Адрес сервера** указан IP-адрес.
2. В разделе **Политика сервисов → Балансировка сервисов** нажмите **Добавить**.
3. В окне **Настройка правила балансировки сервисов** на вкладке **Общие** укажите название правила и включите его.
4. На вкладке **Серверы публикации** добавьте серверы, на которые будет распределяться нагрузка.
5. Сохраните изменения.

Создание правила публикации

Правила публикации позволяют фильтровать запросы к веб-сервисам, контролировать доступ к ним и обеспечивать безопасное соединение.

Созданные правила применяются поочередно сверху вниз в том порядке, в котором они указаны в списке. Выполняется только первое правило, для которого совпали все указанные в нем условия. Это значит, что более специфические правила должны быть выше в списке, чем более общие правила. Вы можете мышью перетаскивать правила в списке для изменения порядка применения правил.

Чтобы создать правило публикации:

1. В разделе **Настройки → Политика сервисов → Правила публикации** нажмите **Добавить**.
2. В окне **Настройка правила публикации** на вкладке **Общие**:
 - Включите правило и укажите его название.
 - В списке **Сервер публикации** выберите сервер публикации или балансировщик, которому UserGate WAF будет пересылать запросы.
 - Укажите порты, на которых UserGate WAF будет слушать входящие запросы.
 - Установите флажок **Использовать HTTPS**, если необходимо, чтобы обмен трафиком с клиентом проходил по защищенному соединению.
 - Если флажок **Использовать HTTPS** установлен, выберите профиль SSL, поддерживающий нужные протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, и сертификат сервера публикации для поддержки HTTPS-соединения.
 - С помощью параметра **Вставить** настройте расположение правила в списке.

Примечание Параметр доступен, если в списке уже есть другие правила.

3. На вкладке **Источник**, выберите минимум одну зону источника трафика, а также, если необходимо, добавьте списки IP-адресов или GeoIP-адреса (не более 15 адресов), для которых будет разрешен обмен трафиком с серверами публикации.

Важно! Не добавляйте в списки строки с символом «*», они будут игнорироваться.

Примечание Вы также можете настроить правило, игнорирующее источники трафика в указанных зонах и с выбранными адресами. Для этого на вкладке «Источник» нужно сформировать список нежелательных зон и/или адресов и в соответствующих блоках параметров включить «Инвертировать».

Примечание Каждые пять минут UserGate WAF выполняет разрешение доменных имен в IP-адреса и хранит полученный результат во внутреннем кэше на время жизни DNS-записи. По истечении времени жизни UserGate WAF автоматически обновляет значение IP-адреса.

Важно! Обработка трафика происходит по следующей логике: условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов; условия объединяются по «И», если указаны GeoIP и списки IP-адресов.

4. На вкладке **Назначение** укажите IP-адреса, назначенные на интерфейсы, которые принимают входящие соединения. Этот параметр следует настраивать, когда на один интерфейс UserGate WAF назначено несколько IP-адресов либо несколько интерфейсов подключены к сети.

Примечание Вы также можете настроить правило, игнорирующее входящие соединения на указанные адреса. Для этого на вкладке «Назначение» укажите адреса и включите «Инвертировать».

Важно! Обработка трафика происходит по следующей логике: условия объединяются по «ИЛИ», если указаны несколько списков IP-адресов.

5. На вкладке **Профили безопасности** при необходимости подключите нужные профили. Подробнее об этом — в разделах [«Настройка параметров безопасности WAF»](#), [«Защита WebSocket-соединений»](#), [«Обработка запросов с данными в формате JSON»](#), [«Обработка запросов с данными в формате XML»](#).

6. На вкладке **Веб-сервисы** нажмите **Добавить** и укажите путь к одному или нескольким веб-сервисам, запросы к которым будет обрабатывать правило.

Примечание Формат записи: <host>/<path>, где <host> — обязательный параметр (совпадение строгое, наличие и отсутствие символа «/» в конце названия узла без пути равнозначно; все названия узлов приводятся к нижнему регистру.), а <path> — необязательный, без которого будет выбираться любой путь (совпадение префиксное, не строгое). При указании пути для <host> в качестве маски можно использовать символ *. Например, запись *.example.org соответствует как www.example.org, так и www.sub.example.org.

Важно! Следует указывать те веб-сервисы, публикацию которых обеспечивает сервер, выбранный на шаге 2. В противном случае правило сработает некорректно.

7. На вкладке **Useragent**, если необходимо, добавьте идентификационные строки клиентских браузеров, для которых будет разрешен обмен трафиком с веб-сервисами.

ПримечаниеВы также можете настроить правило, игнорирующее определенные браузеры, запрашивающие доступ к веб-серверу. Для этого на вкладке «Useragent» нужно сформировать список нежелательных браузеров и включить «Инвертировать».

8. На вкладке **Подмена путей**, если необходимо, настройте переопределение путей URL. Подробнее о подмене путей — в разделе ниже.

9. Сохраните изменения.

Подмена путей в правилах публикации

Подмена путей в правилах публикации используется для модификации HTTP-запроса пользователя. Правило публикации обрабатывает запрос, выполняя в нем подмену пути, и передает модифицированный запрос на указанный сервер публикации. Веб-сервис, доступ к которому контролируется этим сервером публикации, получает и обрабатывает модифицированный запрос и возвращает соответствующий ответ. Таким образом вы можете управлять разделением трафика для разных сервисов.

Чтобы настроить подмену путей в правиле публикации:

1. В разделе **Настройки → Политика сервисов → Правила публикации** создайте или выберите правило.
2. В окне **Настройка правила публикации** на вкладке **Подмена путей** установите флажок **Подмена путей**.
3. Нажмите **Добавить** и укажите пути подмены одним или двумя способами:
 - **Пути для подмены**. Заполните вручную поля, где:
 - **Изменить с** — домен и/или путь URL, который требуется изменить.
 - **Изменить на** — домен и/или путь URL, на который требуется заменить старый.
 - **Веб-сервисы**. В качестве домена и/или пути URL, который требуется изменить, выберите веб-сервис, указанный на вкладке **Веб-сервисы**, и в поле **Изменить на** укажите для него соответствующий домен и/или путь URL, на который требуется его заменить.

ПримечаниеВы можете настраивать подмену путей и для кириллических доменов.

The screenshot shows the 'Настройка правила публикации' (Rule Publication Settings) dialog box with the 'Подмена путей' (Path Substitution) tab selected. The 'Подмена путей' checkbox is checked. Below it are buttons: '+ Добавить' (Add), 'Редактировать' (Edit), 'Удалить' (Delete), and 'Копировать' (Copy). A table with two columns, 'Изменить с' (Change from) and 'Изменить на' (Change to), contains one row with 'example.com/path1' and 'example.local/path2'. At the bottom left are 'Выше' (Up) and 'Ниже' (Down) buttons. A light blue information box at the bottom states: 'Правила переадресации применяются сверху вниз в списке правил. Срабатывает только первое правило переадресации, для которого совпали все условия.' (Redirect rules are applied from top to bottom in the list of rules. Only the first redirect rule for which all conditions match will trigger). At the bottom right are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

4. Сохраните правило.

При обработке HTTP-запроса правило публикации сработает, если путь, указанный на вкладке **Веб-сервисы**, совпадет с путем URL в HTTP-запросе. Затем происходит подмена пути в HTTP-запросе, если она предусмотрена сработавшим правилом: паттерн из поля **Изменить с** меняется на паттерн из поля **Изменить на**. Если запрос пользователя не попадет ни под одно правило публикации, в ответ на него будет получена ошибка: 403 Forbidden.

Условия проверки соответствия

Синтаксис HTTP-запроса представляет собой следующую последовательность: <scheme>://<host>:<port>/<path>.

Паттерн в поле **Изменить с** состоит из последовательности <host>/<path> и должен удовлетворять следующим условиям:

- <host> — обязательный параметр. Совпадение строгое, наличие и отсутствие символа «/» в конце названия узла без пути равнозначно. Все названия узлов приводятся к нижнему регистру.

- <path> — необязательный параметр. Без него будет выбираться любой путь. Совпадение префиксное (не строгое).
- Паттерн из поля **Изменить с** и паттерн из поля **Изменить на** должны оба либо заканчиваться символом «/», либо не содержать его в конце. В противном случае подмена путей сработает некорректно.
- Схема (<scheme>) запроса игнорируется и не изменяется.
- Порт (<port>) запроса игнорируется и не изменяется.

При совпадении запроса и исходного паттерна правило считается сработавшим.

В таблице ниже приведены примеры срабатываний паттернов.

Исходный паттерн в правиле публикации	Примеры запросов, на которые правило работает	Примеры запросов, на которые правило не работает
test.dev	- test.dev - test.dev/ - test.dev/* - http://test.dev - test.dev:<любой порт>	- abc.com - test.develop - test.dev.lol
tesT.deV	- test.deV - tesT.deV/ - TEST.dev	- abc.com - test.develop - test.dev.lol
test.dev/co	- test.dev/co* - http://test.dev/co* - test.dev:<любой порт>/co*	- test.dev.lol/co* - test.dev/kool*
http://test.dev	- http://test.dev - http://test.dev/* - http://test.dev:<любой порт> - http://test.dev:<любой порт>/ - http://test.dev:<любой порт>/*	http://test.develop
http://test.dev/co	- http://test.dev/co* - http://test.dev:<любой порт>/co	http://test.dev/cool*

Примеры срабатывания подмены путей

Рассмотрим детальнее логику работы подмены путей.

Для этого создадим правило test.dev/exa → test.dev/ad/test и сделаем несколько запросов.

Настройка правила публикации

Общие

Источник

Профили безопасности

Назначение

Веб-сервисы

Useragent

Подмена путей

...

☒ Подмена путей ?

+

Добавить

Редактировать

Удалить

Копировать

Изменить с	Изменить на
test.dev/exa	test.dev/ad/test

Выше

Ниже

Правила переадресации применяются сверху вниз в списке правил. Срабатывает только первое правило переадресации, для которого совпали все условия.

Сохранить

Отмена

1) Запрос на `test.dev/exalala`.

Параметр path = `/exalala`. Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается `/exa`. Оставшаяся часть: `lala`.

При дальнейшей конвертации берется полученный остаток `lala` и добавляется к концу path паттерна из поля **Изменить на**, то есть: `/ad/test` + `lala`. В итоге, после преобразования, параметр path получает значение `/ad/testlala`.

Таким образом, конечный запрос будет отправлен по адресу `test.dev/ad/testlala`.

2) Запрос на `test.dev/exa/vvv`.

Параметр path = `/exa/vvv`. Из него убирается path паттерна из поля **Изменить с**, в данном примере убирается `/exa`. Оставшаяся часть: `/vvv`.

При дальнейшей конвертации берется полученный остаток `/vvv` и добавляется к концу path паттерна из поля **Изменить на**, то есть: `/ad/test` + `/vvv`. В итоге, после преобразования, параметр path получает значение `ad/test/vvv`.

Таким образом, конечный запрос будет отправлен по адресу `test.dev/ad/test/vvv`.

Настройка определения реального IP-адреса

Product: WAF

Version: 7.7.x

Когда между веб-клиентом и узлом WAF находятся прокси-серверы, балансировщики нагрузки или другие сетевые узлы, в запросах, проходящих через них, IP-адрес источника (веб-клиента, отправившего исходный запрос), заменяется собственным IP-адресом такого сетевого узла. Для корректного определения реального IP-адреса источника прокси-серверы или балансировщики могут передавать его в специальных HTTP-заголовках, таких как X-Real-IP, X-Forwarded-For или пользовательские заголовки.

В UserGate WAF есть возможность определения реального IP-адреса источника запроса по таким HTTP-заголовкам. Данные, полученные из заголовков X-Real-IP и X-Forwarded-For, а также из пользовательских заголовков, можно использовать для выявления потенциальных угроз, контроля доступа на основе IP-адресов и анализа данных о посетителях сайта.

Алгоритм обработки заголовков X-Real-IP и пользовательских заголовков

HTTP-заголовок X-Real-IP или пользовательский заголовок используется для указания IP-адреса веб-клиента, отправившего исходный запрос. Серверные приложения могут использовать этот заголовок для журналирования или определения местоположения пользователя. Если прокси-сервер, балансировщик или другой сетевой узел передает запрос дальше, этот заголовок может перезаписываться следующим сервером в цепочке.

Если в параметрах правила публикации выбрана обработка заголовка X-Real-IP или пользовательского заголовка, алгоритм обработки этих заголовков выглядит следующим образом:

1. При получении HTTP-запроса UserGate WAF проверяет запрос на наличие заголовка (X-Real-IP или пользовательского заголовка).
2. Если заголовок не найден в запросе, UserGate WAF добавляет его и в качестве реального IP-адреса указывает IP-адрес сетевого узла, передавшего запрос.
3. Если заголовок найден, но не содержит значения, UserGate WAF в качестве реального IP-адреса принимает IP-адрес сетевого узла, передавшего запрос, и добавляет его в заголовок.
4. Если заголовок найден и содержит значение, UserGate WAF выполняет поиск IP-адреса сетевого узла, передавшего запрос, в списке доверенных источников:
 - Если IP-адрес сетевого узла не является доверенным, UserGate WAF заменяет значение в заголовке на этот IP-адрес и принимает его в качестве реального IP-адреса.
 - Если IP-адрес сетевого узла является доверенным, значение в заголовке проверяется на соответствие формату IPv4/IPv6:
 - если формат корректный, UserGate WAF принимает значение, указанное в заголовке, в качестве реального IP-адреса;
 - если формат некорректный, UserGate WAF заменяет значение в заголовке на IP-адрес сетевого узла, передавшего запрос, и принимает его в качестве реального IP-адреса.
5. После обработки запроса значение заголовка, принятое как реальный IP-адрес, сохраняется в записях журнала веб-доступа, а обработанные запросы передаются на анализ и дальнейшую обработку в соответствии с правилами и политикой безопасности в UserGate WAF. При срабатывании правила публикации в записях журнала срабатывания также сохраняется значение реального IP-адреса.

Алгоритм обработки заголовка X-Forwarded-For

HTTP-заголовок X-Forwarded-For содержит список IP-адресов, через которые прошел запрос. IP-адрес веб-клиента, отправившего исходный запрос, добавляется в начало списка, а каждый следующий узел добавляет свой IP-адрес в конец списка. Этот заголовок полезен для отслеживания реального происхождения запроса, особенно в многослойных сетевых конфигурациях.

Пример заголовка:

X-Forwarded-For: 203.0.113.42, 192.168.1.1, 10.0.0.1

Где:

- 203.0.113.42 — IP-адрес веб-клиента, отправившего исходный запрос;
- 192.168.1.1 — IP-адрес первого сетевого узла;
- 10.0.0.1 — IP-адрес второго сетевого узла.

Если в параметрах правила публикации выбрана обработка заголовка X-Forwarded-For, алгоритм обработки этих заголовков выглядит следующим образом:

1. При получении HTTP-запроса UserGate WAF проверяет запрос на наличие заголовка.
2. Если заголовок не найден, UserGate WAF добавляет его и в качестве реального IP-адреса указывает IP-адрес сетевого узла, передавшего запрос.
3. Если заголовок найден, но не содержит значений, UserGate WAF в качестве реального IP-адреса принимает IP-адрес сетевого узла, передавшего запрос, и добавляет его в заголовок.
4. Если заголовок содержит значения и рекурсивный режим выключен, UserGate WAF проверяет формат первого значения (в примере это 203.0.113.42) на соответствие формату IPv4/IPv6:

- Если формат корректный, UserGate WAF принимает этот IP-адрес в качестве реального IP-адреса.
- Если формат некорректный, UserGate WAF принимает IP-адрес сетевого узла, передавшего запрос, в качестве реального IP-адреса.

5. Если заголовок содержит значения и рекурсивный режим включен, UserGate WAF выполняет поиск доверенного IP-адреса, последовательно проверяя значения в заголовке:

- Если первый IP-адрес (в примере это 203.0.113.42) найден в списке доверенных источников, UserGate WAF принимает этот IP-адрес в качестве реального IP-адреса.
- Если доверенный IP-адрес не является первым значением в списке (в примере это 192.168.1.1), UserGate WAF проверяет стоящий перед ним в списке IP-адрес (в примере это 203.0.113.42) на соответствие формату IPv4/IPv6:
 - Если этот IP-адрес прошел проверку, UserGate WAF принимает его в качестве реального IP-адреса.
 - Если этот IP-адрес не прошел проверку, UserGate WAF в качестве реального IP-адреса принимает следующий после него в списке доверенный IP-адрес (в примере это 192.168.1.1).
- Если ни одно из значений в заголовке не является доверенным IP-адресом, UserGate WAF проверяет последнее значение в заголовке на соответствие формату IPv4/IPv6 и в случае успешной проверки принимает последнее значение (в примере это 10.0.0.1) в качестве реального IP-адреса. В противном случае UserGate WAF в качестве реального IP-адреса принимает IP-адрес сетевого узла, передавшего запрос.

6. После обработки запроса значение заголовка, принятое как реальный IP-адрес, сохраняется в записях журнала веб-доступа, а обработанные запросы передаются на анализ и дальнейшую обработку в соответствии с правилами и политиками безопасности в UserGate WAF. При срабатывании правила публикации в записях журнала срабатывания также сохраняется значение реального IP-адреса.

Настройка функции определения реального IP-адреса источника запроса

Чтобы настроить функцию определения реального IP-адреса:

1. В разделе **Настройки → Политика сервисов → Правила публикации** выберите правило, которое необходимо настроить, и нажмите **Редактировать**.
2. В окне **Настройка правила публикации** на вкладке **Реальный IP** установите флажок **Получать реальный IP**.
3. Выберите заголовок, из которого будет извлекаться адрес источника запроса:
 - **X-Real-IP**.
 - **X-Forwarded-For**. При выборе этого заголовка:
 - при необходимости установите флажок **Рекурсивный режим**, чтобы анализировать цепочку IP-адресов в заголовке;
 - при необходимости установите флажок **Добавлять IP-адрес предыдущего узла**, чтобы адрес предыдущего узла, передавшего запрос, был добавлен в конец заголовка.
 - **Пользовательский заголовок**. При выборе этого заголовка укажите его название.
4. Если необходимо, в блоке **Доверенные источники** укажите списки адресов или сетей доверенных источников запроса, например прокси-серверов и балансировщиков.
5. Сохраните изменения.

Примечание Сведения о реальных IP-адресах могут отображаться в разделах «Атаки» и «Журналы и отчеты» → «Журнал веб-доступа».

Балансировка нагрузки

Product: WAF
Version: 7.7.x

UserGate WAF может выполнять балансировку нагрузки на серверы публикации.

Балансировщик распределяет запросы, поступающие на IP-адрес виртуального сервера, на IP-адреса реальных серверов. Чтобы настроить балансировку, необходимо в разделе **Политика сервисов → Балансировка сервисов** создать правила балансировки.

Балансировщик позволяет распределить нагрузку на внутренние серверы или ферму серверов публикации и может быть использован в правилах публикации. Для создания балансировщика необходимо в разделе **Политика сервисов → Балансировка сервисов** нажать **Добавить** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило
Название	Название правила балансировки
Описание	Описание правила балансировки
Серверы публикации	Выбрать серверы публикации, на которые будет распределяться нагрузка. Более подробно о публикации с помощью правил — в разделе « Публикация веб-сервисов »

