

Table of Contents

Table of Contents	1
Глобальный портал	2
Публикация HTTP/HTTPS-ресурсов с помощью reverse-прокси	3

Product: WAF

Version: 7.x

UserGate WAF поддерживает публикацию веб-серверов удаленных приложений в режиме сервера reverse-прокси. Доступ к веб-серверам и безопасность соединений с ними контролируются настраиваемыми правилами reverse-прокси.

Режим сервера reverse-прокси предоставляет следующие возможности:

- **Балансировка нагрузки.** Если обработку запросов к удаленному приложению выполняют несколько веб-серверов, сервер reverse-прокси может равномерно распределять запросы между ними и тем самым предотвращать перегрузку отдельных веб-серверов.
- **Переопределение URL-адресов.** Сервер reverse-прокси может выполнять подмену путей и доменных имен в запросах, чтобы перенаправить их на разные веб-серверы, помогая таким образом разделить трафик для разных приложений.
- **Управление доступом к веб-серверам.** Сервер reverse-прокси может блокировать попытки доступа по идентификационной строке клиентского приложения (useragent) и нежелательным адресам.
- **Поддержка SSL-подключения.** Сервер reverse-прокси может выполнять шифрование и расшифрование запросов и ответов, что позволяет снизить нагрузку на веб-серверы и повысить их производительность.
- **Сигнатурный анализ трафика.** Правила reverse-прокси с подключенными профилями безопасности защищают веб-серверы от атак и других угроз безопасности. Подробнее — в разделе «[Настройки безопасности WAF](#)».
- **Фильтрация WebSocket-трафика.** Сервер reverse-прокси поддерживает обмен трафиком по протоколу WebSocket и обеспечивает безопасность установления WebSocket-соединений (доступно в ПО версии 7.4.1 и выше). Подробнее — в разделе «[Защита WebSocket-соединений](#)».
- **Определение реального IP-адреса источника запроса.** Сервер reverse-прокси может анализировать заголовки HTTP-запросов, чтобы определить реальный IP-адрес (доступно в ПО версии 7.4.0 и выше). Подробнее — в разделе «[Настройка функции определения реального IP-адреса](#)».
- **Фильтрация трафика,** закодированного по стандарту Base64 (доступно в ПО версии 7.4.1 и выше). Подробнее — в разделе «[Фильтрация закодированного трафика](#)».

Чтобы опубликовать веб-сервер:

1. Создайте один или несколько серверов reverse-прокси.
2. Если для доступа к удаленному приложению развернуто несколько веб-серверов, создайте для них правило балансировки.
3. Создайте правила reverse-прокси, которые будут определять условия публикации веб-сервера или группы веб-серверов.

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 reverse-прокси

Чтобы создать сервер reverse-прокси:

1. В разделе **Глобальный портал → Серверы reverse-прокси** нажмите **Добавить**.
 2. В окне **Настройка сервера reverse-прокси** укажите название, IP-адрес или FQDN и TCP-порт публикуемого веб-сервера.
 3. Если необходимо, настройте остальные параметры:
 - Установите флажок **HTTPS до сервера**, чтобы выполнять передачу трафика по защищенному соединению от UserGate WAF до публикуемого веб-сервера. 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 публикуемом веб-сервере. 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 веб-сервер отвечал через тот же сетевой интерфейс UserGate WAF, с которого приходят запросы клиентов. Для этого на веб-сервере 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 серверов reverse-прокси

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

Чтобы создать правило балансировки серверов reverse-прокси:

1. В разделе **Глобальный портал** создайте серверы reverse-прокси для удаленного приложения. Убедитесь, что в окне **Настройка сервера reverse-прокси** для каждого сервера, который участвует в балансировке, в поле **Адрес сервера** указан IP-адрес.
2. В разделе **Настройки** → **Политики сети** → **Балансировка нагрузки** нажмите **Добавить**.
3. В окне **Настройка правила балансировки reverse-прокси** на вкладке **Общие** укажите название правила и включите его.
4. На вкладке **Серверы reverse-прокси** добавьте серверы, на которые будет распределяться нагрузка.
5. Сохраните изменения.

Создание правила reverse-прокси

Правила публикации reverse-прокси позволяют фильтровать запросы к веб-серверам, 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 reverse-прокси:

1. В разделе **Настройки** → **Глобальный портал** → **Правила reverse-прокси** нажмите **Добавить**.
2. В окне **Настройка правила reverse-прокси** на вкладке **Общие**:
 - Включите правило и укажите его название.
 - В списке **Сервер reverse-прокси** выберите сервер или балансировщик reverse-прокси, 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 веб-сервера 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, доменных имен или GeoIP-адреса (не более 15 адресов), для которых будет разрешен обмен трафиком с веб-серверами.

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 производит 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 и/или доменов; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

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 и/или доменов; условия объединяются по И, если указаны GeoIP и списки IP-адресов и/или доменов.

5. На вкладке **Профили безопасности**, если необходимо, включите защиту веб-приложений и WebSocket-соединений. Подробнее об этом — в разделах [«Настройки безопасности WAF»](#) и [«Защита WebSocket-соединений»](#).

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

Примечание Вы 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».

7. На вкладке **Подмена путей** настройте переопределение путей URL. Подробнее о подмене путей — в разделе ниже.

8. Сохраните изменения.

Подмена путей в правилах reverse-прокси

В данном разделе описан порядок работы функции подмены путей в правилах reverse-прокси для версии ПО 7.2.0 и выше.

Подмена путей в правилах reverse-прокси используется для перенаправления HTTP-запроса пользователя на иной путь. Таким образом вы можете управлять разделением трафика для разных сервисов. Например, пользователь выполнил запрос на example.com/path1, а сервер

reverse-прокси перенаправляет запрос на example.local/path2.

Чтобы настроить подмену путей в правиле reverse-прокси:

1. В разделе **Настройки → Глобальный портал → Правила reverse-прокси** создайте или выберите правило.
2. В окне **Настройка правила reverse-прокси** на вкладке **Подмена путей** нажмите **Добавить** и заполните поля:
 - **Изменить с** — домен и/или путь URL, которые требуется изменить. Если в поле **Изменить с** указан домен, то правило reverse-прокси будет применено только для запросов, которые пришли именно на этот домен. То есть в данном случае это будет являться условием срабатывания правила.
 - **Изменить на** — домен и/или путь URL, на которые требуется заменить старый.

ПримечаниеНачиная с версии ПО 7.4.1 вы можете настраивать подмену путей и для кириллических доменов.

ПримечаниеНастройка подмены путей является обязательным условием для создания правила reverse-прокси. Начиная с версии ПО 7.4.1, если необходимо создать правило, но без перенаправления пользовательских запросов, в окне «Подмена путей» можно указать путь только в поле «Изменить с» и установить флажок «Отключить переадресацию».

The diagram illustrates the input fields for the 'Подмена путей' (Path substitution) rule. It shows two rectangular boxes, one for 'Изменить с' (Change from) and one for 'Изменить на' (Change to). Below each box is a horizontal line, likely representing a label or a separator.

3. Сохраните правило.

При обработке HTTP-запроса сработает правило reverse-прокси, паттерн которого в поле **Изменить с** совпадет с путем URL в запросе. При срабатывании правила reverse-прокси происходит подмена пути в HTTP-запросе: паттерн из поля **Изменить с** меняется на паттерн из поля **Изменить на**. Если запрос пользователя не попадет ни под одно правило reverse-прокси, 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 работает 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 reverse-прокси	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 подробнее логику работы подмены путей.

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

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](#).

