

Table of Contents

Table of Contents	1
Настройки безопасности	2
Настройки безопасности WAF	3
Настройка функции определения реального IP-адреса (версия ПО 7.4.0 и выше)	13
Работа с заголовком X-Request-Id	15
Фильтрация закодированного трафика (версия 7.4.1 и выше)	16
Профили ответа (версия 7.5.0 и выше)	17
Защита WebSocket-соединений (версия 7.4.1 и выше)	18

Product: WAF
Version: 7.x
Technology: WAF

Для настройки UserGate WAF необходимо выполнить следующие шаги:

1. Лицензировать WAF.
2. Создать профиль. Профили отвечают за создание и редактирование наборов слоев с UPL-правилами. В профиле могут использоваться как персональные слои с пользовательскими правилами, так и системные слои, содержащие системные правила.
3. В созданном профиле включить слои с необходимыми UPL-правилами.
4. Подключить профиль в правило reverse-прокси.

Системные правила

Системные правила — это правила, загружаемые с серверов UserGate автоматически после активации лицензии. Системные правила отображаются в разделе веб-интерфейса **WAF → Правила**:

У системных правил могут быть изменены следующие параметры:

- состояние (включено/отключено);
- журналирование (включено/отключено);
- действие (No action/Pass/Deny/Force pass/Force deny).

Для редактирования параметров необходимо выбрать нужное правило, нажать **Редактировать** в панели инструментов и в появившемся окне отредактировать соответствующие параметры:

Для быстрого поиска предусмотрен фильтр и сортировка по полям в таблице правил.

В структуре системных правил используются следующие поля:

Название поля	Имя поля	Описание

Название поля	Имя поля	Описание
Уровень угрозы	threat_level	Отображает уровень защиты данного правила • 1 (low): низкий; • 2 (medium): средний; • 3 (high): высокий;
ID правила	id	Отображает идентификатор правила.
Название	name	Название правила.
Ссылка	refs	Отображает ссылки на внешние ресурсы с описаниями уязвимостей.
Время последнего обновления	date	Отображает время последнего обновления правила на серверах UserGate.
Системный слой	layer	Отображает системный слой, к которому относится правило. Системные правила сгруппированы по типам известных уязвимостей: • 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).
Пакет	package name	Название пакета экспертизы, в который входит данное правило.

Название поля	Имя поля	Описание
Действие	action	Действие правила: • No action; • Pass; • Deny; • Force deny; • Force pass. У любого правила в слое может быть префикс PASS, FORCE_PASS, DENY, FORCE_DENY. Когда срабатывает правило с таким префиксом, все остальные правила в слое пропускаются. Срабатывание правила с префиксом FORCE_PASS или FORCE_DENY является окончательным результатом обработки, в противном случае обработка переходит на следующий слой. После обработки всех слоев запрос будет заблокирован или пропущен в зависимости от того, что было последним — DENY/FORCE_DENY или PASS/FORCE_PASS. Действие No action означает, что когда срабатывает правило с таким префиксом, то ничего не предпринимается (за исключением журналирования, если эта опция установлена).

Слои

Слой — это конструкция, используемая для группировки правил и принятия одного решения. Существуют системные и персональные слои.

Системные слои создаются компанией UserGate, они содержат правила, сгруппированные по типам атак.

Принадлежность правил системным слоям можно посмотреть в разделе **WAF → Правила**:

Также состав системного слоя можно посмотреть в свойствах системного слоя. Свойства системного слоя вызываются из профиля WAF. Предусмотрена возможность фильтрации правил в системном слое (Подробнее читайте [ниже](#)).

Нажав на строчку **Настройка правил** в разделе **Правила** можно посмотреть состав системного слоя:

Персональные слои — это наборы UPL-правил, созданные администратором. Раздел **WAF → Персональные слои** в веб-консоли позволяет управлять персональными слоями: создавать, удалять, обновлять и просматривать.

Так как количество слоев может быть большим, в верхней части раздела **Персональные слои** есть фильтр для поиска слоев по имени:

Для создания персонального слоя необходимо нажать **Добавить**, в свойствах персонального слоя указать следующие параметры:

- **Название** — название персонального слоя;
- **Описание** — опциональное описание персонального слоя;
- **Редактирование выражения** — поле для записи/редактирования UPL-выражения, содержащего правила фильтрации трафика;
- **Проверить выражение** — проверка UPL-выражения.

В случае неверного синтаксиса в выражении после проверки будут отображены подсказки и номер строки, где была допущена ошибка:

Подробнее о синтаксисе написания UPL-правил — в разделе [UserGate Policy Language](#).

Профили

Профиль — это набор персональных и/или системных слоев. В разделе веб-интерфейса **WAF → Профили** можно управлять профилями: создавать, удалять,

обновлять и просматривать.

В верхней части страницы **Профили** есть фильтр для поиска профилей по имени:

Для создания профиля необходимо нажать **Добавить**, в свойствах указать следующие параметры:

- **Название** — название профиля;
- **Описание** — опциональное описание профиля;
- **WAF слои** — наборы URL-правил (персональные слои, системные слои), для включения слоя в редактируемый профиль его нужно включить в колонке **Действие**;

В строке **Активных правил** отображает количество активированных правил в профиле.

После сохранения профиля включенные слои автоматически поднимаются вверх в своих группах. Порядок в таком случае определяется так: первый в списке включенный слой поднимается на первое место, затем ищется следующий включенный слой, который поднимается на второе место, и так далее.

Слои можно перемещать только в рамках своих групп, первым идут персональные слои, затем системные.

Включенные слои автоматически поднялись на самый верх списка в своих группах. Можно поменять включенные слои местами (например, передвинуть слой «Layer 3» на самых верх) и после повторного открытия профиля, порядок изменится:

Непосредственно из окна профиля можно создать новый персональный слой. При нажатии кнопки **Добавить персональный слой** откроется диалоговое окно создания персонального слоя:

Предусмотрена возможность фильтровать системные правила в выбранном системном слое, который будет подключен в редактируемый профиль. Для редактирования нужно нажать на системный слой в окне профиля, появится диалоговое окно:

В открывшемся окне предоставлены:

- Флажок для включения/отключения данного системного слоя;
- Технология защиты — фильтр технологий для правил из выбранного системного слоя; в профиль будут подключены правила только с выбранными технологиями;
- Уровень защиты — фильтр правил по уровню защиты; в профиль будут подключены правила только с выбранными уровнями защиты.

Администратор может сбросить в первоначальное состояние выставленные технологии и уровни защиты всего системного слоя, нажав **Восстановить значения по умолчанию**.

Управление WAF-правилами доступно в разделе окна **Правила** по ссылке **Настройка правил**. Открывается таблица, отображающая все отфильтрованные правила, которые будут подключены к редактируемому профилю:

В таблице могут быть изменены следующие параметры отдельных правил, входящих в слой: состояние правила, журналирование, действие и профиль ответа (доступно в версии ПО 7.5.0 и выше). Параметры правил могут быть сброшены в первоначальное состояние с помощью кнопки **Восстановить значения по умолчанию** в панели инструментов.

Для восстановления в исходное состояние всех системных слоев профиля одновременно, необходимо нажать **Восстановить значения по умолчанию** в окне профиля:

Примечание При обновлении экспертизы правила как в профилях, так и в общем списке переводятся в режим логирования (действие — No action, журналирование — включено).

Журналирование правил

Функция журналирования устанавливается на уровне правила.

1. Для системных правил опция журналирования по умолчанию включена. Перенастройка опции журналирования происходит в [окне настройки правил слоя](#) или в общем списке правил, как [указано ранее](#).
2. Для персонального слоя журналирование включается для каждого правила отдельно. Для этого необходимо добавить в UPL-правило свойство " *rule_log(true)*". После этого требуется включить эти слои и сохранить профиль.

Подключение WAF-профиля в правила reverse-прокси

Для активации созданного WAF-профиля необходимо указать его в правилах reverse -прокси. Порядок подключения следующий:

1. Перейти в раздел **Глобальный портал**, выбрать **Правила reverse-прокси**.
2. Нажать кнопку **Добавить**, в появившемся диалоговом окне редактируемого правила выбрать вкладку **WAF**.
3. Поставить флажок **Включить защиту веб-приложений (WAF)**, выбрать необходимый WAF-профиль и сохранить внесенные изменения.

Product: WAF

Version: 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 reverse-прокси 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 политиками безопасности в UserGate WAF. При срабатывании правила 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 reverse-прокси 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 проверят 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 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** → **Глобальный портал** → **Правила reverse-прокси** выберите правило, которое необходимо настроить, и нажмите **Редактировать**.
2. В окне **Настройка правила reverse-прокси** 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:
 - Если необходимо, установите флажок **Рекурсивный режим**, чтобы анализировать цепочку IP-адресов в заголовке.
 - Установите флажок **Добавлять IP-адрес реверс-прокси**, если вы хотите, чтобы адрес прокси-сервера UserGate WAF был добавлен в список IP-адресов в заголовке (доступно в версии 7.4.1 и выше).
 - **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».

Работа с заголовком X-Request-Id

Product: WAF

Version: 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.

WAF проверяет входящие HTTP-запросы на наличие заголовка X-Request-Id и значения идентификатора запроса. Если заголовок X-Request-Id отсутствует, WAF добавляет его в запрос и генерирует уникальное значение идентификатора запроса. Если HTTP-запрос приходит в WAF с уже существующим заголовком X-Request-Id, то 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 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 (версия 7.4.1 и выше)

Product: WAF

Version: 7.x

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.

Если в UserGate WAF настроен reverse-прокси, вы можете создать правила для декодирования и фильтрации таких данных.

Чтобы настроить фильтрацию закодированного трафика:

1. В разделе **Настройки** → **Глобальный портал** → **Правила reverse-прокси** создайте правило. Подробнее о создании и настройке правила reverse-прокси — в разделе [«Создание правила публикации reverse-прокси»](#).
2. В окне **Настройка правила reverse-прокси** 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 вкладка **Base64** станет доступной.
3. На вкладке **Base64** установите флажки для тех элементов клиентского запроса, которые следует проверять на соответствие стандарту кодирования Base64.
4. Укажите количество итераций декодирования для многократно закодированных данных. Максимальное значение — 5.

Примечание Декодирование будет выполняться только для тех элементов запроса, которые были выбраны на шаге 3.

5. Сохраните изменения.

Product: WAF

Version: 7.x

Technology: WAF

В соответствии с политиками безопасности WAF-правила могут блокировать подозрительные запросы к защищаемым веб-ресурсам. С помощью профилей ответа вы можете настроить, какой ответ будет возвращен клиенту при срабатывании блокирующего WAF-правила:

- 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 срабатывании блокирующего WAF-правила 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](#)».**Примечание**Трехзначный 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** → **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 и сохраните изменения.

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

Product: WAF

Version: 7.x

UserGate WAF, работающий в режиме reverse-прокси, может контролировать безопасность установления соединений по протоколу WebSocket.

Протокол WebSocket обеспечивает двустороннюю 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. Двусторонний 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. В разделе **Настройки** → **Политика 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 подключить в правиле reverse-прокси.

Настройка WebSocket-профиля для фильтрации WebSocket-соединений

Чтобы создать WebSocket-профиль, фильтрующий WebSocket-соединения:

1. В разделе **Настройки** → **Политика 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 подключить в правиле reverse-прокси.

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. В разделе **Настройки** → **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. В разделе **Настройки** → **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 слон-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 в правиле reverse-прокси

Чтобы подключить WebSocket-профиль в правиле reverse-прокси:

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

