

Table of Contents

Table of Contents	1
Библиотеки элементов	2
Описание	3
JSON-схемы	4
XML-схемы	7
IP-адреса	9
Useragent браузеров	11
Списки URL	13
Календари	16
Шаблоны страниц	17
Почтовые адреса	18
Профили Netflow	20
Профили LLDP	21
Профили SSL	22
Профили оповещений	25
Номера телефонов	26

Описание

Version: 7.7.x

Product: WAF

Данный большой раздел содержит в себе все записи, адреса сайтов, IP-адреса, шаблоны и прочие элементы, которые используются при настройке правил в UserGate WAF.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередатируемыми, потому что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, имеют механизм автоматического обновления. Автоматическое обновление элементов требует наличия специальной лицензии. Подробнее о лицензии на продукт — в разделе «[Лицензирование](#)».

Version: 7.7.x

Product: WAF

Documentation: 

JSON-схемы описывают структуру и ограничения JSON-данных. Схема представляет собой JSON-документ, в котором задаются допустимые поля и их типы, обязательность полей, разрешенные значения и другие правила проверки.

JSON-схемы, добавленные в JSON-профиль, используются для проверки запросов, содержащих данные в формате JSON. В отличие от синтаксической проверки, которая определяет только корректность формата JSON, схема проверяет соответствие данных заданным требованиям: допустима ли такая структура, присутствуют ли обязательные поля и соответствуют ли значения установленным ограничениям.

Действия с JSON-схемами выполняются в разделе **Настройки** в разделе **Библиотеки → JSON-схемы**. Вы можете создавать схемы, редактировать их и удалять, а также выполнять экспорт и импорт схем.

Создание JSON-схемы

Чтобы создать JSON-схему:

1. В разделе **Библиотеки → JSON-схемы** нажмите **Добавить**. Откроется окно свойства JSON-схемы.
2. Укажите название схемы, при необходимости описание и версию спецификации.

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

3. В поле **Содержимое схемы** опишите JSON-схему.

ПримечаниеВы также можете загрузить JSON-схему из файла, нажав «Загрузить файл».

4. Нажмите **Проверить синтаксис**. Если результат проверки неудовлетворительный, внесите исправления и повторно выполните проверку.

5. Сохраните изменения.

Теперь созданную JSON-схему можно использовать при настройке JSON-профиля. Подробнее об этом — в разделе « [Создание JSON-профиля](#) ».

Общие сведения о JSON-схемах

Любая JSON-схема — это JSON-объект с ключевыми словами (ключами), описывающими ограничения. Основные четыре ключа:

- `schema` — указывает версию спецификации схемы.
- `type` — тип данных (объект, строка, число и т. д.);
- `properties` — описание полей объекта, где каждый ключ — имя поля, а значение — подсхема для этого поля.;
- `required` — массив имен полей, которые должны присутствовать.

ПримечаниеКлюч `required` проверяет только наличие обязательных полей, но не их значения. Пустая строка, `null` или неверный тип будут проверяться другими ключами схемы.

Ключ `type` ограничивает допустимый тип значения. Возможные типы:

- `"string"` — строка;
- `"number"` — число (целое или с плавающей точкой);
- `"integer"` — целое число (без дробной части);
- `"boolean"` — булево значение (`true` или `false`);
- `"null"` — значение `null`;
- `"object"` — объект `{ ... }`;
- `"array"` — массив `[ ... ]`.

Тип можно указать как строку или как массив строк, если допустимо несколько типов.

Также JSON-схемы могут содержать ограничения для строк, чисел, массивов, в том числе вложенных, перечислений и констант.

Подробнее о структуре JSON-схем — в спецификациях: [Draft 03](#), [Draft 04](#), [Draft 06](#).

Пример JSON-схемы.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "id": "http://example.com/user.schema.json",
  "title": "User Schema",
  "description": "Схема для описания пользователя",

```

```
"type": "object",
"properties": {
  "id": {
    "description": "Уникальный идентификатор пользователя",
    "type": "integer",
    "minimum": 1
  },
  "username": {
    "description": "Имя пользователя",
    "type": "string",
    "minLength": 3,
    "maxLength": 20,
    "pattern": "^[a-zA-Z0-9_]+$"
  },
  "email": {
    "description": "Email адрес",
    "type": "string",
    "format": "email"
  },
  "age": {
    "description": "Возраст пользователя",
    "type": "integer",
    "minimum": 0,
    "maximum": 150
  },
  "isActive": {
    "description": "Статус активности",
    "type": "boolean"
  },
  "roles": {
    "description": "Роли пользователя",
    "type": "array",
    "items": {
      "type": "string",
      "enum": ["admin", "user", "guest"]
    },
    "minItems": 1,
    "uniqueItems": true
  },
  "address": {
    "description": "Адрес пользователя",
    "type": "object",
    "properties": {
      "street": {
        "type": "string"
      },
      "city": {
        "type": "string"
      },
      "zipCode": {
        "type": "string",
        "pattern": "^[\\d]{5}$"
      }
    },
    "required": ["street", "city"]
  },
  "phoneNumbers": {
    "description": "Список телефонных номеров",
    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "type": {
          "type": "string",
          "enum": ["home", "work", "mobile"]
        },
        "number": {
          "type": "string"
        }
      },
      "required": ["type", "number"]
    }
  },
  "createdAt": {
    "description": "Дата создания",
    "type": "string",
    "format": "date-time"
  }
},
"required": ["id", "username", "email", "age"],
"additionalProperties": false
```


Version: 7.7.x

Product: WAF

Documentation: ☒

XML-схема — это описание структуры и правил, которым должен соответствовать XML-документ. Схема определяет, какие элементы и атрибуты могут присутствовать в документе, в каком порядке они располагаются, какие значения могут содержать и какие из них являются обязательными.

В UserGate WAF XML-схемы используются для проверки запросов, содержащих данные в формате XML. В отличие от синтаксической проверки, которая определяет только корректность формата XML, схема проверяет соответствие данных заданным требованиям: допустима ли такая структура, присутствуют ли обязательные поля и соответствуют ли значения установленным ограничениям.

Действия с XML-схемами выполняются в разделе **Настройки** в разделе **Библиотеки → XML-схемы**. Вы можете создавать схемы, редактировать их и удалять, а также выполнять экспорт и импорт схем.

Создание XML-схемы

Чтобы создать XML-схему:

1. В разделе **Библиотеки → XML-схемы** нажмите **Добавить**. Откроется окно свойства XML-схемы.
2. Укажите название схемы, при необходимости описание и версию спецификации.
3. В поле **Содержимое схемы** опишите XML-схему.

Примечание Вы также можете загрузить XML-схему из файла, нажав «Загрузить файл».

4. Нажмите **Проверить синтаксис**. Если результат проверки неудовлетворительный, внесите исправления и повторно выполните проверку.
5. Сохраните изменения.

Теперь созданную XML-схему можно использовать при настройке XML-профиля. Подробнее об этом — в разделе « [Создание XML-профиля](#) ».

Общие сведения о XML-схемах

Простейшая XML-схема имеет следующий вид:

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="user">
    <xs:complexType>
      <xs:sequence>

        <xs:element name="name" type="xs:string"/>
        <xs:element name="age" type="xs:integer"/>

      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

XML-схема состоит из следующих основных элементов

- **xs:schema** — корневой элемент, внутри которого описываются все элементы схемы, типы данных, атрибуты и другие правила структуры XML-документа.
- **xmlns:xs** — объявляет пространство имен XML Schema. Пространство имен определяет, к какой схеме или модели данных относится XML-элемент. Оно позволяет использовать одинаковые имена элементов в разных схемах и при этом не путать их.
- **xs:element** — описывает элемент XML-документа. В примере атрибут `name` задаёт имя элемента, а `type` — его тип данных.
- **xs:simpleType** — используется для создания простого типа данных на основе стандартного типа. Это позволяет дополнительно ограничивать допустимые значения.
- **xs:complexType** — описывает структуру сложного элемента, который может содержать вложенные элементы или атрибуты.
- **xs:sequence** — описывает последовательность вложенных элементов.
- **xs:attribute** — описывает атрибут XML-элемента.
- **type** — тип данных элемента или атрибута;
- **minOccurs/maxOccurs** — количество допустимых вхождений элементов. Если эти атрибуты не указаны, элемент по умолчанию является обязательным и может встречаться один раз.

XML-схема содержит набор встроенных типов данных. Наиболее часто используются:

- `xs:string` — строка;
- `xs:integer` — целое число;
- `xs:decimal` — десятичное число;
- `xs:boolean` — булево значение (`true` или `false`);
- `xs:date` — дата;
- `xs:dateTime` — дата и время;
- `xs:anyURI` — URI.

IP-адреса

Version: 7.7.x
Product: WAF

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил UserGate WAF. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать список.	На панели Группы нажать на кнопку Добавить , дать название списку IP-адресов
Шаг 2. Указать адрес обновления списка (не обязательно).	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе
Шаг 3. Добавить IP-адреса.	На панели Адреса из выбранной группы нажать на кнопку Добавить и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все узлы UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл list.txt со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: x.x.x.x y.y.y.y z.z.z.z
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания

Наименование	Описание
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом UserGate WAF создать список IP-адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Useragent браузеров

Version: 7.7.x

Product: WAF

С помощью фильтрации по Useragent браузеров администратор может запретить или разрешить работу пользователей только с определенным типом браузеров.

Первоначальный список Useragent поставляется вместе с продуктом. Для фильтрации по типу Useragent необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список Useragent.	В панели Категории нажать на кнопку Добавить и задать название нового списка Useragent, опционально, описание списка и URL обновления
Шаг 2. Добавить необходимые Useragent браузеров в новый список.	В панели Шаблоны useragent добавить необходимый Useragent. Исчерпывающий список строк Useragent представлен тут: http://www.useragentstring.com/pages/useragentstring.php
Шаг 3. Создать URL-правило, содержащее один или несколько списков.	Подробнее о персональных слоях — в разделе « Настройка параметров безопасности WAF »

Администратор имеет возможность создавать свои списки Useragent и централизованно распространять их на все узлы UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми Useragent.	Создать файл list.txt со списком Useragent
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания

Наименование	Описание
Шаг 5. Создать список Useragent и указать URL для обновления.	На каждом UserGate WAF создать список Useragent. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Списки URL

Version: 7.7.x

Product: WAF

Страница предназначена для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Наименование	Описание
Список поисковых систем без безопасного поиска	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля
Соответствие списку запрещенных URL Министерства Юстиции РФ	Данный список содержит URL, запрещенные Министерством Юстиции Российской Федерации
Соответствие списку запрещенных URL Республики Казахстан	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан
Список образовательных учреждений	Список доменных имен образовательных учреждений РФ
Список фишинговых сайтов	Данный список содержит URL фишинговых сайтов
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru

Для фильтрации с помощью списков URL необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать список URL.	В разделе Библиотеки → Списки URL нажать на кнопку Добавить, задать название нового списка. Выбрать Тип списка — Локальный или Обновляемый. Для обновляемого списка указать URL обновления и настроить Расписание скачивания обновлений. Установить категорию создаваемого списка в поле Чувствительность к регистру: • Чувствительный к регистру — список URL адресов, чувствительных к регистру букв в адресе. • Нечувствительный к регистру — список URL адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах. • Домен — список адресов доменов для использования в правилах DNS-фильтрации. Категория списка задается при его создании. Изменить категорию после создания списка нельзя
Шаг 2. Добавить необходимые записи в новый список.	Добавить записи URL в новый список. В списках можно использовать специальные символы «^», «\$» и «*»: «*» — любое количество любых символов «^» — начало строки «\$» — конец строки Символы «?» и «#» не могут быть использованы

Наименование	Описание
Шаг 3. Создать URL-правило, содержащее один или несколько списков.	Подробнее о персональных слоях — в разделе « Настройка параметров безопасности WAF »

Если URL-запись начинается с http://, «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S) фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

Внимание! Спецсимволы не работают в списках-исключениях для блокировки рекламы. В этих списках применение спецсимволов не рекомендуется.

Если вы хотите заблокировать точный адрес, используйте символы «^» и «\$»:

^http://domain.com/exacturl\$

Для блокирования точного URL всех дочерних папок используйте символ «^»:

^http://domain.com/exacturl/

Для блокирования домена со всеми возможными URL используйте запись такого вида:

domain.com

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Блокируется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com mail.yahoo.com а также: qweryahoo.com	Блокируется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123 http://qwertyyahoo.com/
^mail.yahoo.com\$	Заблокирован только mail.yahoo.com	Заблокированы только: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/\$	Ничего не заблокировано	Ничего не заблокировано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/\$	Ничего не заблокировано	Заблокирован только: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не заблокировано	Заблокированы: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все узлы UserGate WAF. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл list.txt со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания
Шаг 5. Создать список и указать URL для обновления.	На каждом UserGate WAF создать список URL. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в Linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Календари

Version: 7.7.x
Product: WAF

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах WAF. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать календарь.	В панели Группы нажать на кнопку Добавить , указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели Элементы нажать на кнопку Добавить и добавить интервал. Дать название интервалу и указать время.

Шаблоны страниц

Version: 7.7.x

Product: WAF

С помощью шаблонов страниц вы можете настраивать вид страницы блокировки или страницы сетевых ошибок.

Шаблон страницы блокировки предназначен для настройки ответа, который возвращается клиенту, чей запрос был заблокирован WAF-правилом. Подробнее об этом — в разделе «[Профили ответа](#)».

Шаблон страницы сетевых ошибок предназначен для отображения информации об ошибках в работе сервера публикации.

Чтобы создать шаблон страницы:

1. На странице **Настройки** в разделе **Библиотеки → Шаблоны страниц** нажмите **Добавить** и выберите, шаблон какой страницы вы хотите создать.
2. В окне **Свойства шаблона страницы** укажите его название, выберите стандартный шаблон на нужном языке и, если необходимо, назначьте его шаблоном по умолчанию.

Примечание Чтобы применить созданный шаблон страницы сетевых ошибок, его нужно назначить шаблоном по умолчанию.

3. Сохраните изменения.

По умолчанию шаблоны страниц настроены на отображение минимальной информации в стандартном оформлении. Вы можете использовать их в качестве основы для создания пользовательских шаблонов в фирменном стиле компании, на другом языке или с дополнительными блоками информации.

Чтобы создать пользовательский шаблон страницы:

1. Добавьте новый шаблон страницы нужного типа.
2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.
3. Используя текстовый редактор, откройте страницу и внесите нужные изменения.

Примечание Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.

4. Импортируйте измененную страницу в созданный шаблон.

Теперь, чтобы использовать пользовательский шаблон страницы блокировки, необходимо создать профиль ответа с этим шаблоном и затем этот профиль выбрать в параметрах блокирующих WAF-правил. Чтобы использовать пользовательский шаблон страниц сетевых ошибок, его достаточно назначить шаблоном по умолчанию.

Почтовые адреса

Version: 7.7.x
Product: WAF

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов.	В панели Группы почтовых адресов нажать на кнопку Добавить , дать название группе
Шаг 2. Добавить почтовые адреса в группу.	Выделить созданную группу, в панели Почтовые адреса нажать на кнопку Добавить и добавить необходимые почтовые адреса

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все устройства UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл list.txt со списком почтовых адресов
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания

Наименование	Описание
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом UserGate WAF создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

Профили Netflow

Version: 7.7.x
Product: WAF

Netflow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу Netflow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Анализатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

UserGate WAF может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс UserGate WAF, необходимо выполнить следующие действия:

1. Создать профиль Netflow.
2. Назначить созданный профиль Netflow сетевому интерфейсу, на котором необходимо собирать статистику.

Для создания профиля Netflow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили Netflow** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля Netflow
Описание	Описание профиля Netflow
IP-адрес Netflow коллектора	IP-адрес сервера, куда сенсор будет отправлять статистику
Порт Netflow коллектора	UDP-порт, на котором коллектор будет принимать статистику
Версия протокола	Версия протокола Netflow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе
Таймаут активного потока (сек)	При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию — 1800 секунд
Таймаут неактивного потока (сек.)	Время, резервируемое на завершение неактивного потока. Значение по умолчанию — 15 секунд
Количество потоков	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию — 2000000, установите 0 для снятия ограничения
Отправлять информацию NAT	Отправлять информацию о NAT преобразованиях в статистику Netflow
Частота отправки шаблона (пакетов)	Количество пакетов, после которых шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов
Период отправки старого шаблона (сек.)	Время, через которое старый шаблон отправляется на принимающий хост (только для Netflow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд

Профили LLDP

Product: WAF
Version: 7.7.x

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевым устройствам, работающим в локальной сети, объявлять о своём существовании и передавать свои характеристики и получать аналогичные сведения. Информация, собранная при помощи операции LLDP, хранится в сетевом устройстве.

Для создания профиля безопасности необходимо нажать **Добавить** в разделе **Библиотеки → Профили LLDP** и указать следующие параметры:

Наименование	Описание
Название	Название профиля LLDP
Описание	Описание профиля LLDP
Статус порта	Режим: • Приём и передача данных LLDP — UserGate WAF будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • Только приём данных LLDP — UserGate WAF не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • Только передача данных LLDP — UserGate WAF будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей

Профили SSL

Version: 7.7.x
Product: WAF

Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, которые в дальнейшем могут быть использованы в настройках веб-консоли, в настройках правил reverse-прокси.

Для создания профиля SSL необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля SSL
Описание	Описание профиля SSL
Протоколы SSL	Минимальная версия TLS — устанавливает минимальную версию TLS, которая может быть использована в данном профиле. Максимальная версия TLS — устанавливает максимальную версию TLS, которая может быть использована в данном профиле. Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем
Наборы	Данный раздел позволяет выбрать необходимые алгоритмы шифрования и цифровой подписи. Возможные значения указаны в виде строк, в которых перечислены алгоритм и подпись. Администратор может указать только те наборы алгоритмов и подписей, которые считает нужным для безопасной работы организации. Список поддерживаемых комбинаций следующий: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256 • TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384 • TLS ECDH ECDSA WITH AES 256 GCM SHA384 • TLS ECDH RSA WITH 3DES EDE CBC SHA

алгоритмов шифрования	Описание
	• TLS ECDH RSA WITH AES 128 CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA256 • TLS ECDH RSA WITH AES 128 GCM SHA256 • TLS ECDH RSA WITH AES 256 CBC SHA • TLS ECDH RSA WITH AES 256 CBC SHA384 • TLS ECDH RSA WITH AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH 3DES EDE CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA256 • TLS ECDHE ECDSA WITH AES 128 GCM SHA256 • TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS GOST2012256 WITH 28147 CNT IMIT • TLS GOSTR341001 WITH 28147 CNT IMIT • TLS RSA WITH 3DES EDE CBC SHA • TLS RSA WITH AES 128 CBC SHA • TLS RSA WITH AES 128 CBC SHA256 • TLS RSA WITH AES 128 GCM SHA256 • TLS RSA WITH AES 256 CBC SHA • TLS RSA WITH AES 256 CBC SHA256 • TLS RSA WITH AES 256 GCM SHA384
Установка алгоритмов шифрования для стандартных протоколов	Данный раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле Выберите протокол для установки алгоритмов необходимые версии протоколов TLS, нажать на кнопку Применить, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно последовательно добавить несколько версий протокола TLS

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором как есть, либо изменены/удалены при необходимости. Созданы следующие профили SSL:

Наименование	Описание
Default SSL profile	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.1 до TLS v.1.2. Это наиболее распространенные версии протоколов, используемые в сети интернет в данное время
Default SSL profile (TLSv1.3)	Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется

Наименование	Описание
Default SSL profile (GOST)	Содержит алгоритмы и подписи, соответствующие TLS с ГОСТ-алгоритмами (TLS GOST2012256 with 28147 CNT IMIT и TLS GOSTR341001 with 28147 CNT IMIT). Может быть использован в организациях, где требуется использование данных алгоритмов, например, для веб-портала. Поддержка данных протоколов должна также быть обеспечена со стороны используемых браузеров. По умолчанию не используется
Default SSL profile (web console)	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.0 до TLS v.1.2. Данный профиль используется по умолчанию для предоставления SSL-доступа в веб-консоль. Важно! Изменение данного профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа в веб-консоль!

Профили оповещений

Version: 7.7.x

Product: WAF

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP: доставка сообщений по электронной почте.
- SMPP: доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля SMTP-сообщений необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Хост	IP-адрес или FQDN SMTP-сервера, который будет использоваться для отсылки почтовых сообщений
Порт	TCP-порт, используемый SMTP-сервером. Обычно для SMTP-протокола используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL
Авторизация	Включает авторизацию при подключении к SMTP-серверу
Логин	Имя учетной записи для подключения к SMTP-серверу
Пароль	Пароль учетной записи для подключения к SMTP-серверу

Для создания профиля SMPP-сообщений необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля
Описание	Описание профиля
Хост	IP-адрес или FQDN SMPP-сервера, который будет использоваться для отсылки SMS-сообщений
Порт	TCP-порт TCP, используемый SMPP-сервером. Обычно для SMPP-протокола используется порт 2775, для SMPP с использованием SSL -- 3550.
SSL	Использовать или нет шифрацию с помощью SSL
Логин	Имя учетной записи для подключения к SMPP-серверу
Пароль	Пароль учетной записи для подключения к SMPP-серверу
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8

Номера телефонов

Version: 7.7.x
Product: WAF

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров.	В панели Группы телефонных номеров нажать на кнопку Добавить , дать название группе
Шаг 2. Добавить номера телефонов в группу.	Выделить созданную группу, в панели Группа телефонных номеров нажать на кнопку Добавить и добавить необходимые номера

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все узлы UserGate WAF. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл list.txt со списком номеров
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate WAF создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate WAF будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа"

UserGate WAF может проверять чек-сумму файлов обновляемых списков. Для приведенного примера UserGate WAF будет запрашивать файл **list.zip.md5**, содержащий чек-сумму файла **list.zip**. Его наличие не обязательно, но если он есть, чек-сумма должна быть корректной. Получить чек-сумму в linux можно командой:

```
md5sum list.zip
```

Её вывод добавляется в файл как хэш **list.zip**, после чего сохраняется в формате md5. Например, содержимое файла **list.zip.md5**:

```
04d7d1223ba8ff02396355a2bc3b3d52 list.zip
```

