

Table of Contents

Table of Contents	1
Настройки безопасности	2
Настройка параметров безопасности WAF в CLI	3
Настройка профиля ответа в CLI (версия 7.5.0 и выше)	5
Настройка WebSocket-профилей в CLI (версия 7.4.1 и выше)	6

Настройка параметров безопасности WAF в CLI

Product: WAF
Version: 7.x
Technology: WAF

Настройка персональных слоев

Персональные слои WAF настраиваются на уровне waf custom-layers с использованием языка описания политик UPL. Подробнее о структуре команд — в разделе [UserGate Policy Language](#).

Для создания персонального слоя используется команда:

```
Admin@nodename# create waf custom-layers name <custom_layer_name> description <description> upl-rule
```

Команда для изменения параметров персонального слоя:

```
Admin@nodename# set waf custom-layers <custom_layer_name> upl-rule
```

Команда для отображения информации о всех персональных слоях:

```
Admin@nodename# show waf custom-layers
```

Команда для отображения информации об определенном персональном слое:

```
Admin@nodename# show waf custom-layers <custom_layer_name>
```

Пример создания тестового персонального слоя с использованием UPL:

```
Admin@nodename# create waf custom-layers name "Layer 2" upl-rule DENY src.ip = lib.network("Bad ips", "Test ips")
DENY dst.ip = lib.network("Bad ips")
PASS request.header.User-Agent = lib.useragent(Browsers)
DENY time = lib.time(Weekends)
Admin@nodename#
Admin@nodename# show waf custom-layers "Layer 2"
```

```
name      : Layer 2
upl-rule   : DENY src.ip = lib.network("Bad ips", "Test ips")
DENY dst.ip = lib.network("Bad ips")
PASS request.header.User-Agent = lib.useragent(Browsers)
DENY time = lib.time(Weekends)
```

```
Admin@nodename#
```

Команда для удаления существующего персонального слоя:

```
Admin@nodename# delete waf custom-layers <custom_layer_name>
```

Настройка WAF-профилей

WAF-профили настраиваются на уровне waf profiles.

Для создания WAF-профиля используется команда:

```
Admin@nodename# create waf profiles name <profile_name> description <description> enable-layers [ layer_1 layer_2 layer_n ]
```

Команда для изменения параметров WAF-профиля:

```
Admin@nodename# set waf profiles <profile_name> name <new_name> description <new_description> enable-layers [ list of layers to enable ] system
<change_system_layer>
```

Команда для изменения профиля ответа в WAF-профиле (доступно с версии 7.5.0):

```
Admin@nodename# set waf profiles system overridden-rules rules-names [ "#RefRef DoS tool (1)" "#RefRef DoS tool (2)" ] response-profile <tab>
```

По умолчанию выбрано значение Do not use. Другие значения станут доступны после того, как будут созданы профили ответов.

Команда для отображения информации о всех WAF-профилях:

```
Admin@nodename# show waf profiles
```

Команда для отображения информации об определенном WAF-профиле:

```
Admin@nodename# show waf profiles <profile_name>
```

Пример создания WAF-профиля:

```
Admin@nodename# create waf profiles name "Test profile 1" description "Test profile #1" enable-layers [ "Layer 4 (custom)" "HTTP Constraint" ]
Admin@nodename#
Admin@nodename# show waf profiles "Test profile 1"
```

```
name      : Test profile 1
description : Test profile #1
```

enable-layers : Layer 4 (custom); HTTP Constraint

Admin@nodename#

Команда для удаления существующего WAF-профиля:

Admin@nodename# delete waf profiles <profile_name>

Настройка параметров системных правил

Параметры системных правил настраиваются на уровне waf system-rules (доступно с версии 7.4.0).

У системных правил могут быть изменены следующие параметры:

- состояние (enabled) — on/off;
- журналирование (enable-logging) — on/off;
- действие (action) — pass, deny, force-pass, force-deny;
- профиль ответа (response-profile) — do not use, <response-profile name> (доступно в версии ПО 7.5.0 и выше).

Пример команды настройки системного правила:

```
Admin@nodename# set waf system-rules rules ["#RefRef DoS tool (1)"] enabled on enable-logging on action deny response-profile "<response-profile name>"
```

В квадратных скобках указывается название одного или нескольких системных правил, к которым применяются изменения параметров. Названия правил указываются в кавычках и разделяются пробелами.

Пример команды изменения параметров нескольких системных правил:

```
Admin@oulineeladin# set waf system-rules rules ["#RefRef DoS tool (1)" "#RefRef DoS tool (2)"] enabled off
```

Команда для отображения информации о всех системных правилах:

```
Admin@nodename# show waf system-rules
```

Пример отображения информации об определенном системном правиле:

```
Admin@oulineeladin# show waf system-rules "#RefRef DoS tool (1)"
```

```
name      : #RefRef DoS tool (1)
enabled   : on
action     : deny
description : This event is triggered when a malicious/suspicious user-agent is detected in the request.
reference  : https://www.owasp.org/index.php/Denial_of_Service
threat-level : medium
technology : All systems
layer      : Denial of Service
enable-logging : on
last-update : 2016-03-17T00:00Z
response-profile : Do not use
```

Просмотр системных слоев

Команда для отображения информации об имеющихся системных слоях:

```
Admin@nodename# show waf system-layers
```

Команда для отображения информации о конкретном системном слое:

```
Admin@minhanhicon# show waf system-layers <system_layer_name>
```

Настройка профиля ответа в CLI (версия 7.5.0 и выше)

Product: WAF

Version: 7.x

Technology: WAF

Настройка профиля ответа выполняется на уровне response-profiles.

Для создания профиля ответа используется следующая команда:

```
Admin@nodename# create security-policy response-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название профиля ответа
response-type	Выбор политики, определяющей, какой ответ будет возвращен клиенту при срабатывании блокирующего WAF-правила: • redirect — перенаправление запроса на страницу указанного ресурса. Доступны следующие параметры: ◦ custom-redirect — ссылка на ресурс для перенаправления запроса. ◦ response-code — трехзначный код состояния HTTP (должен начинаться с цифры 3). ◦ response-text — текст ответа. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду. • tcp-rst — сообщение о разрыве соединения. • response-page — страница блокировки с указанием кода состояния HTTP. Доступны следующие параметры: ◦ template — указание шаблона страницы. ◦ response-code — трехзначный код состояния HTTP (должен начинаться с цифры 1, 2, 4 или 5). ◦ response-text — текст ответа. Если поле текста ответа не заполнено, будет использован текст по умолчанию, соответствующий указанному коду.
description	Описание профиля ответа

Команда для редактирования параметров профиля ответа:

```
Admin@nodename# set security-policy response-profiles <response-profile_name> <parameter>
```

Параметры, доступные для обновления, представлены в таблице выше.

Команда для удаления профиля ответа:

```
Admin@nodename# delete security-policy response-profiles <response-profile_name>
```

Команда для отображения информации о всех профилях ответа:

```
Admin@nodename# show security-policy response-profiles
```

Команда для отображения информации об определенном профиле ответа:

```
Admin@nodename# show security-policy response-profiles <response-profile_name>
```

Настройка WebSocket-профилей в CLI (версия 7.4.1 и выше)

Product: WAF

Version: 7.x

Technology: WAF

Настройка WebSocket-профилей происходит на уровне **websocket-profiles**.

Для создания WebSocket-профилей используется следующая команда:

```
Admin@nodename# create security-policy websocket-profiles <parameter>
```

Далее необходимо задать следующие параметры.

Параметр	Описание
name	Название WebSocket-профиля
description	Описание WebSocket-профиля
block	Включение/отключение блокирования любого WebSocket-трафика, который приходит в UserGate WAF: • On; • Off
check-request	Проверка целостности handshake-запроса: • On; • Off
log	Включение/отключение журналирования событий: • On; • Off
check-origin	Проверка наличия в запросе заголовка Origin: • On; • Off
origin	Добавление списка URL источников, с которыми разрешается устанавливать WebSocket-соединение. Подробнее о создании списков URL в разделе — «Настройка списков URL»
origin-negate	Добавление списка URL нежелательных источников. WebSocket-соединения с ними будут игнорироваться
check-extension	Включение/отключение проверки расширений в заголовке Sec-WebSocket-Extensions: • On; • Off
extension	Добавление списка разрешенных расширений. WebSocket-соединения будут устанавливаться только по тем запросам, в заголовках которых указаны разрешенные расширения
extension-negate	Инвертация проверки по списку, указанному в параметре extension : • On; • Off. WebSocket-соединения по запросам, в заголовках которых указаны расширения из списка, будут игнорироваться

Параметр	Описание
check-protocol	Включение/отключение проверки субпротоколов в заголовке Sec-WebSocket-Protocols: • On; • Off
protocol	Добавление списка разрешенных субпротоколов. WebSocket-соединения будут устанавливаться только по тем запросам, в заголовках которых указаны разрешенные субпротоколы
protocol-negate	Инвертация проверки по списку, указанному в параметре protocol: • On; • Off. WebSocket-соединения по запросам, в заголовках которых указаны субпротоколы из списка, будут игнорироваться

Команда для редактирования параметров WebSocket-профиля:

```
Admin@nodename# set security-policy websocket-profiles <websocket-profile_name> <parameter>
```

Команда для отображения информации о всех WebSocket-профилях:

```
Admin@nodename# show security-policy websocket-profiles
```

Команда для отображения информации об определенном WebSocket-профиле:

```
Admin@nodename# show security-policy websocket-profiles <profile_name>
```

Команда для удаления существующего WebSocket-профиля используется следующая команда:

```
Admin@nodename# delete security-policy websocket-profiles <profile_name>
```

