

Table of Contents

Table of Contents	1
Настройка публикации веб-сервисов	2
Настройка серверов публикации	3
Настройка правил публикации	4
Настройка балансировки нагрузки	7

Настройка серверов публикации

Product: WAF

Version: 7.7.x

Настройка серверов публикации производится на уровне **global-portal reverse-proxy-servers**.

Для создания сервера публикации используется следующая команда:

```
Admin@nodename# create global-portal reverse-proxy-servers <parameter>
```

Доступно указание следующих параметров:

Параметр	Описание
name	Название сервера публикации
description	Описание сервера публикации
address	Адрес или домен сервера публикации
port	TCP-порт сервера публикации
https	Использование протокола HTTPS до публикуемого сервера: • on: использовать. • off: не использовать.
keep-source-ip	Использование оригинального IP-адреса источника в пакетах, пересылаемых на публикуемый сервер: • on: оставить оригинальный IP-адрес источника. • off: заменить IP-адрес источника на IP-адрес UserGate. Важно!Если в пакетах сохраняется оригинальный 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.

Команда для редактирования параметров сервера публикации:

```
Admin@nodename# set global-portal reverse-proxy-servers <server-name> <parameter>
```

Параметры, которые могут быть обновлены, аналогичны с параметрами команды для добавления нового сервера.

Структура команды для отображения информации о сервере публикации:

```
Admin@nodename# show global-portal reverse-proxy-servers <server-name>
```

Структура команды для удаления сервера публикации:

```
Admin@nodename# delete global-portal reverse-proxy-servers <server-name>
```

Настройка правил публикации

Product: WAF

Version: 7.7.x

Правила публикации в интерфейсе командной строки настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд — в разделе «[UserGate Policy Language](#)».

Структура команды для создания правила публикации:

```
Admin@nodename# create global-portal reverse-proxy-rules <position> upl-rule <parameters>
```

Параметры настройки правил публикации:

Параметр	Описание
OK	Действие для создания правила публикации с помощью UPL
enabled	Включение/отключение правила публикации: - enabled(yes) или enabled(true) — включение; - enabled(no) или enabled(false) — отключение
name	Название правила публикации. Например, name("Reverse proxy rule example")
desc	Описание правила публикации. Например, desc("Reverse proxy rule example set via CLI")
profile	Сервер публикации, куда UserGate WAF будет пересылать запросы. Для указания сервера: profile("Reverse proxy server example")
url.port	Порт, на котором UserGate WAF будет слушать входящие запросы. Например, url.port = 80
is_https	Поддержка HTTPS: - is_https(yes) или is_https(true) — использовать HTTPS; - is_https(no) или is_https(false) — не использовать HTTPS.
ssl_profile	Профиль SSL; указывается при использовании HTTPS: ssl_profile("Default SSL profile"). Подробнее о работе с профилями SSL через CLI — в разделе « Настройка профилей SSL »
certificate	Сертификат, используемый для поддержки HTTPS-соединения. Указывается при использовании HTTPS: certificate("Certificate example")
cert_auth_enabled	Аутентификация по сертификату: - cert_auth_enabled(yes) или cert_auth_enabled(true) — включить авторизацию по сертификату; - cert_auth_enabled(no) или cert_auth_enabled(false) — отключить авторизацию по сертификату
src.zone	Зона источника трафика. Для указания зоны источника, например Untrusted: src.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: <code>src.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, <code>src.geoip = RU</code>). Коды названий стран доступны по ссылке: ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15
user	Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (подробнее о настройке LDAP-коннектора через CLI — в разделе «Настройка LDAP-коннектора»). Пример добавления локального пользователя (<code>local_user</code>) и группы (<code>Local Group</code>), пользователя (<code>example.local\AD_user</code>) и группы LDAP (<code>AD group</code>): <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> Заранее был настроен домен Active Directory <code>example.loc</code>. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп
dst.ip	Один из внешних IP-адресов UserGate WAF, доступный из сети интернет, куда адресован трафик внешних клиентов. Для указания списка IP-адресов: <code>dst.ip = lib.network()</code>; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название URL-списка, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
dst.geoip	Указание GeoIP; необходимо указать код страны (например, <code>dst.geoip = RU</code>). Коды названий стран доступны по ссылке: ISO 3166-1. Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15
request.header.User-Agent	Useragent пользовательских браузеров, для которых будет применено правило публикации. Для указания Useragent пользовательских браузеров: <code>request.header.User-Agent = lib.useragent()</code>; в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка Useragent браузеров»
allowed_web_services	Путь к одному или нескольким веб-сервисам, запросы к которым будет обрабатывать правило. Формат записи: <code><host>/<path></code>, где <code><host></code> — обязательный параметр (совпадение строгое, наличие и отсутствие символа <code></></code> в конце названия узла без пути равнозначно; все названия узлов приводятся к нижнему регистру.), а <code><path></code> — необязательный, без которого будет выбираться любой путь (совпадение префиксное, не строгое). При указании пути для <code><host></code> в качестве маски можно использовать символ <code>*</code>. Например, запись <code>*.example.org</code> соответствует как <code>www.example.org</code>, так и <code>www.sub.example.org</code>.
rewrite_path	Подмена домена и/или пути в URL-запросе пользователя. Например, для преобразования запросов, приходящих на <code>http://www.example.com/path1</code> в <code>http://www.example.loc/path2</code> нужно указать: <code>rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2")</code>

Параметр	Описание
waf_profile	Включение защиты веб-сервисов в правиле публикации. Необходимо указать заранее созданный WAF-профиль. Например, waf_profile("Example WAF profile"). Подробнее о создании и настройке WAF-профилей с использованием интерфейса командной строки — в разделе «Настройки безопасности WAF в CLI»
json_profile_id	Включение обработки HTTP-запросов с данными в формате JSON. Необходимо указать заранее созданный JSIN-профиль. Например, json_profile_id("Example_json_profile")
xml_profile_id	Включение обработки HTTP-запросов с данными в формате XML. Необходимо указать заранее созданный XML-профиль. Например, xml_profile_id("Example_XML_profile")
websocket_profile	Включение обработки websocket-соединений. Необходимо указать заранее созданный websocket-профиль. Например, websocket_profile("Example websocket profile") Подробнее о создании и настройке WAF-профилей с использованием интерфейса командной строки — в разделе «Настройка WebSocket-профилей в CLI»

Для редактирования правила публикации используется команда:

```
Admin@nodename# set global-portal reverse-proxy-rules <position> upl-rule <parameters>
```

Для просмотра параметров правила публикации используется команда:

```
Admin@nodename# show global-portal reverse-proxy-rules <position>
```

Пример создания правила публикации:

```
Admin@nodename# create global-portal reverse-proxy-rules 1 upl-rule OK \
...url.port = 80 \
...src.zone = Untrusted \
...profile("Reverse proxy server1") \
...rewrite_path("example.com/path1", "example.local/path2") \
...waf_profile("Example WAF profile") \
...name("Test reverse proxy rule") \
...desc("Test reverse proxy rule description") \
...enabled(true)
...
Admin@nodename# show global-portal reverse-proxy-rules 1
% ----- 1 -----
OK \
  url.port = 80 \
  src.zone = Untrusted \
  desc("Test reverse proxy rule description") \
  profile("Reverse proxy server1") \
  rewrite_path("example.com/path1", "example.local/path2") \
  waf_profile("Example WAF profile") \
  enabled(true) \
  id("7dc7041a-6538-400b-8f1e-9b18287218ac") \
  name("Test reverse proxy rule")
```

Для удаления правила публикации используется команда:

```
Admin@nodename# delete global-portal reverse-proxy-rules <position>
```

Настройка балансировки нагрузки

Product: WAF
Version: 7.7.x
Technology: Firewall

Настройка правил балансировки нагрузки происходит на уровне **network-policy load-balancing** с использованием языка описания политик UPL. Подробнее о структуре команд — в разделе «[UserGate Policy Language](#)».

Для отображения информации о всех балансировщиках используется команда:

```
Admin@nodename# show network-policy load-balancing
```

Настройка балансировки нагрузки на серверы публикации

Настройка правил балансировки производится на уровне **network-policy load-balancing reverse-proxy**.

Для создания правила балансировки:

```
Admin@nodename# create network-policy load-balancing reverse-proxy <position> upl-rule
```

Параметры правил балансировки:

Параметр	Описание
PASS OK	Действие для создания правила балансировки с помощью UPL.
enabled	Включение/отключение правила балансировки: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название правила балансировки. Например: name("RP balancer") .
desc	Описание правила балансировки. Например: desc("Test reverse-proxy balancing rule") .
profile	Указание серверов публикации, на которые будет распределяться нагрузка. Подробнее о создании и настройке серверов публикации с использованием CLI — в разделе « Настройка серверов публикации ». Например, profile("Reverse proxy server1", "Reverse proxy server2") .

Команда для редактирования параметров правила балансировки:

```
Admin@nodename# set network-policy load-balancing reverse-proxy <position> upl-rule
```

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании правила балансировки.

Команды для отображения информации о всех правилах балансировки:

```
Admin@nodename# show network-policy load-balancing reverse-proxy
```

Для отображения информации об определённом правиле балансировки:

```
Admin@nodename# show network-policy load-balancing reverse-proxy <position>
```

Пример создания правила балансировки с использованием UPL:

```
Admin@nodename# create network-policy load-balancing reverse-proxy 1 upl-rule OK \  
...profile("Reverse proxy server1", "Reverse proxy server2") \  
...desc("Test reverse proxy balancing rule") \  
...name(test_reversep1) \  
...enabled(true)  
...  
Admin@nodename# show network-policy load-balancing reverse-proxy  
  
% ----- 1 -----  
OK \  
  profile("Reverse proxy server1", "Reverse proxy server2") \  
  desc("Test reverse proxy balancing rule") \  
  name(test_reversep1) \  
  enabled(true)
```

```
desc("Test reverse proxy balancing rule") \  
enabled(true) \  
id("1ed892bb-26ee-4ab1-8a55-2f412ce8b55a") \  
name(test_reversep1)
```

Для удаления существующего правила балансировки используется следующая команда:

```
Admin@nodename# delete network-policy load-balancing reverse-proxy <position>
```

