

Table of Contents

Table of Contents	1
Настройки глобального портала	2
Настройка серверов reverse-прокси	3
Настройка правил reverse-прокси	4

Настройка серверов reverse-прокси

Product: WAF

Version: 7.x

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

Для создания сервера reverse-прокси используется следующая команда:

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

Доступно указание следующих параметров:

Параметр	Описание
name	Название сервера reverse-прокси.
description	Описание сервера reverse-прокси.
address	Адрес или домен сервера reverse-прокси.
port	TCP-порт сервера reverse-прокси.
https	Использование протокола HTTPS до публикуемого сервера: <ul style="list-style-type: none">• on: использовать.• off: не использовать.
keep-source-ip	Использование оригинального IP-адреса источника в пакетах, пересылаемых на публикуемый сервер: <ul style="list-style-type: none">• on: оставить оригинальный IP-адрес источника.• off: заменить IP-адрес источника на IP-адрес UserGate. <p>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.</p>

Команда для редактирования параметров сервера reverse-прокси:

```
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 reverse-прокси:

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

Структура команды для удаления сервера:

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

Настройка правил reverse-прокси

Product: WAF
Version: 7.x

Правила reverse-прокси 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 reverse-прокси:

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

Параметры настройки правил reverse-прокси:

Параметр	Описание
OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: <ul style="list-style-type: none">• enabled(yes) или enabled(true) — включение;• enabled(no) или enabled(false) — отключение
name	Название правила reverse-прокси. Например, name("Reverse proxy rule example")
desc	Описание правила. Например, desc("Reverse proxy rule example set via CLI")
profile	Сервер reverse-прокси, куда WAF будет пересылать запросы. Для указания сервера: profile("Reverse proxy server example")
url.port	Порт, на котором WAF будет слушать входящие запросы. Например, url.port = 80
is_https	Поддержка HTTPS: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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	<p>Добавление списков IP-адресов или доменов источника.</p> <p>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».</p> <p>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»</p>
src.geoip	<p>Указание GeoIP источника; необходимо указать код страны (например, <code>src.geoip = RU</code>).</p> <p>Коды названий стран доступны по ссылке: ISO 3166-1.</p> <p>Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15</p>
user	<p>Пользователи и группы пользователей, для которых применяется правило reverse-прокси. Добавление пользователей доступно только при использовании авторизации по сертификату.</p> <p>Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (подробнее о настройке LDAP-коннектора через CLI — в разделе «Настройка LDAP-коннектора»).</p> <p>Пример добавления локальных 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>):</p> <pre>user = (local_user, "CN=Local Group, DC=LOCAL", "example.loc\AD_user", "CN=AD group, OU=Example, DC=example, DC=loc")</pre> <p>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</p>
dst.ip	<p>Один из внешних IP-адресов WAF, доступный из сети интернет, куда адресован трафик внешних клиентов.</p> <p>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».</p> <p>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»</p>
dst.geoip	<p>Указание GeoIP; необходимо указать код страны (например, <code>dst.geoip = RU</code>).</p> <p>Коды названий стран доступны по ссылке ISO 3166-1.</p> <p>Важно! Существует ограничение на количество GeoIP, которое может быть указано: не более 15</p>
request.header.User-Agent	<p>Useragent пользовательских браузеров, для которых будет применено данное правило.</p> <p>Для указания Useragent пользовательских браузеров: <code>request.header.User-Agent = lib.useragent()</code>; в скобках необходимо указать название категории Useragent браузеров.</p> <p>Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки — в разделе «Настройка Useragent браузеров»</p>
rewrite_path	<p>Подмена домена и/или пути в URL-запросе пользователя.</p> <p>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></p>
waf_profile	<p>Включение защиты веб-приложений в правиле reverse-прокси.</p> <p>Необходимо указать заранее созданный WAF-профиль.</p> <p>Например, <code>waf_profile("Example WAF profile")</code>.</p> <p>Подробнее о создании и настройке WAF-профилей с использованием интерфейса командной строки — в разделе «Настройки безопасности WAF в CLI»</p>

Параметр	Описание
websocket_profile	<p>Включение обработки websocket-соединений (доступно в версии ПО 7.4.1 и выше).</p> <p>Необходимо указать заранее созданный websocket-профиль.</p> <p>Например, websocket_profile("Example websocket profile")</p> <p>Подробнее о создании и настройке WAF-профилей с использованием интерфейса командной строки — в разделе «Настройка WebSocket-профилей в CLI»</p>

Для редактирования правила reverse-прокси используется команда:

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

Для просмотра параметров правила reverse-прокси используется команда:

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

Пример создания правила reverse-прокси:

```
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 reverse-прокси используется команда:

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

