

Table of Contents

Table of Contents	1
Настройка глобального портала	2
Настройка веб-портала	3
Настройка правил reverse-прокси	5
Настройка серверов reverse-прокси	8

Настройка веб-портала

Documentation: ☒
Product: NGFW
Version: 7.x

Настройка веб-портала производится на уровне **global-portal web-portal**. О структуре команд подробнее читайте в разделе [UserGate Policy Language](#).

Структура команды создания страницы веб-портала:

Admin@nodename# create global-portal web-portal <position> upl-rule <parameters>

Параметры настройки закладок веб-портала:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
name	Название закладки. Например: name("Example of bookmark publishing") .
desc	Описание закладки. Например: desc("Example of bookmark publishing configured in CLI") .
url	URL ресурса, который необходимо опубликовать через веб-портал. Необходимо указывать полный URL, начиная с http://, https://, ftp://, ssh:// или rdp://. URL указывается как url = "http://www.example.com" .
url.domain	При указанном значении домена прямого доступа пользователь может получить доступ к публикуемому ресурсу, минуя веб-портал, подключаясь к указанному домену. Для указания домена прямого доступа: url.domain = "example.com" .
rdp_check_session_alive	Разрыв сессии RDP по завершению авторизации на веб-портале: • rdp_check_session_alive(yes) или rdp_check_session_alive(true) — разрывать сессию. • rdp_check_session_alive(no) или rdp_check_session_alive(false) — не разрывать сессию.
ssl_profile	Профиль SSL для построения защищенного канала для отображения веб-портала; указывается: ssl_profile("SSL profile example") .
certificate	Сертификат, который будет использоваться для создания HTTPS-соединения. Чтобы задать сертификат: certificate("Certificate example") .
icon	Иконка, которая будет отображаться на веб-портале для данной закладки. Возможно указать одну из предопределенных иконок, указать внешний URL, по которому доступна иконка или загрузить свою иконку. Можно указать: • icon("Default icon name") — использовать штатную иконку (в скобках указывается название штатной иконки). • icon("Icon encoded with Base64") — использовать свою иконку. Необходимо указать содержимое файла, кодированное с использованием Base64. • icon("http://www.icon-url-example.com") — указать URL для использования сторонней иконки.

Параметр	Описание
additional_url	Вспомогательные URL, необходимые для работы основного URL, но которые нет необходимости публиковать для пользователей. Для указания: additional_url("http://additional-url-example.com") .
user	Пользователи и группы пользователей, которым разрешено отображение закладки на веб-портале и которым разрешен доступ к основному и вспомогательным URL. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). Примеры добавления пользователей в правило: <pre> user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1") </pre>

Для редактирования правила веб-портала используется команда:

```
Admin@nodename# set global-portal web-portal <position> upl-rule <parameters>
```

Для просмотра параметров правил веб-портала используется команда:

```
Admin@nodename# show global-portal web-portal <position>
```

Пример создания правила веб-портала с использованием UPL:

```

Admin@nodename# create global-portal web-portal 1 upl-rule OK \
...user = "CN=Default Group,DC=LOCAL" \
...url = "http://www.intranet.loc" \
...name("Test web portal") \
...desc("Test web portal description") \
...enabled(true)
...
Admin@nodename# show global-portal web-portal 1
% ----- 1 -----
OK \
  user = "CN=Default Group,DC=LOCAL" \
  url = "http://www.intranet.loc" \
  icon("default.svg") \
  desc("Test web portal description") \
  enabled(true) \
  id("2fead5a1-29c3-4835-bbdb-1d0e07f84c28") \
  name("Test web portal")

```

Для удаления правила веб-портала используется команда:

```
Admin@nodename# delete global-portal web-portal <position>
```

Настройка правил reverse-прокси

Documentation: ☒

Product: NGFW

Version: 7.x

Правила reverse-прокси настраиваются на уровне **global-portal reverse-proxy-rules**. Подробнее о структуре команд читайте 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: • enabled(yes) или enabled(true). • enabled(no) или enabled(false).
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 NGFW будет пересылать запросы. Для указания сервера: profile("Reverse proxy server example") .
url.port	Порт, на котором NGFW 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 читайте 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 читайте в разделе Зоны .

Параметр	Описание
src.ip	Добавление списков IP-адресов или доменов источника. Для указания списка IP-адресов: src.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL.
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). 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 (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <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 example.loc. 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 NGFW, доступный из сети интернет, куда адресован трафик внешних клиентов. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов. Для указания списка доменов назначения: dst.ip = lib.url(); 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 читайте в разделе Настройка списков URL.
dst.geoip	Указание GeoIP; необходимо указать код страны (например, dst.geoip = RU). 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 данное правило. Для указания Useragent пользовательских браузеров: request.header.User-Agent = lib.useragent(); в скобках необходимо указать название категории Useragent браузеров. Подробнее о создании и настройке собственных списков с использованием интерфейса командной строки читайте в разделе Настройка Useragent браузеров.
rewrite_path	Подмена домена и/или пути в URL в запросе пользователя. Например, позволяет преобразовать запросы, приходящие на http://www.example.com/path1 в http://www.example.loc/path2. Для этого необходимо указать: rewrite_path("http://www.example.com/path1", "http://www.example.loc/path2").

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") \
...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") \
  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>
```

Настройка серверов reverse-прокси

Documentation: ☒

Product: NGFW

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: • 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 UG NGFW, с которого приходят запросы клиентов. Для этого на веб-сервере в качестве шлюза по умолчанию можно указать UG NGFW или можно настроить статические маршруты через UG NGFW для «белых» IP-адресов источников.

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>
```

