

Table of Contents

Table of Contents	1
Настройка правил с использованием UPL	2
Настройка правил с использованием UPL (Описание)	3

Настройка правил с использованием UPL

Настройка правил с использованием UPL (Описание)

Documentation: 

Product: NGFW

Version: 7.0.1

UPL — UserGate Policy Language — язык описания политик (конфигурации правил, применяемых для принятия решений по требованиям аутентификации, правам доступа или преобразования контента) UserGate.

Правила настраиваются с использованием действий, условий и свойств.

Для каждого правила настраивается одно из действий. Действия — настройки, которые управляют обработкой транзакции (**OK**, **WARNING**, **PASS**, **DENY**). При настройке правил, в которых не предусмотрено указание действия (например, правила DNS, NAT и маршрутизации, пропускной способности и т.п.), необходимо указать действия **PASS** или **OK**.

Условия задаются знаками равно (=) или не равно (!=), например, зоны, адреса, GeoIP источников и назначения, сервисы, приложения и т.д.; все условия в правиле проверяются по логическому И, т.е. правило сработает, если будут выполнены все условия.

Свойства правил задаются в круглых скобках и используются для указания дополнительной информации, например, название правил, их описание, функция журналирования и т.д.

Примечание При настройке правил сначала указывается действие, потом условия и затем свойства.

UPL используется для настройки правил в следующих разделах:

- Настройки DNS-прокси (уровень: **network dns dns-proxy dns-rules**).
- Captive-портал (уровень: **users captive-portal**).
- Межсетевой экран (уровень: **network-policy firewall**).
- NAT и маршрутизация (уровень: **network-policy nat-routing**).
- Пропускная способность (уровень: **network-policy traffic-shaping**).
- Фильтрация контента (уровень: **security-policy content-filtering**).
- Веб-безопасность (уровень: **security-policy web-browsing**).
- Инспектирование туннелей (уровень: **security-policy tunnel-inspection**).
- Инспектирование SSL (уровень: **security-policy ssl-inspection**).
- Инспектирование SSH (уровень: **security-policy ssh-inspection**).
- COB (уровень: **security-policy intrusion-prevention**).
- Защита почтового трафика (уровень: **security-policy mail-security**).
- ICAP-правила (уровень: **security-policy icap-rules**).
- Правила защиты DoS (уровень: **security-policy dos-rules**).
- Веб-портал (уровень: **global-portal web-portal**).
- Правила reverse-прокси (уровень: **global-portal reverse-proxy-rules**).
- Серверные правила (уровень: **vpn server-rules**).
- Клиентские правила (уровень: **vpn client-rules**).

Структура команды для создания правила:

```
Admin@UGOS# create <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо создать правило.

<position> — позиция, на которую будет помещено правило.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для обновления существующего правила:

```
Admin@UGOS# set <level> <position> upl-rule <str-upl-syntax>
```

где <level> — уровень, на котором необходимо обновить правило.

<position> — номер правила, которое необходимо обновить.

<str-upl-syntax> строка, в которой описано правило в UPL синтаксисе.

Структура команды для удаления правила:

```
Admin@UGOS# delete <level> <position | all>
```

где <level> — уровень, на котором необходимо удалить правило.

<position> — номер правила, которое необходимо удалить.

<all> — удалить все правила.

Структура команды для отображения правила:

```
Admin@UGOS# show <level> <position | all>
```

где <level> — раздел, правила которого нужно отобразить.

<position> — номер правила, которое необходимо отобразить.

<all> — отобразить все правила.

В качестве примера рассмотрим создание правила межсетевого экрана (использован многострочный ввод):

```
Admin@UGOS# create network-policy firewall 1 upl-rule \  
...DENY \  
...src.zone = Trusted \  
...dst.zone = Untrusted \  
...user = known \  
...service = HTTPS \  
...time = lib.time("Working hours") \  
...rule_log(session) \  
...name("Example of firewall rule created in CLI") \  
...enabled(true)
```

После создания правило отобразится в начале списка правил межсетевого экрана (на позиции 1). Данное правило запрещает HTTPS-трафик из зоны Trusted в зону Untrusted пользователям, идентифицированным системой; правило работает в соответствии с расписанием Working hours. При срабатывании правила в журнал будет записана информация о начале сессии.

