

Table of Contents

Table of Contents	1
Настройки раздела Политики сети	2
Настройка правил межсетевого экрана	3

Настройка правил межсетевого экрана

Product: WAF
Version: 7.7.x
Technology: Firewall

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд — в разделе « [UserGate Policy Language](#) ».

Admin@nodename# create network-policy firewall

Параметры правил межсетевого экрана:

Параметр	Описание
PASS DENY	Действие правила межсетевого экрана: PASS — разрешить трафик. DENY — запретить трафик
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false)
name	Название правила межсетевого экрана. Например: name("Rule example")
desc	Описание правила. Например: desc("Firewall rule example configured in CLI")
reject_with	Настройка доступна для правил с действием Запретить : reject_with(no). reject_with("host_unreach") — посылать ICMP host unreachable — блокировка трафика с отправкой ICMP-сообщения. reject_with("tcp_rst") — посылать TCP reset: блокировка трафика с отправкой сообщения о разрыве TCP-соединения. Важно! При выборе действия Посылать TCP reset необходимо указание сервиса, использующего протокол TCP (подробнее о добавлении и настройке сервисов читайте в разделе ов). reject_with("tcp_reset-both") — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу
rule_log	Запись в журнал информации о трафике при срабатывании правила. Возможны варианты: rule_log(no) или rule_log(false) — отключить журналирование. Если при создании правила rule_log не указано, функция журналирования отключена. rule_log(yes) или rule_log(true) — журналировать все сетевые пакеты без установки лимитов. Для установки лимитов необходимо указать число событий, записываемых в журнал за единицу времени (s — секунда; min — минута; h — час; d — день, нельзя установить лимит журналирования менее 5-ти пакетов в день) и максимальное количество пакетов, журналируемых на событие. Например, rule_log(yes, "3/h", 5) — включение журналирования с установкой лимитов: в журнал записывается 3 события в час; максимальное количество пакетов, журналируемых на событие равно 5. rule_log(session) — журналировать начало сессии
fragmented	Указание пакетов, к которым применяется правило межсетевого экрана: fragmented(yes) или fragmented(true) — применить правило к только фрагментированным пакетам. fragmented(no) или fragmented(false) — применить правило к только нефрагментированным пакетам. fragmented(all) — применить правило ко всем пакетам. Если не указать fragmented при создании правила, то правило межсетевого экрана применяется ко всем пакетам

Параметр	Описание
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
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 — 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 — 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
dst.zone	Зона назначения трафика. Для указания зоны источника, например, Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
dst.ip	Добавление списков IP-адресов или доменов назначения. 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 — 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 — в разделе «Настройка списков URL»
dst.geoip	Указание GeoIP назначения; 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
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей — в разделе «Настройка календарей»

Пример создания правила межсетевого экрана с использованием UPL:

```
Admin@nodename# create network-policy firewall 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...service = HTTP \
...rule_log(session) \
...name("Test firewall rule") \
...enabled(true)
...
Admin@nodename# show network-policy firewall 1
% ----- 1 -----
PASS \
src.zone = Trusted \
dst.zone = Untrusted \
service = HTTP \
rule_log(session) \
enabled(true) \
id("1505d309-621b-4f88-a2e4-98667c477535") \
name("Test firewall rule")
```

