

Table of Contents

Table of Contents	1
Настройка раздела Политики сети	2
Настройка правил межсетевого экрана	3
Настройка правил NAT и маршрутизации	6
Настройка балансировки нагрузки	19
Настройка правил управления пропускной способностью	23

Настройка правил межсетевого экрана

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

Настройка межсетевого экрана происходит на уровне **network-policy firewall**. Подробнее о структуре команд читайте 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") .
ips_profile	Профиль COV. Подробнее о создании и настройке профилей COV с использованием интерфейса командной строки читайте в разделе Настройка профилей COV . Например: ips_profile("Test ips profile") .
I7_profile	Профиль приложений. Подробнее о создании и настройке профилей приложений с использованием интерфейса командной строки читайте в разделе Настройка профилей приложений . Например: I7_profile("Test application-profile") .
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. reject_with("tcp_reset-both") — посылать TCP reset в обе стороны — блокировка трафика с отправкой сообщения о разрыве TCP-соединения клиенту и серверу.
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .

Параметр	Описание
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.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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 межсетевого экрана (локальные или LDAP). 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>
dst.zone	Зона назначения трафика. Для указания зоны назначения, например, Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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.

Параметр	Описание
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.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте 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 \
...user = known \
...service = HTTP \
...rule_log(session) \
...name("Test firewall rule") \
...enabled(true)
...
Admin@nodename# show network-policy firewall 1
% ----- 1 -----
PASS \
  user = known \
  src.zone = Trusted \
  dst.zone = Untrusted \
  service = HTTP \
  rule_log(session) \
  enabled(true) \
  id("1505d309-621b-4f88-a2e4-98667c477535") \
  name("Test firewall rule")
```

Настройка правил NAT и маршрутизации

Documentation: ☒
Product: NGFW
Version: 7.x
Technology: Firewall

Правила NAT и маршрутизации настраиваются на уровне network-policy nat-routing. Правила создаются с помощью языка описания правил UPL. Подробнее о синтаксисе языка UPL — в разделе [UserGate Policy Language](#).

Для создания правила используется команда:

```
Admin@nodename# create network-policy nat-routing <position> upl-rule <parameters>
```

Команда для редактирования ранее созданных правил:

```
Admin@nodename# set network-policy nat-routing <position> upl-rule <parameters>
```

Команда для просмотра ранее созданных правил:

```
Admin@nodename# show network-policy nat-routing <position>
```

Команда для удаления ранее созданных правил:

```
Admin@nodename# delete network-policy nat-routing <position>
```

Подробнее о применении правил NAT — в разделе « [NAT и маршрутизация](#) ».

Настройка правил NAT

При настройке правил NAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила NAT. Например, name("NAT rule example")
desc	Описание правила. Например, desc("NAT rule example set via CLI")
nat	Тип правила
snat_target_ip	IP-адрес, на который будет заменен адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
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(session) — журналировать начало сессии
src.zone	Зона источника трафика. Например, для указания зоны Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »

Параметр	Описание
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: <code>src.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: <code>src.ip = 02:00:00:00:00:00</code>
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • <code>user = known</code>; • <code>user = user1</code>; • <code>user = "testd.local\\user2"</code>; • <code>user = (user1, "testd.local\\user2")</code>
dst.zone	Зона назначения трафика. Для указания зоны назначения трафика, например Untrusted: <code>dst.zone = Untrusted</code>. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
dst.ip	Добавление списков IP-адресов, доменов назначения, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов назначения используйте: <code>dst.ip = 02:00:00:00:00:00</code>
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках укажите название группы сервисов

Пример создания правила NAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...nat \
...rule_log(session) \
...name("Test NAT rule") \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 1
% ----- 1 -----
OK \
src.zone = Trusted \
dst.zone = Untrusted \
direction(input) \
rule_log(session) \
enabled(true) \
id("0344640b-b392-4920-9853-77d85ec1338c") \
name("Test NAT rule") \
nat
```

Настройка правил NoNAT

При настройке правил NoNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила NAT. Например, name("NAT rule example")
desc	Описание правила. Например, desc("NAT rule example set via CLI")
nonat	Тип правила
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(session) — журналировать начало сессии
src.zone	Зона источника трафика. Например, указание зоны Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление адресов источника трафика в виде списков IP-адресов, доменов источника, или MAC-адресов. 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 списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте строку вида: src.ip = 02:00:00:00:00:00
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\\user2"; - user = (user1, "testd.local\\user2")
dst.zone	Зона назначения трафика. Например, указание зоны Untrusted: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. 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 списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов. Подробнее о создании сервисов или групп сервисов — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code> ; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code> ; в скобках укажите название группы сервисов

Пример создания правила NoNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 6 upl-rule PASS \
...src.zone = Trusted \
...dst.zone = Untrusted \
...user = "testd.local\user3" \
...rule_log(session) \
...name("NoNAT rule 1") \
...nonat \
...enabled(true)
...
Admin@nodename# show network-policy nat-routing 6
% ----- 6 -----
OK \
  user = "testd.local\user3" \
  src.zone = Trusted \
  dst.zone = Untrusted \
  rule_log(session) \
  enabled(true) \
  name("NoNAT rule 1")\
  nonat
```

Настройка правил DNAT

При настройке правил DNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — включение правила
name	Название правила DNAT. Например, <code>name("DNAT rule example")</code>
desc	Описание правила. Для описание правила используйте: <code>desc("DNAT rule example created via CLI")</code>
dnat	Тип правила
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, <code>snat_target_ip ("1.1.1.1")</code>

Параметр	Описание
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(session) — журналировать начало сессии
src.zone	Зона источника трафика. Например, чтобы указать зону Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание Geo IP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Список пользователей или групп, для которых применяется данное правило. Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\\user2"; - user = (user1, "testd.local\\user2")
dst.zone	Зона назначения трафика. Например, для указания зоны 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
target_ip	Адрес назначения DNAT. Для указания адреса назначения: target_ip("1.1.1.1")
target_snat	Изменение IP-адреса источника на адрес UserGate: - target_snat(yes) или target_snat(true); - target_snat(no) или target_snat(false)

Параметр	Описание
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее — в разделах « Настройка сервисов » и « Настройка групп сервисов »). Чтобы указать сервис: service = "service name" ; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service() ; в скобках необходимо указать название группы сервисов

Пример создания правила DNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 1 upl-rule PASS \  
...src.zone = Untrusted \  
...target_ip("10.10.0.15") \  
...dnat \  
...rule_log(session) \  
...name("Test DNAT") \  
...enabled(yes)  
...  
Admin@nodename# show network-policy nat-routing 1  
% ----- 1 -----  
OK \  
src.zone = Untrusted \  
target_ip("10.10.0.15") \  
direction(input) \  
rule_log(session) \  
enabled(true) \  
id("00e60d4e-9b93-454b-a424-58e2102f84c2") \  
name("Test DNAT")\  
dnat
```

Настройка правил NoDNAT

При настройке правил NoDNAT укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила DNAT. Например, name("DNAT rule example")
desc	Описание правила. Например, desc("DNAT rule example created via CLI")
dnat	Тип правила
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
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(session) — журналировать начало сессии

Параметр	Описание
src.zone	Зона источника трафика. Например, чтобы указать зону Trusted: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • user = known; • user = user1; • user = "testd.local\\user2"; • user = (user1, "testd.local\\user2")
dst.zone	Зона назначения трафика. Для указания зоны назначения, 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL»
target_ip	Адрес назначения DNAT. Для указания адреса назначения: target_ip("1.1.1.1")
target_snat	Изменение IP-адреса источника на адрес UserGate: • target_snat(yes) или target_snat(true); • target_snat(no) или target_snat(false)
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов

Пример создания правила DNAT с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule PASS \
```

```
...src.zone = Untrusted \  
...dst.zone = Trusted \  
...user = known \  
...rule_log(session) \  
...name("NoDNAT rule") \  
...nodnat \  
...enabled(true)  
...  
Admin@nodename# show network-policy nat-routing 7  
% ----- 7 -----  
OK \  
  user = known \  
  src.zone = Untrusted \  
  dst.zone = Trusted \  
  rule_log(session) \  
  enabled(true) \  
  name("NoDNAT rule")\  
  nodnat
```

Настройка правил трансляции портов

При настройке правил трансляции портов укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила трансляции портов. Например, name("Port forwarding rule example")
desc	Описание правила. Для создания описание правила используйте: desc("Port forwarding rule example created via CLI")
port_mapping	Тип правила.
snat_target_ip	IP-адрес, на который будет заменён адрес источника. Адрес указывается в кавычках. Например, snat_target_ip ("1.1.1.1")
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(session) — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. 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 интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00

Параметр	Описание
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе « Настройка LDAP-коннектора ». Примеры добавления пользователей в правило: • user = known; • user = user1; • user = "testd.local\\user2"; • user = (user1, "testd.local\\user2")
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 интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL »
port_map	Переназначение портов публикуемых сервисов. Для переназначения портов необходимо указать сетевой протокол (tcp, udp, smtp, smtps), оригинальный и новый порты назначения. Например, port_map(tcp, 2000, 2100). Следующие порты не могут быть использованы для переназначения, поскольку они уже используются внутренними службами UserGate NGFW: 2200, 8001, 4369, 9000-9100
target_ip	Адрес назначения DNAT. Например, target_ip("1.1.1.1")
target_snat	Изменение IP-адреса источника на адрес узла UserGate: • target_snat(yes) или target_snat(true); • target_snat(no) или target_snat(false)

Пример создания правила трансляции портов с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
... src.zone = Untrusted \
... dst.ip = lib.network(UG_IP) \
... target_ip("10.10.0.16") \
... port_map(tcp, 2222, 23) \
... rule_log(session) \
... name(port_fw1) \
... port_mapping \
...
Admin@nodename# show network-policy nat-routing 8
% ----- 8 -----
OK \
src.zone = Untrusted \
dst.ip = lib.network(UG_IP) \
target_ip("10.10.0.16") \
port_map(tcp, 2222, 23) \
direction(input) \
rule_log(session) \
enabled(true) \
id("1af47c3f-96a3-4e65-90e3-debf169bb745") \
name(port_fw1)\
port_mapping
```

Настройка правил маршрутизации на основе политик

Для настройки правил маршрутизации на основе политик (policy-based routing, PBR) укажите следующие параметры.

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение/отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила. Например, name("Policy-based routing rule example")
desc	Описание правила. Для создания описание правила используйте: desc("Policy-based routing rule example set via CLI")
route	Тип правила.
gateway	Выбор одного из существующих шлюзов. Например, gateway("1.1.1.1"). О добавлении шлюзов с использованием интерфейса командной строки — в разделе « Настройка шлюзов »
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария используйте: scenario = "Example of a scenario" . Подробнее о настройке сценариев с использованием интерфейса командной строки — в разделе « Настройка сценариев »
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(session) — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе « Зоны »
src.ip	Добавление списков IP-адресов, MAC-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 интерфейса командной строки — в разделе « Настройка IP-адресов ». Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе « Настройка списков URL ». Для указания MAC-адресов источников, например 02:00:00:00:00:00, используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны (например, src.geoip = RU). Коды названий стран доступны по ссылке

Параметр	Описание
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: • user = known; • user = user1; • user = "testd.local\\user2"; • user = (user1, "testd.local\\user2")
dst.ip	Добавление списков IP-адресов, 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: dst.ip = lib.url(); в скобках необходимо указать название списка URL, 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
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов

Пример создания и редактирования правила PBR с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 7 upl-rule OK \
... route \
... gateway("def") \
... name("testpbr1") \
... enabled(true) \
... rule_log(session) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... service = (HTTPS, HTTP) \
...
Admin@nodename# set network-policy nat-routing 7 upl-rule OK \
... user = "CN=Users1,DC=LOCAL"
Admin@nodename# show network-policy nat-routing 7
% ----- 7 -----
OK \
  user = "CN=Users1,DC=LOCAL" \
  service = (HTTPS, HTTP) \
  gateway(def) \
  direction(input) \
  rule_log(session) \
  enabled(true) \
  id("0585a95f-4707-4c11-840d-44643bc2c799") \
  name(testpbr1) \
  route
```

Настройка правил трансляции адресов сетей

При настройке правил трансляции адресов сетей (network mapping) укажите следующие параметры.

Параметр	Описание

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL
enabled	Включение или отключение правила: - enabled(yes) или enabled(true) — включение правила; - enabled(no) или enabled(false) — отключение правила
name	Название правила. Например, name("Network mapping rule example").
desc	Описание правила. Для создания описание правила используйте: desc("Network mapping rule example set via CLI")
netmap	Тип правила.
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(session) — журналировать начало сессии
src.zone	Зона источника трафика. Для указания зоны источника: src.zone = Trusted. Подробнее о настройке зон с использованием интерфейса командной строки — в разделе «Зоны»
src.ip	Добавление списков IP-адресов, доменов источника, или MAC-адресов. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов источника: src.ip = lib.url(); в скобках необходимо указать название списка URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки — в разделе «Настройка списков URL». Для указания MAC-адресов источников используйте: src.ip = 02:00:00:00:00:00
src.geoip	Указание GeoIP источника; необходимо указать код страны. Например, src.geoip = RU. Коды названий стран доступны по ссылке
user	Пользователи или группы пользователей (локальные или доменные), для которых применяется правило. Могут быть использованы пользователи типа Any, Unknown, Known. Для добавления LDAP-групп и пользователей необходим корректно настроенный LDAP-коннектор на устройстве. Подробнее о настройке LDAP-коннектора с использованием интерфейса командной строки — в разделе «Настройка LDAP-коннектора». Примеры добавления пользователей в правило: - user = known; - user = user1; - user = "testd.local\\user2"; - user = (user1, "testd.local\\user2")

Параметр	Описание
dst.ip	Добавление списков IP-адресов или доменов назначения. 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 интерфейса командной строки — в разделе «Настройка IP-адресов». Для указания списка доменов назначения: <code>dst.ip = lib.url()</code>; в скобках необходимо указать название списка URL, 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, <code>dst.geoip = RU</code>. Коды названий стран доступны по ссылке
target_ip	Параметр подмены сетей; адрес сети, на которую будет производиться замена. Например, <code>target_ip("1.1.1.0")</code>
direction	Параметр подмены сетей. Направление: <code>direction(input)</code> — входящий, подменяется IP-сеть назначения. Будут изменены IP-адреса назначения в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении <code>target_ip</code>. <code>direction(output)</code> — исходящий, подменяется IP-сеть источника. Будут изменены IP-адреса источника в трафике, попадающем под условия правила. Изменяется адрес сети на сеть, указанную в значении <code>target_ip</code>
service	Указание типа сервиса. Вы можете указать сервис или группу сервисов (подробнее — в разделах «Настройка сервисов» и «Настройка групп сервисов»). Чтобы указать сервис: <code>service = "service name"</code>; для указания нескольких сервисов: <code>service = (service-name1, service-name2, ...)</code>. Чтобы указать группу сервисов: <code>service = lib.service()</code>; в скобках необходимо указать название группы сервисов

Пример создания правила трансляции адресов сетей с использованием UPL:

```
Admin@nodename# create network-policy nat-routing 8 upl-rule OK \
```

```
... src.zone = External \
... target_ip("192.168.222.0/24") \
... direction(output) \
... netmap \
... rule_log(session) \
... name(netmap1) \
...
```

```
Admin@nodename# show network-policy nat-routing 8
```

```
% ----- 8 -----
```

```
OK \
src.zone = External \
target_ip("192.168.222.0/24") \
direction(output) \
rule_log(session) \
enabled(true) \
id("26cbd3e8-0210-494c-9fd4-57300b47a9fe") \
name(netmap1)\
netmap
```

Documentation: ☒
Product: NGFW
Version: 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 читайте в разделе [UserGate Policy Language](#).

Настройка балансировщиков нагрузки TCP/UDP и reverse-прокси рассмотрена далее.

Для отображения информации о всех балансировщиках используется команда:

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

Настройка балансировщика TCP/UDP

Настройка данного раздела производится на уровне **network-policy load-balancing tcp-udp**.

Структура команды создания балансировщика нагрузки TCP/UDP следующая:

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

Параметры правил балансировки нагрузки TCP/UDP:

Параметр	Описание
OK	Действие для создания правила с помощью UPL.
name	Название правила балансировки. Например: name("TCP_UDP balancer") .
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
desc	Описание правила. Например: desc("TCP_UDP balancing rule") .
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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 . Например: src.ip = lib.network("Test ip-list") .
src.geoip	Указание Гео IP в качестве источника. Например: src.geoip = RU .
url.address	IP-адрес виртуального сервера. Например: url.address = 10.10.0.20 .

Параметр	Описание
url.port	Порт, для которого необходимо производить балансировку нагрузки. Например: url.port = 1812 .
service	Протокол — TCP или UDP, для которого необходимо производить балансировку нагрузки. Например: service = udp .
scheduler	Методы распределения нагрузки на реальные серверы: • rr — round robin — каждое новое подключение передается на следующий сервер в списке, равномерно загружая все серверы. • wrr — weighted round robin — работает аналогично Round robin, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. • lc — least connections — новое подключение передается на сервер, на который в данный момент установлено наименьшее число соединений. • wlc — weighted least connections — работает аналогично Least connections, но загрузка реальных серверов осуществляется с учетом весовых коэффициентов, что позволяет распределить нагрузку с учетом производительности каждого сервера. Например: scheduler(rr).
real_server	Реальные сервера, на которые будет перенаправляться трафик. Для сервера необходимо указать: • ip — IP-адрес сервера. • port — порт сервера, на который будут перенаправлять запросы пользователей. • weight — коэффициент, использующийся для неравномерного распределения нагрузки на реальные серверы. • mode — режим: ◦ gate — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ masq — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ masq-snat — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но UserGate подменяет IP-адрес источника на свой. Например: real_server(masq, 10.10.0.9:1812, 50).
ipvs_fallback	Настройка аварийного режима: • ip — IP-адрес сервера. • port — порт сервера, на который будут пересылаться запросы пользователей. • mode — режим: ◦ gate — режим Шлюз: для перенаправления трафика на виртуальный сервер используется маршрутизация. ◦ masq — режим Маскарадинг: для перенаправления трафика на виртуальный сервер используется DNAT. ◦ masq-snat — режим Маскарадинг с подменой IP-источника: режим аналогичен режиму Маскарадинг, но UserGate подменяет IP-адрес источника на свой. Например: ipvs_fallback(masq, 10.10.100.100:1812).

Параметр	Описание
monitor	Настройка мониторинга реальных серверов: • kind — тип проверки: ◦ ping: проверка доступности узла с использованием утилиты ping. ◦ connect: проверка работоспособности узла путём установления TCP-соединения на определённый порт. ◦ negotiate: проверка работоспособности узла посылкой определенного HTTP- или DNS-запроса и сравнением полученного ответа с ожидаемым ответом. • service — необходимо указать (HTTP или DNS) при использовании проверки типа negotiate. • request — запрос необходимо указать при использовании проверки типа negotiate. • response — ожидаемый ответ; необходимо указать при использовании проверки типа negotiate. • interval — интервал времени, через который должна выполняться проверка. • timeout — интервал времени ожидания ответа на проверку. • max-failures — количество попыток проверки реальных серверов, по истечению которого сервер будет считаться неработоспособным и будет исключен из балансировки. Например: <pre>monitor_kind(ping) \ monitor_interval(60) \ monitor_timeout(60) \ monitor_failurecount(10) \</pre>

Для редактирования существующего правила балансировки нагрузки используется следующая команда:

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

Команды для отображения информации о всех правилах балансировки TCP/UDP:

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

Для отображения информации об определённом правиле балансировки TCP/UDP:

```
Admin@nodename# show network-policy load-balancing tcp-udp <position>
```

Пример создания правила балансировщика нагрузки с использованием UPL:

```
Admin@nodename# create network-policy load-balancing tcp-udp 1 upl-rule OK \
...src.zone = Trusted \
...url.address = 10.10.0.20 \
...url.port = 1812 \
...service = udp \
...scheduler(rr) \
...real_server((gate, 10.10.0.9, 50), (gate, 10.10.0.8, 50)) \
...name(tcpudp_balancer1) \
...enabled(true)
...
Admin@nodename# show network-policy load-balancing tcp-udp
```

```
% ----- 1 -----
OK \
src.zone = Trusted \
url.address = 10.10.0.20 \
url.port = 1812 \
service = udp \
scheduler(rr) \
real_server((gate, 10.10.0.9, 50), (gate, 10.10.0.8, 50)) \
monitor_kind(ping) \
monitor_interval(60) \
monitor_timeout(60) \
monitor_failurecount(10) \
enabled(true) \
id(cbed6ed7-901e-4641-83a1-a05f82dae177) \
name(tcpudp_balancer1)
```

Для удаления существующего балансировщика нагрузки используется следующая команда:

```
Admin@nodename# delete network-policy load-balancing tcp-udp <position>
```

Настройка балансировщика reverse-прокси

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

Для создания правила балансировки reverse-прокси:

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

Параметры правил балансировки нагрузки reverse-proxy:

Параметр	Описание
PASS 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 балансировки. Например: name("RP balancer") .
desc	Описание правила. Например: desc("Test reverse-proxy balancing rule") .
profile	Указание профилей серверов reverse-прокси, на которые будет распределяться нагрузка. Подробнее о создании и настройке серверов reverse-прокси с использованием CLI в разделе Настройка серверов reverse-прокси . Например, profile("Reverse proxy server1", "Reverse proxy server2") .

Команда для редактирования параметров правила балансировки reverse-прокси:

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

Параметры, доступные для обновления, аналогичны параметрам, доступным при создании правила балансировки серверов reverse-прокси.

Команды для отображения информации о всех правилах балансировки reverse-proxy:

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

Для отображения информации об определённом правиле балансировки reverse-proxy:

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

Пример создания правила балансировщика нагрузки reverse-proxy 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") \
  enabled(true) \
  id("1ed892bb-26ee-4ab1-8a55-2f412ce8b55a") \
  name(test_reversep1)
```

Для удаления существующего правила балансировки нагрузки reverse-proxy используется следующая команда:

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

Настройка правил управления пропускной способностью

Documentation: ☒

Product: NGFW

Version: 7.x

Technology: Firewall

Настройка правил управления пропускной способностью производится на уровне **network-policy traffic-shaping** с использованием синтаксиса языка UPL. О структуре команд подробнее читайте в разделе [UserGate Policy Language](#).

Для создания правила управления пропускной способностью используется следующая команда:

```
Admin@nodename# create network-policy traffic-shaping <position> upl-rule
```

Параметры правил управления пропускной способностью:

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 пропускной способности. Например: name("Traffic shaping rule example") .
desc	Описание правила. Для задания описания правила: desc("The example of traffic shaping rule configured in CLI") .
bandwidth_pool	Полоса пропускания, например, bandwidth_pool("1 Mbps") . Подробнее о создании и настройке полос пропускания читайте в разделе Настройка полос пропускания .
scenario	Сценарий, который должен быть активным для срабатывания правила. Для указания сценария: scenario = "Example of a scenario" . Подробнее о настройке сценариев смотрите в разделе Настройка сценариев .
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.
src.zone	Зона источника трафика. Для указания зоны источника, например, Trusted: src.zone = Trusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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 .

Параметр	Описание
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 пропускной способности (локальные или LDAP). 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 управления пропускной способностью: <pre>user = known user = "user" user = "testd.local\\user1" user = ("user", "testd.local\\user1")</pre>
dst.zone	Зона назначения трафика. Для задания зоны назначения используется: dst.zone = Untrusted. Подробнее о настройке зон с использованием интерфейса командной строки читайте 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 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 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.
service	Тип сервиса. Можно указать сервис или группу сервисов (подробнее читайте в разделах Настройка сервисов и Настройка групп сервисов). Чтобы указать сервис: service = "service name"; для указания нескольких сервисов: service = (service-name1, service-name2, ...). Чтобы указать группу сервисов: service = lib.service(); в скобках необходимо указать название группы сервисов.
application	Список приложений, для которых применяется данное правило. Доступно указание: • всех групп приложений: application = lib.category(All). • групп приложений: application = lib.applicationgroup(); в скобках необходимо указать название группы приложений. • категорий приложений: application = lib.category(); в скобках необходимо указать название категорий приложений.
time	Настройка расписания работы правила. Для установки расписания: time = lib.time(); в скобках необходимо указать название группы календарей. Подробнее о настройке календарей читайте в разделе Настройка календарей.

Для редактирования правила управления пропускной способностью используется команда:

```
Admin@nodename# set network-policy traffic-shaping <position> upl-rule
```

Для просмотра всех созданных правил управления пропускной способностью используется команда:

```
Admin@nodename# show network-policy traffic-shaping
```

Для просмотра определенного правила управления пропускной способностью используется команда:

```
Admin@nodename# show network-policy traffic-shaping <position>
```

Пример создания правила управления пропускной способностью с использованием UPL:

```
Admin@nodename# create network-policy traffic-shaping 1 upl-rule OK \
...user = known \
...src.zone = Trusted \
...dst.zone = Untrusted \
...service = (HTTP, HTTPS) \
...time = lib.time("Working hours") \
...rule_log(session) \
...bandwidth_pool("1 Mbps") \
...name("Test traffic shaping rule") \
...desc("Test traffic shaping rule description") \
...enabled(true)
...
Admin@nodename# show network-policy traffic-shaping 1
```

```
% ----- 1 -----
OK \
  user = known \
  src.zone = Trusted \
  dst.zone = Untrusted \
  service = (HTTP, HTTPS) \
  time = lib.time("Working hours") \
  desc("Test traffic shaping rule description") \
  rule_log(session) \
  bandwidth_pool("1 Mbps") \
  enabled(true) \
  id(e63c34e6-af7f-4a4d-a29d-b51d4070655c) \
  name("Test traffic shaping rule")
```

Для удаления правила управления пропускной способностью используется команда:

```
Admin@nodename# delete network-policy traffic-shaping <position>
```

