ОБНОВЛЕНО 16 МАР

# Настройка и управление DosGate через CLI

Данная документация описывает взаимодействие с программным обеспечением DosGate с использованием командного интерфейса (CLI).

CLI является приоритетным способом управления системой, обеспечивая гибкость настройки и возможность автоматизации. Командный интерфейс позволяет администраторам работать с конкретными модулями системы, комбинировать параметры, правила и функции, что упрощает и ускоряет процесс конфигурирования.

Использование CLI обеспечивает полный доступ к функционалу системы и не ограничивает возможности администрирования, включая аварийные ситуации, в отличие от графических интерфейсов, подверженных перегрузке.

## Адресация команд для управления таргетами системы

Взаимодействие с таргетами DosGate осуществляется через командный интерфейс (CLI) с использованием raw socket.

Команды делятся на два типа:

- Системные – выполняют общие операции с системой.
- Целевые – управляют конкретными таргетами системы.

### 1. Системные команды

**Формат выполнения:**

```
dgctl -c command
```

**Доступные команды:**

```
# Вывести справочную информацию
dgctl -c help

# Отобразить текущую версию DosGate.
dgctl -c version

# Отобразить список всех доступных таргетов
dgctl -c targets
```

# 2. Целевые команды

**Формат выполнения:**

```
dgctl -u target://arena-name/target-name/target-options -c command --
command_options
```

**Аргументы:**

- `target://` – префикс, указывающий на обращение к целевому модулю.
- `<arena-name>` – имя арены, если требуется *(необязательный параметр)*.
- `<target-name>` – имя целевого модуля.
- `<target-options>` – дополнительные настройки *(необязательный параметр)*.
- `-c <command>` – команда, выполняемая в указанном модуле.
- `-- <command_options>` – дополнительные аргументы команды *(необязательный параметр)*.

**Доступные целевые таргеты:**

| Таргет | Описание |
|---|---|
| system | Управление системными функциями. |
| license | Управление лицензиями. |
| daemon | Контроль фоновых процессов. |
| geoip | Работа с географическими IP-базами. |
| context | Управление контекстами работы. |
| arena | Работа с аренами. |
| profile | Управление профилями. |

| Таргет | Описание |
|---|---|
| router | Настройка маршрутизации. |
| mark | Управление метками. |
| prefixset | Работа с наборами префиксов. |

**Доступные команды:**

```
# Вывести системную информацию
dgctl -u system:// -c sysinfo

# Получить идентификатор системы
dgctl -u system:// -c id

# Вывести справочную информацию.
dgctl -u system:// -c help

# Показать список лицензий
dgctl -u license:// -c list

# Отобразить информацию о лицензии
dgctl -u license:// -c show license
```

# Управление таргетом: daemon

Для таргета daemon, не требуется указывать арену

daemon - полностью дублирует системные команды

**Пример адресации таргета**

`dgctl -u daemon:// -c help`

# Управление таргетом: system

Таргет *system* предоставляет инструменты для получения информации о системе и проверки её состояния. Используется для мониторинга состояния системы, получения идентификационных данных и проверки доступности компонентов. Таргет не требует указания арены.

**Формат выполнения:**

```
dgctl -u system:// -c help
```

**Доступные команды:**

```
# Вывести справочную информацию
help

# Отобразить сведения о системе и использовании ресурсов DosGate
sysinfo

# Отобразить уникальный идентификатор системы
id

# Проверить доступность таргета
ping
```

# Управление таргетом: license

Управление лицензиями включает в себя просмотр, добавление, удаление и откат изменений, а также их экспорт. Таргет не требует указания арены.

**Формат выполнения:**

```
dgctl -u license:// -c help
```

**Доступные команды:**

```
# Вывести список лицензий.
list

# Отобразить сведения о конкретной лицензии.
show

# Добавить новую лицензию.
add

# Удалить лицензию.
delete

# Отменить удаление лицензии (восстановление).
undelete
```

```
# Применить изменения (удаление или добавление лицензии).
commit

# Экспортировать (скачать) лицензию.
download

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

# Управление таргетом: geoip

DosGate позволяет проверять IP-адрес отправителя и получателя на принадлежность определённому региону с использованием функции *geoip*.

Таргет не требует указания арены.

**Формат выполнения:**

```
dgctl -u geoip:// -c check -- <IP-адрес>
```

Пример:

```
dgctl -u geoip:// -c check -- 1.1.1.1
```

Вызов справки по таргету geoip:

```
dgctl -u geoip:// -c help
```

**Загрузка собственной базы данных**

По умолчанию DosGate загружает базу данных по пути: **/etc/dosgate/GeoLite2-Country.mmdb**

Резервный путь: **/usr/share/dosgate/GeoLite2-Country.mmdb**

Чтобы использовать свою базу данных, необходимо:

1. Разместить файл *GeoLite2-Country.mmdb* в каталоге **/etc/dosgate/**.
2. Перезагрузить сервис DosGate:

```
sudo service dosgate restart
```

### Содержимое базы данных

Для получения актуальной версии базы данных можно направить запрос по адресу: dosgate@servicepipe.ru

### Теги geoip

Список всех тегов geoip

```
Countries
Code Name
==========================================================================

AF Afghanistan
AX Åland Islands
AL Albania
DZ Algeria
AS American Samoa
AD Andorra
AO Angola
AI Anguilla
AQ Antarctica
AG Antigua and Barbuda
AR Argentina
AM Armenia
AW Aruba
AU Australia
AT Austria
AZ Azerbaijan
BS Bahamas
BH Bahrain
BD Bangladesh
BB Barbados
BY Belarus
BE Belgium
BZ Belize
BJ Benin
BM Bermuda
BT Bhutan
BO Bolivia, Plurinational State of
BQ Bonaire, Sint Eustatius and Saba
BA Bosnia and Herzegovina
```

```
BW Botswana
BV Bouvet Island
BR Brazil
IO British Indian Ocean Territory
BN Brunei Darussalam
BG Bulgaria
BF Burkina Faso
BI Burundi
KH Cambodia
CM Cameroon
CA Canada
CV Cape Verde
KY Cayman Islands
CF Central African Republic
TD Chad
CL Chile
CN China
CX Christmas Island
CC Cocos (Keeling) Islands
CO Colombia
KM Comoros
CG Congo
CD Congo, the Democratic Republic of the
CK Cook Islands
CR Costa Rica
CI Côte d'Ivoire
HR Croatia
CU Cuba
CW Curaçao
CY Cyprus
CZ Czech Republic
DK Denmark
DJ Djibouti
DM Dominica
DO Dominican Republic
EC Ecuador
EG Egypt
SV El Salvador
GQ Equatorial Guinea
ER Eritrea
EE Estonia
ET Ethiopia
FK Falkland Islands (Malvinas)
FO Faroe Islands
FJ Fiji
FI Finland
FR France
GF French Guiana
PF French Polynesia
TF French Southern Territories
GA Gabon
GM Gambia
GE Georgia
```

DE Germany
GH Ghana
GI Gibraltar
GR Greece
GL Greenland
GD Grenada
GP Guadeloupe
GU Guam
GT Guatemala
GG Guernsey
GN Guinea
GW Guinea-Bissau
GY Guyana
HT Haiti
HM Heard Island and McDonald Islands
VA Holy See (Vatican City State)
HN Honduras
HK Hong Kong
HU Hungary
IS Iceland
IN India
ID Indonesia
IR Iran, Islamic Republic of
IQ Iraq
IE Ireland
IM Isle of Man
IL Israel
IT Italy
JM Jamaica
JP Japan
JE Jersey
JO Jordan
KZ Kazakhstan
KE Kenya
KI Kiribati
KP Korea, Democratic People's Republic of
KR Korea, Republic of
KW Kuwait
KG Kyrgyzstan
LA Lao People's Democratic Republic
LV Latvia
LB Lebanon
LS Lesotho
LR Liberia
LY Libya
LI Liechtenstein
LT Lithuania
LU Luxembourg
MO Macao
MK Macedonia, the Former Yugoslav Republic of
MG Madagascar
MW Malawi
MY Malaysia

```
MV Maldives
ML Mali
MT Malta
MH Marshall Islands
MQ Martinique
MR Mauritania
MU Mauritius
YT Mayotte
MX Mexico
FM Micronesia, Federated States of
MD Moldova, Republic of
MC Monaco
MN Mongolia
ME Montenegro
MS Montserrat
MA Morocco
MZ Mozambique
MM Myanmar
NA Namibia
NR Nauru
NP Nepal
NL Netherlands
NC New Caledonia
NZ New Zealand
NI Nicaragua
NE Niger
NG Nigeria
NU Niue
NF Norfolk Island
MP Northern Mariana Islands
NO Norway
OM Oman
PK Pakistan
PW Palau
PS Palestine, State of
PA Panama
PG Papua New Guinea
PY Paraguay
PE Peru
PH Philippines
PN Pitcairn
PL Poland
PT Portugal
PR Puerto Rico
QA Qatar
RE Réunion
RO Romania
RU Russian Federation
RW Rwanda
BL Saint Barthélemy
SH Saint Helena, Ascension and Tristan da Cunha
KN Saint Kitts and Nevis
LC Saint Lucia
```

MF Saint Martin (French part)
PM Saint Pierre and Miquelon
VC Saint Vincent and the Grenadines
WS Samoa
SM San Marino
ST Sao Tome and Principe
SA Saudi Arabia
SN Senegal
RS Serbia
SC Seychelles
SL Sierra Leone
SG Singapore
SX Sint Maarten (Dutch part)
SK Slovakia
SI Slovenia
SB Solomon Islands
SO Somalia
ZA South Africa
GS South Georgia and the South Sandwich Islands
SS South Sudan
ES Spain
LK Sri Lanka
SD Sudan
SR Suriname
SJ Svalbard and Jan Mayen
SZ Swaziland
SE Sweden
CH Switzerland
SY Syrian Arab Republic
TW Taiwan, Province of China
TJ Tajikistan
TZ Tanzania, United Republic of
TH Thailand
TL Timor-Leste
TG Togo
TK Tokelau
TO Tonga
TT Trinidad and Tobago
TN Tunisia
TR Turkey
TM Turkmenistan
TC Turks and Caicos Islands
TV Tuvalu
UG Uganda
UA Ukraine
AE United Arab Emirates
GB United Kingdom
US United States
UM United States Minor Outlying Islands
UY Uruguay
UZ Uzbekistan
VU Vanuatu
VE Venezuela, Bolivarian Republic of

```
VN Viet Nam
VG Virgin Islands, British
VI Virgin Islands, U.S.
WF Wallis and Futuna
EH Western Sahara
YE Yemen
ZM Zambia
ZW Zimbabwe
XK Kosovo
```

```
Continents
Code Name
==========================================================================

AF Africa
AN Antarctica
AS Asia
EU Europe
NA North America
OC Oceania
SA South America
```

# Управление таргетом: context

Таргет *context* позволяет централизованно изменять параметры арен и управлять ими без необходимости указывать каждую арену отдельно.

Таргет *context* — необязательный компонент подсистемы, предназначенный для группировки нескольких арен в единый логический объект. Это позволяет упростить массовое управление аренами в процессе конфигурирования dosgate через файл dosgate.conf.

**Формат выполнения:**

```
dgctl -u context:// -c help
```

**Доступные команды:**

```
# Отобразить список всех арен, включенных в контекст.
show
```

```
# Сохранить текущее состояние контекста.
save

# Применить изменения в контексте, включая все арены и профили, входящие в
него.
commit

# Откатить контекст к предыдущему сохраненному состоянию, если команда commit
не была выполнена.
rollback

# Пересобрать все программы dosgate. Используется для отладки. Не рекомендуется
запускать во время активной эксплуатации.
rebuild

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

# Управление таргетом: arena

Таргет *arena* предоставляет ряд функций, позволяющих управлять профилями, их версиями и состоянием в системе DosGate.

**Формат выполнения:**

```
dgctl -u arena://arena-name -c help
```

**Доступные команды:**

```
# Добавить профиль.
add

# Удалить профиль.
delete

# Отобразить список всех профилей арены.
list

# Применить все профили арены.
commit

# Откатить контекст к предыдущему сохраненному состоянию, если команда commit
```

```
не была выполнена.
rollback

# Сохранить все профили арены.
save

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

# Управление таргетом: profile

Таргет *profile* предназначен для управления профилями защиты в системе DosGate. Профиль представляет собой набор правил, применяемых к сетевому трафику, проходящему через систему. С его помощью можно управлять фильтрацией пакетов, анализировать их характеристики и применять необходимые действия.

**Основные возможности профиля:**

1. Определение IP-адресов получателей, привязанных к профилю (один IP-адрес не может быть закреплён за несколькими профилями одновременно).
2. Задание набора правил фильтрации трафика.
3. Применение правил в порядке следования (правила обрабатываются сверху вниз).
4. Использование трёх основных сущностей в правилах:
   - `Match` - параметры пакета, по которым выполняется фильтрация.
   - `Action` - действие, выполняемое при соответствии пакета условиям фильтрации.
   - `Stats` - запись статистики обработки трафика.

При отсутствии `match` в правиле действие `action` применяется ко всем пакетам. Если указан только `match` без `action`, правило не влияет на трафик.

**Формат выполнения команд:**

```
dgctl -u profile://arena-name/profile-name -c <команда>
```

Новые правила применяются только при использовании команды insert:

```
dgctl -u profile://arena-name/profile-name -c insert -- rule
```

Пример добавления правила с фильтрацией TCP-трафика:

```
dgctl -u profile://arena-name/profile-name -c insert -- -m protocol tcp -j DROP
```

**Пример адресации таргета**

`dgctl -u profile://arena-name/profile-name -c command -- rule`

## Команды для цели profile

```
# Добавить правило.
insert

#Можно указать позицию вставки (опция `-i`). Правило будет добавлено на
четвёртую позицию:

dgctl -u profile://first/test -c insert -i 4 -- rule

# Удалить правило. Указывается позиция (или диапазон через `-`).
remove

#Удаление правила на 4-й позиции:
dgctl -u profile://first/test -c remove -i 4

#Удаление нескольких правил на указанных позициях (например, 1, 3 и 5):
dgctl -u profile://first/test -c remove -i 1,3,5

#Удаление диапазона правил (например, с 1-й по 5-ю позицию):
dgctl -u profile://first/test -c remove -i 1-5

# Заменить правило на заданной позиции.
replace

#Замена правила другим правилом на 3 позиции:
dgctl -u profile://first/test -c replace -i 3 -- rule


# Отобразить список правил профиля.
list


# Применить набор правил.
commit
```

```
# Для сохранения набора правил в профиле. Команда доступна только после
выполнения *commit*. Сохраненный набор правил будет автоматически применен при
перезагрузке сервиса DosGate.
save

# Откатить профиль до предыдущей версии (если не был выполнен commit).
rollback


# Переименовать профиль и изменить его описание.
rename

# Проверить доступность таргета.
ping


# Используется для внутренней отладки.
backref_stats

# Вывести справочную информацию.
help
```

## Документация сущностей (match & action rule)

**Основные параметры:**

- `-m` (match) - определяет характеристики пакетов для фильтрации.
- `-j` (action) - указывает действие, выполняемое при соответствии условиям.
- `-c` (comment) — добавляет комментарий к правилу.

```
Usage: [-m <match>]... [-j <action>]... [-c <comment>...]
```

**Комбинирование параметров match и action**
Параметры match и action могут использоваться совместно для точного определения характеристик пакета и применения соответствующих действий.

В командной строке двойное тире `--` используется для разделения команды и параметров правила (match & action).

**Вызов справки по match и action**

Для просмотра доступных параметров фильтрации и возможных действий используйте команду:

```
dgctl -u profile://arena-name/profile-name -c insert -- help
```

**Пример комбинации правил**

Пример 1: Фильтрация по протоколу TCP с выполнением действий `STATS` и `DROP`:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -j STATS
TCP_protocol -j DROP
```

Пример 2: Фильтрация по протоколу TCP, TTL, геолокации с выполнением действий `STATS` и `ACCEPT`:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -m ttl 155 -m geoip
cntr RU -j STATS bypass_for_ru_ttl_155_tcp -j ACCEPT
```

Пример 3: Фильтрация ACL для веб-ресурса, с выполнением действий `MARK` и `DROP`:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -m dport 80,443 -j
MARK value 1 ! -m mark 1 -j STATS WEB_ACL -j DROP
```

**Получение справки по параметрам**

В справке (help) подробно описано, как использовать каждый параметр match и action, а также доступные для них опции.

Пример:

```
dgctl -u profile:/arena-name/profile-name -c insert -- -m protocol help

dgctl -u profile://first/test -c insert -- -j RATELIMIT help

dgctl -u profile://first/test -c insert -- -m icmp help

dgctl -u profile://first/test -c insert -- -m geoip help
```

**Опция "NOT"**

Перед параметром `match` допустимо использование символа `!`, который выполняет функцию логического оператора **NOT**.

Пример:

```
-m protocol tcp ! -m dport 443,80 -j DROP
```

Данное правило означает: если пакет использует протокол TCP, но порт получателя не 80 или 443 — сбросить пакет.

*Примечание:*

> Оператор `!` нельзя использовать с `-m protocol`.

**Список доступных match & action**

Просмотреть все доступные параметры можно с помощью команды:

```
dgctl -u profile://arena-name/profile-name -c insert -- help
```

Match

| Match | Описание |
|---|---|
| protocol | Протокол |
| mark | Общая метка фрейма |
| len | Длина элемента фрейма |
| ttl | Время жизни (TTL) |
| frag | Фрагментация пакета на сетевом уровне |
| src | Сетевой адрес источника |
| dst | Сетевой адрес получателя |
| spi | IPSec SPI |
| tsrc | Туннелированный адрес источника |
| tdst | Туннелированный адрес назначения |
| tspi | Туннелированный IPSec SPI |
| dport | Порт назначения на транспортном уровне |
| sport | Порт источника на транспортном уровне |

| Match | Описание |
|---|---|
| gre | Элементы GRE-заголовка |
| tcpflags | Флаги TCP |
| hmark | Метка хоста источника |
| sdhmark | Метка хоста источника и назначения |
| connmark | Метка соединения |
| dhmark | Метка хоста назначения |
| verdict | Результат предыдущего действия |
| seq | Последовательность байтов |
| dns | Заголовок DNS |
| tcpopts | Опции TCP |
| tcpmss | Максимальный размер сегмента TCP |
| tcpws | Масштаб окна TCP |
| icmp | Тип/код ICMP |
| icmp6 | Тип/код ICMPv6 |
| pset | Совпадение с префиксом из набора, заданного на основе IP-адреса |
| tpset | Совпадение с префиксом из набора, заданного на основе туннелированного IP-адреса |
| geoip | Совпадение с данными в GeoIP-базе на основе IP-адреса |
| tgeoip | Совпадение с данными в GeoIP-базе на основе туннелированного IP-адреса |

## Action

| Action | Описание |
|---|---|
| ACCEPT | Принять фрейм и прекратить дальнейшую обработку |
| DROP | Немедленно отбросить фрейм |
| PASS | Передать пакет в сетевой стек ОС |
| STATS | Собирать статистику по всем обрабатываемым пакетам |
| MARK | Изменить общий маркер фрейма |
| HMARK | Добавить запись в таблицу меток для источника |
| SDHMARK | Добавить запись в таблицу меток для источника и назначения |
| CONNMARK | Добавить запись в таблицу меток для соединения |
| DHMARK | Добавить запись в таблицу меток для назначения |
| VERDICT | Изменить вердикт |
| RATELIMIT | Применить ограничение скорости |
| SAMPLE | Провести выборку трафика |

| Action | Описание |
|---|---|
| TCPAUTH | Выполнить авторизацию TCP |
| SNAT | Источник статического NAT |
| DNAT | Назначение статического NAT |
| CAPTURE | Захватить пакет |
| GOTO | Перейти к указанной цепочке правил |
| RATE | Механизм ограничения скорости с расширенными возможностями подсчёта |

# Управление таргетом: router

Таргет *router* используется для настройки маршрутизации пакетов в рамках профиля. Каждому профилю назначается индивидуальный набор IP-префиксов, которые определяют, какие пакеты должны обрабатываться данным профилем.

Пакеты, чей IP-адрес получателя соответствует указанному в конфигурации префиксу, направляются на профиль. Если IP-адрес отсутствует в маршрутизаторе и пакет не является L2-multicast (при работе в режимах inline или transparent), он передается в операционную систему.

**Формат выполнения:**

```
dgctl -u router://arena-name/profile-name -c command -- prefix
```

Добавление и удаление префиксов поддерживает указание нескольких значений через запятую, а также диапазонов (через тире `-`).

После внесения изменений в конфигурацию маршрутизатора требуется применить их с помощью команд:

```
dgctl -u profile://first/test -c commit
```

```
dgctl -u profile://first/test -c save
```

**Доступные команды:**

```
# Добавить указанный IP-префикс в таблицу маршрутизации профиля.
insert

# Удалить указанный префикс из таблицы маршрутизации.
remove

#Удаляет указанный префикс, автоматически разбивая оставшиеся адреса по маскам.
pin

#Пример: Если в маршрутизаторе имеется запись 1.1.1.0/24 и требуется удалить
1.1.1.88/32, выполняется команда:

 #dgctl -u router://first/test -c pin -- 1.1.1.88

#Система автоматически удалит только 1.1.1.88/32, разделяя оставшийся диапазон
на соответствующие маски.


# Выводит полный список маршрутов, заданных в профиле.
list

# Выводит список маршрутов непосредственно из программы dosgate в ядре Linux.
list_kernel

# Показывает несохраненные изменения в таблице маршрутизации профиля.
diff

# Вывести справочную информацию.
help


# Проверяет доступность таргета.
ping
```

# Управление таргетом: mark

Таргет *mark* используется индивидуально для каждого профиля и представляет собой механизм хранения и обработки меток. Метки позволяют временно сохранять информацию о пакетах и использовать её в последующих правилах фильтрации.

Метка (mark) может как записывать информацию из пакета (например, `-j HMARK id 1 value 1 lifetime 600`), так и проверять её наличие (`-m hmark id 1 status valid`).

Важно: в метках поддерживаются только адреса с маской /32. Другие маски не применяются.

**Типы меток**

Метки представляют собой быстрые таблицы данных:

- **hmark** - Хранит в себе IP-адреса отправителя.
- **sdhmark** - Хранит в себе IP-адреса отправителя и IP-адрес получателя.
- **dmark** - Хранит в себе IP-адрес получателя.
- **connmark** - Хранит в себе IP-адрес отправителя, IP-адрес получателя, протокол, порт отправителя и порт получателя.

**Формат выполнения:**

```
dgctl -u mark://arena-name/profile-name -c command -- command_options
```

**Доступные команды:**

```
# Отобразить содержимое метки.  (Не рекомендуется использовать без фильтров
# которые указываются в \<command-options\>, при большом объёме данных.)
list

# Добавить информацию в метку.
insert

# Удалить информацию из метки.
delete

# Вывести справочную информацию.
help

# Проверить доступность таргета.
ping
```

**Опции команд**

```
Usage: [[type] <type>] id <id> [<field_name> <field_value>]... value <val>
[expire <exp>]
```

Параметры метки:

- **type** – Тип метки. По умолчанию `shost`.
- **id** – Идентификатор метки, диапазон: 0, 2^32-1.

- **field_name** – Имя поля метки. См. ниже.
- **field_value** – Значение поля метки, специфично для протокола.
- **val** – Значение метки, диапазон: 0, 2^32-1.
- **exp** – Время жизни в секундах, начиная с текущего момента. По умолчанию – без срока действия.

Названия полей:

- **l3_proto** – Протокол сетевого уровня
- **l3_src** – Исходный адрес сетевого уровня
- **l3_dst** – Адрес назначения сетевого уровня
- **sec_proto** – Протокол безопасности IP
- **sec_id** – Идентификатор безопасности IP (SPI)
- **tun_proto** – Протокол туннеля
- **tun_id** – Идентификатор туннеля
- **l3_tun_proto** – Туннелируемый протокол сетевого уровня
- **l3_tun_src** – Исходный адрес туннелируемого сетевого уровня
- **l3_tun_dst** – Адрес назначения туннелируемого сетевого уровня
- **sec_tun_proto** – Туннелируемый протокол безопасности IP
- **sec_tun_id** – Идентификатор безопасности туннелируемого IP (SPI)
- **l4_proto** – Протокол транспортного уровня
- **l4_src** – Исходный адрес транспортного уровня (порт)
- **l4_dst** – Адрес назначения транспортного уровня (порт)

Протоколы сетевого уровня:

- **ipv4** – IPv4
- **ipv6** – IPv6

Протоколы безопасности:

- **ah** – Заголовок аутентификации (AH)
- **esp** – Инкапсулированная полезная нагрузка безопасности (ESP)

Протоколы туннелей:

- **ipip** – Туннель IP-IP (ipencap)
- **gre** – Универсальная инкапсуляция маршрутизации (GRE)

Туннелируемые протоколы сетевого уровня:

- **tun_ipv4** – Туннелируемый IPv4

- **tun_ipv6** – Туннелируемый IPv6

Туннелируемые протоколы безопасности:

- **tun_ah** – Туннелируемый заголовок аутентификации (AH)
- **tun_esp** – Туннелируемая инкапсулированная полезная нагрузка безопасности (ESP)

Протоколы транспортного уровня:

- **udp** – Протокол пользовательских датаграмм (UDP)
- **tcp** – Протокол управления передачей (TCP)
- **sctp** – Протокол управления потоком передачи (SCTP)

Типы меток:

- **shost** – Исходный адрес сетевого уровня
- **dhost** – Адрес назначения сетевого уровня
- **sdhost** – Исходный и адрес назначения сетевого уровня
- **conn** – Полное соединение (Ntuple)

# Управление таргетом: prefixset

Таргет *prefixset* может быть двух типов:

- **Глобальный**: применяется ко всей системе.
- **Индивидуальный**: специфичен для конкретного профиля.

В *prefixset* поддерживаются все маски IP-адресов. Префикс-сет представляет собой таблицу данных, которую может редактировать только администратор вручную. Данные в префикс-сет нельзя добавить автоматически через правила, что отличает его от меток (быстрых таблиц данных).

**Функциональность**

- **Поиск**: По префикс-сету можно осуществлять поиск с использованием команды `match`. Поиск может выполняться как по IP-адресу отправителя, так и по IP-адресу получателя.
- **Применение изменений**: После внесения изменений в префикс-сет необходимо применить их с помощью команды `-c commit`. Сохранение (`-c save`) не требуется.

**Формат выполнения:**

Примеры индивидуального префикс-сета:

```
dgctl -u prefixset://arena-name/profile-name/prefixset -c command
```

```
dgctl -u prefixset://arena-name/profile-name/ -c command
```

Примеры глобального префикс-сета:

```
dgctl -u prefixset://arena-name/prefixset-name -c command
```

```
dgctl -u prefixset://arena-name/ -c command
```

**Доступные команды:**

```
#Показать список префикс-сетов или их содержимое.
list

#Создать новый префикс-сет.
new

# Переименовать префикс-сет.
rename

# Очистить префик-сет.
free

# Отменить очистку (до применения commit).
unfree

# Применить изменения.
commit

# Откатить изменения (до применения commit).
rollback

# Добавить данные в префикс-сет.
insert

# Заменить данные в префикс-сете.
replace
```

```
# Удалить данные из префикс-сета.
delete

# Удалить все указанные суб-префиксы.
# Например, указав delete_sub 0.0.0.0/0 - префикс-сет полностью очистится.
delete_sub

# Удалить префикс, автоматически разбивая его
# Например, если в префикс-сете есть 1.1.1.0/24, и нужно удалить 1.1.1.88/32,
# выполните команду: dgctl -u prefixset://first/test/test -c pin -- 1.1.1.88/32
# Система удалит только .88/32, оставив остальные префиксы (1.1.1.0/25,
1.1.1.128/25 и т.д.)
pin


# Показать изменения, ожидающие применения (до выполнения commit).
diff

# Используется для внутренней отладки.
backref

# Проверить доступность таргета.
ping

# Вывести справочную информацию.
help
```

# Управление таргетом: chain

Таргет *chain* позволяет создавать дополнительные цепочки правил, которые могут использоваться для перенаправления пакетов с помощью команды `-j GOTO chain-name`. Цепочки уникальны для каждого профиля защиты.

Перед этим – chain нужно создать

- **Применение изменений**: Применение ( `-c commit` ) и сохранение ( `-c save` ) цепочек происходит автоматически при применении профиля. Отдельно применять цепочки не требуется.

**Формат выполнения:**

```
dgctl -u chain://arena-name/profile-name/chain-name -c command -- command
options` или `dgctl -u chain://arena-name/profile-name -c command
```

**Доступные команды:**

```
# Показать список цепочек в профиле или правила в цепочке.
list

# Добавить новую пустую цепочку или правила в существующую цепочку.
insert

# Удалить цепочку или правила в цепочке.
delete

# Заменить правила в цепочке.
replace

# Удалить все правила из цепочки.
clear

# Отменить предыдущее удаление цепочки.
undelete

# Переименовать существующую цепочку.
rename

# Показать все ссылки на цепочку (используется для внутренней отладки).
backref

# Показать справку по командам.
help

# Проверить доступность таргета.
ping
```

**Примеры использования**

Создать цепочку под именем "acl" с описанием "access list rules set":

```
dgctl -u chain://first/test -c insert acl access list rules set
```

Добавить правило в цепочку:

```
dgctl -u chain://first/test/acl -c insert -- ! -m dport 80,443 -j STATS
incorrect_proto_and_ports -j DROP
```

Добавить второе правило:

```
dgctl -u profile://first/test -c insert -- -m protocol tcp -j GOTO acl
```

Применить и сохранить измнения:

```
dgctl -u profile://first/test -c commit
dgctl -u profile://first/test -c save
```