ОБНОВЛЕНО 16 МАР

FlowSpec-правила

FlowSpec-правила — это механизм BGP Flow Specification для распространения фильтрационных политик на маршрутизаторы.

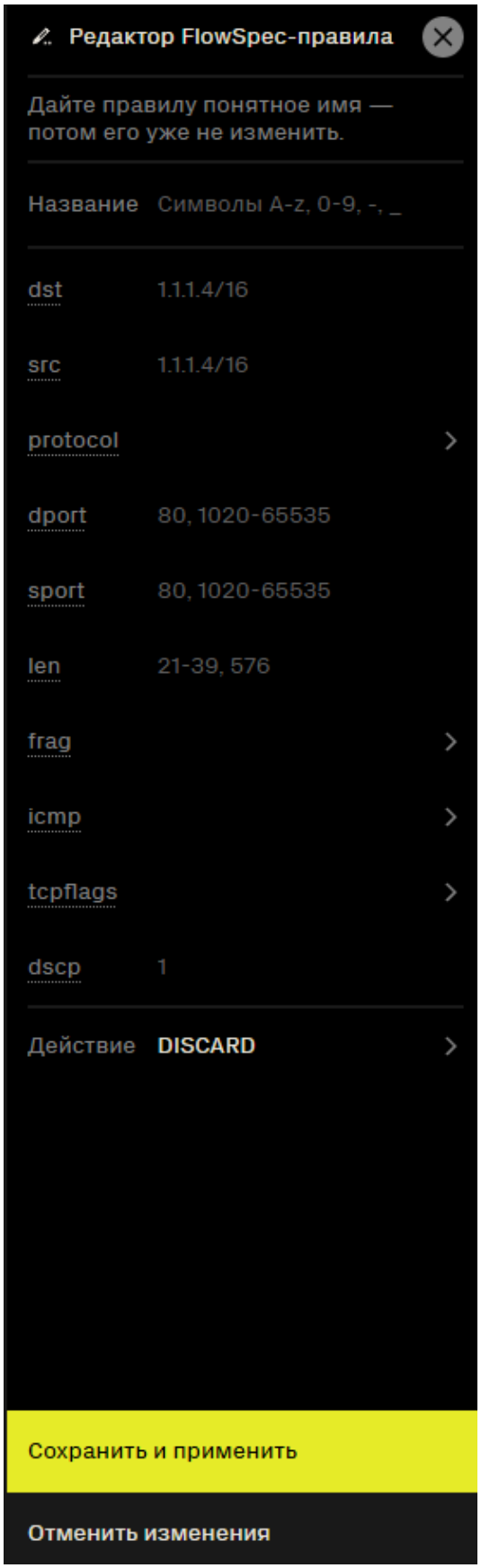
Область применения

FlowSpec-правила применяются для динамической фильтрации на уровне маршрутизаторов в ситуациях, когда требуется быстро ограничить, перенаправить или маркировать трафик без изменений в нижестоящих сервисах. Исполнение происходит на границе сети, до системы очистки; при DDoS-атаках правила позволяют отсечь вредоносный поток на входе и не допустить перегрузки очистителя.

В инфраструктурах без выделенного очистителя FlowSpec-правила выступают основным механизмом быстрой фильтрации. Также используются как дополнительный защитный слой: первичная отсечка нежелательного трафика выносится на вышестоящие BGP-маршрутизаторы, что разгружает внутренние узлы и каналы.

Добавление FlowSpec-правила

Для добавления нового правила в правой части интерфейса **нажать** серую кнопку **«Добавить правило»**. Откроется редактор **FlowSpec-правил**, содержащий три блока: **Название**, **Совпадение** и **Действие**. В блоке **Совпадение** указываются условия отбора трафика, в блоке **Действие** — способ обработки трафика маршрутизатором. Для применения изменений нажать жёлтую кнопку **Сохранить и применить**.


Редактор FlowSpec-правила
Дайте правилу понятное имя — потом его уже не изменить.
Название
Символы A-z, 0-9, -, _
dst
1.1.1.4/16
src
1.1.1.4/16
protocol
dport
80, 1020-65535
sport
80, 1020-65535
len
21-39, 576
frag
icmp
tcpflags
dscp
1
Действие
DISCARD
Сохранить и применить
Отменить изменения

Название

- Допустимые символы: A–Z, 0–9, дефис -, подчёркивание _.
- Рекомендуем давать правилам краткие и однозначные имена, отражающие их назначение. Примеры: *udp-amp-auto*, *ipfrag-drop*, *invalid-ports*

Совпадение

Совпадения — это техническое условие, по которому маршрутизатор выбирает трафик для применения правила.

Для большинства совпадений доступен флаг **NOT**. Он выполняет логическое отрицание: при включении условие работает наоборот, и правило применяется ко всем значениям *кроме указанного*.

> **Примечание**
> Для полей **dst** и **src** флаг **NOT** отсутствует. Отрицание не поддерживается

dst — IP назначения

Параметр	Описание
Адрес	Адрес назначения (IPv4/IPv6 в формате CIDR)

Если поле **оставить пустым — правило используется как шаблон**. Во время аномалии адрес назначения автоматически подставляется из события/счётчика.

src — IP источника

Параметр	Описание
Адрес	Адрес источника (IPv4/IPv6 в формате CIDR)

protocol — Протокол

Протокол	Описание
TCP	Протокол управления передачей (Transmission Control Protocol)
UDP	Протокол пользовательских дейтаграмм (User Datagram Protocol)
ICMP	Протокол управления интернет-сообщениями (Internet Control Message Protocol)

Протокол	Описание
IGMP	Управление членством в мультикаст-группах для IPv4
IP-in-IP	Инкапсуляция IP-пакетов в IP (туннелирование без шифрования)
RSVP	Резервирование сетевых ресурсов и сигнализация QoS
GRE	Протокол инкапсуляции (Generic Routing Encapsulation)
OSPF	Внутренний протокол маршрутизации (IGP) на основе состояния каналов
PIM	Протокол независимой мультикаст-маршрутизации
SCTP	Протокол управления потоками сообщений (Stream Control Transmission Protocol)

dport — Порт назначения

Параметр	Описание
dport	Порты назначения для сопоставления трафика. Формат: значения и/или диапазоны 0–65535, через запятую. Примеры: 80; 53, 123; 1020–65535

sport — Порт источника

Параметр	Описание
sport	Порты источника для сопоставления трафика. Формат: значения и/или диапазоны 0–65535, через запятую. Примеры: 0, 17, 19, 69, 123; 49152–65535

len — Длина пакета

Параметр	Описание
len	Длина IP-пакета в байтах. Формат: значения и/или диапазоны, через запятую. Примеры: 1280; 60–80; 576

frag — Фрагментация

Значение	Описание
any	Любой фрагмент (первый, внутренний, последний)
df	Установлен флаг Don’t Fragment
first	Первый фрагмент
internal	Внутренний фрагмент
last	Последний фрагмент

Значение	Описание
unfrag	Не фрагментированный пакет

icmp — Тип/код

Проверяются сочетания *тип–код*: правило срабатывает только на пакеты, где **тип** и **код** встречаются одновременно; недопустимые комбинации игнорируются.

Параметр	Описание
icmp-тип	Значения или диапазоны типа ICMP. Примеры: 8 (Echo Request), 11 (Time Exceeded)
icmp-код	Значения или диапазоны кода ICMP. Примеры: 0; 1

tcpflags — Флаги TCP

Флаг	Описание
syn	Инициализация соединения
ack	Подтверждение соединения
psh	Передача без задержки
rst	Принудительный сброс
fin	Завершение соединения
ece	Индикация перегрузки (ECN Echo)
cwr	Снижение окна при перегрузке (Congestion Window Reduced)
urg	Срочные данные (Urgent)

Опция **Учитывать совместно (+)** задаёт логику проверки TCP-флагов:

- Если опция включена, правило срабатывает только когда все выбранные флаги выставлены одновременно.
- Если опция выключена, достаточно любого одного из выбранных флагов.

dscp — Класс обслуживания

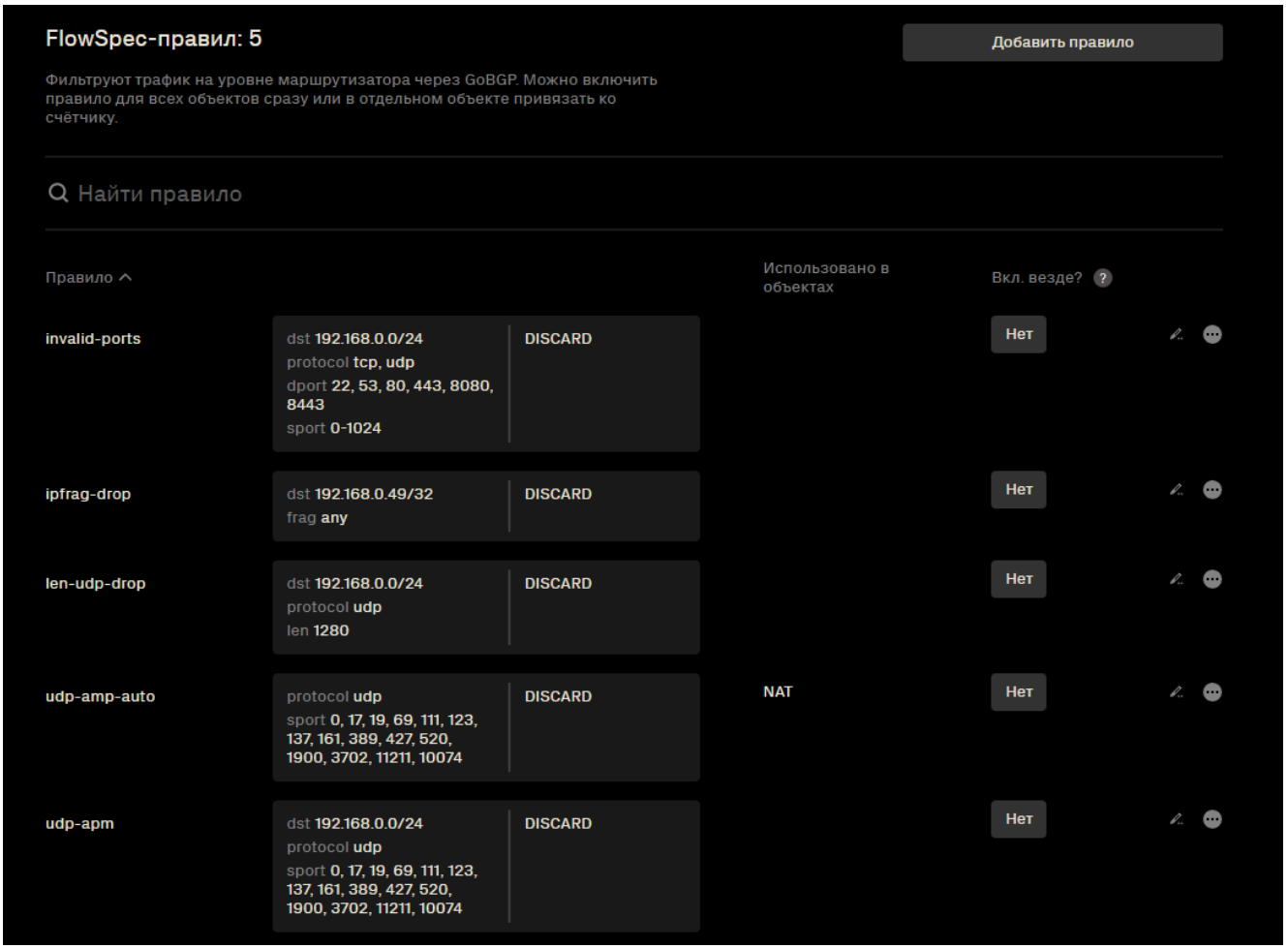
Параметр	Описание
dscp	Класс обслуживания DSCP, диапазон 0–63. Пример: 46

Действие

Определяет реакцию маршрутизатора на трафик, попавший под условия.

Параметр	Аргумент	Описание
ACCEPT	—	Разрешить трафик
DISCARD	—	Отбросить трафик
rate-limit	—	Ограничение скорости; трафик выше порога отбрасывается
	rate-limit	Порог скорости; единицы — по конфигурации системы
	AS	Номер автономной системы для сообщества traffic-rate
redirect	—	Перенаправление в целевой VRF
	route-target (rt)	Формат: **as:vrf** или **cidr:vrf**, например 65000:123
mark	—	Маркировка DSCP для последующей приоритезации
	dscp	Значение 0–63
action sample	—	Семплирование и логирование трафика
action terminal	—	Прекращение дальнейшей фильтрации для совпавшего трафика
action sample-terminal	—	Семплировать и завершить дальнейшую фильтрацию (комбинированное действие)

Примеры FlowSpec-правил



Ниже представлены примеры FlowSpec-правил. Для каждого правила указаны условия совпадения и действие маршрутизатора. Примеры позволяют понять, какой трафик фильтруется и каким образом правило применяется в сети.

- **invalid-ports — DISCARD**
  Отбросить TCP/UDP-трафик к подсети 192.168.0.0/24 на неразрешённые по условию порты (22, 53, 80, 443, 8080, 8443; возможны диапазоны). Назначение: блокировка несанкционированных подключений и сканирований.
- **ipfrag-drop — DISCARD**
  Отбросить фрагментированные IP-пакеты к адресу 192.168.0.49/32. Назначение: защита от атак с использованием фрагментации.
- **len-udp-drop — DISCARD**
  Отбросить UDP-пакеты фиксированной длины 1280 байт к сети 192.168.0.0/24. Назначение: подавление сигнатурных шумов в рамках DDoS.
- **udp-amp-auto — DISCARD**
  Отбросить UDP-трафик с характерных исходных портов усилителей (0, 17, 19, 69, 111, 123, 137, 161, 389, 427, 520, 1900, 3702, 11211, 10074). При пустом поле **dst** правило используется как шаблон: при срабатывании счётчика система подставляет адрес назначения из события и формирует анонс FlowSpec для этого адреса. Действие применяется точечно к подставленному **dst** и не действует глобально само по себе.

- **udp-apm — DISCARD**
  Отбросить UDP-амплификации в подсети 192.168.0.0/24 по тем же исходным портам.
  Назначение: локальная фильтрация в заданной сети.

В столбце **Использовано в объектах** указывается, к каким объектам системы привязано правило.

Столбец **Вкл. везде?** — ручная публикация анонса FlowSpec. При включении система немедленно формирует и отправляет BGP FlowSpec-анонс правила на маршрутизаторы. Пороги и счётчики объектов при этом не учитываются.