Инструкция по эксплуатации программного обеспечения Servicepipe Spider

Оглавление

1 Введение 6

1.1. Общие положения 6

1.2. Назначение программного обеспечения 6

1.3. Требования к квалификации персонала 6

2 Вход в систему и завершение работы 7

2.1 Открытие веб-интерфейса 7

2.2 Завершение работы 8

3 Управление объектами мониторинга 9

3.1 Панель быстрого доступа 9

4 Настройки 11

4.1 Участники 11

4.1.1 Пользователи 11

4.1.2 Роли и права доступа 12

4.1.3 Параметры и синк 13

4.2 Окружение 14

4.2.1 Приложение 14

4.2.2 Фид-сервис 17

4.2.3 SNMP 17

4.2.4 Syslog 19

4.3 Ноды 20

4.3.1 Добавление новой ноды 21

4.4 Мониторинг 22

4.5 Ещё 24

4.6 Syslog Thresholds 26

4.7 HW Bypass 27

5 DosGate 29

5.1 Статистика 29

5.1.1 Общая статистика 29

5.1.2 Статистика по прифилям 30

5.2 Профиль защиты 31

5.2.1 Создание профиля 31

5.2.2 Изменение профиля 32

5.2.3 Экспорт профиля 33

5.2.4 Очистка профиля 33

5.2.5 Удаление профиля 34

5.2.6 История версий 34

5.2.7 Автообновление профиля....35
5.2.8 Переход к компоненту....35
5.2.9 Разрыв связи с пресетом....35
5.3 Правила....36
5.3.1 Созданиеи редактирование правил....36
5.3.2 Пример №1....37
5.3.3 Пример №2....39
5.4 Чейны....42
5.4.1 Назначение чейнов....42
5.4.2 Принцип работы....42
5.4.3 Пример использования чейна....42
5.5 Роутер....43
5.5.1 Общие сведения....43
5.5.2 Принцип работы....44
5.5.3 Настройка роутера в профиле....44
5.6 Метки....45
5.6.1 Общие сведения....45
5.6.2 Типы меток....45
5.6.3 Принцип работы меток....46
5.6.4 Создание метки....46
5.6.5 Применение метки в правилах....46
5.6.6 Обновление и удаление....46
5.6.7 Пример использования HMARK....47
5.6.8 Пример использования CONNMARK....48
5.6.9 Пример использования HMARKC....49
5.6.10 Использование счётчика Value....50
5.7 Префикс-сеты....51
5.7.1 Общие сведения....51
5.7.2 Добавление префикс-сета....51
5.7.3 Создание нового префикс-сета....52
5.7.4 Создание префикс-сета по ссылке....52
5.7.5 Добавление записи в префикс-сет....53
5.7.6 Добавление записей из TXT-файла....53
6 RLog....55
6.2.1 Пример работы RLOG с DosGate....56
6.3.1 Создание профиля....56
6.3.2 Изменение профиля....57

6.3.3 Удаление профиля....57
6.4.1 Навигация и фильтрация....58
6.4.2 Таблица хостов....58
6.4.3 Графики....58
7 FlowCollector....61
7.2.1 Создание объекта....61
7.2.2 Изменение объекта....62
7.2.3 Удаление объекта....62
7.3.1 Рабочая область....62
7.3.2 Общая статистика по аномалиям....63
7.3.3 Поиск и фильтрация аномалий....63
7.3.4 Список аномалий....63
7.3.5 Просмотр сведений об аномалии....64
7.3.6 Визуализация трафика....64
7.4.1 Включение Data Explorer....65
7.4.2 Построение отчёта....66
7.4.3 Просмотр результатов....68
7.4.4 Сброс параметров....68
7.5.1 Назначение....69
7.5.2 Добавление FlowSpec-правила....69
7.5.3 Совпадения....69
7.5.4 Действия....72
7.5.5 Примеры правил....73
7.5.6 Список правил....73
7.6.1 Общие настройки....74
7.6.2 Перенаправление трафика на следующий хоп....74
7.6.3 Количество IP-адресов для сворачивания аномалий....74
7.6.4 Начало аномалии....75
7.6.5 Задержка завершения аномалии....75
7.6.6 Управление счётчиками....75
7.6.7 Добавление счётчика....75
7.6.8 Дублирование счётчика....76
7.6.9 Удаление счётчика....76
7.6.10 Включение и отключение счётчика....76
7.6.11 Приоритет счётчиков....76
7.6.12 Тип подсчёта....76
7.6.13 Векторы трафика....77

7.6.14 Условие срабатывания 78
7.6.15 Фильтрация 79
7.7.1 Принцип работы 80
7.7.2 Добавление CIDR-адреса 80
7.7.3 Удаление CIDR-адреса 80

1 Введение

1.1. Общие положения

Настоящая инструкция по эксплуатации определяет порядок использования программного обеспечения Servicepipe Spider, требования к пользователям системы, а также основные термины и обозначения, применяемые в документе.

1.2. Назначение программного обеспечения

Программное обеспечение Servicepipe Spider предназначено для централизованного управления программными продуктами FlowCollector DosGate и RLog, контроля их состояния и отображения получаемых от них данных через веб-интерфейс.

Servicepipe Spider обеспечивает настройку параметров подключённых компонентов, управление правилами и политиками обработки сетевого трафика, просмотр событий, уведомлений, журналов, статистики и показателей работы системы. Программное обеспечение также используется для передачи команд управления и изменений конфигурации в подключённые программные продукты.

1.3. Требования к квалификации персонала

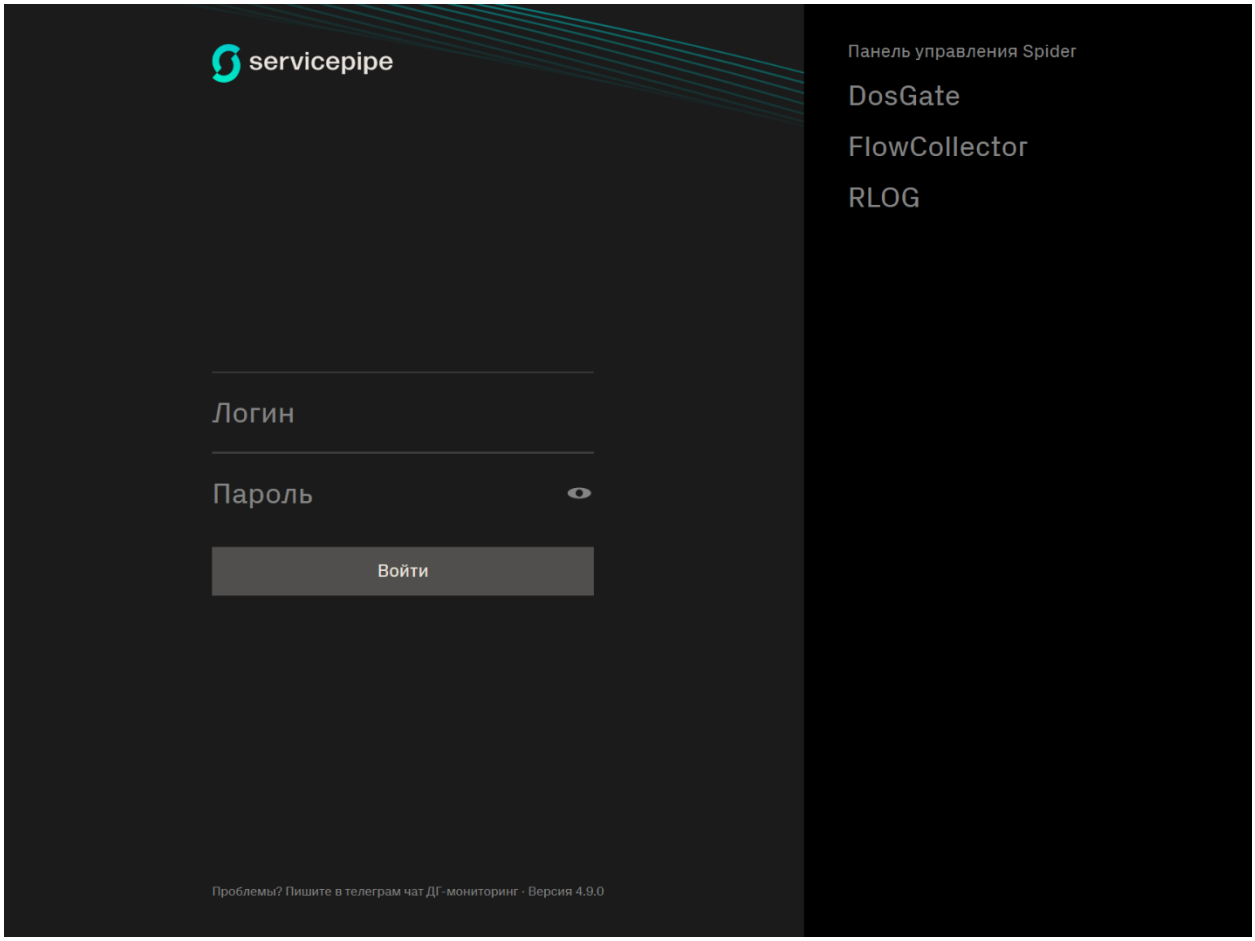
Эксплуатация экземпляра программного обеспечения требует:

- знания и навыки администрирования ОС Linux и СУБД;
- знания и навыки работы с командной строкой;
- понимание работы сетевых протоколов;
- базовые знания языка SQL.

2 Вход в систему и завершение работы

2.1 Открытие веб-интерфейса

Для входа в веб-интерфейс Servicepipe Spider следует открыть в браузере адрес, по которому доступна панель управления Servicepipe Spider. После открытия страницы появится окно авторизации.



В окне авторизации следует указать логин и пароль учётной записи, затем нажать кнопку **Войти**.

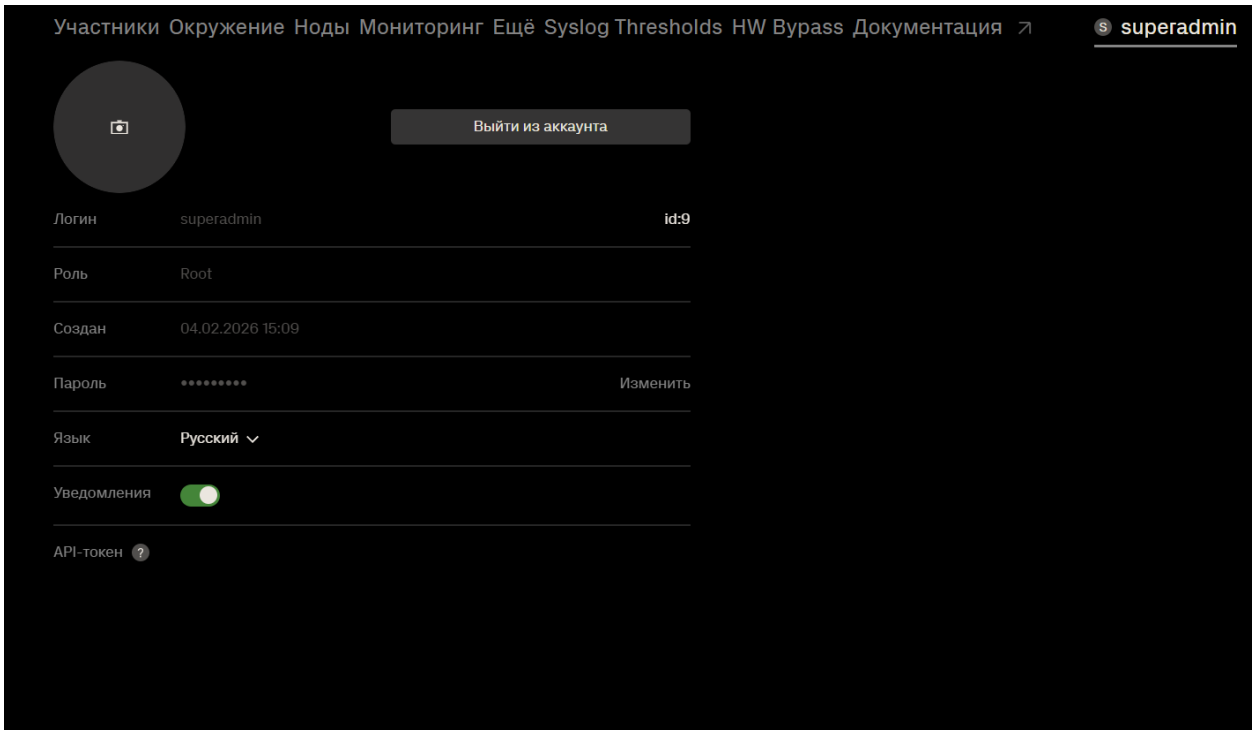
После успешной авторизации откроется панель управления Servicepipe Spider. В левой части окна расположена панель навигации по разделам и объектам выбранного продукта. В центральной части окна отображается рабочая область выбранного раздела.

Если логин или пароль указаны неверно, система не выполнит вход и отобразит сообщение об ошибке авторизации. В этом случае следует проверить введённые данные и повторить вход.

2.2 Завершение работы

Для завершения работы в веб-интерфейсе Servicepipe Spider следует открыть раздел **Настройки** на панели навигации. В разделе **Настройки** следует нажать на логин текущего пользователя в правом верхнем углу окна.

После нажатия откроется личный кабинет пользователя.

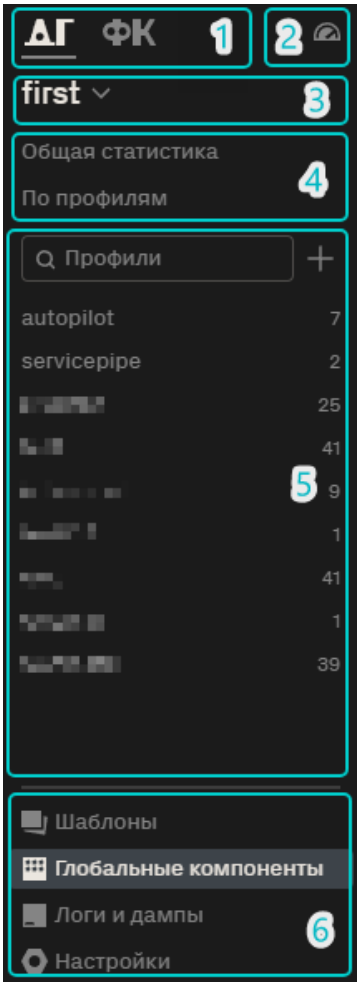


В личном кабинете следует нажать кнопку **Выйти из аккаунта.** После нажатия кнопки сеанс работы пользователя завершается. Система возвращает пользователя на страницу авторизации.

3 Управление объектами мониторинга

3.1 Панель быстрого доступа

Панель быстрого доступа расположена в левой части окна веб-интерфейса Servicepipe Spider и используется для перехода между основными разделами, выбора рабочей области и просмотра доступных объектов.



Панель быстрого доступа включает следующие функциональные блоки:

- Переключение между продуктами — позволяет выбрать продукт, с которым пользователь работает в текущий момент. В зависимости от состава установленного программного обеспечения и прав пользователя могут быть доступны продукты DosGate, FlowCollector и RLog.

- Мониторинг — предоставляет переход к сведениям о текущем состоянии выбранного узла и показателям его работы.
- Выбор арены — используется для выбора рабочей арены, в рамках которой выполняется просмотр данных и настройка объектов.
- Статистика — предоставляет доступ к общей статистике и статистическим данным по профилям.
- Список профилей — отображает перечень профилей, доступных в выбранной арене. В этом блоке пользователь может выбрать профиль для просмотра или дальнейшей настройки.
- Панель управления — содержит дополнительные разделы для работы с объектами и настройками системы:
  - Шаблоны — раздел для работы с шаблонами конфигурации
  - Глобальные компоненты — раздел для работы с общими компонентами системы
  - Логи и дампы — раздел для просмотра журналов и дампов
  - Настройки — раздел для настройки параметров системы и работы с учётной записью пользователя

Каждый объект настраивается индивидуально с использованием отдельного конфигурационного файла.

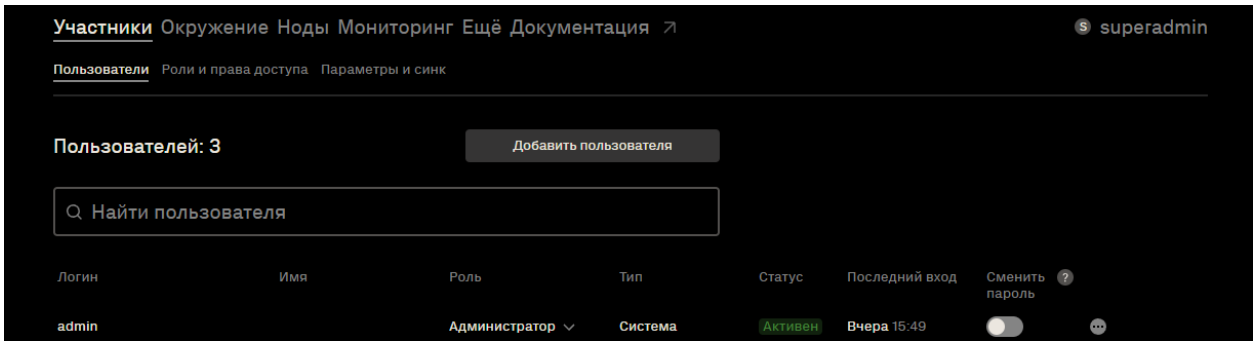
4 Настройки

Раздел предназначен для управления пользователями, ролями доступа, параметрами окружения, интеграциями, узлами системы, мониторингом и дополнительными служебными функциями.

4.1 Участники

4.1.1 Пользователи

Раздел Пользователи предназначен для управления учётными записями пользователей системы.



Чтобы найти пользователя, введите логин, имя или другой параметр учётной записи в строку **Найти пользователя**.

Чтобы создать пользователя:

- Откройте раздел **Пользователи.**
- Нажмите **Добавить пользователя**.
- В открывшейся форме выберите роль пользователя.
- Укажите тип учётной записи.
- Введите логин и пароль.
- При необходимости включите параметр **Сменить пароль** при логине. Параметр включает обязательную смену пароля при следующем входе пользователя в систему.

- Нажмите **Создать.**

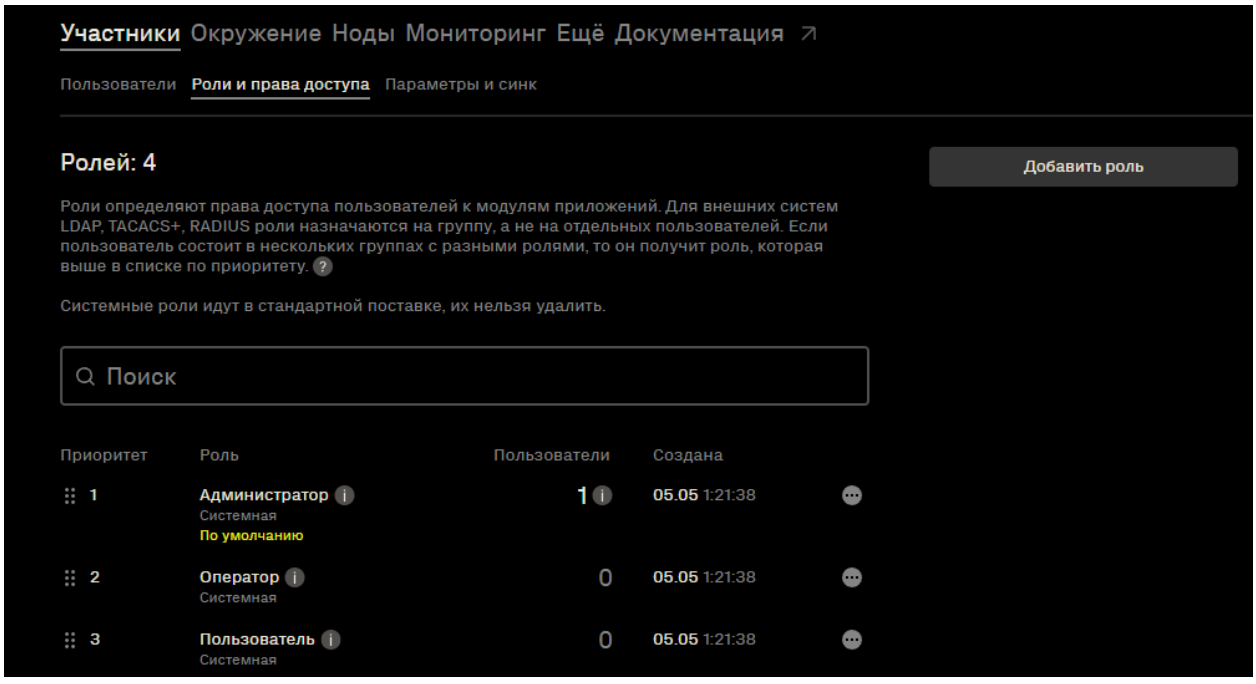
После создания пользователь появится в общем списке. Для каждой учётной записи отображаются роль, тип учётной записи, статус и дата последнего входа.

Чтобы принудительно сменить пароль пользователя, включите параметр **Сменить пароль**. После включения параметра активная сессия пользователя завершится. При следующем входе в систему пользователь должен будет задать новый пароль.

Чтобы заблокировать или удалить пользователя, нажмите на значок с тремя точками напротив нужной учётной записи и выберите соответствующее действие.

4.1.2 Роли и права доступа

Раздел и права доступа предназначен для управления ролями пользователей и настройки прав доступа к функциям системы.



Роль определяет набор разделов и функций, доступных пользователю. Приоритет роли зависит от её положения в списке: чем выше расположена роль, тем выше её приоритет.

Системные роли входят в стандартную поставку и не могут быть удалены. Чтобы найти роль, введите название роли или другой параметр в строку **Поиск**. Чтобы изменить приоритет роли, переместите её выше или ниже в списке ролей.

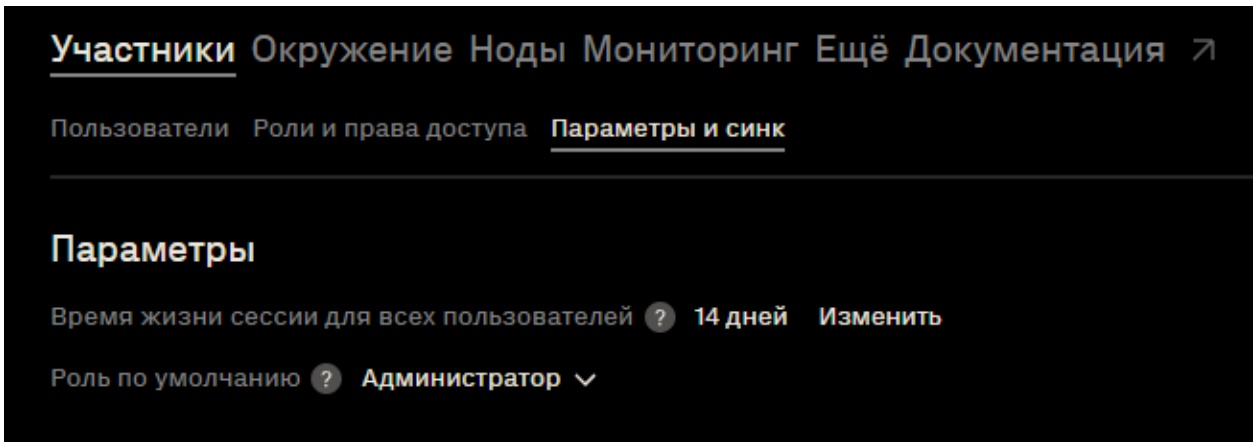
Чтобы создать роль:

- Откройте раздел **Роли и права доступа**.
- Нажмите **Добавить роль**.
- В открывшейся форме укажите название роли.
- Настройте права доступа к разделам системы.
- При необходимости задайте уровень доступа для отдельных прав: ***Чтение*** или ***Запись.***
- При необходимости ограничьте область действия права. В зависимости от раздела доступ может распространяться на все объекты соответствующего типа или только на выбранные элементы, например профили, префикс-сеты или защищаемые объекты.
- Нажмите **Применить.**

Уровень ***Чтение*** предоставляет доступ к просмотру данных. Уровень ***Запись*** предоставляет доступ к изменению данных и выполнению действий в соответствующем разделе. Чтобы отредактировать или дублировать роль, нажмите на значок с тремя точками напротив нужной роли и выберите соответствующее действие.

4.1.3 Параметры и синк

Раздел предназначен для настройки общих параметров пользовательских сессий и выбора роли по умолчанию.



- Время жизни сессии для всех пользователей — период, после которого пользователи должны повторно войти в приложение. Чтобы изменить значение, нажмите **Изменить** и задайте новый период

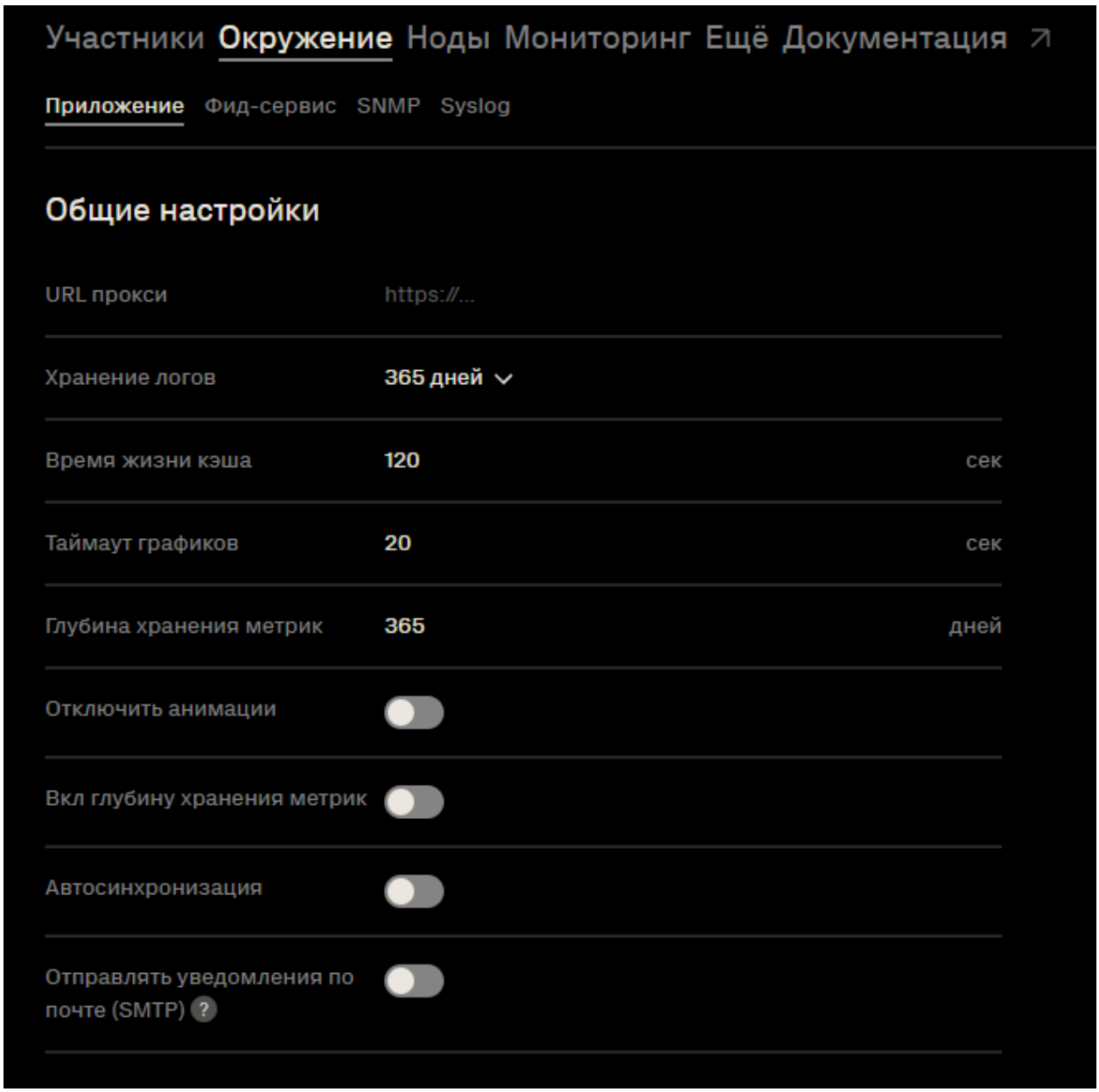
- Роль по умолчанию — роль, которая назначается новым пользователям после синхронизации или первого входа в приложение. Чтобы задать роль по умолчанию, выберите её из раскрывающегося списка доступных ролей

4.2 Окружение

Раздел содержит общие настройки системы, включая параметры API, прокси-сервера, кэширования, хранения журналов, интеграции с внешними сервисами и работы с метриками.

4.2.1 Приложение

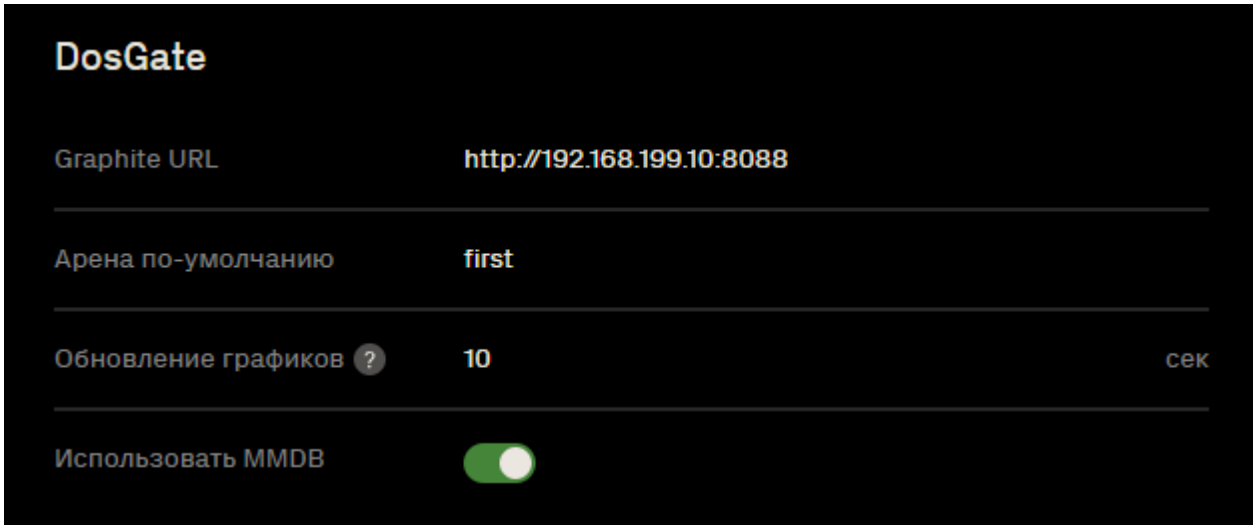
Раздел предназначен для настройки общих параметров веб-интерфейса и параметров интеграции с подключёнными компонентами.



В разделе доступны следующие параметры:

- URL прокси — адрес прокси-сервера, используемый для доступа к фид-сервису Servicepipe
- Хранение логов — срок хранения журналов системы
- Время жизни кэша — период хранения данных о профилях и их содержимом в кэше. Увеличение значения снижает частоту обновления кэша и может повысить производительность в крупных инсталляциях
- Таймаут графиков — время ожидания ответа при загрузке графиков

- Глубина хранения метрик — период, за который в системе сохраняются метрики
- Отключить анимации — параметр, отключающий анимационные эффекты веб-интерфейса. Его рекомендуется использовать при подключении к веб-интерфейсу через RDP
- Включить глубину хранения метрик — параметр, включающий применение заданной глубины хранения метрик
- Автосинхронизация — параметр, обеспечивающий автоматическое приведение конфигурации узлов в соответствие с мастер-сервером при добавлении новых серверов или обнаружении расхождений в политиках
- Отправлять уведомления по почте (SMTP) — параметр, включающий отправку уведомлений по электронной почте при настроенных параметрах SMTP



- Graphite URL — адрес сервера Graphite, используемого для сбора и отображения метрик
- Арена по умолчанию — арена, используемая в системе по умолчанию
- Обновление графиков — интервал обновления графиков в секундах

- Использовать MMDB — параметр, включающий использование базы MMDB для работы с географическими данными

Чтобы изменить параметры приложения:

- Откройте раздел Окружение.
- Перейдите в блок Приложение.
- Измените нужные значения параметров.
- Сохраните изменения.

4.2.2 Фид-сервис

Раздел предназначен для настройки подключения к серверу фидов и параметров обновления данных.

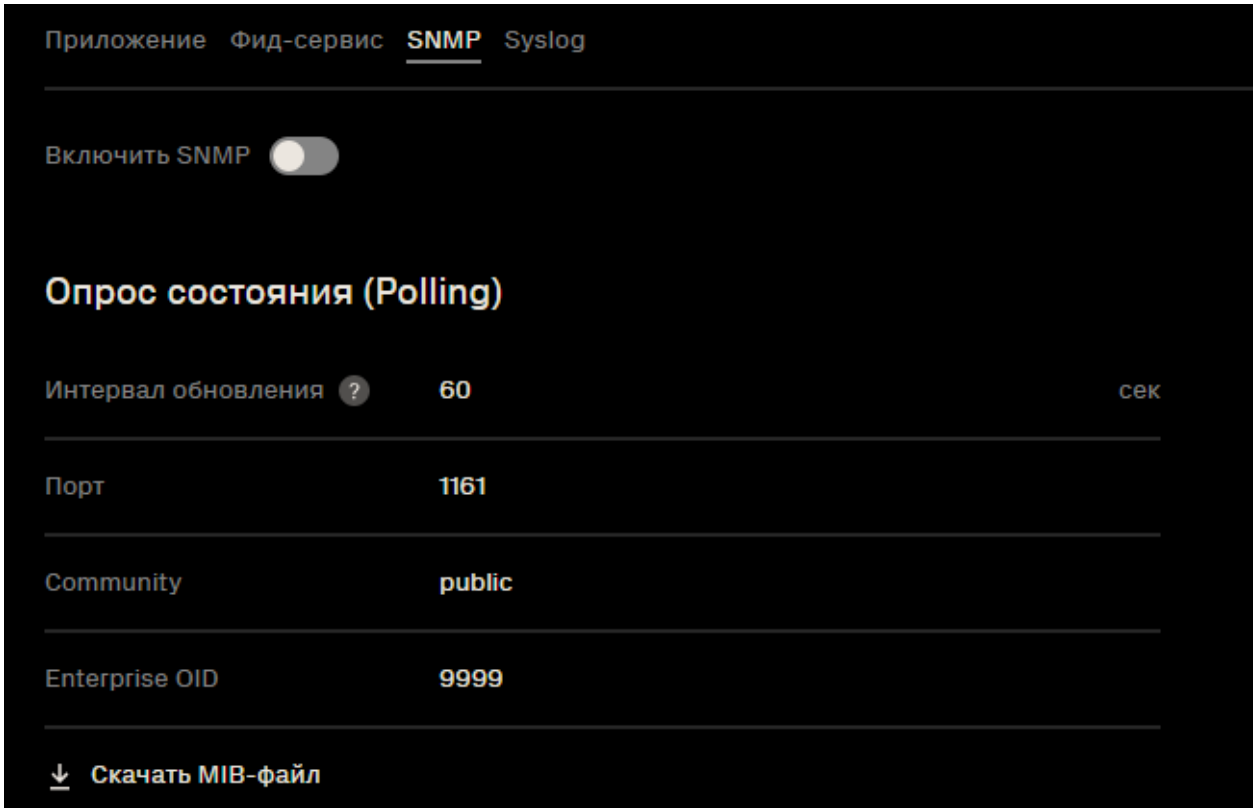


- Мастер-сервер — адрес сервера, с которого приложение получает обновления фидов
- Токен — ключ аутентификации, предоставленный поставщиком
- Интервал обновления — периодичность обновления данных фид-сервиса

Чтобы настроить подключение к фид-сервису, укажите адрес мастер-сервера, токен и интервал обновления, затем сохраните изменения.

4.2.3 SNMP

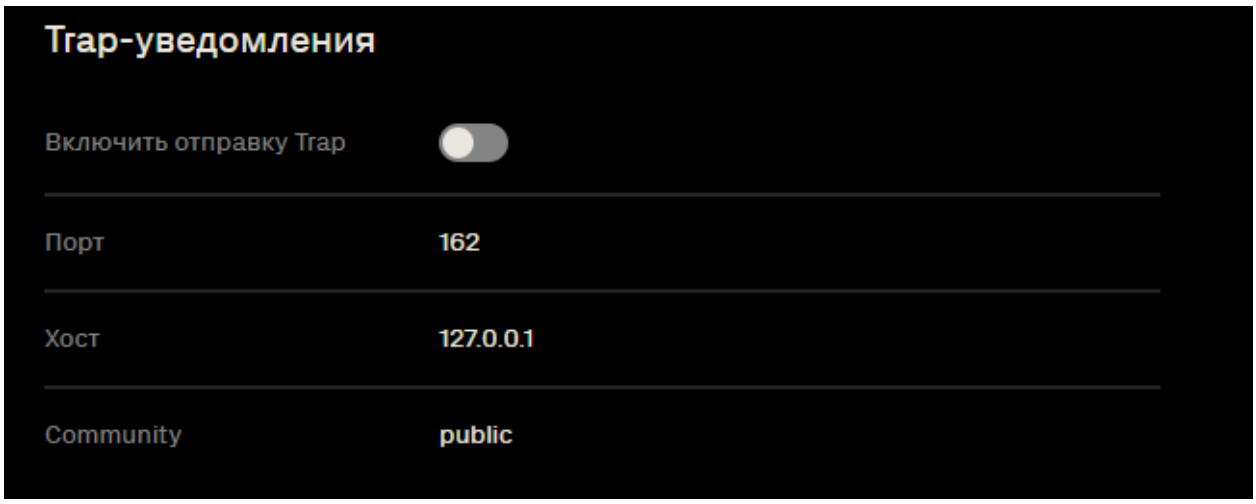
Раздел SNMP предназначен для настройки SNMP-опроса состояния системы и отправки SNMP Trap-уведомлений во внешнюю систему мониторинга.



Блок Опрос состояния содержит параметры, по которым внешняя система мониторинга получает данные о состоянии приложения.

- Интервал обновления — периодичность обновления SNMP-данных
- Порт — порт, на котором доступен SNMP-опрос
- Community — строка сообщества SNMP, используемая для доступа к данным мониторинга
- Enterprise OID — идентификатор предприятия, используемый в структуре SNMP-данных

При необходимости скачайте MIB-файл по ссылке Скачать MIB-файл. Файл содержит описание доступных SNMP-объектов и используется внешними системами мониторинга для интерпретации полученных данных.



Блок Trap-уведомления предназначен для настройки отправки SNMP Trap-уведомлений во внешнюю систему мониторинга.

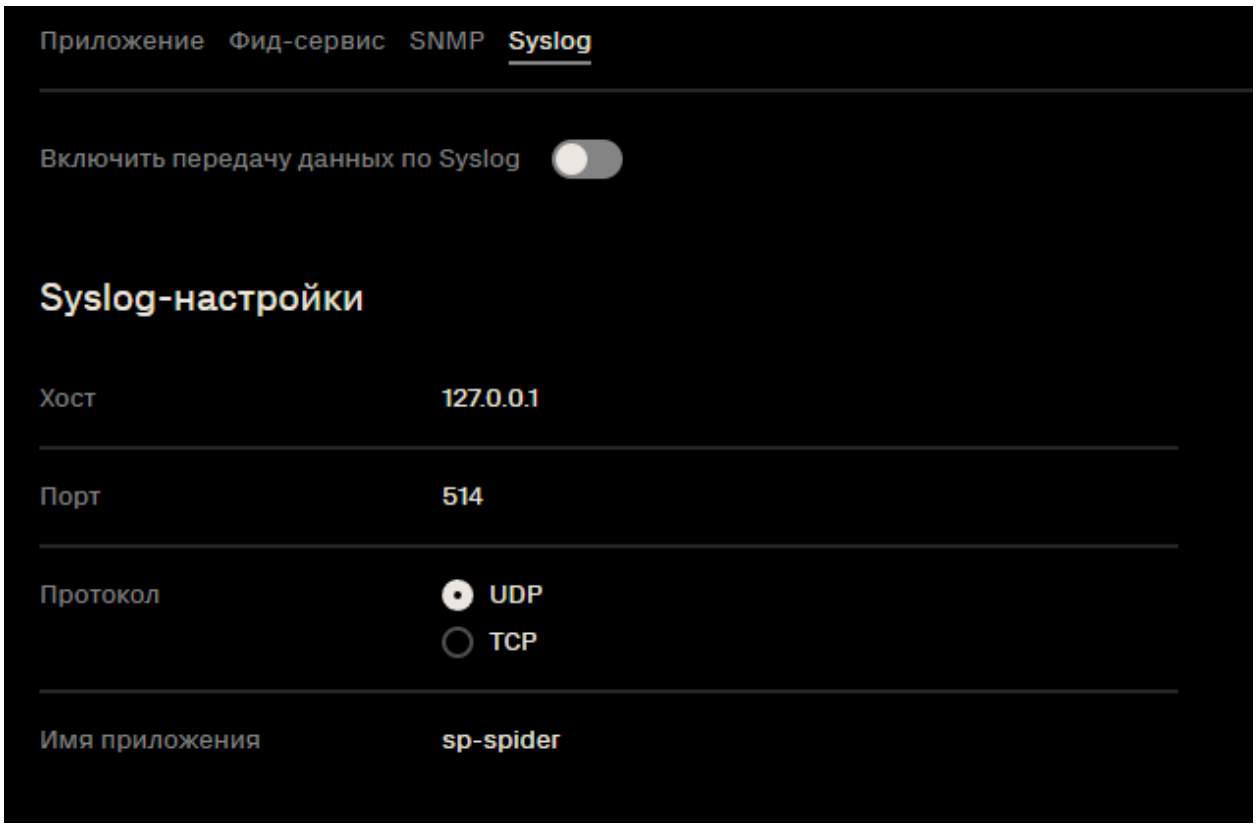
- Порт — порт, на который отправляются Trap-уведомления
- Хост — адрес сервера мониторинга, принимающего Trap-уведомления
- Community — строка сообщества SNMP, используемая при отправке уведомлений

Чтобы настроить SNMP:

- Откройте раздел **Окружение.**
- Перейдите в блок **SNMP**.
- Заполните параметры блока **Опрос состояния**.
- При необходимости скачайте MIB-файл.
- Заполните параметры блока Trap-уведомления.
- Сохраните изменения.

4.2.4 Syslog

Раздел предназначен для настройки передачи данных во внешний Syslog-сервер.

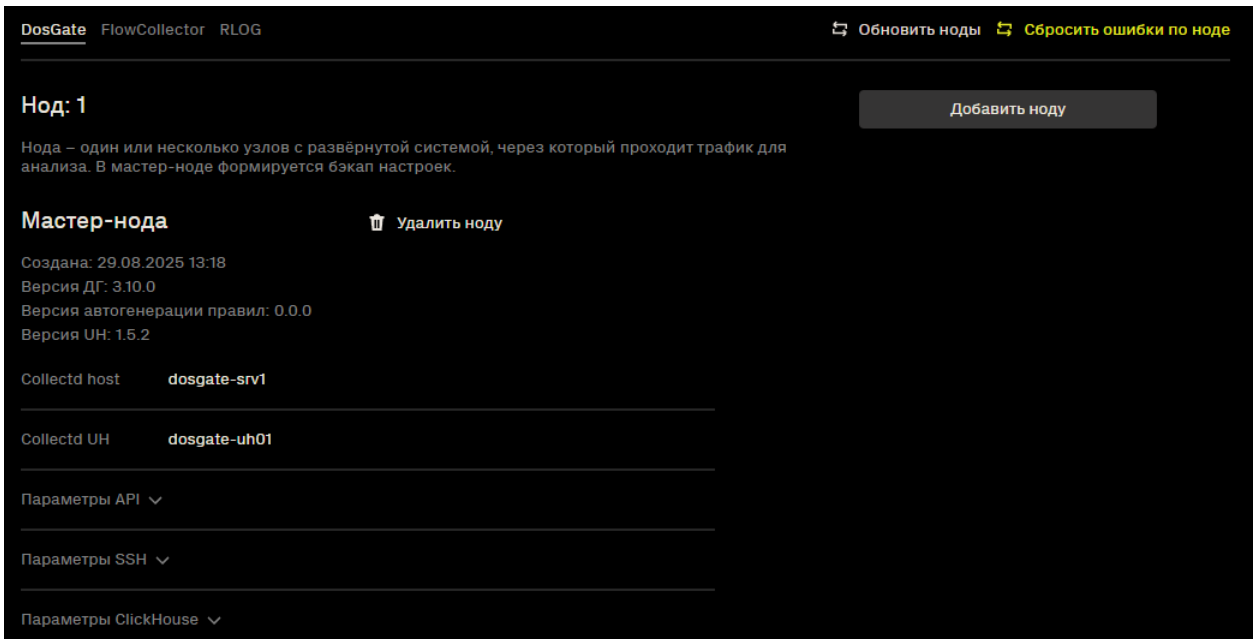


- Хост — адрес Syslog-сервера, принимающего данные
- Порт — порт Syslog-сервера
- Протокол — транспортный протокол, используемый для передачи данных
- Имя приложения — идентификатор приложения, который передаётся в Syslog-сообщениях и используется для фильтрации и поиска событий на стороне Syslog-сервера

Чтобы настроить отправку данных в Syslog, укажите хост, порт, протокол и имя приложения, затем сохраните изменения.

4.3 Ноды

Раздел Ноды предназначен для управления узлами системы. В разделе отображается список доступных нод, их статус и параметры.



В разделе отображаются следующие основные элементы:

- Мастер-нода — узел системы, на котором формируется резервная копия настроек
- Collectd host — имя хоста, с которого собираются системные и сервисные метрики
- Collectd UH — имя хоста, с которого собираются системные и сервисные метрики для сессионной защиты
- Параметры API — настройки доступа к API ноды
- Параметры SSH — настройки SSH-доступа к ноде
- Параметры ClickHouse — параметры подключения к базе данных ClickHouse, используемой для хранения и обработки аналитических данных

В разделе доступны следующие действия:

- Обновить ноды — обновляет данные о текущих нодах
- Синхронизировать — выполняет принудительную синхронизацию конфигурации нод с мастер-нодой

4.3.1 Добавление новой ноды

Чтобы добавить новую ноду:

- Откройте раздел **Ноды**.
- Нажмите **Добавить ноду**.
- Выберите операционную систему узла.
- В поле **Модуль** выберите компонент, который должен работать на ноде.
- В поле **Collectd host** укажите имя хоста.
- В поле **Collectd UH** укажите имя хоста для сессионной защиты.
- При необходимости настройте параметр HW Bypass. Параметр используется для управления сетевыми картами с поддержкой аппаратного обхода и позволяет включать или отключать прямую передачу трафика между портами на физическом уровне.
- Откройте блок **Подключение**.
- Выберите способ подключения: API или SSH.
- Заполните параметры выбранного способа подключения.
- Нажмите **Применить**, чтобы сохранить параметры подключения.
- Нажмите **Добавить ноду**.

После добавления нода появится в общем списке.

4.4 Мониторинг

Раздел Мониторинг предназначен для настройки контроля состояния ресурсов, используемых компонентами платформы.

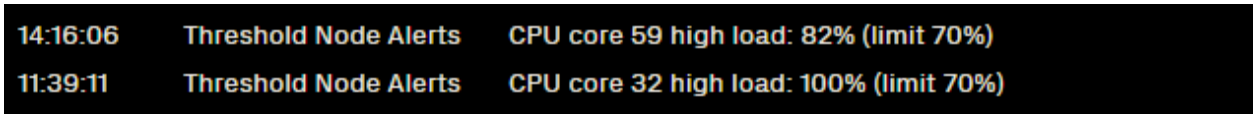


В верхней части раздела расположен переключатель **Включить** уведомления. Он включает отправку предупреждений при превышении заданных порогов нагрузки.

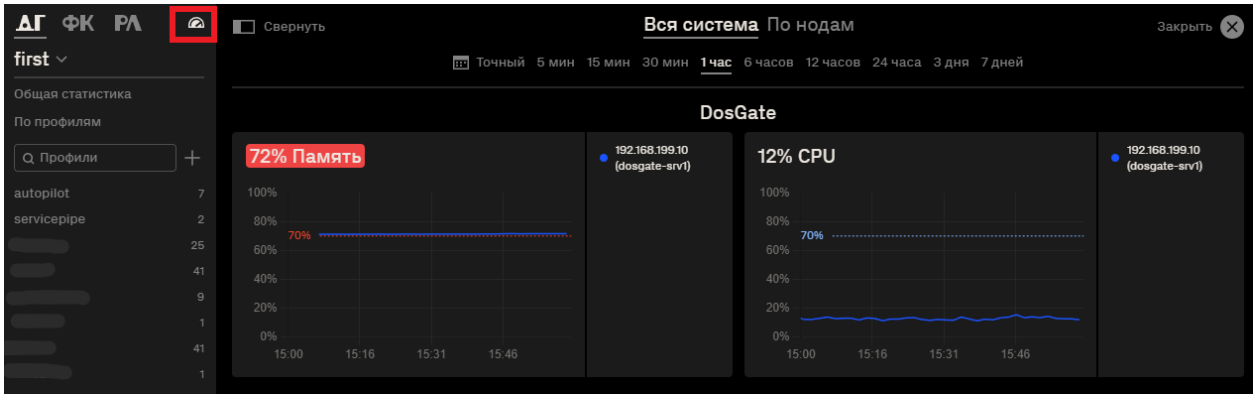
Чтобы включить уведомления мониторинга:

- Откройте раздел **Мониторинг.**
- Включите переключатель **Включить уведомления**.
- Задайте необходимые пороговые значения.
- Сохраните изменения.

Уведомления мониторинга отображаются в общем списке событий раздела **Логи.**

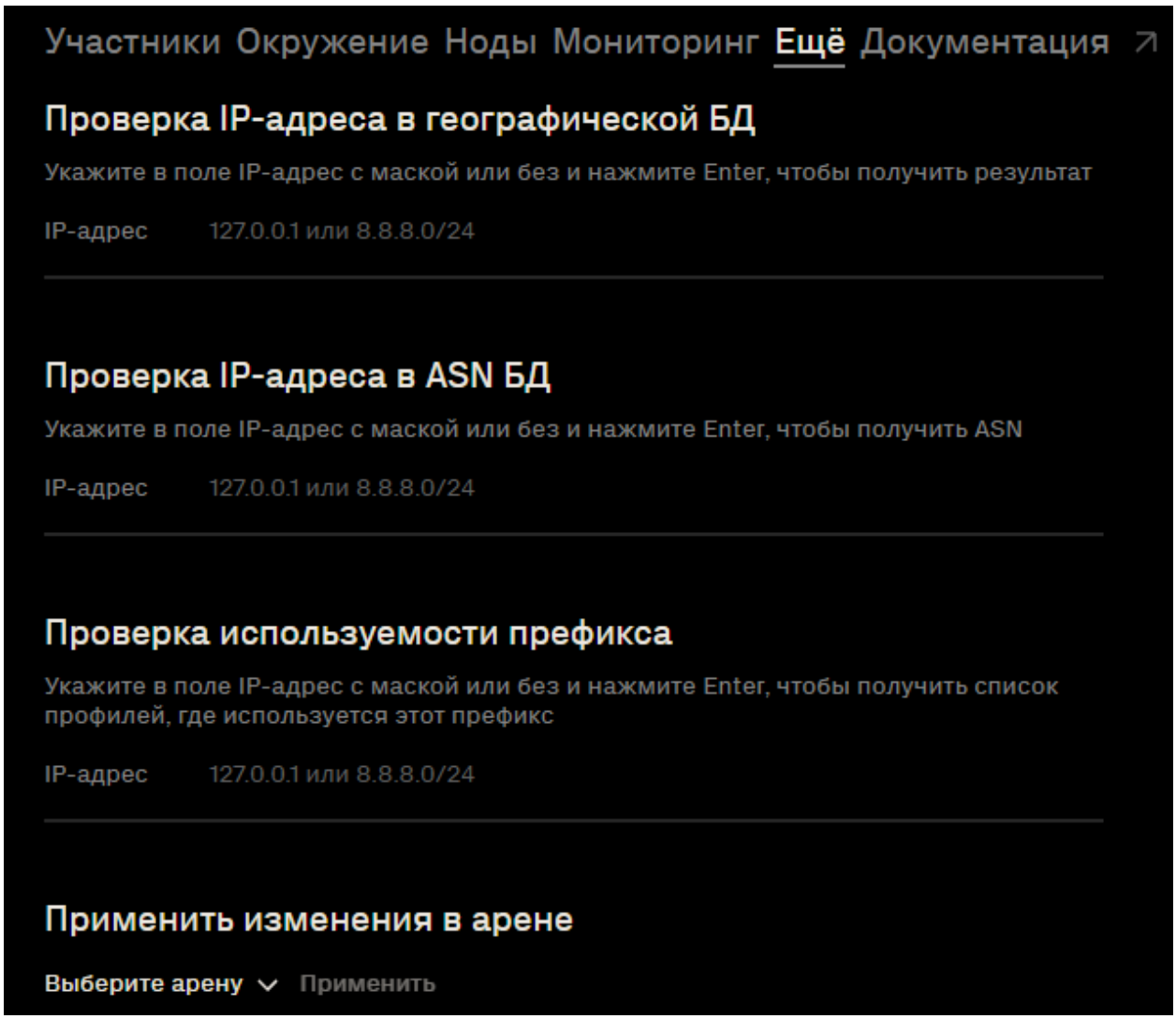


Для быстрого перехода к данным мониторинга в панели быстрого доступа используется иконка мониторинга. Показатели, превышающие пороговые значения, отображаются красным цветом.



4.5 Ещё

Раздел содержит дополнительные инструменты для проверки IP-адресов, анализа используемости префиксов и применения изменений в выбранной арене.



В разделе доступны следующие функции:

- Проверка IP-адреса в географической БД — определяет географическую принадлежность IP-адреса
- Проверка IP-адреса в ASN БД — определяет ASN для указанного IP-адреса
- Проверка используемости префикса — показывает список профилей, в которых используется указанный IP-адрес или префикс
- Применение изменений в арене — позволяет выбрать арену из раскрывающегося списка и применить изменения с помощью кнопки Применить

Чтобы выполнить проверку, откройте нужный инструмент, укажите IP-адрес или префикс и запустите проверку. Результат отобразится в рабочей области раздела.

4.6 Syslog Thresholds

Раздел предназначен для настройки порогов отправки уведомлений в Syslog.

Переключатель **Уведомлять в Syslog** включает отправку уведомлений при превышении заданных порогов.

Пороги задаются отдельно для разных типов трафика:

- ACCEPT — трафик, для которого применено действие ACCEPT
- REPLY — ответный трафик
- ERROR — трафик, обработанный с ошибкой
- DROP — трафик, для которого применено действие DROP
- PASS — трафик, для которого применено действие PASS
- PASS UH — трафик, для которого применено действие UH
- Для каждого типа трафика доступны два параметра:

Параметр	**Описание**
BPS	Порог по скорости трафика, бит/с
PPS	Порог по количеству пакетов, пакетов/с

Если значение порога равно 0, то уведомления по этому параметру не отправляются.

Чтобы настроить пороги отправки уведомлений в Syslog:

- Откройте раздел **Syslog Thresholds**.
- Включите переключатель **Уведомлять в Syslog**.
- Выберите тип трафика.

- Укажите значения BPS и PPS.
- При необходимости повторите настройку для других типов трафика.
- Сохраните изменения.

4.7 HW Bypass

Раздел предназначен для управления аппаратным обходом на сетевых картах Silicom.

В верхней части раздела отображается блок **Ноды DosGate**. В нём выбираются ноды, для которых необходимо получить состояние или изменить режим HW Bypass.

Раздел содержит три блока настроек:

- Silicom NIC HW Bypass — текущее состояние HW Bypass для всех интерфейсов
- Power Up Bypass — состояние HW Bypass при включении питания
- Power Off Bypass — состояние HW Bypass при отключении питания

В каждом блоке доступны следующие действия:

Действие	**Описание**
Получить состояние	Запрашивает текущее состояние HW Bypass
Включить	Включает HW Bypass для выбранного режима
Выключить	Выключает HW Bypass для выбранного режима

Чтобы получить состояние или изменить режим HW Bypass:

- Откройте раздел **HW Bypass**.
- В блоке **Ноды DosGate** выберите одну или несколько нод.

- Выберите нужный блок настроек: Silicom NIC HW Bypass, Power Up Bypass или Power Off Bypass.
- Нажмите **Получить состояние**, чтобы запросить текущее состояние HW Bypass.
- При необходимости нажмите **Включить** или **Выключить,** чтобы изменить режим HW Bypass для выбранного блока.

5 DosGate

5.1Статистика

Раздел предназначен для просмотра графиков сетевого трафика и показателей сессионной защиты. В разделе доступны общая статистика по аренам и детализированная статистика по отдельным профилям.

5.1.1 Общая статистика

Блок **Общая статистика** отображает графики трафика для всех арен. Для каждой арены данные отображаются в виде двух графиков:

- – пропускная способность в битах в секунду (bits/s)
- – количество пакетов в секунду (packets/s)

Чтобы просмотреть общую статистику, откройте раздел **Статистика** и выберите блок **Общая статистика**. После открытия блока система отобразит графики трафика по доступным аренам.

Чтобы просмотреть статистику по сессиям, перейдите на вкладку «**Сессии**». На вкладке отображаются данные по сессиям, которые обрабатываются Сессионной защитой DosGate. Статистика отображается только по тем протоколам, которые выбраны в настройках Сессионной защиты.

По умолчанию на графиках общей статистики отображаются атрибуты трафика, приведённые в таблице.

Атрибут	**Описание**
drop	Пакеты, отброшенные DosGate в соответствии с правилами
error	Пакеты, не прошедшие проверку согласно IP RFC и отброшенные системой
pass	Трафик, переданный в пользовательское пространство операционной системы по действию PASS

pass_uh	Трафик, отправленный в сессионную защиту для дополнительной проверки
reply	Ответный трафик от DosGate в сторону отправителя в рамках механизма TCP-аутентификации
transmit	Трафик, успешно прошедший фильтрацию и отправленный далее

Чтобы построить график по отдельному атрибуту, выберите нужный атрибут на графике. Система сформирует отдельный график, отображающий динамику соответствующего типа трафика.

В правой части интерфейса расположен блок **Период.** Он используется для выбора временного интервала, за который строятся графики трафика.

Чтобы изменить период отображения статистики:

- Откройте раздел **Статистика**
- В правой части интерфейса откройте блок **Период**
- Выберите готовый интервал или пункт **Точный**
- При выборе пункта **Точный** укажите диапазон дат и времени вручную

Пункт **Точный** позволяет задать пользовательский диапазон дат и времени или выбрать интервал от нескольких месяцев до одной минуты.

5.1.2 Статистика по прифилям

Блок предназначен для просмотра детализированной статистики по отдельным профилям.

Чтобы просмотреть статистику по профилю:

- Откройте раздел **Статистика**
- Выберите пункт **По профилям**
- В раскрывающемся списке выберите нужный профиль

– При необходимости задайте период отображения статистики в блоке **Период.**

После выбора профиля система отображает графики, относящиеся к выбранному профилю.

График	**Описание**
Общий трафик по профилю	Отображает общий трафик выбранного профиля в форматах packets/s и bits/s
Трафик по правилу STATS	Отображает трафик по правилу STATS в форматах packets/s и bits/s. График формируется при наличии трафика, который удовлетворяет условию правила STATS

Графики формируются только при наличии соответствующего трафика в пределах заданных условий. Если в правиле указано действие STATS, но трафик, подпадающий под это правило, отсутствует, график не отображается.

На графиках статистики по профилям отображаются атрибуты трафика, приведённые в таблице.

Атрибут	**Описание**
Accept	Принятые пакеты, успешно прошедшие через систему
1d ago	Скорость трафика один день назад
7d ago	Скорость трафика семь дней назад
Drop	Пакеты, отброшенные DosGate в соответствии с правилами
Error	Ошибки при передаче или обработке пакетов
Pass	Трафик, переданный в пользовательское пространство операционной системы по действию PASS
Pass_uh	Трафик, отправленный в сессионную защиту для дополнительной проверки
Reply	Ответный трафик от DosGate в сторону отправителя в рамках механизма TCP-аутентификации

5.2 Профиль защиты

5.2.1 Создание профиля

Для создания нового профиля выполните следующие действия:

- На главной странице откройте раздел **Профили**.
- Нажмите кнопку **Плюс** рядом со списком профилей.
- В открывшейся форме заполните параметры профиля.
- Нажмите **Создать**.

Параметр	**Описание**
Название	Уникальное имя профиля. Рекомендуется использовать имя, которое отражает сегмент инфраструктуры и назначение сервиса, например zapadniy-filial-web или dmz-dns.
Описание	Краткое описание профиля. Используется для пояснения назначения профиля и особенностей его применения.
Пресет	Шаблон для быстрого создания профиля. Параметр используется при наличии доступных пресетов. Выбор пресета не является обязательным.

После создания профиля система откроет страницу созданного профиля. На странице доступны разделы для настройки правил, чейнов, роутера, меток, префикс-сетов и сессионной защиты.

5.2.2 Изменение профиля

Для изменения названия или описания профиля выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на название нужного профиля.
- В контекстном меню выберите **Изменить**.
- В открывшемся окне измените название или описание профиля.

- Сохраните изменения.

После сохранения новые параметры будут отображаться в списке профилей и на странице профиля.

5.2.3 Экспорт профиля

Экспорт профиля используется для создания локального пресета или переноса настроек профиля в формате JSON.

Для экспорта профиля выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на нужный профиль.
- В контекстном меню выберите **Экспорт.**
- Дождитесь загрузки JSON-файла.

После выполнения действия система автоматически сформирует и загрузит файл профиля в формате JSON.

5.2.4 Очистка профиля

Очистка профиля удаляет все правила профиля. При этом остальные атрибуты профиля, включая чейны, роутер, метки и префикс-сеты, остаются без изменений.

Для очистки профиля выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на нужный профиль.
- В контекстном меню выберите **Очистить**.
- Подтвердите действие, если система запросит подтверждение.

После выполнения действия все правила будут удалены из профиля. Остальные параметры профиля сохранятся. Перед очисткой профиля рекомендуется проверить, что удаление правил не нарушит текущую схему обработки трафика.

5.2.5 Удаление профиля

Удаление профиля полностью удаляет профиль из системы.

Для удаления профиля выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на название нужного профиля.
- В контекстном меню выберите **Удалить**.
- Подтвердите удаление, если система запросит подтверждение.

После подтверждения профиль будет удалён из системы. Удаление профиля является необратимым действием. Перед удалением рекомендуется убедиться, что профиль не используется для обработки актуального трафика.

5.2.6 История версий

История версий содержит сохранённые состояния профиля. В версии фиксируются изменения правил, чейнов и роутера. Новая версия создаётся автоматически при применении изменений.

Для просмотра истории версий выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на нужный профиль.
- В контекстном меню выберите **История версий**.
- Просмотрите список изменений в панели **История версий** в правой части интерфейса.

Каждая запись истории содержит имя пользователя, выполнившего изменение, и время сохранения версии. Записи отображаются в хронологическом порядке, начиная с самой последней.

При необходимости к записи можно добавить комментарий. Для отображения только собственных изменений включите **Только мои** в нижней части панели.

5.2.7 Автообновление профиля

Если профиль создан на основе пресета, он может автоматически получать обновления из этого пресета.

Для управления автообновлением выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на профиль, созданный на основе пресета.
- В контекстном меню включите или отключите параметр **Автообновление**.

При отключении автообновления связь профиля с пресетом сохраняется, но изменения, поступающие в пресет, не применяются к профилю автоматически.

5.2.8 Переход к компоненту

Переход к компоненту открывает окно редактирования пресета, на основе которого был создан профиль.

Для перехода к компоненту выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на профиль, созданный на основе пресета.
- В контекстном меню выберите **Перейти к компоненту**.
- В открывшемся окне просмотрите или измените параметры соответствующего пресета.

5.2.9 Разрыв связи с пресетом

Разрыв связи используется, когда требуется самостоятельно изменить правила профиля, созданного на основе пресета.

Пока профиль связан с пресетом, редактирование его правил недоступно. Настройки наследуются из пресета и обновляются автоматически в соответствии с параметрами автообновления.

Для разрыва связи выполните следующие действия:

- В общем списке профилей нажмите правой кнопкой мыши на профиль, связанный с пресетом.
- В контекстном меню выберите **Разорвать связь**.
- Подтвердите действие, если система запросит подтверждение.

После разрыва связи профиль становится автономным. Изменения в пресете больше не распространяются на этот профиль, а правила профиля становятся доступными для редактирования. Перед разрывом связи рекомендуется оценить, нужно ли профилю получать дальнейшие обновления пресета.

5.3 Правила

5.3.1 Созданиеи редактирование правил

Правила могут быть заданы одним из двух способов: с использованием пресета или вручную.

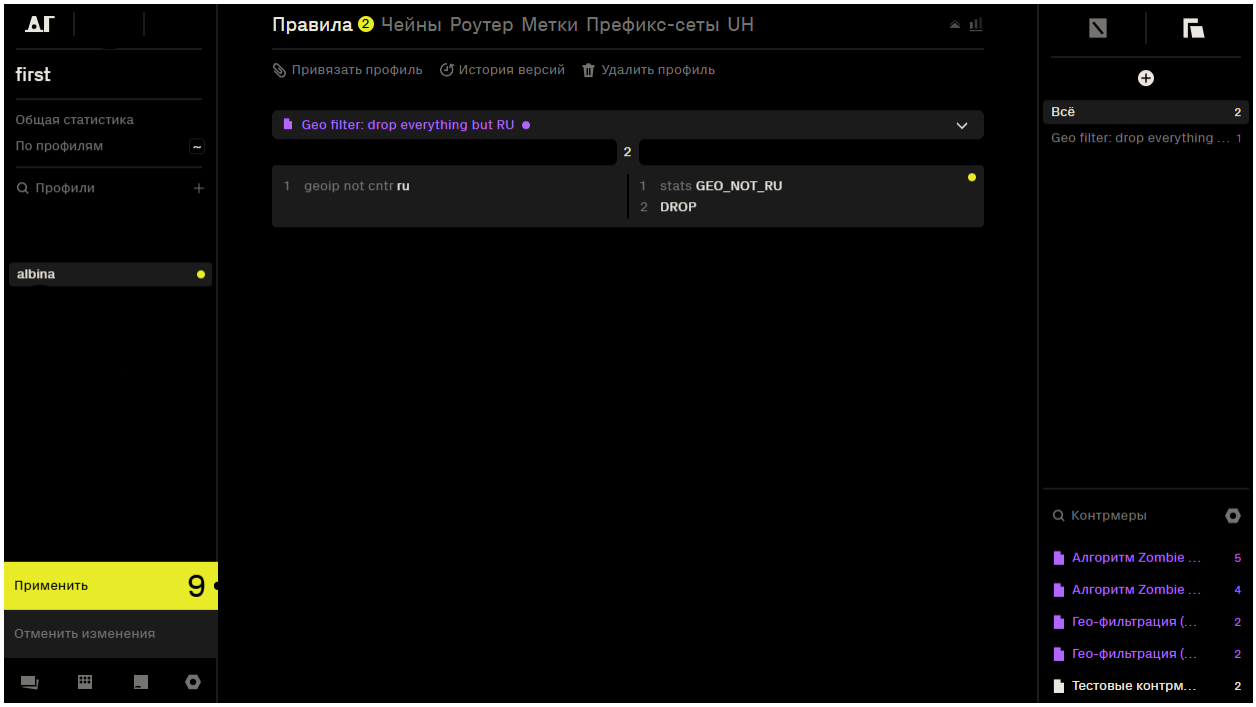
Создание правила через пресет:

- Перейдите в необходимый профиль.
- Выберите опцию **Создать через пресет**.
- В правом нижнем углу отобразятся доступные контрмеры:

Контрмеры отображаются фиолетовым цветом, если подключена база вредоносных сигнатур. Контрмеры отображаются белым цветом, если они были созданы вручную в разделе **Пресеты**.

- Выберите необходимую контрмеру и перетянуть в поле **Правила**.

– Чтобы применить изменения, нажмите **Применить.**



Создание правила вручную:

– Перейдите в необходимый профиль.

– Выберите опцию **Вручную**.

– В DosGate правила создаются путём комбинирования совпадений и действий.

Совпадения определяют условия, при которых правило срабатывает. Действия применяются к трафику, если условия совпадений выполнены. Такой процесс позволяет гибко настраивать фильтрацию и управление трафиком.

5.3.2 Пример №1

Назначение правила: Ограничения доступа на основе географического происхождения IP-адреса. Весь трафик, не относящийся к России, будет отброшен.

1. В интерфейсе профиля нажмите кнопку Вручную. Это откроет форму для настройки совпадений.

2. В поле **Совпадение** выберите параметр geoip -> country -> RU.

3. Активируйте радиокнопку NOT, чтобы применить логическое отрицание. Условие будет выполняться для всех IP-адресов, не принадлежащих России.

4. В поле **Сверяем** установите src, правило будет охватывать весь трафик, источник которого находится за пределами России. Нажмите кнопку Добавить.

5. В поле Действие выберите STATS — это позволяет записывать все срабатывания правила в отдельный счётчик. Введите имя счётчика: GEO_NOT_RU, чтобы в дальнейшем можно было анализировать объём и частоту трафика, не относящегося к России. Нажмите кнопку **Добавить**.

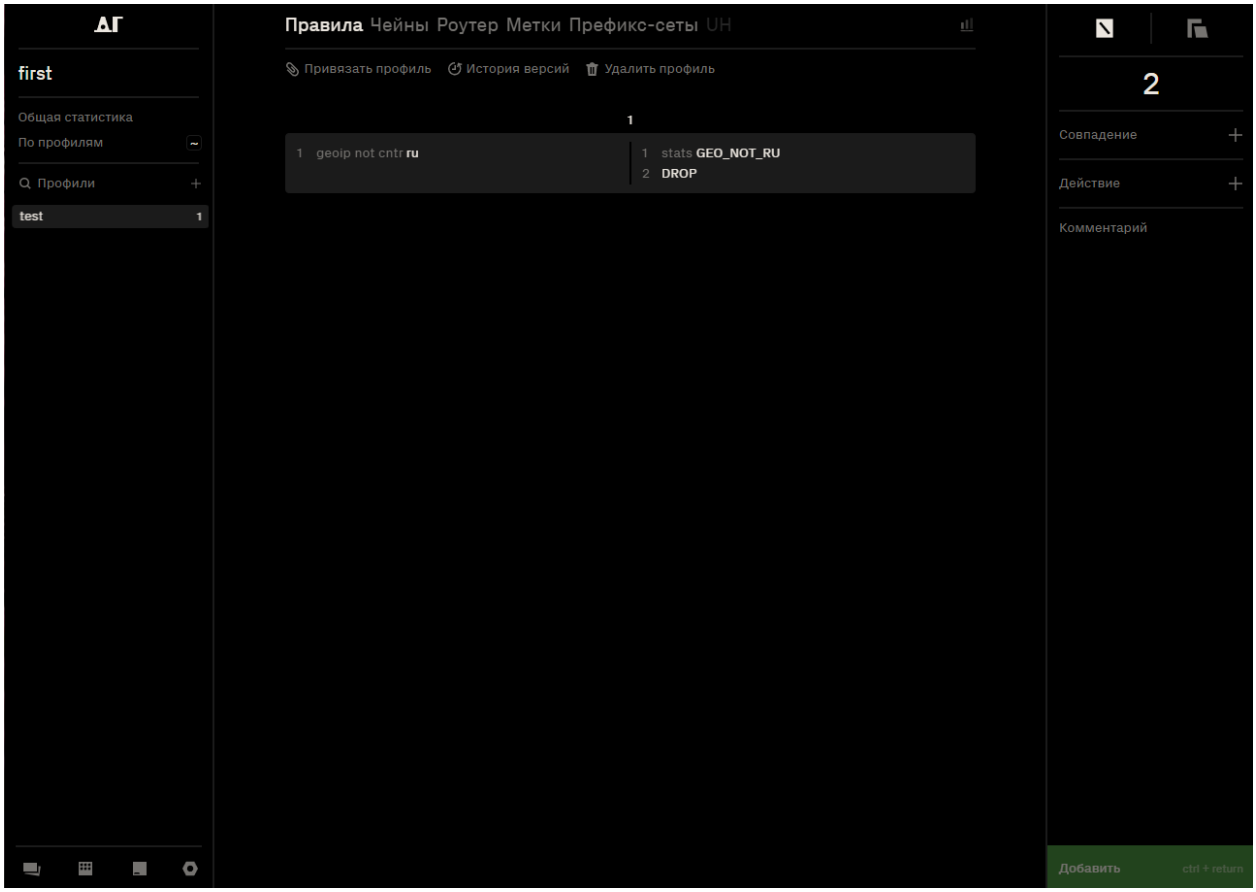
6. В поле Действие выберите DROP — это действие приведёт к немедленному отбрасыванию всех пакетов, соответствующих условию (то есть всех, кто не из России). Пакеты будут сброшены без уведомления отправителя и без дальнейшей обработки.

7. При необходимости добавьте комментарий к правилу. Это может быть пояснение или примечание для администратора.

8. Нажмите зелёную кнопку **Добавить**, чтобы сохранить правило в список.

9. После добавления нажмите кнопку **Применить** в левой части интерфейса. Только после этого правило будет активно и начнёт применяться

к обрабатываемому трафику.



5.3.3 Пример №2

Назначение правила: Ограничение частоты UDP-трафика с последующей временной блокировкой IP-адреса-источника при превышении лимита. Правило также регистрирует статистику по всем срабатываниям.

1. В интерфейсе профиля нажмите кнопку Вручную. Это откроет форму для настройки совпадений.

2. В поле Совпадение выберите параметр protocol -> udp. Нажмите кнопку **Добавить**. Это ограничит обработку правил только UDP-трафиком.

3. В поле Действие выберите **ratelimit**, указав параметры:

```
id — > 8

Bucket key -> l3_proto и l3_src

pps — > rate -> 500
```

Нажмите кнопку **Добавить.** Это ограничение установит максимум 500 пакетов в секунду от одного источника. В правом нижнем углу нажмите зелёную кнопку Добавить для добавления первого правила.

4. Добавьте второе правило. В поле **Совпадение** выберите **verdict**, установите:

`type — > ratelimit`

`value — > exceed`

Нажмите кнопку **Добавить**. Это условие будет выполнено, если лимит, указанный в предыдущем шаге, превышен.

5. В поле **Действие** поочерёдно выберите:

STATS — имя счётчика RL_UDP_SRC_BLOCK. Это позволит учитывать случаи превышения лимита. Нажмите кнопку **Добавить.**

HMARK, указав: — id -> 2 — value -> 2 — lifetime -> 300 Нажмите кнопку **Добавить**. Действие установит метку на IP-адрес на 300 секунд.

DROP — для немедленного отбрасывания пакета.

В правом нижнем углу нажмите кнопку **Добавить** для добавления второго правила.

6. Добавьте третье правило. В поле **Действие** выберите:

`verdict — > clear.`

Нажмите кнопку **Добавить**. Сбрасывает verdict правила, если ни одно из предыдущих условий не выполнено.

В правом нижнем углу нажмите зелёную кнопку Добавить для добавления третьего правила.

7. Добавьте четвёртое правило. В поле **Совпадение** добавить параметр HMARK, указав:

`id — > 2`

`status — > valid`

Нажмите кнопку **Добавить.** Это условие проверяет, что у пакета уже установлена действительная хеш-метка.

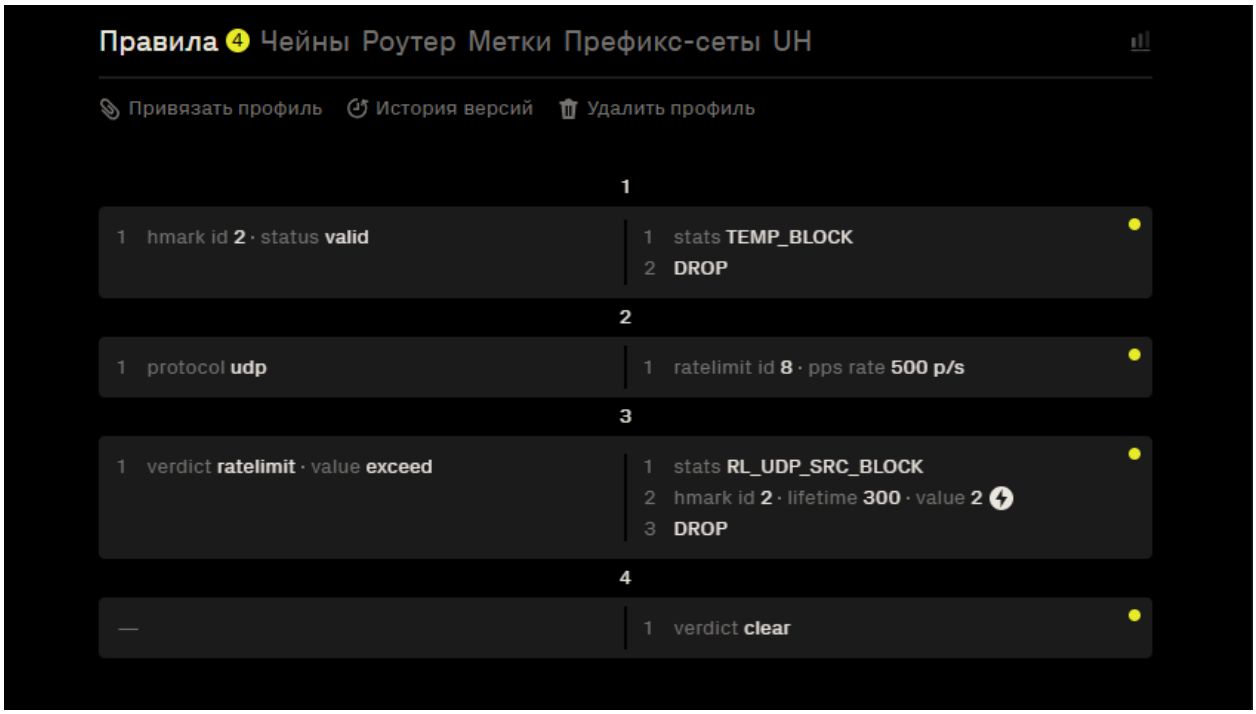
8. В поле Действие выберите **STATS** и введите имя счётчика: TEMP_BLOCK. Нажмите кнопку **Добавить**. Это позволит отслеживать количество срабатываний правила.

9. Добавьте ещё одно действие: DROP.

Все пакеты с валидной меткой 2 будут отброшены. Нажмите зелёную кнопку **Добавить**, чтобы сохранить правило в список.

10. Переместите четвёртое правило в начало списка правил. Это обеспечивает приоритетную фильтрацию пакетов, уже помеченных HMARK id 2, без повторной проверки всех условий, заданных ниже. Такое расположение позволяет сразу отбрасывать трафик, ранее идентифицированный как превышающий лимит, минимизируя нагрузку на последующую обработку.

11. Нажмите **Применить**. Только после этого правила начнут применяться к трафику.



5.4 Чейны

5.4.1 Назначение чейнов

Чейн — отдельная ветка правил, используемая для обработки и фильтрации сетевого трафика. Чейн содержит набор правил, которые определяют порядок обработки пакетов в рамках выбранного сценария.

Чейны применяются для выборочного включения механизмов защиты при прохождении постоянного трафика через DosGate. Такой подход позволяет не включать защитные меры непрерывно и снижает влияние на легитимный трафик.

По структуре чейны аналогичны стандартным правилам фильтрации. В них можно задавать условия обработки пакетов и использовать готовые пресеты для унификации настройки.

5.4.2 Принцип работы

Обработка трафика с использованием чейна выполняется в следующем порядке:

Основной профиль применяет базовый набор правил обработки пакетов. Если пакет соответствует условиям, заданным в профиле, он перенаправляется в определённый чейн. В чейне выполняются дополнительные правила, предназначенные только для перенаправленных пакетов. После выполнения правил чейна пакет отбрасывается, допускается к дальнейшей обработке или возвращается в основной профиль в зависимости от настроенных действий.

Такой порядок позволяет включать дополнительные механизмы защиты только для трафика, который требует отдельной обработки.

5.4.3 Пример использования чейна

Ниже приведён пример использования чейна для фильтрации трафика по географическому признаку. В примере трафик разделяется по стране источника.

1. Анализ входящего трафика.

При поступлении пакета система анализирует IP-адрес источника и определяет страну источника с использованием базы GeoIP.

2. Сопоставление с правилами профиля и перенаправление в чейн.

В профиле настраивается правило, которое проверяет, относится ли трафик к России. Если условие не выполняется, срабатывает действие GOTO. Оно перенаправляет пакет в отдельный чейн Not-RU. Чейн Not-RU является логически изолированным блоком правил и применяется только к трафику, который был в него перенаправлен.

3. Применение дополнительных политик фильтрации.

Внутри чейна Not-RU можно настроить дополнительные механизмы защиты. Например, ограничение количества соединений с одного IP-адреса, фильтрацию по протоколам или блокировку трафика с известных вредоносных IP-адресов.

4. Принятие решения по пакету.

Если пакет соответствует критериям блокировки, он отбрасывается. Если пакет проходит настроенные проверки, он возвращается в основной профиль и продолжает обработку.

5.5 Роутер

5.5.1 Общие сведения

Роутер — это IP-адрес или префикс, по которому система определяет профиль для обработки входящего трафика.

DosGate сравнивает IP-адрес назначения в пакете со значениями роутеров, заданными в профилях. По результату сравнения система выбирает профиль, в который необходимо направить трафик для дальнейшей маршрутизации и фильтрации.

Роутеры могут задаваться для отдельных IP-адресов и для подсетей с разными масками. Это позволяет разделять обработку трафика между профилями и применять разные правила фильтрации к разным адресам или сетям.

5.5.2 Принцип работы

Обработка трафика с использованием роутера выполняется в следующем порядке.

1. Обнаружение интерфейса.

Входящий трафик поступает на интерфейс системы. Интерфейсы могут быть объединены в арены, которые используются как логические группы интерфейсов.

2. Анализ адреса назначения.

После определения интерфейса система анализирует IP-адрес назначения пакета. Затем система ищет в профилях DosGate роутер, в котором указана сеть или конкретный IP-адрес, совпадающий с адресом назначения пакета.

3. Выбор наиболее специфичного совпадения.

Если для одного адреса или сети подходит несколько роутеров, система выбирает наиболее специфичное совпадение, то есть запись с наибольшей маской.

5.5.3 Настройка роутера в профиле

Чтобы настроить роутер для профиля, выполните следующие действия:

1. Откройте нужный профиль.

2. Перейдите на вкладку **Роутер.**

3. Нажмите кнопку добавления записи.

4. Укажите IP-адрес или префикс, по которому трафик должен направляться в выбранный профиль.

5. Сохраните запись.

6. Нажмите **Применить**, чтобы изменения начали использоваться при обработке трафика.

После применения изменений система будет учитывать добавленный роутер при выборе профиля для входящих пакетов.

5.6 Метки

5.6.1 Общие сведения

Раздел предназначен для просмотра и управления быстрыми таблицами данных, которые используются для временной фиксации информации о сетевых пакетах и соединениях.

Метки применяются при обработке трафика, выявлении повторяющихся событий, управлении реакцией системы и отладке правил фильтрации.

5.6.2 Типы меток

В системе поддерживаются следующие типы меток.

Тип метки	**Назначение**
HMARK	Фиксирует IP-адрес источника.
DHMARK	Фиксирует IP-адрес назначения.
SDHMARK	Фиксирует пару адресов: IP-адрес источника и IP-адрес назначения.
CONNMARK	Фиксирует полное описание соединения: IP-адрес источника, IP-адрес назначения, порт источника, порт назначения и транспортный протокол L4.

HMARKC	Административная метка для создания чёрных и белых списков. Префиксы добавляются вручную и не зависят от правил фильтрации.
SD24HMARKC	Административная метка для создания чёрных и белых списков по подсетям источника и назначения. Для IPv4 используются подсети /24, для IPv6 - /64. Префиксы добавляются вручную и не зависят от правил фильтрации.

Для записей меток используются следующие поля.

Поле	**Описание**
ID	Идентификатор записи.
Value	Числовой счётчик, значение которого изменяется правилами.
Age	Время, прошедшее с момента добавления записи.
Lifetime	Время до истечения записи. Значение обновляется при поступлении подходящих пакетов. После истечения срока действия запись получает статус expired.

5.6.3 Принцип работы меток

Описанный ниже механизм не применяется к меткам HMARKC, так как такие метки создаются и изменяются вручную.

5.6.4 Создание метки

Когда срабатывает правило, система создаёт запись с параметрами трафика, характерными для выбранного типа метки.

5.6.5 Применение метки в правилах

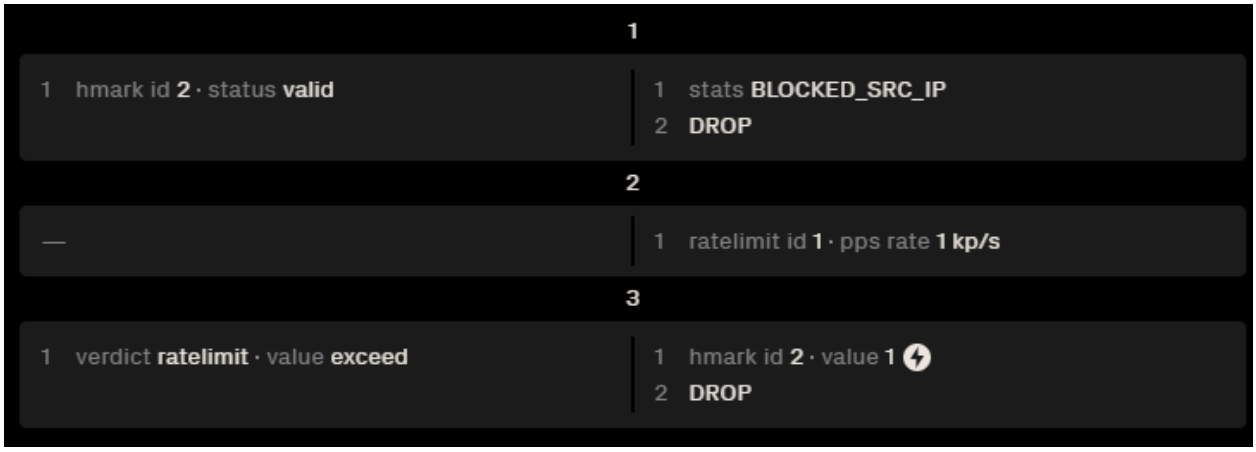
При обработке каждого нового пакета система проверяет наличие подходящей активной метки. Если метка найдена и имеет статус valid, правило может применить заданное действие: блокировку, перенаправление или другое поведение, предусмотренное конфигурацией.

5.6.6 Обновление и удаление

При повторных нарушениях значение lifetime продлевается. За счёт этого метка остаётся активной дольше. После истечения срока действия метка удаляется автоматически. При необходимости запись можно удалить вручную.

5.6.7 Пример использования HMARK

Сценарий: временная блокировка IP-адреса источника при превышении пороговой интенсивности пакетов.



Чтобы настроить временную блокировку с использованием HMARK, выполните следующие действия.

1. Создайте правило, которое проверяет наличие активной метки HMARK id 2 у IP-адреса источника.

2. Добавьте действие STATS с именем счётчика BLOCKED_SRC_IP, чтобы фиксировать срабатывания правила в статистике.

3. Добавьте действие DROP, чтобы отбрасывать пакеты от источника, у которого уже есть активная метка.

4. Создайте правило для измерения интенсивности трафика. Если метки нет, система должна измерять частоту пакетов от одного источника. В примере используется порог 1000 pps.

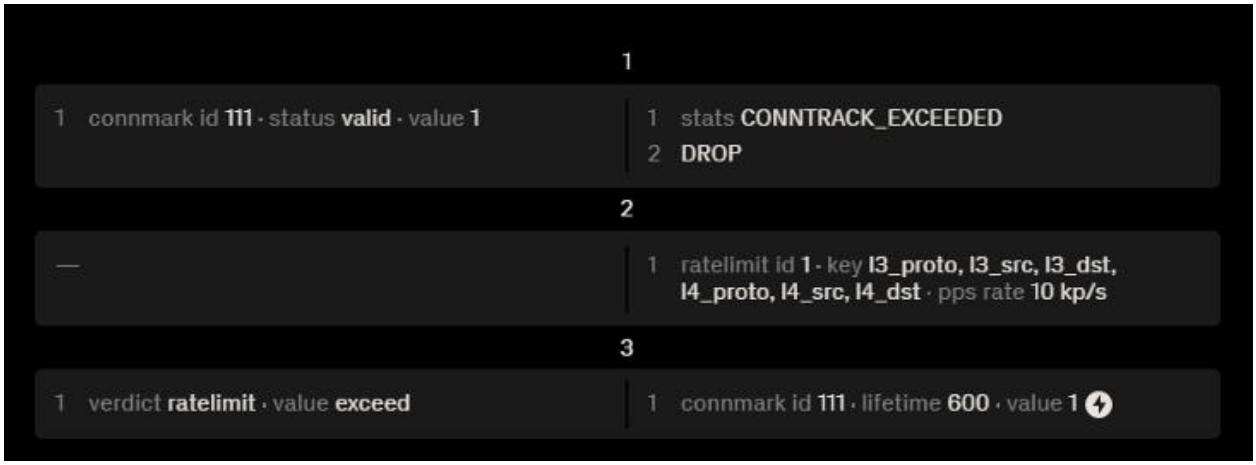
5. Создайте правило реакции на превышение порога. При превышении порога система создаёт запись HMARK id 2 и отбрасывает текущие пакеты.

6. Нажмите «Применить», чтобы сохранить изменения и активировать правила обработки трафика.

Пока запись HMARK id 2 имеет статус valid, трафик источника блокируется без повторного измерения интенсивности. После истечения lifetime измерение возобновляется. При повторном превышении порога создаётся новая запись, а блокировка обновляется.

5.6.8 Пример использования CONNMARK

Сценарий: временная блокировка TCP- или UDP-сессий при превышении порога трафика.



Чтобы настроить блокировку соединений с использованием CONNMARK, выполните следующие действия.

1. Создайте правило, которое проверяет наличие активной метки CONNMARK id 111.

2. Добавьте действие STATS с именем счётчика CONNTRACK_EXCEEDED, чтобы фиксировать срабатывания правила в статистике.

3. Добавьте действие DROP, чтобы отбрасывать пакеты соединения при наличии активной метки.

4. Создайте правило для измерения интенсивности. Если метки нет, система должна считать пакеты для каждого соединения отдельно.

5. Укажите параметры, по которым определяется соединение: l3_proto, l3_src, l3_dst, l4_proto, l4_src и l4_dst.

6. Задайте порог интенсивности. В примере используется значение 10 000 pps на одно соединение.

7. Создайте правило реакции на превышение порога. При превышении порога система создаёт запись CONNMARK id 111 на 600 секунд.

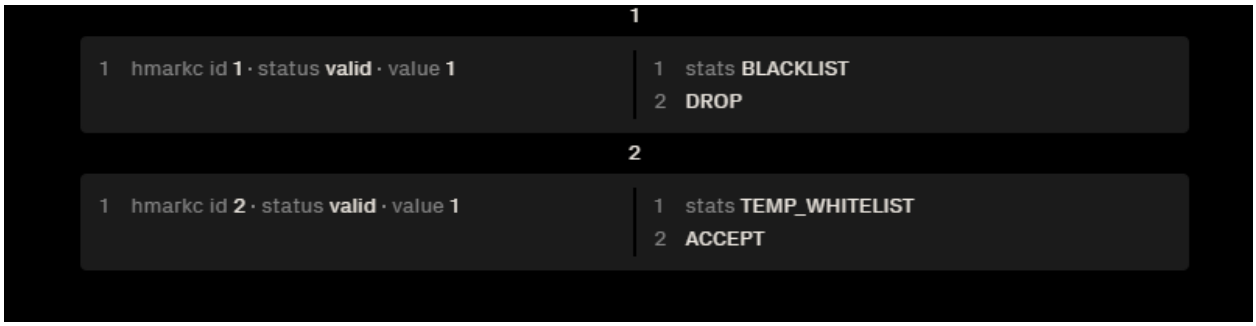
8. Нажмите «Применить», чтобы сохранить изменения и активировать правила обработки трафика.

Параметр соединения	Описание
l3_proto	Протокол сетевого уровня: IPv4 или IPv6.
l3_src	IP-адрес источника.
l3_dst	IP-адрес назначения.
l4_proto	Транспортный протокол: TCP или UDP.
l4_src	Порт источника.
l4_dst	Порт назначения.

Пока метка CONNMARK id 111 активна, трафик соединения блокируется без повторных измерений. После истечения lifetime пакеты снова проходят проверку интенсивности. Если порог снова превышается, система обновляет метку и повторно применяет блокировку.

5.6.9 Пример использования HMARKC

Сценарий: адресное управление трафиком по заранее заданным префиксам.



Метки HMARKC используются как административные списки. Такие метки создаются и наполняются вручную, а правила фильтрации используют их как источник данных для принятия решения по трафику.

Чтобы использовать HMARKC, выполните следующие действия.

1. Откройте раздел **Метки**.

2. Создайте новую метку HMARKC.

3. Добавьте в метку необходимые префиксы.

4. Откройте правило фильтрации, в котором должна использоваться метка.

5. В условии совпадения выберите HMARKC.

6. Задайте действие DROP или ACCEPT в зависимости от требуемого поведения.

7. Нажмите **Применить**, чтобы сохранить изменения и активировать правило.

Действие	**Назначение**
DROP	Блокирует трафик указанных адресов. Правило работает как чёрный список.
ACCEPT	Пропускает трафик без дальнейшей фильтрации. Используется как белый список.

Метка HMARKC управляется вручную. Автоматическое создание и продление lifetime правилами не поддерживается.

5.6.10 Использование счётчика Value

Поле Value используется для фиксации повторных нарушений и усиления реакции системы при эскалации.

При первом превышении порога создаётся метка HMARK со значением value = 1. При каждом новом превышении для того же источника значение увеличивается: value = 2, value = 3 и далее.

Когда значение достигает заданного порога, к источнику можно применить более строгую реакцию: добавить адрес в префикс-сет или обработать его отдельным блокирующим правилом.

Пример: источник 10.0.0.1 отправил 600 TCP SYN-пакетов. Система создаёт метку HMARK со значением value = 1. Через 100 секунд тот же адрес отправил 700 пакетов, после чего значение увеличивается до value = 2. Следующее превышение увеличивает значение до value = 3, после чего источник может быть заблокирован через префикс-сет или отдельное правило.

5.7 Префикс-сеты

5.7.1 Общие сведения

Префикс-сет — это набор IP-адресов или IP-префиксов, который используется в правилах для формирования белых и чёрных списков.

Префикс-сеты бывают двух типов:

- Глобальные — действуют в пределах всей арены и могут использоваться во всех профилях
- Локальные — применяются только в рамках выбранного профиля

5.7.2 Добавление префикс-сета

Чтобы создать новый префикс-сет:

- Откройте нужный раздел:
  - для создания глобального префикс-сета откройте раздел Глобальные префикс-сеты
  - для создания локального префикс-сета откройте раздел Профиль → Префикс-сеты
- В верхней части списка нажмите значок +.
- В выпадающем меню выберите способ создания префикс-сета:
  - Создать новый
  - Создать по ссылке

5.7.3 Создание нового префикс-сета

Чтобы создать новый префикс-сет вручную:

- Выберите пункт Создать новый.
- Укажите название префикс-сета.
- Нажмите Создать.

После сохранения префикс-сет появится в списке и будет доступен для добавления записей.

5.7.4 Создание префикс-сета по ссылке

Префикс-сет можно создать по ссылке на внешний источник данных. В этом случае система загружает список IP-префиксов по HTTP или HTTPS и может обновлять записи автоматически.

Чтобы создать префикс-сет по ссылке:

- Выберите пункт Создать по ссылке.
- Заполните поля формы:
  - Название — укажите имя префикс-сета, например whitelist
  - Ссылка — укажите URL-адрес источника списка
  - Логин — укажите логин для аутентификации на удалённом ресурсе, если требуется
  - Пароль — укажите пароль для аутентификации, если требуется
  - Интервал — задайте периодичность обновления списка в секундах, например 60
  - CRESP Hash — включите обработку хешированного формата списка, если он используется в текущей инсталляции
- Нажмите Создать.

После сохранения префикс-сет появится в списке. При заданном интервале обновления система будет периодически получать данные из указанного источника.

5.7.5 Добавление записи в префикс-сет

Префикс-сет состоит из записей. Каждая запись содержит IP-префикс и значение value.

value — это числовой идентификатор записи. Он относится к конкретной записи, а не ко всему префикс-сету. Значение value используется для группировки записей и выбора отдельных групп при настройке правил фильтрации.

В правилах можно указывать конкретные значения value. Это позволяет применять правило не ко всем записям префикс-сета, а только к тем, у которых задано соответствующее значение. Записи с одинаковым value могут использоваться как одна логическая группа.

Чтобы добавить запись в префикс-сет вручную:

- Откройте нужный префикс-сет.
- В интерфейсе управления нажмите значок +.
- В открывшемся окне укажите IP-адрес с маской, например 10.0.0.0/24.
- Укажите числовое значение value.
- Нажмите Добавить.

Если маска не указана, система автоматически назначит маску /32.

5.7.6 Добавление записей из TXT-файла

Записи можно добавить из TXT-файла с перечнем IP-префиксов. Для этого перетащите файл в область таблицы префикс-сета. После загрузки система добавит записи в префикс-сет и обновит его содержимое.

Файл может содержать только IP-префиксы:

```
192.168.1.0/24
10.0.0.0/8
1.1.1.0/24
```

Если значение value не указано, для записи автоматически устанавливается значение 1. Чтобы назначить value для каждой записи, укажите его после IP-префикса:

```
192.168.1.0/24  1
10.0.0.0/8      2
1.1.1.0/24      1
```

6 RLog

6.1 Назначение RLOG

LOG предназначен для анализа HTTP-логов, поступающих от внешних систем, которые выполняют терминацию TLS. На основании полей логов система рассчитывает показатели активности, выявляет источники с нестандартным поведением и передаёт данные в DosGate для последующей фильтрации трафика.

RLOG позволяет работать с зашифрованным L7-трафиком по данным журналов. При выполнении заданных условий система может присвоить IP-адресу источника временную метку и передать её в DosGate. Блокировка на уровне сетевого трафика выполняется правилами DosGate, которые используют соответствующую метку.

6.2 Принцип работы

RLOG принимает поток HTTP-логов от одного или нескольких источников. Каждая запись журнала разбирается по схеме, выбранной при создании профиля. Извлечённые поля, например HTTP-статус, IP-адрес клиента, время ответа, virtual IP и заголовки запроса, используются для расчёта метрик. На основании метрик срабатывают правила RLOG. Правила определяют допустимую частоту запросов, значения HTTP-заголовков, коды ответов, географические признаки и другие условия.

Если условия правила выполнены, RLOG выполняет действие, например устанавливает метку HMARK для IP-адреса источника. Информация о потенциально опасном источнике передаётся в Servicepipe Spider и далее в DosGate. DosGate применяет блокировку или другое действие, если в соответствующем профиле настроено правило, использующее переданную метку.

Важно: передача метки из RLOG сама по себе не блокирует трафик. Для блокировки необходимо создать правило в DosGate, которое проверяет наличие этой метки и применяет требуемое действие, например DROP.

6.2.1 Пример работы RLOG с DosGate

Пример: правило RLOG отслеживает HTTP-запросы с определённым User-Agent и частотой более 5 запросов за 10 секунд. Если условия выполнены, RLOG присваивает IP-адресу источника временную метку HMARK id 1, value 1 со сроком действия 100 секунд и передаёт её в DosGate в арену first и профиль test123.

В DosGate настраивается правило, которое проверяет наличие активной метки HMARK id 1, value 1. Если метка найдена, трафик от соответствующего IP-адреса блокируется действием DROP, а срабатывание фиксируется в счётчике RLOG_BOT_BAN.

6.3 Профиль

Профиль RLOG определяет, как система разбирает поступающие HTTP-логи, какие правила применяет и какие статистические данные отображает.

6.3.1 Создание профиля

Чтобы создать профиль:

- На главной странице в разделе **Профили** нажмите кнопку **Плюс**.
- В открывшейся форме заполните параметры профиля.
- Нажмите **Создать**.

Параметр	**Описание**
Название	Уникальное имя профиля. Рекомендуется использовать комбинацию обозначения сегмента

	инфраструктуры и названия сервиса, например zapadniy-filial-web.
Описание	Краткое пояснение, которое помогает определить назначение профиля.
Схема	Шаблон формата строк в логах. Определяет, как система будет разбирать поступающие журналы. После создания профиля изменить схему нельзя.

После создания профиля интерфейс откроет страницу нового профиля.

6.3.2 Изменение профиля

В общем списке профилей щёлкните правой кнопкой мыши по названию профиля.

- Выберите пункт **Изменить**.
- Измените название или описание профиля.
- Сохраните изменения.

6.3.3 Удаление профиля

В общем списке профилей щёлкните правой кнопкой мыши по названию профиля.

- Выберите пункт **Удалить**.
- Подтвердите удаление, если система запросит подтверждение.
- После удаления профиль безвозвратно удаляется из системы.

6.4 Статистика

Раздел предназначен для визуального мониторинга состояния трафика, поступающего в RLOG в виде HTTP-логов. Раздел помогает выявлять аномалии и источники нестандартного поведения на основе агрегации данных от разных хостов.

6.4.1 Навигация и фильтрация

В верхней панели выберите временной диапазон: 5 мин, 15 мин, 30 мин, 1 час, 6 часов, 12 часов, 24 часа, 3 дня или 7 дней.

Чтобы отфильтровать данные по виртуальному хосту, введите доменное имя в строку поиска по хосту.

6.4.2 Таблица хостов

В таблице отображаются хосты, по которым поступают HTTP-запросы. Таблица поддерживает сортировку по каждому столбцу. Чтобы изменить порядок сортировки, нажмите заголовок нужного столбца.

Колонка	**Описание**
Хост	Доменное имя виртуального хоста, извлечённое из логов.
RPS	Количество запросов в секунду. Значение рассчитывается как среднее за выбранный интервал.
% non-200	Процент HTTP-ответов с кодами, отличными от 200. Отражает долю ошибок и редиректов.
Уник. IP/s	Количество уникальных IP-адресов источников запросов в секунду.

6.4.3 Графики

График	**Назначение**
Top-12 хостов · RPS	Показывает интенсивность запросов по 12 наиболее активным хостам. Используется для выявления пиков и резких изменений трафика.
Top-12 хостов · % non-200	Показывает процент ответов с HTTP-кодами, отличными от 200, по 12 наиболее активным

	хостам. Используется для выявления источников с высоким уровнем ошибок.
Top-12 хостов · Уник. IP/s	Показывает динамику количества уникальных IP-адресов источников запросов. Может указывать на распределённость трафика или сканирование.
Профиль · RPS	Показывает суммарную нагрузку по запросам в секунду в рамках выбранного профиля.
Профиль · Ответ сервера	Показывает распределение ответов сервера по классам HTTP-кодов: 200, 300, 400 и 500.
Профиль · Время ответа	Показывает распределение запросов по времени ответа сервера: менее 10 мс, 10-50 мс, 50-200 мс, 200-1000 мс и более 1000 мс.

6.5 Правила

Правила RLOG создаются путём комбинирования совпадений и действий. Совпадения определяют условия, при которых правило срабатывает. Действия выполняются, если все условия правила выполнены.

Справа в интерфейсе расположена вкладка Редактор. В этой области задаются совпадения и действия. При необходимости добавьте текстовый комментарий: он сохраняется вместе с правилом и используется для технических пометок.

Также справа расположена вкладка **Папки**. С её помощью можно вручную группировать правила по папкам для упрощения навигации и визуальной организации конфигурации.

6.6 Дампы логов

Функция дампов логов позволяет выгрузить сырые данные, которые поступают в RLOG по выбранному профилю. Данные выгружаются без обработки, в том виде, в котором они поступили в систему.

Чтобы создать дамп логов:

- Откройте нужный профиль RLOG.
- Перейдите к функции создания дампа логов.
- Нажмите **Создать дамп.**
- Укажите объём дампа. Допустимый объём - от 10 до 100 000 записей.
- Дождитесь формирования дампа или скачайте уже собранную часть данных, если она доступна.

Сформированный дамп доступен для скачивания в течение 24 часов после создания. Сбор логов может занять некоторое время.

6.7 Источники

Раздел используется для указания IP-адресов или подсетей, от которых RLOG принимает логи. Каждый источник задаётся в формате CIDR, например 192.168.199.10/32.

Список источников работает как фильтр. Если адрес отправителя лога не входит ни в один из указанных диапазонов, лог не обрабатывается.

Механизм аналогичен роутерам в DosGate: он определяет, к какому профилю относятся входящие данные. Допускается указывать как отдельные IP-адреса, так и сети с масками. Для каждого источника можно добавить комментарий.

Чтобы добавить источник:

- Откройте раздел **Источники** в нужном профиле.
- Добавьте IP-адрес или подсеть в формате CIDR.
- При необходимости укажите комментарий.
- Сохраните изменения.

7 FlowCollector

7.1 Назначение FlowCollector

FlowCollector — интеллектуальная система анализа потокового трафика, предназначенная для раннего выявления DDoS-атак и сетевых аномалий. Обеспечивает высокоскоростную агрегацию и обработку потоковых данных, выявляя подозрительную активность и автоматически инициируя защитные меры. Используется как самостоятельный детектор или как часть комплексной системы с DosGate.

7.2 Управление объектами FlowCollector

Объект — набор IP-префиксов назначения и правил контроля трафика. Объект определяет, какой трафик анализируется системой и какие пороговые значения используются для выявления аномалий.

7.2.1 Создание объекта

Чтобы создать объект:

- На главной странице откройте раздел **Объекты**.
- Нажмите значок **+.**
- В открывшейся форме заполните параметры объекта.

Параметр	**Описание**
Название	Уникальное имя объекта. Рекомендуется использовать обозначение сегмента инфраструктуры и название сервиса, например zapadniy-filial-web или dmz-dns.
Описание	Краткое пояснение о назначении объекта.
Связать с ДГ	Профиль DosGate, с которым связывается объект при настроенной интеграции FlowCollector и DosGate. Связь используется для сопоставления событий и

	мониторинга трафика при обнаружении аномалий.
Папка	Папка для группировки объектов. Можно выбрать существующую папку или создать новую.

- Нажмите **Создать**.

После создания объект появится в общем списке и станет доступен для настройки счётчиков и порогов.

7.2.2 Изменение объекта

- В списке объектов нажмите правой кнопкой мыши название нужного объекта.
- Выберите **Изменить**.
- В открывшемся окне измените параметры и сохраните изменения.

7.2.3 Удаление объекта

- В списке объектов нажмите правой кнопкой мыши название нужного объекта.
- Выберите **Удалить.**
- Подтвердите удаление.

Удалённый объект не может быть восстановлен средствами веб-интерфейса.

7.3 Дашборд FlowCollector

Раздел предназначен для оперативного контроля сетевой активности, просмотра обнаруженных аномалий и анализа трафика защищаемых объектов.

7.3.1 Рабочая область

В рабочей области отображаются общая статистика по аномалиям, средства поиска и фильтрации, список обнаруженных событий и графики трафика.

7.3.2 Общая статистика по аномалиям

В верхней части раздела отображаются: количество аномалий, зафиксированных за последние 30 дней процентное изменение количества аномалий по сравнению с предыдущим периодом, тепловая карта активности по дням за последние шесть месяцев Тепловая карта позволяет оценить распределение аномалий по датам и выделить периоды повышенной активности.

7.3.3 Поиск и фильтрация аномалий

Чтобы найти нужные аномалии:

- Введите в строку поиска название объекта, вектор атаки или IP-адрес.
- Выберите временной интервал в правой части панели фильтрации.
- При необходимости задайте начало и окончание периода вручную.

После настройки фильтров в списке останутся только события, соответствующие заданным условиям.

7.3.4 Список аномалий

Аномалии разделяются на два типа:

Активные — события, для которых текущее значение трафика превышает заданный порог.

Завершённые — ранее обнаруженные события, превышение порога по которым больше не фиксируется.

Для каждой аномалии отображаются следующие сведения:

Параметр	**Описание**
Старт/завершение	Дата и время начала события. Для завершённой аномалии также отображается время окончания.
Порог	Пороговое значение, при превышении которого зарегистрирована аномалия.
Пик	Максимальное значение трафика, зафиксированное в период аномалии.
Профиль	Название защищаемого объекта FlowCollector.
IP	IP-адрес назначения, для которого обнаружена аномалия.
Вектор	Категория трафика, по которой обнаружено превышение, например udp-flood, icmp-flood или total-traffic.

7.3.5 Просмотр сведений об аномалии

Чтобы открыть сведения об аномалии, выберите нужную строку в списке. В интерфейсе отобразятся данные выбранного события и связанные показатели трафика.

7.3.6 Визуализация трафика

В нижней части раздела расположены графики, отображающие показатели трафика за выбранный период.

График	**Назначение**
Total Bits	Отображает общий объём входящего трафика по всем объектам в битах в секунду.
Total Packets	Отображает общее количество входящих сетевых пакетов в секунду.
Top 12 Managed Objects by Bits	Отображает 12 объектов с наибольшим объёмом входящего трафика в битах в секунду.
Top 12 Managed Objects by Packets	Отображает 12 объектов с наибольшим количеством входящих пакетов в секунду.

Чтобы изменить данные на графиках:

- Выберите временной интервал в панели фильтрации.
- При наличии фильтра объектов выберите нужный объект или оставьте значение **Все**.
- Используйте легенду графика для сопоставления линий с объектами.

После изменения временного интервала или объекта графики обновляются автоматически.

7.4 Data Explorer

Data Explorer — раздел FlowCollector для анализа сохранённых данных о сетевых потоках. Раздел позволяет выбирать период, задавать поля и метрики, применять фильтры, строить графики и просматривать агрегированные данные в таблице.

Data Explorer используется для ретроспективного анализа трафика, поиска отклонений и изучения его структуры по IP-адресам, портам, протоколам, автономным системам, географическим признакам и другим параметрам.

7.4.1 Включение Data Explorer

Для отображения Data Explorer в веб-интерфейсе должен быть включён параметр save-flow в конфигурации анализатора FlowCollector.

Откройте конфигурационный файл анализатора:

```
sudo nano /opt/spfc/etc/analyzer.yaml
```

Установите значение параметра save-flow:

```
save-flow: true
```

Сохраните изменения и перезапустите сервис анализатора в соответствии с принятой в инфраструктуре процедурой. В боковом меню веб-интерфейса выберите Data Explorer.

7.4.2 Построение отчёта

Чтобы построить график и таблицу с данными, задайте параметры в панели **Фильтры.**

- Выберите период.
- Укажите количество линий на графике.
- Добавьте одно или несколько полей.
- Добавьте одну или несколько метрик и выберите способы расчёта.
- При необходимости задайте фильтры по значениям выбранных полей.
- Нажмите **Применить.**

После применения параметров в рабочей области отображаются график и таблица с агрегированными значениями.

Параметр «Период» задаёт временной интервал, за который выводятся данные. Можно выбрать готовый интервал или задать точные дату и время начала и окончания периода.

Параметр «Линии на графике» определяет количество строк таблицы, которые отображаются на графике. На график выводятся первые N строк с учётом текущей сортировки. Каждая строка представлена отдельной линией.

Поля определяют признаки, по которым выполняются группировка и фильтрация данных. Можно выбрать несколько полей для более подробного анализа.

Поле	**Описание**
Das	Номер автономной системы получателя
Dasname	Имя автономной системы получателя
Dport	Порт получателя
Dst	IP-адрес получателя

Geoipdst	Страна получателя
Geoipsrc	Страна отправителя
Len	Длина пакета
Protocol	Протокол
Sas	Номер автономной системы отправителя
Sasname	Имя автономной системы отправителя
Sport	Порт отправителя
Src	IP-адрес отправителя
Tcpflags	Флаги TCP
Tos	Тип обслуживания

Метрики определяют количественные показатели, рассчитываемые по выбранным данным. Они используются для анализа объёма трафика, количества пакетов и распределения значений по выбранным признакам.

Метрика	**Описание**
Bits	Объём данных в битах
Das	Количество значений по номеру автономной системы получателя
Dport	Количество значений по порту получателя
Dst	Количество значений по IP-адресу получателя
Geoipdst	Количество значений по стране получателя
Geoipsrc	Количество значений по стране отправителя
Packets	Количество пакетов
Sas	Количество значений по номеру автономной системы отправителя
Sport	Количество значений по порту отправителя
Src	Количество значений по IP-адресу отправителя

Для каждой метрики можно выбрать один или несколько способов расчёта:

Параметр	**Описание**
Avg	Среднее значение
Max	Максимальное значение
Percentile95	95-й перцентиль
Percentile99	99-й перцентиль

Total	Общее значение

Параметр Total установлен по умолчанию и не может быть отключён.

Фильтр ограничивает результаты по значениям выбранных полей.

- В панели Фильтры нажмите + в блоке **Фильтр**.
- Выберите поле.
- Укажите одно или несколько значений. Несколько значений вводите через запятую без пробелов.
- Чтобы исключить указанные значения из результатов, включите параметр **NOT**.
- Нажмите **Создать.**
- После настройки остальных параметров нажмите **Применить**.

7.4.3 Просмотр результатов

После применения настроек в рабочей области отображаются график и таблица. График показывает изменение выбранной метрики во времени. Таблица содержит значения выбранных полей и рассчитанные показатели.

Если для метрики выбрано несколько способов расчёта, переключайтесь между ними в списке над графиком.

При сортировке таблицы график перестраивается по выбранному столбцу. На нём отображаются первые N строк в соответствии со значением параметра Линии на графике.

По умолчанию на графике отображаются все значения, вошедшие в выборку. Чтобы скрыть или отобразить отдельное значение, выберите его в легенде справа от графика.

7.4.4 Сброс параметров

Чтобы удалить заданные поля, метрики и фильтры и вернуться к исходному состоянию рабочей области, нажмите **Сбросить фильтр.**

7.5 FlowSpec-правила

FlowSpec-правила — правила BGP Flow Specification, предназначенные для распространения политик фильтрации на маршрутизаторы.

7.5.1 Назначение

FlowSpec-правила применяются для оперативного ограничения, перенаправления или маркировки трафика на уровне маршрутизаторов. Правила выполняются на границе сети и позволяют отсечь нежелательный трафик до его поступления во внутреннюю инфраструктуру или систему очистки.

При DDoS-атаках FlowSpec-правила используются для снижения нагрузки на каналы и узлы обработки. В инфраструктуре без выделенной системы очистки они могут использоваться как основной механизм быстрой фильтрации.

7.5.2 Добавление FlowSpec-правила

Чтобы добавить правило:

- Откройте раздел FlowSpec-правила.
- В правой части интерфейса нажмите **Добавить правило**.
- В редакторе укажите название правила.
- Задайте условия в блоке **Совпадение.**
- Выберите действие в блоке **Действие.**
- Нажмите **Сохранить и применить.**

После сохранения правило появится в общем списке. Имя правила изменить нельзя, поэтому укажите его до первого сохранения.

7.5.3 Совпадения

Совпадения определяют условия, по которым маршрутизатор выбирает трафик для применения правила. Для большинства совпадений доступен параметр NOT. При его включении правило применяется ко всем значениям, кроме указанного. Для параметров dst и src логическое отрицание не поддерживается.

dst — IP-адрес назначения

Параметр	**Описание**
Адрес	IP-адрес или префикс назначения в формате CIDR

Если значение не указано, правило используется как шаблон. При обнаружении аномалии система подставляет адрес назначения из события или счётчика.

src — IP-адрес источника

Параметр	**Описание**
Адрес	IP-адрес или префикс источника в формате CIDR

protocol — протокол

Значение	**Описание**
TCP	Протокол управления передачей
UDP	Протокол пользовательских дейтаграмм
ICMP	Протокол управляющих сообщений Интернета
IGMP	Управление членством в группах многоадресной рассылки IPv4
IP-in-IP	Инкапсуляция IP-пакетов в IP
RSVP	Резервирование сетевых ресурсов и сигнализация QoS
GRE	Протокол инкапсуляции GRE
OSPF	Внутренний протокол маршрутизации
PIM	Протокол независимой многоадресной маршрутизации
SCTP	Протокол управления потоками сообщений

dport и sport — порты

Параметр	Описание
dport	Порты назначения. Допускаются отдельные значения и диапазоны от 0 до 65535, перечисленные через запятую
sport	Порты источника. Допускаются отдельные значения и диапазоны от 0 до 65535, перечисленные через запятую

Примеры: 80; 53,123; 1020–65535.

len — длина пакета

Параметр	Описание
len	Длина IP-пакета в байтах. Можно указать отдельные значения или диапазоны через запятую

Примеры: 1280; 60–80; 576.

frag — фрагментация

Значение	Описание
any	Любой фрагмент
df	Пакет с установленным флагом Don't Fragment
first	Первый фрагмент
internal	Промежуточный фрагмент
last	Последний фрагмент
unfrag	Нефрагментированный пакет

icmp — тип и код

Для ICMP задаются тип и код сообщения. Правило срабатывает только для допустимого сочетания типа и кода.

Параметр	Описание
icmp-тип	Значение или диапазон типа ICMP, например 8 или 11
icmp-код	Значение или диапазон кода ICMP, например 0 или 1

tcpflags — флаги TCP

Флаг	Описание
syn	Инициализация соединения
ack	Подтверждение соединения
psh	Передача данных без задержки
rst	Принудительный сброс соединения
fin	Завершение соединения
ece	Индикация перегрузки ECN

cwr	Снижение окна при перегрузке
urg	Срочные данные

Параметр **Учитывать совместно (+)** определяет способ проверки выбранных флагов. При включённом параметре должны быть одновременно установлены все выбранные флаги. При выключенном параметре достаточно наличия одного из них.

dscp — класс обслуживания

Параметр	**Описание**
dscp	Значение класса обслуживания DSCP от 0 до 63

7.5.4 Действия

Действие определяет обработку трафика, соответствующего условиям правила.

Действие	**Аргумент**	**Описание**
ACCEPT	—	Разрешить трафик
DISCARD	—	Отбросить трафик
rate-limit	rate-limit	Ограничить скорость; трафик сверх заданного порога отбрасывается
rate-limit	AS	Номер автономной системы для сообщества traffic-rate
redirect	route-target (rt)	Перенаправить трафик в целевой VRF. Формат: as:vrf или cidr:vrf
mark	dscp	Назначить значение DSCP от 0 до 63
action sample	—	Выполнять семплирование и журналирование трафика
action terminal	—	Прекратить дальнейшую фильтрацию совпавшего трафика
action sample-terminal	—	Выполнить семплирование и

		прекратить дальнейшую фильтрацию

7.5.5 Примеры правил

invalid-ports — DISCARD. Отбрасывает TCP- и UDP-трафик к сети 192.168.0.0/24 на порты, не разрешённые условием. Используется для блокировки несанкционированных подключений и сканирования.

ipfrag-drop — DISCARD. Отбрасывает фрагментированные IP-пакеты, направленные на адрес 192.168.0.49/32.

len-udp-drop — DISCARD. Отбрасывает UDP-пакеты длиной 1280 байт, направленные в сеть 192.168.0.0/24.

udp-amp-auto — DISCARD. Отбрасывает UDP-трафик с характерных портов источников усиления. Если поле dst не заполнено, правило используется как шаблон, а адрес назначения подставляется из события.

udp-apm — DISCARD. Отбрасывает UDP-трафик усиления в указанной сети по заданным портам источника.

7.5.6 Список правил

В столбце **Использовано в объектах** отображаются объекты, к которым привязано правило.

Параметр **Вкл. везде?** используется для ручной публикации FlowSpec-анонса. При его включении система немедленно формирует и отправляет BGP FlowSpec-анонс на маршрутизаторы без учёта порогов и счётчиков объектов.

7.6 Счётчики и фильтрация

Раздел предназначен для настройки счётчиков трафика и способов обработки обнаруженных аномалий. Сведения о событиях отображаются на дашборде. При подтверждении аномалии трафик можно оставить без

изменений, перенаправить на следующий хоп или обработать с помощью FlowSpec-правила.

7.6.1 Общие настройки

В верхней части раздела задаются общие параметры обработки подтверждённых аномалий.

7.6.2 Перенаправление трафика на следующий хоп

Параметр **Перенаправлять трафик (next-hop)** определяет маршрут трафика после подтверждения аномалии. В качестве следующего хопа можно выбрать:

- систему фильтрации DosGate
- blackhole для полного отбрасывания трафика
- иной IP-адрес следующего хопа, заданный в конфигурации

Трафик сначала обрабатывается связанными FlowSpec-правилами. На следующий хоп передаётся только трафик, который не был отфильтрован этими правилами.

Имена и адреса следующих хопов задаются в файле analyzer.yaml. Пример:

```
nexthops:
  - name: transit
    ip: 192.168.0.1
  - name: dosgate
    ip: 192.168.10.1
```

7.6.3 Количество IP-адресов для сворачивания аномалий

Параметр определяет, при каком количестве IP-адресов локальные события объединяются в одну глобальную аномалию. Система учитывает уникальные IP-адреса, на которых превышены локальные пороги.

Сворачивание выполняется только при одновременном выполнении двух условий:

- количество IP-адресов достигло заданного значения
- суммарный трафик превысил минимальный глобальный порог и настроен хотя бы один глобальный счётчик

Например, при значении 20 система сначала регистрирует отдельные локальные события. После появления двадцатого IP-адреса и превышения глобального порога события объединяются в одну глобальную аномалию.

7.6.4 Начало аномалии

Параметр задаёт минимальное время непрерывного превышения порога до регистрации аномалии и выполнения выбранного действия. Настройка позволяет исключить кратковременные всплески трафика. Например, при значении 10 превышение должно сохраняться не менее 10 секунд.

7.6.5 Задержка завершения аномалии

Параметр задаёт время ожидания после последнего превышения порога. Если за этот период новые совпадения не зафиксированы, аномалия считается завершённой.

Задержка используется для объединения периодических всплесков, в том числе pulse-wave-атак, в одно событие. Например, если всплески повторяются каждые 30 секунд, а задержка составляет 60 секунд, система не завершает аномалию между волнами.

7.6.6 Управление счётчиками

Счётчик — набор параметров для непрерывного контроля трафика по заданным CIDR-префиксам. Счётчик сравнивает текущие значения трафика с установленным условием и фиксирует аномалию при его выполнении.

7.6.7 Добавление счётчика

- Нажмите **Добавить счётчик**.
- Настройте тип подсчёта, вектор, условие срабатывания и способ фильтрации.
- При необходимости измените положение счётчика в списке.
- Нажмите **Применить.**

7.6.8 Дублирование счётчика

- Откройте меню с тремя точками справа от счётчика.
- Выберите **Дублировать.**
- Измените параметры созданной копии.
- Нажмите **Применить.**

7.6.9 Удаление счётчика

- Откройте меню с тремя точками справа от счётчика.
- Выберите **Удалить.**
- Нажмите **Применить.**

7.6.10 Включение и отключение счётчика

Переключатель **Вкл** управляет активностью счётчика. После отключения счётчик перемещается в конец списка и становится недоступным для редактирования. Изменение вступает в силу после нажатия кнопки Применить.

7.6.11 Приоритет счётчиков

Порядок счётчиков в списке определяет последовательность обработки. Счётчики, расположенные выше, обрабатываются раньше. Новый счётчик получает наивысший приоритет. Для изменения приоритета переместите счётчик в нужную позицию и нажмите Применить.

7.6.12 Тип подсчёта

Тип	**Описание**
global	Трафик суммируется по всем IP-адресам, указанным во вкладке CIDR. Аномалия фиксируется при превышении порога совокупным трафиком.

local	Трафик подсчитывается отдельно для каждого IP-адреса внутри заданного диапазона. Аномалия фиксируется для конкретного адреса.
subnet	Трафик подсчитывается отдельно по подсетям, начиная с префикса /31. Аномалия фиксируется только при превышении порога внутри конкретной подсети.

7.6.13Векторы трафика

Вектор определяет, какой трафик учитывается счётчиком. Можно выбрать один или несколько векторов. Пакеты, не соответствующие выбранным условиям, исключаются из подсчёта.

Категория	**Вектор**	**Описание**
Общие	total-traffic	Любой пакет IPv4 или IPv6
Общие	ip-fragment-flood	Пакет с признаком фрагментации
Общие	http-flood	TCP-трафик на порт назначения 80
Общие	https-flood	TCP-трафик на порт назначения 443
Общие	icmp-flood	ICMP-трафик
Общие	dns-flood	UDP- или TCP-трафик на порт назначения 53
Общие	gre-flood	GRE-трафик
Общие	ip-private-flood	IPv4-трафик с адресом источника из частных диапазонов
Общие	spoofing-flood	Пакеты с подменённым IP-адресом источника
Flood TCP/UDP	tcp-flood	TCP-трафик
Flood TCP/UDP	udp-flood	UDP-трафик
Flood TCP/UDP	tcp-syn-flood	TCP-пакеты с флагом SYN
Flood TCP/UDP	tcp-ack-flood	TCP-пакеты с флагом ACK
Flood TCP/UDP	tcp-cwr-flood	TCP-пакеты с флагом CWR
Flood TCP/UDP	tcp-ece-flood	TCP-пакеты с флагом ECE

Flood TCP/UDP	tcp-fin-flood	TCP-пакеты с флагом FIN
Flood TCP/UDP	tcp-null-flood	TCP-пакеты без установленных флагов
Flood TCP/UDP	tcp-psh-flood	TCP-пакеты с флагом PSH
Flood TCP/UDP	tcp-rst-flood	TCP-пакеты с флагом RST
Flood TCP/UDP	tcp-urg-flood	TCP-пакеты с флагом URG
Flood TCP/UDP	udp-zero-payload-flood	UDP-пакеты без полезной нагрузки
Flood TCP/UDP	udp-big-packets-flood	UDP-пакеты размером 1498 байт и более
Amplification	apple-remote-desktop-amp	UDP-трафик с портом источника 3283
Amplification	chargen-amp	UDP-трафик с портом источника 19
Amplification	dns-amp	UDP-трафик с портом источника 53
Amplification	ibm-cics-amp	UDP-трафик с портом источника 1435
Amplification	ldap-amp	UDP-трафик с портом источника 389
Amplification	memcached-amp	UDP-трафик с портом источника 11211
Amplification	mssql-amp	UDP-трафик с портом источника 1434
Amplification	ntp-amp	UDP-трафик с портом источника 123
Amplification	snmp-amp	UDP-трафик с портом источника 161
Amplification	snmptrap-amp	UDP-трафик с портом источника 162
Amplification	ssdp-amp	UDP-трафик с портом источника 1900
Amplification	ws-discovery-amp	UDP-трафик с портом источника 3702

7.6.14Условие срабатывания

Условие	**Описание**

Порог (Threshold)	Статическое значение. Счётчик срабатывает при превышении заданного порога.
Прирост (Diff)	Абсолютная разница между двумя соседними интервалами измерения. Срабатывание происходит, если прирост превышает заданное значение.
Прирост % (Reldiff)	Относительная разница между соседними интервалами. Срабатывание происходит, если рост превышает заданный множитель или процент.

Для условия укажите единицу измерения: биты в секунду, байты в секунду или пакеты в секунду. Доступны соответствующие кратные единицы, например Mbit/s, MB/s и Kpps.

7.6.15Фильтрация

Для каждого счётчика можно выбрать отдельный способ обработки трафика после срабатывания.

Вариант	**Описание**
Без фильтрации	Аномалия фиксируется и отображается на дашборде и в отчётах. Маршрутизация и обработка трафика не изменяются.
Следующий хоп (next-hop)	Трафик перенаправляется на выбранный следующий хоп только для данного счётчика. Локальная настройка имеет отношение к конкретной аномалии.
FlowSpec-правило	При срабатывании используется выбранное FlowSpec-правило.

При выборе FlowSpec-правила доступны следующие действия:

- Создать новое правило — открыть редактор, задать параметры и сохранить правило
- Выбрать из списка — привязать существующее правило без изменений

- Дублировать и редактировать — создать копию существующего правила, изменить её и сохранить

7.7 Настройка CIDR-адресов объекта

CIDR-адрес — IP-адрес или IP-префикс, для которого FlowCollector выполняет анализ входящего трафика в соответствии с настройками объекта и заданными счётчиками.

7.7.1 Принцип работы

При поступлении трафика FlowCollector сравнивает IP-адрес назначения пакета с CIDR-адресами, указанными в объектах. По результату сравнения система определяет объект, в рамках которого необходимо выполнить дальнейший анализ трафика.

Внимание. Префикс 0.0.0.0/0 не поддерживается.

7.7.2 Добавление CIDR-адреса

Чтобы добавить CIDR-адрес объекту:

- Откройте раздел **Объекты.**
- Выберите нужный объект.
- Откройте вкладку **CIDR**.
- Нажмите значок +.
- Укажите IP-адрес или IP-префикс в формате CIDR, например 192.168.10.0/24.
- Нажмите **Добавить.**

После сохранения CIDR-адрес появится в списке объекта и будет использоваться при сопоставлении входящего трафика.

7.7.3 Удаление CIDR-адреса

Чтобы удалить CIDR-адрес:

- Откройте объект и перейдите на вкладку CIDR.
- Найдите нужную запись.
- Откройте меню дополнительных действий.
- Выберите **Удалить** и подтвердите действие.