ОБНОВЛЕНО 16 МАР

RLOG

Назначение модуля

Модуль RLOG предназначен для анализа HTTP-логов от внешних систем терминирующих TLS. На основании полей логов позволяет формировать правила фильтрации для блокировки IP-адресов источника,тем самым обеспечивая возможность фильтрации зашифрованного L7-трафика.

Принцип работы

RLOG принимает входящий поток логов с одного или нескольких источников. Каждый лог анализируется в соответствии с предварительно заданным шаблоном. Извлечённые данные (статус-код, IP-адрес источника, время отклика, virtual IP и т.д.) используются для расчёта метрик.

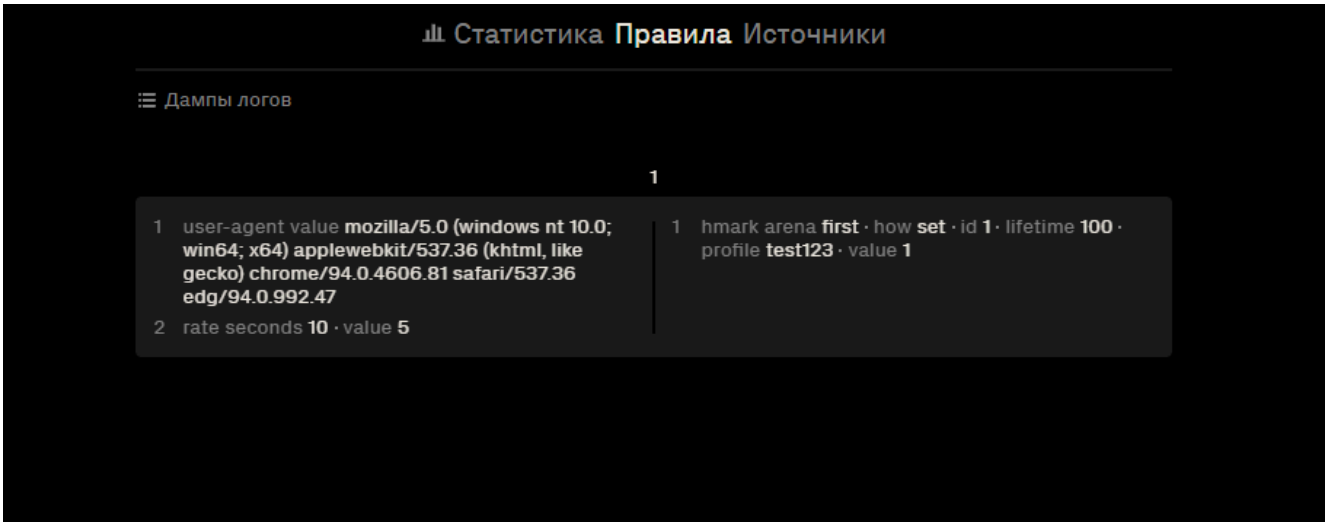
На основе этих метрик могут быть активированы правила, определяющие допустимую частоту запросов (rate limit) и иные условия. При нарушении условий источник помечается, и его IP-адрес передаётся в систему DosGate для блокировки в соответствии с параметрами текущего профиля (арена, метка и пр.).

Для применения фильтрации на уровне DosGate необходимо создать правило, использующее соответствующую метку (HMARK) — с заданным действием, например, сбросить пакет (drop). Без такого правила IP-адрес, переданный из RLOG, не будет заблокирован на уровне трафика.

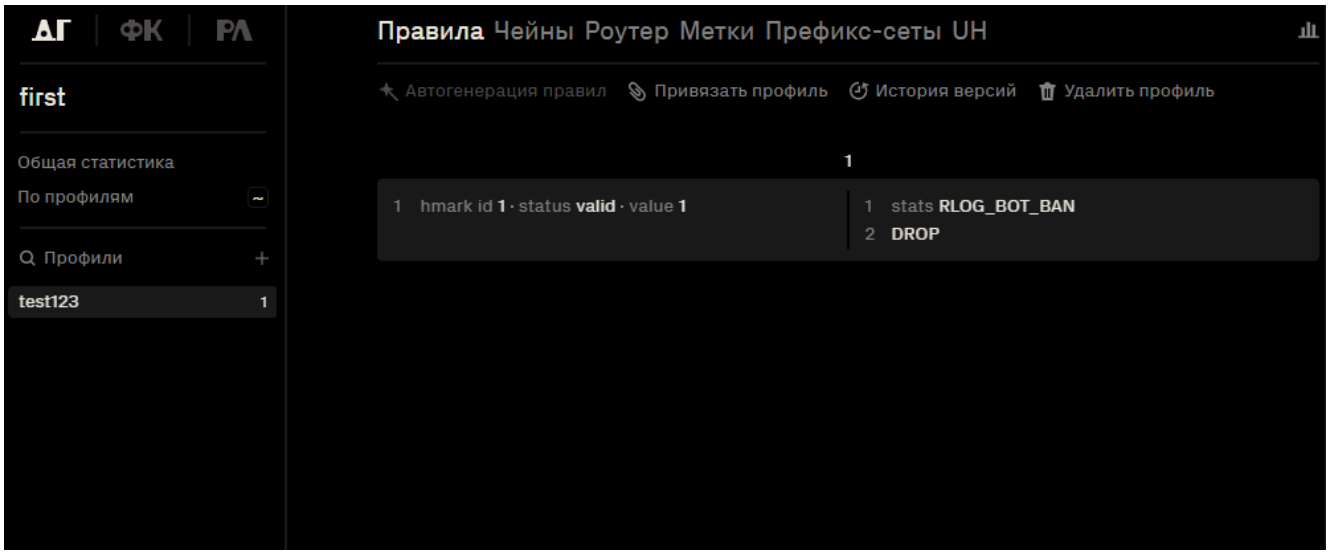
Принцип работы

1. Модуль RLOG осуществляет непрерывный мониторинг HTTP-логов, поступающих с устройств терминации TLS или балансировщиков нагрузки.
2. Система автоматически рассчитывает RPS (запросы в секунду) на основе количества поступающих логов.
3. Статистические данные собираются по выделенным профилям и в рамках правил фильтрации, созданных пользователем.
4. В соответствии с этими правилами RLOG вычисляет частотные характеристики запросов и выявляет отклонения от заданных пороговых значений.
5. При обнаружении нарушения пороговых значений система извлекает IP-адрес источника из заголовка, определённого пользователем.
6. Информация о потенциально опасном источнике передаётся в систему управления Spider.
7. Spider распространяет команды блокировки на все узлы DosGate, записывая данные о нарушителе в динамические таблицы профилей HMARK.

Пример работы RLOG с DosGate



Правило в **RLOG** отслеживает HTTP-запросы с определённым *User-Agent* и частотой более **5 запросов за 10 секунд**. При выполнении этих условий модуль присваивает IP-адресу временную метку **HMARK id 1, value 1**, сроком на **100 секунд** и передаёт её в **DosGate** — в арену *first* и профиль *test123*.



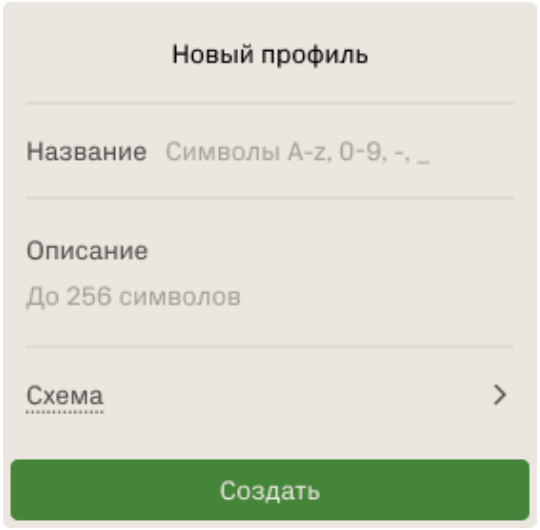
В **DosGate** настроено правило, реагирующее на наличие активной метки **HMARK id 1, value 1**. При наличии такой метки трафик от соответствующего IP-адреса блокируется действием **DROP**, а факт срабатывания фиксируется в счётчике **RLOG_BOT_BAN**. Таким образом обеспечивается автоматическая фильтрация подозрительных источников, выявленных на уровне логов.

Профиль

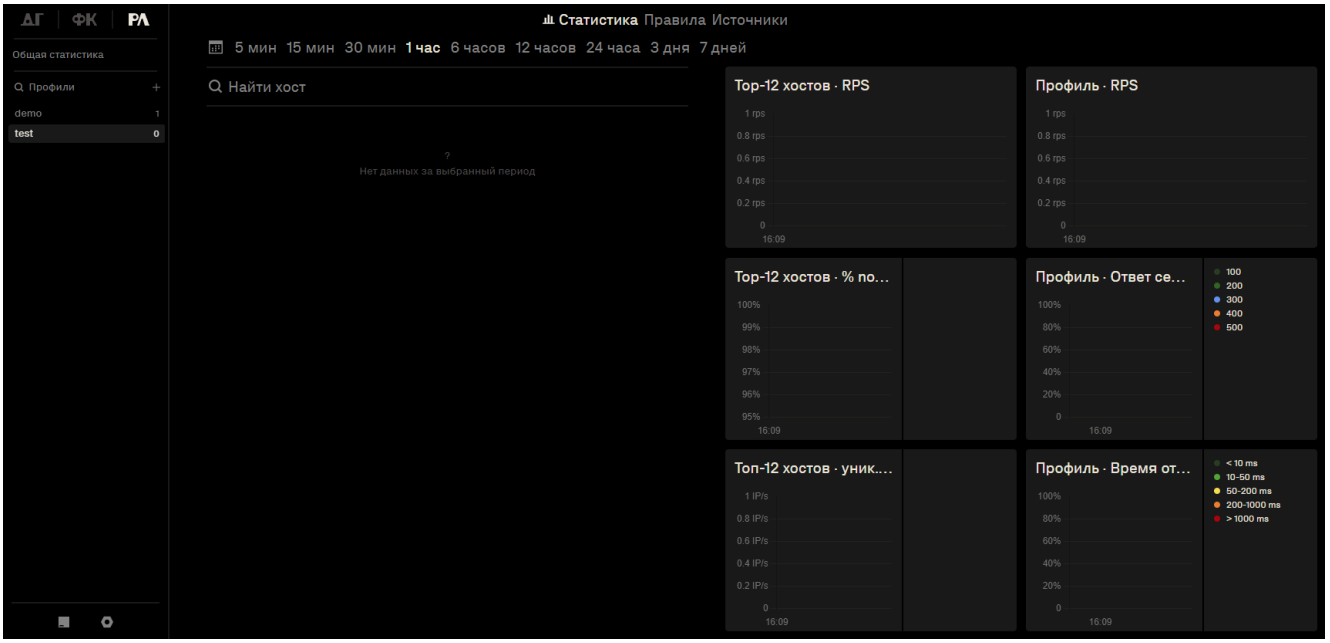
Создание профиля

Для создания нового профиля в системе выполнить следующие действия:

1. На главной странице в разделе **Профили** нажать кнопку "+".
2. Заполнить следующие поля для создания профиля:
   - **Название** - уникальное имя для профиля. Рекомендуется использовать комбинацию из обозначения сегмента инфраструктуры и названия сервиса, например, "zapadniy-filial-web".
   - **Описание** - краткое текстовое пояснение, которое поможет понять назначение профиля.
   - **Схема** - шаблон формата строк в логах. Определяет, как система будет разбирать поступающие журналы. После создания профиля изменить схему нельзя.
3. Нажать кнопку **Создать**.

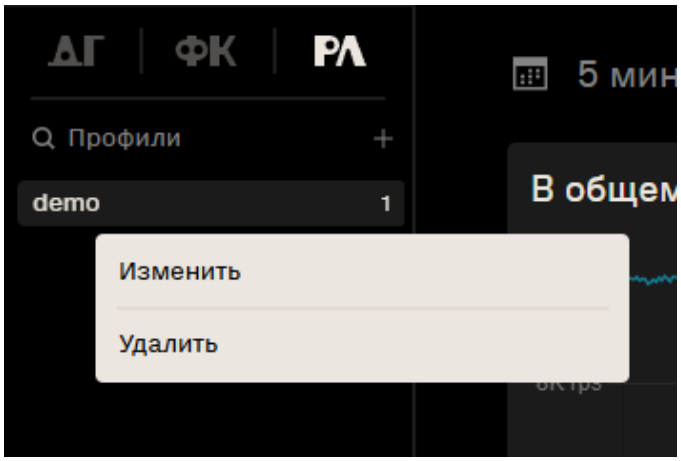


После создания профиля интерфейс переключится на страницу профиля.



Изменение профиля

Для изменения профиля необходимо нажать правой кнопкой мыши на его названии в общем списке профилей и выбрать пункт **Изменить**. Откроется окно, в котором можно изменить название и описание профиля.



Удаление профиля

Для удаления профиля необходимо нажать правой кнопкой мыши на его названии в общем списке профилей и выбрать пункт **Удалить**. После этого профиль будет безвозвратно удален из системы.

Статистика

Раздел **Статистика** предназначен для визуального мониторинга состояния трафика, поступающего в модуль RLOG в виде логов. Он позволяет выявлять потенциальные аномалии и источники нестандартного поведения на основе агрегации логов от разных хостов.

Навигация и фильтрация

- В верхней панели доступен выбор временного диапазона:
  5 мин, 15 мин, 30 мин, 1 час, 6 часов, 12 часов, 24 часа, 3 дня, 7 дней.
- Форма поиска по хосту — позволяет отфильтровать данные по доменному имени виртуального хоста.

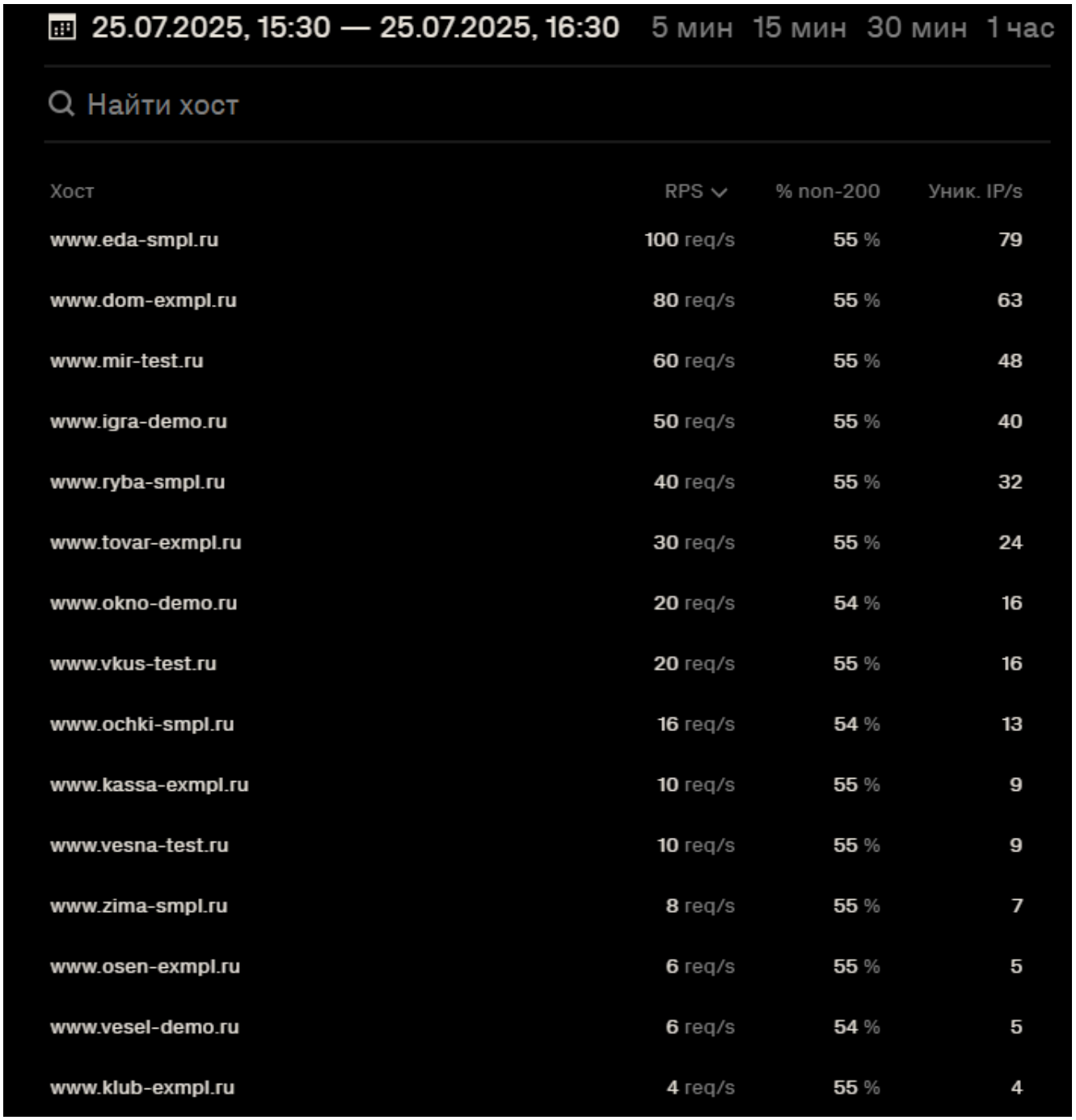


Таблица хостов

Отображается список хостов, по которым поступают HTTP-запросы.

Колонки таблицы:

- **Хост** — доменное имя виртуального хоста, извлечённое из логов.
- **RPS** — количество запросов в секунду, вычисляется как среднее значение за выбранный интервал.

- **% non-200** — процент ответов с HTTP-кодами, отличными от 200. Отражает долю ошибок и редиректов.
- **Уник. IP/s** — количество уникальных IP-адресов источников запросов в секунду.

Таблица поддерживает сортировку по каждому из столбцов. Для изменения порядка необходимо кликнуть по заголовку соответствующей колонки.

Графики

Top-12 хостов · RPS
Линейный график, отображающий интенсивность запросов по 12 наиболее активным хостам. Позволяет отследить пики и резкие изменения в трафике.

Top-12 хостов · % non-200
График показывает процент некорректных ответов (HTTP-коды, отличные от 200) по каждому из 12 наиболее активных хостов. Используется для выявления источников с высоким уровнем ошибок.

Top-12 хостов · Уник. IP/s
Отображает динамику количества уникальных IP-адресов, с которых поступают запросы. Является индикатором распределённости трафика или возможных сканирований.

Профиль · RPS
График суммарной нагрузки по запросам в секунду в рамках текущего выбранного профиля. Используется для мониторинга общего объёма входящего трафика.

Профиль · Ответ сервера
Диаграмма распределения ответов сервера по классам HTTP-кодов:

- 200 — успешные ответы.
- 300 — редиректы.
- 400 — ошибки клиента.
- 500 — ошибки сервера.
  Позволяет оценить качество работы приложения или выявить массовые сбои.

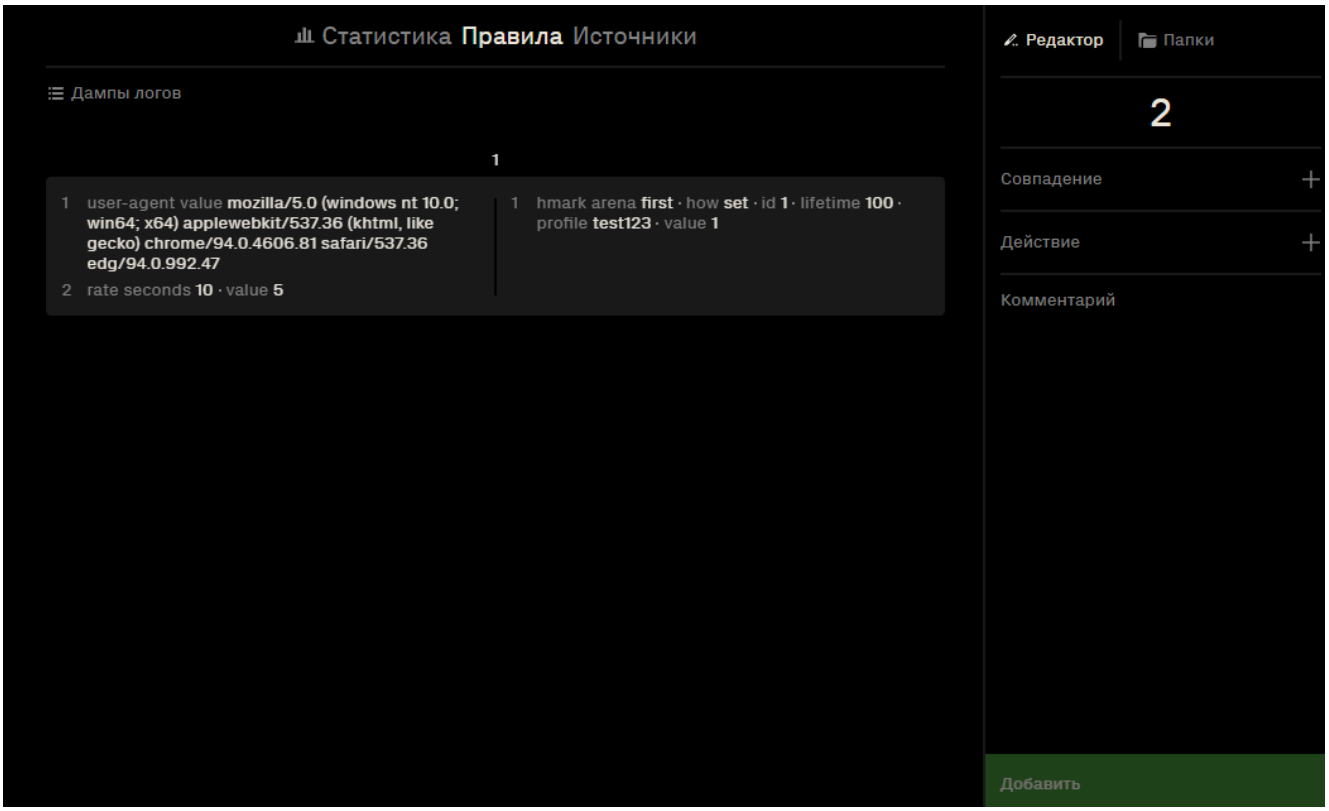
Профиль · Время ответа
Гистограмма распределения запросов по времени ответа сервера:

- менее 10 мс
- 10–50 мс
- 50–200 мс
- 200–1000 мс

- более 1000 мс
  Метрика отражает производительность backend-приложения и может сигнализировать о деградации.

Правила

Правила в системе RLOG создаются путем комбинирования совпадений и действий. Совпадения определяют условия, при которых правило срабатывает. Действия применяется, если условия совпадений выполнены.



Справа в интерфейсе расположена вкладка **Редактор**. В этой области задаются совпадения и действия. При необходимости можно добавить текстовый комментарий — он сохраняется вместе с правилом и используется для технических пометок или пояснений.

Справа находится вкладка **Папки**. В этой области можно вручную группировать правила по папкам для упрощения навигации и визуальной организации конфигурации.

Совпадения

Каждая проверка совпадения содержит один или несколько аргументов, настраиваемых пользователем. Для всех совпадений предусмотрена возможность включения флага **NOT**, реализованного в виде переключателя. **NOT** — логическая операция отрицания, при активации которой условие совпадения инвертируется: правило сработает для всех значений, кроме указанного.

Accept – Заголовок Accept

Параметр	Описание
value	Значение заголовка *Accept* (например, text/html).

Accept-Encoding – Заголовок Accept-Encoding

Параметр	Описание
value	Значение заголовка *Accept-Encoding* (например, gzip).

Accept-Language – Заголовок Accept-Language

Параметр	Описание
value	Значение заголовка *Accept-Language* (например, RU).

BIGIP_CACHED – Геолокация клиента

Используется код страны, полученный из внешних логов.

Параметр	Описание
CN	Китай
RU	Российская Федерация
TW	Тайвань (провинция Китая)
US	Соединённые Штаты Америки

Полный список кодов и стран

Параметр	Описание
CN	Китай
RU	Российская Федерация
TW	Тайвань (провинция Китая)
US	Соединённые Штаты Америки
AD	Андорра
AE	Объединённые Арабские Эмираты
AF	Афганистан
AG	Антигуа и Барбуда
AI	Ангилья
AL	Албания
AM	Армения
AO	Ангола
AQ	Антарктида

Параметр	Описание
AR	Аргентина
AS	Американское Самоа
AT	Австрия
AU	Австралия
AW	Аруба
AX	Аландские острова
AZ	Азербайджан
BA	Босния и Герцеговина
BB	Барбадос
BD	Бангладеш
BE	Бельгия
BF	Буркина-Фасо
BG	Болгария
BH	Бахрейн
BI	Бурунди
BJ	Бенин
BL	Сен-Бартелеми
BM	Бермудские острова
BN	Бруней-Даруссалам
BO	Боливия
BQ	Бонайре, Синт-Эстатиус и Саба
BR	Бразилия
BS	Багамские Острова
BT	Бутан
BV	Остров Буве
BW	Ботсвана
BY	Беларусь
BZ	Белиз
CA	Канада
CC	Кокосовые (Килинг) острова
CD	Демократическая Республика Конго
CF	Центральноафриканская Республика
CG	Республика Конго
CH	Швейцария

Параметр	Описание
CI	Кот-д'Ивуар
CK	Острова Кука
CL	Чили
CM	Камерун
CO	Колумбия
CR	Коста-Рика
CU	Куба
CV	Кабо-Верде
CW	Кюрасао
CX	Остров Рождества
CY	Кипр
CZ	Чехия
DE	Германия
DJ	Джибути
DK	Дания
DM	Доминика
DO	Доминиканская Республика
DZ	Алжир
EC	Эквадор
EE	Эстония
EG	Египет
EH	Западная Сахара
ER	Эритрея
ES	Испания
ET	Эфиопия
FI	Финляндия
FJ	Фиджи
FK	Фолклендские (Мальвинские) острова
FM	Федеративные Штаты Микронезии
FO	Фарерские острова
FR	Франция
GA	Габон
GB	Великобритания
GD	Гренада

Параметр	Описание
GE	Грузия
GF	Французская Гвиана
GG	Гернси
GH	Гана
GI	Гибралтар
GL	Гренландия
GM	Гамбия
GN	Гвинея
GP	Гваделупа
GQ	Экваториальная Гвинея
GR	Греция
GS	Южная Георгия и Южные Сандвичевы острова
GT	Гватемала
GU	Гуам
GW	Гвинея-Бисау
GY	Гайана
HK	Гонконг
HM	Острова Херд и Макдональд
HN	Гондурас
HR	Хорватия
HT	Гаити
HU	Венгрия
ID	Индонезия
IE	Ирландия
IL	Израиль
IM	Остров Мэн
IN	Индия
IO	Британская территория в Индийском океане
IQ	Ирак
IR	Иран
IS	Исландия
IT	Италия
JE	Джерси
JM	Ямайка

Параметр	Описание
JO	Иордания
JP	Япония
KE	Кения
KG	Киргизия
KH	Камбоджа
KI	Кирибати
KM	Коморы
KN	Сент-Китс и Невис
KP	Корейская Народно-Демократическая Республика
KR	Республика Корея
KW	Кувейт
KY	Острова Кайман
KZ	Казахстан
LA	Лаос
LB	Ливан
LC	Сент-Люсия
LI	Лихтенштейн
LK	Шри-Ланка
LR	Либерия
LS	Лесото
LT	Литва
LU	Люксембург
LV	Латвия
LY	Ливия
MA	Марокко
MC	Монако
MD	Молдова
ME	Черногория
MF	Сен-Мартен (французская часть)
MG	Мадагаскар
MH	Маршалловы Острова
MK	Северная Македония
ML	Мали
MM	Мьянма

Параметр	Описание
MN	Монголия
MO	Макао
MP	Северные Марианские острова
MQ	Мартиника
MR	Мавритания
MS	Монтсеррат
MT	Мальта
MU	Маврикий
MV	Мальдивы
MW	Малави
MX	Мексика
MY	Малайзия
MZ	Мозамбик
NA	Намибия
NC	Новая Каледония
NE	Нигер
NF	Остров Норфолк
NG	Нигерия
NI	Никарагуа
NL	Нидерланды
NO	Норвегия
NP	Непал
NR	Науру
NU	Ниуэ
NZ	Новая Зеландия
OM	Оман
PA	Панама
PE	Перу
PF	Французская Полинезия
PG	Папуа — Новая Гвинея
PH	Филиппины
PK	Пакистан
PL	Польша
PM	Сен-Пьер и Микелон

Параметр	Описание
PN	Питкэрн
PR	Пуэрто-Рико
PS	Палестина
PT	Португалия
PW	Палау
PY	Парагвай
QA	Катар
RE	Реюньон
RO	Румыния
RS	Сербия
RW	Руанда
SA	Саудовская Аравия
SB	Соломоновы Острова
SC	Сейшельские Острова
SD	Судан
SE	Швеция
SG	Сингапур
SH	Острова Святой Елены, Вознесения и Тристан-да-Кунья
SI	Словения
SJ	Шпицберген и Ян-Майен
SK	Словакия
SL	Сьерра-Леоне
SM	Сан-Марино
SN	Сенегал
SO	Сомали
SR	Суринам
SS	Южный Судан
ST	Сан-Томе и Принсипи
SV	Сальвадор
SX	Синт-Мартен (нидерландская часть)
SY	Сирия
SZ	Эсватини
TC	Острова Тёркс и Кайкос
TD	Чад

Параметр	Описание
TF	Французские Южные и Антарктические Территории
TG	Того
TH	Таиланд
TJ	Таджикистан
TK	Токелау
TL	Восточный Тимор
TM	Туркменистан
TN	Тунис
TO	Тонга
TR	Турция
TT	Тринидад и Тобаго
TV	Тувалу
TZ	Танзания
UA	Украина
UG	Уганда
UM	Внешние малые острова США
UY	Уругвай
UZ	Узбекистан
VA	Ватикан
VC	Сент-Винсент и Гренадины
VE	Венесуэла
VG	Британские Виргинские острова
VI	Виргинские острова (США)
VN	Вьетнам
VU	Вануату
WF	Уоллис и Футуна
WS	Самоа
XK	Косово
YE	Йемен
YT	Майотта
ZA	Южно-Африканская Республика
ZM	Замбия
ZW	Зимбабве

CLIENT_IP – IP-адрес клиента

Параметр	Описание
ip	IP-адрес клиента (например, 192.168.74.164).

CLIENT_PORT – Порт клиента

Параметр	Описание
port	Номер порта клиента (диапазон от 0 до 65535).

DATE_DD – День запроса

Параметр	Описание
value	День месяца в формате *DD* (от 01 до 31).

DATE_MM – Месяц запроса

Параметр	Описание
value	Месяц в формате *MM* (от 01 до 12).

DATE_YYYY – Год запроса

Параметр	Описание
value	Год в формате *YYYY* (например, 2025).

Host – Заголовок Host

Параметр	Описание
value	Значение заголовка *Host* (например, 127.0.0.1).

HTTP_KEEPALIVE – Признак Keep-Alive

Параметр	Описание
status	Признак наличия заголовка *Connection: keep-alive*.

HTTP_REQUEST – Полный HTTP-запрос

Параметр	Описание
request	Полная строка запроса в формате `$METHOD $URI $VERSION`.

HTTP_STATCODE – HTTP-статус ответа

Параметр	Описание
status	Код статуса HTTP-ответа (например, 200, 403, 500).

ISO_CODE – Код страны по GeoIP

Геолокация вычисляется системой самостоятельно на основе IP-адреса клиента с использованием встроенной базы GeoIP.

Параметры и описание совпадают с описанием BIGIP_CACHED

RATE – Частота срабатываний

Параметр	Описание
seconds	Период времени в секундах, за который измеряется количество срабатываний.
value	Количество срабатываний за указанный период.

Referer – Заголовок Referer

Параметр	Описание
value	Значение заголовка *Referer* (например, localhost).

RESPONSE_MSECS – Время ответа

Параметр	Описание
value	Время ответа сервера в миллисекундах.

RESPONSE_SIZE – Размер ответа

Параметр	Описание
value	Размер тела ответа в байтах.

SERVER_IP – IP-адрес сервера

Параметр	Описание
ip	IP-адрес сервера, который обработал запрос.

SERVER_PORT – Порт сервера

Параметр	Описание
port	Номер порта сервера (диапазон от 0 до 65535).

TIME_HH24 – Час запроса (24-часовой формат)

Параметр	Описание
value	Час запроса в формате **HH** (от 00 до 23).

TIME_MM – Минута запроса

Параметр	Описание
value	Минута запроса в формате **MM** (от 00 до 59).

TIME_MSECS – Время запроса в миллисекундах

Параметр	Описание
value	Количество миллисекунд, прошедших с начала секунды.

TIME_SS – Секунда запроса

Параметр	Описание
value	Секунда запроса в формате **SS** (от 00 до 59).

User-Agent – Заголовок User-Agent

Параметр	Описание
value	Полное значение заголовка *User-Agent* (например, *Mozilla/5.0 ...*).

VIRTUAL_IP – Виртуальный IP-адрес

Параметр	Описание
ip	IP-адрес, на который был направлен запрос (виртуальный адрес сервиса).

VIRTUAL_PORT – Виртуальный порт

Параметр	Описание
port	Номер порта, к которому был направлен запрос (диапазон от 0 до 65535).

X-Forwarded-For – Заголовок X-Forwarded-For

Параметр	Описание
value	IP-адрес клиента, переданный через прокси в заголовке *X-Forwarded-For*.

X-Requested-With – Заголовок X-Requested-With

Параметр	Описание
value	Значение заголовка *X-Requested-With* (например, *XMLHttpRequest*).

Действие

HMARK

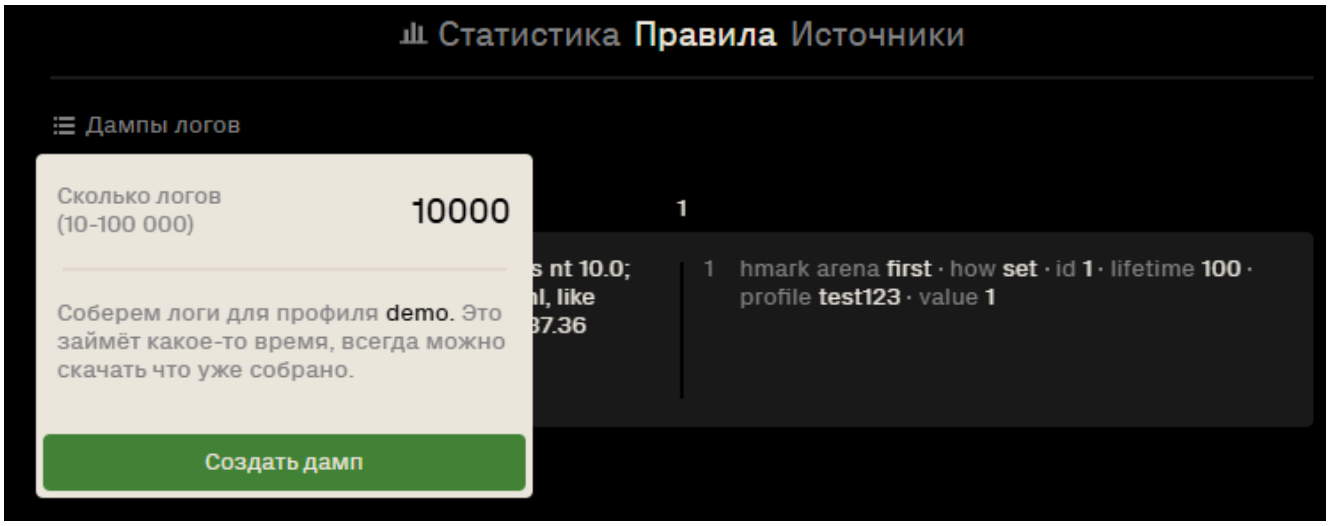
Устанавливает или модифицирует метку для IP-отправителя на основе заданной операции и параметров. Применяется для маркировки пакетов с целью дальнейшей классификации или маршрутизации.

Параметр	Варианты	Описание
id		Идентификатор метки (диапазон от 1 до 255).
how		Действие, выполняемое с меткой:
	add	прибавить значение.
	and	побитовая операция AND.
	dec	уменьшить значение на 1.
	div	разделить на указанное значение.
	inc	увеличить значение на 1.

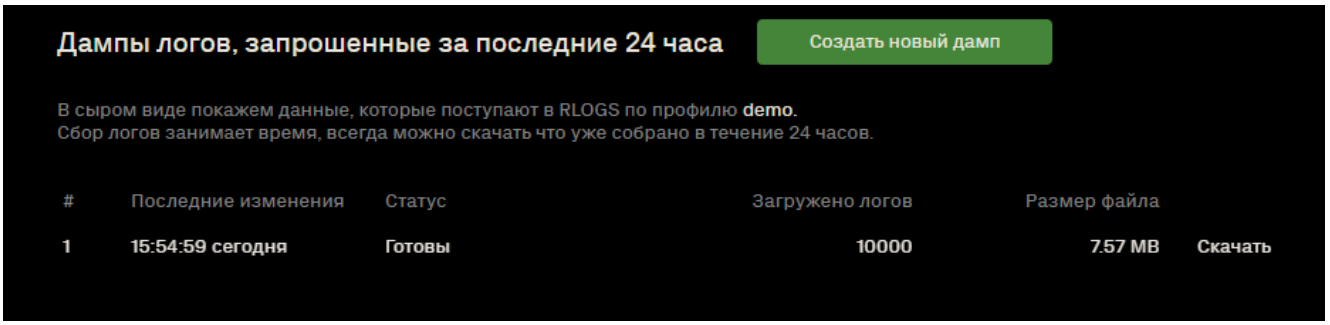
Параметр	Варианты	Описание
	mult	умножить на указанное значение.
	not	побитовая инверсия.
	or	побитовая операция OR.
	restore	восстановить метку сети из общей метки.
	save	сохранить сетевую метку в общую метку.
	set	установить заданное значение.
	sub	вычесть значение.
	xor	побитовая операция XOR.
value		Числовое значение 0 до 2^{32}-1
lifetime		Время жизни метки в секундах. Если не указано или равно 0 — метка считается постоянной.
arena		Имя арены DosGate, к которой относится метка.
profile		Имя профиля DosGate, в рамках которого применяется метка.

Дампы логов

Функция позволяет выгрузить в текстовом виде «сырые» данные, поступающие в модуль RLOG по выбранному профилю.



Кнопка **Создать дамп** запускает процесс выгрузки HTTP-логов по активному профилю. Объём дампа указывается вручную и может составлять от 10 до 100 000 записей. В выгрузку попадают «сырые» логи — без обработки, в том виде, в котором они поступили в систему. Сформированный дамп доступен для скачивания в течение 24 часов после создания.



Сбор логов может занять некоторое время. Уже собранные данные можно скачать сразу, не дожидаясь завершения всей выборки.

Источники

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

Список служит фильтром: если адрес отправителя лога не входит ни в один из указанных диапазонов, лог не обрабатывается.

Механизм аналогичен «роутерам» в DosGate — используется для определения, к какому профилю привязать входящие данные. Допускается использование как отдельных IP, так и сетей с масками. Для каждого источника можно добавить комментарий.