# NetFlowMan G4.1

## ЧЕТВЕРТОЕ ПОКОЛЕНИЕ РЕШЕНИЙ
## Программный Комплекс “Центральный Пульт”

АВГУСТ 2026

# Бизнес зависит от сети, но не видит, что в ней происходит

Компания теряет деньги и производительность, потому что никто не понимает, чем реально загружена сеть и какие сервисы создают проблемы

Организации переплачивают за каналы связи и оборудование, потому что не видят реальную структуру и потребление трафика

Когда сеть или цифровые сервисы начинают работать медленно, ИТ-команда часто не может быстро определить источник проблемы: пользователи недовольны, а бизнес простаивает

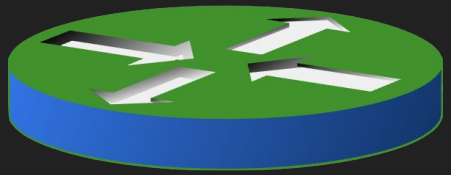
Без анализа сетевого трафика инфраструктура становится «чёрным ящиком»: сложно выявлять перегрузки, утечки данных, неэффективное использование каналов и скрытые угрозы

Любая проблема в сети превращается в долгий поиск виновника между ИТ, безопасностью, операторами связи и подрядчиками.

# Решение NetFlowMan

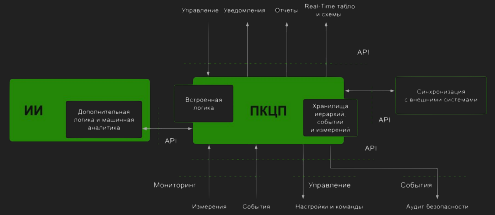
Аналитика NetFlow позволяет видеть фактическое поведение сети и приложений, быстро находить причины деградации сервисов, контролировать использование каналов и выявлять аномальный или нежелательный трафик

Оборудование IP-сети отдает
NetFlow v5, v9
IPFIX
NetStream
sFlow v4, v5



Решение NetFlowMan является подсистемой Программного Комплекса “Центральный Пульт” объединяющего развитые механизмы сетевого, системного и прикладного мониторинга, управляемого и журналируемого доступа

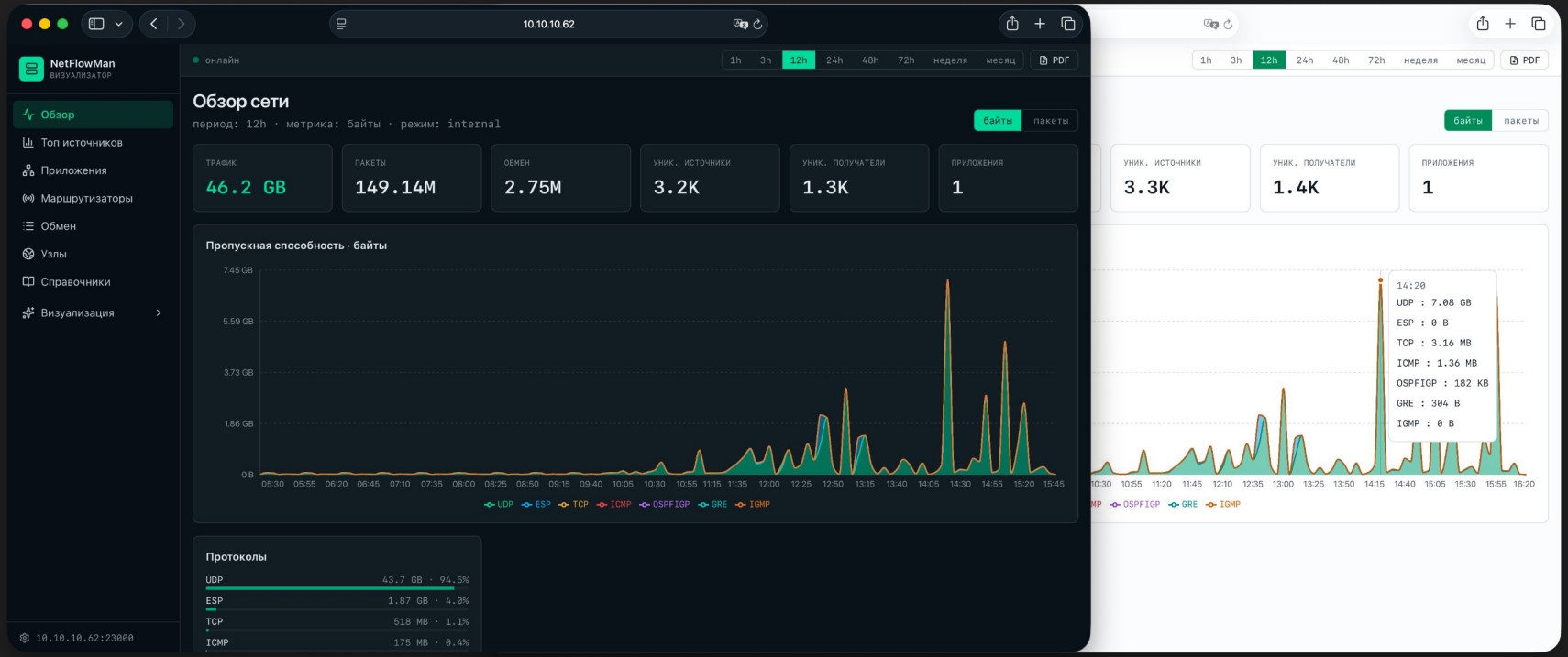
Решение обеспечивает
Долгосрочную аналитику
Обогащение
Топологию



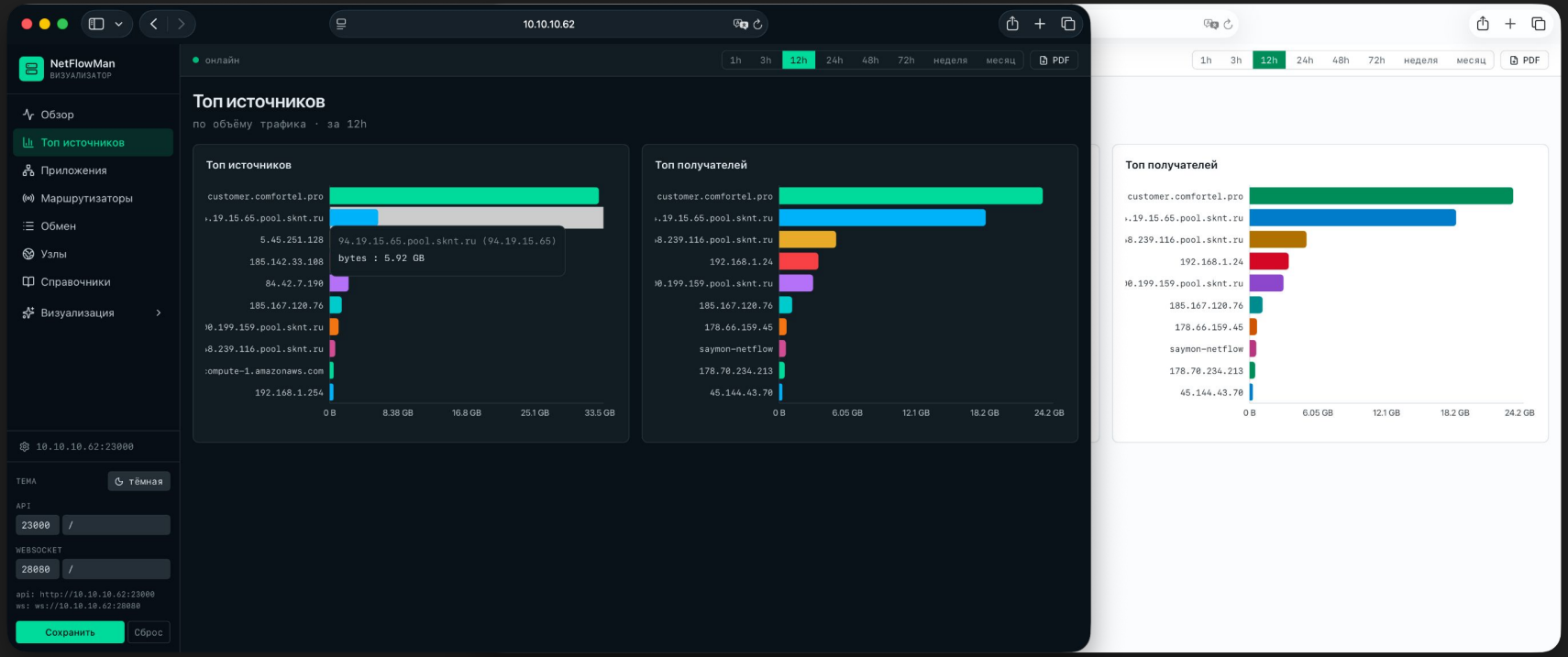
# Архитектура – как работает

streaming-данных
сетевые, системные и корпоративные структуры данных
включение в системы клиента
машинный анализ

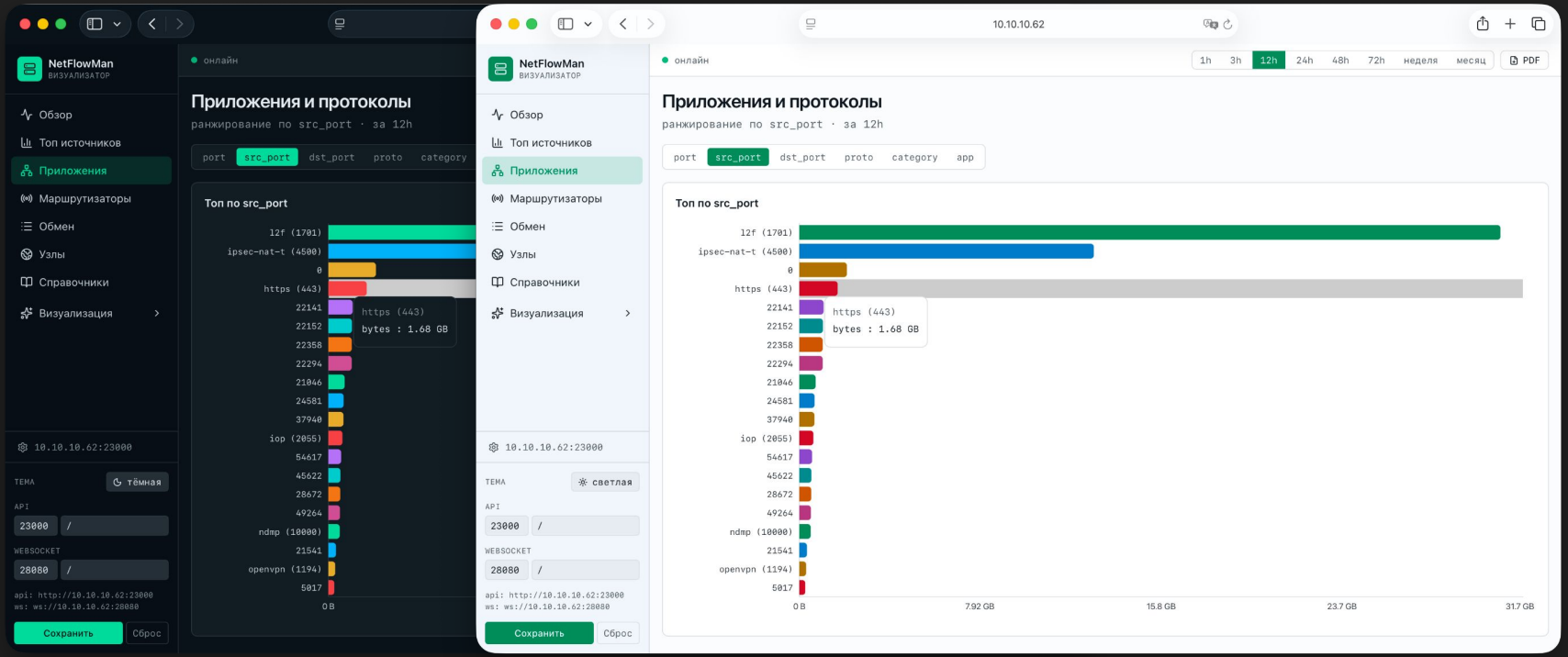
# Обзор сети


10.10.10.62
NetFlowMan
ВИЗУАЛИЗАТОР
онлайн
1h 3h 12h 24h 48h 72h неделя месяц
PDF
Обзор
Топ источников
Приложения
Маршрутизаторы
Обмен
Узлы
Справочники
Визуализация
Обзор сети
период: 12h · метрика: байты · режим: internal
байты пакеты
ТРАФИК 46.2 GB
ПАКЕТЫ 149.14M
ОБМЕН 2.75M
УНИК. ИСТОЧНИКИ 3.2K
УНИК. ПОЛУЧАТЕЛИ 1.3K
ПРИЛОЖЕНИЯ 1
Пропускная способность · байты
7.45 GB
5.59 GB
3.73 GB
1.86 GB
0 B
UDP ESP TCP ICMP OSPFIGP GRE IGMP
Протоколы
UDP 43.7 GB · 94.5%
ESP 1.87 GB · 4.0%
TCP 518 MB · 1.1%
ICMP 175 MB · 0.4%
10.10.10.62:23000
УНИК. ИСТОЧНИКИ 3.3K
УНИК. ПОЛУЧАТЕЛИ 1.4K
ПРИЛОЖЕНИЯ 1
14:20
UDP : 7.08 GB
ESP : 0 B
TCP : 3.16 MB
ICMP : 1.36 MB
OSPFIGP : 182 KB
GRE : 304 B
IGMP : 0 B

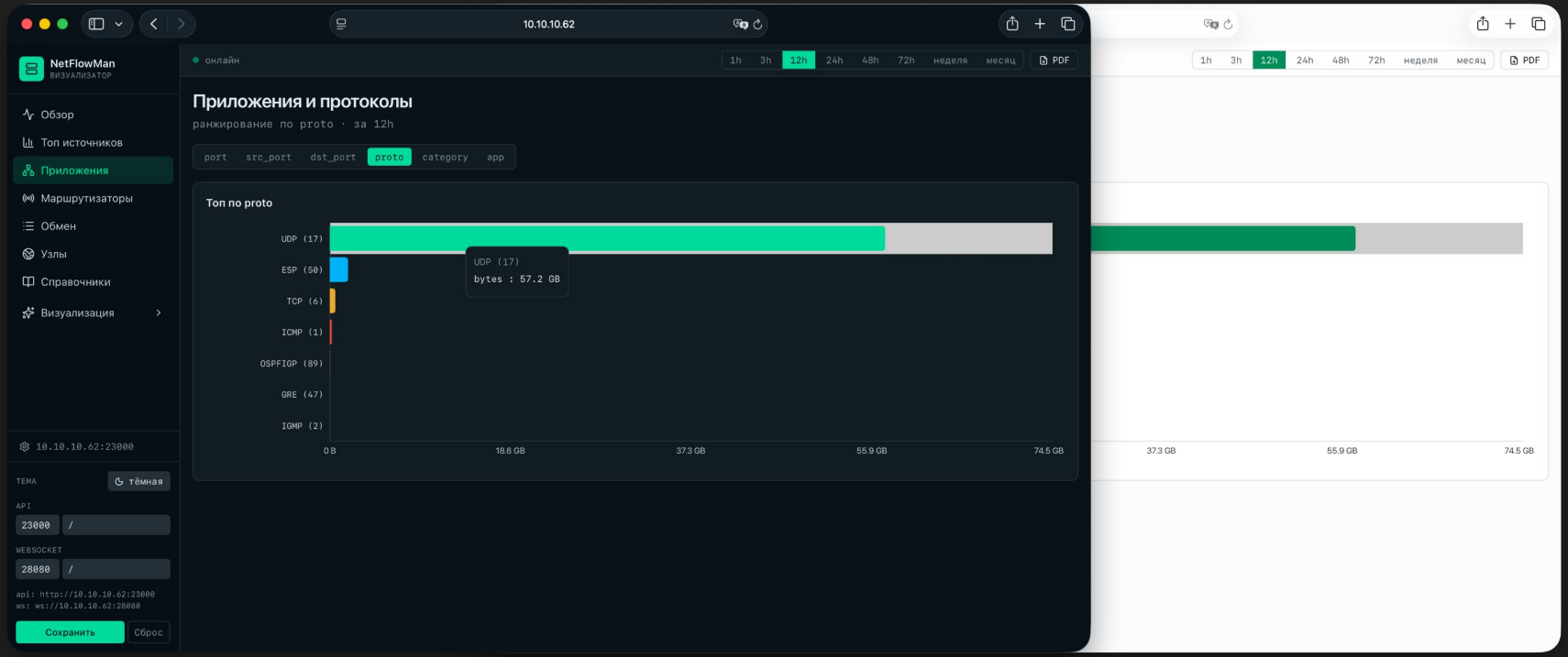
# Наиболее активные узлы сети



# Рейтинг сетевых протоколов

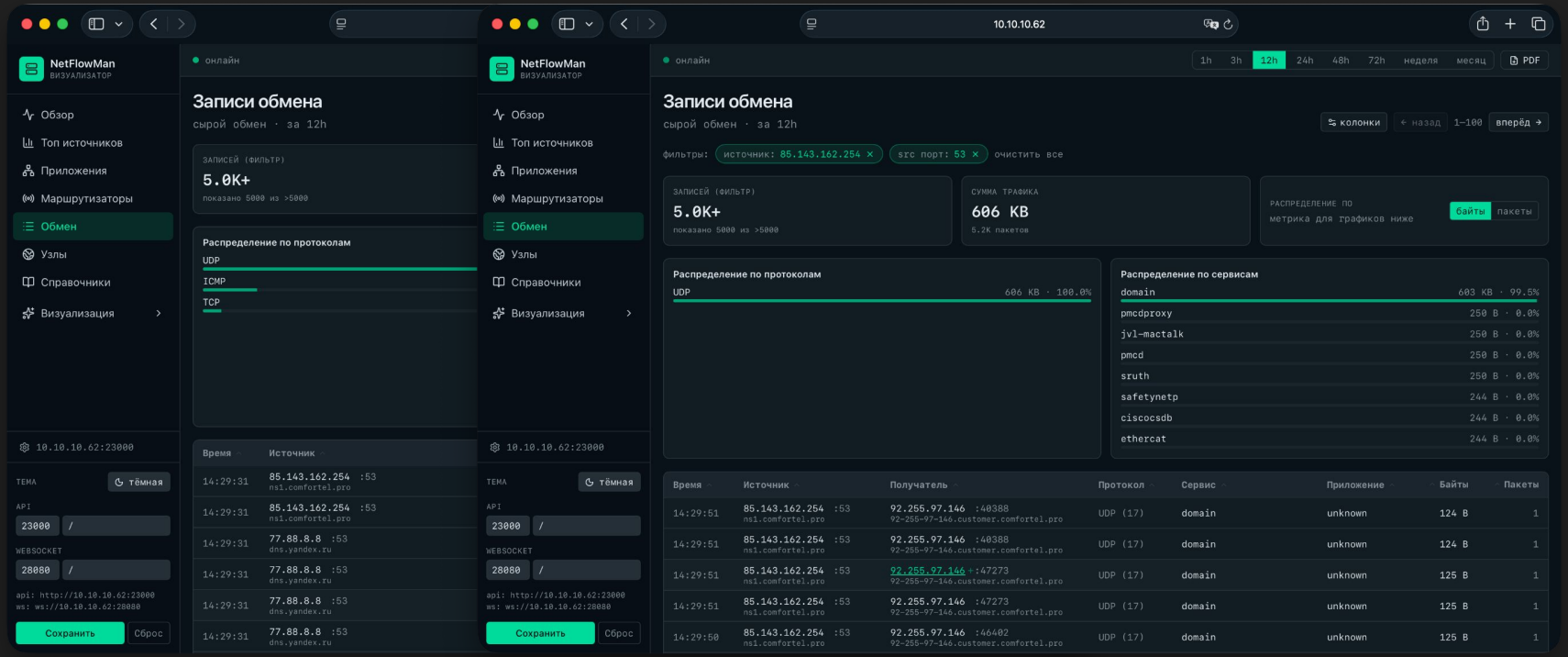


# Активность по типам трафика

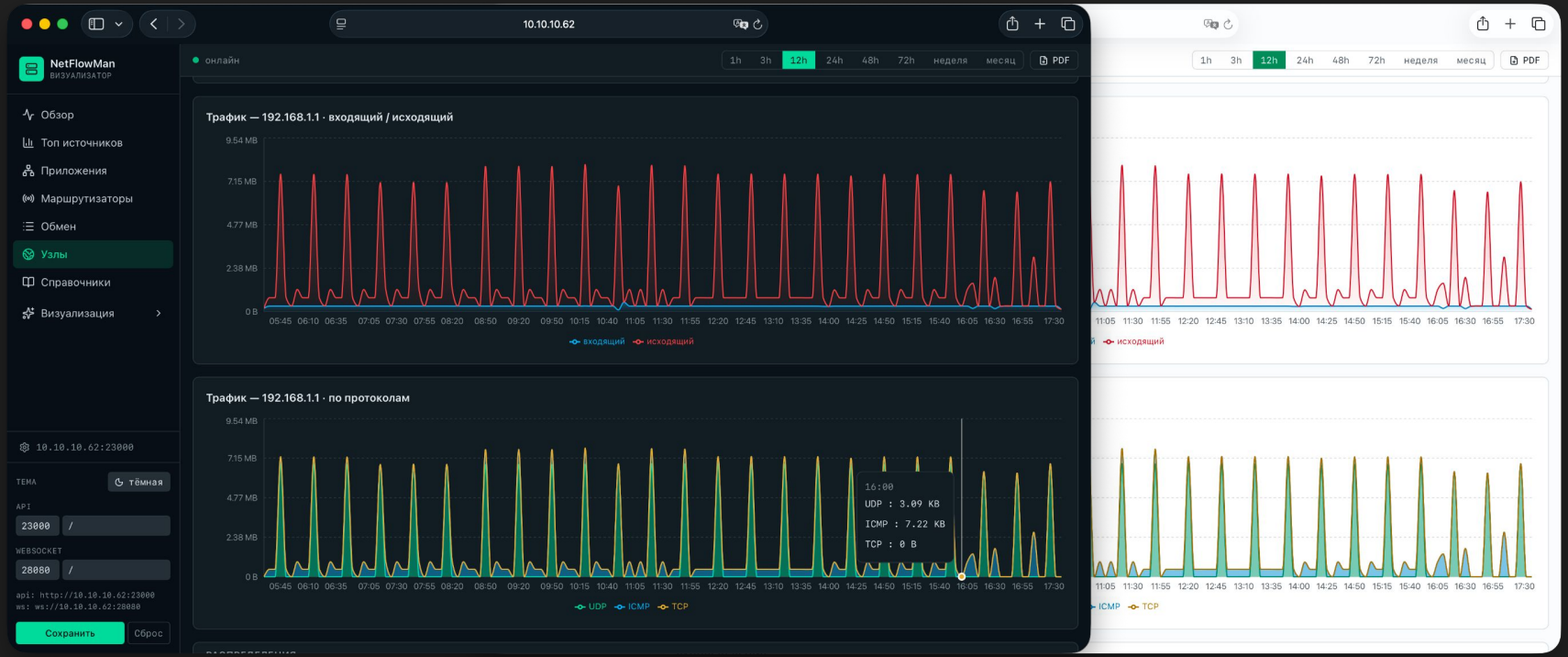


# Активность на маршрутизаторах – донорах данных

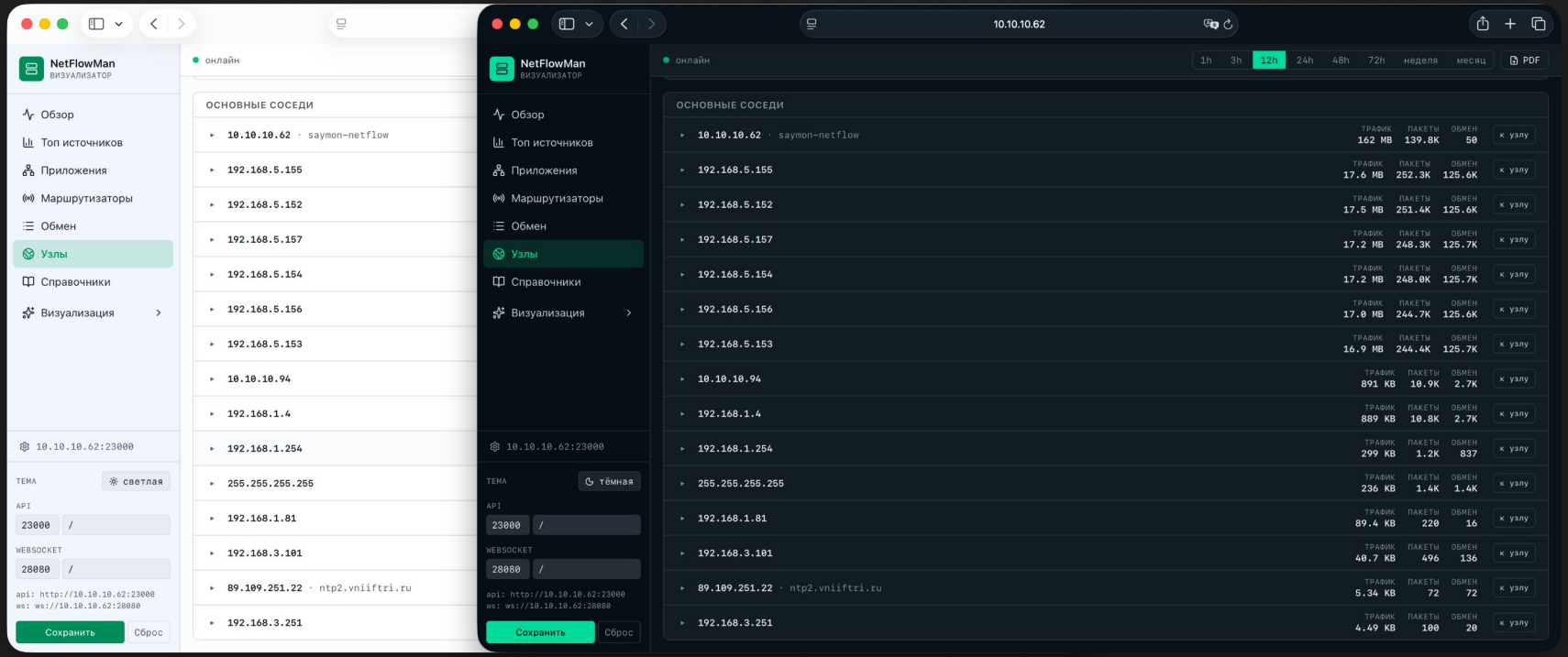
# Подробный анализ трафика



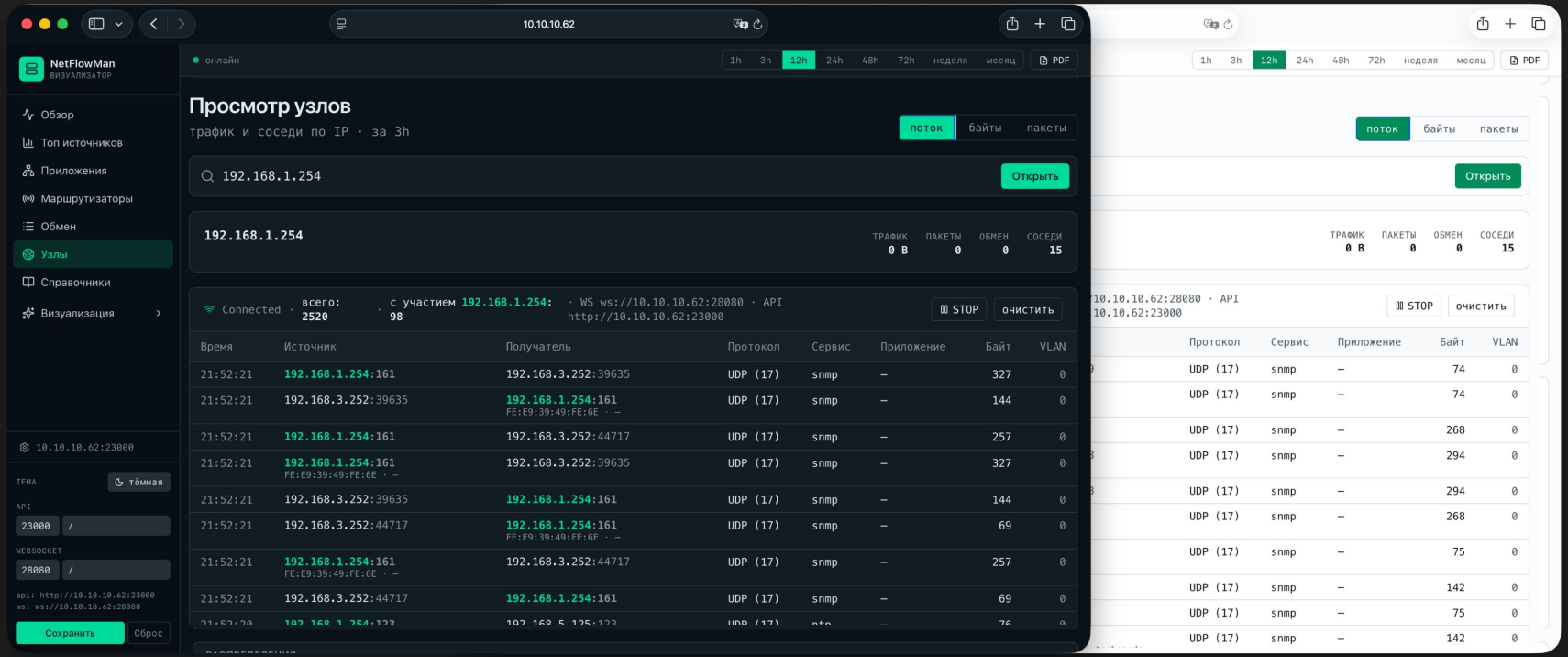
# Индикация активности узлов



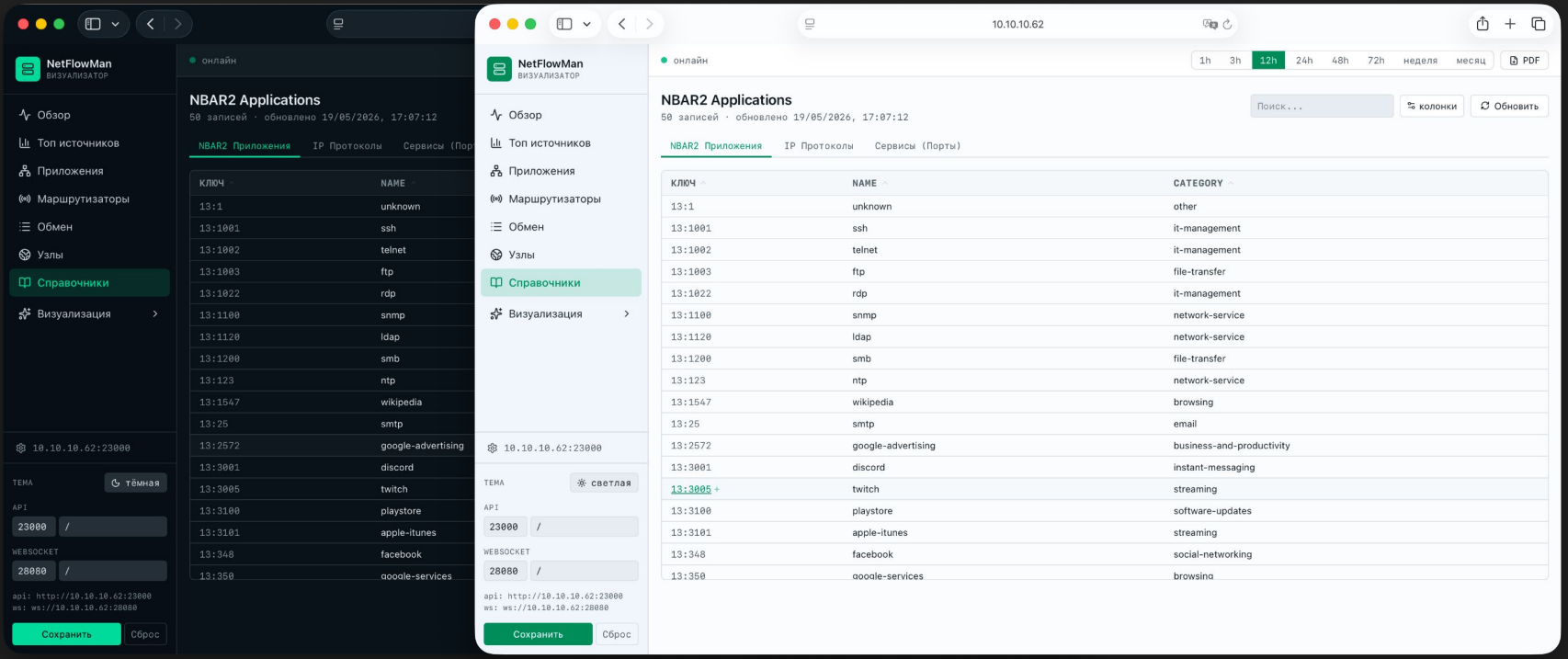
# Партнеры узла по обмену трафиком



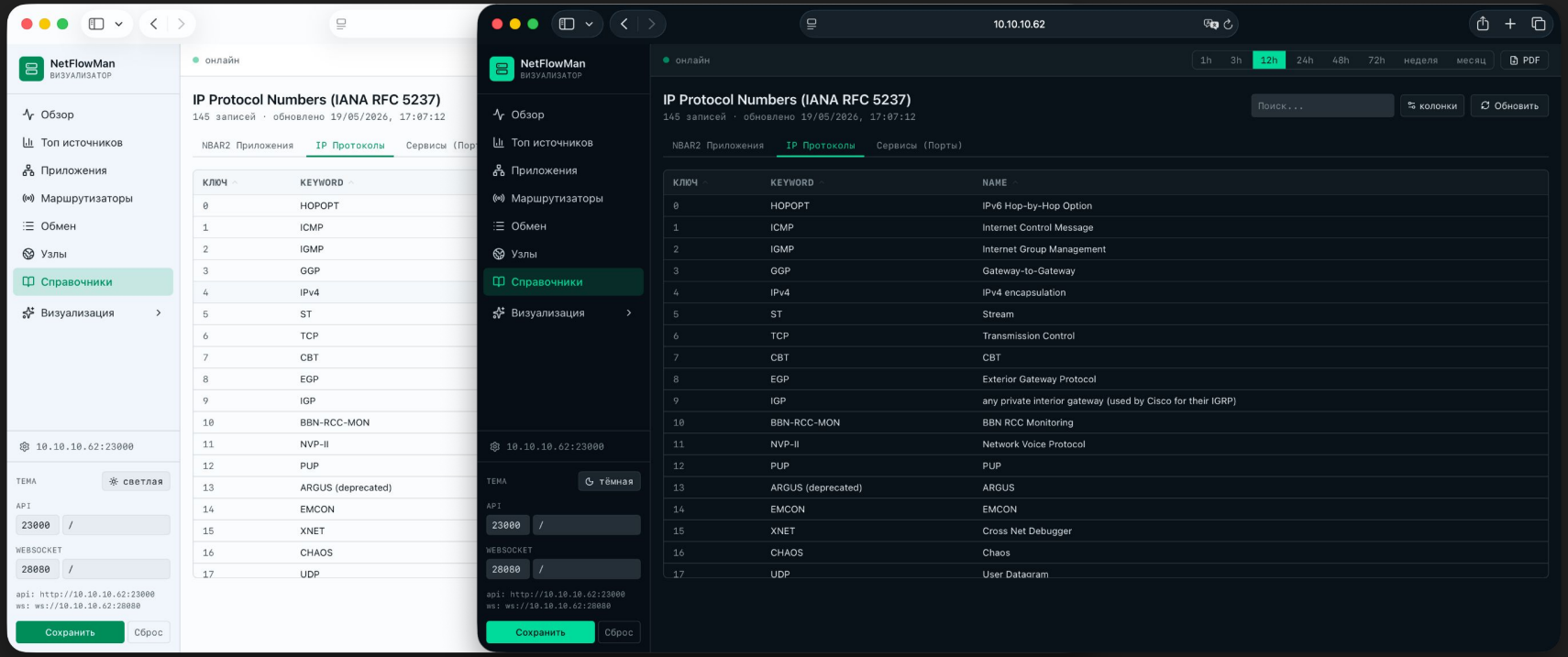
# Живой поток с сетевого устройства в web-консоль



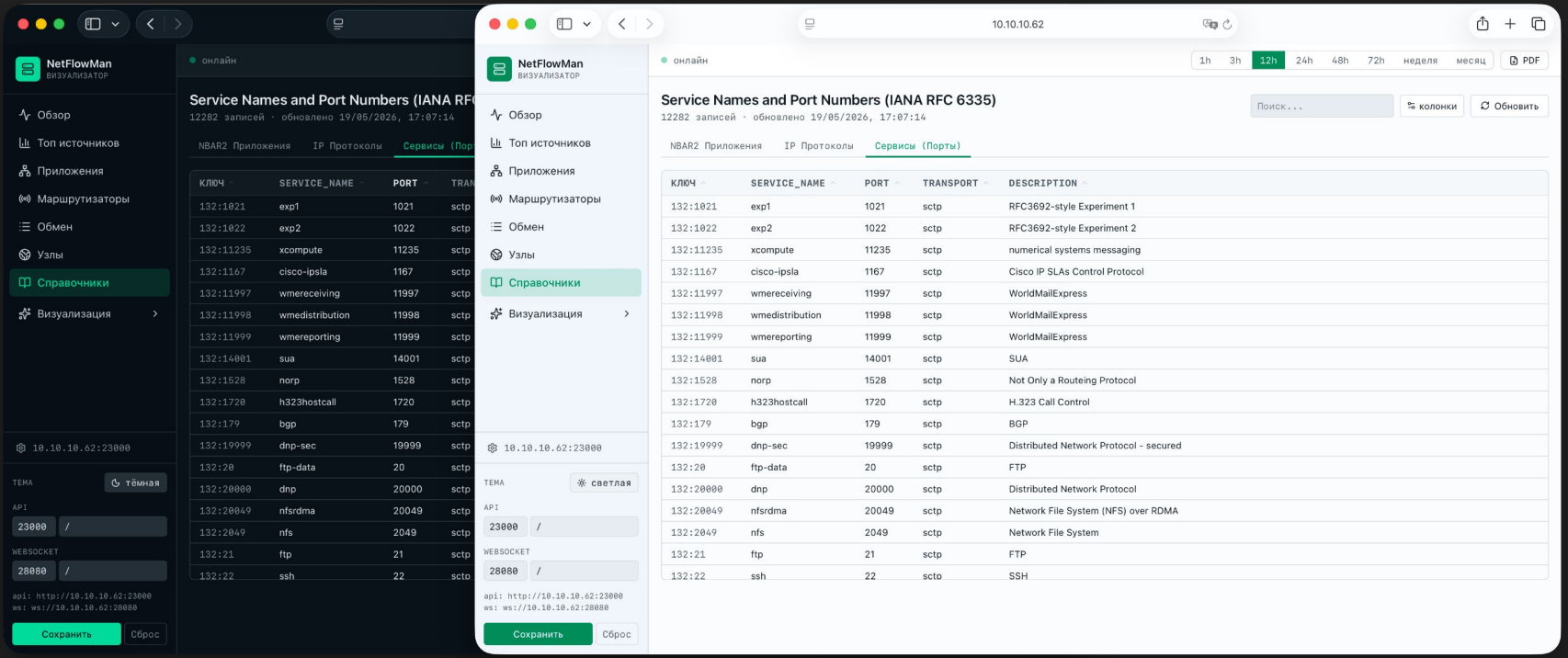
# Справочники приложений



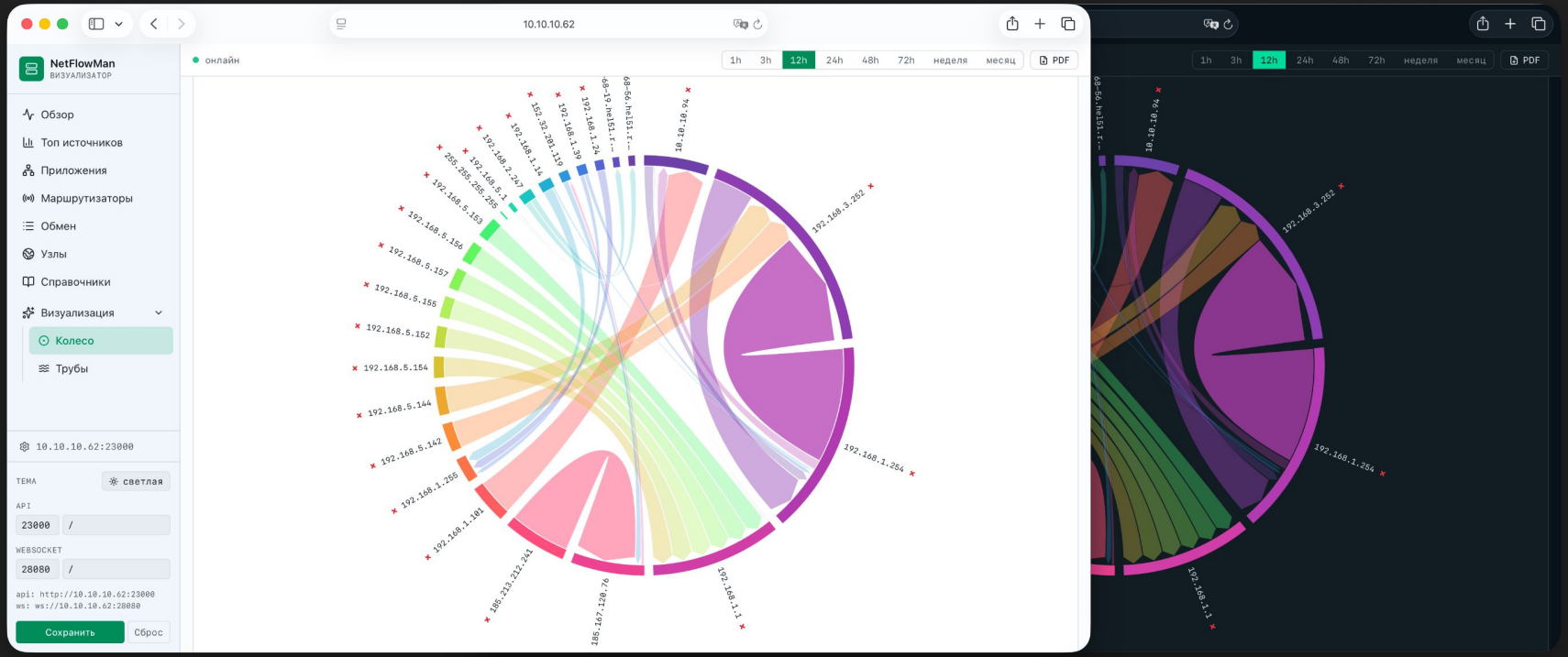
# Справочники портов



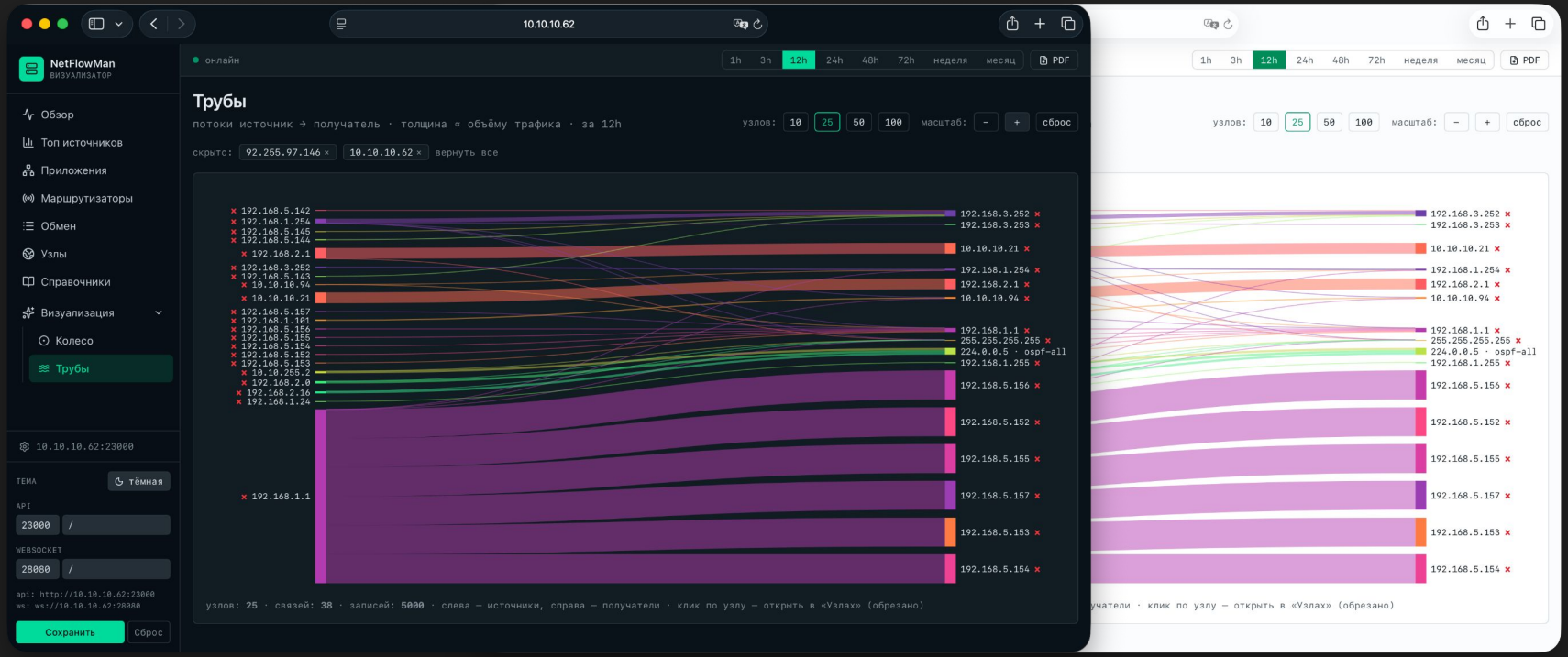
# Справочники сетевых сервисов



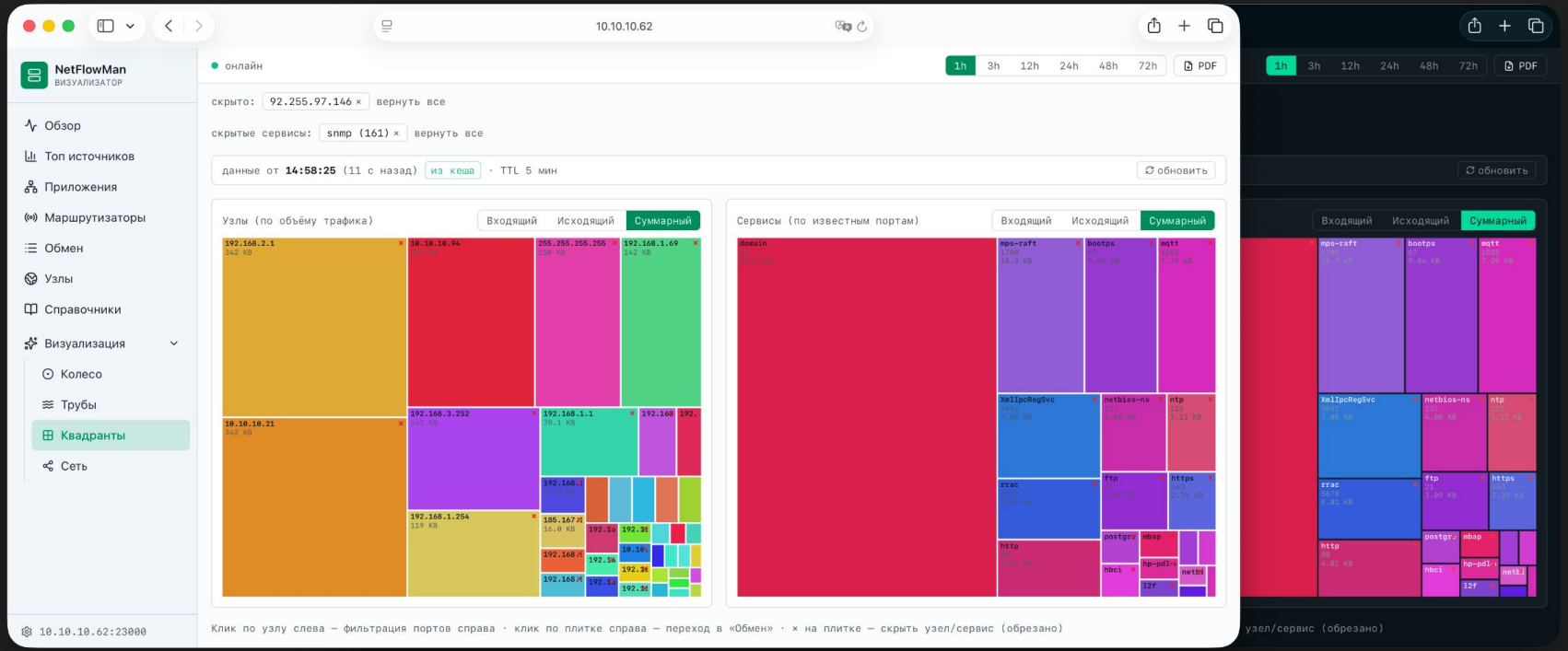
# Интерактивные круговые карты обмена трафиком



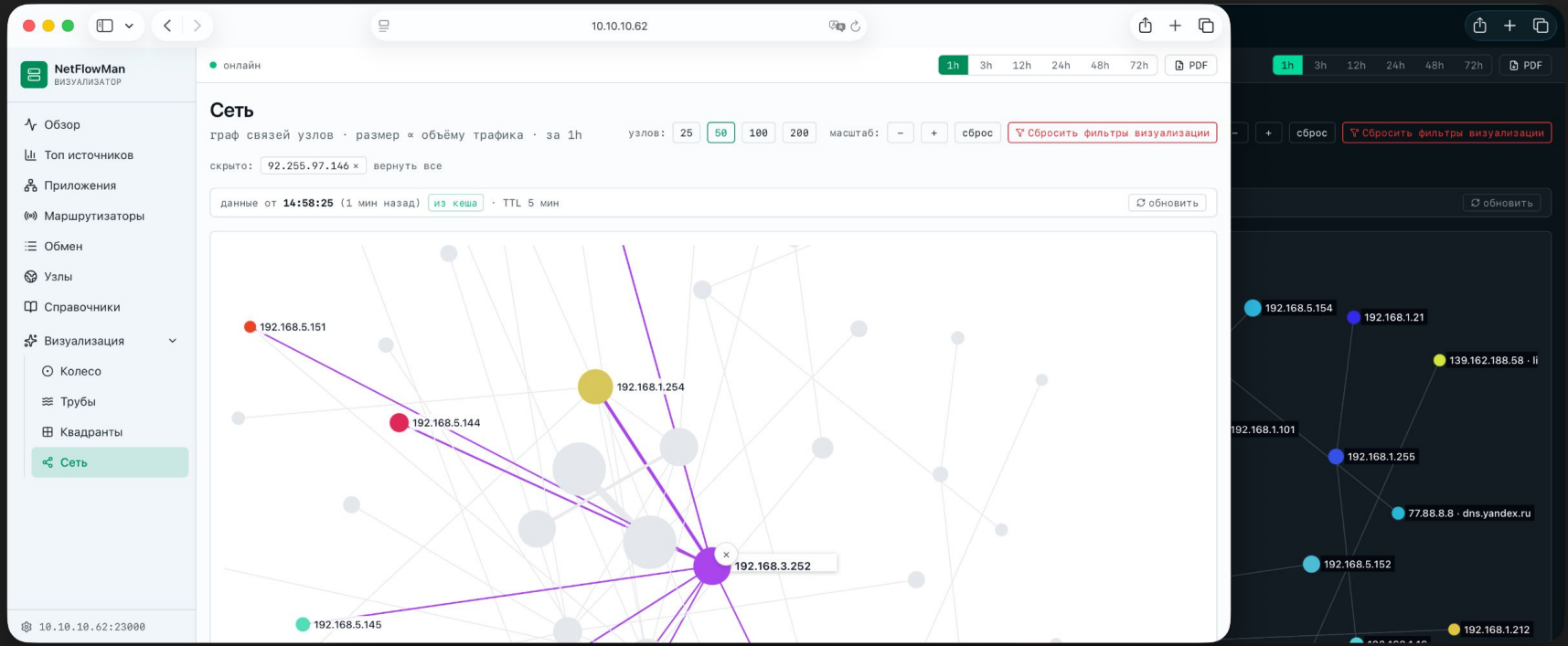
# Развернутые интерактивные карты потоков



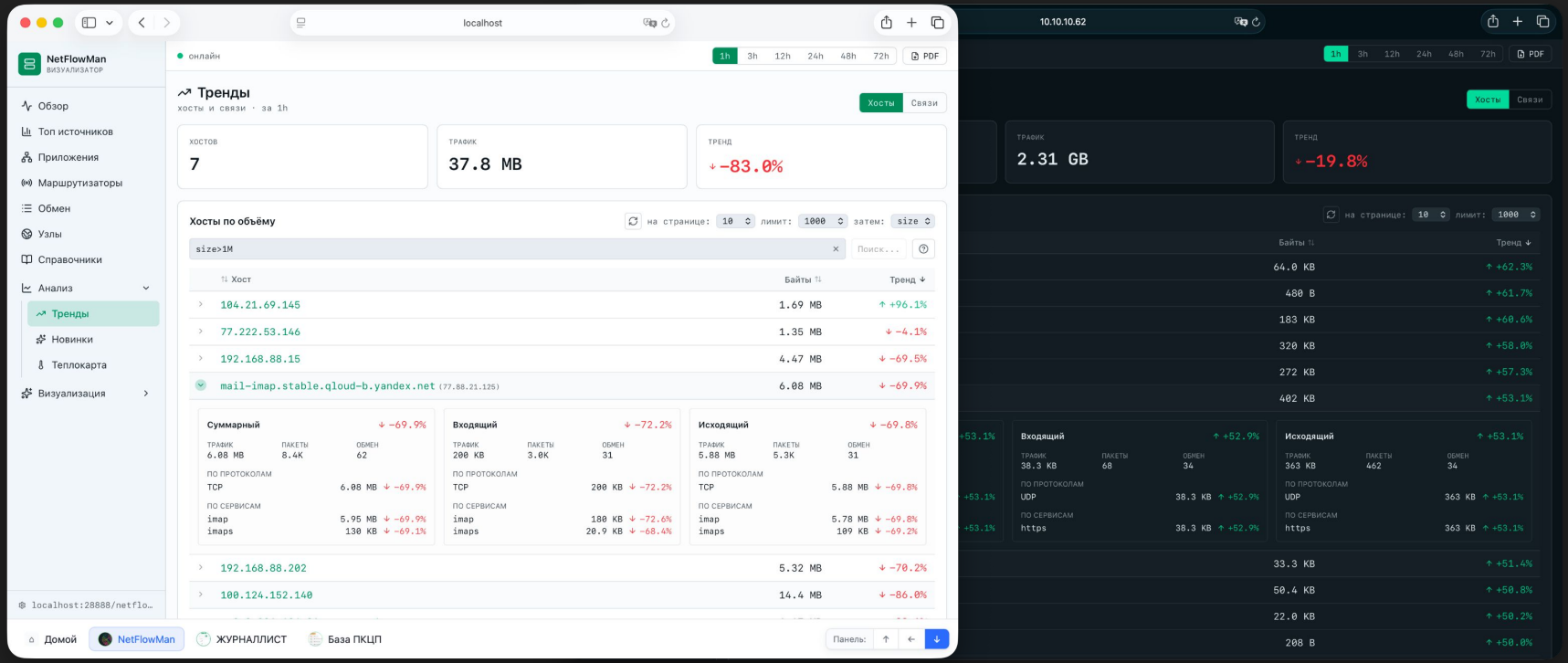
# Квадранты трафика - активность хостов и портов



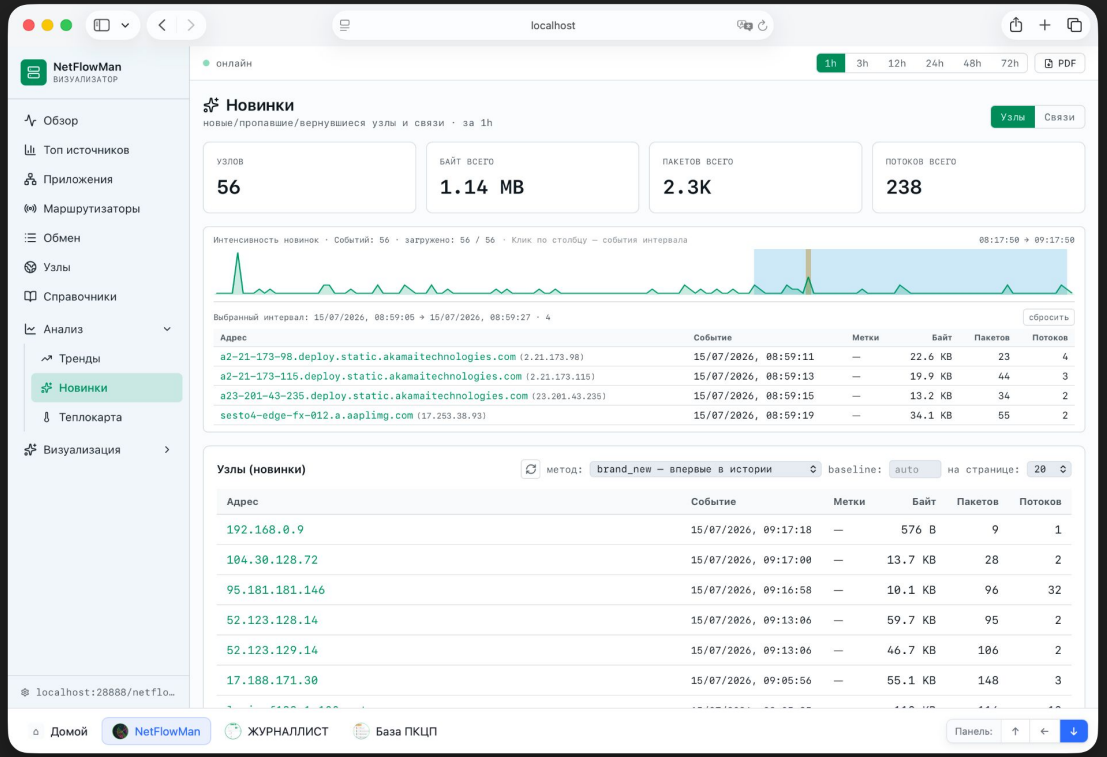
# Взаимодействие узлов и объемы трафика



# Тренды


localhost
NetFlowMan
ВИЗУАЛИЗАТОР
онлайн
1h 3h 12h 24h 48h 72h
PDF
Обзор
Топ источников
Приложения
Маршрутизаторы
Обмен
Узлы
Справочники
Анализ
Тренды
Новинки
Теплокарта
Визуализация
Тренды
хосты и связи · за 1h
Хосты
Связи
ХОСТОВ
7
ТРАФИК
37.8 MB
ТРЕНД
−83.0%
Хосты по объёму
на странице: 10 лимит: 1000 затем: size
size>1M
Поиск...
Хост
Байты
Тренд
104.21.69.145 1.69 MB +96.1%
77.222.53.146 1.35 MB −4.1%
192.168.88.15 4.47 MB −69.5%
mail-imap.stable.qloud-b.yandex.net (77.88.21.125) 6.08 MB −69.9%
Суммарный −69.9%
ТРАФИК 6.08 MB
ПАКЕТЫ 8.4K
ОБМЕН 62
ПО ПРОТОКОЛАМ
TCP 6.08 MB −69.9%
ПО СЕРВИСАМ
imap 5.95 MB −69.9%
imaps 130 KB −69.1%
Входящий −72.2%
ТРАФИК 200 KB
ПАКЕТЫ 3.0K
ОБМЕН 31
ПО ПРОТОКОЛАМ
TCP 200 KB −72.2%
ПО СЕРВИСАМ
imap 180 KB −72.6%
imaps 20.9 KB −68.4%
Исходящий −69.8%
ТРАФИК 5.88 MB
ПАКЕТЫ 5.3K
ОБМЕН 31
ПО ПРОТОКОЛАМ
TCP 5.88 MB −69.8%
ПО СЕРВИСАМ
imap 5.78 MB −69.8%
imaps 109 KB −69.2%
192.168.88.202 5.32 MB −70.2%
100.124.152.140 14.4 MB −86.0%
localhost:28888/netflo...
Домой
NetFlowMan
ЖУРНАЛЛИСТ
База ПКЦП
Панель:
10.10.10.62
2.31 GB
−19.8%
64.0 KB +62.3%
480 B +61.7%
183 KB +60.6%
320 KB +58.0%
272 KB +57.3%
402 KB +53.1%
Входящий +52.9%
ТРАФИК 38.3 KB
ПАКЕТЫ 68
ОБМЕН 34
ПО ПРОТОКОЛАМ
UDP 38.3 KB +52.9%
ПО СЕРВИСАМ
https 38.3 KB +52.9%
Исходящий +53.1%
ТРАФИК 363 KB
ПАКЕТЫ 462
ОБМЕН 34
ПО ПРОТОКОЛАМ
UDP 363 KB +53.1%
ПО СЕРВИСАМ
https 363 KB +53.1%
33.3 KB +51.4%
50.4 KB +50.8%
22.0 KB +50.2%
208 B +50.0%

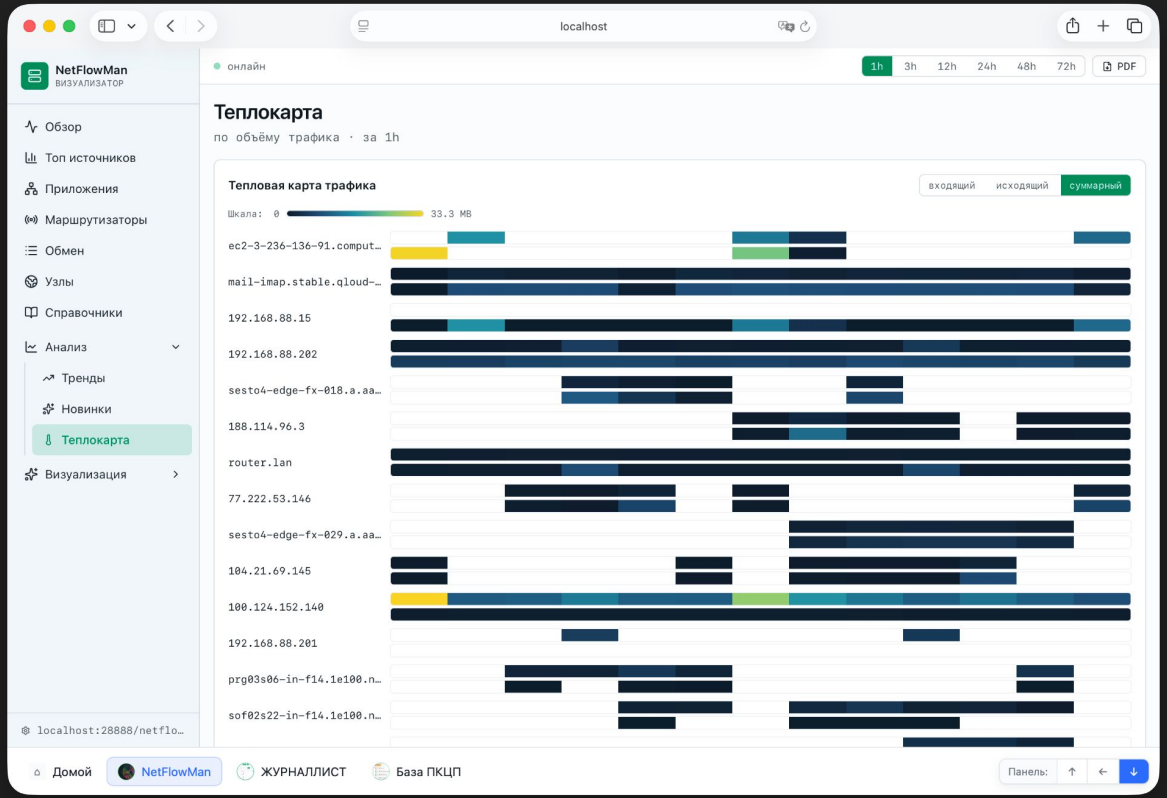
# Новые узлы и связи

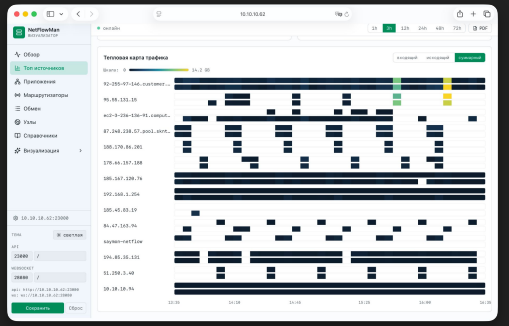



Шесть критериев новизны позволяют отслеживать поведение инфраструктуры.

Интеграция в системы заказчика позволяет усилить и автоматизировать контроль.

# Тепловая карта узлов и связей на периоде

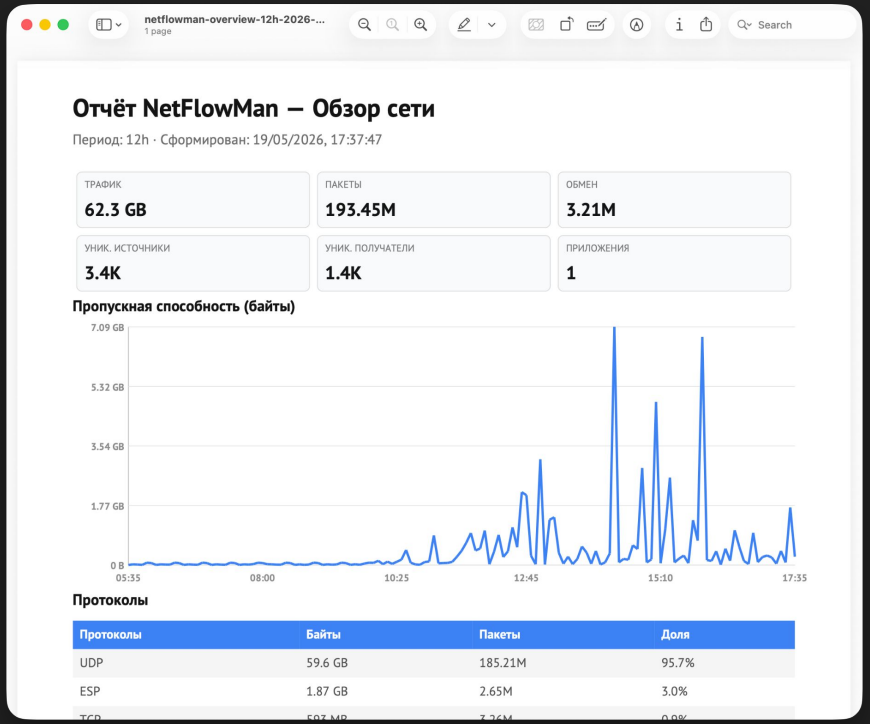


# Пример PDF-отчета

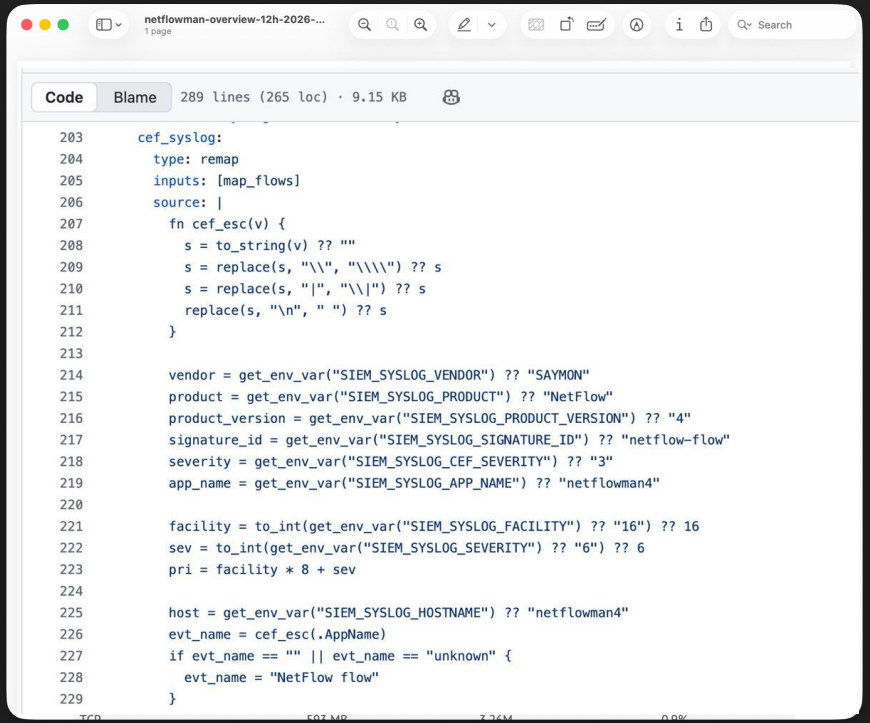
Система обеспечивает встроенную поддержку выгрузки базовых отчетов в формате PDF.

Отфильтрованные данные трафика можно экспортировать в форматы XLSX или CSV.



# Настройка отправки данных в SIEM

Подразделения ИБ
являются важными потребителями
информации о трафике.
Наше решение обеспечивает
встроенную настраиваемую
поддержку передачи событий
в SIEM-системы.

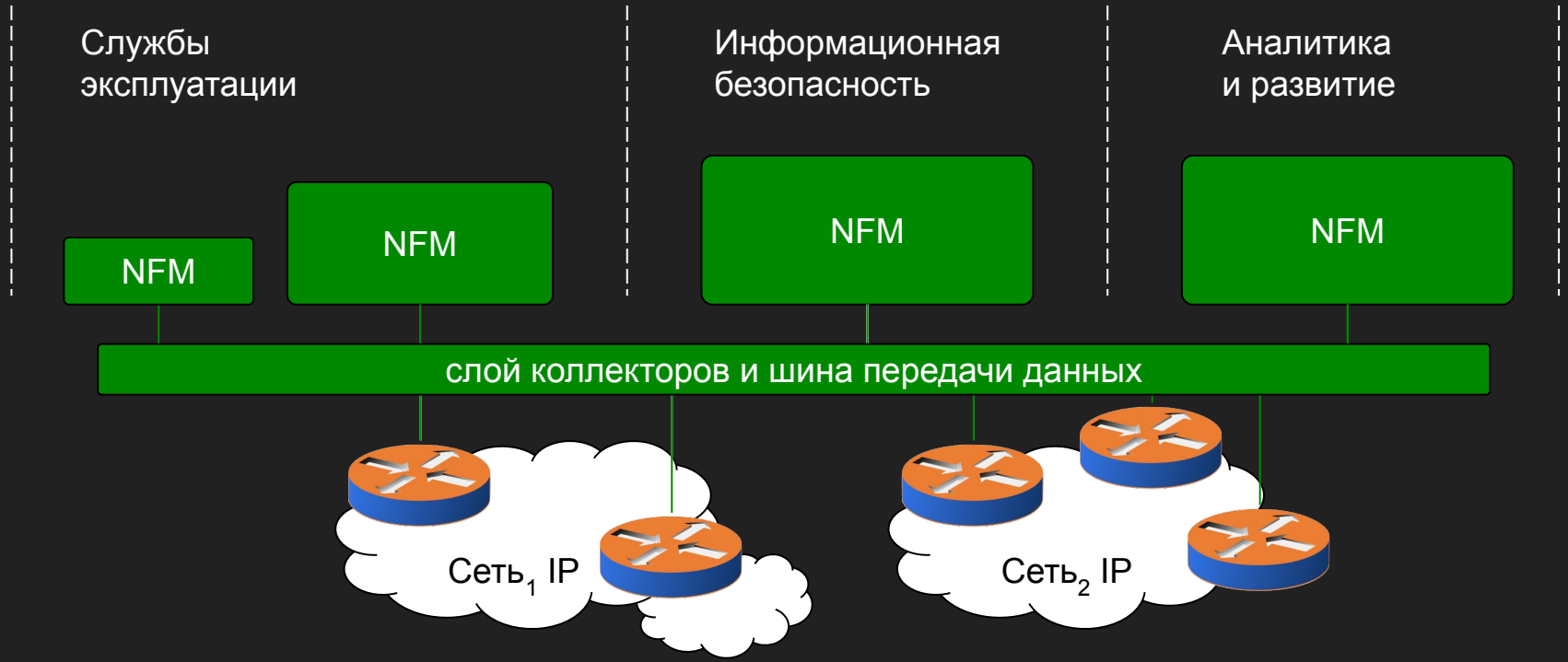



```
203     cef_syslog:
204       type: remap
205       inputs: [map_flows]
206       source: |
207         fn cef_esc(v) {
208           s = to_string(v) ?? ""
209           s = replace(s, "\\", "\\\\") ?? s
210           s = replace(s, "|", "\\|") ?? s
211           replace(s, "\n", " ") ?? s
212         }
213
214         vendor = get_env_var("SIEM_SYSLOG_VENDOR") ?? "SAYMON"
215         product = get_env_var("SIEM_SYSLOG_PRODUCT") ?? "NetFlow"
216         product_version = get_env_var("SIEM_SYSLOG_PRODUCT_VERSION") ?? "4"
217         signature_id = get_env_var("SIEM_SYSLOG_SIGNATURE_ID") ?? "netflow-flow"
218         severity = get_env_var("SIEM_SYSLOG_CEF_SEVERITY") ?? "3"
219         app_name = get_env_var("SIEM_SYSLOG_APP_NAME") ?? "netflowman4"
220
221         facility = to_int(get_env_var("SIEM_SYSLOG_FACILITY") ?? "16") ?? 16
222         sev = to_int(get_env_var("SIEM_SYSLOG_SEVERITY") ?? "6") ?? 6
223         pri = facility * 8 + sev
224
225         host = get_env_var("SIEM_SYSLOG_HOSTNAME") ?? "netflowman4"
226         evt_name = cef_esc(.AppName)
227         if evt_name == "" || evt_name == "unknown" {
228           evt_name = "NetFlow flow"
229         }
```

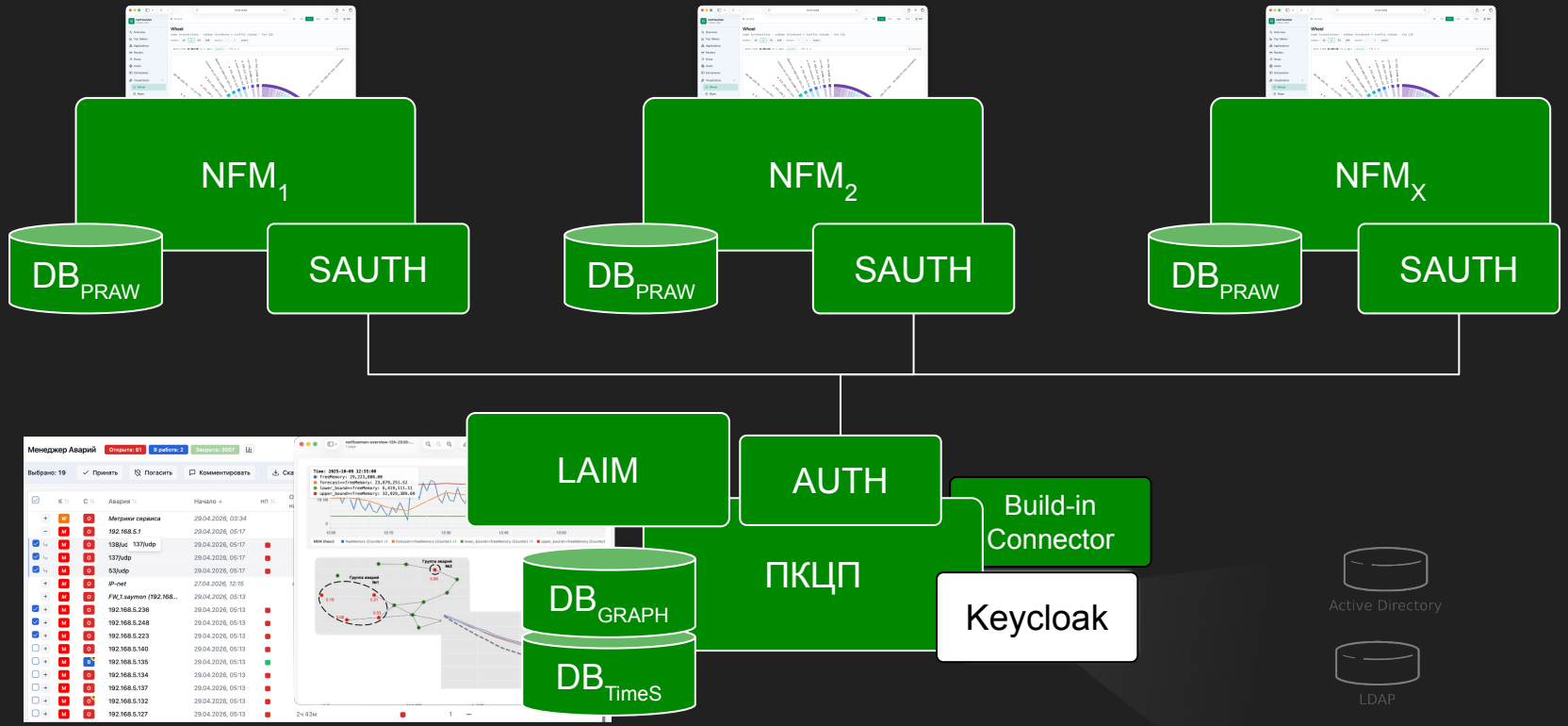
# Машинные методы анализа данных – AI/ML

Команда обладает значительным опытом в таких областях, как обнаружение аномалий с использованием AI и ML. Дополнительно может быть реализовано автоматизированное обнаружение взаимосвязей ресурсов и сервисов, а также машинный анализ первопричин (RCA) развития ситуаций .

# Изолированные потребители, общий слой приема



# Авторизация, Аварии, ML/AI централизованы



# Мониторинг и уведомления

Мониторинг – автоматизированное систематическое наблюдение, классификация, уведомления и корректирующие воздействия

“Центральный Пульт” обеспечивает полный спектр автоматизации операций мониторинга

Подсистемы сканирования сети и многофункциональные агенты мониторинга обеспечивают постоянный контроль

Уведомления ответственных, определение влияния на услуги и передача в Service Desk

# Авторизация и аудит пользователей

Подсистемы используют единый механизм авторизации через “Центральный Пульт”

“Центральный Пульт” поддерживает авторизацию в корпоративных системах и управление ролями

Система прав позволяет разграничивать доступ пользователей к информации и операциям

Осуществляется централизованный контроль и передача информации в подсистемы ИБ

# Лицензирование и поддержка

Основная модель работы
ООО “РОССИННО”
– производство и поддержка ПО

Приоритетная модель распространения для бизнес-клиентов – партнеры

Подсистема NetFlowMan оценивается по количеству источников, объему трафика за период (от PPS[1]) и сроку лицензии

“Центральный Пульт” дополнительно оценивается по масштабу объектов мониторинга, отказоустойчивости и дополнительным модулям

PPS – Packet Per Second

# NetFlowMan G4

ООО “РОССИННО”

САНКТ-ПЕТЕРБУРГ