

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

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

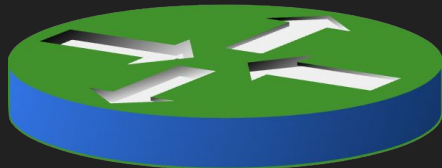
Когда сеть или цифровые сервисы начинают работать медленно, ИТ-команда часто не может быстро определить источник проблемы: пользователи недовольны, а бизнес простаивает

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

Решение NetFlowMan

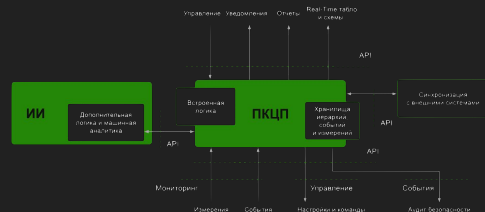
Аналитика NetFlow позволяет видеть фактическое поведение сети и приложений, быстро находить причины деградации сервисов, контролировать использование каналов и выявлять аномальный или нежелательный трафик

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

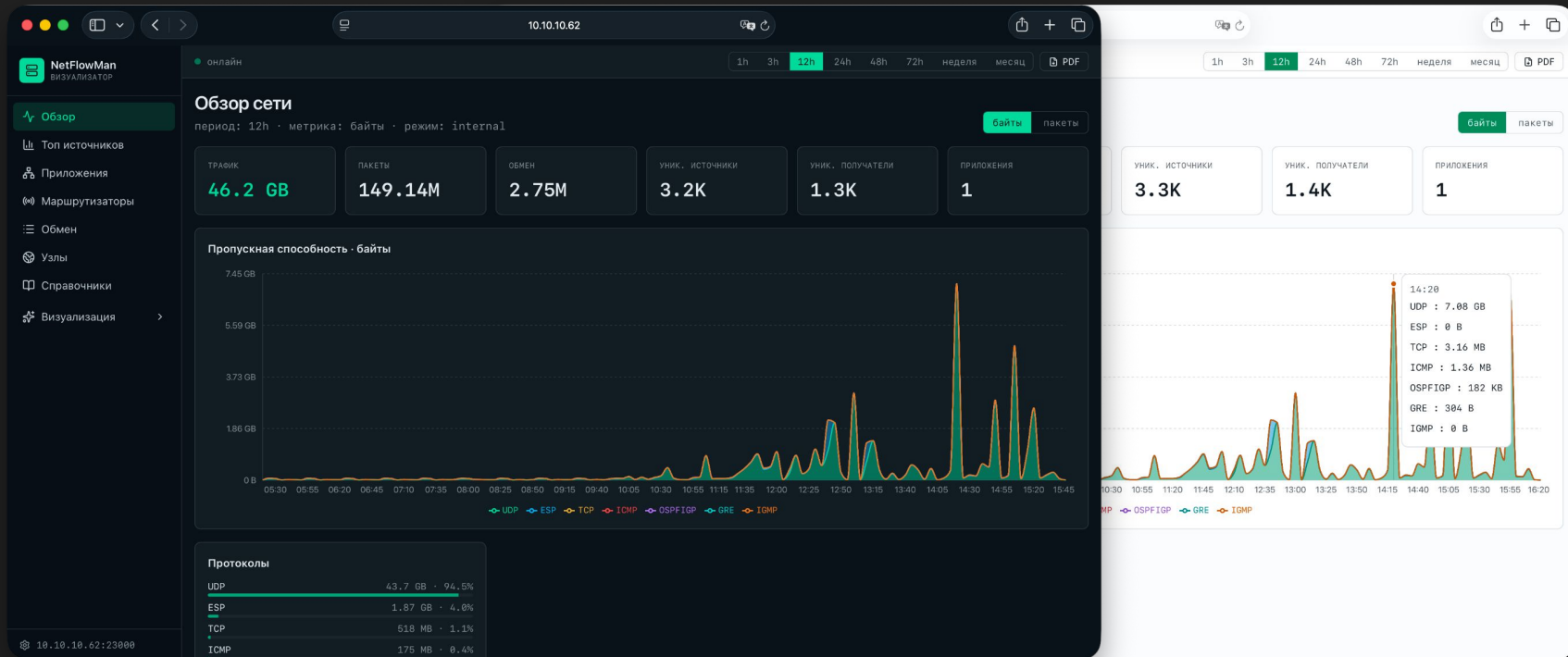


Архитектура – как работает

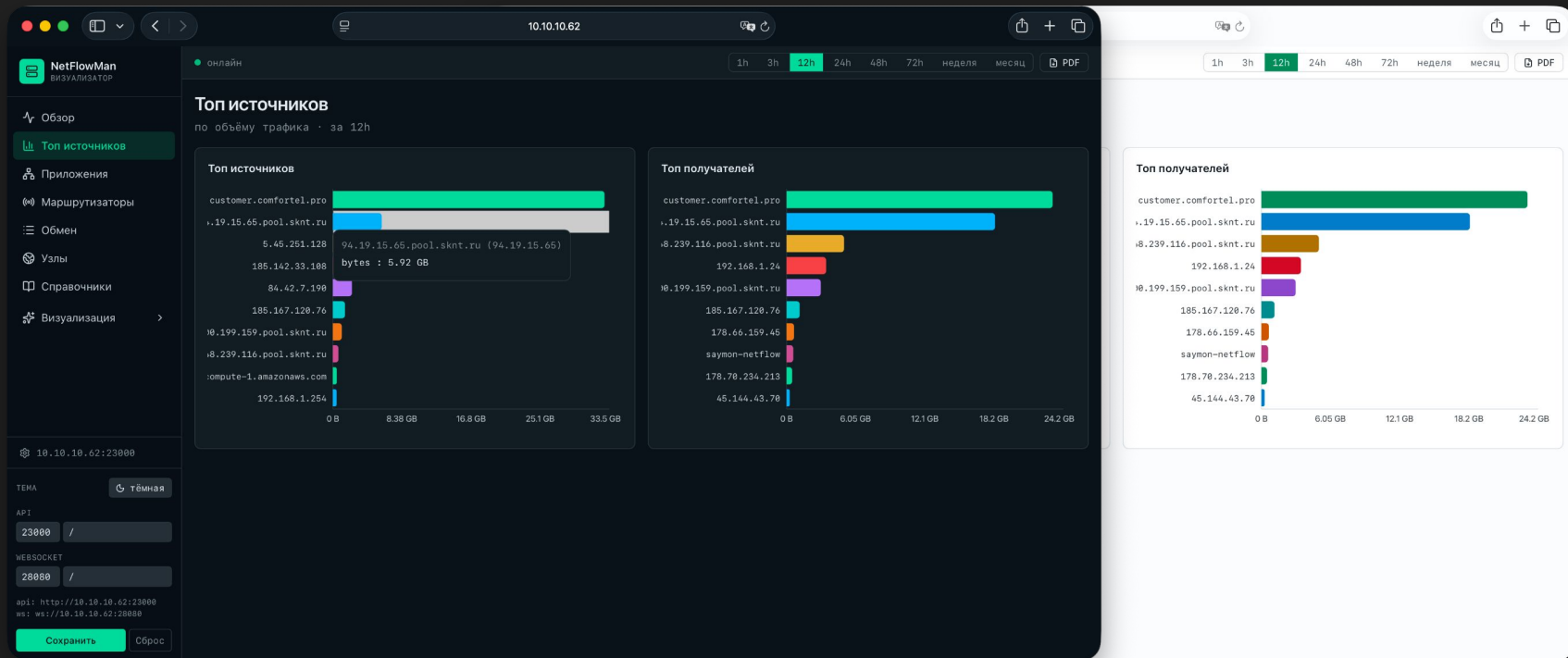
streaming-данных
сетевые, системные и корпоративные структуры данных
включение в системы клиента
машинный анализ



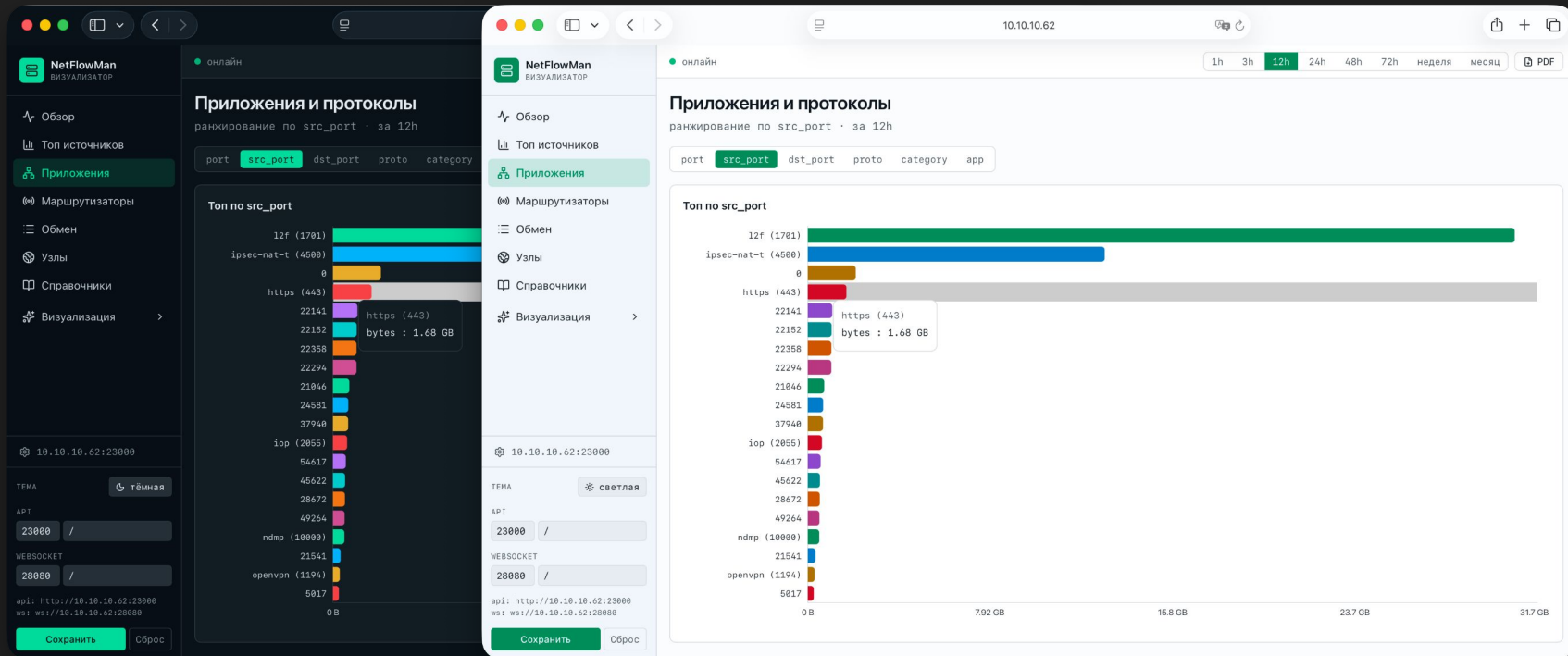
Обзор сети



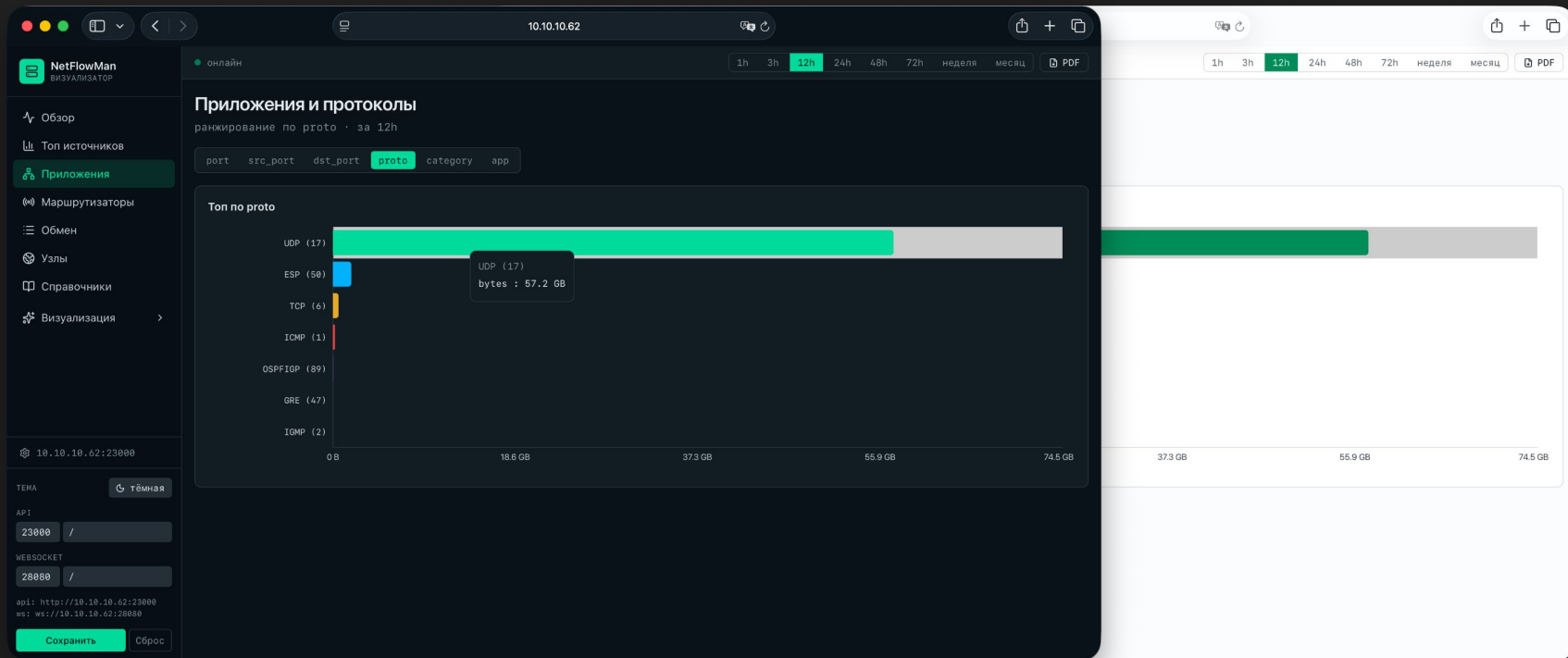
Наиболее активные узлы сети



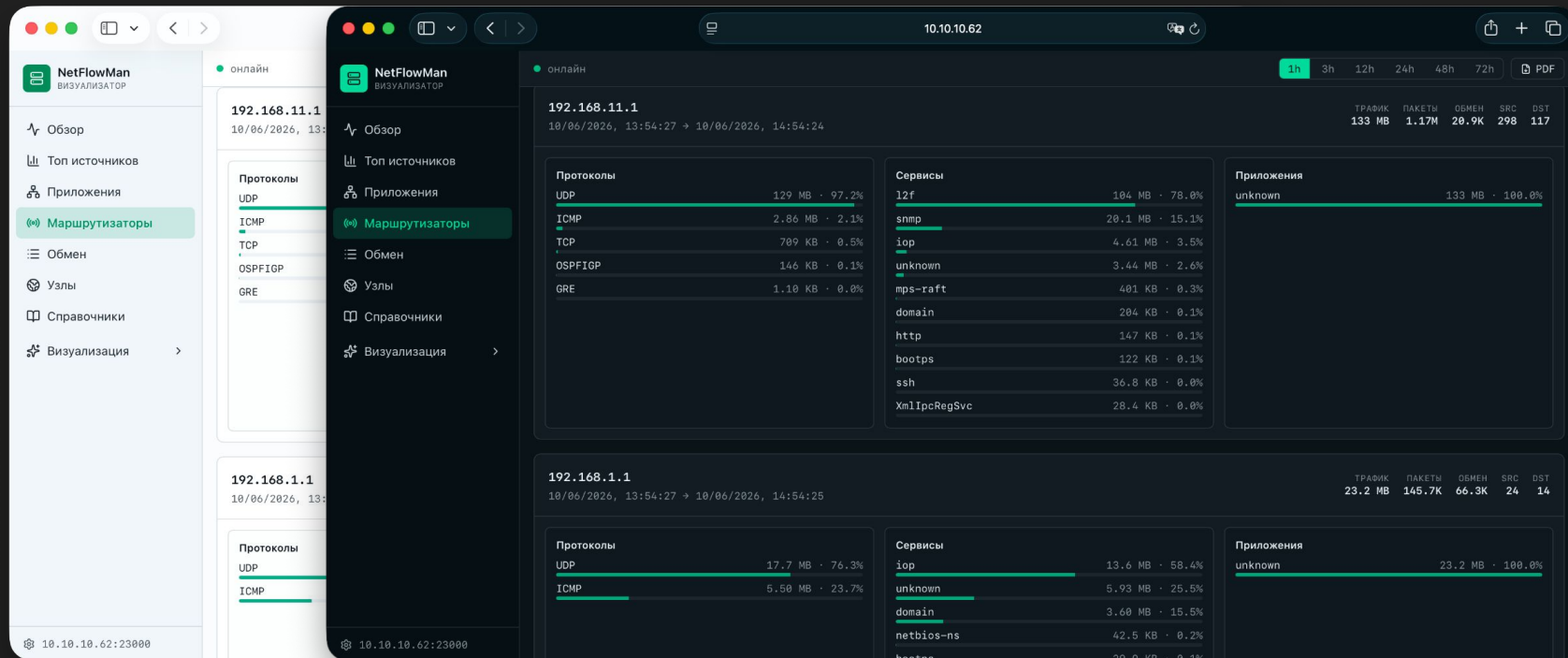
Рейтинг сетевых протоколов



Активность по типам трафика



Активность на маршрутизаторах – донорах данных





Индикация активности узлов



Партнеры узла по обмену трафиком

NetFlowMan ВИЗУАЛИЗАТОР

онлайн

Обзор
Топ источников
Приложения
Маршрутизаторы
Обмен
Узлы
Справочники
Визуализация

10.10.10.62:23000

ТЕМА: светлая

API: 23000 /

WEBSOCKET: 28080 /

api: https://10.10.10.62:23000
ws: ws://10.10.10.62:28080

Сохранить Сброс

ОСНОВНЫЕ СОСЕДИ

- 10.10.10.62 · saymon-netflow
- 192.168.5.155
- 192.168.5.152
- 192.168.5.157
- 192.168.5.154
- 192.168.5.156
- 192.168.5.153
- 10.10.10.94
- 192.168.1.4
- 192.168.1.254
- 255.255.255.255
- 192.168.1.81
- 192.168.3.101
- 89.109.251.22 · ntp2.vniiftri.ru
- 192.168.3.251

10.10.10.62

1h 3h 12h 24h 48h 72h неделя месяц PDF

Обзор
Топ источников
Приложения
Маршрутизаторы
Обмен
Узлы
Справочники
Визуализация

10.10.10.62:23000

ТЕМА: темная

API: 23000 /

WEBSOCKET: 28080 /

api: https://10.10.10.62:23000
ws: ws://10.10.10.62:28080

Сохранить Сброс

ОСНОВНЫЕ СОСЕДИ

	ТРАФИК	ПАКЕТЫ	ОБМЕН	
10.10.10.62 · saymon-netflow	162 MB	139.8K	50	к узлу
192.168.5.155	17.6 MB	252.3K	125.6K	к узлу
192.168.5.152	17.5 MB	251.4K	125.6K	к узлу
192.168.5.157	17.2 MB	248.3K	125.7K	к узлу
192.168.5.154	17.2 MB	248.0K	125.7K	к узлу
192.168.5.156	17.0 MB	244.7K	125.6K	к узлу
192.168.5.153	16.9 MB	244.4K	125.7K	к узлу
10.10.10.94	891 KB	10.9K	2.7K	к узлу
192.168.1.4	889 KB	10.8K	2.7K	к узлу
192.168.1.254	299 KB	1.2K	837	к узлу
255.255.255.255	236 KB	1.4K	1.4K	к узлу
192.168.1.81	89.4 KB	220	16	к узлу
192.168.3.101	40.7 KB	496	136	к узлу
89.109.251.22 · ntp2.vniiftri.ru	5.34 KB	72	72	к узлу
192.168.3.251	4.49 KB	100	20	к узлу

Живой поток с сетевого устройства в web-консоль

NetFlowMan ВИЗУАЛИЗАТОР

онлайн | 1h 3h **12h** 24h 48h 72h неделя месяц PDF

Просмотр узлов

трафик и соседи по IP · за 3h

поиск: 192.168.1.254 **Открыть**

192.168.1.254 | ТРАФИК: 0 В | ПАКЕТЫ: 0 | ОБМЕН: 0 | СОСЕДИ: 15

Connected · всего: 2520 · с участием 192.168.1.254: 98 · WS ws://10.10.10.62:28080 · API http://10.10.10.62:23000 | **STOP** **ОЧИСТИТЬ**

Время	Источник	Получатель	Протокол	Сервис	Приложение	Байт	VLAN
21:52:21	192.168.1.254:161	192.168.3.252:39635	UDP (17)	snmp	—	327	0
21:52:21	192.168.3.252:39635	192.168.1.254:161 FE:E9:39:49:FE:6E · —	UDP (17)	snmp	—	144	0
21:52:21	192.168.1.254:161	192.168.3.252:44717	UDP (17)	snmp	—	257	0
21:52:21	192.168.1.254:161 FE:E9:39:49:FE:6E · —	192.168.3.252:39635	UDP (17)	snmp	—	327	0
21:52:21	192.168.3.252:39635	192.168.1.254:161	UDP (17)	snmp	—	144	0
21:52:21	192.168.3.252:44717	192.168.1.254:161 FE:E9:39:49:FE:6E · —	UDP (17)	snmp	—	69	0
21:52:21	192.168.1.254:161 FE:E9:39:49:FE:6E · —	192.168.3.252:44717	UDP (17)	snmp	—	257	0
21:52:21	192.168.3.252:44717	192.168.1.254:161	UDP (17)	snmp	—	69	0

10.10.10.62:28080 · API 10.10.10.62:23000 | **STOP** **ОЧИСТИТЬ**

Протокол	Сервис	Приложение	Байт	VLAN
UDP (17)	snmp	—	74	0
UDP (17)	snmp	—	74	0
UDP (17)	snmp	—	268	0
UDP (17)	snmp	—	294	0
UDP (17)	snmp	—	294	0
UDP (17)	snmp	—	268	0
UDP (17)	snmp	—	75	0
UDP (17)	snmp	—	142	0
UDP (17)	snmp	—	75	0
UDP (17)	snmp	—	142	0

ТЕМА: **Тёмная**

API: 23000 /

WEBSOCKET: 28080 /

api: https://10.10.10.62:23000
ws: ws://10.10.10.62:28080

Сохранить **Сброс**

Справочники приложений

The image displays two side-by-side screenshots of the NetFlowMan application interface, showing the 'Справочники' (Reference) section for 'NBAR2 Applications'.

Left Screenshot (Dark Mode):

- Header: NetFlowMan ВИЗУАЛИЗАТОР
- Left Sidebar: Обзор, Топ источников, Приложения, Маршрутизаторы, Обмен, Узлы, **Справочники** (highlighted), Визуализация.
- Main Content: NBAR2 Applications (50 записей · обновлено 19/05/2026, 17:07:12). Tabs: NBAR2 Приложения (selected), IP Протоколы, Сервисы (Порты).
- Table:

КЛЮЧ	NAME
13:1	unknown
13:1001	ssh
13:1002	telnet
13:1003	ftp
13:1022	rdp
13:1100	snmp
13:1120	ldap
13:1200	smb
13:123	ntp
13:1547	wikipedia
13:25	smtp
13:2572	google-advertising
13:3001	discord
13:3005	twitch
13:3100	playstore
13:3101	apple-itunes
13:348	facebook
13:350	ooodle-services

Right Screenshot (Light Mode):

- Header: NetFlowMan ВИЗУАЛИЗАТОР
- Left Sidebar: Обзор, Топ источников, Приложения, Маршрутизаторы, Обмен, Узлы, **Справочники** (highlighted), Визуализация.
- Main Content: NBAR2 Applications (50 записей · обновлено 19/05/2026, 17:07:12). Tabs: NBAR2 Приложения (selected), IP Протоколы, Сервисы (Порты).
- Table:

КЛЮЧ	NAME	CATEGORY
13:1	unknown	other
13:1001	ssh	it-management
13:1002	telnet	it-management
13:1003	ftp	file-transfer
13:1022	rdp	it-management
13:1100	snmp	network-service
13:1120	ldap	network-service
13:1200	smb	file-transfer
13:123	ntp	network-service
13:1547	wikipedia	browsing
13:25	smtp	email
13:2572	google-advertising	business-and-productivity
13:3001	discord	instant-messaging
13:3005	twitch	streaming
13:3100	playstore	software-updates
13:3101	apple-itunes	streaming
13:348	facebook	social-networking
13:350	ooodle-services	browsing

Справочники портов

NetFlowMan ВИЗУАЛИЗАТОР

онлайн

Обзор

Топ источников

Приложения

Маршрутизаторы

Обмен

Узлы

Справочники

Визуализация

10.10.10.62:23000

ТЕМА: светлая

API: 23000 /

WEBSOCKET: 28000 /

api: https://10.10.10.62:23000
ws: ws://10.10.10.62:28000

Сохранить Сброс

IP Protocol Numbers (IANA RFC 5237)

145 записей · обновлено 19/05/2026, 17:07:12

NBAR2 Приложения IP Протоколы Сервисы (Порты)

КЛЮЧ	KEYWORD	NAME
0	HOPOPT	IPv6 Hop-by-Hop Option
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IPv4	IPv4 encapsulation
5	ST	Stream
6	TCP	Transmission Control
7	CBT	CBT
8	EGP	Exterior Gateway Protocol
9	IGP	any private interior gateway (used by Cisco for their IGRP)
10	BBN-RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP
13	ARGUS (deprecated)	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram

10.10.10.62

1h 3h 12h 24h 48h 72h неделя месяц PDF

Поиск...

колонки Обновить

NetFlowMan ВИЗУАЛИЗАТОР

онлайн

Обзор

Топ источников

Приложения

Маршрутизаторы

Обмен

Узлы

Справочники

Визуализация

10.10.10.62:23000

ТЕМА: темная

API: 23000 /

WEBSOCKET: 28000 /

api: https://10.10.10.62:23000
ws: ws://10.10.10.62:28000

Сохранить Сброс

Справочники сетевых сервисов

NetFlowMan ВИЗУАЛИЗАТОР

онлайн

Service Names and Port Numbers (IANA RFC 6335)
12282 записей · обновлено 19/05/2026, 17:07:14

НBAR2 Приложения IP Протоколы Сервисы (Порты)

КЛЮЧ	SERVICE_NAME	PORT	TRANSPORT	DESCRIPTION
132:1021	exp1	1021	sctp	RFC3692-style Experiment 1
132:1022	exp2	1022	sctp	RFC3692-style Experiment 2
132:11235	xcompute	11235	sctp	numerical systems messaging
132:1167	cisco-ipsla	1167	sctp	Cisco IP SLAs Control Protocol
132:11997	wmereceiving	11997	sctp	WorldMailExpress
132:11998	wmedistribution	11998	sctp	WorldMailExpress
132:11999	wmereporting	11999	sctp	WorldMailExpress
132:14001	sua	14001	sctp	SUA
132:1528	norp	1528	sctp	Not Only a Routing Protocol
132:1720	h323hostcall	1720	sctp	H.323 Call Control
132:179	bgp	179	sctp	BGP
132:19999	dnp-sec	19999	sctp	Distributed Network Protocol - secured
132:20	ftp-data	20	sctp	FTP
132:20000	dnp	20000	sctp	Distributed Network Protocol
132:20049	nfsrdma	20049	sctp	Network File System (NFS) over RDMA
132:2049	nfs	2049	sctp	Network File System
132:21	ftp	21	sctp	FTP
132:22	ssh	22	sctp	SSH

10.10.10.62

1h 3h 12h 24h 48h 72h неделя месяц PDF

Поиск...

колонки Обновить

NetFlowMan ВИЗУАЛИЗАТОР

онлайн

Service Names and Port Numbers (IANA RFC 6335)
12282 записей · обновлено 19/05/2026, 17:07:14

НBAR2 Приложения IP Протоколы Сервисы (Порты)

КЛЮЧ	SERVICE_NAME	PORT	TRANSPORT	DESCRIPTION
132:1021	exp1	1021	sctp	RFC3692-style Experiment 1
132:1022	exp2	1022	sctp	RFC3692-style Experiment 2
132:11235	xcompute	11235	sctp	numerical systems messaging
132:1167	cisco-ipsla	1167	sctp	Cisco IP SLAs Control Protocol
132:11997	wmereceiving	11997	sctp	WorldMailExpress
132:11998	wmedistribution	11998	sctp	WorldMailExpress
132:11999	wmereporting	11999	sctp	WorldMailExpress
132:14001	sua	14001	sctp	SUA
132:1528	norp	1528	sctp	Not Only a Routing Protocol
132:1720	h323hostcall	1720	sctp	H.323 Call Control
132:179	bgp	179	sctp	BGP
132:19999	dnp-sec	19999	sctp	Distributed Network Protocol - secured
132:20	ftp-data	20	sctp	FTP
132:20000	dnp	20000	sctp	Distributed Network Protocol
132:20049	nfsrdma	20049	sctp	Network File System (NFS) over RDMA
132:2049	nfs	2049	sctp	Network File System
132:21	ftp	21	sctp	FTP
132:22	ssh	22	sctp	SSH

10.10.10.62:23000

ТЕМА * светлая

API 23000 /

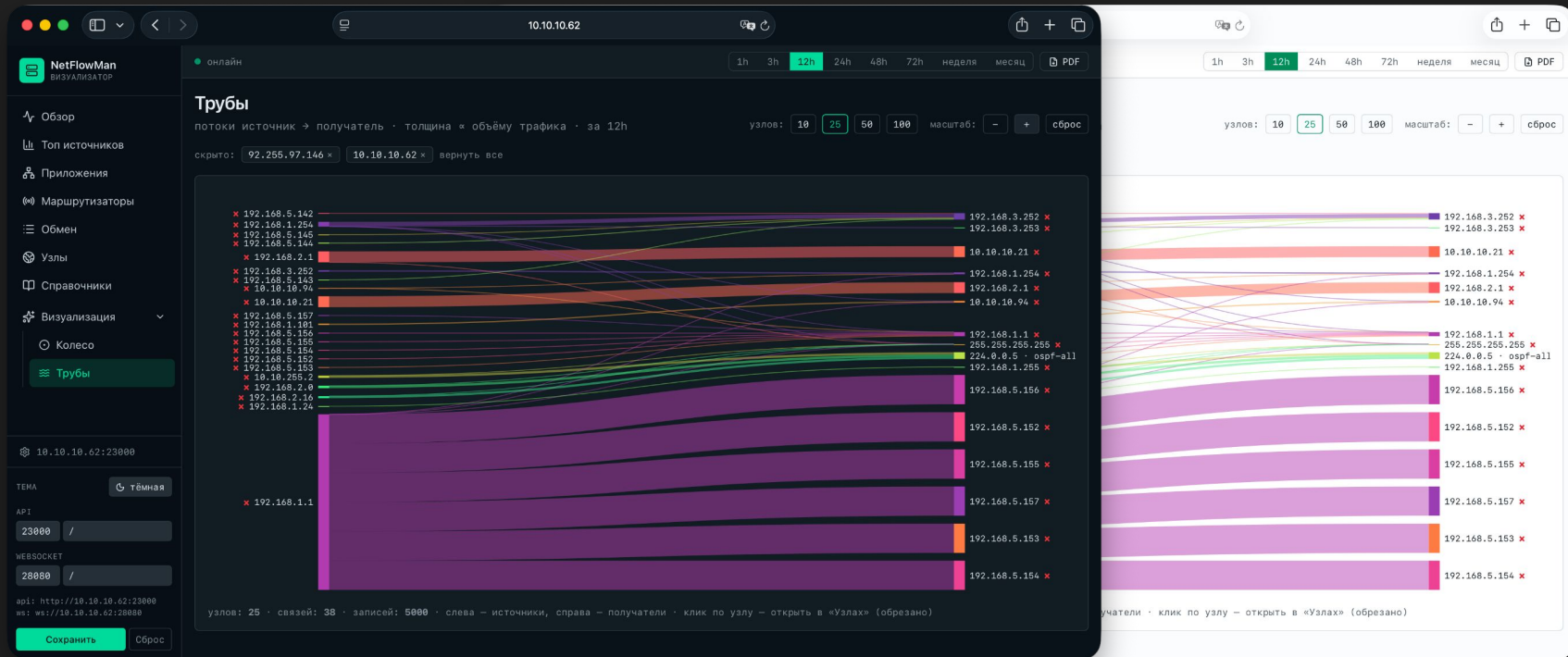
WEBSOCKET 20000 /

api: http://10.10.10.62:23000
ws: ws://10.10.10.62:20000

Сохранить Сброс

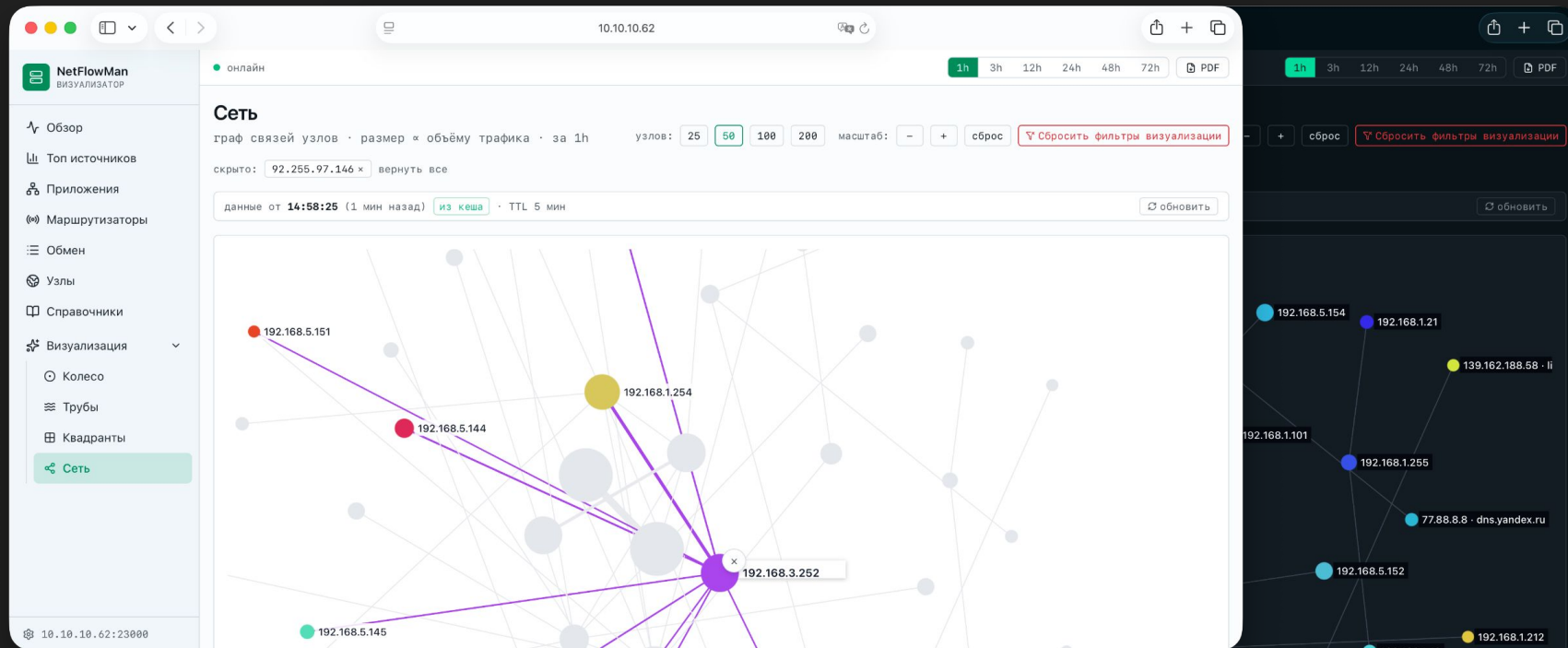


Развернутые интерактивные карты потоков

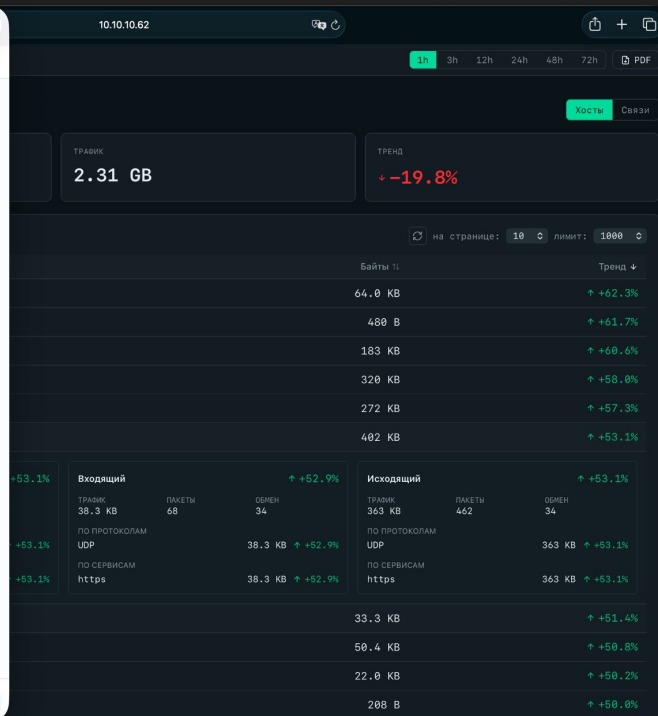
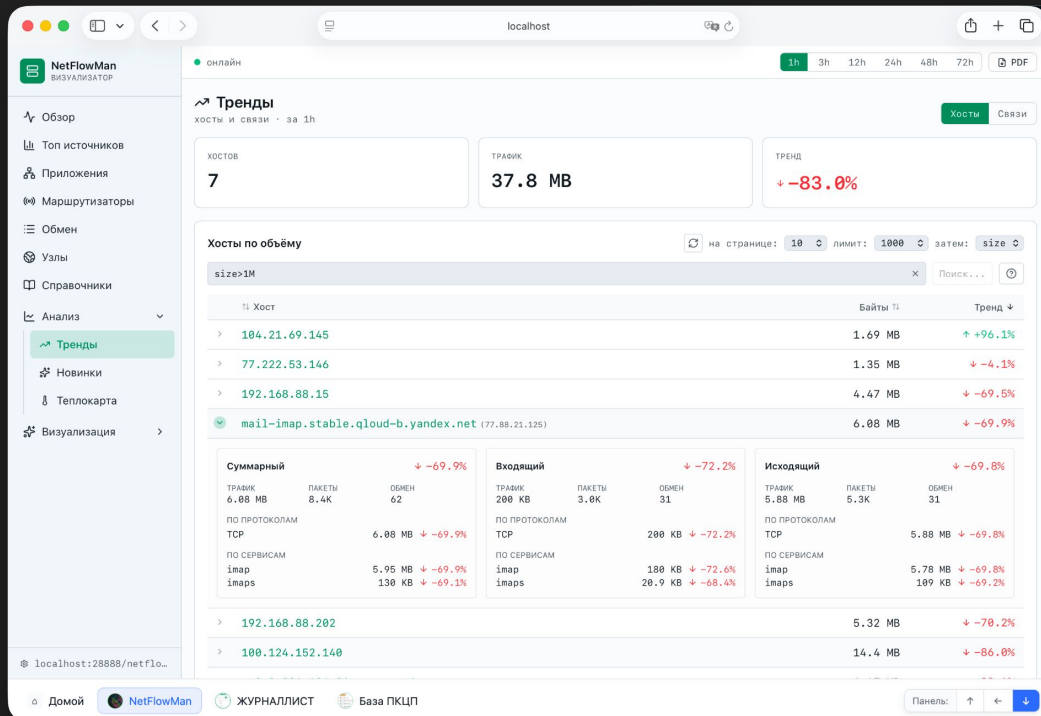




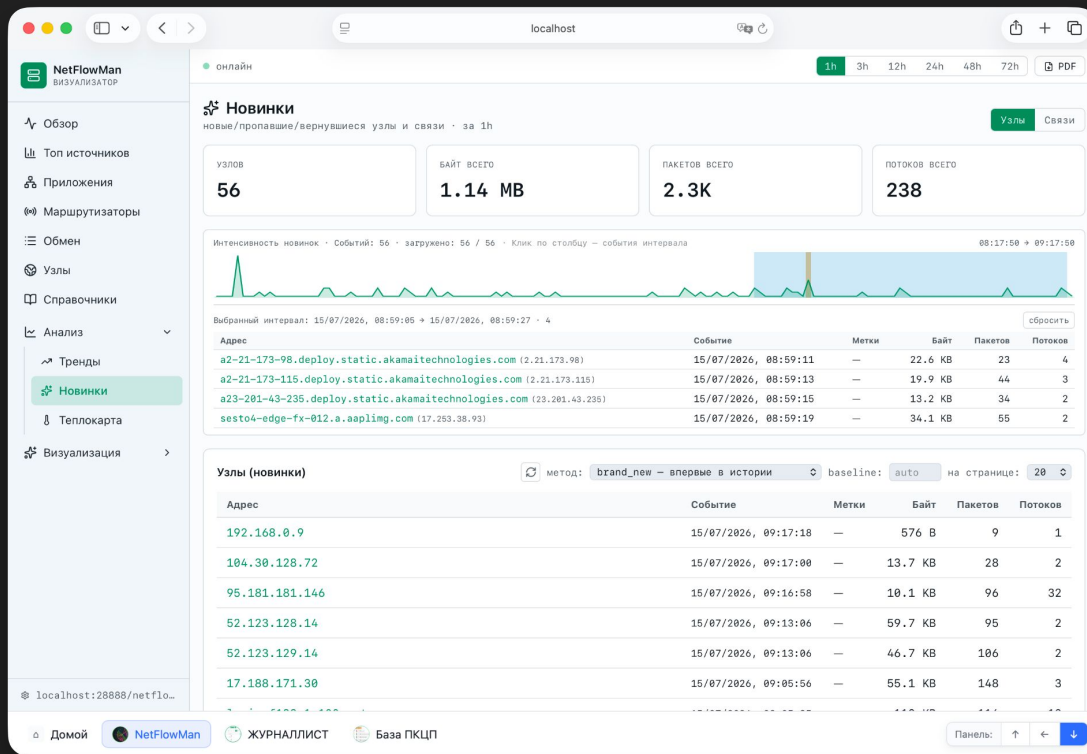
Взаимодействие узлов и объемы трафика



Тренды



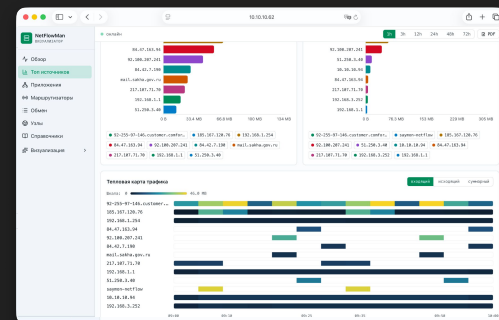
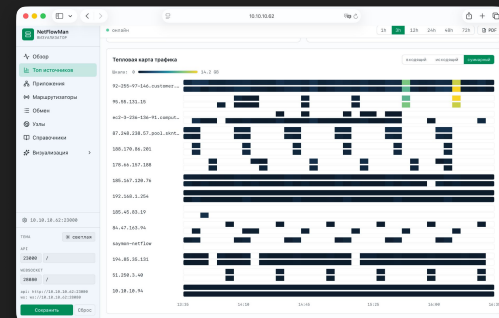
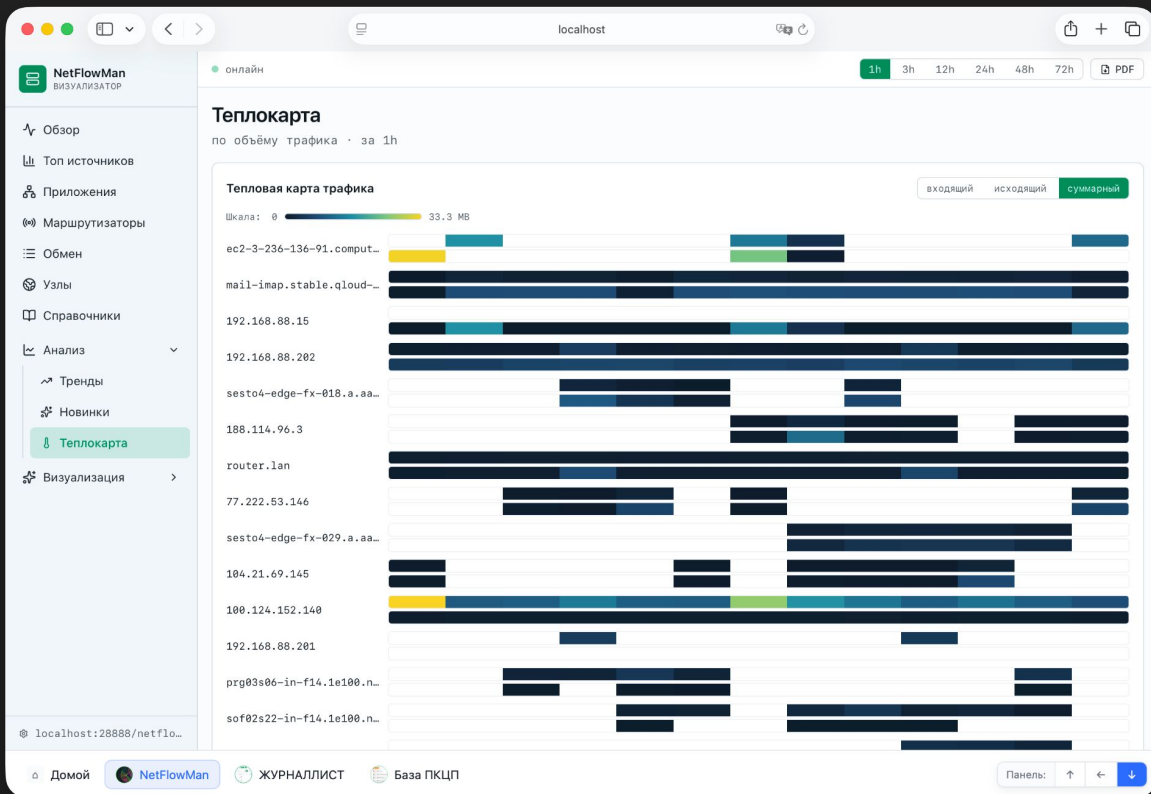
Новые узлы и связи



Шесть критериев новизны позволяют отслеживать поведение инфраструктуры.

Интеграция в системы заказчика позволяет усилить и автоматизировать контроль.

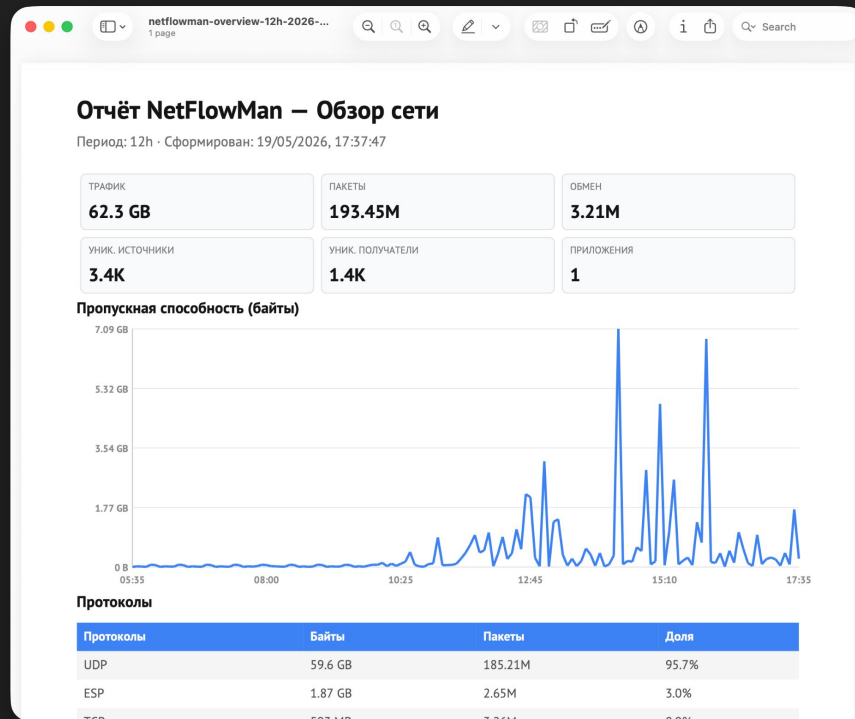
Тепловая карта узлов и связей на периоде



Пример PDF-отчета

Система обеспечивает
встроенную поддержку загрузки
базовых отчетов в формате PDF.

Отфильтрованные данные трафика
можно экспортировать
в форматы XLSX или CSV.

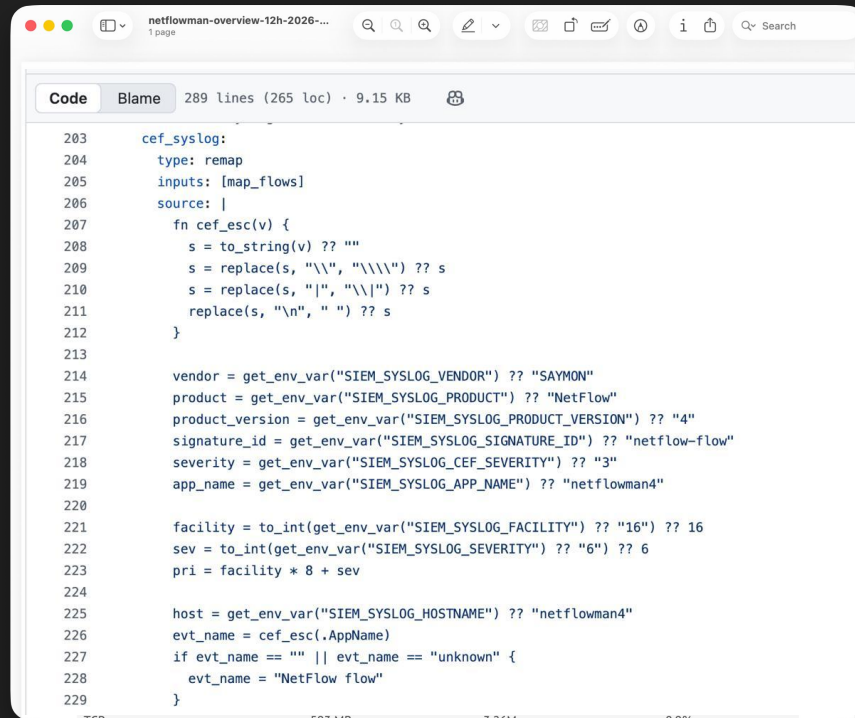


Настройка отправки данных в SIEM

Подразделения ИБ

являются важными потребителями информации о трафике.

Наше решение обеспечивает встроенную настраиваемую поддержку передачи событий в SIEM-системы.

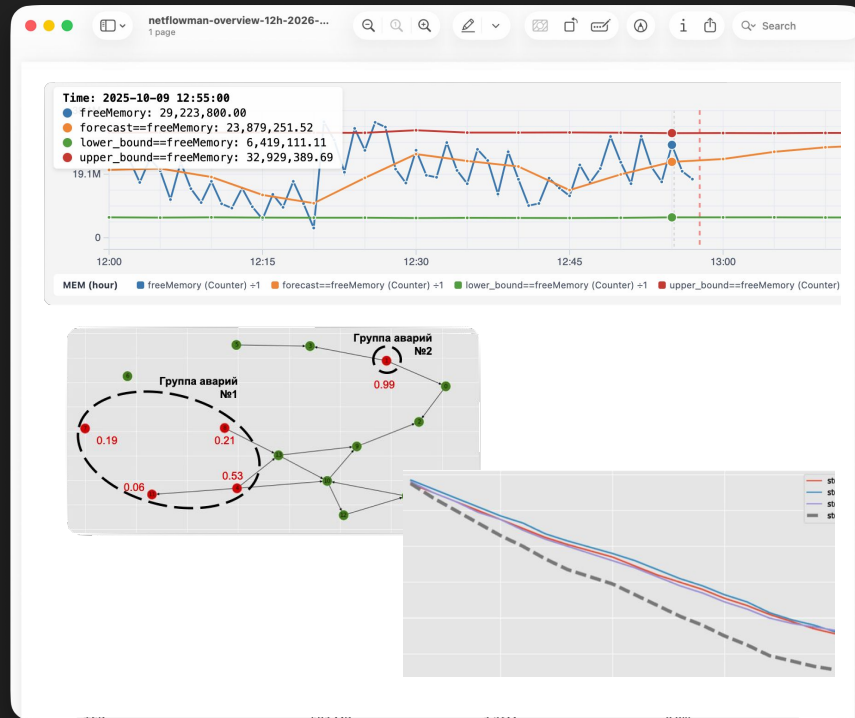


```
203 cef_syslog:
204   type: remap
205   inputs: [map_flows]
206   source: |
207     fn cef_esc(v) {
208       s = to_string(v) ?? ""
209       s = replace(s, "\\\"", "\\\"") ?? s
210       s = replace(s, "|", "\\|") ?? s
211       replace(s, "\n", " ") ?? s
212     }
213
214     vendor = get_env_var("SIEM_SYSLOG_VENDOR") ?? "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     }
```

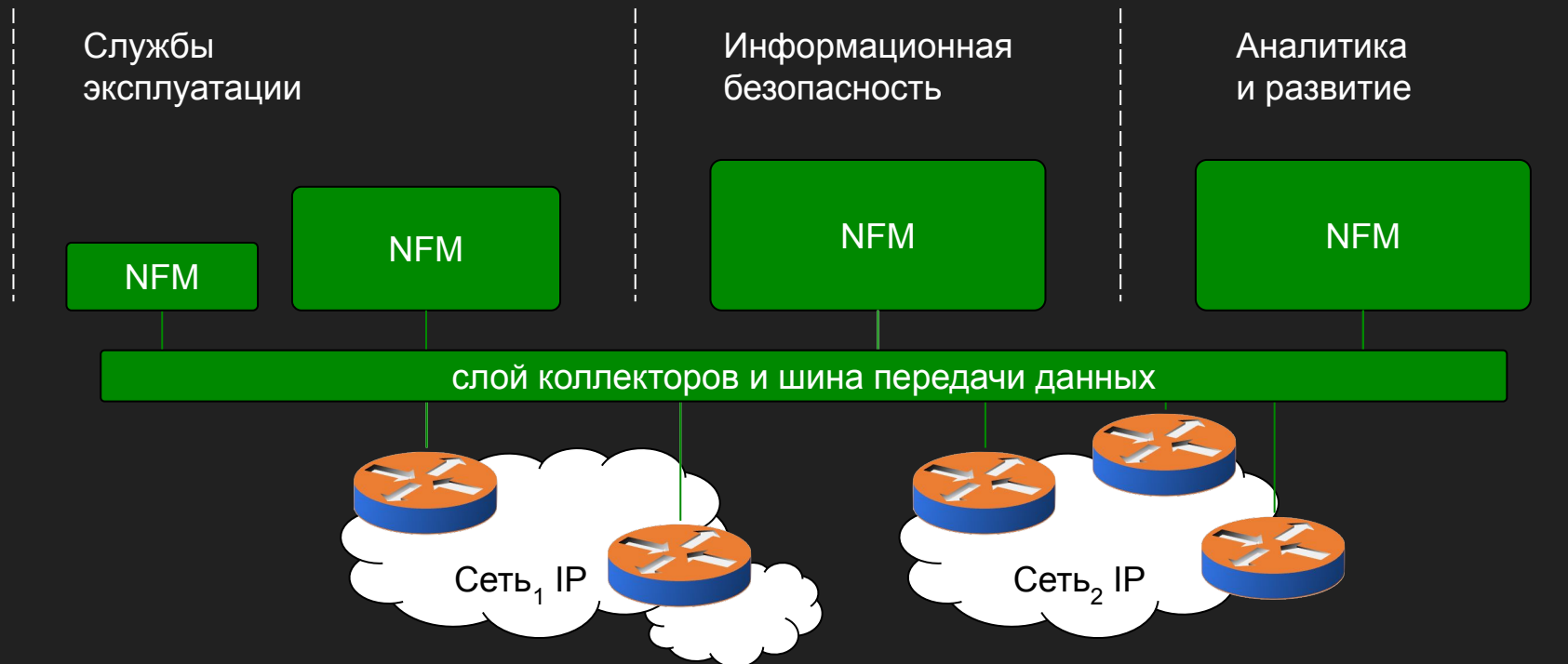
Машинные методы анализа данных – AI/ML

Команда обладает значительным опытом в таких областях, как обнаружение аномалий с использованием AI и ML.

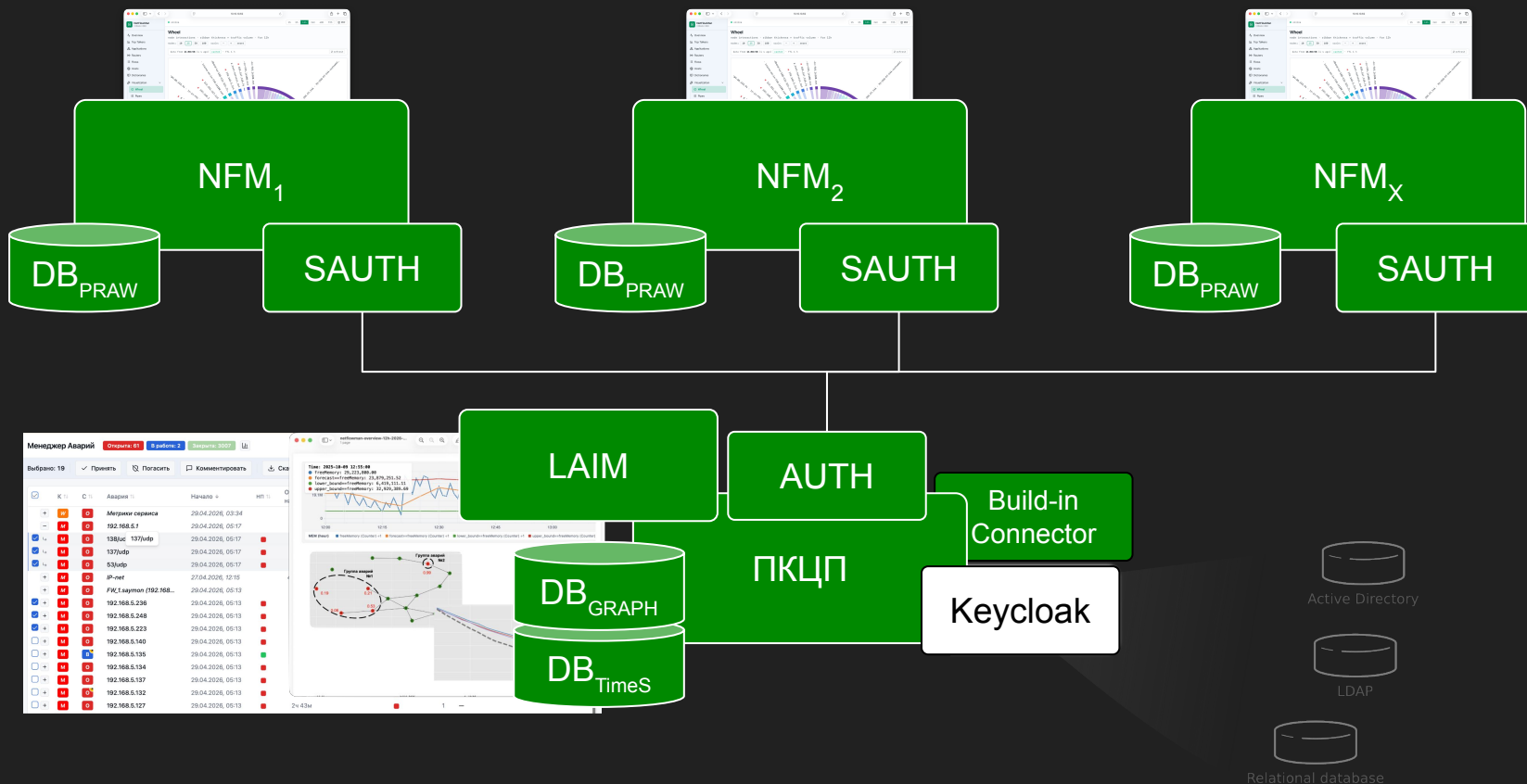
Дополнительно может быть реализовано автоматизированное обнаружение взаимосвязей ресурсов и сервисов, а также машинный анализ первопричин (RCA) развития ситуаций .



Изолированные потребители, общий слой приема



Авторизация, Аварии, ML/AI централизованы



Мониторинг и уведомления

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

Подсистемы сканирования сети и многофункциональные агенты мониторинга обеспечивают постоянный контроль

“Центральный Пульт” обеспечивает полный спектр автоматизации операций мониторинга

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

Авторизация и аудит пользователей

Подсистемы используют единый механизм авторизации через “Центральный Пульт”

Система прав позволяет разграничивать доступ пользователей к информации и операциям

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

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 PPS¹) и сроку лицензии

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

NetFlowMan G4

ООО “РОССИННО”

САНКТ-ПЕТЕРБУРГ