aVistar/V

ПРИМЕНЕНИЕ и РЕШЕНИЯ

USE CASES

примеры использования

Оглавление

Общие подходы 3
Кейсы, связанные с прозрачностью информационных потоков 3
Пример 1. Надо быстро понять, движение трафика и при необходимости детализировать информацию. .3
Пример 2. Надо увидеть детализацию по конкретной сессии....3
Пример 3. Пропускная способность и загрузка канала 7
Пример 4. Посмотреть сессии только с IPv6 7
Аналитика по приложениям 8
Пример 5. Найти определенные DNS-запросы в общем трафике 8
Пример 6. Как задействованы серверные логические порты в информационном обмене 8
Квалиметрия (качество сервисов и каналов связи) 10
Проблемные пакеты 10
Пример 7. Увидеть возможные проблемы с пакетами в канале и как они распределялись во времени....10
Пример 8. Увидеть топ проблемных связей по потерянным пакетам внутри системы под мониторингом 10
Влияние задержек на сетевые сервисы 11
Пример 9. Оценка средних задержек в канале связи 11
Пример 10. Найти в канале все сессии, для которых время круговой задержки превысило 100 миллисекунд....12
Пример 11. Необходимо определить самый медленный прикладной сервер за выделенный интервал времени в канале под мониторингом и оценить его негативное влияние на клиентов 13
Анализ TCP-флагов сессий....14
Пример 12. Необходимо увидеть все сессии, которые содержали флаг PUSH в своём информационном обмене....14
Пример 13. Быстро увидеть распределение сессий по статусам завершения в канале под мониторингом, по группе сервисов «Почта»....15
Пример 14. Задача: узнать, появлялись ли отклики «4xx» HTTP-серверов в информационных потоках 15

В документе представлены только *некоторые* варианты использования системы aVistar, исключая кейсы кибербезопасности, которые изложены в отдельном документе «Система aVistar для исследования киберинцидентов».

Общие подходы

Система aVistar предназначена для визуализации информационных потоков по различным срезам в почти реальном времени и ретроспективе. Она включает общие инструменты и методы, которые используются для всех специализированных вариантов представления информации об информационных потоках под мониторингом:

1. Вертикальный анализ (drill-down) – трёхуровневый анализ.
2. Настраиваемые экраны: возможность убрать лишние виджеты с экранов и возможность настройки расположения и размеров виджетов, чтобы ничто не мешало правильному восприятию информации.
3. Различные механизмы фильтрации и ранжирования данных на экранах, виджетах и таблицах.
4. Исторический анализ данных.
5. *Возможность использования порогов* для автоматического отслеживания параметров и событий в информационных потоках.

Кейсы, связанные с прозрачностью информационных потоков

Пример 1. Надо быстро понять, движение трафика и при необходимости детализировать информацию.

Самый простой способ «понять» – это «увидеть» трафик в буквальном смысле. Визуализация позволяет сделать быстро, без особых усилий. С помощью гибкой системы виджетов система позволяет быстро получить следующую информацию:

- как трафик распределяется во времени,
- какие эндпоинты задействованы,
- топы по сессиям и трафику,
- трафик по географическим направлениям,
- от общего представления до уровня отдельной сессии

Инструменты решения:

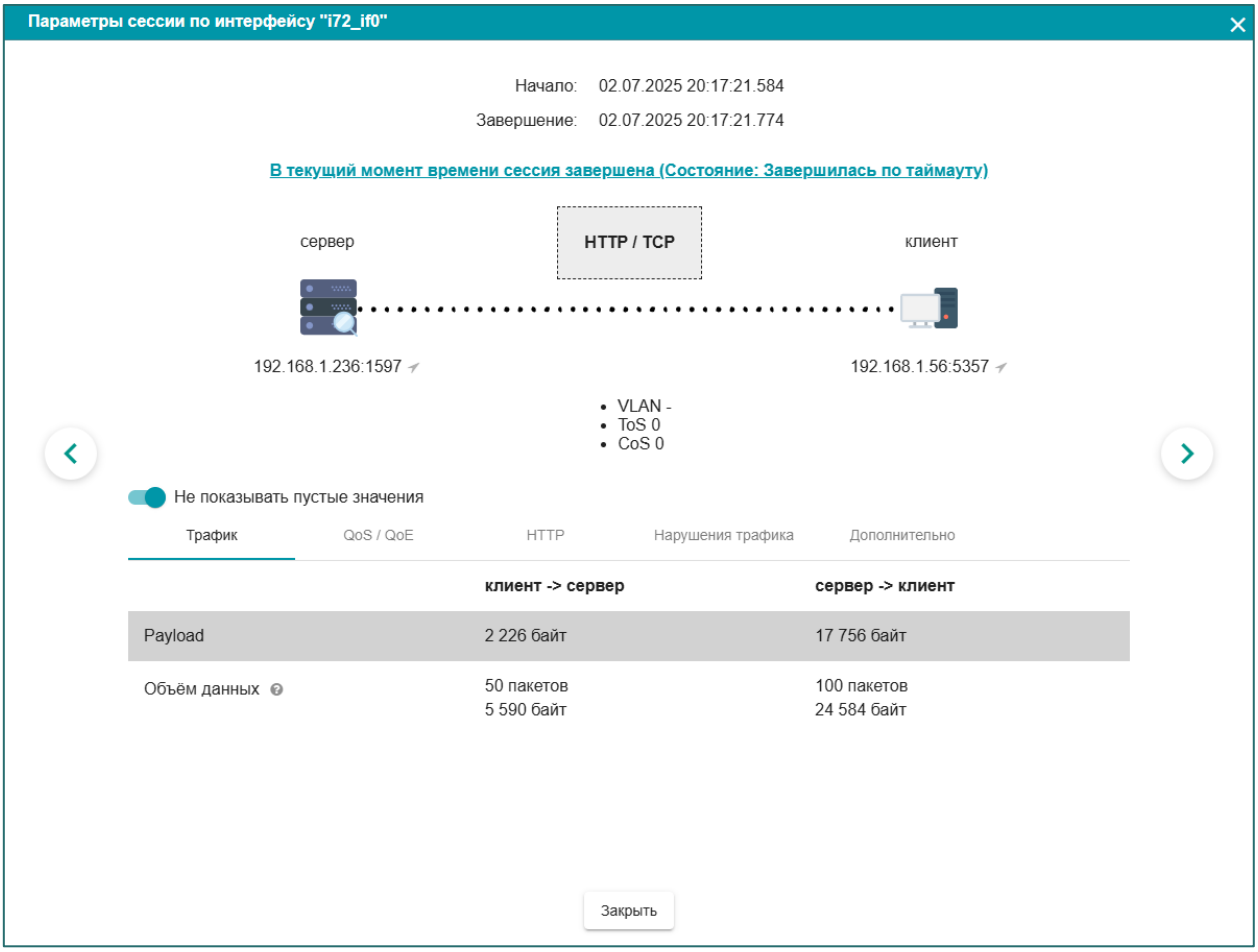
- Типы транспортных протоколов.
- Возможность фильтрации по MAC/IP/VLAN/Протоколам/Подсетям.
- Встроенная машина времени для ретроспективного анализа.
- Возможность детализации данных (drill-down анализ).

Пример 2. Надо увидеть детализацию по конкретной сессии

На нижнем уровне визуализации представлены отдельные сессии. Пользователь получает следующие данные о сессии:

- IPs, ports, VLAN, ToS, QoS, MACs, Domain Names, транспортный протокол, версия IP, версия TLS, время начала и завершения сессии;
- Данные в направлении клиент-> сервер (размер payload, количество пакетов, общий объём данных, переотправлено пакетов/байт, потери пакетов, фрагментировано пакетов, перепутано пакетов/байт)

- Данные в направлении сервер -> клиент (размер payload, количество пакетов, общий объём данных, переотправлено пакетов/байт, потери пакетов, фрагментировано пакетов, перепутано пакетов/байт)
- Флаги TCP
- Время круговой задержки (RTT)
- Время отклика приложжения (ART)
- Для трафика http:
  - Http application context
  - Http cookie
  - Http encoding
  - Http forwarded
  - Request method
  - Http origin
  - Http response
  - Http url
  - Http user agent
  - Http X session type

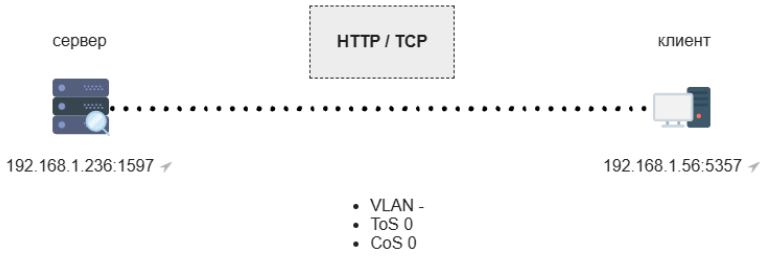


Параметры сессии по интерфейсу "i72_if0"

Начало: 02.07.2025 20:17:21.584

Завершение: 02.07.2025 20:17:21.774

В текущий момент времени сессия завершена (Состояние: Завершилась по таймауту)



- VLAN -
- ToS 0
- CoS 0

Не показывать пустые значения

Трафик | QoS / QoE | HTTP | Нарушения трафика | Дополнительно

Тип сервиса	0
TCP флаги	SAPF
Класс сервиса	0
Время круговой задержки (RTT)	0,92 мс
Время отклика (ART)	153,91 мс

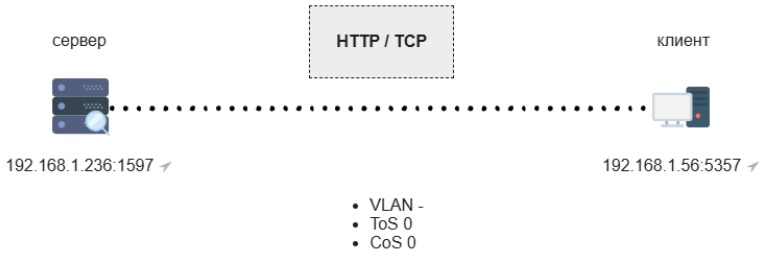
Закрыть

Параметры сессии по интерфейсу "i72_if0"

Начало: 02.07.2025 20:17:21.584

Завершение: 02.07.2025 20:17:21.774

В текущий момент времени сессия завершена (Состояние: Завершилась по таймауту)



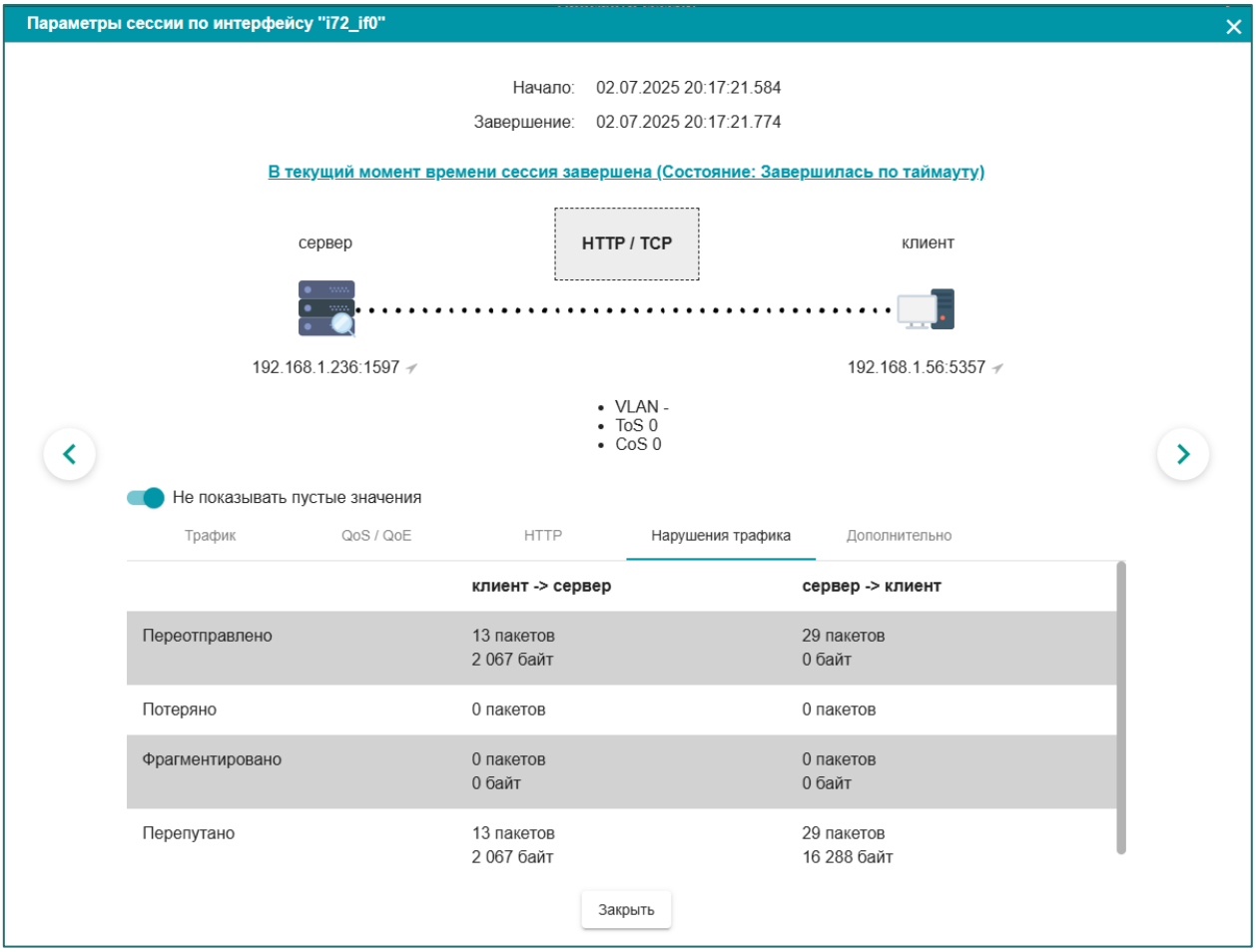
- VLAN -
- ToS 0
- CoS 0

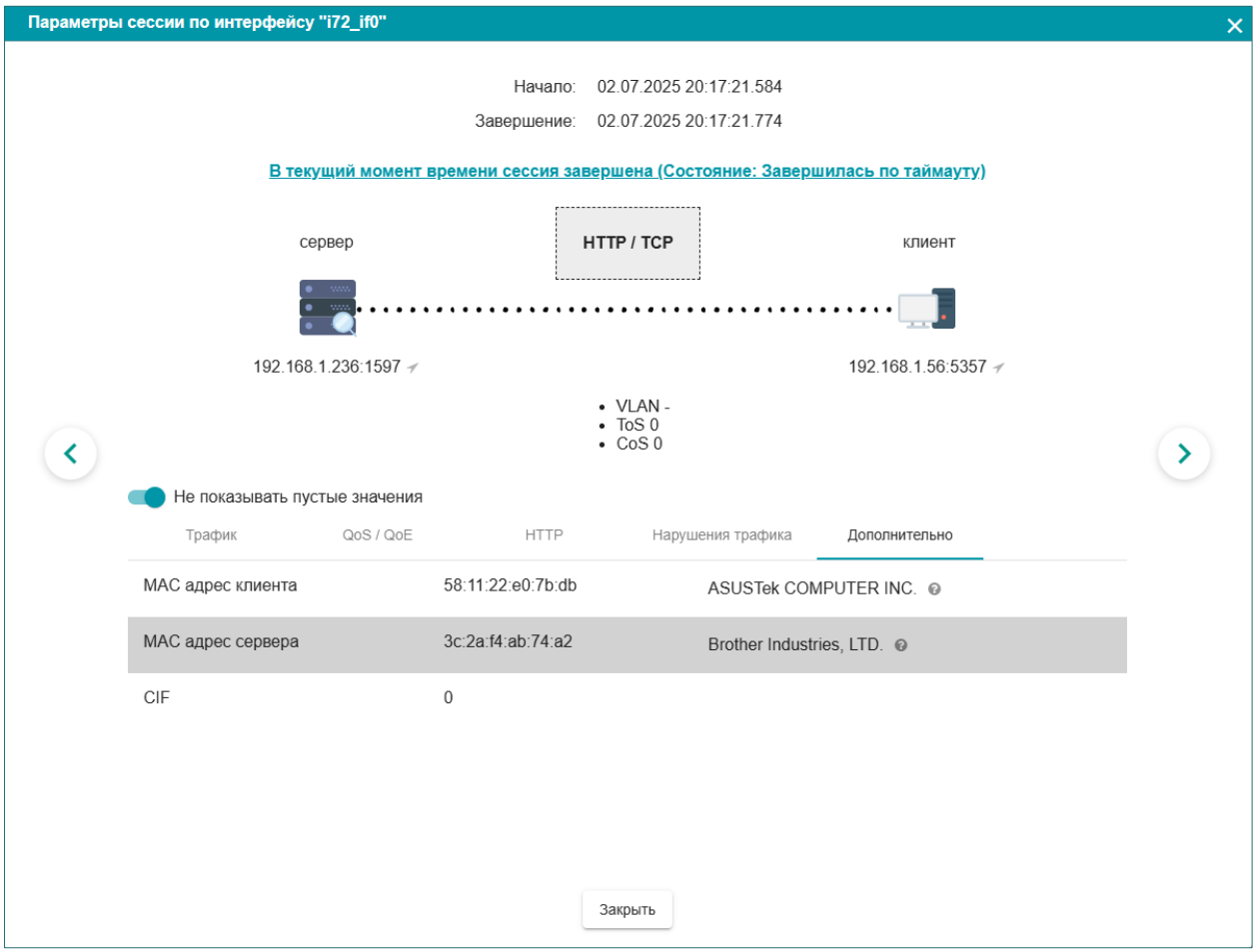
Не показывать пустые значения

Трафик | QoS / QoE | HTTP | Нарушения трафика | Дополнительно

Http application context	application/soap+xml; charset=utf-8
Http url	http://192.168.1.56:5357/1bf2c5ca-dda0-4d6c-b5f1-15ef4a06a960
Http user agent	debut/1.30
Request method	POST

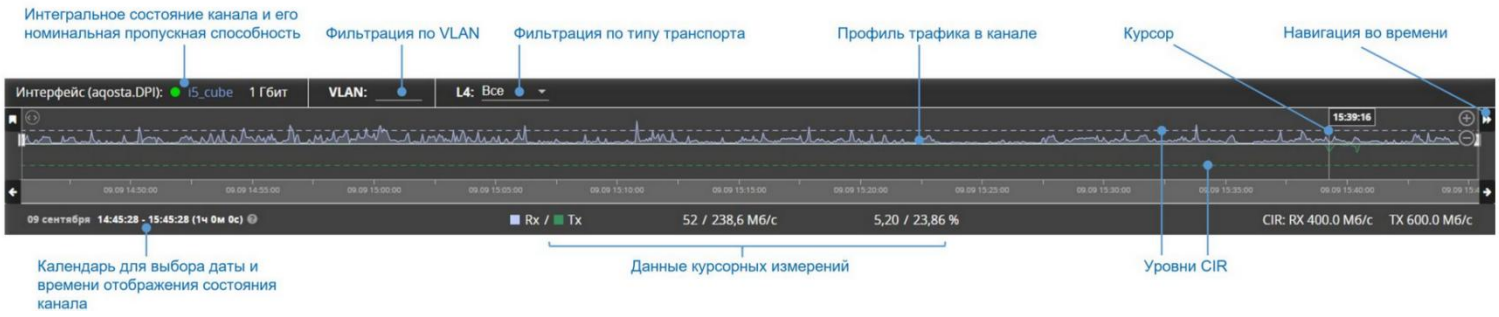
Закрыть


Параметры сессии по интерфейсу "i72_if0"
Начало: 02.07.2025 20:17:21.584
Завершение: 02.07.2025 20:17:21.774
В текущий момент времени сессия завершена (Состояние: Завершилась по таймауту)
сервер
HTTP / TCP
клиент
192.168.1.236:1597
192.168.1.56:5357
VLAN -
ToS 0
CoS 0
Не показывать пустые значения
Трафик
QoS / QoE
HTTP
Нарушения трафика
Дополнительно
клиент -> сервер
сервер -> клиент
Переотправлено
13 пакетов
2 067 байт
29 пакетов
0 байт
Потеряно
0 пакетов
0 пакетов
Фрагментировано
0 пакетов
0 байт
0 пакетов
0 байт
Перепутано
13 пакетов
2 067 байт
29 пакетов
16 288 байт
Закрыть


Параметры сессии по интерфейсу "i72_if0"
Начало: 02.07.2025 20:17:21.584
Завершение: 02.07.2025 20:17:21.774
В текущий момент времени сессия завершена (Состояние: Завершилась по таймауту)
сервер
HTTP / TCP
клиент
192.168.1.236:1597
192.168.1.56:5357
VLAN -
ToS 0
CoS 0
Не показывать пустые значения
Трафик
QoS / QoE
HTTP
Нарушения трафика
Дополнительно
MAC адрес клиента
58:11:22:e0:7b:db
ASUSTek COMPUTER INC.
MAC адрес сервера
3c:2a:f4:ab:74:a2
Brother Industries, LTD.
CIF
0
Закрыть

Пример 3. Пропускная способность и загрузка канала

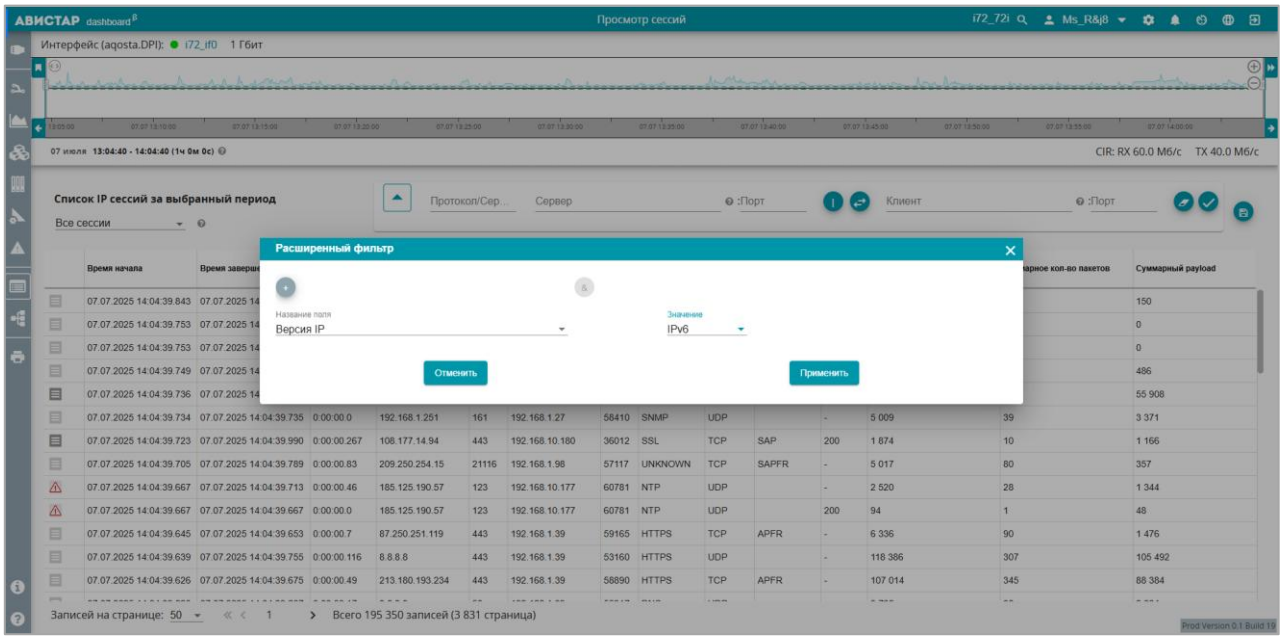
Если объектом мониторинга является целый канал связи, то легко увидеть его загруженность во времени с помощью виджета «Таймлайн»



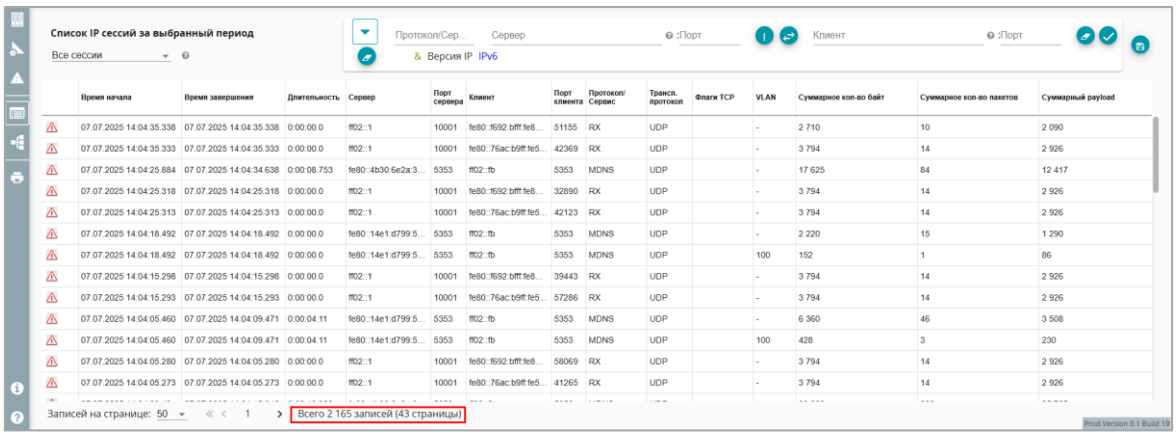
Пример 4. Посмотреть сессии только с IPv6

Шаг 1. Выбираем интервал времени на виджете «Таймлайн».

Шаг 2. На экране «Просмотр сессий» выбираем в расширенном фильтре версию протокола IPv6:



Шаг 3. Получаем список сессий IPv6 (2 165 сессий IPv6):



При необходимости можно посмотреть более детальную информацию о любой из сессий (см. Пример 1).

Аналитика по приложениям

Кейсы, связанные с анализом трафика на прикладном уровне модели OSI.

Пример 5. Найти определенные DNS-запросы в общем трафике

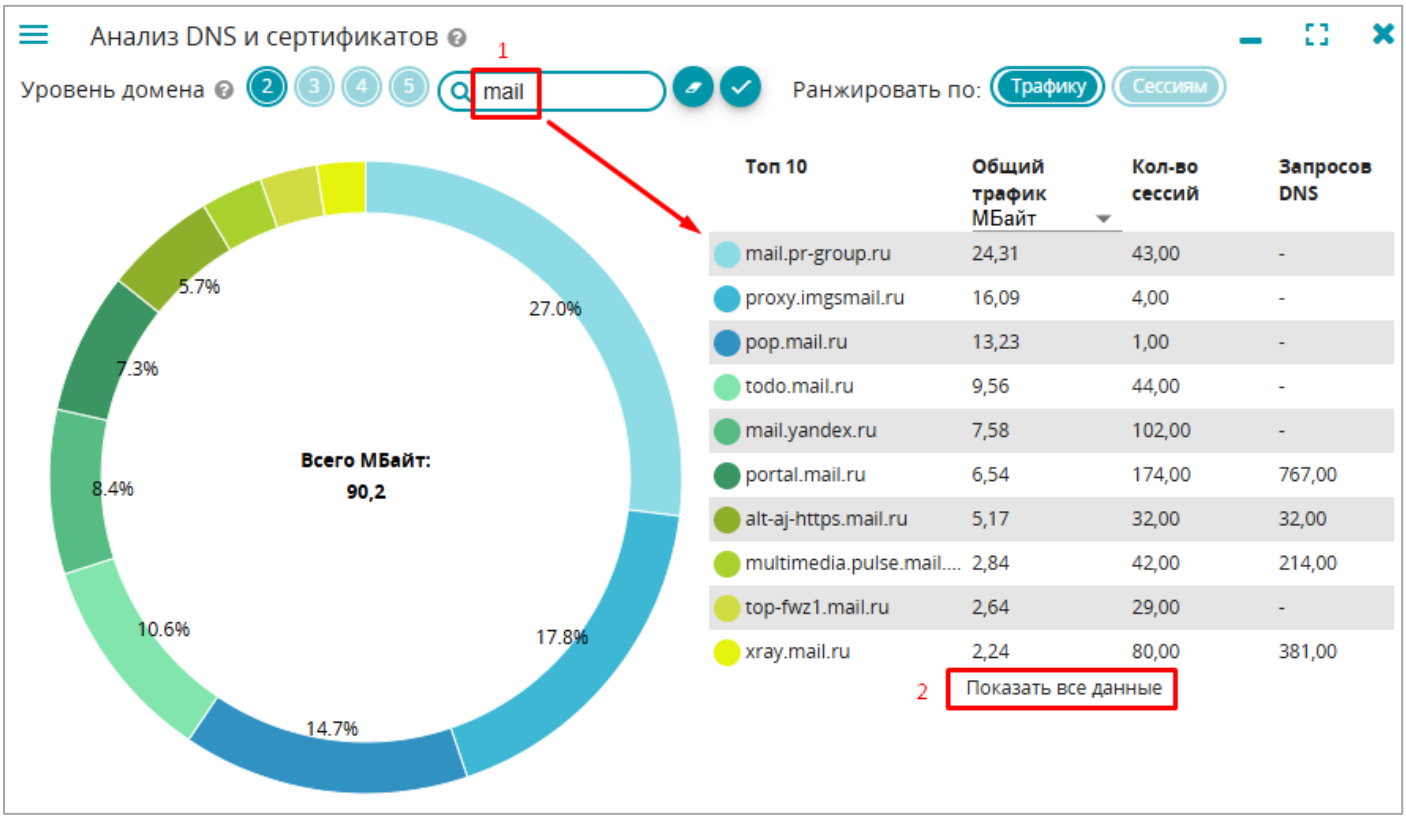
Задача:

1. Найти в потоке любые DNS-запросы, которые содержат слово «mail»
2. посмотреть кто создавал такие запросы

Шаг 1. Открываем виджет «Анализ DNS и сертификатов»

Вводим ключевое слово **mail** в строке поиска, получаем список доменных имен со словом mail.

Шаг 2. Drill-down: выводим весь список доменных имен со словом **mail** :



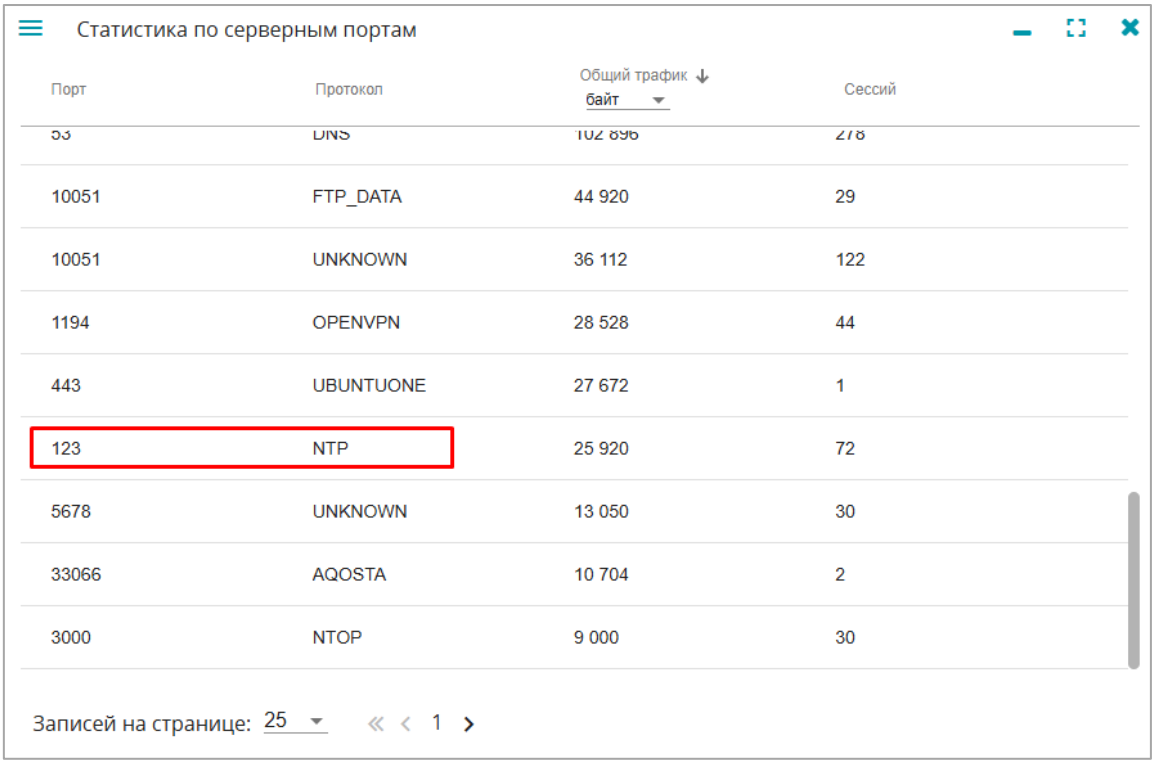
Пример 6. Как задействованы серверные логические порты в информационном обмене

Задача: Увидеть какие серверные порты задействованы в информационном обмене за выбранный интервал времени.

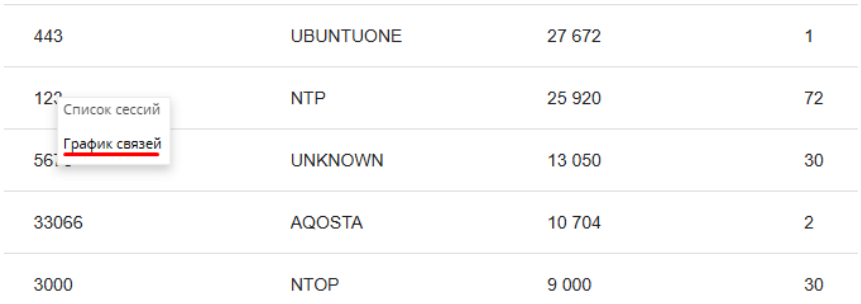
Для чего надо: разбор инцидентов связанных с работой серверов приложений.

Решение: виджет «Статистика по серверным портам»

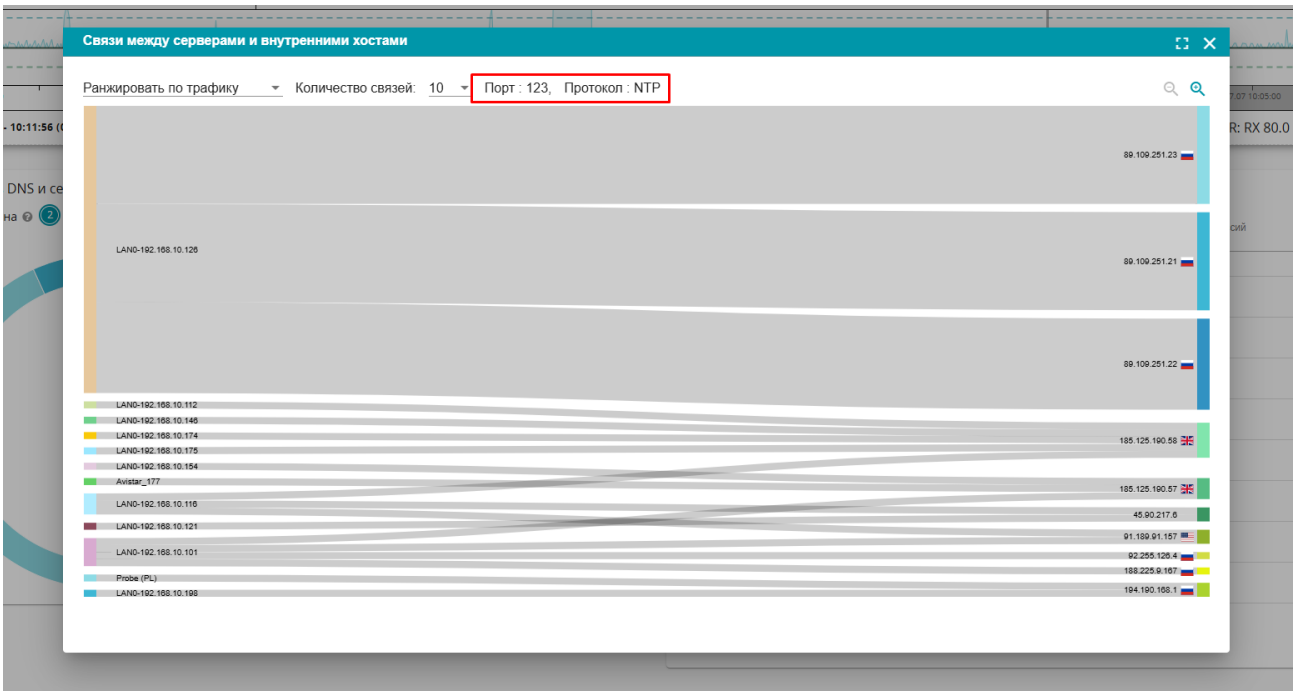
Шаг 1. Выбираем интересующий нас порт:



Шаг 2. Drill-down: смотрим график связей, где «засветился» серверный порт 123:



Шаг 3. Видим все связи (сессий) и все эндпоинты, где был задействован логический порт 123



Мгновенное визуальное представление информации по использованию логических портов серверов приложений:

- Какие порты участвуют в информационном обмене?
- Какие при этом возникают связи между конечными точками обмена информацией?
- Какова интенсивность обмена трафиком между открытыми портами?
- Географическая принадлежность удаленных конечных точек.
- Простая возможность копнуть глубже и проанализировать детали информационного обмена по интересующим направлениям
- Выполнить анализ не только в реальном времени, но и в любой момент в прошлом.

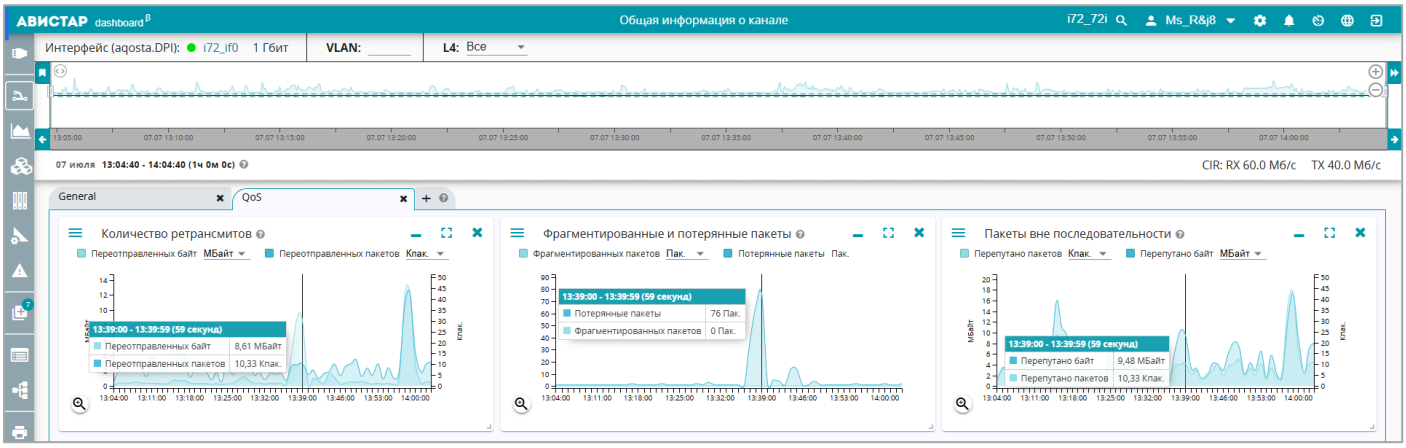
Квалиметрия (качество сервисов и каналов связи)

Проблемные пакеты

Пример 7. Увидеть возможные проблемы с пакетами в канале и как они распределялись во времени.

Шаг 1. Выбираем интервал времени.

Шаг 2. Переходим на экран QoS. Интересующая информация представлена на трёх отдельных виджетах:

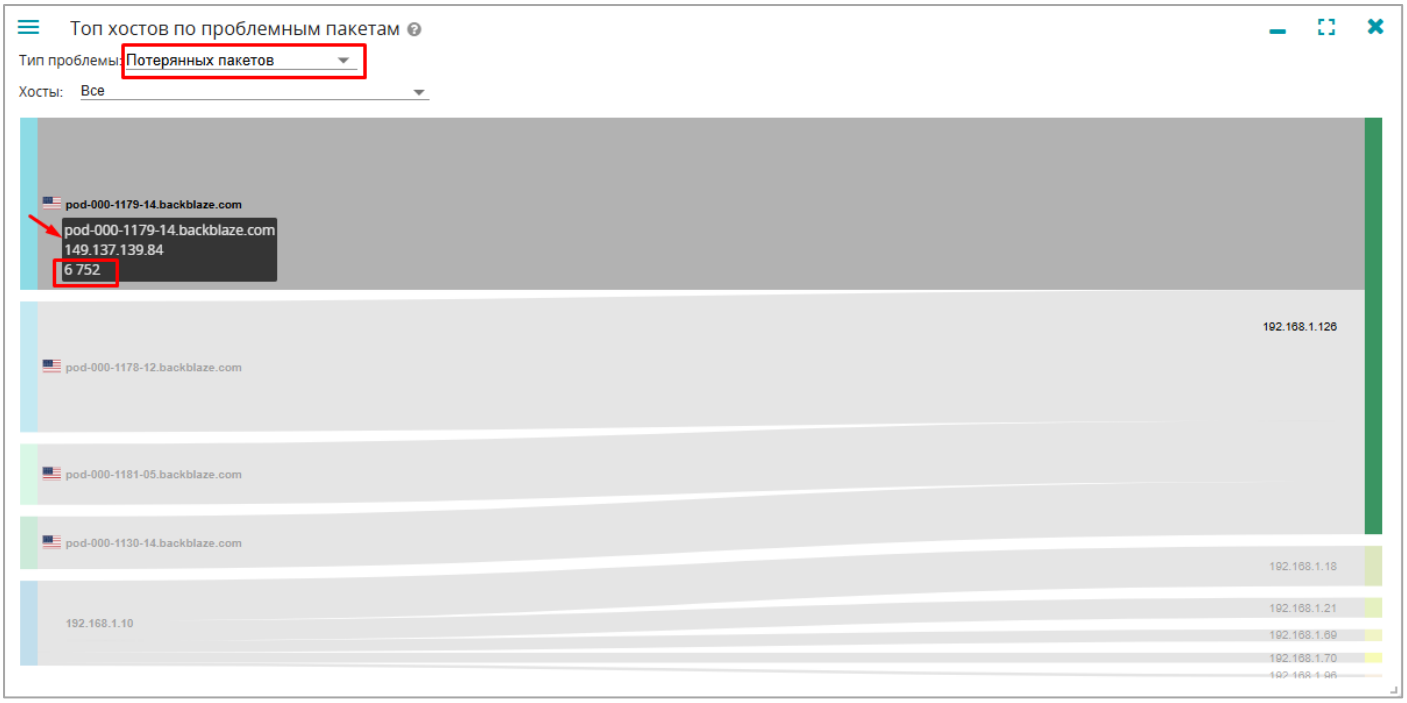


Пример 8. Увидеть топ проблемных связей по потерянным пакетам внутри системы под мониторингом

Шаг 1. Выбираем интервал времени (до 24 часов)

Шаг 2. Открываем виджет «Топ хостов по проблемным пакетам»

Выбираем тип проблемы – «Потерянные пакеты», и получаем интересующие нас связи:



При наведении курсора на эндпоинт, выводится дополнительная информация о связи и хосте.

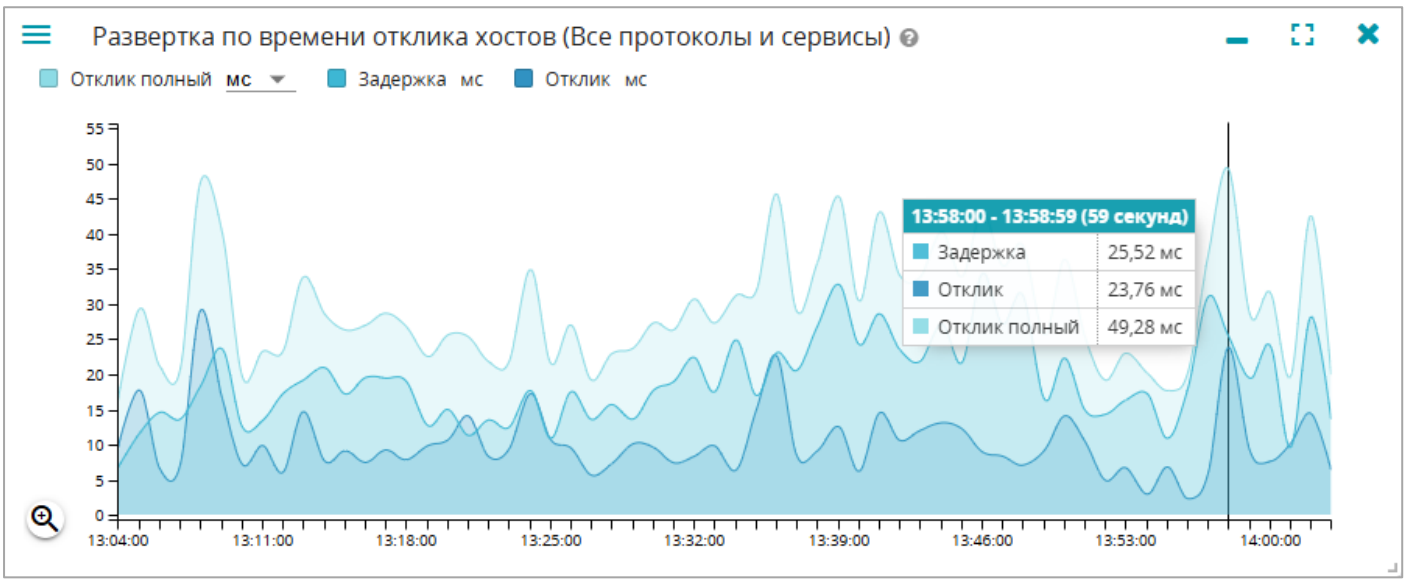
Влияние задержек на сетевые сервисы

Пример 9. Оценка средних задержек в канале связи

Необходимо убедиться, что средняя задержка (application response time) в канале связи не превышала 100 миллисекунд за выбранный интервал времени.

Шаг 1. Выбираем интервал времени.

Шаг 2. Открываем виджет «Развертка по времени отклика хостов» и проверяем условие:

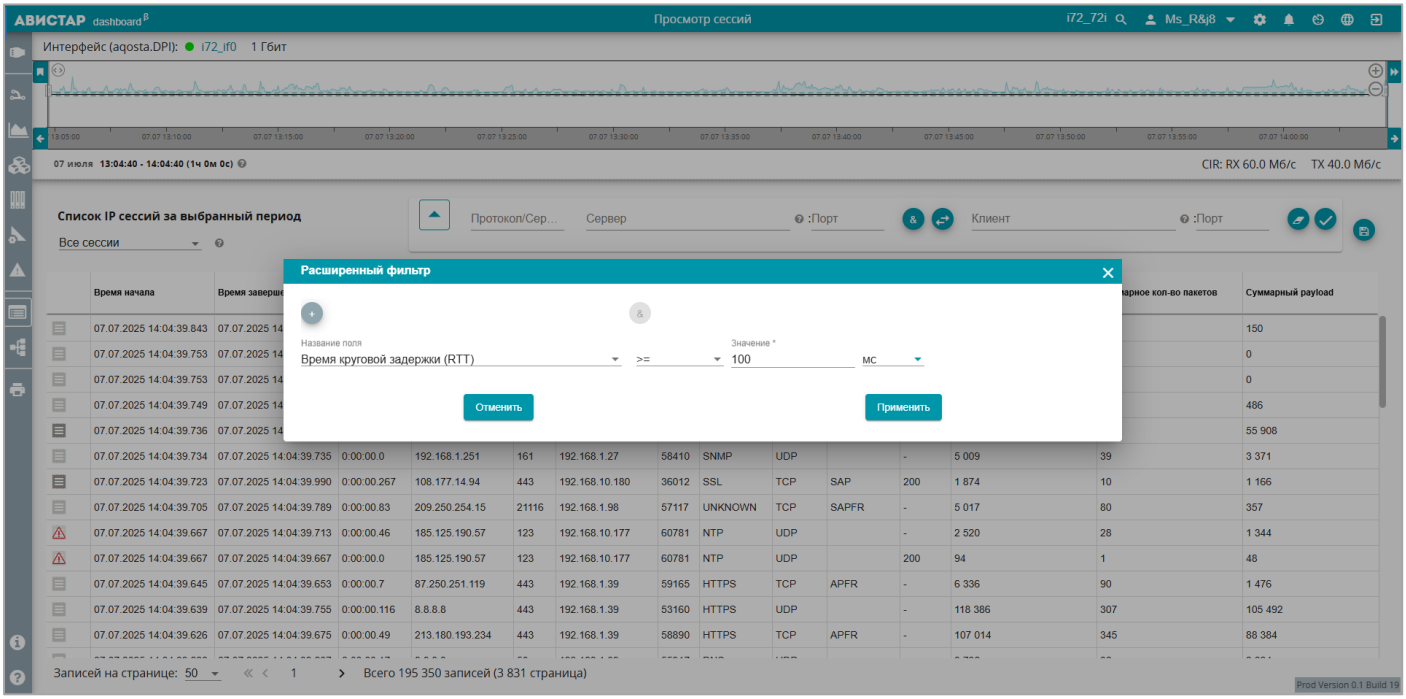


Из данных виджета видно, что за выбранный интервал времени максимальный пик (полный отклик) не превысил 49,25 миллисекунды.

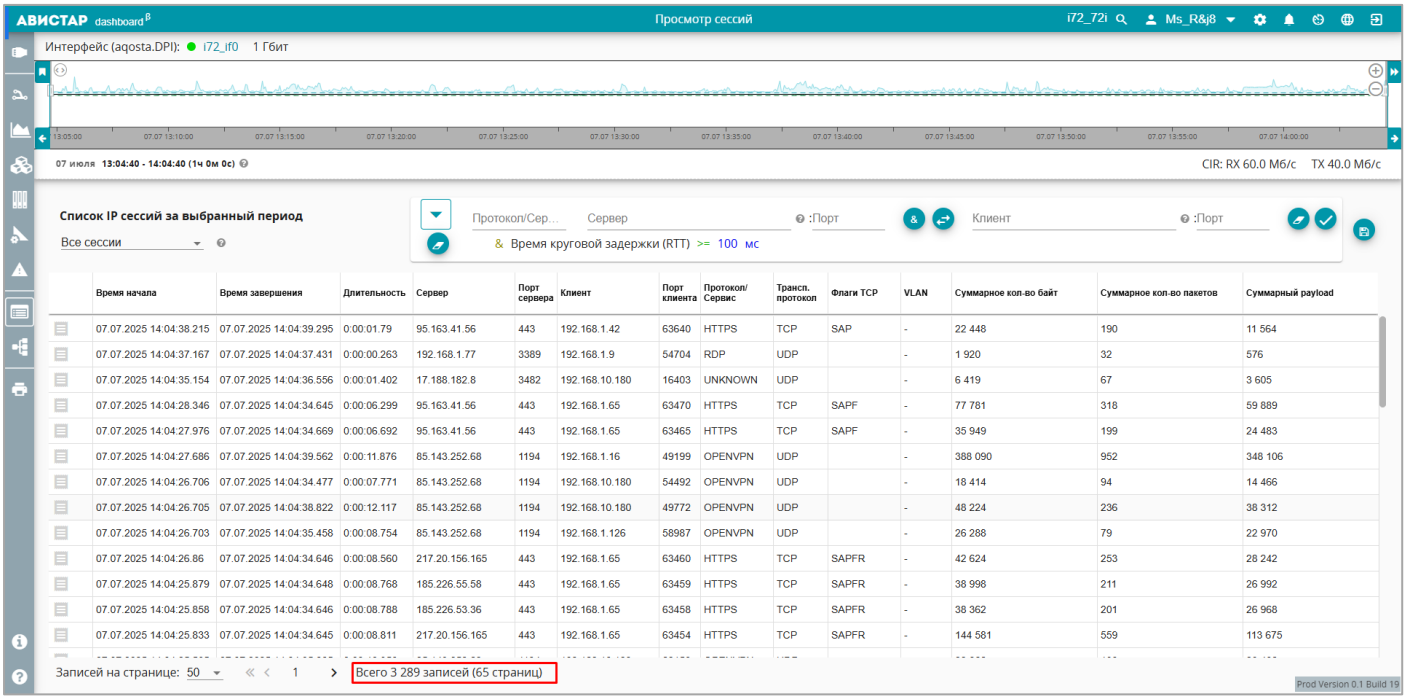
Пример 10. Найти в канале все сессии, для которых время круговой задержки превысило 100 миллисекунд.

Шаг 1. Выбираем интервал времени.

Шаг 2. На экране «Просмотр сессий» выбираем фильтр:



Шаг 3. Смотрим результаты:

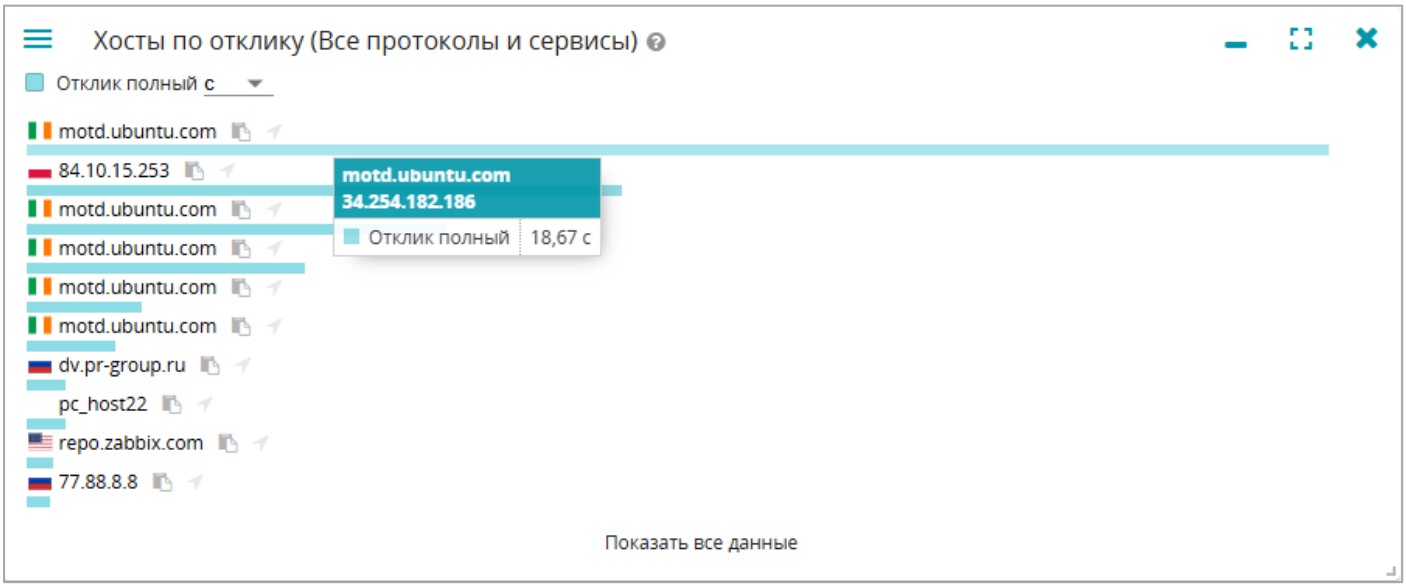


Всего обнаружено 3 289 сессий, удовлетворяющих условию поиска. При необходимости можно раскрыть каждую сессию для более детального изучения (см. Пример 1.)

Пример 11. Необходимо определить самый медленный прикладной сервер за выделенный интервал времени в канале под мониторингом и оценить его негативное влияние на клиентов

Шаг 1. Выбираем интервал времени.

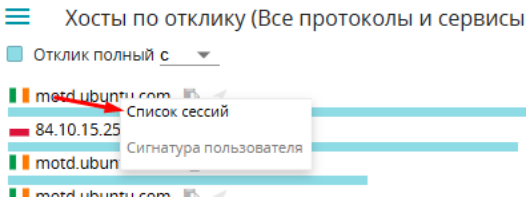
Шаг 2. Открываем виджет «Хосты по отклику (все протоколы и сервисы)»:



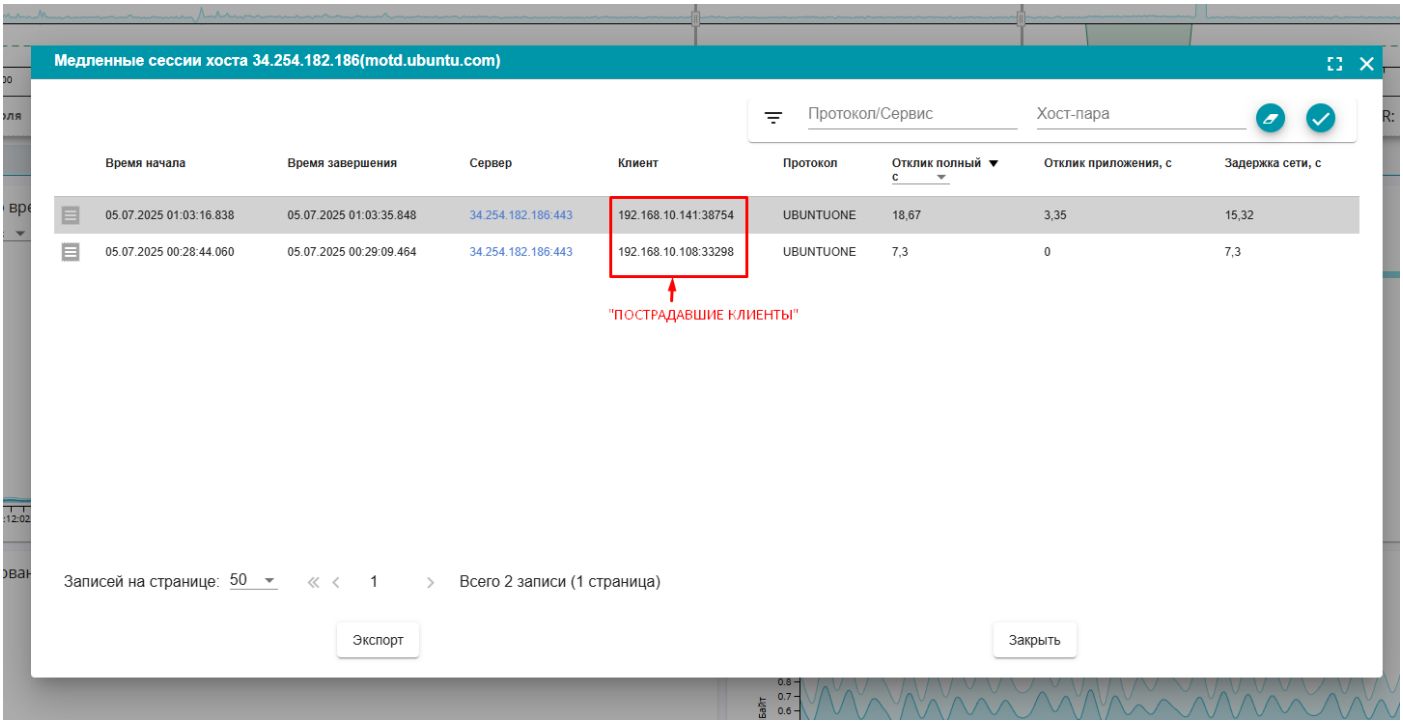
При необходимости можно предварительно выбрать конкретный сетевой сервис или протокол.

Из данных виджета видно, что самым «медленным» сервером был 34.254.182.186 (motd.ubuntu.com). Он имел максимальную задержку 18,67 секунды.

Шаг 3. Drill-down: кликаем на для детализации и оценки его негативного влияния на клиентские хосты:



Шаг 4. Анализируем негативное влияние медленного сервера

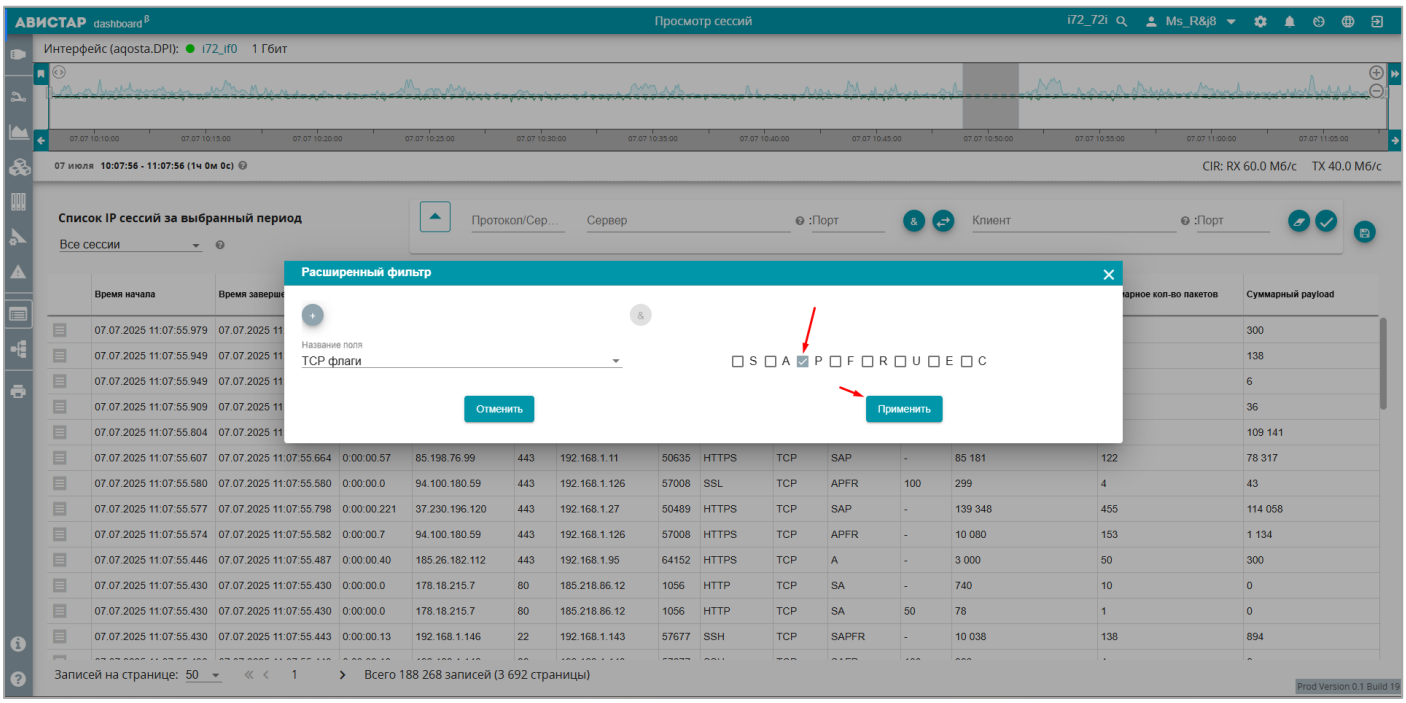


Из этих данных видно, что было всего 2 сессии (2 строки в таблице). Среди «пострадавших» только 2 хост-клиента. Для самой медленной сессии с откликом 18,67 секунды максимум задержки (15,32 секунды) пришлось на круговую задержку сети.

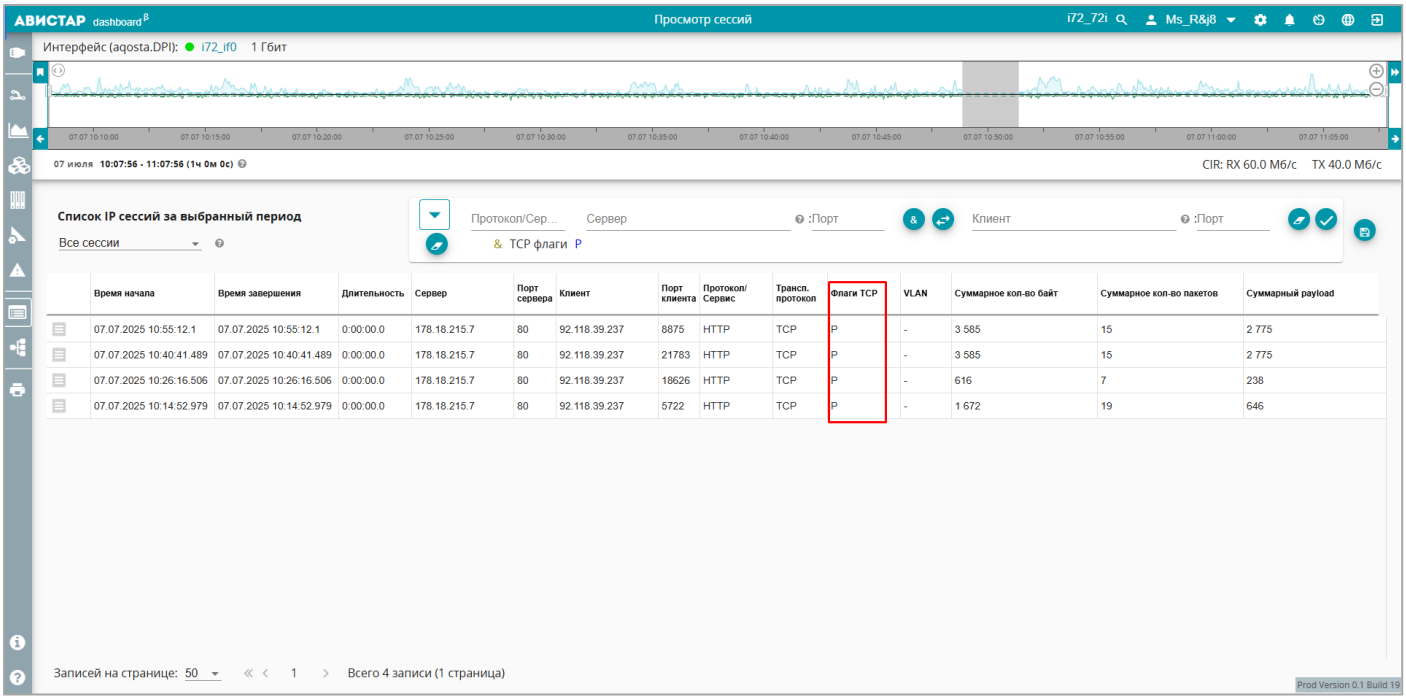
Анализ TCP-флагов сессий

Пример 12. Необходимо увидеть все сессии, которые содержали флаг PUSH в своём информационном обмене

Шаг 1. Выбираем интересующий нас интервал времени и опционально вводим IP адреса и/или логические порты интересующих нас эндпоинтов, и вводим в фильтре необходимые флаги:



Шаг 2. Система выводит список сессий, которые содержат только TCP-флаги «P»:

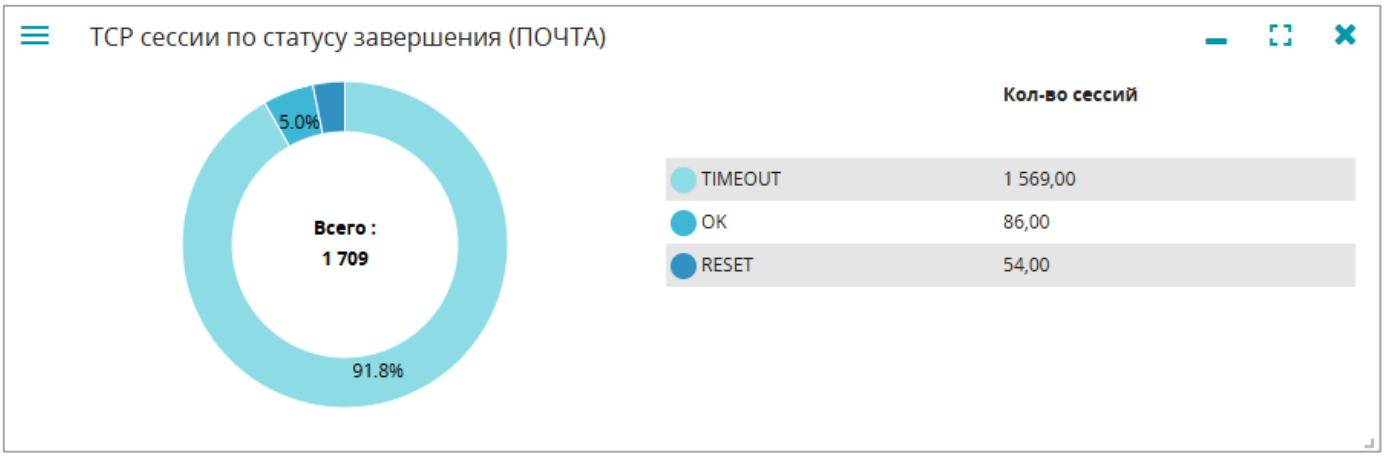


Пример 13. Быстро увидеть распределение сессий по статусам завершения в канале под мониторингом, по группе сервисов «Почта»

Шаг 1. Выбираем интервал времени.

Шаг 2. Выбираем группу сервисов «Почта». В неё входят все почтовые протоколы и сервисы, которые увидела система за интервал.

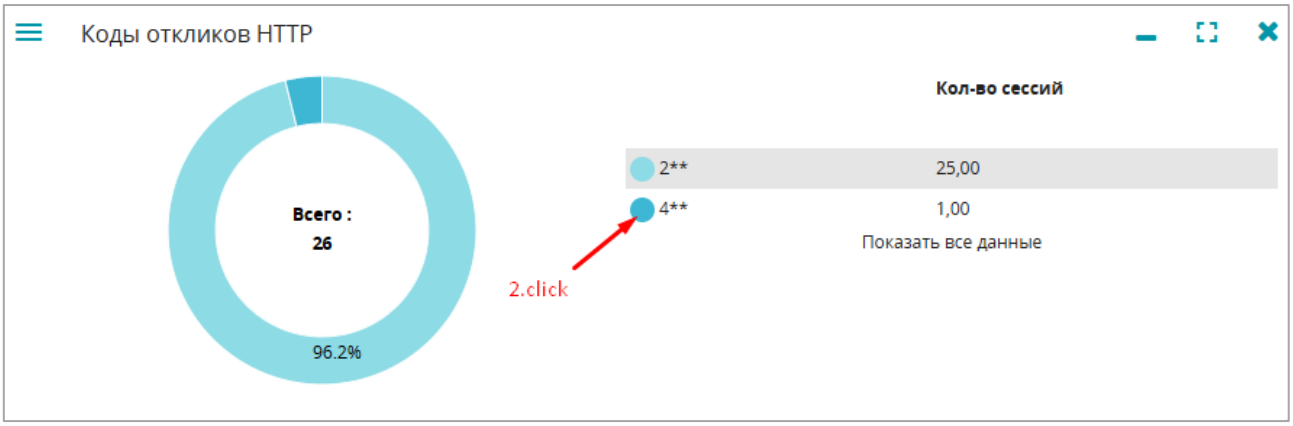
Шаг 3. Смотрим данные на виджете «TCP сессии по статусу завершения»:



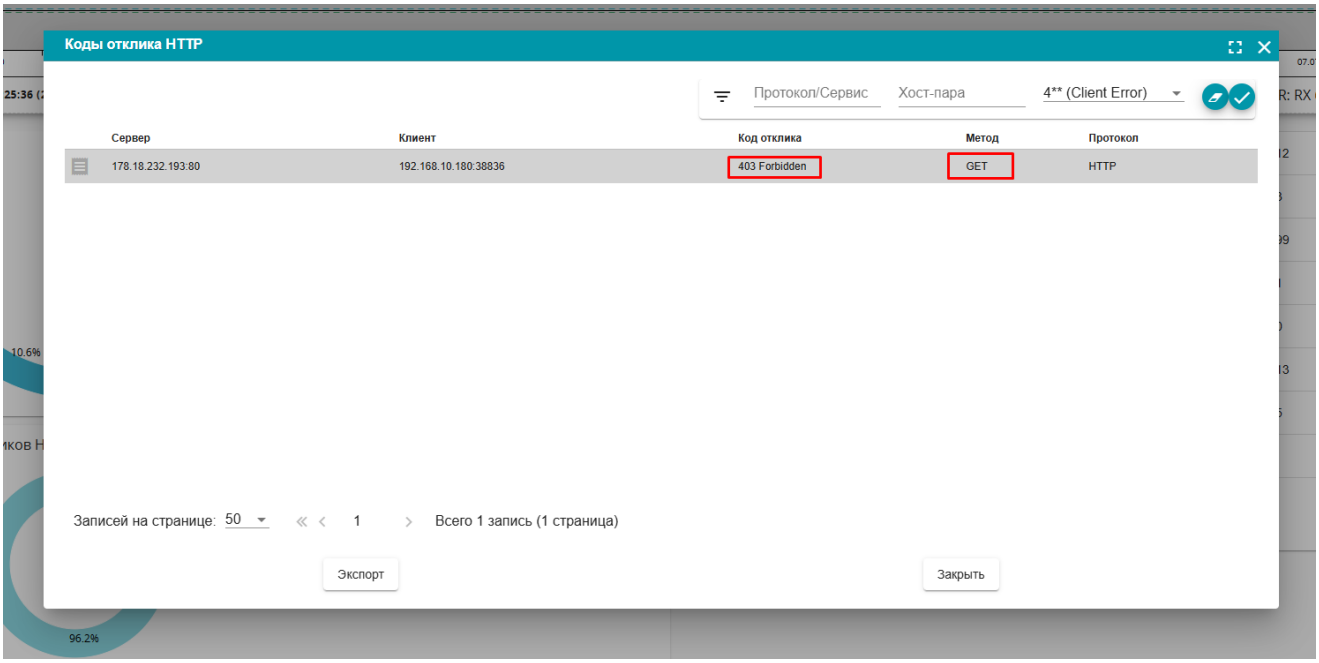
Пример 14. Задача: узнать, появлялись ли отклики «4xx» HTTP-серверов в информационных потоках

Шаг 1. Выбираем интервал времени.

Шаг 2. Открываем виджет «Коды откликов HTTP»:



Шаг 3. Drill-down: смотрим детализацию по обнаруженным сессиям:



перейти на страницу
aVistar/V по QR-коду

МЕТРОЛОГИЧЕСКИЕ
системы

www.mesys.ru

getmail@mesys.ru

Sk Участник