

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 ТСР-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» НТТР-серверов в информационных потоках	15

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

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 ТСР
- 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 интерфейс	y "i72_if0"				×
			Начало: 02. Завершение: 02.	07.2025 20:17:21.584 07.2025 20:17:21.774		
	В тен	<u>кущий момент врем</u>	иени сессия заверш	<u>іена (Состояние: Заве</u>	<u>ршилась по таймауту)</u>	
	с	ервер	нтт	P / TCP	клиент	
			•••••		•••••	
	192.168	8.1.236:1597 🖌			192.168.1.56:5357 🗸	
<			• •	VLAN - ToS 0 CoS 0		\rightarrow
	Трафик	QoS / QoE	HTTP	Нарушения трафика	Дополнительно	
			клиент -> сервер)	сервер -> клиент	
	Payload		2 226 байт		17 756 байт	
	Объём данных 🥹		50 пакетов 5 590 байт		100 пакетов 24 584 байт	
			3ar	фыть		

	сессии по интерфе	ису "1/2_1то"				×
	B	текущий момент врем	Начало: 02 Завершение: 02	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774	лшипась по таймауту)	
	<u>.</u>	текущий момент вре	сти сессия завер		pmunace no raumayry)	
		сервер	нт	P / TCP	клиент	
		•	•••••	•••••••••••	••••••	
	192.	168.1.236:1597 🛷			192.168.1.56:5357 🖌	
			:	VLAN - ToS 0 CoS 0		\bigcirc
$\mathbf{\langle}$				0030		$\mathbf{>}$
	Не показывать	лустые значения			_	
	Трафик	QoS / QoE	HTTP	Нарушения трафика	Дополнительно	
	Тип сервиса				0	_
	ТСР флаги				SAPF	
	Класс сервиса				0	
	Время круговой за	держки (RTT)			0,92 мс	
	Время отклика (AF	RT)			153,91 мс	
			3	акрыть		
Параметры	сессии по интерфе	йсу "i72_if0"				
						×
			Начало: 02	2.07.2025 20:17:21.584		×
			Начало: 02 Завершение: 02	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774		×
	B	текущий момент врем	Начало: 02 Завершение: 02 иени сессия завер	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 2.0 на <u>(</u>Состояние: Заве	<u>ршилась по таймауту)</u>	×
	<u>B</u> .	текущий момент врем сервер	Начало: 02 Завершение: 02 иени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ГР / ТСР	<u>ршилась по таймауту)</u> клиент	×
	B	текущий момент врем сервер	Начало: 02 Завершение: 02 мени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ГР / ТСР	<u>ршилась по таймауту)</u> клиент	×
	B	текущий момент врем сервер	Начало: 02 Завершение: 02 мени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ТР / ТСР	ршилась по таймауту) клиент	×
	<u>₿.</u> 192.	текущий момент вреи сервер 	Начало: 02 Завершение: 02 иени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ТР / ТСР	<u>ршилась по таймауту)</u> клиент 	×
	B - 192-	текущий момент врем сервер 	Начало: 02 Завершение: 02 иени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ГР / ТСР	ршилась по таймауту) клиент 	×
<	₿ 192	текущий момент врем сервер 	Начало: 02 Завершение: 02 мени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ТР / ТСР VLAN - ToS 0 CoS 0	ршилась по таймауту) клиент 	×
<	В 192. Не показывать	текущий момент врем сервер 168.1.236:1597 -/	Начало: 02 Завершение: 02 иени сессия завер НТТ	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ГР / ТСР VLAN - ToS 0 CoS 0	ршилась по таймауту) клиент 	×
<	В : 192. Ме показывать Трафик	текущий момент врем сервер 	Начало: 02 Завершение: 02 иени сессия завер НТТР	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ГР / ТСР VLAN - ТоS 0 СоS 0	ршилась по таймауту) клиент ••••••••••••••••••••••••••••••••••••	×
<	В 192. Ме показывать Трафик Нttp application context	сервер 168.1.236:1597 -/ пустые значения QOS / QOE application/soap+xm	Начало: 02 Завершение: 02 Иени сессия завер НТТР 	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ГР / ТСР VLAN - ТоS 0 СоS 0	ршилась по таймауту) кпиент 	×
<	В 192. Трафик Http application context	текущий момент врем сервер 	Начало: 02 Завершение: 02 иени сессия завер НТТР 	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве Р / ТСР VLAN - ТоS 0 СоS 0 Нарушения трафика 4d6c-b5f1-15ef4a06a960	ршилась по таймауту) Клиент 	×
<	В 192. Ф Не показывать Трафик Нttp application context Http url Http user agent	текущий момент вреи сервер 168.1.236:1597 ≁ 168.1.236:1597 ≮ о пустые значения QoS / QoE application/soap+xm http://192.168.1.56:5 debut/1.30	Начало: 02 Завершение: 02 иени сессия завер НТТР 	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве Р / ТСР VLAN - ТоS 0 Нарушения трафика 4d6c-b5f1-15ef4a06a960	ршилась по таймауту) Клиент 192.168.1.56:5357 -/ Дополнительно	×
<	В 192. 192. Ме показывать Трафик Http application context Http url Http user agent Request method	текущий момент врем сервер 168.1.236:1597 -/ л пустые значения QoS / QoE application/soap+xm http://192.168.1.56:5 debut/1.30 POST	Начало: 02 Завершение: 02 Иени сессия завер НТТР ••• ••• ••• ••• ••• ••• ••• ••• •••	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ТР / ТСР VLAN - ТоS 0 СоS 0 Нарушения трафика 4d6c-b5f1-15ef4a06a960	ршилась по таймауту) Клиент 	×
<	В 192. 192. Трафик Http application context Http url Http user agent Request method	текущий момент врем сервер 168.1.236:1597 ✓ 168.1.236:1597 ✓ апустые значения QoS / QoE application/soap+xm http://192.168.1.56:5 debut/1.30 POST	Начало: 02 Завершение: 02 иени сессия завер НТТР It; charset=utf-8 357/1bf2c5ca-dda0-	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве Р / ТСР VLAN - ТоЅ 0 СоЅ 0 Нарушения трафика 4d6c-b5f1-15ef4a06a960	ршилась по таймауту) Клиент ••••••••••••••••••••••••••••••••••••	×
<	В 192. 192. Трафик Http application context Http url Http user agent Request method	текущий момент вреи сервер 168.1.236:1597 -/ 168.1.236:1597 -/ аррісаtion/soap+xm http://192.168.1.56:5 debut/1.30 POST	Начало: 02 Завершение: 02 Иени сессия завер НТТР • • • • • • • • • • • • • • • • • •	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве Р / ТСР VLAN - Тоб 0 Соб 0 Нарушения трафика 4d6c-b5f1-15ef4a06a960	ршилась по таймауту) КЛИЕНТ ••••••••••••••••••••••••••••••••••••	×
<	В 192. 192. • Не показывать Трафик Http application context Http url Http url Http user agent Request method	текущий момент врей сервер 168.1.236:1597 -/ • пустые значения QoS / QoE application/soap+xm http://192.168.1.56:5 debut/1.30 POST	Начало: 02 Завершение: 02 Иени сессия завер НТТР I; charset=utf-8 357/1bf2c5ca-dda0-	2.07.2025 20:17:21.584 2.07.2025 20:17:21.774 шена (Состояние: Заве ТР / ТСР VLAN - ТоS 0 СоS 0 Нарушения трафика 4d6c-b5f1-15ef4a06a960	ршилась по таймауту) Клиент 	×

Параметры	сессии по интерфейсу	"i72_if0"						×
			Нациял	. 02 07 2025 20	1.17.21 281			
			Завершение	e: 02.07.2025 20):17:21.304			
	-	u l						
	В теку	щии момент вј	ремени сессия :	завершена (Сост	ояние: Заверши	<u>илась по таимауту)</u>		
	Cel	рвер		HTTP / TCP		клиент		
						_		
	•		• • • • • • • • • • • • •	•••••	• • • • • • • • • • •	••••• 🛄		
	192.168.	1.236:1597 🗸				192.168.1.56:5357	1	
				• VLAN -				
(ToS 0 CoS 0 				\mathbf{S}
$\mathbf{\mathbf{U}}$	П Не показывать пус	тые значения						$\mathbf{\cdot}$
	Трафик	QoS / QoE	HTTP	Наруш	ения трафика	Дополнительно		
						H		
			клиент -> со	ервер	cep	вер -> клиент		
	Переотправлено		13 пакетов 2 067 байт		29 r 0 6a	18КӨТОВ ЭЙТ		
	-		2 001 0411		0.00			
	Потеряно		0 пакетов		0 па	акетов		
	Фрагментировано		0 пакетов 0 байт		0 па 0 ба	акетов		
	_		o oum					
	Перепутано		13 пакетов 2 067 байт		29 r 16 2	акетов 288 байт	l	
				Закрыть				
				Закрыть				
Параметры	сессии по интерфейсу	"i72 if0"						~
Параметры	і сессии по интерфейсу	"i72_if0"						×
Параметры	і сессии по интерфейсу`	"i72_if0"	Начало	p: 02.07.2025 20):17:21.584			×
Параметры	і сессии по интерфейсу	"i72_if0"	Начало Завершение	p: 02.07.2025 20 e: 02.07.2025 20):17:21.584):17:21.774			×
Параметры	і сессии по интерфейсу В теку	"i72_if0" щий момент в	Начала Завершения ремени сессия :	о: 02.07.2025 20 е: 02.07.2025 20 завершена (Сост):17:21.584):17:21.774 :ояние: Заверши	илась по таймауту)		×
Параметры	і сессии по интерфейсу <u>В теку</u>	"i72_if0" щий момент вј	Начали Завершении ремени сессия г	о: 02.07.2025 2(e: 02.07.2025 2(завершена (Сост):17:21.584):17:21.774 гояние: Заверши	илась по таймауту)		×
Параметры	і сессии по интерфейсу <u>В теку</u> сеј	" i72_if0" тщий момент вј	Начали Завершени ремени сессия :	о: 02.07.2025 20 е: 02.07.2025 20 завершена (Сост НТТР / ТСР):17:21.584):17:21.774 гояние: Заверши	илась по таймауту) клиент		×
Параметры	і сессии по интерфейсу <u>В теку</u> сеј	" i72_if0" лщий момент в рвер	Начали Завершении ремени сессия (о: 02.07.2025 20 е: 02.07.2025 20 завершена (Сост НТТР / ТСР):17:21.584):17:21.774 : сояние: Заверши	илась по таймауту) клиент		×
Параметры	і сессии по интерфейсу <u>В теку</u> сеј	" і72_іf0" «щий момент в рвер	Начали Завершении ремени сессия : 	о: 02.07.2025 20 е: 02.07.2025 20 завершена (Сост НТТР / ТСР):17:21.584):17:21.774 тояние: Заверши	илась по таймауту) клиент		×
Параметры	I сессии по интерфейсу В теку сеј 192.168.	" і72_іі0 " ч щий момент в рвер 1.236:1597 <i>-</i>	Начали Завершении ремени сессия (о: 02.07.2025 20 е: 02.07.2025 20 завершена (Сост НТТР / ТСР):17:21.584):17:21.774 :ояние: Заверши	илась по таймауту) клиент ••••• 192.168.1.56:5357	1	×
Параметры	і сессии по интерфейсу В теку сеј 192.168.	" i72_if0" <u>ищий момент в</u> рвер 1.236:1597 <i>-</i>	Начали Завершении ремени сессия :	о: 02.07.2025 20 e: 02.07.2025 20 завершена (Сост НТТР / ТСР • VLAN - • TOS 0):17:21.584):17:21.774 тояние: Заверши	илась по таймауту) клиент •••••• []] 192.168.1.56:5357	1	×
Параметры	I сессии по интерфейсу В теку сеј 192.168.	" і72_іі0 " лщий момент в рвер 1.236:1597 <i>-</i> /	Начали Завершении ремени сессия : [о: 02.07.2025 20 e: 02.07.2025 20 завершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0):17:21.584):17:21.774 :ояние: Заверши	илась по таймауту) клиент ••••• []] 192.168.1.56:5357	Ť	×
Параметры	I сессии по интерфейсу В теку сер 192.168.	" i72_if0" <u>ищий момент в</u> рвер 1.236:1597 <i>-</i> тые значения	Начали Завершении ремени сессия :	о: 02.07.2025 20 e: 02.07.2025 20 завершена (Сост HTTP / TCP • VLAN - • ToS 0 • CoS 0):17:21.584):17:21.774 тояние: Заверши	илась по таймауту) клиент •••••• 192.168.1.56:5357	7	×
Параметры	I сессии по интерфейсу В теку сер 192.168. Ф Не показывать пус Трафик	" і72_іі0 " м <u>иий момент в</u> рвер 1.236:1597 <i>-</i> / тые значения _{QOS / QOE}	Начали Завершении ремени сессия и [о: 02.07.2025 20 e: 02.07.2025 20 завершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0 Наруш	::17:21.584 ::17:21.774 ::ояние: Заверши	1ЛАСЬ ПО ТАЙМАУТУ) КЛИЕНТ ••••• П 192.168.1.56:5357 Дополнительно	7	×
Параметры	I сессии по интерфейсу В теку сер 192.168. ФНе показывать пус Трафик МАС адрес клиента	"'172_if0'' /ЩИЙ МОМЕНТ E рвер 1.236:1597 -/ Тые значения 	Начали Завершении ремени сессия : 	о: 02.07.2025 20 e: 02.07.2025 20 вавершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0 Наруш b	2:17:21.584 2:17:21.774 2:09ние: Заверши сояние: Заверши ения трафика ASUSTek COMF	клиент клиент 192.168.1.56:5357 Дополнительно	1	×
Параметры	I сессии по интерфейсу В теку сер 192.168. ••••••••••••••••••••••••••••••••••••	"I72_if0" щий момент в рвер 1.236:1597 -/ тые значения QOS / QOE	Начали Завершении ремени сессия : [[] 	о: 02.07.2025 20 e: 02.07.2025 20 завершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0 Наруш Ib	2:17:21.584 2:17:21.774 сояние: Заверши сояние: Заверши	алась по таймауту) клиент •••••• []] 192.168.1.56:5357 Дополнительно 2UTER INC. @	7	×
Параметры	I сессии по интерфейсу В теку сер 192.168. ФАС адрес клиента МАС адрес сервера	"'172_if0'' ищий момент в рвер 1.236:1597 -/ тые значения доб / доб	Начали Завершении ремени сессия : [[]]]] 58:11:22:e0:7b:d] 3c:2a:14:ab:74:a;	о: 02.07.2025 20 e: 02.07.2025 20 вавершена (Сост HTTP / TCP • VLAN - • ToS 0 • CoS 0 Наруш Ib	0:17:21.584 0:17:21.774 сояние: Заверши сения трафика ASUSTek COMF Brother Industrie	илась по таймауту) клиент ••••••••••••••••••••••••••••••••••••	7	×
К	I сессии по интерфейсу В теку сер 192.168. ••••••••••••••••••••••••••••••••••••	" !72_if0'' лщий момент в рвер 1.236:1597 <i>-</i> / тые значения _{QOS / QOE}	Начали Завершении ремени сессия : [[] 58:11:22:e0:7b:d 3c:2a:f4:ab:74:a2 0	о: 02.07.2025 20 e: 02.07.2025 20 завершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0 Наруш b	9:17:21.584 9:17:21.774 сояние: Заверши ения трафика ASUSTek COMF Brother Industrie	илась по таймауту) клиент •••••• []] 192.168.1.56:5357 Дополнительно PUTER INC. @ s, LTD. @	7	×
К	I сессии по интерфейсу В теку сер 192.168. • Не показывать пус Трафик МАС адрес клиента МАС адрес сервера CIF	"I72_if0" ЩИЙ МОМЕНТ В рвер 1.236:1597 -/ Тые значения QOS / QOE	Начали Завершении ремени сессия : [о: 02.07.2025 20 e: 02.07.2025 20 вавершена (Сост HTTP / TCP • VLAN - • ToS 0 • CoS 0 Наруш Ib	2:17:21.584 2:17:21.774 сояние: Заверши сояние: Заверши ения трафика ASUSTek COMF Brother Industrie	клиент клиент ••••••••••••••••••••••••••••••••••••	1	×
К	I сессии по интерфейсу В теку сер 192.168. ••••••••••••••••••••••••••••••••••••	"I72_if0" щий момент в рвер 1.236:1597 -/ тые значения QoS / QoE	Начали Завершении ремени сессия з [[58:11:22:е0:7b:d 3c:2a:14:ab:74:a/ 0	о: 02.07.2025 20 e: 02.07.2025 20 вавершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0 Наруш b	2:17:21.584 2:17:21.774 сояние: Заверши ения трафика ASUSTek COMF Brother Industrie	илась по таймауту) клиент •••••• []] 192.168.1.56:5357 Дополнительно PUTER INC. @ s, LTD. @	7	×
К	I сессии по интерфейсу В теку сер 192.168. Ф Не показывать пус Трафик МАС адрес клиента МАС адрес сервера CIF	"I72_if0" ПЦИЙ МОМЕНТ В рвер 1.236:1597 -/ ТЫЕ ЗНАЧЕНИЯ QOS / QOE	Начали Завершении ремени сессия : [о: 02.07.2025 20 e: 02.07.2025 20 вавершена (Сост HTTP / TCP • VLAN - • ToS 0 • CoS 0 Наруш Ib	2:17:21.584 2:17:21.774 сояние: Заверши сения трафика ASUSTek COMF Brother Industrie	илась по таймауту) клиент ••••••••••••••••••••••••••••••••••••	7	×
К	I сессии по интерфейсу В теку сер 192.168. • Не показывать пуст Трафик МАС адрес клиента МАС адрес сервера CIF	"I72_if0" пций момент в рвер 1.236:1597 // Тые значения QOS / QOE	Начали Завершении ремени сессия : [[58:11:22:е0:7b:d 3c:2a:f4:ab:74:a: 0	о: 02.07.2025 20 e: 02.07.2025 20 вавершена (Сост НТТР / ТСР • VLAN - • ToS 0 • CoS 0 Наруш b	2:17:21.584 2:17:21.774 сояние: Заверши ения трафика ASUSTek COMF Brother Industrie	илась по таймауту) клиент •••••• []] 192.168.1.56:5357 Дополнительно PUTER INC. @ s, LTD. @	7	×

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»

Интегральное состояние канала и его номинальная пропускная способность Фильтрация по VLAN	Фильтрация по типу транспорта	Профиль трафика в канале	Курсор Навигация	а во времени
Интерфейс (aqosta.DPI): 🖣5_cube 1 Гбит VLAN: 📥 L4: Все	<u> • +</u>			
			15:35	:16 🕀 🖟
and the second second second second	M			
09 сентября 14:45:28 - 15:45:28 (14 Ом Ос) @	Rx / 1x 52 / 238,6 M6/c	5,20 / 23,86 %	CIR: RX 400.0 M	5/c TX 600.0 M6/c
Календарь для выбора даты и времени отображения состояния канала	Данные курсорных измерен	ий	 Уровни CIR	

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:

CTAP	dashboard*							просм	отр сессий					112_121 0	R ≚ Ms_R8j8 ▼	13 8 69	œ
Интерф	рейс (aqosta.DPI): 🌻 i7	2_if0 1 Гбит															
	adates and a	- <u>~~</u>	ana			<u>a</u>	THEFT			J.M.			seeres too bo				1
13 03 00	07.07 13.10 00	87.07 13.1	13:00	87.07 13.25	100 07.07 V	25.00	07.07.12.00:00		07.07 12 39:00		17.0712-40.00	07/1	07.13.45.00 07.07 i	150.00	07.07 13:55-00	07.07 14.00.00	ST.
07 inte	n# 13:04:40 - 14:04:40 (14 0)	м Oc) 🔘													CIR: R	X 60.0 M6/c TX 40	0.0 N
Спи	сок IP сессий за выбр	анный пери	од		Прото	кол/Сер	Сервер			@ :I	Торт	0	С Клиент		ө :Порт	00	
Bce	сессии 👻	0											-				
	Время начала	Время заверши	Расши	иренный фи	ињтр									×	арное кол-во пакетов	Суммарный payload	
	07.07.2025 14:04:39.843	07.07.2025 14	0				6									150	
	07.07.2025 14:04:39.753	07.07.2025 14	Названи Верси	e nons s IP					BHANNANA IPv6							0	
	07.07.2025 14:04:39.753	07.07.2025 14	in the second													0	
	07.07.2025 14:04:39.749	07.07.2025 14			Отме	аль					_	Трименить				486	
	07.07.2025 14:04:39.736	07.07.2025 14				_										55 908	
	07.07.2025 14:04:39.734	07.07.2025 14:	04:39.735	0.00:00.0	192.168.1.251	161	192.168.1.27	58410	SNMP	UDP			5 009	39		3 371	
	07.07.2025 14:04:39.723	07.07.2025 14:	04:39.990	0:00:00.267	108.177.14.94	443	192.168.10.180	36012	SSL	TCP	SAP	200	1 874	10		1 166	
	07.07.2025 14:04:39.705	07.07.2025 14:	04:39.789	0:00:00.83	209.250.254.15	21116	192.168.1.98	57117	UNKNOWN	TCP	SAPFR		5 017	80		357	
	07.07.2025 14:04:39.667	07.07.2025 14:	04:39.713	0:00:00.46	185.125.190.57	123	192.168.10.177	60781	NTP	UDP			2 520	28		1 344	
	07.07.2025 14:04:39.667	07.07.2025 14:	04:39.667	0:00:00.0	185.125.190.57	123	192.168.10.177	60781	NTP	UDP		200	94	1		48	
	07.07.2025 14:04:39.645	07.07.2025 14	04:39.653	0:00:00.7	87.250.251.119	443	192.168 1.39	59165	HTTPS	TCP	APFR		6 336	90		1 476	
	07.07.2025 14:04:39.639	07.07.2025 14:	04:39.755	0:00:00.116	8.8.8.8	443	192.168.1.39	53160	HTTPS	UDP			118 386	307		105 492	
	07.07.2025 14:04:39.626	07.07.2025 14:	04:39.675	0:00:00.49	213.180.193.234	443	192.168.1.39	58890	HTTPS	TCP	APFR		107 014	345		88 384	

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

Bce	сессии 👻	0		۵ ۵	Версия	IP IPv6								_
	Время начала	Время завершения	Длительность	Сервер	Порт сервера	Клиент	Порт клиента	Протокол/ Сервис	Транся. протокоя	Флаги ТСР	VLAN	Суммарное кол-во байт	Суммарное кол-во пакетов	Суммарный payload
Δ	07.07.2025 14:04:35.338	07.07.2025 14:04:35.338	0:00:00.0	ff02::1	10001	fe80::f692:bfff.fe8	51155	RX	UDP		-	2 710	10	2 090
Δ	07.07.2025 14:04:35.333	07.07.2025 14:04:35.333	0:00:00.0	ff02::1	10001	fe80::76ac:b9ff.fe5	42369	RX	UDP		-	3 794	14	2 926
Δ	07.07.2025 14:04:25.884	07.07.2025 14:04:34.638	0:00:08.753	fe80::4b30:6e2a:3	5353	ff02::fb	5353	MDNS	UDP		-	17 625	84	12 417
Δ	07.07.2025 14:04:25.318	07.07.2025 14:04:25.318	0:00:00.0	#02::1	10001	fe80::f692:bfff.fe8	32890	RX	UDP		-	3 794	14	2 926
Δ	07.07.2025 14:04:25.313	07.07.2025 14:04:25.313	0:00:00.0	#02::1	10001	fe80::76ac:b9ff.fe5	42123	RX	UDP		-	3 794	14	2 926
	07.07.2025 14:04:18.492	07.07.2025 14:04:18.492	0:00:00.0	fe80::14e1:d799:5	5353	ff02::fb	5353	MDNS	UDP		-	2 220	15	1 290
Δ	07.07.2025 14:04:18.492	07.07.2025 14:04:18.492	0:00:00.0	fe80::14e1:d799:5	5353	ff02::fb	5353	MDNS	UDP		100	152	1	86
Δ	07.07.2025 14:04:15.298	07.07.2025 14:04:15.298	0:00:00.0	1102::1	10001	fe80::f692:bfff.fe8	39443	RX	UDP		-	3 794	14	2 926
	07.07.2025 14:04:15.293	07.07.2025 14:04:15.293	0:00:00.0	1102::1	10001	fe80::76ac:b9ff.fe5	57286	RX	UDP		-	3 794	14	2 926
Δ	07.07.2025 14:04:05.460	07.07.2025 14:04:09.471	0:00:04.11	fe80::14e1:d799:5	5353	ff02::fb	5353	MDNS	UDP		-	6 360	46	3 508
Δ	07.07.2025 14:04:05.460	07.07.2025 14:04:09.471	0:00:04.11	fe80::14e1:d799:5	5353	ff02::fb	5353	MDNS	UDP		100	428	3	230
	07.07.2025 14:04:05.280	07.07.2025 14:04:05.280	0:00:00.0	ff02::1	10001	fe80::f692:bfff.fe8	58069	RX	UDP		-	3 794	14	2 926
ŝ	07.07.2025 14:04:05.273	07.07.2025 14:04:05.273	0:00:00.0	ff02::1	10001	fe80::76ac:b9ff.fe5	41265	RX	UDP		-	3 794	14	2 926

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

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:

Порт	Протокол	Общий трафик ↓ байт	Сессий	
ეკ	DIN2	102 896	210	
10051	FTP_DATA	44 920	29	
10051	UNKNOWN	36 112	122	
1194	OPENVPN	28 528	44	
443	UBUNTUONE	27 672	1	
123	NTP	25 920	72	
5678	UNKNOWN	13 050	30	
33066	AQOSTA	10 704	2	
3000	NTOP	9 000	30	

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

443	UBUNTUONE	27 672	1
12? Список сессий	NTP	25 920	72
График связей 567 -	UNKNOWN	13 050	30
33066	AQOSTA	10 704	2
3000	NTOP	9 000	30

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

-marala	Связи между серверами и внутренними хостами	E × <u>acon m</u>
	Ранжировать по трафику 🔹 Количество связей: 10 👻 Порт : 123, Протокол : NTP	Q Q 707 10-05-00
- 10:11:56 ((DNS и се		89.109.251.23 🕳
на 🛛 2	LANG-192.198.10.128	S0.100.251.21
	LANG-192.168.10.112	88.109.251.22
	LANO-122 168 10 146 LANO-122 168 10 14 LANO-122 168 10 173 LANO-122 168 10.175	185.125.190.58 💥
	LANG 192 188 10.154 Avidse_177 LANG 192 188 10.116	185.125.190.57 💥
	LANG-192 195 10 121	45.90.217.6
	LAND 192.168.10.101	91.139.91.157
	Proba (PL)	188 225 9 107
		_

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:

Топ хостов по проблемным пакетам Тип проблемы: Потерянных пакетов Хосты: Все	-	::	×
pod-000-1179-14.backblaze.com pod-000-1179-14.backblaze.com 149.137.139.84 6 752			
pod-000-1178-12.backblaze.com	192.168	.1.126	
pod-000-1181-05.backblaze.com			l
pod-000-1130-14.backblaze.com	192.16	38.1.18	ī
192,168.1.10	192.16	/8.1.21 38.1.69	
	192.16	18.1.70 38.1.96	

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 З. Смотрим результаты:

AB	ИСТАР	dashboard ^β						Просмо	отр сессий				17	2_72i Q 💄 Ms_R&j8 🔹	- 🔹 🌢 🕲 🕀 🖻
	Интеро	þейс (aqosta.DPI): 🌒 🛙	72_if0 1 Гбит												
 చి		<u> </u>	<u></u>	<u></u>	<u>^</u>	<u></u>			/****	James March	~^^~		mann halan		• • • • • • • • • • • • • • • • • • •
	13:05:00	07.07 13:10:00	07.07 13:15:00	07.07 13:20:	00 07.07	13:25:00	07.07 13:30:00		07.07 13:35:00	07	.07 13:40:00	07.0	7 13:45:00 07.07 13:50:	00 07.07 13:55:00	07.07 14:00:00
&	07 ию	ля 13:04:40 - 14:04:40 (1ч 0	0m 0c) @											CIR: F	X 60.0 M6/c TX 40.0 M6/c
*	Спи Все	сок IP сессий за выбр сессии —	ранный период ©			окол/Сер « Время к	Сервер руговой задерж	ки (RTT)	>= 100 мс	© :П	орт	8	- Клиент	@ :Порт	00 8
		Время начала	Время завершения	Длительность	Сервер	Порт сервера	Клиент	Порт клиента	Протокол/ Сервис	Трансп. протокол	Флаги ТСР	VLAN	Суммарное кол-во байт	Суммарное кол-во пакетов	Суммарный payload
		07.07.2025 14:04:38.215	07.07.2025 14:04:39.295	0:00:01.79	95.163.41.56	443	192.168.1.42	63640	HTTPS	TCP	SAP	-	22 448	190	11 564
-6		07.07.2025 14:04:37.167	07.07.2025 14:04:37.431	0:00:00.263	192.168.1.77	3389	192.168.1.9	54704	RDP	UDP		-	1 920	32	576
		07.07.2025 14:04:35.154	07.07.2025 14:04:36.556	0:00:01.402	17.188.182.8	3482	192.168.10.180	16403	UNKNOWN	UDP		-	6 419	67	3 605
		07.07.2025 14:04:28.346	07.07.2025 14:04:34.645	0:00:06.299	95.163.41.56	443	192.168.1.65	63470	HTTPS	TCP	SAPF	-	77 781	318	59 889
		07.07.2025 14:04:27.976	07.07.2025 14:04:34.669	0:00:06.692	95.163.41.56	443	192.168.1.65	63465	HTTPS	TCP	SAPF	-	35 949	199	24 483
		07.07.2025 14:04:27.686	07.07.2025 14:04:39.562	0:00:11.876	85.143.252.68	1194	192.168.1.16	49199	OPENVPN	UDP		-	388 090	952	348 106
		07.07.2025 14:04:26.706	07.07.2025 14:04:34.477	0:00:07.771	85.143.252.68	1194	192.168.10.180	54492	OPENVPN	UDP		-	18 414	94	14 466
		07.07.2025 14:04:26.705	07.07.2025 14:04:38.822	0:00:12.117	85.143.252.68	1194	192.168.10.180	49772	OPENVPN	UDP		-	48 224	236	38 312
		07.07.2025 14:04:26.703	07.07.2025 14:04:35.458	0:00:08.754	85.143.252.68	1194	192.168.1.126	58987	OPENVPN	UDP		-	26 288	79	22 970
		07.07.2025 14:04:26.86	07.07.2025 14:04:34.646	0:00:08.560	217.20.156.165	443	192.168.1.65	63460	HTTPS	TCP	SAPFR	-	42 624	253	28 242
		07.07.2025 14:04:25.879	07.07.2025 14:04:34.648	0:00:08.768	185.226.55.58	443	192.168.1.65	63459	HTTPS	TCP	SAPER	-	38 998	211	26 992
		07.07.2025 14:04:25.858	07.07.2025 14:04:34.646	0:00:08.788	185.226.53.36	443	192.168.1.65	63458	HTTPS	TCP	SAPFR	-	38 362	201	26 968
6		07.07.2025 14:04:25.833	07.07.2025 14:04:34.645	0:00:08.811	217.20.156.165	443	192.168.1.65	63454	HTTPS	TCP	SAPER	-	144 581	559	113 675
	-														
?	Запи	сей на странице: 50	✓ ≪ < 1 >	Bcero 3 2	89 записей (65 ст	границ)									Prod Version 0.1 Build 19

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)»:

Хосты по отклику (Все протоколы и сервисы) @									
motd.ubuntu.com			_						
 84.10.15.253 motd.ubuntu.com motd.ubuntu.com	тосс. из и полный 18,67 с								
Показать все данные									

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

~~~	M		and the second						
00	Мед	пенные сессии хоста 34	.254.182.186(motd.ubunt	u.com)					C × -
оля						= Протокол	/Сервис	Хост-пара	🥑 🔗 🛛 R:
		Время начала	Время завершения	Сервер	Клиент	Протокол	Отклик полный 🔻 с 🛛 👻	Отклик приложения, с	Задержка сети, с
вре		05.07.2025 01:03:16.838	05.07.2025 01:03:35.848	34.254.182.186:443	192.168.10.141:38754	UBUNTUONE	18,67	3,35	15,32
	目	05.07.2025 00:28:44.060	05.07.2025 00:29:09.464	34.254.182.186:443	192.168.10.108:33298	UBUNTUONE	7,3	0	7,3
					ПОСТРАДАВШИЕ КЛ	ИЕНТЫ"			
:12:02									
ован	Зап	исей на странице: 50 🔹	<u> </u>	Всего 2 записи (1 стр	раница)				
			Экспорт				3	акрыть	
						0.7-			

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

Анализ ТСР-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:

АВИСТА	AP dashboard ^B						Просм	отр сессий					i72_72i q 💄	Ms_R&j8 🔻	🌣 🌲 😌	<b>() (</b> )
Инте	ерфейс (aqosta.DPI): 🏾 🖬	72_if0 1 Гбит														
<mark>⊼</mark> ↔	La Antonio de la Constante de	<u>whater</u>	- <del></del>	<u>Mary Mary</u>		·····	<del>~~~</del>	^	<del>4,,</del> A	was M. M.	Maraa	<u>~~</u>	-M-room	<u> Handhar</u>	Lever worker,	+ 
× • •	07.07 10:10:00 07.07 10	10:15:00 07.	07 10:20:00	07.07 10:25:00	07.07 10	1:30:00 07.0	7 10:35:00	07.0	7 10:40:00	07.07 10	45:00	07.07 10:50:00	07.07 10:55:00	07.07 11:00:00	07.07 11:05	1:00
3 07 1	июля 10:07:56 - 11:07:56 (1ч 0	IM Oc) 🚱												CIR: R)	K 60.0 M6/c TX 40	0.0 M6/c
Сп	исок IP сессий за выбј	ранный период		Прот	окол/Сер	о Сервер				Порт		🛃 Клиент		• Порт		
	Время начала	Время заверше	Расширенный фі	ильтр			_						× нарное ко	п-во пакетов	Суммарный payload	
	07.07.2025 11:07:55.979 07.07.2025 11						&							3		
6 🔳	07.07.2025 11:07:55.949	07.07.2025 11	Название поля ТСР флаги											138		
. 8	07.07.2025 11:07:55.949	07.07.2025 11										] - [] 0			6	
	07.07.2025 11:07:55.909	07.07.2025 11		Отм	енить						Трименить				36	
	07.07.2025 11:07:55.804	07.07.2025 11													109 141	
	07.07.2025 11:07:55.607	07.07.2025 11:07:5	55.664 0:00:00.57	85.198.76.99	443	192.168.1.11	50635	HTTPS	TCP	SAP		85 181	122		78 317	
	07.07.2025 11:07:55.580	07.07.2025 11:07:5	55.580 0:00:00.0	94.100.180.59	443	192.168.1.126	57008	SSL	TCP	APFR	100	299	4		43	
	07.07.2025 11:07:55.577	07.07.2025 11:07:5	55.798 0:00:00.221	37.230.196.120	443	192.168.1.27	50489	HTTPS	TCP	SAP		139 348	455		114 058	
	07.07.2025 11:07:55.574	07.07.2025 11:07:5	55.582 0:00:00.7	94.100.180.59	443	192.168.1.126	57008	HTTPS	TCP	APFR	-	10 080	153		1 134	
	07.07.2025 11:07:55.446	07.07.2025 11:07:5	55.487 0:00:00.40	185.26.182.112	443	192.168.1.95	64152	HTTPS	TCP	A		3 000	50		300	
	07.07.2025 11:07:55.430	07.07.2025 11:07:5	55.430 0:00:00.0	178.18.215.7	80	185.218.86.12	1056	HTTP	TCP	SA	-	740	10		0	
	07.07.2025 11:07:55.430	07.07.2025 11:07:5	55.430 0:00:00.0	178.18.215.7	80	185.218.86.12	1056	HTTP	TCP	SA	50	78	1		0	
	07.07.2025 11:07:55.430	07.07.2025 11:07:5	55.443 0:00:00.13	192.168.1.146	22	192.168.1.143	57677	SSH	TCP	SAPFR	-	10 038	138		894	
-				100.000											-	
3ar	писеи на странице: 50	<u>▼</u> ≪ < 1	> BCELO	тоо доо записеи (	3 692 CT	заницы)									Prod Vers	ion 0.1 Build

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

АВИ	СТАР	dashboard ^β						Просмо	тр сессий				i72_	72i Q, 💄 Ms_R&j8 👻	🌣 🌲 😊	Ф Э	
	Интерф	ейс (aqosta.DPI): 🍨 i7	2_if0 1 Гбит														
يم ا	↔ <u>₩</u>	hannan d	whomen and	d	havvv									€			
<b>•</b>	🛓 ar ar 16 10.00 ar ar ar 16 25.00 ar ar ar 16 25.00 ar ar 16 25.00 ar																
æ	07 июл	R 10:07:56 - 11:07:56 (14 0)	M Oc) ©											CIR: R)	( 60.0 M6/c TX	40.0 M6/c	
	Список IP сессий за выбранный период Все сессии 🗸 💿				ГротоколіСер Сервер Ф:Порт В Сервер Клиент						Клиент	@ :Порт		•			
		Время начала	Время завершения	Длительность	Сервер	Порт сервера	Клиент	Порт клиента	Протокол/ Сервис	Трансп. протокол	Флаги ТСР	VLAN	Суммарное кол-во байт	Суммарное кол-во пакетов	Суммарный раую	ad	
		07.07.2025 10:55:12.1	07.07.2025 10:55:12.1	0:00:00.0	178.18.215.7	80	92.118.39.237	8875	HTTP	TCP	Р	-	3 585	15	2 775		
-6		07.07.2025 10:40:41.489	07.07.2025 10:40:41.489	0:00:00.0	178.18.215.7	80	92.118.39.237	21783	HTTP	TCP	Р	-	3 585	15	2 775		
		07.07.2025 10:26:16.506	07.07.2025 10:26:16.506	0:00:00.0	178.18.215.7	80	92.118.39.237	18626	HTTP	TCP	Р	-	616	7	238		
•		07.07.2025 10:14:52.979	07.07.2025 10:14:52.979	0:00:00.0	178.18.215.7	80	92.118.39.237	5722	HTTP	TCP	P	-	1 672	19	646		
() ()	Запис	ей на странице: <u>50</u>	<u>•</u> «< 1 >	Bcero 4 sar	иси (1 страница)										Prod V	ersion 0.1 Build 19	

# 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 «ТСР 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»:

≡	Коды откликов	HTTP			-	53	×
				Кол-во сессий			
			2**	25,00			
		Bcero :	4**	1,00			
		<b>26</b> 96.2%	2.click	Показать все данные			

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

	Коды отклика НТТР					🖸 🛛 🗙	07.0
25:36 (;			- Протокол/Сервис	Хост-пара	4** (Client Error) 👻		R: RX
	Сервер	Клиент	Код отклика	Метод	Протокол		
	178.18.232.193:80	192.168.10.180:38836	403 Forbidden	GET	HTTP		12
							3
							20
							)
10.6%							
							13
							5
іков Н							
	Записей на странице: 50 💌 « < 1	> Всего 1 запись (1 страница)					
	Экспорт			Закрыть			
	96.2%						



перейти на страницу aVistar/V по QR-коду



- © ООО «Метрологические системы»
- 🌐 www.mesys.ru
  - getmail@mesys.ru



rev. 2.18 (Q2'25)