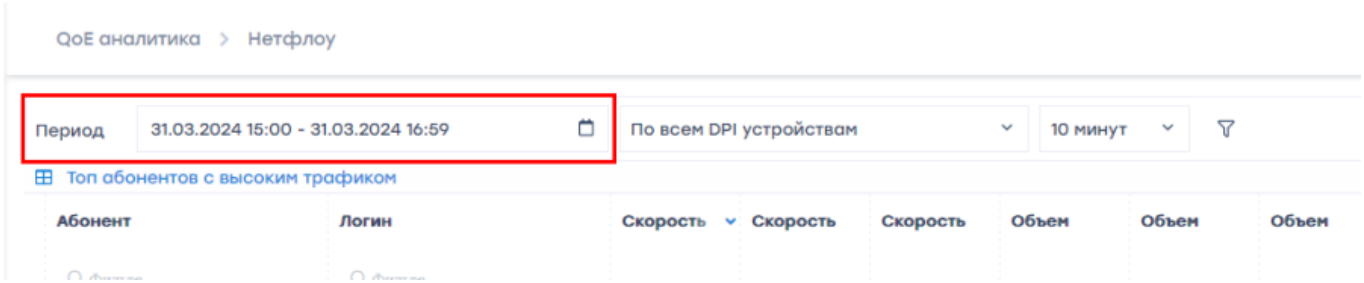
Содержание

Фильтры в отчетах QoE

Описание и сценарии применения

Фильтры в отчетах позволяют пользователю отфильтровать данные по определенным критериям. Это удобно для быстрого поиска нужной информации в больших объемах данных.

Фильтрация отчетов происходит в разделах QoE аналитики: Нетфлоу, Сырой полный нетфлоу, Кликстрим, Сырой кликстрим.
Перед применением фильтров к отчетам нужно сделать отбор данных по определенному временному интервалу с помощью поля “Период”:



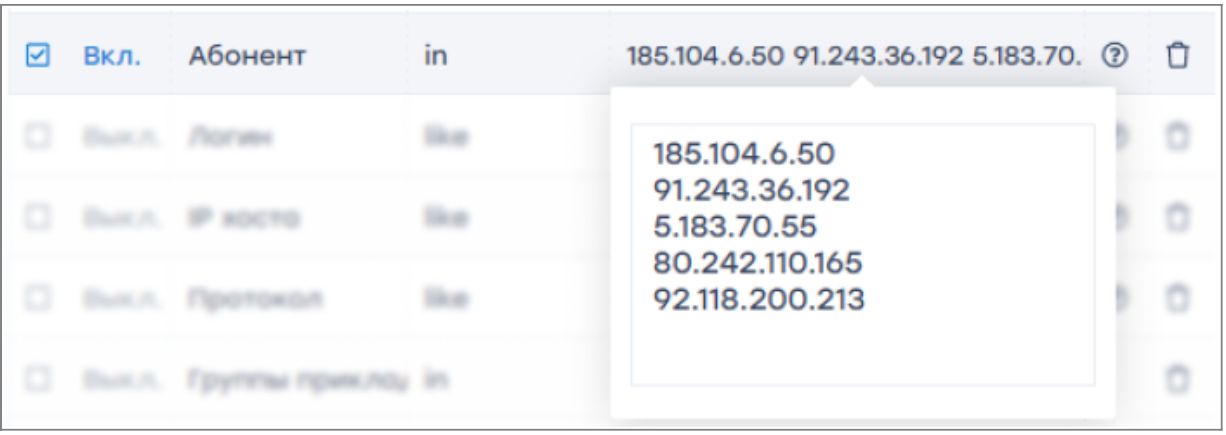
Есть два варианта выбора периода:

1. Пользовательский диапазон — произвольное Начало и Конец периода, задаются вручную;
2. Быстрые диапазоны — готовые интервалы даты и времени, выбираются из приведенного списка.

Сценарий 1. Фильтрация по абонентам

Применяется, если нужно отследить активность конкретного абонента, пула абонентов или списка абонентов.
1. Выбрать фильтр “Абонент”;
2. Настроить фильтр по одному из трех вариантов:

Один абонент	☑	Вкл.	Абонент	like	80.242.102.109	? 🗑
Пул абонентов	☑	Вкл.	Абонент	match	80\.242\.100\.	? 🗑

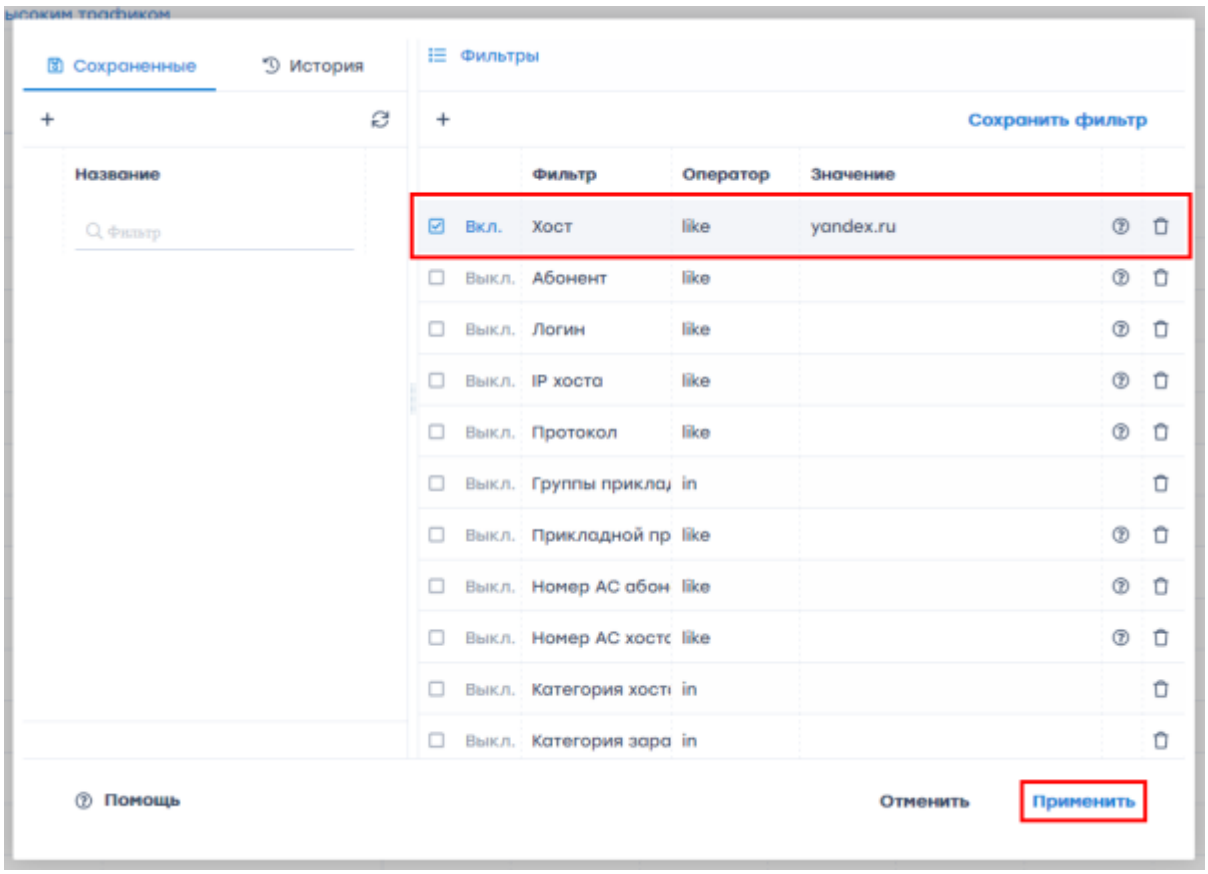
Список абонентов	

3. Включить фильтр, поставив галочку в чекбоксе слева от настраиваемого фильтра;
4. Нажать “Применить”.

Сценарий 2. Фильтрация по ресурсу

Применяется, если нужно найти абонентов, посещавших определенный ресурс или список ресурсов.

1. Выбрать фильтр “Хост”;
2. Выбрать оператор “=” или “like”;
3. Ввести название ресурса;
4. Включить фильтр, поставив галочку в чекбоксе слева от настраиваемого фильтра;
5. Нажать “Применить”.



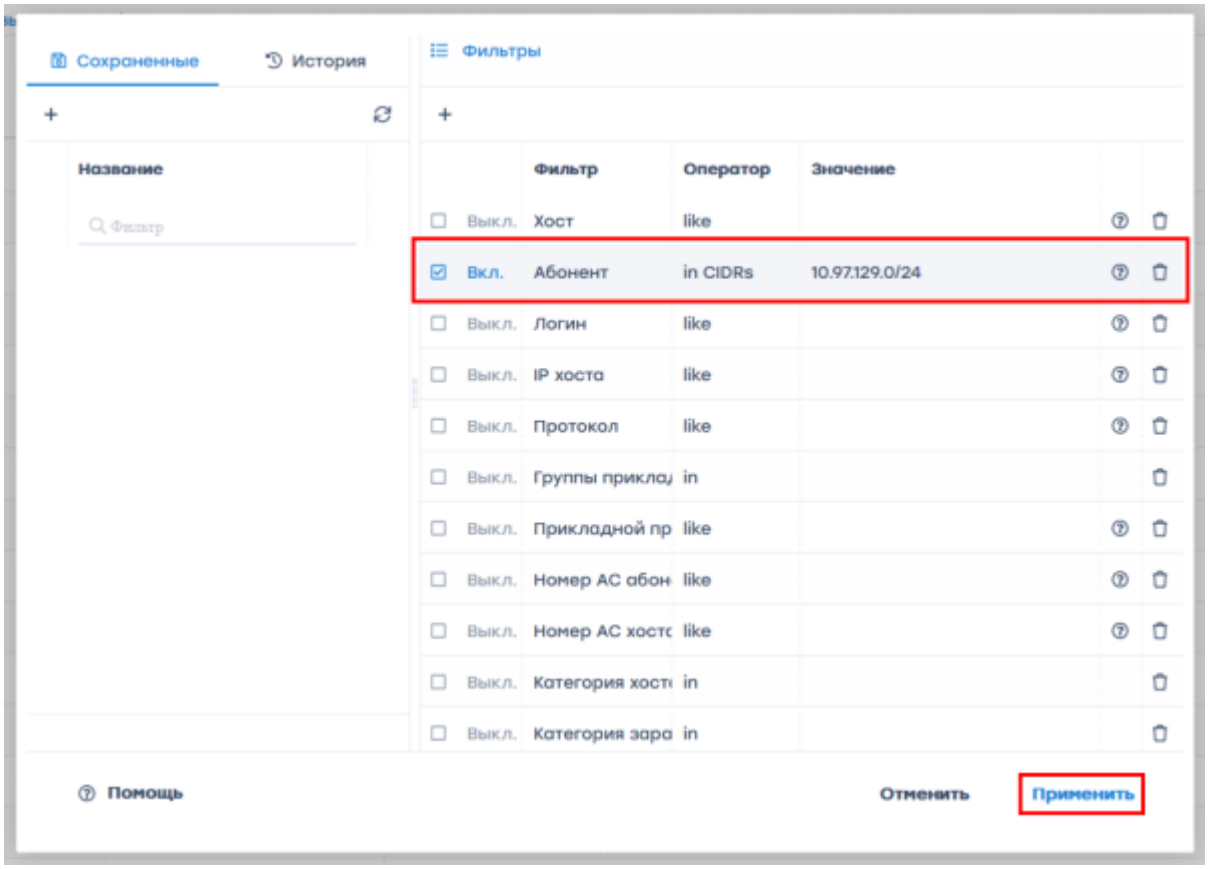
Для фильтрации по списку ресурсов следуйте принципу из Сценария 1. Фильтрация по

абонентам → Список абонентов.

Сценарий 3. Фильтрация по адресу CIDR

Применяется, если нужно отфильтровать данные по определенному IP-адресу с маской подсети.

1. Выбрать фильтр “Абонент”;
2. Выбрать оператор “in CIDR’s”;
3. Ввести IP-адрес с маской подсети;
4. Включить фильтр, поставив галочку в чекбоксе слева от настраиваемого фильтра;
5. Нажать “Применить”.



Списки фильтров, доступных в разделах QoE Аналитики

Нетфлоу

Поле	Пояснение	Часто используемые операторы
Хост	Наименование хоста. Примеры: zen.yandex.ru *.mail.ru 149.154.167.151:80	= like

Поле	Пояснение	Часто используемые операторы
Абонент	IP-адрес абонента	= like in CIDR’s not in CIDR’s
Логин	Числовое обозначение абонента в биллинге	= like
IP хоста	IP-адрес хоста	= like in CIDR’s not in CIDR’s
Протокол	Сетевой протокол Пример: TCP 6	= like
Группы прикладных протоколов	Выбор значения фильтра осуществляется из выпадающего списка с группами протоколов	in not in
Прикладной протокол	Пример: https 443	= like
Номер АС абонента	Номер АС, закрепленный за определенным абонентом. В каждом запросе к абоненту или от абонента — одинаковый номер АС	= like
Номер АС хоста	Номер АС, закрепленный за определенным хостом. В каждом запросе к хосту или от хоста — одинаковый номер АС	= like
Категория хоста	Выбор значения фильтра осуществляется из выпадающего списка с категориями	in not in
Категория зараженного трафика	Доступные категории: Ботнет хосты (Kaspersky) Вредоносные хосты (Kaspersky) Фишинговые хосты (Kaspersky)	in not in
Канал/Мост	Канал – номер vChannel Мост – номер моста, через который идет трафик В поле указывается Канал **или** Мост, значение присылает DPI. В зависимости от режима работы, он присылает либо Мост, либо Канал в который попал тот или иной IP	= like
IPv4-адрес источника после nat	IP-адрес, преобразованный NAT из приватного в публичный для связи с внешними устройствами и доступа в интернет	= like in CIDR’s not in CIDR’s
Порт источника после nat	Порт, преобразованный NAT из приватного в публичный для связи с внешними устройствами и доступа в интернет	= like

Поле	Пояснение	Часто используемые операторы
Класс	Классы трафика cs0 — cs7. Подробнее в разделе Распределение трафика по классам для тарифного плана 0 — cs0 1 — cs1 ... 7 — cs7	= like
DSCP	Расширенные значения классов трафика. Подробнее в разделе Разметка приоритета трафика в зависимости от протокола или направления	= like
Направление трафика	Возможные значения: От абонента К абоненту	= !=
MPLS метки	Метки, отвечающие за передачу пакетов данных в сети. Передается в формате base64. Пример: C7pB/w==	= like

Сырой полный нетфлоу

Поле	Описание	Часто используемые операторы
ИД сессии	Идентификатор сессии Пример: 101292583003281746	= like
IPv4-адрес источника	IPv4-адрес источника запроса. Если запрос **от** абонента — здесь будет указан адрес абонента, если наоборот — адрес хоста	= like in CIDR's not in CIDR's
IPv6-адрес источника	IPv6-адрес источника запроса. Если запрос **от** абонента — здесь будет указан адрес абонента, если наоборот — адрес хоста	= like
Порт источника	Порт источника запроса. Если запрос **от** абонента — здесь будет указан порт абонента, если наоборот — порт хоста	= like
Номер АС источника	Номер АС источника запроса. Если запрос **от** абонента — здесь будет указан АС абонента, если наоборот — АС хоста	= like
IPv4-адрес получателя	IPv4-адрес получателя запроса. Если запрос направлен **к** хосту — здесь будет указан адрес хоста, если наоборот — адрес абонента	= like in CIDR's not in CIDR's
IPv6-адрес получателя	IPv6-адрес получателя запроса. Если запрос направлен **к** хосту — здесь будет указан адрес хоста, если наоборот — адрес абонента	= like
Порт получателя	Порт получателя запроса. Если запрос направлен **к** хосту — здесь будет указан порт хоста, если наоборот — порт абонента	= like

Поле	Описание	Часто используемые операторы
Номер АС получателя	Номер АС получателя запроса. Если запрос направлен **к** хосту — здесь будет указан АС хоста, если наоборот — АС абонента	= like
Сетевой протокол	Пример: TCP 6	= like
Прикладной протокол	Пример: https 443	= like
Группы прикладных протоколов	Выбор значения фильтра осуществляется из выпадающего списка с группами протоколов	in not in
Логин	Числовое обозначение абонента в биллинге	= like
Абонент	IP-адрес абонента	= like in CIDR’s not in CIDR’s
Номер АС абонента	Номер АС, закрепленный за определенным абонентом. В каждом запросе к абоненту или от абонента — одинаковый номер АС	= like
Порт абонента	Порт, закрепленный за определенным абонентом. В каждом запросе к абоненту или от абонента — одинаковый порт	= like
Хост	Наименование хоста Примеры: zen.yandex.ru *.mail.ru 149.154.167.151:80	= like
Номер АС хоста	Номер АС, закрепленный за определенным хостом. В каждом запросе к хосту или от хоста — одинаковый номер АС	= like
Порт хоста	Порт, закрепленный за определенным хостом. В каждом запросе к хосту или от хоста — одинаковый порт	= like
IP хоста	IP-адрес хоста	= like in CIDR’s not in CIDR’s
Канал/Мост	Канал – номер vChannel Мост – номер моста, через который идет трафик В поле указывается Канал **или** Мост, значение присылает DPI. В зависимости от режима работы, он присылает либо Мост, либо Канал в который попал тот или иной IP	= like
IPv4-адрес источника после nat	IP-адрес, преобразованный NAT из приватного в публичный для связи с внешними устройствами и доступа в интернет	= like in CIDR’s not in CIDR’s

Поле	Описание	Часто используемые операторы
Порт источника после nat	Порт, преобразованный NAT из приватного в публичный для связи с внешними устройствами и доступа в интернет	= like
Направление трафика	Возможные значения: От абонента К абоненту	= !=
ИД VLAN	Идентификатор VLAN, через который вошел трафик. Задается числом, пример: 4038	= like
ИД Post VLAN	Идентификатор VLAN, через который вышел трафик. Задается числом, пример: 4031	= like
MPLS метки	Метки, отвечающие за передачу пакетов данных в сети. Передается в формате base64. Пример: C7pB/w==	= like
Класс	Классы трафика cs0 — cs7. Подробнее в разделе Распределение трафика по классам для тарифного плана 0 — cs0 1 — cs1 … 7 — cs7	= like
DSCP	Расширенные значения классов трафика. Подробнее в разделе Разметка приоритета трафика в зависимости от протокола или направления	= like
Дельта октетов	Разница трафика (байт) в начале и в конце заданного периода	= like
Дельта пакетов	Разница IP-пакетов в начале и в конце заданного периода	= like

Кликстрим

Поле	Пояснение	Часто используемые операторы
Хост	Наименование хоста Примеры: zen.yandex.ru *.mail.ru 149.154.167.151:80	= like
Абонент	IP-адрес абонента	= like in CIDR’s not in CIDR’s
Логин	Числовое обозначение абонента в биллинге	= like
Устройство	Позволяет понять, с какого устройства сделан запрос	= like

Поле	Пояснение	Часто используемые операторы
IP хоста	IP-адрес хоста	= like in CIDR’s not in CIDR’s
Урл	Домен + адрес, по которому перешел абонент	= like
Категория хоста	Выбор значения фильтра осуществляется из выпадающего списка с категориями	in not in
Категория зараженного трафика	Доступные категории: Ботнет хосты (Kaspersky) Вредоносные хосты (Kaspersky) Фишинговые хосты (Kaspersky)	in not in
Канал/Мост	Канал – номер vChannel Мост – номер моста, через который идет трафик В поле указывается Канал **или** Мост, значение присылает DPI. В зависимости от режима работы, он присылает либо Мост, либо Канал в который попал тот или иной IP	= like
Заблокирован	Возможные значения: 0 — **не**заблокированный трафик 1 — заблокированный трафик	= !=
Направление трафика	Возможные значения: От абонента К абоненту	= !=

Сырой кликстрим

Поле	Пояснение	Часто используемые операторы
ИД сессии	Идентификатор сессии Пример: 101292583003281746	= like
IPv4-адрес источника	IPv4-адрес источника запроса. Если запрос **от** абонента — здесь будет указан адрес абонента, если наоборот — адрес хоста	= like in CIDR’s not in CIDR’s
IPv4-адрес получателя	IPv4-адрес получателя запроса. Если запрос направлен **к** хосту — здесь будет указан адрес хоста, если наоборот — адрес абонента	= like in CIDR’s not in CIDR’s
IPv6-адрес источника	IPv6-адрес источника запроса. Если запрос **от** абонента — здесь будет указан адрес абонента, если наоборот — адрес хоста	= like
IPv6-адрес получателя	IPv6-адрес получателя запроса. Если запрос направлен **к** хосту — здесь будет указан адрес хоста, если наоборот — адрес абонента	= like
Логин	Числовое обозначение абонента в биллинге	= like

Поле	Пояснение	Часто используемые операторы
Хост	Наименование хоста Примеры: zen.yandex.ru *.mail.ru 149.154.167.151:80	= like
Путь	Адрес, по которому перешел абонент	= like
УРЛ источника запроса	Ресурс, с которого поступил запрос. Используется при переадресации: запоминается адрес, с которого пользователь перешел на страницу переадресации	= like
Агент пользователя	User agent. Позволяет понять, с какого устройства сделан запрос	= like
Канал/Мост	Канал – номер vChannel Мост – номер моста, через который идет трафик В поле указывается Канал **или** Мост, значение присылает DPI. В зависимости от режима работы, он присылает либо Мост, либо Канал в который попал тот или иной IP	= like
Заблокирован	Возможные значения: 0 — **не**заблокированный трафик 1 — заблокированный трафик	= !=
Направление трафика	Возможные значения: От абонента К абоненту	= !=

Операторы

Оператор	Описание	Формат ввода данных
=	Возвращает записи, равные введенному значению	
!=	Возвращает записи, не равные введенному значению	
like	Возвращает записи, содержащие определённый шаблон символов	
ilike	Работает так же, как like, но не зависит от регистра	
not like	Возвращает записи, **не** содержащие определённый шаблон символов	
not ilike	Работает так же, как not like, но не зависит от регистра	
match	Возвращает записи, соответствующие регулярному выражению – последовательности специальных символов, формирующих паттерн или шаблон, который сопоставляется со строкой	Формат ввода и примеры см. по ссылке
not match	Возвращает записи, **не** соответствующие регулярному выражению	Формат ввода и примеры см. по ссылке
>	Возвращает записи, которые больше введенного значения	
>=	Возвращает записи, которые больше или равны введенному значению	

Оператор	Описание	Формат ввода данных
<	Возвращает записи, которые меньше введенного значения	
⇐	Возвращает записи, которые меньше или равны введенному значению	
in	Позволяет вводить несколько значений и возвращает все, что совпали со значениями из списка. Каждое значение нужно вводить с новой строки	Каждое значение с новой строки
not in	Позволяет вводить несколько значений и возвращает все, **кроме** тех, что совпали со значениями из списка. Каждое значение нужно вводить с новой строки	Каждое значение с новой строки
between	Возвращает записи, где выражение находится в диапазоне значений value1 и value2 включительно	Каждое значение с новой строки
not between	Возвращает все записи, где выражение **не** находится в диапазоне между value1 и value2 включительно	Каждое значение с новой строки
in CIDRs	Позволяет вводить несколько значений CIDR и возвращает все, что совпали со значениями из списка. Каждое значение нужно вводить с новой строки	192.0.2.32/27 Каждое значение с новой строки
not in CIDRs	Позволяет вводить несколько значений CIDR и возвращает все, **кроме** тех, что совпали со значениями из списка. Каждое значение нужно вводить с новой строки	192.0.2.32/27 Каждое значение с новой строки

Фильтрами осуществляется проверка строки на соответствие простому регулярному выражению. Регулярное выражение может содержать метасимволы:

- % обозначает любое количество любых символов (в т.ч. нулевое количество символов).
- _ обозначает один любой символ.

Пример использования регулярного выражения приведен в Сценарии 1. Фильтрация по абонентам → Пул абонентов.