

Table of Contents

- 19 Законный перехват 3
 - Разбор трафика* 3
 - Оборудование 3
 - Раздел 3
 - Логи разбора трафика 14

19 Законный перехват

Разбор трафика

Оборудование

Для настройки корректной работы раздела Разбора трафика необходимо добавить оборудование типа "Сервер разбора Pсар" в [раздел Управления списка оборудования](#).

Конфигурация оборудования для разбора трафика:

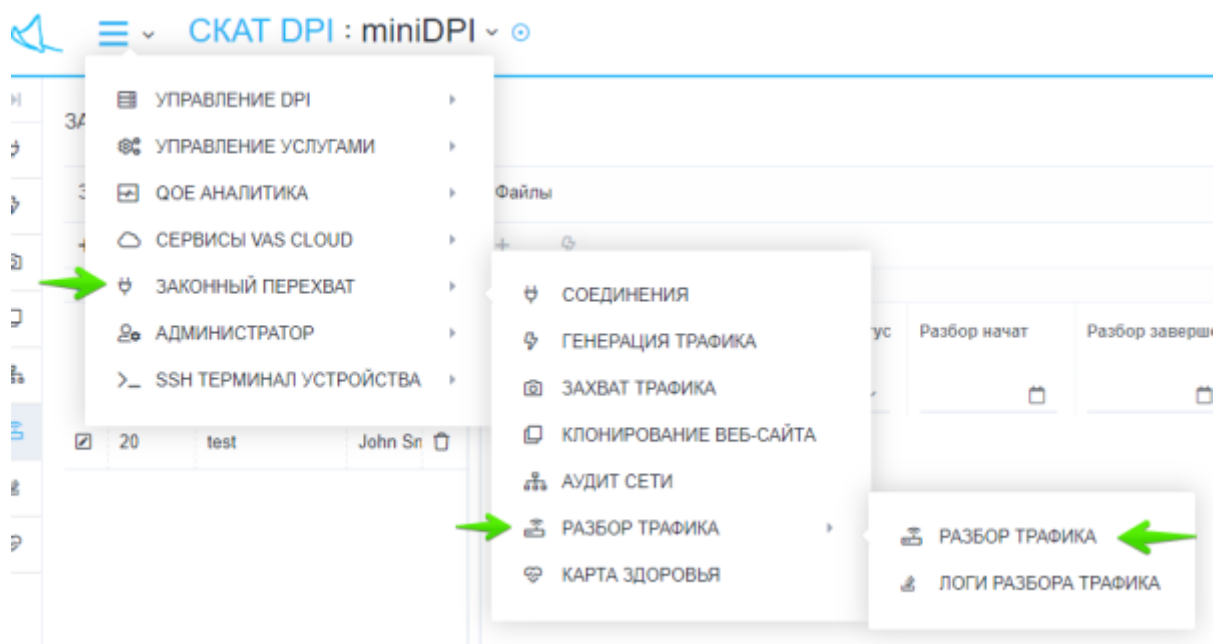
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

Для установки необходимых для работы утилит необходимо выполнить следующую команду:

```
apt install wireshark tshark sox
```

Раздел

Для перехода в раздел разбора траффика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Разбора трафика".



Раздел Разбора трафика выглядит как на рисунке ниже.

Обновить список задач

Добавить файл в задачу

Перезапустить разбор трафика для файла

Обновить список файлов

Обновить результаты разбора

Добавление задачи

Редактировать задачу

Удалить задачу

Редактировать файл

Скачать файл

Удалить файл

Задачи

Задачи для Разбора трафика находятся в левой части страницы Разбора трафика.

Создание задачи

Для создания новой задачи Разбора трафика нажмите на кнопку "+" в тулбаре над списком существующих задач.

Добавить задачу

Форма создания задачи

Разбор трафика

Название

Описание

Отменить

Сохранить

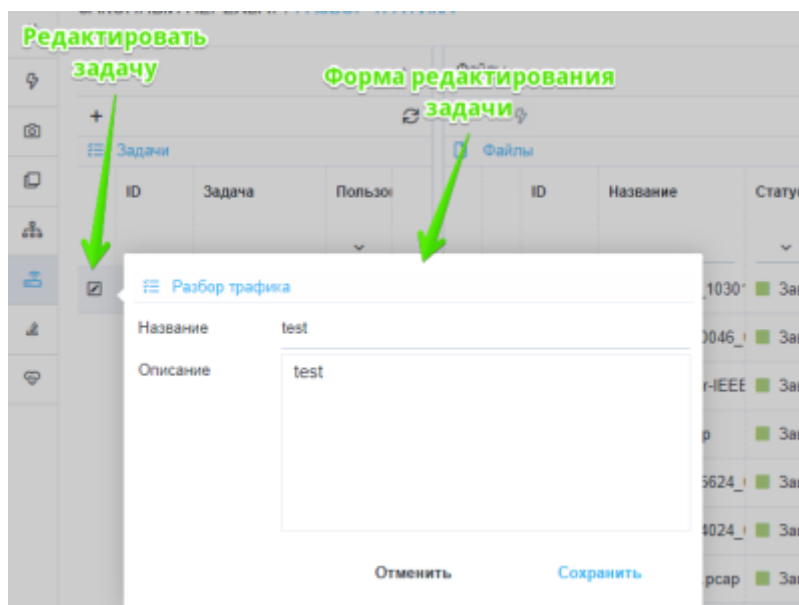
В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.



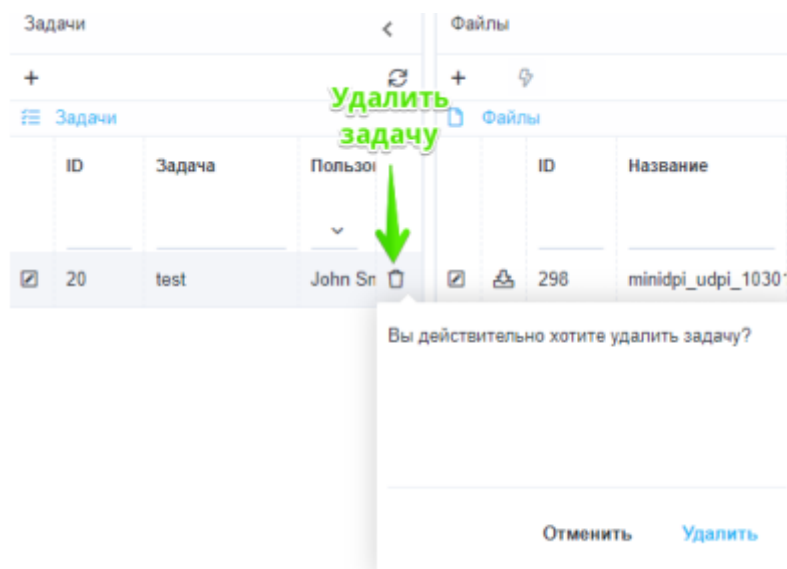
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

Для удаления задачи нажмите на кнопку "Удалить" напротив существующей задачи и подтвердите либо отмените действие.

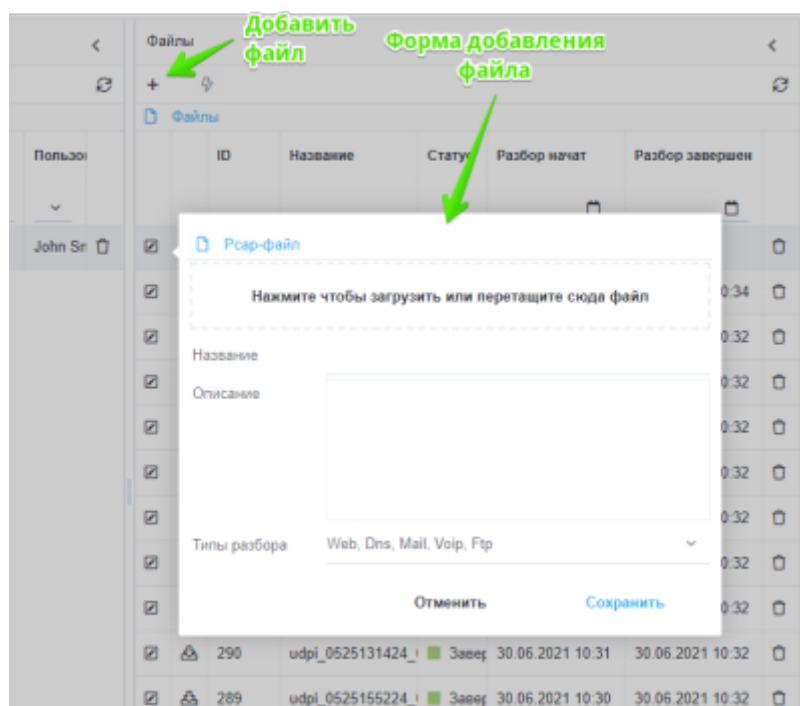


Файлы

Файлы для Разбора трафика находятся в центральной части страницы Разбора трафика.

Добавление файла

Для добавления нового файла для Разбора трафика нажмите на кнопку "+" в тулбаре над списком добавленных файлов.



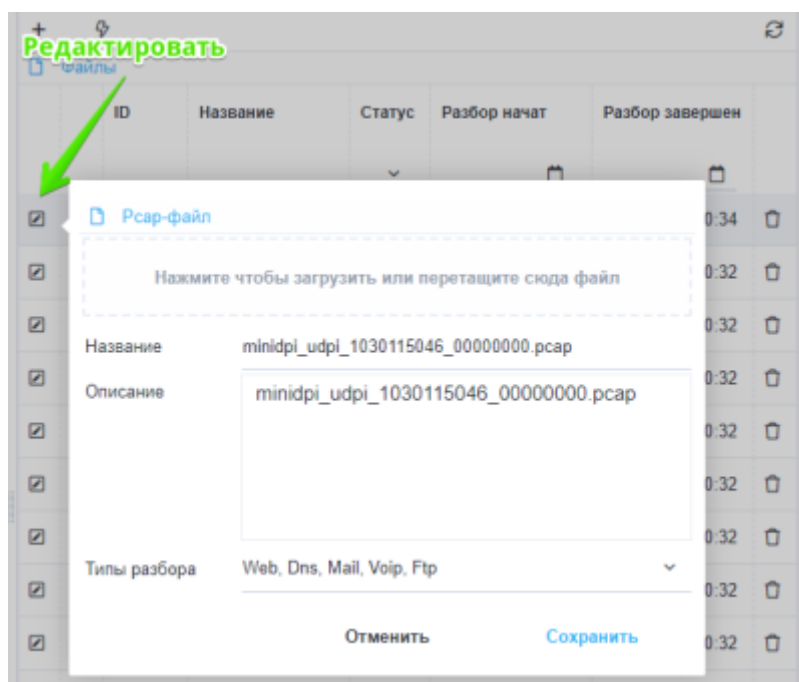
В открывшейся форме добавления файла:

- Загрузите или перетащите рсар-файл;
- При необходимости задайте отображаемое название и описание для файла;
- Укажите необходимые типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

Нажмите кнопку "Сохранить".

Редактирование файла

Для редактирования файла для Разбора трафика нажмите на кнопку редактирования напротив существующего файла.



В открывшейся форме редактирования файла можно изменить:

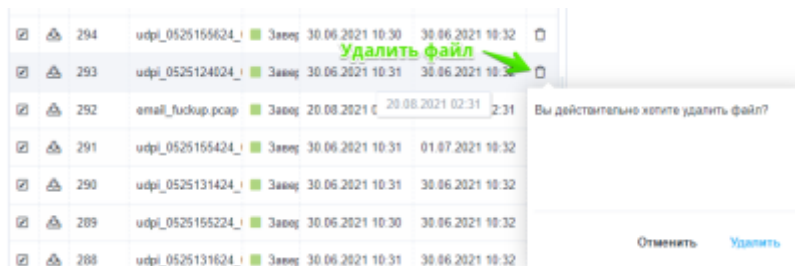
- Отображаемое название файла;
- Описание файла;
- Типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

Нажмите кнопку "Сохранить".

В случае, если были внесены изменения в типы разбора трафика - на экране появится форма подтверждения перезапуска разбора трафика для этого файла.

Удаление файла

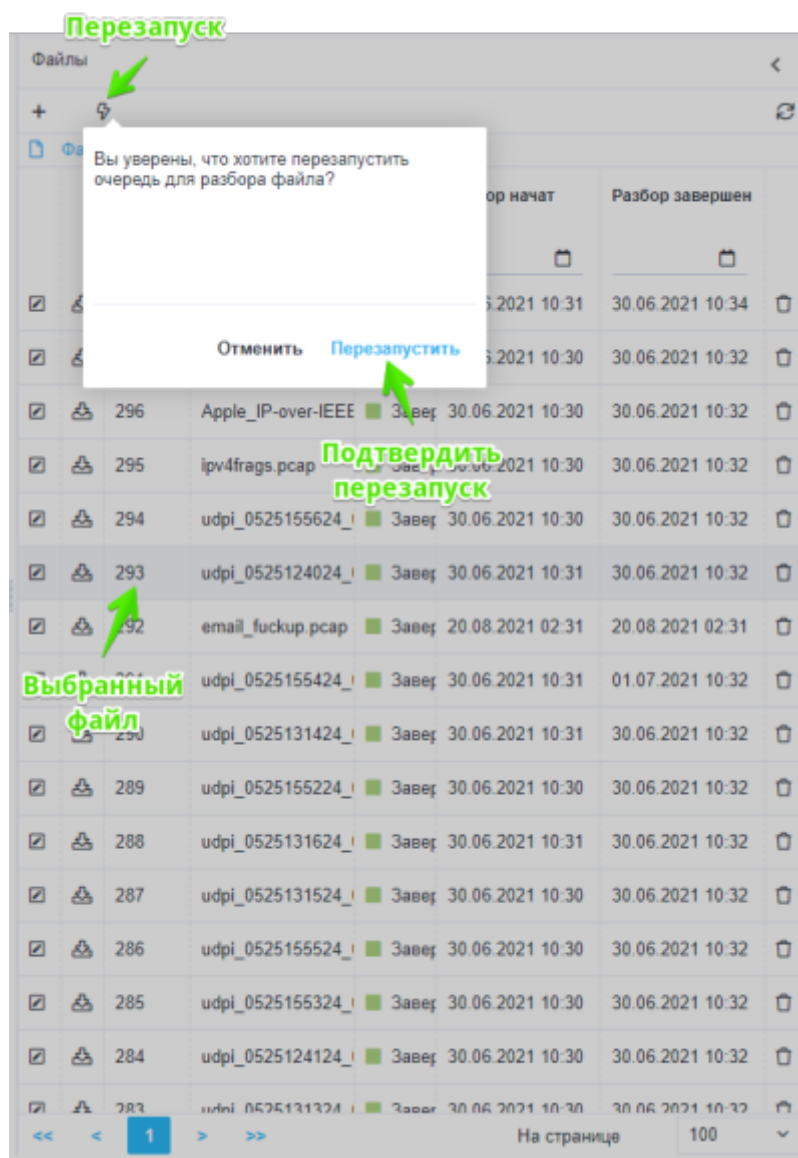
Для удаления файла нажмите на кнопку "Удалить" напротив существующего файла и подтвердите либо отмените действие.



Перезапуск разбора файла

Для перезапуска разбора файла:

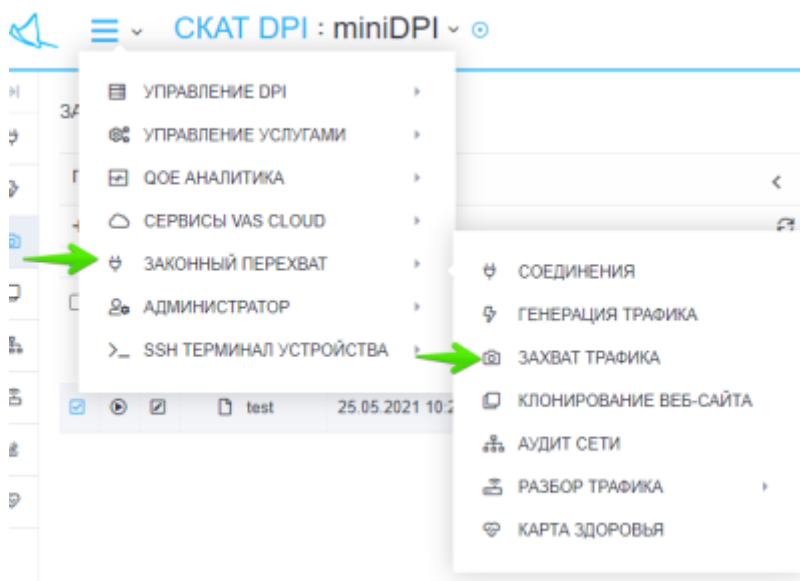
1. Выберите необходимый файл из списка;
2. Нажмите на кнопку перезапуска разбора в тулбаре;
3. Подтвердите либо отмените действие.



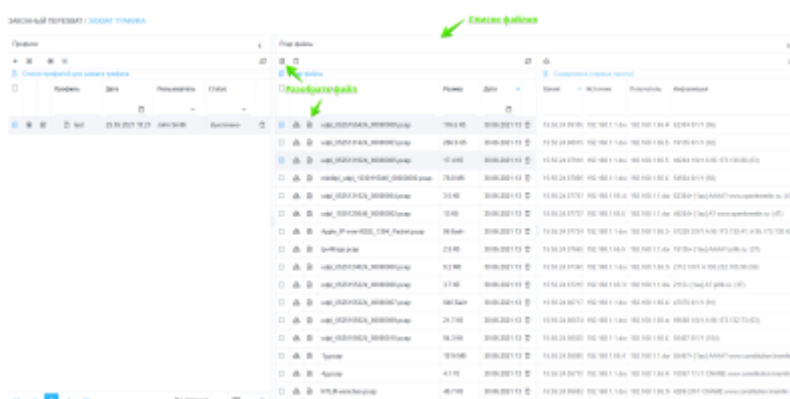
Импорт файлов из раздела захвата трафика

Файлы для разбора трафика можно импортировать из раздела "Захват трафика".

Перейдите в раздел "Законный перехват"→"Захват трафика".



В списке файлов выберите файлы, которые необходимо разобрать и нажмите кнопку разбора.



В открывшейся форме:

- Выберите задачу Разбора трафика, в которую будут импортированы файлы.
- В случае выбора "Новой задачи" - введите имя задачи, которая будет создана при импорте.
- Типы разбора для импортируемых файлов (Web,Dns,Mail,Voip,Ftp).

- Адрес запроса
- Размер ответа в байтах
- Метод

Результаты

Web (49) Dns (55) Mail (1) Voip (0) Ftp (35)

Декодированные веб-элементы

Запросы Изображения

Дата	Урл	Размер	Метод	
30.10.2020 08:54:00	ocsp.pki.goog/gts1o1core	472	GET	?
30.10.2020 08:53:00	ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?bf757d	0	GET	?
30.10.2020 08:53:00	ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?261fc1	0	GET	?
30.10.2020 08:52:00	ocsp.digicert.com/	279	GET	?
30.10.2020 08:51:00	en.kremlin.ru/events/president/news	0	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/photo.svg	280	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/video.svg	347	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/big_text.svg	210	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/small_text.svg	225	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/medium_text.svg	224	GET	?
30.10.2020 08:51:00	en.kremlin.ru/events/president/news/calendar/2020	0:31	GET	?
30.10.2020 08:51:00	en.kremlin.ru/structure/president/standart	0	GET	?
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/Ty6y5wbIsAqJR47S3O9Rju5bxiEBuKA	388035	GET	?
30.10.2020 08:51:00	static.kremlin.ru/media/events/presidents/medium/y9GgT364rwY.jpg	55126	GET	?

На странице 100

При нажатии на кнопку "Дополнительная информация о запросе"(?) откроется попап с дополнительной информацией о запросе:

- Агент
- Хост
- Урл
- Тип содержимого
- Кодировка
- Метод запроса
- Код ответа
- Размер ответа в байтах
- Порт отправителя
- Порт получателя
- Время ТСР
- Протокол IP
- Версия IP

- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Идентификатор файла для разбора
- Имя файла для разбора
- Имя файла с содержимым ответа

Результаты

Web (49)

Декодированные веб-элементы

Запросы

Дата

Ури

30.10.2020 08:54:00	oscar.kremlin.ru
30.10.2020 08:53:00	static.kremlin.ru
30.10.2020 08:53:00	static.kremlin.ru
30.10.2020 08:52:00	oscar.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	an.kremlin.ru
30.10.2020 08:51:00	static.kremlin.ru
30.10.2020 08:51:00	static.kremlin.ru

Http info

Платформы

Время Тср

80

15.486977

Ip

Протокол Ip

Версия Ip

Ip отправителя

Ip получателя

6

4

192.168.88.13

95.173.136.70

Eth

Тип Eth

Eth отправителя

Eth получателя

0x00000000

68:1d:af:14:1d:d2

4c:5e:0c:f3:48:50

Файл

Имя файла

Имя файла

Файл ответа

290

minidpi_udp_1030115046_00000000.pcap

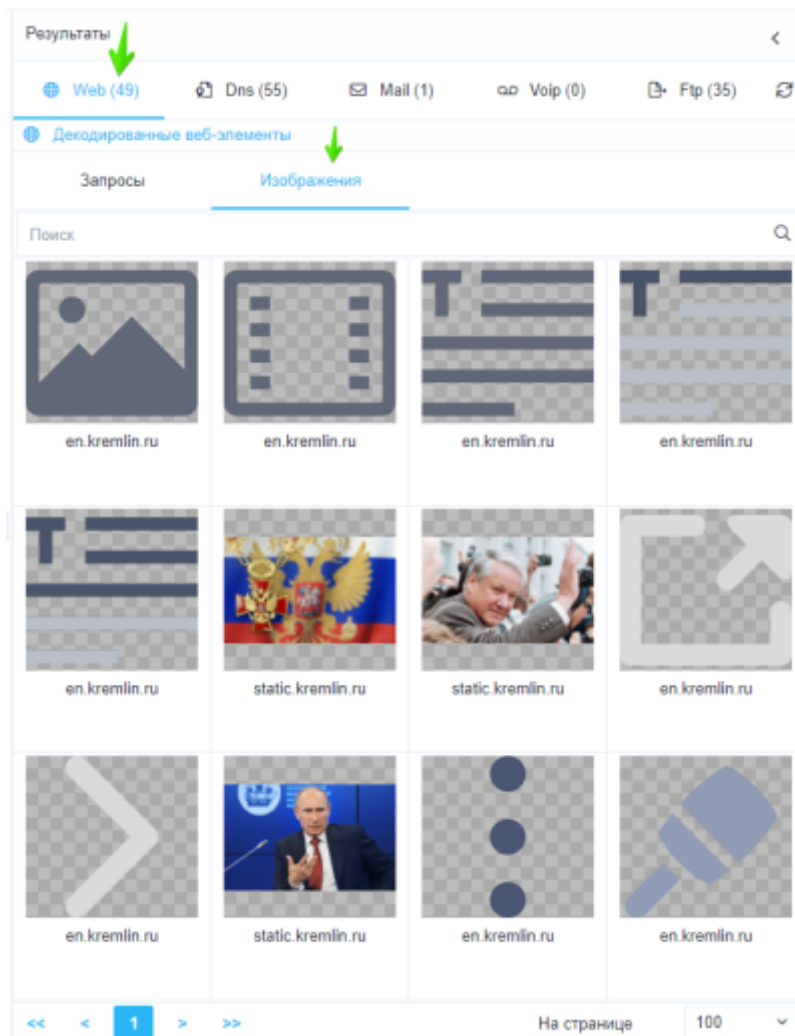
2020

Закрыть

На странице

100

Во вкладке "Изображения" отображаются запросы, в в ответ на которые возвращались изображения.



DNS

В разработке.

Mail

В разработке.

Voip

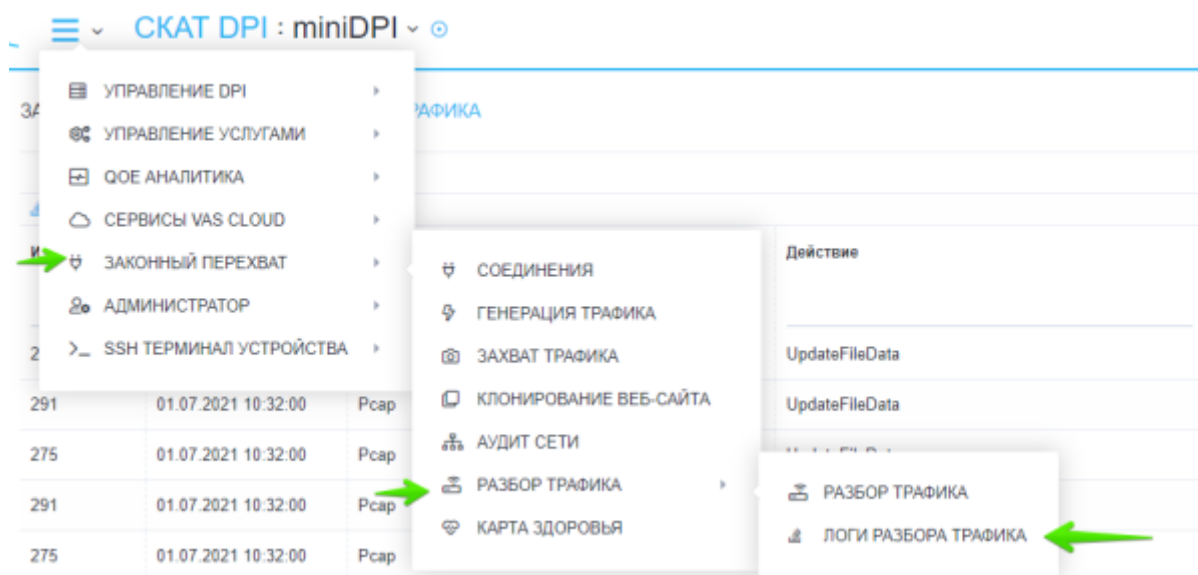
В разработке.

Ftp

В разработке.

Логи разбора трафика

Для перехода в раздел логов разбора трафика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Логи разбора трафика".



Раздел Логов разбора трафика выглядит как на рисунке ниже.

