

Table of Contents

- 19 Законный перехват 3
 - Разбор трафика* 3
 - Оборудование 3
 - Раздел 3
 - Логи разбора трафика 4

19 Законный перехват

Разбор трафика

Оборудование

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

Конфигурация оборудования для разбора трафика:

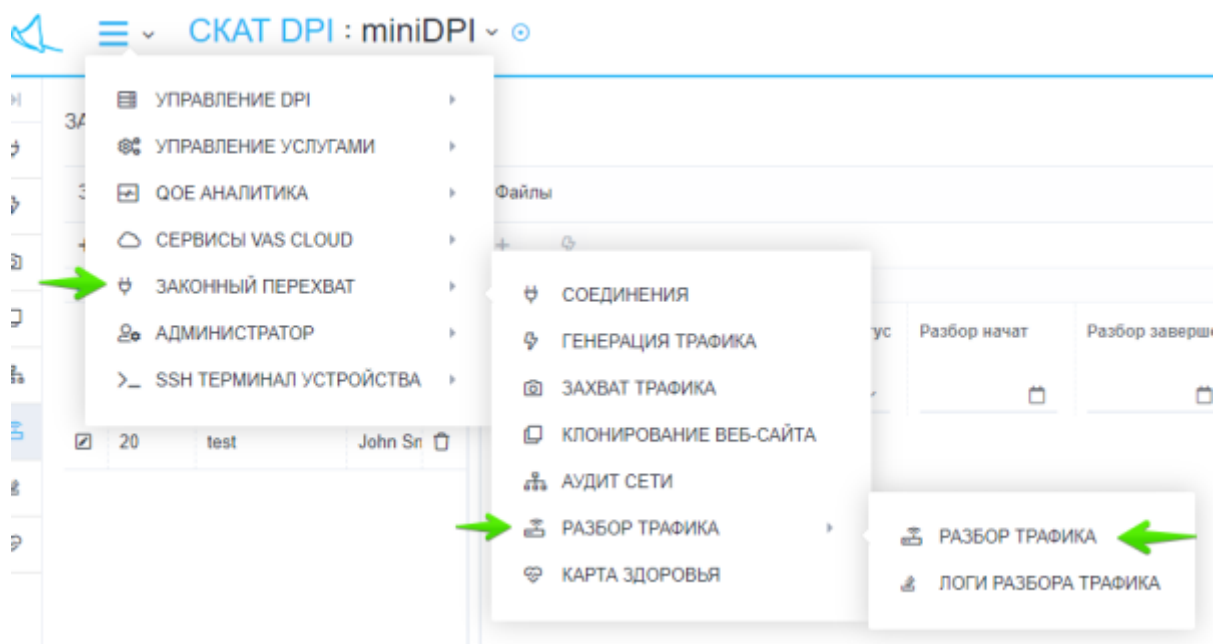
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

Для установки необходимых для работы утилит необходимо выполнить следующую команду:

```
apt install wireshark tshark sox
```

Раздел

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



Раздел Разбора трафика выглядит как на рисунке ниже.

СКAT DPI : miniDPI

Обновить список задач

Добавить файл в задачу

Перезапустить разбор трафика для файла

Обновить результаты разбора

Добавление задачи

Редактировать задачу

Удалить задачу

Редактировать файл

Скачать файл

Удалить файл

ID	Имя	Пользователь	ID	Имя	Статус	Разбор начал	Разбор завершил
20	test	John Se	290	miniDPI_udp_1030	Заверш	30.06.2021 10:31	30.06.2021 10:34
291	udp_1030120048_		297	udp_1030120048_	Заверш	30.06.2021 10:30	30.06.2021 10:32
295	Apple_IP-over-IEEE		296	Apple_IP-over-IEEE	Заверш	30.06.2021 10:30	30.06.2021 10:32
295	ip4Image.pcap		295	ip4Image.pcap	Заверш	30.06.2021 10:30	30.06.2021 10:32
294	udp_0525155624_		294	udp_0525155624_	Заверш	30.06.2021 10:30	30.06.2021 10:32
293	udp_0525124024_		293	udp_0525124024_	Заверш	30.06.2021 10:31	30.06.2021 10:32
292	email_fuckup.pcap		292	email_fuckup.pcap	Заверш	30.06.2021 10:30	30.06.2021 10:32
291	udp_0525155424_		291	udp_0525155424_	Заверш	30.06.2021 10:31	01.07.2021 10:32
290	udp_0525131424_		290	udp_0525131424_	Заверш	30.06.2021 10:31	30.06.2021 10:32
289	udp_0525155224_		289	udp_0525155224_	Заверш	30.06.2021 10:30	30.06.2021 10:32
288	udp_0525131624_		288	udp_0525131624_	Заверш	30.06.2021 10:31	30.06.2021 10:32
287	udp_0525131524_		287	udp_0525131524_	Заверш	30.06.2021 10:30	30.06.2021 10:32
286	udp_0525155524_		286	udp_0525155524_	Заверш	30.06.2021 10:30	30.06.2021 10:32
285	udp_0525155324_		285	udp_0525155324_	Заверш	30.06.2021 10:30	30.06.2021 10:32
284	udp_0525124124_		284	udp_0525124124_	Заверш	30.06.2021 10:30	30.06.2021 10:32
293	udp_0525155124_		293	udp_0525155124_	Заверш	30.06.2021 10:30	30.06.2021 10:32

На странице 100

Результаты

Web (45) Des (55) Mail (1) Voip (0) Ftp (35)

Детализированные веб-элементы

Дата	Ура	Размер	Метод
30.10.2020 08:54:00	ocsp.letsencrypt.org	472	GET
30.10.2020 08:53:00	cfst.windowsupdate.com/microsoftupdate/v3/staticcontent/en/default/download/cab794752d	0	GET
30.10.2020 08:53:00	cfst.windowsupdate.com/microsoftupdate/v3/staticcontent/en/default/download/cab72616c1	0	GET
30.10.2020 08:52:00	ocsp.digicert.com/	279	GET
30.10.2020 08:51:00	en.kremlin.ru/ventra/president/news	0	GET
30.10.2020 08:51:00	en.kremlin.ru/static/inspy/photos.asp	260	GET
30.10.2020 08:51:00	en.kremlin.ru/static/inspy/videos.asp	347	GET
30.10.2020 08:51:00	en.kremlin.ru/static/inspy/bin_test.asp	210	GET
30.10.2020 08:51:00	en.kremlin.ru/static/inspy/email_test.asp	225	GET
30.10.2020 08:51:00	en.kremlin.ru/static/inspy/medium_test.asp	224	GET
30.10.2020 08:51:00	en.kremlin.ru/ventra/president/news/calendar/2020	231	GET
30.10.2020 08:51:00	en.kremlin.ru/structure/president/standard	0	GET
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/TvGv5ubhAoJR4TS3O8Rk6wEBuKA	360035	GET
30.10.2020 08:51:00	static.kremlin.ru/media/events/president/medium/2GqT34mY.jpg	55126	GET

На странице 100

Задачи

Файлы

Результаты разбора

Логи разбора трафика

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

СКAT DPI : miniDPI

УПРАВЛЕНИЕ DPI

УПРАВЛЕНИЕ УСЛУГАМИ

QOE АНАЛИТИКА

СЕРВИСЫ VAS CLOUD

ЗАКОННЫЙ ПЕРЕХВАТ

АДМИНИСТРАТОР

SSH ТЕРМИНАЛ УСТРОЙСТВА

СОЕДИНЕНИЯ

ГЕНЕРАЦИЯ ТРАФИКА

ЗАХВАТ ТРАФИКА

КЛОНИРОВАНИЕ ВЕБ-САЙТА

АУДИТ СЕТИ

РАЗБОР ТРАФИКА

КАРТА ЗДОРОВЬЯ

Действие

UpdateFileData

UpdateFileData

РАЗБОР ТРАФИКА

ЛОГИ РАЗБОРА ТРАФИКА

Раздел Логов разбора трафика выглядит как на рисунке ниже.

СКАТ DPI : miniDPI

25 John Smith

RU

+2 28 0 5

ЗАКОННЫЙ ПЕРЕХВАТ / ЛОГИ РАЗБОРА ТРАФИКА

Обновить список задач

Удалить задачу

Создать задачу

ИД

Статус

Дата

Тип

Действие

Тип разбора

Статус

Описание

🔍

🗑️

275		01.07.2021 18:32:00	Риср	UpdateFileData	Рпр	Успешно		🔍 🗑️
291		01.07.2021 18:32:00	Риср	UpdateFileData	Рпр	Успешно		🔍 🗑️
276		01.07.2021 18:32:00	Риср	UpdateFileData	Успр	Успешно		🔍 🗑️
391		01.07.2021 18:32:00	Риср	ParseDecodedData	Рпр	Успешно		🔍 🗑️
275		01.07.2021 18:32:00	Риср	UpdateFileData	Мал	Успешно		🔍 🗑️
275		01.07.2021 18:34:00	Риср	UpdateFileData	Омс	Успешно		🔍 🗑️
275		01.07.2021 18:34:00	Риср	UpdateFileData	Видс	Успешно		🔍 🗑️
275		01.07.2021 18:35:00	Риср	ParseDecodedData	Рпр	Успешно		🔍 🗑️
275		01.07.2021 18:35:00	Риср	ParseDecodedData	Успр	Успешно		🔍 🗑️
275		01.07.2021 18:35:00	Риср	ParseDecodedData	Мал	Успешно		🔍 🗑️
275		01.07.2021 18:35:00	Риср	ParseDecodedData	Омс	Успешно		🔍 🗑️
276		01.07.2021 18:35:00	Риср	ParseDecodedData	Видс	Успешно		🔍 🗑️
276		01.07.2021 18:35:00	Риср	DecodeAction	Рпр	Успешно		🔍 🗑️
275		01.07.2021 18:35:00	Риср	DecodeAction	Успр	Успешно		🔍 🗑️
275		01.07.2021 18:36:00	Риср	DecodeAction	Мал	Успешно		🔍 🗑️
275		01.07.2021 18:36:00	Риср	DecodeAction	Омс	Успешно		🔍 🗑️
276		01.07.2021 18:36:00	Риср	DecodeAction	Видс	Успешно		🔍 🗑️

1

2

3

4

5

...

Постраничный переход

Количество записей на странице

100