ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Network Traffic Analysis»

Руководство администратора

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Определение**
АС	Автоматизированная Система
Заказчик	Зарегистрированный пользователь в системе заказчика передавший третьим лицам все необходимы данные и реквизиты для управления приложением или выполняющий указания третьих лиц за вознаграждение.
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО БУДУЩЕЕ; • Компанией-интегратором, по выбору Заказчика
ЛВС	Локальная вычислительная сеть
ОС	Операционная Система
ПО	Программное обеспечение F6 Network Traffic Analysis, NTA.
ТС	(«Технический Сервис») Система взаимодействия Заказчика, позволяющая обмениваться сообщениями и создавать цепочки обращений, которая представляет из себя отдельный раздел «Службу Поддержки» в панели управления «F6 Network Traffic Analysis». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
CEF	Common Event Format
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
JSON	JavaScript Object Notation
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol

Kerberos	Система аутентификации
LAN	Local Area Network
MDP	F6 Malware Detonation Platform
MXDR	Программный комплекс Managed Extended Detection and Response (Managed XDR)
MXDR Console	F6 XDR, MXDR
NTLM	NT LAN Manager
RDP	Remote Desktop Protocol
SMB	Server Message Block
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TI	Threat intelligence
UDP	User Datagram Protocol
URI	Uniform Resource Identifier

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает процесс установки экземпляра программного обеспечения «F6 Network Traffic Analysis» (далее – ПО, Network Traffic Analysis, NTA).

В случае возникновения проблем с разворачиванием ПО необходимо обратиться в техническую поддержку

1.2 Назначение ПО

«F6 Network Traffic Analysis» — это программное обеспечение для обнаружения и реагирования на сетевые угрозы (Network Detection and Response), предназначенное для мониторинга, анализа и предотвращения кибератак в режиме реального времени. ПО предоставляет комплексный мониторинг сетевого трафика, анализируя его для выявления подозрительных действий и угроз. Используя передовые методы, такие как поведенческий анализ, машинное обучение и сигнатурный анализ, ПО может обнаруживать сложные атаки, в том числе сетевые атаки, использование вредоносного ПО, фишинговые атаки и эксплуатацию уязвимостей. Благодаря интеграции с другими продуктами АО «БУДУЩЕЕ», такими как «F6 Threat Intelligence», ПО повышает точность обнаружения угроз и позволяет более эффективно управлять инцидентами безопасности.

ПО также поддерживает функции охоты на угрозы (Threat Hunting) и проведения форензики, что позволяет специалистам детально анализировать инциденты и выявлять их причины и последствия.

Выявление вредоносной активности, аномалий и скрытых каналов в сетевом трафике осуществляется в несколько шагов:

1. Сетевой трафик проходит через модуль сигнатурного анализа.
2. Трафик сети анализируется с помощью ML-классификаторов.
3. Сетевые сигналы (алерты) автоматически соотносятся с другими инцидентами в XDR для последующего анализа.
4. Выделенные из потока объекты отправляются на анализ в MDP платформу контролируемого запуска («детонации») вредоносных программ.
5. В XDR отправляются подробные сетевые логи для проактивного поиска недетектируемых угроз.

2 ТРЕБОВАНИЯ К СИСТЕМЕ

ПО может быть установлено либо на физический сервер, либо на виртуальную машину.

2.1 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к физическому серверу в зависимости от типа Network Traffic Analysis - 1000, 5000 или 10K.

При наличии нескольких процессоров модуль NTA на физическом сервере не будет поддерживать анализ SPAN-трафика.

Параметр	**1000**	**5000**	**10 000**
Процессор	Intel Xeon Gold 5315Y 3.2GHz, 8C/16T, 11.2 GT/s, 12MB Cache, Turbo 3.6GHz, HT (140W) DDR4-2933	Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M CacheTurbo 3,6GHz HT (185W) DDR4-3200	Intel Xeon Gold 6348 2.6GHz, 28C/56T, 11.2GT/s, 42 M Cache Turbo 3,5GHz, HT (235W) DDR4-3200
Объем оперативной памяти	64 GB	64 GB	128 GB
Объем хранилища	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1
Сетевые интерфейсы			
Интерфейс управления	1 Ethernet	1 Ethernet	1 Ethernet
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

2.2 Минимальные технические требования для виртуальной машины

Ниже приведены минимальные технические требования к конфигурации оборудования виртуальной машины.

Параметр	1000	5000	10 000
Виртуальный процессор	16	40	56
Объем хранилища	480 GB SSD, Random write 44500 IOPS	960 GB SSD, Random write 44500 IOPS	960 GB SSD, Random write 44500 IOPS
Объем оперативной памяти	64 GB	64 GB	128 GB

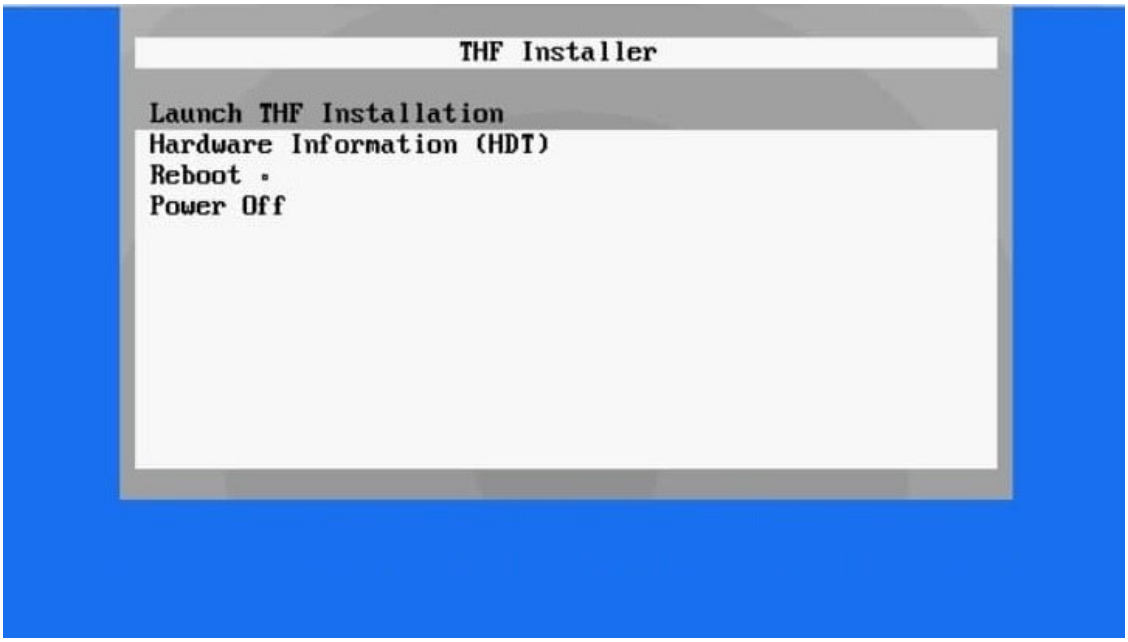
Параметр	1000	5000	10 000
Интерфейс анализатора сетевого трафика (NTA)	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter	1 port, Intel Ethernet Network Adapter

3 УСТАНОВКА ТЕСТОВОЙ ВЕРСИИ ПО

Образ **Network Traffic Analysis** можно установить, как на виртуальную машину, так и на физический сервер.

Для обновления ПО, проверки ссылок, отправки алертов и использования преимуществ *MXDR Console*, необходимо обеспечить доступ к *MXDR Console* через порт управления. При необходимости взаимодействие с *MXDR Console* может осуществляться через прокси-сервер. В этом случае должен поддерживаться метод `CONNECT` для установления подключений на 443 порт.

Во время загрузки с образа будет предложено установить **Network Traffic Analysis**. Здесь же можно просмотреть информацию об аппаратном обеспечении, перезапустить/выключить сервер или виртуальную машину.



Для установки **NTA** выполните следующие шаги:

1. В появившемся окне MXDR Installer выберите Install.

2. Появится окно с предложением выбрать язык отображения лицензионного соглашения.

3. Чтобы ознакомиться с текстом лицензионного соглашения используйте клавиши Page Up и Page Down.

4. Необходимо выбрать устройство, на котором будет установлен модуль NTA.

5. Начнется установка NTA.

6. В конце установки Вам будет предложено перезагрузить сервер или виртуальную машину.

7. Если установка прошло успешно, после перезагрузки откроется окно с приветственным экраном NTA.

3.1 Первоначальная настройка

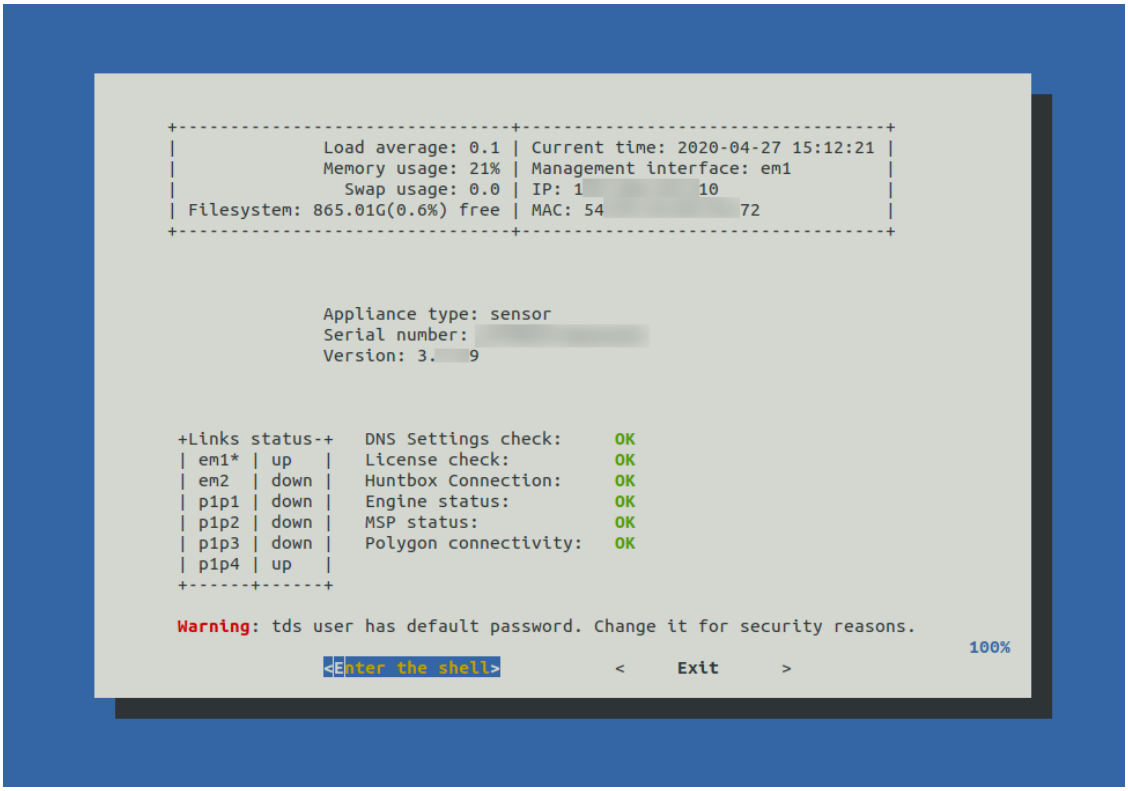
Для корректной работы модуля **NTA** необходимо провести первоначальную настройку через консоль. Доступ к консоли **NTA** можно получить любым из способов:

- С помощью KVM (D-SUB для видео и USB для клавиатуры).
- С помощью последовательного порта:
  - Baudrate: 115200
  - 8-bit
  - Flow control: ON
- Через SSH при условии настроенного сетевого подключения.

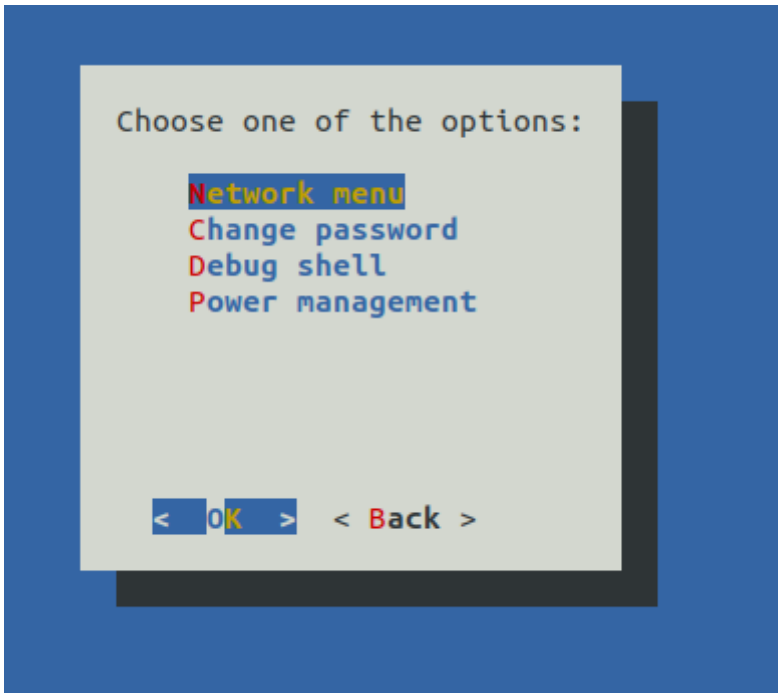
3.1.1 Логин/Пароль по умолчанию консоли NTA

Для управления сервером используйте учетную запись с логином **tds** и паролем **tds**.

После ввода логина и пароля на экран будет выведена основная информация о модуле **NTA**. Для входа в главное меню выберите опцию `Enter the Shell`.



3.1.2 Главное меню NTA

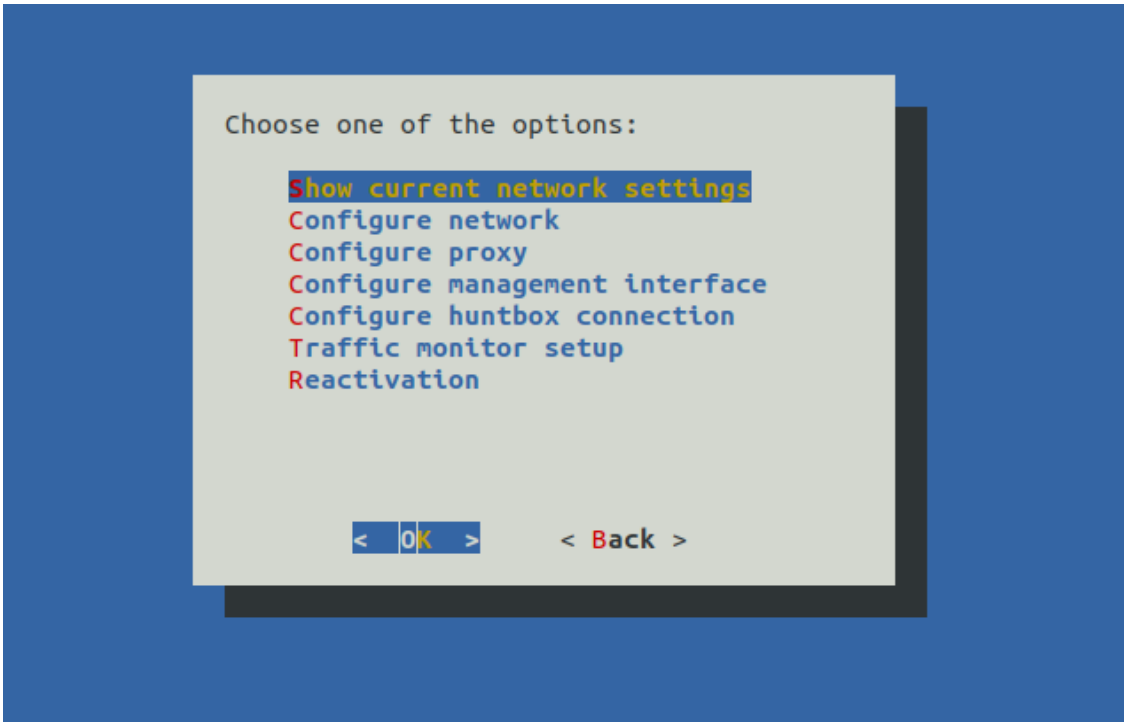


Пункт меню	Описание
Network menu	Просмотр и изменение настройки сети.
Change password	Меню изменения административного пароля пользователя *Managed XDR*.
Debug shell	Доступ до инструментов отладки в режиме командной строки.
Power management	Меню выключения или перезагрузки устройства.
Back	Вывод основной информации о статусе сервера. Эта информация также выводится при входе в систему.

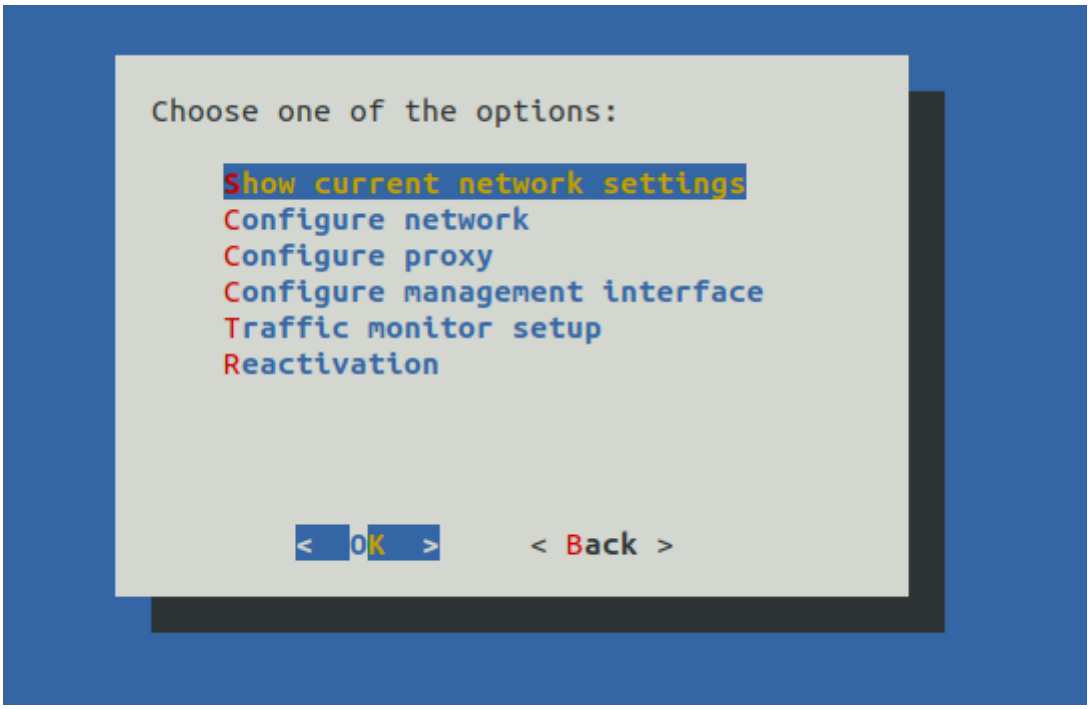
После нажатия кнопки **OK** откроется окно просмотра и изменения настройки сети.

3.1.3 Настройки сети

Если *MXDR Console* установлена локально в сети клиента, будут доступны следующие опции для настройки:



Если используется облачная *MXDR Console*, будут доступны следующие опции для настройки:



Пункт меню “Configure huntbox connection” будет отображаться только после активации **NTA** через *MXDR Console*.

Пункт меню	Описание
Show current network settings	Вывод текущей настройки сетевого интерфейса управления.
Configure network	Настройки сетевого интерфейса.

Пункт меню	Описание
Configure proxy	Настройки прокси для работы с *CERT / MXDR Console*.
Configure management interface	Предоставляет возможность задания управляющего интерфейса в **NTA**. Для задания выберите из списка интерфейсов нужный и нажмите “Ок”.
Configure huntbox connection	Позволяет задать IP адрес управляющего интерфейса *MXDR Console* (доступно только в случаях использования локального установки).
Traffic monitor Setup	Меню для ввода пула адресов, принадлежащих внутренней сетевой инфраструктуре, а также для указания SPAN интерфейсов.
Reactivation	Реактивация позволяет заново запустить процесс синхронизации с облачным или локальным *MXDR Console*.
Back	Возврат на уровень меню выше.

3.1.3.1 Configure network

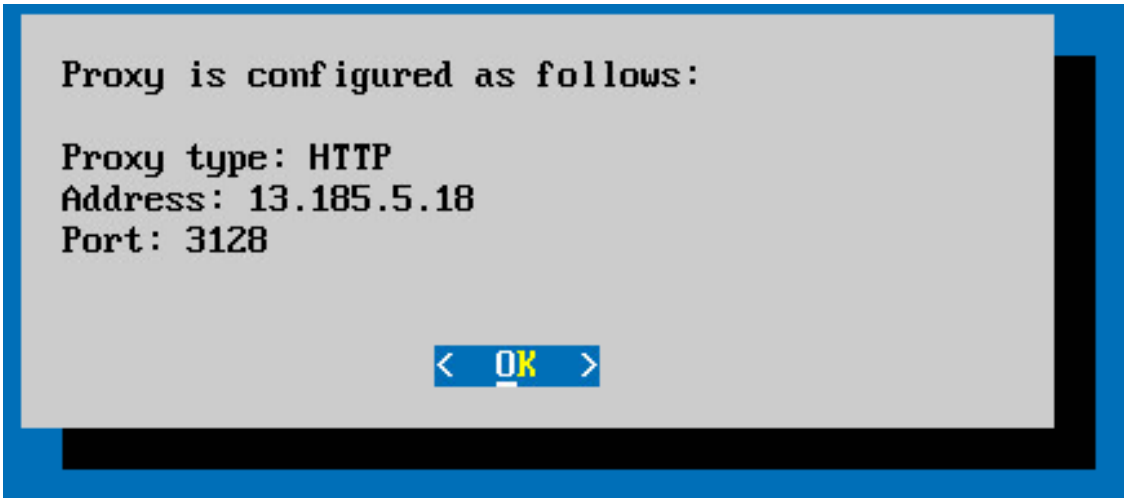
Доступны следующие варианты настроек:

- **DHCP**: автоконфигурация адреса и прочих настроек по протоколу DHCP. Производится автоконфигурация интерфейса и перезапуск сети.
- **Static**: статическая конфигурация параметров. Требуется ввод всех сетевых параметров вручную, после чего производится перезапуск сети. Для отмены ввода параметров в любой момент используется сочетание Ctrl+C.
- ***Cancel***: возврат на уровень меню выше.

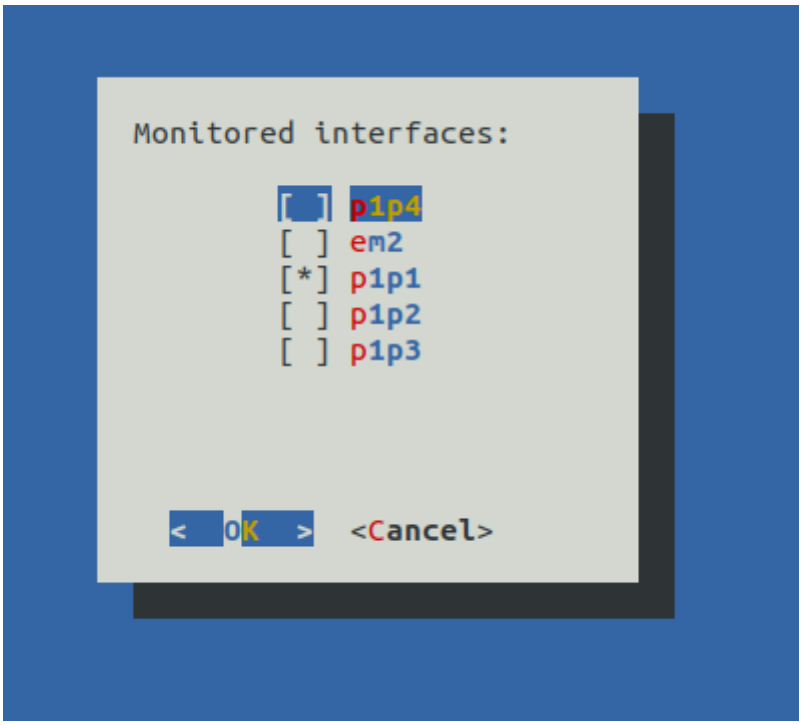
3.1.3.2 Configure proxy

NTA позволяет настроить использование прокси-сервера для доступа к обновлению базы сигнатур и правил анализа трафика, а также связи с облачным или локальным сервисом *MXDR Console*. В процессе настройки необходимо:

- Передать на устройство конфигурационную строку в следующем формате: Login:pass@domen_proxy:port
- Выбрать тип проксирования: http-proxy или socks-proxy.
- Проверить введенные значения в разделе меню Proxy Settings - Show current proxy settings.



Для успешного использования прокси-сервер должен поддерживать возможность осуществления запросов методом CONNECT с открытием соединений на 443 порт.



4 Сценарии проверки работоспособности ПО

4.1 Проверка физической работоспособности NTA

1. Проверить наличие и размещение оборудования Системы.
2. Проверить подачу питания на серверы Системы.
3. Проверить интеграцию с инфраструктурой заказчика.
4. Убедиться, что оборудование включается при нажатии кнопки включения.

4.2 Проверка корректности загрузки исполняемого программного обеспечения NTA

1. После корректной загрузки программного обеспечения на устройствах Системы отображается поле для ввода логина и пароля на вход в программную оболочку.

2. После входа в программную оболочку проверить статус соединения с MXDR Console: Huntbox connection - OK.

4.3 Проверка связности модулей XDR с Malware Detonation Platform

После загрузки ПО MDP необходимо проверить инфраструктурную связь модуля с другими компонентами системы.

1. Проверить наличие доступов, прописанных в карте взаимодействия.

2. При наличии локальной MXDR Console: перейти в раздел **Настройки** → **Модули** → **MXDR Console** → **Основные настройки** и добавить запись MDP из выпадающего списка доступных MDP модулей. Проверить, что статус модуля в настройке интеграции зеленый.

3. При наличии модуля NTA: перейти в раздел **Настройки** → **Модули** → **Network Traffic Analysis** → **Основные настройки** → **Интеграция с MDP** и добавить запись MDP (локальная или облачная). Проверить, что статус модуля в настройке интеграции зеленый.

4.4 Проверка поступления зеркалированного трафика на сетевые интерфейсы NTA и корректности обработки этого трафика

1. Проверить наличие прописанных сетей для анализа/исключений:

Перейти в раздел **Настройки** → **Модули** → **Network Traffic Analysis** → **Общие настройки** → **Сетевой трафик** → **Анализ сетевого трафика** и проверить наличие указанных домашних подсетей, подлежащих анализу, а также подсетей/адресов, исключаемых из анализа (Через настройки Белого списка или BPF фильтр).

2. Проверить активность модуля сигнатурного анализа:

– в программной оболочке NTA Engine status в состоянии OK;

– в разделе **Настройки → Модули → Network Traffic Analysis → Общие настройки → Сетевой трафик → Сетевые сигнатуры → Статус** “ON”. (Можно оставить включенные по умолчанию пакеты сигнатур).

3. Проверить корректность интеграции модуля и подачи трафика:

Индикатор состояния устройства в разделе **Настройки → Модули → Network Traffic Analysis** зеленый, а график **span** трафика/значение загрузки канала соответствуют ожидаемому значению (например, уровню среднего уровня загрузки канала сети организации).

4. Провести тестирование качества поданного трафика и наличие детекта:

o С устройства внутри инфраструктуры, трафик которого зеркалируется на NTA, перейдите по ссылке: https://trebuchet.f6.security/?tab=network (Нет необходимости использовать тестовую машину, так как в проводимом далее тестировании отсутствует реальная вредоносная нагрузка).

o В окне введите "start" и нажмите клавишу Enter.

o В Web-интерфейсе XDR проверьте наличие тестовых событий в разделе **Атаки → Алерты**.

o IP-адрес узла, с которого был проведен тест, должен отражаться в теле алерта.

– Детектирование синтетических запросов, генерируемых в процессе теста, указывает на следующее:

o Трафик тестового стенда действительно зеркалируется на NTA.

o NTA получает пригодные для сборки сессий кадры.

o NTA готов осуществлять детектирование угроз в сети предприятия.

4.5 Проверка функциональности сбора метаинформации о сетевых соединениях

1. Проверить, что зеркалированный трафик корректно поступает на сетевые интерфейсы NTA (см. предыдущий пункт), а график span трафика/значение загрузки канала соответствуют ожидаемому значению (например, среднему уровню загрузки канала сети организации).

2. Проверить наличие настройки сбора метаинформации устройством:

3. Перейти в раздел **Настройки → Модули → Network Traffic Analysis → Общие настройки → Сетевой трафик → Сбор метаинформации о сетевых соединениях** и перевести в статус ON сбор метаинформации по конкретным или всем перечисленным в разделе протоколам.

4. Перейти в раздел **Расследование → Сетевые соединения** и проверить наличие данных в разделе (заложить время ~ 5 мин.).

4.6 Подсистема интеграции с общими ресурсами

Для корректного проведения данного тестирования, необходимо выполнение пунктов по работоспособности MXDR Console и MDP, а также наличие корректной интеграции NTA с MDP.

1. Настройка инфраструктуры на стороне заказчика: сетевая доступность между NTA и файловым хранилищем, наличие отдельной учетной записи для доступа в хранилище, поддержка работы по протоколам.

2. Настройка интеграции на NTA:

Перейти в раздел **Настройки → Модули → Network Traffic Analysis → Основные настройки → Общие настройки → Монтирование общих ресурсов**, добавить новый ресурс. Для добавления необходимо добавить адрес хранилища, выбрать протокол доступа и ввести учетные данные для доступа. После добавления ресурса должны появиться данные о загрузке хранилища и индикатор успешного статуса интеграции.

3. Настройка режима работы с файловым хранилищем и анализа файлов:

Перейти в раздел **Настройки → Модули → NTA → Основные настройки → Файлы → Анализ общих ресурсов** и добавить запись о режиме работы для любого из доступных для настройки хранилищ.

4. Проверить работоспособность интеграции:

Перейти в раздел **Расследование → Проверенные файлы**, установить фильтр **Источник файла** в значение **DIR**.

5. Наличие файлов в данном режиме фильтрации свидетельствует о корректной интеграции с файловым хранилищем.

4.7 Модуль извлечения файлов из трафика

Для корректного проведения данного тестирования, необходимо выполнение пунктов по работоспособности MXDR Console и MDP, а также наличие корректной интеграции NTA с MDP.

1. Проверить, что зеркалированный трафик корректно поступает на сетевые интерфейсы NTA: Настройки → **Модули** → **Network Traffic Analysis** → **Индикатор** слева горит зеленым, а график span трафика/значение загрузки канала соответствуют ожидаемому значению (например, уровню среднего уровня загрузки канала сети организации).

2. Если MDP установлен локально, то необходимо убедиться, что на MDP нет очереди:

Перейти в раздел **Настройки** → **Модули** → **Malware Detonation Platform** → **На графике состояния** модуля во вкладке **Задачи** нет очереди.

3. Проверить, что включена опция извлечения файлов и протоколы для извлечения: **Настройки** → **Модули** → **Название Модуля** → **Общие настройки** → **Файлы** → **Анализ файлов из трафика** → **Протоколы** → **“Название протокола” – ON**.

4. Провести загрузку файла по протоколу HTTP (Ссылка на файл будет предоставлена вендором).

5. Проверить результаты тестирования в разделе **Расследование** → **Проверенные файлы**, установив фильтр **Источник файла** в значение протоколов, по которым происходит извлечение (HTTP).

5 Администрирование Network Traffic Analysis

5.1 Активация Network Traffic Analysis

Процедура активации Network Traffic Analysis включает в себя активацию лицензии и синхронизацию **Network Traffic Analysis** с **локальной MXDR Console** или **MXDR Console Cloud**.

5.1.1 Лицензионный ключ (UUID)

Перед активацией Network Traffic Analysis на облачном или **локальном MXDR Console** необходимо получить лицензионный ключ (UUID). Воспользуйтесь одним из следующих вариантов:

1. При активации на **MXDR Console** Cloud обратитесь к менеджеру или технической поддержке.
2. При активации на **локальном MXDR Console** используйте пункт меню **Добавить устройство**.

5.1.2 Перед активацией

Для взаимодействия Network Traffic Analysis с **MXDR Console** необходимы следующие порты:

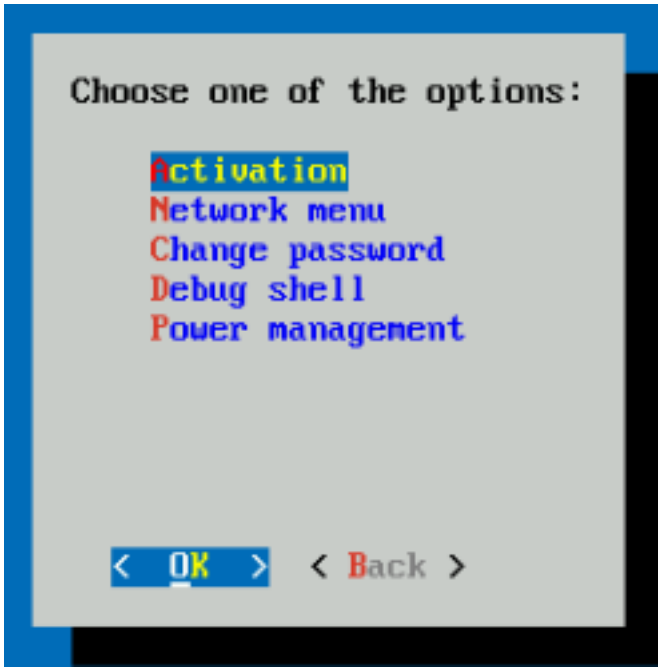
- **443/tcp** – для первичной активации и подключения к локальному **MXDR Console**;
- **443/tcp** — для подключения и дальнейшего взаимодействия Network Traffic Analysis с **MXDR Console Cloud**;
- **40500/tcp** — для первичной активации в **MXDR Console Cloud**;
- **1443/udp** – для дальнейшего взаимодействия модуля **NTA** с **MXDR Console** – только для локальной версии;
- **3000/tcp** – для взаимодействия **Network Traffic Analysis** с **Malware Detonation Platform**.

5.1.3 Активация

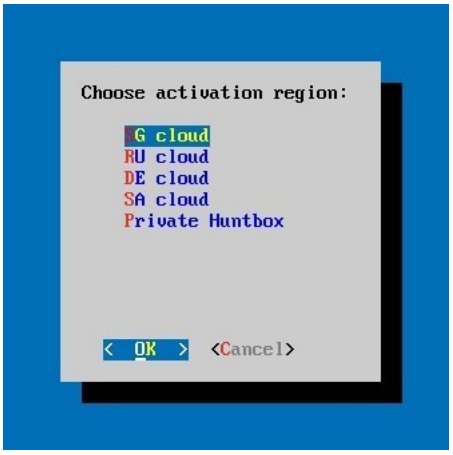
Примечание: активация и синхронизация осуществляется через консоль **Network Traffic Analysis**.

На данном этапе статус **MXDR Console** Connection равен **Fail,** так как **Network Traffic Analysis** не привязан к **MXDR Console**.

1. Выберите **Enter the shell** и нажмите **Enter**.
2. В открывшемся меню выберите **Activation**.



3. В открывшемся меню выберите регион активации при подключении к **MXDR Console Cloud** или **Private MXDR Console** в случае подключения к локальному **MXDR Console**.

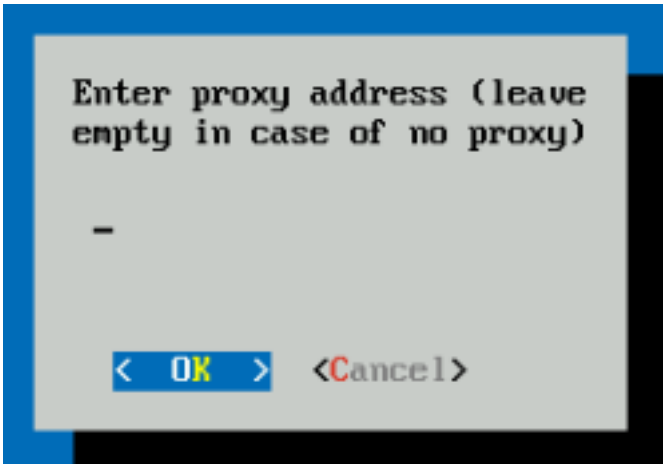


Если вы выбрали **MXDR Console Cloud**, перейдите к шагу **5**.

Если вы выбрали **Private MXDR Console**, появится окно, представленное на рисунке ниже.

4. Введите доменное имя или IP адрес и нажмите **Enter**.

После этого появится диалоговое окно, предлагающее задать адрес прокси.



5. Укажите адрес прокси сервера, если это необходимо, или оставьте поле пустым. После этого нажмите **Enter**.

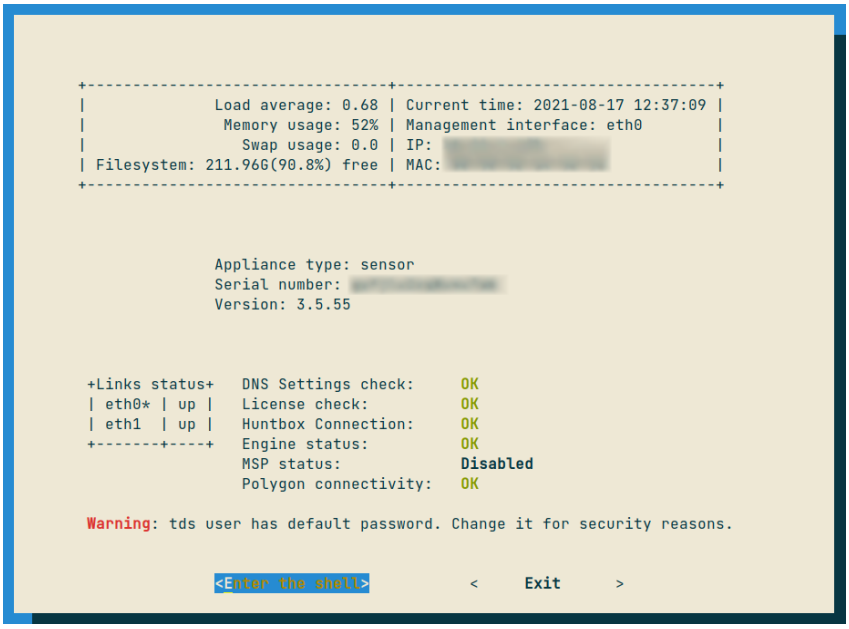
После появится диалоговое окно, предлагающее задать UUID.

6. Укажите UUID устройства и нажмите **Enter**.

Появится диалоговое окно, предлагающее подтвердить действие.

7. Выберите **Yes** и нажмите **Enter**.

Если необходимая информация была указана верно, то устройство перезапустится. После загрузки появится окно, представленное на рисунке ниже.



8. В UI **MXDR Console** перейдите в Меню **Настройки** → **Модули** → выберите устройство **Network Traffic Analysis**.

Здесь будет предоставлена информация по состоянию подключенного устройства. Как изображено на рисунке ниже.

5.2 Интеллектуальный анализ трафика Network Traffic Analysis

Данный блок содержит в себе набор функций, позволяющих: выявлять взаимодействия с управляющими серверами через **DGA**, а также управлять модулем выявления туннелей в верхнеуровневых протоколах.

1. Модуль выявления DGA-коммуникаций
2. Выявление горизонтального перемещения
3. Выявление скрытых каналов

5.2.1 Модуль выявления DGA-коммуникаций

Настройка позволяет выявлять взаимодействия с управляющими серверами через DGA.

Для того чтобы запустить процесс, необходимо заполнить поля:

- **Порог обращений** – количество DGA запросов для порождения одного события безопасности.
- **Порог секунд** – время, за которое учитываются DGA запросы в количестве заданном в пороге обращений.

После того как поля будут заполнены, нажмите на кнопку **Сохранить**.

5.2.2 Выявление горизонтального перемещения

В блоке **Интеллектуальный анализ трафика** настройка **Выявление горизонтального перемещения** представляет собой модуль для выявления распространения угроз во внутренней инфраструктуре.

5.2.3 Логика обработки

Используются ML классификаторы.

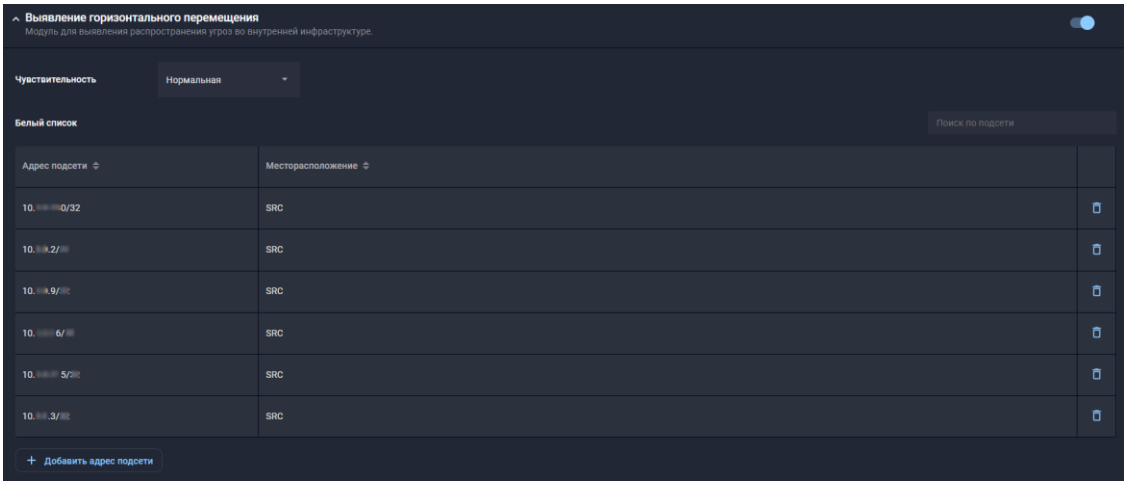
Network Traffic Analysis анализирует *kerberos* (update), *smb*, *ntlm*, *dce-rpc* протоколы на предмет обращения к файловым хранилищам администратора, записи на них файлов, использования *wmi* и т.п. используя ML классификаторы.

В зависимости от выбранной чувствительности алгоритм на основе совокупности индикаторов, описанных выше, создаёт события и алерты.

По умолчанию весь трафик настроенный на обработку в пункте **Анализ сетевого трафика** подпадает под классификатор **Выявление горизонтального перемещения** сразу после включения описываемого функционала.

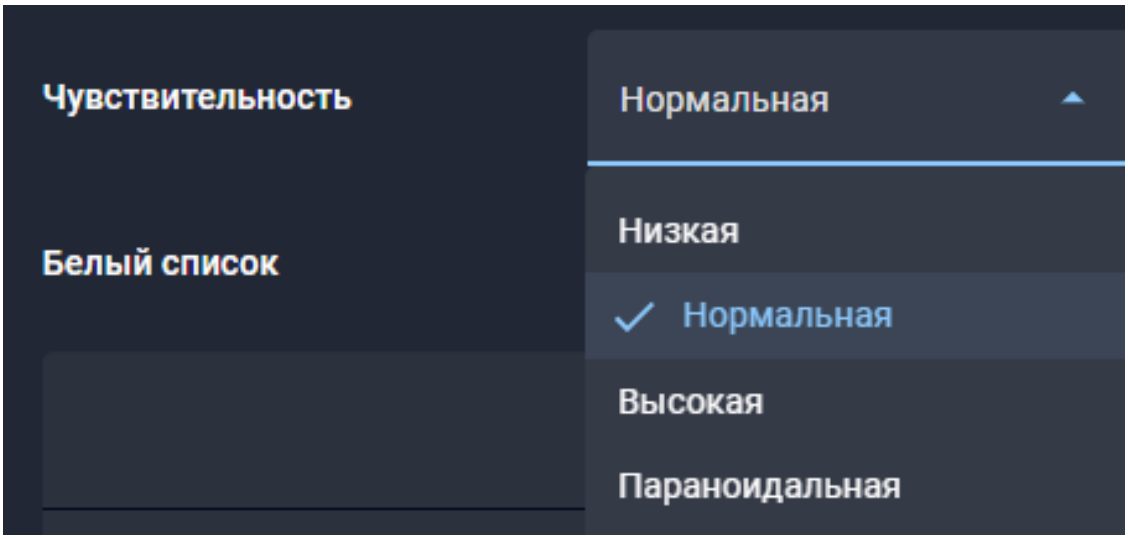
Для исключения лишних сетевых потоков необходимо воспользоваться белыми списками.

5.2.4 Настройка выявления горизонтального перемещения



5.2.4.1 Чувствительность

В поле **Чувствительность** выбирается степень чувствительности классификатора при выставлении алерта. Чувствительность – это отсечка по разнообразию и количеству анализируемых событий от одной машины за 10 минут, в течении которых определяется злоумышленное поведение. При этом, в случае выявления числа событий, переходящих определённый порог, злоумышленное поведение может быть определено в более короткие периоды.



5.2.4.2 Белый список

Для добавления IP-адреса в белый список, необходимо нажать на кнопку **Добавить адрес подсети**, и заполнить появившееся поле и сохранить настройки. Помимо непосредственно IP адреса возможно задать направление анализируемого потока для исключения из анализа. Таким образом возможно эффективно использовать ресурсы Network Traffic Analysis, уменьшается количество false-positive алертов, а также позволяет

целенаправленно обнаружить факты выявления скрытых каналов и горизонтальных перемещений, проводимых в нужном направлении.

Если необходимо изменить настройки детектирования для уже имеющегося IP-адреса, то его можно найти в строке поиска *Поиск по подсети*.

5.2.5 Выявление скрытых каналов

Переключатель **Выявление скрытых каналов** предназначен для управления верхнеуровневыми протоколами:

- DNS
- SSL
- HTTP
- ICMP

При обнаружении в сети соединений, создаваемых разными фреймворками (*meterpreter*, *dnscat*, *assitsov* и т.п.) автоматически создается алерт, который будет отображен в разделе **Алерты**.

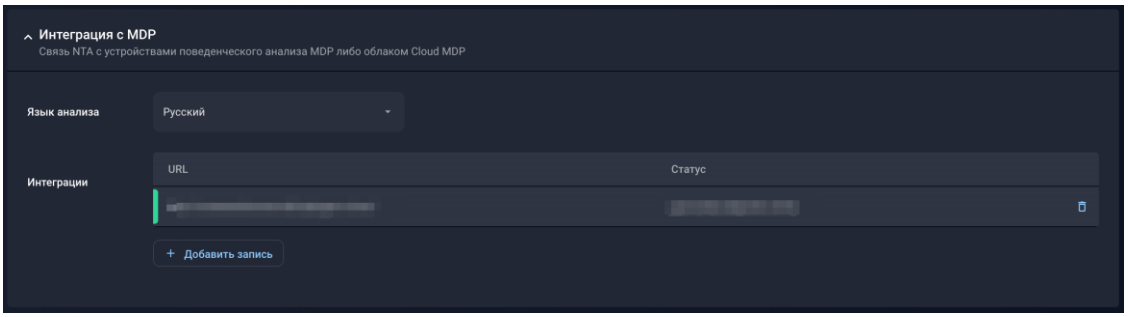
Для настройки управления модулем выявления туннелей в верхнеуровневых протоколах необходимо включить/выключить переключатель, затем нажать кнопку **Сохранить**.

5.3 Общие настройки Network Traffic Analysis

Данный блок содержит в себе набор функций, позволяющих: связывать Network Traffic Analysis с устройствами поведенческого анализа (**Malware Detonation Platform**, **Cloud Malware Detonation**), создавать белые списки индикаторов для исключения из анализа, создавать правила по разрешению сетевых адресов в доменные и сетевые имена, передавать регистрируемые события во внешние системы через Syslog, изменять синхронизацию времени устройства с **MXDR Console**, настраивать функции для мониторинга работы и состояния устройства.

5.3.1 Интеграция с MDP

Данная настройка позволяет интегрировать выбранный **Network Traffic Analysis** с определенным **Malware Detonation Platform** для осуществления функций поведенческого анализа.



- **Интеграции**

В меню задаётся запись в виде доменного имени или IP адреса **Malware Detonation Platform**. Существует возможность задавать более одной записи, чтобы обеспечить распределение нагрузки по поведенческому анализу. Управление очередью производится на стороне **Network Traffic Analysis**. **Network Traffic Analysis** осуществляет опрос всех подключённых к нему **Malware Detonation Platform** на предмет размера очереди поведенческого анализа и выбирает минимальную для следующего анализа.

- **Язык анализа**

Задаёт использование определённых образов операционных систем внутри подключённых **Malware Detonation Platform**. Данные операционные системы будут настроены для поддержания защиты от актуальных угроз в регионах с выбранной языковой системой (по умолчанию поддерживаются Русский и Английский языки).

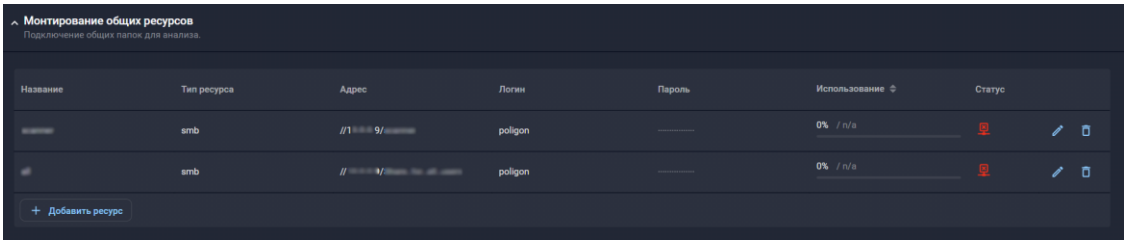
Для использования **Cloud Malware Detonation** (облачной версии MDP) используется одна из следующих записей:

- `http://command-server.tds/polygon_cloud`
- `10.144.178.1:3000`

5.3.2 Монтирование общих ресурсов

`Расположение:` UI > **Настройки** > **Модули** > в списке модулей выбрать необходимый Network Traffic Analysis и нажать **Основные настройки**> Блок **Общие настройки** > **Монтирование общих ресурсов**

В разделе **Монтирование общих ресурсов** выполняется только подключение папок для дальнейшего анализа.



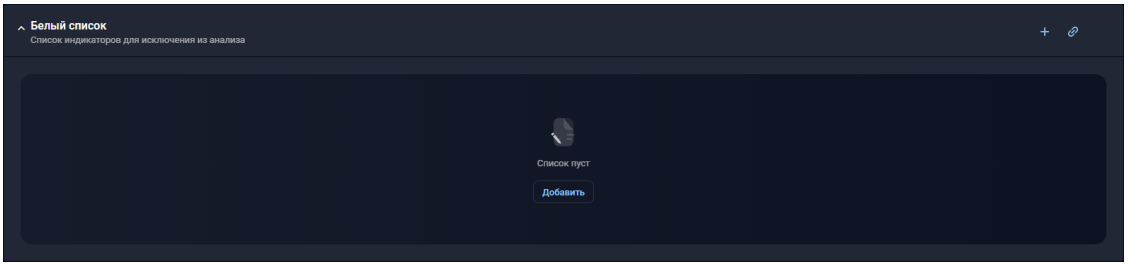
Чтобы добавить папки для подключения к общей сетевой папке Network Traffic Analysis необходимо нажать на кнопку **Добавить ресурс** и заполнить следующие поля:

- **Название** – наименование папки, присвоенное пользователем, которое будет отображаться разделе “Анализ общих ресурсов”.
- **Тип ресурса** – протокол, по которому будет проходить соединение с ресурсом (SMB, WebDAV, NFS, FTP).
- **Адрес** – расположение ресурса.
- **Логин** – логин для подключения к выбранному ресурсу.
- **Пароль** – пароль для подключения к выбранному ресурсу.
- **Использование** – размер хранилища.
- **Статус** – состояние подключения к выбранному ресурсу.

Кнопка	Описание
+ Добавить ресурс	Добавление нового ресурса.
	Редактирование существующей записи.
	Удаление существующего ресурса.
	Сохранение новых изменений.
	Отмена изменений в новой записи.
	Успешное подключение.
	Неуспешное соединение.

5.3.3 Белый список

Белые списки позволяют исключить из анализа внесенные в них объекты в компонентах Network Traffic Analysis и Malware Detonation Platform. Оптимизация работы решения с помощью данного инструмента – обязательное условие высокого качества обнаружения атак.



Белый список можно создать по следующим индикаторам:

- Подсети
- Email-адреса
- Домены
- URLs
- Хэши
- Подписи файлов

Email-адреса берутся из параметров SMTP-сессии (MAIL FROM и RCPT TO). В случае выявления добавленных в белый список email-адресов письма не будут проанализированы и сразу отправятся получателю.

Данные типы записей группируются по соответствующим вкладкам по мере пополнения списка.

5.3.3.1 Работа с белым списком

Для работы с блоком настроек **Белый список** в модуле **NTA** следуйте шагам, описанным ниже:

1. Перейдите во вкладку Общие настройки и выберите настройку Белый список.

Если список пуст, вы увидите сообщение Список пуст. Иначе, вы увидите существующий список объектов, разделенный на вкладки.

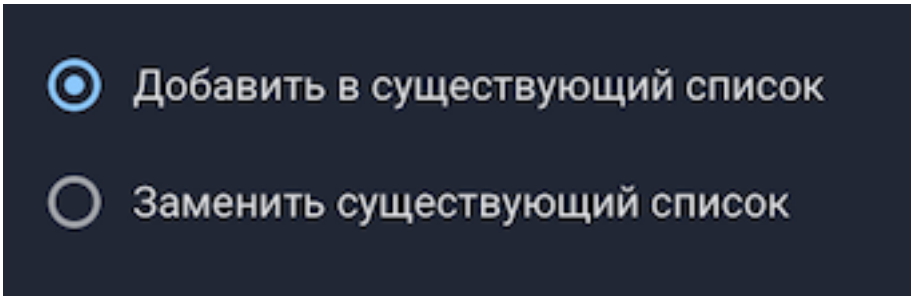
2. Нажмите **Добавить** или **plus-icon**, затем выберите тип записи, которую необходимо добавить в белый список. Справа появится боковая панель.
3. Заполните обязательные поля:

Тип записи	Поля
Подсети	Позволяет исключать потоки данных на сетевом уровне в различных направлениях (от и/или к целевым, защищаемым хостам). Система поддерживает **IPv4** и **IPv6**.

Тип записи	Поля
Email-адреса	Поле для записи Email-адресов построчно. Система поддерживает ввод, как единичных адресов, так и целых доменов. Например, можно добавить в **Белый список** один адрес **info@f6.ru** или все почтовые аккаунты в домене **.*@f6.ru** с помощью регулярных выражений.
Домены	Домены построчно.
URLs	Ссылки на веб-ресурсы построчно.
Хэши	Для каждого типа хешей - MD5, SHA1, SHA256 - отдельное поле для записи построчно.
Подписи файлов	Подписи файлов построчно.

Вы можете добавлять записи, указывая их построчно или загружать их в файле с расширением **.txt**. Для составления списка необходимо использовать регулярные выражения. Чтобы загрузить файл нажмите file-icon и перетащите необходимый файл или выберите его в проводнике.

4. Решите, хотите ли вы добавить записи в существующий список или создать новый, и нажмите соответствующую кнопку.



5. Если вы добавляете Подсети, то выберите опции из блоков Направление и Типы событий.

Направление:

- **SRC** – искать в отправителе
- **DST** – искать в получателе

Типы событий

- **Ссылки в почте –** применять к ссылкам на скачивание в письмах
- **Файлы из трафика –** применять к извлеченным из трафика файлам
- **Сигнатурный анализ –** применять к срабатываниям сигнатур при анализе трафика

6. Если вы добавляете Email-адреса, выберите направление анализа для электронных писем:

- **От кого — искать в отправителе.**

- **Кому — искать в получателе.**

7. если вы добавляете Домены или URLs, то выберите необходимые опции из блока Типы событий:

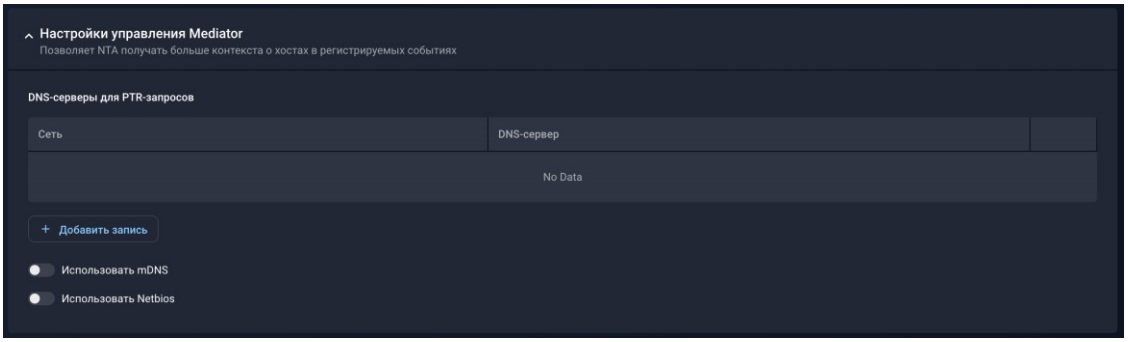
- **Ссылки в почте – применять к ссылкам на скачивание в письмах**
- **Файлы из трафика – применять к извлеченным из трафика файлам**
- **Сигнатурный анализ – применять к срабатываниям сигнатур при анализе трафика**

8. Нажмите **Добавить** в правом верхнем углу.

Новые записи появятся в списке в соответствующей вкладке.

5.3.4 Настройки управления Mediator

Данный раздел активирует возможности сенсора по разрешению сетевых адресов в доменные и сетевые имена. Таким образом, аналитикам предоставляется удобный инструмент для быстрого определения принадлежности хостов к обнаруженным инцидентам и тем самым сокращается время реагирования.



5.3.4.1 DNS-сервера для PTR запросов

Настройка позволяет изменить стандартные маршруты по выполнению PTR (reverse DNS) запросов и позволяет задать статические маршруты для выполнения подобных запросов. Чтобы настроить нестандартные маршруты PTR-запросов заполните записи в формате:

- **Сеть**

  Подсеть/сеть/IP адрес – настройка задаёт подсеть/сеть/адрес для которых необходимо разрешать IP адреса в доменные имена.

- **DNS-сервер**

  Настройка задаёт сервер, который будет отвечать за обслуживание PTR запросов для указанных подсетей/сетей/адресов.

5.3.4.2 Использование mDNS

Активирует на сенсоре протокол mDNS и позволяет осуществлять мультикаст DNS запросы для разрешения адресов в доменные/сетевые имена.

5.3.4.3 Использование Netbios

Активирует на сенсоре использование протокола Netbios для определения сетевых имён хостов.

5.3.5 Экспорт данных

Система **MXDR** предоставляет Пользователю возможность экспорта событий и сведений о состоянии устройств во внешние системы. При этом события можно экспортировать в двух форматах: JSON и CEF. Сведения о состоянии устройств (heartbeats) можно экспортировать в формате JSON.

- **CEF** - (нативный для SIEM ArcSight), с уровнями угроз Low (1-2), Medium (3), High (4) и Very-High (5)
- **JSON** - формат с уровнем угрозы (severity) от 1 до 5.

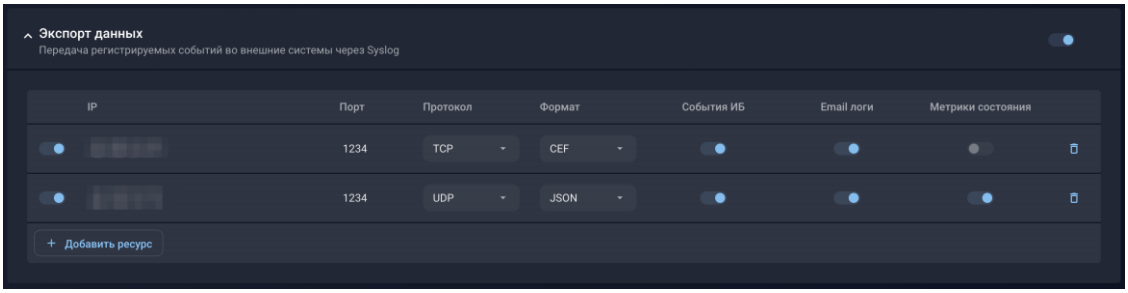
Функция экспорта обладает следующими свойствами:

- Сообщения будут отправляться напрямую от устройства до указанных в настройке серверов.
- Для экспорта сообщений во внешние системы необходимо задать сетевой адрес, порт и протокол (UDP/TCP), формат экспортируемого сообщения, а также отметить необходимые экспортируемые данные
- Существует возможность задавать только один сервер для каждого доступного формата.

Для функции экспорта доступны следующие данные:

- События ИБ.
- Email логи.
- Метрики состояния (доступно только при формате экспорта JSON).

Таким образом возможна интеграция с любой аналитической системой, которая может обрабатывать стандартный формат syslog.



5.3.5.1 События ИБ в формате JSON

Описание возможных полей при получении события ИБ в формате JSON представлено в таблице ниже.

Поле	Описание
`id`	ID события.
`alert_id`	ID алерта MXDR.
`timestamp`	Дата и время события. Время в UTC.
`host`	UUID сенсора, на котором случилось событие.
`company_id`	ID компании MXDR.
`event_type`	Тип события. Ниже приведен список возможных типов событий в формате: "Значение поля – Описание"
`event_classifier`	Внутреннее наименование классификатора событий. Ниже приведен список возможных типов классификаторов в формате: "Значение поля – Описание"
`integration_system`	Подсистема, которая обнаруживает угрозу.
`target`	Цели атаки (IP-адреса, домены, и т.д.)
`target.ip_addresses`	IP адрес.
`message`	Описание события.
ioc	Индикаторы компрометации (могут быть разные). Вложенность указана ниже.
`ioc.event`	Словарь, в котором находятся индикаторы компрометации.
`ioc.event.urls`	URL событий.
`ioc.event.protocols`	Протоколы событий.
`ioc.event.sids`	Идентификаторы сигнатур.
`ioc.suricata_rules`	Название сигнатуры.
`ioc.domains`	Домены.
`ioc.extended`	Дополнительная информация.
`ioc.extended.categories`	Категория вредоносного ПО (если применимо).
`ioc.extended.ip_addresses`	IP адреса.
`action`	Примененное действие. Может быть:
`severity`	Уровень угрозы (от 1 до 5).
`verdict`	Вердикт по событию.

Поле	Описание
data	Данные, информация. Вложенность указана ниже.
data.network_info	Список информации о сети. Вложенность указана ниже.
data.network_info.target	Цель атаки. Может быть:
data.network_info.sourse.ip	IP отправителя.
data.network_info.source.port	Port отправителя.
data.network_info.payload	Различная дополнительная информация об атаке.
data.network_info.destination.ip	IP получателя.
data.network_info.destination.port	Port получателя.
data.network_info.transport_protocol	Протокол транспортного уровня: TCP, UDP и т.д.
data.signatures_info	Список информации о сигнатурах. Вложенность указана ниже.
data.signatures_info.revision	Ревизия.
data.signatures_info.signature_id	ID сигнатуры.
data.signatures_info.name	Наименование.
data.http_info	Детали HTPP сессии.
data.http_info.request_headers	Заголовки запроса.
data.http_info.request_headers.Host	Хост сервера.
data.http_info.request_headers.Method	Метод HTTP запроса.
data.http_info.request_headers.User-Agent	User agent.
data.http_info.response_headers	Заголовки ответа.
data.http_info.response_headers.Protocol	Версия http.
data.http_info.response_headers.StatusCode	Код ответа.
data.http_info.response_headers.Content-Length	Длина ответа.
data.http_info.uri	URI запроса.
huntbox_host	Хост
attribution	Список атрибутов

Поле	Описание
attribution.mitre_tags	Идентификаторы тактик, методов и процедур по классификации MITRE.
attribution.malware	Отношение к известному вредоносному ПО. Будет список со словарями:
attribution.threatactor	Отношение к известной хакерской группировке. Будет список со словарями:

Пример события ИБ “Скрытй канал” в формате JSON приведен ниже:


```
{
  "id": "001bsnd1fv",
  "alert_id": "",
  "timestamp": "2024-04-24T08:14:42.788223+0000",
  "host": "host",
  "company_id": 0,
  "event_type": "Covert Channel",
  "event_classifier": "void",
  "integration_system": "example",
  "target": {
    "ip_addresses": [
      "1.1.1.1"
    ]
  },
  "message": "Possible DNS Tunneling",
  "ioc": {
    "event": {
      "domains": [
        "ops.beeline.ru"
      ]
    },
    "extended": {
      "ip_addresses": [
        "1.1.1.1"
      ]
    }
  },
  "action": "allowed",
  "severity": 2,
  "verdict": true,
  "data": {
    "network_info": {
      "target": "source",
      "source": {
        "ip": "2.2.2.2",
        "port": 49892
      },
      "destination": {
        "ip": "3.3.3.3",
        "port": 53
      },
      "payload": "proto: mklwaybona3rmprq53j7vp4x74.n3.r.dmg.digitaltarget.ru",
      "payload_ascii": ""
    }
  },
  "huntbox_host": "",
  "attribution": {
```

```
    "mitre_tags": [
      "T1572",
      "T1071.004"
    ]
  }
}
```

5.3.5.2 События ИБ в формате CEF

Описание возможных хедеров при получении события ИБ в формате CEF представлено в таблице ниже.

Поле	Описание
timestamp	Дата и время создания события в формате UTC.
hostname	UUID устройства в системе MXDR, проводящего анализ письма.
start	Дата и время события.
src	Порт источника события.
cat	Порт назначения.
dpt	IP-адрес назначения.
dhost	Хост назначения.
app	Приложение.
reportedResourceID	Идентификатор ресурса.
Request	Запрос.
dvchost	Хост устройство.
cs1	IOC (индикатор компрометации) - домен
cs1Label	Всегда будет иметь значение “IOC Domain”
cs2	IOC (индикатор компрометации) - IP-адрес
cs2Label	Всегда будет иметь значение “IOC IP”
cs3	ID письма, связанного с атакой
cs3Label	Всегда будет иметь значение “Envelope ID”
cs4	Тема письма, связанного с атакой
cs4Label	Всегда будет иметь значение “Envelope Subject”
fileHash	Hash файла
fname	Имя файла
suser	Отправитель.
duser	Получатель.
eventId	ID эвента.

Пример события ИБ “Скрытй канал” в формате JSON приведен ниже:

```
<timestamp> <hostname> CEF:0||XDR|1.1|0|Possible DNS Tunneling|Low|start=<datetime>
src=<source_IP_address> spt=<source_port> dst=<destination_IP_address> dpt=<destinat
```

```
ion_port> cat=<category> dhost=<destination_host> app=<application_name> reportedRes
ourceID=<reported_resource_ID> Request=<request> dvchost=<device_host> cs1=<...> cs1
Label=IOC_domain cs2=<...> cs2Label=IOC IP cs3=<....> cs3Label=Envelope ID cs4=<...>
cs4Label=Envelope Subject fileHash=<hash> fname=<file_name> suser=from@from.from dus
er=to@to.to eventId=<event_ID>
```

5.3.5.3 События по обработанным письмам в формате JSON

Описание возможных полей при получении события ИБ в формате JSON представлено в таблице ниже.

Поле	Описание
id	ID события.
_type	Тип события.
device_id	Идентификатор устройства, которое отправило сообщение.
sender_ip	IP-адрес отправителя.
sender_helo	HELO/EHLO идентификатор отправителя.
mail_from	Адрес электронной почты отправителя.
rcpt_to	Адрес электронной почты получателя.
size	Размер исходного файла письма(Байт).
sha256	SHA-256 хэш сообщения
whitelisted	Наличие отправителя в белом списке.
spam_whitelisted	Наличие отправителя в белом списке спама.
verdict	Вердикт по письму
unwanted	Флаг, указывающий, что письмо нежелательно.
amnesty	Флаг, указывающий, что письмо может проигнорировать ряд проверок.
ts_created	Временная метка создания письма.
ts_sent	Временная метка отправки письма.
delivered	Временная метка доставки письма.
delivery_attempts	Количество попыток доставки письма.
auth	Статусы проверки письма. Вложенность указана ниже.
auth.spf	Результат проверки SPF.
auth.dkim	Результат проверки DKIM.

Пример события по обработанным письмам в формате JSON приведен ниже

```json
{
    "id": 11002,
    "_type": "example",
    "device_id": "ascdmd",
    "sender_ip": "192.168.144.4",
    "sender_helo": "",
    "mail_from": "from@from.from",
    "rcpt_to": "to@to.to",
    "size": 8376,
    "sha256": "5sdvfdcx23cxvvzlm2l34",
    "whitelisted": false,
```

```
    "spam_whitelisted": false,
    "verdict": false,
    "unwanted": true,
    "retro": false,
    "amnesty": false,
    "ts_created": "2023-04-27T12:54:23.580036737Z",
    "ts_sent": null,
    "delivered": null,
    "delivery_attempts": 0,
    "auth": {
        "spf": "none",
        "dkim": false,
        "dmarc": null
    },
    "subject": "xxckdnviehgsnvcojsg",
    "yara": [],
    "attaches": [],
    "links": [],
    "timestamp": "2023-04-27T12:54:37.028915717Z",
    "event": "Analyzed",
    "state": "Analyzed"
}
```


5.3.5.4 События по обработанным письмам в формате CEF

Описание возможных хедеров при получении события по обработанным письмам в формате CEF представлено в таблице ниже.

Поле	Описание
timestamp	Дата и время создания события в формате UTC.
hostname	UUID устройства в системе MXDR, проводящего анализ письма.
suser	Отправитель.
duser	Получатель.
filehash	Хэш сумма исходного файла письма.
fsize	Размер исходного файла письма.
cs1	Статус доставки письма. Может принимать следующие значения:- Received - письмо получено,- Whitelisted - письмо добавлено в белый список (проанализировано не будет),- Parsed - из письма извлечены заголовки, файлы, ссылки и т.д.,- Analysed - письмо проанализировано,- Bypassed - письмо не было проверено за отведенное время и было отправлено далее,- Blocked - письмо заблокировано по результатам анализа и не будет доставлено

Поле	Описание
	получателю,- Delivered - письмо доставлено успешно,- Rejected - доставка отклонена,- Failed - доставка письма не удалась.
cs1Label	Всегда имеет значение event
cs2	Статус проверки письма.
cs2Label	Всегда имеет значение state.
cs3	Тема письма, по которому было сформировано данное событие.
cs3Label	Всегда имеет значение subject.
cs4	Статусы проверки записей **SPF**, **DKIM** и **DMARC**. Для каждого типа записи может быть отображено одно из значений:- none - не проводилась,- True - проверка пройдена,- False - проверка не пройдена.
cs4Label	Всегда имеет значение auth.
cs5	Основания вердикта.
cs5Label	Всегда имеет значение verdictDetails.
cs6	Ответ почтового сервера.
cs6Label	Всегда имеет значение serverResponse.
cnt	Количество попыток доставки письма.
cn1	Наличие отправителя в белом списке.- 0 - не занесен в белый список,- 1 - обнаружен в белом списке.
cn1Label	Всегда имеет значение whitelisted.
cn2	Присвоен ли письму статут “Нежелательное”.- 0 - не присвоен,- 1 - присвоен.
cn2Label	Всегда имеет значение unwanted.
cn3	Статус доставки письма. - 0 - не доставлено,- 1 - доставлено.
cn3Label	Всегда имеет значение delivered.
start	Дата и время появления письма в системе в формате UTC.
end	Дата и время окончания анализа в формате UTC.
rt	Дата и время отправки текущего сообщения в формате UTC.

Пример события по обработанным письмам в формате CEF приведен ниже:

```
<timestamp> <hostname> CEF:0||BEP|1.0|0|LOGS|0|src=<IP-address> suser=from@from.from
duser=to@to.to filehash=<hash> fsize=<size_in_bytes> cs1=Rejected cs1Label=event cs2
=Analyzed cs2Label=state cs3=<...> cs3Label=subject cs4=SPF:none,DKIM:False,DMARC:No
```

```
ne cs4Label=auth cs5=<...> cs5Label=verdictDetails cs6=<...> cs6Label=serverResponse
cnt=0 cn1=0 cn1Label=whitelisted cn2=1 cn2Label=unwanted cn3=0 cn3Label=delivered st
art=<timestamp> end=<unknown> rt=<timestamp>
```

5.3.5.5 Метрики состояния в формате JSON

Метрики состояния - это набор количественных показателей, которые используются для оценки текущего состояния системы, устройства или процесса.

Экспорт метрик состояния на текущий момент доступен только в формате JSON.

Экспортируемый JSON содержит информацию о конфигурации и состоянии системы:

- os - используемая операционная система.
- hardware - содержит информацию об аппаратном обеспечении, в том числе:
  - cpu0 - параметры центрального процессора, включая модель (cascadelake), количество ядер (cores) и набор поддерживаемых инструкций (flags).
- memory - информацию о памяти можно оценить по ключам vmmem_free (свободная виртуальная память) и vmmem_used (используемая виртуальная память), ram_percent (процент использования оперативной памяти).
- disk - информация о дисковом пространстве представлена ключами disk_free (свободное место) и disk_used (занятое место), а также hdd_percent (процент занятости диска).
- services (службы) - обширный раздел, описывающий различные службы, запущенные в системе, такие как MSP, analgin, atmosphere, bread и другие.
- interface - сетевой интерфейс, используемый устройством eth0.

Пример экспорта метрик состояния в формате JSON представлен ниже:


```
{
    "os": "arch",
    "host": "512313123w",
    "uptime": 176597.16,
    "timestamp": "2024-04-25T16:05:24.168704",
    "cpu_percent": 10.1,
    "disk_free": 30887964672,
    "disk_used": 22145843200,
    "hdd_percent": 41.8,
    "vmmem_free": 7528194048,
    "vmmem_used": 10861416448,
    "ram_percent": 60.1,
    "swapm_free": 0,
    "swapm_used": 0,
    "bios_version": "0.0.0",
    "kernel_version": "5.15.14-1-lts",
    "krnl_drops": 0,
    "krnl_packets": 1723907,
```

```
    "tcp_segment_memcap_drop": 0,
    "tcp_reassembly_gap": 55,
    "tcp_reassembly_memuse": 98304,
    "flow_memuse": 184777216,
    "ifaces_packets": 1723902,
    "ifaces_bytes": 1320539974,
    "ifaces_drops": 0,
    "time_delta": 61.380366,
    "ifaces_packets_delta": 0,
    "ifaces_bytes_delta": 0,
    "ifaces_drops_delta": 0,
    "krnl_packets_delta": 0,
    "krnl_drops_delta": 0,
    "tcp_segment_memcap_drop_delta": 0,
    "tcp_reassembly_gap_delta": 0,
    "BPS": 0.0,
    "PPS": 0.0,
    "ifaces_packets_drops": 0,
    "kernel_packets_drops": 0,
    "ansible_playbook_tag": "4.13.1",
    "tds_registry": {
        "MSP": {
            "api_url": "http://127.0.0.1/msp/",
            "block": false,
            "bypass_interval": 15,
            "cleanup_interval": 5,
            "db": {
                "user": "msp",
                "password": ""
            },
            "debug": false,
            "deep_cleanup": true,
            "deep_cleanup_interval": 14,
            "download_archive": true,
            "enabled": true,
            "links_analysis": {
                "enabled": true,
                "retry_intervals": [
                    [60, 5],
                    [1380, 60]
                ],
                "strategy": "balanced"
            },
            "max_workers": 10,
            "mta": false,
            "notify_on_block": true,
            "notify_on_fail": {
                "enabled": false,
                "mail_from": "",
                "relay": {},
                "retries": 1440
            },
            "postman_timeout": 300,
            "proxy": {},
            "slow_internet": 5,
            "trust_mailfrom": false,
            "trust_rcpt": false,
            "verification": {
```

```
            "custom_dns": "",
            "enabled": true
        }
    },
    "analgin": {
        "cache_ttl": 60,
        "db": {
            "host": "localhost",
            "name": "analgin",
            "password": "",
            "port": 5432,
            "user": "analgin"
        },
        "endpoint": "http://127... ",
        "host": "127.0.0.1",
        "local": true,
        "port": 8050
    },
    "ansible_playbook_original_tag": "4.13.1",
    "ansible_playbook_tag": "4.13.1",
    "appliance_type": "sensor",
    "atmosphere": {
        "api_url": "http://127... ",
        "cloudy": {
            "env": {
                "NUT_DOMAIN": "127…"
            },
            "mail_retention": {
                "keep_benign_days": 7,
                "keep_malicious_days": 90,
                "keep_spam_days": 30
            },
            "mongodb": {
                "database": "cloudy",
                "password": "",
                "username": "cloudy"
            },
            "s3": {
                "access_key": "...",
                "bucket_name": "cloudy",
                "secret_key": "..."
            }
        },
        "enabled": true,
        "mta": {
            "enabled": true
        },
        "phemida": {
            "mongodb": {
                "database": "db",
                "password": "...",
                "username": "db"
            }
        },
        "thundercloud": {
            "file_retention_days": 2,
            "mongodb": {
                "database": "db",
```

```
                "password": "...",
                "username": "db"
            },
            "s3": {
                "access_key": "...",
                "secret_key": "..."
            }
        }
    },
    "bread": {
        "bpf": "",
        "enabled": false,
        "ftp": true,
        "http": true,
        "pop3": true,
        "smb": false,
        "smtp": true,
        "workers": 4
    },
    "cappuccino": {
        "block": true,
        "enabled": true,
        "host": "0.0.0.0:1344",
        "yara": false
    },
    "cheko": {
        "db": {
            "host": "db",
            "name": "...",
            "password": "",
            "port": 5432,
            "user": "..."
        },
        "passive": {
            "enabled": false
        }
    },
    "device_activated": true,
    "dga": {
        "enabled": false
    },
    "disabled_services": [],
    "dumper": {
        "days_to_store": 14,
        "enabled": false,
        "fileshare": "",
        "iface": "",
        "path": "/captures/",
        "rotate_sec": 60
    },
    "environment": "env-stage",
    "hardware": {
        "cpu0": {
            "architecture": "db",
            "cores": 6,
            "flags": [
                "fpu",
                "vme",
```

```
                    "de",
                    "pse",
                    "tsc",
                    "msr",
                    "pae",
                    "mce",
                    "cx8",
                    "apic",
                    "sep",
                    "mtrr",
                    "pge",
                    "mca",
                    "cmov",
                    "pat",
                    "pse36",
                    "clflush",
                    "mmx",
                    "fxsr",
                    "sse",
                    "sse2",
                    "ss",
                    "ht",
                    "syscall",
                    "nx",
                    "pdpe1gb",
                    "rdtscp",
                    "lm",
                    "constant_tsc",
                    "arch_perfmon",
                    "rep_good",
                    "nopl",
                    "xtopology",
                    "cpuid",
                    "tsc_known_freq",
                    "pni",
                    "pclmulqdq",
                    "vmx",
                    "ssse3",
                    "fma",
                    "cx16",
                    "pdcm",
                    "pcid",
                    "sse4_1",
                    "sse4_2",
                    "x2apic",
                    "movbe",
                    "popcnt",
                    "tsc_deadline_timer",
                    "aes",
                    "xsave",
                    "avx",
                    "f16c",
                    "rdrand",
                    "hypervisor",
                    "lahf_lm",
                    "abm",
                    "3dnowprefetch",
                    "cpuid_fault",
```

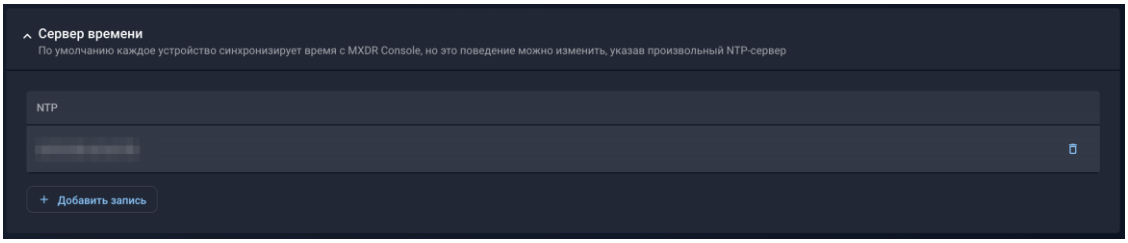
```
                    "invpcid_single",
                    "ssbd",
                    "ibrs",
                    "ibpb",
                    "stibp",
                    "ibrs_enhanced",
                    "tpr_shadow",
                    "vnmi",
                    "flexpriority",
                    "ept",
                    "vpid",
                    "ept_ad",
                    "fsgsbase",
                    "tsc_adjust",
                    "bmi1",
                    "avx2",
                    "smep",
                    "bmi2",
                    "erms",
                    "invpcid",
                    "mpx",
                    "avx512f",
                    "avx512dq",
                    "rdseed",
                    "adx",
                    "smap",
                    "clflushopt",
                    "clwb",
                    "avx512cd",
                    "avx512bw",
                    "avx512vl",
                    "xsaveopt",
                    "xsavec",
                    "xgetbv1",
                    "xsaves",
                    "arat",
                    "umip",
                    "pku",
                    "ospke",
                    "avx512_vnni",
                    "md_clear",
                    "tsc_type=constant_tsc"
                ],
                "hdd_firmware": "G987.0104",
                "vendor": "Intel"
            }
        },
        "interface": "eth0",
        "kerberos": {
            "db": {
                "host": "localhost",
                "name": "kerb",
                "password": "",
                "port": 5432,
                "user": "kerb"
            }
        },
        "license_status": "valid",
```

```
        "maxmind": {
            "key": "..."
        },
        "mq": {
            "enabled": false,
            "log_max_age": 7,
            "log_max_size": 1000,
            "log_retention": 2,
            "psql": {
                "host": "localhost",
                "password": "...",
                "port": 5432,
                "user": "mq"
            }
        },
        "optica": {
            "enabled": false,
            "listen": "localhost: ",
            "sensor_id": "00000000-0000-0000-0000-000000000000"
        },
        "os": "arch",
        "postoffice": {
            "db": {
                "host": "fb",
                "name": "fb",
                "password": "",
                "port": 5432,
                "user": "fb"
            }
        },
        "proxy_enable": true,
        "queues": [
            "mq",
            "smpp"
        ],
        "sensor": {
            "host": "localhost"
        },
        "sqlmap": {
            "block": false,
            "enabled": true,
            "threshold": 5
        },
        "syslog": {
            "enabled": true,
            "target": "127.0.0.1"
        },
        "tasks": {
            "analyzer": {
                "enabled": true,
                "log_max_age": 7,
                "log_max_size": 100,
                "log_retention": 2,
                "update_interval": 15
            }
        },
        "timesync": {
            "enabled": true,
```

```
            "url": "http://127.0.0.1/timesync"
        },
        "trustar": {
            "enabled": true,
            "key": "...",
            "url": "https://... "
        },
        "versatile": {
            "cache_size": 100,
            "enabled": false,
            "log_max_age": 7,
            "log_max_size": 1000,
            "log_retention": 2,
            "target": "127.0.0.1"
        },
        "watchdog": {
            "enabled": true,
            "interval": 60,
            "retry_attempts": 3,
            "timeout": 300
        },
        "zonefile": {
            "db": {
                "host": "localhost",
                "name": "db",
                "password": "",
                "port": 5432,
                "user": "zonefile"
            }
        }
    }
}
```


5.3.6 Сервер времени

По умолчанию каждый сенсор синхронизирует время с MXDR Console, но это поведение можно изменить, указав произвольный NTP-сервер. Для того чтобы добавить новый произвольный NTP-сервер, необходимо нажать на кнопку Добавить запись и внести адрес NTP-сервера в формате FQDN или сетевой IP-адрес.



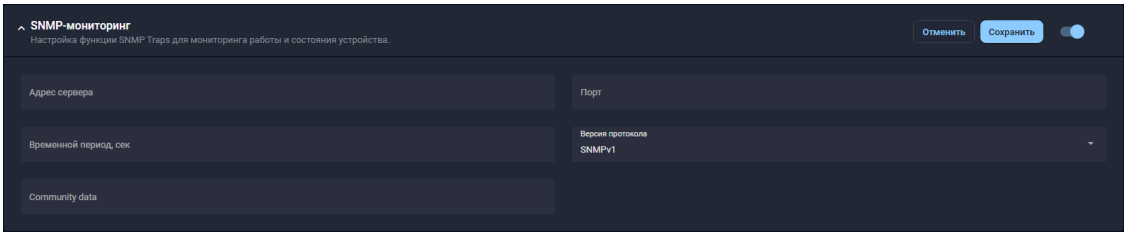
5.3.7 SNMP-мониторинг

Настройка позволяет обеспечивать мониторинг состояния оборудования, а также мониторинг статистических данных используемых модулей в MXDR. Поддерживаемые версии протокола SNMP:

- SNMPv1
- SNMPv2
- SNMPv3

При выборе версии протокола появляется возможность задать дополнительные параметры – специфичные для выбранного протокола.

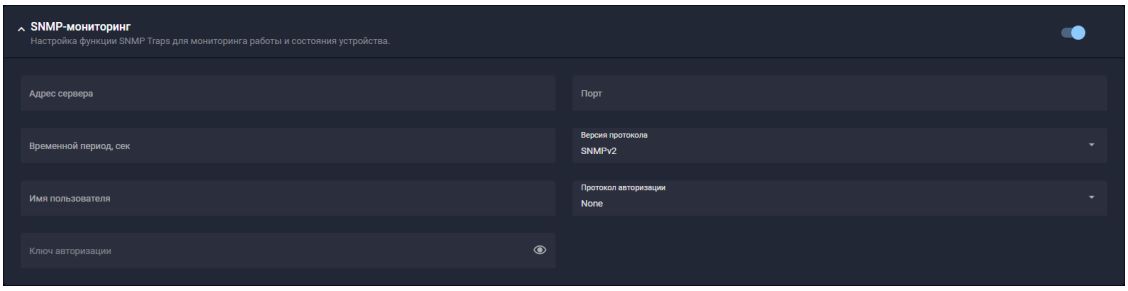
5.3.8 SNMPv1



Доступные настройки:

- Адрес сервера
- Порт
- Community Data

5.3.9 SNMPv2



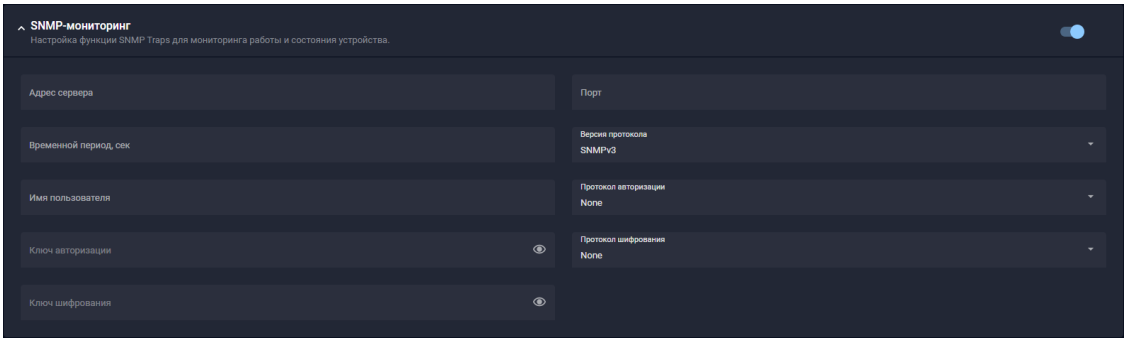
Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
  - MD5

- SHA
- SHA224
- SHA256
- SHA384
- SHA512

- Ключ авторизации

5.3.10 SNMPv3



Доступные настройки:

- Адрес сервера
- Порт
- Имя пользователя
- Протокол авторизации:
  - MD5
  - SHA
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Ключ авторизации
- Протокол шифрования:
  - DES
  - 3DES
  - AES128
  - AES192

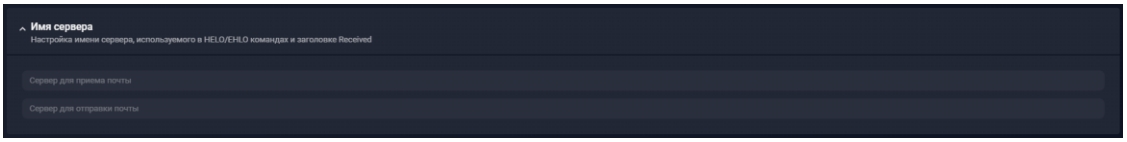
- AES256
- Ключ шифрования

5.4 Почта Network Traffic Analysis

Данный блок содержит в себе набор функций, позволяющих настраивать работу сервиса проверки писем **BEP**, поставляемого вместе с решением **NTA**.

5.4.1 Имя сервера

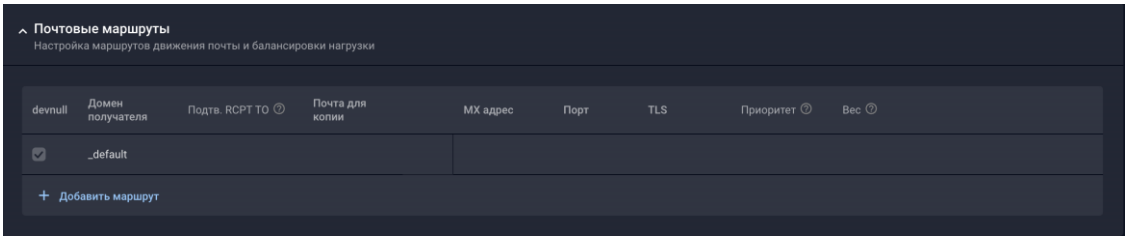
В данном блоке настроек можно указать имя/домен своей компании с целью снизить риск компрометации факта использования средств защиты почты.



- В поле **Сервер** для приема почты указываются данные, которыми **NTA** представляется при приёме почты. Это имя пишется в приветственном баннере при SMTP-подключении и оно же указывается в заголовке Received. По-умолчанию в данном поле указан UUID модуля **NTA**, используемого для анализа входящей почты.
- В поле **Сервер** для отправки почты указываются данные, которыми **NTA** представляемся при отправке почты. Это имя передаётся в команде HELO во время отправки. В данном поле можно указать любое имя/домен. Например: mydomain.ru

5.4.2 Почтовые маршруты

Настройки **NTA** позволяют задавать маршруты, по которым будет отправляться проверенная модулями XDR входящая почта. По умолчанию в качестве домена получателя указано значение `_default` и параметр `devnull`. В этом случае **NTA** будет работать в *режиме приема копии писем по протоколу SMTP*, то есть проверенная почта **не будет** отправляться далее по маршруту.



Для корректного анализа писем необходимо указывать каждый защищаемый домен (**Домен получателя**) и соответствующий ему маршрут. Для создания маршрута нажмите кнопку **Добавить маршрут** и укажите необходимые параметры:

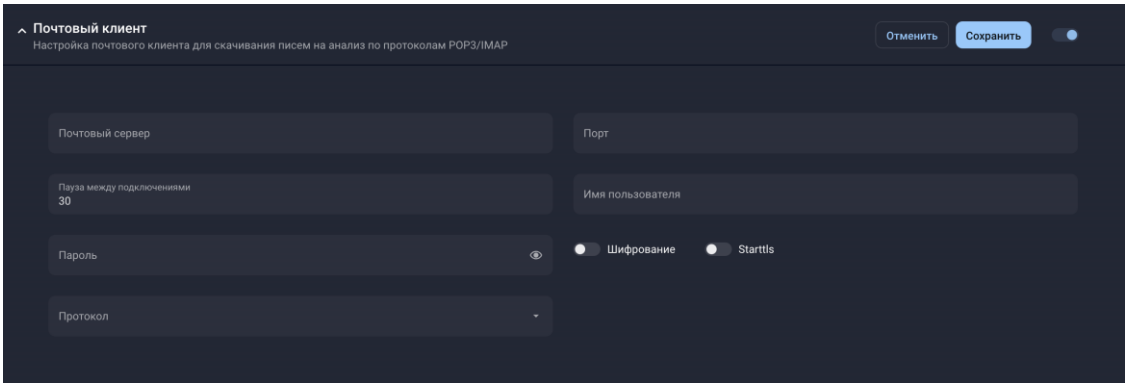
Параметр	Значение
devnull	Включает режим анализа почты, полученной через скрытую копию (*BCC*) по протоколу *SMTP*.
Домен получателя	Имя почтового домена, для которого настраивается новый маршрут.
Подтв. RCPT TO	Подтверждать адрес получателей у MX-сервера и отклонять сообщения к неизвестным получателям.
Почта для копии	Почтовый адрес, на который можно отправлять копии получаемых писем.
MX адрес	Адрес сервера, на который будет отправляться почта после проверки.
Порт	Порт принимающего сервера, на котором работает запущенный сервис по получению писем.
TLS	Варианты шифрования принимающего почтового сервера
Приоритет	Приоритет использования сервера. В случае необходимости выбора сервера для отправки предпочтение отдается серверам с меньшим приоритетом.
Вес	Значение используется для балансировки потока писем между несколькими серверами с *одинаковым* приоритетом. Серверы с большим весом будут получать пропорционально большую нагрузку.

При включении опции **Подтв. RCPT TO** необходимо убедиться, что принимающий сервер поддерживает функцию предоставления списка получателей.

5.4.3 Почтовый клиент

Настройка почтового клиента позволяет **NTA** подключаться к почтовым серверам, хранящим клиентские письма и анализировать содержимое указанного почтового ящика.

NTA подключается только к одному ящику почтового сервера – на данный ящик необходимо направлять копии почтовых сообщений для анализа (Организуется через внутренние BCC функции почтовых серверов или почтовых сервисов).



Параметр	Значение
Почтовый сервер	FQDN или сетевой адрес почтового сервера, к которому будет подключаться **NTA** по протоколу POP3/IMAP.
Порт	Порт подключения к почтовому серверу.
Пауза между подключениями	Таймаут между подключением к почтовому ящику для скачивания почтовых сообщений. По умолчанию **NTA** запрашивает у почтового сервера первые 100 доступных сообщений (вне зависимости от выбранного протокола). Таким образом, если почтовый сервер не корректно обрабатывает команды на удаление от сенсора, возникнет бесконечный цикл.
Имя пользователя	Логин от почтового ящика, на котором агрегируются копии почтовых сообщений для анализа.
Пароль	Пароль от почтового ящика.
Протокол	POP3 / IMAP
Шифрование	Поддерживаемые версии протоколов шифрования SSLv2, SSLv3, TLS, TLSv1, TLSv1.1, TLSv1.2. За дополнительной информацией по поддержке протоколов со стороны клиента обращайтесь к ответственному менеджеру.
Starttls	Опция включает использование шифрования при обмене сообщениями по POP3/IMAP протоколу.

5.4.3.1 Поддерживаемые протоколы

Протокол	Особенности работы
POP3	При использовании данного протокола, вся проанализированная почта будет автоматически удаляется сенсором после скачивания сообщений из ящика. Почта удаляется безвозвратно, только при наличии достаточных прав у используемого сенсором аккаунта.

Протокол	Особенности работы
IMAP	При использовании протокола применяются стандартные команды на удаление скаченных из сообщений почтового ящика.

5.4.3.2 Папки

Доступно при выборе протокола `IMAP`.

Параметр позволяет задать имя папки в подключаемом почтовом ящике для скачивания сообщений.

5.4.3.3 Прокси сервер для обработки ссылок

Если для выхода в Интернет в организации используется прокси-сервер, укажите его в формате `http://proxy-server-address:port`. Это необходимо для проверки ссылок сервисами **NTA**. Если прокси сервер не используется, оставьте поле пустым.

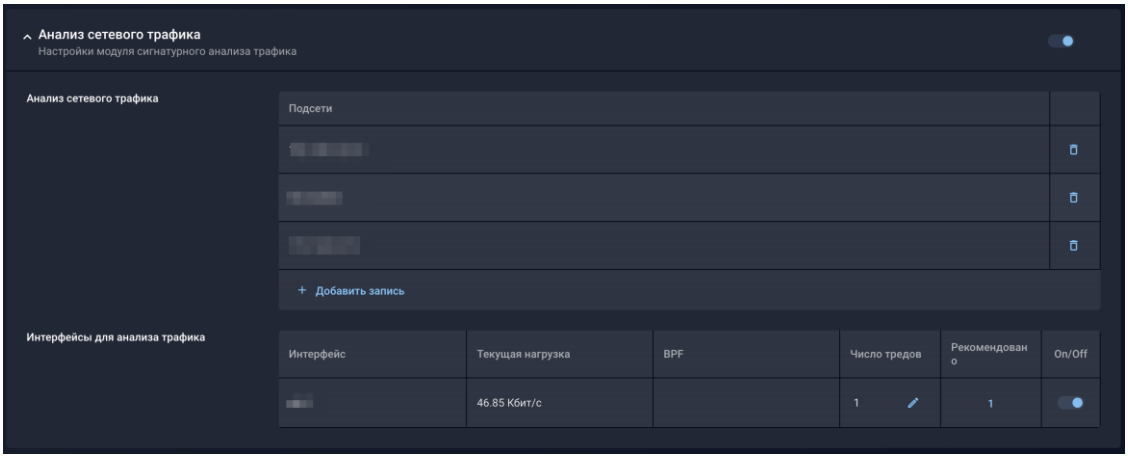
Для использования локального MXDR Console в качестве прокси-сервера, укажите: `http://command-server.tds:3128`.

5.5 Сетевой трафик Network Traffic Analysis

Данный блок содержит в себе набор функций, позволяющих: собирать метаинформацию о сетевых соединениях по протоколам уровня L7; анализировать web-трафик, получаемый от прокси-серверов компании через ICAP; настраивать модуль сигнатурного анализа трафика; управлять загружаемыми файлами с сигнатурами на сетевой трафик; загружать специфичные для Network Traffic Analysis правила анализа сетевого трафика.

5.5.1 Анализ сетевого трафика NTA

Важный раздел при настройке сигнатурного анализа. Настройки раздела позволяют системе дифференцировать зловредный трафик относительно легитимного. Позволяет указать локальные интерфейсы, а также интерфейсы для SPAN/RSAN/SPANinGRE. Разделён на два подраздела.



5.5.1.1 Анализ сетевого трафика

Позволяет явно указать локальные адреса, сети/подсети, а также адреса локальных Proxy. Данный список определяет так называемую домашнюю сеть (Homenet) для сигнатурного анализа трафика. Выбор Homenet важен для группировки событий по подразделениям.

Введите список локальных подсетей и исключите из них адреса Proxy-серверов (используйте знак отрицания. >Пример:`!proxy-ip/32`

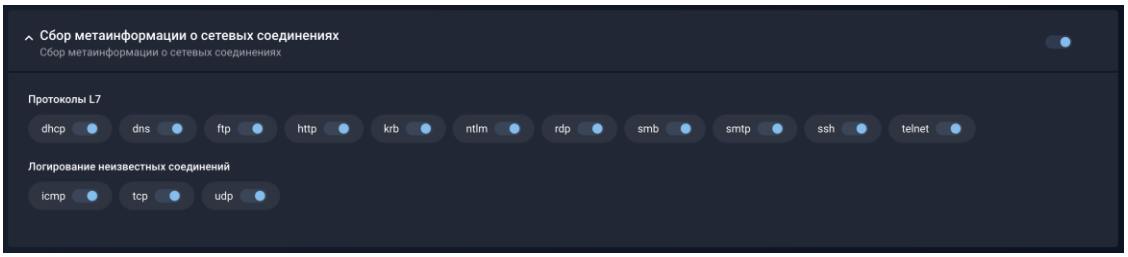
Это позволит различать взаимодействия целевых хостов, сетей/подсетей с открытой сетью Интернет.

5.5.1.2 Интерфейсы для анализа трафика

Параметр	Описание
Интерфейс	Имена интерфейсов
Текущая нагрузка	Это поток трафика, который подается на конкретный интерфейс – без учёта того анализируется данный трафик или нет.
BPF	Фильтр BPF для анализа трафика по сигнатурным правилам
On/Off	Toggle switch enabling/disabling an interface
Число тредов	Установленное число потоков для каждого процесса сигнатурного анализа SPAN трафика на выбранном интерфейсе. (*по умолчанию задано рекомендуемое значение. Изменение значения может повлиять на производительность системы!*))

5.5.2 Сбор метаинформации о сетевых соединениях

Для обеспечения безопасности работы коммерческих сетей необходимо осуществлять контроль данных, передаваемых посредством протоколов передачи данных. Изначально переключатель для каждого модуля включен.



5.5.2.1 Протоколы L7

При включении L7 протокола система будет производить запись метаинформации о сессиях с использованием данного протокола. Таким образом можно восстанавливать данные сессии, анализировать и ассоциировать их с файлами, передаваемыми в данных сессиях.

5.5.2.2 Логирование неизвестных соединений

Для логирования сессий с использованием нестандартных портов и протоколов необходимо активировать требуемые протоколы UDP, TCP или ICMP. Таким образом, все сессии не подпадающие под стандартно используемые протоколы седьмого уровня модели OSI будут логироваться и размещаться в разделе `Сетевые соединения`.

5.5.3 ICAP сервер

Network Traffic Analysis может взаимодействовать по протоколу ICAP в качестве сервера с сетевым оборудованием, поддерживающим данный протокол в качестве клиента. Например: Web Proxy, UTM, NGFW, и т.п. При таком взаимодействии ICAP сервер в пассивном режиме ожидает подключение клиентов. ICAP-клиент передает файлы для проведения поведенческого анализа с ожиданием вердикта, либо без ожидания (в зависимости от настройки блокировки). Доступные настройки:

5.5.3.1 TCP-порт

Порт для подключения ICAP-клиентов. На данном порту будет работать сервис ICAP-сервера.

5.5.3.2 Блокировать скачиваемые вредоносные файлы

Позволяет активировать режим блокировки для ICAP-клиентов. В данном режиме ICAP-клиенты ожидают от Network Traffic Analysis ответа по вердикту для файла по итогам

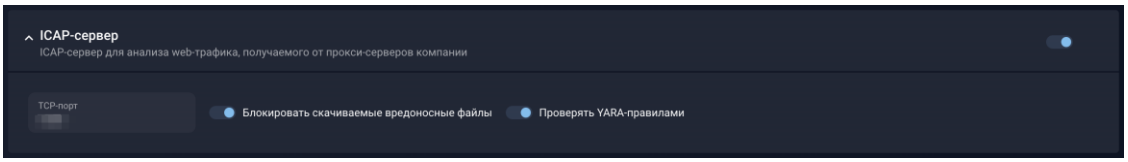
поведенческого анализа на Malware Detonation Platform. В случае, если файл вредоносный, Network Traffic Analysis присылает ICAP-клиенту команду на блокировку проанализированного файла.

Примечание: в случае получения от ICAP-клиентов архивов или зашифрованных архивов, Network Traffic Analysis разархивирует или попытается разархивировать шифрованный архив произведя подбор пароля по встроенному словарю. Дальнейший анализ будет производиться штатно.

5.5.3.3 Проверять YARA-правилами

Позволяет включать механизм проверки YARA-правил.

Примечание: использование YARA правил позволяет отвечать на запросы ICAP клиентов, не дожидаясь результатов анализа файлов от Malware Detonation Platform, а также не зависеть от данных результатов. То есть возможно реализовать блокировку сессии передачи файловых объектов без поведенческого вердикта.



5.5.4 Хранилище дампов сетевого трафика

Данная настройка предназначена для сбора и сохранения дампов сетевого трафика.

5.5.4.1 Папка

В данном разделе Пользователь может выбрать папку для сохранения сетевого трафика и указать путь до нее, или создать новую.

1. В поле **Папка** выберите нужный ресурс, в который будет сохраняться трафик.
2. В поле **Путь** укажите расположение папки.
3. В поле **Период хранения** из ниспадающего списка выберите срок хранения дампов сетевого трафика в папке (по умолчанию указано 14 дней).

5.5.4.2 Сетевой интерфейс

В данном разделе Пользователь может выбрать интерфейс для анализа трафика и указать ограничение времени обновления.

1. В поле Интерфейс выберите один из интерфейсов для анализа сетевого трафика. Добавить интерфейс можно в настройке Анализ сетевого трафика раздел Сетевой трафик.

2. В поле Ограничение времени обновления из ниспадающего списка выберите период времени, который является длительностью сбора данных для одного файла дампа сетевого трафика (по умолчанию 60 секунд). После этого сетевой трафик собирается в другой файл.

5.5.5 Сетевые сигнатуры

В настройке представлен список подклассов сигнатур, с возможностью выборочного отключения или включения определенных подклассов.

Примечание: Включение новых правил, как и загрузка новых пользовательских правил анализа трафика, может приводить к снижению работоспособности устройства. Меняя перечень активных правил и загружая новые пользовательские правила, всегда взвешивайте работоспособность устройства в части параметра “Дропы в ядре”. Сенсоры протестированы на поддержку номинальной полосы пропускания только при условии использования конфига по умолчанию.

В таблице приведено краткое описание возможных сигнатур.

Сигнатура	Описание
Целевые атаки	Кибератаки, направленные на компрометацию информационной системы конкретной компании, организации или государственной службы. Целевая атака хорошо спланирована и включает несколько этапов, сочетая в себе комбинацию методов: социальной инженерии, эксплуатации уязвимостей, применения ВПО и т.д. Как правило проводится преступными группами – APT-группировками, которые обладают значительными техническими возможностями и финансовыми ресурсами
Уязвимости в серверном ПО	Уязвимости, которые заставляют веб-приложение работать неожиданным или непредсказуемым образом. Могут привести к утечке личных данных, несанкционированному доступу к базе данных сервера, а также к другим файлам таким же образом, как и уполномоченные администраторы сервера
Уязвимости прикладного ПО	Ошибки разработчиков программного обеспечения, позволяющие

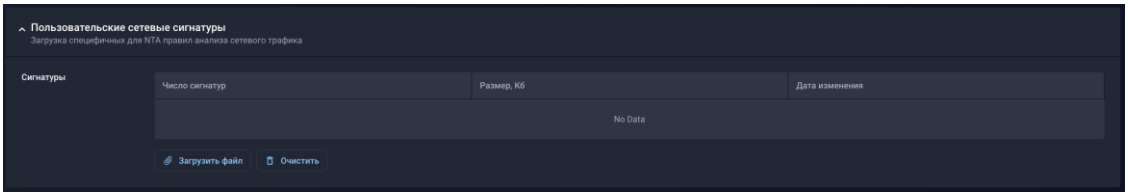
Сигнатура	Описание
	злоумышленнику получить несанкционированный доступ к функциональности программы, нарушить ее работоспособность или иным путем поставить под угрозу конфиденциальность, целостность, доступность обрабатываемой информации
Бэкдоры и нелегальные средства удаленного управления	Класс вредоносного программного обеспечения, которое предоставляет возможность удаленного управления компьютером жертвы. В отличие от обычных утилит удаленного администрирования, трояны этого типа устанавливаются, запускаются и работают незаметно для пользователя. После установки бэкдоры могут получать команду на отправку, прием, исполнение и удаление файлов, сбор конфиденциальных данных, информации о действиях пользователя и многое другое
Банковские трояны	Банковские трояны или «банкеры» – вредоносные программы, созданные для кражи денег через онлайн-банкинг. Подменяя страницу официальных банковских приложений, крупных онлайн-магазинов, программа похищает логины и пароли, а также данные банковских карт. Для обхода двухфакторной аутентификации программа способна перехватывать отправленные банком смс-сообщения и перенаправлять их
Мобильные трояны	Предназначенное для вмешательства в работу мобильного телефона ВПО, которое записывает, повреждает или удаляет данные и распространяется на другие устройства через SMS и Интернет. Основной целью мобильных троянов является получение персональной информации для продажи или использования в личных нуждах злоумышленником
Неспецифичная активность троянов	Троян - вредоносное программное обеспечение, проникающее в систему под видом легитимной программы. Существует множество видов, которые отличаются функциональностью, однако в общем случае к неспецифичной активности троянов относится: сбор информации об устройстве и его владельце, использование, удаление или

Сигнатура	Описание
	злонамеренное изменение хранящихся на компьютере данных
Drive-by атаки	Drive-by атака — привычный метод распространения вредоносного ПО. Злоумышленники ищут незащищенные сайты и внедряют вредоносные скрипты в их HTTP- или PHP-код. Этот скрипт может установить вредоносное ПО напрямую на компьютер пользователя, посетившего сайт или создать IFRAME-форму, которая перенаправит жертву на сайт, контролируемый злоумышленниками. Для успеха атаки жертве не нужно выполнять никаких действий: достаточно посетить зараженный ресурс
Подозрительные события	Вид событий, которые не классифицируются как вредоносные, однако могут сведетельствовать о причинении вреда пользователям
Фишинговые ресурсы	Ресурсы целью которых является хищение конфиденциальных данных пользователя (логины, пароли, данные банковских карт и др.). Обычно фишинговые сайты — это копии известных платформ, которые очень сложно отличить от оригинала, поскольку они полностью копируют дизайн, а в некоторых случаях и функциональность
Нарушение политик	Нарушение норм, правил, организационно-распорядительных актов компании, на которых строится управление и защита информации. Примерами нарушений политики являются: оставленный без присмотра компьютер, открытие e-mail от незнакомцев, простые пароли, сокрытие фактов нарушения информационной безопасности
Нежелательное ПО	Категория программного обеспечения, задачей которого не является однозначно вредоносная деятельность. Однако при этом возможна установка дополнительного нежелательного программного обеспечения, изменение рабочих процессов цифрового устройства, а также выполнение действий без запроса или разрешения пользователя
Троян-вымогатель	Вредоносное программное обеспечение, предназначенное для вымогательства, блокирует доступ к компьютерной системе или предотвращает считывание записанных на нём данных (часто с помощью методов шифрования), а затем требует от жертвы

Сигнатура	Описание
	выкуп для восстановления исходного состояния
Исследование сетевого периметра	Процесс сбора общей информации о компьютерной сети компании, такой как структура сети, активные хосты, службы и приложения
Шпионское ПО	Тип вредоносного ПО, присутствие которого в системе часто не поддается обнаружению. Как правило программы-шпионы не имеют каких-либо выраженных вредоносных функций для устройства жертвы, они собирают информацию о пользователе или же его конфиденциальные данные и без ведома пересылают собранную информацию на удаленные серверы, принадлежащие злоумышленникам

5.5.6 Пользовательские сетевые сигнатуры

Данная настройка позволяет загружать собственные сигнатур в формате Suricata в систему.



Примечание: ID загружаемых пользовательских сигнатур должны быть в пределах 1300001 — 1500000. Иначе система не позволит их использовать и отбросит.

5.6 Состояние устройства Network Traffic Analysis

Расположение: UI → **Настройки** → **Модули** → в списке устройств выбрать необходимый Network Traffic Analysis

На странице представлены общие показатели работоспособности подключенного Network Traffic Analysis. Данные по каждому Network Traffic Analysis доступны при раскрытии карты Network Traffic Analysis в списке подключённых устройств.

В списке устройств содержится краткая информация, которая включает в себя следующие параметры:

- **Версия** – версия ПО
- **Имя** – наименование устройства

- **Тип** – тип устройства – модуль MXDR (в данном случае Network Traffic Analysis)
- **Компания** – наименование компании, в которой находится данное устройство
- **Лицензия** – тип лицензии для данного устройства
- **Дата создания** – дата выдачи лицензии
- **Конец лицензии** – дата окончания срока действия лицензии

5.6.1 Общая информация

- **Имя** – заданный идентификатор может быть любым
- **Номер лицензии** – получен при покупке или тестировании решения
- **Серийный номер** – серийный номер оборудования
- **Комментарий**
- **VPN IP** – адрес внутри VPN туннеля получаемый при подключении Network Traffic Analysis к MXDR Console для управляющих коммуникаций
- **Внешний IP** – адрес управляющего интерфейса, выданный на стороне клиента (через DHCP или статическими правилами)
- **Компания** – задаются при создании нового устройства из списка Настройки → Компании

5.6.2 Состояние устройства

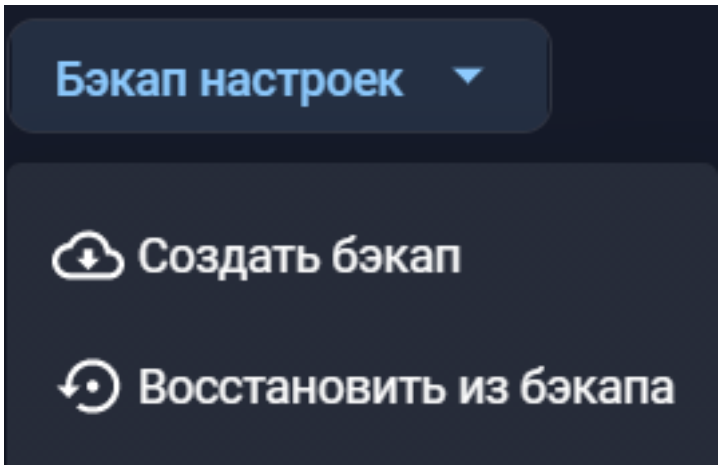
- **Последний HeartBeat** – последний замеченный heartbeat с данного устройства
- **Последнее обновление** – дата последнего обновления
- **CPU / RAM / HDD**
- **Дропы в ядре / на интерфейсе**
- **TCP Gaps / TCP Retransmissions / TCP Middlestreams** – сбор и интерфейсное отображение нескольких метрик, позволяющих определить некачественную интеграцию. В норме все три параметра должны быть около нуля; если же они не нулевые это указывает на недостатки в организации зеркалирования трафика
- **Последняя активность** – крайнее время активности VPN между NTA и управляющим MXDR Console
- **Длительность** – временной отрезок в течении которого между NTA и MXDR Console был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами
- **Загрузка канала**

5.6.3 Графики состояния устройства

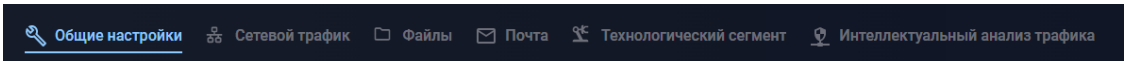
Предоставляют двумерный график на временном отрезке в 24 часа по следующим показателям:

- **Производительность** – задействованные ресурсы системы
  - CPU average (%)
  - RAM maximum (%)
  - HDD maximum (%)
- **SPAN** – средняя загрузка канала приёма копии трафика аккумулированная по всем SPAN интерфейсам NTA
- **MSP** – статистика по количеству принятых для анализа почтовых сообщений при наличии почтовой интеграции
  - **Envelopers** – статистика по принятым письмам
  - **Files** – статистика файлов, приложенных к данному количеству писем
  - **Malware Detonation Platform Queue** – размер очереди на Malware Detonation Platform к выбранному моменту времени
- **DROPS** – отбрасываемые пакеты на физическом интерфейсе приёма копии трафика Кнопка редактирования базовых свойств  – доступны для редактирования:
- **Имя**
- **Комментарий**
- **Скрыть от CERT** > **Примечание:** данная кнопка доступна только для пользователей с типом аккаунта *owner*.

Кнопка **Бэкап настроек** позволят как создавать резервную копию текущей версии настроек данного устройства, так и восстанавливать необходимую версию настроек из уже имеющихся резервных копий.



Кнопка **Основные настройки** открывает раздел конфигурации устройства, который разделен на следующие разделы:



При нажатии на кнопку **Управление лицензией** (позволяет изменить лицензию для выбранного устройства) происходит автоматический переход в раздел **Лицензии**.

5.7 Файлы Network Traffic Analysis

Данный блок содержит в себе набор функций, позволяющих: управлять анализом и извлечением файлов из трафика, а также настраивать общие ресурсы для сбора и анализа файлов.

1. Анализ файлов из трафика
2. Анализ общих ресурсов
3. Пользовательские YARA-правила Network Traffic Analysis

5.7.1 Анализ файлов из трафика

При активации данной настройки Network Traffic Analysis будет пытаться получать файлы из анализируемой копии трафика и отправлять их на поведенческий анализ. При подобном способе интеграции необходимо учитывать следующие моменты:

Дропы – если зеркалирующее устройство (с которого поступают SPAN сессии) будет дропать пакеты при формировании копии трафика, то высока вероятность невозможности собрать из SPAN сессий файлов или почтовых сообщений.

5.7.1.1 BPF для захвата трафика

BPF фильтр – это open-source проект позволяющий задавать фильтры извлечения данных из анализируемого трафика. Подробнее по ссылке http://biot.com/capstats/bpf.html. Фильтры действуют по принципу *whitelist* списка.

5.7.1.2 Протоколы

Переключатели активируют предустановленные BPF фильтры для анализа файлов из указанных протоколов.

5.7.1.2.1 SMTP/POP3

Данный переключатель активирует функциональность по анализу почтовых сообщений в отсутствие возможности полноценной почтовой интеграции.

При реализации полноценной почтовой интеграции данную функцию необходимо отключить.

5.7.1.2.2 HTTP

Восстанавливает из SPAN сессий файлы, передаваемые протоколом http (обычно при скачивании из сети Интернет).

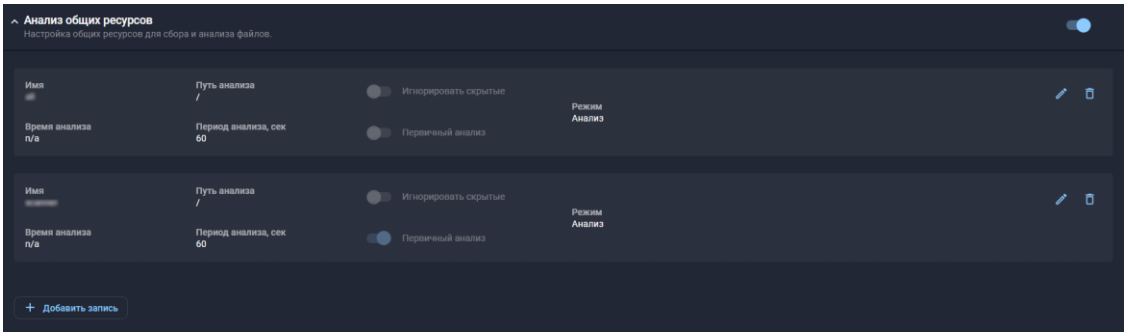
5.7.1.2.3 FTP/SMB

Восстанавливает из SPAN сессий файлы, передаваемые при работе с файловыми хранилищами.

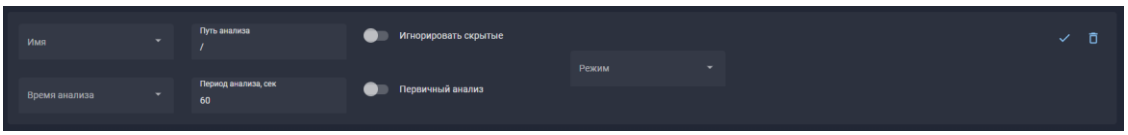
5.7.2 Анализ общих ресурсов

Расположение: UI > **Настройки** > **Модули** > в списке устройств выбрать необходимый **Network Traffic Analysis** и нажать **Основные настройки** > блок **Файлы** > **Анализ общих ресурсов**.

В разделе **Анализ общих ресурсов** осуществляется настройка режима обработки заранее подключенных в разделе Монтирование общих ресурсов файловых ресурсов для сбора и анализа файлов.



Чтобы начать анализ ресурсов, необходимо нажать на кнопку **Добавить ресурс** и заполнить следующие поля:



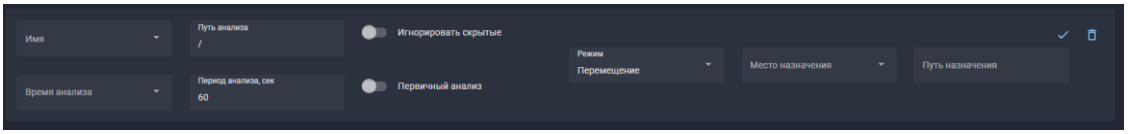
- **Имя** – наименование ресурса из списка смонтированных.
- **Путь анализа** – указываем путь относительно указанного в разделе “Монтирование общих ресурсов” (путь до дополнительного элемента в папке).
- **Время анализа** – временная метка создания или модификации файла, начиная с которой будет производиться анализ.
- **Период анализа** – периодичность, с которой производится проверка ресурса на появление новых файлов.

- **Игнорировать скрытые** – не проверять скрытые файлы
- **Первичный анализ** – проверить все существующие на момент включения анализа файлы.
- **Режим** – режим работы:
  - **Анализ** – режим мониторинга, при котором только выдаётся алерт на вредоносный файл. Файл остаётся в папке неизменным.
  - **Удаление** – режим мониторинга, при котором выдаётся алерт на вредоносный файл. Вредоносный файл удаляется из папки.
  - **Перемещение** – режим работы с двумя папками, при котором выдаётся алерт на вредоносный файл. Вредоносные файлы остаются в исходной папке. Проверенные безопасные файлы перемещаются в указанную папку назначения.

В режиме **Удаление** для типа ресурса NFS, со стороны NFS-сервера требуются следующие настройки: `(rw,async,no_subtree_check,all_squash,anonuid={UID},anongid={GID})` В качестве идентификатора пользователя и группы - указать UID и GID пользователя, которому принадлежат NFS-ресурсы на NFS-сервере.

При выборе режима работы **Перемещение** будут доступны следующие поля:

- **Место назначения** — наименование папки, созданной в разделе Монтирование общих ресурсов, в которую будут перемещаться проанализированные безопасные файлы.
- **Путь назначения** — относительный путь внутри папки, в которую будут перемещаться проанализированные безопасные файлы.



После того, как все необходимые параметры заданы, нажмите кнопку **Сохранить**.

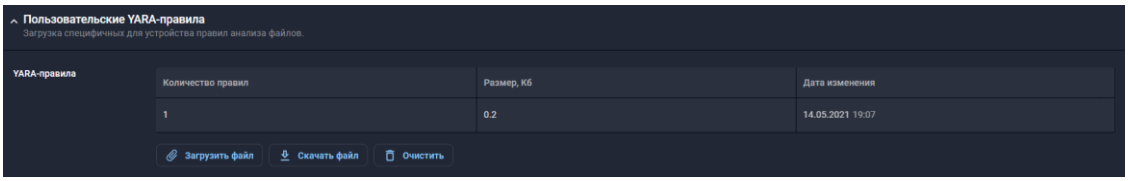
5.7.3 Пользовательские YARA-правила

В данном разделе настроек **NTA** Пользовать может добавлять собственные YARA-правила.

Данные правила влияют на файловые объекты проходящие через Network Traffic Analysis (например ICAP, SPAN, файловые хранилища и т.п.). С помощью них возможно

задать реакции на объекты не дожидаясь поведенческого анализа от Malware Detonation Platform и / или иметь независимую реакцию от результатов анализа.

Внимание: не путайте с YARA-правилами на Malware Detonation Platform. Учитывайте коллизии данных правил между разными типами устройств!

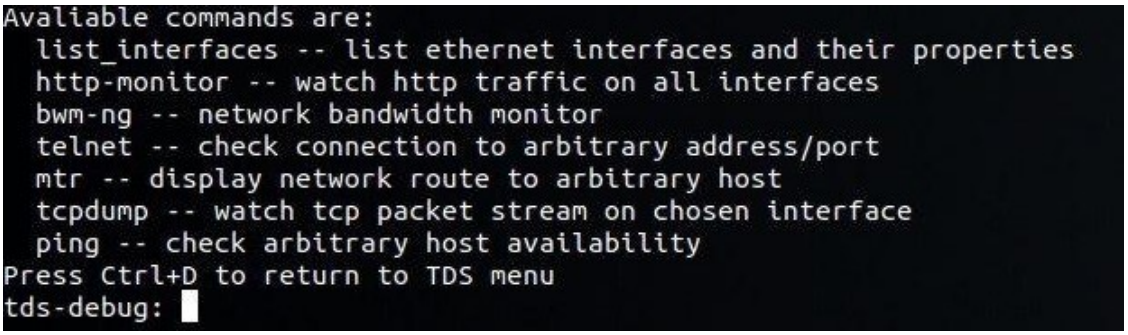


Нажмите **Загрузить файл**, чтобы прикрепить сформированный ранее файл из своего устройства.

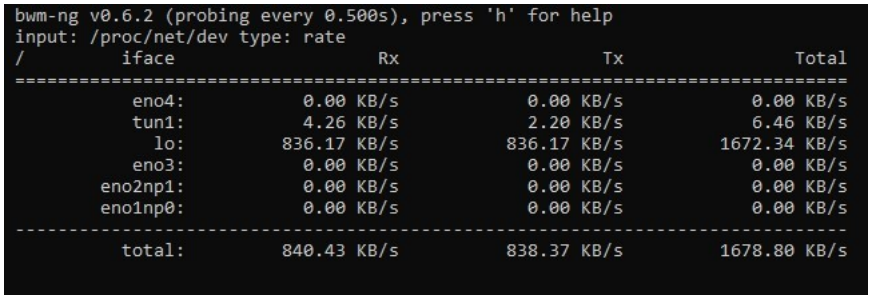
Нажмите **Очистить**, чтобы удалить лишние / устаревшие файлы.

5.8 Управление модулем NTA через Debug Shell

Debug Shell предоставляет низкоуровневые инструменты для анализа сетевого подключения и анализа состояния устройства.



Инструмент	Описание
list_interfaces	Список интерфейсов с обозначением работающих и отключенных интерфейсов с обозначаем управляющего.
http-monitor	Показывает http сессии, выявленные в SPAN трафике.
bwm-ng	Монитор загруженности интерфейсов в реальном времени. Для открытия страницы помощи нажмите h.
telnet	Стандартная утилита проверки telnet соединения.
mtr	Трассировка сети.
tcpdump	Стандартная утилита снятия дампа трафика.
ping	Стандартная утилита ping.


bwm-ng v0.6.2 (probing every 0.500s), press 'h' for help
input: /proc/net/dev type: rate
/ iface Rx Tx Total
eno4: 0.00 KB/s 0.00 KB/s 0.00 KB/s
tun1: 4.26 KB/s 2.20 KB/s 6.46 KB/s
lo: 836.17 KB/s 836.17 KB/s 1672.34 KB/s
eno3: 0.00 KB/s 0.00 KB/s 0.00 KB/s
eno2np1: 0.00 KB/s 0.00 KB/s 0.00 KB/s
eno1np0: 0.00 KB/s 0.00 KB/s 0.00 KB/s
total: 840.43 KB/s 838.37 KB/s 1678.80 KB/s

6 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка осуществляется в соответствии с условиями контракта следующими способами:

- Приоритетный способ осуществления техподдержки через создание запросов во вкладке «Поддержка» по ссылке https://xdr.f6.security/service-desk
- по электронной почте: info@f6.ru;
- по номеру телефона: +7 495 984-33-64;

В рамках технической поддержки оказываются следующие услуги:

- консультация по фактическому наличию имеющегося функционала в системе;
- помощь в настройке и интеграции ПО;
- помощь в эксплуатации ПО;
- решение технических проблем;
- пояснение принципов работы имеющихся механизмов ПО;
- поиск, тестирование и фиксирование найденных ошибок;
- предоставление актуальной документации по настройке, эксплуатации и работе ПО.

Время работы технической поддержки: с понедельника по пятницу с 9:00 до 18:00 UTC+3.

Фактический адрес размещения службы поддержки ПО «Network Traffic Analysis»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1