ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Malware Detonation Platform»

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 Malware Detonation Platform, MDP.
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 Malware Detonation Platform». В случае недоступности указанных систем формат взаимодействия осуществляется через электронный почтовый ящик.
CV	Computer vision
MXDR	Программное обеспечение «F6 XDR»
BEP	Программное обеспечение «F6 Business Email Protection»
EDR	Программное обеспечение «F6 Endpoint Detection and Response»
NTA	Программное обеспечение «F6 Network Traffic Analysis»
SMPT	Simple Mail Transfer Protocol

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ является руководством администратора ПО «F6 Malware Detonation Platform» (далее – ПО, Malware Detonation Platform, MDP).Также документ включает в себя руководство по установке ПО.

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

1.2 Назначение ПО

«F6 Malware Detonation Platform» представляет собой специализированное решение для анализа вредоносного программного обеспечения, которое запускает подозрительные файлы в изолированной среде (песочнице), чтобы безопасно изучить их поведение (поведенческий анализ). ПО позволяет детально отслеживать взаимодействие вредоносного ПО с операционной системой, реестром, файлами и сетевыми ресурсами, предоставляя полную картину его активности без риска заражения реальной информационной инфраструктуры. ПО не только анализирует простые вредоносные файлы, но и помогает выявлять эксплойты — программы, использующие уязвимости систем для выполнения атак. Платформа поддерживает различные типы файлов для анализа, включая исполняемые файлы, документы и скрипты.

2 ТРЕБОВАНИЯ К СИСТЕМЕ

ПО может быть установлено только на физический сервер.

2.1 Минимальные технические требования для физического сервера

Ниже приведены минимальные технические требования к физическому серверу в зависимости от типа Malware Detonation Platform - **Standard** или **Enterprise**.

Параметр	**Standard**	**Enterprise**
Процессор(ы)	Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M Cache, Turbo 3,6GHz, HT (185W) DDR4-3200	2 x Intel Xeon Gold 6336Y 2.4GHz, 24C/48T, 11.2GT/s, 36M Cache, Turbo 3,6GHz, HT (185W) DDR4-3200
Объем оперативной памяти	128 GB	256 GB
Объем хранилища	2 x 960 GB SSD, SATA 6 Gb/s, Mixed Use, Random write 44500 IOPS RAID1	2 x 960 GB SSD, SATA 6Gb/s, Mixed Use, Random write 44500 IOPS RAID1
Сетевой интерфейс	1 Ethernet port	1 Ethernet port

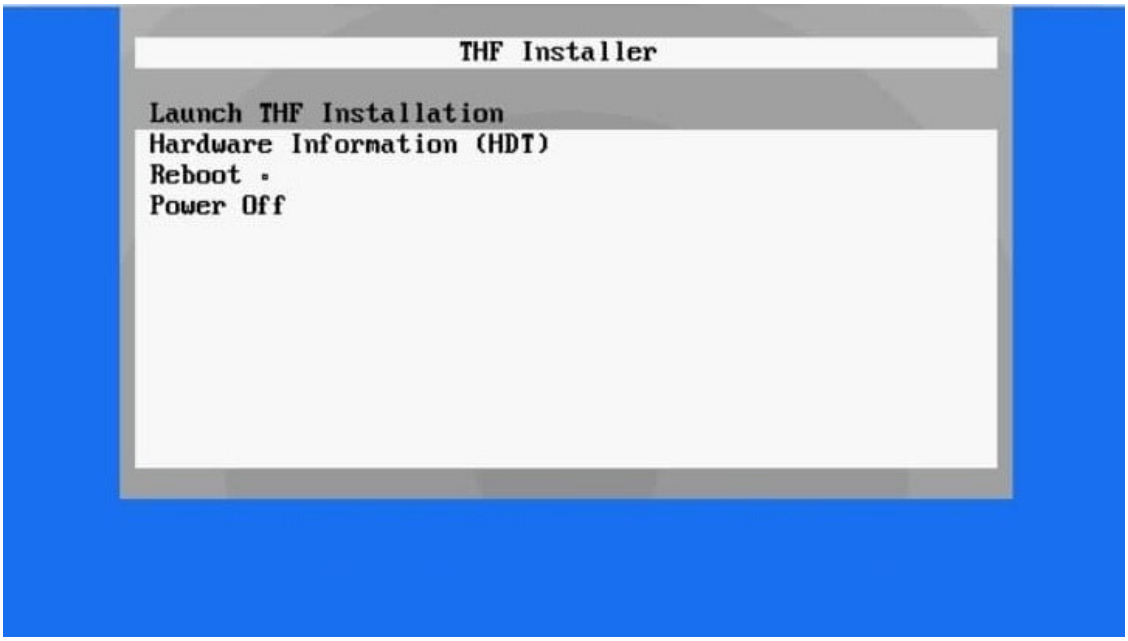
3 УСТАНОВКА ТЕСТОВОЙ ВЕРСИИ ПО

Программное обеспечение Malware Detonation Platform может быть установлено только на физический сервер.

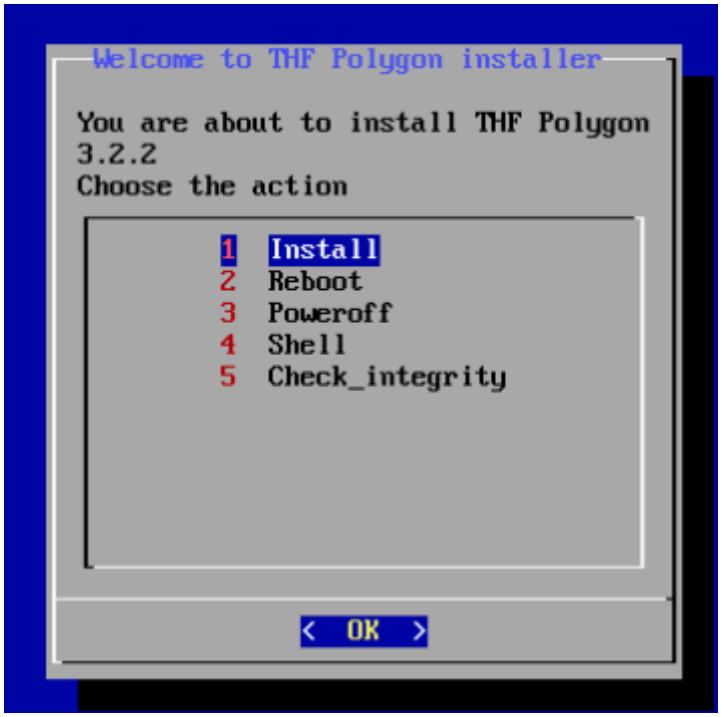
3.1 Технические требования для установки

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 Malware Detonation Platform. Здесь же можно просмотреть информацию об аппаратном обеспечении, перезапустить/выключить сервер.



В появившемся окне `MXDR Installer` выберите `Install`.



Появится окно с предложением выбрать язык отображения лицензионного соглашения.

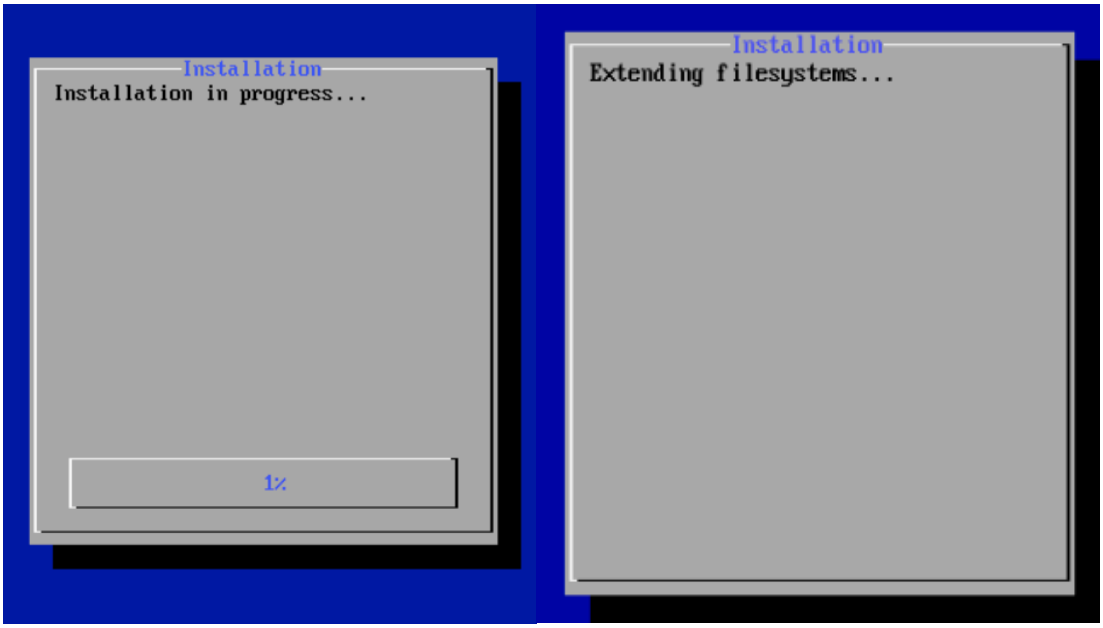
Чтобы ознакомиться с текстом лицензионного соглашения используйте клавиши Page Up и Page Down.

Необходимо выбрать устройство, на котором будет установлено ПО Malware Detonation Platform:

`/dev/sdb` — установочная флешка

`/dev/sda` — диск для установки MDP

Начнется установка MDP.



В конце установки вам будет предложено перезагрузить сервер.

Если все прошло успешно, откроется окно с приветственным экраном Malware Detonation Platform.

3.2 Консоль Malware Detonation Platform

3.2.1 Подключение к консоли MDPlink

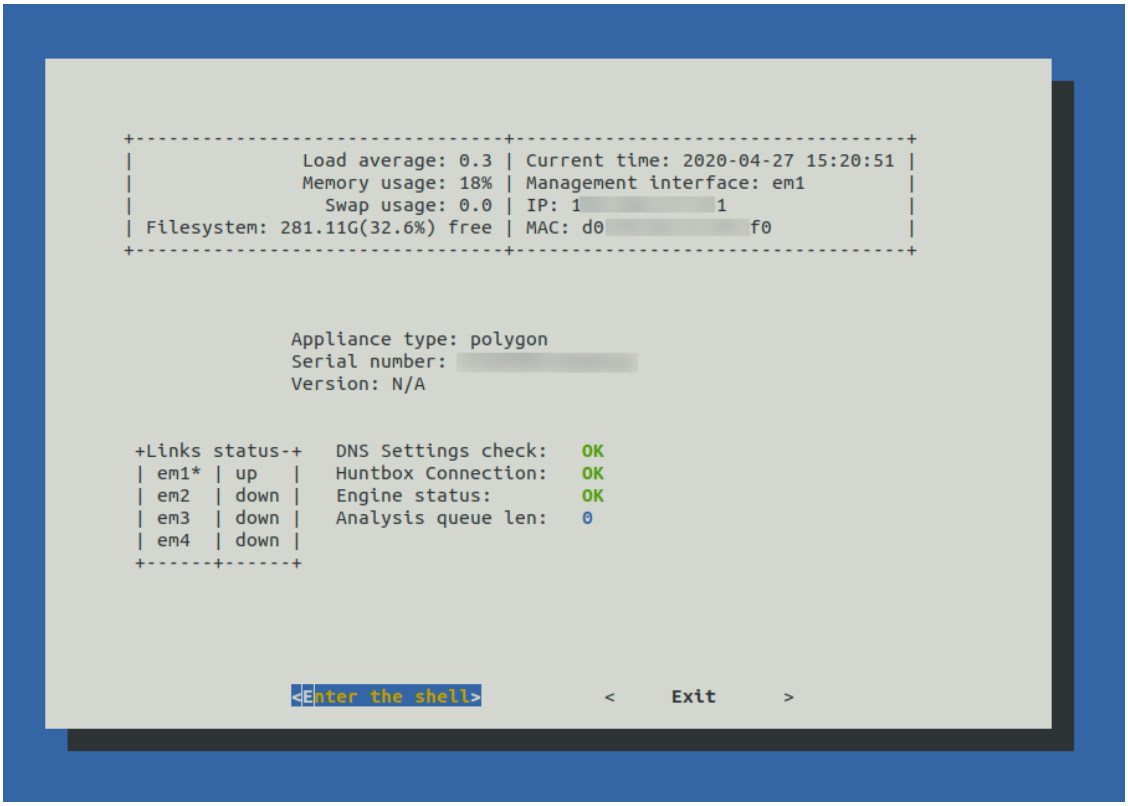
Доступ к консоли Malware Detonation Platform можно получить любым из нижеперечисленных способов:

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

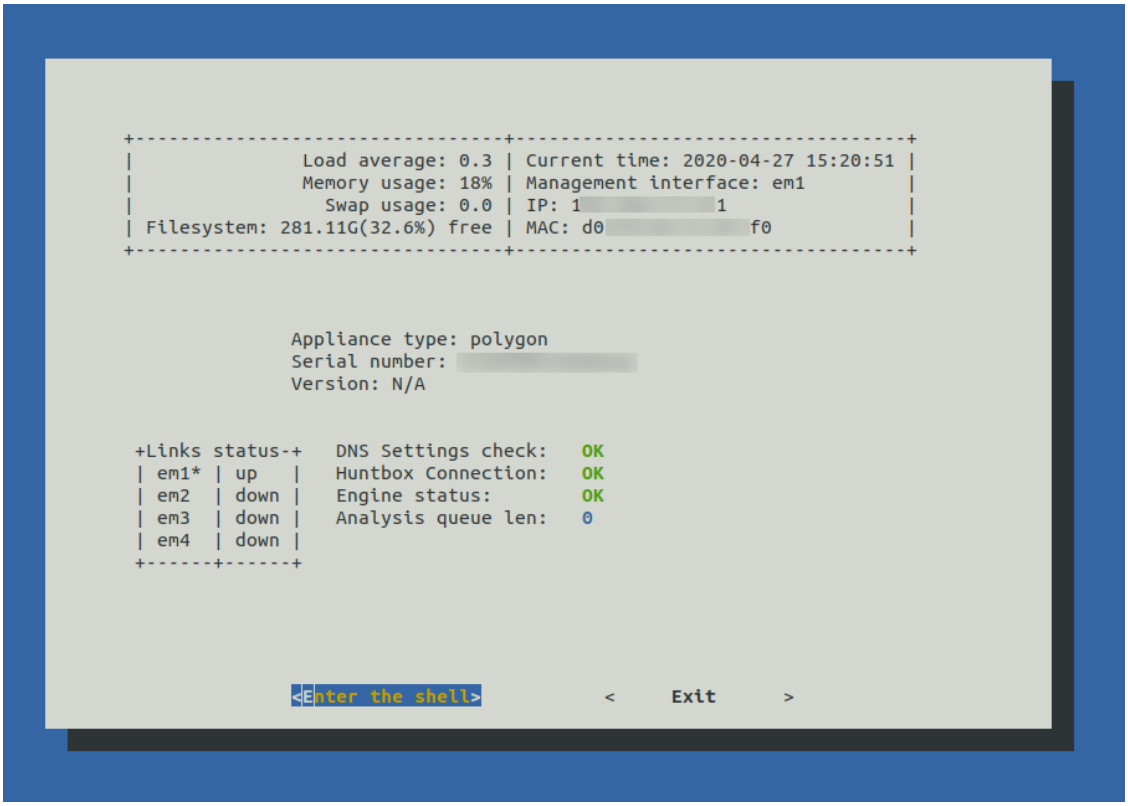
После ввода логина и пароля на экран будет выведена основная информация о MDP. Для входа в главное меню выберите Enter the Shell. Не забудьте изменить пароль по умолчанию!

3.2.2 Главное меню Malware Detonation Platform

Ниже приведено приветственное окно состояние компонента MDP при подключении по SSH.



После нажатия `Enter the shell` доступно основное меню `MDP Shell`.



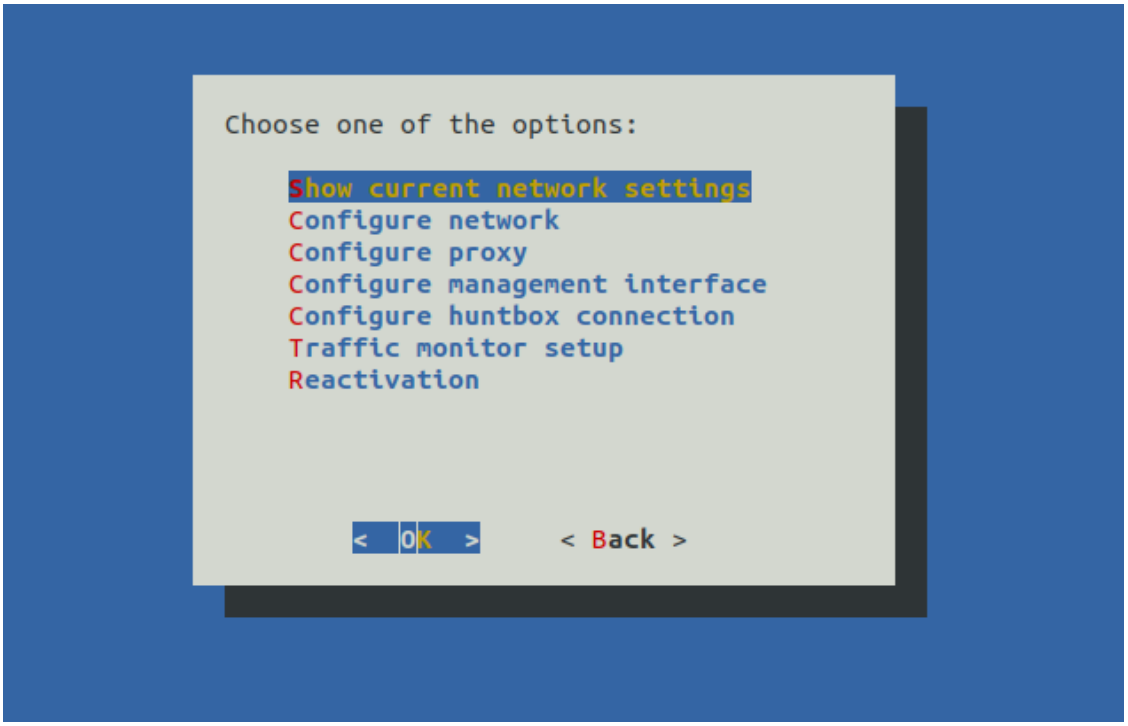
Пункты главного меню:

- **Network menu** – просмотр и изменение настроек сетевых интерфейсов
- **Change Password** – изменение пользовательского пароля от Shell
- **Debug shell** – режим отладки
- **Power management** – меню управления питанием

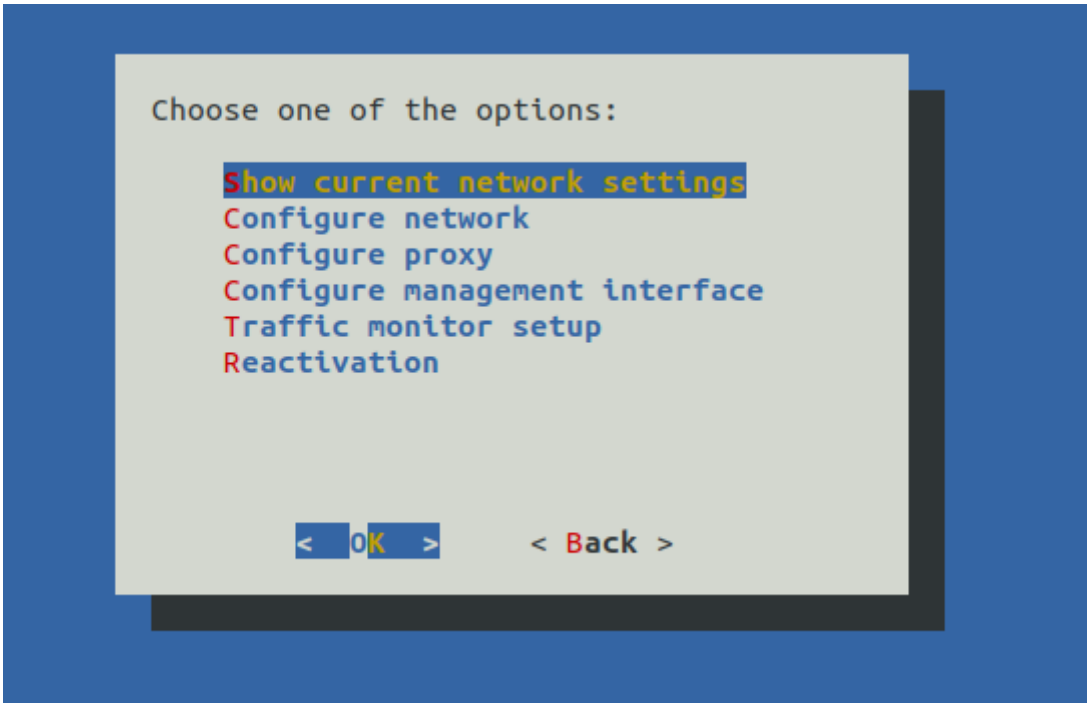
3.2.3 Настройка сети Malware Detonation Platform

Для работы с сетевыми настройками необходимо подключиться к MDP используя любой удобный SSH-клиент.

Если у Клиента используется локальный MXDR Console, то окно `Network menu` будет отображаться в следующем виде:



Если Клиент использует облачный MXDR Console, то окно `Network menu` будет отображаться в следующем виде:



Пункт меню `Configure huntbox connection` будет отображаться только после активации Network Traffic Analysis за локальным MXDR Console

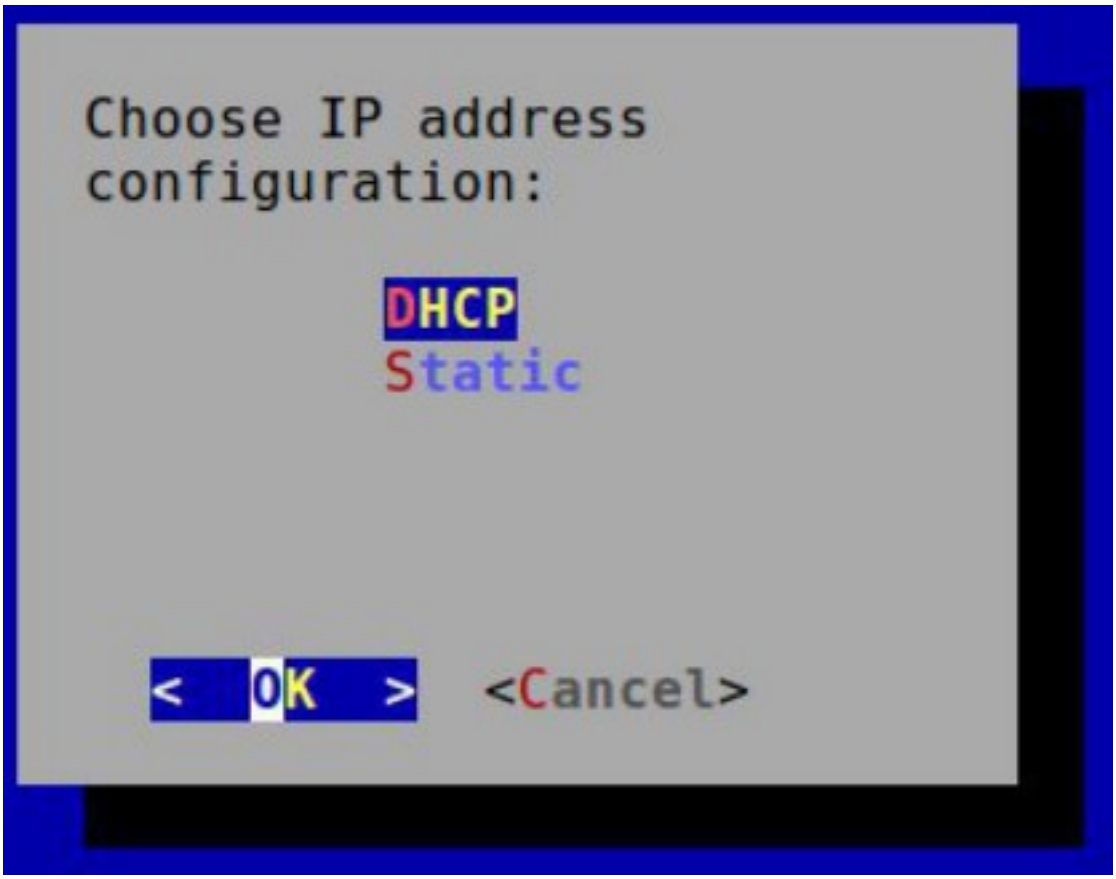
Пункты меню настройки сети:

- **Show current network settings** — вывод текущей настройки сетевого интерфейса управления

- **Configure network** — настройка сетевого интерфейса
- **Configure proxy** — настройки прокси для работы с внутреннего SOC / MXDR Console
- **Configure management interface** — настройки управляющего интерфейса
- **Configure huntbox connection** — настройки подключения к MXDR Console
- **Reactivation** — повторная активация компонента
- **< Back >** — возврат на уровень меню выше

Для настройки сети необходимо проделать следующее:

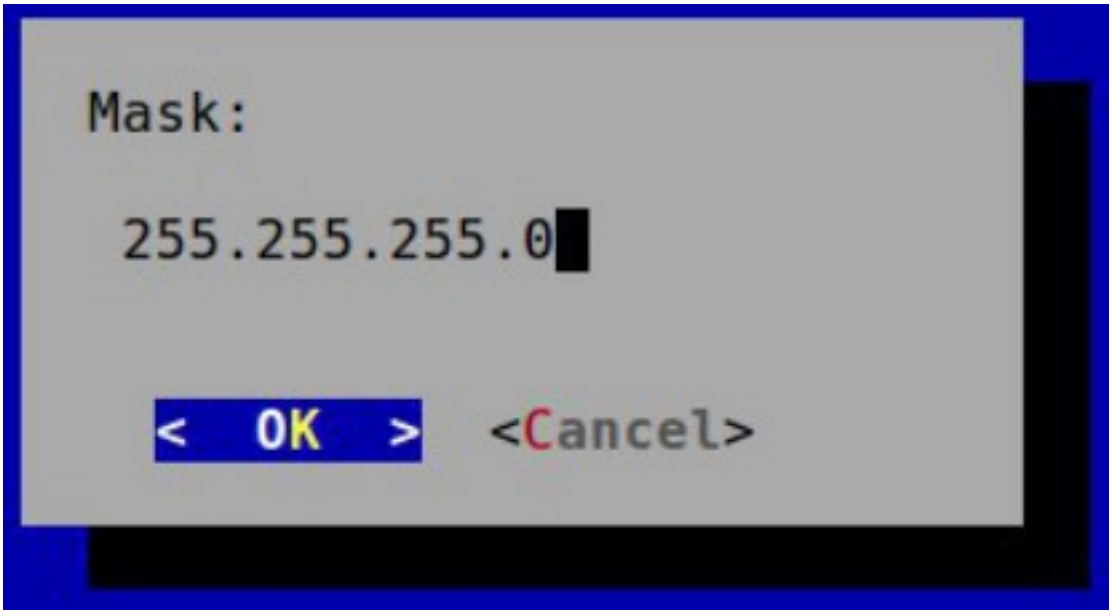
1. Перейдите в `Network menu` → `Configure network`
2. Выберите необходимый способ получения сетевых настроек

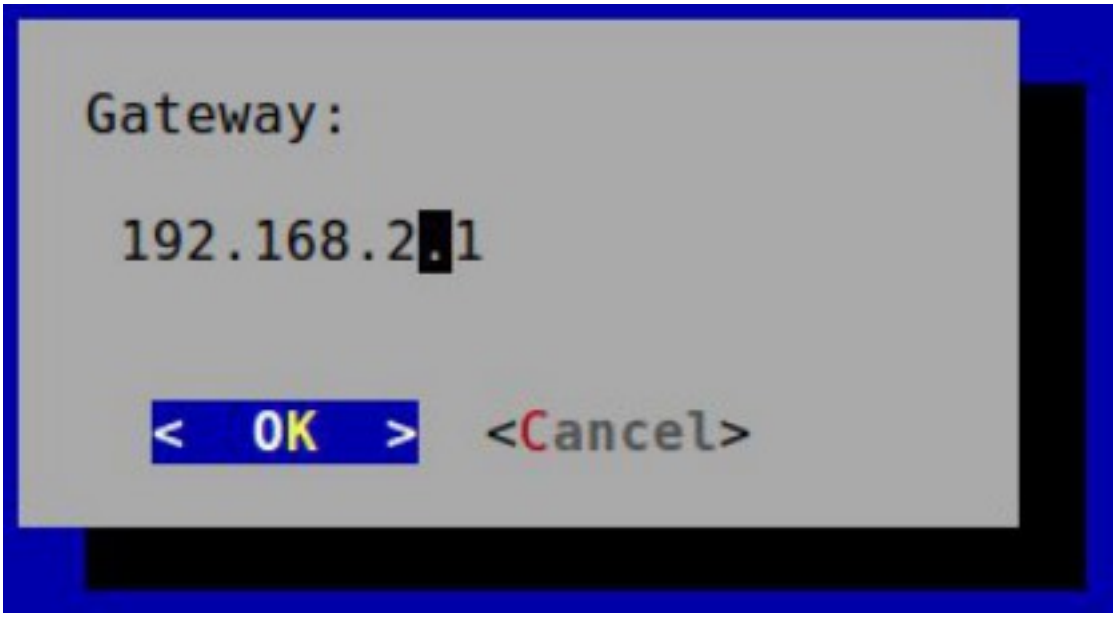


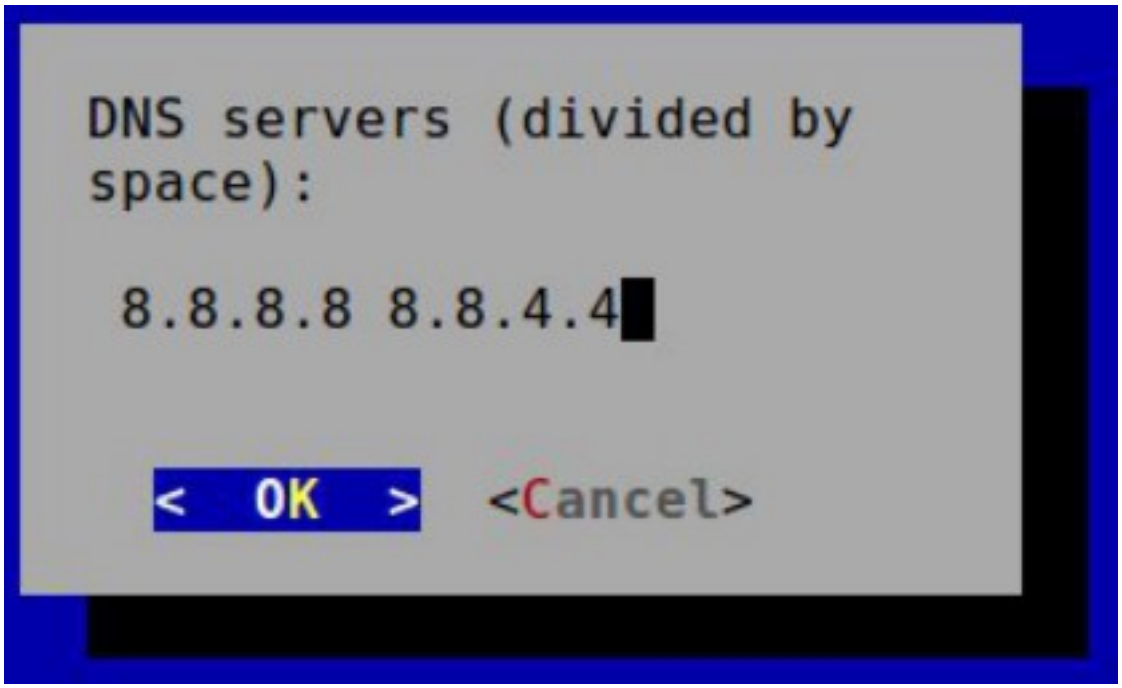
- **DHCP —** позволяет автоматически получить и сохранить необходимые сетевые настройки;
- **STATIC —** переходит в разделы для статической конфигурации сетевого интерфейса:

3. Укажите необходимые параметры


IP address:
192.168.2.1
< OK >
<Cancel>

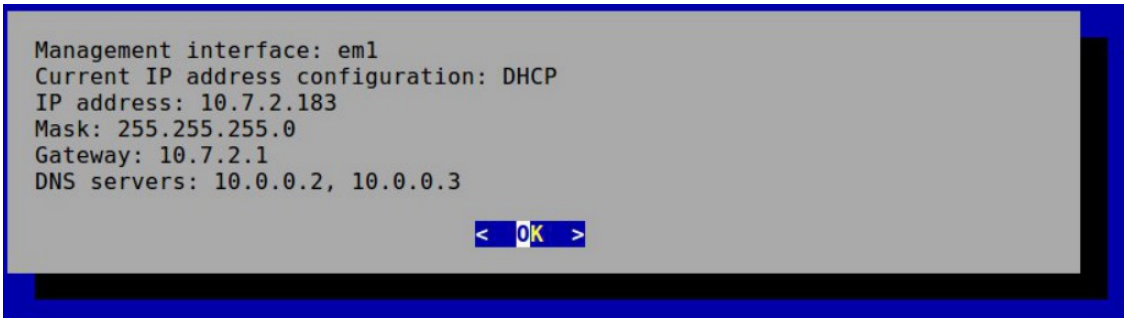

Mask:
255.255.255.0
< OK >
<Cancel>


Gateway:
192.168.2.1
< OK >
<Cancel>



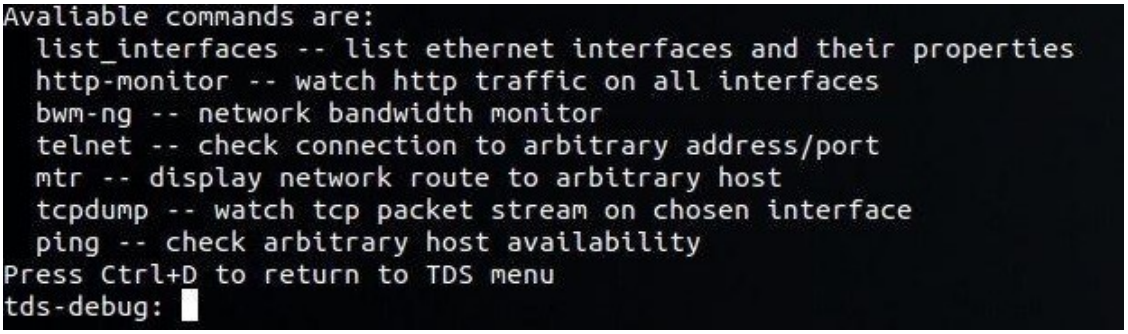
Если вы хотите указать несколько IP-адресов DNS-серверов, разделите их пробелом.

4. Проверьте информацию о настроенном сетевом интерфейсе: Network menu → Show current network settings

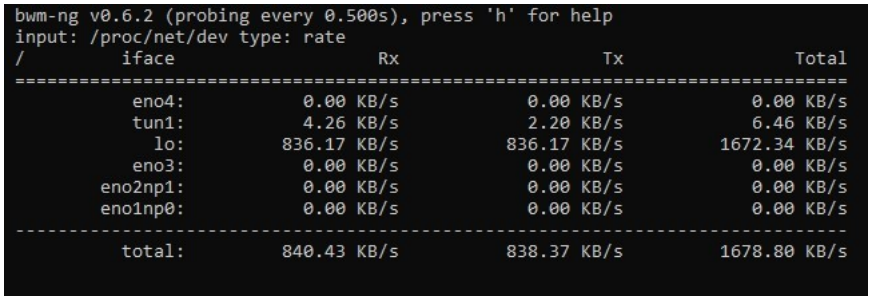


3.3 Debug Shell

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



- **list_interfaces** — список интерфейсов с обозначением как работающих, так и отключенных, а также с обозначаем управляющего интерфейса
- **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

3.4 Активация Malware Detonation Platform и синхронизация с MXDR Console

Активация Malware Detonation Platform – включает функциональность MDP. **Синхронизация Malware Detonation Platform** – привязывает MDP к MXDR Console либо к MXDR Console cloud, тем самым предоставляя возможность управления MDP через обозначенные системы.

3.4.1 Лицензионный ключ (UID)

Перед активацией Malware Detonation Platform на облачном или локальном MXDR Console необходимо получение лицензионного ключа (UID). Воспользуйтесь одним из следующих вариантов:

- при активации на MXDR Console cloud обратитесь к менеджеру или технической поддержке
- при активации на локальном MXDR Console используйте пункт меню Добавить устройство

Для взаимодействия MDP с MXDR Console необходимы следующие порты:

- 443/tcp - для первичной активации и привязки MDP (единоразово) - вне зависимости от выбора типа MXDR Console
- 1443/udp - для дальнейшего взаимодействия MDP с MXDR Console - только для локальной версии
- 3000/tcp - для взаимодействия Malware Detonation Platform с Network Traffic Analysis

Активация и синхронизация осуществляется через консоль Malware Detonation Platform

На данном этапе статус `Galaxy Connection` равен `Fail`. Так как Malware Detonation Platform не привязан к MXDR Console.

4 Сценарии проверки работоспособности ПО

4.1 Локальное размещение Malware Detonation Platform

4.1.1 Проверка физической работоспособности MDP

1. Проверить наличие и размещение оборудования Системы.

Результат: Сервер установлен в серверную стойку.

2. Проверить подачу питания на серверы Системы.

Результат: наличие подключения блоков питания сервера к сети электропитания.

3. Проверить интеграцию с инфраструктурой заказчика.

Результат: необходимые сетевые интерфейсы подключены к локальной сети заказчика.

4. Убедиться, что оборудование включается при нажатии кнопки включения.

4.1.2 Проверка корректности загрузки исполняемого программного обеспечения MDP

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.

4.2 Облачное размещение Malware Detonation Platform

4.2.1 Проверка доступности модуля

Перейти в раздел **Настройки** → **Модули**, должен присутствовать модуль “Cloud Malware Detonation”, индикатор модуля с левой стороны должен быть зеленым.

4.2.2 Проверка работоспособности локально размещенного модуля MDP и проведение анализа файла

Данный пункт распространяется только на инсталляции с локально размещенным MXDR Console.

1. Проверить, корректность настроек вывода виртуальных машин MDP в интернет:

– При наличии физического сетевого доступа MDP в Интернет (а также при наличии доступа к общедоступным DNS, например, 8.8.8.8) в разделе **Настройки** → **Модули** → **Malware Detonation Platform** → **Основные настройки** → **Доступ виртуальных машин в Интернет** → Требуется, Маршрут для вывода трафика → через mgmt-порт;

– При отсутствии физического сетевого доступа MDP в Интернет, но наличии доступа в Интернет у MXDR Console (а также при наличии доступа к общедоступным DNS, например, 8.8.8.8) в разделе **Настройки** → **Модули** → **Malware Detonation Platform** → **Основные настройки** → **Доступ виртуальных машин в Интернет** → Требуется, Маршрут для вывода трафика → через MXDR Console.

– При отсутствии физического сетевого доступа MDP и MXDR Console в Интернет, в разделе **Настройки** → **Модули** → **Malware Detonation Platform** → **Основные настройки** → **Доступ виртуальных машин в Интернет** → Отключен.

2. Проверить, что индикатор состояния устройства (слева) в разделе **Настройки** → **Модули** → **MDP** зеленый.

3. Перейти в раздел **Расследование** → **Проверенные файлы** → **Загрузить файл** → **Загрузить**. Если доступ в Интернет у ВМ MDP отсутствует, в сайдбаре загрузки файла настройку “Соединение с интернетом” перевести в состояние Выключено.

4. В разделе **Расследование** → **Проверенные файлы** установить фильтр по источнику файла в значение **Manual**. Наличие записи о завершенном анализе файла, загруженного на предыдущем этапе,и наличие отчета MDP свидетельствуют о корректности работы модуля. Предельное время ожидания результата анализа - 60 минут.

4.2.2.1 Проверка работоспособности модуля MDP (облачное размещение) и проведение анализа файла

Данный пункт распространяется и на инсталляции с облачной MXDR Console, и на инсталляции с локальной MXDR Console.

1. Проверить, что индикатор состояния устройства (слева) в разделе **Настройки** → **Модули** → **Malware Detonation Platform** зеленый.

2. Перейти в раздел **Расследование** → **Проверенные файлы** → **Загрузить файл** → **Загрузить**.

3. В разделе **Расследование** → **Проверенные файлы** установить фильтр по источнику файла в значение **Manual**. Наличие записи о завершенном анализе файла, загруженного на предыдущем этапе, и наличие отчета MDP свидетельствуют о корректности работы модуля. Предельное время ожидания результата анализа - 60 минут.

5 Администрирование Malware Detonation Platform

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

- **Версия** – версия ПО,
- **Имя** – наименование устройства,
- **Тип** – тип устройства,
- **Компания** – наименование компании, в которой находится оборудование,
- **Лицензия** – тип лицензии,
- **Дата создания** – дата выдачи лицензии,
- **Конец лицензии** – дата окончания срока – действия лицензии,
- **Свойства** – информация по устройству.

5.1 Общая информация

- **Имя** – заданный идентификатор может быть любым,
- **Номер лицензии** – получен при покупке или тестировании решения,
- **Серийный номер** – серийный номер оборудования, Комментарий – может быть любым,

- **VPN IP** – адрес внутри VPN туннеля получаемый при подключении Malware Detonation Platform к MXDR Console для управляющих коммуникаций,
- **Внешний IP** – адрес управляющего интерфейса выданный на стороне клиента (через DHCP или статическими правилами),
- **Компания** – наименование компании, в которой находится оборудование – задаются при создании нового устройства из списка **Настройки –> Компании**,
- **Номер лицензии** – получен при покупке или тестировании решения.

5.2 Состояние устройства

- **Последний HeartBeat** – последний замеченный heartbeat с данного устройства,
- **Последнее обновление**,
- **CPU / RAM / HDD**,
- **Дропы в ядре / на интерфейсе**,
- **Последняя активность в VPN** – крайнее время активности VPN между Malware Detonation Platform и управляющим MXDR Console,
- **Длительность** – временной отрезок в течении которого между Malware Detonation Platform и MXDR Console был установлен управляющий VPN канал. Отчитывается с момента последней потери связи между устройствами.
- **Длина очереди** - количество находящихся в очереди на анализ объектов на момент просмотра карточки устройства MDP.

5.3 Графики состояния устройства

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

Производительность

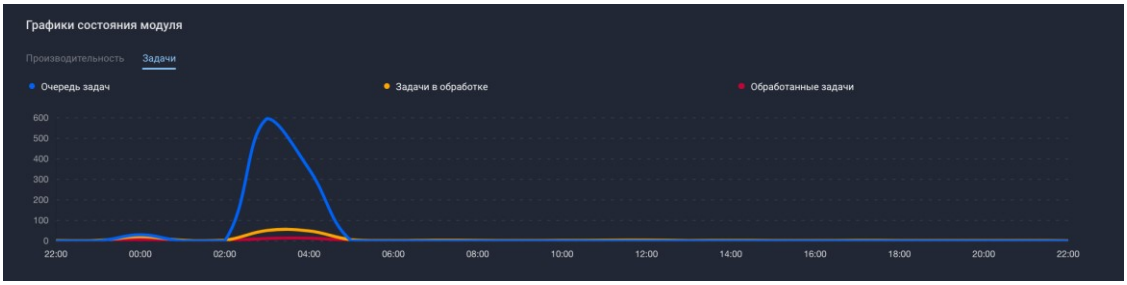
- **Среднее CPU (%),**
- **Макс. RAM (%),**
- **Макс. HDD (%).**

Задачи

Вкладка содержит подробный график формирования очереди задач по количеству анализируемых объектов. Можно настраивать внешний вид графика, комбинируя следующие данные:

- **Очередь задач** - количество задач на обработку объектов, находящихся в очереди в выбранный отрезок времени.
- **Задачи в обработке** - количество задач, которые в выбранный период времени находились в обработке.
- **Обработанные задачи** - количество завершенных задач на обработку объектов за выбранный временной отрезок.

График отображает показатели за последние 24 часа. При наведении на любую точку графика отобразится подробная информация о числе задач в указанное время.



Для редактирования базовых свойств нажмите на кнопку  – редактируемые параметры:

- **Имя,**
- **Комментарий.**

Данная кнопка доступна только для пользователей с типом аккаунта owner.

Для редактирования расширенных настроек нажмите на кнопку **Основные настойки**. Доступные настройки:

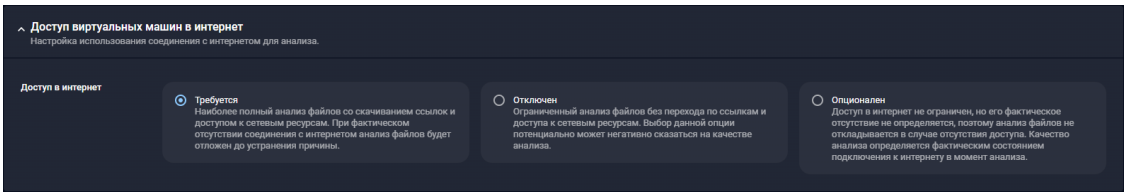
1. Доступ виртуальных машин в Интернет
2. Маршрут для выхода виртуальных машин в интернет
3. Сервер времени Malware Detonation Platform
4. Пользовательские YARA-правила Malware Detonation Platform
5. SNMP-мониторинг
6. Пользовательский словарь паролей

7. Белый список

Кнопка **Управление лицензией** используется для настройки лицензии данного устройства.

5.4 Доступ виртуальных машин в Интернет

Одной из крайне важных настроек Malware Detonation Platform является возможность предоставления доступа в открытую сеть Интернет образа ОС развёрнутым в виртуальной среде.

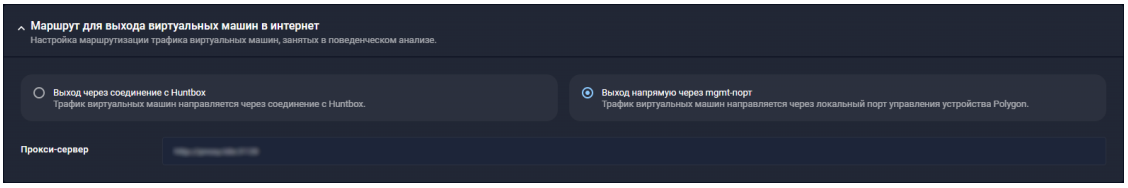


Доступны следующие опции доступа в Интернет:

- **Требуется** – наиболее полный анализ файлов с переходами по ссылкам на скачивание и доступом к сетевым ресурсам. При фактическом отсутствии соединения с интернетом, анализ файлов будет отложен до восстановления соединения.
- **Отключен** – ограниченный анализ файлов без перехода по ссылкам и доступа к сетевым ресурсам. Выбор данной опции потенциально может негативно сказаться на качестве анализа.
- **Опционален** – анализ файлов не откладывается в случае отсутствия доступа к Интернету. Качество анализа определяется фактическим состоянием подключения к интернету в момент анализа.

5.5 Маршрут для выхода виртуальных машин в интернет

Настройка позволяет, в первую очередь, определять используемый для доступа в Интернет маршрут.



Доступны следующие опции:

- **Выход через соединение с MXDR Console** – все сетевые запросы из виртуальной среды в открытую сеть Интернет инкапсулируются в VPN соединение до MXDR

Console. Таким образом запросы анализируемого ПО в Интернет обрабатываются MXDR Console.

- **Выход напрямую через mgmt-порт** – все сетевые запросы из виртуальной среды в открытую сеть Интернет направляются на маршрутизатор по умолчанию через интерфейс управления Malware Detonation Platform. Таким образом запросы анализируемого ПО в Интернет обрабатываются Malware Detonation Platform.

Для проведения качественного поведенческого анализа анализируемому ПО необходимо предоставлять неблокируемый доступ до требуемых ресурсов в открытой сети Интернет, даже если эти ресурсы являются заведомо вредоносными! Учитывая данный факт, при выбранной настройке **MXDR Console** в первой опции и **MDP** во второй необходимо предоставлять неблокируемый доступ до открытой сети Интернет без ограничений!

5.5.1 Контроль обращения по ссылкам из виртуальной среды

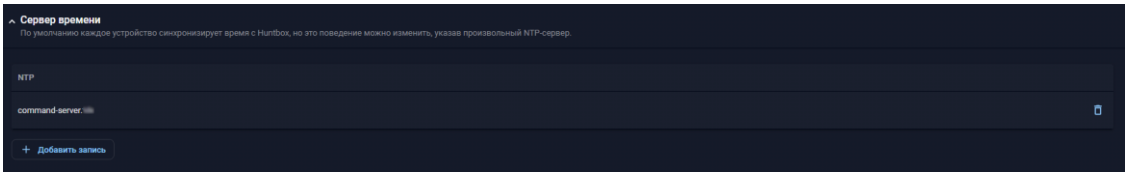
В Malware Detonation Platform присутствует отдельный модуль, обрабатывающий сценарии обращения по ссылкам, обнаруженным в файлах анализируемого ПО. Существует возможность проксировать такие обращения отдельно от остального потока обращений из виртуальной среды в открытую сеть Интернет.

Для настройки проксирования задайте адрес прокси-сервера в поле **Прокси-сервер для анализа ссылок** в следующем формате:

```
Адрес прокси-сервера:порт
```

5.6 Сервер времени Malware Detonation Platform

По умолчанию каждый Malware Detonation Platform 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.



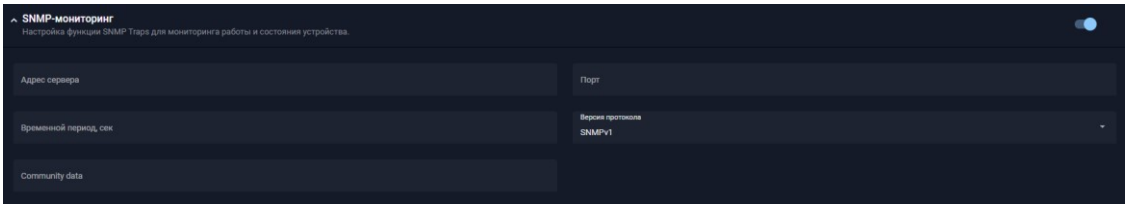
5.7 SNMP-мониторинг

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.

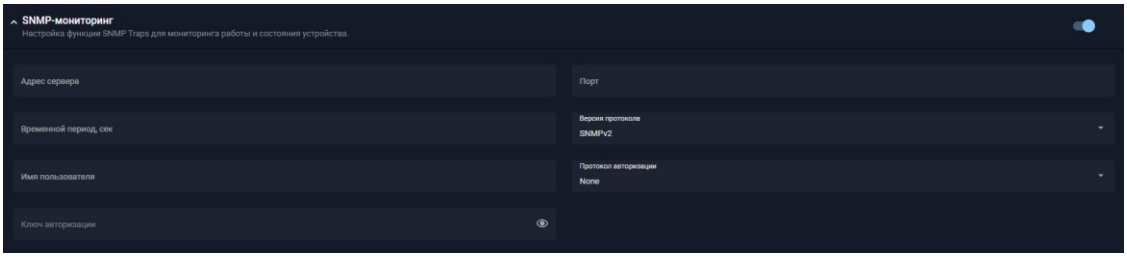
5.7.1 SNMPv1



Доступные настройки:

- Адрес сервера,
- Порт,
- Временной период,
- Community Data.

5.7.2 SNMPv2

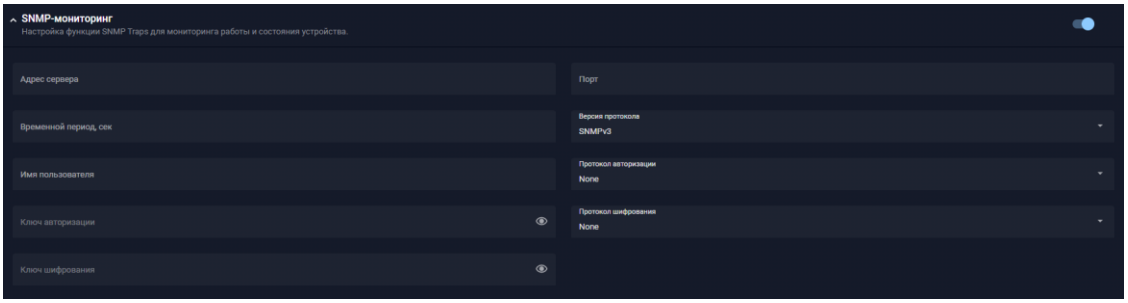


Доступные настройки:

- Адрес сервера,
- Порт,
- Временной период,

- Имя пользователя,
- Протокол авторизации:
    - MD5,
    - SHA,
    - SHA224,
    - SHA256,
    - SHA384,
    - SHA512.
- Ключ авторизации.

5.7.3 SNMPv3



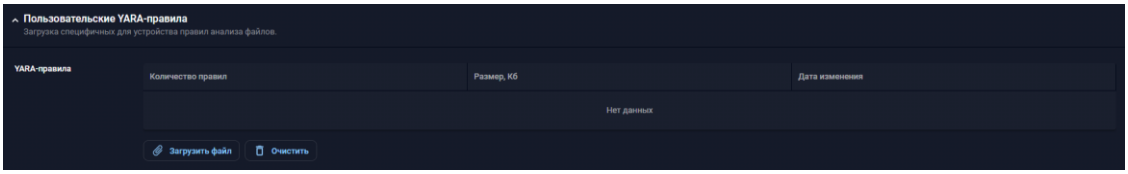
Доступные настройки:

- Адрес сервера,
- Порт,
- Временной период,
- Имя пользователя,
- Протокол авторизации:
    - MD5,
    - SHA,
    - SHA224,
    - SHA256,
    - SHA384,
    - SHA512.

- Ключ авторизации,
- Протокол шифрования:
  - DES,
  - 3DES,
  - AES128,
  - AES192,
  - AES256.
- Ключ шифрования.

5.8 Пользовательские YARA-правила Malware Detonation Platform

В данном разделе Пользовать может добавлять собственные YARA-правила. Данные правила влияют на файловые объекты попадающие на анализ в MDP. С помощью них можно изменить конечный вердикт по данному объекту независимо от детонации файла.



Не путайте с YARA правила на Network Traffic Analysis. А также учитывайте коллизии между YARA-правилами на обоих типах устройств!

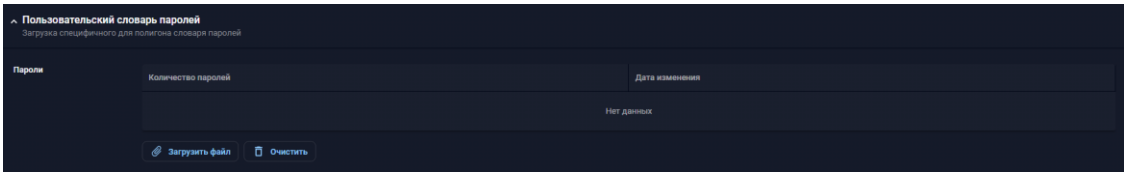
Чтобы прикрепить сформированный ранее файл со своего устройства, нажмите на кнопку **Загрузить файл**.

Чтобы удалить ненужные/устаревшие файлы, нажмите на кнопку **Очистить**.

5.9 Пользовательский словарь паролей

В данном разделе можно задать собственную базу паролей, используемых при вскрытии архивов, найденных в анализируемых потоках данных и направленных на детонацию в Malware Detonation Platform.

Пароли необходимо подавать списком, каждый элемент которого разделен знаком перевода строки.



Важно понимать, что заданные в данном разделе пароли не заменяют заводские способы обнаружения и подбора паролей к архивам. Заданная настоящими настройками дополнительная база паролей будет использована, как крайнее средство перебора после неудачи всех первичных методов.

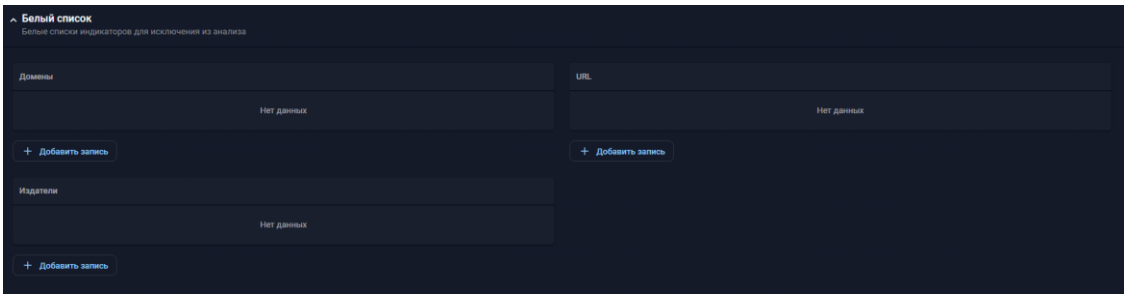
5.10 Белый список

Белые списки позволяют исключать из анализа объекты, которые могут быть как непосредственно направлены в Malware Detonation Platform от модулей MXDR, так и получены в процессе анализа изначального файлового объекта.

Оптимизация работы решения с помощью данного инструмента является обязательным условием высокого качества обнаружения атак.

Основные индикаторы:

- **Домены,**
- **URL,**
- **Издатели.**



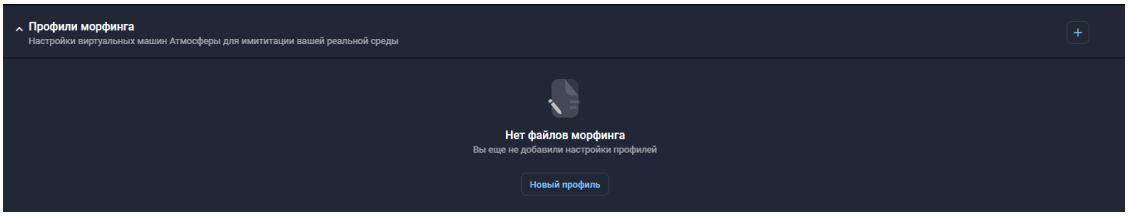
Для управления блоком используйте следующие кнопки:

Кнопка	Описание
+ Добавить запись	Создание новой записи
✓	Подтверждение создания новой записи
✗	Отмена создания новой записи
🗑	Удаление записи

5.11 Профили морфинга

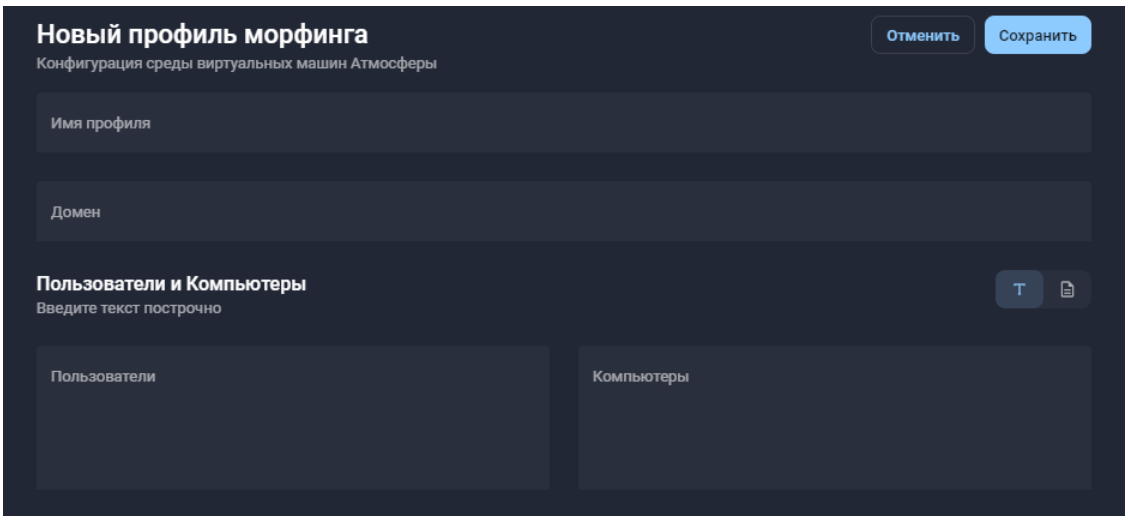
Профиль морфинга - это текстовый список данных позволяющий применять специфичные клиентские свойства на виртуальных машинах, используемых для анализа писем: например, присоединять виртуальные машины к контроллерам домена с конкретным именем, использовать конкретные имена пользователей и компьютеров.

Профили морфинга позволяют имитировать доменные рабочие ПК клиента при детонации файлов в Malware Detonation Platform.



Для добавления новых профилей используйте соответствующие кнопки **Новый профиль** или  в правом верхнем углу настройки.

Редактировать раннее созданные профили морфинга невозможно. Чтобы внести изменения нужно создать новый профиль и по его готовности переключить все необходимые анализы на него. Старый профиль можно удалить, если необходимость в нем отпала.



Профилей морфинга может быть несколько, но активен всегда только один (выбранный).

Необходимые настройки профиля:

- **Имя профиля**
- **Домен** – в виде FQDN

- **Пользователи** – список имен пользователей используемых в виртуальных образах ОС MXDR Malware Detonation Platform

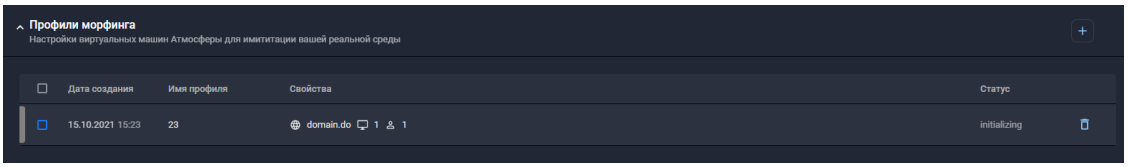
- **Компьютеры** – список имён компьютеров используемых в виртуальных образах ОС MXDR Malware Detonation Platform

Для имен пользователей и компьютеров должны учитываться **валидационные требования**. Они повторяют требования ОС Windows.

Имена короче **4 символов** недопустимы.

	Требования
Имя пользователя	- Локальные имена пользователей должны быть уникальными на автоматизированном рабочем месте - Глобальные имена - всюду по доменной области - Имя не должно быть длиннее 20 знаков - Не могут содержать знаки: " / \ [ ] : ; = , + * ? < > | - Имена могут содержать другие специальные знаки (пробелы, точки дефисы, подчеркивания и т.д.), но предпочтительнее этого избегать.
Имя компьютера	- Имя компьютера не может быть длиннее 15 символов - Не может быть полностью числовым - Содержать следующие символы: " / \ [ ] : ; = , + * ? < > @ $ # ! & ( ) { } `` ~ % ^ _ ' |

Списки имен пользователей и компьютеров выбираются случайным образом и обновляются через заданное производителем число анализов.



Создание профиля морфинга является сложным процессом. Операция по созданию одного профиля может занимать до 2х часов времени.

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 «F6 Malware Detonation Platform»: 115088, г. Москва, ул. Шарикоподшипниковская, д. 1