

МИРАЖ

Система раннего обнаружения внутренних угроз

**Инструкция по установке экземпляра
программного обеспечения,
предоставленного для проведения
экспертной проверки**

Содержание

1. Общие сведения.....	3
2. Системные требования.....	3
2.1. Требования к аппаратному обеспечению.....	3
2.2. Требования к программному обеспечению.....	3
2.3. Сетевые требования.....	4
2.4. Поддерживаемые браузеры.....	4
3. Предварительные условия.....	5
4. Установка Data Plane (VM2).....	6
4.1. Распаковка дистрибутива.....	6
4.2. Запуск установщика.....	6
4.3. Настройка сети.....	6
4.4. Автоматические действия.....	6
4.5. Настройка сетевых bridge.....	6
5. Установка Control Plane (VM1).....	7
5.1. Распаковка дистрибутива.....	7
5.2. Запуск установщика.....	7
5.3. Настройка сети.....	7
5.4. Автоматические действия.....	7
5.5. Копирование сертификатов Data Plane.....	7
6. Первичная настройка системы.....	8
6.1. Доступ к веб-интерфейсу.....	8
6.2. Активация лицензии.....	8
6.3. Создание администратора.....	8
6.4. Первые шаги после установки.....	8
7. Проверка работоспособности.....	9
7.1. Проверка Control Plane (VM1).....	9
7.2. Проверка Data Plane (VM2).....	9
7.3. Проверка связи VM1 ↔ VM2.....	9
8. Обновление системы.....	10
9. Расположение файлов.....	10
9.1. Control Plane (VM1).....	10
9.2. Data Plane (VM2).....	10
10. Полезные команды.....	11
10.1. Control Plane (VM1).....	11
10.2. Data Plane (VM2).....	11
11. Контакты технической поддержки.....	12

1. Общие сведения

Программа «Мираж» предназначена для раннего обнаружения внутренних угроз информационной безопасности в корпоративных сетях. В отличие от традиционных средств защиты (межсетевые экраны, IDS/IPS), которые пытаются не допустить атакующего в сеть, данный продукт предполагает, что злоумышленник уже находится внутри периметра, и создаёт условия для его обнаружения. Система развёртывается на двух виртуальных машинах:

- **Control Plane (VM1)** — управление, API, база данных, веб-интерфейс
- **Data Plane (VM2)** — инфраструктура ловушек на базе контейнеров

Установка осуществляется с помощью интерактивного установщика `install-mirage.sh`, который автоматизирует весь процесс: проверку требований, установку зависимостей, настройку сертификатов, развёртывание сервисов и миграцию базы данных.

2. Системные требования

2.1. Требования к аппаратному обеспечению

Параметр	VM1 (Control Plane)	VM2 (Data Plane)
Операционная система	Ubuntu Server 22.04/24.04 LTS, Debian 11/12, Astra Linux SE 1.7/1.8, РЕД ОС 7.3/8, Альт СП 10, Альт Сервер 10, Альт Виртуализация 10, РОСА ХРОМ Сервер	Ubuntu Server 22.04/24.04 LTS, Debian 11/12, Astra Linux SE 1.7/1.8, РЕД ОС 7.3/8, Альт СП 10, Альт Сервер 10, Альт Виртуализация 10, РОСА ХРОМ Сервер
СРU	4 vCPU	8 vCPU
Оперативная память	8 GB	16 GB
Диск	100 GB SSD	200 GB SSD (ZFS)
Сеть	1 сетевой интерфейс	1+ интерфейсов (по VLAN)

2.2. Требования к программному обеспечению

VM1 (Control Plane):

- Docker 20.10+ и Docker Compose 2.0+ (устанавливаются автоматически установщиком)
- Открытые порты: 443/tcp (Web UI), 8443/tcp (API для honeypots)
- Учётная запись с правами root (или sudo)

VM2 (Data Plane):

- LXD 5.x (устанавливается автоматически установщиком)
- ZFS для storage pool
- Открытый порт: 8443/tcp (LXD API)
- Сетевые bridge-интерфейсы для каждого VLAN
- Учётная запись с правами root (или sudo)

2.3. Сетевые требования

Между VM1 и VM2 должна быть сетевая связность по порту 8443/tcp. Связь осуществляется по mTLS.

Источник	Назначение	Порт	Описание
Браузер	VM1	443/HTTPS	Веб-интерфейс
VM1 API	VM2 LXD	8443/HTTPS	Управление контейнерами
Honeypots	VM1 API	8443/mTLS	Телеметрия, heartbeat
Атакующий	Honeypots	22, 80, 445...	Взаимодействие с ловушками

2.4. Поддерживаемые браузеры

Google Chrome 90+, Mozilla Firefox 90+, Safari 14+, Microsoft Edge 90+.

3. Предварительные условия

1. Подготовить две виртуальные машины с установленной ОС Ubuntu, согласно требованиям, раздела 2.
2. Обеспечить сетевую связность между VM1 и VM2 по порту 8443/tcp.
3. Подготовить учётные записи с правами администратора (root/sudo) на обеих VM.
4. Получить дистрибутив установщика **mirage-installer.tar.gz** и разместить его на обеих виртуальных машинах.
5. Определить IP-адреса VM1 и VM2, а также VLAN-сегменты для размещения ловушек.

⚠ Важно: сначала устанавливается *Data Plane (VM2)*, затем *Control Plane (VM1)*.

4. Установка Data Plane (VM2)

4.1. Распаковка дистрибутива

Войдите на VM2 под учётной записью с правами root. Распакуйте архив и перейдите в каталог установщика:

```
tar -xzf mirage-installer-v1.3.2.tar.gz
cd mirage-installer-v1.3.2
sudo chmod +x install-mirage.sh
```

4.2. Запуск установщика

Запустите установщик:

```
sudo ./install-mirage.sh
```

Установщик отобразит ASCII-баннер и выполнит проверку системных требований (ОС, CPU, RAM, диск). При выборе типа установки выберите опцию:

```
2) Data Plane
```

4.3. Настройка сети

Установщик запросит следующие параметры:

- **IP этого сервера (Data Plane)** — IP-адрес VM2 (определяется автоматически)
- **IP адрес Control Plane** — IP-адрес VM1
- **HTTPS порт Control Plane** — порт для Web UI (по умолчанию 443)

4.4. Автоматические действия

Установщик автоматически выполнит:

- Установку LXD 5.x через snap
- Инициализацию LXD с ZFS storage pool
- Импорт образов ловушек (Linux и Windows)
- Настройку LXD API на порту 8443
- Генерацию клиентского сертификата для подключения VM1
- Установку утилит управления сетями в /usr/local/bin/

4.5. Настройка сетевых bridge

Для каждого VLAN, в котором будут размещаться ловушки, создайте bridge-интерфейс и LXD-профиль:

```
sudo mirage-add-network.sh
```

Скрипт интерактивно запросит: имя bridge, имя профиля, физический интерфейс и VLAN ID. Проверить результат можно командой:

```
sudo mirage-list-networks.sh
```

i Сертификаты для подключения VM1 сохраняются в /etc/mirage/lxd-client-cert/. Они понадобятся на следующем шаге.

5. Установка Control Plane (VM1)

5.1. Распаковка дистрибутива

Войдите на VM1 под учётной записью с правами root. Распакуйте архив:

```
tar -xzf mirage-installer-v1.3.2.tar.gz
cd mirage-installer-v1.3.2
sudo chmod +x install-mirage.sh
```

5.2. Запуск установщика

```
sudo ./install-mirage.sh
```

При выборе типа установки выберите:

- 1) Control Plane

5.3. Настройка сети

Установщик запросит:

- **IP адрес Control Plane** — IP-адрес VM1 (определяется автоматически)
- **HTTPS порт** — порт Web UI (по умолчанию 443)
- **IP адрес Data Plane** — IP-адрес VM2

5.4. Автоматические действия

Установщик автоматически выполнит:

- Установку Docker и Docker Compose
- Создание рабочих директорий в /opt/mirage/
- Генерацию SSL-сертификатов (самоподписанных)
- Загрузку Docker-образов (offline-режим)
- Генерацию конфигурации .env
- Запуск Docker-контейнеров (PostgreSQL 16, Redis 7, FastAPI, Celery, nginx)
- Применение миграций базы данных (Alembic)
- Установку Trial-лицензии (14 дней)
- Генерацию hardware fingerprint

5.5. Копирование сертификатов Data Plane

После завершения установки необходимо скопировать клиентские сертификаты с VM2 для подключения к LXD. Выполните на VM1:

```
sudo mkdir -p /opt/mirage/certs/lxd
sudo scp root@<IP_VM2>:/etc/mirage/lxd-client-cert/* /opt/mirage/certs/lxd/
sudo chown -R 1000:1000 /opt/mirage/certs/lxd
cd /opt/mirage && sudo docker compose restart backend
```

⚠ Замените <IP_VM2> на реальный IP-адрес VM2 (Data Plane).

6. Первичная настройка системы

6.1. Доступ к веб-интерфейсу

Откройте в браузере:

`https://<IP_VM1>`

При использовании самоподписанного сертификата браузер отобразит предупреждение о безопасности — примите исключение для продолжения.

i Для продуктивной эксплуатации замените сертификаты на валидные (`deploy/nginx/ssl/server.crt` и `server.key`).

6.2. Активация лицензии

При первом обращении система автоматически активирует Trial-лицензию (14 дней, 5 ловушек, 2 приманок, 2 пользователя). При наличии коммерческой лицензии загрузите файл `.lic` через интерфейс.

6.3. Создание администратора

Система предложит создать первого администратора:

6. Введите email и полное имя.
7. Задайте пароль (минимум 12 символов: заглавные/строчные буквы, цифры, спецсимволы).
8. Сохраните одноразовые коды восстановления в безопасном месте.

⚠ Первый администратор получает статус суперпользователя. Эту учётную запись нельзя удалить или понизить в правах.

⚠ Коды восстановления — единственный способ восстановить доступ без настроенного Email. Каждый код одноразовый.

6.4. Первые шаги после установки

9. Войдите в систему с созданными учётными данными.
10. Перейдите в **Настройки** → **Интеграции** и настройте канал оповещения (Telegram или Email).
11. Перейдите в раздел **Сети** и создайте сетевые профили для VLAN.
12. Перейдите в раздел **Ловушки** и создайте первую ловушку.
13. Создайте **приманки**, связанные с ловушкой, и разместите их в сети.
14. Убедитесь, что ловушка получила IP-адрес и отправляет heartbeat (статус "Работает").

7. Проверка работоспособности

7.1. Проверка Control Plane (VM1)

На VM1 выполните следующие команды:

Статус Docker-контейнеров:

```
cd /opt/mirage && docker compose ps
```

Все контейнеры должны быть в статусе Up (healthy):

Контейнер	Назначение	Ожидаемый статус
mirage-postgres	База данных	Up (healthy)
mirage-redis	Кэш и broker	Up (healthy)
mirage-backend	FastAPI API	Up (healthy)
mirage-celery-worker	Фоновые задачи	Up
mirage-celery-beat	Планировщик	Up
mirage-frontend	nginx + React UI	Up (healthy)

Проверка API:

```
curl -k https://localhost/health
```

Ожидаемый ответ: {"status": "healthy"}

7.2. Проверка Data Plane (VM2)

На VM2 выполните:

Статус LXD:

```
snap services lxd
```

Образы ловушек:

```
lxc image list
```

Профили сетей:

```
lxc profile list
```

Доступность API:

```
ss -tlnp | grep 8443
```

7.3. Проверка связи VM1 ↔ VM2

На VM1 проверьте логи backend на отсутствие ошибок подключения к LXD:

```
docker compose logs backend | grep LXD
```

8. Обновление системы

Для обновления Control Plane запустите установщик и выберите опцию 3:

```
sudo ./install-mirage.sh
```

3) Обновление Control Plane

Процесс обновления включает:

- Автоматический бэкап базы данных перед обновлением
- Обновление Docker-образов backend и frontend
- Применение миграций Alembic
- Перезапуск всех сервисов
- Rollback при неудаче

9. Расположение файлов

9.1. Control Plane (VM1)

Путь	Описание
/opt/mirage/	Корневой каталог платформы
/opt/mirage/.env	Конфигурация окружения
/opt/mirage/docker-compose.yml	Конфигурация Docker-контейнеров
/opt/mirage/licenses/	Файлы лицензии и ключи
/opt/mirage/certs/	SSL и LXD-сертификаты
/opt/mirage/data/postgres/	Данные PostgreSQL
/opt/mirage/logs/	Журналы приложения

9.2. Data Plane (VM2)

Путь	Описание
/etc/mirage/	Конфигурация Data Plane
/etc/mirage/lxd-client-cert/	Клиентские сертификаты LXD
/usr/local/bin/mirage-*.sh	Утилиты управления сетями

10. Полезные команды

10.1. Control Plane (VM1)

Команда	Описание
<code>docker compose ps</code>	Статус контейнеров
<code>docker compose logs -f backend</code>	Логи backend
<code>docker compose logs -f celery-worker</code>	Логи фоновых задач
<code>docker compose restart backend</code>	Перезапуск backend
<code>curl -k https://localhost/health</code>	Проверка здоровья API
<code>docker compose exec postgres psql -U mirage mirage</code>	Подключение к БД

10.2. Data Plane (VM2)

Команда	Описание
<code>lxc list</code>	Список контейнеров ловушек
<code>lxc image list</code>	Список образов
<code>lxc profile list</code>	Список сетевых профилей
<code>mirage-add-network.sh</code>	Добавить сеть для honeypots
<code>mirage-list-networks.sh</code>	Показать текущие сети
<code>mirage-remove-network.sh</code>	Удалить сеть

11. Контакты технической поддержки

При возникновении вопросов по установке или эксплуатации обращайтесь в службу технической поддержки:

Канал	Данные
Email	support@tomhunter.ru
Телефон	_____
Сайт	https://tomhunter.ru