

Общество с ограниченной ответственностью
«Инфрасек»

Infrasec Deception

Инструкция по установке

Версия 1.2

ОГЛАВЛЕНИЕ

1. Системные требования.....3

2. Инфраструктура и сетевые взаимодействия.....5

3. Установка.....8

4. Активация лицензии.....8

.

1. Системные требования

1.1. Системные требования к Серверу контроля

Ресурс	**Минимум**
ОС	Linux x86-64 (Astra Linux SE 1.7, РЕД ОС 7.3, Ubuntu 22.04 LTS, Debian 12)
CPU	4 vCPU
RAM	8 Гбайт
Диск	40 Гбайт свободного места

1.2 Минимальные системные требования к Узлу ловушек

Ресурс	**Минимум**
ОС	Linux x86-64 (Astra Linux SE 1.7, РЕД ОС 7.3, Ubuntu 22.04 LTS, Debian 12)
CPU	1 vCPU
RAM	2 Гбайт
Диск	4 Гбайт свободного места

Полный перечень сетевых взаимодействий всех компонентов решения, включая Защищаемые хосты и DDProxy, приведён в разделе 2.

2. Инфраструктура и сетевые взаимодействия

Перед установкой убедитесь, что между компонентами решения разрешены сетевые взаимодействия, перечисленные в настоящем разделе. Правила межсетевых экранов рекомендуется настроить до запуска установщика.

2.1. Состав решения

Компонент	**Назначение**
Сервер контроля (Control Plane)	Управляющий сервер: веб-интерфейс, приём и обработка событий от агентов, управление ловушками и приманками.
Node	Агент, на который распространяются ловушки.
RealOS	Агент RealOS-ловушки — полноценный узел-приманка с реальной операционной системой.
Agentless Node	Узел, на котором ловушки развёрнуты без установки агента.
Protected Host (Защищаемый хост)	Рабочая станция или сервер, на которые распространяются приманки и canary-токены.
DDProxy	Прокси-сервис для подключения удалённых (частных) сетей, не имеющих прямой связности с Сервером контроля. Терминирует трафик агентов сегмента и передаёт его на Сервер контроля по mTLS (8078/tcp).

2.2. Схема сетевого взаимодействия

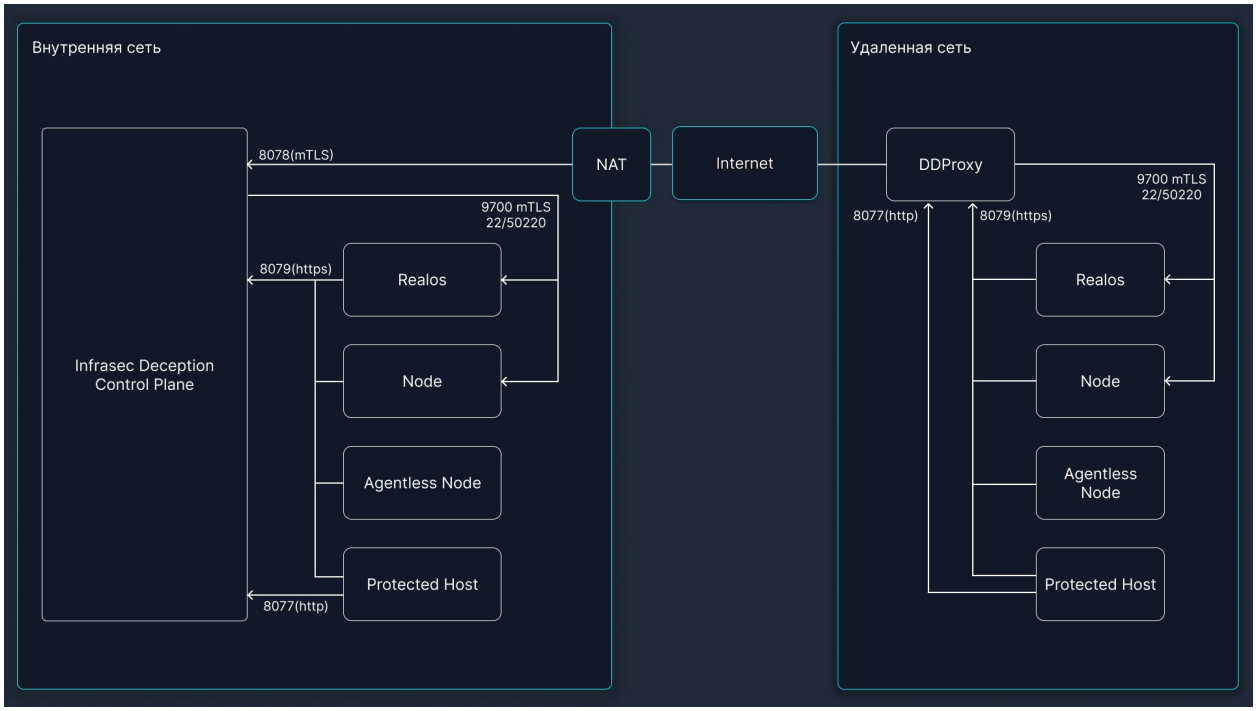

Рисунок 1 — Схема сетевого взаимодействия компонентов Infrasec Deception

2.3. Матрица сетевых доступов

Источник	**Получатель**	**Назначение**	**Протокол/порт**
Сеть Infrasec Deception			
Node	Сервер контроля	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
Сервер контроля	Node	Установка Node	SSH (22/tcp)
		Проверка установки Node	SSH (50220/tcp)
		Управление	mTLS (9700/tcp)
RealOS	Сервер контроля	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
Сервер контроля	RealOS	Установка RealOS	SSH (22/tcp)
		Проверка установки RealOS	SSH (50220/tcp)
		Управление	mTLS (9700/tcp)
Agentless Node	Сервер контроля	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)

Источник	Получатель	Назначение	Протокол/порт
Protected Host	Сервер контроля	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
		Обращения canary-токенов	HTTP (8077/tcp)
Частная сеть (за DDProxy)			
DDProxy	Сервер контроля	Управление агентами. Информация от агентов	mTLS (8078/tcp)
Node	DDProxy	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
DDProxy	Node	Установка Node	SSH (22/tcp)
		Проверка установки Node	SSH (50220/tcp)
		Управление	mTLS (9700/tcp)
RealOS	DDProxy	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
DDProxy	RealOS	Установка RealOS	SSH (22/tcp)
		Проверка установки RealOS	SSH (50220/tcp)
		Управление	mTLS (9700/tcp)
Agentless Node	DDProxy	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
Protected Host	DDProxy	Взаимодействие с сервисами Infrasec Deception	HTTPS (8079/tcp)
		Обращения canary-токенов	HTTP (8077/tcp)
Внешние ресурсы			
Сервер контроля	harbor.infra-sec.ru	Загрузка компонентов ПО при установке и обновлении	HTTPS (443/tcp)

Примечание. Агенты в удалённых сетях не обращаются к Серверу контроля напрямую: весь их трафик терминируется на DDProxy, который устанавливает с Сервером контроля единственное соединение по mTLS (8078/tcp).

3. Установка

3.1. Скопируйте архив на сервер (пример с scp)

scp production-server-main.zip user@server:/opt/

3.2. Произведите следующие команды на сервере:

sudo apt update && sudo apt install -y unzip

unzip production-server-main.zip

cd production-server-main

3.3. Запустите установщик

sudo bash install-scripts/installing.sh

Во время установки система запросит:

1) IP-адрес сервера контроля (адрес, по которому будут собираться данные от киберловушек).
2) Логин и токен для доступа к Harbor. Аутентификационные данные направляются вместе с установочным пакетом по электронной почте.

3.4. После завершения появится сообщение:

«*Сервис Infrasec Deception успешно установлен!*»

В терминал будут выведены учётные записи для входа в веб-интерфейс.

При первом входе необходимо сменить пароль.

4. Активация лицензии

4.1. В веб-интерфейсе перейдите Настройки → Лицензия.

4.2. Скопируйте отображённый challenge-код.

4.3. Отправьте письмо на license@infra-sec.ru с корпоративной почты следующего содержания:

Тема: Активация лицензии

Номер договора: <ваш_номер>

Challenge-код: <скопированный_код>

4.4. Получите файл <Компания>.license в ответном письме.

4.5. Загрузите его в блоке Активация лицензии.

4.6. Система готова к работе!