ИНТЕЛЛЕКТУАЛЬНЫЙ СЕТЕВОЙ ЭКРАН ДЛЯ ЗАЩИТЫ ИИ-ПРИЛОЖЕНИЙ SOLIDWALL AI SECURITY GATEWAY

Руководство по установке

Листов: 7

2026 г.

АННОТАЦИЯ

Настоящий документ является руководством по установке и описывает установку интеллектуального сетевого экрана для защиты ИИ-приложений SolidWall AI Security Gateway (далее по тексту — SolidWall AI Security Gateway).

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ 4

1.1 Область применения 4

1.2 Краткое описание возможностей 4

2 УСТАНОВКА SOLIDWALL AI SECURITY GATEWAY 5

2.1 Аргументы командной строки 5

2.2 Поддерживаемые сценарии 6

2.3 Запуск 6

2.3.1 Интерактивный режим (по умолчанию) 6

2.3.2 Только preflight-проверки 6

2.3.3 Генерация файла inventory без запуска установки 6

2.3.4 Повторный запуск по сохранённому файлу inventory 6

2.3.5 Политика установки коллекций 7

1 ВВЕДЕНИЕ

1.1 Область применения

Область применения программы для ЭВМ «Интеллектуальный сетевой экран для защиты ИИ-приложений SolidWall AI Security Gateway» (сокращенное наименование программы для ЭВМ: «SolidWall AI Security Gateway» (далее – SolidWall AI Security Gateway)) – мониторинг состояния защищённости ИИ-приложений.

1.2 Краткое описание возможностей

SolidWall AI Security Gateway является межсетевым экраном прикладного уровня и предназначен для защиты ИИ-приложений от интернет-угроз.

SolidWall AI Security Gateway выполняет следующие функции:

- анализ трафика веб-приложений с искусственным интеллектом и обнаружение атак (вторжений);
- блокирование попыток сетевых атак при работе с веб-приложениями с искусственным интеллектом;
- контроль доступа к функциям и журналирование действий пользователей защищаемых приложений с искусственным интеллектом;
- обнаружение подозрительной активности пользователей веб-приложений с искусственным интеллектом;
- автоматическая настройка защитных механизмов «SolidWall AI Security Gateway», версия 1.0 под конкретное защищаемое приложение с искусственным интеллектом (обучение);
- контроль и фильтрацию трафика, включая запросы пользователя к языковым моделям;
- идентификацию и аутентификацию пользователей, являющихся работниками оператора;
- регистрацию событий безопасности (аудит);
- бесперебойное функционирование и восстановление;
- тестирование и контроль целостности;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации.

2 УСТАНОВКА SOLIDWALL AI SECURITY GATEWAY

Для установки SolidWall AI Security Gateway необходимы следующие компоненты:

- операционная система Ubuntu 22.04 или Astra Linux 1.8;
- дистрибутив в виде архива «*.tgz» объемом порядка 1 ГБ.

Дистрибутив ПО SolidWall AI Security Gateway необходимо загрузить по предоставленной после подписания договора ссылке. Для скачивания дистрибутива требуется авторизоваться с использованием выданных учётных данных (логина и пароля). Перед началом установки необходимо создать пользователя операционной системы с правами администратора, после чего скопировать архив в домашний каталог пользователя и выполнить распаковку. Также необходимо настроить параметры сетевого интерфейса в соответствии с требованиями, указанными в эксплуатационной документации, переданной вместе с дистрибутивом.

Для развертывания используется WAF Installation Wizard — интерактивный мастер установки (скрипт), запускающий установку SolidWall AI Security Gateway через программный инструмент Ansible.

Процесс установки с помощью WAF Installation Wizard включает следующие этапы:

1. Проверка окружения (наличие Ansible, соответствие версии, доступность сценариев playbook).
2. Проверка и, при необходимости, установка Ansible-коллекций в каталог проекта.
3. Выбор параметров установки в диалоговом режиме (интерактивный мастер).
4. Выполнение preflight-проверок для удалённых хостов (проверка DNS, выполнение Ansible ping, доступность по SSH).
5. Генерация inventory-файла и его сохранение в директорию `inventories/`.
6. Вывод итоговой сводки параметров и запуск установки.
7. Обработка ошибок: в случае ошибки файл inventory сохраняется и выводится команда повторного запуска.

2.1 Аргументы командной строки

Аргументы командной строки приведены в таблице 1.

Таблица 1 – Аргументы командной строки

Аргумент	Описание
`--preflight-only`	Только preflight-проверки, без запуска установки
`--inventory PATH`	Путь к файлу inventory: если файл существует — мастер загружает его параметры; если отсутствует — создаёт новый по указанному пути

2.2 Поддерживаемые сценарии

Поддерживаемые сценарии установки следующие:

- **Локальная установка** — все компоненты развёртываются на localhost.
- **Single-host** — один удалённый хост для развёртывания компонентов управления `management` и фильтрации `filter`.
- **Multi-host** — разные хосты для развёртывания компонентов управления `management` и фильтрации `filter`, при этом хост управления может быть только один.
- **Только inventory** — генерация файла inventory без запуска установки (playbook).
- **Повторный запуск** — установка по ранее сохранённому файлу inventory.

2.3 Запуск

Для начала работы необходимо перейти в установочный каталог, запустить скрипт и следовать указаниям мастера настройки.

2.3.1 Интерактивный режим (по умолчанию)

Запуск установки осуществляется следующей командой:

```
python3 install_wizard.py
```

Далее последуют запросы от системы для настройки параметров установки.

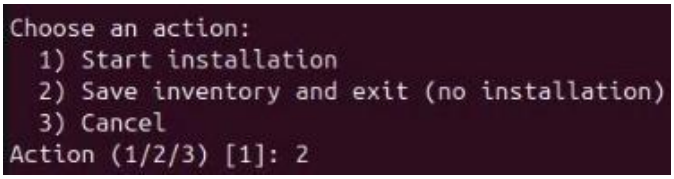
2.3.2 Только preflight-проверки

Для выполнения всех проверок (окружение, коллекции, доступность хостов) и сохранения файла inventory без запуска установки используется следующая команда:

```
python3 install_wizard.py --preflight-only
```

2.3.3 Генерация файла inventory без запуска установки

Для генерации файла inventory без запуска установки, необходимо выбрать пункт меню № 2 «Save inventory and exit» (см. снимок экрана 1).



Снимок экрана 1 — Пункт № 2 «Save inventory and exit»

2.3.4 Повторный запуск по сохранённому файлу inventory

Для запуска установки по сохранённому файлу inventory используется следующая команда:

```
python3 install_wizard.py --inventory
inventories/inventory_20250401_123456.yml
```

При этом мастер установки пропускает шаги интерактивного ввода параметров.

2.3.5 Политика установки коллекций

Ansible-коллекции устанавливаются в каталог проекта `.ansible/collections/`, не затрагивая глобальное окружение.