SecDNS

Руководство системного администратора

Версия 1.0

Содержание

1 ОБЩИЕ СВЕДЕНИЯ О СЕРВИСЕ 3

2 АППАРАТНЫЕ ТРЕБОВАНИЯ 4

2.1 Требования к Прокси-Серверу (DNS Proxy) 4

2.2 Требования к Центру Управления (Control Center) 4

2.3 Дополнительные требования 4

3 СКАЧИВАНИЕ И ИНСТАЛЛЯЦИЯ УСТАНОВОЧНЫХ ФАЙЛОВ 5

4 ПРОВЕРКА ФУНКЦИОНИРОВАНИЯ 6

1 Общие сведения о сервисе

SecDNS — это сервис фильтрации пользовательских DNS-запросов, обладающий следующим функционалом:

- Управление доступом в интернет на основе правил фильтрации на основе заданных категорий доменов.
- Работа по «чёрному» и «белому» спискам доменов. Сервис позволяет создавать собственные списки сайтов, доступ к которым будет всегда разрешен или запрещен. «Черный» список помогает блокировать конкретные сайты, «белый» — добавляет ресурс в доверенные.
- Настройка страницы блокировки. Можно использовать как стандартную страницу блокировки, так и настроить собственную страницу, на которую происходит переход в случае запроса доступа к запрещенному ресурсу.
- Защита от интернет-угроз. Автоматическая система выявления вредоносных ресурсов защищает сеть от многочисленных интернет-угроз: вирусных и фишинговых сайтов, ботнетов и криптомайнинговых атак.

На рисунке 1 изображен вариант подключения и разворачивания сервиса SecDNS в инфраструктуре Компании.

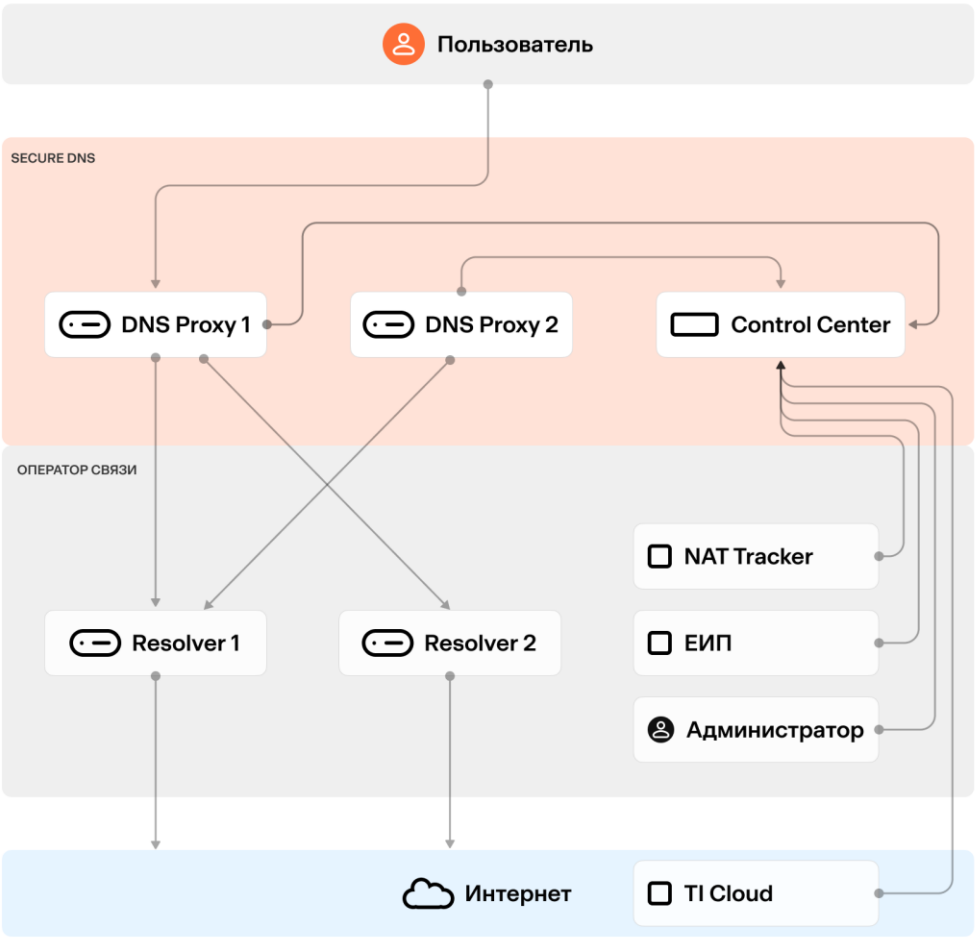

Рисунок 1 - Вариант подключения сервиса SecDNS в инфраструктуре Компании

2 Аппаратные требования

Для обеспечения стабильной и надежной работы сервиса SecDNS, необходимо учитывать аппаратные требования, которые могут варьироваться в зависимости от масштаба и нагрузки на систему. В данном пункте представлены рекомендуемые требования для ключевых компонентов сервиса: прокси-сервера и центра управления (Control Center) развернутых на виртуальных машинах.

2.1 Требования к Прокси-Серверу (DNS Proxy)

Прокси-сервер (DNS Proxy) играет ключевую роль в фильтрации и мониторинге DNS-трафика. Его производительность напрямую влияет на общую производительность системы. Рекомендуемые требования к DNS Proxy:

- Процессор: 8 vCPU.
- Оперативная память: 16 ГБ vRAM.
- Диск: 50 ГБ HDD.
- Количество запросов: 30000 RPS.
- Операционная система: РЕД ОС 7+, Debian 11+, Ubuntu 20+.
- Платформа контейнеризации: Docker 22+.

2.2 Требования к Центру Управления (Control Center)

Центр управления (Control Center) отвечает за конфигурацию, мониторинг и управление всеми компонентами сервиса SecDNS. Его производительность и надежность критически важны для эффективного управления системой. Рекомендуемые требования к Control Center:

- Минимальная конфигурация без обеспечения отказоустойчивости: 1 VM (16 vCPU, 32GB vRAM, 300 GB Storage).
- Минимальная конфигурация с обеспечением отказоустойчивости: 3 VM (8 vCPU, 32GB vRAM, 300 GB Storage).

2.3 Дополнительные требования

Резервное копирование: Регулярное резервное копирование баз данных и конфигурационных файлов и журналов.

Мониторинг: Установка и настройка систем мониторинга для отслеживания производительности и состояния серверов.

Безопасность: Применение мер по защите включая использование брандмауэров, аутентификации, антивирусных решений и регулярное обновление ПО.

Масштабируемость: Рассмотрение возможности развертывания кластеров для обеспечения высокой доступности и масштабируемости.

3 Скачивание и инсталляция установочных файлов

Для получения установочного комплекта необходимо обратиться к специалистам по сопровождению по адресу электронной почты support.tic@rt-solar.ru. Необходимо распаковать полученный архив локально в папку из которой планируется запускать Docker-образ агента.

Установочный комплект включает в себя Docker-образа контейнеров и конфигурационные файлы, с помощью которых можно настраивать агента без внесения изменений в программный код.

Необходимо сохранить в одной папке все полученные файлы. Для запуска агента должно быть установлена платформа контейнеризации Docker версии 22+. Для загрузки SecDNS необходимо перейти в папку с распакованными файлами и ввести команду:

$ startup.bat для ОС Windows или $ startup.sh для ОС Linux

Для проверки того, что контейнер успешно загружен введите команду:

$ docker image list

Если в консоли появилась информация о запуске контейнеров (Рисунок 2), значит сервис SecDNS успешно загружен.

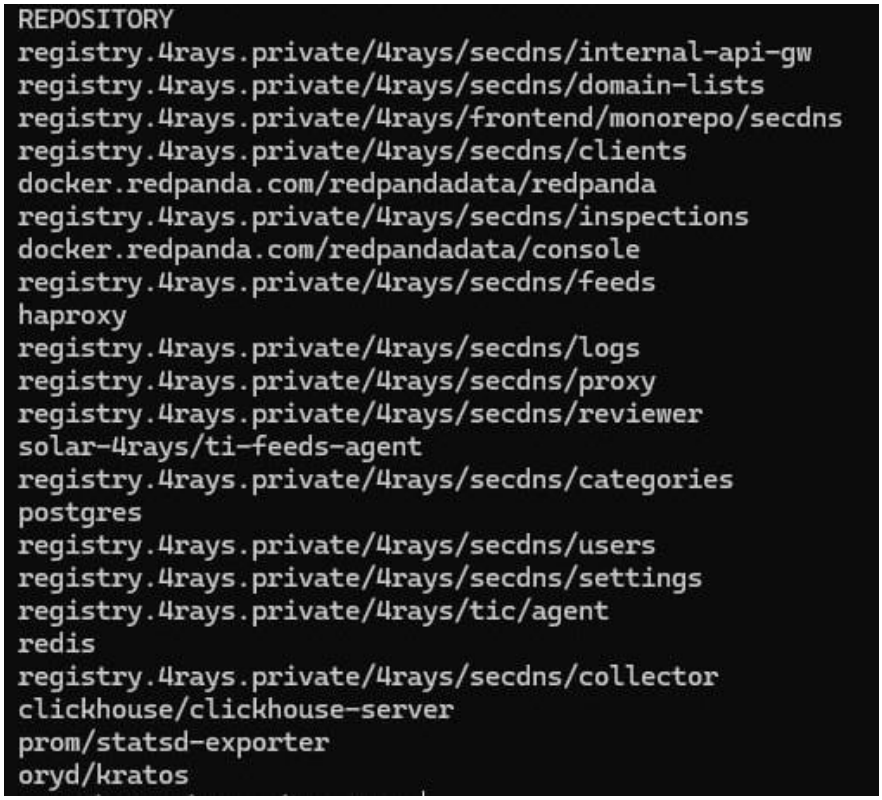

Рисунок 2 – Контейнеры SecDNS

4 Проверка функционирования

Для проверки функционирования откройте браузер и введите в адресную строку:

Localhost:8080 или адрес, на котором будет развернут сервис.

В браузер загрузиться сервис SecDNS и станет доступно окно аутентификации (Рисунок 3).

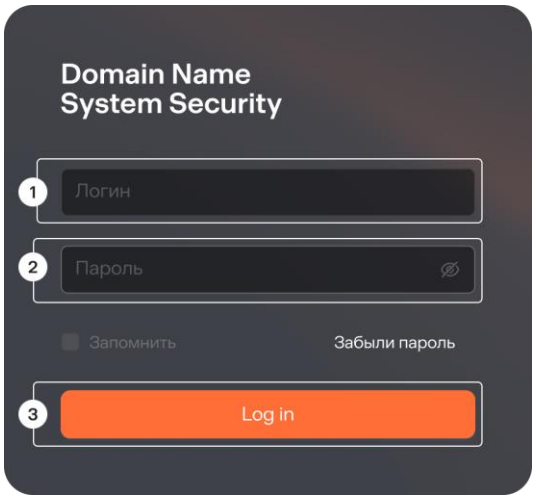

Рисунок 3 - Экран однофакторной аутентификации

Необходимо ввести ваш логин в поле (1) и пароль в поле (2) и нажать кнопку «Log in» (3).

После аутентификации становится доступен Интерфейс управления Компаниями (Рисунок 4).

Для дальнейшей работы необходимо в интерфейсе управления Компаниями нажать кнопку «Добавить компанию», в появившемся окне создать новую компанию, название которой соответствует названию вашей компании.

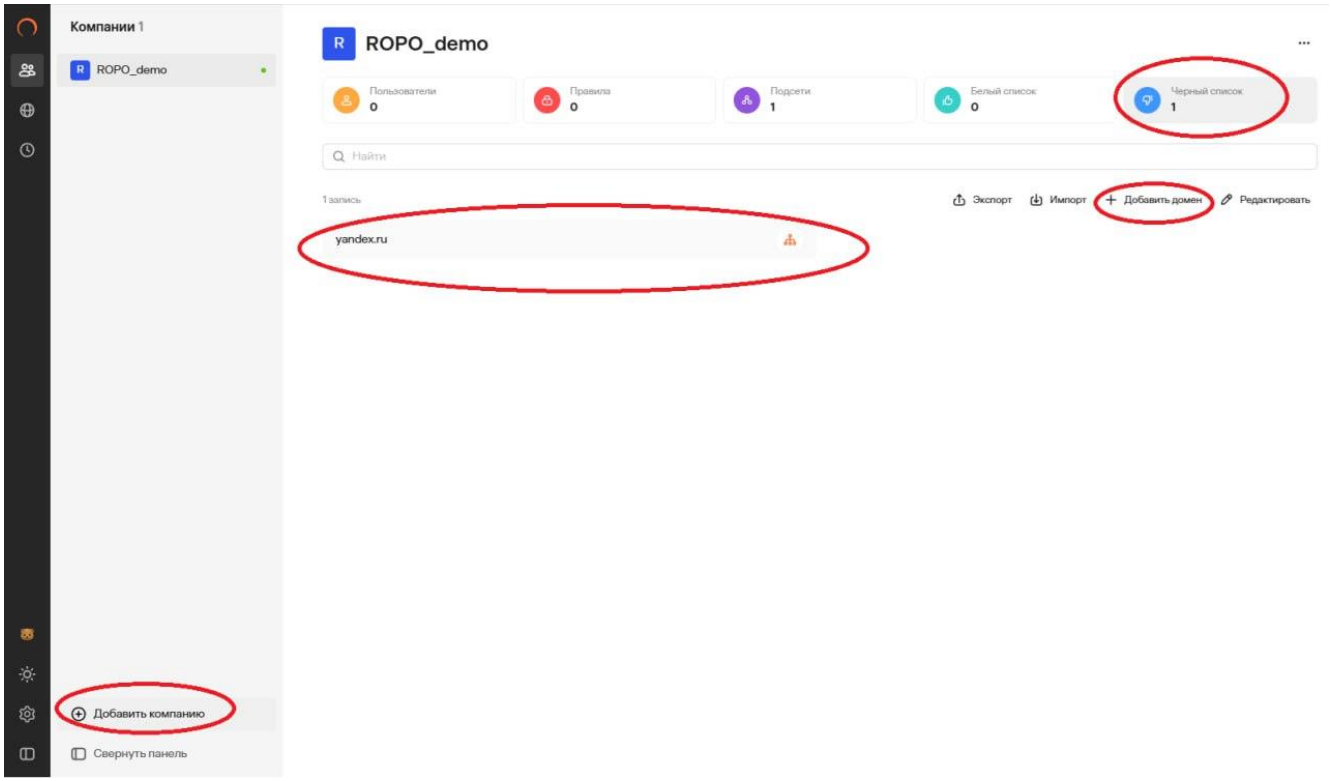

Рисунок 4 – Интерфейс управления Компаниями

Далее необходимо ввести команду:

$ nslookup yandex.ru 127.0.0.1

И убедиться, что сайт доступен. После этого в Интерфейсе управления Компаниями (Рисунок 3) необходимо перейти на вкладку «Черный список», нажать кнопку «Добавить домен» и добавить в черный список домен Yandex.ru.

После этого в командную строку снова ввести команду:

$ nslookup yandex.ru 127.0.0.1

И убедиться, что домен заблокирован.

Так же можно перейти на страницу логов и убедиться, что информация о доступе к домену до блокировки и после доступна в Журнале событий (Рисунок 5).

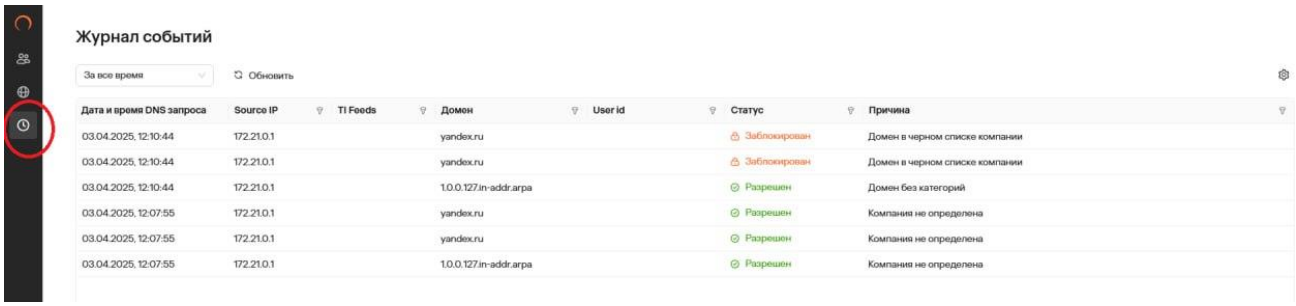

Рисунок 5 – Журнал событий

Если в логах есть информация о блокировке доступа, значит сервис работает.

Для остановки сервиса введите команду:

$ docker compose -f docker-compose.proxy.yaml down --volumes --remove-orphan