

SecDNS

Инструкция по установке для экспертов

Версия 1.0

Скачивание установочных файлов

Для получения установочного комплекта необходимо перейти по ссылке <https://drive.rtsolar.ru/s/tiZqNGzQ4P5Yi68> и ввести пароль ZcFHH58bGc. Далее войти в папку SecDNS v1.0 и скачать файл solar-secdns-v1.0.0.zip. Необходимо распаковать данный архив локально в папку из которой планируется запускать Docker-образ агента. Пароль от архива - 7MidMFMD06A1.

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

Инсталляция установочных файлов

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:

\$.\start.cmd для ОС Windows или \$ start.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 1), значит сервис SecDNS успешно загружен.

```
REPOSITORY
registry.4rays.private/4rays/secdns/internal-api-gw
registry.4rays.private/4rays/secdns/domain-lists
registry.4rays.private/4rays/frontend/monorepo/secdns
registry.4rays.private/4rays/secdns/clients
docker.redpanda.com/redpandadata/redpanda
registry.4rays.private/4rays/secdns/inspections
docker.redpanda.com/redpandadata/console
registry.4rays.private/4rays/secdns/feeds
haproxy
registry.4rays.private/4rays/secdns/logs
registry.4rays.private/4rays/secdns/proxy
registry.4rays.private/4rays/secdns/reviewer
solar-4rays/ti-feeds-agent
registry.4rays.private/4rays/secdns/categories
postgres
registry.4rays.private/4rays/secdns/users
registry.4rays.private/4rays/secdns/settings
registry.4rays.private/4rays/tic/agent
redis
registry.4rays.private/4rays/secdns/collector
clickhouse/clickhouse-server
prom/statsd-exporter
oryd/kratos
```

Рисунок 1 – Контейнеры SecDNS

Запуск и проверка функционирования

Откройте браузер и введите в адресную строку:

Localhost:8080

В браузер загрузится сервис SecDNS и станет доступно окно аутентификации (Рисунок 2).

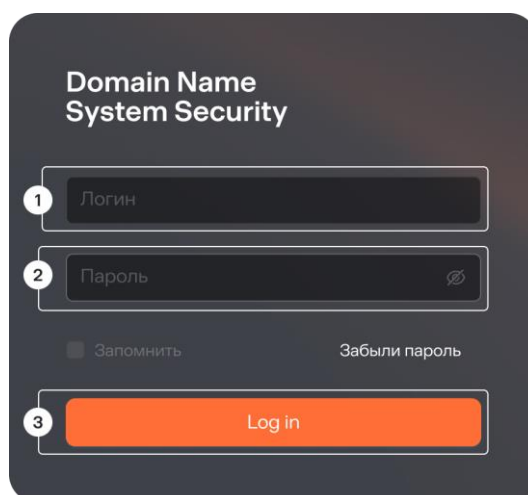


Рисунок 2 - Экран однофакторной аутентификации

Необходимо ввести логин **ux@test.com** в поле (1), пароль **the-password** в поле (2) и нажать кнопку «Log in» (3).

После аутентификации становится доступен Интерфейс управления Компаниями (Рисунок 3).

Для дальнейшей работы необходимо в интерфейсе управления Компаниями нажать кнопку «Добавить компанию», в появившемся окне создать новую компанию, например, **ROPO-demo**.

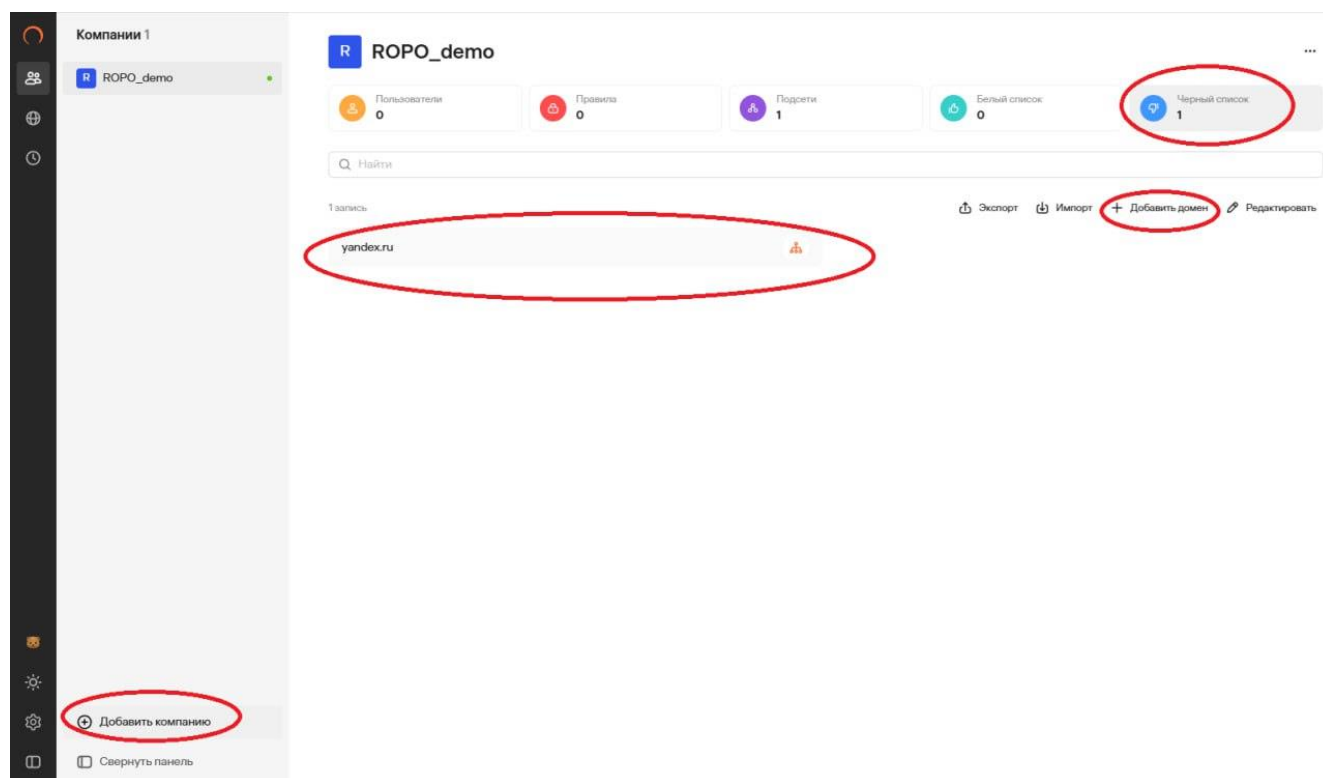


Рисунок 3 – Интерфейс управления Компаниями

Далее необходимо ввести команду:

```
$ nslookup yandex.ru 127.0.0.1
```

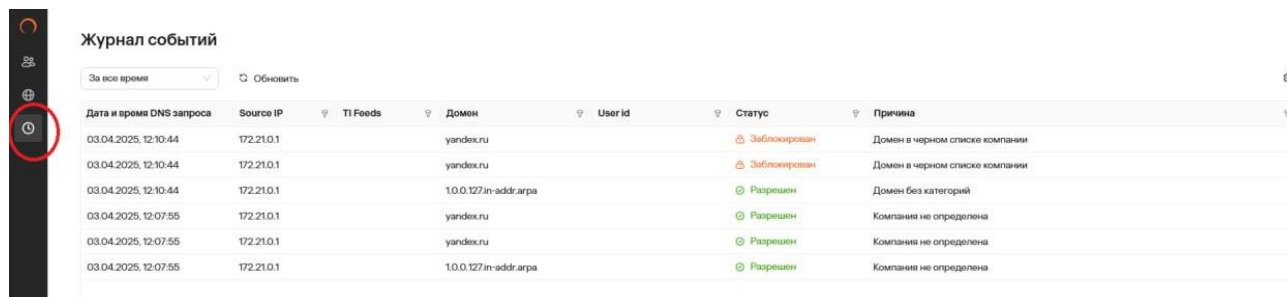
И убедиться, что сайт доступен. После этого в Интерфейсе управления Компаниями (Рисунок 3) необходимо перейти на вкладку «Черный список», нажать кнопку «Добавить домен» и добавить в черный список домен Yandex.ru.

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 4).



Дата и время DNS запроса	Source IP	TTL Feeds	Домен	User id	Статус	Причина
03.04.2025, 12:10:44	172.21.0.1		yandex.ru		Заблокирован	Домен в черном списке компании
03.04.2025, 12:10:44	172.21.0.1		yandex.ru		Заблокирован	Домен в черном списке компании
03.04.2025, 12:10:44	172.21.0.1		1.0.0.127in-addr.arpa		Разрешен	Домен без категорий
03.04.2025, 12:07:55	172.21.0.1		yandex.ru		Разрешен	Компания не определена
03.04.2025, 12:07:55	172.21.0.1		yandex.ru		Разрешен	Компания не определена
03.04.2025, 12:07:55	172.21.0.1		1.0.0.127in-addr.arpa		Разрешен	Компания не определена

Рисунок 4 – Журнал событий

Для остановки SecDNS необходимо перейти в папку с распакованными файлами и ввести команду:

```
$ .\stop.cmd для ОС Windows или $ stop.sh для ОС Linux
```

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.

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+.

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).

Контакты технических специалистов

Контакты технических специалистов, которые могут проконсультировать по процессу развёртывания и настройки ПО и его функционирования: специалисты по сопровождению, адрес электронной почты: support.tic@rt-solar.ru.