ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ИНСАЙТТЕХСОЛЮШНС"

Руководство по первичной настройке Intecso

Оглавление

1. Введение

В этом разделе представлено руководство по первичной настройке Intecso, универсального решения для управления сетевым трафиком. Intecso обеспечивает широкие возможности для настройки маршрутизации, безопасности сети, а также мониторинга и администрирования сетевой инфраструктуры. Важно отметить, что под Intecso подразумевается специализированное программное обеспечение, предназначенное для управления сетевым оборудованием.

1.1 Общие сведения о Intecso

Intecso — это мощное и гибкое программное решение для сетевого администрирования. Оно предлагает функции, такие как маршрутизация, межсетевой экран, NAT, VPN и многие другие. Основное предназначение Intecso — обеспечение безопасности и эффективности сетевого трафика. Система обладает интуитивно понятным веб-интерфейсом, который позволяет администраторам легко настраивать и контролировать различные аспекты сетевой инфраструктуры.

1.2 Цели и задачи настройки

Основная цель настройки Intecso — обеспечение надежной и безопасной работы сети. Оно включает в себя настройку маршрутизации, фильтрацию трафика, настройку VPN, контроль доступа и мониторинг сетевой активности. Более детально задачи настройки включают в себя:

- Инициализацию и базовую настройку системы.
- Настройку правил межсетевого экрана для обеспечения безопасности.
- Конфигурацию маршрутизации и NAT для оптимизации трафика.

- Установку и настройку VPN для защищенного доступа.
- Мониторинг и администрирование сетевой активности.

2. Подготовка к настройке

2.1 Доступ к Intecso через LAN интерфейс

Описание: Для первичной настройки Intecso необходимо подключение к устройству через LAN интерфейс. После установки Intecso доступ к веб-интерфейсу осуществляется через локальную сеть, обычно это адрес 192.168.1.1 (или другой IP в зависимости от настроек сети).

Шаги:

1. Подключение к Intecso через Ethernet-кабель.
2. Ввод IP-адреса Intecso в браузере для доступа к веб-интерфейсу.

2.2 Необходимые условия и предварительные требования

Основные требования:

1. Наличие компьютера с сетевым интерфейсом Ethernet.
2. Ethernet-кабель для подключения к LAN порту Intecso.
3. Наличие браузера для доступа к веб-интерфейсу.

Предварительные настройки:

1. Убедитесь, что IP-адрес компьютера находится в той же подсети, что и Intecso (например, 192.168.1.x).
2. Отключите все файрволы и блокировщики рекламы, которые могут мешать доступу к веб-интерфейсу Intecso.
3. При необходимости настройте статический IP-адрес на компьютере для упрощения доступа к Intecso.

Примечания:

- Опционально можно настроить доступ к Intecso через Wi-Fi, если эта возможность поддерживается устройством.
- Важно убедиться в правильности подключения кабеля и исправности сетевой карты на компьютере.

3. Основные шаги настройки Intecso

3.1 Изменение пароля пользователя "root"

При первичной настройке Intecso крайне важно изменить пароль для пользователя "root", чтобы обеспечить безопасность системы. Для этого:

1. Войдите в меню «**System > Access > Users**».
2. Нажмите на кнопку «**Edit user**» (иконка с изображением карандаша) напротив пользователя "root".
3. В открывшемся окне введите новый пароль в поле «**Password**» и подтвердите его.
4. Завершите процесс, нажав на кнопку «**Save**» внизу страницы.

Это обеспечит первоначальную безопасность вашего Intecso.

3.2 Прописывание доступа к веб-интерфейсу Intecso с определённого IP

Для обеспечения контролируемого доступа к веб-интерфейсу Intecso можно ограничить доступ только с определенных IP-адресов. Это делается следующим образом:

1. Перейдите в «**Firewall > Rules > WAN**».
2. Нажмите на кнопку «**Add**» для добавления нового правила. Заполните поля согласно следующей таблице:

Action	Pass	
Interface	WAN	
Address Family	IPv4	
Protocol	TCP	
Source	Single host or Network	указывается IP-адрес, с которого нужно разрешить доступ к веб-интерфейсу Intecso
Destination	WAN address	
Destination Port Range	HTTPS	разрешение доступа только по https

Таблица 1 – Настройка доступа с определённого IP

3. Сохраните правило, нажав на кнопку «**Save»**, и примените изменения, нажав на «**Apply changes»**.

Это позволит обеспечить контролируемый доступ к устройству.

3.3 Настройка правил Firewall

Настройка правил брандмауэра (Firewall) является ключевым элементом в обеспечении безопасности сети. Основные шаги:

1. **Блокировка несанкционированного доступа**: По умолчанию доступ через WAN интерфейс блокируется. Однако, если вы сталкиваетесь с

ошибкой *"The HTTP_REFERER does not match the predefined settings"* при попытке входа, это можно исправить следующим образом:

- Перейдите в «**System > Settings > Administration**».
- Активируйте опцию «**Disable HTTP_REFERER enforcement check**».
- Нажмите «**Save**», чтобы сохранить изменения.

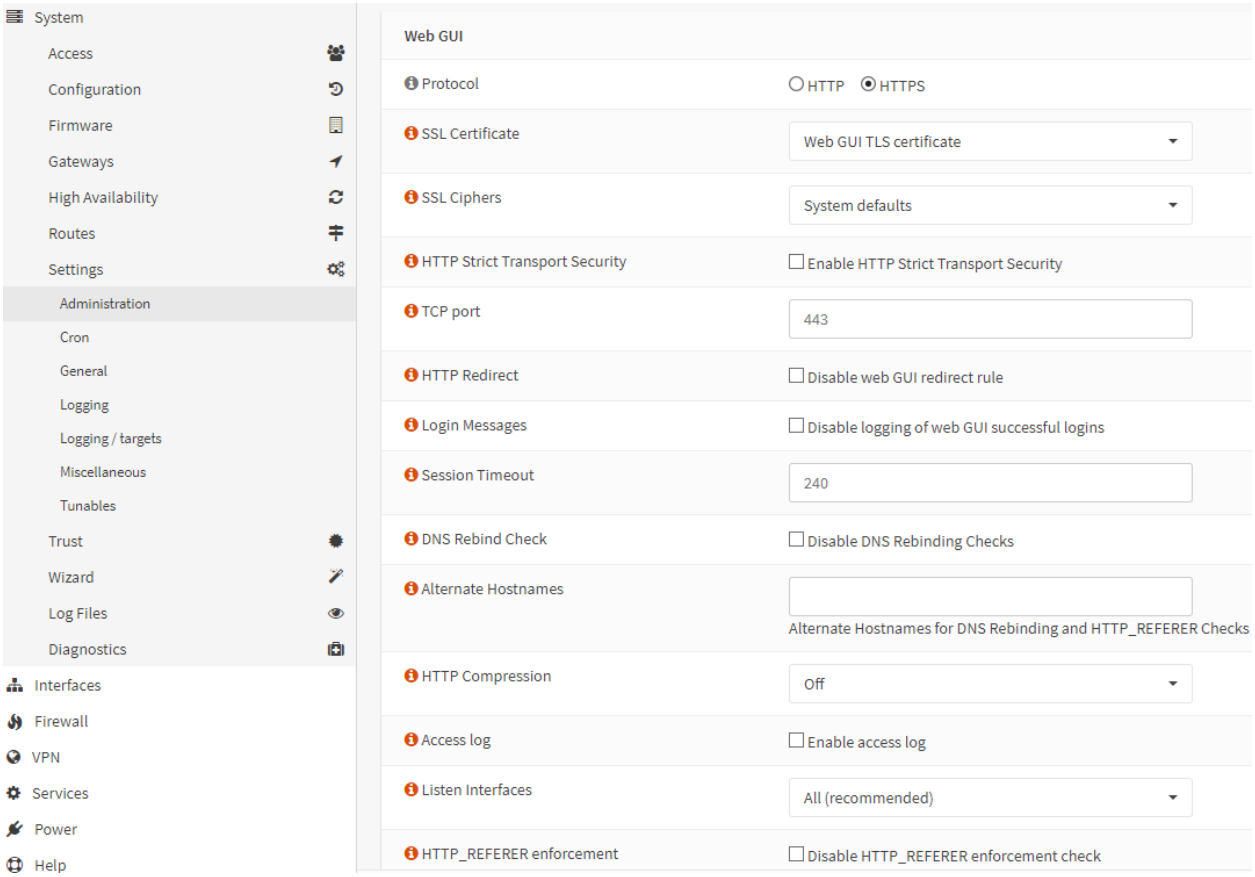

Рисунок 1 – Блокирование несанкционированного доступа

2. **Настройка правил для специфических услуг**: Например, если вы хотите разрешить доступ к определенным сервисам через Интернет, следует создать соответствующие правила в разделе «**Firewall > Rules**». Выберите соответствующий интерфейс (например, WAN или LAN) и добавьте правила, определяющие тип трафика (TCP/UDP), порты и адреса назначения.

Рисунок 2 – Настройка правил файрвола

Эти шаги помогут настроить основные параметры безопасности вашего Intecso, обеспечивая как защиту, так и необходимую гибкость в управлении доступом к сетевым ресурсам.

4. Дополнительные настройки

4.1 Исправление ошибок доступа к веб-интерфейсу

При настройке и использовании Intecso в сетевой инфраструктуре могут возникать различные ошибки доступа к веб-интерфейсу. Эти ошибки часто связаны с конфигурацией сетевых правил, параметров безопасности или проблемами с сетевыми интерфейсами.

a. Настройка правил брандмауэра для доступа к веб-интерфейсу

При настройке доступа к веб-интерфейсу через WAN-интерфейс необходимо настроить правила брандмауэра в Intecso. Правила должны быть настроены таким образом, чтобы разрешить входящие подключения к веб-интерфейсу через HTTPS. Необходимо убедиться, что правило для доступа настроено на интерфейсе WAN с протоколом TCP и портом, указанным для HTTPS.

b. Исправление ошибок, связанных с HTTP_REFERER

При попытке доступа к веб-интерфейсу Intecso может возникнуть ошибка, связанная с HTTP_REFERER. Это может произойти, если веб-сервер

обнаруживает, что запрос пришел не с ожидаемого адреса. Чтобы решить эту проблему, можно отключить проверку HTTP_REFERER в настройках Intecso. Для этого необходимо перейти в раздел **«System > Settings > Administration»** и отметить опцию **«Disable HTTP_REFERER enforcement check»**.

4.2 Смена языка интерфейса

Смена языка интерфейса в Intecso позволяет адаптировать веб-интерфейс к потребностям пользователей, которые предпочитают работать с системой на их родном языке.

a. Выбор языка интерфейса

Для смены языка интерфейса необходимо перейти в меню **«System > Settings > General»**. В этом разделе находится выпадающий список с доступными языками. Выбрав нужный язык из списка, например, русский, пользователь может легко изменить язык интерфейса.

b. Применение и сохранение изменений

После выбора желаемого языка необходимо сохранить изменения, нажав на кнопку **«Save»** внизу страницы. Это приведет к изменению языка интерфейса на выбранный, обеспечивая более удобное взаимодействие пользователя с системой.

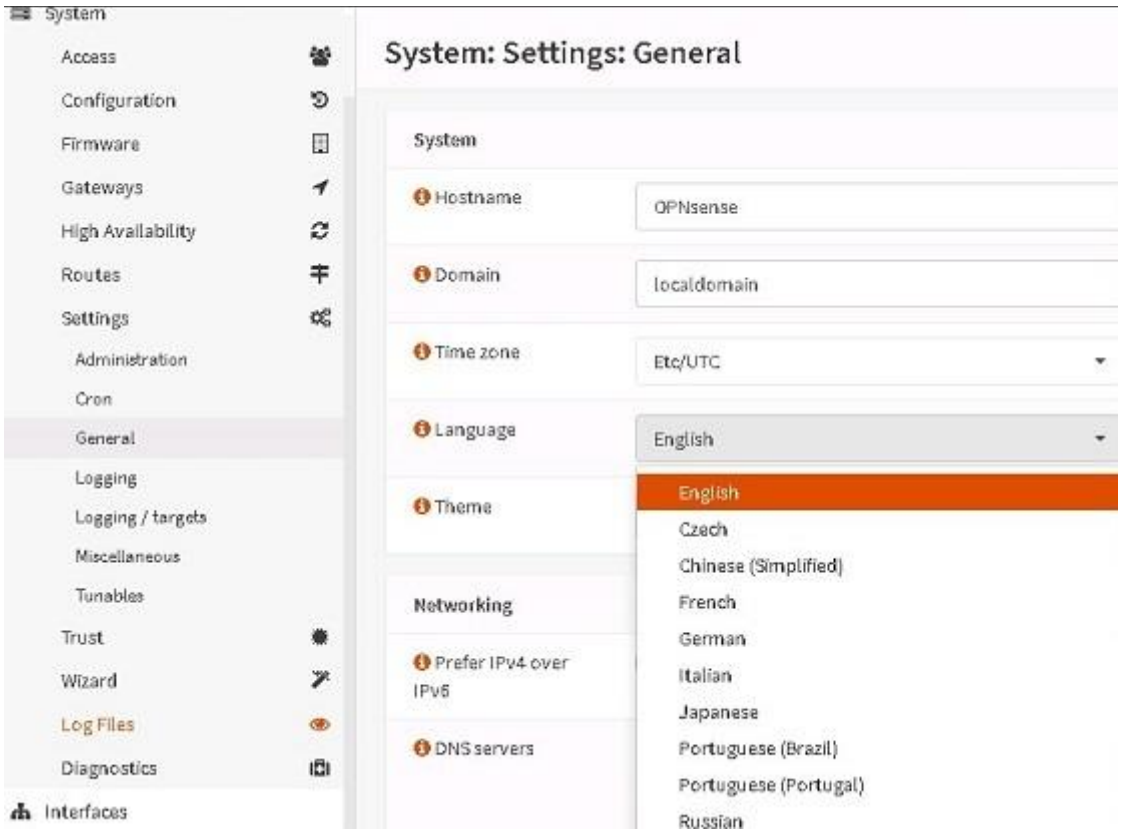

Рисунок 3 – Установка языка интерфейса

5. Конфигурация сети

В этом разделе мы рассмотрим процесс конфигурации сети для Intecso. Ключевыми аспектами являются использование мастера настройки для упрощения процесса и следование определенным рекомендациям для оптимизации работы сети.

5.1 Использование мастера настройки

Мастер настройки в Intecso представляет собой интуитивно понятный инструмент, который направляет пользователя через основные шаги конфигурации сети. Это удобный способ для быстрой и эффективной настройки сетевых параметров, особенно для новых пользователей.

а. Доступ к мастеру настройки

Для начала работы с мастером настройки перейдите в раздел **«System»** и выберите **«Wizard»**. Этот раздел предоставит последовательные шаги, которые необходимо выполнить для настройки сетевых параметров Intecso.

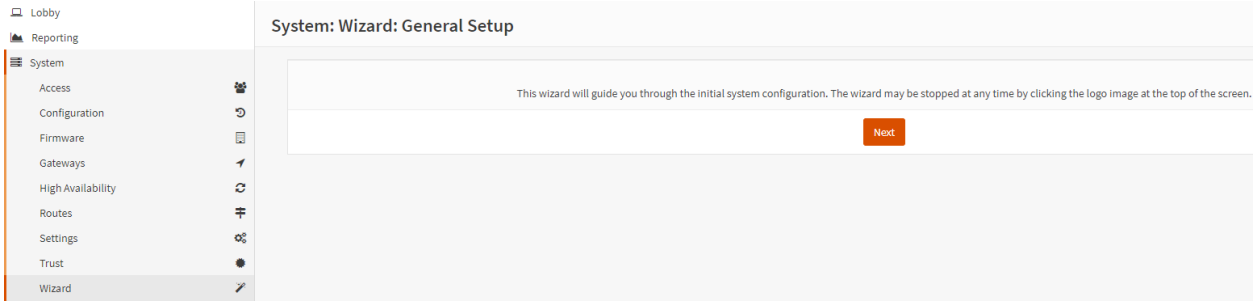

Рисунок 4 – Запуск мастера настройки

b. Шаги конфигурации

Мастер настройки предложит ряд шагов, включая настройку интерфейсов LAN и WAN, настройку DHCP-сервера, настройку правил брандмауэра и другие важные аспекты конфигурации сети. Просто следуйте указаниям на каждом шаге, внося необходимые данные.

5.2 Рекомендации по конфигурации

Правильная конфигурация сети имеет решающее значение для обеспечения надежности, безопасности и эффективности сетевой инфраструктуры.

a. Настройка сетевых интерфейсов

Убедитесь, что сетевые интерфейсы настроены правильно. Для интерфейса WAN обязательно настройте внешний IP-адрес и параметры подключения к Интернету. Для LAN-интерфейса важно настроить внутренний IP-адрес и параметры DHCP-сервера для распределения IP-адресов в локальной сети.

b. Безопасность и правила брандмауэра

Важно установить строгие правила брандмауэра для защиты сети. Данная группа настроек включает ограничение доступа к сети только необходимым сервисам и блокировку всех неавторизованных попыток доступа.

c. Резервное копирование и восстановление конфигурации

Рекомендуется регулярно создавать резервные копии конфигурации Intecso. В случае сбоев или ошибок это позволит быстро восстановить рабочее состояние системы.

d. Мониторинг и журналирование

Настройте систему мониторинга и журналирования для отслеживания состояния сети и обнаружения возможных проблем. Это позволит своевременно реагировать на сетевые инциденты и поддерживать стабильную работу системы.

6. Управление журналированием

Управление журналированием в Intecso – ключевой элемент в обеспечении безопасности и стабильности системы. Настройки журналирования включают в себя определение размера файлов журналов и управление их хранением.

6.1 Настройка размера файлов журналов

Размер файлов журналов влияет на количество информации, которое можно хранить и анализировать. В Intecso размер файлов журналов можно настроить, чтобы оптимизировать использование ресурсов и обеспечить достаточный объем данных для мониторинга и отладки.

a. Установка размера файлов журналов

В этом разделе вы найдете параметр для установки размера файлов журналов. Размер указывается в байтах.

По умолчанию Intecso хранит логи в 20 файлах размером около 500 КБ, чего может быть недостаточно. В этом случае рекомендуется увеличение размера файлов логов, что выполняется по следующему пути: **«System > Settings > Logging»**.

Размер указывается в байтах: зададим, например, размер одного файла в 5 МБ, что составит 5000000. Для применения настроек нужно нажать **«Сохранить»** внизу страницы.

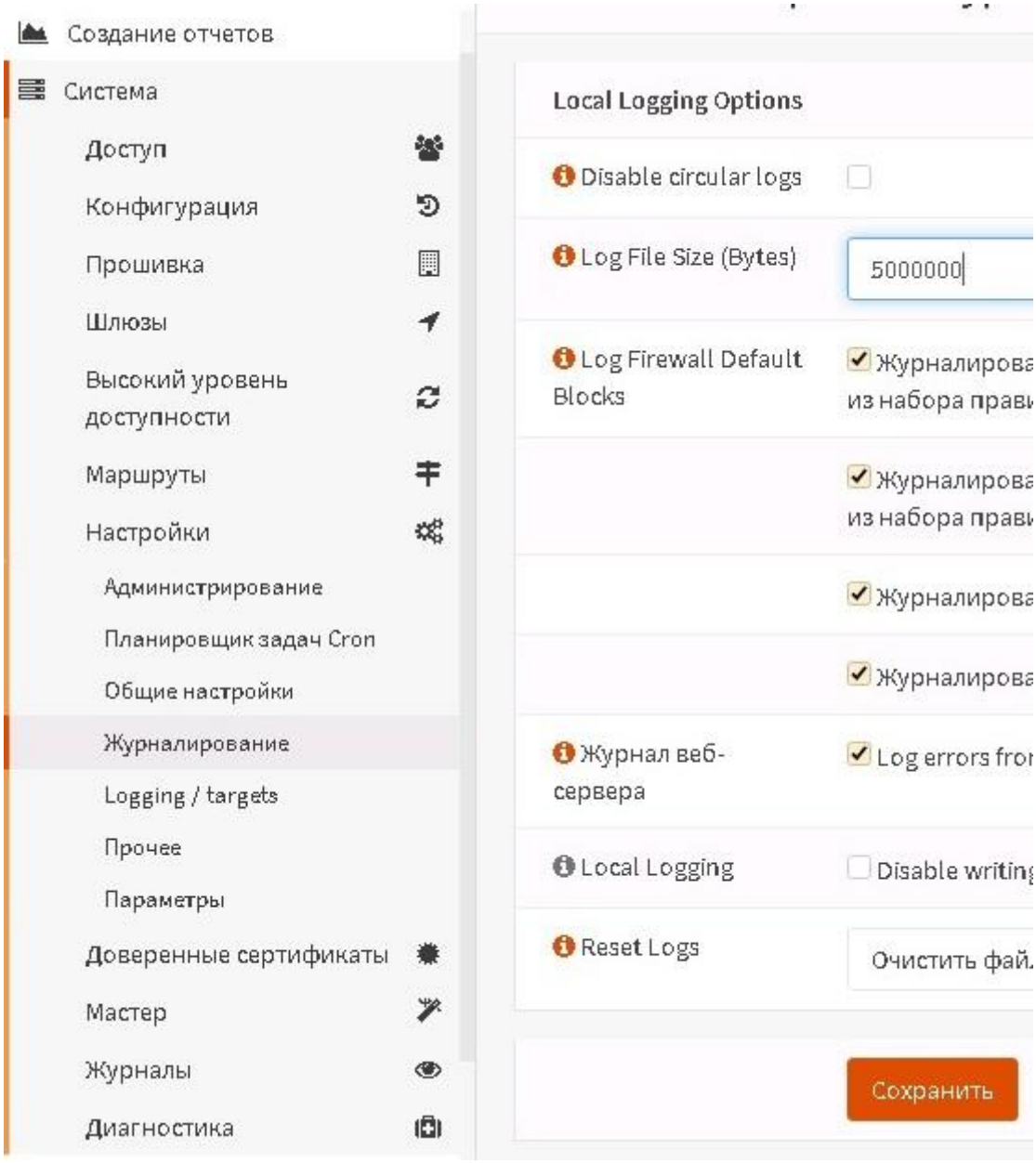

Рисунок 5 – Настройки журналирования

Однако вместо указания размера логов можно указать, за какое количество дней хранить логи, для чего нужно поставить галочку **«Disable circular logs»** и ввести количество дней, в течении которых будут храниться логи:

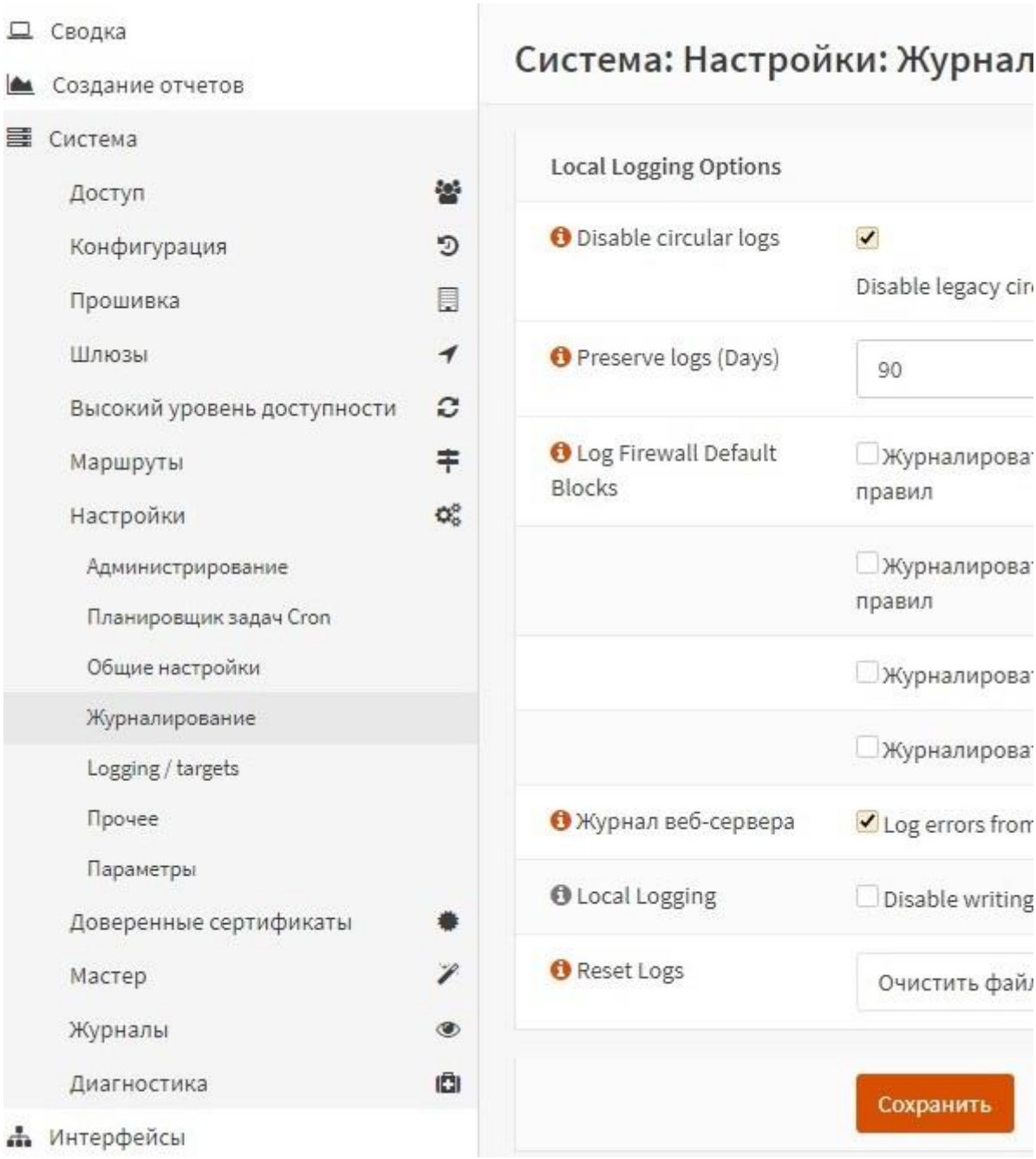

Рисунок 6 – Настройки журналирования (2)

После установки желаемого размера файлов журналов нажмите кнопку **«Сохранить»** внизу страницы, чтобы применить изменения.