МЭ серии RTT-M300. Руководство пользователя

Выпуск 0.1

RTT

июл. 19, 2024

Оглавление

Глава 1

МЭ серии RTT-M300

1.1 Общее описание

Многофункциональные межсетевые экраны серий RTT-M300 и RTT-M300F (далее - RTT-M300) – это программно-аппаратные комплексы, реализующие широкий набор функций защиты сетевой инфраструктуры, таких как:

- Межсетевое экранирование (Firewall);
- Журналирование трафика (Logging);
- Глубокая инспекция пакетов (DPI);
- Проксирование трафика (Proxy);
- Трансляция сетевых адресов (NAT);
- Создание «частных» сетей (VPN);
- Потоковая антивирусная защита (AV);
- Обнаружение и детектирование вторжений (IDS/IPS).

Межсетевые экраны серии RTT-M300 предназначены для работы в корпоративных телекоммуникационных сетях. Внешний вид RTT-M300 представлен на рисунке.

Межсетевые экраны серии RTT-M300F предназначены для работы в промышленных телекоммуникационных сетях. Внешний вид RTT-M300F представлен на рисунке.

RTT-M300 (далее - изделие) обеспечивает комплексную защиту периметра сети от несанкционированного доступа и используется в качестве межсетевого экрана (шлюза безопасности) в корпоративных или промышленных сетях.

Изделие имеет форм-фактор 1U 19” в промышленном и корпоративном исполнениях, каждое из которых может быть оснащено различным набором интерфейсов, объемом постоянной и оперативной памяти.

Рис. 1: Внешний вид RTT-M300

Рис. 2: Внешний вид RTT-M300F

1.1.1 Программное обеспечение

В качестве программного обеспечения изделия используется операционная система REFOS с дополнительным слоем интеграции для корректности работы на аппаратной платформе. При этом в зависимости от применения (промышленное или корпоративное) существенно отличаются настройки дистрибутива REFOS и необходимый для функционирования в целевой сети состав лицензий.

Описание и характеристики операционной системы REFOS, а также руководство по работе с операционной системой, приведены в соответствующем разделе *руководства пользователя (ОС REFOS)*.

1.1.2 Аппаратное обеспечение

Аппаратная часть межсетевых экранов RTT-M300 строится на платформе RTT-UNA в корпоративном исполнении, разработанной ООО «РТТ» (далее - производитель). Аппаратная платформа реализована на базе процессора Baikal-M.

Аппаратная часть межсетевых экранов RTT-M300F строится на платформе RTT-UNA в промышленном исполнении, разработанной производителем. Аппаратная платформа реализована на базе процессора Baikal-M.

Также в состав версий изделия входят слои интеграции, реализующие аппаратно-зависимые функции на уровне функциональной части изделия и позволяющие корректно работать дистрибутиву REFOS на конкретной аппаратной платформе.

Описание и характеристики платформы RTT-UNA, а также руководство по монтажу и работе с платформой, приведены в соответствующем разделе *руководства пользователя (платформа RTT-UNA)*.

1.2 Варианты исполнения

Изделие представлено следующими вариантами исполнения:

Таблица 1: Модельный ряд МЭ RTT-M300

Наименование	Описание
RTT-M300 (корпоративное исполнение)	2xGE Combo, 4xGE, OOB, 2xUSB 3.0, 2xUSB 2.0, БП AC 110/220V
RTT-M300F (промышленное исполнение)	2xGE Combo, 4xGE, OOB, 2xUSB 3.0, 2xUSB 2.0, БП AC 110/220V, DC 36-72V
RTT-M300F-P (промышленное исполнение)	2xGE Combo, 4xGE, OOB, 2xUSB 3.0, 2xUSB 2.0, БП AC 110/220V, DC 36-72V, промышленные интерфейсы RS232/485/CAN/DIO/AIO/Relay

Каждый вариант исполнения изделия может быть расширен при помощи дополнительных съемных карт, в соответствии с таблицей

Таблица 2: Расширение варианта исполнения RTT-M300 при помощи дополнительных съемных карт

Карта	Описание
8xGE	Восемь маршрутизируемых интерфейсов 10/100/1000 BASE-T
2x10G SFP+	Два маршрутизируемых интерфейса для подключения SFP+ 10G-BASE-LR/SR/T
4xGE Switch	Четыре маршрутизируемых интерфейса 10/100/1000 BASE-T

По запросу может быть изменено входное напряжение питания для основного и резервного блоков аппаратной питания платформы.

1.3 Сценарии применения

1.3.1 Межсетевой экран для сетей ГИС

Межсетевой экран для сетей ГИС представлен на рисунке.

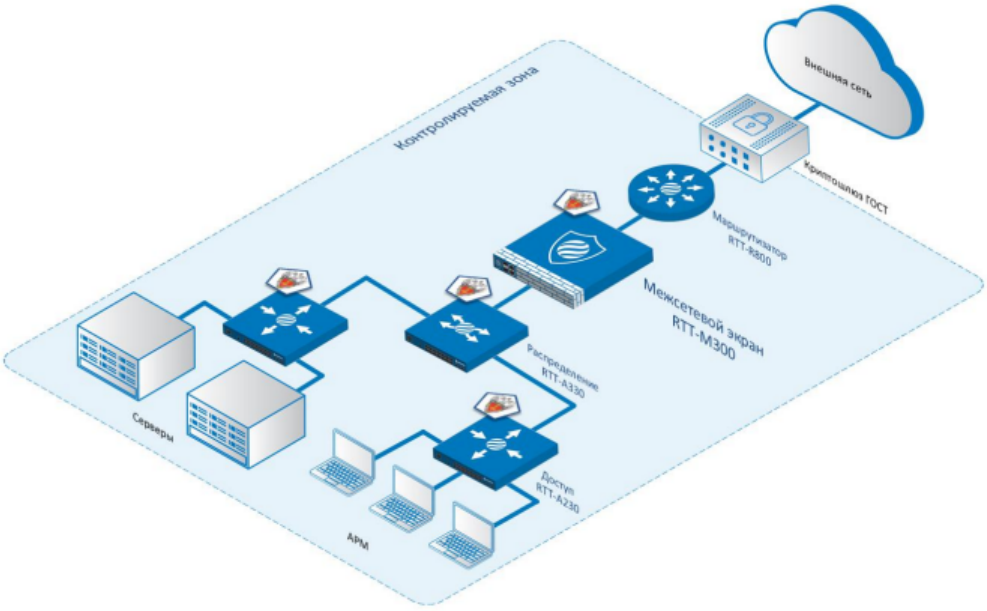


Рис. 3: Межсетевой экран для сетей ГИС

1.3.2 Универсальный шлюз безопасности для распределенной корпоративной сети

Универсальный шлюз безопасности для распределенной корпоративной сети представлен на рисунке.

1.3.3 Универсальный шлюз безопасности для промышленной сети

Универсальный шлюз безопасности для промышленной сети представлен на рисунке.

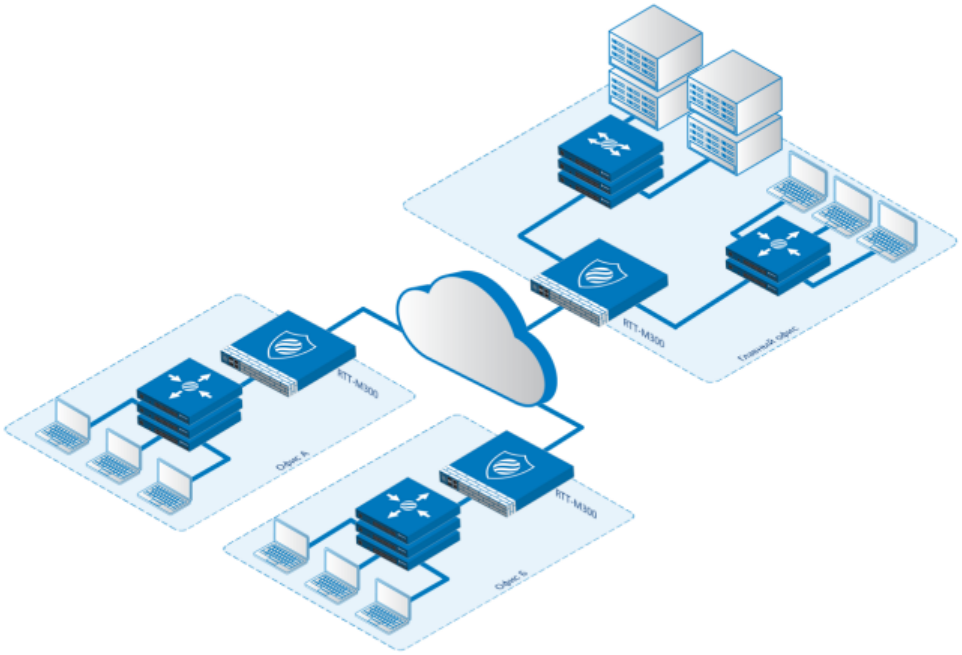


Рис. 4: Универсальный шлюз безопасности для распределенной корпоративной сети

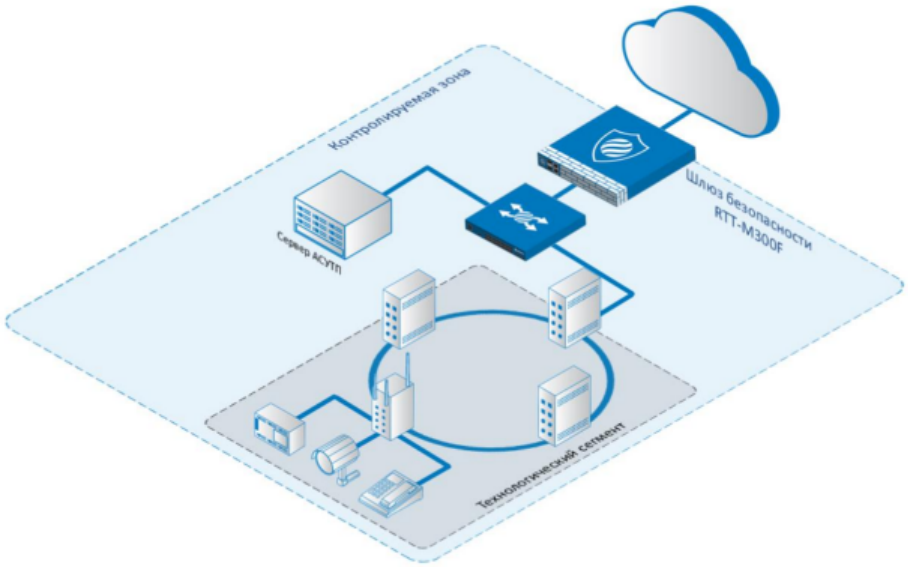


Рис. 5: Универсальный шлюз безопасности для промышленной сети

1.3.4 Безопасное подключение сегментов распределенной промышленной сети

Безопасное подключение сегментов распределенной промышленной сети представлен на рисунке.

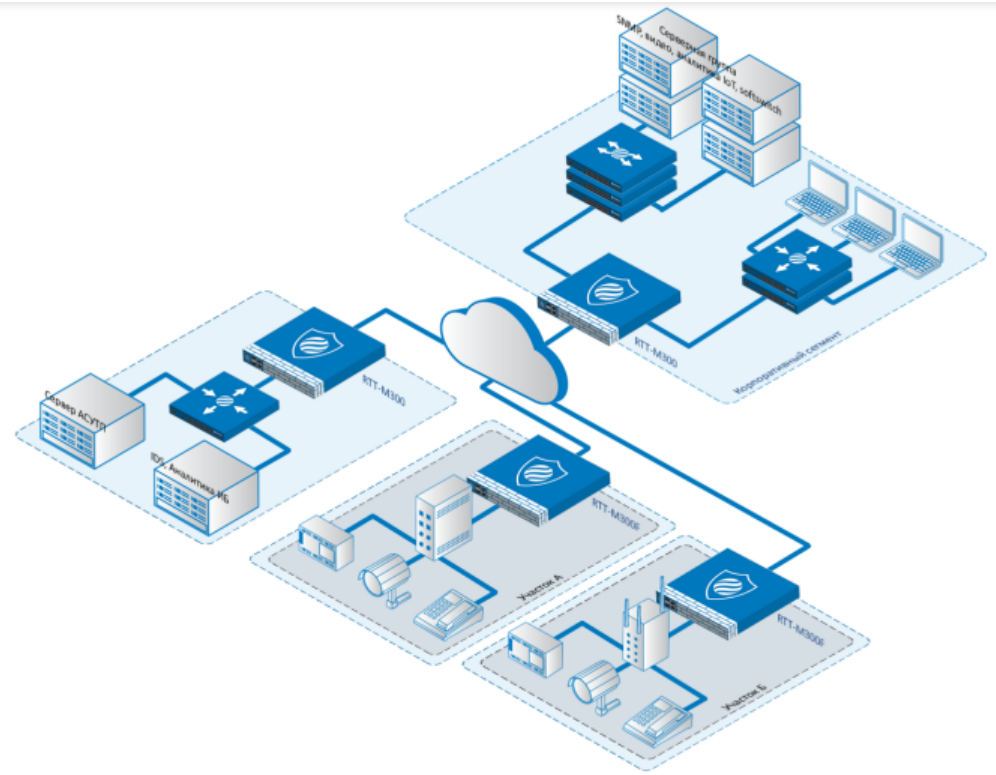


Рис. 6: Безопасное подключение сегментов распределенной промышленной сети

1.4 Функциональные возможности

1.4.1 Система и управление

Изделие обеспечивает выполнение следующих функций системы и управления:

- Полное управление через Web-интерфейс
- Подключение по SSH
- Мониторинг служб
- Мониторинг аппаратной платформы
- Резервные копии системы и сервисов
- Обновление из доверенного репозитория
- Журналирование системы
- Резервирование (CARP)
- Экспорт/импорт настроек
- Оповещение об обнаруженных ошибках

- Доверенная загрузка системы
- Автоматическое восстановление после сбоев

1.4.2 Межсетевой экран

Изделие обеспечивает выполнение следующих функций межсетевого экрана:

- Режим Stateful Firewall
- Режим Stateless Firewall
- **Параметры фильтрации:**
  - Операции Drop, Accept, Reject
  - Направления Input, Output, Forward
  - Фильтрация по IP отправителя, получателя
  - Фильтрация по протоколу
  - Фильтрация по номеру порта
  - Фильтрация по MAC-адресу
- **Расширенные настройки фильтрации:**
  - Уникальный ID пакета
  - Маркировка пакета и его отслеживание
  - Проверка контрольной суммы пакета
  - Проверка длины заголовка пакета
  - Отслеживание состояния соединения
  - Отслеживание направление пакета
  - Отслеживание статуса соединения
  - Отслеживание времени истечения срока действия подключения
  - Ограничение пропускной способности
  - Ограничение количества пакетов
  - Отслеживание среднего размера пакета
  - Отслеживание флагов (FIN, SYN, RST, PSH, ACK, URG, ECN, CWR)
- Фильтрация трафика по географическому признаку (GeoIP)
- Изменение политики фильтрации
- Переход в безопасное состояние при сбоях
- Псевдонимы (Alias)
- Журналирование пакетов
- Оповещение об обнаруженных аномалиях
- Перенаправление и зеркалирование трафика

1.4.3 Lite DPI

Изделие обеспечивает выполнение следующих функций Lite DPI:

- Контроль данных промышленных протоколов (MODBUS/TCP, MQTT)
- Raw offset
- Обнаружение аномалий
- Правила фильтрации отдельных типов сообщений

1.4.4 Сеть

Изделие обеспечивает выполнение следующих функций работы сети:

- xNAT (NAT, DNAT, SNAT, PAT)
- NTP/SNTP
- DHCP-сервер/клиент
- DNS-сервер
- Статическая маршрутизация
- Приоритизация потоков (QoS)
- Профилирование трафика

1.4.5 Веб-прокси

Изделие обеспечивает выполнение следующих функций Веб-прокси:

- HTTP-proxy
- Фильтрация URL
- Фильтрация мобильного кода
- Собственный список фильтрации URL/IP
- Гибкая система фильтрации мобильного кода и вложенных файлов
- Проверка почтовых сообщений
- Проверка сертификатов SSL

1.4.6 VPN

Изделие обеспечивает выполнение следующих функций VPN:

- Сервер OpenVPN
- Клиент OpenVPN
- Антивирус
- Встроенный потоковый антивирус ClamAV
- Интеграция с внешними антивирусами (Kaspersky и др.)

1.4.7 Функции безопасности

Изделие обеспечивает выполнение следующих функций безопасности:

- Фильтрация трафика L2-L4 с контролем состояний (Statefull firewall)
- Инспекция пакетов (Lite DPI)
- Туннелирование трафика (Tunneling)
- Маршрутизация (Routing)
- Проксирование трафика (Proxy)
- Трансляция адресов (xNAT)
- Потоковый антивирус (AV)
- Горячее резервирование сервисов
- Интеграция с SOC/SIEM
- stateless режим (в разработке)

1.4.8 Администрирование

Изделие обеспечивает следующие возможности администрирования:

- Полнофункциональный Web-интерфейс
- CLI для базовой настройки
- Групповое управление через NMS (в разработке)

1.4.9 Мониторинг

Изделие обеспечивает выполнение следующих функций мониторинга:

- Мониторинг аппаратных ресурсов
- Мониторинг системы и сервисов
- Мониторинг через NMS (в разработке)

1.4.10 Журналы и отчеты

Изделие обеспечивает следующие возможности журналирования:

- Журнал межсетевого экрана
- Журнал событий, отчет состояния трафика
- Отчеты о состоянии системы

1.5 Производительность

Изделие имеет следующие характеристики.

Таблица 3: Пропускная способность изделия при 100 правилах фильтрации (RTT-M300/RTT-M300F)

Характеристика	Размер пакета 64 байта	Размер пакета 1500 байт
Пропускная способность в режиме фильтрации L4, Мбит/с	120	2 500
Пропускная способность в режиме фильтрации L4, кпак/с	205	300
Пропускная способность в режиме LiteDPI (100 правил), Мбит/с	120	2 500
Пропускная способность в режиме фильтр L4 + IDS, Мбит/с	35	800
Пропускная способность в режиме фильтр L4 + IPS, Мбит/с	15	200

Глава 2

Руководство пользователя операционной системы REFOS

2.1 О REFOS

REFOS является специализированным дистрибутивом для обеспечения комплексной защиты периметра сети и её подключения к внешним сетям, в том числе дистрибутив позволяет фильтровать трафик на уровнях L2-L7, обнаруживать угрозы и вредоносный трафик, динамически маршрутизировать трафик, обеспечивать подключение к нескольким операторам связи, создавать VPN соединения и т. д.

REFOS поддерживает работу в IPv4 и IPv6 сетях.

Для мониторинга и управления REFOS имеет Web-интерфейс, CLI и API. При этом CLI используется для базовой конфигурации и мониторинга неисправностей, тогда как полнофункциональные управление и мониторинг осуществляются через Web-интерфейс и API.

REFOS создана на базе ядра Linux и является самостоятельным дистрибутивом (не является «форком» других дистрибутивов GNU/Linux). Система поддерживает работу на процессорах с архитектурой Amd64 и Aarch64, полный перечень поддерживаемых аппаратных платформ уточняйте в ООО «РТТ».

2.2 Начало работы

При первом включении или после сброса настроек до значений по умолчанию доступ к системе может быть осуществлён через Web-интерфейс по протоколу http.

Адрес при использовании интерфейса:

- LAN - имеет адрес 192.168.7.2 (по умолчанию)
- WAN - получает IP адрес по DHCP

Стандартные данные для входа в систему:

- Пользователь: **Admin**
- Пароль: **Rusteletech$**

Примечание

Соответствие интерфейсов WAN/LAN и физических интерфейсов по умолчанию может отличаться для различных аппаратных платформ. Уточняйте назначение LAN и WAN в описании для соответствующего программно-аппаратного комплекса.

Поддерживаются следующие браузеры:

- Chrome
- Firefox
- Яндекс.Браузер

Примечание

Не рекомендуется использовать протокол http для доступа к системе, поэтому при первом подключении и до начала конфигурации рекомендуется установить сертификат для https и использовать для доступа https. В случае продолжения использования http при каждом входе система будет предупреждать об использовании небезопасного протокола для доступа.

К CLI *(Интерфейс командной строки)* системы можно подключиться локально через порт **Консоль** (устройство определяется как usb device) или через ssh.

Стандартные данные для подключения к CLI:

- Пользователь: **Admin**
- Пароль: **rusteletech**

2.3 Лицензирование

Управление доступной функциональностью программного обеспечения REFOS осуществляется при помощи системы лицензирования. В версии ПО REFOS 1.x.x предусмотрены лицензии, соответствующие таблице

Таблица 1: Лицензии ПО REFOS 1.x.x

Лицензия	Описание
rttlicensefirewall	Базовая лицензия с набором функций ФСТЭК А4/Д4 +
rttlicenseopenvpn	Дополнительная лицензия на подсистему VPN
rttlicenseclamav	Дополнительная лицензия на потоковый антивирус
rttlicenseldpi	Дополнительная лицензия на анализатор протоколов LiteDPI
rttlicenseids	Дополнительная лицензия на систему обнаружения вторжений

Базовой лицензией является лицензия на межсетевой экран (rttlicensefirewall), обеспечивающий фильтрацию трафика до уровня L4 модели OSI включительно и необходимую дополнительную функциональность в рамках требований ФСТЭК к межсетевым экранам классов А4 и Д4 (журналирование, прокси-сервер, фильтрация мобильного кода, интерфейсы взаимодействия с внешними средствами защиты информации и т.д.). Кроме этого, в составе лицензии присутствует ряд дополнительных функций (расширенное администрирование, сертификаты SSL и т.д.).

В рабочую конфигурацию REFOS в обязательном порядке входит базовая лицензия rttlicensefirewall, остальные лицензии могут комбинироваться. Все лицензии, доступные в REFOS, являются неограниченными по сроку действия, а обновления для функциональных модулей в составе лицензионного пакета доступны в течение всего периода поддержки версии дистрибутива.

Для приобретения лицензий обратитесь к дистрибьютору, региональному представителю или в коммерческий отдел производителя (список актуальных адресов указан в разделе «Контакты» на сайте производителя).

2.3.1 Активация лицензий

Для активации приобретенных лицензий используйте страницу **«Система - Программное обеспечение»** в Web-интерфейсе

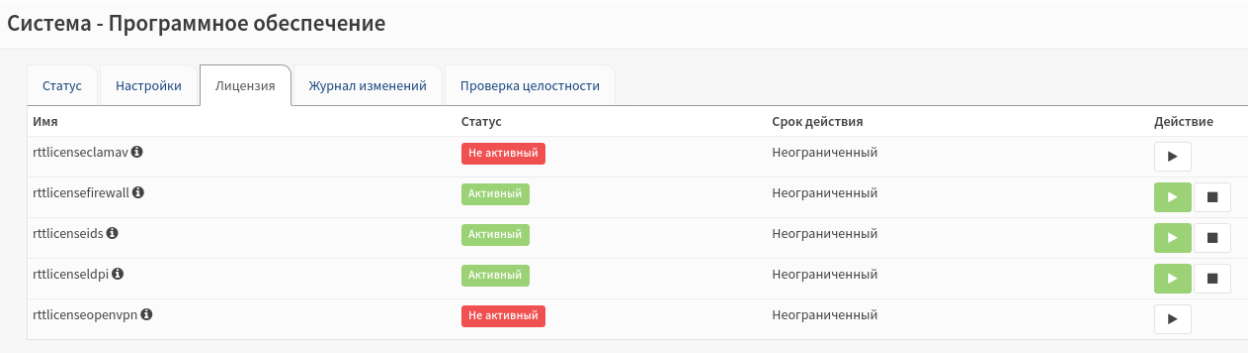


Рис. 1: Активация лицензий

Для активации или прекращения действия лицензии используйте настройку **«Действие»**

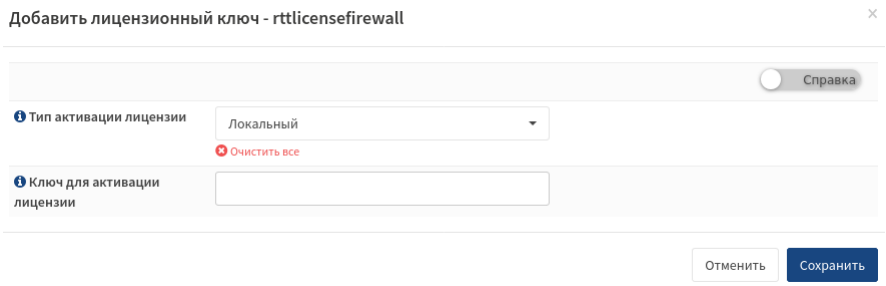


Рис. 2: Переход к активации или прекращению действия лицензии

2.4 Обновление системы

Система может обновляться в ручном и автоматическом режимах. В режиме ручного обновления пользователь может выбрать следующие опции обновления: полное обновление, базовое обновление и обновление безопасности. В автоматическом режиме (по расписанию) в текущей версии дистрибутива REFOS доступно только полное обновление системы.

Примечание

Мы рекомендуем настроить полное обновление системы по расписанию, это гарантирует своевременную установку всех необходимых обновлений системы и совместимость вашей системы с актуальной версией на централизованном репозитории.

При полном обновлении происходит обновление всех пакетов в составе дистрибутива до актуальной версии, всей дополнительной информации и системных настроек (пользовательские настройки остаются без изменений), то есть происходит полное обновление до актуальной версии. При этом возможна несовместимость отдельных компонентов предыдущих релизов и актуального релиза, в случае существенного расхождения их версий.

Примечание

Если версия вашей системы существенно отличается от актуальной версии (отличаются первые числа версии релизов или вторые числа релизов более чем на пять пунктов), необходимо обратиться в техподдержку для уточнения возможности полного обновления. В случае возникновения проблем при полном обновлении также необходимо обратиться в техподдержку.

При базовом обновлении будет установлен и(или) обновлён ограниченный набор пакетов, исправляющий известные текущие ошибки. При обновлении безопасности будет установлен и(или) обновлён набор пакетов для устранения текущих известных уязвимостей. Базовый набор пакетов уже содержит в себе подмножество обновлений безопасности.

Управление обновлением доступно на странице Web-интерфейса дистрибутива: **«Система - Программное обеспечение»**. Во вкладке **«Статус»** представлена основная информация о версии установленного ПО, последнем обновлении и репозитории, с которого оно осуществлялось. Здесь же представлена кнопка для ручного обновления системы с возможностью выбора типа обновления.

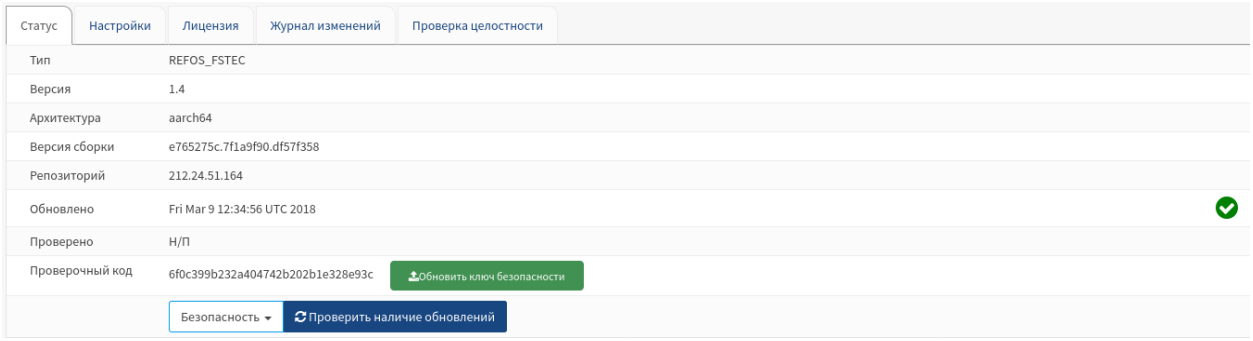


Рис. 3: Ручное обновление системы

Выбор репозитория из списка доверенных репозиториев и настройка обновления по расписанию доступны во вкладке **«Настройки»**.

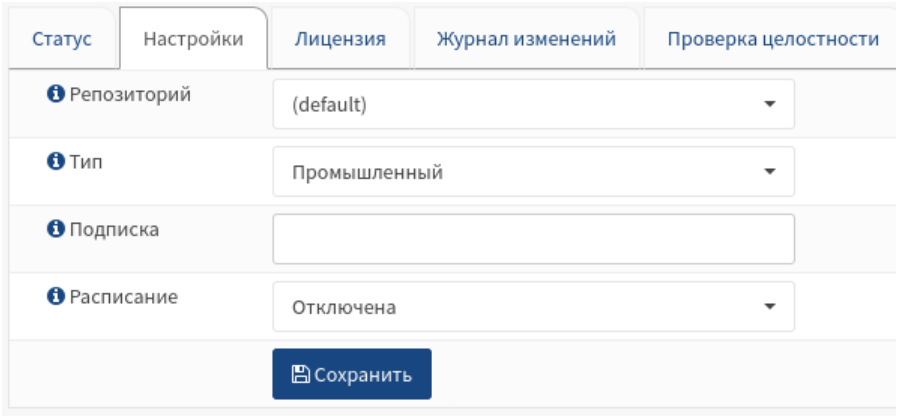


Рис. 4: Выбор репозитория и настройка обновления

2.5 Интерфейс командной строки

Интерфейс командой строки является вспомогательным интерфейсом управления и содержит базовые команды управления, конфигурирования и мониторинга.

Интерфейс доступен через локальную консоль аппаратной платформы или по протоколу SSH.

Внешний вид интерфейса командной строки представлен на рисунке

Список доступных команд администратора CLI соответствует таблице

Таблица 2: Команды администратора CLI

Направление	Значение
interface-list	Вывод интерфейсов в системе
ping	Диагностика сетевого подключения, проверка, доступно ли удаленное устройство
change-password	Сменить пароль
reset-rules	Сброс правил межсетевого экрана
system-info	Вывести информацию о системе
log-check	Вывод log-подключений
logout	Выход из системы
poweroff	Выключить
reboot	Перезагрузка
commands	Вывести список команд

2.6 Настройка функций

2.6.1 Фильтрация

2.6.1.1 Введение

Фильтрация трафика является основной функциональной задачей REFOS. Поэтому наличие широкого количества параметров и атрибутов, по которым система может производить фильтрацию разнородного трафика, является важной особенностью REFOS.

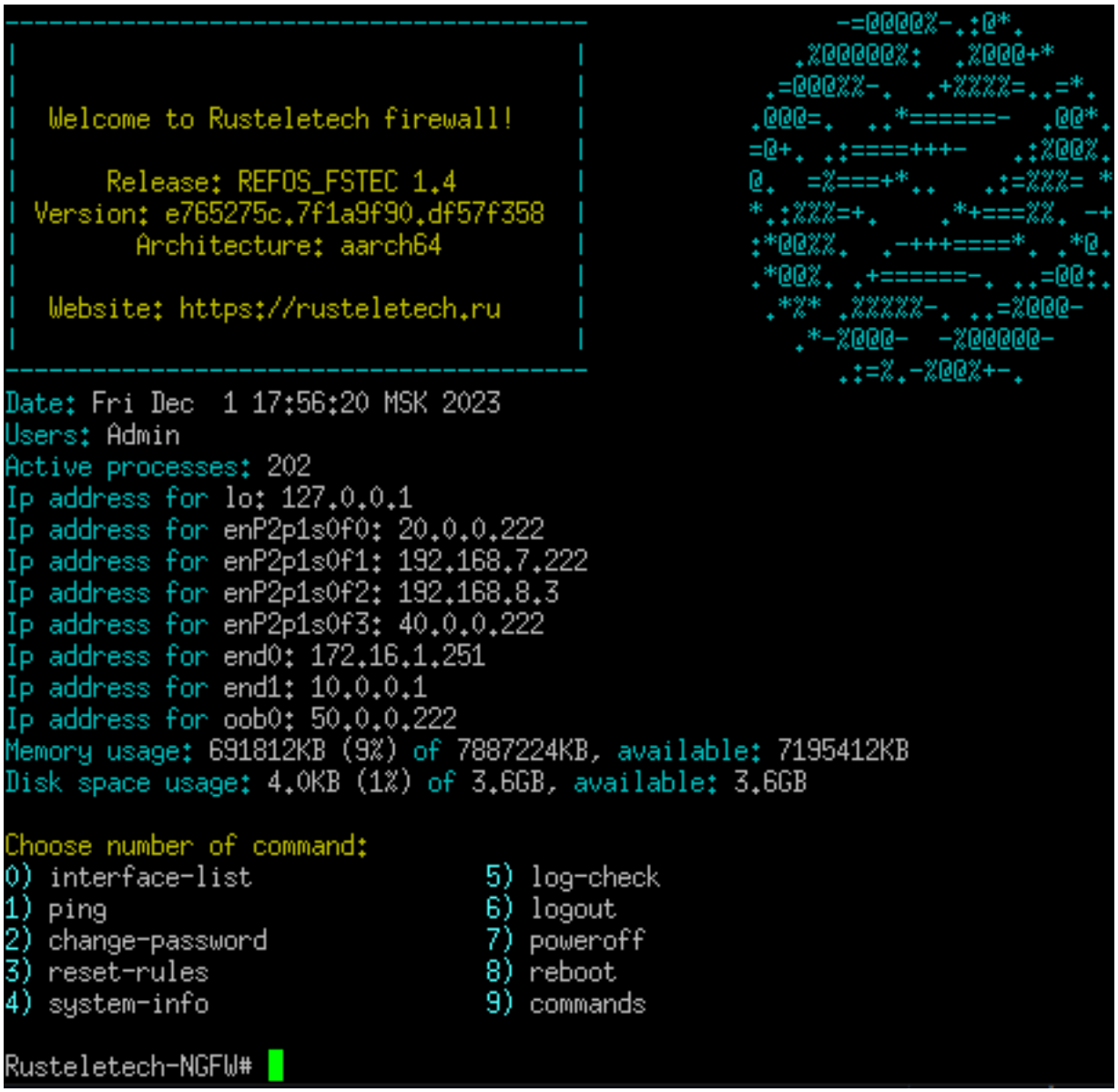


Рис. 5: Интерфейс командной строки

Основной принцип фильтрации состоит в том, что система анализирует трафик, используя набор сконфигурированных пользователем правил (ruleset). Следуя заданным параметрам правил фильтрации, система принимает решение (Действие) по каждому пакету из потока трафика.

Решение (Действие) может быть следующим:

- **Принимать** (Accept);

Система принимает и обрабатывает все пакеты, подходящие под правила фильтрации;

- **Блокировать** (Drop);

Система блокирует(откидывает) все пакеты, подходящие под правила фильтрации;

- **Отклонять** (Reject);

Система блокирует(откидывает) все пакеты, подходящие под правила фильтрации и отправляет ответное ICMP-сообщение об ошибке;

Важным параметром фильтрации является Направление. В данном случае речь идет о трафике, который должна обработать система.

Трафик условно можно разделить на:

- Входящий;

Трафик, который непосредственно предназначается системе (любой службе, сервису). В заголовке пакетов трафика IP-адрес получателя является любой интерфейс системы.

- Исходящий;

Трафик, который непосредственно инициируется самой системой (службой, сервисом). В заголовке пакетов трафика IP-адрес отправителя является любой интерфейс системы.

- Транзитный;

Трафик, который не предназначается и не инициируется системой. Т.е. данный трафик имеет отличные IP-адреса отправителя и получателя в заголовке пакет от IP-адреса интерфейсов системы. В данном случае система должна принять, обработать (фильтрация, коммутация, маршрутизация) и отправить в место назначения данный трафик.

Важно

Входящий трафик обрабатывается Направлением **Input**.

Важно

Исходящий трафик обрабатывается Направлением **Output**.

Важно

Транзитный трафик обрабатывается Направлением **Forward**.

При конфигурировании правила фильтрации важно выбрать корректное Направление трафика. Все транзитные пакеты, которые не предназначаются и не инициируются системой, должны обрабатываться Направлением **Forward**. Правила фильтрации с Направлением **Input** и **Output** будут игнорировать транзитные пакеты. Аналогичная ситуация с входящим и исходящим трафиком. Например, если

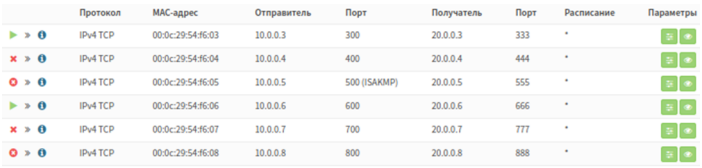
необходимо заблокировать доступ по протоколу SSH к системе (REFOS), в данном случае в правиле фильтрации должно использоваться Направление **Input**, т.к. предполагаемый блокируемый трафик будет предназначаться системе (REFOS).

2.6.1.2 Приоритет обработки трафика правилами фильтрации

Правила фильтрации имеют свой приоритет. Трафик обрабатывается правилами фильтрации сверху вниз, т.е. чем выше правило фильтрации находится в списке правил, тем выше его приоритет.

Например, в списке правил фильтрации на рисунке, система произведет обработку трафика правилами фильтрации поочередно сверху вниз. Если параметры трафика не попали под условия фильтрации всех правил, система использует стандартную политику фильтрации.

Список фильтрации правил представлен на рисунке.



	Протокол	MAC-адрес	Отправитель	Порт	Получатель	Порт	Расписание	Параметры
▶ » ℹ	IPv4 TCP	00:0c:29:54:f6:03	10.0.0.3	300	20.0.0.3	333	*	
✖ » ℹ	IPv4 TCP	00:0c:29:54:f6:04	10.0.0.4	400	20.0.0.4	444	*	
○ » ℹ	IPv4 TCP	00:0c:29:54:f6:05	10.0.0.5	500 (ISAKMP)	20.0.0.5	555	*	
▶ » ℹ	IPv4 TCP	00:0c:29:54:f6:06	10.0.0.6	600	20.0.0.6	666	*	
✖ » ℹ	IPv4 TCP	00:0c:29:54:f6:07	10.0.0.7	700	20.0.0.7	777	*	
○ » ℹ	IPv4 TCP	00:0c:29:54:f6:08	10.0.0.8	800	20.0.0.8	888	*	

Рис. 6: Список правил фильтрации

2.6.1.3 Стандартная политика фильтрации трафика

Стандартная политика фильтрации позволяет принимать или блокировать весь трафик, который не попал под другие сконфигурированные правила фильтрации. Условно стандартной политикой фильтрации можно назвать правило с самым низким приоритетом, которое принимает или блокирует трафик. Т.е. трафик обработается стандартной политикой фильтрации в любом случае, если не обработался по условиям правил фильтрации с более высоким приоритетом.

Существует несколько политик фильтрации:

- Стандартная политика INPUT;
- Стандартная политика OUTPUT;
- Стандартная политика FORWARD;
- Стандартная политика DNAT;
- Стандартная политика SNAT.

Каждое **Направление** обрабатывается своей стандартной политикой.

Конфигурация производится в разделе **Межсетевой экран - Настройки - Общие настройки**.

По умолчанию все политики сконфигурированы на прием любого трафика.

> **Важно**
>
> Правильной практикой является ограничение трафика в стандартных политиках фильтрации Input, Output, Forward. Т.е. трафик, который не попал под условия правил фильтрации с более высоким приоритетом, должен быть заблокирован стандартной политикой фильтрации.

Журналирование позволяет фиксировать обработку трафика стандартной политикой фильтрации. По умолчанию журналирование отключено.

Политики DNAT и SNAT должны использоваться с большей осторожностью. При использовании параметра **Сбросить**, все пакеты, поступающие на обработку, будут отброшены, несмотря на правила фильтрации с более высоким приоритетом.

Важно

Для правильного функционирования фильтра системы. Политики DNAT и SNAT должны использовать параметр **Принимать** (установлен по умолчанию).

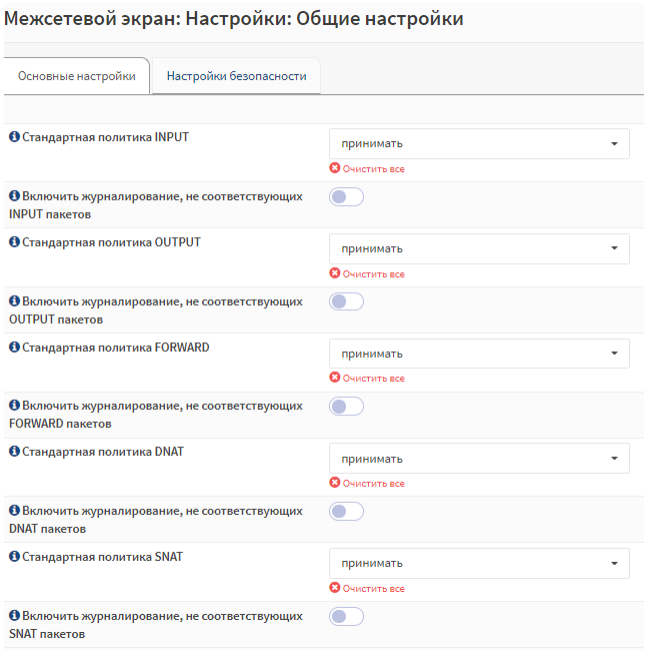


Рис. 7: Межсетевой экран - Настройки - Общие настройки

2.6.1.4 Настройки параметров безопасности

Интерфейсы системы логически разделены на две зоны – LAN и WAN. Сделано это с целью повысить безопасность доступа к системе. По умолчанию весь трафик на интерфейсах LAN для всех Направлений разрешен. Для интерфейсов WAN по умолчанию сконфигурирован набор правил фильтрации по доступу к системе, представленный в таблице:

Таблица 3: Набор правил фильтрации по доступу к системе

Направление	Правило фильтрации
Input	Запрещен Web доступ
Output	Запрещен SSH доступ
	Запрещен ответ на ICMP-запросы

Так как Направления Input и Output при конфигурации правил фильтрации используются крайне редко, в основном обработка касается транзитных пакетов Направлением Forward, поэтому присутствует возможность ограничить использование данных Направлений – параметры:

- Предотвращение конфигурации INPUT правил;

- Предотвращение конфигурации OUTPUT правил.

Настройки параметров безопасности показаны на рисунке

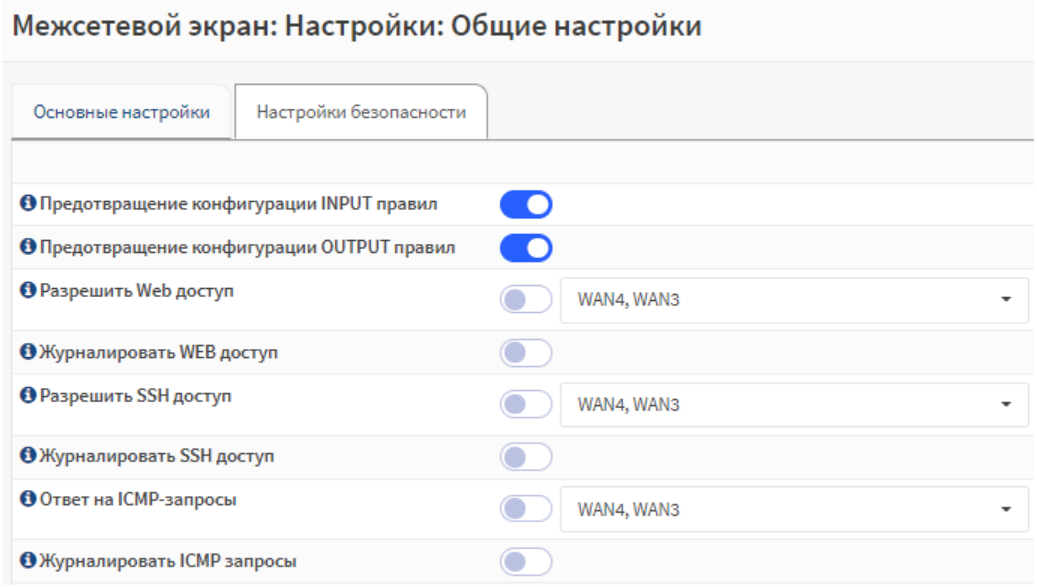


Рис. 8: Настройки параметров безопасности

2.6.1.5 Основные параметры правил фильтрации

REFOS позволяет производить фильтрацию по разным уровням OSI: L2, L3, L4 и выше.

Основные параметры фильтрации представлены в таблице

Таблица 4: Основные параметры фильтрации

Параметр	Описание
Действие	Выбор действия по пакету, если параметры пакета подходят под условия фильтрации: • Принимать (Accept); • Блокировать (Drop); • Отклонять (Reject);
Отключить	Отключить правило фильтрации, не удаляя из системы
Интерфейс	Интерфейс, на котором применяется правило фильтрации
Направление	Выбор направления, которое будет обрабатывать соответствующий трафик: • Input • Output • Forward

продолжается на следующей странице

Таблица 4 – продолжение с предыдущей страницы

Параметр	Описание
MAC-адрес / Инвертировать; Отправитель / Инвертировать; Получатель/ Инвертировать;	Трафик, который попадает под правила фильтрации с использованием данной функции, будет игнорироваться и обрабатываться последующими правилами фильтрации, а трафик, который не попадает по параметрам под заданные правила фильтрации с инверсией, будет обрабатываться данным правилом.
Исходный MAC-адрес	MAC-адрес отправителя (source MAC-address).
Версии TCP/IP	Выбор протокола: • IPv4; • ARP;
Параметры при выборе протокола IPv4	
Протокол	Выбор протокола L3, L4 уровней: TCP, UDP, ICMP, ESP, AH, GRE, IGMP, PIM, OSPF, GGP, IPENCAP, ST, EGP, IGP, PUP, HMP, XNS-IDP, RDP, ISO-TP4, DCCP, XTP, DDP, IDPR-CMTP, IPv6, IPv6-ROUTE, IPv6-FRAG, IDRP, RSVP, SKIP, IPv6-ICMP, IPV6-NONXT, IPv6-OPTS, RSPF, VMTP, EIGRP, AX.25, IPIP, ETHERIP, ENCAP, IPCOMP, VRRP, L2TP, ISIS, SCTP, FC, MOBILITY-HEADER, UDPLITE, MPLS-IN-IP, MANET, HIP, SHIM6, WESP, ROHC. По умолчанию используется значение Любой.
Тип ICMP (Параметр доступен только при выборе протокола ICMP)	Выбор ICMP-сообщения: • Любой; • Эхо-запрос; • Эхо-ответ; • Адресат недоступен; • Подавление источника; • Перенаправить; • Объявления маршрутизатора; • Запрос маршрутизатора; • Время истекло; • Некорректный параметр; • Временная метка; • Ответ с меткой времени; • Информационный запрос (устаревшее сообщение); • Ответ на информационный запрос (устаревшее сообщение); • Запрос адресной маски (устаревшее сообщение); • Ответ на запрос адресной маски (устаревшее сообщение); По умолчанию используется значение Любой.
Отправитель; Получатель;	Указать IP-адрес или целую сеть отправителя или получателя. По умолчанию используется значение Любой.

продолжается на следующей странице

Таблица 4 – продолжение с предыдущей страницы

Параметр	Описание
Диапазон портов источника; Диапазон портов получателя; (Параметры доступны только при выборе протоколов TCP, UDP).	Возможно задать любой порт или список портов источника или получателя, используя параметр Другое. А также можно использовать список портов из поля Хорошо известные порты: FTP, SSH, Telnet, SMTP, DNS, TFTP, HTTP, POP3, IDENT/AUTH, NNTP, NTP, NetBIOS-NS, NetBIOS-DGM, NetBIOS-SSN, IMAP, SNMP, SNMP-Trap, LDAP, HTTPS, MS DS, SMTP/S, ISAKMP, ModBus(TCP), SUBMISSION, IMAP/S, POP3/S, OpenVPN, MS WINS, L2TP, PPTP, MMS/TCP, RADIUS, RADIUS accounting, MSN, MQTT, IEK 60870-5-104; HBCI, MS RDP, STUN, Teredo, IPsec NAT-T, RTP, SIP, VNC, CVSup, MMS/UDP, MQTT(SSL). По умолчанию используется значение Любой.
DSCP	Фильтрация по коду DSCP. Указать Выражение: • Равный; • Не равен; По умолчанию используется значение Отсутствует. Указать Значения: • CS0 – CS1; AF11-AF13; AF21-AF23;AF31-AF-33; AF41-AF43; По умолчанию используется значение Отсутствует.
Параметры при выборе протокола ARP	
Тип ARP	Выбор ARP-сообщения: • Request; • Reply; По умолчанию используется значение Отсутствует.
Журналирование	Запуск журналирования. Журналируется каждый пакет, который попадает под текущее правило фильтрации.
Счетчики	Запуск счетчиков пакетов, которые подходят под параметры правил фильтрации.
Описание	Общие комментарии к правилу фильтрации.
Расписание	Задать сконфигурированное расписание, по которому будет функционировать правило фильтрации. Конфигурация расписания доступна в разделе Расписание.
Ограничение скорости	Задать ограничение по количеству и размеру трафика. Для запуска ограничения необходимо выбрать: • Параметр Выражение – Больше, чем; • В поле Ограничение указать количество пакетов; • Параметр Тип – пкт/сек, пкт/мин, пкт/ч; Дополнительно возможно установить ограничение по размеру: • Задать значение в поле Размер пакета; • Тип – байты, килобайты; По умолчанию используется значение Отсутствует.

2.6.1.6 Пример конфигурации правила с основными параметрами

Предположим, что необходимо произвести фильтрацию транзитного трафика с определенными параметрами и определенным Действием

Таблица 5: Пример фильтрации транзитного трафика

№	Параметры транзитного пакета	Должны выполнять следующее действие:
1	MAC-адрес отправителя - 00:0C:29:54:F6:03; IP-адрес отправителя - 10.0.0.3; TCP-порт отправителя - 300; IP-адрес получателя - 20.0.0.3; Порт получателя - 333;	Принимать

В данном случае, следуя заданным параметрам транзитного пакета, необходимо сконфигурировать правило фильтрации. Т.к. планируется обработка транзитного пакета, использоваться будет Направление **Forward**.

Добавление правил фильтрации происходит в разделе **Межсетевой экран - Правила фильтрации**, используя соответствующий интерфейс.

2.6.1.7 Lite DPI. Фильтрация трафика по смещению

Механизм Lite DPI позволяет производить фильтрацию по смещению в пакете, а также предусматривает фильтрацию по основным параметрам промышленных протоколов.

Фильтрация по смещению в пакете

Любой передаваемый блок данных (PDU) можно представить в виде набора битов. Профиль **Смещение** позволяет указать место в блоке данных (с определенного бита/байта) и задать значение, по которому необходимо производить фильтрацию. Т.е. система при обработке блока данных будет анализировать заданную последовательность битов/байтов и сопоставлять эти значения с заданными параметрами фильтрации.

При конфигурации профиль **Смещение** позволяет задать параметры смещения:

- Заголовок;
- Смещение в битах;
- Длину анализируемой части в битах;
- Значение по которому необходимо анализировать заданную часть.

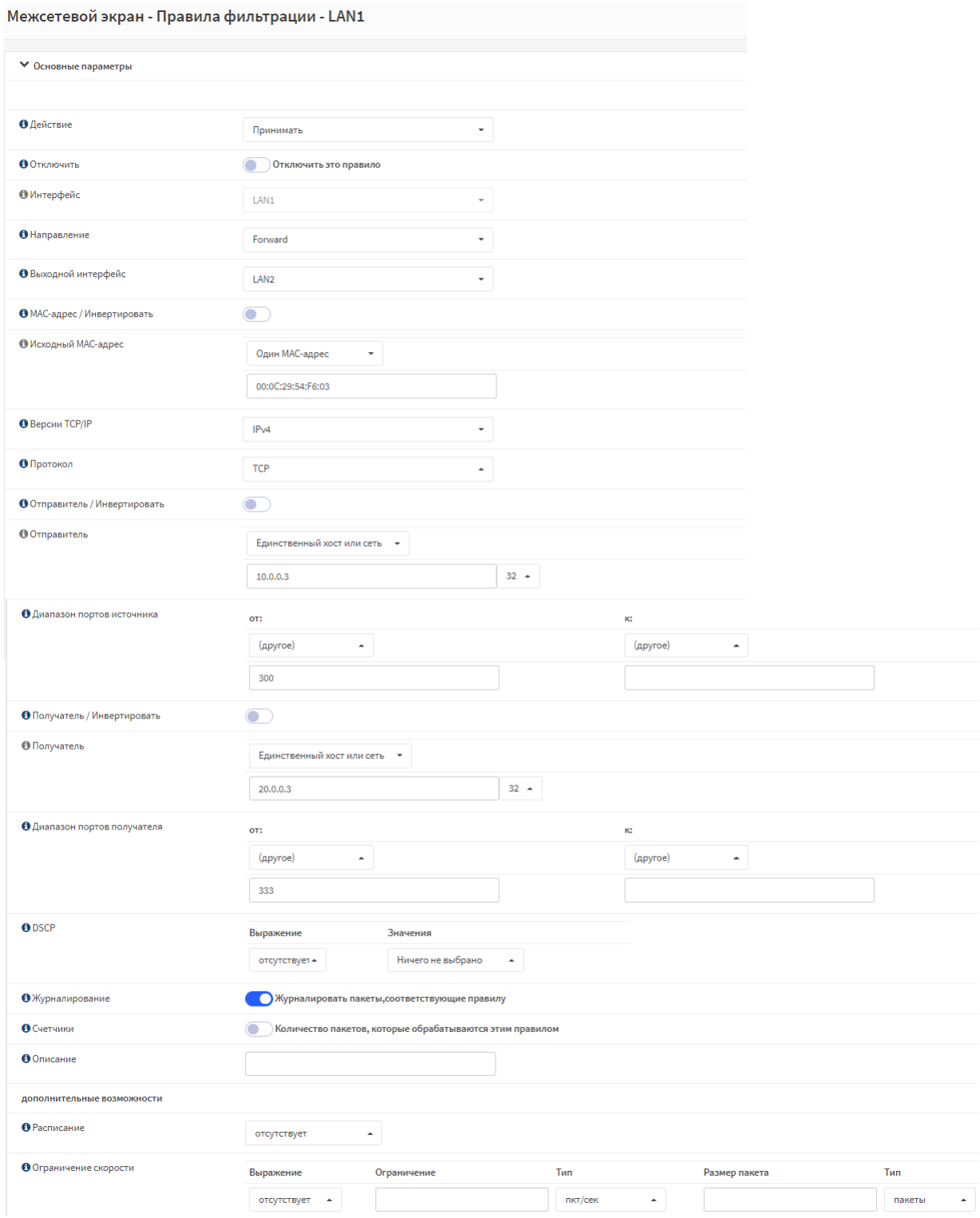


Рис. 9: Пример конфигурации правила фильтрации

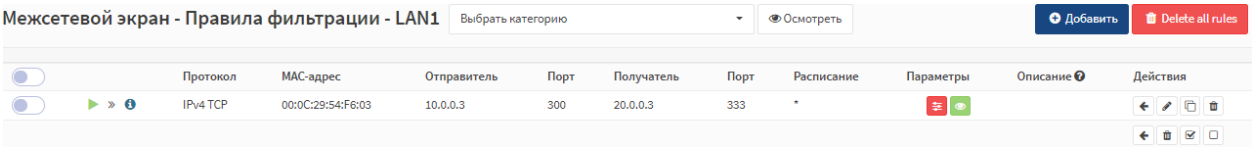


Рис. 10: Статус правила фильтрации

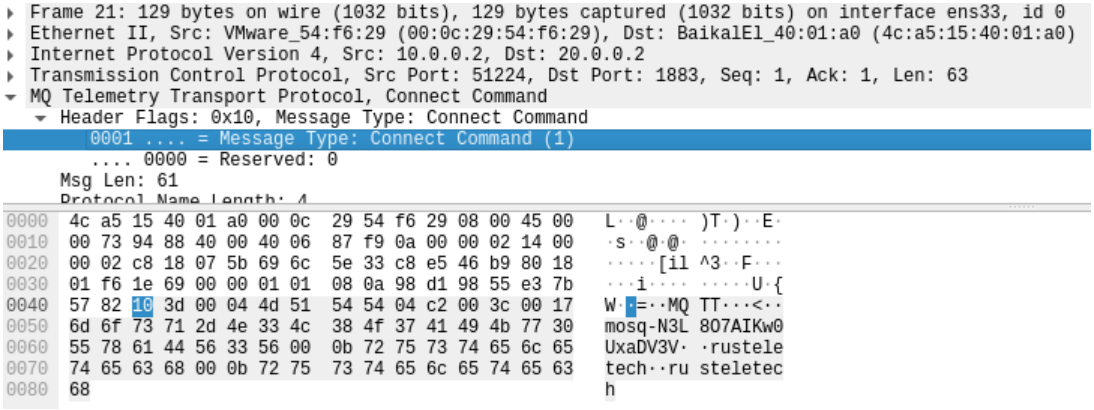


Рис. 11: Представленный блок данных в виде последовательности байтов

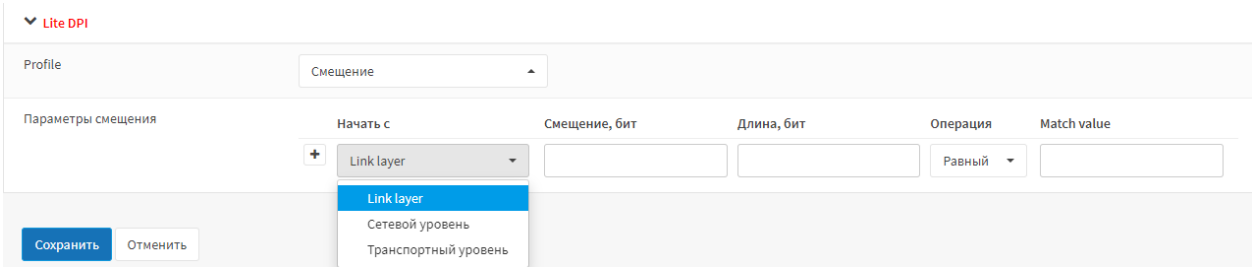


Рис. 12: Параметры профиля смещение

Пример

Предположим, необходимо анализировать значение в поле Sequence Number (Raw) TCP-сегмента

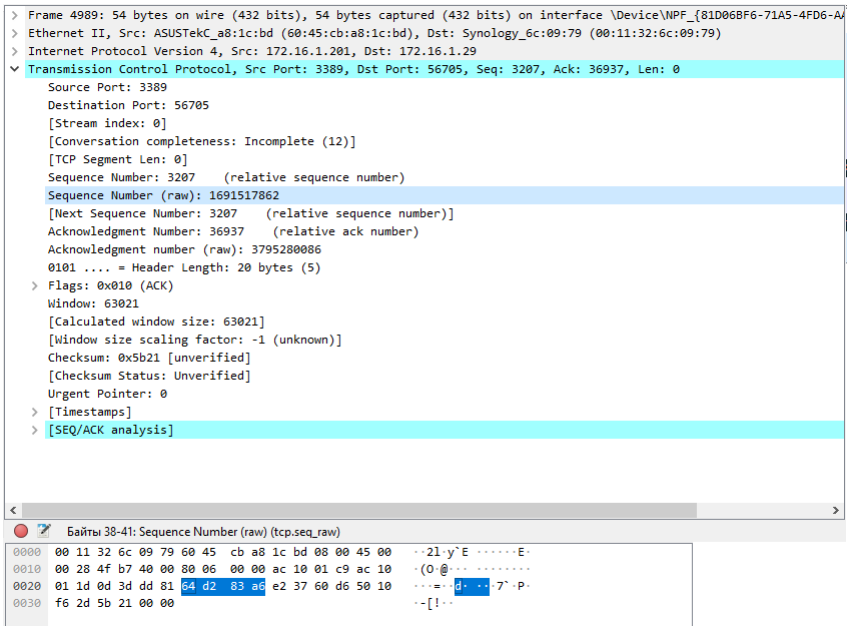


Рис. 13: Поле Sequence Number (Raw) TCP-сегмента

Если представить данный блок данных в байтах, тогда значение поля Sequence Number (Raw) будет доступно в 38-41 байте и принадлежит заголовку TCP-сегмента. В данном случае для анализа этого поля необходимое смещение является 37 байт, а анализировать необходимо 4 байта.

Для корректной конфигурации необходимо задать **Заголовок** и значение **Смещение** в битах. Т.к. значение поля Sequence Number (Raw) находится в TCP сегменте, корректно задать в параметрах **Начать с – Сетевой уровень** и **Смещение – 32**. **Сетевой уровень** заканчивается на 33 байте (смещение до 33 байта) и **Смещение** 32 бита (4 байта) – это часть заголовка транспортного уровня. Т.е. 37 байта (33+4) полностью игнорируются(смещаются) для обработки и анализируется только 4 байтовое(32 бита) поле Sequence Number (Raw).

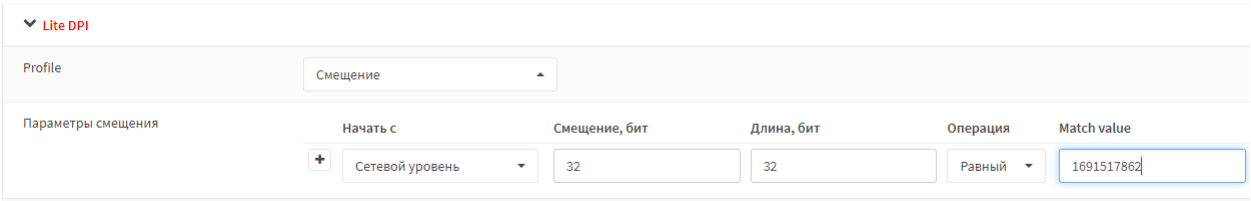


Рис. 14: Конфигурация по фильтрации значения в поле Sequence Number (Raw) TCP-сегмента

Фильтрация по основным параметрам промышленных протоколов

Система позволяет производить фильтрацию по основным параметрам промышленных протоколов MQTT и ModBus.

Профили фильтрации протокола MQTT

- Профиль **Connect** представлен на рисунке.

Включает параметры **Client ID**, **Client name**, **Client password**.

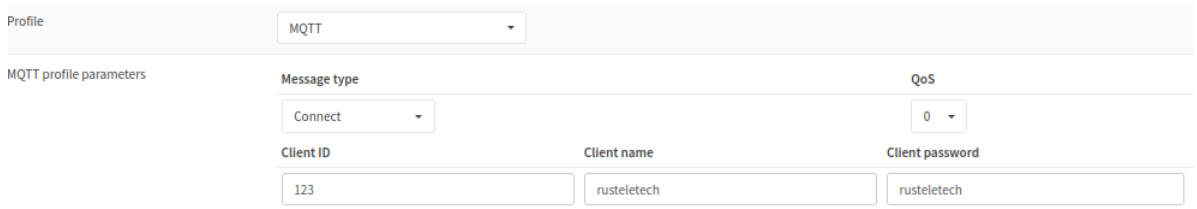


Рис. 15: Профиль Connect

- Профиль **Subscribe** представлен на рисунке.

Включает параметры **Message Id**, **Topic**.

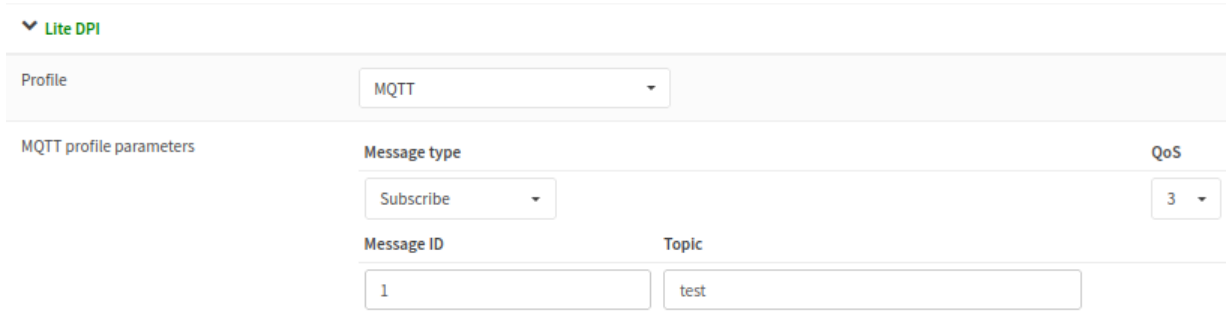


Рис. 16: Профиль Subscribe

- Профиль **Publish** представлен на рисунке.

Включает параметры **Message + Topic length**, **Topic length**, **Topic**, **Сообщение**.

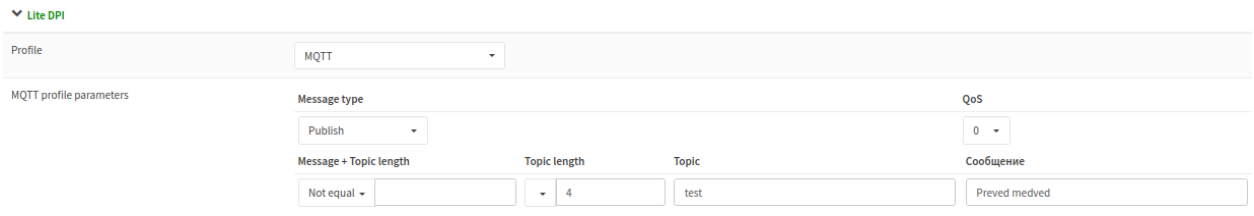


Рис. 17: Профиль Publish

- Профиль **Unsubscribe** представлен на рисунке.

Включает параметры **Message ID**, **Topic**.

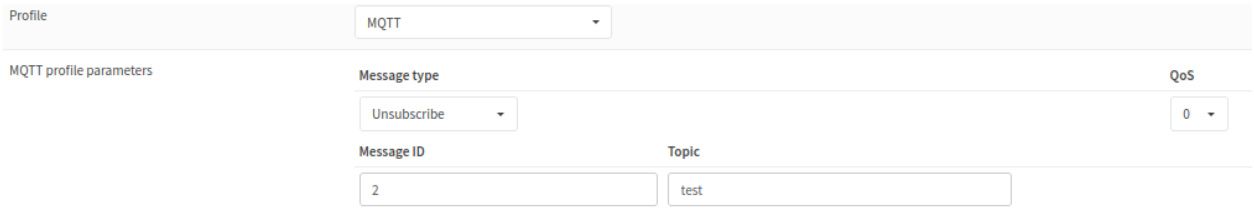


Рис. 18: Профиль Unsubscribe

- Профиль **Disconnect** представлен на рисунке.

Включает параметры **Messsage type**.

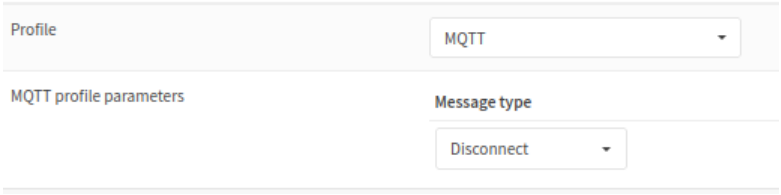


Рис. 19: Профиль Disconnect

Профили фильтрации протокола ModBus

- Профиль **Transaction ID** представлен на рисунке.

Включает параметры **ModBus field type**, **Operation**, **Данные**.

Рис. 20: Профиль Transaction ID

- Профиль **Unit ID** представлен на рисунке.

Включает параметры **ModBus field type**, **Операция**, **Данные**.

- Профиль **Function code** представлен на рисунке.

Включает параметры **ModBus field type**, **Операция**, **Данные**.

2.6.2 Настройка трансляции адресов (NAT)

2.6.2.1 Введение

REFOS имеет механизм трансляции(преобразования) адресов (NAT), который может производить следующие процессы преобразования IP-адресов в заголовке пакета:

- DNAT(Prerouting) – используется для преобразования IP-адреса и номера порта получателя в заголовке пакета;
- SNAT(Postrouting) – используется для преобразования IP-адреса и номера порта отправителя в заголовке пакета;

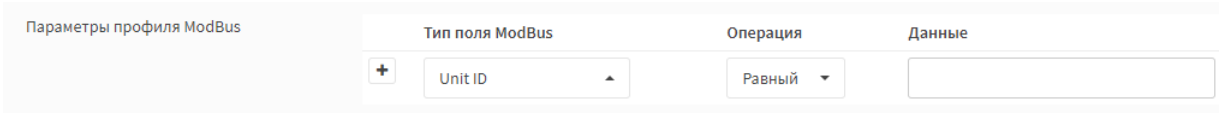


Рис. 21: Профиль Unit ID

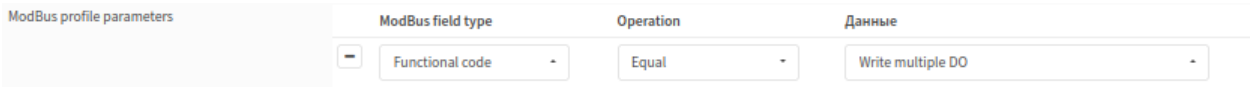


Рис. 22: Профиль Function code

- BINAT – используется для преобразования IP-адреса отправителя и получателя в заголовке пакета.

2.6.2.2 DNAT(Prerouting)

Механизм позволяет перенаправлять поступающий трафик на определенный хост в сети. Система (REFOS) производит преобразование IP-адреса и номера порта получателя в заголовках поступающего трафика, который подходит под условие трансляции.

Весь процесс преобразования адресов DNAT(Prerouting) регулируются правилами перенаправления в разделе **Межсетевой экран - NAT - DNAT (Prerouting)**.

Для конфигурации правила трансляции DNAT(Prerouting) необходимо задать параметры трафика, который подлежит преобразованию, а также параметры перенаправления в соответствии с таблицей.

Таблица 6: Параметры правила перенаправления DNAT(Prerouting)

Параметры трафика, который подлежит преобразованию	
Отключить	Отключить правило перенаправления без его удаления из системы
Интерфейс	Указать интерфейс, на котором будет происходить преобразование адресов. Преобразование должно производиться до процесса обработки и маршрутизации на входящем интерфейсе
Версии TCP/IP	Выбор протокола: • IPv4;
Протокол	Выбор протокола TCP, UDP, ICMP. По умолчанию используется значение Any (Любой)
Отправитель / Инвертировать; Получатель/ Инвертировать;	Трафик, который попадает под правила перенаправления с использованием данной функции, будет игнорироваться и обрабатываться последующими правилами фильтрации, а трафик, который не попадает по параметрам под заданные правила перенаправления с инверсией, будет обрабатываться данным правилом
Отправитель; Получатель;	Указать IP-адрес или целую сеть отправителя или получателя По умолчанию используется значение Любой

продолжается на следующей странице

Таблица 6 – продолжение с предыдущей страницы

Параметры трафика, который подлежит преобразованию	
Диапазон портов источника; Диапазон портов получателя; (Параметры доступны только при выборе протоколов TCP, UDP)	Возможно задать любой порт или список портов источника или получателя, используя параметр Другое. А также можно использовать список портов из поля Хорошо известные порты: FTP, SSH, Telnet, SMTP, DNS, TFTP, HTTP, POP3, IDENT/AUTH, NNTP, NTP, NetBIOS-NS, NetBIOS-DGM, NetBIOS-SSN, IMAP, SNMP, SNMP-Trap, LDAP, HTTPS, MS DS, SMTP/S, ISAKMP, ModBus(TCP), SUBMISSION, IMAP/S, POP3/S, OpenVPN, MS WINS, L2TP, PPTP, MMS/TCP, RADIUS, RADIUS accounting, MSN, MQTT, IEK 60870-5-104; HBCI, MS RDP, STUN, Teredo, IPsec NAT-T, RTP, SIP, VNC, CVSup, MMS/UDP, MQTT(SSL)
Параметры преобразования трафика	
Перенаправление целевого IP-адреса	Задать IP-адрес получателя, на который будет производиться перенаправление. Возможно задать один IP-адрес хоста или Диапазон IP-адресов.
Перенаправлять на порт (ы)	Задать порт(ы) получателя, на который будет производиться перенаправление. Возможно задать любой порт или список портов источника или получателя, используя параметр Другое. А также можно использовать список портов из поля Хорошо известные порты: FTP, SSH, Telnet, SMTP, DNS, TFTP, HTTP, POP3, IDENT/AUTH, NNTP, NTP, NetBIOS-NS, NetBIOS-DGM, NetBIOS-SSN, IMAP, SNMP, SNMP-Trap, LDAP, HTTPS, MS DS, SMTP/S, ISAKMP, ModBus(TCP), SUBMISSION, IMAP/S, POP3/S, OpenVPN, MS WINS, L2TP, PPTP, MMS/TCP, RADIUS, RADIUS accounting, MSN, MQTT, IEK 60870-5-104; HBCI, MS RDP, STUN, Teredo, IPsec NAT-T, RTP, SIP, VNC, CVSup, MMS/UDP, MQTT(SSL).
Журналирование	Запуск журналирования. Журналируется каждый пакет, который попадает под текущее правило перенаправления.
Описание	Общее описание правила преобразования.

Пример конфигурирования правила перенаправления (DNAT) ICMP-трафика

Например, сконфигурируем правило перенаправление DNAT таким образом, чтобы приходящие ICMP запросы на LAN интерфейс с IP-адресом отправителя 10.0.0.2 на IP-адрес получателя 20.0.0.2 направлялись на IP-адрес 20.0.0.3.

2.6.2.3 SNAT(Postrouting)

Механизм позволяет преобразовывать сетевые адреса, т.е. производить изменения исходящего IP адреса в заголовке пакета, который подходит под условие правила перенаправления SNAT (Postrouting).

Процесс преобразования SNAT(Postrouting) состоит в следующем: после обработки пакета (фильтрация, маршрутизация и т.п.) пакет анализируется правилом перенаправления SNAT(Postrouting), где сопоставляются параметры трафика и параметры правила перенаправления SNAT(Postrouting), если происходит совпадение, система производит преобразование порта и/или IP-адреса отправителя.

В системе используются определенные методы преобразования:

- Трансляция по статически заданному IP-адресу - система использует только заданный IP-адрес для замены IP-адреса отправителя в заголовке пакета;

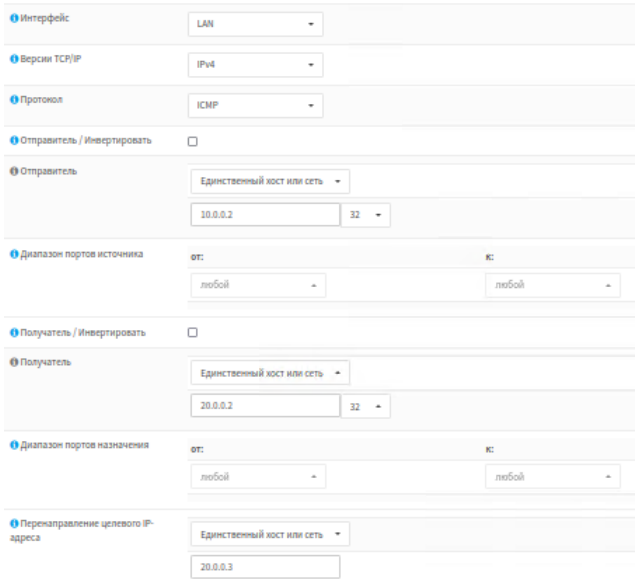


Рис. 23: Пример конфигурирования правила перенаправления (DNAT) ICMP-трафика

- Persistent - система использует только IP-адрес исходящего интерфейса для замены IP-адреса отправителя в заголовке пакета;
- Random и Fully-Random - система использует IP-адрес исходящего интерфейса для замены IP-адреса отправителя и случайный(свободный) номер порта для замены порта отправителя в заголовке пакета.

Весь процесс преобразования адресов SNAT(Postrouting) регулируются правилами перенаправления в разделе **Межсетевой экран - NAT - SNAT(Postrouting)**.

Для конфигурации правила перенаправления SNAT(Postrouting) необходимо задать параметры трафика, который подлежит преобразованию, а также параметры перенаправления SNAT(Postrouting) в соответствии с таблицей.

Таблица 7: Параметры правила перенаправления SNAT(Postrouting)

Параметры трафика, который подлежит преобразованию	
Отключить	Отключить правило перенаправления без его удаления из системы
Интерфейс	Указать интерфейс, на котором будет происходить преобразование адресов. Преобразование должно производиться до процесса обработки и маршрутизации на исходящем интерфейсе
Версии TCP/IP	Выбор протокола: • IPv4;
Протокол	Выбор протокола TCP, UDP, ICMP. По умолчанию используется значение Any (Любой)

продолжается на следующей странице

Таблица 7 – продолжение с предыдущей страницы

Параметры трафика, который подлежит преобразованию	
Отправитель / Инвертировать; Получатель/ Инвертировать;	Трафик, который попадает под правила перенаправления с использованием данной функции, будет игнорироваться и обрабатываться последующими правилами фильтрации, а трафик, который не попадает по параметрам под заданные правила перенаправления с инверсией, будет обрабатываться данным правилом
Отправитель; Получатель;	Указать IP-адрес или целую сеть отправителя или получателя По умолчанию используется значение Любой
Диапазон портов источника; Диапазон портов получателя; (Параметры доступны только при выборе протоколов TCP, UDP)	Возможно задать любой порт или список портов источника или получателя, используя параметр Другое. А также можно использовать список портов из поля Хорошо известные порты: FTP, SSH, Telnet, SMTP, DNS, TFTP, HTTP, POP3, IDENT/AUTH, NNTP, NTP, NetBIOS-NS, NetBIOS-DGM, NetBIOS-SSN, IMAP, SNMP, SNMP-Trap, LDAP, HTTPS, MS DS, SMTP/S, ISAKMP, ModBus(TCP), SUBMISSION, IMAP/S, POP3/S, OpenVPN, MS WINS, L2TP, PPTP, MMS/TCP, RADIUS, RADIUS accounting, MSN, MQTT, IEK 60870-5-104; HBCI, MS RDP, STUN, Teredo, IPsec NAT-T, RTP, SIP, VNC, CVSup, MMS/UDP, MQTT(SSL)
Параметры преобразования трафика	
Перенаправить с исходного IP	Задать IP-адрес отправителя, который будет меняться(преобразовываться) в заголовке пакета. Возможно задать один IP-адрес хоста или Диапазон IP-адресов.
Masquerade	Выбор механизма преобразования IP-адреса и порта отправителя. • Отсутствует – используются заданные параметры из поля Перенаправить с исходного IP; • Persistent - система использует только IP-адрес исходящего интерфейса для замены • IP-адреса отправителя в заголовке пакета; • Random и Fully-Random - система использует IP-адрес исходящего интерфейса для замены • IP-адреса отправителя и случайный(свободный) номер порта для замены порта отправителя в заголовке пакета.
Журналирование	Запуск журналирования. Журналируется каждый пакет, который попадает под текущее правило перенаправления.
Описание	Общее описание правила преобразования.

Пример конфигурирования правила перенаправления (SNAT) ICMP-трафика

Например, сконфигурируем правило перенаправление SNAT таким образом, чтобы перенаправления применялось только к трафику, параметры которого указаны в таблице ниже.

Таблица 8: Пример конфигурирования правила перенаправления (SNAT) ICMP-трафика

Параметры пакета	Значение
Протокол	TCP
Сеть отправителя	10.0.0.0/24
Порт отправителя	200-250
IP-адрес получателя	40.0.0.1
Порт получателя	251-298
Параметры трансляции SNAT	20.0.0.3

В данном случае порты и IP-адреса отправителя в заголовках пакетов, которые инициированы хостами из сети 10.0.0.0/24 в сторону IP-адреса получателя 40.0.0.1, TCP-портом отправителя 200-250 и получателя 251-298, будут меняться на заданный правилом перенаправления IP-адрес - 20.0.0.3.

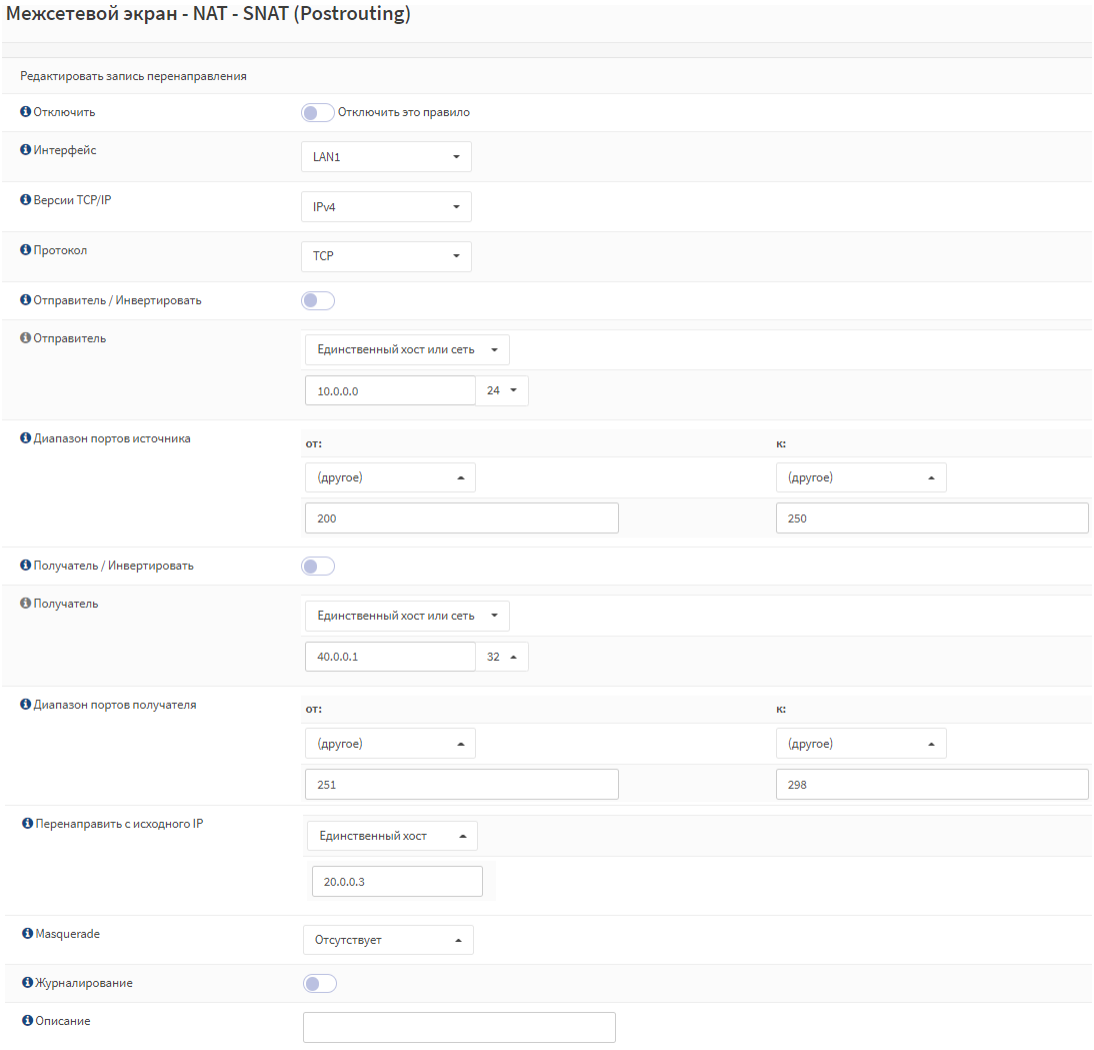


Рис. 24: Пример конфигурирования правила перенаправления (SNAT)

2.6.2.4 BINAT

Двойная трансляция(преобразование) по IP-адресу один к одному. При использовании данного метода трансляции, необходимо задать IP-адрес отправителя и соответственно IP-адрес трансляции(преобразования). Условно говоря, система создает два правила перенаправления SNAT(Postrouting) и DNAT(Prerouting). При прохождении пакета от отправителя, система при помощи SNAT(Postrouting) делает замену IP-адреса отправителя на IP-адрес трансляции(преобразования). При прохождении пакета в обратную сторону, все пакеты с заданным IP-адресом получателя при помощи DNAT(Prerouting) меняются на первоначального отправителя.

Весь процесс преобразования адресов BINAT регулируются правилами перенаправления в разделе **Межсетевой экран - NAT - BINAT** в соответствии с таблицей.

Таблица 9: Параметры правила перенаправления BINAT

Параметры трафика, который подлежит преобразованию	
Отключить	Отключить правило перенаправления без его удаления из системы
Интерфейс	Указать интерфейс, на котором будет происходить преобразование адресов.
Версии TCP/IP	Выбор протокола: • IPv4;
Протокол	Выбор протокола TCP, UDP, ICMP. По умолчанию используется значение Any (Любой)
Отправитель	Указать IP-адрес отправителя
Параметры преобразования трафика	
Перенаправить на IP	Задать IP-адрес получателя, который будет меняться(преобразовываться) в заголовке пакета.
Журналирование	Запуск журналирования. Журналируется каждый пакет, который попадает под текущее правило перенаправления.
Описание	Общее описание правила преобразования.

Пример конфигурирования правила перенаправления (BINAT)

В рамках данного примера сконфигурируем условие трансляции, в котором укажем, что IP-адрес всех пакетов приходящих от хоста ПК 1(10.0.0.2) транслируется(преобразуются) в заданный адрес трансляции (SNAT - 20.0.0.3).

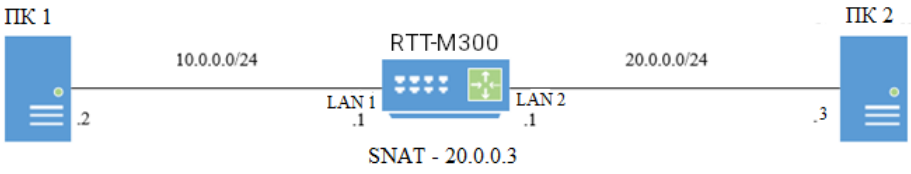


Рис. 25: Пример конфигурации условий трансляции

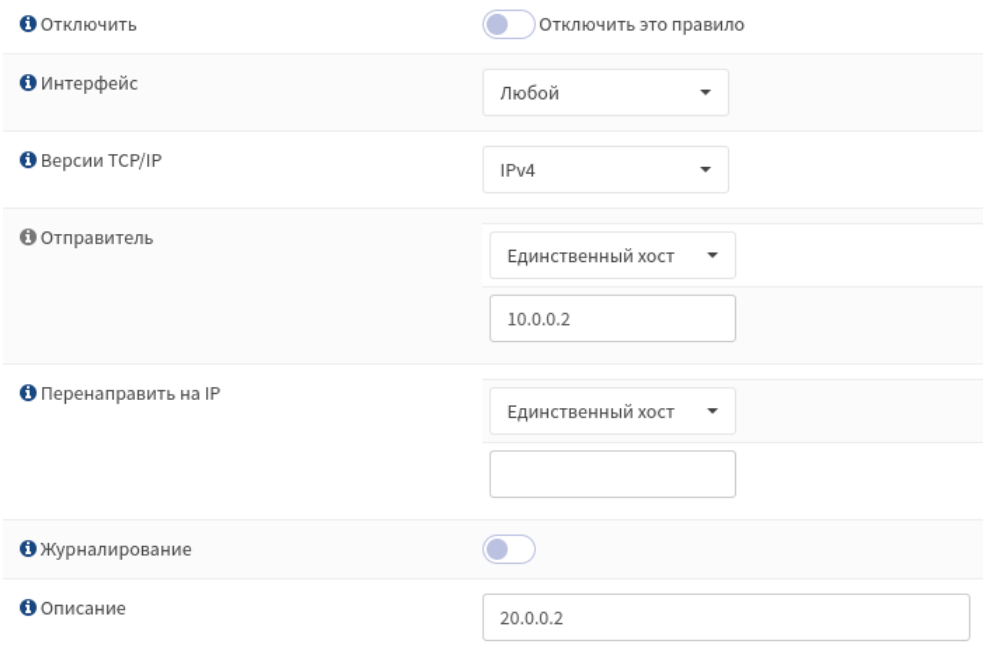


Рис. 26: Пример конфигурирования правила перенаправления (BINAT)

2.6.3 Географическая привязка IP-адресов (GeoIP)

2.6.3.1 Настройка правил фильтрации и перенаправления (NAT) на основе геолокации

Общее описание фильтрации на основе геолокации

Правила фильтрации на основе геолокации позволяют пропускать или ограничивать трафик на основе местонахождения отправителя или получателя.

Система использует базу данных геолокации, которая содержит сопоставление IP-адресов каждому континенту и стране. В процессе обработки пакета, система анализирует IP-адрес в заголовке пакета и сопоставляет его с базой данных геолокации. База данных включает набор континентов и стран, соответствующий таблице.

Таблица 10: Набор континентов и стран

Континенты	Страны
Africa	Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cabo Verde, Cameroon, Central Africa Republic, Chad, Comoros, Congo Republic, Djibouti, DR Congo, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Bissau, Guinea, Ivory Coast, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Mayotte, Morocco, Mozambique, Namibia, Nigeria, Niger, Reunion, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia, Zimbabwe.

продолжается на следующей странице

Таблица 10 – продолжение с предыдущей страницы

Континенты	Страны
Asia	Afghanistan, Armenia, Azerbaijan, Bahrain, Bangladesh, Bhutan, Brunei, Cambodia, China, Georgia, Hong Kong, India, Indonesia, Iran, Iraq, Israel, Japan, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Laos, Lebanon, Macao, Malaysia, Maldives, Mongolia, Myanmar, Nepal, North Korea, Oman, Pakistan, Palestine, Philippines, Qatar, Saudi Arabia, Singapore, South Korea, Sri Lanka, Syria, Taiwan, Tajikistan, Thailand, Turkey, Turkmenistan, United Arab Emirates, Uzbekistan, Vietnam, Yemen.
Europe	Aland, Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Italy, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Russia, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom, Vatican City.
North_Americ	Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, Bonaire Sint Eustatius and Saba, British Virgin Islands, Canada, Cayman Islands, Costa Rica, Cuba, Curacao, Dominica, Dominican Republic, El Salvador, Greenland, Grenada, Guadeloupe.
Oceania	Cook Islands, East Timor, Federated States of Micronesia, Fiji, French Polynesia, Guam, Kiribati, Marshall Islands, Nauru, New Caledonia, New Zealand, Niue, Norfolk Islands, Northern Mariana Islands, Palau, Papua New Guinea, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis and Futuna.
South_Americ	Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Falkland Islands, French Guiana, Guyana, Paraguay, Peru, Suriname, Uruguay, Venezuela.

Фильтрация трафика на основе геолокации регулируется параметрами заданного правила фильтрации и подключенного к нему Псевдонима с базой данных IP-адресов континентов и стран. Псевдонимы — это именованные списки сетей, хостов или портов, которые можно использовать как единое целое в правилах фильтрации и перенаправления (NAT). Псевдонимы позволяют более гибко настроить правила фильтрации, сокращая их количество.

Настройка правил фильтрации с геолокацией

Для настройки правил фильтрации и перенаправления (NAT) на основе геолокации используются Псевдонимы.

Настройка Псевдонимов производится в разделе **Межсетевой экран - Псевдонимы**. Параметр **Тип** – **GeoIP** относится к геолокации.

В параметрах Псевдонима GeoIP необходимо указать Имя и задать любое количество континентов или стран.

Псевдоним можно применить в любом правиле фильтрации и перенаправления (NAT) в параметрах Отправитель/Получатель. В данном случае система будет производить анализ пакета, сопоставляя значения в заголовке с базой данных геолокации заданного псевдонима.

Важно

При увеличении количества правил фильтрации с псевдонимами геолокации, производительность системы будет снижаться

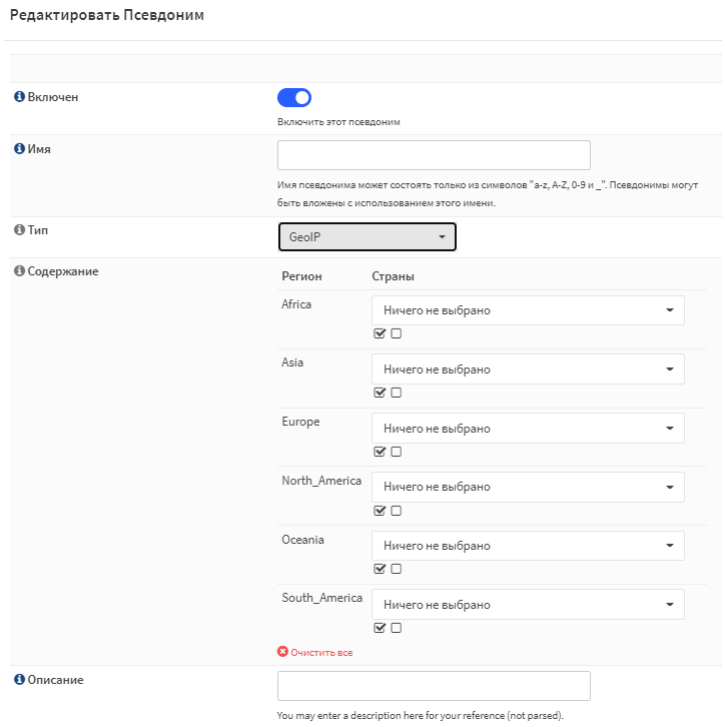


Рис. 27: Псевдоним GeoIP

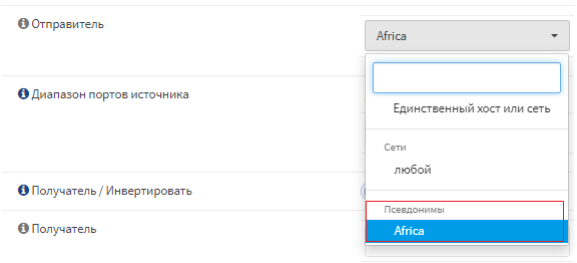


Рис. 28: Применение Псевдонима в параметре Получатель правила фильтрации

Пример настройки правила фильтрации на основе геолокации континента Africa и South_America

Предположим, что необходимо запретить прохождение трафика, инициированного хостами с Африканского континента, а весь трафик с континента Южной Америки разрешить.

Произведем настройку двух Псевдонимов, каждый из которых будет включать по континенту:

1. Перейти в раздел **Межсетевой экран - Псевдонимы** и добавить два псевдонима GeoIP.
2. Задать имя каждому Псевдониму и Локацию (1-й Africa, 2-й South_America).

Рис. 29: Два псевдонима GeoIP

3. Создать два правила фильтрации в соответствии с примером и присвоить каждому правилу соответствующий псевдоним. Т.к. пакет инициируется отправителем, псевдоним необходимо применить к параметру **Отправитель** правила фильтрации.

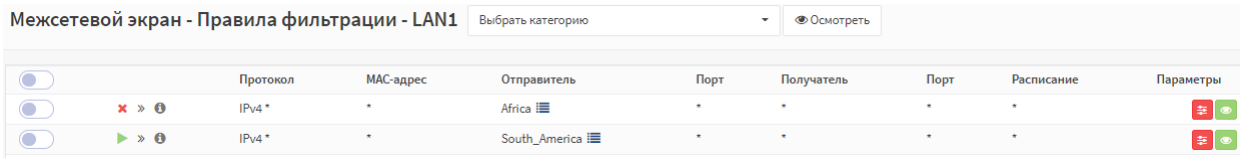


Рис. 30: Два правила фильтрации с примененными Псевдонимами

Настройка правил перенаправления (NAT) с геолокацией

Система позволяет применять Псевдонимы геолокации в правилах перенаправления (NAT).

Процесс применения аналогичен правилам фильтрации. При применении псевдонима геолокации, например, в параметре **Отправитель** правила перенаправления (NAT), система будет производить преобразования адреса (NAT) в тех пакетах, IP-адрес которых сопоставляется с базой данных псевдонима.

Пример настройки правила перенаправления (NAT) на основе геолокации континента Africa и South_America.

Предположим, что необходимо механизмом DNAT произвести перенаправление трафика, инициированный хостами с Африканского континента.

При данной конфигурации все пакеты с IP-адресом отправителя, которые сопоставляются с Псевдонимом **Africa**, будут перенаправляться на IP-адрес 20.0.0.3 вне зависимости от IP-адреса получателя.

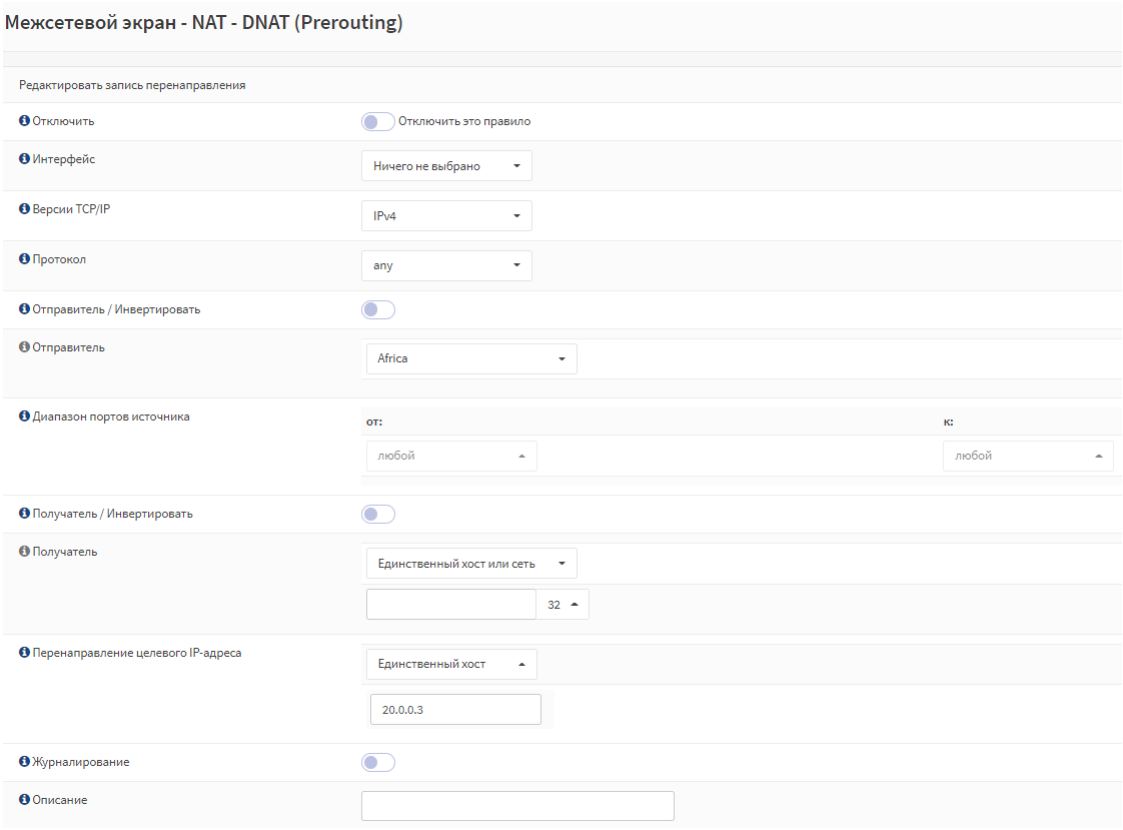


Рис. 31: Конфигурация правила перенаправления (NAT) с геолокацией

2.6.4 Веб-прокси

REFOS позволяет организовать кэширующий прокси-сервер (Веб-прокси), который снижает пропускную способность и улучшает время отклика за счет кэширования и повторного использования часто запрашиваемых веб-страниц. Веб-прокси является посредником между клиентом, инициирующим запрос (HTTP, HTTPs, FTP и др.), и ресурсом (сайт, сервер). Клиент отправляет запрос к ресурсу через прокси-сервер, который, в свою очередь, либо делает запрос от своего имени и возвращает ответ клиенту, либо берет его из кэша.

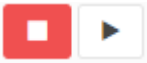
Прокси-сервер выполняет следующие задачи:

- Повышение безопасности сети с помощью шифрования запросов;
- Предотвращение перехвата конфиденциальной информации;
- Блокировка вредоносных сайтов и рекламы;
- Кэширование сайтов для экономии трафика;
- Организация доступа к заблокированным страницам.

REFOS позволяет настроить частный и прозрачный прокси-сервер. Две реализации могут использоваться вместе или один из двух. Частный позволяет настроить аутентификацию доступа для пользователя к запрашиваемому ресурсу. Т.е. при инициировании, например, HTTPs запроса, клиенту необходимо пройти аутентификацию. Прозрачный прокси-сервер просто перехватывает любой (HTTP, HTTPs, FTP и др.) трафик, при этом клиент может использовать все преимущества прокси-сервера без дополнительных настроек браузера.

2.6.4.1 Статус службы прокси-сервера

Служба имеет два состояния:

- Служба запущена  ;
- Служба остановлена  .

Пример конфигурации прозрачного прокси-сервера

Основные настройки прокси-сервера производятся в разделе **Службы: Веб-прокси: Администрирование**.

Базовая настройка прокси-сервера

Конфигурация включает базовые(основные) параметры прокси сервера.

Вкладка **Основные настройки прокси**:

- Запуск прокси-сервера производится параметром **Включить прокси**;
- Для обмена кэша между прокси-серверами используется протокол ICP. Укажите номер UDP-порта для настройки взаимодействия с другими прокси-серверами.

Вкладка **Настройка локального кэша**:

По умолчанию размер кэша ограничен 256Мб. В расширенном режиме возможно управлять параметрами кэша (Размер, расположение и т.д.).

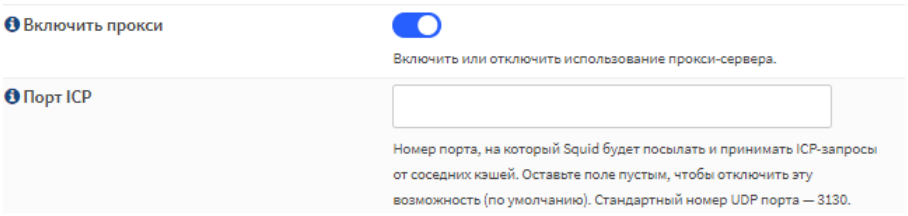


Рис. 32: Основные настройки прокси

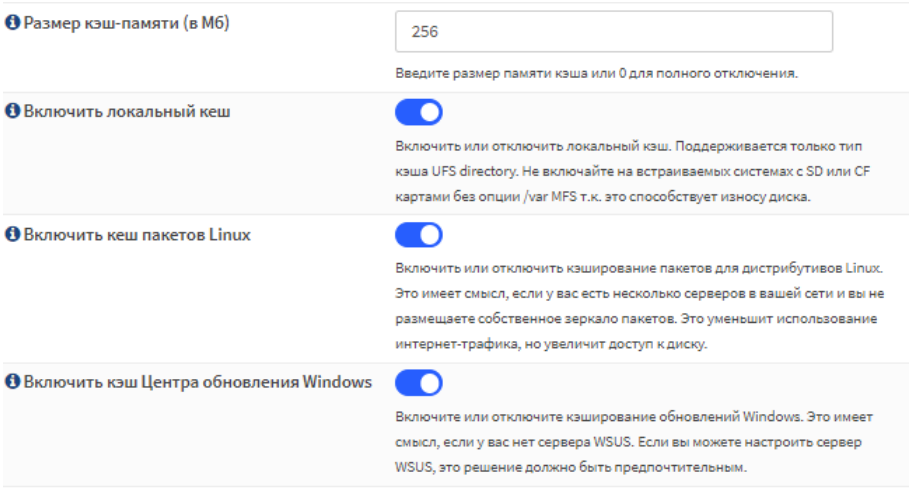


Рис. 33: Настройка локального кэша

Вкладка **Настройка управления трафиком** :

По умолчанию ограничений по управлению трафиком не предусмотрено. Система позволяет задать ограничения размера загружаемых/скачиваемых файлов, а также ограничение пропускной способности.

Вкладка **Настройки родительского прокси-сервера** :

Если в инфраструктуре используется несколько прокси-серверов, в системе возможно указать родительский прокси-сервер для последующего перенаправления трафика.

Для настройки перенаправления запросов на родительский прокси-сервер необходимо выполнить следующие действия:

- Запустить функцию параметром **Включить родительский прокси**;
- Указать IP-адрес родительского прокси-сервера в поле параметра **Хост**;
- Указать порт назначения родительского прокси-сервера в поле параметра **Порт**;
- При наличии аутентификации на родительском прокси-сервере запустить параметр **Включить аутентификацию**, и задать **Имя пользователя** и **Пароль**;
- В дополнительных параметрах **Локальные домены** и **Локальные IP-адреса** возможно указать ограничения по доменам и IP-адресам.

На вкладке **Основные настройки перенаправления** возможно задать основные параметры прокси-сервера:

- Выбрать интерфейсы в параметре **Интерфейсы прокси**, которые будут использоваться для приема запросов прокси-сервером. Если интерфейсы не выбраны, система по умолчанию будет

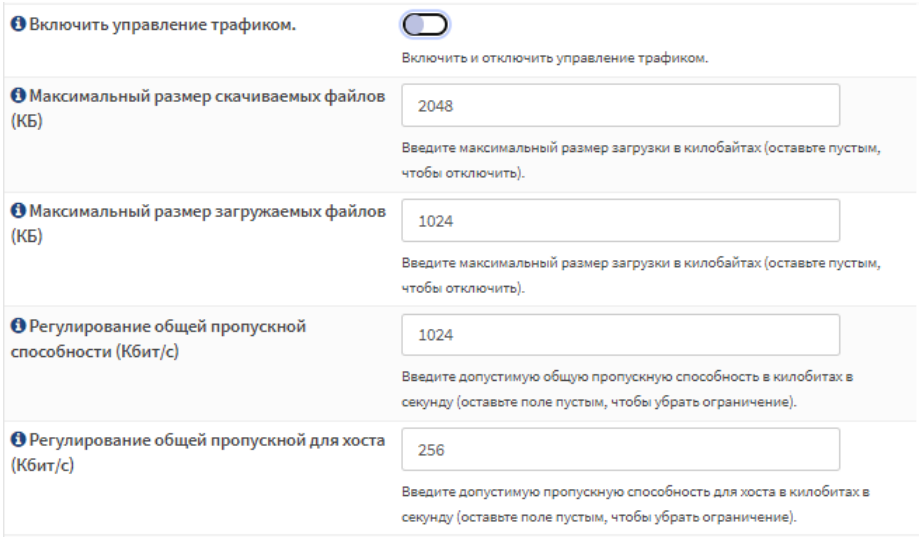


Рис. 34: Настройка управления трафиком

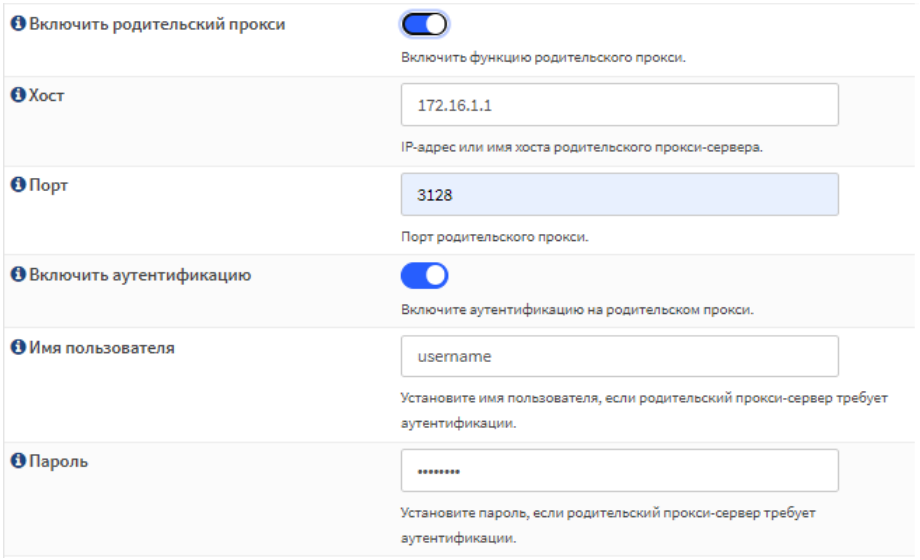


Рис. 35: Настройки родительского прокси-сервера

принимать запросы на всех интерфейсах;

- Указать номер порта в параметре **Номер порта прокси-сервера** для приема запросов прокси-сервером;
- Параметр **Включить прозрачный HTTP-прокси** позволяет настроить прокси-сервер таким образом, чтобы все запросы инициированные клиентом обрабатывались прокси-сервером без предварительной настройки параметров прокси-сервера на самом клиенте.

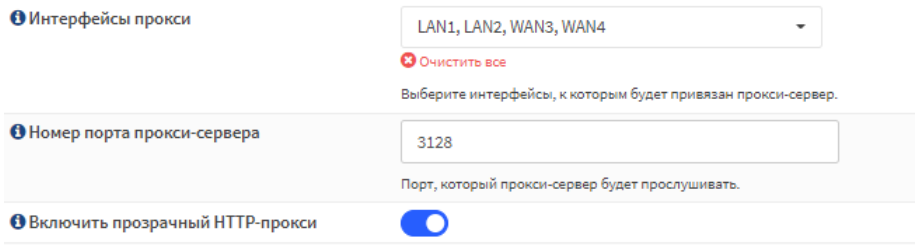


Рис. 36: Основные настройки перенаправления

На вкладке **Настройки FTP-прокси** возможно задать параметры приема FTP-запросов:

- Выбрать интерфейсы в параметре **Интерфейсы FTP-прокси**, которые будут использоваться для приема FTP-запросов прокси-сервером;
- Указать номер порта в параметре **Порт FTP-прокси** для приема FTP-запросов прокси-сервером;
- Параметр **Включить прозрачный режим** позволяет настроить прокси-сервер таким образом, чтобы все FTP-запросы инициированные клиентом обрабатывались прокси-сервером без предварительной настройки параметров прокси-сервера на самом клиенте.

На вкладке **Список управления доступом** возможно задать ограничения пользователей по IP-адресам/подсетям.

- В параметре **Разрешенные подсети** задаются целые адреса подсетей, клиентам которых будет разрешено прохождение запросов через прокси-сервер;
- В параметре **IP-адреса без ограничений** задаются IP-адреса клиентов, которым будет разрешено прохождение запросов через прокси-сервер;
- В параметре **Заблокированные IP-адреса хоста** задаются IP-адреса клиентов, которым будет запрещено прохождение запросов через прокси-сервер.

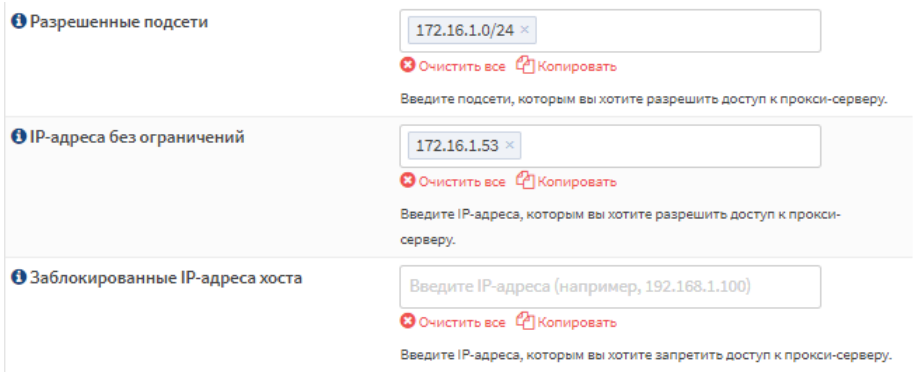


Рис. 37: Список управления доступом

На вкладке **Настройка аутентификации** возможно указать параметры аутентификации для подключения клиента к прокси-серверу:

- В параметре **Метод аутентификации** возможно выбрать метод, при помощи которого клиент будет производить аутентификацию. Local Database – использовать локальную базу данных пользователей системы. Radius Server – аутентификация с использованием локальной базы пользователей системы с дополнительной проверкой на стороннем Radius-сервере;
- В параметре **Принудительно использовать локальную группу** возможно указать группу, пользователей которой можно использовать для аутентификации.

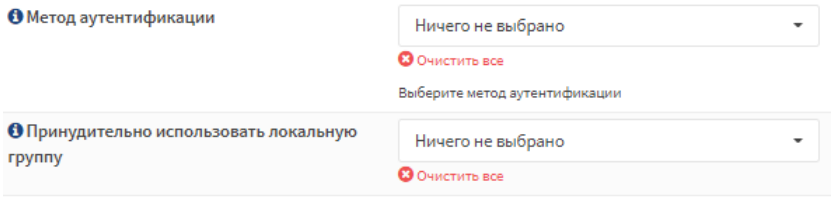


Рис. 38: Настройка аутентификации

2.6.5 Работа с журналами

При работе с устройством необходимо получать информацию о его состоянии и работоспособности. Данную возможность предоставляет пользователю подсистема журналирования.

Благодаря записям в журналах можно узнать о произошедшем инциденте и провести его расследование. Журналы отображают статус работы служб, помогают найти ошибки в их работе.

2.6.5.1 Настройки журналирования

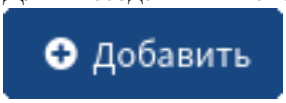
Настройки журналирования (**Система - Настройки - Журналирование**) позволяют настроить параметры, соответствующие таблице.

Таблица 11: Настраиваемые параметры

Наименование параметра	Описание
Максимальный размер журнала	Позволяет настроить размер журналов
Отключить сжатие	Сжатие позволяет сократить количество использованного журналами места на диске
Количество архивных файлов	Максимальное кол-во хранимых журналов каждого типа. Текущий журнал помещается в архив после достижения максимального размера
Количество циклов затирания журналов	После удаления, файлы журналов перезапишутся случайным содержимым указанное количество раз
Удалить журналы	Удаление журналов

2.6.5.2 Сохранение журналов на удаленном сервере

Доступно сохранение журналов на удаленном сервере (**Система - Настройки - Экспорт журналов**).

Для создания нового пункта назначения необходимо нажать кнопку **«Добавить»** 

.

В появившемся окне,, есть возможность указать следующие данные, представленные в таблице.

Таблица 12: Настраиваемые данные

Наименование	Описание
Включен	Включить пункт назначения
Транспортный протокол	Используемый транспортный протокол
Log files	Отправляемые журналы
Имя хоста	Адрес, куда будут отправляться журналы
Порт	Используемый порт
Описание	Описание созданного пункта назначения

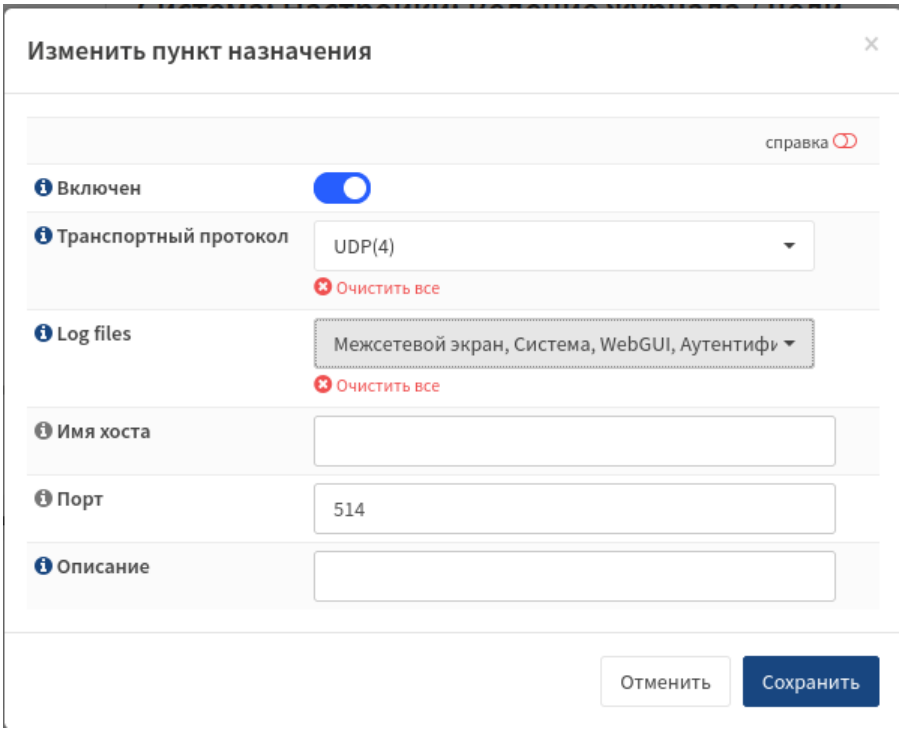


Рис. 39: Создание нового пункта назначения

Далее необходимо нажать кнопку **«Сохранить»** 

и **«Применить»** 

.

После проведенных настроек журналы будут отправляться на указанный адрес.

2.6.5.3 Журналы

Журналы содержат информацию, представленную в таблице.

Таблица 13: Информация, содержащаяся в журналах

Наименование колонки	Описание
Дата	Дата создания записи
Процесс	Процесс-инициатор
Линия	Записанная информация

При помощи кнопки поиска 

можно найти необходимую информацию.

Кнопка **«Обновить»**  предназначена для обновления журнала.

REFOS позволяет указать количество отображаемых записей и скрыть ненужные колонки.

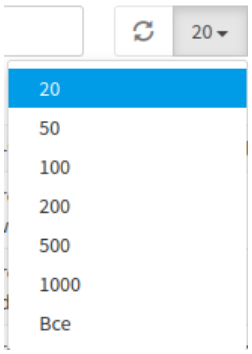


Рис. 40: Указание количества отображаемых записей

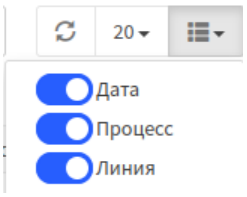


Рис. 41: Скрыть ненужные колонки

2.6.5.4 Журналы межсетевого экрана

Журналы межсетевого экрана содержат информацию, представленную в таблице.

Таблица 14: Информация, содержащаяся в журналах межсетевого экрана

Наименование колонки	Описание
Интерфейс	Наименование интерфейса, вызвавшего срабатывание правила
Время	Время срабатывания правила
Отправитель	Адрес отправителя
Получатель	Адрес получателя
Протокол	Используемый протокол
Метка	Подсказка, используемая в правиле

При нажатии на кнопку информации  , можно получить подробную информацию о сработавшем правиле.

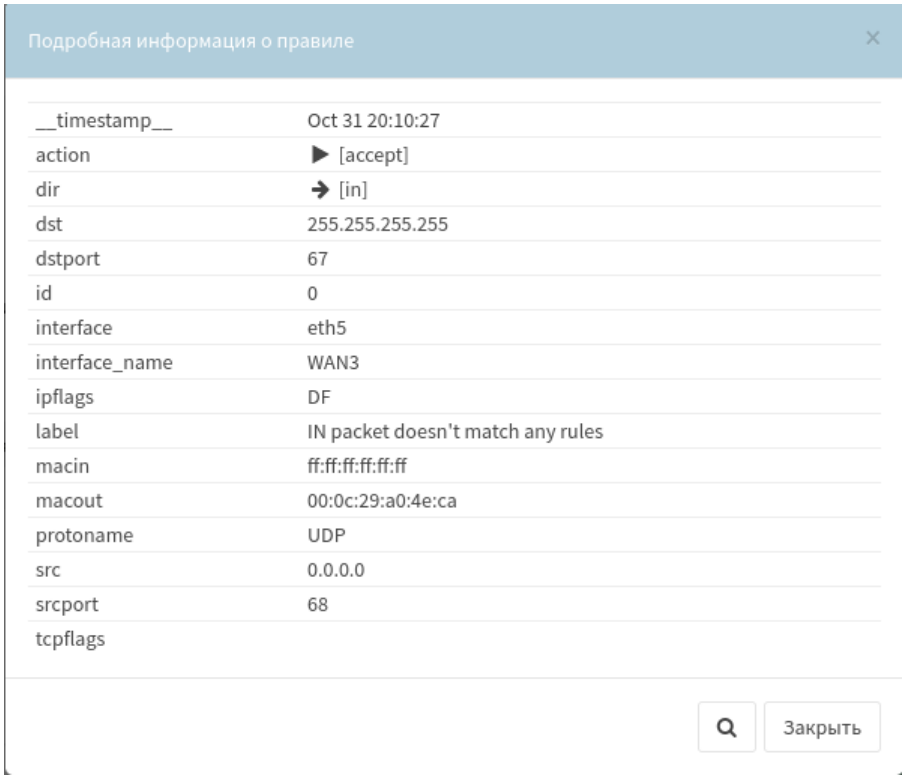
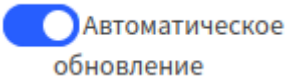


Рис. 42: Подробная информация о сработавшем правиле

Для сортировки записей необходимо выбрать критерий и нажать на кнопку **«Добавить»**  .

REFOS позволяет остановить обновление журнала с помощью кнопки 

и выбрать количество записей.

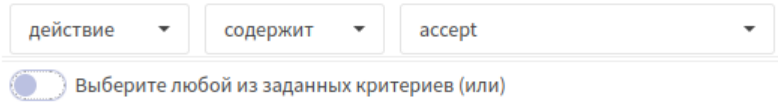


Рис. 43: Выбор необходимого критерия сортировки

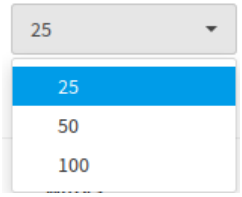


Рис. 44: Выбор количества записей

Для обновления журнала необходимо нажать на кнопку **«Обновить»**  .

2.6.5.5 Журналы вкладки «Обзор»

С помощью журналов во вкладке «Обзор» можно посмотреть диаграмму по необходимым атрибутам. Перечень доступных атрибутов соответствует таблице.

Таблица 15: Доступные атрибуты диаграммы

Название атрибута
Действия
Интерфейсы
Протоколы
IP-адреса источника
IP-адреса назначения
Порты источника
Порты назначения

Диаграмма представлена на рисунке

в случае необходимости можно перестроить данную диаграмму, исключив ненужные данные.

Для исключения данных необходимо нажать на их кружок.

2.6.5.6 Доступные журналы

В REFOS доступны журналы, приведенные в таблице.

Таблица 16: Доступные журналы

Наименование журнала	Расположение
Общий журнал	Система - Файлы журнала
Ошибки ядра	Сиситема - Файлы журнала - Ошибки системы

продолжается на следующей странице

Таблица 16 – продолжение с предыдущей страницы

Наименование журнала	Расположение
Службы	Сиситема - Файлы журнала - Ошибки системы
Система	Сиситема - Файлы журнала - Аутентификация
Web	Сиситема - Файлы журнала - Аутентификация
Предупреждения	Сиситема - Файлы журнала - Web-интерфейс
Ошибки веб-сервера	Сиситема - Файлы журнала - Web-интерфейс
Информация о веб-сервере	Сиситема - Файлы журнала - Web-интерфейс
Аудит	Сиситема - Файлы журнала - Web-интерфейс
Фильтр трафика	Межсетевой экран - Файлы журнала - Прямая трансляция
NAT	Межсетевой экран - Файлы журнала - Прямая трансляция
Действия	Межсетевой экран - Файлы журнала - Обзор
Интерфейсы	Межсетевой экран - Файлы журнала - Обзор
Протоколы	Межсетевой экран - Файлы журнала - Обзор
IP-адреса источника	Межсетевой экран - Файлы журнала - Обзор
IP-адреса назначения	Межсетевой экран - Файлы журнала - Обзор
Порты источника	Межсетевой экран - Файлы журнала - Обзор
Порты назначения	Межсетевой экран - Файлы журнала - Обзор
Журнал (VPN)	VPN - OpenVPN - Журнал
Журнал / Clamd	Службы - ClamAV - Журнал / Clamd
Журнал / Freshclam	Службы - ClamAV - Журнал / Freshclam
Журнал (Сетевое время)	Службы - Сетевое время - Журнал
Журнал кэша	Службы - Веб-прокси - Журнал кэша
Журнал доступа	Службы - Веб-прокси - Журнал доступа
Store Log	Службы - Веб-прокси - Store Log

2.6.6 Источник системного времени

В качестве системного времени дистрибутива REFOS используется аппаратное время, то есть время модуля RTC (real time clock) аппаратной платформы, или сетевое время, получаемое по протолку NTP.

Приоритетным является сетевое время, в случае его доступности. Оно также является источником для обновления (корректировки) аппаратного времени.

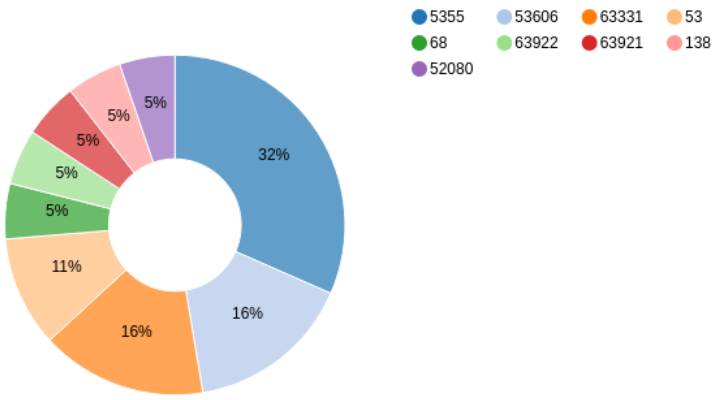
Примечание

В случае отсутствия источников аппаратного и сетевого времени используется внутреннее несинхронизированное с каким-либо источниками время, которое может существенно отличаться от актуального астрономического времени. Данная ситуация говорит о серьезной неисправности аппаратной платформы (модуль RTC содержит неактуальное время или недоступен)

Аппаратное время не доступно для изменения пользователем и обновляется автоматически. Для получения сетевого времени необходимо настроить его источник на странице Web-интерфейса устройства **«Службы - Сетевое время - Общие настройки»**.

Для этого нужно настроить интерфейсы, через которые будет получаться сетевое время (на которых доступны серверы времени).

Далее необходимо указать адреса серверов, которые система будет использовать как источник времени.



Порты источника	#
5355	6
53606	3
63331	3
53	2
68	1
63922	1
63921	1
138	1
52080	1

Рис. 45: Диаграмма

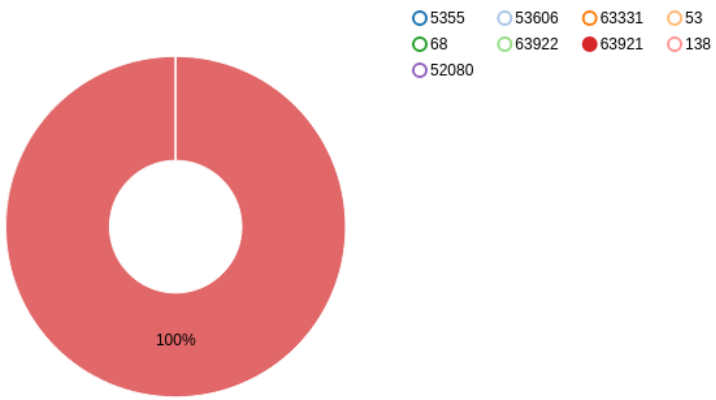


Рис. 46: Исключение данных

Рис. 47: Настройка интерфейсов

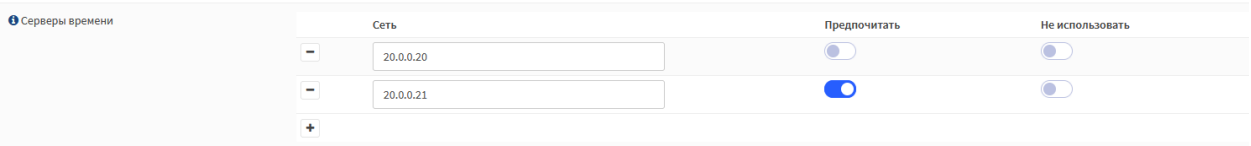


Рис. 48: Адреса серверов

Для обеспечения достаточного резервирования желательно настроить от трех до пяти серверов. Опция **«Предпочитать»** указывает, что для NTP более предпочтителен отмеченный сервер, чем остальные.

Опция **«Не использовать»** указывает, что NTP не должен использовать этот сервер для синхронизации времени, но статистика для этого сервера будет собираться и отображаться.

2.6.7 Настройка VPN соединения

2.6.7.1 Введение

VPN (Virtual Private Network - Виртуальная частная сеть) – технология, которая позволяет организовать защищенное соединение поверх любой IP-сети (инфраструктуры). Все данные, которые передаются по соединениям VPN шифруются различными алгоритмами шифрования. Поэтому обеспечивается полная конфиденциальность и целостность передаваемой информации.

REFOS позволяет организовывать защищенные соединения, используя функциональное расширение OpenVPN.

Важно

Функциональное расширение OpenVPN распространяется по платной лицензии

OpenVPN позволяет организовать защищенные соединения следующих типов:

- Организация удаленного доступа пользователей к ресурсам удаленной сети (Remote access VPN). В данном случае REFOS выступает в качестве VPN-сервера, который предоставляет защищенный доступ VPN-клиентам. VPN-клиентом может являться любой ПК с соответствующим установленным ПО;
- Организация защищенного соединения между офисами (Site-to-Site VPN). В данном случае REFOS может выступать в роли как сервера, так и клиента. VPN-клиент инициирует подключение к VPN-серверу, а VPN-сервер согласовывает подключения и объединяет территориально распределенные офисы компании в одну логическую сеть.

VPN-соединением между клиентом и сервером также называют туннелем.

Для настройки VPN-соединений используются следующие режимы работы:

- Peer to Peer Server (SSL/TLS) – режим сервера с TLS-аутентификацией для подключения удаленных VPN-клиентов;
- Peer to Peer Client (SSL/TLS) – режим клиента с TLS-аутентификацией;
- Удаленный доступ (SSL/TLS) - режим сервера с TLS-аутентификацией и расширенным сетевыми параметрами для подключения удаленных пользователей;
- Удаленный доступ (Аутентификация пользователя) - режим сервера с аутентификацией по локальной базе сервера и дополнительными сетевыми параметрами для подключения удаленных пользователей;
- Удаленный доступ (SSL/TLS+Аутентификация пользователя) - режим сервера с TLS-аутентификацией и дополнительной аутентификацией по локальной базе сервера, а также дополнительными сетевыми параметрами для подключения удаленных пользователей.

2.6.7.2 Настройка конфигурации VPN-соединения между офисами (Site-to-Site VPN)

Предположим, необходимо объединить VPN-туннелем два территориально распределенных офиса.

Одна система REFOS будет выступать в качестве сервера, а вторая в качестве клиента.

Для аутентификации пользователя и согласования VPN-соединения необходимо использоваться сертификат клиента, сертификат удостоверяющего цента и общий ключ при использовании TLS-аутентификации.

Важно

Процесс генерации и управления сертификатами изложен в разделе **Доверенные сертификаты**

2.6.7.3 Настройка конфигурации VPN-сервера в режиме Peer to Peer Server (SSL/TLS)

В разделе **VPN - OpenVPN - Серверы/клиенты** в соответствии с таблицей производится добавление конфигурации.

Таблица 17: Добавление конфигурации VPN-сервера

Параметр	Описание
Общая информация	
Описание	Задать общее наименование соединения.
Режим	Выбрать режим VPN-сервера – Peer to Peer Server (SSL/TLS).
Протокол	Используется по умолчанию – UDP.
Режим работы устройства	Используется по умолчанию – TUN.
Интерфейс	Выбрать интерфейс, на котором будет производится прослушивание входящих соединений от VPN-клиентов. Используется по умолчанию – Any.
Локальный порт	Номер порта, который использует сервис OpenVPN. Используется по умолчанию – 1194.
Криптографические установки	

продолжается на следующей странице

Таблица 17 – продолжение с предыдущей страницы

Параметр	Описание
Аутентификация TLS	В данном примере используется Аутентификация TLS. Поэтому необходимо: • Включить аутентификацию пакетов TLS; • Автоматически генерировать совместно использующийся ключ аутентификации TLS. Общий ключ аутентификации TLS генерируется во время сохранения конфигурации. Поэтому после сохранения конфигурации для просмотра и передачи общего ключа клиенту необходимо открыть данную конфигурацию заново.
Центр сертификации пиров	Добавить центр сертификации. Первоначально необходимо создать или импортировать центр сертификации.
Список отзыва сертификатов узлов	Необязательный параметр. Используется по умолчанию – None.
Сертификат сервера	Задать сертификат VPN-сервера. Первоначально необходимо создать или импортировать сертификат VPN-сервера.
Длина параметров DH	Задать длину ключа Диффи-Хеллмана. Используется по умолчанию – 2048 бит.
Алгоритм шифрования	Задать алгоритм шифрования. Используется по умолчанию – AES-128-CBC.
Дайджест-алгоритм аутентификации	Задать алгоритм хеширования. Используется по умолчанию – SHA-1.
Уровень сертификата	Задать уровень сертификата. Используется по умолчанию – Один (клиент+сервер).
Настройки туннеля	
Туннельная сеть IPv4	Задать параметры туннельной сети. Пример ввода – 99.0.0.0/24. Данный параметр относится к адресации сети, которая используется в созданном туннеле. Туннель является двух точечным соединением с использованием сторонней заданной адресацией, которая не пересекается с адресацией физических интерфейсов. При использовании адреса сети 99.0.0.0/24, адрес локального интерфейса туннеля VPN-сервера будет использоваться первый из данной сети – 99.0.0.1, а для клиента будет использоваться второй 99.0.0.2.
Локальная сеть IPv4	Необязательный параметр. Задать сети, напрямую подключенные к шлюзу. В данном случае возможно анонсировать напрямую подключенные сети удаленному шлюзу. В таблице маршрутизации удаленного шлюза появится информация о данных сетях, доступных через созданный туннель. Пример ввода – 10.0.0.0/24.

продолжается на следующей странице

Таблица 17 – продолжение с предыдущей страницы

Параметр	Описание
Удаленная сеть IPv4	Необязательный параметр. Задать удаленные сети, которые доступны для данного сервера через VPN-тоннель. Пример ввода – 20.0.0.0/24.
Число одновременных подключений	Необязательный параметр. Задать количество подключаемых клиентов. По умолчанию ограничение не стоит.
Сжатие	Необязательный параметр. Задать сжатие туннельных пакетов для оптимизации производительности. По умолчанию параметры не настроены.
Тип сервиса	Необязательный параметр. По умолчанию параметры не настроены.
Динамический IP-адрес	Необязательный параметр. По умолчанию параметры не настроены.
Топология сети	Необязательный параметр. По умолчанию параметры не настроены.

Пример конфигурации VPN-сервера представлен на рисунке.

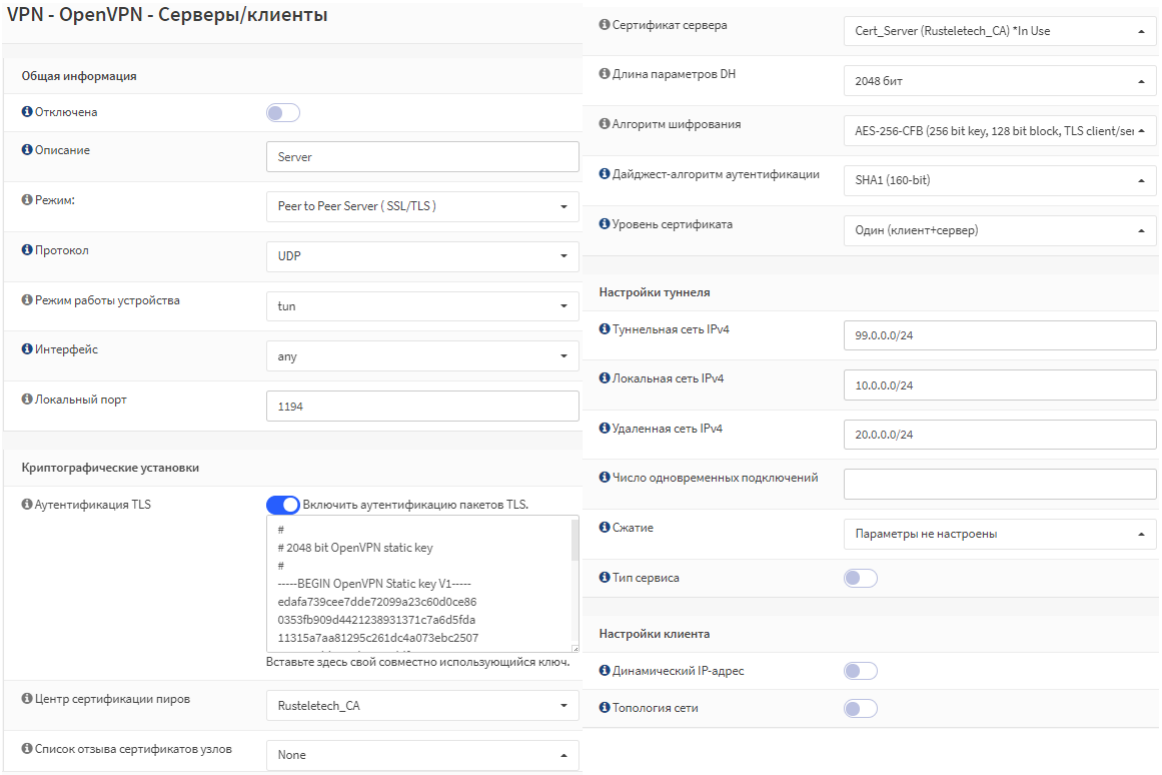


Рис. 49: Пример конфигурации VPN-сервера

2.6.7.4 Настройка конфигурации VPN-клиента в режиме Peer to Peer Client (SSL/TLS)

Настройка конфигурации VPN-клиента на второй системе REFOS. В разделе **VPN - OpenVPN - Серверы/клиенты** в соответствии с таблицей производится добавление конфигурации.

Таблица 18: Добавление конфигурации VPN-клиента

Параметр	Описание
Общая информация	
Описание	Задать общее наименование соединения.
Режим	Выбрать режим VPN-сервера – Peer to Peer Client (SSL/TLS).
Протокол	Используется по умолчанию – UDP.
Режим работы устройства	Используется по умолчанию – TUN.
Интерфейс	Выбрать интерфейс, на котором будет инициировать подключение к VPN-серверу. Используется по умолчанию – LAN1.
Удаленный сервер	Задать IP-адрес интерфейса и номер порта VPN-сервиса.
Локальный порт	Используется по умолчанию – 1195.
Настройки Аутентификации пользователей	
Имя пользователя/пароль	Необязательный параметр. Задать имя пользователя и пароль из локальной базы пользователей VPN-сервера. Дополнительный метод аутентификации.
Время пересогласования	Необязательный параметр. По умолчанию не используется.
Криптографические установки	
Аутентификация TLS	В данном примере используется Аутентификация TLS. Поэтому необходимо: • Включить аутентификацию пакетов TLS. Ввести в поле Общий ключ аутентификации TLS, который генерируется на VPN-сервере.
Центр сертификации пиров	Добавить центр сертификации. Первоначально необходимо импортировать сертификат корневого. центра сертификации VPN-сервера.
Список отзыва сертификатов узлов	Необязательный параметр. Используется по умолчанию – None.
Сертификат клиент	Задать сертификат VPN-клиента. Первоначально необходимо импортировать сертификат. VPN-клиента.
Длина параметров DH	Задать длину ключа Диффи-Хеллмана. Используется по умолчанию – 2048 бит. Значение параметра должно быть сопоставимо с значением конфигурации VPN-сервера.
Алгоритм шифрования	Задать алгоритм шифрования. Используется по умолчанию – AES-128-CBC. Значение параметра должно быть сопоставимо с значением конфигурации VPN-сервера.

продолжается на следующей странице

Таблица 18 – продолжение с предыдущей страницы

Параметр	Описание
Дайджест-алгоритм аутентификации	Задать алгоритм хеширования. Используется по умолчанию – SHA-1. Значение параметра должно быть сопоставимо с значением конфигурации VPN-сервера.
Уровень сертификата	Задать уровень сертификата. Используется по умолчанию – Один (клиент+сервер).
Настройки туннеля	
Туннельная сеть IPv4	Задать параметры туннельной сети. Пример ввода – 99.0.0.0/24. Данный параметр относится к адресации сети, которая используется в созданном туннеле Туннель является двух точечным соединением с использованием сторонней заданной адресацией, которая не пересекается с адресацией физических интерфейсов. При использовании адреса сети 99.0.0.0/24, адрес локального интерфейса туннеля VPN-сервера будет использоваться первый из данной сети – 99.0.0.1, а для клиента будет использоваться второй 99.0.0.2.
Удаленная сеть IPv4	Необязательный параметр. Задать удаленные сети, которые доступны для данного клиента через VPN-тоннель. Пример ввода – 10.0.0.0/24.
Ограничить исходящую пропускную способность	Необязательный параметр. Ограничение исходящей пропускной способности туннеля в байтах/сек. По умолчанию ограничение не стоит.
Сжатие	Необязательный параметр. Задать сжатие туннельных пакетов для оптимизации производительности. По умолчанию параметры не настроены.
Тип сервиса	Необязательный параметр. По умолчанию параметры не настроены.
Не получать маршруты	Необязательный параметр. По умолчанию не используется.
Не добавлять/удалять маршруты	Необязательный параметр. По умолчанию не используется.

Пример конфигурации VPN-клиента представлен на рисунке.

2.6.7.5 Статус VPN-соединения

Проверка состояния соединения между VPN-сервером и VPN-клиентом производится в разделе **VPN - OpenVPN - Статус соединения**.

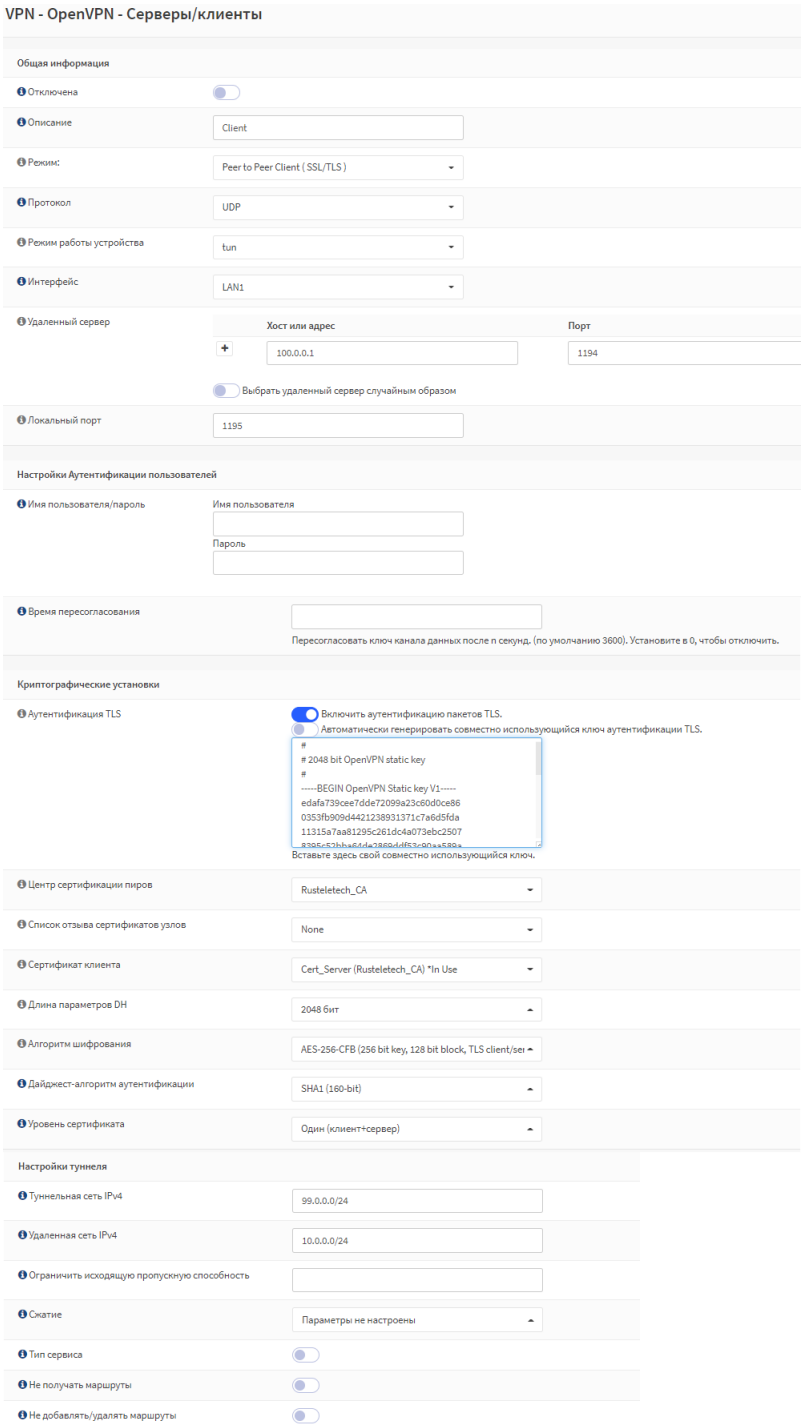


Рис. 50: Пример конфигурации VPN-клиента

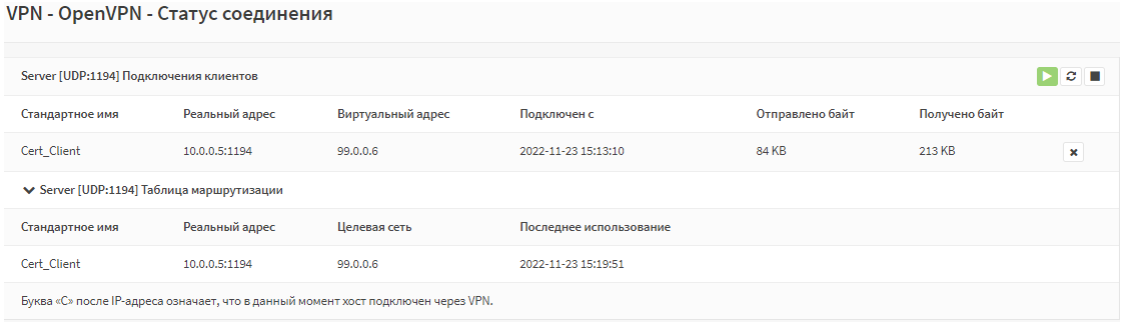


Рис. 51: Статус соединения

2.6.7.6 Настройка конфигурации VPN-сервера с использованием режима Удаленный доступ

Режимы Peer to Peer позволяют связать несколько территориально распределенных сегментов сети защищенным каналом. В данном случае речь идет о филиальной сети. Но также существует потребность предоставления защищенного канала одному или нескольким пользователям для удаленного доступа к информационным ресурсам компании. Режим Удаленный доступ с разным типом аутентификации позволяет настроить VPN-сервер с дополнительными сетевыми параметрами для удаленного пользователя.

К дополнительным сетевым параметрам относится:

- Предоставление параметров DNS-серверов клиентам;
- Предоставление параметров NTP-серверов клиентам.

Описание дополнительных сетевых параметров приведено в таблице.

Таблица 19: Описание дополнительных сетевых параметров

Параметр	Описание
Домен DNS по умолчанию	Указать доменное имя клиентам
DNS-серверы	Указать клиентам список используемых DNS - серверов
NTP-серверы	Указать клиентам список используемых NTP - серверов

2.6.8 ClamAV

Потоковый антивирус, который позволяет при интеграции с прокси-сервером ограничивать доступ к определенным ресурсам и проводить проверку загружаемых файлов. Для анализа ресурсов и данных система использует базу данных антивирусных сигнатур.

2.6.8.1 Интеграция ClamAV с прокси-сервером

Для корректного использования антивирусного модуля ClamAV необходимо настроить интеграцию с прокси-сервером по протоколу ICAP, который позволяет производить обмен данными между двумя функциями. Протокол ICAP настраивается на каждой стороне двух сервисов прокси-сервера и ClamAV.

Важно

Сервис ClamAV функционирует только при интеграции с прокси-сервером. Т.е. перед настройкой ClamAV, необходимо настроить прокси-сервер

Настройка протокола ICAP на стороне прокси-сервера доступна в разделе **Службы: Веб-прокси: Администрирование** – вкладка **Настройки ICAP**.

Достаточно запустить протокол ICAP и указать Антивирус.

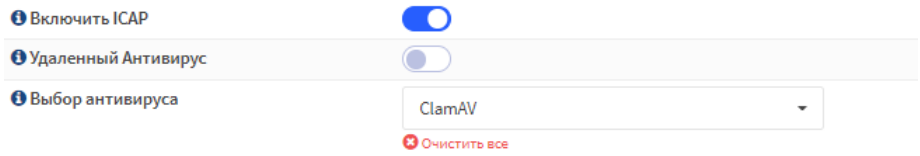


Рис. 52: Настройки ICAP

2.6.8.2 Настройка сервиса ClamAV

Настройка параметров ClamAV производится в разделе **Службы: ClamAV: Конфигурация**.

Описание общих параметров приведено в таблице.

Таблица 20: Описание общих параметров ClamAV

Параметр	Описание
Включить службу	Запустить основную службу ClamAV - ClamAV Service.
Включить службу обновления вирусных баз данных	Запустить службу обновления антивирусных баз - DB update Service. При использовании основной службы данная служба должна быть также запущена.
Максимальное количество запущенных потоков	Ограничение запущенных потоков позволяет избежать отказа работы основного сервиса.
Максимальное количество элементов в очереди	Максимальное количество файлов, которые могут быть в очереди на сканирование.
Значение тайм-аута бездействия	Параметр используется для разрыва неактивного соединения.

продолжается на следующей странице

Таблица 20 – продолжение с предыдущей страницы

Параметр	Описание
Максимальная рекурсия директории	Ограничение глубины дерева каталогов. Сканер ClamAV может работать бесконечно в цикле, если текущий параметр не задан.
Отключить кэш	Отключить кэширование результатов сканирования.
Сканировать переносимый исполняемый файл	Для сканирования PE-файлов(.exe, .dll и т.д) используется данный параметр.
Сканировать исполняемый файл и формат ссылки	Для сканирования ELF-файлов(используются в UNIX-системах) используется данный параметр.
Обнаруживать повреждённые исполняемые файлы	Если исполняемый файл не соответствует спецификации, данный файл помечается как поврежденный и блокируется. Исполняемый файл может быть поврежден из-за проблемы с загрузкой или иными манипуляциями.
Сканировать OLE2	Анализ файлов OLE2 (например, файлы Microsoft Office).
Блокировать OLE2 макросы	Блокировка всех документов, содержащих макросы.
Сканировать файлы PDF	Сканирование файлов PDF. Файлы PDF могут содержать другие файлы или мультимедиа, а также javascript и шрифты. Рекомендуется использовать сканирование PDF-файлов.
Сканировать SWF	Сканирование файлов с Flash-контентом. Flash используется для интерактивного контента и видеоплееров.
Сканировать XMLDOCS	Сканирование XML-документов.
Сканировать HWP3	Сканирование HWP-документов.
Декодировать файлы почты	Сканирование вложение писем электронной почты.
Сканировать HTML	Сканирование HTML-файлов, которые могут содержать опасный встроенный JavaScript.
Сканировать архивы	Сканирование файлы внутри архивов. Архивы могут содержать вредоносное ПО.
Блокировать зашифрованные архивы	Блокировать зашифрованные архивы, т.к. данные архивы могут содержать вредоносное ПО.
Максимальный размер сканирования	Задать максимальное количество данных для сканирования каждого файла. Архивы и другие контейнеры рекурсивно извлекаются и сканируются до этого значения.
Максимальный размер файла	Ограничение по объему файла, который система просканирует. Файл по объему выше ограничения просканирован не будет.
Максимальная рекурсия	Задать максимальную рекурсию вложеных архивов.
Максимум файлов	Ограничение сканирования по количеству файлов в архиве.
Детальность лога freshclam	Запуск подробного логирования в Журнал / Freshclam.
Зеркало базы данных freshclam	Репозиторий обновления антивирусных баз.
Таймаут соединения freshclam	Таймаут в секундах для подключения к серверу базы данных.
Добавьте сигнатуры экспертов по вредоносным программам	Активация сигнатур третьих лиц от Malware Expert.
Добавить подписи BLURL	Активация сторонних подписей от BLURL.
Добавить подписи JURLBLA	Активация сторонних подписей от Sanesecurtiy JURLBLA.
Добавить подписи BOFHLand	Активация сторонних подписей от Sanesecurtiy BOFHLand.

Описание параметров протокола ICAP на стороне сервиса ClamAV приведено в таблице

Таблица 21: Описание параметров протокола ICAP на стороне сервиса ClamAV

Параметр	Описание
Включить сервис icap	Запустить протокол ICAP.
Тайм-аут	Время в секундах после которого неактивное соединение может быть прервано.
Максимум keepalive запросов	Максимальное число запросов, которое может обслужить одно соединение.
Максимальный таймаут keepalive	Время в секундах после которого неактивное соединение может быть прервано, если соединение также остается неактивным.
Старт серверов	Количество серверных процессов, которые будут запущены.
Максимум серверов	Ограничение количества процессов.
Минимальное количество свободных потоков	Максимальное число процессов сервера.
Использовать ICAP совместно с прокси сервером squid	Использовать настройки имени пользователя локального squid.
Максимальный размер объекта	Максимальный размер файлов для сканирования службой антивируса. Вы можете использовать K и M индикаторы для обозначения размера в килобайтах и мегабайтах.

2.6.8.3 Состояние служб сервиса ClamAV

Сервис ClamAV использует для работы две службы:

- ClamAV Service – основная служба ClamAV;
- DB update Service - служба для обновления антивирусных баз ClamAV.

Для корректной работы сервиса ClamAV, службы должны находится в активном состянии.

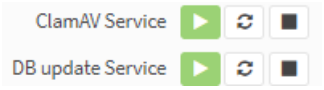


Рис. 53: Активное состояние сервиса ClamAV

Неактивное состояние служб сервиса ClamAV показано на рисунке.

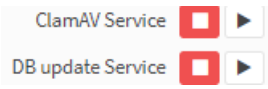


Рис. 54: Неактивное состояние сервиса ClamAV

Для запуска служб достаточно нажать кнопку  .

2.6.8.4 Логирование служб сервиса ClamAV

В разделе **Службы: ClamAV: Журнал / Clamd** производится логирование основной службы ClamAV Service. Логи помогают разобраться с проблемами запуска и настройки сервиса ClamAV.

В разделе **Службы: ClamAV: Журнал / Freshclam** производится журналирование процесса подключения к репозиторию и синхронизации антивирусных баз. Логи помогают разобраться с проблемами обновления антивирусных баз.

2.6.9 Настройка резервирования на основе CARP

2.6.9.1 Резервирование IP-адреса шлюза посредством протокола CARP

В рамках резервирования IP-адреса шлюза посредством протокола CARP проверяется отказоустойчивость шлюза на уровне IP-адреса.

Для резервирования шлюза используется два физических подключения, которые подключены в разные юниты RTT-M300, которые соединяют два сегмента сети LAN и WAN. CARP позволяет произвести резервирование шлюза на уровне IP-адреса, распределяя роли юнитов ведущий и ведомый. Ведущий будет шлюзом для каждого сегмента до момента аварии или повреждения линка. Если ведущий юнит откажет, тогда роль ведущего примет ведомый и будет выступать в качестве шлюза.

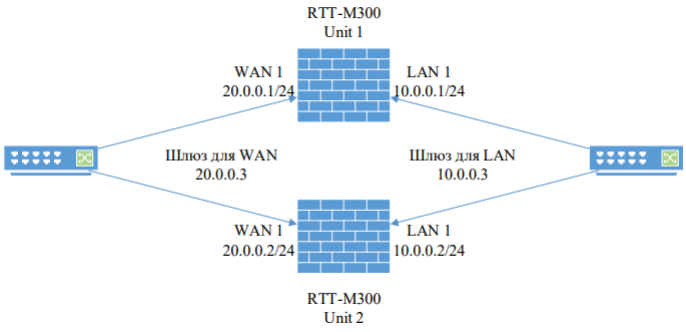


Рис. 55: Топология

В первую очередь необходимо настроить адресацию интерфейсов каждого юнита в соответствии со схемой. Шлюз для каждого сегмента настраивается через виртуальные интерфейсы. Конфигурация виртуальных интерфейсов ведущего юнита (Unit 1) представлена на рисунках.

Далее необходимо аналогично настроить ведомый юнит.

Описание параметров:

- Режим: CARP – режим резервирования шлюза на уровне IP-адреса;
- Интерфейс – интерфейс, который участвует в резервировании шлюза;
- Адрес – виртуальный адрес шлюза, который используется конечными хостами в соответствующем сегменте сети;
- Пароль виртуального IP-адреса – аутентификация юнитов в группе, использующих один общий виртуальный адрес;
- Группа VHID – группирование для изоляции разных виртуальных IP-шлюзов;
- Частота синхронизации – периодичность синхронизации юнитов в группе;

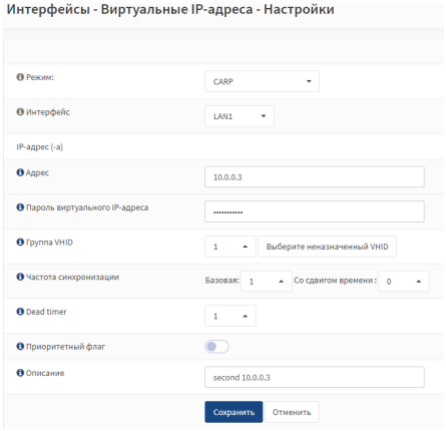


Рис. 56: Конфигурация первого виртуального интерфейса ведущего юнита (Unit 1)

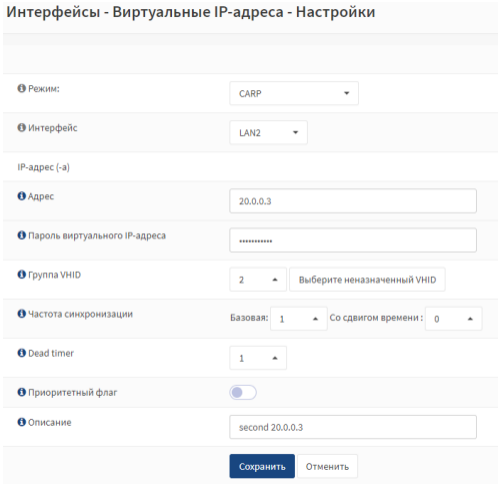


Рис. 57: Конфигурация второго виртуального интерфейса ведущего юнита (Unit 1)

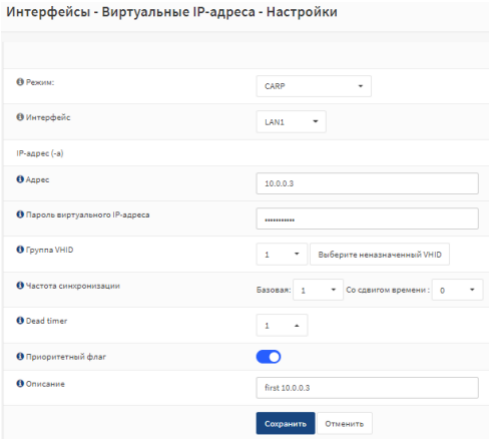


Рис. 58: Конфигурация первого виртуального интерфейса ведомого юнита (Unit 2)

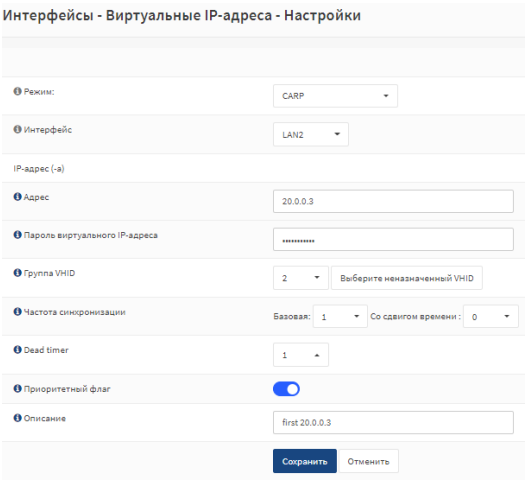


Рис. 59: Конфигурация второго виртуального интерфейса ведомого юнита (Unit 2)

- Сдвиг времени(приоритет) – чем больше значение, тем ниже вероятность, что юнит станет ведущим;
- Dead timer – таймер, который используется для определения доступности соседнего юнита;
- Приоритетный флаг – параметр, который позволяет зафиксировать роль ведущего юнита(параметр не фиксирует состояние юнита, как ведущий);
- Описание – общее описание.

После конфигурирования виртуальных интерфейсов каждого юнита, необходимо проверить статус виртуальных соединений

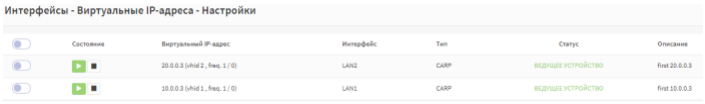


Рис. 60: Статус виртуальных соединений ведущего юнита

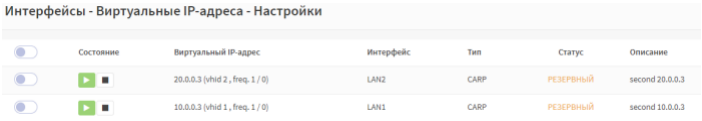


Рис. 61: Статус виртуальных соединений ведомого юнита

Произведем проверку доступности шлюза с хостов из сегмента LAN и WAN:

```
Pinging 10.0.0.3 with 18 bytes of data:

18 bytes from 10.0.0.3: icmp_seq=1. time=0 ms

18 bytes from 10.0.0.3: icmp_seq=2. time=0 ms

18 bytes from 10.0.0.3: icmp_seq=3. time=0 ms
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
18 bytes from 10.0.0.3: icmp_seq=4. time=0 ms

----10.0.0.3 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

console#ping 20.0.0.3

Pinging 20.0.0.3 with 18 bytes of data:

18 bytes from 20.0.0.3: icmp_seq=1. time=0 ms

18 bytes from 20.0.0.3: icmp_seq=2. time=0 ms

18 bytes from 20.0.0.3: icmp_seq=3. time=0 ms

18 bytes from 20.0.0.3: icmp_seq=4. time=0 ms

----20.0.0.3 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0
```

Далее для проверки отказоустойчивости выключим основной юнит, через который проходит трафик и проверим доступность шлюза.

```
console#ping 10.0.0.3

Pinging 10.0.0.3 with 18 bytes of data:

18 bytes from 10.0.0.3: icmp_seq=1. time=0 ms

18 bytes from 10.0.0.3: icmp_seq=2. time=0 ms

18 bytes from 10.0.0.3: icmp_seq=3. time=0 ms

18 bytes from 10.0.0.3: icmp_seq=4. time=0 ms

----10.0.0.3 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

console#ping 20.0.0.3

Pinging 20.0.0.3 with 18 bytes of data:
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
18 bytes from 20.0.0.3: icmp_seq=1. time=0 ms

18 bytes from 20.0.0.3: icmp_seq=2. time=0 ms

18 bytes from 20.0.0.3: icmp_seq=3. time=0 ms

18 bytes from 20.0.0.3: icmp_seq=4. time=0 ms

----20.0.0.3 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0
```

Резервирование шлюза на уровне IP-адреса корректно работает. При отключении основного юнита, который выполняет маршрутизацию трафика, второй юнит автоматически берет на себя роль основного и выполняет пересылку трафика.

Для каждого сегмента резервируется ближайший шлюз, т.е., например, если пускать трафик из сегмента LAN в WAN, при неисправности одного из линков интерфейса LAN 1, трафик стабильно пройдет используя альтернативный интерфейс (виртуальный адрес шлюза). Но если выйдет из строя удаленный интерфейс WAN 2, в данном случае резервирование линка для трафика из сегментов LAN в WAN не произойдет.

2.6.9.2 Подробное описание реализации CARP

После конфигурирования и запуска виртуального интерфейса, система подключается к IGMP группе и начинает отправлять анонсы протокола VRRP (CARP для взаимодействия с соседней стороной использует VRRP) на мультикастный адрес 224.0.0.18.

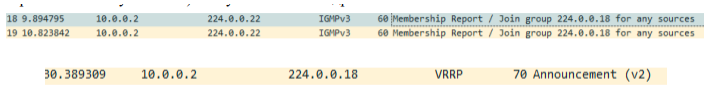


Рис. 62: Подключение к IGMP

Анонсы отправляет только ведущий юнит тем самым показывает, что доступен и необходимо использовать его физический интерфейс. Как только происходит авария на данном линке или юните, вещать начинает резервный юнит, тем самым становясь ведущим.

Факторы, влияющие на синхронизацию юнитов:

- Виртуальный IP-адрес – адрес должен быть одинаковым на каждом юните;
- Пароль виртуального IP-адреса – пароль должен быть одинаковым на каждом юните.

Состав пакета приведен на рисунке

Описание основных полей приведено в таблице

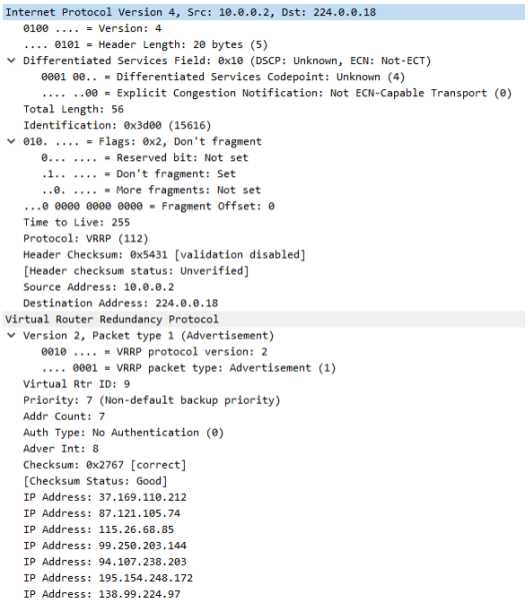


Рис. 63: Состав пакета

Таблица 22: Описание основных полей

Параметр	Примечание
Virtual Rtr ID	Группа VHID
Priority	Частота синхронизации со сдвигом во времени(приоритет)
Adver int	Частота синхронизации базовая

Список 1: Разбор конфигурации в /conf/config.xml

```
<virtualip>
  <vip>
    <type>single</type>
    <subnet_bits>32</subnet_bits>
    <mode>carp</mode>                    # Режим
    <interface>lan1</interface>          # Интерфейс
    <subnet>10.0.0.3</subnet>            # Виртуальный IP - адрес
    <vhid>1</vhid>                       # Группа VHID
    <advskew>40</advskew>                # Частота синхронизации со сдвигом времени, а␣
↪должен быть приоритет.
    <advbase>3</advbase>                 # Частота синхронизации
    <deadtime>1</deadtime>               # Dead timer
    <password>Rusteletech</password>     # Пароль виртуального IP-адреса
    <pflag>1</pflag>                     # Приоритетный флаг
  </vip>
</virtualip>
```

2.6.10 Доступ

2.6.10.1 Пользователи и Группы

REFOS позволяет создавать пользователей, группировать пользователей по группам и гибко настраивать привилегии.

Создание и редактирование Пользователей

Для создания учетной записи достаточно добавить пользователя в разделе **Система - Доступ** – **Пользователи** и указать **Имя пользователя**, **Пароль**. Все остальные параметры являются дополнительными. По умолчанию пользователю доступны все привилегии.

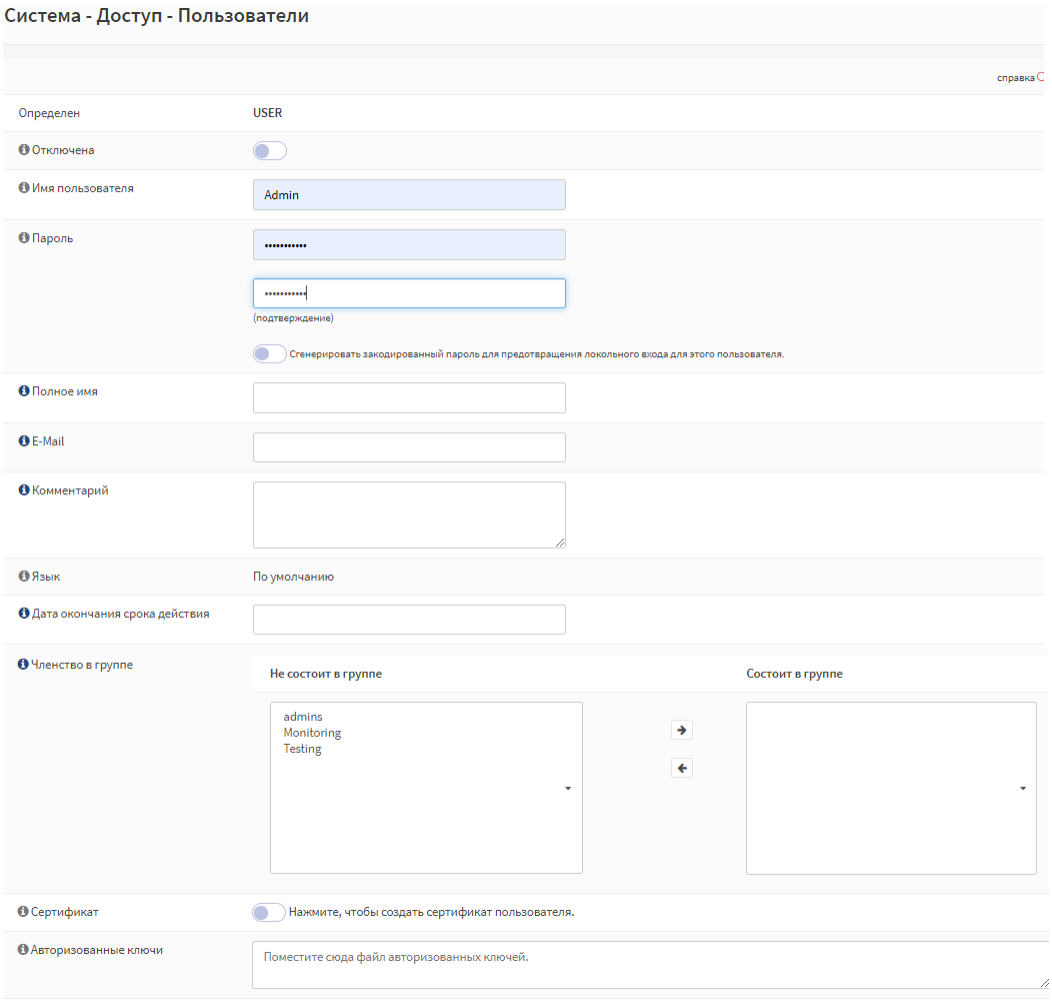


Рис. 64: Параметры учетной записи

Описание параметров учетной записи приведено в таблице.

Таблица 23: Описание параметров учетной записи

Параметр	Описание
Отключена	Параметр, который позволяет отключить пользователя без удаления из локальной базы
Имя пользователя	В имени пользователя допускается латиница любого регистра, цифры, подчёркивание и дефис. Длина строки имени пользователя до 32-х символов
Пароль	Минимальный размер пароля 8 символов
Полное имя	Дополнительный параметр для личного использования
E-Mail	Дополнительный параметр для личного использования
Комментарий	Дополнительный параметр для личного использования
Дата окончания срока действия	Параметр, который позволяет задать срок действия учетной записи
Членство в группе	Параметр, который позволяет определить учетную запись в выделенной группе
Действующие привилегии	Параметр, который позволяет задать определенные привилегии учетной записи. Ограничений по количеству привилегий нет
Сертификаты пользователя	Добавление и генерация пользовательского сертификата VPN
Ключи API	Добавление и генерация API-ключа
Авторизованные ключи	Для доступа к консоли через SSH достаточно указать закрытый SSH-ключ

Распределение пользователей по группам

Привилегии возможно назначить не только пользователям, но и группам, поэтому группирование пользователей позволяет упростить распределение привилегий большому количеству пользователей. Редактирование и создание групп производится в разделе **Система – Доступ – Группы**.

Описание параметров групп приведено в таблице.

Таблица 24: Описание параметров групп

Параметр	Описание
Имя группы	В имени группы допускается латиница любого регистра, цифры, подчёркивание и дефис. Длина строки имени пользователя до 32-х символов
Описание	Дополнительный параметр для личного использования
Членство в группе	Для того, чтобы перенести пользователя в группу, его достаточно выделить и перенести в поле **Состоит в группе**
Присвоенные привилегии	Параметр, который позволяет задать определенные привилегии группе. Ограничений по количеству привилегий нет

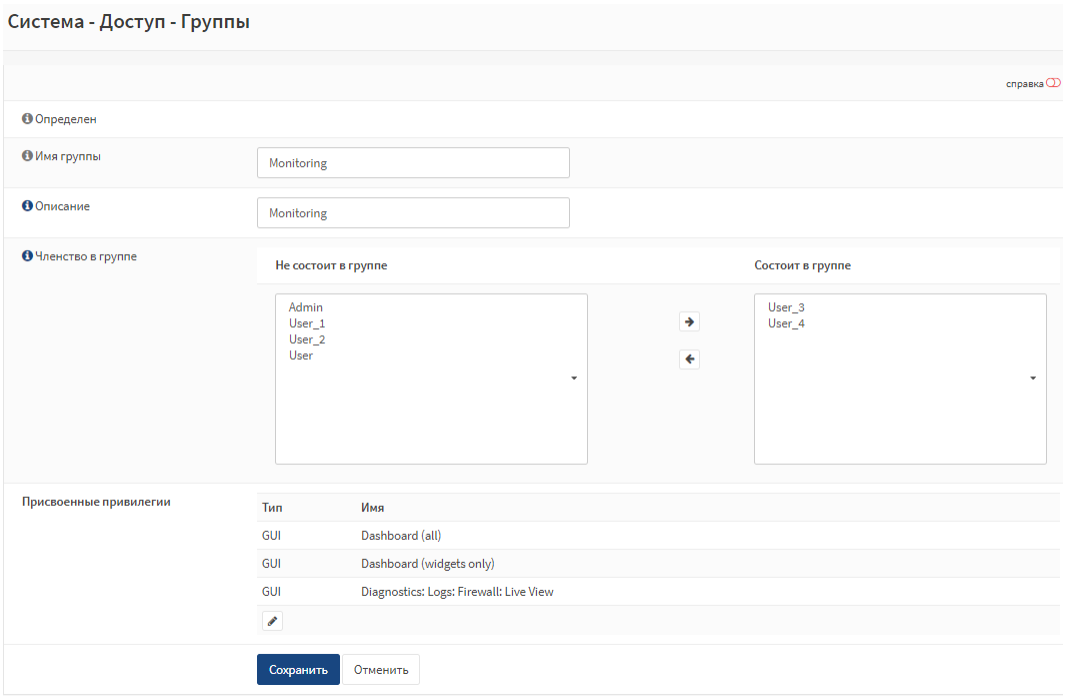


Рис. 65: Параметры групп

Привилегии

Привилегии позволяют гибко настроить доступ с возможностью просмотра и редактирования к разным разделам системы.

Описание привилегий приведено в таблице.

Таблица 25: Описание привилегий

Привилегия	Описание
Все страницы	Доступ и редактирование всех параметров системы
Инструментальная панель	Доступ ко всем параметрам Инструментальной панели
Система - Доступ - Средство проверки	Доступ к параметрам раздела Система - Доступ - Средство проверки
Система - Конфигурация - Резервные копии	Доступ к параметрам раздела Система - Конфигурация - Резервные копии
Система - Конфигурация - История изменений	Доступ и редактирование параметров раздела Система - Конфигурация - История изменений
Питание - Выключение	Доступ к параметрам раздела Питание – Выключение
Межсетевой экран - Файлы журнала - Прямая трансляция	Доступ к параметрам раздела Межсетевой экран - Файлы журнала - Прямая трансляция
Межсетевой экран - Файлы журнала - Обзор	Доступ к параметрам раздела Межсетевой экран - Файлы журнала – Обзор
Система - Настройки - Журналирование	Доступ и редактирование параметров раздела Система - Настройки – Журналирование
Питание - Перезагрузка	Доступ к параметрам раздела Питание – Перезагрузка
Межсетевой экран – Псевдонимы - Редактирование	Доступ и редактирование параметров раздела Межсетевой экран – Псевдонимы

продолжается на следующей странице

Таблица 25 – продолжение с предыдущей страницы

Привилегия	Описание
Межсетевой экран – Псевдонимы - Просмотр	Доступ к параметрам раздела Межсетевой экран – Псевдонимы
Межсетевой экран - NAT – BINAT- Просмотр	Доступ к параметрам раздела Межсетевой экран - NAT – BINAT
Межсетевой экран - NAT - BINAT - Редактирование	Доступ и редактирование параметров раздела Межсетевой экран - NAT – BINAT
Межсетевой экран - Настройки - Общие настройки	Доступ и редактирование параметров раздела Межсетевой экран - Настройки - Общие настройки
Межсетевой экран - NAT - DNAT (Prerouting) - Просмотр	Доступ к параметрам раздела Межсетевой экран - NAT - DNAT (Prerouting)
Межсетевой экран - NAT - DNAT (Prerouting) - Редактирование	Доступ и редактирование параметров раздела Межсетевой экран - NAT - DNAT (Prerouting)
Межсетевой экран - Правила фильтрации - Просмотр	Доступ к параметрам раздела Межсетевой экран - Правила фильтрации
Межсетевой экран - Правила фильтрации - Редактирование	Доступ и редактирование параметров раздела Межсетевой экран - Правила фильтрации
Межсетевой экран - Настройки - Расписания - Просмотр	Доступ к параметрам раздела Межсетевой экран - Настройки – Расписания
Межсетевой экран - Настройки - Расписания - Редактирование	Доступ и редактирование параметров раздела Межсетевой экран - Настройки – Расписания
Межсетевой экран - NAT - SNAT - Просмотр	Доступ к параметрам раздела Межсетевой экран - NAT – SNAT
Межсетевой экран - NAT - SNAT - Редактирование	Доступ и редактирование параметров раздела Межсетевой экран - NAT – SNAT
Интерфейсы - Виртуальные IP-адреса - Редактирование	Доступ и редактирование параметров раздела Интерфейсы - Виртуальные IP-адреса
Интерфейсы - Виртуальные IP-адреса - Просмотр	Доступ к параметрам раздела Интерфейсы - Виртуальные IP-адреса
Интерфейсы - Назначения портов	Доступ и редактирование параметров раздела Интерфейсы - Назначения портов
Межсетевой экран - Группы - Просмотр	Доступ к параметрам раздела Межсетевой экран - Группы
Межсетевой экран - Группы - Редактирование	Доступ и редактирование параметров раздела
Службы – Потоковый антивирус - Конфигурация	Доступ и редактирование параметров раздела Службы -Потоковый антивирус – Конфигурация
Службы - Сетевое время - Общие настройки	Доступ и редактирование параметров раздела Службы - Сетевое время - Общие настройки
Службы - Веб-прокси	Доступ и редактирование параметров раздела Службы - Веб-прокси
Интерфейсы - Обзор	Доступ к параметрам раздела Интерфейсы – Обзор
Службы - Сетевое время - Статус	Доступ к параметрам раздела Службы - Сетевое время – Статус
VPN - OpenVPN - Статус соединения	Доступ к параметрам раздела VPN - OpenVPN - Статус соединения
Службы - Сетевое время - Журнал	Доступ к параметрам раздела Службы - Сетевое время – Журнал
VPN - OpenVPN - Журнал	Доступ к параметрам раздела VPN - OpenVPN – Журнал

продолжается на следующей странице

Таблица 25 – продолжение с предыдущей страницы

Привилегия	Описание
Система - Настройки - Администрирование	Доступ и редактирование параметров раздела Система - Настройки – Администрирование
Система - Доступ - Серверы	Доступ и редактирование параметров раздела Система - Доступ – Серверы
Система - Доверенные сертификаты - Полномочия	Доступ и редактирование параметров раздела Система - Доверенные сертификаты – Полномочия
Система - Доверенные сертификаты - Сертификаты	Доступ и редактирование параметров раздела Система - Доверенные сертификаты – Сертификаты
Система - Доверенные сертификаты - Отзыв сертификатов	Доступ к параметрам раздела Система - Доверенные сертификаты - Отзыв сертификатов
Система - Программное обеспечение	Доступ к параметрам раздела Система - Программное обеспечение
Система - Шлюзы - Группа - Просмотр	Доступ к параметрам раздела Система - Шлюзы – Группа
Система - Шлюзы - Просмотр	Доступ к параметрам раздела Система – Шлюзы
Система - Шлюзы - Редактирование	Доступ и редактирование параметров раздела Система – Шлюзы
Система - Шлюзы - Группа - Редактирование	Доступ и редактирование параметров раздела Система - Шлюзы – Группа
Система - Настройки - Общие настройки	Доступ и редактирование параметров раздела Система - Настройки - Общие настройки
Система - Доступ - Группы	Доступ и редактирование параметров раздела Система - Доступ – Группы
Система - Доступ - Пользователи	Доступ и редактирование параметров раздела Система - Доступ – Пользователи
Сводка - Пароль	Доступ и редактирование параметров раздела Сводка – Пароль
VPN - OpenVPN - Экспорт настроек клиента	Доступ и редактирование параметров раздела VPN - OpenVPN - Экспорт настроек клиента
VPN - OpenVPN - Серверы/клиенты	Доступ и редактирование параметров раздела VPN - OpenVPN - Серверы/клиенты
Службы – Мониторинг служб	Доступ и редактирование параметров раздела Службы – Мониторинг служб

Серверы аутентификации и авторизации

Аутентификация и авторизация пользователей стандартно производится по логину и паролю, используя локальную базу пользователей или внешние сервисы RADIUS/LDAP.

RADIUS

Добавление сервиса аутентификации и авторизации через внешний RADIUS-сервер происходит в разделе **Система – Доступ – Серверы**. Для взаимодействия REFOS с внешний RADIUS-сервером достаточно указать IP-адрес RADIUS-сервера и общий секретный ключ, все остальные параметры могут использоваться по умолчанию.

Описание параметров сервиса аутентификации и авторизации RADIUS приведено в таблице.

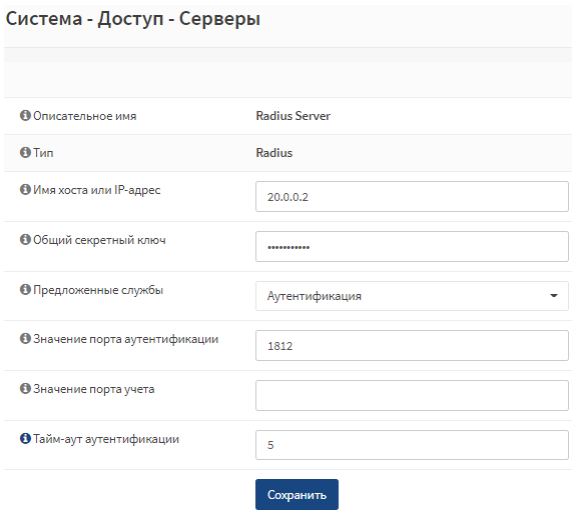


Рис. 66: Конфигурация сервиса аутентификации и авторизации RADIUS

Таблица 26: Описание параметров сервиса аутентификации и авторизации RADIUS

Параметр	Описание
Описательное имя	Уникальное имя сервиса. Допускается латиница любого регистра, цифры, подчёркивание и дефис. Длина строки имени пользователя до 32-х символов
Тип	Тип внешнего сервиса аутентификации и авторизации – **RADIUS** или **LDAP**
Имя хоста или IP-адрес	IP-адрес внешнего RADIUS-сервера
Общий секретный ключ	Общий секретный ключ, который должен использоваться и внешним RADIUS-сервером, и REFOS. Первоначально общий секретный ключ конфигурируется на внешнем RADIUS-сервере
Предложенные службы	Выбор службы Аутентификация или Аутентификация и учет
Значение порта аутентификации	Значение порта аутентификации по умолчанию – 1812. Конфигурация порта аутентификации внешнего RADIUS-сервере должна совпадать с данным параметром
Значение порта учета	Значение порта учета по умолчанию – 1812. Конфигурация порта учета внешнего RADIUS-сервере должна совпадать с данным параметром
Тайм-аут аутентификации	Значение определяет ответ в секундах на запрос аутентификации RADIUS-сервера. По умолчанию значение равно 5 секундам.

Пример конфигурации нескольких пользователей с последующим распределением по группам, предоставлением уникальных привилегий, аутентификацией и авторизацией с внешним RADIUS-сервером

В рамках данного теста производится проверка аутентификации и авторизации пользователей, используя локальную базу пользователей и протокол RADIUS. Для проверки будет использоваться две группы пользователей с разными привилегиями, приведенными в таблице.

Таблица 27: Группы пользователей с разными привилегиями

Имя пользователя	Имя группы	Привилегии	Метод авторизации
User_1	Testing	Межсетевой экран - NAT - BINAT : Просмотр Межсетевой экран - NAT - BINAT : Редактирование Межсетевой экран - Настройки - Общие настройки Межсетевой экран - NAT - DNAT (Prerouting) : Просмотр Межсетевой экран - NAT - DNAT (Prerouting) : Редактирование Межсетевой экран - Правила фильтрации : Просмотр Межсетевой экран - Правила фильтрации : Редактирование Межсетевой экран - NAT - SNAT : Просмотр Межсетевой экран - NAT - SNAT : Редактирование	Локальная база
User_2			
User_3	Monitoring	Инструментальная панель Инструментальная панель(Только виджеты) Межсетевой экран - Файлы журнала - Прямая трансляция	Локальная база и RADIUS - сервер
User_4			

В группу Testing будут входить два пользователя User_1 и User_2. Которым будут доступны функции фильтрации, трансляции (DNAT, SNAT, BINAT). Данные пользователи могут создавать, редактировать и просматривать правила фильтрации и трансляции. Аутентификация и авторизация будет происходить через локальную базу пользователей в системе.

В группу Monitoring будут входить два пользователя User_3 и User_4. Которым будут доступны функции просмотра состояния системы – Инструментальная панель и Журнал логов. Аутентификация и авторизация будет происходить через локальную базу пользователей в системе, а также система будет отправлять запрос аутентификации на RADIUS-сервер, тем самым проверяя пользователя по базе пользователей RADIUS-сервера.

Схема подключения изображена на рисунке.

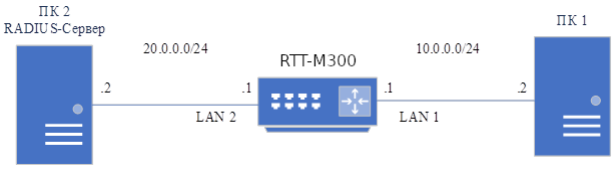


Рис. 67: Схема подключения

Следуя схеме теста, ПК 1 подключается к REFOS и проходит аутентификацию и авторизацию, используя учетные данные пользователей User_1, User_2, User_3, User_4. Процесс аутентификации

использует локальную базу пользователей REFOS, а также дополнительную проверку на RADIUS-сервере для пользователей User_3, User_4. Процесс авторизации использует только локальную базу пользователей REFOS.

В первую очередь, создадим учетные записи User_1, User_2, User_3, User_4 в локальной базе пользователей REFOS.

Вкладка **Система - Доступ – Пользователи**.

Для создания учетной записи достаточно указать **Имя пользователя** и **Пароль**, все остальные параметры являются дополнительными.

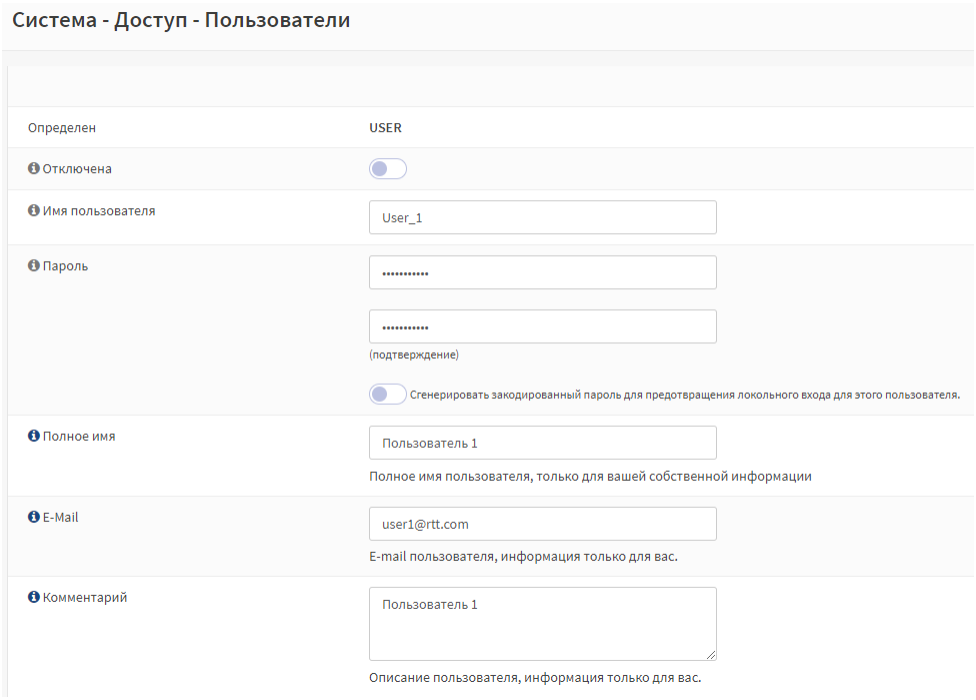


Рис. 68: Создание учетной записи пользователя User_1

Аналогично созданию учетной записи пользователя User_1 создадим других пользователей: User_2, User_3, User_4.

Создадим две группы Testing и Monitoring. Каждой группе предоставим определенные условиями теста привилегии, а также распределим пользователей.

Далее сконфигурируем параметры соединения с RADIUS-сервером. Для этого,, укажем IP-адрес RADIUS-сервера и общий секретный ключ, остальные параметры являются второстепенными и используются по умолчанию.

Для удачной аутентификации пользователей User_3, User_4, данные учетные записи должны быть продублированы на удаленном RADIUS-сервере.

Средством проверки произведем проверку аутентификации пользователя удаленным RADIUS-сервером через вкладку **Система - Доступ - Средство проверки**.

Неудачная проверка аутентификации пользователя показана на рисунке.

Подсказка

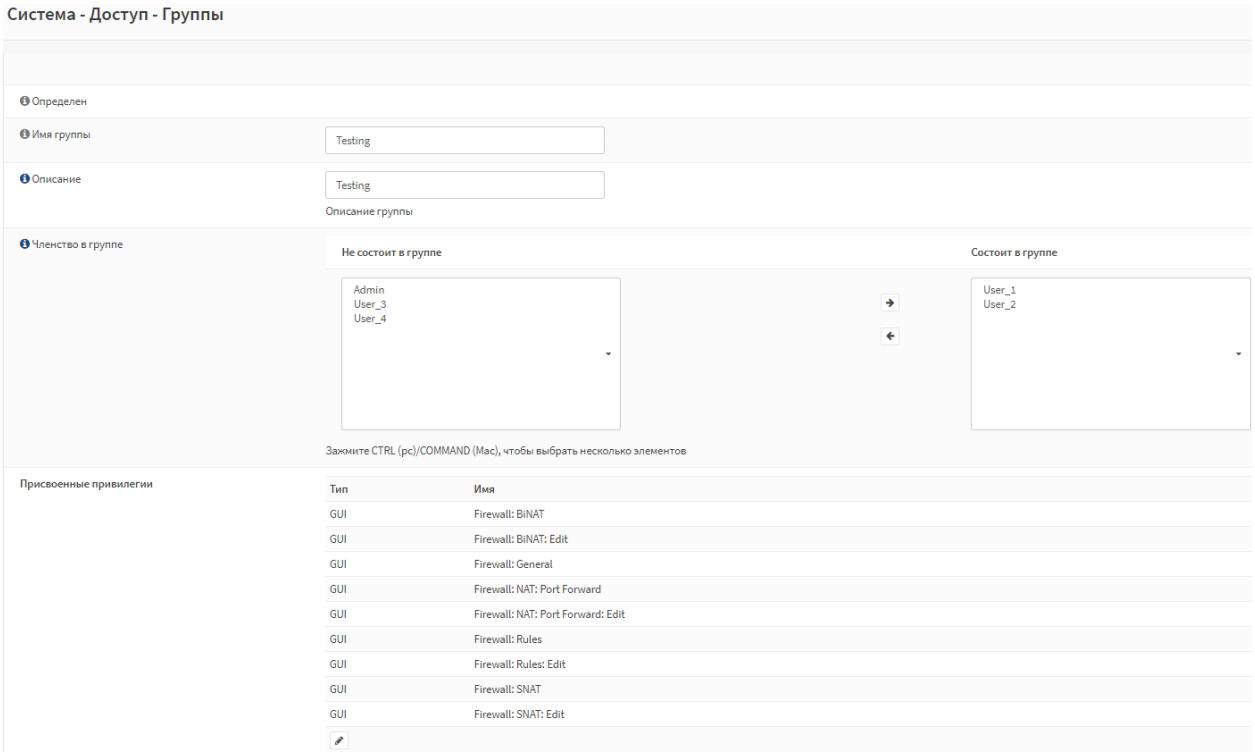


Рис. 69: Создание группы Testing

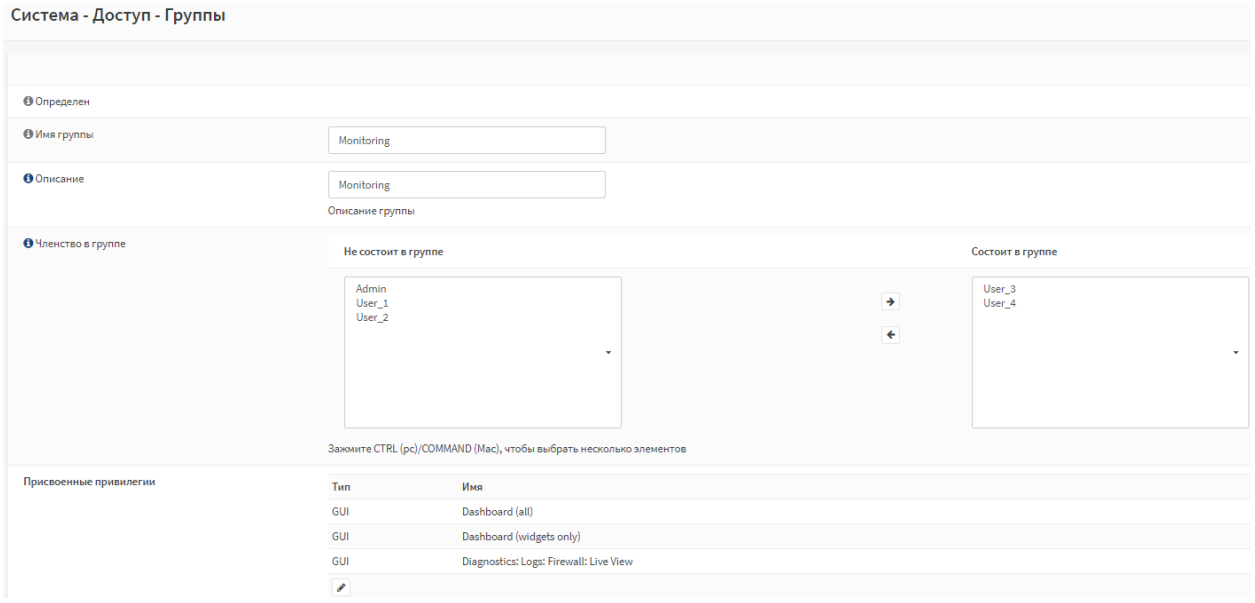


Рис. 70: Создание группы Monitoring

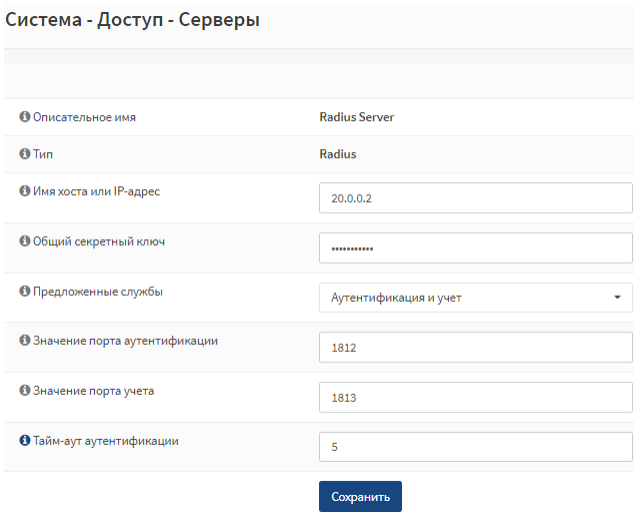


Рис. 71: Параметры соединения с RADIUS-сервером

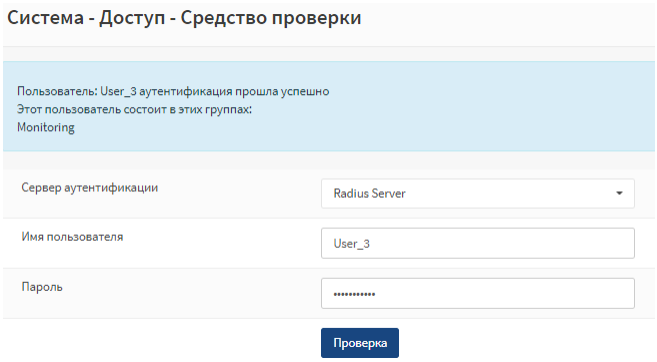


Рис. 72: Удачная проверка аутентификации пользователя User_3

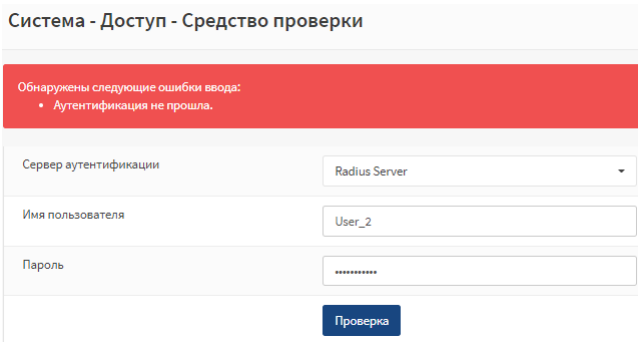


Рис. 73: Неудачная проверка аутентификации пользователя User_2

Неудачная проверка аутентификации пользователя User_2, т.к. данный пользователь отсутствует в базе пользователей удаленного RADIUS-сервера

Произведем итоговую проверку аутентификации и авторизации пользователей User_1, User_2, User_3, User_4. Результаты итоговой проверки аутентификации и авторизации приведены на рисунках.

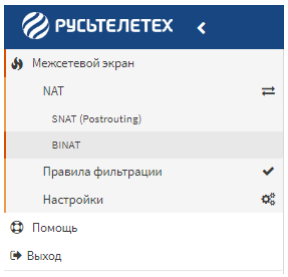


Рис. 74: Результат авторизации пользователей User_1 и User_2

Подсказка

В соответствии с предоставленными привилегиями, пользователям доступны только основные функции фильтрации и трансляции

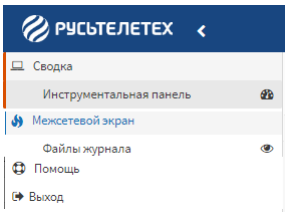


Рис. 75: Результат авторизации пользователей User_3 и User_4

Подсказка

В соответствии с предоставленными привилегиями, пользователям доступны только основные функции просмотра состояния системы и системных сообщений

2.6.11 DHCP

2.6.11.1 Введение

Для каждого устройства, подключенного к сети, требуется уникальный IP-адрес. Внедрение сервера с протоколом динамической конфигурации узла (DHCP) в локальную сеть упрощает процесс присвоения IP-адресов сетевым устройствам. Использование централизованного сервера DHCP позволяет организации управлять присвоением всех динамических IP-адресов с одного сервера. Подобная практика делает управление IP-адресацией более эффективной и обеспечивает последовательность процессов и согласованность данных по всей организации, включая филиалы.

Операционная система REFOS имеет полноценную поддержку DHCPv4-протокола.

2.6.11.2 Первоначальная конфигурация DHCPv4-сервера

Первоначальная конфигурация DHCPv4-сервера включает в себя создание диапазона IP-адресов, которые распределяются по запросу клиентов. Каждый диапазон привязан к IP-адресации интерфейса. Поэтому необходимо указывать корректный диапазон в соответствии с IP-адресацией интерфейса.

Важно

В стартовой конфигурации операционной системы REFOS служба DHCPv4-сервера запущена на интерфейсах GE3-GE6

Для создания диапазона DHCPv4 необходимо в разделе **Службы - DHCPv4** перейти на вкладку интерфейса, который используется шлюзом для локальной сети, где планируется распределение IP-адресов клиентам. На вкладке интерфейса необходимо задать параметры пула IP-адресов и DHCP-опции, соответствующие таблице.

Таблица 28: Набор правил фильтрации по доступу к системе

Параметр	Описание
Включить	Запустить сервис DHCP на интерфейсе
Блокировать неизвестные клиенты	Блокировать клиентов не указанных в Статическая таблица клиентов DHCP
Подсеть	Фиксированные параметры, указанного интерфейса
Маска подсети	Фиксированные параметры, указанного интерфейса
Доступный диапазон	Фиксированные параметры, указанного интерфейса
Диапазон	Задать диапазон IP-адресов, который будет использоваться для распределения DHCP-клиентам
Дополнительные пулы	Создание дополнительных диапазонов
WINS-серверы	DHCP-опция 44. IP-адрес WINS - серверов, выдаваемых клиентам DHCP
DNS-серверы	DHCP-опция 6. IP-адрес DNS - серверов, выдаваемых клиентам DHCP
Шлюз	DHCP-опция 3. IP-адрес шлюза, выдаваемый клиентам DHCP
Имя домена	DHCP-опция 15. Название домена, выдаваемое клиентам DHCP
Список поиска доменов	DHCP-опция 119. Список поиска DNS
Время аренды по умолчанию (секунд)	DHCP-опция Задать время в секундах, которое будет предоставлено клиентам, которые не запрашивают конкретное время аренды. Значение по умолчанию – 7200 секунд
Максимальное время аренды (с)	Задать максимальное значение времени, которое будет назначено для аренды в секундах. Значение по умолчанию – 86400 секунд.
Задержка ответа (с)	Задать количество секунд, прошедших с момента попытки получить или продлить аренду клиентом. Параметр особенно актуален, когда используется несколько DHCP-серверов
MTU интерфейса	DHCP-опция 26. Значение MTU для данного интерфейса
Контроль доступа по MAC-адресам	
NTP-серверы	DHCP-опция 42. IP-адрес NTP - серверов, выдаваемых клиентам DHCP

2.6.11.3 Пример стандартной конфигурации DHCPv4-сервера

В разделе **Службы - DHCPv4** на вкладке соответствующего интерфейса произвести следующие настройки:

- Параметром **Включить** запусти сервис DHCP на интерфейсе;
- Задать корректный диапазон IP-адресов в соответствии с IP-адресацией интерфейса в поле параметра **Диапазон**;
- Задать IP-адрес DNS – серверов в поле параметра **DNS-серверы**;
- Задать IP-адрес шлюза в поле параметра **Шлюз**;
- Задать имя домена в поле параметра **Имя домена**;
- Задать IP-адрес NTP – серверов в поле параметра NTP-серверы.

Пример стандартной конфигурации DHCPv4-сервера представлен на рисунке.

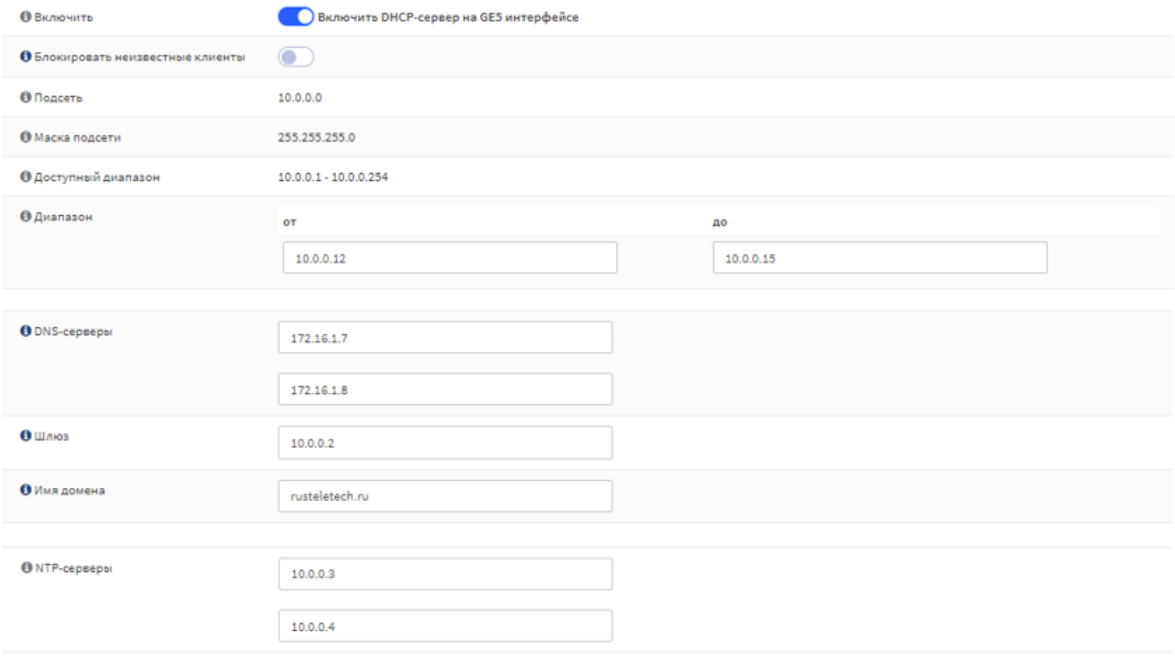


Рис. 76: Пример стандартной конфигурации DHCPv4-сервера

На вкладке **Аренда адресов** возможно проверить статус выданных IP-адресов из заданного пула.

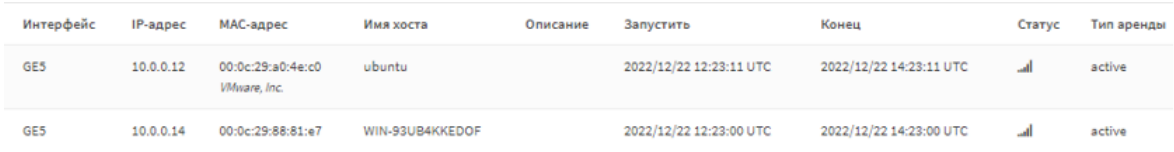


Рис. 77: Аренда адресов

Описание параметров интерфейса вкладки **Аренда адресов** приведено в таблице.

Таблица 29: Описание параметров интерфейса вкладки **Аренда адресов**

Параметр	Описание
Интерфейс	
IP-адрес	Зарезервированный IP-адрес DHCP-клиентом
MAC-адрес	MAC-адрес DHCP-клиента
Имя хоста	Системное имя DHCP-клиента
Описание	Описание для справки
Запустить	Начальное время аренды IP-адреса
Конец	Конечное время аренды IP-адреса
Статус	Состояние взаимодействия с DHCP-клиентом
Тип аренды	Состояние аренды: • Active – IP-адрес зарезервирован; • Expired – Время аренды истекло.

2.6.11.4 DHCP опция 82

DHCP опция 82 (DHCP option 82) – опция протокола DHCP, которая позволяет проинформировать DHCP-сервер о том, от какого DHCP-ретранслятора и через какой порт был получен DHCP-запрос. Опция используется для привязки IP-адреса к порту коммутатора, а также для защиты от атак с использованием протокола DHCP (DHCP snooping).

Протокол DHCP является удобным решением для настройки стека TCP/IP. Используя сконфигурированные пулы IP-адресов, DHCP-сервер выдает по запросу доступный IP-адрес клиенту в рамках одного локального широковещательного домена. DHCP опция 82 позволяет предоставлять IP-адрес клиенту, который находится в другой локальной сети другого широковещательного домена. При этом возможно предоставлять определенный IP-адрес клиенту, в зависимости от порта, на который пришел запрос и/или MAC-адреса DHCP-ретранслятора.

DHCP-ретранслятор (relay agent) — сетевое устройство, посредник между клиентом и сервером. Используется в тех случаях, когда у клиента нет возможности обратиться к серверу напрямую, в частности, в том случае, если они находятся в разных широковещательных доменах. DHCP-ретранслятор обрабатывает стандартный широковещательный DHCP-запрос и перенаправляет его на DHCP-сервер в виде целенаправленного (unicast) пакета, а полученный от DHCP-сервера ответ, в свою очередь, перенаправляет DHCP-клиенту.

DHCP опция 82 состоит из двух параметров:

- **Agent Circuit ID** — содержит информацию о том, с какого порта пришел запрос на DHCP-ретранслятор;
- **Agent Remote ID** — идентификатор самого DHCP-ретранслятора, который задается при настройке сетевого устройства.

При получении DHCP-запроса DHCP-ретранслятор (с предварительно настроенными параметрами Circuit ID и Remote ID) перенаправляет запрос с уникальными параметрами Circuit ID и Remote ID DHCP-серверу. DHCP сервер (с предварительно настроенным IP-адресом и соответствующим ему параметрами Circuit ID и Remote ID) анализирует параметры Circuit ID и Remote ID в теле пакета и предоставляет соответствующий IP-адрес.

Важно

Операционная система REFOS в текущей версии не имеет поддержки функции DHCP-ретранслятора (DHCP relay)

2.6.11.5 Пример конфигурации DHCP-сервера с опцией 82

В рамках данного примера DHCP-клиент формирует DHCP-запрос на получение параметров TCP/IP.

DHCP-ретранслятор, с предварительно настроенными параметрами:

- Circuit ID – порт коммутатора - **LAN 1**, на который пришел запрос от DHCP-клиента;
- Remote ID – MAC-адрес DHCP-ретранслятора – C4:36:DA:00:00:01.

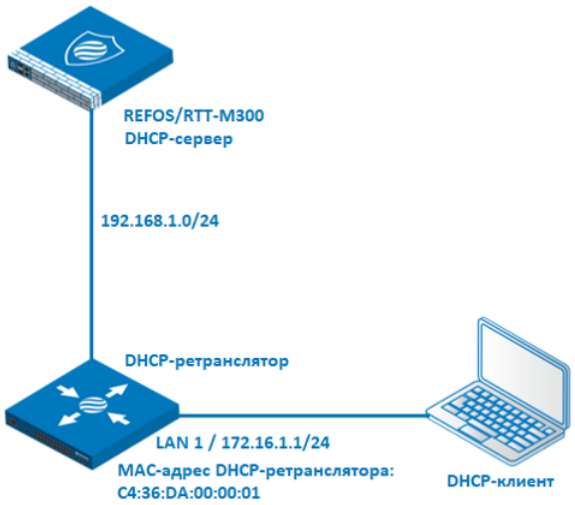


Рис. 78: Схема реализации DHCP-сервера с опцией 82

DHCP-ретранслятор, получив DHCP-запрос на порт LAN 1, добавляет параметры Circuit ID и Remote ID в тело пакета и перенаправляет запрос REFOS/RTT-M300/DHCP-серверу.

REFOS/RTT-M300/DHCP-сервер получив запрос, производит обработку параметров Circuit ID и Remote ID в соответствии с конфигурацией DHCP-сервера. И предоставляет заданный конфигурацией IP-адрес - **172.16.1.5**.

2.6.11.6 Пример конфигурации REFOS/DHCP-сервера с опцией 82

Конфигурация DHCP-сервера с опцией 82 производится в разделе **Службы - DHCPv4**.

В разделе необходимо выбрать интерфейс, который будет принимать запросы и произвести следующие настройки:

- Параметром **Включить** запусти сервис DHCP на интерфейсе;
- Задать корректный диапазон IP-адресов в соответствии с IP-адресацией интерфейса в поле параметра **Диапазон**;
- В разделе **DHCP option 82 mapping** добавить конфигурацию параметров опции 82:
  - Задать значение параметра **Порт - Circuit ID**;

– Задать IP-адрес, который будет предоставляться DHCP-клиенту на DHCP-запрос с соответствующими значениями параметров Circuit ID и Remote ID;

– Задать значение параметра **MAC-адрес ретранслятора - Remote ID**;

– Задать общее описание конфигурации.

Конфигурация DHCP-сервера с опцией 82 представлена на рисунке

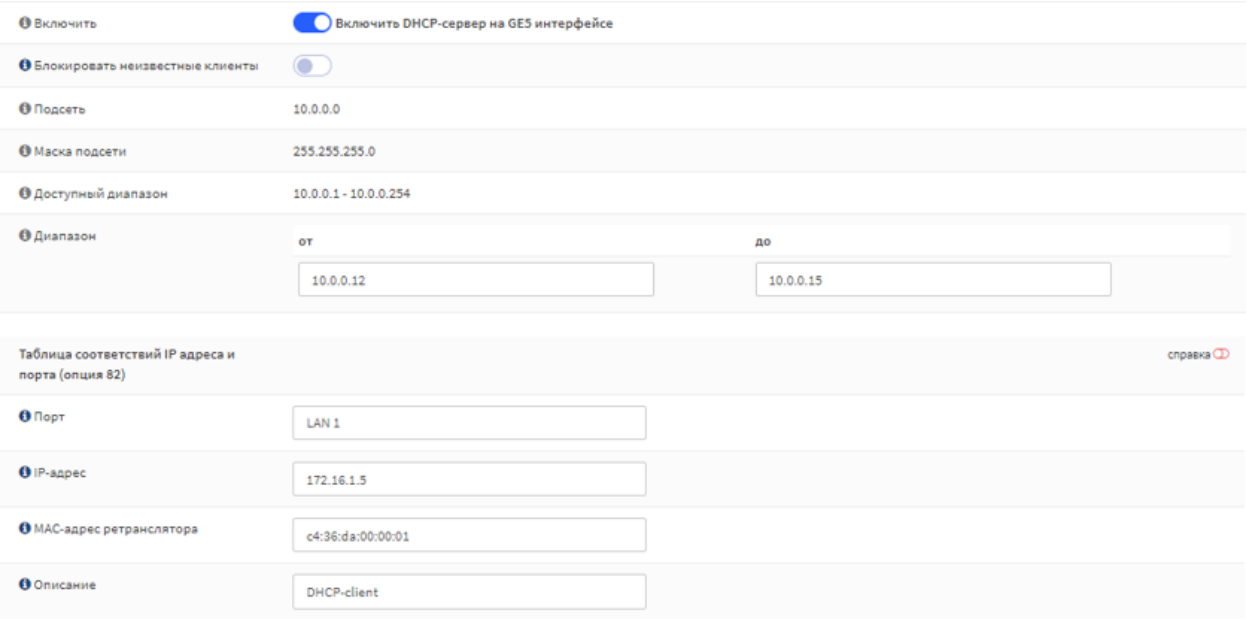


Рис. 79: Конфигурация DHCP-сервера с опцией 82

2.6.12 Система обнаружения вторжений (СОВ)

2.6.12.1 Введение

Система обнаружения вторжений (СОВ) позволяет детектировать сетевые атаки и предотвращать угрозы, включая защиту сетевых устройств.

СОВ производит анализ трафика, используя набор правил (базу данных уязвимостей), который содержит более 100 000 сигнатур - шаблонов вредоносного трафика. Система также позволяет настраивать уникальные пользовательские правила, которые могут производить анализ пакетов на уровнях L3 – L7.

К системе обнаружения вторжений можно отнести два режима работы:

- IDS – система анализирует трафик, сравнивая с базой данных уязвимостей, и сигнализирует о наличие вредоносного трафика;
- IPS – система не только анализирует и сигнализирует, но и предотвращает прохождение вредоносного трафика.

Важно

Система обнаружения вторжений является отдельным модулем операционной системы REFOS и распространяется только по лицензии

2.6.12.2 Общие сведения режимов работы IDS/IPS

IDS (Intrusion Detection System), или система обнаружения вторжений – основной задачей которой является обнаружение и регистрация атак, а также оповещение при срабатывании определённого правила. В отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS анализирует данные до уровня приложения (до седьмого уровня OSI).

IDS позволяет:

- Выявлять различные виды сетевых атак;
- Обнаруживать попытки неавторизованного доступа или повышения привилегий;
- Обнаруживать появление вредоносного ПО;
- Отслеживать открытие нового порта и т.д.

IPS (Intrusion Prevention System), или система предотвращения вторжения – в данном случае система не только производит обнаружение и регистрацию атак, а также предпринимает самостоятельные действия – **Разрешить** или **Запретить** прохождение трафика, параметры которого соответствуют сигнатурам базы данных правил.

2.6.12.3 Механизм обработки трафика системой обнаружения вторжения

Принцип работы системы обнаружения вторжения заключается в следующем – трафик после получения интерфейсом системы, анализируется установленными пользователем правилами. Анализ трафика может производиться на уровнях L3 - L7.

Если параметры трафика совпадают с сигнатурами правил, система предпринимает следующие действия:

- Сигнализирует и журналирует обнаруженные угрозы;
- Разрешает или запрещает прохождение трафика в зависимости от конфигурации системы.

После обработки трафика, если прохождение разрешено, производится обработка правилами фильтрации межсетевого экрана. Если прохождение запрещено, трафик блокируется системой.

Механизм обработки трафика системой обнаружения вторжения представлен на рисунке

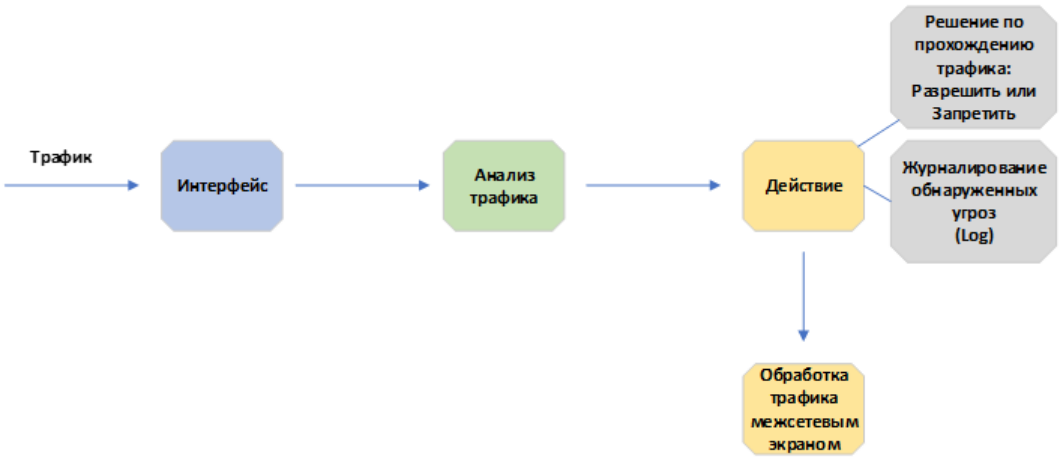


Рис. 80: Механизм обработки трафика системой обнаружения вторжения

2.6.12.4 Наборы правил IDS/IPS

Система обнаружения вторжений в базовой версии имеет следующий набор правил:

- **RTT (abuse.ch)/Feodo Tracker** - набор правил содержит список управляющих серверов для троянской программы Feodo. Feodo (также известный как Cridex или Bugat) используется злоумышленниками для кражи чувствительной информации в сфере электронного банкинга (данные по кредитным картам, логины/пароли) с компьютеров пользователей. В настоящее время существует четыре версии троянской программы (версии A, B, C и D), главным образом отличающиеся инфраструктурой управляющих серверов;
- **RTT (abuse.ch)/SSL Fingerprint Blacklist, SSL IP Blacklist, SSL IP Blacklist Aggressive** - набор правил содержит списки вредоносных SSL сертификатов, т.е. сертификатов, в отношении которых установлен факт их использования вредоносным ПО и ботнетами. В списках содержатся SHA1 отпечатки публичных ключей из SSL сертификатов;
- **RTT ET open/botcc, RTT ET open/botcc.portgrouped** - набор правил содержит список известных ботнетов и управляющих серверов. Источники: Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker;
- **RTT ET open/ciarmy** - набор правил содержит список вредоносных хостов по классификации проекта www.cinsarmy.com;
- **RTT ET open/compromised** – набор правил содержит список известных скомпрометированных и вредоносных хостов. Источники: Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects;
- **RTT ET open/drop** - набор правил содержит список спамерских хостов / сети по классификации проекта www.spamhaus.org;
- **RTT ET open/dshield** - набор правил содержит список вредоносных хостов по классификации проекта www.dshield.org;
- **RTT ET open/emerging-activex** – набор правил содержит список сигнатур использования ActiveX-контента;
- **RTT ET open/emerging-adware_pup** - набор правил содержит список сигнатур вирусов семейства PUP;
- **RTT ET open/emerging-attack_response** - набор правил, детектирующие поведение хоста после успешно проведенных атак;
- **RTT ET open/emerging-chat** - набор правил описывают признаки обращения к популярным чатам;
- **RTT ET open/emerging-coinminer** - набор правил содержит список сигнатур вирусов семейства COINMINER;
- **RTT ET open/emerging-current_events** - набор временных правил, ожидающие возможного включения в постоянные списки правил;
- **RTT ET open/emerging-dns** - набор правил содержит сигнатуры уязвимостей в протоколе DNS, признаки использования DNS вредоносным ПО, некорректного использования протокола DNS;
- **RTT ET open/emerging-dos** - набор правил содержит сигнатуры DOS-атак;
- **RTT ET open/emerging-exploit** - набор правил содержит сигнатуры эксплойтов;
- **RTT ET open/emerging-ftp** - набор правил содержит сигнатуры уязвимостей в протоколе FTP, признаки некорректного использования протокола FTP;

- **RTT ET open/emerging-games** - набор правил описывает признаки обращения к популярным игровым сайтам: World of Warcraft, Starcraft и т.п;
- **RTT ET open/emerging-icmp** - набор правил содержит сигнатуры некорректного использования протокола ICMP;
- **RTT ET open/emerging-icmp_info** - набор правил содержит сигнатуры информационных ICMP-сообщений;
- **RTT ET open/emerging-imap** - набор правил содержит сигнатуры уязвимостей в протоколе IMAP, признаки некорректного использования протокола IMAP;
- **RTT ET open/emerging-inappropriate** - набор правил описывает признаки обращения к нежелательным ресурсам;
- **RTT ET open/emerging-info** - набор правил содержит сигнатуры различных уязвимостей;
- **RTT ET open/emerging-malware** - набор правил содержит сигнатуры вредоносного ПО, использующего в своей работе протокол HTTP;
- **RTT ET open/emerging-misc** - набор правил содержит сигнатуры различных уязвимостей;
- **RTT ET open/emerging-mobile_malware** - набор правил содержит сигнатуры вредоносного ПО для мобильных платформ;
- **RTT ET open/emerging-netbios** - набор правил содержит содержит сигнатуры уязвимостей в протоколе NetBIOS, признаки некорректного использования протокола NetBIOS;
- **RTT ET open/emerging-p2p** - набор правил описывает признаки обращения к P2P-сетям (Bittorrent, Gnutella, Limewire);
- **RTT ET open/emerging-policy** - набор правил описывает нежелательную сетевую активность (обращение к MySpace, Ebay);
- **RTT ET open/emerging-pop3** - набор правил содержит сигнатуры уязвимостей в протоколе POP3, признаки некорректного использования протокола POP3;
- **RTT ET open/emerging-rpc** - набор правил содержит сигнатуры уязвимостей в протоколе RPC, признаки некорректного использования протокола RPC;
- **RTT ET open/emerging-scada** - набор правил содержит сигнатуры уязвимостей для SCADA-систем;
- **RTT ET open/emerging-scan** - набор правил описывает признаки активности, связанной с сетевым сканированием (Nessus, Nikto, portscanning);
- **RTT ET open/emerging-shellcode** - набор правил описывает признаки активности, связанной с попытками получить шелл-доступ в результате выполнения эксплойтов;
- **RTT ET open/emerging-smtp** - набор правил содержит сигнатуры уязвимостей в протоколе SMTP, признаки некорректного использования протокола SMTP;
- **RTT ET open/emerging-snmp** - набор правил содержит сигнатуры уязвимостей в протоколе SNMP, признаки некорректного использования протокола SNMP;
- **RTT ET open/emerging-sql** - набор правил содержит сигнатуры уязвимостей для СУБД SQL;
- **RTT ET open/emerging-telnet** - набор правил содержит сигнатуры уязвимостей для протокола telnet, признаки некорректного использования протокола telnet;
- **RTT ET open/emerging-tftp** - набор правил содержит сигнатуры уязвимостей для протокола TFTP, признаки некорректного использования протокола TFTP;

- **RTT ET open/emerging-user_agents** - набор правил содержит признаки подозрительных и потенциально опасных HTTP-клиентов (идентифицируются по значениям в HTTP-заголовке User-Agent);
- **RTT ET open/emerging-web_client** - набор правил содержит сигнатуры уязвимостей для WEB-клиентов;
- **RTT ET open/emerging-web_server** - набор правил содержит сигнатуры уязвимостей для WEB -серверов;
- **RTT ET open/emerging-web_specific_apps** - набор правил содержит сигнатуры уязвимостей для WEB -приложений;
- **RTT ET open/emerging-worm** - набор правил описывает признаки активности сетевых червей.

Набор правил, который распространяется по **дополнительной лицензии**:

- **Kaspersky Suricata Rules** – комплексный набор правил для системы обнаружения и предотвращения вторжений, разработанный «Лабораторией Касперского» для обнаружения новейших и наиболее совершенных угроз с целью защиты пользователей решений компании. Общее количество правил составляет около 5 000.

Kaspersky Suricata Rules предназначены для обнаружения угроз из следующих категорий:

- APT (таргетированные угрозы);
- Botnet C&C (центры управления ботнетами);
- Банковские трояны и средства похищения персональных данных;
- DNS-туннели;
- Программы-вымогатели;
- Эксплоиты;
- Хакерские инструменты;
- Крипто-майнеры.

Совет

Список доступных пользователю правил системы обнаружения вторжения находится в разделе **Службы - Обнаружение вторжений – Администрирование** на вкладке **Обновление правил**

2.6.12.5 Описание параметров конфигурации СОВ

Конфигурирование параметров системы обнаружения вторжения производится в разделе Службы - Обнаружение вторжений - Администрирование в соответствии с таблицей.

Таблица 30: Описание параметров конфигурации СОВ

Параметр	Описание
Включить	Запуск основного режима работы системы обнаружения вторжений - IDS
Режим IPS	Запуск режима работы системы предотвращения вторжений - IPS
Включить обработку пакетов, назначенных этому устройству (IPS)	По умолчанию системой обнаружения вторжений обрабатываются только транзитные пакеты. Активации параметра позволяет системе обнаружения вторжений производить обработку входящих пакетов, предназначенных только системе
Enable filter rules (IPS)	Задать механизм обработки трафика системой обнаружения вторжений: * Не использовать правила – в первую очередь трафик обрабатывается системой обнаружения вторжений, далее система производит обработку правилами фильтрации * Использовать правила - в первую очередь трафик обрабатывается правилами фильтрации межсетевого экрана, далее система производит обработку системой обнаружения вторжений
Неразборчивый режим	Активация данного режима позволяет системе анализировать трафик с любым MAC-адресом получателя, отличным от MAC-адреса входящего интерфейса
Сравнение маршрутов	Обработка трафика с учетом использования алгоритма Aho-Corasick. Вариации алгоритма влияют на производительность обработки трафика
Интерфейсы	Выбор интерфейса, на котором будет производиться анализ трафика
Домашние сети	Задать зону источника трафика в виде списка IP-адресов источника трафика
Размер пакета по умолчанию	Задать размер обрабатываемого пакета. Размер обрабатываемого пакета влияет на производительность системы. Размер пакета по умолчанию - 1514 байт
Полезная нагрузка пакета журнала	Журналирование полезной нагрузки пакета при попадании трафика под условия правил IDS/IPS

2.6.12.6 Стандартная настройка системы обнаружения вторжения в режиме IDS/IPS

Стандартная конфигурация СОВ включает основные параметры для анализа проходящего трафика.

Для конфигурации СОВ необходимо перейти на вкладку **Настройки** раздела **Службы - Обнаружение вторжений – Администрирование** и произвести следующие настройки:

- Произвести запуск основного режима IDS параметром **Включен**;
- в случае необходимости, активация режима IPS производится параметром **Режим IPS**;

Важно

Режим IPS функционирует только при запущенном режиме IDS

- Задать механизм обработки трафика системой обнаружения вторжений - **Использовать правила**;
- Задать интерфейс в поле параметра **Интерфейсы**, на котором будет производиться анализ входящего трафика;

- Перейти в расширенный режим и поле параметра **Домашние сети** и указать адрес сети зоны источника трафика.

Стандартная конфигурация системы обнаружения вторжений представлена на рисунке.

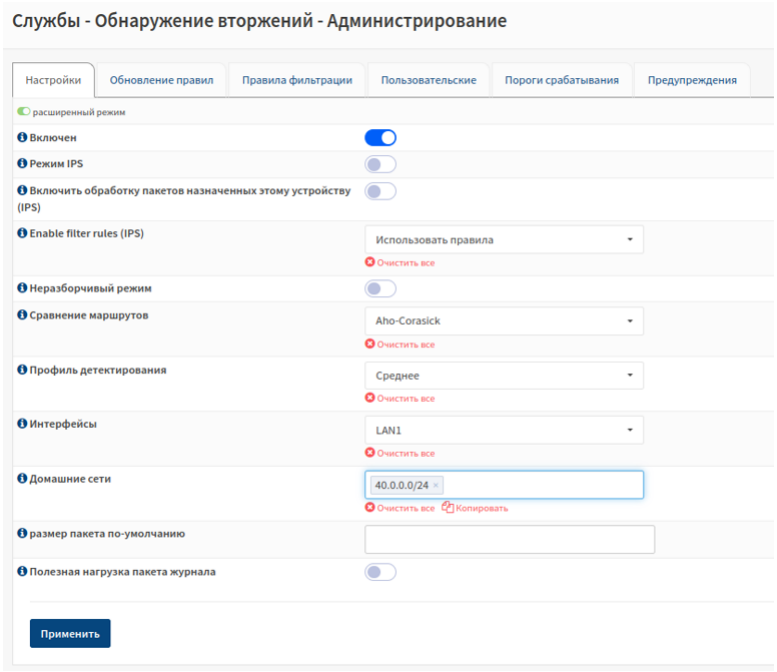


Рис. 81: Стандартная конфигурация системы обнаружения вторжений представлена на рисунке.

На вкладке **Обновление правил** произвести выбор необходимых наборов правил, представленных на рисунке.

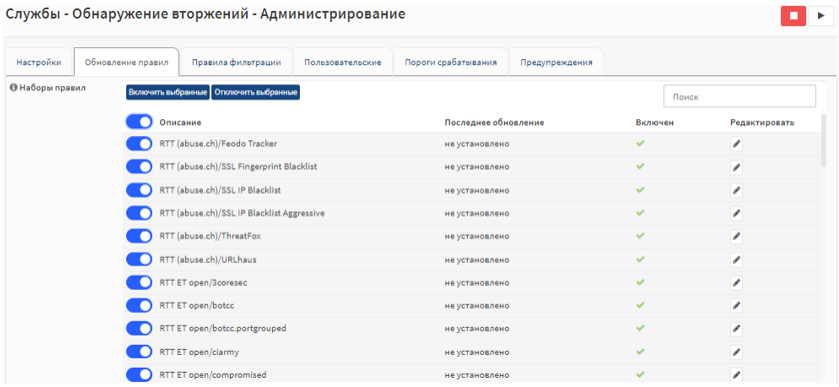


Рис. 82: Список доступных правил

После сохранения данной конфигурации модуль СОВ операционной системы REFOS начнет анализировать и детектировать весь входящий трафик на заданный конфигурацией интерфейс.

Предупреждения система транслирует на вкладку **Предупреждения**.

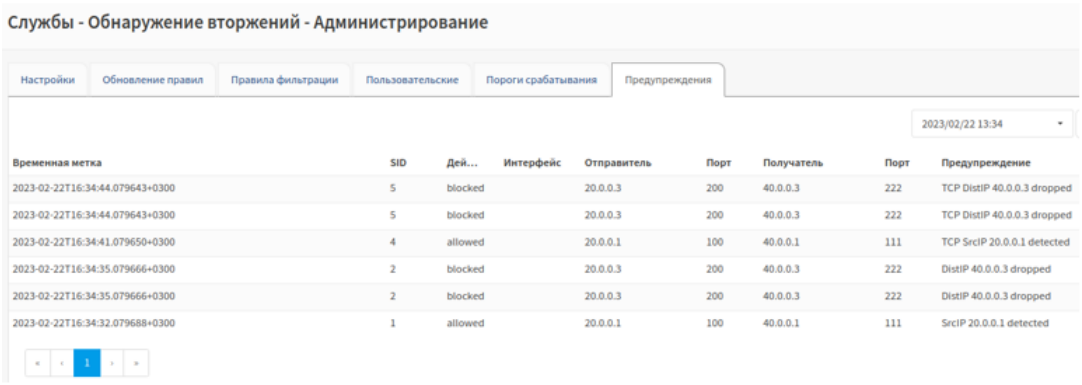


Рис. 83: Вкладка **Предупреждения**

2.6.12.7 Пользовательские правила системы обнаружения вторжений

Функциональный модуль СОВ операционной системы REFOS позволяет использовать не только готовый набор правил детектирования, а также производить конфигурацию пользовательских правил детектирования.

Пользовательские правила состоят из следующих параметров:

- **Действие (Action)** – параметр, который определяет, что необходимо делать с трафиком при совпадении его параметров с параметрами правил детектирования;
- **Заголовок (Header)** – ряд параметров, которые определяют в правиле детектирования протоколы, IP-адреса, порты и направление детектирования трафика;
- **Опции правила детектирования** – определяет ряд параметров полезной нагрузки пакета.

Пример пользовательского правила детектирования показан на рисунке.

```
tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USSR +..)";
flow:established,to_server; flowbits:isset,is_proto_irc; content:"Alexander"; pcre:"/
Alexander .*USSR.*[0-9]{3,}/i"; reference:url,doc.emergingthreats.net/2008124;
classtype:trojan-activity; sid:2008124; rev:2;)
```

Рис. 84: Пример пользовательского правила детектирования

В данном примере:

- Зеленым текстом выделен ряд параметров Заголовка (Header);
- Синим текстом выделены Опции правила детектирования.

2.6.12.8 Описание основных параметров пользовательских правил системы обнаружения вторжений

- Параметр **Действие (Action)**

Допустимые значения параметра **Действие (Action)**:

- **Предупреждать** – генерировать предупреждение;
- **Отбрасывать** - прекратить дальнейшую проверку пакета;
- **Разрешать** - отбросить пакет и генерировать предупреждение;

- Значения параметра **Заголовок**
- **Протокол**;

```
tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USSR
+..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"Alexander";
pcre:"/ Alexander .*USSR.*[0-9]{3,}/i";
reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity;
sid:2008124; rev:2;)
```

Рис. 85: Протокол

Допустимые значения представлены в таблице.

Таблица 31: Основные параметры фильтрации

Значения
• tcp • dns • nfs • tftp • udp • dcerpc • ikev2 • sip • icmp • ssh • krb5 • http2 • ip • smtp • ntp • http • imap • dhcp • ftp • Modbus • rfb • tls (включая ssl) • dnp3 • rdp • smb • enip • snmp

- **IP-адреса отправителя и получателя**;

Первая выделенная часть - $HOME_NET является источником, вторая — $EXTERNAL_NET пунктом назначения (обратите внимание на направление стрелки направления). С помощью данных значений можно назначать IP-адреса и диапазоны IP-адресов, а также комбинировать значения с операторами в соответствии с таблицей.

```
tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USSR
+..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"Alexander";
pcre:"/ Alexander .*USSR.*[0-9]{3,}/i";
reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity;
sid:2008124; rev:2;)
```

Рис. 86: IP-адреса отправителя и получателя

Таблица 32: Параметры для комбинирования

Оператор	Описание
../..	Диапазон IP-адресов
!	Исключить IP-адрес или диапазон
[.., ..]	Группа IP-адресов
any	Любой IP-адрес

Пример пользовательского правила с параметрами **IP-адреса Отправителя и получателя** показан на рисунке .

```
udp 20.0.0.1 any -> 40.0.0.0/24 any (msg:"SrcIP 20.0.0.1 detected."; sid: 1;)
```

Рис. 87: Пример пользовательского правила с параметрами **IP-адреса Отправителя и получателя**

- **Порты отправителя и получателя**;

```
tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC (USSR
+..)"; flow:established,to_server; flowbits:isset,is_proto_irc; content:"Alexander";
pcre:"/ Alexander .*USSR.*[0-9]{3,}/i";
reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity;
sid:2008124; rev:2;)
```

Рис. 88: Порты отправителя и получателя

Первая выделенная часть - any является портом источника, вторая — any портом назначения. С помощью данных значений можно назначать порты и диапазоны портов, а также комбинировать значения с операторами в соответствии с таблицей.

Таблица 33: Параметры для комбинирования

Оператор	Описание
../..	Диапазон портов
!	Исключить порт или диапазон портов
[.., ..]	Группа портов
any	Любой порт

Пример пользовательского правила с параметрами **портов отправителя и получателя** показан на рисунке.

- **Направление**;

Позволяет задать направление трафика от отправителя до получателя. Т.е. при использовании значения - (->) будут анализироваться пакеты инициированные отправителем в сторону получателя.

```
tcp any 300 -> any any (msg:"TCP Port 300 accept"; sid: 6;)
```

Рис. 89: Пример пользовательского правила с параметрами **портов отправителя и получателя**

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET TROJAN Likely Bot Nick in IRC
(USSR +..)"; flow:established,to_server; flowbits:isset,is_proto_irc;
content:"Alexander"; pcre:"/ Alexander .*USSR.*[0-9]{3,}/i";
reference:url,doc.emergingthreats.net/2008124; classtype:trojan-activity;
sid:2008124; rev:2;)
```

Рис. 90: Направление

Также возможно анализировать пакеты в обе стороны (особенно актуально для TCP-соединения) при помощи значения – (< >).

Например, при данных значениях:

- udp **20.0.0.1** any -> **40.0.0.0/24** any - будут анализироваться только пакеты инициированные отправителем с IP-адресом 20.0.0.1 в сторону получателя сети 40.0.0.0/24;
- udp **20.0.0.1** any <> **40.0.0.0/24** any - будут анализироваться пакеты инициированные отправителем с IP-адресом 20.0.0.1 в сторону получателя сети 40.0.0.0/24, а также в обратно направлении.

Важно

Направление с таким значением – (<-) не существует

- **Опции правила детектирования**

Остальная часть правила состоит из опций. Они заключаются в круглые скобки и разделяются точкой с запятой. Некоторые параметры имеют значение (например, msg), которые определяются ключевым словом параметра, за которым следует двоеточие, а затем параметры. Другие не имеют настроек и представляют собой просто ключевое слово (например, nocase).

```
<keyword>: <settings>;
<keyword>;
```

Рис. 91: Опции правила детектирования

Параметры правила имеют определенный порядок, и изменение их порядка изменит значение правила.

Важно

Символы ; и « имеют особое значение в языке правил и должны быть исключены при использовании в значении параметра правила

Совет

Например: msg:»Message with semicolon;»;

Важно

Также необходимо избегать обратной косой черты, поскольку она функционирует как escape-символ

2.6.12.9 Пример конфигурации системы обнаружения вторжений с использованием пользовательских правил детектирования

Для конфигурации СОВ необходимо перейти на вкладку **Настройки** раздела **Службы - Обнаружение вторжений – Администрирование** и произвести следующие настройки:

- Произвести запуск основного режима IDS параметром **Включен**;
- в случае необходимости активация режима IPS производится параметром **Режим IPS**;
- Задать механизм обработки трафика системой обнаружения вторжений - **Использовать правила**;
- Задать интерфейс в поле параметра **Интерфейсы**, на котором будет производиться анализ входящего трафика;

Конфигурация СОВ показана на рисунке.

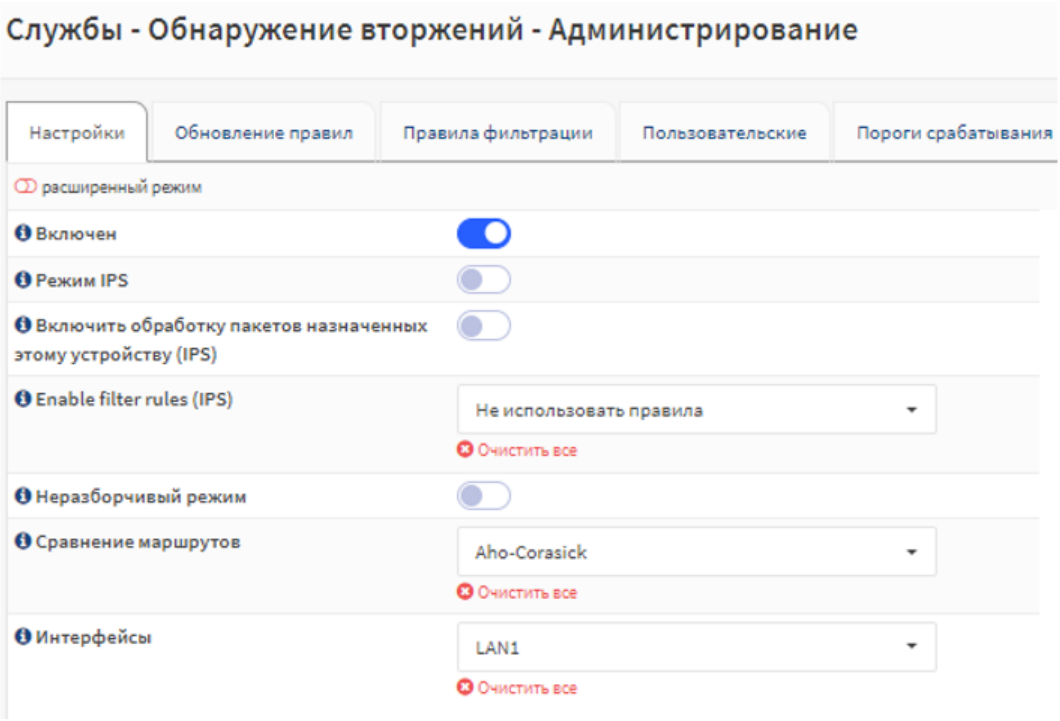


Рис. 92: Конфигурация СОВ

На вкладке **Пользовательские** задать пользовательские правила детектирования. Например, необходимо детектировать трафик с заданными параметрами.

Таблица 34: Заданные параметры

Протокол	IP-адрес отправителя	IP-адрес получателя
UDP	20.0.0.1	40.0.0.1
UDP	20.0.0.3	40.0.0.3

На вкладке **Пользовательские** создается пользовательское правило детектирования символом  .

В окне **Описание правила** задать следующие параметры:

- Параметром **Включен** произвести активацию правила детектирования;
- В параметре **Тип** выбрать значение **Пользовательские**;
- В поле параметра **User defined rule** задать правило детектирования;
- В параметре **Действие** выбрать;
- В параметре **Описание** задать общее описание правила детектирования.

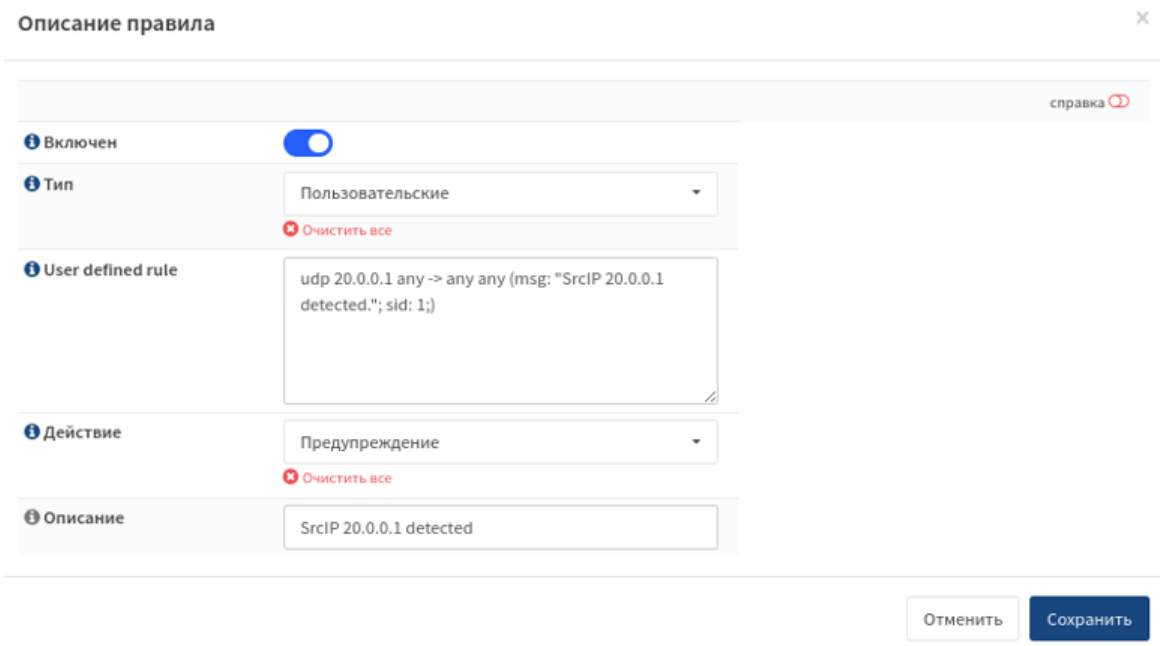


Рис. 93: Первое пользовательское правило детектирования

После сохранения конфигурации пользовательских правил детектирования, результаты анализа трафика данными правилами представлены на вкладке **Предупреждения** и показан на рисунке.

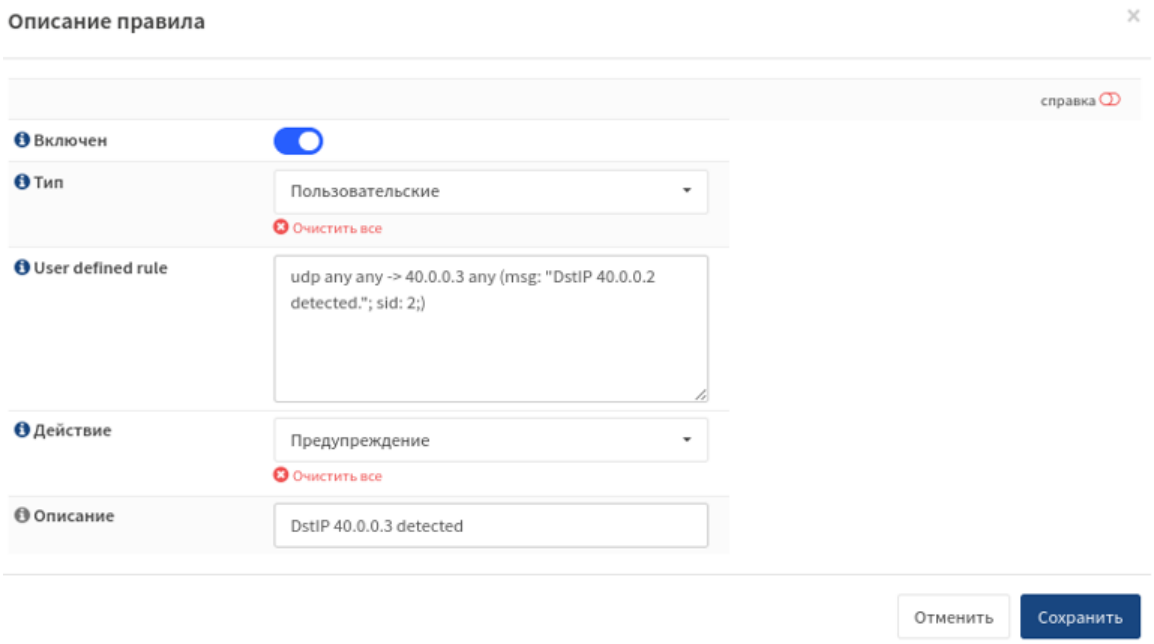


Рис. 94: Второе пользовательское правило детектирования

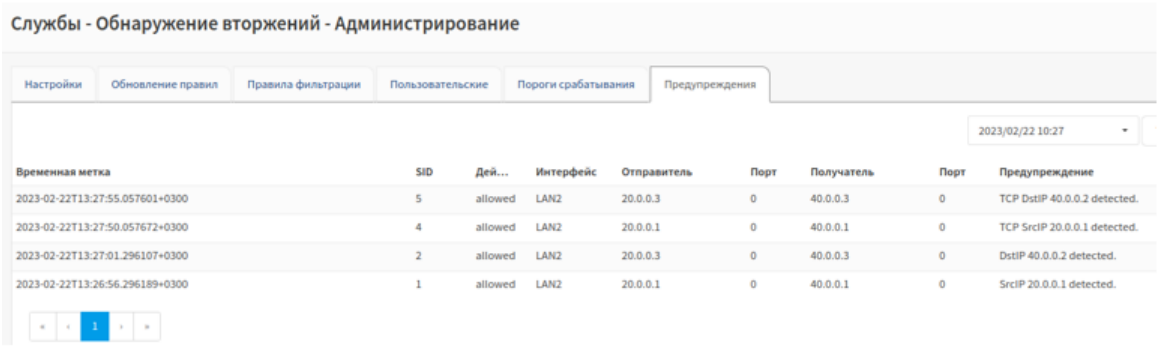


Рис. 95: Результат анализа трафика на вкладке **Предупреждения**

2.6.13 Маршрутизация

2.6.13.1 Статическая маршрутизация

Введение

Маршрутизация одна из основных функций операционной системы REFOS и построенных на её основе многофункциональных межсетевых экранов RTT-M300, которая позволяет производить маршрутизацию трафика из одной сети в другую.

Система производит анализ IP-адреса получателя в заголовке пакета и сопоставляет его с маршрутом в таблице маршрутизации. Заполнение и актуализация маршрутов может производиться вручную пользователем - статически, или динамически – протоколами динамической маршрутизации.

Операционная система REFOS позволяет задавать статические маршруты и использовать их для маршрутизации трафика.

Наличие поддержки протокола BFD (Bidirectional Forwarding Detection protocol) позволяет фиксировать канальные сбои, а работа в связке с протоколами маршрутизации улучшает актуализацию маршрутной информации.

Маршрут по умолчанию (default routing)

Маршрут по умолчанию используется в том случае, если не найдены соответствия ни одному маршруту в таблице маршрутизации. Данный маршрут также называют шлюзом последней надежды (Gateway of Last Resort), который будет использоваться для маршрутизации пакета, если отсутствует явный маршрут.

Маршрут по умолчанию имеет следующий вид **0.0.0.0/0**.

Добавление или редактирование статического маршрута

Для добавления статического маршрута необходимо:

- Перейти в раздел **Система - Маршруты** – **Конфигурация** и нажатием значка  создать новый статический маршрут.
- Заполнить параметры статического маршрута, указанные в таблице

Таблица 35: Параметры статического маршрута

Параметр	Описание
Отключить	Отключить использование статического маршрута без удаления из конфигурации системы
Адрес сети	Ввести адрес IP-адрес сети получателя и маску подсети. Например, маршрут по умолчанию – 0.0.0.0/0
Шлюз	Выбрать шлюз, который будет ассоциирован с маршрутом
Описание	Общее описание маршрута

Важно

Для создания статического маршрута необходимо произвести конфигурацию шлюза

Совет

Параметры конфигурации шлюза доступны в разделе **Система - Шлюзы**

Пример конфигурации статического маршрута представлен на рисунке.

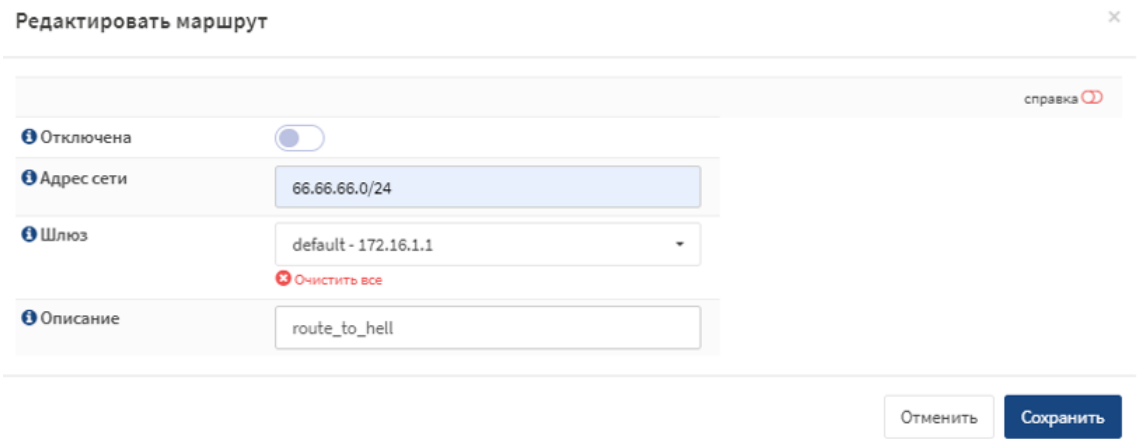


Рис. 96: Пример конфигурации статического маршрута

Важно

После сохранения параметров статического маршрута в окне **Редактировать маршрут**, конфигурацию созданного маршрута необходимо применить, нажав кнопку Применить на основной странице раздела **Система - Маршруты – Конфигурация** для вступления настроек в силу

Просмотр статических маршрутов в таблице маршрутизации

Просмотр статических маршрутов доступен в таблице маршрутизации в разделе **Система - Маршруты – Статус**

Получатель	Шлюз	Флаги	Маска	Инт-йс
0.0.0.0	50.0.0.2	UG	0.0.0.0	enP2p1s0f0
0.0.0.0	172.16.1.2	UG	0.0.0.0	eth4
0.0.0.0	40.0.0.2	UG	0.0.0.0	eth5
0.0.0.0	172.16.1.1	UG	0.0.0.0	eth4
10.0.0.0	0.0.0.0	U	255.255.255.0	enP2p1s0f3
20.0.0.0	0.0.0.0	U	255.255.255.0	enP2p1s0f2
40.0.0.0	0.0.0.0	U	255.255.255.252	eth5
50.0.0.0	0.0.0.0	U	255.255.255.252	enP2p1s0f0
66.66.66.0	172.16.1.1	UG	255.255.255.0	eth4
172.16.1.0	0.0.0.0	U	255.255.255.0	eth4

Рис. 97: Таблица маршрутизации

Таблица 36: Описание значений таблицы маршрутизации

Значение	Описание
Получатель	IP-адрес сети получателя
Шлюз	IP-адрес шлюза. Используется как адрес следующего перехода в данном маршруте
Флаги	Флаги, которые описывают маршрут: G – в маршруте используется IP-адрес шлюза; U – интерфейс активен(up); H – только один хост может быть доступен через маршрут. Например, Loopback-интерфейс 127.0.0.1
Маска	Сетевая маска сети получателя
Максимальный размер сегмента	Определяет максимальный размер полезного блока данных в байтах для TCP-пакета (сегмента). 0 – значение по умолчанию
IRTT	Начальное время приёма-передачи (Initial Round Trip Time, RTT). Начальное время приема-передачи — это значение, которое протокол TCP будет использовать при первом установлении соединения. 0 – значение по умолчанию
Инт-йс	Системное имя исходящего интерфейса
Инт-йс(имя)	Заданное пользователем имя исходящего интерфейса
Действие	Позволяет производить удаление записи маршрута из таблицы маршрутизации

2.6.13.2 Асимметричная маршрутизация

В основе ассиметричной маршрутизации лежит разделение маршрутов исходящего и входящего трафика. Например, входящий трафик может приниматься от одного провайдера, а исходящий будет отправляться через другого.

Например, рассматривая TCP-соединение, если пакеты в направлениях запроса и ответа следуют по разным путям, REFOS при неактивном процессе асимметричной маршрутизации заблокирует прохождение пакетов, поскольку трехстороннее рукопожатие TCP не установлено через REFOS.

По умолчанию процесс ассиметричной маршрутизации запущен. Конфигурация ассиметричной маршрутизации производится в разделе **Система - Настройки - Общие настройки**.

Рис. 98: Ассиметричная маршрутизация

2.6.13.3 Динамическая маршрутизация

Введение

Определение оптимального маршрута в сетях передачи данных является важным процессом для поддержки межсетевого взаимодействия удаленных сегментов сети. Операционная система REFOS имеет поддержку не только статической маршрутизации, но и обладает поддержкой ряда динамических протоколов маршрутизации. Условно список поддерживаемых протоколов можно разделить на протоколы внутренней маршрутизации (IGP) и протоколы внешней маршрутизации (EGP).

Протоколы внутренней маршрутизации используются для маршрутизации внутри автономной системы. Например, в рамках одной организации. Организация может быть территориально распределенной и использовать большое количество частных сетей.

Операционная система REFOS поддерживает следующие протоколы маршрутизации IGP:

- RIP v2;
- OSPFv2.

Протоколы внешней маршрутизации (EGP) используются для маршрутизации между автономными системами. Данные тип протоколов чаще используется для взаимодействия в сетях операторов связи.

Операционная система REFOS поддерживает следующий протокол маршрутизации EGP:

- BGP.

Параметры конфигурирования протоколов динамической маршрутизации

Для запуска подсистемы динамической маршрутизации необходимо на вкладке **Маршрутизация - Общие настройки** активировать параметр **Включить**.

Параметр **Включить журналирование** позволяет производить журналирование активности протоколов маршрутизации. Результаты транслируются в раздел **Маршрутизация - Диагностика – Журналирование**.

Для корректной работы сервиса маршрутизации, службы должны находится в активном состоянии .

Неактивное состояние служб сервиса маршрутизации представлено на рисунке.

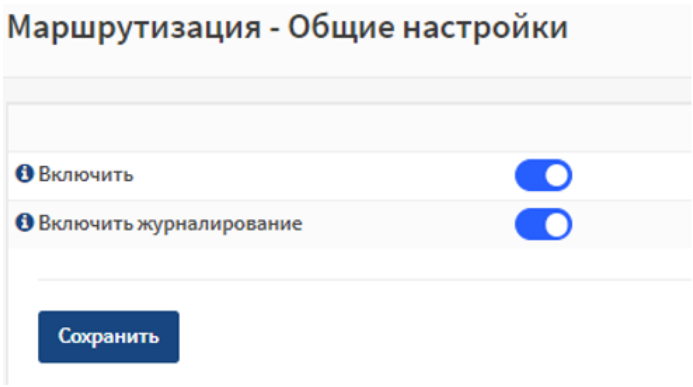


Рис. 99: Вкладка **Маршрутизация - Общие настройки**

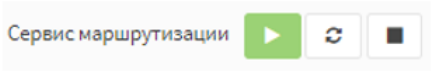


Рис. 100: Активное состояние сервиса маршрутизации

Протокол динамической маршрутизации RIPv2

RIPv2 – протокол дистанционно-векторной маршрутизации, который в качестве метрики маршрутизации использует переходы – транзитные интерфейсы сетевых устройств (хопы). Максимальное количество транзитных переходов, разрешенное в RIP — 15 (метрика 16 означает «бесконечно большую метрику»). Служба протокола RIP по умолчанию вещает в сеть свою полную таблицу маршрутизации раз в 30 секунд. RIP работает в сетях TCP/IP, используя UDP порт 520.

Протокол RIP в основном используется в небольших коммерческих сетях.

Параметры конфигурирования протокола динамической маршрутизации RIPv2

Основные параметры конфигурации протокола RIP находятся в разделе **Маршрутизация** – **RIP** – **Общие настройки**.

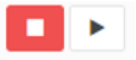


Рис. 101: Неактивное состояние сервиса маршрутизации

Таблица 37: Основные параметры конфигурации протокола RIP

Параметр	Описание
Включить	Активирует сервис протокола RIP
Пассивные интерфейсы	Ограничение отправки обновлений маршрутизации. Если необходимо ограничить отправку обновлений маршрутизации RIP в определенный сегмент сети, достаточно указать интерфейс системы, который ассоциирован с данной сетью
Перераспределение маршрута	Параметр, который позволяет включать в обновления маршрутизации RIP информацию о других маршрутах, которыми располагает RTT-M300: • Непосредственно подключенные сети – **Directly connected routes**; • **Статически настроенные маршруты**; • Маршруты из домена маршрутизации OSPF - **OSPF**; • Маршруты из домена маршрутизации BGP - **BGP**
Networks IPv4	Запуск процесса анонсирования маршрутов. Пример ввода IPv4 адреса сети - X.X.X.X/X
Default Metric	Параметр, который используется совместно с перераспределением маршрута, чтобы заставить текущий протокол маршрутизации использовать одно и то же значение метрики для всех перераспределяемых маршрутов. **Default Metric** помогает решить проблему перераспределения маршрутов с несовместимыми метриками. Всякий раз, когда показатели не преобразуются, использование показателя по умолчанию обеспечивает разумную замену и позволяет продолжить перераспределение
Update timer	Частота отправки обновлений маршрутизации. По умолчанию значение таймера равно 30 секундам
Route timeout	Таймер обновления маршрутной информации. По истечении таймера маршрут больше не действителен; однако он сохраняется в таблице маршрутизации в течение короткого времени, чтобы соседи могли быть уведомлены о том, что маршрут был удален. По умолчанию значение таймера равно 180 секундам
Garbage timer	Таймер удаления устаревшей маршрутной информации. По истечении таймера маршрут окончательно удаляется из таблицы маршрутизации. По умолчанию значение таймера равно 120 секундам

Дополнительные параметры конфигурации протокола RIP в разделе **Маршрутизация – RIP – Интерфейсы**.

Таблица 38: Дополнительные параметры конфигурации протокола RIP

Параметр	Описание
Включить	Запуск процесса аутентификации обновлений маршрутизации
Интерфейс	Выбор интерфейса, которому будут применяться параметры процесса аутентификации
Тип аутентификации	Выбор метода аутентификации: • Text – использование простого пароля (Ключ аутентификации), который передается в обновлениях маршрутизации в открытом виде, что является небезопасным. • MD5 - метод использует для аутентификации хеш-сумму заданного Ключа аутентификации. Предоставляет больший уровень защиты, чем Text-аутентификация
Ключ аутентификации	Установка пароля аутентификации. Ограничение по паролю – не более 16 символов

Пример конфигурации протокола RIP

Предположим, что необходимо настроить обмен маршрутной информации с соседним устройством (Маршрутизатором) при помощи протокола RIP в рамках сетевой топологии ниже.

Важно

RIP для обмена маршрутными данными использует UDP порт 520. Для корректного получения и отправки анонсов маршрутизации необходимо предусмотреть соответствующее разрешающее правило межсетевого экрана двух направлений – **Input** и **Output**.

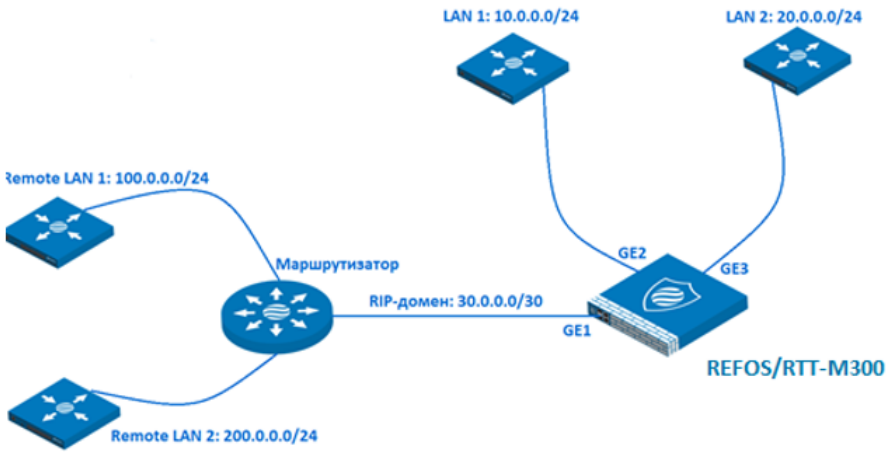


Рис. 102: Сетевая топология

Операционная система REFOS и Маршрутизатор имеют по три непосредственно подключенных сети (directly connected).

Пример конфигурации протокола RIP представлен ниже:

1. В разделе **Маршрутизация – RIP** на вкладке **Общие настройки** производится основная настройка протокола RIP :

- Параметром **Включен** произвести запуск протокола RIP;
- В параметре **Пассивные интерфейсы** ограничить рассылку маршрутизации по портам GE2, GE3, так как локальные сети пользователей (LAN1 и LAN2) не нуждаются в анонсах маршрутной информации;
- В параметре **Перераспределение маршрута** указать маршруты, которые подлежат добавлению в обновления маршрутной информации. В данном примере – непосредственно подключенные (directly connected routes);
- Параметр **Networks IPv4** позволяет согласовать обмен маршрутной информации RIP. Задается адрес сети, которая используется для обмена маршрутной информации.

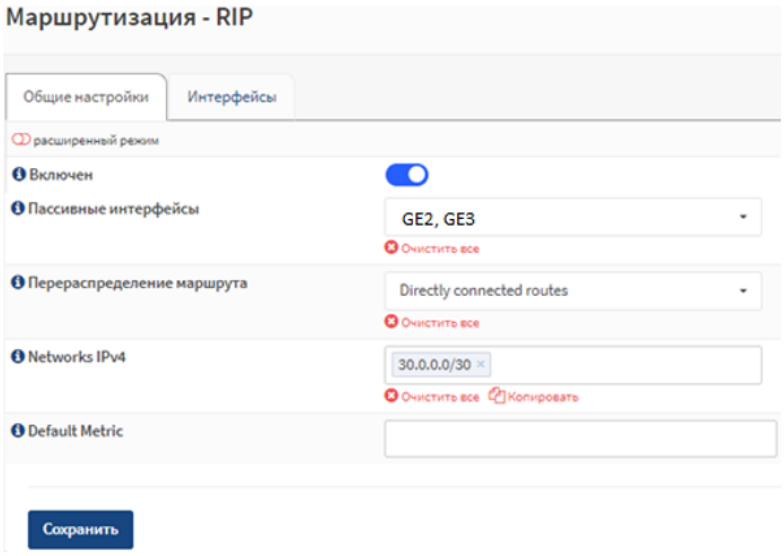


Рис. 103: Пример конфигурации. Вкладка **Общие настройки**

2. На вкладке **Интерфейсы** производится настройка аутентификации протокола RIP:

- Добавить интерфейс и произвести запуск маршрутизации RIP параметром **Включен**;
- В параметре **Интерфейс** указываем порт, который используется для обмена маршрутной информации с соседним устройством;
- Выбираем тип аутентификации и задаем пароль.

После сохранения конфигурации и запуска сервиса протокола RIP, Операционная система REFOS и Маршрутизатор должны обменяться маршрутной информацией. В результате обмена маршрутной информацией, каждый участник обмена (Операционная система REFOS и Маршрутизатор) должен иметь маршрутную информацию (запись в таблице маршрутизации) по сетям, которые непосредственно подключены (directly connected) к противоположному соседу. Проверить состояние сервиса и таблицу маршрутизации возможно в разделе **Маршрутизация – Диагностика**.

Общий статус таблицы маршрутизации представлен на рисунке.

Операционная система REFOS после обмена маршрутной информации получила информацию соседнего маршрутизатора о сетях, которые до обмена были ему недоступны.

Текущая конфигурация протокола RIP представлена на рисунке.

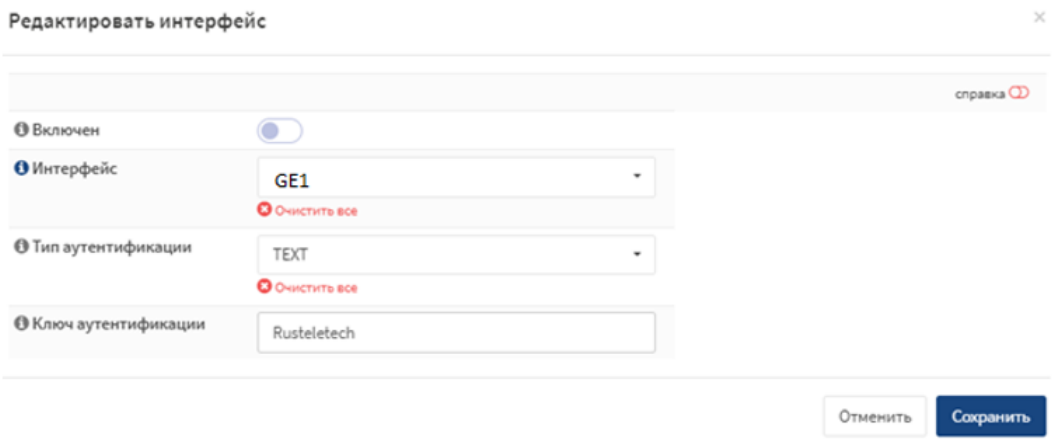


Рис. 104: Пример конфигурации. Вкладка **Интерфейсы**

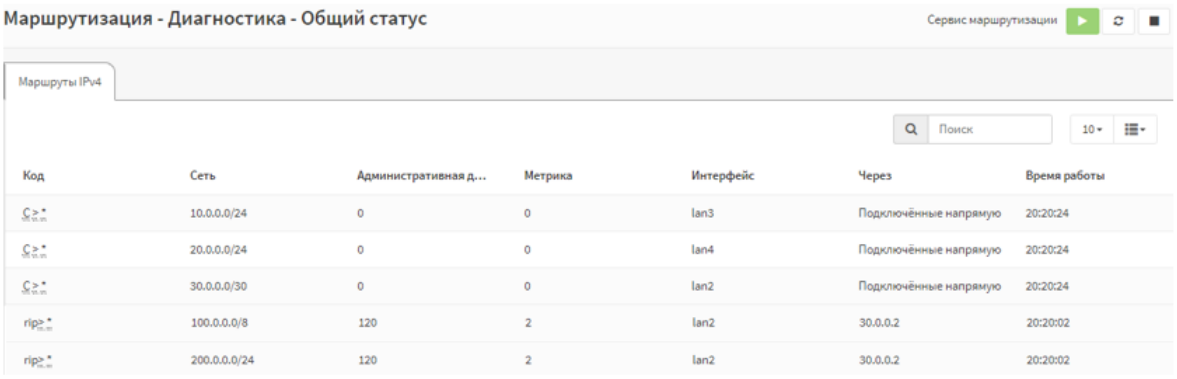


Рис. 105: Общий статус таблицы маршрутизации

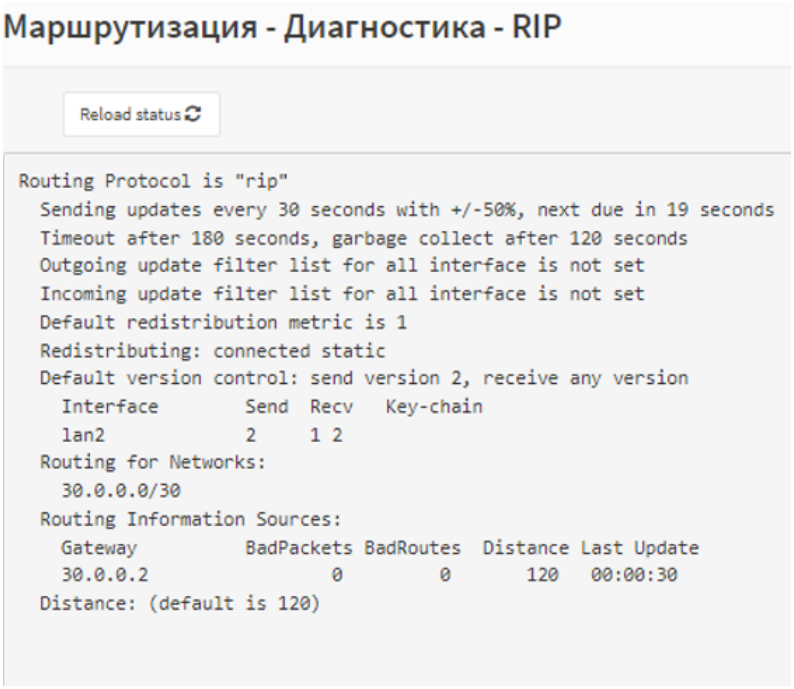


Рис. 106: Текущая конфигурация протокола RIP

Более подробная информация о параметрах диагностики протокола RIP представлена в разделе **Диагностика и журналирование протоколов маршрутизации**.

Протокол динамической маршрутизации OSPF

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры.

Основные преимущества:

- Высокая скорость сходимости по сравнению с дистанционно-векторными протоколами маршрутизации (например, RIP);
- Поддержка сетевых масок переменной длины (VLSM);
- Оптимальное использование пропускной способности с построением дерева кратчайших путей.

OSPF является масштабируемым протоколом, т.е. может функционировать как в небольших сетях, так и использоваться в очень крупных территориально-распределенных сетях.

Параметры конфигурирования протокола динамической маршрутизации OSPFv2

Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Общие настройки**.

Таблица 39: Дополнительные параметры конфигурации протокола RIP

Параметр конфигурации протокола OSPF	Описание
Включить	Активирует сервис протокола OSPF
Reference Cost	Эталонная OSPF-метрика(стоимость) интерфейса. По умолчанию используется значение 100 Мбит/с (т.е. канал с пропускной способностью 100 Мбит/с или выше будет стоить 1. Стоимость каналов с меньшей пропускной способностью будет масштабироваться с учетом этой стоимости). Значение эталонной OSPF-метрики должно быть одним на всех сетевых устройствах в OSPF-сегменте
Перераспределение маршрута	Параметр, который позволяет включать в обновления маршрутизации OSPF информацию о других маршрутах, которыми располагает операционная система REFOS: • Непосредственно подключенные сети – **Directly connected routes**; • **Статически настроенные маршруты**; • Маршруты из домена маршрутизации RIP - **RIP**; • Маршруты из домена маршрутизации OSPF - **OSPF**; • Маршруты из домена маршрутизации BGP - **BGP**
Карта перераспределения	
Объявить шлюз по умолчанию	Распространение маршрута по умолчанию (0.0.0.0/0) в OSPF домене
Всегда объявлять шлюз по умолчанию	Распространение маршрута по умолчанию (0.0.0.0/0) в OSPF домен независимо от того, имеет ли система маршрут по умолчанию
Объявить метрику шлюза по умолчанию	Изменение метрики распространяемого маршрута по умолчанию (0.0.0.0/0)

Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Сети**.

Таблица 40: Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Сети**

Параметр конфигурации протокола OSPF	Описание
Включить	Запуск рассылки анонсов маршрутизации OSPF
Адрес сети	Адрес сети интерфейса, который участвует в анонсе маршрутизации
Маска сети	Сетевая маска адреса сети
Область	Идентификатор зоны маршрутизации
Диапазон области	Суммирование маршрутов в заданной зоне маршрутизации. Параметр можно использовать только, если система выступает как ABR-маршрутизатор
Список префиксов входящих	Указать префикс-лист, который будет применен к анонсируемым маршрутам
Список префиксов исходящих	Указать префикс-лист, который будет применен к принимаемым маршрутам

Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Интерфейсы**

Таблица 41: Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Интерфейсы**

Параметр конфигурации протокола OSPF	Описание
Включить	Ассоциировать интерфейс с OSPF-доменом маршрутизации
Passive	Запретить IP-интерфейсу обмениваться протокольными сообщениями с соседями через указанный физический интерфейс
Интерфейс	Выбор интерфейса системы для отправки и приема OSPF-анонсов маршрутизации
Тип аутентификации	Выбрать тип аутентификации MD5
Ключ аутентификации	Задать ключ аутентификации
Идентификатор ключа аутентификации	Параметр задается автоматически системой
Область	Задать область(area) в которой будет использоваться интерфейс
Стоимость	Установить метрику состояния интерфейса, которая является условным показателем *стоимости* пересылки данных по интерфейсу
Интервал приветствия	Установить интервал времени в секундах, по истечении которого маршрутизатор отправляет следующий hello-пакет с интерфейса
Dead Interval	Установить интервал времени в секундах, по истечении которого сосед будет считаться неактивным. Этот интервал должен быть кратным значению hello-interval. dead-interval равен 4 интервалам отправки hello-пакетов
Интервал повторной передачи	Установить интервал времени в секундах, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении (например, Database Description или Link State Request пакеты)
Пауза повторной передачи	Установить примерное время в секундах, необходимое для передачи пакета состояния канала
Приоритет	Установить приоритет маршрутизатора, который используется для выбора DR и BDR
BFD	Запустить функционирование протокола BFD на интерфейсе
Тип сети	Выбрать тип сети: • широковещательная сеть с множественным доступом; • point-to-point сеть; • point-to-multipoint сеть; • Сеть NBMA

Префикс-листы позволяют фильтровать принимаемые и анонсируемые маршруты протоколов динамической маршрутизации.

Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Списки префиксов**

Таблица 42: Параметры конфигурации протокола OSPFv2 в разделе **Маршрутизация – RIP – Списки префиксов**

Параметр конфигурации протокола OSPF	Описание
Включить	Активация префикс-листов
Имя	Задать имя префикс-листа
Номер	Номер записи в списке префиксов
Действие	• Разрешить — разрешающее действие для маршрута • Запретить — запрещающее действие для маршрута
Сеть	Задать IP-адрес сети, которая должна фильтроваться. Пример ввода - 199.0.8.0/24

Пример конфигурации протокола OSPF

Предположим, что необходимо настроить обмен маршрутной информации с соседним устройством (Маршрутизатором) при помощи протокола OSPF в рамках сетевой топологии ниже.

Важно

Для корректного получения и отправки анонсов маршрутизации необходимо предусмотреть разрешающее правило межсетевого экрана (Параметр **Протокол - OSPF**) двух направлений – **Input** и **Output**.

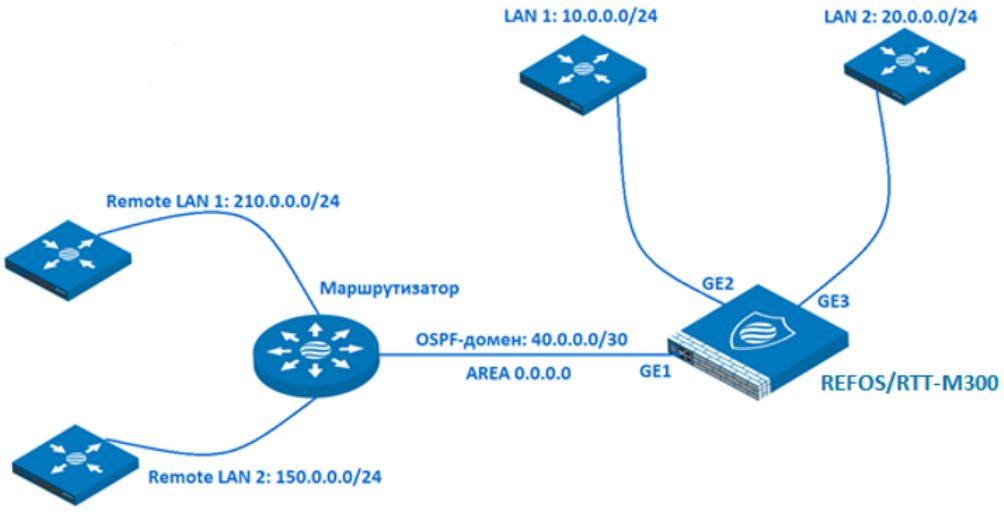


Рис. 107: Сетевая топология

Межсетевой экран RTT-M300 и Маршрутизатор имеют по три непосредственно подключенных сети (directly connected).

Пример конфигурации протокола RIP представлен на рисунках ниже.

На вкладке **Маршрутизация – OSPF - Общие настройки**:

1. Параметром **Включен** производим запуск протокола OSPF;
2. В параметре **Перераспределение маршрута** указываем маршруты, которые подлежат добавлению в обновления маршрутной информации. В данном примере – непосредственно подключенные (directly connected routes).

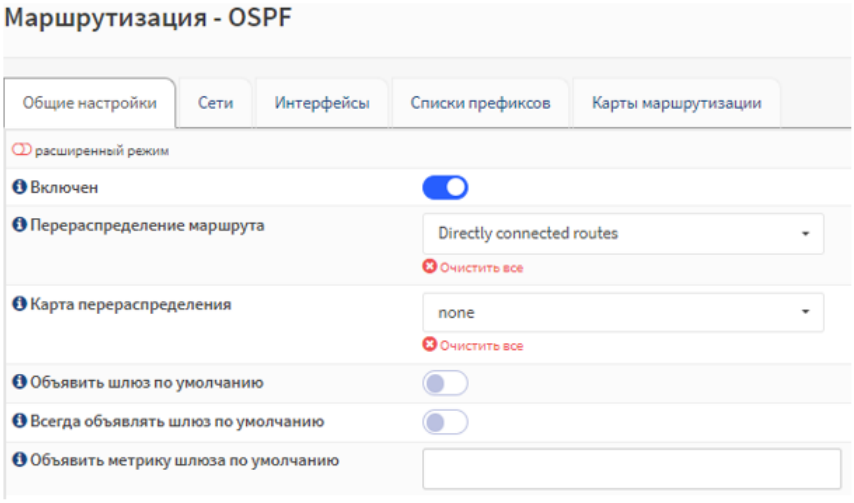


Рис. 108: Вкладка **Маршрутизация – OSPF -Общие настройки**

На вкладке **Маршрутизация – OSPF – Сети**:

1. Добавить интерфейс и запустить рассылку анонсов маршрутизации OSPF параметром **Включен**;
2. В параметре **Адрес сети** указать сеть, которая используется для обмена маршрутной информации (в рамках данного теста – 40.0.0.0);
3. В параметре **Маска сети** указать маску сети, которая относиться к параметру **Адрес сети** (в рамках данного теста – 30);
4. В параметре **Область** указать идентификатор зоны (в рамках данного теста – 0.0.0.0).

На вкладке **Маршрутизация/OSPF/Интерфейсы**:

1. Добавить интерфейс и произвести запуск аутентификации протокола OSPF параметром **Включен**;
2. В параметре **Интерфейс** указать интерфейс, который должен рассылать анонсы маршрутизации (в рамках данного теста – GE1);
3. В параметре **Тип аутентификации** указать MD5-аутентификацию;
4. В параметре **Ключ аутентификации** задать ключ MD5-аутентификации;
5. В параметре **Область** указать идентификатор зоны (в рамках данного теста – 0.0.0.0).

После сохранения конфигурации и запуска сервиса протокола OSPF, Операционная система REFOS и Маршрутизатор должны обменяться маршрутной информацией. В результате обмена маршрутной информации, каждый участник обмена (Операционная система REFOS и Маршрутизатор) должен иметь маршрутную информацию (запись в таблице маршрутизации) по сетям, которые непосредственно подключены (directly connected) к противоположному соседу. Проверить состояние сервиса и таблицу маршрутизации возможно в разделе **Маршрутизация – Диагностика – OSPF – Таблица маршрутизации**.

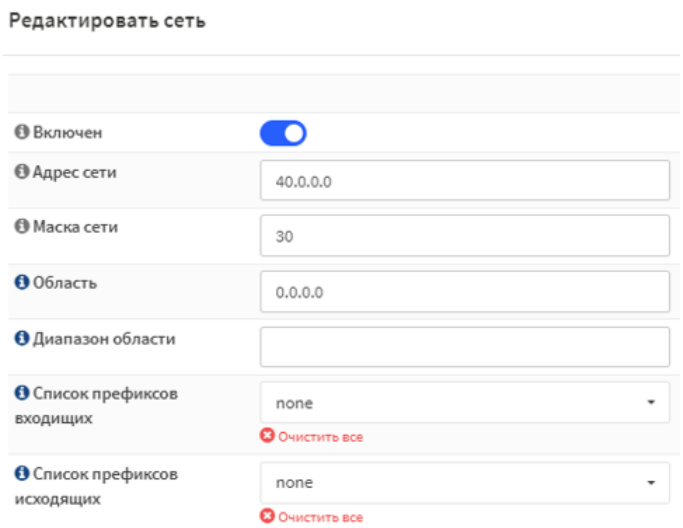


Рис. 109: Вкладка **Маршрутизация – OSPF – Сети**

Операционная система REFOS после обмена маршрутной информации получила информацию соседнего маршрутизатора о сетях, которые до обмена были ему недоступны. Общий статус маршрутов OSPF представлен на рисунке.

После сохранения конфигурации и запуска протокола OSPF, проверить статус и состояние сервиса возможно в разделе **Маршрутизация – Диагностика - OSPF**.

Протокол динамической маршрутизации BGP

BGP-протокол динамической маршрутизации, относящийся к классу протоколов маршрутизации внешнего шлюза (EGP — Exterior Gateway Protocol). Является основным протоколом маршрутизации в сетях интернет провайдеров и предназначен для обмена информацией о достижимости подсетей между автономными системами.

Важно

BGP для согласования параметров и обмена маршрутных данных использует TCP порт 179. Для корректного взаимодействия с BGP-соседом необходимо предусмотреть соответствующее разрешающее правило межсетевого экрана

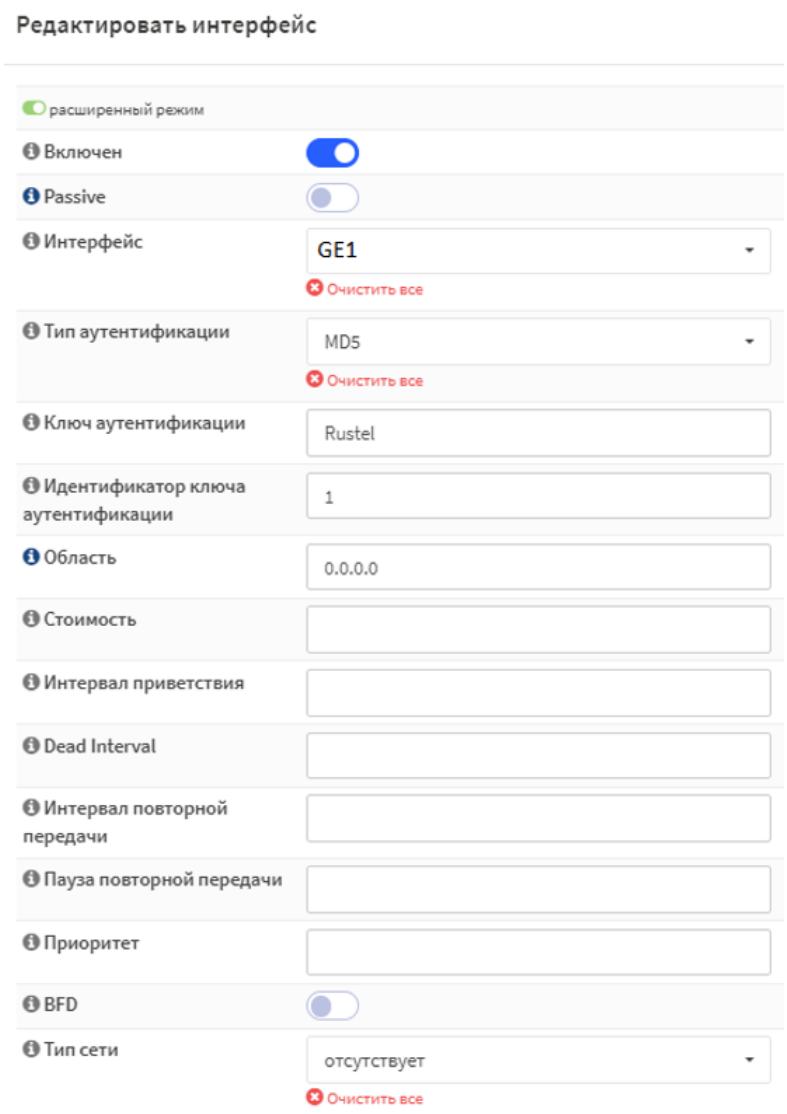


Рис. 110: Вкладка **Маршрутизация - OSPF - Интерфейсы**

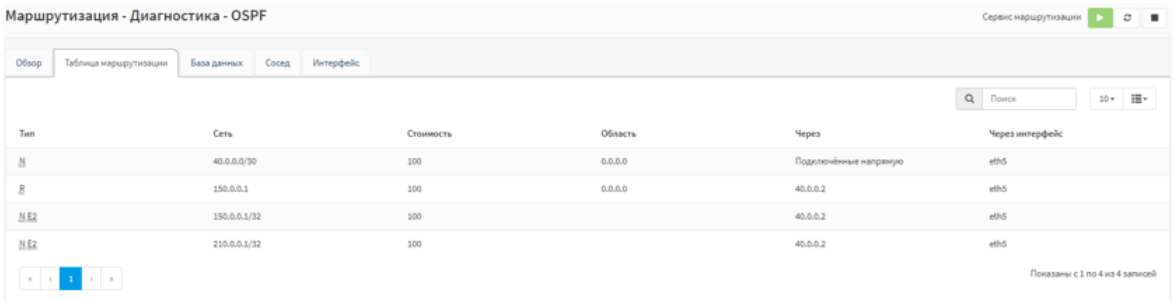


Рис. 111: Маршруты OSPF

Параметры конфигурирования протокола динамической маршрутизации BGP

Параметры конфигурации протокола BGP в разделе **Маршрутизация – BGP – Общие настройки**

Таблица 43: Параметры конфигурации протокола BGP в разделе **Маршрутизация – BGP – Общие настройки**

Параметр конфигурации протокола BGP	Описание
Включить	Активирует сервис протокола BGP
Номер AS BGP	Задать идентификатор автономной системы (AS)
ID роутера	Задать идентификатор BGP-маршрутизатора
Graceful Restart	Функция плавного перезапуска BGP. Определяет механизмы, которые позволяют узлу BGP продолжать пересылать пакеты данных по известным маршрутам, пока восстанавливается информация протокола маршрутизации
Сети	Задать подсеть, которая анонсируется BGP-соседям Пример ввода - 199.0.8.0/24
Перераспределение маршрута	Параметр, который позволяет включать в обновления маршрутизации BGP информацию о других маршрутах, которыми располагает RTT-M300: • Непосредственно подключенные сети – Directly connected routes; • Статически настроенные маршруты; • Маршруты из домена маршрутизации RIP - RIP; • Маршруты из домена маршрутизации OSPF - OSPF

Параметры конфигурирования протокола динамической маршрутизации BGP

Параметры конфигурации протокола BGP в разделе **Маршрутизация – BGP – Соседи**

Таблица 44: Параметры конфигурации протокола BGP в разделе **Маршрутизация – BGP – Соседи**

Параметр конфигурации протокола BGP	Описание
Включить	Активирует сервис протокола BGP
Описание	Задать описание
Одноранговый IP	Задать IP-адрес соседа. Пример ввода – 50.0.0.2
Удаленная AS	Задать номер автономной системы, в которой находится BGP-сосед. Установление соседства невозможно, пока соседу не назначен номер AS
Интерфейс источника обновлений	Назначить интерфейс, который будет использован в качестве исходящего при соединении с соседом
Next-Hop-Self	Включить подмену значения атрибута NEXT_HOP на локальный адрес маршрутизатора. Все обновления для соседа отправлять с указанием в качестве next-hop локального маршрутизатора
Next-Hop-Self All	
Multi-Hop	Устанавливать сеансы с соседями eBGP, которые находятся на расстоянии нескольких переходов
Route Reflector Client	Назначить BGP-соседа Route-Reflector клиентом. BGP-маршрутизатор является route-reflector-ом, если хотя бы один его сосед сконфигурирован как клиент route-reflector
BFD	Включить протокол BFD на Peer-группе
Посылать маршрут по умолчанию	Запустить рассылку маршрута по умолчанию
Enable AS-Override	Используется для замены номера AS соседа в параметре AS-PATH на свой собственный номер AS
Disable Connected Check	Разрешить пиринги между непосредственно подключенными одноранговыми узлами eBGP с использованием Loopback-адресов

Пример конфигурации протокола BGP

Предположим, что необходимо настроить обмен маршрутной информации между автономными системами, используя протокол BGP. При этом в автономной системе 64501 используется внутренний протокол маршрутизации OSPF. Поддержка распределения маршрутов в операционной системе REFOS позволяет распределять маршруты из разнопротокольных доменов маршрутизации.

Пример конфигурации протоколов представлен на рисунках

На вкладке **Маршрутизация – BGP - Общие настройки**:

1. Параметром **Включен** произвести запуск протокола BGP.
2. В поле параметра **Номер AS BGP** указать номер автономной системы.
3. В параметре **Перераспределение маршрута** указать маршруты, которые подлежат добавлению в обновления маршрутной информации. В данном примере – непосредственно подключенные (directly connected routes) и маршруты из домена маршрутизации OSPF.

На вкладке **Маршрутизация – BGP - Соседи**:

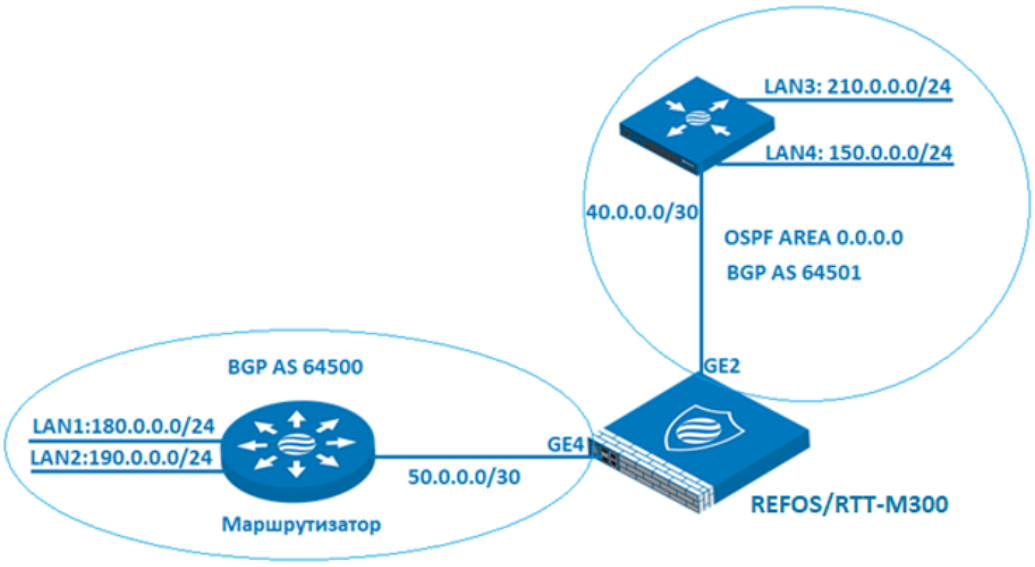


Рис. 112: Сетевая топология

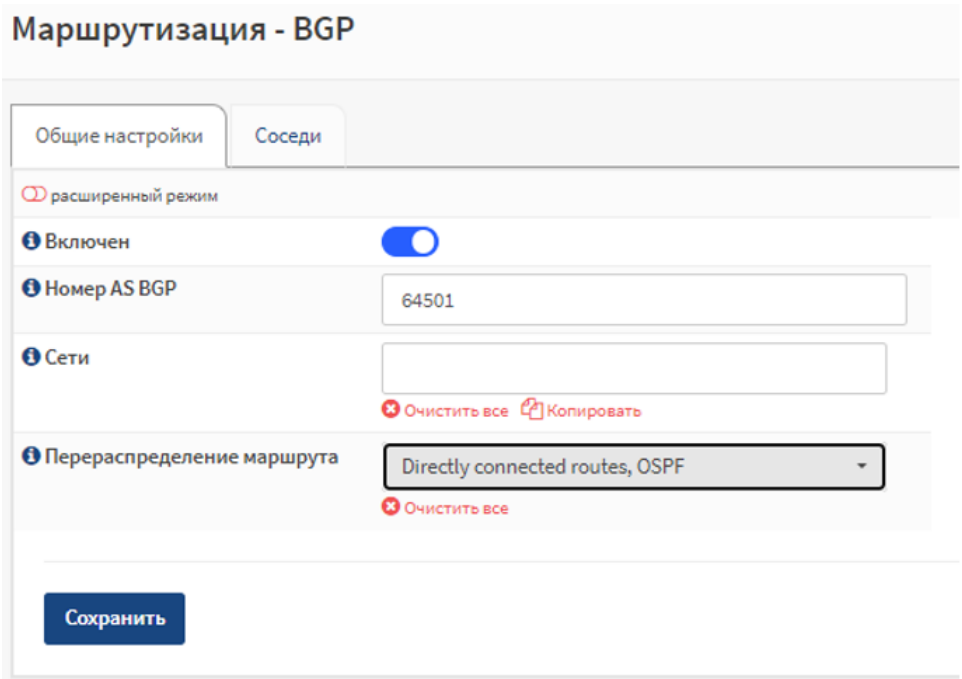


Рис. 113: Вкладка **Маршрутизация - BGP - Общие настройки**

1. Нажатием значка  создать конфигурацию подключения к BGP-соседу.
2. Параметром **Включен** применить конфигурацию.
3. Задать в поле параметра **Одноранговый IP** IP-адрес интерфейса BGP-соседа.
4. Задать в поле параметра **Удалённый AS** номер автономной системы BGP-соседа.
5. Задать в поле параметра **BGP MD5 Password** ключ для BGP-аутентификации.

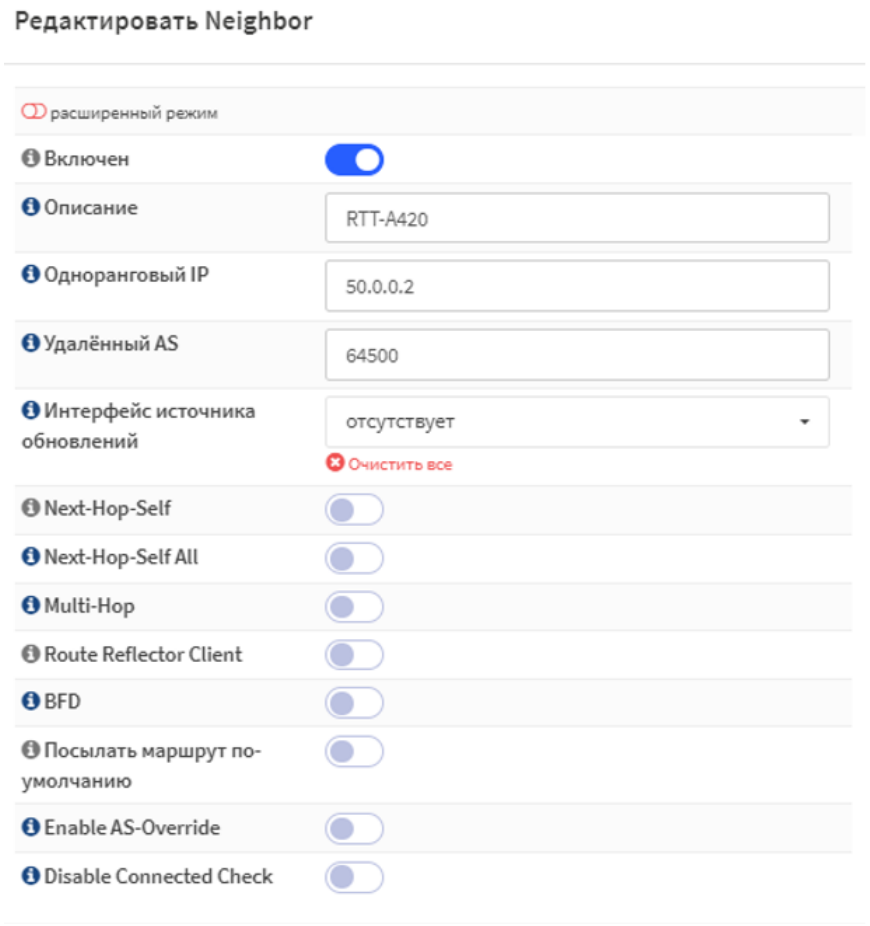
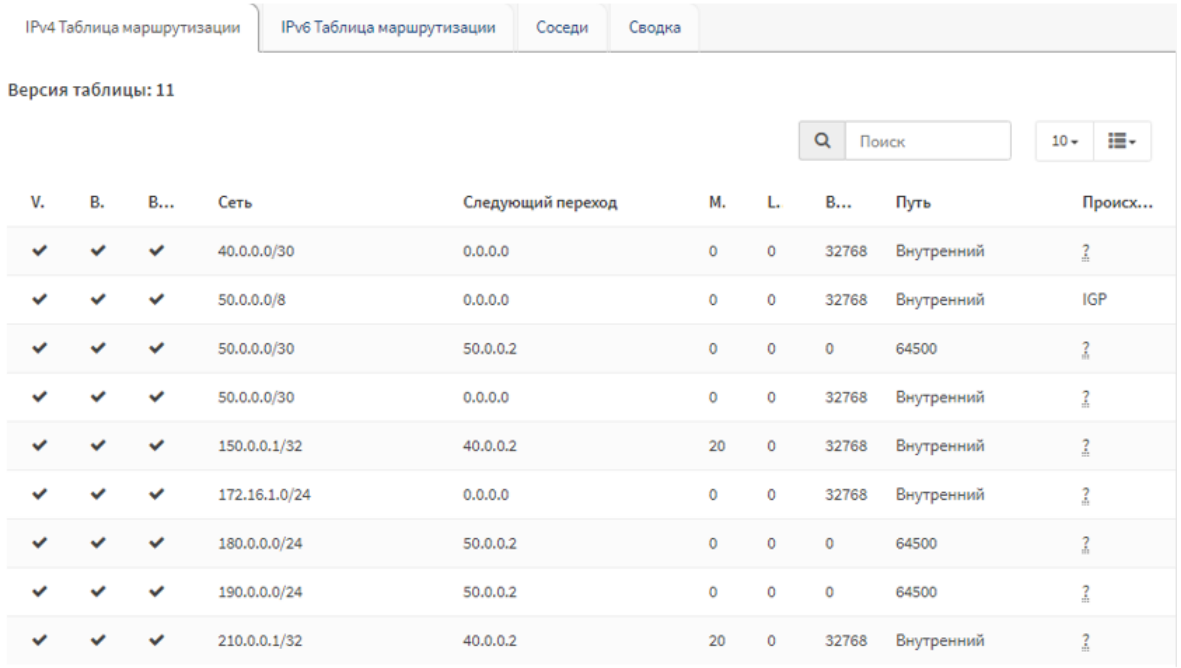


Рис. 114: Вкладка **Маршрутизация - BGP - Соседи**

После сохранения конфигурации и запуска сервиса протокола BGP, Операционная система REFOS и Маршрутизатор должны обменяться маршрутной информацией. В результате обмена маршрутной информации, каждый участник обмена (RTT-M300 и Маршрутизатор) должен иметь маршрутную информацию (запись в таблице маршрутизации). Проверить состояние сервиса и таблицу маршрутизации возможно в разделе **Маршрутизация – Диагностика – BGP**.



V.	B.	B...	Сеть	Следующий переход	M.	L.	B...	Путь	Происх...
✔	✔	✔	40.0.0.0/30	0.0.0.0	0	0	32768	Внутренний	?
✔	✔	✔	50.0.0.0/8	0.0.0.0	0	0	32768	Внутренний	IGP
✔	✔	✔	50.0.0.0/30	50.0.0.2	0	0	0	64500	?
✔	✔	✔	50.0.0.0/30	0.0.0.0	0	0	32768	Внутренний	?
✔	✔	✔	150.0.0.1/32	40.0.0.2	20	0	32768	Внутренний	?
✔	✔	✔	172.16.1.0/24	0.0.0.0	0	0	32768	Внутренний	?
✔	✔	✔	180.0.0.0/24	50.0.0.2	0	0	0	64500	?
✔	✔	✔	190.0.0.0/24	50.0.0.2	0	0	0	64500	?
✔	✔	✔	210.0.0.1/32	40.0.0.2	20	0	32768	Внутренний	?

Рис. 115: Вкладка **Ipv4 Таблица маршрутизации** в разделе **Маршрутизация - Диагностика – BGP**

Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection protocol (BFD) — протокол используется для быстрого обнаружения канальных сбоев.

Системы, работающие под управлением BFD, отправляют hello-пакеты друг другу с согласованной скоростью. Если система перестает получать hello-пакеты, сервис BFD передает данную информацию соответствующим протоколам маршрутизации. Это помогает обнаружить односторонний сбой устройства и используется для быстрой сходимости протоколов маршрутизации.

BFD может определить неисправность канала менее чем за 1 секунду.

Важно

BFD функционирует только в связке с протоколами динамической маршрутизации OSPF и BGP

Параметры конфигурирования протокола BFD

Запуск протокола BFD производится на вкладке **Общие настройки** раздела **Маршрутизация – BFD**.

На вкладке Соседи раздела **Маршрутизация – BFD** производится настройка соединения BFD-соседа (BFD-neighbor)

Таблица 45: Параметры конфигурации BFD-neighbor

Параметр конфигурации BFD-neighbor	Описание
Включить	Активирует рассылку bfd-пакетов для согласования соединения с BFD-соседом (BFD-neighbor)
Описание	Задать описание соединения
Одноранговый IP	Задать IP-адрес BFD-соседа BFD-neighbor
Passive	Установить режим работы протокола • passive — система начинает отправлять bfd-пакеты только при наличии bfd-пакетов со встречной стороны. По умолчанию система использует режим active, т.е. всегда рассылает bfd-пакеты
Интервал получения	Задать минимальный интервал приёма для обнаружения ошибки
Интервал передачи	Задать минимальный интервал передачи для обнаружения ошибки
Detect multiplier	Задать количество потерянных пакетов до разрыва сессии

Пример конфигурации протокола BFD

В рамках данного примера используется связка протокола BFD и протокола динамической маршрутизации BGP. Конфигурация BGP-процесса подробно описана в разделе **Пример конфигурации протокола BGP**. Далее рассматривается только процесс настройки протокола BFD.

1. На вкладке **Общие настройки** раздела **Маршрутизация** – **BFD** произвести запуск протокола BFD

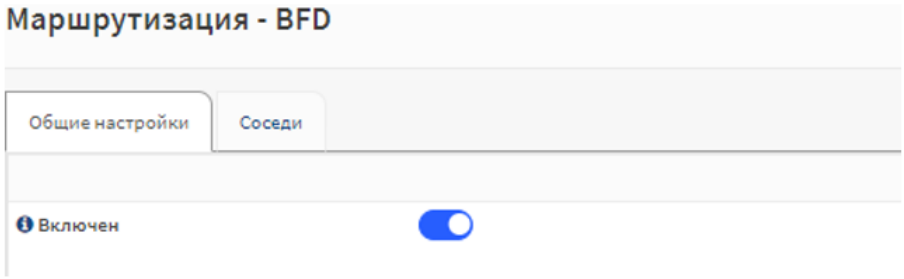


Рис. 116: Вкладка **Общие настройки** раздела **Маршрутизация** – **BFD**

2. На вкладке **Соседи** раздела **Маршрутизация** – **BFD** произвести настройку соединения BFD-соседа (BFD-neighbor)

- Активировать рассылку bfd-пакетов параметром **Включен**;
- Задать описание соединения;
- Задать IP-адрес BFD-соседа (BFD-neighbor).

Проверить состояние BFD-сервиса возможно в разделе **Маршрутизация** – **Диагностика** – **BGP**

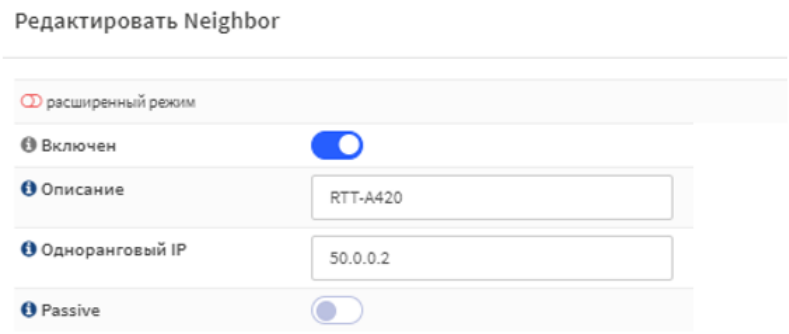


Рис. 117: Вкладка **Соседи** раздела **Маршрутизация** – **BFD**

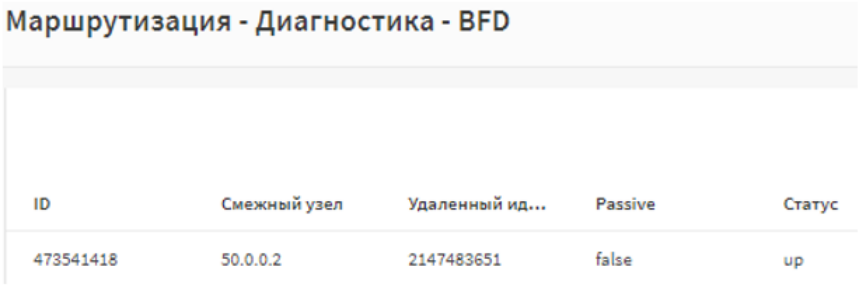


Рис. 118: Мониторинг состояния BFD-сервиса

2.6.14 DNS

2.6.14.1 Введение

ОС REFOS имеет поддержку многофункционального DNS-resolver, который выполняет роль посредника между пользовательскими устройствами и DNS серверами, что позволяет устройствам осуществлять эффективный процесс преобразования доменных имен в соответствующие IP-адреса.

Благодаря DNS-resolver возможно получать быстрый и безопасный доступ к ресурсам сети, облегчая навигацию и обмен данных для пользователей.

Основные функциональные особенности:

- Кэширование запросов для ускорения времени обработки повторных запросов;
- Проверка запросов с применением стандартов для обеспечения надежности;
- Создание авторизированных зон для переадресации или перезаписи запросов;
- Организация черного списка для блокировки определенных доменных имен;
- Предоставление защиты от перегрузки системы запросами.

2.6.14.2 Статус службы DNS

Служба имеет следующие состояния активности:

- Служба запущена  ;
- Служба остановлена  .

2.6.14.3 Процесс конфигурации и основные параметры

Конфигурация DNS-resolver производится на основных вкладках, обеспечивающих весь базовый функционал.

Вкладка **Общие настройки** представлена в таблице.

Таблица 46: Описание параметров на вкладке **Общие настройки**

Параметр	Описание
Включен	Запуск службы DNS-resolver.
Сетевые интерфейсы	Интерфейсы, которые используются для ответа на запросы пользователям.
Исходящие сетевые интерфейсы	Интерфейсы, которые используются для ответа на запросы пользователям.
Сетевые интерфейсы	Выбор сетевого интерфейса системы, который используется для приема DNS-запросов.
DNSSEC	Запуск функции DNSSEC, которая используется для защиты от атак, связанных с подменой доменного имени.
DNS64	Запуск функции DNS64, которая используется для синтеза AAAA из A записей (если актуальная AAAA запись отсутствует).
Локальная ссылка IPv6	Регистрация локальных IPv6 адресов для предотвращения недостижимого адреса при назначении нескольких интерфейсов прослушивания.
Переадресация DNS-запросов	В данном режиме все запросы будут переадресованы системному доменному серверу. Для активации режима переадресации запросов необходимо указать во вкладке **Система** -> **Настройки** -> **Общие настройки** IP адрес DNS сервера.
Тип локальной зоны	Задать тип локальной зоны для localhost. Параметр необходим для удовлетворения некоторых требований для NS и NOA записей и для обновления DNS.

Всего существует 11 типов локальных зон, описанных в таблице.

Таблица 47: Описание типов локальных зон

Параметр	Описание
transparent	Если есть совпадение с локальными данными, на запрос дается ответ. В противном случае, если запрос имеет другое имя, запрос разрешается нормально. Если запрос относится к имени, указанному в локальных данных, но такой тип данных не указан в локальных данных, то возвращается ответ noerror nodata. Если локальная зона не указана, локальные данные вызывают создание прозрачной зоны по умолчанию.
deny	Ответ блокируется, запрос сбрасывается. Если есть совпадение с локальными данными, на запрос дается ответ.
inform	На запрос отвечает нормально, так же, как transparent. IP-адрес клиента (@portnumber) печатается в файл журнала. Сообщение журнала: timestamp, unbound-pid, info: zonename inform IP@port queryname class type. Эту опцию можно использовать для нормального разрешения, но машины ищущие зараженные имена, регистрируются.
inform_deny	Запрос отбрасывается, как «deny», и регистрируется, как «inform». Т.е. найти зараженные машины, не отвечая на запросы.
nodefault	Используется для отключения содержимого по умолчанию для зон AS112. Другие типы также отключают содержимое зоны по умолчанию. Параметр «nodefault» не имеет никакого другого эффекта, кроме отключения содержимого по умолчанию для данной зоны. Используйте nodefault, если вы используете именно эту зону, если вы хотите использовать подзону, используйте transparent.
refuse	Отправить ответное сообщение об ошибке с rcode REFUSED. Если есть совпадение с локальными данными, на запрос дается ответ.
static	Если есть совпадение с локальными данными, на запрос дается ответ. В противном случае на запрос отвечает nodata или nxdomain. При отрицательном ответе SOA включается в ответ, если он представлен как локальные данные для домена вершины зоны.
typetransparent	Если есть совпадение с локальными данными, на запрос дается ответ. Если запрос для другого имени или для того же имени, но для другого типа, запрос разрешается нормально. Таким образом, аналогично прозрачному, но типы, которые не указаны в локальных данных, разрешаются нормально, поэтому, если запись A находится в локальных данных, это не вызывает ответа nodata для запросов AAAA.

продолжается на следующей странице

Таблица 47 – продолжение с предыдущей страницы

Параметр	Описание
always_refuse	Аналогично refuse, но игнорирует локальные данные и отклоняет запрос.
always_nxdomain	Аналогичен static, но игнорирует локальные данные и возвращает для запроса nxdomain.
always_transparent	Как и transparent, но игнорирует локальные данные и разрешается нормально.

Для применения конфигурации необходимо нажать на кнопку **Сохранить** с последующем подтверждением применения изменений.

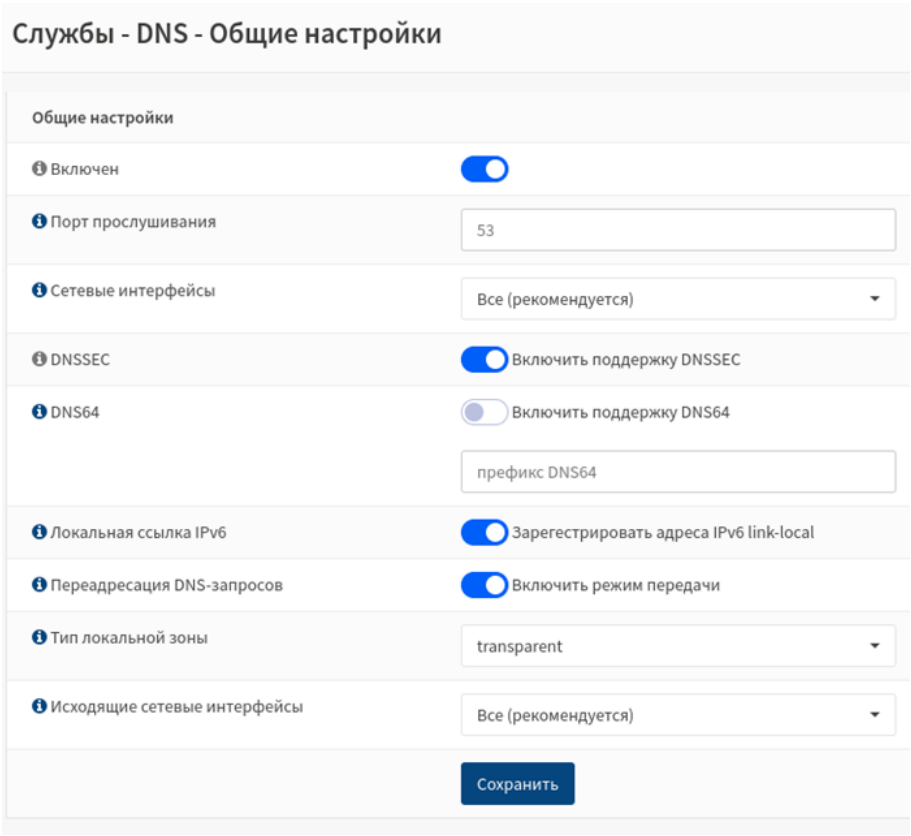


Рис. 119: Стандартная настройка DNS-resolver в режиме переадресации с включенным DNSSEC

Вкладка **Переопределение**.

В данном разделе можно задать как переопределение непосредственно для зон и клиентов, так и переопределение всего домена в целом.

Переопределение хоста при добавлении имеет параметры, указанные в таблице.

Таблица 48: Описание параметров переопределения хоста

Параметр	Описание
Тип записи	Указывается какой тип записи будет иметь переопределение, для хоста, или для зоны.
Хост / Тип зоны	В случае если в типе записи был указан хост, то здесь вписывается его имя без доменной части, например если домен хоста host1.nyc1.testrustel1234.com, то в запись идет только host1. В случае с зоной выбирается её тип
Домен	Указывается доменная часть хоста.
Тип	Тип ресурсной записи. Возможен выбор из: A или AAAA запись, почтовый MX сервер.
IP-адрес	IPv4 или IPv6 адрес хоста в случае записи для хоста и IP адрес зоны в случае для записи обслуживания зоны.
Описание	Условное описание правила переопределения.
Псевдонимы	Здесь по необходимости пользователь может указать дополнительных хостов которые будут использовать зоны, или хостов для переопределения.

На рисунке представлен пример использования переопределения хоста. В данном случае DNS-resolver обслуживает зону nyc1.testrustel1234.com с типом A и IP адресом 192.168.7.1 в transparent режиме. Также для этой зоны существуют записи для двух хостов host1 и host2.

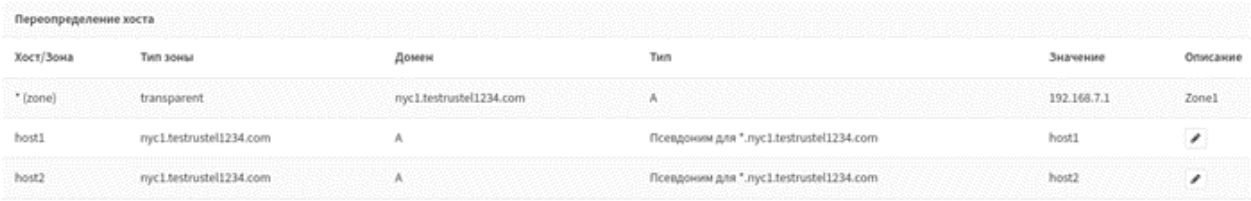


Рис. 120: Пример использования переопределения хоста

Переопределение домена указывается при помощи следующих параметров:

- Указать домен для переопределения при помощи параметра **Домен**;
- Указать IP адрес полномочного DNS сервера в параметре **IP-адрес**;
- По желанию указать название для записи в параметре **Описание**;

На рисунке представлен пример использования переопределения домена. В данном случае DNS будет отправлять запросы по домену nyc1.testrustel1234.com на IP адрес 192.168.7.1.

Рис. 121: Пример использования переопределения домена

Важно

При создании записей переопределения, для их работы убедитесь, что не включен режим переадресации запросов во вкладке **Общие настройки**.

Вкладка **Дополнительно**

Данный используется для настройки дополнительных функций управления DNS-resolver. Для стандартной работы ответчика достаточно оставить все пункты по умолчанию. Каждый пункт описан в таблице.

Таблица 49: Описание параметров переопределения хоста

Параметр	Описание
Скройте идентификационные данные Версия скрытия	Данные параметры позволяют отклонять запросы, в которых запрашивается информация об id или версии DNS сервера соответственно.
Поддержка предварительной выборки	Функция запускает предварительную выборку, что может влиять на производительность DNS-resolver при большом количестве запросов.
Поддержка Ключа DNS предварительной выборки	Используется для лучшего функционирования DNSSEC, а точнее ускорения работы этого механизма путем предварительного получения DNSKEY записей перед истечением их TTL (позволяет ускорить валидацию).
Жесткие данные DNSSEC	Функция используется для защиты от DNS-ответов, у которых удалены DNSSEC-сигнатуры. Если эта функция включена, сервер Unbound будет отклонять ответы без корректных DNSSEC-сигнатур для доменов, которые ожидается иметь DNSSEC.
Обслуживание просроченных ответов	Опция позволяет серверу продолжать отвечать на запросы из своего кэша, даже если время жизни TTL для записи истекло.
Размер кэша сообщений	Параметр задает размер кэша сообщения, отправляемого клиентам. Минимально влияет на производительность DNS-resolver.
Буфера исходящего TCP Входящие буферы TCP	Параметры, которые определяют максимальное количество одновременных TCP-соединений для исходящих и входящих запросов соответственно.
Тайм-аут компрессии	Функция отвечает за время ожидания (в миллисекундах) для запросов, которые ожидают ответа от удаленного сервера. Используется, когда сервер очень загружен запросами. Защищает от атак типа “Отказ в обслуживании.
Максимальный TTЛ для RRsets и сообщений Минимальный TTЛ для RRsets и сообщения	Функции определяют максимальное и минимальное время в секундах, в течении которого запись будет храниться в кеше после того, как она была получена.

продолжается на следующей странице

Таблица 49 – продолжение с предыдущей страницы

Параметр	Описание
TTL для записей кэша хоста	Определяется время жизни для записей в кэше хоста. Кэш хоста содержит двустороннее время прохождения пакета и информацию о поддержке EDNS.
Количество кэшируемых хостов	Функция определяет количество хостов, информация о которых будет храниться в кэше.
Пороговое значение нежелательных ответов	Параметр используется для защиты DNS сервера от потенциального DNS Amplifiers attack. Это количество нежелательных (не обязательно несуществующих) ответов, которые вызовут ограничения трафика на сокетах. Если это значение будет превышено, то ответы будут отбрасываться до тех пор, пока скорость не снизится.
Уровень детализации журнала	Возможность выбрать уровень детализации журналирования. Уровень 0 означает отсутствие многословия, только ошибки. Уровень 1 дает оперативную информацию. Уровень 2 дает подробную оперативную информацию. Уровень 3 предоставляет информацию об уровне запроса, выводимую для каждого запроса. Уровень 4 дает информацию об уровне алгоритма. Уровень 5 регистрирует идентификацию клиента для промахов кеша. По умолчанию используется уровень 1.
Расширенная статистика	При включении во вкладке **Статистические данные** появляется дополнительная статистическая информация.
Журнал запросов	При включении функции начинает выводить в журнал запросы в виде: <IP> <доменное имя> <тип> <класс>.

Вкладка **Списки доступа**

На данной вкладке присутствует возможность добавления дополнительных списков доступа помимо тех, что указываются по стандарту при указании интерфейсов во вкладке **Общие настройки**.

Для создания списка доступа необходимо:

- Задать имя списка доступа в параметре **Имя списка доступа**;
- Указать необходимое действие для сети в пункте **Действие**, описание каждого действия представлено в таблице;
- Указать Сеть(-и). Для этого указать саму сеть и необходимый CIDR в пункте **Сети**, по желанию можно добавить описание для каждой сети;
- По желанию добавить описание для списка доступа в параметре **Описание**.

Пример создания списка доступа представлен на рисунке.

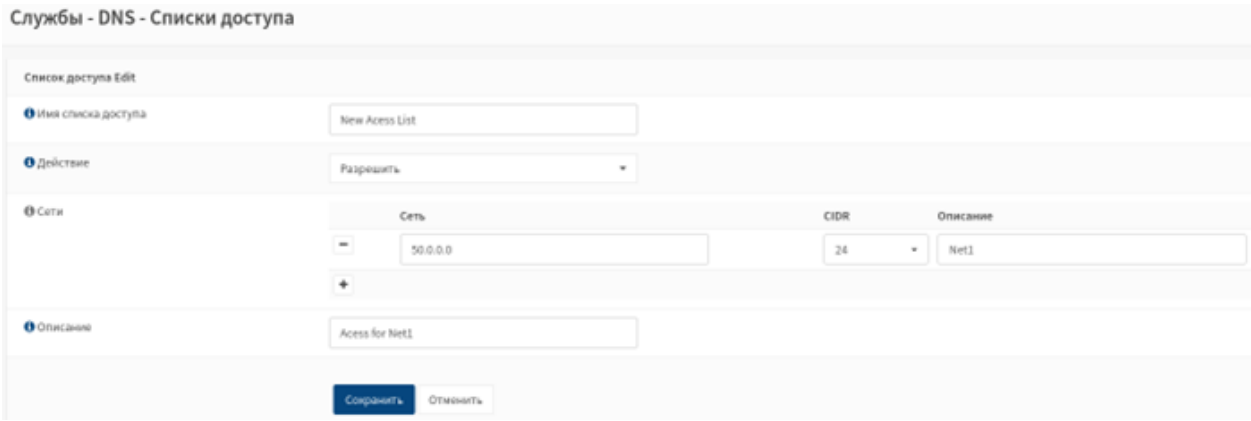


Рис. 122: Пример создания списка доступа

Таблица 50: Описание действий списка доступа

Действие	Описание
Разрешить	Действие разрешает запросы от хостов, указанных в параметре **Сети**.
Запретить	Действие запрещает запросы от хостов, указанных в параметре **Сети**.
Отклонить	Действие запрещает запросы от хостов, указанных в параметре **Сети**, но отправляет обратно клиенту сообщение об ошибке DNS rcode REFUSED.
Разрешить отслеживание	Действие разрешает рекурсивный и нерекурсивный доступ из хостов в параметре **Сети**, и используется для отслеживания кэша (в идеале должно быть настроено только для административного хоста).
Запретить Non-local	Разрешать только авторитетные запросы локальных данных от хостов в пределах, указанных в параметре **Сети**. Запрещенные сообщения удаляются.
Отказаться от Non-local	Разрешать только авторитетные запросы локальных данных от хостов в пределах, указанных в параметре **Сети**. Отправляет сообщение об ошибке DNS rcode REFUSED обратно клиенту для запрещенных сообщений.

Вкладка **Черный список**.

В данной вкладке присутствует возможность управления черными списками доменов.

Для загрузки черного списка необходимо:

- Указать желаемый тип черного списка в параметре **Тип черного списка**. **Описание** ;
- в случае необходимости загрузки собственных списков, можно нажать на кнопку **расширенный режим** в левом верхнем углу, после чего появится пункт **URL черных списков**, в котором указывается ссылка, с которой можно загрузить пользовательский черный список;

- По необходимости указать список доменов, которые будут исключены из черного списка в параметре **Белый список доменов**.

Важно

При любом действии с черным списком необходимо нажать кнопку применить и дождаться пока он загрузится. Обычно это занимает не более 1-2 минут. Если загрузка идет дольше, то необходимо перезагрузить страницу.

Если черный список был успешно загружен, тогда появится значок  .

Если черный список не был загружен, тогда появится значок восклицательного знака  , при наведении на который отобразится ошибка, связанная с загрузкой черного списка.

Пример выбора черного списка представлен на рисунке.

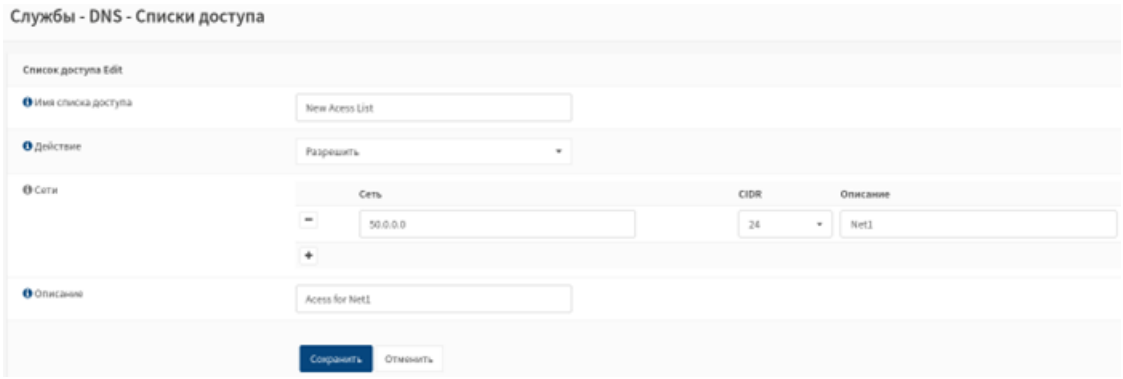


Рис. 123: Пример выбора черного списка

Вкладка **Прочее**.

На данный момент на вкладке присутствует только функция **Частные домены**, которая позволяет указать список доменов, которые не должны быть отправлены на общедоступные DNS-сервера. В основном эта функция нужна для некоторых списков DNSBL, которые разрешаются в частные адреса.

Вкладки **Статистические данные** и **Журнал**.

Данные вкладки необходимы для сбора информации о работе DNS ответчика, а также статистики по обработанным запросам.

в случае необходимости возможно отключить автоматическое обновление статистических данных. Необходимо это затем, чтобы не нагружать систему, т.к. сбор статистики (особенно с включенным параметром расширения статистики) может занимать некоторое место в памяти процессора.

Также существует возможность загрузки логов журнала и его очистки.

Пример вкладки **Статистические данные** представлен на рисунке.

Пример вкладки **Журнал** представлен на рисунке

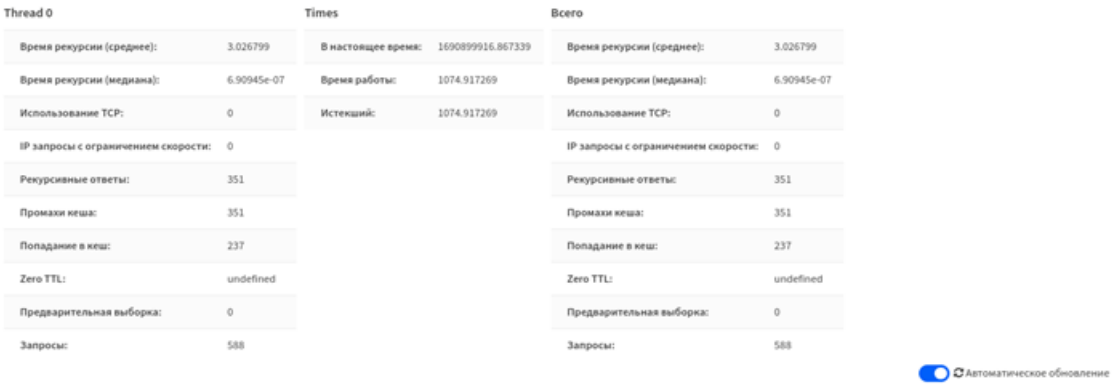


Рис. 124: Пример вкладки Статистические данные

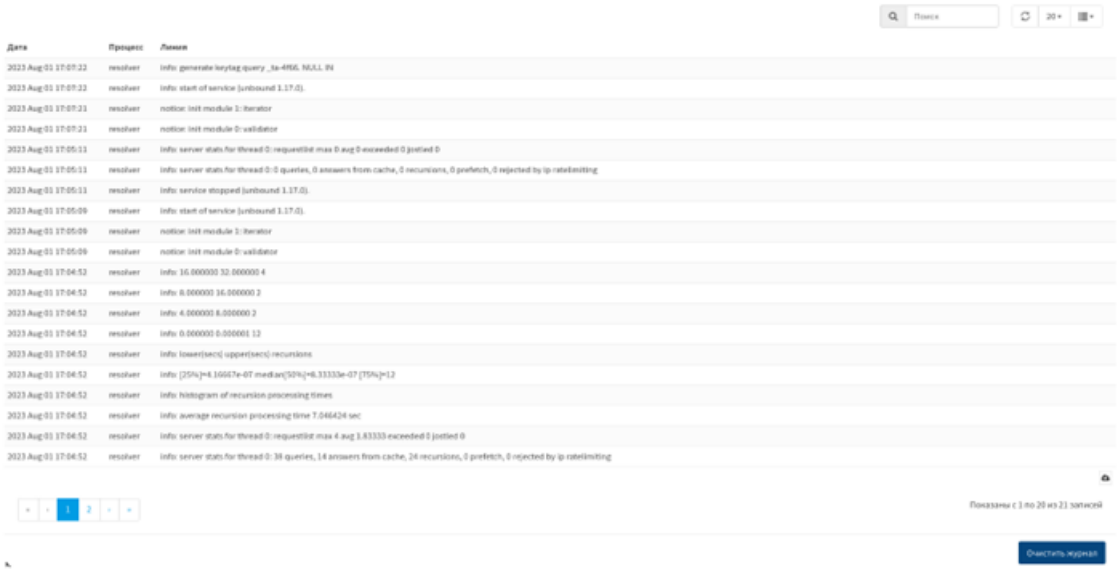


Рис. 125: Пример вкладки Журнал

2.6.15 Кластеризация

Кластеризацией называется процесс объединения нескольких экземпляров сетевых устройств (далее, нода) в одну логическую группу - кластер для обеспечения высокой доступности, масштабируемости и отказоустойчивости. Основной целью кластеризации является обеспечение непрерывного доступа к сетевым ресурсам и выполнение основных функций межсетевого экрана даже в случае сбоя одного или нескольких устройств в кластере.

2.6.15.1 Основные преимущества кластеризации

1. **Высокая доступность**: В случае сбоя одного устройства в кластере другая нода может взять на себя его задачи, что минимизирует время простоя.
2. **Масштабируемость**: Можно добавлять новые устройства в кластер по мере роста требований к производительности. Количество нод в кластере ограничено производительностью синхронизации.
3. **Отказоустойчивость**: Кластеризация позволяет защитить сеть от различных типов отказов оборудования или программного обеспечения.
4. **Балансировка нагрузки**: Трафик может равномерно распределяться между устройствами в кластере, что улучшает общую производительность сети.

2.6.15.2 Основные компоненты и механизмы кластеризации:

1. **Контроль состояния устройств в кластере**: Каждое устройство в кластере постоянно отслеживает состояние соседних нод. В случае выявления неисправности резервная нода берет на себя функции управления и обработки трафика.
2. **Синхронизация конфигурации:** Обеспечивает синхронизацию конфигурации между нодами кластера. Возможно настроить полную или частичную синхронизацию конфигурации между нодами для последующего выполнения функций межсетевого экрана при сбое одной из нод.
3. **Обмен сессиями и состояний соединений**: Для обеспечения бесперебойной работы сессий между сетевыми клиентами производится обмен состояний текущих соединений между нодами в кластере.
4. **Виртуальные IP-адреса:** В рамках кластера производится резервирование IP-адреса шлюза на внешнем и внутреннем сетевом сегменте. Для конечного клиента IP-адрес шлюза остается неизменным при сбое активной ноды в кластере.

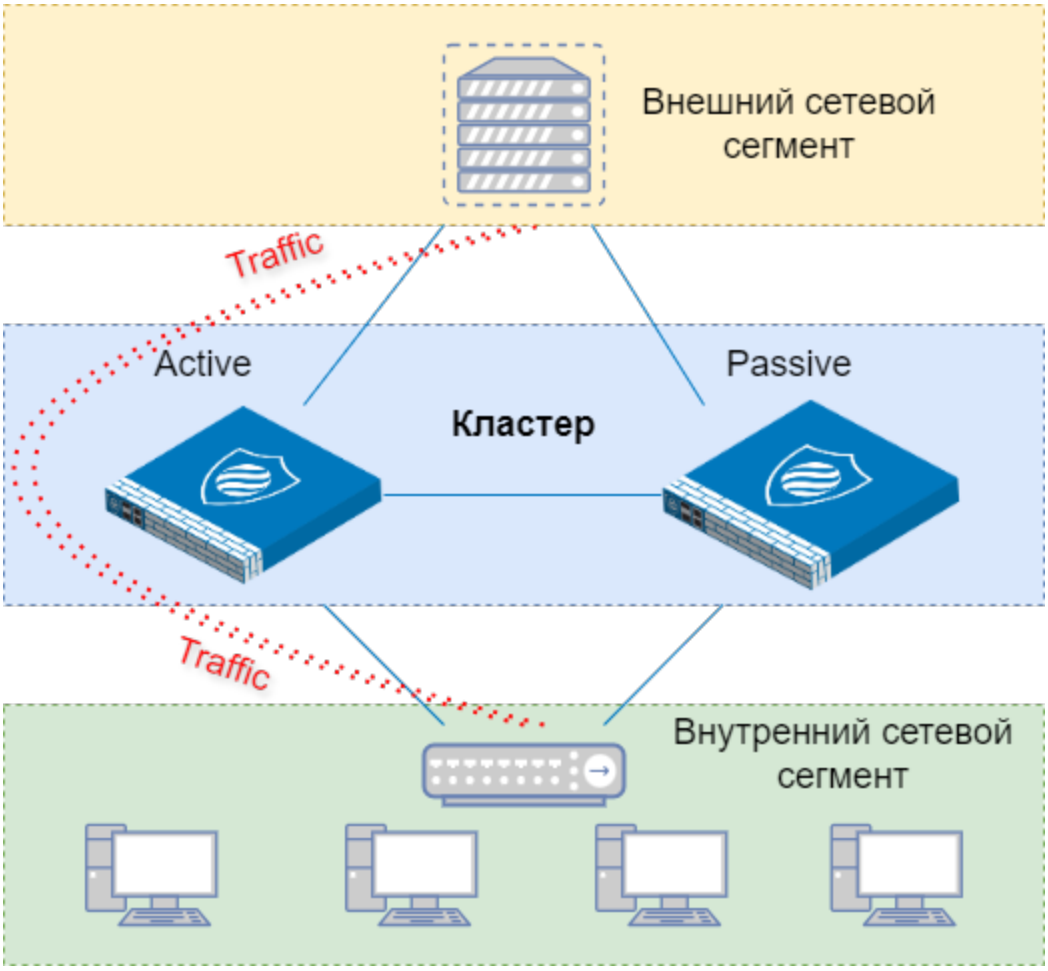
2.6.15.3 Режимы работы кластера

Существует несколько режимов работы кластера:

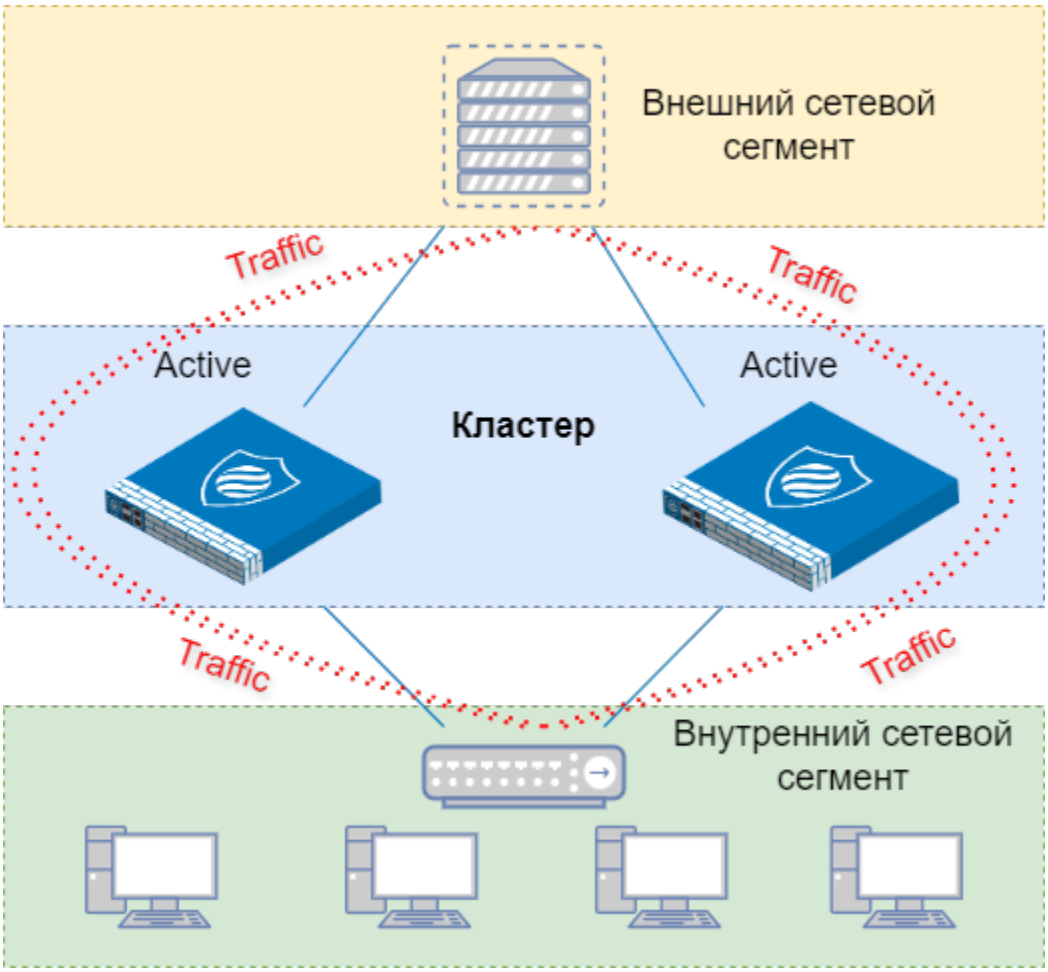
- **Active - Passive**

Ноды в кластере делятся на роли - Активная и Пассивная (Резервная). Активная нода производит обработку всего поступающего в кластер трафика, пассивная нода производит непрерывный мониторинг состояния активной ноды. При возникновении сбоя активной ноды, пассивная нода берет на себя роль и функции активной ноды. В рамках данного режима только одна нода в кластере может обрабатывать трафик.

- **Active - Active**


Внешний сетевой сегмент
Traffic
Active
Passive
Кластер
Traffic
Внутренний сетевой сегмент

Все ноды в кластере являются активными и производят обработку поступающего трафика. Нагрузка распределяется между всеми активными нодами, что позволяет максимально использовать доступные ресурсы.



2.6.15.4 Режимы балансировки трафика в кластере

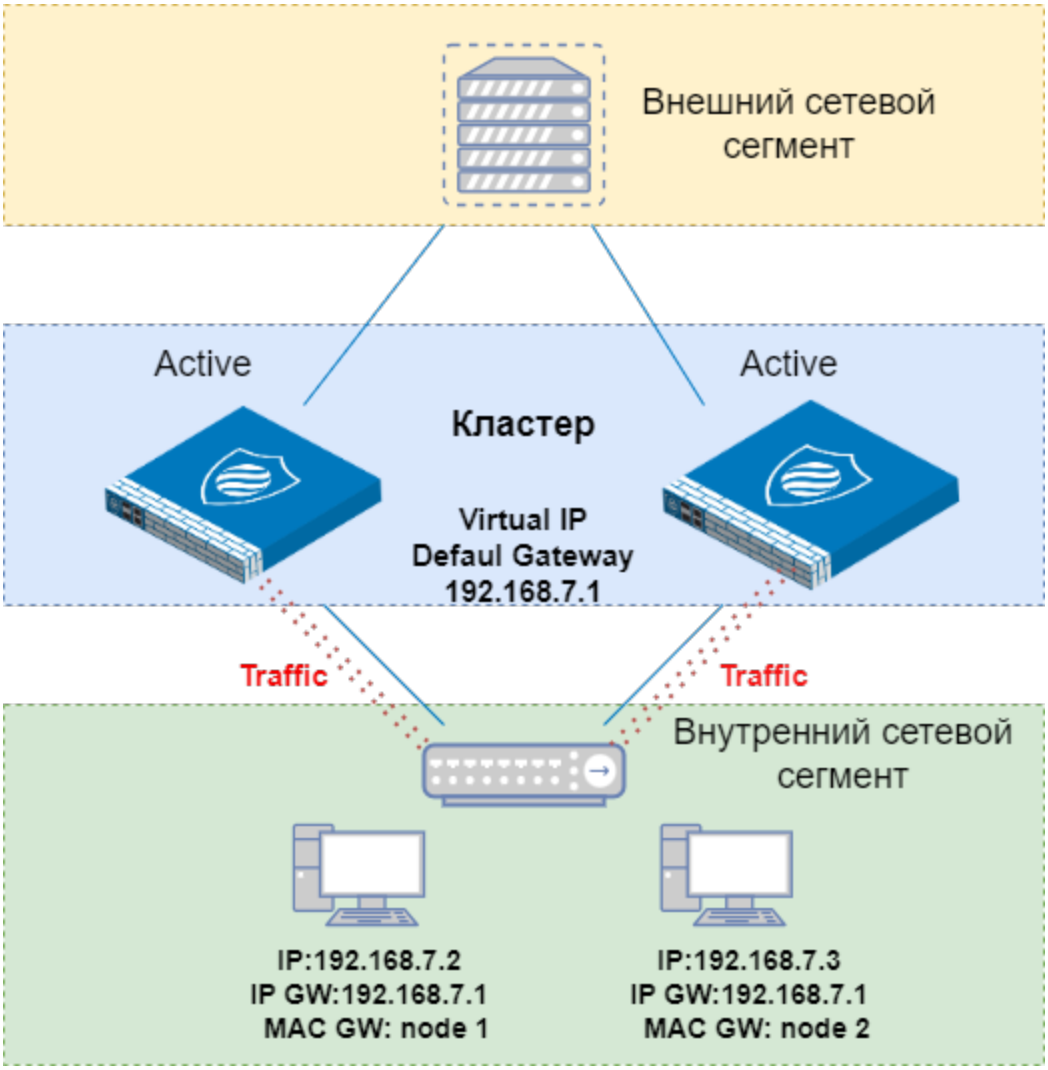
В режиме работы кластера Active - Active возможно использовать несколько подходов по распределению (балансировки) трафика в кластере:

- **ARP-балансировка;**

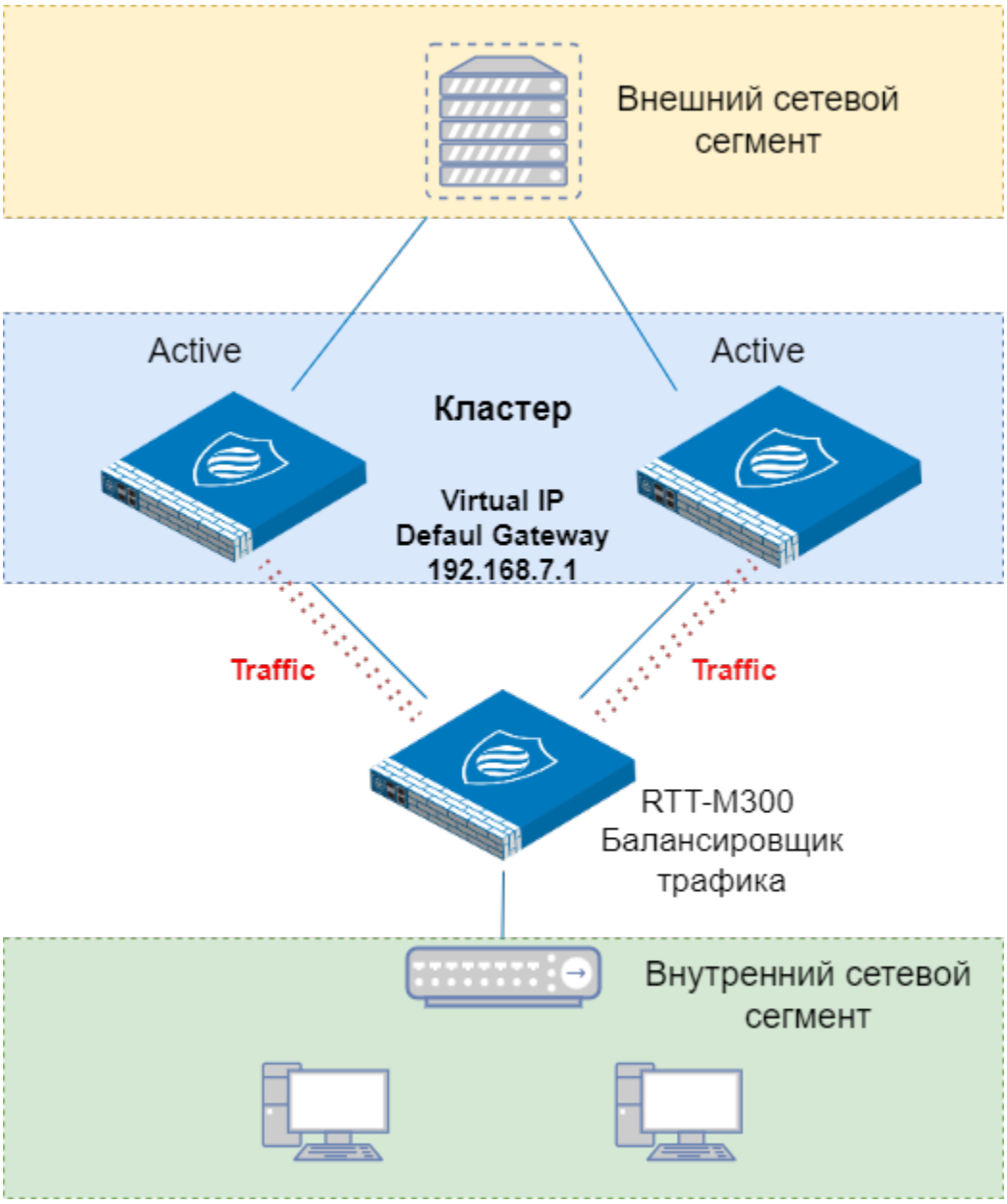
Данный подход предполагает использование распределения нагрузки по всем нодам в кластере с использованием динамического распределения MAC-адреса шлюза для каждого клиента в зависимости от его MAC-адреса. В данном случае каждый клиент во внутреннем сетевом сегменте использует один IP-адрес шлюза по умолчанию. Перед передачей трафика клиент инициирует ARP-запрос на получение актуального MAC-адреса шлюза по умолчанию. Основная нода в свою очередь, анализируя MAC-адрес клиента предоставляет MAC-адрес интерфейса основной или соседней ноды.

- **Балансировщик трафика;**

Данный подход предполагает использование дополнительного экземпляра устройства RTT-M300 для распределения трафика по всем нодам в кластере. В данном случае отдельный балансировщик берет на себя все процессы распределения трафика, ноды в кластере только производят обработку поступающего трафика. Балансировщик использует следующие механизмы распределения трафика:


Внешний сетевой сегмент
Active
Active
Кластер
Virtual IP
Defaul Gateway
192.168.7.1
Traffic
Traffic
Внутренний сетевой сегмент
IP:192.168.7.2
IP GW:192.168.7.1
MAC GW: node 1
IP:192.168.7.3
IP GW:192.168.7.1
MAC GW: node 2

1. **Циклический** - пакеты распределяются равномерно в порядке очереди между всеми нодами в кластере;
2. **Весовой коэффициент** - для каждой ноды возможно задать процентное соотношение от общего объема распределяемого трафика. Например, первая нода обрабатывает 60% всего перераспределяемого трафика, вторая нода только 40%.
3. **JHash** - для распределения трафика используются значения IP-адреса и номера порта отправителя.



2.6.15.5 Описание параметров конфигурации кластера

Конфигурация кластера производится в разделе **Кластеризация - Настройки - Cluster**.

Описание параметров кластеризации представлены в таблице:

Параметр	Описание параметра
Включен	Активация функции кластеризации
Список нод в кластере	Список доменных имен или IP-адресов интерфейсов синхронизации нод кластера, которые будут использоваться для синхронизации конфигурации.
Mode cluster	Режим работы кластера: **Active/Passive** , **Active / Active**.
Интерфейс внутренней сети	Сетевой интерфейс ноды, который будет использоваться для виртуального адреса (Virtual IP) внутренней сети кластера.
Интерфейс внешней сети	Сетевой интерфейс ноды, который будет использоваться для виртуального адреса (Virtual IP) внешней сети кластера.
Интерфейс синхронизации (В режиме Active/Passive)	Сетевой интерфейс синхронизации сессий между нодами кластера.
Приоритет (В режиме Active/Passive)	Приоритет ноды в кластере. Возможный диапазон значений от 1 до 100. Узел с наибольшим приоритетом берет роль MASTER.
Интервал оповещения (В режиме Active/Passive)	Интервал оповещений ноды с ролью MASTER в секундах. Если при истечении данного интервала MASTER не оповестит другие ноды, в кластере будут производится выборы нового MASTER.
Виртуальный IP-адрес внутренней сети	Виртуальный IP-адрес шлюза (Virtual IP) во внутренней сети кластера.
Виртуальный IP-адрес внешней сети	Виртуальный IP-адрес шлюза (Virtual IP) во внешней сети кластера.
Групповой IP-адрес синхронизации сетевых сессий кластера (В режиме Active/Passive)	Групповой IP-адрес синхронизации сессий. По умолчанию используется **225.0.0.50**.
Пароль аутентификации (В режиме Active/Passive)	Пароль аутентификации нод в кластере.
Список синхронизируемых настроек	Разделы конфигурации, которые будут синхронизироваться между нодами. Описание списка конфигураций представлен в таблице **Список синхронизируемых настроек**.
Длина ключа	Интерфейсы синхронизации использует шифрованное SSL-соединение между нодами. Для организации данного SSL-соединения генерируется сертификат с заданной длинной ключа. По умолчанию используется значение **1024** бита.
Load balancing mode (В режиме Active/Active)	Активировать режим ARP-балансировки.
Priority for load balancing (В режиме Load balancing mode)	Укажите приоритет ноды для ARP балансировки. Возможный диапазон значений от 0 до 255. Нода с меньшим значением первая ответит на ARP-запрос.

Важно

- Длина ключа задается один раз при первоначальной конфигурации кластера. В последующем данный параметр будет не доступен для конфигурирования. Не желательно менять значение

заданного параметра по умолчанию;

- Запрещена смена доменного имени ноды после создания кластера;
- В режиме Active/Active важно, чтобы в параметре “Список нод в кластере” были указаны исключительно внутренние IP адреса устройств в кластере;
- В режиме active/active с использованием балансировщика используется два уникальных виртуальных IP (Virtual IP) для каждой внешней и внутренней сети.

Описание параметров конфигурации балансировщика трафика

Конфигурация балансировщика трафика производится в разделе **Кластеризация - Настройки - Load balancing**.

Описание параметров балансировщика трафика представлены в таблице ниже:

Параметр	Описание параметра
Включен	Активация функции кластеризации
Список нод в кластере	Список доменных имен или IP-адресов интерфейсов синхронизации нод кластера, которые будут использоваться для синхронизации конфигурации.
Mode cluster	Режим работы кластера: **Active/Passive** , **Active / Active**.
Интерфейс внутренней сети	Сетевой интерфейс ноды, который будет использоваться для виртуального адреса (Virtual IP) внутренней сети кластера.
Интерфейс внешней сети	Сетевой интерфейс ноды, который будет использоваться для виртуального адреса (Virtual IP) внешней сети кластера.
Интерфейс синхронизации (В режиме Active/Passive)	Сетевой интерфейс синхронизации сессий между нодами кластера.
Приоритет (В режиме Active/Passive)	Приоритет ноды в кластере. Возможный диапазон значений от 1 до 100. Узел с наибольшим приоритетом берет роль MASTER.
Интервал оповещения (В режиме Active/Passive)	Интервал оповещений ноды с ролью MASTER в секундах. Если при истечении данного интервала MASTER не оповестит другие ноды, в кластере будут производится выборы нового MASTER.
Виртуальный IP-адрес внутренней сети	Виртуальный IP-адрес шлюза (Virtual IP) во внутренней сети кластера.
Виртуальный IP-адрес внешней сети	Виртуальный IP-адрес шлюза (Virtual IP) во внешней сети кластера.
Групповой IP-адрес синхронизации сетевых сессий кластера (В режиме Active/Passive)	Групповой IP-адрес синхронизации сессий. По умолчанию используется **225.0.0.50**.
Пароль аутентификации (В режиме Active/Passive)	Пароль аутентификации нод в кластере.
Список синхронизируемых настроек	Разделы конфигурации, которые будут синхронизироваться между нодами. Описание списка конфигураций представлен в таблице **Список синхронизируемых настроек**
Длина ключа	Интерфейсы синхронизации использует шифрованное SSL-соединение между нодами. Для организации данного SSL-соединения генерируется сертификат с заданной длинной ключа. По умолчанию используется значение **1024** бита.
Load balancing mode (В режиме Active/Active)	Активировать режим ARP-балансировки.

продолжается на следующей странице

Таблица 51 – продолжение с предыдущей страницы

Параметр	Описание параметра
Priority for load balancing (В режиме Load balancing mode)	Укажите приоритет ноды для ARP балансировки. Возможный диапазон значений от 0 до 255. Нода с меньшим значением первая ответит на ARP-запрос.

Важно

- Механизм балансировки JHash производит обработку только TCP-трафика. Весь остальной трафик (например, UDP или ICMP) балансировщик игнорирует.
- Весь поступающий трафик на Интерфейс внутренней сети балансировщик перенаправляет на Интерфейс внешней сети, т.е. балансировщик может не иметь маршрут до удаленной сети перенаправляемого пакета.

2.6.15.6 Описание списка синхронизируемых настроек разделов конфигурации

ОС REFOS позволяет гибко настраивать частичную синхронизацию конфигурации между нодами. Администратор имеет возможность указать только те разделы конфигурации, которые необходимо синхронизировать с другой нодой.

Конфигурация	Описание
System - Access	Перенос конфигурации раздела **Система - Доступ**
Система - Шлюзы	Перенос конфигурации раздела **Система - Шлюзы**
System - Routes	Перенос конфигурации раздела **Система - Маршруты**
Система - Настройки - Администрирование	Перенос конфигурации раздела **Система - Настройки - Администрирование**
System - Settings - General	Перенос конфигурации раздела **Система - Настройки - Общие настройки**
System - Settings - Logging	Перенос конфигурации раздела **Система - Настройки - Журналирование**
System - Settings - Logging/Goals	Перенос конфигурации раздела **Система - Настройки - Экспорт журналов**
System - Manager certificates	Перенос конфигурации раздела **Система - Менеджер сертификатов**
Интерфейсы	Перенос конфигурации раздела **Интерфейсы**
Межсетевой экран - Псевдонимы	Перенос конфигурации раздела **Межсетевой экран - Псевдонимы**
Межсетевой экран - Группы	Перенос конфигурации раздела **Межсетевой экран - Группы**
Firewall - NAT	Перенос конфигурации раздела **Межсетевой экран - NAT**
Firewall - Filter	Перенос конфигурации раздела **Межсетевой экран - Правила фильтрации**
Firewall - Settings	Перенос конфигурации раздела **Межсетевой экран - Настройки**
Маршрутизация	Перенос конфигурации раздела **Маршрутизация**
Сервисы - Обнаружение вторжений	Перенос конфигурации раздела **Службы - Обнаружение вторжений**
Services - Monitoring services	Перенос конфигурации раздела **Службы - Мониторинг служб**
Services - Network Time	Перенос конфигурации раздела **Службы - Сетевое время**
Services - DNS	Перенос конфигурации раздела **Службы - DNS**
Сервисы - Прокси	Перенос конфигурации раздела **Службы - Веб-прокси**
Services - DHCP	Перенос конфигурации раздела **Службы - DHCPv4**

Важно

В некоторых случаях, когда конфигурация не переносится / не перенеслась полностью необходимо повторное применение конфигурации в вкладке **Кластеризация - Настройки - Cluster**.

Важно

Не рекомендуется осуществлять перенос настройки интерфейсов для предотвращения повреждения топологии сети.

Примечание

В режиме active/passive на активной ноде по умолчанию запущена служба DHCP, на пассивной ноде служба DHCP не активна.

2.6.15.7 Мониторинг состояния нод в кластере

ОС REFOS позволяет производить мониторинг состояния ноды и назначенной ей роли в кластере. В разделе **Кластеризация - Статус** фиксируются основные параметры состояния нод в кластере.

Параметр	Описание параметра
Состояние	Состояние службы кластеризации: • **Running** – служба кластеризации на ноде запущена; • **Stopped** - служба кластеризации остановлена; • **Disable** - служба кластеризации на ноде отключена;
Роль ноды	Роль ноды в кластере: • **UNDEFINED** - роль в кластере не назначена. Используется при отключенной службе кластеризации. • **MASTER** - активная нода, которая участвует в обработке трафика; • **BACKUP** - пассивная нода, которая производит мониторинг активной ноды и в случае сбоя активной берет на себя роль MASTER;
Количество синхронизаций между нодами	Счетчик количества синхронизаций конфигурации между нодами.

2.6.15.8 Журналы и основные события

ОС REFOS производит регистрацию событий функционирования службы кластеризации. В разделе **Кластеризация - Журнал** представлен журнал с основными событиями.

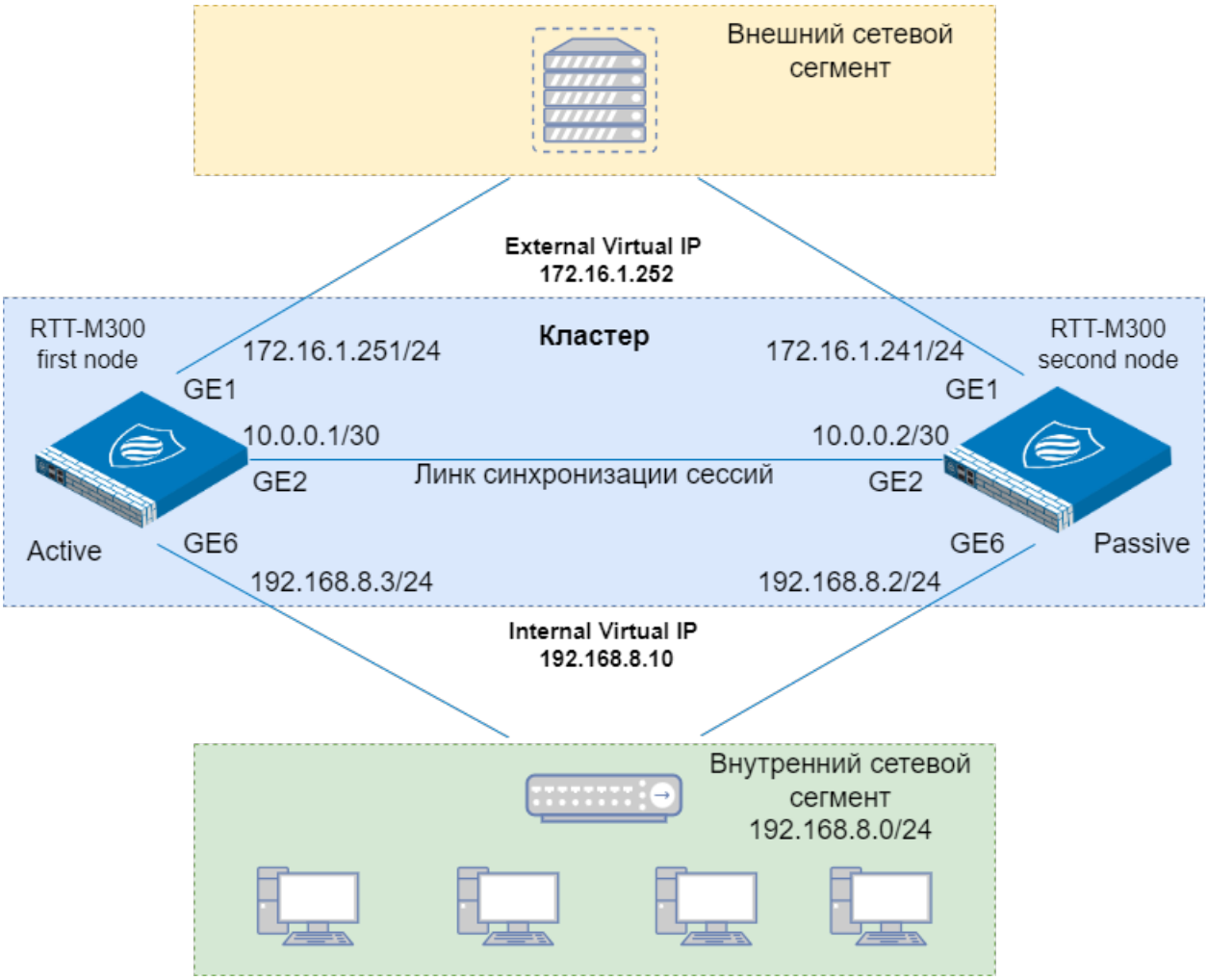
События делятся на два типа: - INFO - информация о состоянии и функционировании службы кластеризации; - ERROR - ошибки и замечания в работе кластеризации;

Событие в журнале	Описание
[INFO]: Synchronization finished without errors	Синхронизация конфигурации завершена без ошибок
[INFO]: HA started	Служба кластеризации запущена
[INFO]: HA stopped	Служба кластеризации остановлена
[INFO]: Load balancing active	Функция балансировки нагрузки включена
[INFO]: Load balancing inactive	Функция балансировки нагрузки выключена
[INFO]: Config synchronized	Конфигурация устройств синхронизирована
[INFO]: Entering BACKUP STATE	Переход устройства в режим BACKUP
[INFO]: Started dhcpv4	Запуск dhcp сервера
[INFO]: The platform and version firmware in cluster equal	Версия служб и ПО устройств в кластере совпадают.
[ERROR]: LB: 192.168.8.1 not available	Устройство с ip 192.168.8.1 недоступно для балансировки.
[ERROR]: Synchronization finished with 1 errors.	Синхронизация завершена с 1 ошибкой.
[ERROR]: LB: Cluster nodes are not available!	Кластер недоступен для балансировки.

2.6.15.9 Пример конфигурации кластера

Пример конфигурации кластера в режиме Active/Passive

Предположим, что необходимо настроить кластер из двух нод в режиме Active/Passive в рамках сетевой топологии ниже.



В рамках данного примера предполагается, что активная нода с ролью MASTER берет на себя обработку трафика, а пассивная нода с ролью BACKUP мониторит состояние активной ноды. Используя линк синхронизации между нодами, производится перенос сессий (таблица состояния соединений) с активной ноды на пассивную. Виртуальные интерфейсы позволяют резервировать шлюз по умолчанию. Также в рамках кластера производится перенос конфигурации с активной ноды на пассивную.

Важно

Для исключения возможных ошибок применения конфигурации и исправной работы кластера рекомендуется использование одинаковых физических интерфейсов в топологии кластера.

Пример конфигурации активной ноды представлен ниже.

В разделе **Кластеризация - Настройки - Cluster** произвести конфигурацию активной ноды, используя следующие параметры:

Параметр	Описание/Значение параметра
Включен	Произвести запуск функции кластеризации.
Список нод в кластере	Указать для каждой ноды IP-адреса интерфейсов синхронизации конфигурации - **10.0.0.1 , 10.0.0.2**.
Mode cluster	Задать режим работы кластера - **Active** / **Passive**.
Интерфейс внутренней сети	Указать сетевой интерфейс ноды, который будет использоваться виртуальным IP-адресом внутренней сети (Internal Virtual IP) - **GE6**.
Интерфейс внешней сети	Указать сетевой интерфейс ноды, который будет использоваться виртуальным IP-адресом внешней сети (External Virtual IP) - **GE1**.
Интерфейс синхронизации	Указать сетевой интерфейс синхронизации сессий - **GE2**.
Приоритет	Задать приоритет ноды в кластере - **1**.
Интервал оповещения	Задать интервал оповещения ноды - **1**.
Виртуальный IP-адрес внутренней сети	Задать виртуальный IP-адрес внутренней сети - **192.168.8.10**.
Виртуальный IP-адрес внешней сети	Задать виртуальный IP-адрес внешней сети - **172.16.1.252**.
Групповой IP-адрес синхронизации сетевых сессий кластера	Задать групповой IP-адрес синхронизации - **225.0.0.50**.
Пароль аутентификации	Задать уникальный пароль аутентификации нод в кластере.
Список синхронизируемых настроек	Выбрать из списка синхронизируемые части конфигурации текущей ноды.

Пассивная нода имеет аналогичную конфигурацию, исключением является параметр Приоритет, значение которого равно 2.

Для проверки работоспособности кластера необходимо проверить состояние нод в кластере. В разделе **Кластеризация - Статус** фиксируется состояние, роль ноды, количество синхронизаций. Состояние running и правильное назначение роли ноде (в соответствии с приоритетом) является показателем корректного функционирования кластера.

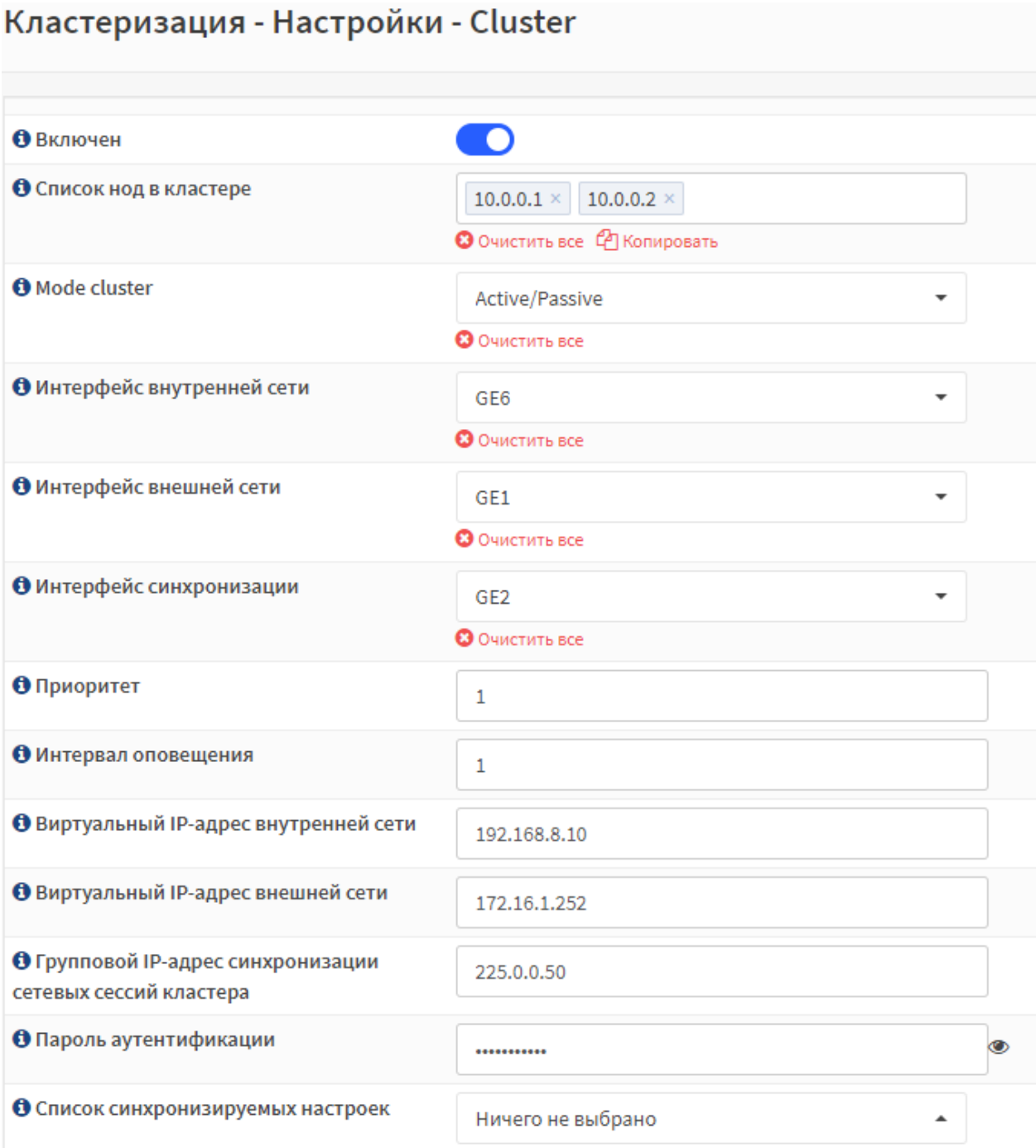
Статус активной ноды в разделе **Кластеризация - Статус**.

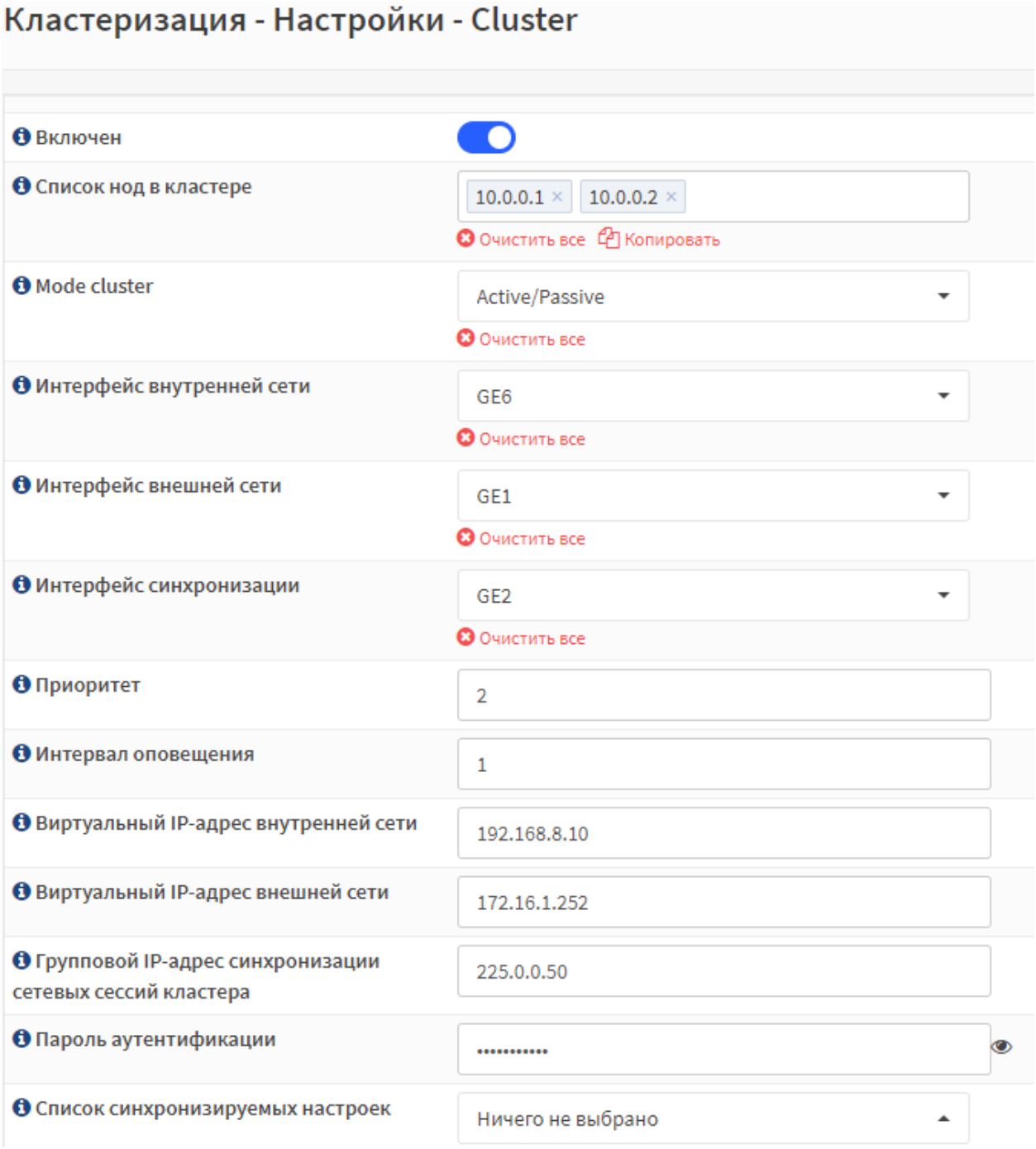
Статус пассивной ноды в разделе **Кластеризация - Статус**.

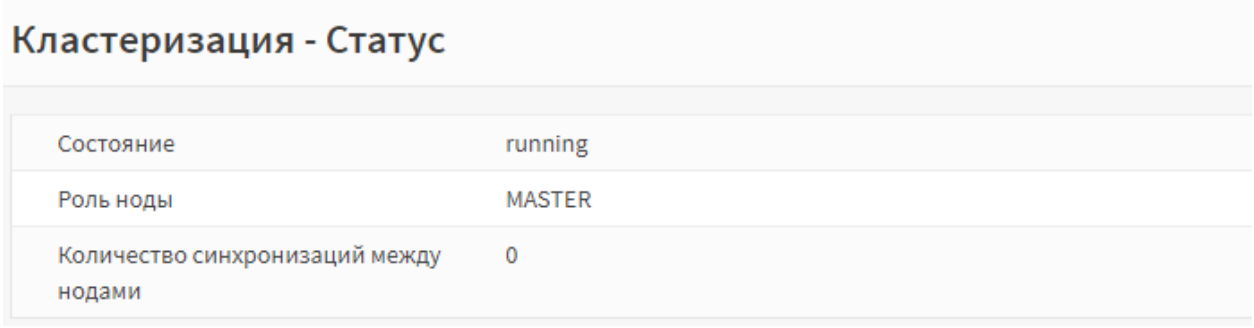
После проверки работоспособности кластера можно выбрать необходимые для переноса на резервную ноду списки конфигурации. В случае неисправности ноды с ролью MASTER (MASTER перестанет обмениваться сообщениями с резервной нодой) - резервная нода возьмет на себя роль MASTER и все его функции.

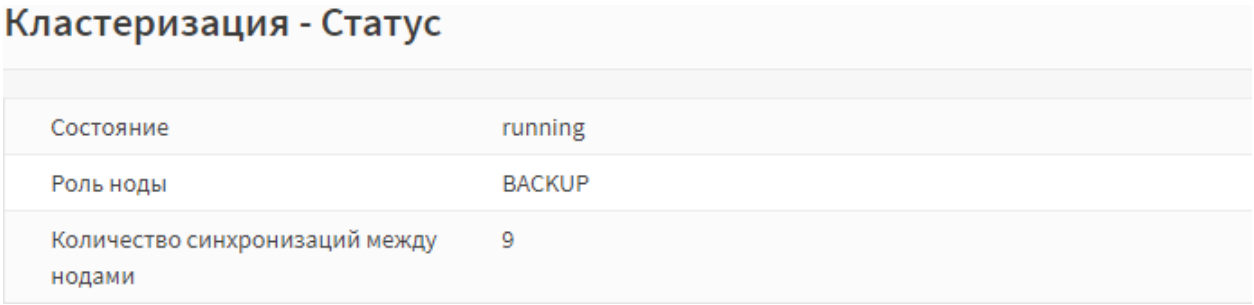
Примечание

В режиме active/passive после возобновления работы, MASTER автоматически возвращает себе статус основной ноды.


Кластеризация - Настройки - Cluster
Включен
Список нод в кластере
10.0.0.1
10.0.0.2
Очистить все
Копировать
Mode cluster
Active/Passive
Очистить все
Интерфейс внутренней сети
GE6
Очистить все
Интерфейс внешней сети
GE1
Очистить все
Интерфейс синхронизации
GE2
Очистить все
Приоритет
1
Интервал оповещения
1
Виртуальный IP-адрес внутренней сети
192.168.8.10
Виртуальный IP-адрес внешней сети
172.16.1.252
Групповой IP-адрес синхронизации сетевых сессий кластера
225.0.0.50
Пароль аутентификации
Список синхронизируемых настроек
Ничего не выбрано


Кластеризация - Настройки - Cluster
Включен
Список нод в кластере
10.0.0.1
10.0.0.2
Очистить все
Копировать
Mode cluster
Active/Passive
Очистить все
Интерфейс внутренней сети
GE6
Очистить все
Интерфейс внешней сети
GE1
Очистить все
Интерфейс синхронизации
GE2
Очистить все
Приоритет
2
Интервал оповещения
1
Виртуальный IP-адрес внутренней сети
192.168.8.10
Виртуальный IP-адрес внешней сети
172.16.1.252
Групповой IP-адрес синхронизации сетевых сессий кластера
225.0.0.50
Пароль аутентификации
Список синхронизируемых настроек
Ничего не выбрано





Пример конфигурации кластера в режиме Active/Active с ARP-балансировкой

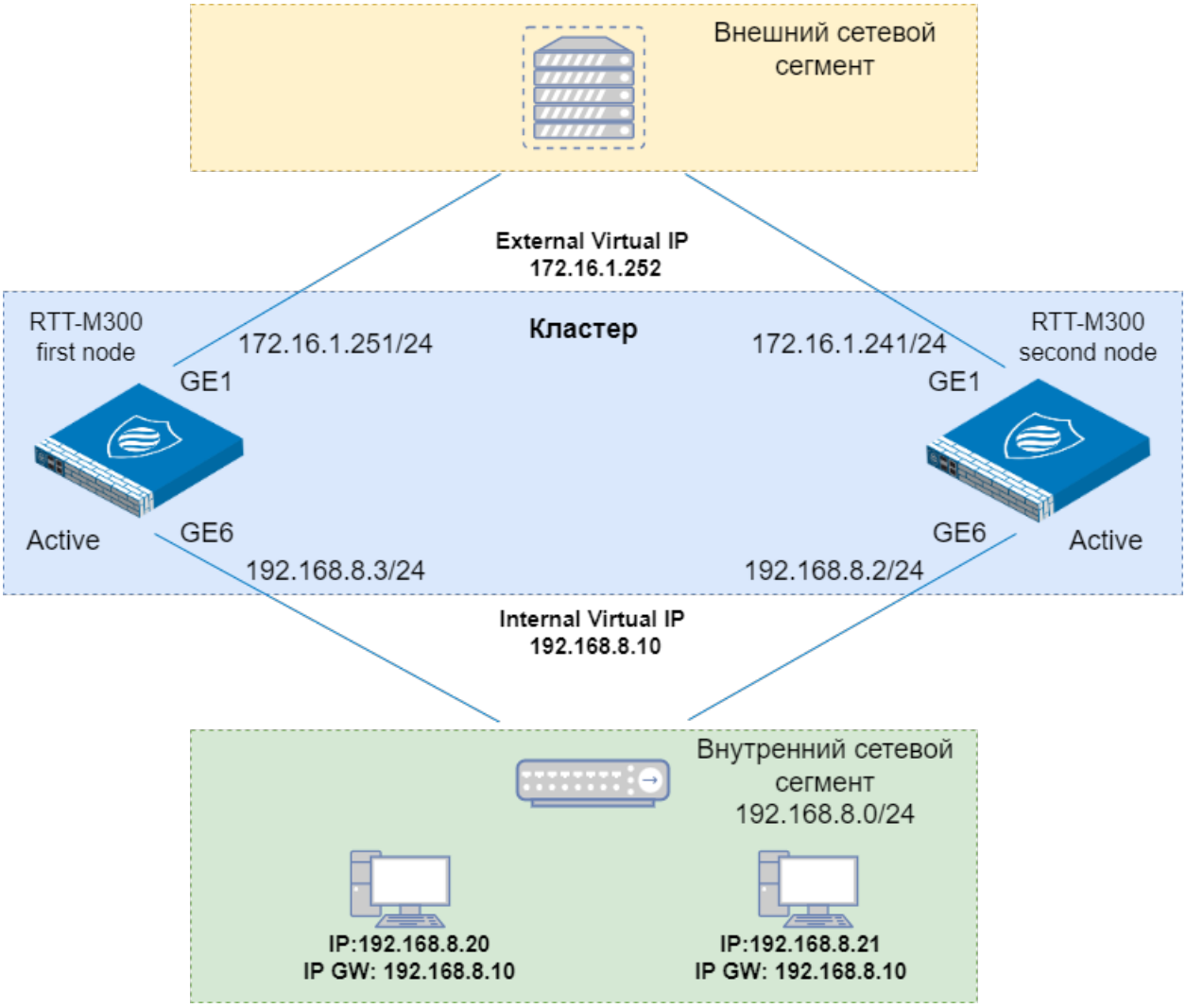
В следующем примере предположим, что необходимо настроить кластер из двух нод в режиме Active/Active с ARP-балансировкой в рамках сетевой топологии ниже.

В рамках данного примера используются две активные ноды, которые могут обрабатывать трафик. Для балансировки трафика между нодами используется механизм ARP-балансировки, который позволяет при использовании одного виртуального IP-адреса распределять MAC-адреса интерфейсов нод между клиентами внутреннего сетевого сегмента. Т.е. клиенты внутреннего сетевого сегмента используют виртуальный IP-адрес (Internal Virtual IP), как основной шлюз по умолчанию, но MAC-адресом шлюза может выступать интерфейс любой ноды в зависимости от MAC-адреса клиента. Основная активная нода отвечает на ARP-запросы во внутреннем сетевом сегменте, распределяя MAC-адреса интерфесов нод соответствующему виртуальному IP-адресу. Например, в рамках представленной схемы, трафик клиента с IP-адресом 192.168.8.20 будет обрабатываться первой активной нодой, а трафик клиента с IP-адресом 192.168.8.21 будет обрабатываться второй активной нодой, тем самым производится распределение трафика по всем активным нодам.

Выбор основной активной ноды (MASTER) производится при помощи параметра **Приоритет**. Чем выше значение приоритета, тем выше вероятность того, что нода возьмет роль MASTER.

Пример конфигурации первой активной ноды представлен ниже.

В разделе **Кластеризация - Настройки - Cluster** произвести конфигурацию первой активной ноды, используя следующие параметры:


Внешний сетевой сегмент
External Virtual IP
172.16.1.252
RTT-M300
first node
172.16.1.251/24
Кластер
172.16.1.241/24
RTT-M300
second node
GE1
GE1
Active
GE6
192.168.8.3/24
192.168.8.2/24
GE6
Active
Internal Virtual IP
192.168.8.10
Внутренний сетевой сегмент
192.168.8.0/24
IP:192.168.8.20
IP GW: 192.168.8.10
IP:192.168.8.21
IP GW: 192.168.8.10

Параметр	Описание/Значение параметра
Включен	Произвести запуск функции кластеризации.
Список нод в кластере	Указать для каждой ноды IP-адреса интерфейсов синхронизации конфигурации - **192.168.8.2, 192.168.8.3**.
Mode cluster	Задать режим работы кластера - **Active / Active**.
Интерфейс внутренней сети	Указать сетевой интерфейс ноды, который будет использоваться виртуальным IP-адресом внутренней сети (Internal Virtual IP) - **GE6**.
Интерфейс внешней сети	Указать сетевой интерфейс ноды, который будет использоваться виртуальным IP-адресом внешней сети (External Virtual IP) - **GE1**.
Приоритет	Задать приоритет ноды в кластере - **1**.
Интервал оповещения	Задать интервал оповещения ноды - **1**.
Виртуальный IP-адрес внутренней сети	Задать виртуальный IP-адрес внутренней сети - **192.168.8.10**.
Виртуальный IP-адрес внешней сети	Задать виртуальный IP-адрес внешней сети - **172.16.1.252**.
Групповой IP-адрес синхронизации сетевых сессий кластера	Задать групповой IP-адрес синхронизации - **225.0.0.50**.
Пароль аутентификации	Задать уникальный пароль аутентификации нод в кластере.
Список синхронизируемых настроек	Выбрать из списка синхронизируемые части конфигурации текущей ноды.

Вторая активная нода имеет аналогичную конфигурацию, исключением является параметр **Priority for load balancing**, значение которого равно 2.

Для проверки работоспособности кластера необходимо проверить состояние нод в кластере. В разделе **Кластеризация - Статус** фиксируется состояние, роль ноды, количество синхронизаций.

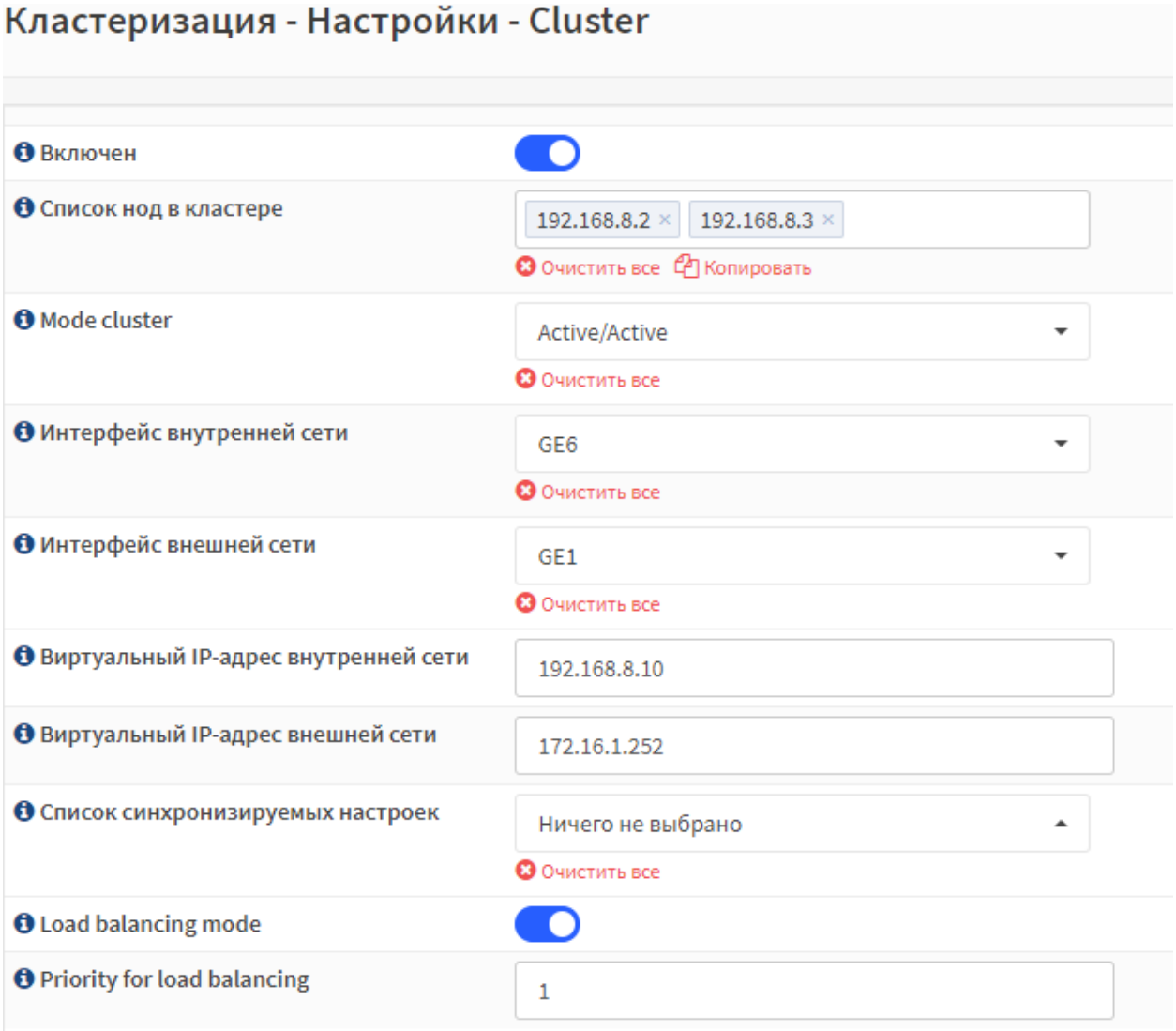
Важно

В рамках режима Active/Active используется две роли в кластере: - MASTER - BACKUP Ноды вне зависимости от роли в режиме Active/Active являются активными, т.е. производят обработку трафика. Роль BACKUP также в рамках Active/Active является активной.

Параметры раздела **Кластеризация - Статус** первой активной ноды.

Параметры раздела **Кластеризация - Статус** второй активной ноды.

После проверки работоспособности кластера можно выбрать необходимые для переноса на резервную ноду списки конфигурации.

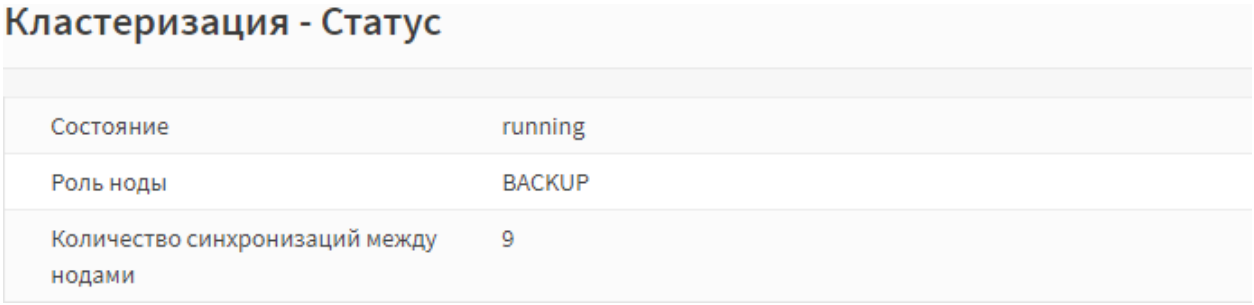

Кластеризация - Настройки - Cluster
Включен
Список нод в кластере
192.168.8.2
192.168.8.3
Очистить все
Копировать
Mode cluster
Active/Active
Очистить все
Интерфейс внутренней сети
GE6
Очистить все
Интерфейс внешней сети
GE1
Очистить все
Виртуальный IP-адрес внутренней сети
192.168.8.10
Виртуальный IP-адрес внешней сети
172.16.1.252
Список синхронизируемых настроек
Ничего не выбрано
Очистить все
Load balancing mode
Priority for load balancing
1

Кластеризация - Настройки - Cluster

Включен	
Список нод в кластере	192.168.8.2 × 192.168.8.3 × Очистить все Копировать
Mode cluster	Active/Active Очистить все
Интерфейс внутренней сети	GE6 Очистить все
Интерфейс внешней сети	GE1 Очистить все
Виртуальный IP-адрес внутренней сети	192.168.8.10
Виртуальный IP-адрес внешней сети	172.16.1.252
Список синхронизируемых настроек	Ничего не выбрано Очистить все
Load balancing mode	
Priority for load balancing	2

Кластеризация - Статус

Состояние	running
Роль ноды	MASTER
Количество синхронизаций между нодами	0



Пример конфигурации кластера в режиме Active/Active с балансировщиком трафика

В заключительном примере рассмотрена реализация кластеризации с внешним балансировщиком трафика. Предположим, что необходимо настроить кластер из двух нод в режиме Active/Active с внешним балансировщиком трафика, который производит распределение всего поступающего в кластер трафика.

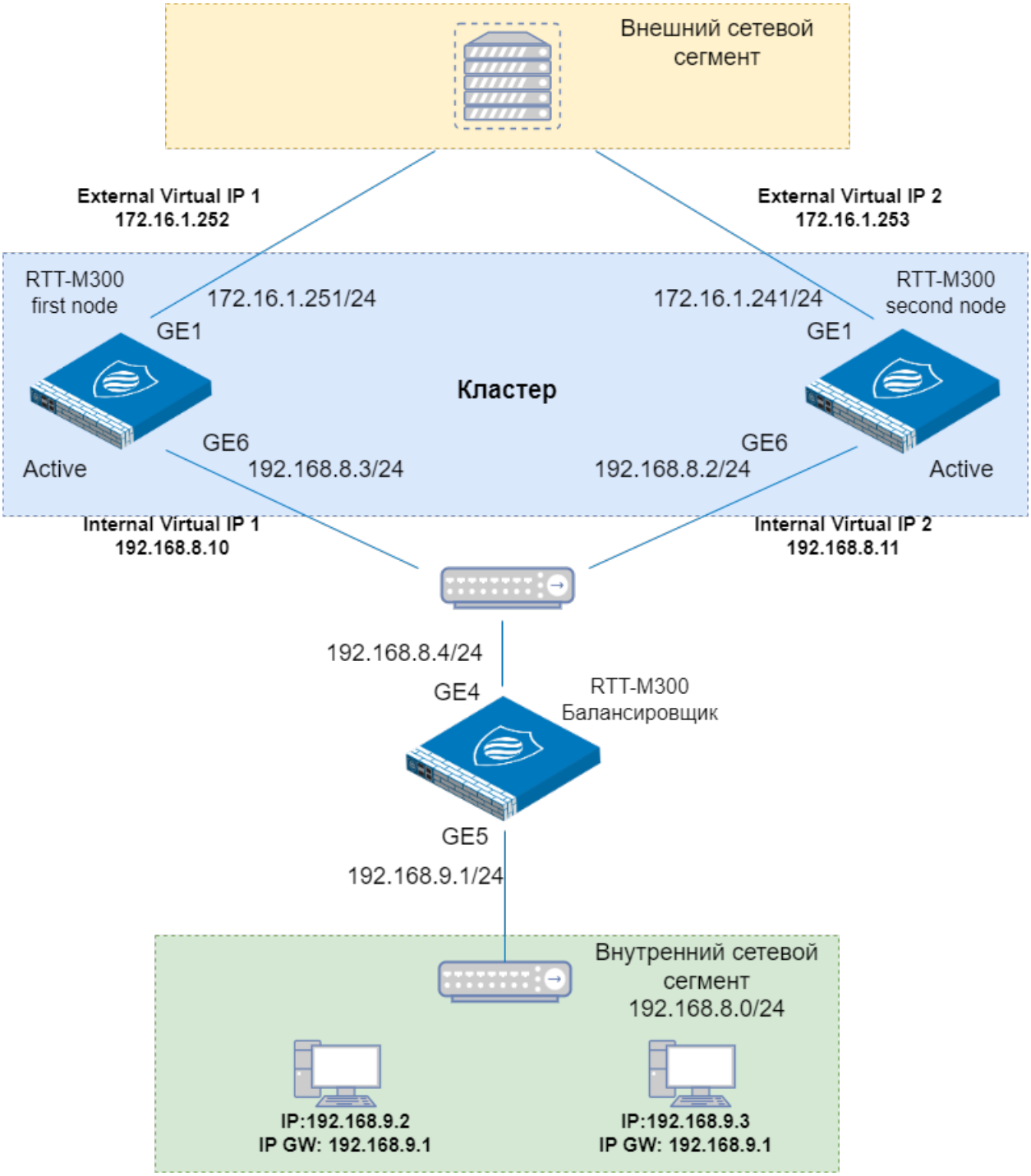
В рамках примера производится конфигурация двух нод в кластере в режиме работы Active/Active. После конфигурации кластера производится настройка внешнего балансировщика. Следует обратит внимание, что в рамках данного примера используется два виртуальных IP-адреса во внутренней и внешней сети кластера (**Internal - 192.168.8.10, 192.168.8.11; External - 172.16.1.252, 172.16.1.253**), по которым балансировщик производит перераспределение трафика.

Важно

В качестве балансировщика может выступать отдельный экземпляр RTT-M300 или любой иной брокер пакетов.

Пример конфигурации первой активной ноды представлен ниже.

В разделе **Кластеризация - Настройки - Cluster** произвести конфигурацию первой активной ноды, используя следующие параметры:


Внешний сетевой сегмент
External Virtual IP 1
172.16.1.252
External Virtual IP 2
172.16.1.253
RTT-M300
first node
172.16.1.251/24
GE1
172.16.1.241/24
RTT-M300
second node
GE1
Кластер
GE6
Active
192.168.8.3/24
192.168.8.2/24
GE6
Active
Internal Virtual IP 1
192.168.8.10
Internal Virtual IP 2
192.168.8.11
192.168.8.4/24
GE4
RTT-M300
Балансировщик
GE5
192.168.9.1/24
Внутренний сетевой сегмент
192.168.8.0/24
IP:192.168.9.2
IP GW: 192.168.9.1
IP:192.168.9.3
IP GW: 192.168.9.1

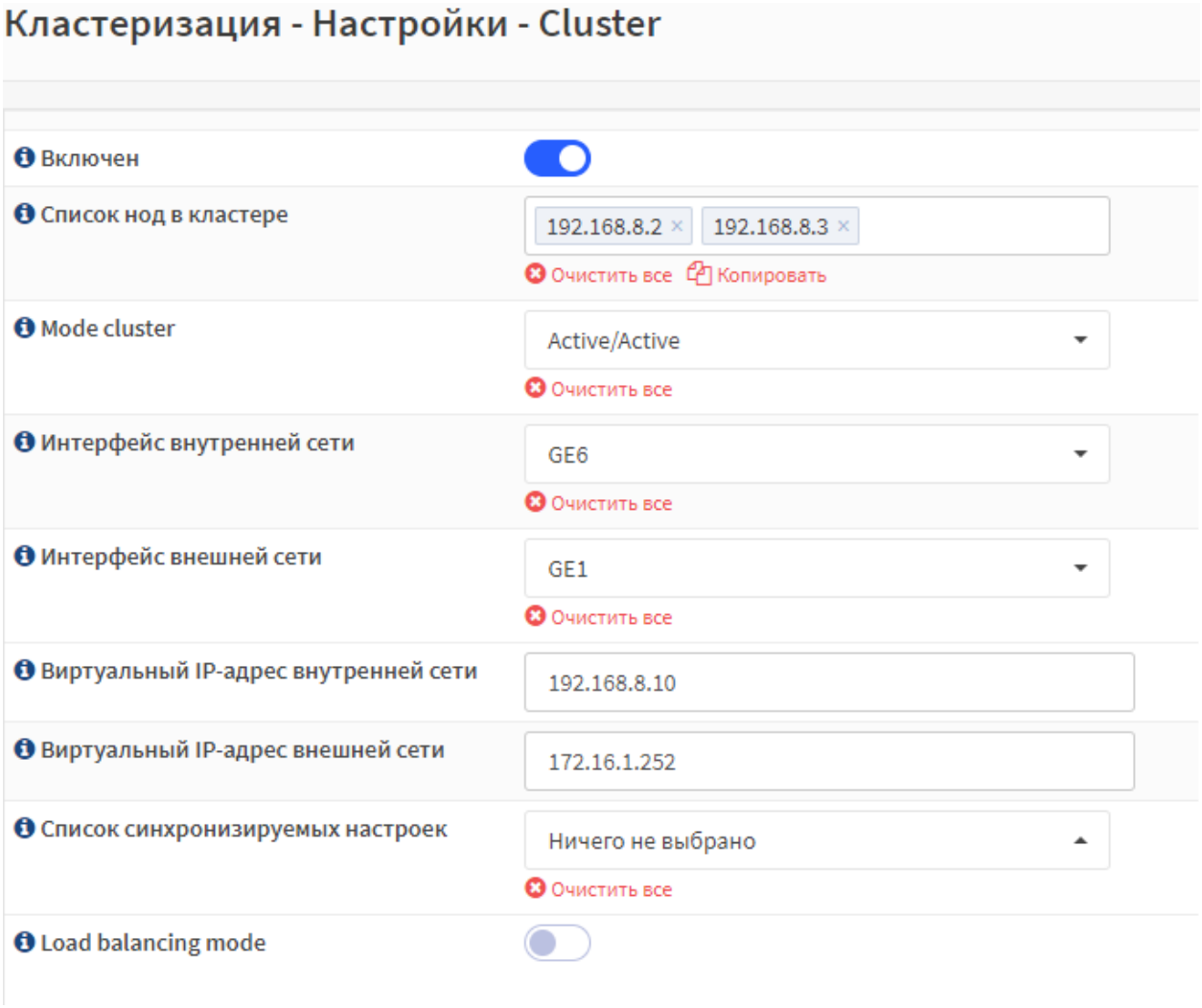
Параметр	Описание/Значение параметра
Включен	Произвести запуск функции кластеризации.
Список нод в кластере	Указать для каждой ноды IP-адреса интерфейсов синхронизации конфигурации - **192.168.8.2, 192.168.8.3**.
Mode cluster	Задать режим работы кластера - **Active / Active**.
Интерфейс внутренней сети	Указать сетевой интерфейс ноды, который будет использоваться виртуальным IP-адресом внутренней сети (Internal Virtual IP) - **GE6**.
Интерфейс внешней сети	Указать сетевой интерфейс ноды, который будет использоваться виртуальным IP-адресом внешней сети (External Virtual IP) - **GE1**.
Виртуальный IP-адрес внутренней сети	Задать виртуальный IP-адрес внутренней сети - **192.168.8.10**.
Виртуальный IP-адрес внешней сети	Задать виртуальный IP-адрес внешней сети - **172.16.1.252**.
Групповой IP-адрес синхронизации сетевых сессий кластера	Задать групповой IP-адрес синхронизации - **225.0.0.50**.
Список синхронизируемых настроек	Выбрать из списка синхронизируемые части конфигурации текущей ноды.

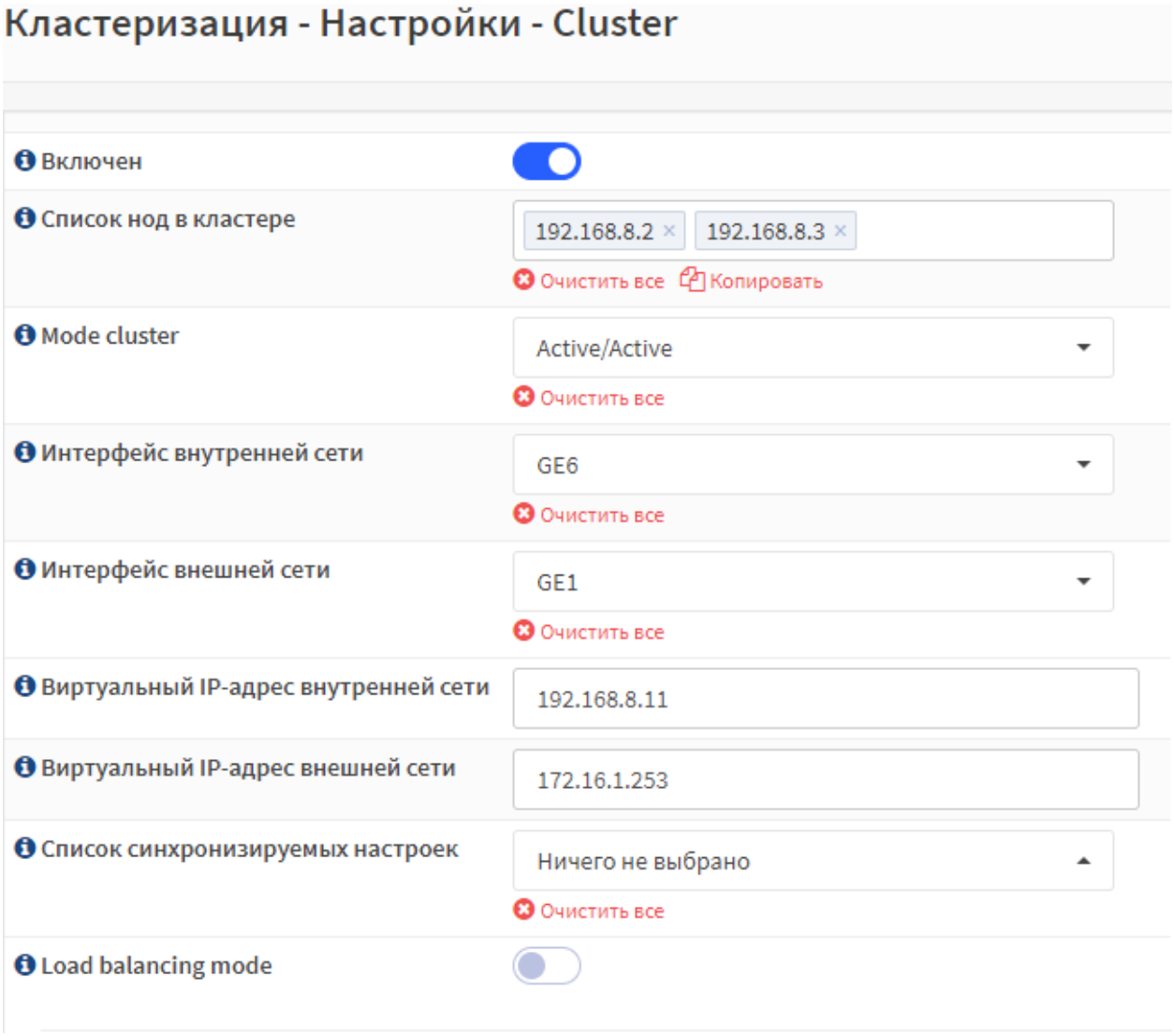
Вторая активная нода имеет аналогичную конфигурацию, исключением является параметры **Виртуальный IP-адрес внутренней сети - 192.168.8.11**, **Виртуальный IP-адрес внешней сети**-172.16.1.253**.

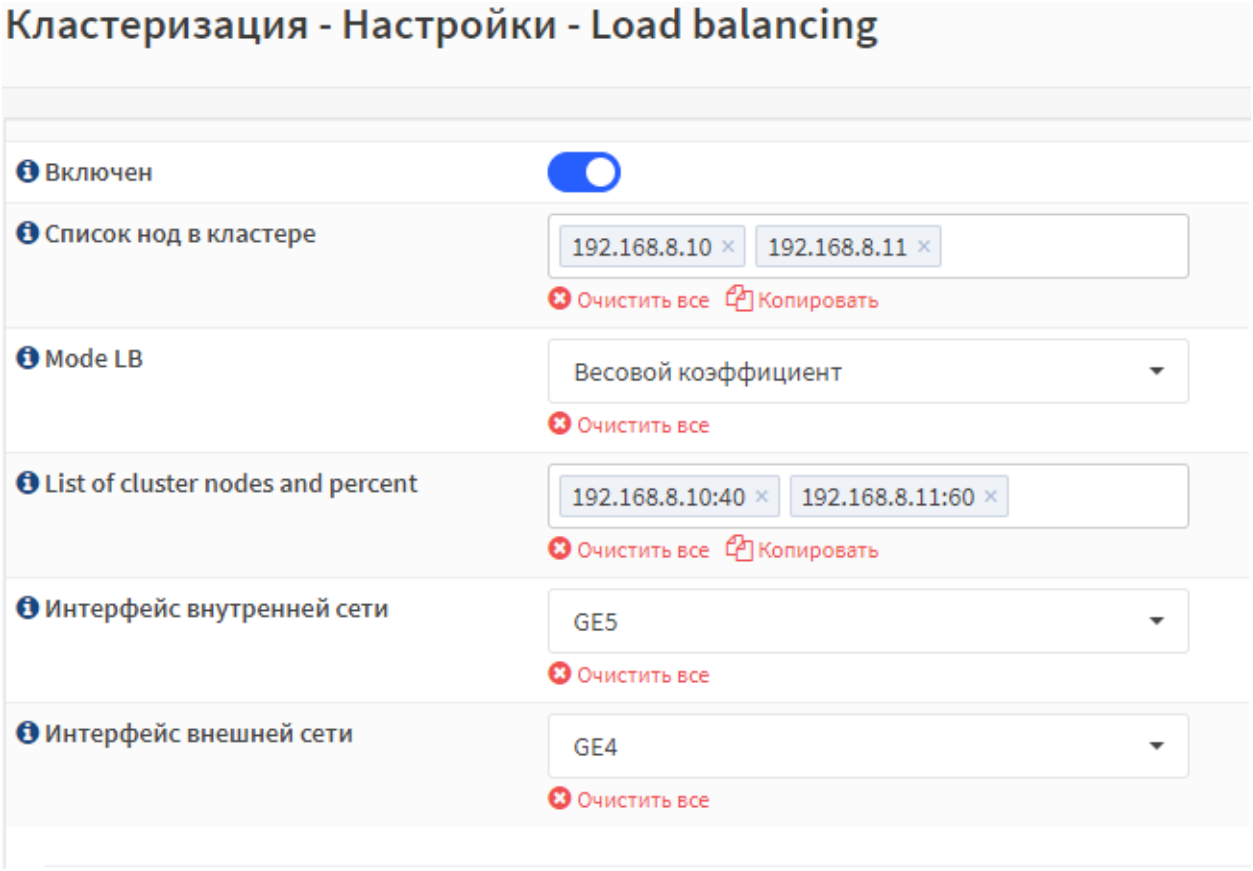
В разделе **Кластеризация - Настройки - Load balancing** произвести конфигурацию балансировщика трафика, используя следующие параметры:

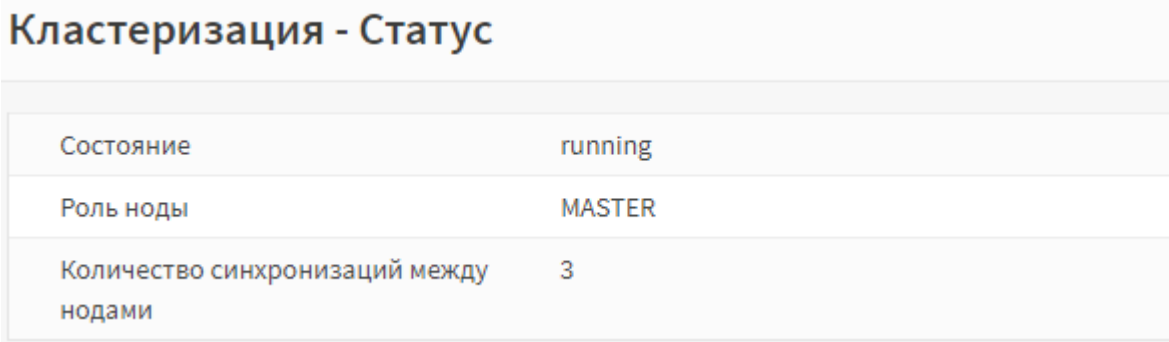
Параметр	Описание параметра
Включен	Запустить функцию балансировки трафика на устройстве.
Список нод в кластере	Указать виртуальные IP адреса (Virtual IP), которые используются нодами в кластере для синхронизации во внутреннем сетевом сегменте - **192.168.8.10, 192.168.8.11**.
Mode LB	Указать механизм балансировки. В рамках примера используется механизм **Весовой коэффициент**.
List of cluster nodes and percent (В режиме Весовой коэффициент)	Указать виртуальные IP адреса (Virtual IP), которые используются нодами в кластере во внутреннем сетевом сегменте и процентное соотношение распределяемого трафика. В рамках примера данные вводятся в формате **192.168.8.10:40, 192.168.8.11:60** (где 40/60 - это 40/60 процентов от общего количество распределяемого трафика);
Интерфейс внутренней сети	Укажите сетевой интерфейс, который «смотрит» в сторону сетевого сегмента (противоположная сторона от кластера) - **GE5**.
Интерфейс внешней сети	Укажите сетевой интерфейс, который «смотрит» в сторону кластера - **GE4**.

Для проверки работоспособности кластера необходимо проверить состояние нод в кластере. В разделе **Кластеризация - Статус** фиксируется состояние, роль ноды, количество синхронизаций. В режиме active/active каждая нода должна иметь роль MASTER. Состояние службы кластеризации должно иметь статус - **running** (служба запущена).


Кластеризация - Настройки - Cluster
Включен
Список нод в кластере
192.168.8.2
192.168.8.3
Очистить все
Копировать
Mode cluster
Active/Active
Очистить все
Интерфейс внутренней сети
GE6
Очистить все
Интерфейс внешней сети
GE1
Очистить все
Виртуальный IP-адрес внутренней сети
192.168.8.10
Виртуальный IP-адрес внешней сети
172.16.1.252
Список синхронизируемых настроек
Ничего не выбрано
Очистить все
Load balancing mode


Кластеризация - Настройки - Cluster
Включен
Список нод в кластере
192.168.8.2
192.168.8.3
Очистить все
Копировать
Mode cluster
Active/Active
Очистить все
Интерфейс внутренней сети
GE6
Очистить все
Интерфейс внешней сети
GE1
Очистить все
Виртуальный IP-адрес внутренней сети
192.168.8.11
Виртуальный IP-адрес внешней сети
172.16.1.253
Список синхронизируемых настроек
Ничего не выбрано
Очистить все
Load balancing mode

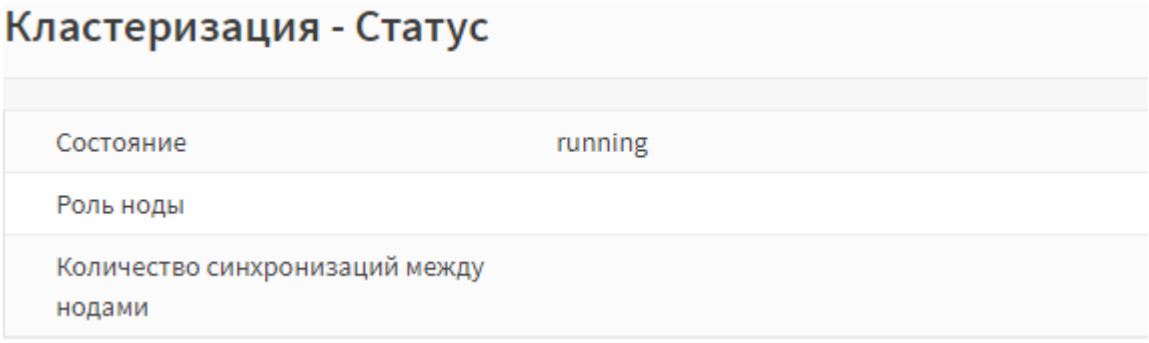

Кластеризация - Настройки - Load balancing
Включен
Список нод в кластере
192.168.8.10
192.168.8.11
Очистить все
Копировать
Mode LB
Весовой коэффициент
Очистить все
List of cluster nodes and percent
192.168.8.10:40
192.168.8.11:60
Очистить все
Копировать
Интерфейс внутренней сети
GE5
Очистить все
Интерфейс внешней сети
GE4
Очистить все


Кластеризация - Статус
Состояние
running
Роль ноды
MASTER
Количество синхронизаций между нодами
3

Примечание

В режиме active/active после возобновления работы, MASTER берет роль BACKUP и сохраняет ее до новых выборов основной ноды в кластере.

Балансировщик в активном состоянии должен иметь статус - **running**.



После проверки работоспособности кластера можно выбрать необходимые для переноса на соседнюю ноду списки конфигурации.

2.6.15.10 Обновление системного ПО (REFOS) каждой ноды в кластере.

При наличии новой версии ПО обновляется каждая нода последовательно. В рамках кластера версия ПО не должна отличаться. В режиме active/passive синхронизация сессий напрямую зависит от версии ПО каждой ноды. При наличии в кластере нод с разными версиями ПО, синхронизация сессий производиться не будет.

2.7 Web-интерфейс

2.7.1 Общая информация

Web-интерфейс является основным полнофункциональным интерфейсом управления ОС REFOS.

В данном разделе приведено подробное описание Web-интерфейса версии ОС REFOS 1.x.x.

2.7.2 Сводка

Для перехода к просмотру общей информации о продукте необходимо:

- нажать на вкладку **«Сводка»** - **«Инструментальная панель»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться общая информация о продукте, соответствующая рисунку;

Для перехода к смене пароля учетной записи необходимо:

- нажать на вкладку **«Сводка»** - **«Пароль»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться информация о смене пароля учетной записи.

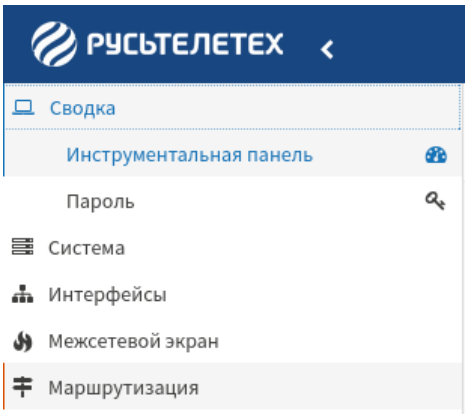


Рис. 126: Переход к просмотру общей информации о продукте

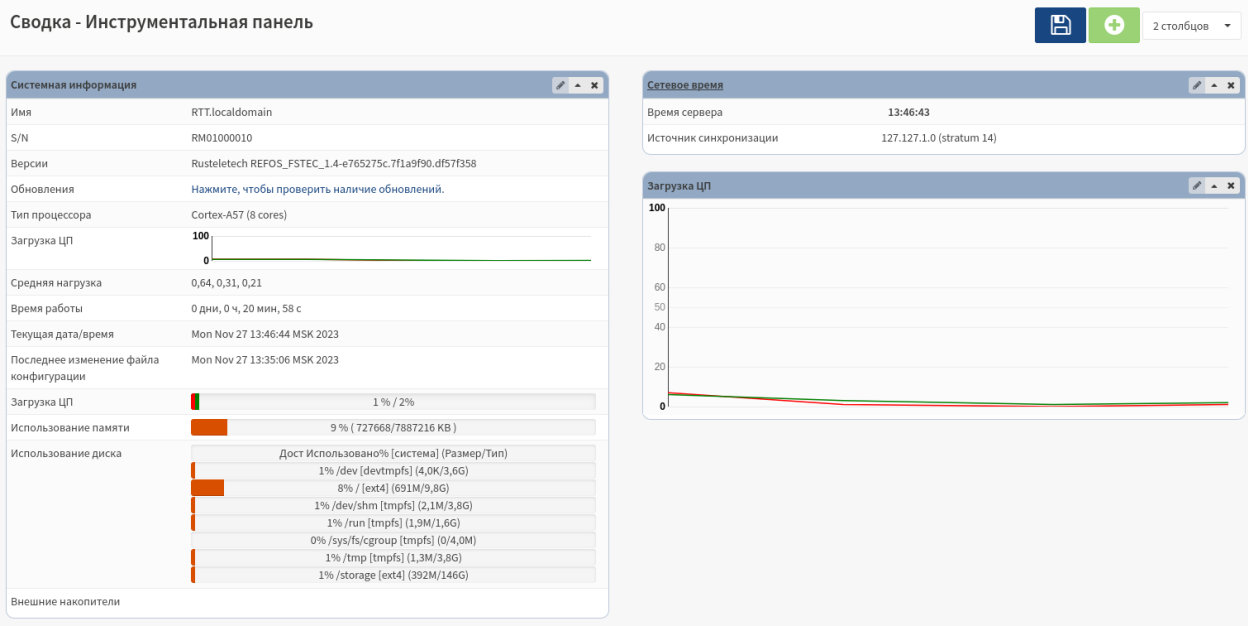


Рис. 127: Общая информация о продукте

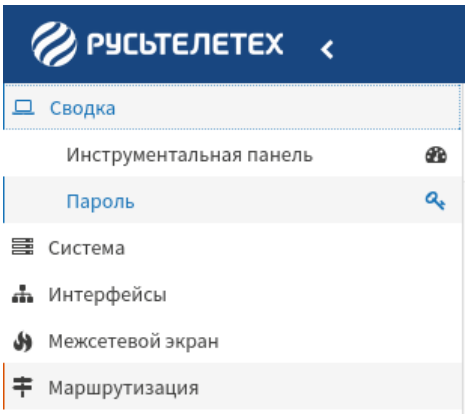


Рис. 128: Переход к смене пароля учетной записи

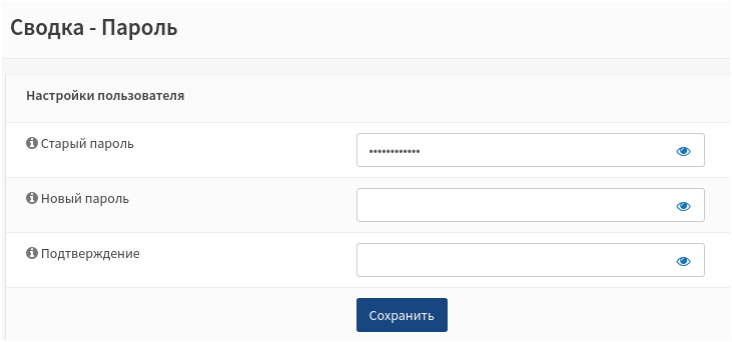


Рис. 129: Смена пароля учетной записи

2.7.2.1 Инструментальная панель

Вкладка **«Инструментальная панель»** отражает общую информацию о продукте, и реализована в виде виджетов.

По умолчанию доступны следующие виджеты:

- **«Системная информация»**;
- **«Сетевое время»**;
- **«Загрузка ЦП»**.

Для добавления новых виджетов на инструментальную панель необходимо:

- нажать кнопку **«Добавить виджет»**  ;
- в открывшемся окне выбрать доступные виджеты, соответствующие таблице.

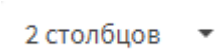
Рис. 130: Выбор виджетов

Таблица 54: Таблица доступных виджетов

Доступные виджеты
Шлюзы
Интерфейсы
Статистика интерфейса
Monit
Датчики температуры

- нажать кнопку **«Сохранить»**  .

Для изменения расположения виджетов необходимо:

- выбрать из выпадающего списка 

один из способов расположения виджетов, соответствующих таблице;

Таблица 55: Таблица способов расположения виджетов

Способы расположения виджетов
1 столбец
2 столбцов
3 столбцов

Системная информация

Виджет **«Системная информация»** содержит следующие сведения о продукте:

- **«Имя»** - имя продукта;
- **«S/N»** - серийный номер продукта;
- **«Версии»** - версии продукта;
- **«Обновления»** - обновления продукта;
- **«Тип процессора»** - тип/модель установленного процессора;
- **«Загрузка ЦП»** - показатель загрузки процессора;
- **«Средняя нагрузка»** - показатель средней нагрузки;
- **«Время работы»** - время работы продукта;
- **«Текущая дата/время»** - текущая дата и время;
- **«Последнее изменение файла конфигурации»** - дата и время последнего изменения файла конфигурации;
- **«Загрузка ЦП»** - показатель загрузки процессора (в %);
- **«Использование памяти»** - объем использованной памяти (в %);
- **«Использование диска»** - объем использования диска (в %).

Сетевое время

Виджет **«Сетевое время»** содержит следующие сведения:

- **«Время сервера»** - время, полученное с NTP-сервера;
- **«Источник синхронизации»** - IP-адрес источника синхронизации.

Совет

Для перехода к просмотру статуса протокола сетевого времени необходимо нажать на ссылку **«Сетевое время»** и в открывшемся окне появится статус протокола сетевого времени

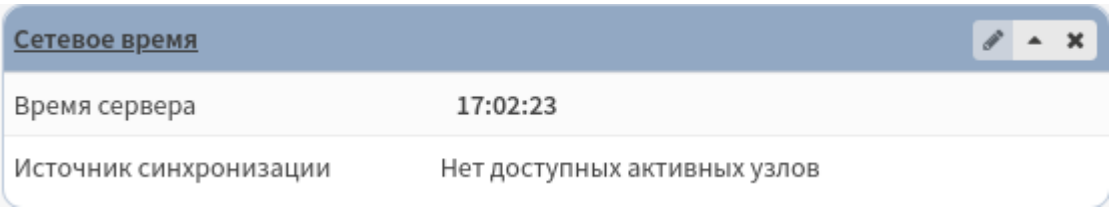


Рис. 131: Статус протокола сетевого времени

Загрузка ЦП

Виджет **«Загрузка ЦП»** содержит диаграмму загрузки ЦП в определенный момент времени.

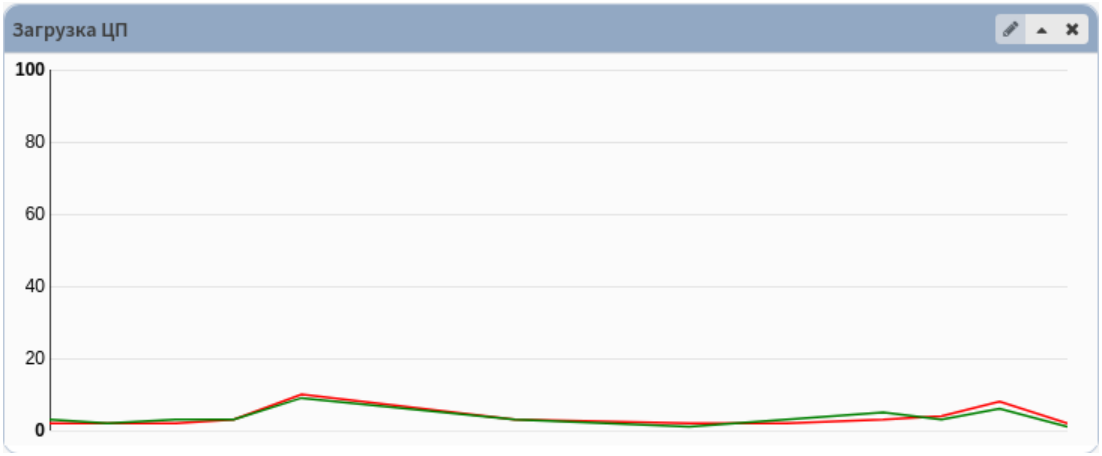


Рис. 132: Загрузка ЦП

Шлюзы

Виджет **«Шлюзы»** содержит таблицу шлюзов.

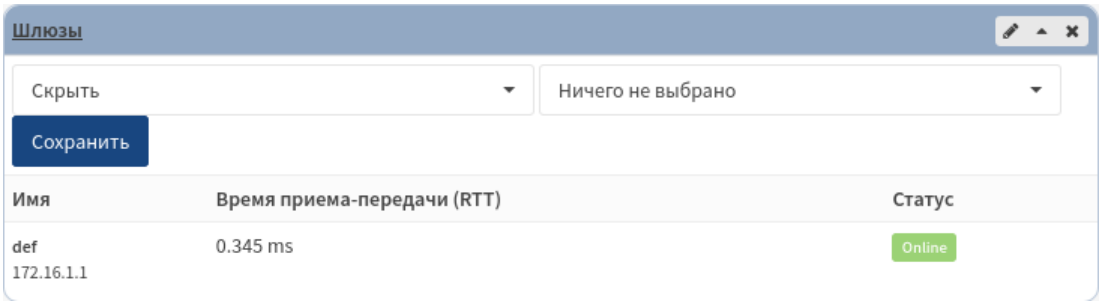


Рис. 133: Виджет **«Шлюзы»**

Для того, чтобы скрыть/показать необходимый шлюз следует:

- нажать на кнопку  ;
- выбрать из выпадающего списка один из соответствующих параметров;
- выбрать из выпадающего списка необходимый шлюз;
- нажать кнопку **«Сохранить»** 

.

Интерфейсы

Виджет **«Интерфейсы»** содержит список интерфейсов продукта.

Рис. 134: Виджет **«Интерфейсы»**

Для того, чтобы скрыть/показать необходимый интерфейс следует:

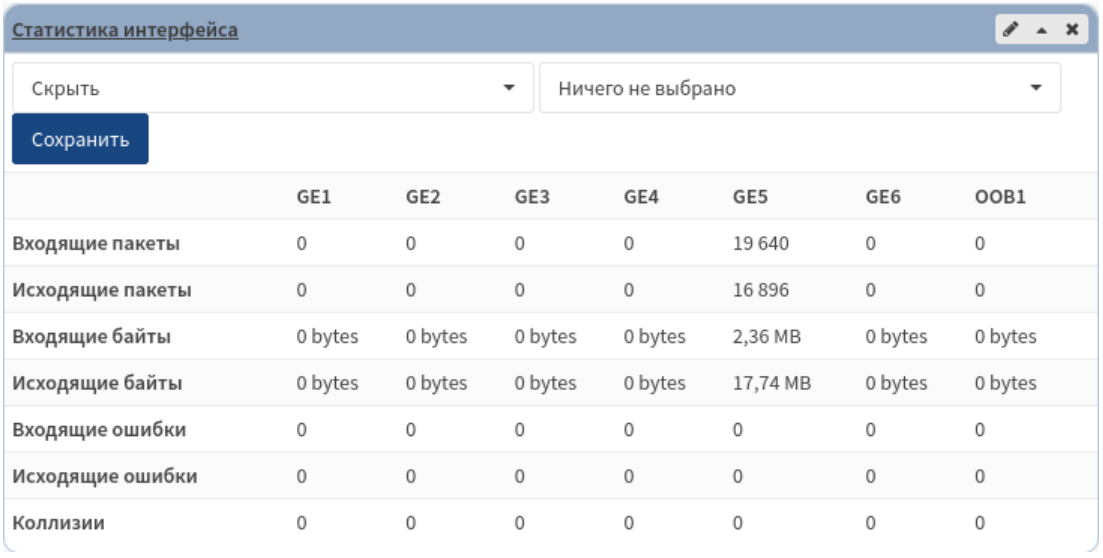
- нажать на кнопку  ;
- выбрать из выпадающего списка один из соответствующих параметров;
- выбрать из выпадающего списка необходимый интерфейс;
- нажать кнопку **«Сохранить»** 

.

Статистика интерфейса

Виджет **«Статистика интерфейса»** содержит статистические данные интерфейса, а именно:

- **«Входящие пакеты»**;
- **«Исходящие пакеты»**;
- **«Входящие байты»**;
- **«Исходящие байты»**;
- **«Входящие ошибки»**;
- **«Исходящие ошибки»**;
- **«Коллизии»**.



	GE1	GE2	GE3	GE4	GE5	GE6	OOB1
Входящие пакеты	0	0	0	0	19 640	0	0
Исходящие пакеты	0	0	0	0	16 896	0	0
Входящие байты	0 bytes	0 bytes	0 bytes	0 bytes	2,36 MB	0 bytes	0 bytes
Исходящие байты	0 bytes	0 bytes	0 bytes	0 bytes	17,74 MB	0 bytes	0 bytes
Входящие ошибки	0	0	0	0	0	0	0
Исходящие ошибки	0	0	0	0	0	0	0
Коллизии	0	0	0	0	0	0	0

Рис. 135: Виджет **«Статистика интерфейса»**

Для того, чтобы скрыть/показать необходимый интерфейс следует:

- нажать на кнопку  ;
- выбрать из выпадающего списка один из соответствующих параметров;
- выбрать из выпадающего списка необходимый интерфейс;

- нажать кнопку **«Сохранить»** 

.

Monit

Виджет **«Monit»** содержит систему мониторинга системы.

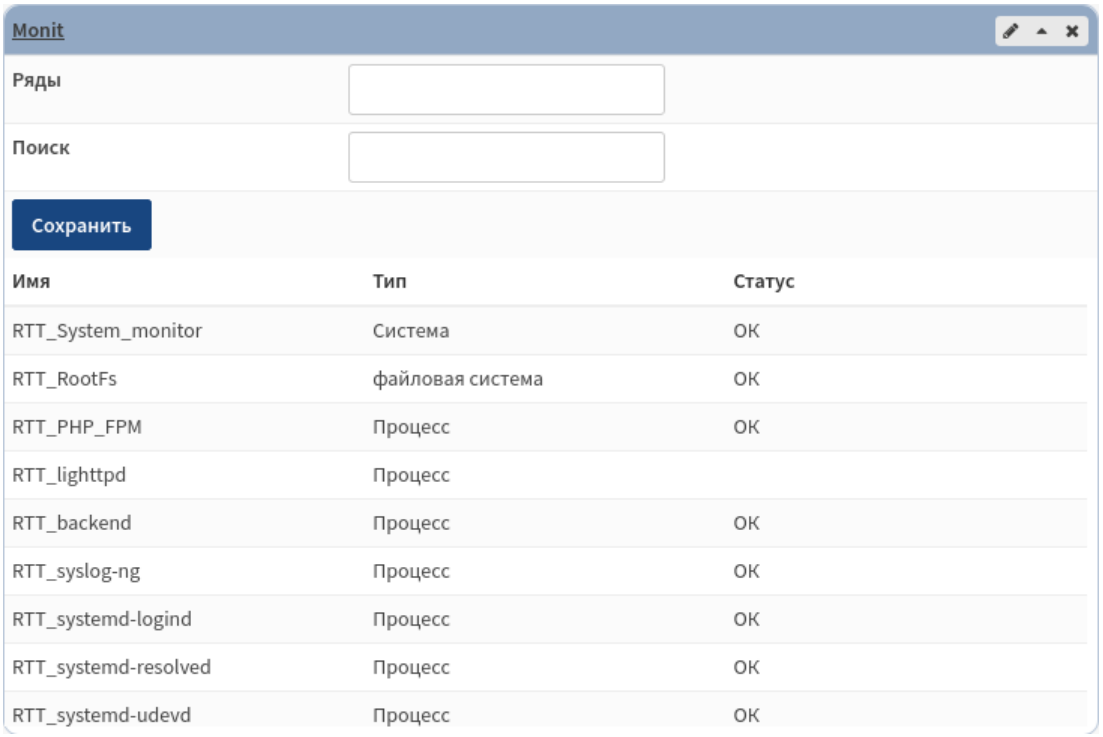


Рис. 136: Виджет **«Статистика интерфейса»**

Для поиска необходимой информации следует:

- нажать на кнопку  ;
- ввести в строки **«Ряды»** и **«Поиск»** необходимую информацию;
- нажать кнопку **«Сохранить»** 

.

Тепловые датчики

Виджет **«Тепловые датчики»** содержит сведения о тепловых датчиках процессора.

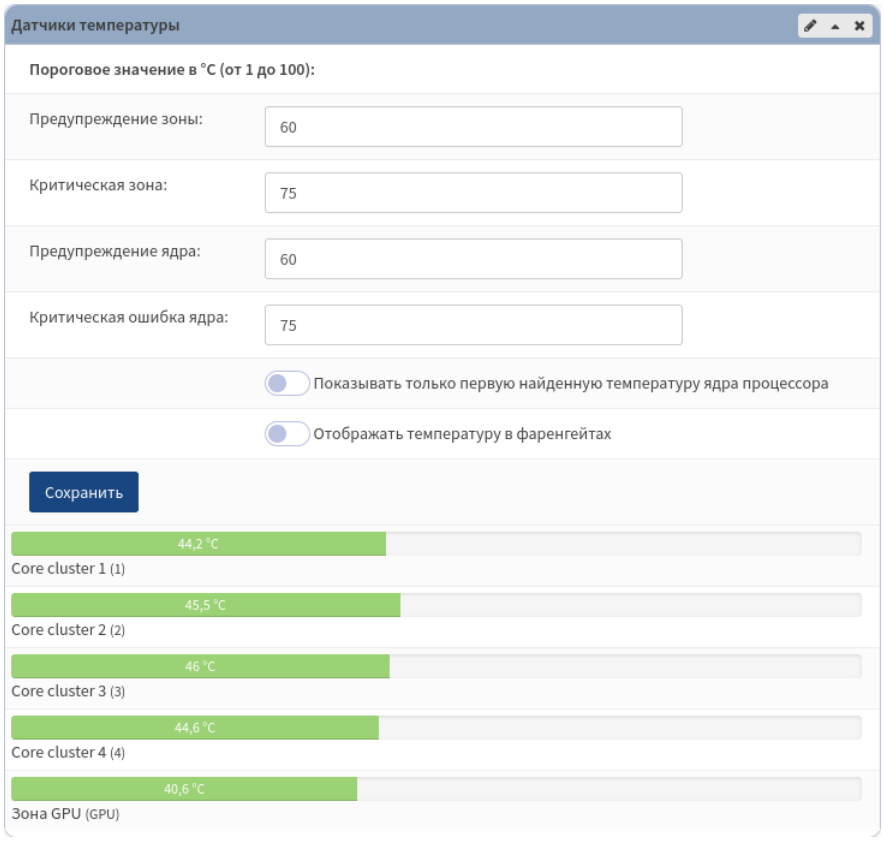


Рис. 137: Виджет **«Тепловые датчики»**

Для выставления пороговых значений температуры необходимо:

- нажать на кнопку  ;
- в открывшемся окне выставить необходимые пороговые значения температуры;
- нажать кнопку **«Сохранить»** 

.

2.7.2.2 Пароль

Смена пароля учетной записи

В разделе **«Настройки пользователя»** необходимо:

- в поле **«Старый пароль»** ввести действующий пароль учетной записи;
- в поле **«Новый пароль»** ввести новый пароль учетной записи;
- в поле **«Подтверждение»** ввести новый пароль учетной записи для подтверждения;

- нажать кнопку **«Сохранить»** 

.

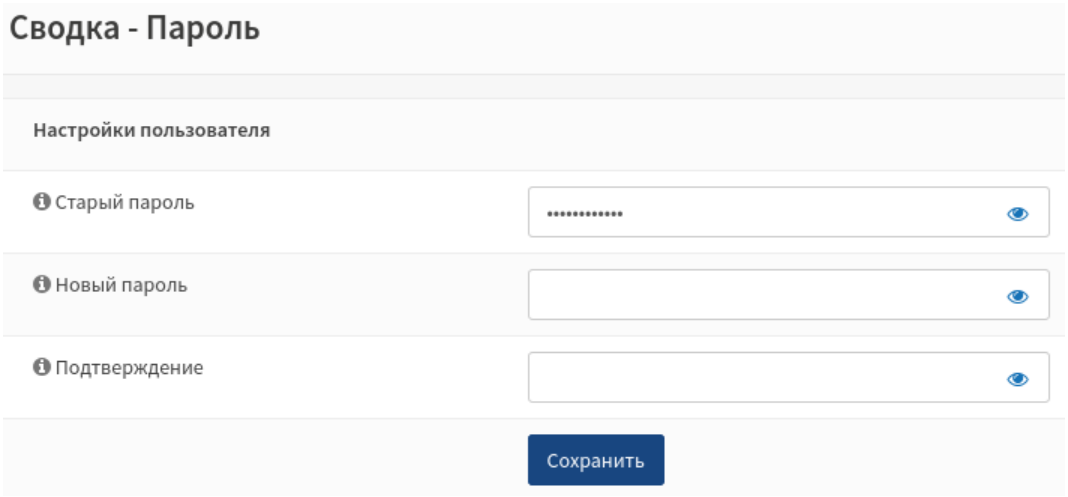


Рис. 138: Смена пароля учётной записи пользователя

2.7.3 Система

Раздел **«Система»** содержит описание процедур для настройки устройства.

2.7.3.1 Доступ

Вкладка **«Доступ»** дает возможность осуществлять проверку наличия пользователя в системе, а также просматривать, редактировать и создавать:

- учетные записи пользователей;
- группы пользователей;
- серверы;

Для перехода к просмотру, редактированию и созданию учетных записей пользователей необходимо:

- нажать на вкладку **«Система»** - **«Доступ»** - **«Пользователи»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица учетных записей пользователей;
- нажать кнопку **«Добавить»** 

для добавления новой учетной записи пользователя в таблицу пользователей.

Для перехода к просмотру, редактированию и созданию групп пользователей необходимо:

- нажать на вкладку **«Система»** - **«Доступ»** - **«Группы»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица групп пользователей;

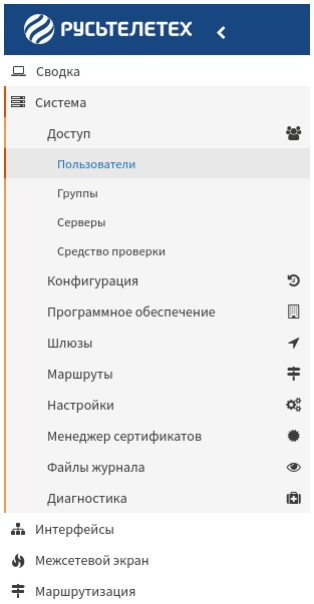


Рис. 139: Переход к просмотру, редактированию и созданию учетных записей пользователей

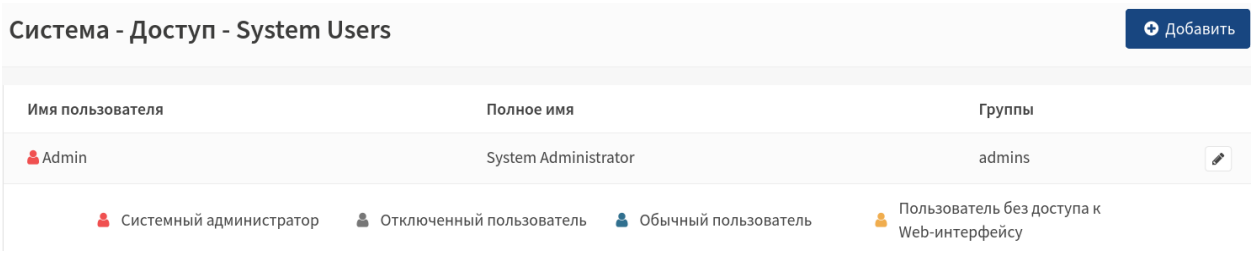


Рис. 140: Таблица учетных записей пользователей

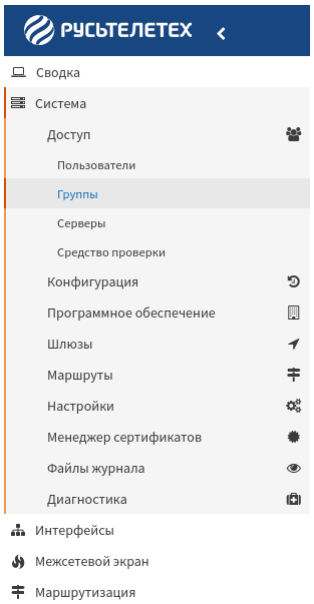


Рис. 141: Переход к просмотру, редактированию и созданию групп пользователей

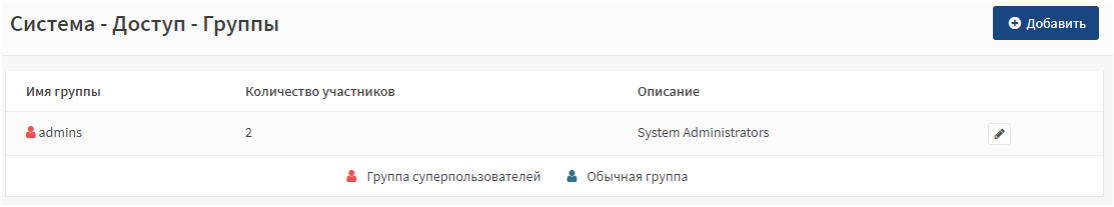


Рис. 142: Таблица групп пользователей

- нажать кнопку **«Добавить»**  для добавления новой группы пользователей в таблицу групп.

Для перехода к просмотру, редактированию и созданию серверов необходимо:

- нажать на вкладку **«Система»** - **«Доступ»** - **«Серверы»**, расположенную в левой части списка объектов управления;

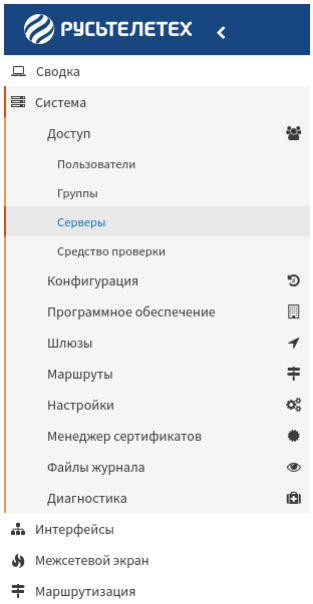


Рис. 143: Переход к просмотру, редактированию и созданию серверов

- в правой части экрана появиться таблица серверов;

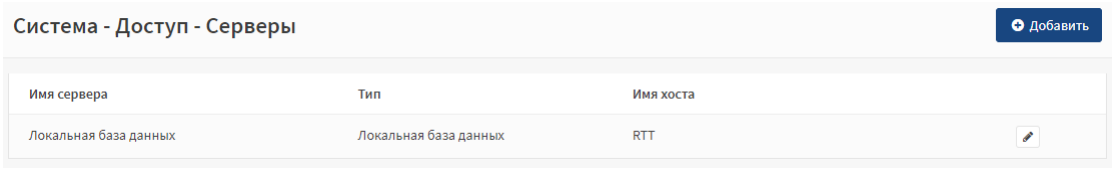
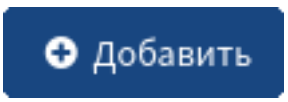


Рис. 144: Таблица серверов

- нажать кнопку **«Добавить»**  для добавления нового сервера в таблицу

серверов.

Для перехода к проведению проверки наличия пользователя в системе необходимо:

- нажать на вкладку **«Система»** - **«Доступ»** - **«Средство проверки»**, расположенную в левой части списка объектов управления;

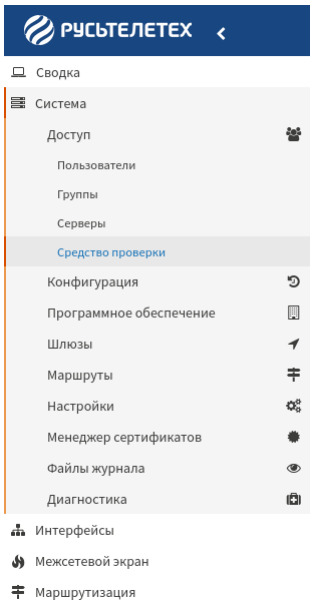


Рис. 145: Переход к проведению проверки наличия пользователя в системе

- в правой части экрана появиться средство проверки.

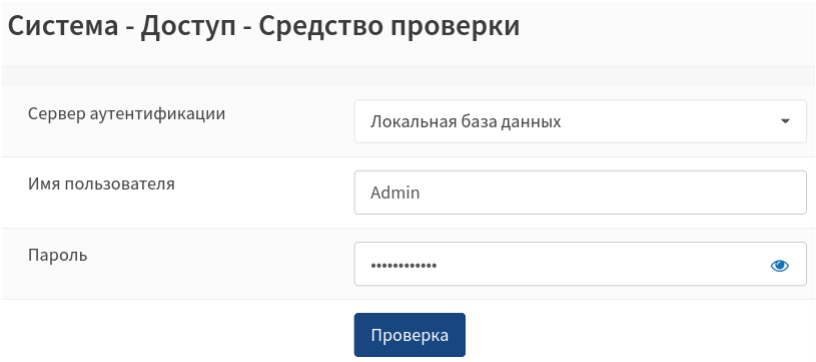


Рис. 146: Средство проверки

Пользователи

Отключение учетной записи пользователя

В разделе **«Пользователи»** необходимо:

- в поле **«Отключена»** установить переключатель в случае необходимости отключить доступ пользователю;

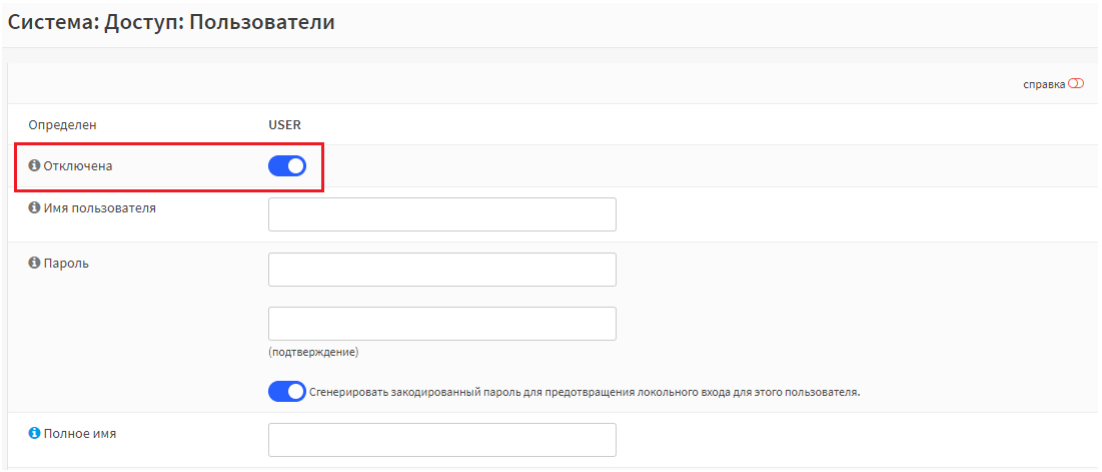


Рис. 147: Отключение доступа пользователю

Создание учетной записи пользователя

В разделе **«Пользователи»** необходимо:

- в поле **«Имя пользователя»** ввести имя пользователя;

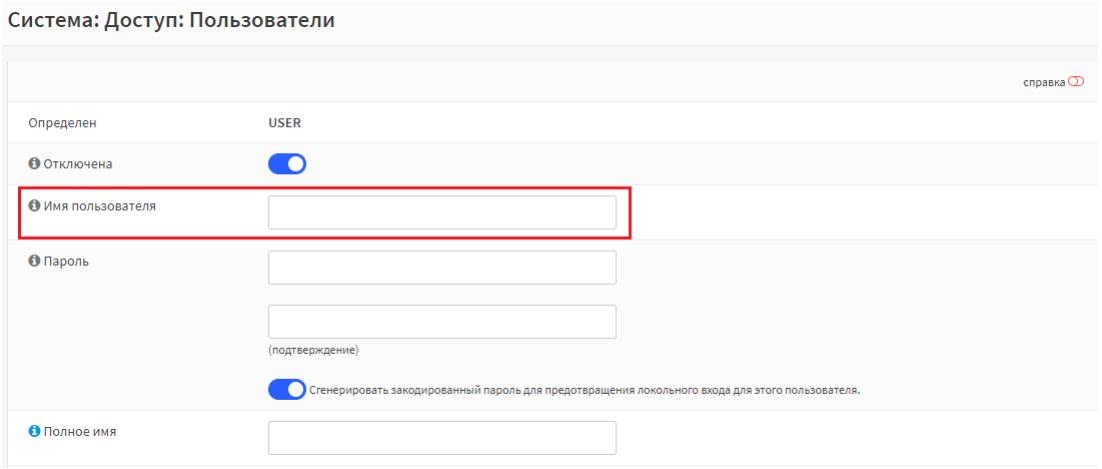


Рис. 148: Имя пользователя

- в поле **«Пароль»** ввести пароль и подтвердить его;

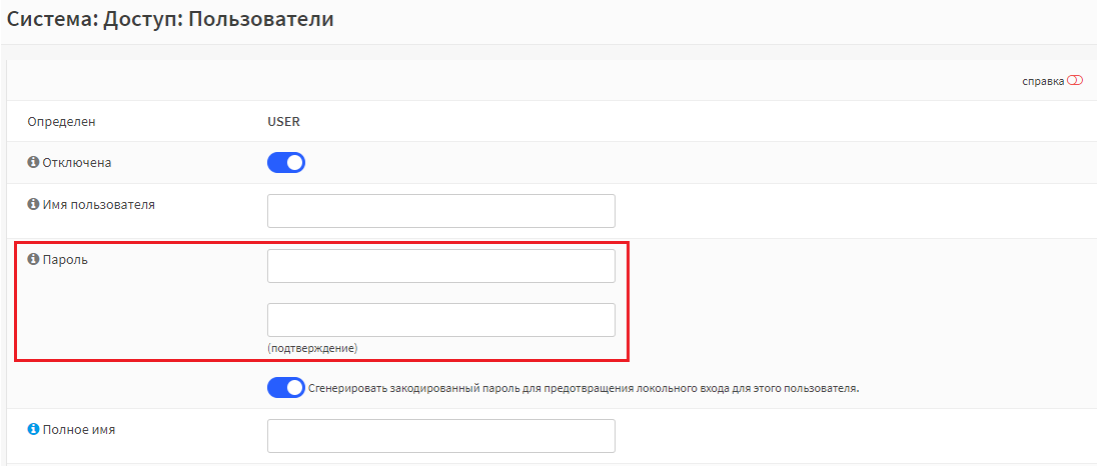


Рис. 149: Пароль

Примечание

Пользователь может установить переключатель в случае необходимости сгенерировать закодированный пароль для предотвращения локольного входа для этого пользователя

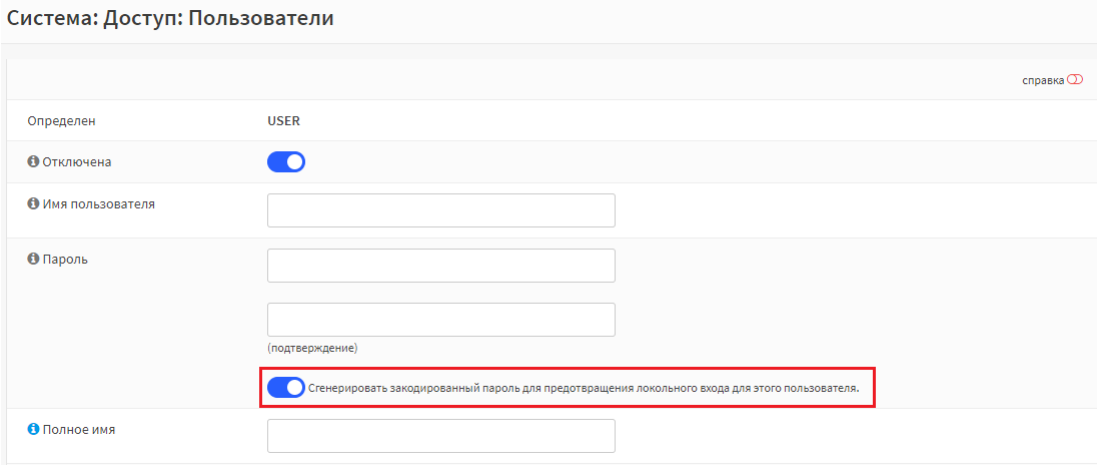


Рис. 150: Генерирование закодированного пароля

- в поле **«Полное имя»** ввести полное имя пользователя;

Примечание

Полное имя пользователя вводится для собственной информации пользователя

- в поле **«E-Mail»** ввести адрес электронной почты пользователя;

Примечание

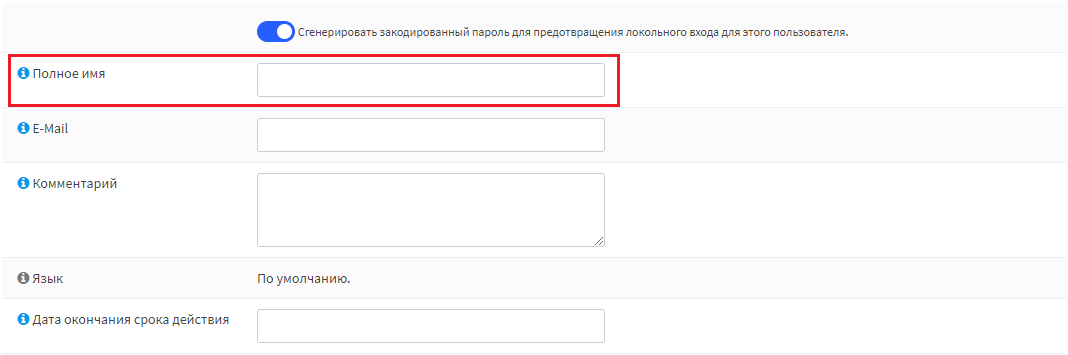


Рис. 151: Полное имя пользователя

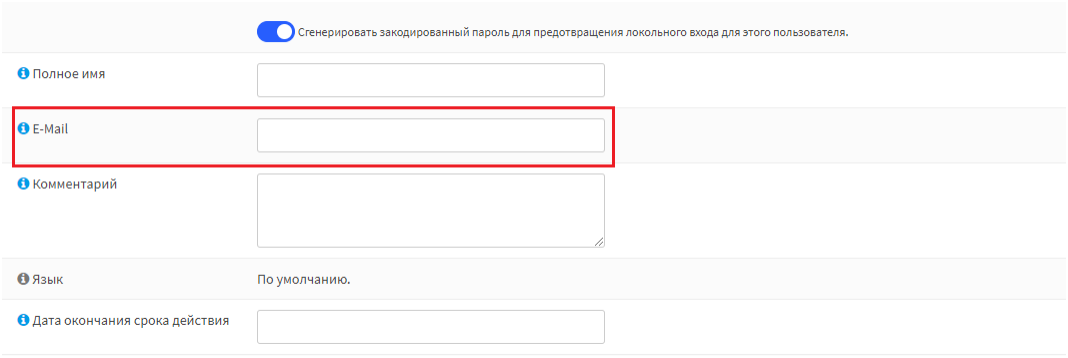


Рис. 152: E-Mail пользователя

E-Mail пользователя вводится для собственной информации пользователя

- в поле **«Комментарий»** ввести описание пользователя;

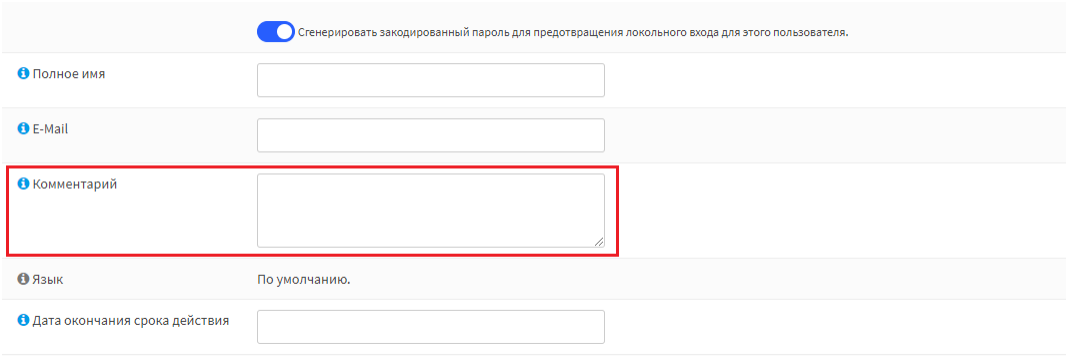


Рис. 153: Описание пользователя

Примечание

Описание пользователя вводится для собственной информации пользователя

- в поле **«Язык»** ознакомиться с настройкой языка по умолчанию;

- в поле **«Дата окончания срока действия»** ввести дату окончания срока действия в формате ДД.ММ.ГГГГ;

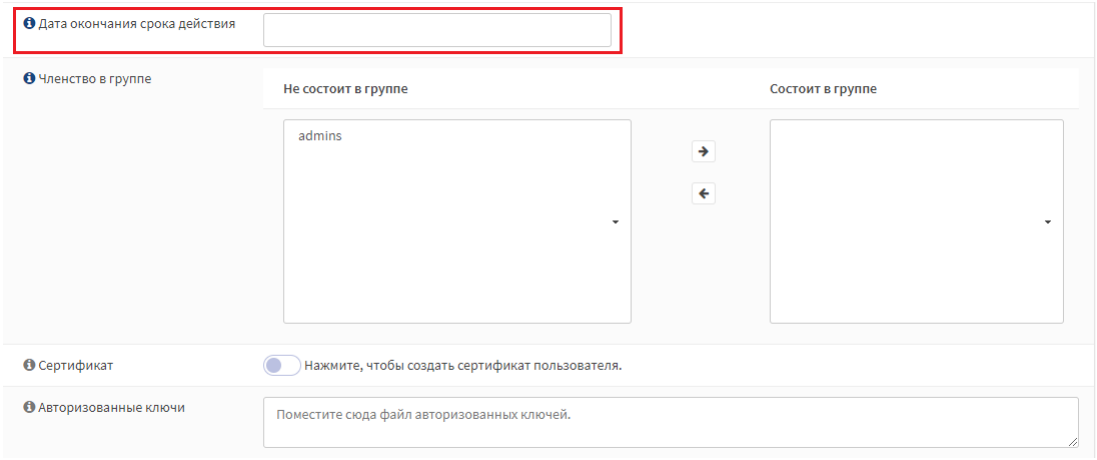


Рис. 154: Дата окончания срока действия

Примечание

Необходимо оставить поле пустым при отсутствии у учетной записи пользователя срока действия

- в поле «Членство в группе» назначить в каких группах состоит пользователь, используя команды «Добавить пользователей» и «Удалить пользователей»;

Примечание

Определение происходит путем добавления групп в соответствующие колонки

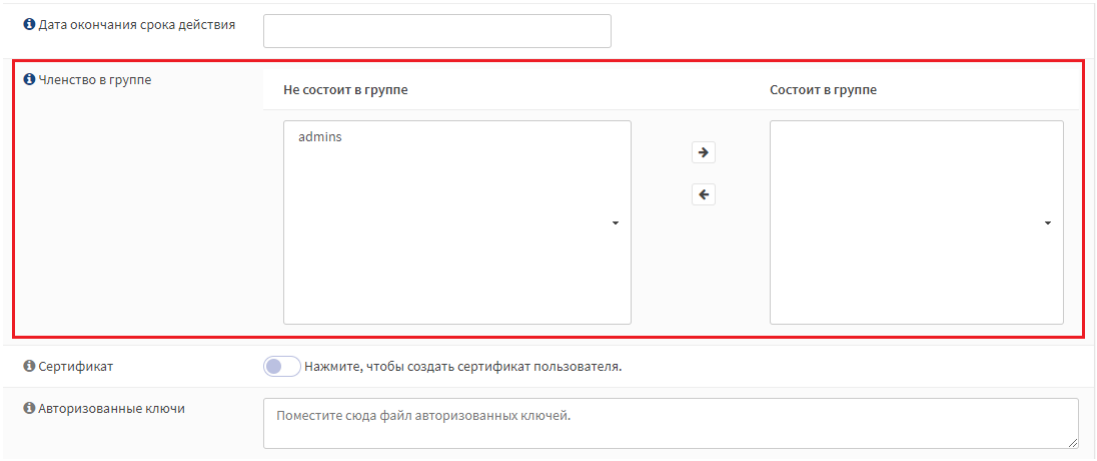


Рис. 155: Членство в группе

- в поле **«Сертификат»** установить переключатель в случае необходимости получения сертификата пользователя;
- в поле **«Авторизованные ключи»** поместить файл авторизованных ключей;

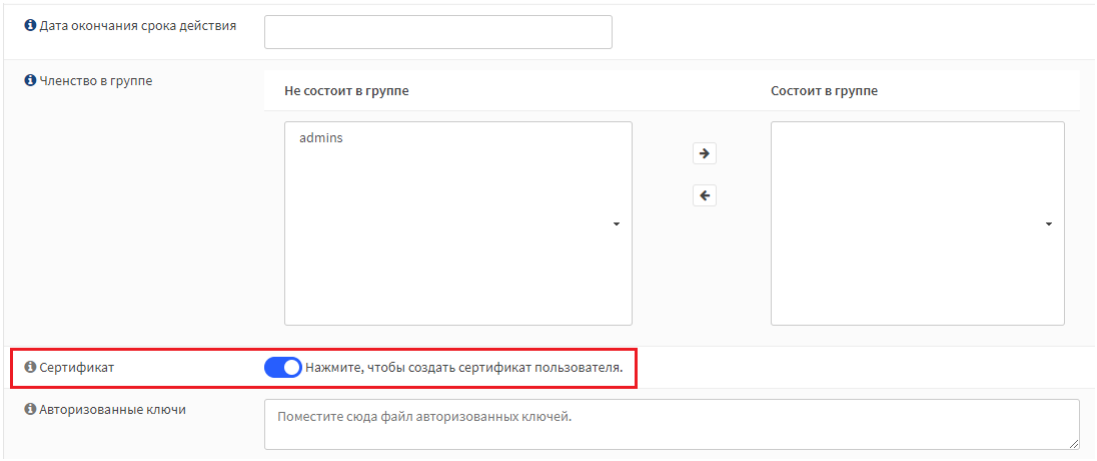


Рис. 156: Сертификат

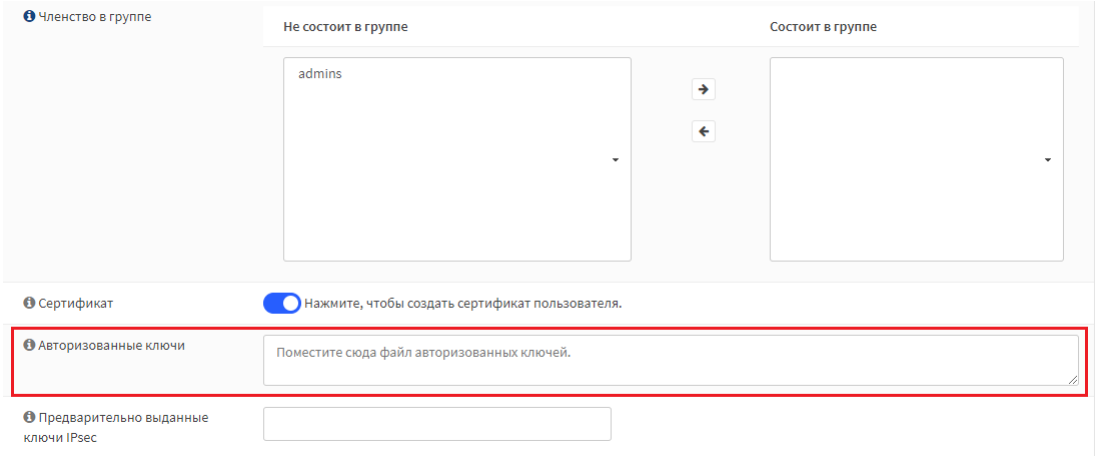


Рис. 157: Авторизованные ключи

- в поле **«Предварительно выданные ключи IPsec»** указать ключи IPsec;

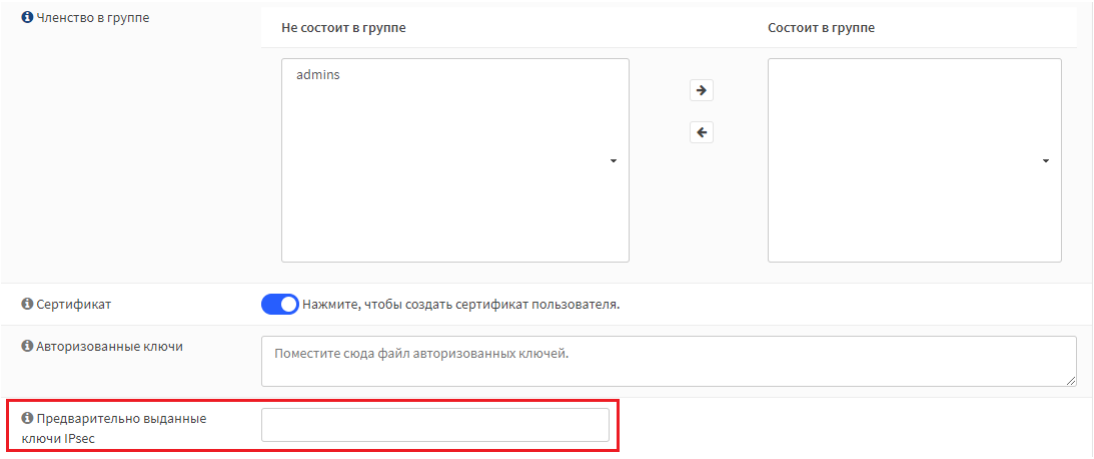
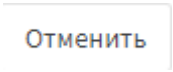


Рис. 158: Ключи IPsec

- нажать кнопку **«Сохранить»**  в случае сохранения данных учетной записи пользователя.

- нажать кнопку **«Сохранить и вернуться»**  в случае сохранения данных учетной записи пользователя и возврата к таблице пользователей.

- нажать кнопку **«Отменить»**  в случае отмены внесенных данных и возврата к таблице пользователей.

Для редактирования привилегий членов группы необходимо:

- нажать кнопку редактирования данных пользователя;

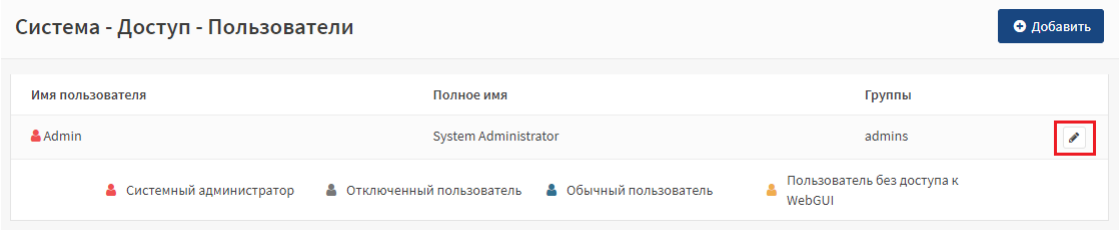


Рис. 159: Редактирование данных пользователя

- в поле **«Действующие привилегии»** нажать кнопку **«Редактировать привилегии»**;
- в открывшемся окне, используя переключатель, необходимо разрешить/запретить доступ пользователя ко всем или к определенным вкладкам устройства;
- в поле **«Сертификаты пользователя»** нажать кнопку **«Создать или соединить сертификат пользователя»**;
- в поле **«Ключи API»** нажать кнопку **«Создать API ключ»**.

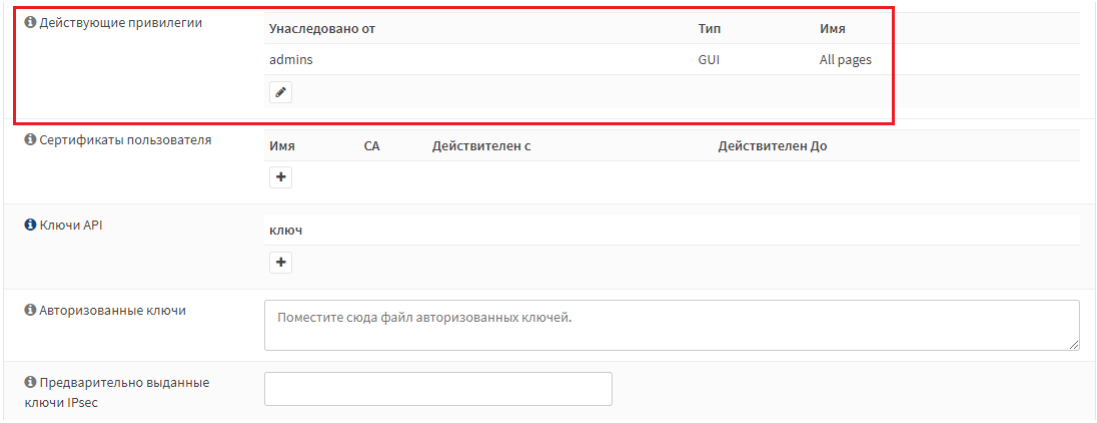


Рис. 160: Действующие привилегии

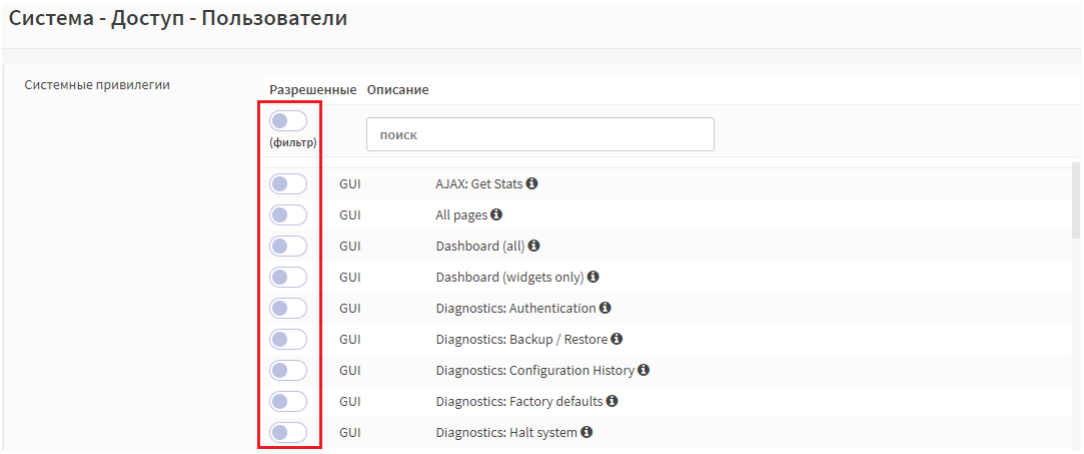


Рис. 161: Доступ к вкладкам устройства

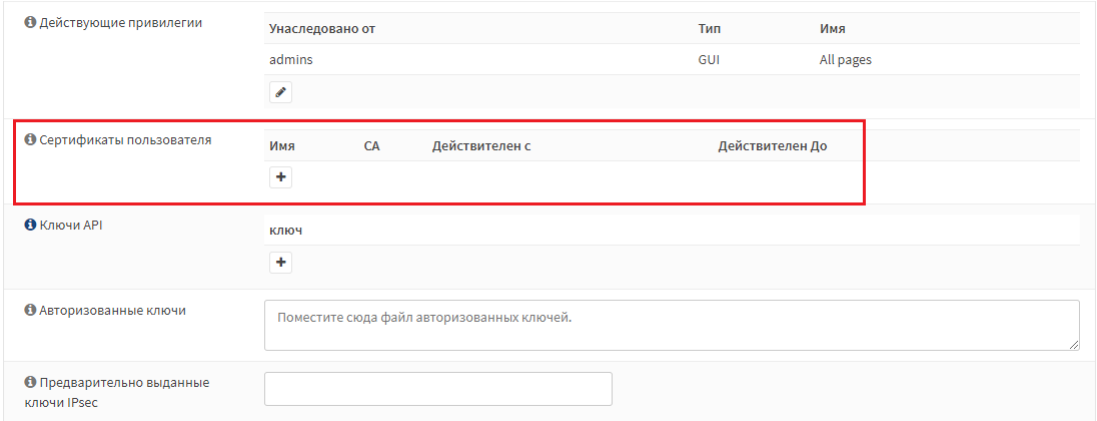


Рис. 162: Сертификаты пользователя

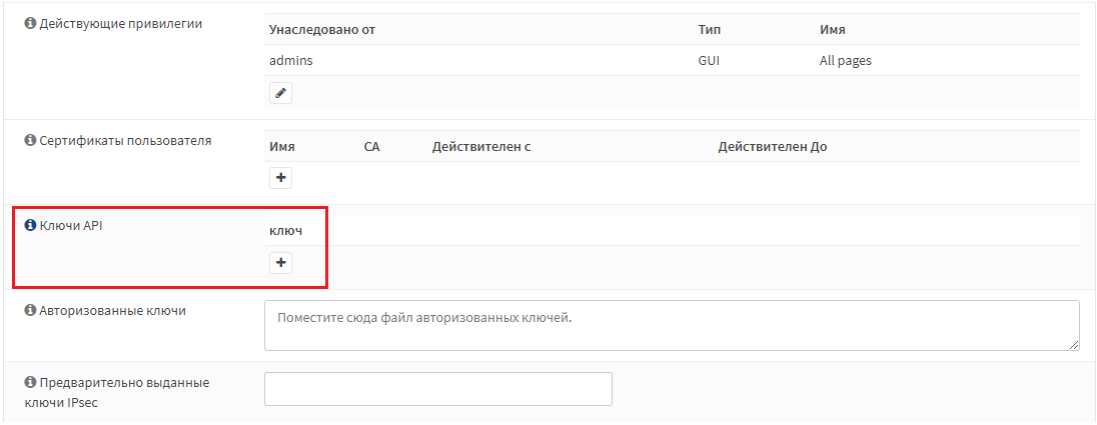


Рис. 163: Добавление ключей API

Примечание

Ключ API будет автоматически сгенерирован и подставлен в соответствующее поле

Группы

Создание группы

В разделе **«Группы»** необходимо:

- в поле **«Имя группы»** ввести имя группы;

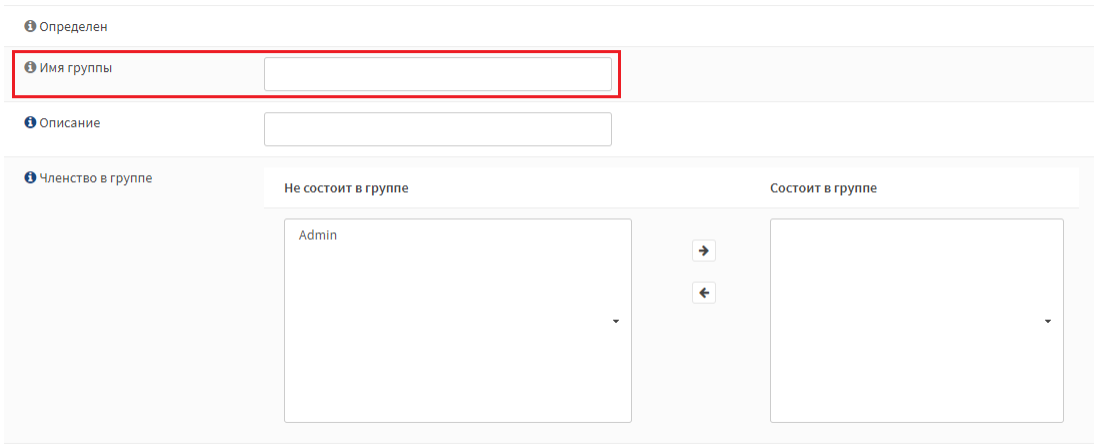


Рис. 164: Имя группы

- в поле **«Описание»** ввести описание группы;

Примечание

Описание группы вводится для собственной информации пользователя

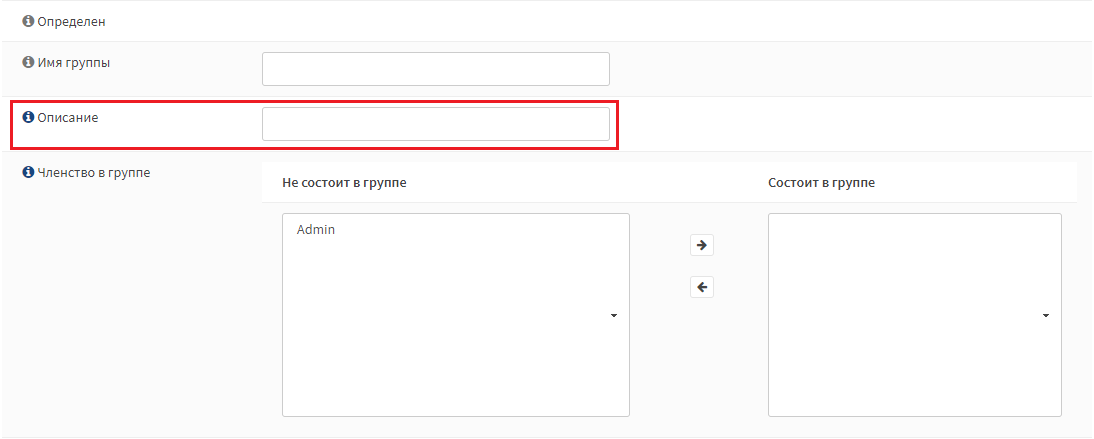


Рис. 165: Описание группы

- в поле «Членство в группе» назначить в каких группах состоит пользователь, используя команды «Добавить пользователей» и «Удалить пользователей»;

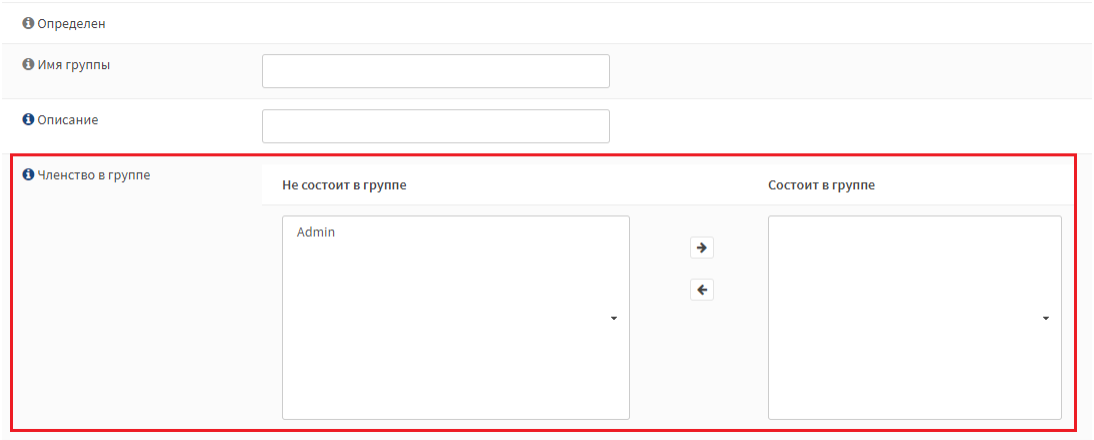


Рис. 166: Членство в группе

Примечание

Определение происходит путем добавления пользователей в соответствующие колонки

- в поле **«Присвоенные привилегии»** установить необходимые привилегии группы, нажав кнопку  ;
- в открывшемся окне **«Системные привилеги»** установить с помощью переключателя необходимые привилегии группы,;
- нажать кнопку **«Сохранить»** 

в случае сохранения настроек привилегий группы.

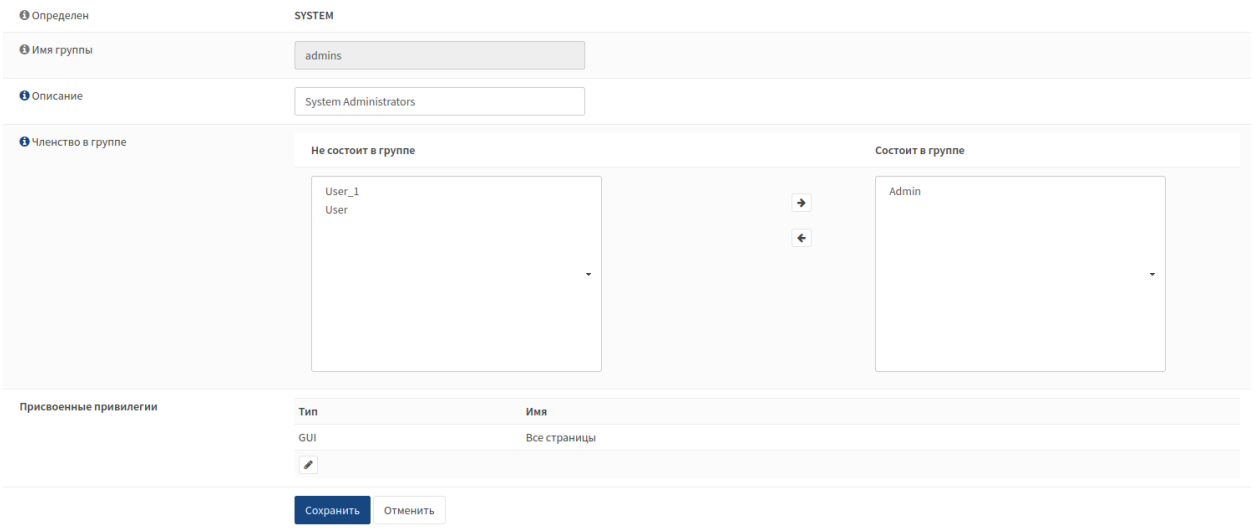


Рис. 167: Привилегии группы

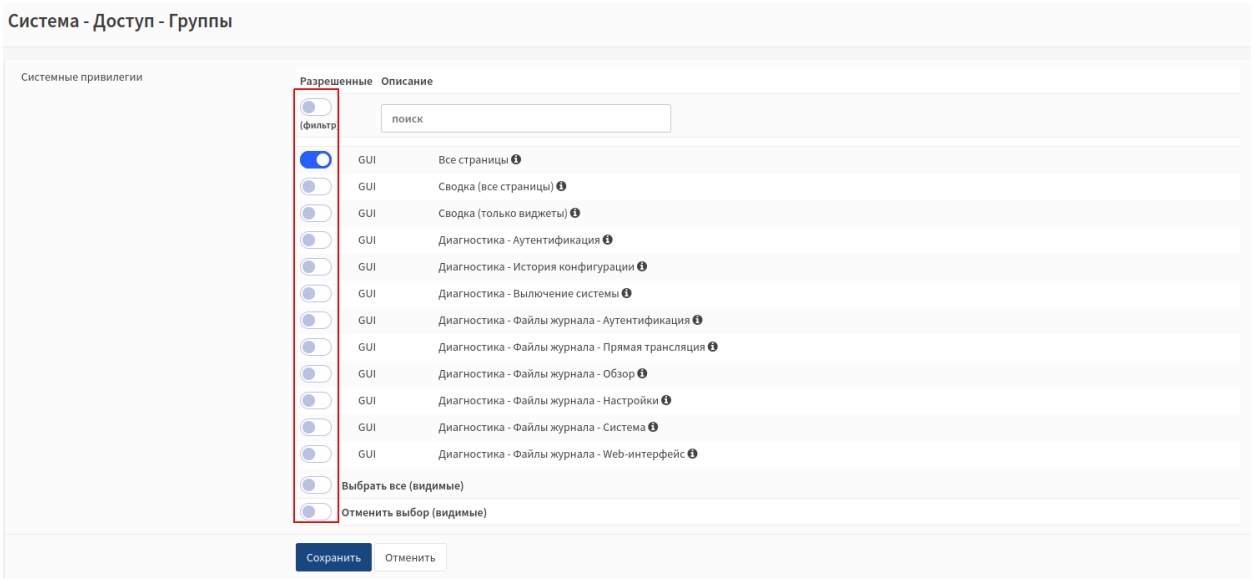


Рис. 168: Настройка привилегий группы

- нажать кнопку **«Сохранить»** 

в случае сохранения данных группы.

Серверы

LDAP

В разделе **«Серверы»** необходимо:

- в поле **«Описательное имя»** ввести описательное имя сервера;
- в поле **«Тип»** выбрать из выпадающего списка тип сервера **«LDAP»**;
- в поле **«Имя хоста или IP-адрес»** ввести имя хоста или IP-адрес;

Примечание

При использовании SSL имя хоста должно совпадать с общим именем (CN) сертификата SSL-сервера LDAP

- в поле **«Значение порта»** ввести числовое значение порта;
- в поле **«Транспортный протокол»** выбрать из выпадающего списка один из протоколов, соответствующих таблице;

Таблица 56: Протоколы

Протокол
TCP
StartTLS
SSL

Примечание

При выборе протокола StartTLS или SSL следует настроить необходимые частные центры сертификации в разделе **«Система»** - **«Доверенные сертификаты»**

- в поле **«Версия протокола»** выбрать из выпадающего списка одну из версий протокола LDAP, соответствующую таблице;

Таблица 57: Протоколы

Версия протокола
2
3

- в поле **«Привязать параметры доступа»** ввести **«Уникальное имя пользователя»** и **«Пароль»** в соответствующие поля;

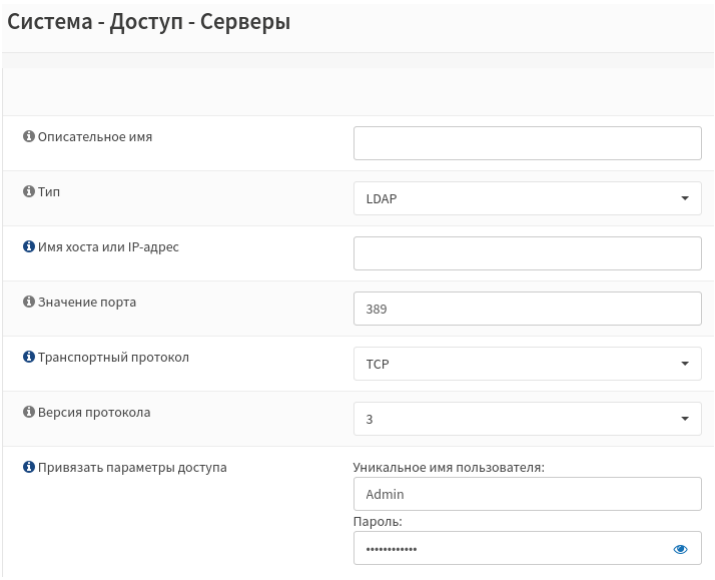


Рис. 169: Последующие настройки LDAP сервера

Примечание

При использовании анонимных привязок для преобразования уникальных имен необходимо оставить поле пустым

- в поле **«Область поиска»** выбрать из выпадающего списка одну из областей поиска, соответствующую таблице;

Таблица 58: Область поиска

Область поиска
Единичный уровень
Целое поддерево

- в поле **«Базовое отличительное имя (DN)»** ввести доменное имя;
- в поле **«Контейнеры для аутентификации»** ввести разделенный точкой с запятой список отличительных имен, содержащих компоненты DC;

Совет

Например: DC=components,OU=Freelancers,O=Company,DC=example,DC=com;

- в поле **«Расширенный запрос»** ввести расширенный запрос;

Совет

Например: &(objectClass=inetOrgPerson)(mail=*@example.com)

- в поле **«Начальный шаблон»** выбрать из выпадающего списка один из шаблонов, соответствующих таблице;

Таблица 59: Начальные шаблоны

Начальные шаблоны
OpenLDAP
Microsoft AD
Novell eDirectory

- в поле **«Атрибут присвоения имени пользователю»** ввести атрибут присвоения имени пользователю;

Совет

«cn» для шаблона OpenLDAP и Novell eDirectory, а «sAMAccountName» для шаблона Microsoft AD

- в поле **«Читать свойства»** установить переключатель и необходимости не только привязаться к удаленному серверу, но и также извлечь свойства объектов;
- в поле **«Синхронизировать группы»** установить переключатель в случае необходимости синхронизировать группы

Примечание

Синхронизировать группы, указанные атрибутом memberOf, после входа в систему

Примечание

Опция **«Синхронизировать группы»** требует включения опции **«Читать свойства»**

- в поле **«Ограничить локальной группы»** выбрать из выпадающего списка группы, которые будет использовать сервер;

Совет

Когда группы выбраны, можно назначить пользователю неназначенные группы вручную

- в поле **«Совпадение без учета регистра»** установить переключатель в случае необходимости разрешить ввод смешанного регистра при сборе локальных пользовательских настроек;
- нажать кнопку **«Сохранить»** 

в случае сохранения данных сервера.

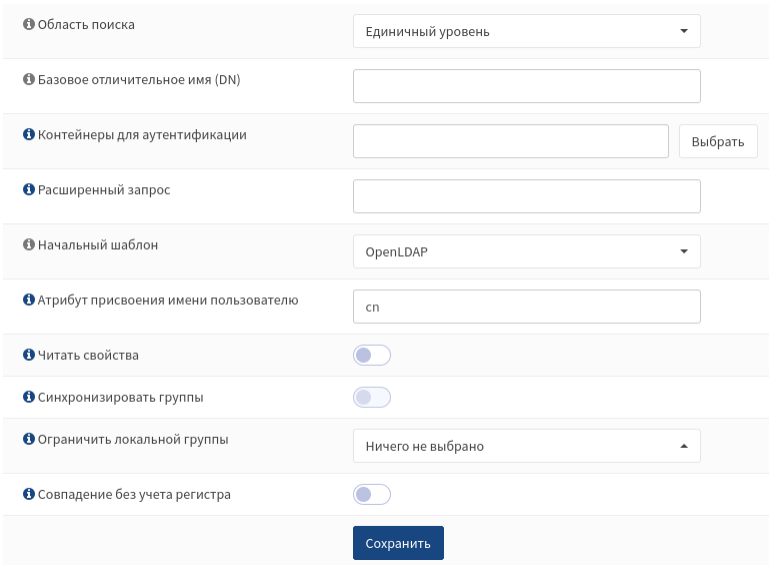


Рис. 170: Настройка LDAP сервера

Radius

В разделе **«Серверы»** необходимо:

- в поле **«Описательное имя»** ввести описательное имя сервера;
- в поле **«Тип»** выбрать из выпадающего списка тип сервера **«Radius»**;
- в поле **«Имя хоста или IP-адрес»** ввести имя хоста или IP-адрес;
- в поле **«Общий секретный ключ»** ввести общий секретный ключ;
- в поле **«Предложенные службы»** выбрать из выпадающего списка одну службу, соответствующую таблице;

Таблица 60: Предложенные службы

Предложенные службы
Аутентификация и учет
Аутентификация

- в поле **«Значение порта аутентификации»** ввести числовое значение порта аутентификации;
- в поле **«Значение порта учета»** (при выборе службы **«Аутентификация и учет»** в поле **«Предложенные службы»**) ввести числовое значение порта учета;
- в поле **«Тайм-аут аутентификации»** ввести числовое значение тайм-аута аутентификации;

Примечание

Это значение определяет сколько времени в секундах сервер RADIUS отвечает на запрос аутентификации

Примечание

Если поле оставлено пустым, то значение по умолчанию равно 5 секундам

Совет

Если используется интерактивная система двухфакторной аутентификации, необходимо увеличить тайм-аут, чтобы определить, сколько времени займет получение и ввод токена для пользователя

- нажать кнопку **«Сохранить»** 

в случае сохранения данных сервера.

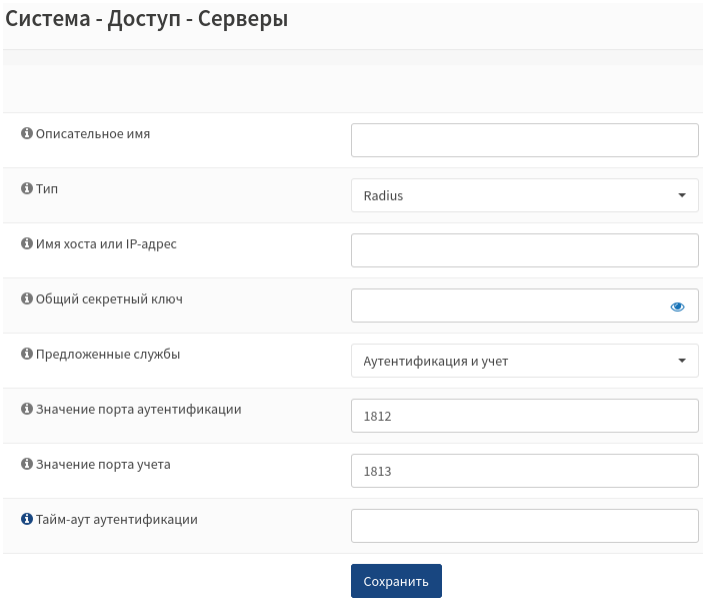


Рис. 171: Настройка Radius сервера

Средство проверки

Для проведения проверки необходимо:

- в поле **«Сервер аутентификации»** выбрать из выпадающего списка один из серверов, соответствующих таблице;

Таблица 61: Сервер аутентификации

Сервер аутентификации
Локальная база данных
RADIUS
LDAP

- в поле **«Имя пользователя»** ввести имя пользователя;
- в поле **«Пароль»** ввести пароль;

- нажать кнопку **«Проверка»** 

.

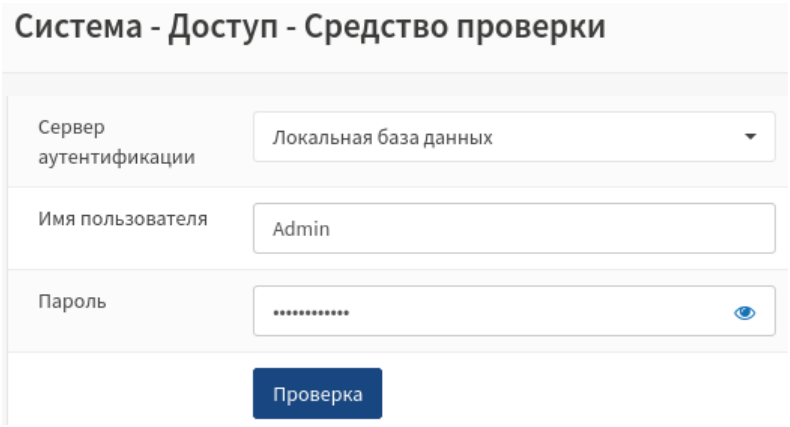


Рис. 172: Настройка средства проверки

2.7.3.2 Конфигурация

Вкладка **«Конфигурация»** дает пользователю возможность сохранять и восстанавливать конфигурацию системы, а так же просматривать историю изменений с возможностью просмотра отличий между версиями конфигурации.

Для перехода к сохранению и восстановлению конфигурации системы необходимо:

- нажать на вкладку **«Система»** - **«Конфигурация»** - **«Резервные копии»**, расположенную в левой части списка объектов управления;

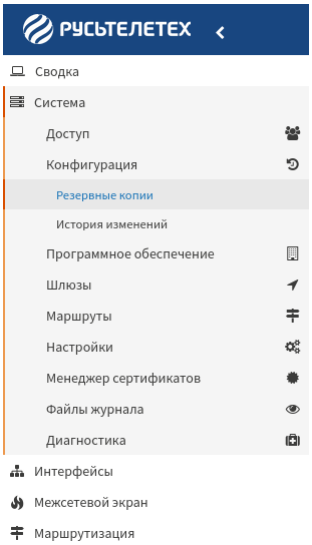


Рис. 173: Переход к сохранению и восстановлению конфигурации системы

Для перехода к просмотру истории изменений конфигурации системы необходимо:

- нажать на вкладку **«Система»** - **«Конфигурация»** - **«История изменений»**, расположенную в левой части списка объектов управления;

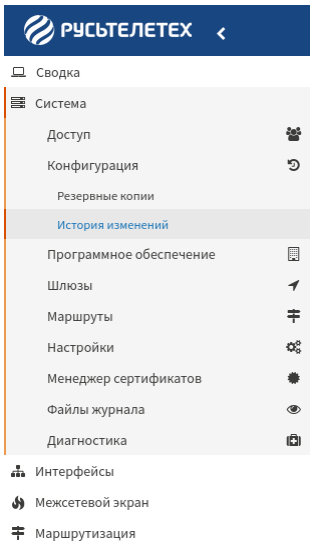


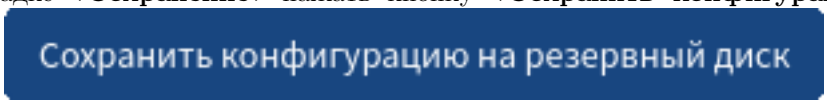
Рис. 174: Переход к просмотру истории изменений конфигурации системы

Резервные копии

Сохранение конфигурации

В разделе **«Резервные копии»** необходимо:

- на вкладке **«Сохранение»** нажать кнопку **«Сохранить конфигурацию на ПК»** 

в случае необходимости сохранения конфигурации на ПК пользователя в зашифрованном формате;
- на вкладке **«Сохранение»** нажать кнопку **«Сохранить конфигурацию на резервный диск»** 

в случае необходимости скопируйте конфигурацию на зарезервированный SSD-диск. Если что-то случится с основным SSD.

Совет

Резервный диск будет содержать всю сохраненную конфигурацию;

Восстановление конфигурации

В разделе **«Резервные копии»** на вкладке **«Восстановить конфигурацию»** необходимо:

- в поле **«Восстановить зону»** выбрать из выпадающего списка одну из восстанавливаемых зон, соответствующих таблице;

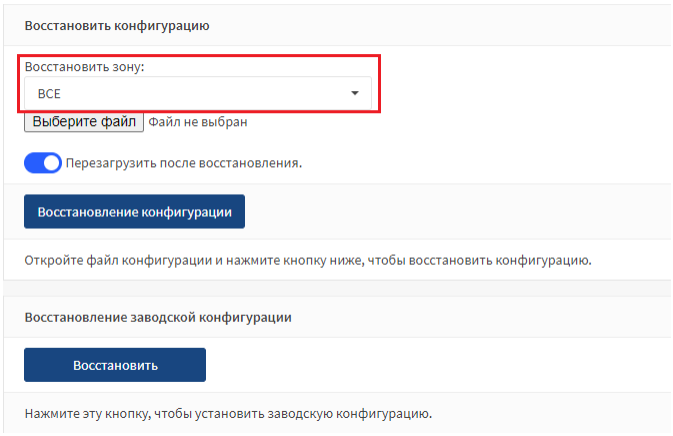


Рис. 175: Восстановление зоны

Таблица 62: Зоны

Зоны
ВСЕ
Центр сертификации SSL
Сертификаты SSL
Правила межсетевого экрана
Шлюзы
Интерфейсы
Преобразование сетевых адресов
Сетевое время
OpenVPN
Системный журнал

- нажать кнопку **«Выберите файл»**;
- в открывшемся окне выбрать необходимый файл;
- нажать кнопку **«Открыть»**;
- в поле **«Перезагрузить после восстановления.»** установить переключатель в случае необходимости перезагрузить систему после восстановления;
- нажать кнопку **«Восстановление конфигурации»** 

.

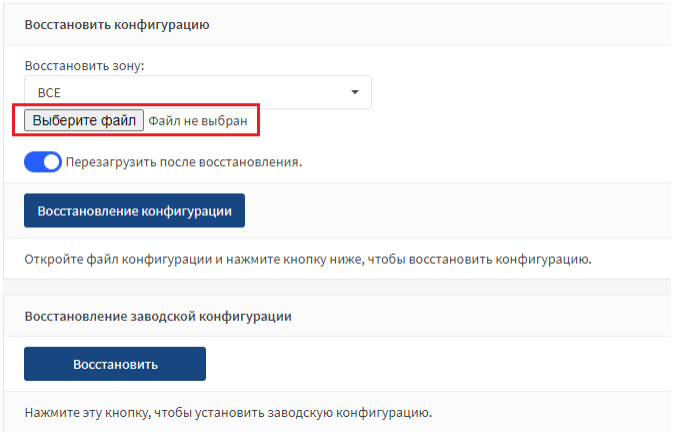


Рис. 176: Выбор файла

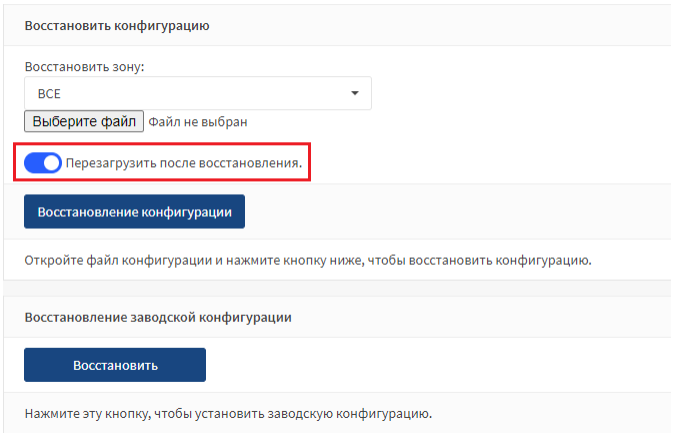


Рис. 177: Выбор перезагрузки системы

Восстановление заводской конфигурации

Для восстановления заводской конфигурации необходимо:

- нажать кнопку **«Восстановить»** 

.

История изменений

Количество резервных копий

В разделе **«Количество резервных копий»** необходимо:

- в поле **«Количество резервных копий»** ввести числовое значение предыдущих конфигураций, которые будут храниться в кэше локальной резервной копии;

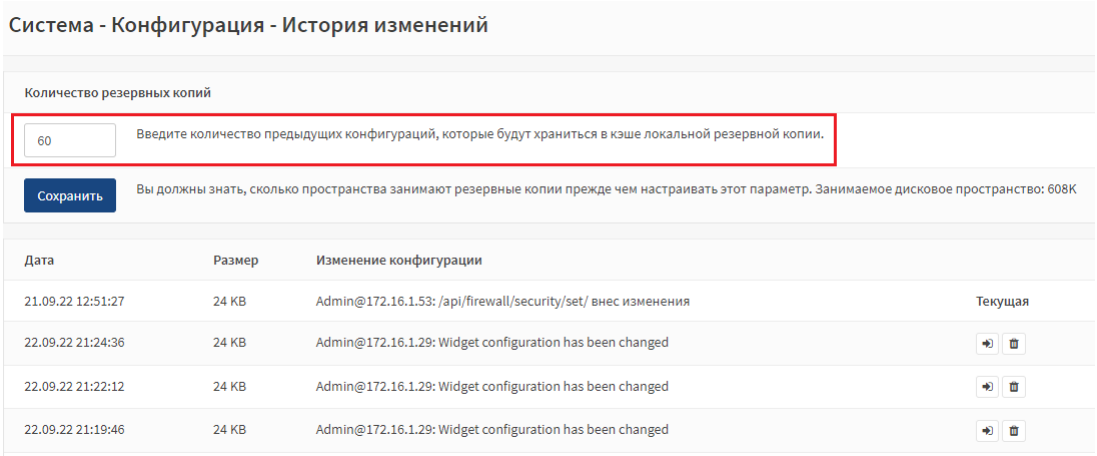


Рис. 178: Количество резервных копий

- нажать кнопку **«Сохранить»** 

.

Совет

Необходимо знать, сколько пространства занимают резервные копии прежде чем настраивать этот параметр. Занимаемое дисковое пространство: 220K

История изменений

В разделе **«История изменений»** содержится таблица конфигураций системы

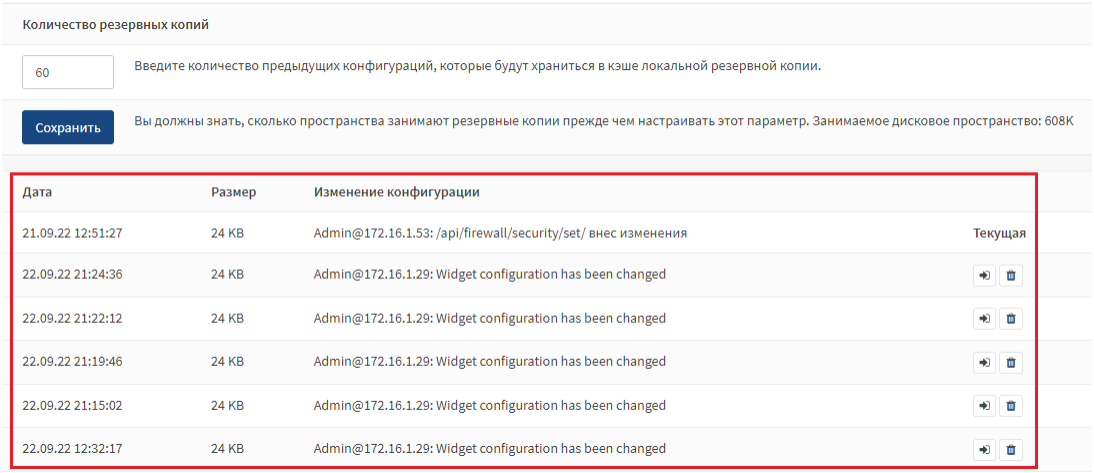


Рис. 179: Таблица конфигураций системы

Для возвращения к необходимой конфигурации следует:

- в крайней правой колонке напротив необходимой конфигурации нажать кнопку **«Вернуться к этой конфигурации**.

Для удаления необходимой конфигурации следует:

- в крайней правой колонке напротив необходимой конфигурации нажать кнопку **«Удалить эту резервную копию**.

2.7.3.3 Программное обеспечение

Для перехода к просмотру параметров программного обеспечения необходимо:

- нажать на вкладку **«Система»** - **«Программное обеспечение»** - **«Статус»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться вкладка с параметрами программного обеспечения;

Для перехода к настройкам программного обеспечения необходимо:

- нажать на вкладку **«Система»** - **«Программное обеспечение»** - **«Настройки»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться вкладка с настройками программного обеспечения;

Для перехода к активации необходимой лицензии необходимо:

- нажать на вкладку **«Система»** - **«Программное обеспечение»** - **«Лицензия»**, расположенную в левой части списка объектов управления;

Для перехода к списку изменений необходимо:

- нажать на вкладку **«Система»** - **«Программное обеспечение»** - **«Журнал изменений»**, расположенную в левой части списка объектов управления;

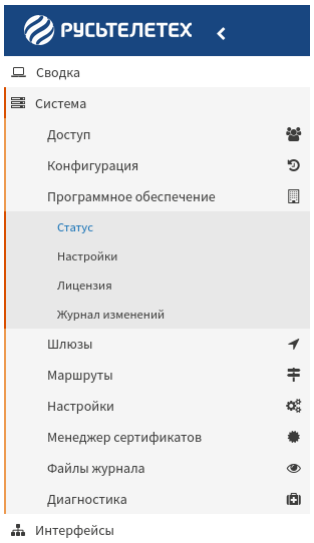


Рис. 180: Переход к параметрам программного обеспечения

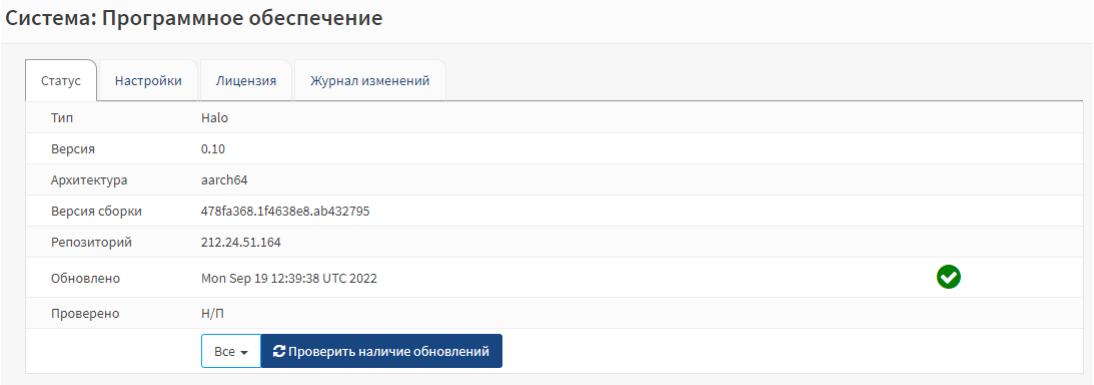


Рис. 181: Вкладка с программного обеспечения

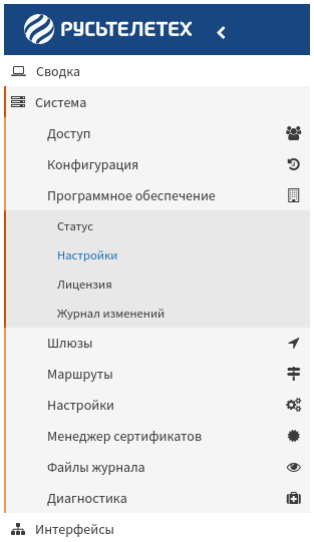


Рис. 182: Переход к настройкам программного обеспечения

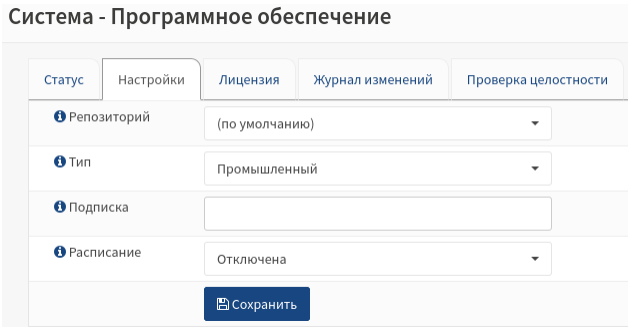


Рис. 183: Вкладка с настройками прошивки

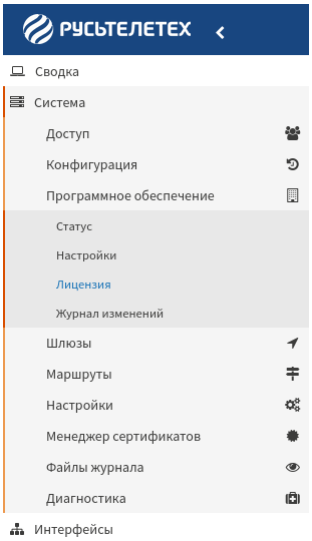


Рис. 184: Переход к активации лицензии

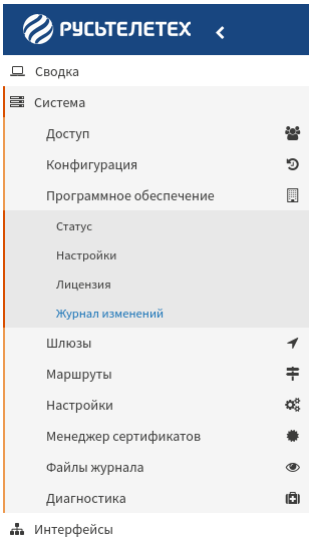


Рис. 185: Переход к списку изменений

Статус

На вкладке **«Статус»** отражены параметры программного обеспечения, соответствующие таблице.

Таблица 63: Параметры программного обеспечения

Параметр	Значение
Тип	Тип программного обеспечения
Версия	Версия программного обеспечения
Архитектура	Разрядность системы
Версия сборки	Hash изменения
Репозиторий	Адрес хранения программного обеспечения
Обновлено	Дата и время обновления
Проверено	Дата и время последней проверки

Для проверки наличия обновлений необходимо:

- на вкладке **«Статус»** выбрать из выпадающего списка один из типов, соответствующих таблице.

Таблица 64: Типы обновлений

Тип	Значение
Все	Все обновления
Базовая	Обновление функциональности
Безопасность	Обновление безопасности

- нажать кнопку **«Проверить наличие обновлений»** 

.

Настройки

Для настройки обновления программного обеспечения необходимо:

- в поле **«Репозиторий»** выбрать из выпадающего списка один из источников программного обеспечения, соответствующих таблице;

Таблица 65: Выбор источника программного обеспечения

Выбор источника программного обеспечения
(по умолчанию)
Альтернативный репозиторий REFOS

- в поле **«Тип»** выбрать из выпадающего списка тип **«Промышленный»**;
- в поле **«Подписка»** предоставить ключ подписки;
- в поле **«Расписание»** выбрать из выпадающего списка один из временных интервалов, соответствующих таблице;

Таблица 66: Выбор временных интервалов

Выбор временных интервалов
Отключена
Ежедневно
Еженедельно
Ежемесячно

- нажать кнопку **«Сохранить»** 

.

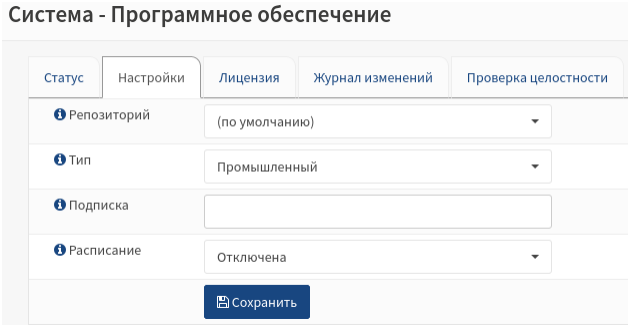


Рис. 186: Настройка обновления программного обеспечения

Лицензия

На вкладке *«Лицензирование»* представлен актуальный список лицензий и их описание.

Для активации лицензии необходимо:

- нажать кнопку  в колонке **«Действие»**.

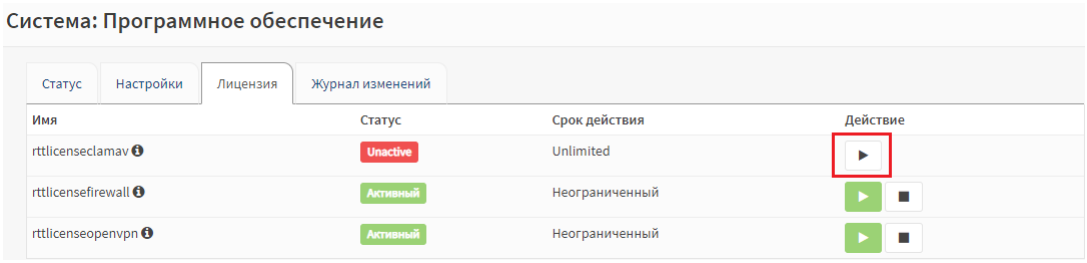


Рис. 187: Активация лицензии

- в открывшемся окне необходимо:
- в поле **«Тип активации лицензии»** выбрать из выпадающего необходимый тип активации лицензии;

Примечание

Тип активации **«Локальный»** - для активации без доступа к интернету

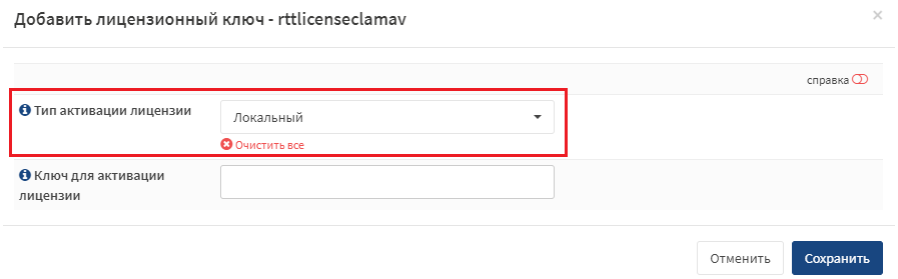


Рис. 188: Выбор необходимого типа активации лицензии

- в поле **«Ключ для активации лицензии»** введите лицензионный ключ активации;

Примечание

Ключ должен быть длинной 64 символа

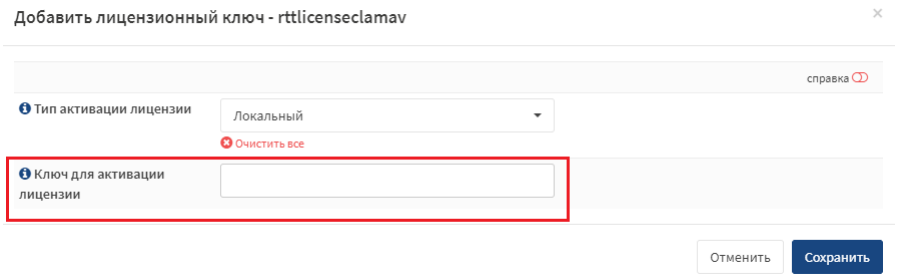


Рис. 189: Ввод ключа

- нажать кнопку 

для вступления настроек в силу;
- активная лицензия соответствует рисунку.

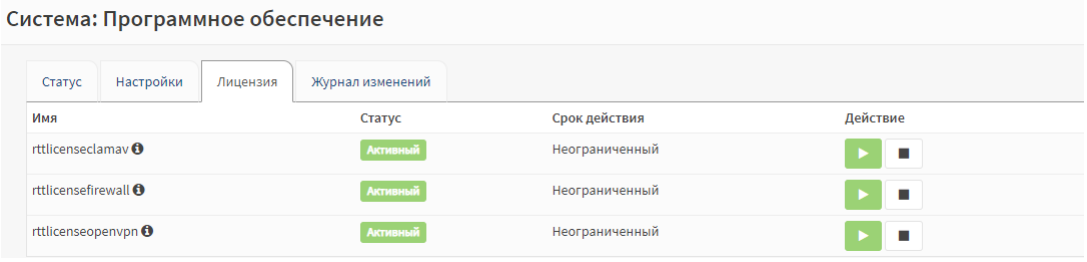


Рис. 190: Активная лицензия

Журнал изменений

Вкладка **«Журнал изменений»** содержит журнал изменений программного обеспечения

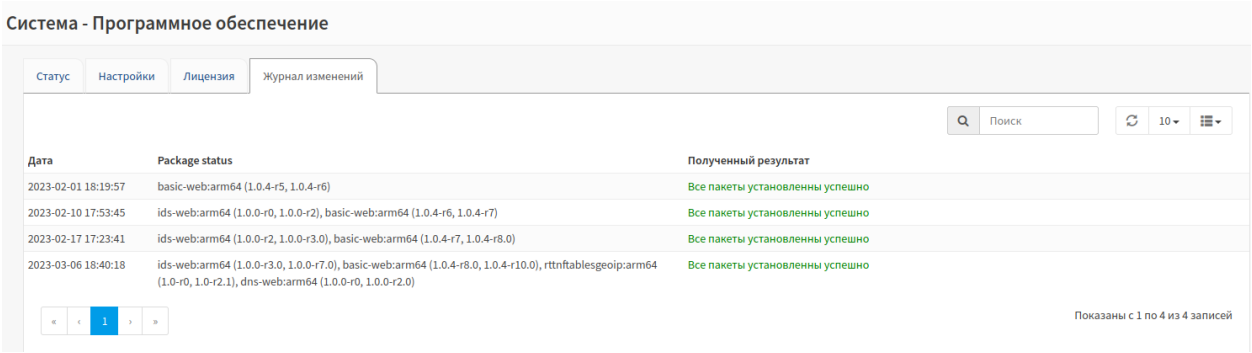


Рис. 191: Журнал изменений

2.7.3.4 Шлюзы

Для перехода к настройкам одиночного шлюза необходимо:

- нажать на вкладку **«Система»** - **«Шлюзы»** - **«Одиночный»**, расположенную в левой части списка объектов управления;

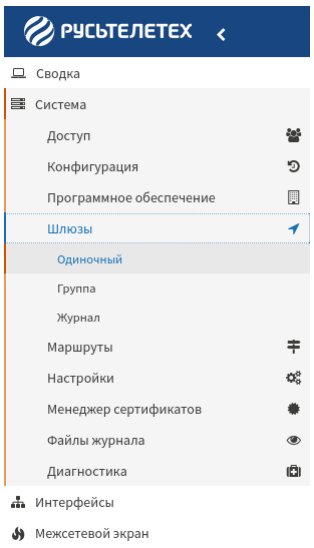


Рис. 192: Переход к настройкам одиночного шлюза

- в правой части экрана появится таблица одиночных шлюзов;
- нажать кнопку **«Добавить»** 

.

Для вступления сконфигурированных настроек одиночного шлюза в силу необходимо нажать кнопку

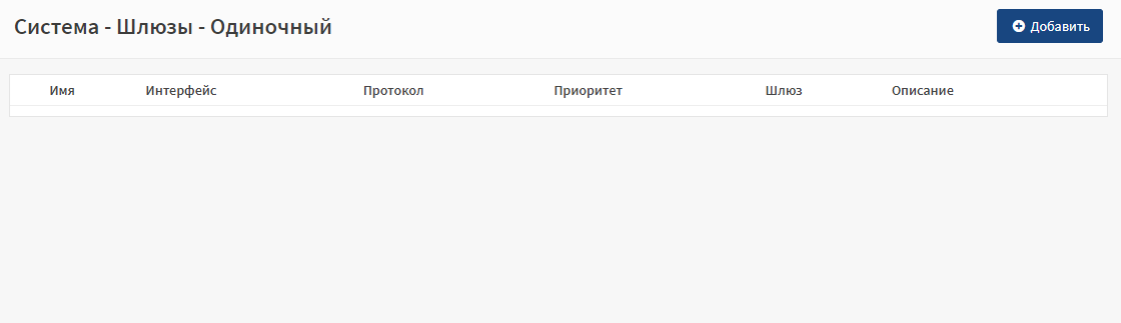


Рис. 193: Таблица одиночных шлюзов

«Применить изменения» 

.

Для перехода к настройкам группового шлюза необходимо:

- нажать на вкладку **«Система»** - **«Шлюзы»** - **«Группа»**, расположенную в левой части списка объектов управления;

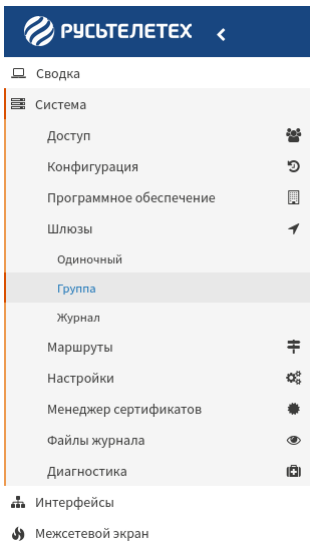


Рис. 194: Переход к настройкам группового шлюза

- в правой части экрана появится таблица групповых шлюзов;

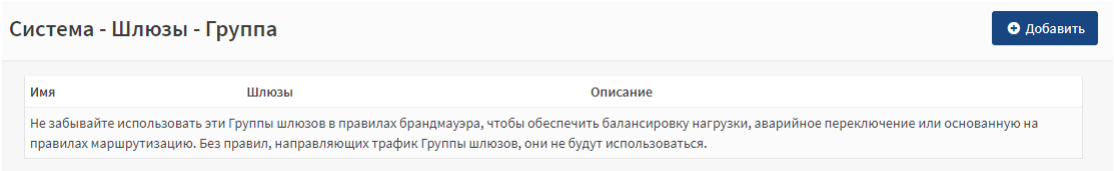
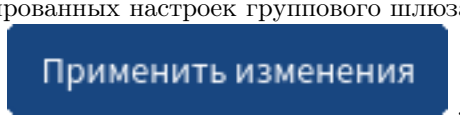


Рис. 195: Таблица групповых шлюзов

- нажать кнопку **«Добавить»** 

.

Для вступления сконфигурированных настроек группового шлюза в силу необходимо нажать кнопку **«Применить изменения»** 

.

Для перехода к журналам шлюза необходимо:

- нажать на вкладку **«Система»** - **«Шлюзы»** - **«Журнал»**, расположенную в левой части списка объектов управления;

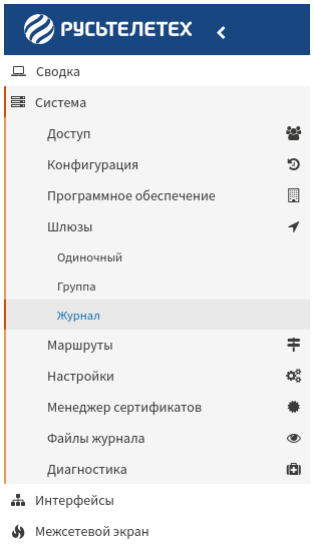


Рис. 196: Переход к журналам шлюза

- в правой части экрана появится таблица журналов шлюза;

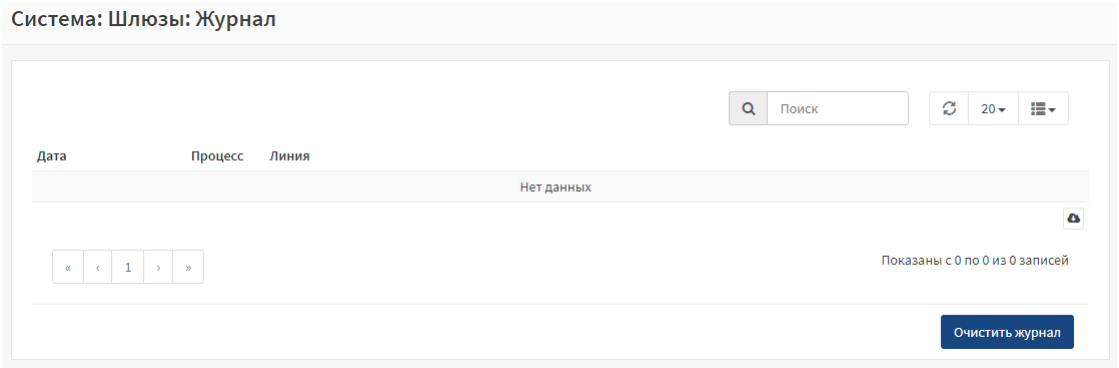


Рис. 197: Таблица журналов шлюза

Одиночный шлюз

Отключение одиночного шлюза

В окне **«Редактировать шлюз»** необходимо:

- в поле **«Отключить»** установить переключатель;
- нажать кнопку **«Сохранить»** 

.

Настройка одиночного шлюза

В окне **«Редактировать шлюз»** необходимо:

- в поле **«Имя»** указать имя шлюза;
- в поле **«Описание»** ввести описание шлюза;
- в поле **«Интерфейс»** выбрать из выпадающего списка интерфейс для применения правила;
- в поле **«Семейство адресов»** выбрать из выпадающего списка протокол интернета, соответствующий таблице, который использует этот шлюз;

Таблица 67: Выбор протокола интернета

Выбор протокола интернета
IPv4
IPv6

- в поле **«IP-адрес»** ввести IP адрес;
- в поле **«Основной шлюз»** установить переключатель в случае необходимости сделать шлюз в качестве кандидата шлюза по умолчанию;
- в поле **«Удаленный шлюз»** установить переключатель в случае необходимости дать шлюзу возможность существовать вне интерфейса подсети;
- в поле **«Отключить мониторинг шлюзов»** установить переключатель в случае необходимости рассматривать этот шлюз как всегда «работающий»;
- в поле **«Монитор IP»** ввести альтернативный адрес, который будет использоваться для мониторинга ссылки;
- в поле **«Пометить шлюз как недоступный»** установить переключатель в случае необходимости заставить шлюз считаться неработающим;
- в поле **«Приоритет»** выбрать из выпадающего списка порядок сортировки при выборе шлюза;

Совет

Чем ниже, тем важнее

- нажать кнопку **«Сохранить»** 

.

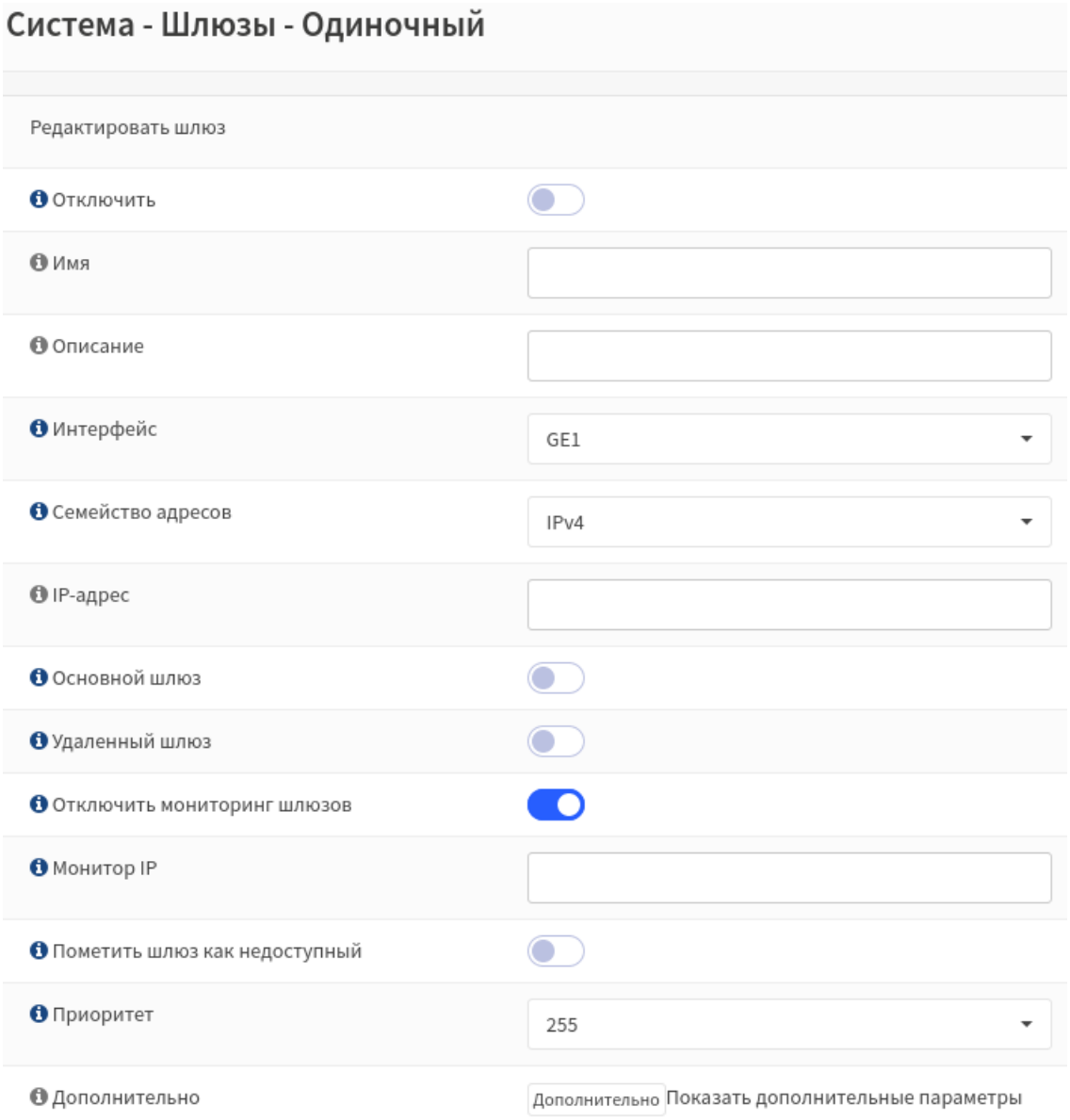


Рис. 198: Настройка одиночного шлюза

Для настройки дополнительных параметров шлюза необходимо нажать кнопку 

.

- в поле **«Весовой коэффициент»** выбрать из выпадающего списка вес (приоритет) данного шлюза при использовании в группе шлюзов;
- в поле **«Пороговое значение задержки»** установить пороги задержки в миллисекундах;

Совет

По умолчанию 200/500

- в поле **«Пороговые значения потери пакетов»** установить нижний и верхний пороги для потери пакетов в %;

Совет

По умолчанию 10/20

- в поле **«Интервал опроса»** установить, как часто будет отправляться запрос ICMP в секундах;

Совет

По умолчанию 1

- в поле **«Интервал оповещения»** установить интервал времени между предупреждениями;

Совет

По умолчанию 1

- в поле **«Временной период»** установить период времени, за который усредняются результаты;

Совет

По умолчанию 60

- в поле **«Интервал потерь»** установить интервал времени, по истечении которого пакеты считаются потерянными;

Совет

По умолчанию 2

- в поле **«Длина данных»** установить количество байтов данных для отправки;

Совет

По умолчанию 0

- нажать кнопку **«Сохранить»** 

.

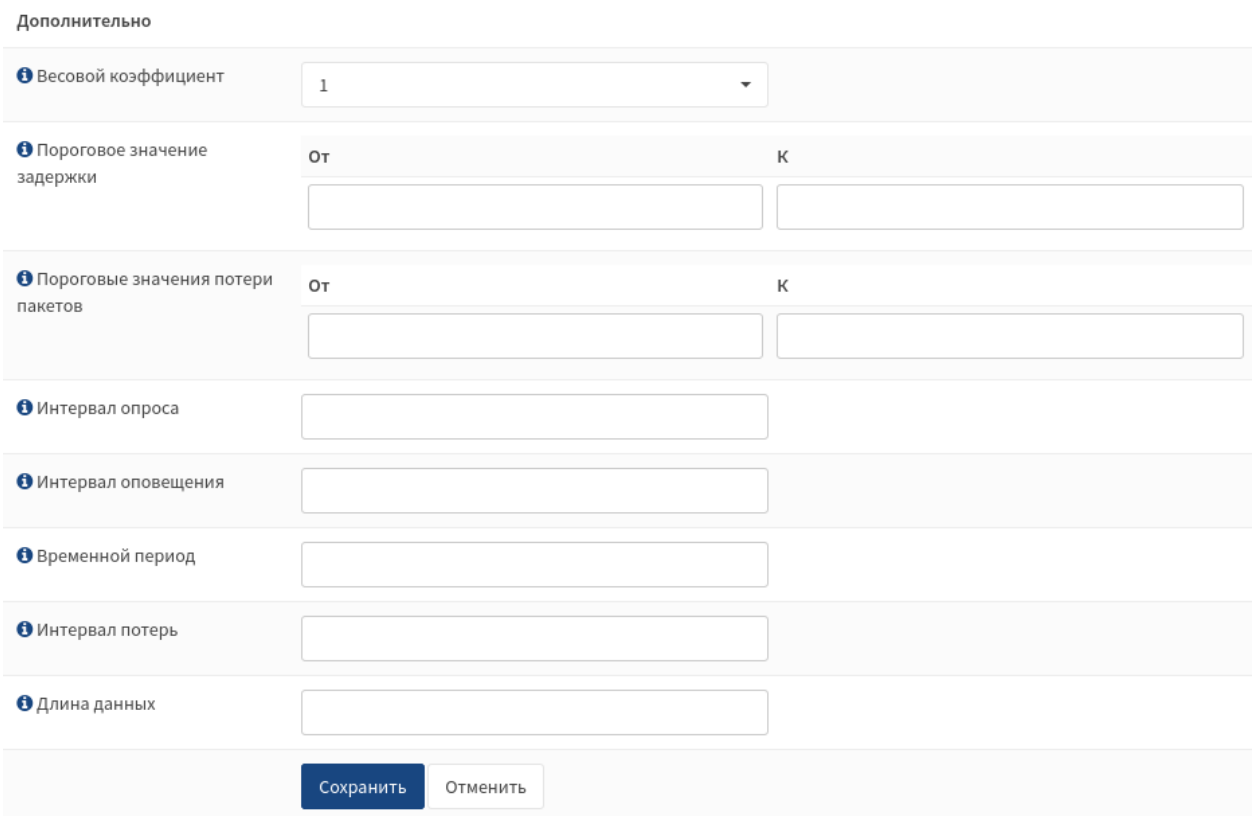


Рис. 199: Дополнительный настройки одиночного шлюза

Журнал

Для загрузки log-файла журнала необходимо нажать кнопку **«выбор загрузки»**

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

.

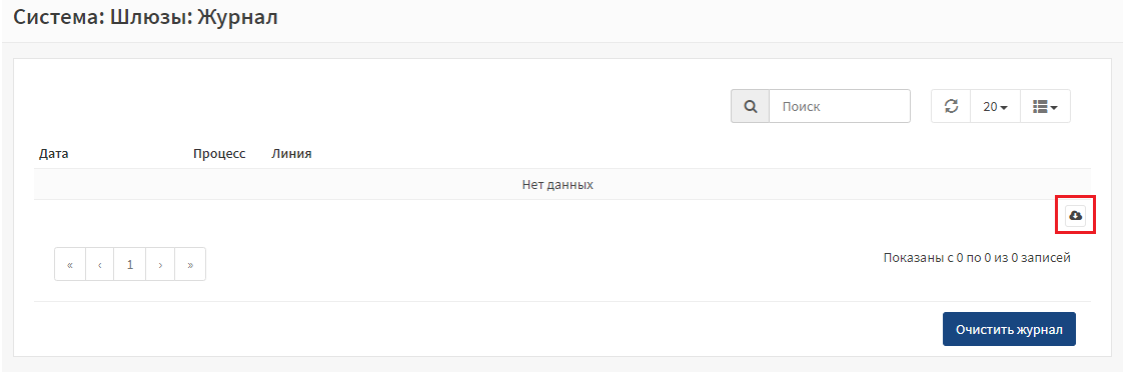


Рис. 200: Загрузка log-файла

2.7.3.5 Маршруты

Для перехода к редактированию маршрутов необходимо:

- нажать на вкладку **«Система»** - **«Маршруты»** - **«Конфигурация»**, расположенную в левой части списка объектов управления;

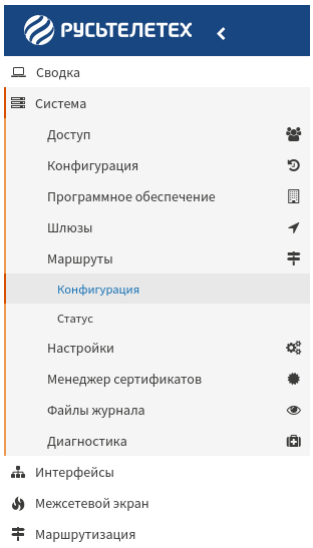


Рис. 201: Переход к редактированию маршрутов

- в правой части экрана появиться таблица маршрутов;
- нажать кнопку «+».

Для перехода к просмотру маршрутов необходимо:

- нажать на вкладку **«Система»** - **«Маршруты»** - **«Статус»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица маршрутов;

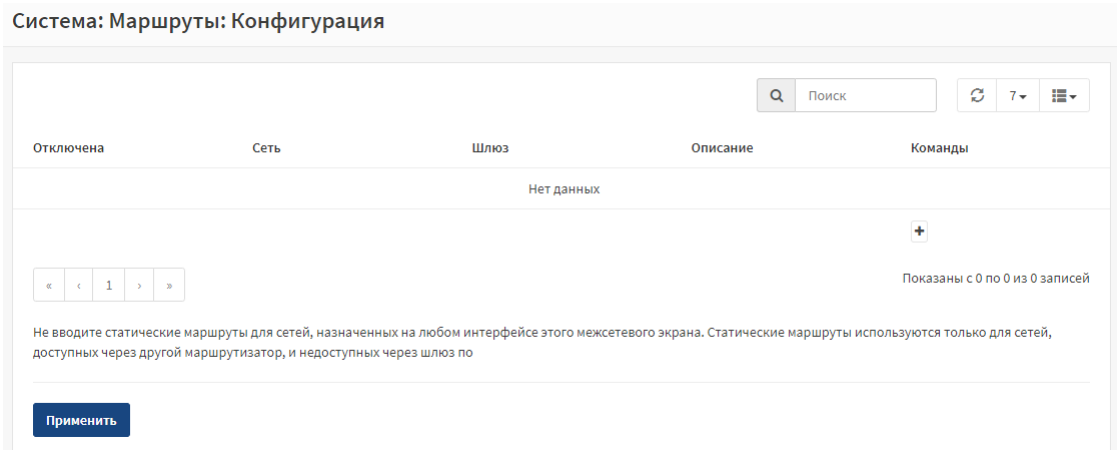


Рис. 202: Таблица маршрутов

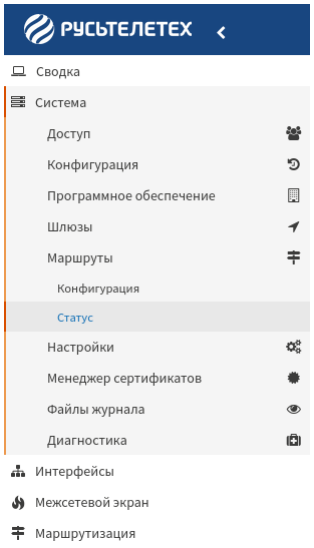


Рис. 203: Переход к просмотру маршрутов

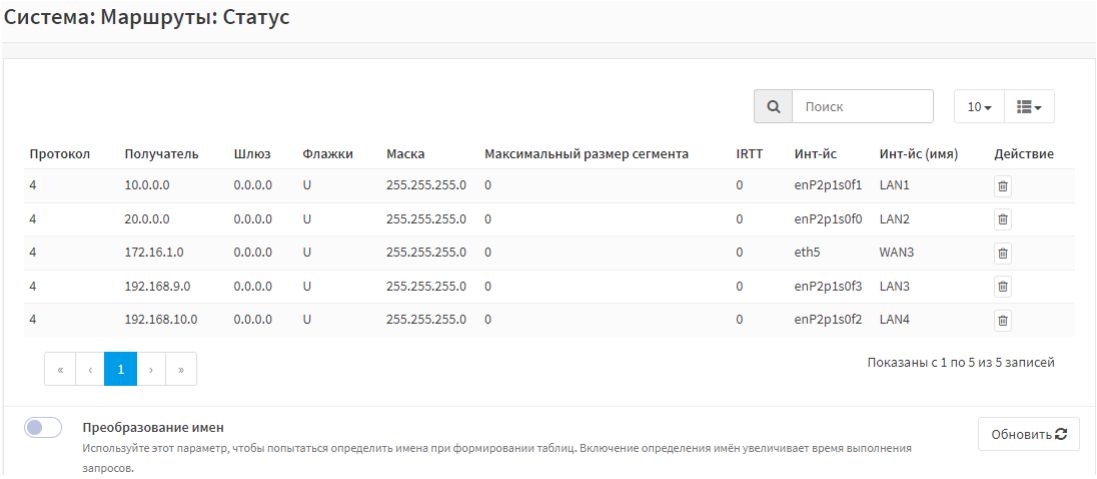


Рис. 204: Таблица маршрутов

Конфигурация

В окне **«Редактировать маршрут»** необходимо:

- в поле **«Адрес сети»** указать сеть назначения для этого статического маршрута;
- в поле **«Шлюз»** выбрать из выпадающего списка необходимый шлюз, соответствующий таблице;

Таблица 68: Шлюзы

Шлюзы
Null4-127.0.0.1
Null6 - ::1
Добавленные пользователем

Примечание

Необходимо выбрать, к какому шлюзу относится этот маршрут, или добавить новый

- в поле **«Описание»** ввести описание маршрута;
- в поле **«Отключена»** установить переключатель в случае необходимости отключения этого статического маршрута, без удаляя его из списка;
- нажать кнопку **«Сохранить»** 

.

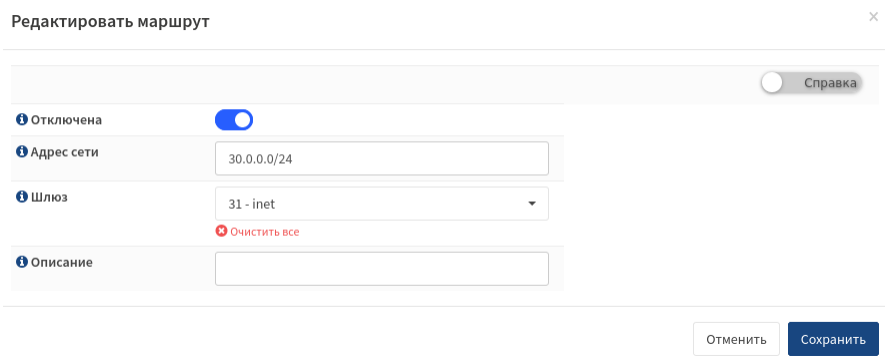


Рис. 205: Отключение маршрута

Статус

Раздел **«Статус»** включает в себя таблицу маршрутов, состоящую из следующих колонок:

- **«Протокол»** - содержит протокол;
- **«Получатель»** - содержит адрес получателя пакетов;
- **«Шлюз»** - содержит адрес шлюза;
- **«Флажки»** - содержит флаги;
- **«Маска»** - содержит маску;

- **«Максимальный размер сегмента»** - содержит максимальный размер сегмента;
- **«IRTT»** - Isochronous Round-Trip Time;
- **«Инт-йс»** - содержит имя интерфейса в системе;
- **«Инт-йс (имя)»** - содержит имя интерфейса;
- **«Действие»** - содержит список производимых действий.

Для обновления таблицы маршрутов необходимо нажать кнопку **«Обновить»**

.

Для определения имен при формировании таблиц необходимо установить переключатель **«Преобразование имен»**.

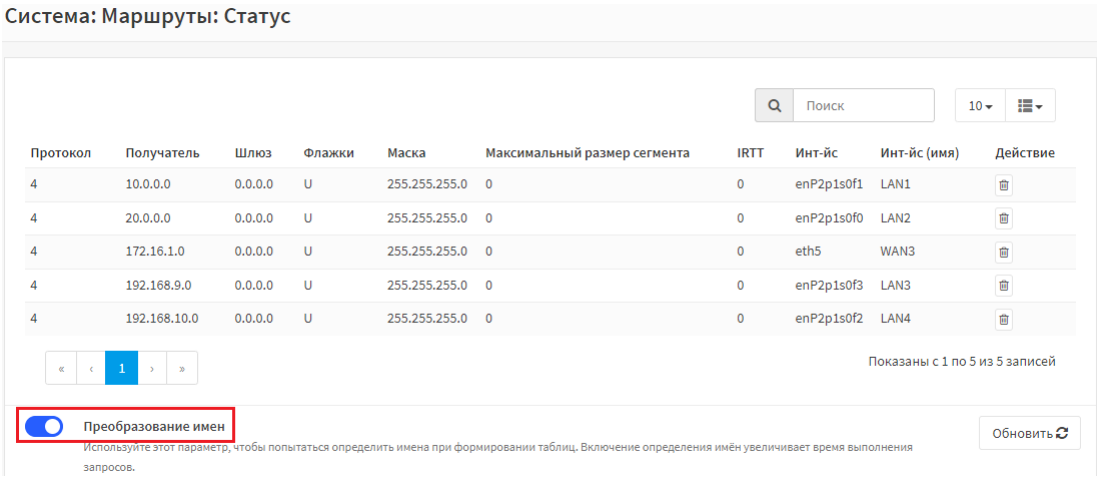


Рис. 206: Преобразование имен

Примечание

Включение определения имён увеличивает время выполнения запросов

2.7.3.6 Настройки

Для перехода к настройкам администрирования необходимо:

- нажать на вкладку **«Система»** - **«Настройки»** - **«Администрирование»**, расположенную в левой части списка объектов управления;

Для перехода к общим настройкам необходимо:

- нажать на вкладку **«Система»** - **«Настройки»** - **«Общие настройки»**, расположенную в левой части списка объектов управления;

Для перехода к настройкам журналирования необходимо:

- нажать на вкладку **«Система»** - **«Настройки»** - **«Журналирование»**, расположенную в левой части списка объектов управления;

Для перехода к настройкам Ведение журнала/цели необходимо:

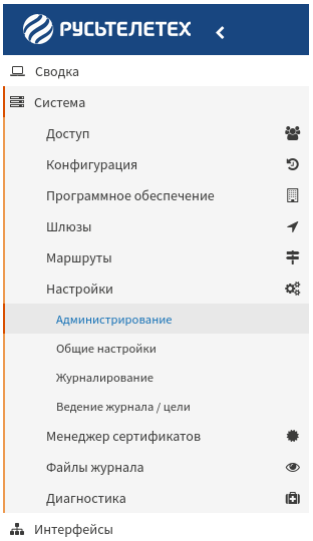


Рис. 207: Переход к настройкам администрирования

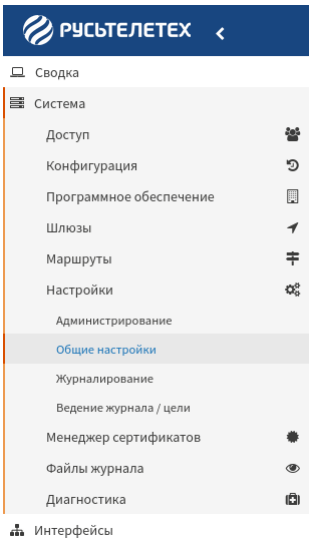


Рис. 208: Переход к общим настройкам

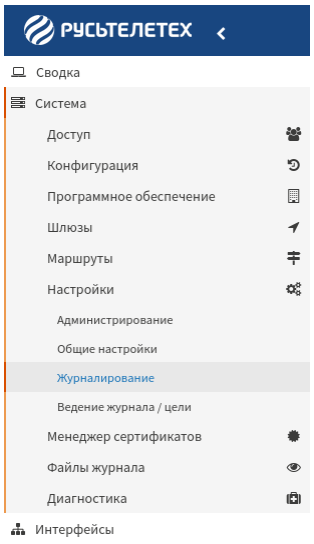


Рис. 209: Переход к настройкам журналирования

- нажать на вкладку **«Система»** - **«Настройки»** - **«Ведение журнала/цели»**, расположенную в левой части списка объектов управления;

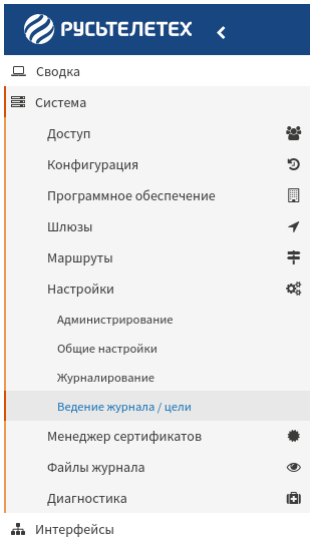


Рис. 210: Настройки Ведение журнала/цели

- в правой части экрана появится таблица Ведение журнала/цели;
- нажать кнопку «+», находящуюся в правой части таблицы.

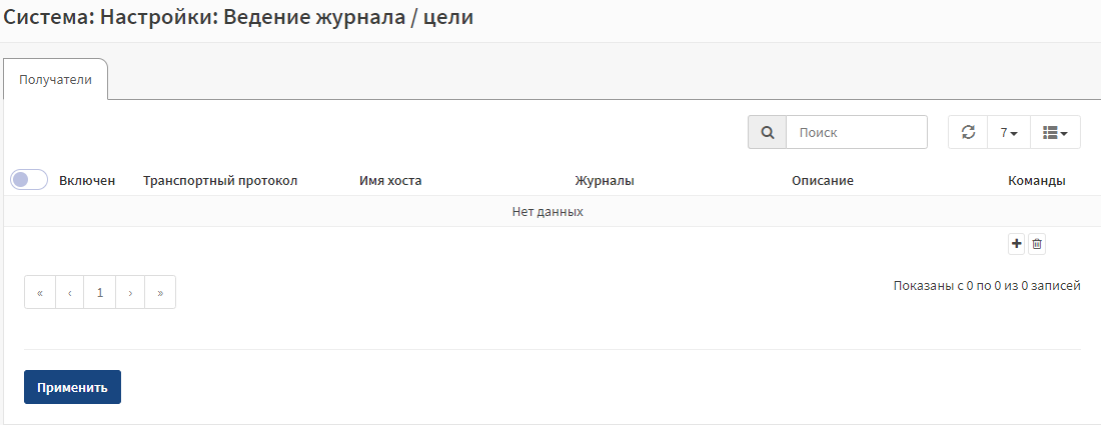


Рис. 211: Таблица Ведение журнала/цели

Администрирование

Web-интерфейс

Для настройки Web-интерфейса необходимо:

- в поле **«Протокол»** выбрать один из протоколов, соответствующих таблице;

Таблица 69: Протоколы

Протокол
HTTP
HTTPS

- в поле **«Строгая транспортная безопасность HTTP»** установить переключатель в случае необходимости включить HTTP Strict Transport Security (HSTS);

Примечание

Строгая транспортная безопасность HTTP — это механизм политики веб-безопасности, который помогает защитить веб-сайты от атак с понижением версии протокола и перехвата файлов cookie

- в поле **«Порт TCP»** ввести номер порта для web GUI, если необходимо переопределить значение по умолчанию;

Совет

80 для HTTP, 443 для HTTPS

Примечание

Изменения вступят в силу сразу после сохранения

- в поле **«Аудит входа в систему»** установить переключатель в случае необходимости отключения протоколирования успешных входов в Web-интерфейс;
- в поле **«Продолжительность сессии»** ввести числовое значение времени простоя для сеансов в минутах;

Примечание

По умолчанию время простоя для сеансов составляет 4 часа (240 минут)

- в поле **«Проверка DNS Rebinding»** установить переключатель для защиты системы от DNS Rebinding атак;

Примечание

Опция **«Проверка DNS Rebinding»** блокирует частные IP-ответы с Ваших DNS серверов

Совет

Выберите эту опцию для отключения этой защиты, если это мешает доступу к WebGUI или разрешению доменных имён в вашем окружении

- в поле **«Альтернативные имена хостов»** указать альтернативные имена хостов, с помощью которых маршрутизатор может быть запрошен, чтобы обойти проверку атаки DNS Rebinding;

Совет

Альтернативные имена хостов указываются с разделением через пробел

- в поле **«Сжатие HTTP»** выбрать из выпадающего списка одну из форм сжатия HTTP-страниц и динамического контента, соответствующих таблице;

Таблица 70: Протоколы

Сжатия HTTP-страниц
Выкл.
Низкий
Среднее
Высокое

Совет

Функция **«Сжатие HTTP»** позволяет передавать меньше данных клиенту за счёт избыточной нагрузки на обработку

- в поле **«Журнал доступа»** установить переключатель в случае необходимости включить журналирование доступа к Web-интерфейсу в целях отладки и анализа;
- в поле **«Прослушивание интерфейсов»** выбрать из выпадающего списка один из интерфейсов для прослушивания, соответствующих таблице;

Таблица 71: Интерфейсы

Интерфейсы
Все (рекомендуется)
[Интерфейс]

Совет

Функция **«Прослушивание интерфейсов»** позволяет принимать соединения только с выбранных интерфейсов

Совет

Необходимо выбрать **«Все (рекомендуется)»** для прослушивания всех интерфейсов

Примечание

При выборе интерфейса необходимо подтвердить выбор в открывшемся окне

- в поле **«Обеспечение соблюдения HTTP_REFERER»** установить переключатель в случае необходимости защиты доступа к web GUI от попыток перенаправления HTTP_REFERER;

Совет

Необходимо выбрать опцию **«Обеспечение соблюдения HTTP_REFERER»** для отключения защиты из-за помех доступа к web GUI в некоторых нестандартных случаях вроде использования внешних скриптов для взаимодействия с этой системой

- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

SSH

Для настройки SSH-сервера необходимо:

- в поле **«SSH-сервер»** установить переключатель в случае необходимости включить протокол Secure Shell;
- в поле **«Метод аутентификации»** установить переключатель для разрешения парольного входа в учётную запись;

Примечание

При отключенной функции **«Метод аутентификации»** авторизованные ключи необходимо настроить для каждого, которому предоставлен доступ к защищенной оболочке

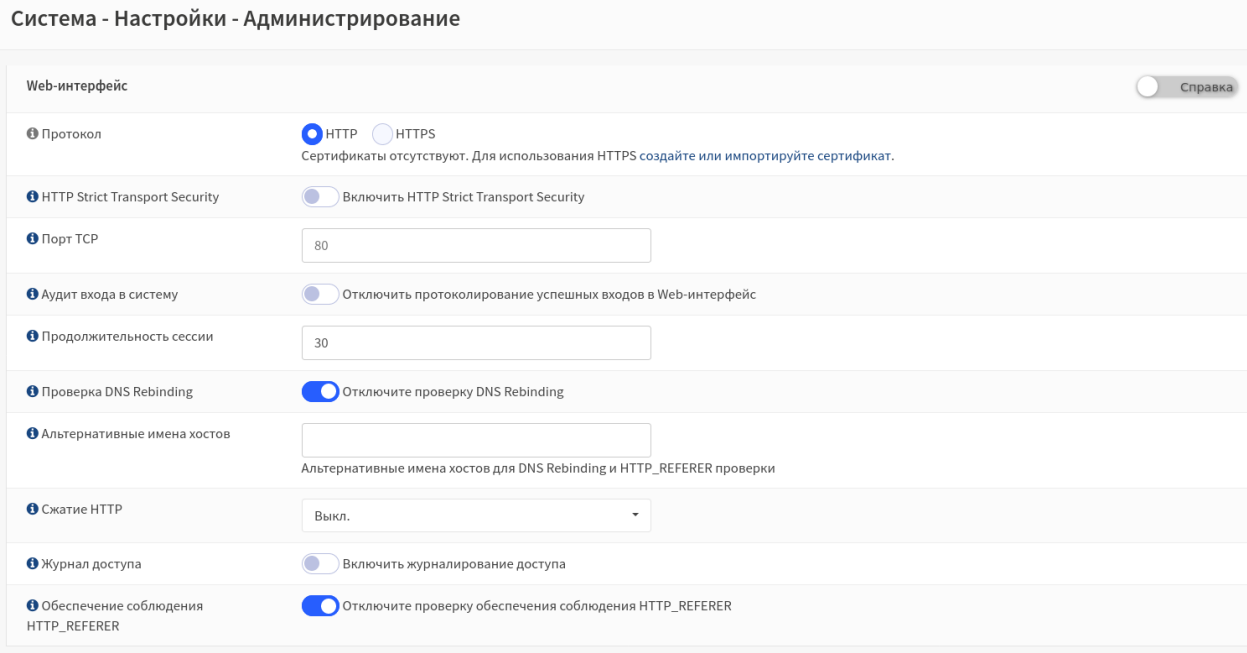


Рис. 212: Настройка Web-интерфейса

- в поле **«Порт SSH»** ознакомиться со значением порта по умолчанию 9022;
- в поле **«Прослушивание интерфейсов»** выбрать из выпадающего списка один из интерфейсов для прослушивания, соответствующих таблице;

Таблица 72: Интерфейсы

Интерфейсы
Все (рекомендуется)
[Интерфейс]

Совет

Функция **«Прослушивание интерфейсов»** позволяет принимать соединения только с выбранных интерфейсов

Совет

Необходимо выбрать **«Все (рекомендуется)»** для прослушивания всех интерфейсов

Совет

Необходимо использовать функцию **«Прослушивание интерфейсов»** с осторожностью

- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

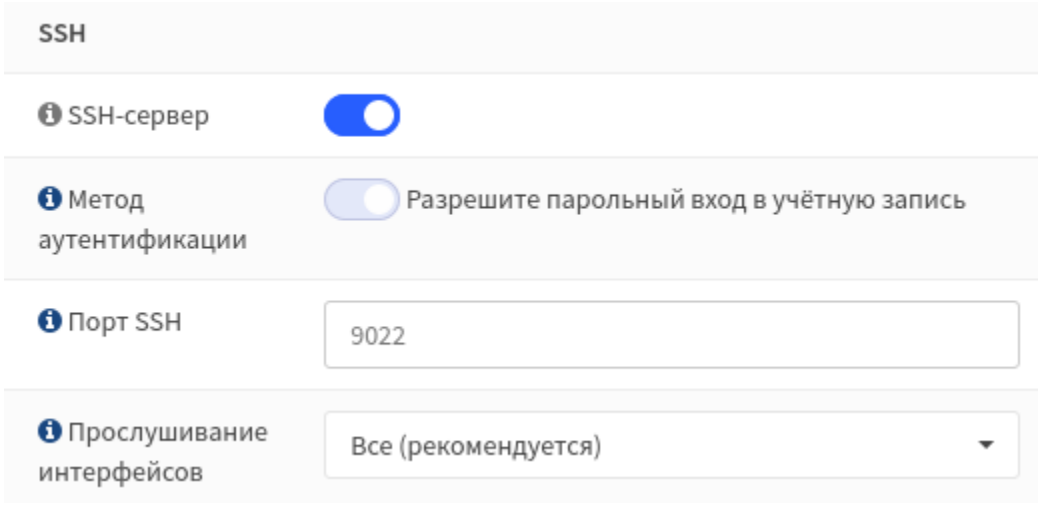


Рис. 213: Настройка SSH

Аутентификация

Для настройки аутентификации необходимо:

- в поле **«Сервер»** выбрать из выпадающего списка один или несколько серверов аутентификации для проверки учетных данных пользователя, соответствующих таблице;

Таблица 73: Серверы

Серверы
Локальная база данных

Примечание

Несколько серверов могут иметь смысл с удаленными методами аутентификации, чтобы обеспечить запасной вариант при проблемах с подключением

Примечание

Если ни один сервер не выбран, то по умолчанию используется сервер **«Локальная база данных»**

- в поле **«Отключить встроенную аутентификацию»** установить переключатель в случае необходимости отключить встроенную аутентификацию;
- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигуриро-

ванных настроек в силу.

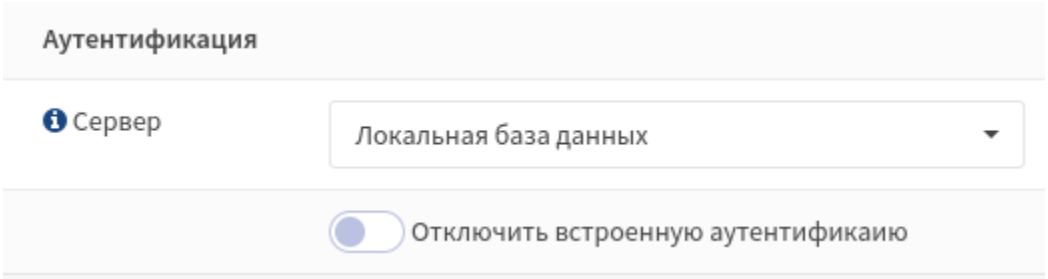


Рис. 214: Настройка аутентификации

Общие настройки

Система

Для настройки системы необходимо:

- в поле **«Имя хоста»** указать имя хоста без доменной части;
- в поле **«Домен»** указать доменное имя;

> **Совет**
>
> Не используйте «local» в качестве доменного имени. В противном случае локальные хосты, запускающие mDNS (avahi, bonjour и т. д.), не смогут корректно обрабатывать запросы с хостов, на которых не запущена служба mDNS

> **Совет**
>
> Используйте в качестве доменного имени mycorp.com, дом, офис, частный, и т. д.

- в поле **«Часовой пояс»** выбрать из выпадающего списка ближайший часовой пояс;
- в поле **«Язык»** выбрать из выпадающего списка язык интерфейса;
- в поле **«Тайм-аут подтверждения конфигурации»** установить значение, соответствующее таблице;

Таблица 74: Значение

Значение
Отсутствует
5
15
30

- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

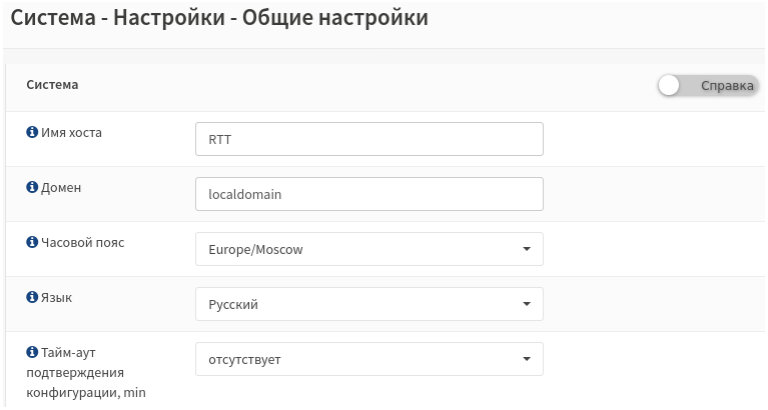


Рис. 215: Общие настройки системы

Параметры организации сети

Для настройки параметров организации сети необходимо:

- в поле **«Выбрать IPv4 через IPv6»** установить переключатель для принудительного использования IPv4 вместо IPv6;
- в поле **«Асимметричная маршрутизация»** установить переключатель для маршрутизации пакетов асимметрично;
- в поле **«DNS-серверы»** указать IP-адреса, которые будут использоваться системой для разрешения DNS;

Примечание

IP-адреса будут использоваться для службы DHCP, службы DNS и для клиентов PPTP VPN

- в поле **«System DNS resolver»** установить переключатель для исключения локальной службы DNS из списка DNS-серверов;
- нажать кнопку **«Сохранить»** Сохранить для сохранения и вступления сконфигурированных настроек в силу.

Особые возможности

Для установки контроля пропускной способности интерфейса необходимо:

- в поле **«Аппаратный контроль пропускной способности»** установить для каждого интерфейса необходимый статус производительности
- нажать кнопку **«Сохранить»** Сохранить для сохранения и вступления сконфигурированных настроек в силу.

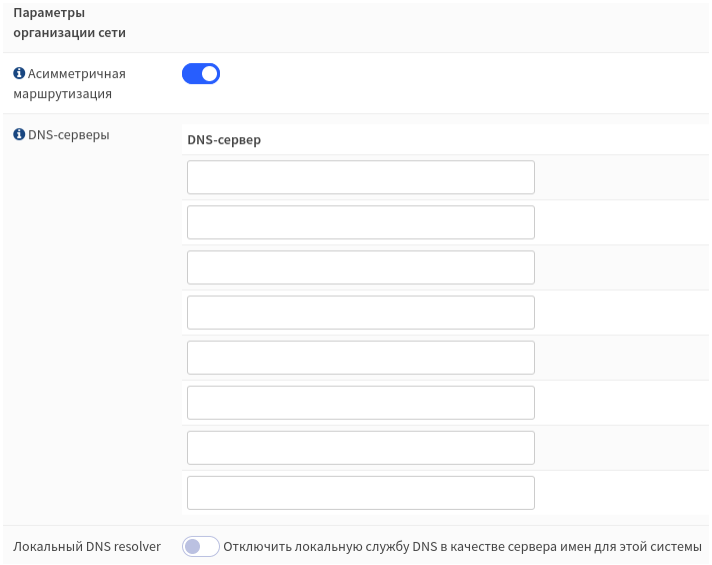


Рис. 216: Настройка параметров организации сети

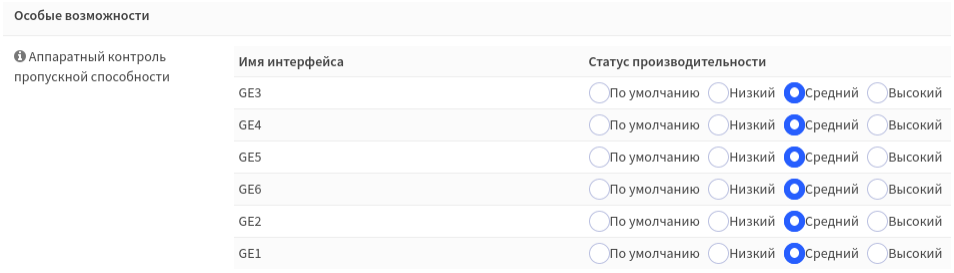


Рис. 217: Настройка аппаратного контроля пропускной способности

Журналирование

На вкладке **«Параметры локального ведения журнала»** необходимо:

- в поле **«Максимальный размер системных файлов журнала»** ввести числовое значение максимального размера журнала в мегабайтах;

> **Примечание**
>
> Допустимый диапазон - от 1Мб до 20Мб

- в поле **«Кол-во архивных файлов журналов системы»** ввести числовое значение количества архивных файлов;
- в поле **«Максимальный размер файлов журнала фильтра»** ввести числовое значение максимального размера журнала в мегабайтах;

> **Примечание**
>
> Допустимый диапазон - от 10Мб до 20Мб

- в поле **«Кол-во архивных файлов журнала фильтра»** ввести числовое значение количества архивных файлов;
- в поле **«Отключить сжатие»** установить переключатель в случае необходимости отключить сжатие;
- в поле **«Количество циклов затирания журналов»** выбрать из выпадающего списка необходимое количество циклов затирания журналов, соответствующих таблице;

Таблица 75: Количество циклов затирания журналов

Количество циклов затирания журналов
1
2
3

- в поле **«Удалить журналы»** нажать кнопку **«Очистить файлы журналов»** в случае необходимости очистить все локальные файлы журналов и повторно инициализировать их как пустые журналы;
  - в открывшемся окне подтвердить Использование функции **«Удалить журналы»**;

> **Примечание**
>
> Использование функции **«Удалить журналы»** также перезапустит daemon протокола DHCP

> **Совет**
>
> Сначала используйте кнопку **«Сохранить»**, если вы внесли какие-либо изменения в настройки

- в поле **«Сохранить файлы журнала»** выберете устройство и нажмите кнопку **«Сохранить на USB / MMC»** для сохранения всех журналов на устройство.
- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

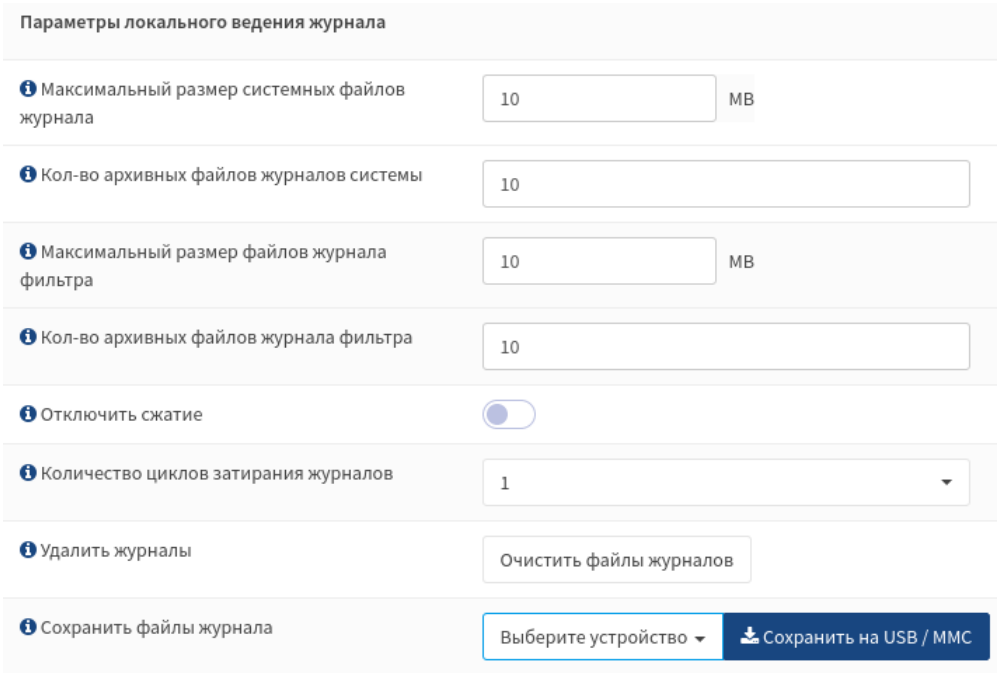


Рис. 218: Настройка журналирования

Экспорт журналов

Экспорт журналов

В окне **«Изменить пункт назначения»** необходимо:

- в поле **«Включен»** установить переключатель;
- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

Настройка функции Экспорт журналов

В окне **«Изменить пункт назначения»** необходимо:

- в поле **«Транспортный протокол»** выбрать из выпадающего списка необходимый протокол, соответствующий таблице;

Таблица 76: Выбор транспортного протокола

Выбор транспортного протокола
UDP (4)
TCP (4)

- в поле **«Файлы журнала»** выбрать из выпадающего списка необходимые для отправки на удаленный сервер файлы журналов, соответствующие таблице;

Таблица 77: Файлы журналов

Файлы журналов
Межсетевой экран
Система
WebGUI
Аутентификация
Прокси сервер
VPN
ClamAV

- в поле **«Имя хоста»** указать имя хоста;
- в поле **«Порт»** указать порт;
- в поле **«Описание»** ввести описание настраиваемого назначения;
- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

2.7.3.7 Менеджер сертификатов

Для создания или импортирования центра сертификации необходимо:

- нажать на вкладку **«Система»** - **«Менеджер сертификатов»** - **«Корневые сертификаты»**, расположенную в левой части списка объектов управления;
- в правой части экрана появится таблица центров сертификации;
- нажать кнопку **«Добавить»** 

, находящуюся в правой части таблицы.

Для создания или импортирования сертификатов необходимо:

- нажать на вкладку **«Система»** - **«Менеджер сертификатов»** - **«Сертификаты»**, расположенную в левой части списка объектов управления;
- в правой части экрана появится таблица сертификатов;

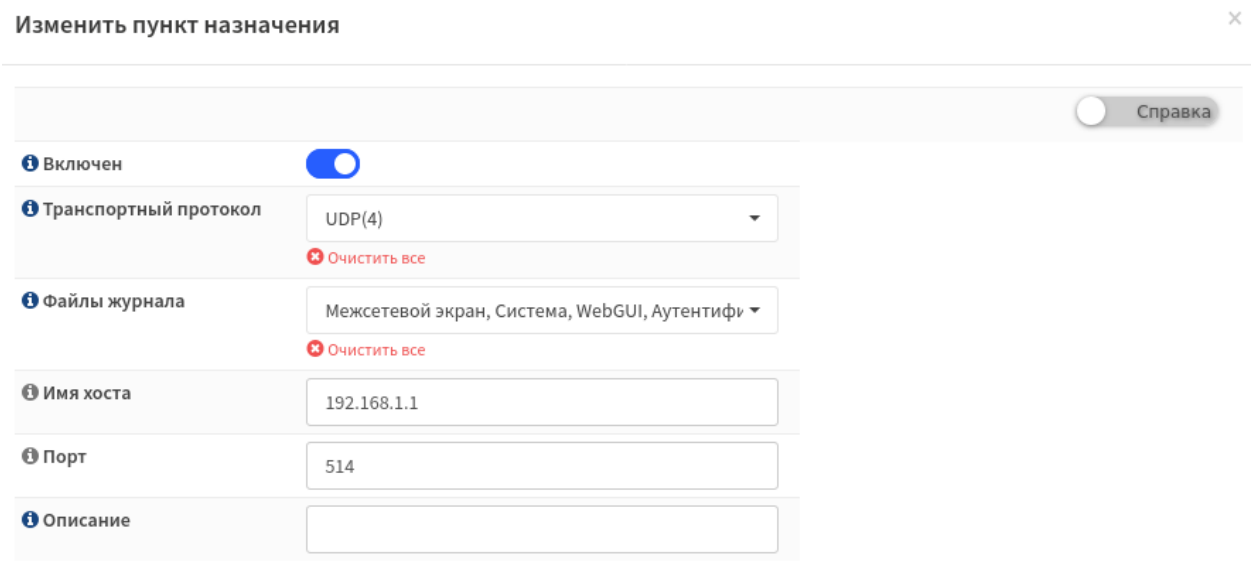


Рис. 219: Описание

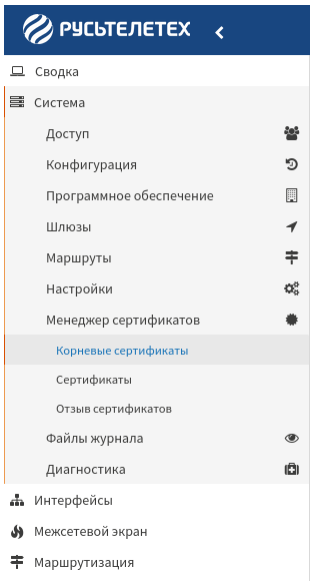


Рис. 220: Переход к созданию или импортированию центра сертификации

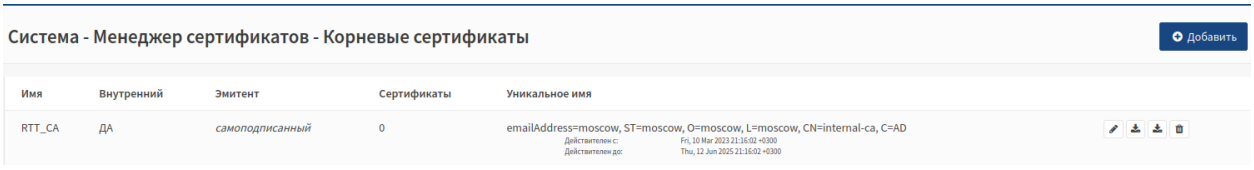


Рис. 221: Таблица центров сертификации

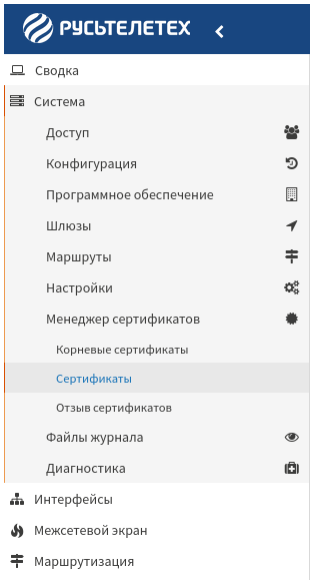


Рис. 222: Переход к созданию или импортированию сертификатов

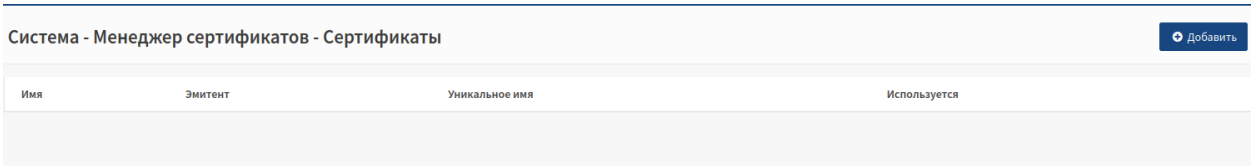


Рис. 223: Таблица сертификатов

- нажать кнопку **«Добавить»** 

, находящуюся в правой части таблицы.

Для отзыва сертификатов необходимо:

- нажать на вкладку **«Система»** - **«Менеджер сертификатов»** - **«Отзыв сертификатов»**, расположенную в левой части списка объектов управления.

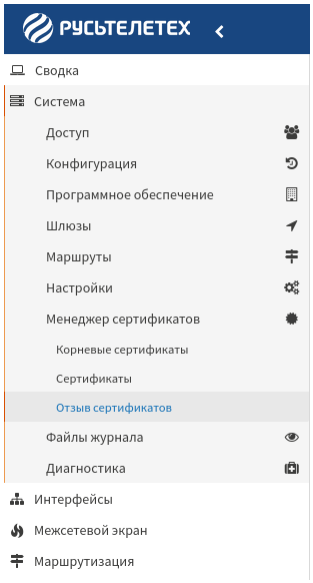


Рис. 224: Переход к отзыву сертификатов

- в правой части экрана появится таблица сертификатов;

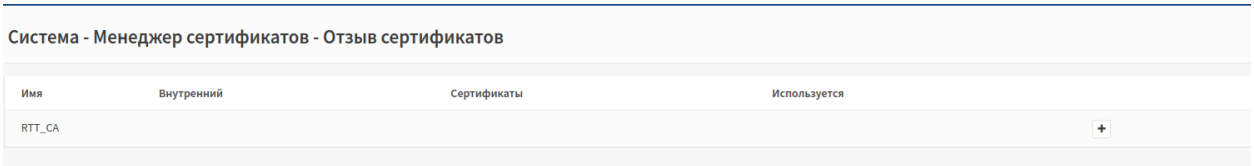


Рис. 225: Таблица отзывов сертификатов

- нажать кнопку «+» , находящуюся в правой части таблицы, для создания нового отзыва сертификатов.

Корневые сертификаты

Импорт существующего центра сертификации

Для импортирования существующего центра сертификации необходимо:

- в поле **«Описательное имя»** ввести имя центра сертификации;
- в поле **«Метод»** выбрать из выпадающего меню **«Импортировать существующий центр сертификации»**;

Существующий центр сертификации

- в поле **«Данные сертификата»** вставить сертификат в X.509 формате PEM;
- в поле **«Секретный ключ сертификата (необязательно)»** вставить секретный ключ сертификата;

> **Примечание**
>
> Секретный ключ сертификата вводится в случае необходимости сгенерировать Список Отзыва Сертификатов (CRL)

- в поле **«Серийный номер для следующего сертификата»** ввести десятичное число, которое будет использоваться как серийный номер для следующего сертификата, который должен быть создан с помощью этого центра сертификации;
- нажать кнопку **«Сохранить»** 

.

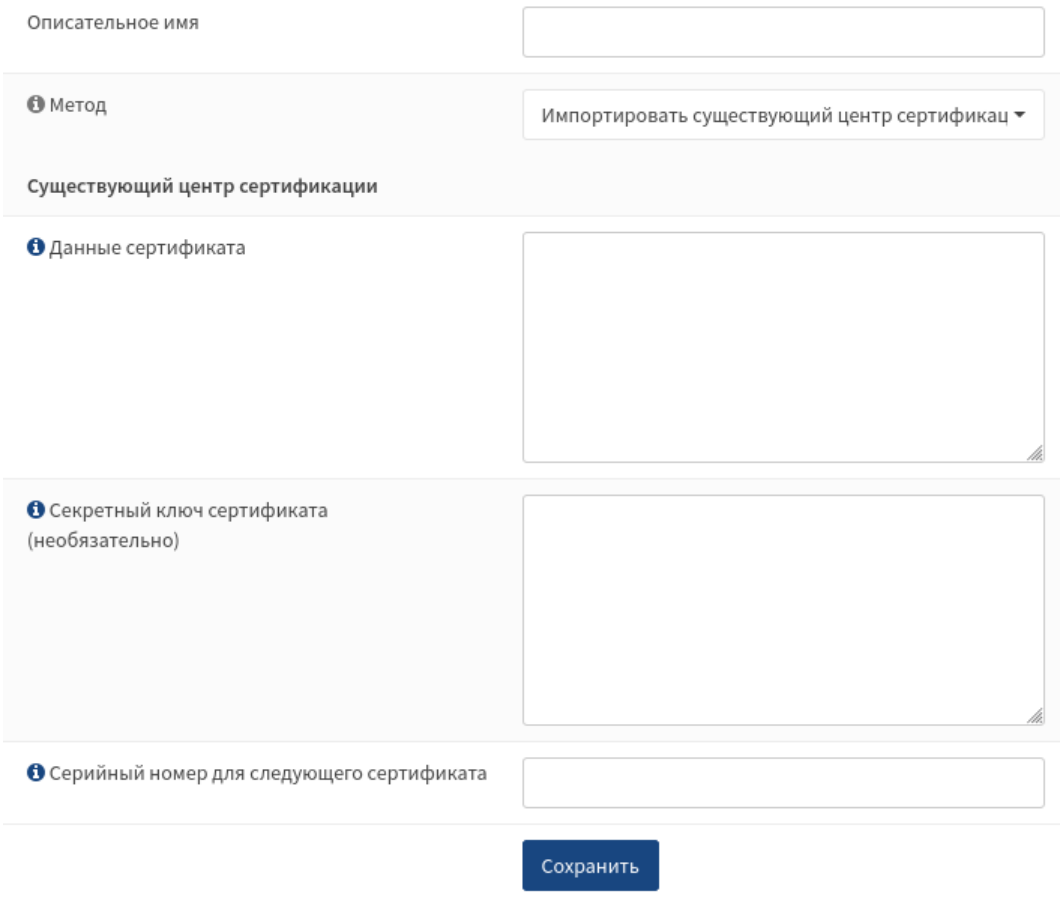


Рис. 226: Импорт существующего центра сертификации

Создание внутреннего центра сертификации

Для создания внутреннего центра сертификации необходимо:

- в поле **«Описательное имя»** ввести имя центра сертификации;
- в поле **«Метод»** выбрать из выпадающего списка **«Создать внутренний центр сертификации»**;

Внутренний Центр сертификации

- в поле **«Тип ключа»** выбрать из выпадающего списка один из типов ключа, соответствующих таблице;

Таблица 78: Выбор типа ключа

Тип ключа
RSA
Эллиптическая кривая

- в поле **«Длина ключа (бит)»** (при выборе в поле **«Тип ключа»** тип ключа **«RSA»**) выбрать из выпадающего списка одно из значений длины ключа, соответствующих таблице;

Таблица 79: Выбор длины ключа

Длина ключа
512
1024
2048
3072
4096
8192

- в поле **«Кривая»** (при выборе в поле **«Тип ключа»** тип ключа **«Эллиптическая кривая»**) выбрать из выпадающего списка одну из эллиптических кривых, соответствующих таблице;

Таблица 80: Выбор эллиптической кривой

Эллиптическая кривая
prime256v1
secp384r1
secp521r1

- в поле **«Алгоритм шифрования»** выбрать из выпадающего списка один из необходимых алгоритмов, соответствующих таблице;

Таблица 81: Выбор алгоритма

Алгоритмы
SHA1
SHA224
SHA256
SHA384
SHA512

Примечание

Рекомендуется использование более сильного, чем SHA1, алгоритма, когда это возможно

- в поле **«Время существования (дни)»** ввести время существования центра;

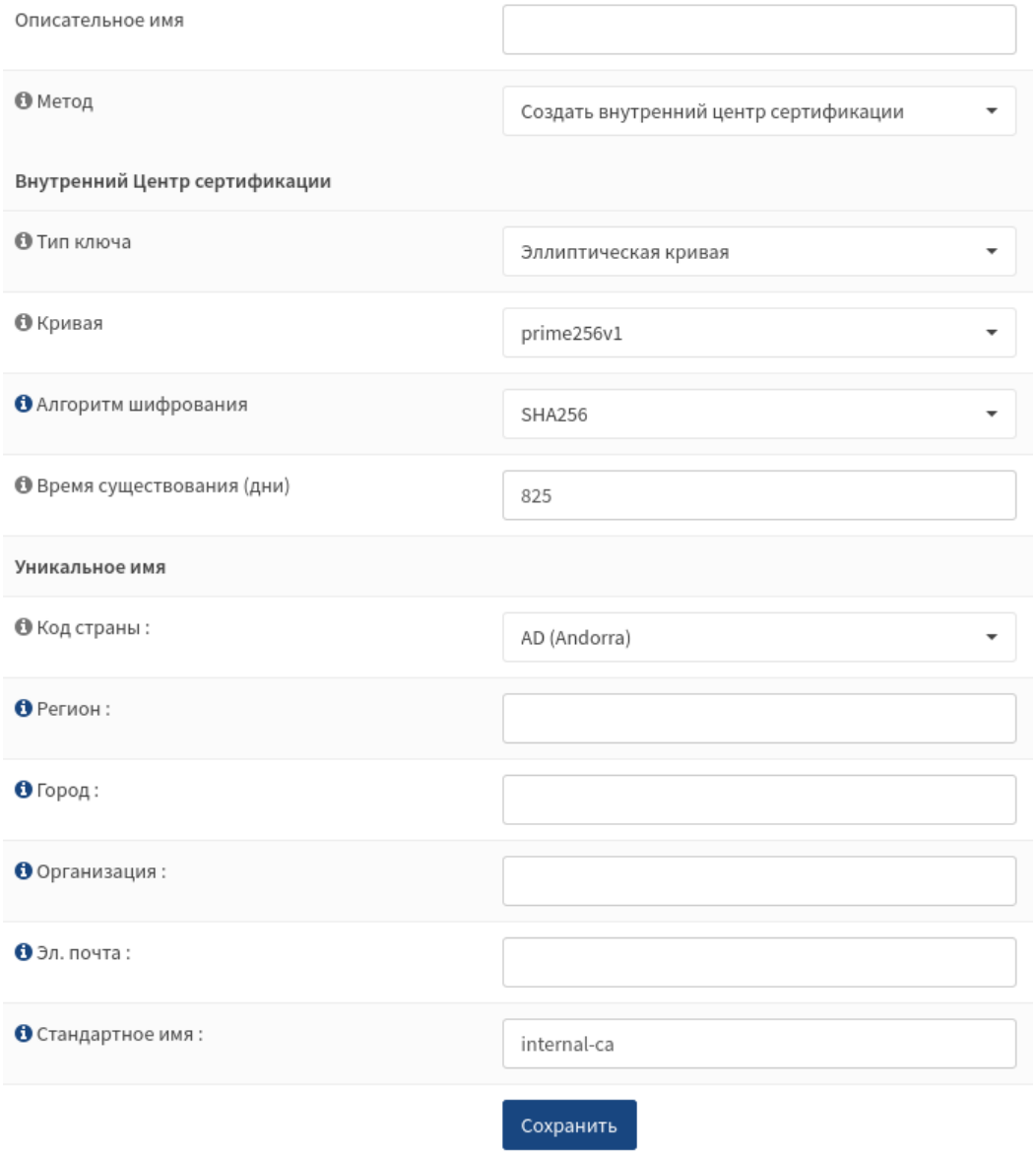


Рис. 227: Создание внутреннего центра сертификации

Уникальное имя

- в поле **«Код страны»** выбрать из выпадающего списка требуемую страну мира;
- в поле **«Регион»** ввести требуемый регион;
- в поле **«Город»** ввести требуемый город;
- в поле **«Организация»** ввести необходимую организацию;
- в поле **«Эл. почта»** ввести необходимый адрес электронной почты;
- в поле **«Стандартное имя»** ввести необходимое имя;
- нажать кнопку **«Сохранить»** 

.

Создание промежуточного центра сертификации

Для создания промежуточного центра сертификации необходимо:

- в поле **«Описательное имя»** ввести имя центра сертификации;
- в поле **«Метод»** выбрать из выпадающего списка **«Создать промежуточный центр сертификации»**;

Внутренний Центр сертификации

- в поле **«Подписание центра сертификации»** выбрать из выпадающего списка необходимый центр сертификации;
- в поле **«Тип ключа»** выбрать из выпадающего списка один из типов ключа, соответствующих таблице;

Таблица 82: Выбор типа ключа

Тип ключа
RSA
Эллиптическая кривая

- в поле **«Длина ключа (бит)»** (при выборе в поле **«Тип ключа»** тип ключа **«RSA»**) выбрать из выпадающего списка одно из значений длины ключа, соответствующих таблице;

Таблица 83: Выбор длины ключа

Длина ключа
512
1024
2048
3072
4096
8192

- в поле **«Кривая»** (при выборе в поле **«Тип ключа»** тип ключа **«Эллиптическая кривая»**) выбрать из выпадающего списка одну из эллиптических кривых, соответствующих таблице;

Таблица 84: Выбор эллиптической кривой

Эллиптическая кривая
prime256v1
secp384r1
secp521r1

- в поле **«Алгоритм шифрования»** выбрать из выпадающего списка один из необходимых алгоритмов, соответствующих таблице;

Таблица 85: Выбор алгоритма

Алгоритмы
SHA1
SHA224
SHA256
SHA384
SHA512

Примечание

Рекомендуется использование более сильного, чем SHA1, алгоритма, когда это возможно

- в поле **«Время существования (дни)»** ввести время существования центра;

Уникальное имя

- в поле **«Код страны»** выбрать из выпадающего списка требуемую страну мира;
- в поле **«Регион** ввести требуемый регион;
- в поле **«Город»** ввести требуемый город;
- в поле **«Организация»** ввести необходимую организацию;
- в поле **«Эл. почта»** ввести необходимый адрес электронной почты;
- в поле **«Стандартное имя»** ввести необходимое имя;
- нажать кнопку **«Сохранить»** 

.

Сертификаты

Импорт существующего сертификата

Для импорта существующего сертификата необходимо:

- в поле **«Метод»** выбрать из выпадающего меню **«Импортировать существующий сертификат»**;
- в поле **«Описательное имя»** ввести имя сертификата;

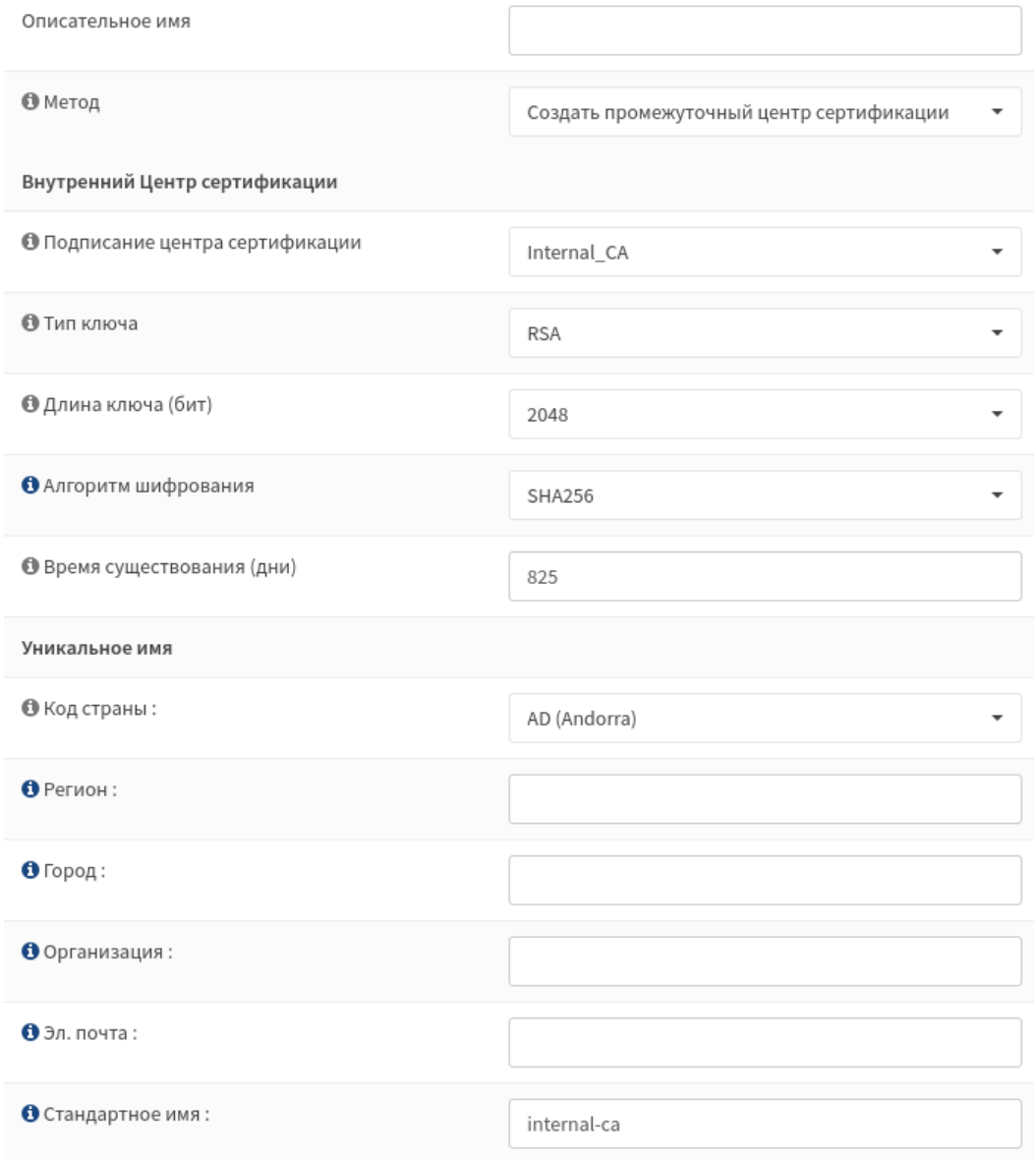


Рис. 228: Создание внутреннего центра сертификации

Импортировать сертификат

- в поле **«Данные сертификата»** вставить сертификат в X.509 формате PEM;
- в поле **«Данные секретного ключа»** вставить секретный ключ в X.509 формате PEM;
- нажать кнопку **«Сохранить»** 

.

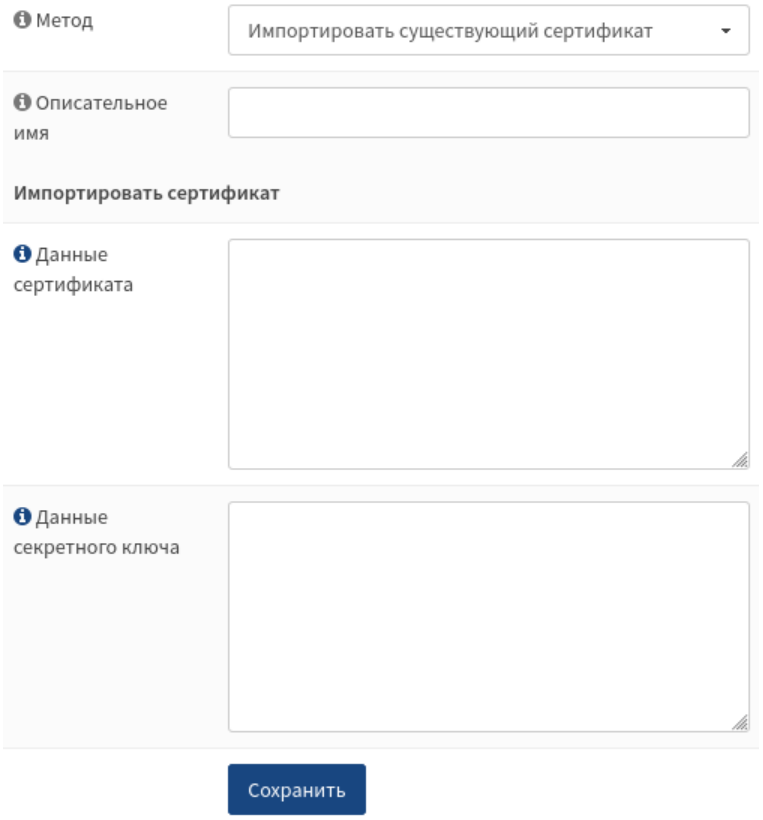


Рис. 229: Импортирование существующего центра сертификации

Создание внутреннего сертификата

Для создания внутреннего сертификата необходимо:

- в поле **«Метод»** выбрать из выпадающего меню **«Создать внутренний сертификат»**;
- в поле **«Описательное имя»** ввести имя сертификата;

Внутренний Сертификат

- поле **«Центр сертификации»** добавить внутренний центр сертификации;
- в поле **«Тип»** выбрать из выпадающего списка один из типов сертификатов, соответствующих таблице;

Таблица 86: Выбор типа сертификата

Тип сертификата
Сертификат клиента
Сертификат сервера
Комбинированный сертификат клиент/сервер
Центр сертификации

- в поле **«Тип ключа»** выбрать из выпадающего списка один из типов ключа, соответствующих таблице;

Таблица 87: Выбор типа ключа

Тип ключа
RSA
Эллиптическая кривая

- в поле **«Длина ключа (бит)»** (при выборе в поле **«Тип ключа»** тип ключа **«RSA»**) выбрать из выпадающего списка одно из значений длины ключа, соответствующих таблице;

Таблица 88: Выбор длины ключа

Длина ключа
512
1024
2048
3072
4096
8192

- в поле **«Кривая»** (при выборе в поле **«Тип ключа»** тип ключа **«Эллиптическая кривая»**) выбрать из выпадающего списка одну из эллиптических кривых, соответствующих таблице;

Таблица 89: Выбор эллиптической кривой

Эллиптическая кривая
prime256v1
secp384r1
secp521r1

- в поле **«Digest Algorithm»** выбрать из выпадающего списка один из необходимых алгоритмов, соответствующих таблице;

Таблица 90: Выбор алгоритма

Алгоритмы
SHA1
SHA224
SHA256
SHA384
SHA512

Примечание

Рекомендуется использование более сильного, чем SHA1, алгоритма, когда это возможно

- в поле **«Время существования (дни)»** ввести время существования сертификата;
- в поле **«Местоположение закрытого ключа»** выбрать из выпадающего списка один из вариантов хранения ключа, соответствующих таблице;

Таблица 91: Варианты хранения ключа

Параметр	Примечание
Сохранить на этом межсетевом экране	Хранить на этом устройстве (Необходимо выбрать это вариант)
Скачать и не сохранять	Если сертификат предназначен для использования устройством, отличным от этого устройства, и существует возможность загрузить закрытый ключ вскоре после сохранения, необходимо выбрать этот вариант. С помощью этой опции существует возможность загрузить закрытый ключ, который не сохраняется на этом устройстве

Уникальное имя

- в поле **«Код страны»** выбрать из выпадающего списка требуемую страну мира;
- в поле **«Штат или область»** ввести требуемый штат или область;
- в поле **«Город»** ввести требуемый город;
- в поле **«Организация»** ввести необходимую организацию;
- в поле **«Эл. почта»** ввести необходимый адрес электронной почты;
- в поле **«Стандартное имя»** ввести необходимое имя;
- в поле **«Альтернативные Имена»** следует:
- колонке **«Тип»** выбрать из выпадающего списка необходимый тип альтернативного имени, соответствующий таблице;

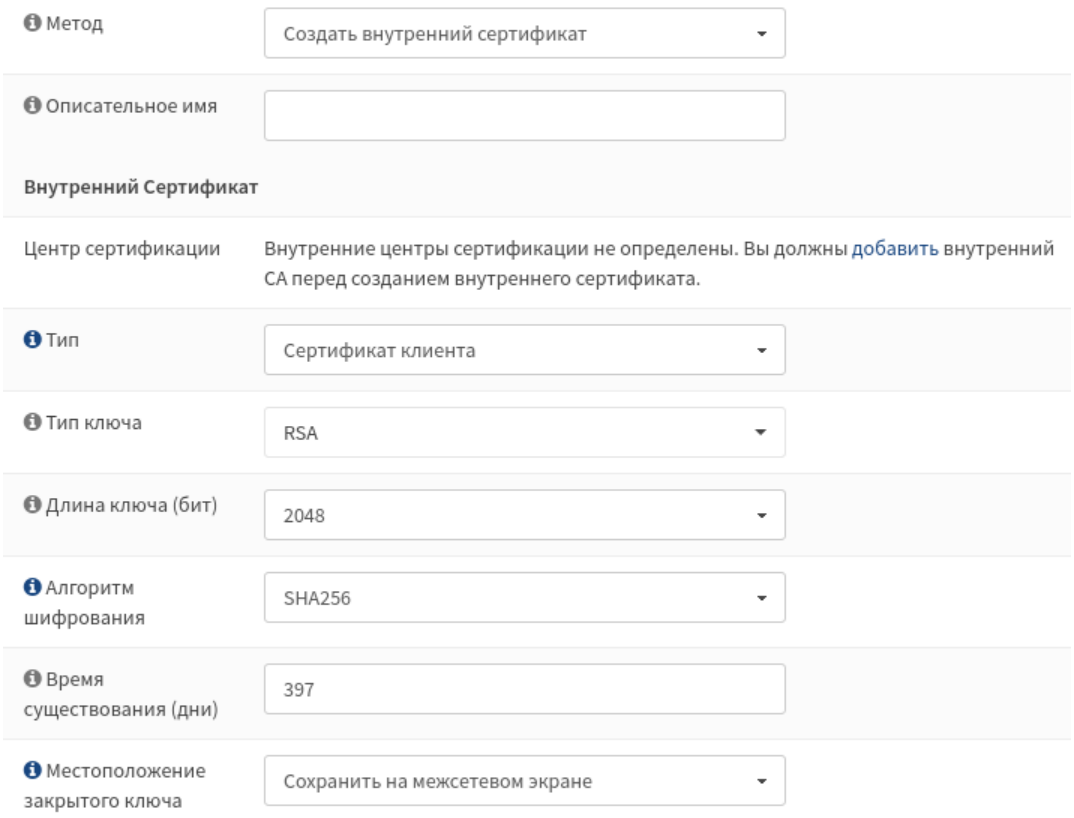


Рис. 230: Создание внутреннего центра сертификации»

Таблица 92: Выбор типа альтернативного имени

Тип
DNS
IP-адрес
Электронная почта
URI

- в колонке **«Значение»** указать значение, соответствующее выбранному типу;
- нажать кнопку «+» в случае необходимости указать дополнительное альтернативное имя;
- нажать кнопку **«Сохранить»** 

.

Создание запроса на подпись сертификата

Для создания запроса на подпись сертификата необходимо:

- в поле **«Метод»** выбрать из выпадающего меню **«Создать запрос на подпись сертификата»**;
- в поле **«Описательное имя»** ввести имя запроса на подпись сертификата;

Запрос внешнего подписания

- в поле **«Тип ключа»** выбрать из выпадающего списка один из типов ключа, соответствующих таблице;

Таблица 93: Выбор типа ключа

Тип ключа
RSA
Эллиптическая кривая

- в поле **«Длина ключа (бит)»** (при выборе в поле **«Тип ключа»** тип ключа **«RSA»**) выбрать из выпадающего списка одно из значений длины ключа, соответствующих таблице;

Таблица 94: Выбор длины ключа

Длина ключа
512
1024
2048
3072
4096
8192

- в поле **«Кривая»** (при выборе в поле **«Тип ключа»** тип ключа **«Эллиптическая кривая»**) выбрать из выпадающего списка одну из эллиптических кривых, соответствующих таблице;

Таблица 95: Выбор эллиптической кривой

Эллиптическая кривая
prime256v1
secp384r1
secp521r1

- в поле **«Digest Algorithm»** выбрать из выпадающего списка один из необходимых алгоритмов, соответствующих таблице;

Таблица 96: Выбор алгоритма

Алгоритмы
SHA1
SHA224
SHA256
SHA384
SHA512

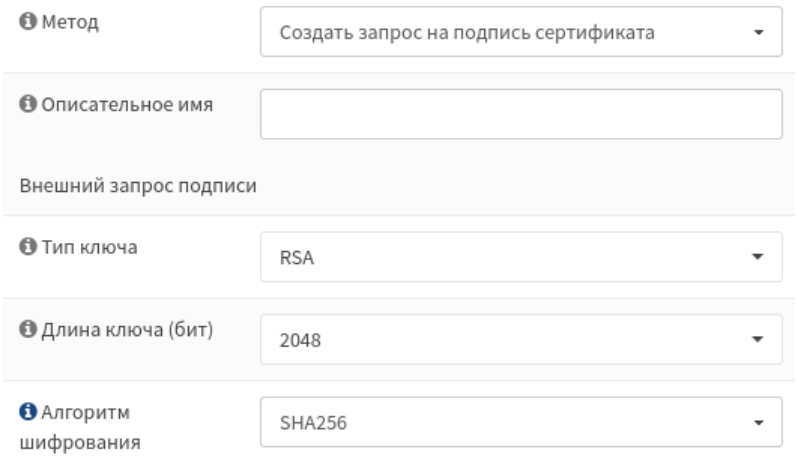


Рис. 231: Создание запроса на подпись сертификата

Уникальное имя

- в поле **«Код страны»** выбрать из выпадающего списка требуемую страну мира;
- в поле **«Штат или область»** ввести требуемый штат или область;
- в поле **«Город»** ввести требуемый город;
- в поле **«Организация»** ввести необходимую организацию;
- в поле **«Организационное подразделение»** ввести необходимое организационное подразделение выбранной организации;
- в поле **«Эл. почта»** ввести необходимый адрес электронной почты;
- в поле **«Стандартное имя»** ввести необходимое имя;
- в поле **«Альтернативные Имена»** следует:

- в колонке **«Тип»** выбрать из выпадающего списка необходимый тип альтернативного имени, соответствующий таблице;

Таблица 97: Выбор типа альтернативного имени

Тип
DNS
IP-адрес
Электронная почта
URI

- в колонке **«Значение»** указать значение, соответствующее выбранному типу;
- нажать кнопку «+» в случае необходимости указать дополнительное альтернативное имя;
- нажать кнопку **«Сохранить»** 

.

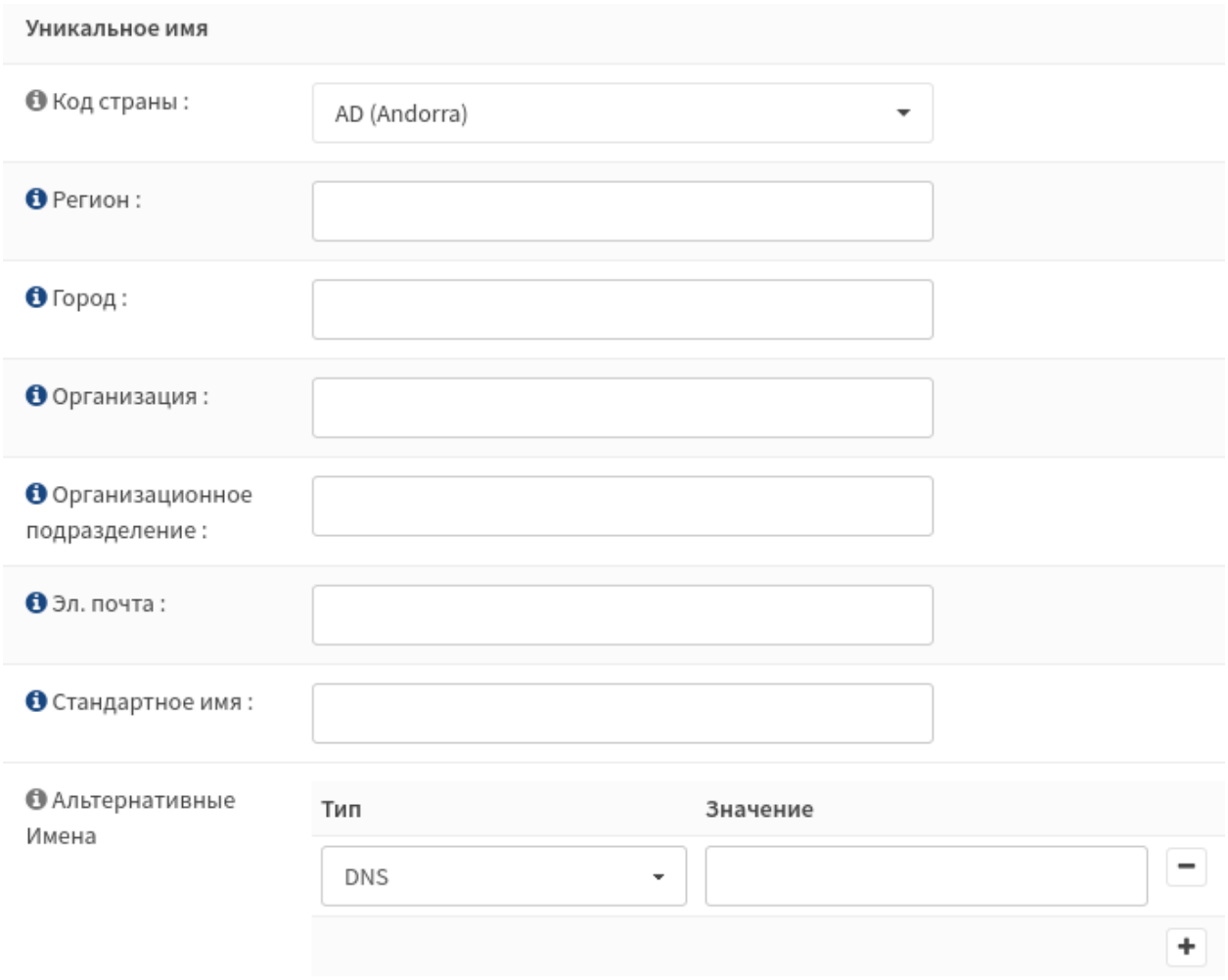


Рис. 232: Настройка уникального имени

Подписание запроса на подпись сертификата

Для подписания запроса на подпись сертификата необходимо:

- в поле **«Метод»** выбрать из выпадающего меню **«Подписать запрос на подпись сертификата»**;
- в поле **«Описательное имя»** ввести имя запроса на подпись сертификата;

Подписать запрос на выпуск сертификата (Certificate Signing Request)

- в поле **«Центр сертификации»** выбрать необходимый центр сертификации;
- в поле **«Digest Algorithm»** выбрать из выпадающего списка один из необходимых алгоритмов, соответствующих таблице;

Таблица 98: Выбор алгоритма

Алгоритмы
SHA1
SHA224
SHA256
SHA384
SHA512

- в поле **«Время существования (дни)»** ввести время существования запроса;
- в поле **«файл CSR (Certificate Signing Request)»** вставить CSR-файл;
- нажать кнопку **«Показать детали»** 

в случае необходимости показать детали запроса сертификата;
- нажать кнопку **«Далее»** 

.

Отзыв сертификатов

Создать внутренний список отзыва сертификатов

Для отзыва сертификата необходимо:

- в поле **«Метод»** выбрать из выпадающего списка **«Создать внутренний список отзыва сертификатов»**;
- в поле **«Описательное имя»** указать имя списка;
- в поле **«Центр сертификации»** выбрать из выпадающего списка **«RTT_CA»**;
- в поле **«Время существования (дни)»** указать время существования списка;

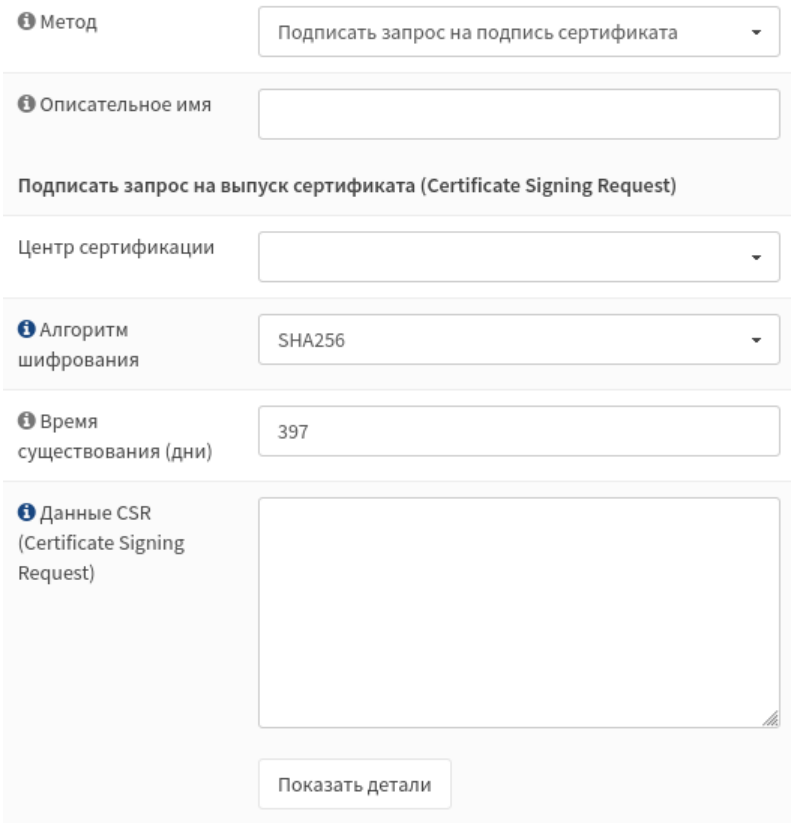


Рис. 233: Имя запроса на подпись сертификата

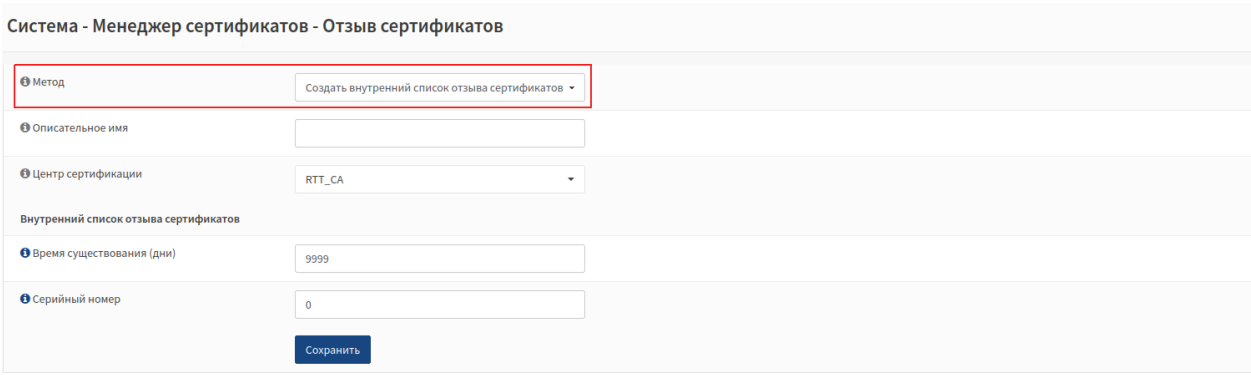


Рис. 234: Выбор метода отзыва сертификата

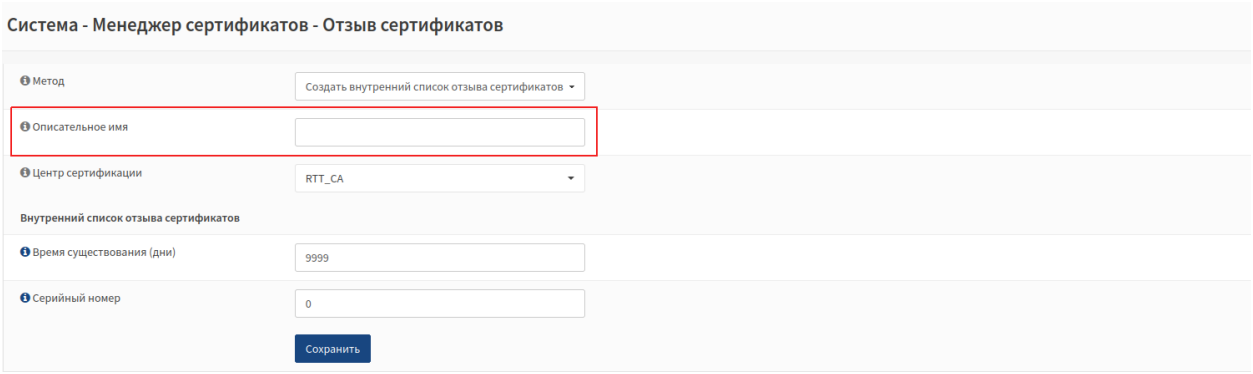


Рис. 235: Описательное имя

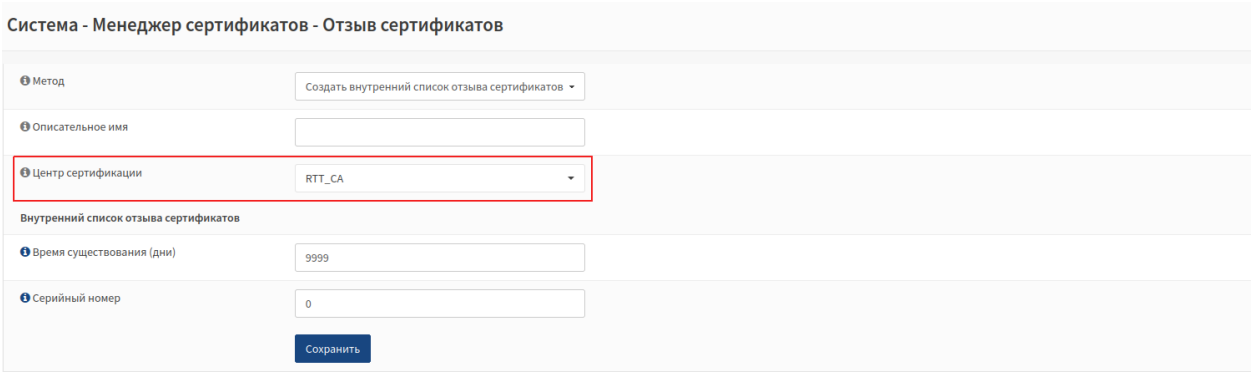


Рис. 236: Выбор центра сертификации

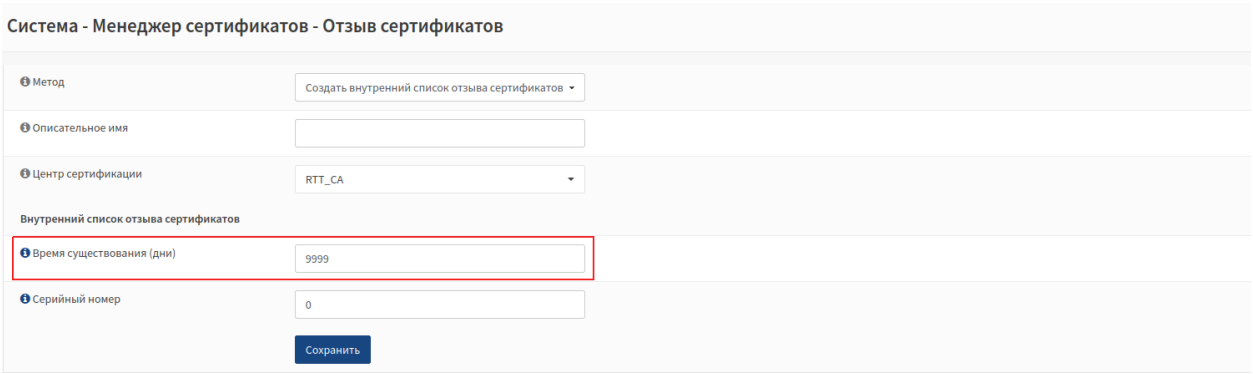


Рис. 237: Время существования (дни)

Совет

По умолчанию 9999 дней

- в поле **«Серийный номер»** указать серийный номер списка;

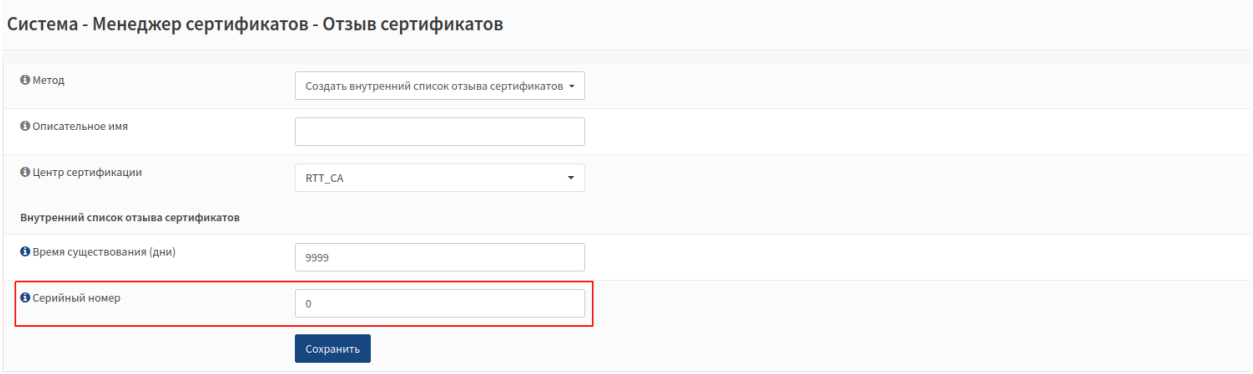


Рис. 238: Серийный номер

Совет

По умолчанию 0

- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

Импортировать существующий список отзыва сертификатов

Для отзыва сертификата необходимо:

- в поле **«Метод»** выбрать из выпадающего списка **«Импортировать существующий список отзыва сертификатов»**;
- в поле **«Описательное имя»** указать имя списка;
- в поле **«Центр сертификации»** выбрать из выпадающего списка **«RTT_CA»**;
- в поле **«Данные CRL»** вставить список отзыва сертификатов в формате X.509 CRL;
- нажать кнопку **«Сохранить»** 

для сохранения и вступления сконфигурированных настроек в силу.

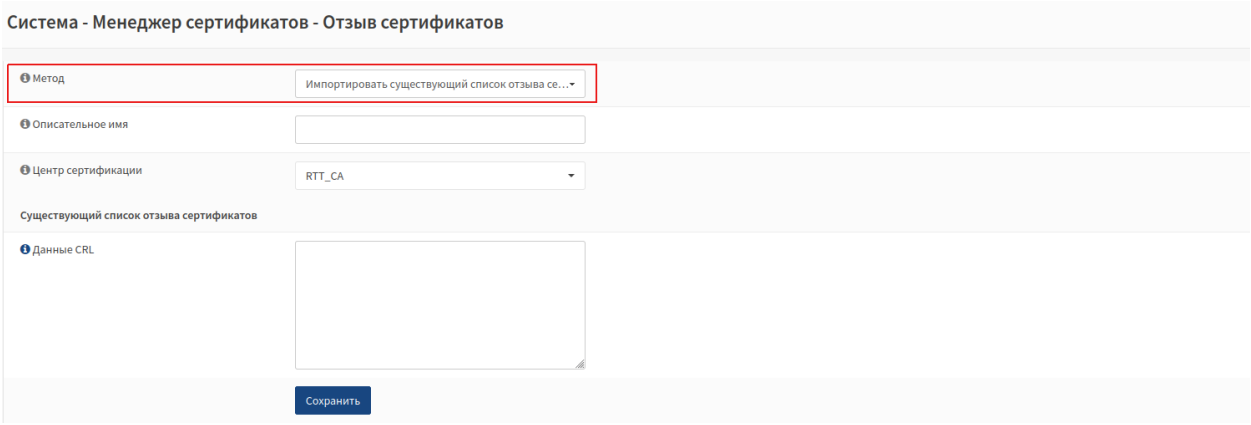


Рис. 239: Выбор метода отзыва сертификата

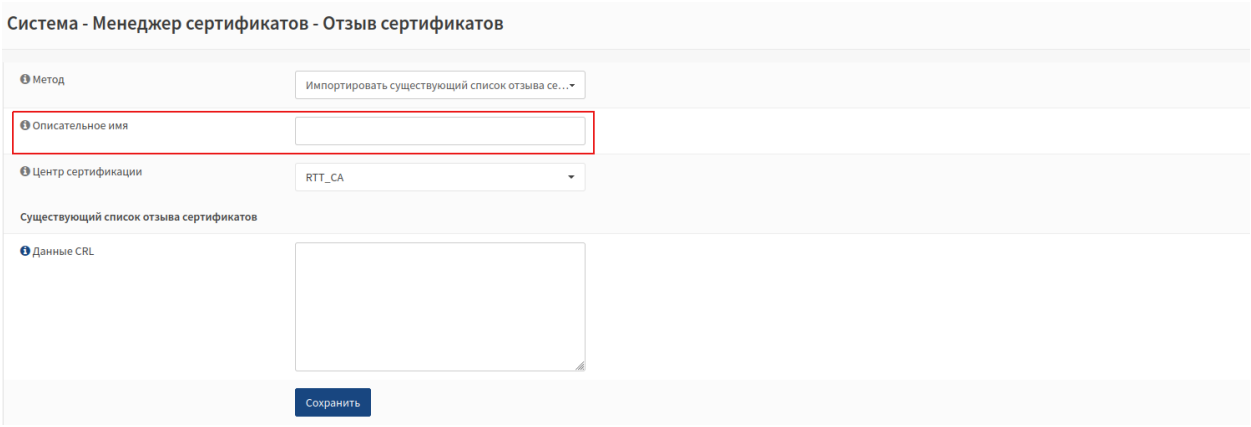


Рис. 240: Описательное имя

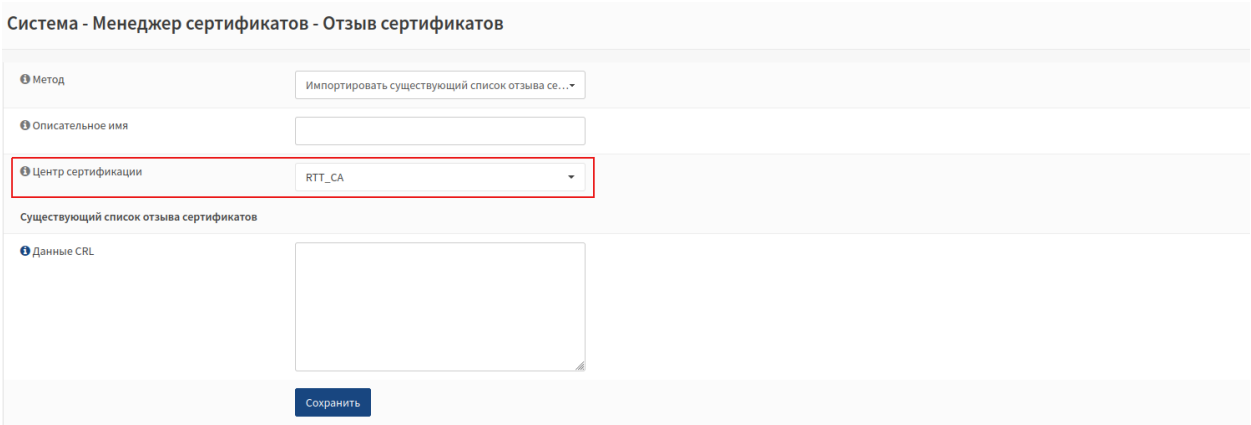


Рис. 241: Выбор центра сертификации

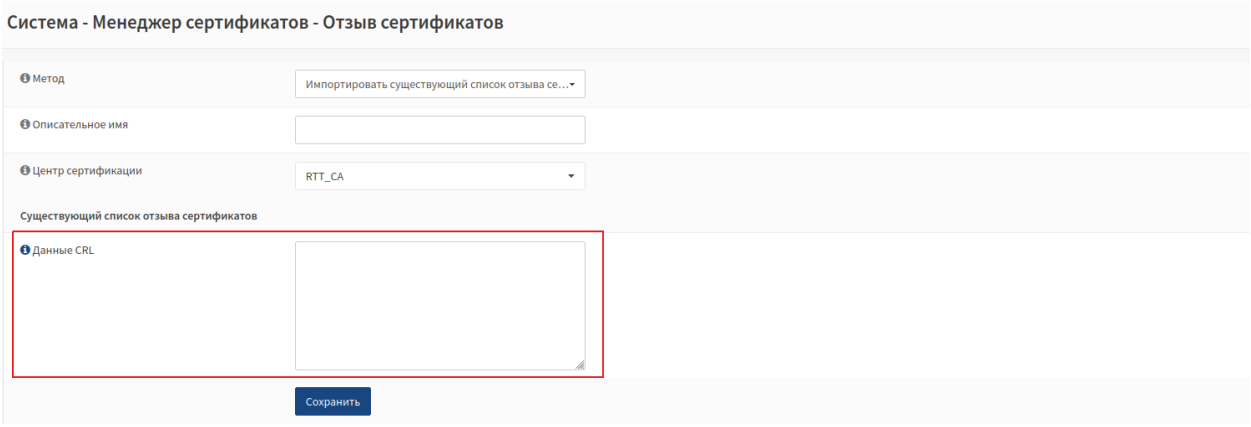


Рис. 242: Данные CRL

2.7.3.8 Файлы журнала

Для перехода к просмотру общего журнала необходимо:

- нажать на вкладку **«Система»** - **«Файлы журнала»** - **«Общий журнал»**, расположенную в левой части списка объектов управления;

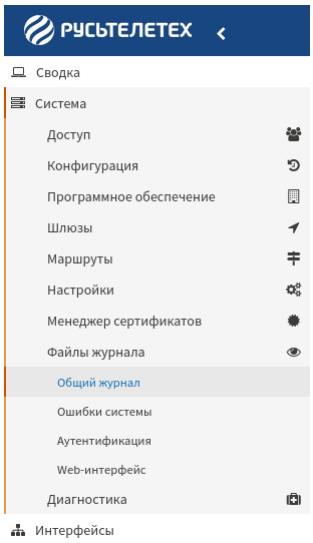


Рис. 243: Переход к просмотру общего журнала

- в правой части экрана появиться таблица общего журнала;

Для перехода к просмотру журнала ошибок системы необходимо:

- нажать на вкладку **«Система»** - **«Файлы журнала»** - **«Ошибки системы»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица журнала ошибок системы;

Для перехода к просмотру журнала аутентификации необходимо:

- нажать на вкладку **«Система»** - **«Файлы журнала»** - **«Аутентификация»**, расположенную в левой части списка объектов управления;

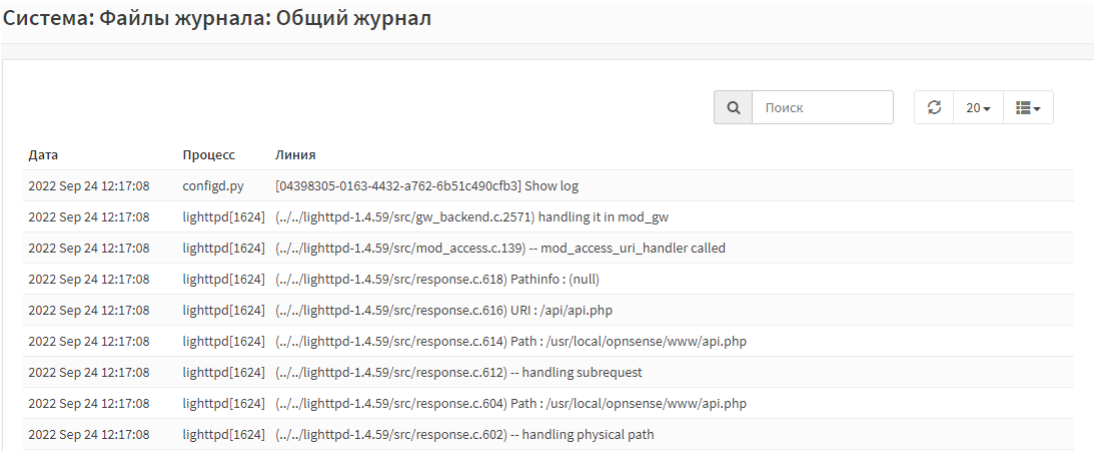


Рис. 244: Таблица общего журнала

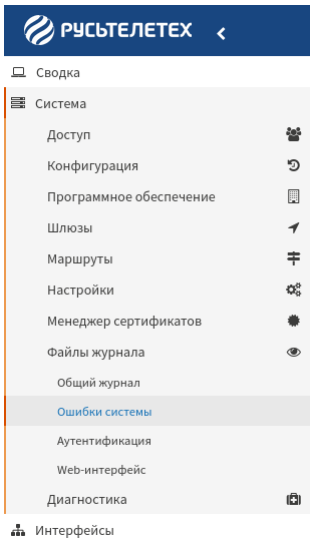


Рис. 245: Переход к просмотру журнала ошибок системы

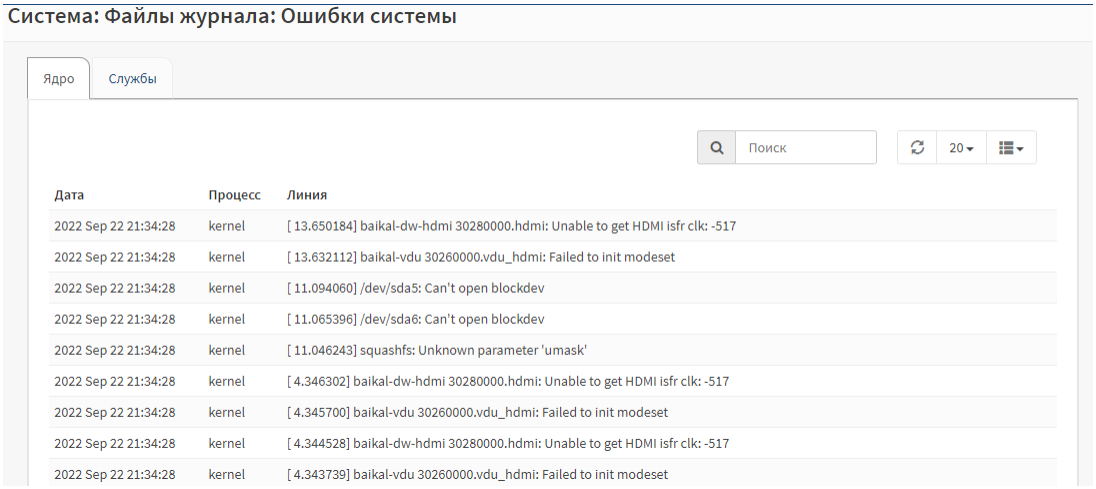


Рис. 246: Таблица журнала ошибок системы

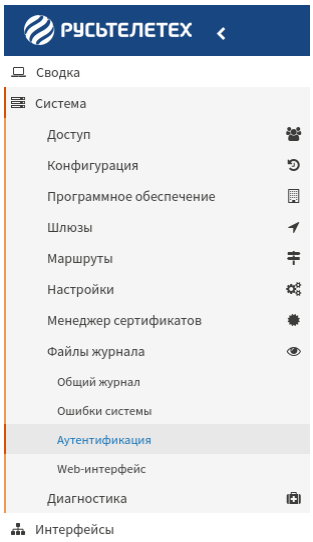


Рис. 247: Переход к просмотру журнала аутентификации

- в правой части экрана появиться таблица журнала аутентификации;

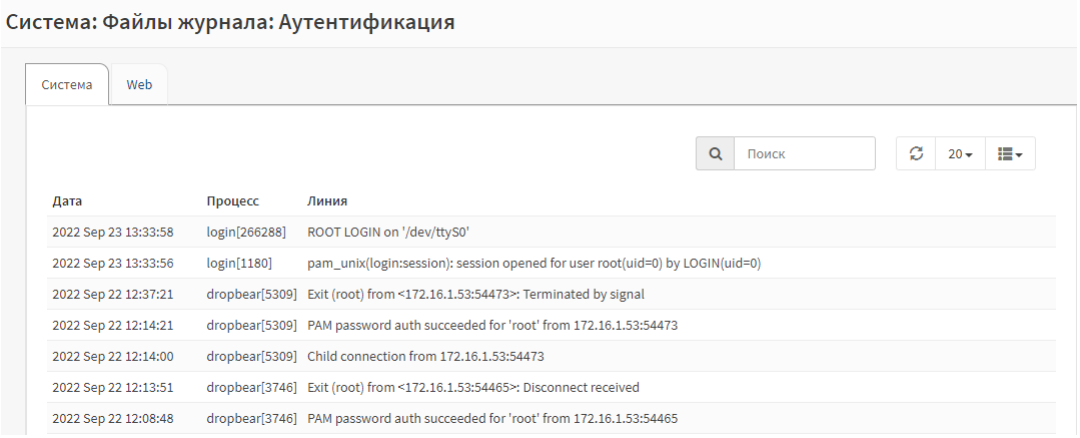


Рис. 248: Таблица журнала аутентификации

Для перехода к просмотру журнала Web-интерфеса необходимо:

- нажать на вкладку **«Система» - «Файлы журнала» - Web-интерфес»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица журнала Web-интерфеса;

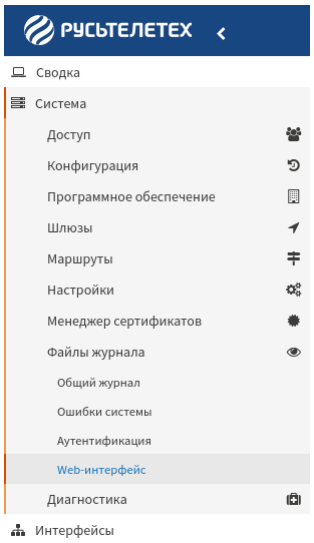


Рис. 249: Переход к просмотру журнала Web-интерфеса

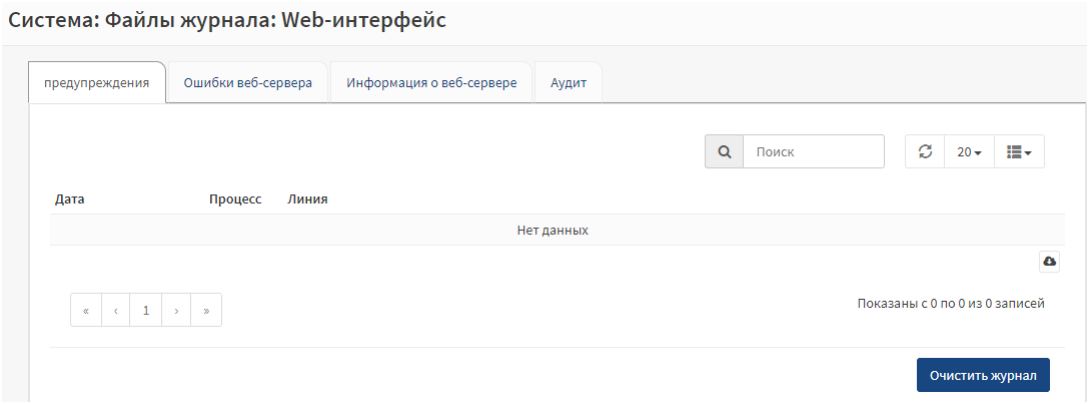


Рис. 250: Таблица журнала Web-интерфеса

Общий журнал

Вкладка Общий журнал содержит таблицу общего журнала, состоящую из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

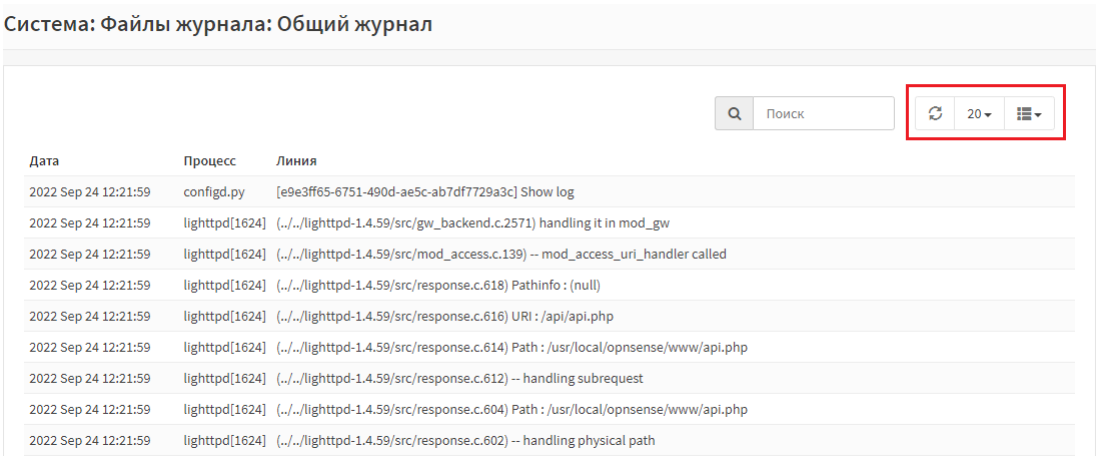


Рис. 251: Фильтры таблицы общего журнала

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы общего журнала
- подтвердить действие в появившемся окне.

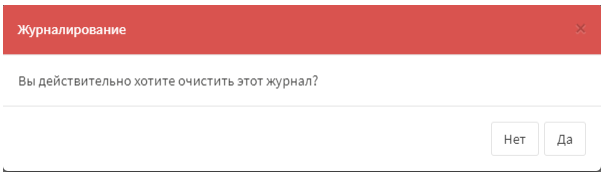


Рис. 252: Подтверждение очистки журнала

Ошибки системы

Ядро

Вкладка **«Ядро»** содержит журнал с информацией об ошибках ядра, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

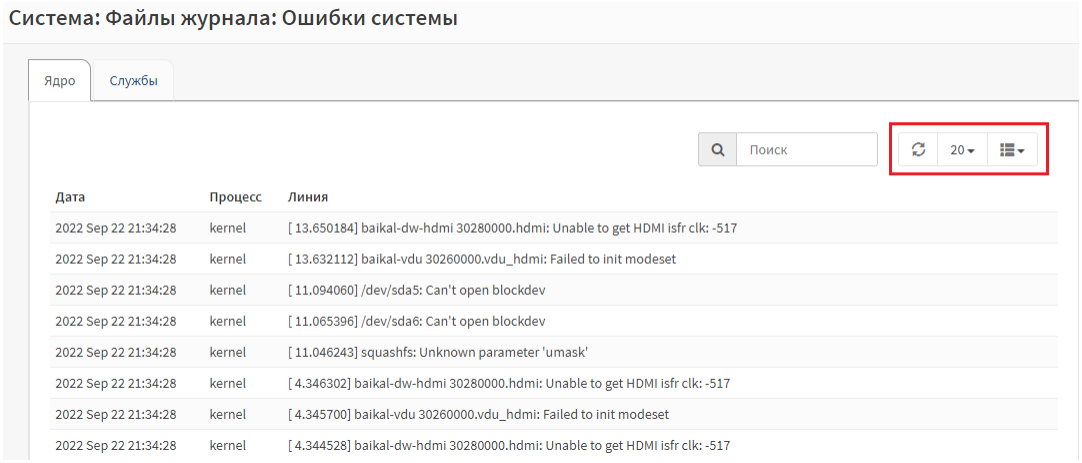


Рис. 253: Фильтры таблицы

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы;
- подтвердить действие в появившемся окне.

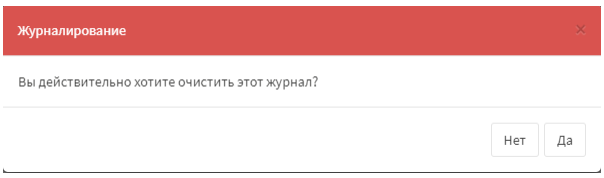


Рис. 254: Подтверждение очистки журнала

Службы

Вкладка **«Службы»** содержит журнал с информацией о системных ошибках служб, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

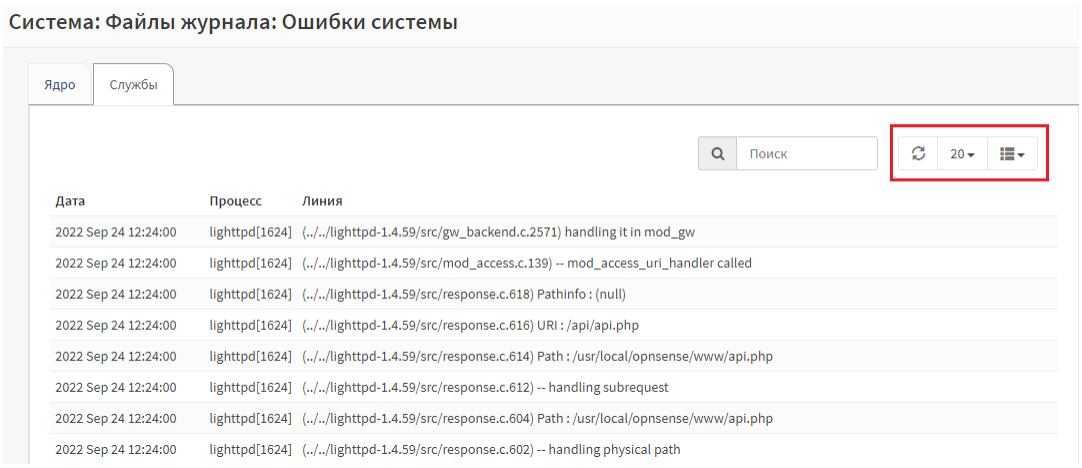


Рис. 255: Фильтры таблицы

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы;

Аутентификация

Система

Вкладка **«Система»** содержит журнал с информацией об аутентификации системы, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы;

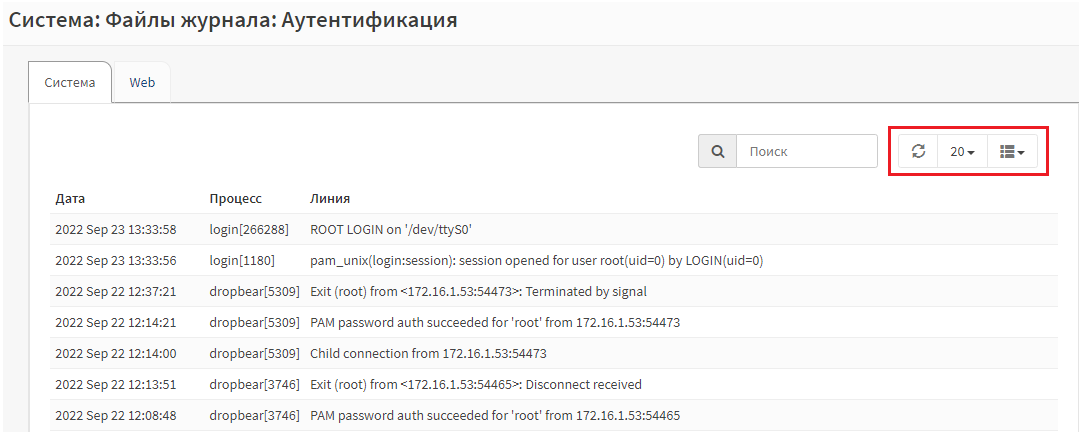


Рис. 256: Фильтры таблицы

- подтвердить действие в появившемся окне.

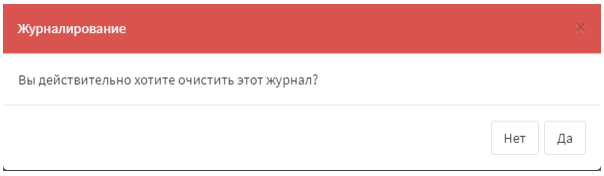


Рис. 257: Подтверждение очистки журнала

Веб

Вкладка **«Веб»** содержит журнал с информацией об аутентификации Веб, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы.

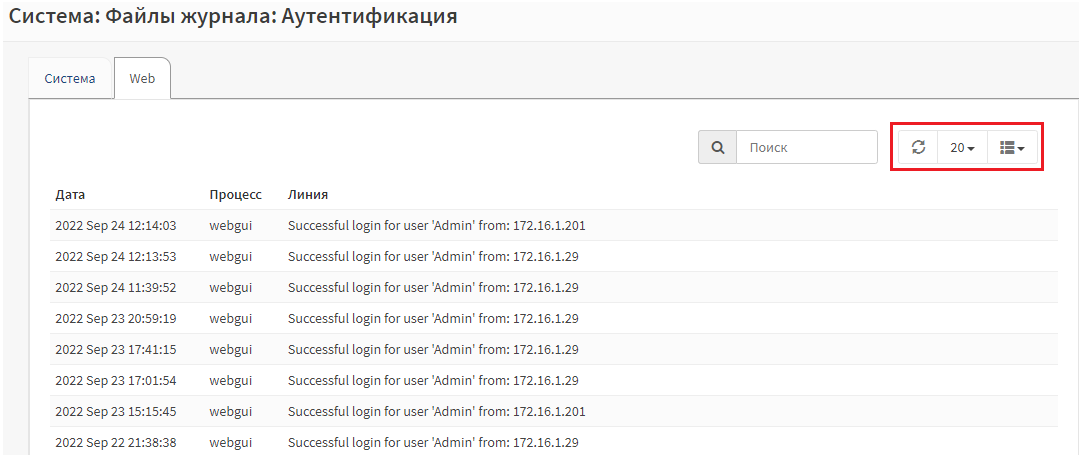


Рис. 258: Фильтры таблицы

Web-интерфейс

Предупреждения

Вкладка **«Предупреждения»** содержит журнал с информацией о предупреждениях веб, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

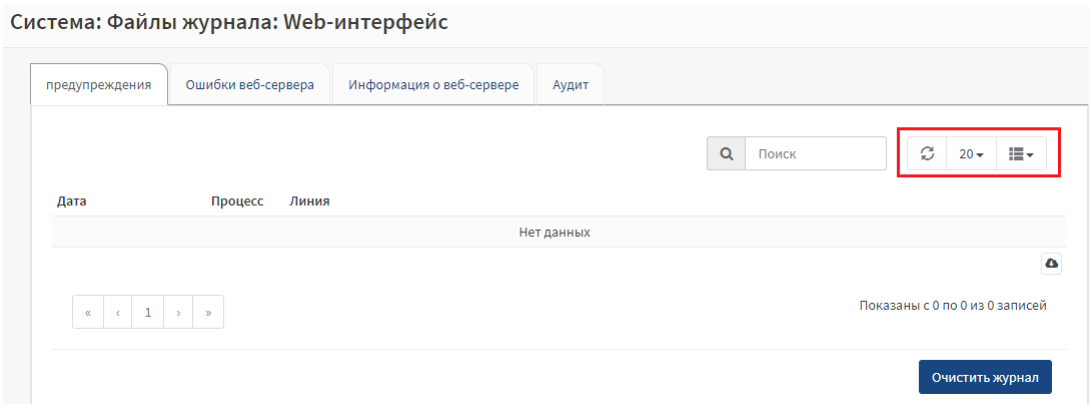


Рис. 259: Фильтры таблицы

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы;
- подтвердить действие в появившемся окне.

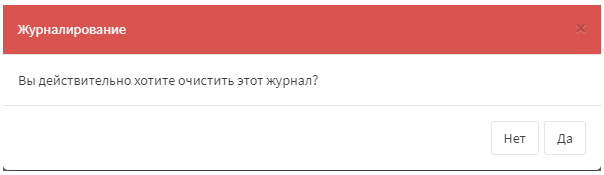


Рис. 260: Подтверждение очистки журнала

Ошибки Веб-сервера

Вкладка **«Ошибки Веб-сервера»** содержит журнал с информацией об ошибках Веб-сервера, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

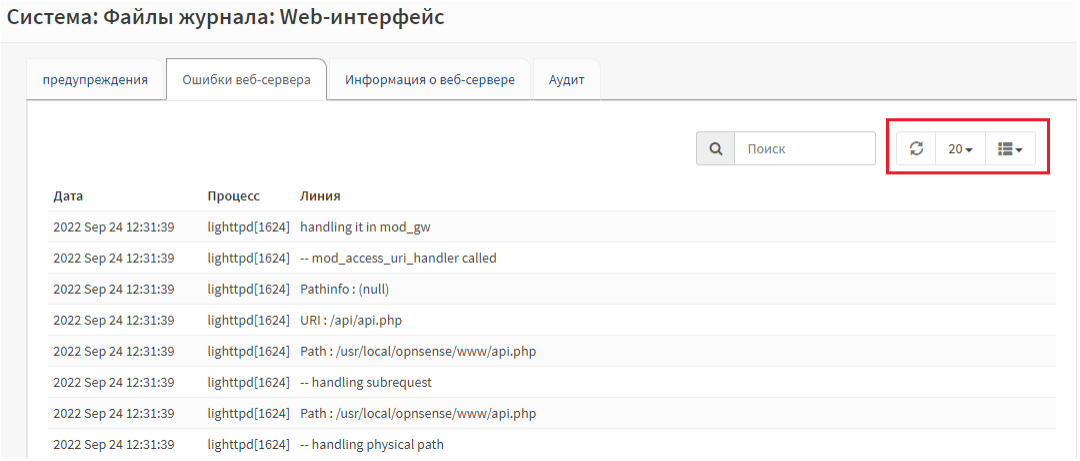


Рис. 261: Фильтры таблицы

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы;

Информация о Веб-сервере

Вкладка **«Информация о веб-сервере»** содержит журнал с информацией о Веб-сервере, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

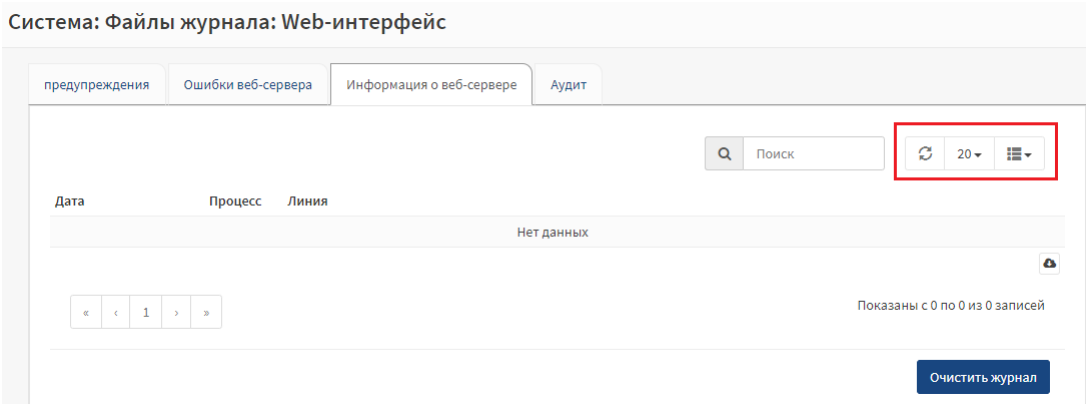


Рис. 262: Фильтры таблицы

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы;

Аудит

Вкладка **«Аудит»** содержит журнал с информацией аудита Web-интерфейса, состоящий из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные таблицы.

Для очистки журнала необходимо:

- нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу таблицы.

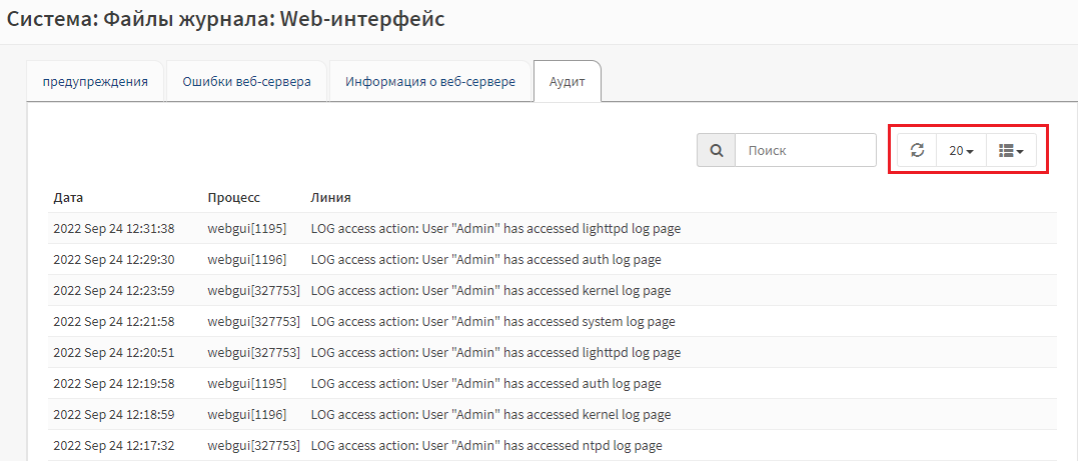


Рис. 263: Фильтры таблицы

2.7.3.9 Диагностика

Для перехода к просмотру служб необходимо:

- нажать на вкладку **«Система»** - **«Диагностика»** - **«Службы»**, расположенную в левой части списка объектов управления;

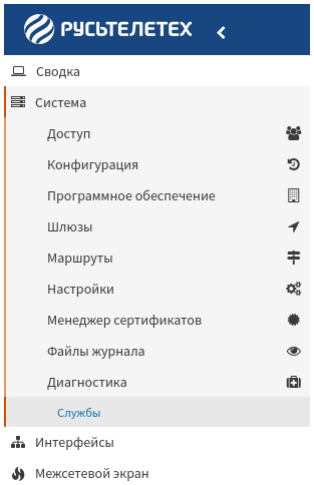


Рис. 264: Переход к просмотру служб

- в правой части экрана появиться таблица служб.

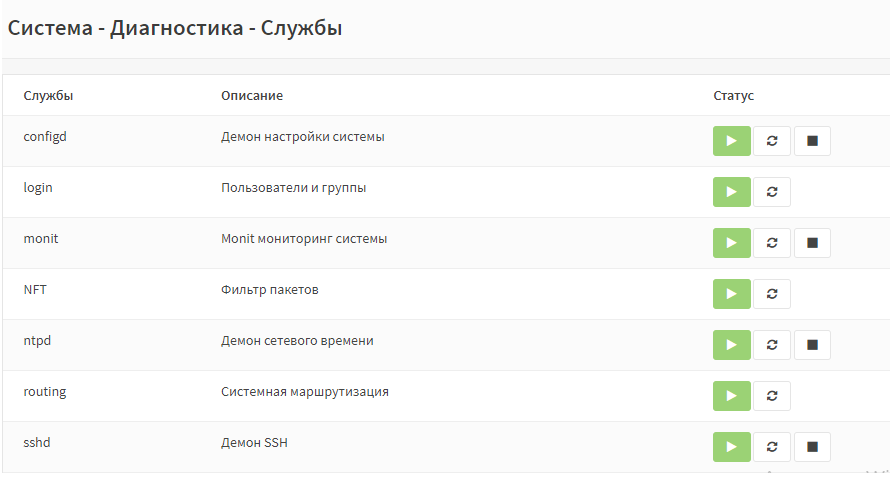


Рис. 265: Таблица служб

Службы

Вкладка **«Службы»** содержит таблицу, состоящую из следующих колонок:

- **«Службы»** - наименование службы;
- **«Описание»** - краткое описание службы;
- **«Статус»** - позволяет запустить, остановить, перезапустить необходимую службу;
- **«Проверка целостности»** - проверка целостности служб.

2.7.4 Интерфейсы

Для редактирования интерфейса необходимо:

- нажать на вкладку **«Интерфейсы»** - **«[LAN]»**, расположенную в левой части списка объектов управления;

Для просмотра назначения портов необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Назначения портов»**, расположенную в левой части списка объектов управления;

Для просмотра общей информации интерфейса необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Обзор»**, расположенную в левой части списка объектов управления;

Для просмотра виртуальных IP-адресов необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Виртуальные IP-адреса»** - **«Настройки»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица виртуальных IP-адресов;
- нажать кнопку  для добавления нового виртуального IP-адреса в таблицу.
- нажать кнопку  для удаления виртуального IP-адреса из таблицы.

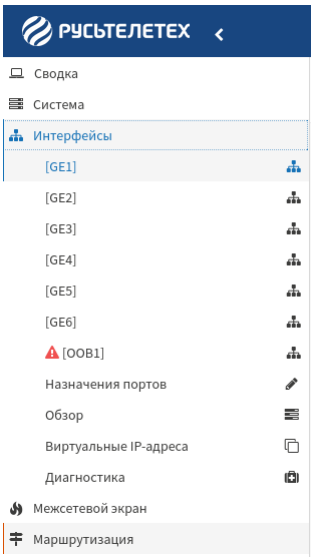


Рис. 266: Переход к редактированию интерфейса

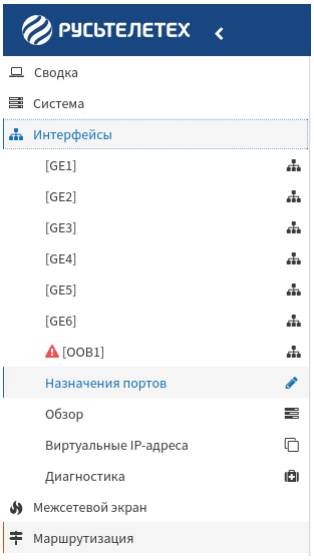


Рис. 267: Переход к просмотру назначения портов

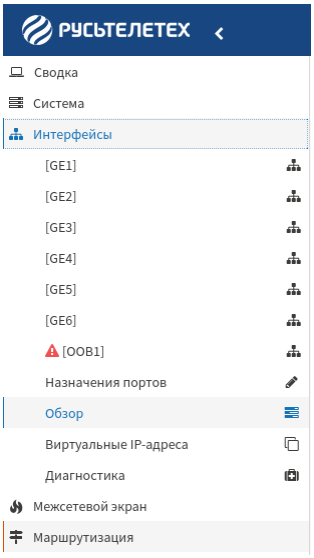


Рис. 268: Переход к просмотру общей информации интерфейса

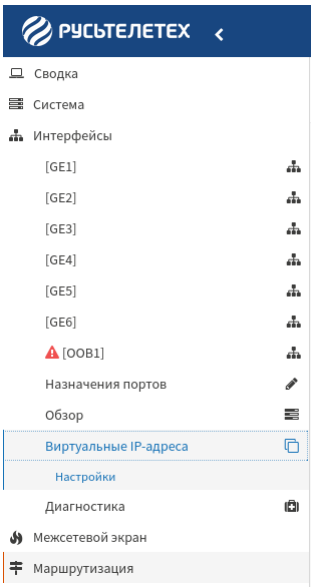


Рис. 269: Переход к просмотру виртуальных IP-адресов

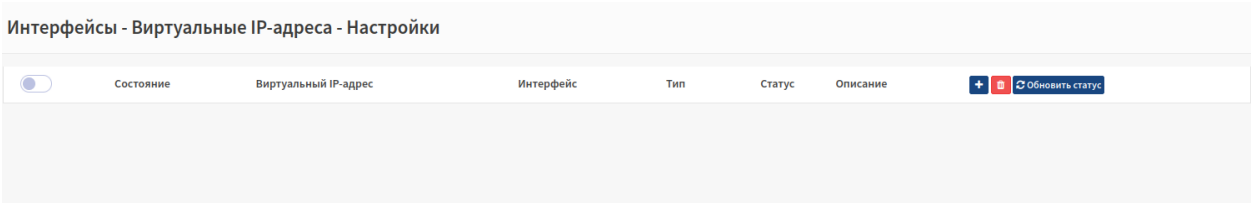


Рис. 270: Таблица виртуальных IP-адресов

- нажать кнопку 

для обновления статуса виртуального IP-адреса в таблице.

Для просмотра ARP-таблицы необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Диагностика»** - **«ARP-таблица»**, расположенную в левой части списка объектов управления;

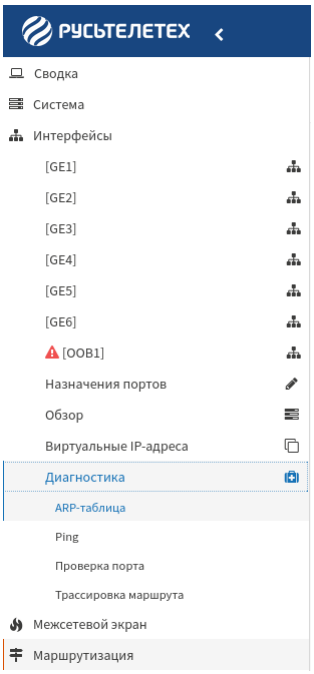


Рис. 271: Переход к просмотру ARP-таблицы

Для просмотра Ping необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Диагностика»** - **«Ping»**, расположенную в левой части списка объектов управления;

Для просмотра проверки порта необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Диагностика»** - **«Проверка порта»**, расположенную в левой части списка объектов управления;

Для просмотра трассировки маршрута необходимо:

- нажать на вкладку **«Интерфейсы»** - **«Диагностика»** - **«Трассировка маршрута»**, расположенную в левой части списка объектов управления;

2.7.4.1 [LAN]

Включение интерфейса

В разделе **«Базовая конфигурация»** необходимо:

- в поле **«Включить»** установить переключатель напротив параметра **«Включить интерфейс»** в случае необходимости включить интерфейс;

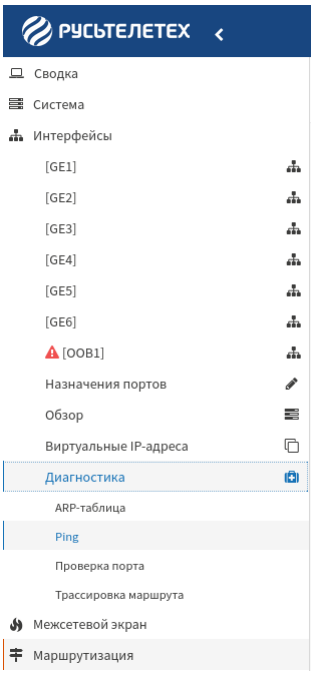


Рис. 272: Переход к просмотру Ping

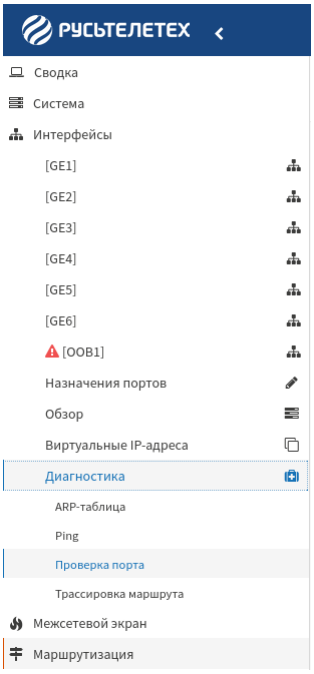


Рис. 273: Переход к просмотру проверки порта

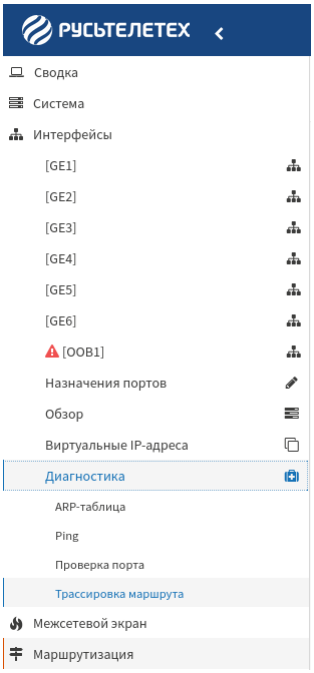


Рис. 274: Переход к просмотру трассировки маршрута

Базовая конфигурация

В разделе **«Базовая конфигурация»** необходимо:

- в поле **«Блокировать»** установить переключатель напротив параметра **«Предотвращение удаления интерфейса»** в случае необходимости предотвращения удаления интерфейса;
- в поле **«Системное имя интерфейса»** ознакомиться с настоящим именем устройства интерфейса;
- в поле **«Описание»** ввести описание/имя для интерфейса (в случае необходимости).

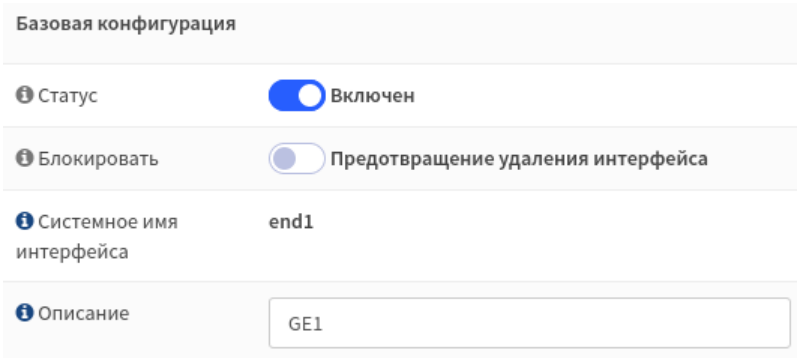


Рис. 275: Настройка базовой конфигурации

Общая конфигурация

В разделе **«Общая конфигурация»** необходимо:

- в поле **«Тип конфигурации IPv4»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 99: Выбор параметров

Параметр
Отсутствует
Статический IPv4
DHCP

- в поле **«Включить IPv6 маршрутизацию»** установить переключатель в случае необходимости включить IPv6 маршрутизацию;
- в поле **«Тип конфигурации IPv6»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 100: Выбор параметров

Параметр
Отсутствует
Статический IPv6

- в поле **«Максимальный размер кадра»** установить численное значение максимального размера кадра.

Примечание

При отсутствии численного значения максимального размера кадра будет использоваться значение по умолчанию сетевой карты. По умолчанию это значение равно 1500 байтам, но может варьироваться в зависимости от обстоятельств

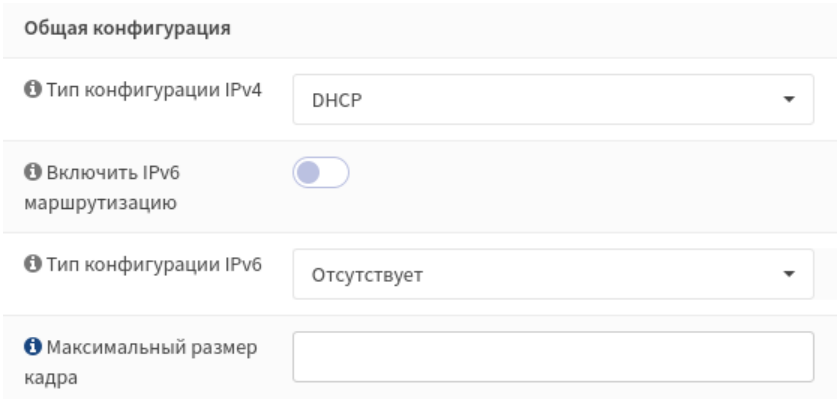


Рис. 276: Настройка общей конфигурации

Конфигурация статического IPv4-адреса

Важно

Конфигурацию статического IPv4-адреса можно провести при выборе параметра **«Статический IPv4»** в поле **«Тип конфигурации IPv4»** раздела **«Общая конфигурация»**

В разделе **«Конфигурация статического IPv4-адреса»** необходимо:

- в поле **«IPv4-адрес»** указать IP адрес в CIDR формате, затем указать длину префикса маски подсети (от 1 до 32);
- в поле **«Публичный IPv4-адрес шлюза»** выбрать из выпадающего списка существующий шлюз или автоматическое обнаружение шлюза.

Примечание

Если интерфейс является интерфейсом с несколькими глобальными сетями, необходимо выбрать существующий шлюз из списка или добавить новый шлюз

Примечание

Для одиночных интерфейсов WAN необходимо создать шлюз, но настроить его на автоматическое обнаружение

Примечание

Для локальной сети нет необходимости в настройке шлюза

Для добавления нового шлюза необходимо:

- в поле **«Публичный IPv4-адрес шлюза»** нажать кнопку **«+»**;
- в открывшейся вкладке **«Добавить новый шлюз»** следует:
  - в поле **«Шлюз по умолчанию»** установить переключатель в случае необходимости сделать новый шлюз шлюзом по умолчанию;
  - в поле **«Дальний шлюз»** установить переключатель в случае необходимости сделать новый шлюз дальним шлюзом;
  - в поле **«Шлюз с несколькими глобальными сетями»** установить переключатель в случае необходимости делать новый шлюз шлюзом с несколькими глобальными сетями;
  - в поле **«Имя Шлюза»** указать имя шлюза;
  - в поле **«IPv4-адрес шлюза»** указать адрес шлюза;
  - в поле **«Описание»** ввести описание шлюза.

Для сохранения отредактированного интерфейса необходимо нажать кнопку **«Сохранить»**

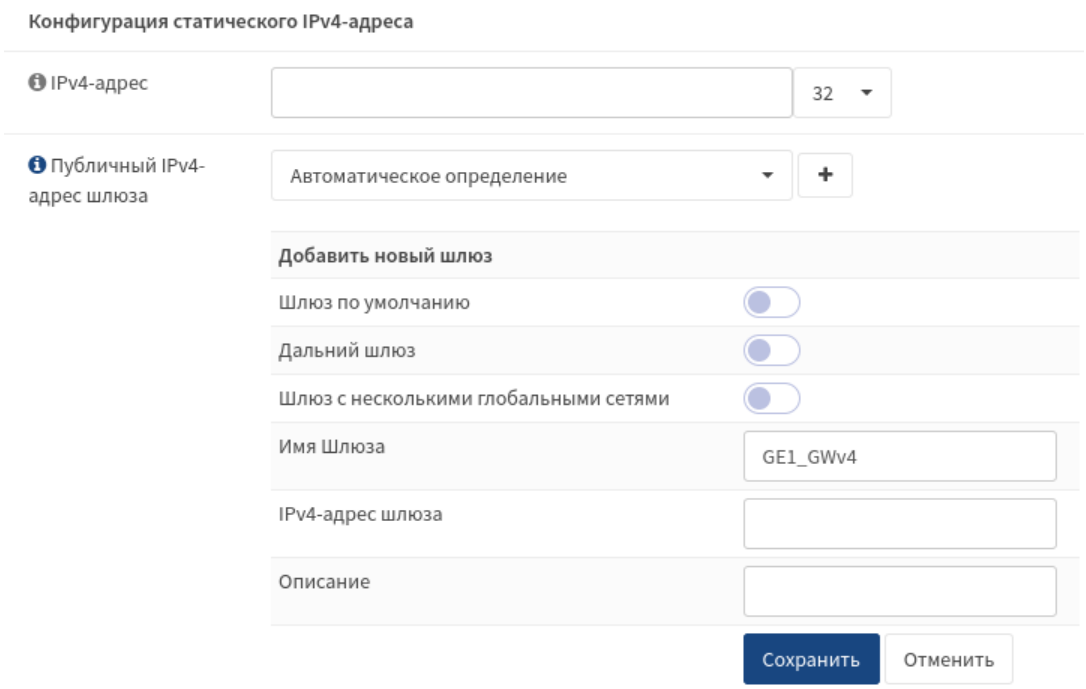
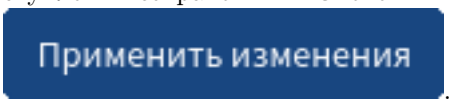


Рис. 277: Настройка статического IPv4-адреса

.

Для вступления сохраненных изменений в силу необходимо нажать кнопку **«Применить изменения»** 

.

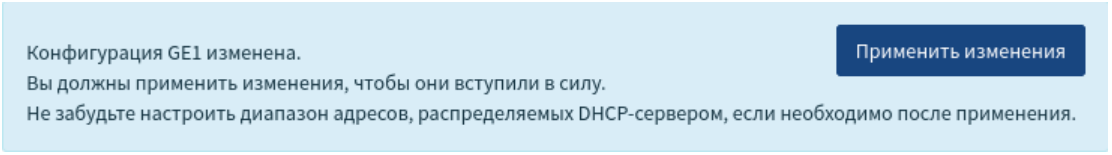


Рис. 278: Вступление сохраненных изменений в силу

2.7.4.2 Назначения портов

В данном разделе пользователь может привязать выбранный порт одного из локальных сетевых интерфейсов устройства к определенному сетевому порту.

Для редактирования назначений портов необходимо:

- в колонке **«Системный интерфейс»** выбрать из выпадающего списка один из портов, соответствующих интерфейсу из колонки **«Интерфейс»**

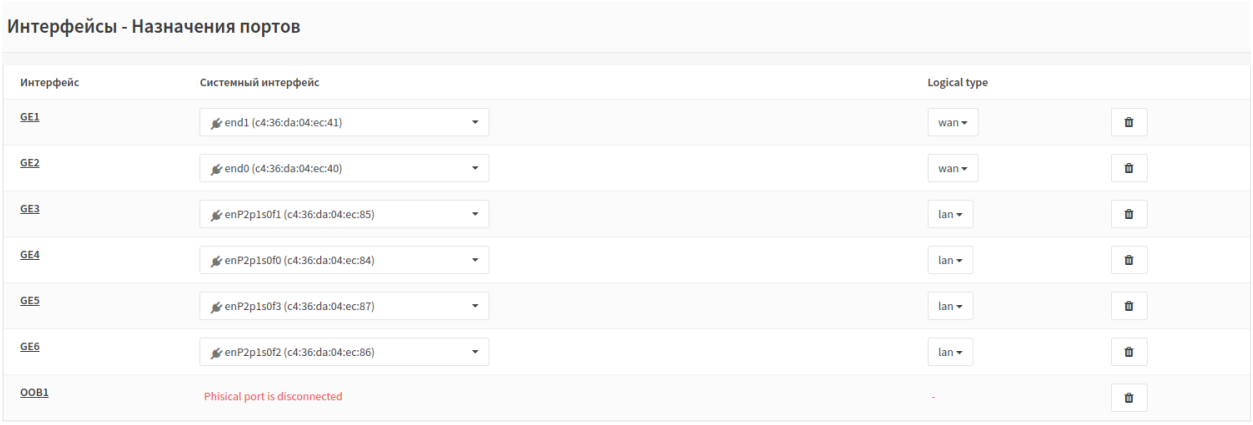


Рис. 279: Таблица назначения портов

2.7.4.3 Обзор

В данном разделе пользователь может ознакомиться с дополнительными техническими характеристиками и статистическими данными используемого интерфейса.

Дополнительные технические характеристики и статистические данные используемого интерфейса соответствуют таблице.

Рис. 280: Список интерфейсов

Таблица 101: Характеристики

Параметр	Значение
Статус	Пропустить пакет
DHCP	Состояние DHCP сервера
MAC-адрес	Используемый MAC-адрес
Максимальный размер кадра	Числовое значение максимального размера кадра
IPv4-адрес	IP адрес
IPv6-адрес	IP адрес
IPv6 link-local	IPv6 unicast address
Входящие/исходящие пакеты	Количество входящих/исходящих пакетов
Входящие/исходящие байты	Количество входящих/исходящих байтов
Входящие/исходящие пакеты отброшены	Количество входящих/исходящих отброшенных пакетов
Входящие/исходящие ошибки	Количество входящих/исходящих ошибок
Коллизии	Количество произошедших коллизий

2.7.4.4 Виртуальные IP-адреса

Для редактирования виртуальных IP-адресов необходимо:

- в поле **«Режим»** выбрать из выпадающего списка один из необходимых режимов
- в поле **«Интерфейс»** выбрать из выпадающего списка один из необходимых интерфейсов
- в поле **«Адрес»** ввести необходимый адрес

Примечание

Это должно быть маска подсети, она не задает CIDR-диапазон

- в поле **«Пароль виртуального IP-адреса»** ввести пароль группы VHID
- в поле **«Группа VHID»** ввести группу VHID, которая будет распределена между компьютерами
- в поле **«Частота синхронизации»** ввести частоту, с которой это устройство будет отправлять сообщения

Примечание

Частота ведущего устройства равна 0. В противном случае ведущее устройство определяет наименьшая комбинация обоих значений в кластере

- в поле **«Dead timer»** установить Dead timer

Примечание

Как долго ждать не отвечающего мастера, прежде чем считать его оконченным

- в поле **«Описание»** ввести необходимое описание

Для сохранения настроек необходимо нажать кнопку **«Сохранить»** 

.

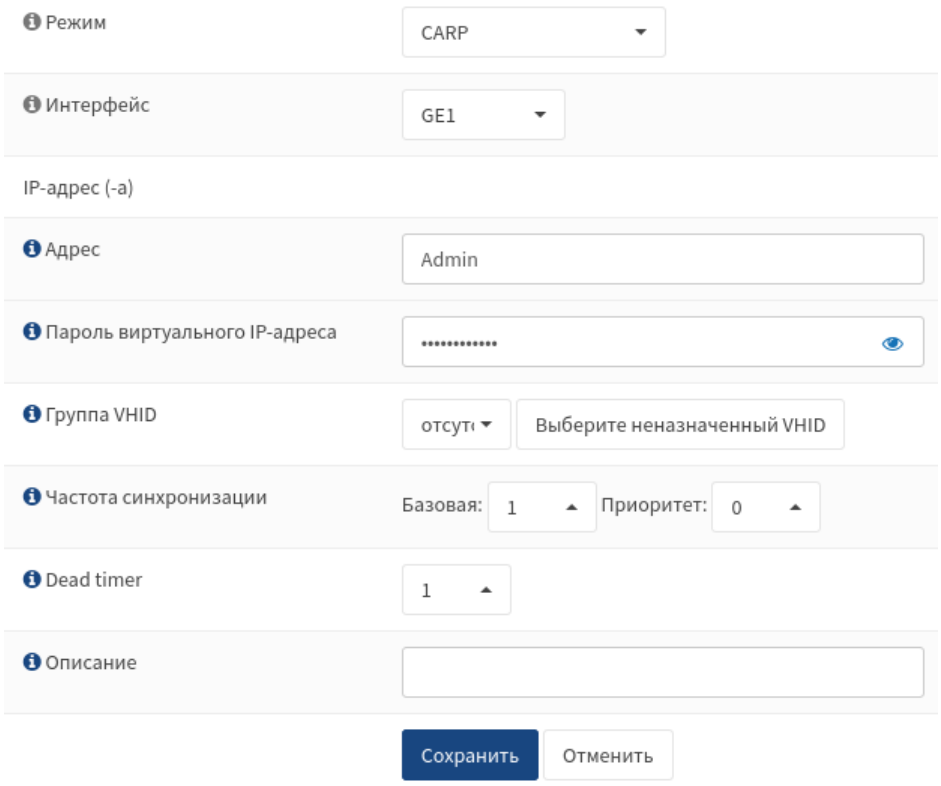


Рис. 281: Настройка виртуального IP-адреса

2.7.4.5 Диагностика

Раздел **«Диагностика»** необходим для обработки информации о состоянии сети по средствам ARP-таблицы. Раздел содержит настройку пинг, проверку портов и трассировку маршрутов.

ARP-таблица

ARP-таблица необходима для преобразования IP-адреса в MAC-адрес.

ARP-таблица отображает:

- IP-адреса подключенных к серверу сетевых устройств;
- MAC-адреса подключенных к серверу сетевых устройств;
- производителя сетевых устройств;
- имя устройства интерфейса;
- имя интерфейса;
- имя хоста.

Для обновления ARP-таблицы необходимо нажать кнопку **«Обновить»** 

.

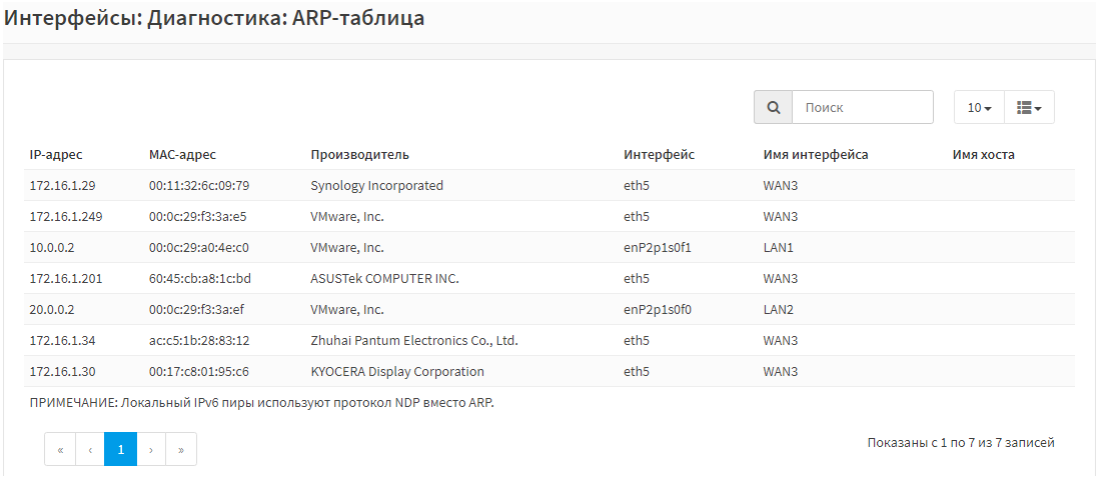


Рис. 282: ARP-таблица

Для очистки ARP-таблицы необходимо нажать кнопку **«Очистить»** 

.

Ping

Для Ping необходимо:

- в поле **«Хост»** указать адрес хоста;
- в поле **«Протокол IP»** выбрать из выпадающего списка необходимый протокол IP;
- в поле **«IP-адрес источника»** выбрать из выпадающего списка необходимый IP-адрес источника;
- в поле **«Количество»** выбрать из выпадающего списка необходимое количество;

Нажать кнопку 

.

Проверка порта

Для проверки порта необходимо:

- в поле **«Хост»** указать адрес хоста;
- в поле **«Порт»** указать адрес порта;
- в поле **«Протокол IP»** выбрать из выпадающего списка необходимый протокол IP;
- в поле **«Порт источника»** выбрать из выпадающего списка необходимый порт источника;
- в поле **«Порт источника»** описать порт источника;

Нажать кнопку 

.

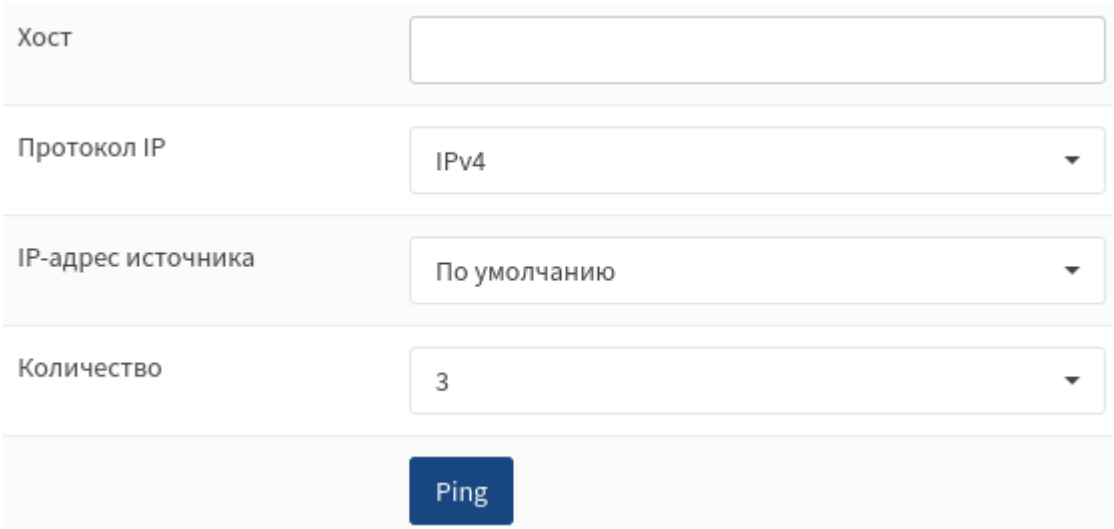


Рис. 283: Настройка ping

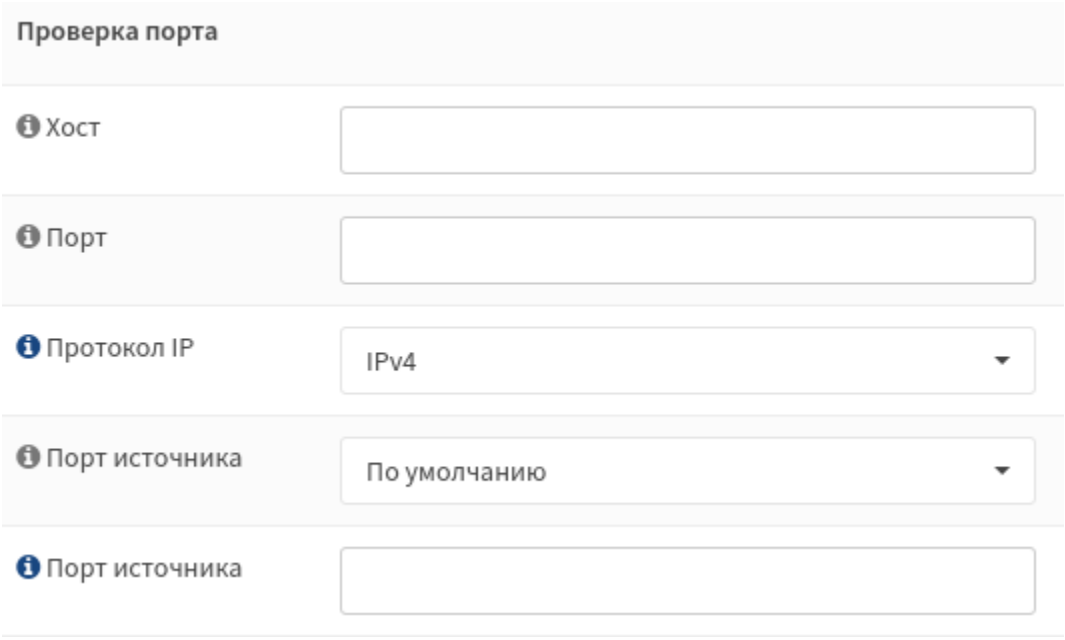


Рис. 284: Настройка проверки порта

Трассировка маршрута

Для трассировки маршрута необходимо:

- в поле **«Хост»** указать адрес хоста;
- в поле **«Протокол IP»** выбрать из выпадающего списка необходимый протокол IP;
- в поле **«IP-адрес источника»** выбрать из выпадающего списка необходимый IP-адрес источника;
- в поле **«Максимальное количество переходов»** выбрать из выпадающего списка максимальное количество переходов;
- в поле **«Обратное преобразование адресов»** установить переключатель в случае необходимости обратного преобразования адресов;
- в поле **«Использовать ICMP»** установить переключатель в случае необходимости использовать ICMP;

Нажать кнопку 

.

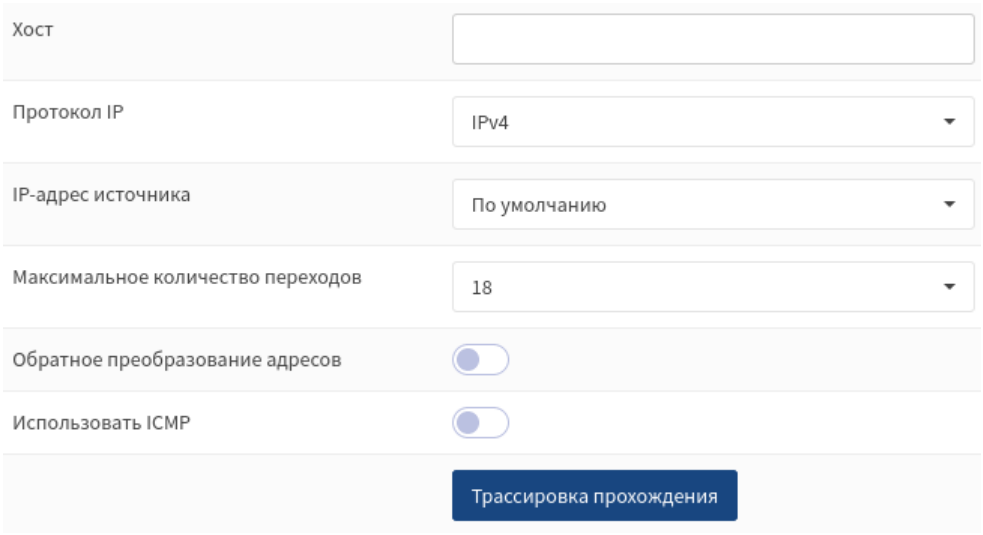


Рис. 285: Настройка трассировки маршрута

2.7.5 Межсетевой экран

Межсетевой экран предназначен для защиты сегментов сети от несанкционированного доступа и разграничения сетевого доступа в информационных системах.

Для перехода к настройкам псевдонимов необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«Псевдонимы»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица псевдонимов;
- нажать кнопку «+» для добавления нового псевдонима в таблицу.

Для перехода к настройкам групп необходимо:

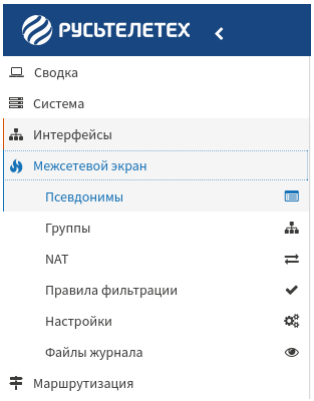


Рис. 286: Переход к настройкам псевдонимов

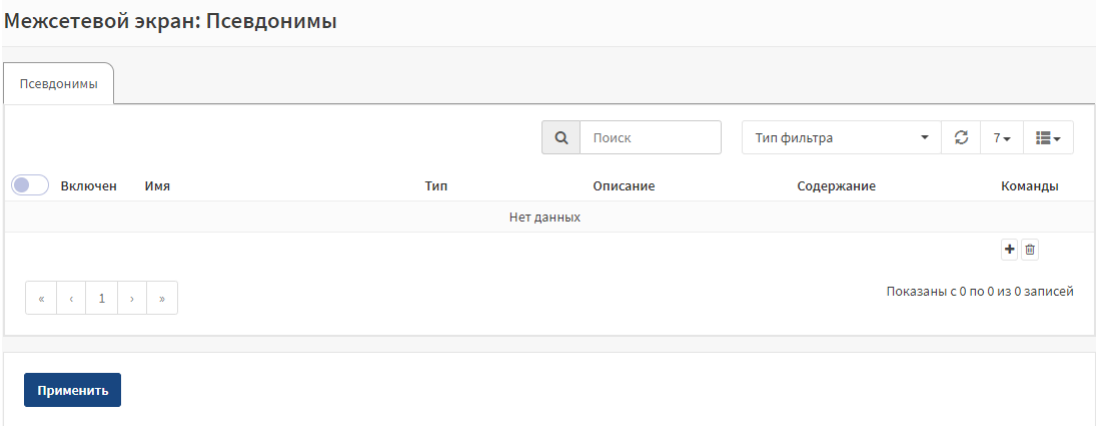


Рис. 287: Таблица псевдонимов

- нажать на вкладку **«Межсетевой экран»** - **«Группы»**, расположенную в левой части списка объектов управления;

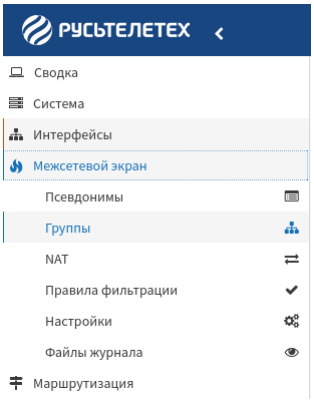


Рис. 288: Переход к настройкам групп

- в правой части экрана появиться таблица групп;

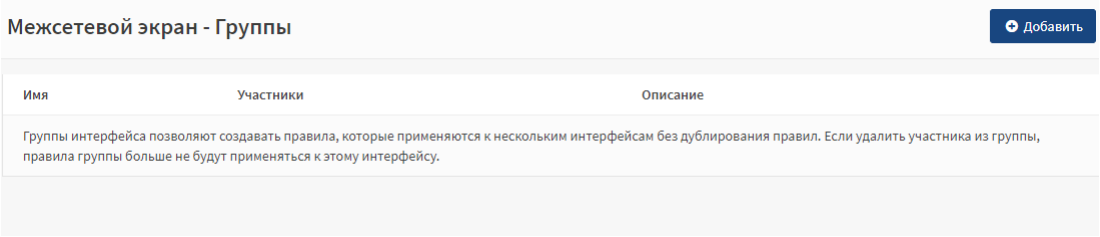


Рис. 289: Таблица групп

- нажать кнопку **«Добавить»**  для добавления новой группы в таблицу.

Для перехода к настройкам правил NAT необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«NAT»**, расположенную в левой части списка объектов управления;

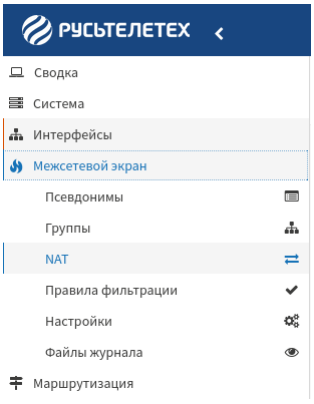


Рис. 290: Переход к настройкам NAT

2.7.5.1 Псевдонимы

Псевдонимы позволяют объединять в себе различные типы данных, это удобно использовать при создании правил межсетевого экрана.

Для настройки псевдонимов необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости включить созданный псевдоним;
- в поле **«Имя»** ввести имя псевдонима;

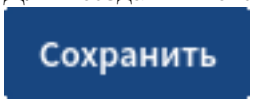
> **Примечание**
>
> Имя псевдонима может состоять только из символов «a-z, A-Z, 0-9 и _». Псевдонимы могут быть вложены с использованием этого имени

- в поле **«Тип»** выбрать из выпадающего списка один из поддерживаемых типов псевдонимов, соответствующих таблице;

Таблица 102: Выбор типа псевдонима

Тип псевдонима	Примечание
Хост(ы)	Позволяет задавать одиночные ip-адреса, а также инвертировать их для последующей блокировки или разрешения
Сеть(и)	Позволяет задавать ip-адреса сетей в формате бесклассовой адресации, а также инвертировать их для последующей блокировки или разрешения
Порт(ы)	Позволяет задавать диапазон портов, а также инвертировать их для последующей блокировки или разрешения
Сетевая группа	Позволяет задавать в себе псевдонимы типа «сети».
MAC-адресс	Позволяет задавать MAC-адреса для последующей их блокировки или разрешения
GeoIP	Позволяет выбрать континенты и страны для последующей их блокировки или разрешения

- в поле **«Содержание»**:
  - задать одиночные IP адреса (при выборе типа псевдонима Хост(ы));
  - задать IP адреса сетей (при выборе типа псевдонима Сеть(и));
  - задать диапазон портов (при выборе типа псевдонима Порт(ы));
  - указать входящие псевдонимы (при выборе типа псевдонима Сетевая группа);
  - задать MAC адреса (при выборе типа псевдонима MAC-адресс);
  - выбрать из колонки **«Регион»** необходимые регионы/континенты и выбрать из колонки **«Страны»** страны (при выборе типа псевдонима GeoIP).
- в поле **«Описание»** ввести описание псевдонима.

Для создания сконфигурированного псевдонима необходимо нажать кнопку **«Сохранить»** 

.

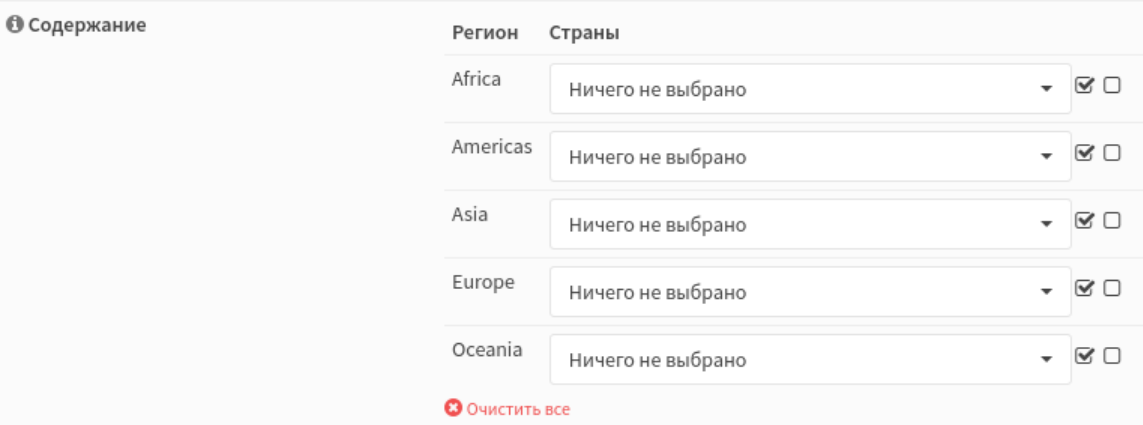


Рис. 291: Настройка псевдонимов GeoIP

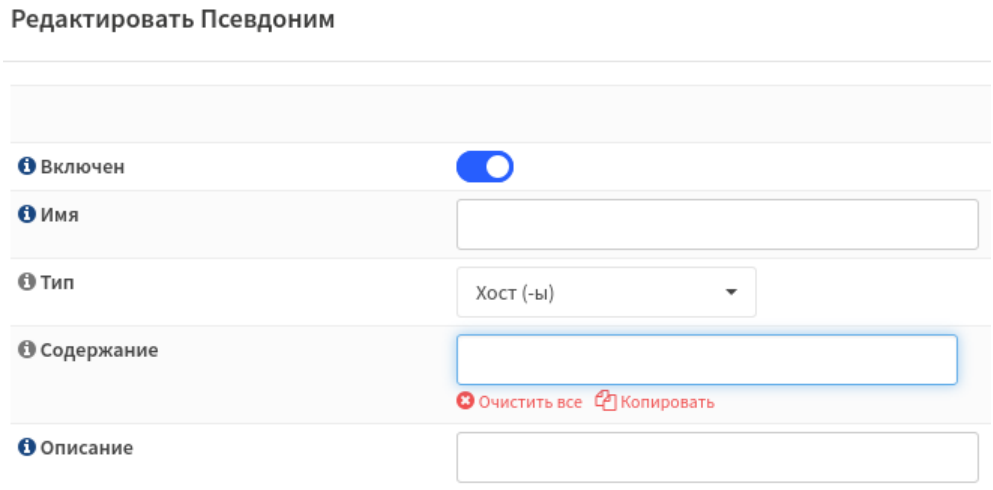


Рис. 292: Добавление псевдонима

Для вступления сконфигурированного псевдонима в силу необходимо нажать кнопку **«Применить»**

Применить .

Для пользователя существует возможность осуществлять поиск, управлять созданными псевдонимами с помощью фильтров таблицы псевдонимов

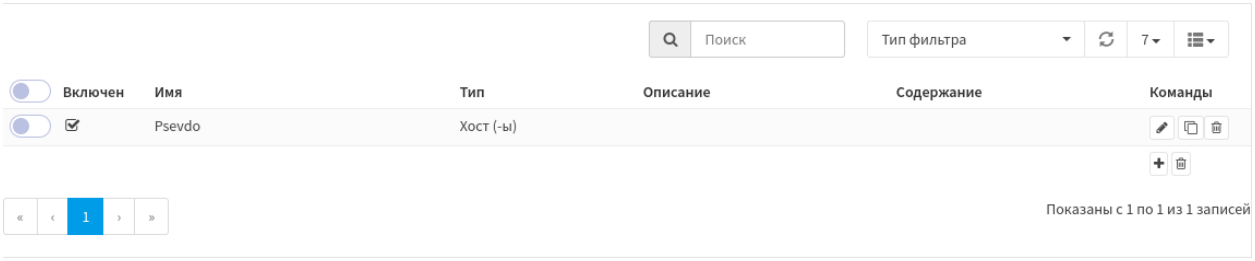


Рис. 293: Фильтры таблицы псевдонимов

2.7.5.2 Группы

Группы позволяют создавать правила, которые применяются к нескольким интерфейсам без дублирования правил. Если удалить участника из группы, правила группы больше не будут применяться к этому интерфейсу.

Для настройки группы необходимо указать:

- в поле **«Имя»** - имя группы;

Примечание

Имя группы не должно содержать цифры или пробелы. Только буквы A–Z, a–z

- в поле **«Описание»** - описание группы;

Примечание

Пользователь может ввести в это поле описание ссылки

- в поле **«Участники»** - выбрать из выпадающего списка один из интерфейсов, входящих в состав группы, и соответствующих таблице.

Таблица 103: Интерфейсы, входящие в состав группы

Интерфейсы, входящие в состав группы
[Интерфейс]
loopback

Для создания сконфигурированной группы необходимо нажать кнопку **«Сохранить»**

Сохранить .

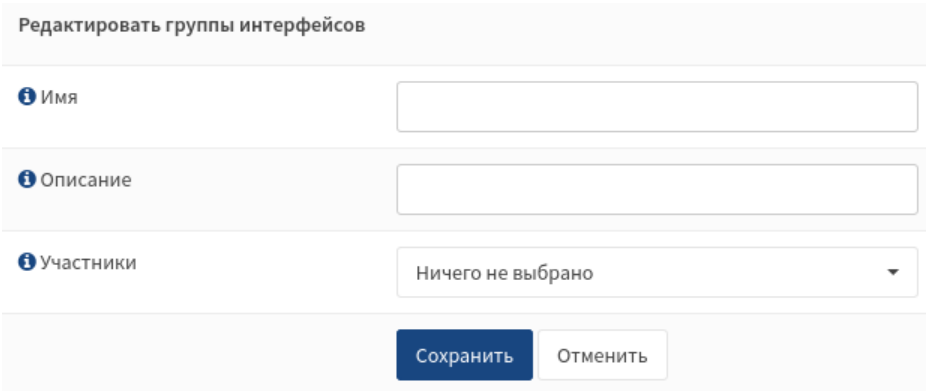


Рис. 294: Настройка группы интерфейсов

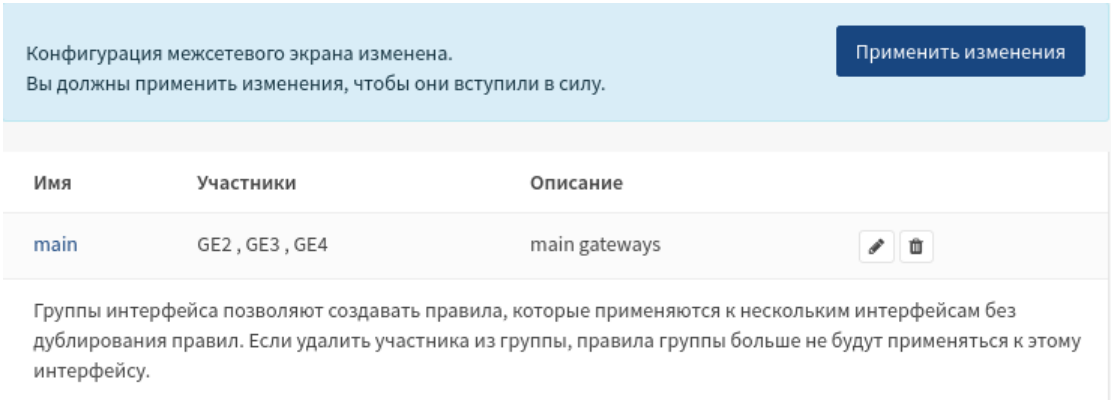
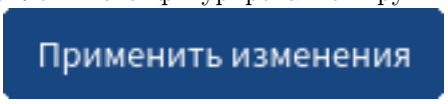


Рис. 295: Сконфигурированная группа

Сконфигурированная группа появиться в таблице групп.

Для вступления сконфигурированной группы в силу необходимо нажать кнопку **«Применить изменения»** 

.

2.7.5.3 NAT

Для перехода к настройкам DNAT (Prerouting) необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«NAT»** - **«DNAT (Prerouting)»**, расположенную в левой части списка объектов управления;

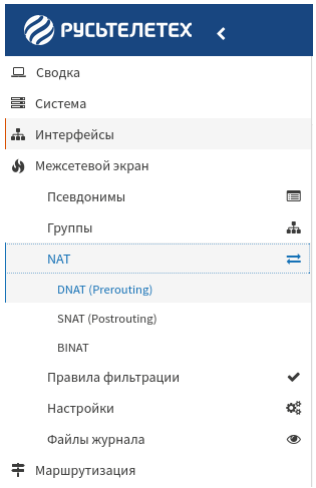


Рис. 296: Переход к настройкам DNAT (Prerouting)

- в правой части экрана появиться таблица DNAT (Prerouting);

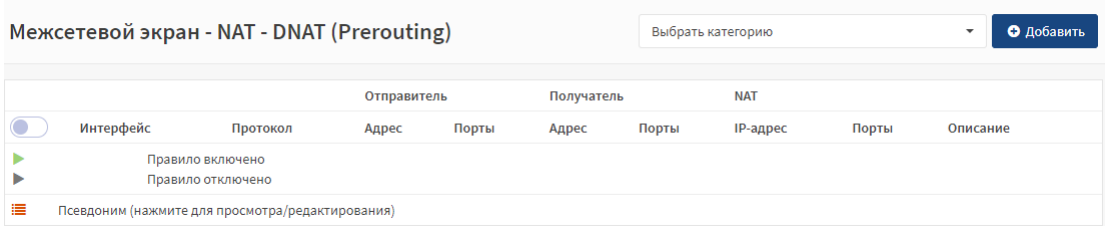


Рис. 297: Таблица DNAT (Prerouting)

- нажать кнопку **«Добавить»** 

для добавления новой группы в таблицу.

Для перехода к настройкам SNAT (Postrouting) необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«NAT»** - **«SNAT (Postrouting)»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица SNAT (Postrouting);

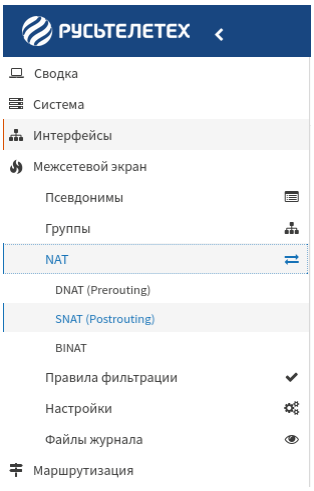


Рис. 298: Переход к настройкам SNAT (Postrouting)

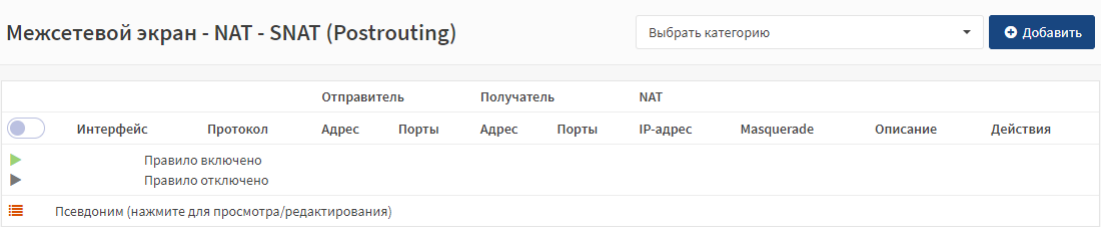


Рис. 299: Таблица SNAT (Postrouting)

- нажать кнопку **«Добавить»**  для добавления новой группы в таблицу.

Для перехода к настройкам BINAT необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«NAT»** - **«BINAT»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица BINAT;
- нажать кнопку **«Добавить»**  для добавления новой группы в таблицу.

DNAT (Prerouting)

DNAT (Destination NAT) необходим для изменения ip-адреса получателя сетевого пакета. В DNAT присутствует возможность переадресации хостов или портов.

Примечание

Правила DNAT обрабатываются первыми

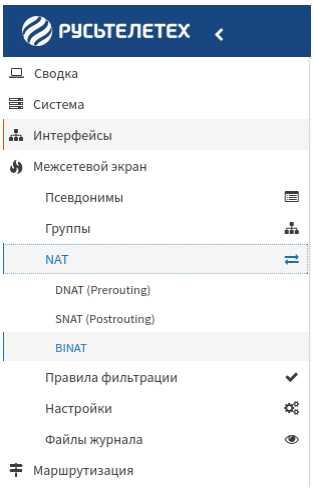


Рис. 300: Переход к настройкам BINAT

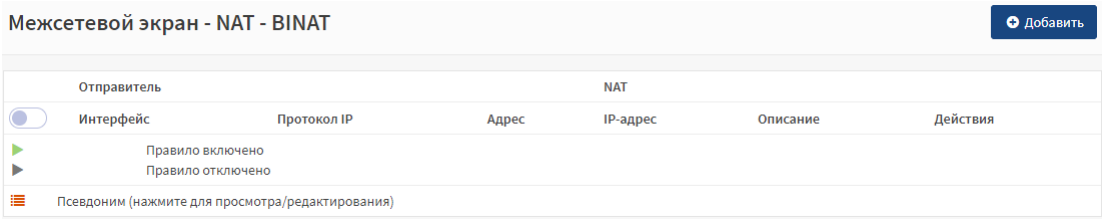


Рис. 301: Таблица BINAT

Отключение правила

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Отключить»** установить переключатель в случае необходимости отключить это правило, не удаляя его из списка;

Интерфейс

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Интерфейс»** выбрать из выпадающего списка один из интерфейсов, соответствующих таблице;

Таблица 104: Интерфейсы

Интерфейсы
Любой
[LAN]
Loopback
[Группы]

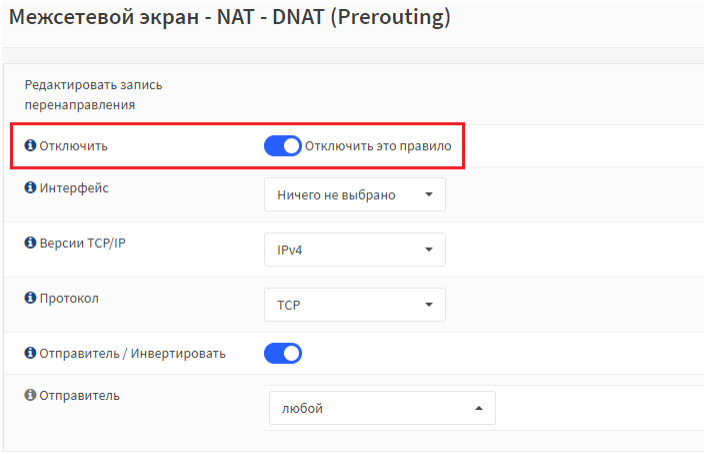


Рис. 302: Отключение настроенного правила DNAT

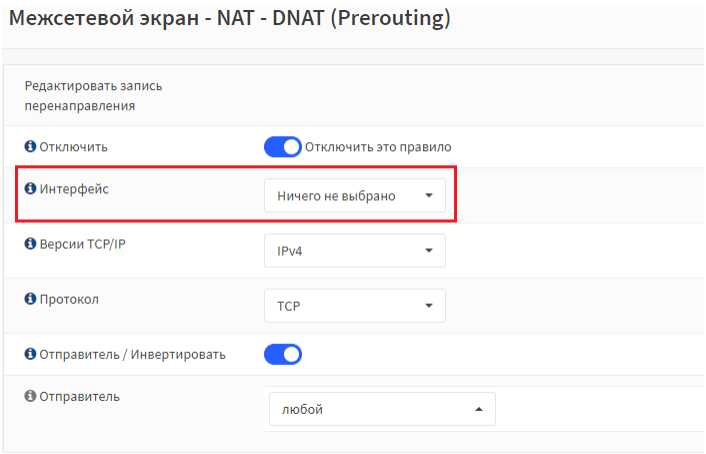


Рис. 303: Выбор интерфейса

Протокол передачи данных

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Версии TCP/IP»** выбрать из выпадающего списка интернет-протокол IPv4;

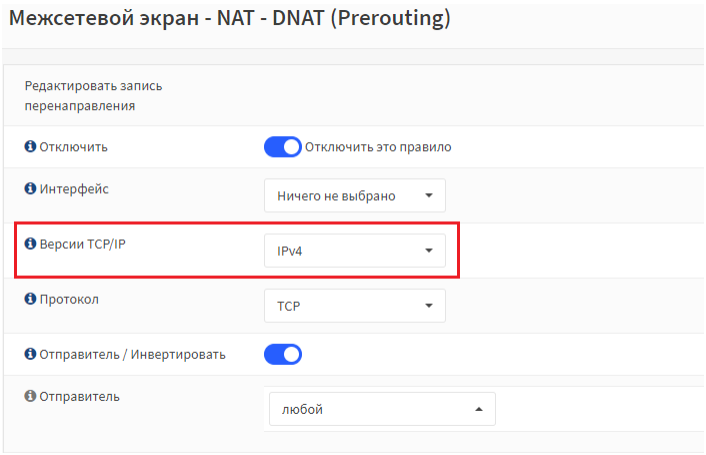


Рис. 304: Выбор версии TCP/IP

- в поле **«Протокол»** выбрать из выпадающего списка один из IP-протоколов, соответствующих таблице;

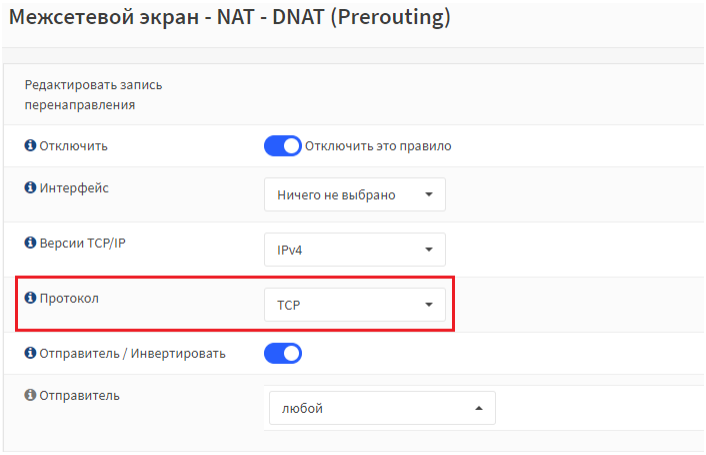


Рис. 305: Выбор протокола

Таблица 105: IP протоколы

IP протоколы
any (Любой)
TCP
UDP
ICMP

Адрес отправителя пакета

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Отправитель/инвертировать»** установить переключатель в случае необходимости инверсии выбранного значения;

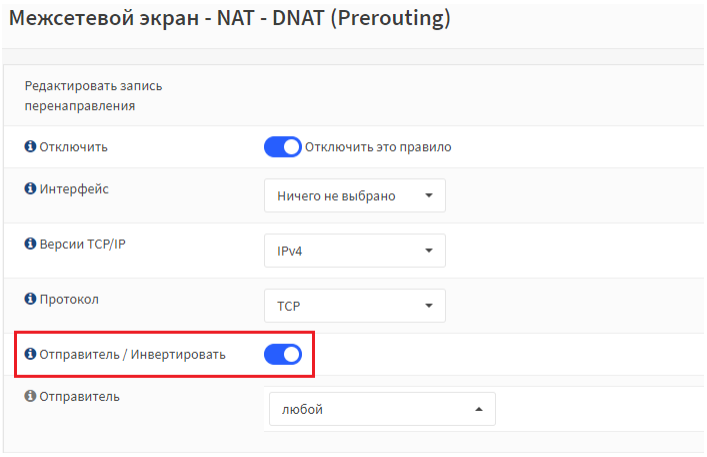


Рис. 306: Установка параметра

- в поле **«Отправитель»** выбрать из выпадающего списка один из следующих параметров:
  - **«Любой»** для установки любого адреса отправителя;

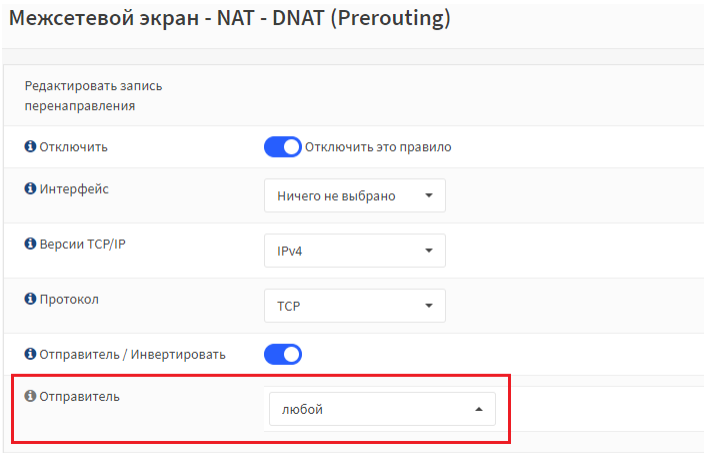


Рис. 307: Выбор параметра **«любой»**

  - **«Единственный хост или сеть»** для установки определенного адреса отправителя, затем в открывшейся строке установить определенный адрес отправителя;

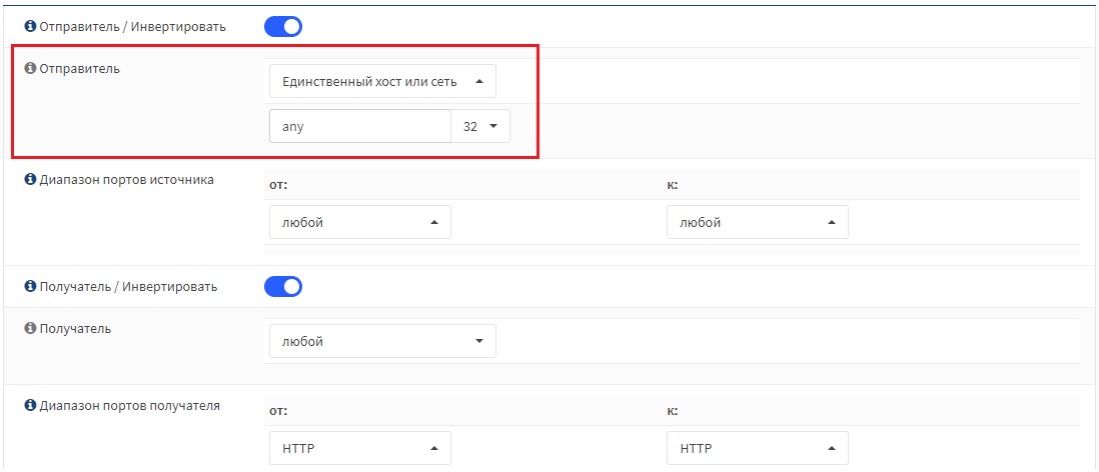


Рис. 308: Выбор параметра **«Единственный хост или сеть»**

Адрес получателя пакета

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Получатель/инвертировать»** установить переключатель в случае необходимости использовать этот параметр, чтобы инвертировать смысл правила совпадения;

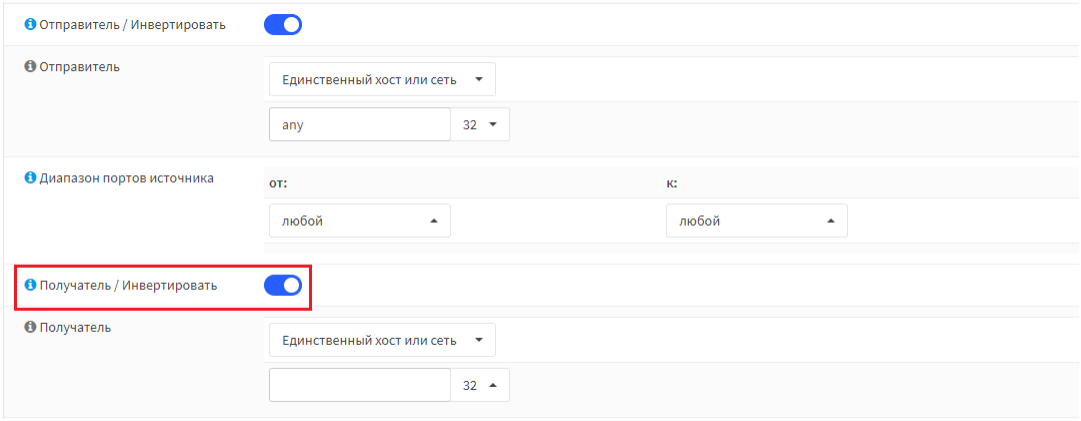


Рис. 309: Установка параметра

- в поле **«Получатель»** выбрать из выпадающего списка один из следующих параметров:
  - **«Любой»** для установки любого адреса получателя;
  - **«Единственный хост или сеть»** для установки определенного адреса получателя, затем в открывшейся строке установить определенный адрес получателя;

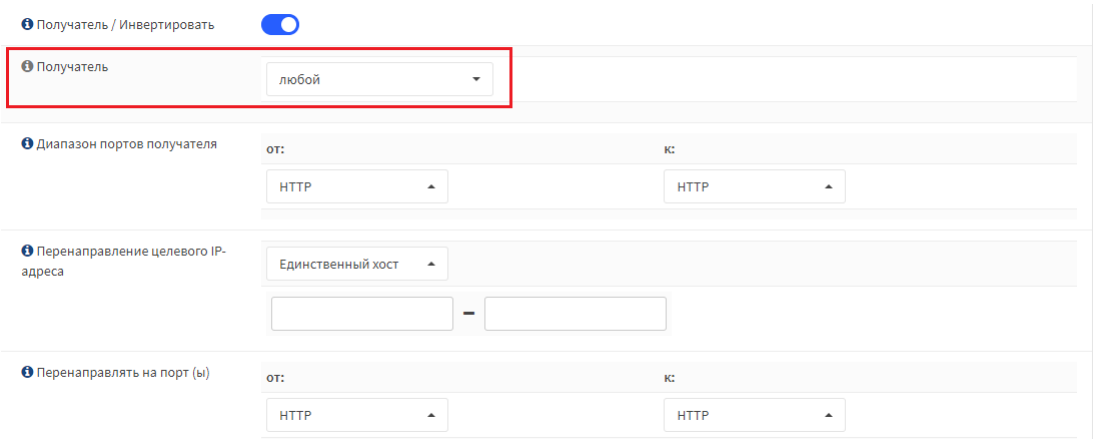


Рис. 310: Выбор параметра **«любой»**

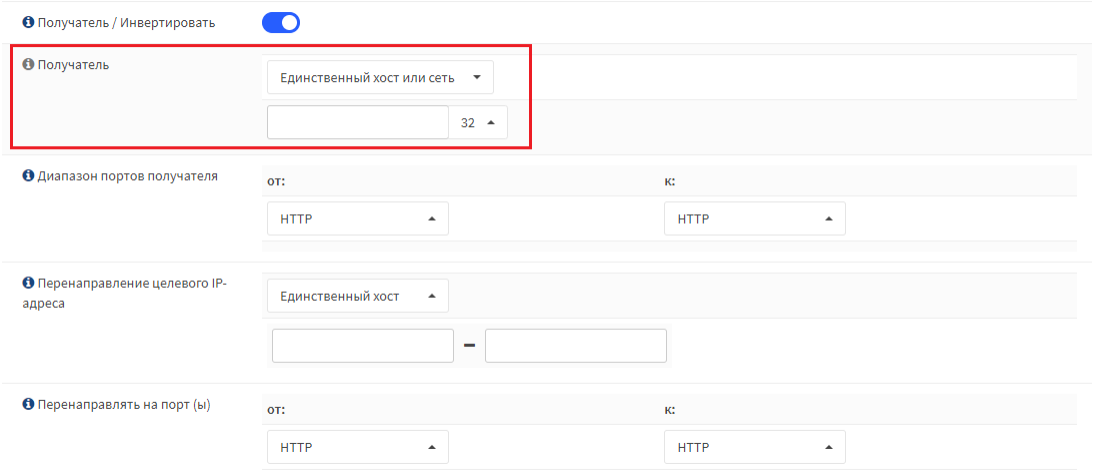


Рис. 311: Выбор параметра **«Единственный хост или сеть»**

Порты

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Диапазон портов источника»** указать:
  - порт источника (любой или определенный);
  - диапазон портов источника.

Примечание

Обычно используется случайный порт и почти никогда не используется порт из диапазона портов отправления

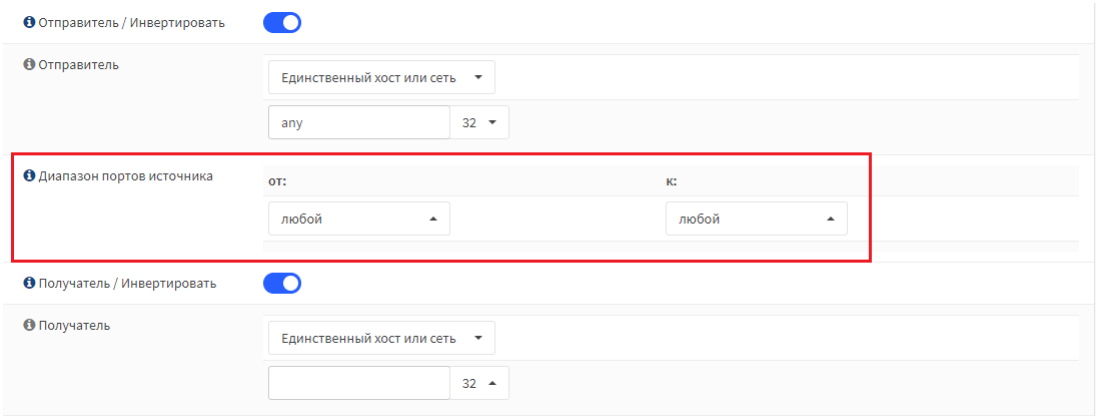


Рис. 312: Выбор параметра **«Диапазон портов источника»**

- в поле **«Диапазон портов получателя»** указать:
  - порт получателя (любой или определенный);
  - диапазон портов получателя.

Примечание

Обычно используется случайный порт и почти никогда не используется порт из диапазона портов получателя

Перенаправление целевого IP-адреса

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Перенаправление целевого IP-адреса»** выбрать из выпадающего списка один из следующих параметров:
  - **«Единственный хост»** для перенаправления пакетов данных на сервер, затем в открывшейся строке установить определенный адрес сервера;
  - **«Диапазон IP-адресов»** для перенаправления пакетов данных на диапазон IP адресов, затем в открывшейся строке установить необходимый диапазон IP адресов;

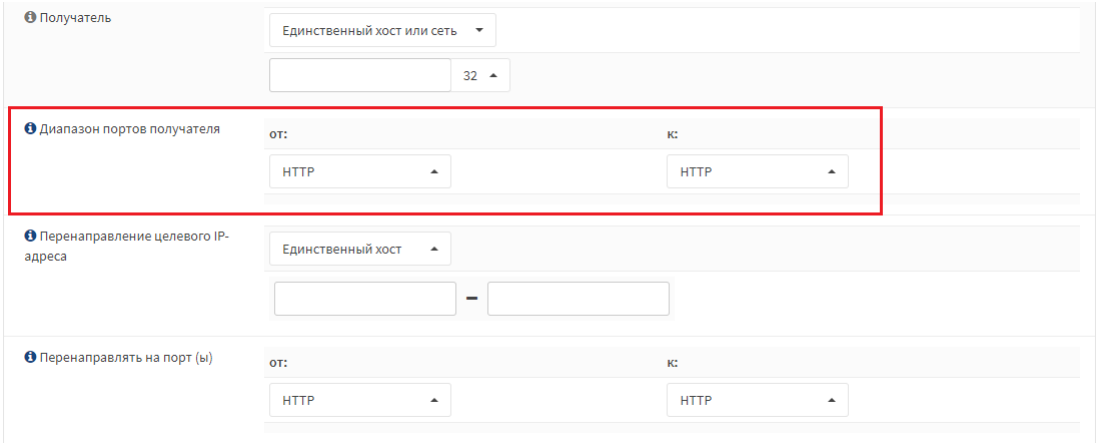


Рис. 313: Выбор параметра **«Диапазон портов получателя»**

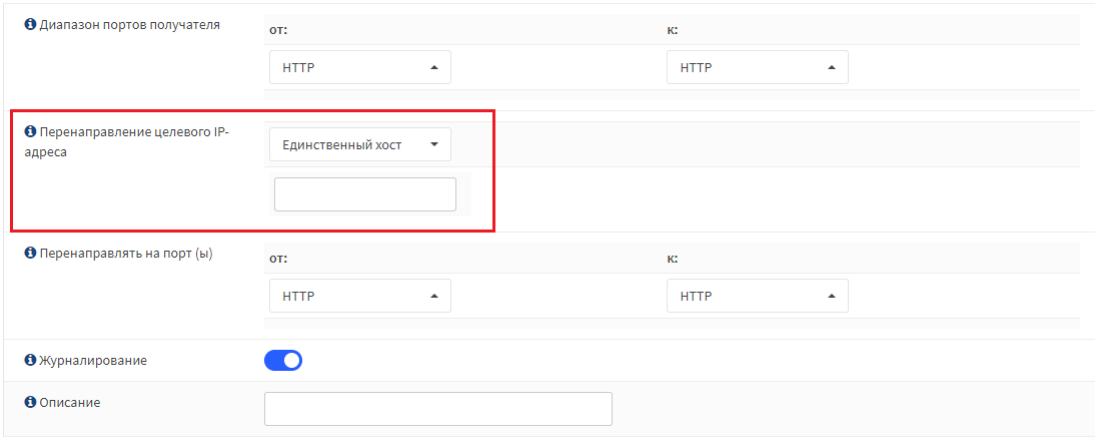


Рис. 314: Выбор параметра **«Единственный хост»**

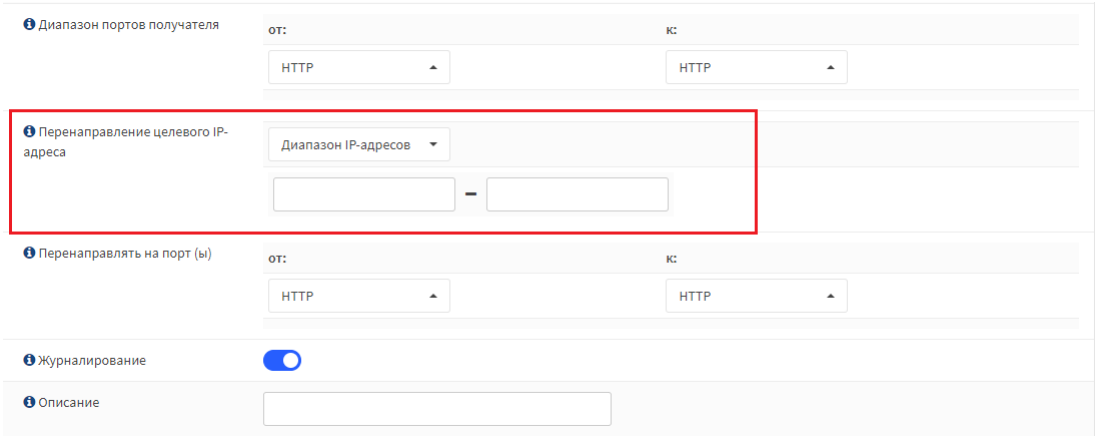


Рис. 315: Выбор параметра **«Диапазон IP-адресов»**

Перенаправление на выбранный порт

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Перенаправлять на порт (ы)»** необходимо указать порты компьютера отправителя/получателя с введенными IP адресами;

> **Примечание**
>
> Если есть диапазон портов, необходимо указать начальный порт диапазона (конечный порт будет рассчитан). Этот порт равен указанному выше порту в поле **«от:»**

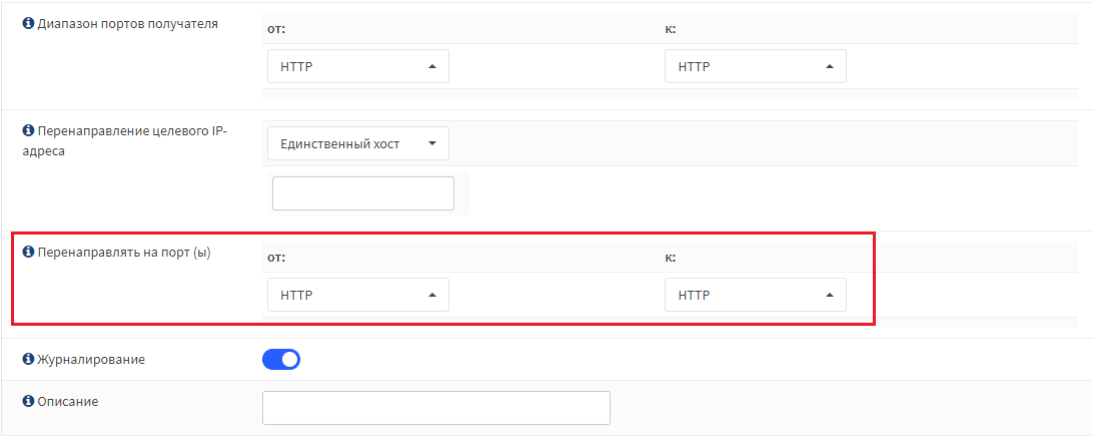


Рис. 316: Выбор параметра **«Перенаправлять на порт (ы)»**

Журналирование пакетов, проходящих через правило

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Журналирование»** установить переключатель в случае необходимости журналировать пакеты;

> **Примечание**
>
> Пространство для хранения локальных журналов межсетевого экрана ограничено. в случае необходимости журналировать все пакеты, пользователь должен использовать удалённый сервер syslog

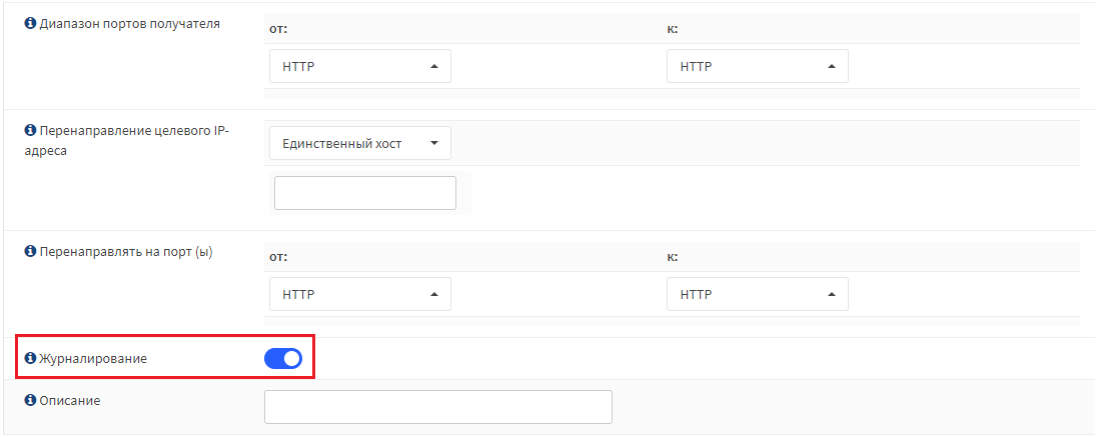


Рис. 317: Выбор параметра **«Журналирование»**

Добавление описания к правилу

В разделе **«DNAT (Prerouting)»** необходимо:

- в поле **«Описание»** ввести необходимую информацию о настраиваемом правиле.

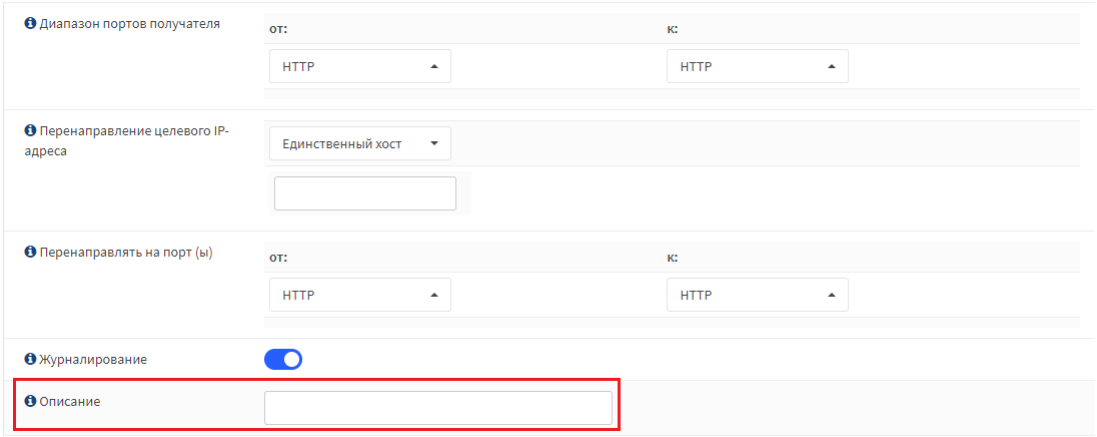
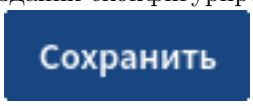
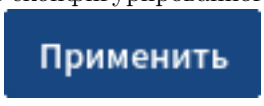


Рис. 318: Выбор параметра **«Описание»**

Для создания сконфигурированного правила DNAT (Prerouting) необходимо нажать кнопку **«Сохранить»** 

.

Для вступления сконфигурированного правила DNAT (Prerouting) в силу необходимо нажать кнопку **«Применить»** 

.

SNAT (Postrouting)

SNAT (Source NAT) необходим для изменения IP адреса отправителя сетевого пакета. В SNAT присутствует возможность автоматически изменять адрес источника на адрес интерфейса-отправителя.

> **Примечание**
>
> Правила SNAT обрабатываются последними

Отключение правила

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Отключить»** установить переключатель в случае необходимости отключить это правило, не удаляя его из списка;

> **Примечание**
>
> Выберите этот параметр, чтобы отключить правило не удаляя из списка

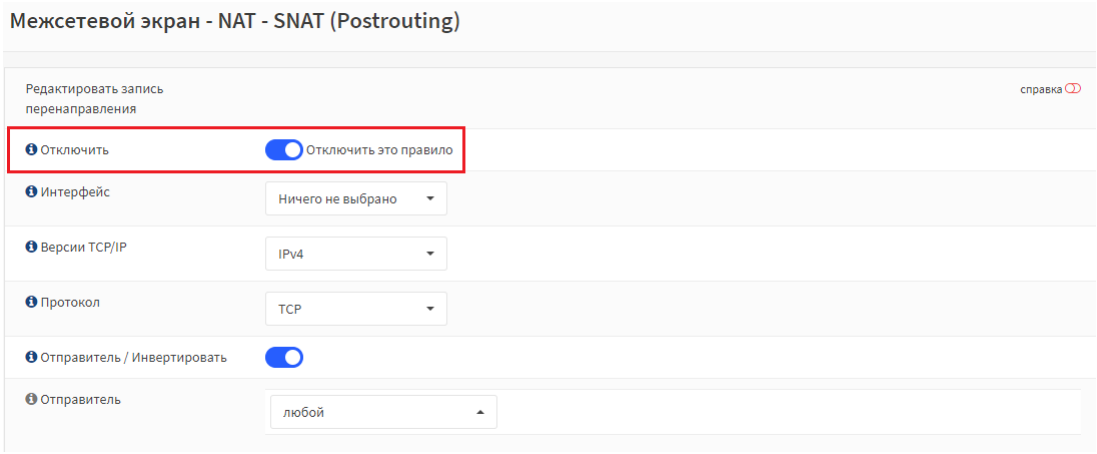


Рис. 319: Отключение настроенного правила SNAT (Postrouting)

Интерфейс

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Интерфейс»** выбрать из выпадающего списка один из интерфейсов, соответствующих таблице;

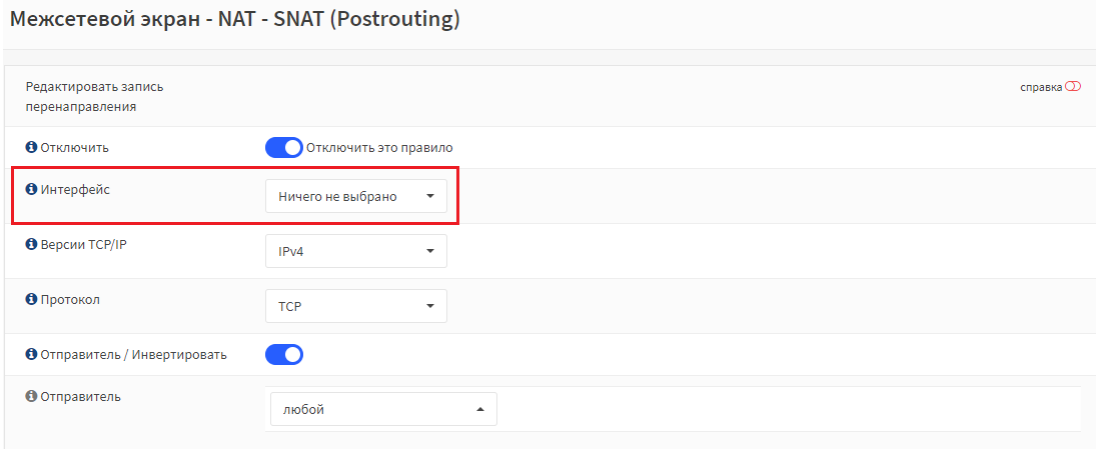


Рис. 320: Выбор интерфейса

Таблица 106: Интерфейсы

Интерфейсы
Любой
LAN
loopback
One

Протокол передачи данных

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Версии TCP/IP»** выбрать из выпадающего списка интернет-протокол IPv4;

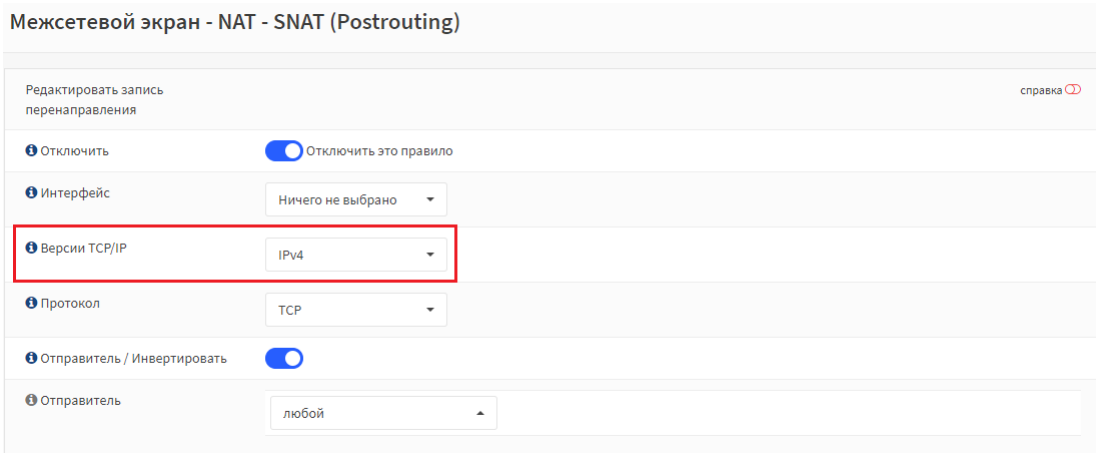


Рис. 321: Выбор Интернет-протокола

- в поле **«Протокол»** выбрать из выпадающего списка один из IP-протоколов, соответствующих таблице;

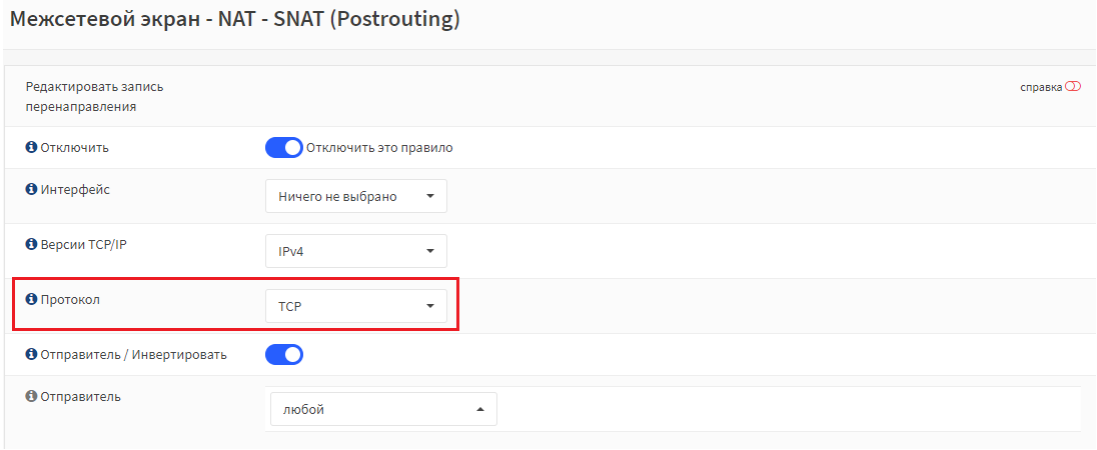


Рис. 322: Выбор IP протокола

Таблица 107: IP протоколы

IP протоколы
any (Любой)
TCP
UDP
ICMP

Адрес отправителя пакета

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Отправитель/инвертировать»** установить переключатель в случае необходимости использовать этот параметр, чтобы инвертировать смысл правила совпадения;

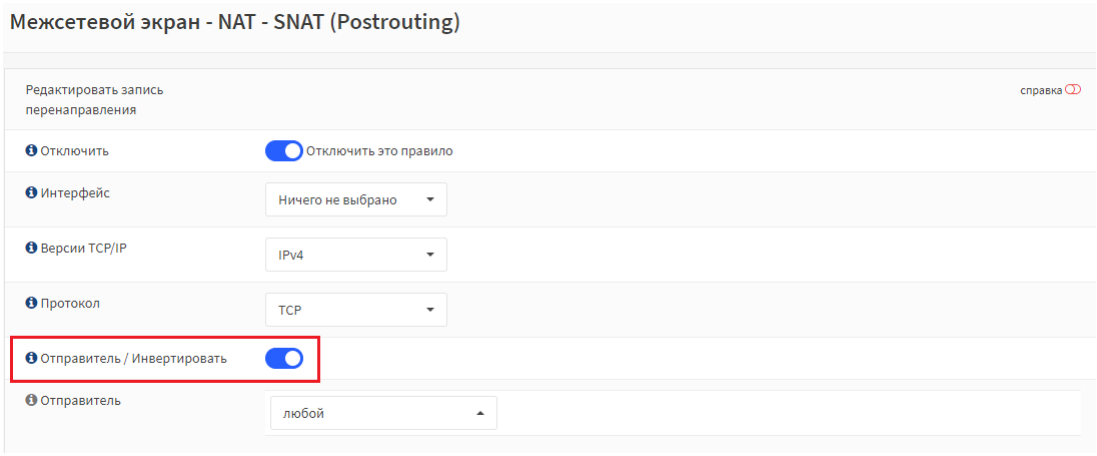


Рис. 323: Установка параметра

- в поле **«Отправитель»** выбрать из выпадающего списка один из следующих параметров:
- **«любой»** для установки любого адреса отправителя;

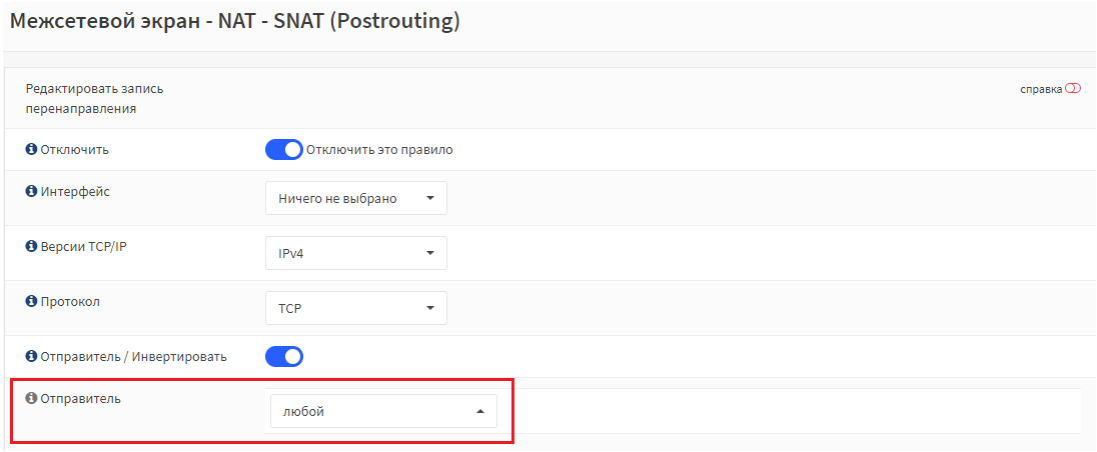


Рис. 324: Выбор параметра **«любой»**

- **«Единственный хост или сеть»** для установки определенного адреса отправителя, затем в открывшейся строке установить определенный адрес отправителя;

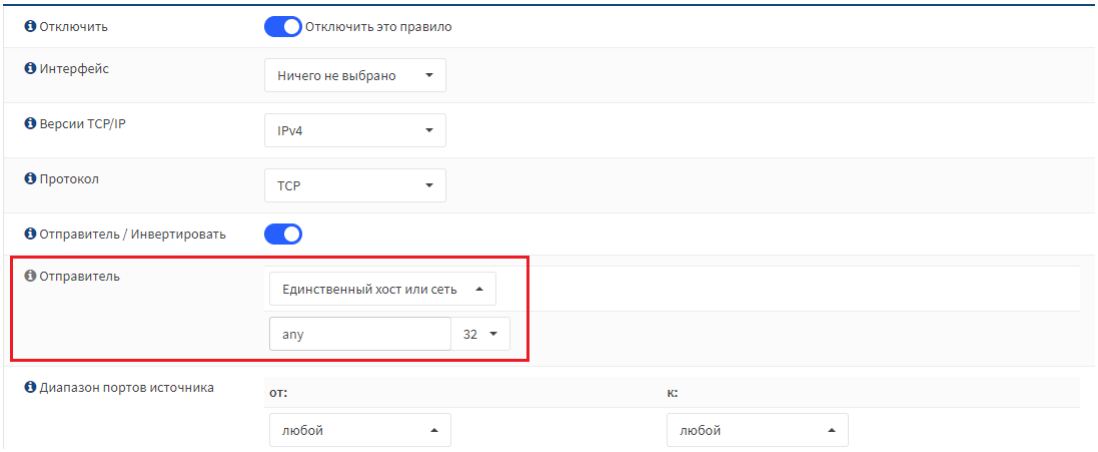


Рис. 325: Выбор параметра **«Единственный хост или сеть»**

Адрес получателя пакета

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Получатель/инвертировать»** установить переключатель в случае необходимости использовать этот параметр, чтобы инвертировать смысл правила совпадения;
- в поле **«Получатель»** выбрать из выпадающего списка один из следующих параметров:
- **«любой»** для установки любого адреса получателя;
- **«Единственный хост или сеть»** для установки определенного адреса получателя, затем в открывшейся строке установить определенный адрес получателя;

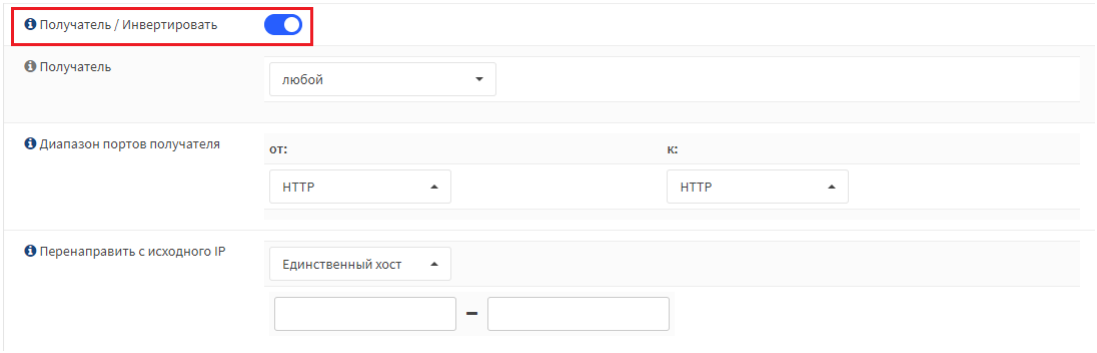


Рис. 326: Установка параметра

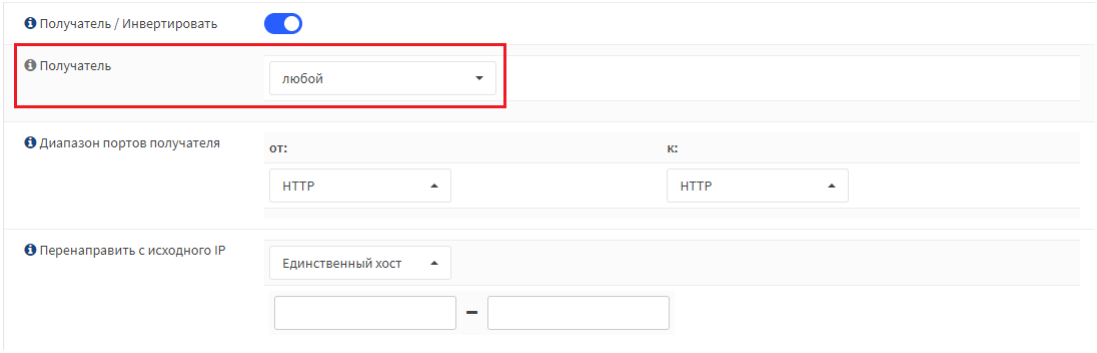


Рис. 327: Выбор параметра **«любой»**

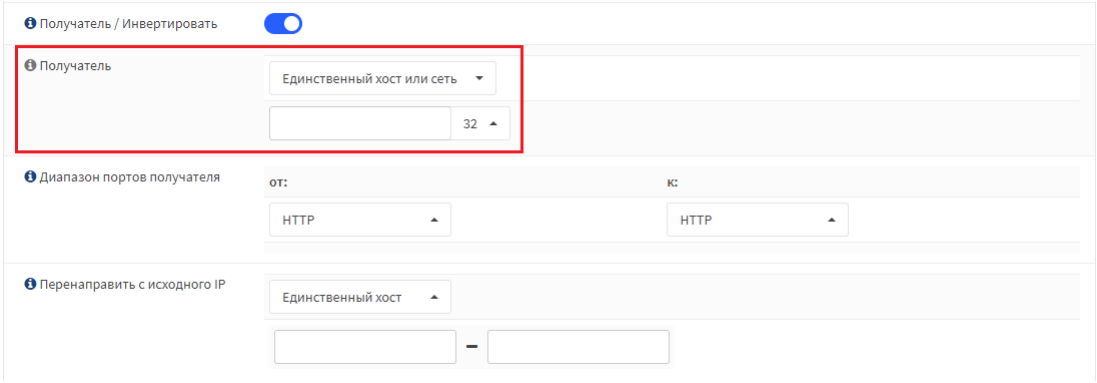


Рис. 328: Выбор параметра **«Единственный хост или сеть»**

Порты

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Диапазон портов источника»** указать:
- порт источника (любой или определенный);
- диапазон портов источника.

> **Примечание**
>
> Определенный порт источника и диапазон портов источника можно выбрать при использовании TCP или UDP протокола

> **Примечание**
>
> Обычно используется случайный порт и почти никогда не используется порт из диапазона портов отправления

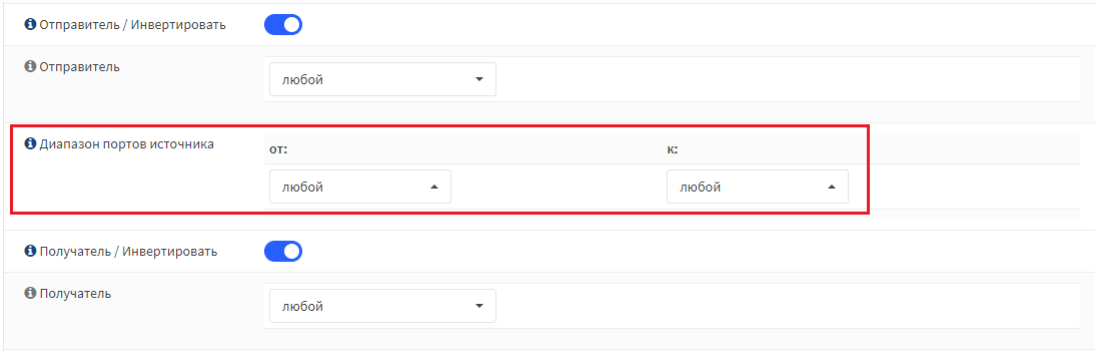


Рис. 329: Выбор параметра **«Диапазон портов источника»**

- в поле **«Диапазон портов получателя»** указать:
- порт получателя (любой или определенный);
- диапазон портов получателя.

> **Примечание**
>
> Определенный порт получателя и диапазон портов получателя можно выбрать при использовании TCP или UDP протокола

> **Примечание**
>
> Обычно используется случайный порт и почти никогда не используется порт из диапазона портов получателя

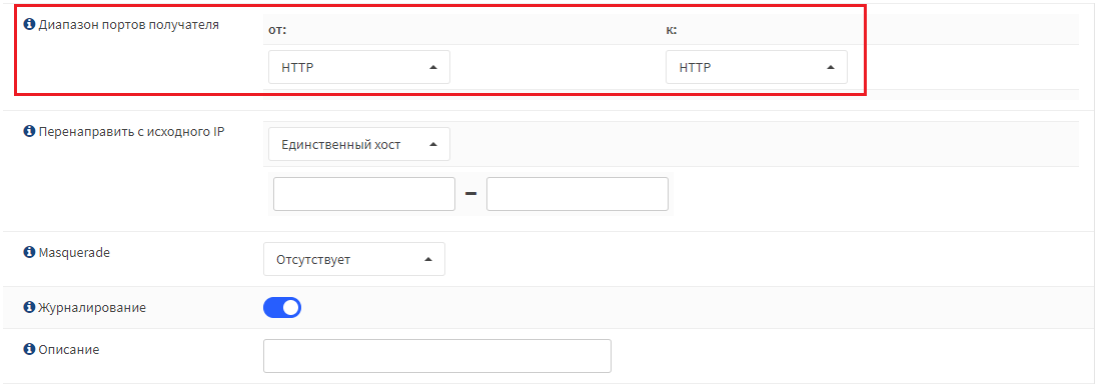


Рис. 330: Выбор параметра **«Диапазон портов получателя»**

Перенаправление с исходного IP-адреса

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Перенаправить с исходного IP»** выбрать из выпадающего списка один из следующих параметров:
- **«Единственный хост»** для перенаправления пакетов данных на сервер, затем в открывшейся строке установить определенный адрес сервера;

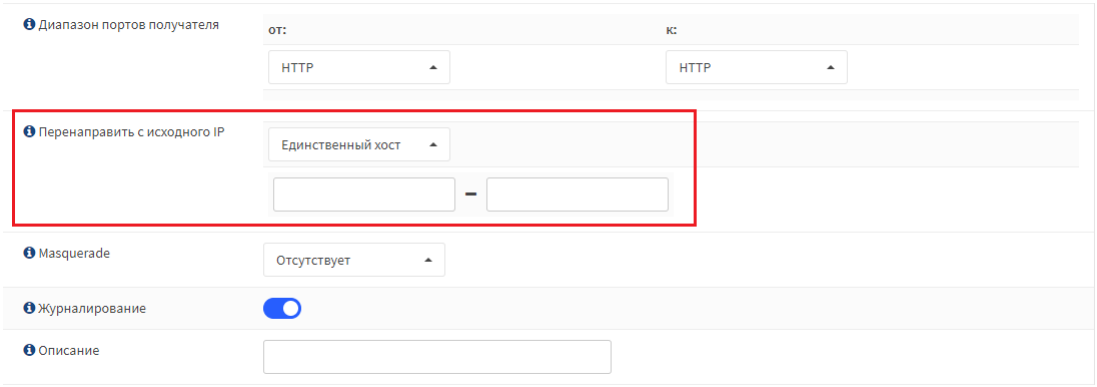


Рис. 331: Выбор параметра **«Единственный хост»**

- **«Диапазон IP-адресов»** для перенаправления пакетов данных на диапазон IP адресов, затем в открывшейся строке установить необходимый диапазон IP адресов;

Masquerade

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Masquerade»** выбрать из выпадающего списка один из параметров, соответствующих таблице

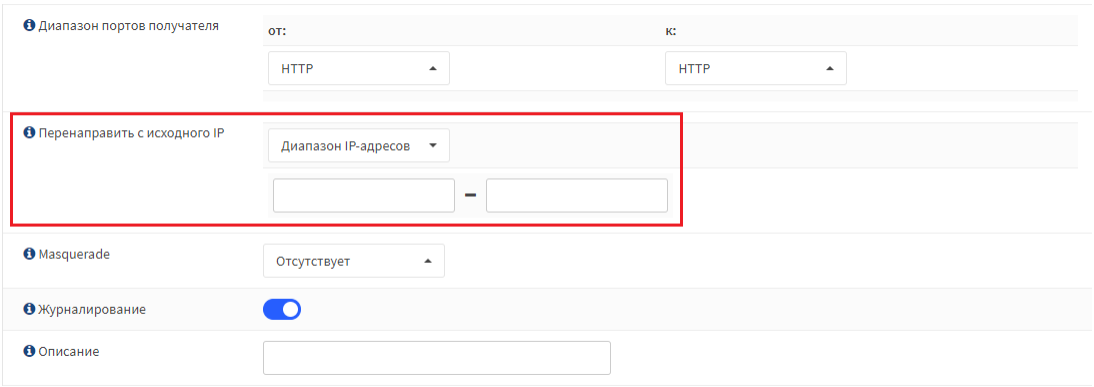


Рис. 332: Выбор параметра **«Диапазон IP-адресов»**

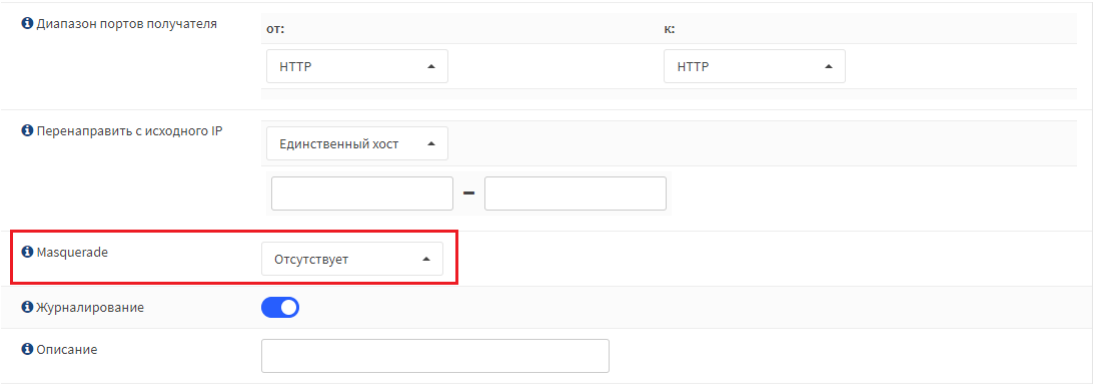


Рис. 333: Выбор параметра **«Masquerade»**

Таблица 108: Выбор параметра

Параметр	Примечание
отсутствует	
persistent	Задает клиенту тот же входящий и исходящий адрес для каждого соединения
random	Случайная переадресация пакетов отправителя
fully-random	Полностью случайные порты

Журналирование пакетов, проходящих через правило

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Журналирование»** установить переключатель в случае необходимости журналировать пакеты;

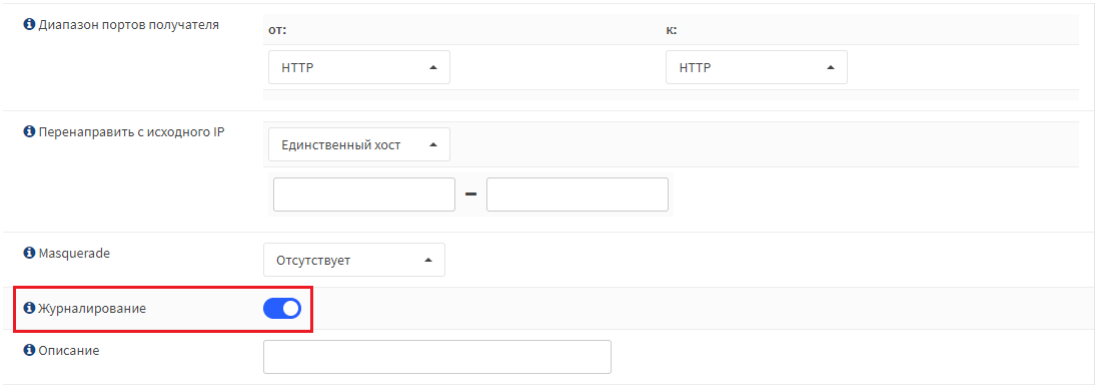


Рис. 334: Выбор параметра **«Журналирование»**

Добавление описания к правилу

В разделе **«SNAT (Postrouting)»** необходимо:

- в поле **«Описание»** ввести необходимую информацию о настраиваемом правиле.

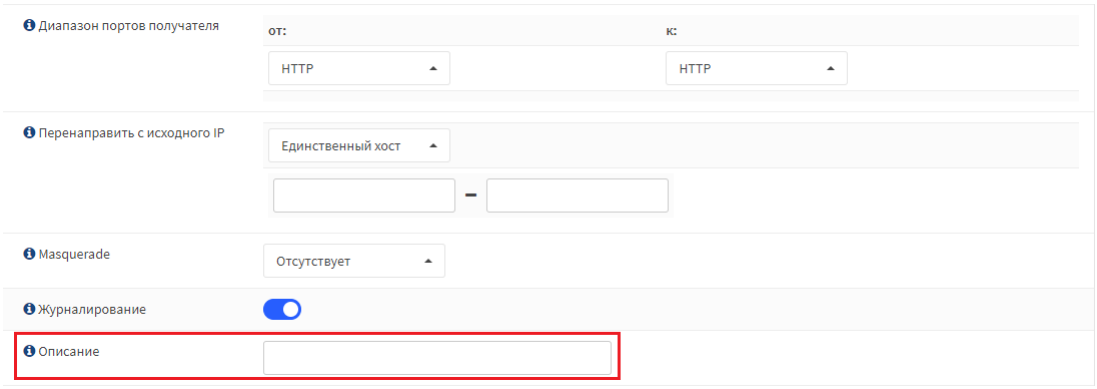


Рис. 335: Выбор параметра **«Описание»**

Для создания сконфигурированного правила SNAT (Postrouting) необходимо нажать кнопку **«Сохранить»** Сохранить .

Для вступления сконфигурированного правила SNAT (Postrouting) в силу необходимо нажать кнопку **«Применить»** Применить .

BINAT

BINAT необходим для изменения IP адреса отправителя и получателя. Состоит из SNAT и DNAT. BINAT работает только для 1:1 (хост - IP адрес)

Отключение правила

В разделе **«BINAT»** необходимо:

- в поле **«Отключить»** установить переключатель в случае необходимости отключить это правило, не удаляя его из списка;

Примечание

Выберите этот параметр, чтобы отключить правило не удаляя из списка

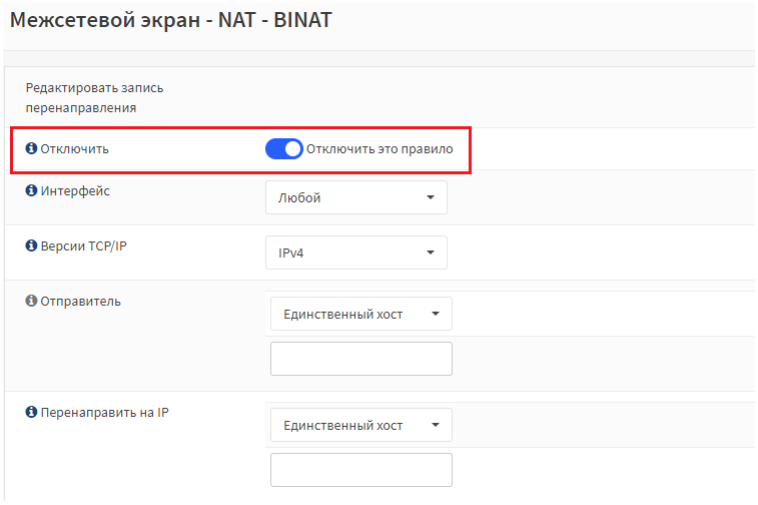


Рис. 336: Отключение настроенного правила BINAT

Интерфейс

В разделе **«BINAT»** необходимо:

- в поле **«Интерфейс»** выбрать из выпадающего списка один из интерфейсов, соответствующих таблице;

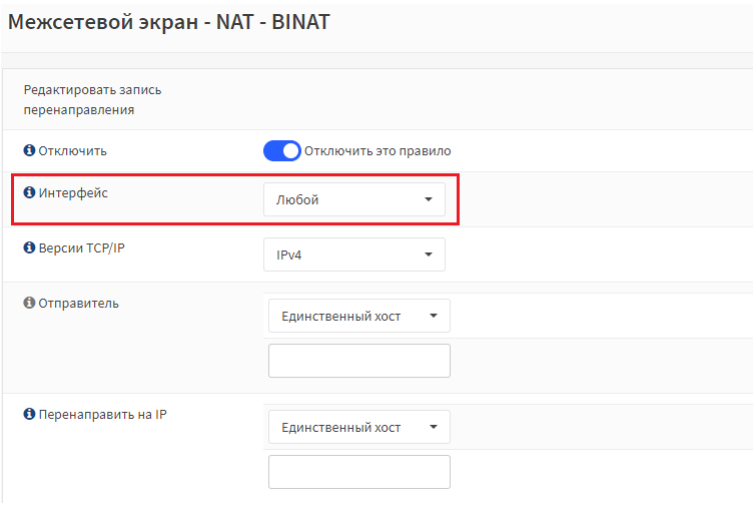


Рис. 337: Выбор интерфейса

Таблица 109: Интерфейсы

Интерфейсы
Любой
LAN
loopback
One

Протокол передачи данных

В разделе **«BINAT»** необходимо:

- в поле **«Версии TCP/IP»** выбрать из выпадающего списка интернет-протокол IPv4;

Адрес отправителя пакета

В разделе **«BINAT»** необходимо:

- в поле **«Отправитель»** выбрать из выпадающего списка параметр **«Единственный хост»**, затем установить определенный IP адрес отправителя;

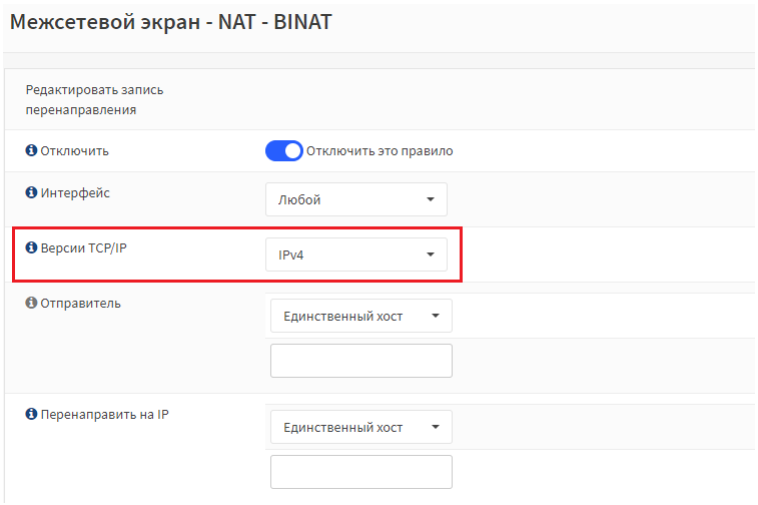


Рис. 338: Выбор Интернет-протокола

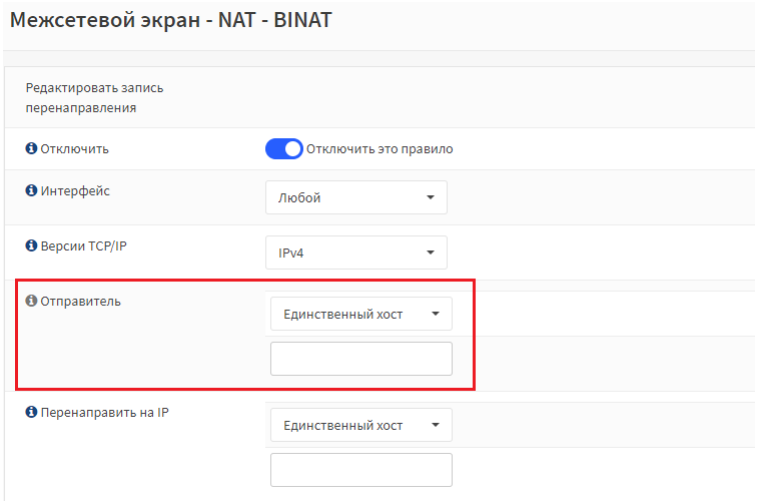


Рис. 339: Адрес отправителя пакета

Перенаправление на выбранный IP адрес

В разделе **«BINAT»** необходимо:

- в поле **«Перенаправить на IP»** выбрать из выпадающего списка параметр **«Единственный хост»**, затем установить определенный IP адрес, на который необходимо перенаправить пакет;

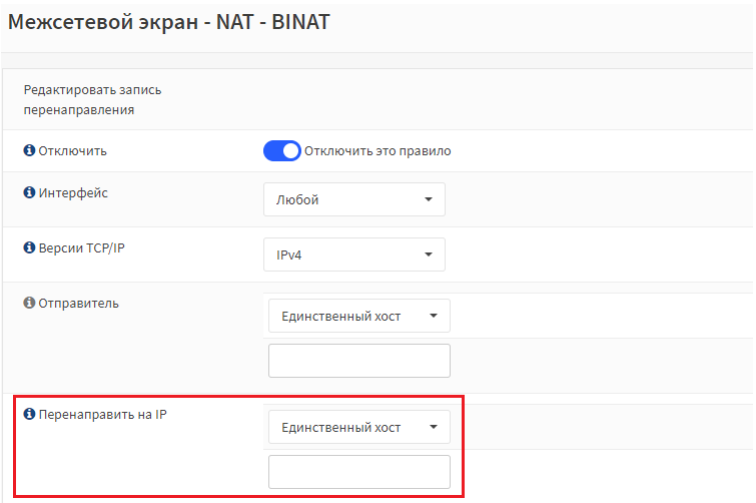


Рис. 340: Перенаправление на выбранный IP адрес

Журналирование пакетов, проходящих через правило

В разделе **«BINAT»** необходимо:

- в поле **«Журналирование»** установить переключатель в случае необходимости журналировать пакеты;

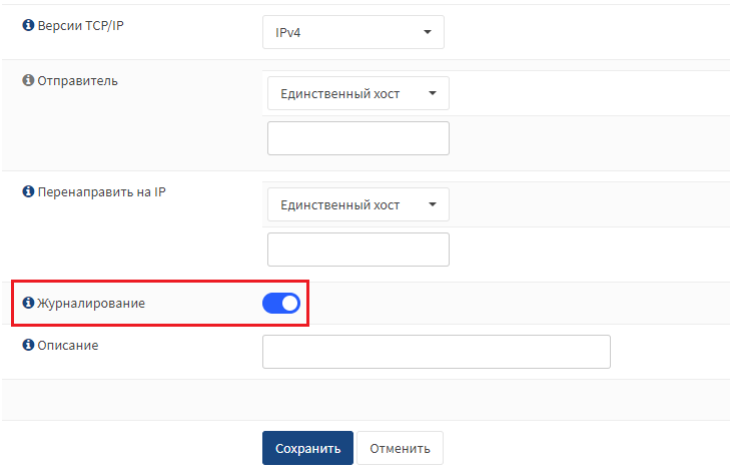


Рис. 341: Выбор параметра **«Журналирование»**

Добавление описания к правилу

В разделе **«BINAT»** необходимо:

- в поле **«Описание»** ввести необходимую информацию о настраиваемом правиле.

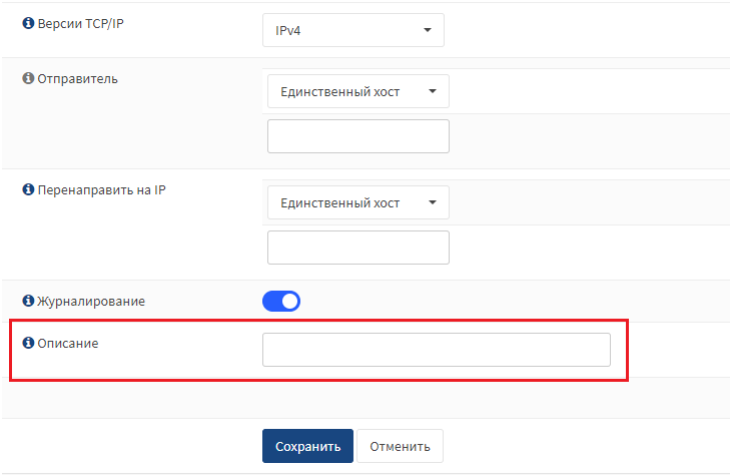
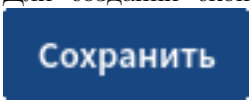


Рис. 342: Выбор параметра **«Описание»**

Для создания сконфигурированного правила BINAT необходимо нажать кнопку **«Сохранить»** 

.

Для вступления сконфигурированного правила BINAT в силу необходимо нажать кнопку **«Применить»** 

.

2.7.5.4 Правила фильтрации

При настройках правил фильтрации (далее - правил) пользователь может выбрать один из необходимых интерфейсов

> **Примечание**
>
> Интерфейс LAN и интерфейс loopback имеют одинаковый набор формируемых правил

Для перехода к настройкам правил, используя интерфейс LAN, необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«Правила фильтрации»** - **«LAN»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться таблица правил;

> **Примечание**

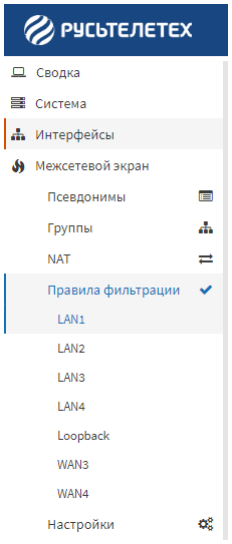


Рис. 343: Переход к настройкам правил фильтрации, используя интерфейс LAN

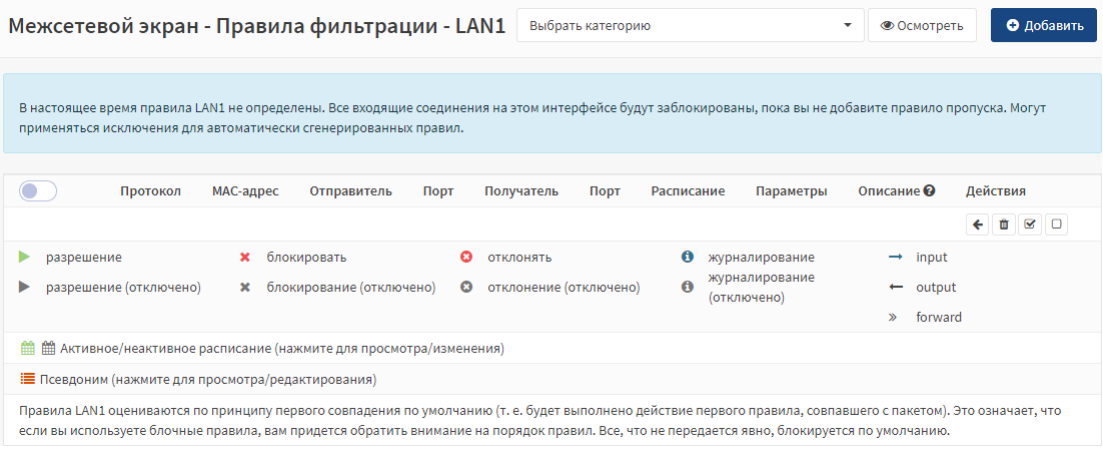


Рис. 344: Таблица правил

Информация, представленная в блоке (1), является справочной и говорит о том, что в настоящее время правила в интерфейсе LAN не определены; все входящие соединения на этом интерфейсе будут заблокированы, пока не будет добавлено правило пропуска; могут применяться исключения для автоматически сгенерированных правил

- нажать кнопку **«Добавить»** 

для добавления нового правила в таблицу правил LAN.

В открывшемся окне пользователю доступны разделы настраиваемых правил, соответствующие таблице.

Таблица 110: Разделы настраиваемых правил

Раздел настраиваемых правил	Примечание
Основные параметры	В разделе содержатся основные правила пакетов данных
Дополнительные параметры	В разделе содержатся расширенные правила пакетов данных
Lite DPI	Возможность помимо проверки заголовка пакета данных настроить проверку данных, содержащихся в пакете

После настройки правила необходимо:

- нажать кнопку **«Сохранить»** 

;
- нажать кнопку **«Применить изменения»** 

;

Примечание

Межсетевой экран просматривает таблицу правил последовательно от верхнего правила к нижнему правилу

Основные параметры

Действия, производимые с пакетами

В разделе **«Основные параметры»** необходимо:

- в поле **«Действие»** выбрать из выпадающего списка действие, проводимое с пакетами.

Список действий, проводимых с пакетами соответствует таблице.

Таблица 111: Список действий

Действие	Значение
Принимать	Пропустить пакет
Блокировать	Отбросить пакет
Отклонять	Отбросить пакет и вернуть его отправителю

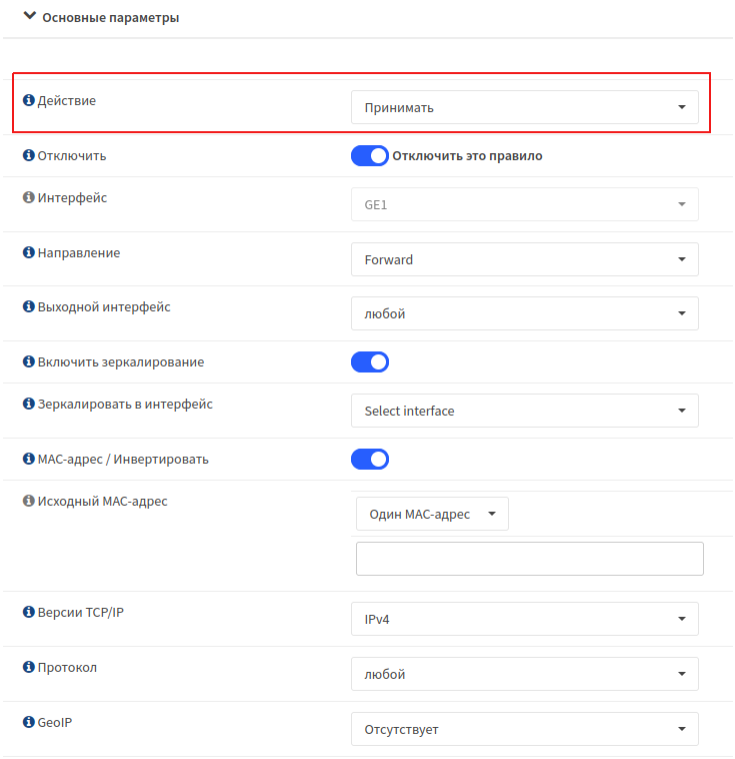


Рис. 345: Действия, производимые с пакетами

Отключение правила

В разделе **«Основные параметры»** необходимо:

- в поле **«Отключить»** установить переключатель в случае необходимости отключить это правило, не удаляя его из списка;

Направление пакета

В разделе **«Основные параметры»** необходимо:

- в поле **«Направление»** выбрать из выпадающего списка необходимое направление движения пакета.

Список направлений движения пакета соответствует таблице

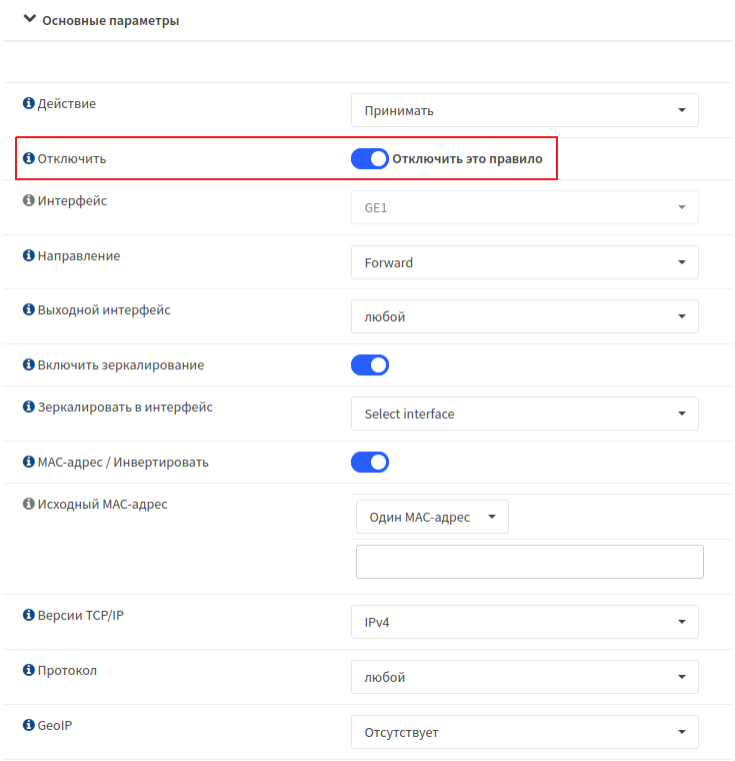


Рис. 346: Отключение правила

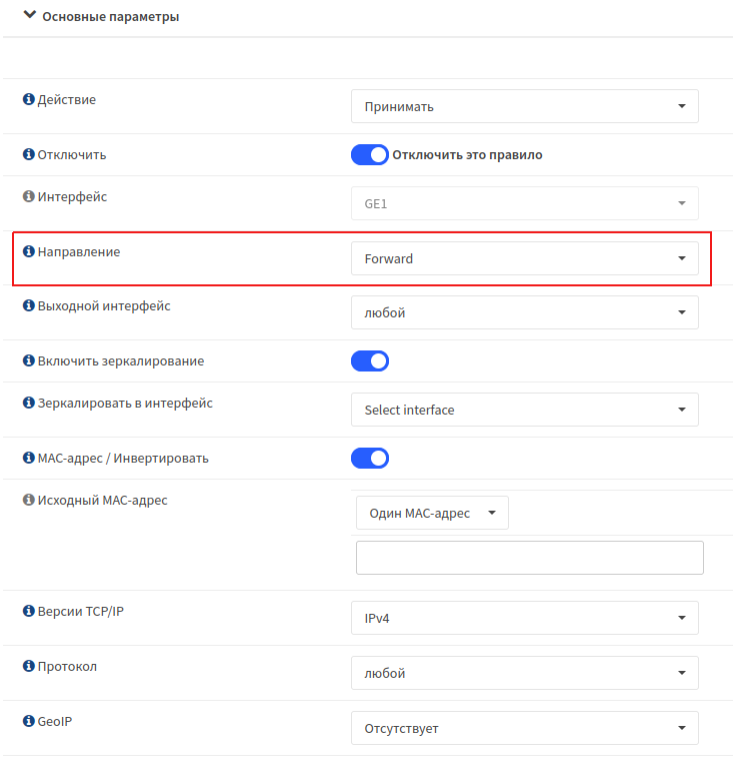


Рис. 347: Направление пакета

Таблица 112: Список направлений движения пакета

Направление	Значение
Input	Входящий пакет
Output	Исходящий пакет
Forvard	Транзитный пакет

- в поле **«Выходной интерфейс»** выбрать из выпадающего списка необходимый выходной интерфейс.

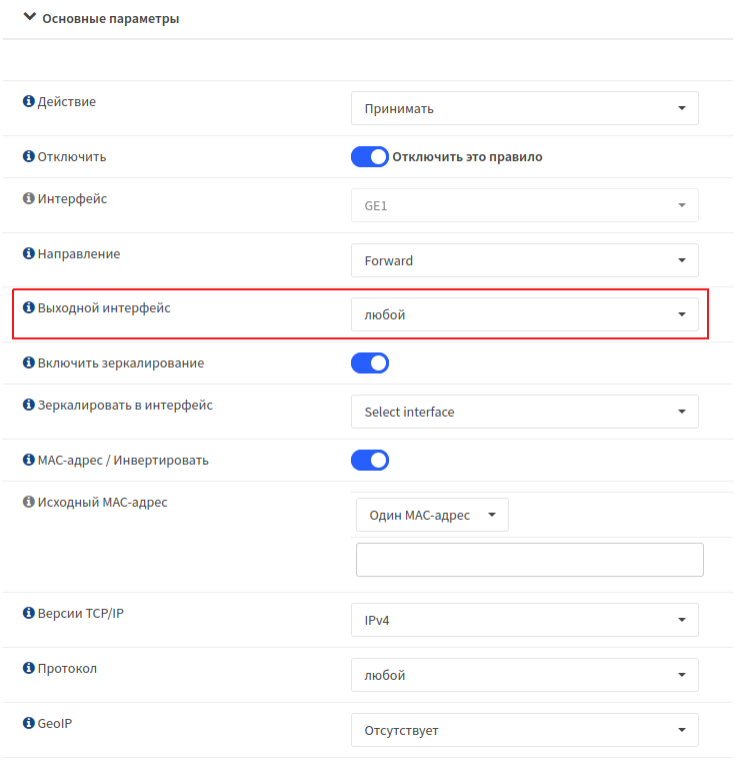


Рис. 348: Выходной интерфейс

- в поле **«Включить зеркалирование»** установить переключатель в случае необходимости, чтобы все пакеты, которые подходят под это правило будут перенаправлены в выбранный порт. Работать будут только параметры из секции **«Основные параметры»**.
- в поле **«Зеркалировать в интерфейс»** (при включенной функции **«Включить зеркалирование»**) выбрать из выпадающего списка необходимый интерфейс.
- в поле **«MAC-адрес / Инвертировать»** установить переключатель в случае необходимости инвертировать MAC-адрес.
- в поле **«Исходный MAC-адрес»** выбрать из выпадающего списка количество MAC-адресов и указать MAC-адрес.

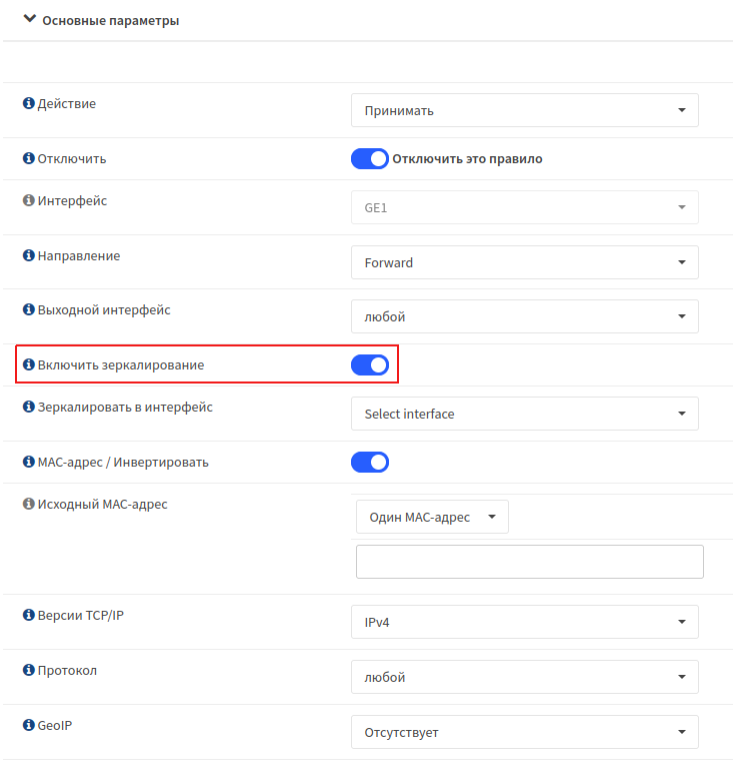


Рис. 349: Включить зеркалирование

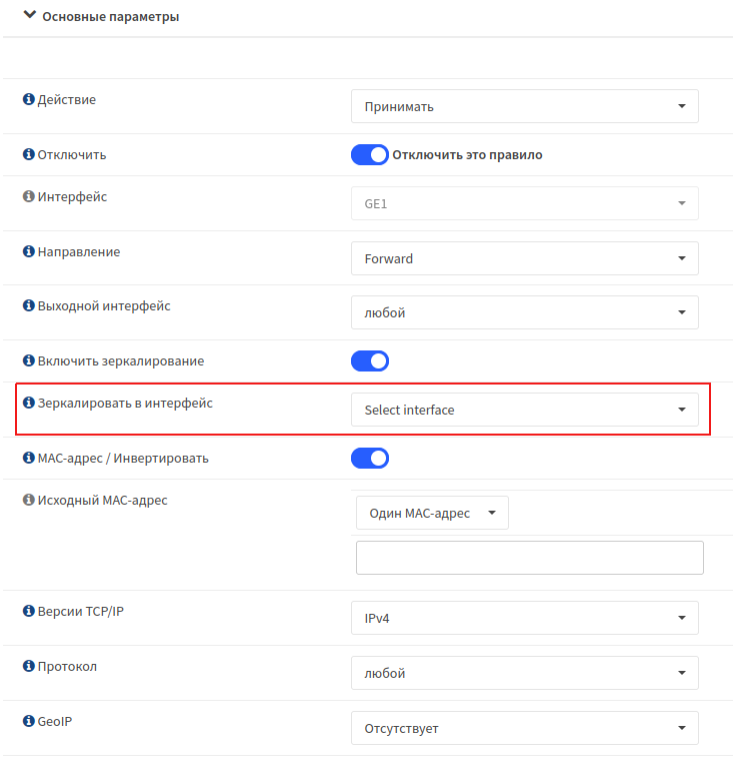


Рис. 350: Зеркалировать в интерфейс

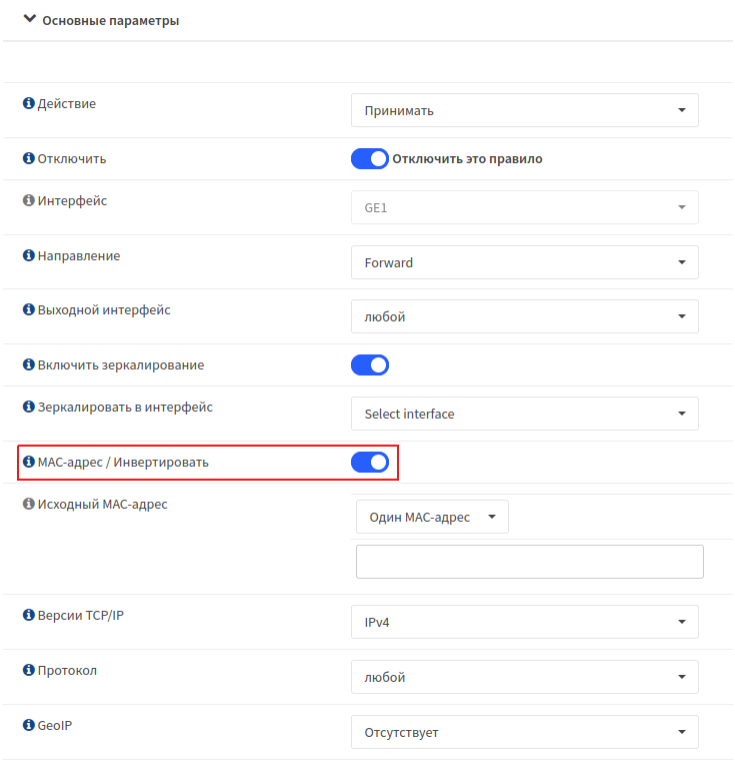


Рис. 351: MAC-адрес / Инвертировать

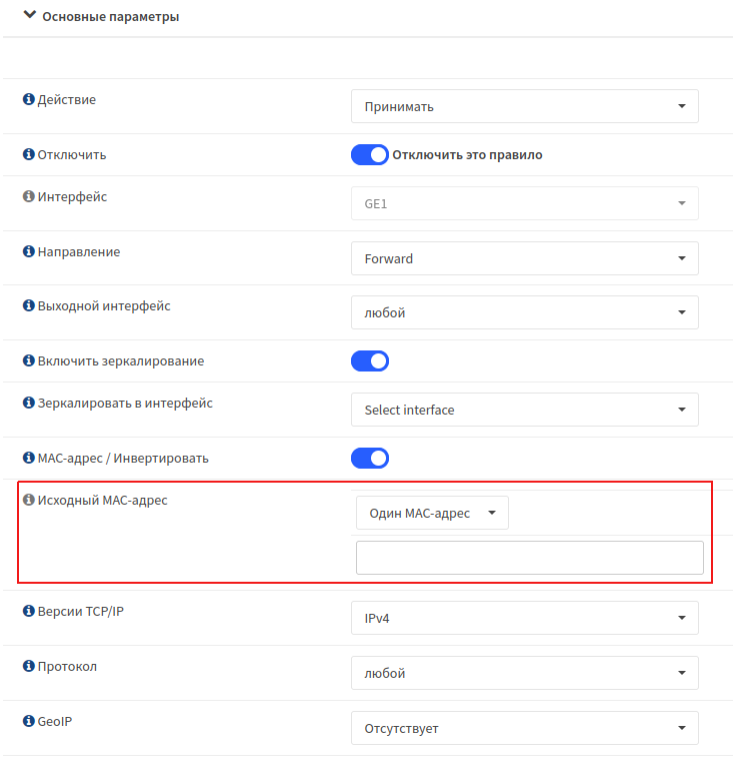


Рис. 352: Исходный MAC-адрес

Протокол передачи данных

В разделе **«Основные параметры»** необходимо:

- в поле **«Версии TCP/IP»** выбрать из выпадающего списка необходимую версию Интернет – протокола;

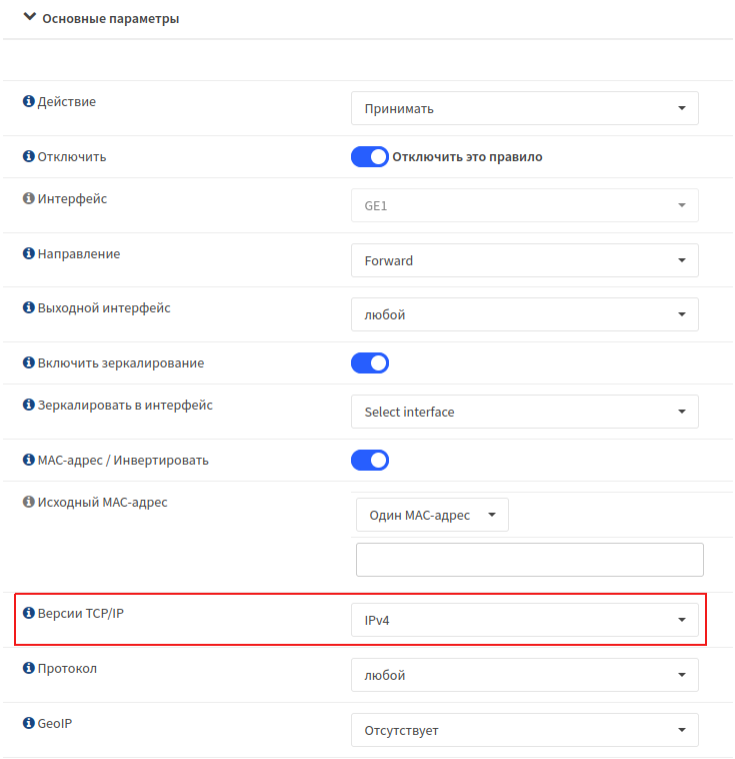


Рис. 353: Выбор версии Интернет - протокола

Версии Интернет – протокола соответствуют таблице

Таблица 113: Версии Интернет – протокола

Версии Интернет – протокола
IPv4
ARP

- в поле **«Протокол»** выбрать из выпадающего списка необходимый IP – протокол;

IP – протоколы соответствуют таблице

Таблица 114: IP-протоколы

IP – протоколы
любой
TCP
UDP
ICMP
ESP

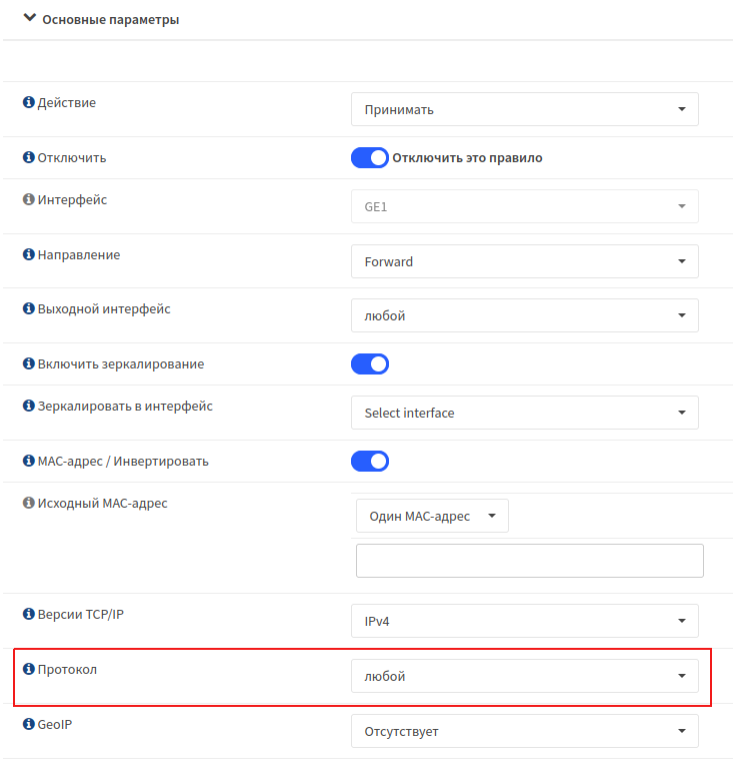


Рис. 354: Выбор IP – протокола

Примечание

В большинстве случаев пользователь должен указать TCP протокол.

- в поле **«GeoIP»** выбрать из выпадающего списка необходимый GeoIP;

Адрес отправителя пакета

В разделе **«Основные параметры»** необходимо:

- в поле **«Отправитель/инвертировать»** установить переключатель в случае необходимости использовать этот параметр, чтобы инвертировать смысл правила совпадения;
- в поле **«Отправитель»** выбрать из выпадающего списка один из следующих параметров:
- **«любой»** для установки любого адреса отправителя;
- **«Единственный хост или сеть»** для установки определенного адреса отправителя затем установить определенный адрес отправителя в открывшейся строке;

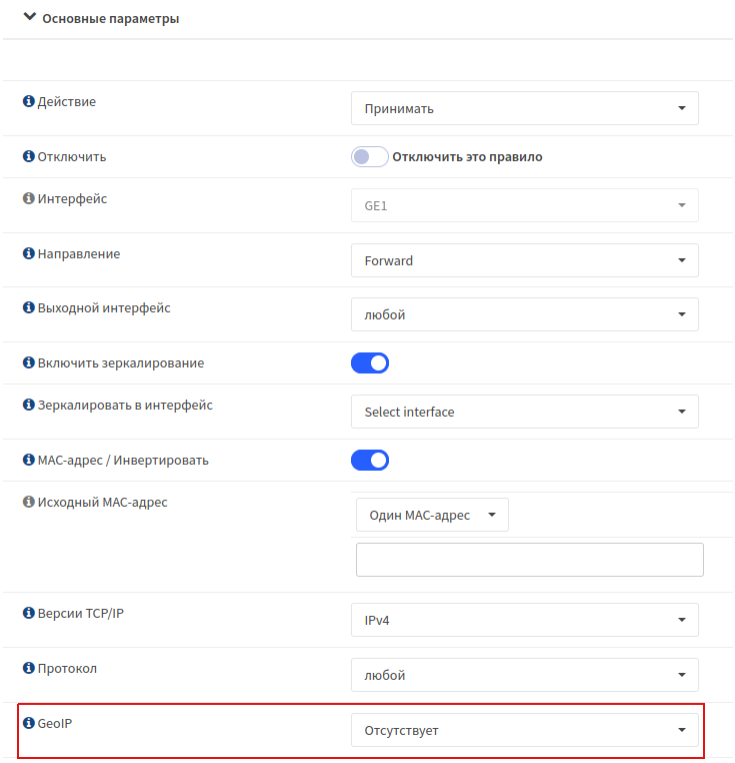


Рис. 355: GeoIP

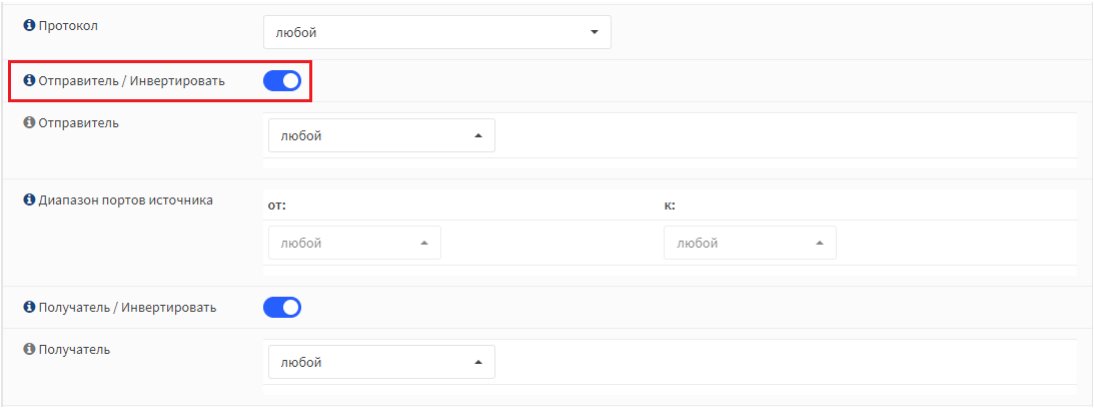


Рис. 356: Инвертирование смысла правила совпадения

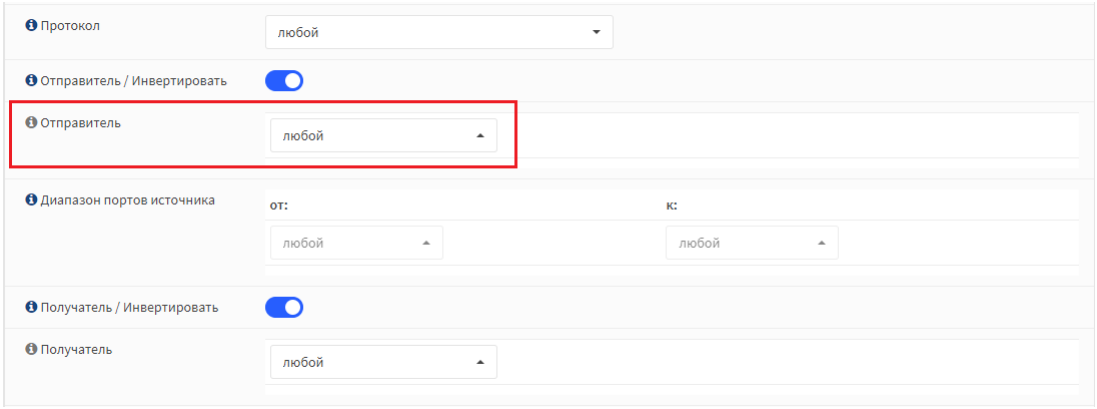


Рис. 357: Выбор параметра **«любой»**

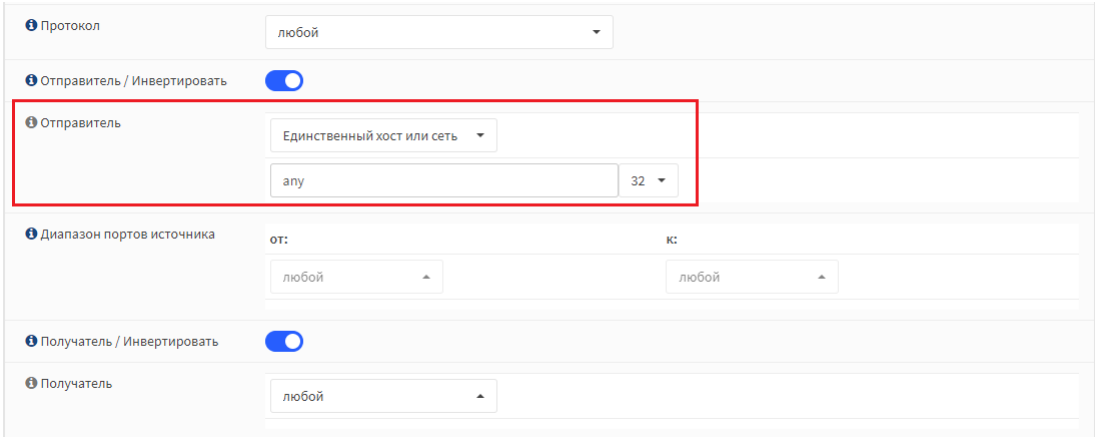


Рис. 358: Выбор параметра **«Единственный хост или сеть»**

Адрес получателя пакета

В разделе **«Основные параметры»** необходимо:

- в поле **«Получатель/инвертировать»** установить переключатель в случае необходимости использовать этот параметр, чтобы инвертировать смысл правила совпадения;

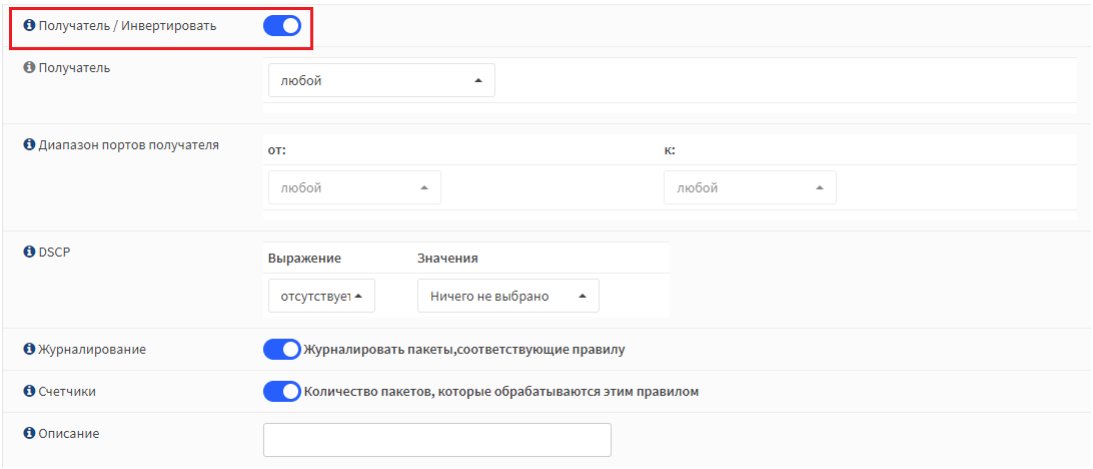


Рис. 359: Инвертирование смысла правила совпадения

- в поле **«Получатель»** выбрать из выпадающего списка один из следующих параметров:
  - **«любой»** для установки любого адреса получателя;

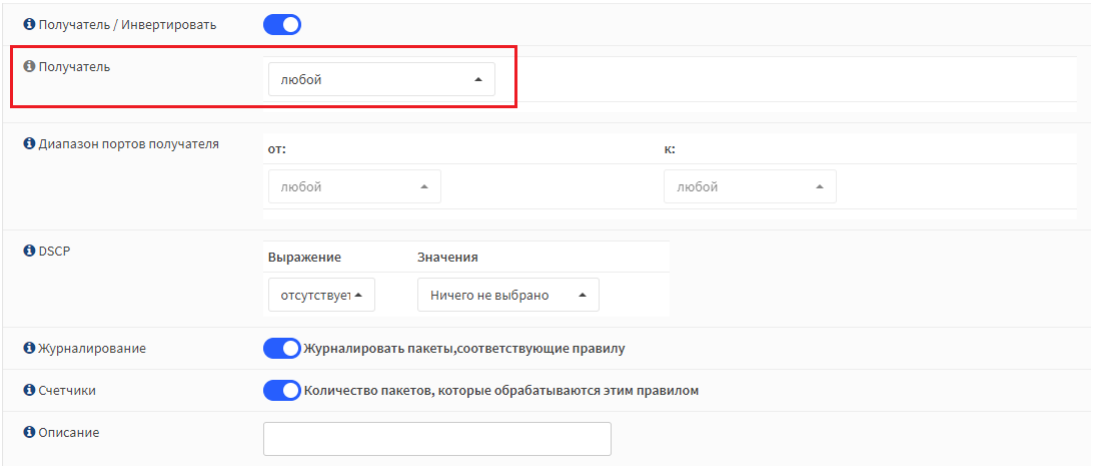


Рис. 360: Выбор параметра **«любой»**

  - **«Единственный хост или сеть»** для установки определенного адреса получателя затем установить определенный адрес получателя в открывшейся строке;

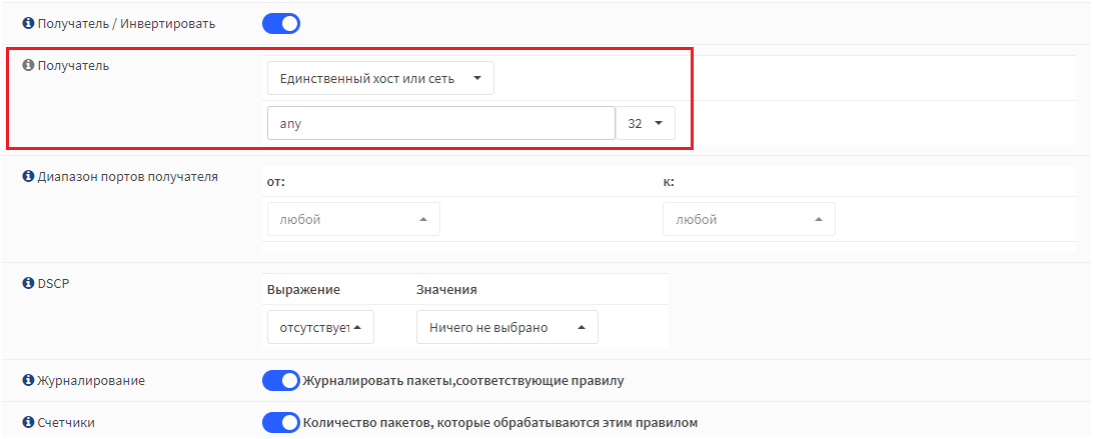


Рис. 361: Выбор параметра **«Единственный хост или сеть»**

Порты

В разделе **«Основные параметры»** необходимо:

- в поле **«Диапазон портов источника»** указать:
  - порт источника (любой или определенный);
  - диапазон портов источника.

> **Примечание**
>
> Обычно используется случайный порт и почти никогда не используется порт из диапазона портов отправления

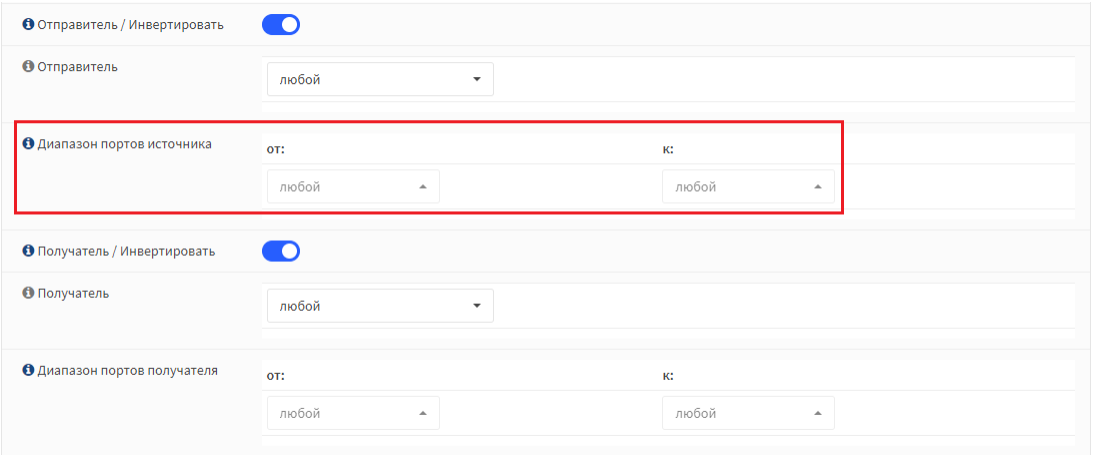


Рис. 362: Выбор параметра **«Диапазон портов источника»**

- в поле **«Диапазон портов получателя»** указать:
  - порт получателя (любой или определенный);
  - диапазон портов получателя.

Примечание

Обычно используется случайный порт и почти никогда не используется порт из диапазона портов получателя

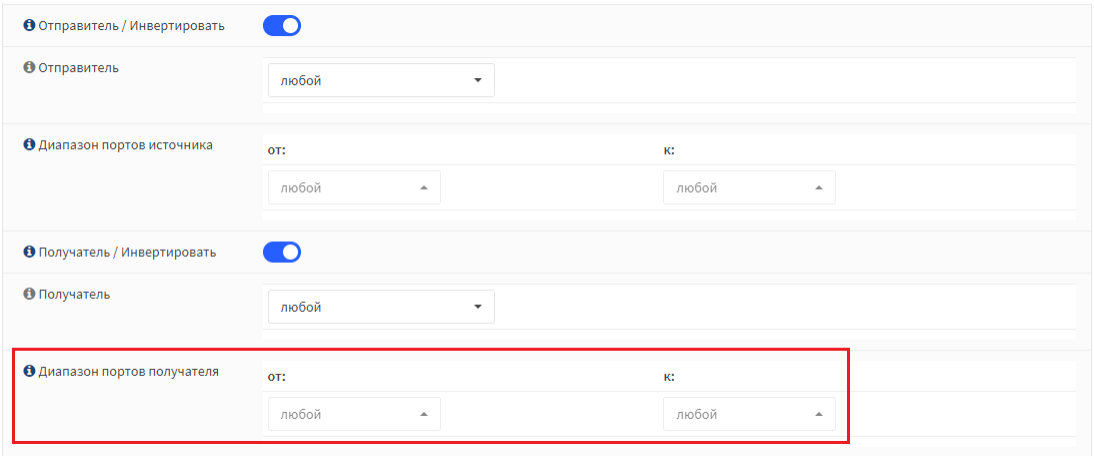


Рис. 363: Выбор параметра **«Диапазон портов получателя»**

Соответствие DSCP

В разделе **«Основные параметры»** необходимо:

- в поле **«DSCP»** указать:
  - в колонке **«Выражение»** необходимое выражение, соответствующее таблице
  - в колонке **«Значения»** бит QoS, соответствующий таблице

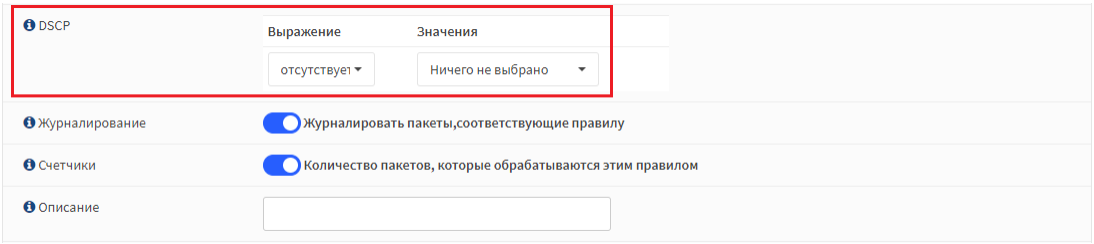


Рис. 364: Выбор параметра **«Диапазон портов получателя»**

Журналирование пакетов, проходящих через правило

В разделе **«Основные параметры»** необходимо:

- в поле **«Журналирование»** установить переключатель в случае необходимости журналировать пакеты;

> **Примечание**
>
> Пространство для хранения локальных журналов межсетевого экрана ограничено. в случае необходимости журналировать все пакеты, пользователь должен использовать удалённый сервер syslog

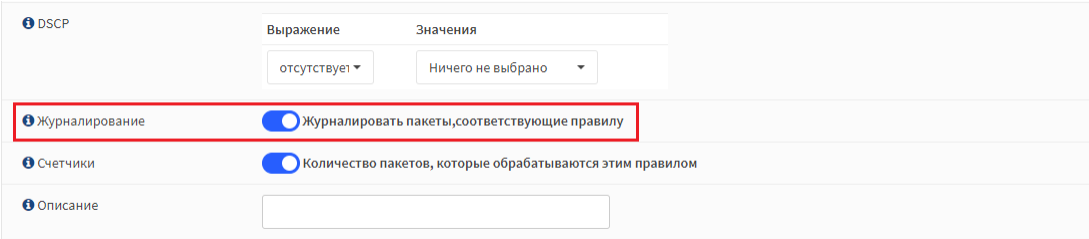


Рис. 365: Выбор параметра **«Журналирование»**

Подсчет пакетов, обработанных правилом

В разделе **«Основные параметры»** необходимо:

- в поле **«Счетчики»** установить переключатель в случае необходимости проводить подсчет пакетов, обработанных правилом.

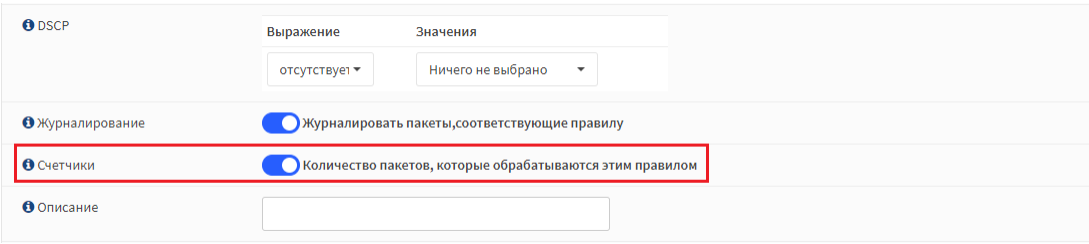


Рис. 366: Выбор параметра **«Счетчики»**

Добавление описания к правилу

В разделе **«Основные параметры»** необходимо:

- в поле **«Описание»** ввести необходимую информацию о настраиваемом правиле.

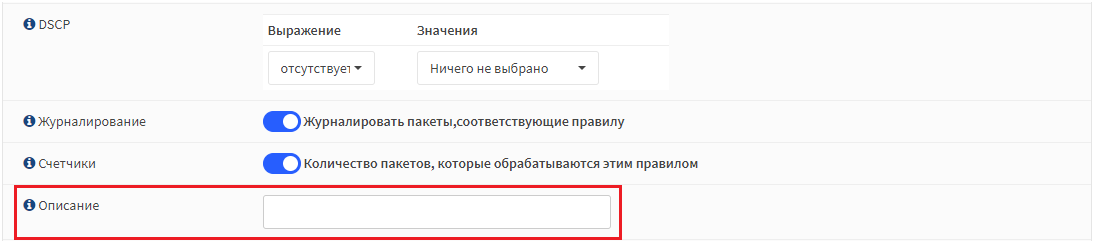


Рис. 367: Выбор параметра **«Описание»**

Дополнительные возможности

Расписание

Для выбора расписания, по которому будет работать правило необходимо:

- в разделе **«Основные параметры»** в поле **«Расписание»** выбрать из выпадающего списка:
  - **«отсутствует»** в случае отсутствия выбора расписания;
  - пустое поле для введения расписания, по которому будет работать правило.

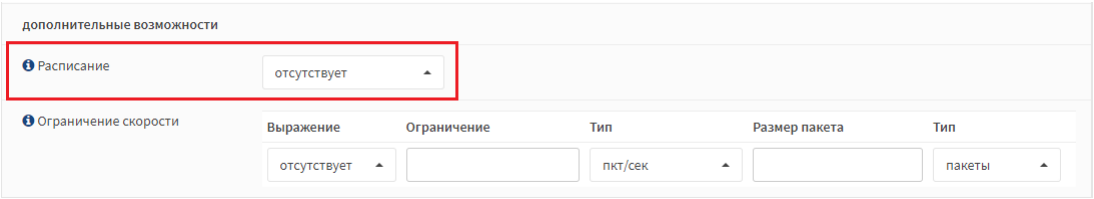


Рис. 368: Выбор параметра **«Расписание»**

Ограничение скорости

В разделе **«Основные параметры»** в поле **«Ограничение скорости»** необходимо:

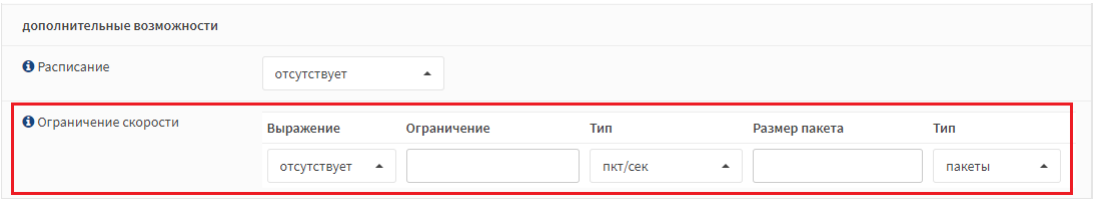


Рис. 369: Настройка парамера **«Ограничение скорости»**

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 115: Выбор параметра

Параметр	Примечание
Отсутствует	Использовать ограничение эквивалентно обычному
Больше, чем	Больше, чем указанное ограничение

- в колонке **«Ограничение»** указать ограничение;
- в колонке **«Тип»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 116: Выбор типа

Тип	Примечание
пкт/сек	Пакеты в секунду
пкт/мин	Пакеты в минуту
пкт/час	Пакеты в час
pkt/day	Пакеты в день
пкт/нед	Пакеты в неделю
байты/сек	Байты в секунду
килобайты/сек	Килобайты в секунду
мегабайты/сек	Мегабайты в секунду

- в колонке **«Размер пакета»** указать размер пакета данных;
- в колонке **«Тип»** выбрать из выпадающего списка один из необходимых параметров.

Дополнительные параметры

ID правила

В разделе **«Дополнительные параметры»** необходимо:

- в поле **«Установить идентификатор правила»** указать (присвоить) необходимый ID.

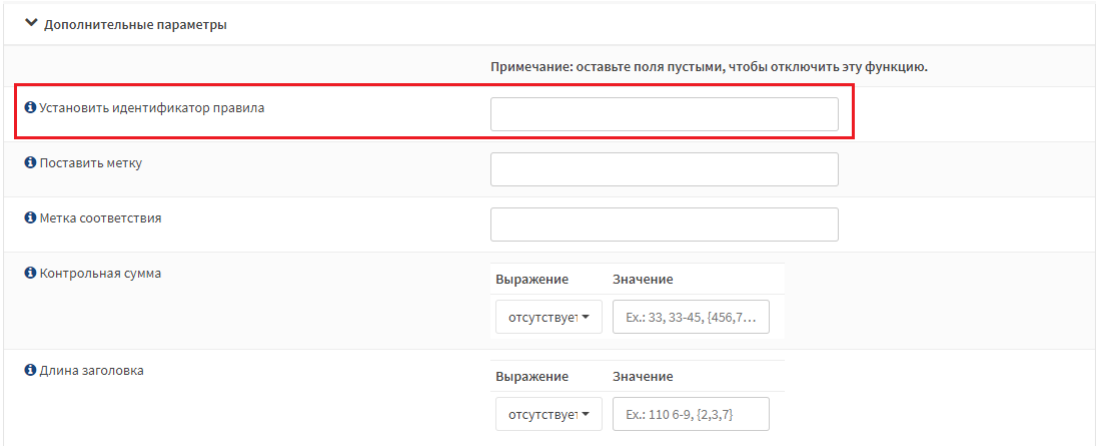


Рис. 370: Установить идентификатор правила

Маркировка пакета

В разделе **«Дополнительные параметры»** необходимо:

- в поле **«Поставить метку»** указать необходимую метку пакета данных, которая будет соответствовать выбранному правилу.

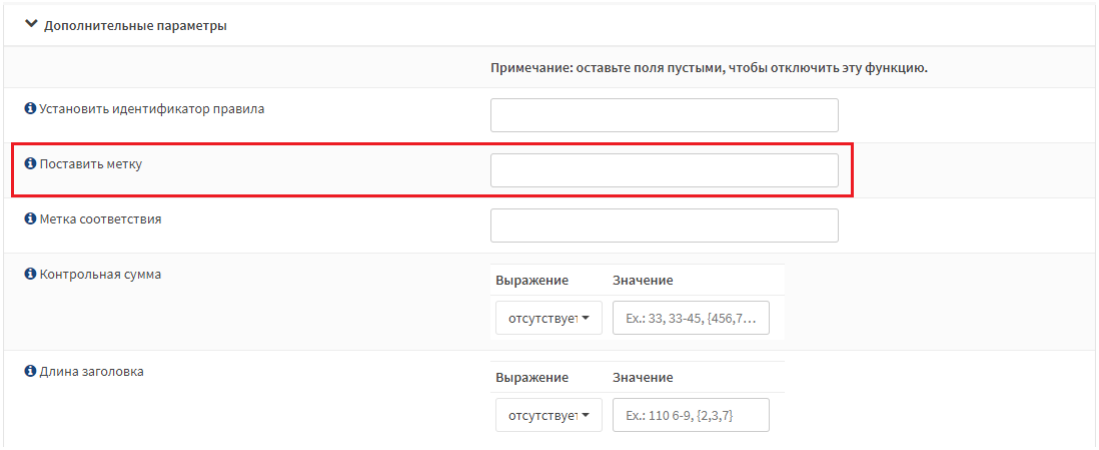


Рис. 371: Маркировка пакета данных

Отслеживание маркированного пакета

В разделе **«Дополнительные параметры»** необходимо:

- в поле **«Метка соответствия»** указать именованную метку (дескриптор), на основании которой будет проводиться отслеживание маркированного пакета.

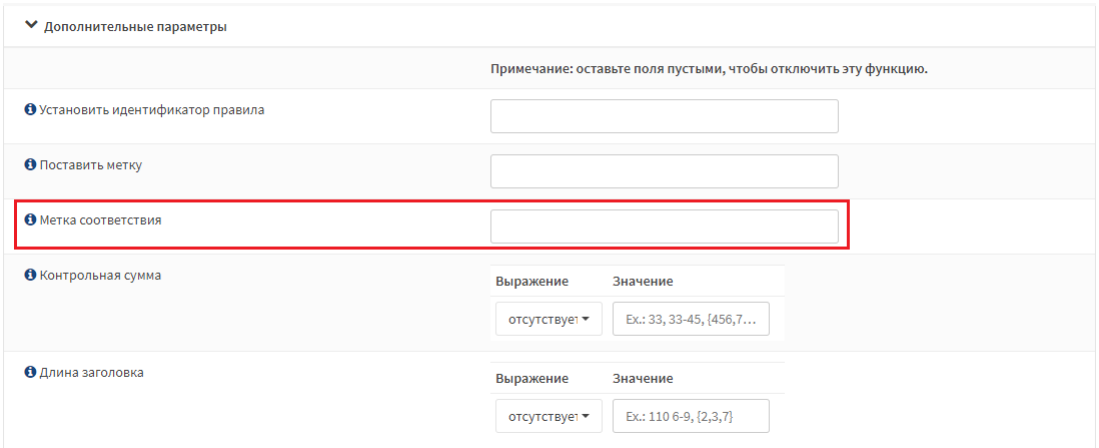


Рис. 372: Отслеживание маркированного пакета

Контрольная сумма пакета

В разделе **«Дополнительные параметры»** в поле **«Контрольная сумма»** необходимо:

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 117: Выбор параметра

Параметр	Примечание
Отсутствует	
Равный	Равно заданному значению
Не равен	Не равно заданному значению

- в колонке **«Значение»** указать необходимую контрольную сумму пакета.

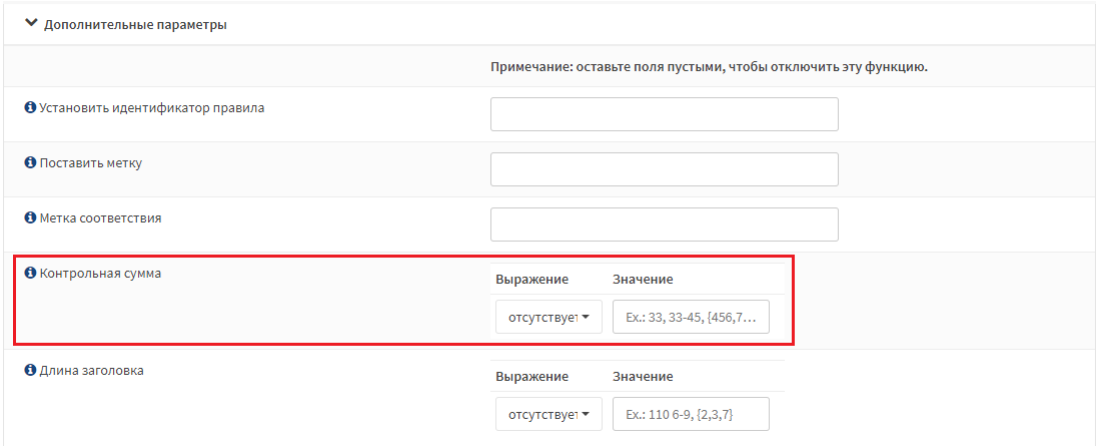


Рис. 373: Установка контрольной суммы

Длина заголовка пакета

В разделе **«Дополнительные параметры»** в поле **«Длина заголовка»** необходимо:

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 118: Выбор параметра

Параметр	Примечание
Отсутствует	
Равный	Равно заданному значению
Не равен	Не равно заданному значению

- в колонке **«Значение»** указать необходимую длину заголовка.

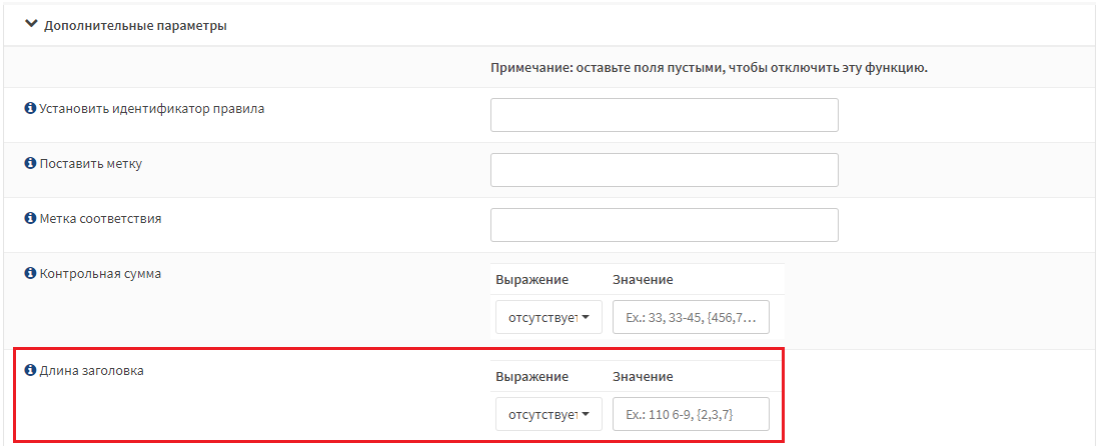


Рис. 374: Установка длины заголовка

Состояние соединения

В разделе **«Дополнительные параметры»** в поле **«Состояние соединения»** необходимо:

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 119: Выбор параметра

Параметр	Примечание
Отсутствует	
Равный	Равно заданному значению
Не равен	Не равно заданному значению

- в колонке **«Значение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 120: Выбор параметра

Параметр	Примечание
Отсутствует	
New	Пакет инициирует новое соединение, либо связан с соединением, по которому ещё не проходили пакеты в обоих направлениях
Establisl	Пакет связан с соединением, по которому уже проходили пакеты в обоих направлениях
Related	Пакет инициирует новое соединение, но также связан с уже существующим соединением, например при передаче данных по FTP или сообщении об ошибке ICMP
Untracke	Исключенные пакеты
Invalid	Пакет не связан с каким-либо известным соединением

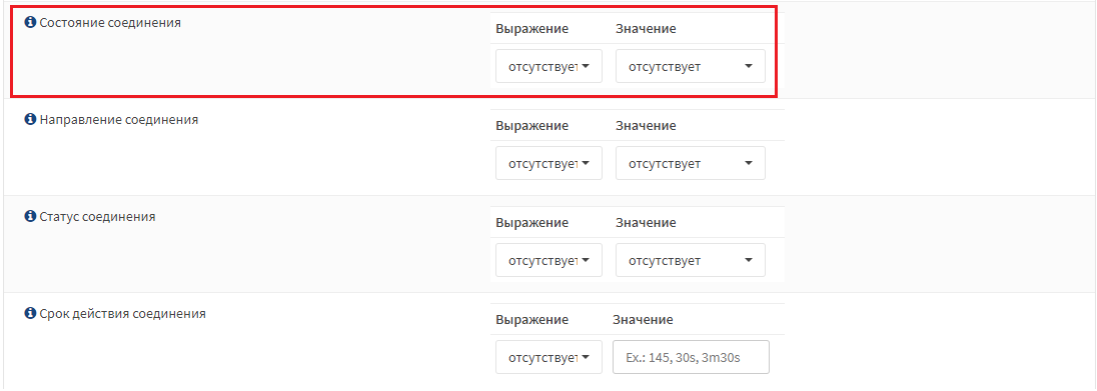


Рис. 375: Установка состояния соединения

Направление пакета

В разделе **«Дополнительные параметры»** в поле **«Направление соединения»** необходимо:

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 121: Выбор параметра

Параметр	Примечание
Отсутствует	
Равный	Равно заданному значению
Не равен	Не равно заданному значению

- в колонке **«Значение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 122: Выбор параметра

Параметр	Примечание
Original	Отправленные пакеты
Reply	Ответные пакеты

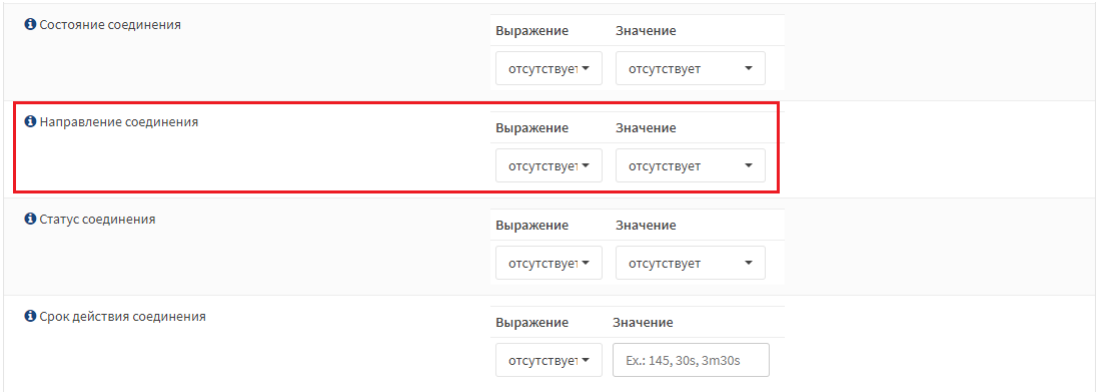


Рис. 376: Направление пакета

Статус соединения

В разделе **«Дополнительные параметры»** в поле **«Статус соединения»** необходимо:

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 123: Выбор параметра

Параметр	Примечание
Отсутствует	
Равный	Равно заданному значению
Не равен	Не равно заданному значению

- в колонке **«Значение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 124: Выбор параметра

Параметр	Примечание
Отсутствует	
Expe	Ожидаемое соединение
Conf	Подтвержденное соединение. Такой статус присваивается соединению после того, как пакет покинул локальный хост
Seen-reply	Дидит соединение в двух направлениях reply и original
Assu	Соединение можно считать полностью установленным. Этот статус присваивается соединению после передачи определенного количества данных. Присвоение данного статуса приводит к увеличению conntrack-тайм-аута для данного соединения (эти тайм-ауты используются для определения и удаления «повисших» и оборванных соединений)
Dyin	Соединение удалено из листа
Snat	Соединению нужен snat в original направлении
Dnat	Соединению нужен dnat в original направлении

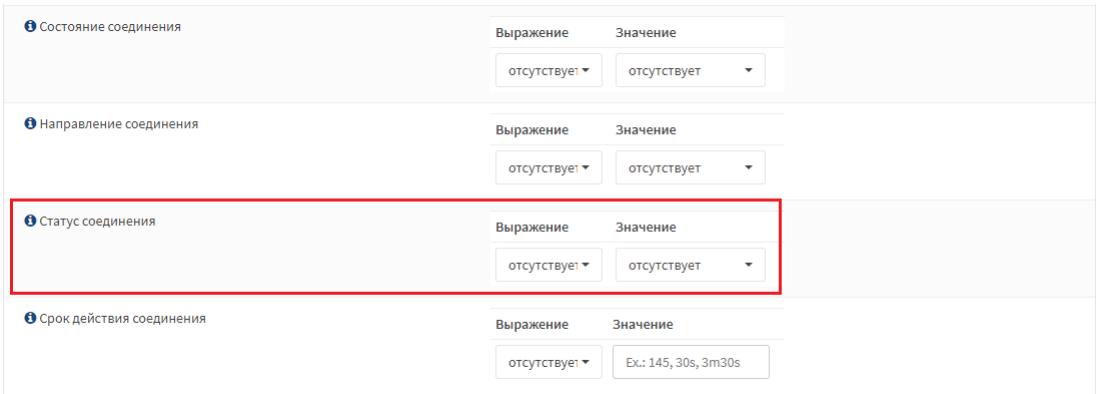


Рис. 377: Статус соединения

Время истечения срока действия подключения

В разделе **«Дополнительные параметры»** в поле **«Срок действия соединения»** необходимо:

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 125: Выбор параметра

Параметр	Примечание
Отсутствует	
Равный	Равно заданному значению
Не равен	Не равно заданному значению

- в колонке **«Значение»** указать значение истечения срока соединения.

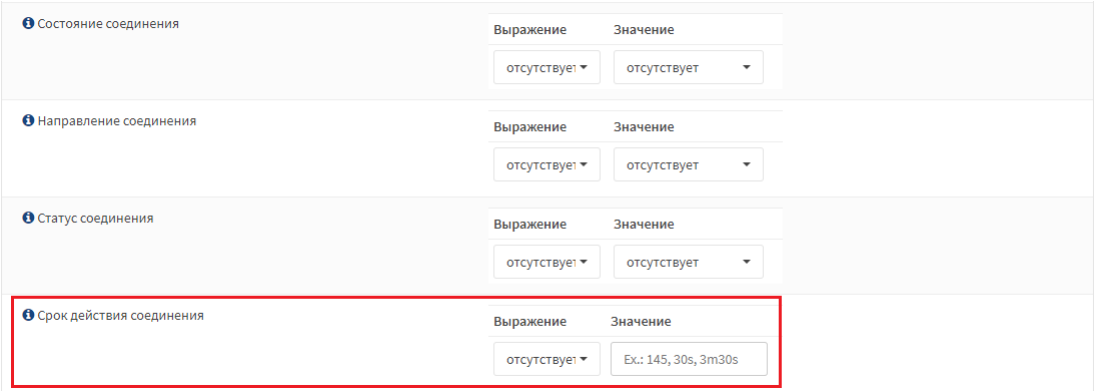


Рис. 378: Установка времени истечения срока действия подключения

Ограничению пропускной способности

В разделе **«Дополнительные параметры»** в поле **«Ограничение пропускной способности соединения»** необходимо:

- в колонке **«Направление»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 126: Выбор параметра

Параметр	Примечание
отсутствует	
Оба	
Оригинал	Отправленные пакеты
Отвечать	Ответные пакеты

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 127: Выбор параметра

Параметр	Примечание
Равный	Равно заданному значению

- в колонке **«Значение»** указать значение пропускной способности.

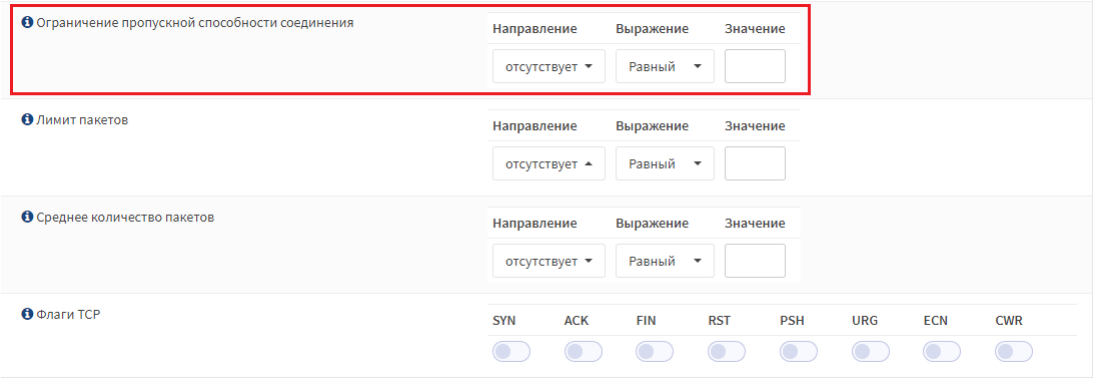


Рис. 379: Ограничение пропускной способности соединения

Ограничение количества пакетов

В разделе **«Дополнительные параметры»** в поле **«Лимит пакетов»** необходимо:

- в колонке **«Направление»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 128: Выбор параметра

Параметр	Примечание
отсутствует	
Оба	
Оригинал	Отправленные пакеты
Отвечать	Ответные пакеты

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 129: Выбор параметра

Параметр	Примечание
Равный	Равно заданному значению

- в колонке **«Значение»** указать количество пакетов.

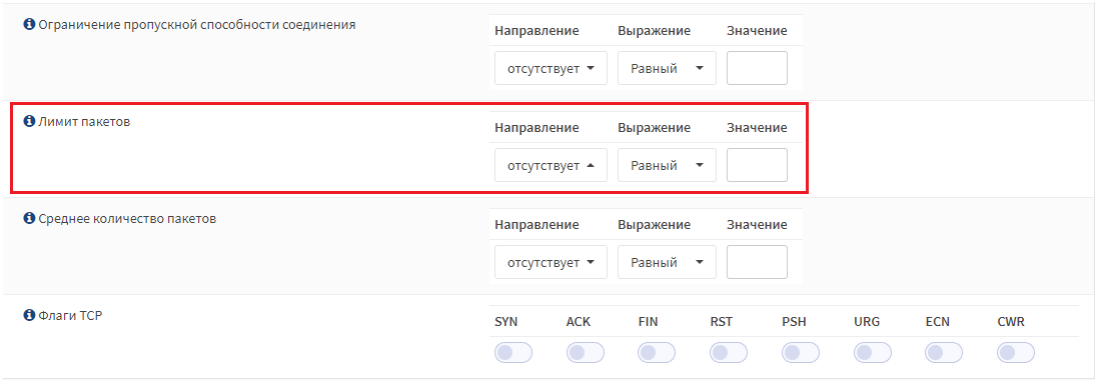


Рис. 380: Ограничение количества пакетов

Среднее количество пакетов

В разделе **«Дополнительные параметры»** в поле **«Среднее количество пакетов»** необходимо:

- в колонке **«Направление»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 130: Выбор параметра

Параметр	Примечание
отсутствует	
Оба	
Оригинал	Отправленные пакеты
Отвечать	Ответные пакеты

- в колонке **«Выражение»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 131: Выбор параметра

Параметр	Примечание
Равный	Равно заданному значению

- в колонке **«Значение»** указать средний размер пакета.

Флаги, содержащиеся в пакете

В разделе **«Дополнительные параметры»** необходимо:

- в поле **«Флаги TCP»** поставить галочку напротив выбранного флага.

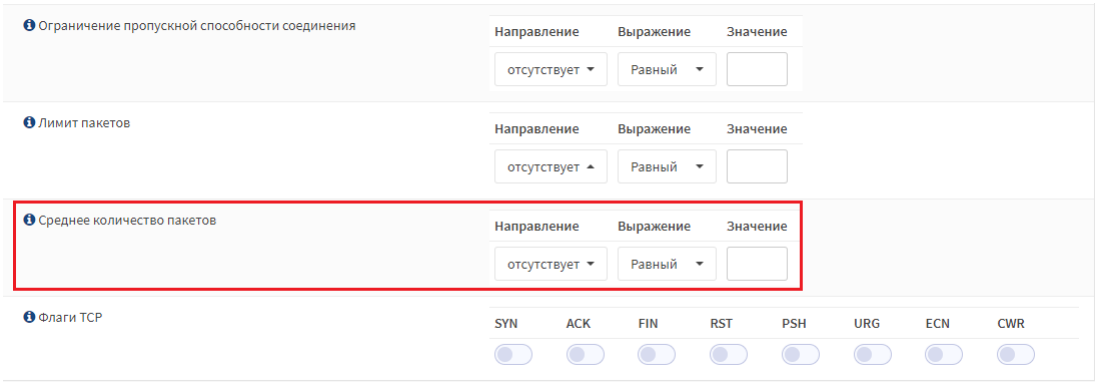


Рис. 381: Средний размер пакета

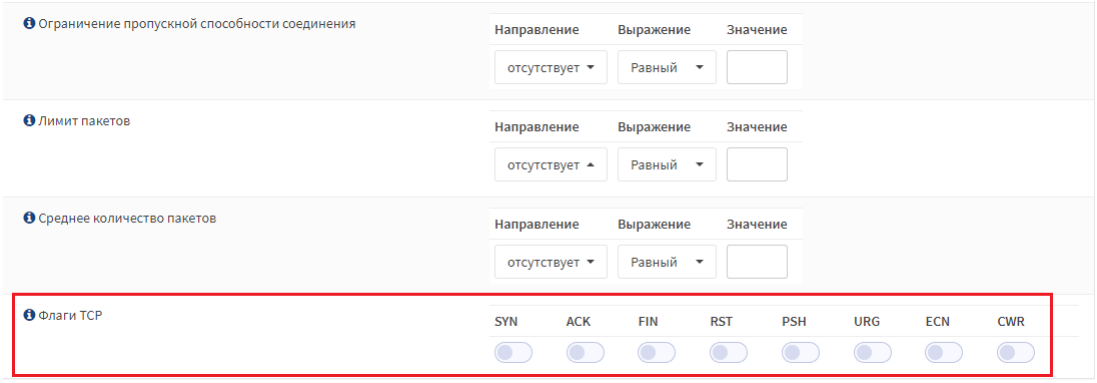


Рис. 382: Флаги, содержащимся в пакете

Lite DPI

Для настроек Lite DPI необходимо:

- в поле **«Профиль»** выбрать из выпадающего списка необходимый тип профиля;

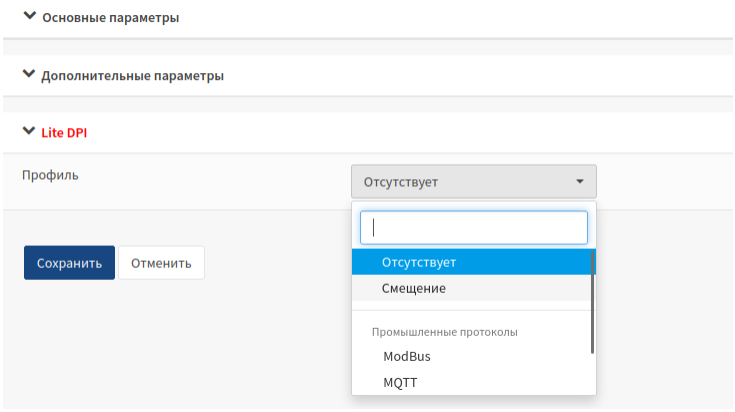


Рис. 383: Выбор профиля

Смещение

Для настроек смещения необходимо:

- в поле **«Профиль»** выбрать из выпадающего списка тип профиля **«Смещение»**;

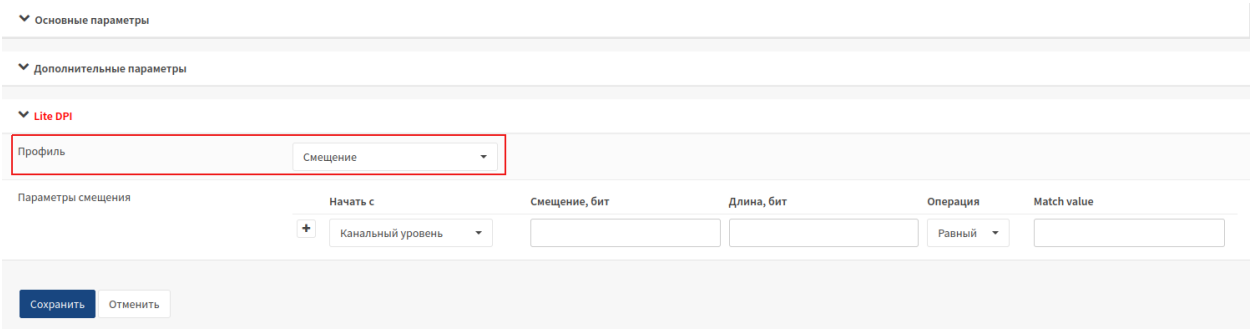


Рис. 384: Настройка смещения

- в поле **«Параметры смещения»** настроить параметры смещения;
- нажать кнопку 

для сохранения сконфигурированных настроек.

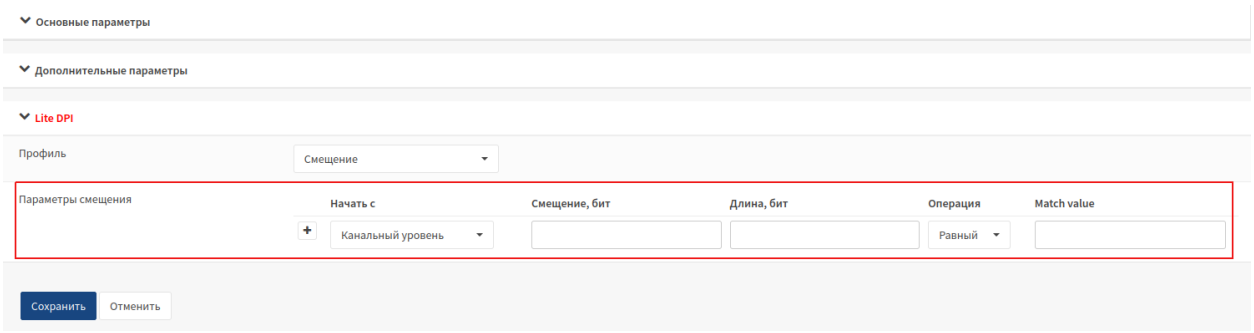


Рис. 385: Настройка параметров смещения

ModBus

Для настроек ModBus необходимо:

- в поле **«Профиль»** выбрать из выпадающего списка тип профиля **«ModBus»**;

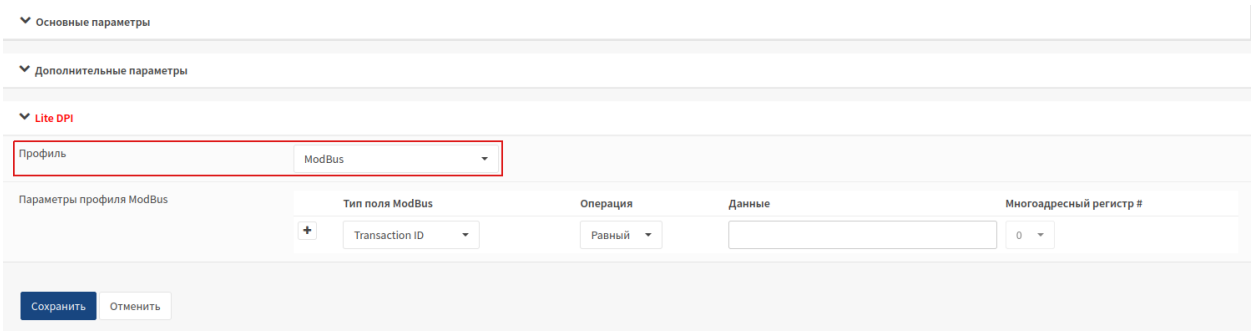


Рис. 386: Настройка ModBus

- в поле **«Параметры профиля ModBus»** настроить параметры профиля ModBus;

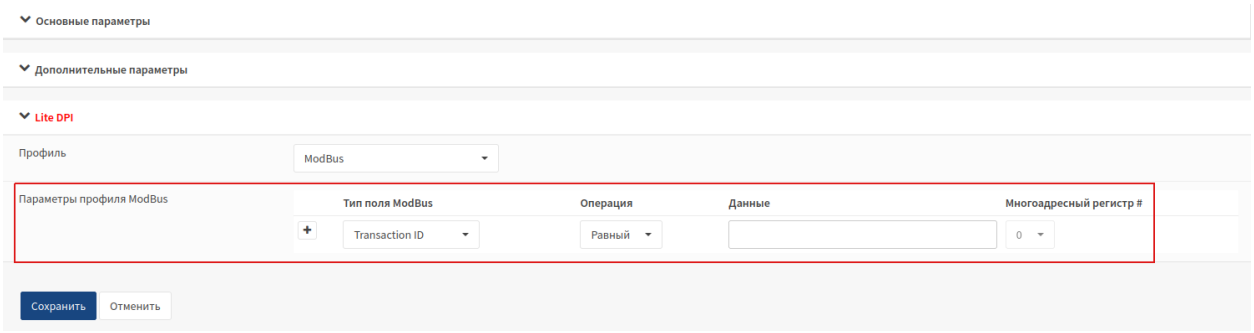


Рис. 387: Настройка параметров профиля ModBus

- нажать кнопку 

для сохранения сконфигурированных настроек.

MQTT

Для настроек MQTT необходимо:

- в поле **«Профиль»** выбрать из выпадающего списка тип профиля **«MQTT»**;

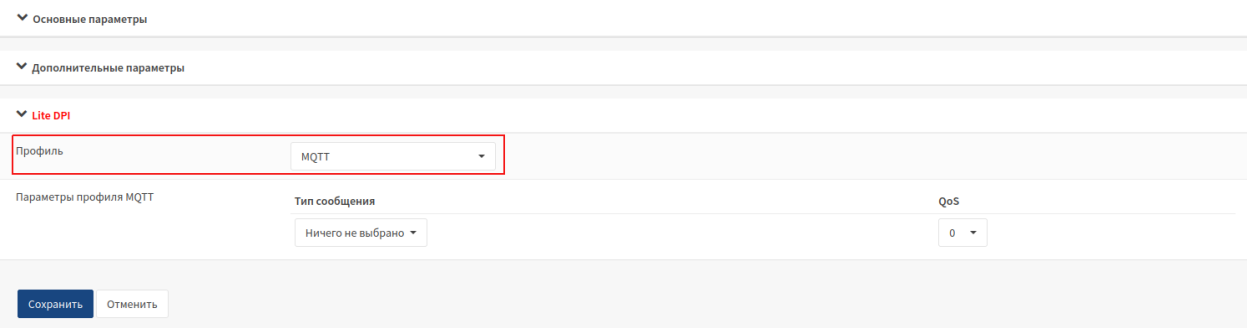


Рис. 388: Настройка MQTT

- в поле **«Параметры профиля MQTT»** настроить параметры профиля MQTT;

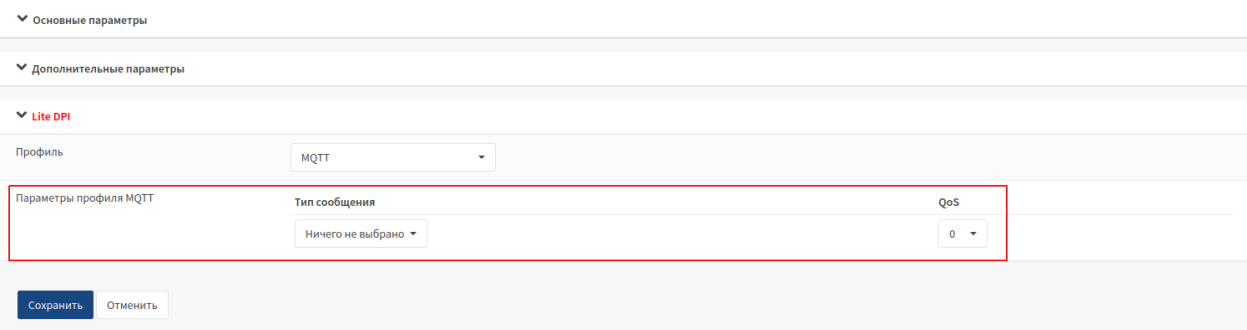


Рис. 389: Настройка параметров профиля MQTT

- нажать кнопку 

для сохранения сконфигурированных настроек.

Open communications Platforms

Для настроек Open communications Platforms необходимо:

- в поле **«Профиль»** выбрать из выпадающего списка тип профиля **«Open communications Platforms»**;
- нажать кнопку 

для сохранения сконфигурированных настроек.

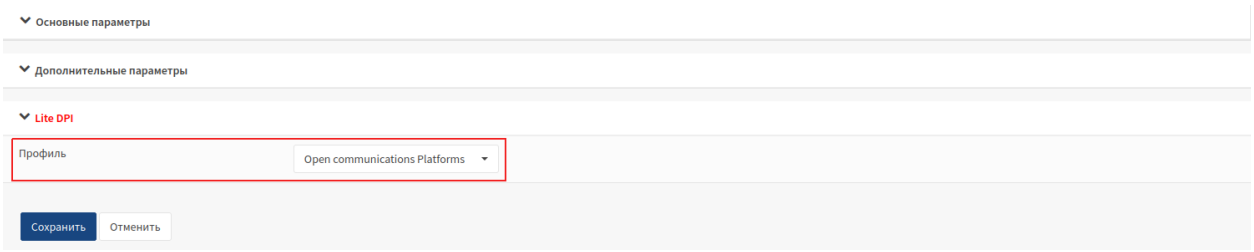


Рис. 390: Настройка Open communications Platforms

IEC-104

Для настроек IEC-104 необходимо:

- в поле **«Профиль»** выбрать из выпадающего списка тип профиля **«IEC-104»**;

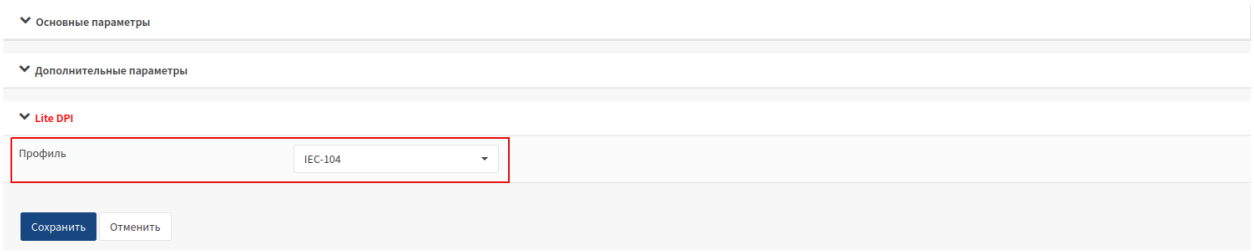


Рис. 391: Настройка IEC-104

- нажать кнопку 

для сохранения сконфигурированных настроек.

2.7.5.5 Настройки

Для перехода к настройкам необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«Настройки»**, расположенную в левой части списка объектов управления;

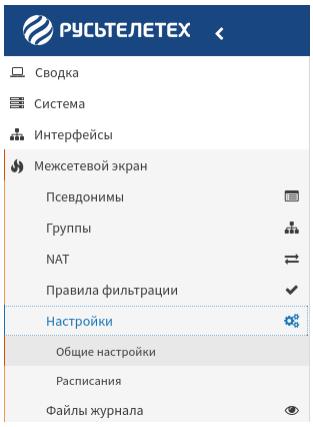


Рис. 392: Переход к настройкам

После выполненных настроек необходимо:

- нажать кнопку **«Сохранить»** 

.

Для перехода к настройкам расписаний необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«Настройки»** - **«Расписания»**, расположенную в левой части списка объектов управления;

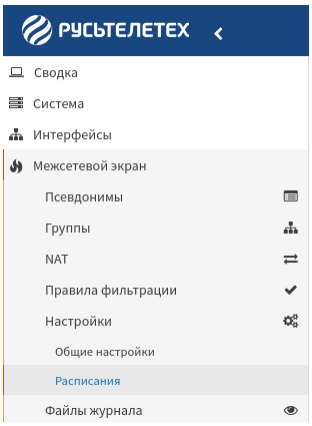


Рис. 393: Переход к настройкам расписаний

- в правой части экрана появиться таблица расписаний;

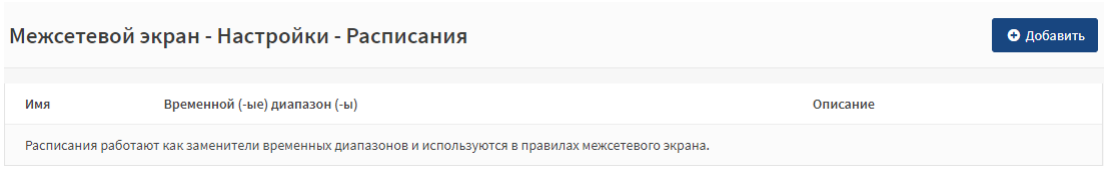


Рис. 394: Таблица расписаний

- нажать кнопку **«Добавить»** 

для добавления нового расписания в таблицу.

Общие настройки

Основные настройки

Входное состояние

На вкладке **«Основные настройки»** необходимо:

- в поле **«Стандартная политика INPUT»** выбрать из выпадающего списка один из параметров, соответствующих таблице.

Таблица 132: Выбор параметра

Параметр	Примечание
принимать	Принимать пакет
сбросить	Отклонить пакет

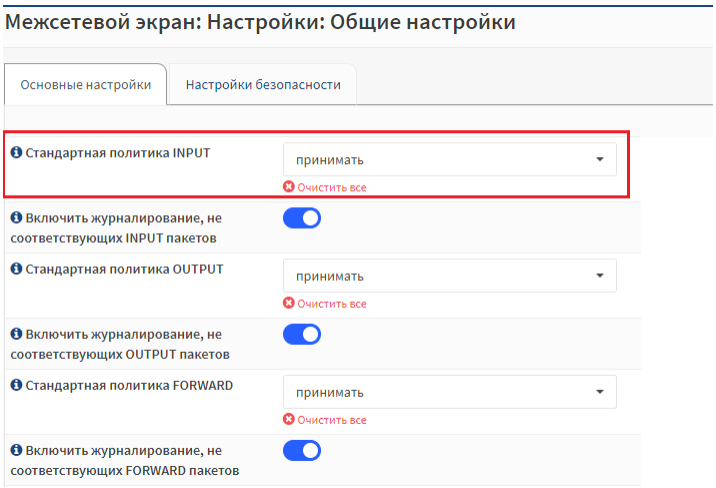


Рис. 395: Настройка входного состояния по умолчанию

- в поле **«Включить журналирование не соответствующих INPUT пакетов»** установить переключатель в случае необходимости включить ведение журнала для несоответствующих правил входного фильтра.

Примечание

Каждый входной пакет, который не соответствует наборам правил, будет записываться в log-файл.

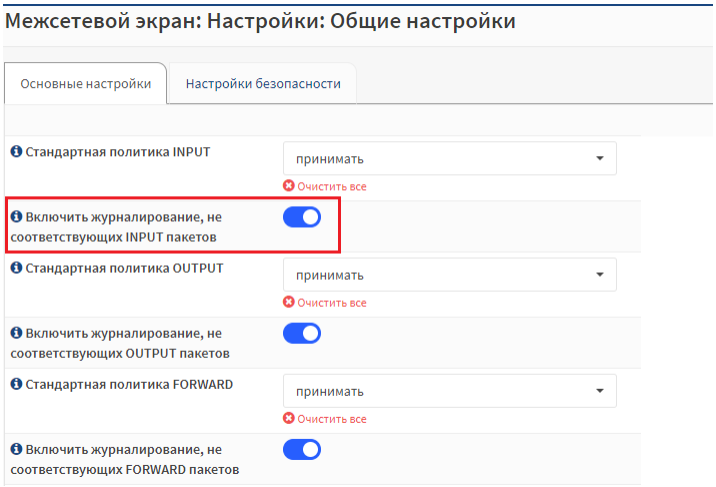


Рис. 396: Включить журналирование не соответствующих INPUT пакетов

Выходное состояние

На вкладке **«Основные настройки»** необходимо:

- в поле **«Стандартная политика OUTPUT»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 133: Выбор параметра

Параметр	Примечание
принимать	Принимать пакет
сбросить	Отклонить пакет

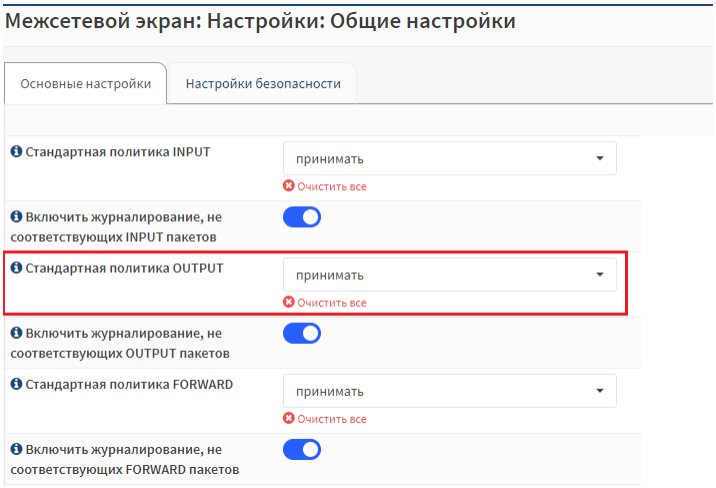


Рис. 397: Настройка выходного состояния по умолчанию

- в поле **«Включить журналирование не соответствующих OUTPUT пакетов»** установить переключатель в случае необходимости включить ведение журнала для несоответствующих правил выходного фильтра.

Примечание

Каждый выходной пакет, который не соответствует наборам правил, будет записываться в log-файл.

Транзитное состояние

На вкладке **«Основные настройки»** необходимо:

- в поле **«Стандартная политика FORWARD»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 134: Выбор параметра

Параметр	Примечание
принимать	Принимать пакет
сбросить	Отклонить пакет

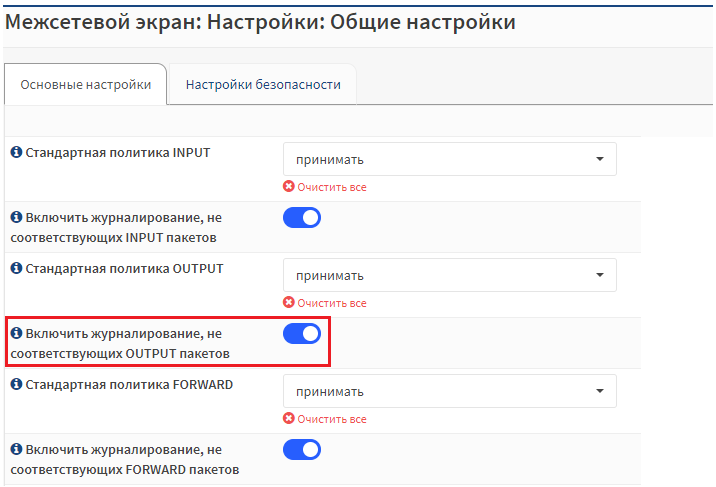


Рис. 398: Включить журналирование не соответствующих OUTPUT пакетов

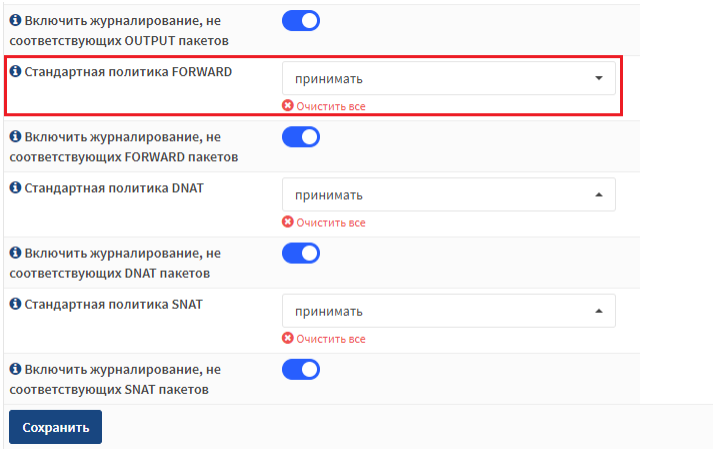


Рис. 399: Настройка транзитного состояния по умолчанию

- в поле **«Включить журналирование не соответствующих FORWARD пакетов»** установить переключатель в случае необходимости включить ведение журнала для несоответствующих правил транзитного фильтра.

Примечание

Каждый транзитный пакет, который не соответствует наборам правил, будет записываться в log-файл.

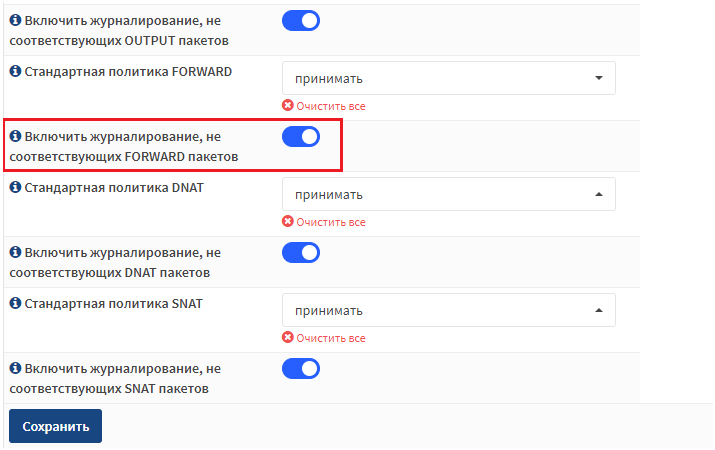


Рис. 400: Включить журналирование не соответствующих FORWARD пакетов

Настройка DNAT

- в поле **«Стандартная политика DNAT»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 135: Выбор параметра

Параметр	Примечание
принимать	Принимать пакет
сбросить	Отклонить пакет

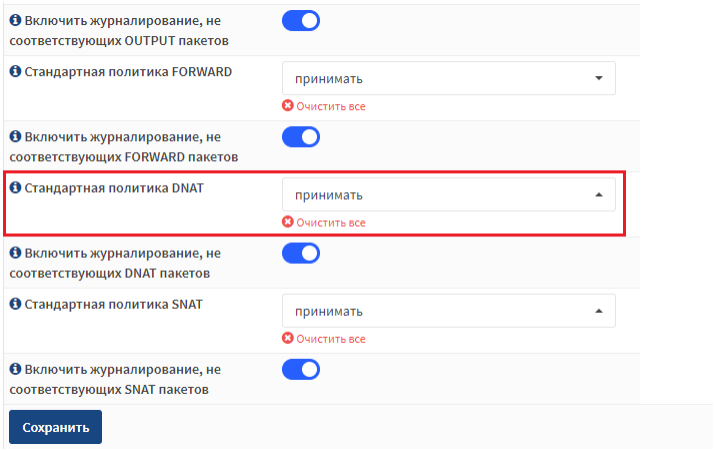


Рис. 401: Настройка DNAT

- в поле **«Включить журналирование не соответствующих DNAT пакетов»** установить переключатель в случае необходимости включить ведение журнала для несовпадающих пакетов DNAT.

Примечание

Каждый выходной пакет, который не соответствует наборам правил, будет записываться в log-файл.

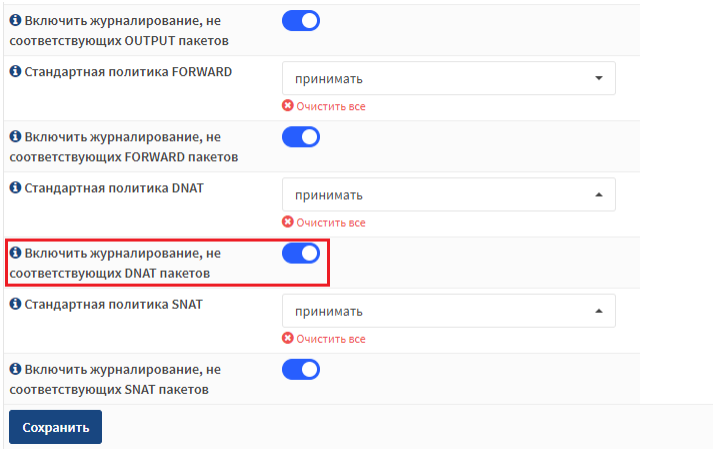


Рис. 402: Включить журналирование не соответствующих DNAT пакетов

Настройка SNAT

- в поле **«Стандартная политика SNAT»** выбрать из выпадающего списка один из параметров, соответствующих таблице;

Таблица 136: Выбор параметра

Параметр	Примечание
принимать	Принимать пакет
сбросить	Отклонить пакет

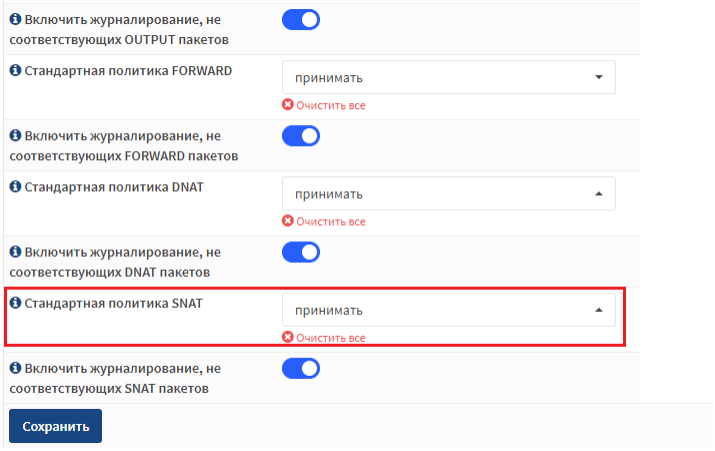


Рис. 403: Настройка SNAT

- в поле **«Включить журналирование не соответствующих SNAT пакетов»** установить переключатель в случае необходимости включить ведение журнала для несовпадающих пакетов SNAT;

Примечание

Каждый выходной пакет, который не соответствует наборам правил, будет записываться в log-файл.

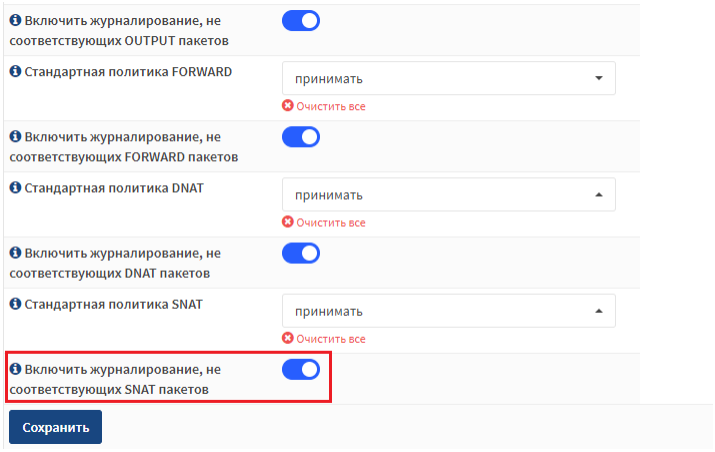


Рис. 404: Включить журналирование не соответствующих SNAT пакетов

- нажать кнопку **«Сохранить»**  для сохранения настроек.

Настройки безопасности

Для настроек безопасности необходимо:

- в поле **«Предотвращение конфигурации INPUT правил»** установить переключатель в случае необходимости предотвращения конфигурации INPUT правил;

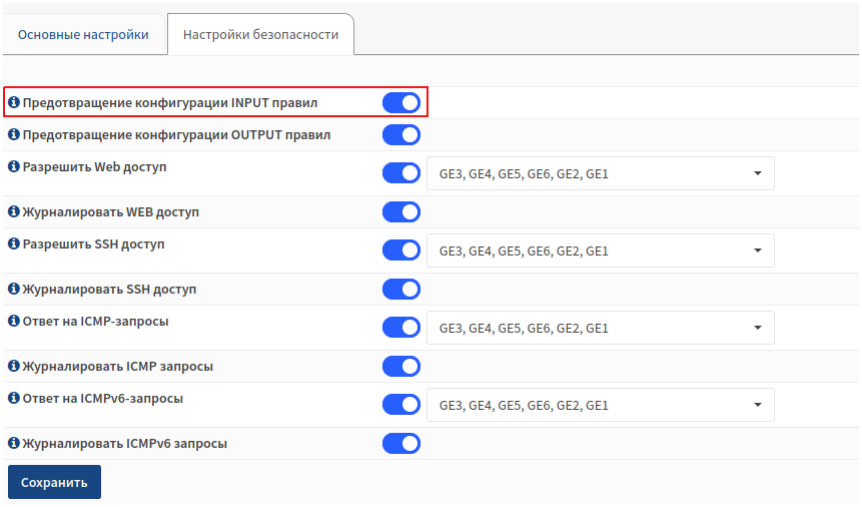


Рис. 405: Предотвращение конфигурации INPUT правил

Примечание

Настройка INPUT правил межсетевого экрана отключена по умолчанию. Пожалуйста, активируйте только в случае необходимости!

- в поле **«Предотвращение конфигурации OUTPUT правил»** установить переключатель в случае необходимости предотвращения конфигурации OUTPUT правил;

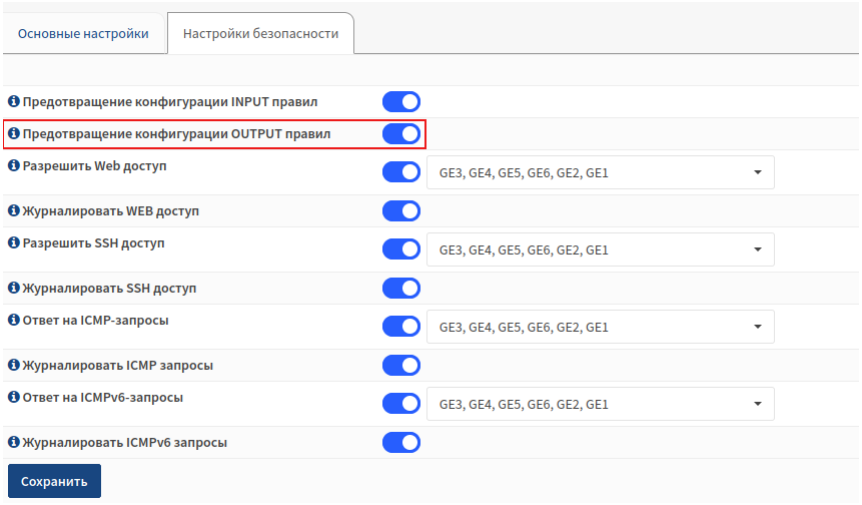


Рис. 406: Предотвращение конфигурации OUTPUT правил

Примечание

Настройка OUTPUT правил межсетевого экрана отключена по умолчанию. Пожалуйста, активируйте только в случае необходимости!

- в поле **«Разрешить Web доступ»** установить переключатель в случае необходимости разрешить Веб-доступ, затем из выпадающего списка выбрать необходимый интерфейс;

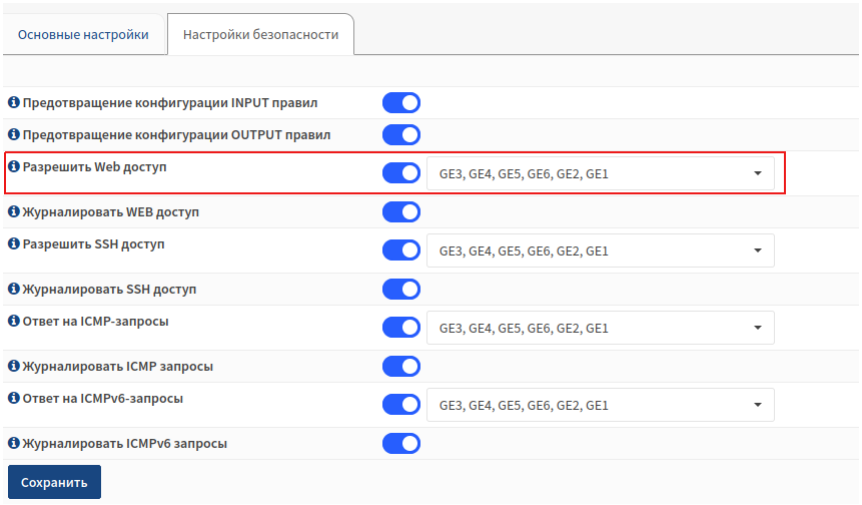


Рис. 407: Разрешить Веб-доступ

- в поле **«Журналировать WEB доступ»** установить переключатель в случае необходимости установить логин для входящих пакетов HTTP, HTTPS;

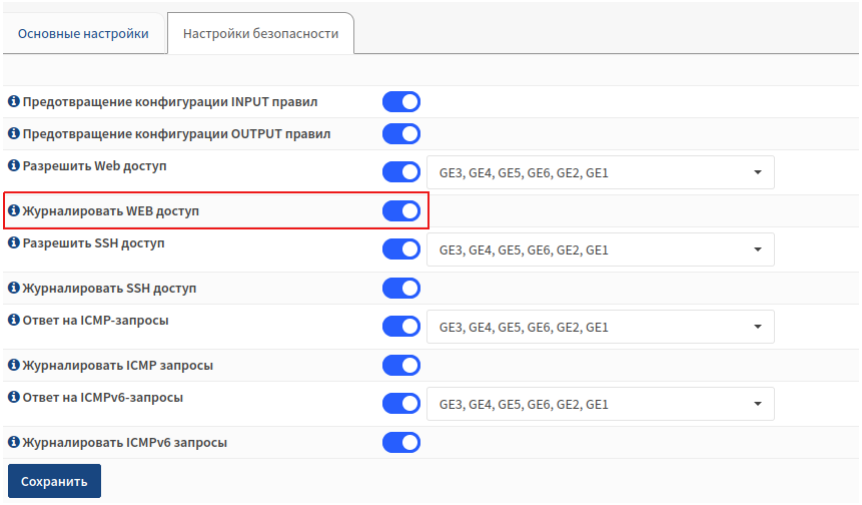


Рис. 408: Журналировать Веб-доступ

- в поле **«Разрешить SSH доступ»** установить переключатель в случае необходимости разрешить SSH доступ, затем из выпадающего списка выбрать необходимый интерфейс;

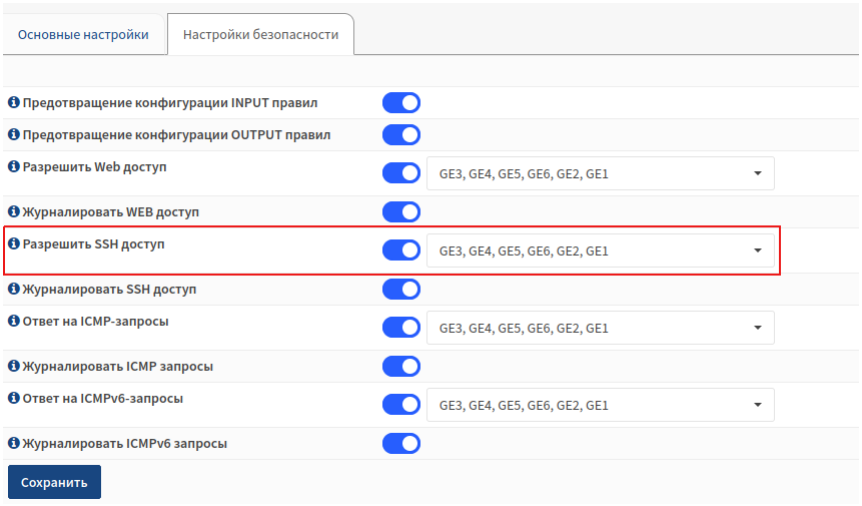


Рис. 409: Разрешить SSH доступ

- в поле **«Журналировать SSH доступ»** установить переключатель в случае необходимости установить логин для входящих пакетов SSH;
- в поле **«Ответ на ICMP-запросы»** установить переключатель в случае необходимости ответа на ICMP-запросы, затем из выпадающего списка выбрать необходимый интерфейс;

Примечание

Не активируйте, если хотите блокировать ответ на ICMP-запросы

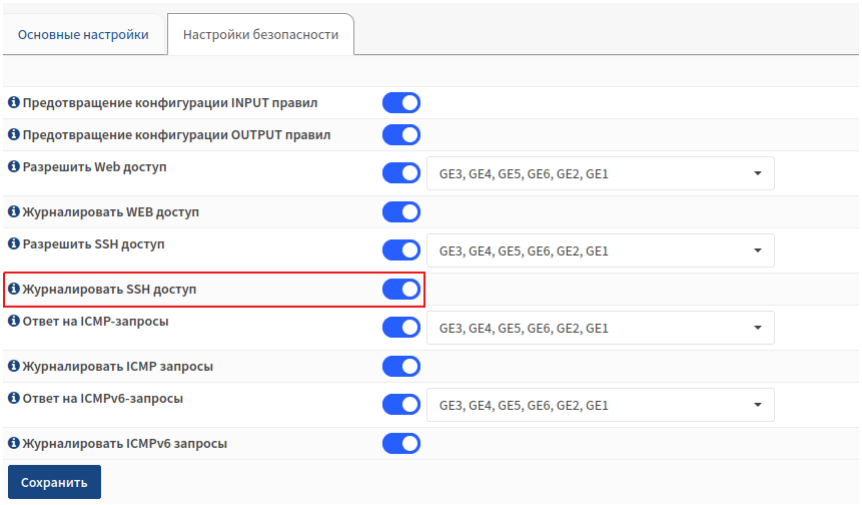


Рис. 410: Журналировать SSH доступ

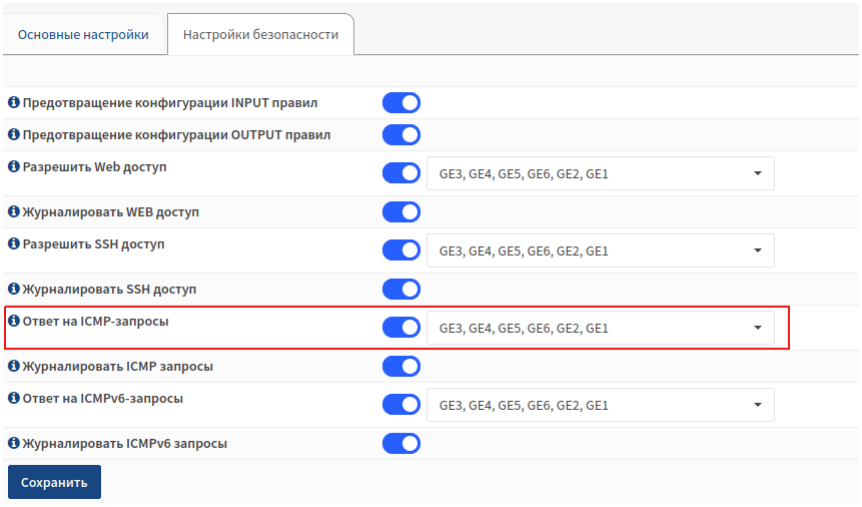


Рис. 411: Ответ на ICMP-запросы

- в поле **«Журналировать ICMP запросы»** установить переключатель в случае необходимости установить для входящих ICMP-пакетов;

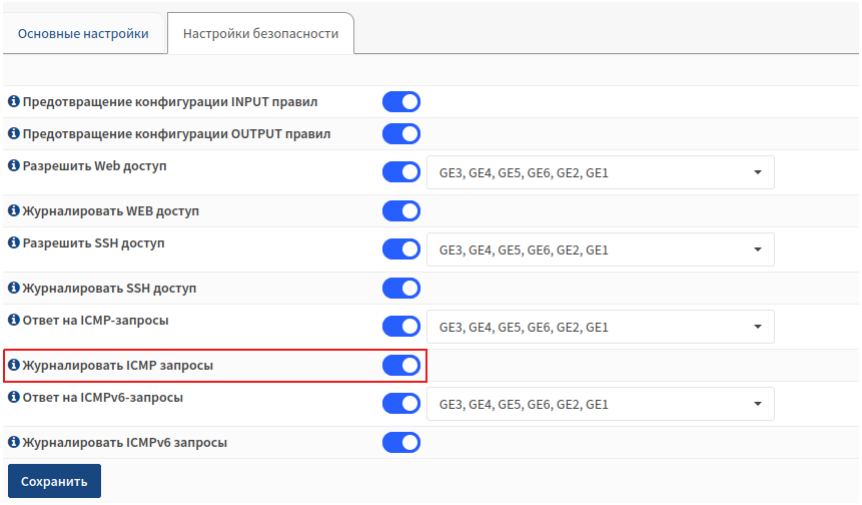


Рис. 412: Журналировать ICMP запросы

- в поле **«Ответ на ICMPv6-запросы»** установить переключатель в случае необходимости пропускать запросы icmpv6;

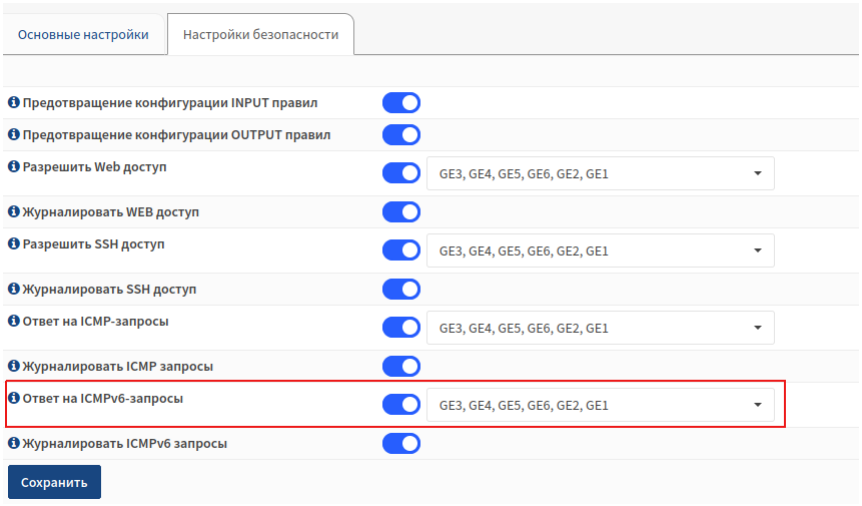


Рис. 413: Ответ на ICMPv6-запросы

- в поле **«Журналировать ICMPv6 запросы»** установить переключатель в случае необходимости Установить ведение журнала для входящих пакетов ICMPv6;
- нажать кнопку **«Сохранить»**  для сохранения настроек.

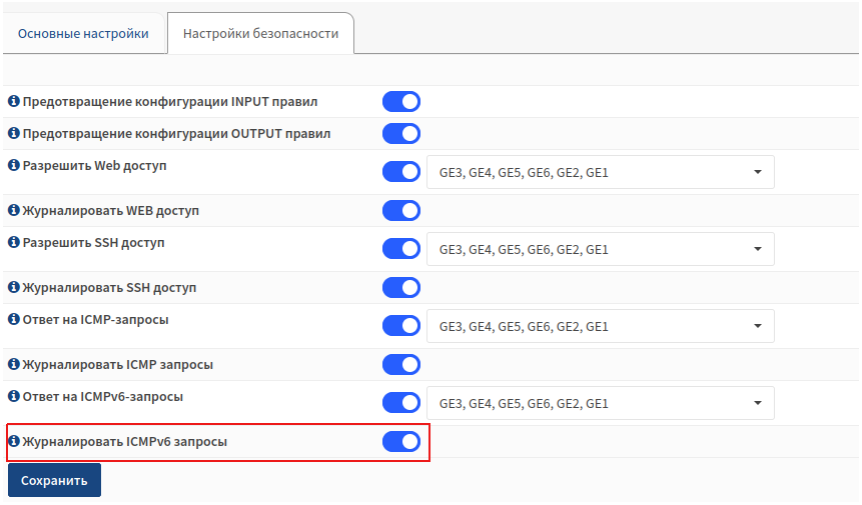


Рис. 414: Журналировать ICMPv6 запросы

Расписания

Расписание необходимо для задания временных интервалов выполнения правил межсетевого экрана.

Для настройки расписания необходимо:

- в поле **«Имя»** - имя расписания;

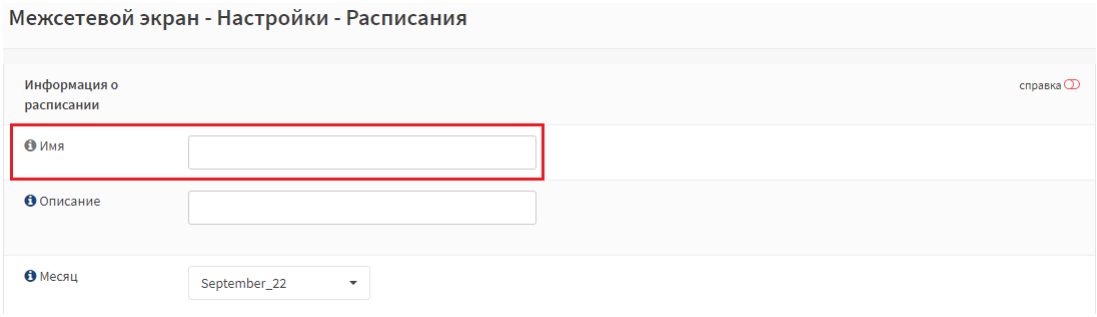


Рис. 415: Введение имени

- в поле **«Описание»** - описание расписания;
- в поле **«Месяц»** - нужный месяц и выберите дату расписания (день, неделя);
- в поле **«Время»** - время начала и время окончания действия расписания;
- в поле **«Описание временного диапазона»** - описание заданного временного диапазона;

После конфигурации настроек необходимо нажать кнопку **«Добавить время»** 

.

В разделе **«Повторение расписания»** в поле **«Настроенные диапазоны»** отражены ранее созданные временные диапазоны. Эти диапазоны можно корректировать и удалять (в случае необходимости).

Для создания сконфигурированного расписания необходимо нажать кнопку **«Сохранить»**

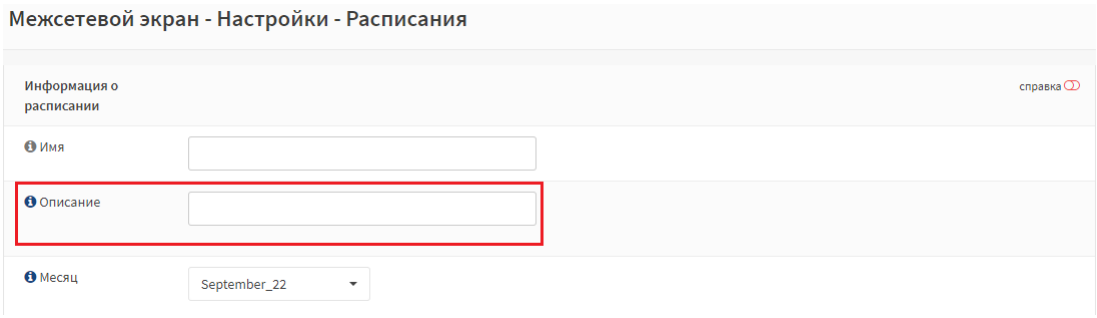


Рис. 416: Введение описания

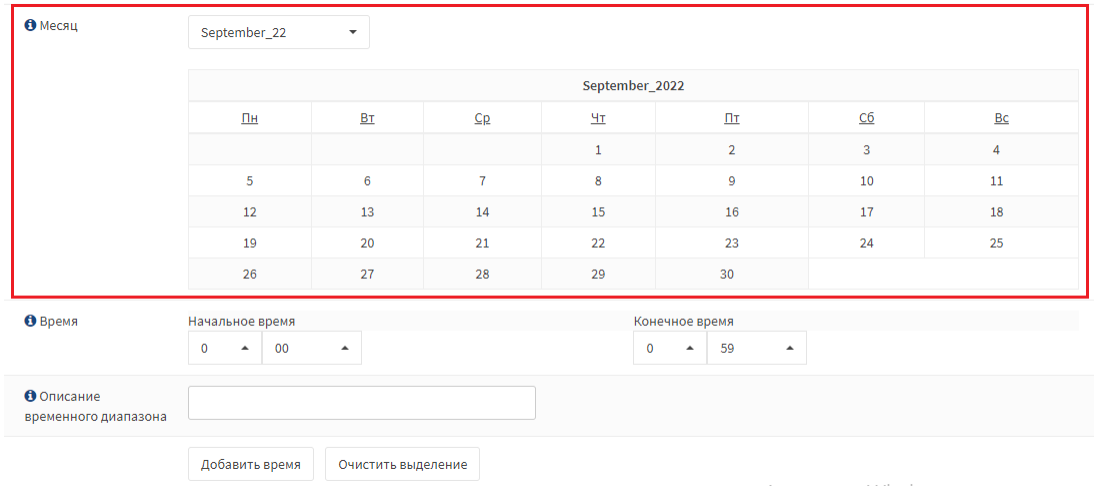


Рис. 417: Введение необходимой даты

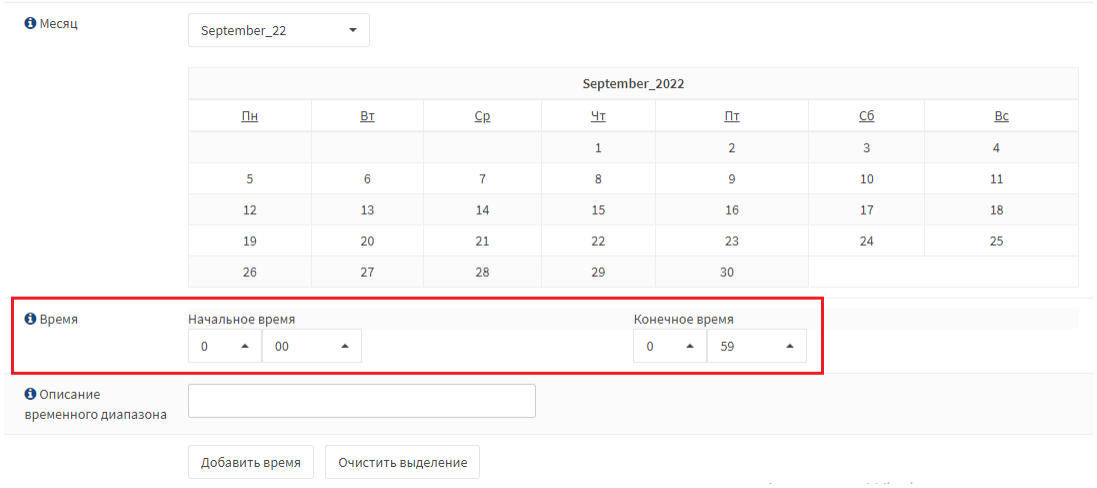


Рис. 418: Введение необходимого времени

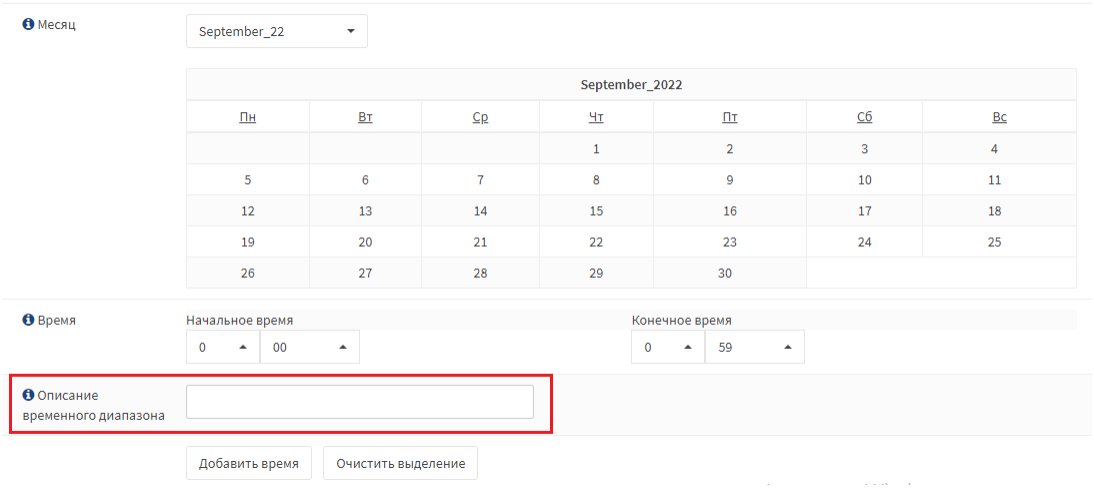


Рис. 419: Описание временного диапазона

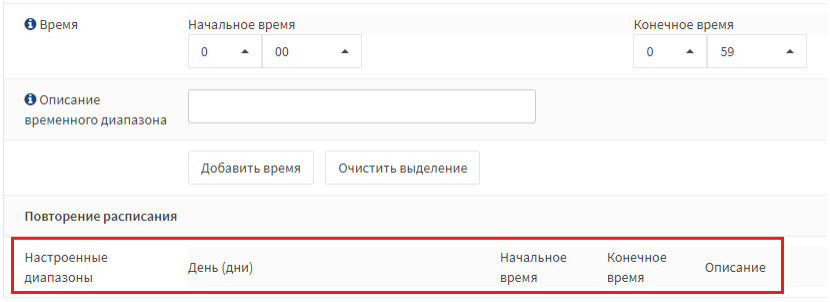


Рис. 420: Настроенные диапазоны

Сохранить .

Сконфигурированное расписание появиться в таблице расписаний,.

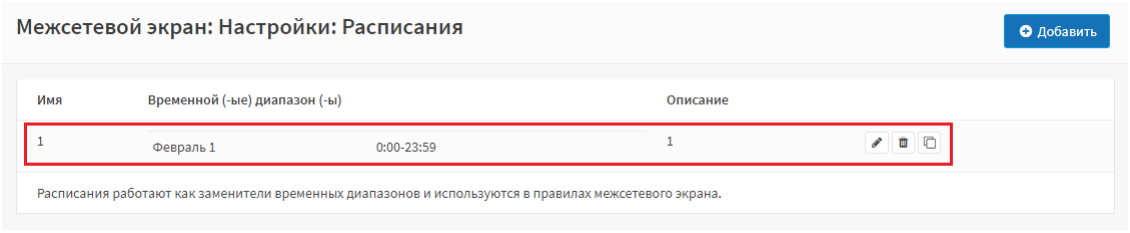


Рис. 421: Вступление сконфигурированного расписания в силу

2.7.5.6 Файлы журнала

Для перехода к просмотру таблицы журналов необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«Файлы журнала»** - **«Прямая трансляция»**, расположенную в левой части списка объектов управления;

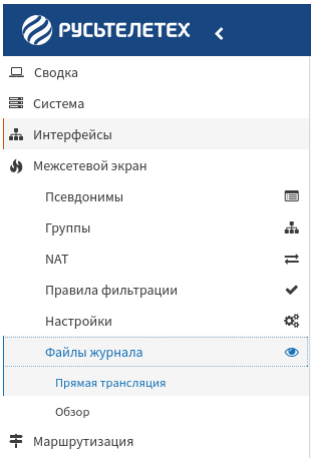


Рис. 422: Переход к просмотру таблицы журналов

Для перехода к просмотру статистики передаваемых и принимаемых данных необходимо:

- нажать на вкладку **«Межсетевой экран»** - **«Файлы журнала»** - **«Обзор»**, расположенную в левой части списка объектов управления;

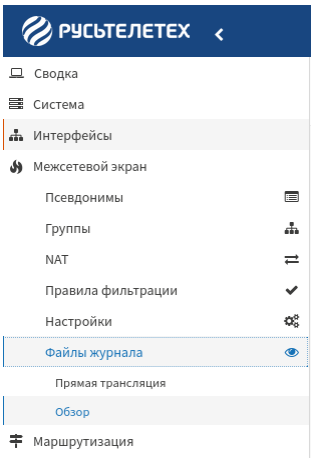


Рис. 423: Переход к просмотру статистики передаваемых и принимаемых данных

Прямая трансляция

Прямая трансляция предоставляет возможность просматривать и сортировать информацию, а так же результаты обработки пакета, добавленного в журнал межсетевого экрана.

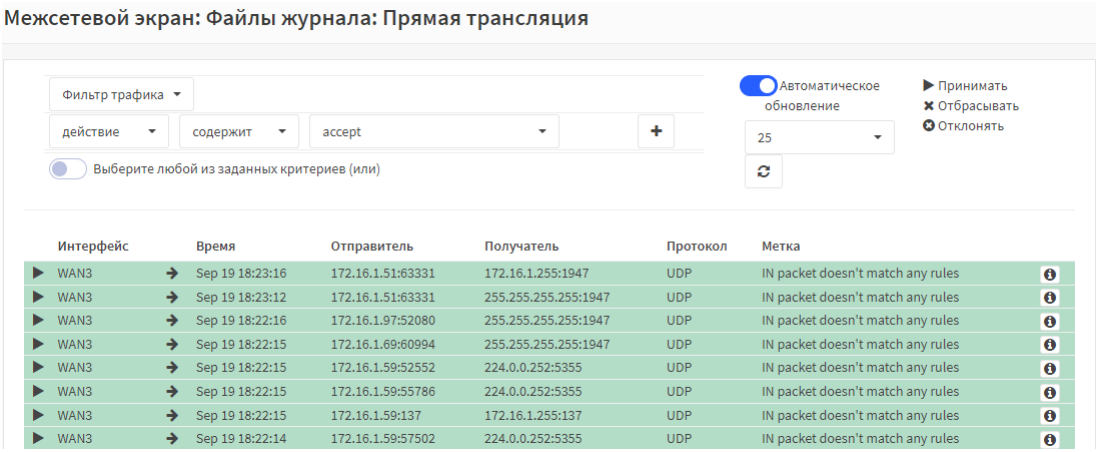


Рис. 424: Таблица обработанных пакетов

В колонке **«Интерфейс»** отражены типы используемых интерфейсов.

В колонке **«Время»** отражено время прохождения пакета через межсетевой экран.

В колонке **«Отправитель»** отражен IP адрес отправителя пакета.

В колонке **«Получатель»** отражен IP адрес получателя пакета.

В колонке **«Протокол»** отражен протокол передачи данных.

В колонке **«Метка»** содержится информация о соответствии пакета заданным правилам.

Для просмотра подробной информации о правиле необходимо:

- нажать на кнопку  ;

В открывшемся окне отражена подробная информация о правиле

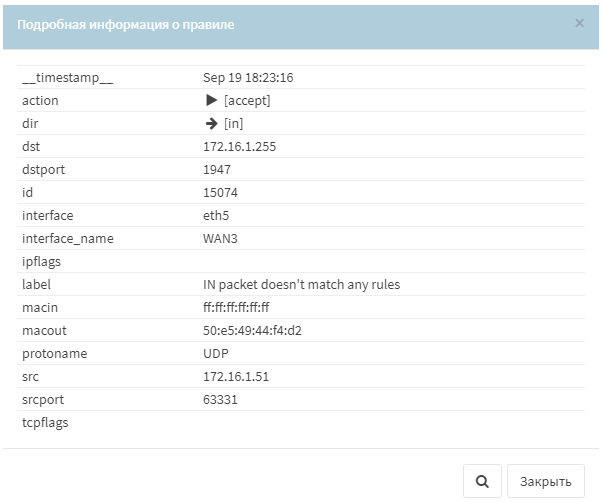


Рис. 425: Подробная информация о правиле

Для автоматического обновления таблицы обработанных пакетов необходимо установить переключатель **«Автоматическое обновление»**.

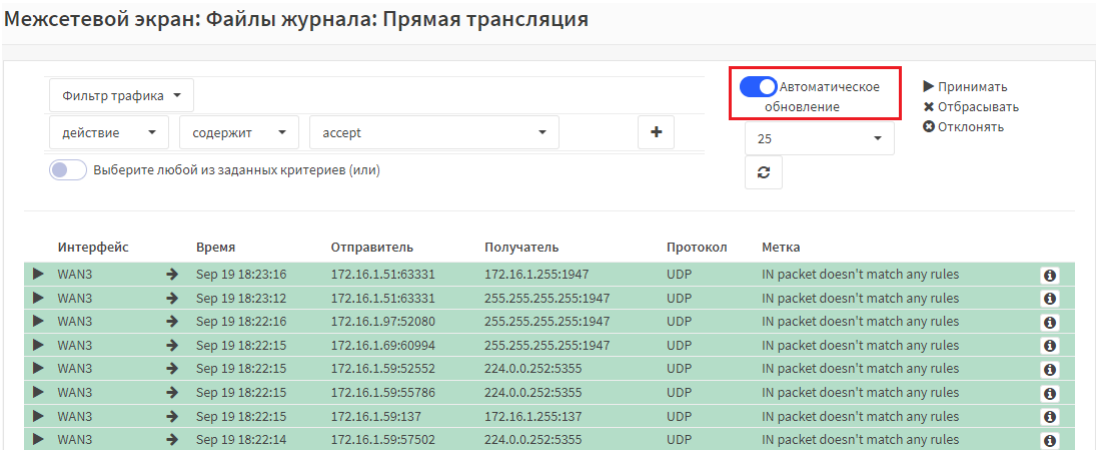


Рис. 426: Автоматическое обновление обработанных пакетов

Для ручного обновления таблицы обработанных пакетов необходимо выключить переключатель **«Автоматическое обновление»** и нажать кнопку  .

Для выбора отображения количественного значения обработанных пакетов необходимо:

- выбрать из выпадающего списка одно из значений, соответствующих таблице

Таблица 137: Выбираемое значение обработанных пакетов

Выбираемое значение
25
50
100

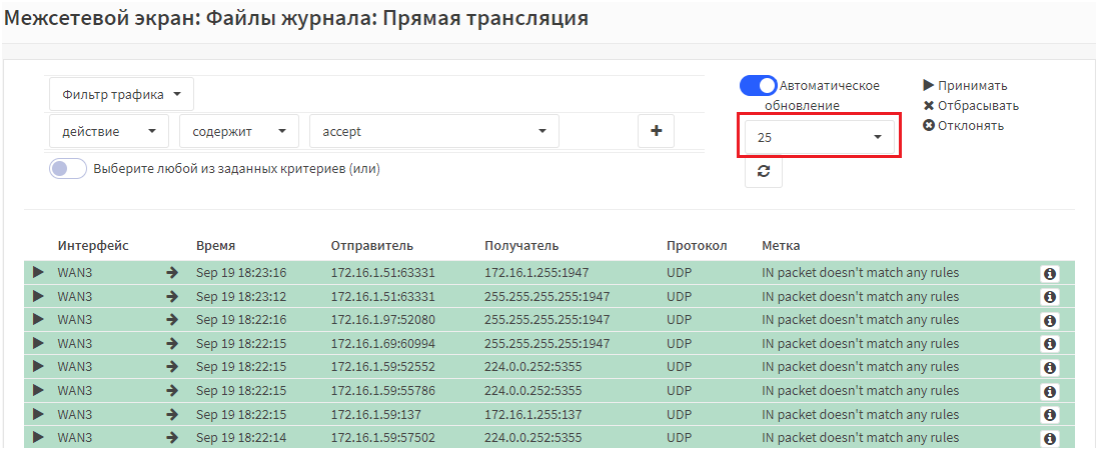


Рис. 427: Выбираемое значение обработанных пакетов

Сортировка обработанных пакетов

- выбрать из выпадающего списка один из фильтров, соответствующих таблице;

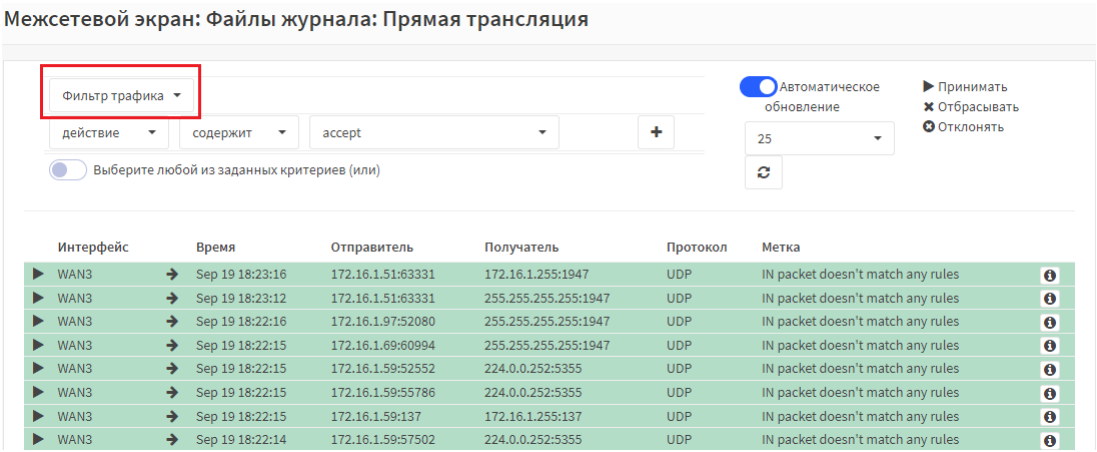


Рис. 428: Фильтры

Таблица 138: Фильтры

Фильтры
Filter IPv4
Filter IPv6

- выбрать из выпадающего списка один из параметров, соответствующих таблице;

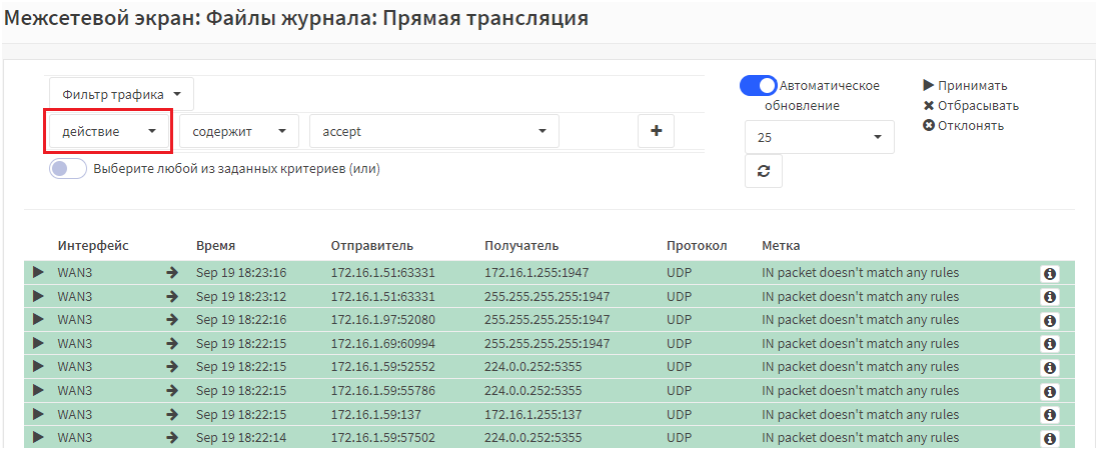


Рис. 429: Выбор параметра

Таблица 139: Выбор параметра

Параметр	Примечание
действие	Действие, проводимое с пакетом
интерфейс	Используемый интерфейс передачи данных
dir	Тип пакета (входящий/исходящий)
Время	Время прохождения пакета
src	IP адрес отправителя
src_port	Порт отправителя
dst	IP адрес получателя
dst_port	Порт получателя
хост	src и dst
порт	src_port и dst_port
protoname	Тип протокола передачи данных
метка	Информация о соответствии пакета заданным правилам

- выбрать из выпадающего списка один из параметров, соответствующих таблице;

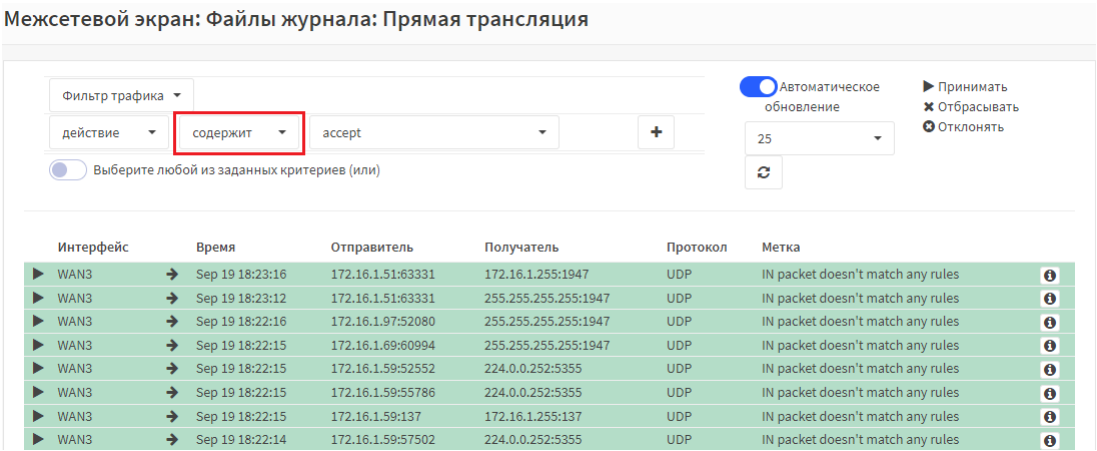


Рис. 430: Выбор параметра

Таблица 140: Выбор параметра

Параметр	Примечание
содержит	Содержит правило
является	Является правилом
не содержит	Не содержит правило
не является	Не является правилом

- выбрать из выпадающего списка один из параметров, соответствующих таблице;

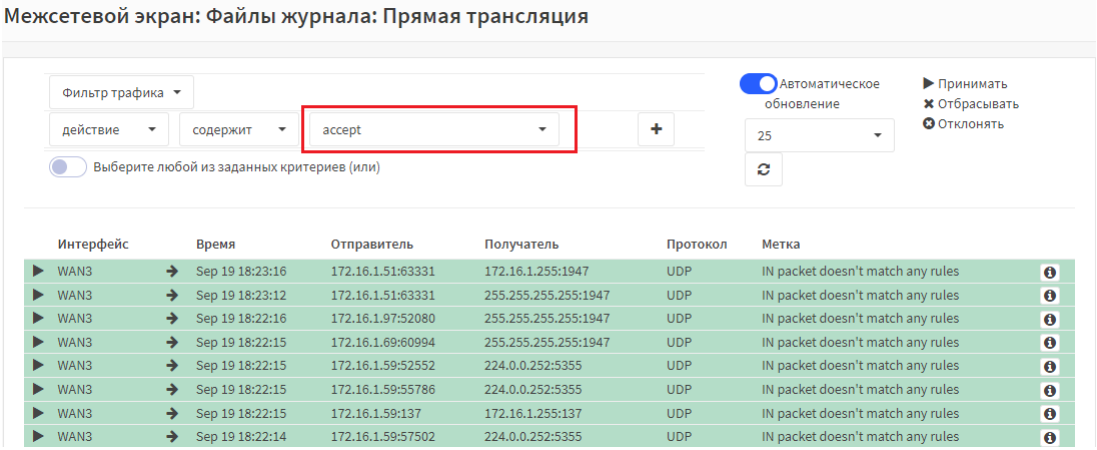


Рис. 431: Выбор параметра

Таблица 141: Выбор параметра

Параметр	Значение
Accept	Пропустить пакет
Drop	Отбросить пакет
Reject	Отбросить пакет и вернуть его отправителю

- в поле **«Выберите любой из заданных критериев (или)»** установить переключатель для выбора любого из заданных критериев.

Обзор

Раздел **«Обзор»** содержит статистические данные обработанных пакетов

Действия

На вкладке **«Действия»** находится:

- диаграмма, отражающая действия, проводимые с обработанными пакетами;
- таблица, отражающая действия, проводимые с обработанными пакетами и количественное значение действий.

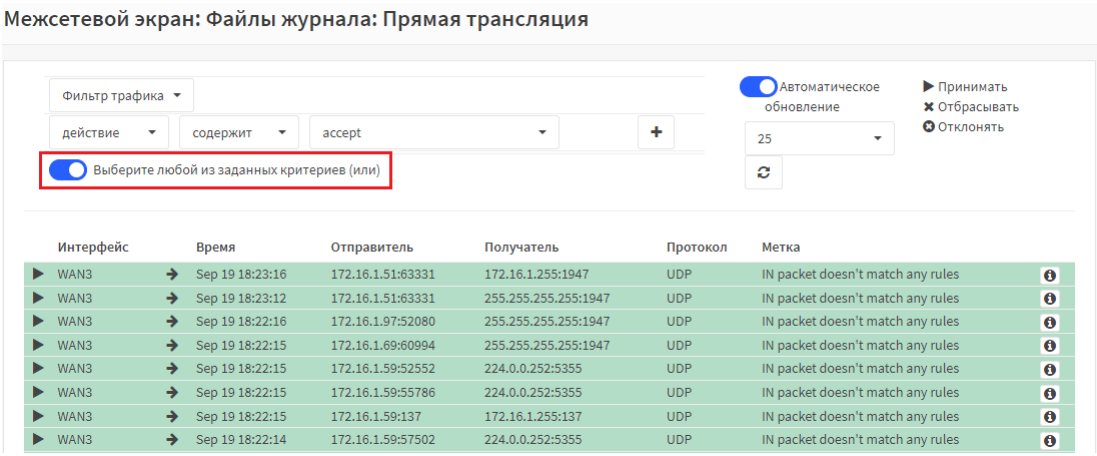


Рис. 432: Выбор критерия

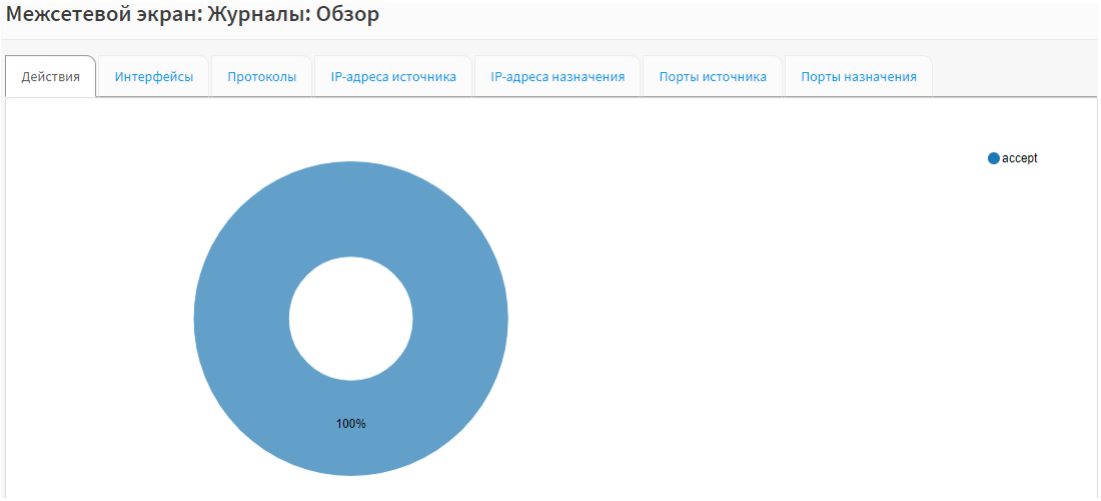


Рис. 433: Диаграмма действий

Действия	#
accept	71

Рис. 434: Таблица действий

Примечание

Разные цветовые индикаторы соответствуют разным действиям

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

Интерфейсы

На вкладке **«Интерфейсы»** находится:

- диаграмма, отражающая типы интерфейсов передачи данных;

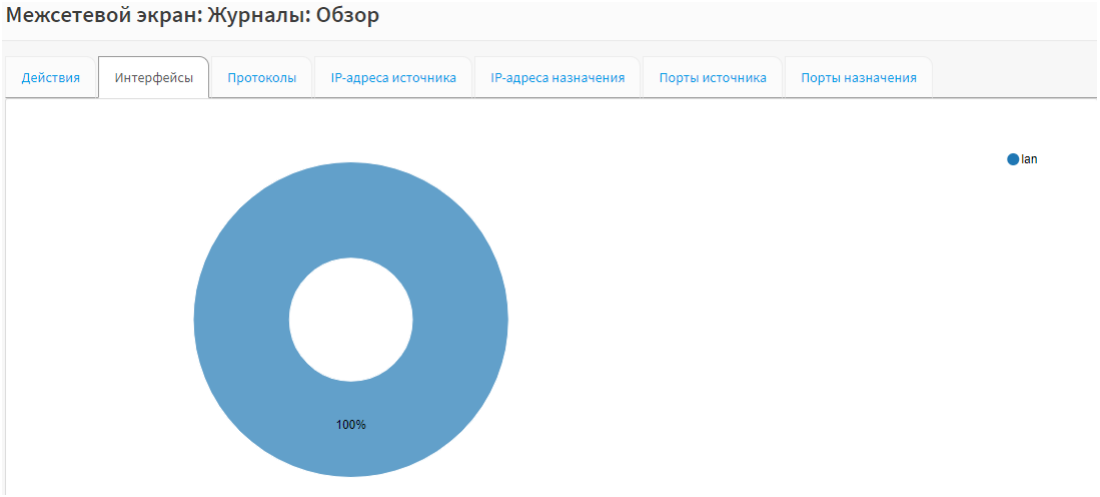


Рис. 435: Интерфейсы

- таблица, отражающая типы интерфейсов передачи данных и количественное значение интерфейсов.

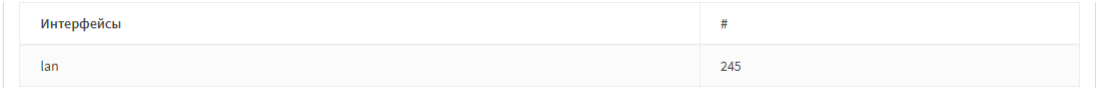


Рис. 436: Таблица интерфейсов

Примечание

Разные цветовые индикаторы соответствуют разным интерфейсам

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

Протоколы

На вкладке **«Протоколы»** находится:

- диаграмма, отражающая типы протоколов передачи данных;

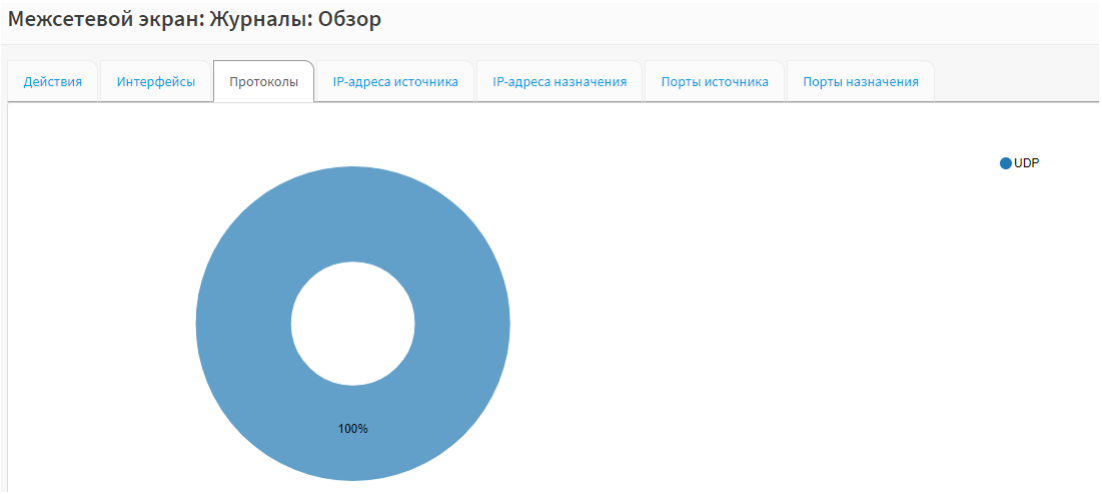


Рис. 437: Протоколы передачи данных

- таблица, отражающая типы протоколов передачи данных и количественное значение протоколов.

Протоколы	#
UDP	15

Рис. 438: Таблица протоколов

Примечание

Разные цветовые индикаторы соответствуют разным протоколам

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

IP адрес источника

На вкладке **«IP-адрес источника»** находится:

- диаграмма, отражающая IP адреса источников;

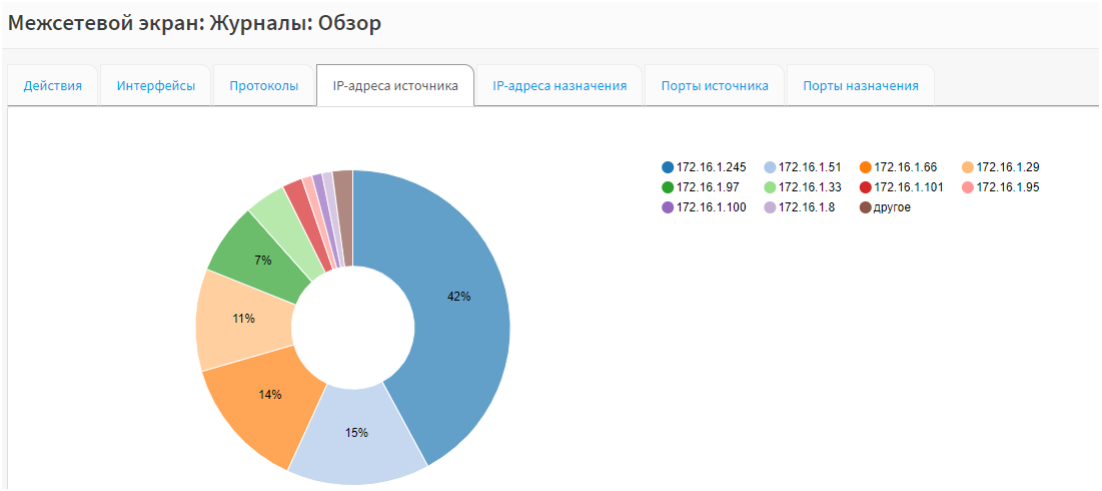


Рис. 439: IP адреса источников

- таблица, отражающая IP адреса источников и количественное значение IP адресов.

IP-адреса источника	#
172.16.1.245	40
172.16.1.51	14
172.16.1.66	13
172.16.1.29	10
172.16.1.97	7
172.16.1.33	4
172.16.1.101	2
172.16.1.95	1
172.16.1.100	1
172.16.1.8	1

Рис. 440: Таблица IP адресов

Примечание

Разные цветовые индикаторы соответствуют разным IP адресам источников

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

IP адрес назначения

На вкладке **«IP-адрес назначения»** находится:

- диаграмма, отражающая IP адреса назначения;

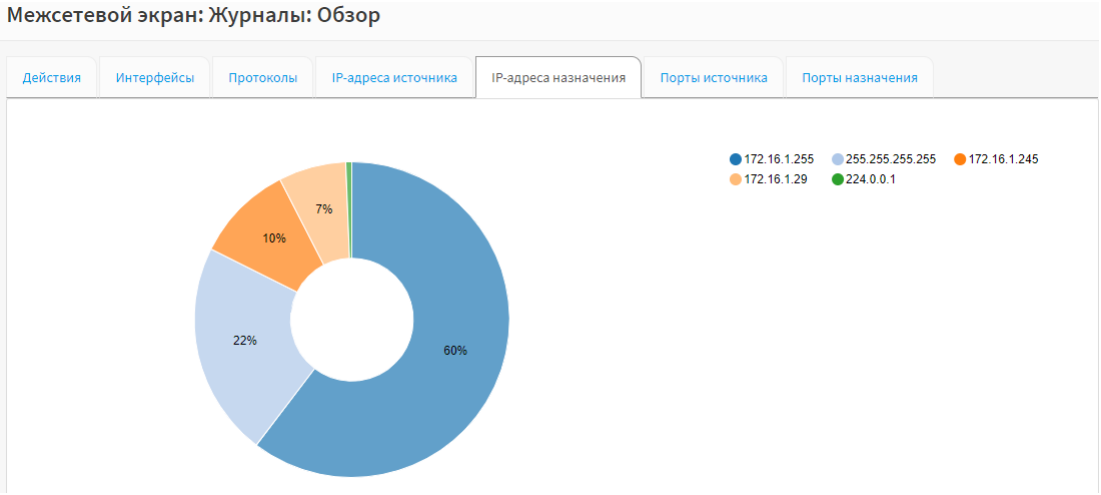


Рис. 441: IP адреса назначения

- таблица, отражающая IP адреса назначения и количественное значение IP адресов.

IP-адреса назначения	#
172.16.1.255	96
255.255.255.255	35
172.16.1.245	16
172.16.1.29	11
224.0.0.1	1

Рис. 442: Таблица IP адресов

Примечание

Разные цветовые индикаторы соответствуют разным IP адресам назначения

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

Порты источника

На вкладке **«Порты источника»** находится:

- диаграмма, отражающая порты источника;

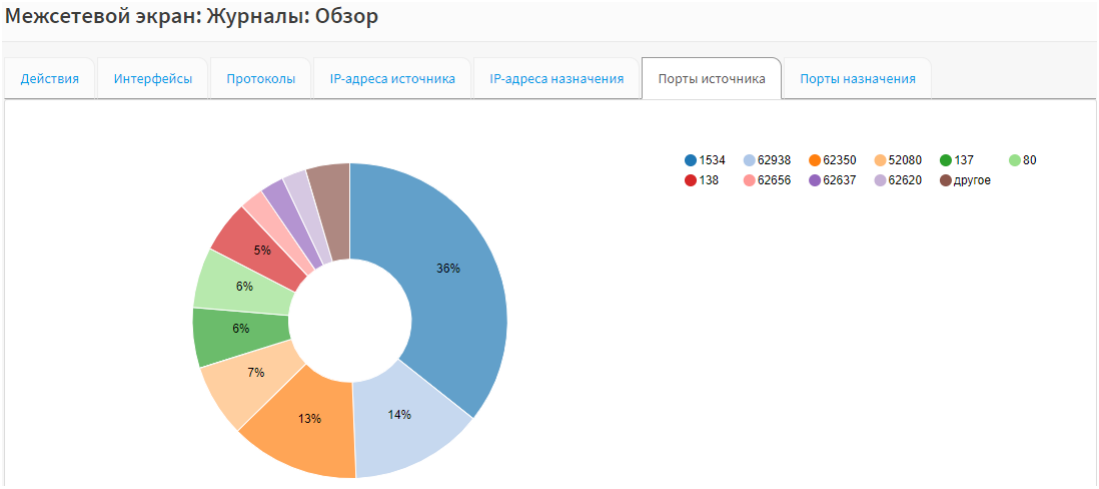


Рис. 443: Порты источника

- таблица, отражающая порты источников и количественное значение портов источника.

Порты источника	#
1534	86
62938	33
62350	32
52080	18
137	15
80	15
138	13
62656	6
62637	6
62620	6

Рис. 444: Таблица портов источника

Примечание

Разные цветовые индикаторы соответствуют разным портам источника

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

Порты назначения

На вкладке **«Порты назначения»** находится:

- диаграмма, отражающая порты назначения;

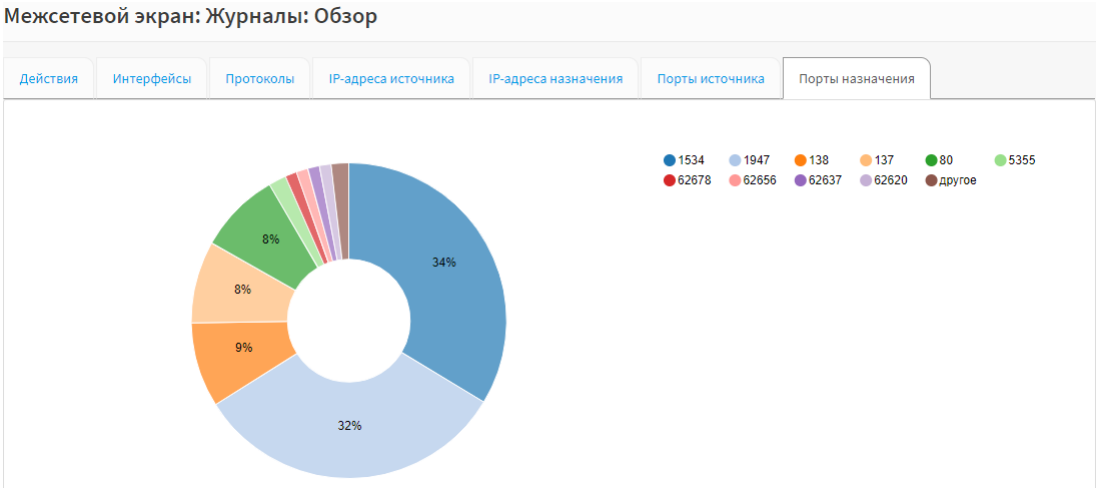


Рис. 445: Порты назначения

- таблица, отражающая порты источников и количественное значение портов назначения.

Порты назначения	#
1534	112
1947	108
138	29
137	28
80	28
5355	6
62678	4
62656	4
62637	4
62620	4

Рис. 446: Таблица портов назначения

Примечание

Разные цветовые индикаторы соответствуют разным портам назначения

Совет

При наведении курсора в область диаграммы появиться информация, аналогичная информации, присутствующей в таблице

2.7.6 Маршрутизация

Для перехода к общим настройкам необходимо:

- нажать на вкладку **«Маршрутизация» - «Общие настройки»**, расположенную в левой части списка объектов управления;

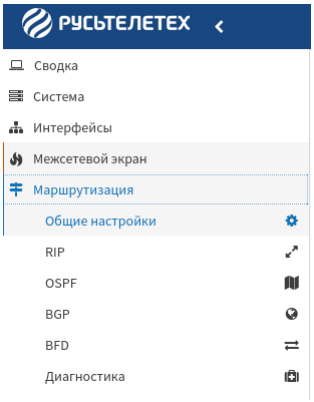


Рис. 447: Переход к общим настройкам

- в правой части экрана появиться окно общих настроек;

Рис. 448: Окно общих настроек

Для перехода к настройкам RIP необходимо:

- нажать на вкладку **«Маршрутизация» - «RIP»**, расположенную в левой части списка объектов управления;

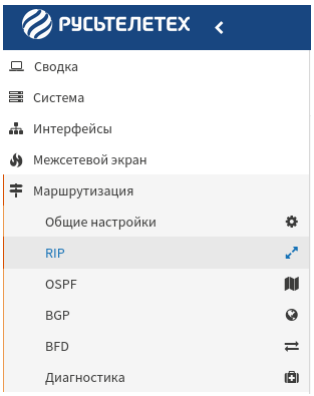


Рис. 449: Переход к настройкам RIP

- в правой части экрана появиться окно настроек RIP;

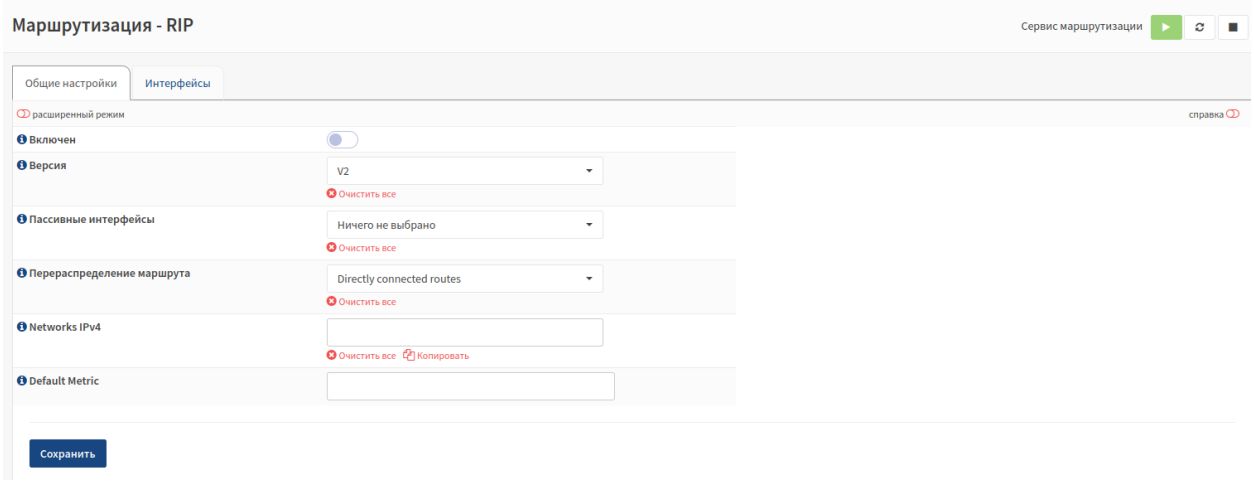


Рис. 450: Окно настроек RIP

Для перехода к настройкам OSPF необходимо:

- нажать на вкладку **«Маршрутизация»** - **«OSPF»**, расположенную в левой части списка объектов управления;

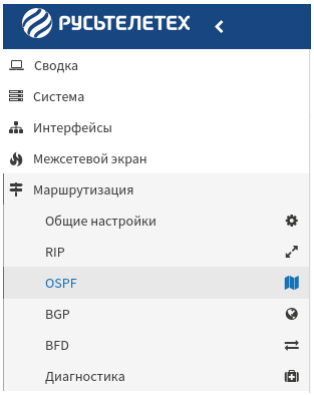


Рис. 451: Переход к настройкам OSPF

- в правой части экрана появиться окно настроек OSPF;

Для перехода к настройкам BGP необходимо:

- нажать на вкладку **«Маршрутизация»** - **«BGP»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться окно настроек BGP;

Для перехода к настройкам BFD необходимо:

- нажать на вкладку **«Маршрутизация»** - **«BFD»**, расположенную в левой части списка объектов управления;
- в правой части экрана появиться окно настроек BFD;

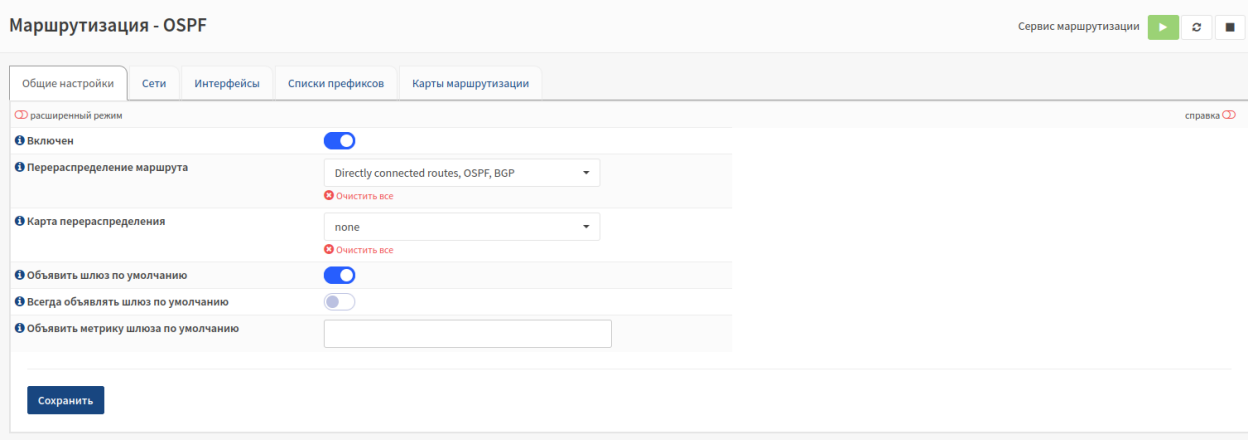


Рис. 452: Окно настроек OSPF

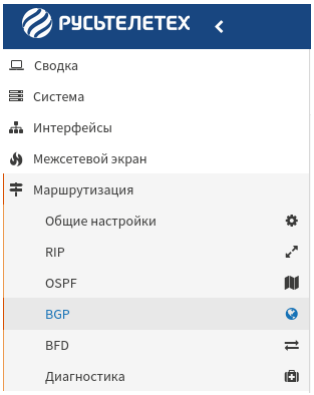


Рис. 453: Переход к настройкам BGP

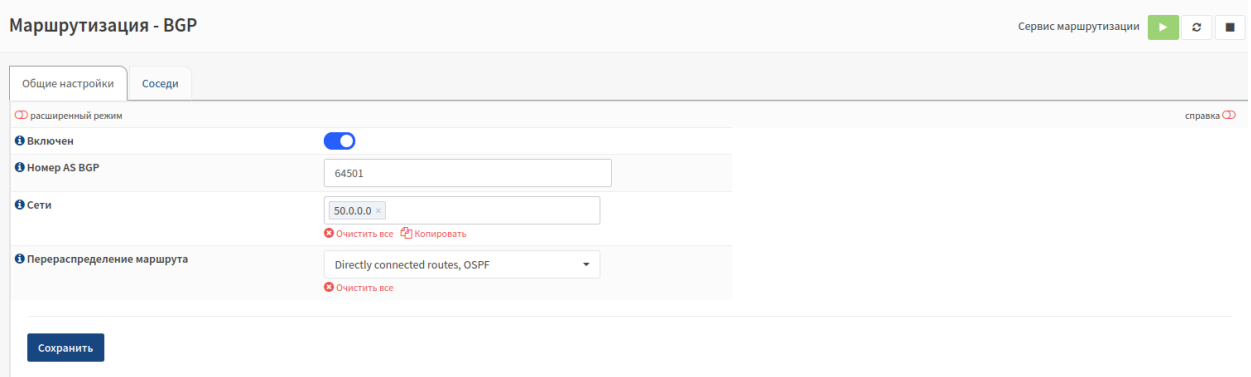


Рис. 454: Окно настроек BGP

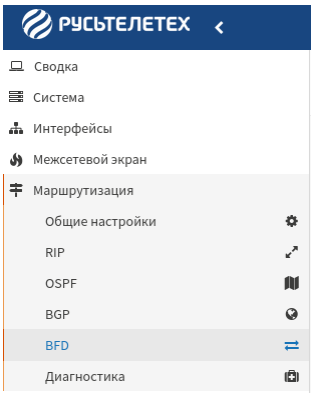


Рис. 455: Переход к настройкам BFD

Рис. 456: Окно настроек BFD

2.7.6.1 Общие настройки

Для конфигурации общих настроек необходимо:

- в поле **«Включить»** установить переключатель в случае необходимости включения подсистемы динамической маршрутизации;

Рис. 457: Включение подсистемы динамической маршрутизации

- в поле **«Включить журналирование»** установить переключатель в случае необходимости включения ведения журнала протоколов динамической маршрутизации;
- нажать кнопку 

для вступления сконфигурированных настроек в силу.

в случае необходимости включить, обновить или отключить общие настройки необходимо нажать кнопку

Рис. 458: Включение ведения журнала протоколов динамической маршрутизации

Рис. 459: Включение, обновление и отключение общих настроек

2.7.6.2 RIP

Общие настройки

Для конфигурации общих настроек сервиса RIP необходимо:

- в поле **«Включить»** установить переключатель в случае необходимости активации сервиса RIP, если протоколы маршрутизации включены в разделе **«Общие настройки»**;

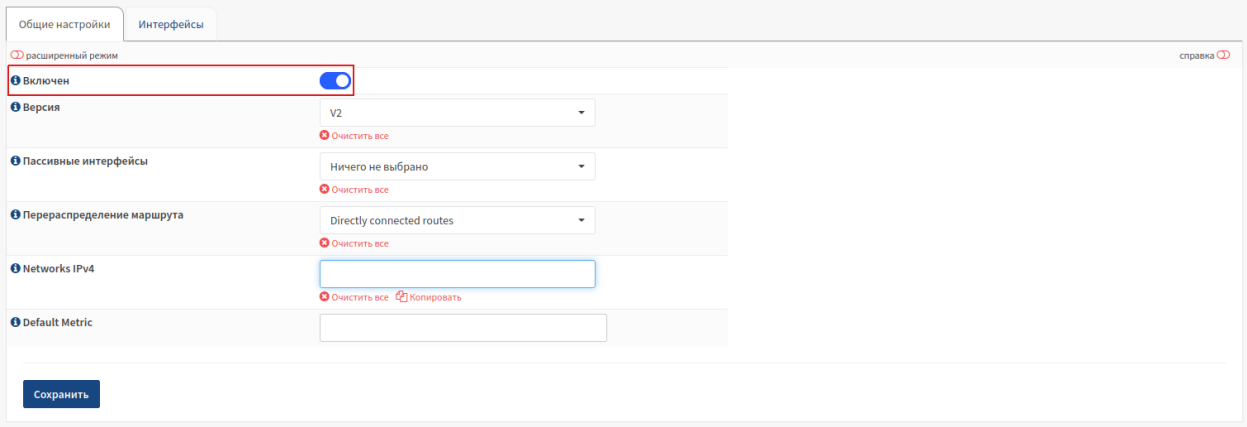


Рис. 460: Активация сервиса RIP

- в поле **«Версия»** выбрать из выпадающего списка версию сервиса RIP;

Совет

1 - классический, 2 - с поддержкой CIDR

- в поле **«Пассивные интерфейсы»** выбрать из выпадающего списка интерфейсы, куда не надо

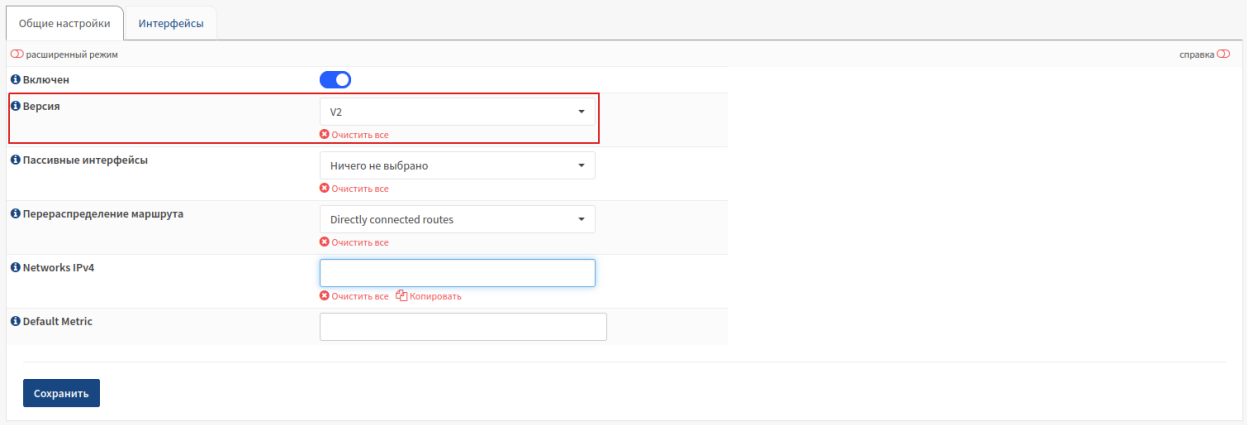


Рис. 461: Выбор версии сервиса RIP

посылать пакеты RIP;

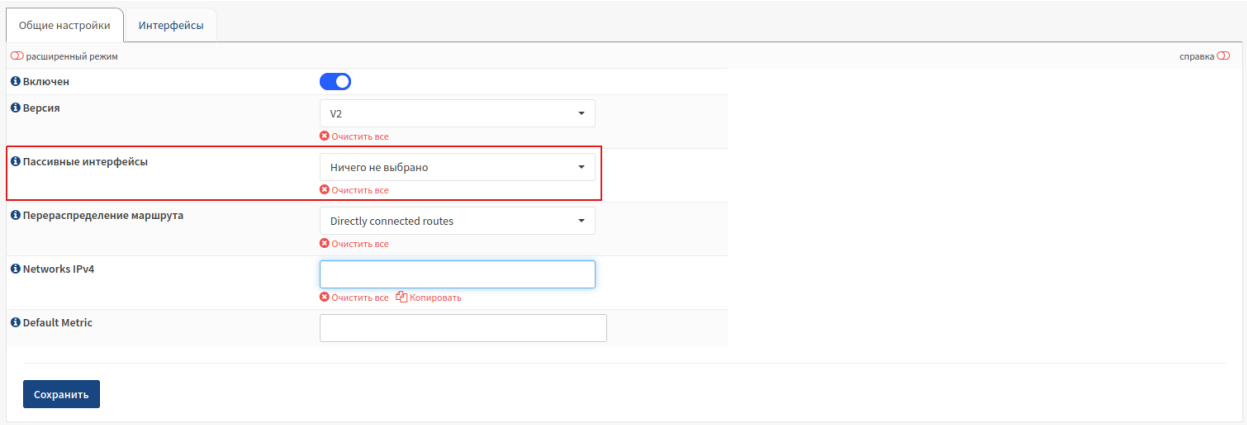


Рис. 462: Выбор пассивных интерфейсов

- в поле **«Перераспределение маршрута»** выбрать из выпадающего списка источники маршрутизации, которые должны быть переданы (перераспределены) другим узлам;
- в поле **«Networks IPv4»** ввести IPv4 сети в нотации CIDR (бесклассовой адресации);
- в поле **«Default Metric»** установить для метрики по умолчанию значение от 1 до 16;

Для включения режима расширенных настроек необходимо установить переключатель

В режиме расширенных настроек необходимо:

- в поле **«Update timer»** установить таймер обновлений маршрутной информации;

Совет

По умолчанию 30 секунд

- в поле **«Route timeout»** установить таймер хранения маршрутной информации;

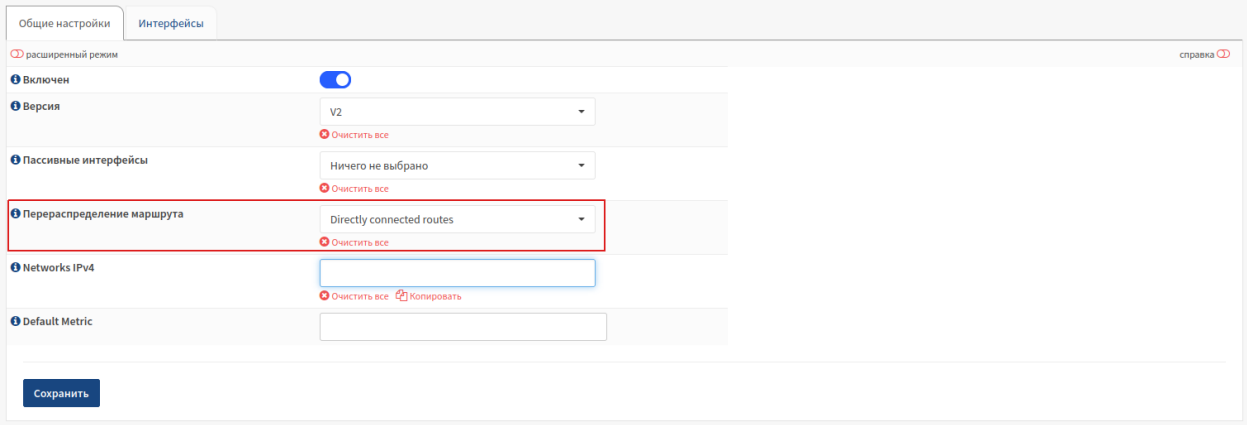


Рис. 463: Выбор источников маршрутизации

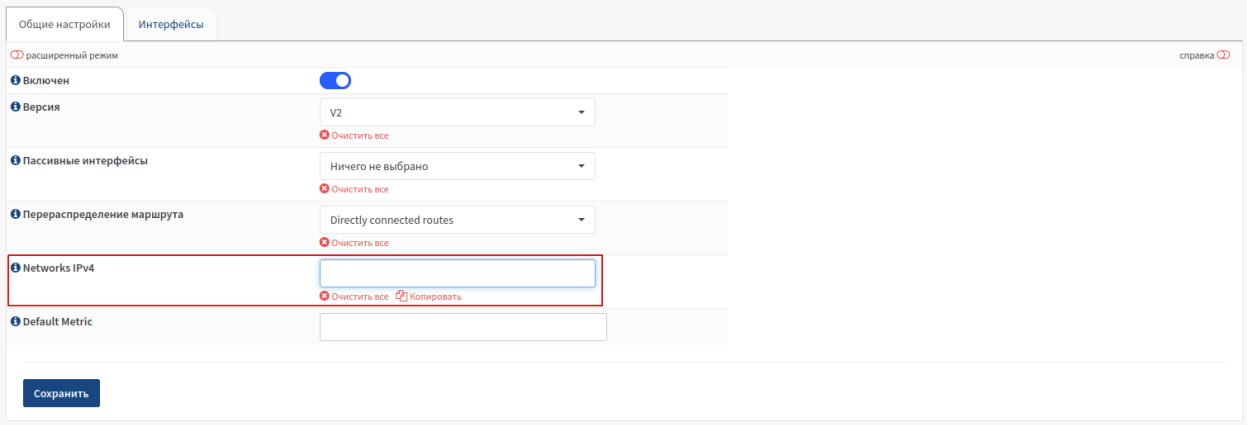


Рис. 464: Ввод IPv4

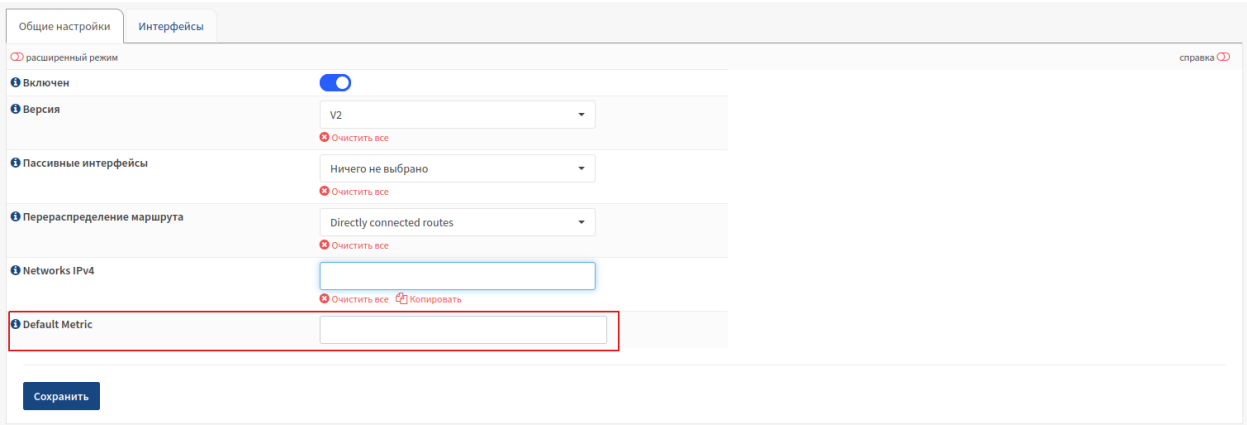


Рис. 465: Установка метрики

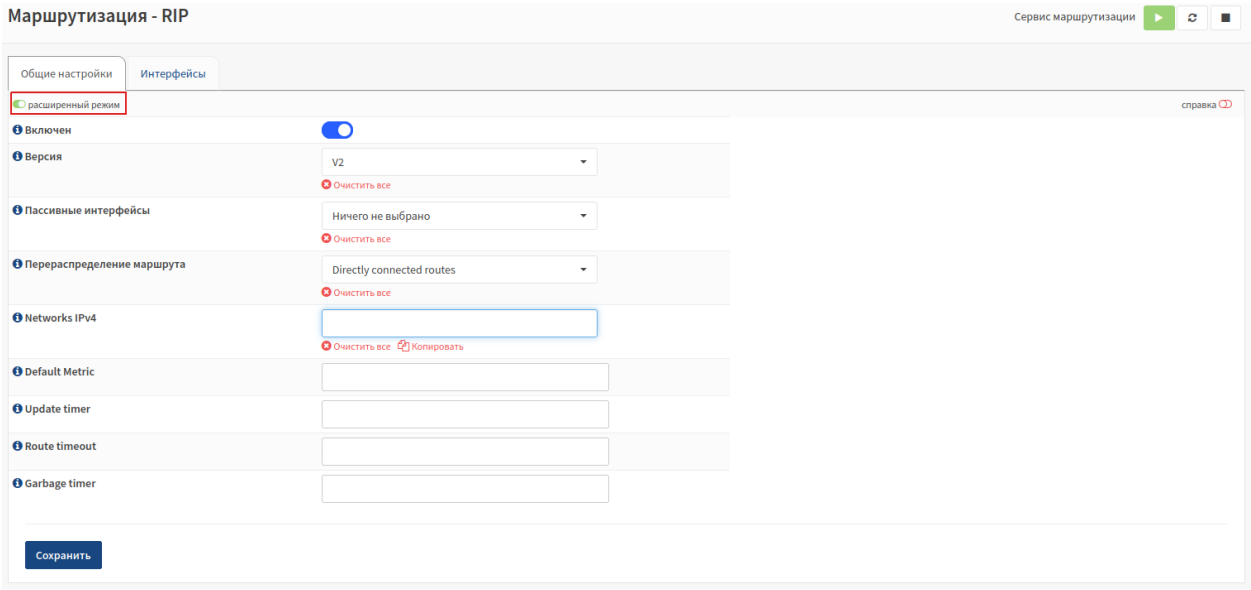


Рис. 466: Включение расширенных настроек

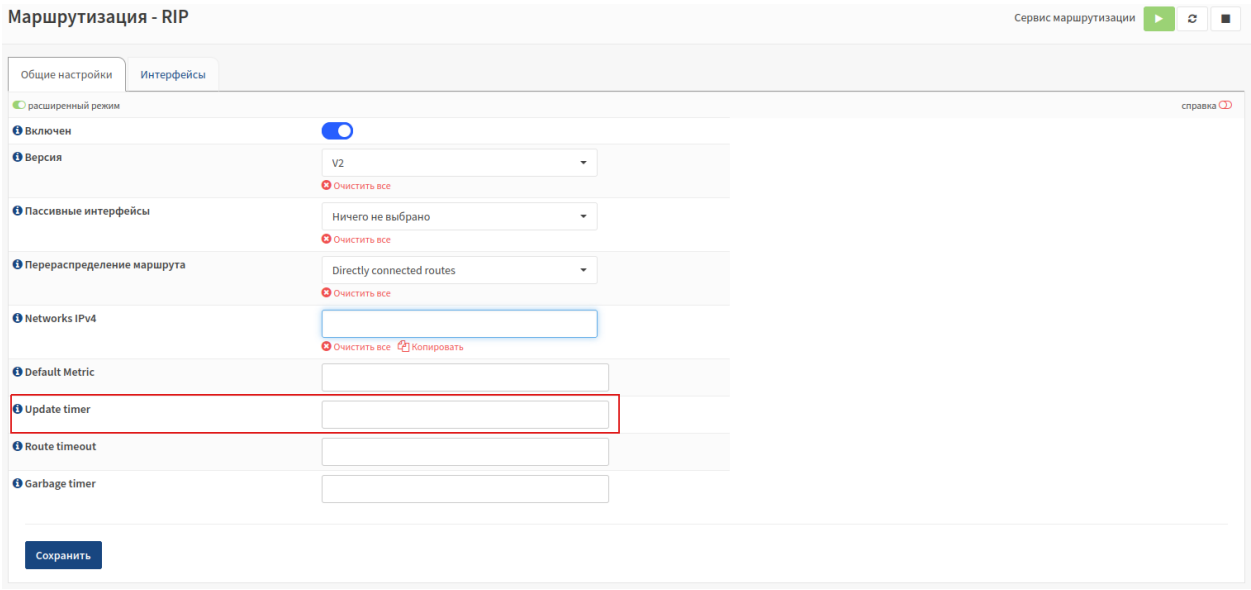


Рис. 467: Установка таймера обновлений маршрутной информации

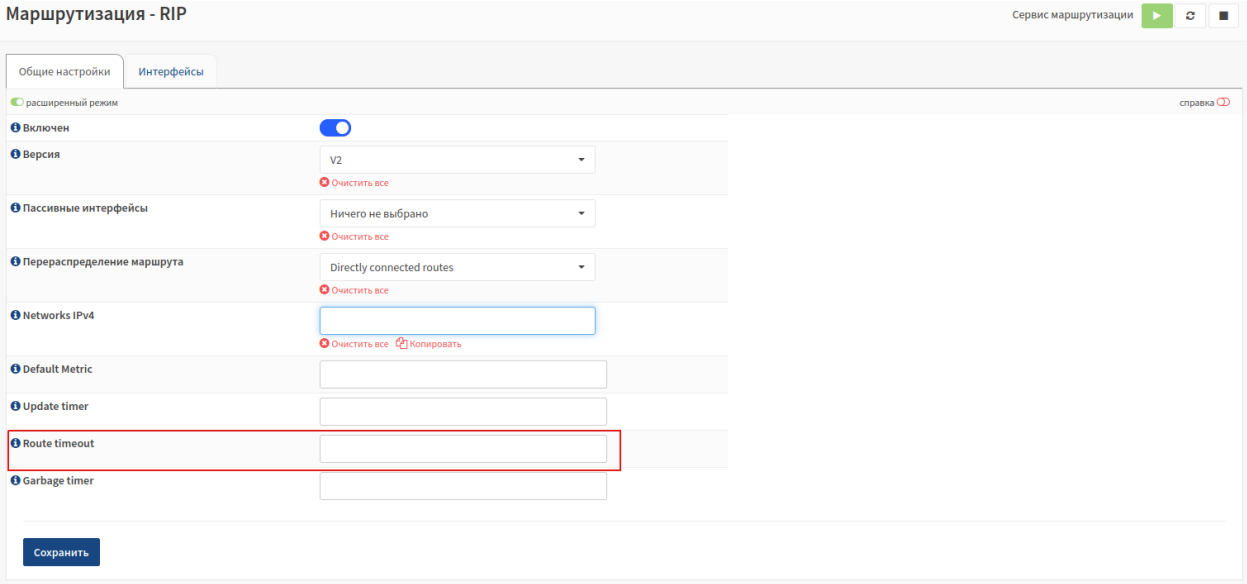


Рис. 468: Установка таймера хранения маршрутной информации

Совет

По умолчанию 180 секунд

- в поле **«Garbage timer»** установить таймер удаления устаревшей маршрутной информации;

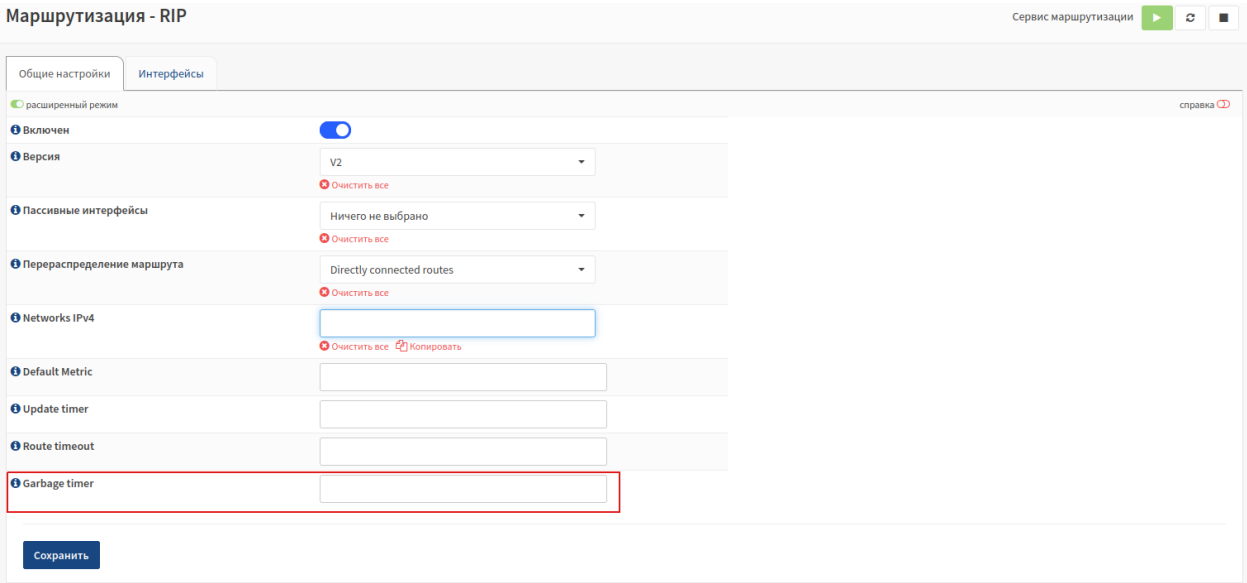


Рис. 469: Установка таймера удаления устаревшей маршрутной информации

Совет

По умолчанию 120 секунд

- нажать кнопку 

для вступления проведенных настроек в силу.

Интерфейсы

Таблица интерфейсов представлена на рисунке.

С помощью фильтров можно ограничить или расширить данные таблицы.

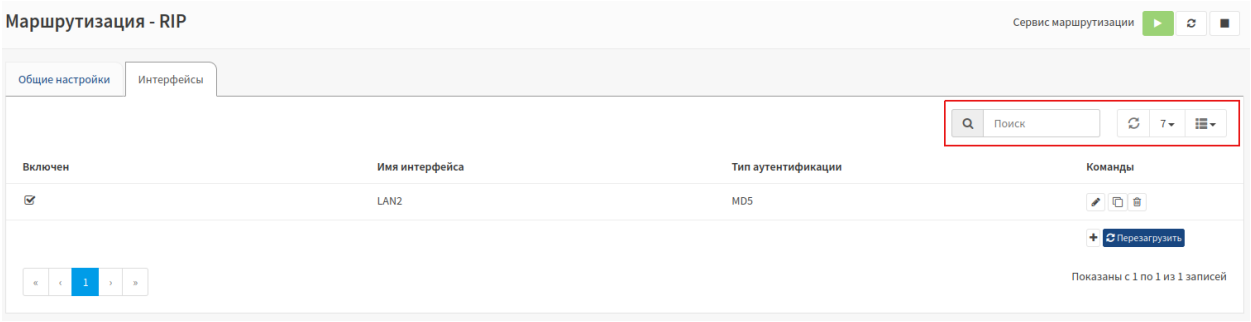


Рис. 470: Фильтры таблицы интерфейсов

Для редактирования интерфейса из таблицы необходимо нажать кнопку  , расположенную напротив необходимого интерфейса в столбце **«Команды»**.

Для обновления таблицы интерфейсов необходимо нажать кнопку 

, расположенную в правом нижнем углу таблицы.

Для добавления нового интерфейса в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации интерфейса;

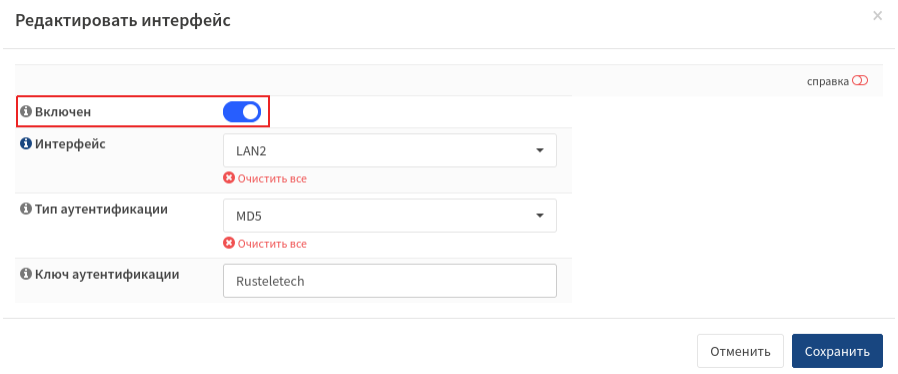


Рис. 471: Активация интерфейса

- в поле **«Интерфейс»** выбрать из выпадающего списка интерфейс, где применить эти настройки;

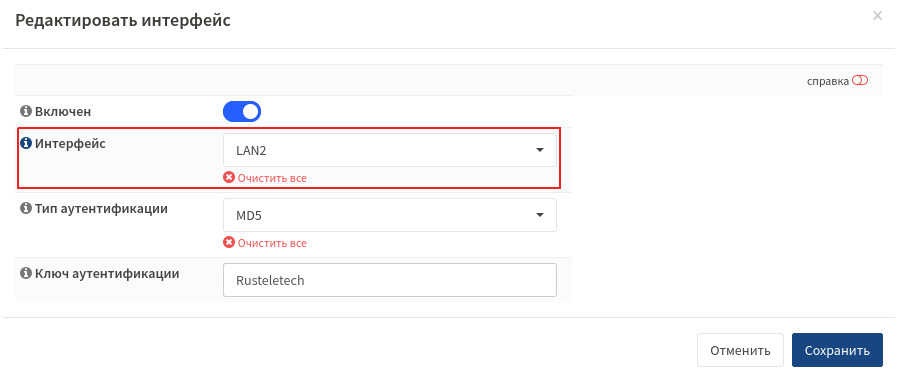


Рис. 472: Выбор интерфейса

- в поле **«Тип аутентификации»** выбрать из выпадающего списка необходимый тип аутентификации;

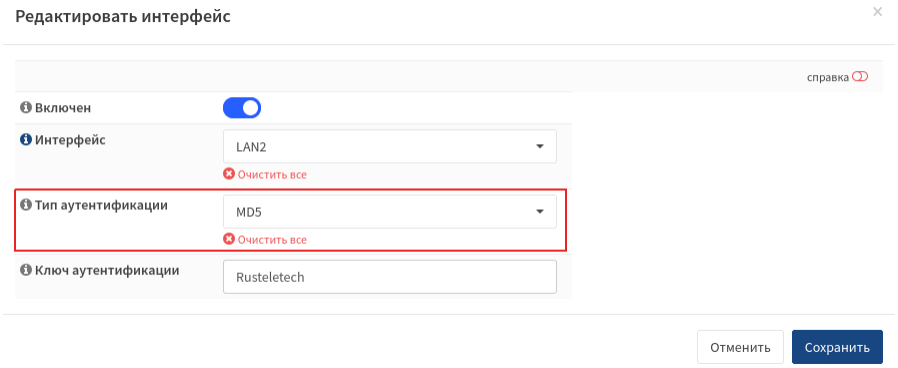


Рис. 473: Выбор типа аутентификации

- в поле **«Ключ аутентификации»** ввести ключ аутентификации;
- нажать кнопку 

для вступления проведенных настроек в силу.

2.7.6.3 OSPF

Общие настройки

Для конфигурации общих настроек сервиса OSPF необходимо:

- в поле **«Включить»** установить переключатель в случае необходимости активации сервиса OSPF, если протоколы маршрутизации включены в разделе **«Общие настройки»**;
- в поле **«Перераспределение маршрута»** выбрать из выпадающего списка источники маршрутизации, которые должны быть переданы (перераспределены) другим узлам;
- в поле **«Карта перераспределения»** выбрать из выпадающего списка карту маршрутов для редистрибуции;

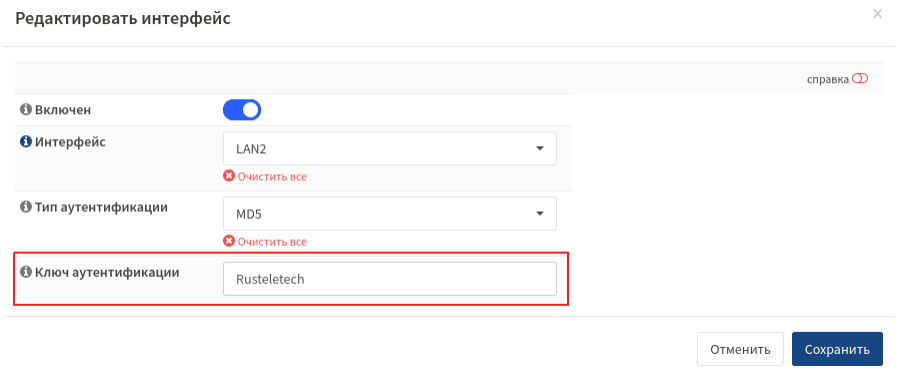


Рис. 474: Ввод ключа аутентификации

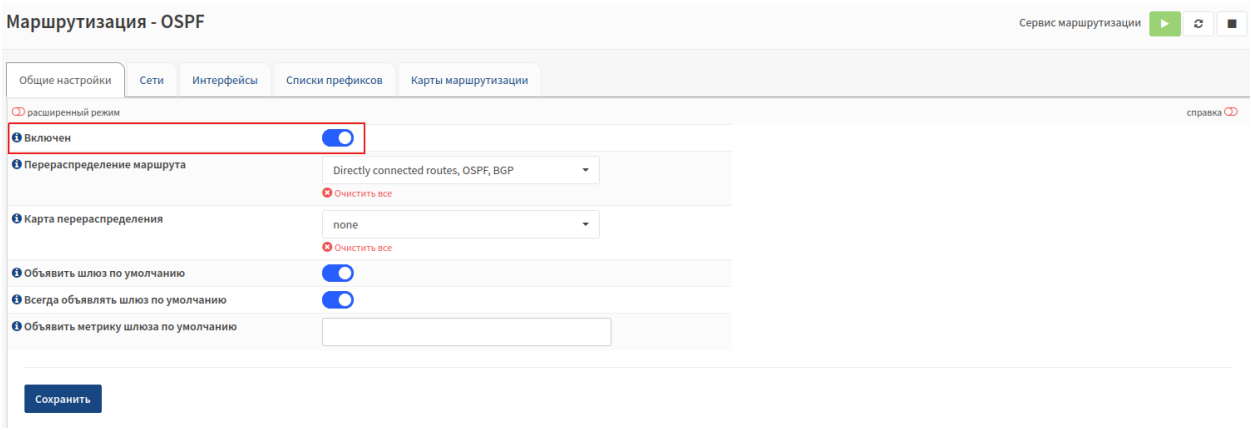


Рис. 475: Активация сервиса OSPF

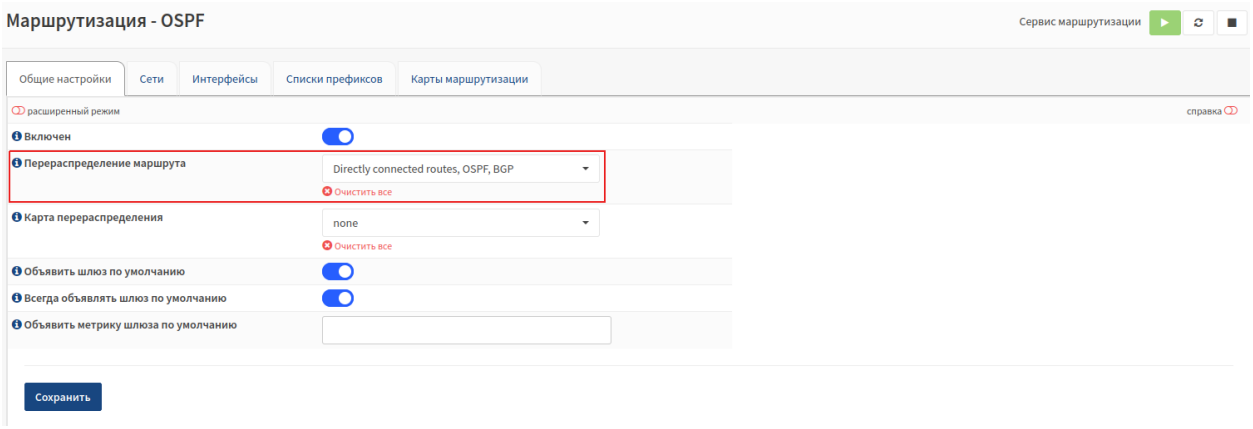


Рис. 476: Выбор источников маршрутизации

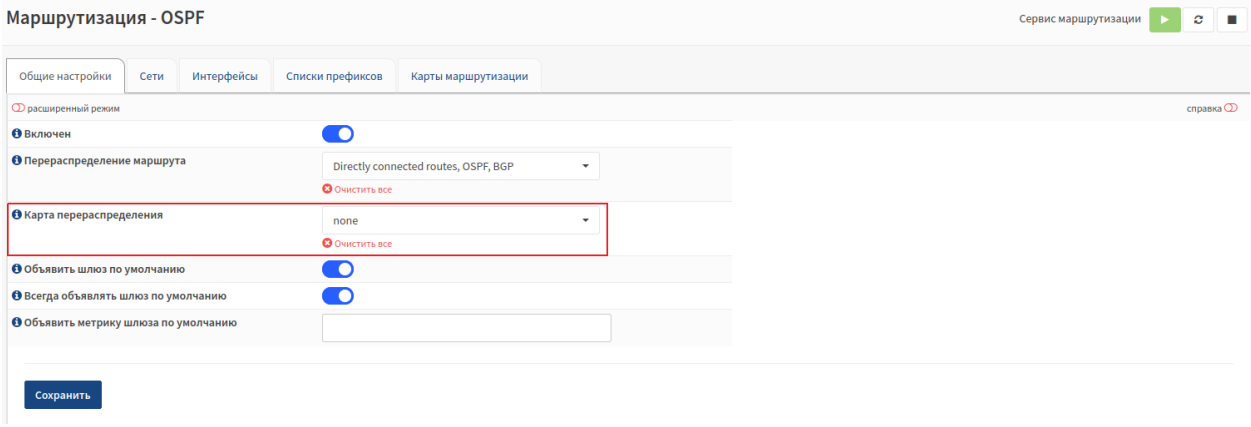


Рис. 477: Выбор карту маршрутов для редистрибуции

- в поле **«Объявить шлюз по умолчанию»** установить переключатель в случае необходимости включения передачи информации о том, что есть шлюз по умолчанию;

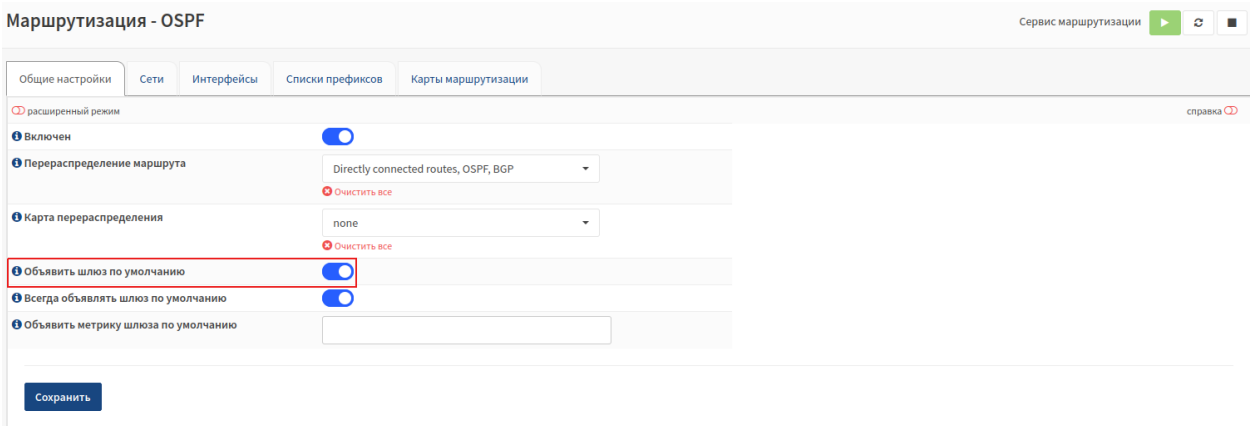


Рис. 478: Объявление шлюза по умолчанию

- в поле **«Всегда объявлять шлюз по умолчанию»** установить переключатель в случае необходимости включения передачи информации о том, что есть шлюз по умолчанию, независимо от того, доступен ли он;
- в поле **«Объявить метрику шлюза по умолчанию»** установить метрику при объявлении шлюза по умолчанию;

Для включения режима расширенных настроек необходимо установить переключатель

В режиме расширенных настроек необходимо:

- в поле **«Reference Cost»** настроить эталонную пропускную способность для расчета стоимости, которая считается эквивалентом стоимости кратчайшего пути равном 1, указанным в Мб/с;
- нажать кнопку 

для вступления проведенных настроек в силу.

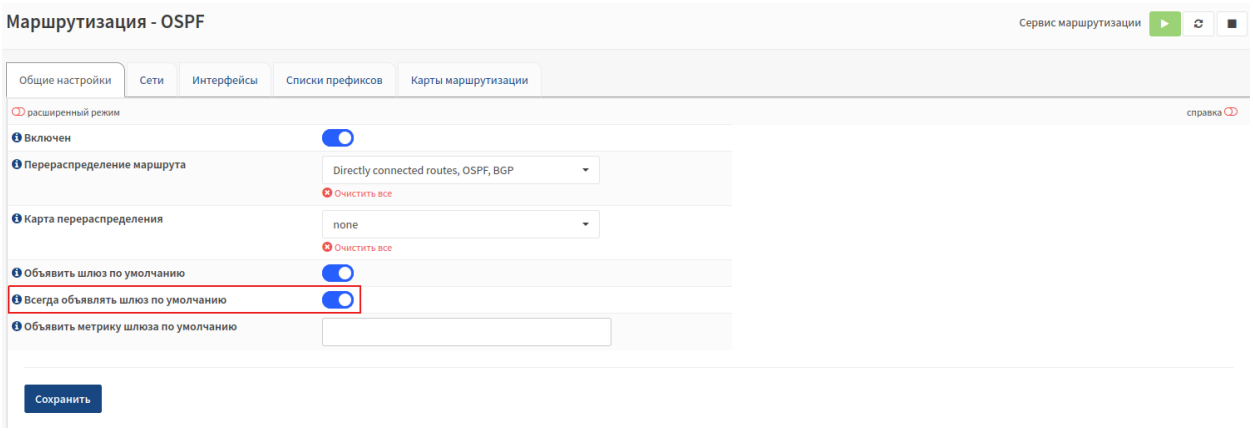


Рис. 479: Объявление шлюза по умолчанию вне зависимости от его доступности

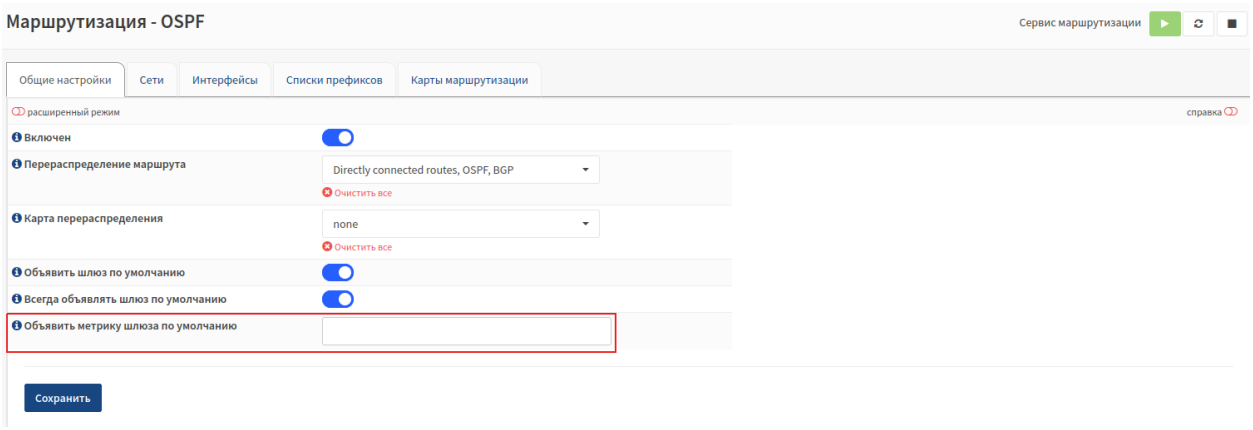


Рис. 480: Установка метрики

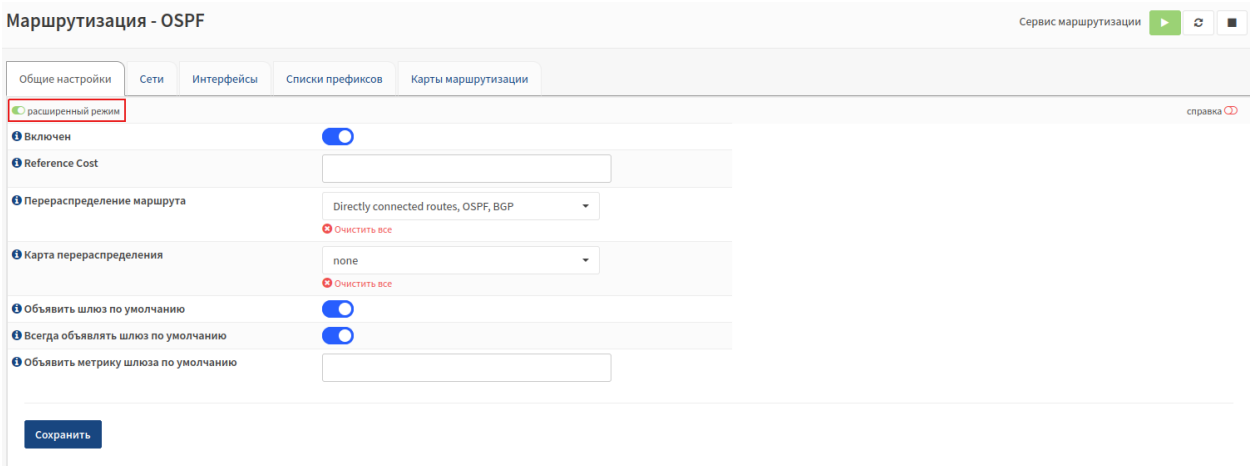


Рис. 481: Включение расширенных настроек

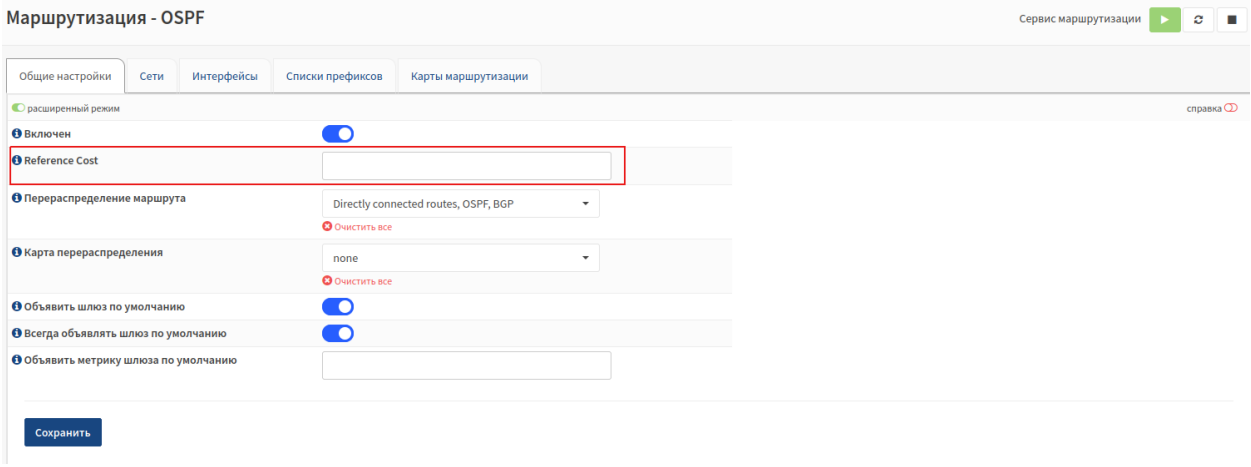


Рис. 482: Настройка эталонной пропускной способности

Сети

Таблица сетей представлена на рисунке

С помощью фильтров можно ограничить или расширить данные таблицы.

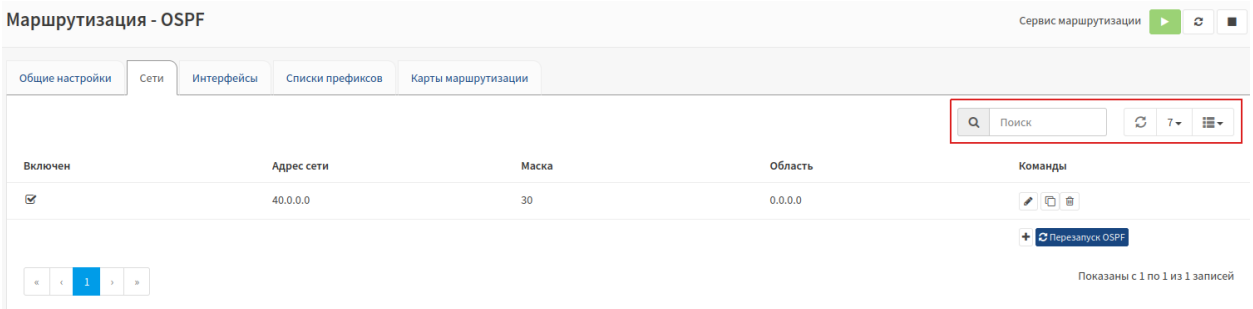


Рис. 483: Фильтры таблицы сетей

Для редактирования сети из таблицы необходимо нажать кнопку  , расположенную напротив необходимой сети в столбце **«Команды»**.

Для обновления таблицы сетей необходимо нажать кнопку 

, расположенную в правом нижнем углу таблицы.

Для добавления новой сети в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации сети;
- в поле **«Адрес сети»** установить адрес сети;
- в поле **«Маска сети»** установить маску сети;
- в поле **«Область»** указать область в виде обратной маски;

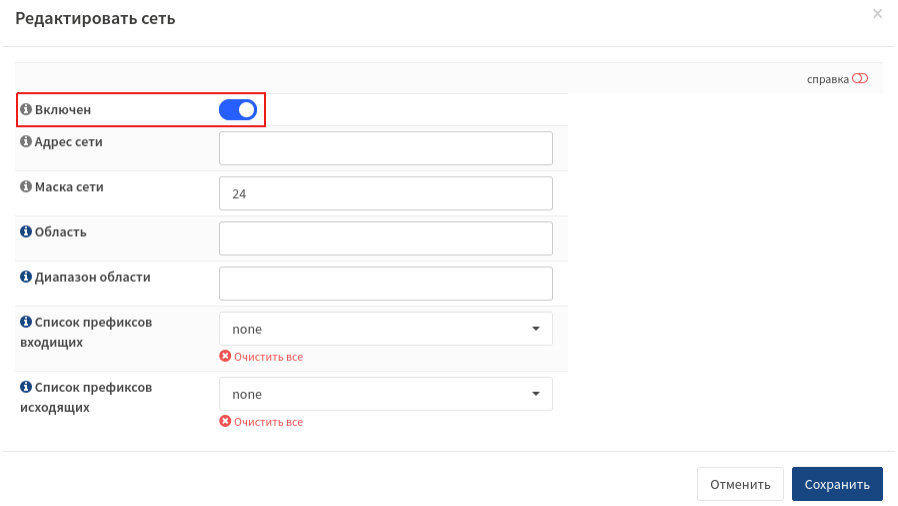


Рис. 484: Активация сети

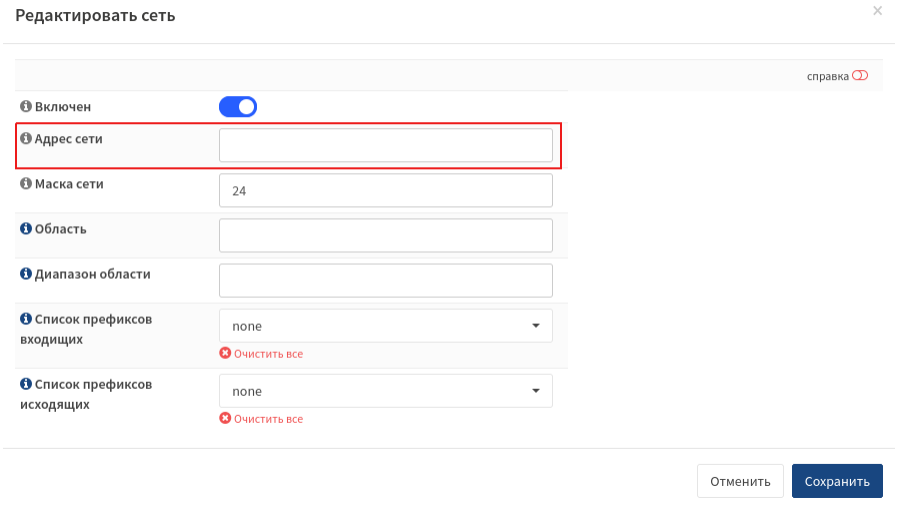


Рис. 485: Адрес сети

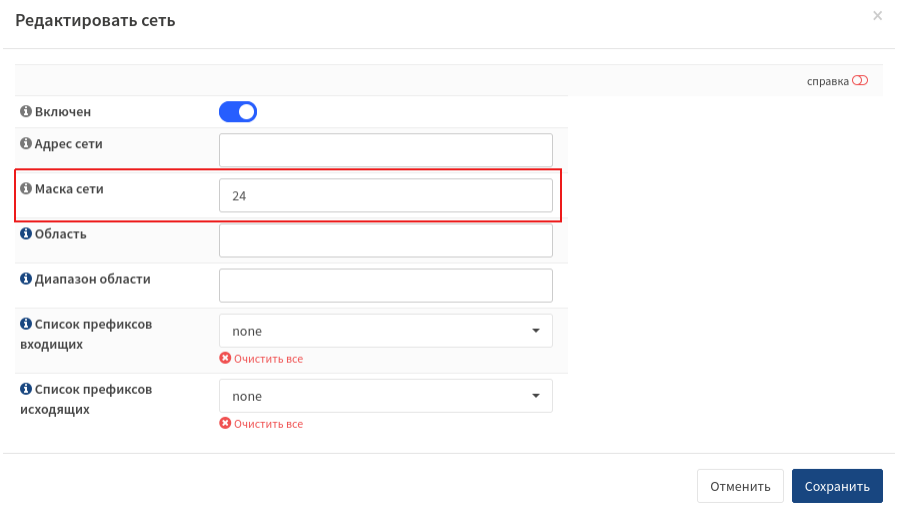


Рис. 486: Маска сети

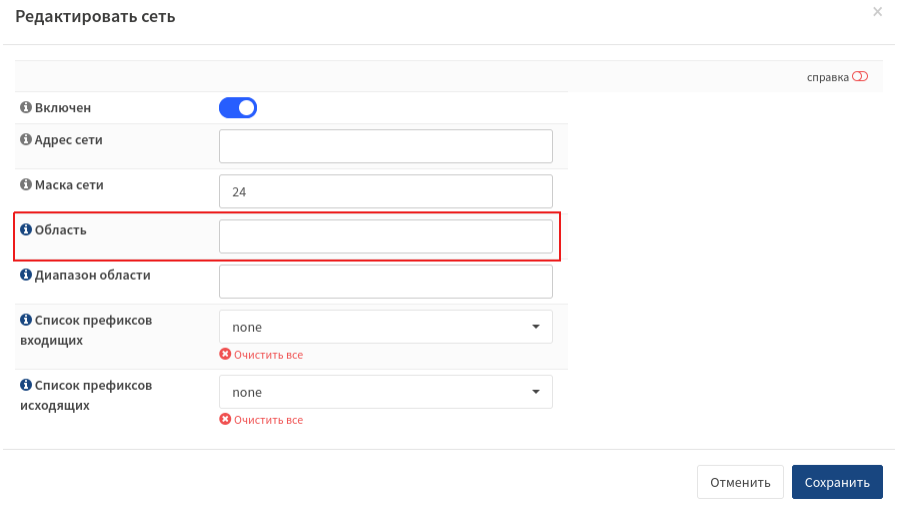


Рис. 487: Установка области

Совет

Например, 0.0.0.1

Важно

Не дублируйте **«Область»** во вкладках **«Интерфейс»** или **«Сеть»**

- в поле **«Диапазон области»** указать диапазон области для суммирования сеть для этой области в виде обратной маски;

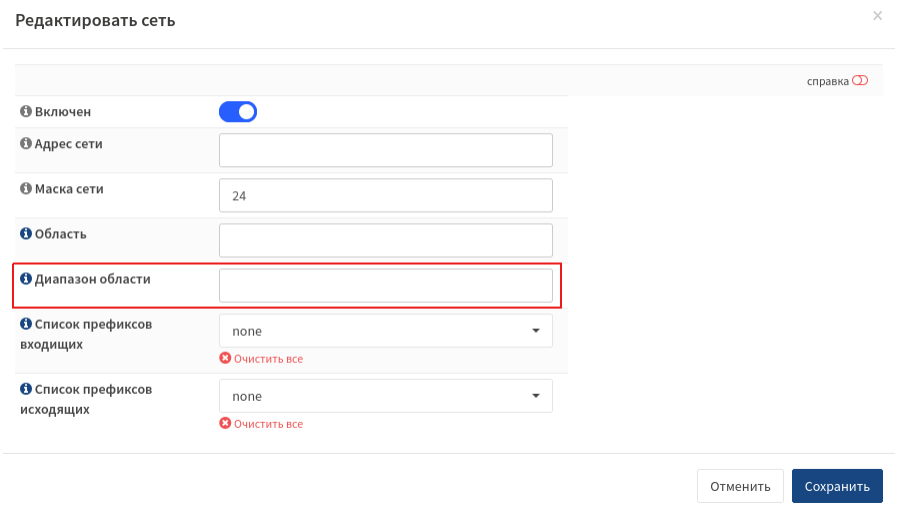


Рис. 488: Установка диапазона области

Совет

Например, 192.168.0.0/23

- в поле **«Список префиксов входящих»** выбрать из выпадающего списка список префиксов для входящего направления;
- в поле **«Список префиксов исходящих»** выбрать из выпадающего списка список префиксов для исходящего направления;
- нажать кнопку 

для вступления проведенных настроек в силу.

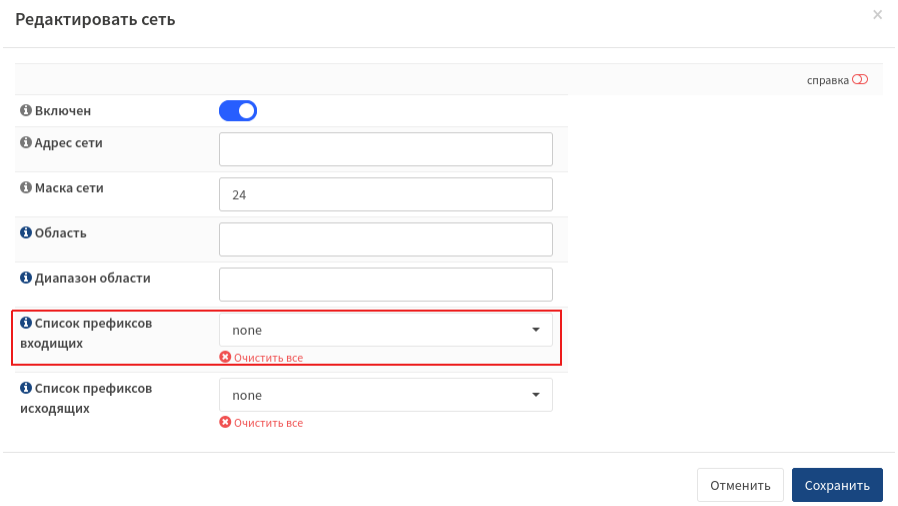


Рис. 489: Выбор списка префиксов для входящего направления

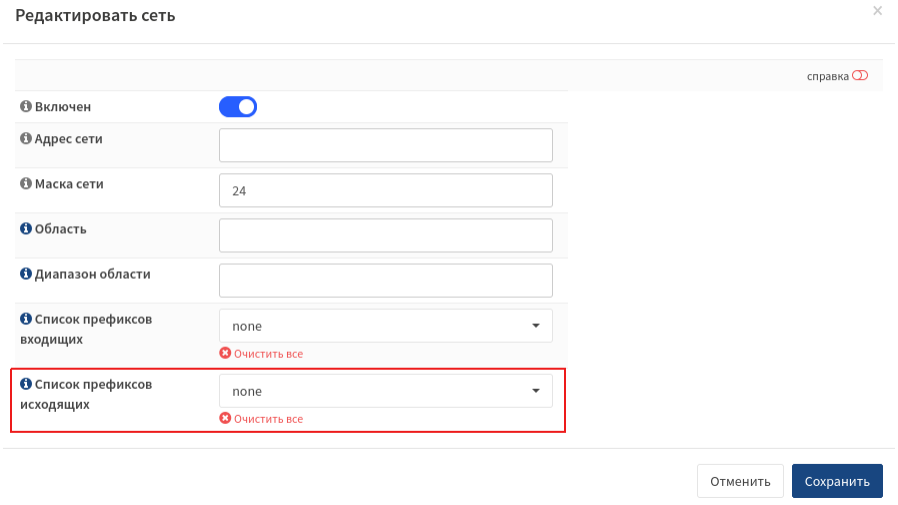


Рис. 490: Выбор списка префиксов для исходящего направления

Интерфейсы

Таблица интерфейсов представлена на рисунке.

С помощью фильтров можно ограничить или расширить данные таблицы.

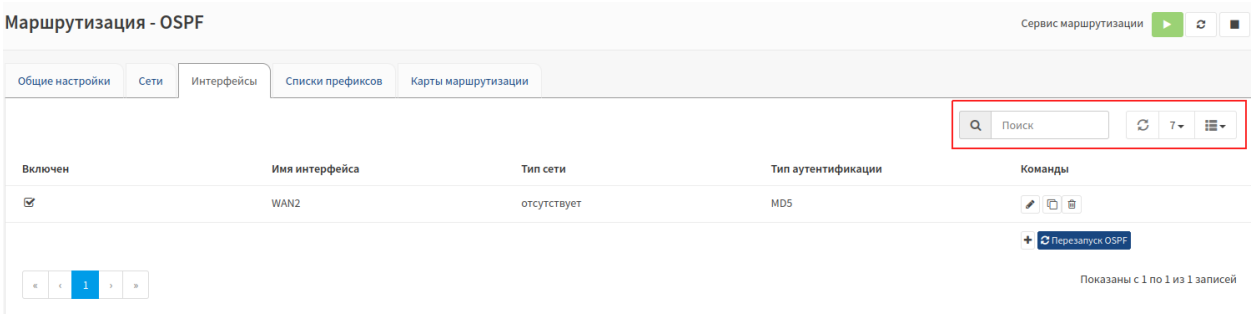


Рис. 491: Фильтры таблицы интерфейсов

Для редактирования интерфейса из таблицы необходимо нажать кнопку  , расположенную напротив необходимого интерфейса в столбце **«Команды»**.

Для обновления таблицы интерфейсов необходимо нажать кнопку 

, расположенную в правом нижнем углу таблицы.

Для добавления нового интерфейса в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации интерфейса;
- в поле **«Passive»** установить переключатель в случае необходимости случая, когда пассивные интерфейсы не будут производить обмен маршрутной информацией;
- в поле **«Интерфейс»** выбрать из выпадающего списка интерфейс, где применить эти настройки;
- в поле **«Тип аутентификации»** выбрать из выпадающего списка необходимый тип аутентификации;
- в поле **«Ключ аутентификации»** ввести ключ аутентификации;
- в поле **«Область»** указать область в виде обратной маски;

Совет

Например, 0.0.0.1

Важно

Не дублируйте **«Область»** во вкладках **«Интерфейс»** или **«Сеть»**

- в поле **«Стоимость»** указать стоимость;

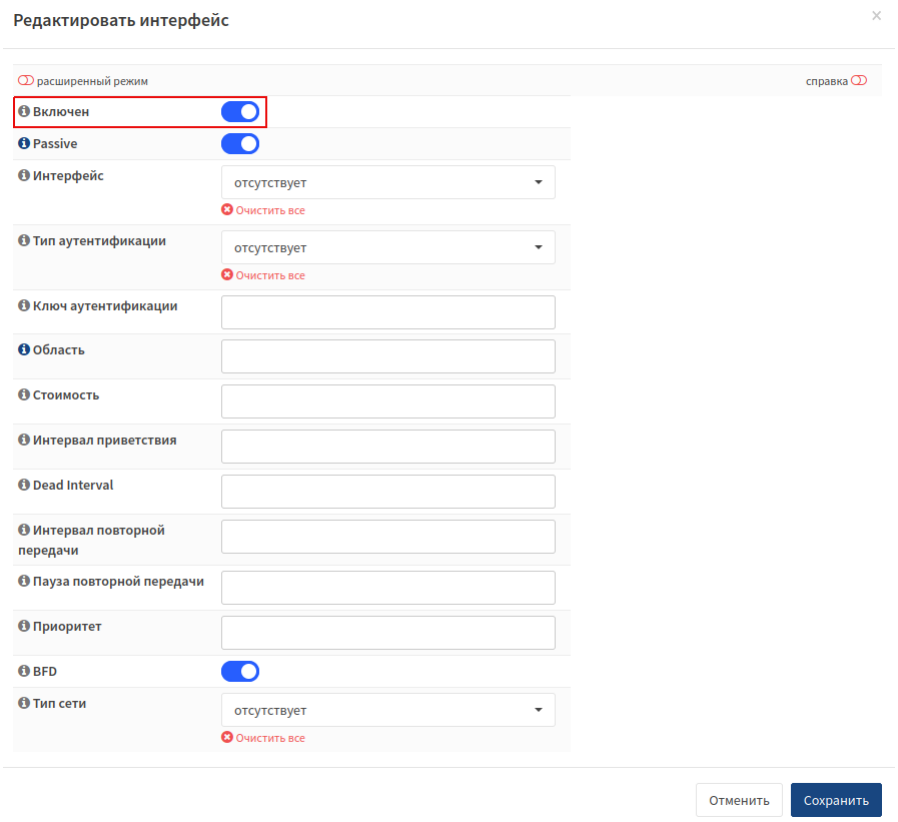


Рис. 492: Активация интерфейса

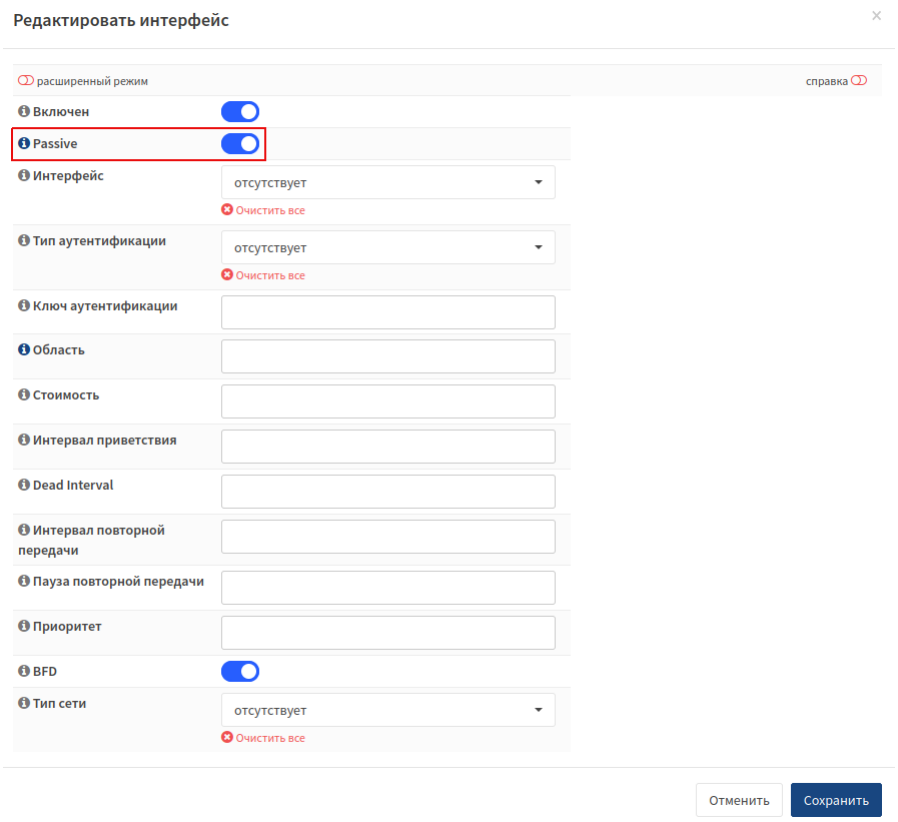


Рис. 493: Активация функции Passive

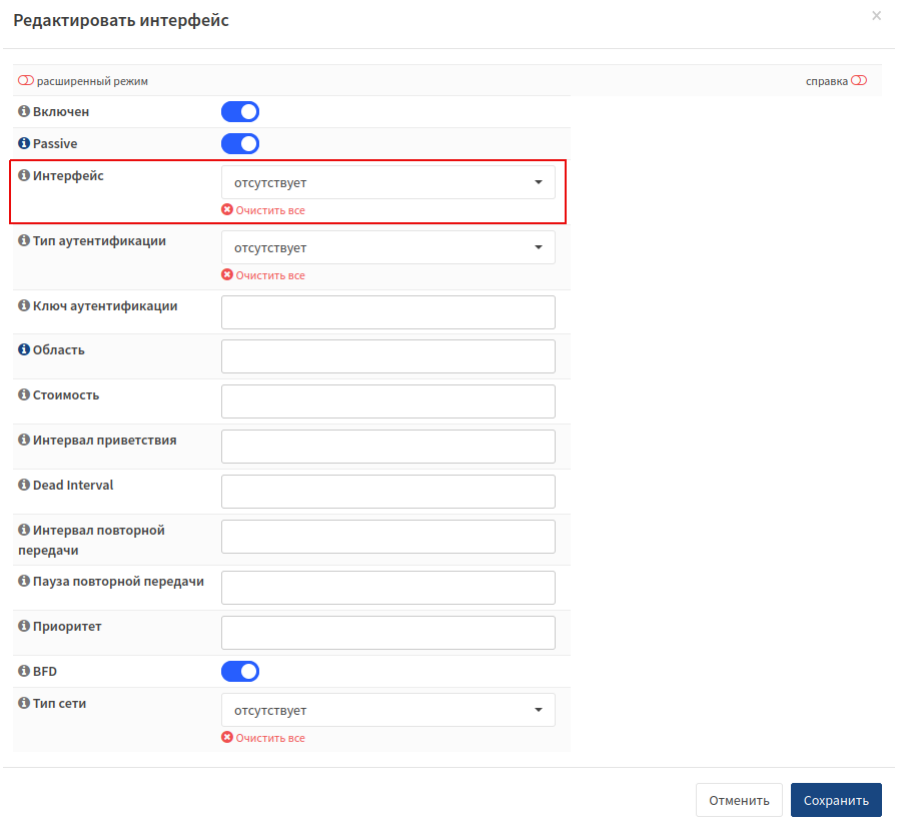


Рис. 494: Выбор интерфейса

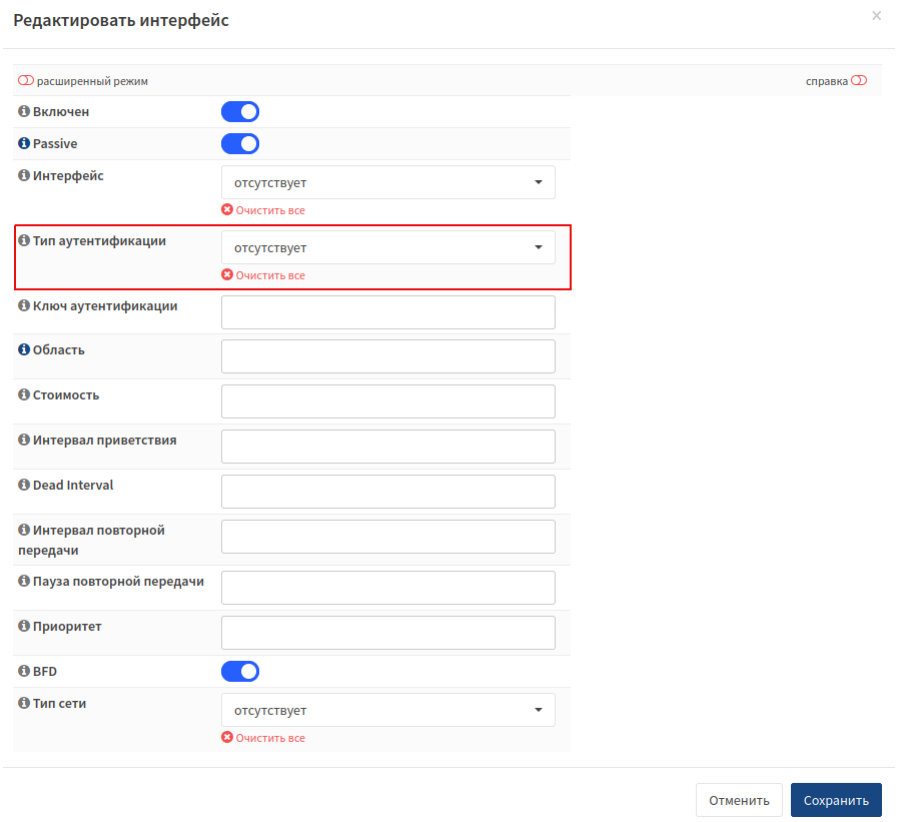


Рис. 495: Выбор типа аутентификации

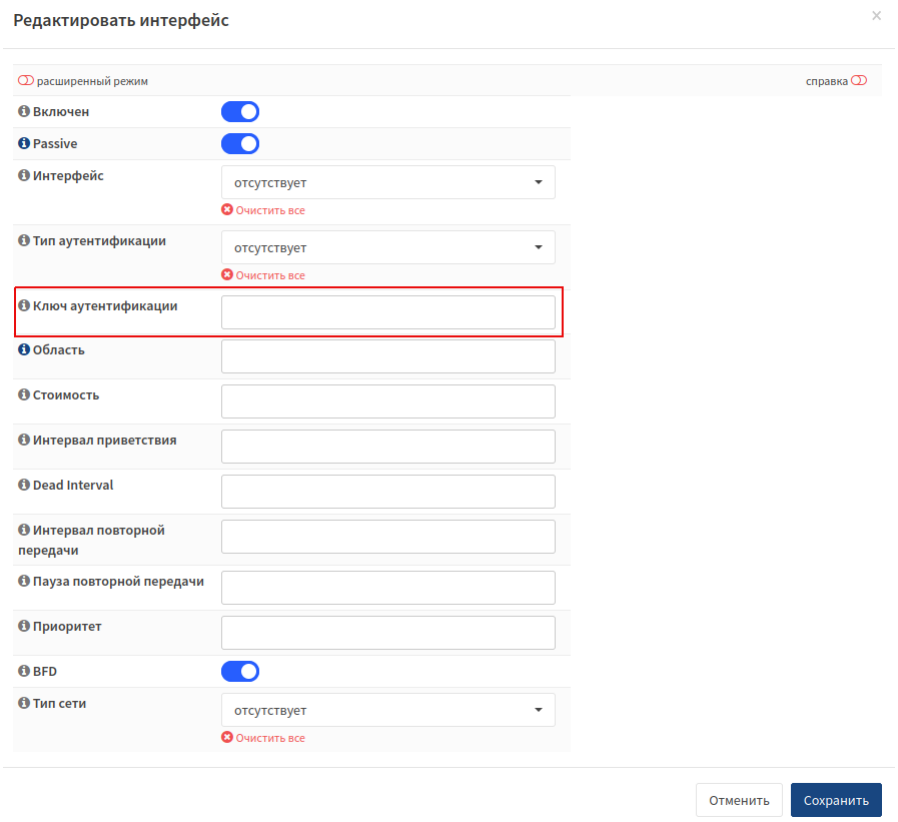


Рис. 496: Ввод ключа аутентификации

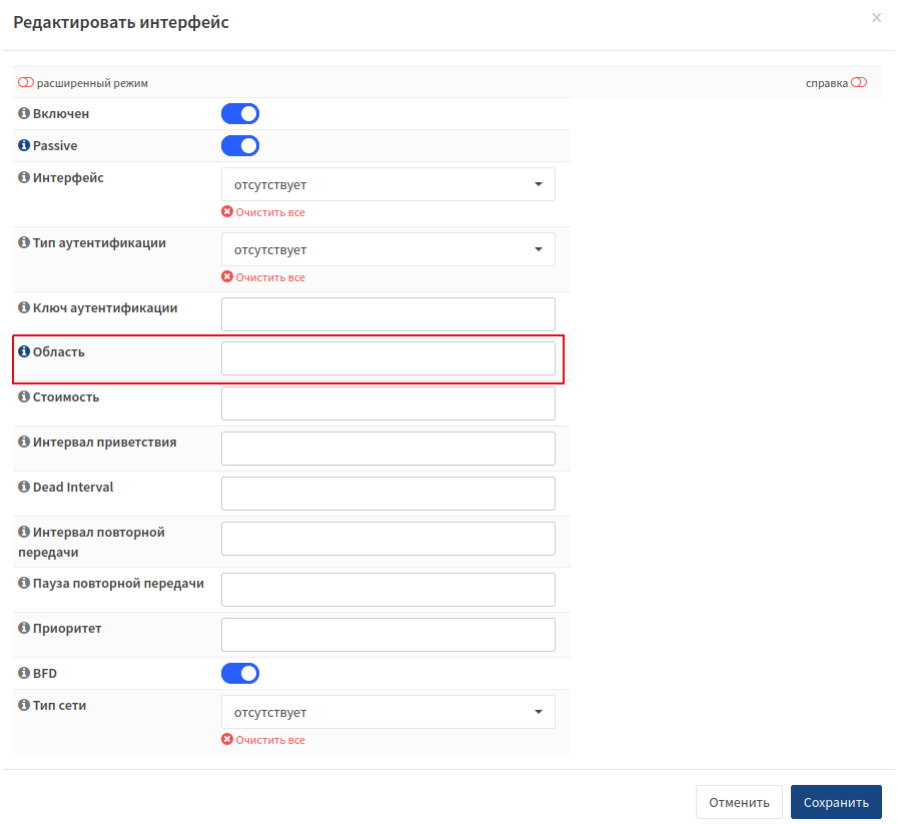


Рис. 497: Установка области

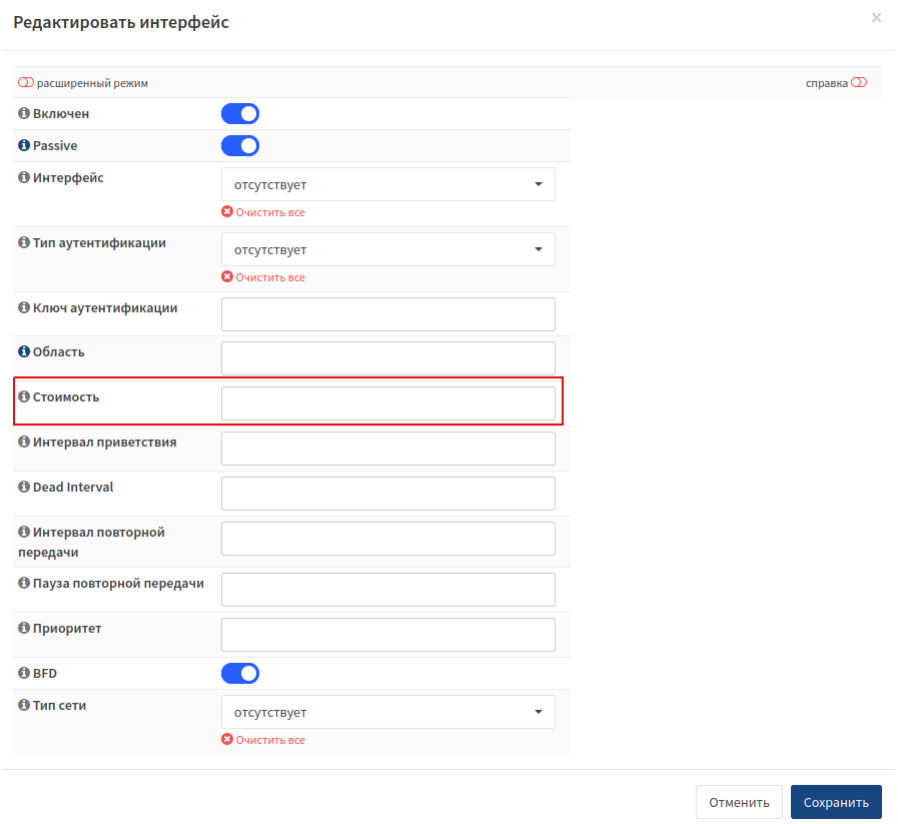


Рис. 498: Установка стоимости

- в поле **«Интервал приветствия»** указать интервал приветствия;

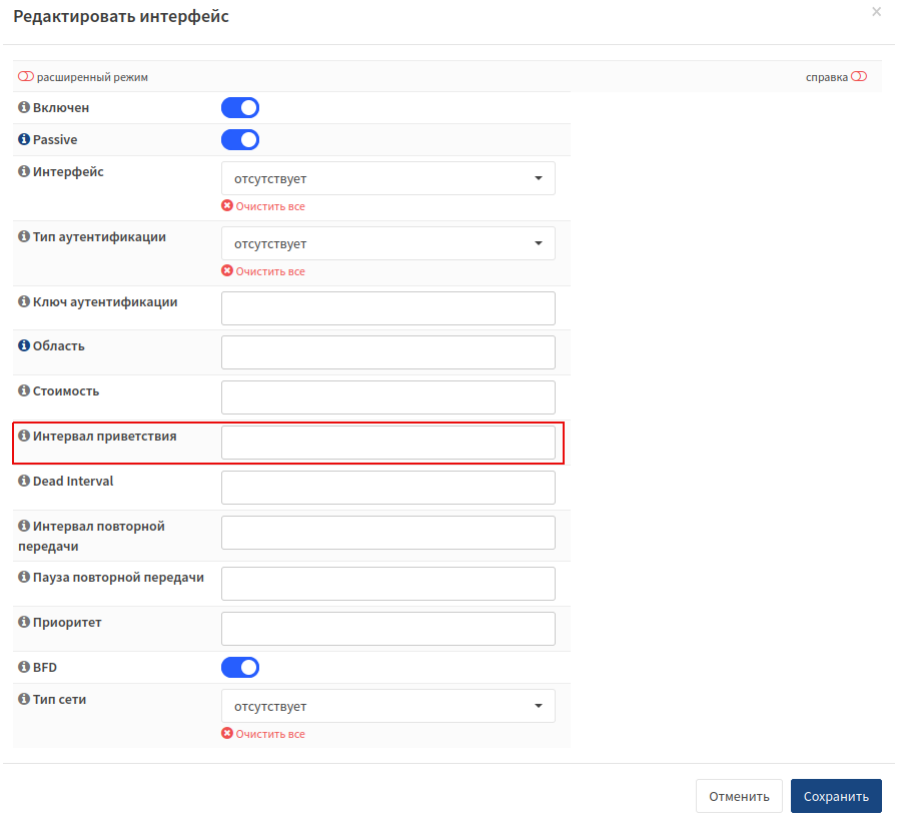


Рис. 499: Установка интервала приветствия

- в поле **«Dead Interval»** указать Dead Interval;
- в поле **«Интервал повторной передачи»** установить интервал повторной передачи;
- в поле **«Пауза повторной передачи»** установить паузу повторной передачи;
- в поле **«Приоритет»** указать приоритет;
- в поле **«Passive»** установить переключатель в случае необходимости активации сервиса BFD;
- в поле **«Тип сети»** выбрать из выпадающего списка необходимый тип сети;

Для включения режима расширенных настроек необходимо установить переключатель

В режиме расширенных настроек необходимо:

- в поле **«Идентификатор ключа аутентификации»** указать идентификатор ключа аутентификации
- нажать кнопку 

для вступления проведенных настроек в силу.

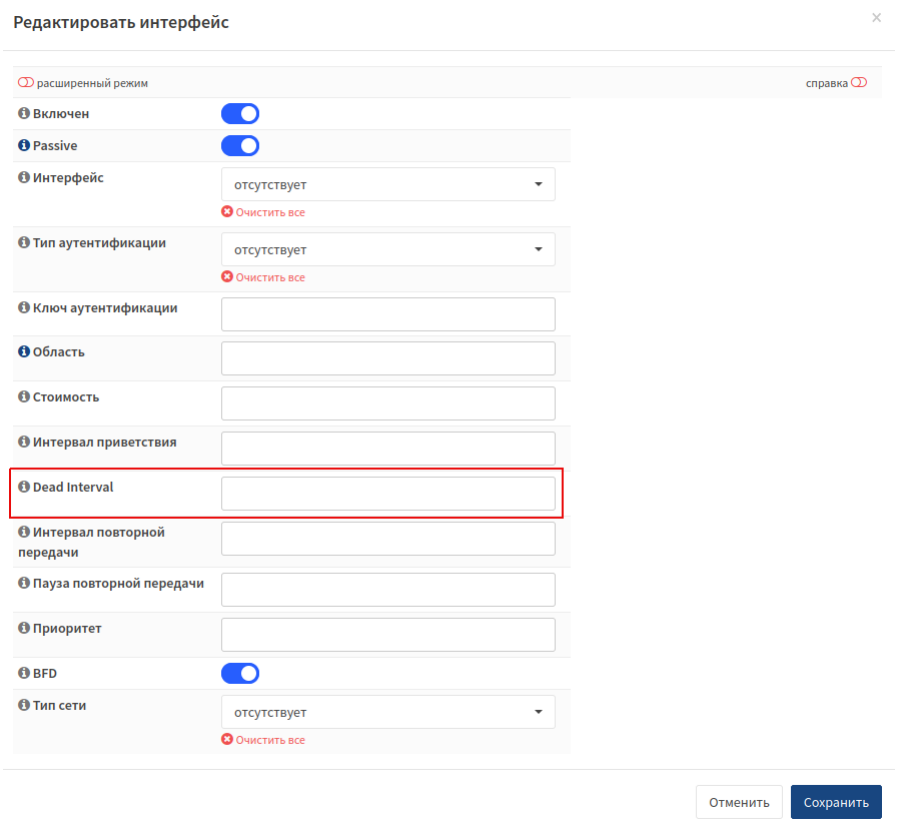


Рис. 500: Установка Dead Interval

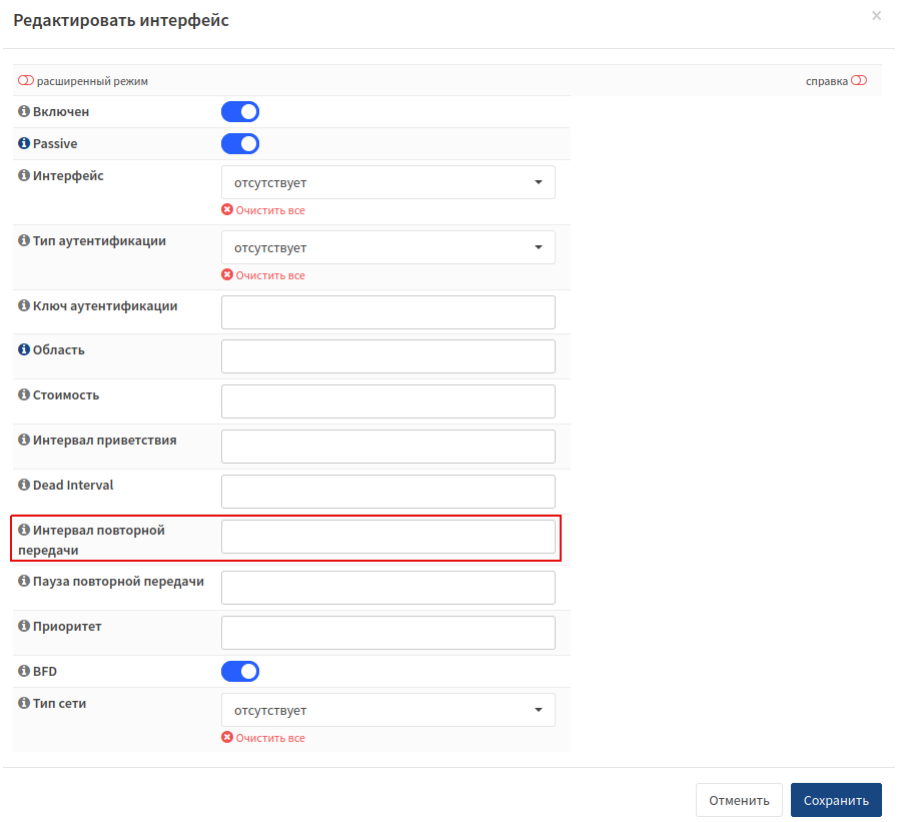


Рис. 501: Установка интервала повторной передачи

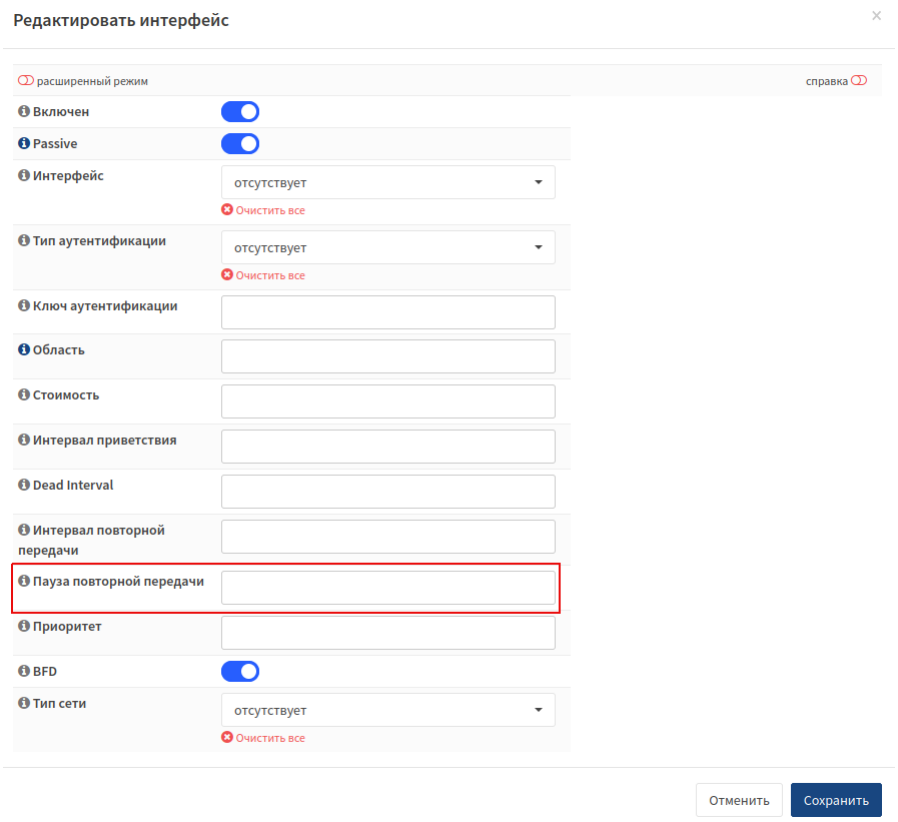


Рис. 502: Установка паузы повторной передачи

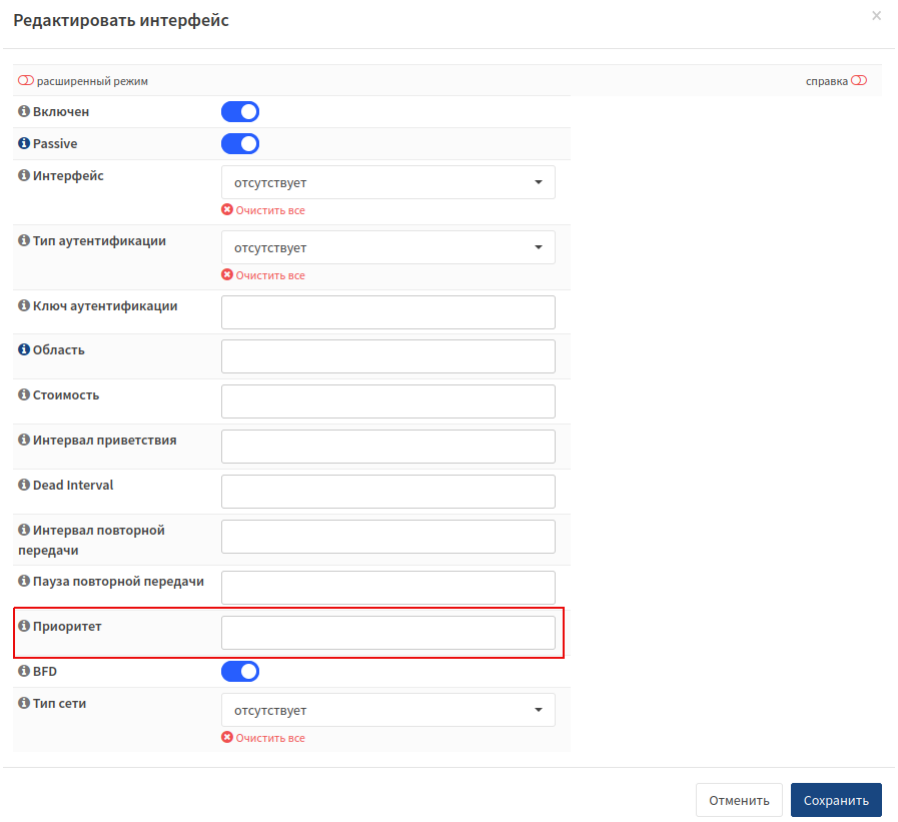


Рис. 503: Установка приоритета

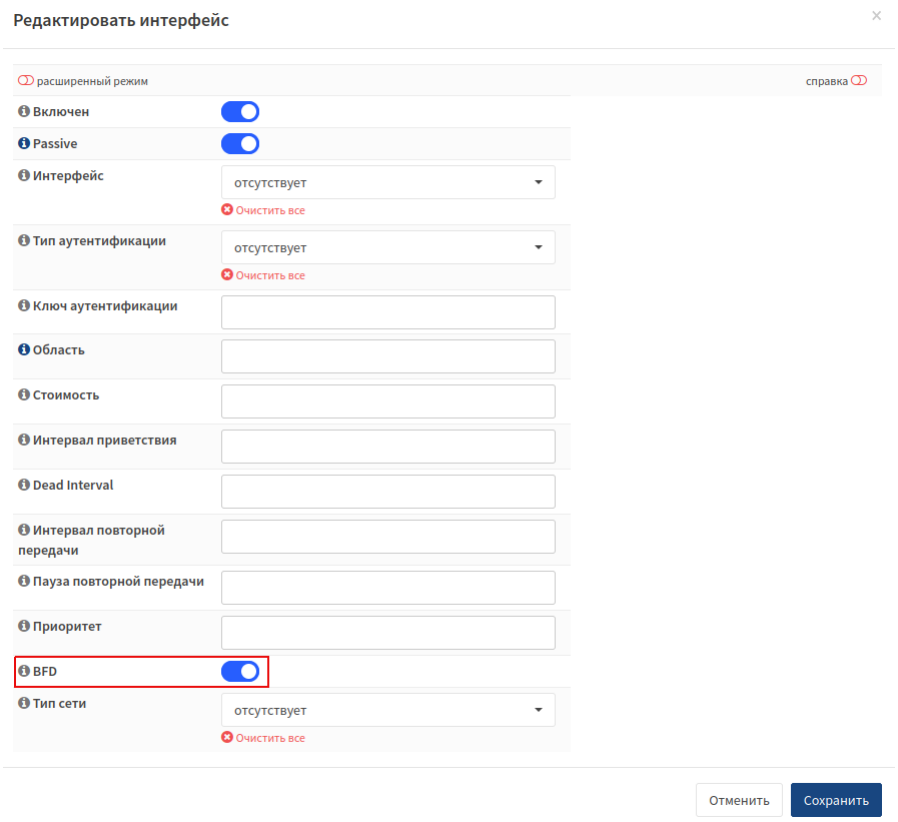


Рис. 504: Активация сервиса BFD

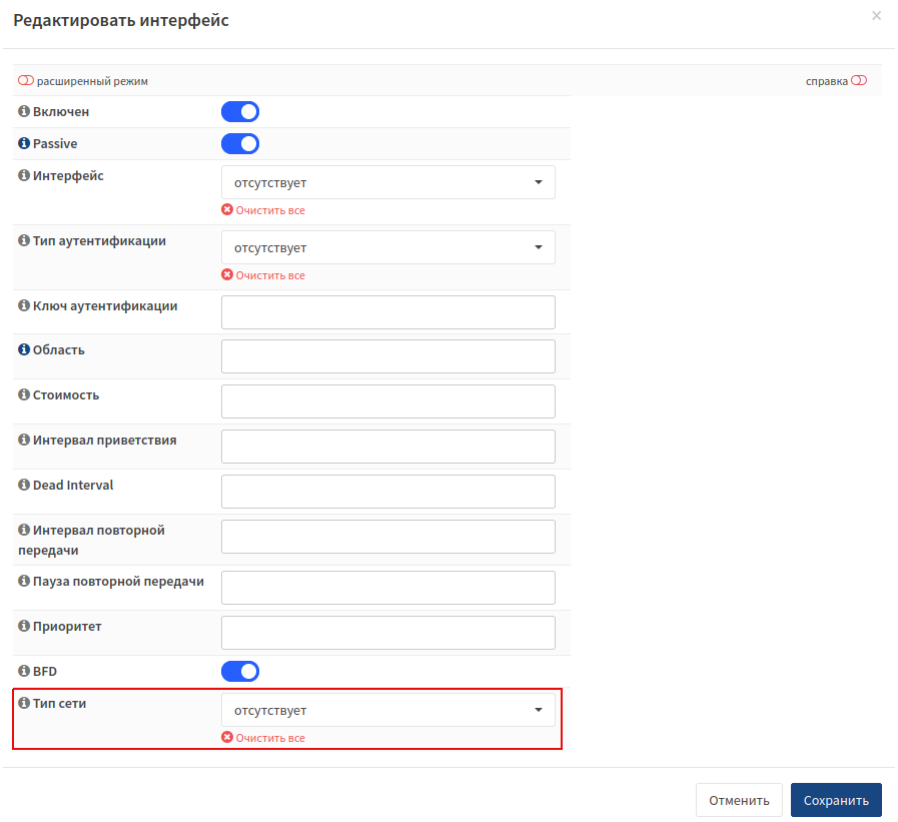


Рис. 505: Выбор типа сети

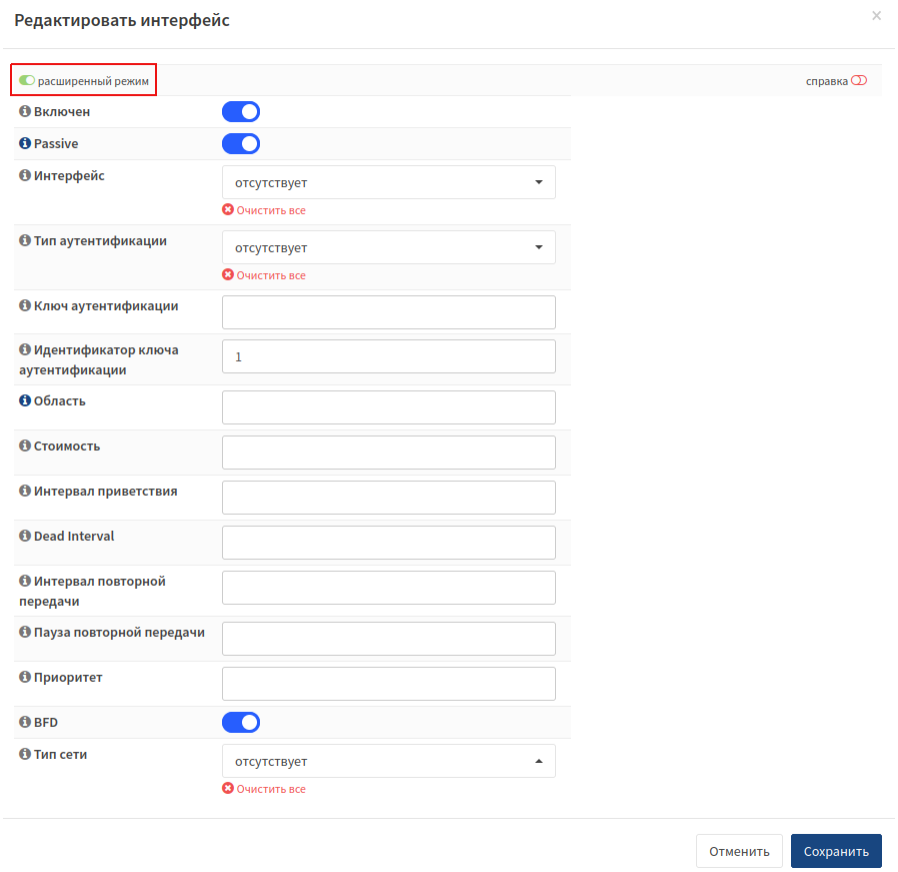


Рис. 506: Включение расширенных настроек

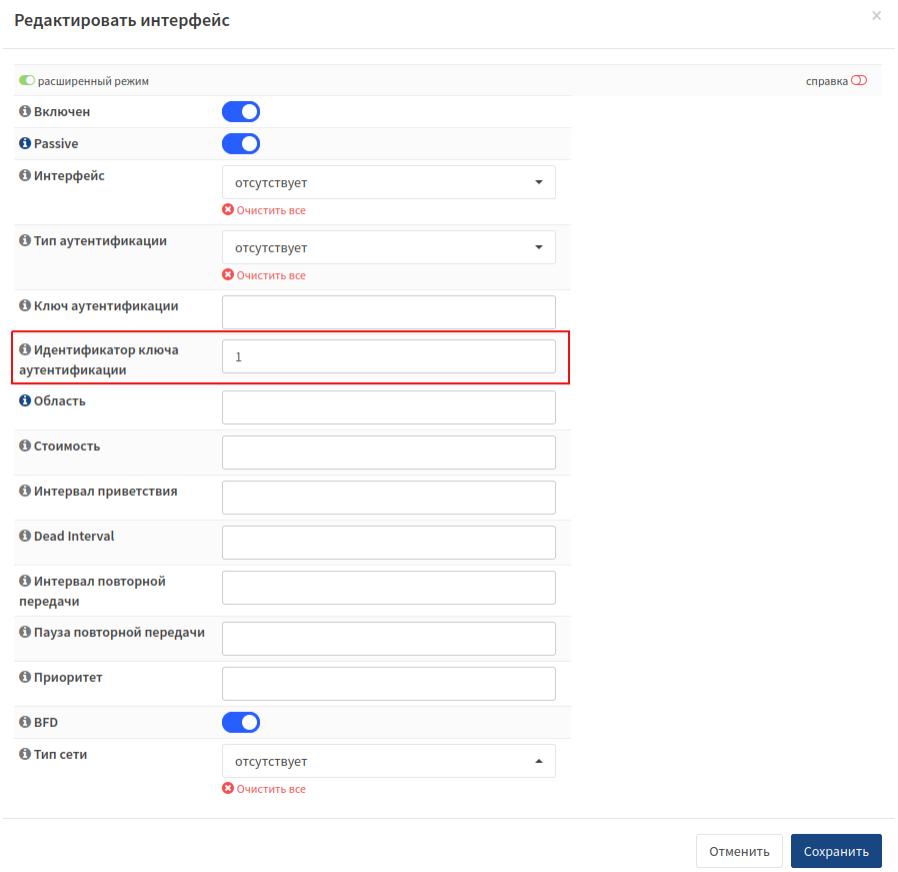


Рис. 507: Установка идентификатора ключа аутентификации

Списки префиксов

Таблица списков префиксов представлена на рисунке.

С помощью фильтров можно ограничить или расширить данные таблицы.

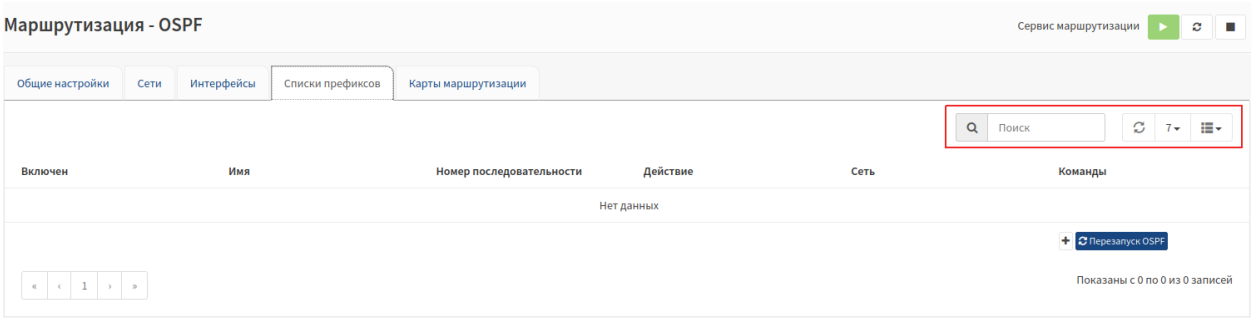


Рис. 508: Фильтры таблицы списков префиксов

Для обновления таблицы списка префиксов необходимо нажать кнопку 

, расположенную в правом нижнем углу таблицы.

Для добавления нового списка префиксов в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации списка префиксов;

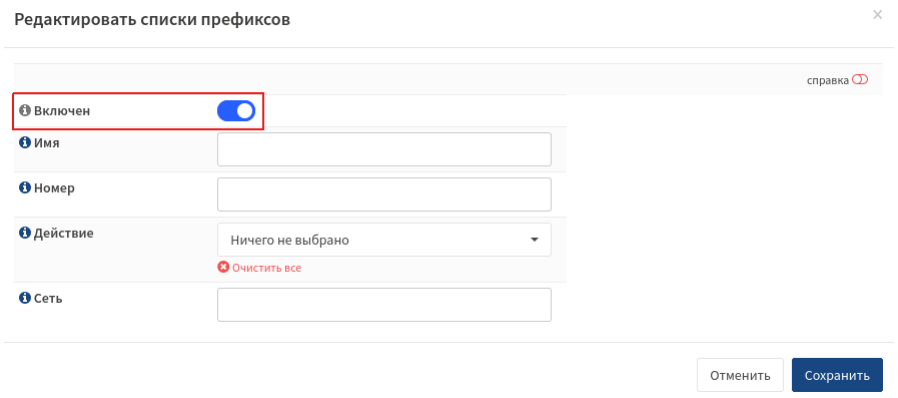


Рис. 509: Активация списка префиксов

- в поле **«Имя»** указать имя списка префиксов, которые можно использовать на странице добавления сетей;
- в поле **«Номер»** указать порядковый номер ACL (10-99);
- в поле **«Действие»** выбрать из выпадающего списка необходимое действие, производимое с правилом;

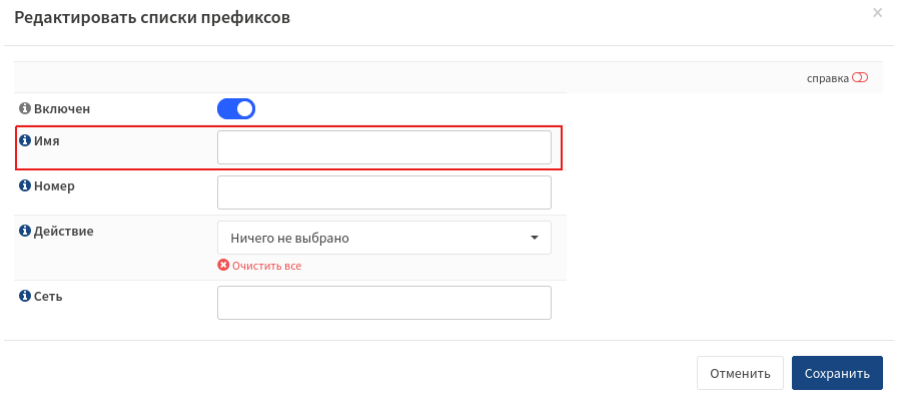


Рис. 510: Установка имен списков префиксов

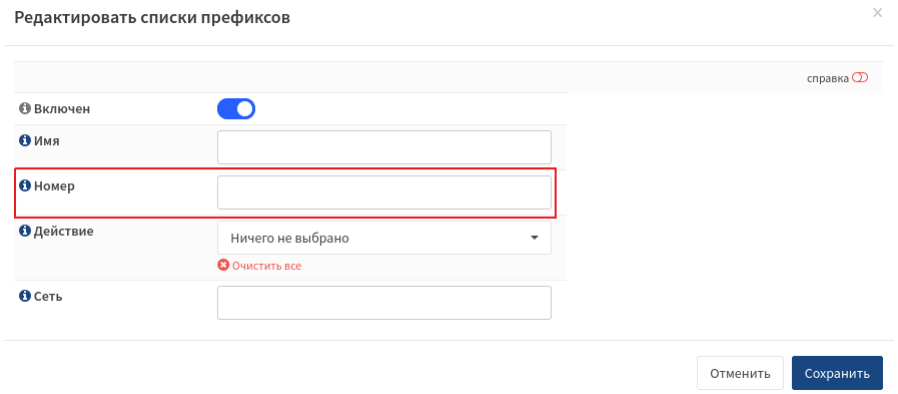


Рис. 511: Установка номера ACL

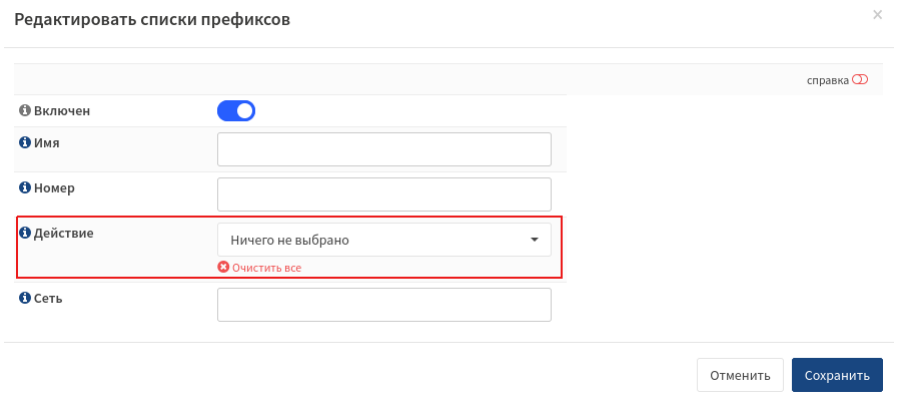


Рис. 512: Выбор действия

Совет

Укажите **«Разрешать»** для соответствия или **«Запретить»** для отмены правила

- в поле **«Сеть»** указать шаблон сети для поиска;

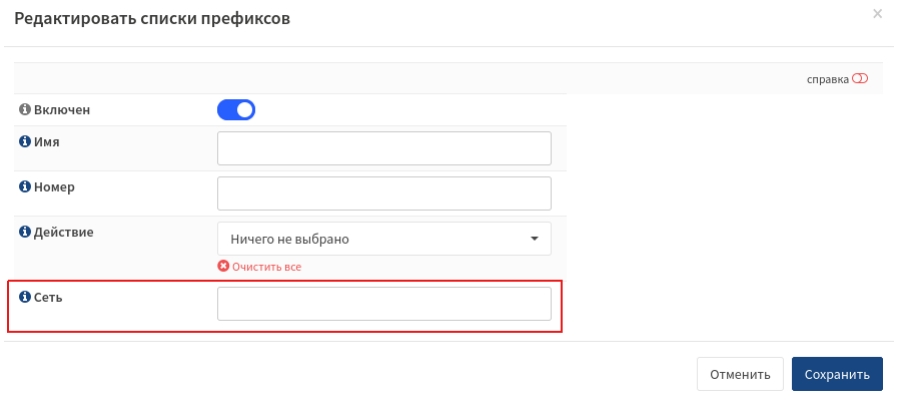


Рис. 513: Установка шаблона сети

Совет

Например: 10.0.3.0/24

- нажать кнопку 

для вступления проведенных настроек в силу.

Карты маршрутизации

Таблица карт маршрутизации представлена на рисунке.

С помощью фильтров можно ограничить или расширить данные таблицы.

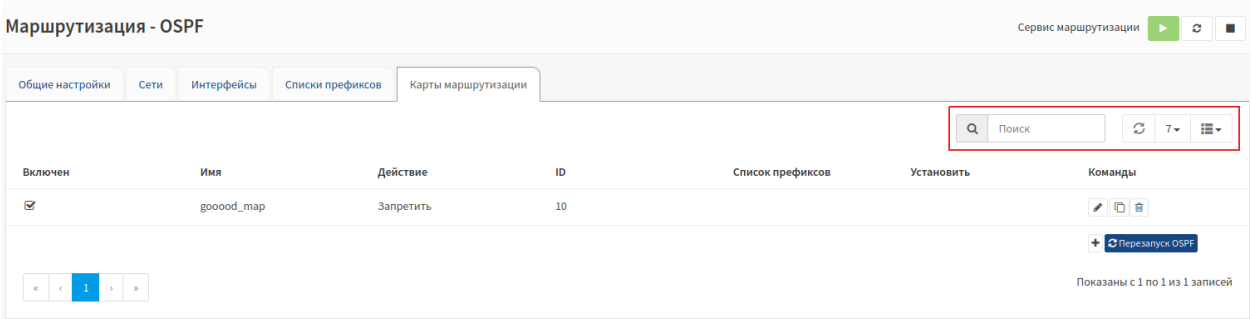


Рис. 514: Фильтры таблицы карт маршрутизации

Для редактирования карт маршрутизации из таблицы необходимо нажать кнопку  , расположенную напротив необходимого интерфейса в столбце **«Команды»**.

Для обновления таблицы карт маршрутизации необходимо нажать кнопку 

, расположенную в правом нижнем углу таблицы.

Для добавления новой карты маршрутизации в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации карт маршрутизации;

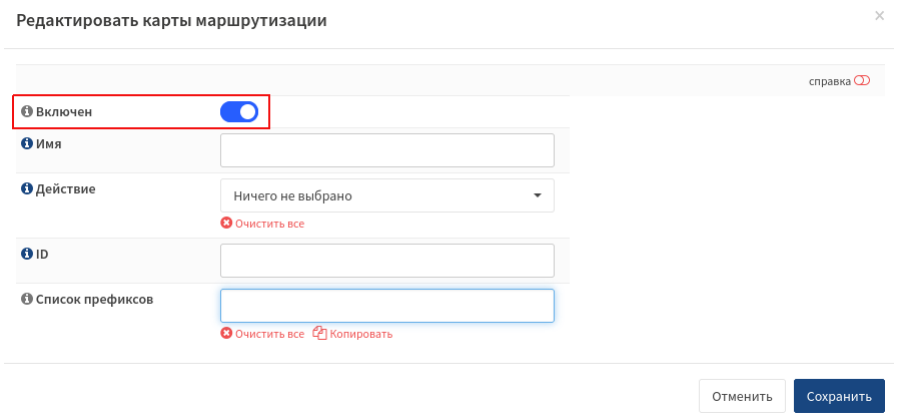


Рис. 515: Активация карт маршрутизации

- в поле **«Имя»** указать имя карты маршрута, которое может быть использовано в редистрибуции;

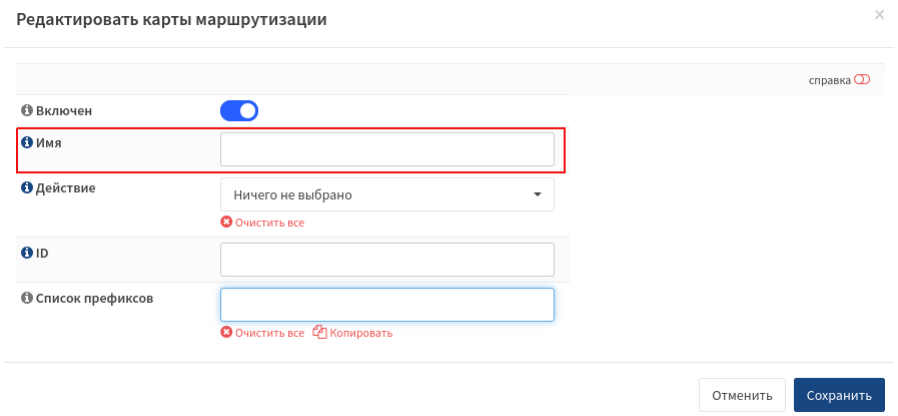


Рис. 516: Установка имени карты маршрута

- в поле **«Действие»** выбрать из выпадающего списка необходимое действие, производимое с правилом;

Совет

Укажите **«Разрешать»** для соответствия или **«Запретить»** для отмены правила

- в поле **«ID»** указать ID карты маршрутов между 10 и 99;

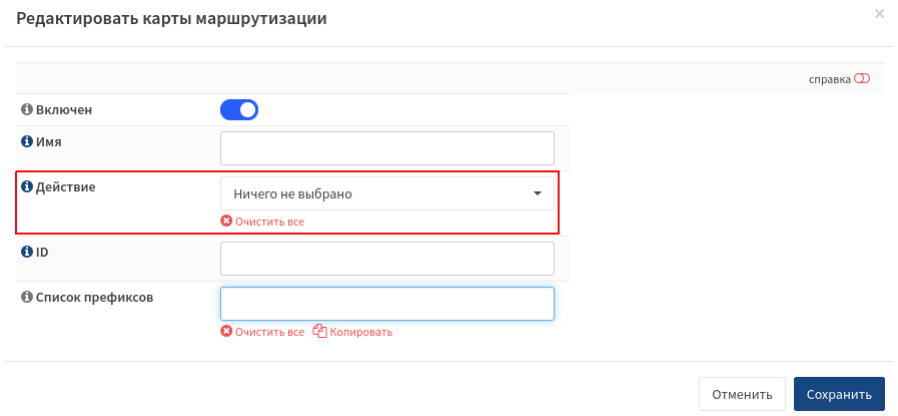


Рис. 517: Выбор действия

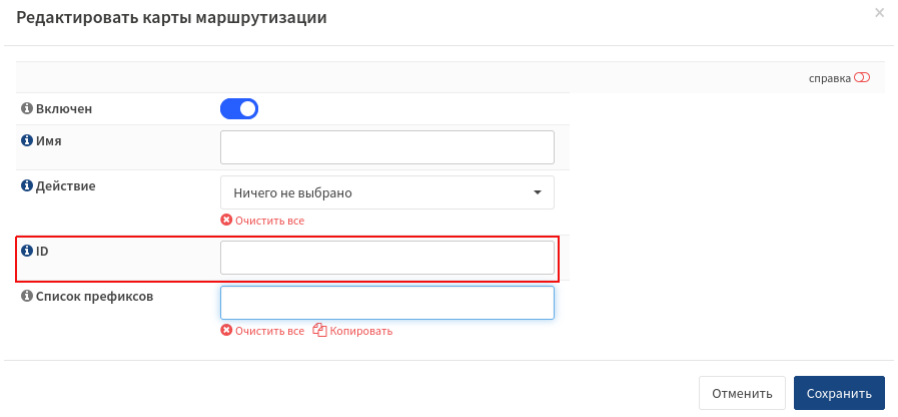


Рис. 518: Установка ID карты маршрутов

- в поле **«Список префиксов»** указать список префиксов;

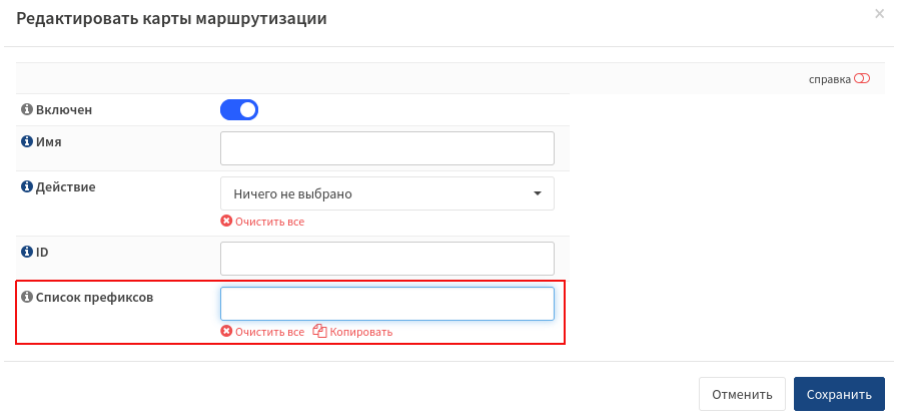


Рис. 519: Установка списка префиксов

- нажать кнопку 

для вступления проведенных настроек в силу.

2.7.6.4 BGP

Общие настройки

Для конфигурации общих настроек сервиса BGP необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации сервиса BGP;

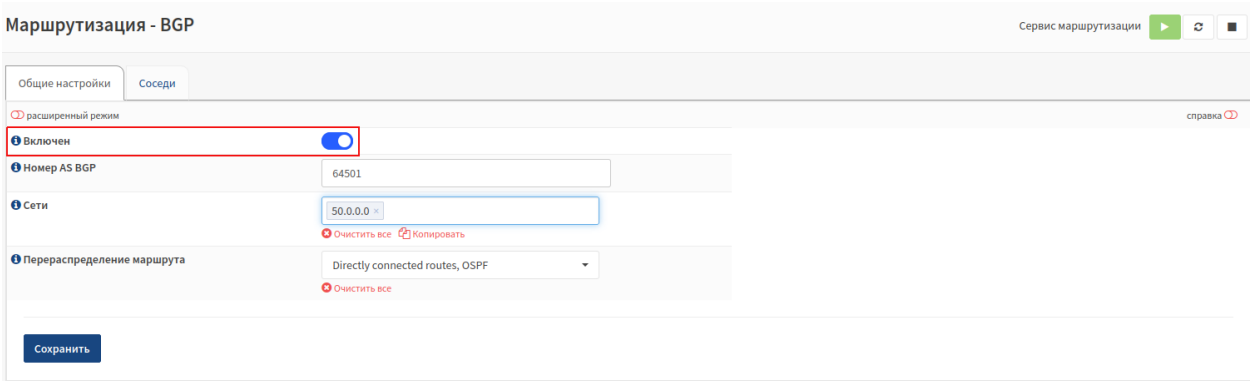


Рис. 520: Активация сервиса BGP

- в поле **«Номер AS BGP»** установить номер AS BGP;
- в поле **«Сети»** выбрать сети для оповещения;
- в поле **«Перераспределение маршрута»** выбрать из выпадающего списка источники маршрутизации, которые должны быть переданы (перераспределены) другим узлам;

Для включения режима расширенных настроек необходимо установить переключатель

В режиме расширенных настроек необходимо:

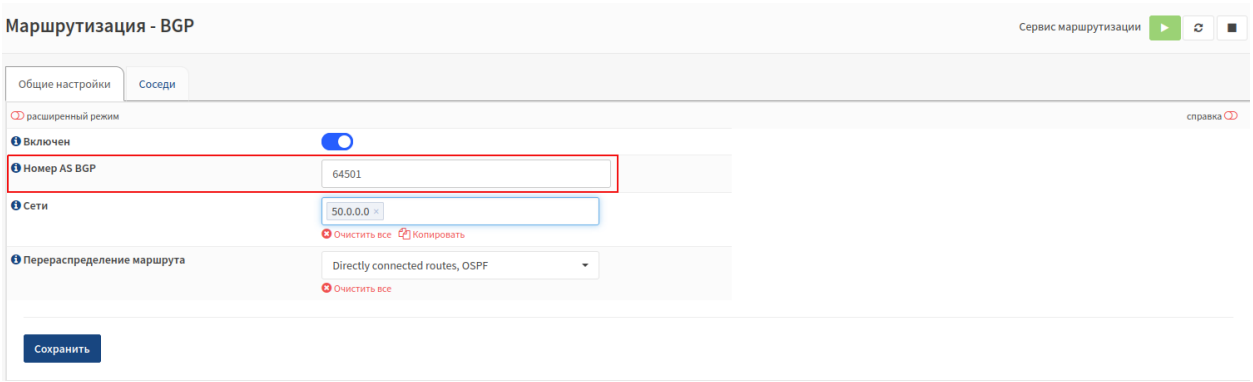


Рис. 521: Установка номера AS BGP

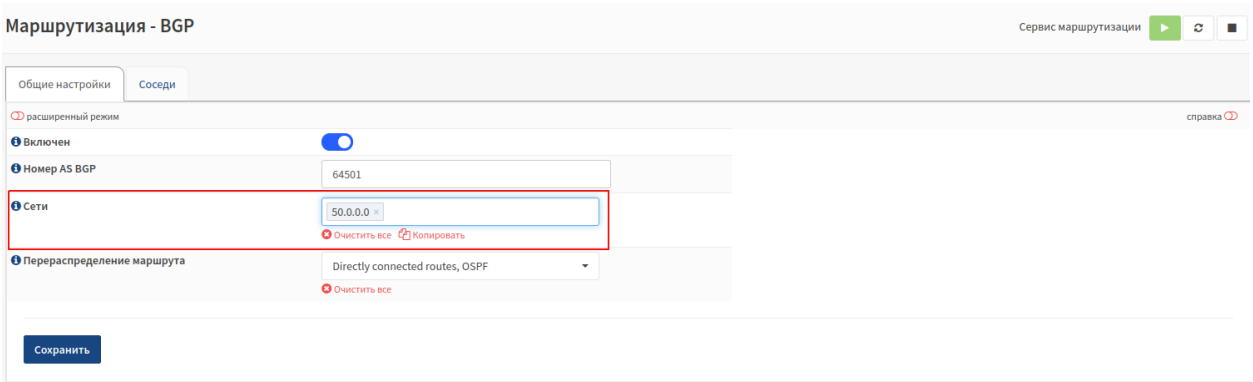


Рис. 522: Выбор сетей

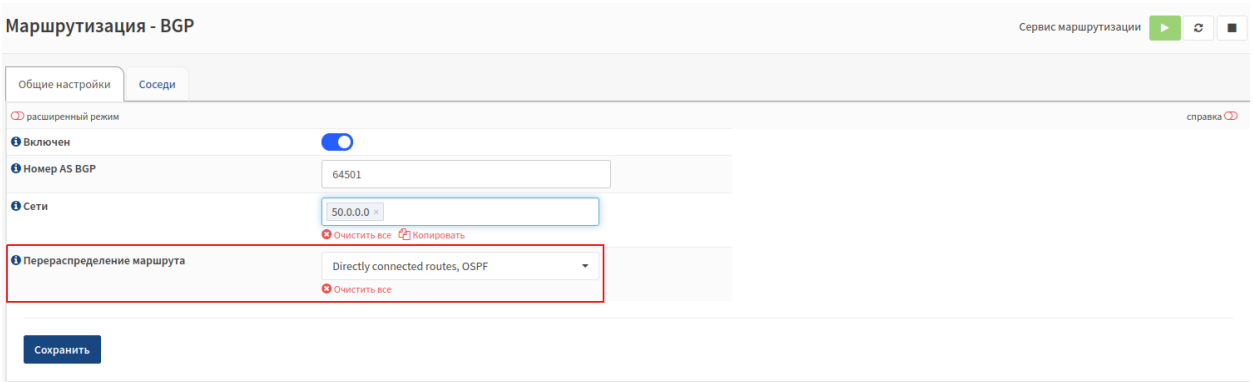


Рис. 523: Выбор источников маршрутизации

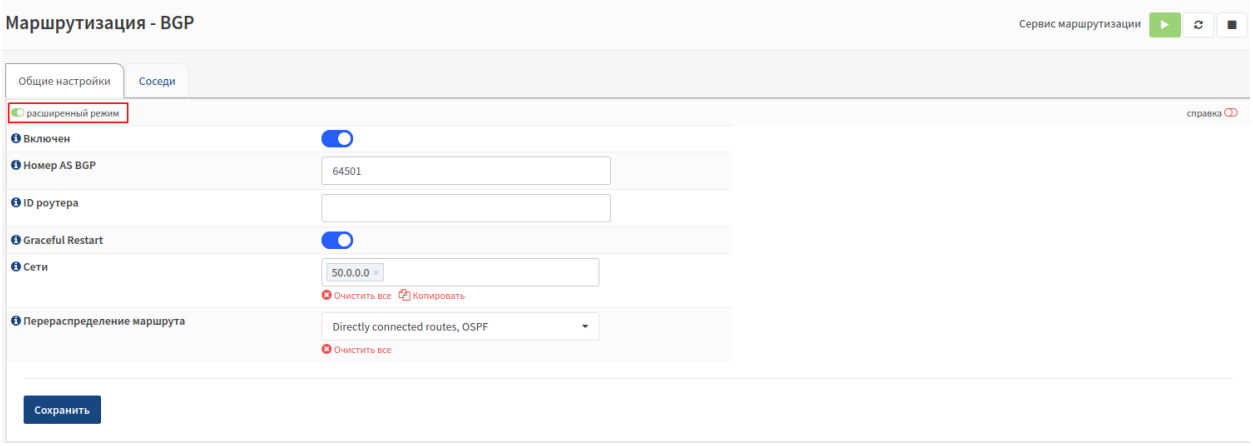


Рис. 524: Включение расширенных настроек

- в поле **«ID роутера»** установить фиксированный идентификатор маршрутизатора;

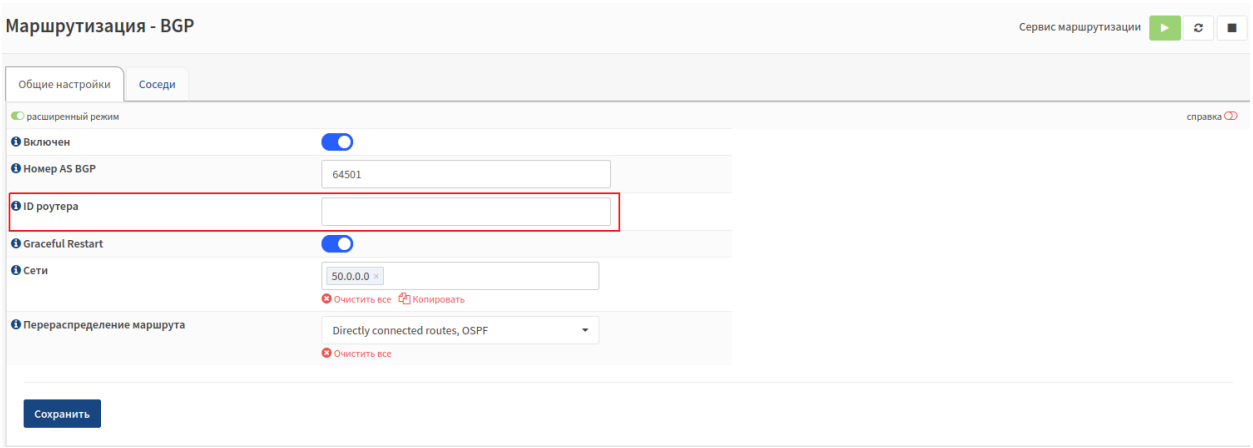


Рис. 525: Установка ID роутера

- в поле **«Graceful Restart»** установить переключатель в случае плавного перезапуска BGP, как определено в RFC-4724;

Важно

Данная функция определяет механизмы, которые позволяют узлу BGP продолжать пересылать пакеты данных по известным маршрутам, пока восстанавливается информация протокола маршрутизации

- нажать кнопку 

для вступления проведенных настроек в силу.

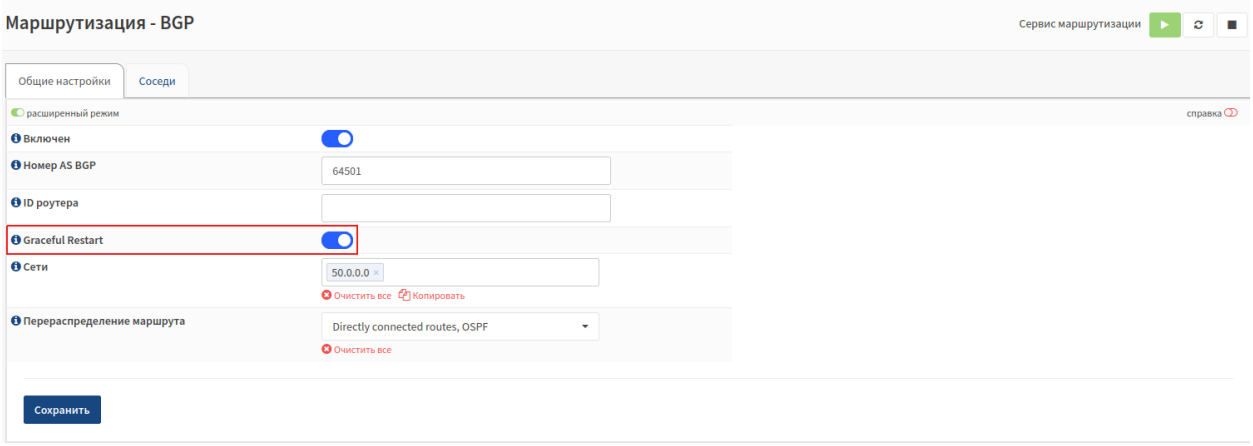


Рис. 526: Активация сервиса BGP

Соседи

Таблица соседей представлена на рисунке.

С помощью фильтров можно ограничить или расширить данные таблицы.

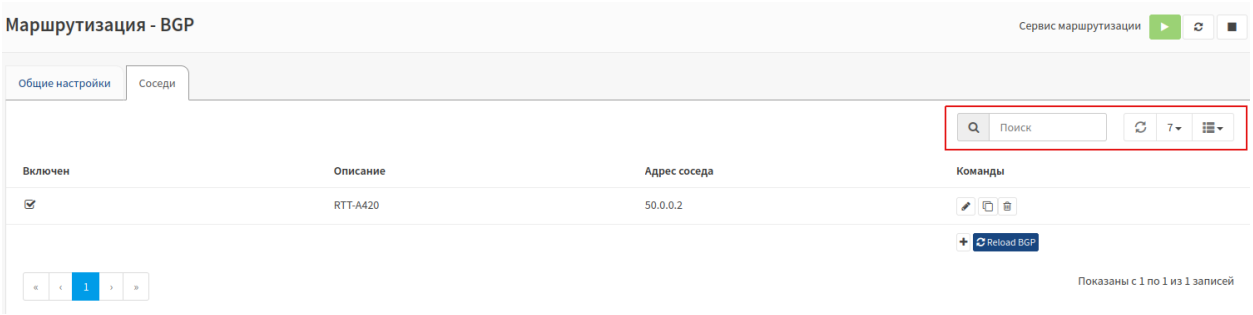


Рис. 527: Фильтры таблицы соседей

Для редактирования соседей из таблицы необходимо нажать кнопку  , расположенную напротив необходимой сети в столбце **«Команды»**.

Для обновления таблицы соседей необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

Для добавления нового соседа в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации соседа;
- в поле **«Описание»** указать краткое описание соседа;
- в поле **«Одноранговый IP»** указать IP соседа;
- в поле **«Удалённый AS»** указать AS соседа;

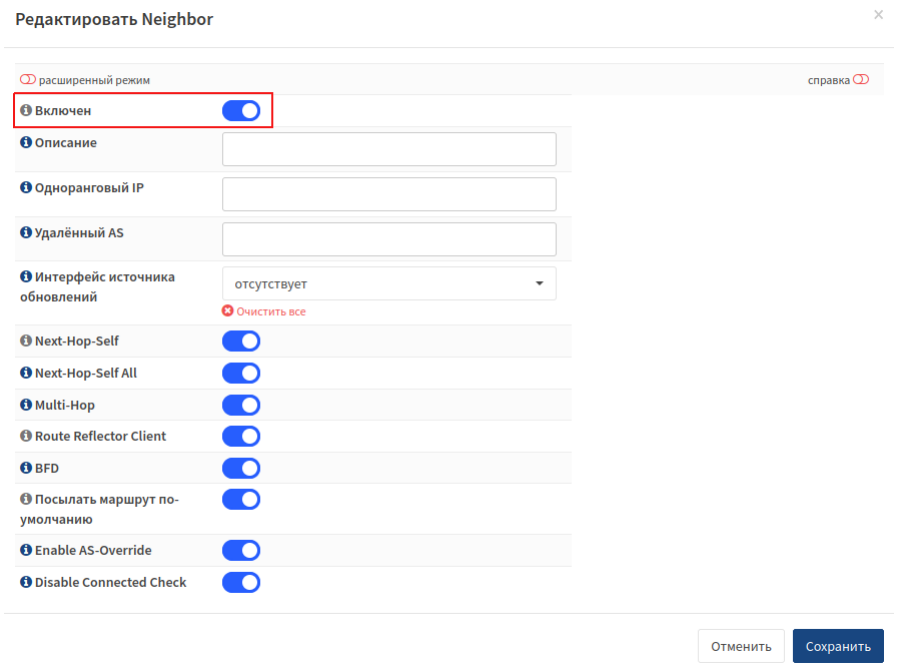


Рис. 528: Активация соседа

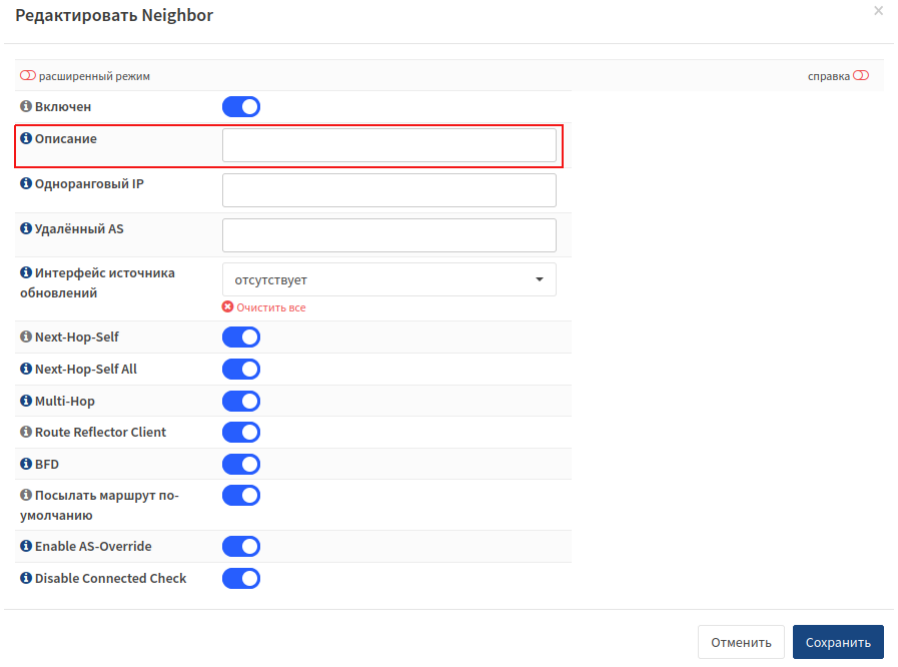


Рис. 529: Описание соседа

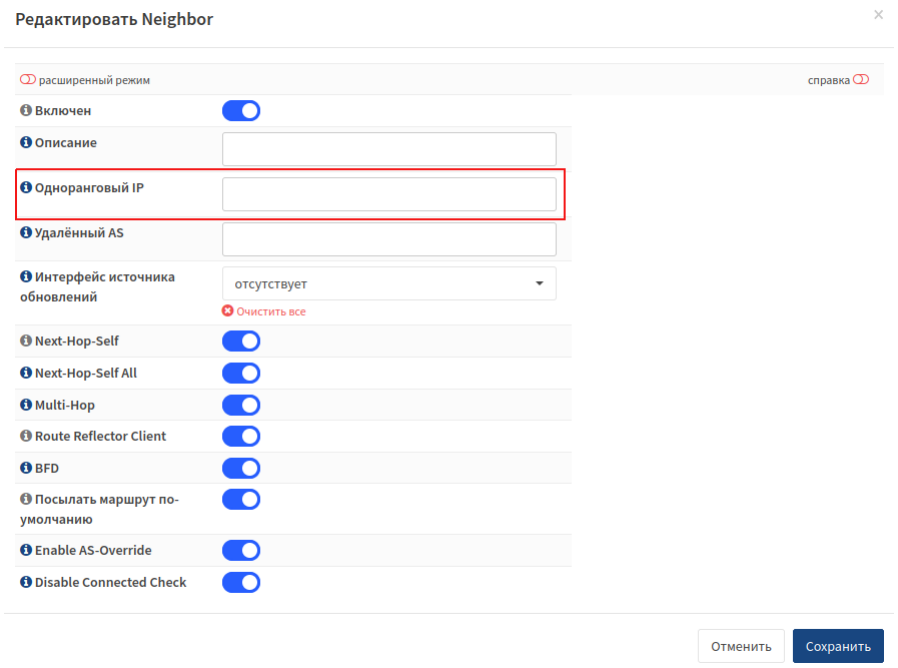


Рис. 530: IP соседа

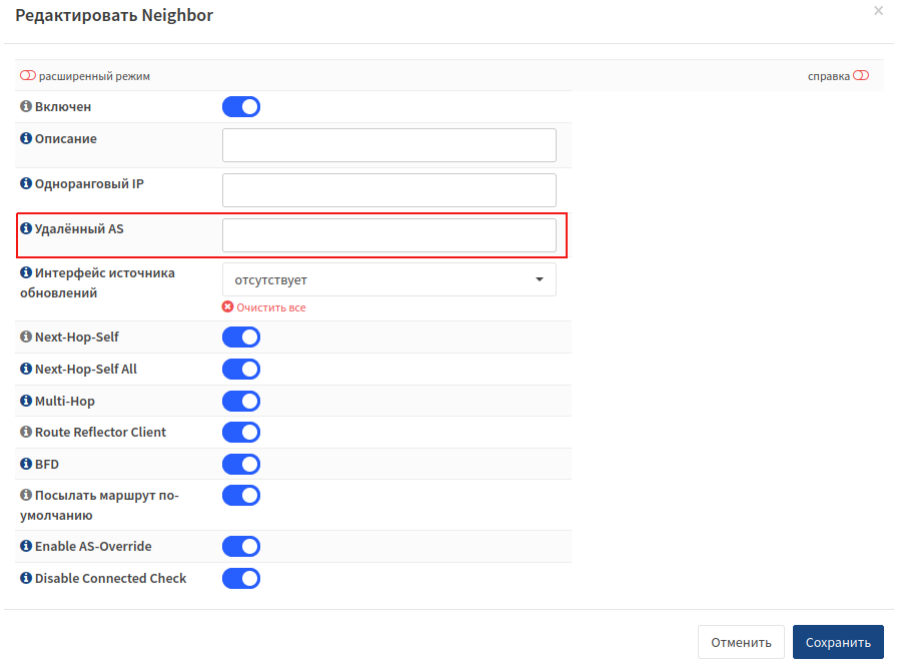


Рис. 531: AS соседа

- в поле **«Интерфейс источника обновлений»** выбрать из выпадающего списка физическое имя интерфейса IPv4, обращенного к узлу;

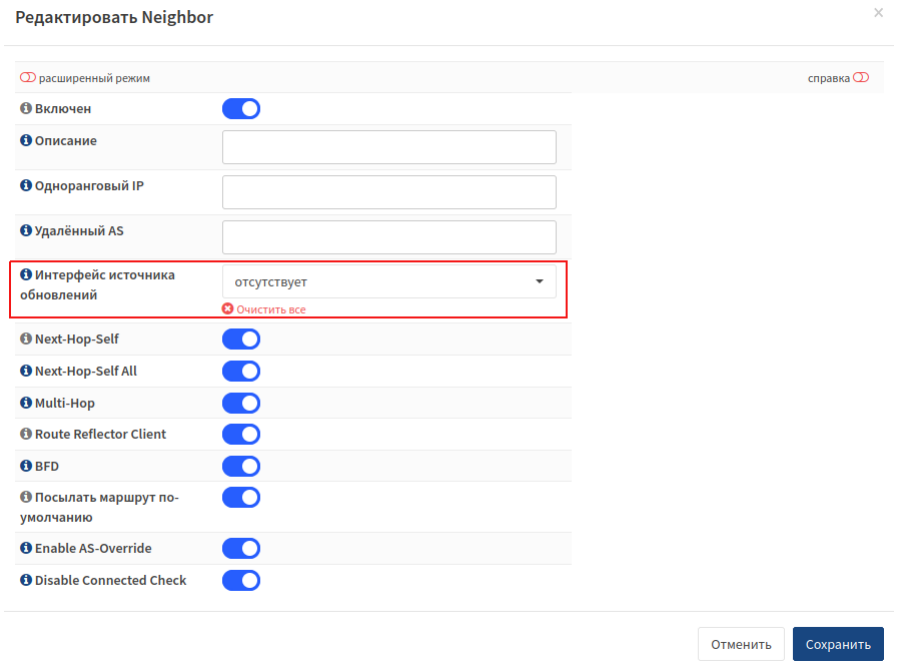


Рис. 532: Выбор источника обновлений

- в поле **«Next-Hop-Self»** установить переключатель в случае необходимости активации функции Next-Hop-Self;
- в поле **«Next-Hop-Self All»** установить переключатель в случае необходимости добавления параметра All после активации функции Next-Hop-Self;
- в поле **«Multi-Hop»** установить переключатель в случае необходимости устанавливать сеансы с соседями eBGP, когда они находятся на расстоянии нескольких переходов;

Важно

Когда сосед не подключен напрямую и этот переключатель не включен - сеанс не будет установлен

- в поле **«Route Reflector Client»** установить переключатель в случае необходимости активации функции Route Reflector Client;
- в поле **«BFD»** установить переключатель в случае необходимости включить поддержку BFD для этого соседа;
- в поле **«Посылать маршрут по умолчанию»** установить переключатель в случае необходимости посылать маршрут по умолчанию;
- в поле **«Enable AS-Override»** установить переключатель в случае необходимости заменить номер AS исходного маршрутизатора на локальный номер AS;

Важно

Эта команда разрешена только для одноранговых узлов eBGP

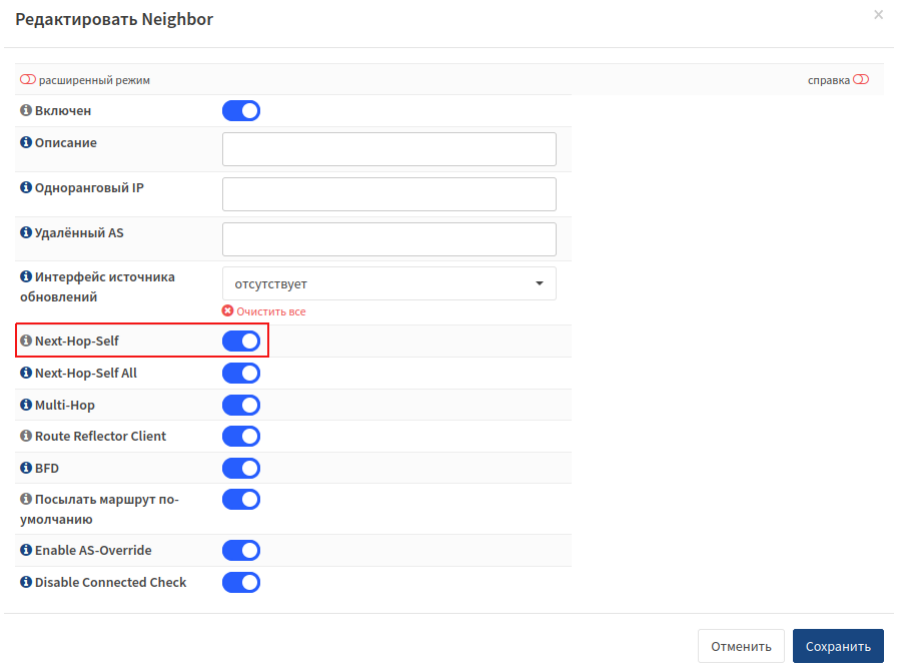


Рис. 533: Активация Next-Hop-Self

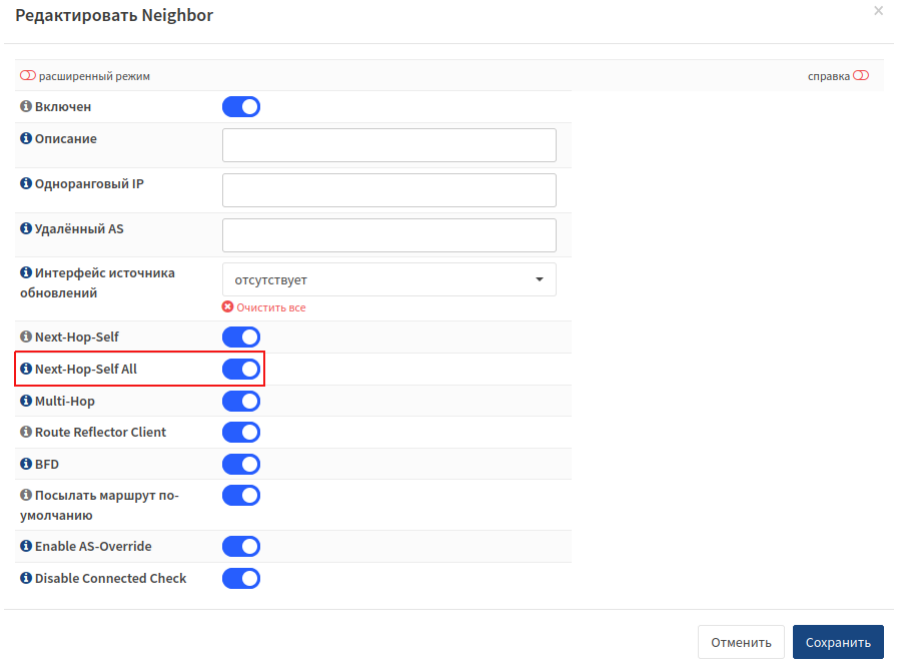


Рис. 534: Активация Next-Hop-Self All

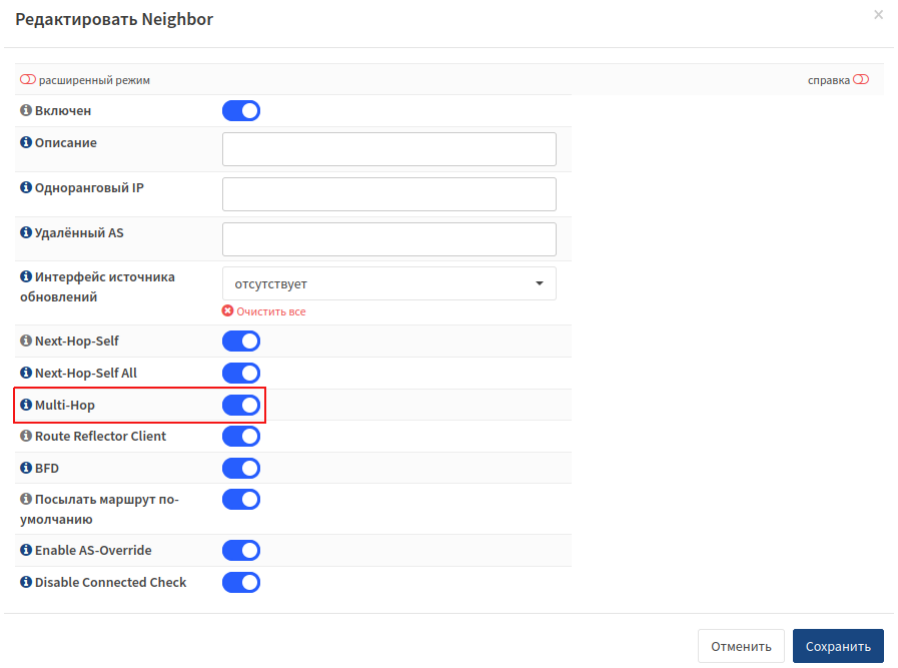


Рис. 535: Активация Multi-Hop

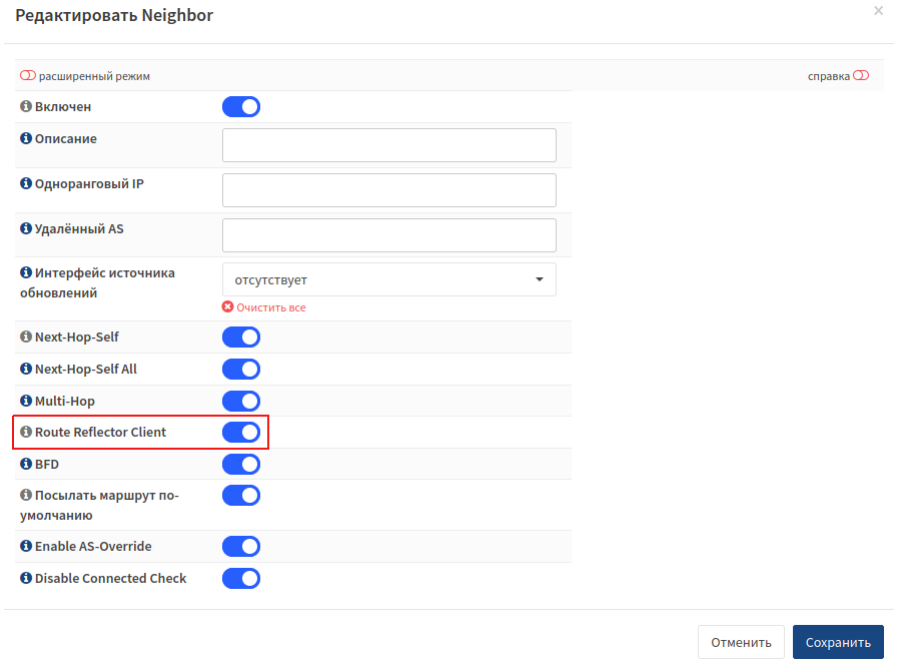


Рис. 536: Активация Route Reflector Client

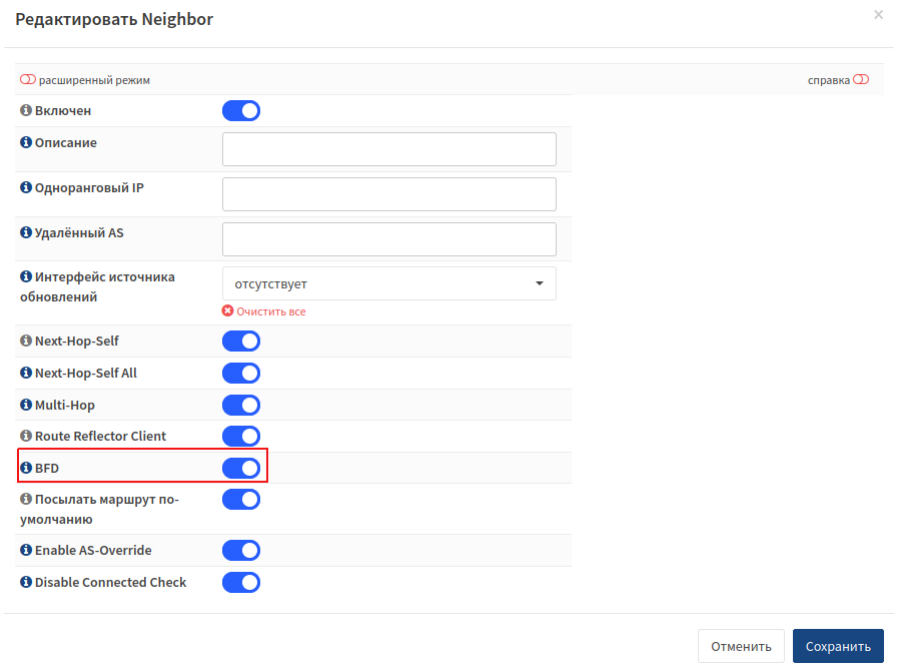


Рис. 537: Активация поддержки BFD

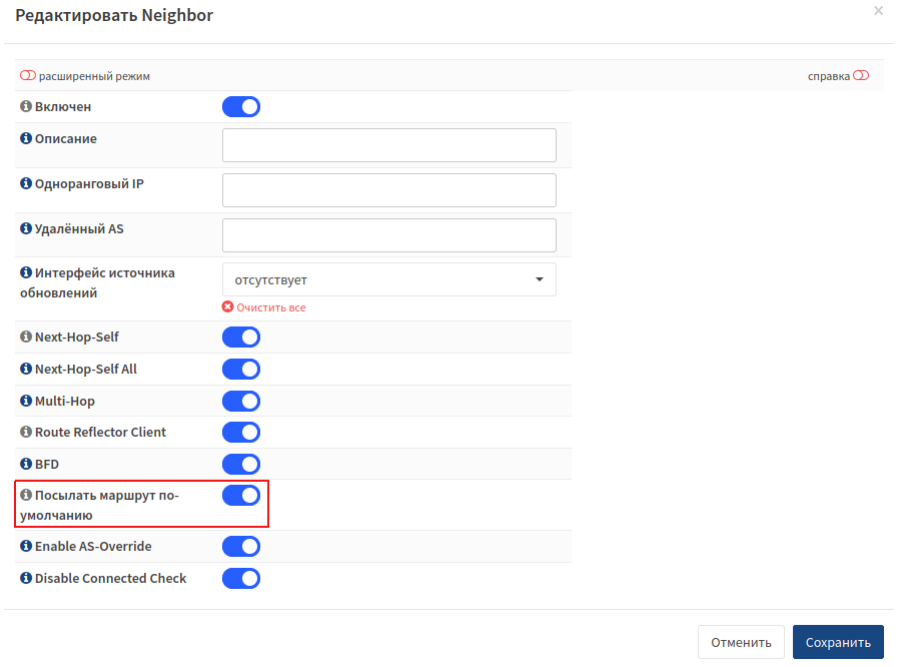


Рис. 538: Активация функции Посылать маршрут по умолчанию

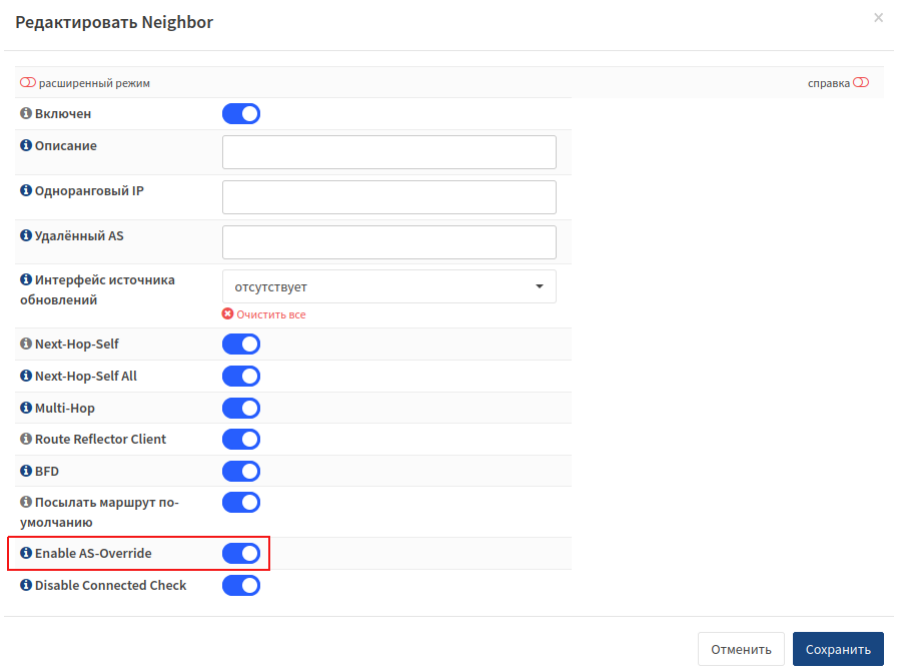


Рис. 539: Активация Enable AS-Override

- в поле **«Disable Connected Check»** установить переключатель в случае необходимости разрешить пиринг между напрямую подключенными одноранговыми узлами eBGP с использованием адресов обратной связи;

Для включения режима расширенных настроек необходимо установить переключатель

В режиме расширенных настроек необходимо:

- в поле **«BGP MD5 Password»** установить пароль для аутентификации BGP;
- в поле **«Весовой коэффициент»** указать значение веса по умолчанию для маршрутов соседа;
- в поле **«Local Initiater IP»** установить локальный IP-адрес для подключения к соседу;

Совет

Требуется только для аутентификации BGP

- в поле **«IPv6 link-local interface»** выбрать из выпадающего списка интерфейс для использования для локальных соседей IPv6;
- в поле **«Multi-Protocol»** установить переключатель в случае необходимости отключить функцию Multi-Protocol;
- в поле **«Keepalive»** установить таймер Keepalive для проверки работоспособности соседа;

Совет

Значение по умолчанию, когда не установлено, составляет 60 секунд

- в поле **«Hold Down Time»** установить время в секундах, когда сосед считается неактивным;

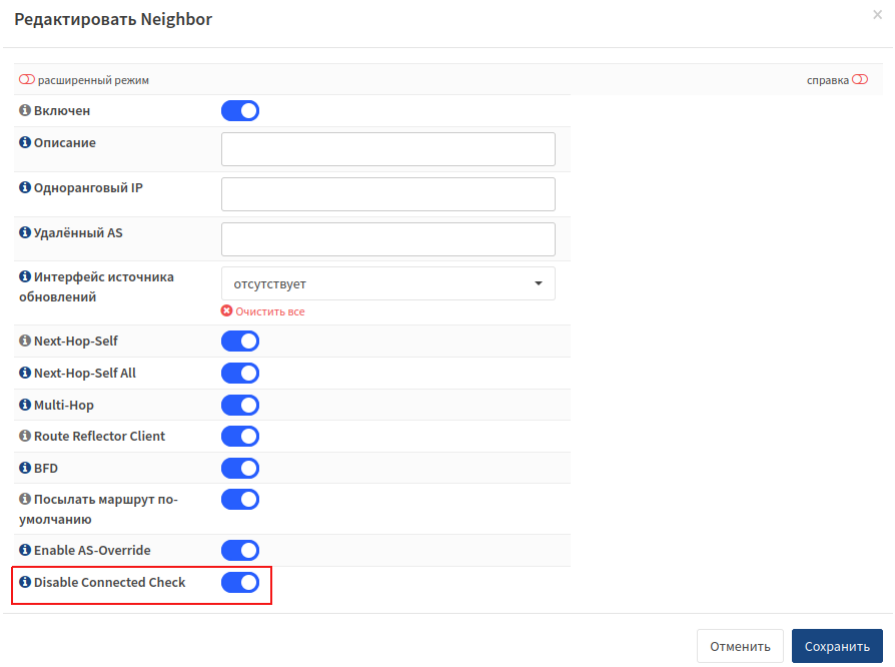


Рис. 540: Активация Disable Connected Check

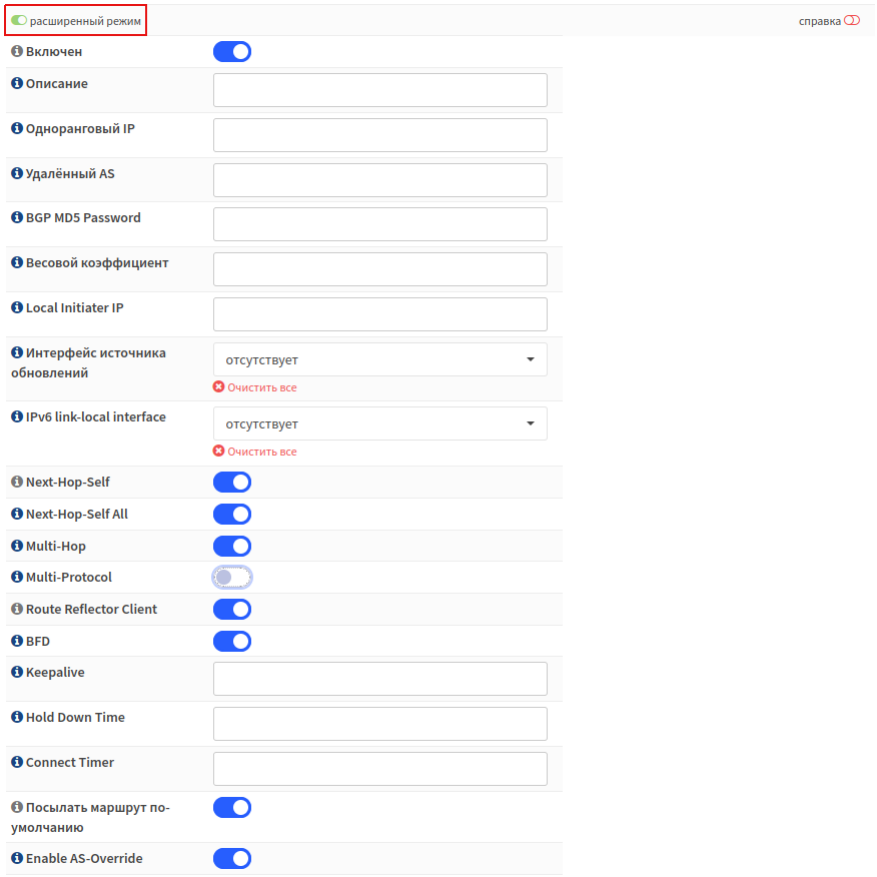


Рис. 541: Включение расширенных настроек

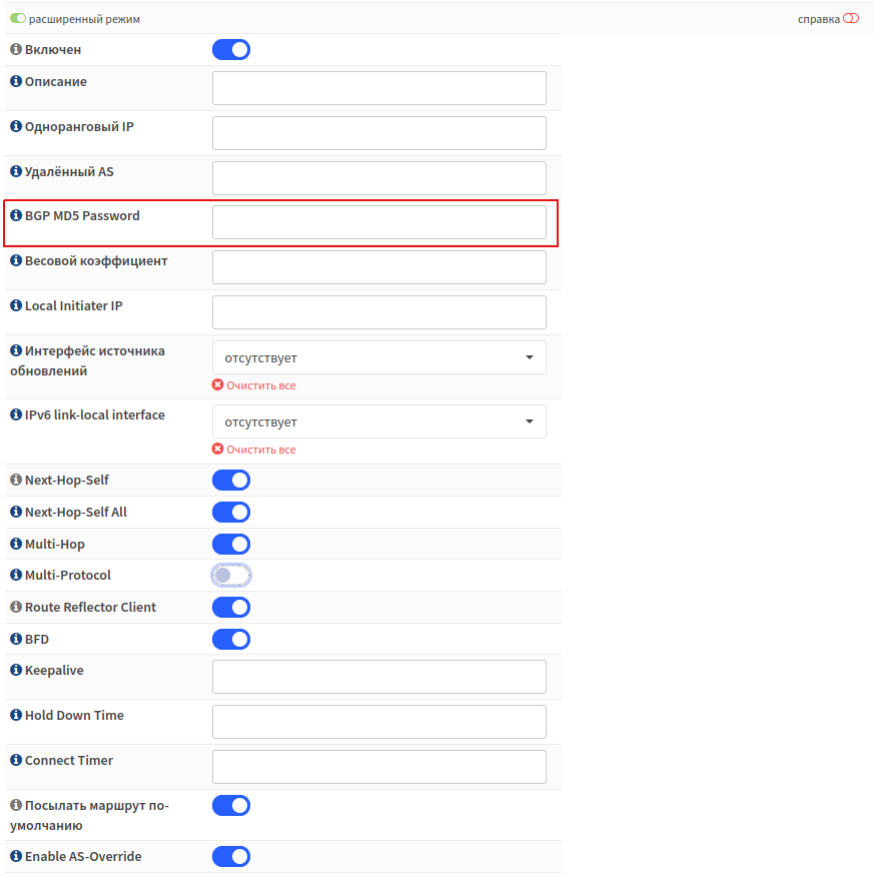


Рис. 542: Установка пароля

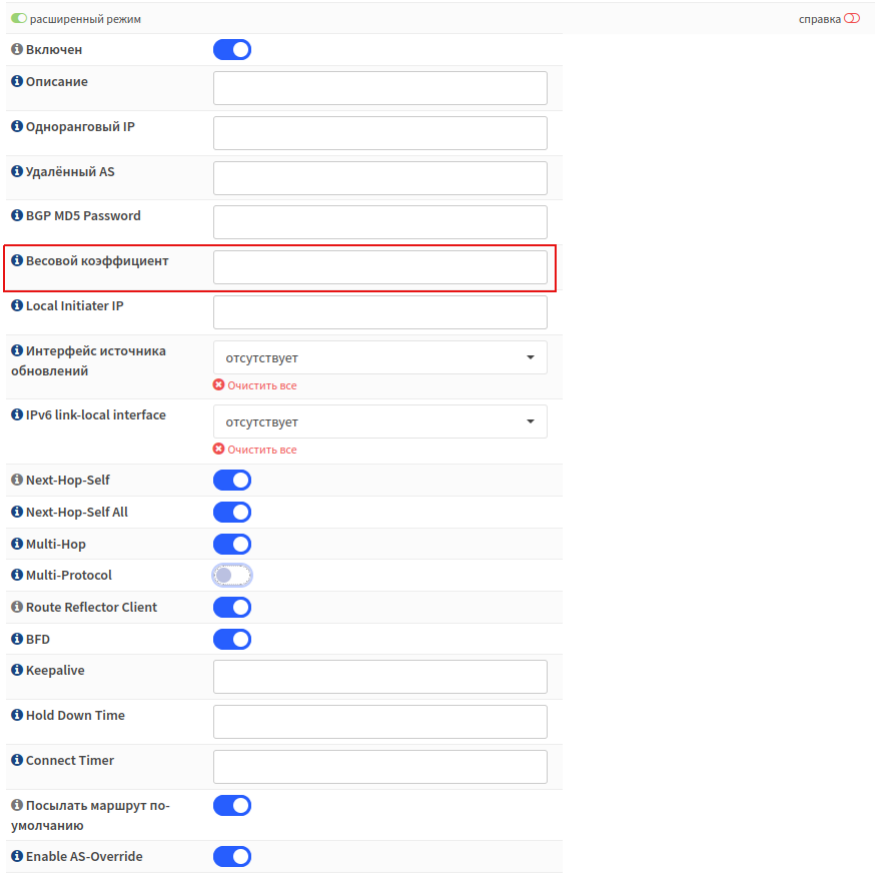


Рис. 543: Установка весового коэффициента

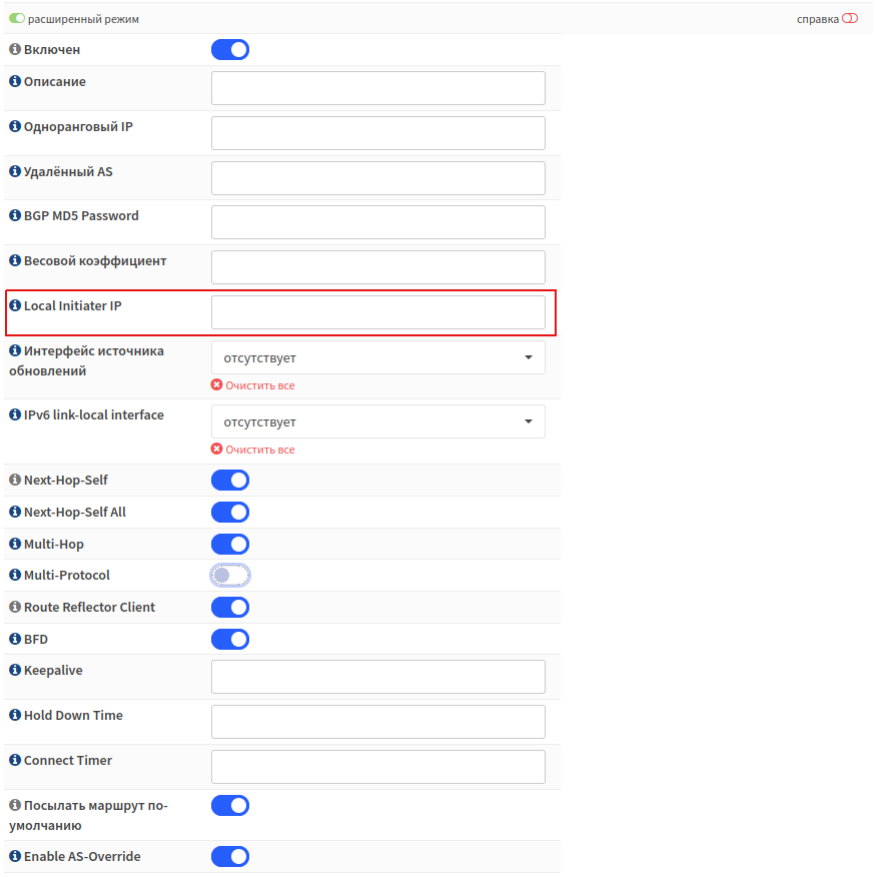


Рис. 544: Установка локального IP-адреса

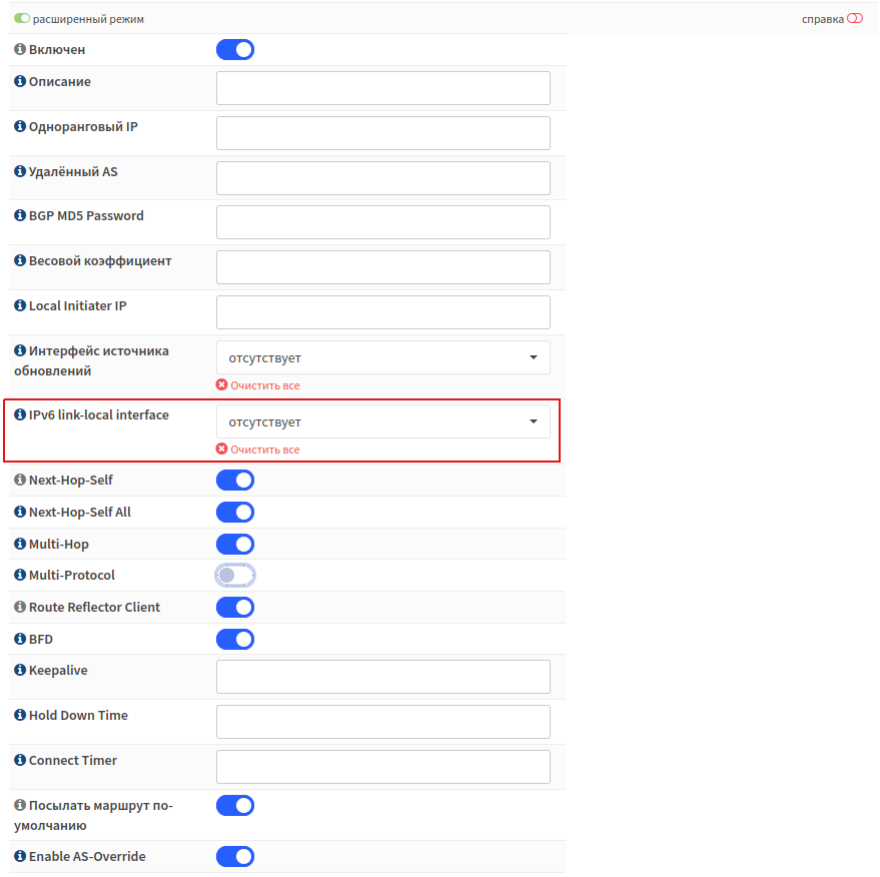


Рис. 545: Выбор интерфейса для локальных соседей IPv6

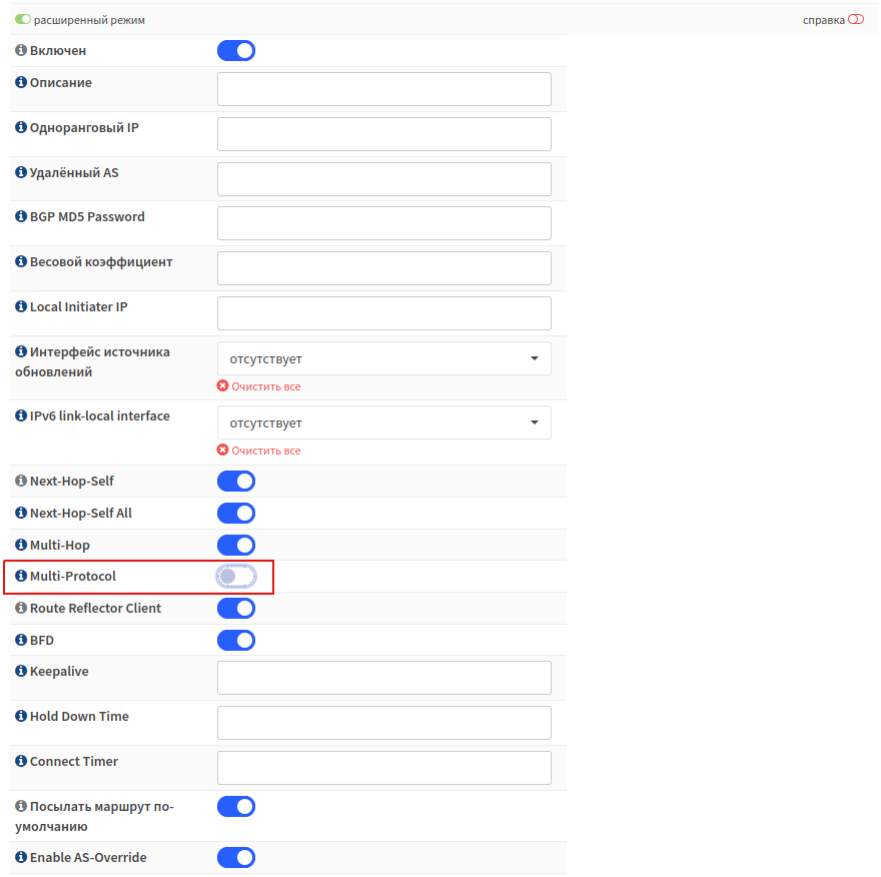


Рис. 546: Активация Multi-Protocol

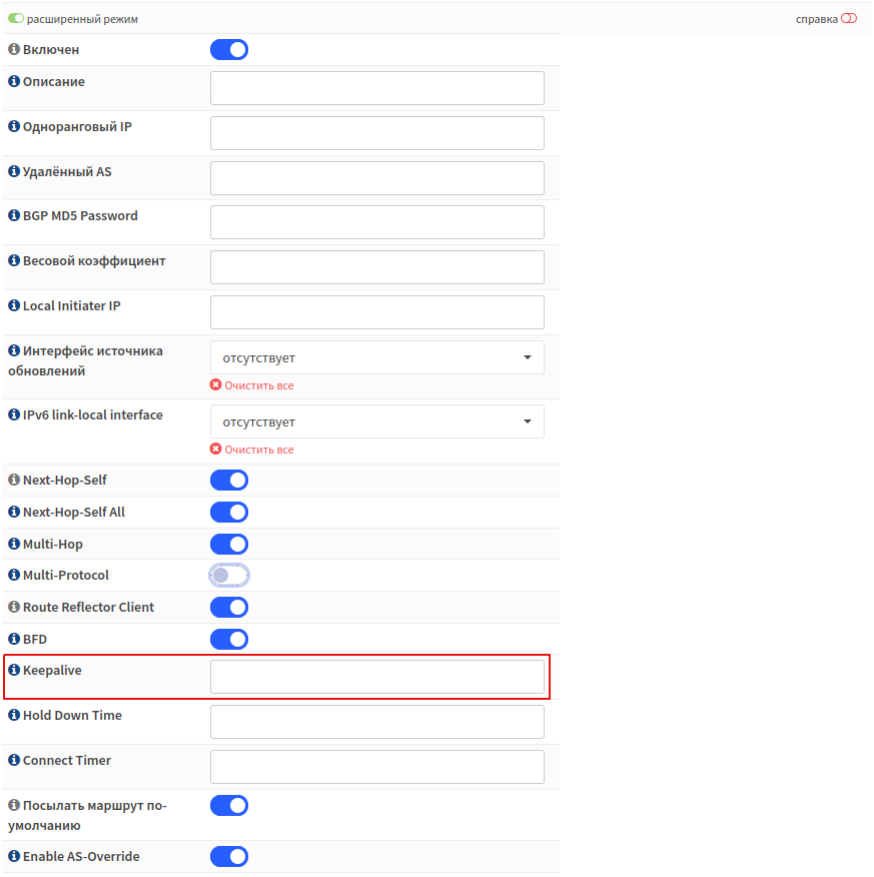


Рис. 547: Установка таймера Keepalive

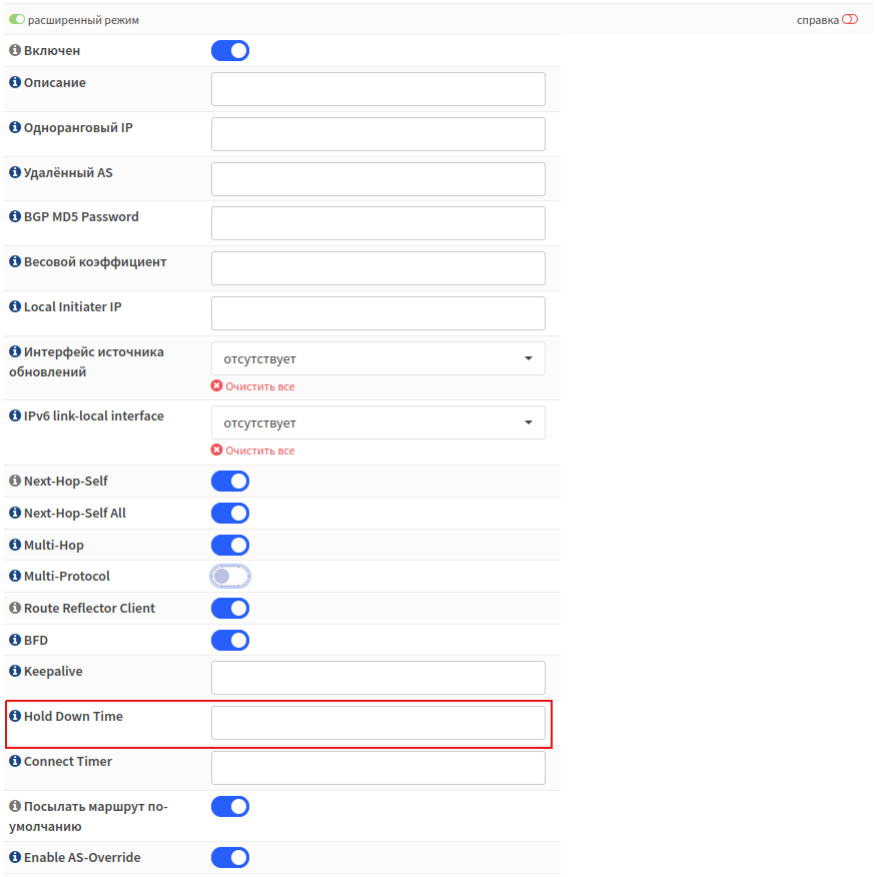


Рис. 548: Установка Hold Down Time

Совет

Обычно это в 3 раза больше таймера Keeplive, а при отключении 180 секунд

- в поле **«Connect Timer»** установить время в секундах, показывающее, насколько быстро сосед пытается переподключиться;

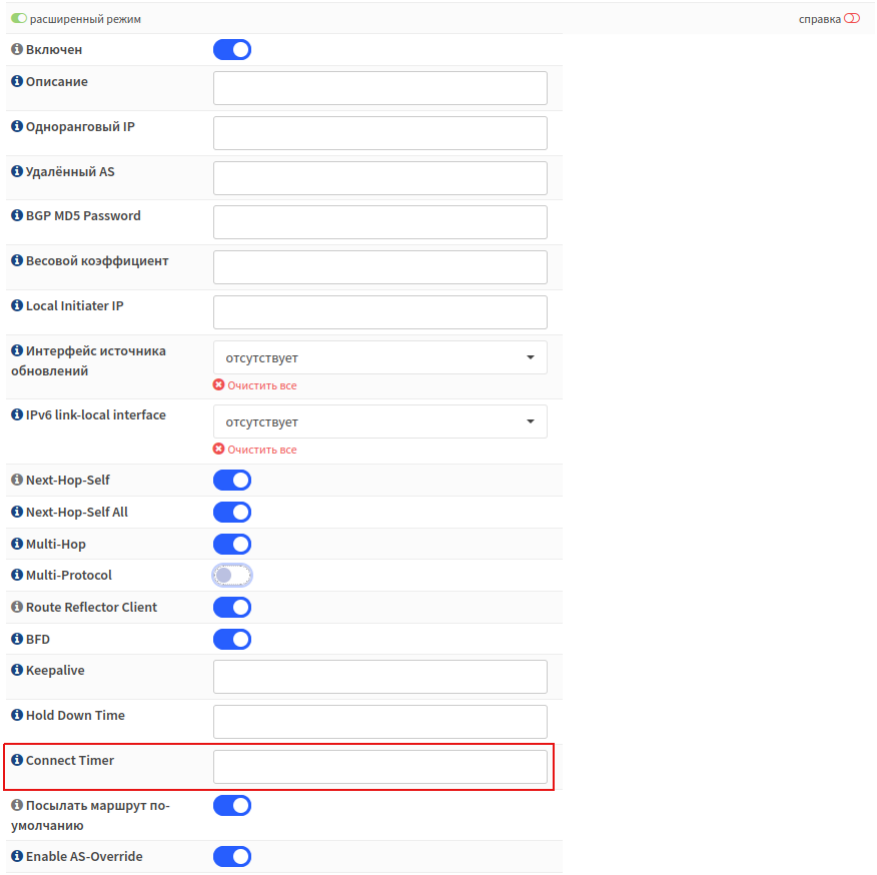


Рис. 549: Установка Connect Timer

- нажать кнопку 

для вступления проведенных настроек в силу.

2.7.6.5 BFD

Общие настройки

Для конфигурации общих настроек сервиса BFD необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации сервиса BFD;
- нажать кнопку 

для вступления проведенных настроек в силу.

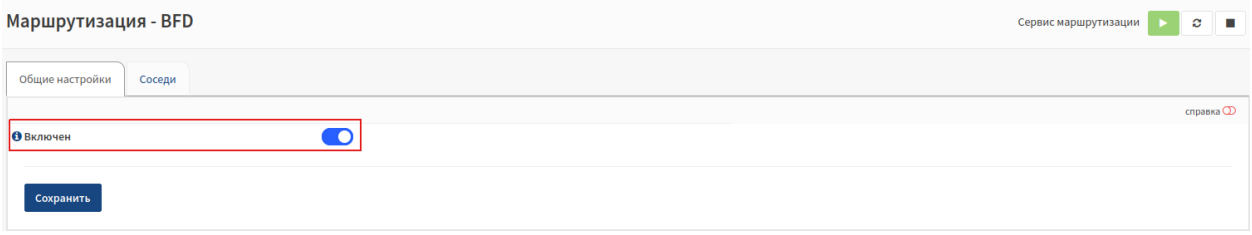


Рис. 550: Активация сервиса BFD

Соседи

Таблица соседей представлена на рисунке.

С помощью фильтров можно ограничить или расширить данные таблицы.

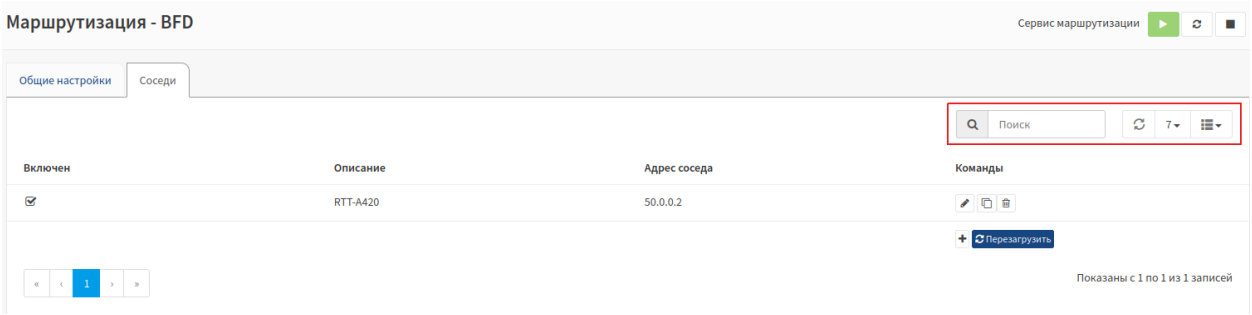


Рис. 551: Фильтры таблицы соседей

Для редактирования соседей из таблицы необходимо нажать кнопку  , расположенную напротив необходимой сети в столбце **«Команды»**.

Для обновления таблицы соседей необходимо нажать кнопку 

, расположенную в правом нижнем углу таблицы.

Для добавления нового соседа в таблицу необходимо нажать кнопку  , расположенную в правом нижнем углу таблицы.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости активации соседа;
- в поле **«Описание»** указать краткое описание соседа;
- в поле **«Одноранговый IP»** указать IP соседа;
- в поле **«Passive»** установить переключатель в случае когда пассивная сессия не будет начинать соединение,а будет ждать контрольного пакета от пира;

Для включения режима расширенных настроек необходимо установить переключатель

В режиме расширенных настроек необходимо:

- в поле **«Интервал получения»** указать минимальный интервал времени в мс, который система выделяет на прием контрольных пакетов данных;

Рис. 552: Активация соседа

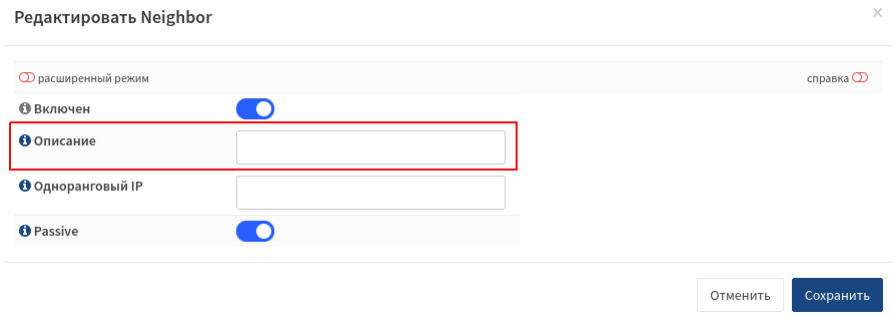


Рис. 553: Описание соседа

Рис. 554: IP соседа

Рис. 555: Активация Passive

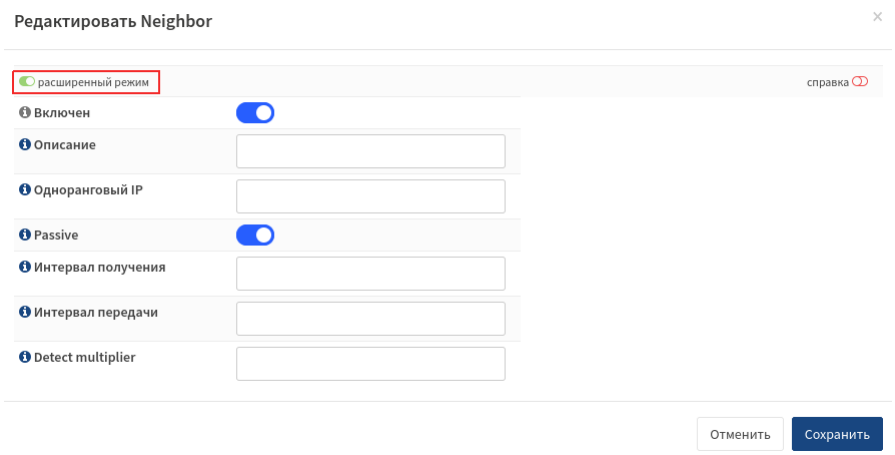


Рис. 556: Включение расширенных настроек

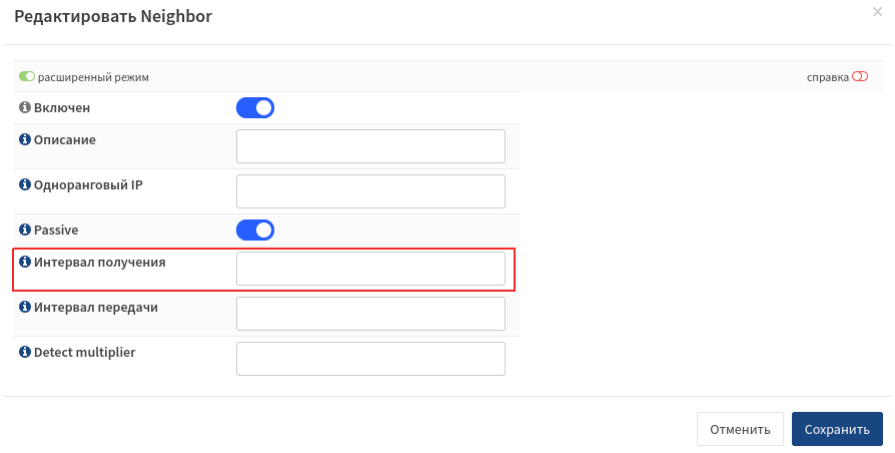


Рис. 557: Установка интервала времени

Совет

По умолчанию 300 мс

- в поле **«Интервал передачи»** указать минимальный интервал передачи (малый джиттер), который система выделяет, что бы принять контрольный пакет данных BFD;

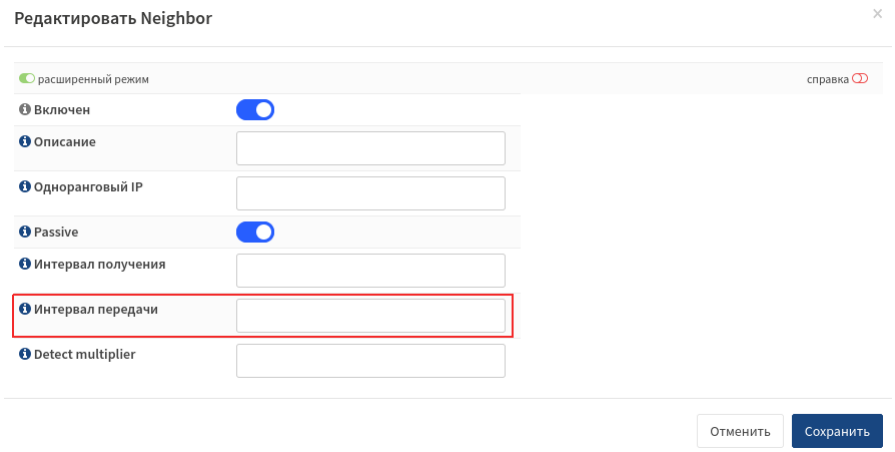


Рис. 558: Установка интервала передачи

Совет

По умолчанию 300 мс

- в поле **«Detect multiplier»** указать множитель детектирования для сокращения потерянных пакетов;

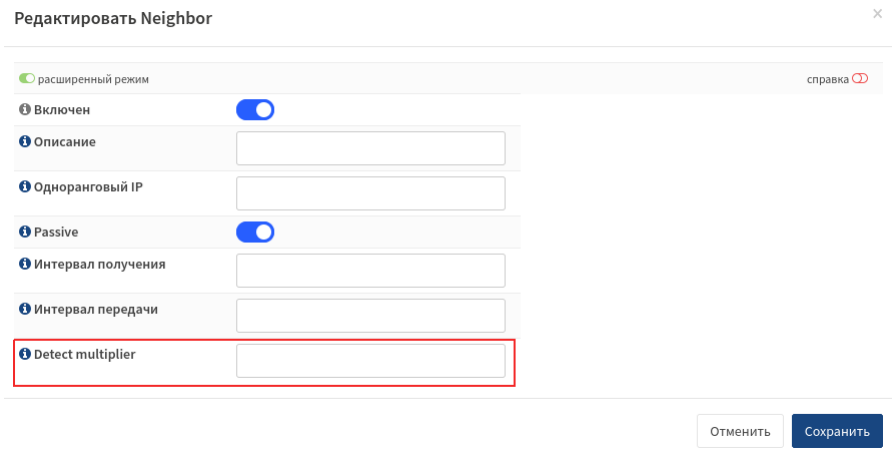


Рис. 559: Установка множителя Detect multiplier

Совет

Удаленный интервал передачи контрольных BFD пакетов будет умножен на это значение, что бы уменьшить потерю пакетов

- нажать кнопку Сохранить для вступления проведенных настроек в силу.

2.7.6.6 Диагностика

Для перехода к просмотру общей диагностики необходимо:

- нажать на вкладку **«Маршрутизация»** - **«Диагностика»** - **«Общий статус»**, расположенную в левой части списка объектов управления;

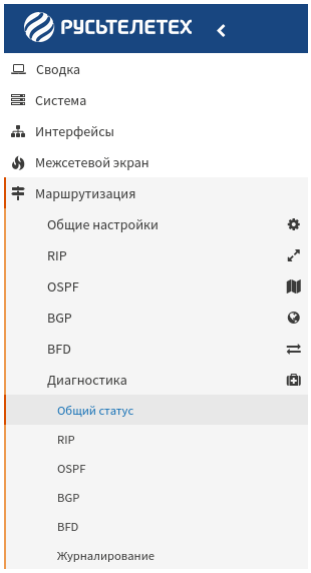


Рис. 560: Переход к просмотру общей диагностики

Для перехода к просмотру диагностики сервиса RIP необходимо:

- нажать на вкладку **«Маршрутизация»** - **«Диагностика»** - **«RIP»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру диагностики сервиса OSPF необходимо:

- нажать на вкладку **«Маршрутизация»** - **«Диагностика»** - **«OSPF»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру диагностики сервиса BGP необходимо:

- нажать на вкладку **«Маршрутизация»** - **«Диагностика»** - **«BGP»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру диагностики сервиса BFD необходимо:

- нажать на вкладку **«Маршрутизация»** - **«Диагностика»** - **«BFD»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала диагностики необходимо:

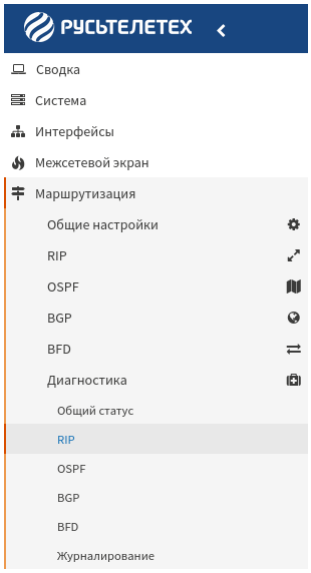


Рис. 561: Переход к просмотру диагностики сервиса RIP

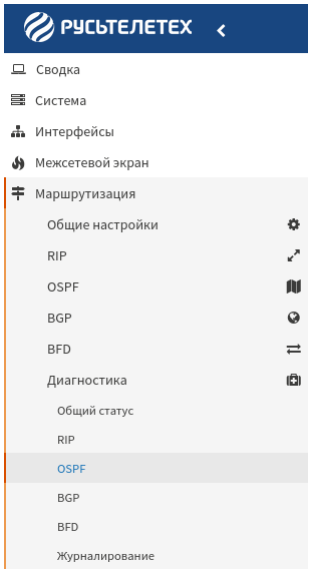


Рис. 562: Переход к просмотру диагностики сервиса OSPF

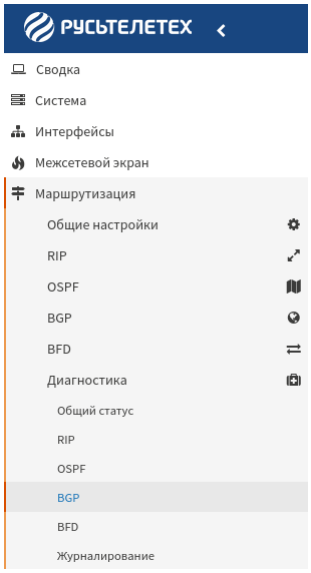


Рис. 563: Переход к просмотру диагностики сервиса BGP

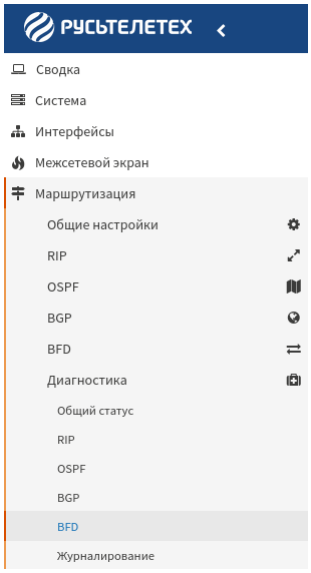


Рис. 564: Переход к просмотру диагностики сервиса BFD

- нажать на вкладку **«Маршрутизация»** - **«Диагностика»** - **«Журналирование»**, расположенную в левой части списка объектов управления;

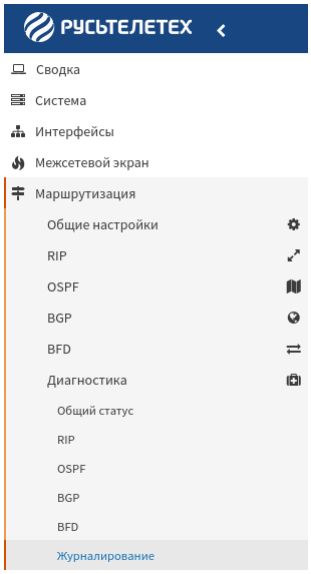


Рис. 565: Переход к просмотру журнала диагностики

Общий статус

Раздел **«Общий статус»** содержит общие данные о диагностике системы.

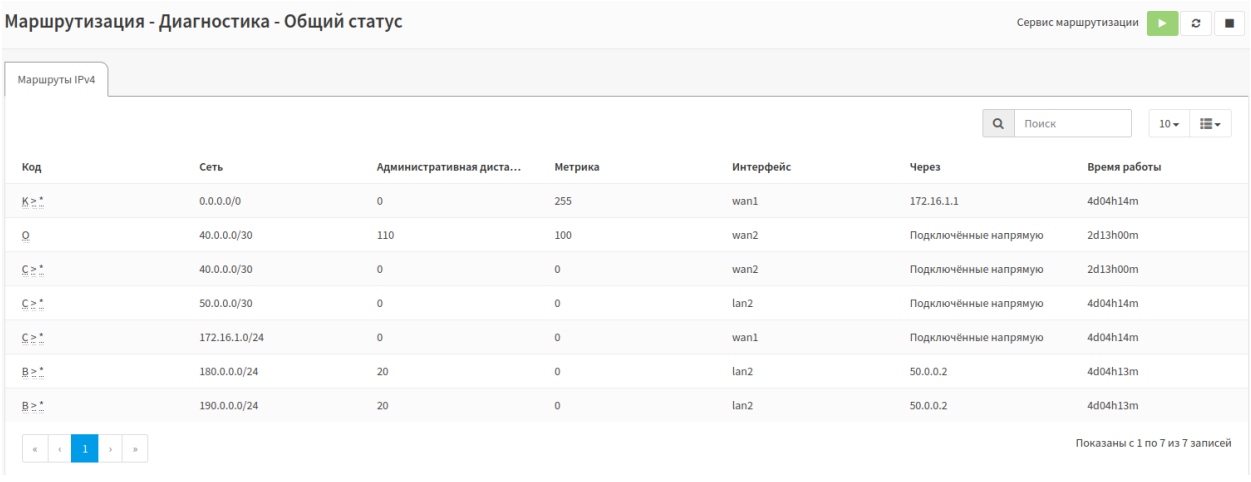


Рис. 566: Общий статус

С помощью фильтров можно ограничить или расширить данные таблицы.

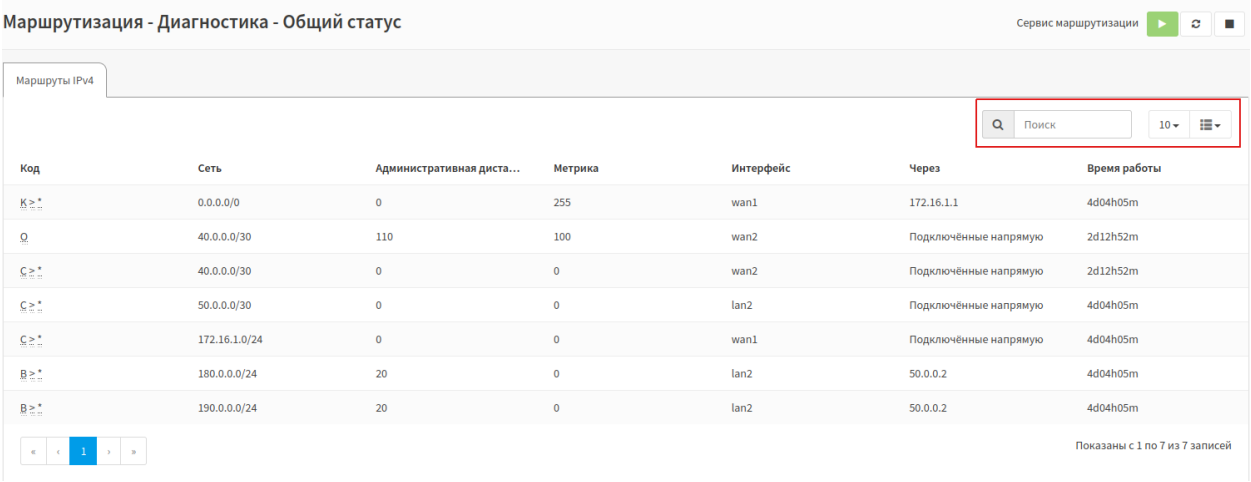


Рис. 567: Фильтры таблицы

RIP

Раздел **«RIP»** содержит данные о диагностике сервиса RIP.

Рис. 568: Сервис RIP

OSPF

Обзор

Таблица маршрутизации

С помощью фильтров можно ограничить или расширить данные таблицы.

База данных

Сосед

С помощью фильтров можно ограничить или расширить данные таблицы.

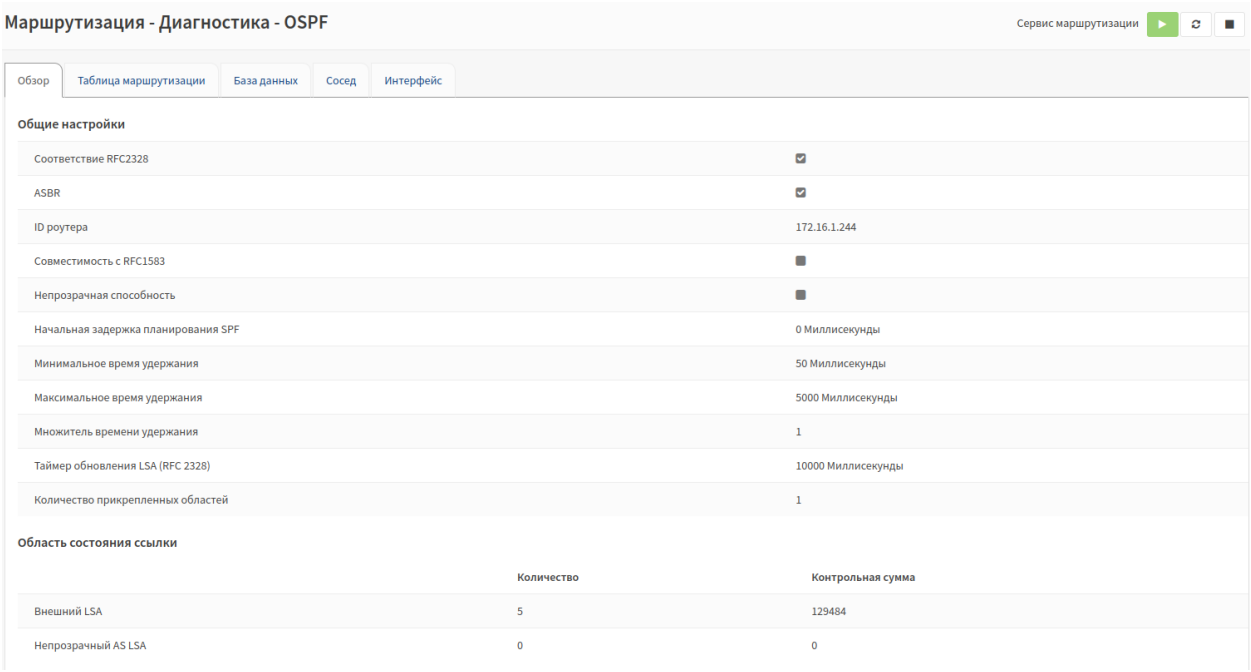


Рис. 569: Вкладка Обзор

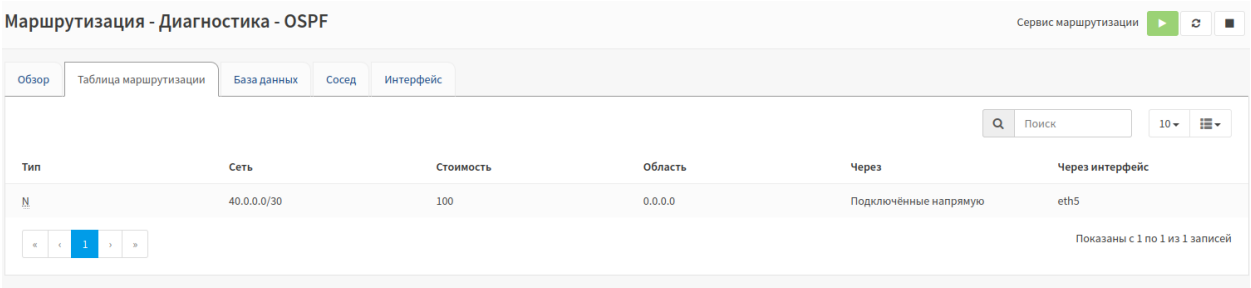


Рис. 570: Таблица маршрутизации

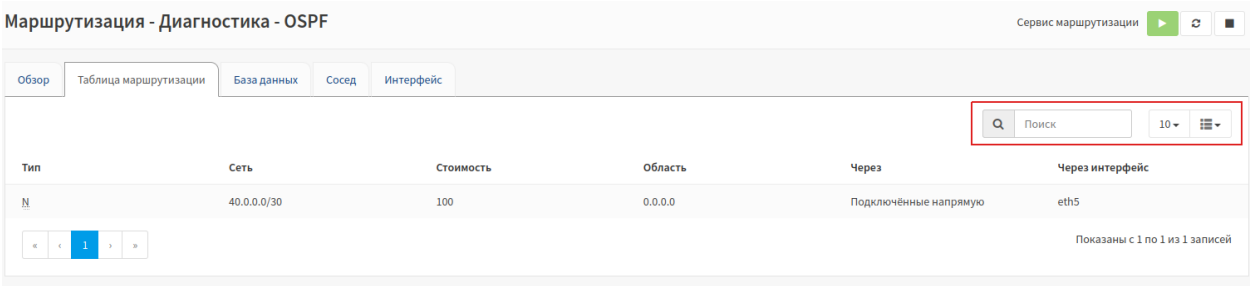


Рис. 571: Фильтры таблицы

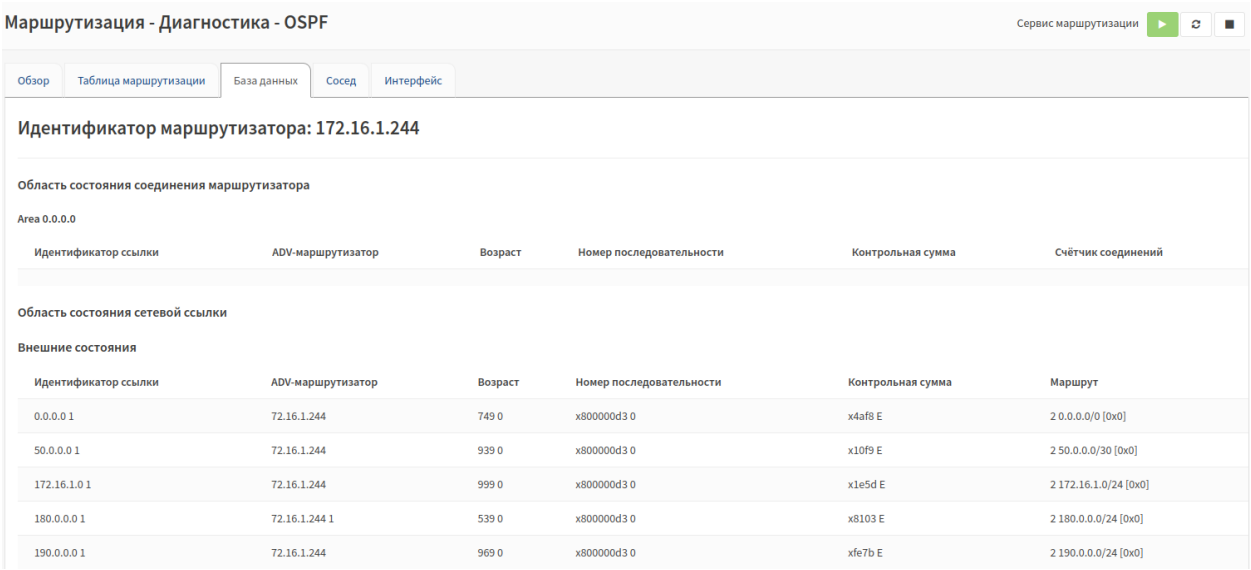


Рис. 572: База данных

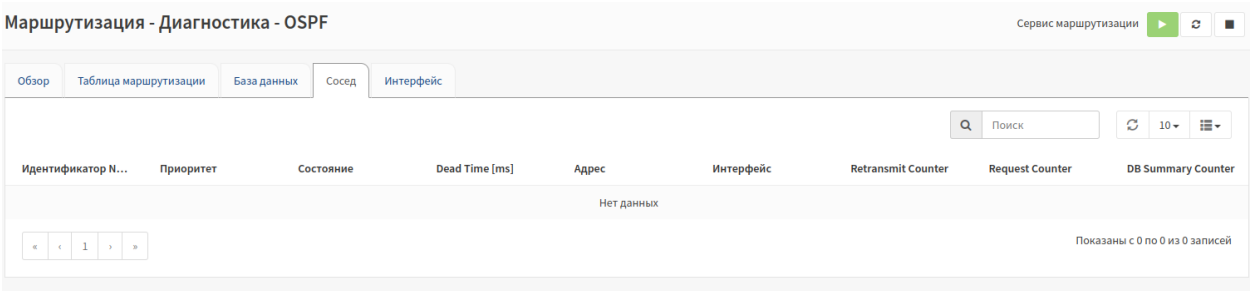


Рис. 573: Сосед

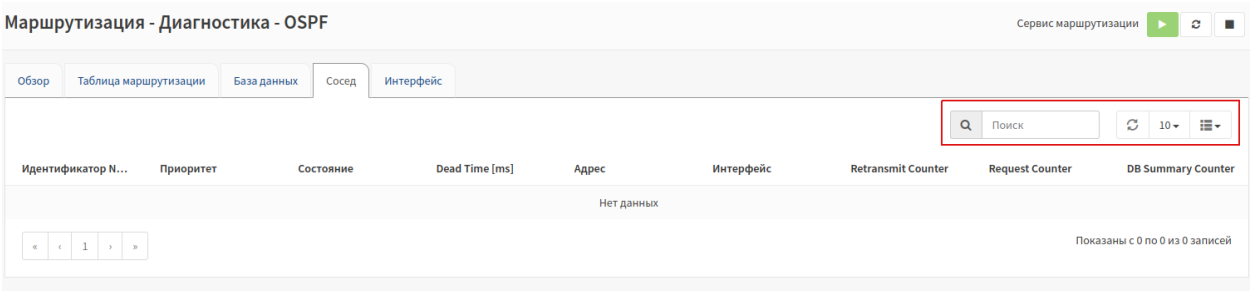


Рис. 574: Фильтры таблицы

Интерфейс

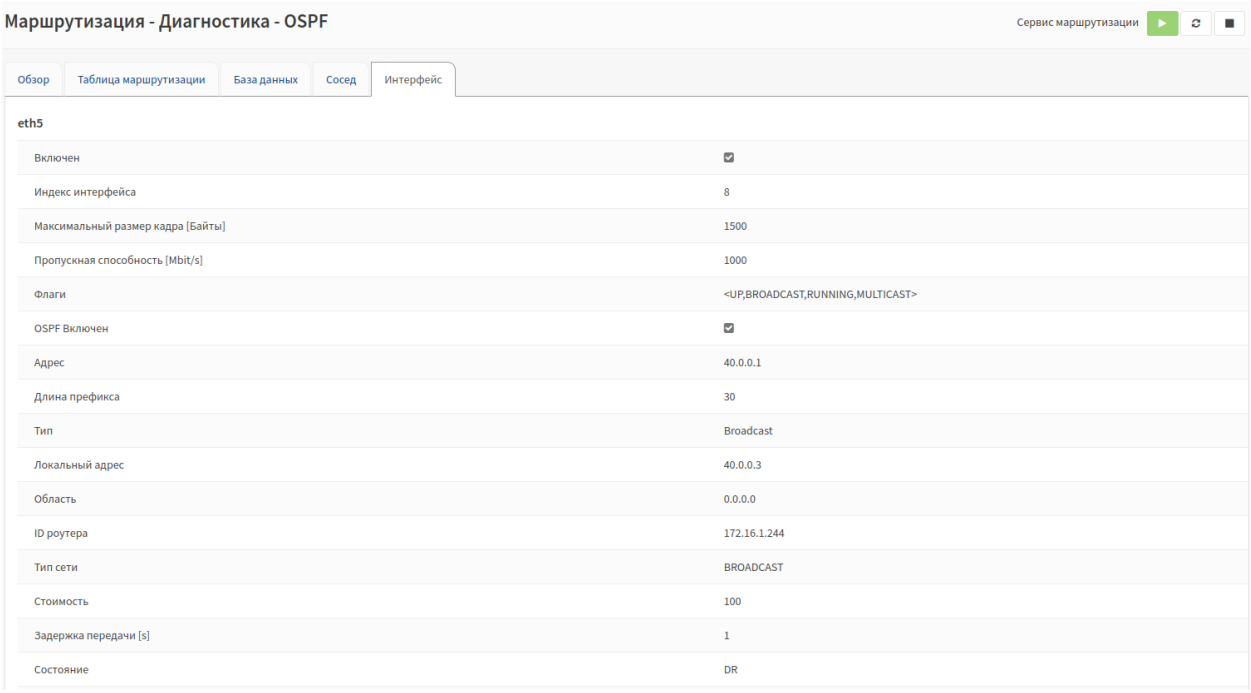


Рис. 575: Интерфейс

BGP

IPv4 таблица маршрутизации

С помощью фильтров можно ограничить или расширить данные таблицы.

IPv6 таблица маршрутизации

С помощью фильтров можно ограничить или расширить данные таблицы.

Соседи

Сводка

BFD

С помощью фильтров можно ограничить или расширить данные таблицы.

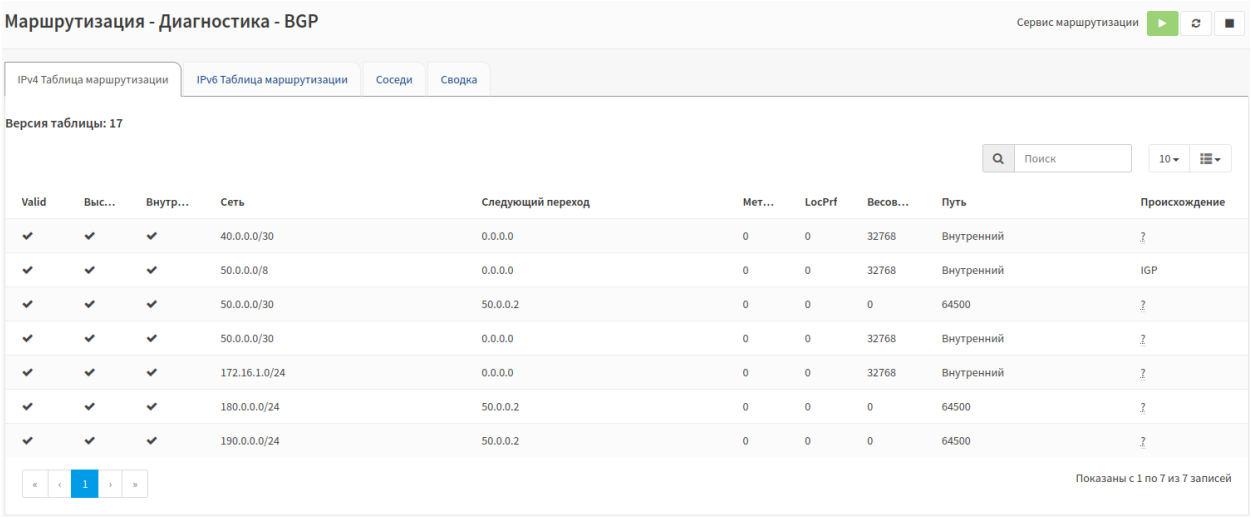


Рис. 576: IPv4 таблица маршрутизации

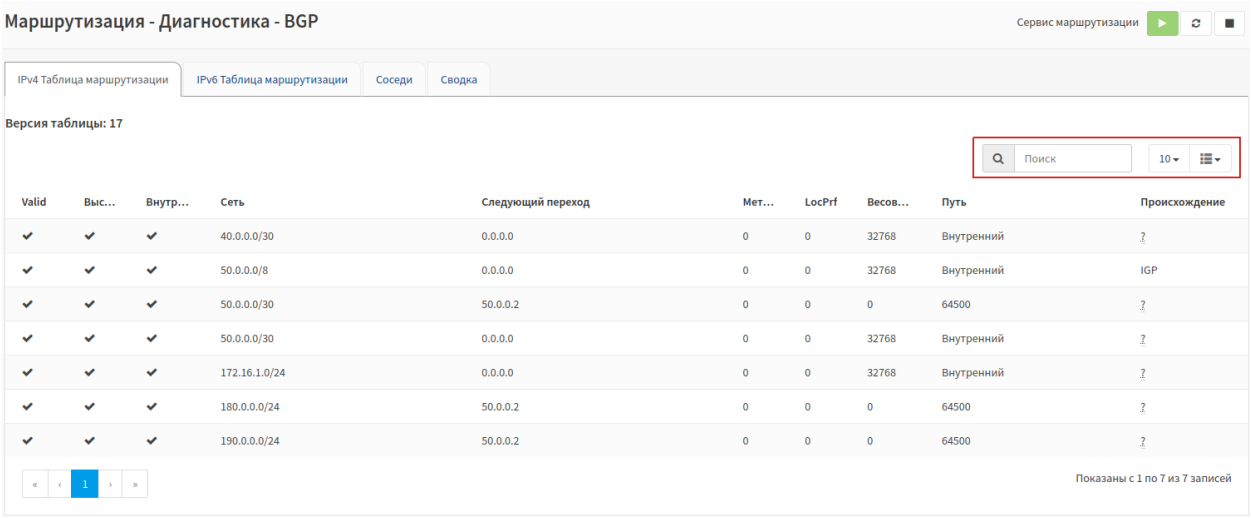


Рис. 577: Фильтры таблицы

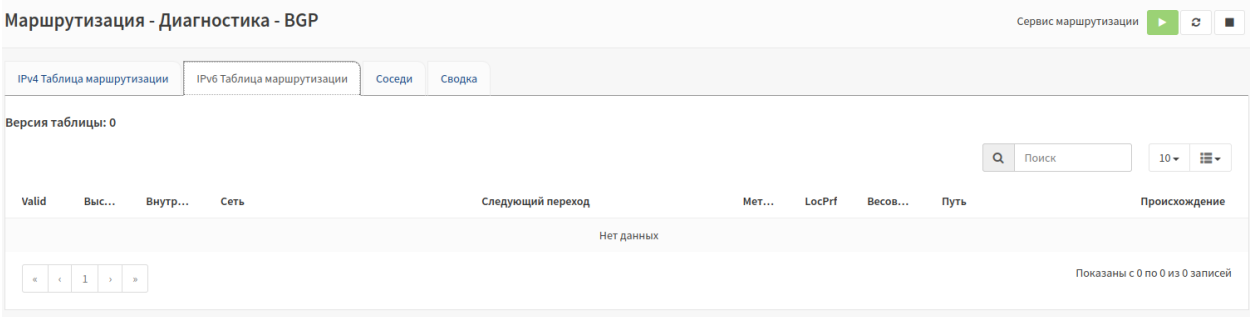


Рис. 578: IPv6 таблица маршрутизации

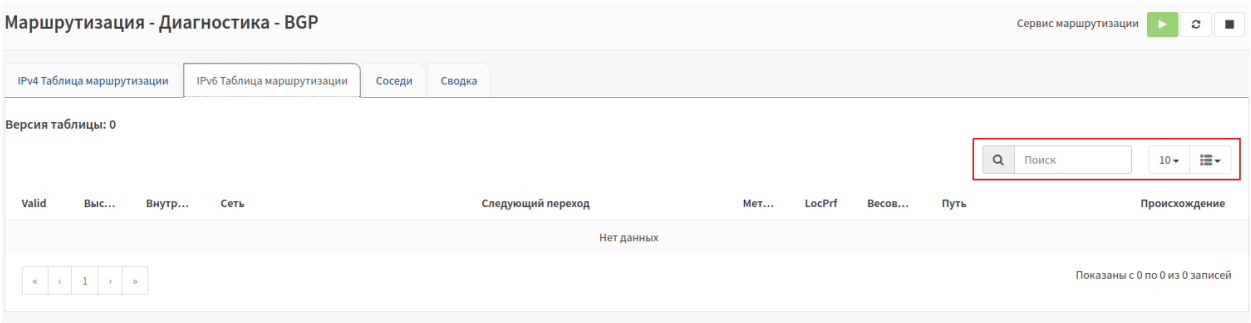


Рис. 579: Фильтры таблицы

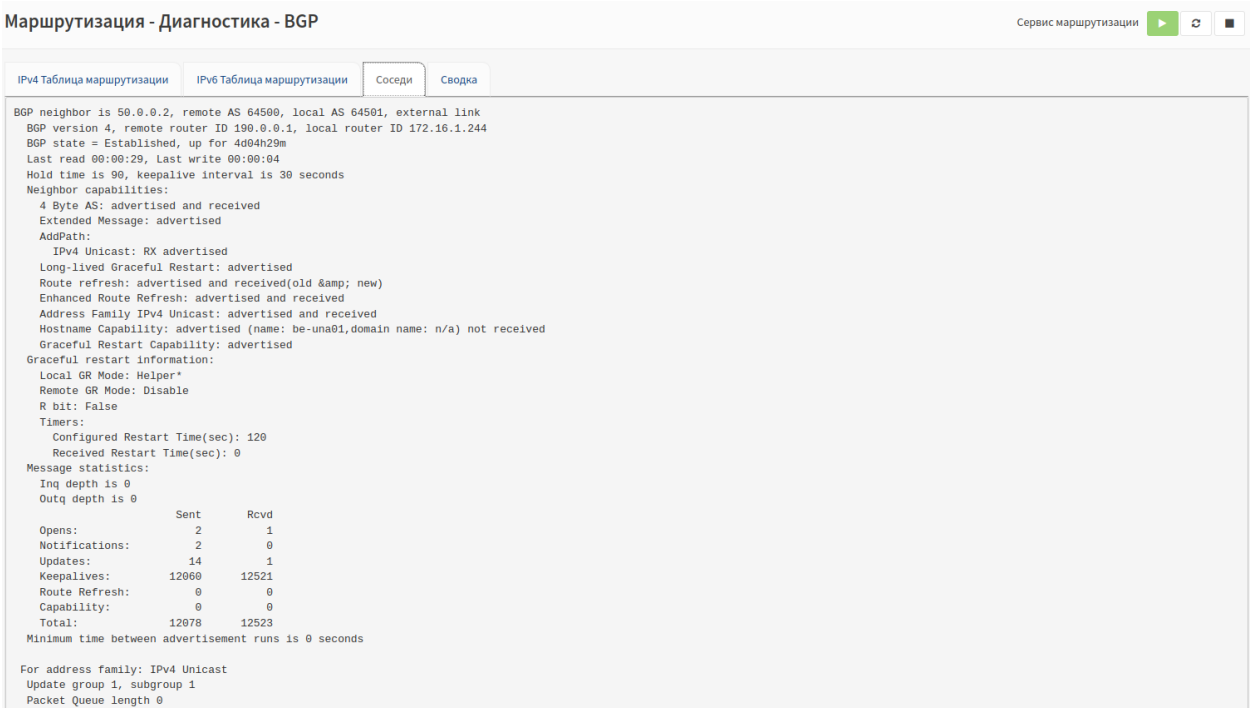


Рис. 580: Соседи

Рис. 581: Сводка

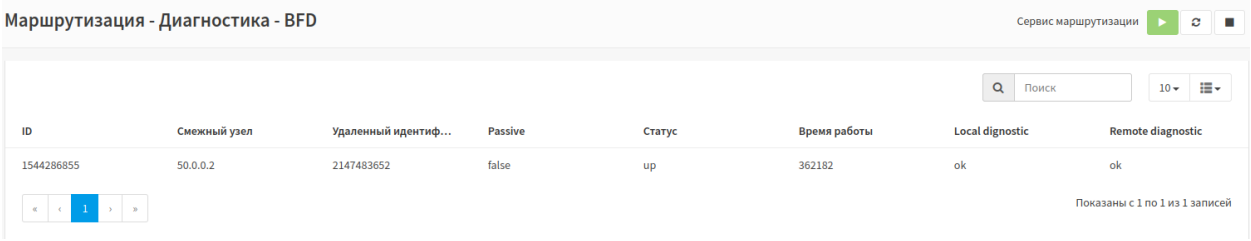


Рис. 582: Сервис BFD

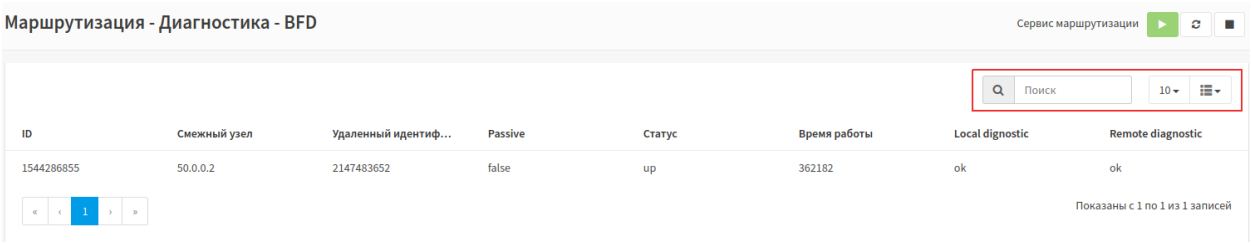


Рис. 583: Фильтры таблицы

Журналирование

RIP

Раздел **«RIP»** содержит журнал сервиса RIP.

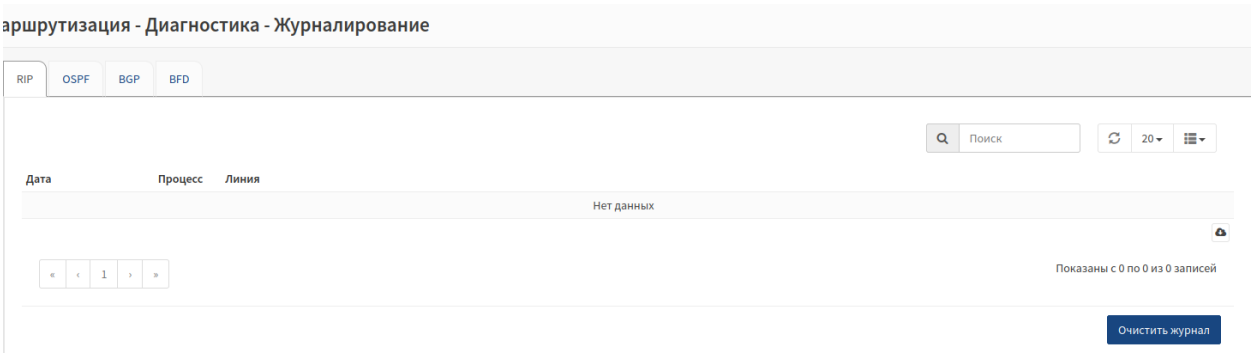


Рис. 584: Журнал сервиса RIP

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

Рис. 585: Фильтры журнала

OSPF

Раздел **«OSPF»** содержит журнал сервиса OSPF.

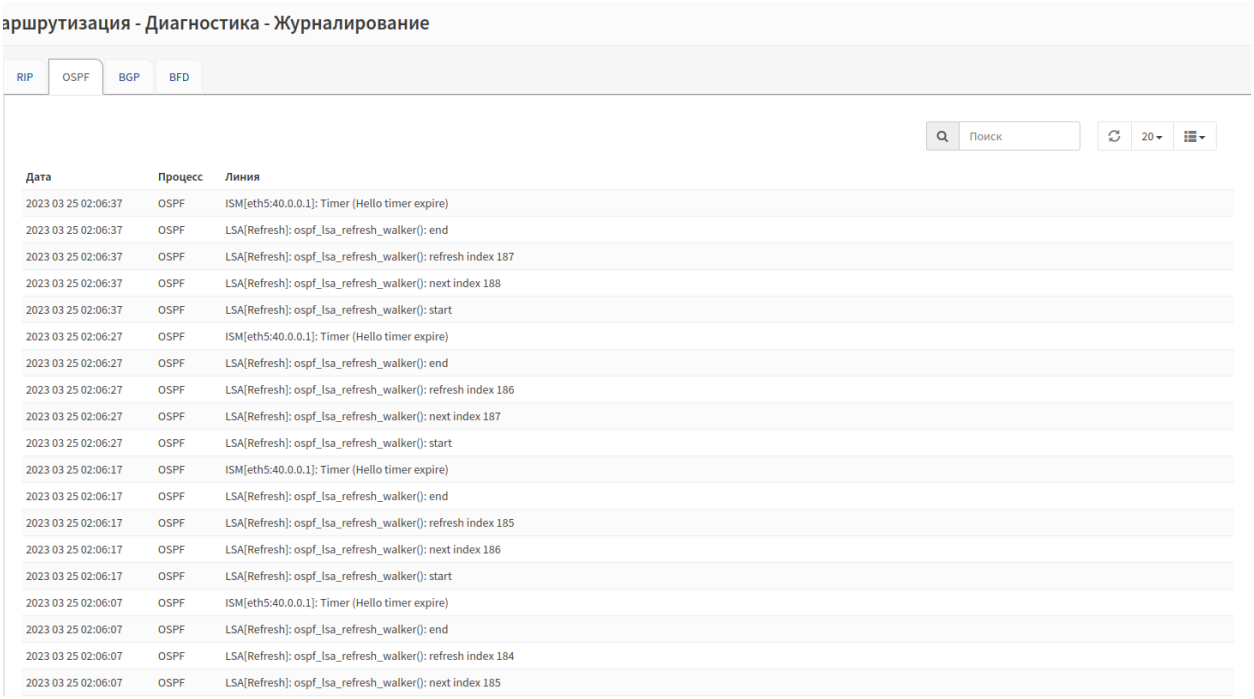


Рис. 586: Журнал сервиса OSPF

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

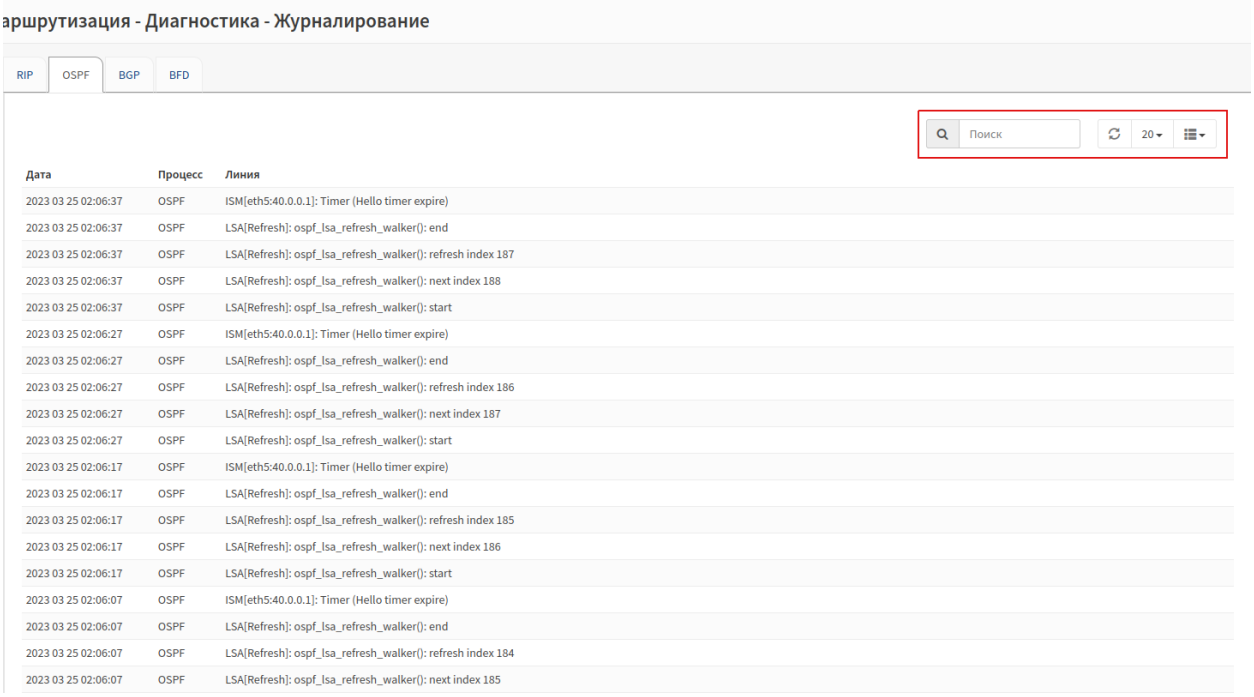


Рис. 587: Фильтры журнала

, расположенную в правом нижнем углу журнала.

BGP

Раздел **«BGP»** содержит журнал сервиса BGP.

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

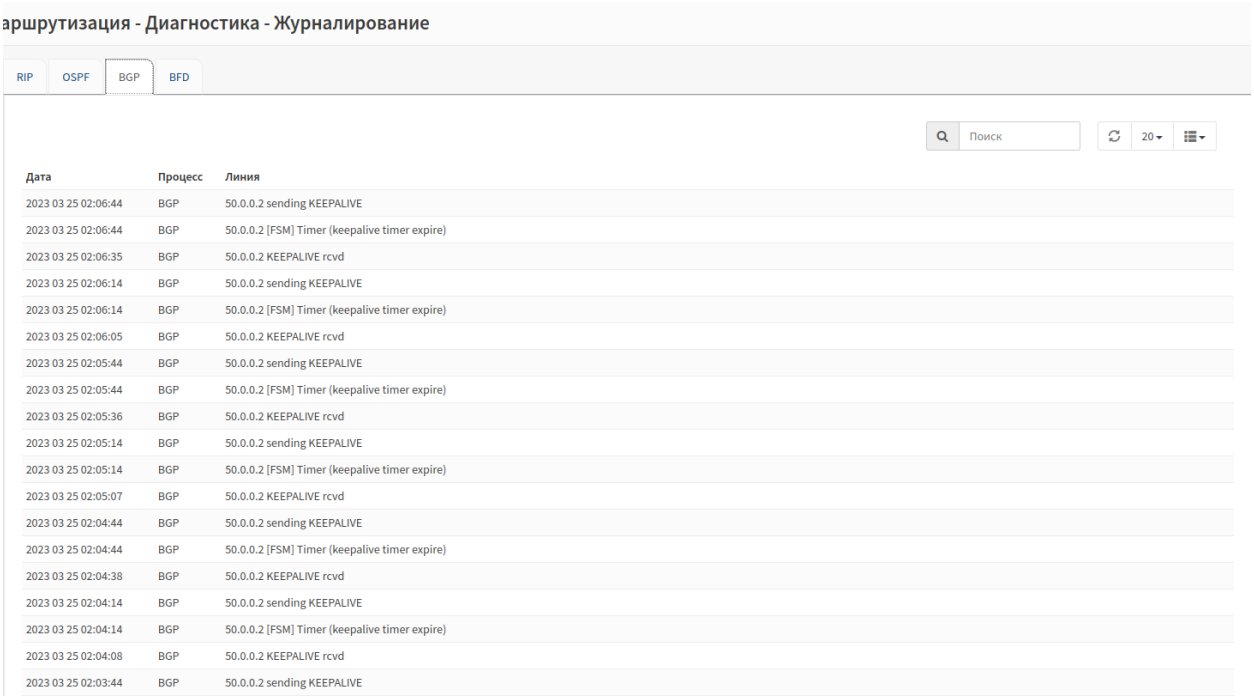


Рис. 588: Журнал сервиса BGP

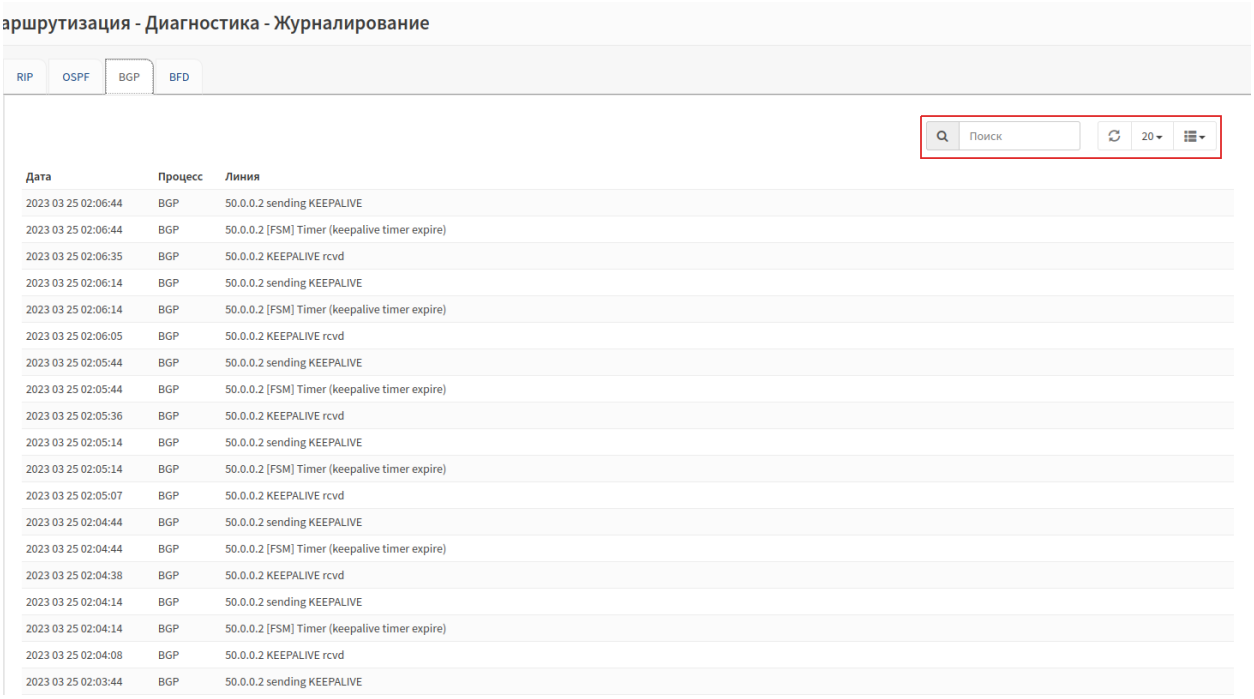


Рис. 589: Фильтры журнала

BFD

Раздел **«BFD»** содержит журнал сервиса BFD.

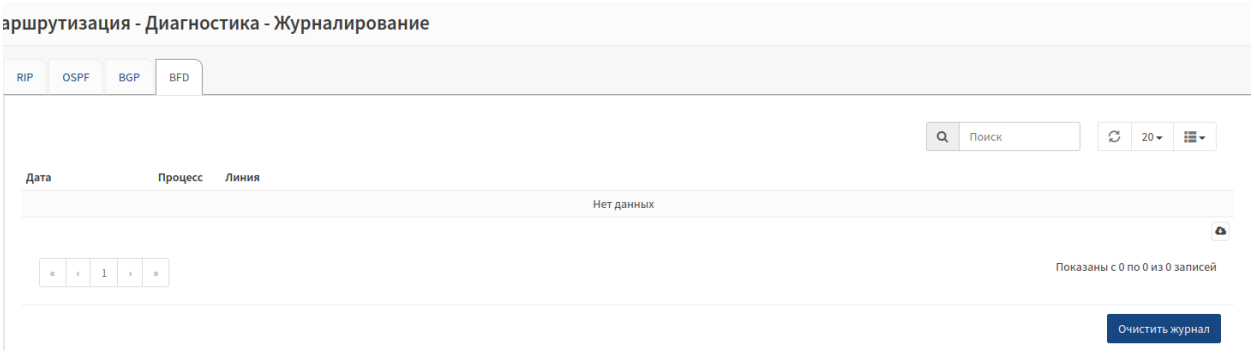


Рис. 590: Журнал сервиса BFD

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Рис. 591: Фильтры журнала

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

2.7.7 VPN

Для перехода к созданию зашифрованных каналов типа сервер-клиенты необходимо:

- нажать на вкладку **«VPN»** - **«OpenVPN»** - **«Серверы/клиенты»**, расположенную в левой части списка объектов управления;

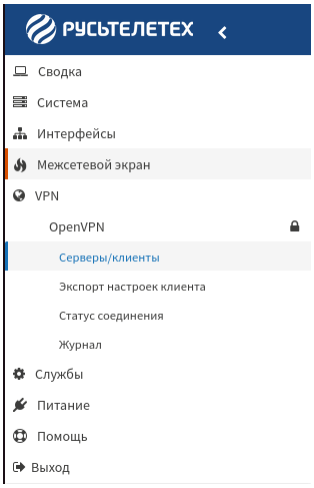


Рис. 592: Переход к созданию зашифрованных каналов типа сервер-клиенты

- в правой части экрана появиться таблица Серверы/клиенты;

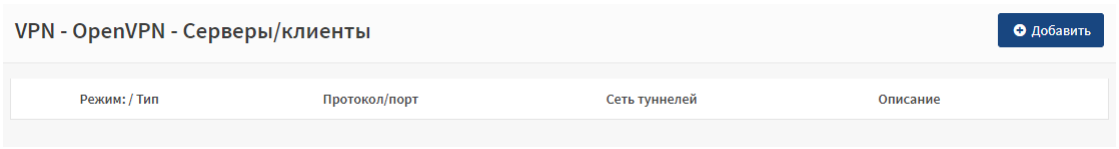


Рис. 593: Таблица Серверы/клиенты

- нажать кнопку **«Добавить»** 

для добавления нового канала Серверы/клиенты.

Для перехода к экспорту настроек клиента необходимо:

- нажать на вкладку **«VPN»** - **«OpenVPN»** - **«Экспорт настроек клиента»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру статуса соединения необходимо:

- нажать на вкладку **«VPN»** - **«OpenVPN»** - **«Статус соединения»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала VPN необходимо:

- нажать на вкладку **«VPN»** - **«OpenVPN»** - **«Журнал»**, расположенную в левой части списка объектов управления;

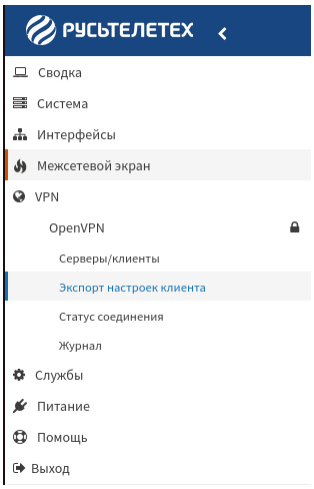


Рис. 594: Переход к экспорту настроек клиента

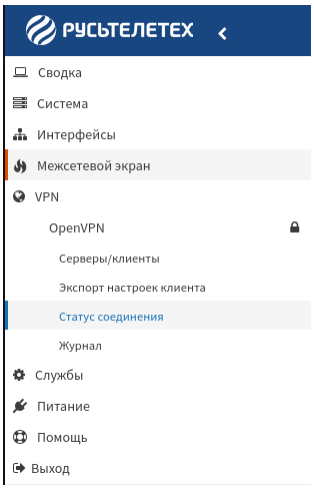


Рис. 595: Переход к просмотру статуса соединения

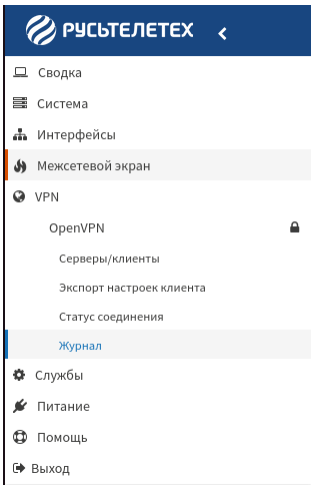


Рис. 596: Переход к просмотру журнала VPN

2.7.7.1 Серверы/клиенты

Общая информация

Для создания зашифрованного канала типа сервер-клиенты необходимо:

- в поле **«Отключить»** установить переключатель в случае необходимости отключить сервер, не удаляя его из списка;

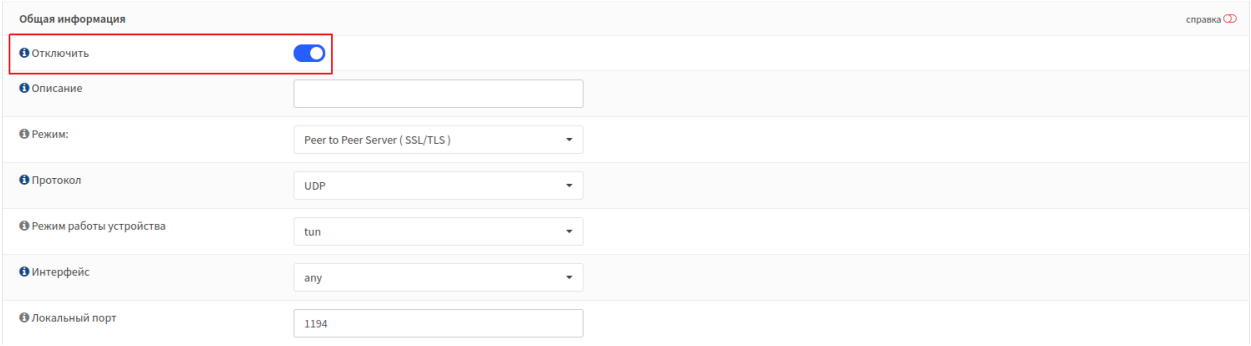


Рис. 597: Отключение сервера, не удаляя его из списка

- в поле **«Описание»** ввести краткое описание зашифрованного канала;

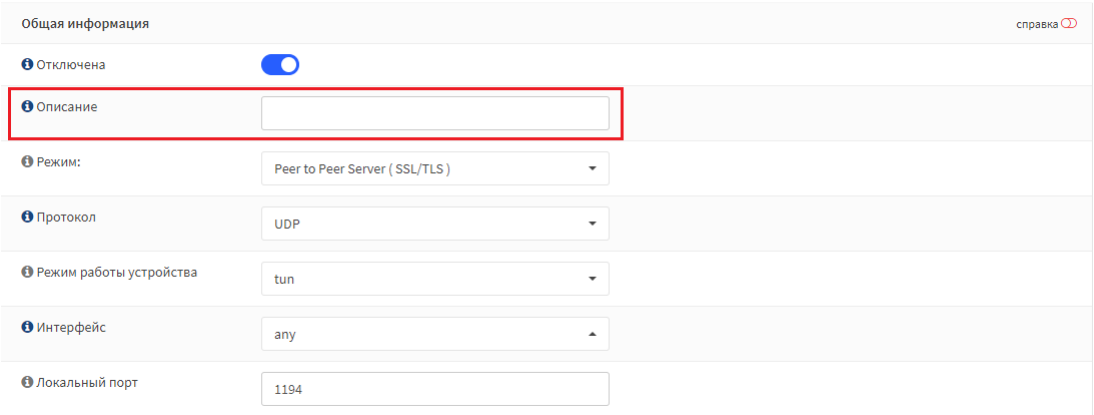


Рис. 598: Описание зашифрованного канала

Режим Peer to Peer Server (SSL/TLS)

Для настройки режима Peer to Peer Server (SSL/TLS) необходимо:

- в поле **«Режим»** выбрать режим **«Peer to Peer Server (SSL/TLS)»** из выпадающего списка;
- в поле **«Протокол»** выбрать из выпадающего списка необходимый протокол, соответствующий таблице;

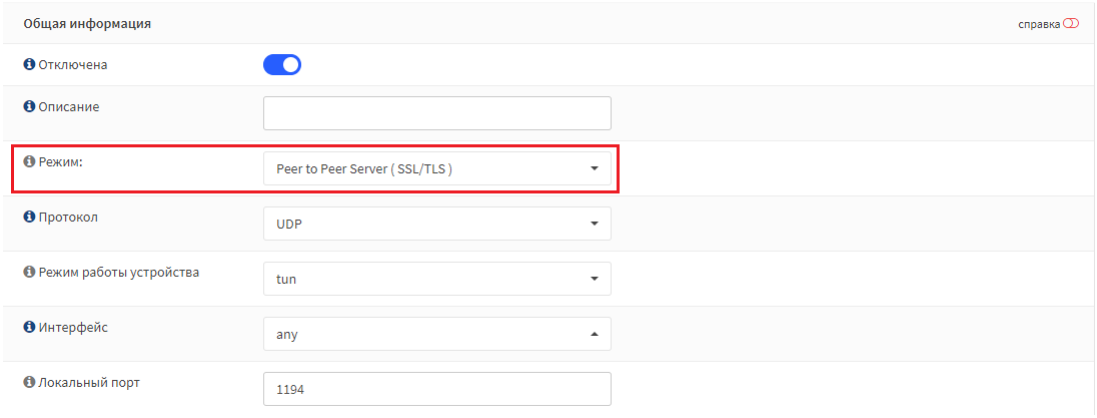


Рис. 599: Выбор режима Peer to Peer Server (SSL/TLS)

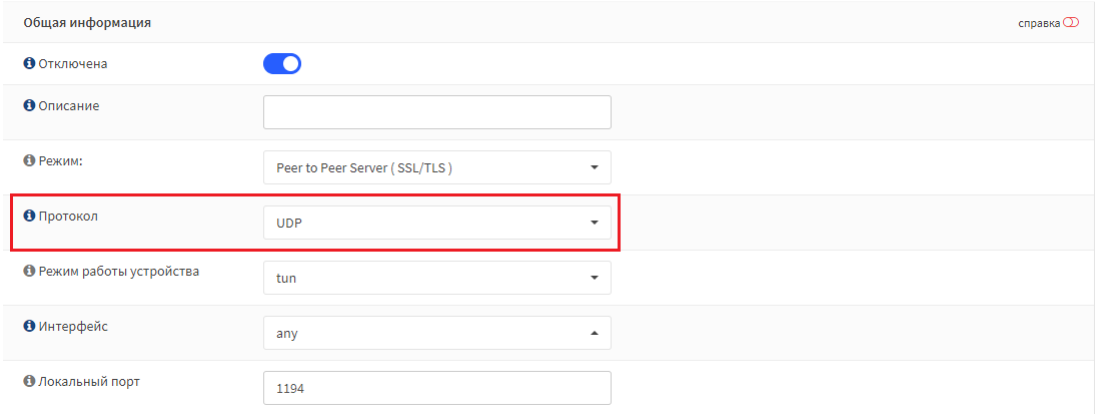


Рис. 600: Выбор протокола

Таблица 142: Выбор протокола

Протокол
UDP
TCP

Примечание

Обратите внимание, что использование обоих семейств с UDP/TCP не работает с явным интерфейсом, поскольку OpenVPN не поддерживает прослушивание более одного указанного IP-адреса. В этом случае в настоящее время предполагается IPv4.

- в поле **«Режим работы устройства»** выбрать из выпадающего списка необходимый режим работы, соответствующий таблице;

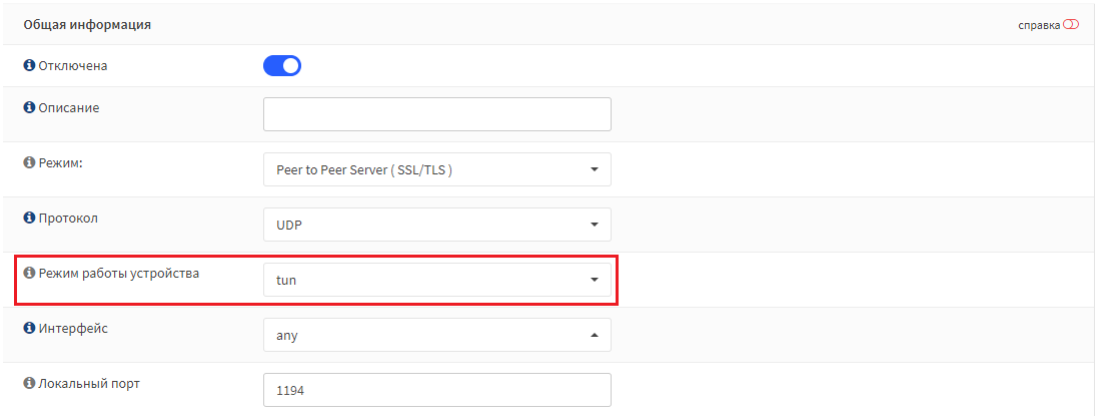


Рис. 601: Выбор режима работы устройства

Таблица 143: Выбор режима работы устройства

Режим работы устройства
tun
tap

- в поле **«Интерфейс»** выбрать из выпадающего списка необходимый интерфейс;

Примечание

При выборе любого из них в сочетании с UDP мы будем предполагать, что сервер используется в многосетевом режиме. Это имеет некоторые небольшие последствия для производительности, чтобы обеспечить правильный поиск обратного адреса

- в поле **«Локальный порт»** установить числовое значение порта;

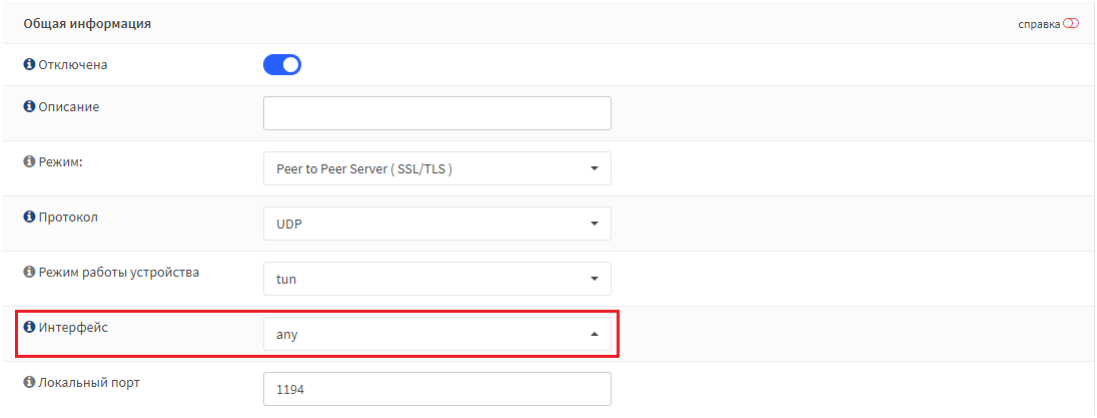


Рис. 602: Выбор интерфейса

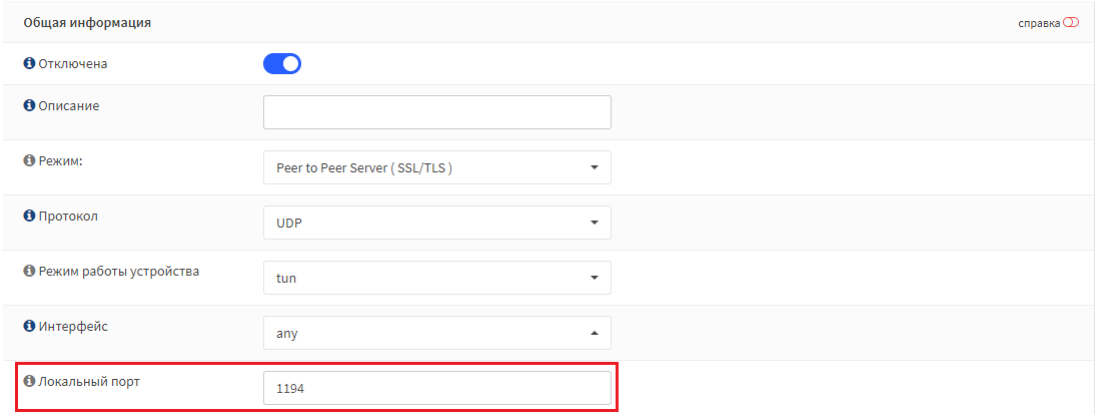


Рис. 603: Значение порта

Режим Peer to Peer Client (SSL/TLS)

Для настройки режима Peer to Peer Client (SSL/TLS) необходимо:

- в поле **«Режим»** выбрать режим **«Peer to Peer Client (SSL/TLS)»** из выпадающего списка;

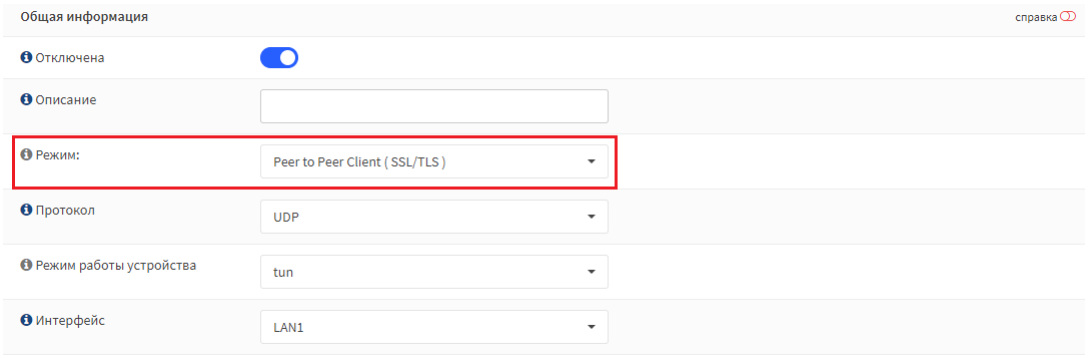


Рис. 604: Выбор режима Peer to Peer Client (SSL/TLS)

- в поле **«Протокол»** выбрать из выпадающего списка необходимый протокол, соответствующий таблице;

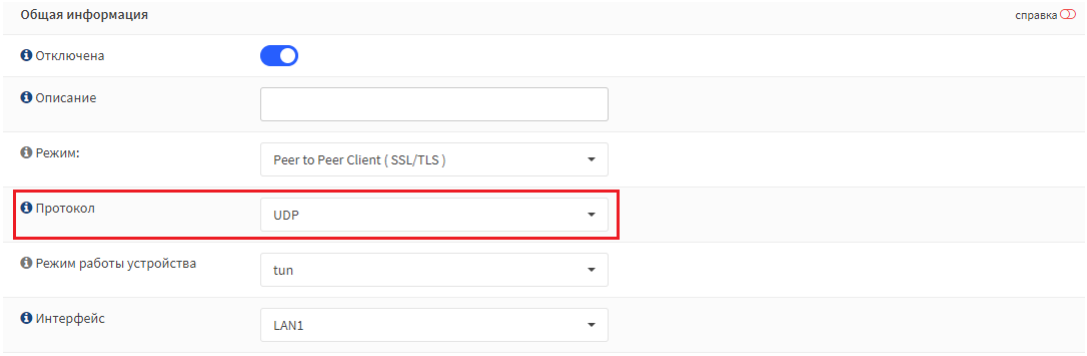


Рис. 605: Выбор протокола

Таблица 144: Выбор протокола

Протокол
UDP
TCP

Примечание

Обратите внимание, что использование обоих семейств с UDP/TCP не работает с явным интерфейсом, поскольку OpenVPN не поддерживает прослушивание более одного указанного IP-адреса. В этом случае в настоящее время предполагается IPv4

- в поле **«Режим работы устройства»** выбрать из выпадающего списка необходимый режим работы, соответствующий таблице;

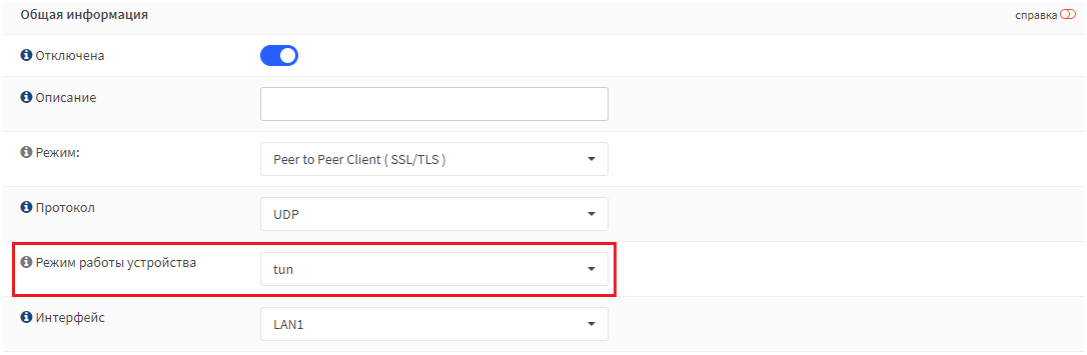


Рис. 606: Выбор режима работы устройства

Таблица 145: Выбор режима работы устройства

Режим работы устройства
tun
tap

- в поле **«Интерфейс»** выбрать из выпадающего списка необходимый интерфейс;

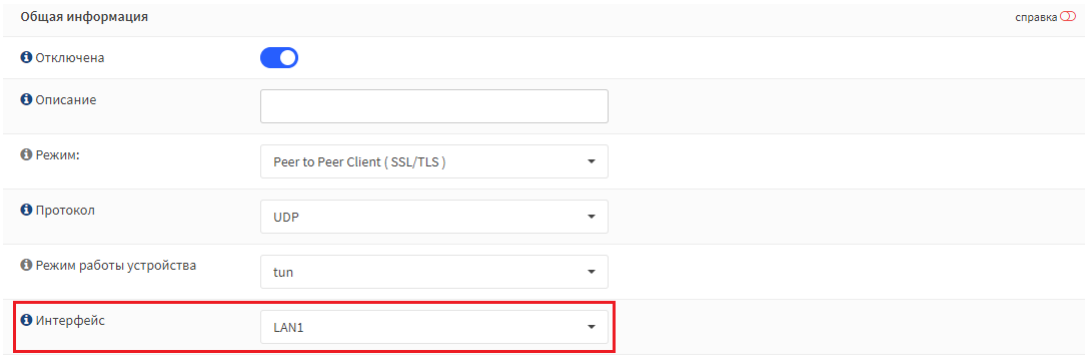


Рис. 607: Выбор интерфейса

Примечание

При выборе любого из них в сочетании с UDP мы будем предполагать, что сервер используется в многосетевом режиме. Это имеет некоторые небольшие последствия для производительности, чтобы обеспечить правильный поиск обратного адреса

- в поле **«Удаленный сервер»** в колонке **«Хост или адрес»** и **«Порт»** ввести соответствующие значения, либо установить переключатель в случае необходимости выбора удаленного сервера случайным образом;
- в поле **«Локальный порт»** установить числовое значение порта;
- в поля **«Имя пользователя»** и **«Пароль»** ввести имя пользователя и пароль;

Примечание

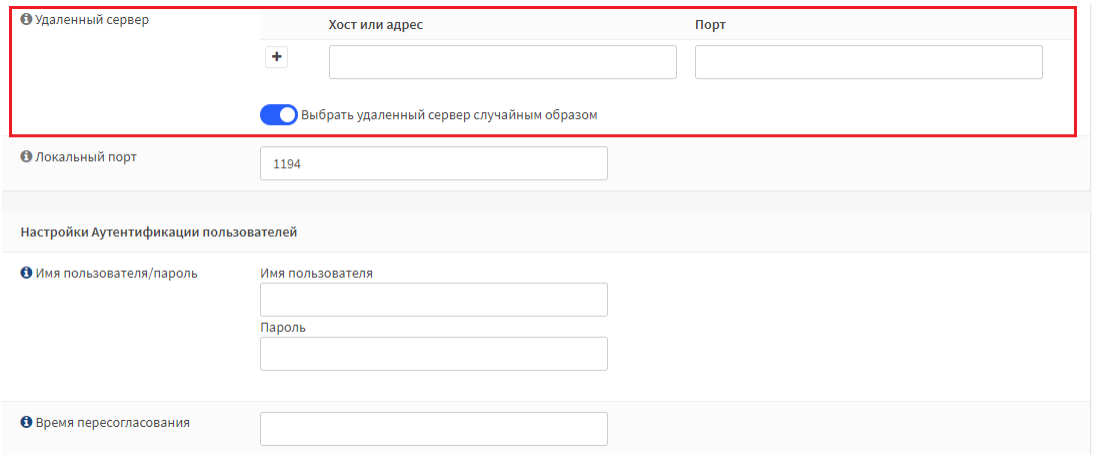


Рис. 608: Выбор удаленного сервера

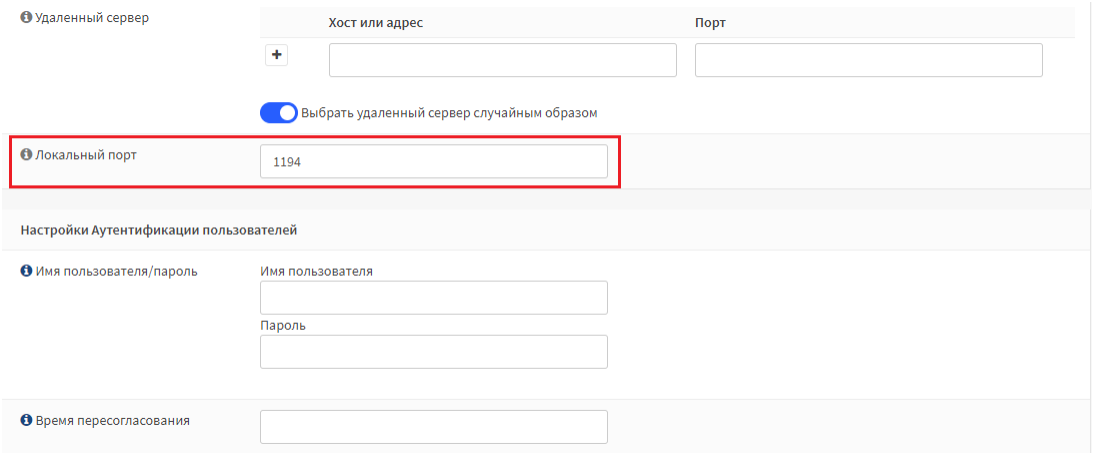


Рис. 609: Значение порта

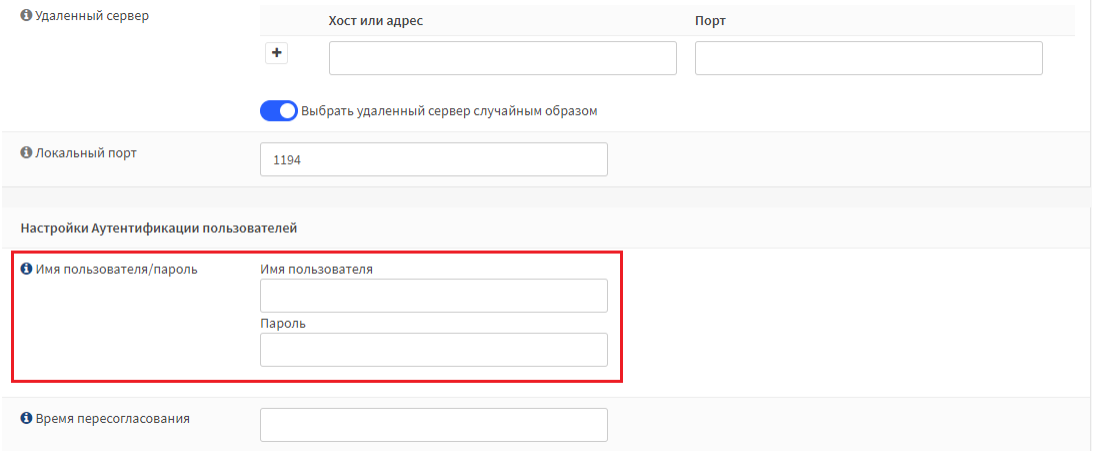


Рис. 610: Имя пользователя/пароль

Оставьте пустым, когда не требуется имя пользователя и пароль

- в поле **«Время пересогласования»** ввести числовое значение пересогласования ключа канала данных после n секунд;

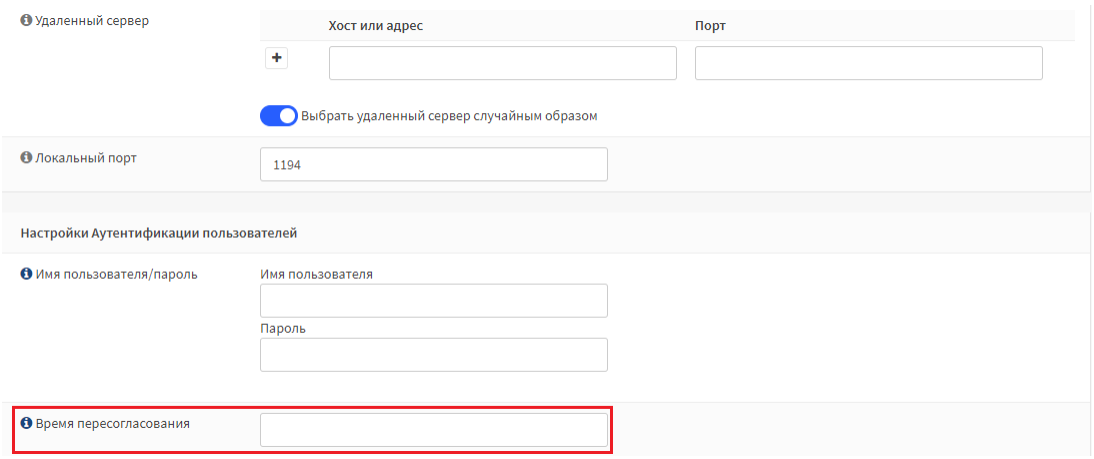


Рис. 611: Значение времени пересогласования

Примечание

По умолчанию 3600. Установите 0, чтобы отключить.

Режим Удаленный доступ (SSL/TLS)

Для настройки режима Удаленный доступ (SSL/TLS) необходимо:

- в поле **«Режим»** выбрать режим **«Удаленный доступ (SSL/TLS)»** из выпадающего списка;

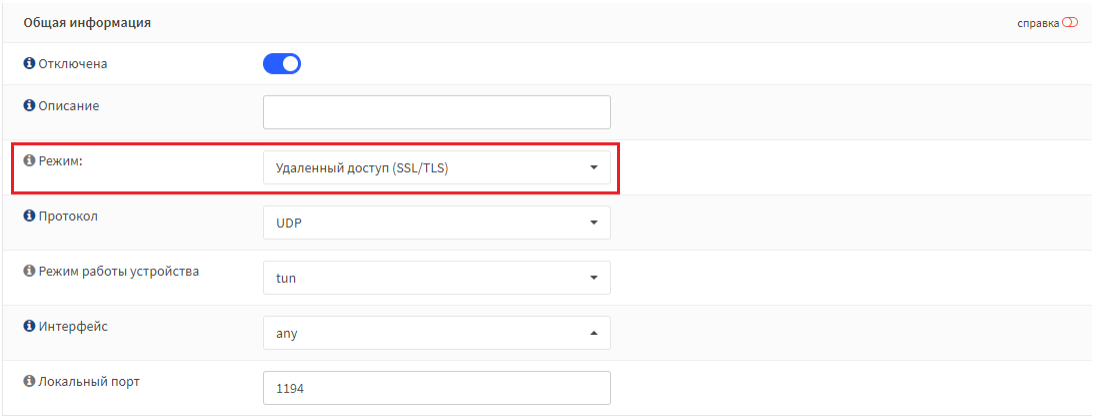


Рис. 612: Выбор режима Удаленный доступ (SSL/TLS)

- в поле **«Протокол»** выбрать из выпадающего списка необходимый протокол, соответствующий таблице;

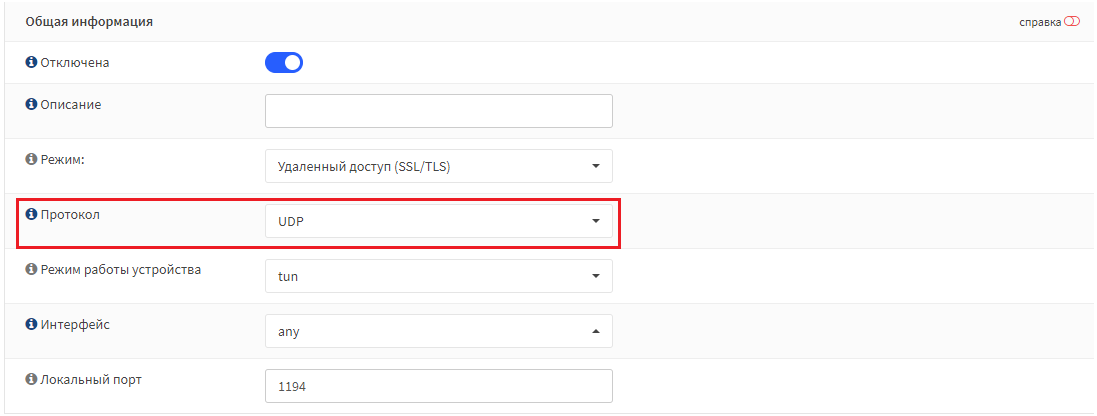


Рис. 613: Выбор протокола

Таблица 146: Выбор протокола

Протокол
UDP
TCP

Примечание

Обратите внимание, что использование обоих семейств с UDP/TCP не работает с явным интерфейсом, поскольку OpenVPN не поддерживает прослушивание более одного указанного IP-адреса. В этом случае в настоящее время предполагается IPv4

- в поле **«Режим работы устройства»** выбрать из выпадающего списка необходимый режим работы, соответствующий таблице;

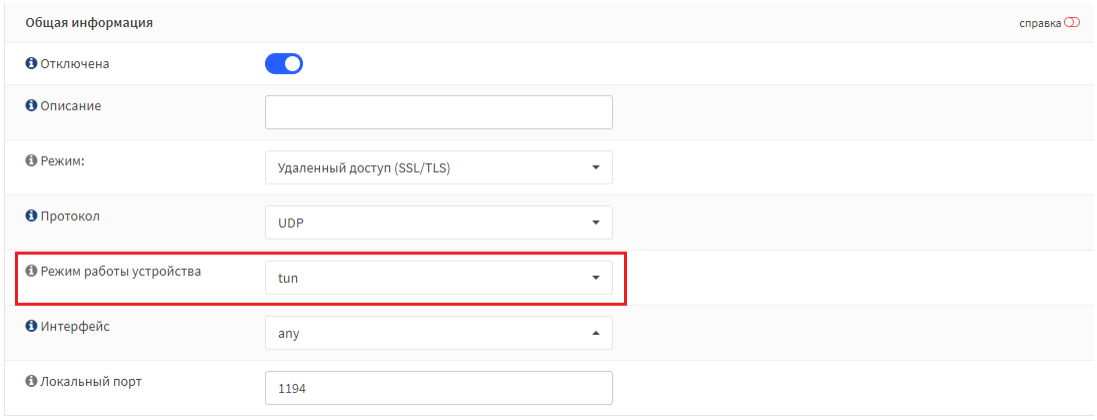


Рис. 614: Выбор режима работы устройства

Таблица 147: Выбор режима работы устройства

Режим работы устройства
tun
tap

- в поле **«Интерфейс»** выбрать из выпадающего списка необходимый интерфейс;

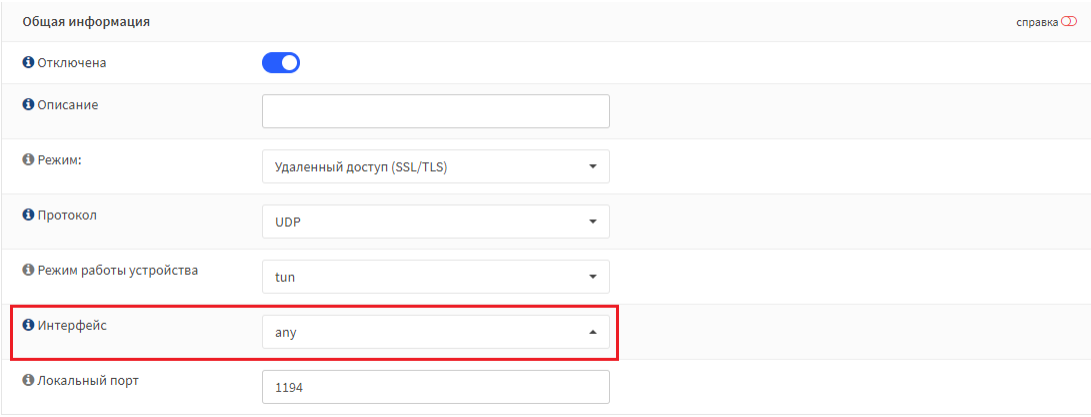


Рис. 615: Выбор интерфейса

Примечание

При выборе любого из них в сочетании с UDP мы будем предполагать, что сервер используется в многосетевом режиме. Это имеет некоторые небольшие последствия для производительности, чтобы обеспечить правильный поиск обратного адреса

- в поле **«Локальный порт»** установить числовое значение порта;

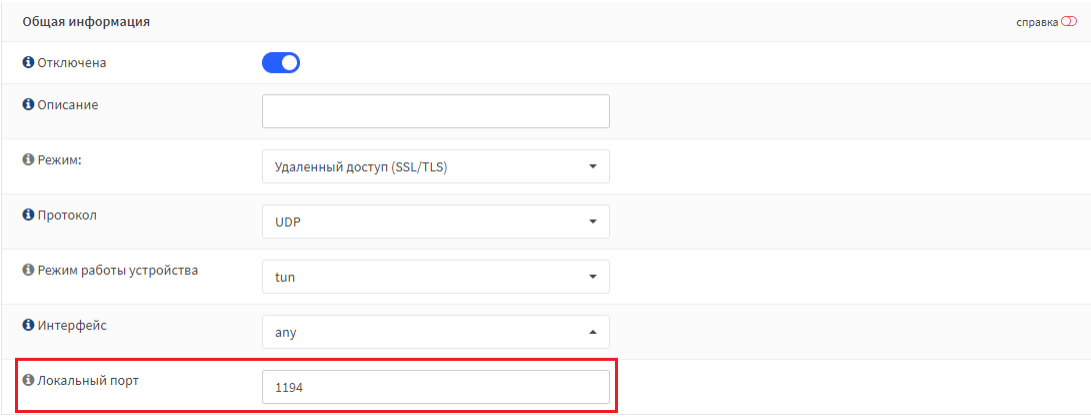


Рис. 616: Значение порта

Режим Удаленный доступ (аутентификация пользователя)

Для настройки режима Удаленный доступ (аутентификация пользователя) необходимо:

- в поле **«Режим»** выбрать режим **«Удаленный доступ (аутентификация пользователя)»** из выпадающего списка;

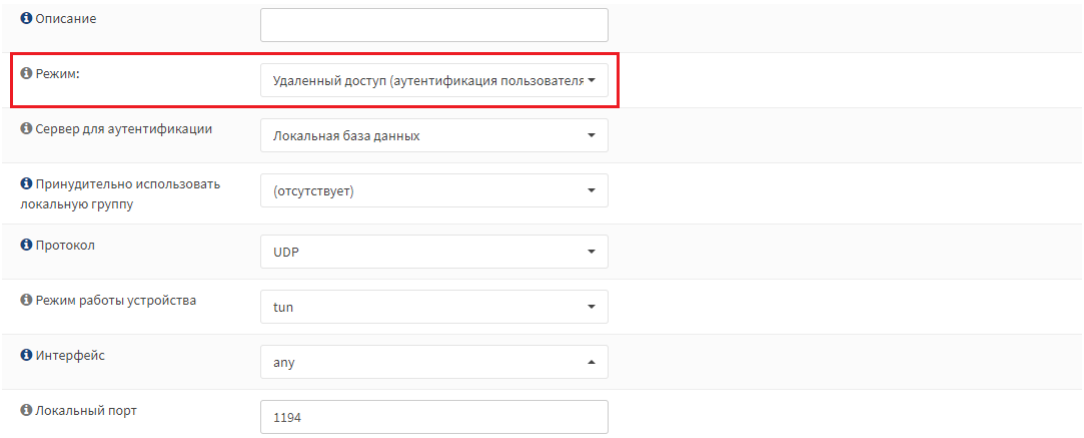


Рис. 617: Выбор режима Удаленный доступ (аутентификация пользователя)

- в поле **«Сервер для аутентификации»** выбрать из выпадающего списка необходимый сервер, соответствующий таблице;

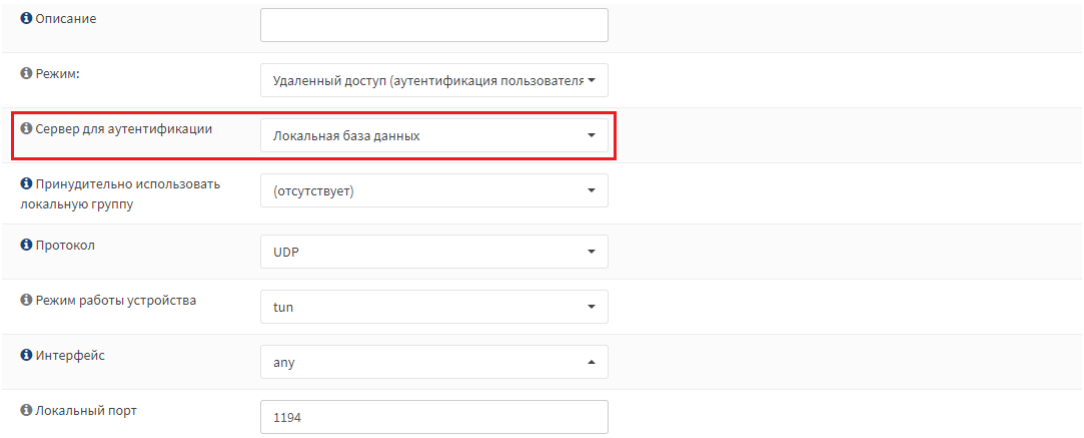


Рис. 618: Выбор сервера для аутентификации

Таблица 148: Выбор сервера для аутентификации

Сервер для аутентификации
Ничего не выбрано
Локальная база данных

- в поле **«Принудительно использовать локальную группу»** выбрать из выпадающего списка необходимую группу, пользователям которой необходимо разграничить доступ;
- в поле **«Протокол»** выбрать из выпадающего списка необходимый протокол, соответствующий таблице;

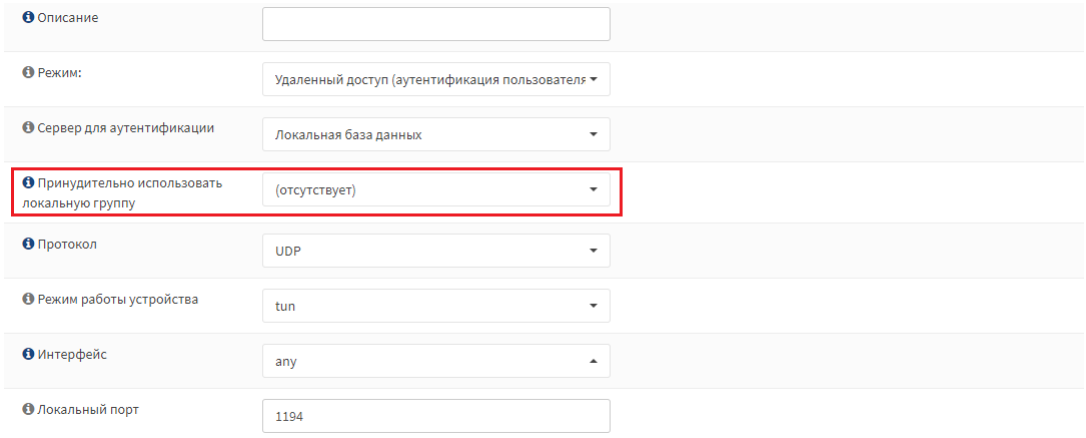


Рис. 619: Выбор локальной группы

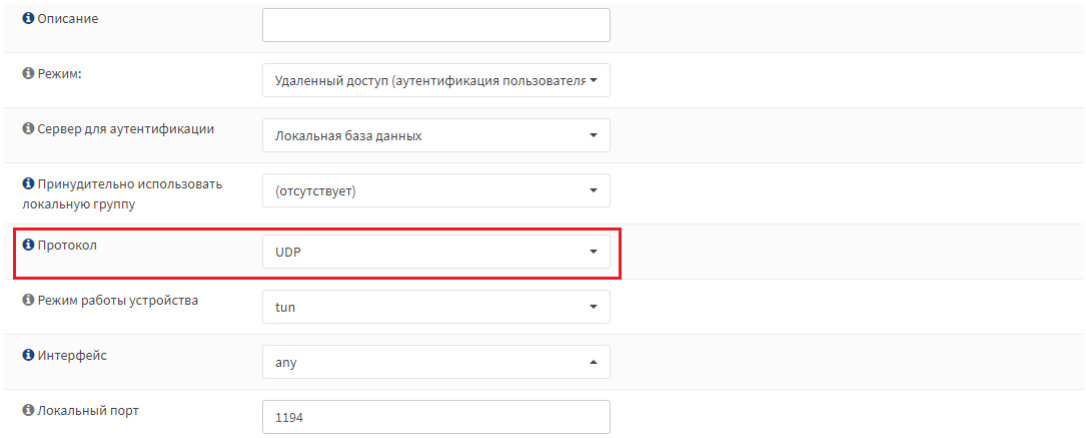


Рис. 620: Выбор протокола

Таблица 149: Выбор протокола

Протокол
UDP
TCP

Примечание

Обратите внимание, что использование обоих семейств с UDP/TCP не работает с явным интерфейсом, поскольку OpenVPN не поддерживает прослушивание более одного указанного IP-адреса. В этом случае в настоящее время предполагается IPv4

- в поле **«Режим работы устройства»** выбрать из выпадающего списка необходимый режим работы, соответствующий таблице;

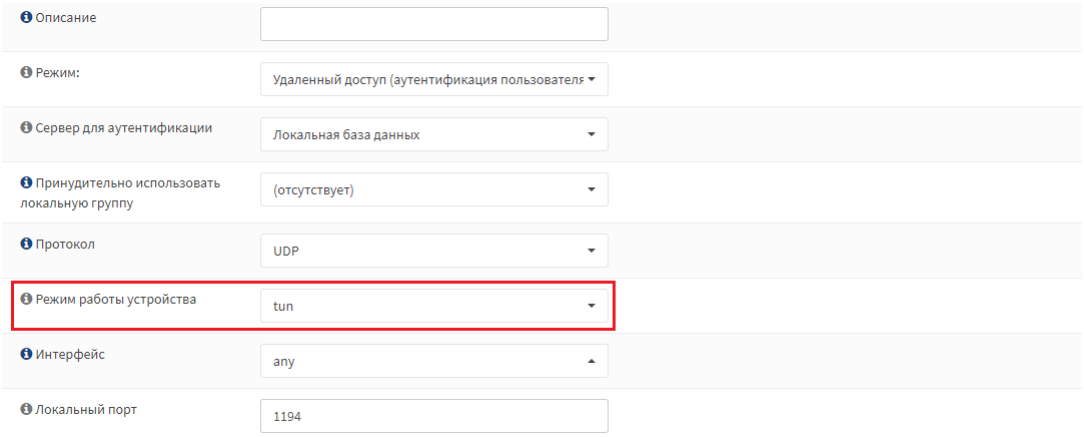


Рис. 621: Выбор режима работы устройства

Таблица 150: Выбор режима работы устройства

Режим работы устройства
tun
tap

- в поле **«Интерфейс»** выбрать из выпадающего списка необходимый интерфейс;

Примечание

При выборе любого из них в сочетании с UDP мы будем предполагать, что сервер используется в многосетевом режиме. Это имеет некоторые небольшие последствия для производительности, чтобы обеспечить правильный поиск обратного адреса

- в поле **«Локальный порт»** установить числовое значение порта;

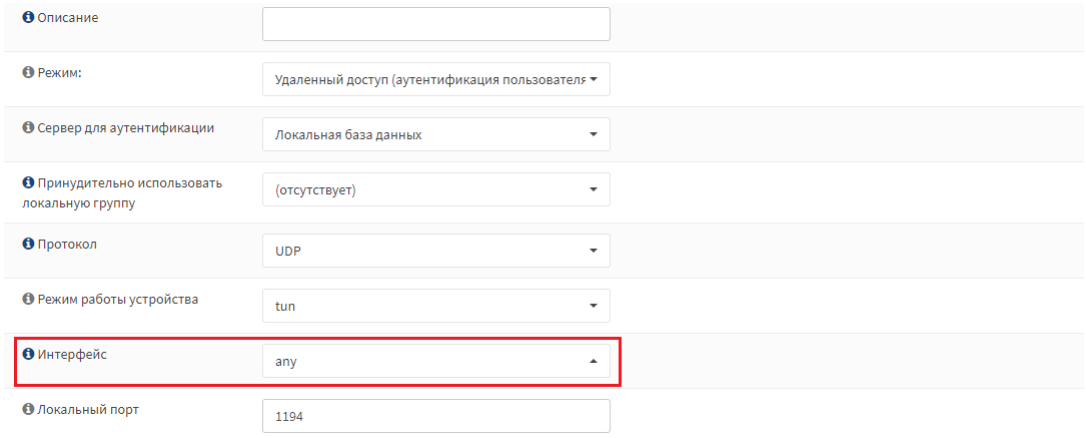


Рис. 622: Выбор интерфейса

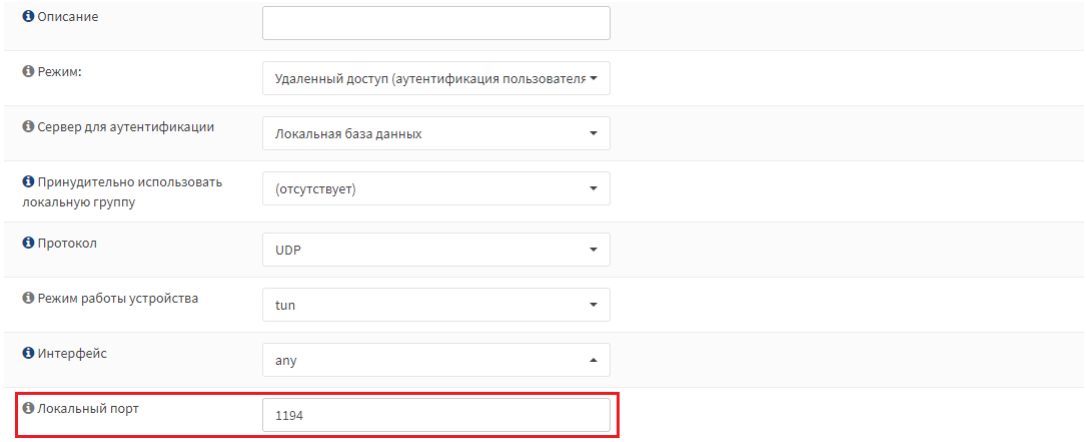


Рис. 623: Значение порта

Режим Удаленный доступ (SSL/TLS+аутентификация пользователя)

Для настройки режима Удаленный доступ (SSL/TLS+аутентификация пользователя) необходимо:

- в поле **«Режим»** выбрать режим **«Удаленный доступ (SSL/TLS+аутентификация пользователя)»** из выпадающего списка;

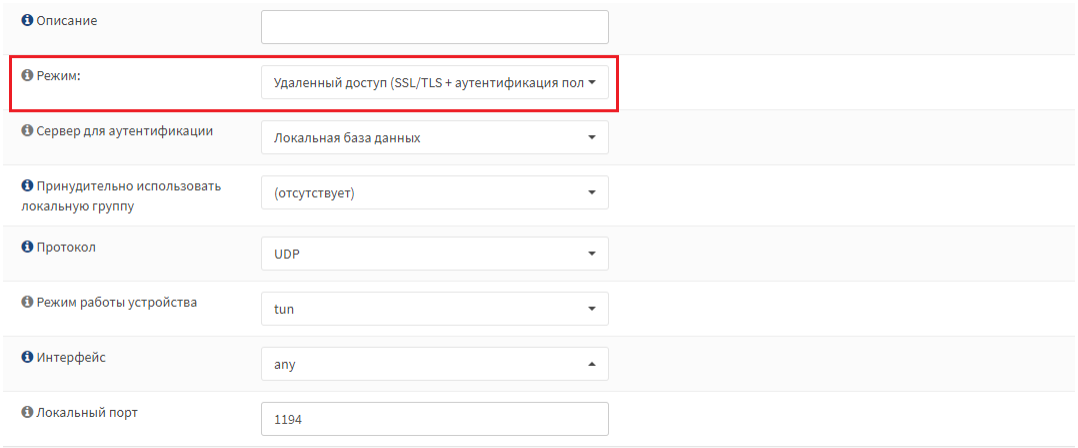


Рис. 624: Выбор режима Удаленный доступ (SSL/TLS+аутентификация пользователя)

- в поле **«Сервер для аутентификации»** выбрать из выпадающего списка необходимый сервер, соответствующий таблице;

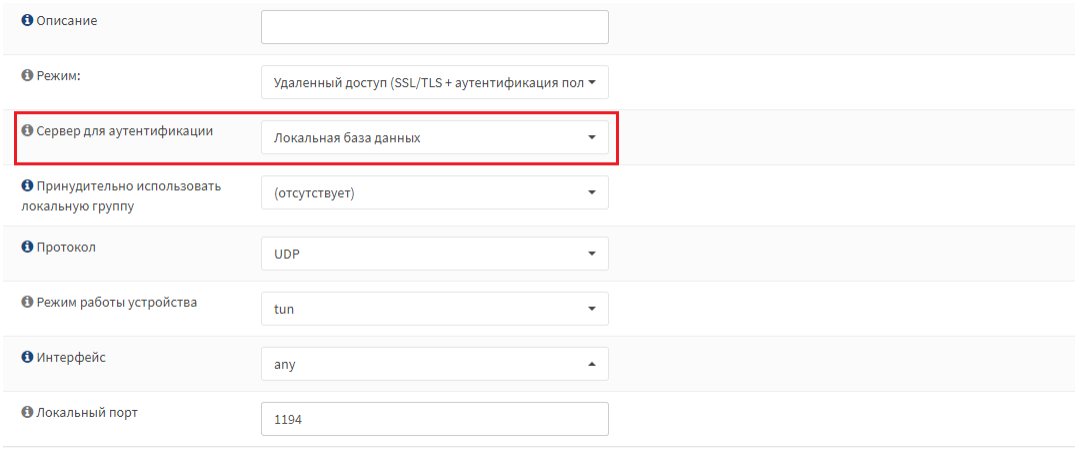


Рис. 625: Выбор сервера для аутентификации

Таблица 151: Выбор сервера для аутентификации

Сервер для аутентификации
Ничего не выбрано
Локальная база данных

- в поле **«Принудительно использовать локальную группу»** выбрать из выпадающего списка необходимую группу, пользователям которой необходимо разграничить доступ;
- в поле **«Протокол»** выбрать из выпадающего списка необходимый протокол, соответствующий таблице;

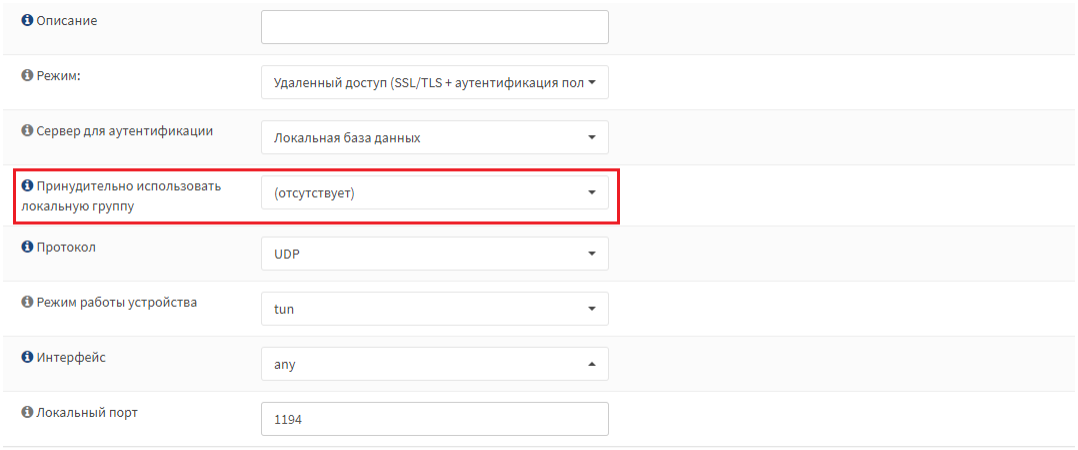


Рис. 626: Выбор локальной группы

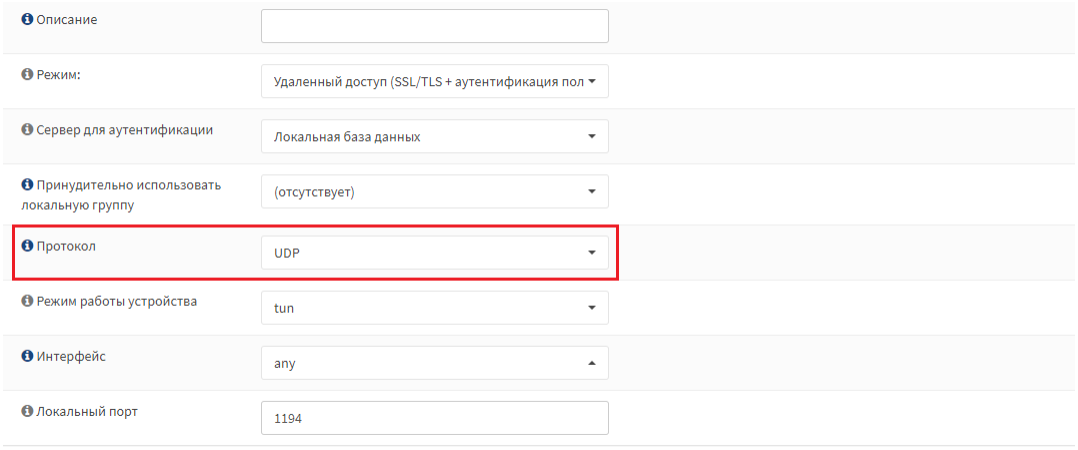


Рис. 627: Выбор протокола

Таблица 152: Выбор протокола

Протокол
UDP
TCP

Примечание

Обратите внимание, что использование обоих семейств с UDP/TCP не работает с явным интерфейсом, поскольку OpenVPN не поддерживает прослушивание более одного указанного IP-адреса. В этом случае в настоящее время предполагается IPv4

- в поле **«Режим работы устройства»** выбрать из выпадающего списка необходимый режим работы, соответствующий таблице;

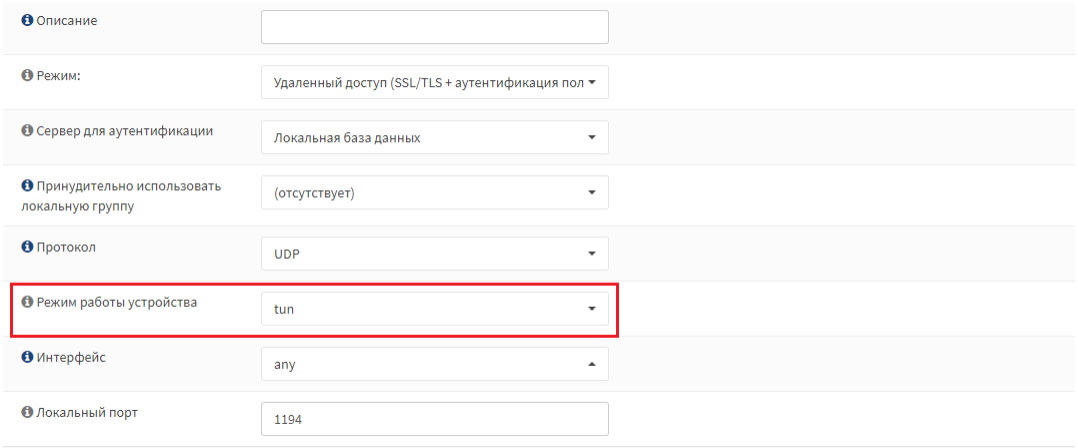


Рис. 628: Выбор режима работы устройства

Таблица 153: Выбор режима работы устройства

Режим работы устройства
tun
tap

- в поле **«Интерфейс»** выбрать из выпадающего списка необходимый интерфейс;

Примечание

При выборе любого из них в сочетании с UDP мы будем предполагать, что сервер используется в многосетевом режиме. Это имеет некоторые небольшие последствия для производительности, чтобы обеспечить правильный поиск обратного адреса

- в поле **«Локальный порт»** установить числовое значение порта;

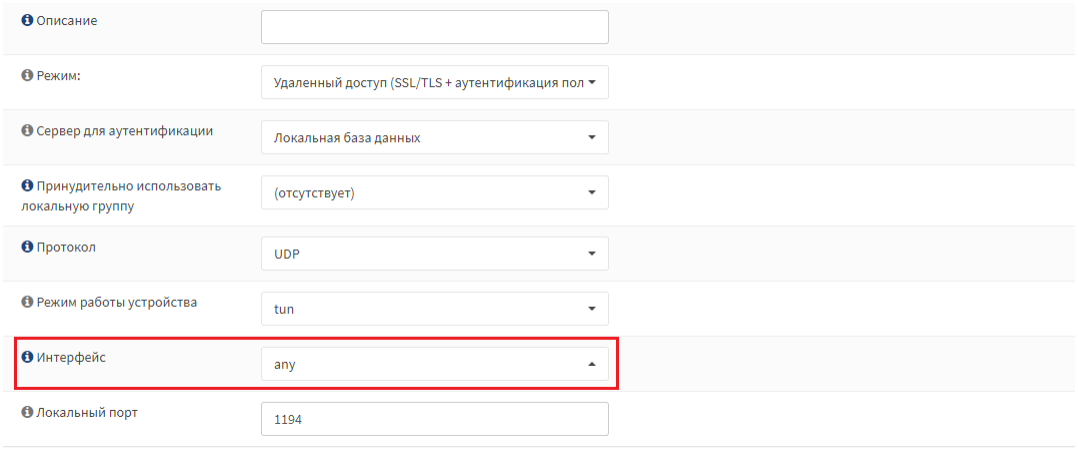


Рис. 629: Выбор интерфейса

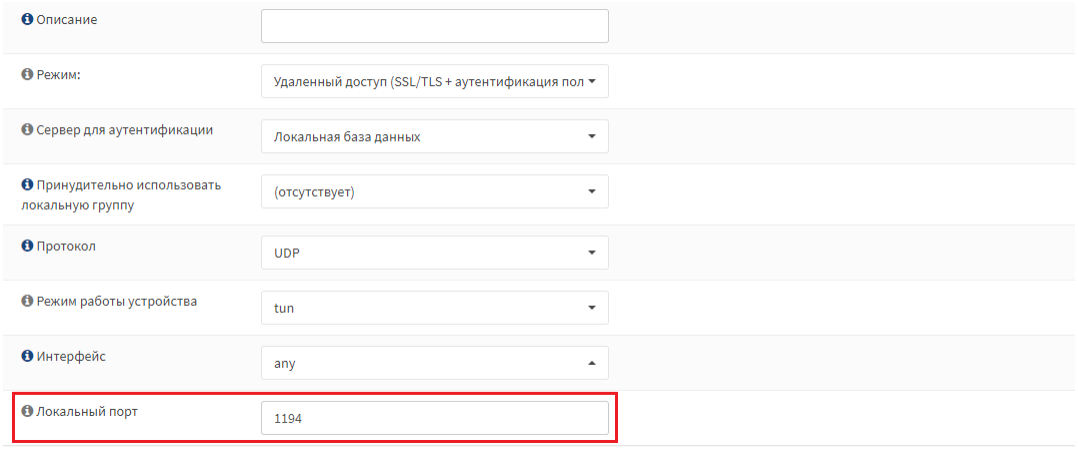


Рис. 630: Значение порта

Криптографические установки

Для создания криптографических установок необходимо:

- в поле **«Аутентификация TLS»** установить переключатель в случае необходимости включить аутентификацию пакетов TLS и автоматически генерировать совместно использующийся ключ аутентификации TLS;

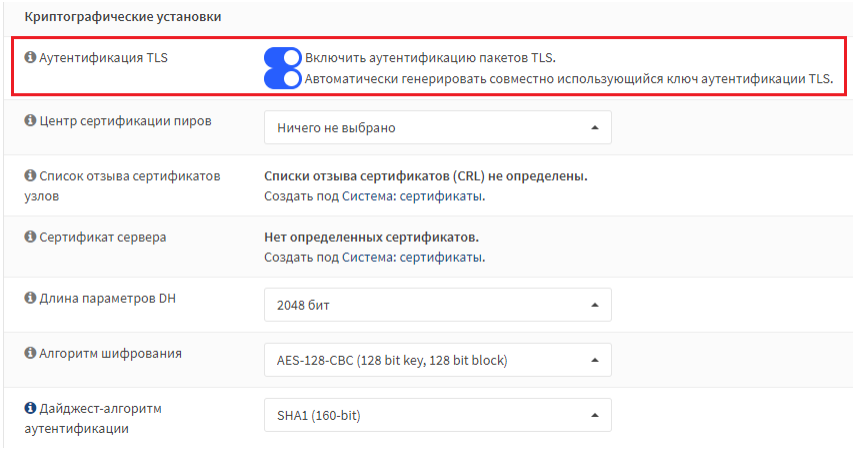


Рис. 631: Выбор аутентификации TLS

- в поле **«Центр сертификации пиров»** выбрать из выпадающего списка необходимый центр сертификации;

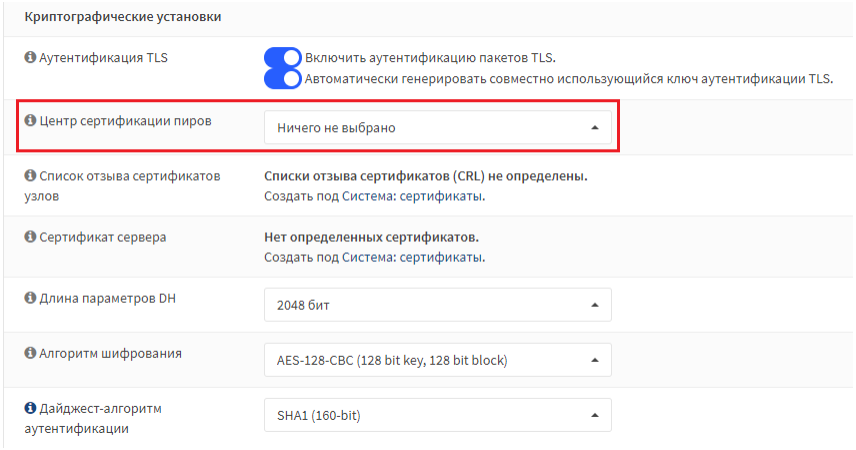


Рис. 632: Выбор центра сертификации пиров

- в поле **«Список отзыва сертификатов узлов»** установить необходимый список отзыва;
- в поле **«Сертификат сервера»** установить необходимый сертификат сервера;
- в поле **«Длина параметров DH»** выбрать из выпадающего списка необходимую длину, соответствующую таблице;

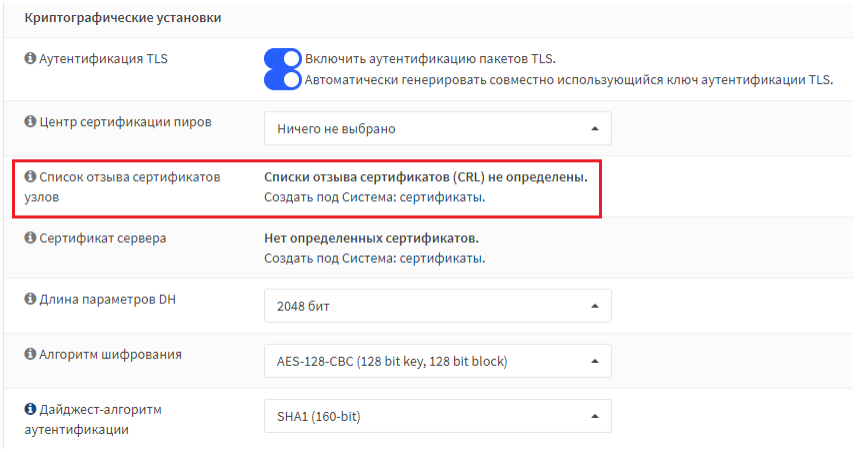


Рис. 633: Выбор списка отзыва сертификатов узлов

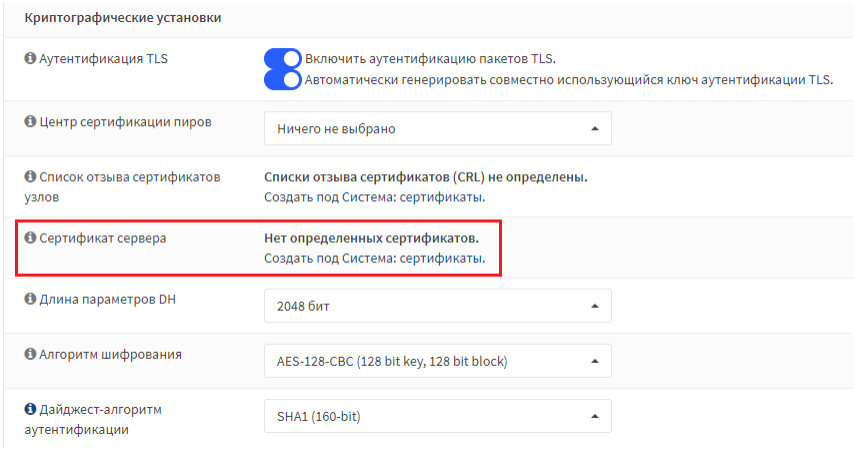


Рис. 634: Выбор сертификата сервера

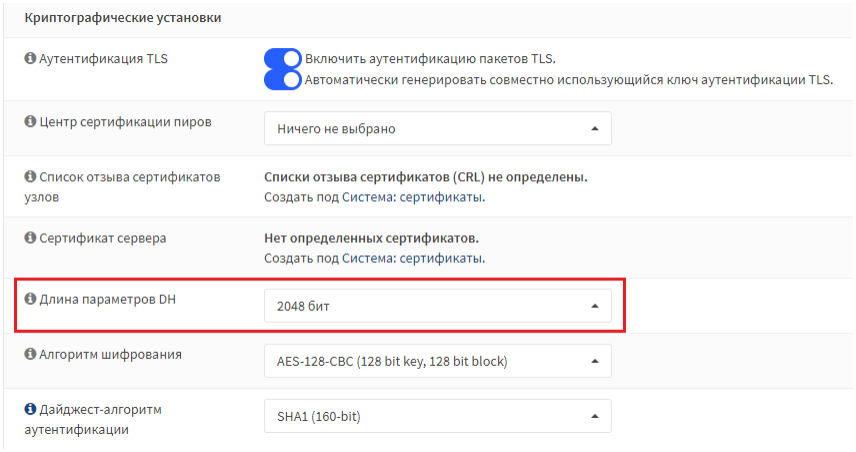


Рис. 635: Длина параметров DH

Таблица 154: Длина параметров DH

Длина параметров DH
1024 бит
2048 бит
4096 бит

- в поле **«Алгоритм шифрования»** выбрать из выпадающего списка необходимый алгоритм;

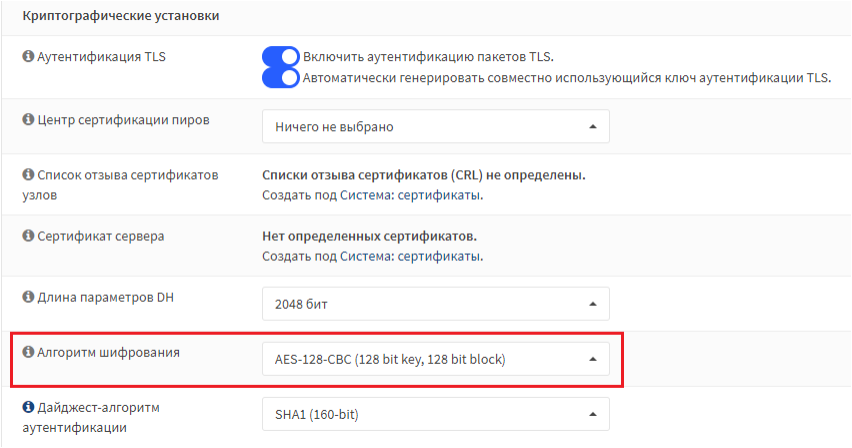


Рис. 636: Выбор алгоритма шифрования

- в поле **«Дайджест-алгоритм аутентификации»** выбрать из выпадающего списка необходимый алгоритм;

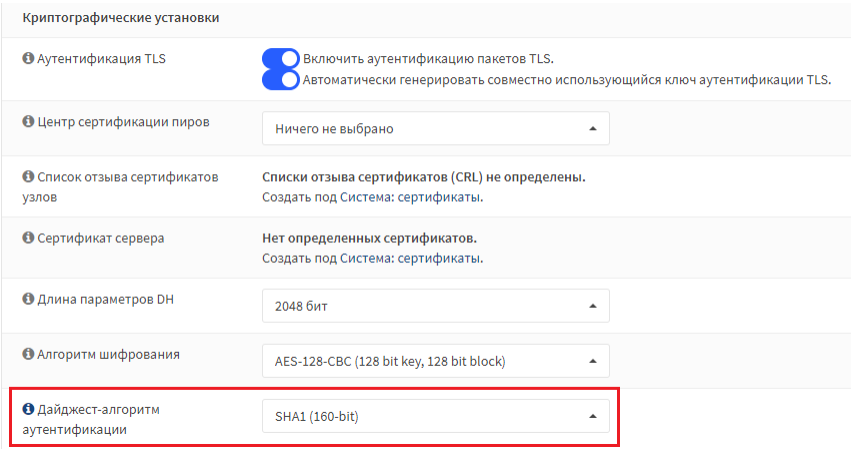


Рис. 637: Дайджест-алгоритм аутентификации

Примечание

Не изменяйте эти настройки, если все клиенты поддерживают установленный по умолчанию для OpenVPN алгоритм хеширования SHA1

- в поле **«Уровень сертификата»** выбрать из выпадающего списка необходимый уровень;

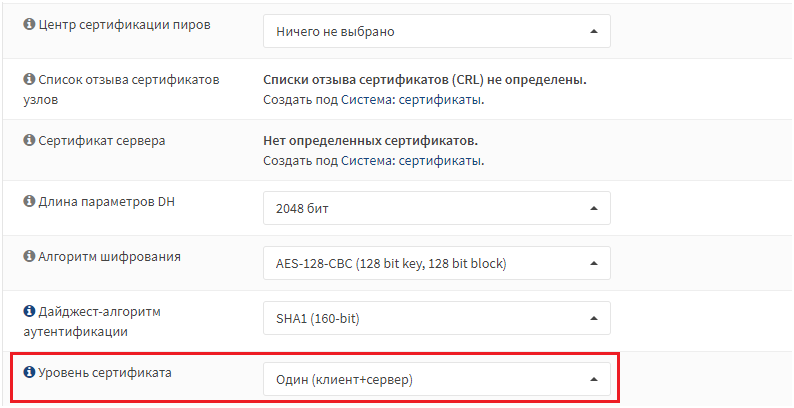


Рис. 638: Выбор уровня сертификата

Примечание

Если клиент входит в систему на основе сертификата, не принимать сертификаты ниже указанного уровня. Позволяет отклонять сертификаты, выданные промежуточными центрами сертификации, сгенерированные на основе того же корневого сертификата, что и сертификат сервера

- в поле **«Ограниченный пользователь/совпадение с общим именем сертификата»** (при выборе режима **«Удаленный доступ (SSL/TLS+аутентификация пользователя)»**) установить переключатель для успешной аутентификации пользователей общее имя сертификата клиента должно совпадать с именем пользователя, полученным при входе в систему;

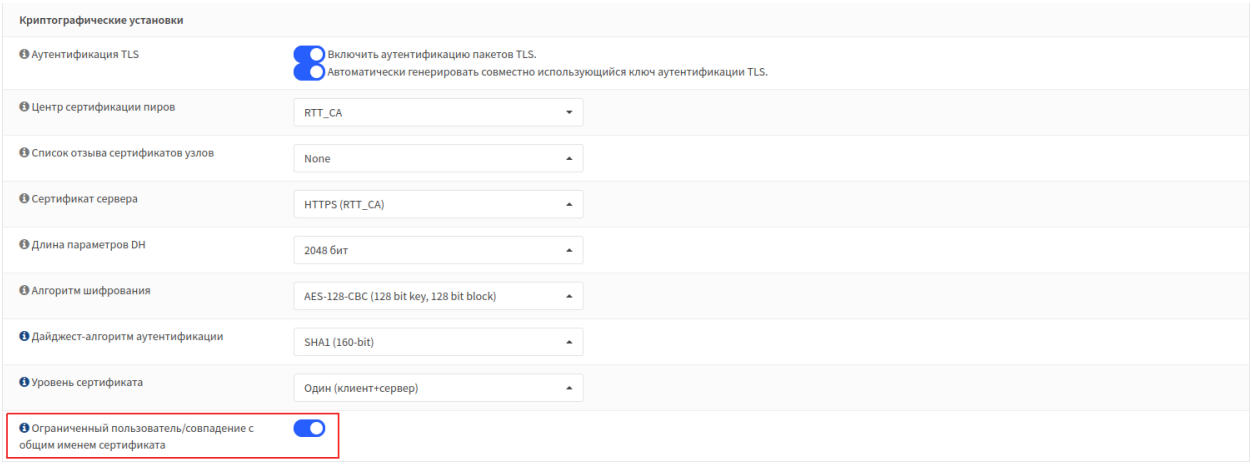


Рис. 639: Ограниченный пользователь/совпадение с общим именем сертификата

Настройки туннеля

Для настроек туннеля необходимо:

- в поле **«Туннельная сеть IPv4»** указать туннельную сеть IPv4;

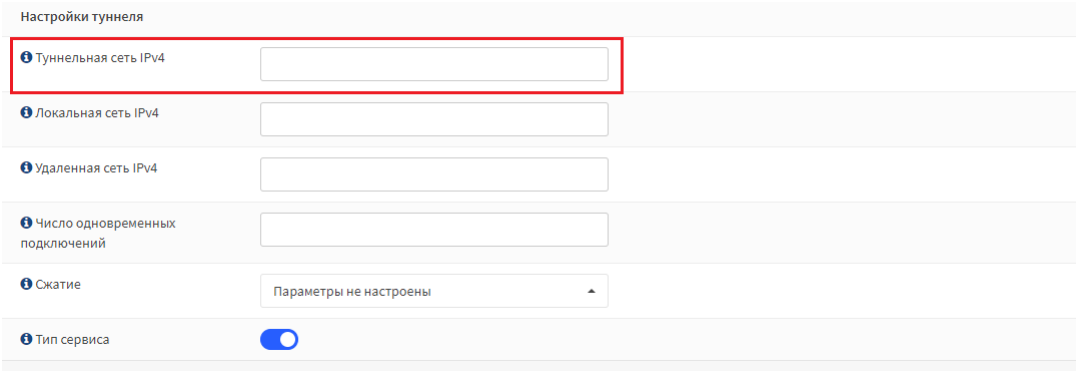


Рис. 640: Туннельная сеть IPv4

Примечание

Эта виртуальная сеть IPv4 используется для частных соединений между этим сервером и клиентскими хостами в формате CIDR (например, 10.0.8.0/24). Первый сетевой адрес будет назначен интерфейсу виртуального сервера. Остальные сетевые адреса могут быть дополнительно назначены подключаемым клиентам (см. пул IP-адресов)

Для настроек туннеля необходимо:

- в поле **«Локальная сеть IPv4»** указать локальную сеть IPv4;

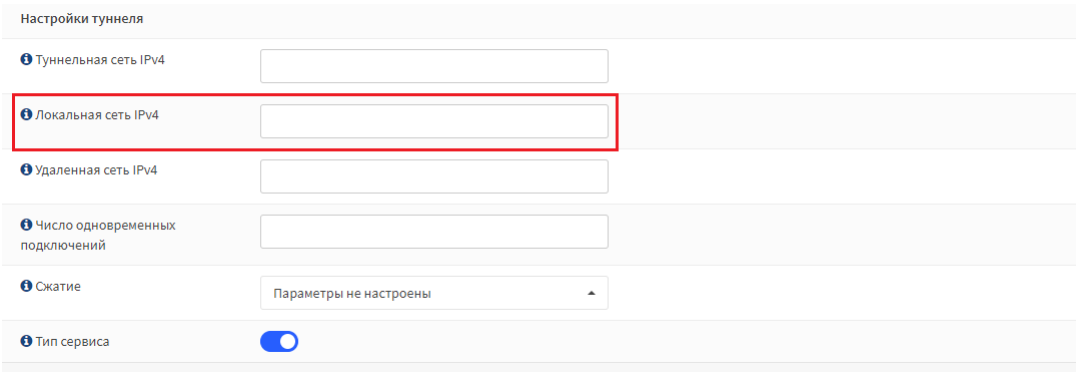


Рис. 641: Локальная сеть IPv4

Примечание

Сети IPv4, которые будут доступны из удаленной точки, представляют собой разделенный запятыми список из одного или нескольких CIDR-диапазонов. Вы можете оставить это поле пустым, если вы не хотите добавлять маршрут к локальной сети через этот туннель на удаленном компьютере. Как правило, определен маршрут к вашей сети LAN

- в поле **«Удаленная сеть IPv4»** указать удаленную сеть IPv4;

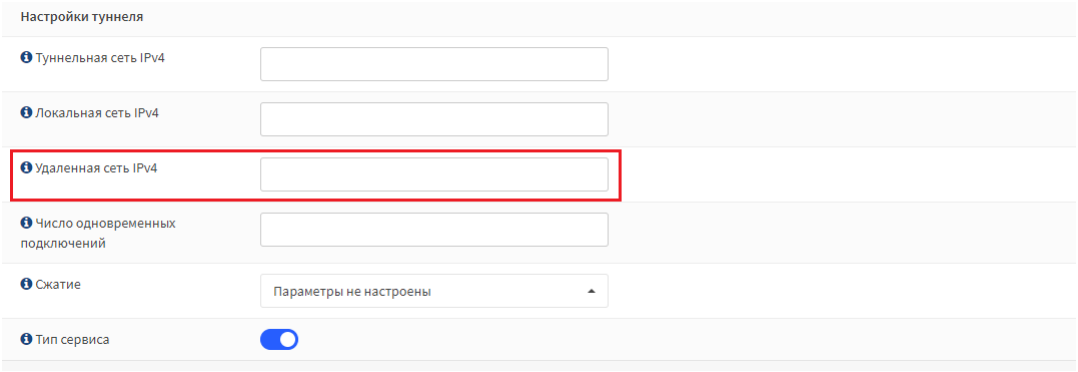


Рис. 642: Удаленная сеть IPv4

Примечание

Сети IPv4, для которых будет создан маршрут через туннель, чтобы установить VPN-соединение между двумя пунктами, не изменяя таблицы маршрутизации вручную, представляют собой разделенный запятыми список из одного или нескольких CIDR-диапазонов. Для VPN-соединения между двумя пунктами, необходимо ввести адрес удаленной сети LAN. Вы можете оставить это поле пустым, если не хотите использовать VPN-соединение между двумя пунктами

- в поле **«Число одновременных подключений»** указать максимальное количество клиентов, которым разрешено одновременно подключаться к этому серверу;

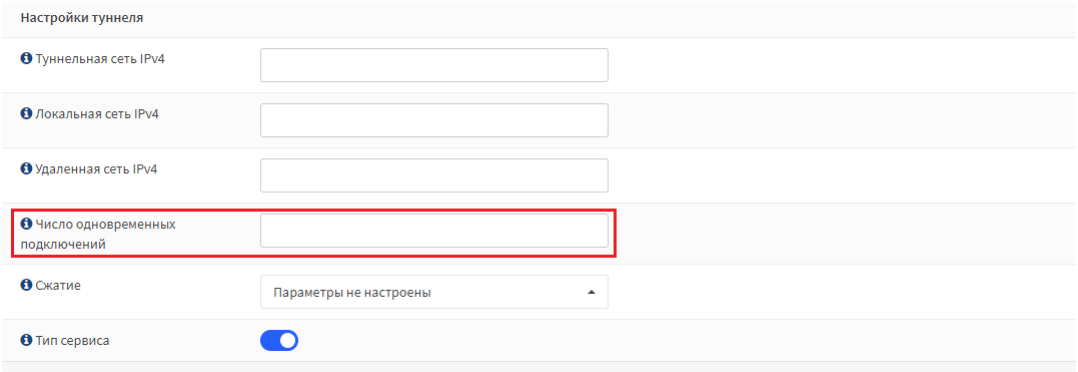


Рис. 643: Число одновременных подключений

- в поле **«Сжатие»** указать параметры сжатия;

Примечание

Сжимайте туннельные пакеты с помощью алгоритма LZ4/LZO. LZ4 обычно предлагает наилучшую производительность при наименьшей загрузке ЦП. Для обратной совместимости используйте LZO (который идентичен старой опции –comp-lzo yes). В частичном режиме (опция –compress с пустым алгоритмом) сжатие отключено, но кадрирование пакетов для сжатия по-прежнему включено, что позволяет позже установить другой параметр. Устаревший алгоритм LZO с адаптивным режимом сжатия будет динамически отключать сжатие на определенный период времени, если OpenVPN

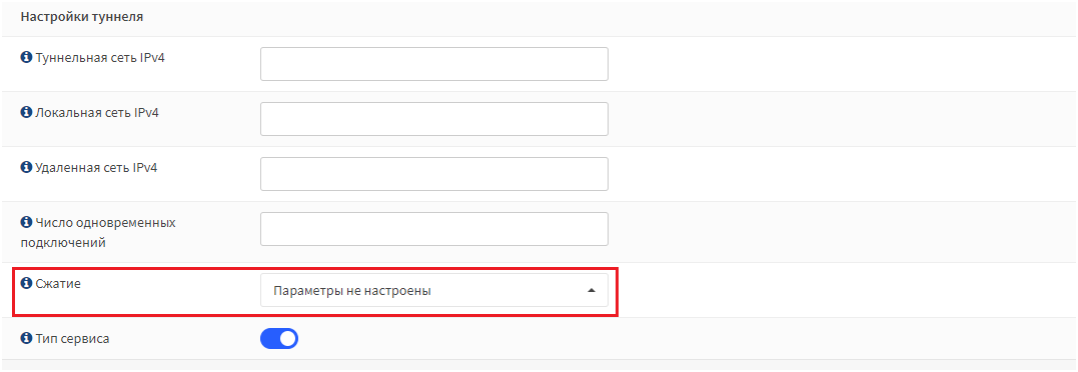


Рис. 644: Сжатие

обнаружит, что данные в пакетах не сжимаются эффективно

- в поле **«Pass through TOS»** установить переключатель в случае необходимости указать значение поля **«Тип сервиса»** заголовка IP для туннельных пакетов так, чтобы оно совпадало со значением инкапсулированного пакета;

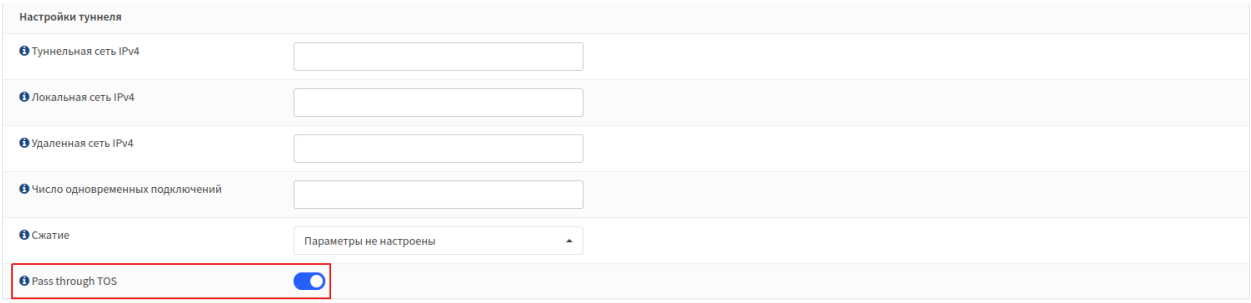


Рис. 645: Pass through TOS

Настройки клиента

Для настроек клиента необходимо:

- в поле **«Динамический IP-адрес»** установить переключатель в случае необходимости разрешить подключенным клиентам сохранять соединения, если их IP-адрес изменился;
- в поле **«Топология сети»** установить переключатель в случае необходимости выделить только один IP-адрес для клиента (топология подсети) вместо изолированной подсети (топология net30);

Примечание

Актуально при указании IP-адреса виртуального адаптера для клиентов, когда используется режим TUN на IPv4

- в поле **«Домен DNS по умолчанию»** предоставить клиентам доменное имя по умолчанию;
- в поле **«DNS-серверы»** предоставить клиенту список NTP-серверов;

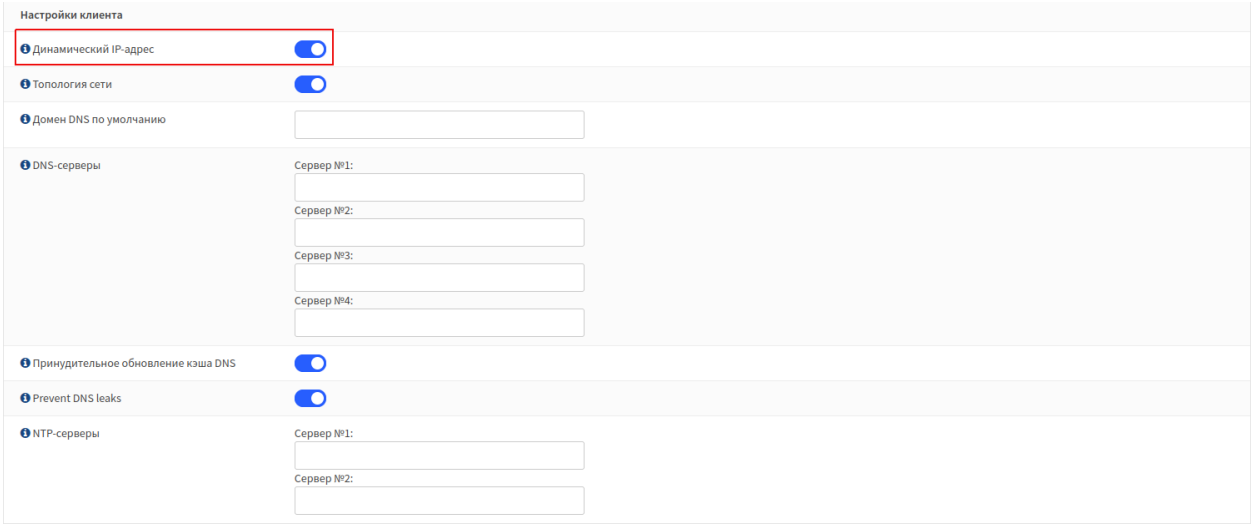


Рис. 646: Динамический IP-адрес

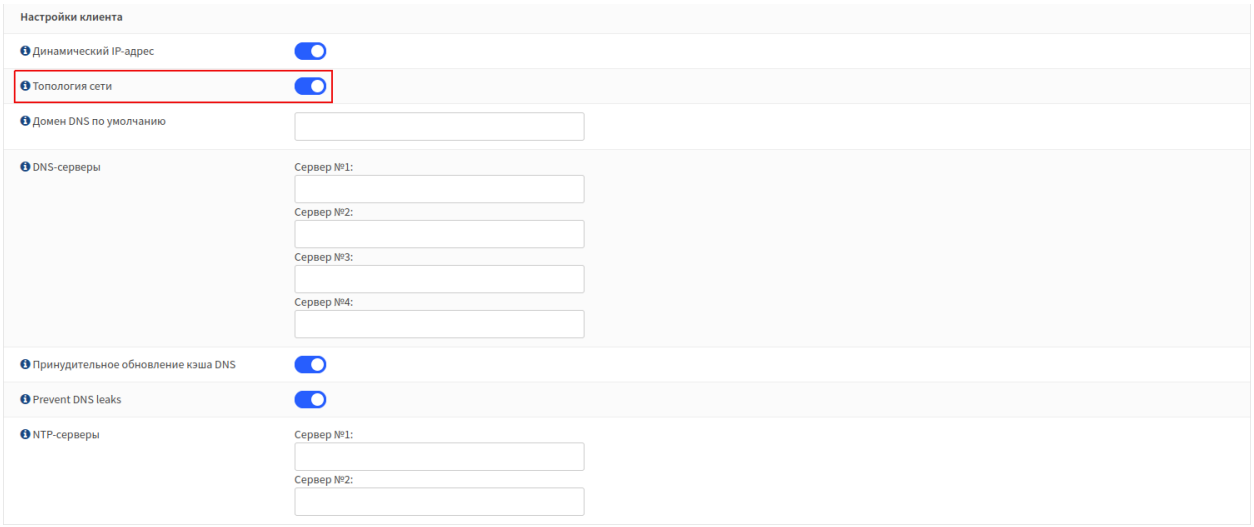


Рис. 647: Топология сети

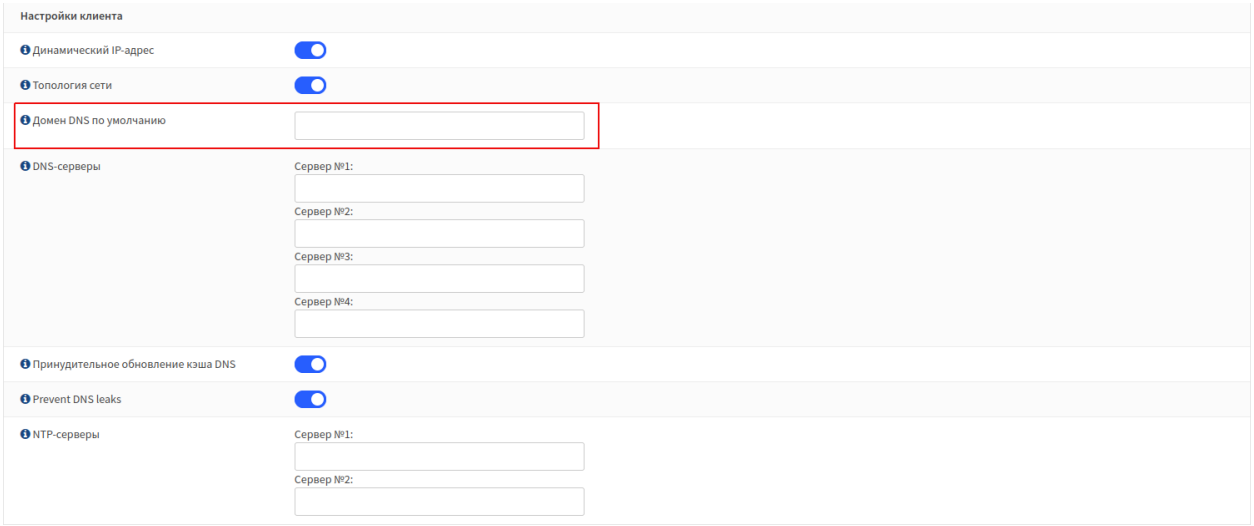


Рис. 648: Домен DNS по умолчанию

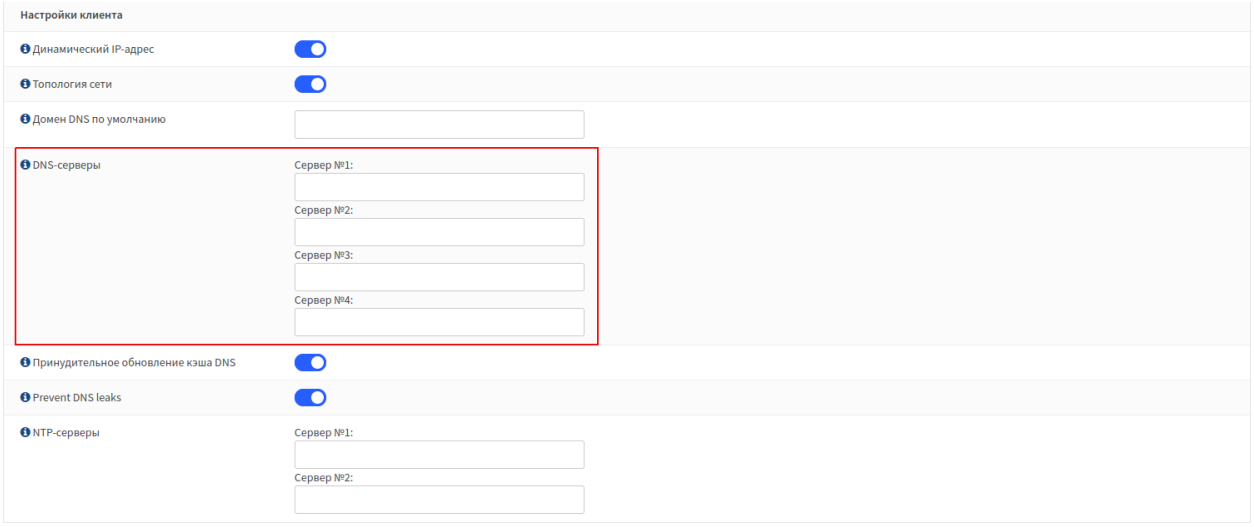


Рис. 649: DNS-серверы

- в поле **«Принудительное обновление кэша DNS»** установить переключатель в случае необходимости запустить «net stop dnscache», «net start dnscache», «ipconfig /flushdns» и «ipconfig /registerdns» при инициации соединения;

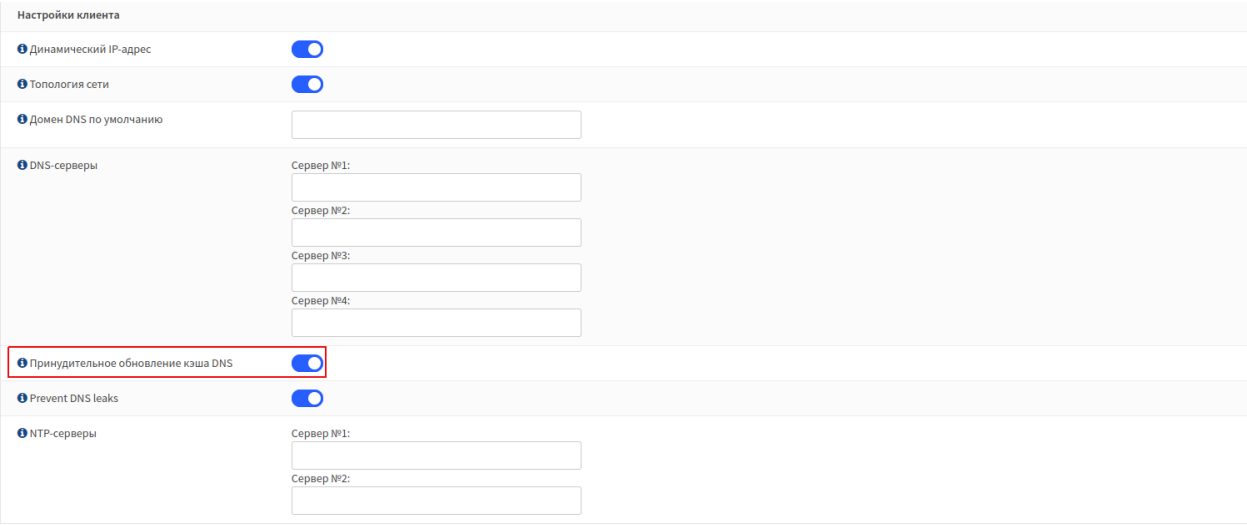


Рис. 650: Принудительное обновление кэша DNS

Примечание

Это заставляет Windows распознавать развернутые DNS-серверы

- в поле **«Prevent DNS leaks»** установить переключатель в случае необходимости блокировать DNS-серверы на других сетевых адаптерах, чтобы предотвратить утечку DNS;

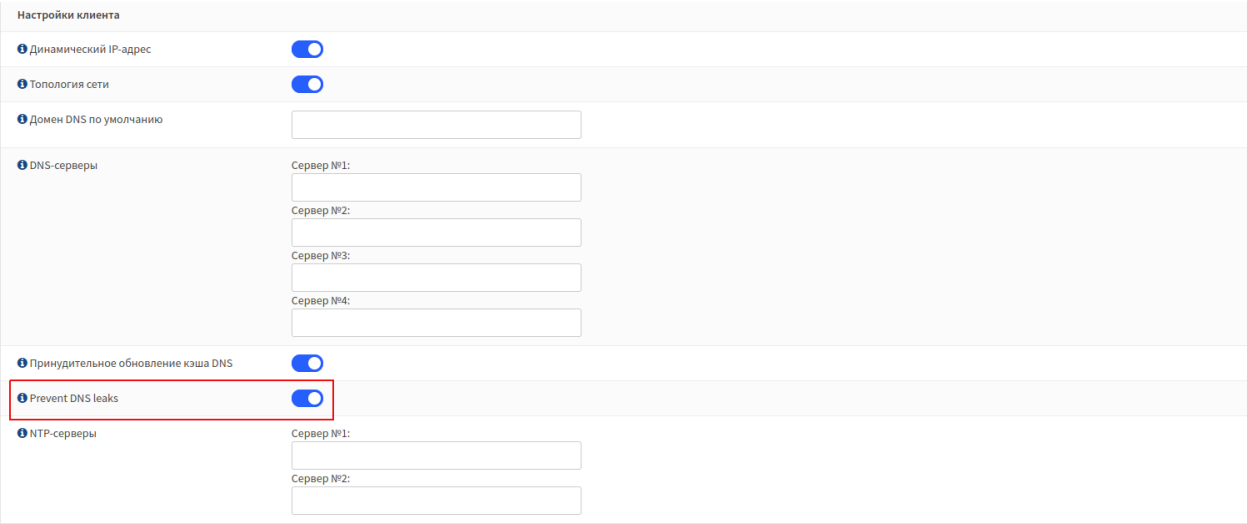


Рис. 651: Prevent DNS leaks

Примечание

Совместим только с клиентами Windows

- в поле **«NTP-серверы»** предоставить клиенту список NTP-серверов;

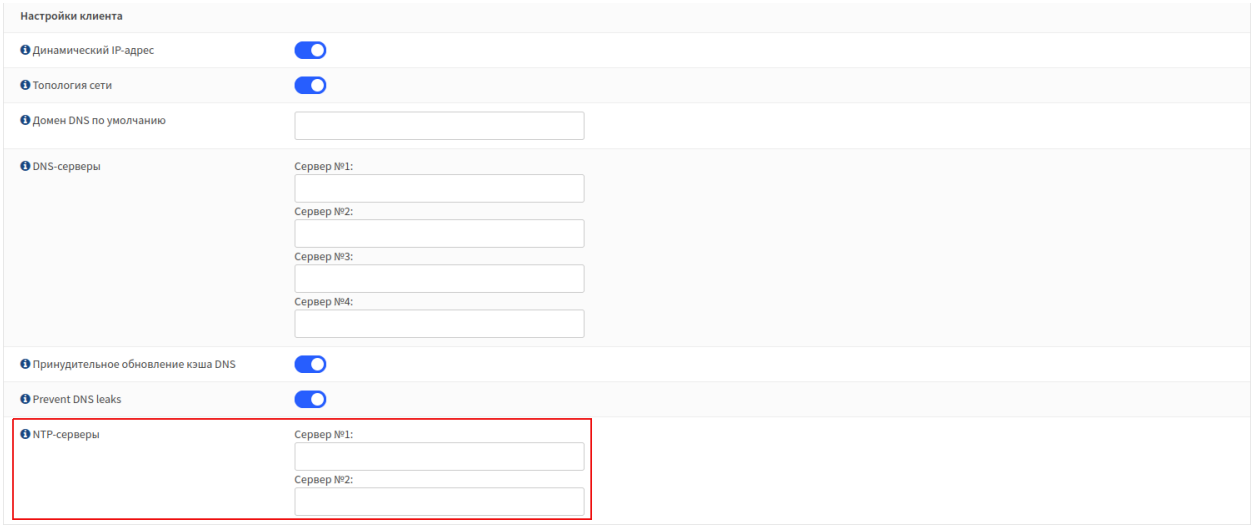


Рис. 652: NTP-серверы

- нажать кнопку **«Сохранить»** 

.

2.7.7.2 Экспорт настроек клиента

Для экспорта настроек клиента необходимо:

- в поле **«Сервер удаленного доступа»** выбрать из выпадающего списка сервер OpenVPN для экспорта профилей;

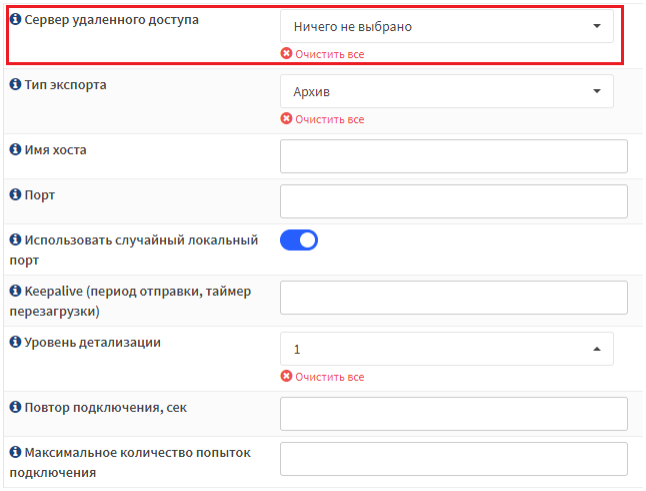


Рис. 653: Сервер удаленного доступа

- в поле **«Тип экспорта»** выбрать из выпадающего списка формат файла для экспорта;

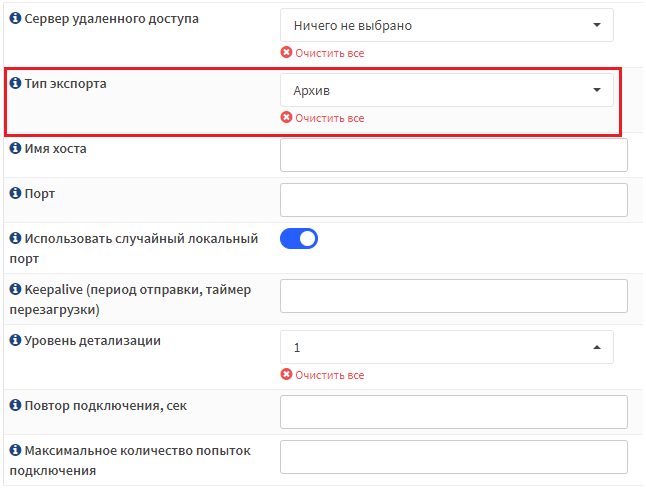


Рис. 654: Тип экспорта

- в поле **«Имя хоста»** указать адреса или имена хостов, к которым должен подключаться этот клиент;

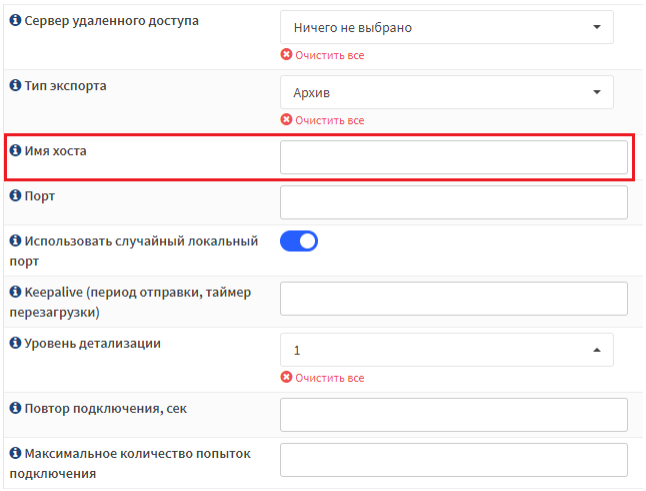


Рис. 655: Имя хоста

Примечание

Используйте запятые, чтобы указать более одного

- в поле **«Порт»** указать порт, на котором прослушивается OpenVPN;
- в поле **«Использовать случайный локальный порт»** установить переключатель в случае необходимости использовать случайный локальный порт источника (lport) для трафика от клиента;

Примечание

Если этот параметр не включен, два клиента не смогут работать

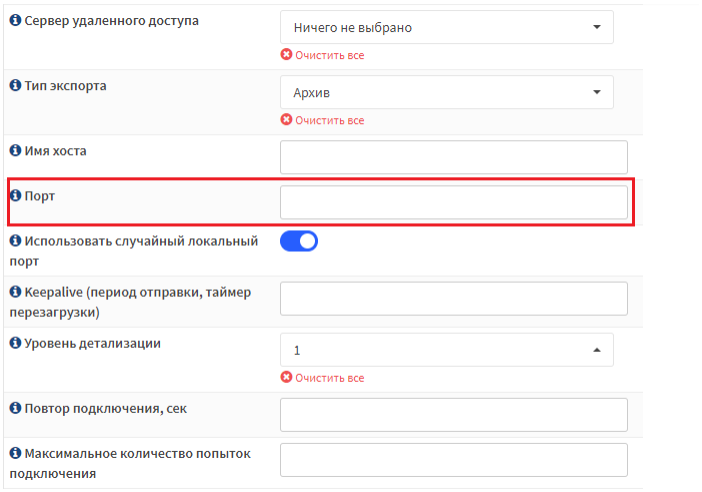


Рис. 656: Порт

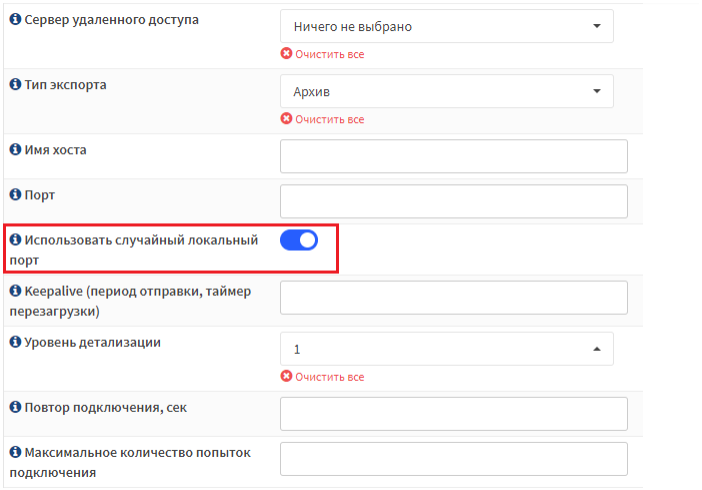


Рис. 657: Использовать случайный локальный порт

- в поле **«Keepalive (период отправки, таймер перезагрузки)»** указать пинг-сообщения с «периодом отправки» и перезагрузку соединения с «таймером перезагрузки»;

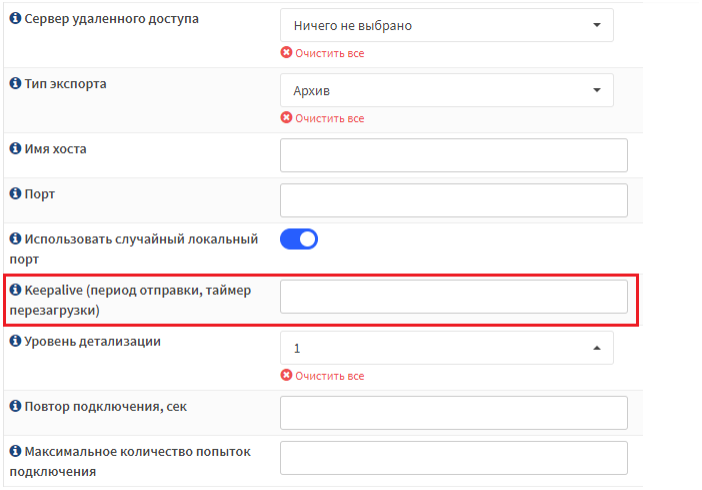


Рис. 658: Keepalive (период отправки, таймер перезагрузки)

- в поле **«Уровень детализации»** выбрать из выпадающего списка необходимый уровень детализации;

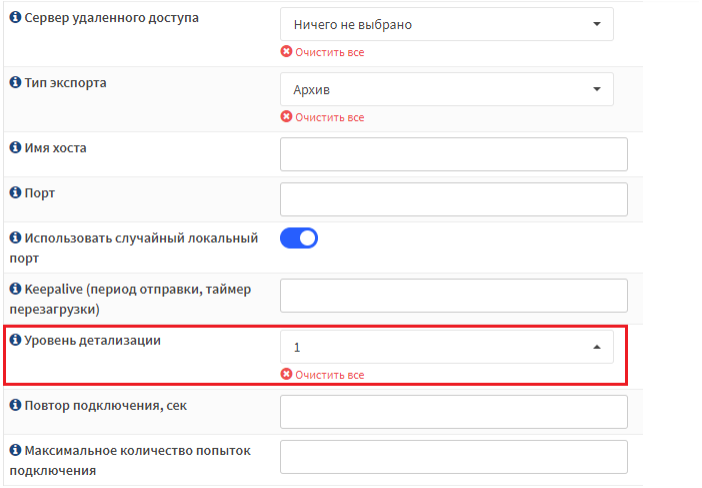


Рис. 659: Уровень детализации

Примечание

Оставьте пустым, чтобы сохранить уровень детализации 1 по умолчанию

- в поле **«Повтор подключения, сек»** указать время для повторного подключения;

Примечание

Переподключите vpn через заданные секунды, если он выйдет из строя

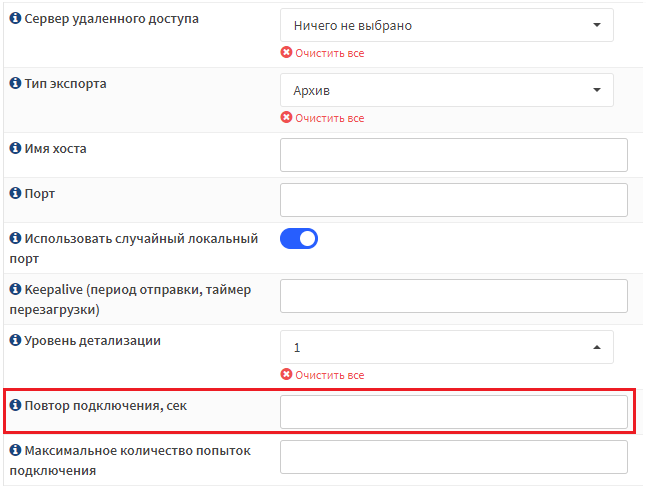


Рис. 660: Повтор подключения

- в поле **«Максимальное количество попыток подключения»** указать максимальное количество переподключений;

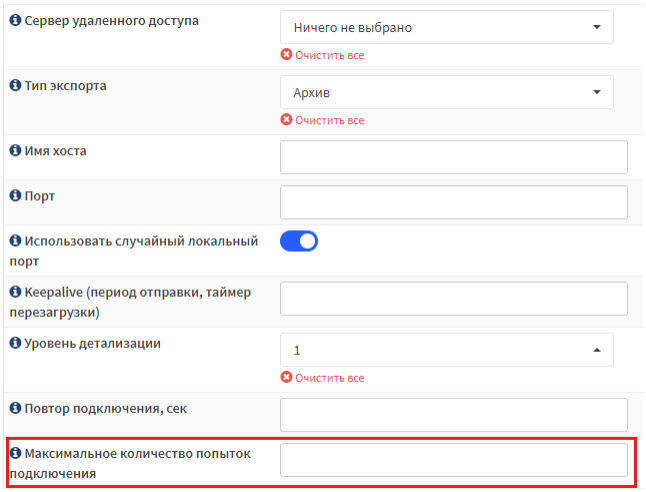


Рис. 661: Максимальное количество попыток подключения

- в поле **«P12 Пароль/подтверждение»** указать пароль для защиты содержимого файла pkcs12;
- в поле **«Подтвердить тему сервера»** установить переключатель в случае необходимости проверять имя сертификата сервера при подключении клиента;
- в поле **«Системное хранилище сертификатов Windows»** установить переключатель в случае отсутствия необходимости загружать сертификат и закрытый ключ из системного хранилища сертификатов Windows (только для Windows/OpenSSL);
- в поле **«Отключить сохранение пароля»** установить переключатель в случае необходимости устанавливать auth-nocache в экспортируемой конфигурации при использовании аутентификации по паролю;

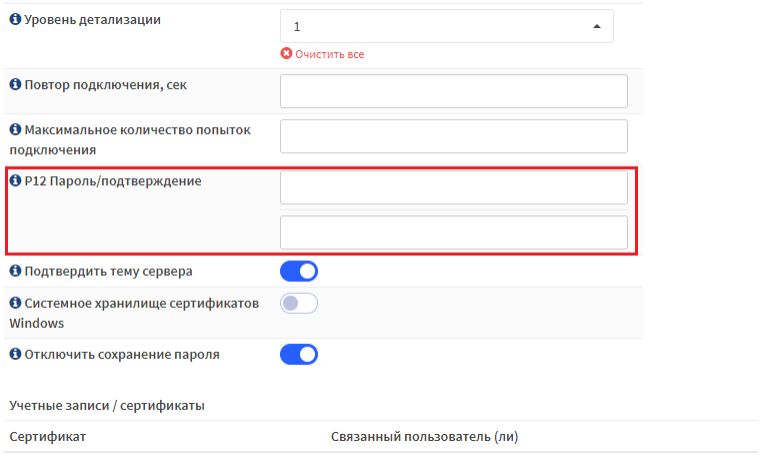


Рис. 662: P12 Пароль/подтверждение

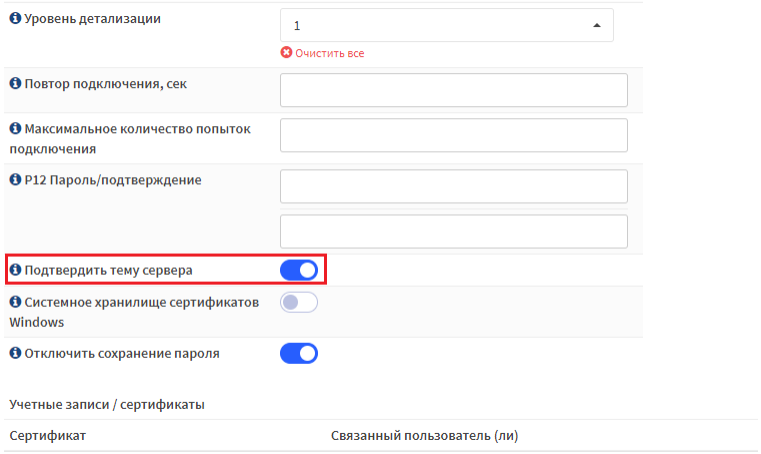


Рис. 663: Подтвердить тему сервера

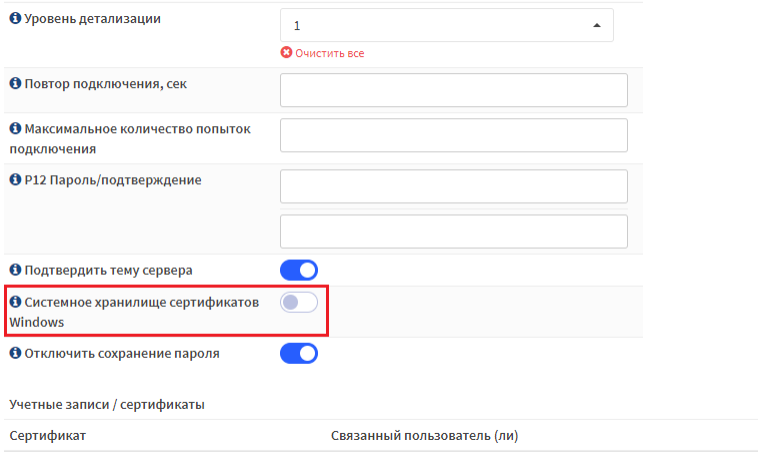


Рис. 664: Системное хранилище сертификатов Windows

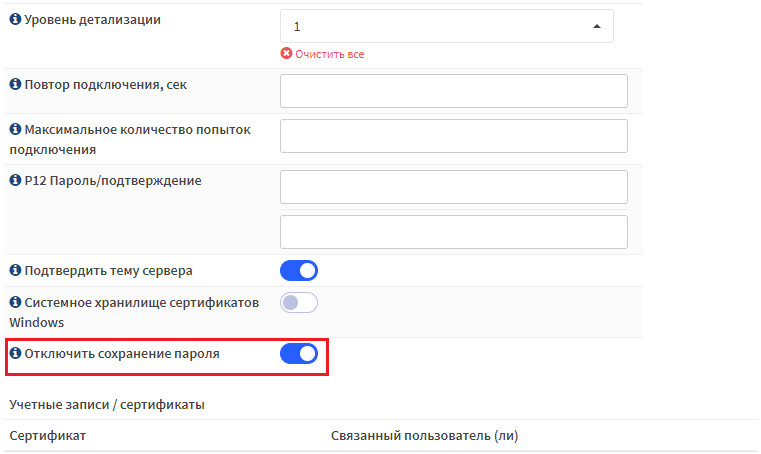


Рис. 665: Отключить сохранение пароля

Примечание

Это предотвращает кэширование паролей OpenVPN в памяти

2.7.7.3 Статус соединения

Статус соединения OpenVPN соответствует рисунку

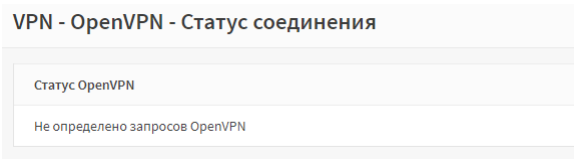


Рис. 666: Статус соединения OpenVPN

2.7.7.4 Журнал

Раздел **«Журнал»** содержит журнал OpenVPN.

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

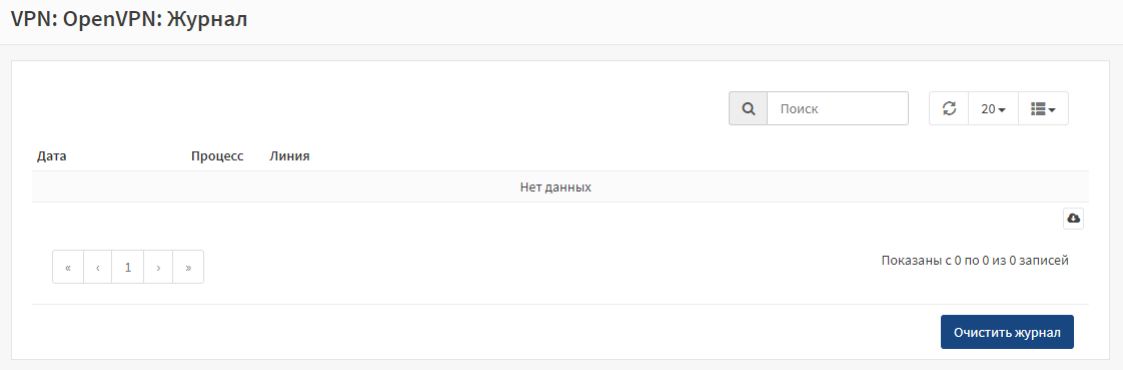


Рис. 667: Журнал OpenVPN

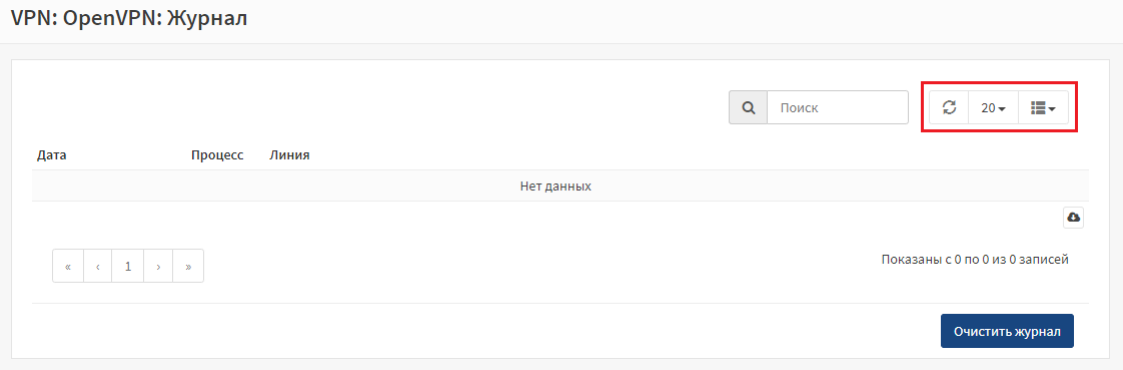


Рис. 668: Фильтры журнала OpenVPN

2.7.8 Службы

Вкладка **«Службы»** содержит:

- **«Потоковый антивирус»** - пакет антивирусного ПО;
- **«Обнаружение вторжений»** - систему обнаружения вторжений;
- **«Мониторинг служб»** - систему мониторинга серверов;
- **«Сетевое время»** - настройки NTP-сервера;
- **«DNS»** - настройки системы DNS;
- **«Веб-прокси»** - прокси сервер;
- **«DHCPv4»** - настройка протокола DHCPv4;
- **«DHCPv6»** - настройка протокола DHCPv6;

2.7.8.1 Потоковый антивирус

Для перехода к настройкам потокового антивируса необходимо:

- нажать на вкладку **«Службы»** - **«Потоковый антивирус»** - **«Конфигурация»**, расположенную в левой части списка объектов управления;

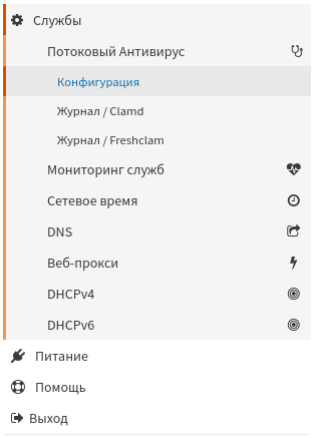


Рис. 669: Переход к настройкам потокового антивируса

Для перехода к просмотру журнала демона **«Clamd»** необходимо:

- нажать на вкладку **«Службы»** - **«Потоковый антивирус»** - **«Журнал/Clamd»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала модуля обновления сигнатур **«Freshclam»** необходимо:

- нажать на вкладку **«Службы»** - **«Потоковый антивирус»** - **«Журнал/Freshclam»**, расположенную в левой части списка объектов управления;

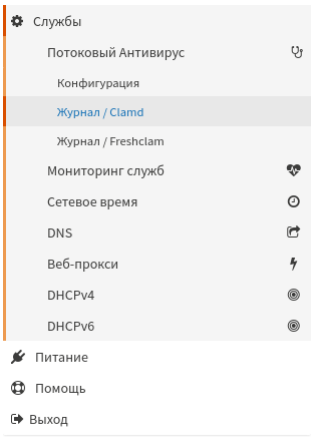


Рис. 670: Переход к просмотру журнала демона **«Clamd»**

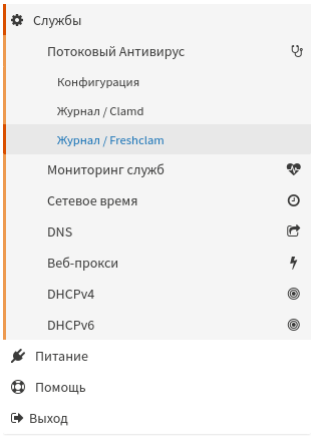


Рис. 671: Переход к просмотру журнала модуля обновления сигнатур **«Freshclam»**

Конфигурация

Общие настройки

Для выполнения общих настроек необходимо:

- в поле **«Включить службу»** установить переключатель в случае необходимости включения сервиса clamd;

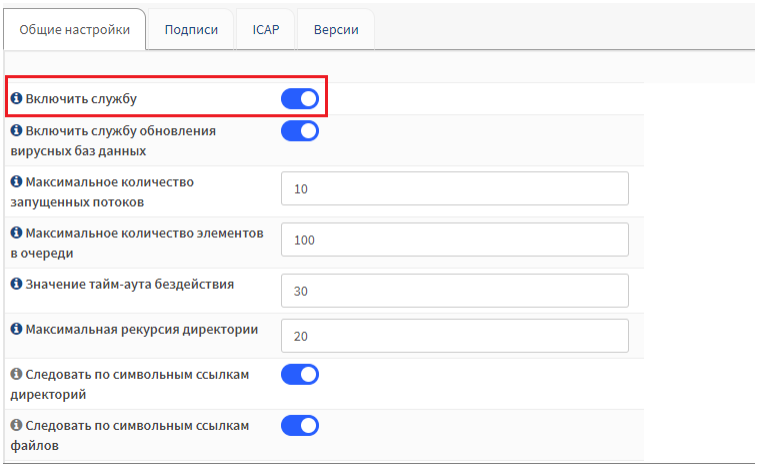


Рис. 672: Включение сервиса clamd

- в поле **«Включить службу обновления вирусных баз данных»** установить переключатель в случае необходимости активировать службу обновления;

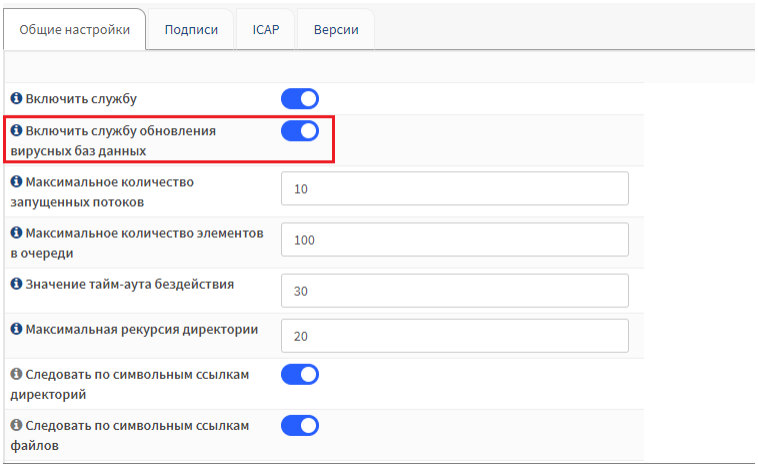


Рис. 673: Включение службы обновления

Примечание

Эта служба будет периодически проверять базу данных на наличие новых вирусов

- в поле **«Максимальное количество запущенных потоков»** указать числовое значение максимального количества потоков, запущенных одновременно;

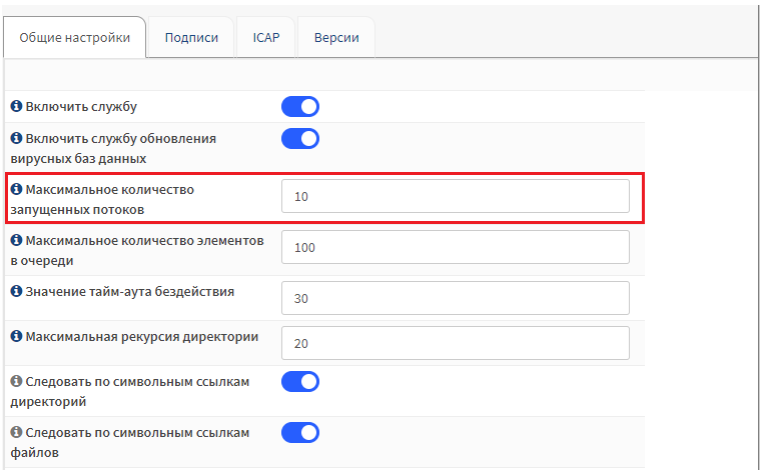


Рис. 674: Установка максимального количества запущенных потоков

- в поле **«Максимальное количество элементов в очереди»** указать числовое значение максимального количества элементов в очереди (включая те, которые обрабатываются потоками MaxThreads);

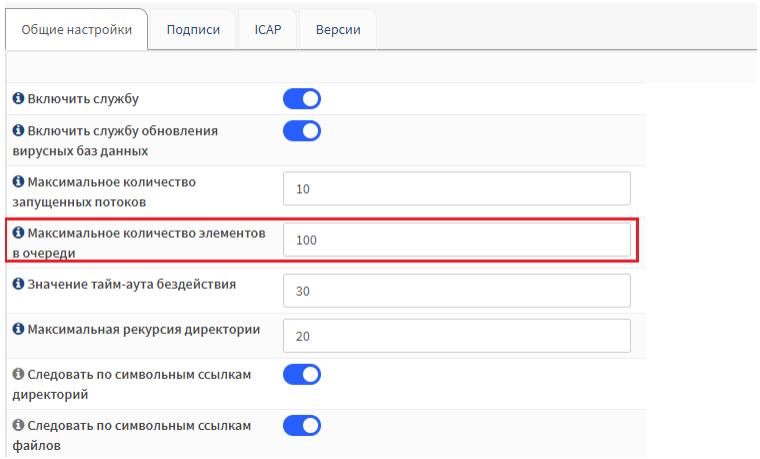


Рис. 675: Установка максимального количества элементов в очереди

Примечание

Рекомендуемое значение как минимум в два раз больше, чем MaxThreads если возможно

- в поле **«Значение тайм-аута бездействия»** указать числовое значение тайм-аута бездействия;

Примечание

Ожидание новой задачи будет окончено после указанного количества секунд

- в поле **«Максимальная рекурсия директории»** указать числовое значение максимальной рекурсии директории;

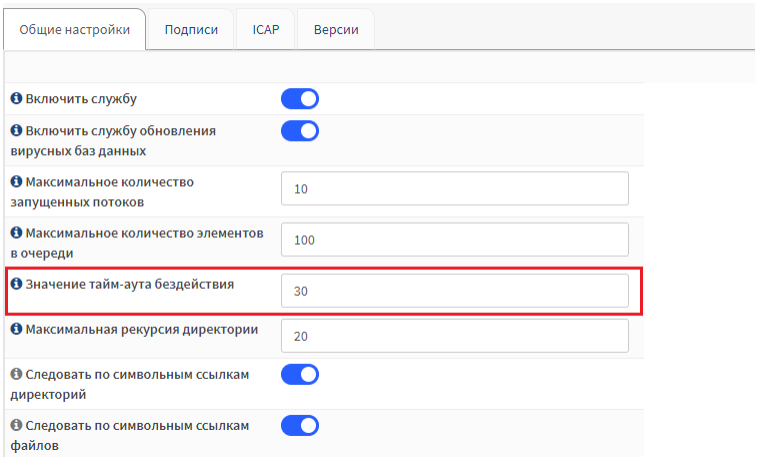


Рис. 676: Установка значения тайм-аута бездействия

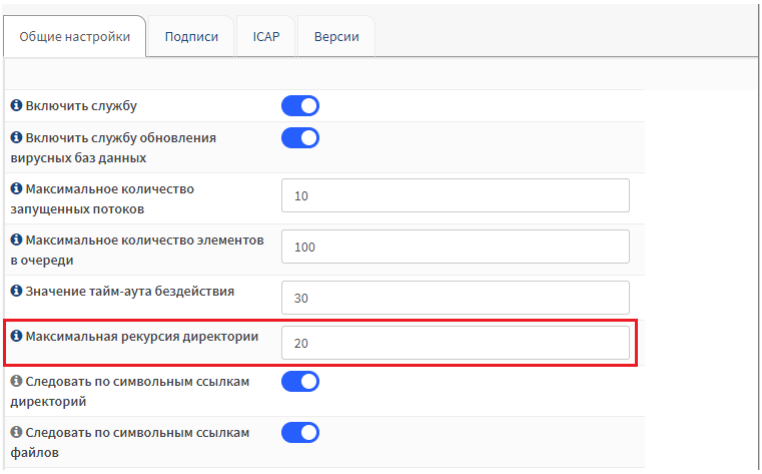


Рис. 677: Установка максимальной рекурсии директории

Примечание

Максимальная глубина директорий для сканирования

- в поле **«Следовать по символьным ссылкам директорий»** установить переключатель в случае необходимости следовать по символьным ссылкам директорий;

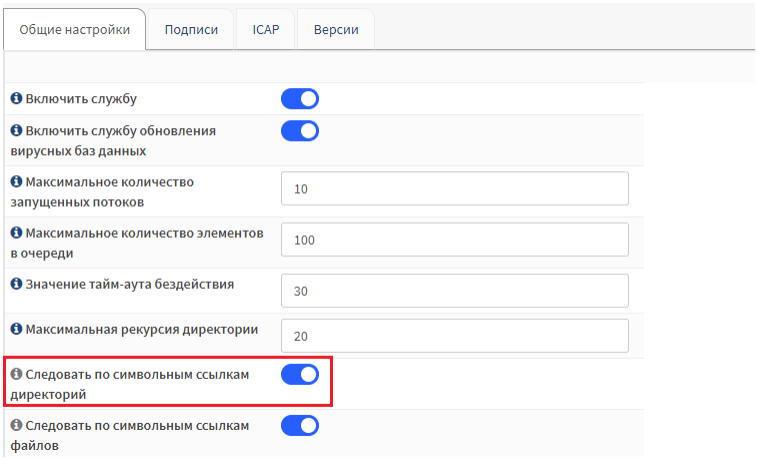


Рис. 678: Установка следования по символьным ссылкам директорий

- в поле **«Следовать по символьным ссылкам файлов»** установить переключатель в случае необходимости следовать по символьным ссылкам файлов;

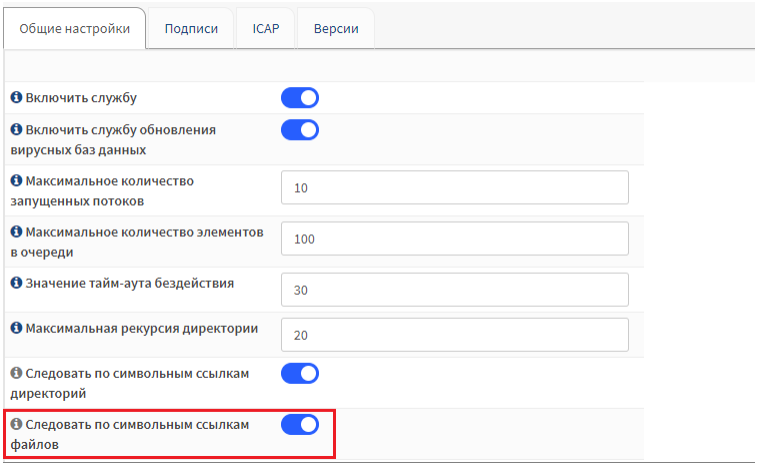


Рис. 679: Установка следования по символьным ссылкам файлов

- в поле **«Отключить кэш»** установить переключатель в случае необходимости отключить кэш;
- в поле **«Сканировать переносимый исполняемый файл»** установить переключатель в случае необходимости сканировать исполняемые файлы;
- в поле **«Сканировать исполняемый файл и формат ссылки»** установить переключатель в случае необходимости сканировать исполняемый файл и формат ссылки;
- в поле **«Обнаруживать повреждённые исполняемые файлы»** установить переключатель в случае необходимости обнаруживать повреждённые исполняемые файлы;

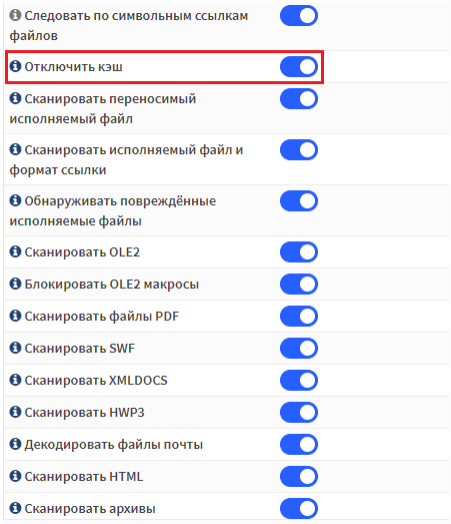


Рис. 680: Отключение кэша

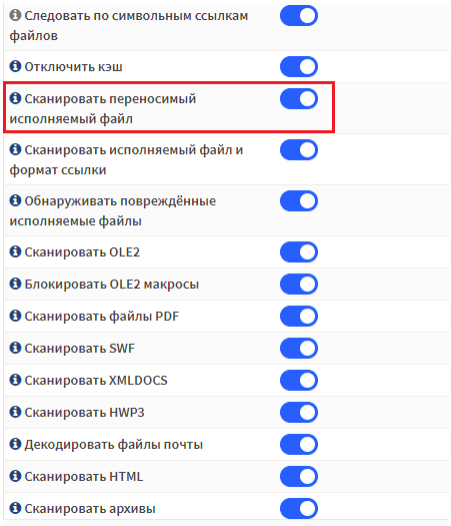


Рис. 681: Сканирование исполняемых файлов

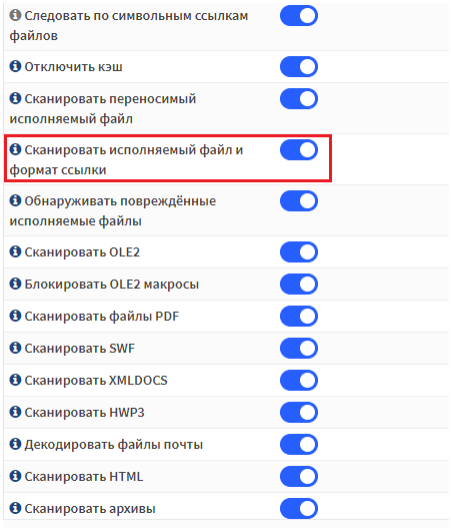


Рис. 682: Сканирование исполняемых файлов и форматов ссылок

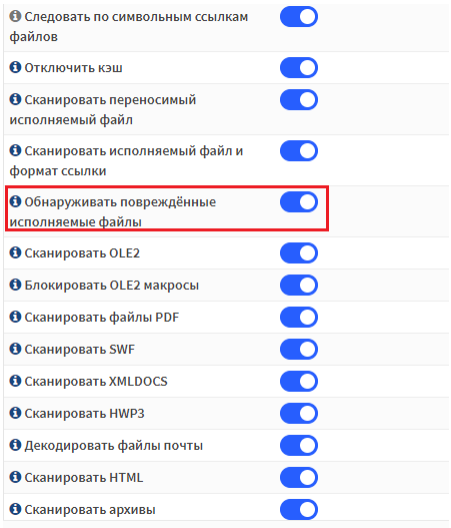


Рис. 683: Поиск повреждённых исполняемых файлов

Примечание

С этой опцией clamav будет пытаться обнаружить повреждённые исполняемые файлы (как PE, так и ELF) и помечать их как Broken

- в поле **«Сканировать OLE2»** установить переключатель в случае необходимости сканировать OLE2-файлы такие, как документы Microsoft Office и .msi файлы;

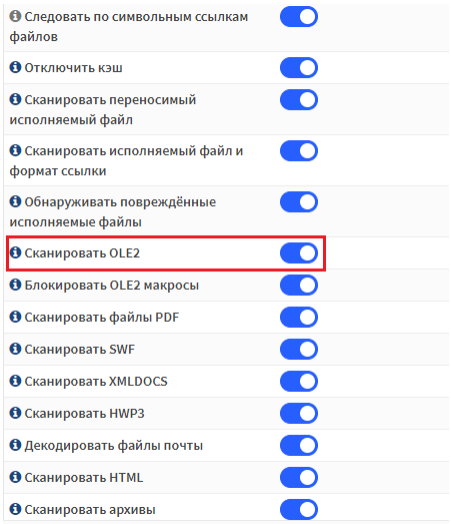


Рис. 684: Сканирование OLE2-файлов

- в поле **«Блокировать OLE2 макросы»** установить переключатель в случае необходимости, чтобы разрешённые файлы OLE2 с VBA макросами, в которых не найдены сигнатуры помечались как «Heuristics.OLE2.ContainsMacros»;

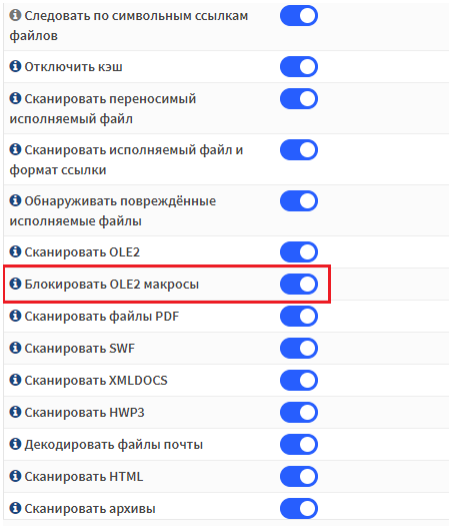


Рис. 685: Блокирование OLE2 макросов

- в поле **«Сканировать файлы PDF»** установить переключатель в случае необходимости сканировать PDF-файлы;

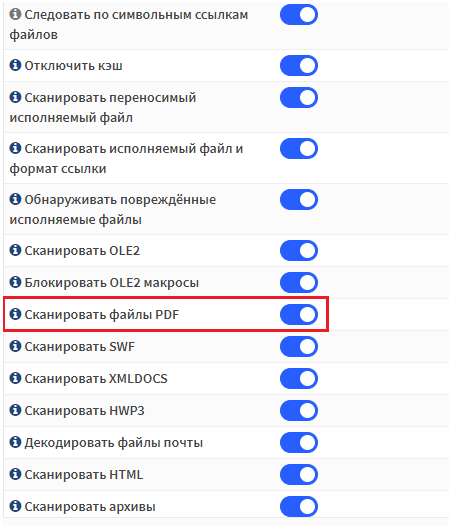


Рис. 686: Сканирование файлов PDF

- в поле **«Сканировать SWF»** установить переключатель в случае необходимости сканировать SWF-файлы;

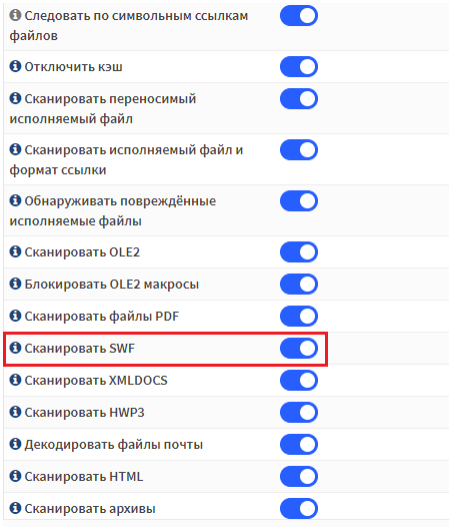


Рис. 687: Сканирование файлов SWF

- в поле **«Сканировать XMLDOCS»** установить переключатель в случае необходимости сканировать файлы xml-документов поддерживаемые libclamav;
- в поле **«Сканировать HWP3»** установить переключатель в случае необходимости сканировать HWP3-файлы;
- в поле **«Декодировать файлы почты»** установить переключатель в случае необходимости декодировать файлы почты;

Примечание

Если вы отключите эту опцию, исходные файлы будут просканированы, но без разбора индивиду-

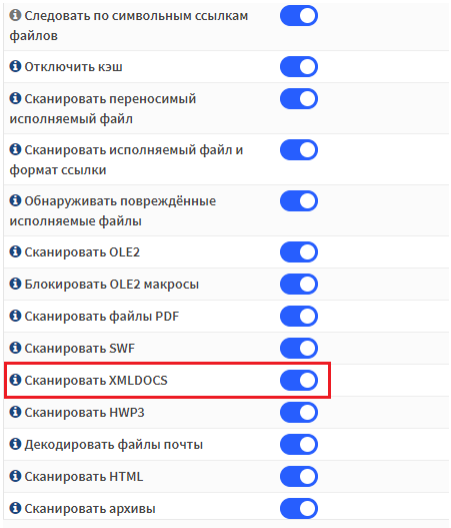


Рис. 688: Сканирование XMLDOCS

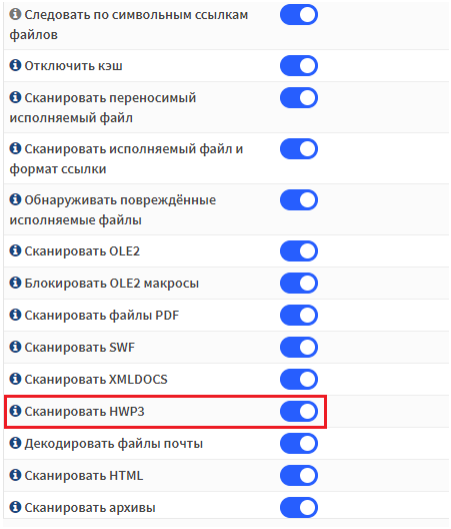


Рис. 689: Сканирование HWP3

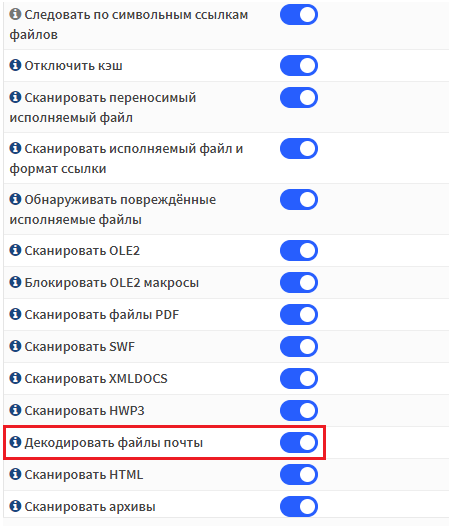


Рис. 690: Декодирование файлов почты

альных сообщений/вложений

- в поле **«Сканировать HTML»** установить переключатель в случае необходимости производить нормализацию HTML и расшифровку кода скриптов MS Script Encoder;

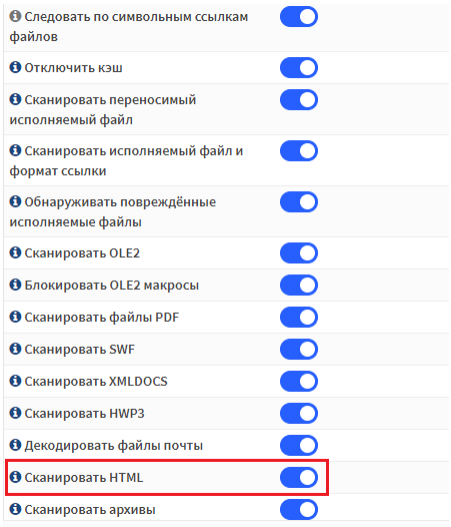


Рис. 691: Сканировать HTML

- в поле **«Сканировать архивы»** установить переключатель в случае необходимости сканировать архивы;
- в поле **«Блокировать зашифрованные архивы»** установить переключатель в случае необходимости помечать зашифрованные архивы, как вирусы (Encrypted.Zip, Encrypted.RAR);
- в поле **«Максимальный размер сканирования»** указать числовое значение максимального количества данных для сканирования для каждого файла;

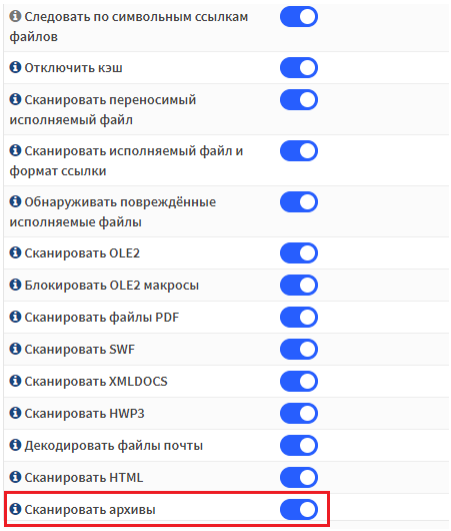


Рис. 692: Сканировать архивы

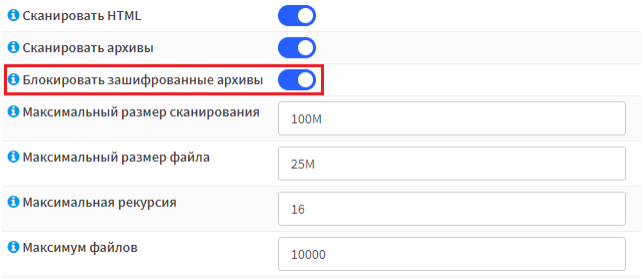


Рис. 693: Блокировать зашифрованные архивы

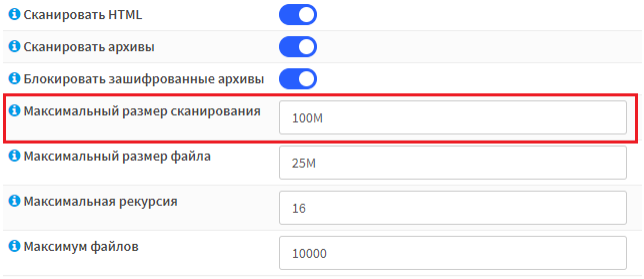


Рис. 694: Максимальный размер сканирования

Примечание

Архивы и другие контейнеры рекурсивно извлекаются и сканируются до этого значения

- в поле **«Максимальный размер файла»** указать числовое значение максимального размера файла для сканирования;

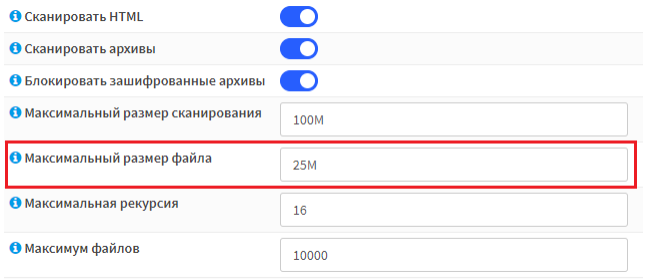


Рис. 695: Максимальный размер файла

Примечание

Файлы большие, чем этот лимит не будут сканироваться

- в поле **«Максимальная рекурсия»** указать числовое значение максимальной рекурсии;

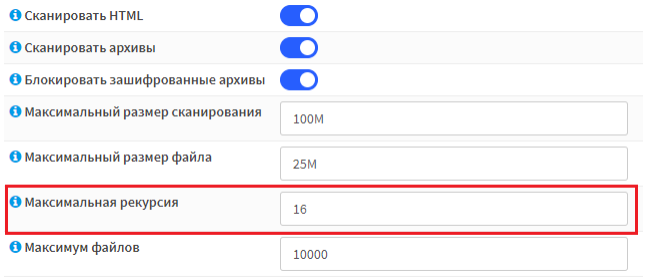


Рис. 696: Максимальная рекурсия

Примечание

Вложенные архивы сканируются рекурсивно, т.е. если Zip архив содержит RAR файл, все файлы в нём также будут просканированы

- в поле **«Максимум файлов»** указать максимальное числовое значение сканируемых файлов, сканируемых в архиве, документе, или любом другом контейнере;
- в поле **«Детальность лога freshclam»** установить переключатель в случае необходимости подробного протоколирования;
- в поле **«Зеркало базы данных freshclam»** ознакомиться с зеркалом базы данных;

Примечание

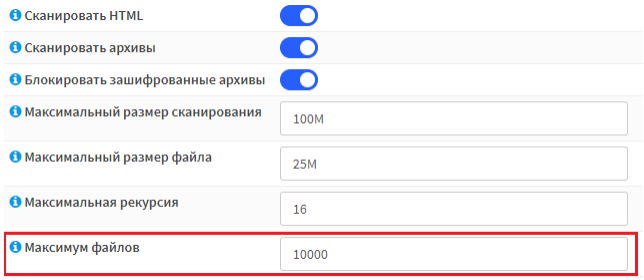


Рис. 697: Максимум файлов

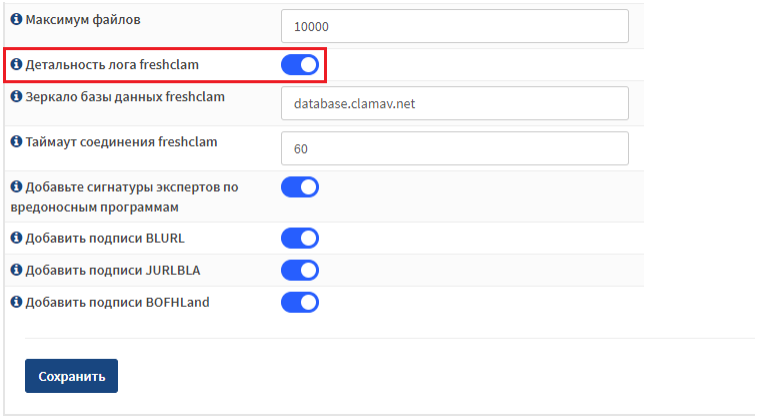


Рис. 698: Детальность лога freshclam

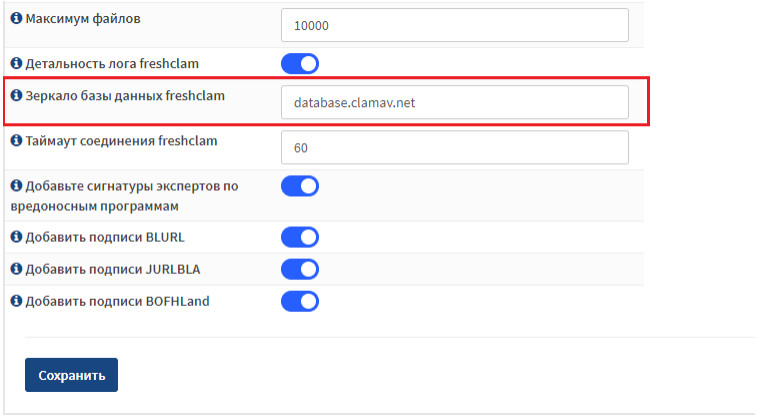


Рис. 699: Зеркало базы данных freshclam

database.clamav.net это кольцевой массив, указывающий на наиболее надёжные зеркала

Внимание

Не трогайте данную настройку, только если вы не знаете, что вы делаете

- в поле **«Таймаут соединения freshclam»** указать числовое значение таймаута в секундах для подключения к серверу базы данных;

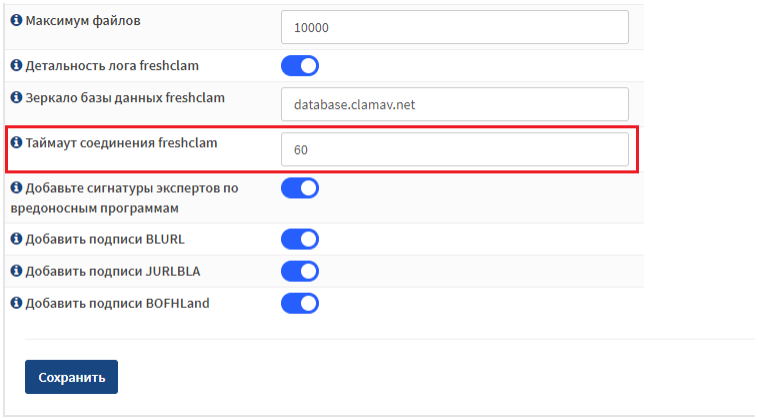


Рис. 700: Таймаут соединения freshclam

- в поле **«Добавьте сигнатуры экспертов по вредоносным программам»** установить переключатель в случае необходимости активировать сигнатуры третьих лиц от Malware Expert;

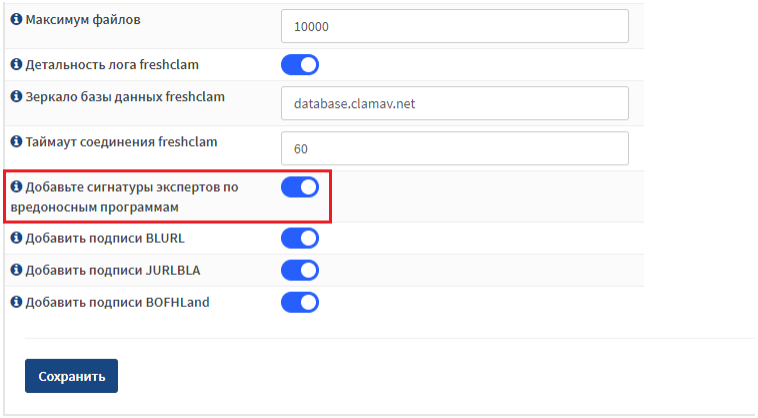


Рис. 701: Добавьте сигнатуры экспертов по вредоносным программам

Осторожно

Используйте на свой риск

- в поле **«Добавить подписи BLURL»** установить переключатель в случае необходимости активировать сторонние подписи из BURL;

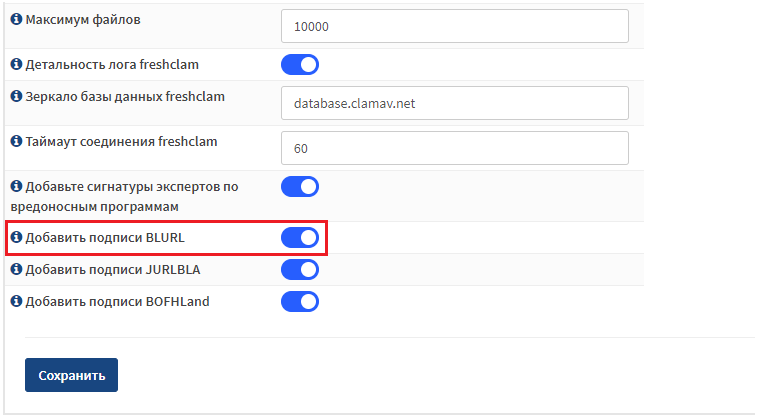


Рис. 702: Добавить подписи BLURL

Осторожно

Используйте на свой риск

- в поле **«Добавить подписи JURLBLA»** установить переключатель в случае необходимости активировать сторонние подписи от Sanesecurtiy JURLBLA;

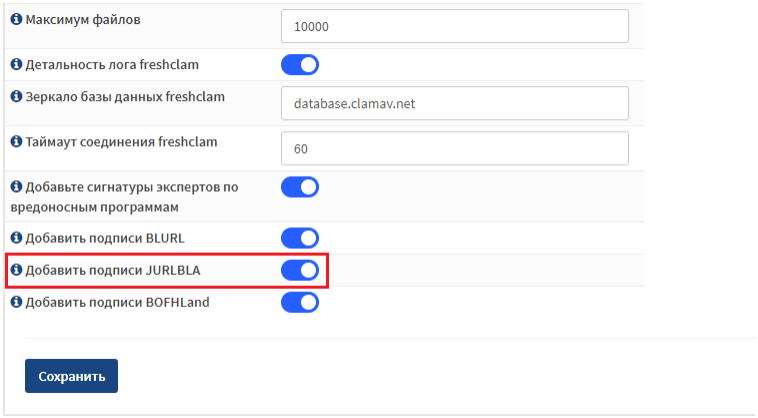


Рис. 703: Добавить подписи JURLBLA

Осторожно

Используйте на свой риск

- в поле **«Добавить подписи BOFHLand»** установить переключатель в случае необходимости активировать сторонние подписи от Sanesecurtiy BOFHLand;

Осторожно

Используйте на свой риск

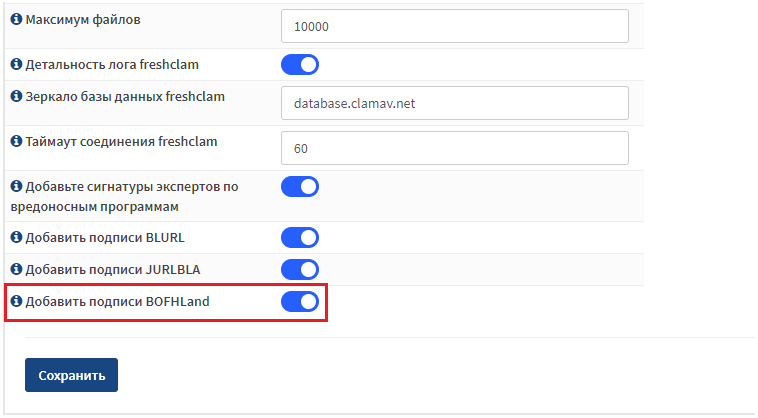


Рис. 704: Добавить подписи BOFHLand

- нажать кнопку **«Сохранить»** 

.

Подписи

Для добавления новой подписи в таблицу подписей необходимо нажать кнопку «+» 
.

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости включить список;

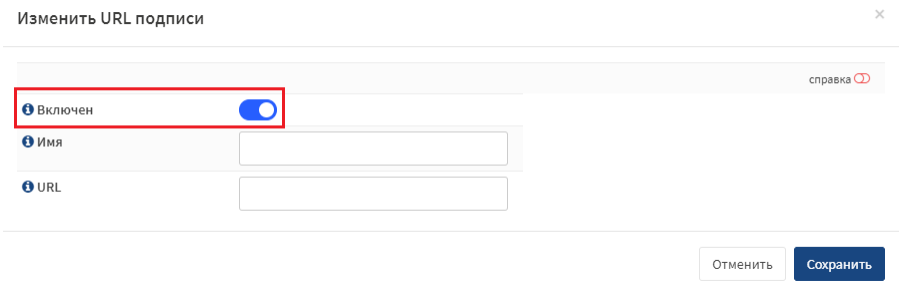


Рис. 705: Включение списка

- в поле **«Имя»** установить имя для этой подписи;
- в поле **«URL»** установить URL базы данных подписей;
- нажать кнопку **«Сохранить»** 

.

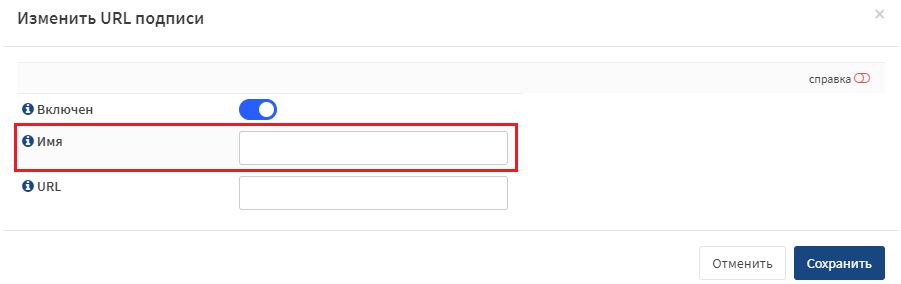


Рис. 706: Установка имени подписи

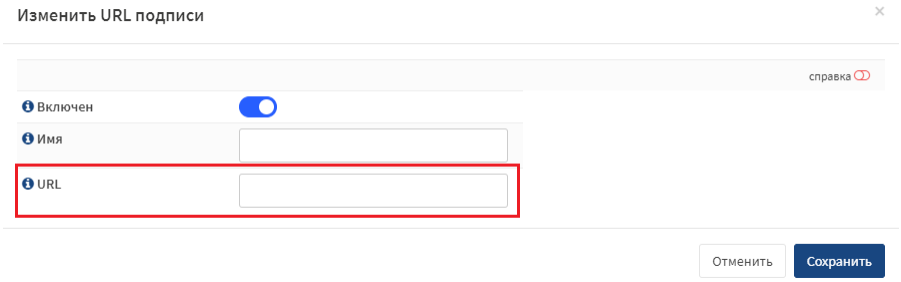


Рис. 707: Установка URL базы данных подписей

ICAP

Общие настройки

В разделе **«Общие настройки»** необходимо:

- в поле **«Включить сервис icap»** установить переключатель в случае необходимости включить сервис ICAP;

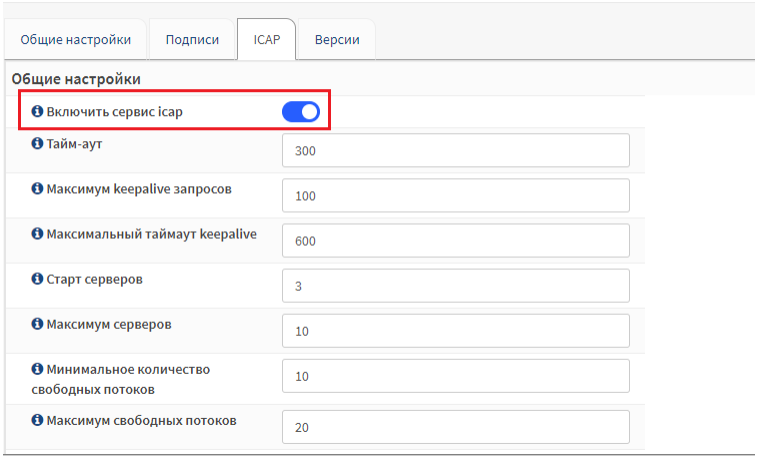


Рис. 708: Включить сервис icap

- в поле **«Тайм-аут»** указать числовое значение таймаута в секундах после которого неактивное соединение может быть прервано;

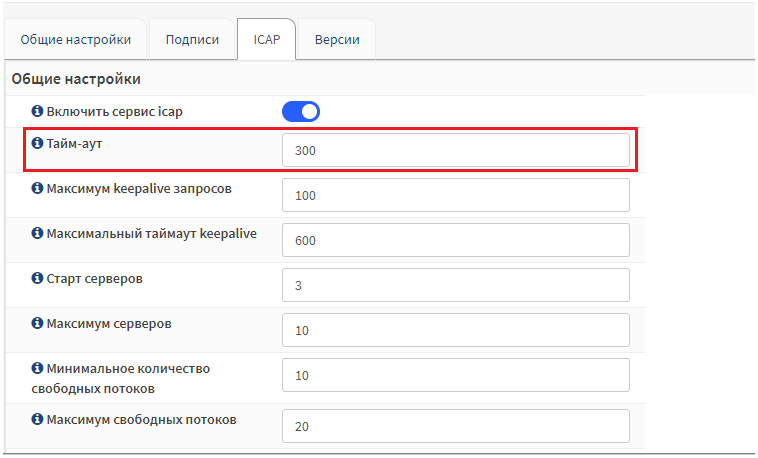


Рис. 709: Тайм-аут

- в поле **«Максимум keepalive запросов»** указать максимальное числовое значение запросов, которое может обслужить одно соединение

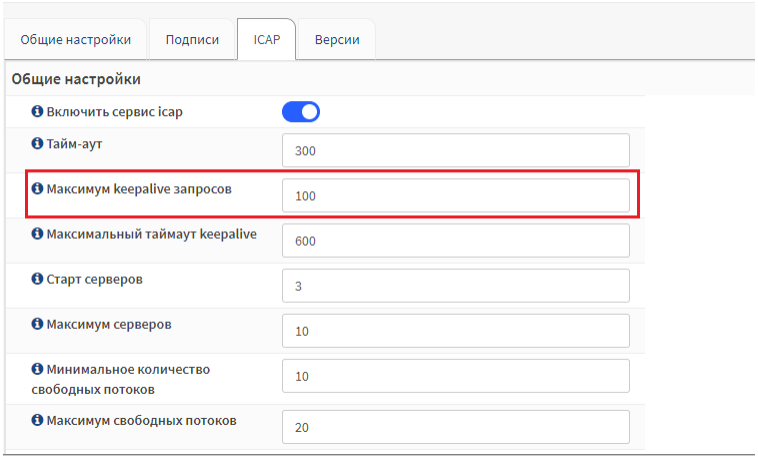


Рис. 710: Максимум keepalive запросов

- в поле **«Максимальный таймаут keepalive»** указать максимальное числовое значение времени в секундах ожидания нового запроса, прежде чем соединение будет закрыто;
- в поле **«Старт серверов»** указать исходное число процессов сервера;

Примечание

Каждый процесс сервера генерирует определённое число потоков, которые обслуживают запросы

- в поле **«Максимум серверов»** указать максимальное число процессов сервера;
- в поле **«Минимальное количество свободных потоков»** указать числовое значение минимального количества свободных потоков;

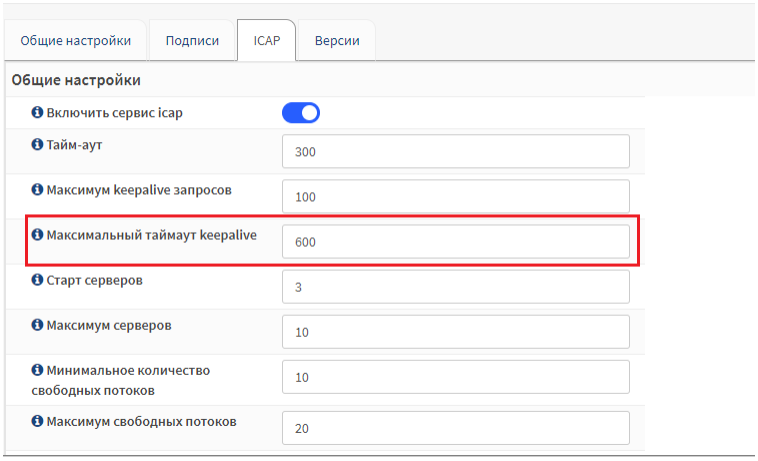


Рис. 711: Максимальный таймаут keepalive

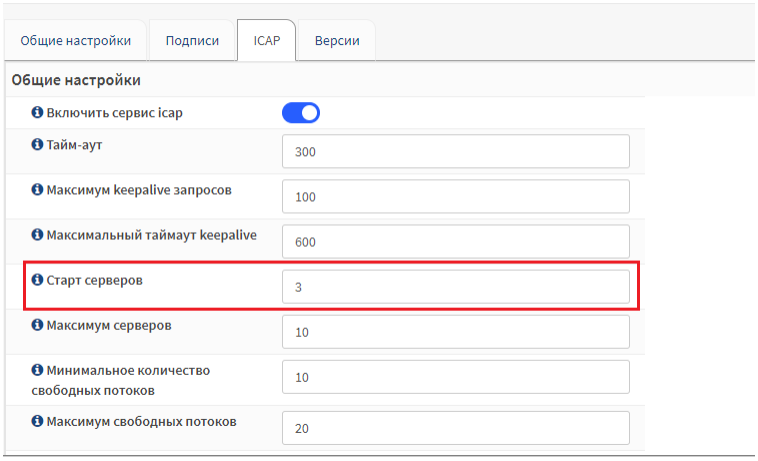


Рис. 712: Старт серверов

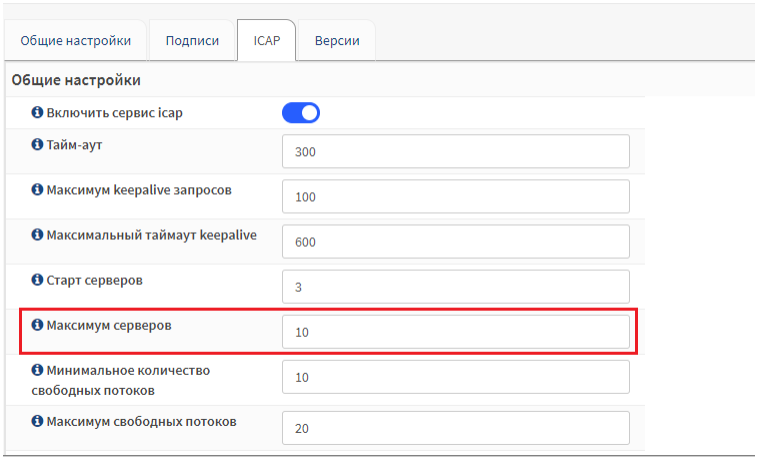


Рис. 713: Максимум серверов

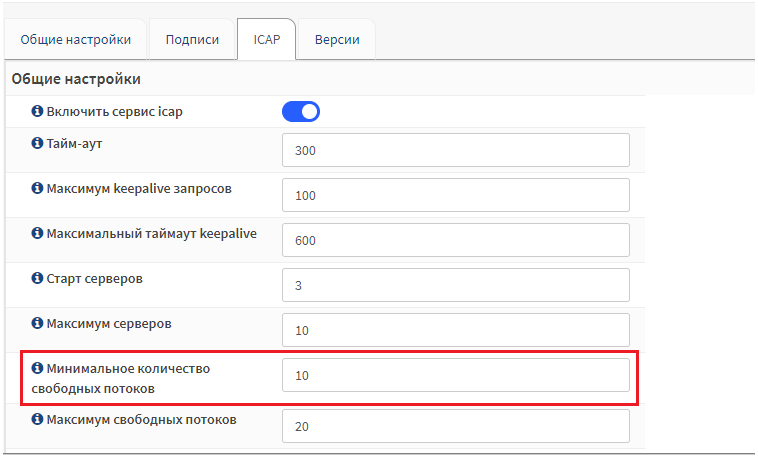


Рис. 714: Минимальное количество свободных потоков

Примечание

Если количество доступных потоков меньше числа, сервер icap запускает новый дочерний поток

- в поле **«Максимум свободных потоков»** указать числовое значение максимального количества свободных потоков;

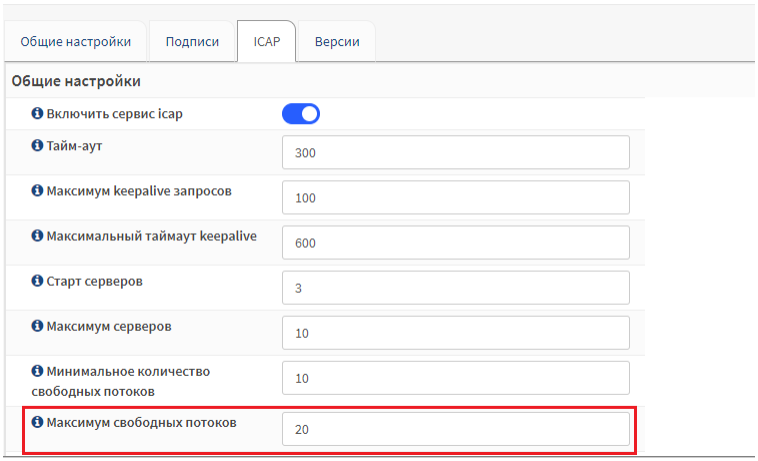


Рис. 715: Максимум свободных потоков

Примечание

Если количество доступных потоков больше числа, то icap-сервер убивает дочерний процесс

- в поле **«Потоков на потомка»** указать числовое значение потоков в дочернем процессе;
- в поле **«Максимум запросов на потомка»** указать максимальное числовое значение запросов, которое может обслужить дочерний процесс;

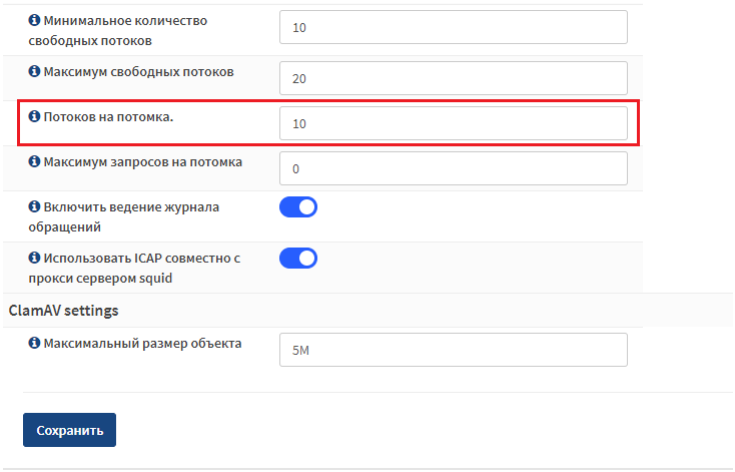


Рис. 716: Потоков на потомка

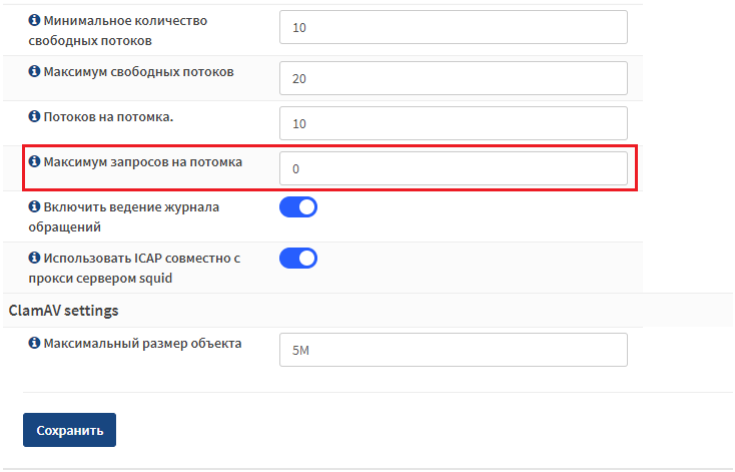


Рис. 717: Максимум запросов на потомка

Примечание

При достижении этого числа процесс завершается

- в поле **«Включить ведение журнала обращений»** установить переключатель в случае необходимости вести журнал доступа;

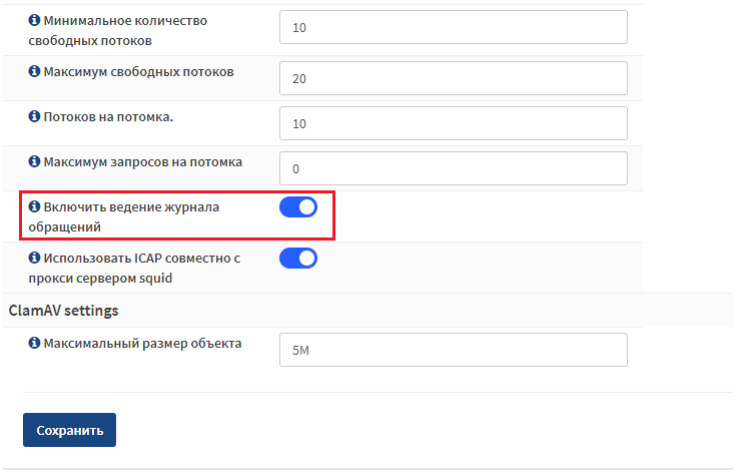


Рис. 718: Включить ведение журнала обращений

- в поле **«Использовать ICAP совместно с прокси сервером squid»** установить переключатель в случае необходимости взять настройки имени пользователя из локального squid;

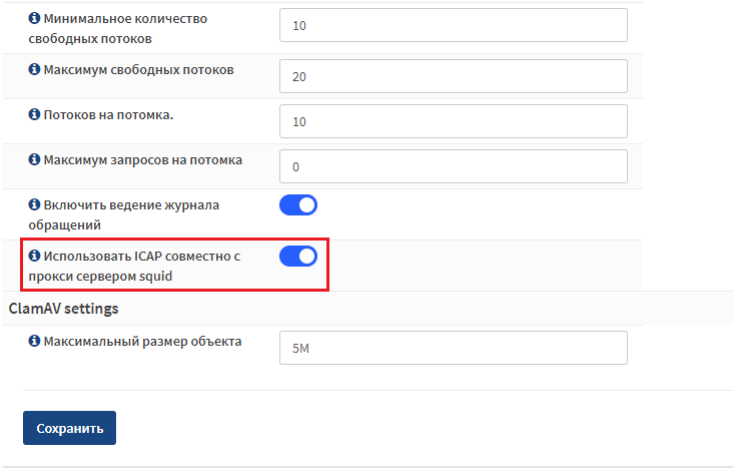


Рис. 719: Использовать ICAP совместно с прокси сервером squid

ClamAV settings

В разделе **«ClamAV settings»** необходимо:

- в поле **«Максимальный размер объекта»** указать максимальное числовое значение размера файлов для сканирования службой антивируса;

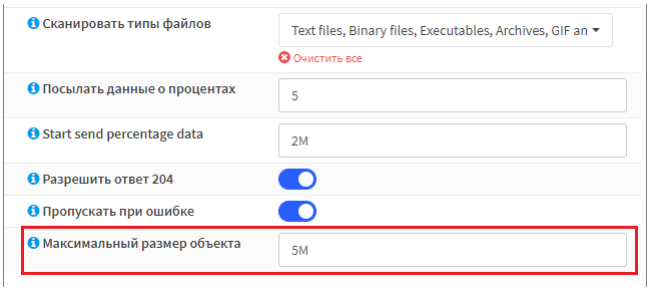


Рис. 720: Максимальный размер объекта

Совет

Пользователь может использовать K и M индикаторы для обозначения размера в килобайтах и мегабайтах

- нажать кнопку **«Сохранить»** 

.

Версии

На вкладке **«Версии»** содержится информация о текущей версии антивируса Clam AV.

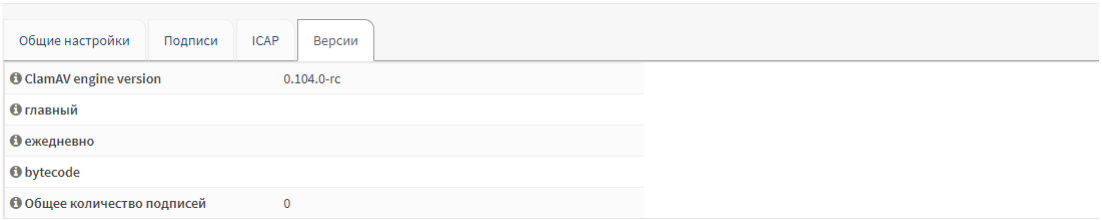


Рис. 721: Вкладка **«Версии»**

Журнал/Clamd

Раздел **«Журнал/Clamd»** содержит журнал демона Clamd.

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

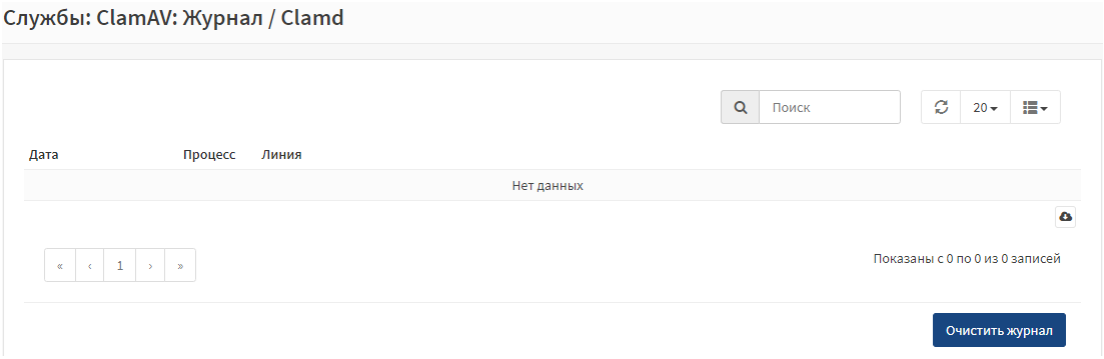


Рис. 722: Журнал демона Clamd

С помощью фильтров можно ограничить или расширить данные журнала.

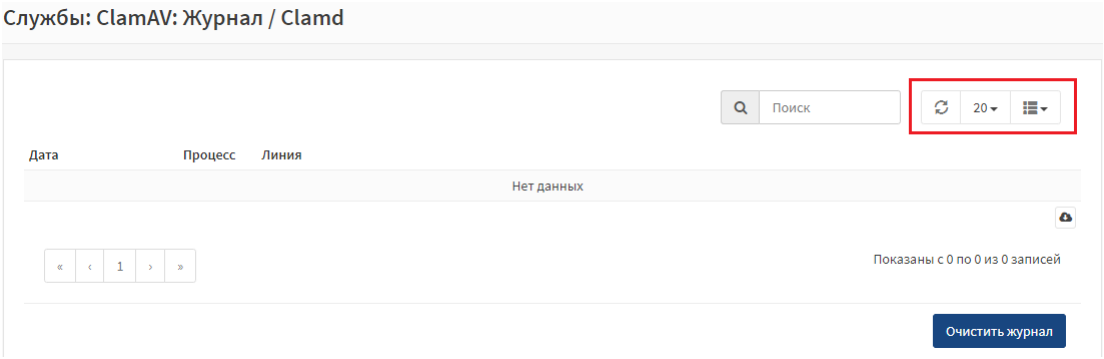


Рис. 723: Фильтры журнала демона **«Clamd»**

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

Журнал/Freshclam

Раздел **«Журнал/Freshclam»** содержит журнал модуля обновления сигнатур **«Freshclam»**.

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

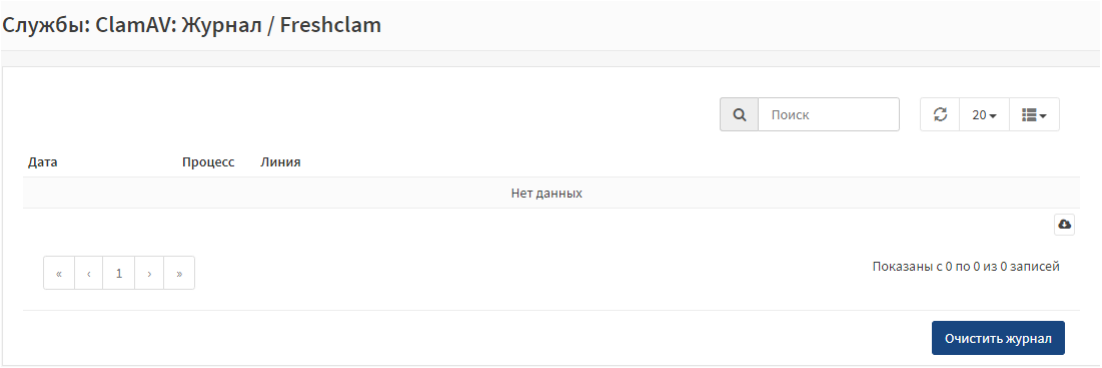


Рис. 724: Журнал модуля обновления сигнатур **«Freshclam»**

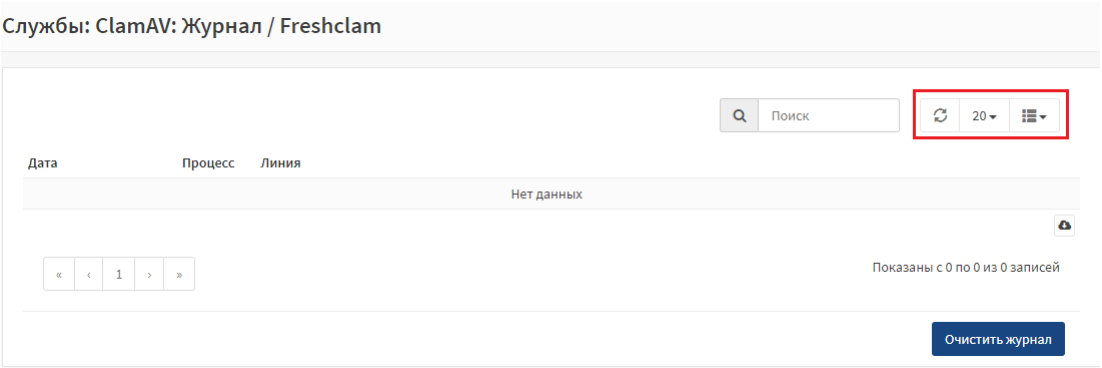


Рис. 725: Фильтры журнала модуля обновления сигнатур **«Freshclam»**

2.7.8.2 Обнаружение вторжений

Для перехода к настройкам системы обнаружения вторжений необходимо:

- нажать на вкладку **«Службы»** - **«Обнаружение вторжений»** - **«Администрирование»**, расположенную в левой части списка объектов управления;

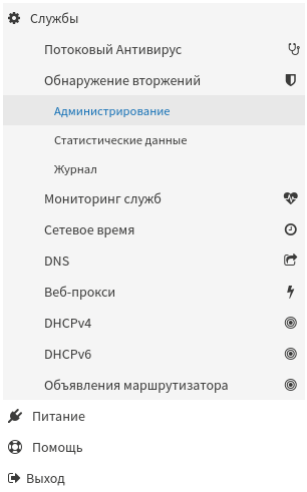


Рис. 726: Переход к настройкам системы обнаружения вторжений

Для перехода к просмотру статистических данных необходимо:

- нажать на вкладку **«Службы»** - **«Обнаружение вторжений»** - **«Статистические данные»**, расположенную в левой части списка объектов управления;

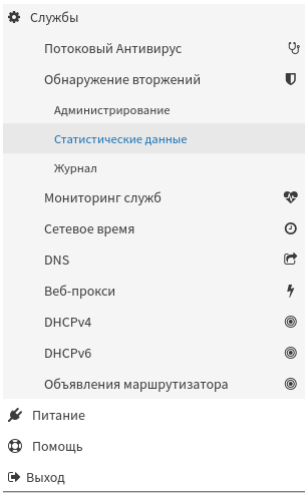


Рис. 727: Переход к просмотру статистических данных

Для перехода к просмотру журнала системы обнаружения вторжений необходимо:

- нажать на вкладку **«Службы»** - **«Обнаружение вторжений»** - **«Журнал»**, расположенную в левой части списка объектов управления;

Для запуска службы необходимо нажать кнопку  , находящуюся в верхнем правом углу окна.

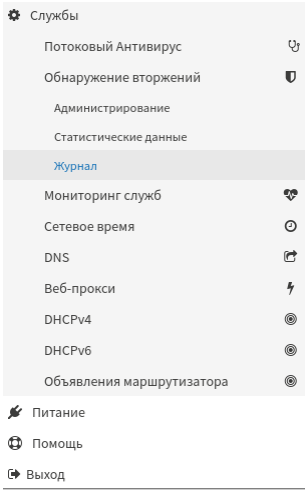


Рис. 728: Переход к просмотру журнала системы обнаружения вторжений

Администрирование

Настройки

Для выполнения настроек необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости включения системы обнаружения вторжений;

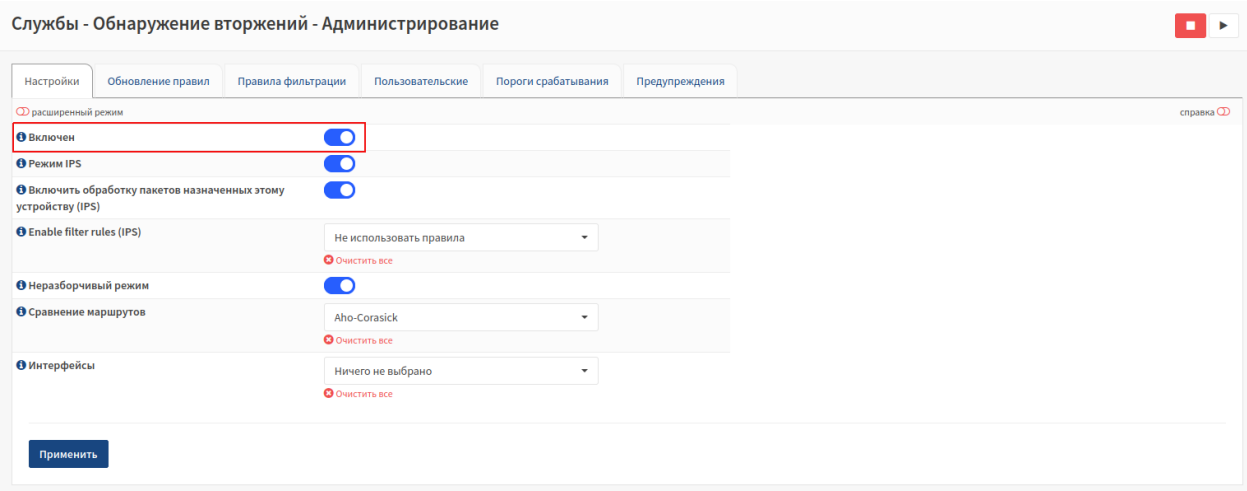


Рис. 729: Включение системы обнаружения вторжений

- в поле **«Режим IPS»** установить переключатель в случае необходимости включения режима предотвращения вторжений (блокировка вредоносных данных);
- в поле **«Включить обработку пакетов назначенных этому устройству (IPS)»** установить переключатель в случае необходимости Включить обработку пакетов, предназначенных устройству;

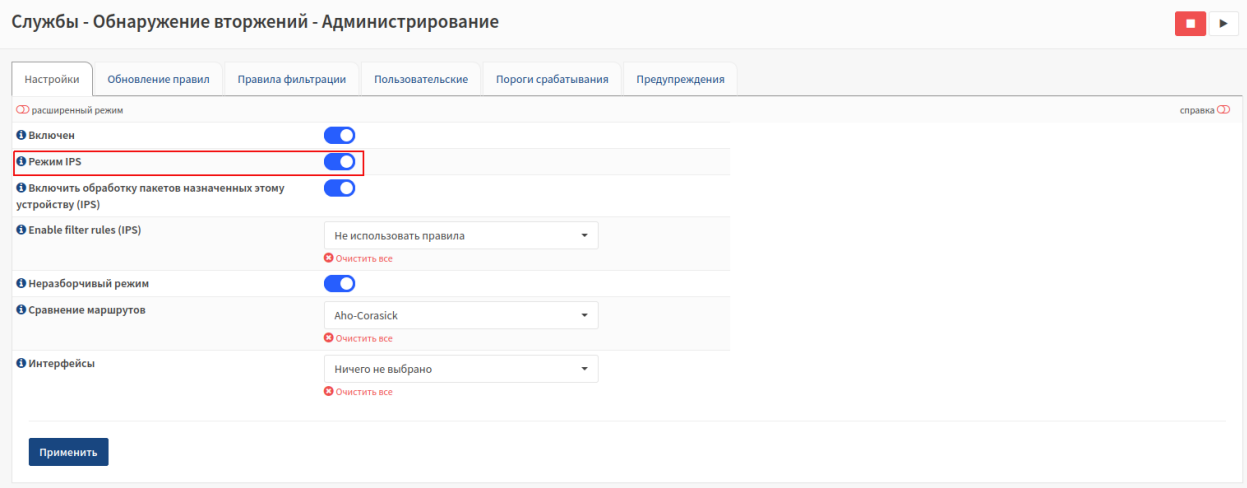


Рис. 730: Включение режима IPS

Совет

Во включенном состоянии будут обрабатываться только пакеты, пересылаемые к другим хостам

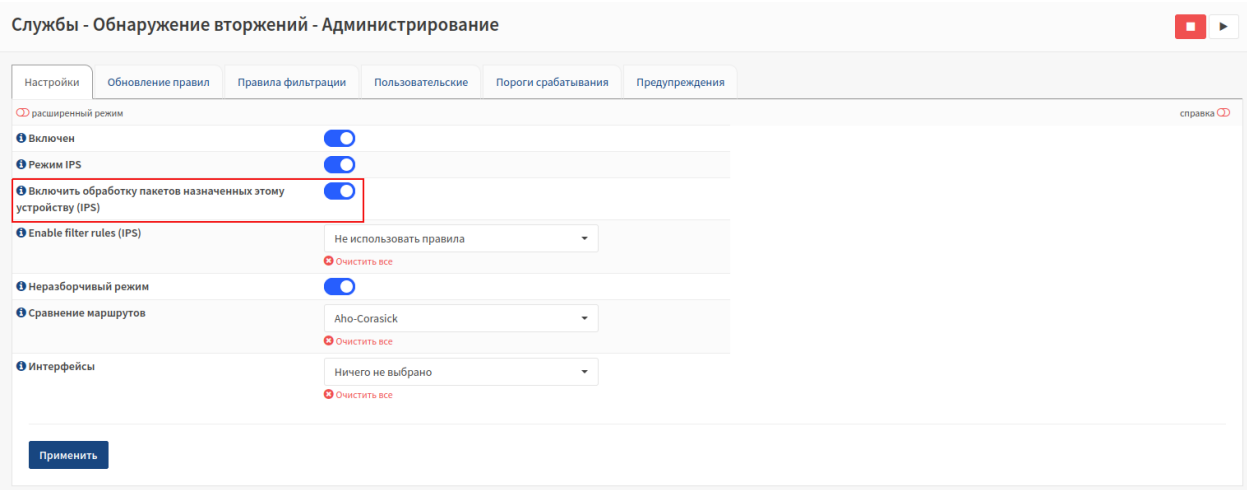


Рис. 731: Включение обработки пакетов

- в поле **«Enable filter rules (IPS)»** выбрать из выпадающего списка необходимые действия, производимые с правилами фильтрации на заданных интерфейсах;
- в поле **«Неразборчивый режим»** установить переключатель в случае необходимости захвата данных на физическом интерфейсе;
- в поле **«Сравнение маршрутов»** выбрать из выпадающего списка необходимые алгоритм поиска совпадений множественных шаблонов;
- в поле **«Интерфейсы»** выбрать из выпадающего списка необходимые интерфейсы, которые будут использоваться;

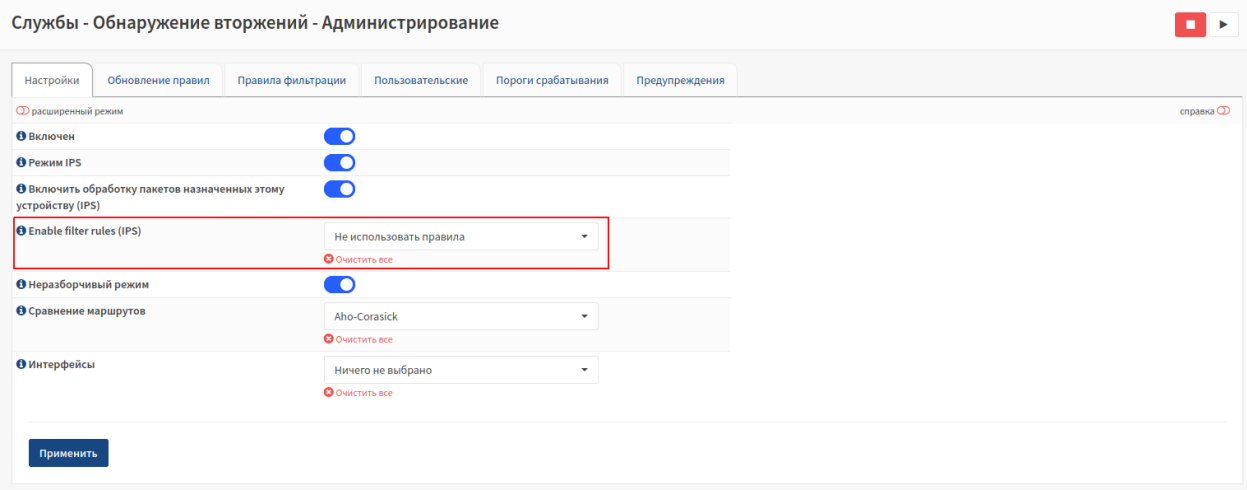


Рис. 732: Включение правил фильтрации

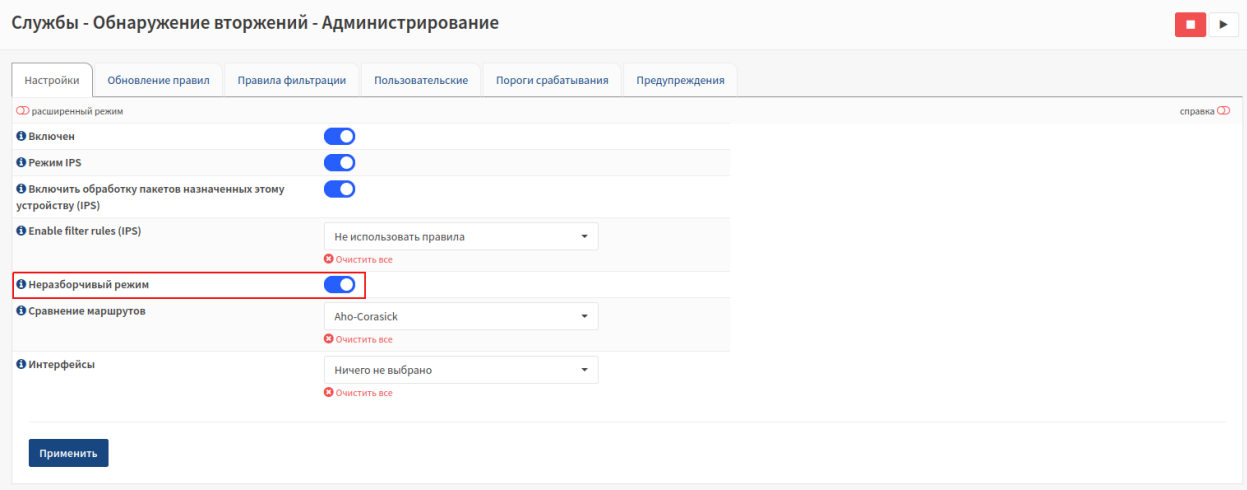


Рис. 733: Включение функции Неразборчивый режим

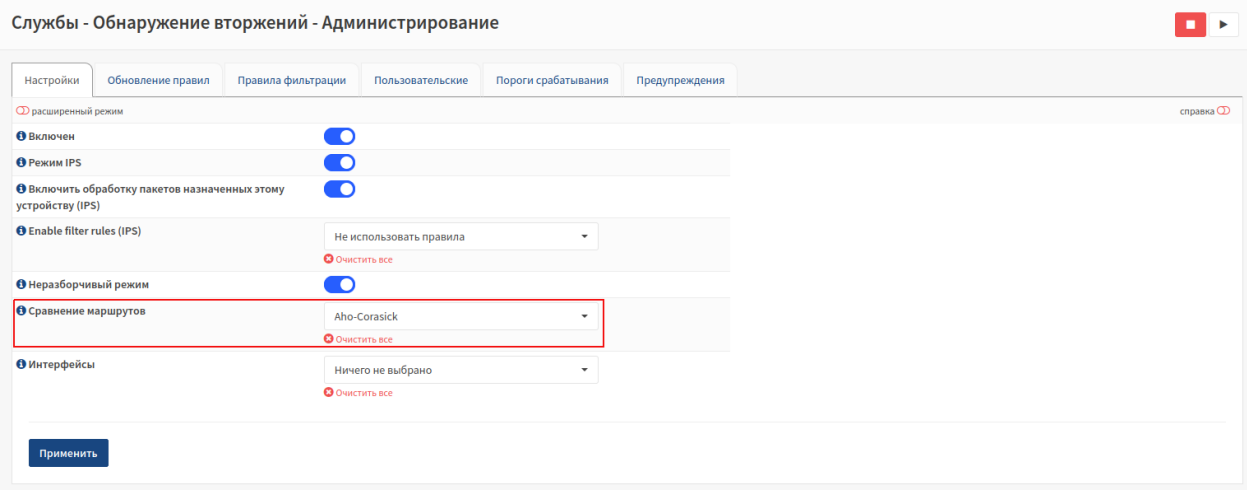


Рис. 734: Включение функции Сравнение маршрутов

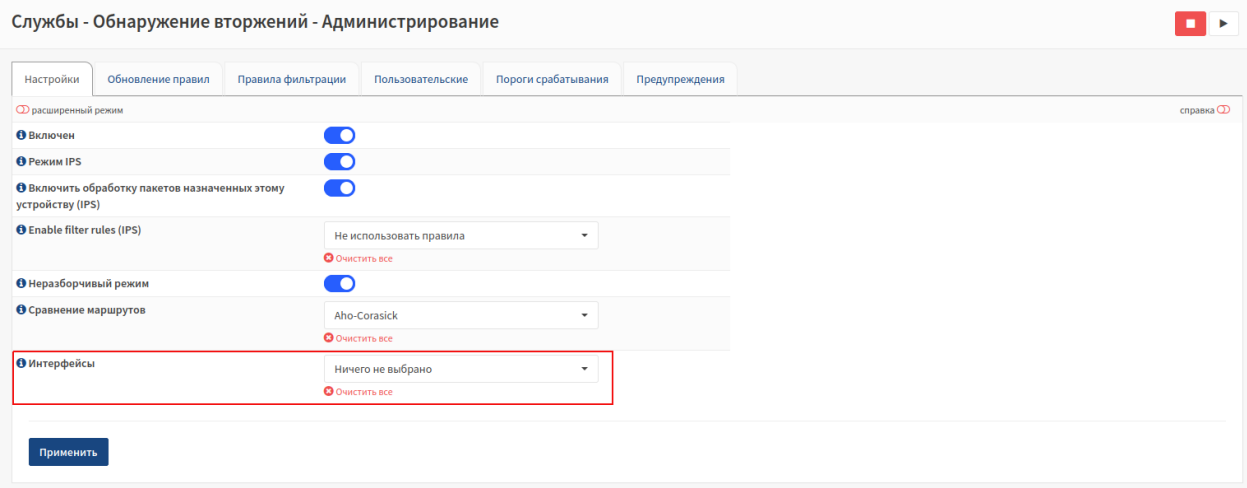


Рис. 735: Выбор интерфейса

Совет

Если включен IPS, необходимо использовать только физические интерфейсы (не VLAN и т. д.)

Для включения режима расширенных настроек необходимо установить переключатель.

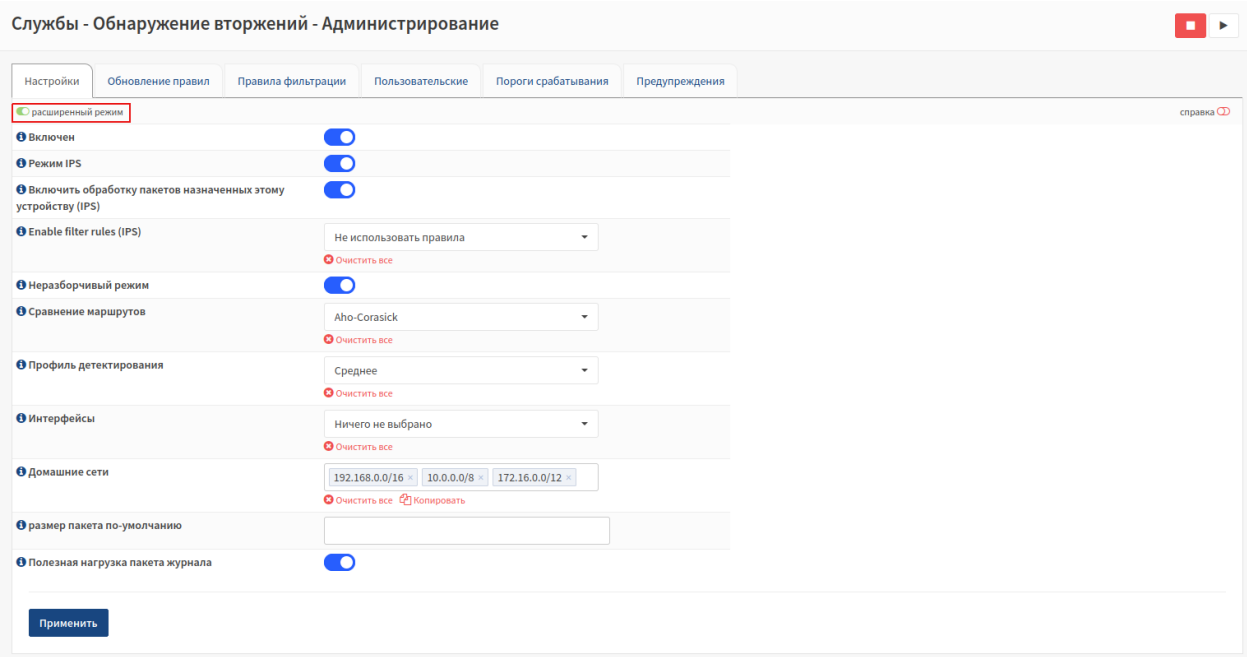


Рис. 736: Включение расширенных настроек

В режиме расширенных настроек необходимо:

- в поле **«Профиль детектирования»** выбрать из выпадающего списка необходимое значение загрузки оперативной памяти;

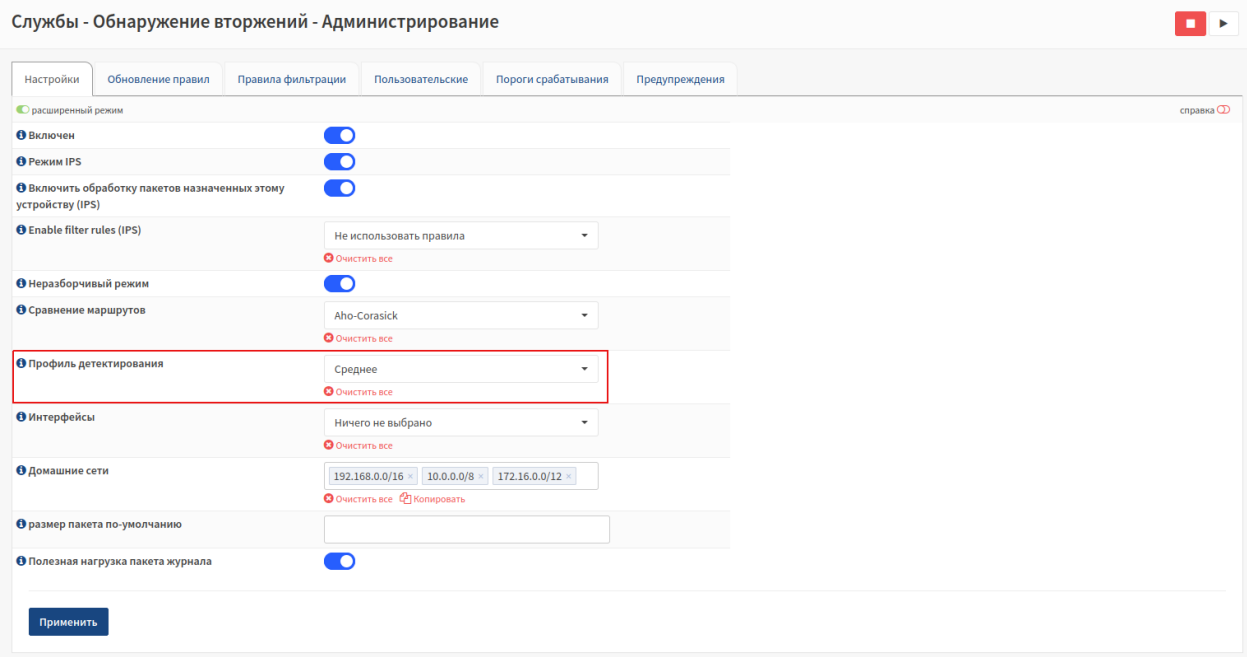


Рис. 737: Выбор Профиля детектирования

Совет

Система обнаружения вторжений генерирует внутренние группы сигнатур. Профиль позволяет эффективно управлять оперативной памятью, что в конечном результате влияет на производительность

- в поле **«Домашние сети»** ввести IP-адреса сетей, которые следует интерпретировать как локальные;
- в поле **«размер пакета по умолчанию»** установить размер пакетов в вашей сети;

Совет

Иногда должны быть обработаны пакеты большего размера. Механизм обработки может обработать эти большие пакеты, но их обработка снижает производительность

- в поле **«Полезная нагрузка пакета журнала»** установить переключатель в случае необходимости отправки полезной нагрузки пакета в журнал для дальнейшего анализа;

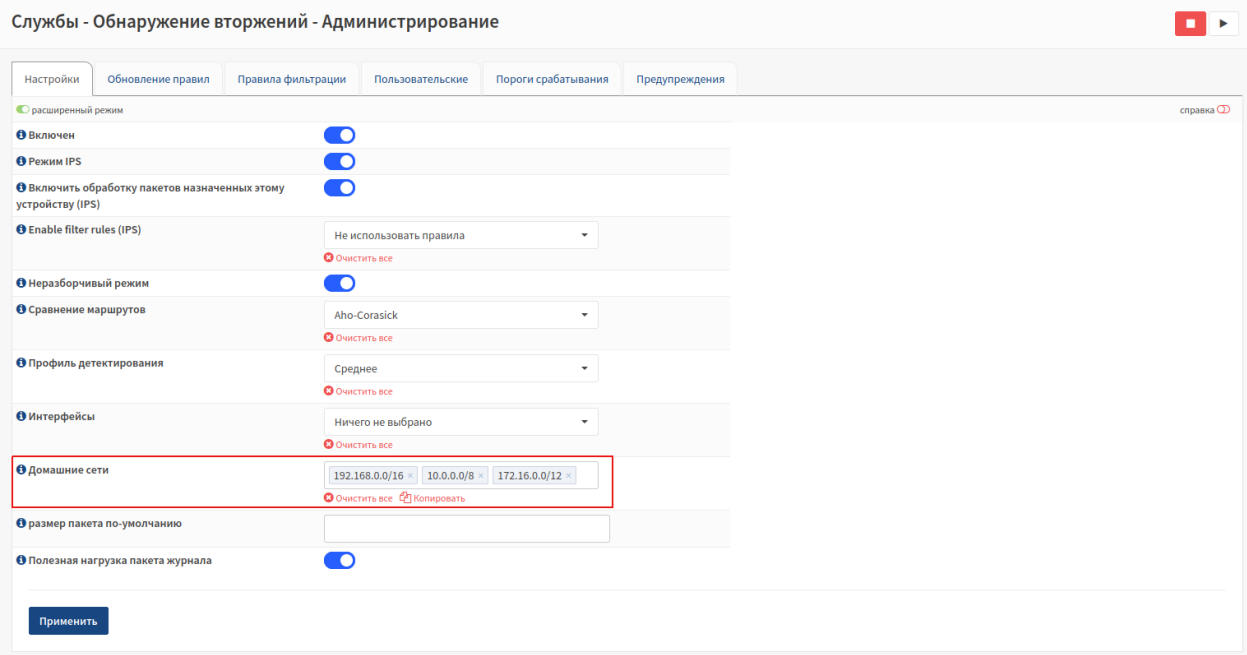


Рис. 738: Установка домашних сетей

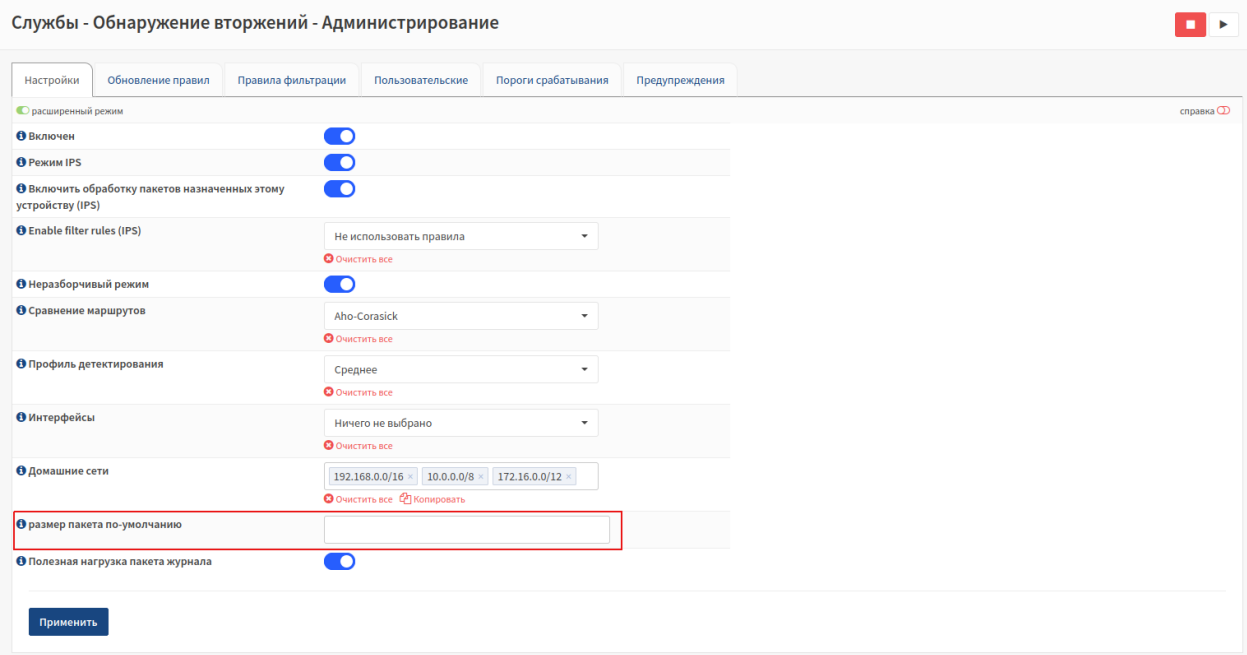


Рис. 739: Установка размера пакета

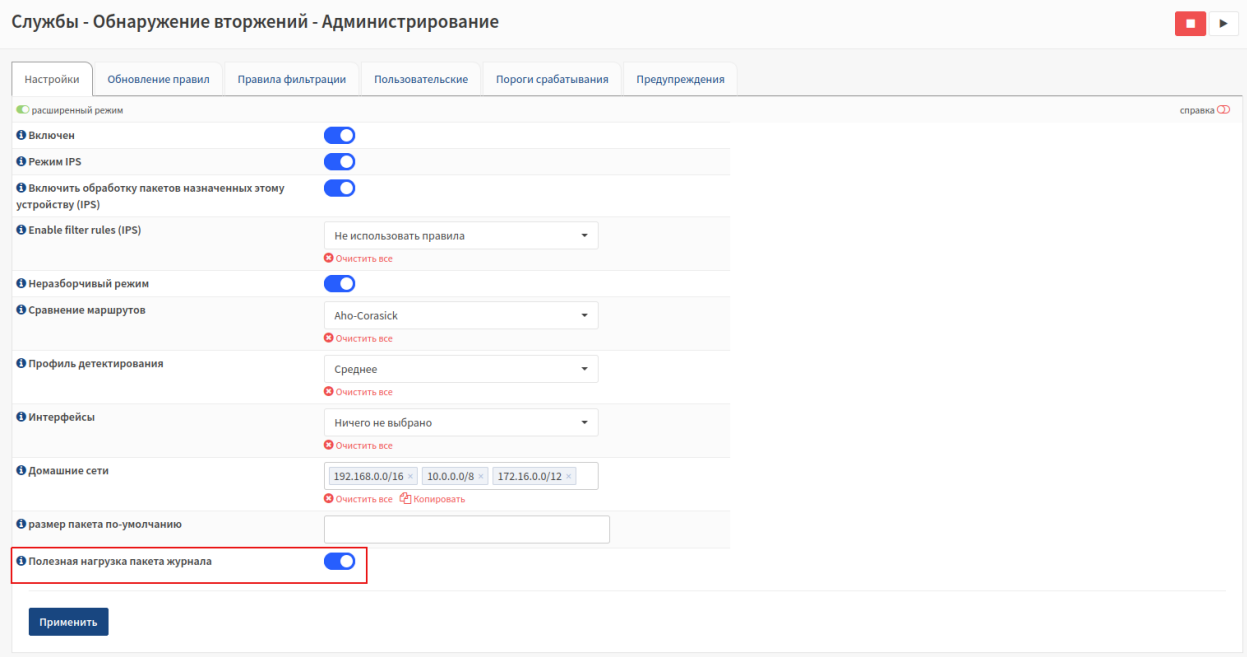


Рис. 740: Включение полезной нагрузки пакета журнала

Обновление правил

Вкладка **«Обновление правил»** содержит таблицу наборов правил, представленную на рисунке.

Для работы с актуальными правилами необходимо скачать и обновить правила, нажав кнопку Скачать и обновить правила .

Для редактирования правила необходимо нажать кнопку  , находящуюся в колонке **Редактировать**.

В открывшемся окне можно включить/отключить набор правил.

Правила фильтрации

Вкладка **«Правила фильтрации»** содержит таблицу правил фильтрации, представленную на рисунке.

Строка **Фильтр** позволяет установить наборы необходимых критериев для отбора правил.

С помощью фильтров можно ограничить или расширить данные таблицы.

Для вступления проведенных настроек в силу необходимо нажать кнопку Сохранить .

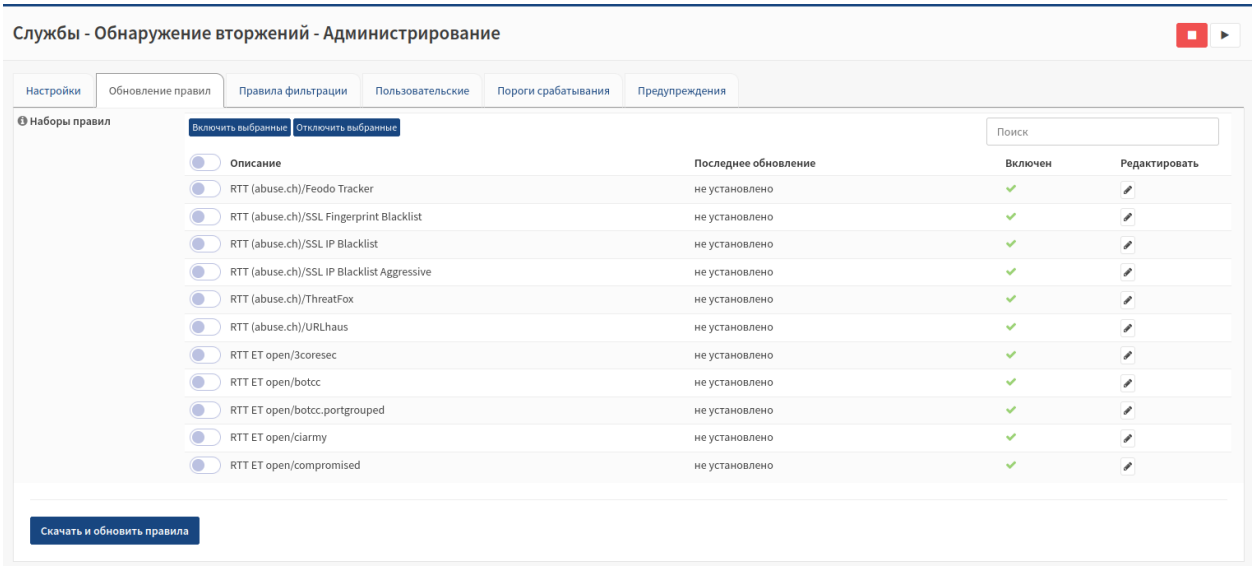


Рис. 741: Таблица наборов правил

Рис. 742: Редактирование наборов правил

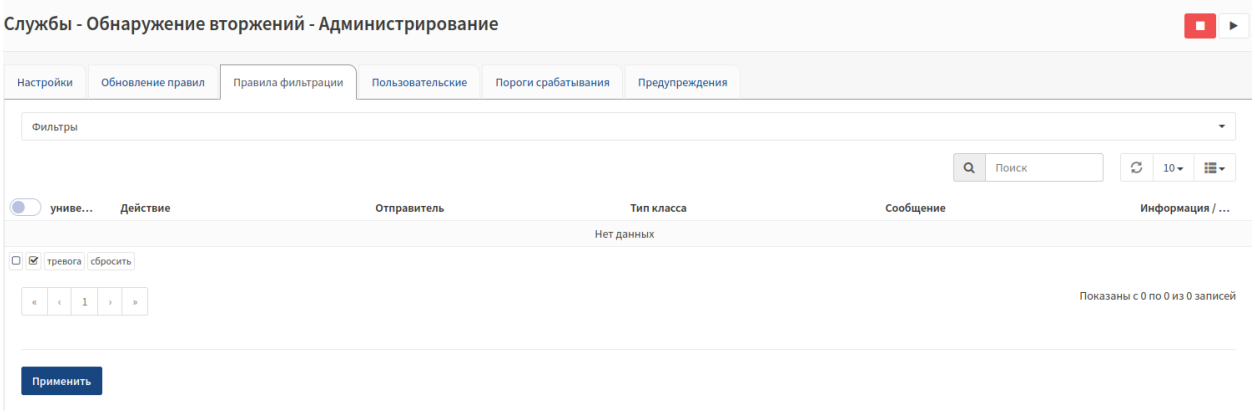


Рис. 743: Таблица правил фильтрации

Рис. 744: Фильтры таблицы

Пользовательские

Вкладка **«Пользовательские»** содержит таблицу правил пользователя, представленную на рисунке.

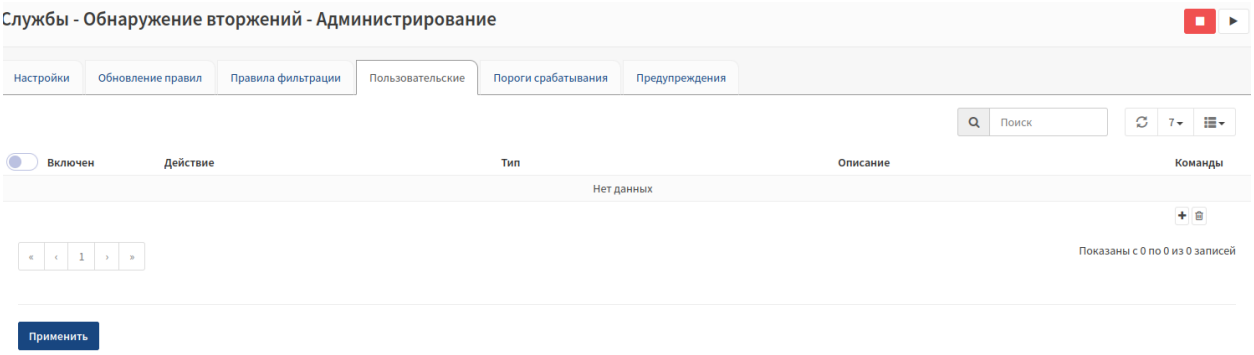


Рис. 745: Таблица правил пользователя

С помощью фильтров можно ограничить или расширить данные таблицы.

Рис. 746: Фильтры таблицы

Для добавления нового правила в таблицу необходимо нажать кнопку  .

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости включить правило;

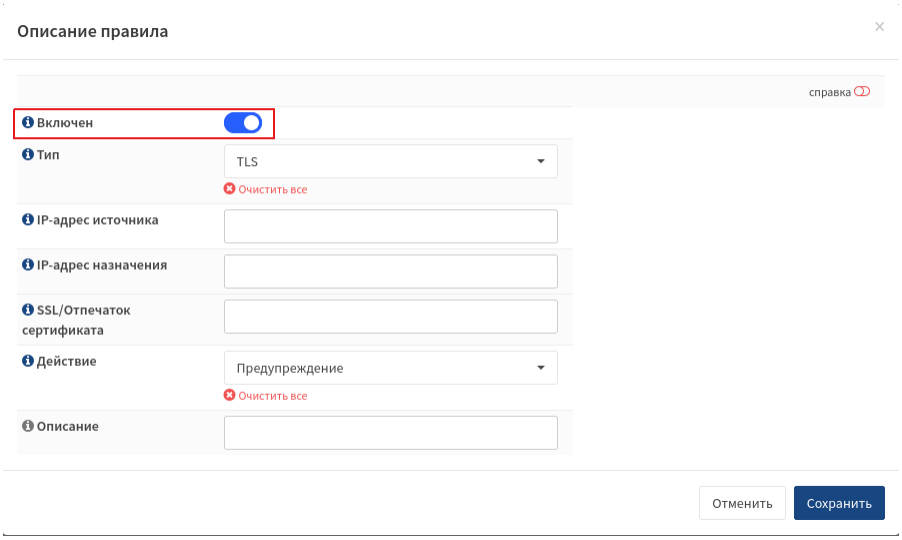


Рис. 747: Включение правила

- в поле **«Тип»** выбрать из выпадающего списка тип правила;

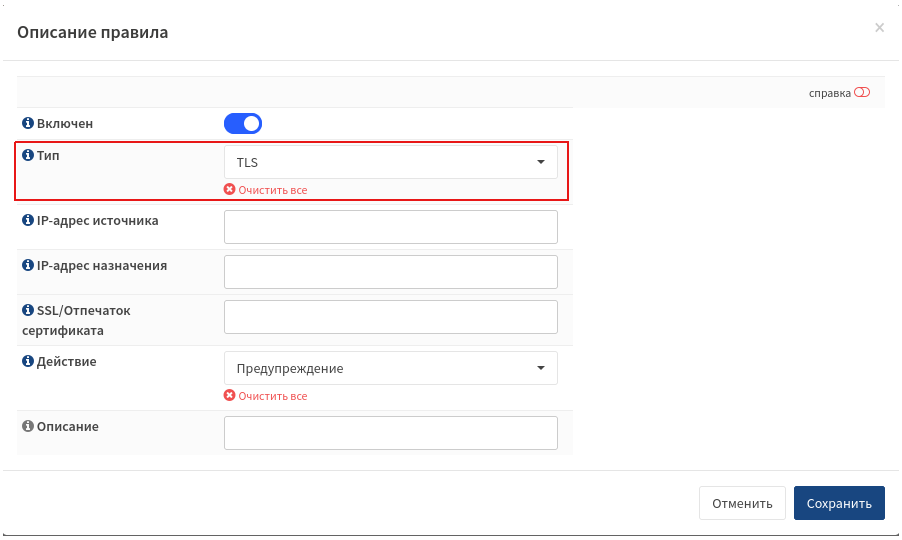


Рис. 748: Выбор типа правила

Совет

TLS - для обработки подписей сертификатов. Пользовательские - для ввода правила целиком

- в поле **«IP-адрес источника»** установить исходный IP-адрес или сеть для соответствия;

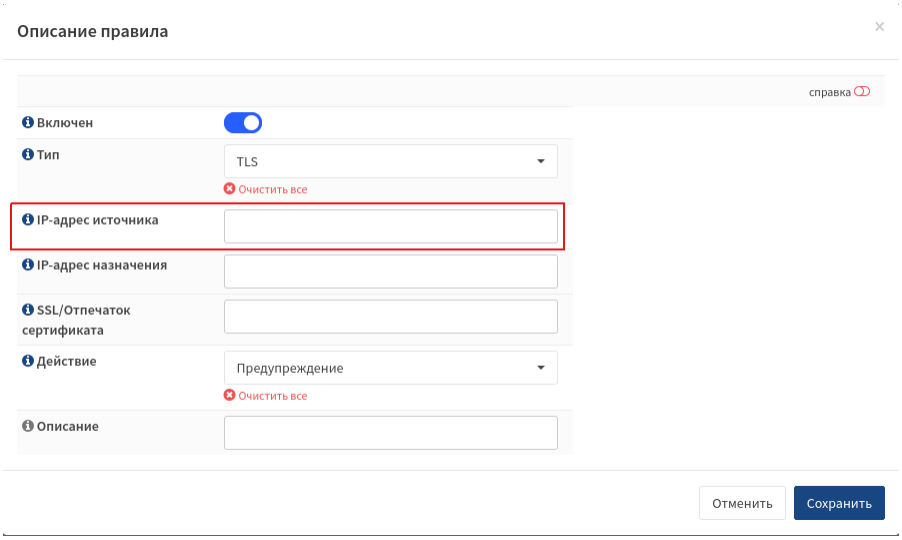


Рис. 749: Установка IP-адреса источника

Совет

Оставьте это поле пустым для использования «любой»

- в поле **«IP-адрес назначения»** установить целевой IP-адрес или сеть для соответствия;

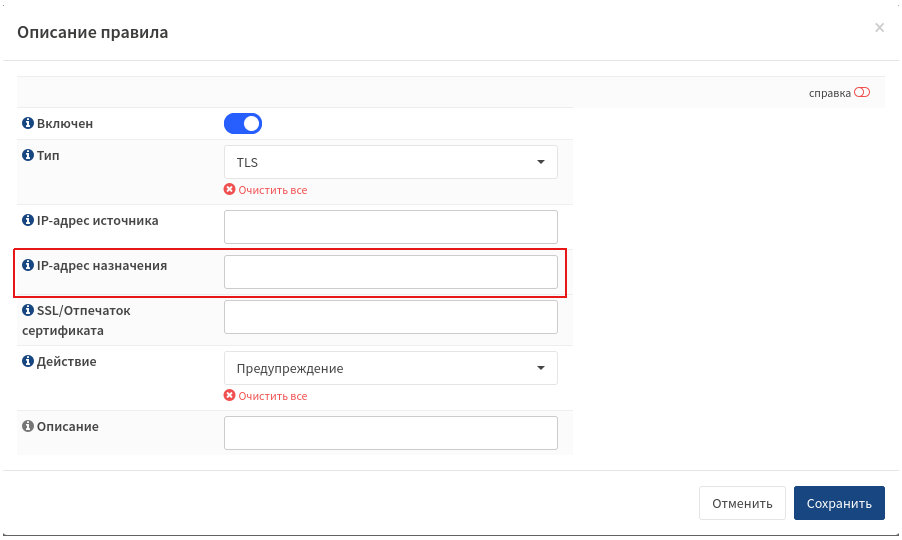


Рис. 750: Установка IP-адреса назначения

Совет

Оставьте это поле пустым для использования «любой»

- в поле **«SSL/Отпечаток сертификата»** установить отпечаток SSL-сертификата;

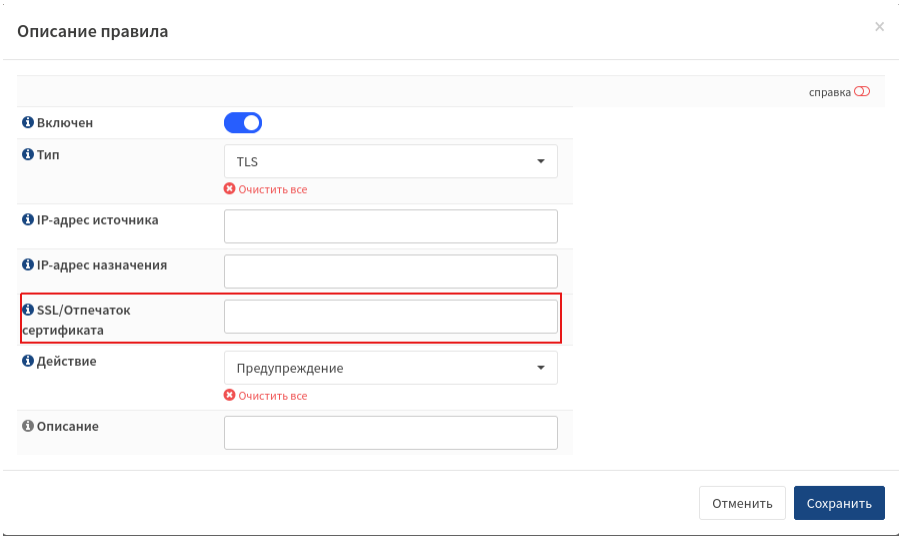


Рис. 751: Установка отпечатка SSL-сертификата

Совет

Например, «B5:E1:B3:70:5E:7C:FF:EB:92:C4:29:E5:5B:AC:2F:AE:70:17:E9:9E»

- в поле **«Действие»** выбрать из выпадающего списка подлежащее выполнению действие, когда включена система предотвращения вторжений (IPS);

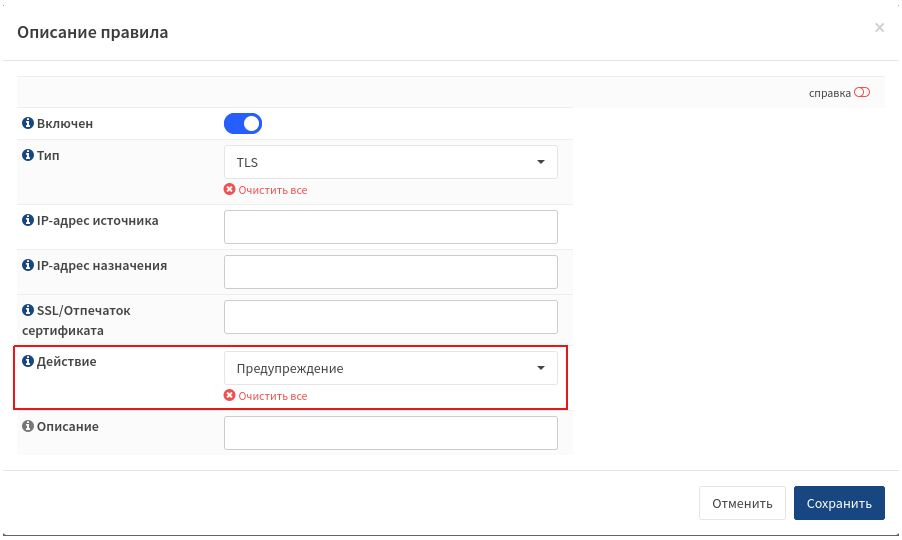


Рис. 752: Выбор действия

- в поле **«Описание»** ввести описание к правилу;

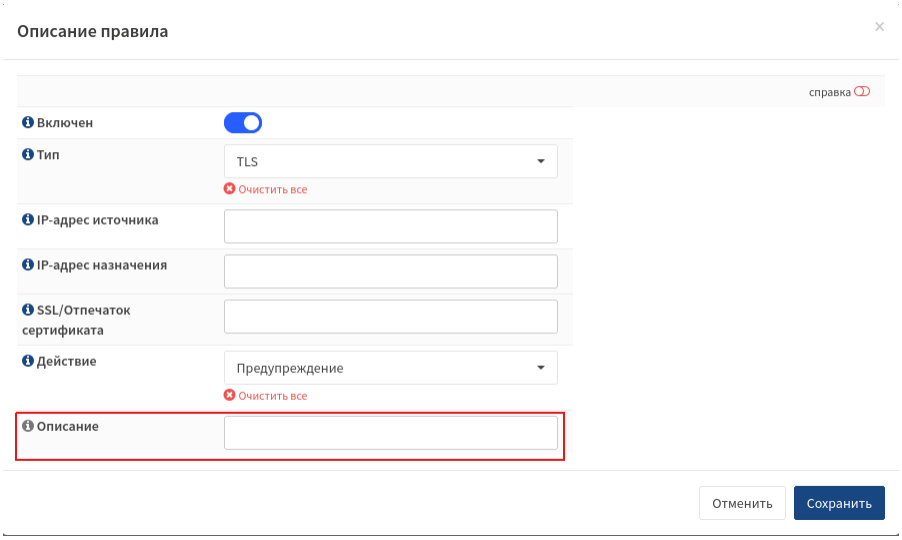


Рис. 753: Ввод описания

Нажать кнопку 

чтобы проведенные настройки вступили в силу.

Пороги срабатывания

Вкладка **«Пороги срабатывания»** содержит таблицу правил, представленную на рисунке.

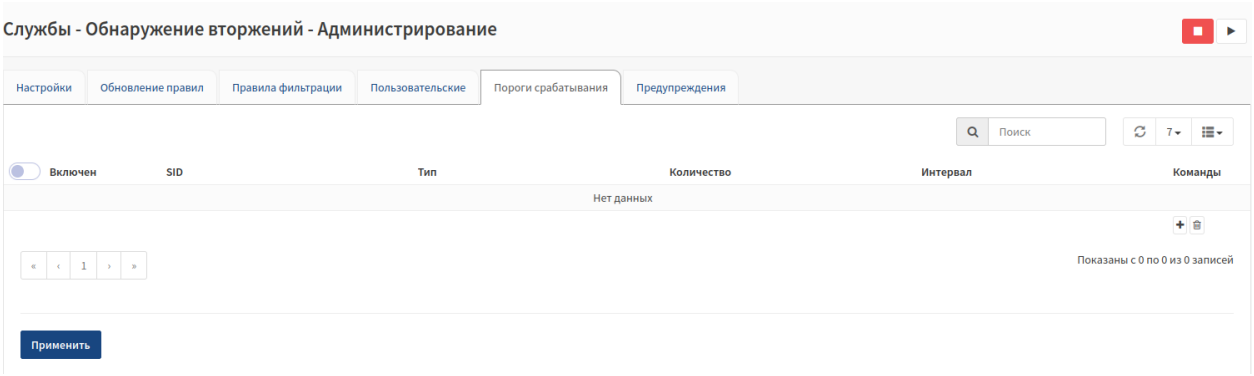


Рис. 754: Таблица правил

С помощью фильтров можно ограничить или расширить данные таблицы.

Рис. 755: Фильтры таблицы

Для добавления нового правила в таблицу необходимо нажать кнопку  .

В открывшемся окне необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости включить правило порога срабатывания;

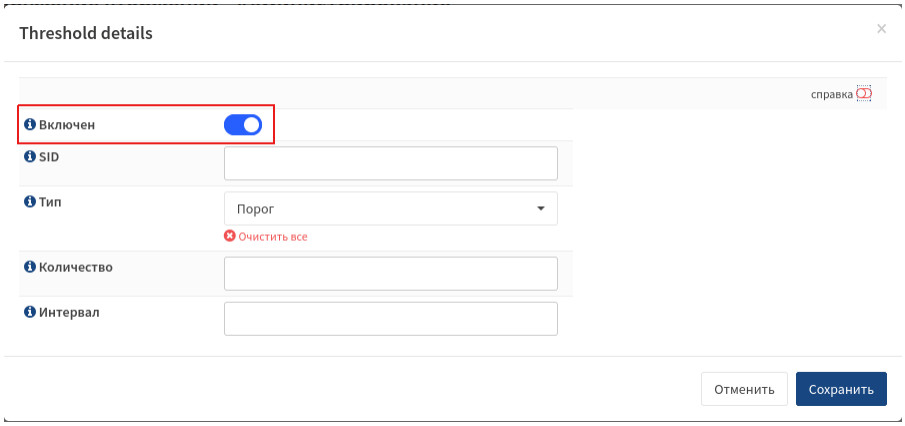


Рис. 756: Включение правила

- в поле **«SID»** ввести ID сигнатуры, для которого действует порог срабатывания;
- в поле **«Тип»** выбрать из выпадающего списка тип правила;
- в поле **«Количество»** ввести числовое значение для того, чтобы предупреждение появится после N-ого предупреждения (эта опция) и определенного интервала времени;

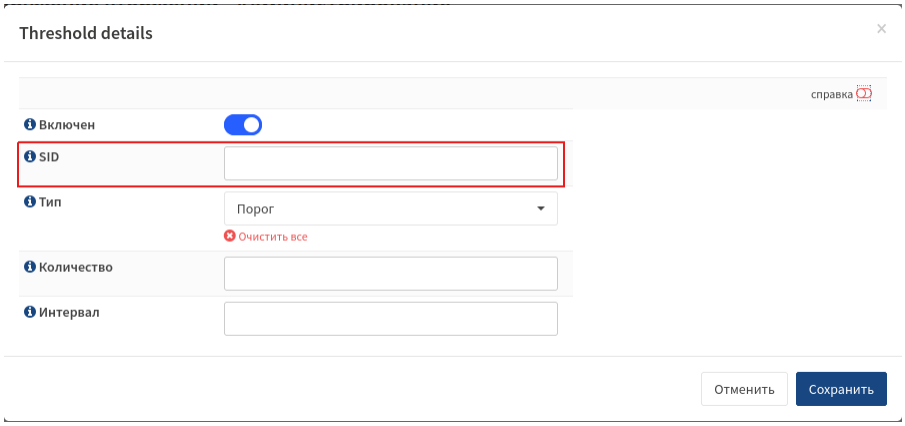


Рис. 757: Ввод ID сигнатуры

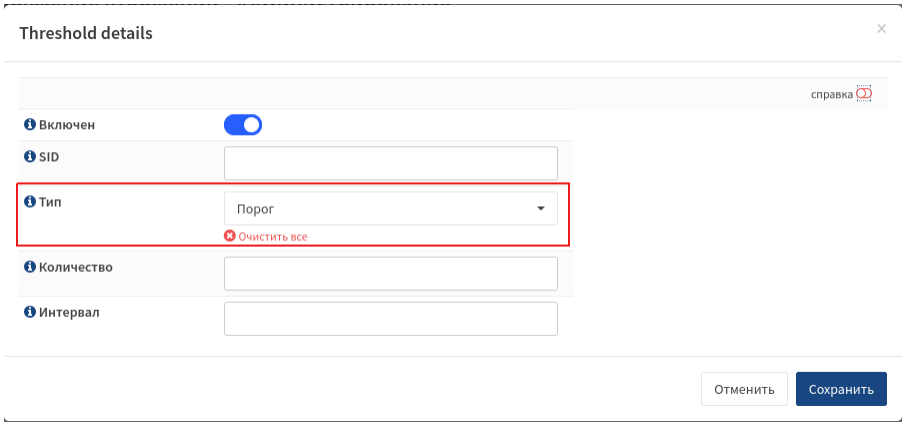


Рис. 758: Выбор правила

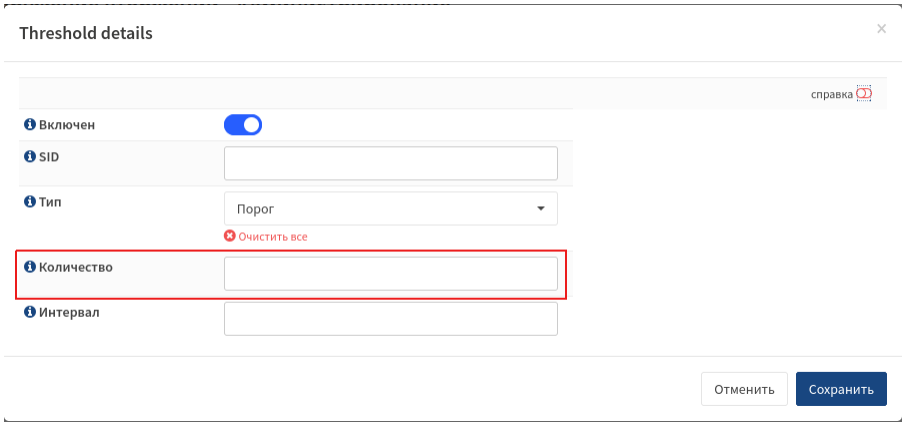


Рис. 759: Ввод количества

- в поле **«Интервал»** ввести числовое значение интервала времени для того, чтобы предупреждение появится после N-ого предупреждения (эта опция);

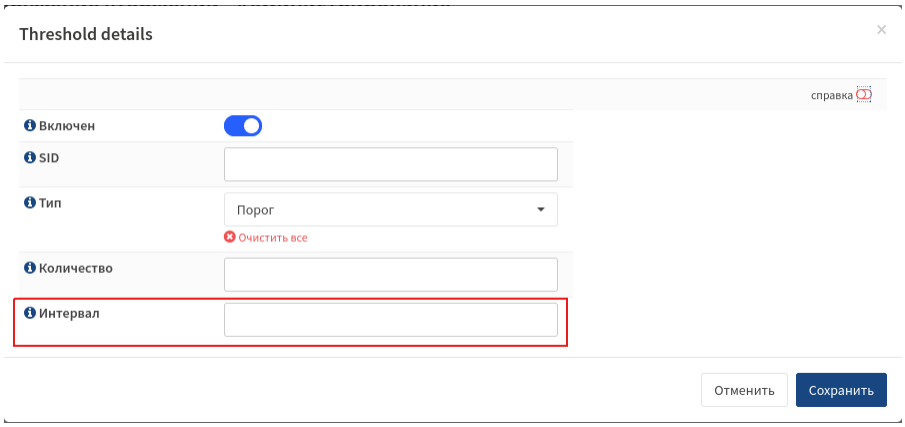


Рис. 760: Ввод интервала времени

Нажать кнопку 

чтобы проведенные настройки вступили в силу.

Предупреждения

Вкладка **«Предупреждения»** содержит таблицу предупреждений, представленную на рисунке.

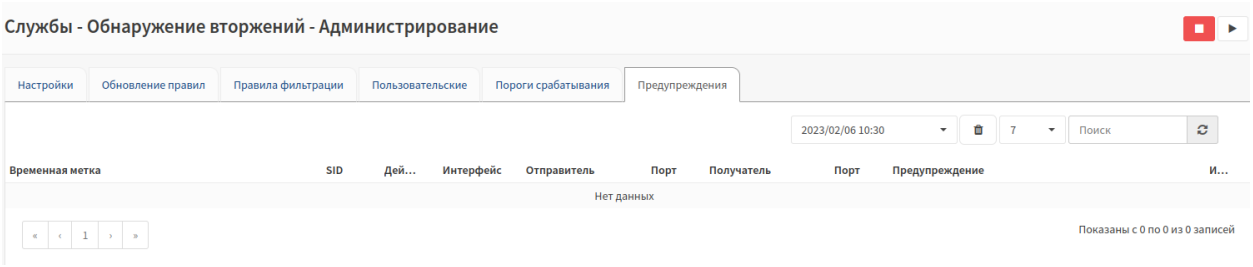


Рис. 761: Таблица предупреждений

С помощью фильтров можно ограничить или расширить данные таблицы.

Рис. 762: Фильтры таблицы

Статистические данные

В данном разделе представлены вкладки со статистическими данными системы обнаружения вторжений

Рис. 763: Статистические данные системы обнаружения вторжений

Журнал

Раздел **«Журнал»** содержит журнал системы обнаружения вторжений.

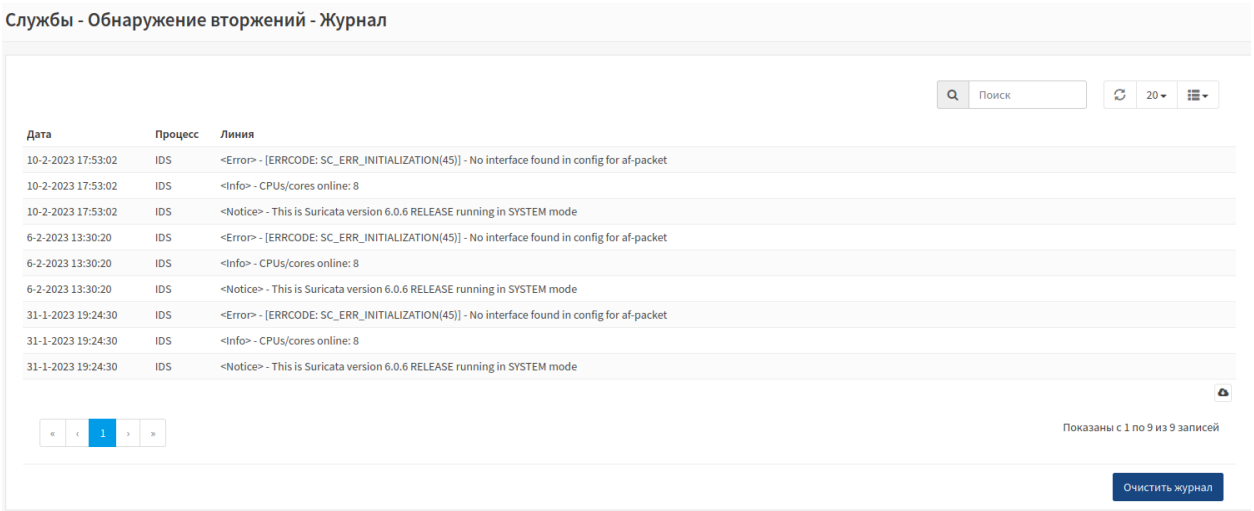


Рис. 764: Журнал системы обнаружения вторжений

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

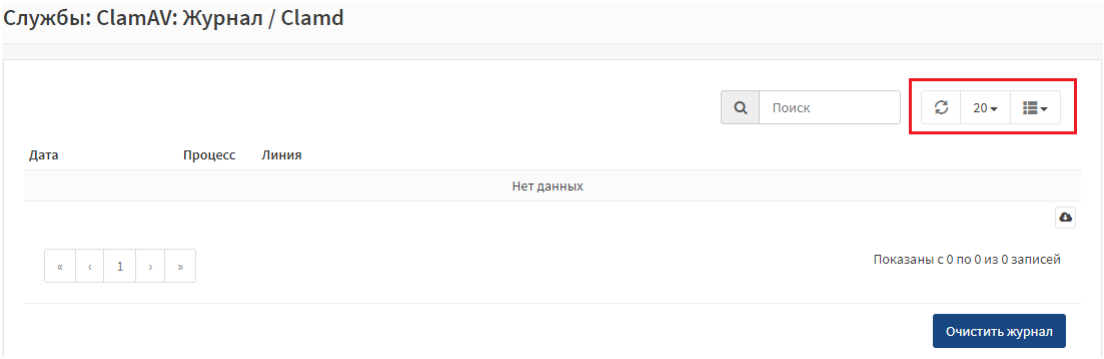


Рис. 765: Фильтры журнала

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

2.7.8.3 Мониторинг служб

Для перехода к настройкам системы мониторинга серверов необходимо:

- нажать на вкладку **«Службы»** - **«Мониторинг служб»** - **«Настройки»**, расположенную в левой части списка объектов управления;

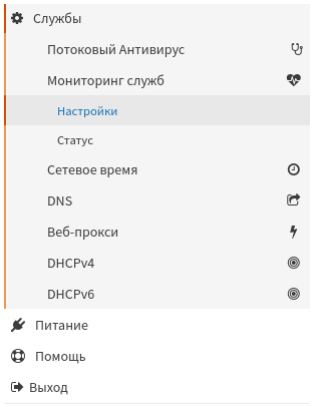


Рис. 766: Переход к настройкам мониторинга служб

Для перехода к просмотру мониторинга служб необходимо:

- нажать на вкладку **«Службы»** - **«Мониторинг служб»** - **«Статус»**, расположенную в левой части списка объектов управления;

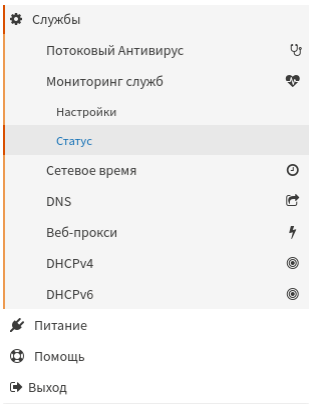


Рис. 767: Переход к просмотру мониторинга служб

Настройки

Основные настройки

Для выполнения основных настроек необходимо:

- в поле **«Адрес почтового сервера»** указать разделенный запятыми список SMTP-серверов для доставки предупреждений;

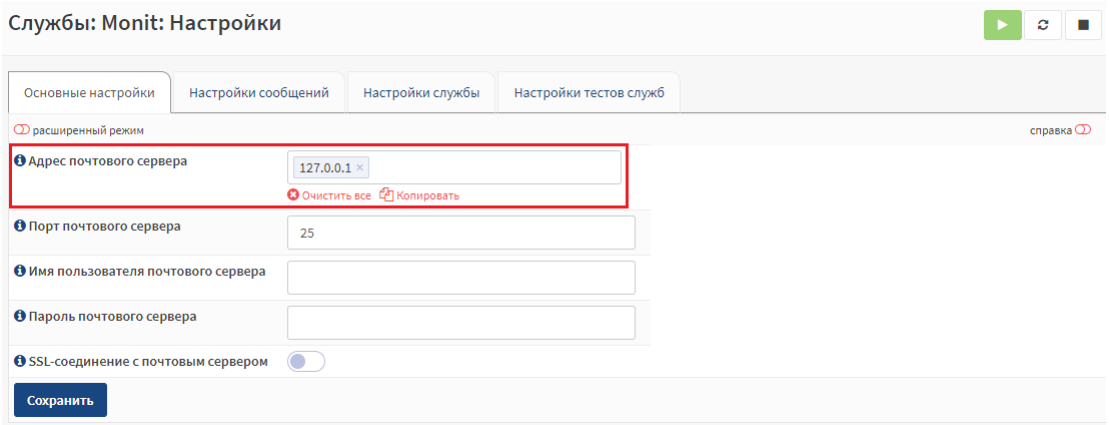


Рис. 768: Адрес почтового сервера

- в поле **«Порт почтового сервера»** указать числовое значение порта почтового сервера;

> **Совет**
>
> Как правило 465 для SSL или 25 для TLS и не безопасных соединений

- в поле **«Имя пользователя почтового сервера»** указать имя пользователя для аутентификации почтового сервера;
- в поле **«Пароль почтового сервера»** указать пароль почтового сервера;
- в поле **«SSL-соединение с почтовым сервером»** установить переключатель в случае необходимости включения шифрования для связи с почтовым сервером;

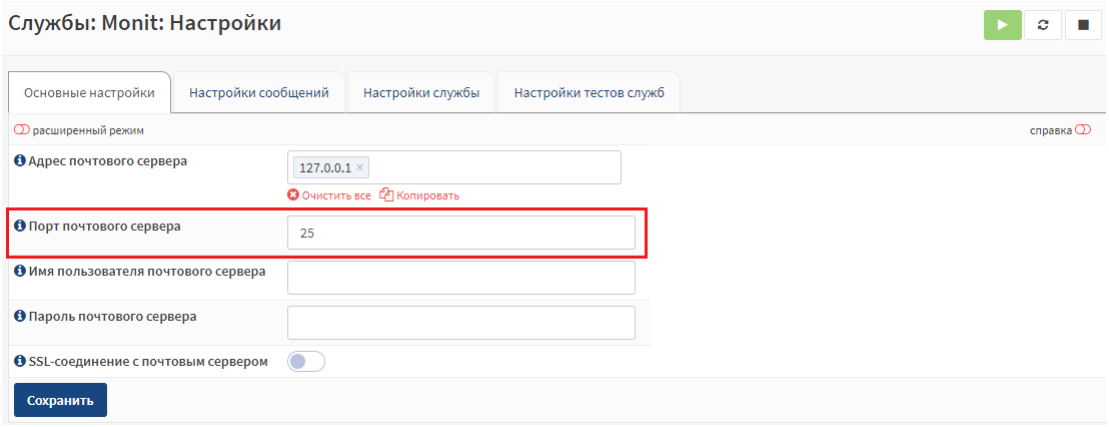


Рис. 769: Порт почтового сервера

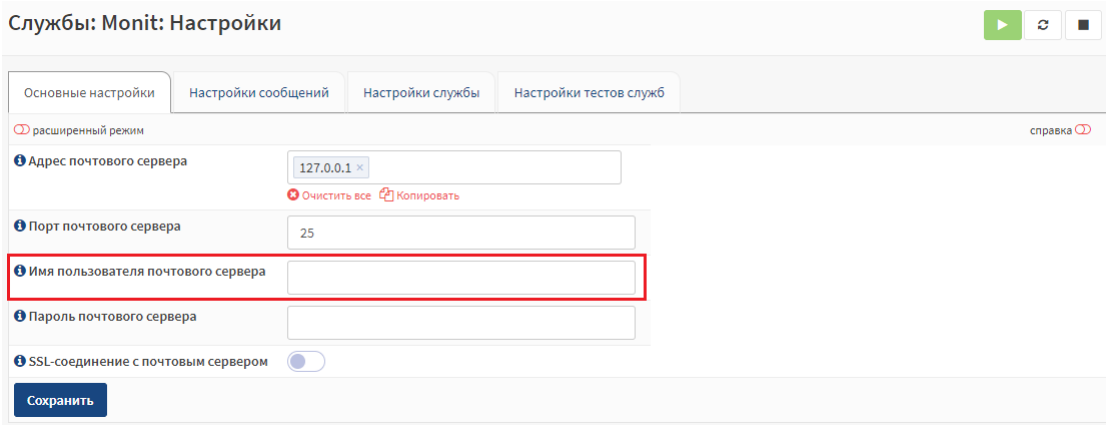


Рис. 770: Имя пользователя почтового сервера

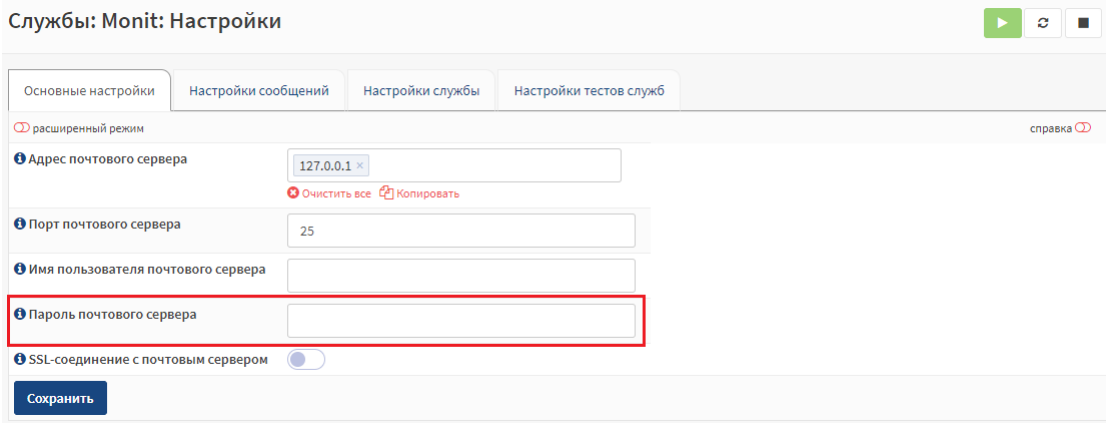


Рис. 771: Пароль почтового сервера

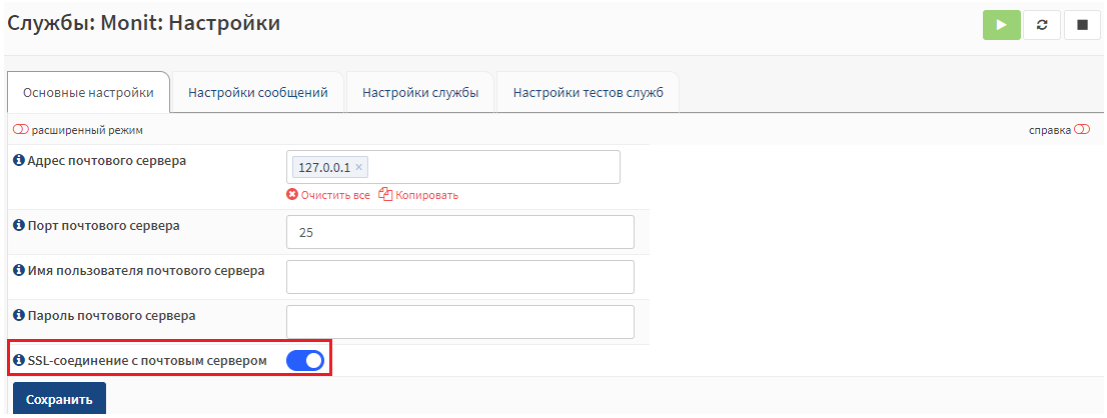


Рис. 772: SSL-соединение с почтовым сервером

- нажать кнопку **«Сохранить»** 

.

Для включения режима расширенных настроек необходимо установить переключатель.

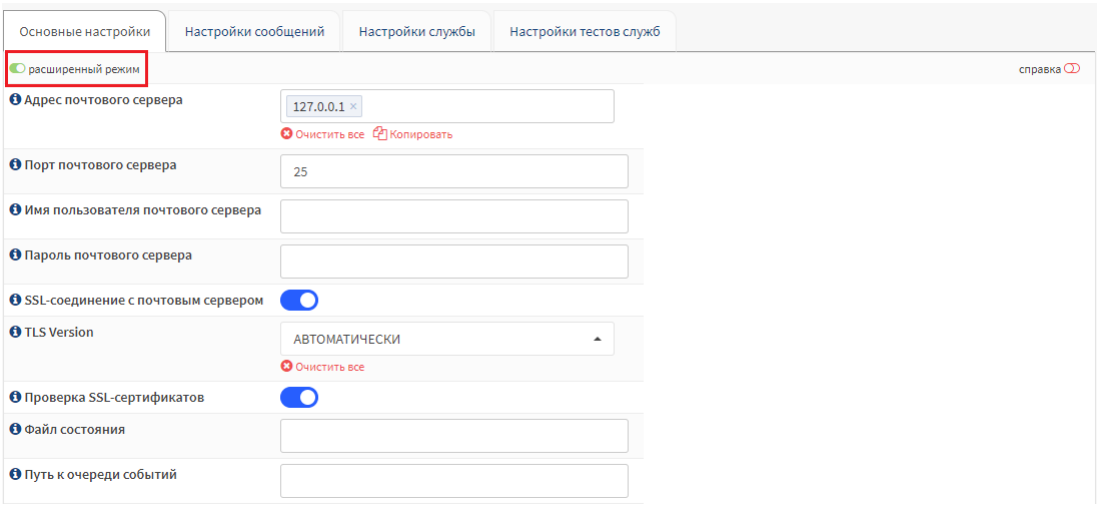


Рис. 773: Включение расширенных настроек

В режиме расширенных настроек необходимо:

- в поле **«TLS Version»** (при включенной функции **«SSL-соединение с почтовым сервером»**) выбрать из выпадающего списка необходимую версию SSL, соответствующую таблице;

Таблица 155: Версии TLS

Версия TLS
AUTO
TLSV1
TLSV11
TLSV12
TLSV13

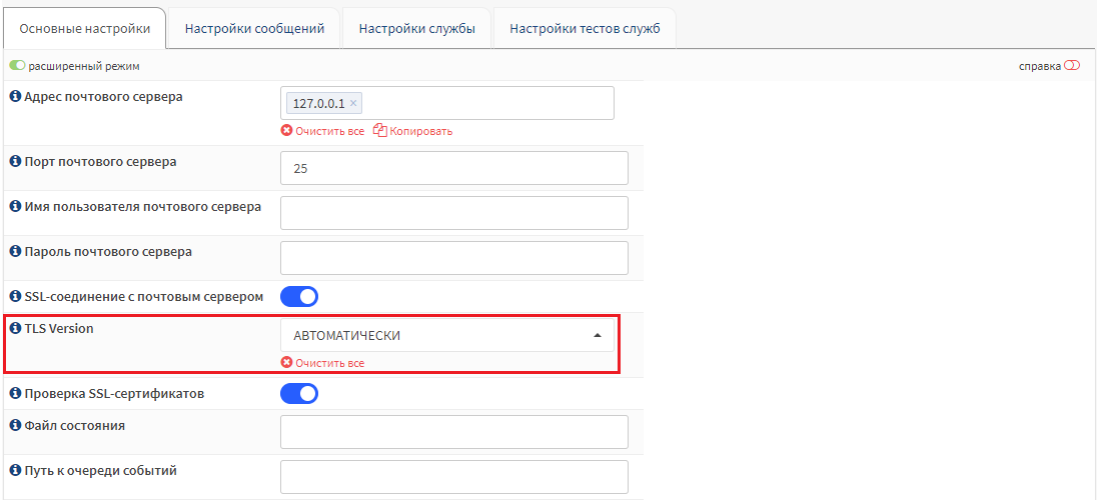


Рис. 774: TLS Version

Примечание

В режиме AUTO используется только TLS

- в поле **«Проверка SSL-сертификатов»** установить переключатель в случае необходимости проверки SSL-сертификатов;

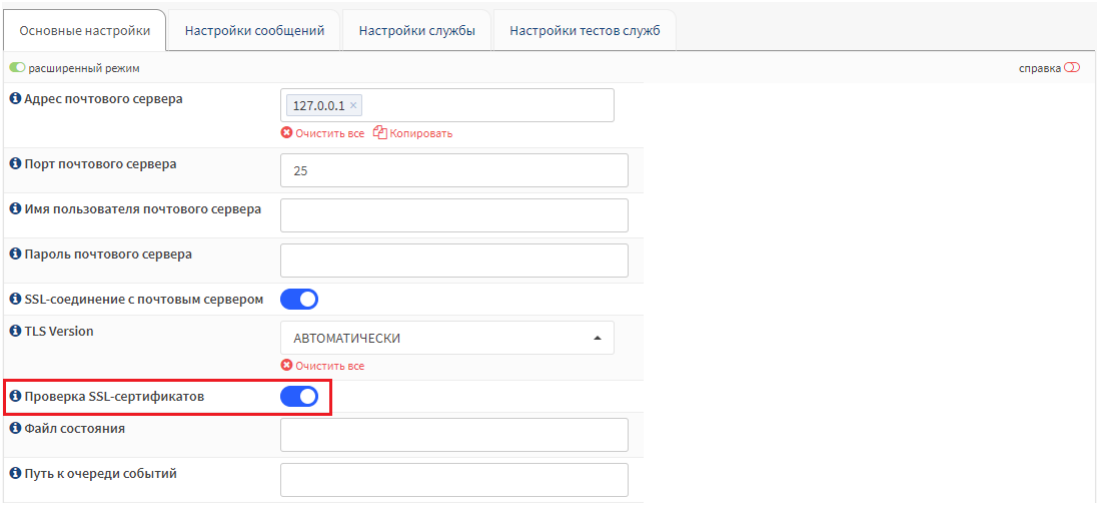


Рис. 775: Проверка SSL-сертификатов

- в поле **«Файл состояния»** указать файл состояния процесса Monit;
- в поле **«Путь к очереди событий»** указать путь к каталогу очереди событий;
- в поле **«Слоты очереди событий»** указать количество слотов очереди событий;
- в поле **«Включить HTTPD»** установить переключатель в случае необходимости запустить службу Monit httpd;
- в поле **«Порт Monit HTTPD»** (при включенной функции **«Включить HTTPD»**) указать порт прослушивания службы Monit httpd;

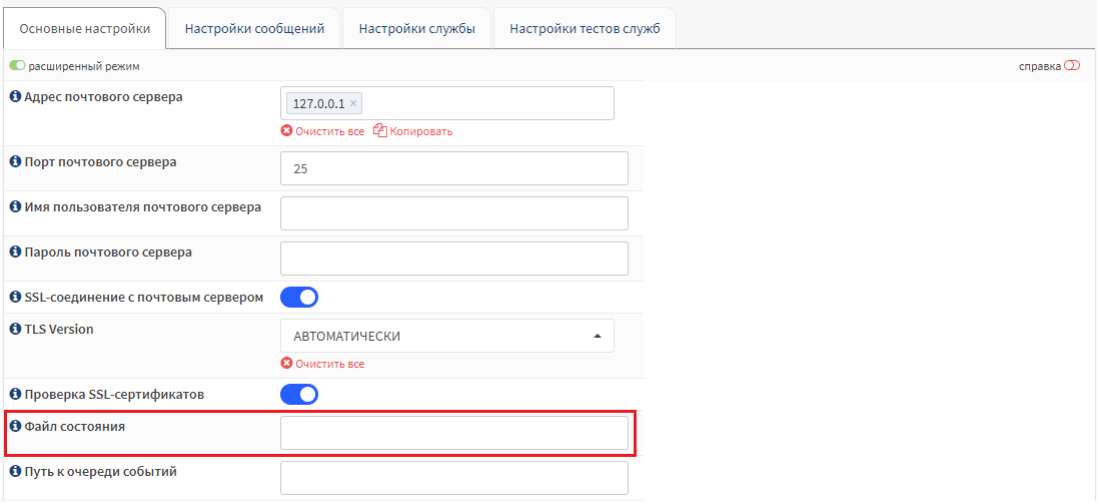


Рис. 776: Файл состояния

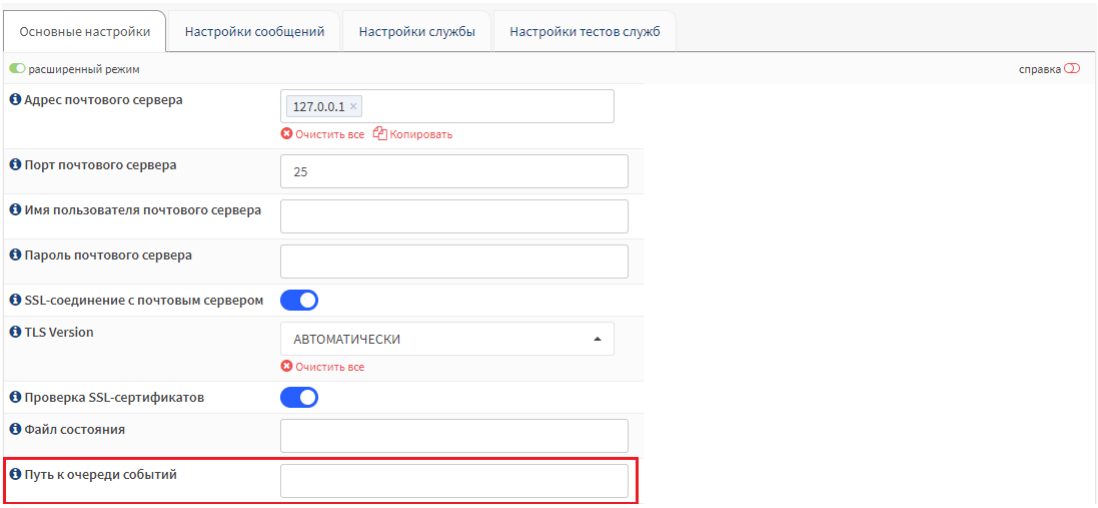


Рис. 777: Путь к очереди событий

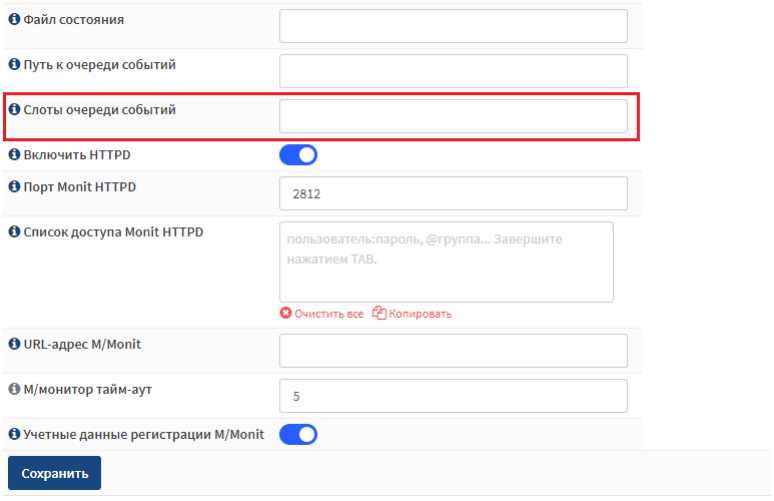


Рис. 778: Слоты очереди событий

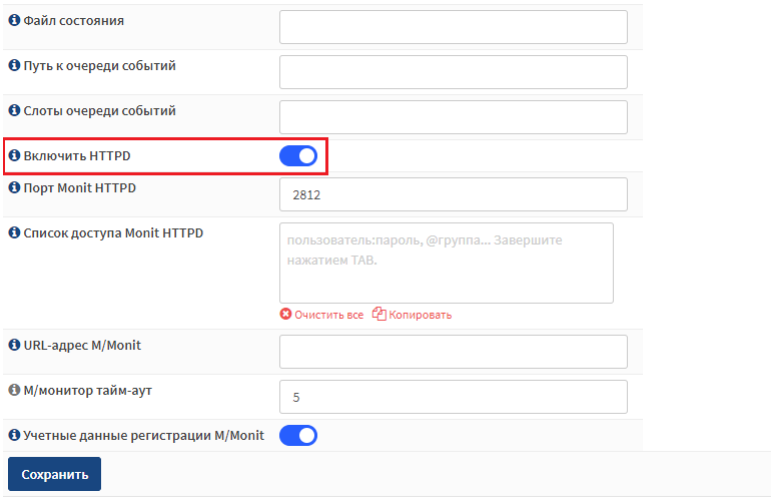


Рис. 779: Включить HTTPD

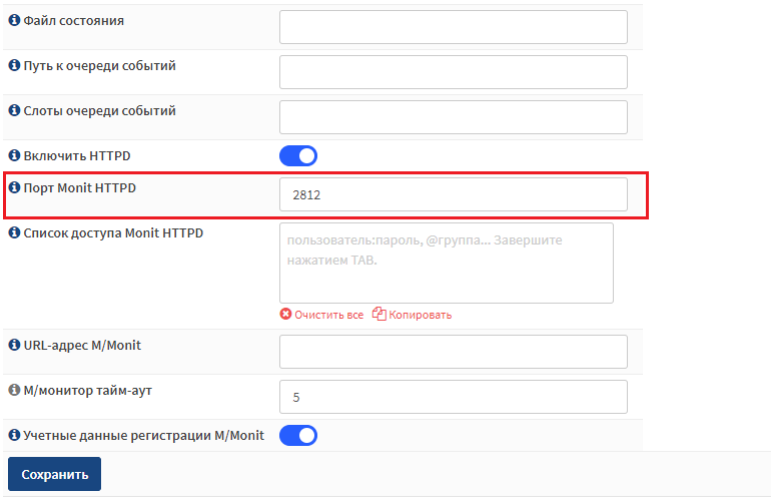


Рис. 780: Порт Monit HTTPD

- в поле **«Список доступа Monit HTTPD»** (при включенной функции **«Включить HTTPD»**) указать имя пользователя: пароль или хост/сеть и т. д. для доступа к службе Monit httpd;

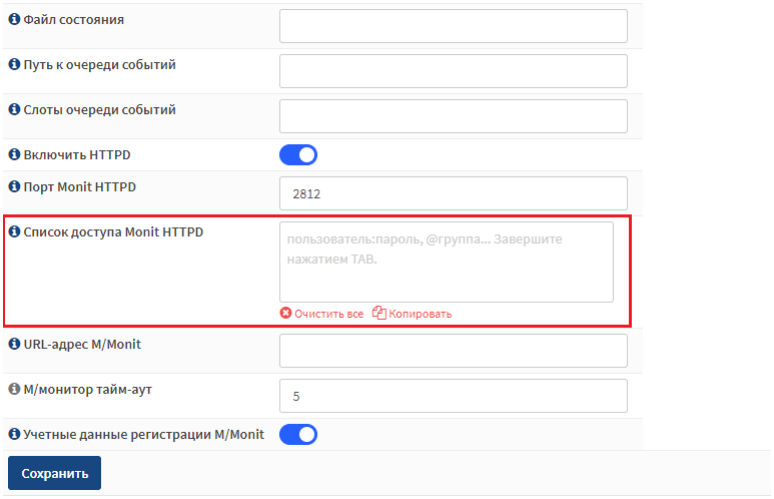


Рис. 781: Список доступа Monit HTTPD

- в поле **«URL-адрес M/Monit»** (при включенной функции **«Включить HTTPD»**) указать URL-адрес M/Monit;

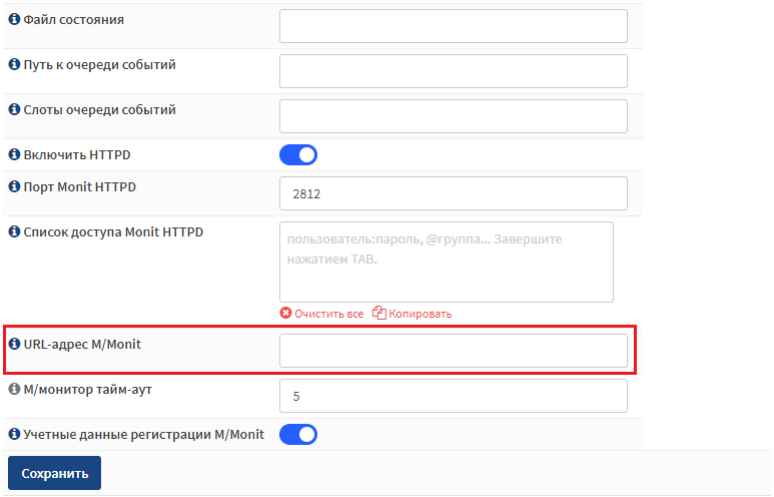


Рис. 782: URL-адрес M/Monit

Примечание

URL-адрес M/Monit https://user:pass@192.168.1.10:8443/collector

Примечание

Если вы хотите управлять службами Monit из своего экземпляра M/Monit, вам также необходимо настроить порт Monit и добавить соответствующие правила брандмауэра

- в поле **«M/монитор тайм-аут»** (при включенной функции **«Включить HTTPD»**) указать тайм-аут M/Monit;

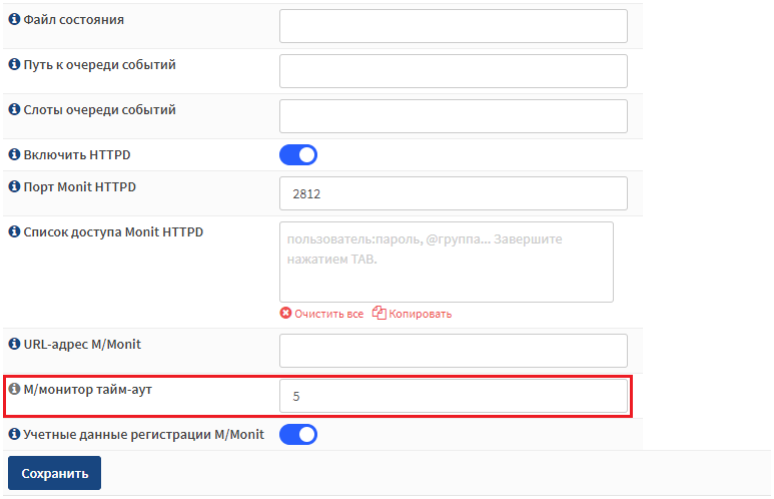


Рис. 783: M/монитор тайм-аут

- в поле **«Учетные данные регистрации M/Monit»** (при включенной функции **«Включить HTTPD»**) установить переключатель в случае необходимости автоматически зарегистрироваться в M/Monit, отправив учетные данные Monit;

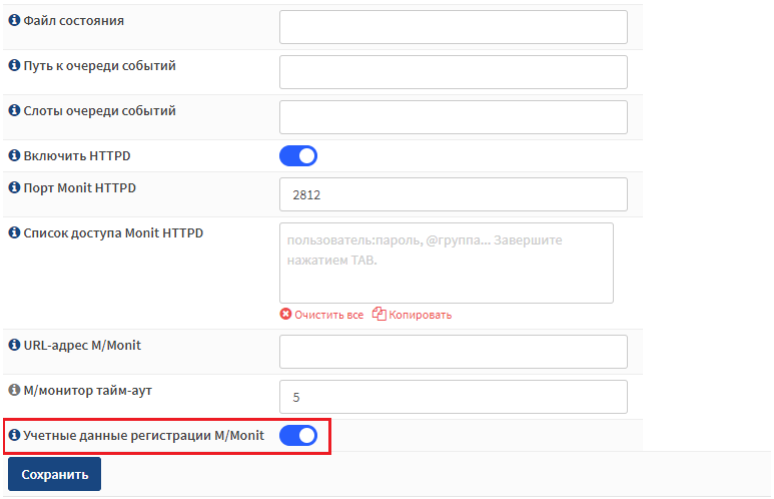


Рис. 784: Учетные данные регистрации M/Monit

- нажать кнопку **«Сохранить»** 

.

Настройки сообщений

Для настройки сообщений необходимо нажать кнопку «+»

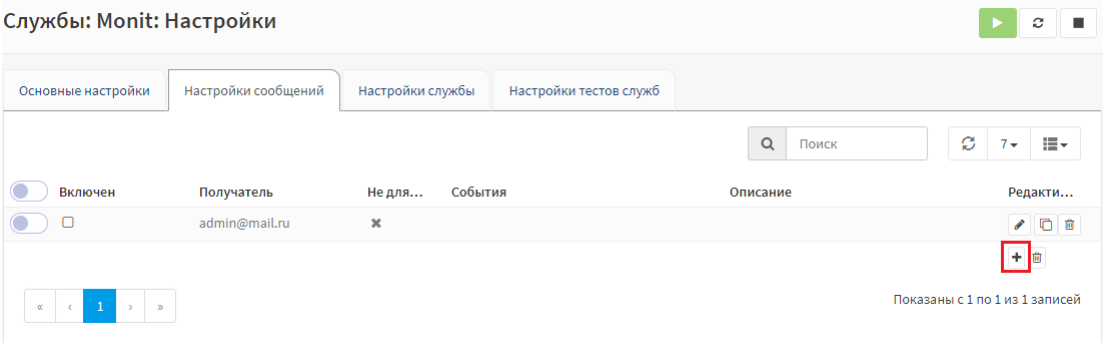


Рис. 785: Настройка нового сообщения

В открывшемся окне необходимо:

- в поле **«Включить сообщения»** установить переключатель в случае необходимости включить оповещение;

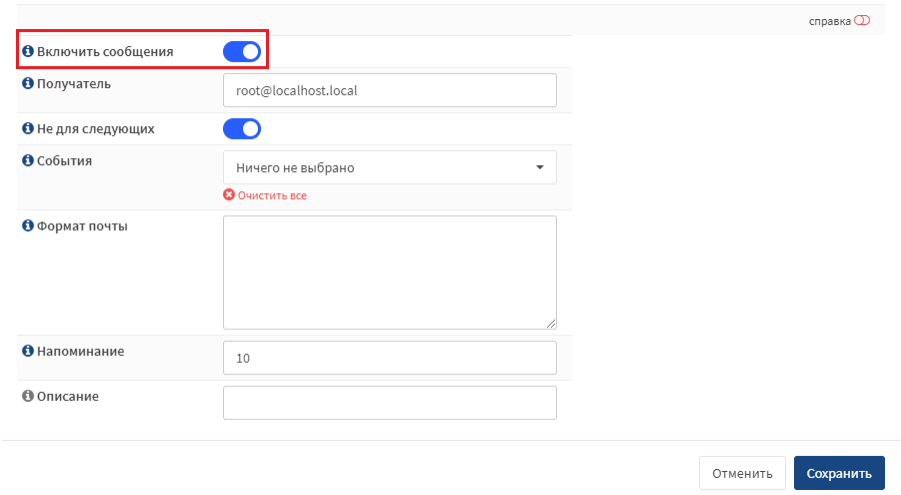


Рис. 786: Включить сообщения

- в поле **«Получатель»** указать E-mail адрес для отправки оповещений;
- в поле **«Не для следующих»** установить переключатель в случае необходимости не посылать сообщения для следующих событий, но не для остальных;
- в поле **«События»** выбрать из выпадающего списка необходимое событие, соответствующее таблице;

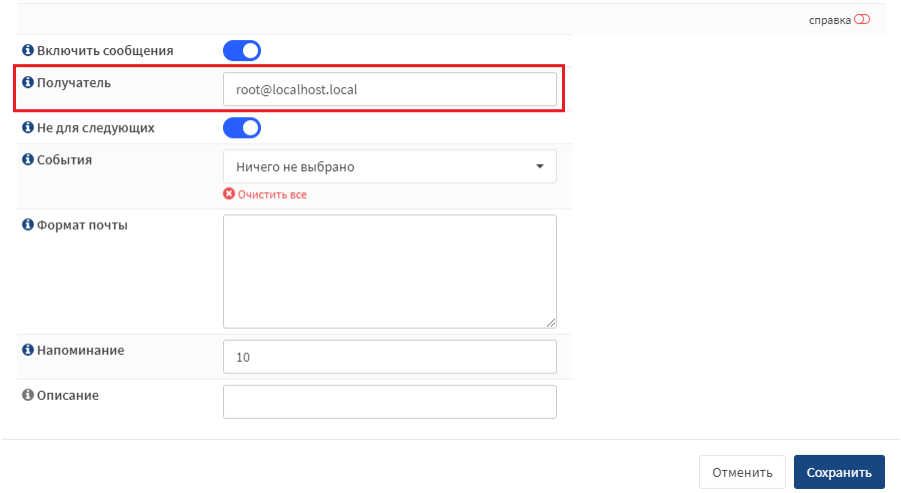


Рис. 787: Получатель

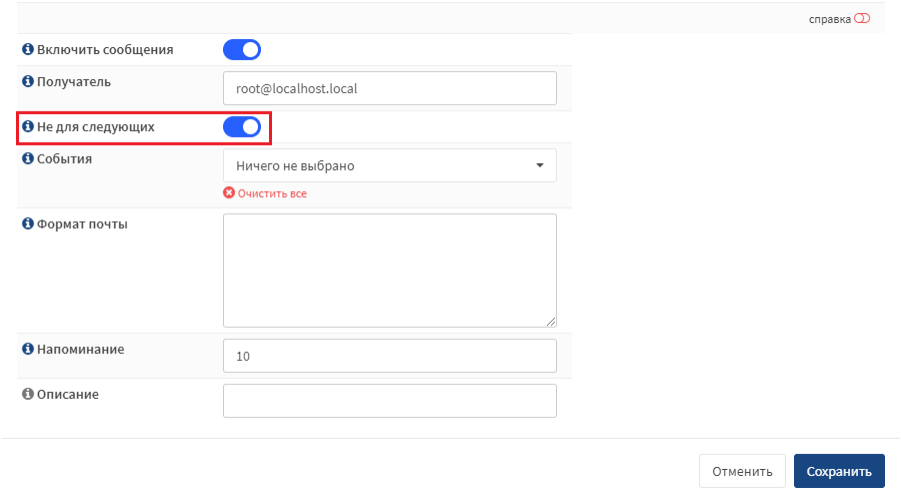


Рис. 788: Не для следующих

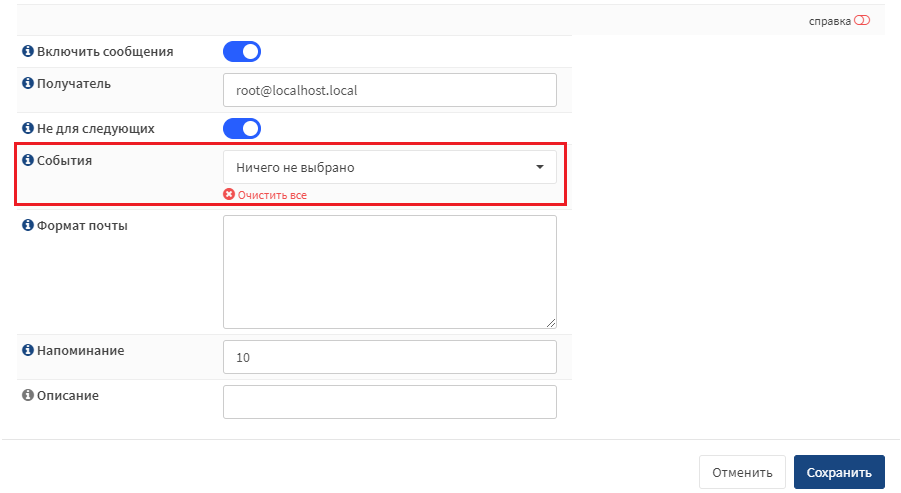


Рис. 789: События

Таблица 156: Список событий

Событие	Примечание
Action done	Действие выполнено
Checksum failed	Ошибка контрольной суммы
Download bytes exceeded	Загрузка байтов превышена
Connection failed	Ошибка подключения
Content failed	Не удалось выполнить контент
Data access error	Ошибка доступа к данным
Execution failed	Выполнение не выполнено
Filesystem flags failed	Не удалось установить флаги файловой системы
GID failed	Ошибка GID
Ping failed	Ошибка соединения
Monit instance changed	Экземпляр Monit изменен
Invalid type	Недопустимый тип
Does not exist	Не существует
Download packets exceeded	Пакеты загрузки превышены
Upload packets exceeded	Превышено количество загружаемых пакетов
Permission failed	Ошибка доступа
PID failed	Ошибка PID
PPID failed	Ошибка PPID
Resource limit matched	Лимит ресурсов соответствует
Saturation exceeded	Насыщенность превышена
Size failed	Ошибка размера
Speed failed	Ошибка скорости
Status failed	Статус не выполнен
Timeout	Тайм-аут
Timestamp failed	Отметка времени не удалась
UID failed	UID не удалось

Совет

Оставьте пустым для всех событий

- в поле **«Формат почты»** указать формат электронной почты для оповещений;

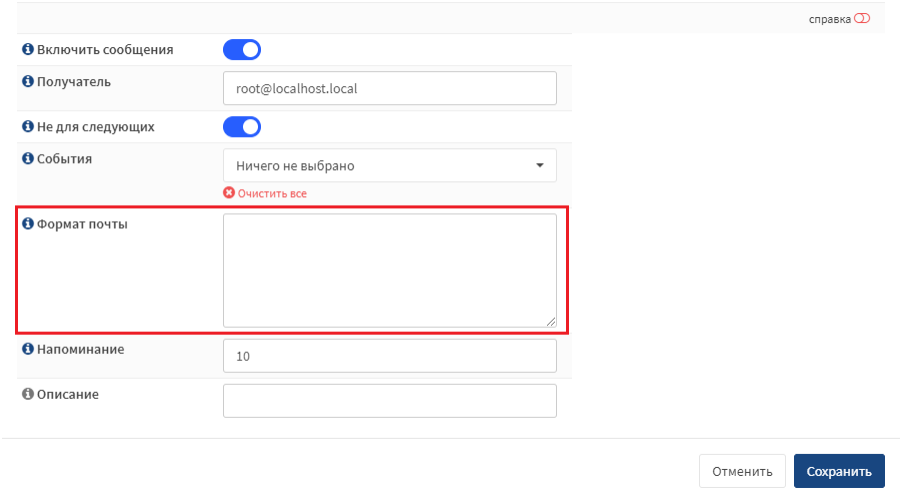


Рис. 790: Формат почты

- в поле **«Напоминание»** указать количество циклов, через которые будет осуществляться напоминание;

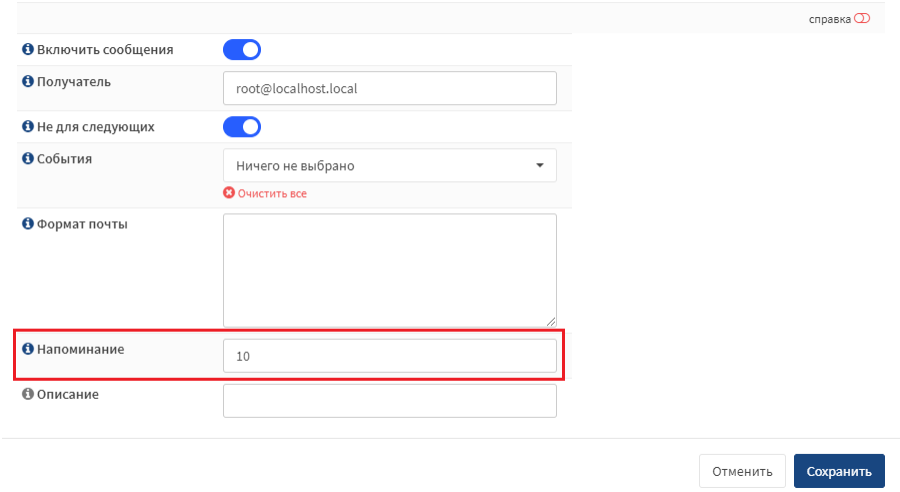


Рис. 791: Напоминание

- в поле **«Описание»** ввести описание;
- нажать кнопку **«Сохранить»** 

;
- нажать кнопку **«Применить»** 

для вступления сконфигурированного сообщения в силу.

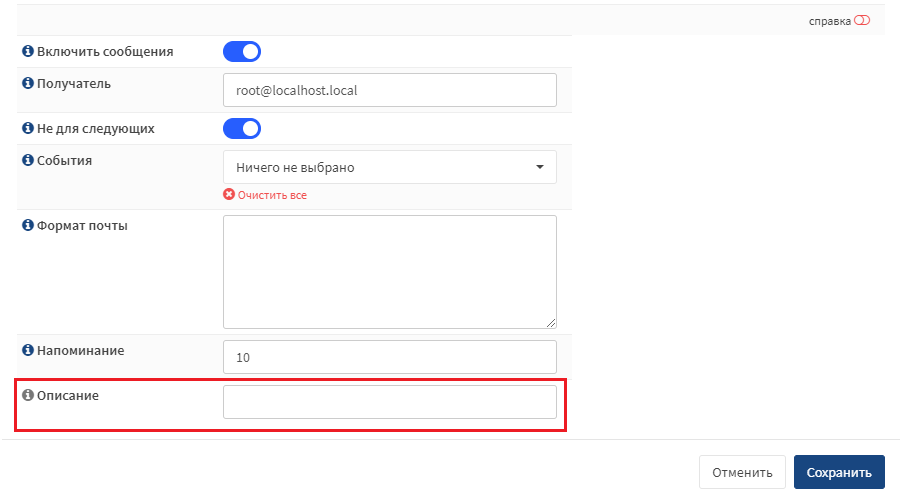


Рис. 792: Описание

Настройки службы

Для настройки службы необходимо нажать кнопку «+»

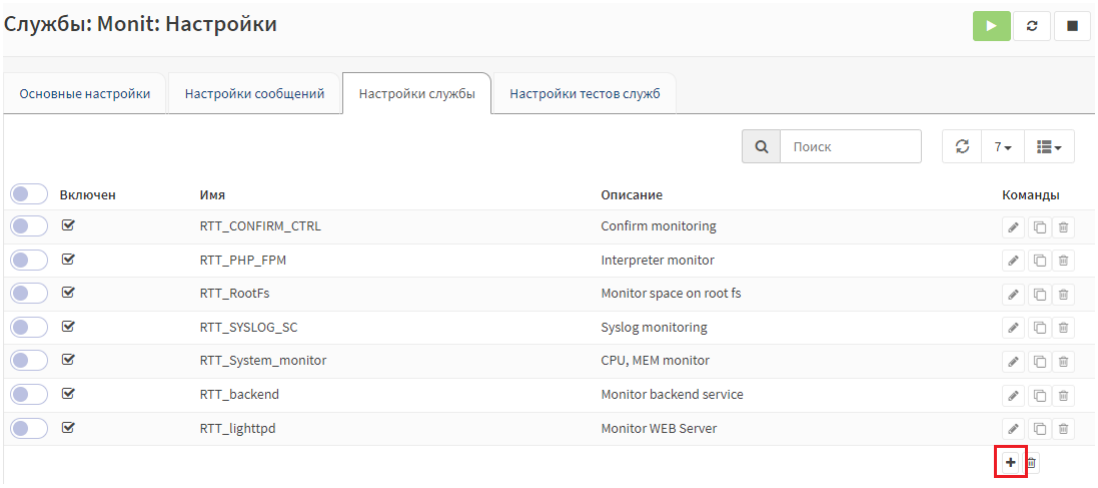


Рис. 793: Настройка службы

Удаленный хост

Для проверки удаленного хоста необходимо:

- в поле **«Тип»** окна **«Edit Service»** выбрать из выпадающего списка тип **«Удаленный хост»**
- в поле **«Включить проверки служб»** установить переключатель в случае необходимости проверки сервисов;
- в поле **«Имя»** ввести имя сервиса;
- в поле **«Адрес»** ввести целевой IP-адрес для проверок удалённого хоста;

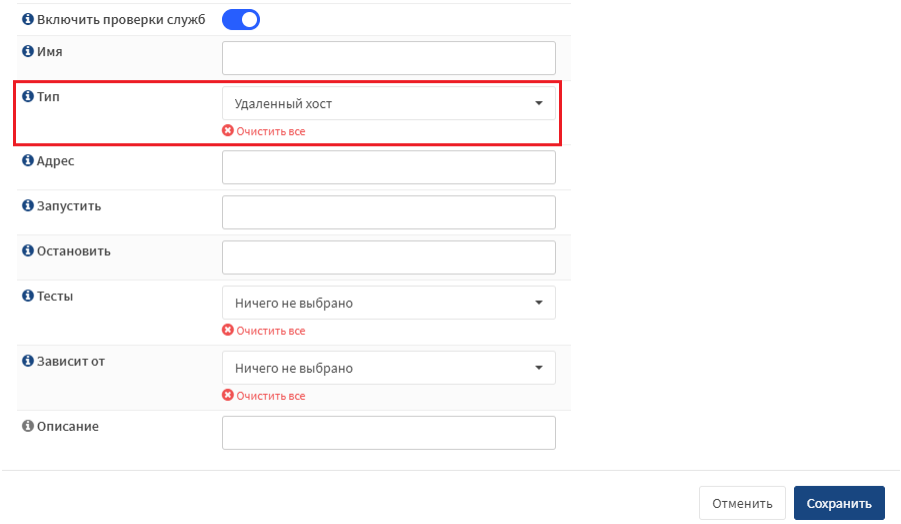


Рис. 794: Выбор удаленного хоста

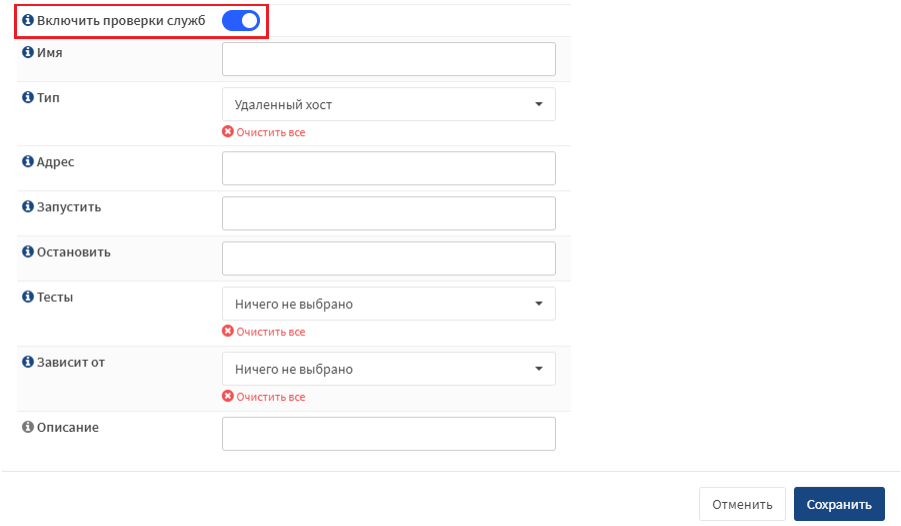


Рис. 795: Включить проверки служб

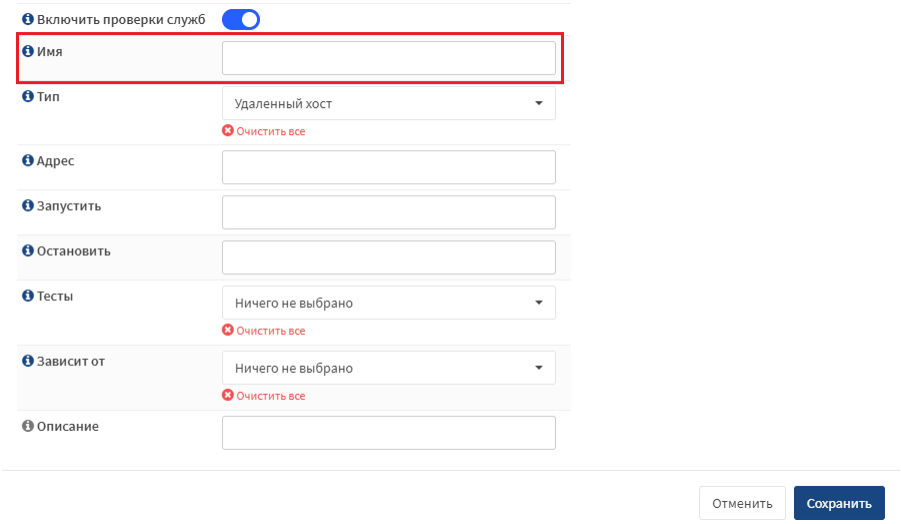


Рис. 796: Имя

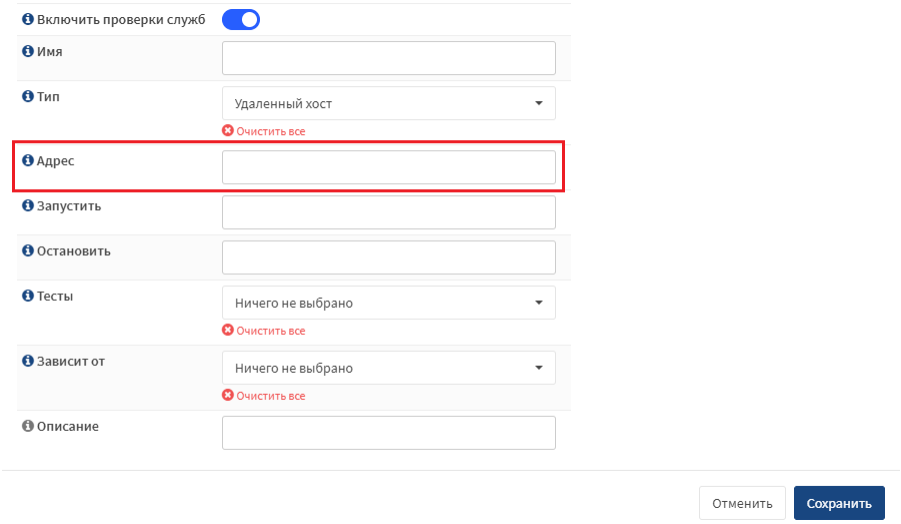


Рис. 797: Адрес

- в поле **«Запустить»** ввести сценарий запуска службы;

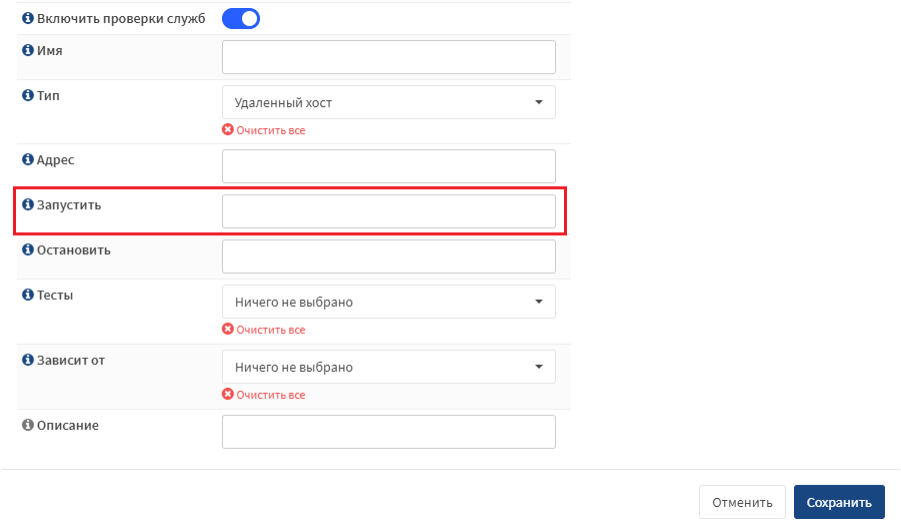


Рис. 798: Запустить

- в поле **«Остановить»** ввести скрипт остановки службы;

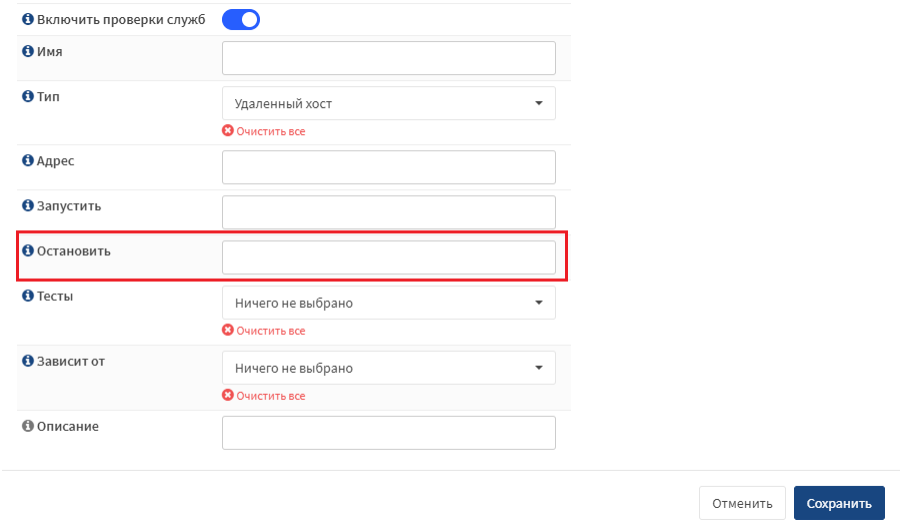


Рис. 799: Остановить

- в поле **«Тесты»** выбрать из выпадающего списка необходимый тест сервиса, соответствующий таблице;

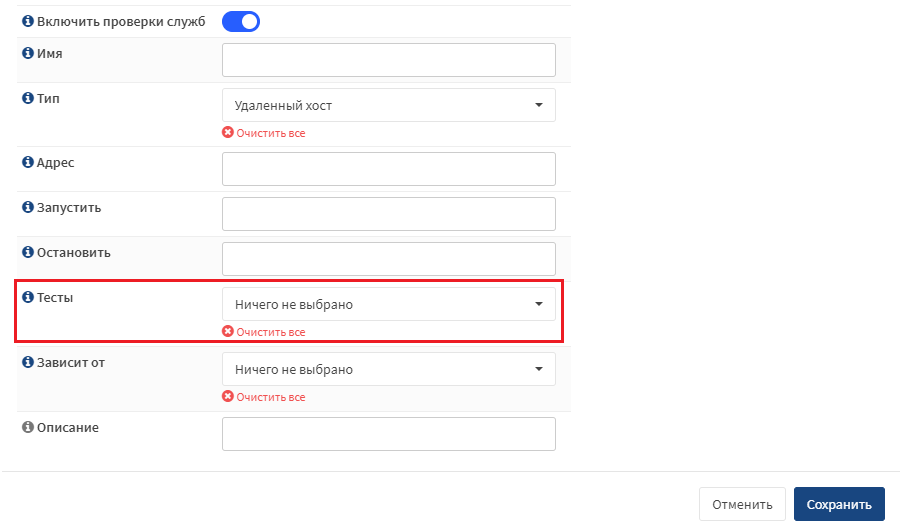


Рис. 800: Выбор теста

Таблица 157: Список тестов

Тест
ChangedStatus
CPUUsage
FAIL PORT 80 LOCALHOST
FAIL PORT 443 LOCALHOST
LoadAvg1
LoadAvg5
LoadAvg15
MemoryUsage
NetworkLink
NetworkSaturation
NonZeroStatus
Ping
SpaceUsage

- в поле **«Зависит от»** выбрать из выпадающего списка необходимую службу, соответствующую таблице;

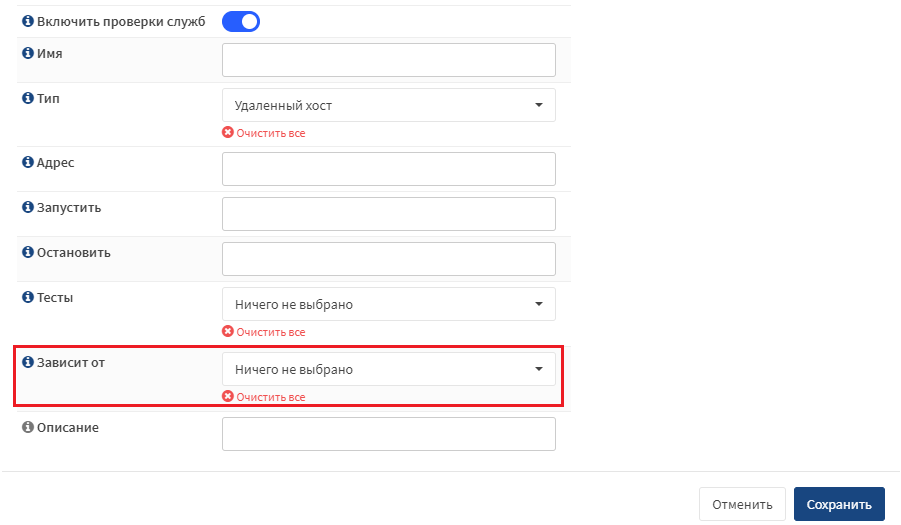


Рис. 801: Зависит от

Таблица 158: Список служб

Служба
RTT_backend
RTT_lighttpd
RTT_lighttpd_443
RTT_PHP_FPM
RTT_RootFs
RTT_systemd-journald
RTT_systemd-logind
RTT_systemd-resolved
RTT_systemd-timesyncd
RTT_systemd-udevd
RTT_System_monitor
Ping
SpaceUsage

- в поле **«Описание»** ввести описание;
- нажать кнопку **«Сохранить»** 

;
- нажать кнопку **«Применить»** 

для вступления сконфигурированного сообщения в силу.

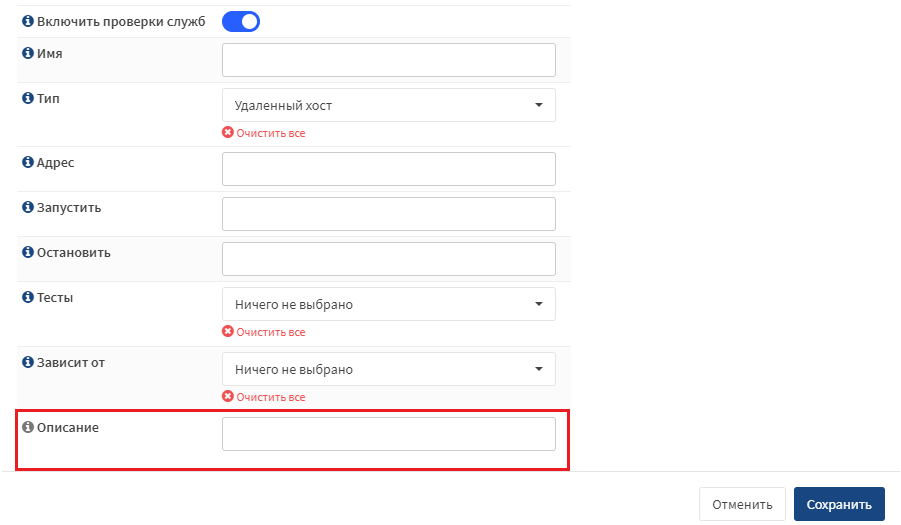


Рис. 802: Описание

Система

Для проверки системы необходимо:

- в поле **«Тип»** окна **«Edit Service»** выбрать из выпадающего списка тип **«Система»**

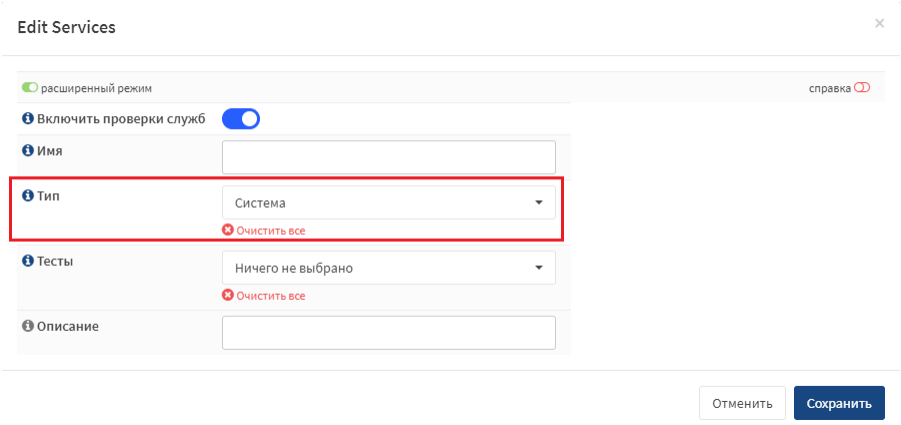


Рис. 803: Выбор системы

- в поле **«Включить проверки служб»** установить переключатель в случае необходимости проверки сервисов;
- в поле **«Имя»** ввести имя сервиса;
- в поле **«Тесты»** выбрать из выпадающего списка необходимый тест сервиса, соответствующий таблице;

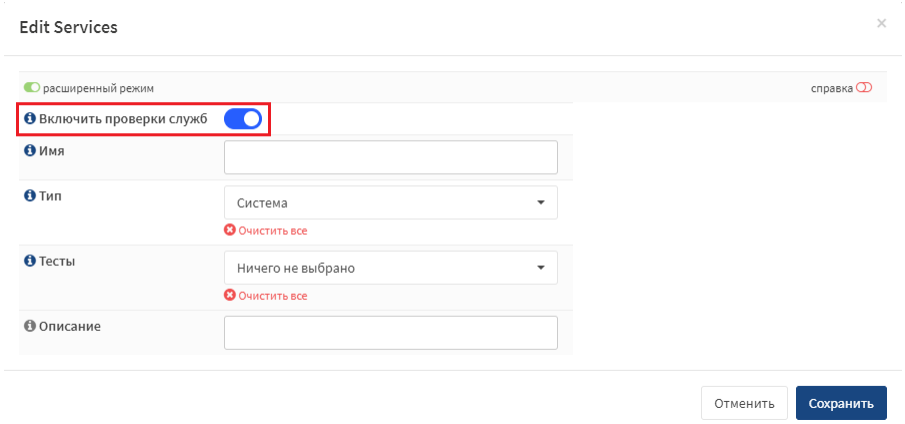


Рис. 804: Включить проверки служб

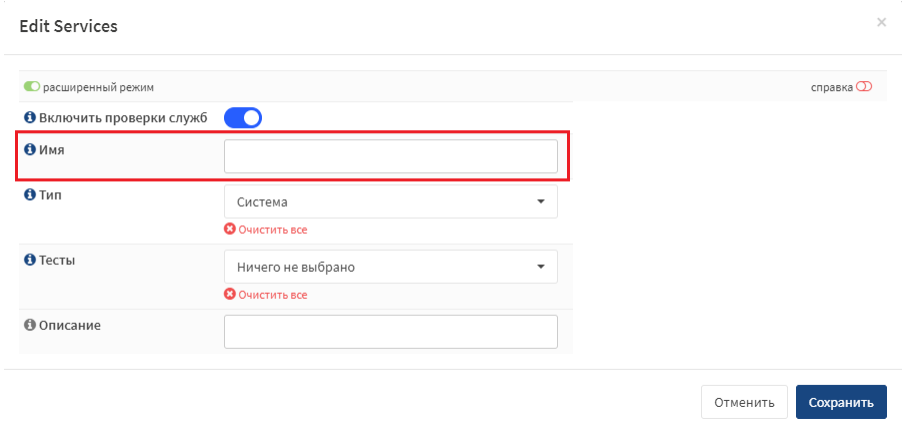


Рис. 805: Имя

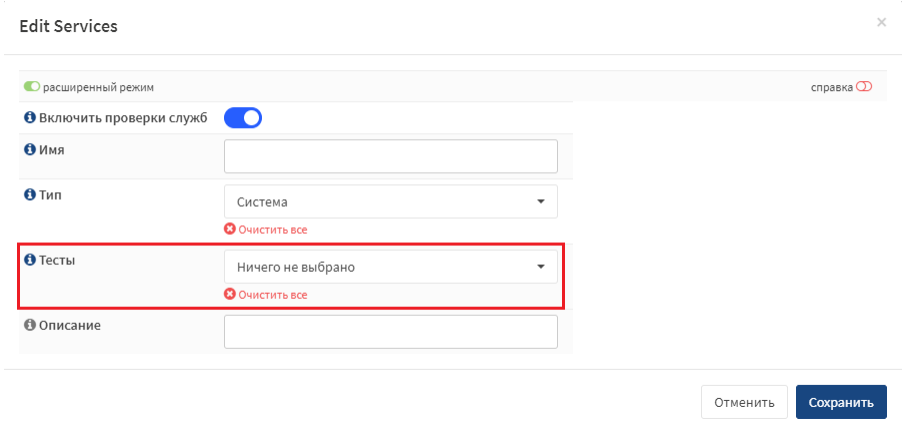


Рис. 806: Выбор теста

Таблица 159: Список тестов

Тест
ChangedStatus
CPUUsage
FAIL PORT 80 LOCALHOST
FAIL PORT 443 LOCALHOST
LoadAvg1
LoadAvg5
LoadAvg15
MemoryUsage
NetworkLink
NetworkSaturation
NonZeroStatus
Ping
SpaceUsage

- в поле **«Описание»** ввести описание;

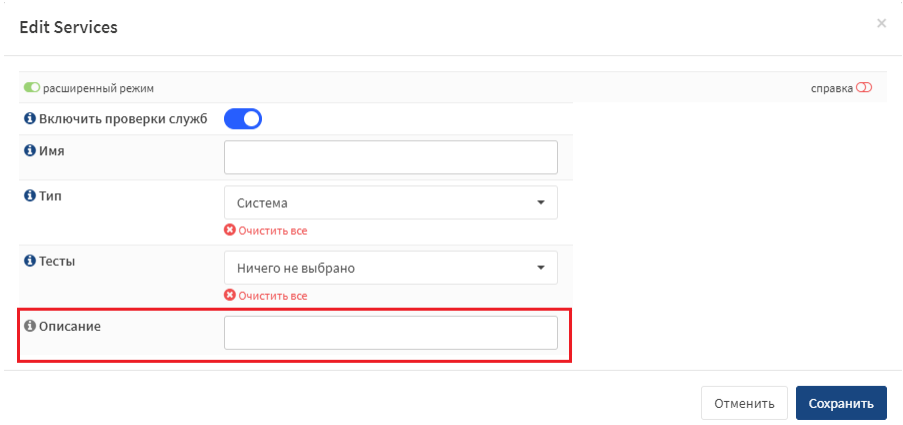


Рис. 807: Описание

- нажать кнопку **«Сохранить»** 

;
- нажать кнопку **«Применить»** 

для вступления сконфигурированного сообщения в силу.

Сеть

Для проверки сети необходимо:

- в поле **«Тип»** окна **«Edit Service»** выбрать из выпадающего списка тип **«Сеть»**

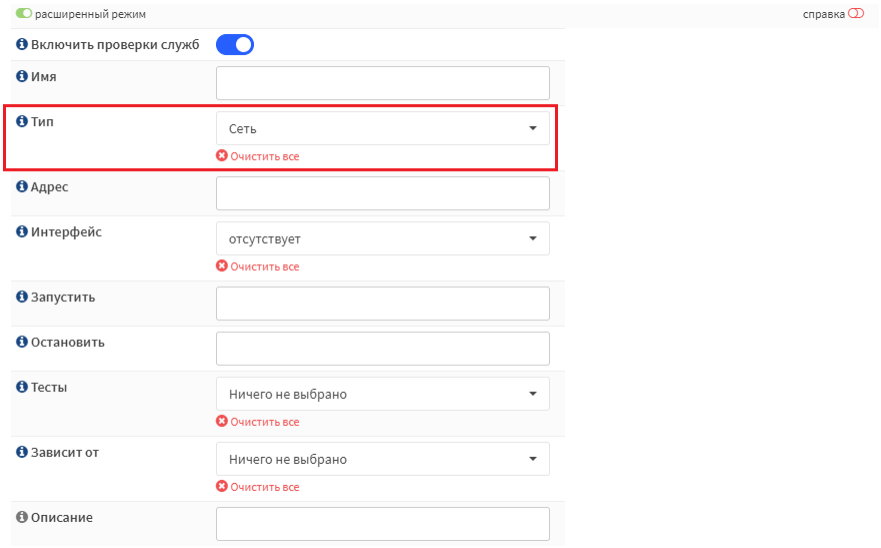


Рис. 808: Выбор сети

- в поле **«Включить проверки служб»** установить переключатель в случае необходимости проверки сервисов;

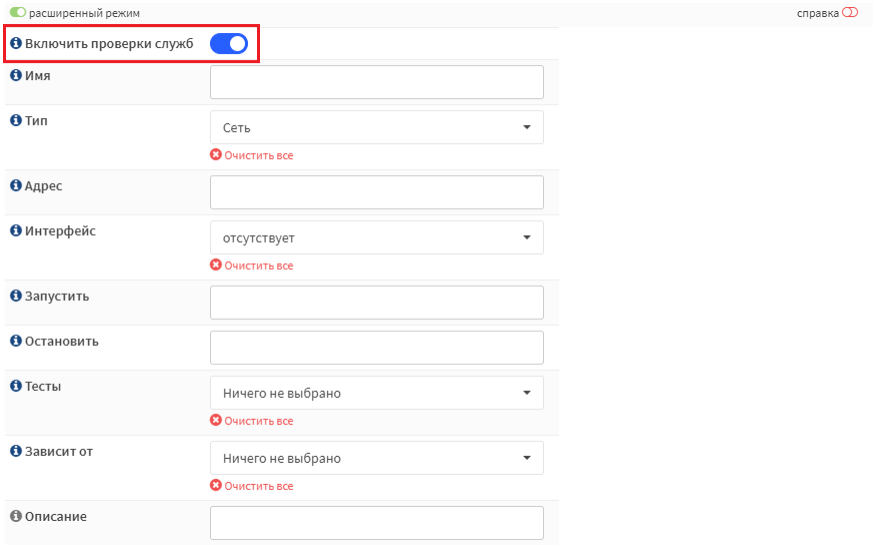


Рис. 809: Включить проверки служб

- в поле **«Имя»** ввести имя сервиса;
- в поле **«Адрес»** ввести целевой IP-адрес для проверок удалённой сети;
- в поле **«Интерфейс»** выбрать из выпадающего списка необходимый интерфейс, соответствующий таблице;

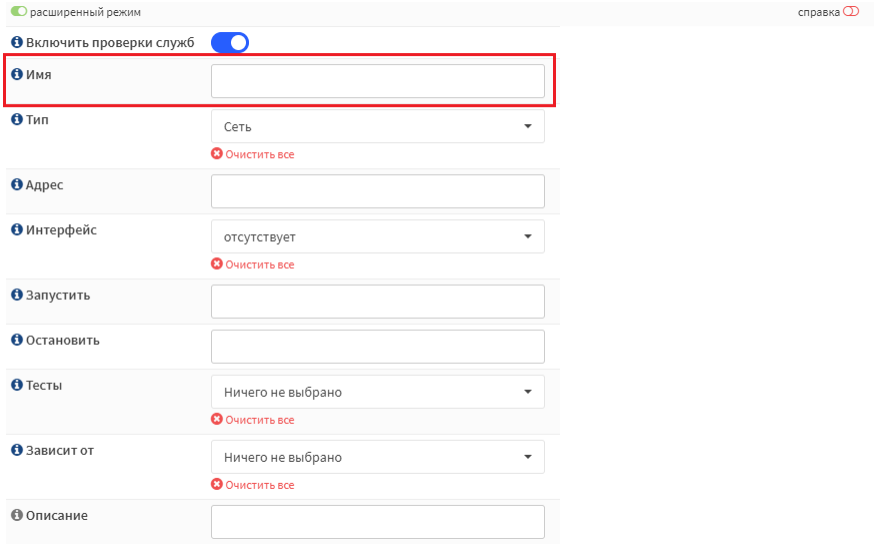


Рис. 810: Имя

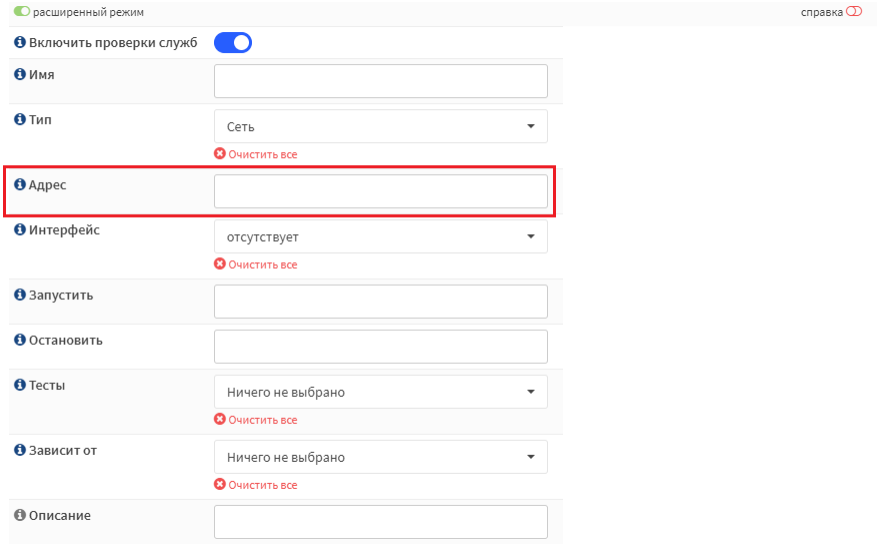


Рис. 811: Адрес

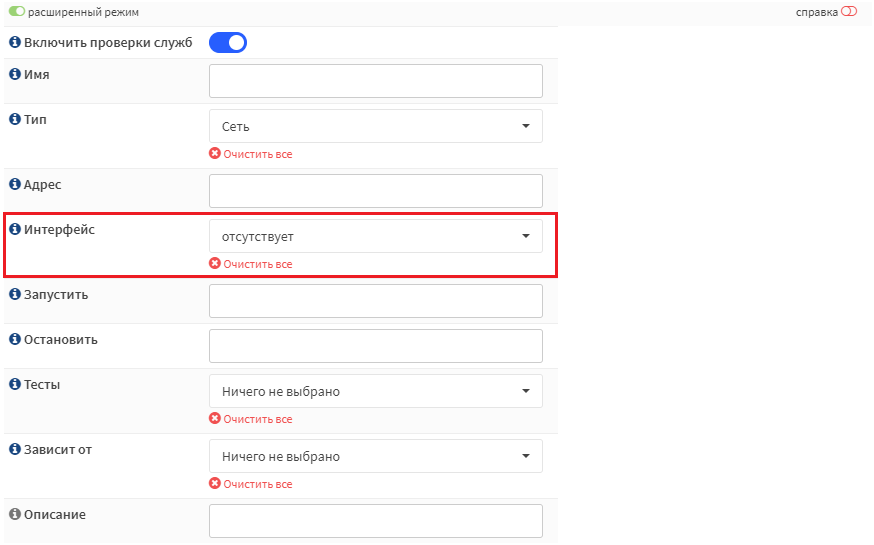


Рис. 812: Интерфейс

Таблица 160: Список интерфейсов

Интерфейс
отсутствует
LAN

- в поле **«Запустить»** ввести сценарий запуска службы;

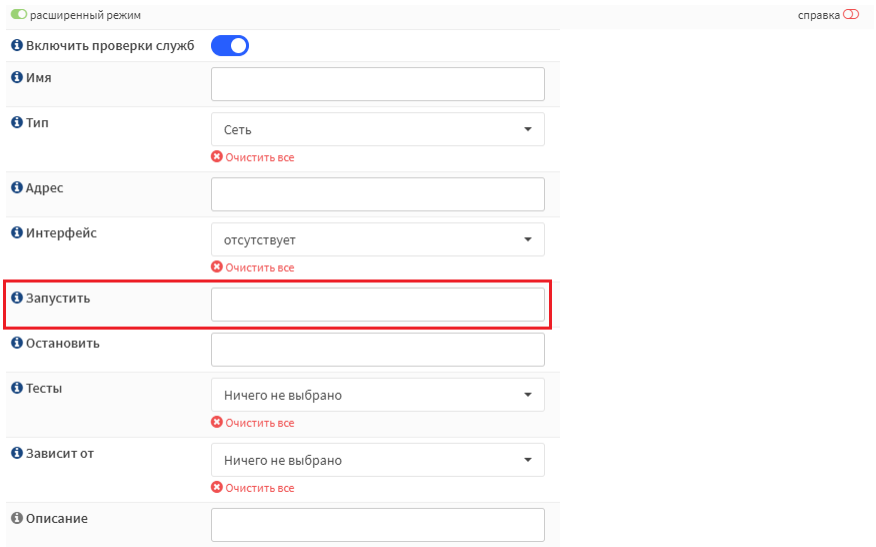


Рис. 813: Запустить

- в поле **«Остановить»** ввести скрипт остановки службы;
- в поле **«Тесты»** выбрать из выпадающего списка необходимый тест сервиса, соответствующий таблице;

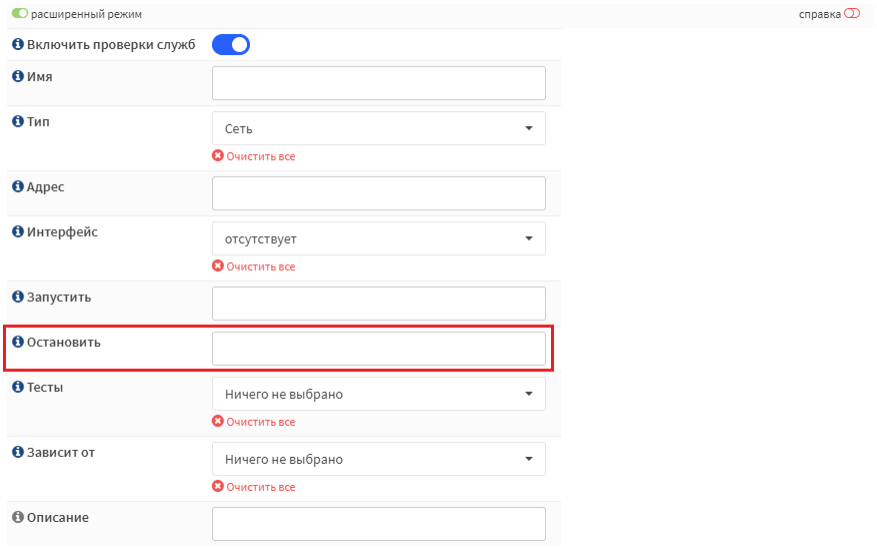


Рис. 814: Остановить

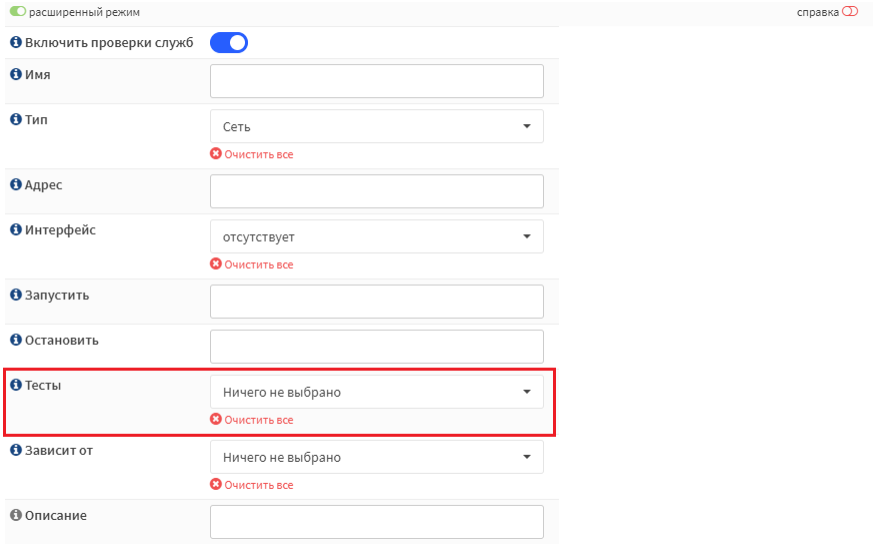


Рис. 815: Выбор теста

Таблица 161: Список тестов

Тест
ChangedStatus
CPUUsage
FAIL PORT 80 LOCALHOST
FAIL PORT 443 LOCALHOST
LoadAvg1
LoadAvg5
LoadAvg15
MemoryUsage
NetworkLink
NetworkSaturation
NonZeroStatus
Ping
SpaceUsage

- в поле **«Зависит от»** выбрать из выпадающего списка необходимую службу, соответствующую таблице;

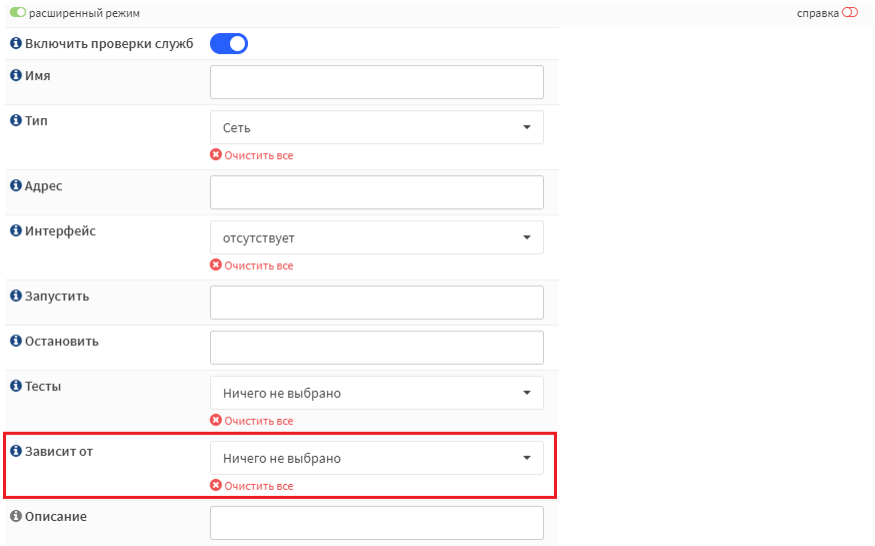


Рис. 816: Зависит от

Таблица 162: Список служб

Служба
RTT_backend
RTT_lighttpd
RTT_lighttpd_443
RTT_PHP_FPM
RTT_RootFs
RTT_systemd-journald
RTT_systemd-logind
RTT_systemd-resolved
RTT_systemd-timesyncd
RTT_systemd-udevd
RTT_System_monitor
Ping
SpaceUsage

- в поле **«Описание»** ввести описание;

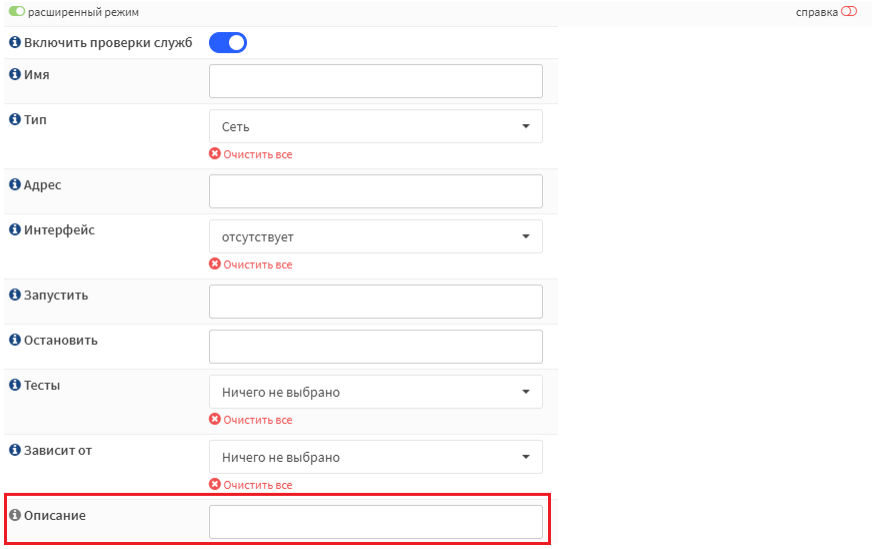


Рис. 817: Описание

- нажать кнопку **«Сохранить»** 

;
- нажать кнопку **«Применить»** 

для вступления сконфигурированного сообщения в силу.

Настройки тестов служб

Для настройки тестов служб необходимо нажать кнопку «+».

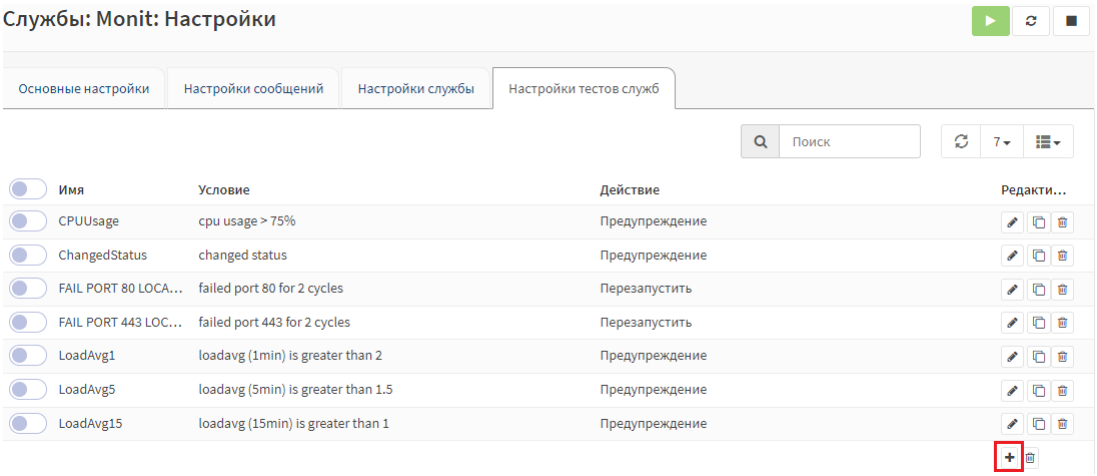


Рис. 818: Настройка тестов служб

В открывшемся окне необходимо:

- в поле **«Имя»** ввести имя теста;

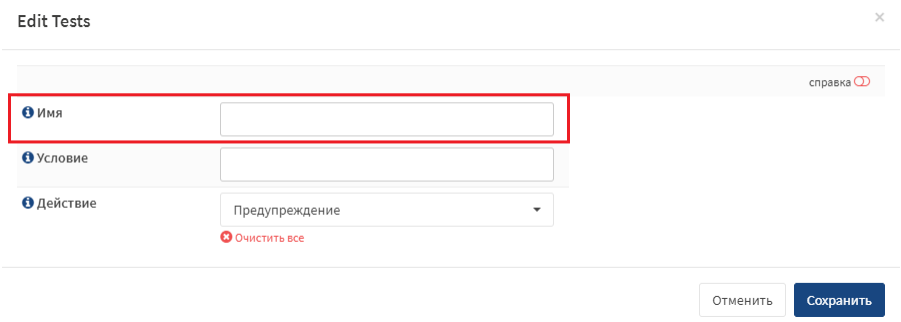


Рис. 819: Имя

- в поле **«Условие»** ввести условие теста;

> **Примечание**
>
> Например, cpu is greater than 50%

- в поле **«Действие»** выбрать из выпадающего списка необходимое действие, соответствующее таблице;

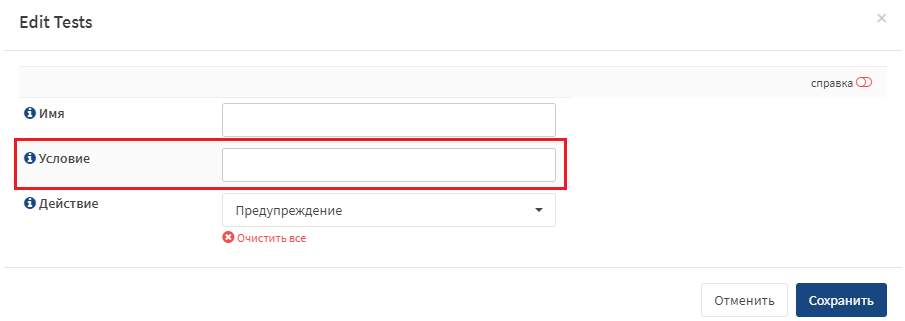


Рис. 820: Условие

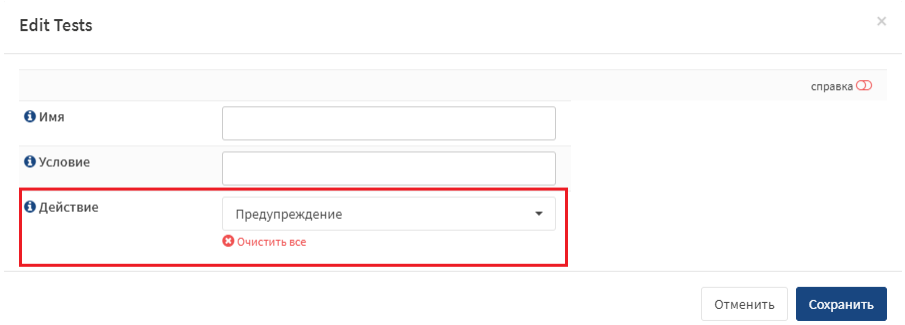


Рис. 821: Действие

Таблица 163: Список действий

Действие
Предупреждение
Перезапустить
Запустить
Остановить
Выполнять
Не контролировать

- при выборе действия **«Выполнять»** дополнительно указать путь

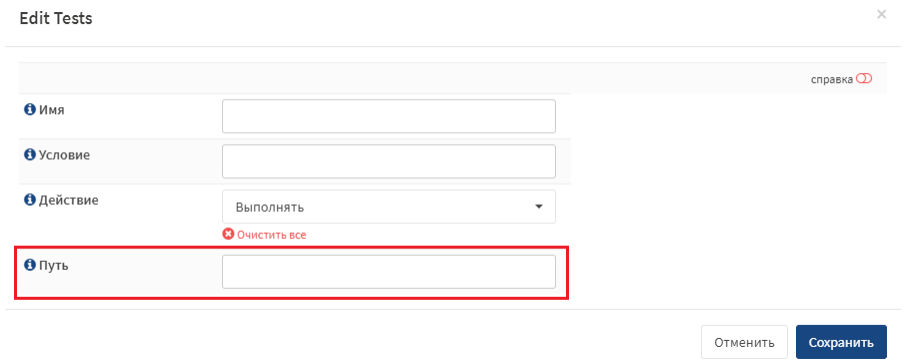


Рис. 822: Путь

Примечание

Убедитесь, что скрипт может быть выполнен сервисом Monit.

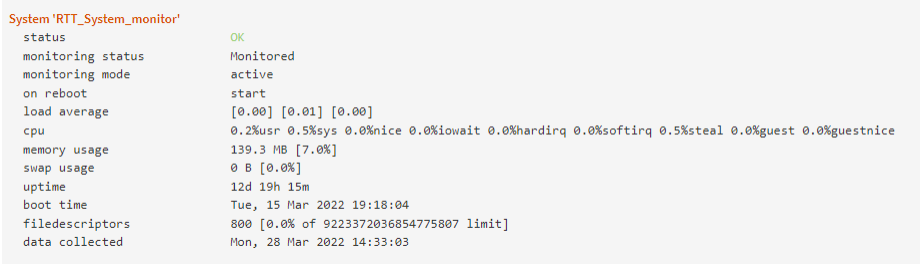
- нажать кнопку **«Сохранить»** 

;
- нажать кнопку **«Применить»** 

для вступления сконфигурированного сообщения в силу.

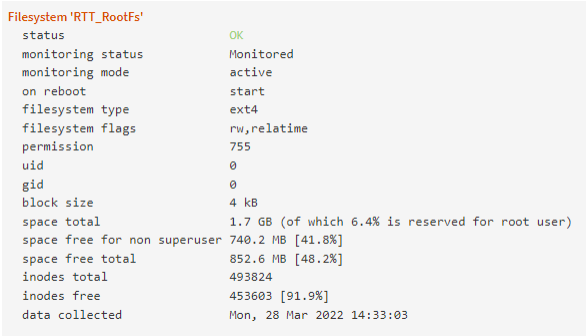
Статус

Вкладка **«Статус»** содержит информацию о проведенном мониторинге служб.



```
System 'RTT_System_monitor'
  status                       OK
  monitoring status            Monitored
  monitoring mode              active
  on reboot                    start
  load average                 [0.00] [0.01] [0.00]
  cpu                          0.2%usr 0.5%sys 0.0%nice 0.0%iowait 0.0%hardirq 0.0%softirq 0.5%steal 0.0%guest 0.0%guestnice
  memory usage                 139.3 MB [7.0%]
  swap usage                   0 B [0.0%]
  uptime                       12d 19h 15m
  boot time                    Tue, 15 Mar 2022 19:18:04
  filedescriptors              800 [0.0% of 9223372036854775807 limit]
  data collected               Mon, 28 Mar 2022 14:33:03
```

Рис. 823: Мониторинг службы **«RTT_System_monito»**



```
Filesystem 'RTT_RootFs'
  status                       OK
  monitoring status            Monitored
  monitoring mode              active
  on reboot                    start
  filesystem type              ext4
  filesystem flags             rw,relatime
  permission                   755
  uid                          0
  gid                          0
  block size                   4 kB
  space total                  1.7 GB (of which 6.4% is reserved for root user)
  space free for non superuser 740.2 MB [41.8%]
  space free total             852.6 MB [48.2%]
  inodes total                 493824
  inodes free                  453603 [91.9%]
  data collected               Mon, 28 Mar 2022 14:33:03
```

Рис. 824: Мониторинг службы **«RTT_RootFs»**

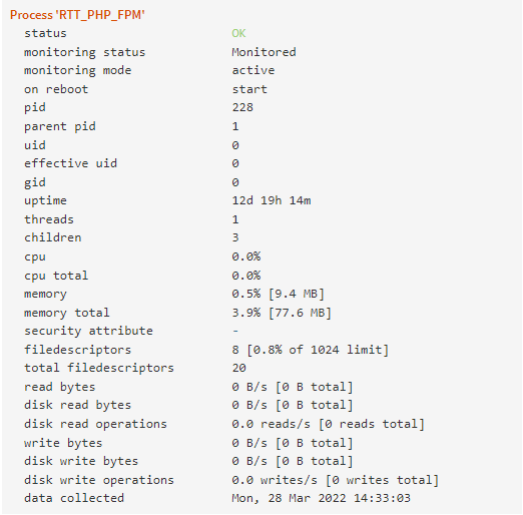
2.7.8.4 Сетевое время

Для перехода к настройкам сетевого времени необходимо:

- нажать на вкладку **«Службы»** - **«Сетевое время»** - **«Общие настройки»**, расположенную в левой части списка объектов управления;

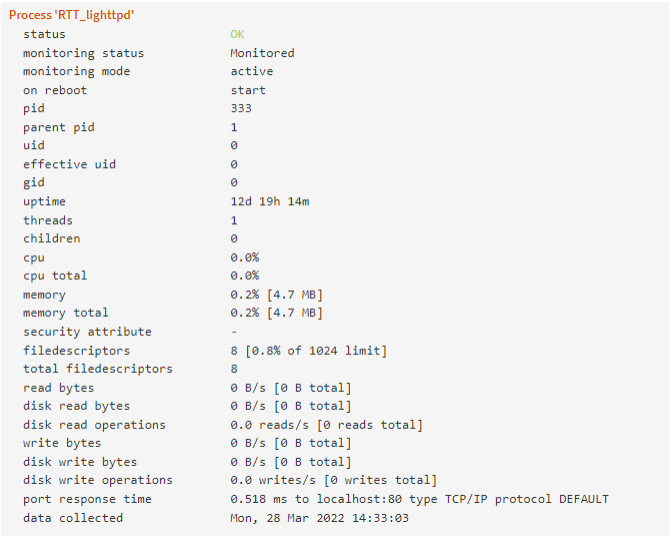
Для перехода к просмотру статуса сетевого времени необходимо:

- нажать на вкладку **«Службы»** - **«Сетевое время»** - **«Статус»**, расположенную в левой части списка объектов управления;



```
Process 'RTT_PHP_FPM'
  status                            OK
  monitoring status                 Monitored
  monitoring mode                   active
  on reboot                         start
  pid                               228
  parent pid                        1
  uid                               0
  effective uid                     0
  gid                               0
  uptime                            12d 19h 14m
  threads                           1
  children                          3
  cpu                               0.0%
  cpu total                         0.0%
  memory                            0.5% [9.4 MB]
  memory total                      3.9% [77.6 MB]
  security attribute                -
  filedescriptors                   8 [0.8% of 1024 limit]
  total filedescriptors             20
  read bytes                        0 B/s [0 B total]
  disk read bytes                   0 B/s [0 B total]
  disk read operations              0.0 reads/s [0 reads total]
  write bytes                       0 B/s [0 B total]
  disk write bytes                  0 B/s [0 B total]
  disk write operations             0.0 writes/s [0 writes total]
  data collected                    Mon, 28 Mar 2022 14:33:03
```

Рис. 825: Мониторинг службы **«RTT_PHP_FPM»**



```
Process 'RTT_lighttpd'
  status                            OK
  monitoring status                 Monitored
  monitoring mode                   active
  on reboot                         start
  pid                               333
  parent pid                        1
  uid                               0
  effective uid                     0
  gid                               0
  uptime                            12d 19h 14m
  threads                           1
  children                          0
  cpu                               0.0%
  cpu total                         0.0%
  memory                            0.2% [4.7 MB]
  memory total                      0.2% [4.7 MB]
  security attribute                -
  filedescriptors                   8 [0.8% of 1024 limit]
  total filedescriptors             8
  read bytes                        0 B/s [0 B total]
  disk read bytes                   0 B/s [0 B total]
  disk read operations              0.0 reads/s [0 reads total]
  write bytes                       0 B/s [0 B total]
  disk write bytes                  0 B/s [0 B total]
  disk write operations             0.0 writes/s [0 writes total]
  port response time                0.518 ms to localhost:80 type TCP/IP protocol DEFAULT
  data collected                    Mon, 28 Mar 2022 14:33:03
```

Рис. 826: Мониторинг службы **«RTT_lighttpd»**

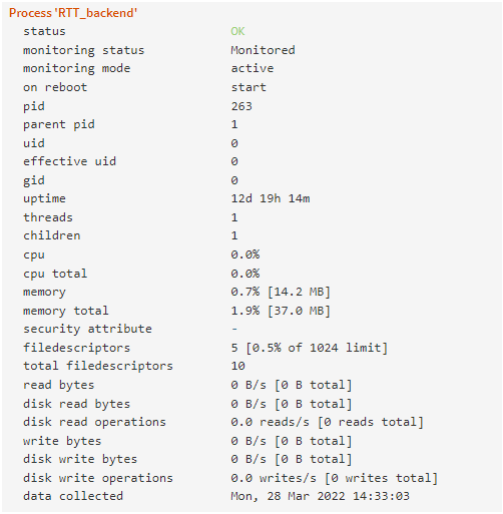


Рис. 827: Мониторинг службы **«RTT_backend»**

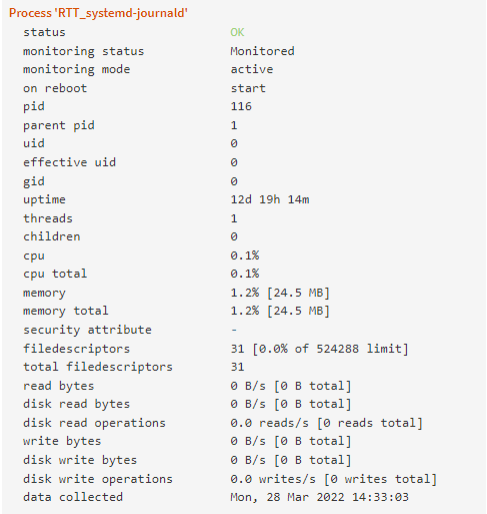


Рис. 828: Мониторинг службы **«RTT_systemd-journald»**

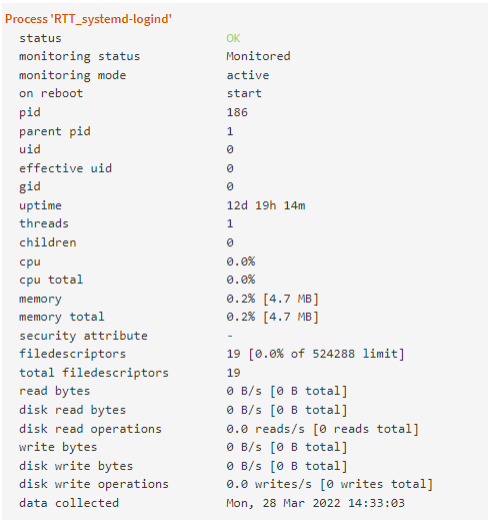


Рис. 829: Мониторинг службы **«RTT_systemd-logind»**

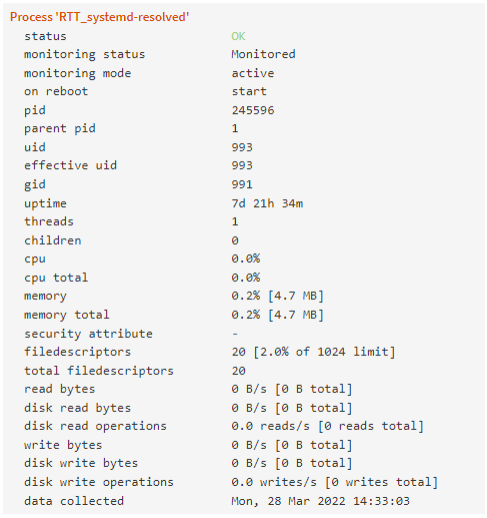


Рис. 830: Мониторинг службы **«RTT_systemd-resolved»**

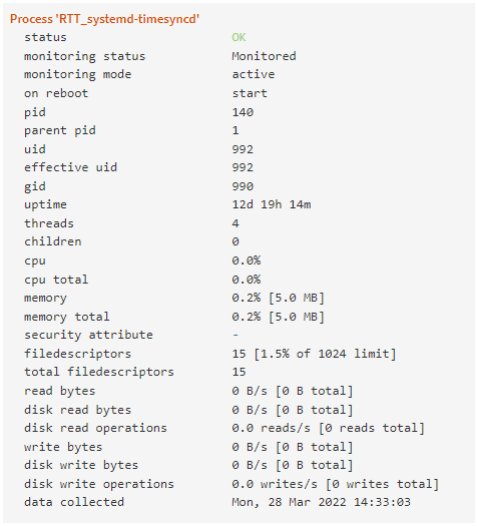


Рис. 831: Мониторинг службы **«RTT_systemd-timesyncd»**

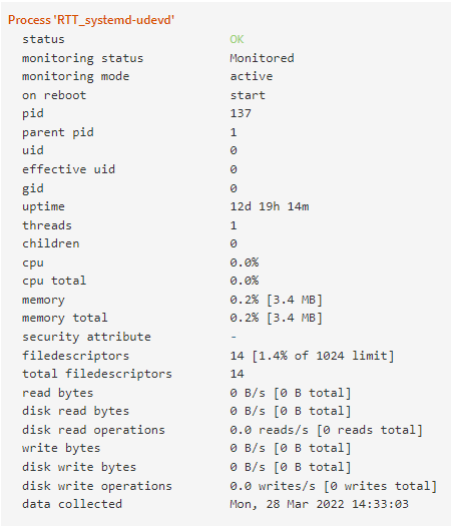


Рис. 832: Мониторинг службы **«RTT_systemd-udevd»**

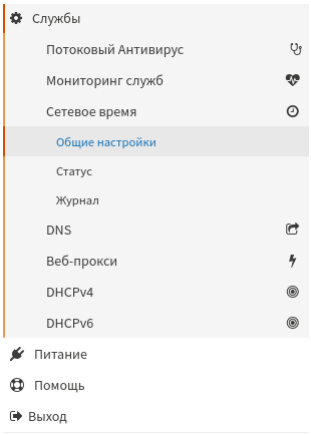


Рис. 833: Переход к настройкам сетевого времени

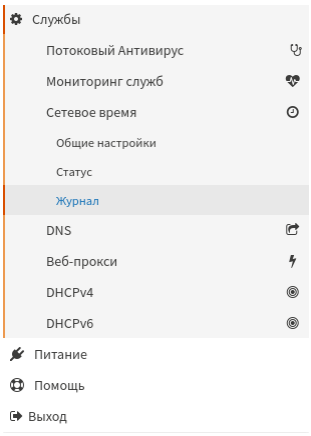


Рис. 834: Переход к просмотру статуса сетевого времени

Для перехода к просмотру журнала сетевого времени необходимо:

- нажать на вкладку **«Службы»** - **«Сетевое время»** - **«Журнал»**, расположенную в левой части списка объектов управления;

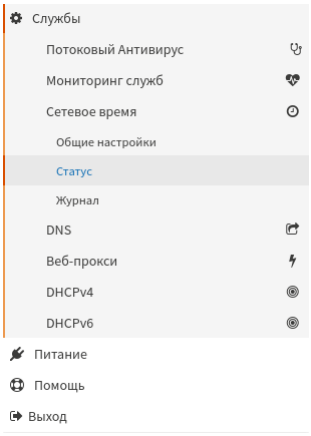


Рис. 835: Переход к просмотру журнала сетевого времени

Общие настройки

В разделе **«Конфигурация NTP-сервера»** необходимо:

- в поле **«Интерфейс (-ы)»** выбрать из выпадающего списка необходимые интерфейсы;

Примечание

Интерфейсы без IP-адресов не будут показаны

Примечание

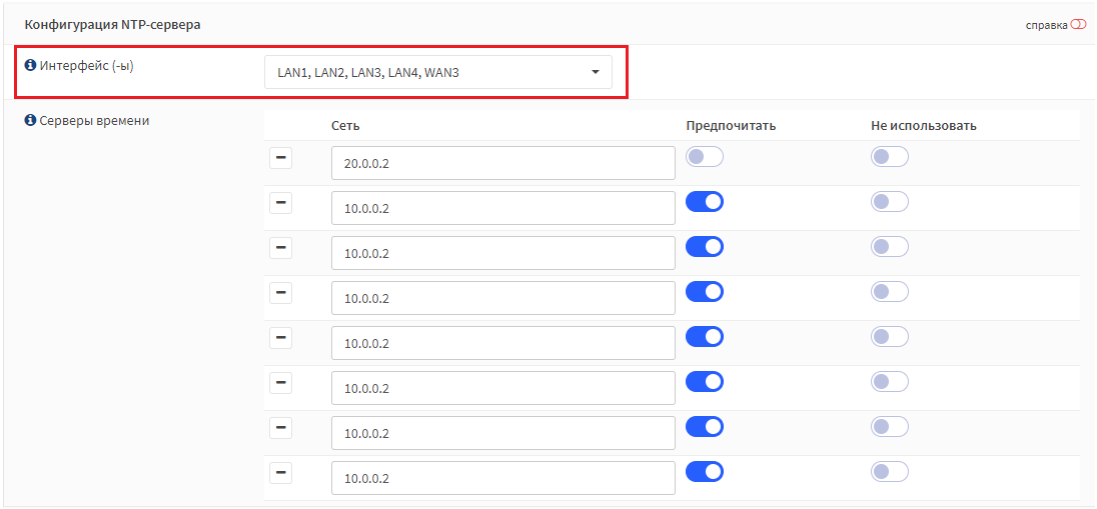


Рис. 836: Выбор интерфейса

Параметр **«Ничего не выбрано»** будет прослушивать все интерфейсы с помощью специального символа

Примечание

Выбор всех интерфейсов будет явно прослушивать только указанные интерфейсы/IP

- в поле **«Серверы времени»** следует:
  - нажать кнопку «+»  для добавления нового сервера;
  - в колонке **«Сеть»** указать сервер;
  - колонке **«Предпочитать»** напротив выбранного сервера установить переключатель в случае необходимости указать, что для NTP более предпочтителен этот сервер, чем остальные;
  - колонке **«Не использовать»** напротив выбранного сервера установить переключатель в случае необходимости указать, что NTP не должен использовать этот сервер для времени, но статистика для этого сервера будет собираться и отображаться;

Примечание

Для лучшего результата необходимо настроить от трех до пяти серверов

  - нажать кнопку **«Сохранить»** 

.

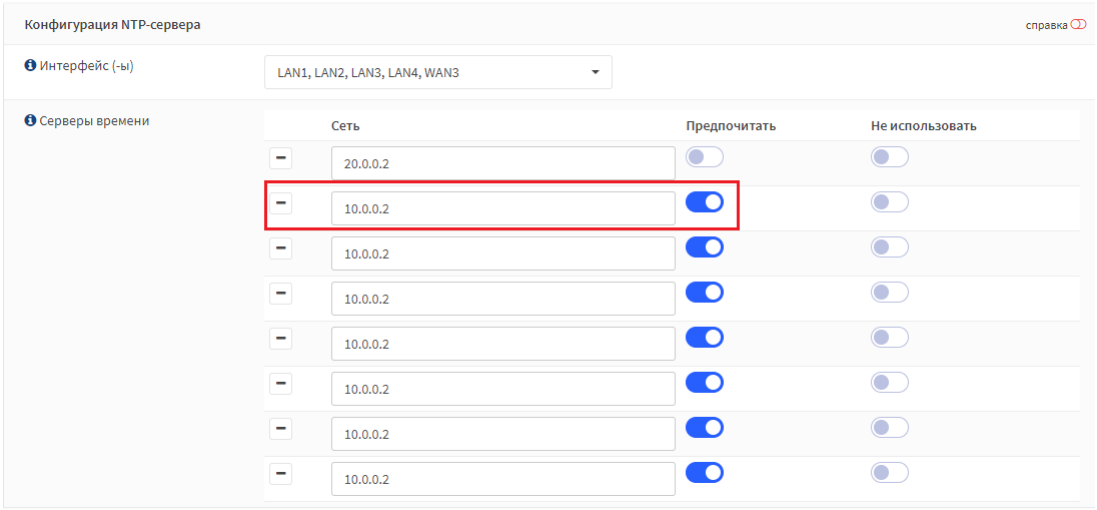


Рис. 837: Выбор предпочтения сервера

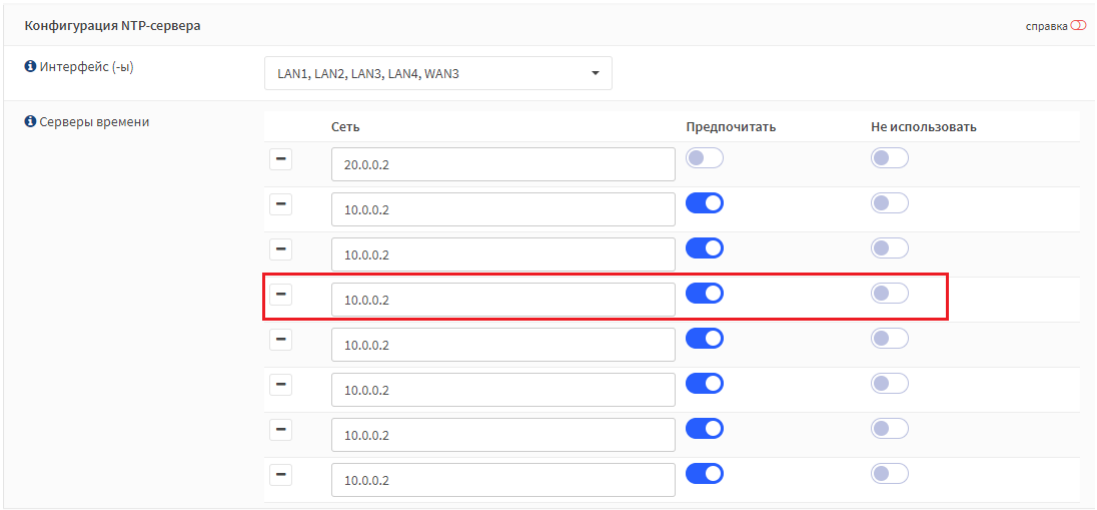


Рис. 838: Ограничение использования сервера

Статус

В разделе **«Статус»** отражена информация о текущем статусе

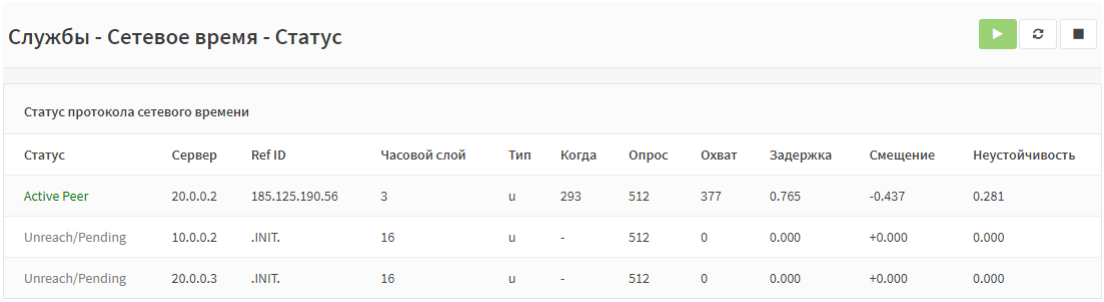


Рис. 839: Статус

Журнал

Раздел **«Журнал»** содержит журнал сетевого времени.

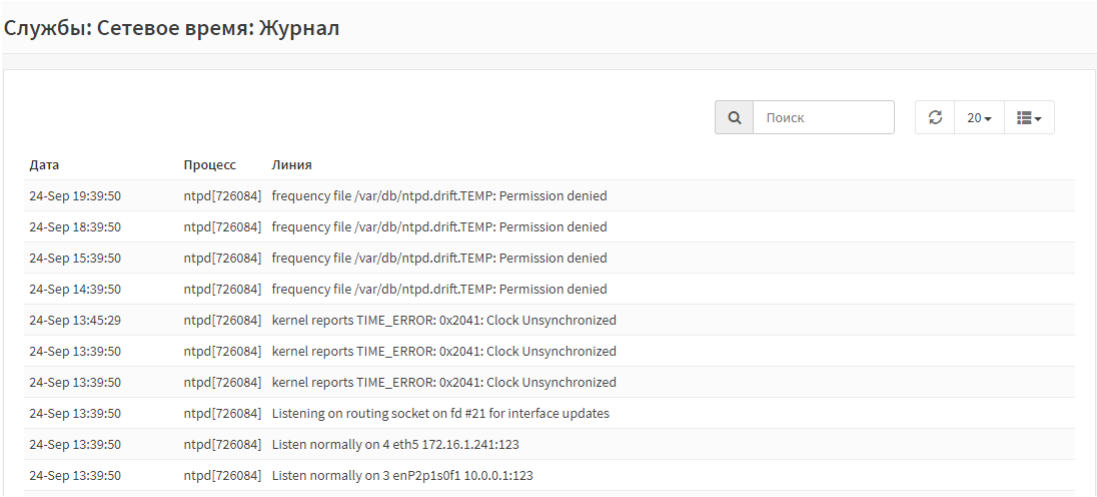


Рис. 840: Журнал сетевого времени

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

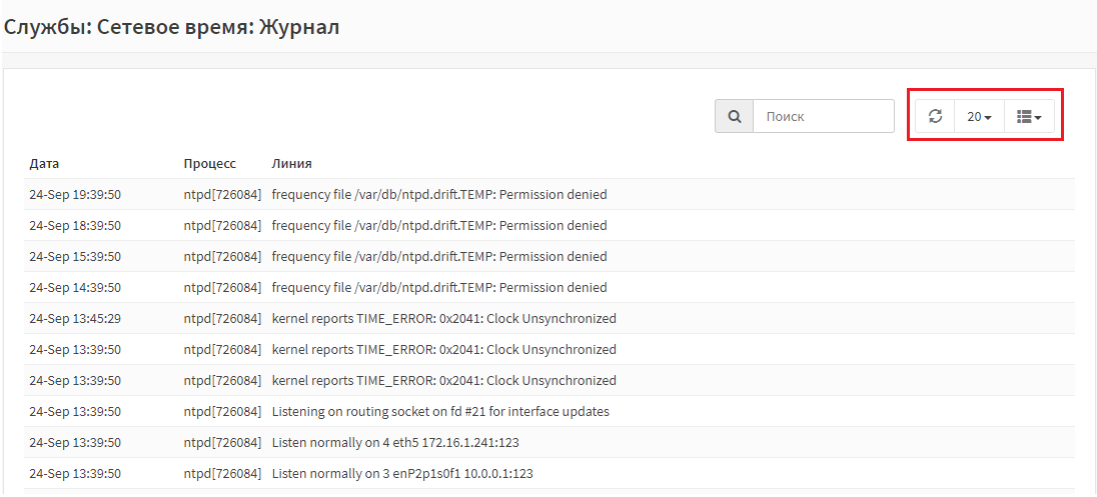


Рис. 841: Фильтры журнала сетевого времени

2.7.8.5 DNS

Для перехода к настройкам системы DNS необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Общие настройки»**, расположенную в левой части списка объектов управления;

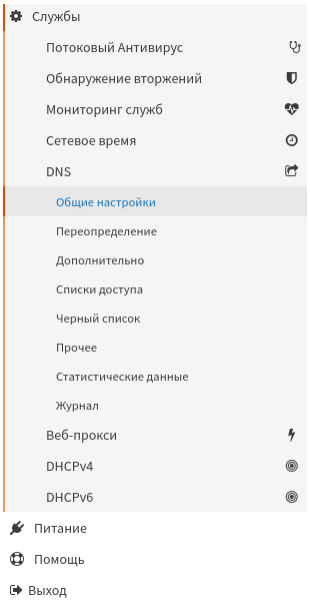


Рис. 842: Переход к настройкам DNS

Для перехода к настройкам переопределения результатов необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Переопределение»**, расположенную в левой части списка объектов управления;

Для перехода к настройкам дополнительных параметров преобразователя необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Дополнительно»**, расположенную в левой части

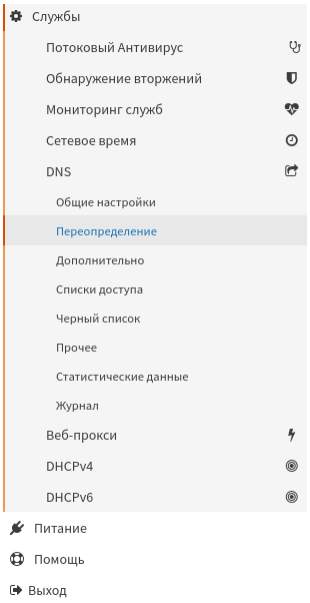


Рис. 843: Переход к настройкам переопределения результатов

списка объектов управления;

Для перехода к настройкам списков доступа необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Списки доступа»**, расположенную в левой части списка объектов управления;

Для перехода к настройкам черного списка необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Черный список»**, расположенную в левой части списка объектов управления;

Для перехода к прочим настройкам необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Прочее»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру статистических данных необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Статистические данные»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала необходимо:

- нажать на вкладку **«Службы»** - **«DNS»** - **«Журнал»**, расположенную в левой части списка объектов управления;

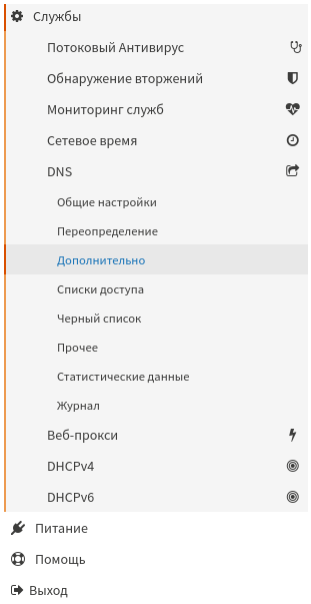


Рис. 844: Переход к настройкам дополнительных параметров преобразователя

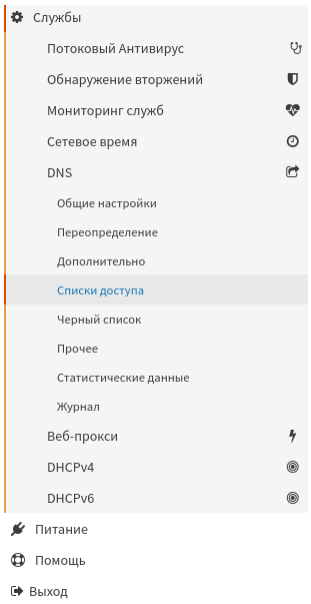


Рис. 845: Переход к настройкам списков доступа

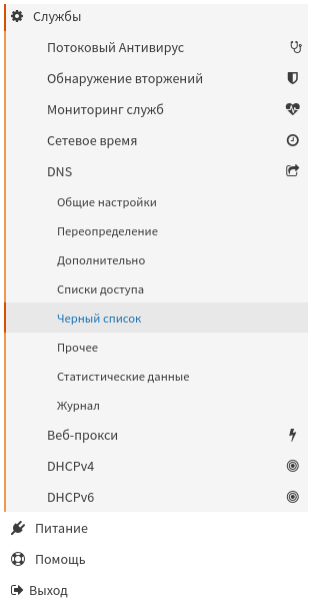


Рис. 846: Переход к настройкам черного списка

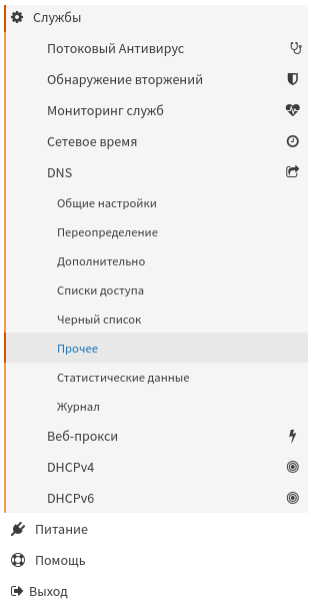


Рис. 847: Переход к прочим настройкам

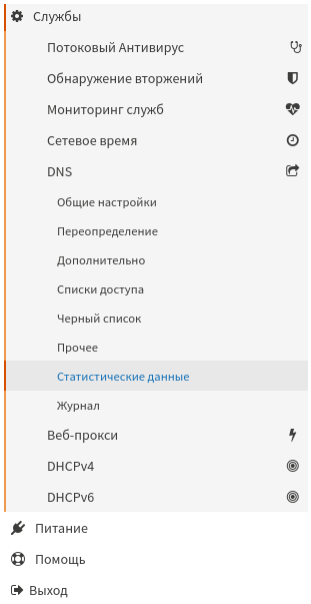


Рис. 848: Переход к просмотру статистических данных

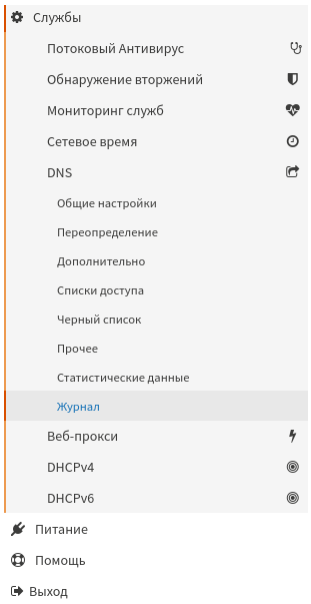


Рис. 849: Переход к просмотру журнала

Общие настройки

Для выполнения настроек системы DNS необходимо:

- в поле **«Включен»** установить переключатель в случае необходимости включения системы DNS;

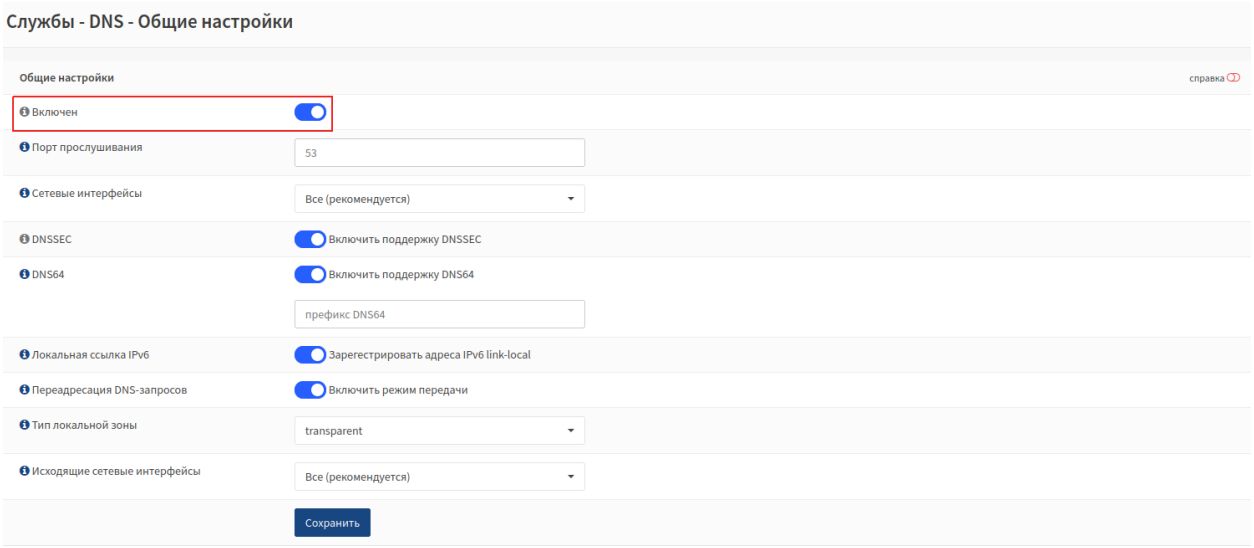


Рис. 850: Включение системы DNS

- в поле **«Порт прослушивания»** установить значение порта, который отвечает за DNS запросы;

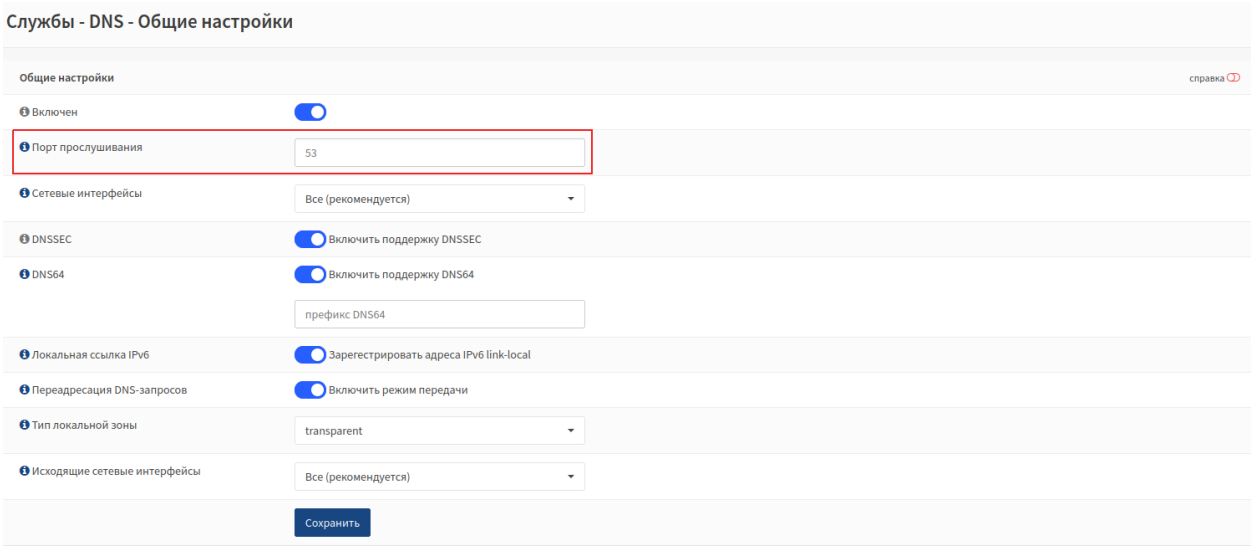


Рис. 851: Установка порта

Совет

Как правило, это поле оставляют пустым, если нет других служб, которые необходимо привязать к порту 53 TCP/UDP

- в поле **«Сетевые интерфейсы»** выбрать из выпадающего списка сетевые интерфейсы;

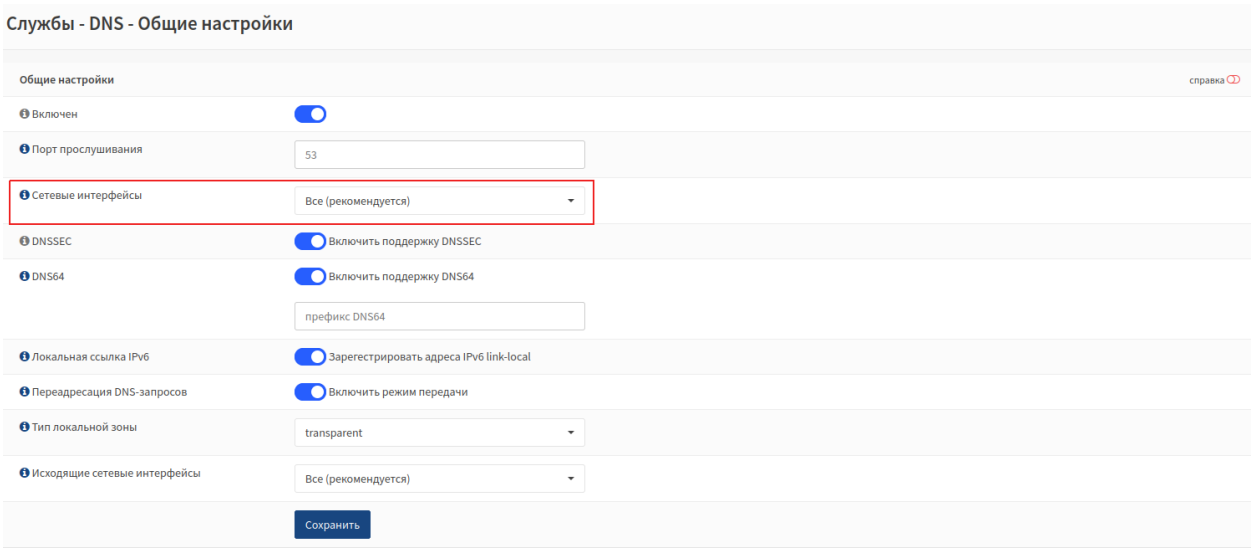


Рис. 852: Выбор сетевых интерфейсов

Совет

IP-адреса интерфейса, используемые для ответа на запросы от клиентов. Если интерфейс имеет IPv4 и IPv6 IP, используются оба

Совет

Запросы к другим IP-адресам интерфейса, не выбранным ниже, отбрасываются. Поведение по умолчанию — отвечать на запросы по каждому доступному адресу IPv4 и IPv6

- в поле **«DNSSEC»** установить переключатель в случае необходимости включения поддержки DNSSEC;
- в поле **«DNS64»** установить переключатель, указать префикс в случае необходимости включения поддержки DNS64;

Совет

Если опция включена, DNS синтезировать AAAA запись из A записи, если актуальная AAAA запись отсутствует

Совет

Если префикс не указан, по умолчанию будет 64:ff9b::/96 (RFC 6052)

- в поле **«Локальная ссылка IPv6»** установить переключатель в случае необходимости регистрации локальных IPv6-адресов в Unbound;

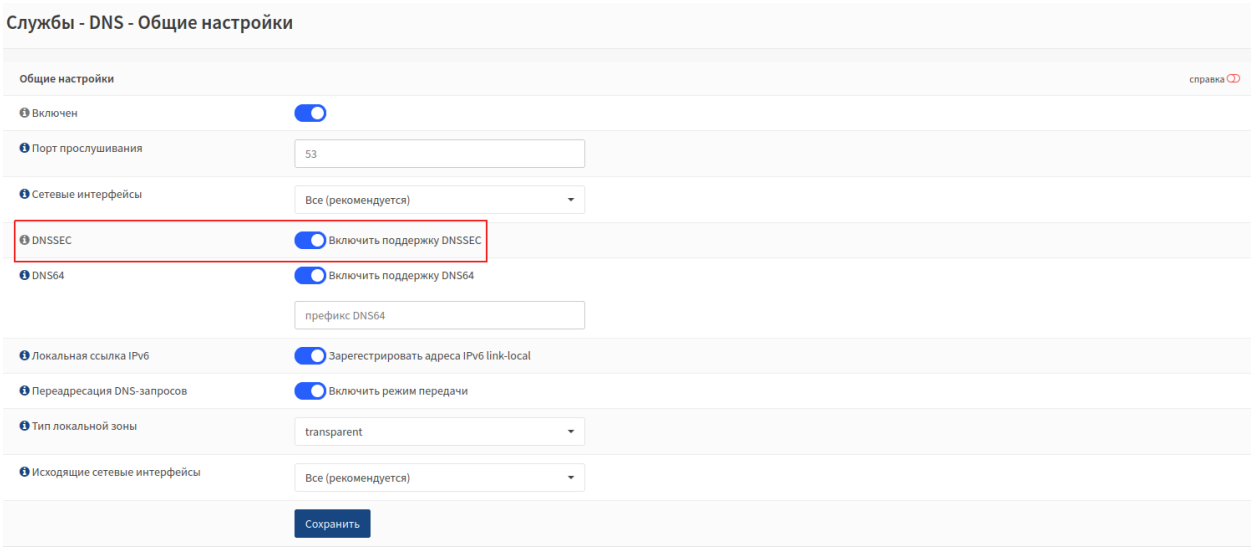


Рис. 853: Включение DNSSEC

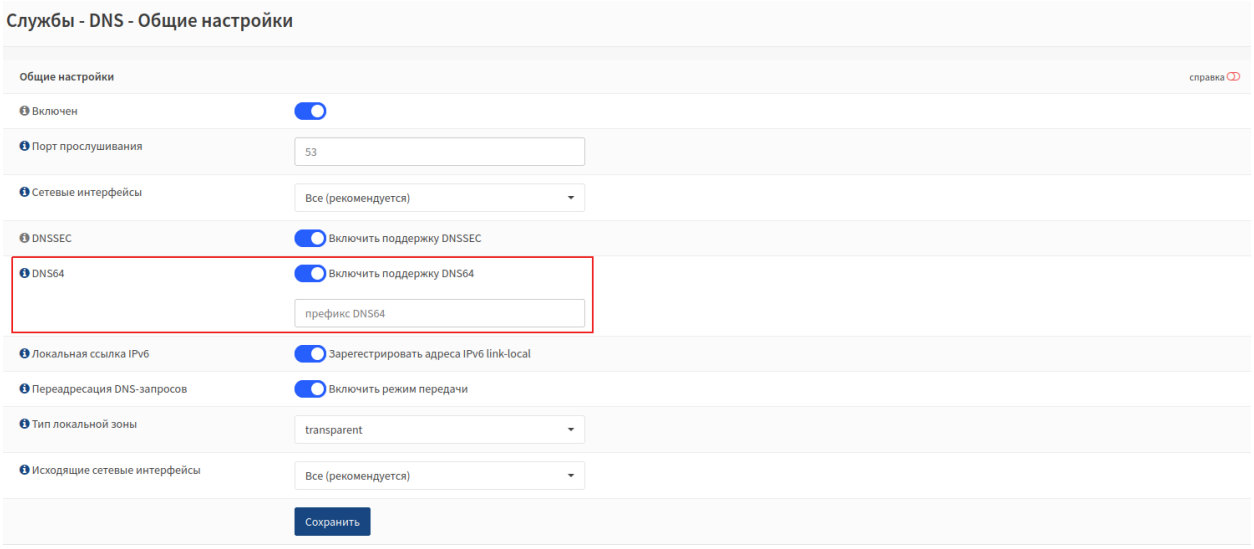


Рис. 854: Включение DNS64

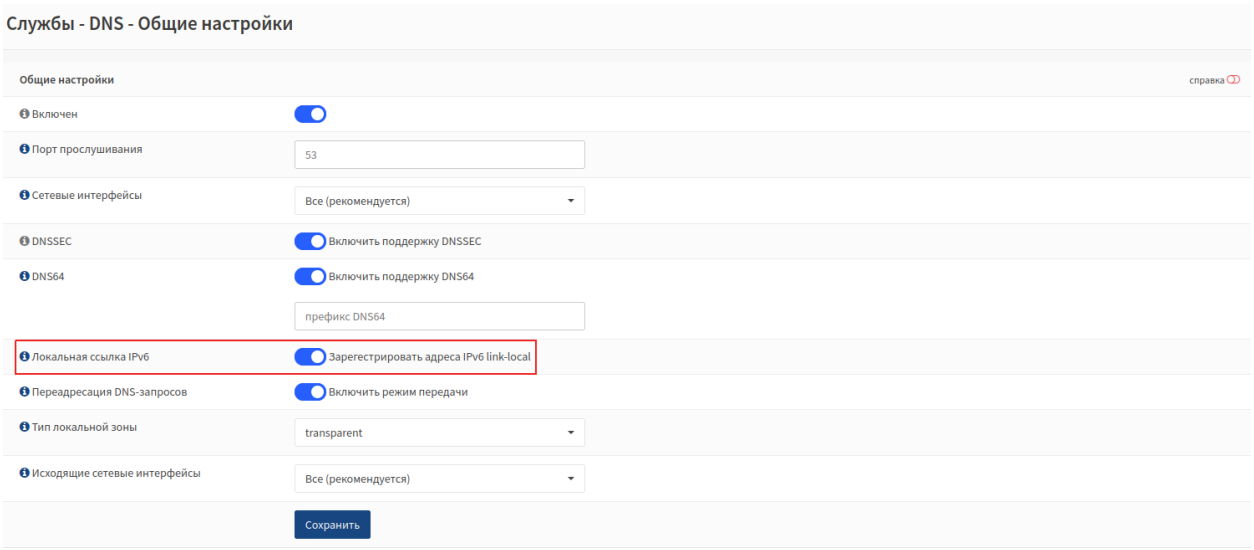


Рис. 855: Регистрация адресов

Совет

Если этот параметр не установлен, локальные IPv6-адреса не будут зарегистрированы в Unbound, что предотвратит возврат недостижимого адреса, когда настроено более одного интерфейса прослушивания

- в поле **«Переадресация DNS-запросов»** установить переключатель в случае необходимости использования настроенных системных серверов имен для переадресации запросов;

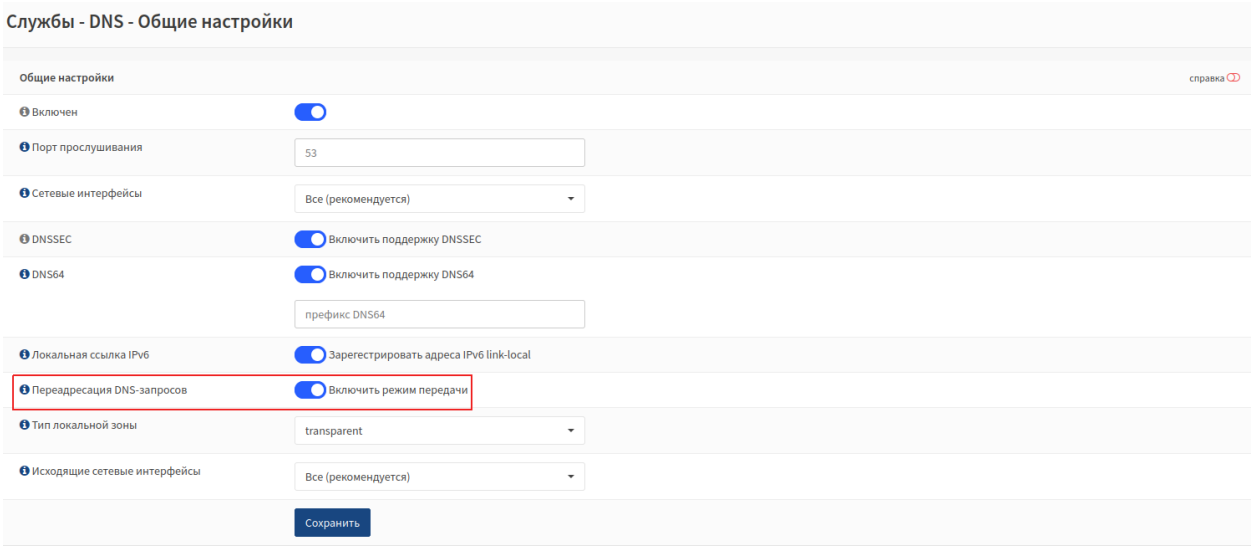


Рис. 856: Включение переадресации DNS-запросов

- в поле **«Тип локальной зоны»** выбрать из выпадающего списка необходимый тип локальной зоны, используемый для системного домена;

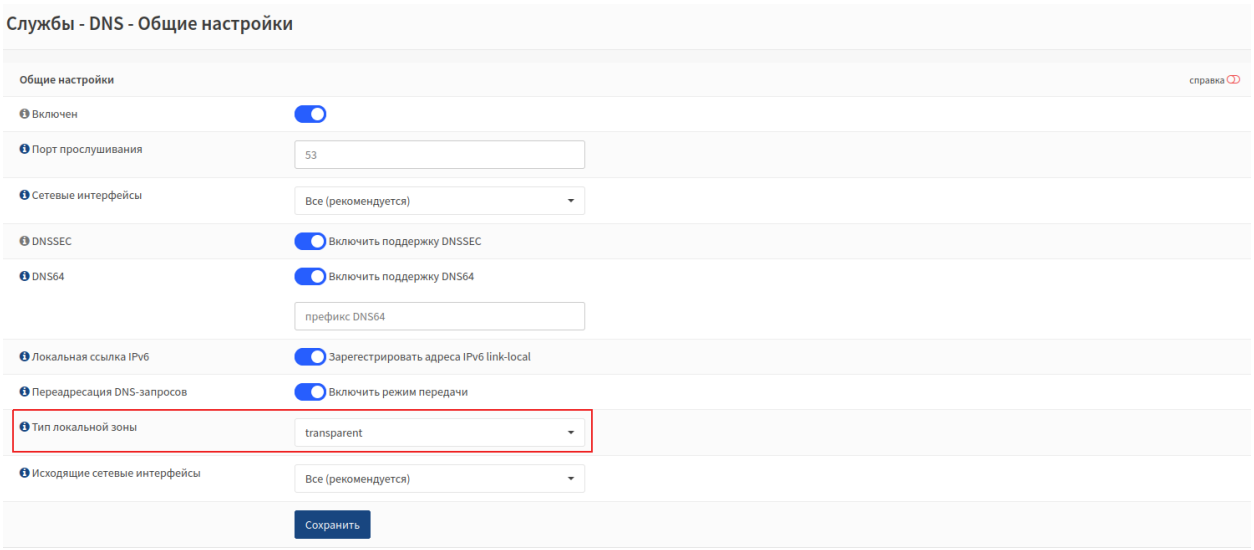


Рис. 857: Выбор типа локальной зоны

Совет

Описания типов доступны в разделе «local-zone:» на странице руководства unbound.conf(5)

Совет

По умолчанию «transparent»

- в поле **«Исходящие сетевые интерфейсы»** выбрать из выпадающего списка необходимые сетевые интерфейсы;

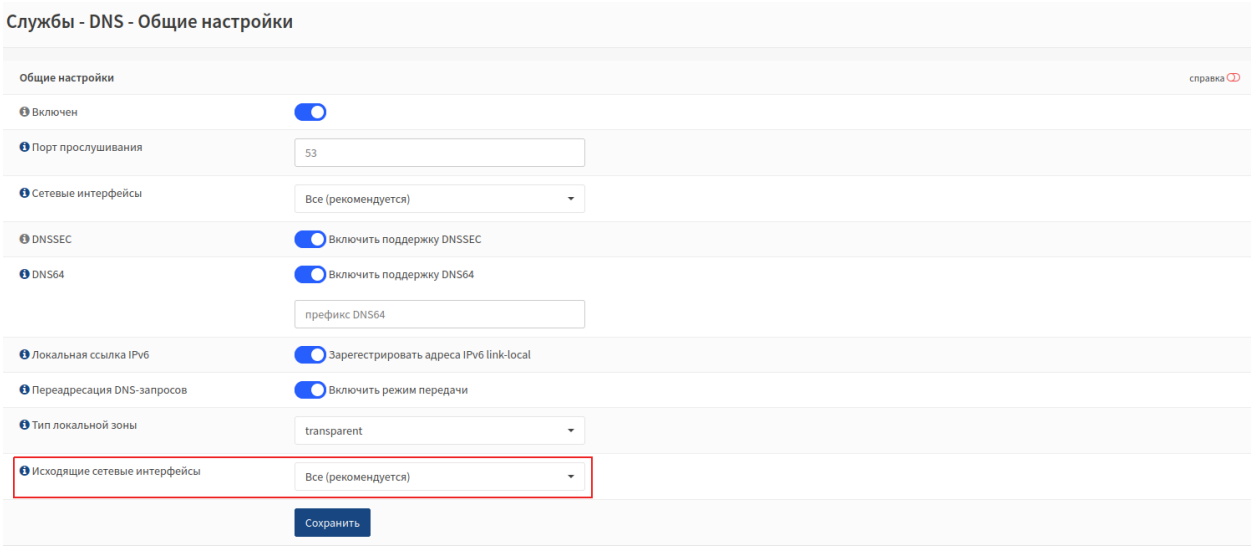


Рис. 858: Выбор исходящих сетевых интерфейсов

Совет

Используйте различные сетевые интерфейсы, которые Unbound будет использовать для отправки запросов на авторитетные серверы и получения их ответов

Совет

По умолчанию используются все интерфейсы

Внимание

Установка явных исходящих интерфейсов работает только в том случае, если они настроены статически

Для вступления проведенных настроек в силу необходимо нажать кнопку Сохранить .

Переопределение

Вкладка **«Переопределение»** представлена на рисунке.

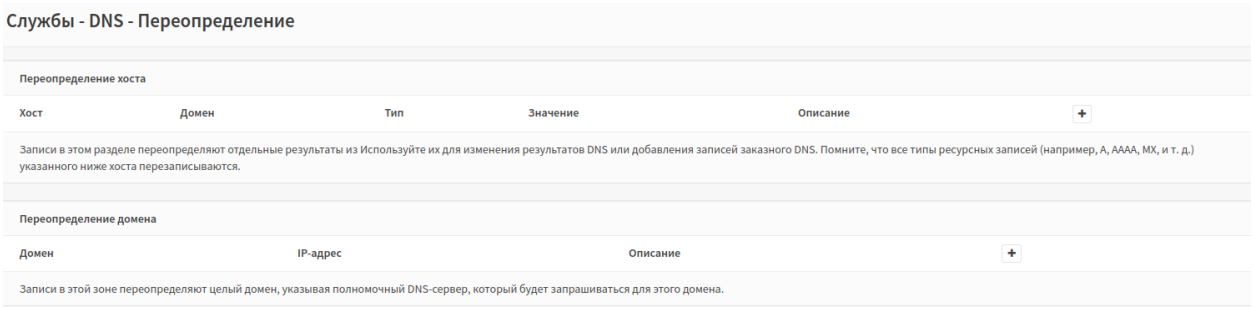


Рис. 859: Вкладка «Переопределение»

Переопределение хоста

Для переопределения хоста необходимо нажать кнопку + .

В открывшемся окне необходимо:

- в поле **«Хост»** указать имя хоста без доменной части;

Совет

Используйте «*» для создания wildcard-записи

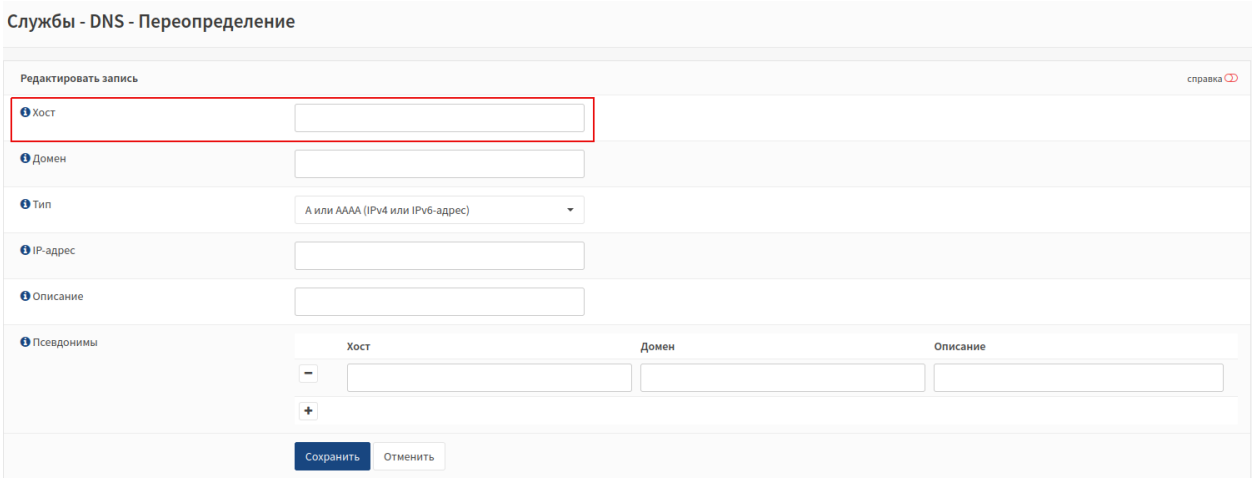


Рис. 860: Установка хоста

- в поле **«Домен»** указать домен хоста;

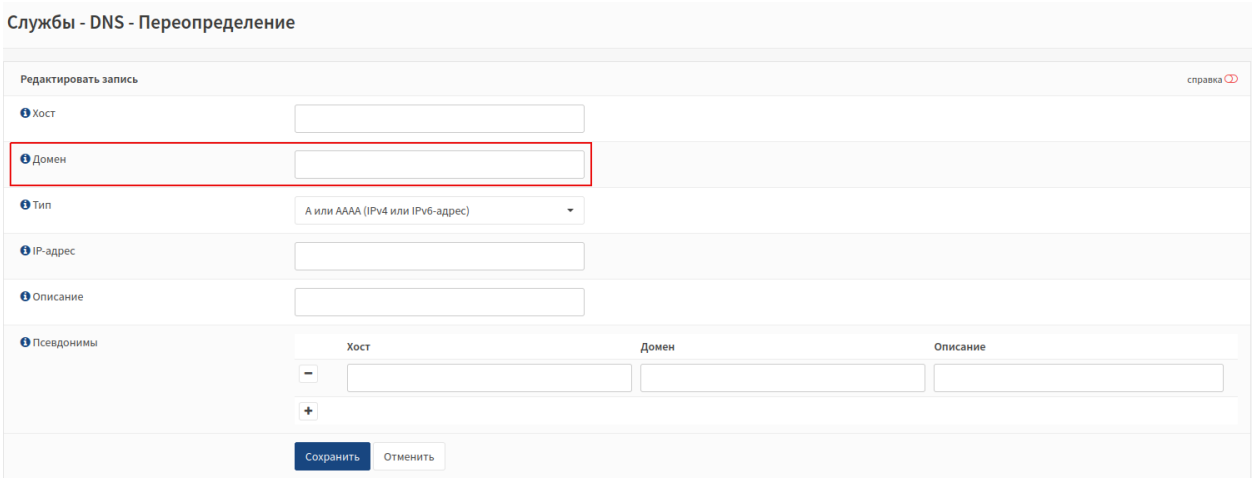


Рис. 861: Установка домена хоста

- в поле **«Тип»** выбрать из выпадающего списка тип доменной записи;
- в поле **«IP-адрес»** указать IP-адрес хоста (при выборе тип доменной записи **«A или AAAA для IPv4 или IPv6-адресов»**);
- в поле **«Приоритет MX-записи»** установить приоритет MX-записи (при выборе тип доменной записи **«MX (почтовый сервер)»**);
- в поле **«Хост MX»** ввести имя хоста MX (при выборе тип доменной записи **«MX (почтовый сервер)»**);
- в поле **«Описание»** задать краткое описание;
- в поле **«Псевдонимы»** ввести дополнительные имена для этого хоста;

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

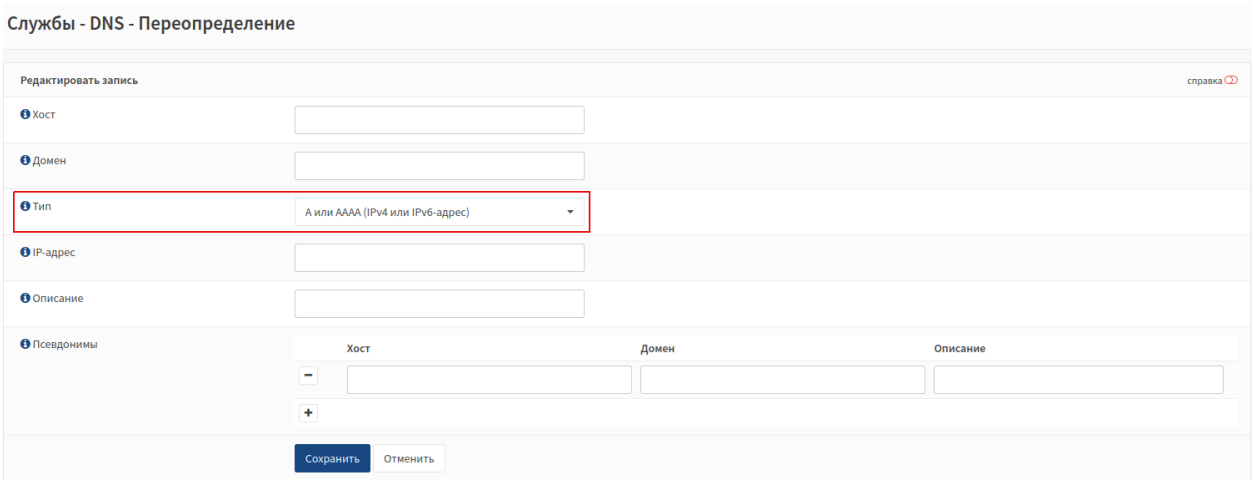


Рис. 862: Выбор типа доменной записи

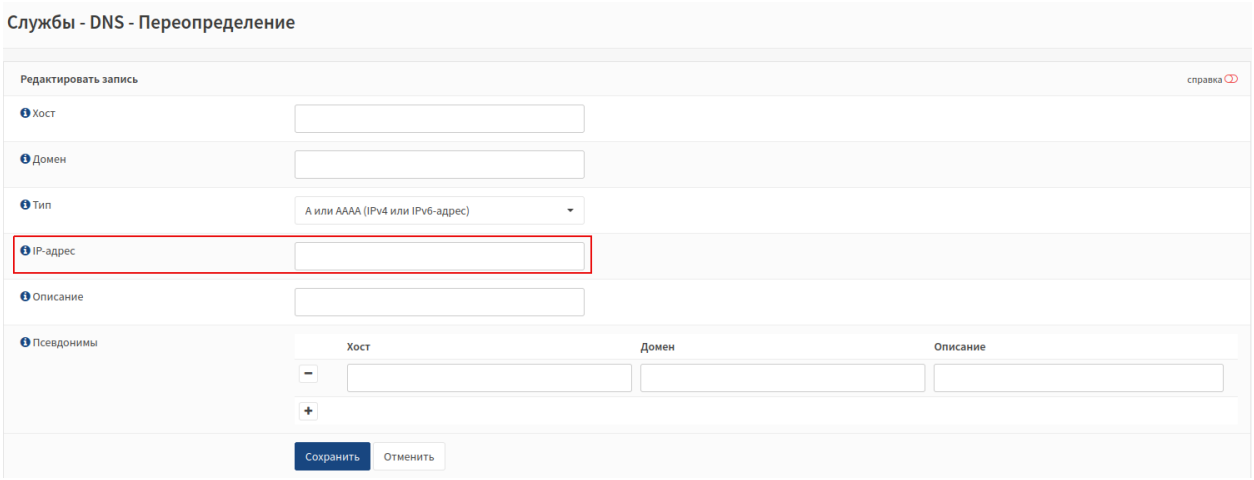


Рис. 863: Выбор IP-адреса

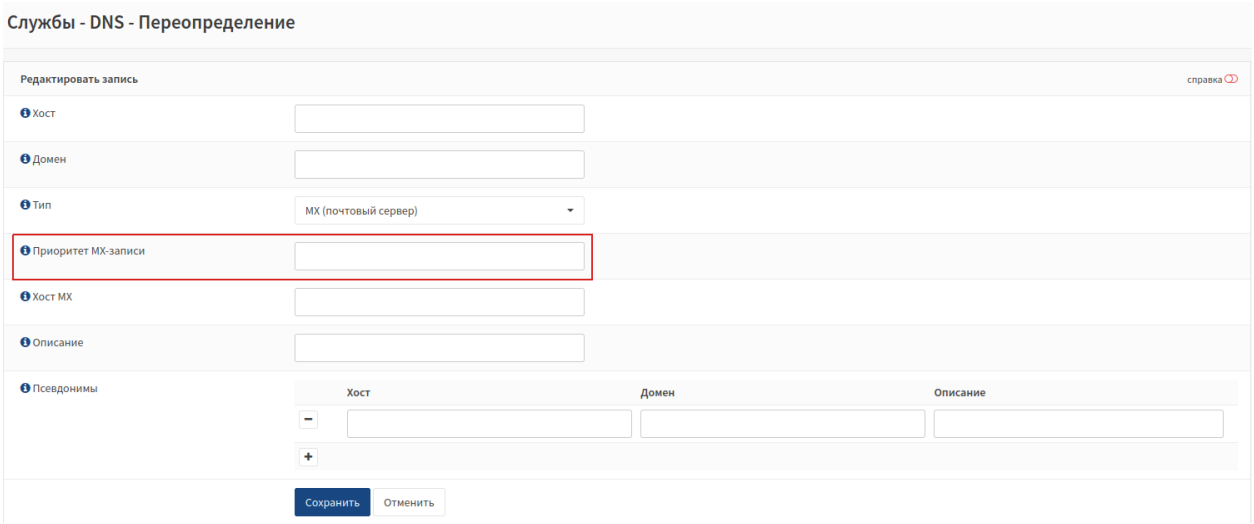


Рис. 864: Установка приоритета MX-записи

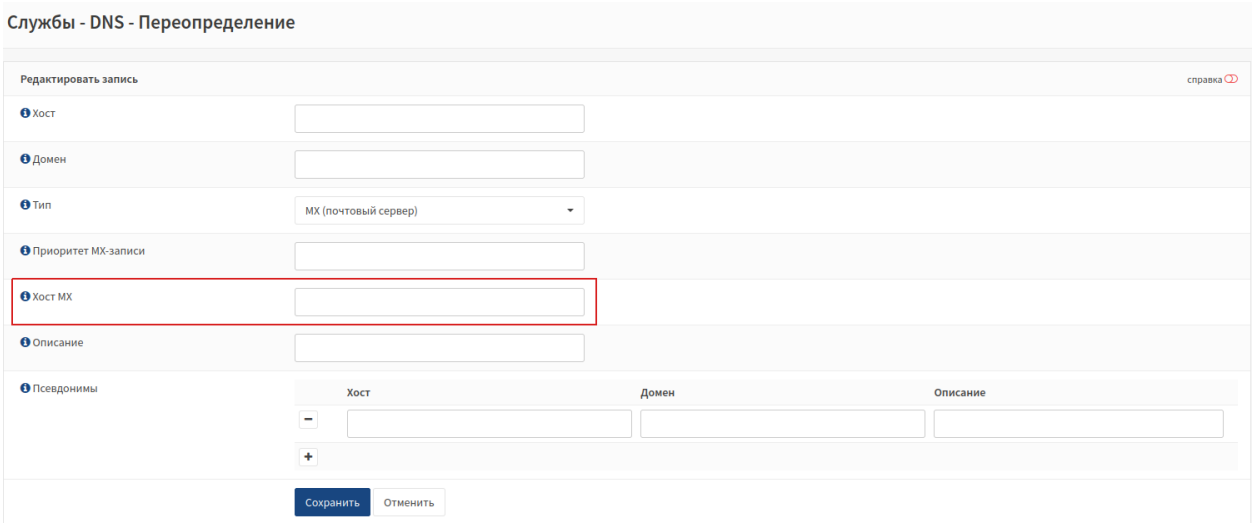


Рис. 865: Установка имени хоста

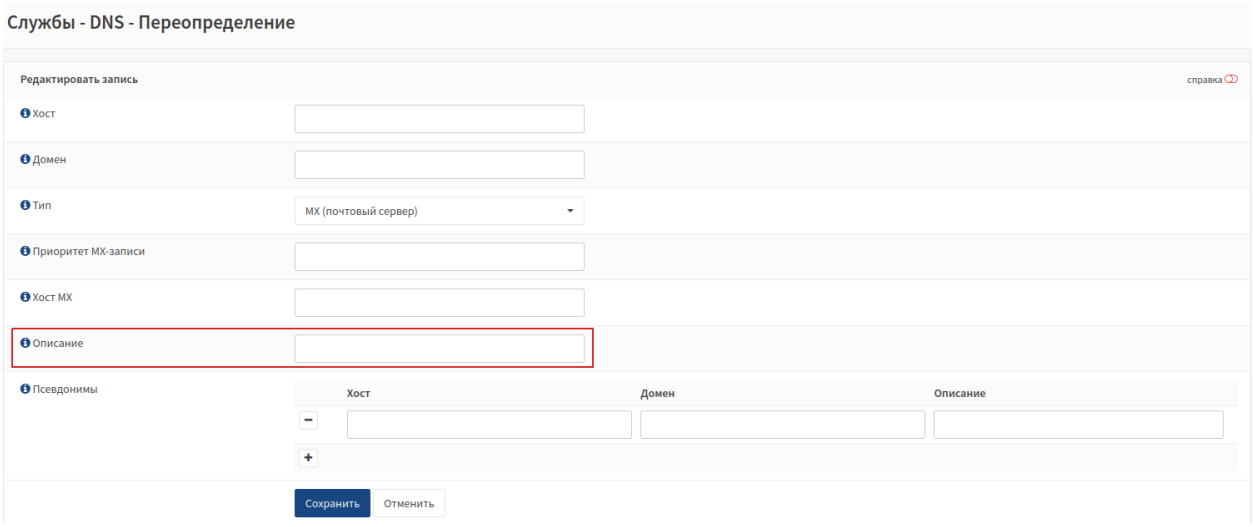


Рис. 866: Описание

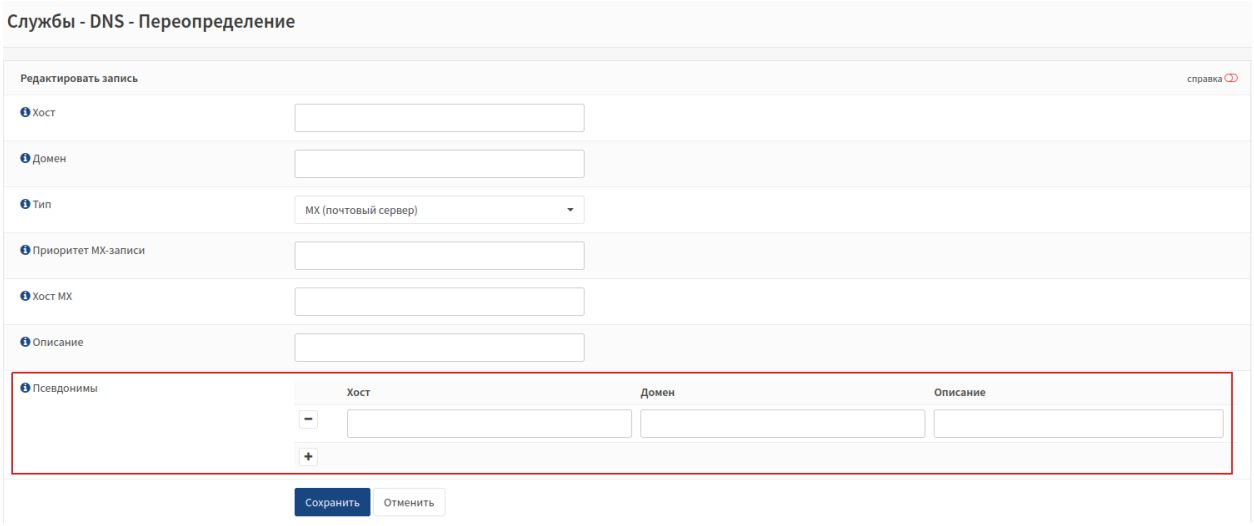


Рис. 867: Ввод псевдонимов

Переопределение домена

Для переопределения домена необходимо нажать кнопку  .

В открывшемся окне необходимо:

- в поле **«Домен»** указать домен для переопределения;

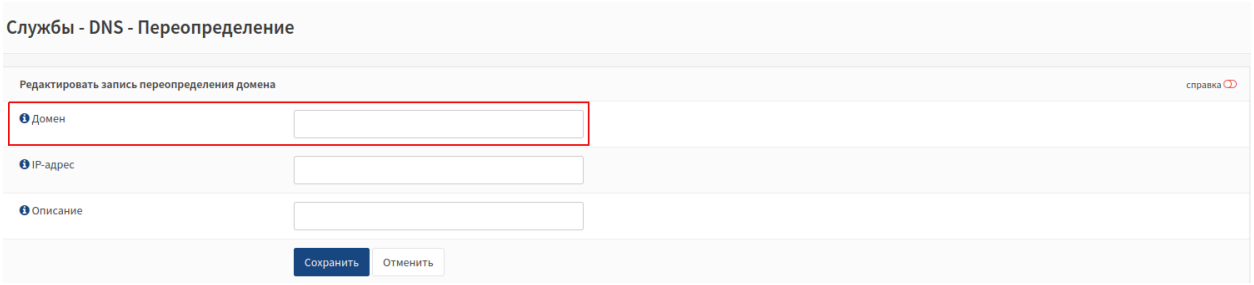


Рис. 868: Установка домена для переопределения

Примечание

Это не должен быть домен верхнего порядка

- в поле **«IP-адрес»** указать IP-адрес полномочного DNS-сервера для этого домена;

Совет

Чтобы использовать для передачи порт не по умолчанию, добавьте символ «@» вместе с номером порта

- в поле **«Описание»** задать краткое описание;

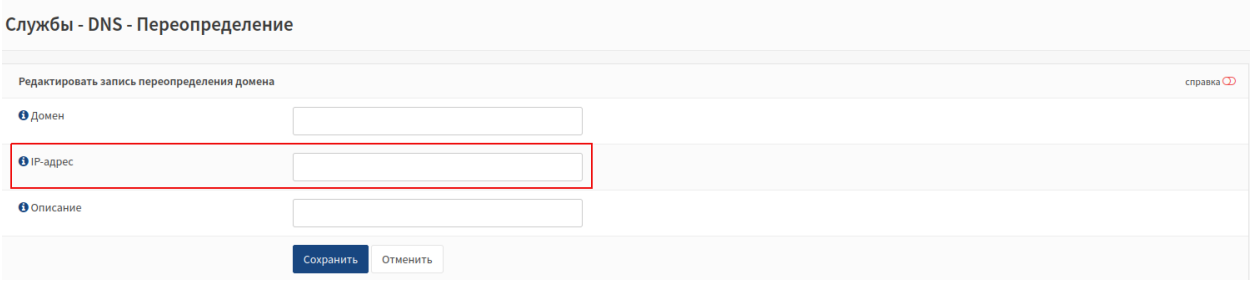


Рис. 869: Выбор IP-адреса

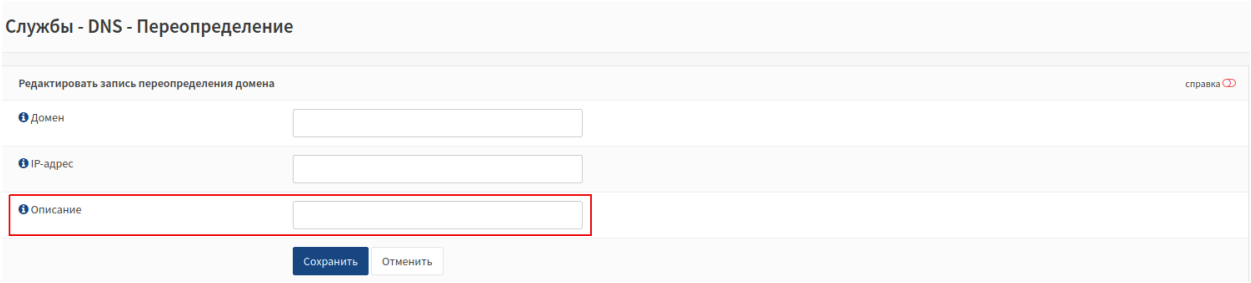


Рис. 870: Описание

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

Дополнительно

Для выполнения настроек необходимо:

- в поле **«Скройте Идентификационные данные»** установить переключатель в случае необходимости отклонять запросы id.server и hostname.bind;
- в поле **«Версия скрытия»** установить переключатель в случае необходимости отклонять запросы version.serve и version.bind;
- в поле **«Поддержка предварительной выборки»** установить переключатель когда элементы кэшей сообщений выбраны заранее до того, как они истекут, чтобы помочь держать кэш актуальным;

Совет

Когда настройка включена, она может вызвать увеличение трафика DNS примерно на 10% и увеличить нагрузку сервера, но часто запрошенные элементы в кэше не истекают

- в поле **«Поддержка Ключа DNS предварительной выборки»** установить переключатель в случае необходимости уменьшить очередь запросов, но немного больше использует ЦП;

Совет

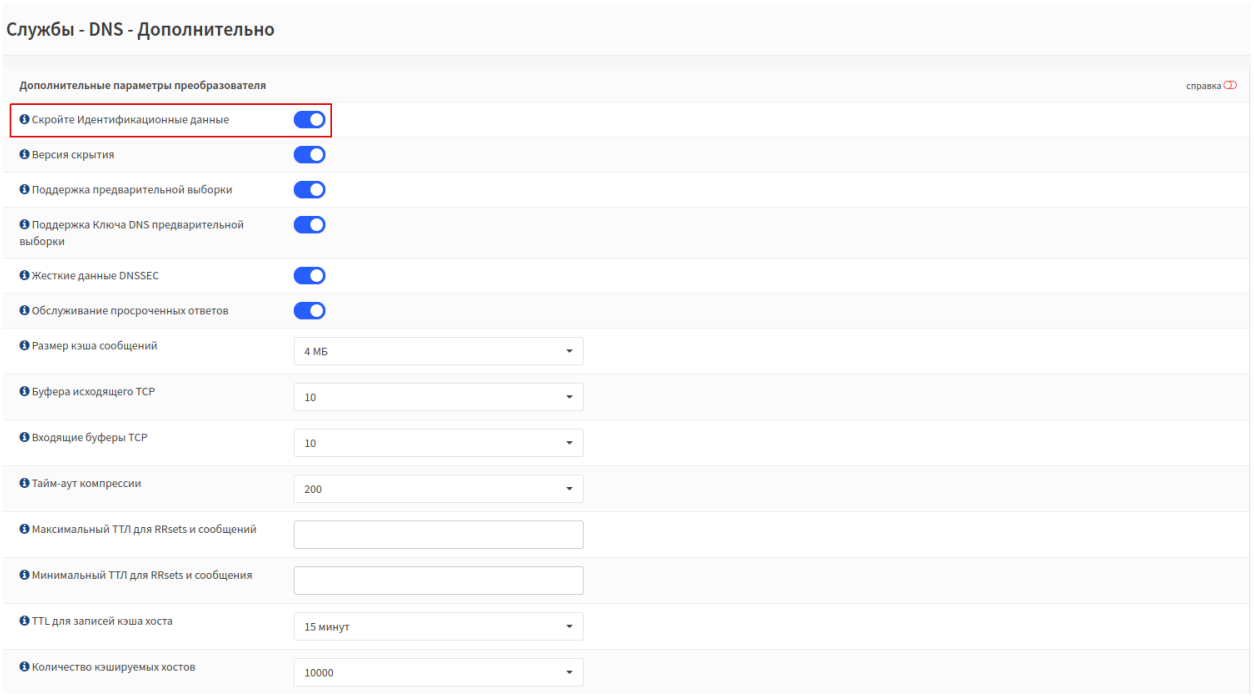


Рис. 871: Отклонение запросов id.server и hostname.bind

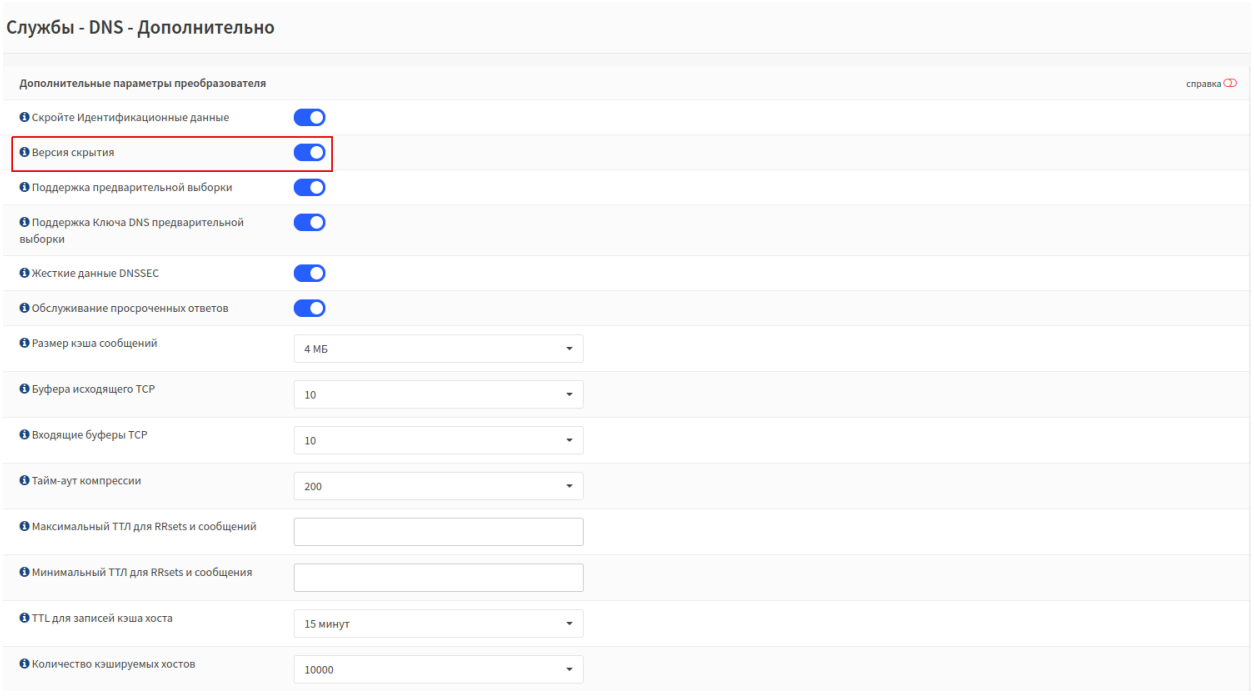


Рис. 872: Отклонение запросов version.serve и version.bind

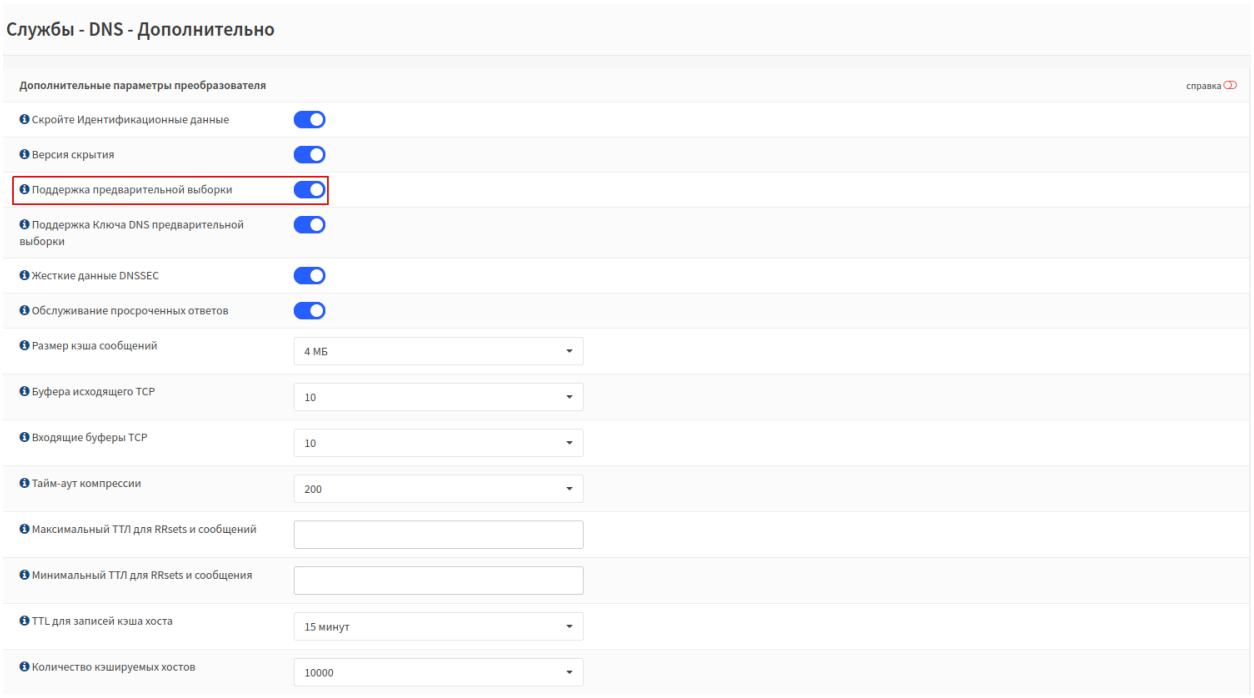


Рис. 873: Поддержка предварительной выборки

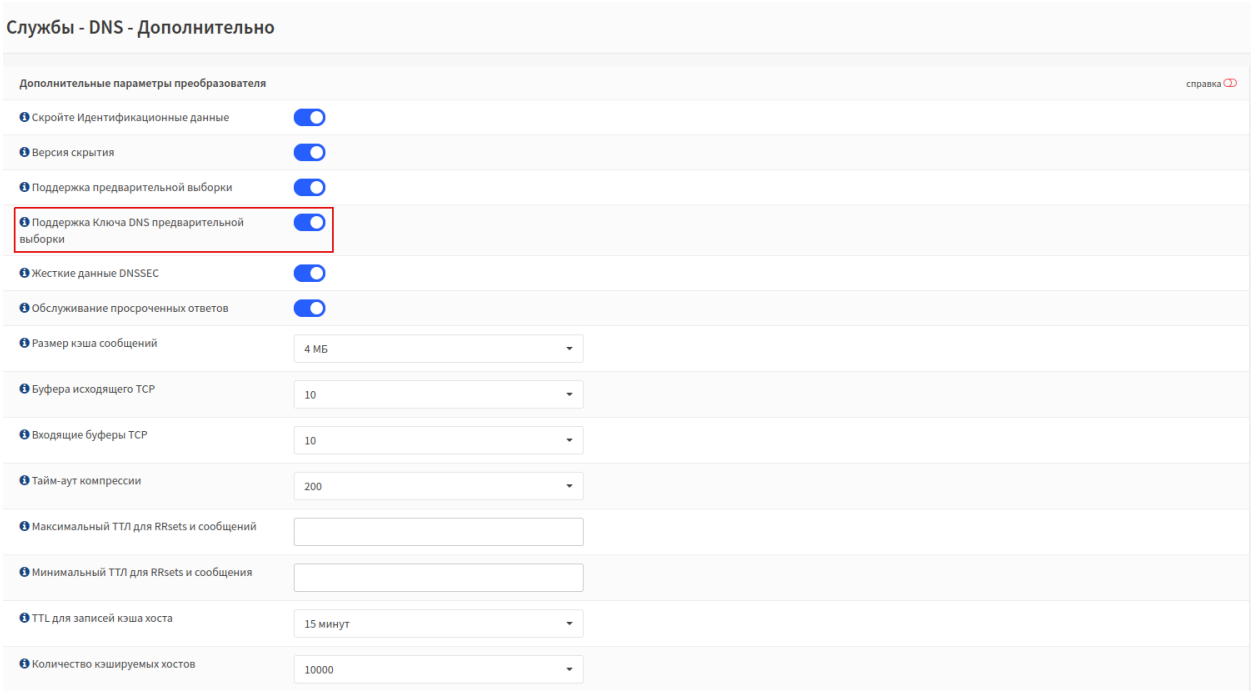


Рис. 874: Поддержка Ключа DNS предварительной выборки

DNSKEY выбираются на упреждение в процессе проверки, когда встречается Подписчик делегирования

- в поле **«Жесткие данные DNSSEC»** установить переключатель в случае необходимости сделать зону DNSSEC безопасной;

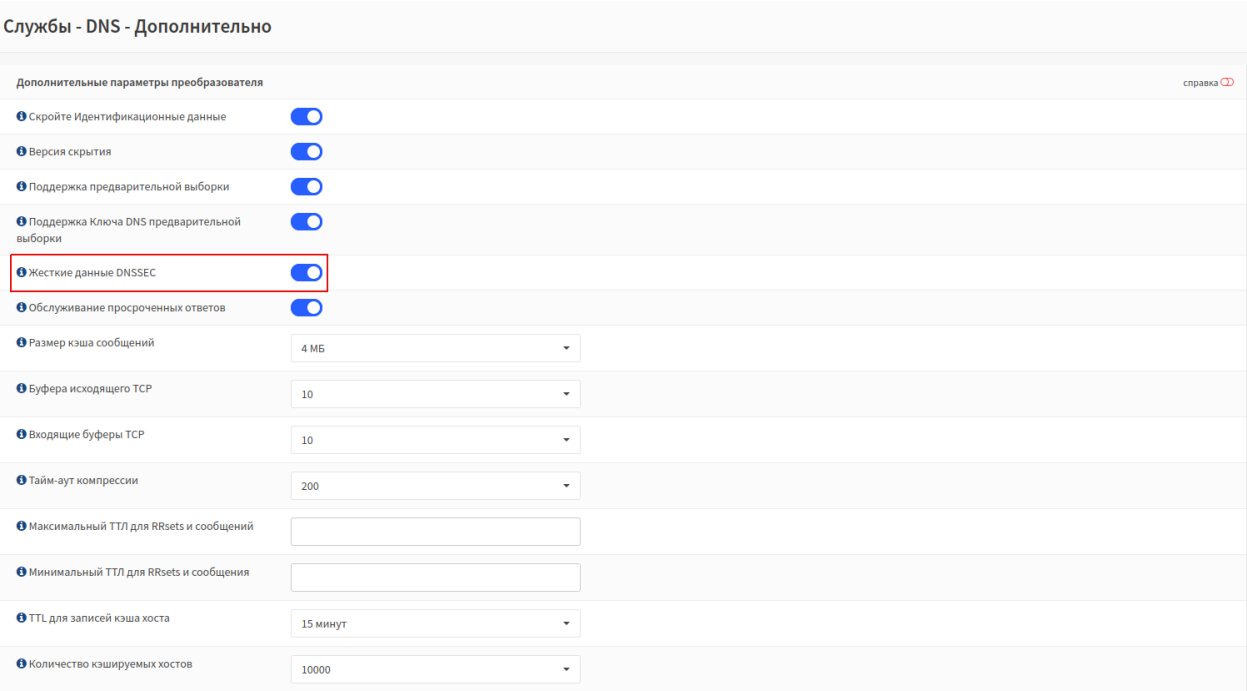


Рис. 875: Жесткие данные DNSSEC

- в поле **«Обслуживание просроченных ответов»** установить переключатель в случае необходимости выдавать просроченные ответы из кэша с TTL 0 без ожидания когда произойдёт реальное разрешение;
- в поле **«Размер кэша сообщений»** установить размер кэша сообщений;

Совет

Кэш сообщений хранит DNS rcodes и статусы проверки. Кэш RRSet будет автоматически настроен на двойную величину. Кэш RRSet содержит фактические данные RR

Совет

Настройки по умолчанию – 4 мегабайта

- в поле **«Буфера исходящего TCP»** установить количество буферов исходящего TCP для распределения потока согласно условиям;

Совет

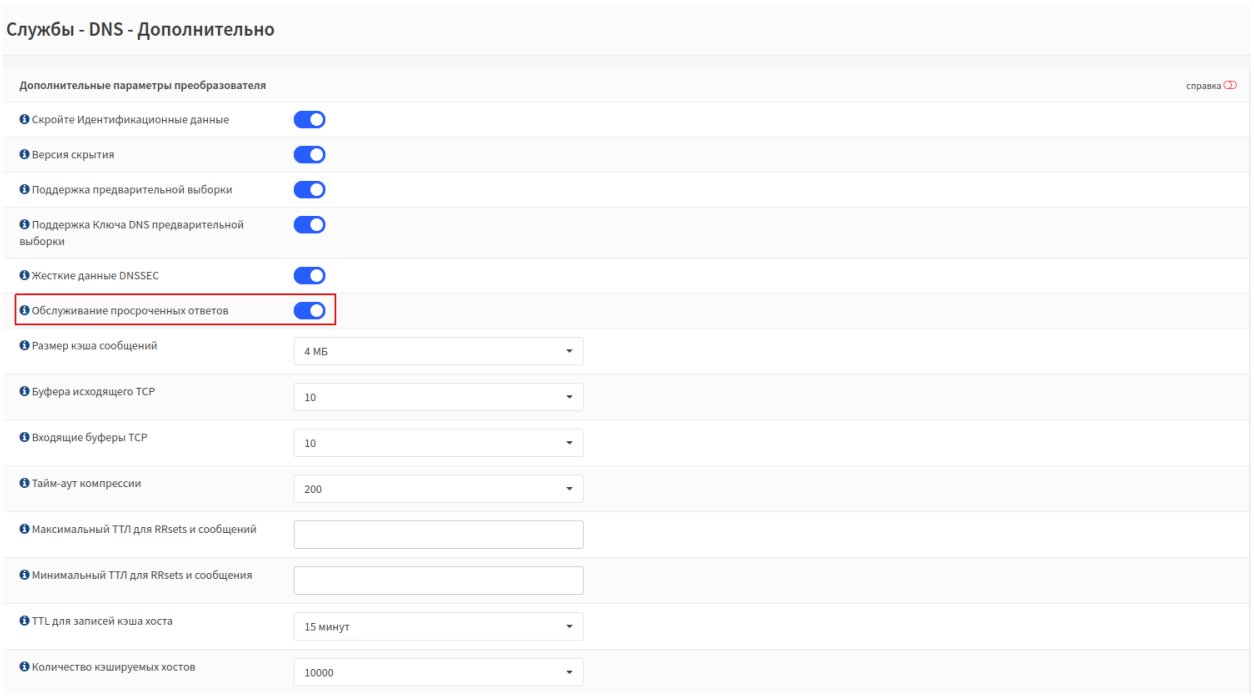


Рис. 876: Обслуживание просроченных ответов

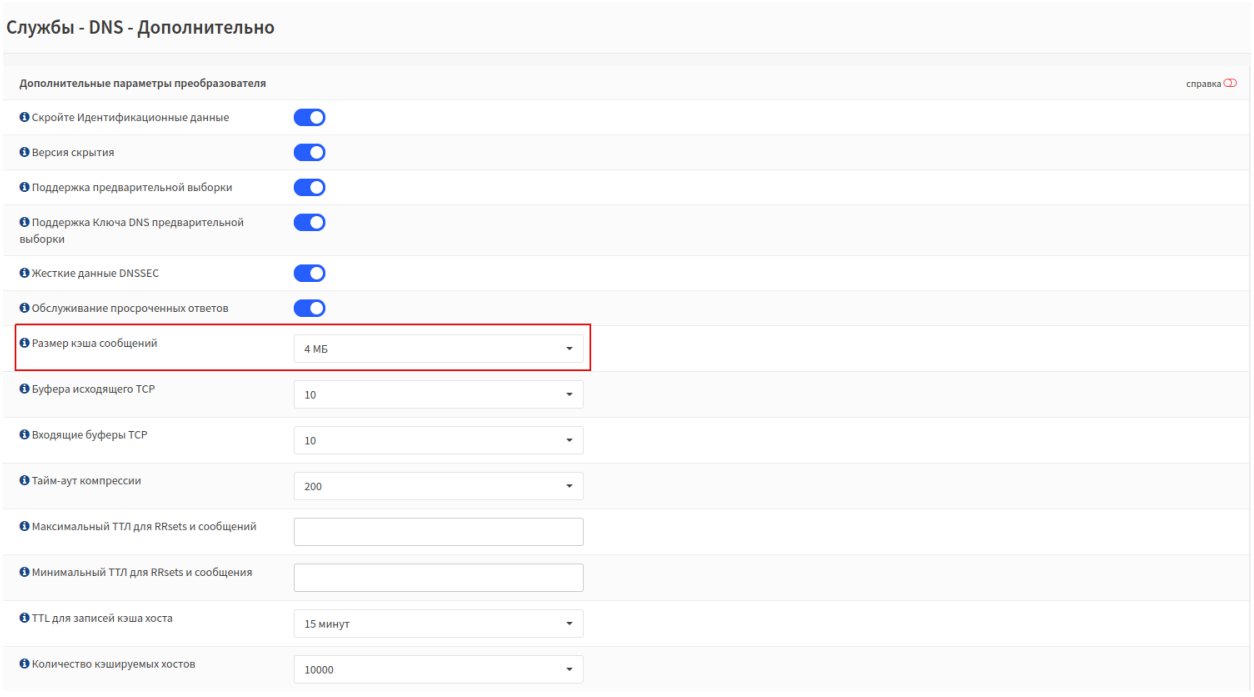


Рис. 877: Установка размера кэша сообщений

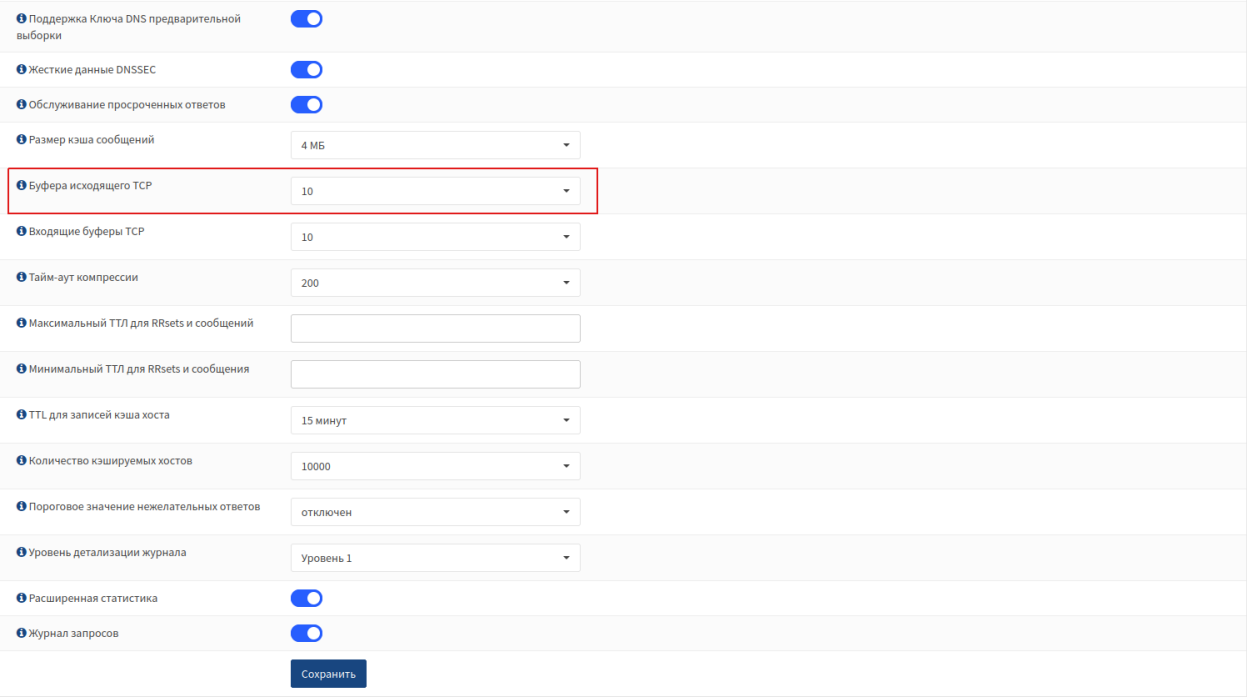


Рис. 878: Установка буферов исходящего TCP

Значение по умолчанию – 10

Совет

Если выбрано 0, то TCP-зарпросы к полномочным серверам производятся

- в поле **«Входящие буферы TCP»** установить количество буферов входящего TCP для распределения потока согласно условиям;

Совет

Значение по умолчанию – 10

Совет

Если выбрано 0, то TCP-запросы от клиентов

- в поле **«Тайм-аут компрессии»** установить значение тайм-аута, когда сервер очень занят;

Совет

Защищает от отказа в обслуживания с помощью медленных запросов или запросов с высоким рейтингом

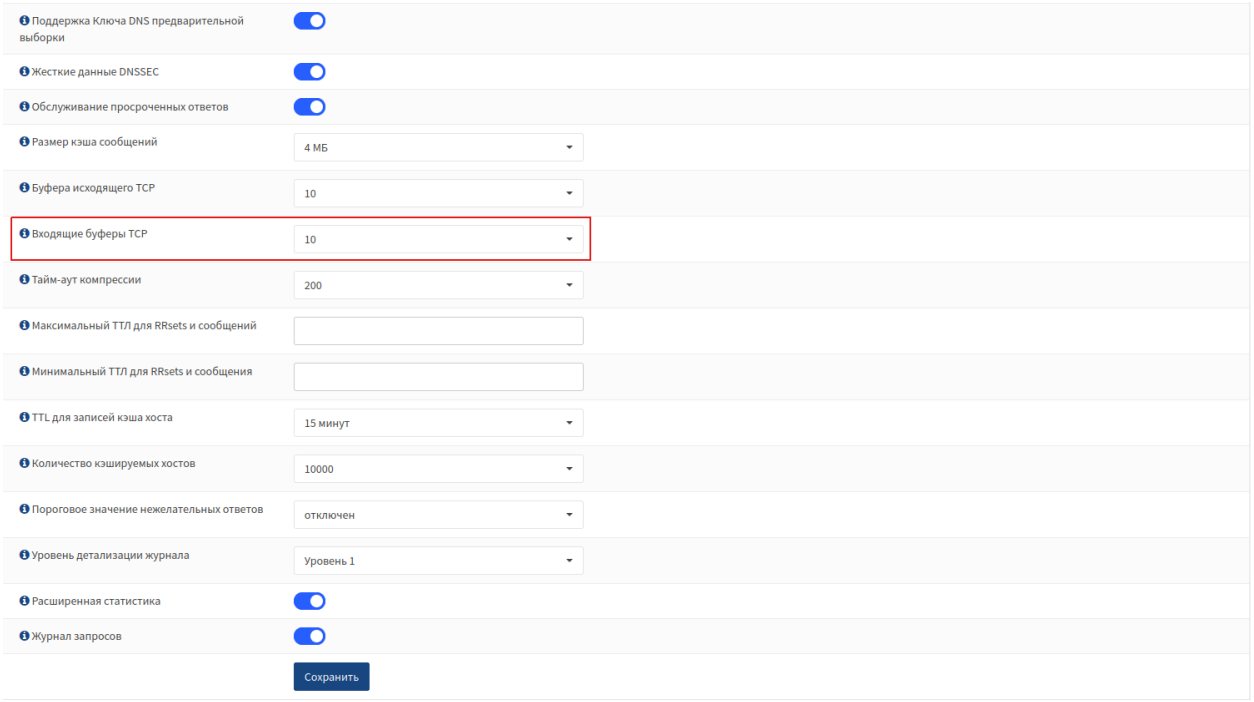


Рис. 879: Установка буферов входящего TCP

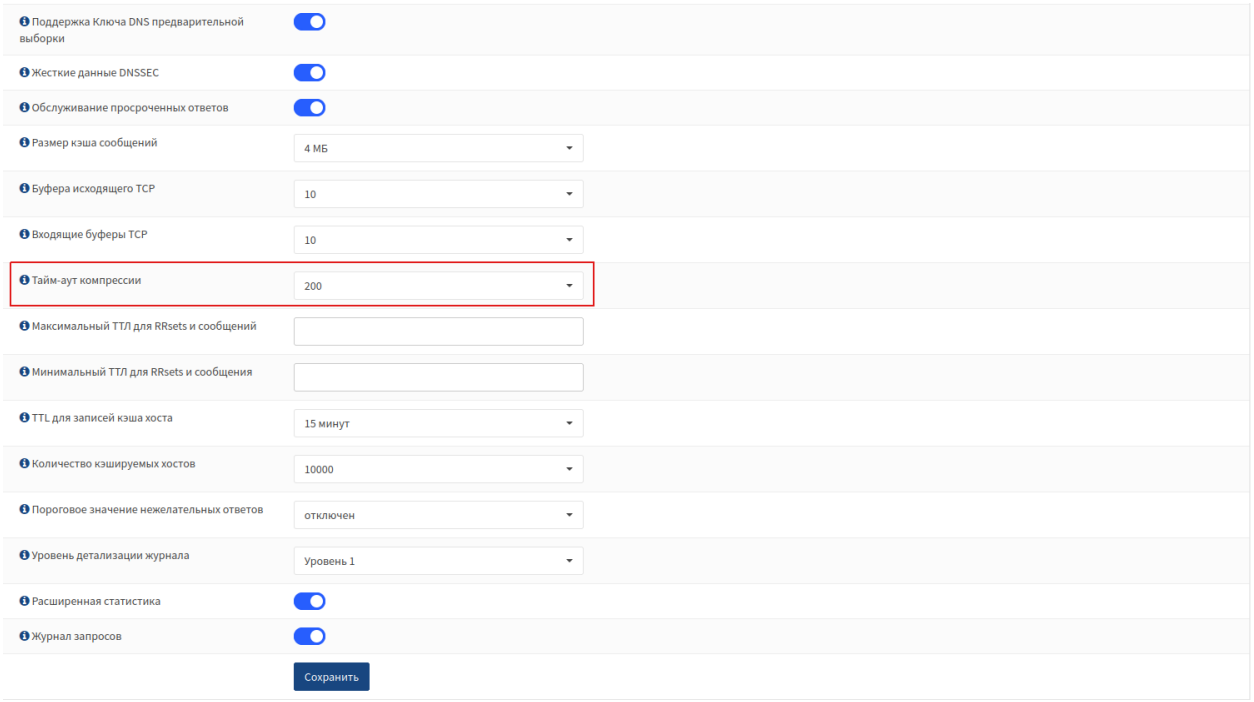


Рис. 880: Установка тайм-аута

Совет

Значение по умолчанию 200 миллисекунд

- в поле **«Максимальный TTЛ для RRsets и сообщений»** сконфигурировать максимальное время жизни для RRsets и сообщений в кэше;

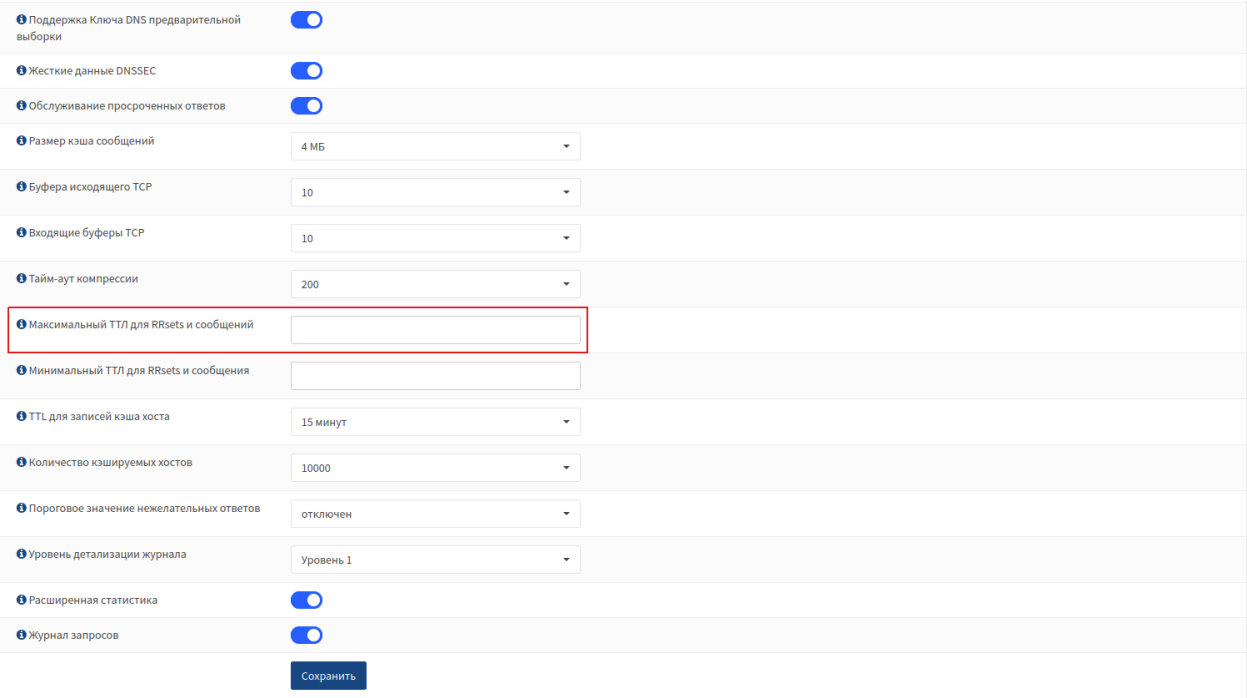


Рис. 881: Установка максимального TTЛ для RRsets и сообщений

Совет

По умолчанию – 86400 секунд (1 день)

Совет

Когда внутренний TTL истекает, элемент кэша тоже истекает

Совет

Настройка может использоваться, чтобы заставить разрешатель запрашивать данные чаще и не доверять (очень большим) значениям

- в поле **«Минимальный TTЛ для RRsets и сообщений»** сконфигурировать минимальное время жизни для RRsets и сообщений в кэше;

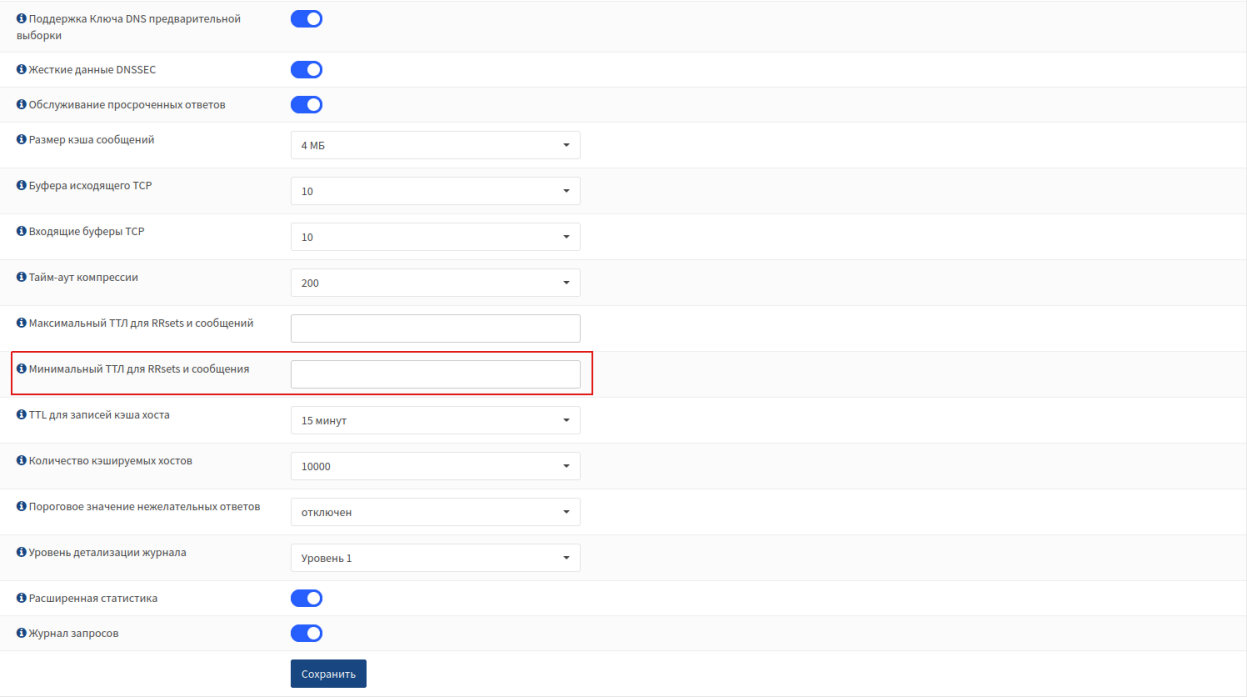


Рис. 882: Установка минимального TTЛ для RRsets и сообщений

Совет

По умолчанию – 0 секунд

Совет

Если включается минимальное значение, данные кэшируются на дольше, чем планирует владелец домена, и, таким образом, совершается меньше запросов для поиска данных

Совет

Значение 0 гарантирует, что в кэше имеются данные, запланированные владельцем домена

Совет

Высокие значения могут привести к проблемам, поскольку данные в кэше могут больше не соответствовать фактическим данным

- в поле **«TTL для записей кэша хоста»** установить время жизни для записей в кэше хоста;

Совет

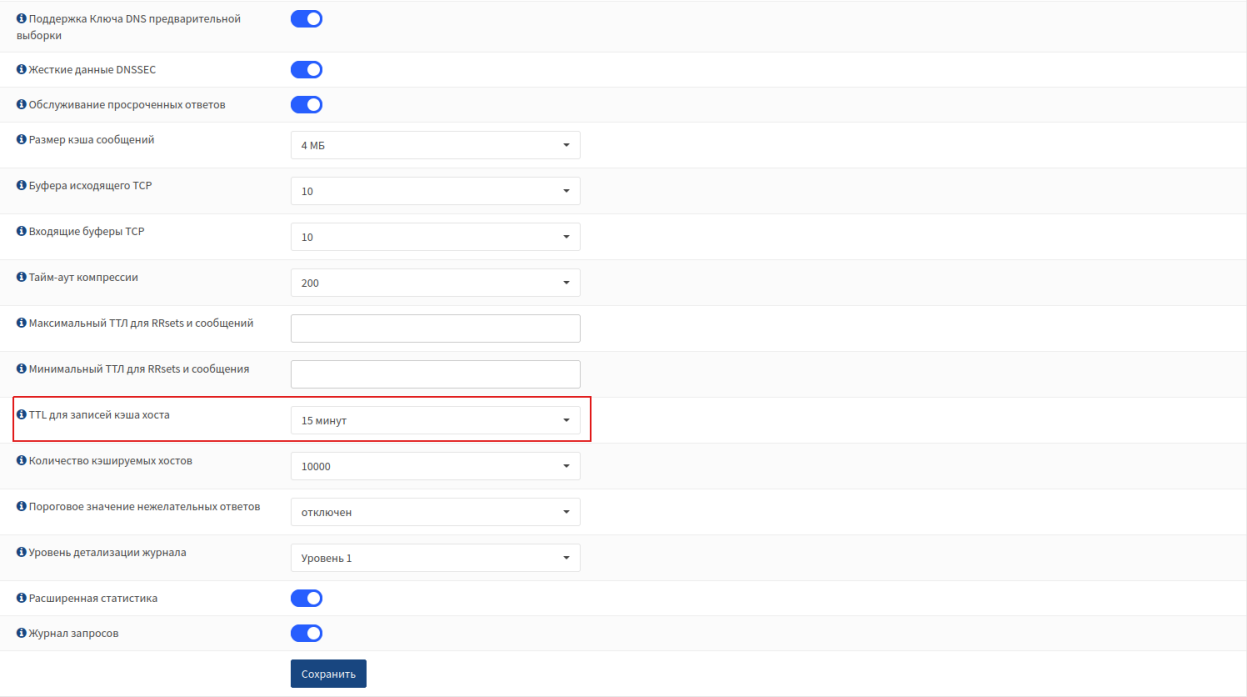


Рис. 883: TTL для записей кэша хоста

Кэш хоста содержит двустороннее время прохождения пакета и информацию о поддержке EDNS

Совет

Значение по умолчанию составляет 15 минут

- в поле **«Количество кэшируемых хостов»** установить количество хостов, для которых информация кэширована;

Совет

Значение по умолчанию — 10000

- в поле **«Пороговое значение нежелательных ответов»** установить значение, при котором общее количество нежелательных ответов продолжают отслеживаться в каждом потоке;

Совет

Когда оно доходит до порога, принимаются защитные меры, и в журнал заносится предупреждение

Совет

Это защитное поведение служит для очистки RRSet и кэшей сообщений

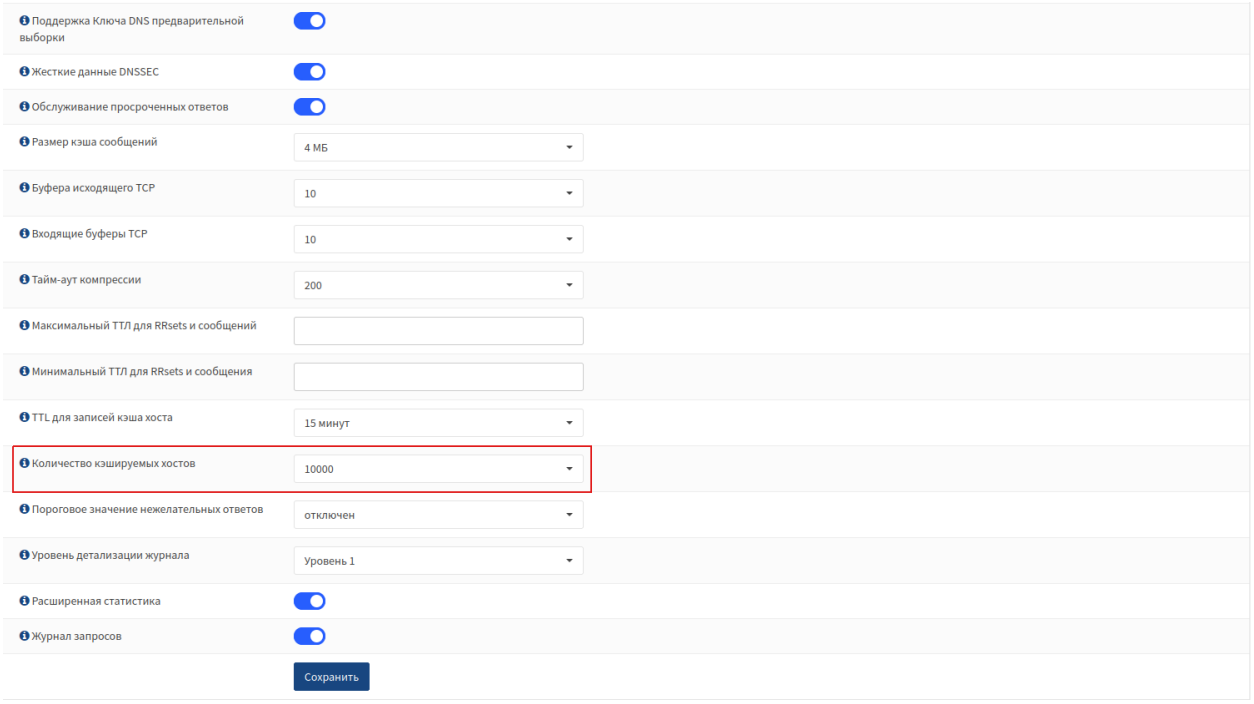


Рис. 884: Количество кэшируемых хостов

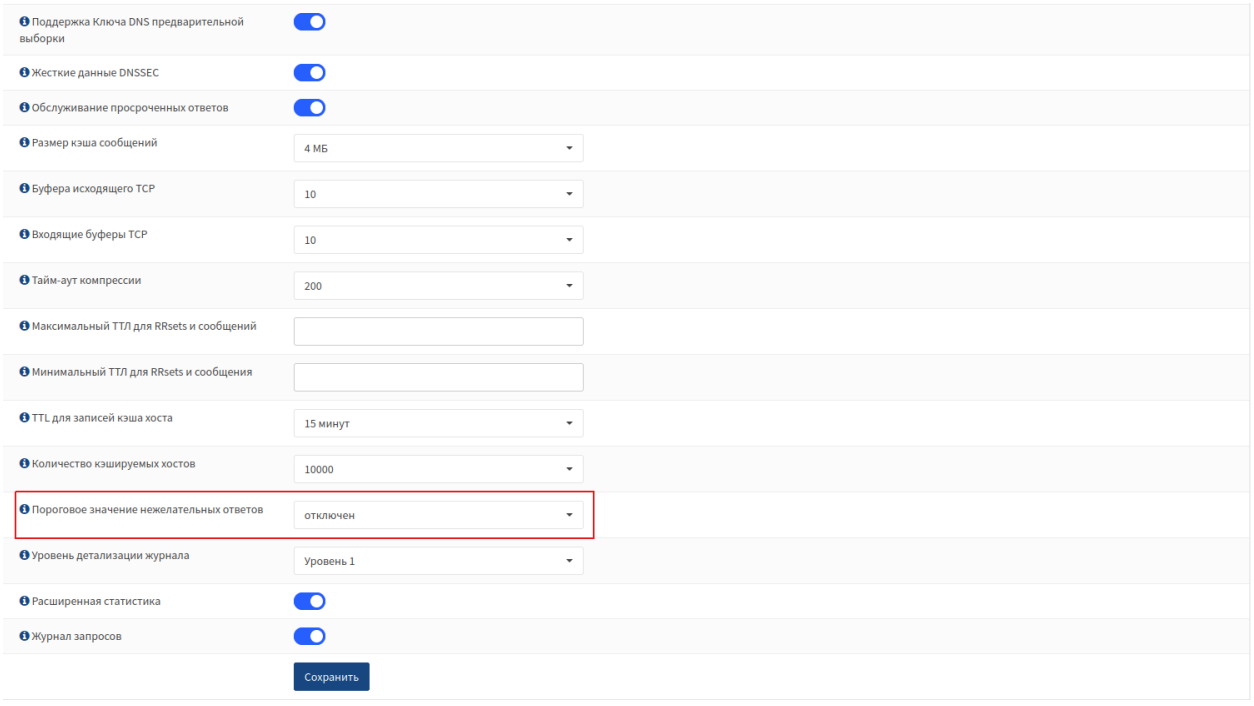


Рис. 885: Пороговое значение нежелательных ответов

Совет

По умолчанию отключён, но если включен, предлагается значение в 10 миллионов

- в поле **«Уровень детализации журнала»** из выпадающего списка выбрать уровень детализации журнала;

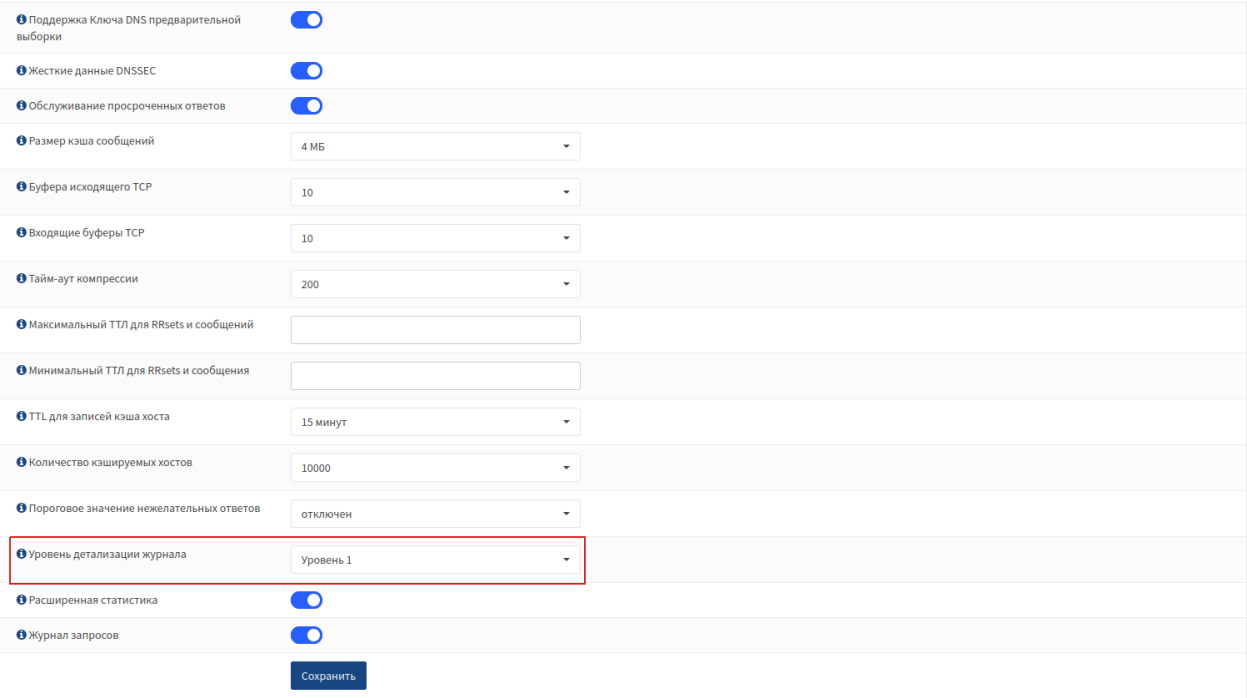


Рис. 886: Уровень детализации журнала

Совет

Уровень 0 означает отсутствие многословия, только ошибки

Совет

Уровень 1 дает оперативную информацию

Совет

Уровень 2 дает подробную оперативную информацию

Совет

Уровень 3 предоставляет информацию об уровне запроса, выводимую для каждого запроса

Совет

Уровень 4 дает информацию об уровне алгоритма

Совет

Уровень 5 регистрирует идентификацию клиента для промахов кеша

Совет

По умолчанию уровень 1

- в поле **«Расширенная статистика»** установить переключатель в случае необходимости распечатывать расширенную статистику;

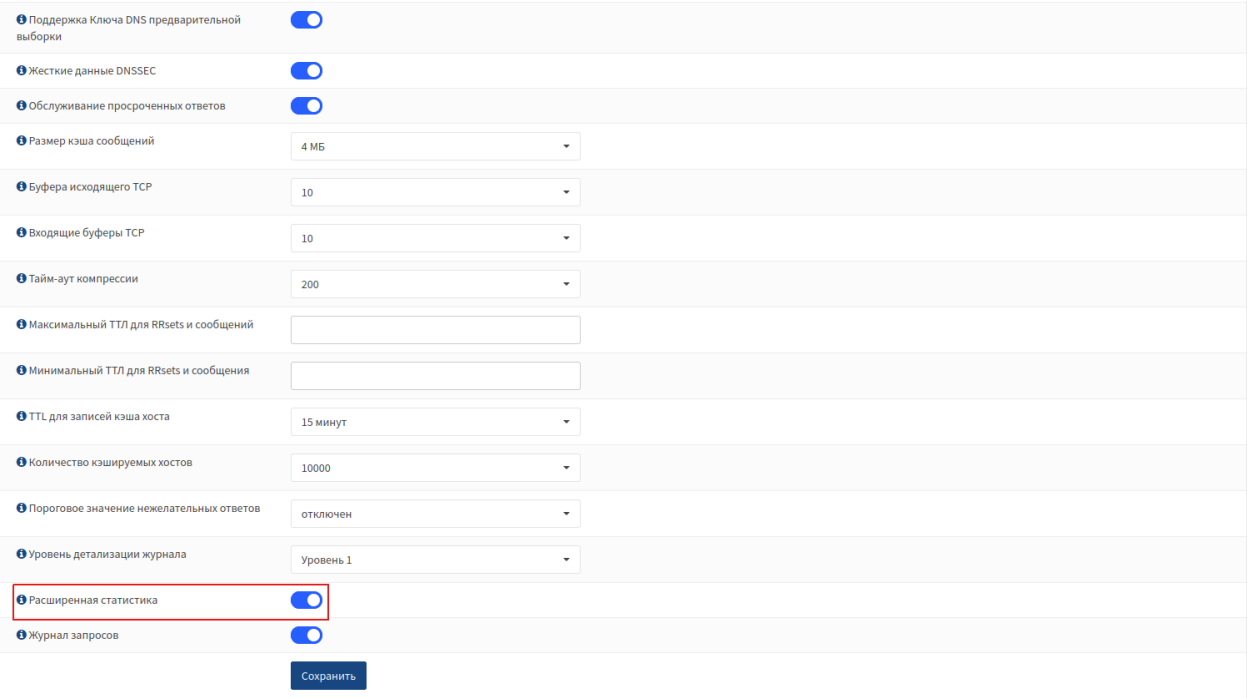


Рис. 887: Расширенная статистика

- в поле **«Журнал запросов»** установить переключатель в случае необходимости печатать одну строку для каждого запроса в журнал с отметкой времени журнала и IP-адресом, именем, типом и классом;

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

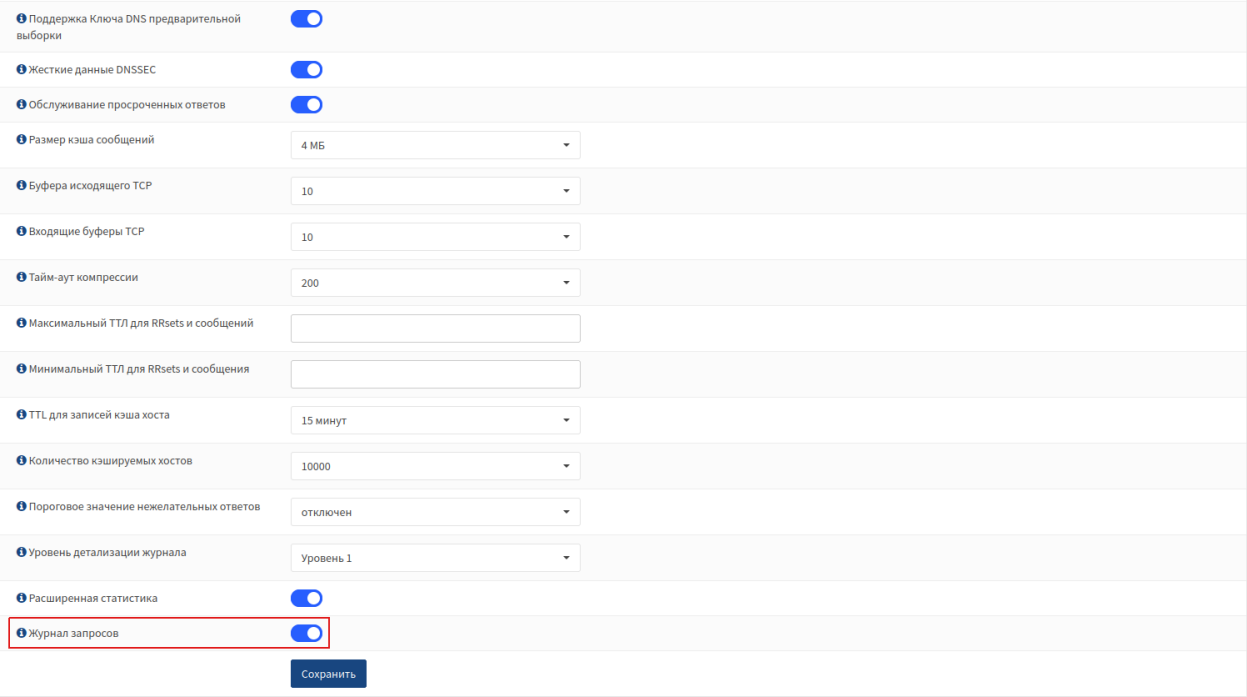


Рис. 888: Журнал запросов

Списки доступа

Таблица списков доступа представлена на рисунке.

Для добавления нового объекта в таблицу необходимо нажать кнопку 

.

В открывшемся окне необходимо:

- в поле **«Имя списка доступа»** указать имя списка доступа;
- в поле **«Действие»** выбрать из выпадающего списка действие, производимое с DNS-запросами;

Список направлений движения пакета соответствует таблице.

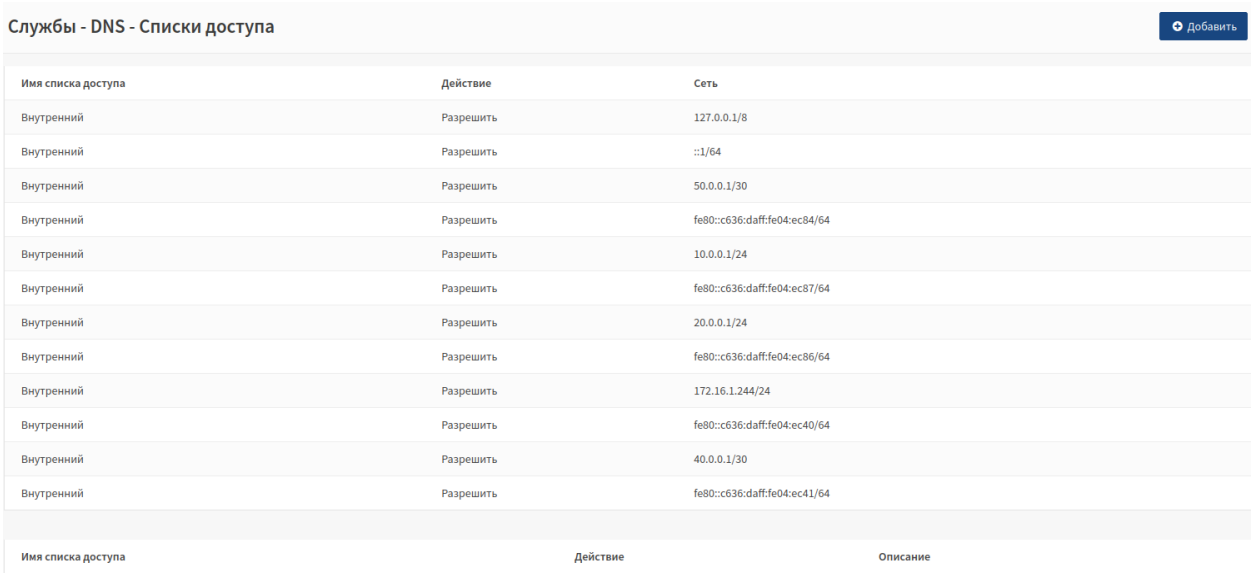


Рис. 889: Списки доступа

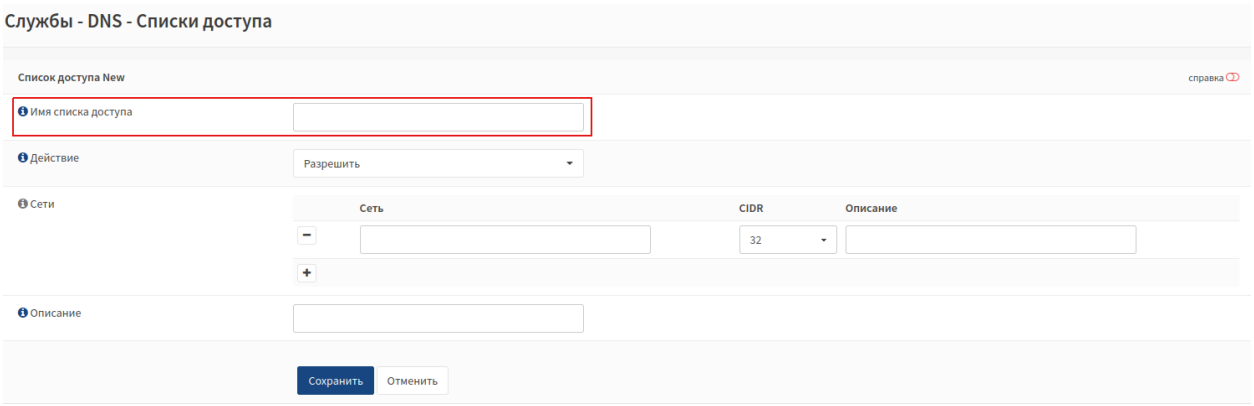


Рис. 890: Ввод имени списка доступа

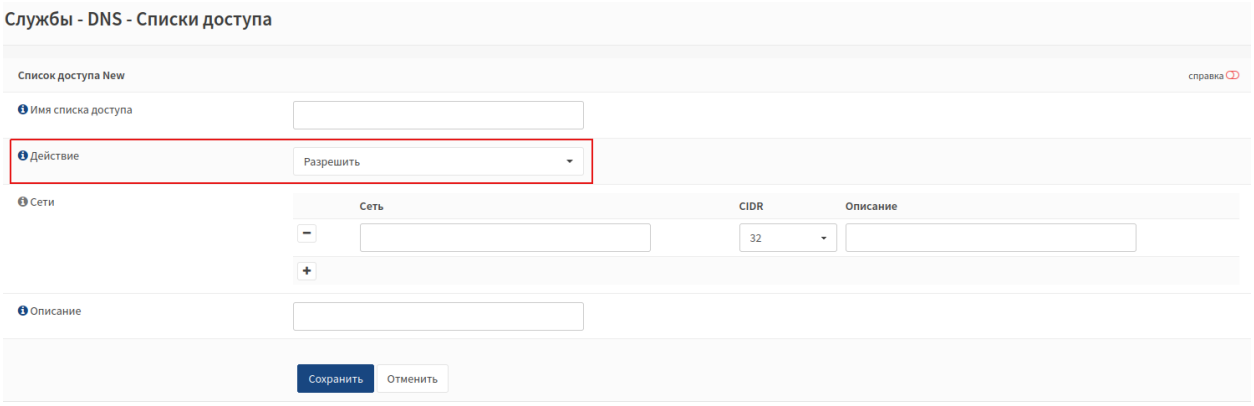


Рис. 891: Выбор действия

Таблица 164: Действие, производимое с DNS-запросами

Действие	Примечание
Блокировать	Это действие запрещает запросы от хостов, указанных в блоке сетевых адресов ниже
Запретить	это действие также запрещает запросы от хостов, указанных в блоке сетевых адресов ниже, но отправляет обратно клиенту сообщение об ошибке DNS rcode REFUSED
Разрешить	Это действие разрешает запросы от хостов, указанных в блоке сетевых адресов ниже
Разрешить отслеживание	Это действие разрешает рекурсивный и нерекурсивный доступ из хостов в определенном ниже блоке сетевых адресов, и используется для отслеживания кэша (в идеале должно быть настроено только для административного хоста)
Запретить нелокальные	Разрешать только авторитетные запросы локальных данных от хостов в пределах сетевого блока, определенного ниже. Запрещенные сообщения удаляются
Отказаться от нелокальных	Разрешать только авторитетные запросы локальных данных от хостов в пределах сетевого блока, определенного ниже. Отправляет сообщение об ошибке DNS rcode REFUSED обратно клиенту для запрещенных сообщений

- в поле **«Сети»** указать адреса необходимых сетей;

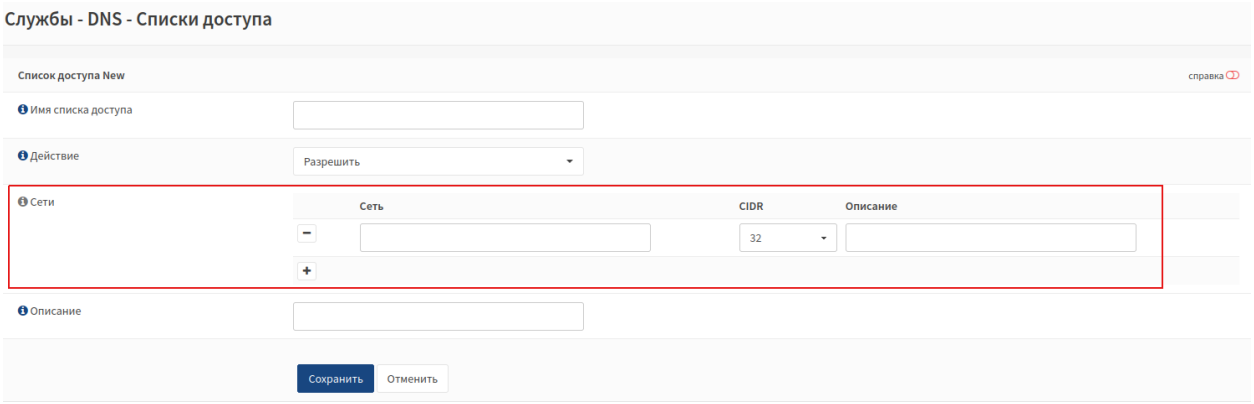


Рис. 892: Добавление сетей

- в поле **«Описание»** указать краткое описание ссылки;

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

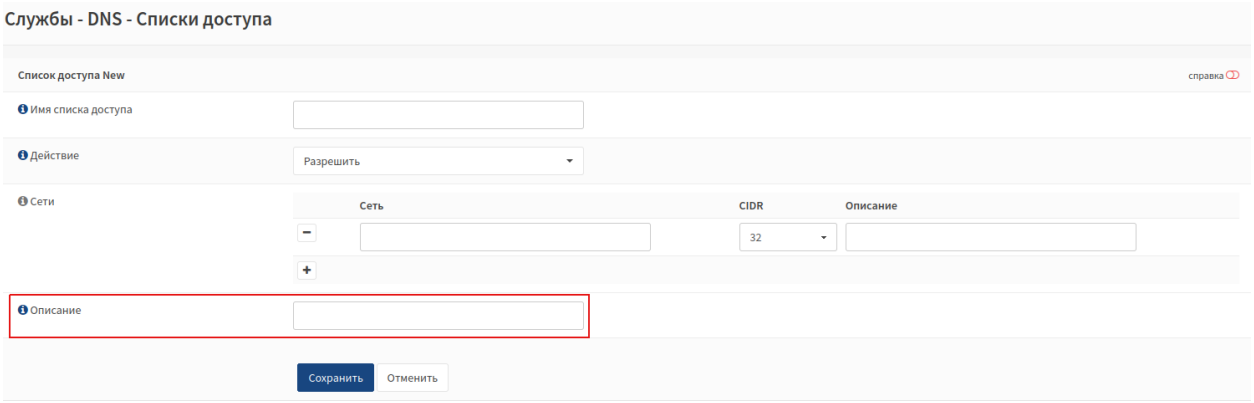


Рис. 893: Описание

Черный список

Для настройки черного списка необходимо:

- в поле **«Включить»** установить переключатель в случае необходимости использования черных списков DNS;

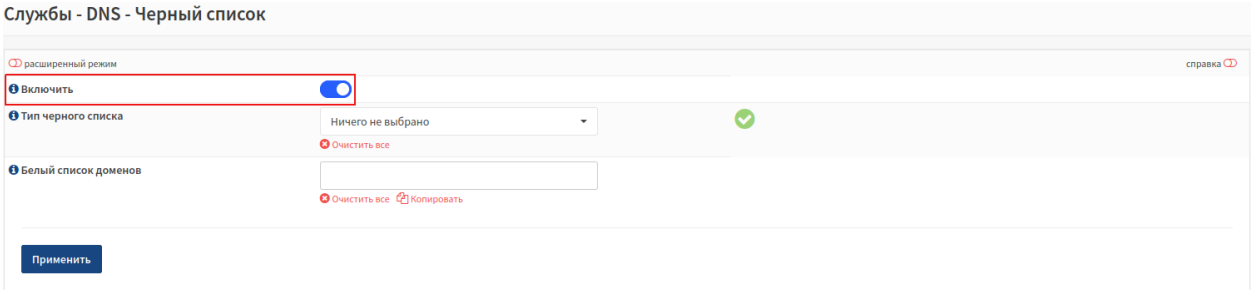


Рис. 894: Включение черных списков DNS

- в поле **«Тип черного списка»** выбрать из выпадающего списка необходимый тип черного списка;

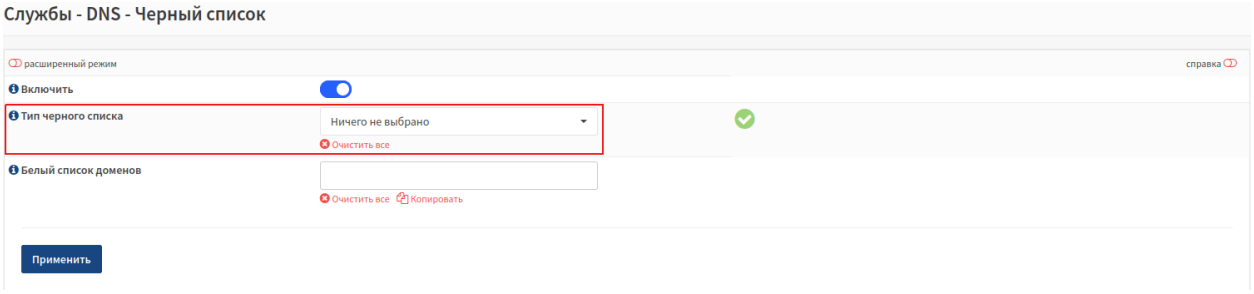


Рис. 895: Выбор типа черного списка

- в поле **«Белый список доменов»** указать список доменов для белого списка;

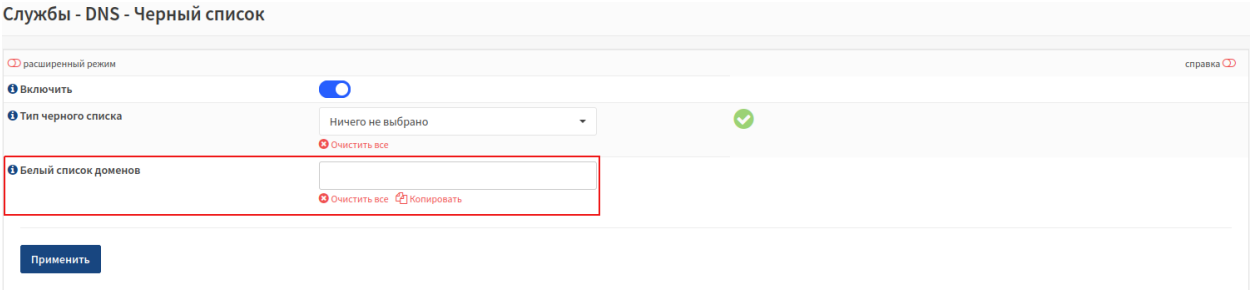


Рис. 896: Установка списка доменов для белого списка

Совет

Вы можете использовать регулярные выражения

Для включения режима расширенных настроек необходимо установить переключатель.

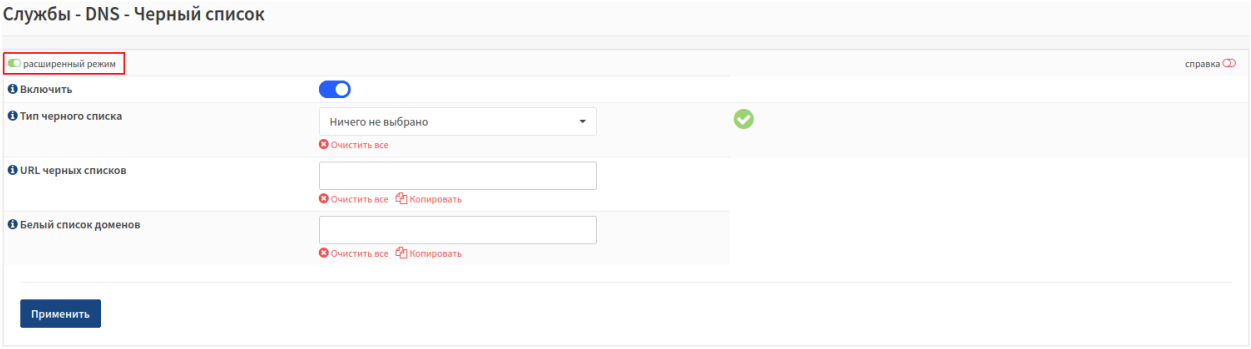


Рис. 897: Включение расширенных настроек

В режиме расширенных настроек необходимо:

- в поле **«URL черных списков»** указать список доменов, откуда будет загружен черный список;

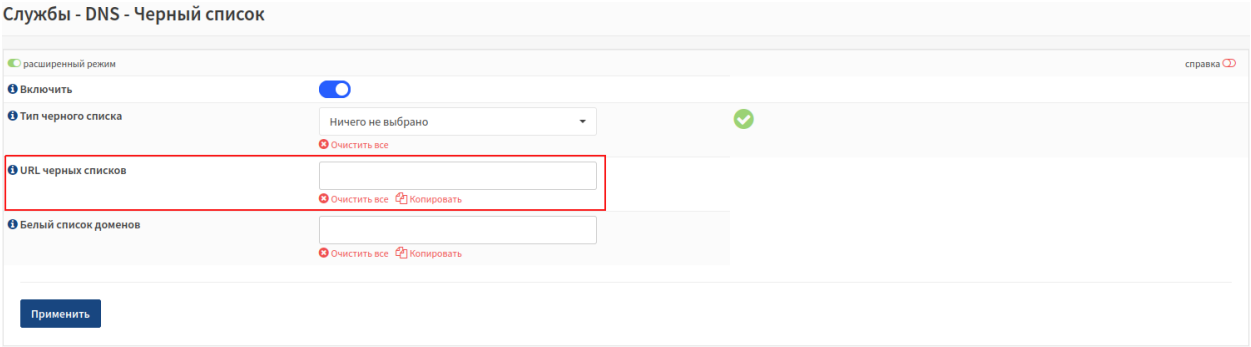


Рис. 898: Установка URL адресов

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

Прочее

Для конфигурации прочих настроек необходимо:

- в поле **«Частные домены»** указать список доменов, которые следует пометить как частные;

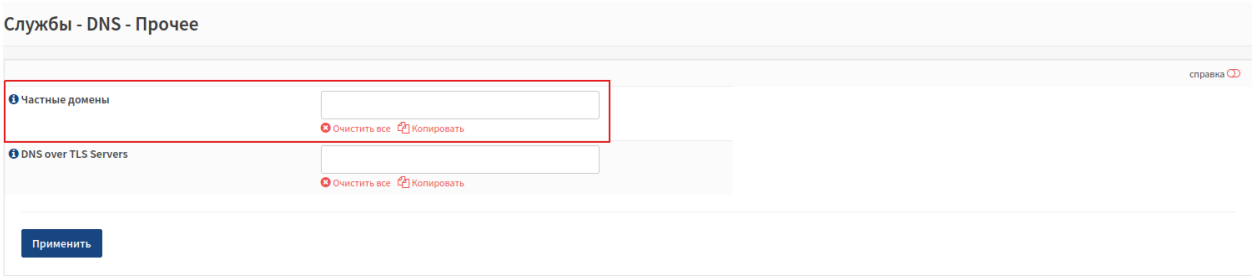


Рис. 899: Установка частных доменов

Совет

Это нужно только для некоторых списков DNSBL, которые разрешаются в частные адреса

- в поле **«DNS over TLS Servers»** указать список DNS-серверов, которые можно использовать для DoT;

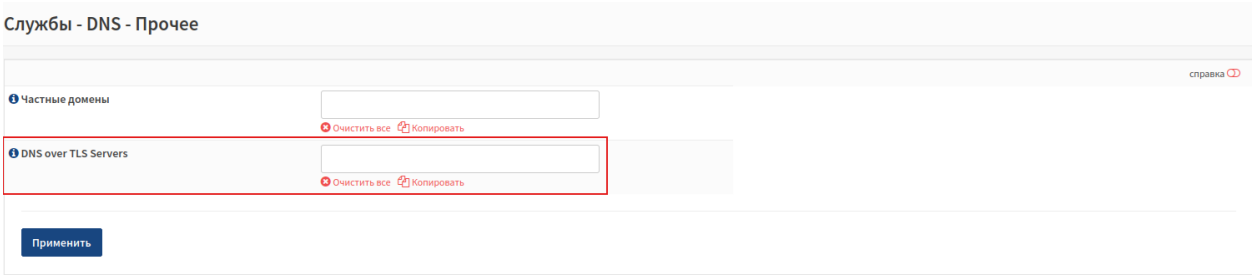


Рис. 900: Ввод списка DNS-серверов для DoT

Совет

Используйте синтаксис ip@port, например, 9.9.9.9@853

Для вступления сконфигурированных настроек в силу необходимо нажать кнопку Применить .

Статистические данные

Вкладка **«Статистические данные»** представлена на рисунке.

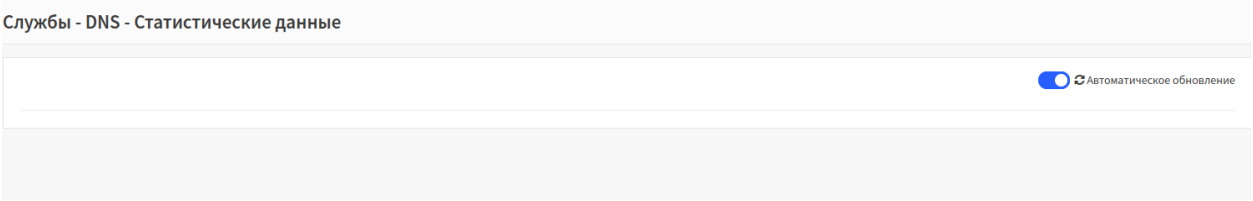
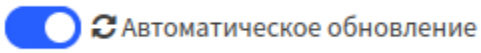


Рис. 901: Статистические данные

Для автоматического обновления статистических данных необходимо установить переключатель 

.

Журнал

Раздел **«Журнал»** содержит журнал системы DNS.

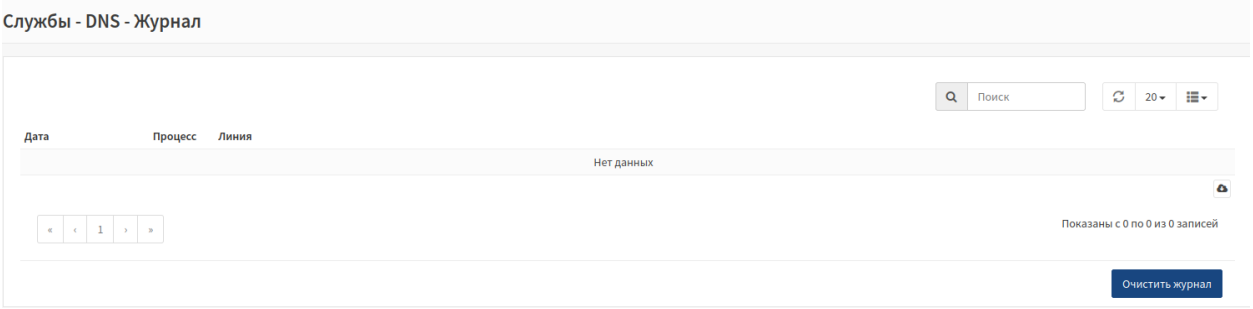


Рис. 902: Журнал системы DNS

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

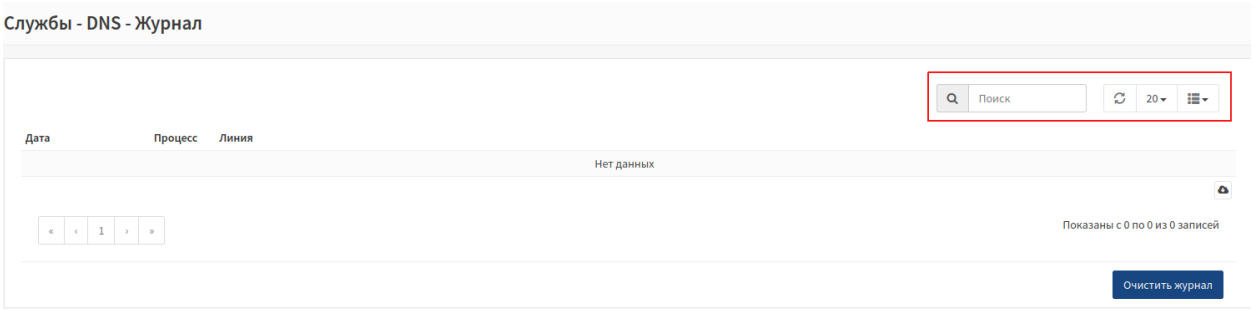


Рис. 903: Фильтры журнала системы DNS

2.7.8.6 Вэб-прокси

Для перехода к настройкам прокси-сервера необходимо:

- нажать на вкладку **«Службы»** - **«Веб-прокси»** - **«Администрирование»**, расположенную в левой части списка объектов управления;

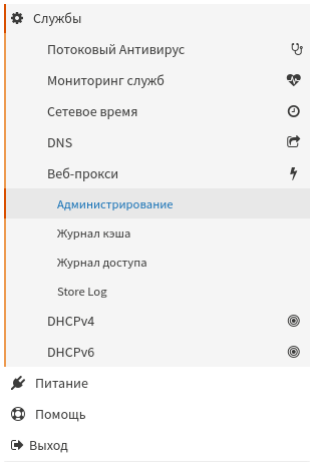


Рис. 904: Переход к настройкам прокси-сервера

Для перехода к просмотру журнала кеша необходимо:

- нажать на вкладку **«Службы»** - **«Веб-прокси»** - **«Журнал кэша»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала доступа необходимо:

- нажать на вкладку **«Службы»** - **«Веб-прокси»** - **«Журнал доступа»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала хранения необходимо:

- нажать на вкладку **«Службы»** - **«Веб-прокси»** - **«Store Log»**, расположенную в левой части списка объектов управления;

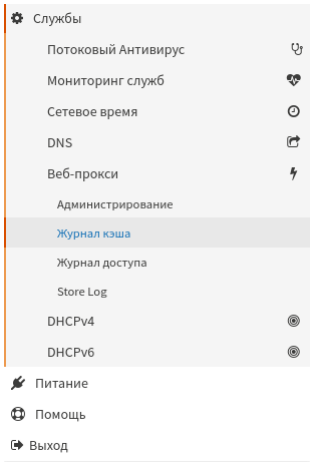


Рис. 905: Переход к просмотру журнала кеша

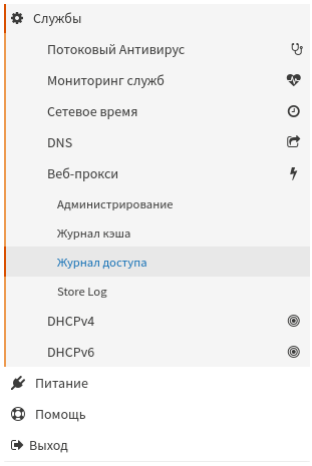


Рис. 906: Переход к просмотру журнала доступа

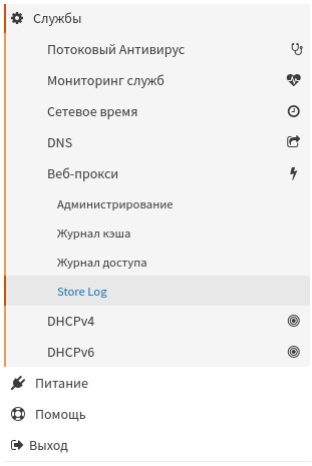


Рис. 907: Переход к просмотру журнала хранения

Администрирование

Основные настройки прокси

Для выполнения основных настроек прокси-сервера необходимо:

- выбрать из выпадающего списка **«Основные настройки прокси»**;

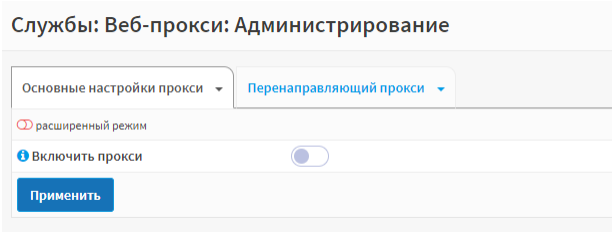


Рис. 908: Переход к основным настройкам прокси-сервера

- в поле **«Включить прокси»** установить переключатель в случае необходимости включения прокси-сервера;

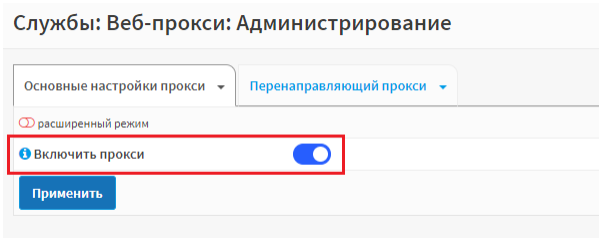


Рис. 909: Включение проки-сервера

- нажать кнопку **«Применить»** 

.

Для включения режима расширенных настроек необходимо установить переключатель.

В режиме расширенных настроек необходимо:

- в поле **«Порт ICP»** указать номер порта, на который Squid будет посылать и принимать ICP-запросы от соседних кэшей;

> **Совет**
>
> Необходимо оставить поле пустым, чтобы отключить эту возможность (по умолчанию)

> **Совет**
>
> Стандартный номер UDP порта — 3130

- в поле **«Включить ведение журнала обращений»** установить переключатель в случае необходимости включить ведение журнала запросов клиентов;

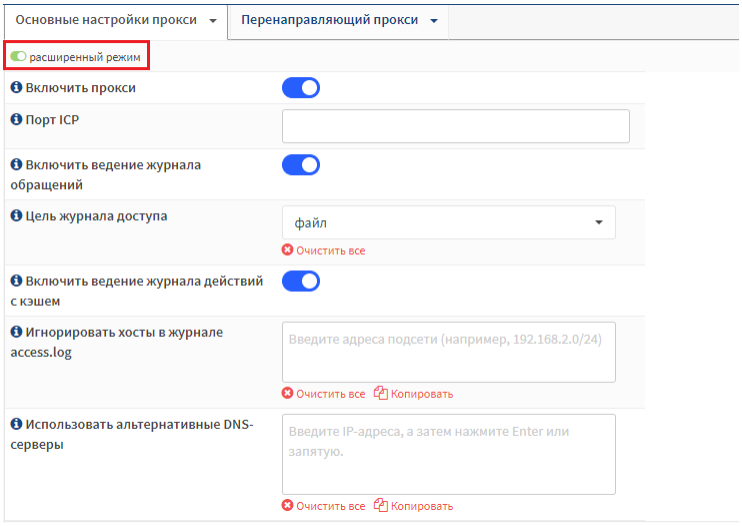


Рис. 910: Включение расширенных настроек

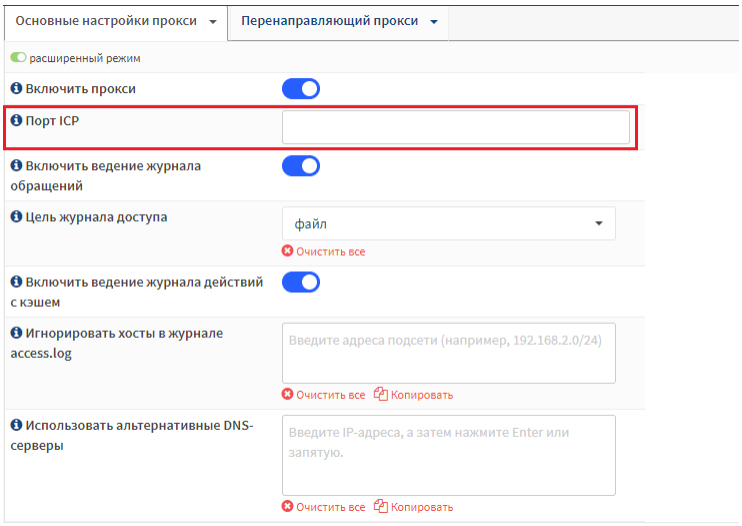


Рис. 911: Порт ICP

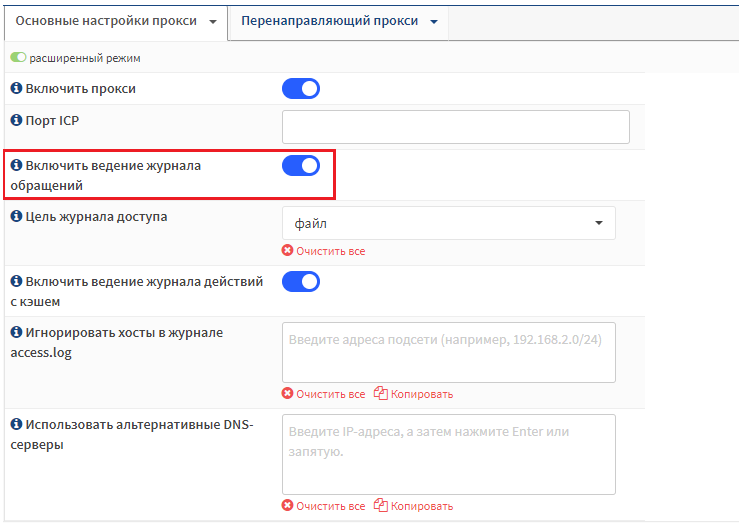


Рис. 912: Включение ведения журнала обращений

- в поле **«Цель журнала доступа»** указать цель, в которую будут отправляться данные журнала;

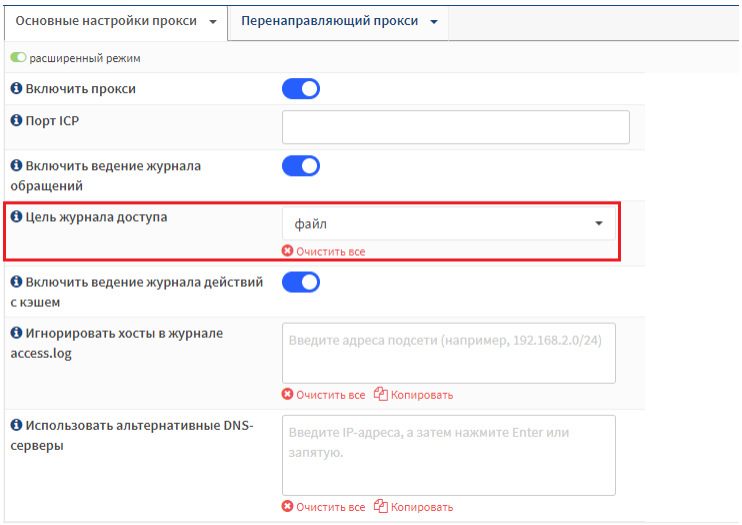


Рис. 913: Цель журнала доступа

Примечание

Когда выбран системный журнал для отправки сообщений информационного уровня, для этих журналов будет использоваться локальная служба

- в поле **«Включить ведение журнала действий с кэшем»** установить переключатель в случае необходимости включить ведение журнала действий с кэшем;
- в поле **«Игнорировать хосты в журнале access.log»** указать подсети/адреса, которые следует игнорировать для access.log;
- в поле **«Использовать альтернативные DNS-серверы»** указать IP-адреса альтернативных DNS-серверов, которые необходимо использовать;

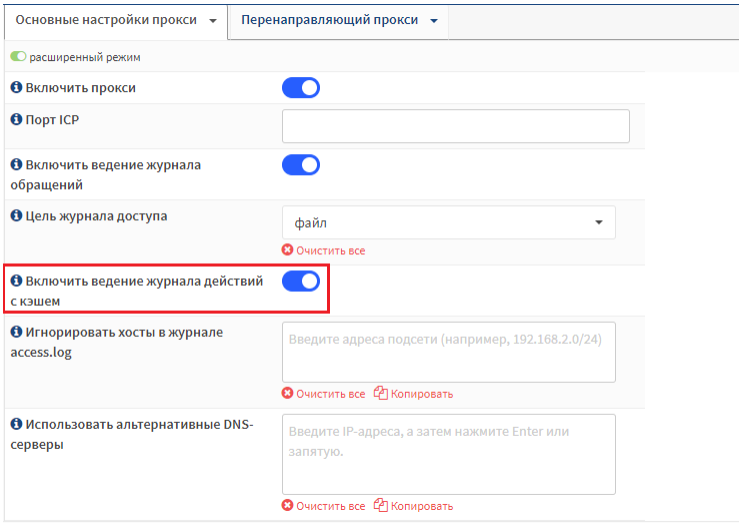


Рис. 914: Включение ведения журнала действий с кэшем

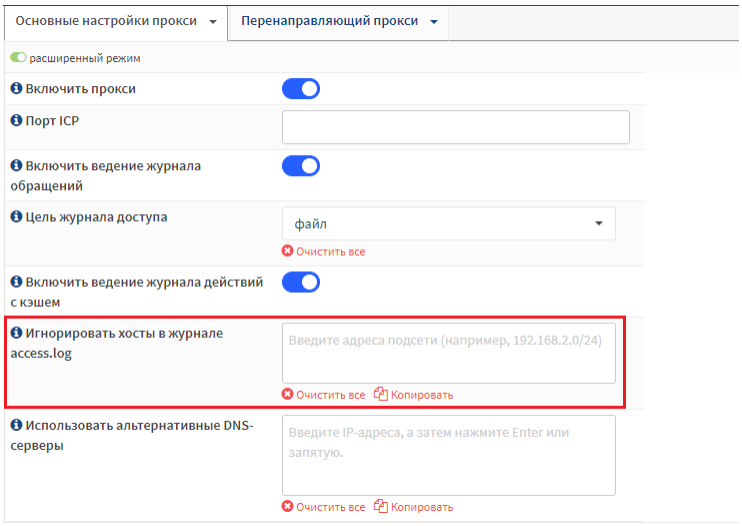


Рис. 915: Игнорировать хосты в журнале access.log

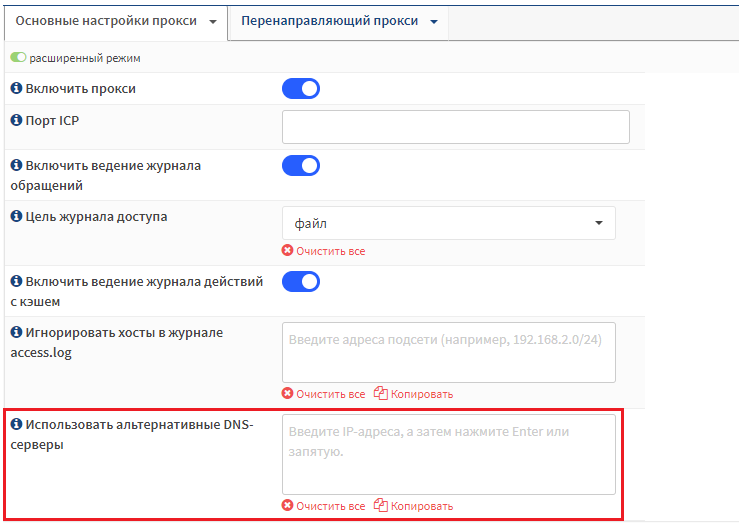


Рис. 916: Использовать альтернативные DNS-серверы

- в поле **«Включить сначала DNS v4»** установить переключатель в случае необходимости изменить порядок предпочтения, чтобы Squid сначала связывался с веб-сайтами с двойным стеком через IPv4;

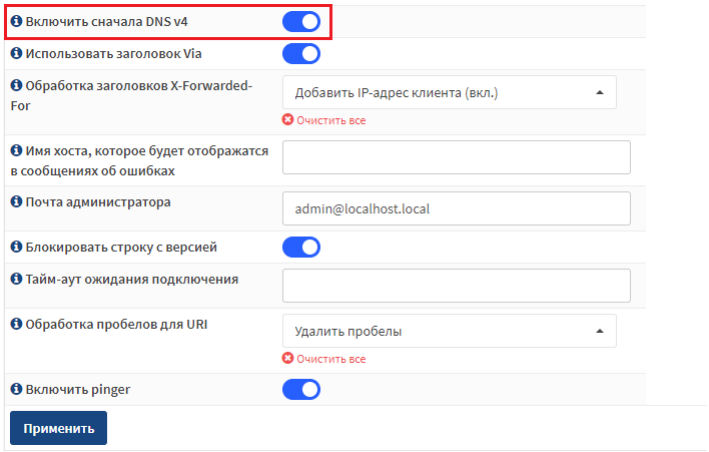


Рис. 917: Включить сначала DNS v4

Примечание

Squid по-прежнему будет выполнять DNS-запрос IPv6 и IPv4 перед подключением

Примечание

Этот параметр ограничит ситуации, в которых используется (и тестируется) подключение IPv6, и скроет сетевые проблемы, которые в противном случае были бы обнаружены и предупреждены

- в поле **«Использовать заголовок Via»** установить переключатель в случае необходимости Squid добавлять Via заголовок в запросы и ответы, как того требует RFC2616;

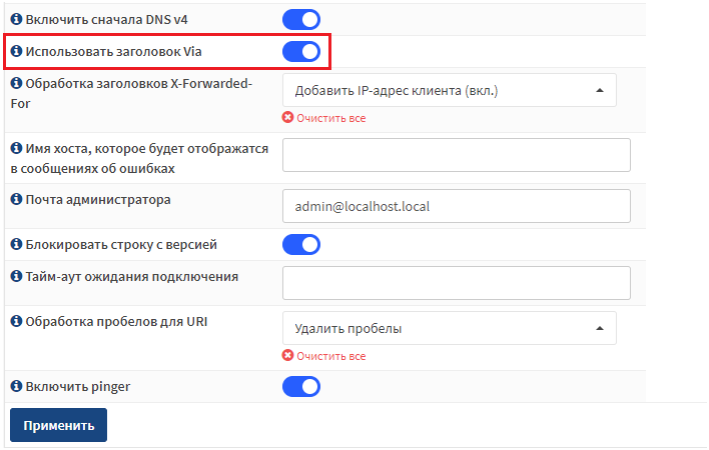


Рис. 918: Использовать заголовок Via

- в поле **«Обработка заголовков X-Forwarded-Fo»** указать действие, проводимое с заголовком X-Forwarded-For;

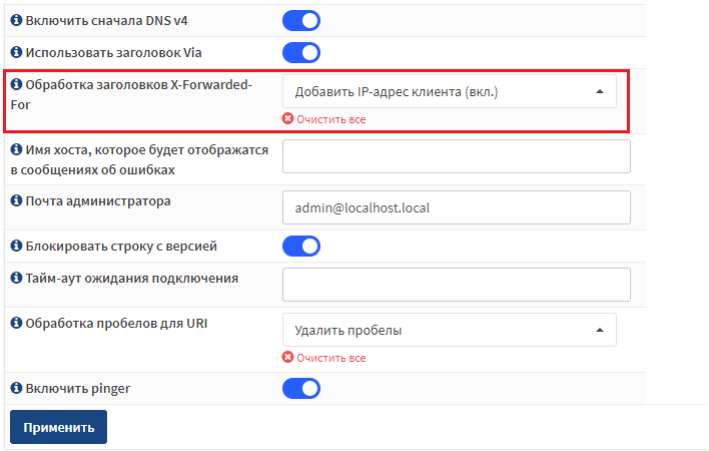


Рис. 919: Обработка заголовков X-Forwarded-Fo

- в поле **«Имя хоста, которое будет отображаться в сообщениях об ошибках»** указать имя хоста, которое будет отображаться в сообщениях об ошибке прокси-сервера;
- в поле **«Почта администратора»** указать адрес электронной почты, который будет отображаться пользователям в сообщениях об ошибке;
- в поле **«Блокировать строку с версией»** установить переключатель в случае необходимости пресекать выдачу версии Squid в HTTP-заголовках и HTML-страницах об ошибках;
- в поле **«Тайм-аут ожидания подключения»** указать значение тайм-аута ожидания подключения (в секундах) при проблемах с подключением к серверам с поддержкой IPv6;
- в поле **«Обработка пробелов для URI»** указать действие, проводимое с URI, содержащими пробелы;

Внимание

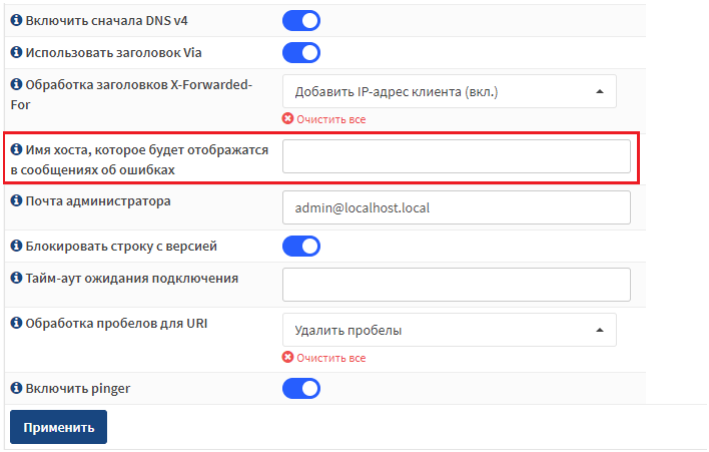


Рис. 920: Имя хоста, которое будет отображаться в сообщениях об ошибках

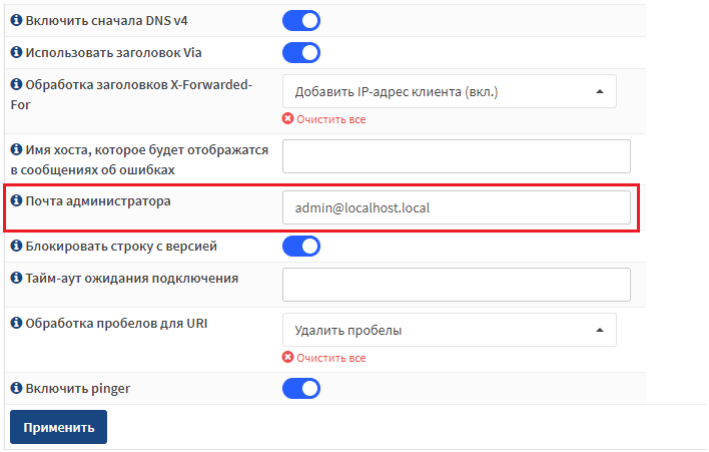


Рис. 921: Почта администратора

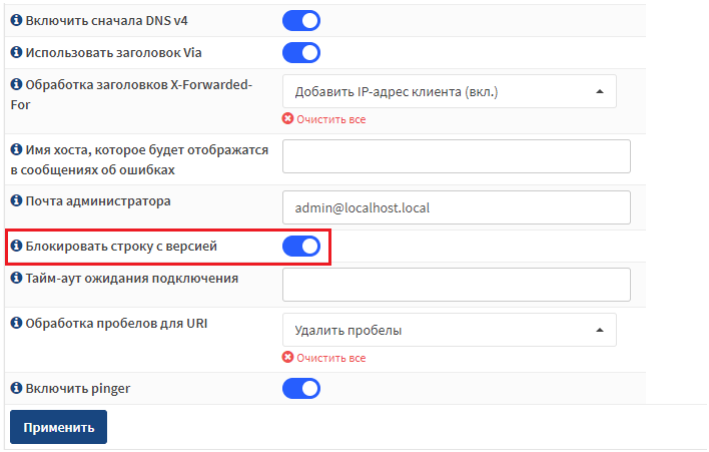


Рис. 922: Блокировать строку с версией

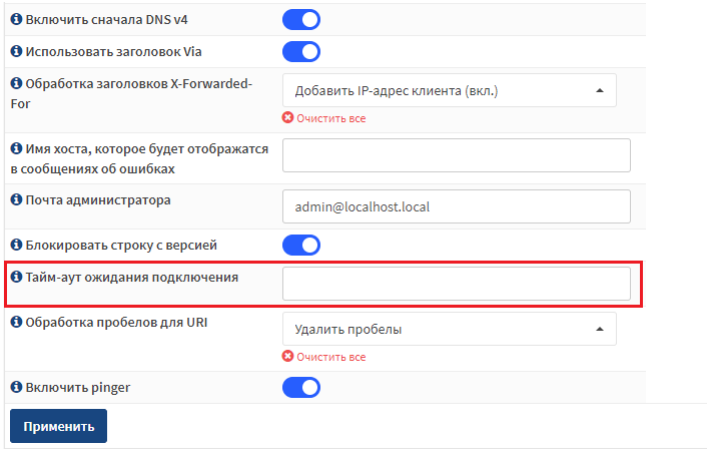


Рис. 923: Тайм-аут ожидания подключения

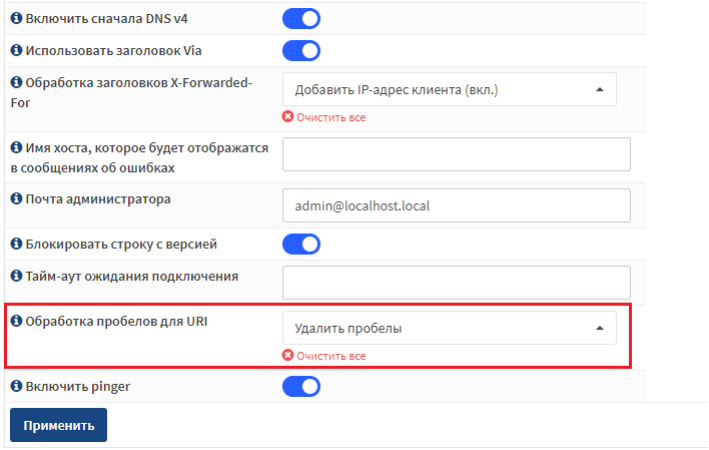


Рис. 924: Обработка пробелов для URI

Текущая реализация Squid кодирования и измельчения нарушает RFC2616, поскольку не использует перенаправление 301 после изменения URL-адреса

- в поле **«Включить pinger»** установить переключатель в случае необходимости переключить службу проверки связи Squid;

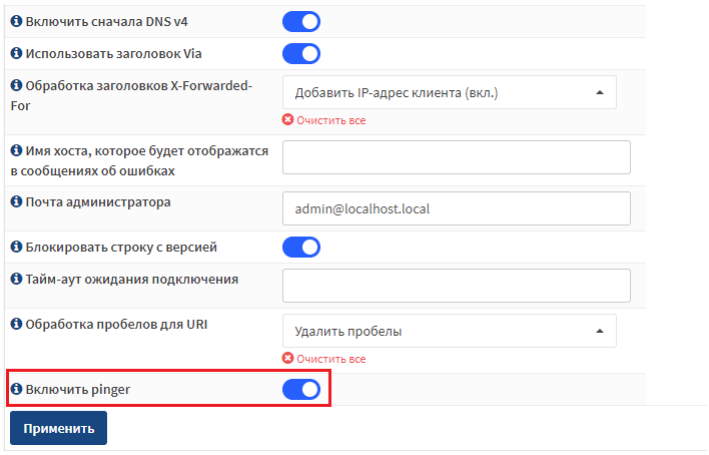


Рис. 925: Включить pinger

- нажать кнопку **«Применить»** 

.

Настройки локального кэша

Для выполнения настроек локального кэша необходимо:

- выбрать из выпадающего списка **«Настройки локального кэша»**;

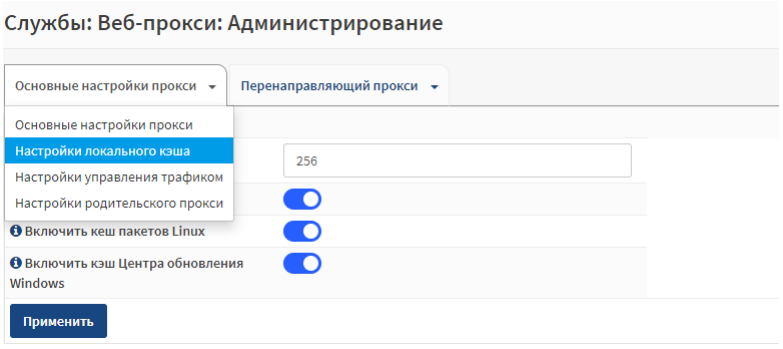


Рис. 926: Переход к настройкам локального кэша

- в поле **«Размер кэш-памяти (в Мб)»** указать размер памяти кэша или 0 для полного отключения;
- в поле **«Включить локальный кеш»** установить переключатель в случае необходимости включить локальный кэш;

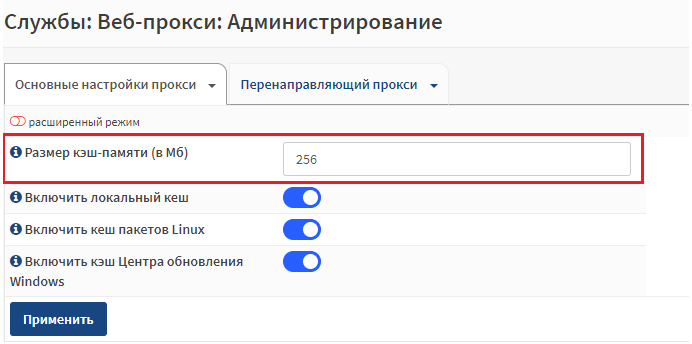


Рис. 927: Размер кэш-памяти (в Мб)

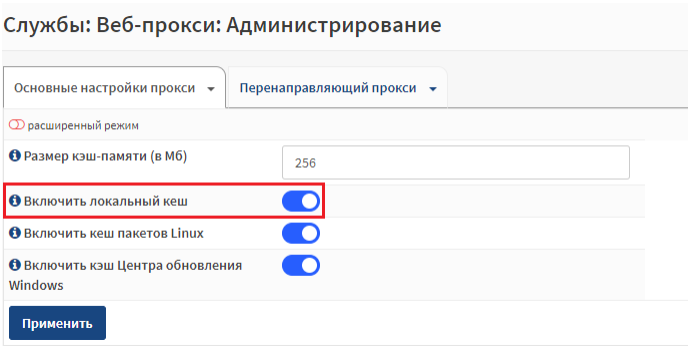


Рис. 928: Включить локальный кеш

Примечание

Поддерживается только тип кэша UFS directory

Примечание

Не включайте на встраиваемых системах с SD или CF картами без опции /var MFS т.к. это способствует износу диска

- в поле **«Включить кеш пакетов Linux»** установить переключатель в случае необходимости включить кэширование пакетов для дистрибутивов Linux;

Совет

Использование функции **«Включить кеш пакетов Linux»** необходимо, если у пользователя есть несколько серверов в его сети и он не размещает собственное зеркало пакетов. Это уменьшит использование интернет-трафика, но увеличит доступ к диску

- в поле **«Включить кэш Центра обновления Windows»** установить переключатель в случае необходимости включить кэширование обновлений Windows;

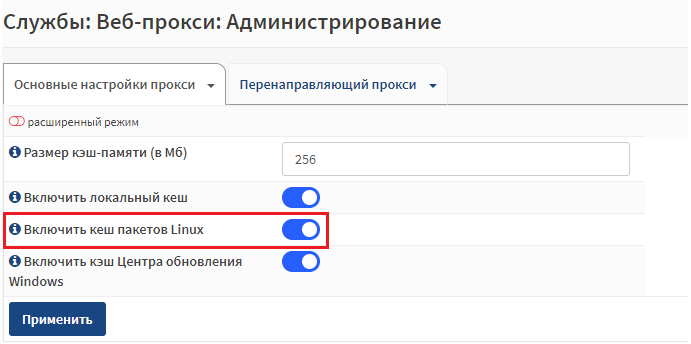


Рис. 929: Включить кеш пакетов Linux

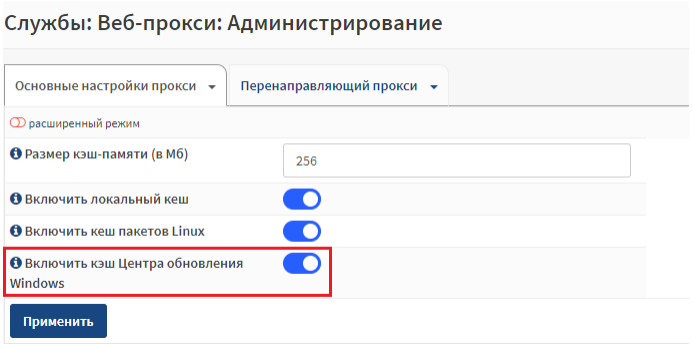


Рис. 930: Включить кэш Центра обновления Windows

Примечание

Использование функции **«Включить кэш Центра обновления Windows»** необходимо, если у пользователя нет сервера WSUS. Если пользователь может настроить сервер WSUS, это решение должно быть предпочтительным

- нажать кнопку **«Применить»** 

.

Для включения режима расширенных настроек необходимо установить переключатель.

В режиме расширенных настроек необходимо:

- в поле **«Размер кэша (в Мб)»** указать количество дискового пространства для хранения локального кэша;

Примечание

По умолчанию 100 Мб

- в поле **«Расположение директории кэша»** указать расположение директории для локального кэша;

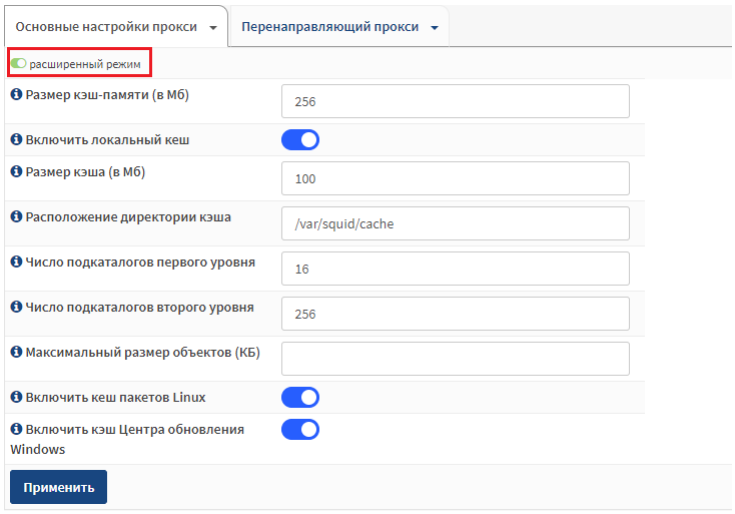


Рис. 931: Включение расширенных настроек

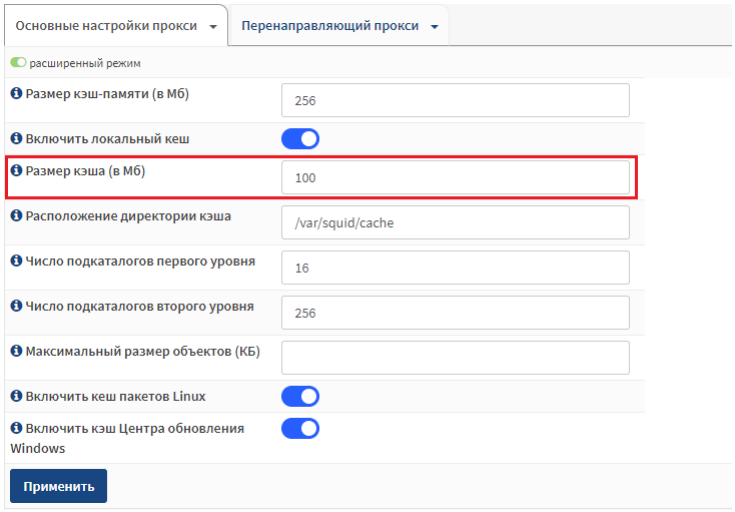


Рис. 932: Размер кэша (в Мб)

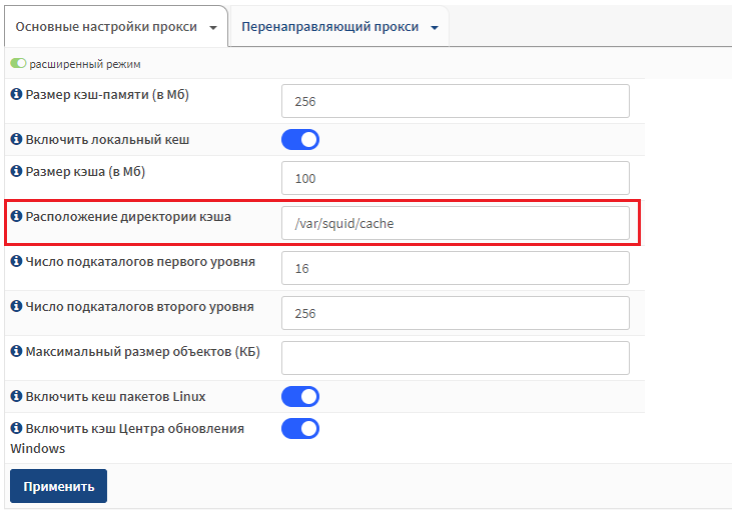


Рис. 933: Расположение директории кэша

Примечание

По умолчанию /var/squid/cache

- в поле **«Число подкаталогов первого уровня»** указать количество подкаталогов первого уровня, которые будут созданы в директории для хранения локального кэша;

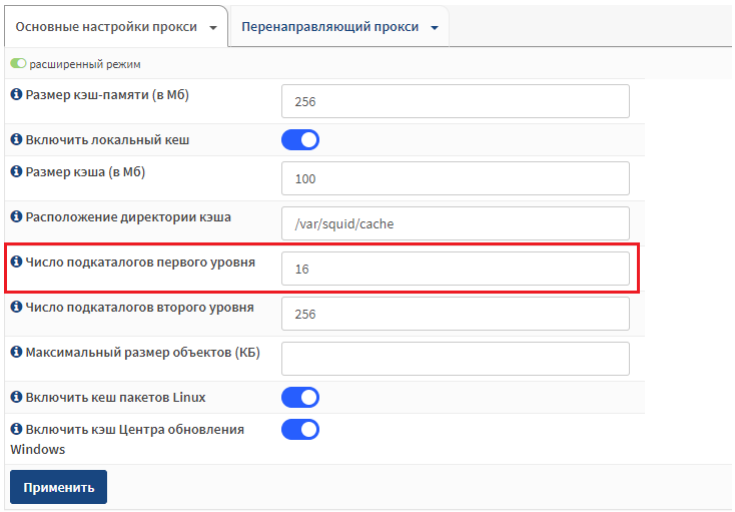


Рис. 934: Число подкаталогов первого уровня

Примечание

По умолчанию 16

- в поле **«Число подкаталогов второго уровня»** указать количество подкаталогов второго уровня, которые будут созданы в директории для хранения локального кэша;

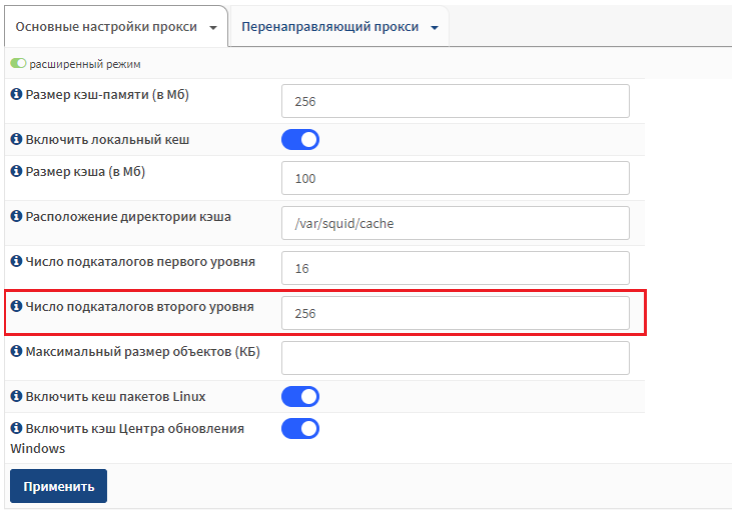


Рис. 935: Число подкаталогов второго уровня

Примечание

По умолчанию 256

- в поле **«Максимальный размер объектов (КБ)»** указать максимальный размер объекта;

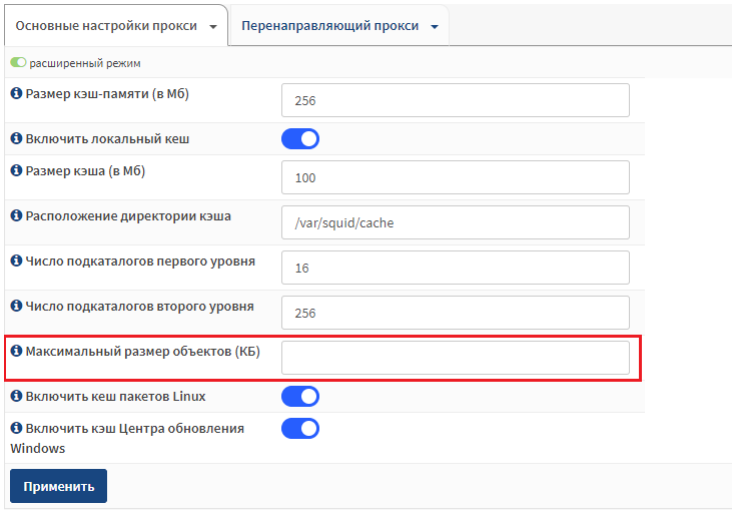


Рис. 936: Число подкаталогов второго уровня

Примечание

Если после **«Максимальный размер объектов (КБ)»** пустое, используется значение по умолчанию равно 4 МБ

- нажать кнопку **«Применить»** 

.

Настройки управления трафиком

Для выполнения настроек управления трафиком необходимо:

- выбрать из выпадающего списка **«Настройки управления трафиком»**;

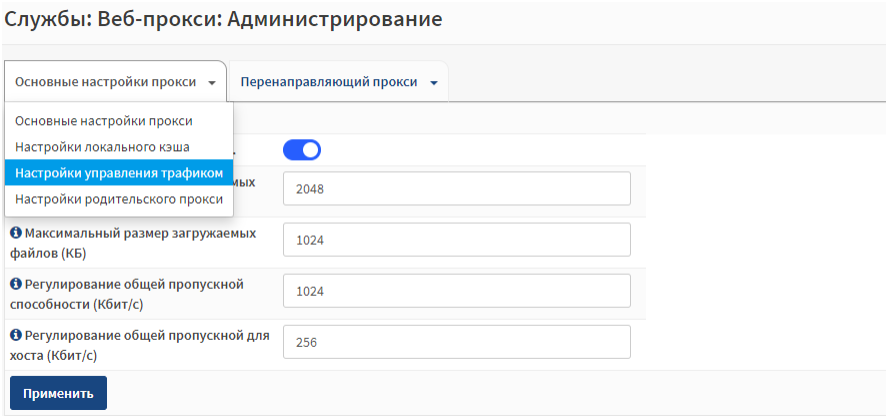


Рис. 937: Переход к настройкам управления трафиком

- в поле **«Включить управление трафиком»** установить переключатель в случае необходимости включить управление трафиком;

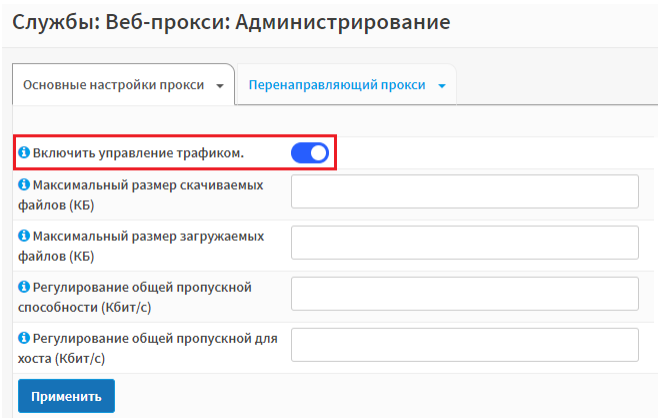


Рис. 938: Включить управление трафиком

- в поле **«Максимальный размер скачиваемых файлов (КБ)»** указать максимальный размер скачиваемых файлов в килобайтах;

Совет

Для отключения настройки необходимо оставить поле пустым

- в поле **«Максимальный размер загружаемых файлов (КБ)»** указать максимальный размер загружаемых файлов в килобайтах;

Совет

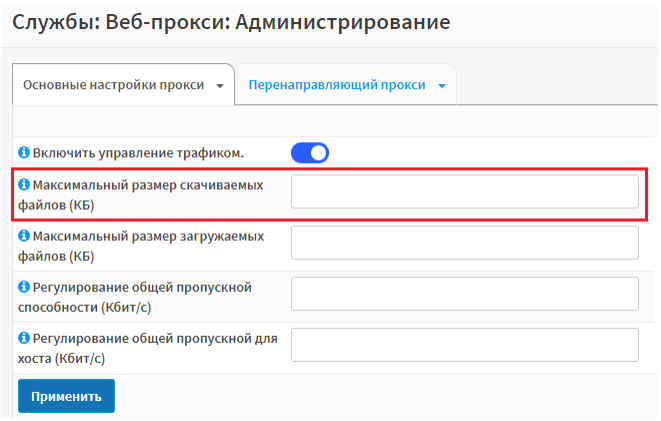


Рис. 939: Максимальный размер скачиваемых файлов (КБ)

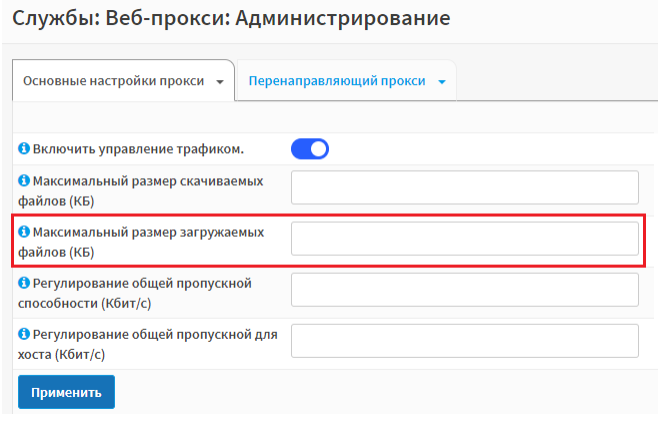


Рис. 940: Максимальный размер загружаемых файлов (КБ)

Для отключения настройки необходимо оставить поле пустым

- в поле **«Регулирование общей пропускной способности (Кбит/с)»** указать допустимую общую пропускную способность в килобитах в секунду;

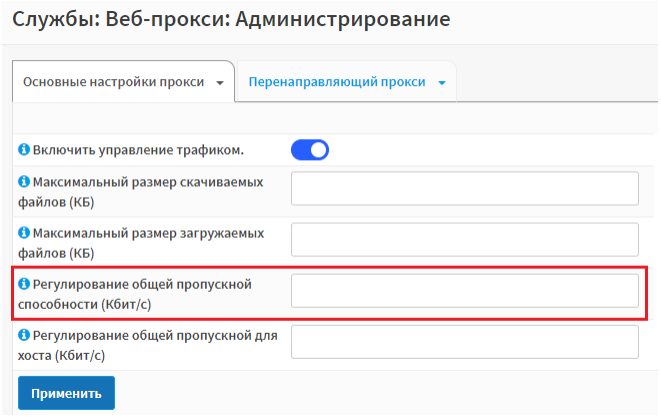


Рис. 941: Регулирование общей пропускной способности (Кбит/с)

Совет

Для отключения ограничения необходимо оставить поле пустым

- в поле **«Регулирование общей пропускной для хоста (Кбит/с)»** указать допустимую пропускную способность для хоста в килобитах в секунду;

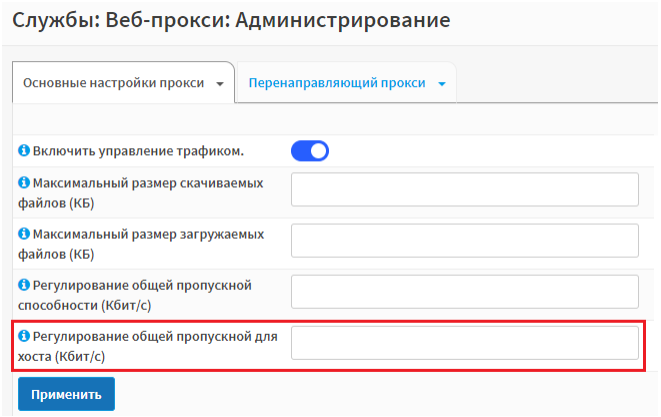


Рис. 942: Регулирование общей пропускной для хоста (Кбит/с)

Совет

Для отключения ограничения необходимо оставить поле пустым

- нажать кнопку **«Применить»** 

.

Настройки родительского прокси

Для выполнения настроек родительского прокси необходимо:

- выбрать из выпадающего списка **«Настройки родительского прокси»**;

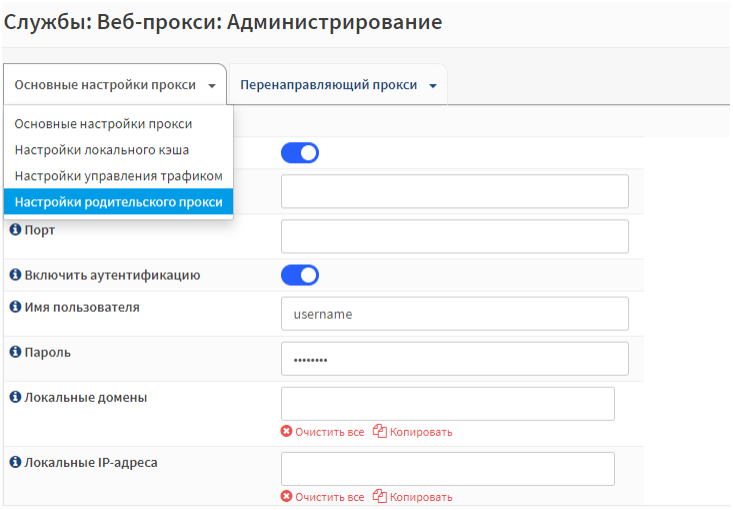


Рис. 943: Переход к настройкам родительского прокси

- в поле **«Включить родительский прокси»** установить переключатель в случае необходимости включить родительский прокси;

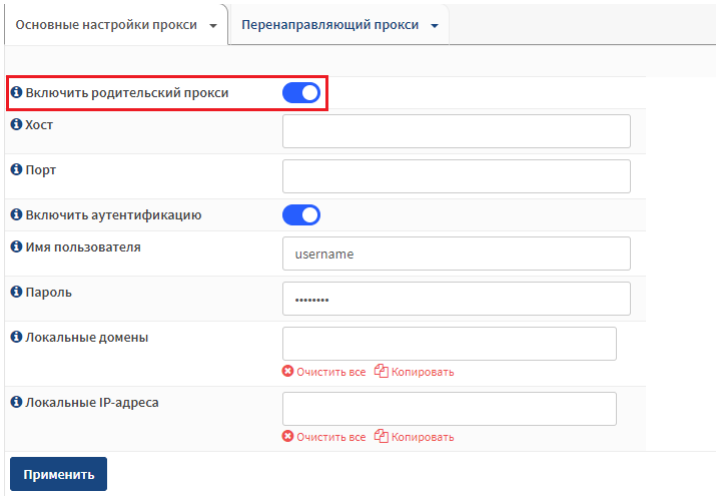


Рис. 944: Включить родительский прокси

- в поле **«Хост»** указать IP-адрес или имя хоста родительского прокси-сервера;
- в поле **«Порт»** указать порт родительского прокси-сервера;
- в поле **«Включить аутентификацию»** установить переключатель в случае необходимости включить аутентификацию на родительском прокси-сервере;
- в поле **«Имя пользователя»** указать имя пользователя, если родительский прокси-сервер требует аутентификации;

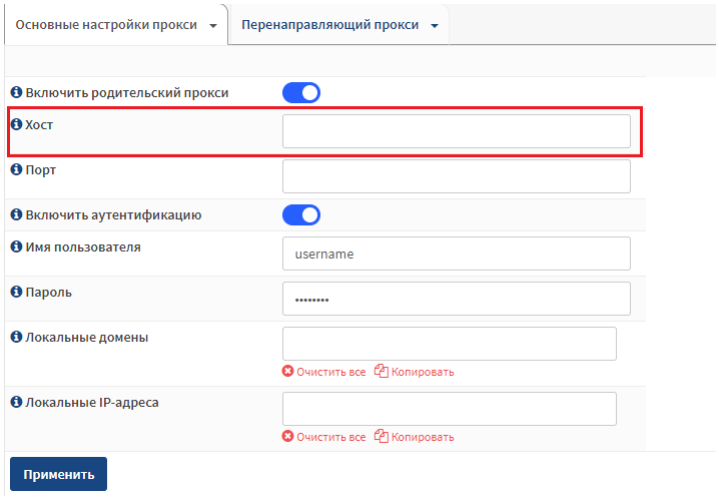


Рис. 945: Хост

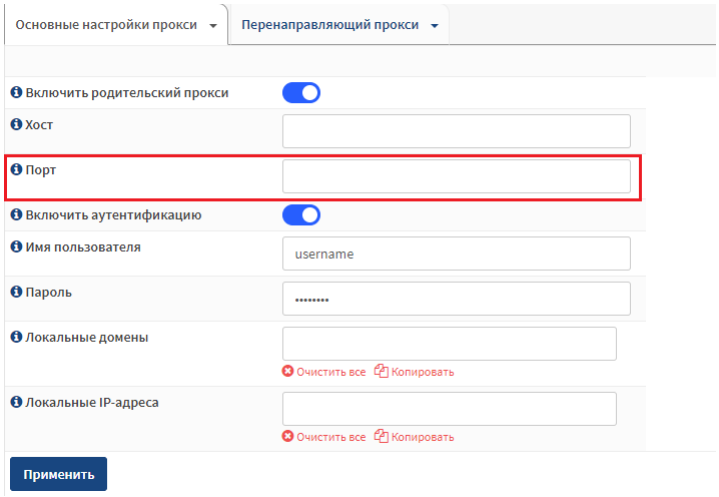


Рис. 946: Порт

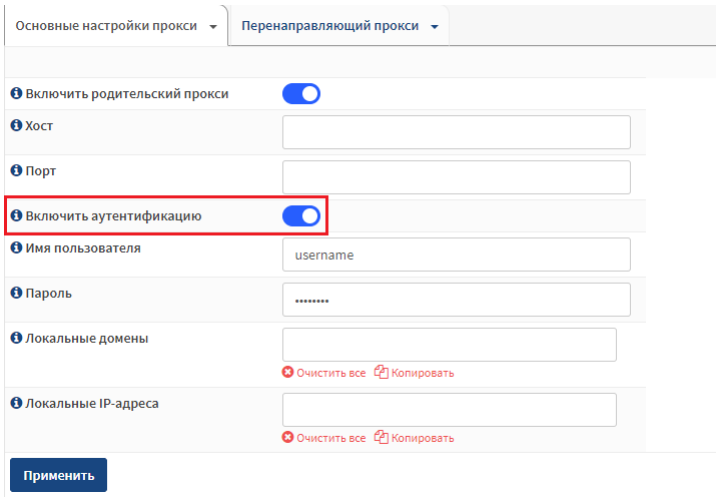


Рис. 947: Включить аутентификацию

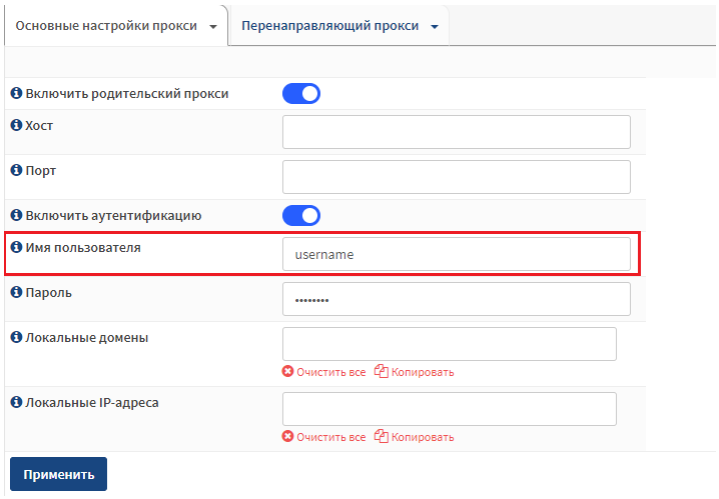


Рис. 948: Имя пользователя

- в поле **«Пароль»** указать пароль, если родительский прокси-сервер требует аутентификации;

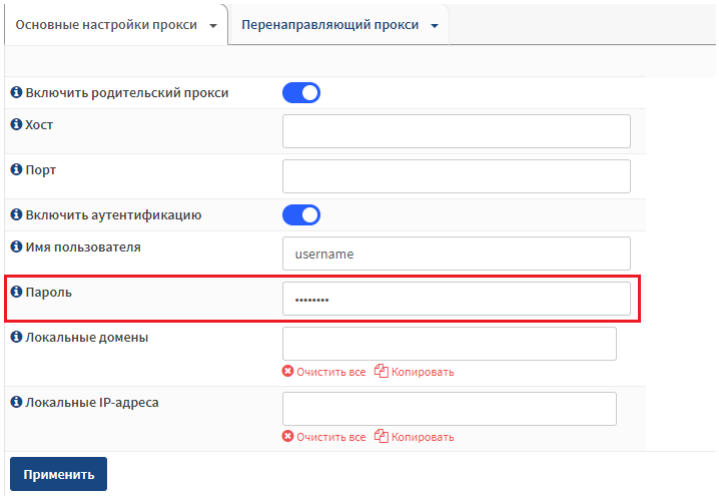


Рис. 949: Пароль

- в поле **«Локальные домены»** указать список доменов, которые нельзя отправлять через родительский прокси-сервер;
- в поле **«Локальные IP-адреса»** указать список IP-адресов, которые нельзя отправлять через родительский прокси-сервер;
- нажать кнопку **«Применить»** 

.

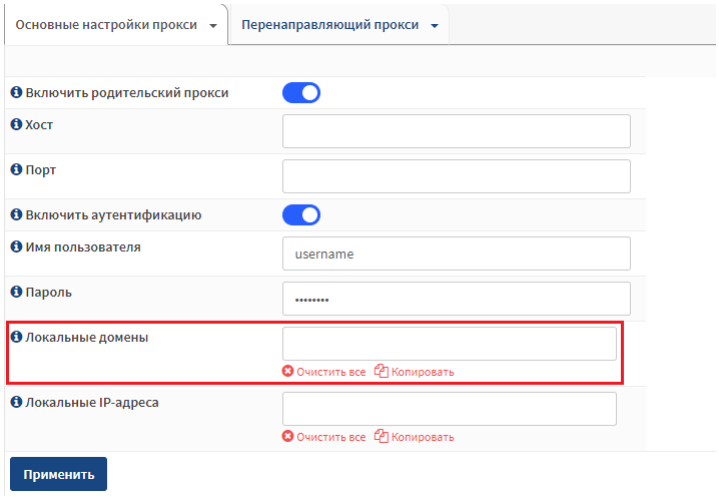


Рис. 950: Локальные домены

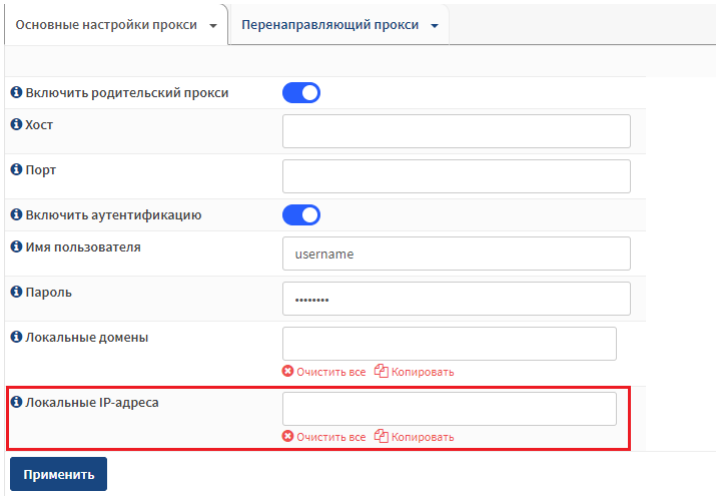


Рис. 951: Локальные IP-адреса

Основные настройки перенаправления

Для выполнения основных настроек перенаправления необходимо:

- выбрать из выпадающего списка **«Основные настройки перенаправления»**;

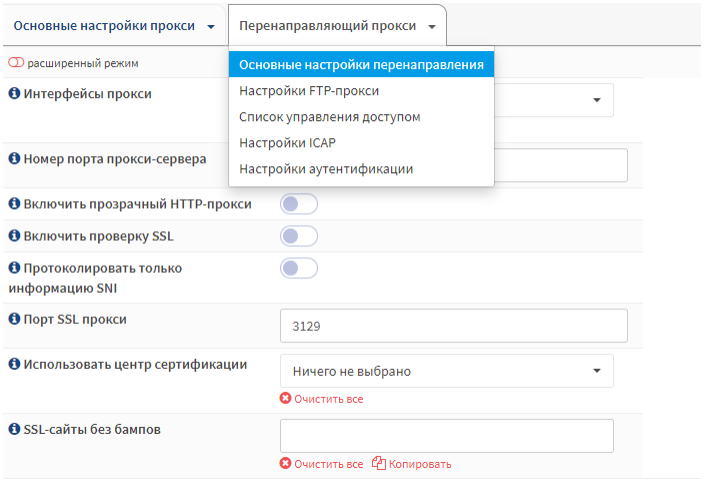


Рис. 952: Переход к основным настройкам перенаправления

- в поле **«Интерфейсы прокси»** выбрать из выпадающего списка интерфейсы, к которым будет привязан прокси-сервер;

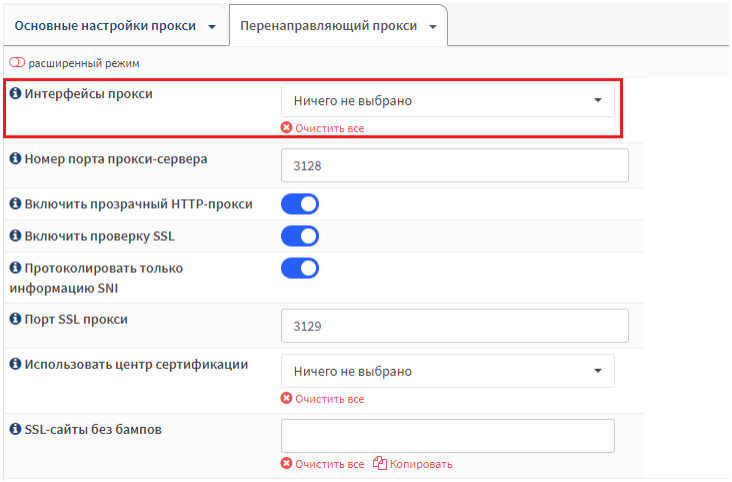


Рис. 953: Интерфейсы прокси

- в поле **«Номер порта прокси-сервера»** указать порт, который прокси-сервер будет прослушивать;
- в поле **«Включить прозрачный HTTP-прокси»** установить переключатель в случае необходимости включить прозрачный HTTP-прокси;

Примечание

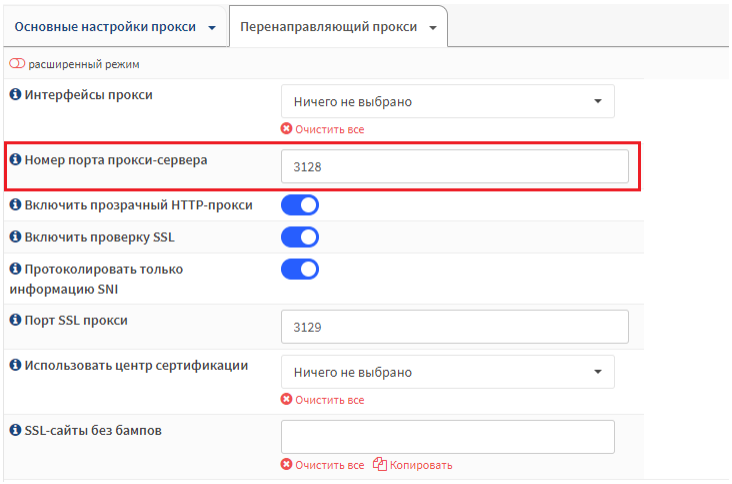


Рис. 954: Номер порта прокси-сервера

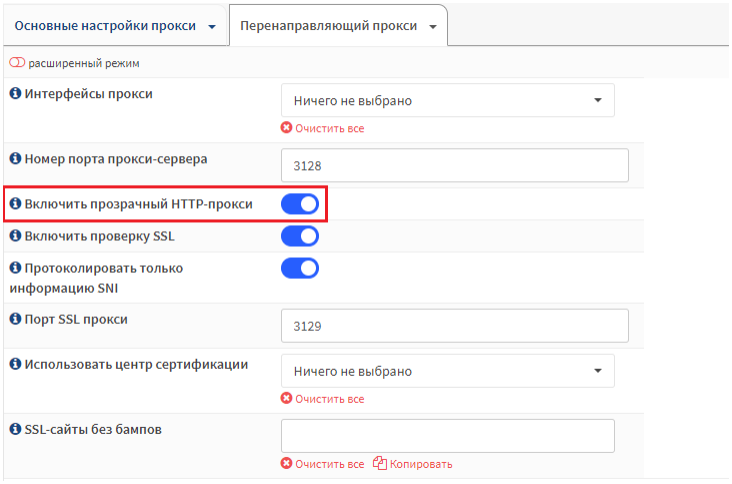


Рис. 955: Включить прозрачный HTTP-прокси

Пользователю потребуется правило межсетевого экрана для перенаправления трафика с межсетевого экрана на прокси-сервер

Примечание

Пользователь может оставить прокси-интерфейсы пустыми, но в этом случае необходимо установить действительный ACL

- в поле **«Включить проверку SSL»** установить переключатель в случае необходимости включить режим проверки SSL;

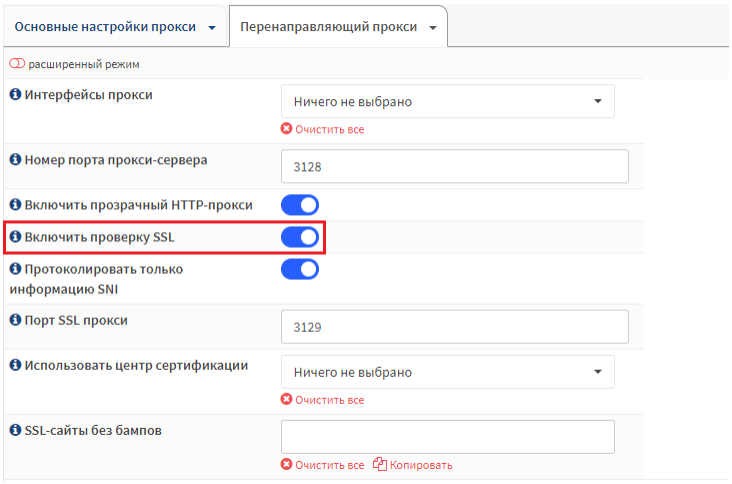


Рис. 956: Включить проверку SSL

Примечание

Режим проверки SSL позволяет регистрировать информацию о HTTPS-соединениях, такую как запрошенный URL-адрес, и/или заставлять прокси действовать как человек между Интернетом и клиентами пользователя

Внимание

Помните о последствиях для безопасности, прежде чем включать опцию **«Включить проверку SSL»**

Примечание

Если вы планируете использовать прозрачный режим HTTPS, вам нужны правила nat для отражения вашего трафика

- в поле **«Протоколировать только информацию SNI»** установить переключатель в случае необходимости протоколировать только информацию SNI;

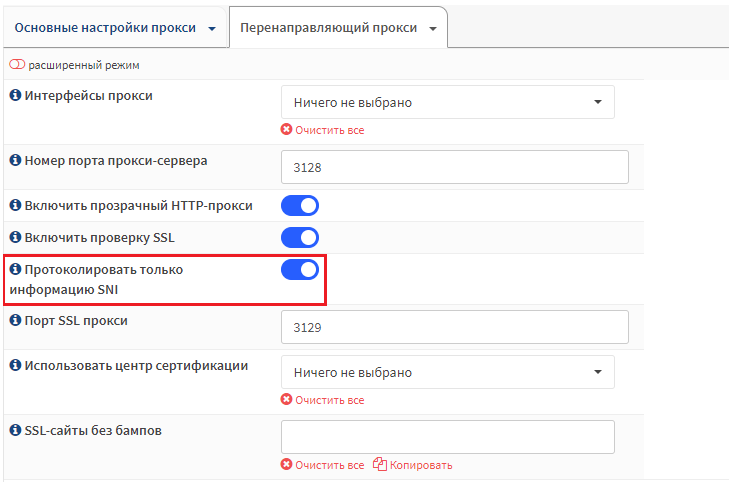


Рис. 957: Протоколировать только информацию SNI

Внимание

Не декодируйте и/или не фильтруйте содержимое SSL, регистрируйте только запрошенные домены и IP-адреса

Примечание

Некоторые старые сервера могут не предоставлять SNI, поэтому их адреса указываться не будут

- в поле **«Порт SSL прокси»** указать порт, который служба SSL-прокси будет прослушивать;

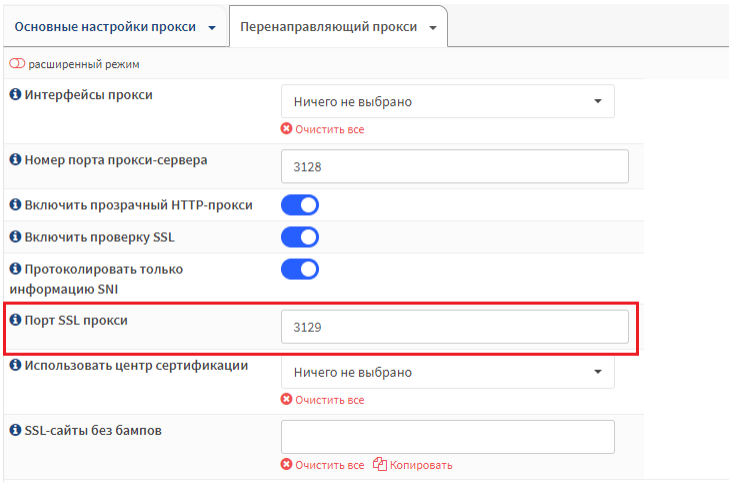


Рис. 958: Порт SSL прокси

- в поле **«Использовать центр сертификации»** выбрать из выпадающего списка центр сертификации для использования;

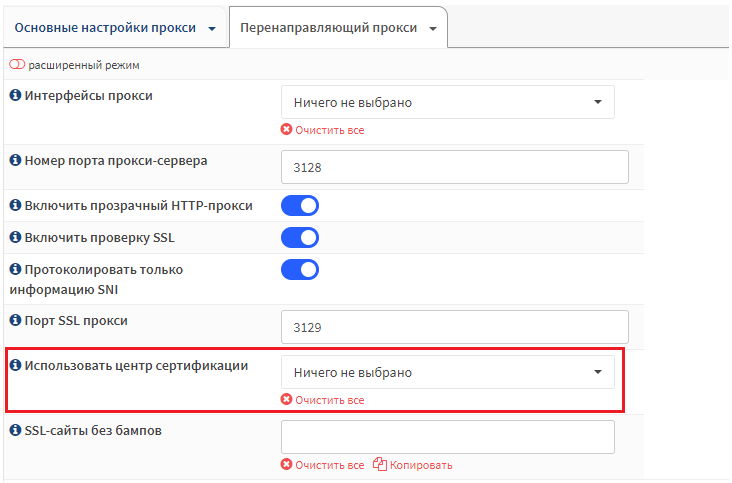


Рис. 959: Использовать центр сертификации

Примечание

Чтобы создать центр сертификации, перейдите **«Система»** - **«Доверенные сертификаты»** - **«Полномочия»**

- в поле **«SSL-сайты без бампов»** указать список сайтов, которые нельзя проверять;

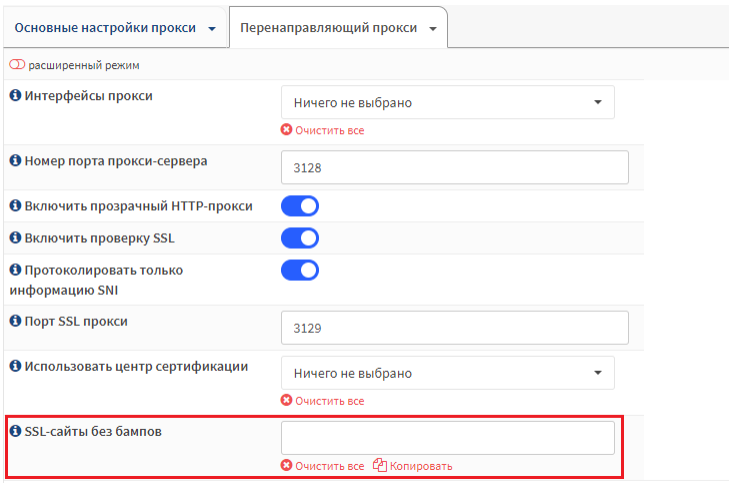


Рис. 960: SSL-сайты без бампов

- нажать кнопку **«Применить»** 

.

Для включения режима расширенных настроек необходимо установить переключатель.

В режиме расширенных настроек необходимо:

- в поле **«Размер кэша SSL»** указать максимальный размер кэша (в МБ) для сертификатов SSL;
- в поле **«Рабочие сертификаты SSL»** указать количество используемых рабочих сертификатов SSL (sslcrtd_children);

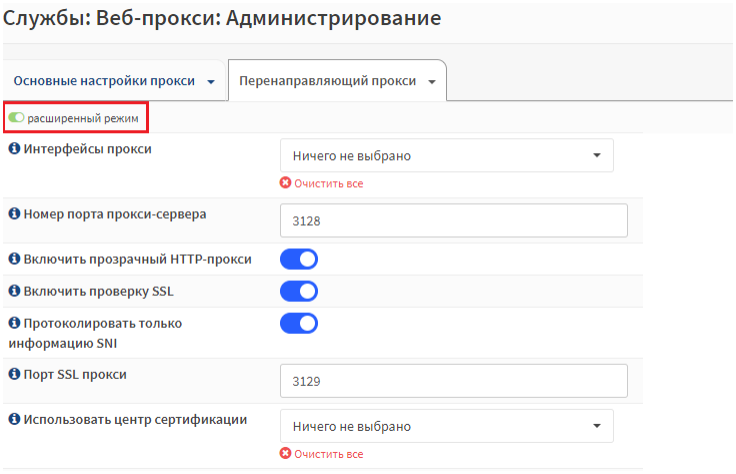


Рис. 961: Включение расширенных настроек

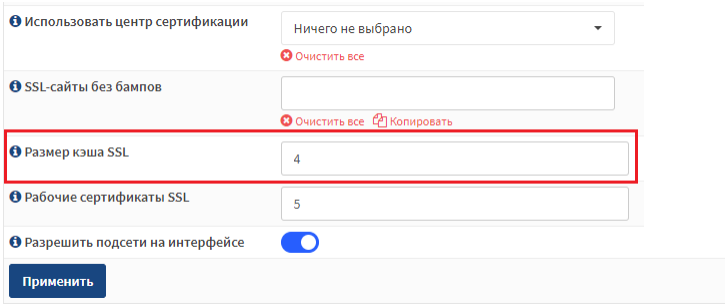


Рис. 962: Размер кэша SSL

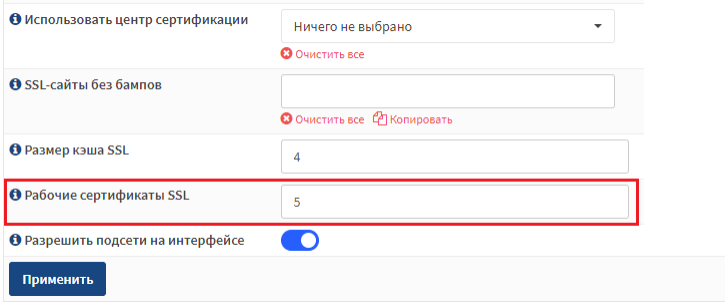


Рис. 963: Рабочие сертификаты SSL

- в поле **«Разрешить подсети на интерфейсе»** установить переключатель в случае необходимости добавления подсетей выбранных интерфейсов в список с правами доступа;

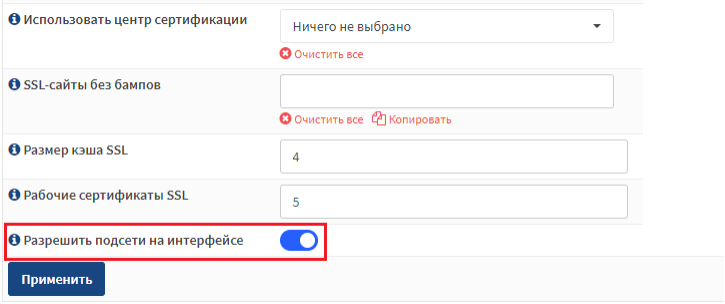


Рис. 964: Разрешить подсети на интерфейсе

- нажать кнопку **«Применить»** 

.

Настройки FTP-прокси

Для выполнения настроек FTP-прокси необходимо:

- выбрать из выпадающего списка **«Настройки FTP-прокси»**;

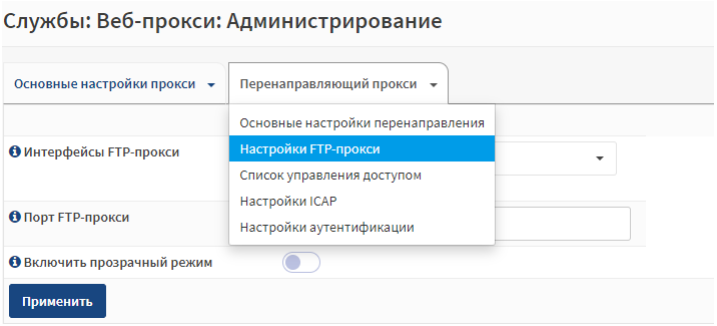


Рис. 965: Переход к настройкам FTP-прокси

- в поле **«Интерфейсы FTP-прокси»** выбрать из выпадающего списка интерфейсы, к которым будет привязан прокси-сервер FTP;

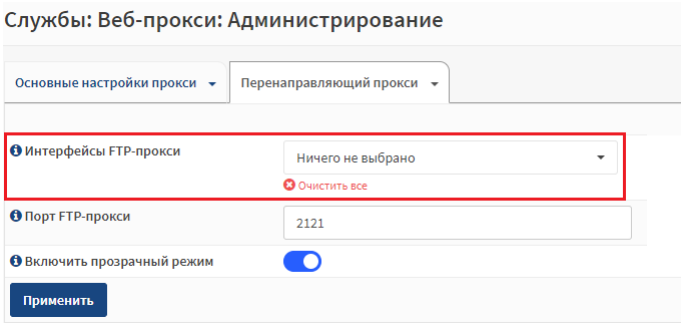


Рис. 966: Интерфейсы FTP-прокси

- в поле **«Порт FTP-прокси»** указать порт, который прокси-сервер будет прослушивать;

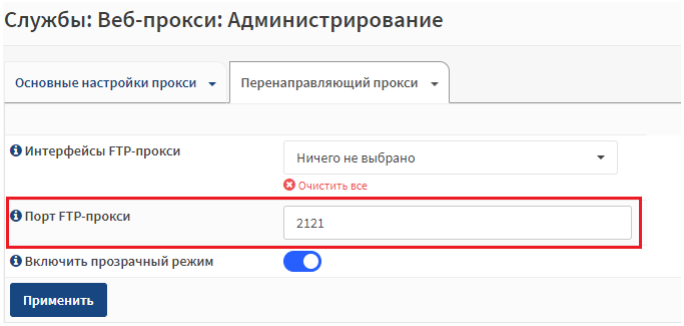


Рис. 967: Порт FTP-прокси

- в поле **«Включить прозрачный режим»** установить переключатель в случае необходимости включить прозрачный режим FTP-прокси, чтобы без дополнительной настройки перенаправлять запросы для порта назначения номер 21 на прокси-сервер;

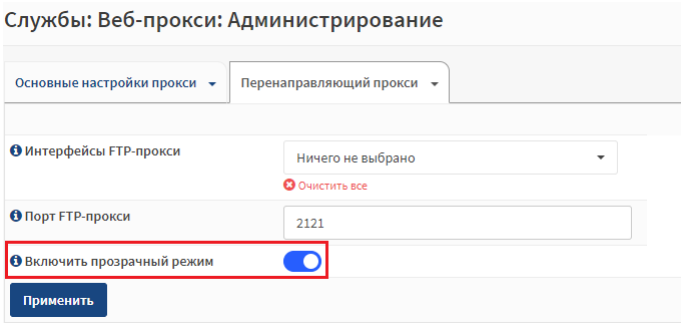


Рис. 968: Включить прозрачный режим

- нажать кнопку **«Применить»** 

.

Список управления доступом

Для выполнения настроек списка управления доступом необходимо:

- выбрать из выпадающего списка **«Список управления доступом»**;
- в поле **«Разрешенные подсети»** указать подсети, которым необходимо разрешить доступ к прокси-серверу;
- в поле **«IP-адреса без ограничений»** указать IP-адреса, которым необходимо разрешить доступ к прокси-серверу;
- в поле **«Заблокированные IP-адреса хоста»** указать заблокированные IP-адреса хоста;
- в поле **«Белый список»** указать белый список целевых доменов;

Примечание

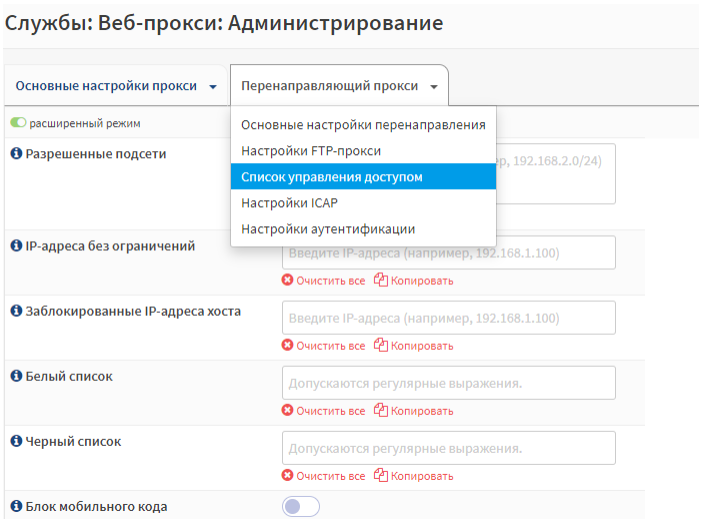


Рис. 969: Переход к настройкам списка управления доступом

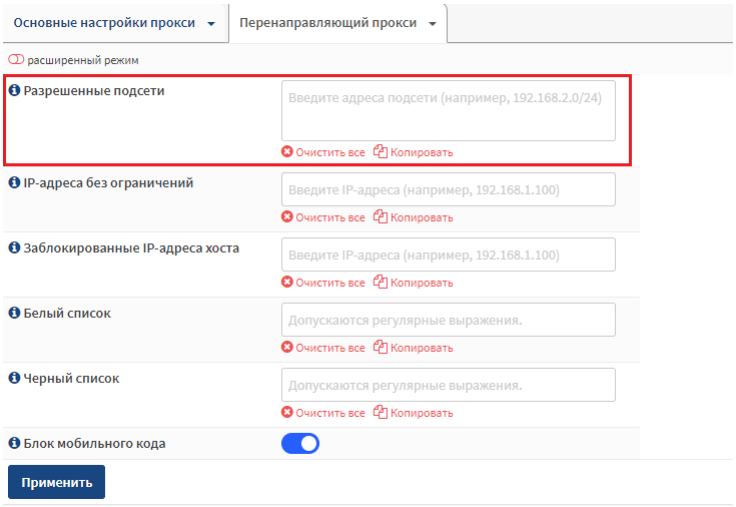


Рис. 970: Разрешенные подсети

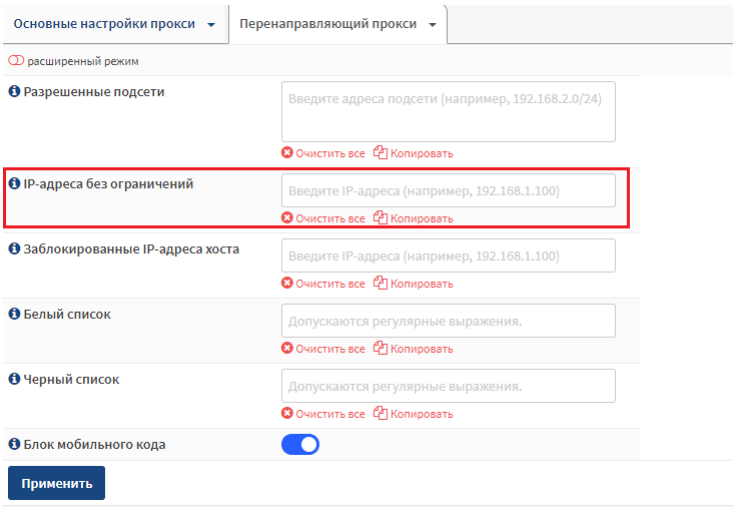


Рис. 971: IP-адреса без ограничений

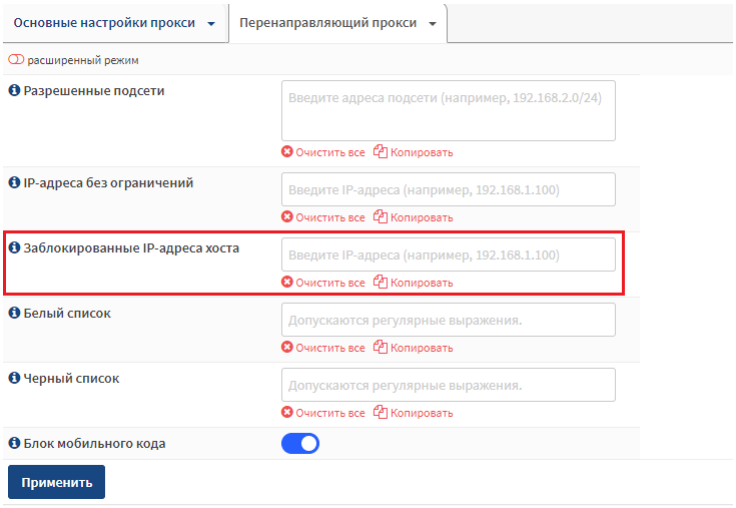


Рис. 972: Заблокированные IP-адреса хоста

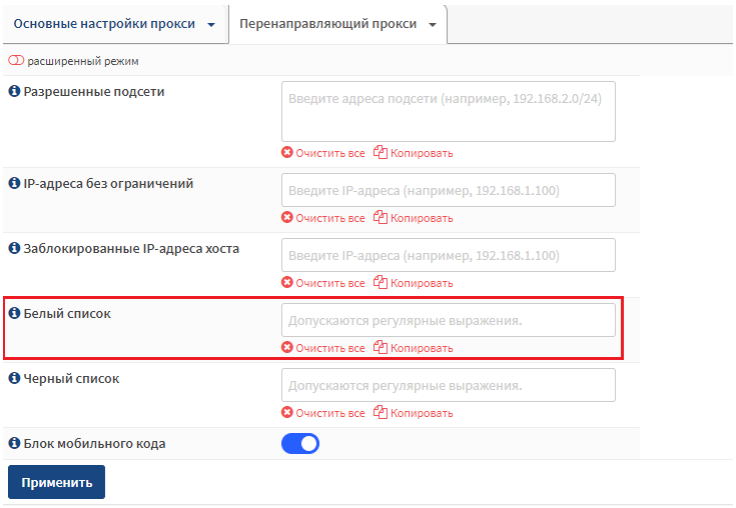


Рис. 973: Белый список

Пользователь может использовать регулярное выражение, использовать запятую или нажать Enter для нового элемента

- в поле **«Черный список»** указать черный список целевых доменов;

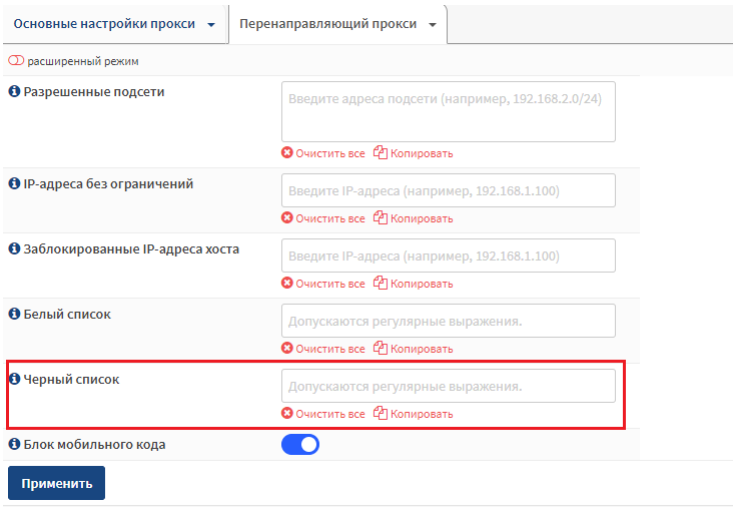


Рис. 974: Черный список

Примечание

Пользователь может использовать регулярное выражение, использовать запятую или нажать Enter для нового элемента

- в поле **«Блок мобильного кода»** установить переключатель в случае необходимости заблокировать javascript, файлы cookie и ActiveX;

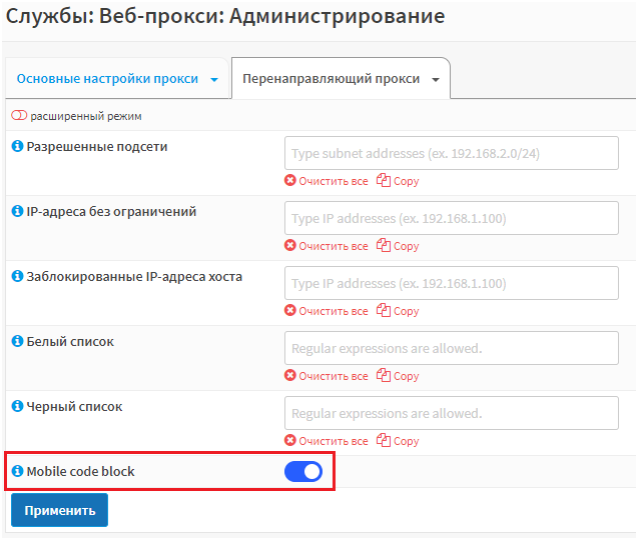


Рис. 975: Блок мобильного кода

- нажать кнопку **«Применить»** 

.

Для включения режима расширенных настроек необходимо установить переключатель.

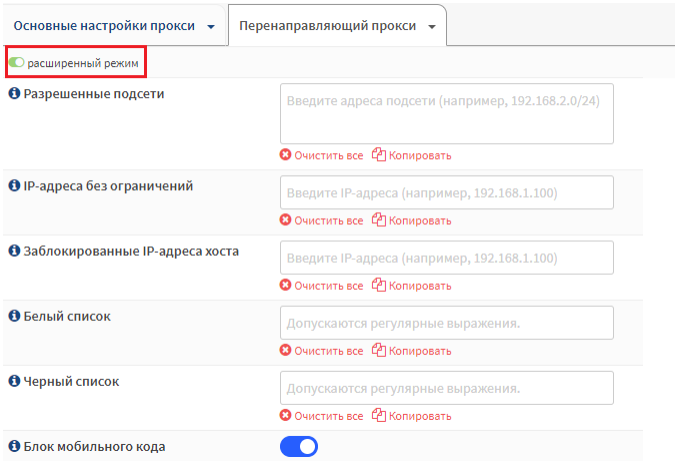


Рис. 976: Включение расширенных настроек

В режиме расширенных настроек необходимо:

- в поле **«Блокировать browser/user-agent строки»** использовать регулярное выражение, использовать запятую для блокировки юзер-агентов;

Примечание

Примеры: «^(.)+Macintosh(.)+Firefox/37.0» соответствует «версия Firefox для Macintosh версии 37.0»; «^Mozilla» соответствует «всем браузерам на основе Mozilla»

- в поле **«Блокировать ответы с конкретным MIME-типом»** использовать регулярное вы-

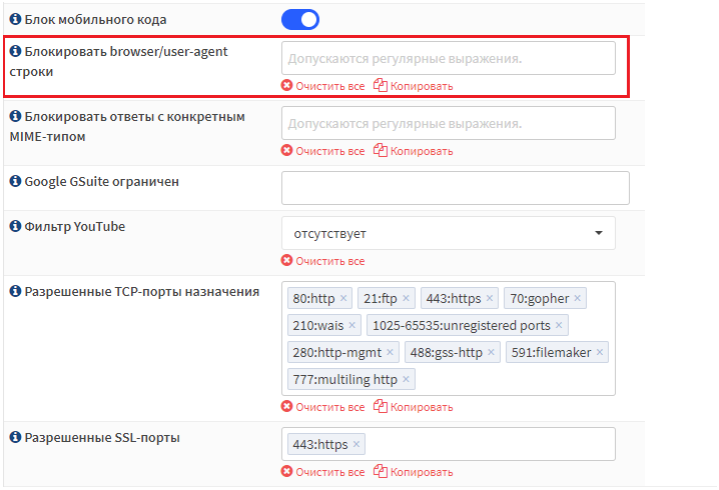


Рис. 977: Блокировать browser/user-agent строки

ражение, использовать запятую для блокировки ответа определенного типа MIME;

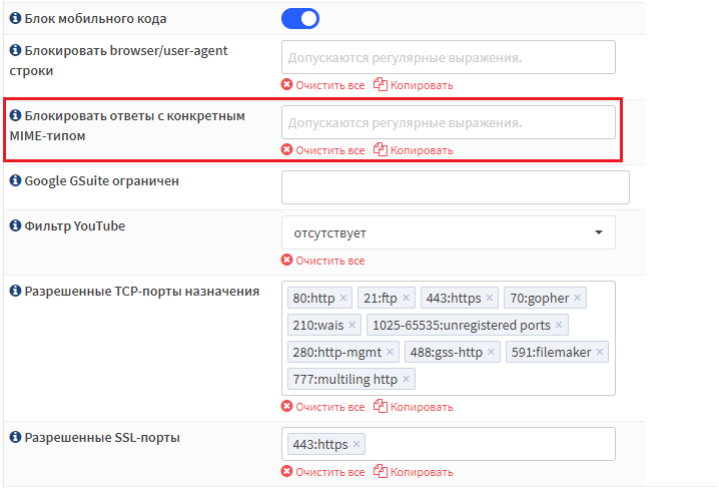


Рис. 978: Блокировать ответы с конкретным MIME-типом

Примечание

Примеры: «video/flv» соответствует «Flash Video»; «application/x-javascript» соответствует «javascripts»

- в поле **«Google GSuite ограничен»** указать домен, которому будет разрешено использовать Google G Suite;

Примечание

Все учетные записи, не относящиеся к этому домену, будут заблокированы для его использования

- в поле **«Фильтр YouTube»** выбрать из выпадающего списка уровень фильтра Youtube;

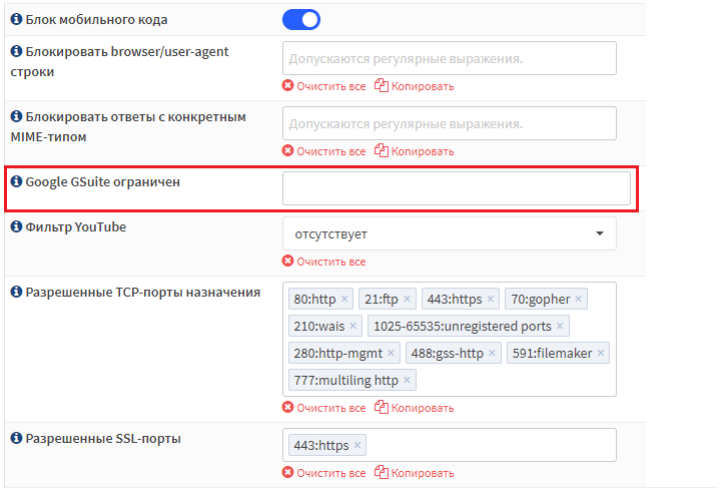


Рис. 979: Google GSuite ограничен

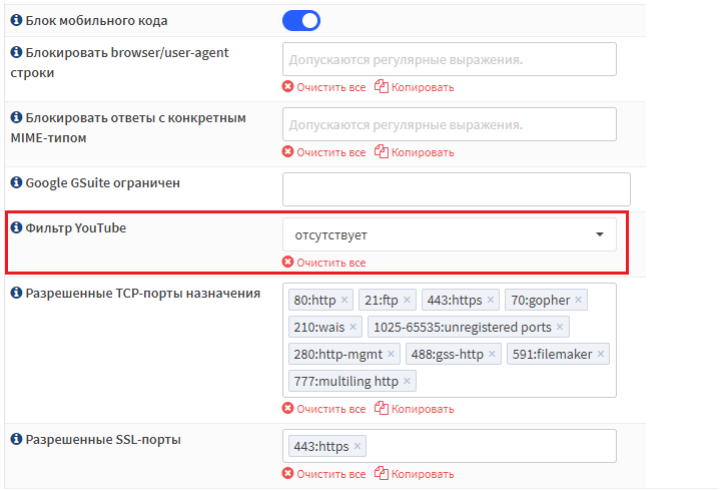


Рис. 980: Фильтр YouTube

- в поле **«Разрешенные TCP-порты назначения»** указать разрешенные TCP-порты назначения;

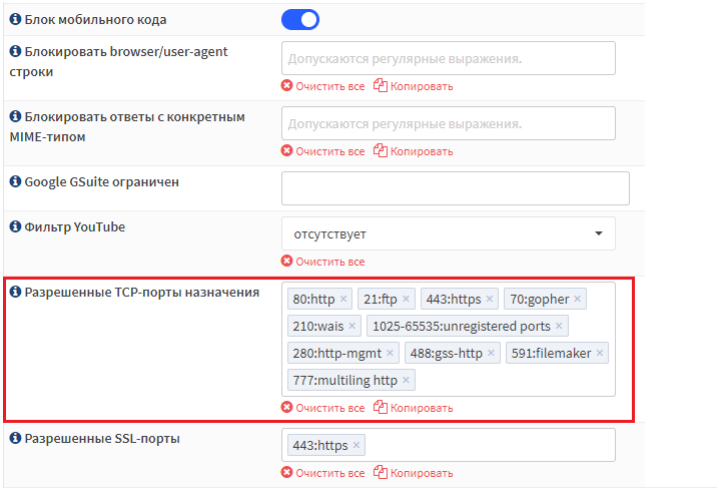


Рис. 981: Разрешенные TCP-порты назначения

Примечание

Пользователь может использовать диапазоны (например, 222-226) и добавлять комментарии с двоеточием (например, 22: ssh)

- в поле **«Разрешенные SSL-порты»** указать разрешенные SSL-порты назначения;

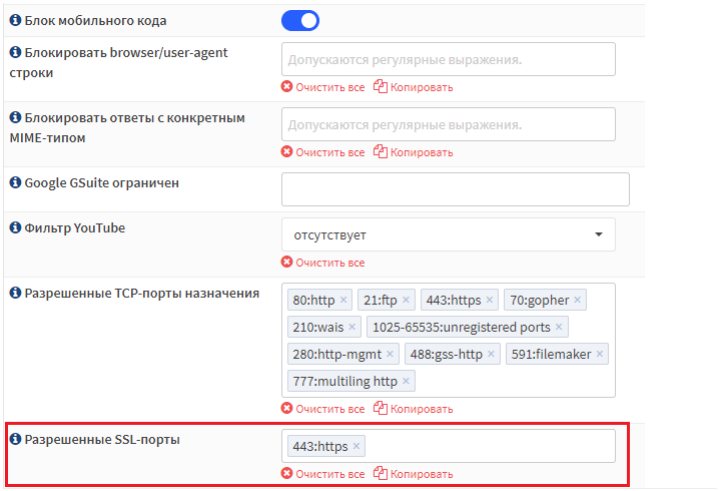


Рис. 982: Разрешенные SSL-порты

Примечание

Пользователь может использовать диапазоны (например, 222-226) и добавлять комментарии с двоеточием (например, 22:ssh)

- нажать кнопку **«Применить»** 

.

Настройки ICAP

Для выполнения настроек ICAP необходимо:

- выбрать из выпадающего списка **«Настройки ICAP»**;

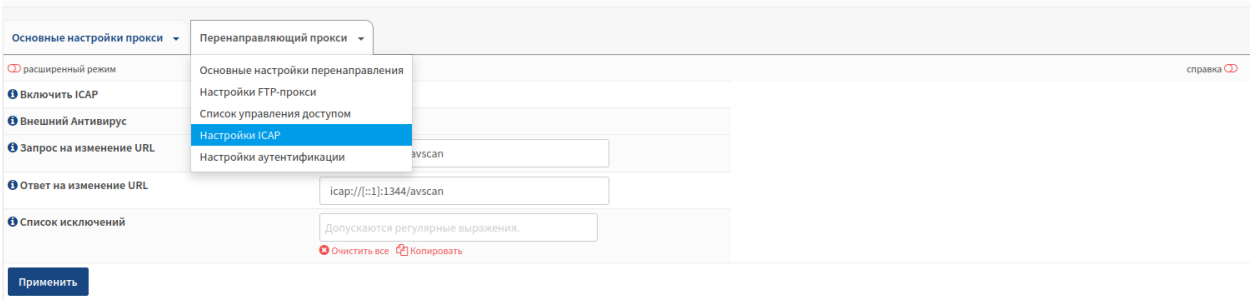


Рис. 983: Переход к настройкам ICAP

- в поле **«Включить ICAP»** установить переключатель в случае необходимости использовать ICAP-сервер для фильтрации или замены содержимого;

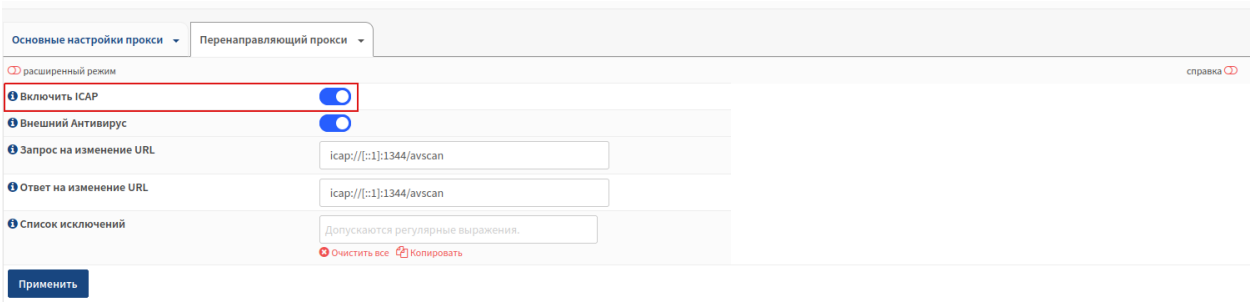


Рис. 984: Включить ICAP

- в поле **«Внешний Антивирус»** установить переключатель в случае необходимости использовать удаленную антивирусную защиту;

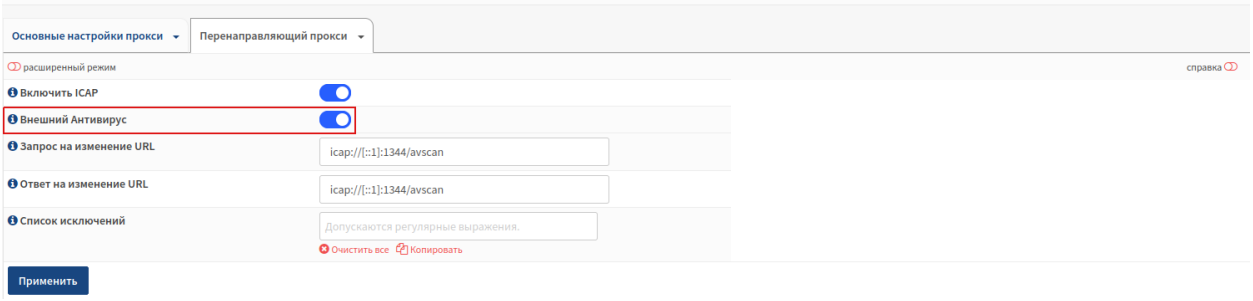


Рис. 985: Внешний Антивирус

- в поле **«Запрос на изменение URL»** (при активной функции **«Внешний Антивирус»**) указать URL, на который должны посылаться REQMOD запросы;

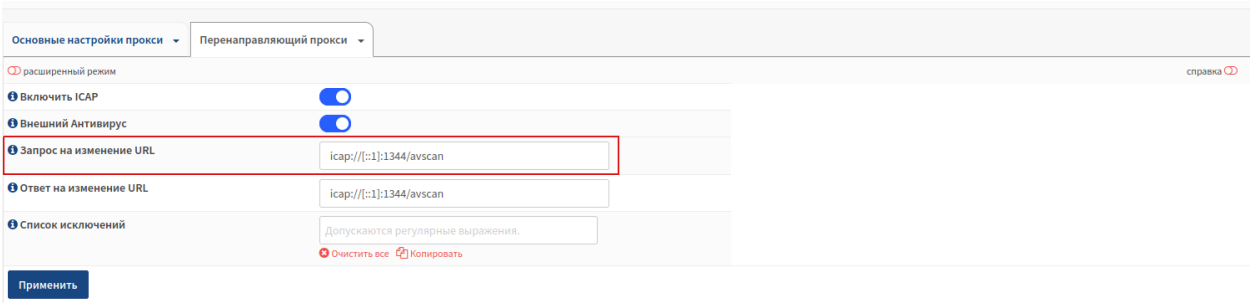


Рис. 986: Запрос на изменение URL

- в поле **«Ответ на изменение URL»** (при активной функции **«Внешний Антивирус»**) указать URL, на который должны посылаться REQMOD ответы;

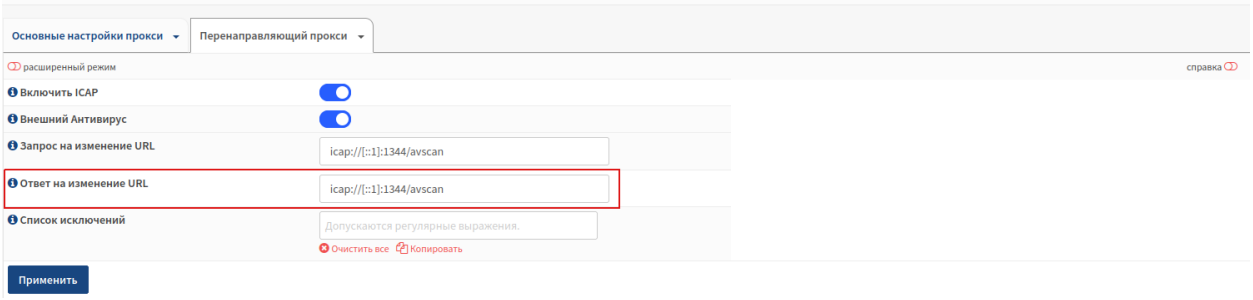


Рис. 987: Ответ на изменение URL

- в поле **«Выбор антивируса»** (при отключенной функции **«Внешний Антивирус»**) выбрать из выпадающего списка встроенный антивирус;

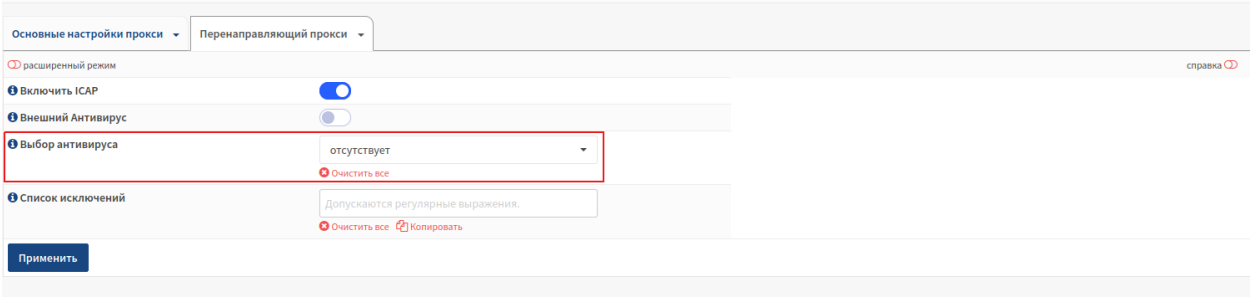


Рис. 988: Выбор антивируса

- в поле **«Список исключений»** указать целевые домены списка исключений;

Примечание

Пользователь может использовать регулярное выражение, использовать запятую или нажать Enter для нового элемента

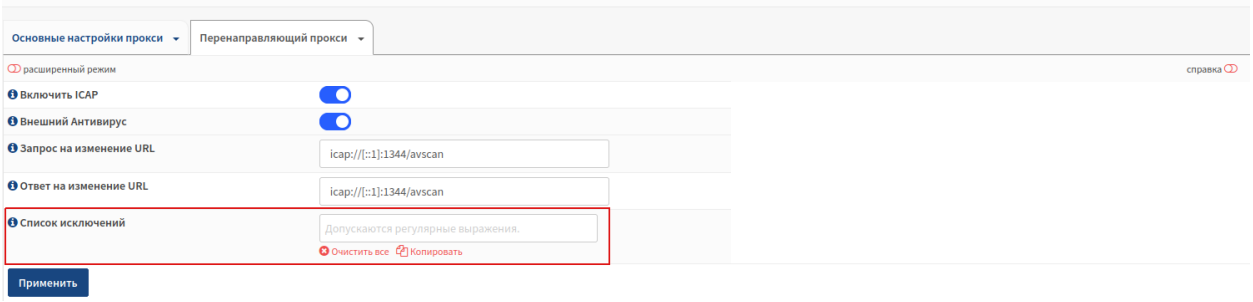


Рис. 989: Список исключений

Примечание

Примеры: «mydomain.com» соответствует *«.mydomain.com»; «https://([a-zA-Z]+).mydomain.»* соответствует *«http(s)://textONLY.mydomain.»*; «.gif$» совпадает с «*.gif», но не с «*.giftest»; «[0-9]+.gif$» совпадает с «123.gif», но не с «test.gif»

- нажать кнопку **«Применить»** 

.

Для включения режима расширенных настроек необходимо установить переключатель.

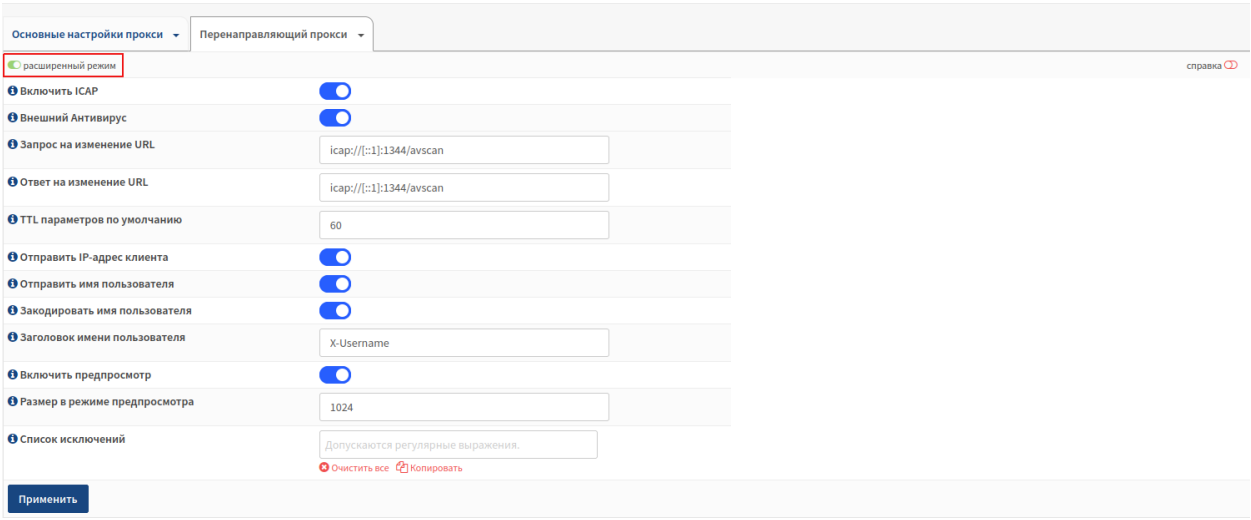


Рис. 990: Включение расширенных настроек

В режиме расширенных настроек необходимо:

- в поле **«TTL параметров по умолчанию»** указать время по умолчанию;
- в поле **«Отправить IP-адрес клиента»** установить переключатель в случае необходимости отправить IP-адрес клиента на ICAP-сервер;

Совет

Это параметр может быть полезен, если вы хотите отфильтровать трафик по IP-адресам

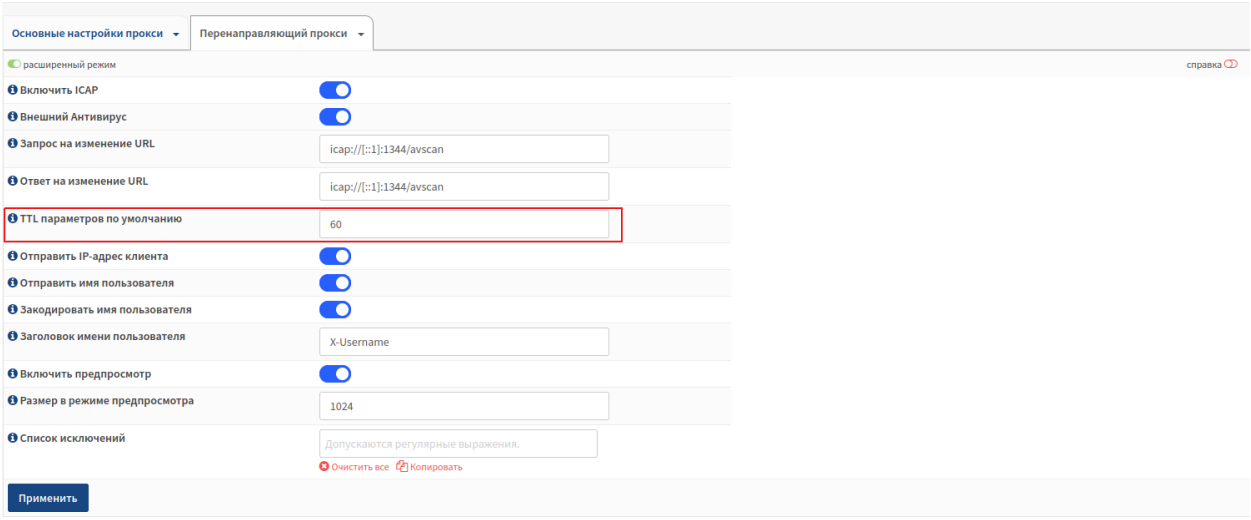


Рис. 991: TTL параметров по умолчанию

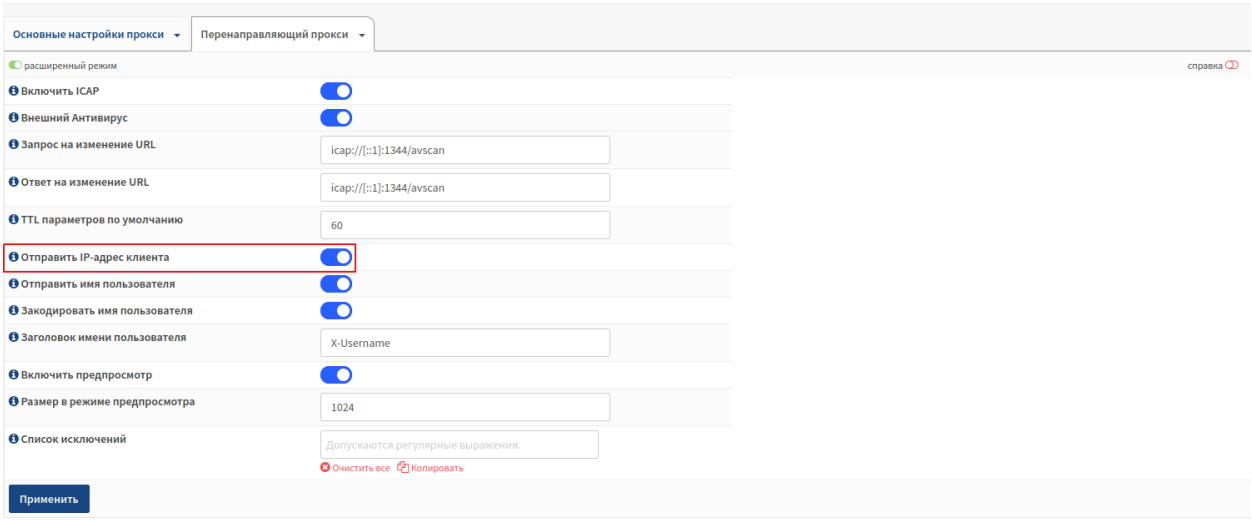


Рис. 992: Отправить IP-адрес клиента

- в поле **«Отправить имя пользователя»** установить переключатель в случае необходимости отправить имя пользователя клиента на ICAP-сервер;

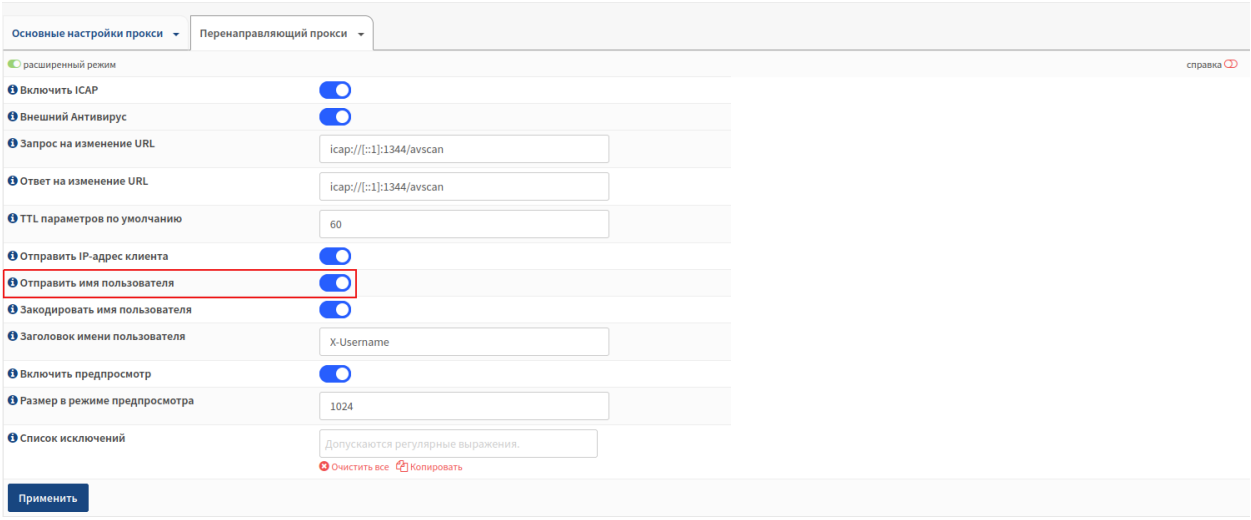


Рис. 993: Отправить имя пользователя

Совет

Это параметр может быть полезен, если вы хотите фильтровать трафик на основе имен пользователей

Примечание

Для использования имен пользователей требуется аутентификация

- в поле **«Закодировать имя пользователя»** установить переключатель в случае необходимости закодировать имя пользователя;
- в поле **«Заголовок имени пользователя»** указать заголовок, который должен использоваться для отправки имени пользователя на сервер;
- в поле **«Включить предпросмотр»** установить переключатель в случае необходимости включить предпросмотр;

Примечание

При использовании параметра **«Включить предпросмотр»** только часть данных отправляется на ICAP-сервер

Внимание

Установка этого параметра может увеличить производительность

- в поле **«Размер в режиме предпросмотра»** указать размер превью, которое отправляется на

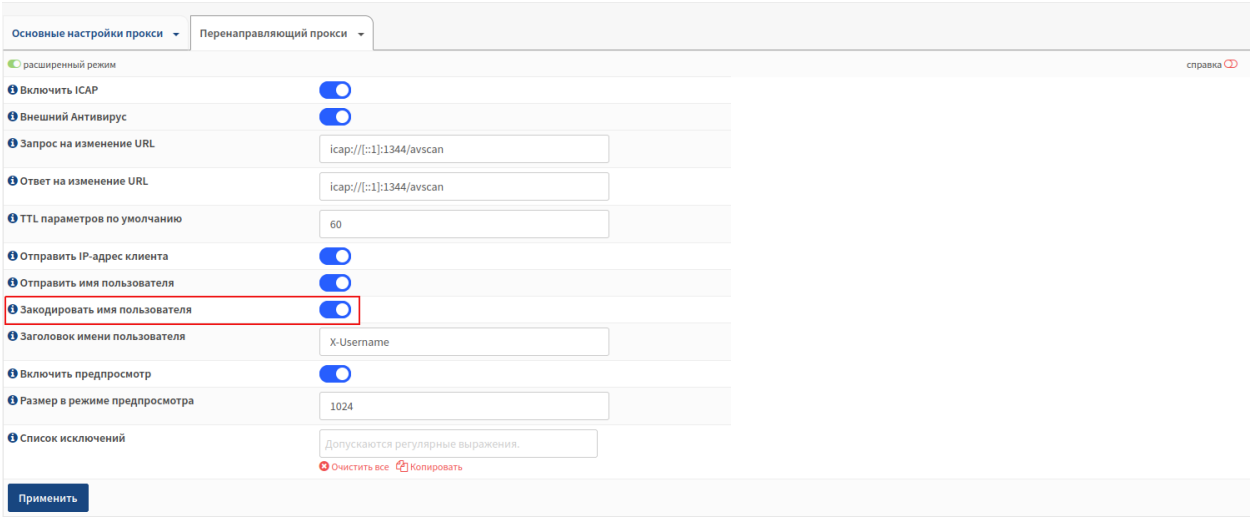


Рис. 994: Закодировать имя пользователя

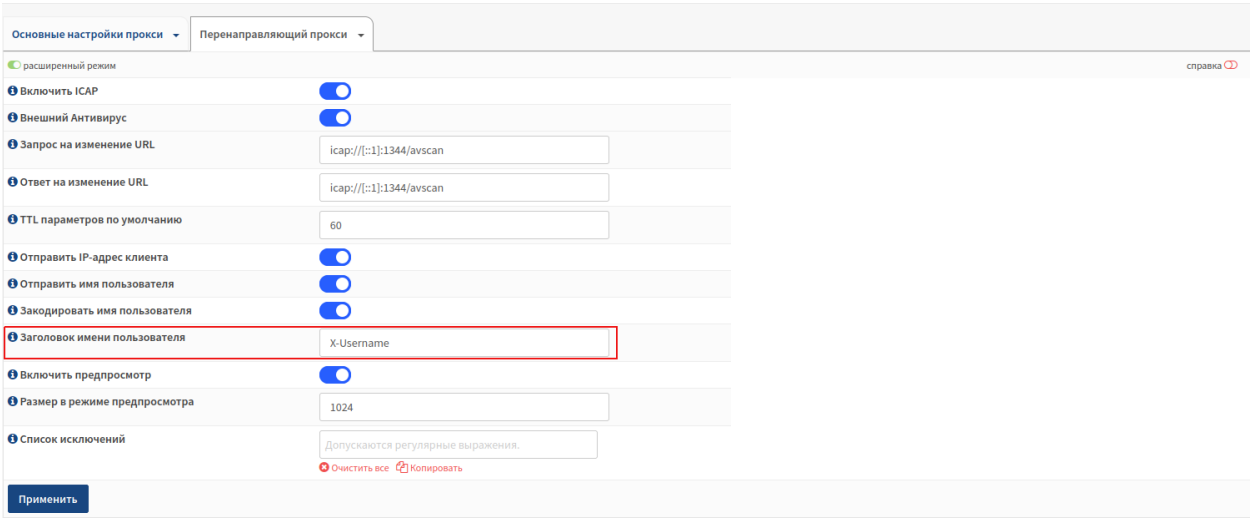


Рис. 995: Заголовок имени пользователя

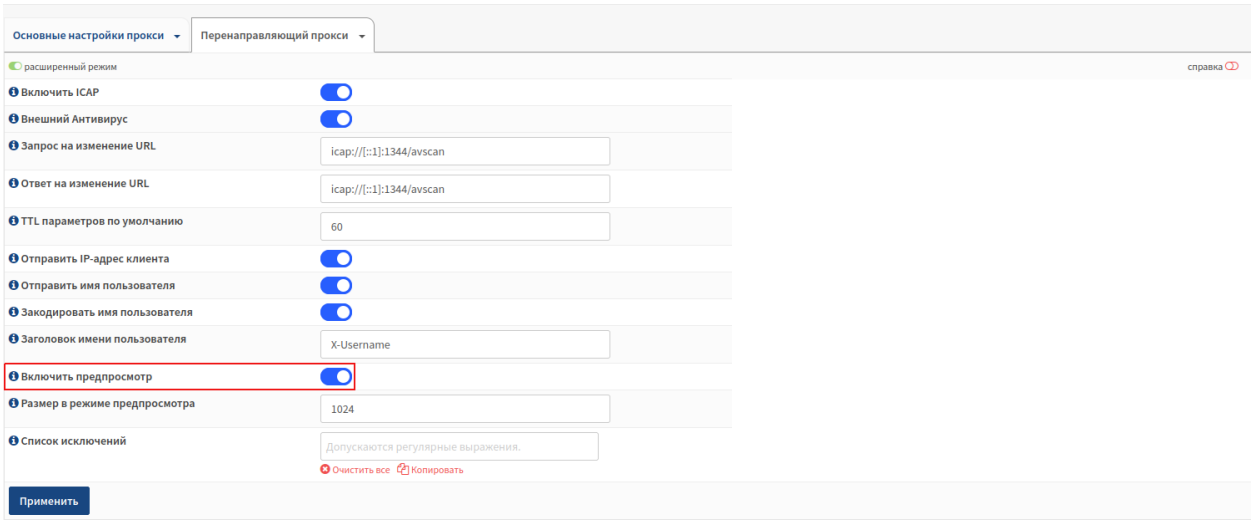


Рис. 996: Включить предпросмотр

ICAP-сервер;

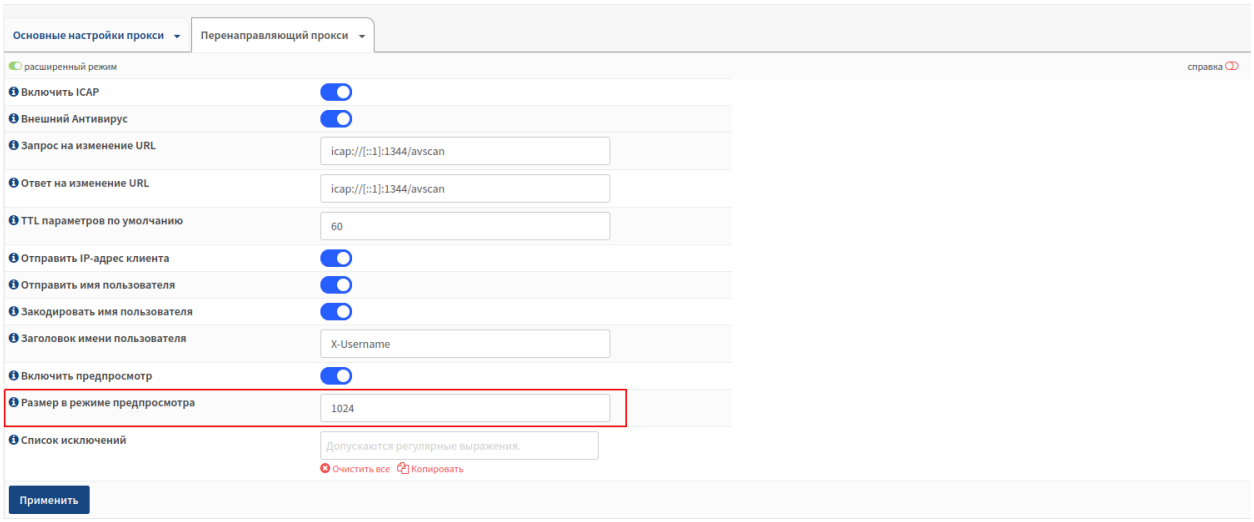


Рис. 997: Размер в режиме предпросмотра

- нажать кнопку **«Применить»** 

.

Настройки аутентификации

Для выполнения настроек аутентификации необходимо:

- выбрать из выпадающего списка **«Настройки аутентификации»**;

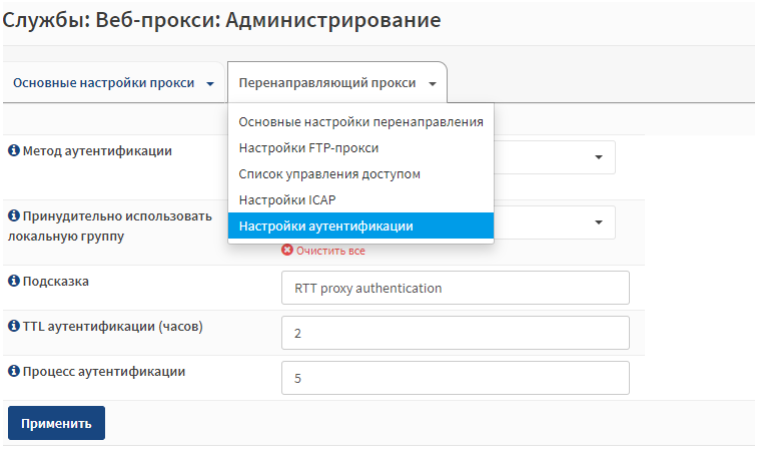


Рис. 998: Переход к настройкам аутентификации

- в поле **«Метод аутентификации»** выбрать из выпадающего списка метод аутентификации;

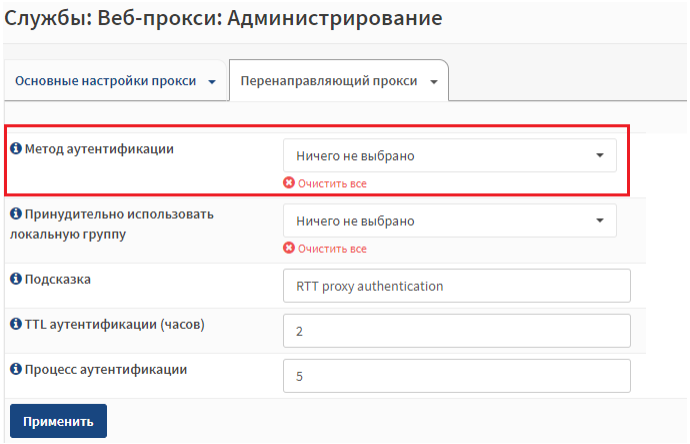


Рис. 999: Метод аутентификации

- в поле **«Принудительно использовать локальную группу»** выбрать из выпадающего списка необходимую группу, пользователям которой необходимо разграничить доступ;;

> **Примечание**
>
> Пользователи (или ваучеры), которые не администрируются локально, будут отклонены при использовании этой опции

- в поле **«Подсказка»** указать подсказку, которая будет отображаться в окне запроса аутентификации;
- в поле **«TTL аутентификации (часов)»** указать как долго (в часах) прокси-сервер предполагает, что проверенная извне комбинация имени пользователя и пароля действительна (время

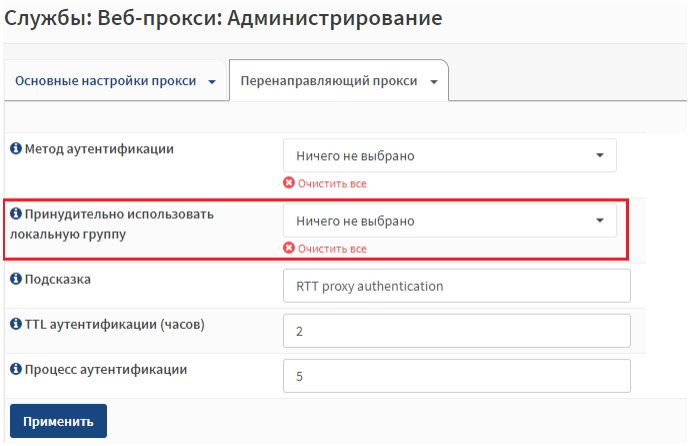


Рис. 1000: Принудительно использовать локальную группу

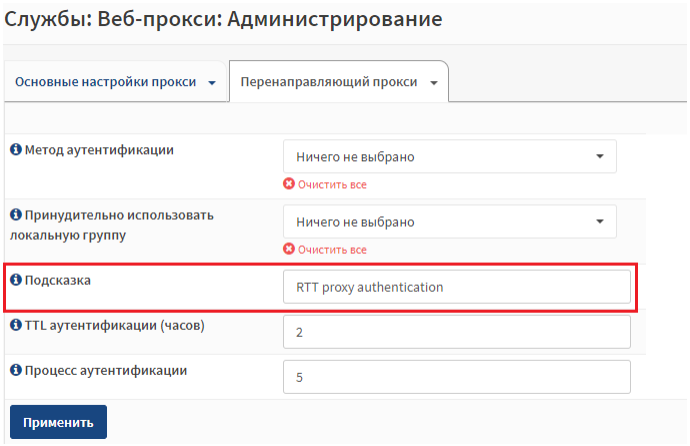


Рис. 1001: Подсказка

жизни);

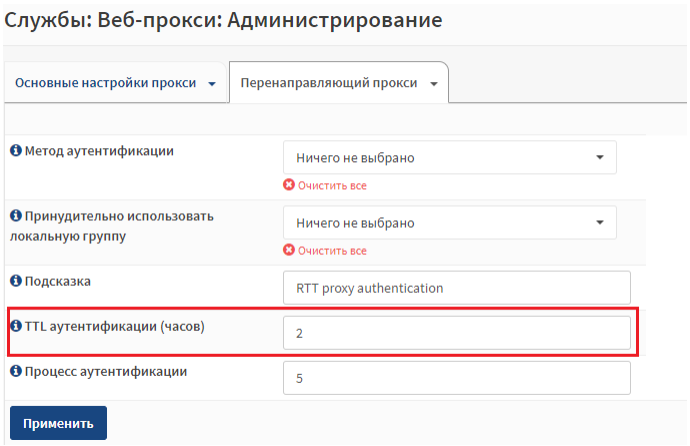


Рис. 1002: TTL аутентификации (часов)

Примечание

Когда TTL истечет, пользователю снова будет предложено ввести учетные данные

- в поле **«Процесс аутентификации»** указать количество процессов аутентификатора, которые могут быть запущены одновременно;

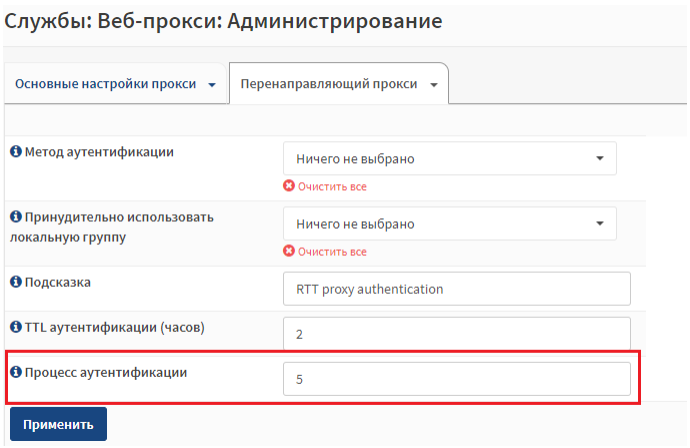


Рис. 1003: Процесс аутентификации

- нажать кнопку **«Применить»** 

.

Журнал кэша

Раздел **«Журнал кэша»** содержит журнал кэша.

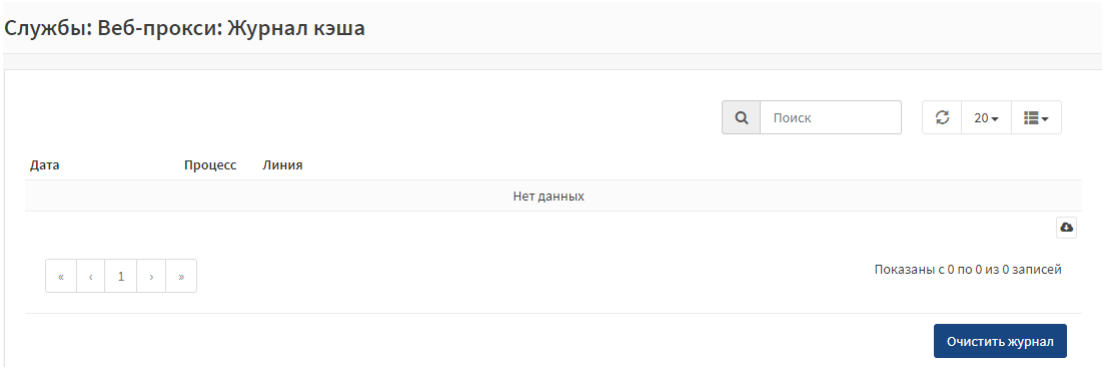


Рис. 1004: Журнал кэша

С помощью фильтров можно ограничить или расширить данные журнала.

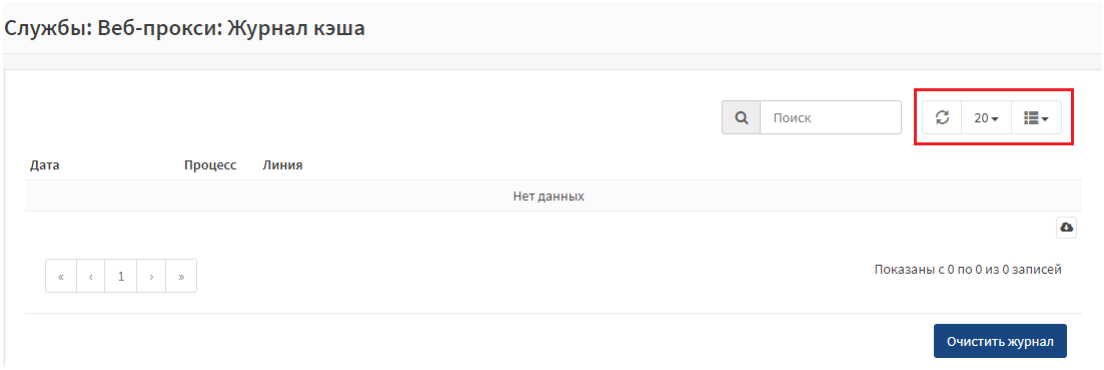


Рис. 1005: Фильтры журнала кэша

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

Журнал доступа

Раздел **«Журнал доступа»** содержит журнал доступа

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

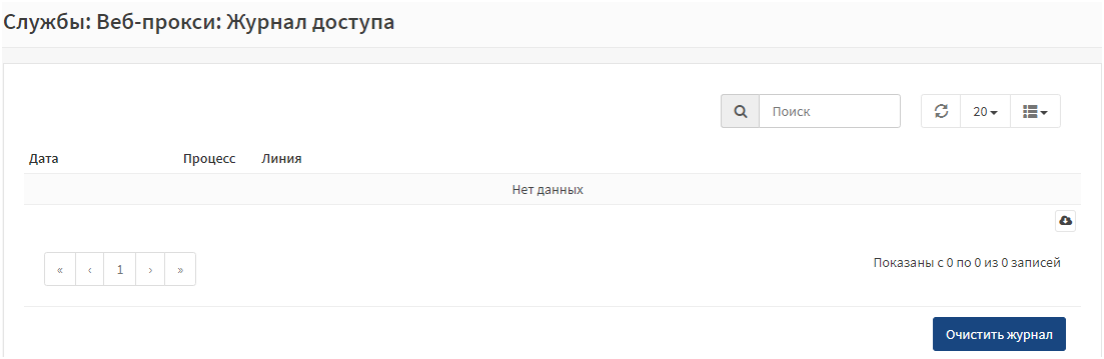


Рис. 1006: Журнал доступа

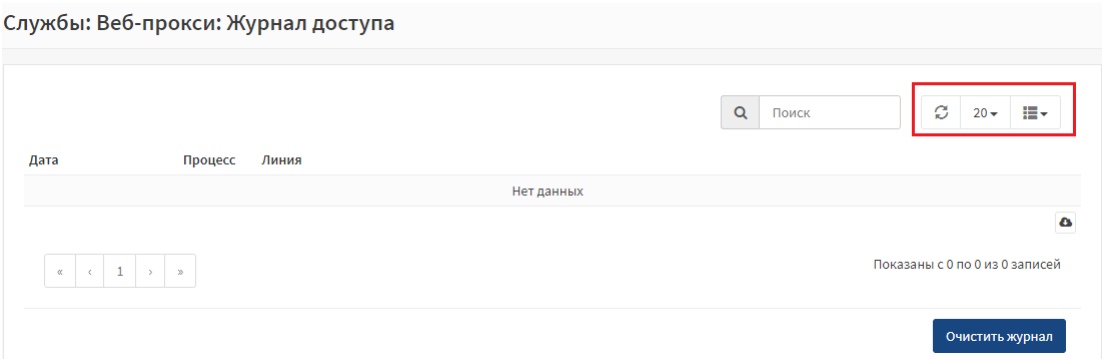


Рис. 1007: Фильтры журнала доступа

Store Log

Раздел **«Store Log»** содержит журнал хранения.

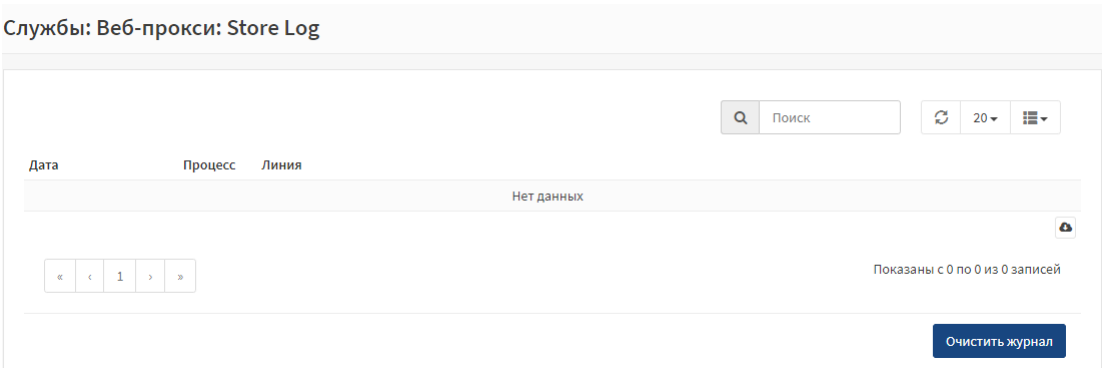


Рис. 1008: Журнал хранения

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

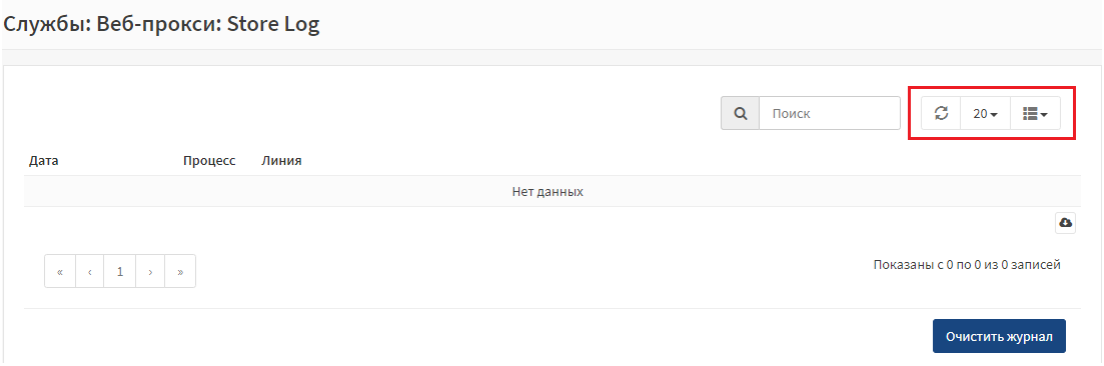


Рис. 1009: Фильтры журнала хранения

2.7.8.7 DHCPv4

Для перехода к настройкам сервера DHCPv4 на примере интерфейса LAN2 необходимо:

- нажать на вкладку **«Службы»** - **«DHCPv4»** - **«[LAN2]»**, расположенную в левой части списка объектов управления;

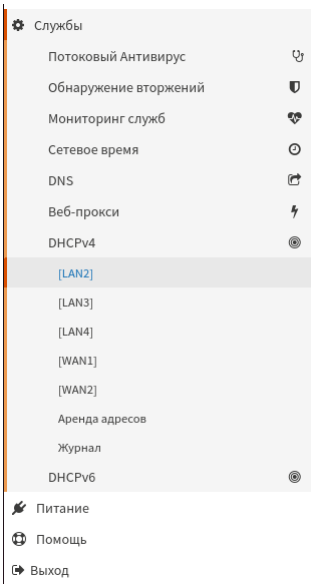


Рис. 1010: Переход к настройкам сервера DHCPv4 на примере интерфейса LAN2

Для перехода к просмотру аренды адресов необходимо:

- нажать на вкладку **«Службы»** - **«DHCPv4»** - **«Аренда адресов»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала системы обнаружения вторжений необходимо:

- нажать на вкладку **«Службы»** - **«DHCPv4»** - **«Журнал»**, расположенную в левой части списка объектов управления;

Для запуска службы необходимо нажать кнопку  , находящуюся в верхнем правом углу окна.

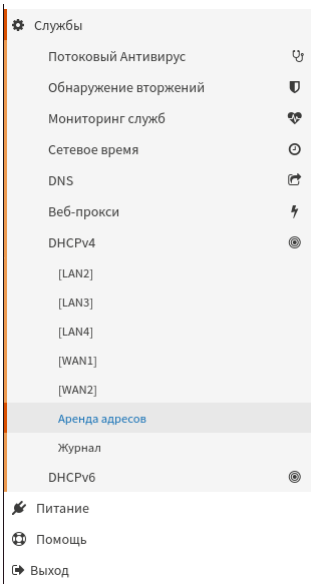


Рис. 1011: Переход к просмотру аренды адресов

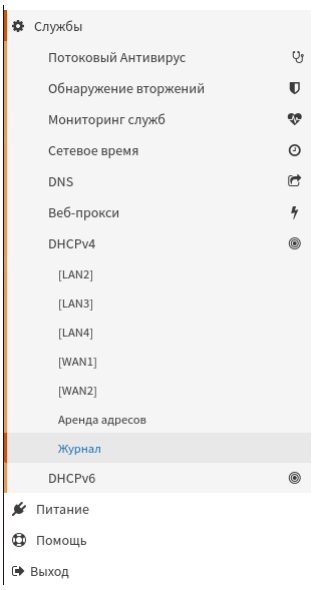


Рис. 1012: Переход к просмотру журнала

[LAN2]

Для выполнения настроек сервера DHCPv4 для интерфейса LAN2 необходимо:

- в поле **«Включить»** установить переключатель в случае необходимости включения сервера DHCPv4 для интерфейса LAN2;

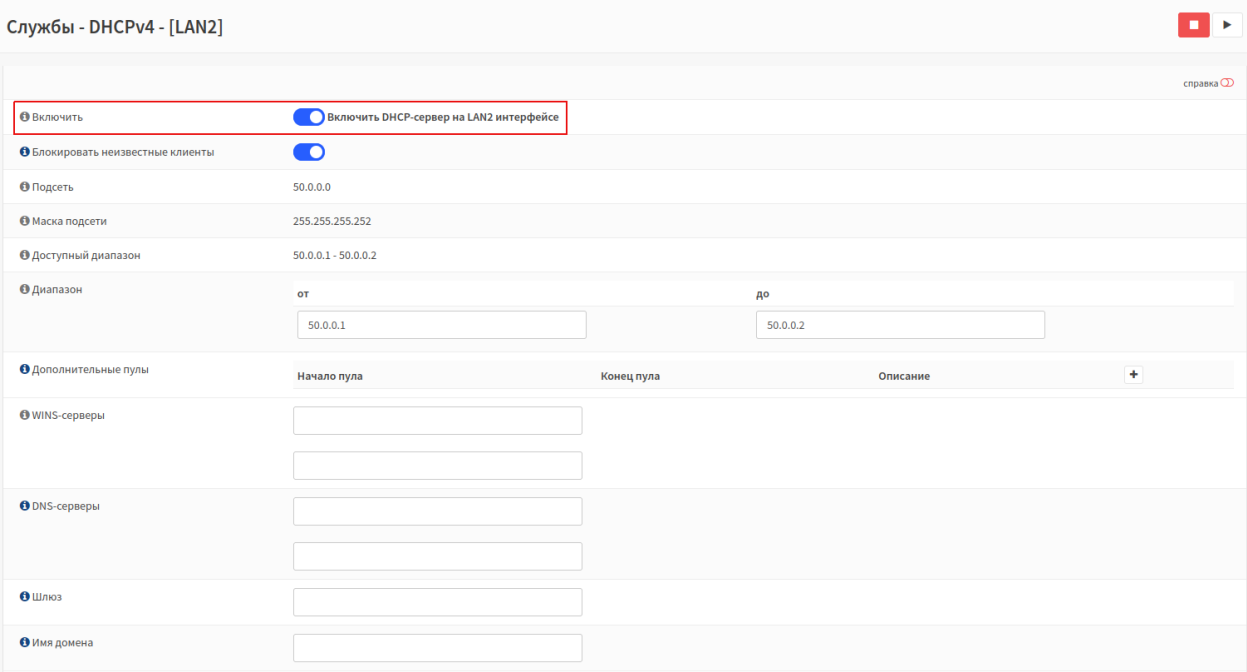


Рис. 1013: Включение сервера

- в поле **«Блокировать неизвестные клиенты»** установить переключатель, чтобы только клиенты, определенные ниже, получали IP-адреса в аренду от этого сервера;
- в полях **«Подсеть»**, **«Маска подсети»**, **«Доступный диапазон»** представлена информация об интерфейсе;
- в поле **«Диапазон»** задать диапазон адресов внутри подсети;

в случае необходимости задать дополнительные пулы адресов внутри подсети, которые не входят в указанный выше диапазон, в поле **«Дополнительный диапазон»** следует нажать кнопку  .

В открывшемся окне необходимо:

- в поле **«Описание»** задать краткое описание пула;
- в поле **«Блокировать неизвестные клиенты»** установить переключатель, чтобы только клиенты, определенные ниже, получали IP-адреса в аренду от этого сервера
- в полях **«Подсеть»**, **«Маска подсети»**, **«Доступный диапазон»** представлена информация об интерфейсе;
- в поле **«Диапазон»** задать диапазон адресов внутри подсети;
- в поле **«WINS-серверы»** задать IP адрес этого интерфейса, если служба WINS включена или настроены глобальные WINS-серверы;

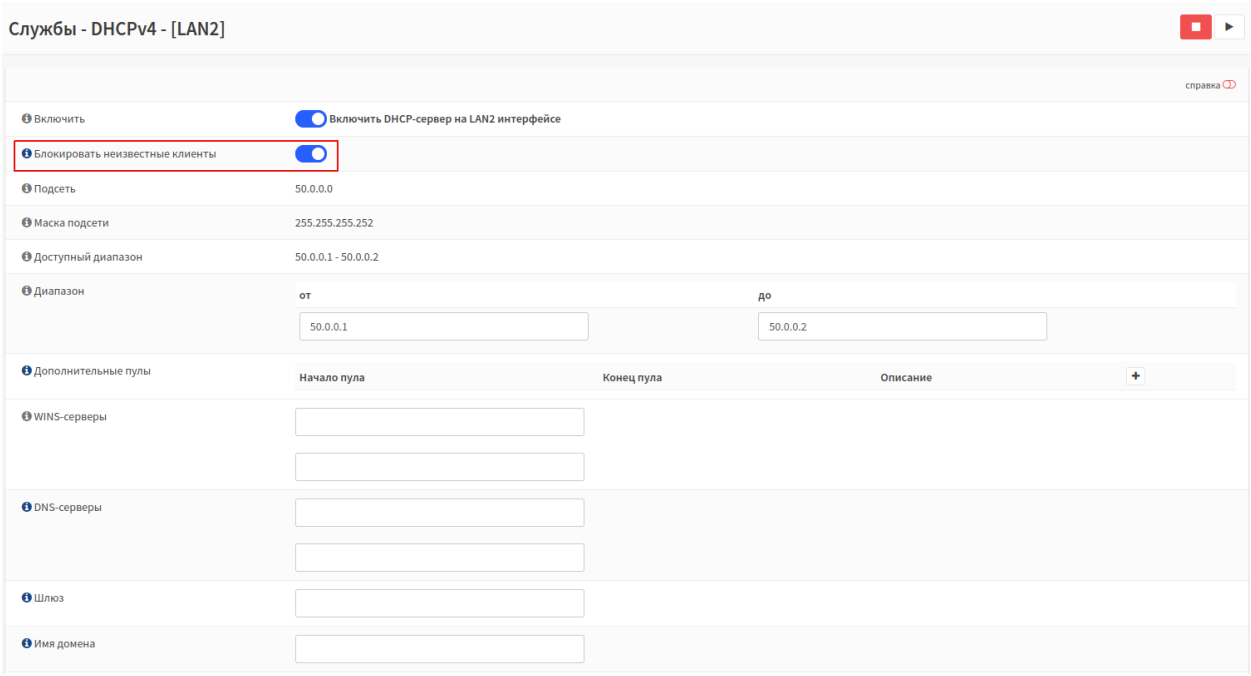


Рис. 1014: Блокирование неизвестных клиентов

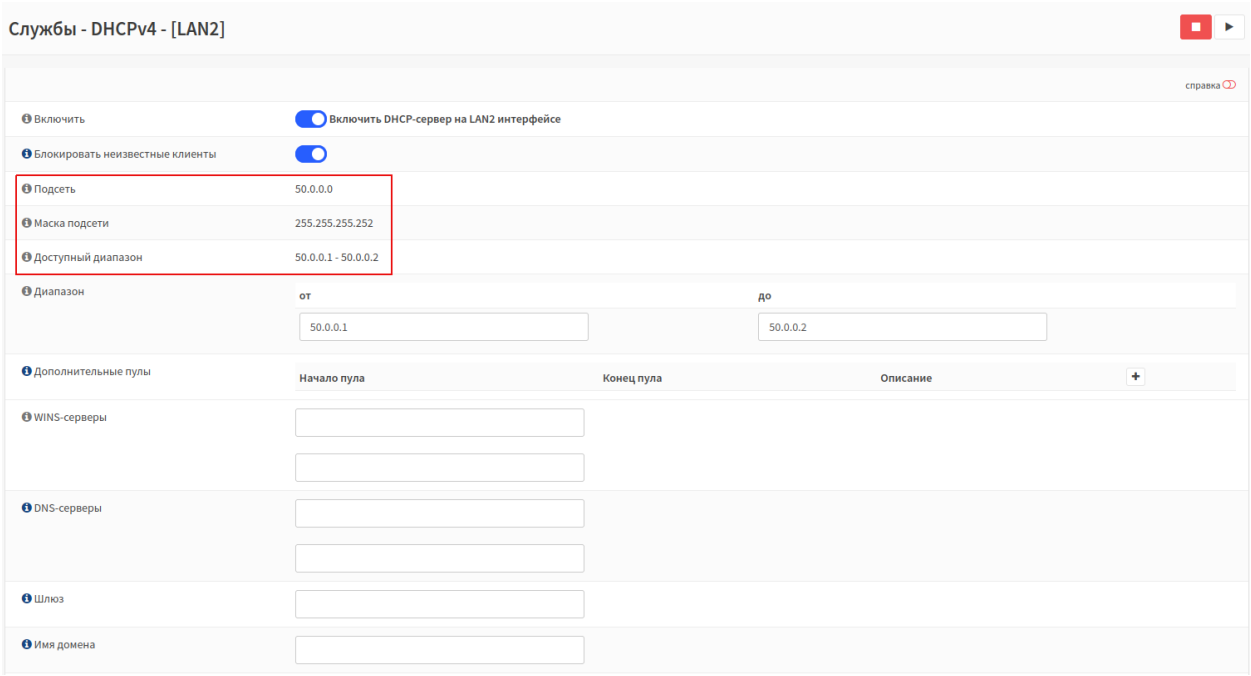


Рис. 1015: Параметры сервера

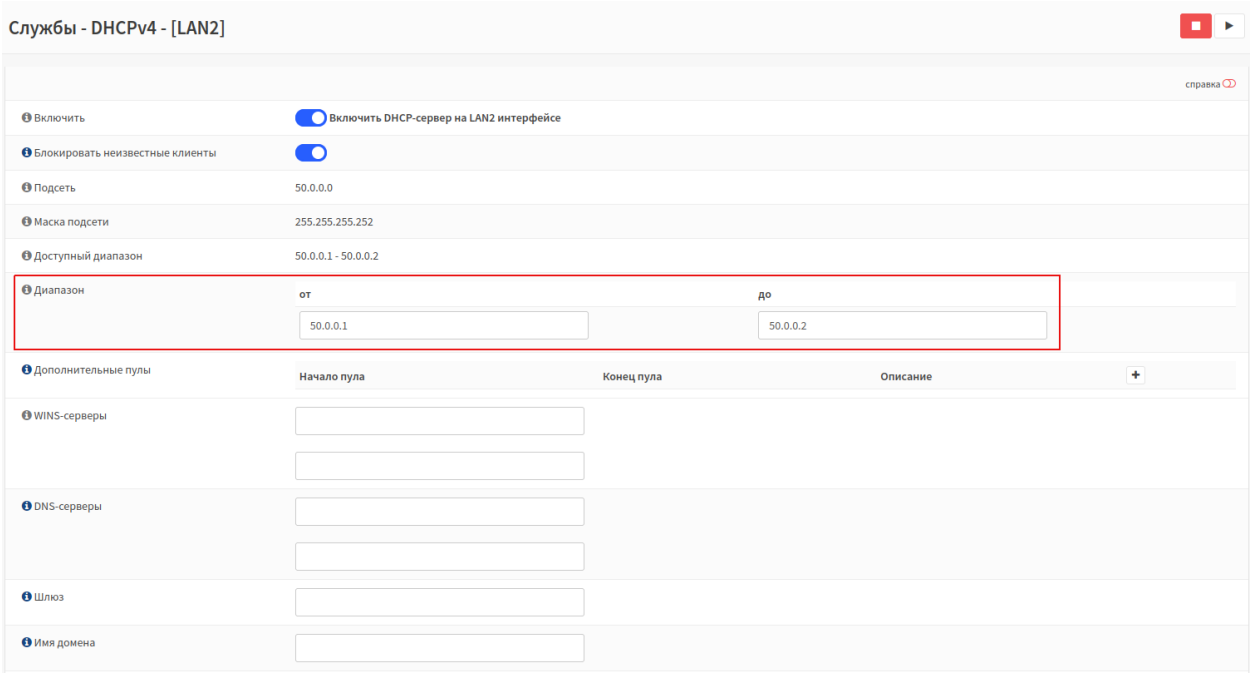


Рис. 1016: Установка диапазона адресов

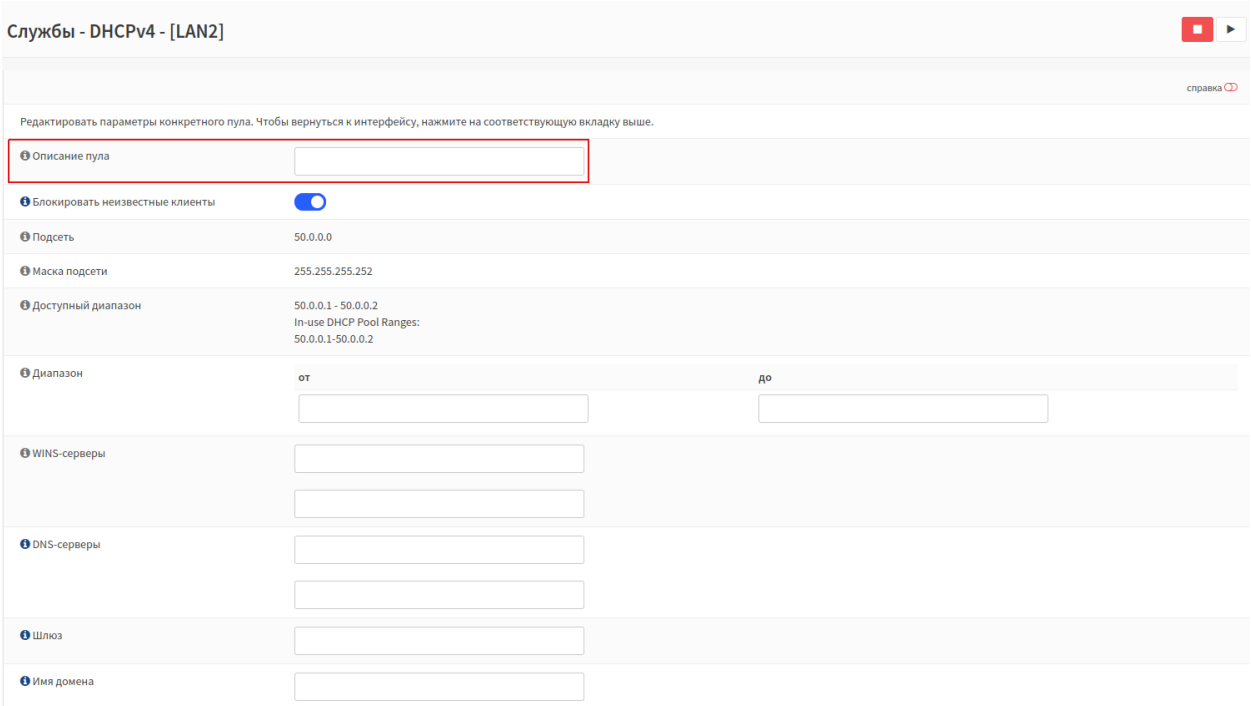


Рис. 1017: Описание пула

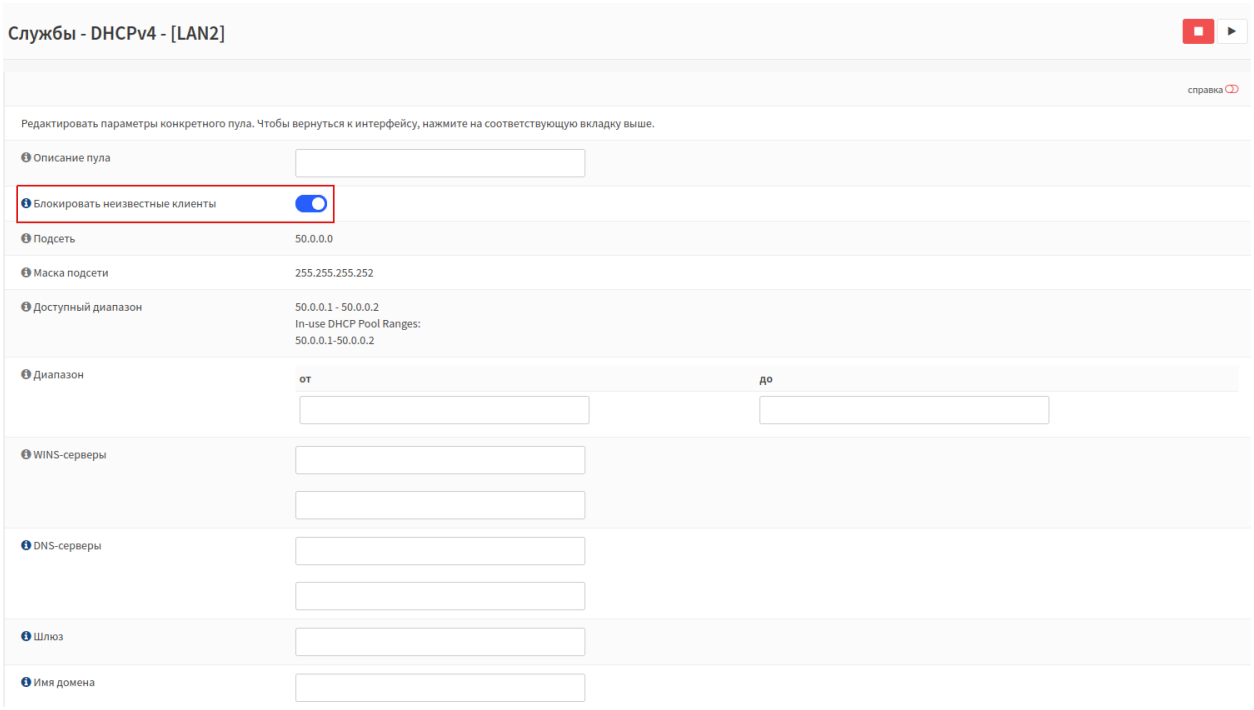


Рис. 1018: Блокирование неизвестных клиентов

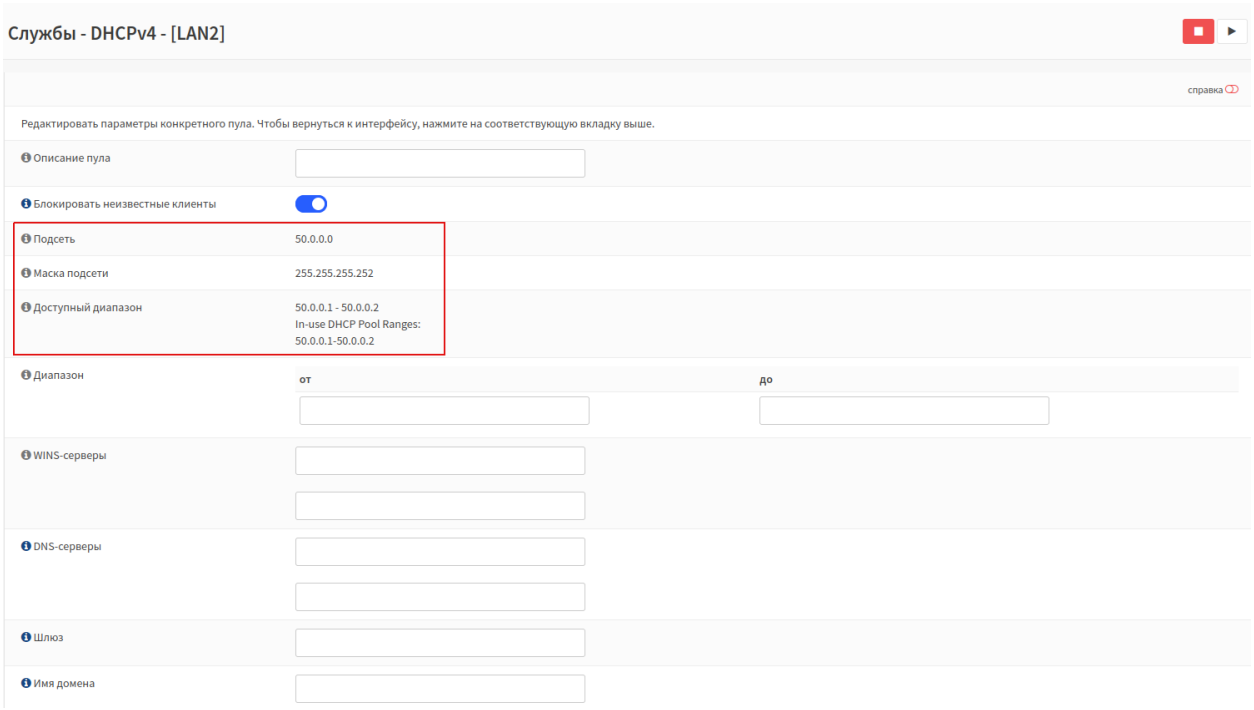


Рис. 1019: Параметры сервера

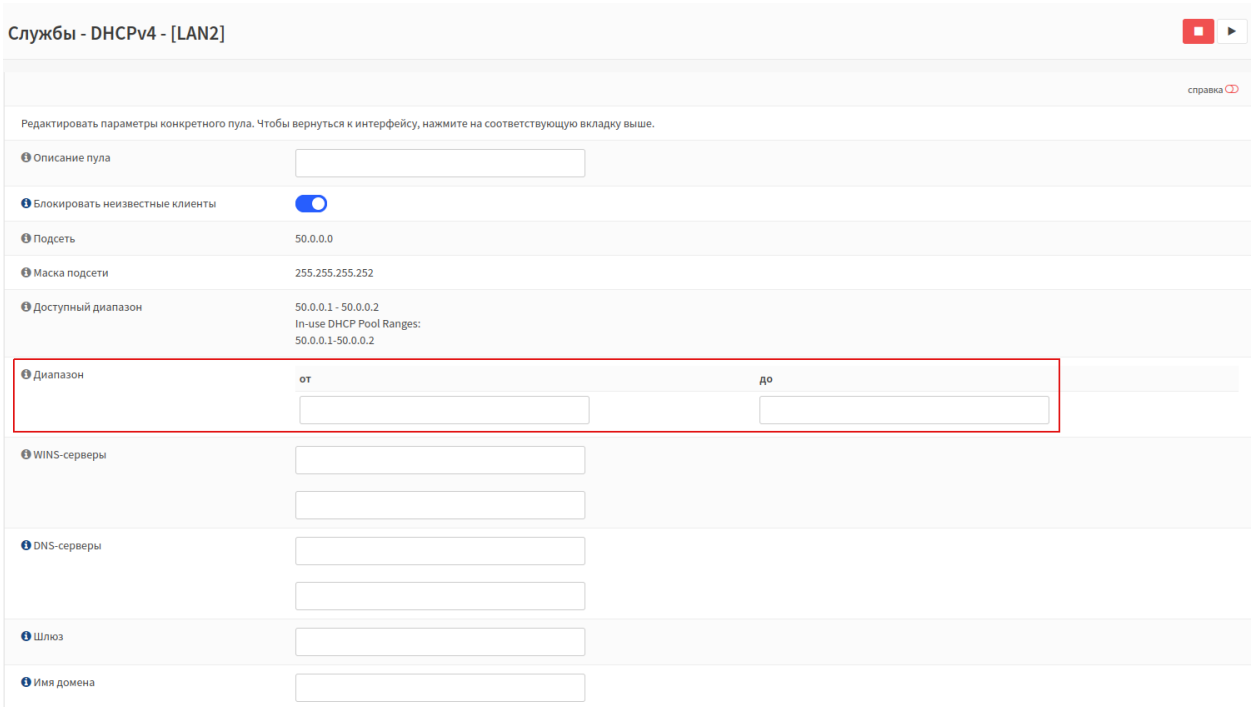


Рис. 1020: Установка диапазона адресов

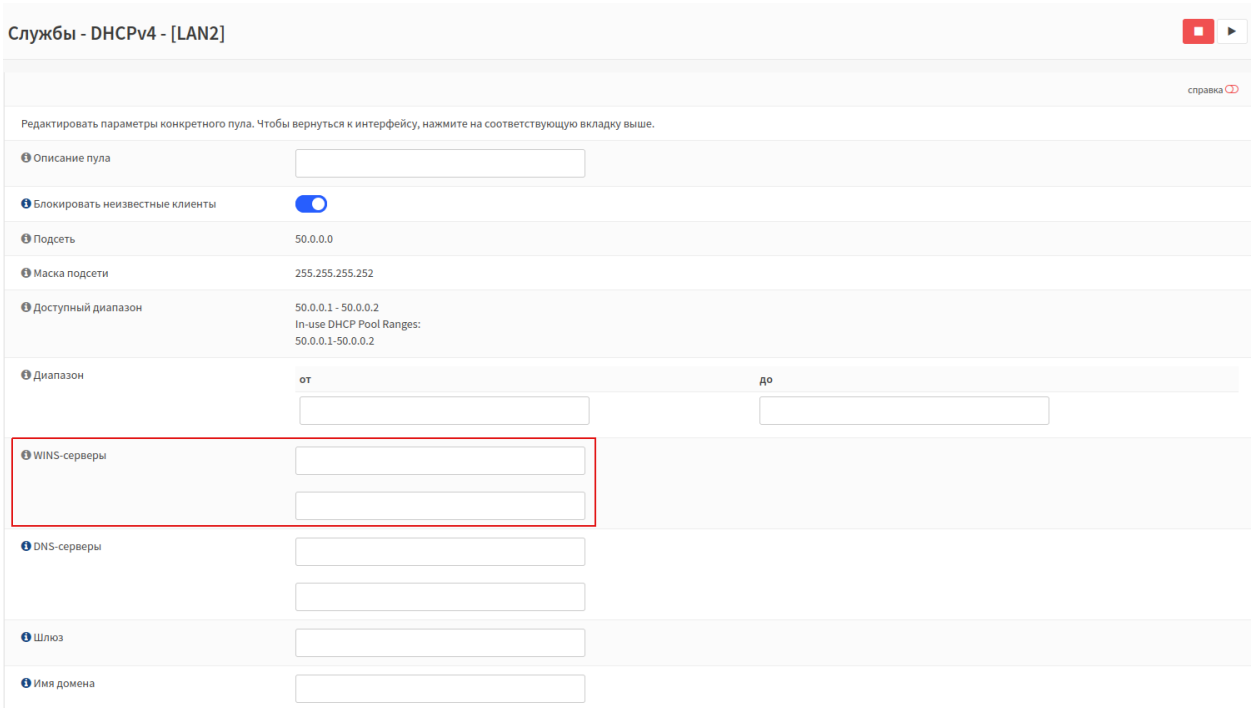


Рис. 1021: Настройка WINS-сервера

Совет

Оставьте пустым, чтобы использовать системные WINS-серверы по умолчанию

- в поле **«DNS-серверы»** задать IP адрес этого интерфейса, если служба DNS включена или настроены глобальные DNS-серверы;

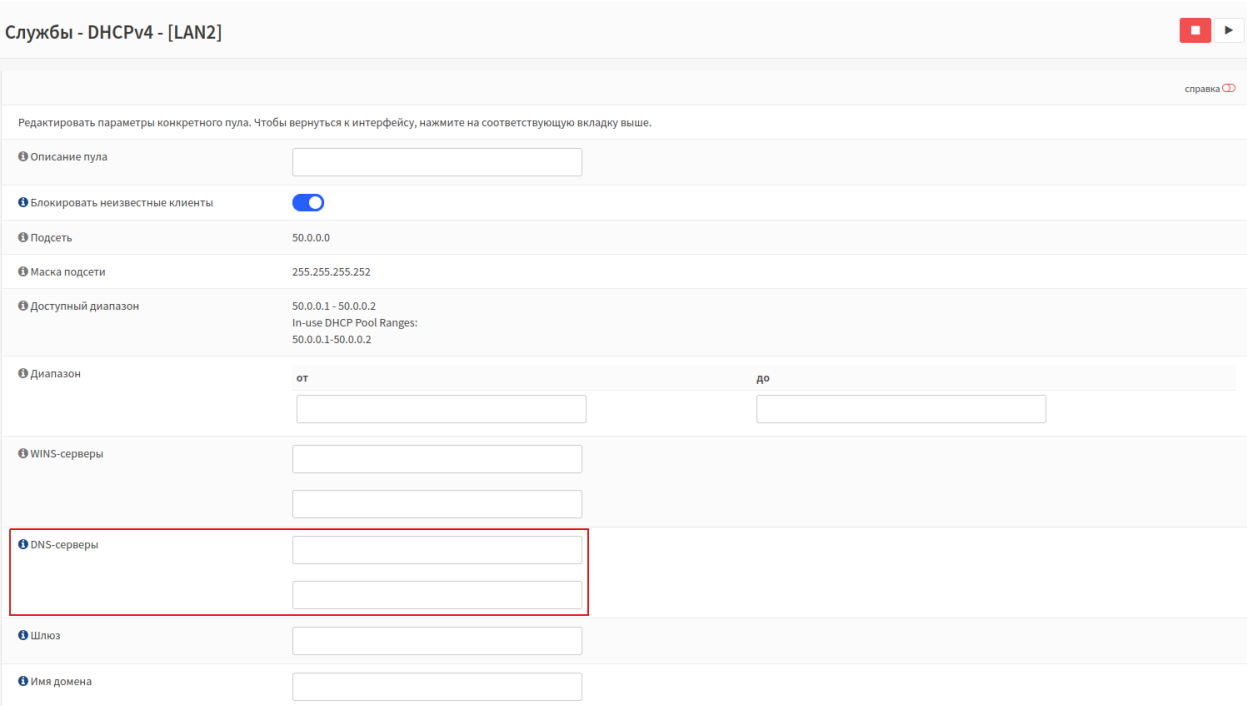


Рис. 1022: Настройка DNS-сервера

Совет

Оставьте пустым, чтобы использовать системные DNS-серверы по умолчанию

- в поле **«Шлюз»** указать альтернативный шлюз, если он не подходит для вашей сети;

Совет

По умолчанию IP-адрес на этом интерфейсе межсетевого экрана используется в качестве шлюза, если действующий (онлайн) шлюз был настроен в **Система - Шлюзы**

Совет

Введите «none» для отсутствия назначения шлюза

- в поле **«Имя домена»** указать альтернативное имя домена;

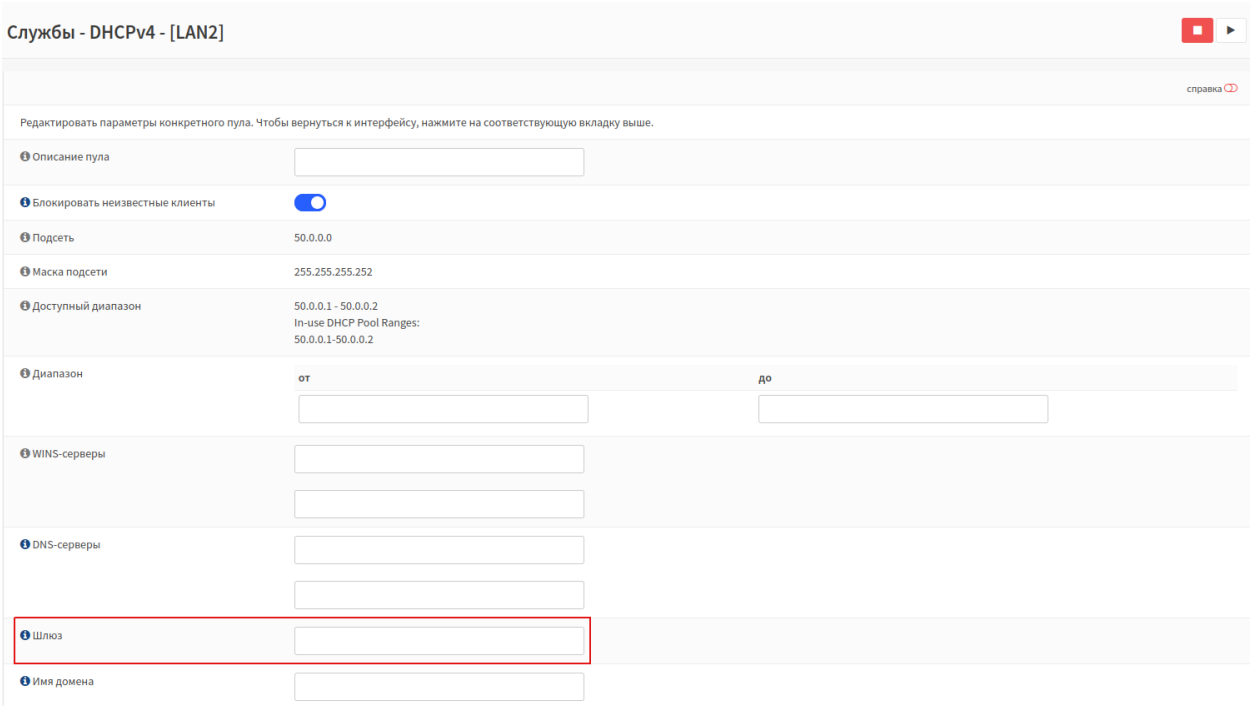


Рис. 1023: Установка шлюза

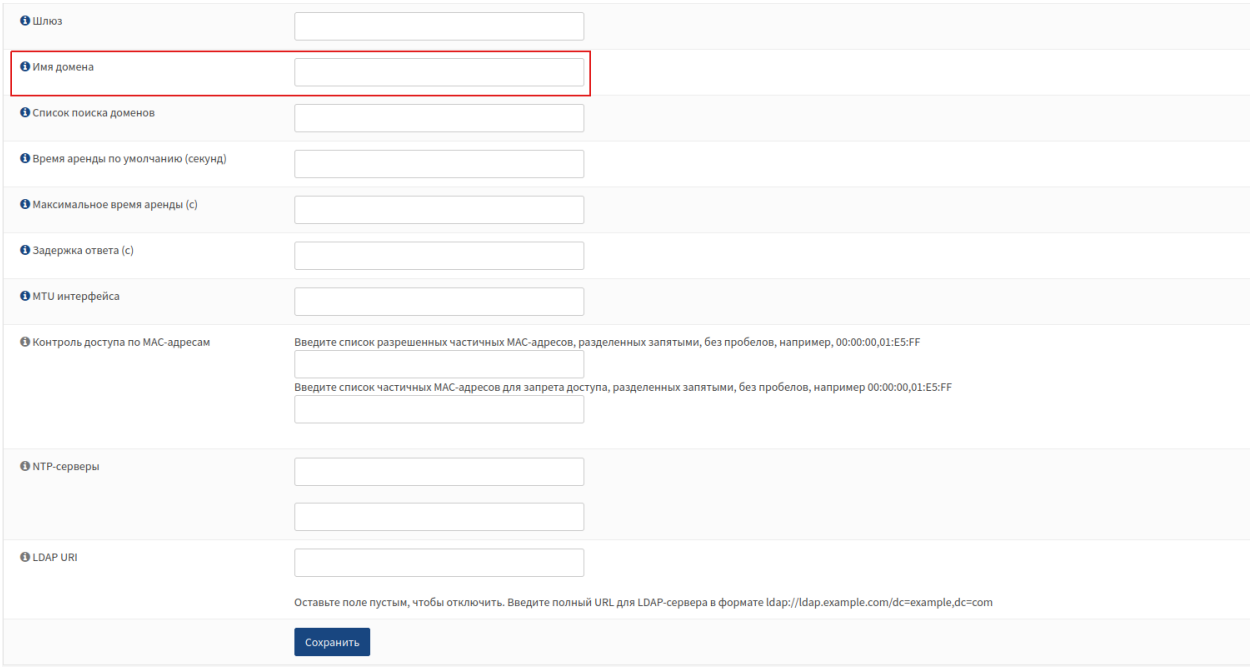


Рис. 1024: Установка имени домена

Совет

По умолчанию в качестве доменного имени используется доменное имя, выданное DHCP

- в поле **«Список поиска доменов»** указать список поиска домена;

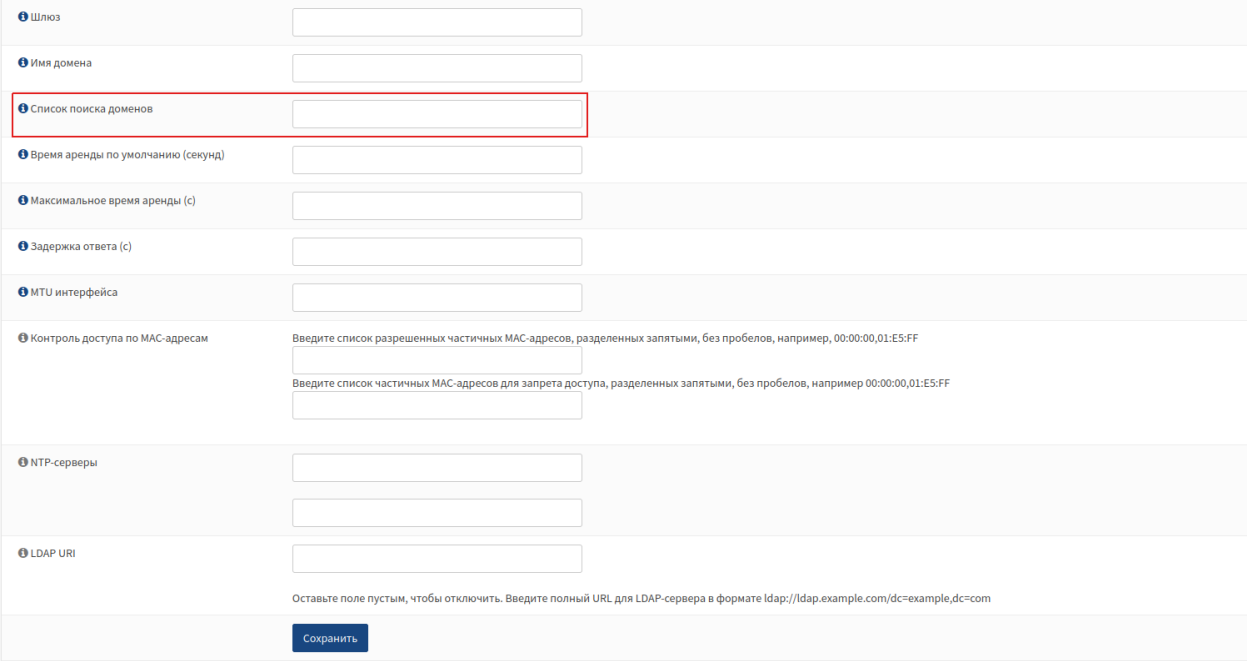


Рис. 1025: Установка списка поиска домена

Совет

Используйте точку с запятой в качестве разделителя

- в поле **«Время аренды по умолчанию (секунд)»** указать время для клиентов, которые не запрашивают конкретное время аренды;

Совет

Значение по умолчанию 7200 секунд

- в поле **«Максимальное время аренды (с)»** указать максимальное время аренды для клиентов, которые запрашивают точное время;

Совет

Значение по умолчанию 86400 секунд

- в поле **«Задержка ответа (с)»** указать минимальное количество секунд с момента, когда клиент начал пытаться получить новую аренду, прежде чем DHCP-сервер ответит на его запрос;

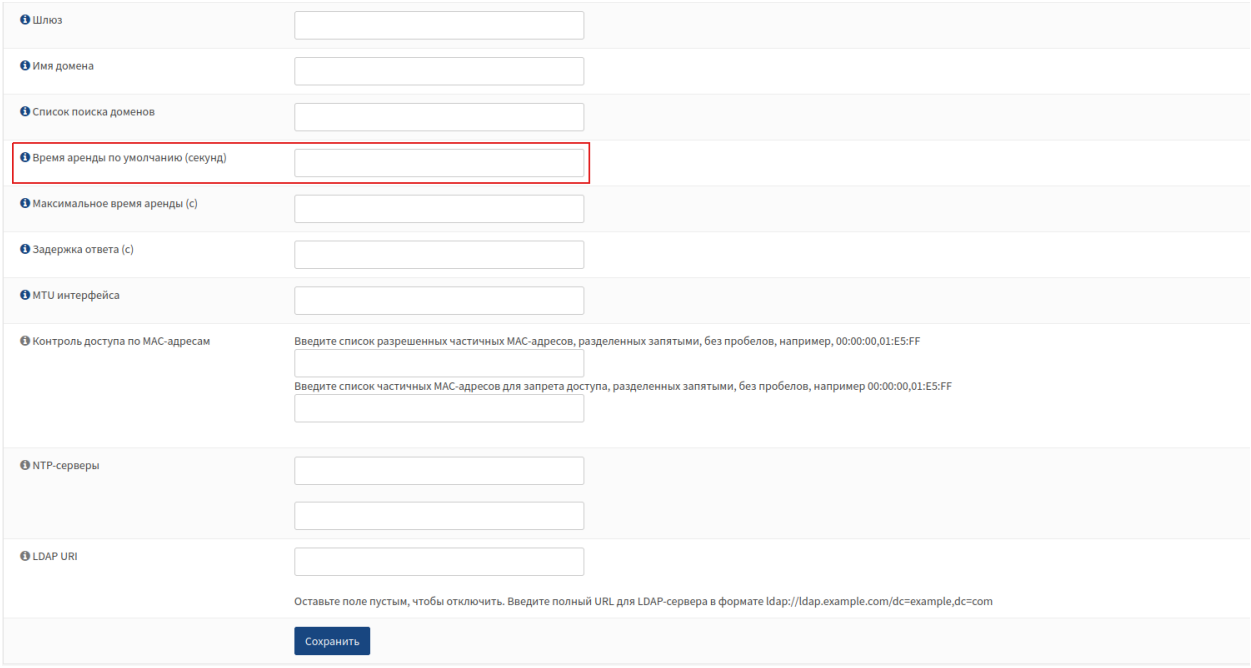


Рис. 1026: Установка времени аренды

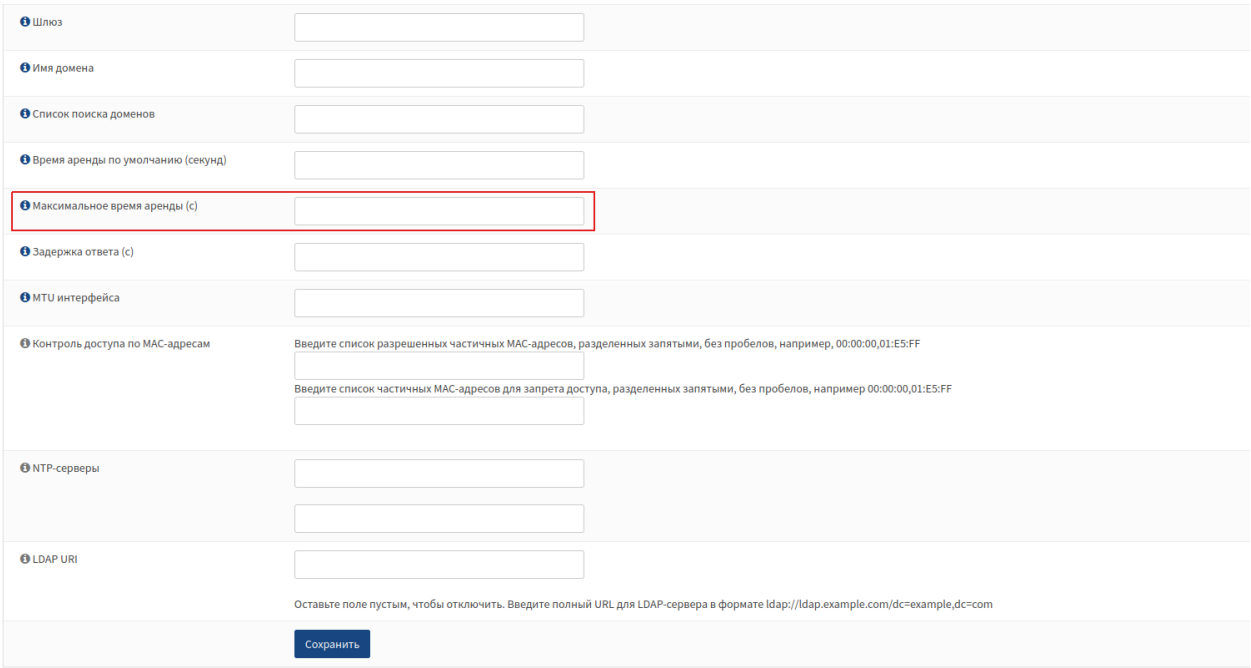


Рис. 1027: Установка максимального времени аренды

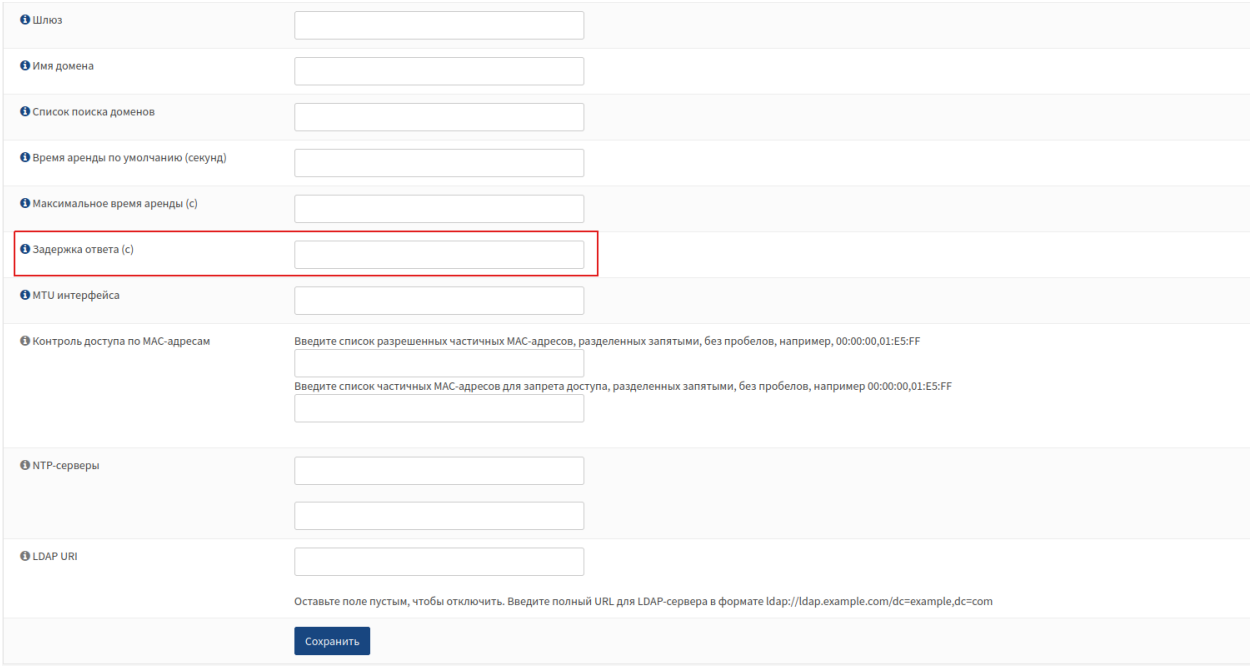


Рис. 1028: Установка задержки ответа

Совет

Значение по умолчанию 0 секунд (без задержки)

- в поле **«MTU интерфейса»** указать значение MTU интерфейса;

Совет

Минимальная легальная величина для MTU: 68

- в поле **«Контроль доступа по MAC-адресам»** установить разрешенные и запрещенные MAC-адреса;
- в поле **«NTP-серверы»** задать IP адрес этого интерфейса, если служба NTP включена или настроены глобальные NTP-серверы;

Совет

Оставьте пустым, чтобы использовать системные NTP-серверы по умолчанию

- в поле **«LDAP URI»** задать полный URL для LDAP-сервера в формате ldap://ldap.example.com/dc=example,dc=com;

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

- в поле **«WINS-серверы»** задать IP адрес этого интерфейса, если служба WINS включена или настроены глобальные WINS-серверы;

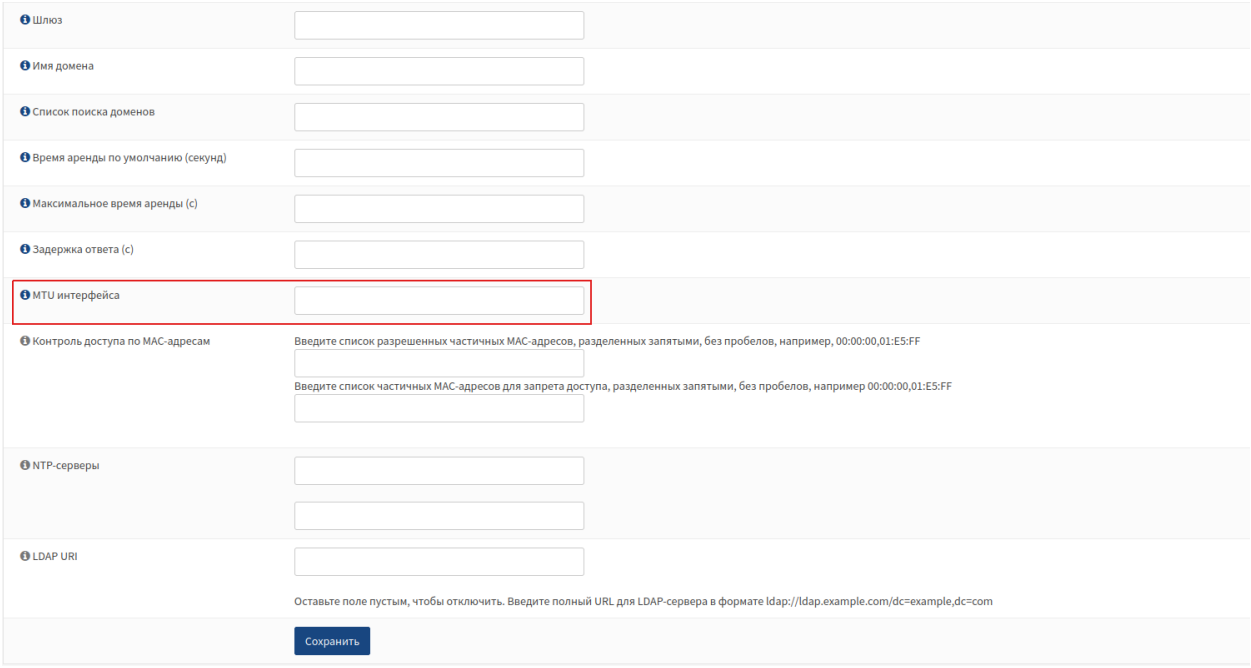


Рис. 1029: Установка значения MTU интерфейса

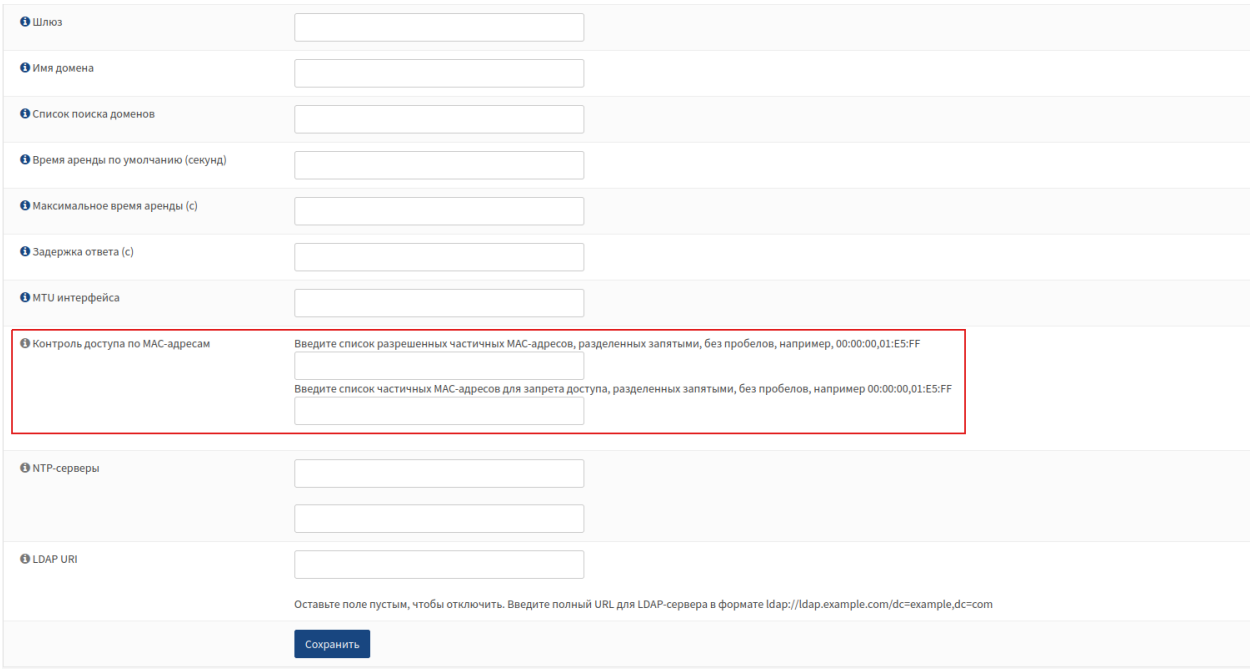


Рис. 1030: Установка MAC-адресов

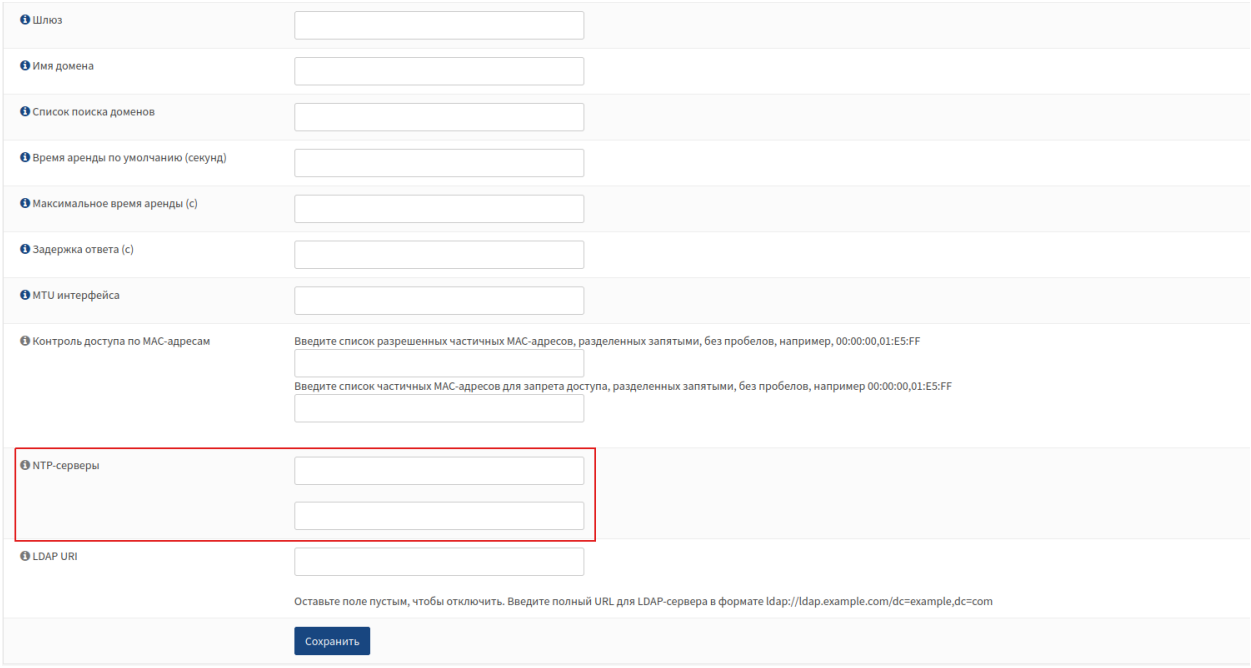


Рис. 1031: Настройка NTP-сервера

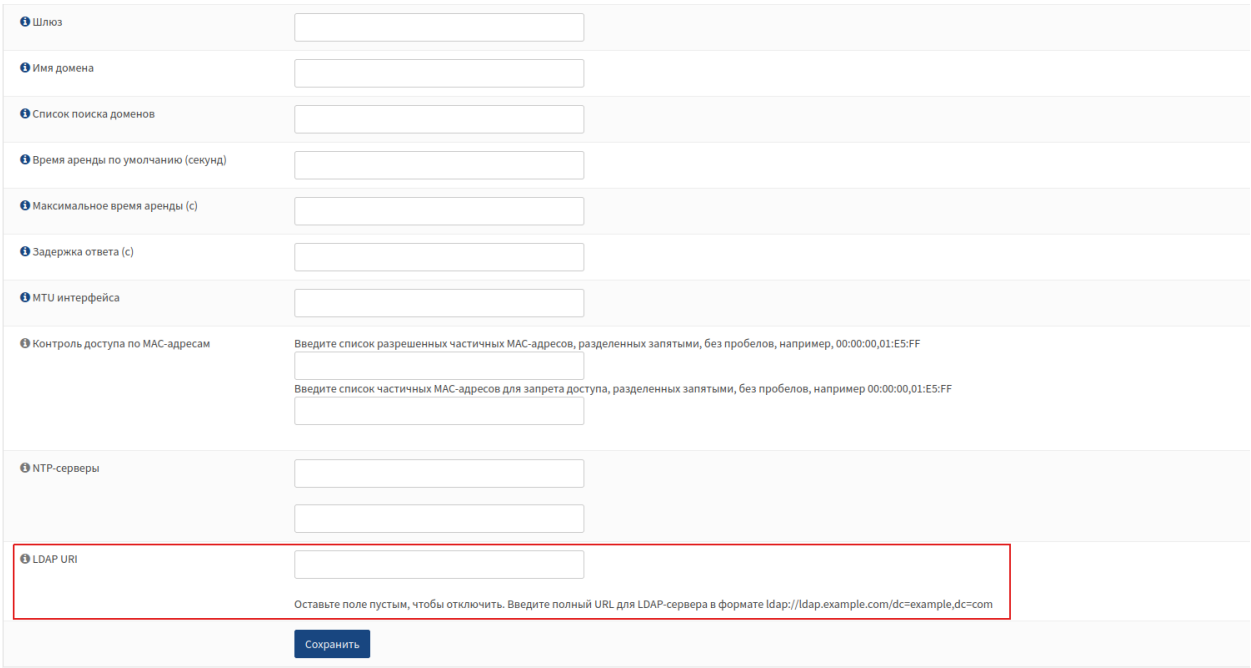


Рис. 1032: Установка URL для LDAP-сервера

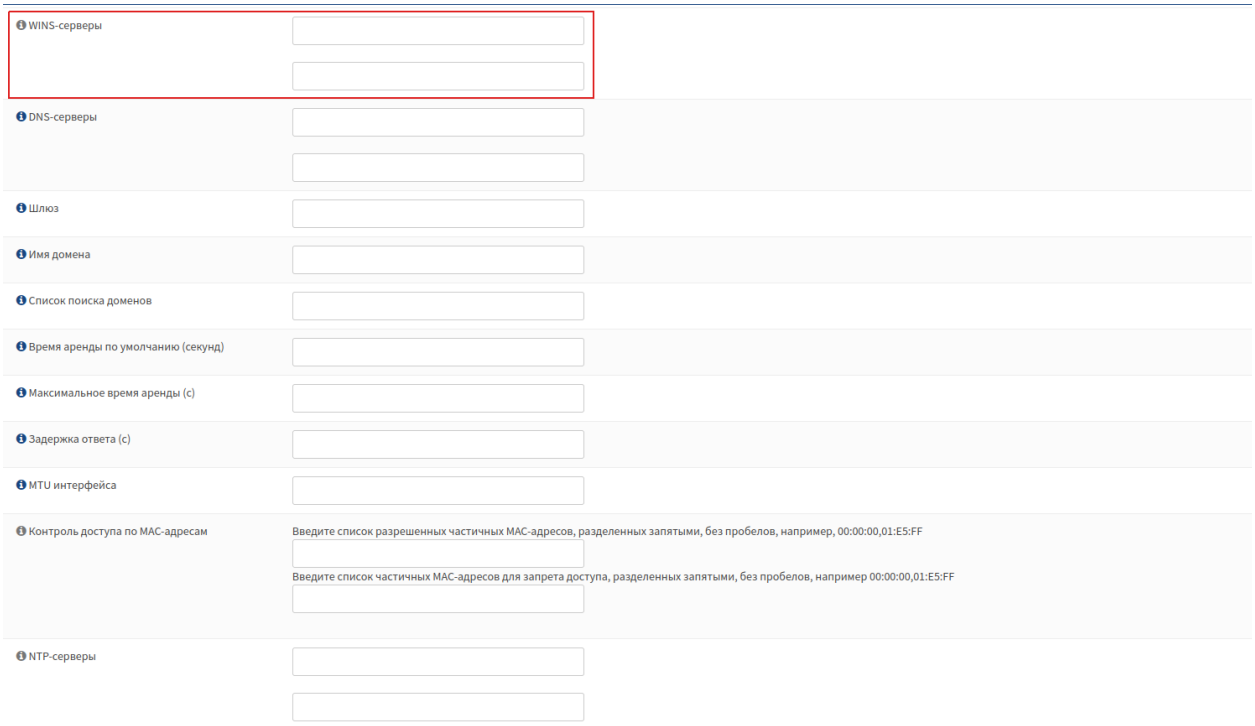


Рис. 1033: Настройка WINS-сервера

Совет

Оставьте пустым, чтобы использовать системные WINS-серверы по умолчанию

- в поле **«DNS-серверы»** задать IP адрес этого интерфейса, если служба DNS включена или настроены глобальные DNS-серверы;

Совет

Оставьте пустым, чтобы использовать системные DNS-серверы по умолчанию

- в поле **«Шлюз»** указать альтернативный шлюз, если он не подходит для вашей сети;

Совет

По умолчанию IP-адрес на этом интерфейсе межсетевого экрана используется в качестве шлюза, если действующий (онлайн) шлюз был настроен в **Система - Шлюзы**

Совет

Введите «none» для отсутствия назначения шлюза

- в поле **«Имя домена»** указать альтернативное имя домена;

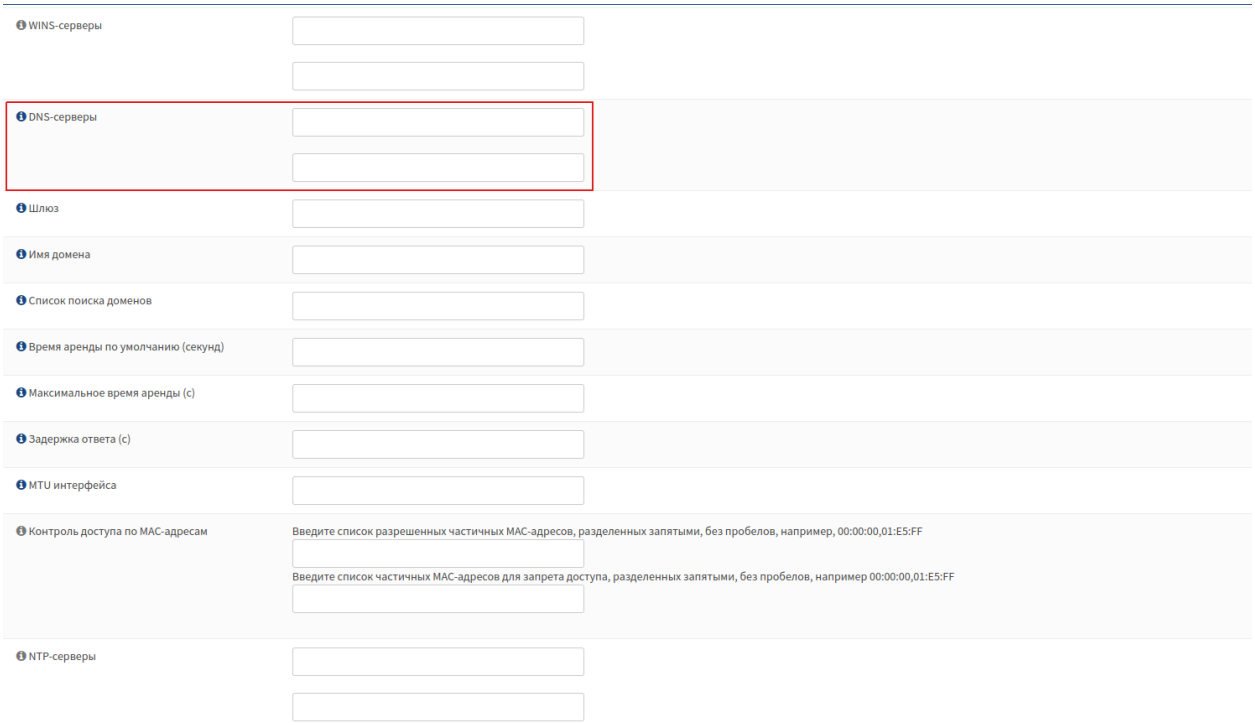


Рис. 1034: Настройка DNS-сервера

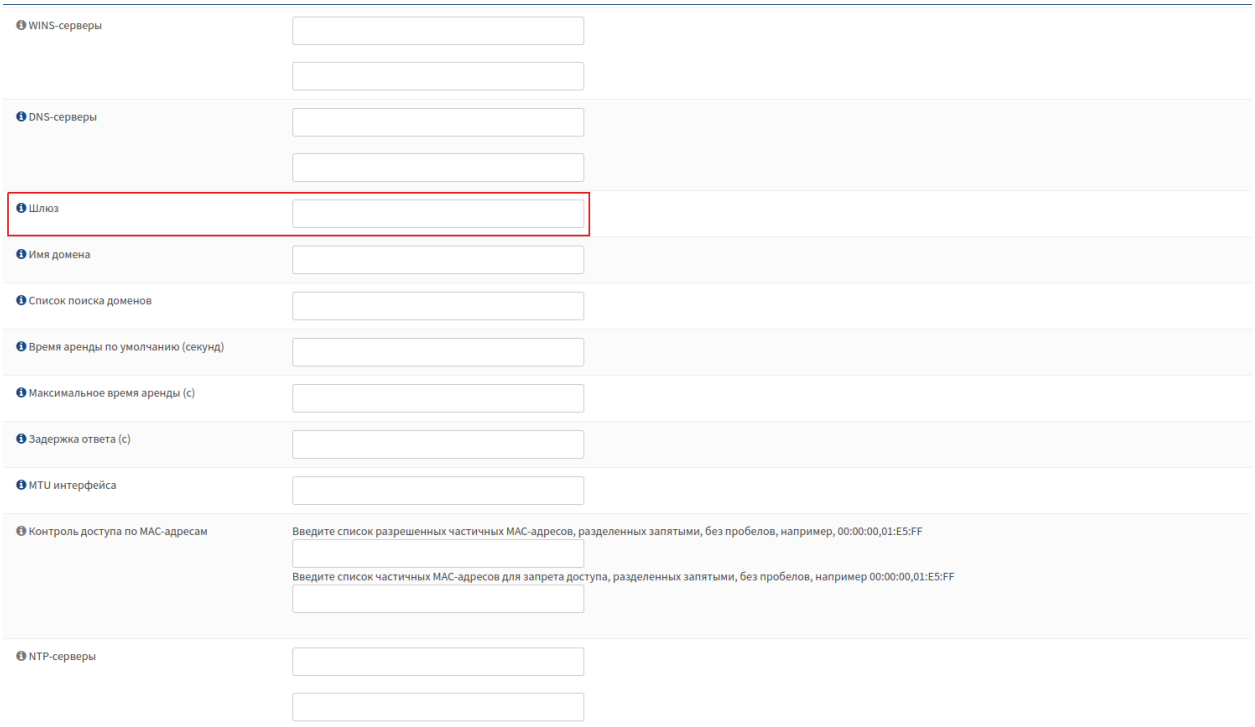


Рис. 1035: Установка шлюза

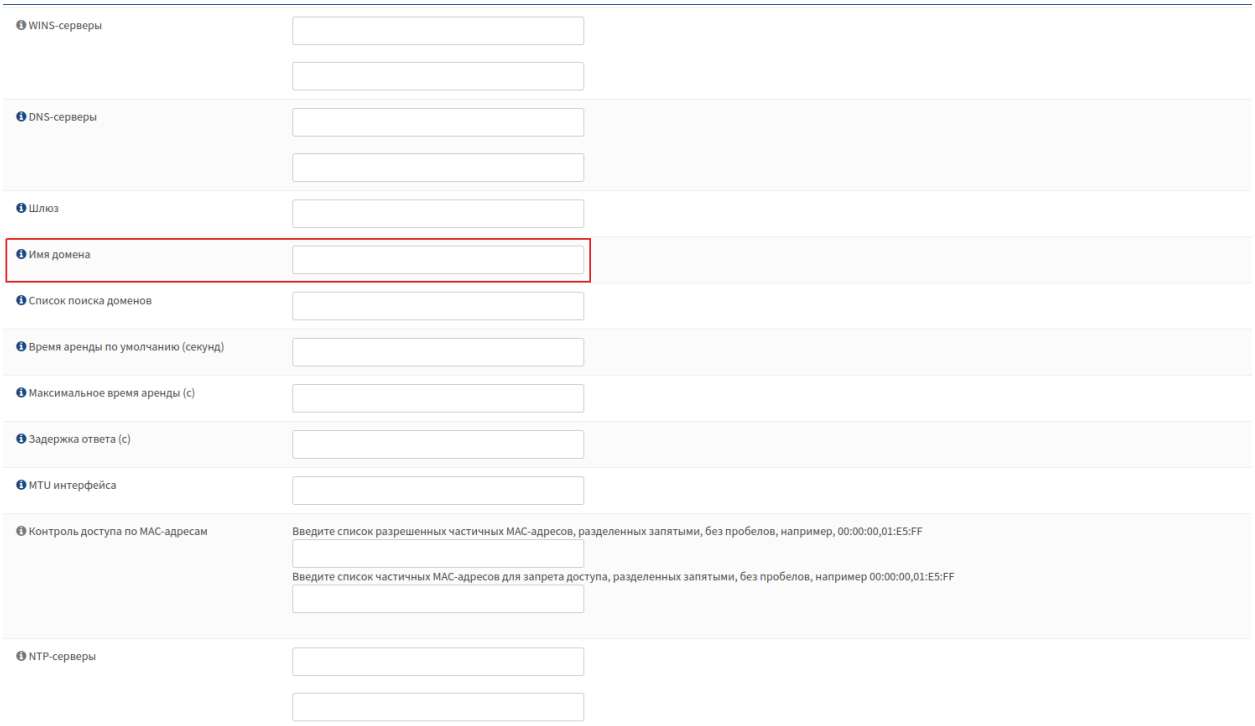


Рис. 1036: Установка имени домена

Совет

По умолчанию в качестве доменного имени используется доменное имя, выданное DHCP

- в поле **«Список поиска доменов»** указать список поиска домена;

Совет

Используйте точку с запятой в качестве разделителя

- в поле **«Время аренды по умолчанию (секунд)»** указать время для клиентов, которые не запрашивают конкретное время аренды;

Совет

Значение по умолчанию 7200 секунд

- в поле **«Максимальное время аренды (с)»** указать максимальное время аренды для клиентов, которые запрашивают точное время;

Совет

Значение по умолчанию 86400 секунд

- в поле **«Задержка ответа (с)»** указать минимальное количество секунд с момента, когда клиент

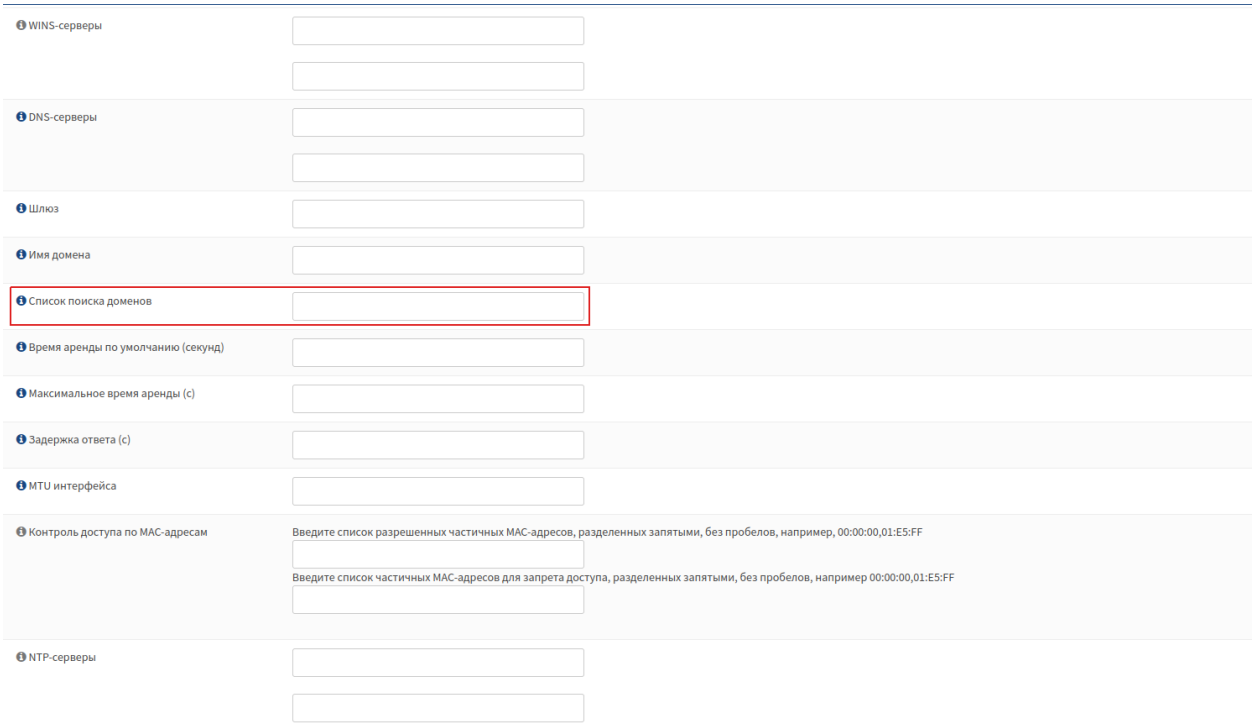


Рис. 1037: Установка списка поиска домена

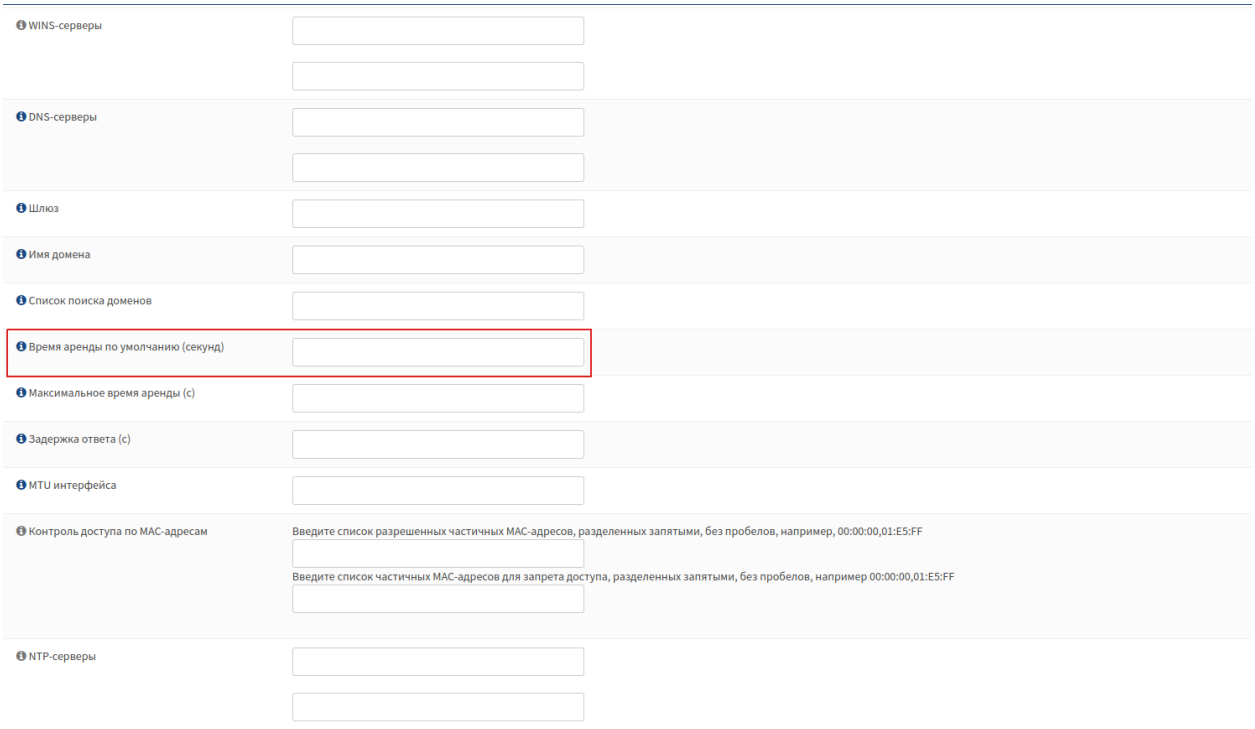


Рис. 1038: Установка времени аренды

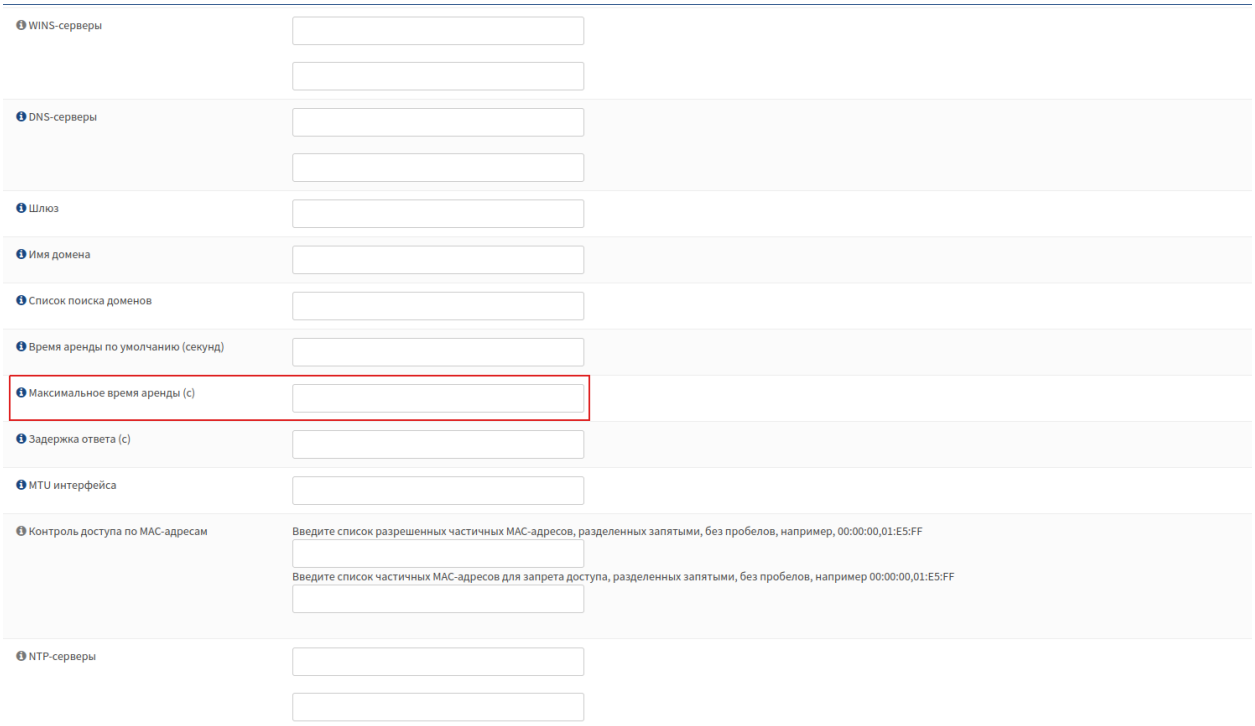


Рис. 1039: Установка максимального времени аренды

начал пытаться получить новую аренду, прежде чем DHCP-сервер ответит на его запрос;

Совет

Значение по умолчанию 0 секунд (без задержки)

- в поле **«MTU интерфейса»** указать значение MTU интерфейса;

Совет

Минимальная легальная величина для MTU: 68

- в поле **«Контроль доступа по MAC-адресам»** установить разрешенные и запрещенные MAC-адреса;
- в поле **«NTP-серверы»** задать IP адрес этого интерфейса, если служба NTP включена или настроены глобальные NTP-серверы;

Совет

Оставьте пустым, чтобы использовать системные NTP-серверы по умолчанию

- в поле **«LDAP URI»** задать полный URL для LDAP-сервера в формате ldap://ldap.example.com/dc=example,dc=com;

Для настройки дополнительных параметров BOOTP/DHCP необходимо нажать кнопку

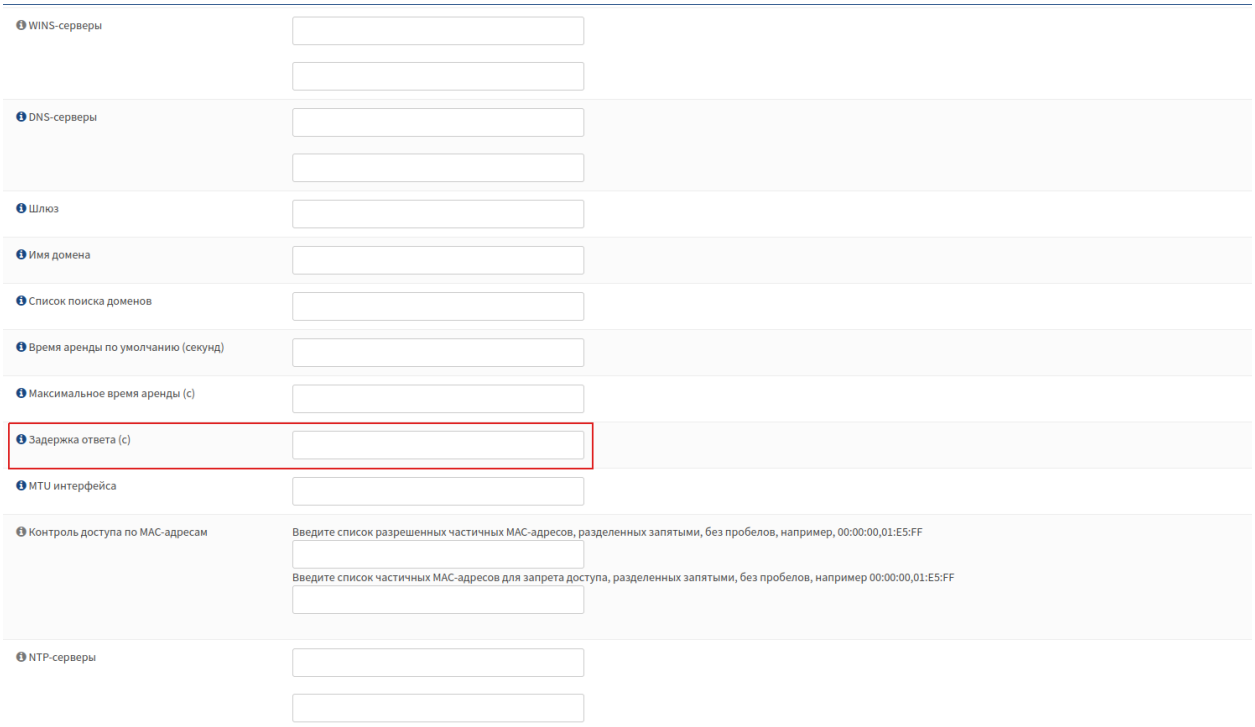


Рис. 1040: Установка задержки ответа

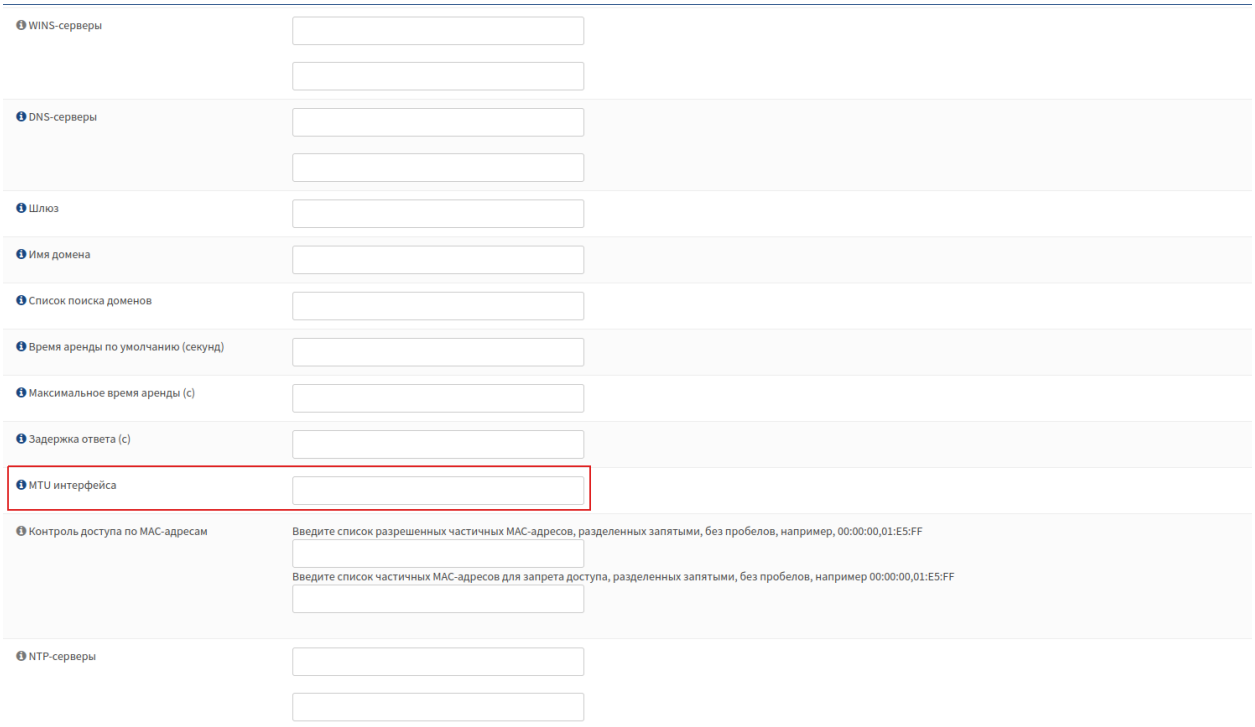


Рис. 1041: Установка значения MTU интерфейса

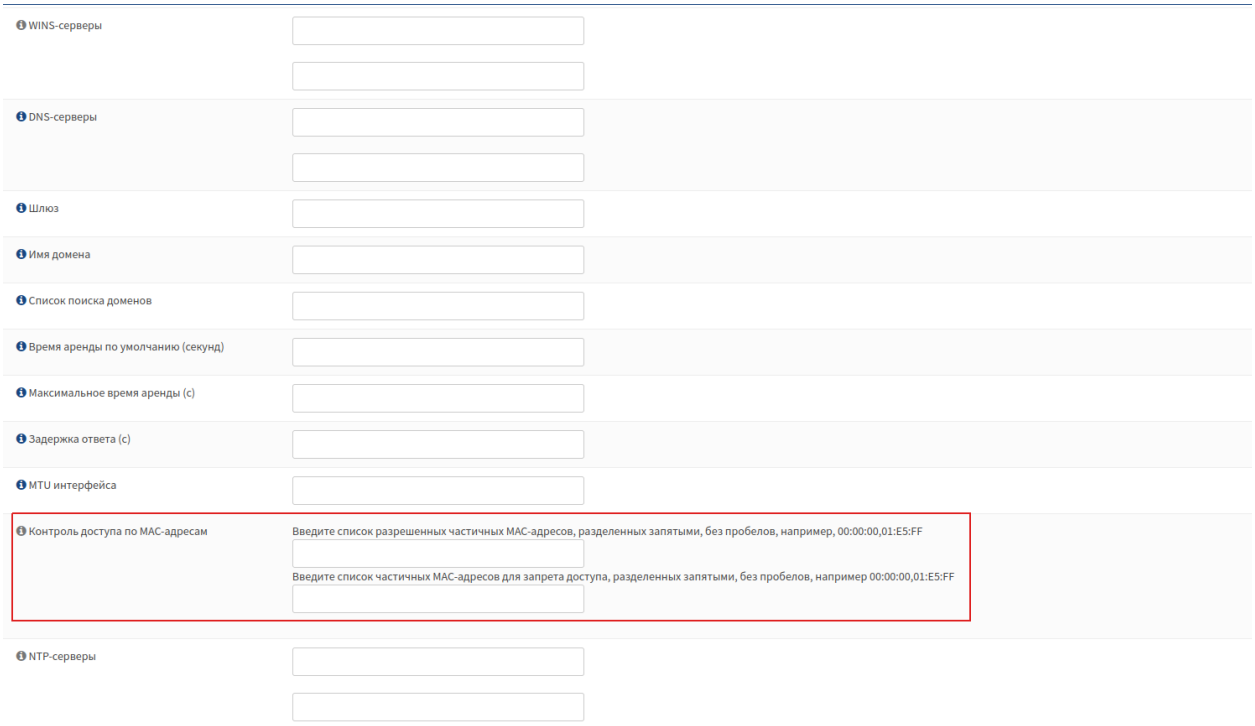


Рис. 1042: Установка MAC-адресов

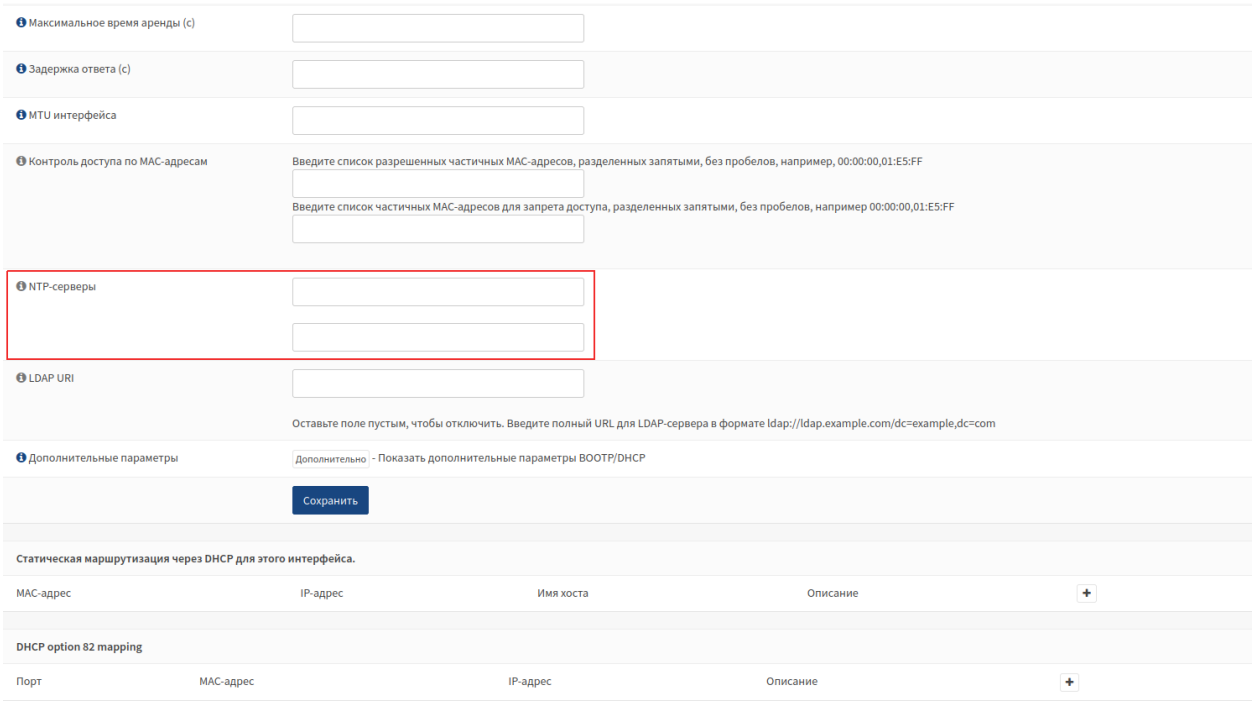


Рис. 1043: Настройка NTP-сервера

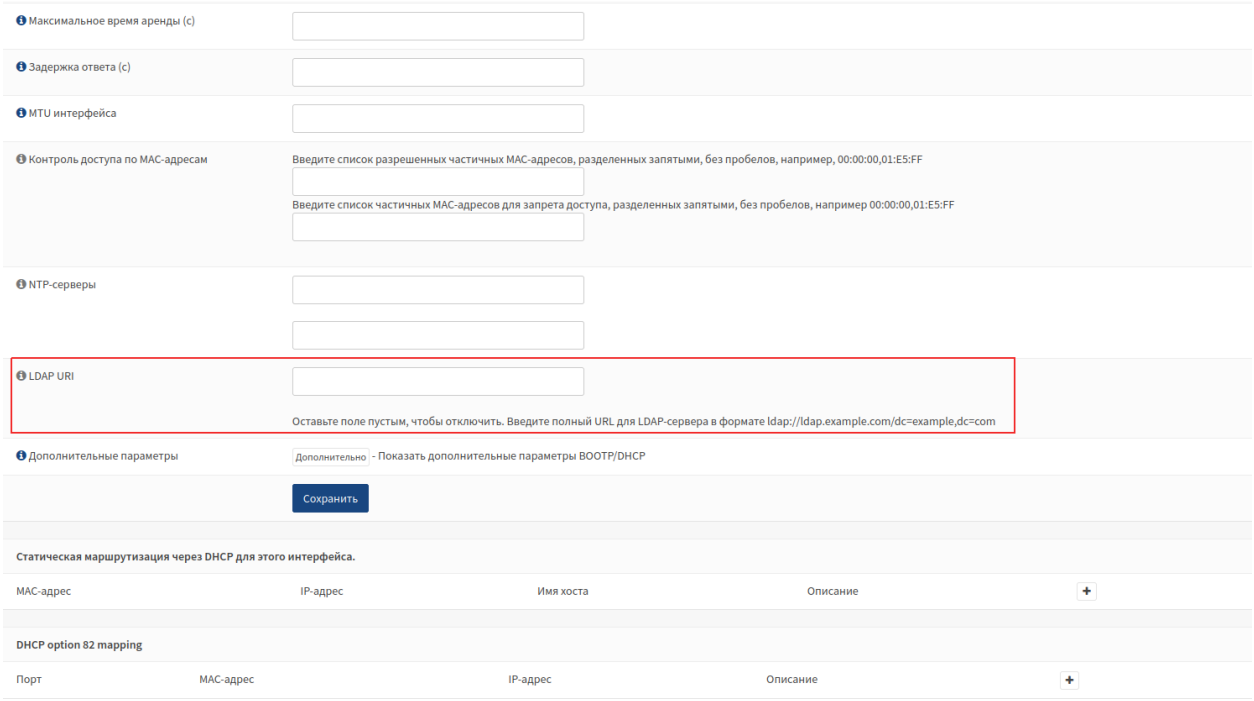
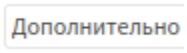


Рис. 1044: Установка URL для LDAP-сервера



.

- в поле **«Дополнительные параметры»** задать необходимые значения;

Для вступления проведенных настроек в силу необходимо нажать кнопку 

.

Для настройки статической маршрутизации через DHCP для этого интерфейса необходимо нажать кнопку 

.

В открывшемся окне необходимо:

- в поле **«MAC-адрес»** задать MAC-адрес в формате «xx:xx:xx:xx:xx:xx», либо скопировать свой;
- в поле **«Идентификатор клиента»** задать идентификатор клиента;
- в поле **«IP-адрес»** установить IP-адрес;

Совет

Если введен адрес IPv4, адрес должен находиться в подсети интерфейса

Совет

Если IPv4-адрес не указан, другой адрес будет динамически выделен из пула

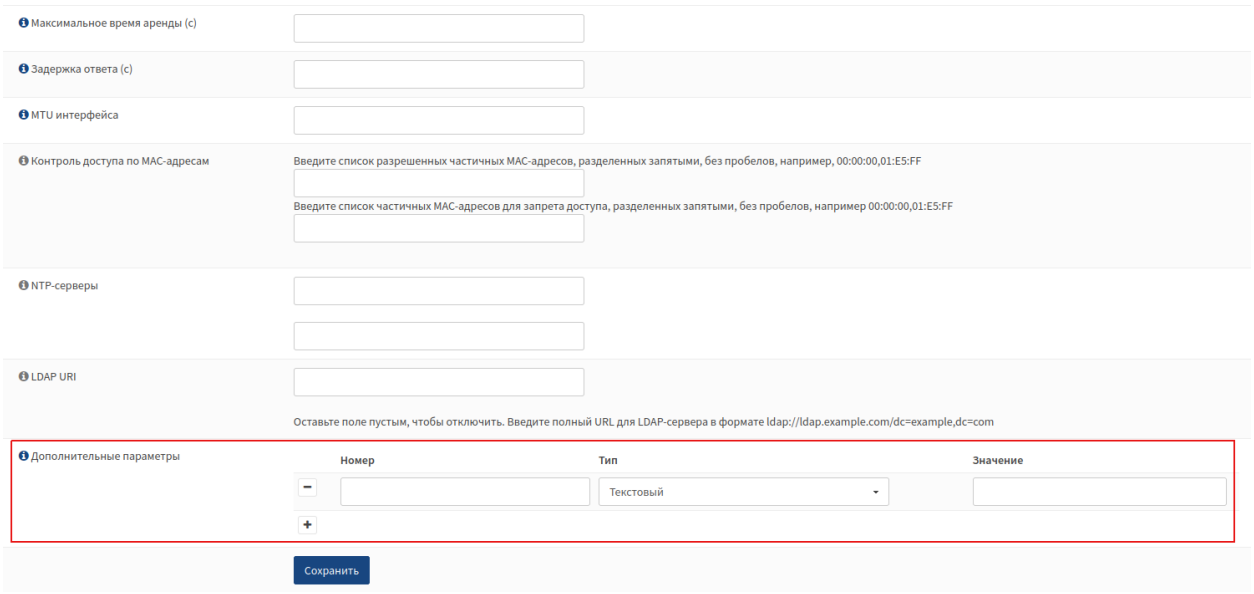


Рис. 1045: Установка дополнительных параметров

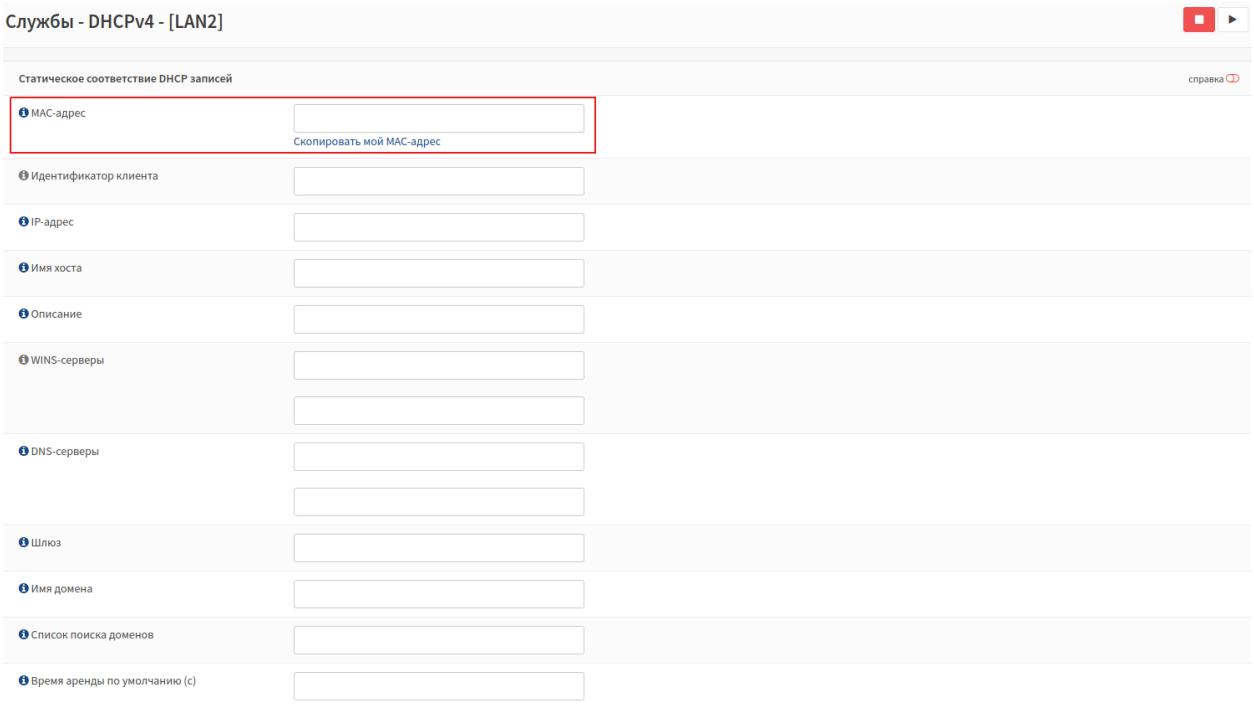


Рис. 1046: Установка MAC-адреса

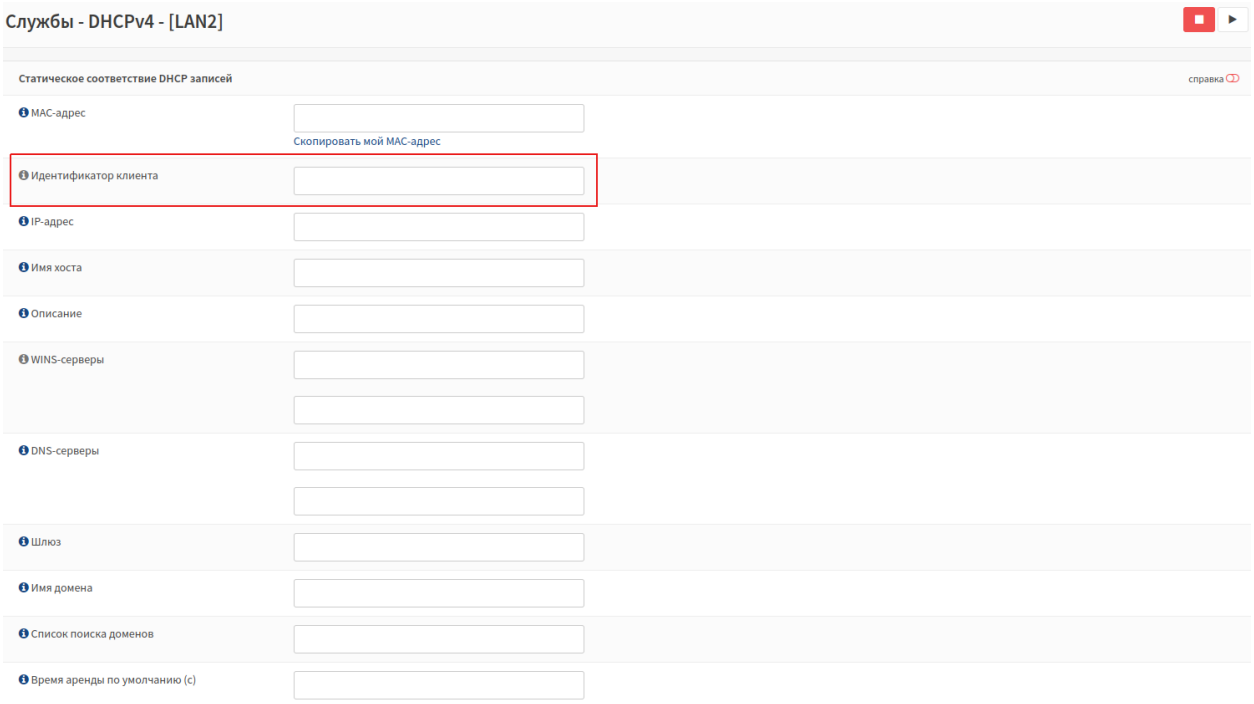


Рис. 1047: Установка идентификатора клиента

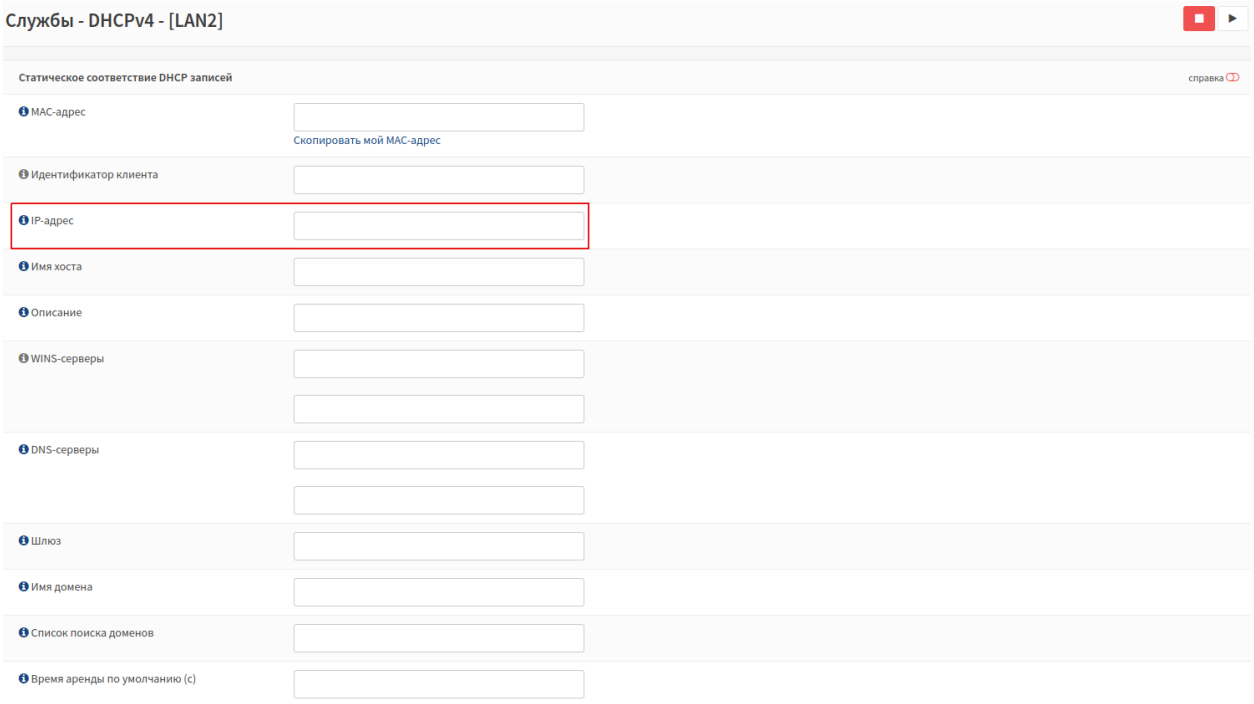


Рис. 1048: Установка IP-адреса

- в поле **«Имя хоста»** указать имя хоста без доменной части;

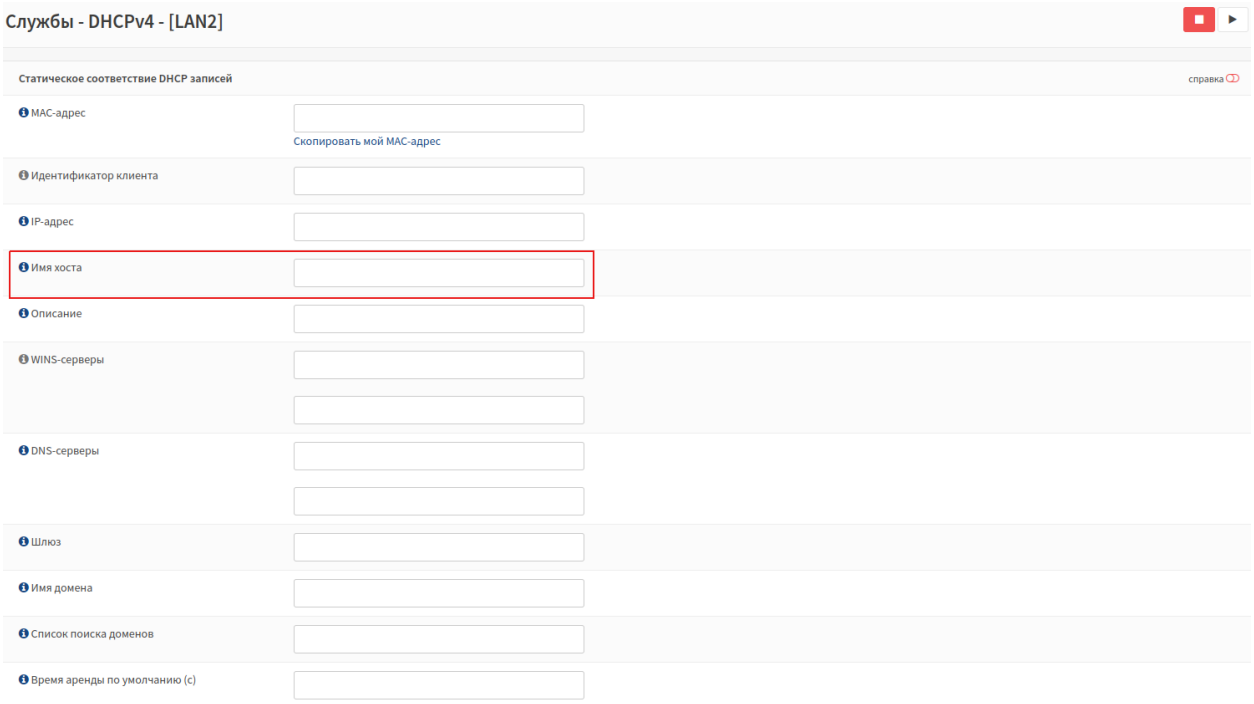


Рис. 1049: Установка имени хоста

Совет

Если IP-адрес не указан выше, имя хоста не будет видно службам с включенной регистрацией

- в поле **«Описание»** задать краткое описание;
- в поле **«WINS-серверы»** задать IP адрес этого интерфейса, если служба WINS включена или настроены глобальные WINS-серверы;

Совет

Оставьте пустым, чтобы использовать системные WINS-серверы по умолчанию

- в поле **«DNS-серверы»** задать IP адрес этого интерфейса, если служба DNS включена или настроены глобальные DNS-серверы;

Совет

Оставьте пустым, чтобы использовать системные DNS-серверы по умолчанию

- в поле **«Шлюз»** указать альтернативный шлюз, если он не подходит для вашей сети;

Совет

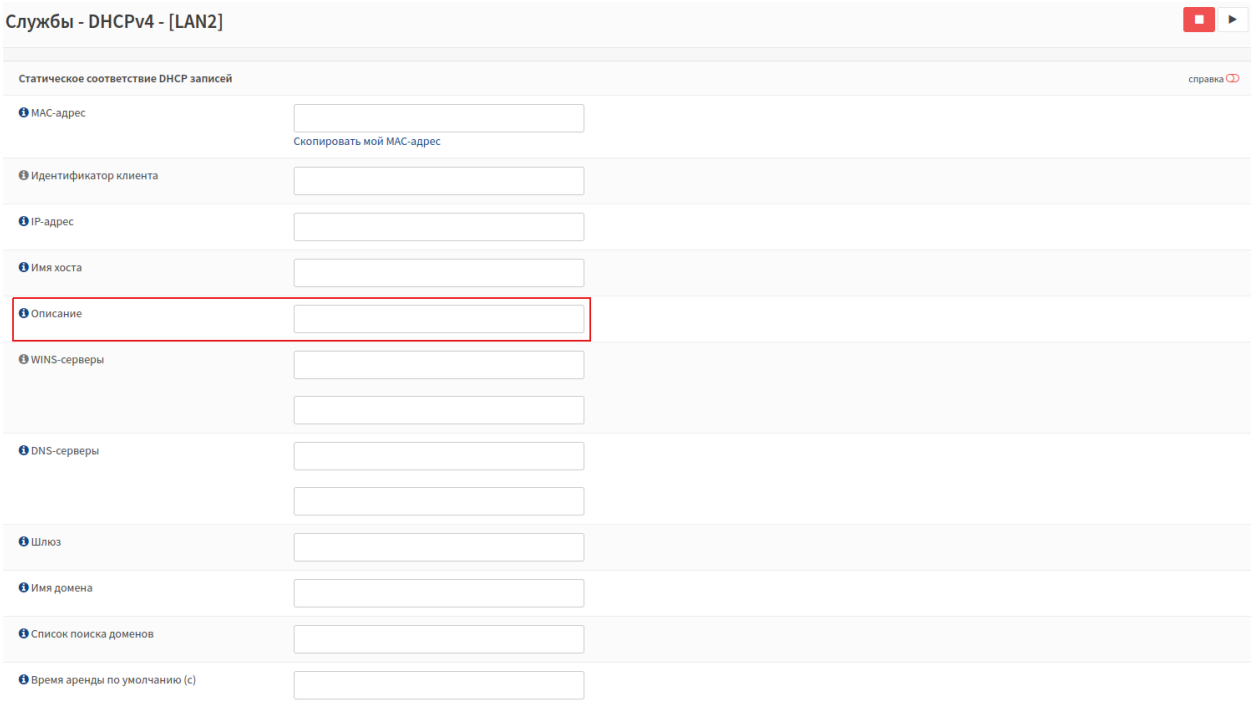


Рис. 1050: Описание

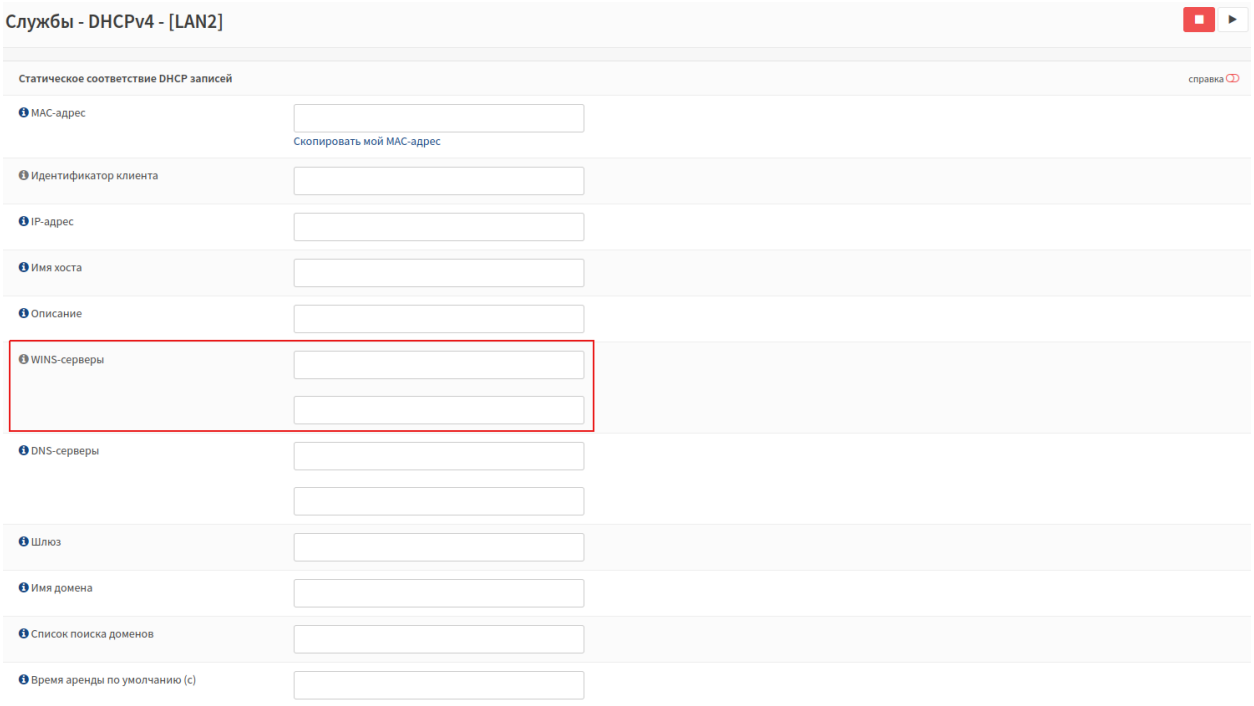


Рис. 1051: Настройка WINS-сервера

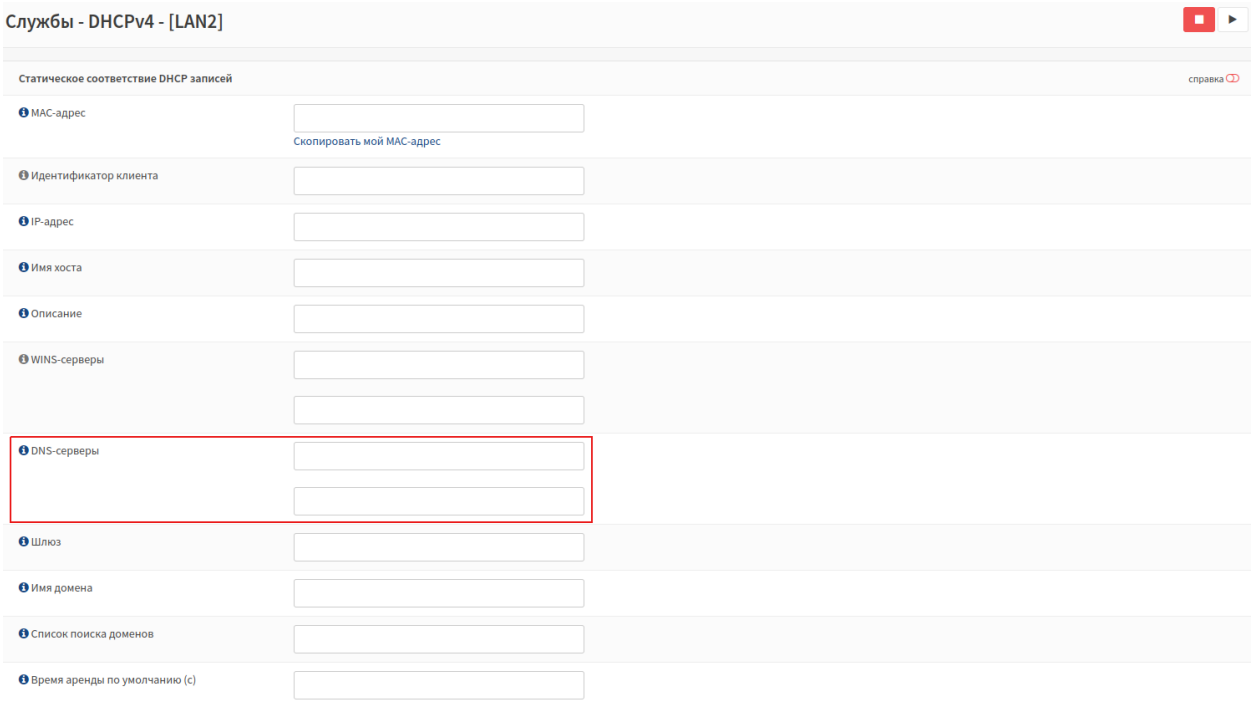


Рис. 1052: Настройка DNS-сервера

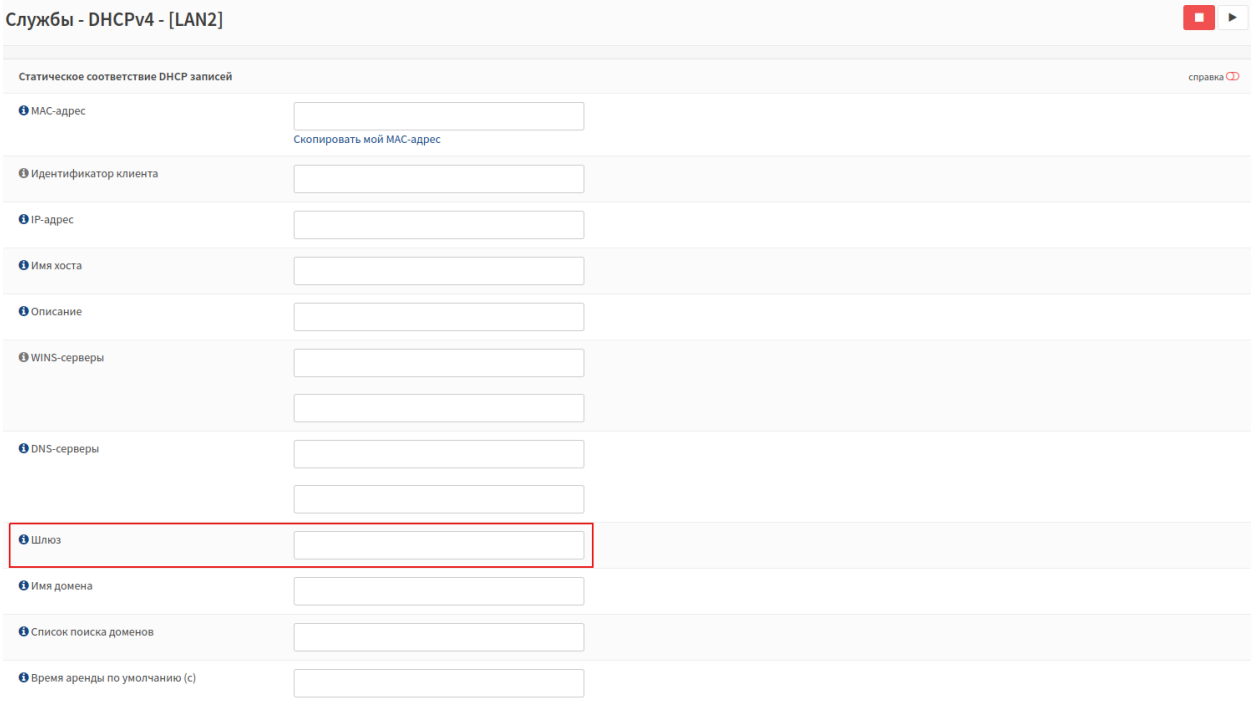


Рис. 1053: Установка шлюза

По умолчанию IP-адрес на этом интерфейсе межсетевого экрана используется в качестве шлюза, если действующий (онлайн) шлюз был настроен в **Система - Шлюзы**

Совет

Введите «none» для отсутствия назначения шлюза

- в поле **«Имя домена»** указать альтернативное имя домена;

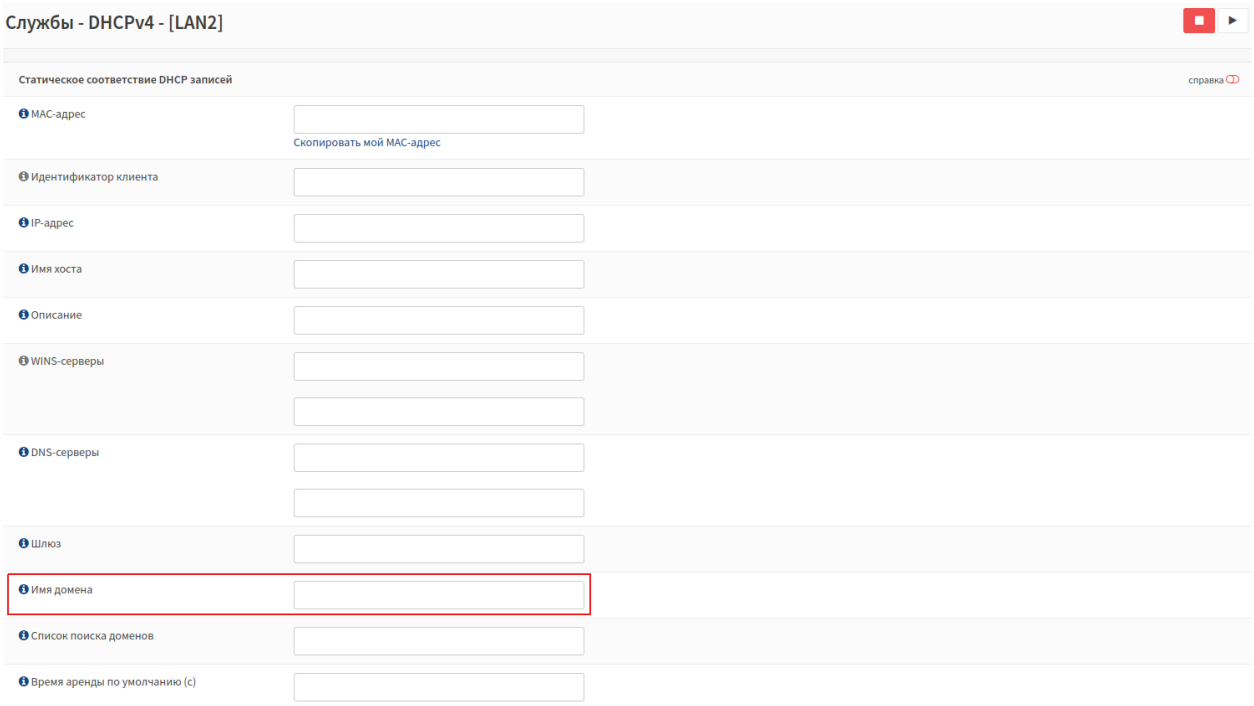


Рис. 1054: Установка имени домена

Совет

По умолчанию в качестве доменного имени используется доменное имя, выданное DHCP

- в поле **«Список поиска доменов»** указать список поиска домена;

Совет

Используйте точку с запятой в качестве разделителя

- в поле **«Время аренды по умолчанию (секунд)»** указать время для клиентов, которые не запрашивают конкретное время аренды;

Совет

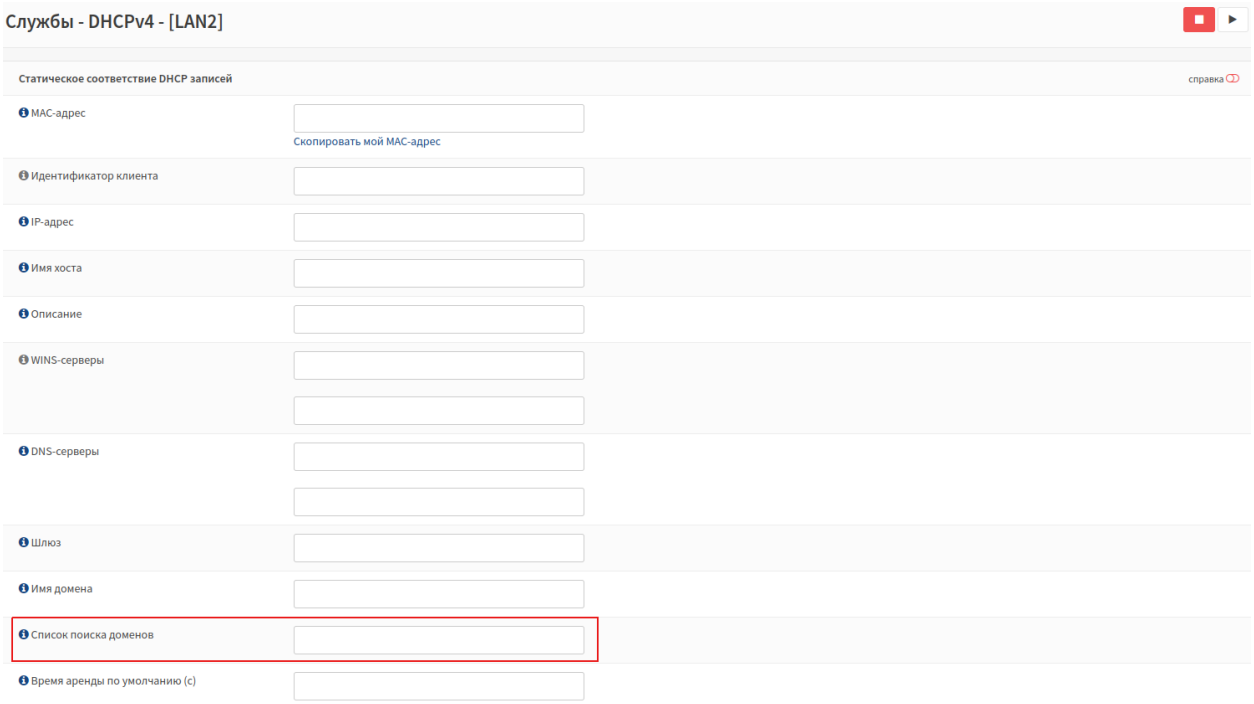


Рис. 1055: Установка списка поиска домена

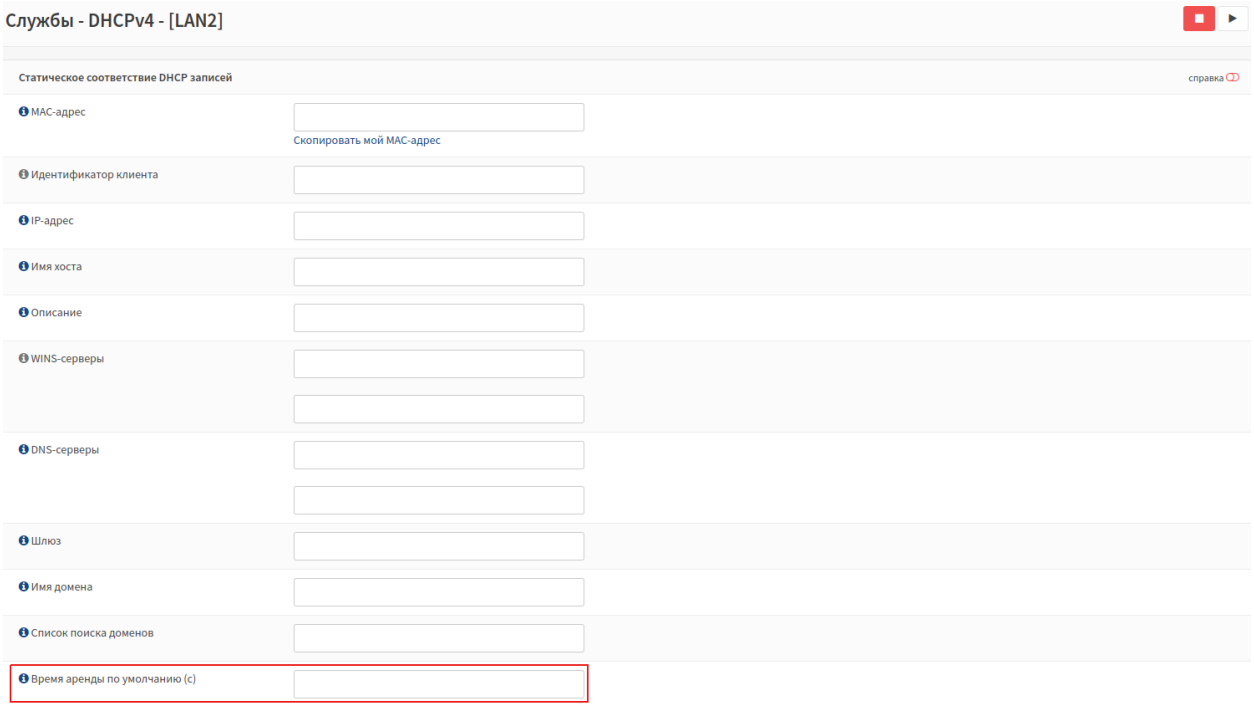


Рис. 1056: Установка времени аренды

Значение по умолчанию 7200 секунд

- в поле **«Максимальное время аренды (с)»** указать максимальное время аренды для клиентов, которые запрашивают точное время;

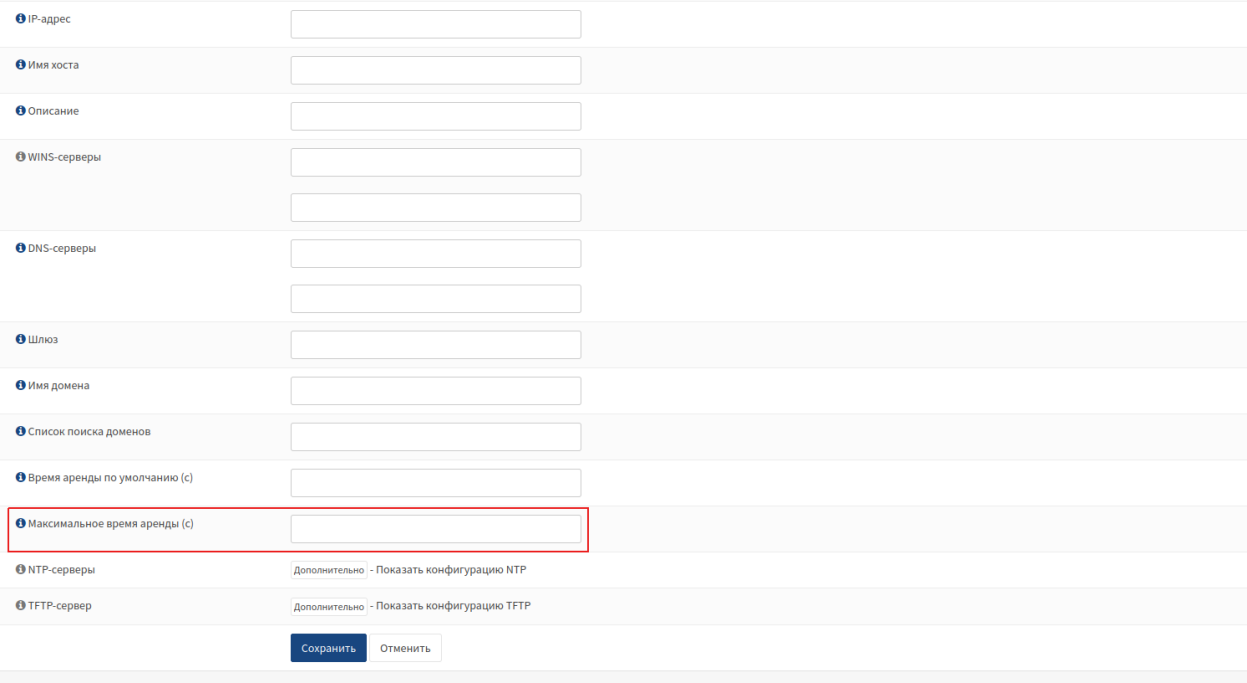


Рис. 1057: Установка максимального времени аренды

Совет

Значение по умолчанию 86400 секунд

Для конфигурации NTP необходимо нажать кнопку Дополнительно .

- в поле **«NTP-серверы»** задать IP адрес этого интерфейса, если служба NTP включена или настроены глобальные NTP-серверы;

Совет

Оставьте пустым, чтобы использовать системные NTP-серверы по умолчанию

Для конфигурации TFTP необходимо нажать кнопку Дополнительно .

- в поле **«TFTP-сервер»** указать имя хоста TFTP и загрузочный файл;

Для вступления проведенных настроек в силу необходимо нажать кнопку Сохранить .

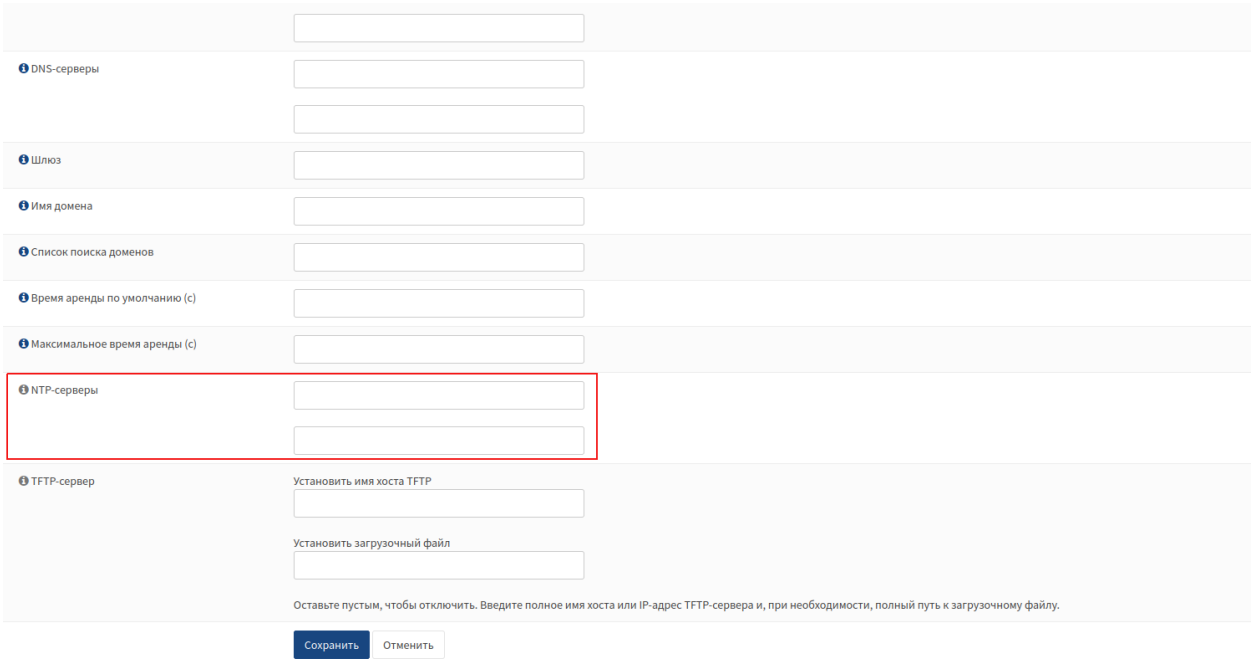


Рис. 1058: Настройка NTP-сервера

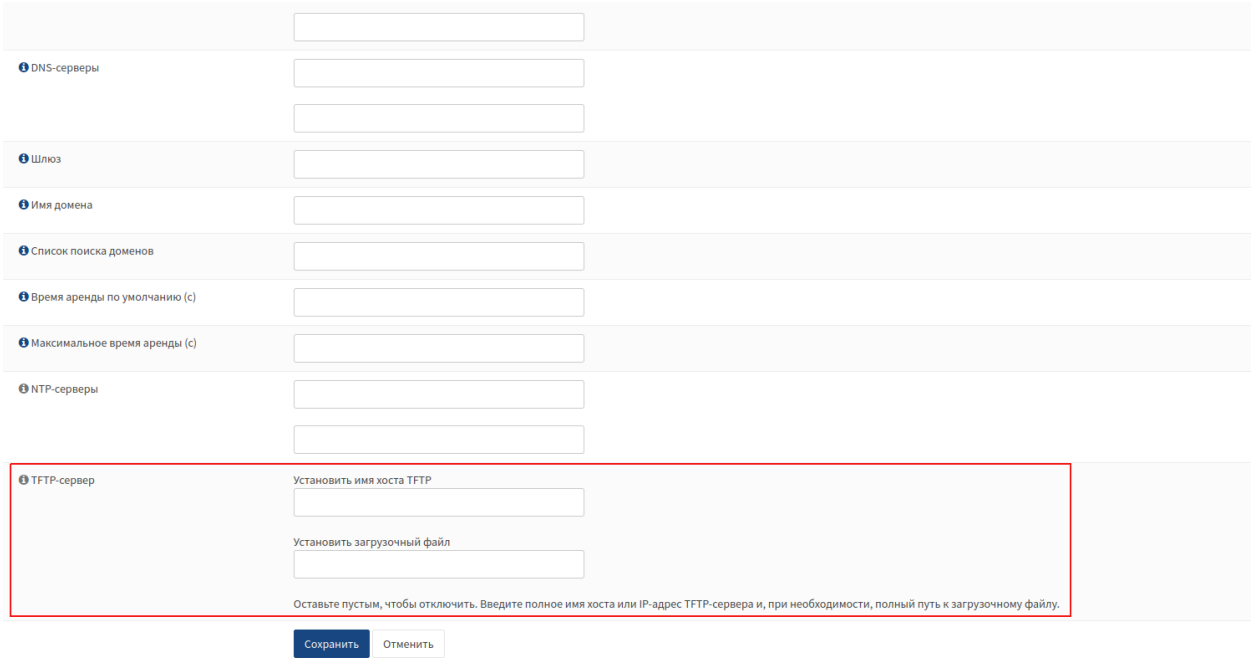


Рис. 1059: Настройка TFTP-сервера

Для настройки DHCP option 82 mapping необходимо нажать кнопку Дополнительно.

В открывшемся окне необходимо:

- в поле **«Порт»** указать порт коммутатора для сопоставления статического IP-адреса пользователя;

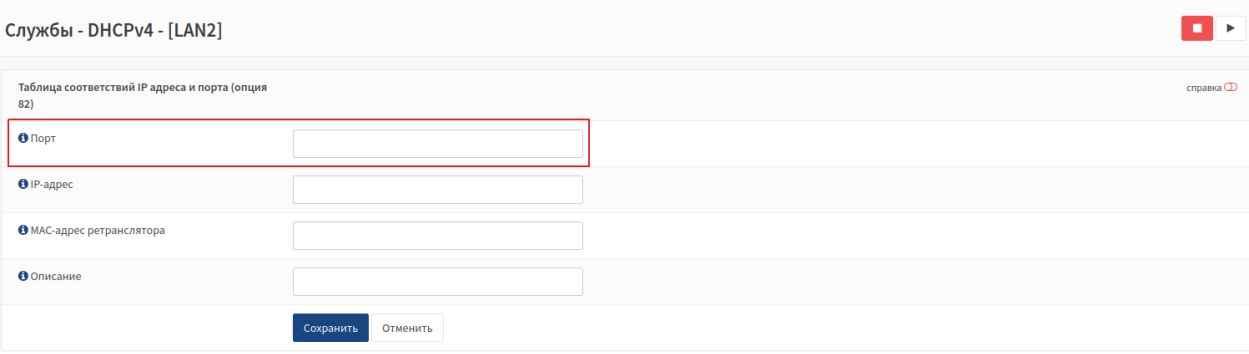


Рис. 1060: Ввод порта коммутатора

- в поле **«IP-адрес»** указать IP-адрес, назначенный порту коммутатора;

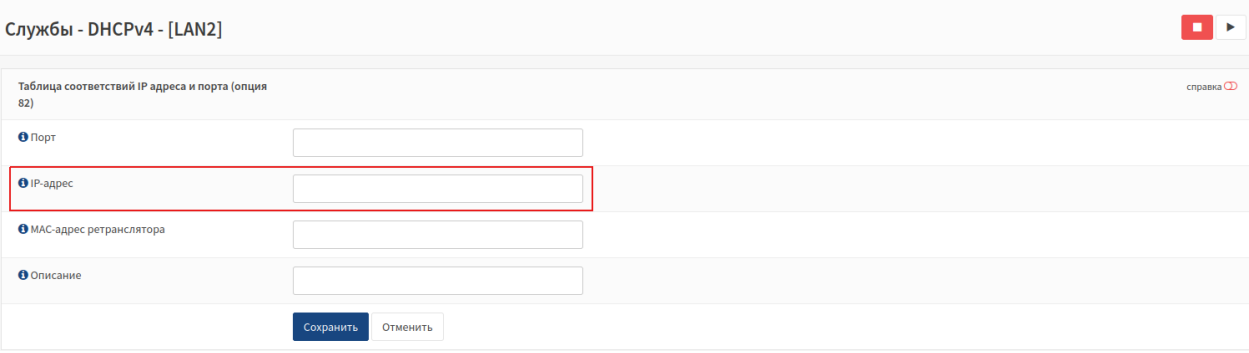


Рис. 1061: Ввод IP-адреса

- в поле **«MAC-адрес ретранслятора»** указать MAC-адрес в формате «xx:xx:xx:xx:xx:xx»;
- в поле **«Описание»** указать описание для справки;

Для вступления проведенных настроек в силу необходимо нажать кнопку Сохранить.

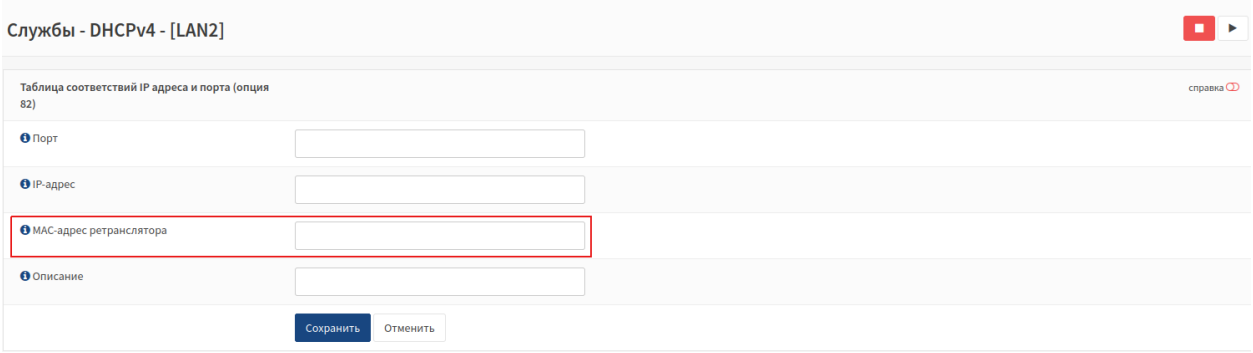


Рис. 1062: Ввод MAC-адреса

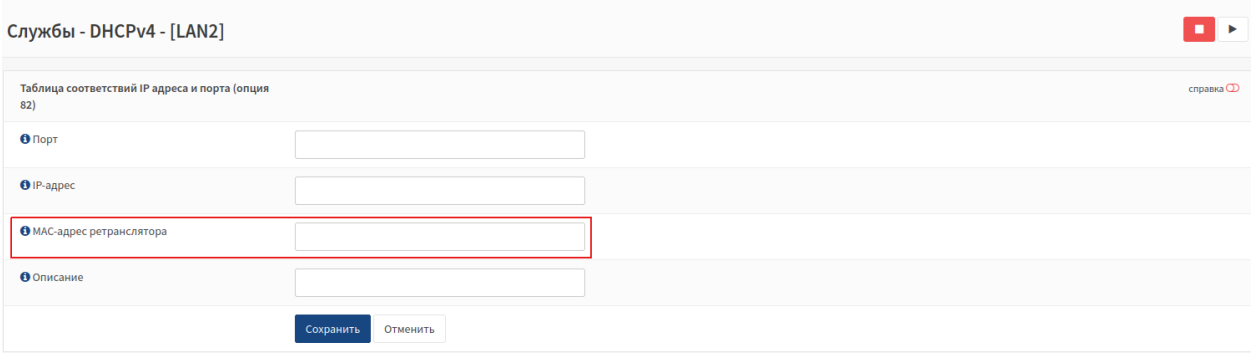


Рис. 1063: Ввод описания

Аренда адресов

Таблица файлов аренды адресов представлена на рисунке.

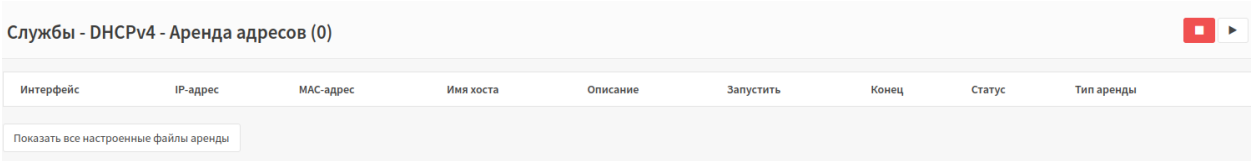
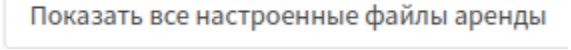


Рис. 1064: Таблица файлов аренды

Для просмотра всех настроенных файлов необходимо нажать кнопку



.

Для просмотра активных и статических файлов необходимо нажать кнопку

.

Журнал

Раздел **«Журнал»** содержит журнал DHCPv4.

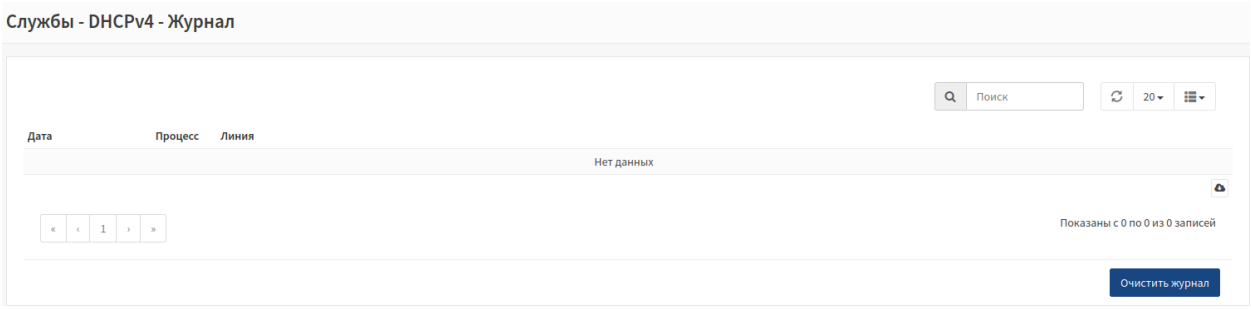


Рис. 1065: Журнал DHCPv4

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

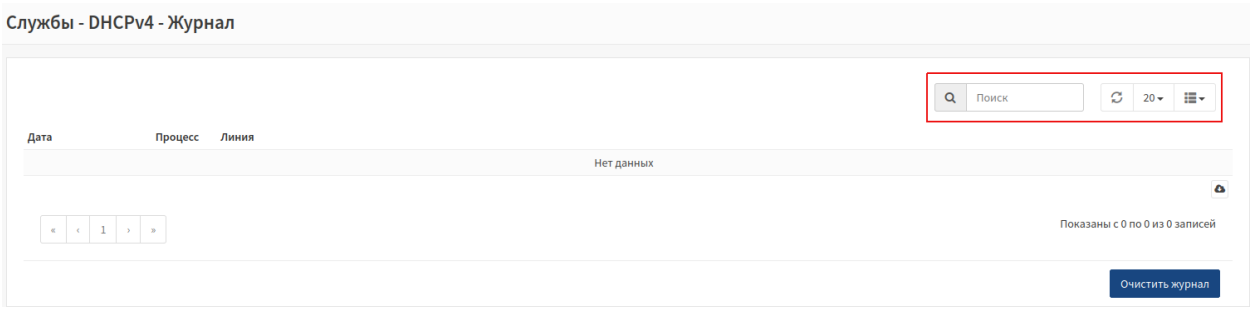


Рис. 1066: Фильтры журнала DHCPv4

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

2.7.8.8 DHCPv6

Для перехода к просмотру аренды адресов необходимо:

- нажать на вкладку **«Службы»** - **«DHCPv6»** - **«Аренда адресов»**, расположенную в левой части списка объектов управления;

Для перехода к просмотру журнала системы обнаружения вторжений необходимо:

- нажать на вкладку **«Службы»** - **«DHCPv6»** - **«Журнал»**, расположенную в левой части списка объектов управления;

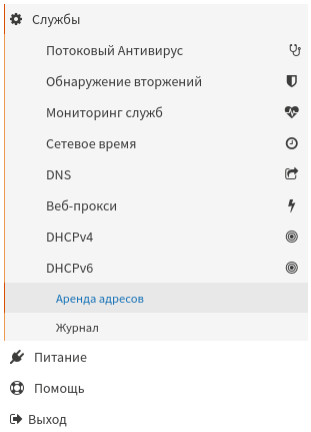


Рис. 1067: Переход к просмотру аренды адресов

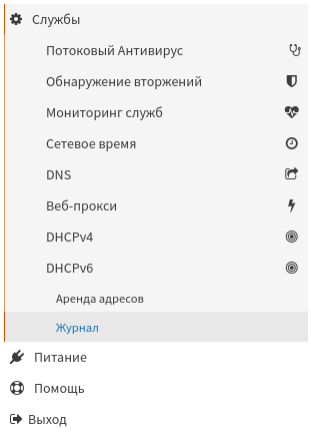


Рис. 1068: Переход к просмотру журнала

Аренда адресов

Таблица файлов аренды адресов представлена на рисунке.

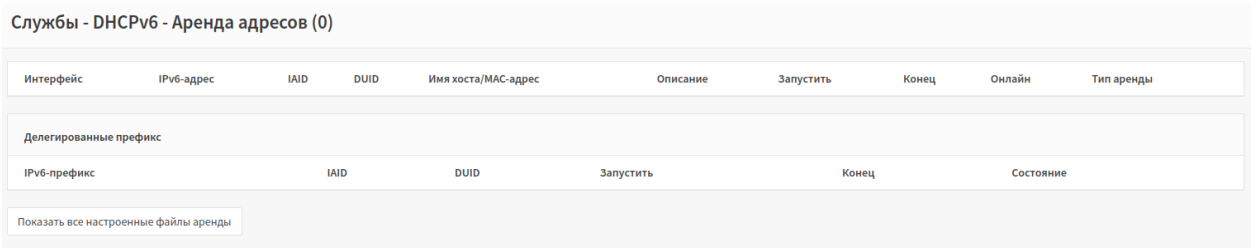
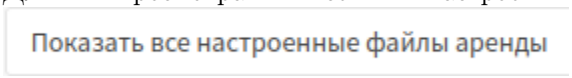
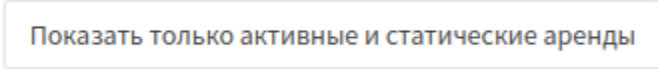


Рис. 1069: Таблица файлов аренды

Для просмотра всех настроенных файлов необходимо нажать кнопку 

.

Для просмотра активных и статических файлов необходимо нажать кнопку 

.

Журнал

Раздел **«Журнал»** содержит журнал DHCPv6.

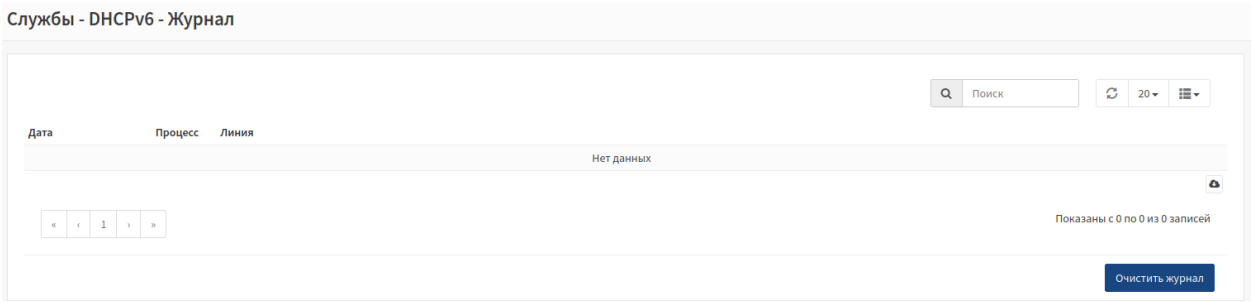


Рис. 1070: Журнал DHCPv6

Журнал состоит из следующих колонок:

- **«Дата»** - дата и время сообщения журнала;
- **«Процесс»** - процесс;
- **«Линия»** - сообщение журнала.

С помощью фильтров можно ограничить или расширить данные журнала.

Для очистки журнала необходимо нажать кнопку **«Очистить журнал»** 

, расположенную в правом нижнем углу журнала.

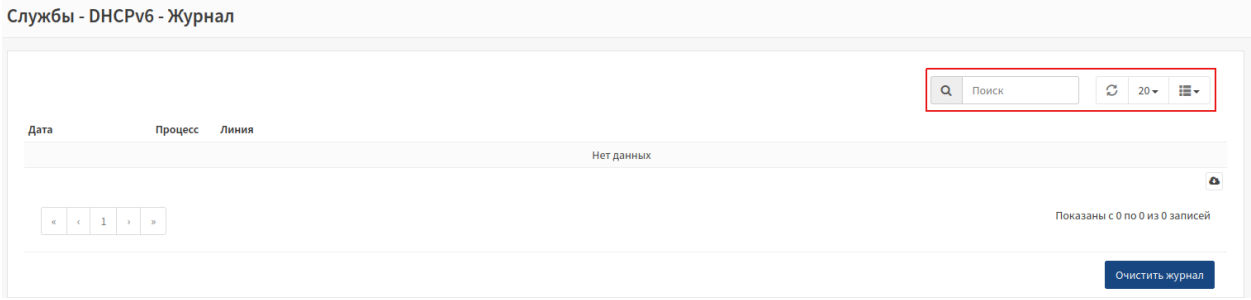


Рис. 1071: Фильтры журнала DHCPv6

2.7.9 Питание

Для перехода к перезагрузке системы необходимо:

- нажать на вкладку **«Питание»** - **«Перезагрузка»**, расположенную в левой части списка объектов управления.

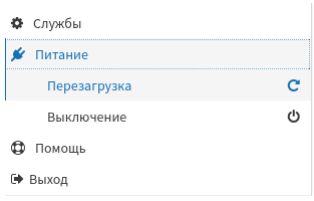


Рис. 1072: Переход к перезагрузке системы

Для перехода к выключению системы необходимо:

- нажать на вкладку **«Питание»** - **«Выключение»**, расположенную в левой части списка объектов управления.

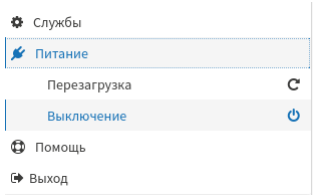
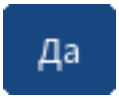


Рис. 1073: Переход к выключению системы

2.7.9.1 Перезагрузка

Для перезагрузки системы необходимо:

- нажать на кнопку **«Да»** 

при ответе на вопрос о перезагрузке системы.

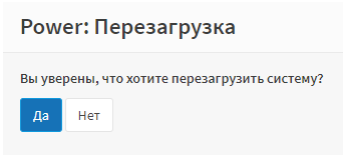
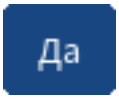


Рис. 1074: Перезагрузка системы

2.7.9.2 Выключение

Для выключения системы необходимо:

- нажать на кнопку **«Да»**  при ответе на вопрос о выключении системы.

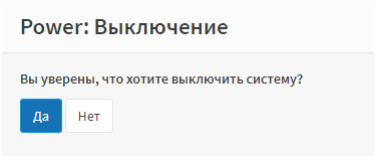


Рис. 1075: Выключение системы

2.7.10 Помощь

Для перехода к просмотру документации необходимо:

- нажать на вкладку **«Помощь»** - **«Документация»**, расположенную в левой части списка объектов управления;

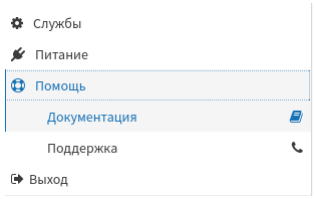


Рис. 1076: Переход к просмотру документации

Для перехода к поддержке пользователей необходимо:

- нажать на вкладку **«Помощь»** - **«Поддержка»**, расположенную в левой части списка объектов управления;

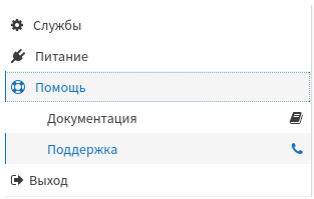


Рис. 1077: Переход к поддержке пользователей

2.7.10.1 Документация

В разделе **«Документация»** находиться руководство пользователя на изделие

2.7.10.2 Поддержка

Для осуществления технической поддержки пользователей обходимо:

- войти в учетную запись пользователя;

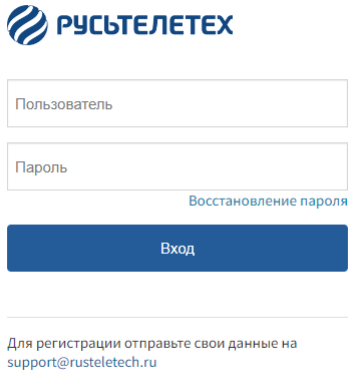


Рис. 1078: Вход в учетную запись пользователя

- нажать на вкладку **«Поддержка»**;

Рис. 1079: Переход на вкладку **«Поддержка»**

- в открывшемся окне нажать на кнопку **«Задать вопрос»**;
- в открывшемся окне в раздел **«Форма обращения»** в соответствующие графы следует ввести:
  - **«Фамилию и Имя»**;
  - **«Адрес электронной почты»**;
  - **«Контактный телефон»**;
  - **«Текст сообщения»**;

Рис. 1080: **«Задать вопрос»**

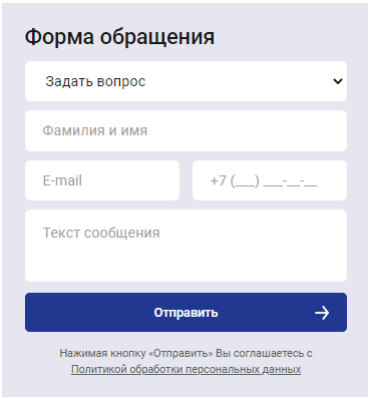
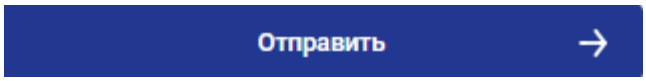


Рис. 1081: Ввод необходимой информации

- нажать на кнопку **«Отправить»** 

.

2.7.11 Выход

Вкладка **«Выход»** необходима для выхода из учетной записи пользователя.

Глава 3

Аппаратная платформа RTT-UNA

3.1 Об устройстве

Аппаратная платформа RTT-UNA (далее - аппаратная платформа UNA) применяется для реализации устройств интеллектуальной обработки и маршрутизации трафика в технологических и корпоративных сетях. Промышленное исполнение платформы может применяться также в качестве промышленного компьютера, а корпоративное исполнение в качестве мини-сервера.

Аппаратная платформа UNA выпускается в корпоративном (с активным охлаждением) и промышленном (с пассивным охлаждением и расширенным температурным диапазоном) исполнениях, имеет возможность установки оперативной памяти и двух ssd дисков различной ёмкости, а также расширения интерфейсов ввода-вывода при помощи установки дополнительных карт.

В телекоммуникационных сетях аппаратная платформа UNA подходит для создания: межсетевых экранов, маршрутизаторов, систем обнаружения вторжений, систем глубокой инспекции пакетов, универсальных шлюзов безопасности, устройств доступа в сеть, концентраторов для IoT устройств (при использовании карточки расширения промышленных интерфейсов), компактных серверов для размещения VPN, WEB и т.д. сервисов.

В промышленных сетях аппаратная платформа UNA может использоваться для создания инфраструктуры цифровых подстанций, ПЛК, устройств релейной защиты и автоматики, модулей предиктивной диагностики трансформаторов, устройств диспетчерской связи и т. д.

Аппаратная платформа UNA имеет возможность установки плат расширения, в том числе доступны для установки следующие карты расширения: карта расширения интерфейсов 8xGigabit Ethernet (8xGE), карта расширения 2x10 Gigabit Ethernet (SFP+), карта расширения промышленных интерфейсов (CAN, RS485/RS232 и т. д.).

3.2 Корпоративное исполнение

Общий вид аппаратной платформы UNA в корпоративном исполнении представлен на рисунке.

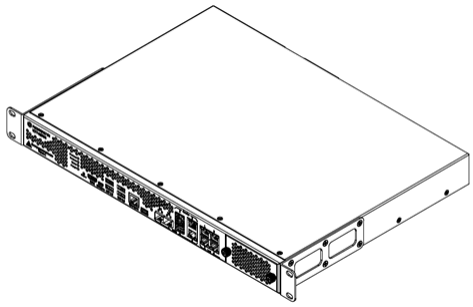


Рис. 1: Внешний вид аппаратной платформы UNA

Габаритные размеры аппаратной платформы UNA в корпоративном исполнении приведены на рисунках ниже.

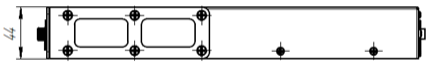


Рис. 2: Вид сбоку

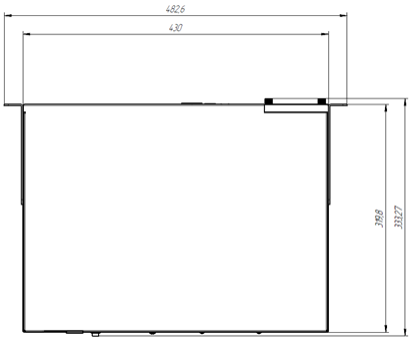


Рис. 3: Вид снизу

Передняя панель аппаратной платформы UNA показана на рисунке .

Описание элементов передней панели аппаратной платформы UNA приведено в таблице.

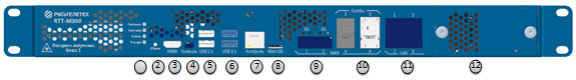


Рис. 4: Передняя панель аппаратной платформы UNA

Таблица 1: Описание элементов передней панели аппаратной платформы UNA

Порядковый номер	Описание элемента	Примечание
1	Индикация	
2	Кнопка сброса	
3	Разъём HDMI 2.0	
4	Консоль	
5	Порт USB 2.0 Host	2 шт.
6	Порт USB 3.0 Host	2 шт.
7	Контроль	
8	Слот для подключения microSD	
9	Порт 10G SFP+ WAN	
10	Порт 1GE SFP	2 шт.
	Порт 1GE RJ-45 WAN	2 шт. (Размещаются на плате)
11	Порт 1G Ethernet LAN (медные)	4 шт. (Размещаются на плате)
12	Модуль расширения 8 Gigabit Ethernet	

Задняя панель аппаратной платформы UNA показана на рисунке.

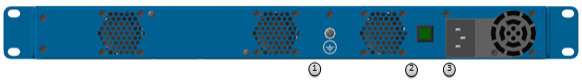


Рис. 5: Задняя панель аппаратной платформы UNA

Описание элементов задней панели аппаратной платформы UNA приведено в таблице.

Таблица 2: Описание элементов задней панели аппаратной платформы UNA

Порядковый номер	Описание элемента	Примечание
1	Винт заземления	
2	Кнопка питания	
3	Разъём подключения кабеля питания	

Компоновка элементов внутри корпуса аппаратной платформы UNA представлена на рисунке.

Описание компоновки элементов внутри корпуса аппаратной платформы UNA приведено в таблице.

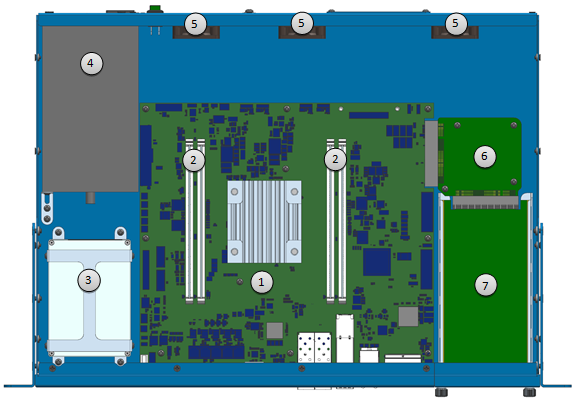


Рис. 6: Компоновка элементов внутри корпуса аппаратной платформы UNA

Таблица 3: Описание компоновки элементов внутри корпуса аппаратной платформы UNA

Порядковый номер	Описание элемента	Примечание
1	Основная плата	
2	ОЗУ	DIMM DDR4
3	ПЗУ	SSD SATA3
4	Блок питания	
5	Вентиляторы	
6	Плата-переходник	
7	Модуль расширения Ethernet	

Аппаратной платформа в корпоративном исполнении UNA имеет две версии, которые приведены в таблице.

Таблица 4: Версии аппаратной платформы UNA в корпоративном исполнении

Обозначение изделия	Описание
RTT-UNA	Исполнение с активным охлаждением (при помощи внутренних вентиляторов) для применения в корпоративных коммуникационных сетях
RTT-UNA-X	Исполнение с активным охлаждением (при помощи внутренних вентиляторов) для применения в корпоративных коммуникационных сетях с двумя интегрированным интерфейсами 10 GE (SFP+)

3.3 Промышленное исполнение

Общий вид аппаратной платформы UNA в промышленном исполнении представлен на рисунке.

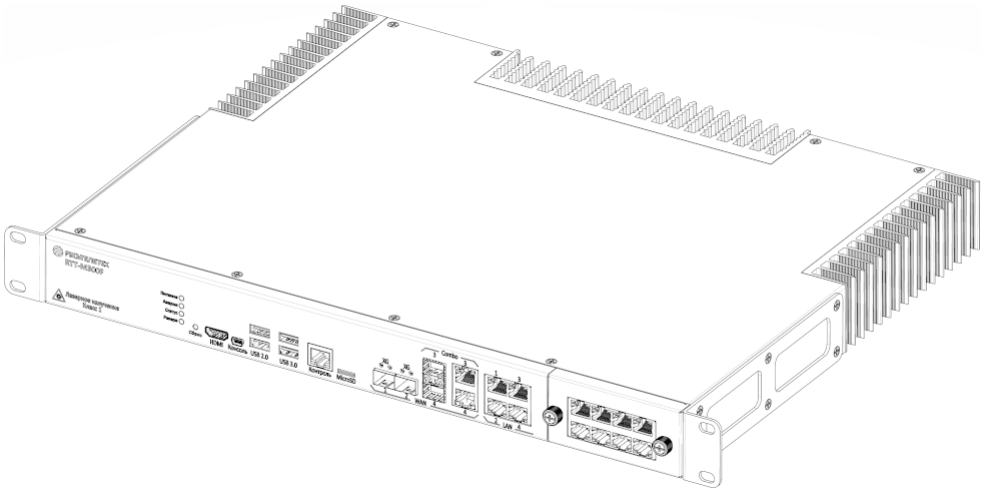


Рис. 7: Внешний вид аппаратной платформы UNA

Габаритные размеры аппаратной платформы UNA в промышленном исполнении приведены на рисунке ниже.

Передняя панель аппаратной платформы UNA показана на рисунке.

Описание элементов передней панели аппаратной платформы UNA приведено в таблице.

Таблица 5: Описание элементов передней панели аппаратной платформы UNA

Порядковый номер	Описание элемента	Примечание
1	Индикация	
2	Кнопка сброса	
3	Разъём HDMI 2.0	
4	Консоль	
5	Порт USB 2.0 Host	2 шт.
6	Порт USB 3.0 Host	2 шт.
7	Порт Контроль Fast Ethernet	
8	Слот для подключения microSD	
9	Порт 10G SFP+	2 шт.
10	Порт 1GE SFP (combo)	2 шт.
11	Порт 1GE RJ-45 (combo)	2 шт.
12	Порт 1G Ethernet (медные)	4 шт.
13	Слот для установки модуля расширения	

Задняя панель аппаратной платформы UNA показана на рисунке.

Описание элементов задней панели аппаратной платформы UNA приведено в таблице .

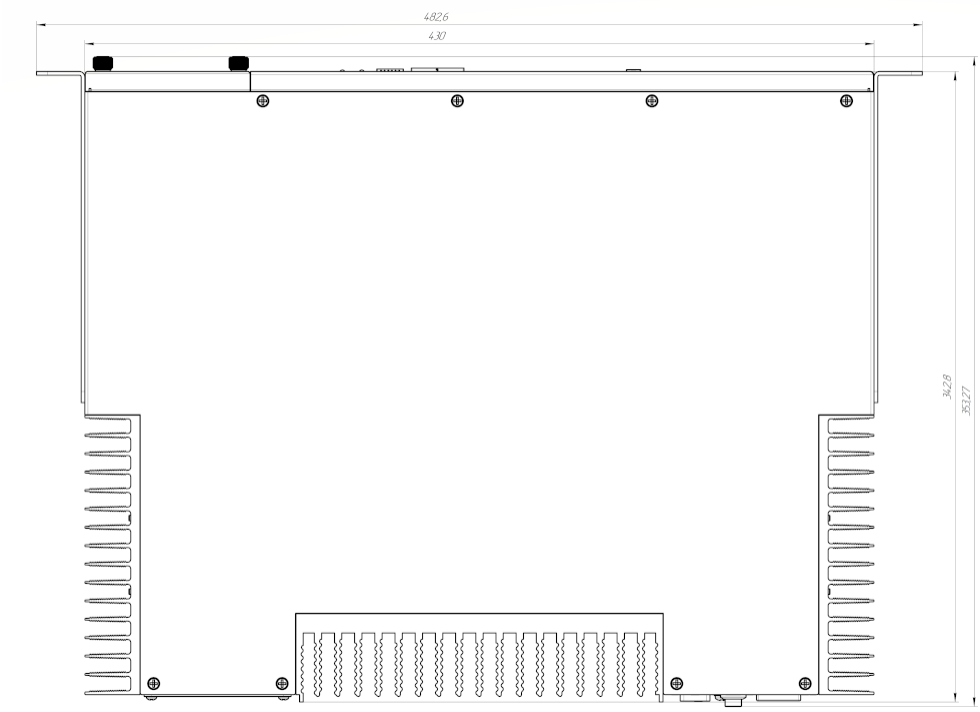


Рис. 8: Вид сверху

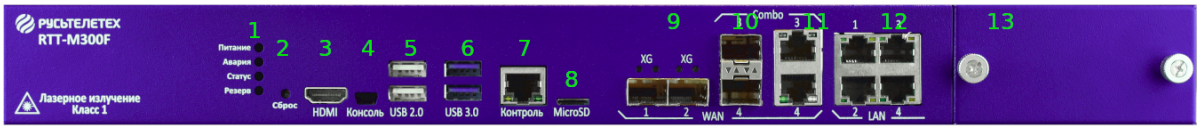


Рис. 9: Передняя панель аппаратной платформы UNA

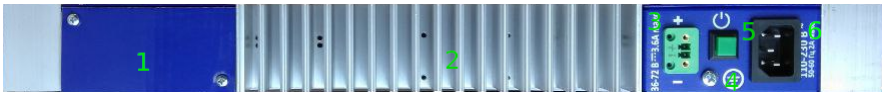


Рис. 10: Задняя панель аппаратной платформы UNA

Таблица 6: Описание элементов задней панели аппаратной платформы UNA

Порядковый номер	Описание элемента	Примечание
1	Слот для установки модуля расширения	
2	Радиатор	
3	Разъём подключения питания 36-72DC	
4	Винт заземления	
5	Кнопка включения	
6	Разъём подключения питания 110В/220В AC	

Компоновка элементов внутри корпуса аппаратной платформы UNA представлена на рисунке.

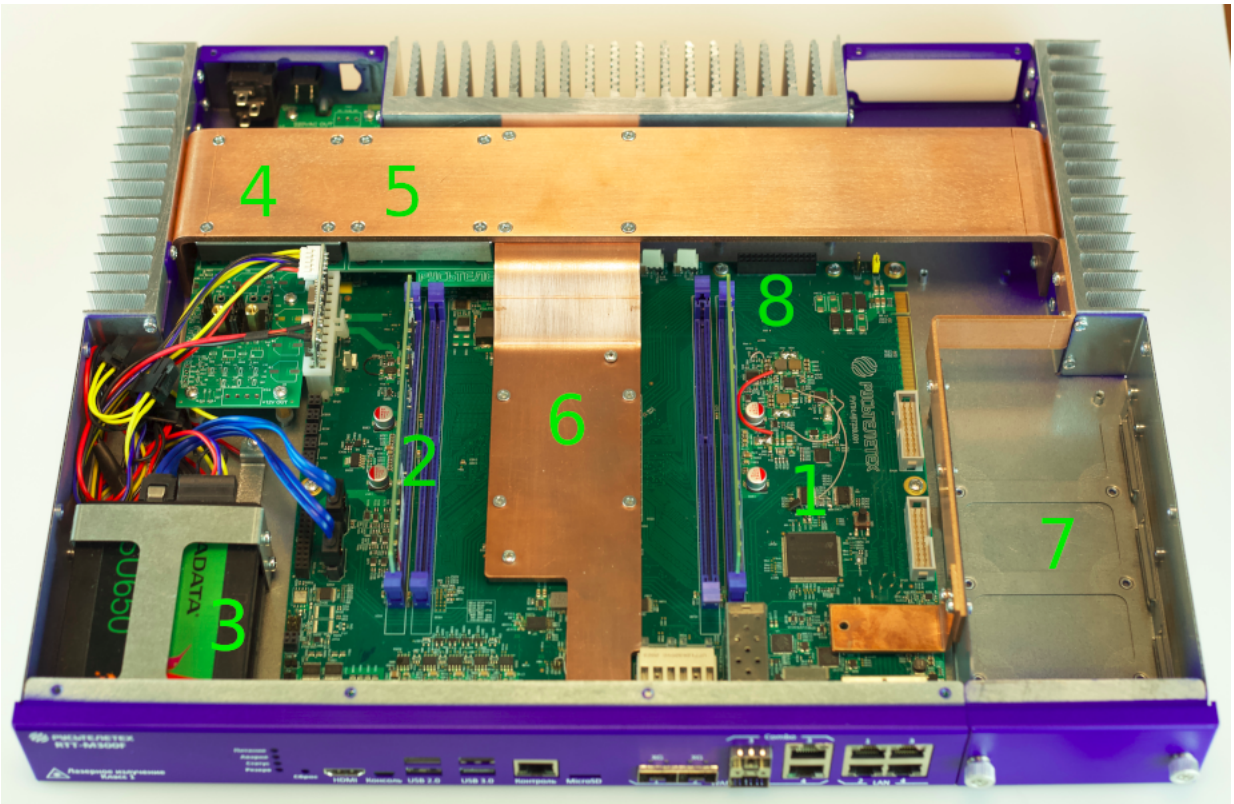


Рис. 11: Компоновка элементов внутри корпуса аппаратной платформы UNA

Описание компоновки элементов внутри корпуса аппаратной платформы UNA приведено в таблице.

Таблица 7: Описание компоновки элементов внутри корпуса аппаратной платформы UNA

Порядковый номер	Описание элемента	Примечание
1	Основная плата	
2	ОЗУ	DIMM DDR4
3	ПЗУ	SSD SATA3
4	Блок питания 1	
5	Блок питания 2	
6	Медная шина	
7	Модуль расширения 1	
8	Модуль расширения 2	

Аппаратной платформа UNA в промышленном исполнении имеет две версии, описание которых приведены в таблице.

Таблица 8: Версии аппаратной платформы UNA в корпоративном исполнении

Обозначение изделия	Описание
RTT-UNAF	Исполнение с пассивным охлаждением для применения в промышленных коммуникационных сетях
RTT-UNAF-X	Исполнение с пассивным охлаждением для применения в промышленных коммуникационных сетях с двумя интегрированным интерфейсами 10 GE (SFP+)

3.4 Карты расширения

Для гибкого расширения портовой ёмкости и возможности конфигурации интерфейсов ввода-вывода для специфических задач в платформу могут устанавливаться разные модули расширения.

Для установки модулей расширения в платформе предусмотрен слот расширения на передней панели и слот расширения на задней панели.

Слот расширения на передней панели предназначается для установки модулей с высокоскоростными интерфейсами ввода-вывода (10GE SFP+, GE). Карты, устанавливаемые в этот слот, являются съёмными и могут меняться в процессе эксплуатации устройства.

Слот расширения на задней панели предназначается для установки модулей с низкоскоростными интерфейсами ввода-вывода (CAN, RS485, Реле и т. д.). Карты, устанавливаемые в этот слот, являются несъемными и не могут меняться в процессе эксплуатации устройства. Карты устанавливаются и(или) меняются при производстве или в сервисе ООО «РТТ».

Примечание

Все модули по умолчанию являются «Cold Plug», то есть при установке и(или) замене модуля необходима перезагрузка устройства для корректной инициализации модуля. Реализация «Hop Plug» дочерних карт возможна в специальных версиях изделия.

Список доступных карт расширения представлен в таблице ниже:

Таблица 9: Сведения о встроенном программном обеспечении

Наименование карты	Описание	Способ установки
UNA-8xGE	8 маршрутизируемых портов GE	Слот на передней панели
UNA-2x10G-SFP+	2 маршрутизируемых порта XGE SFP+	Слот на передней панели
UNA-P	2xCAN/2xRS485/DI/DO/AI/AO/Relay (в разработке)	Слот на задней панели
UNA-8xSW	8-портовый управляемый коммутатор GE (в разработке)	Слот на передней панели

3.5 Технические характеристики

Аппаратные, технические и климатические характеристики аппаратной платформы UNA приведены в таблице.

Таблица 10: Аппаратные, технические и климатические характеристики аппаратной платформы UNA

Характеристика	Корпоративное исполнение	Промышленное исполнение
Исполнение/форм-фактор	1U (19” rack)	
Центральный процессор	BE-M1000 (Baikal-M)	
Количество ядер	8	
Архитектура процессора	ARM Cortex-A57	
Частота процессора	1500 МГц	
ОЗУ	До 64 Гбайт (до 4 модулей DIMM) 2400МГц DDR4	
Подключение жестких дисков	2 порта SATA 3.0	
Сетевые порты	4x1GE 2x10GE (версии с индексом X) 2x2GE (комбинированный)	
Карты расширения сетевых портов	2 порта SATA 3.0	
Выделенный (out-of-band) порт управления	1xFastEthernet	
Степень защиты от пыли и влаги	IP20	IP30
Пассивное охлаждение	Нет	Да
Диапазон рабочих температур	-5 °C … +50 °C	-10 °C … +60 °C
Подключение промышленной периферии	CAN RS-485 RS-232/422 Аналоговый вх. 20мА Аналоговый вых. Цифровой вх. 12V Цифровой вых. 12V «Сухие контакты»	

Сведения о встроенном программном обеспечении представлены в таблице.

Таблица 11: Сведения о встроенном программном обеспечении

Характеристика	Примечание
Загрузчик	EDK II UEFI
Интерфейсы управления	USB 2.0 (host) USB 3.0 (host) Mini-USB2.0 (device)
Интерфейс для подключения монитора	HDMI
Интерфейсы загрузки прикладного ПО	USB 2.0 (host) USB 3.0 (host) SATA (внутренний разъем)
Поддерживаемые операционные системы	ОС семейств GNU/Linux и FreeBSD (актуальный лист совместимости уточняйте у производителя)
Передача конфигурации аппаратного обеспечения в прикладное ПО	Переменные EFI

Сведения об электропитании аппаратной платформы UNA приведены в таблице.

Таблица 12: Сведения об электропитании

Характеристика	Корпоративная версия	Промышленная версия
Резервные блоки питания	Нет	Да
БП1	110В/220В AC	110В/220В AC
БП2	Нет	36В...72В DC

3.6 Сценарии применения

3.6.1 Целевые применения

Платформа UNA в промышленном исполнении используется в качестве аппаратной платформы для:

- Сетевых устройств обработки и маршрутизации трафика в технологических сетях (маршрутизаторов, межсетевых экранов, шлюзов безопасности и т.д.);
- Управляемых коммутаторов для технологических сетей (с картой расширения UNA-8xSW);
- Промышленных компьютеров с разнообразной периферией для подключения в сеть и(или) устройств автоматизации;
- Промышленных контроллеров (при установке карты расширения промышленных интерфейсов);
- IoT шлюзов.

Аппаратная платформа UNA в корпоративном исполнении используется в качестве:

- Сетевых устройств обработки и маршрутизации трафика в корпоративных сетях (маршрутизаторов, межсетевых экранов, шлюзов безопасности и т.д.);
- Управляемых коммутаторов для корпоративных сетей (с картой расширения UNA-8xSW);
- Устройств доступа в сеть (network access device);
- IoT шлюзов.

Примечание

На базе платформы UNA построена линейка межсетевых экранов RTT-M300(F)

3.6.2 Программное обеспечение

Аппаратная платформа UNA поставляется с предустановленным системным программным обеспечением (загрузчики, дерево устройств), необходимым для корректной работы операционных систем семейства GNU/Linux.

Дополнительно вместе с аппаратной платформой поставляется BSP в виде исходных кодов программ, содержащий адаптированное ядро Linux, набор драйверов периферии и модуль интеграции для пространства пользовательских приложений.

Следующие дистрибутивы семейства GNU/Linux могут быть запущены на аппаратной платформе UNA без переборки и(или) адаптации ядра:

- дистрибутив REFOS;
- Alt Linux Workstation (сборка для Baikal-M).

Примечание

О возможности поддержки дистрибутивов уточняйте в отделе сервиса ООО «РТТ»

3.7 Требования безопасности

Для предотвращения перегрева аппаратной платформы UNA не эксплуатируйте ее в зоне, где окружающая температура превышает максимальное рекомендуемое значение плюс 50 °C (для корпоративного исполнения) и плюс 60 °C (для промышленного исполнения).

Чтобы обеспечить нормальный воздушный поток для корпоративного исполнения аппаратной платформы UNA, оставьте зазор не менее 7,5 см вокруг вентиляционных отверстий.

К эксплуатации аппаратной платформы UNA допускаются лица, изучившие данное **Руководство**.

При проведении работ с аппаратной платформой UNA должны выполняться требования по технике безопасности, пожарной безопасности и производственной санитарии в соответствии с инструкциями, действующими на эксплуатирующем предприятии.

Чтобы избежать травм при монтаже или обслуживании аппаратной платформы UNA в стойке необходимо принять особые меры предосторожности, обеспечивающие механическую устойчивость стойки, в которую установлена аппаратная платформа UNA:

- если аппаратная платформа UNA является единственным в стойке, то следует ее монтировать внизу стойки;
- при установке аппаратной платформы UNA в частично заполненную стойку наполняйте стойку снизу вверх, устанавливая самые тяжелые компоненты в нижней части стойки;
- если стойка оснащена устройствами повышения устойчивости, устанавливайте стабилизаторы перед началом монтажа или обслуживания аппаратной платформы UNA в стойке.

Изделие подлежит заземлению. Никогда не повреждайте провод заземления и не эксплуатируйте оборудование без правильно смонтированного провода заземления. При возникновении любых сомнений

по поводу заземления обратитесь в соответствующий орган по контролю электрооборудования или электрику.

При установке или замене аппаратной платформы UNA заземляющее соединение должно всегда выполняться в первую очередь и отключаться в последнюю.

Вилка кабеля питания и розетка сети электропитания должны быть постоянно доступны.

Установку, замену и обслуживание данного оборудования может выполнять только специально обученный и квалифицированный персонал.

При выборе места для размещения аппаратной платформы UNA необходимо соблюдать следующие требования:

- зазор до передней и задней панели должен соответствовать следующим условиям:
  - пользователь видит светодиодные индикаторы на передней панели;
  - доступ к портам достаточен для свободной подводки кабелей;
  - силовой разъем на задней панели находится вблизи розетки переменного тока.
- кабели проложены на безопасном расстоянии от других устройств, которые могли бы повредить их;
- поток воздуха вокруг аппаратной платформы UNA и сквозь вентиляционные отверстия (для «вентиляторного» исполнения) не перекрыт.

3.8 Подключение и начало работы

Для корректной работы аппаратной платформы UNA необходимо:

- подключить аппаратную платформу UNA к сети питания (стандарт питания указывается в паспорте Изделия);

Примечание

При подключении на лицевой панели аппаратной платформы UNA индикатор загорится желтым цветом

Рис. 12: Подключение аппаратной платформы UNA к сети

- нажать кнопку включения питания, находящуюся на задней панели аппаратной платформы UNA;

Рис. 13: Включение питания

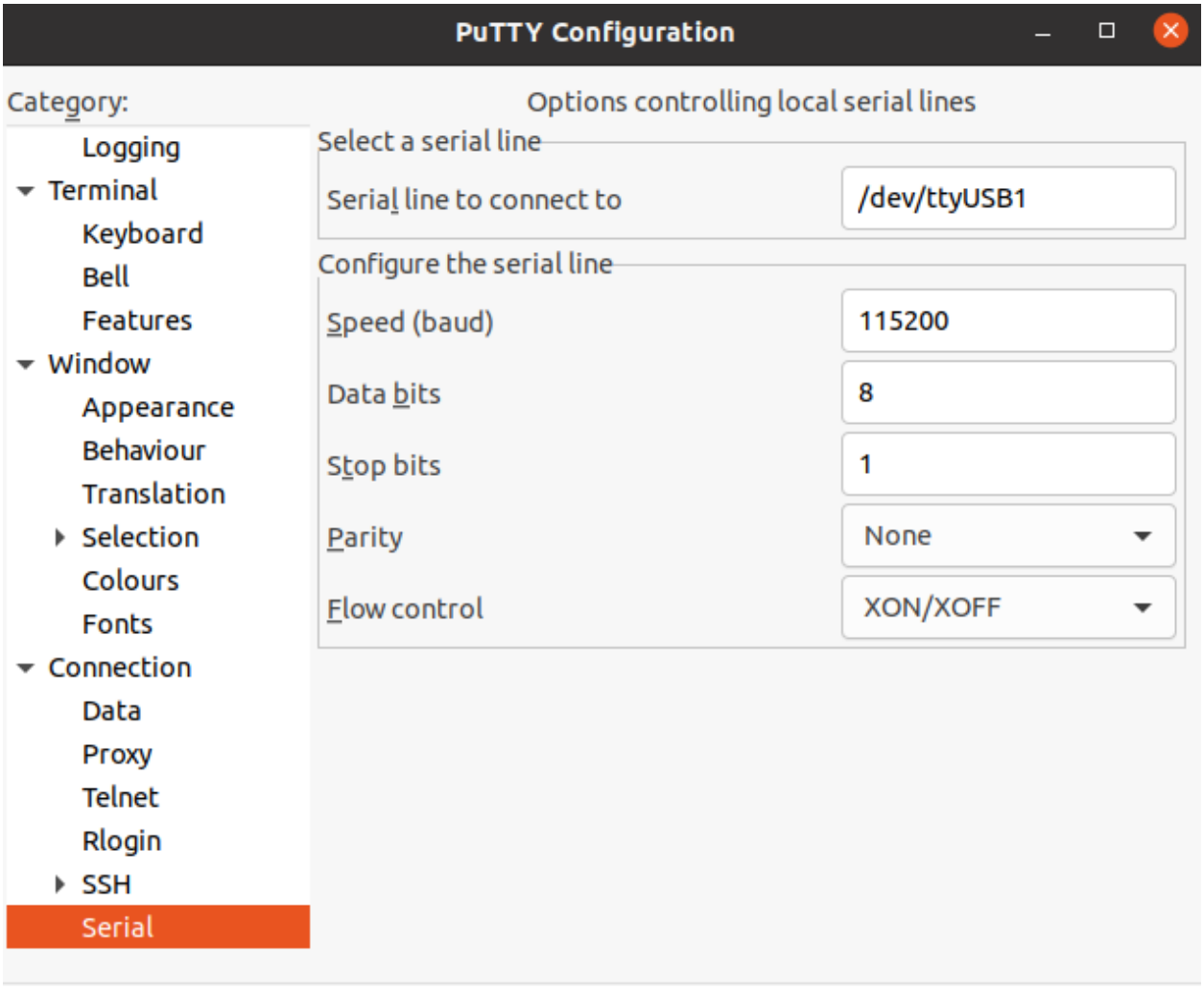
Примечание

При подключении питания аппаратной платформы UNA индикатор загорится зеленым цветом

Примечание

Признаком корректной работы аппаратной платформы UNA являются три индикатора на лицевой панели, горящие зеленым цветом

- Для работы с консолью устройства необходимо подключиться к интерфейсу **«Консоль»** при помощи кабеля Mini USB и открыть сессию консоли в терминале (putty, pricocom или аналогичные программы). Настройки последовательного порта приведены ниже;
- При запуске устройства будут выведены системные сообщения об основных этапах загрузки платформы и возникающих при этом ошибках (в случае неисправности). В случае отсутствия операционной системы на дисках, загрузка останавливается на меню UEFI загрузчика, где можно в ручном режиме указать диск, с которого будет произведена загрузка ОС, а также представлены основные системные настройки.


PuTTY Configuration
Category:
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Fonts
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Options controlling local serial lines
Select a serial line
Serial line to connect to
/dev/ttyUSB1
Configure the serial line
Speed (baud)
115200
Data bits
8
Stop bits
1
Parity
None
Flow control
XON/XOFF

3.9 Световая индикация

Системные индикаторы (Power, Master, Fan, RPS) служат для определения состояния работы узлов МЭ серии RTT-M300.

Таблица 13: Системные индикаторы

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Питание	Состояние источника питания	Выключен	Питание выключено
		Желтый	Питание на устройство подано, но система не запущена
		Зеленый	Питание включено, нормальная работа устройства
		Красный	Устройство аварийно выключилось.
Авария	Индикатор возникновения аварий	Зеленый	Нормальная работа устройства
	Переключение режима работы МЭ	Зеленый (Моргание)	Режим Пользовательский
		Красный (Моргание 200мс)	Режим Пропускать всё
		Красный (Моргание 500мс)	Режим Отклонять всё
Статус	Индикатор загрузки ЦП	Зеленый	Загрузка ресурсов ЦП не более 65%
		Желтый	Загрузка ресурсов ЦП более 65%
Резерв	Индикатор службы резервирования IP-адреса (CARP)	Выключен	Служба резервирования IP-адреса (CARP) не запущена.
		Зеленый	Служба резервирования IP-адреса (CARP) запущена.