IVA SBC 6.X

Admin Guide

TECHNOLOGIES

Оглавление

Введение

Настоящий документ является руководством администратора **пограничного контроллера сессий IVA SBC**.

Руководство администратора описывает назначение, условия и порядок функционирования системы, а также действия Администратора по настройке IVA SBC.

О системе

IVA Technologies – российский производитель телекоммуникационного оборудования и программного обеспечения. Решения на базе оборудования и программного обеспечения IVA позволяют выстраивать безопасную, высокопроизводительную ИТ-инфраструктуру различных масштабов.

Пограничный контроллер сессий IVA SBC устанавливается на границе сетей для обеспечения фильтрации трафика, не соответствующего установленным правилам, и безопасного соединения между пользователями в режиме реального времени, а также позволяет подключить корпоративную коммуникационную инфраструктуру к другим сетям (Интернет, внутренняя сеть).

Требования к Администратору IVA SBC

Базовые знания ОС Linux	Удалённый доступ к консоли с помощью SSH Понимание файловой структуры и навигации по ней Редактирование текстовых файлов с помощью vi и nano Использование распространённых сетевых утилит ping, ifconfig, traceroute и т. д. Знание базовых утилит для System Troubleshooting: top, ps, netstat и т. д.
Начальные знания сетевых технологий и стека протоколов TCP / IP	Знание понятий: IP-адрес, маска сети, шлюз Общее понимание принципов IP-маршрутизации Знания особенностей протоколов TCP и UDP Общее представление о протоколах DNS, NTP, SMTP, HTTP Понимание принципов работы NAT, межсетевых экранов, прокси-серверов

	Общее представление о протоколе SSL, о методах обеспечения защищённого обмена данными с использованием SSL-сертификатов
Общее понимание протоколов работы телефонии и видео-конференцсвязи	Представление о протоколе SIP Представление о протоколе H.323 Представление о технологии WebRTC Понимание принципов передачи медиапотоков (SDP, RTP)

Требования к параметрам серверов

Перед настройкой IVA SBC необходимо проверить серверное оборудование на соответствие следующим минимальным требованиям:

	Сервер проксирования (до 100 подключений) Сервер управления и конфигурации (до 1000 подключений)
Процессор	Intel: не менее Intel Core-i3 AMD: аналогичный процессорам семейства Intel
Количество ядер	не менее 2 ядер с частотой не менее 2 ГГц
Микроархитектура	Sandy Bridge / Zen
Оперативная память	не менее 4 ГБ
Жесткий диск	не менее 20 ГБ
Сетевые интерфейсы	1 Гбит/с и более

Нагрузка на сервер проксирования IVA SBC зависит от типа и скорости передачи данных. В среднем на одного участника (с подключением любого типа) проходящего через IVA SBC мероприятия необходимо 1,2 % ядра процессора при скорости передачи и приема данных 1 Мбит/с.

Для поддержания 300 пользователей, не участвующих в мероприятии, серверу проксирования требуется производительность одного ядра процессора.

Схема работы IVA SBC

Пограничный контроллер сессий IVA SBC позволяет Администратору настраивать возможность анализа и пропуска трафика различного типа из одной сети в другую.

IVA SBC позволяет добавлять и настраивать следующие типы маршрутизации:

- VoIP-маршрутизацию – маршрутизация SIP- и H.323-трафика
- HTTP Reverse-маршрутизацию – маршрутизация HTTP-трафика на внутренние сетевые адреса
- HTTP Proxy-маршрутизацию – маршрутизация HTTP-трафика на внешние сетевые адреса
- TURN-маршрутизацию – пропуск RTP через TURN-сервер

Общая схема работы IVA SBC представлена ниже Рисунок 1.

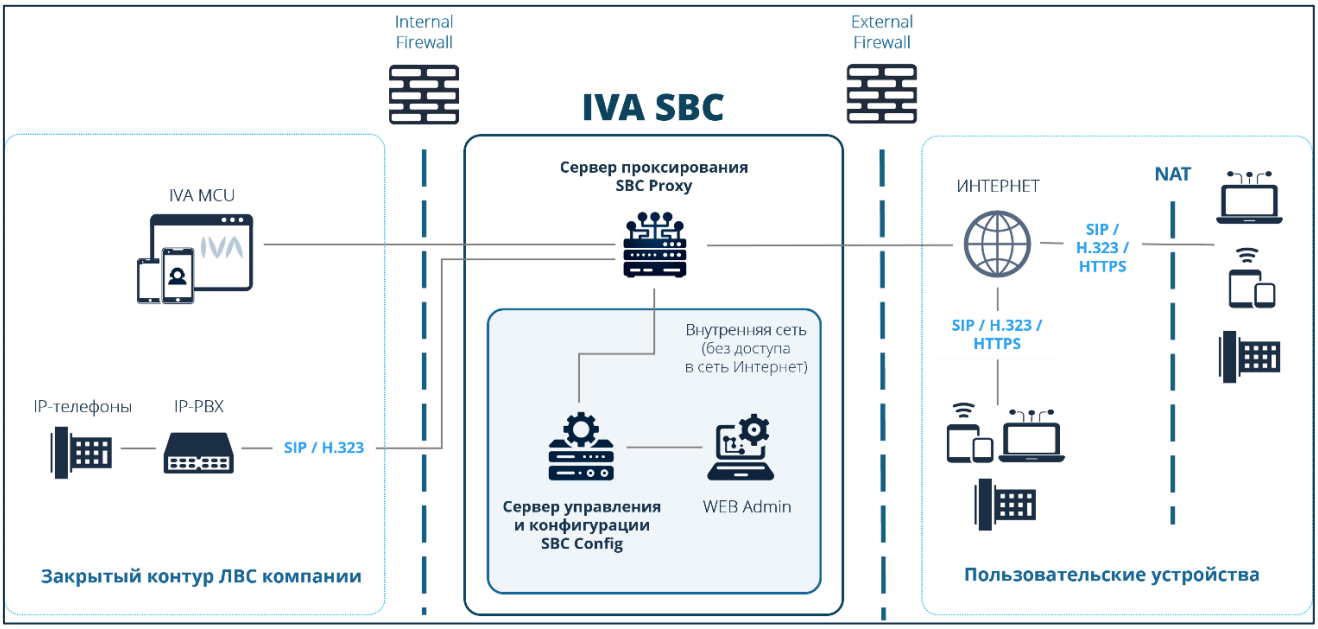

Рисунок 1. Схема работы IVA SBC

IVA SBC представляет собой модульное ПО, обеспечивающее работу двух типов серверов:

- Сервер проксирования – выполняет основную работу по проксированию, анализу и пропуску трафика из одной сети в другую. Сервер проксирования отвечает за маршрутизацию различных типов трафика (HTTP, SIP, H.323, TURN) как всех вместе, так и по отдельности. Сервер проксирования загружает свою конфигурацию с сервера управления и конфигурации, но может работать и без него (если ранее уже была загружена конфигурация)

- Сервер управления и конфигурации – выполняет функции управления серверами проксирования, настраивается и управляется Администратором системы через web-панель администрирования. Сервер управления и конфигурации также собирает и хранит данные от журналов аудита и VVoIP-звонков, сервисов мониторинга и т. д. Для работы сервера управления и конфигурации не требуется доступ в интернет, он должен иметь доступ только к серверам проксирования по локальной сети.

Вход в IVA SBC

Вход в систему

Настройка и управление IVA SBC выполняется в **web-панели администрирования**. Доступ к web-панели администрирования есть у пользователей, которые обладают правами Администратора или Оператора.

Чтобы начать администрирование IVA SBC, необходимо: Авторизоваться.

Авторизация

Доступ в систему предоставляется только авторизованным пользователям.
Чтобы авторизоваться в IVA SBC, необходимо:

1. в адресной строке браузера ввести **<SBC_CFG_IP>:11960**, где **<SBC_CFG_IP>** – IP-адрес сервера управления и конфигурации IVA SBC
2. в окне **Вход в систему** Рисунок 2 ввести:
   - **Логин**: логин пользователя IVA SBC
   - **Пароль**: пароль пользователя IVA SBC
3. нажать кнопку **Войти**

> Для первого входа в IVA SBC после установки необходимо использовать учётные данные администратора, созданные по умолчанию:
> - **Логин**: admin
> - **Пароль**: Iva#Sbc23

> Если **ввести пароль неправильно** 3 раза в течение 5 минут, то вход с данного IP-адреса будет **заблокирован** на 30 минут

После первого входа в IVA SBC, для обеспечения безопасности, **необходимо изменить стандартный пароль** администратора. В противном случае IVA SBC подвержена риску несанкционированного доступа. В дальнейшем для доступа в IVA SBC необходимо использовать персонализированные учётные записи, а стандартную учётную запись администратора заблокировать или удалить

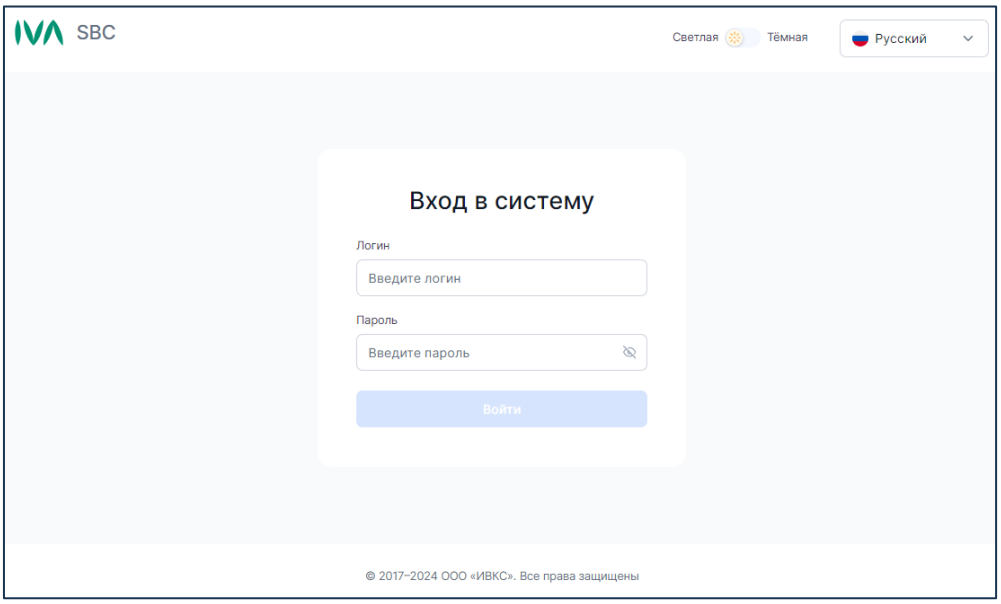

Рисунок 2. Вход в систему

На странице **Вход в систему** Рисунок 2 доступны возможности:

- сменить язык интерфейса: Русский / Английский
- сменить тему интерфейса: Светлая / Тёмная

Основной экран авторизованного пользователя

После авторизации пользователь попадает в **Web-панель администрирования** системы IVA SBC Рисунок 3.

С помощью панели навигации осуществляется переход в разделы web-панели администрирования.

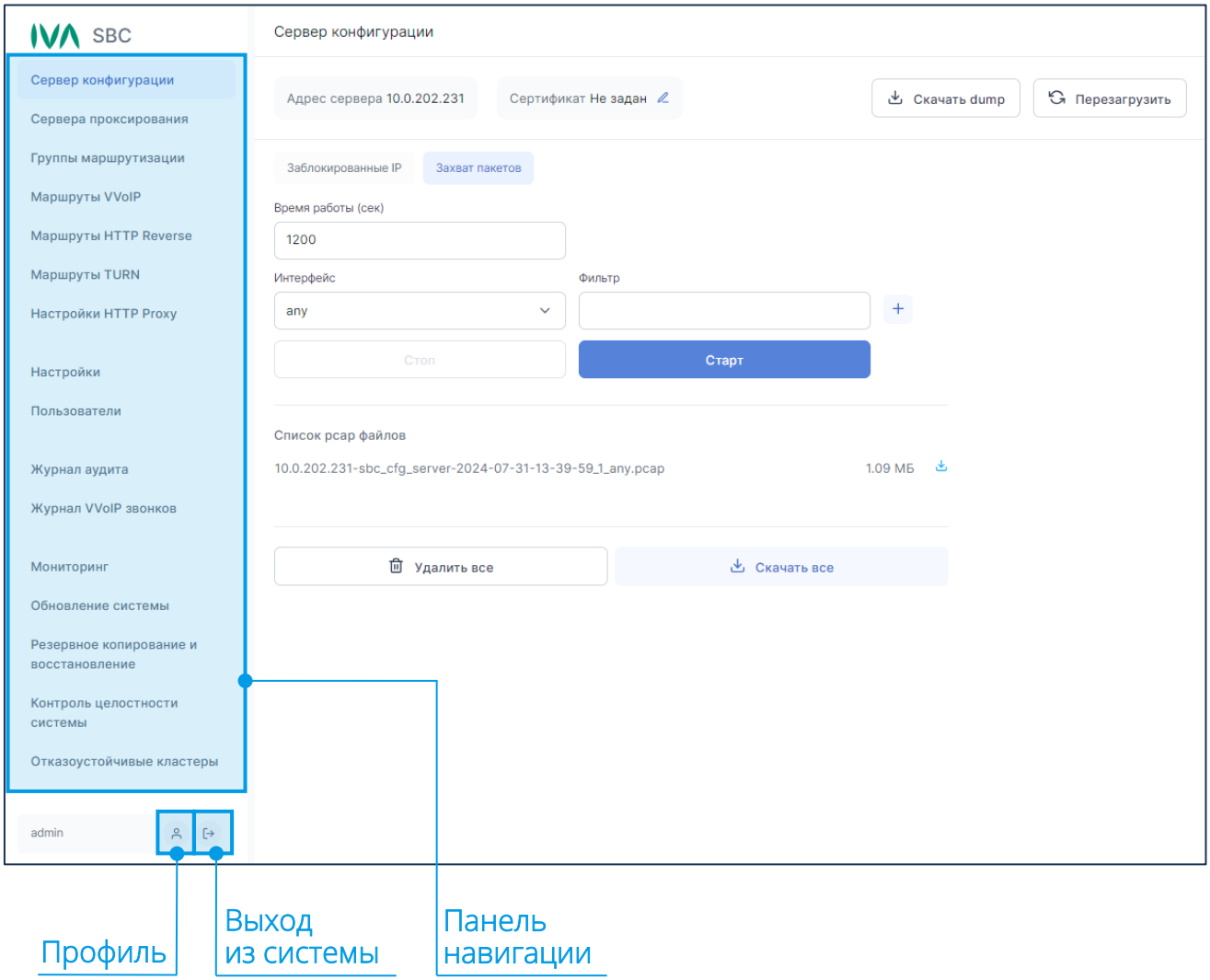

Рисунок 3. Web-панель администрирования

Основные разделы Web-панели администрирования:

- Сервер конфигурации – добавление и изменение сертификата (используемого для web-администрирования), просмотр заблокированных IP-адресов, скачивание dump, снятие pcap-данных и перезагрузка сервера конфигурации
- Сервера проксирования – подключение, настройка и отключение серверов проксирования
- Группы маршрутизации – настройка групп маршрутизации трафика
- Маршруты VoIP – настройка правил маршрутизации VoIP-звонков
- Маршруты HTTP Reverse – настройка правил маршрутизации HTTP-запросов из внешней сети на внутренние сетевые адреса
- Маршруты TURN – настройка правил для TURN-подключений

- Настройки HTTP Proxy - настройка параметров HTTP-проксирования из внутренней сети на внешние сетевые адреса по паролю пользователя и его IP-адресу
- Настройки:
  - Настройки сертификата – настройка используемых SSL-сертификатов
  - Внешние HTTP прокси сервера – настройка доверенных внешних HTTP-прокси-серверов
  - Системные настройки – настройки системы (NTP, Zabbix, DNS и т. д.)
- Пользователи – управление администраторами и операторами системы
- Журнал аудита – журнал действий операторов и администраторов
- Журнал VoIP звонков – журнал VoIP-звонков, прошедших через систему
- Мониторинг – мониторинг нагрузки на серверах IVA SBC
- Обновление системы – настройка параметров сервера обновления и обновление серверов IVA SBC
- Резервное копирование – настройка и создание резервной копии базы данных, восстановление базы данных из резервной копии
- Контроль целостности системы – просмотр изменений и восстановление изменений в файловой системе
- Отказоустойчивые кластеры – настройка плавающих IP-адресов, переходящих между серверами проксирования
- Профиль – управление собственным профилем пользователя
- Выход из системы – выход из системы IVA SBC

Управление сервером конфигурации

Раздел **Сервер конфигурации** Рисунок 4 позволяет выполнить следующие действия с сервером управления и конфигурации:

- настроить используемый SSL-сертификат для web-интерфейса сервера управления и конфигурации
- посмотреть список заблокированных IP-адресов на сервере управления и конфигурации
- выполнить захват пакетов на сервере управления и конфигурации
- **скачать dump-файл:** нажать кнопку **Скачать dump**
- перезагрузить сервер управления и конфигурации

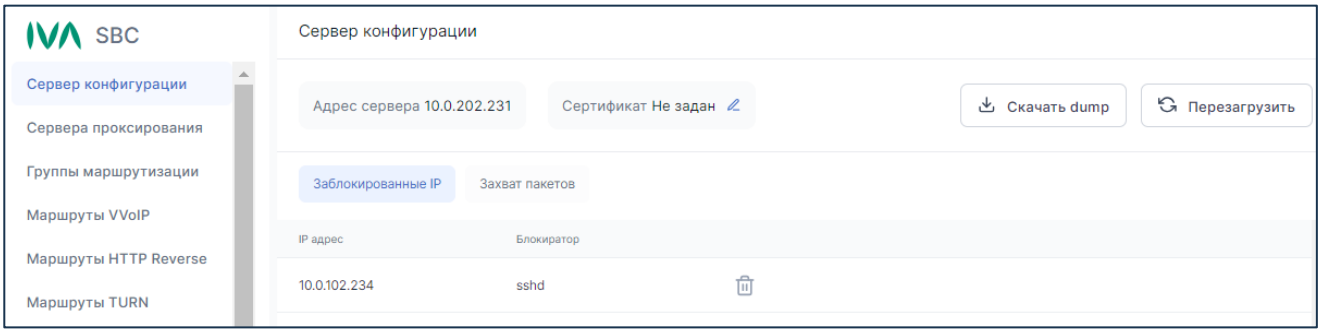

Рисунок 4. Раздел Сервер конфигурации

Настройка используемого SSL-сертификата для web-интерфейса

Чтобы изменить **SSL-сертификат** для **web-интерфейса** сервера управления и конфигурации, необходимо:

1 перейти в раздел **Сервер конфигурации** Рисунок 4

2 **Сертификат:** нажать кнопку

3 в окне **Выбор сертификата** Рисунок 5 открыть **выпадающий список** и **выбрать сертификат**

4 нажать кнопку **Сохранить**

> Выбор SSL-сертификата доступен из уже добавленных SSL-сертификатов

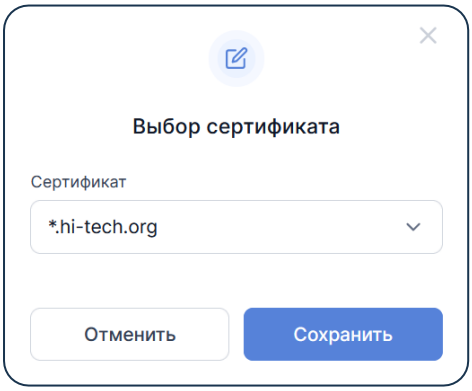

Рисунок 5. Выбор сертификата

Список заблокированных IP-адресов на сервере управления и конфигурации

В IVA SBC стандартно настроен Fail2Ban, который автоматически блокирует IP-адреса, активность которых является подозрительной.

Например, если с определенного IP-адреса происходит более 4 раз подряд (в течение 10 минут) неправильное введение пароля для доступа к **серверу управления и конфигурации** IVA SBC по SSH, то этот IP-адрес будет заблокирован (на 5 минут) и отображён в разделе **Сервер конфигурации** на вкладке **Заблокированные IP** Рисунок 4.

Чтобы **разблокировать** заблокированный IP-адрес, необходимо на вкладке **Заблокированные IP** Рисунок 4 удалить его из списка: **нажать кнопку**

> Удаление заблокированных IP-адресов из списка заблокированных IP-адресов происходит **без подтверждения удаления**

Захват пакетов на сервере управления и конфигурации

Чтобы **проанализировать сетевой трафик** сервера управления и конфигурации IVA SBC, необходимо:

1 перейти на вкладку **Захват пакетов** Рисунок 6:

- **Время работы (сек)**: ввести время работы в секундах (например **1200**)
- Интерфейс:
  - **any**: любой интерфейс

  - eth0: сетевой интерфейс Ethernet
  - lo: виртуальный интерфейс для локальных тестов и отладки (loopback device)
- Фильтр: установить значение (в формате tcpdump)

2 нажать кнопку Старт

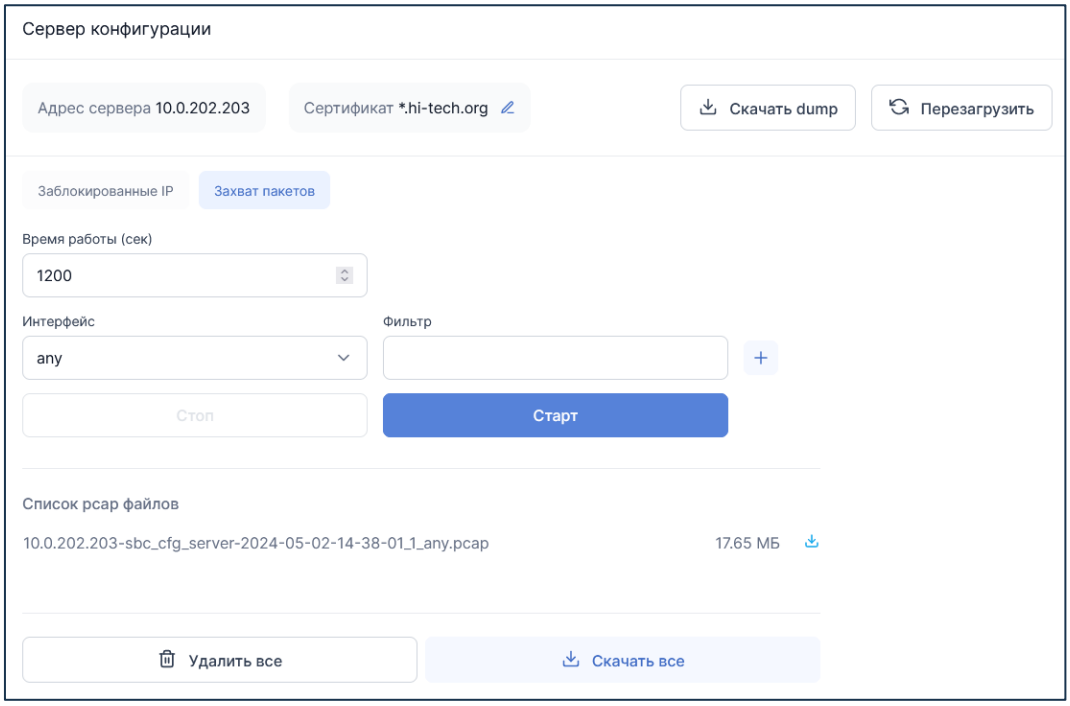

Рисунок 6. Захват пакетов сервера конфигурации

После завершения захвата трафика Рисунок 6 можно:

- скачать сформированные pcap-файлы: выбрать pcap-файл из списка с pcap-файлами и нажать кнопку
- скачать архив с pcap-файлами: нажать кнопку Скачать все
- удалить все сформированные pcap-файлы файлы: нажать кнопку Удалить все

Перезагрузка сервера управления и конфигурации

Чтобы перезагрузить сервер управления и конфигурации, необходимо:

1 в разделе Сервер конфигурации Рисунок 4 нажать кнопку Перезагрузить

2 в окне Перезагрузка сервера Рисунок 7 нажать кнопку Перезагрузить

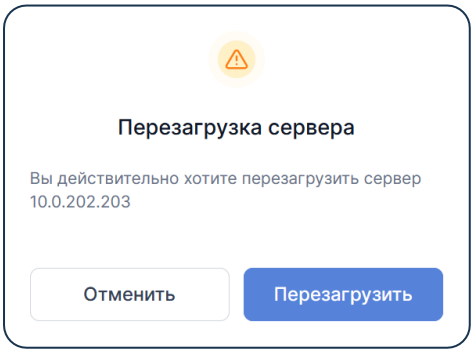

Рисунок 7. Перезагрузка сервера

Настройка сервера проксирования

Раздел **Сервера проксирования** Рисунок 8 отображает **все добавленные сервера проксирования**, содержит информацию с **адресом** и **именем** добавленных серверов, отображает **статус** и добавленные **роли** (HTTP Reverse Proxy, VVoIP Proxy, TURN Proxy и HTTP Proxy) серверов, а также позволяет:

- добавлять новые сервера
- отслеживать информацию о статусе добавленных серверов **Онлайн / Оффлайн**
- добавлять роли проксирования
- настроить правила NAT
- контролировать заблокированные IP-адреса
- настроить TURN-сервер
- анализировать сетевой трафик
- просматривать информацию об IP-адресах на сервере
- выполнять действия над серверами (перезагрузить, скачать dump, удалить)
- редактировать имя сервера проксирования
- настроить список отображаемых серверов

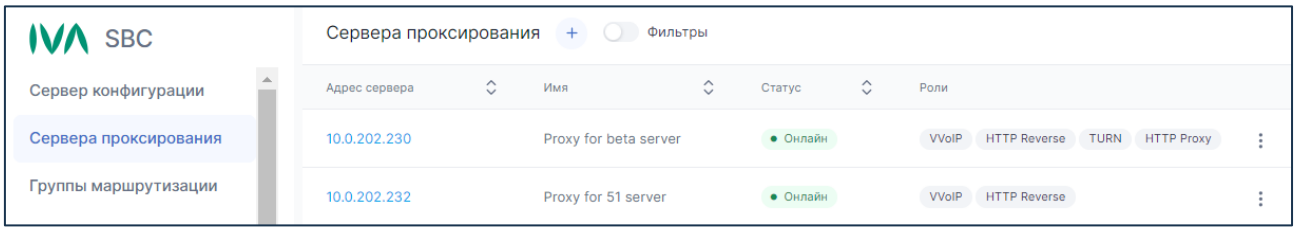

Рисунок 8. Раздел Сервера проксирования

Добавление сервера проксирования

Чтобы **добавить сервер проксирования**, необходимо:

1 перейти в раздел **Сервера проксирования** Рисунок 8 и **нажать кнопку** +

2 в окне **Добавление сервера** Рисунок 9:

- **Адрес сервера:** ввести IP-адрес сервера проксирования SBC (например 10.0.202.201)

- **Имя сервера:** ввести имя (рекомендуется вводить имя, которое кратко описывает назначение сервера проксирования (например Proxy for 51 Server)

3 нажать кнопку **Добавить**

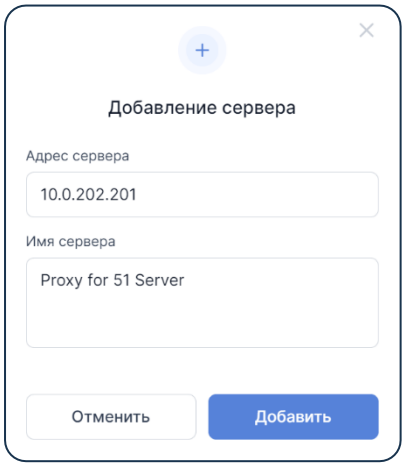

Рисунок 9. Добавление сервера проксирования

> Для добавления **новых серверов проксирования** необходимо в консоли сервера проксирования добавить IP-адрес сервера управления и конфигурации (см. руководство по установке Install Guide IVA SBC)

Просмотр серверов проксирования

Список отображаемых серверов проксирования можно **фильтровать по статусу** (Онлайн / Оффлайн / Все) и / или по **ролям** (VoIP, HTTP Reverse, TURN, HTTP Proxy) Рисунок 10.

Чтобы включить фильтр серверов проксирования, необходимо: нажать **переключатель Фильтры**

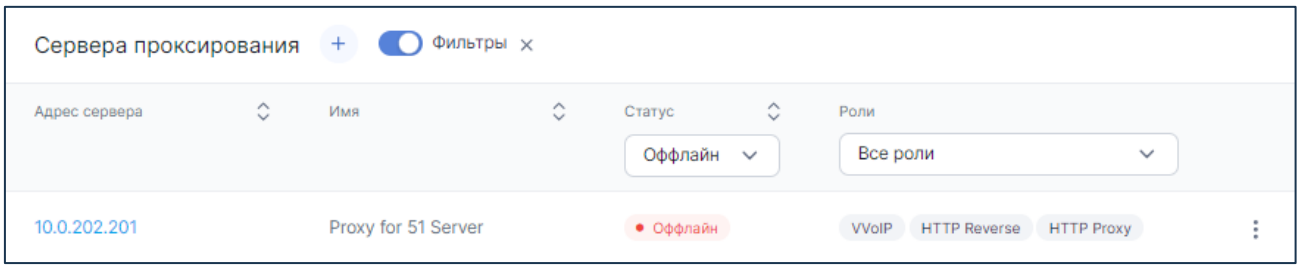

Рисунок 10. Фильтр отображаемых серверов

Добавление ролей проксирования

Сервер проксирования IVA SBC может выполнять несколько ролей проксирования:

- VVoIP
- HTTP Reverse
- TURN
- HTTP Proxy

Чтобы **Сервер проксирования** выполнял определенные роли проксирования, необходимо:

1 перейти в раздел **Сервера проксирования** Рисунок 8

2 нажать ссылку <**IP-адрес сервера проксирования**> (например **10.0.202.232**)

3 на странице **Информация о сервере проксирования** Рисунок 11 перейти на вкладку **Роли** и настроить роли:

- для роли VVoIP: выбрать группу маршрутизации VVoIP и нажать переключатель Активность
- для роли HTTP Reverse: выбрать группу маршрутизации HTTP Reverse и нажать переключатель Активность
- для роли TURN: выбрать группу маршрутизации TURN и нажать переключатель Активность
- для роли HTTP Proxy: нажать переключатель Активность

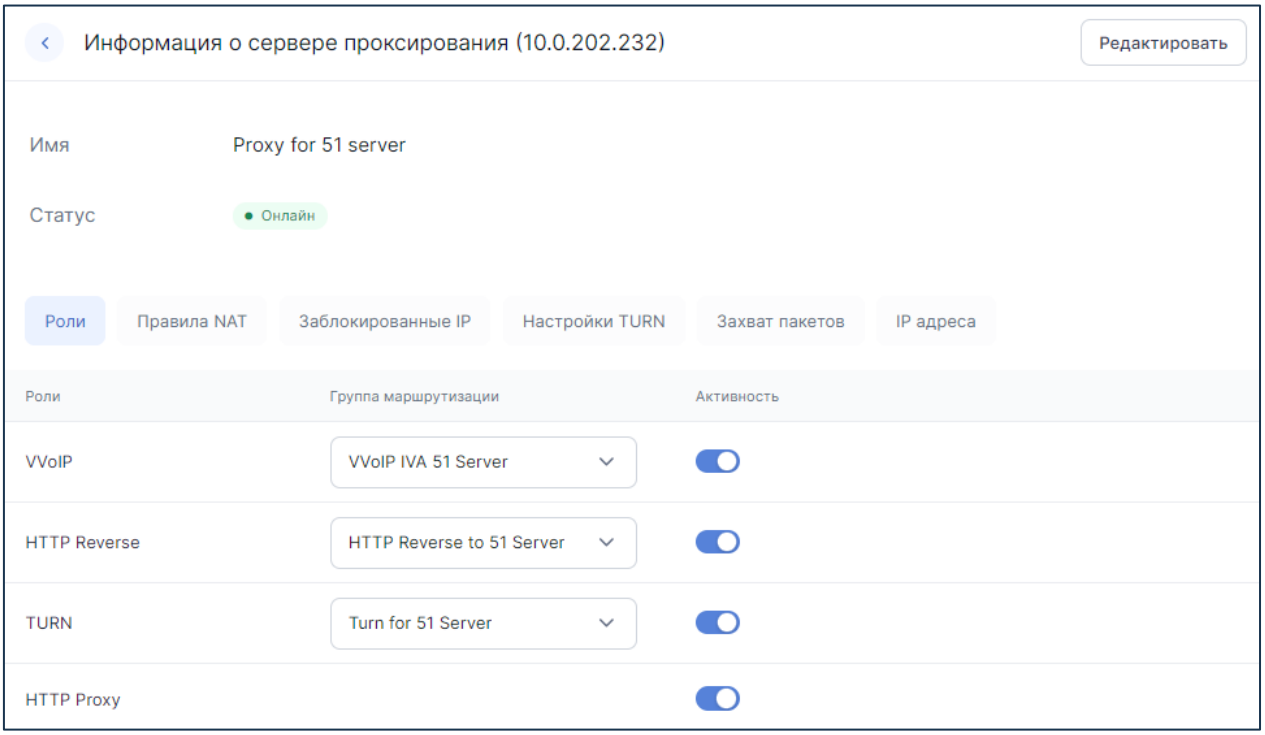

Рисунок 11. Правила фильтрации маршрутов HTTP

Правила NAT

В случае, если сервер проксирования IVA SBC находится за Static NAT или имеет несколько IP-адресов, то чтобы сервер проксирования IVA SBC мог правильно отдавать свой IP-адрес, необходимо настроить список NAT-адресов.

> Правила NAT используются в сервисах для VVoIP-проксирования. Для TURN- и HTTP-проксирования настройка правил NAT не требуется

Добавление правил NAT

Чтобы **добавить правило NAT**, необходимо:

1 перейти в раздел **Сервера проксирования** и нажать ссылку <**Адрес сервера проксирования**> (например **10.0.202.232**)

2 перейти на вкладку **Правила NAT** Рисунок 12 и нажать кнопку **Добавить**

3 в окне **Добавление правила NAT** Рисунок 12:

- **Маска подсети**: ввести маску подсети, для которой будет использоваться специфический IP-адрес (например **10.10.0.0/24**)

- **IP-адрес**: ввести IP-адрес, по которому сервер проксирования будет доступен пользователю из данной сети (например **10.0.202.232**)

4 нажать кнопку **Добавить**

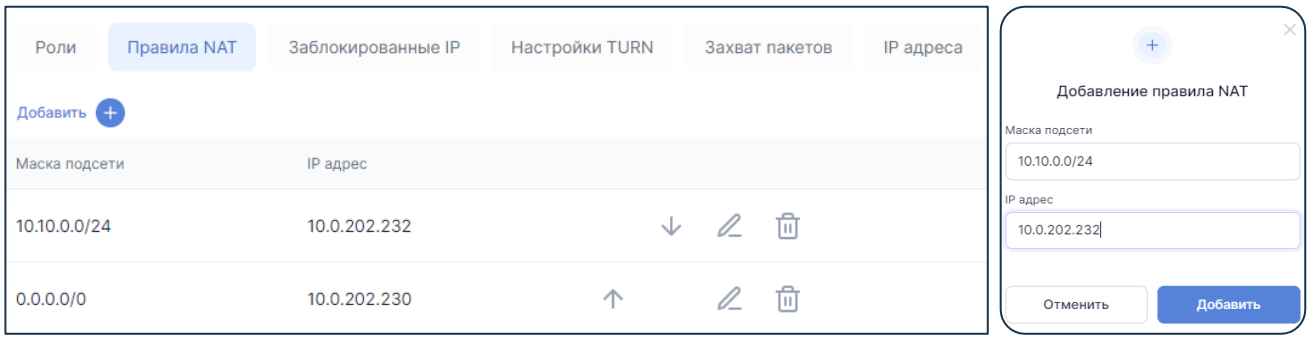

Рисунок 12. Правила NAT и добавление правила NAT

Добавленные правила NAT Рисунок 12 применяются в порядке очереди. Чтобы **изменить порядок** применения добавленных правил (**поднять** или **опустить** правило в очереди), необходимо использовать кнопки ↑ и ↓ соответственно.

Редактирование и удаление правил NAT

На странице **Информация о сервере проксирования** на вкладке **Правила NAT** Рисунок 12 можно выполнить следующие действия:

- **редактировать** правило NAT: **нажать кнопку** , в окне **Редактирование правила NAT** Рисунок 13 внести изменения и нажать кнопку **Сохранить**
- **удалить** правило NAT: **нажать кнопку**

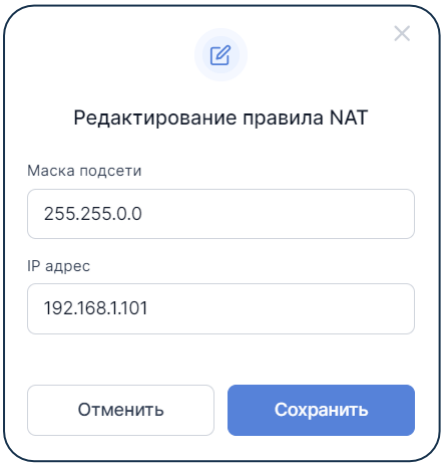

Рисунок 13. Добавление / Редактирование правила NAT

> Удаление правила NAT происходит **без подтверждения удаления**

Список заблокированных IP-адресов

В IVA SBC стандартно настроен Fail2Ban, который автоматически блокирует IP-адреса, активность которых является подозрительной.

> Вкладка **Заблокированные IP** отображается только для серверов со статусом **Онлайн**

Например, если с определенного IP-адреса происходит более 4 раз подряд (в течение 10 минут) неправильное введение пароля для доступа к серверу проксирования IVA SBC по SSH, или генерируется более 8 звонков (в течение 10 минут) с одного и того же не доверенного IP-адреса, то этот IP-адрес будет заблокирован (на 5 минут) и отображён в разделе **Информация о сервере проксирования** на вкладке **Заблокированные IP** Рисунок 14.

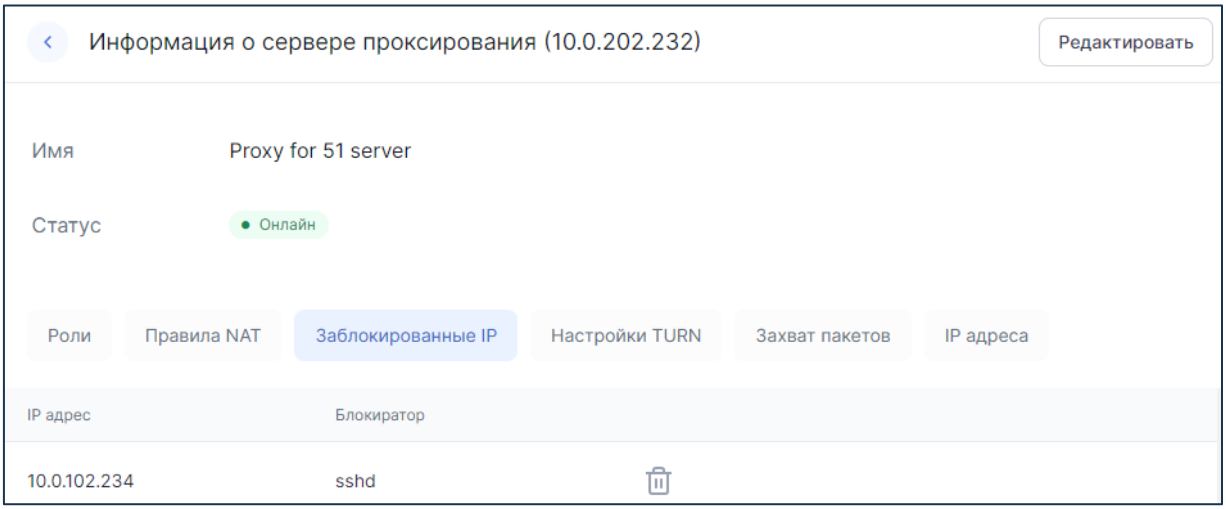

Рисунок 14. Заблокированные IP

Чтобы разблокировать IP-адрес, необходимо удалить его из списка **Заблокированные IP** Рисунок 14: **нажать кнопку** 🗑

> Удаление заблокированных IP-адресов из списка заблокированных IP-адресов происходит **без подтверждения удаления**

Настройка TURN

Вкладка **Настройка TURN** Рисунок 15 будет доступна, если на сервере проксирования добавлена и активирована группа маршрутизации для роли **TURN**.

Аутентификация на TURN-сервере осуществляется с помощью статического логина и пароля.

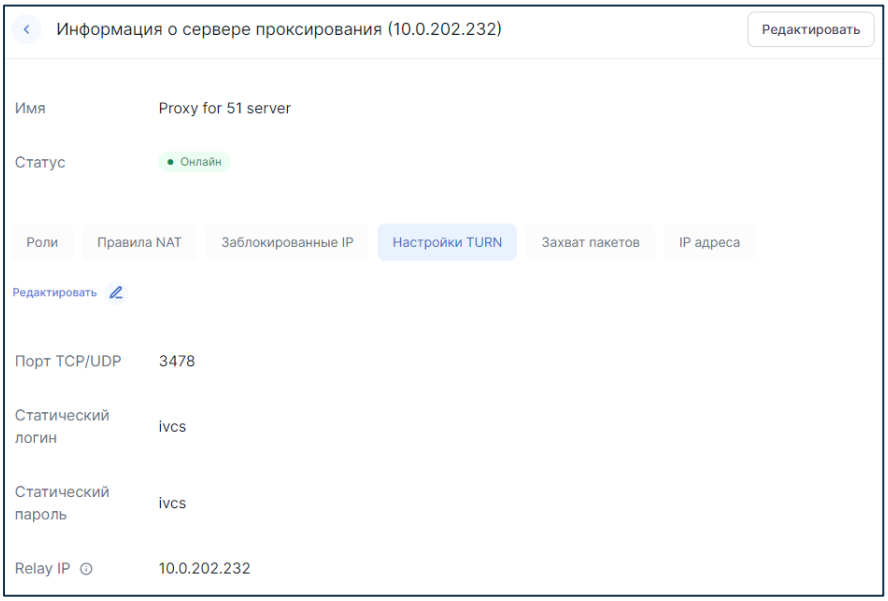

Рисунок 15. Настройки TURN

Чтобы выполнить **настройки TURN-сервера**, необходимо:

1 перейти в раздел **Сервера проксирования** и нажать ссылку <**Адрес сервера проксирования**> (например **10.0.202.232**)

2 перейти на вкладку **Настройки TURN** Рисунок 15 и нажать кнопку **Редактировать**

3 в окне **Настройки TURN**:

- **Порт TCP / UDP**: ввести порт (например **3478**)
- **Порт TLS**: ввести порт (например **443** (HTTPS) или **993** (IMAPS))
- **Сертификат**: выбрать сертификат из списка доступных сертификатов
- **Статический логин**: ввести логин для доступа к TURN-серверу (например **ivcs**)
- **Статический пароль**: ввести пароль для доступа к TURN-серверу (например **ivcs**)
- **Relay IP**: ввести IP-адрес сервера проксирования IVA SBC (например **10.0.202.232**), по которому он будет доступен для получения пакетов внутри сети (например от медиасерверов IVA MCU)

4 нажать кнопку **Сохранить**

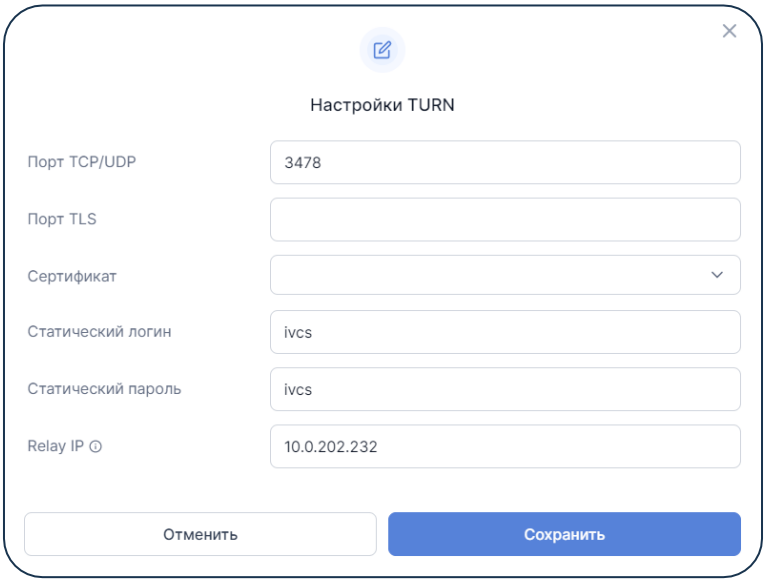

Рисунок 16. Редактирование настроек TURN

Захват пакетов на сервере проксирования

Чтобы проанализировать сетевой трафик сервера проксирования IVA SBC, необходимо:

1 перейти в раздел **Сервера проксирования** и нажать ссылку <**Адрес сервера проксирования**> (например **10.0.202.232**)

2 перейти на вкладку **Захват пакетов** Рисунок 17:

- **Время работы (сек)**: ввести время работы в секундах (например **1200**)
- Интерфейс:
  - **any**: любой интерфейс
  - **eth0**: сетевой интерфейс Ethernet
  - **lo**: виртуальный интерфейс для локальных тестов и отладки (loopback device)
- **Фильтр**: установить значение (в формате **tcpdump**)

3 нажать кнопку **Старт**

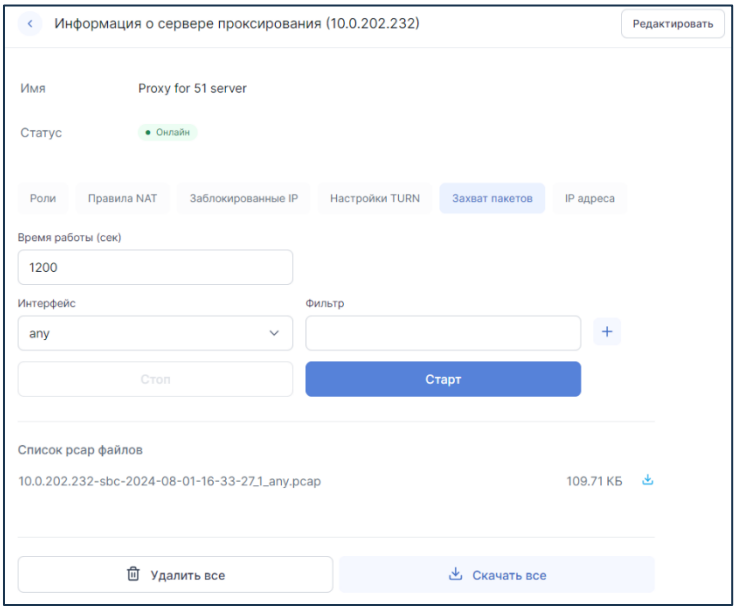

Рисунок 17. Захват пакетов

После завершения захвата трафика можно Рисунок 17:

- скачать сформированные pcap-файлы: выбрать **pcap-файл из списка с pcap-файлами и нажать кнопку**
- скачать архив с pcap-файлами: нажать кнопку **Скачать все**
- удалить все сформированные pcap-файлы файлы: нажать кнопку **Удалить все**

IP-адреса сервера проксирования

Чтобы просмотреть информацию об IP-адресах на сервере IVA SBC, необходимо:

1 перейти в раздел **Сервера проксирования** и нажать ссылку <**Адрес сервера проксирования**> (например **10.0.202.230**)

2 перейти на вкладку **IP адреса** Рисунок 18:

- **Активные плавающие** – список плавающих IP-адресов, которые используются на сервере проксирования в данный момент
- **Основные** – список основных IP-адресов сервера проксирования
- **Потенциально плавающие** – список IP-адресов, которые могут быть использованы на данном сервере

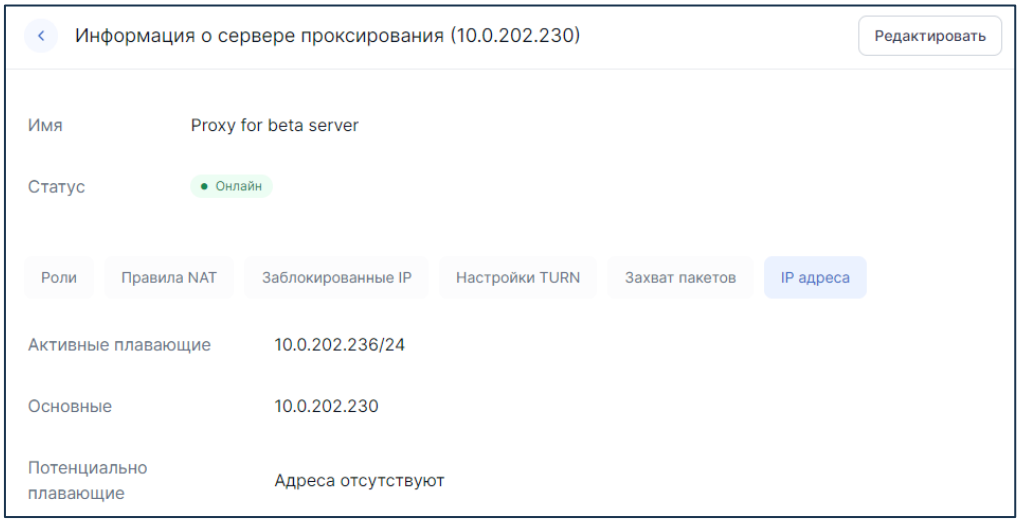

Рисунок 18. IP-адреса сервера проксирования

> Наличие информации о плавающих IP-адресах, которые используются или могут быть использованы на сервере проксирования зависит от настроек отказоустойчивого кластера, в котором данный сервер проксирования является узлом

Редактирование имени сервера проксирования

Для редактирования имени сервера проксирования необходимо:

1. перейти в раздел **Сервера проксирования** и нажать ссылку <**Адрес сервера проксирования**> (например **10.0.202.232**)
2. нажать кнопку **Редактировать** Рисунок 11
3. в окне **Редактирование сервера** Рисунок 19 ввести **Имя сервера** (рекомендуется вводить имя, которое кратко описывает назначение сервера проксирования (например **Proxy for 51 Server**)
4. нажать кнопку **Сохранить**

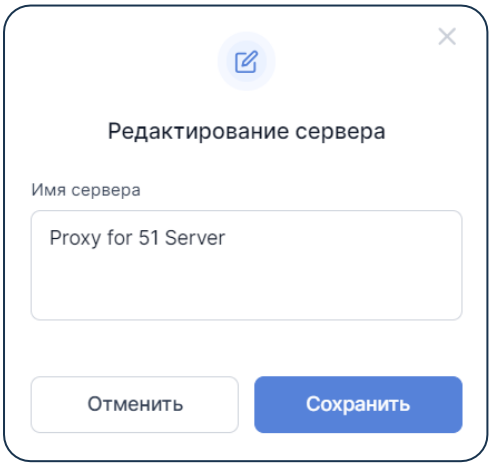

Рисунок 19. Редактирование имени сервера проксирования

Действия над сервером проксирования

Над сервером проксирования IVA SBC можно выполнить следующие действия:

- перезагрузить сервер
- скачать dump-файл сервера
- удалить сервер

Чтобы **перезагрузить** сервер проксирования, необходимо: перейти в раздел **Сервера проксирования** Рисунок 8, выбрать **сервер проксирования** (например **10.0.202.232**), **нажать кнопку** ⋮ и выбрать **Перезагрузить**, в окне **Перезагрузка сервера** Рисунок 20 нажать кнопку **Перезагрузить**.

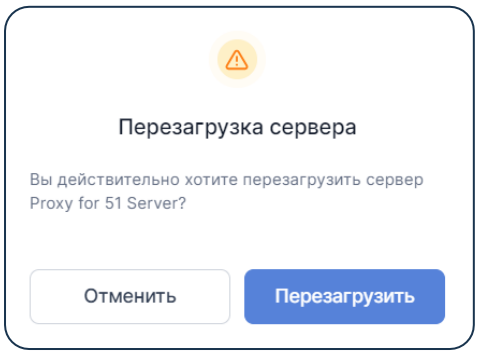

Рисунок 20. Перезагрузка сервера

Чтобы **скачать dump-файл** сервера проксирования, необходимо: перейти в раздел **Сервера проксирования** Рисунок 8, выбрать **сервер проксирования** (например **10.0.202.232**), **нажать кнопку** ⋮ и выбрать **Скачать dump-файл**.

> Невозможно скачать dump-файл сервера проксирования, который находится в статусе **Оффлайн**

Чтобы **удалить** сервер проксирования, необходимо: перейти в раздел **Сервера проксирования** Рисунок 8, выбрать **сервер проксирования** (например **10.0.20.104**), **нажать кнопку** ⋮ , выбрать **Удалить** и в окне **Удаление сервера** Рисунок 21 нажать кнопку **Удалить**.

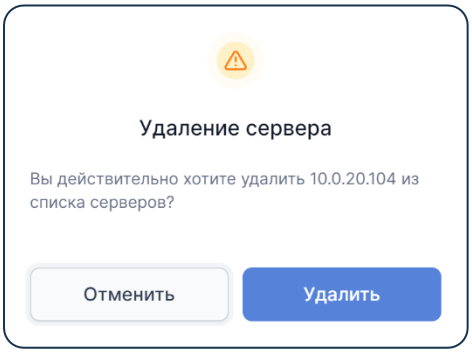

Рисунок 21. Удаление сервера

Настройка групп маршрутизации

В разделе **Группы маршрутизации** Рисунок 22 можно создавать, редактировать и удалять группы маршрутизации на основе созданных маршрутов.

Группы маршрутизации используются для объединения добавленных маршрутов. Это позволяет обрабатывать несколько маршрутов на одном сервере. Каждая группа содержит последовательный набор маршрутов одного из типов:

- VVoIP
- HTTP Reverse
- TURN

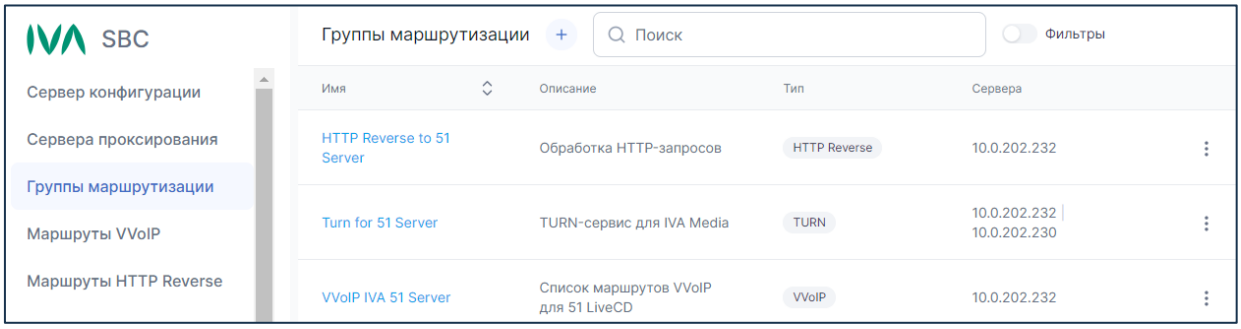

Рисунок 22. Группы маршрутизации

При работе в разделе **Группы маршрутизации** можно:

- просматривать группы маршрутизации
- создать группу маршрутизации: нажать кнопку +
- перейти к редактированию группы маршрутизации и добавлению списка маршрутов: нажать ссылку <**Имя маршрута**>
- редактировать описание группы маршрутизации
- удалить группу правил маршрутизации

Просмотр групп маршрутизации

При большом количестве групп маршрутизации, для упрощения навигации по группам, можно включить и выбрать фильтр отображения по типу маршрутизации (например, по типу **VVoIP**): нажать **переключатель Фильтры** Рисунок 23.

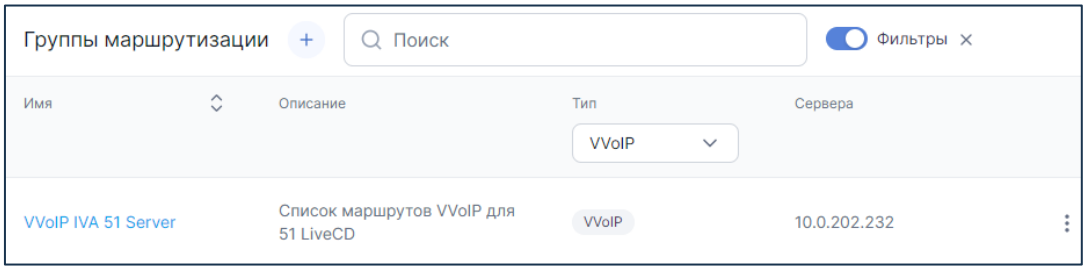

Рисунок 23. Фильтр групп маршрутизации

Создание, редактирование и удаление групп маршрутизации

Создание группы маршрутизации

Чтобы **добавить и настроить группу маршрутизации**, необходимо:

1 нажать кнопку + Рисунок 22

2 в окне **Добавление группы** Рисунок 24:

- **Имя**: рекомендуется вводить имя, которое кратко описывает назначение группы маршрутизации (например **SIP & H.323 в IVA MCU и АТС**)
- **Описание**: рекомендуется вводить описание, отражающее результат работы группы маршрутизации (например: **Разрешение SIP- и H.323-вызовов для IVA MCU**, и т. д.)
- **Тип**: выбрать тип маршрутизации VVoIP / HTTP / TURN (например **VVoIP Proxy)**

3 нажать кнопку **Добавить**

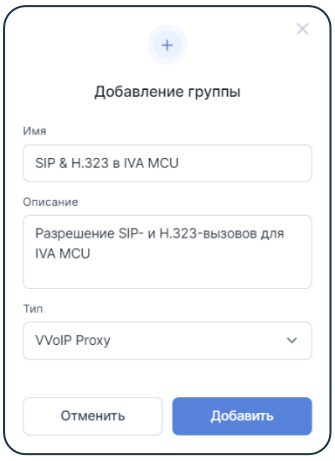

Рисунок 24. Добавление группы VVoIP

После создания группы маршрутизации необходимо добавить список маршрутов.

Редактирование описания группы маршрутизации

Чтобы **редактировать описание группы маршрутизации** Рисунок 22, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование группы** Рисунок 25 внести изменения (описание полей приведено в разделе Создание группы маршрутизации)

3 нажать кнопку **Сохранить**

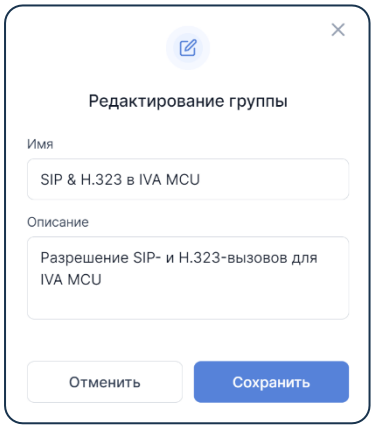

Рисунок 25. Редактирование описания группы маршрутизации

Удаление группы правил маршрутизации

Чтобы удалить **Группу маршрутизации** Рисунок 22, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление группы правил** Рисунок 26 нажать кнопку **Удалить**

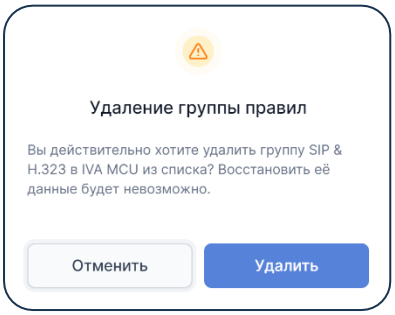

Рисунок 26. Удаление группы правил маршрутзации

> При удалении группы маршрутизации она автоматически удаляется с каждого сервера проксирования

Редактирование группы маршрутизации и добавление маршрутов

Добавление и редактирование маршрутов для групп маршрутизации проводится на странице Информация о группе маршрутизации Рисунок 27:

Перейти в раздел Группы маршрутизации и нажать ссылку <Имя группы маршрутизации>

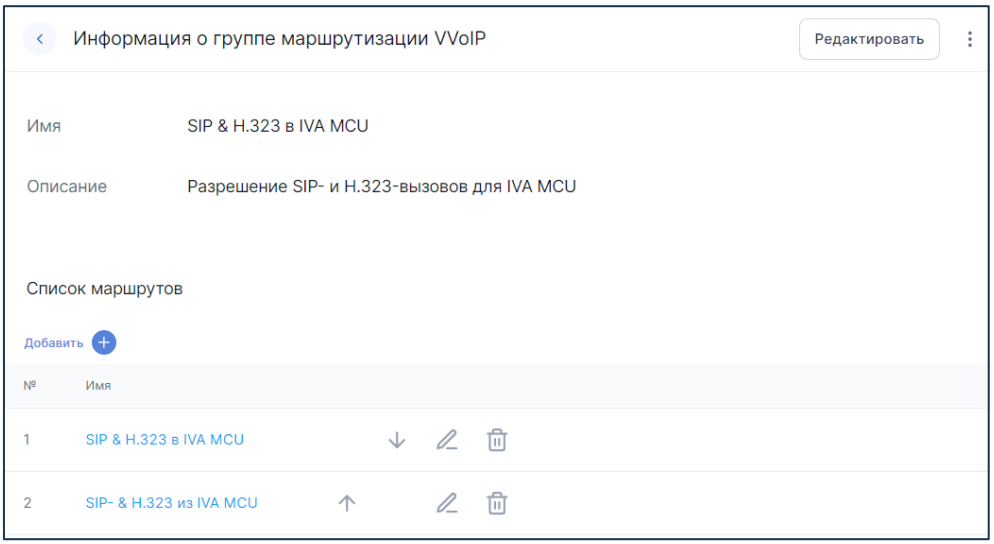

Рисунок 27. Информация о группе маршрутизации VVoIP

При работе на странице Информация о группе маршрутизации, можно:

- посмотреть список маршрутов Рисунок 27
- добавить маршрут в группу маршрутизации: нажать кнопку Добавить
- редактировать описание группы маршрутизации: нажать кнопку Редактировать
- редактировать маршрут группы маршрутизации: нажать кнопку или ссылку <Имя маршрута>
- удалить группу правил маршрутизации: нажать кнопку и выбрать Удалить
- удалить маршрут из группы маршрутизации: нажать кнопку
- изменить порядок применения маршрутов

Добавление маршрута в группу маршрутизации

Чтобы **добавить маршрут**, необходимо:

1 нажать кнопку **Добавить** Рисунок 27

2 в окне **Добавление маршрута** Рисунок 28 выбрать маршрут из ранее созданных маршрутов данного типа (например **SIP & H.323 в IVA MCU**) и нажать кнопку **Добавить.** Маршруты в группу маршрутизации добавляются по одному

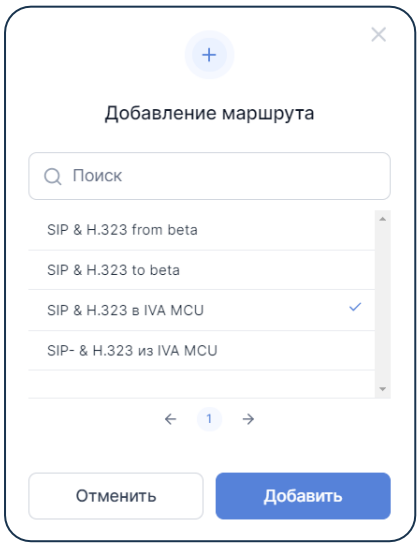

Рисунок 28. Добавление маршрута

3 повторить добавление маршрута для всех требуемых для данной группы маршрутов

Для включения на сервере проксирования группы маршрутизации и назначения соответствующей роли необходимо настроить сервер проксирования.

Изменение порядка применения маршрутов

Добавленные маршруты Рисунок 27 (для групп маршрутизации типа **VoIP** и **HTTP Reverse**) применяются в порядке очереди.

Чтобы **изменить** порядок применения маршрутов, необходимо использовать кнопки:

- ↑ для перемещения маршрута вверх
- ↓ для перемещения маршрута вниз

Редактировать описание группы маршрутизации

На странице **Информация о группе маршрутизации** Рисунок 27 можно **редактировать описание** группы маршрутизации:

1 нажать кнопку **Редактировать**

2 в окне **Редактирование группы** Рисунок 29 внести изменения

3 нажать кнопку **Сохранить**

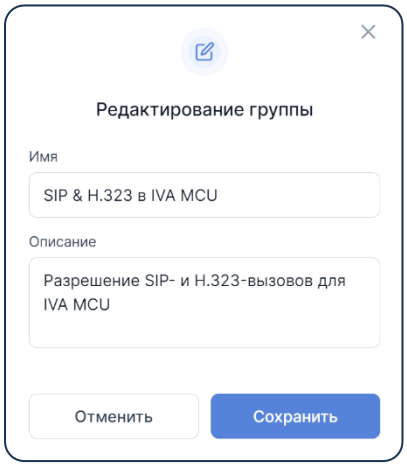

Рисунок 29. Редактирование описания группы маршрутизации

Редактирование маршрута группы маршрутизации

На странице **Информация о группе маршрутизации** Рисунок 27 можно **редактировать маршрут группы маршрутизации**:

1 **выбрать маршрут**, который необходимо редактировать

2 **нажать кнопку** или ссылку <**Имя маршрута**>

3 на странице **Информация о маршруте** VoIP, HTTP Reverse, TURN внести изменения

Удаление маршрута из группы маршрутизации

На странице **Информация о группе маршрутизации** Рисунок 27 можно **удалить маршрут** из группы маршрутизации:

1 **выбрать маршрут**, который необходимо удалить и **нажать кнопку**

2 в окне **Удаление маршрута** нажать кнопку **Удалить** Рисунок 30

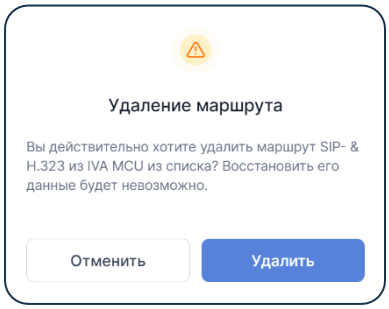

Рисунок 30. Удаление маршрута

Проксирование SIP- и H.323-звонков

IVA SBC позволяет настроить проксирование SIP-, H.323-звонков и RTP-трафика из одной сети в другую.

Чтобы IVA SBC выполняло проксирование VoIP, необходимо:

1 добавить маршруты VoIP, которые состоят из последовательного набора правил обработки поступающих звонков

2 добавить группу маршрутизации VoIP, которая состоит из упорядоченного набора маршрутов VoIP

3 назначить серверу проксирования роль VoIP и созданную группу маршрутизации VoIP

Алгоритм обработки входящего звонка на сервере проксирования:

1 выполняется обработка звонка на **сервере проксирования** в соответствии с правилами в назначенной для сервера **группе маршрутизации VoIP**

2 выполняется обработка звонка в соответствии с **последовательностью маршрутов**, добавленных в **группу маршрутизации VoIP**

3 для каждого VoIP-маршрута в группе маршрутизации VoIP **последовательно проверяются правила обработки входящих звонков (INVITE)** из маршрутов VoIP

4 если звонок попадает под правило обработки, то выполняется действие, указанное в данном правиле, и обработка завершается

5 если правило обработки не найдено, то звонок отклоняется

Настройка маршрутов VoIP

VoIP-маршрут определяет, как нужно обрабатывать входящий звонок.

В разделе **Маршруты VoIP** Рисунок 31 отображается список существующих в системе маршрутов VoIP:

- **Имя** – имя маршрута, заданное при создании маршрута
- **Описание** – описание маршрута, заданное при создании маршрута
- **Группы маршрутизации** – список групп маршрутизаций, в которых данный маршрут используется

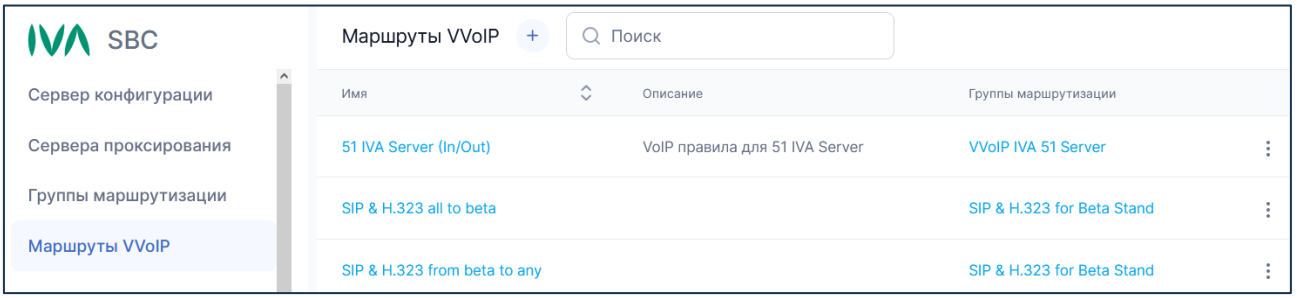

Рисунок 31. Раздел Маршруты VVoIP

При работе в разделе **Маршруты VVoIP** Рисунок 31 можно:

- посмотреть список маршрутов VVoIP
- добавить маршрут VVoIP: нажать кнопку +
- редактировать описание маршрута VVoIP: нажать кнопку ⋮ и выбрать **Редактировать**
- удалить маршрут VVoIP: нажать кнопку ⋮ и выбрать **Удалить**
- перейти к изменению правил обработки для маршрута VVoIP: нажать ссылку <Имя маршрута>
- перейти к изменению списка маршрутов группы маршрутизации VVoIP: нажать ссылку <Имя группы маршрутизации>

Добавление, редактирование и удаление маршрута VVoIP

Добавление маршрута VVoIP

Маршруты VVoIP необходимы для группировки правил обработки входящих звонков.

Чтобы **создать маршрут VVoIP**, необходимо:

1 нажать кнопку + Рисунок 31

2 в окне **Добавление маршрута** Рисунок 32 ввести:

- **Имя**: рекомендуется вводить имя, которое кратко описывает назначение маршрута (например **SIP & H.323 в IVA MCU**, **SIP & H.323 из IVA MCU**, **Drop All** и т. п.)

- **Описание**: рекомендуется вводить описание, отражающее результат работы маршрута (например: **Разрешение входящих SIP- и H.323-вызовов для IVA MCU**, и т. д.)

3 нажать кнопку **Добавить**

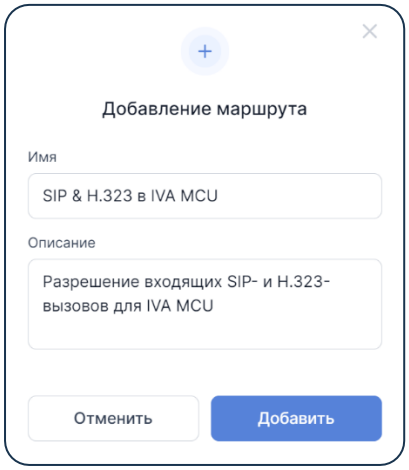

Рисунок 32. Добавление маршрута

После создания маршрута VVoIP необходимо добавить правила обработки входящего звонка и правила обработки SIP-регистрации.

Редактирование описания маршрута VVoIP

Чтобы **редактировать описание маршрута**, необходимо:

1 в разделе **Маршруты VVoIP** Рисунок 31 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование маршрута** Рисунок 33 внести изменения

3 нажать кнопку **Сохранить**

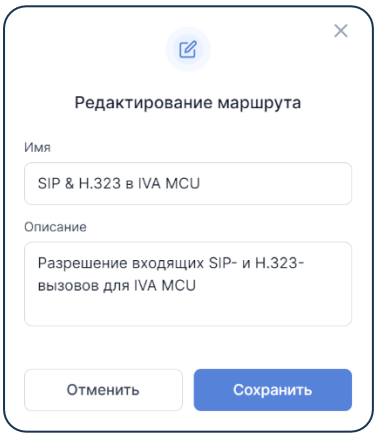

Рисунок 33. Редактирование описания маршрута VVoIP

Удаление маршрута VoIP

Чтобы удалить маршрут, необходимо:

1 в разделе **Маршруты VoIP** Рисунок 31 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление маршрута** Рисунок 34 нажать кнопку **Удалить**

> При удалении маршрут будет автоматически удален из всех **групп маршрутизации**

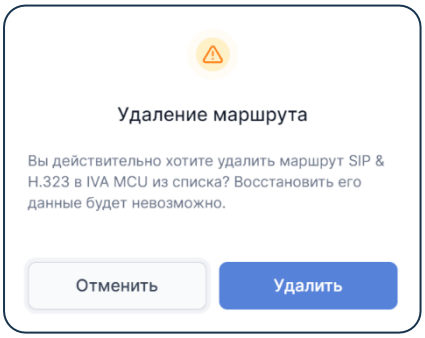

Рисунок 34. Удаление маршрута VoIP

Информация о маршруте VoIP и редактирование его описания

Добавление и редактирование правил обработки маршрута VoIP проводится на странице **Информация о маршруте VoIP** Рисунок 35:

Перейти в раздел **Маршруты VoIP** Рисунок 31 и нажать ссылку <**Имя правила фильтрации**>

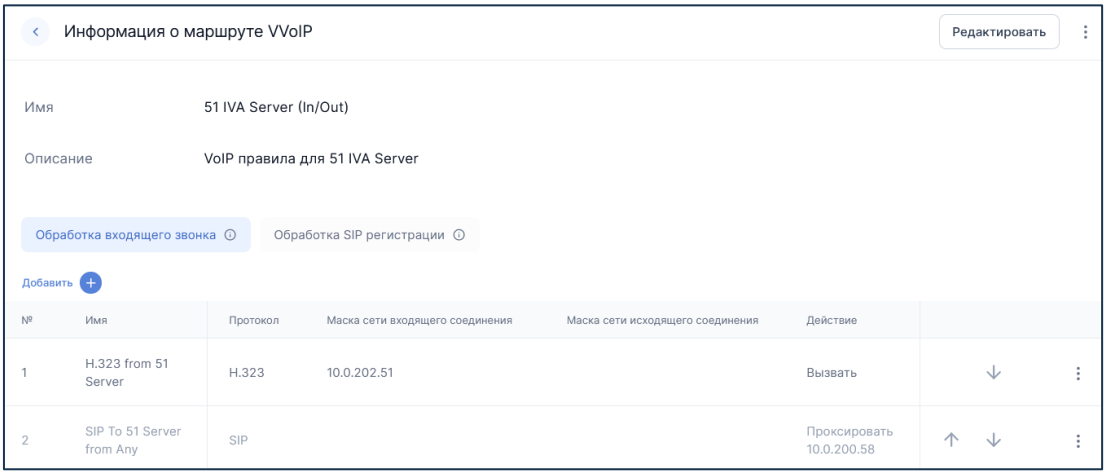

Рисунок 35. Список правил обработки маршрута VoIP

На странице Информация о маршруте VoIP Рисунок 35 можно:

- настроить обработку входящего звонка
- настроить обработку SIP-регистрации
- редактировать описание маршрута: нажать кнопку Редактировать

Правила обработки маршрута VoIP. Обработка входящего звонка

На вкладке Обработка входящего звонка Рисунок 35 можно:

- добавить правило обработки входящих звонков: нажать кнопку ⊕
- изменить порядок выполнения правил обработки входящих звонков
- редактировать правило обработки входящих звонков: нажать кнопку ⋮ и выбрать Редактировать
- удалить правило обработки входящих звонков: нажать кнопку ⋮ и выбрать Удалить

Добавление правила обработки входящих звонков

Чтобы добавить правило обработки входящего звонка, необходимо:

1 на вкладке Обработка входящего звонка: нажать кнопку ⊕

2 в окне Создание обработки INVITE Рисунок 36:

- Включено: нажать переключатель для включения правила обработки

> В списке правил обработки входящего звонка Рисунок 35 Отключённое правило отображается серым цветом

- Имя: ввести имя (например Прием звонка из сети 211.0.0.2)
- Протокол (обязательное поле): выбрать, какой протокол (SIP или H.323) звонка будет обрабатывать данное правило

- **Маска сети входящего соединения:** задать перечень масок сетей (можно указывать через запятую, например **211.0.0.2/32, 211.0.1.0/24**). Правило считается выполненным, если звонок совершается с IP-адреса, принадлежащего указанным сетям. Если значение не указано, правило применяется ко всем сетям
- **Маска сети исходящего соединения:** задать перечень масок сетей (можно указывать через запятую, например **211.0.0.2/32, 211.0.1.0/24**). Правило будет считаться выполненным, если IP-адрес, определяемый по полю **To**, соответствует одной из этих сетей. Если значение не указано, правило применяется ко всем сетям
- **Фильтр адреса FROM**: задать фиксированное или регулярное выражение (RegExp), по которому будет проверяться, что звонок удовлетворяет правилу (например **^sip:(.*)@ivcs.ru$** – от кого идет звонок)
- **Фильтр адреса TO**: задать фиксированное или регулярное выражение (RegExp), по которому будет проверяться, что звонок удовлетворяет правилу (например **^sip:(.*)@ivcs.ru$** – кому идет звонок)
- Статус регистрации:
  - **Любой**: правило будет считаться выполненным для вызовов от любых пользователей
  - **Не задано**: технологический статус, при котором текущее правило обработки входящего звонка не может быть активным. Если для заданного домена удаляется правило обработки SIP-регистрации, и если ранее правило обработки входящего звонка выполнялось для пользователей, зарегистрированных в этом домене, то данное правило будет автоматически отключено, а **Статус регистрации** изменится на **Не задано**
  - **Только зарегистрированные**: правило будет считаться выполненным только для вызовов от зарегистрированных пользователей на любом из доменов
  - **Только незарегистрированные**: правило будет считаться выполненным только для вызовов от незарегистрированных пользователей
  - **Зарегистрирован в <Имя домена>**: правило будет считаться выполненным, если пользователь зарегистрирован в домене SIP-регистрации

> Не рекомендуется настраивать **статус SIP-регистрации**, если для звонков выбран протокол **H.323**, т. к. это может вызвать проблемы или ограничения при обработке звонков

- Действие:
    - **Вызвать** – будет совершен входящий / исходящий вызов через IVA SBC на адрес, который запросил пользователь в поле **To** (например, от платформы IVA MCU, расположенной во внутренней сети, будет совершен вызов пользователя, находящегося во внешней сети) или на модифицированный адрес
    - **Отклонить –** вызов, попадающий под заданное правило, будет отклонен (REJECT)
    - **Не отвечать** – вызов, попадающий под заданное правило, будет проигнорирован без ответа по сигнализации
    - **Проксировать** – будет выполнен звонок в сторону сервера проксирования (необходимо дополнительно ввести адрес сервера проксирования), без изменения поля **To**
- **Использовать DNS SRV записи**: если звонок выполняется по протоколу **SIP** и выбрано действие **Вызвать**, то при вызове желаемого пользователя будет осуществлён звонок на IP-адрес, указанный в DNS-SRV записях, определяемый по домену вызываемого адреса (например, если звонок осуществляется на адрес **sip:1000@iva.ru**, то система обращается к DNS-SRV записям для домена **iva.ru** для определения IP-адреса SIP-сервера)
- **Проксировать RTP**: при включении данной опции RTP-трафик будет проксироваться IVA SBC, и в SIP- или H.323-сигнализации адреса RTP будут заменены на адреса сервера проксирования
- **Транспорт** (для исходящих SIP-соединений): по умолчанию – будет использоваться тот транспортный протокол, по которому получен входящий звонок. Выбор другого транспортного протокола (UDP, TCP, TLS, DTLS) приведет к использованию выбранного транспортного протокола для исходящего SIP-соединения
- **Модификация адреса FROM:** фиксированное или регулярное выражение (RegExp) для преобразования исходящего **адреса FROM** при прохождении вызова через IVA SBC. Например, при звонке исходящий адрес пользователя будет заменён на адрес, указанный в строке **Модификация адреса FROM** (например **sip:user@ivcs.ru**). **Модификация адреса FROM** (**sip:$1@ivcs.ru**) может использоваться в паре с **Фильтр адреса FROM** (**sip:(.*)@iva.ru**), тогда при звонке **адрес FROM** (**sip:user@iva.ru**) будет заменен на **sip:user@ivcs.ru**

- **Модификация адреса TO:** фиксированное или регулярное выражение (RegExp) для преобразования вызываемого **адреса TO** при прохождении вызова через IVA SBC. Например, при звонке на **sip:1000@iva.ru**, если выбрано действие **Вызвать**, то звонок будет направлен на адрес **iva.ru**, а если выбрано действие **Проксировать**, то звонок будет направлен на адрес сервера проксирования с модифицированным адресом **TO**. **Модификация адреса TO** (**sip:$1@ivcs.ru**) может использоваться в паре с **Фильтр адреса TO** (**sip:(.*)@iva.ru**), тогда при звонке **адрес TO sip:1000@iva.ru** будет заменен на **sip:1000@ivcs.ru**
- **Использовать туннелирование** (для исходящих H.323-соединений): при включении данной опции система автоматически попытается использовать для исходящего звонка режим туннелирования протокола H.245 в H.323. Если вызываемая сторона не поддерживает туннелирование, система автоматически переключится на режим без туннелирования

3 нажать кнопку **Создать**

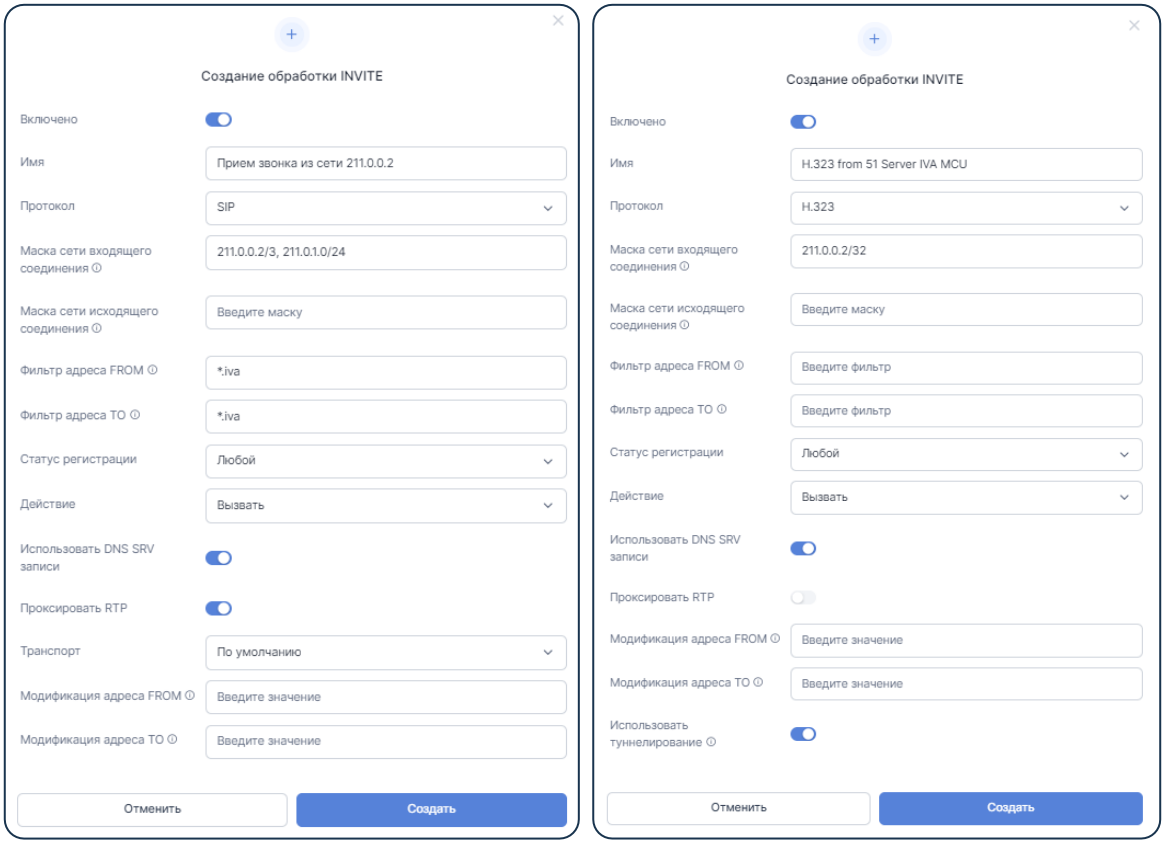

Рисунок 36. Создание правила обработки INVITE

Изменение порядка выполнения правил обработки входящих звонков

Правила обработки Рисунок 35 выполняются в порядке очереди. При совпадении требований правило выполняется, а дальнейший поиск прекращается.

Чтобы **изменить** порядок применения правил, необходимо использовать кнопки:

- ↑ для перемещения правила вверх
- ↓ для перемещения правила вниз

Редактирование правила обработки входящих звонков

Чтобы редактировать правило обработки входящего звонка, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование обработки INVITE** Рисунок 37 внести изменения (описание полей приведено в разделе Правила обработки маршрута VoIP. Обработка входящего звонка)

3 нажать кнопку **Сохранить**

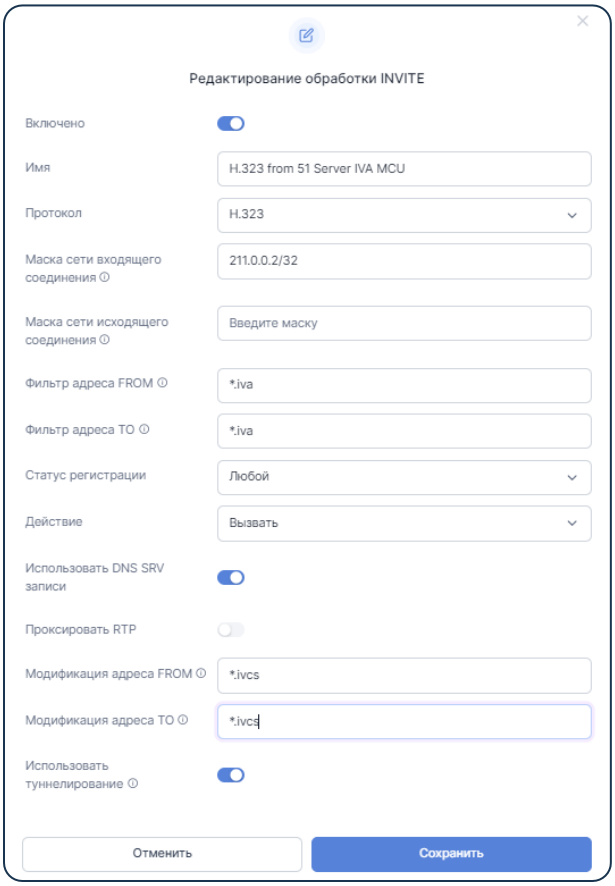

Рисунок 37. Редактирование правила обработки INVITE

Удаление правила обработки входящих звонков

Чтобы удалить правило обработки входящего звонка, необходимо:

1 нажать кнопку ⋮ и выбрать **Удалить**

2 в окне **Удаление правила** Рисунок 38 нажать кнопку **Удалить**

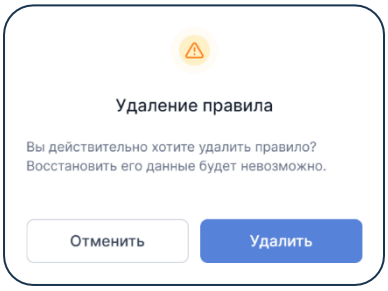

Рисунок 38. Удаление правила обработки INVITE

Правила обработки маршрута VoIP. Обработка SIP-регистрации

Система IVA SBC поддерживает проксирование SIP-регистрации:

- проксирование на разные сервера SIP-регистрации в зависимости от домена регистрации
- преобразование транспорта сигнализации при регистрации в **TCP** / **UDP** / **TLS**

На вкладке **Обработка SIP регистрации** Рисунок 39 можно:

- добавить правило обработки SIP-регистрации: нажать кнопку ⊕
- редактировать правило обработки SIP-регистрации: нажать кнопку ⋮ и выбрать **Редактировать**
- удалить правило обработки SIP-регистрации: нажать кнопку ⋮ и выбрать **Удалить**

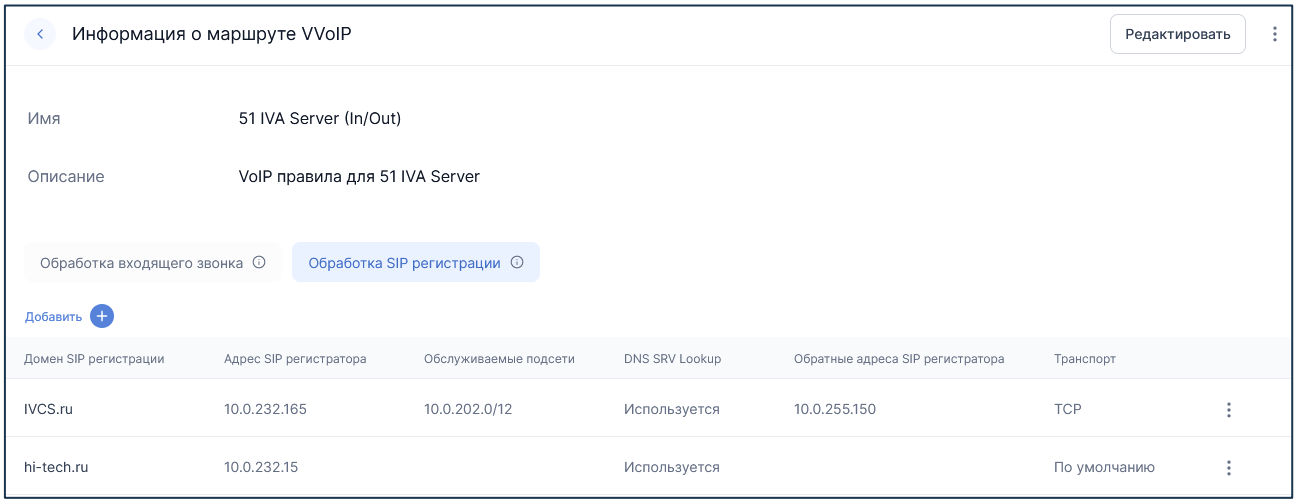

Рисунок 39. Обработка SIP-регистрации

Добавление правила обработки SIP-регистрации

Чтобы добавить правило обработки SIP-регистрации, необходимо:

1 на вкладке **Обработка SIP регистрации нажать кнопку** ⊕

2 в окне **Создание обработки REGISTER** Рисунок 40:

- **Домен SIP регистрации:** ввести имя домена учетных записей (например **sip.iva.ru**), для которого будет применяться данное правило
- **Адрес SIP регистратора**: ввести доменный или IP-адрес сервера, выполняющего функции регистрации SIP-устройств, на который будет перенаправляться запрос на SIP-регистрацию (например **10.0.202.120**)
- **Обслуживаемые подсети:** задать перечень масок обслуживаемых сетей, с которых будут приниматься запросы на регистрацию для этого правила (можно указывать через запятую, например **211.0.0.2/32, 211.0.1.0/24**). Если значение не указано, правило будет применяться к запросам со всех сетей
- **DNS SRV Lookup:** если **Адрес SIP регистратора** указан в виде доменного имени, то для определения IP-адреса сервера, на который будет отправлен запрос, будут использованы данные из DNS-SRV записей
- **Обратные адреса SIP регистратора**: ввести IP-адреса, с которых могут приходить SIP-сообщения (**NOTIFY** и т. п.) от SIP-регистратора для зарегистрированных пользователей

- **Транспорт**: по умолчанию – будет использоваться тот транспортный протокол, по которому получен входящий запрос на регистрацию. Выбор другого транспортного протокола (UDP, TCP, TLS, DTLS) приведет к использованию выбранного транспортного протокола для исходящего SIP-соединения

3 нажать кнопку **Создать**

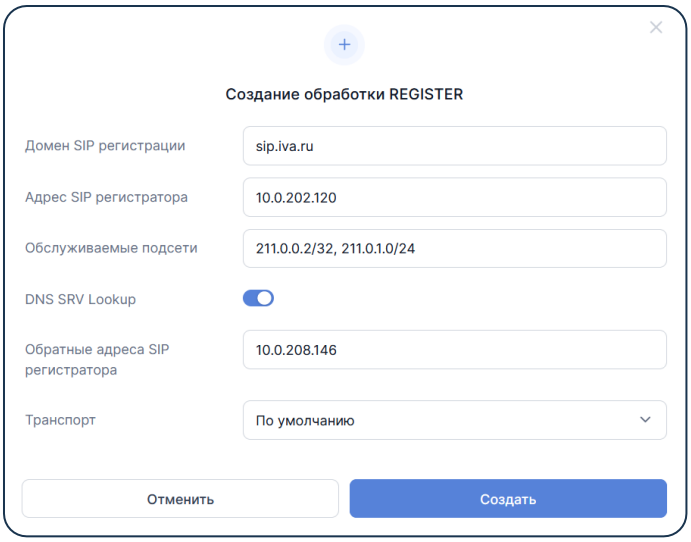

Рисунок 40. Создание правила обработки SIP-регистрации

Редактирование правила обработки SIP-регистрации

Чтобы редактировать правило обработки SIP-регистрации, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Редактировать правило**

2 в окне **Редактирование обработки REGISTER** Рисунок 41 внести изменения (описание полей приведено в разделе Правила обработки маршрута VoIP. Обработка SIP-регистрации)

3 нажать кнопку **Сохранить**

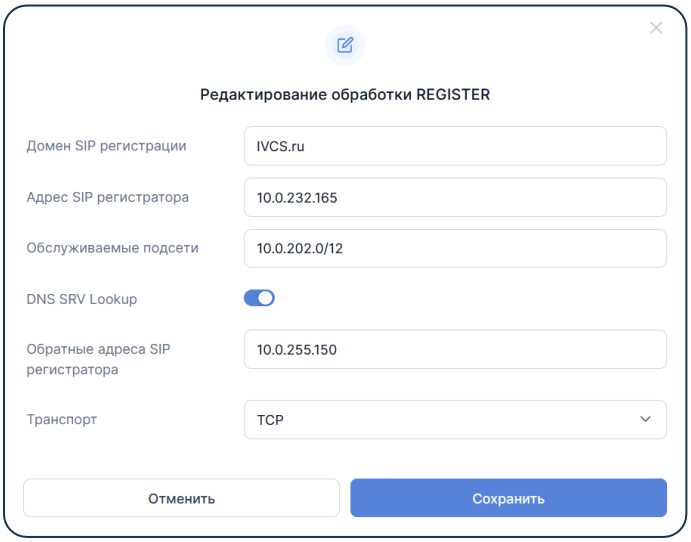

Рисунок 41. Редактирование правила обработки SIP-регистрации

Удаление правила обработки SIP-регистрации

Чтобы удалить правило обработки SIP-регистрации, необходимо:

1 нажать кнопку ⋮ и выбрать **Удалить правило**

2 в окне **Удаление правила** Рисунок 42 нажать кнопку **Удалить**

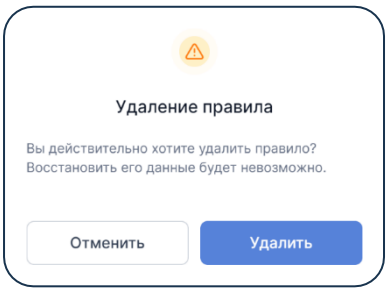

Рисунок 42. Удаление правила обработки SIP-регистрации

> При удалении правила обработки SIP-регистрации все связанные правила обработки входящих звонков, использующие указанный в удаляемом правиле домен, будут автоматически отключены

Настройка правил маршрутизации обработки запросов HTTP Reverse

IVA SBC позволяет настроить правила для проксирования HTTP-запросов на различные внутренние сетевые адреса.

Чтобы IVA SBC выполняло обработку трафика HTTP Reverse, необходимо:

1. добавить правила фильтрации маршрутов HTTP Reverse, состоящие из набора фильтров, которые ограничивают или разрешают доступ к заданным URL-адресам
2. добавить маршруты HTTP Reverse, которые состоят из последовательного набора правил фильтрации маршрутов HTTP Reverse
3. добавить группу маршрутизации HTTP Reverse, которая состоит из упорядоченного списка маршрутов HTTP Reverse
4. назначить серверу проксирования роль HTTP Reverse и созданную группу маршрутизации HTTP Reverse
5. добавить SSL-сертификат сервера проксирования IVA SBC, необходимый для корректной работы сервера по протоколу SSL

Алгоритм обработки трафика HTTP Reverse на сервере проксирования:

1. обработка трафика HTTP Reverse на **сервере проксирования** выполняется в соответствии с правилами в назначенной **группе маршрутизации HTTP Reverse**
2. обработка HTTP-запросов выполняется в соответствии с **последовательностью маршрутов**, добавленных в группу маршрутизации HTTP Reverse
3. для каждого маршрута в группе маршрутизации HTTP Reverse при совпадении адреса запроса HOST с **URL-адресом сервера**, указанным в маршруте, последовательно проверяется список правил фильтрации маршрутов HTTP Reverse
4. для каждого правила фильтрации последовательно проверяются фильтры, входящие в него
5. если запрос попадает под фильтр, который настроен на проверку OpenAPI-схемы, решение о разрешении или отклонении зависит от результата валидации:
   - если запрос соответствует OpenAPI-схеме, запрос разрешается, и обработка завершается

- если запрос не соответствует OpenAPI-схеме, запрос отклоняется, и обработка завершается

6 если запрос попадает под фильтр, который настроен на проверку **по заданным вручную параметрам**, то при совпадении с фильтром выполняется действие, указанное в данном фильтре, и обработка завершается

7 если не найден подходящий фильтр, то запрос отклоняется

> **Файл с логами** HTTP Reverse сохраняется на серверах проксирования в директории: **/var/log/sbc/reverse_proxy.log**

В разделе **Маршруты HTTP Reverse**:

- на вкладке **Схемы проверки OpenAPI** добавляются схемы для проверки запросов
- на вкладке **Правила фильтрации** задаются параметры обработки HTTP-запросов для определённого сервиса по заданным вручную параметрам или по OpenAPI-схеме
- на вкладке **Маршруты** указывается, для каких доменов будут применяться эти правила фильтрации и куда будут перенаправляться соответствующие запросы

Например, можно определить группу правил для обработки запросов сервиса IVA MCU. В случае наличия двух сервисов IVA MCU создаются два маршрута:

- для домена **iva1.iva.ru** запросы будут перенаправляться на один внутренний адрес
- для домена **iva2.iva.ru** – на другой внутренний адрес

Настройка маршрутов HTTP Reverse

Раздел **Маршруты HTTP Reverse** содержит следующие вкладки:

- **Маршруты** Рисунок 43 – определяют связь между доменным именем обращения и внутренним адресом сервиса куда запрос необходимо отправить и список правил фильтрации, которые необходимо наложить на эти запросы

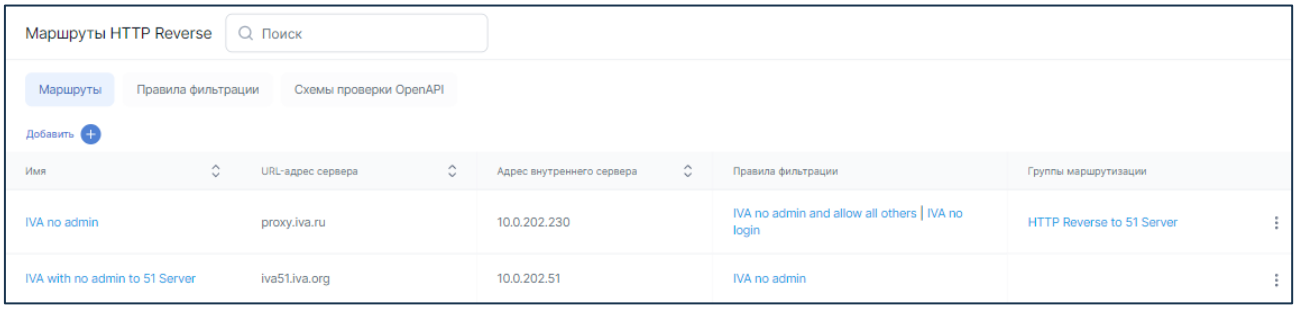

Рисунок 43. Вкладка Маршруты

- Правила фильтрации Рисунок 44 – определяют список фильтрации доступных / недоступных URL-обращений

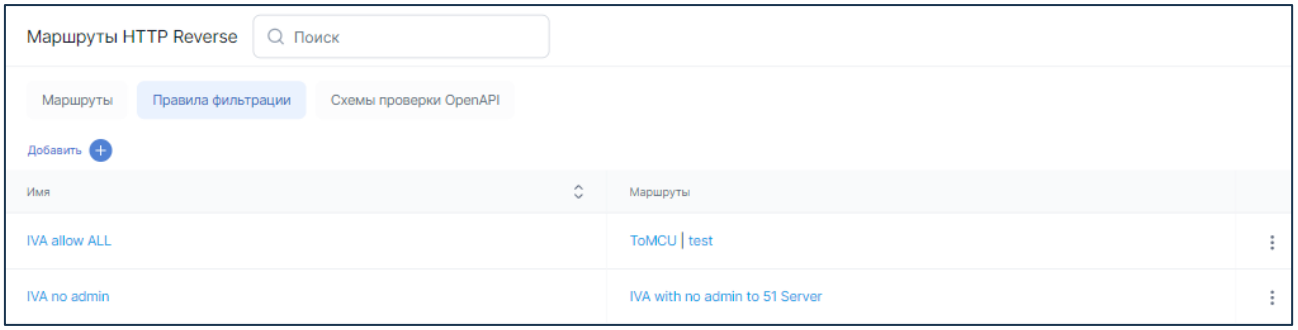

Рисунок 44. Вкладка Правила фильтрации

- Схемы проверки OpenAPI Рисунок 45 – позволяют добавить и настроить схемы для проверки запросов

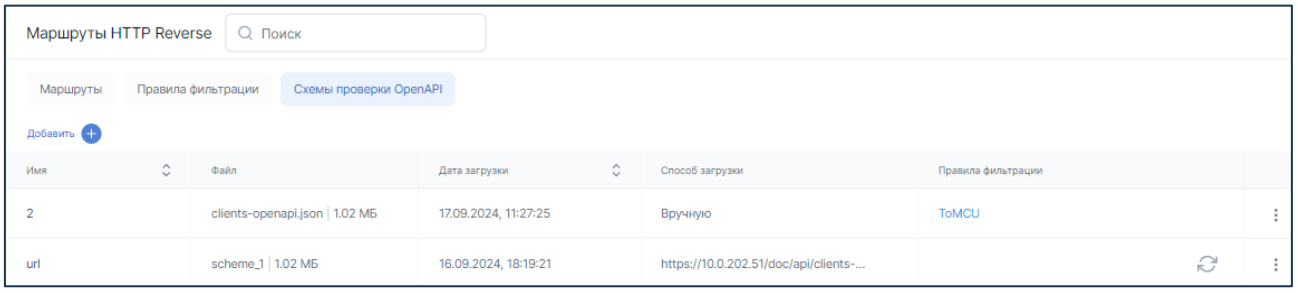

Рисунок 45. Вкладка Схемы проверки OpenAPI

Маршруты HTTP Reverse. Правила фильтрации

На вкладке Правила фильтрации Рисунок 44 можно управлять правилами фильтрации.

Фильтры в Правилах фильтрации определяют, какие HTTP-запросы разрешены / запрещены.

При работе на вкладке Правила фильтрации Рисунок 44 можно:

- посмотреть список правил фильтрации

- добавить новое правило фильтрации HTTP-запросов: нажать кнопку ⊕
- редактировать описание правила фильтрации: нажать кнопку ⋮ и выбрать Редактировать
- редактировать правило фильтрации входящего HTTP-запроса и его фильтров: нажать ссылку <Имя правила фильтрации>
- импортировать правило фильтрации: нажать кнопку Импортировать
- экспортировать правило фильтрации: нажать кнопку ⋮ и выбрать Экспортировать
- удалить правило фильтрации: нажать кнопку ⋮ и выбрать Удалить

Добавление правила фильтрации HTTP-запросов

Чтобы **добавить правило** фильтрации, необходимо:

1 нажать кнопку **Добавить** ⊕ Рисунок 44

2 в окне **Добавление правила** Рисунок 46: ввести **Имя** (рекомендуется вводить имя, которое кратко описывает назначение правила фильтрации (например IVA no admin)

3 нажать кнопку **Добавить**

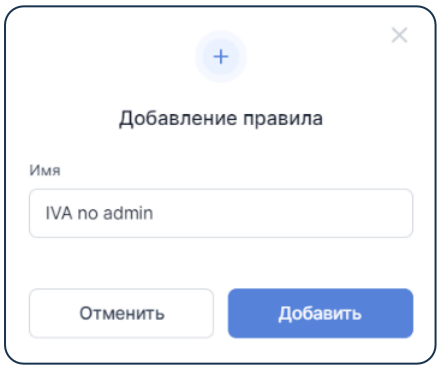

Рисунок 46. Добавление правила фильтрации

После создания правила фильтрации необходимо настроить фильтры.

Созданные правила фильтрации добавляются в маршруты HTTP Reverse.

Редактирование описания правила фильтрации

Чтобы **редактировать описание** правила фильтрации, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование правила** Рисунок 47 внести изменения

3 нажать кнопку **Сохранить**

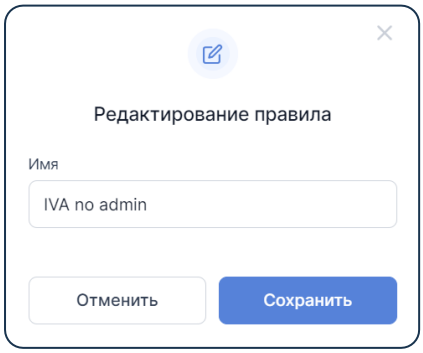

Рисунок 47. Редактирование описания правила маршрута HTTP Reverse

Экспортирование правила фильтрации

Чтобы **экспортировать правило** фильтрации с набором фильтров, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Экспортировать**

2 файл (в формате (***.json**) с именем и настройками правила фильтрации сохранится в загрузке браузера

> При экспорте правила фильтрации в JSON-файл сохраняются только фильтры с вручную заданными параметрами. Фильтры, использующие OpenAPI-схемы, **не экспортируются**

Импортирование правила фильтрации

Правило фильтрации со всеми входящими в него фильтрами можно импортировать.

Перед импортированием правила фильтрации необходимо подготовить файл (в формате (***.json**) с набором фильтров.

Чтобы **импортировать правило** фильтрации, необходимо:

1 нажать ссылку **Импортировать** Рисунок 44

2 в окне **Открытие** выбрать файл (в формате (***.json**) и нажать кнопку **Открыть**

После импортирования будет создано новое правило фильтрации с именем, соответствующим имени файла, и набором фильтров из файла.

Удаление правила фильтрации

Чтобы **удалить правило** фильтрации, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление правила** Рисунок 48 нажать кнопку **Удалить**

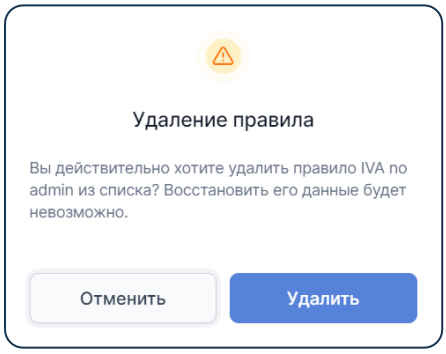

Рисунок 48. Удаление правила фильтрации маршрута HTTP Reverse

Добавление и редактирование фильтров для правила фильтрации маршрутов HTTP Reverse

Добавление и редактирование фильтров для правила фильтрации маршрута HTTP Reverse проводится на странице **Информация о правиле фильтрации HTTP** Рисунок 49:

Перейти в раздел **Маршруты HTTP Reverse**, открыть вкладку **Правила фильтрации** и нажать ссылку <**Имя правила фильтрации**>

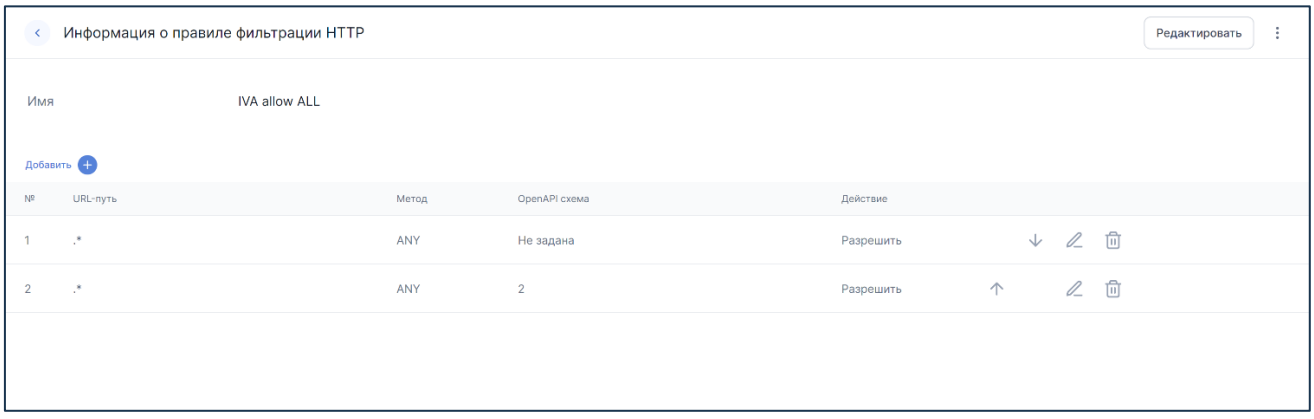

Рисунок 49. Информация о правиле фильтрации HTTP

При работе на странице **Информация о правиле фильтрации HTTP** Рисунок 49 можно:

- посмотреть список фильтров

- добавить фильтр HTTP-запроса: нажать кнопку **Добавить**
- редактировать описание правила фильтрации: нажать кнопку **Редактировать**
- редактировать фильтр правила фильтрации HTTP: **нажать кнопку**
- удалить правило фильтрации: **нажать кнопку** и выбрать **Удалить**
- удалить фильтр правила фильтрации HTTP: **нажать кнопку**
- изменить порядок применения фильтров

Добавление фильтра HTTP-запроса

Существует два способа фильтровать HTTP-запросы в IVA SBC:

- фильтрация по **заданным вручную параметрам** — позволяет настроить гибкие правила для отдельных маршрутов
- фильтрация по OpenAPI-схеме — позволяет проверять запросы на соответствие заранее загруженной спецификации API, описанной в OpenAPI-схеме

Чтобы добавить фильтр правила фильтрации маршрута HTTP Reverse по **заданным вручную параметрам**, необходимо:

1 нажать кнопку **Добавить** Рисунок 49

2 в окне **Добавление фильтра** Рисунок 50:

- URL-путь: ввести URL-адрес (фиксированный или регулярное выражение (Regexp), для которого будет выполняться фильтрация, например **/administration/(.*)** будет охватывать все URL-адреса, связанные с администрированием.
- Метод:
  - **Любой (ANY)** – любой из перечисленных ниже
  - **GET** – запрашивает содержимое конкретного ресурса, получает данные и не может изменять эти данные
  - **POST** – создает новый ресурс из переданных данных в запросе
  - **HEAD** – запрашивает содержимое конкретного ресурса, в ответе получает только стартовую строку и заголовки
  - **PUT** – изменяет содержимое запроса по указанному URI
  - **PATCH** – изменяет только фрагмент ресурса по указанному URI

  - DELETE – удаляет конкретный ресурс по указанному URI
  - CONNECT – запускает двустороннюю связь с запрошенным ресурсом
  - OPTIONS – определяет возможности и используемые методы web-сервера
  - TRACE – возвращает служебную отладочную информацию
- Действие:
  - Разрешить – разрешает доступ к указанному URL-адресу
  - Запретить – запрещает доступ к указанному URL-адресу

3 нажать кнопку Создать

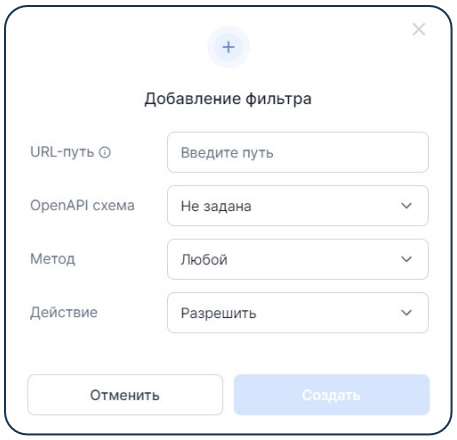

Рисунок 50. Добавление фильтра маршрута HTTP Reverse

Чтобы добавить фильтр правила фильтрации маршрута HTTP Reverse по OpenAPI-схеме, необходимо:

1 загрузить схему OpenAPI во вкладке Схемы проверки OpenAPI

2 нажать кнопку Добавить Рисунок 49

3 в окне Добавление фильтра Рисунок 50:

- URL-путь: ввести URL-адрес (фиксированный или регулярное выражение (Regexp), для которого будет выполняться фильтрация.
  Пример: /api/rest/.* будет охватывать все клиентские REST-запросы IVA MCU, начинающиеся с /api/rest и соответствующие указанной OpenAPI-схеме.
- OpenAPI схема: выбрать загруженную схему для проверки запросов.

4 нажать кнопку Создать

Изменение порядка применения фильтров

Добавленные фильтры правил фильтрации маршрутов HTTP Reverse Рисунок 49 применяются в порядке очереди.

Чтобы **изменить** порядок применения фильтров, необходимо использовать кнопки:

- ↑ для перемещения фильтра вверх
- ↓ для перемещения фильтра вниз

Редактирование описания правила фильтрации

На странице Информация о правиле фильтрации HTTP Рисунок 49 можно **редактировать правило** фильтрации:

1 нажать кнопку **Редактировать**

2 в окне **Редактирование правила** Рисунок 47 внести изменения

3 нажать кнопку **Сохранить**

Редактирование фильтра правила фильтрации HTTP

На странице Информация о правиле фильтрации HTTP Рисунок 49 можно **редактировать фильтр** правила фильтрации HTTP:

1 **выбрать фильтр**, который необходимо редактировать, и **нажать кнопку** Рисунок 49

2 в окне **Редактирование фильтра** Рисунок 51 внести изменения (описание полей приведено в разделе Добавление фильтра HTTP-запроса)

3 нажать кнопку **Сохранить**

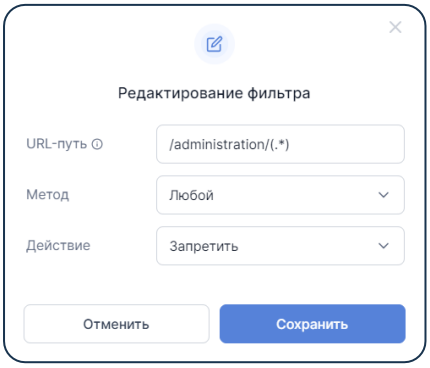

Рисунок 51. Редактирование фильтра правила фильтрации HTTP

Удаление правила фильтрации

На странице Информация о правиле фильтрации HTTP Рисунок 49 можно **удалить правило** фильтрации:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление правила** Рисунок 48 нажать кнопку **Удалить**

Удаление фильтра правила фильтрации HTTP

На странице Информация о правиле фильтрации HTTP Рисунок 49 можно **удалить фильтр** правила фильтрации HTTP:

1 **выбрать фильтр**, который необходимо удалить и **нажать кнопку** 🗑 Рисунок 51

2 в окне **Удаление фильтра** нажать кнопку **Удалить** Рисунок 52

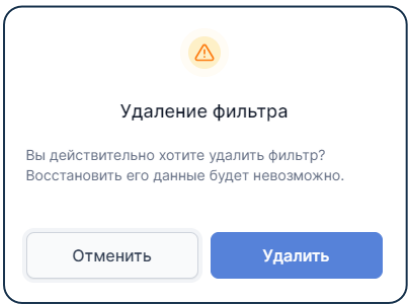

Рисунок 52. Удаление фильтра правила фильтрации HTTP

Схемы проверки OpenAPI

IVA SBC позволяет проверять корректность запросов к API на основе заранее определенных схем OpenAPI.

OpenAPI-схема — это стандартизированное описание API, которое помогает структурировать и документировать взаимодействие с web-сервисами. С помощью OpenAPI-схемы можно определить, какие запросы и ответы поддерживает API, какие данные необходимы и каким образом они должны быть переданы.

Использование OpenAPI-схемы упрощает настройку правил фильтрации, так как схема уже содержит всю необходимую информацию о структуре и допустимых параметрах запросов.

> При проверке GET-запросов по OpenAPI-схемам **лишние query-параметры не вызывают ошибок валидации**, даже если параметры не описаны в схеме.

Добавление схем OpenAPI

Добавить и настроить схемы для проверки запросов можно на вкладке **Схемы проверки OpenAPI** Рисунок 53.

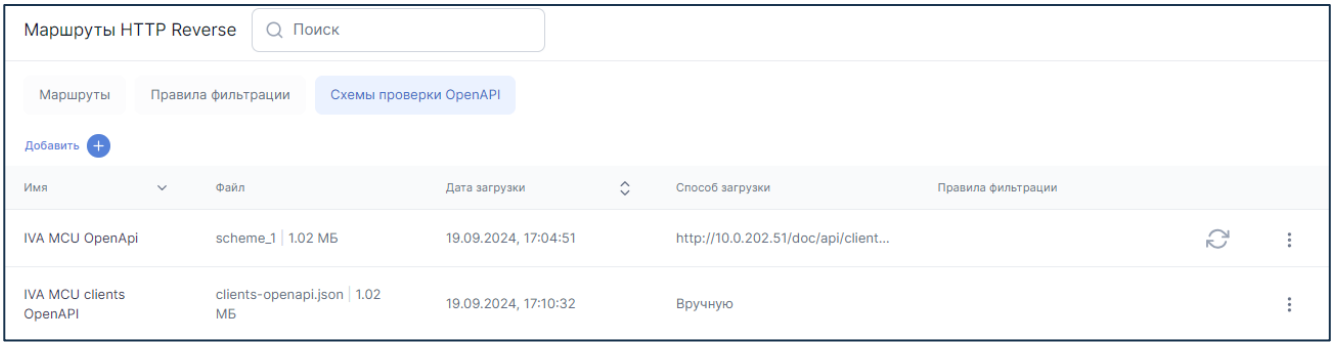

Рисунок 53. Схемы проверки OpenAPI

Для добавления схемы OpenAPI необходимо:

1 нажать кнопку **Добавить** 

2 в окне **Создание схемы OpenAPI** Рисунок 54:

- **Имя:** ввести имя схемы
- **Способ загрузки:** выбрать один из способов загрузки схемы:
  - **Вручную**: выбрать файл схемы и прикрепить его
  - **По URL**: указать URL-адрес, по которому доступна схема
- Нажать кнопку **Создать**

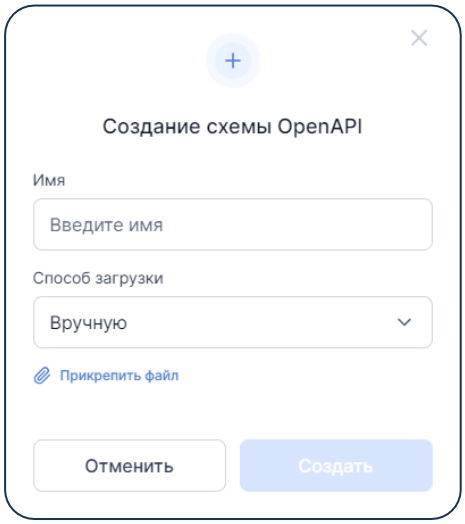

Рисунок 54. Создание схемы OpenAPI

Редактирование и обновление схемы OpenAPI

На вкладке **Схемы проверки OpenAPI** можно **редактировать** схемы OpenAPI:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование схемы OpenAPI** внести изменения

3 нажать кнопку **Сохранить**

Чтобы **обновить** схему OpenAPI, доступную по URL-адресу: нажать кнопку

Удаление схемы OpenAPI

Чтобы удалить схему OpenAPI:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление схемы** нажать кнопку **Удалить**

Маршруты HTTP Reverse. Маршруты

Маршруты HTTP Reverse необходимы для установления связи внутреннего сервера и доменного имени, по которому к нему будут обращаться, с указанием применяемых правил фильтрации для обработки URL-запросов.

В разделе **Маршруты HTTP Reverse** на вкладке **Маршруты** Рисунок 55 отображаются добавленные маршруты HTTP Reverse, позволяющие связать обращения по URL и внутренний HTTP-сервис с применением заданных правил фильтрации.

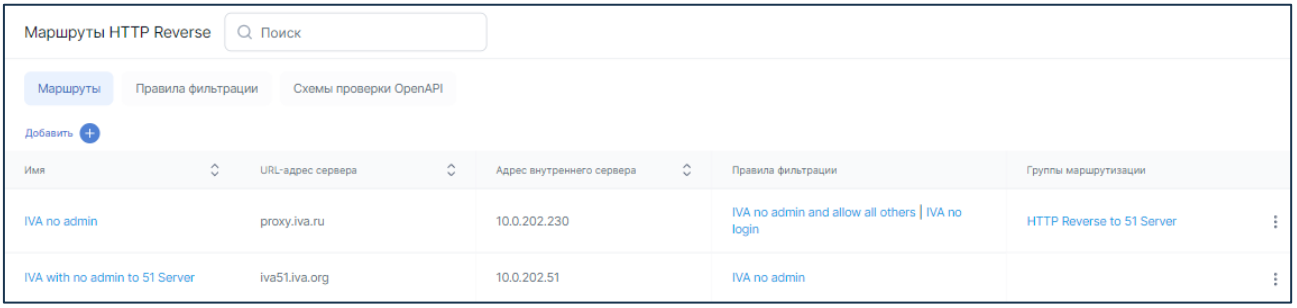

Рисунок 55. Маршруты HTTP Reverse

При работе на вкладке **Маршруты** Рисунок 55 можно:

- просмотреть список добавленных маршрутов
- добавить маршрут HTTP Reverse: нажать кнопку **Добавить** ⊕
- редактировать описание маршрута HTTP Reverse: нажать кнопку ⋮ и выбрать Редактировать Рисунок 57
- удалить маршрут HTTP Reverse: нажать кнопку ⋮ и выбрать Удалить Рисунок 58
- редактировать маршрут HTTP Reverse и его правила фильтрации: нажать ссылку <Имя маршрута>
- добавлять и редактировать фильтры правила фильтрации: нажать ссылку <Имя правила фильтрации>

Добавление маршрута HTTP Reverse

Чтобы добавить маршрут HTTP Reverse, необходимо:

1 нажать кнопку **Добавить** ⊕ Рисунок 55

2 в окне **Добавление маршрута** Рисунок 56 ввести:

- **Имя**: рекомендуется вводить имя, которое кратко описывает назначение маршрута (например **IVA**)
- **URL-адрес сервера**: ввести внешний доменный адрес, по которому будет подключаться пользователь (например доменный адрес сервера IVA SBC **ivcs.iva.ru**)
- **Адрес внутреннего сервера**: ввести IP-адрес внутреннего сервера, на который будут проксироваться запросы

3 нажать кнопку **Создать**

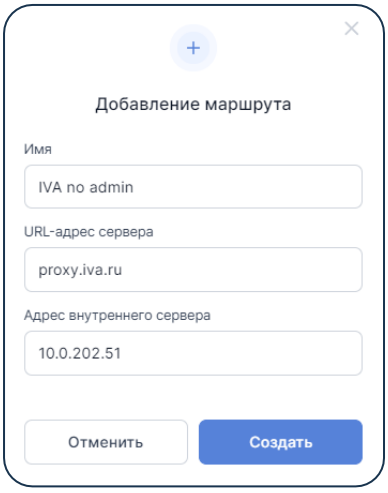

Рисунок 56. Добавление маршрута HTTP Reverse

После создания маршрута HTTP Reverse необходимо добавить в него правила фильтрации, которые будут применяться. Если правила фильтрации не добавить, то все запросы будут отклонены.

Редактирование описания маршрута HTTP Reverse

Чтобы **редактировать описание маршрута HTTP Reverse**, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование маршрута** Рисунок 57 внести изменения

3 нажать кнопку **Сохранить**

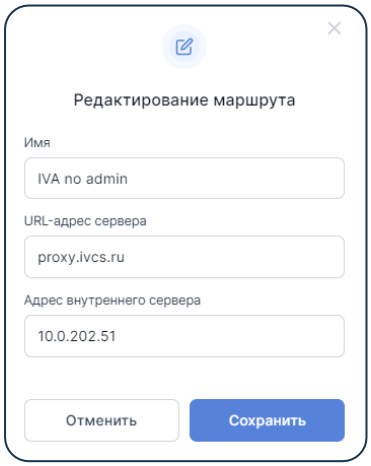

Рисунок 57. Редактирование маршрута HTTP Reverse

Удаление маршрута HTTP Reverse

Чтобы **удалить маршрут HTTP Reverse**, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление маршрута** Рисунок 58 нажать кнопку **Удалить**

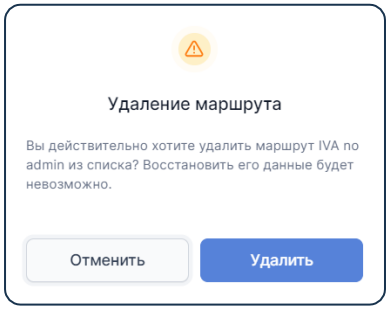

Рисунок 58. Удаление маршрута HTTP Reverse

> При удалении маршрут будет автоматически удален из всех **групп маршрутизации**

Редактирование маршрута HTTP Reverse и его правил фильтрации

Редактирование маршрута HTTP Reverse осуществляется на странице **Информация о маршруте HTTP Reverse** Рисунок 59:

В разделе **Маршруты HTTP Reverse** перейти на вкладку **Маршруты** и нажать ссылку <**Имя маршрута**>

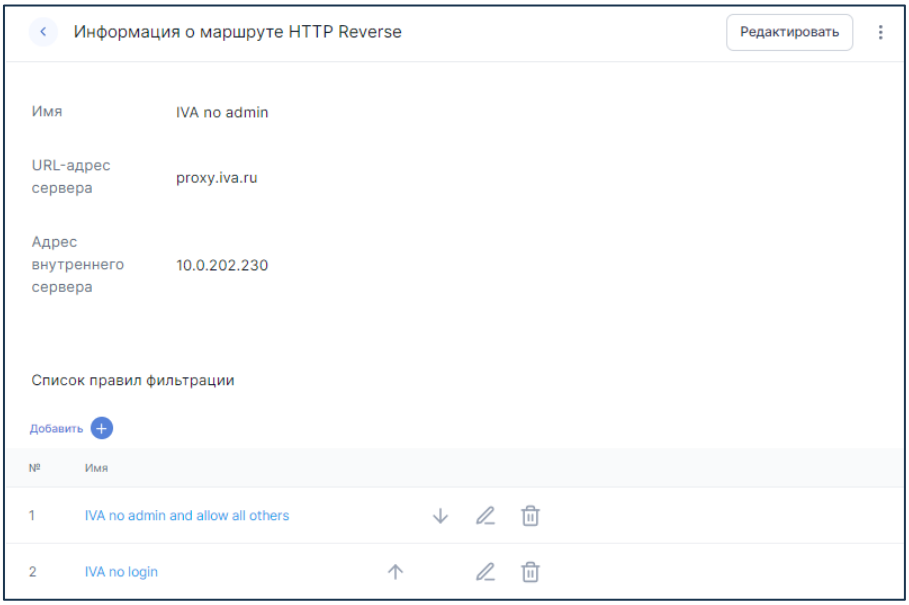

Рисунок 59. Информация о маршруте HTTP Reverse

При работе на странице Информация о маршруте HTTP Reverse Рисунок 59 можно:

- посмотреть список правил фильтрации
- добавить правило фильтрации в список правил фильтрации маршрута HTTP Reverse: нажать кнопку **Добавить**
- редактировать описание правила фильтрации: нажать кнопку
- удалить правило фильтрации из списка: нажать кнопку
- изменить порядок применения правил фильтрации

Добавление правила фильтрации в список правил фильтрации маршрута HTTP Reverse

Чтобы **добавить правило фильтрации** в маршрут HTTP Reverse, необходимо:

1 нажать кнопку **Добавить** Рисунок 59

2 в окне **Добавление правила** Рисунок 60 **выбрать правило** из ранее созданных (например **IVA no admin**) и нажать кнопку **Добавить**

3 повторить добавление правил фильтрации, необходимых для данного маршрута

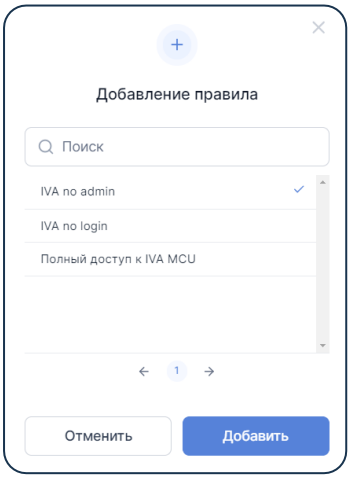

Рисунок 60. Добавление маршрута

Изменение порядка применения правил фильтрации

Добавленные правила фильтрации Рисунок 59 применяются в порядке очереди.

Чтобы **изменить** порядок применения правил фильтрации, необходимо использовать кнопки:

- ↑ для перемещения правила вверх
- ↓ для перемещения правила вниз

Удаление правила фильтрации из списка

На странице **Информация о маршруте HTTP Reverse** Рисунок 59 можно удалить правило фильтрации HTTP из списка правил:

1 **выбрать правило**, которое необходимо удалить и **нажать кнопку** 🗑

2 в окне **Удаление правила** нажать кнопку **Удалить** Рисунок 61

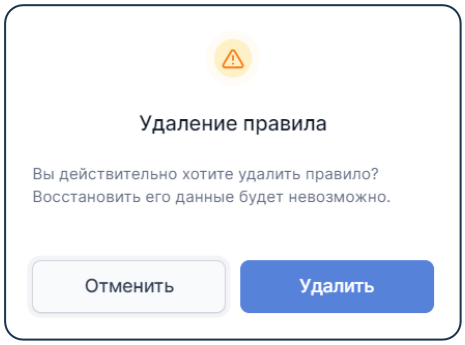

Рисунок 61. Удаление правила фильтрации из списка

Настройки проксирования RTP-трафика через TURN-протокол

IVA SBC может выполнять роль TURN-сервера для подключения пользователей к разрешённым IP-адресам.

Чтобы IVA SBC выполняло проксирование RTP-трафика через TURN-протокол, необходимо:

1. создать маршрут TURN со списком IP-адресов, на которые разрешено проксировать RTP-трафик
2. добавить группу маршрутизации TURN, содержащую список маршрутов (неупорядоченный)
3. назначить серверу проксирования роль и группу маршрутизации TURN Proxy
4. настроить дополнительные параметры TURN для сервера проксирования, выполняющего роль TURN Proxy

Алгоритм обработки TURN-трафика на сервере проксирования:

1. выполняется авторизация запроса от пользователя на сервере проксирования
2. обрабатывается запрос от пользователя с возможностью проксирования трафика на определённый IP-адрес и порт
3. для каждого запроса выполняется проверка IP-адреса на наличие в списке разрешённых IP-адресов
4. если запрашиваемый IP-адрес совпадает с разрешённым IP-адресом и портом, трафик проксируется через IVA SBC
5. если совпадений не найдено, то трафик не проксируется

Настройка TURN-сервиса

В разделе **Маршруты TURN** Рисунок 62 отображаются все добавленные маршруты TURN со списком IP-адресов, для которых разрешено проксировать RTP-трафик.

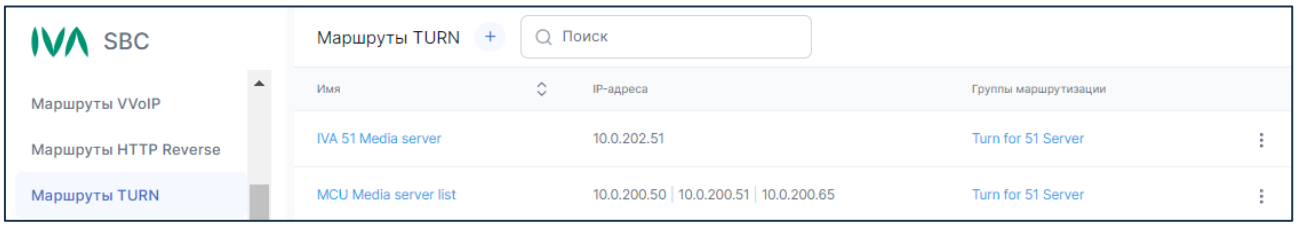

Рисунок 62. Маршруты TURN

При работе в разделе **Маршруты TURN** можно:

- посмотреть список маршрутов TURN
- создать новый маршрут TURN: нажать кнопку +
- добавить и редактировать список разрешённых IP-адресов: нажать ссылку <Имя маршрута>
- редактировать описание маршрута TURN: нажать кнопку ⋮ и выбрать **Редактировать**
- удалить маршрут TURN: нажать кнопку ⋮ и выбрать **Удалить**

Создание и редактирование маршрутов TURN

Создание маршрута TURN

Чтобы создать маршрут TURN, необходимо:

6 нажать кнопку + Рисунок 62

7 в окне **Добавление маршрута** Рисунок 63: ввести **имя** (рекомендуется вводить имя, которое кратко описывает назначение маршрута, например **MCU Media Server List**)

8 нажать кнопку **Создать**

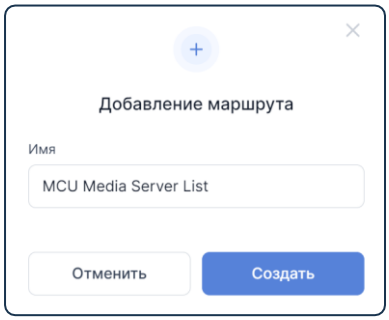

Рисунок 63. Добавление маршрута TURN

После создания маршрута TURN необходимо добавить список разрешённых IP-адресов.

Без указания разрешённых IP-адресов проксирование TURN не выполняется.

Редактирование описание маршрута TURN

Чтобы **редактировать описание** маршрута TURN, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование маршрута** Рисунок 64 внести изменения

3 нажать кнопку **Сохранить**

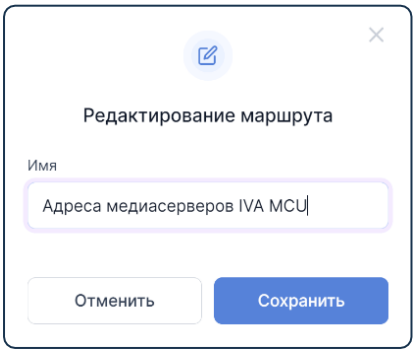

Рисунок 64. Редактировние описание маршрута TURN

Удаление маршрута TURN

Чтобы **удалить маршрут** TURN, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление маршрута** Рисунок 65 нажать кнопку **Удалить**

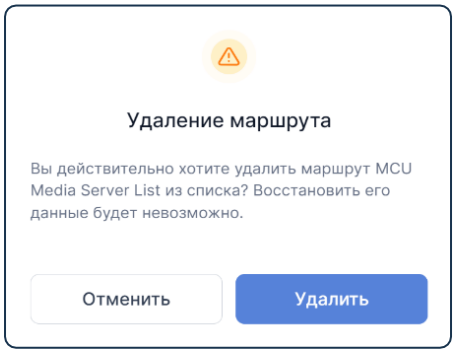

Рисунок 65. Удаление маршрута TURN

При удалении маршрут будет автоматически удален из всех групп маршрутизации

Добавление и редактирование разрешённых IP-адресов

Добавление и редактирование разрешённых IP-адресов проводится на странице Информация о маршруте TURN Рисунок 66:

Перейти в раздел Маршруты TURN и нажать ссылку <Имя маршрута TURN>

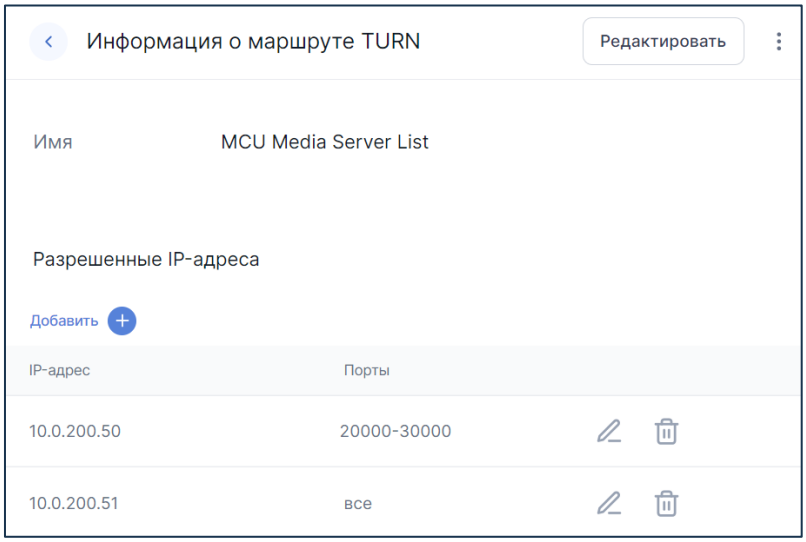

Рисунок 66. Информация о маршруте TURN

При работе на странице Информация о маршруте TURN можно:

- посмотреть список разрешённых IP-адресов
- добавить разрешённый IP-адрес: нажать кнопку Добавить

- редактировать описание маршрута TURN: нажать кнопку **Редактировать**
- редактировать разрешённый IP-адрес маршрута TURN: нажать кнопку
- удалить маршрут TURN: нажать кнопку и выбрать **Удалить**
- удалить разрешённый IP-адрес маршрута TURN: нажать кнопку

Добавление разрешённого IP-адреса

Чтобы добавить разрешённый IP-адрес, необходимо:

1 на странице **Информация о маршруте TURN** Рисунок 66 нажать кнопку **Добавить**

2 в окне **Добавление IP-адреса** Рисунок 67:

- **IP-адрес** – ввести адрес, для которого нужно разрешить проксирование RTP-трафика (например **10.0.200.50**)
- **Порты** – ввести значение портов, через которые разрешено проксирование RTP-трафика (для IVA MCU используются порты **20000-30000**). Порты допускается записывать как по одному, так и перечислением (например 3000, 4000-6000). Если значение порта не указано, то IVA SBC будет использовать все доступные порты

3 нажать кнопку **Добавить**

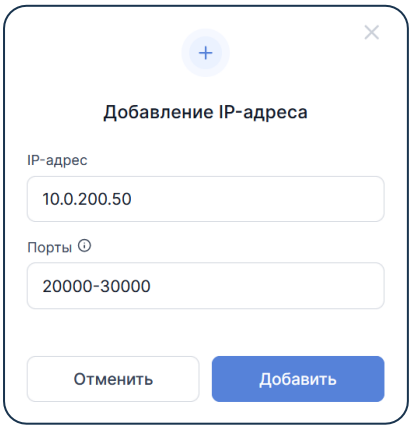

Рисунок 67. Добавление разрешённого IP-адреса

Редактирование разрешённого IP-адреса маршрута TURN

На странице Информация о маршруте TURN Рисунок 66 можно **редактировать** разрешённые IP-адреса маршрута TURN:

1 выбрать **разрешённый IP-адрес**, который необходимо редактировать, и **нажать кнопку**

2 в окне **Редактирование IP-адреса** Рисунок 68: внести изменения (описание полей приведено в разделе Добавление разрешённого IP-адреса)

3 нажать кнопку **Сохранить**

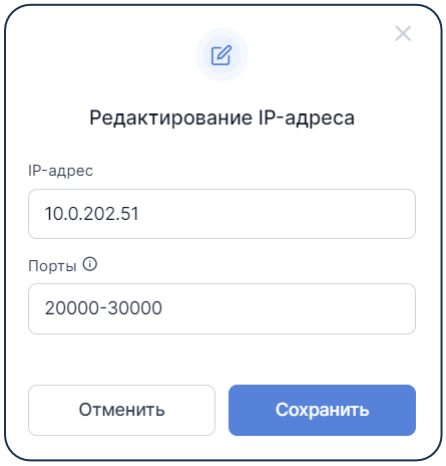

Рисунок 68. Редактирование IP-адреса маршрута TURN

Удаление разрешённого IP-адреса маршрута TURN

На странице Информация о маршруте TURN Рисунок 66 можно удалить разрешенный IP-адрес маршрута TURN: **нажать кнопку**

> Удаление правила разрешенного IP-адреса маршрута TURN происходит **без подтверждения удаления**

Настройки HTTP Proxy

IVA SBC позволяет реализовать HTTP-проксирование для доступа к внешним серверам из внутренней сети. Система выполняет аутентификацию и авторизацию пользователя по его паролю и IP-адресу.
Например, HTTP Proxy может использоваться для отправки push-уведомлений со стороны IVA MCU без предоставления IVA MCU прямого доступа в Интернет.

Чтобы IVA SBC выполняло HTTP-проксирование, необходимо:

1. добавить группы доступа со списком разрешенных адресов серверов
2. добавить пользователей HTTP Proxy, указав их аутентификационные данные и список IP-адресов, с которых пользователи могут выполнять запросы
3. назначить пользователям HTTP Proxy группы доступа
4. назначить серверу проксирования роль HTTP Proxy

Алгоритм обработки HTTP-трафика на сервере проксирования:

1. выполняется авторизация запроса от пользователя на **сервере проксирования**, включая проверку логина, пароля и IP-адреса пользователя
2. для каждого запроса выполняется проверка сетевого адреса на наличие в **списке разрешённых адресов** для группы доступа пользователя
3. если запрашиваемый адрес **совпадает с разрешённым** адресом в группе доступа пользователя, трафик проксируется через IVA SBC
4. если совпадений не найдено, то трафик не проксируется
5. сервер проксирования логирует информацию о запросах HTTP Proxy

> **Файл с логами** HTTP Proxy сохраняется на серверах проксирования в директории: **/var/log/sbc/http_proxy.log**

В разделе **Настройки HTTP Proxy**:

- на вкладке **Группы доступа** Рисунок 69 определяют, к каким серверам можно обращаться пользователю

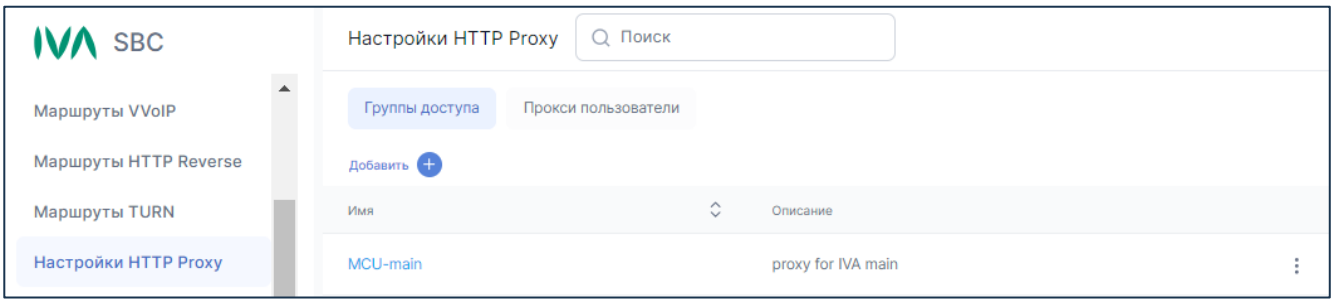

Рисунок 69. Вкладка Группы доступа

- на вкладке **Прокси пользователи** Рисунок 70 для каждого пользователя указываются логин, пароль и список IP адресов, с которых он может выполнять запросы на разрешённые группой доступа адреса серверов

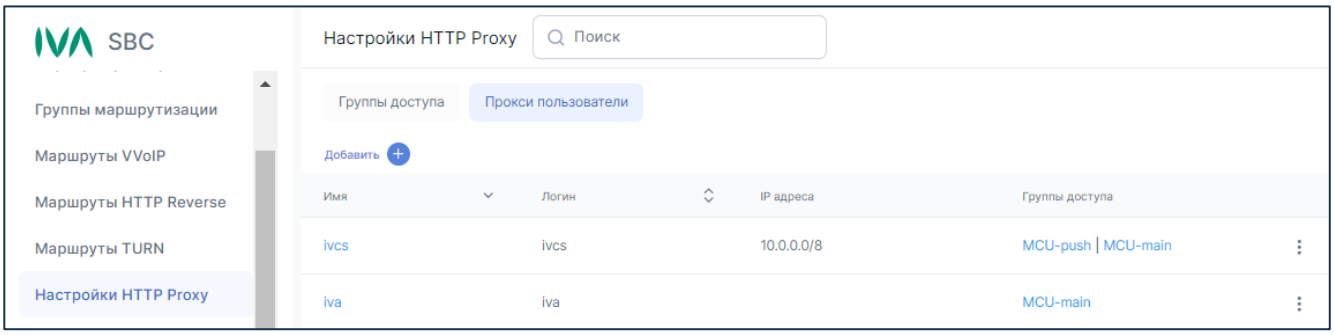

Рисунок 70. Вкладка Прокси пользователи

Группы доступа

В разделе **Настройки HTTP Proxy** на вкладке **Группы доступа** Рисунок 69 отображаются добавленные группы доступа для HTTP-проксирования на внешние сайты.

При работе на вкладке **Группы доступа** Рисунок 69 можно:

- просмотреть список добавленных групп доступа
- добавить группу доступа: нажать кнопку **Добавить**
- редактировать описание группы доступа: нажать кнопку ⋮ и выбрать Редактировать Рисунок 72
- удалить группу доступа: нажать кнопку ⋮ и выбрать Удалить Рисунок 73

- редактировать список разрешенных адресов серверов: нажать ссылку <Имя группы доступа>

Добавление группы доступа

Чтобы добавить группу доступа HTTP Proxy:

1 нажать кнопку **Добавить** Рисунок 69

2 в окне **Создание группы доступа** Рисунок 71 ввести:

- **Имя**: рекомендуется вводить имя, которое кратко описывает назначение группы доступа (например **MCU-push**)
- **Описание**: рекомендуется вводить описание, отражающее результат работы HTTP-проксирования (например **Отправка push IVA MCU через HTTP Proxy**)

3 нажать кнопку **Создать**

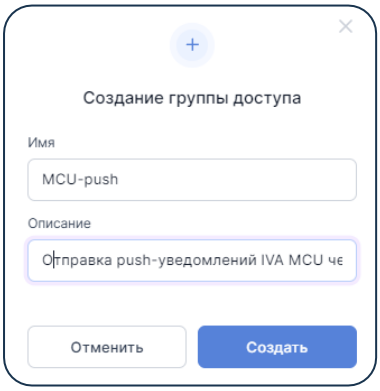

Рисунок 71. Создание группы доступа HTTP Proxy

После создания группы доступа необходимо добавить список разрешённых адресов.

Без указания разрешённых адресов проксирование HTTP не выполняется.

Редактирование описания группы доступа

Чтобы **редактировать описание группы доступа HTTP Proxy**:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование группы доступа** Рисунок 72 внести изменения

3 нажать кнопку **Сохранить**

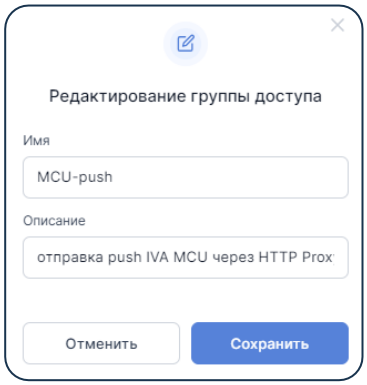

Рисунок 72. Редактирование группы доступа HTTP Proxy

Удаление группы доступа

Чтобы **удалить группу доступа HTTP Proxy**:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление маршрута** Рисунок 73 нажать кнопку **Удалить**

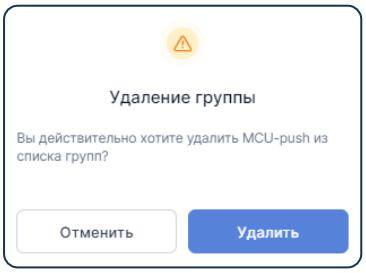

Рисунок 73. Удаление группы доступа HTTP Proxy

Добавление и редактирование разрешённых адресов

Добавление и редактирование разрешённых адресов серверов проводится на странице **Информация о группе доступа** Рисунок 74:

Перейти в раздел **Настройки HTTP Proxy** и нажать ссылку <**Имя группы доступа**>

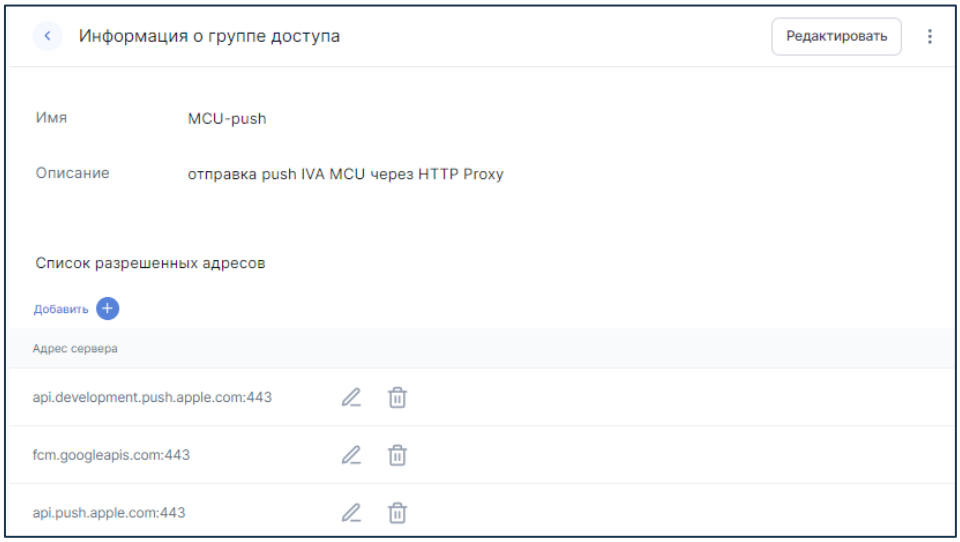

Рисунок 74. Информация о группе доступа

При работе на странице **Информация о группе доступа** можно:

- посмотреть список разрешённых адресов
- добавить разрешённый адрес: нажать кнопку **Добавить**
- редактировать описание группы доступа: нажать кнопку **Редактировать**
- редактировать разрешённый адрес группы доступа: **нажать кнопку**
- удалить группу доступа: **нажать кнопку** и выбрать **Удалить**
- удалить разрешённый адрес группы доступа: **нажать кнопку**

Добавление разрешённого адреса в группу доступа

Чтобы добавить разрешённый адрес сервера, необходимо:

1 на странице **Информация о группе доступа** Рисунок 74 нажать кнопку **Добавить**

2 в окне **Добавление разрешённого адреса** Рисунок 75 ввести адрес сервера, для которого нужно разрешить HTTP-проксирование (например **api.push.apple.com:443**)

3 нажать кнопку **Добавить**

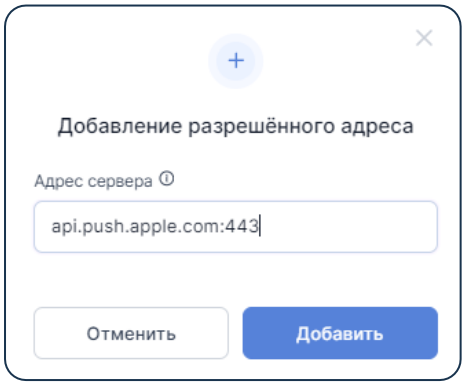

Рисунок 75. Добавление разрешённого адреса

Редактирование разрешённого адреса группы доступа

На странице **Информация о группе доступа** Рисунок 74 можно **редактировать** разрешённые адреса группы доступа HTTP Proxy:

1 выбрать **разрешённый адрес**, который необходимо редактировать, и **нажать кнопку**

2 в окне **Редактирование разрешённого адреса** Рисунок 76: внести изменения

3 нажать кнопку **Сохранить**

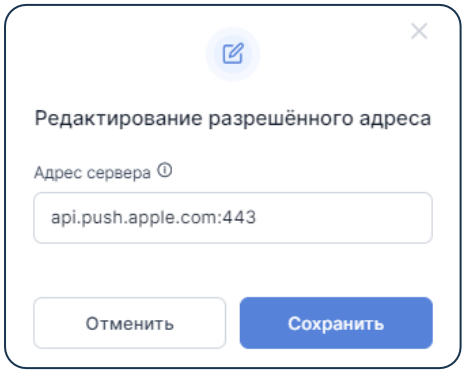

Рисунок 76. Редактирование разрешённого адреса

Удаление разрешённого адреса из группы доступа

На странице **Информация о группе доступа** Рисунок 74 можно удалить разрешённый адрес из группы доступа HTTP Proxy: **нажать кнопку**

> Удаление правила разрешённого адреса из группы доступа происходит **без подтверждения удаления**

Прокси пользователи

На вкладке **Прокси пользователи** Рисунок 70 для каждого пользователя HTTP Proxy можно указать логин, пароль и список IP-адресов, с которых будет разрешено выполнять запросы.

При работе на вкладке **Прокси пользователи** можно:

- посмотреть список пользователей HTTP Proxy и назначенные им группы доступа
- добавить нового прокси пользователя: нажать кнопку ⊕
- редактировать данные прокси пользователя: нажать кнопку ⋮ и выбрать **Редактировать**
- добавить для прокси пользователя группу доступа нажать кнопку ⋮ и выбрать **Добавить группу доступа**
- редактировать список групп доступа прокси пользователя: нажать ссылку **<Имя прокси пользователя>**
- удалить прокси пользователя: нажать кнопку ⋮ и выбрать **Удалить**

Добавление прокси пользователя

Чтобы **добавить прокси пользователя**:

1 нажать кнопку **Добавить** ⊕ Рисунок 70

2 в окне **Создание прокси пользователя** Рисунок 77:

- **Имя:** ввести имя пользователя (например **IVA**)
- **Логин** и **Пароль**: ввести аутентификационные данные пользователя
- **IP адреса:** ввести IP-адреса, с которых пользователю разрешено обращаться на внешние сервера (можно указывать через запятую, например 10.0.0.0/8,172.16.0.0/12)

3 нажать кнопку **Создать**

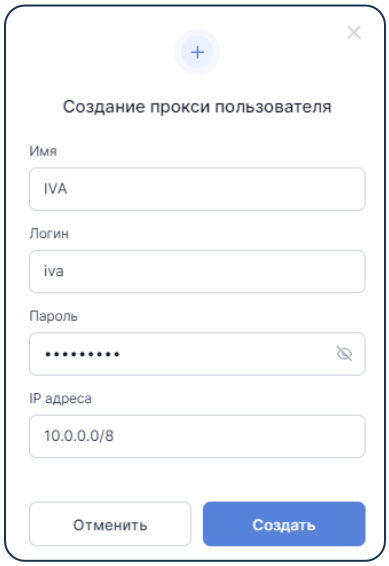

Рисунок 77. Добавление прокси пользователя

После создания прокси пользователя необходимо добавить ему группы доступа.

Редактирование данных прокси пользователя

Чтобы **редактировать данные прокси пользователя**:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование прокси пользователя** Рисунок 78 внести изменения

3 нажать кнопку **Сохранить**

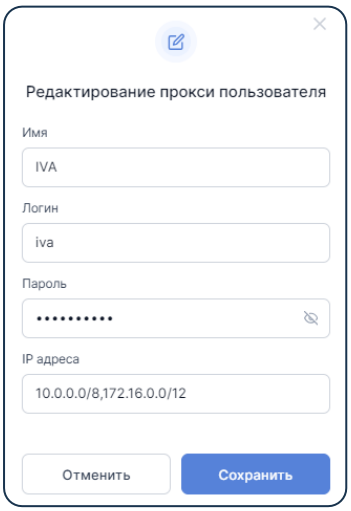

Рисунок 78. Редактирование данных прокси пользователя

Добавление группы доступа для прокси пользователя

Чтобы **назначить пользователю группу доступа:**

1 **нажать кнопку** ⋮ и выбрать **Добавить группу доступа**

2 в окне **Добавление группы доступа** Рисунок 79 выбрать группу

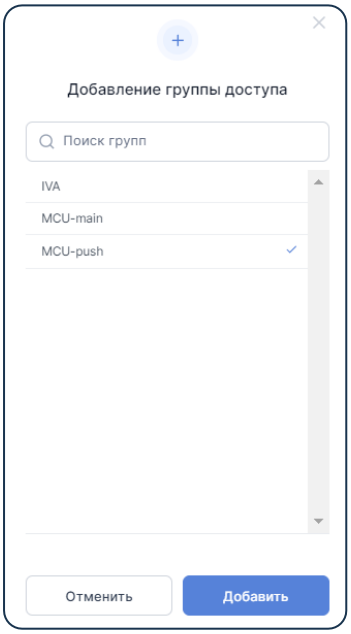

Рисунок 79. Добавление группы доступа

3 нажать кнопку **Добавить**

Редактирование списка групп доступа прокси пользователя

Редактирование списка групп доступа прокси пользователя проводится на странице **Информация о прокси пользователе** Рисунок 80:

В разделе **Настройки HTTP Proxy** на вкладке **Прокси пользователи** нажать ссылку <**Имя прокси пользователя**>

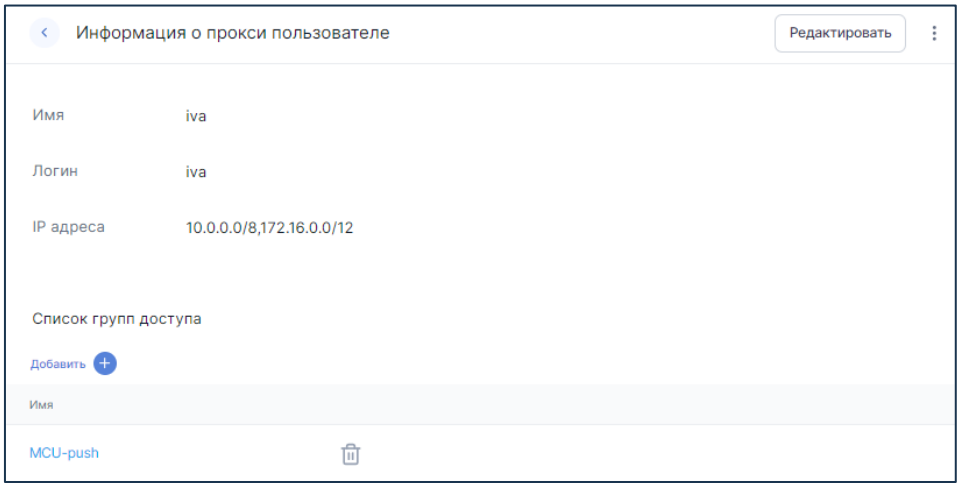

Рисунок 80. Информация о прокси пользователе

При работе на странице **Информация о прокси пользователе** можно:

- посмотреть информацию о прокси пользователе и список групп доступа пользователя
- редактировать данные прокси пользователя: нажать кнопку **Редактировать**
- удалить прокси пользователя: **нажать кнопку** ⋮ и выбрать **Удалить**
- добавить группу доступа в список: нажать кнопку **Добавить** ⊕
- удалить группу доступа из списка: нажать кнопку 🗑

> Удаление группы из списка групп доступа происходит **без подтверждения удаления**

Удаление прокси пользователя

Чтобы **удалить прокси пользователя**:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление прокси пользователя** Рисунок 81 нажать кнопку **Удалить**

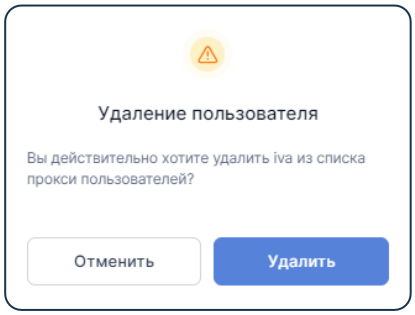

Рисунок 81. Удаление прокси пользователя

Настройки

В разделе **Настройки** Рисунок 82 можно:

- управлять используемыми SSL-сертификатами
- управлять списком доверенных внешних HTTP-прокси-серверов
- управлять системными настройками

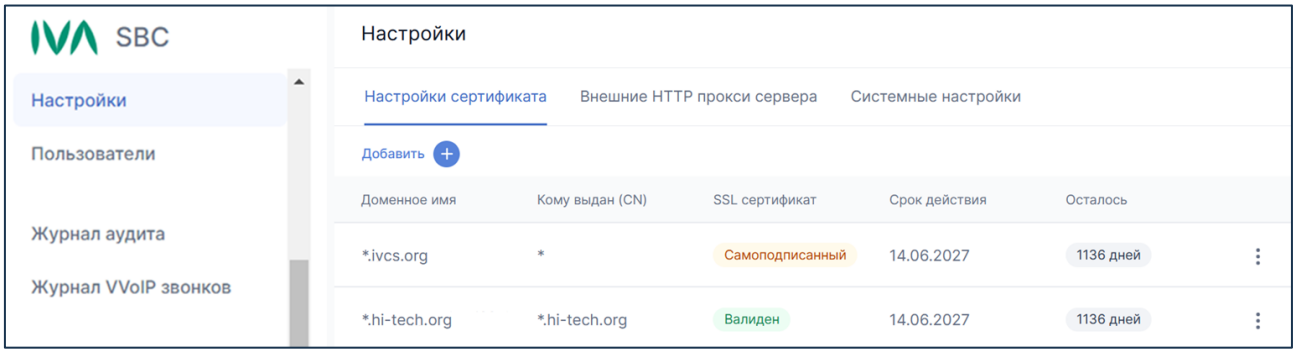

Рисунок 82. Раздел Настройки

Настройка SSL-сертификатов

IVA SBC позволяет добавлять SSL-сертификаты, которые могут использоваться для:

- входящих HTTPS-запросов
- TLS в SIP
- TLS в H.323
- TLS TURN-серверов

При работе на вкладке **Настройки сертификата**, можно:

- посмотреть список сертификатов Рисунок 82
- добавить сертификат: нажать кнопку **Добавить** ⊕
- удалить сертификат: **нажать кнопку** ⋮ и выбрать **Удалить**

На вкладке настройки сертификата отображены:

- **Доменное имя** – имя, указанное при добавлении сертификата
- **Кому выдан** –имя владельца (CN), организации (O) или подразделения (OU)
- **SSL сертификат** – отображает статус (Валиден / Самоподписанный / Отозван)

- **Срок действия** – дата окончания действия сертификата
- **Осталось** – оставшееся время действия сертификата (в днях)

Добавление SSL-сертификата

Чтобы **добавить сертификат**, необходимо:

1 нажать кнопку **Добавить** ⊕

2 в окне **Добавление сертификата** Рисунок 83:

- **Доменное имя**: ввести имя (например ***.test.org**)
- **Сертификат**: ввести сертификат (содержимое файла с расширением ***.pem)**
- **Приватный ключ**: ввести ключ (содержимое файла с расширением ***.key**)
- нажать кнопку **Проверить** (будет проведена проверка сертификата на валидность)

3 в окне **Добавление сертификата** Рисунок 83 нажать кнопку **Добавить**

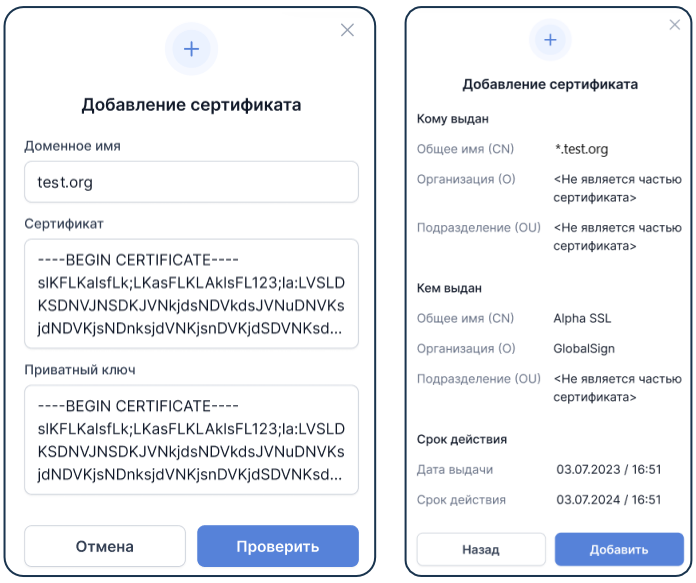

Рисунок 83. Добавление сертификата

Удаление SSL-сертификата

Для **удаления сертификата** необходимо:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление сертификата** Рисунок 84 нажать кнопку **Удалить**

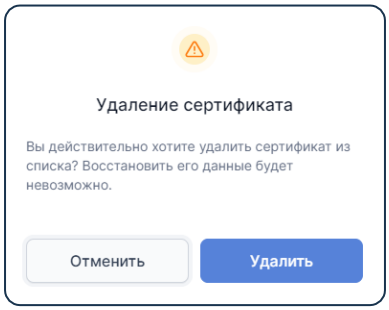

Рисунок 84. Подтверждение удаления сертификата

Настройка адреса внешнего HTTP-прокси-сервера

В разделе **Настройки**, на вкладке **Внешние HTTP прокси сервера** Рисунок 85 можно добавлять, редактировать и удалять адреса внешних HTTP-прокси-серверов (например WAF).

Внешние HTTP-прокси-сервера стоят перед IVA SBC, и чтобы узнать реальный IP-адрес пользователя необходимо использовать один из заголовков HTTP-запроса: X-Real-IP или X-Forwarded-For.

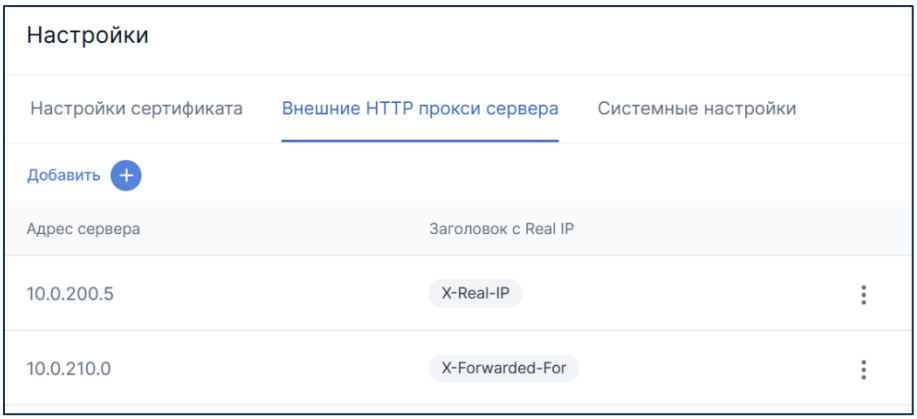

Рисунок 85. Добавление внешних HTTP-серверов проксирования

При работе на вкладке **Внешние HTTP прокси сервера**, можно:

- посмотреть список серверов Рисунок 85
- добавить адрес внешнего HTTP-прокси-сервера: нажать кнопку **Добавить** ⊕
- редактировать адрес внешнего HTTP-прокси-сервера: нажать кнопку ⋮ и выбрать Редактировать
- удалить адрес внешнего HTTP-прокси-сервера: **нажать кнопку** ⋮ и выбрать **Удалить**

Добавление адреса внешнего HTTP-прокси-сервера

Чтобы добавить внешний HTTP-прокси-сервер, необходимо:

1 нажать кнопку **Добавить**

2 в окне **Добавление внешнего HTTP прокси сервера** Рисунок 86:

- **Адрес сервера**: ввести IP-адрес внешнего HTTP-прокси-сервера (например 10.0.200.110)
- **Заголовок с Real IP**: выбрать X-Real-IP или X-Forwarded-For

3 нажать кнопку **Сохранить**

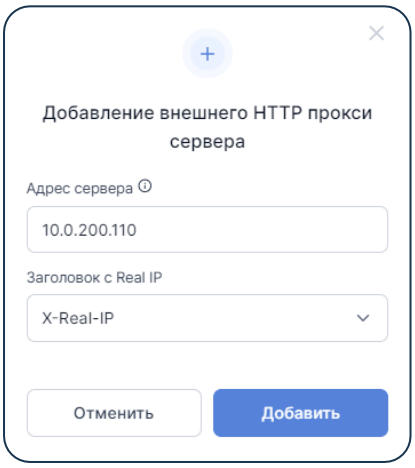

Рисунок 86. Добавление внешнего HTTP-прокси-сервера

Редактирование адреса внешнего HTTP-прокси-сервера

Чтобы **редактировать** внешний HTTP-прокси-сервер, необходимо:

1 **нажать кнопку** и выбрать **Редактировать**

2 в окне **Редактирование внешнего HTTP прокси сервера** Рисунок 87 внести изменения

3 нажать кнопку **Сохранить**

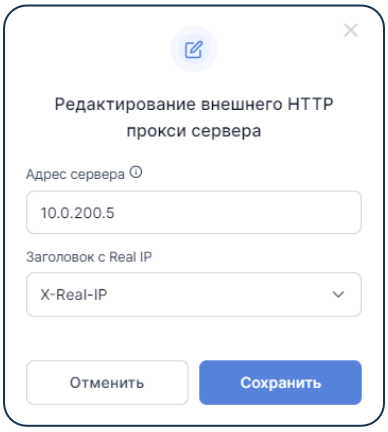

Рисунок 87. Редактирование внешнего HTTP-прокси-сервера

Удаление адреса внешнего HTTP-прокси-сервера

Чтобы **удалить** внешний HTTP-прокси-сервер, необходимо:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаления сервера** Рисунок 88 нажать кнопку **Удалить**

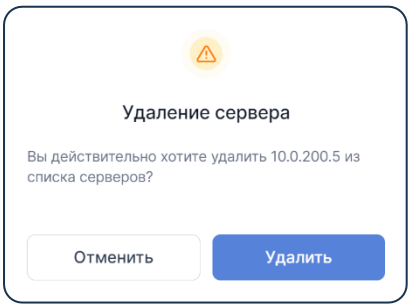

Рисунок 88. Удаление адреса внешнего HTTP-прокси-сервера

Системные настройки

При работе на вкладке **Системные настройки** Рисунок 89, можно выполнить настройку:

- параметров логирования
- списка NTP-сервера
- обработки SNMP-запросов
- Zabbix agent
- списка используемых DNS-серверов
- доступа к серверам по протоколу SSH
- локальных DNS-записей
- безопасности web-панели администрирования

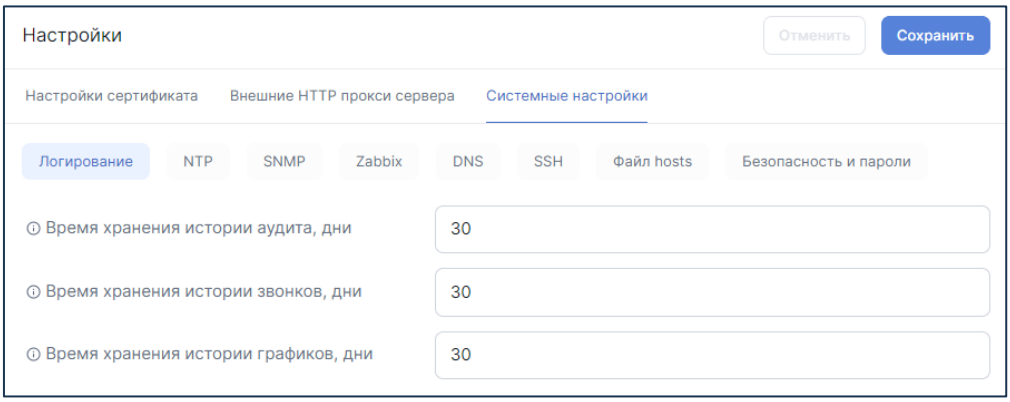

Рисунок 89. Вкладка Системные настройки

> Системные настройки применяются **на всех серверах** IVA SBC автоматически

Если в **Системных настройках** были осуществлены изменения на какой-либо из **вкладок** (Логирование, NTP, SNMP и т. д.) и не были сохранены, то при переходе на другую вкладку или в другой раздел система выдаёт предупреждение Рисунок 90 со следующими вариантами действий:

1 нажать кнопку **Отменить**: для отмены изменений

2 нажать кнопку **Вернуться**: для продолжения изменения и сохранения настроек

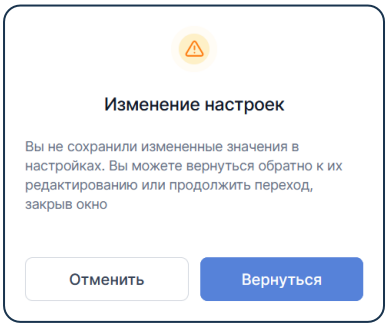

Рисунок 90. Предупреждение об изменении настроек

Настройка параметров Логирования

На вкладке **Логирование** Рисунок 89 можно настроить время хранения данных истории Аудита и Мониторинга.

Чтобы **настроить время хранения истории**, необходимо:

1 указать значение времени хранения истории:

- Время хранения истории аудита, дни: ввести значение времени хранения событий журнала аудита (в днях)
- Время хранения истории звонков, дни: ввести значение времени хранения истории журнала VoIP-звонков (в днях)
- Время хранения истории графиков, дни: ввести значение времени хранения истории графиков (в днях)

2 нажать кнопку **Сохранить**

> Значение **0** времени хранения истории означает, что события не удаляются

> Настройки параметров логирования применяются **на всех серверах IVA SBC** автоматически

Настройка списка NTP-серверов

На вкладке **NTP** Рисунок 91 можно **включить синхронизацию времени, добавить NTP-сервера** и **опции для них**.

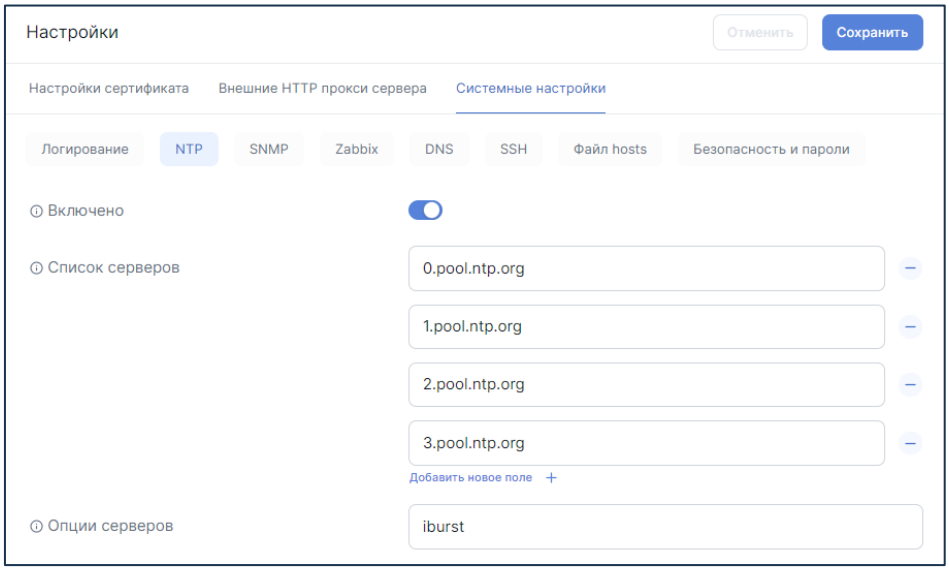

Рисунок 91. Настройка NTP-серверов

Чтобы **настроить синхронизацию времени**, необходимо:

1 **Включено**: нажать **переключатель** для включения синхронизации времени

> Дальнейшая настройка синхронизации времени возможна только после её активации

2 **Список серверов**: ввести **адрес NTP-сервера**

- при необходимости добавить **дополнительный NTP-сервер**: нажать ссылку **Добавить новое поле** + и ввести **адрес NTP-сервера**
- при необходимости **удалить адрес NTP-сервера** из списка серверов: **нажать кнопку** −

3 **Опции серверов**: добавить опции (например опция **iburst** для повышения точности синхронизации)

4 нажать кнопку **Сохранить**

> Настройки NTP-серверов применяются **на всех серверах IVA SBC** автоматически

Настройка обработки SNMP-запросов

На вкладке **SNMP** Рисунок 92 можно **включить и настроить обработку SNMP-запросов v2 и v3**.

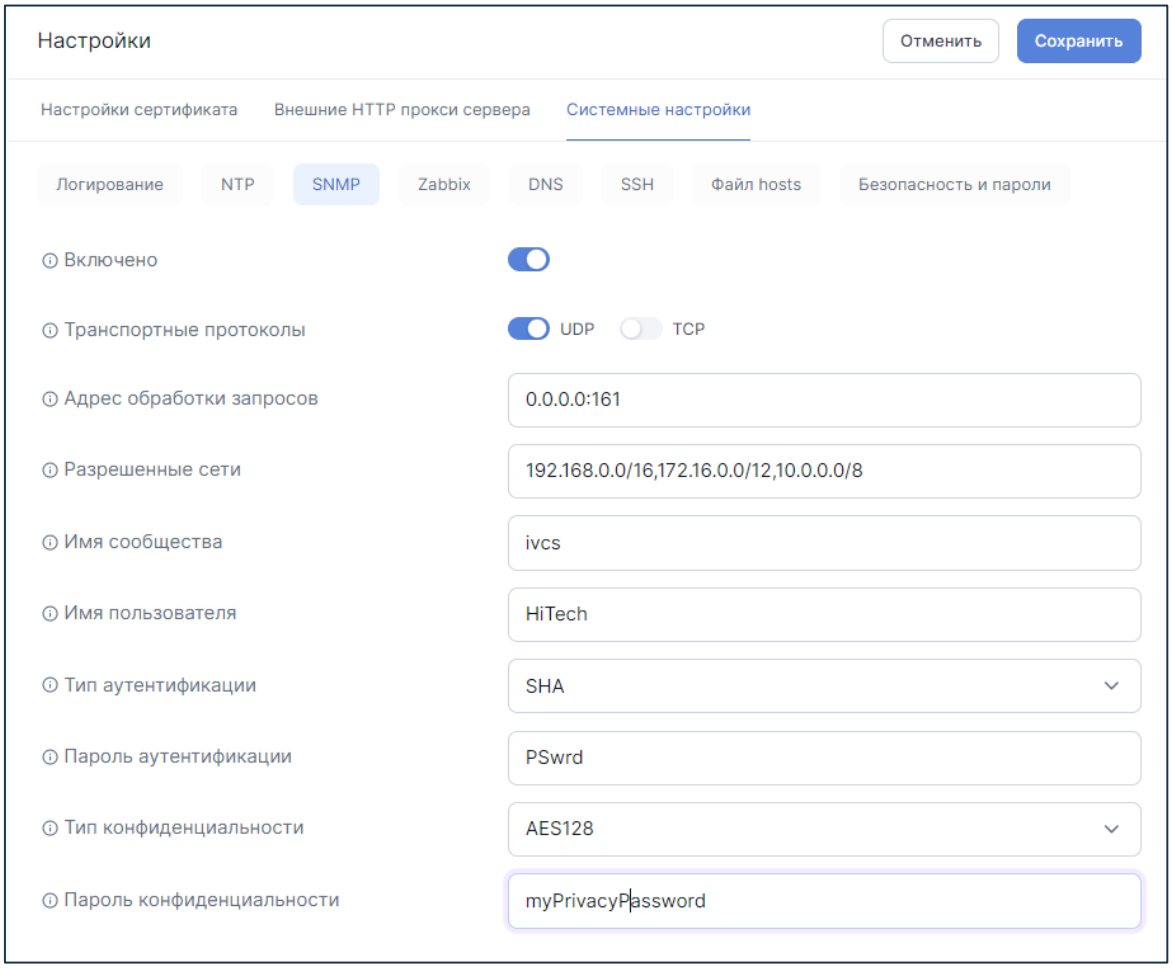

Рисунок 92. Настройка SNMP

Чтобы **включить и настроить SNMP-агента**, необходимо:

1 **Включено**: нажать **переключатель** для включения поддержки обработки SNMP-запросов от внешних систем

> Дальнейшая настройка SNMP-агента возможна только после его активации

2 **Транспортные протоколы**: выбрать транспортный протокол (**UDP** и / или **TCP**) и нажать соответствующие переключатели

3 **Адрес обработки запросов**: ввести IP-адрес, на котором система должна слушать SMNP-запросы (обычно **0.0.0.0:161**)

4 **Разрешенные сети**: добавить список подсетей, из которых разрешено обращение по протоколу SNMP (можно указывать через запятую, например **192.168.0.0/16,172.16.0.0/12**)

5 **Имя сообщества**: ввести имя сообщества, которое будет использоваться для обмена информацией в **SNMP v2** (например **ivcs**)

6 **Имя пользователя**: ввести имя **SNMP v3** пользователя (например **HiTech**)

7 **Тип аутентификации**: выбрать тип аутентификации для учётной записи **SNMP v3**:

- **MD5** – создает хеш длиной 128 бит, быстрее по сравнению с SHA, не рекомендуется для использования в новых системах из-за уязвимостей
- **SHA** – семейство функций, включая SHA-1 (160 бит), SHA-256, SHA-384, и SHA-512. SHA-256 и выше считаются более безопасными и устойчивыми к коллизиям (разные входные данные, дающие одинаковый хеш)

8 **Пароль аутентификации**: ввести пароль для аутентификации учётной записи SNMP v3 (например **PSwrd**)

9 **Тип конфиденциальности**: выбрать тип конфиденциальности для учётной записи **SNMP v3**:

- **AES128** / **AES192** / **AES256** – варианты симметричного алгоритма блочного шифрования, где числа 128, 192 и 256 обозначают размер ключа в битах. Больший размер ключа обеспечивает более высокий уровень безопасности
- **DES** / **DES3** – устаревшие алгоритмы блочного шифрования, считаются небезопасным для использования

10 **Пароль конфиденциальности**: ввести пароль конфиденциальности для учётной записи **SNMP v3** (например **myPrivacyPassword**)

11 нажать кнопку **Сохранить**

> Настройки обработки SNMP-запросов применяются **на всех серверах IVA SBC** автоматически

Настройка Zabbix agent

На вкладке **Zabbix** Рисунок 93 можно **включить и настроить zabbix agent** для возможности самостоятельной настройки системы мониторинга средствами Zabbix.

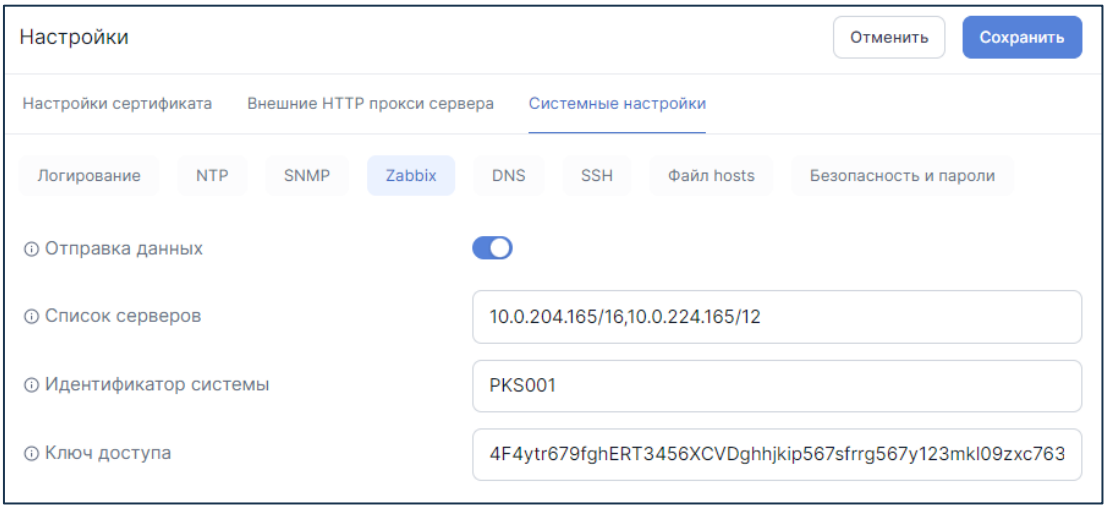

Рисунок 93. Настройка Zabbix

Чтобы **включить и настроить Zabbix**, необходимо:

1 **Отправка данных**: нажать **переключатель** для отправления данных на Zabbix-сервер

> Дальнейшая настройка Zabbix возможна только после её активации

2 **Список серверов**: ввести IP-адреса и подсети Zabbix-серверов, с которых разрешён доступ к системе (можно указывать через запятую, например 10.0.204.165/16,10.0.224.165/12)

3 **Идентификатор системы**: ввести идентификатор системы для аутентификации обращений от Zabbix-сервера (например **PKS001**)

4 **Ключ доступа**: ввести секретный ключ доступа для аутентификации обращений от Zabbix-сервера (значение должно быть шестнадцатеричной строкой). Ключ можно сгенерировать в консоли управления, выполнив команду **openssl rand -hex 32**

5 нажать кнопку **Сохранить**

> Настройки Zabbix применяются **на всех серверах IVA SBC** автоматически

Настройка списка используемых DNS-серверов

На вкладке DNS Рисунок 94 можно **добавить адреса DNS-серверов.**

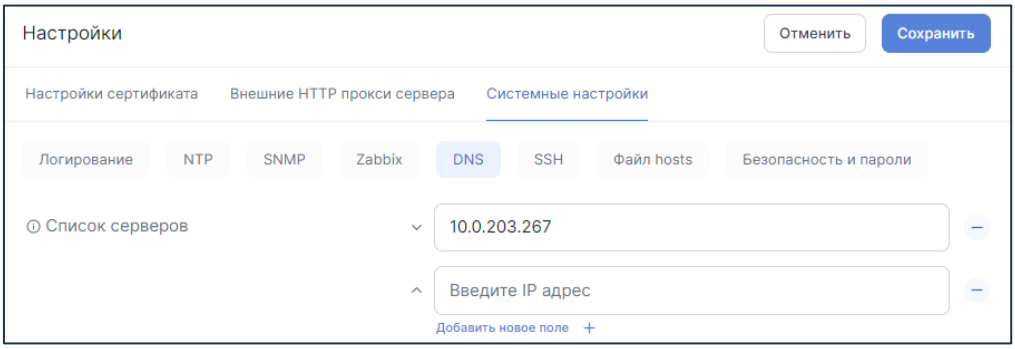

Рисунок 94. Настройка DNS

- Чтобы **добавить DNS-сервер**, необходимо: в строке **Список серверов** ввести IP-адрес DNS-сервера (например 10.0.203.267) и нажать кнопку **Сохранить**
- Чтобы **добавить дополнительный DNS-сервер**, необходимо: нажать ссылку **Добавить новое поле** + , в добавленном поле ввести **IP-адрес DNS-сервера** и нажать кнопку **Сохранить**
- Чтобы **удалить DNS-сервер**, необходимо: **нажать кнопку** — и нажать кнопку **Сохранить**

Добавленные адреса DNS-серверов Рисунок 94 применяются в порядке очереди. Чтобы изменить порядок применения DNS-серверов (**поднять** или **опустить** DNS-сервер в очереди), необходимо использовать кнопки ^ и v соответственно, а затем нажать кнопку **Сохранить**.

> Настройки используемых DNS-серверов применяются **на всех серверах IVA SBC** автоматически

Настройка доступа к серверам по протоколу SSH

На вкладке SSH Рисунок 95 можно выполнить настройку удалённого доступа по протоколу SSH.

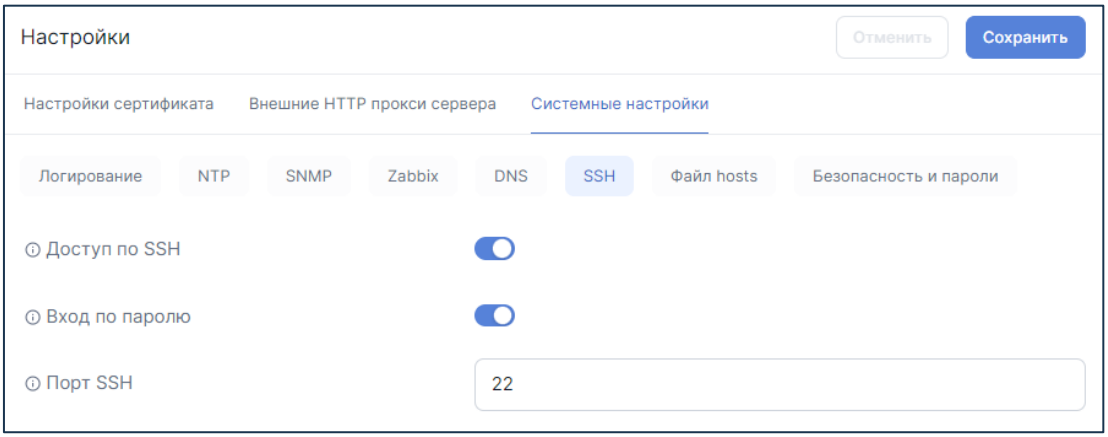

Рисунок 95. Настройка SSH

- Чтобы разрешить удаленный доступ по протоколу SSH, необходимо:
  Доступ по SSH: нажать переключатель и нажать кнопку Сохранить

> Дальнейшая настройка доступа по протоколу SSH возможна только после его активации

- Чтобы разрешить удаленный доступ по протоколу SSH с помощью пароля, необходимо:
  Вход по паролю: нажать переключатель и нажать кнопку Сохранить

> Пароль для входа задаётся во время установки системы IVA SBC (см. руководство по установке Install Guide IVA SBC)

- Чтобы настроить порт для подключения по протоколу SSH, необходимо:
  Порт SSH: ввести номер порта для подключения по SSH (например 22) и нажать кнопку Сохранить

> Настройки доступа к серверам по протоколу SSH применяются на всех серверах IVA SBC автоматически

Настройка локальных DNS-записей

На вкладке **Файл hosts** Рисунок 96 можно выполнить настройку локальных DNS-записей.

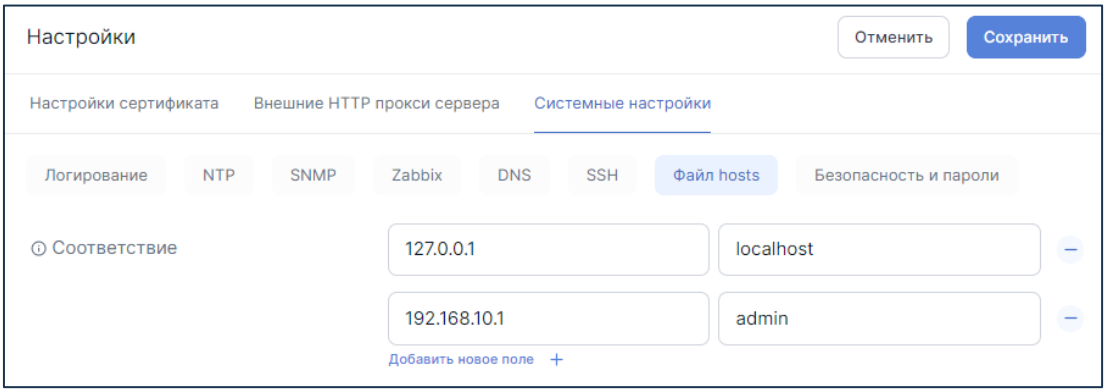

Рисунок 96. Настройка Файл hosts

Чтобы **настроить локальные DNS-записи**, необходимо:

1 в строке **Соответствие**:

- **IP адрес**: ввести IP-адрес сервера (например **127.0.0.1**)
- **Имя хоста или доменное имя**: ввести имя хоста или доменное имя (например **localhost**)

2 при необходимости **добавить новое соответствие**: нажать ссылку **Добавить новое поле** + и ввести **IP адрес** и **Имя хоста или доменное имя**

3 при необходимости **удалить лишнее поле**: **нажать кнопку** −

4 нажать кнопку **Сохранить**

> Настройка **локальных DNS-записей** сохраняется в отдельном файле на сервере управления и конфигурации

> Настройки локальных DNS-записей применяются **на всех серверах IVA SBC** автоматически

Настройка безопасности web-панели администрирования

На вкладке **Безопасность и пароли** Рисунок 97 можно выполнить настройку безопасности web-панели администрирования IVA SBC.

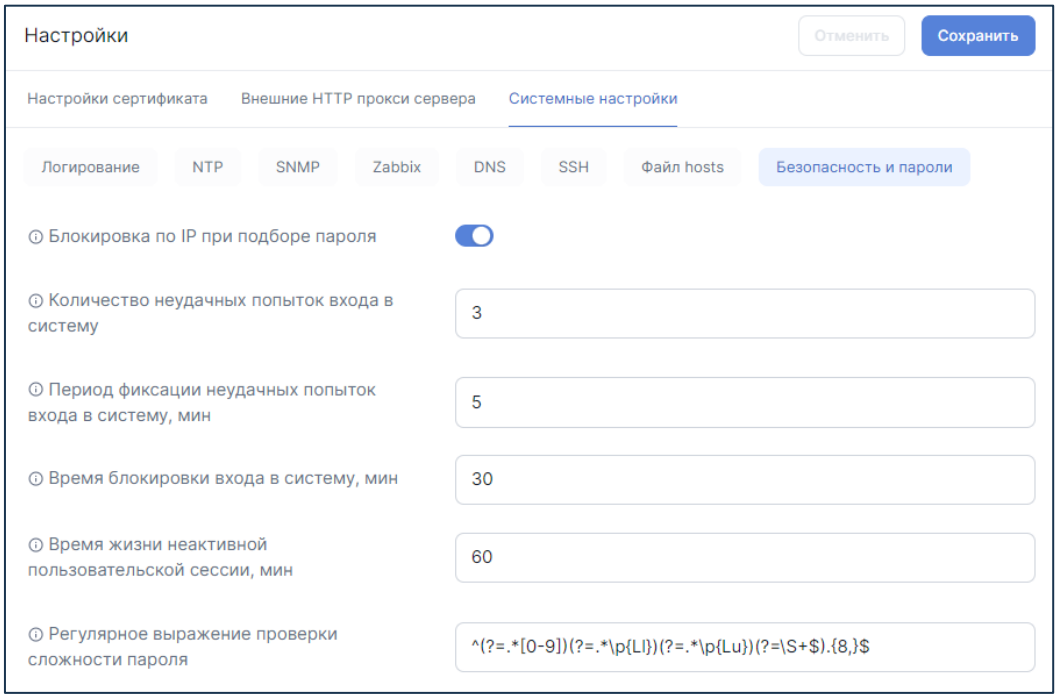

Рисунок 97. Настройка Безопасность и пароли

Чтобы **настроить безопасность** web-панели администрирования IVA SBC, необходимо:

1 **Блокировка по IP при подборе пароля**: нажать **переключатель** для включения проверки и блокировки по IP-адресу. Если функция включена, то при работе защиты от подбора пароля будет заблокирован IP-адрес и логин пользователя. Если функция отключена, то будет заблокирован только логин пользователя

2 **Количество неудачных попыток входа в систему**: ввести разрешенное количество неудачных попыток входа в систему при включенной защите

3 **Период фиксации неудачных попыток входа в систему, мин**: ввести период времени в минутах, в течение которого фиксируются неудачные попытки входа в систему. Если за установленный период времени было превышено количество неудачных подряд попыток, то происходит блокировка входа в систему

4 **Время блокировки входа в систему, мин**: ввести период времени в минутах, в течение которого вход в систему будет заблокирован в случае превышения пользователем допустимого количества попыток входа

5 **Время жизни неактивной сессии, мин**: ввести период времени в минутах, по истечении которого система автоматически завершит неактивную сессию пользователя

> Обновление параметров, необходимых для графиков раздела **Мониторинг**, **не влияет** на время жизни пользовательской сессии

6 **Регулярное выражение проверки сложности пароля**: ввести регулярное выражение (RegExp), которое будет определять требования к сложности пароля. При пустом значении проверка сложности пароля выполняться не будет

7 нажать кнопку **Сохранить**

Управление пользователями

IVA SBC позволяет Администратору создавать, редактировать, блокировать и удалять учётные записи пользователей. Управление **учётными записями** пользователей выполняется в разделе **Пользователи** Рисунок 98.

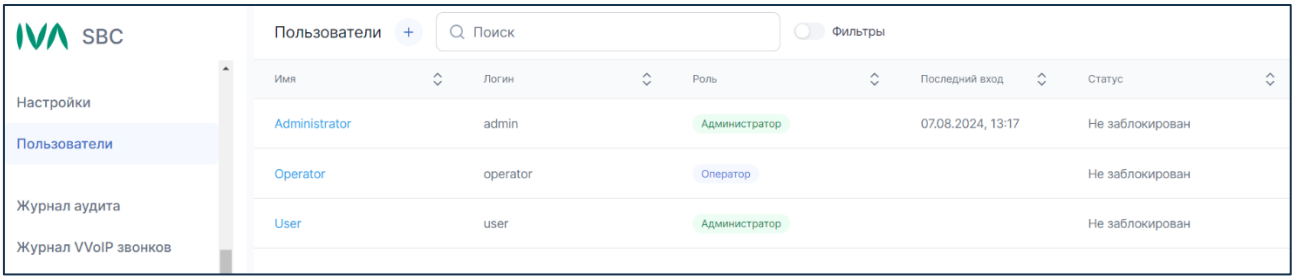

Рисунок 98. Список пользователей

Просмотр списка пользователей

В разделе **Пользователи** Администратор может настроить фильтр отображения списка пользователей. Чтобы настроить фильтр необходимо: нажать **переключатель Фильтры** Рисунок 99.

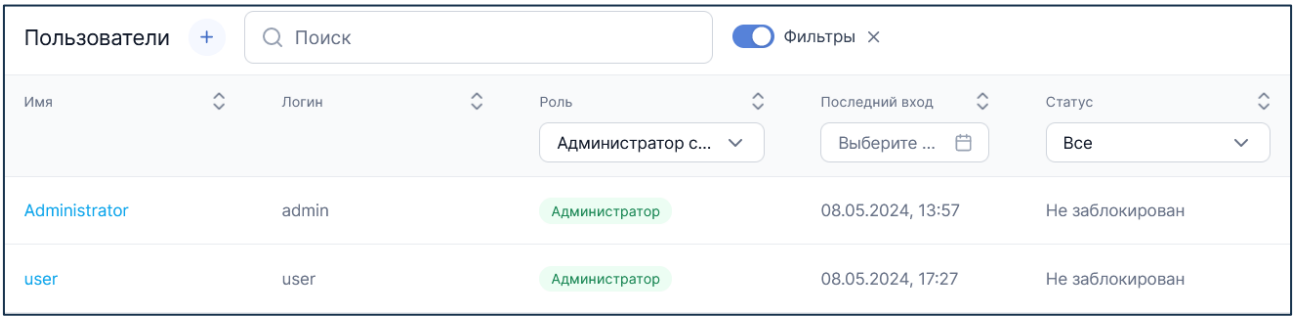

Рисунок 99. Фильтр пользователей

Права и роли пользователей

В IVA SBC существуют пользователи со следующими ролями:

- **Администратор системы** – обладает полным доступом к настройке системы IVA SBC и управлению пользователями (создание, редактирование, блокирование и удаление), журналам и графикам мониторинга
- **Оператор системы** – не может вносить изменения в настройки системы IVA SBC, имеет возможность просматривать настройки, журналы и графики мониторинга

Создание пользователей

Чтобы **создать пользователя**, необходимо:

1 перейти в раздел **Пользователи** Рисунок 98 и нажать кнопку +

2 в окне **Создание пользователя** Рисунок 100:

- **Имя**: ввести персонализированное имя пользователя (например **local admin**)
- **Логин**: ввести логин, который будет использоваться для авторизации в IVA SBC (например **user**)
- **Роль**: выбрать роль Администратор системы / Оператор системы
- **Пароль**: ввести пароль, удовлетворяющий заданным настройкам сложности пароля (по умолчанию: не менее 8 символов, включая как минимум одну цифру, одну строчную и одну прописную букву)
- **Подтверждение пароля**: ввести пароль повторно

3 нажать кнопку **Создать**

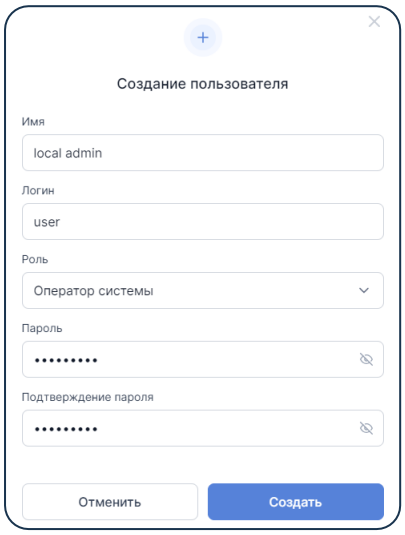

Рисунок 100. Создание пользователя

> Логин должен быть уникальным для каждого пользователя

Редактирование и удаление пользователей

Администратор может выполнить следующие действия с пользователями:

- редактировать информацию о пользователе
- заблокировать учётную запись пользователя
- изменить пароль учётной записи пользователя
- удалить учётную запись пользователя

Редактирование информации о пользователе

Чтобы редактировать информацию о пользователе, необходимо:

1 перейти в раздел **Пользователи** Рисунок 98

2 выбрать пользователя (например **user**) и нажать ссылку <**Имя пользователя**>

3 в окне **Информация о пользователе** Рисунок 101 нажать кнопку **Редактировать**

4 в окне **Редактирование пользователя** Рисунок 101:

- **Имя:** ввести новое имя пользователя
- **Логин:** ввести новый логин
- **Роль:** выбрать Администратор системы / Оператор системы
- **Статус**: выбрать Не заблокирован / Заблокирован

5 нажать кнопку **Сохранить**

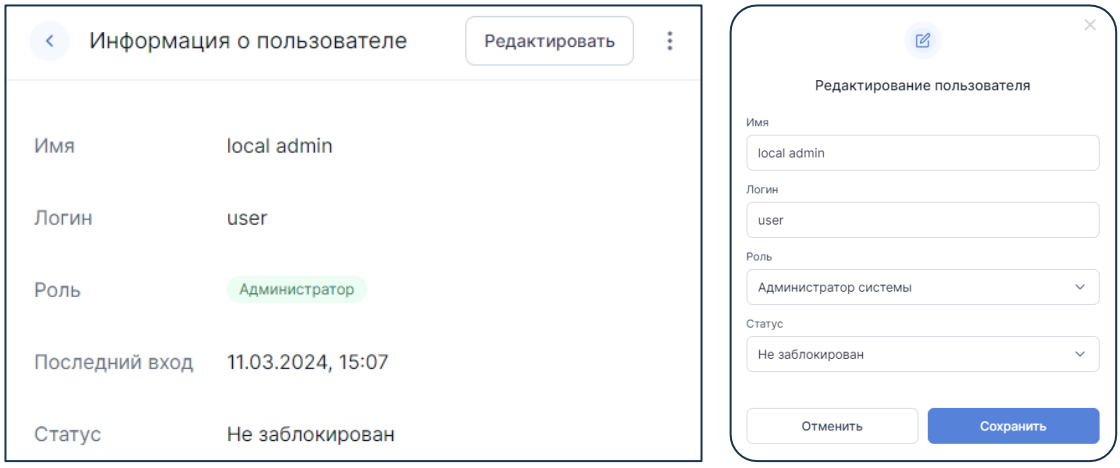

Рисунок 101. Информация и редактирование данных пользователя

Блокирование учётной записи пользователя

Заблокированный пользователь будет перемещен на страницу **Входа в систему** Рисунок 102 и не сможет выполнить авторизацию в IVA SBC.

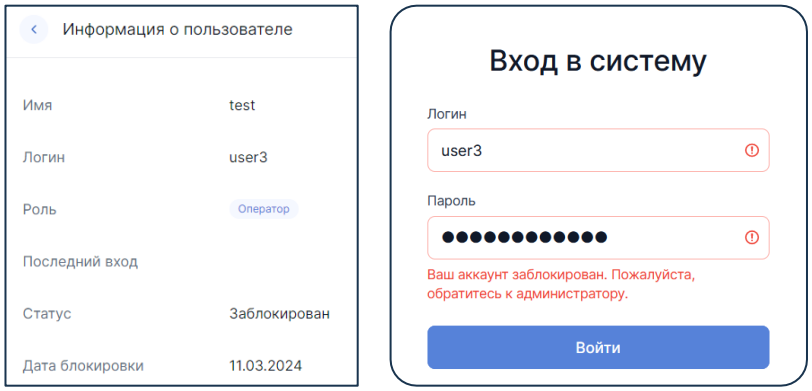

Рисунок 102. Заблокированная учётная запись

Чтобы **заблокировать** учётную запись пользователя, необходимо: **в окне** редактирование пользователя Рисунок 101 выбрать статус **Заблокирован.**

Администратор может также заблокировать пользователя с ролью Оператор через дополнительные действия в окне **Информация о пользователе** Рисунок 101: **нажать кнопку** ⋮ и выбрать **Заблокировать**.

Чтобы **разблокировать** учётную запись пользователя, необходимо: **в окне** редактирование пользователя Рисунок 101 выбрать статус **Не заблокирован**; или (для учётной записи Оператора) в окне **Информация о пользователе** Рисунок 101: **нажать кнопку** ⋮ и выбрать **Разблокировать**.

Изменение пароля учётной записи пользователя

Администратор может изменить пароль пользователям с ролью Оператор. Чтобы изменить пароль Оператору, необходимо:

1 перейти в раздел **Пользователи** Рисунок 98

2 выбрать пользователя с ролью **Оператор** и нажать ссылку <**Имя пользователя**>

3 в окне **Информация о пользователе** Рисунок 101 **нажать кнопку** ⋮ и выбрать **Изменить пароль**

4 в окне Изменение пароля пользователя <Имя пользователя> Рисунок 103:

- Пароль: ввести пароль, удовлетворяющий заданным настройкам сложности пароля (по умолчанию: не менее 8 символов, включая как минимум одну цифру, одну строчную и одну прописную букву)
- Подтверждение пароля: ввести пароль повторно

5 нажать кнопку Сохранить

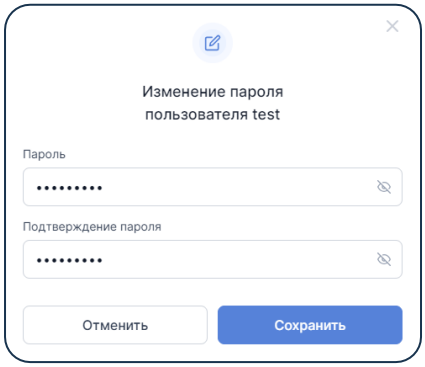

Рисунок 103. Изменение пароля пользователя

> Администратор не может изменить пароль другому Администратору

Удаление учётной записи пользователя

Администратор может удалить учётную запись пользователя с ролью Оператор. Чтобы удалить учётную запись Оператора, необходимо:

1 перейти в раздел Пользователи Рисунок 98

2 выбрать пользователя с ролью Оператор и нажать ссылку <Имя пользователя>

3 в окне Информация о пользователе Рисунок 101 нажать кнопку ⋮ и выбрать Удалить

4 в окне Удаление пользователя Рисунок 104 нажать кнопку Удалить

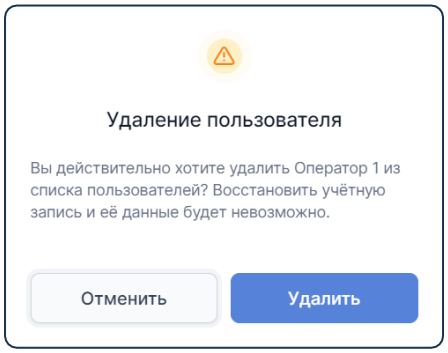

Рисунок 104. Удаление пользователя

Администратор не может удалить учётную запись с ролью Администратор. Чтобы удалить учётную запись с ролью **Администратор**, необходимо: изменить роль на Оператор, а затем удалить пользователя

Настройка собственного профиля пользователя

Профиль пользователя

Профиль пользователя Рисунок 105 позволяет:

- смотреть данные своего профиля
- выполнить настройку web-панели администрирования:
  - выбрать язык (**Русский** / **Английский**)
  - выбрать тему (**Светлая** / **Тёмная**)
- редактировать информацию о себе
- изменить собственный пароль

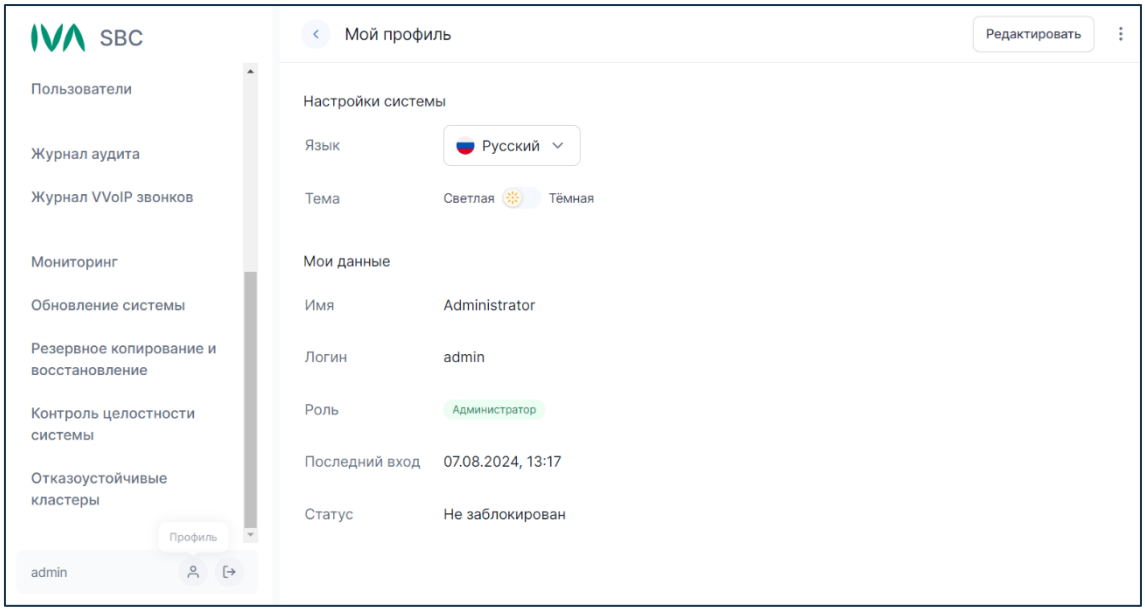

Рисунок 105. Профиль пользователя

Редактирование профиля пользователя

Чтобы **редактировать профиль пользователя**, необходимо:

1 в **Web-панели администрирования** нажать кнопку

2 в окне **Мой профиль** Рисунок 105 нажать кнопку **Редактировать**

3 в окне **Редактирование пользователя** Рисунок 106 внести изменения

4 нажать кнопку **Сохранить**

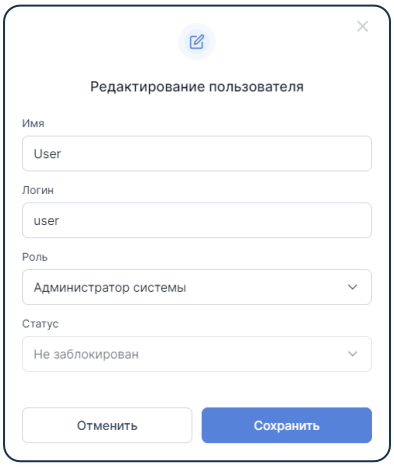

Рисунок 106. Редактирование пользователя

Изменение собственного пароля пользователя

Чтобы **изменить пароль пользователя**, необходимо:

1 в **Web-панели администрирования нажать кнопку**

2 в окне **Мой профиль** Рисунок 105 **нажать кнопку** и выбрать **Изменить пароль**

3 в окне **Изменение пароля** Рисунок 107 внести изменения

4 нажать кнопку **Сохранить**

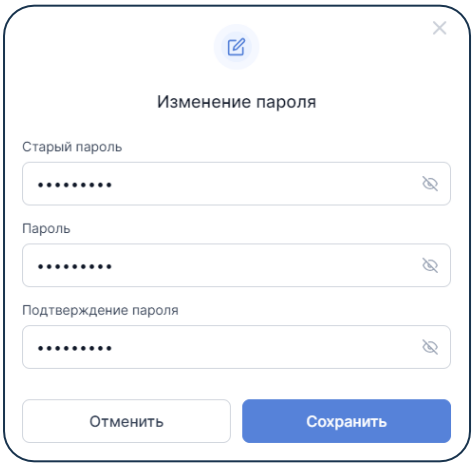

Рисунок 107. Изменение пароля пользователя

Аудит в IVA SBC

IVA SBC предоставляет возможность пользователям:

- отслеживать все изменения, происходящие в IVA SBC – Журнал аудита
- просматривать все совершённые через IVA SBC VVoIP-звонки – Журнал VVoIP звонков

> Информацию о логах, создаваемых системой IVA SBC, можно найти в приложении Логи системы

Журнал аудита

В IVA SBC отслеживаются все происходящие изменения:

- вход / выход пользователей
- изменение параметров и настроек пользователей
- изменение параметров и настроек системы
- возникающие ошибки и пр.

Чтобы смотреть все хранящиеся в системе записи, необходимо: Перейти в раздел Журнал аудита Рисунок 108

Чтобы обновить список журнала аудита, необходимо: нажать кнопку Рисунок 108

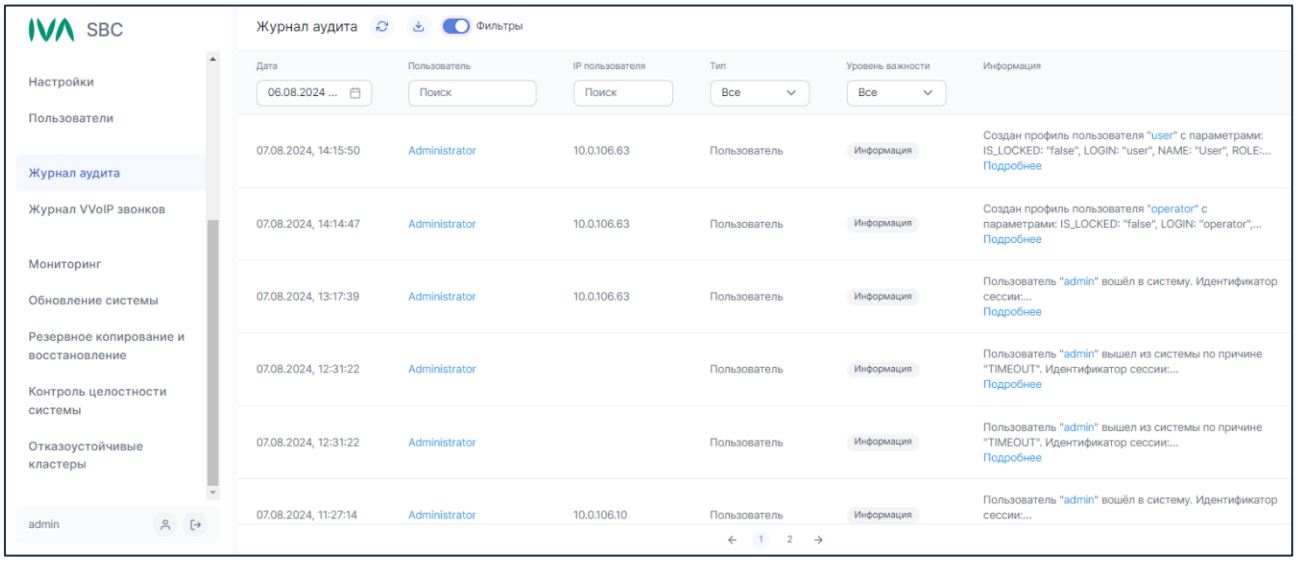

Рисунок 108. Раздел Журнал аудита

Пользователь может экспортировать журнал аудита, для чего необходимо:

1 перейти в раздел **Журнал аудита** Рисунок 108 и **нажать кнопку**

2 в окне **Экспорт журнала аудита** Рисунок 109 нажать кнопку **Экспортировать**

3 в окне **Сохранение** выбрать место сохранения и нажать кнопку **Сохранить**

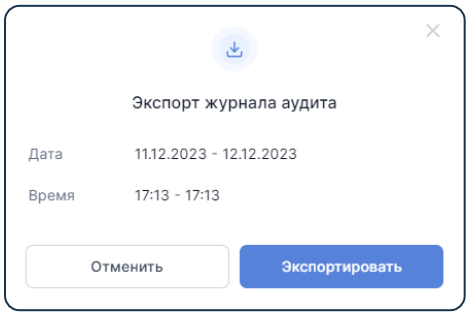

Рисунок 109. Экспорт журнала аудита

Просмотр логируемых событий

В разделе **Журнал аудита** можно настроить фильтр отображения логируемых событий Рисунок 110. Чтобы настроить фильтр отображения логируемых событий, необходимо: нажать **переключатель Фильтры** Рисунок 110.

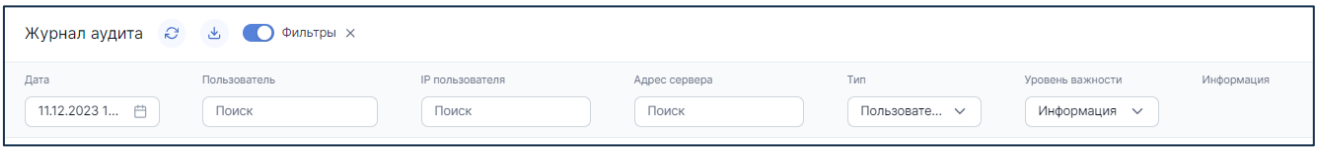

Рисунок 110. Фильтры журнала аудита

Журнал VoIP-звонков

В IVA SBC ведётся журнал VoIP-звонков, в котором отображаются все совершённые через IVA SBC VoIP-звонки, а также детальная информация о каждом звонке и связанное с ним правило обработки.

Чтобы смотреть все совершённые VoIP-звонки, необходимо: перейти в раздел **Журнал VoIP звонков** Рисунок 111

Чтобы обновить список журнала VoIP-звонков, необходимо: **нажать кнопку** Рисунок 111

Чтобы смотреть детальную информацию о звонке, необходимо: **выбрать звонок** Рисунок 111 **и нажать кнопку**

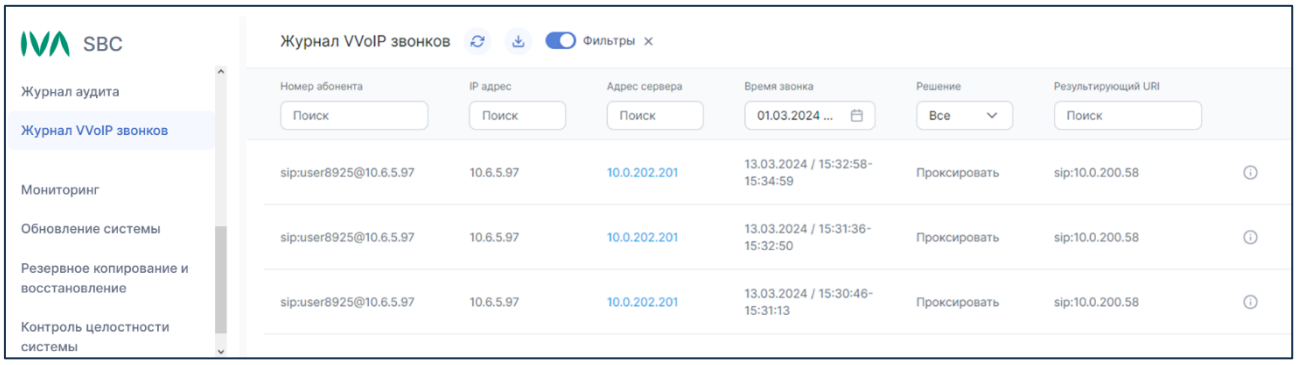

Рисунок 111. Раздел Журнал VoIP звонков

Пользователь может экспортировать журнал VoIP-звонков, для чего необходимо:

1 перейти в раздел **Журнал VoIP-звонков** Рисунок 111 и **нажать кнопку**

2 в окне **Экспорт журнала VoIP звонков** Рисунок 112 нажать кнопку **Экспортировать**

3 в окне **Сохранение** выбрать место сохранения и нажать кнопку **Сохранить**

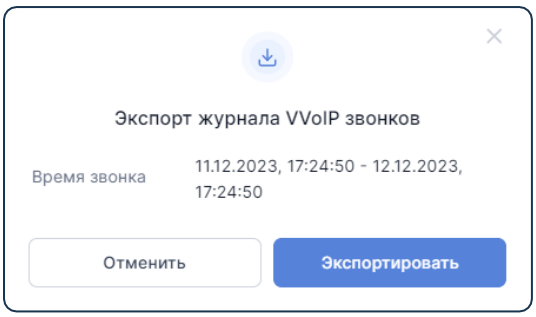

Рисунок 112. Экспорт журнала аудита

Фильтр отображения журнала звонков

В разделе **Журнал VVoIP звонков** можно настроить фильтр отображения звонков Рисунок 113. Чтобы настроить фильтр отображения, необходимо: нажать переключатель Фильтры Рисунок 113.

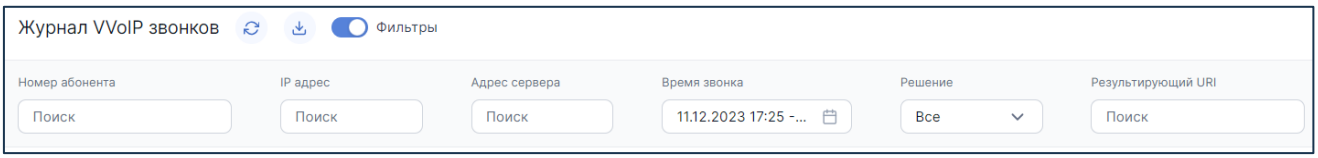

Рисунок 113. Фильтры журнала VVoIP звонков

Мониторинг

Статистика использования системы

IVA SBC предоставляет пользователям графический отчёт (dashboard), который выдаёт статистику использования системы в удобной для восприятия форме и позволяет оценить нагрузку на оборудование.

Чтобы провести мониторинг производительности IVA SBC необходимо:

1 перейти в раздел **Мониторинг** Рисунок 114

2 выбрать **сервер IVA SBC** (например, сервер проксирования с IP-адресом **10.0.202.202** или сервер управления и конфигурации с IP-адресом **10.0.202.203**)

3 выбрать **период вывода статистики**

4 выбрать **значение вывода графика** (отображает **Максимальное** / **Среднее** / **Минимальное** значение кривой графика в выбранный промежуток времени)

5 перейти на необходимую вкладку (Система, Сеть, Диск, Модули, Среда исполнения, HTTP, VVoIP, Внутренности, TURN сервер) и выбрать график

> Вкладки **HTTP**, **VVoIP**, и **TURN сервер** не отображаются для сервера управления и конфигурации

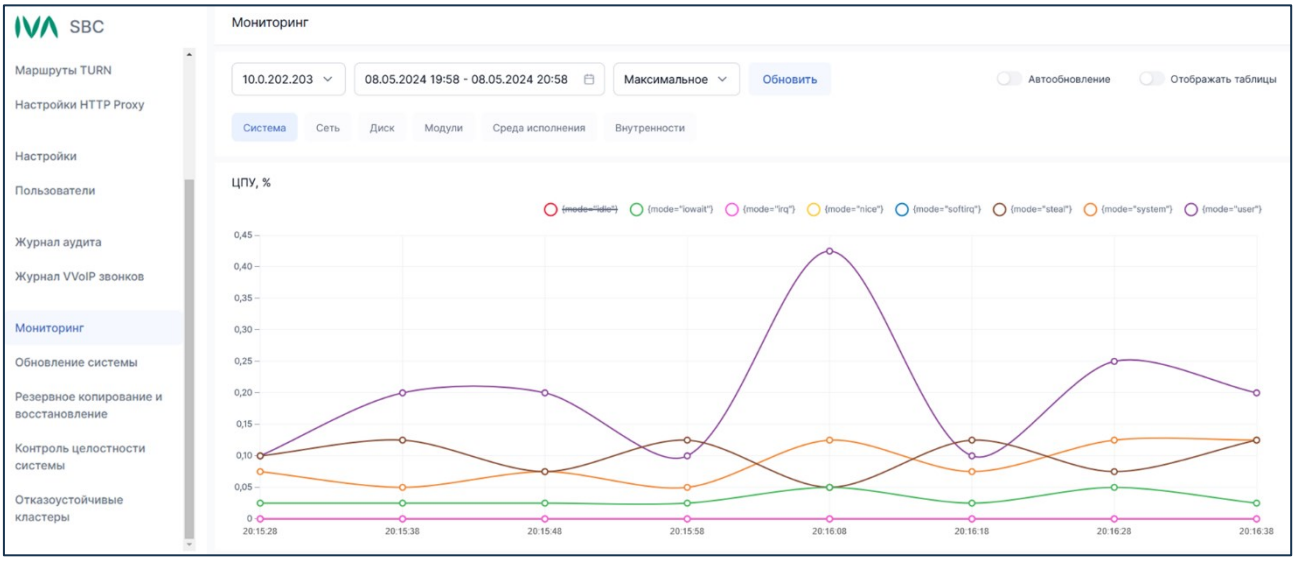

Рисунок 114. Мониторинг IVA SBC

При необходимости можно:

- отключить отображение определенного графика: выбрать и нажать на название графика в списке отображаемых графиков Рисунок 114 (например {mode = “idle”})
- включить автообновление графиков: нажать переключатель Автообновление Рисунок 114
- включить отображение таблиц с минимальными / средними / максимальными / последними показателями графика: нажать переключатель Отображать таблицы Рисунок 114

Используемые метрики Мониторинга IVA SBC

> **Графики, отображаемые кривые, вкладки и их содержание могут отличаться** в зависимости от выбранного сервера, **модулей серверной части** и запущенных служб

Вкладка Система

На вкладке **Система** для сервера проксирования и сервера управления и конфигурации отображаются следующие графики:

1 график **ЦПУ, %** Рисунок 115 показывает загрузку процессора в реальном времени на следующих кривых:

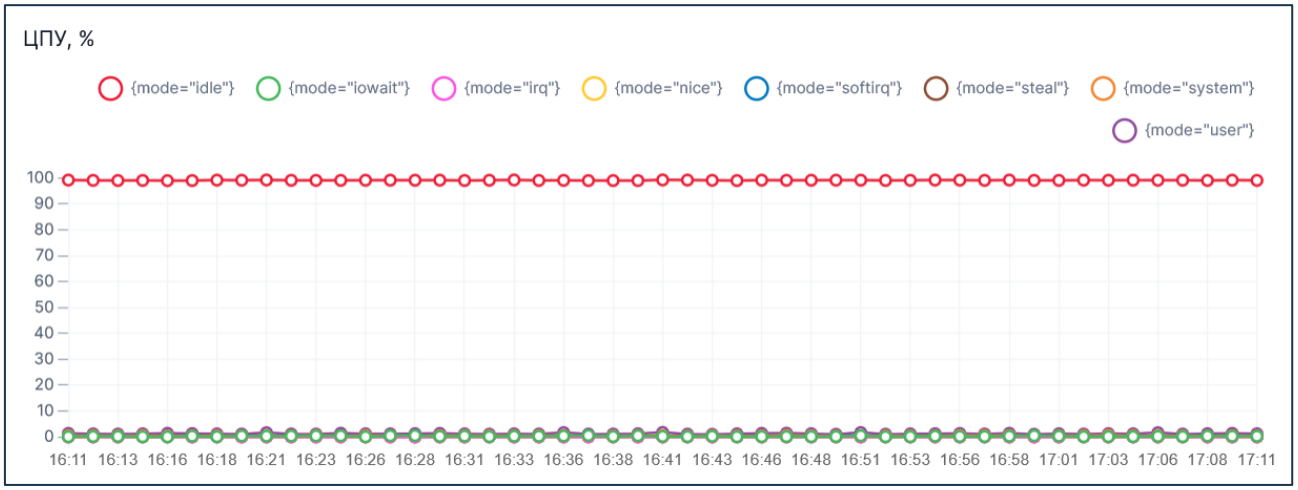

Рисунок 115. График ЦПУ, %

- кривая **{mode="idle"}** – отображает процент времени, в течение которого ЦПУ находится в состоянии ожидания, не выполняя никаких задач

- кривая {mode="iowait"} – отображает процент времени, в течение которого ЦПУ ожидает завершения операций ввода-вывода
- кривая {mode=" irq "} – отображает процент времени, в течение которого ЦПУ занимается обработкой прерываний от оборудования
- кривая {mode="nice"} – отображает процент времени, в течение которого ЦПУ занимается выполнением пользовательских задач с увеличенным приоритетом (nice)
- кривая {mode="softirq"} – отображает процент времени, в течение которого ЦПУ обрабатывает программные прерывания (softirq)
- кривая {mode="steal"} – отображает процент времени, в течение которого виртуальная машина не получает ресурсы процессора для своего выполнения
- кривая {mode="system"} – отображает процент времени, в течение которого ЦПУ занимается выполнением системных задач
- кривая {mode="user"} – отображает процент времени, в течение которого ЦПУ занимается выполнением пользовательских задач

При **корректной работе системы** значения кривой {mode="idle"} должны находиться **в диапазоне от 10 до 100 %**.
Аварийными считаются значения кривой {mode="idle"} **менее 10 %** на протяжении 2 минут, при этом возможно система перегружена, и необходимо определить источник возникновения данной проблемы

Для остальных кривых **корректная работа системы** обеспечивается, если значения находятся в диапазоне от 0 до 80 %, при этом превышения значений выше 80 % может привести к нестабильной работе системы

2 график **Средняя загрузка** Рисунок 116 показывает среднюю загрузку процессора в реальном времени на следующих кривых:

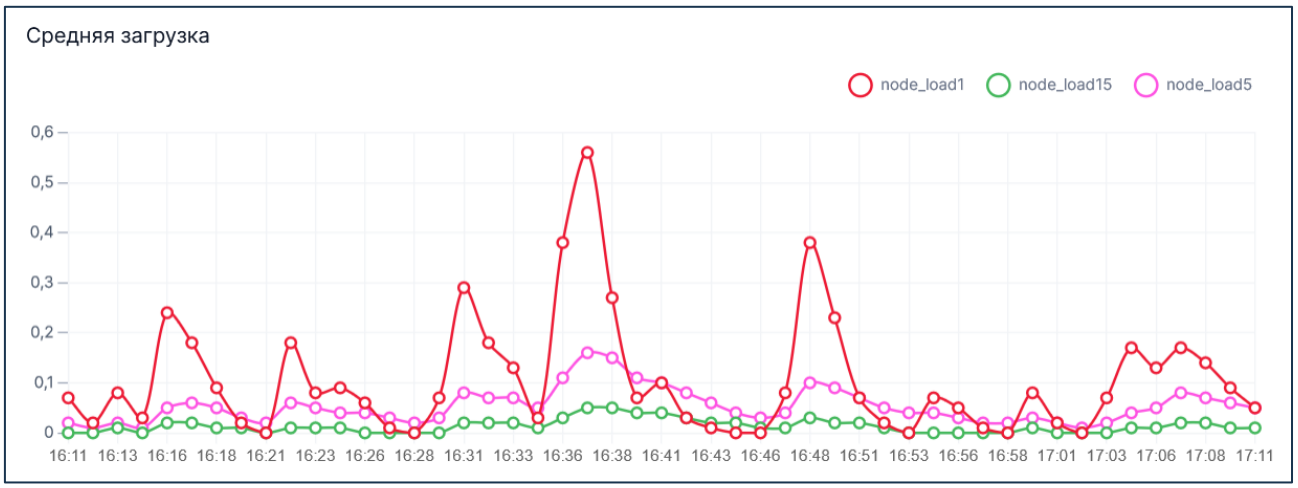

Рисунок 116. График Средняя загрузка

- кривая **node_load1** – отображает среднюю загрузку системы за 1 минуту
- кривая **node_load5** – отображает среднюю загрузку системы за 5 минут
- кривая **node_load15**– отображает среднюю загрузку системы за 15 минут

При **корректной работе системы** значения кривых должны находиться в диапазоне от **0** до **n**, где **n** – общее количество ядер процессора

Превышение значения n более чем на 70 %, означает что на процессор идёт **повышенная нагрузка**, которая может привести к медленному отклику процесса, что повлияет на нормальную работу системы

3 график **Память, ГБ** Рисунок 117 показывает информацию об использованной и неиспользованной памяти в реальном времени на следующих кривых:

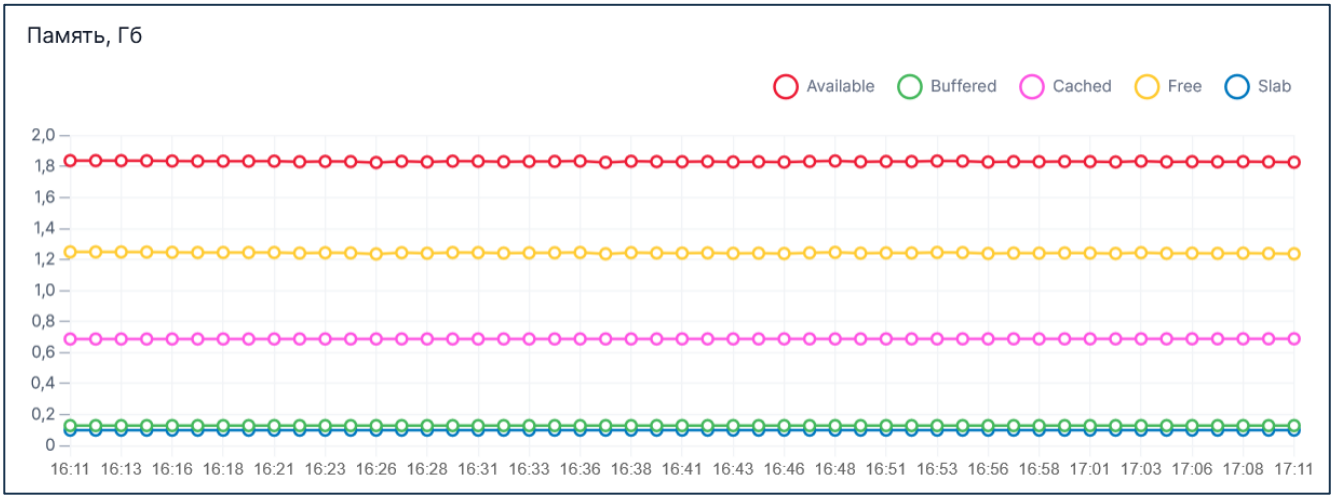

Рисунок 117. График Память, ГБ

- кривая **Avaible** – отображает объём памяти, который доступен для выделения новому или существующему процессу
- кривая **Buffered** – отображает объём памяти, зарезервированный системой для выделения её процессам, когда им это потребуется
- кривая **Cached** – отображает объём данных, которые недавно были использованы системой / процессами и временно сохранены для быстрого доступа в случае их повторного использования
- кривая **Free** – отображает объём свободной памяти, которая в данный момент не используется
- кривая **Slab** – отображает объём памяти, за счёт которого кэш (Cached) может увеличиваться или уменьшаться

При **корректной работе системы** значения кривых не должны превышать объём доступной памяти

Если **значения кривых близки к максимальным** (с учетом файла подкачки), то система может не иметь достаточного места для хранения временных файлов, кэша и других данных, что может **привести к их потере**

4 график Временные файловые системы, ГБ Рисунок 118 показывает информацию об использованной и неиспользованной памяти для хранения временных файлов в реальном времени на следующих кривых:

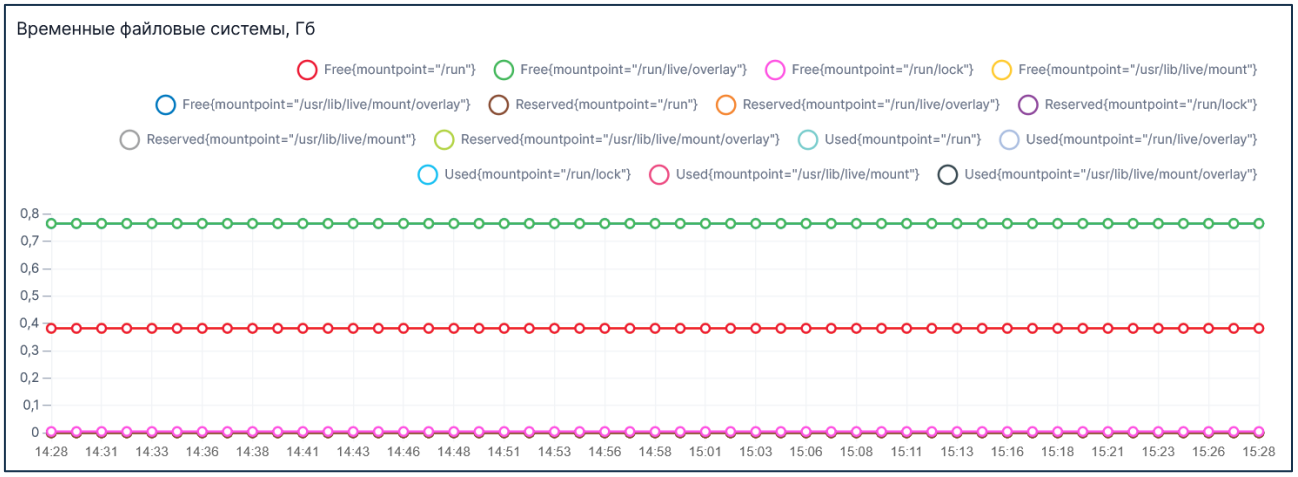

Рисунок 118. График Временные файловые системы, ГБ

- кривая Free{mountpoint="/run"} – отображает общий объём свободной памяти
- кривая Free{mountpoint="/run/live/overlay"} – отображает объём свободной памяти для временных изменений и кэширования файлов Live-системы
- кривая Free{mountpoint="/run/lock} – отображает свободную память для файлов блокировки, используемых для предотвращения одновременного доступа к ресурсам между несколькими процессами
- кривая Free{mountpoint="/run/user/1000”} – отображает свободную память для временных файлов пользователя
- кривая Free{mountpoint="/usr/lib/live/mount"} – отображает объём свободной памяти для временного монтирования Live-образов файловой системы
- кривая Free{mountpoint="/usr/lib/live/mount/overlay"} – отображает объём свободной памяти для записи временных изменений и кэширования файлов во время работы Live-системы
- кривая Reserved{mountpoint="/run"} – отображает общий объём зарезервированной памяти
- кривая Reserved{mountpoint="/run/live/overlay"} – отображает зарезервированную память для временных изменений и кэширования файлов для Live-системы

- кривая Reserved{mountpoint="/run/lock} – отображает зарезервированную память для файлов блокировки, используемых для предотвращения одновременного доступа к ресурсам между несколькими процессами
- кривая Reserved{mountpoint="/run/user/1000”} – отображает зарезервированную память для временных файлов пользователя
- кривая Reserved{mountpoint="/usr/lib/live/mount"} – отображает зарезервированную память для временного монтирования Live-образов файловой системы
- кривая Reserved{mountpoint="/usr/lib/live/mount/overlay"} – отображает зарезервированную память для записи временных изменений и кэширования файлов во время работы Live-системы
- кривая Used{mountpoint="/run"} – отображает общий объём используемой памяти
- кривая Used{mountpoint="/run/live/overlay"} – отображает используемую память для временных изменений и кэширования файлов для Live-системы
- кривая Used{mountpoint="/run/lock} – отображает используемую память для файлов блокировки, используемых для предотвращения одновременного доступа к ресурсам между несколькими процессами
- кривая Used {mountpoint="/run/user/1000”} – отображает используемую память для временных файлов пользователя
- кривая Used{mountpoint="/usr/lib/live/mount"} – отображает используемую память для временного монтирования образов файловой системы
- кривая Used{mountpoint="/usr/lib/live/mount/overlay"} – отображает используемую память для записи временных изменений и кэширования файлов во время работы Live-системы

> При **корректной работе системы** значения кривых не должны превышать объём доступной памяти

Если **значения кривых близки к максимальным** (с учетом файла подкачки), то система может не иметь достаточного места для хранения временных файлов, кэша и других данных, что может **привести к их потере**

5 график **Переключения контекста/с** Рисунок 119 показывает количество переключений в секунду между контекстом **userspace** и **systemspace** в реальном времени на кривой **Context switches**

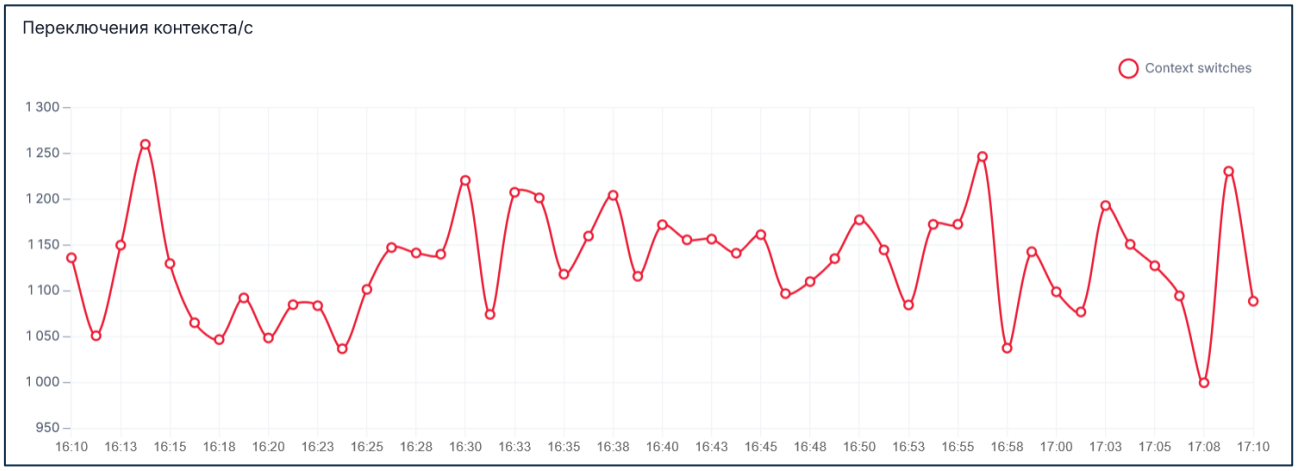

Рисунок 119. График Переключения контекста/с

График **Переключения контекста** используется для комплексной оценки работы системы. Данный график **необходимо анализировать совместно с другими метриками** (например, с показателем **загрузки системы**)

Резкий рост количества переключений может свидетельствовать о возможных **проблемах в системе**

6 график **Время работы, часы** Рисунок 120 показывает количество времени беспрерывной работы системы в реальном времени на кривой **Uptime**

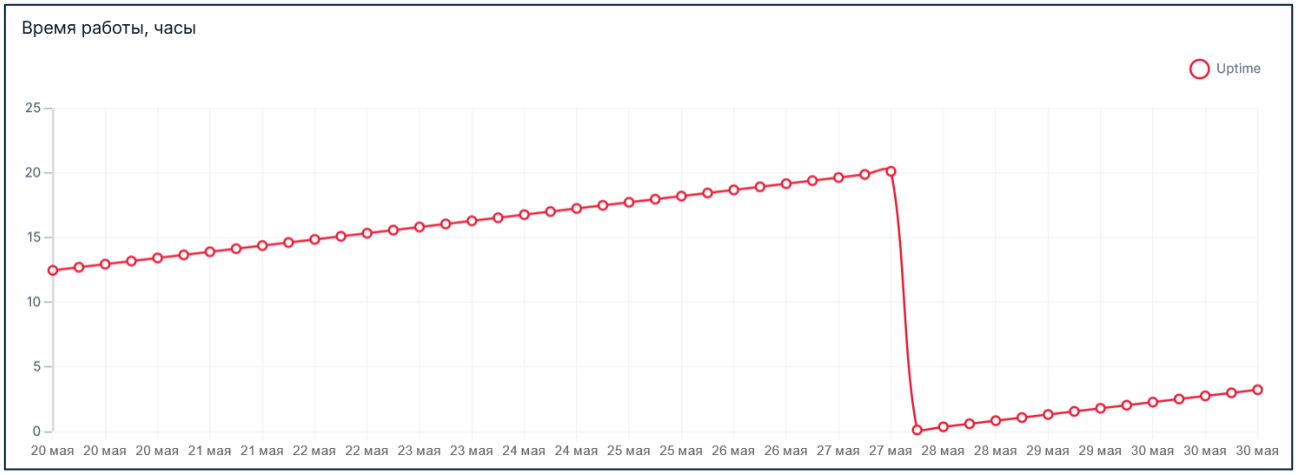

Рисунок 120. График Время работы, часы

> График носит информационный характер и не предназначен для оценки работы системы

Вкладка Сеть

На вкладке **Сеть** для сервера проксирования и сервера управления и конфигурации отображаются следующие графики:

1 график **Трафик, мбит/с** Рисунок 121 показывает загрузку сетевых каналов в реальном времени на следующих кривых:

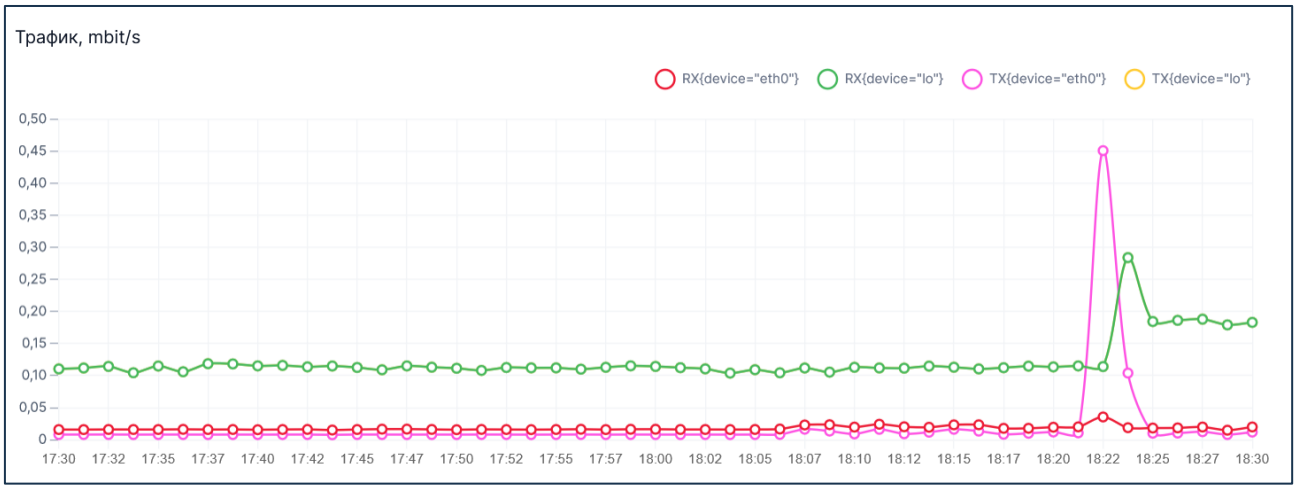

Рисунок 121. График Трафик, мбит/с

- кривая RX{device="eth0"} – отображает загрузку сетевого канала приёма через интерфейс eth0
- кривая RX{device="lo"} – отображает загрузку сетевого канала приёма через интерфейс loopback
- кривая TX{device="eth0"} – отображает загрузку сетевого канала передачи через интерфейс eth0
- кривая TX{device="lo"} – отображает загрузку сетевого канала передачи через интерфейс loopback

> Значения на графике **должны отображать ожидаемую среднюю нагрузку системы** (в соответствии с опытом эксплуатации)

2 график **Ошибки** Рисунок 122 показывает количество возникших ошибок в реальном времени на следующих кривых:

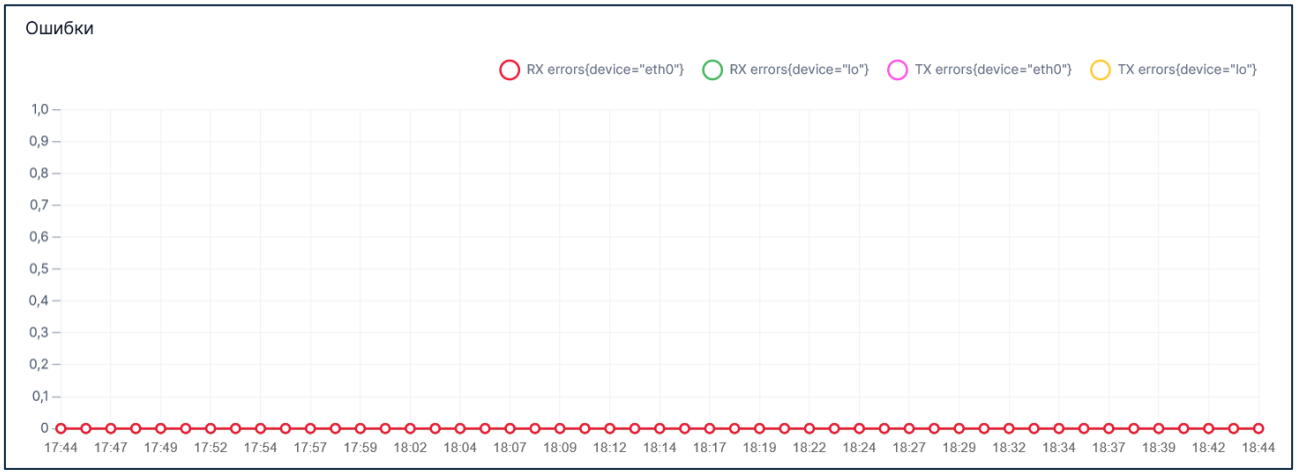

Рисунок 122. График Ошибки

- кривая RX errors{device="eth0"} – отображает количество ошибок по сетевому каналу приёма через интерфейс eth0
- кривая RX errors{device="lo"} – отображает количество ошибок по сетевому каналу приёма через интерфейс loopback
- кривая TX errors{device="eth0"} – отображает количество ошибок по сетевому каналу передачи через интерфейс eth0
- кривая TX errors{device="lo"} – отображает количество ошибок по сетевому каналу передачи через интерфейс loopback

При **корректной работе системы** количество ошибок **не должно быстро расти**. Если происходят частые ошибки, это может быть связано с перегрузкой оборудования или каналов.
Данный график **необходимо анализировать в сочетании с другими метриками** (например, с **анализом объема трафика сети** и **нагрузки на систему**)

3 график **Пакеты** Рисунок 123 показывает количество пакетов на прием / передачу в реальном времени на следующих кривых:

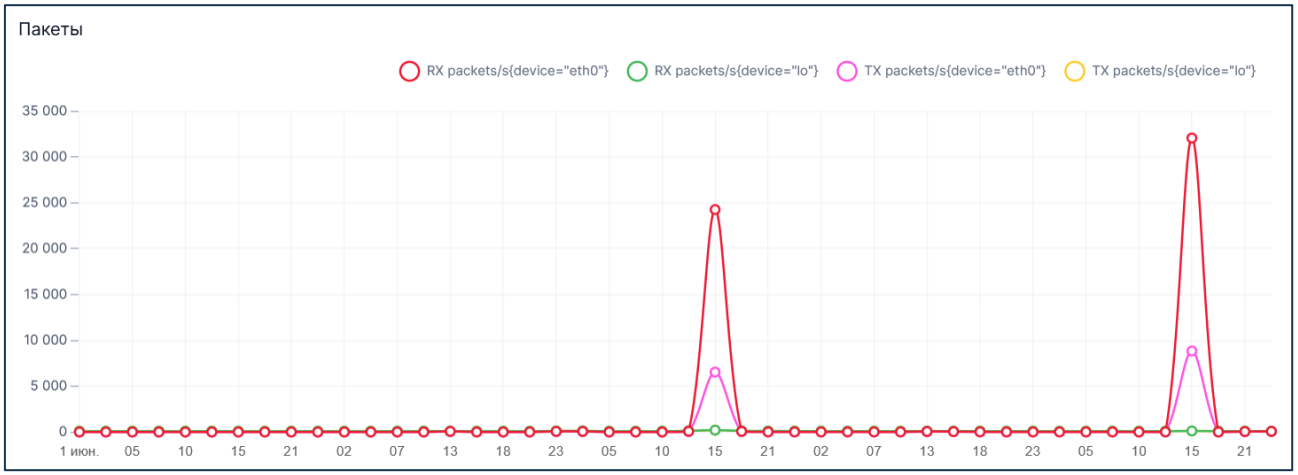

Рисунок 123. График Пакеты

- кривая **RX packets/s{device="eth0"}** – отображает количество принятых пакетов по сетевому каналу через интерфейс eth0
- кривая **RX packets/s{device="lo"}** – отображает количество принятых пакетов по сетевому каналу через интерфейс loopback
- кривая **TX packets/s{device="eth0"}** – отображает количество переданных пакетов по сетевому каналу через интерфейс eth0
- кривая **TX packets/s{device="lo"}** – отображает количество переданных пакетов по сетевому каналу через интерфейс loopback

График **Пакеты** используется для комплексного анализа исходящего / входящего трафика в системе

4 график **Размеры UDP очередей, Кб** Рисунок 124 показывает размер UDP-очередей в реальном времени на следующих кривых:

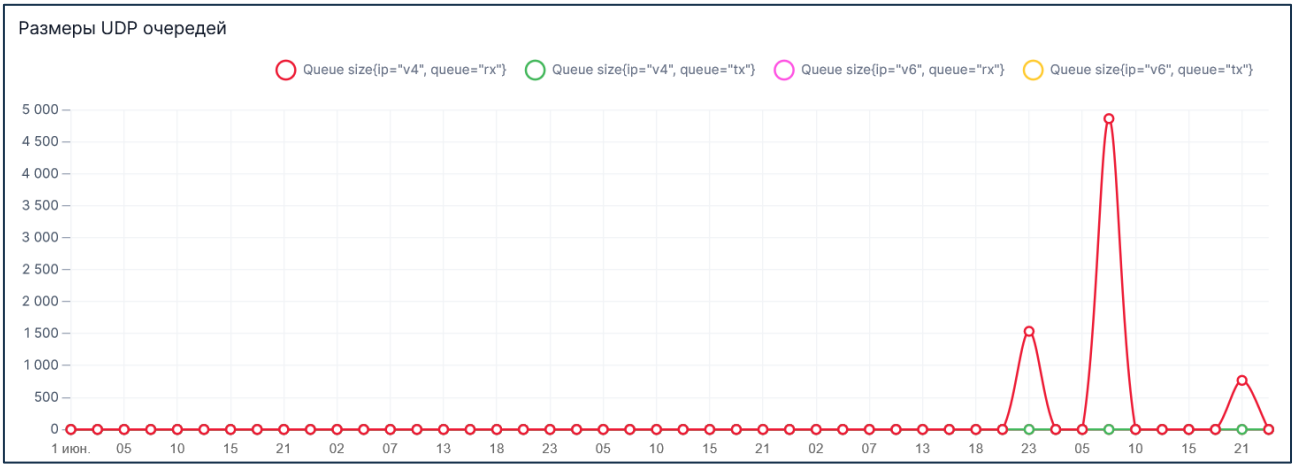

Рисунок 124. График Размеры UDP очередей, Кб

- кривая **Queue size{ip="v4", queue="rx"}** – отображает размер UDP-очередей по протоколу IPv4 при приёме
- кривая **Queue size{ip="v4", queue="tx"}** – отображает размер UDP-очередей по протоколу IPv4 при передаче
- кривая **Queue size{ip="v6", queue="rx"}** – отображает размер UDP-очередей по протоколу IPv6 при приёме
- кривая **Queue size{ip="v6", queue="tx"}** – отображает размер UDP-очередей по протоколу IPv6 при передаче

> При **корректной работе системы** размеры UDP-очередей **не должны превышать среднюю нагрузку системы**. Резкий рост очереди означает, что система не успевает отправлять пакеты в сеть, и они копятся в сетевом интерфейсе, что приводит к задержке отправки данных в сеть

5 график **Задержки сетевых вызовов, мс** Рисунок 125 показывает время задержки вызова между серверами системы в реальном времени на кривых **<IP-адрес добавленного сервера>**

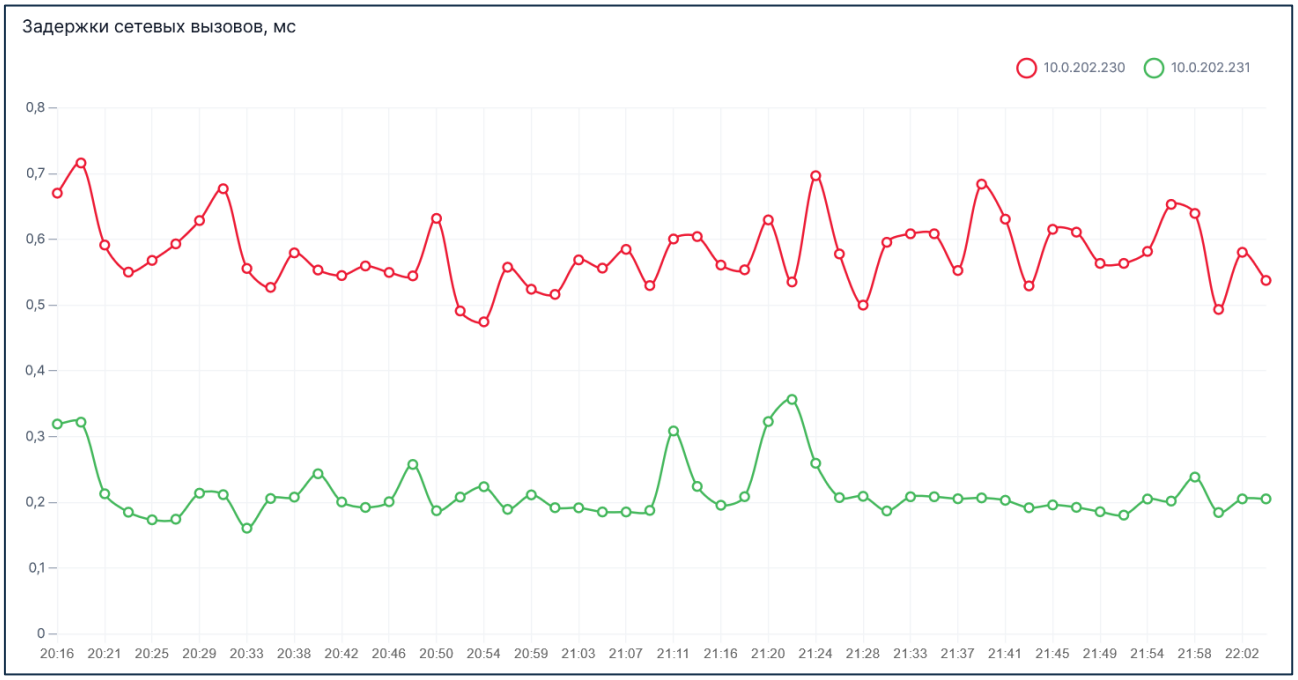

Рисунок 125. График Задержки сетевых вызовов, мс

> При **корректной работе системы** задержка сетевых вызовов между различными серверами не должна превышать 20 мс

6 график **Таймауты сетевых вызовов** Рисунок 126 показывает количество таймаутов, возникающих при сетевых вызовах в реальном времени на кривых **<IP-адрес добавленного сервера>**

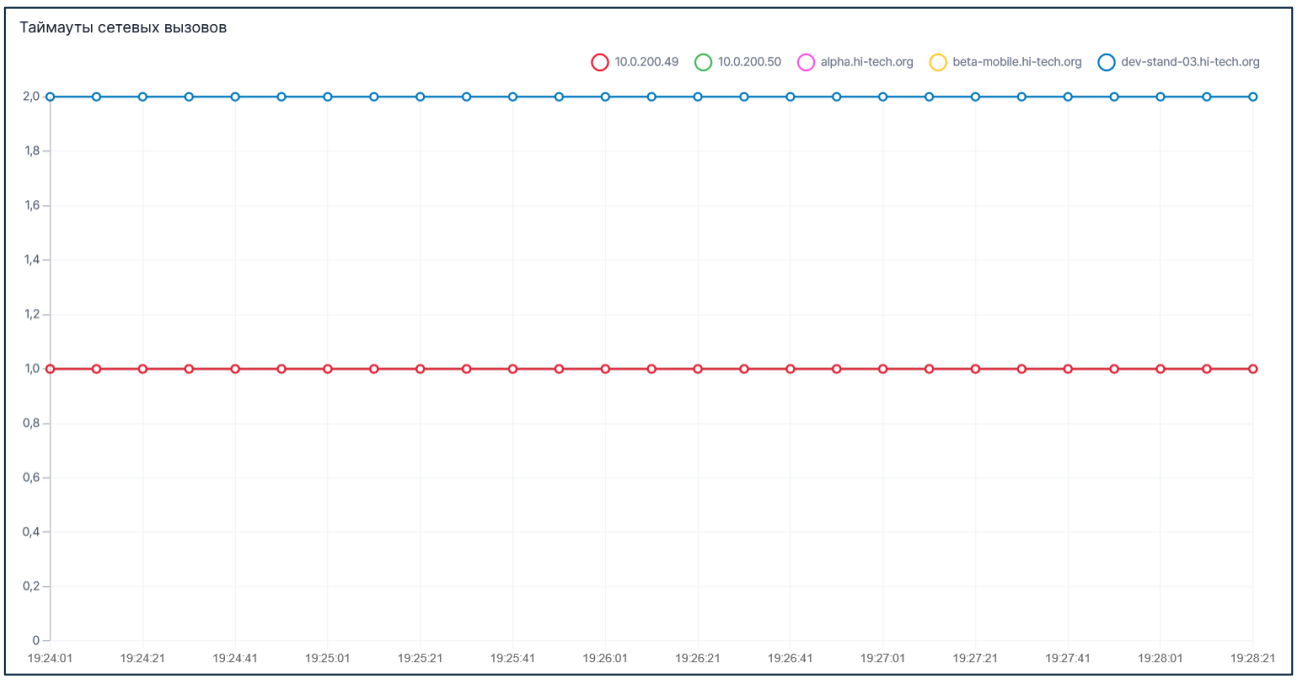

Рисунок 126. График Таймауты сетевых вызовов

При **корректной работе системы** значение времени таймаутов сетевых вызовов должно быть минимальным

7 график **Расширенные метрики TCP** Рисунок 127 показывает расширенные метрики TCP-соединений в реальном времени на следующих кривых:

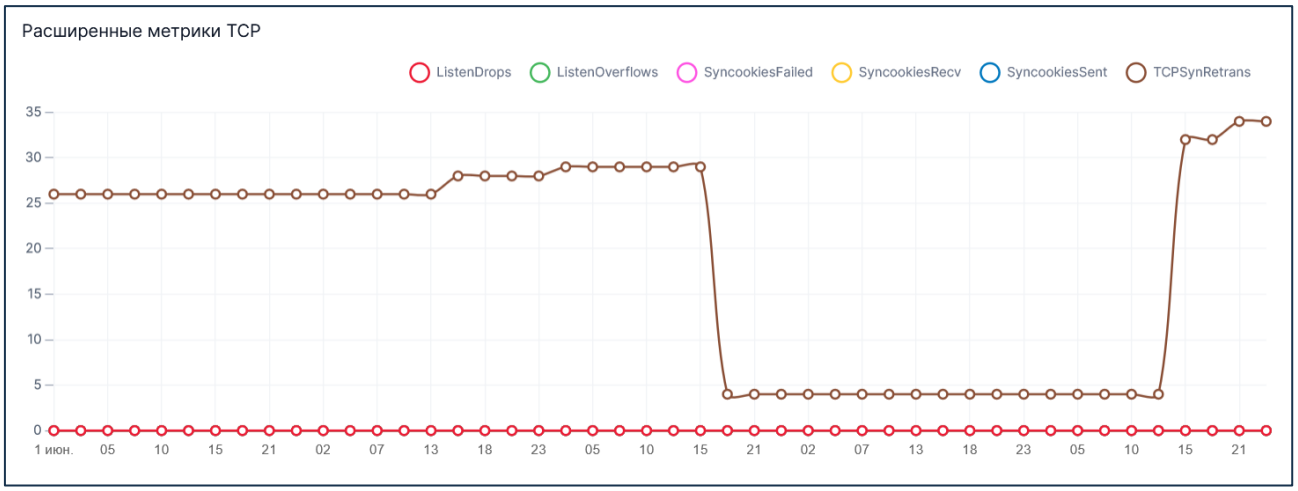

Рисунок 127. График Расширенные метрики TCP

- кривая **ListenDrops** – отображает количество входящих соединений (пакетов SYN), прерванных по какой-либо причине
- кривая **Listenoverflows** – отображает число случаев превышения верхнего предела очереди прослушивания
- кривая **SyncookiesFailed** – отображает количество полученных пакетов с неверной информацией SYN Cookie
- кривая **SyncookiesRecv** – отображает количество пакетов SYN / ACK, полученных через SYN Cookie
- кривая **SyncookiesSent** – отображает количество пакетов SYN / ACK, отправленных через SYN Cookie
- кривая **TCPSynRetrans** – отображает количество повторных соединений (пакетов SYN)

При **корректной работе системы** расширенные метрики TCP-соединений должны иметь минимальные значения. Увеличение значений с образованием пиков на графике может свидетельствовать о проблемах с сетью

Вкладка Диск

На вкладке **Диск** для сервера проксирования и сервера управления и конфигурации отображаются следующие графики:

1 график **/, ГБ** Рисунок 128 показывает информацию об использованной и неиспользованной памяти для хранения системных файлов в реальном времени на следующих кривых:

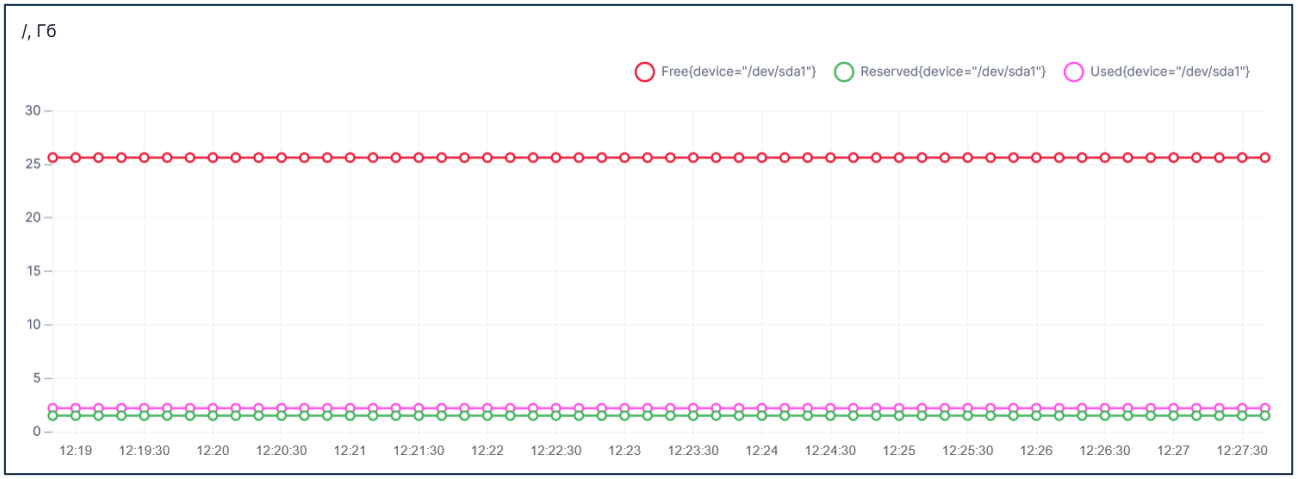

Рисунок 128. График /, ГБ

- кривая **Free{device="/dev/sda1"}** – отображает информацию о свободном объёме памяти физического диска
- кривая **Reserved{device="/dev/sda1"}** – отображает информацию о зарезервированном объёме памяти физического диска
- кривая **Used{device="/dev/sda1"}** – отображает информацию об используемом объёме памяти физического диска

> Для **корректной работы системы** необходимо, чтобы доступное свободное пространство составляло не менее 2 ГБ

2 график **Число операций слияния в секунду** Рисунок 129 показывает число объединённых операций в секунду в реальном времени на следующих кривых:

Рисунок 129. График Число операций слияния в секунду

- кривая **Reads merged{device="sda"}** – отображает число объединённых операций чтения в секунду на физическом диске
- кривая **Reads merged{device="sr0"}** – отображает число объединённых операций чтения в секунду на логическом диске
- кривая **Writes merged{device="sda"}** – отображает число объединённых операций записи в секунду на физическом диске
- кривая **Writes merged{device="sr0"}** – отображает число объединённых операций записи в секунду на логическом диске

> График **Число операций слияния в секунду** используется для комплексной оценки работы системы.
> Возрастание нагрузки обычно связано с записью данных логов на диск

3 график **Операции ввода/вывода, МБ/с** Рисунок 130 показывает объём операций ввода / вывода в реальном времени на следующих кривых:

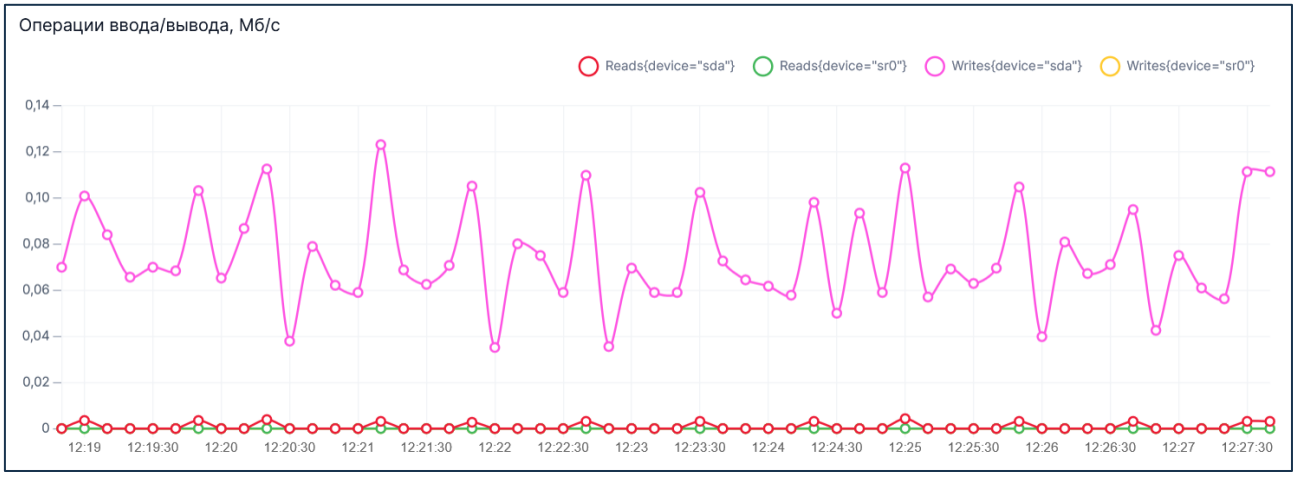

Рисунок 130. График Операции ввода/вывода, МБ/с

- кривая **Reads{device="sda"}** – отображает объём операций чтения на физическом диске
- кривая **Reads{device="sr0"}** – отображает объём операций чтения на логическом диске
- кривая **Writes{device="sda"}** – отображает объём операций записи на физическом диске
- кривая **Writes{device="sr0"}** – отображает объём операций записи на логическом диске

> График **Операции ввода / вывода** используется для комплексной оценки работы системы.
> Возрастание нагрузки обычно связано с записью данных логов на диск

4 график **Число дисковых операций в секунду** Рисунок 131 показывает число дисковых операций в секунду в реальном времени на следующих кривых:

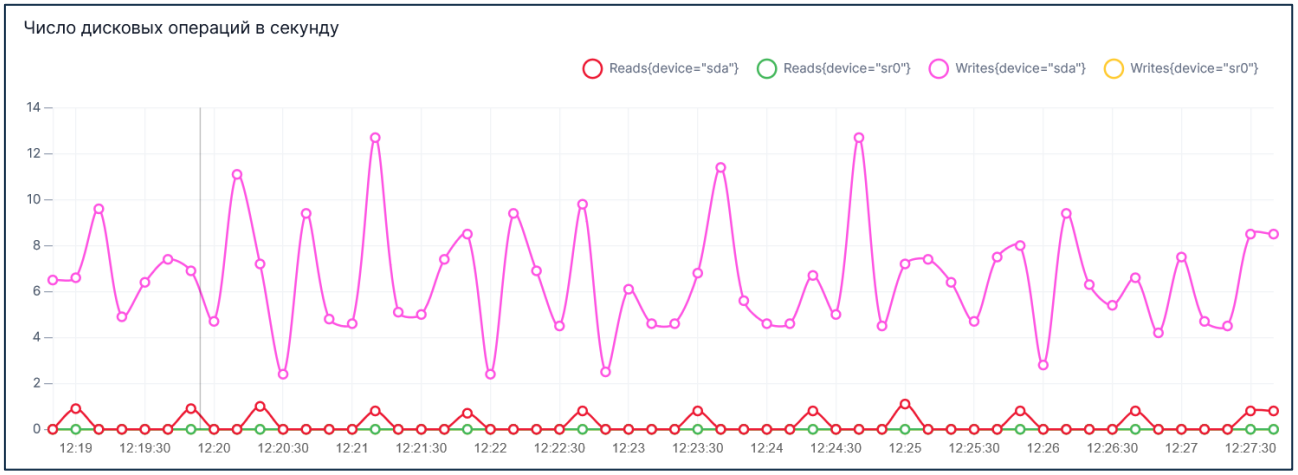

Рисунок 131. График Число дисковых операций в секунду

- кривая **Reads{device="sda"}** – отображает число дисковых операций записи на физическом диске
- кривая **Reads{device="sr0"}** – отображает число дисковых операций записи на логическом диске
- кривая **Writes{device="sda"}** – отображает число дисковых операций записи на физическом диске
- кривая **Writes{device="sr0"}** – отображает число дисковых операций записи на логическом диске

> График **Число дисковых операций в секунду** используется для комплексной оценки работы системы.
> Возрастание нагрузки обычно связано с записью данных логов на диск

5 график **Использование пропускной способности, %** Рисунок 132 показывает использование пропускной способности диска в реальном времени на следующих кривых:

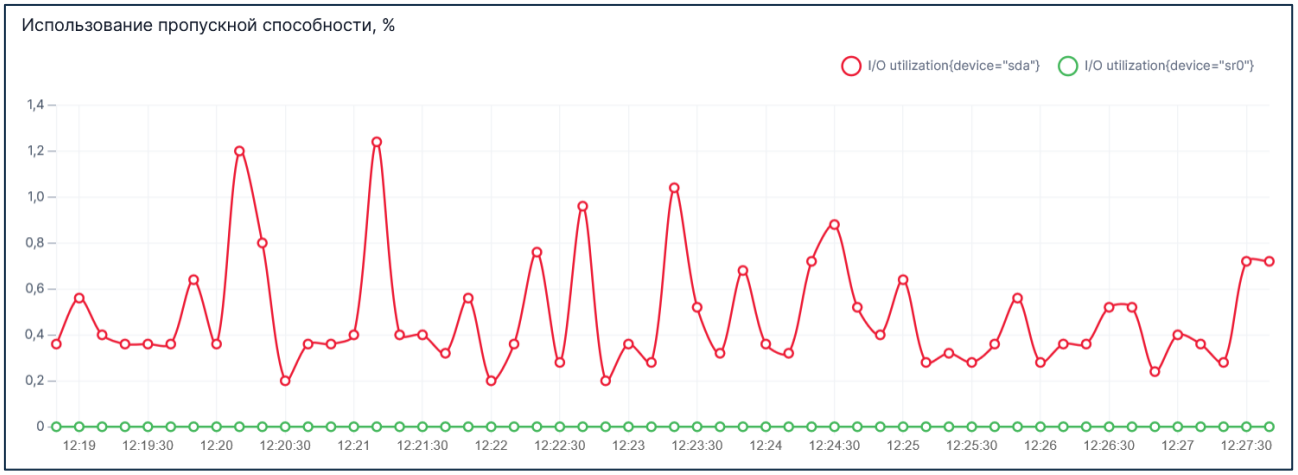

Рисунок 132. График Использование пропускной способности, %

- кривая **I/O utilization{device="sda"}** – отображает процент используемой пропускной способности на физическом диске
- кривая **I/O utilization{device="sr0"}** – отображает процент используемой пропускной способности на логическом диске

> График **Использование пропускной способности** используется для комплексной оценки работы системы.
> Возрастание нагрузки обычно связано с записью данных логов на диск

6 график **Среднее время операции, мс** Рисунок 133 показывает среднее время операции в реальном времени на следующих кривых:

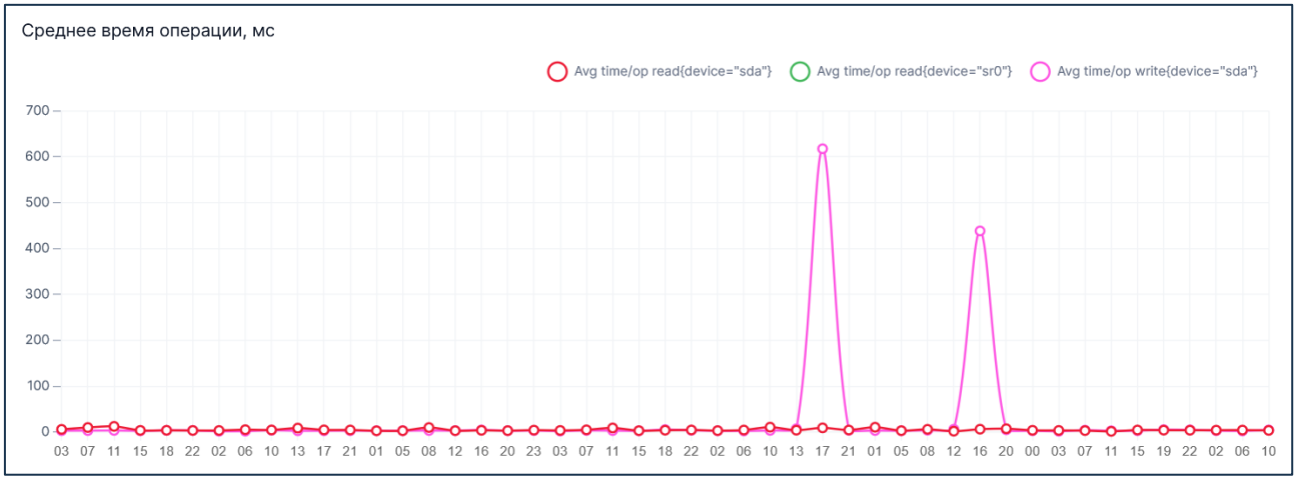

Рисунок 133. График Среднее время операции, мс

- кривая **Avg time/op read{device="sda"}** – отображает среднее время операции чтения на физическом диске
- кривая **Avg time/op read{device="sr0"}** (для сервера проксирования) – отображает среднее время операции чтения на логическом диске
- кривая **Avg time/op write{device="sda"}** – отображает среднее время операции записи на физическом диске

> График **Среднее время операции** используется для комплексной оценки работы системы.
> Возрастание нагрузки обычно связано с записью данных логов на диск

Вкладка Модули

В IVA SBC могут отображаться следующие модули:

- **Auditbeat** – модуль, отвечающий за аудит системных событий в операционной системе
- **Auditd** – модуль, отвечающий за аудит системных событий в операционной системе
- **Collectd** – модуль, собирающий статистику в rdd-файлы (по умолчанию отключен)
- **Corosync** – модуль, отвечающий за согласование и синхронизацию между узлами кластера

- Fail2ban-server – сервер, блокирующий IP-адреса по различным событиям
- Filebeat – модуль, отвечающий за аудит системных событий в операционной системе
- Keepalived – модуль, отвечающий за управление плавающими IP-адресами
- Kesl – антивирус Kaspersky Endpoint Security для Linux (если установлен)
- Klnagent – модуль Агента администрирования антивируса Kaspersky (если установлен)
- Monitoring – модуль, отвечающий за мониторинг и управление сервером и его параметрами
- Nginx (только на сервере управления и конфигурации) – модуль, отвечающий за HTTP Reverse Proxy для администрирования SBC
- Pacemaker (не используется на всех серверах и отключен) – модуль, отвечающий за автоматическое управление и мониторинг нескольких серверов одновременно
- Postgres (только на сервере управления и конфигурации) – модуль, отвечающий за базу данных
- Prometheus-node-exporter – модуль, отвечающий за сбор статистики для Victoria-metrics с параметрами работы системы
- Registry – модуль, отвечающий за регистрацию компонент
- Sbc (только на сервере проксирования) – модуль, отвечающий за TURN и HTTP Reverse Proxy
- Sbc-cfg-server (только на сервере управления и конфигурации) – модуль, отвечающий за конфигурирование серверов проксирования
- Victoria-metrics – модуль, отвечающий за локальное хранение статистики параметров работы сервера
- Vmalert – модуль, отвечающий за сбор системных аварий
- Voip-signalling-gateway (только на сервере проксирования) – модуль, отвечающий за VoIP-проксирование для SIP- /H.323-сигнализации и RTP
- Wdserver – модуль, отвечающий за системный сервис анализа

На вкладке **Модули** для сервера проксирования и сервера управления и конфигурации отображаются следующие графики:

1 график **ЦПУ, %** Рисунок 134 показывает использование ЦПУ различными модулями в реальном времени на кривых <**Название модуля**>

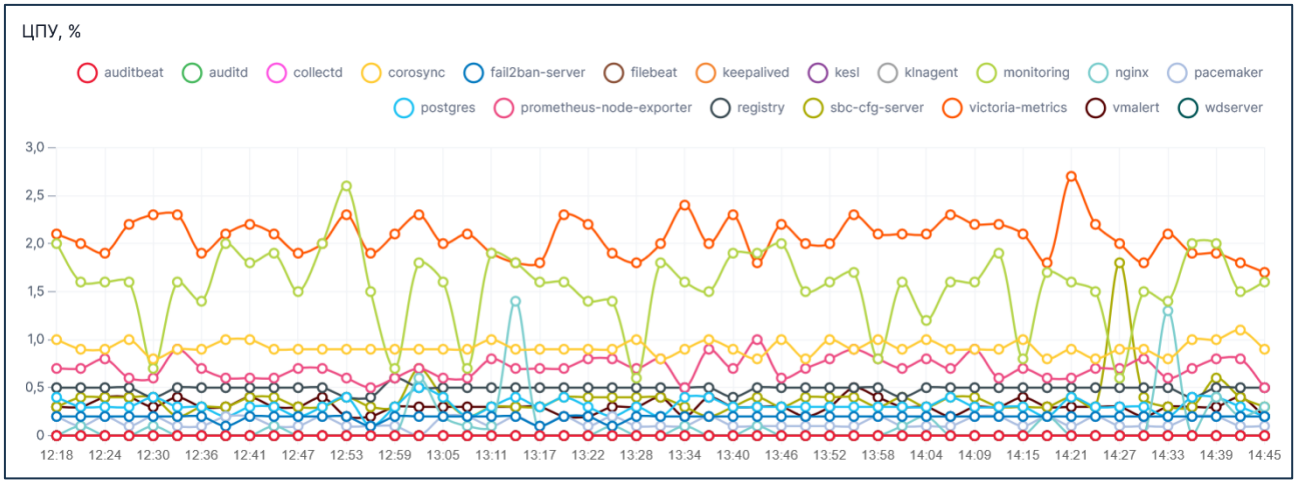

Рисунок 134. График ЦПУ, %

> График **ЦПУ** используется для комплексной оценки работы системы (например, для выявления модуля, оказывающего наибольшую нагрузку на систему)

2 график **Память, МБ** Рисунок 135 показывает использование памяти различными модулями в реальном времени на кривых **<Название модуля>**

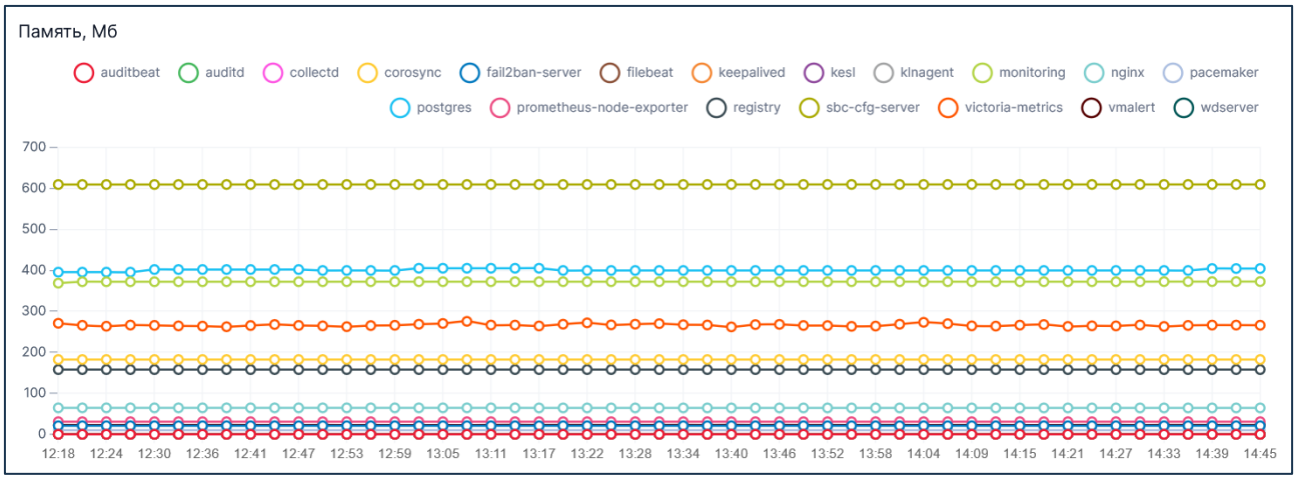

Рисунок 135. График Память, МБ

> График **Память** используется для комплексной оценки работы системы

3 график **Дисковые чтения, Кб/с** Рисунок 136 показывает количество дисковых операции чтения в реальном времени на кривых **<Название модуля>**

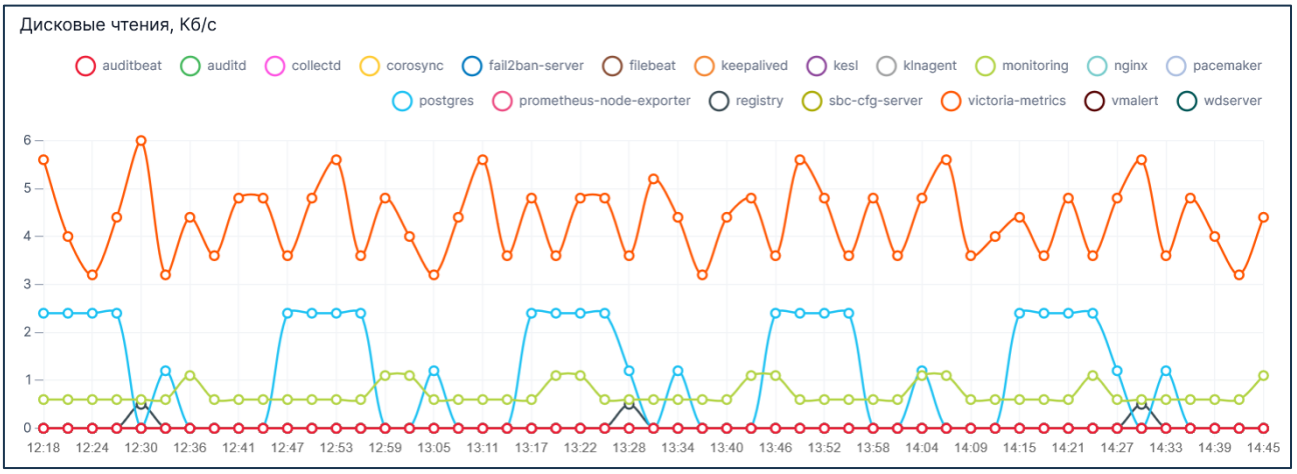

Рисунок 136. График Дисковые чтения, Кб/с

> График **Дисковые чтения** используется для комплексной оценки работы системы

4 график **Дисковые записи, Кб/с** Рисунок 137 показывает количество дисковых операций записи в реальном времени на кривых **<Название модуля>**

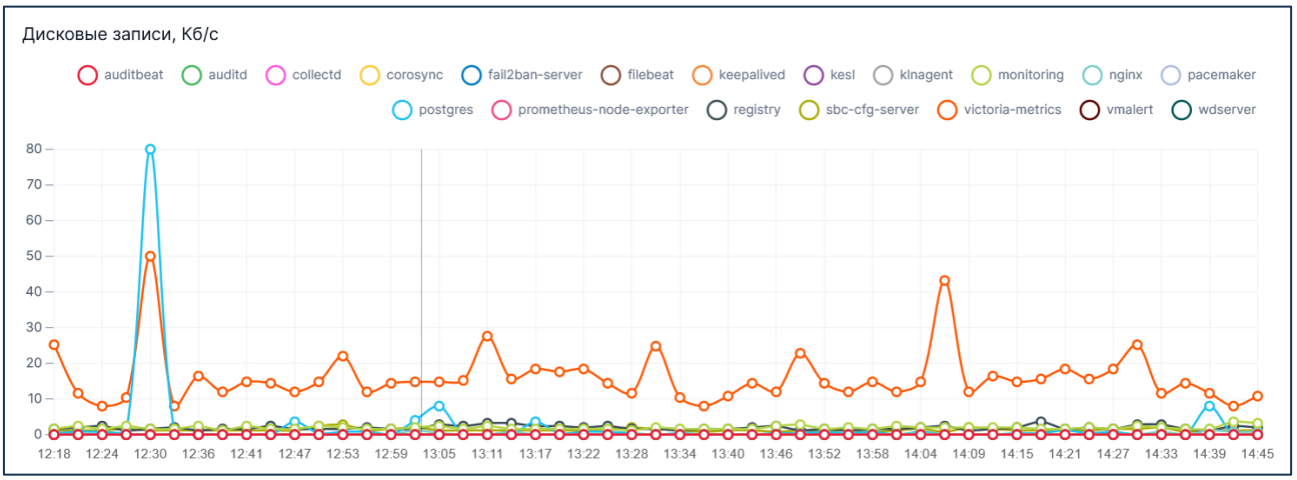

Рисунок 137. График Дисковые записи, Кб/с

> График **Дисковые записи** используется для комплексной оценки работы системы (например, для определения, какой модуль больше всех нагружает систему)

5 график **Процессы** Рисунок 138 показывает количество процессов, запущенных модулем в реальном времени, на кривых **<Название модуля>**

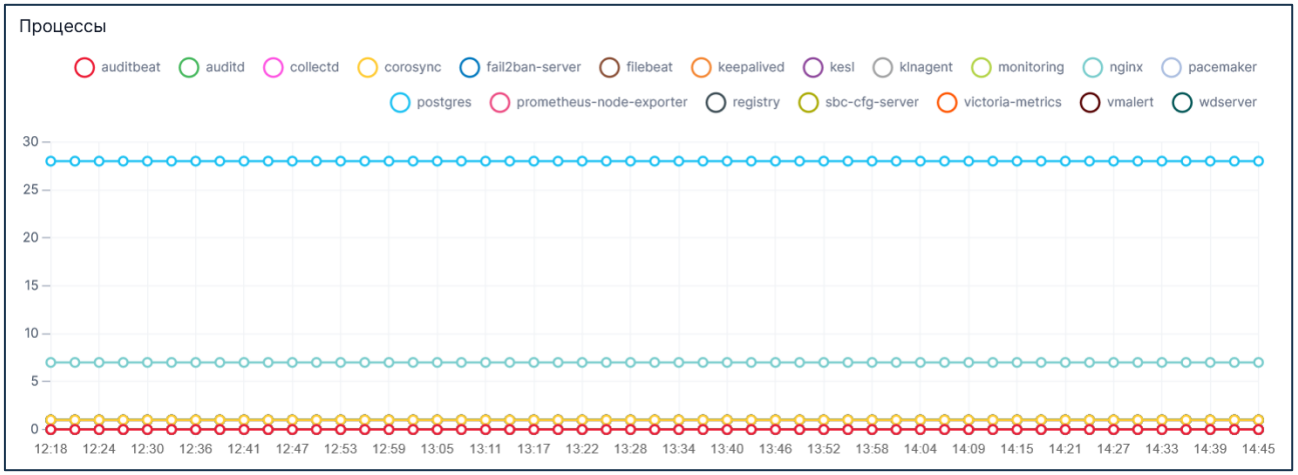

Рисунок 138. График Процессы

> График **Процессы** используется для комплексной оценки работы системы

6 график **Потоки** Рисунок 139 показывает количество потоков, исполняемых модулем в реальном времени, на кривых **<Название модуля>**

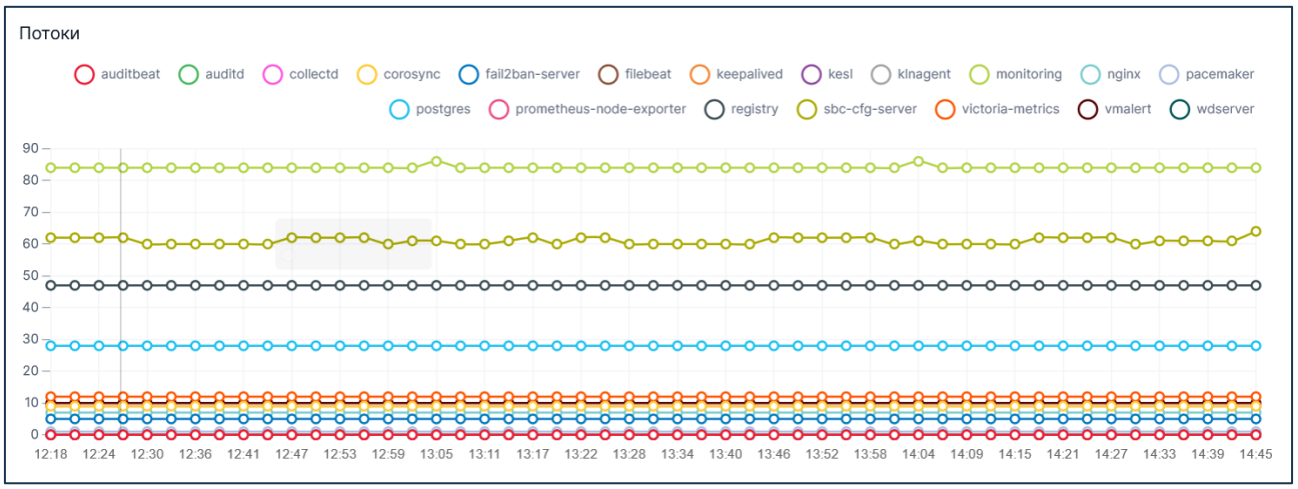

Рисунок 139. График Потоки

> График **Потоки** используется для комплексной оценки работы системы. При **корректной работе системы** количество потоков не должно возрастать

7 график **Открытые файловые дескрипторы** Рисунок 140 показывает количество открытых модулем файловых дескрипторов в реальном времени на кривых <Название модуля>

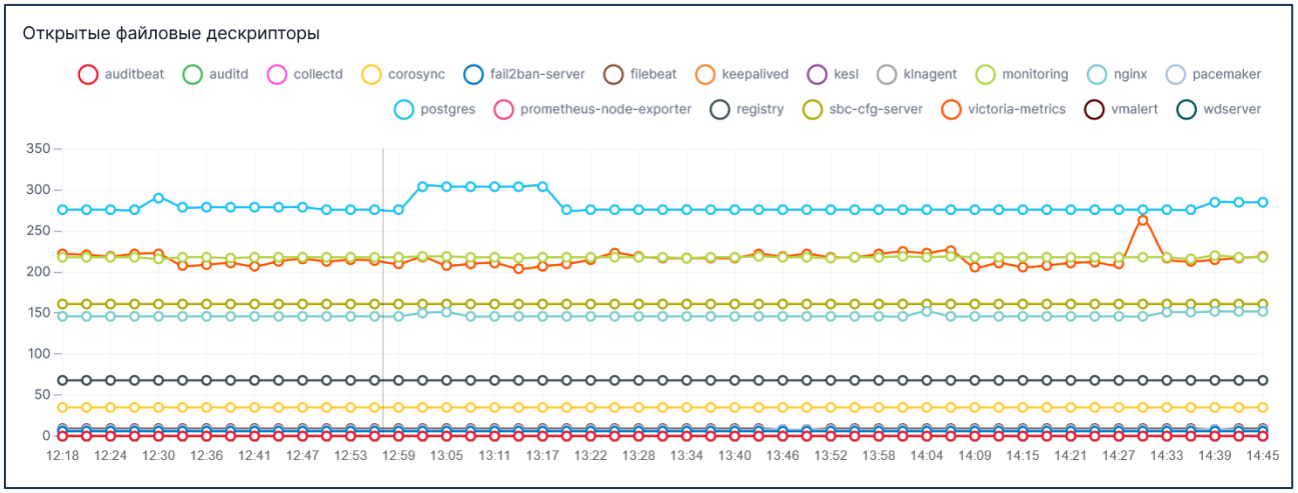

Рисунок 140. График Открытые файловые дескрипторы

> График **Открытые файловые дескрипторы** используется для комплексной оценки работы системы

Вкладка Среда исполнения

На вкладке **Среда исполнения** для сервера проксирования ('sbc', 'monitoring' и 'voip-signalling-gateway') и сервера управления и конфигурации ('sbc-cfg-server' и 'monitoring') отображаются следующие графики:

1 график **Утилизация областей памяти ('sbc' / 'sbc-cfg-server'), МБ** Рисунок 141 показывает утилизацию памяти в реальном времени на следующих кривых:

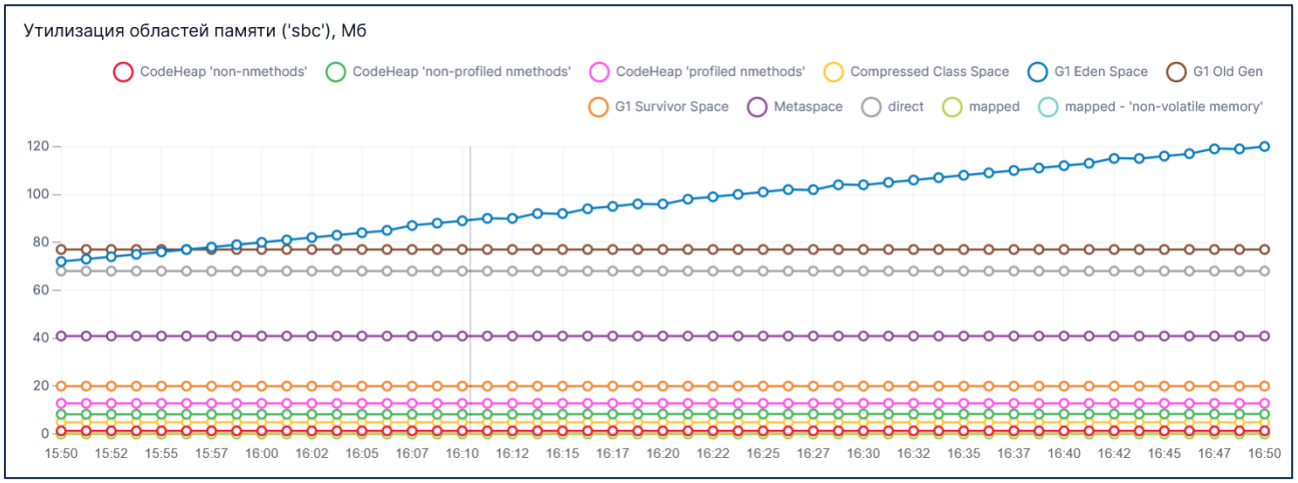

Рисунок 141. График Утилизация областей памяти ('sbc' / 'sbc-cfg-server'), МБ

- кривая **CodeHeap 'non-nmethods'** – отображает утилизацию памяти внутреннего кода
- кривая **CodeHeap 'non-profiled nmethods'** – отображает утилизацию памяти непрофилированного кода
- кривая **CodeHeap 'profiled nmethods'** – отображает утилизацию памяти профилированного кода
- кривая **Compressed Class Space** – отображает утилизацию памяти, где хранится информация о загруженных классах
- кривая **G1 Eden Space** – отображает утилизацию памяти, где хранятся все создаваемые в программе объекты
- кривая **G1 Old Gen** – отображает утилизацию памяти, занятой долгоживущими объектами

> Рекомендуется выполнять мониторинг значений G1 Old Gen

- кривая **G1 Survivol Space** – отображает утилизацию памяти, где хранятся объекты из Par Eden Space (признаны долгоживущими)
- кривая **Metaspace** – отображает утилизацию памяти, где хранится статическая информация приложения
- кривая **direct** – отображает изменение использования памяти прямого доступа (Direct Memory)
- кривая **mapped** – отображает соотношения памяти и процесса
- кривая **mapped - 'non-volatile memory'** – отображает использование энергозависимой памяти

> График **Утилизация областей памяти** используется для комплексной оценки работы системы

2 график **Время затраченное на сбор мусора ('sbc' / 'sbc-cfg-server'), с** Рисунок 142 показывает время, затраченное на сбор мусора в реальном времени, на следующих кривых:

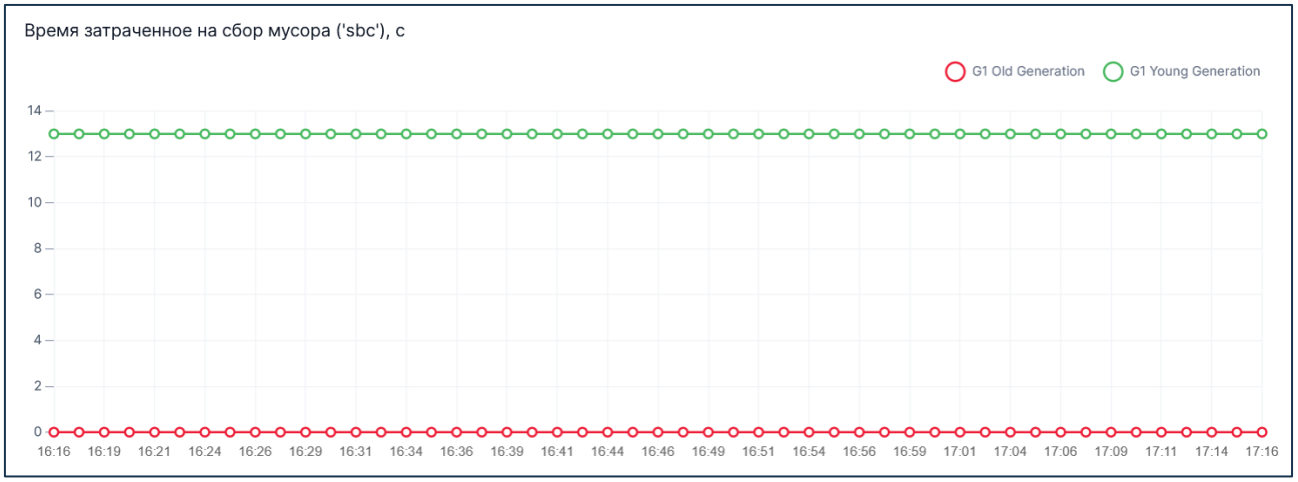

Рисунок 142. График Время затраченное на сбор мусора ('sbc' / 'sbc-cfg-server'), с

- кривая **G1 Old Generation** – отображает время, затраченное на сбор мусора G1 Old Generation
- кривая **G1 Young Generation** – отображает время, затраченное на сбор мусора G1 Young Generation

> График **Время затраченное на сбор мусора** используется для комплексной оценки работы системы. При **корректной работе системы** кривые на графике должны расти медленно и равномерно

3 график **Утилизация областей памяти ('monitoring'), МБ** Рисунок 143 показывает утилизацию памяти в реальном времени на следующих кривых:

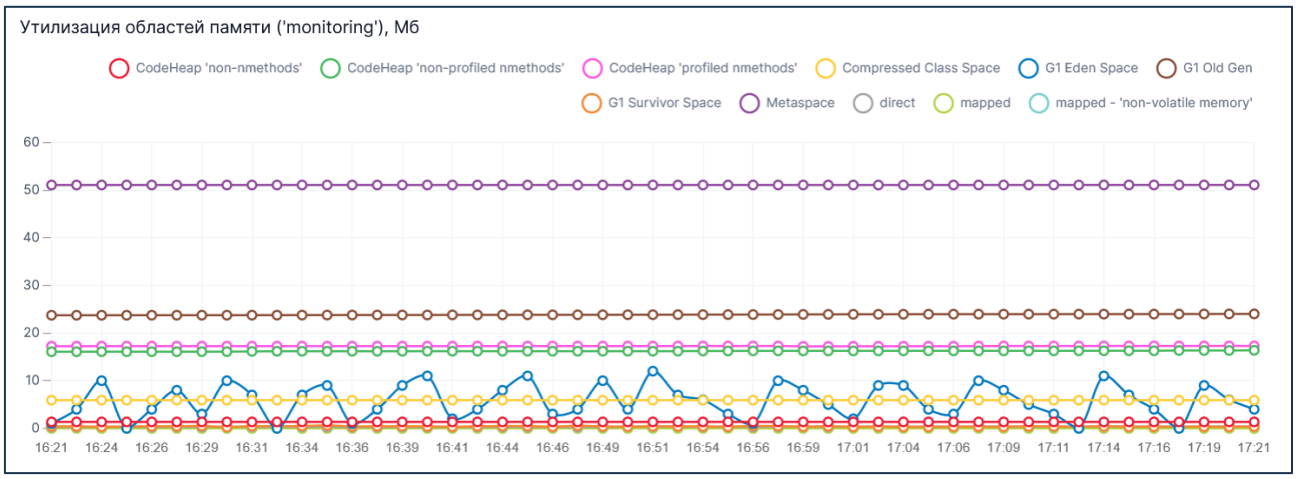

Рисунок 143. График Утилизация областей памяти ('monitoring'), МБ

- кривая **CodeHeap 'non-nmethods'** – отображает утилизацию памяти внутреннего кода
- кривая **CodeHeap 'non-profiled nmethods'** – отображает утилизацию памяти непрофилированного кода
- кривая **CodeHeap 'profiled nmethods'** – отображает утилизацию памяти профилированного кода
- кривая **Compressed Class Space** – отображает утилизацию памяти, где хранится информация о загруженных классах
- кривая **G1 Eden Space** – отображает утилизацию памяти, где хранятся все созданные в программе объекты
- кривая **G1 Old Gen** – отображает утилизацию памяти, которая занята долгоживущими объектами

> Рекомендуется выполнять мониторинг значений G1 Old Gen

- **G1 Survivol Space** – отображает утилизацию памяти, где хранятся объекты из Par Eden Space (признаны долгоживущими)
- кривая **Metaspace** – отображает утилизацию памяти, где хранится статическая информация приложения

- кривая **direct** – отображает изменение использования памяти прямого доступа (Direct Memory)
- кривая **mapped** – отображает соотношение памяти и процесса в реальном времени
- кривая **mapped - 'non-volatile memory'** – отображает использование энергозависимой памяти

> График **Утилизация областей памяти ('monitoring')** используется для комплексной оценки работы системы

4 график **Время затраченное на сбор мусора ('monitoring')**, с Рисунок 144 показывает время, затраченное на сбор мусора в реальном времени, на следующих кривых:

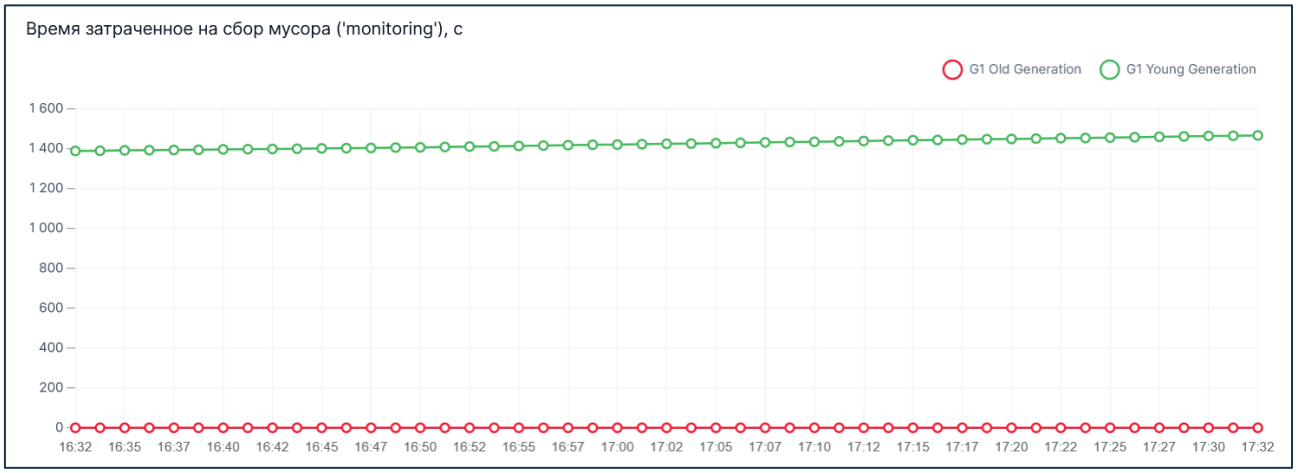

Рисунок 144. График Время затраченное на сбор мусора ('monitoring'), с

- кривая **G1 Old Generation** – отображает время, затраченное на сбор мусора G1 Old Generation
- кривая **G1 Young Generation** – отображает время, затраченное на сбор мусора G1 Young Generation

> График **Время затраченное на сбор мусора ('monitoring')** используется для комплексной оценки работы системы. При **корректной работе системы** кривые на графике должны расти медленно и равномерно

5 график **Утилизация областей памяти ('voip-signalling-gateway'), МБ** Рисунок 145 показывает утилизацию памяти в реальном времени на следующих кривых:

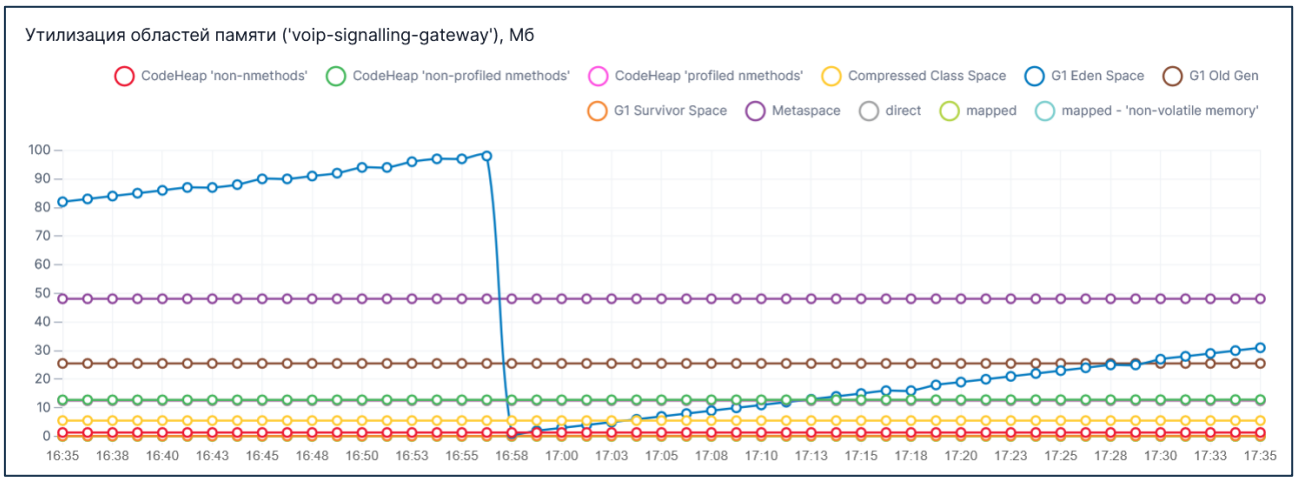

Рисунок 145. График Утилизация областей памяти ('voip-signalling-gateway'), МБ

- кривая **CodeHeap 'non-nmethods'** – отображает утилизацию памяти внутреннего кода
- кривая **CodeHeap 'non-profiled nmethods'** – отображает утилизацию памяти непрофилированного кода
- кривая **CodeHeap 'profiled nmethods'** – отображает утилизацию памяти профилированного кода
- кривая **Compressed Class Space** – отображает утилизацию памяти, где хранится информация о загруженных классах
- кривая **G1 Eden Space** – отображает утилизацию памяти, где хранятся все созданные в программе объекты
- кривая **G1 Old Gen** – отображает утилизацию памяти, которая занята долгоживущими объектами

> Рекомендуется выполнять мониторинг значений G1 Old Gen

- кривая **G1 Survivol Space** – отображает утилизацию памяти, где хранятся объекты из Par Eden Space (признаны долгоживущими)
- кривая **Metaspace** – отображает утилизацию памяти, где хранится статическая информация приложения

- кривая **direct** – отображает изменение использования памяти прямого доступа (Direct Memory)
- кривая **mapped** – отображает соотношение памяти и процесса в реальном времени
- кривая **mapped - 'non-volatile memory'** – отображает использование энергозависимой памяти

> График **Утилизация областей памяти ('voip-signalling-gateway')** используется для комплексной оценки работы системы

6 график **Время затраченное на сбор мусора ('voip-signalling-gateway'), с** Рисунок 146 показывает время, затраченное на сбор мусора в реальном времени, на следующих кривых:

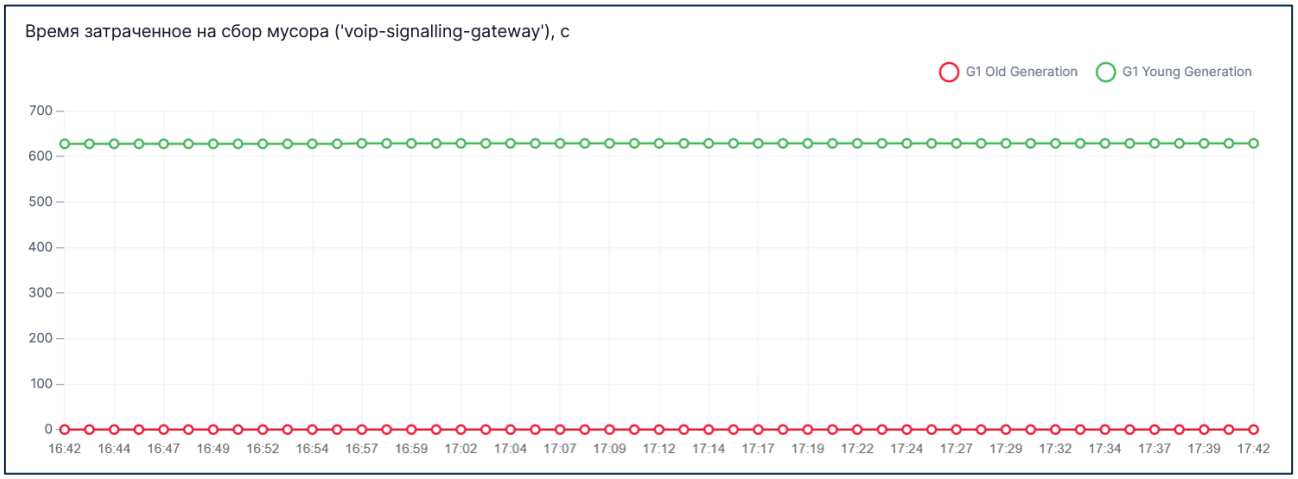

Рисунок 146. График Время затраченное на сбор мусора ('voip-signalling-gateway'), с

- кривая **G1 Old Generation** – отображает время, затраченное на сбор мусора G1 Old Generation
- кривая **G1 Young Generation** – отображает время, затраченное на сбор мусора G1 Young Generation

> График **Время затраченное на сбор мусора ('voip-signalling-gateway')** используется для комплексной оценки работы системы. При **корректной работе системы** кривые на графике должны расти медленно и равномерно

7 график **Загруженные классы** Рисунок 147 показывает количество классов, загруженных модулем в реальном времени, на кривых **<Название модуля>**

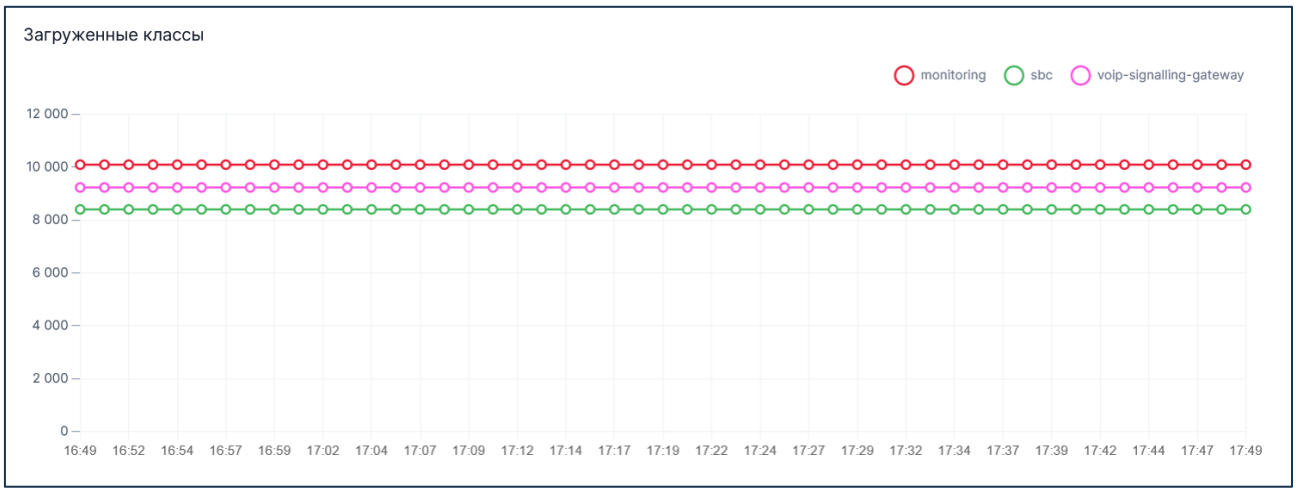

Рисунок 147. График Загруженные классы

> График **Загруженные классы** используется для комплексной оценки работы системы и предназначен для поставщика IVA SBC

Мониторинг G1 Old Gen

Чтобы избежать снижения производительности и аварийной остановки модуля, важно отслеживать метрики **G1 Old Gen** на графиках утилизации областей памяти.

Пороговое значение для области памяти G1 Old Gen высчитывается по формуле:

Ограничение использования памяти модулем × 80 %

Примеры пороговых значений G1 Old Gen:

Имя модуля	Ограничение использования памяти, МБ	Пороговое значение G1 Old Gen, МБ
sbc	512	409
sbc-cfg-server	256	204
monitoring	64	51
voip-signalling-gateway	256	204

Превышение данного порога в течение **более 2 минут подряд** означает, что модуль испытывает высокую нагрузку. Это приводит к снижению его производительности и повышению риска аварийной остановки модуля.

Вкладка Внутренности

На вкладке **Внутренности** для сервера проксирования (**sbc**) и сервера управления и конфигурации (**sbc-cfg-server**) отображаются следующие графики:

1 график **Паузы монотонного таймера, с** (для **sbc** / **sbc-cfg-server**) Рисунок 148 показывает паузы монотонного таймера в каждом из модулей **<Название модуля>.** Расчет осуществляется как разница между временем, когда модуль получает управление от сервера, и ожидаемым временем его получения

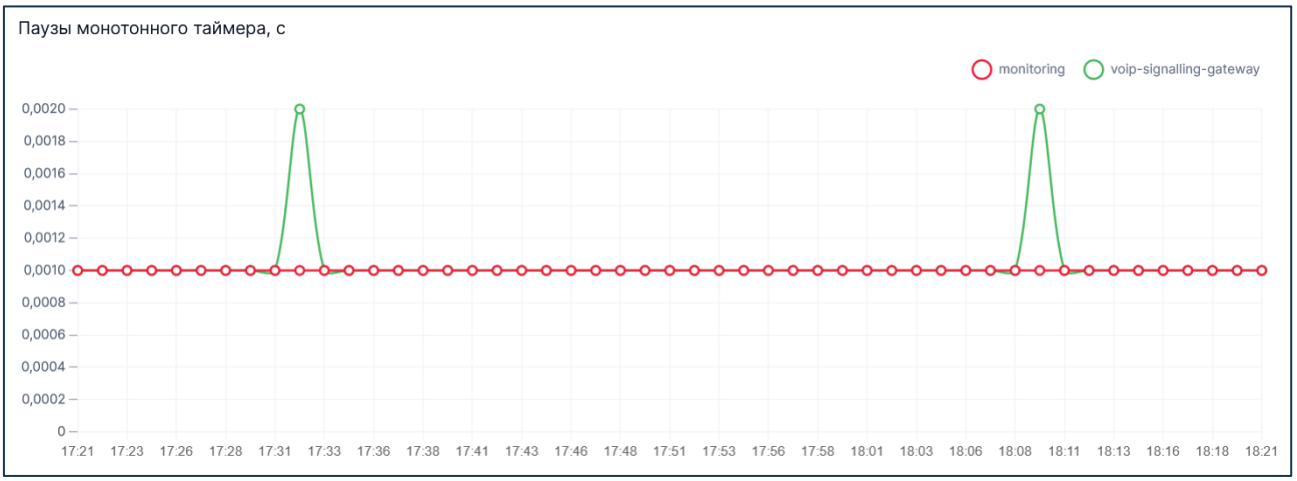

Рисунок 148. График Паузы монотонного таймера, с

> При **корректной работе системы Паузы монотонного таймера** не должны превышать 20 мс. Превышение значения может свидетельствовать о перегрузке системы, замирании виртуальной машины или других проблемах

2 график **Паузы не монотонного таймера, с** (для **sbc** / **sbc-cfg-server**) Рисунок 149 показывает паузы не монотонного таймера перед запуском служб в модуле в реальном времени на кривых **<Название модуля>**

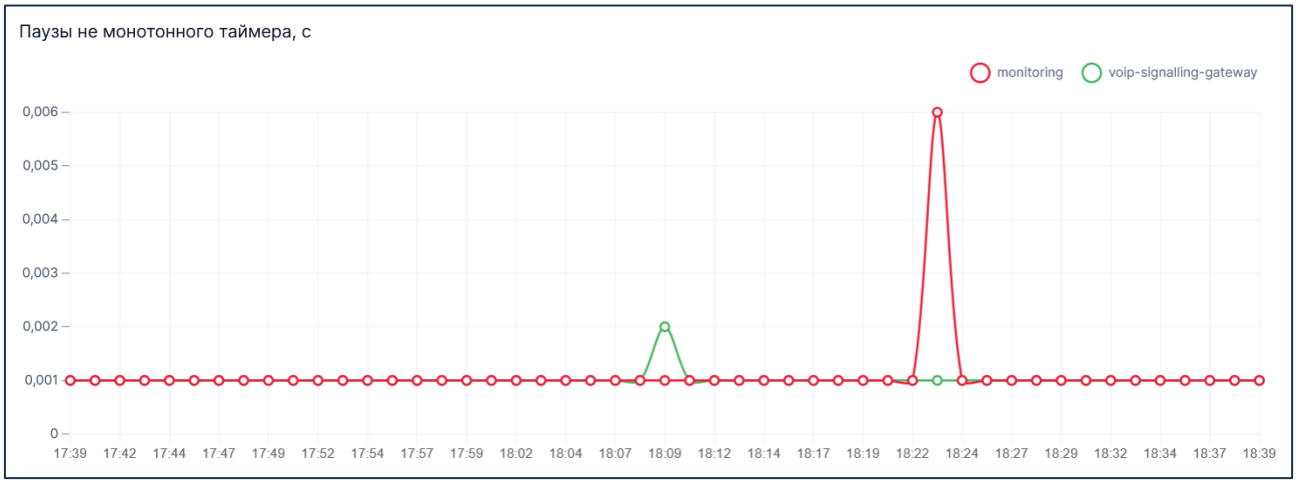

Рисунок 149. График Паузы не монотонного таймера, с

> График **Паузы не монотонного таймера** используется для комплексной оценки работы системы

3 график **Срабатывания Fail2ban** (для **sbc** / **sbc-cfg-server**) Рисунок 150 показывает срабатывания Fail2ban в реальном времени на следующих кривых:

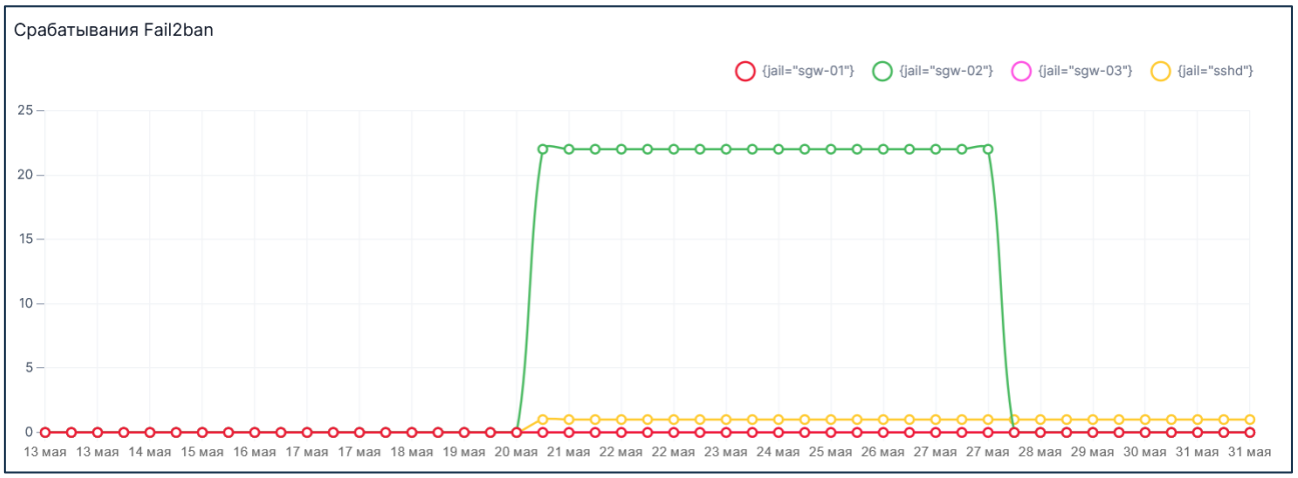

Рисунок 150. График Срабатывания Fail2ban

- кривая **{jail="sgw-01"}** – отображает количество срабатываний блокировки Fail2ban по числу SIP- / H.323-регистраций с одного IP-адреса
- кривая **{jail="sgw-02"}** – отображает количество срабатываний блокировки Fail2ban по числу звонков с одного IP-адреса
- кривая **{jail="sgw-03"}** – отображает количество срабатываний блокировки Fail2ban по числу коротких (небольшие по длительности) вызовов с одного IP-адреса

- кривая **{jail="sshd"}** – отображает количество срабатываний блокировки Fail2ban по числу неправильного ввода пароля для доступа по SSH с одного IP-адреса

> Сильный рост количества **срабатываний Fail2ban** может означать наличие DoS-атак по соответствующему протоколу

4 график **Количество IP заблокированных Fail2ban** (для **sbc / sbc-cfg-server**) Рисунок 151 показывает количество IP-адресов, заблокированных Fail2ban в реальном времени на следующих кривых:

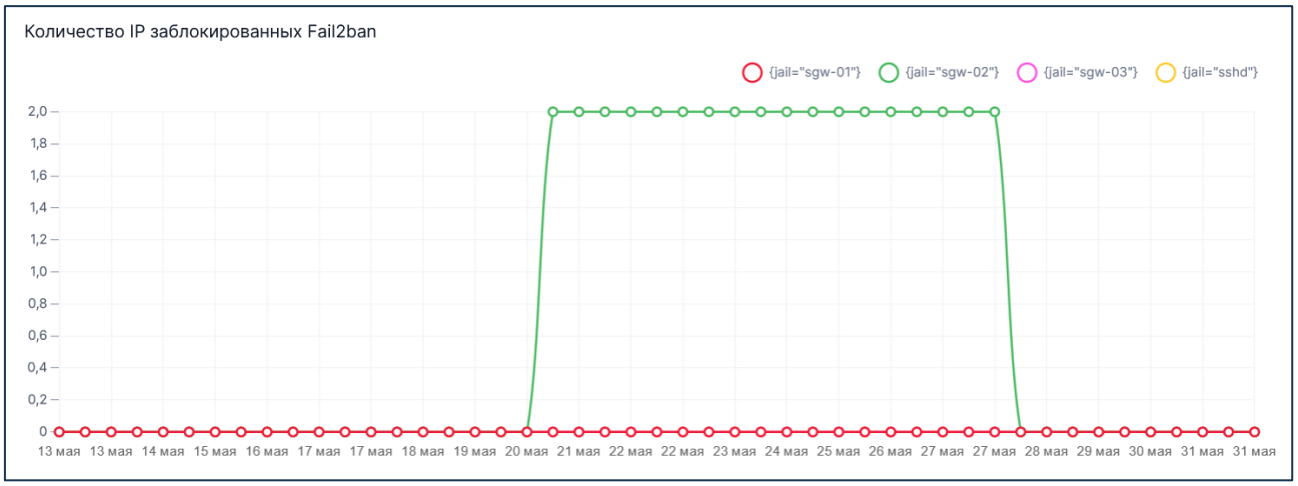

Рисунок 151. График Количество IP заблокированных Fail2ban

- кривая **{jail="sgw-01"}** – отображает количество IP-адресов, заблокированных Fail2ban по числу SIP- / H.323-регистраций с одного IP-адреса
- кривая **{jail="sgw-02"}** – отображает количество IP-адресов, заблокированных Fail2ban по числу звонков с одного IP-адреса
- кривая **{jail="sgw-03"}** – отображает количество IP-адресов, заблокированных Fail2ban по количеству коротких (небольшие по длительности) вызовов с одного IP-адреса
- кривая **{jail="sshd"}** – отображает количество IP-адресов, заблокированных Fail2ban по причине неправильного ввода пароля для доступа по SSH с одного IP-адреса

> Рост **количества IP-адресов, заблокированных Fail2ban**, может говорить о наличии DoS-атаки по соответствующему протоколу

5 график **Nginx соединения** (для **sbc-cfg-server**) Рисунок 152 показывает количество Nginx-соединений в реальном времени на следующих кривых:

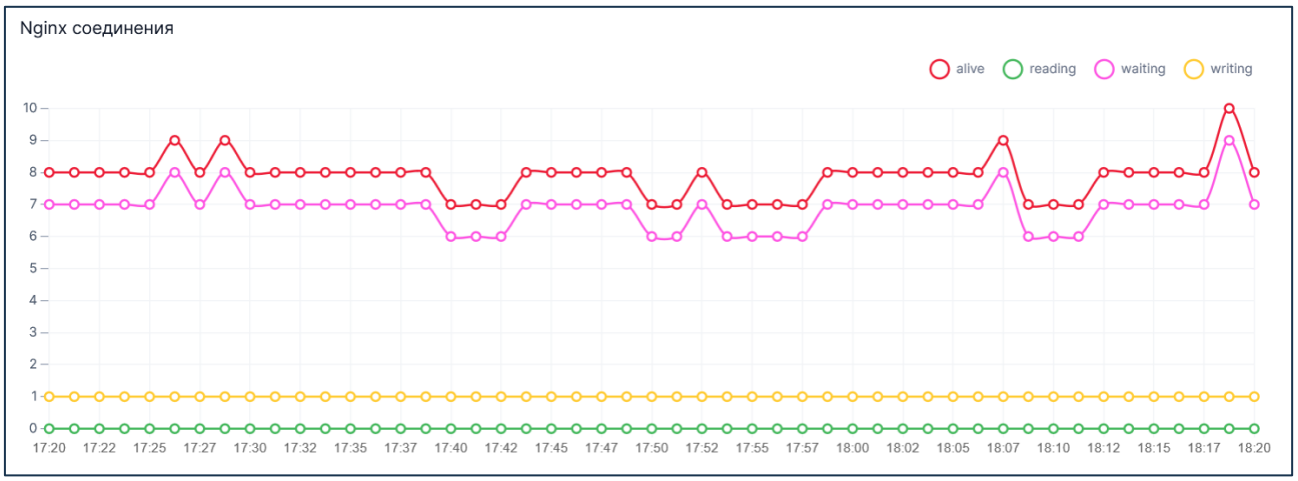

Рисунок 152. График Nginx соединения

- кривая **alive** – отображает количество активных подключений включая ожидающие
- кривая **reading** – отображает количество подключений, при которых Nginx читает заголовок запроса
- кривая **waiting** – отображает количество простаивающих клиентских подключений, ожидающих запроса
- кривая **writing** – отображает текущее количество подключений, при которых Nginx записывает ответ обратно клиенту

> График **Nginx соединения** используется для комплексной оценки работы системы. Количество соединений не должно иметь большого значения, т. к. доступ к серверу используется только для администрирования IVA SBC.
> **Увеличение количества соединений** может свидетельствовать о том, что к серверу пытаются получить несанкционированный доступ

6 график **Nginx запросы в секунду** (для **sbc-cfg-server**) Рисунок 153 показывает количество Nginx-запросов в секунду в реальном времени на кривой **rps**

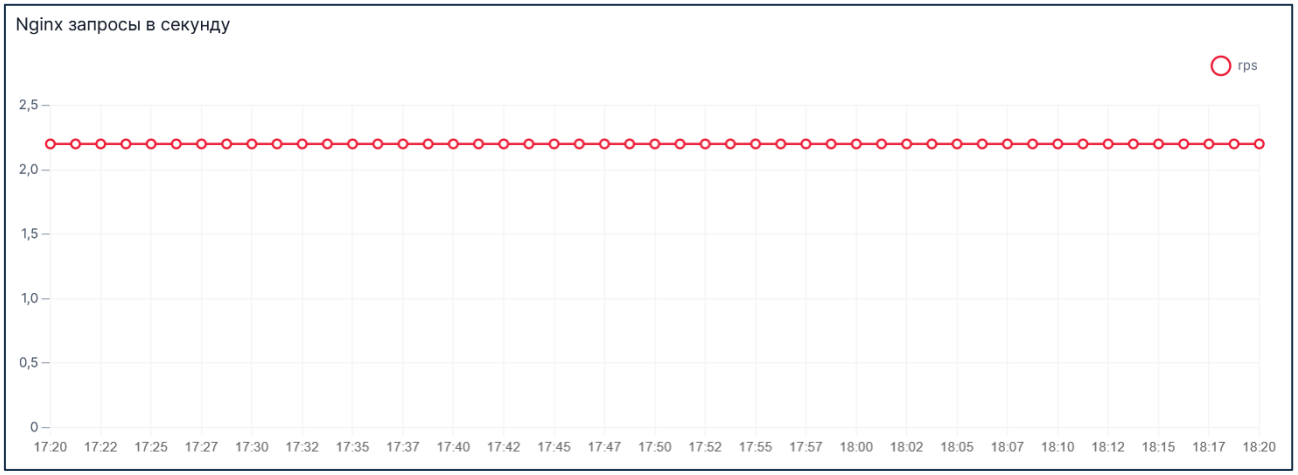

Рисунок 153. График Nginx запросы в секунду

> График **Nginx запросы в секунду** используется для комплексной оценки работы системы. Количество запросов не должно иметь большого значения, т. к. доступ к серверу используется только для администрирования IVA SBC.
>
> **Увеличение количества запросов**, может свидетельствовать о том, что к серверу пытаются получить несанкционированный доступ

7 график **Размер баз данных, МБ** (для **sbc-cfg-server**) Рисунок 154 показывает количество памяти, выделенное в базе данных для различных частей в реальном времени на кривых **<Название базы данных>**

Рисунок 154. График Размер баз данных, МБ

Размер баз данных зависит от времени хранения логов в системе.
Рост размера баз данных может говорить о DDoS-атаке или о необходимости уменьшения времени хранения истории аудита и событий

8 график **Подключения к базе данных** (для **sbc-cfg-server**) Рисунок 155 показывает количество подключений к базам данных и их статус в реальном времени на кривых **<Название базы данных и статус подключения>**

Статус подключения может иметь следующие значения:

- **active** – активно выполняющийся запрос
- **idle in transaction** – началась транзакция в БД, но еще не произошел commit в данной транзакции
- **unknown –** состояние подключения не определено

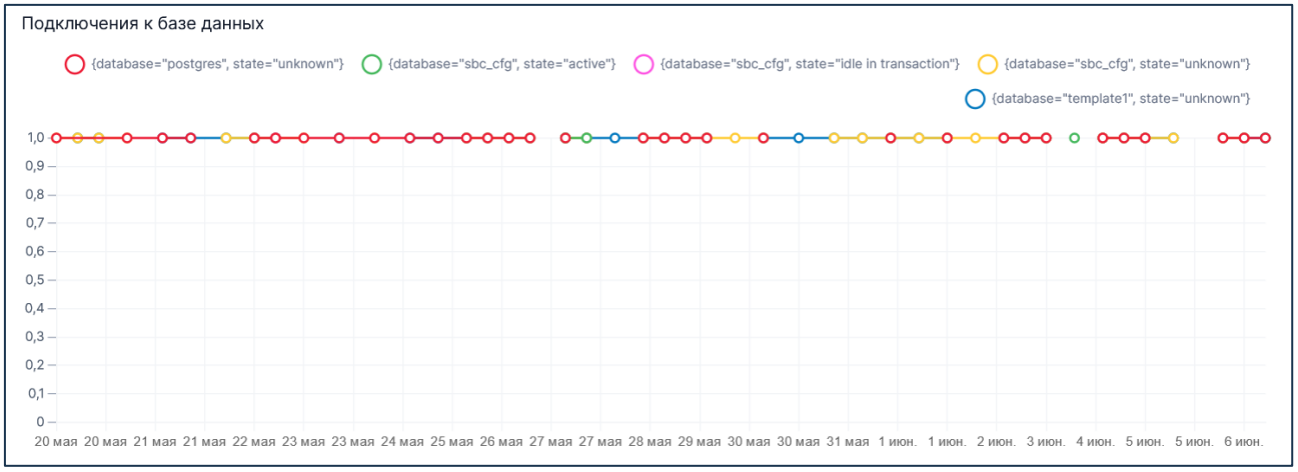

Рисунок 155. График Подключения к базе данных

График **Подключения к базе данных** используется для комплексной оценки работы системы.
При корректной работе системы в состоянии **active** и **idle in transaction** должно быть не более 5 запросов (в коротком промежутке времени). Постоянное число подключений более 5 и их рост означает наличие проблем с БД или с ростом нагрузки на систему

9 график **Взаимные блокировки** (для **sbc-cfg-server**) Рисунок 156 показывает количество взаимных блокировок в реальном времени на кривых **<Название базы данных>**

Рисунок 156. График Взаимные блокировки

> Для **корректной работы системы** необходимо отсутствие взаимных блокировок

10 график **Задержка репликации, байты** (для **sbc-cfg-server**) Рисунок 157 показывает количество байт задержки репликации в реальном времени

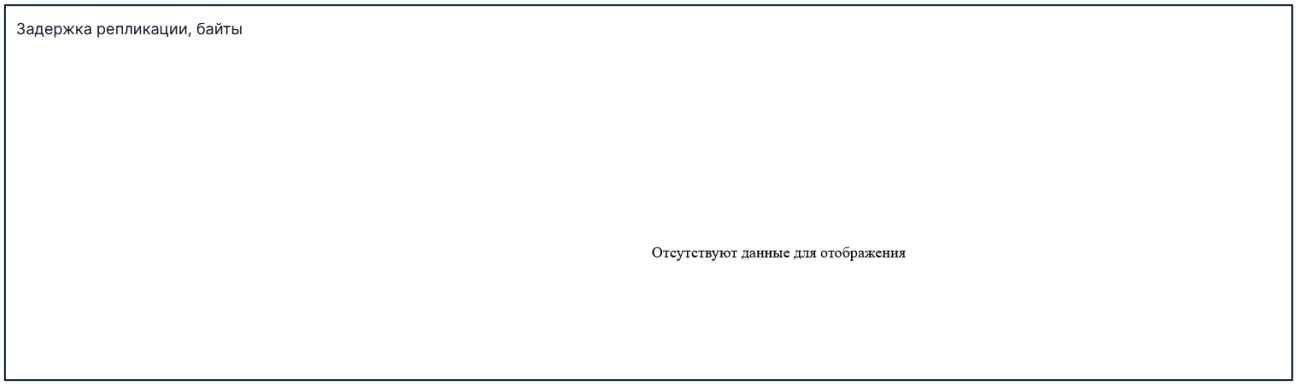

Рисунок 157. График Задержка репликации, байты

> В текущей версии IVA SBC данная метрика не используется

Вкладка HTTP

На вкладке **HTTP** для сервера проксирования отображаются следующие графики:

1 график **Запросы в секунду к HTTP reverse proxy серверу** Рисунок 158 показывает количество запросов в секунду к внутреннему HTTP-серверу в реальном времени на кривой **rps{port="443"}**

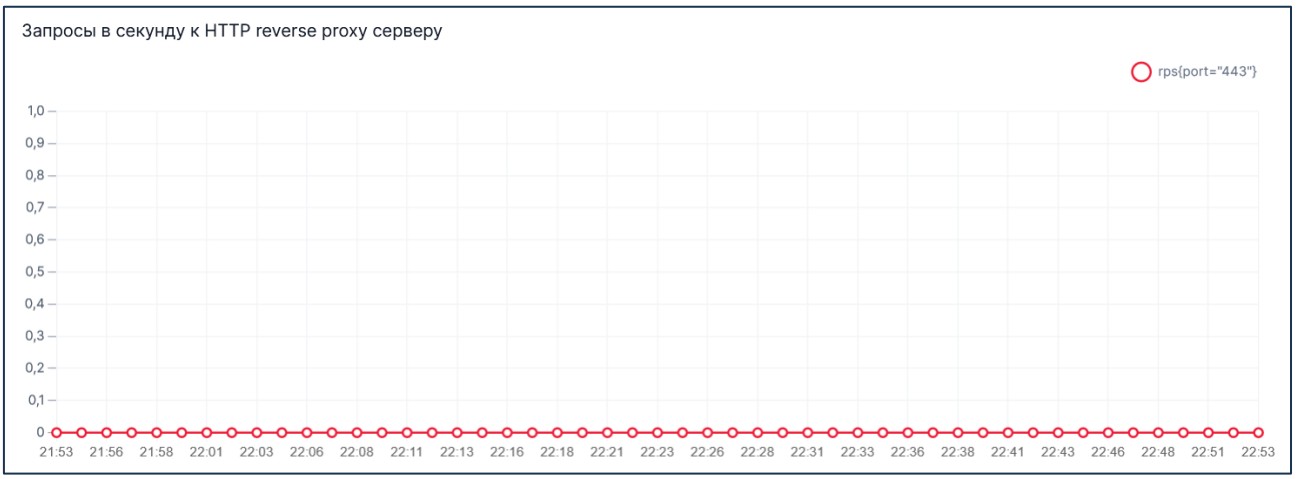

Рисунок 158. График Запросы в секунду к HTTP reverse proxy серверу

> График **Запросы в секунду к HTTP reverse proxy серверу** используется для комплексной оценки работы системы.
> Оценка проводится по той нагрузке, которая свойственна для системы (с учётом наличия больших конференций и плановой нагрузки на систему). Большое количество запросов может сигнализировать о DDoS-атаке на сервер

2 график **Количество активных запросов к HTTP reverse proxy серверу** Рисунок 159 показывает количество активных запросов к внутреннему HTTP-серверу в реальном времени на кривой **active_requests{port="443"}**

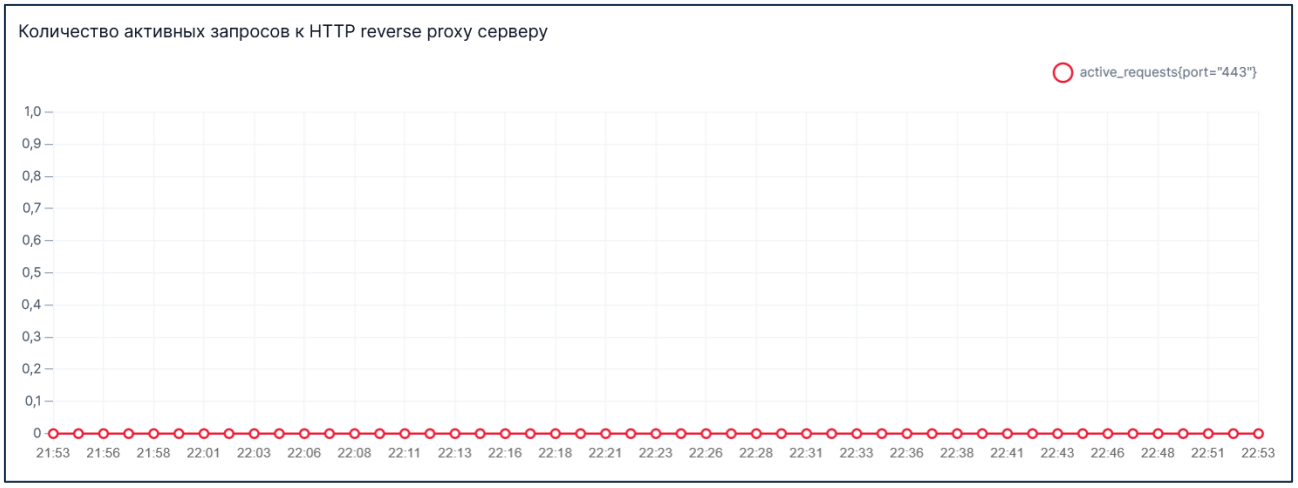

Рисунок 159. График Количество активных запросов к HTTP reverse proxy серверу

График **Количество активных запросов к HTTP reverse proxy серверу** используется для комплексной оценки работы системы.

Оценка проводится по той нагрузке, которая свойственна для системы в соответствии с количеством пользователей сервера (обычно оценивается в ретроспективе в соответствии с историей использования).

Если сервер получает **большое количество запросов**, это может указывать на DDoS-атаку, проведение масштабной конференции, или наличие проблем в работе внутреннего HTTP-сервера, который не справляется с обработкой запросов

3 график **Время обработки запросов HTTP reverse proxy** Рисунок 160 показывает время обработки запросов к внутреннему HTTP-серверу в реальном времени на кривой **rate{port="443"}**

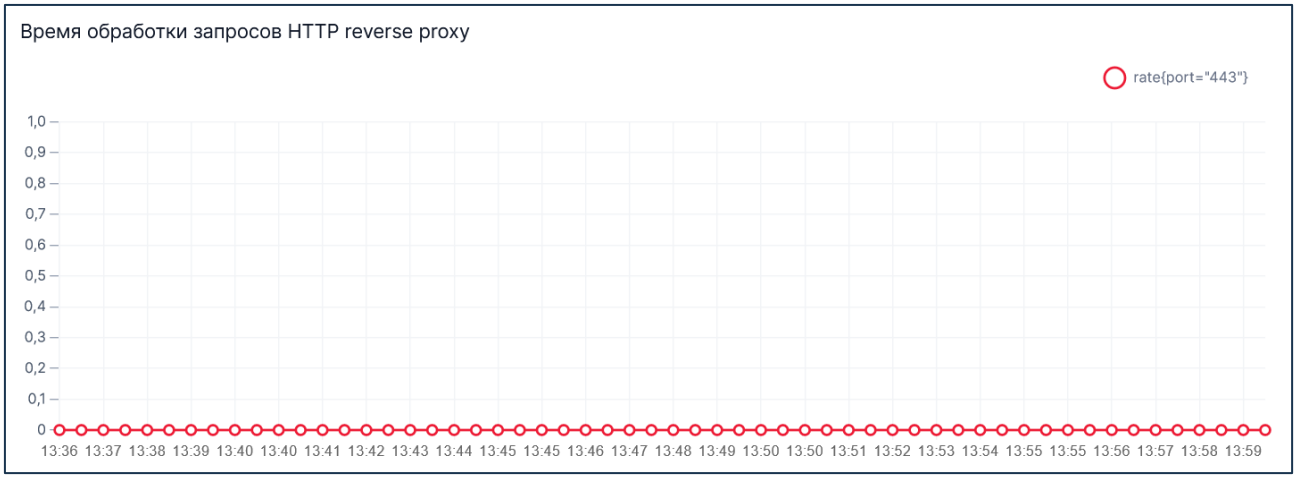

Рисунок 160. График Время обработки запросов HTTP reverse proxy

> Время обработки запросов к внутреннему HTTP-серверу должно быть **не более 200 мс**. Увеличение значения свыше 200 мс может свидетельствовать об ошибках на HTTP-сервере

4 график **Исходящий трафик HTTP reverse proxy сервера, кб/с** Рисунок 161 показывает объём исходящего трафика от внутреннего HTTP-сервера в реальном времени на кривой **kbps{port="443"}**

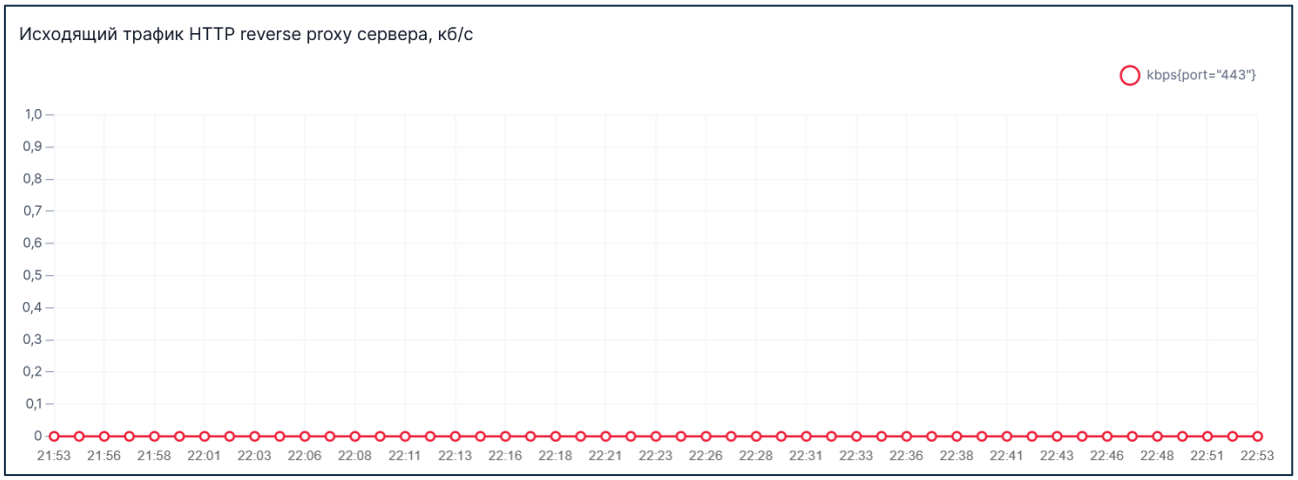

Рисунок 161. График Исходящий трафик HTTP reverse proxy сервера, кб/с

> График **Исходящий трафик HTTP reverse proxy сервера** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Увеличение количества исходящего трафика** может означать проведение масштабных конференций или выгрузку пользователями больших файлов (например запись мероприятия)

5 график **Статистика ответов HTTP reverse proxy сервера** Рисунок 162 показывает статистику ответов от внутреннего HTTP-сервера в реальном времени на следующих кривых:

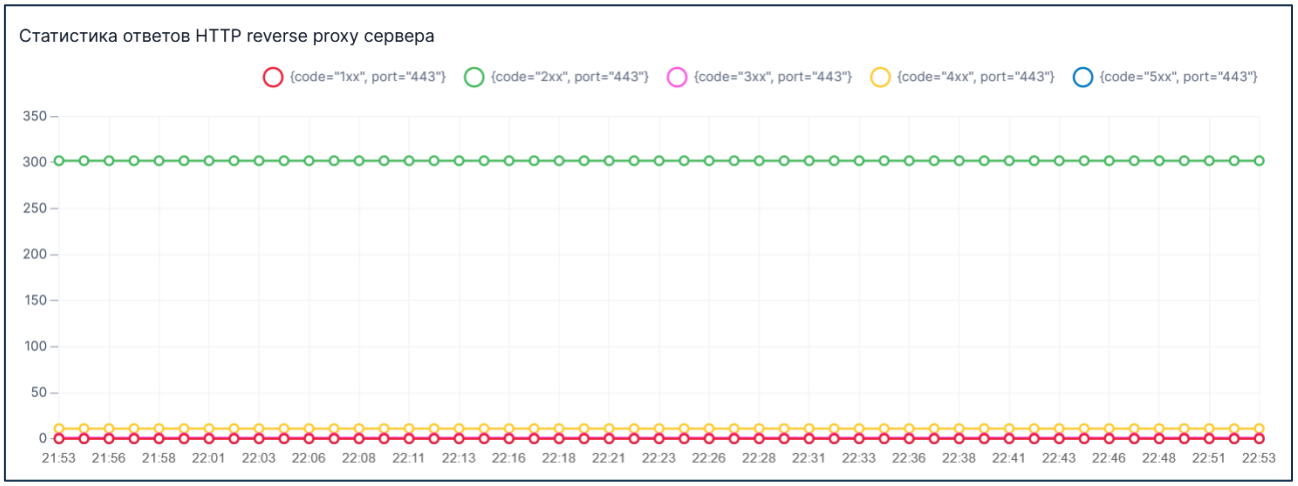

Рисунок 162. График Статистика ответов HTTP reverse proxy сервера

- кривые {code="1xx", port="443"}, {code="2xx", port="443"}, {code="3xx", port="443"}, {code="4xx", port="443"}, {code="5xx", port="443"} – отображают количество различных кодов ответа обратного HTTP-прокси сервера

> Наличие большого количества **ошибок 4xx** или **5xx** означает потенциально **некорректную работу системы**

6 график **Входящий трафик (Websocket) reverse proxy сервера, кб/с** Рисунок 163 показывает трафик от клиентов к серверу через внутренней прокси сервер в реальном времени на кривой **TX_kbps{port="443"}**

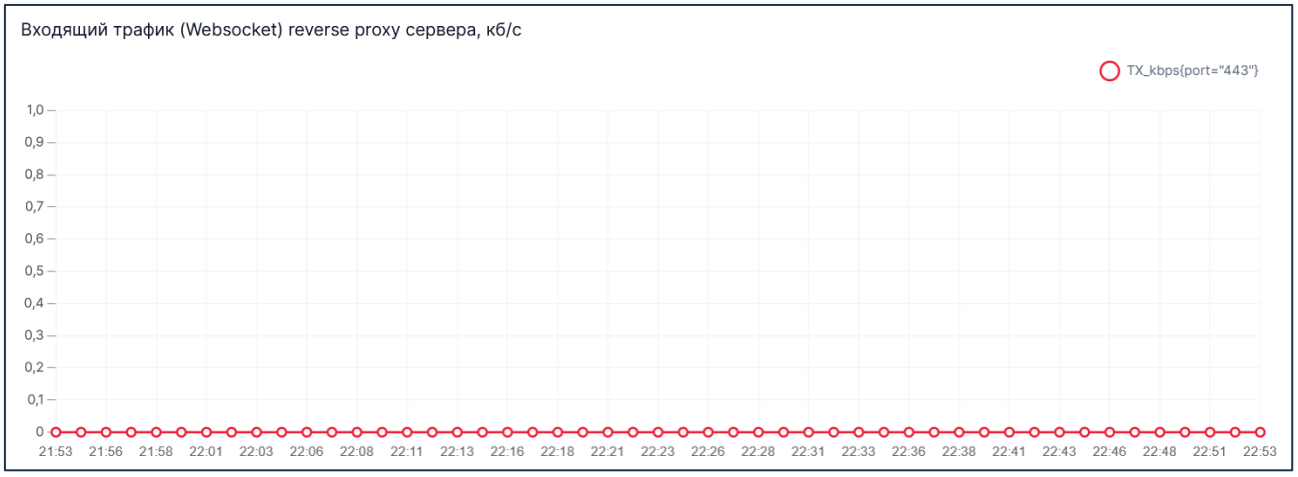

Рисунок 163. График Входящий трафик (Websocket) reverse proxy сервера, кб/с

> График **Входящий трафик (Websocket) reverse proxy сервера** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Увеличение количества входящего трафика** относительно обычного значения может означать проведение внеплановых конференций

7 график **Исходящий трафик (Websocket) reverse proxy сервера, кб/с** Рисунок 164 показывает трафик от сервера к клиенту через внутренней прокси сервер в реальном времени на кривой **RX_kbps{port="443"}**

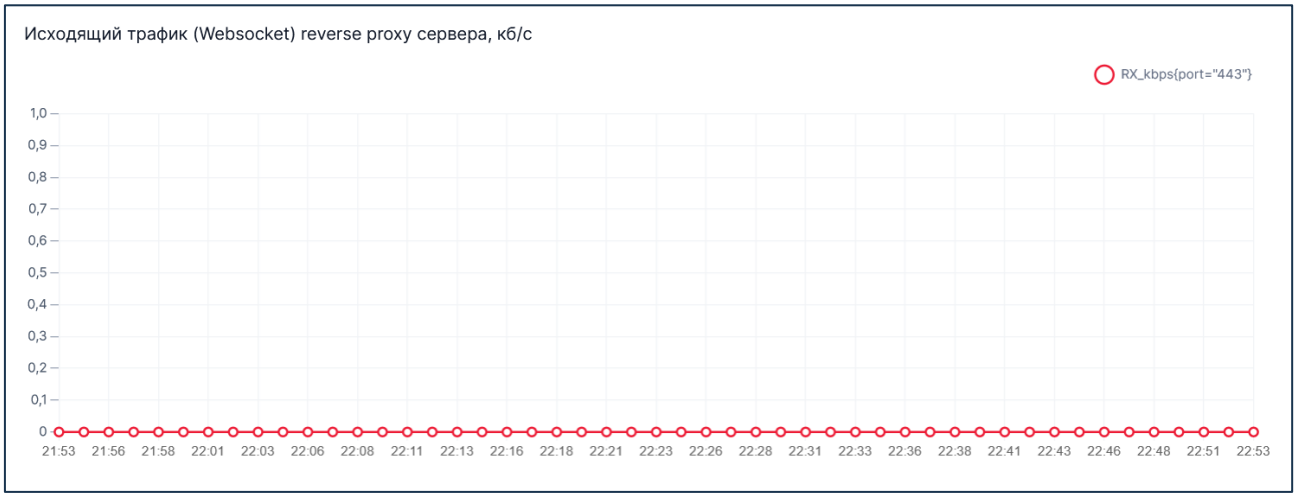

Рисунок 164. График Исходящий трафик (Websocket) reverse proxy сервера, кб/с

> График **Исходящий трафик (Websocket) reverse proxy сервера** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Увеличение количества исходящего трафика** относительно обычного значения может означать проведение внеплановых конференций

Вкладка VoIP

На вкладке **VoIP** для сервера проксирования отображаются следующие графики:

1 график **Размеры SIP таблиц в SGW** Рисунок 165 показывает размеры SIP-таблиц в реальном времени на следующих кривых:

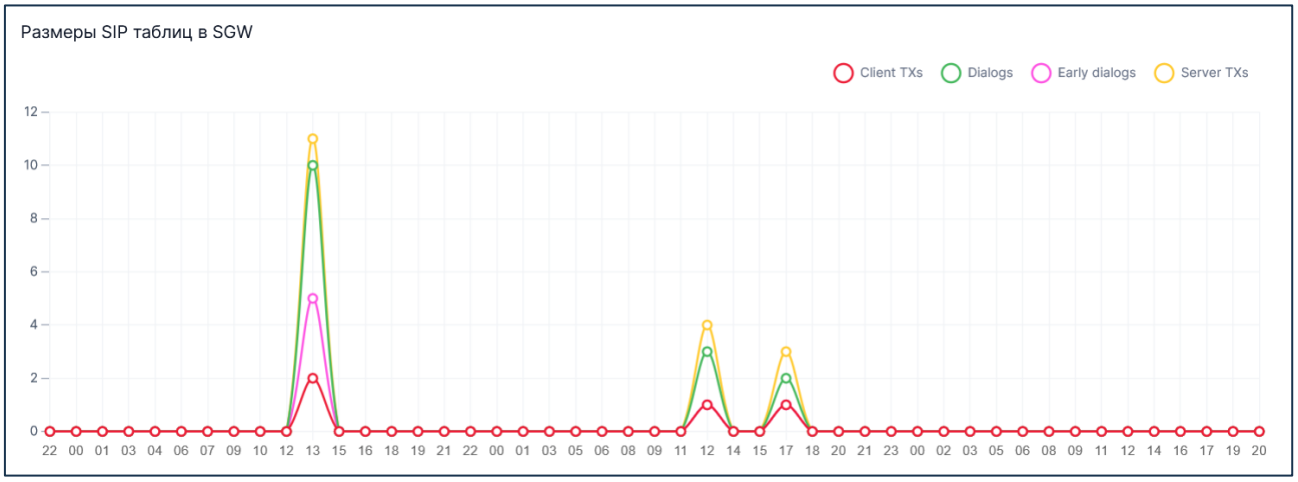

Рисунок 165. График Размеры SIP таблиц в SGW

- кривая **Client TXs** – отображает число SIP-транзакций от клиента к серверу
- кривая **Dialogs** – отображает текущие активные SIP-диалоги
- кривая **Early dialogs** – отображает текущие активные SIP-диалоги
- кривая **Server TXs** – отображает число SIP-транзакций от сервера к клиенту

> Значение **Dialogs** зависит от ретроспективы в соответствии с историей использования. **Рост числа активных диалогов** может означать DDoS-атаку по протоколу SIP

2 график **SGW вызовы** Рисунок 166 показывает количество SGW-вызовов в зависимости от протокола в реальном времени на следующих кривых:

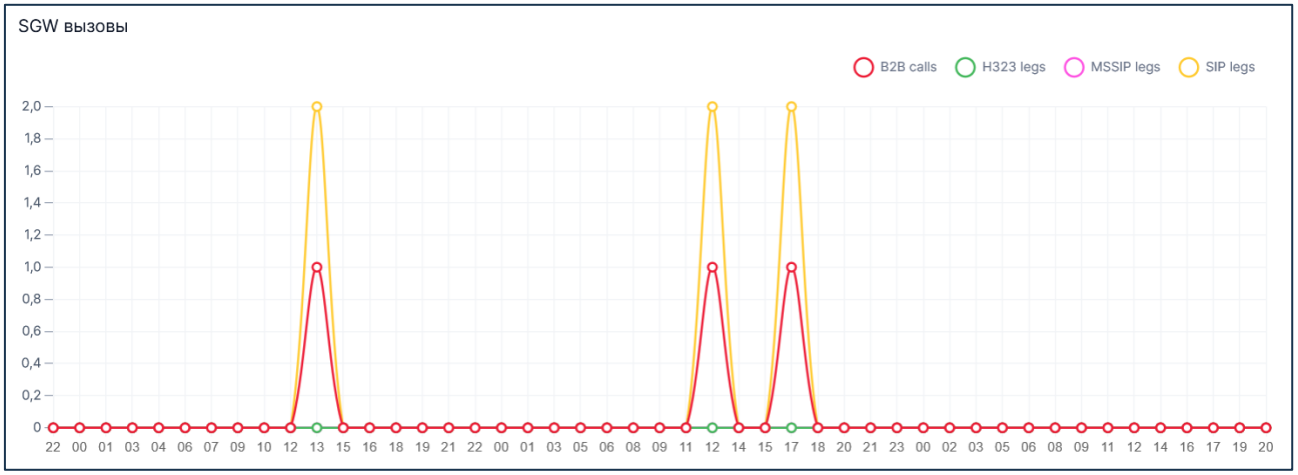

Рисунок 166. График SGW вызовы

- кривая **B2B calls** – отображает количество полностью активных звонков (установлено соединение между внешним и внутренним контуром)
- кривая **H.323 legs** – отображает количество активных звонков между сервером и клиентами по протоколу H.323 (полностью установленный звонок между внешним и внутренним контуром требует двух активных звонков между сервером и клиентами)
- кривая **MSSIP legs** – отображает количество активных звонков между сервером и клиентами по протоколу MSSIP
- кривая **SIP legs** – отображает количество активных звонков между сервером и клиентами по протоколу SIP

> График **SGW вызовы** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Увеличение количества активных звонков** может означать DDoS-атаку по соответствующему протоколу

3 график **SGW вызовы в секунду** Рисунок 167 показывает количество обрабатываемых или инициируемых gateway SGW-вызовов в течение одной секунды в зависимости от протокола в реальном времени на следующих кривых:

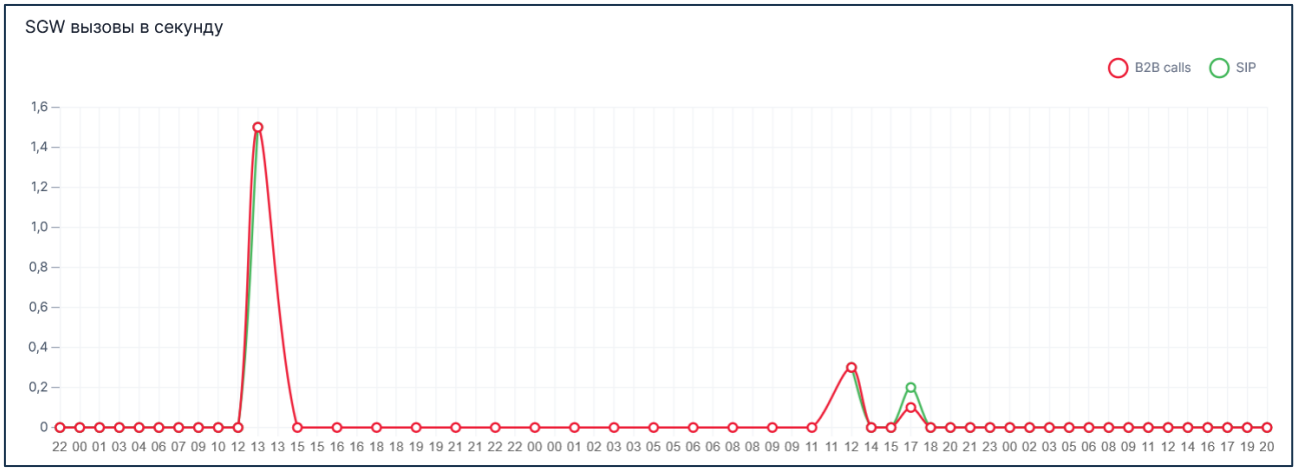

Рисунок 167. График SGW вызовы в секунду

- кривая **B2B calls** – отображает количество полностью активных вызовов в течении одной секунды
- кривая **SIP** – отображает количество SIP-вызовов в течении одной секунды

> График **SGW вызовы в секунду** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Увеличение количества активных звонков** может означать DDoS-атаку по соответствующему протоколу

4 график **Число SIP регистраций по доменам** Рисунок 168 показывает количество SIP-регистраций по доменам в реальном на кривых **<Название / IP-адрес домена>**

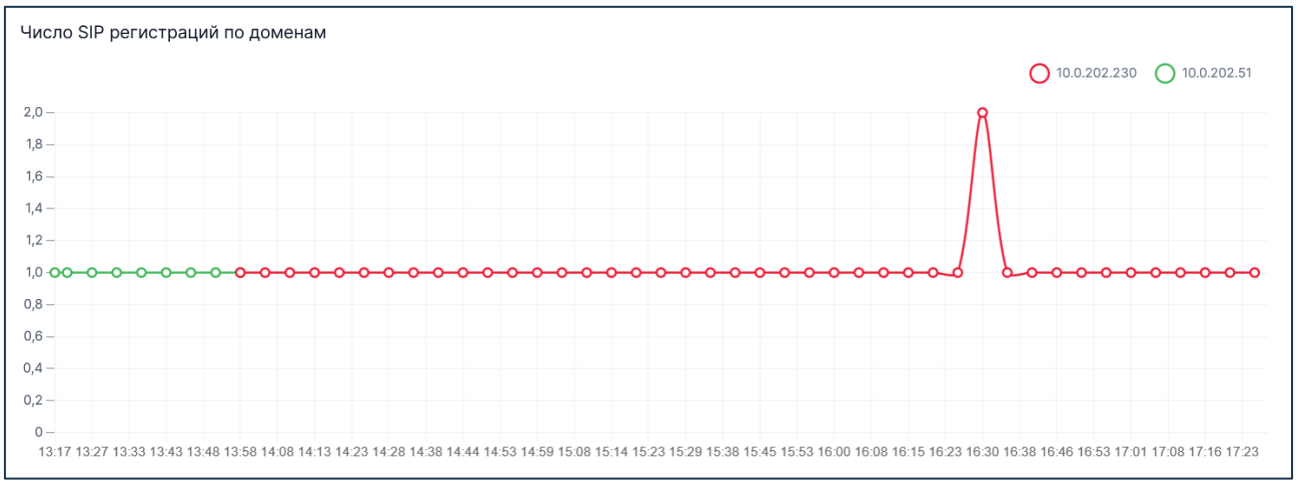

Рисунок 168. График Число SIP регистраций по доменам

> График **Число SIP регистраций по доменам** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Увеличение числа активных SIP-регистраций** может означать DDoS-атаку по соответствующему протоколу (если их значительно больше, чем ожидается) и потенциальную утечку данных учётных записей пользователей

Вкладка TURN-сервер

На вкладке **TURN-сервер** для сервера проксирования отображаются следующие графики:

1 график **Активные соединения** Рисунок 169 показывает количество активных TURN-соединений в реальном времени на кривой **turn_connections**

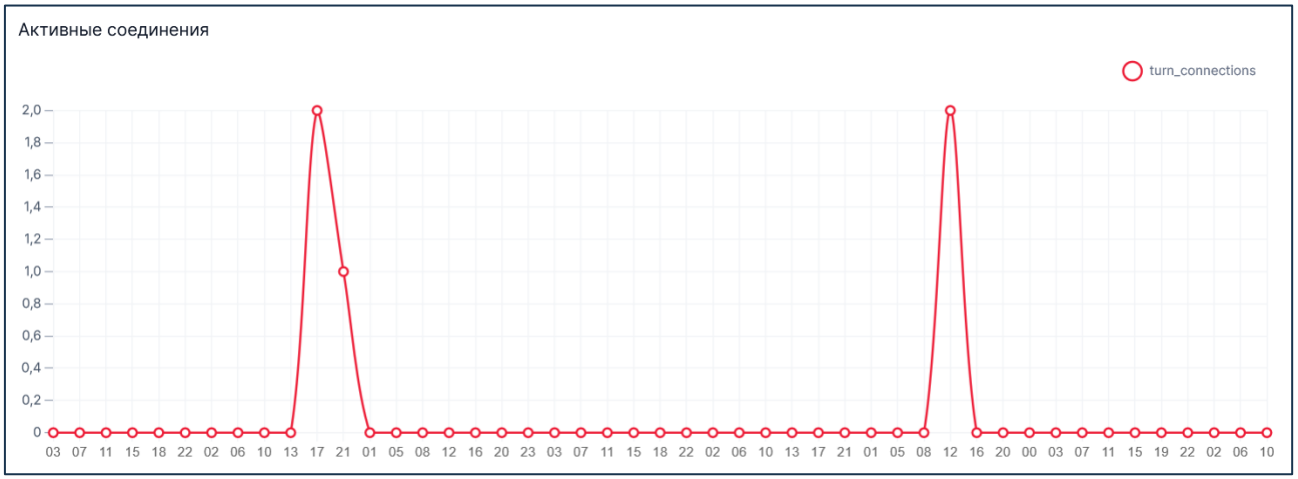

Рисунок 169. График Активные соединения

> График **Активные соединения** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Число TURN-соединений** не должно превышать удвоенное число участников в рамках WebRTC-конференций

2 график **Объём входящего трафика, Кб** Рисунок 170 показывает объём входящего трафика от TURN-сервера в реальном времени на кривых **all**, **<IP-адрес сервера>**

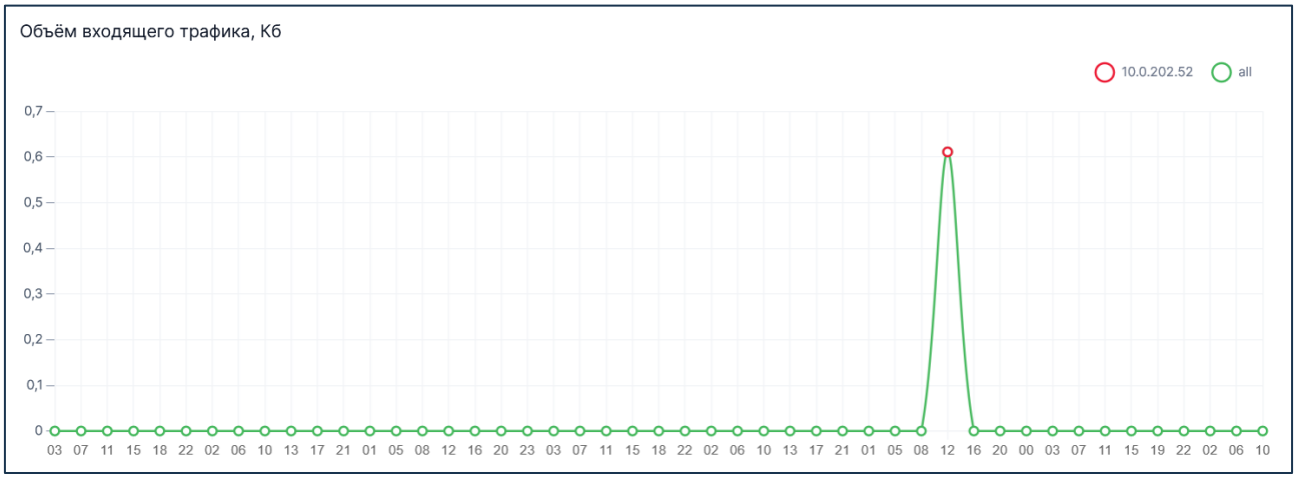

Рисунок 170. График Объём входящего трафика, Кб

> График **Объём входящего трафика** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Объём входящего трафика** при корректной работе не должен быть больше, чем число пользователей в WebRTC конференциях, умноженное на 1 Мбит/с

3 график **Объём исходящего трафика, Кб** Рисунок 171 показывает объём исходящего трафика от TURN-сервера в реальном времени на кривых **all**, **<IP-адрес сервера>**

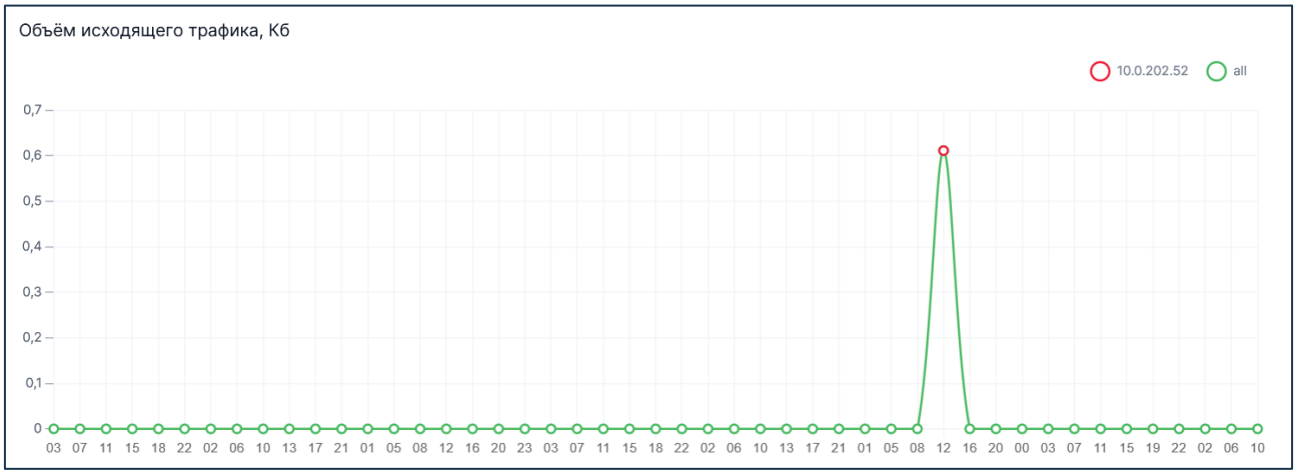

Рисунок 171. График Объём исходящего трафика, Кб

> График **Объём исходящего трафика** используется для комплексной оценки работы системы (обычное значение зависит от ретроспективы в соответствии с историей использования).
> **Объём исходящего трафика** при корректной работе не должен быть больше, чем число пользователей в WebRTC конференциях, умноженное на 2 Мбит/с

Обновление системы

IVA SBC предоставляет возможность обновления системы до последней версии.

Настройка параметров подключения к серверу обновлений

Для обновления системы необходимо настроить сервер обновлений, на котором будут размещены новые версии программного обеспечения серверов.

> Сервер обновления должен быть доступен со всех серверов IVA SBC, включая сервер управления и конфигурации, а также все добавленные сервера проксирования, по одному из протоколов: **http, https, smb, cifs, nfs, s3, s3s**

Чтобы добавить / редактировать адрес сервера обновления IVA SBC, необходимо:

1 перейти в раздел **Обновление системы** Рисунок 172 и нажать кнопку **Редактировать**

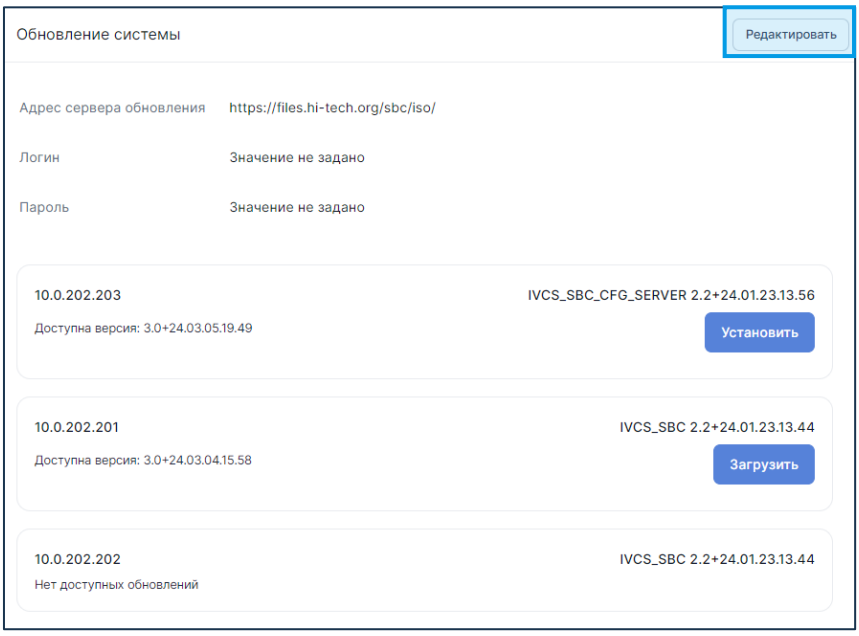

Рисунок 172. Обновление системы

2 в окне **Редактирование параметров обновления** Рисунок 173:

- Адрес сервера обновления: ввести URI сервера обновления, с которого будут доступны обновления для серверов проксирования и сервера управления и конфигурации (например https://files.hi-tech.org/sbc/iso/)
- Логин: ввести логин для доступа к серверу обновлений (например ivcs)
- Пароль: ввести пароль для доступа к серверу обновлений (например ivcs)

3 нажать кнопку Сохранить

При настройке HTTP-сервера обновления необходимо разместить на нем корректный JSON-файл index.json следующего формата:

```
[
   {
      "file" : " iva-sbc-cfg-server-live_4.0.iso",
      "size" : 700448768
   },
   {
      "file" : " iva-sbc-live_4.0.iso",
      "size" : 638582784
   }
]
```

После сохранения изменений осуществляется проверка доступности указанного сервера обновлений, а также проводится проверка на наличие доступных обновлений.

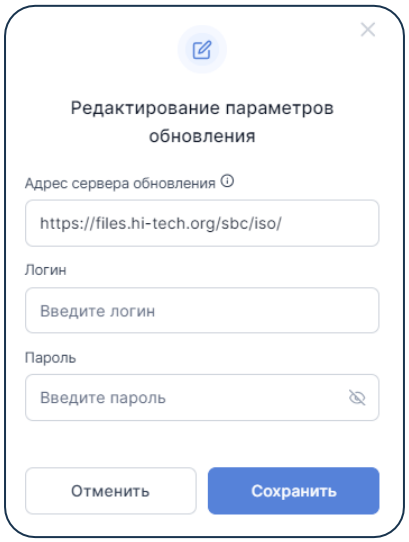

Рисунок 173. Редактирование параметров обновления системы

Если на сервере уже установлена последняя версия, то в строке с этим сервером будет отображено сообщение Нет доступных обновлений Рисунок 172.

Если для сервера доступна новая версия программного обеспечения, в строке с этим сервером активируется кнопка Загрузить Рисунок 172.

Если сервер обновлений не доступен, то будет отображено оповещение о недоступности сервера Рисунок 174.

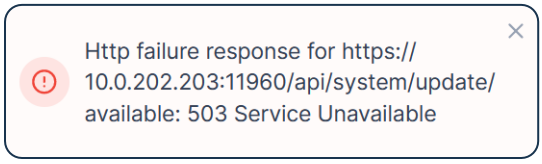

Рисунок 174. Оповещение о недоступности сервера обновлений

Обновление серверов IVA SBC

Чтобы обновить сервер, необходимо:

1 нажать кнопку Загрузить, после чего начнется загрузка файлов обновления. После успешной загрузки станет доступна кнопка Установить Рисунок 172

> Загрузка файлов обновления может занять продолжительное время

2 нажать кнопку Установить, чтобы запустить процесс установки обновления. По завершении обновления активируется кнопка Перезапустить

3 нажать кнопку Перезапустить для перезагрузки сервера, на который установлено обновление

Резервное копирование и восстановление

IVA SBC предоставляет возможность создавать резервную копию настроек системы. Резервная копия может использоваться для восстановления или переноса на другой сервер IVA SBC.

Настройка подключения к хранилищу резервных копий

Для сохранения резервных копий необходимо настроить адрес хранилища резервных копий, на котором будут храниться резервные копии базы данных системы IVA SBC.

> Сервер хранилища резервных копий должен быть доступен только с сервера управления и конфигурации

Чтобы добавить адрес хранилища резервных копий, необходимо:

1 перейти в раздел **Резервное копирование и восстановление** и нажать кнопку **Редактировать** Рисунок 175

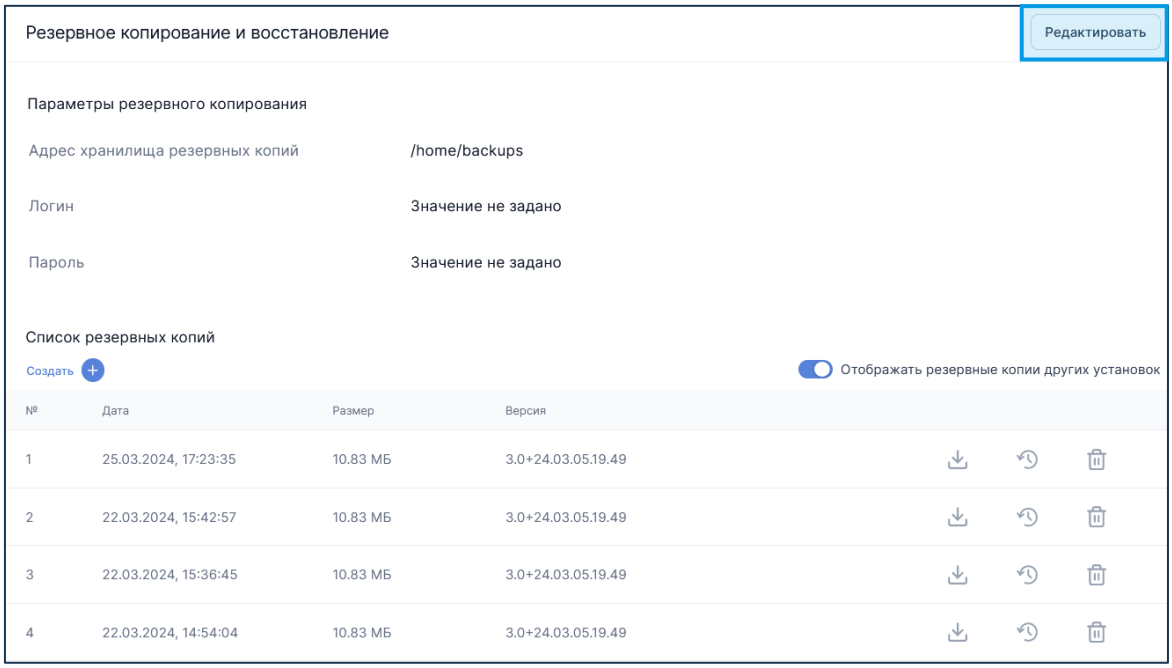

Рисунок 175. Раздел Резервное копирование и восстановление

2 в окне **Редактирование параметров резервного копирования** Рисунок 176 ввести:

- **Адрес хранилища резервных копий**: ввести URI сервера резервного копирования (например **/home/backup**), на котором будут храниться созданные резервные копии
- **Логин**: ввести логин для доступа к серверу резервных копий (например **ivcs**)
- **Пароль**: ввести пароль для доступа к серверу резервных копий (например **ivcs**)

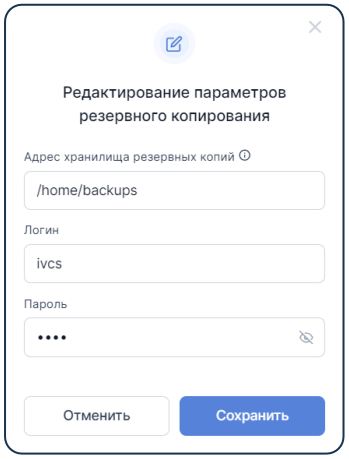

Рисунок 176. Редактирование параметров резервного копирования

Создание резервной копии

Чтобы создать резервную копию, необходимо: в разделе **Резервное копирование и восстановление** Рисунок 175 нажать кнопку **Создать** +

Созданная резервная копия будет отображена в списке резервных копий Рисунок 175.

Чтобы посмотреть резервные копии других установок IVA SBC, необходимо: нажать **переключатель Отображать резервные копии других установок**

Восстановление и удаление резервной копии

Для **восстановления резервной копии** необходимо: в разделе **Резервное копирование и восстановление** Рисунок 175 выбрать ранее созданную резервную копию и **нажать кнопку** Рисунок 177.

> После восстановления резервной копии все активные пользователи автоматически выйдут из системы и будут перемещены на страницу **Входа в систему** Рисунок 2

Для **удаления резервной копии** необходимо: в разделе **Резервное копирование и восстановление** Рисунок 175 выбрать созданную резервную копию и **нажать** кнопку Рисунок 177.

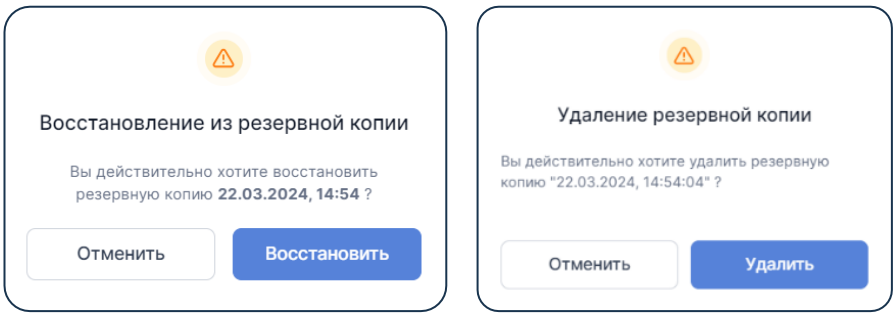

Рисунок 177. Восстановление и удаление резервной копии

Контроль целостности системы

В разделе **Контроль целостности системы** Рисунок 178 отображаются все изменения базовой версии (версия системы после установки / обновления) файловой системы серверов проксирования и сервера управления и конфигурации, содержится информацию о пути, типе, размере, владельце и разрешениях для проведённых изменений в системе.

Список изменений в файловой системе отсортирован по дате изменения.

Раздел **Контроль целостности системы** позволяет выполнить следующие действия:

- просматривать изменения в файловой системе
- скачать все изменения в файловой системе в виде SquashFS: нажать кнопку **Скачать**
- восстановить файловую систему

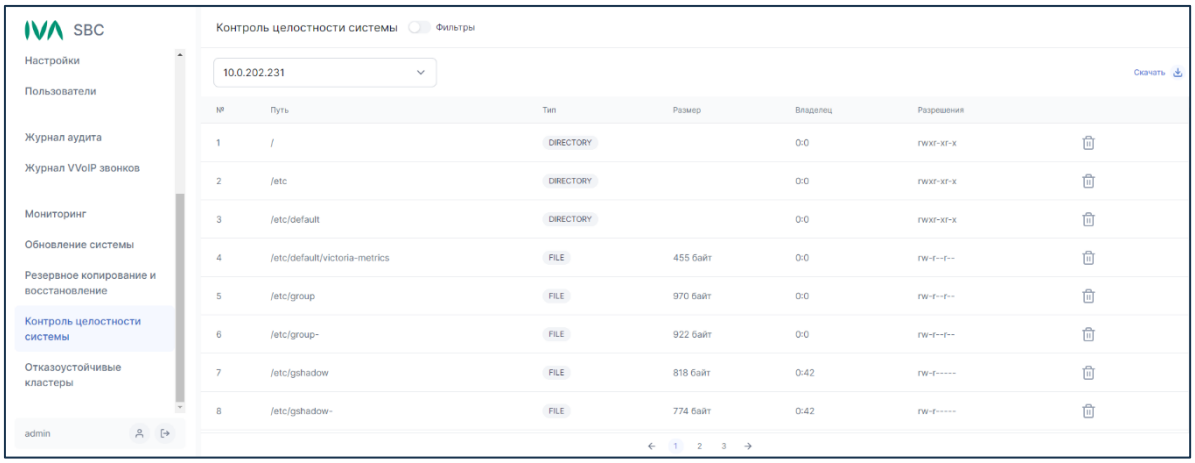

Рисунок 178. Раздел контроль целостности системы

Просмотр изменений в файловой системе

В разделе **Контроль целостности системы** Администратор может настроить фильтр отображения списка изменений в файловой системе серверов. Чтобы настроить фильтр, необходимо: в выпадающем списке выбрать **сервер IVA SBC** и нажать **переключатель Фильтры** Рисунок 179.

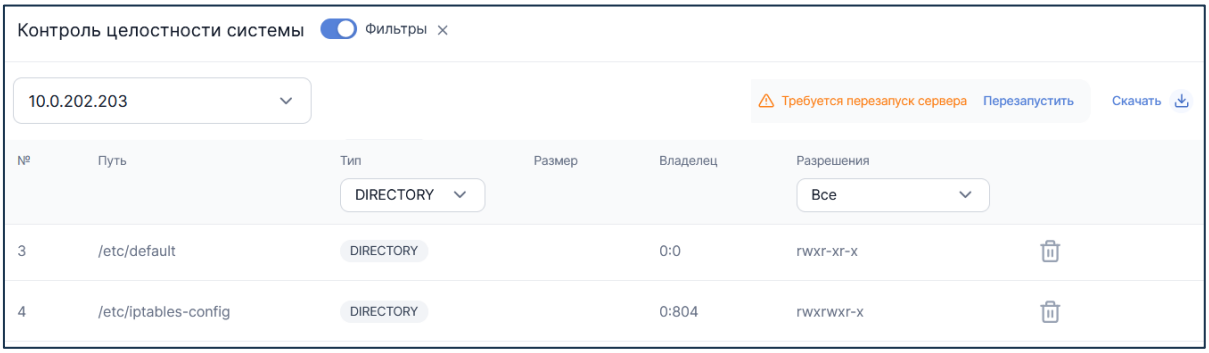

Рисунок 179. Фильтр списка изменений в файловой системе

Скачивание изменений в файловой системе

Чтобы скачать все изменения в файловой системе в формате SquashFS, необходимо:

1 в разделе Контроль целостности системы Рисунок 178 выбрать сервер IVA SBC и нажать кнопку Скачать

2 файл (в формате *.squashfs) со списком изменений файловой системы сохранится в загрузке браузера

Восстановление файловой системы

Чтобы отменить изменения в файловой системе и восстановить исходное состояние, необходимо:

1 перейти в раздел Контроль целостности системы Рисунок 178

2 выбрать файл с изменением и нажать кнопку

3 в окне Удаление файла нажать кнопку Удалить

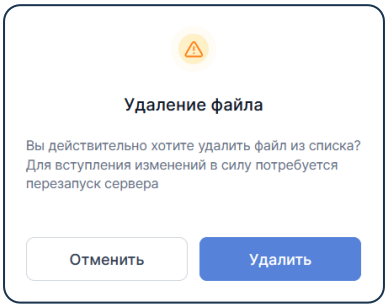

Рисунок 180. Удаление изменений в файловой системе

4 нажать ссылку Перезапустить Рисунок 179 и в окне Перезагрузка сервера Рисунок 181 нажать кнопку Перезапустить

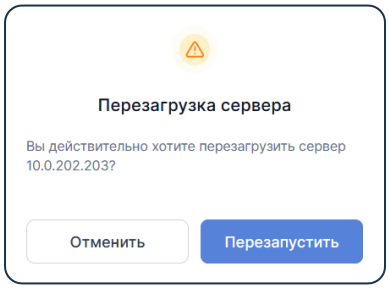

Рисунок 181. Перезагрузка сервера

Отказоустойчивые кластеры

IVA SBC позволяет создавать кластеры и настраивать плавающие IP-адреса, переходящие между серверами проксирования.
Плавающий IP-адрес можно назначить на несколько серверов проксирования. При отключении одного из серверов, являющихся узлом кластера, плавающий IP-адрес будет использоваться на другом сервере проксирования в этом кластере.

> В качестве технологии в отказоустойчивом кластере используются протокол VRRP и сервис keepalived

В разделе **Отказоустойчивые кластеры** Рисунок 182 отображается информация о созданных кластерах:

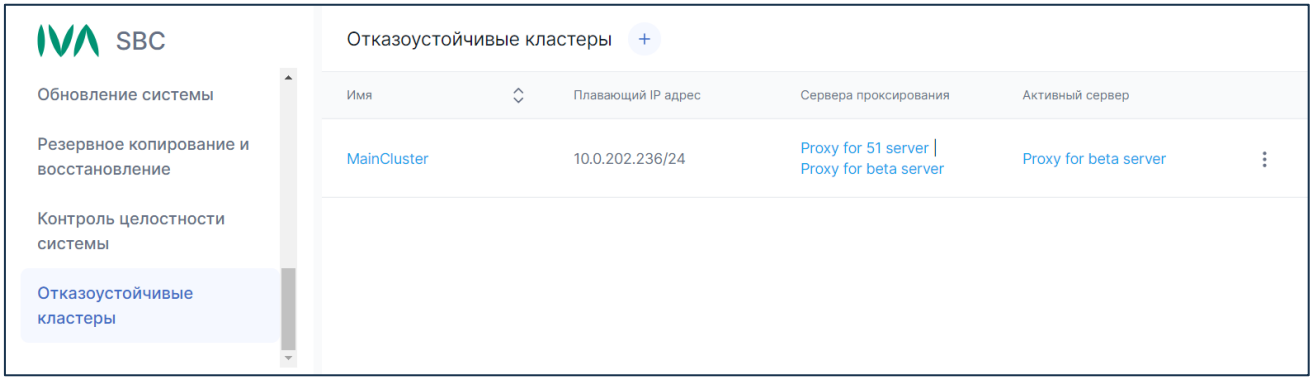

Рисунок 182. Отказоустойчивые кластеры

- **Имя** – имя кластера, используемое для описания
- **Плавающий IP адрес** – плавающий IP-адрес кластера и подсеть данного IP-адреса
- **Сервера проксирования** – список серверов проксирования, на которых может использоваться плавающий IP-адрес
- **Активный сервер** – сервер, на котором в данный момент используется плавающий IP-адрес

При работе в разделе **Отказоустойчивые кластеры** можно:

- добавить кластер: нажать кнопку **Создать кластер** +
- редактировать описание кластера: нажать кнопку ⋮ и выбрать Редактировать Рисунок 184
- удалить кластер: нажать кнопку ⋮ и выбрать Удалить Рисунок 185

- редактировать список узлов кластера: нажать ссылку <Имя кластера>
- перейти к информации о сервере проксирования: нажать ссылку <Имя сервера проксирования>

Создание отказоустойчивого кластера

Чтобы создать отказоустойчивый кластер:

1 перейти в раздел **Отказоустойчивые кластеры** Рисунок 182 и **нажать кнопку** +

2 в окне **Создание кластера** Рисунок 183:

- **Имя:** ввести имя кластера (рекомендуется вводить имя, которое кратко описывает назначение или плавающий IP-адрес, например **MainCluster**)
- **Плавающий IP-адрес**: ввести плавающий IP-адрес и маску подсети (например 10.0.202.236/24)

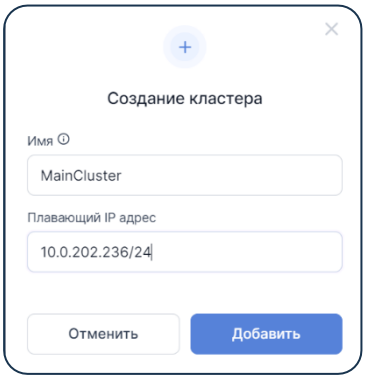

Рисунок 183. Создание кластера

После создания кластера необходимо настроить список узлов кластера, между которыми может переходить заданный плавающий IP-адрес.

Редактирование описания кластера

Чтобы **редактировать описание кластера**:

1 **нажать кнопку** ⋮ и выбрать **Редактировать**

2 в окне **Редактирование кластера** Рисунок 184 внести изменения

3 нажать кнопку **Сохранить**

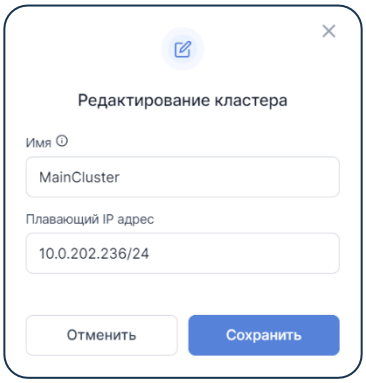

Рисунок 184. Редактирование кластера

Удаление кластера

Чтобы **удалить кластер**:

1 **нажать кнопку** ⋮ и выбрать **Удалить**

2 в окне **Удаление кластера** Рисунок 185 нажать кнопку **Удалить**

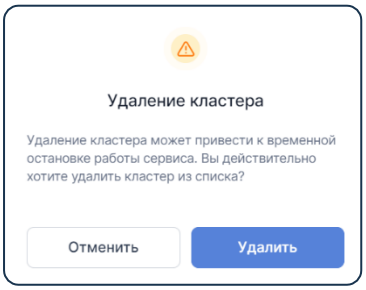

Рисунок 185. Удаление кластера

Настройка узлов кластера

Информация о кластере

Добавление и редактирование узлов кластера проводится на странице **Информация о кластере** Рисунок 186:

Перейти в раздел **Отказоустойчивые кластеры** и нажать ссылку <**Имя кластера**>

Рисунок 186. Информация о кластере

При работе на странице **Информация о кластере** можно:

- посмотреть список и параметры **узлов кластера**
- добавить узел кластера: нажать кнопку **Добавить**
- редактировать узел кластера: **нажать кнопку**
- удалить узел из кластера: **нажать кнопку**
- редактировать описание кластера: нажать кнопку **Редактировать**
- удалить кластер: **нажать кнопку** и выбрать **Удалить**

Добавление узла кластера

Узел кластера – это сервер проксирования, на котором может использоваться плавающий IP-адрес кластера.

Чтобы добавить узел кластера:

1 на странице **Информация о кластере** Рисунок 186 нажать кнопку **Добавить**

2 в окне **Добавление узла кластера** Рисунок 187:

- **Сервер проксирования**: выбрать сервер проксирования, который должен участвовать в кластере
- **Интерфейс для плавающего IP**: выбрать интерфейс, на котором будет назначен плавающий IP-адрес
- **Служебный интерфейс**: выбрать интерфейс, который будет использоваться для служебного обмена данными VRRP
- **Служебный IP**: ввести IP-адрес, который будет использоваться для служебного обмена данными VRRP

- **Роль**: выбрать роль сервера в кластере по умолчанию (MASTER, SLAVE). Назначить роль MASTER можно только одному серверу проксирования в кластере.

3 нажать кнопку **Добавить**

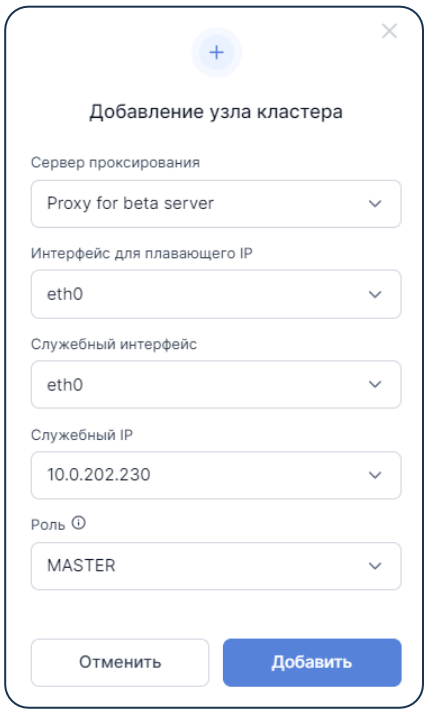

Рисунок 187. Добавление узла кластера

Редактирование узла кластера

На странице Информация о кластере Рисунок 186 можно **редактировать** параметры узлов кластера:

1 выбрать **сервер проксирования** в группе кластера, параметры которого необходимо редактировать, и **нажать кнопку**

2 в окне **Редактирование узла кластера** Рисунок 188: внести изменения (описание полей приведено в разделе Добавление узла кластера)

3 нажать кнопку **Сохранить**

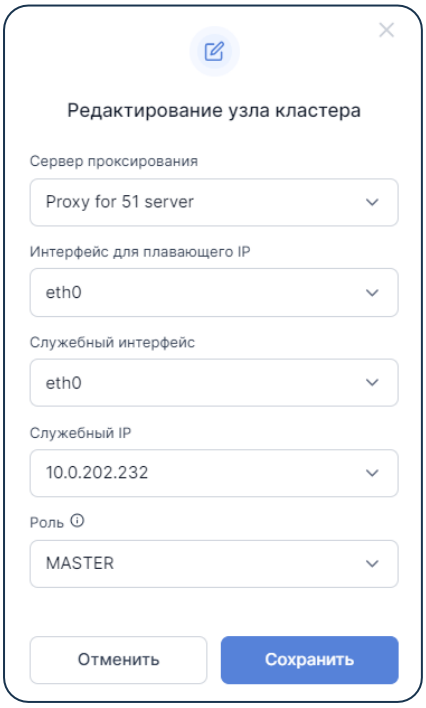

Рисунок 188. Редактирование узла кластера

Удаление узла кластера

На странице Информация о кластере Рисунок 186 можно удалить узел из группы кластера

1 выбрать **сервер проксирования**, который нужно удалить, и **нажать кнопку**

2 в окне **Удаление узла** Рисунок 189 нажать кнопку **Удалить**

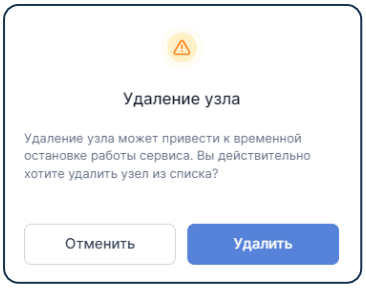

Рисунок 189. Удаление узла кластера

Выход из системы

Для выхода из системы необходимо: **в Web-панели администрирования нажать кнопку** Рисунок 190

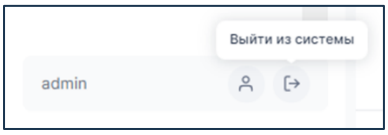

Рисунок 190. Выход из системы

> Выход из системы происходит без подтверждения

Дисковое пространство

В этом разделе описывается, как рассчитать необходимый объём дискового пространства для установки серверов IVA SBC.

Расчёт общего объёма дискового пространства

В расчёте общего объёма дискового пространства учитываются следующие файлы системы:

- переменные данные
- операционная система — 3 ГБ
- временные данные — 2 ГБ
- обновления системы — 2 ГБ
- резервные копии, если они хранится локально. Рекомендуется хранить резервные копии на выделенном сервере

Рекомендуемый минимальный размер диска для сервера проксирования — 13 ГБ без учёта резервных копий.

Рекомендуемый минимальный размер диска для сервера управления и конфигурации — 16 ГБ без учёта резервных копий.

Расчёт объёма переменных данных

Система IVA SBC хранит несколько видов переменных данных:

Данные	Процессы	Расположение
Логи	См. Логи системы	См. Логи системы
Журналы аудита в БД	sbc-cfg-server	/var/lib/postgresql/13/main на сервере управления и конфигурации
Данные счётчиков VictoriaMetrics	victoria-metrics	/var/lib/victoria-metrics на каждом сервере IVA SBC

Расчёт объёма журналов аудита в БД

Необходимый объём диска для каждого типа события вычисляется по формуле:

Объем записи × Количество записей в день × Количество дней хранения

Тип события	Время хранения	Объем записи	Необходимый объем диска
События звонков	30 дней	около 1 КБ	3 ГБ при одной попытке звонка в секунду
События аудита	30 дней	около 2 КБ	120 ГБ при 2000 записях аудита в день

Расчёт объёма переменных данных сервера проксирования

Тип данных	Параметры	Размер
Общие логи	—	2,7 ГБ
Логи модулей сервера проксирования	—	1,7 ГБ
Данные счетчиков VictoriaMetrics	Время хранения — 1 месяц	1 ГБ
		Итого: 5,4 ГБ

Расчёт объёма переменных данных сервера управления и конфигурации

Тип данных	Параметры	Размер
Общие логи	—	2,7 ГБ
Логи модулей сервера управления и конфигурации	—	1,61 ГБ
Данные счетчиков VictoriaMetrics	Время хранения — 1 месяц	1 ГБ
События аудита	Число сообщений — 2 000 шт. в день	0,12 ГБ

Тип данных	Параметры	Размер
	Время хранения — 1 месяц	
События звонков	Число звонков — 90 000 шт. в день Время хранения — 1 месяц	3 ГБ

Итого: 8,5 ГБ

Методы API в IVA SBC

REST API предоставляет доступ к функциям IVA SBC и используется для управления сервером через web-интерфейс администратора.

Доступ к API

Описание методов REST API доступно по адресу:

https://<SBC_CFG_IP>:11960/api/doc#section/Introduction

где <SBC_CFG_IP> — фактический адрес сервера управления и конфигурации IVA SBC.

Приложения

Настройки проксирования для Платформы IVA MCU

В приложении описана настройка VoIP, HTTP Reverse, TURN и HTTP Proxy маршрутизации в IVA SBC для платформы IVA MCU.

Перед настройкой маршрутизации в IVA SBC необходимо:

- подготовить IP-адреса добавляемых серверов:
  - IVA_MCU_IP, IVA_MCU_IP2 – IP-адреса головных серверов IVA MCU
  - IVA_MCU_FLOAT_IP – плавающий IP-адрес головного сервера для кластера
  - IVA_MEDIA_IP – IP-адрес медиасервера IVA MCU (может быть несколько)
- добавить сервер проксирования
- подготовить и добавить SSL-сертификаты для доменных имён

Настройка маршрутизации VoIP

Ниже приведен пример настройки сервера проксирования IVA SBC для маршрутизации исходящего и входящего SIP- и H.323-трафика головного сервера IVA MCU с IP-адресом 10.0.202.51.

Чтобы настроить сервер проксирования для маршрутизации VoIP-трафика, необходимо:

1 войти в Web-интерфейс администрирования IVA SBC

2 в разделе Маршруты VoIP добавить маршрут (см. Добавление маршрута VoIP), задав имя и описание, например:

- Имя: 51 Server IVA MCU (In/Out)
- Описание: VoIP правила для 51 Server IVA MCU

3 в окне Информация о маршруте VoIP добавить правило обработки SIP-регистрации (см. Правила обработки маршрута VoIP. Обработка SIP-регистрации) со следующими параметрами:

- Домен SIP регистрации: sip.iva.ru
- Адрес SIP регистратора: IVA_MCU_IP или IVA_MCU_FLOAT_IP (10.0.202.51)
- Транспорт: По умолчанию

4 в окне Информация о маршруте VoIP добавить правила (см. Правила обработки маршрута VoIP. Обработка входящего звонка) со следующими параметрами:

- правило для исходящих SIP-вызовов с заданной маской сети:
  - **Включено**: кнопка-переключатель активна
  - **Имя:** SIP from 51 Server IVA MCU
  - **Протокол**: SIP
  - **Маска сети входящего соединения** (входящие звонки со стороны IVA MCU в интернет): IVA_MCU_IP/32, IVA_MCU_FLOAT_IP/32, IVA_MCU_IP2/32
  - **Статус регистрации**: Любой
  - **Действие**: Вызвать
  - **Использовать DNS SRV записи**: активно
  - **Проксировать RTP**: активно
  - **Транспорт:** По умолчанию
- правило для входящих SIP-вызовов с любых адресов:
  - **Включено**: кнопка-переключатель активна
  - **Имя**: SIP To 51 Server IVA MCU from Any
  - **Протокол**: SIP
  - **Статус регистрации**: Любой
  - **Действие**: Проксировать, ввести IP-адрес головного сервера IVA_MCU_IP или IVA_MCU_FLOAT_IP
  - **Проксировать RTP**: активно
  - **Транспорт**: По умолчанию
- аналогичные правила (H.323 from 51 Server IVA MCU и H.323 To 51 Server IVA MCU) для протокола H.323. **Для H.323-вызовов** дополнительно настроить:
  - **Использовать туннелирование**: активно

> Правила применяются в порядке очереди. **Важно**, чтобы правило **SIP from 51 Server IVA MCU** и правило **H.323 from 51 Server IVA MCU** применялись в первую очередь

5 в разделе **Группы маршрутизации** создать группу маршрутизации (см. Настройка групп маршрутизации) с параметрами:

- **Имя**: VoIP 51 Server IVA MCU
- **Описание**: Список маршрутов Voip для 51 Server IVA MCU

- **Тип**: VVoIP Proxy

6 в окне Информация о группе маршрутизации VVoIP добавить созданный маршрут (см. Создание группы маршрутизации) 51 Server IVA MCU (In/Out)

7 в разделе **Сервера проксирования** выбрать сервер проксирования

8 в окне Информация о сервере проксирования для роли **VVoIP** выбрать группу маршрутизации (VVoIP 51 Server IVA MCU) и активировать роль (см. Добавление Ролей проксирования)

9 в окне Информация о сервере проксирования на вкладке **Правила NAT** добавить правила NAT (см. Добавление правил NAT)

10 войти в **Web-интерфейс администрирования** Платформы IVA MCU:

- в разделе Системные настройки выбрать секцию Настройки VVoIP Рисунок 191 и настроить параметры:
  - **Прокси исходящего sip-звонка:** IP-адрес сервера проксирования IVA SBC (например 10.0.202.201)
  - **Прокси исходящего H.323 звонка:** IP-адрес сервера проксирования IVA SBC (например 10.0.202.201)
  - **Локальные сети без прокси**: IP-адреса локальной сети, в которые звонки осуществляются без использования сервера проксирования IVA SBC (например 127.0.0.1;10.0.0.1/24)
  - проверить отсутствие / отключить **настройки NAT** адресации платформы IVA MCU на странице **Внешние IP** раздела **Настройки сервера**, так как применяются Правила NAT, настроенные для сервера проксирования IVA SBC

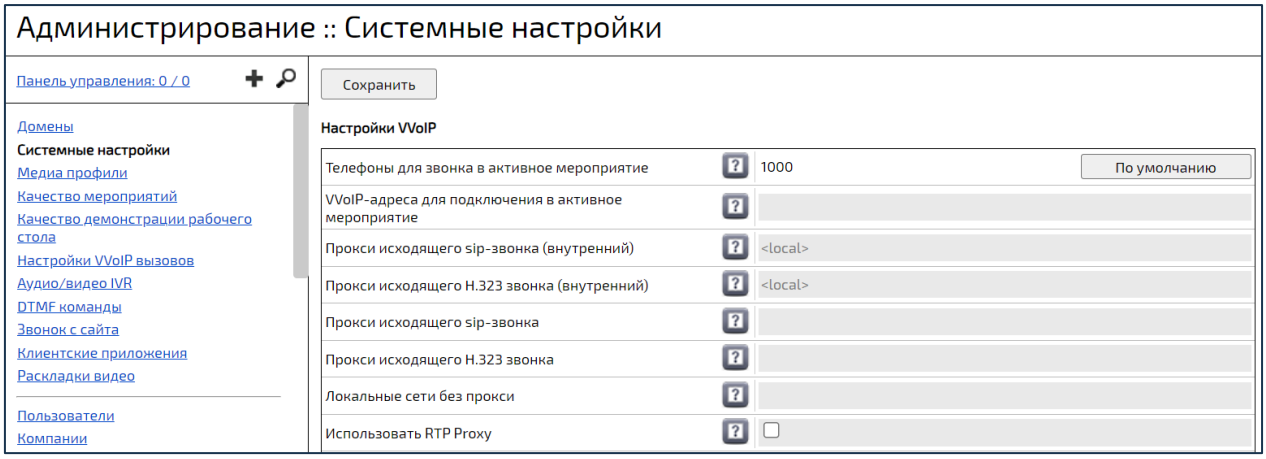

Рисунок 191. Настройки VVoIP в IVA MCU

Настройка маршрутизации HTTP Reverse

Пример настройки для ограничения доступа к web-интерфейсу администрирования

Ниже приведен пример настройки сервера проксирования IVA SBC для ограничения входящих HTTP-запросов к web-интерфейсу администрирования головного сервера IVA MCU с IP-адресом **10.0.202.51**.

Чтобы настроить сервер проксирования для маршрутизации трафика HTTP Reverse, необходимо:

1 войти в **Web-интерфейс администрирования** IVA SBC

2 в разделе **Маршруты HTTP Reverse** на вкладке **Правила фильтрации** добавить правило фильтрации (см. Добавление правил фильтрации маршрутов HTTP Reverse), задав имя, например: **IVA MCU no admin and allow all others**

3 в окне Информация о правиле фильтрации HTTP добавить и упорядочить фильтры (см. Добавление и редактирование фильтров для правила фильтрации маршрутов HTTP Reverse) со следующими параметрами:

- фильтр для запрета доступа на страницу web-интерфейса администрирования:
  - **URL-путь:** /administration/(.*)
  - **Метод**: Любой
  - **Действие**: Запретить
- фильтр для доступа ко всем ресурсам Платформы IVA MCU:
  - **URL-путь:** (.*)
  - **Метод**: Любой
  - **Действие**: Разрешить

4 в разделе **Маршруты HTTP Reverse** на вкладке **Маршруты** добавить маршрут (см. Добавление маршрута HTTP Reverse), с параметрами:

- **Имя**: IVA MCU With No Admin To 51 Server
- **URL-адрес сервера**: URL-адрес сервера проксирования IVA SBC (например iva51.hi-tech.org)
- **Адрес внутреннего сервера**: IVA_MCU_IP или IVA_MCU_FLOAT_IP (**10.0.202.51**)

5 в окне Информация о маршруте HTTP Reverse добавить созданное правило фильтрации (см. Добавление правил фильтрации в список правил фильтрации маршрута HTTP Reverse) IVA MCU no admin and allow all others

6 в разделе Группы маршрутизации создать группу маршрутизации (см. Настройка групп маршрутизации) с параметрами:

- Имя: HTTP to 51 Server IVA MCU
- Описание: Список маршрутов HTTP для 51 Server IVA MCU
- Тип: HTTP Reverse Proxy

7 в окне Информация о группе маршрутизации HTTP добавить созданный маршрут HTTP (см. Создание группы маршрутизации) IVA MCU With No Admin To 51 Server

8 в разделе Сервера проксирования выбрать сервер проксирования

9 в окне Информация о сервере проксирования для роли HTTP Reverse выбрать группу маршрутизации (HTTP to 51 Server IVA MCU) и активировать роль (см. Добавление Ролей проксирования)

Пример настройки для обеспечения доступа к IVA MCU

Ниже приведён пример настройки фильтрации REST API для работы с IVA MCU. Эти настройки необходимы для обеспечения доступа к ресурсам IVA MCU.

Описанная настройка фильтрации обеспечит корректную работу:

- новой версии web-интерфейса
- IVA Connect Desktop
- IVA Connect Android
- IVA Connect iOS

Описанная настройка фильтрации не поддерживает работу:

- старой версии web-интерфейса
- iframe
- администрирования IVA MCU через IVA SBC
- чат-ботов
- интеграционного API

- SOAP API

> Все запросы, которые не соответствуют установленным правилам фильтрации, будут блокироваться.

Чтобы настроить фильтрацию REST API для работы с IVA MCU, необходимо:

- загрузить OpenAPI-схемы
- настроить правила фильтрации

Загрузка OpenAPI-схем

Для корректной работы правил фильтрации необходимо добавить несколько OpenAPI-схем (см. Добавление схем OpenAPI).

Имя схемы	URL для загрузки схемы
ClientAPI	http://<INTERNAL_ADDRESS_IVAMCU>/doc/api/clients-openapi.json, где <INTERNAL_ADDRESS_IVAMCU> — IP-адрес сервера IVA MCU
Resource	Доступен по запросу в техподдержку: https://sd.iva.ru/
Comet	Доступен по запросу в техподдержку: https://sd.iva.ru/

Настройка правил фильтрации

Существует два способа настройки правил фильтрации:

- Использование готового правила

Для упрощения настройки фильтрации можно использовать готовый файл с набором фильтров. Для этого необходимо:

1. получить файл по запросу в техподдержку: https://sd.iva.ru/
2. импортировать файл на странице **Правила фильтрации** (см. Импортирование правила фильтрации)
3. перейти в добавленное из импортированного файла правило **IVA MCU Rules (New WEB)**
4. добавить в правило **IVA MCU Rules (New WEB)** фильтры (см. Добавление фильтра HTTP-запроса) по загруженным ранее OpenAPI-схемам:

№	Параметры				Назначение
	URL-путь	OpenAPI схема	Метод	Действие	
1	/comet?(.*)	Comet	—	—	Канал получения событий
2	/services/resource(.*)	Resource	—	—	Загрузка различных файлов
3	/api/rest/(.*)	ClientAPI	—	—	методы клиентского REST API

- Добавление правила вручную

Добавление правила фильтрации вручную позволит более гибко настроить входящие в него фильтры. Для этого необходимо:

1 добавить правила фильтрации (см. Добавление правила фильтрации HTTP-запросов):

   a. BASE_IVA_MCU
   б. IVA-MCU Patched
   в. IVA-MCU Block Std
   г. IVA-MCU Allow URI

> Важно соблюдать порядок добавления правил для их корректного применения (см. Изменение порядка применения фильтров)

2 в каждое правило фильтрации добавить фильтры (см. Добавление фильтра HTTP-запроса). Ниже приведён список фильтров, актуальных для IVA MCU версии 21.X:

Фильтры правила BASE_IVA_MCU:

№	Параметры				Назначение
	URL-путь	OpenAPI-схема	Метод	Действие	
Для работы страницы входа					
1	/	Не задана	GET	Разрешить	Открытие базовой страницы
2	/(favicon|favicon-loading).ico	Не задана	GET	Разрешить	Иконки для страницы, отображаемые в браузере

№	Параметры				Назначение
	URL-путь	OpenAPI-схема	Метод	Действие	
Для работы первого входа					
3	/common.js	Не задана	GET	Разрешить	JavaScript-код
4	/imaged_background.jpg	Не задана	GET	Разрешить	Фоновое изображение
5	/videoconference/(.*).js	Не задана	GET	Разрешить	JavaScript-файлы для отображения главной страницы
6	/fonts.css	Не задана	GET	Разрешить	CSS
7	/domain-theme/theme.css	Не задана	GET	Разрешить	CSS
8	/jwplayer/(.*).js	Не задана	GET	Разрешить	JS player
9	/eventsource/(.*).js	Не задана	GET	Разрешить	JS для получения событий через comet-канал
10	/fonts/Exo2Regular.(eot|ttf|woff)	Не задана	GET	Разрешить	Шрифты
11	/videoconference/service/login	Не задана	POST	Разрешить	Вызов GWT-методов для EndPoint для возможности автоматического входа в систему. На данный момент глубокого анализа данного запроса не выполняется. Отказ от данной точки планируется в будущих версиях IVA MCU
12	/videoconference/service/conferencesession	Не задана	POST	Разрешить	Вызов GWT методов для EndPoint для возможности автоматического входа в систему. На данный момент глубокого анализа данного запроса не выполняется.

№	Параметры				Назначение
	URL-путь	OpenAPI-схема	Метод	Действие	
					Отказ от данной точки планируется в будущих версиях IVA MCU
Статическая информация для работы нового web-интерфейса					
13	/v2/(.*)	Не задана	GET	Разрешить	Статика для нового интерфейса: • HTML • JS • Images • CSS • Fonts • файлы для наложения фона и шумоподавления
REST API, не описанное в OpenAPI-схеме IVA MCU					
14	/comet?(.*)	Comet	—	—	Канал получения событий
15	/services/resource(.*)	Resource	—	—	Загрузка различных файлов
16	/api/rs/media/proxy/media/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}?(.*)	Не задана	POST	Разрешить	media для подключения к конференции

Фильтры правила IVA-MCU Patched:

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
Исправление ошибок REST API, описанного в OpenAPI-схеме IVA MCU						
1	/api/rest/resources/create	Не задана	POST	Разрешить	При создании файлов	Неизвестный параметр shared Некорректное использование запроса web-клиентом

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
2	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/start-all-inquiries	Не задана	POST	Разрешить	При попытке запустить заранее созданные опросы	<EMPTY_POST>
3	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/inquiries/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/start	Не задана	POST	Разрешить	При попытке начать конкретный опрос	<EMPTY_POST>
4	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/stop-all-inquiries	Не задана	POST	Разрешить	При попытке остановить все начатые опросы	<EMPTY_POST>
5	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/inquiries/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/stop	Не задана	POST	Разрешить	При попытке остановить конкретный начатый опрос	<EMPTY_POST>
6	/api/rest/contacts/presences/find-for-users	Не задана	POST	Разрешить	При подписке на статусы пользователей	Ошибка в использовании схемы и её описании 1. Array must not contain duplicate elements: []

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
						2. Array is too short: must have at least 1 elements but instance has 0 elements: []
7	/api/rest/chats/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/typing	Не задана	POST	Разрешить	Возникает, когда пользователь пишет в чат сообщение и сервер уведомляет других участников	<EMPTY_POST>
8	/api/rest/chat-calls/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/screenshare/start	Не задана	POST	Разрешить	Возникает в p2p-звонке при попытке запустить трансляцию экрана	<EMPTY_POST>
9	/api/rest/chat-calls/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/screenshare/stop	Не задана	POST	Разрешить	Возникает в p2p-звонке при попытке остановить трансляцию экрана	<EMPTY_POST>
10	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/screenshare/start	Не задана	POST	Разрешить	Возникает в мероприятии при попытке остановить трансляцию экрана	<EMPTY_POST>
11	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/screenshare/stop	Не задана	POST	Разрешить	Возникает в мероприятии при попытке остановить трансляцию экрана	<EMPTY_POST>

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
12	/api/rest/chats/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/clear-history	Не задана	POST	Разрешить	Возникает при очистке чата или группового чата	<EMPTY_POST>
13	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/leave	Не задана	POST	Разрешить	Возникает при нажатии на кнопку для выхода из конференции	<EMPTY_POST>
14	/api/rest/chat-calls/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/leave	Не задана	POST	Разрешить	Возникает при нажатии на кнопку для выхода из звонка	<EMPTY_POST>
15	/api/rest/chats/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/allow-notifications	Не задана	POST	Разрешить	Возникает при включении уведомлений в чате	<EMPTY_POST>
16	/api/rest/chats/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/forbid-notifications	Не задана	POST	Разрешить	Возникает при отключении уведомлений в чате	<EMPTY_POST>
17	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/reject-incoming-call	Не задана	POST	Разрешить	Возникает при отклонении входящего звонка из мероприятия	<EMPTY_POST>
18	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/stop	Не задана	POST	Разрешить	Возникает при попытке завершить мероприятие	<EMPTY_POST>
19	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}	Не задана	PATCH	Разрешить	При изменении мероприятия / сессии мероприятия	[Path '/backgroundImageId/value'] Instance type (null) does not

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
						match any allowed primitive type (allowed: ["string"]): []
20	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/participants/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/start-outgoing-call	Не задана	POST	Разрешить	Возникает при попытке позвонить внешнему пользователю из мероприятия	<EMPTY_POST>
21	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/participants/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/cancel-outgoing-call	Не задана	POST	Разрешить	Возникает при отмене звонка внешнему пользователю из мероприятия	<EMPTY_POST>
22	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/start	Не задана	POST	Разрешить	Возникает при попытке начать запланированное мероприятие	<EMPTY_POST>
23	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/whiteboard/start	Не задана	POST	Разрешить	Возникает при попытке начать трансляцию белой доски	Object instance has properties which are not allowed by the schema: ["height","width"]: []

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
24	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/whiteboard/books/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/pages/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/undo	Не задана	POST	Разрешить	Возникает при попытке отменить последнее действие на белой доске	<EMPTY_POST>
25	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/whiteboard/books/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/pages/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/clear	Не задана	POST	Разрешить	Возникает при попытке очистить белую доску	<EMPTY_POST>
26	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/whiteboard/stop	Не задана	POST	Разрешить	Возникает при попытке остановить трансляцию белой доски	<EMPTY_POST>
27	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/whiteboard/state	Не задана	PATCH	Разрешить	Возникает при первоначальном запуске трансляции после входа в конференцию	Object instance has properties which are not allowed by the schema: ["height","width"]: []

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
28	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/participants/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/hand-up	Не задана	POST	Разрешить	Возникает при попытке поднять руку в мероприятии	<EMPTY_POST>
29	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/participants/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/hand-down	Не задана	POST	Разрешить	Возникает при попытке опустить руку в мероприятии	<EMPTY_POST>
30	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/documents/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/create-document-for/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}	Не задана	POST	Разрешить	Возникает при загрузке документа в мероприятие	<EMPTY_POST>
31	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/document/stop	Не задана	POST	Разрешить	Возникает при остановке трансляции документа	<EMPTY_POST>

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
32	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/document/state	Не задана	PATCH	Разрешить	Возникает при первоначаль-ном запуске трансляции документа после входа в конференцию.	Object instance has properties which are not allowed by the schema: ["documentId"]: []
33	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/record/start	Не задана	POST	Разрешить	Возникает при попытке начать запись конференции	<EMPTY_POST>
34	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/record/stop	Не задана	POST	Разрешить	Возникает при попытке остановить запись конференции	<EMPTY_POST>
35	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/video-document/pause	Не задана	POST	Разрешить	Возникает при паузе трансляции видеозаписи в конференции	<EMPTY_POST>
36	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/video-document/stop	Не задана	POST	Разрешить	Возникает при остановке трансляции видеозаписи в конференции	<EMPTY_POST>
37	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/demonstration/video-document/play	Не задана	POST	Разрешить	Возникает при возобновлении трансляции видеозаписи после паузы в конференции	<EMPTY_POST>

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
38	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/lobby/participants/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/approve	Не задана	POST	Разрешить	Возникает при попытке добавления конкретного пользователя в мероприятие из комнаты ожидания	<EMPTY_POST>
39	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/lobby/participants/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/reject	Не задана	POST	Разрешить	Возникает при попытке отказа добавления конкретного пользователя в мероприятие из комнаты ожидания	<EMPTY_POST>
40	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/lobby/approve-all	Не задана	POST	Разрешить	Возникает при попытке добавления всех пользователей из комнаты ожидания в мероприятие	<EMPTY_POST>
41	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/lobby/reject-all	Не задана	POST	Разрешить	Возникает при попытке отказа добавления всех пользователей из комнаты ожидания в мероприятие	<EMPTY_POST>

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
42	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/lobby/leave	Не задана	POST	Разрешить	Возникает при нажатии на кнопку «Выйти из мероприятия» в комнате ожидания	<EMPTY_POST>
43	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/join	Не задана	POST	Разрешить	Возникает при попытке в хода в мероприятие по гостевой ссылке	[Path '/ticketInfo/passcode'] Instance type (null) does not match any allowed primitive type (allowed: ["string"]): []
44	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/messages?(.*)	Не задана	GET	Разрешить	При загрузке сообщений от пользователя в конференции	Невалидное описание схемы: Instance value ("66621362-5ca0-4935-a6e0-b0d2fd44125b") not found in enum (possible values: ["ALL","COMMON","Target participant id as string <uuid>"]): []
45	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/inquiries	Не задана	POST	Разрешить	При создании опроса в мероприятии в вариациях: 1. Тип ответа: Выбор нескольких вариантов	Object instance has properties which are not allowed by the schema: ["allowFreeInput"]: []

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
					2. Тип ответа: Выбор одного варианта из нескольких	
46	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/media/public-audio-stream	Не задана	GET	Разрешить	При использовании синхронного перевода	Нет описания в схеме
47	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/groups/create	Не задана	POST	Разрешить	В конференциях с группами и длительностью бесконечное	Невалидное описание в схеме: требуется указать duration не меньше 60000, хотя разрешено использовать 0
48	/api/rest/conferences	Не задана	POST	Разрешить	При создании мероприятия с дополнительным параметром: «Регистрация на мероприятие» с опросом	Неправильное описание в схеме или неправильное использование в web-клиенте [Path '/questionnaire/polls/0'] Object instance has properties which are not allowed by the schema: ["id"]: [] – возникает всегда при создании опроса

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
						[Path '/questionnaire/polls/0/choices/0'] Object instance has properties which are not allowed by the schema: ["innerId"]: [] — количество подобных ошибок зависит от количества вариантов ответа
49	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/media/broadcast-language	Не задана	POST	Разрешить	При использовании синхронного перевода	Неправильное описание в схеме: [Path '/language'] Instance value ("ORIGINAL") not found in enum (possible values:
50	/api/rest/conferences/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}	Не задана	PATCH	Разрешить	При изменении планируемого периодического мероприятия	Неправильное описание в схеме
51	/api/rest/conference-sessions/sessions?(.*)	Не задана	GET	Разрешить	При получении всех сессий мероприятия в web-клиенте	limit=100&dateFrom=NaN
52	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/transcription/start	Не задана	POST	Разрешить	Возникает при попытке запустить стенограмму	<EMPTY_POST>

№	Параметры				Когда используется	Какую ошибку исправляет
	URL-путь	OpenAPI-схема	Метод	Действие		
53	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/media/request-attention	Не задана	POST	Разрешить	Возникает при запросе помощи из группы	<EMPTY_POST>
54	/api/rest/conference-sessions/[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12}/media/revoke-attention-request	Не задана	POST	Разрешить	Возникает при отмене запроса помощи из группы	<EMPTY_POST>

Фильтры правила IVA-MCU Block Std:

Не определены. В это правило можно добавить фильтры для любых запросов, которые необходимо заблокировать.

Фильтры правила IVA-MCU Allow URI:

№	Параметры				Назначение
	URL-путь	OpenAPI-схема	Метод	Действие	
Стандартные проверки					
1	/api/rest/(.*)	ClientAPI	—	—	Вызов методов клиентского REST API
Подключение iOS- / Android-приложений					
2	/api/ws/InstantMessagingWebService/InstantMessaging	Не задана	POST	Разрешить	SOAP-запросы для клиентов с ОС iOS / Android
3	/api/ws/NotificationWebService	Не задана	POST	Разрешить	SOAP-запросы для клиентов с ОС iOS / Android

№	Параметры				Назначение
	URL-путь	OpenAPI-схема	Метод	Действие	
4	/api/ws/UserWebService/User	Не задана	POST	Разрешить	SOAP-запросы для клиентов с ОС iOS / Android
5	/api/ws/ContactWebService/Contact	Не задана	POST	Разрешить	SOAP-запросы для клиентов с ОС iOS / Android
6	/api/ws/DocumentsWebService/Documents	Не задана	POST	Разрешить	SOAP-запросы для клиентов с ОС iOS / Android
7	/api/ws/MobileAppWebService/MobileApp	Не задана	POST	Разрешить	SOAP-запросы для клиентов с ОС iOS / Android

Настройка маршрутизации TURN

Ниже приведен пример настройки сервера проксирования IVA SBC для маршрутизации TURN-трафика на разрешённые IP-адреса медиасерверов платформы IVA MCU.

Чтобы настроить сервер проксирования для маршрутизации TURN, необходимо:

1 войти в **Web-интерфейс администрирования** IVA SBC

2 в разделе **Маршруты TURN** добавить маршрут (см. Создание и редактирование маршрутов TURN), задав имя, например: **IVA MCU 51 Media Server**

3 в окне Информация о маршруте TURN добавить (см. Добавление и редактирование разрешённых IP-адресов):
- **IP-адрес**: IVA_MEDIA_IP
- **Порты**: 20000-30000

4 в разделе **Группы маршрутизации** создать группу маршрутизации (см. Настройка групп маршрутизации) с параметрами:

- **Имя**: Turn for 51 Server IVA MCU
- **Описание**: Список разрешённых IP-адресов для 51 сервера IVA MCU
- **Тип**: TURN Proxy

5 в окне **Информация группе маршрутизации TURN** добавить созданный маршрут (см. Создание группы маршрутизации) **IVA MCU 51 Media Server**

6 в разделе **Сервера проксирования** выбрать сервер проксирования

7 в окне Информация о сервере проксирования для роли **TURN** выбрать группу маршрутизации (**Turn for 51 Server IVA MCU**) и активировать роль (см. Добавление Ролей проксирования)

8 в окне Информация о сервере проксирования выполнить настройку TURN (см. Настройка TURN) с параметрами:

- Порт TCP/UDP: 3478
- **Сертификат**: выбрать сертификат (для добавленных IVA_MEDIA_IP) из списка доступных сертификатов
- **Статический логин**: логин для доступа к TURN-серверу (например **ivcs**)
- **Статический пароль**: пароль для доступа к TURN-серверу (например **ivcs**)
- **Relay IP**: IP-адрес сервера проксирования IVA SBC (**10.0.202.201**), по которому он будет доступен для получения пакетов внутри сети (от медиасерверов IVA MCU)

9 войти в **Web-интерфейс администрирования** Платформы IVA MCU:

- в разделе Настройки STUN/TURN серверов Рисунок 192 создать сервер Рисунок 193 и настроить параметры:
  - **Url**: URL-адрес до STUN / TURN сервера (turn:200.0.210.110:3478?transport=udp)
  - **Имя пользователя**: ivcs
  - **Пароль**: ivcs

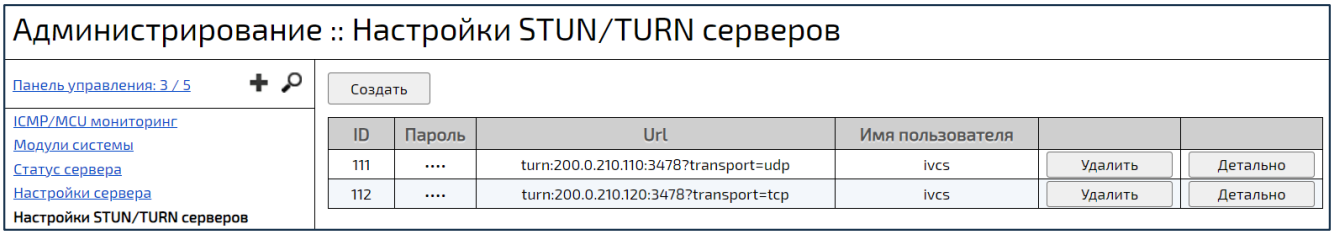

Рисунок 192. Настройки STUN/TURN серверов

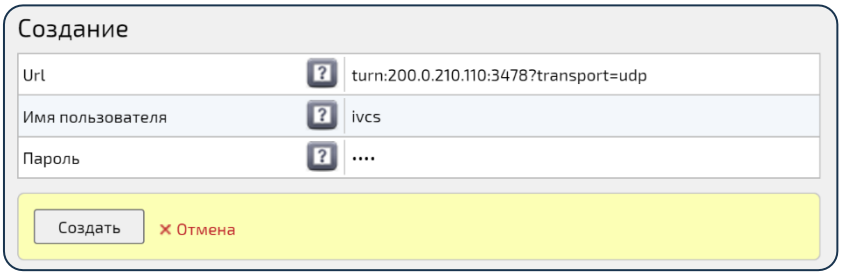

Рисунок 193. Создание STUN/TURN сервера

Настройка HTTP Proxy

Ниже приведен пример настройки сервера проксирования IVA SBC для маршрутизации исходящих HTTP-запросов от сервера IVA MCU, не имеющего прямого доступа в Интернет для отправки push-уведомлений Google и Apple.

Чтобы настроить отправку push-уведомлений от IVA MCU на сервера Google (GCM) и Apple (APNS) через сервер проксирования с ролью HTTP Proxy:

1 войти в **Web-интерфейс администрирования** IVA SBC

2 в разделе **Настройки HTTP Proxy** добавить группу доступа (см. Добавление группы доступа), задав имя (например **MCU-push**) и описание

3 в окне Информация о группе доступа добавить (см. Добавление разрешённого адреса в группу доступа) адреса внешних серверов:

- **fcm.googleapis.com:443** – для отправки push-уведомлений Google
- **api.push.apple.com:443** – для отправки push-уведомлений Apple

> При настройке HTTP Proxy в указанной конфигурации отправка с сервера IVA MCU web push-уведомлений для чат-ботов **будет недоступна**

4 на вкладке Прокси пользователи добавить пользователя (см. Добавление прокси пользователя), указав имя, логин, пароль и список IP-адресов и сетей, с которых можно выполнять авторизацию пользователя

5 назначить прокси пользователю созданную группу доступа (см. Добавление группы доступа для прокси пользователя)

6 в разделе **Сервера проксирования** выбрать сервер проксирования

7 в окне Информация о сервере проксирования для выбранного сервера активировать роль **HTTP Proxy** (см. Добавление Ролей проксирования)

8 войти в **Web-интерфейс администрирования** Платформы IVA MCU:

- в разделе Системные настройки перейти к секции Настройки клиентских приложений
- в поле Прокси для push-уведомлений Рисунок 194 ввести адрес севера проксирования в формате: http://<login>:<pwd>@<SBC_PROXY_IP>, где:
  - **login** – логин прокси пользователя
  - **pwd** – пароль прокси пользователя
  - **SBC_PROXY_IP** – IP-адрес сервера проксирования с ролью HTTP Proxy

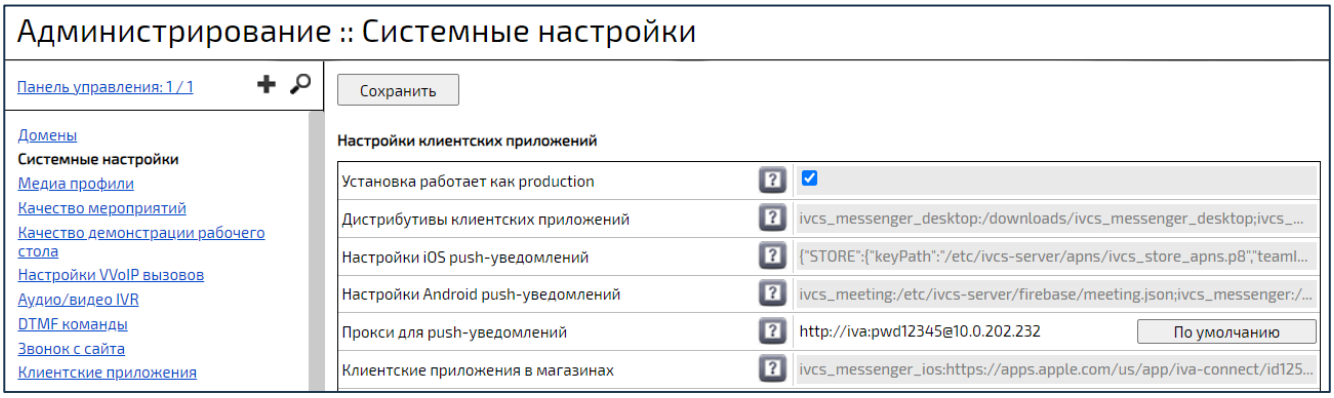

Рисунок 194. Настройки Прокси для push-уведомлений

Если требуется настроить проксирование запросов от сервера IVA MCU к внешним сервисам распознавания речи:

1 выполнить аналогичные **Настройки HTTP Proxy**, добавив в окне Информация о группе доступа адреса серверов внешних онлайн-сервисов распознавания речи

2 в **Web-интерфейсе администрирования** Платформы IVA MCU:

- в разделе Системные настройки перейти к секции Настройки распознавания речи
- в поле Прокси сервер для доступа к системе распознавания речи Рисунок 195 ввести адрес севера проксирования в формате: http://<login>:<pwd>@<SBC_PROXY_IP>

> Обращения к API онлайн-сервисов распознавания речи выполняются с **медиасерверов IVA MCU**

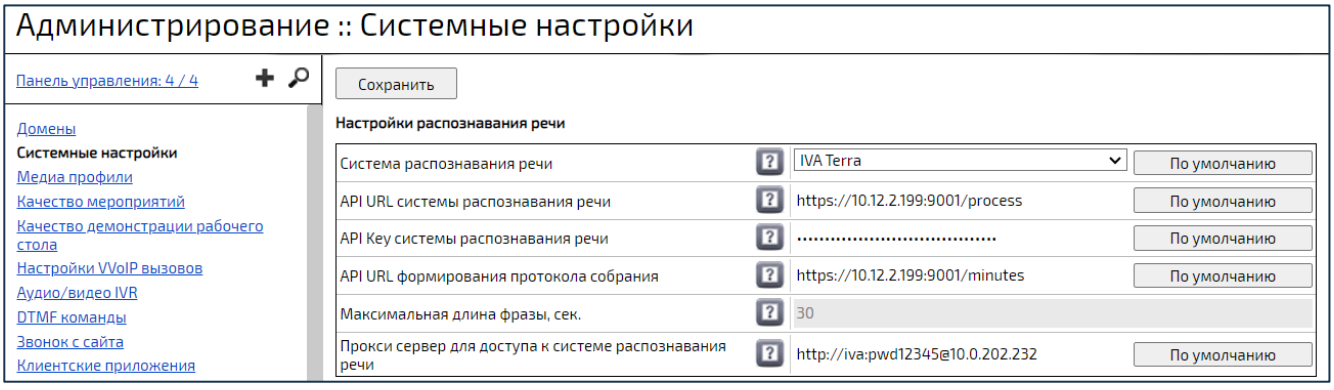

Рисунок 195. Настройки Прокси для систем распознавания речи

Примеры регулярных выражений

При составлении фильтров и модификаций адресов используются регулярные выражения (RegExp). Ниже приведены:

- Примеры выражений фильтров и модификаций
- Примеры преобразования адресов
- Синтаксис регулярных выражений

Примеры выражений фильтров и модификаций

RegExp	Пример адреса	Примечание
^sip:(.*)@domain1.ru$	sip:test@domain1.ru	sip:<N>@domain1.ru
^sip:\+(.*)@(.*)	sip:+74951234567@domain1.ru	sip:+<N>@<N>
^sip:|H.323:(.*)@(.*)	sip:+74951234567@10.0.0.10	sip:<N>@<N>
	H.323:test@domain1.ru	H.323:<N>@<N>
sip:(.*)@10\.0\.0\.10$	sip:1010@10.0.0.10	sip:<N>@10.0.0.10
(.*)@mydomain\.(.*)	sip:test@mydomain.com	<N>@mydomain.<N>
(.*)@10\.0\.0\.10:[0-9]{5}$	sip:user@10.0.0.10:11100	<N>@10.0.0.10:XXXXX (где XXXXX – номер порта, состоящий из 5 цифр)

где <N> – изменяемое значение, содержащее любое произвольное количество символов.

Примеры преобразования адресов

- пример 1:

Фильтр адреса ТО	Примечание
^sip:000([0-9]{3,5})@(.*).com$	sip:000XXXX@<N>.com где <N> – любое произвольное количество символов
Модификация адреса ТО	
sip:$1@$2.ru	sip:XXXX@<N>.ru

где:
- строка замены $1 – переменная, которой в данном случае является первое заключенное в скобках выражение ([0-9]{3,5})
- строка замены $2 – переменная, которой в данном случае является второе заключенное в скобках выражение (.*)

Фильтр адреса ТО ^sip:000([0-9]{3,5})@(.*).com$ ищет номера формата sip:000XXXX@<N>.com, где после sip:000 идут любые цифры в количестве от 3 до 5 символов, а <N> – любое произвольное количество символов.

Модификация адреса ТО sip:$1@$2.ru преобразует найденный номер в номер формата sip:XXXX@<N>.ru.

- пример 2:

Фильтр адреса ТО	Примечание
^sip:000([0-9]{7,8})@<HOST_NAME>$ где <HOST_NAME> – название вызываемого физического / виртуального хоста	sip:000XXXXXXXX@<HOST_NAME>
Модификация адреса ТО	
sip:$1@<SERVER_IP>	sip:XXXXXXXX@<SERVER_IP>

где:
- строка замены $1 – переменная, которой, в данном случае, является заключенное в скобках выражение ([0-9]{7,8})
- <SERVER_IP> – вызываемый IP-адрес физического / виртуального сервера

Фильтр адреса TO **^sip:000([0-9]{7,8})@<HOST_NAME>$** ищет номера формата **sip:000XXXXXXXX@<HOST_NAME>**, где после **sip:000** идут любые цифры в количестве от 7 до 8 символов, а **<HOST_NAME>** – название вызываемого физического / виртуального хоста.

Модификация адреса TO **sip:$1@<SERVER_IP>** преобразует найденный номер в номер формата **sip:XXXXXXXX@<SERVER_IP>**, где **<SERVER_IP>** – вызываемый IP-адрес физического / виртуального сервера.

Синтаксис регулярных выражений

Синтаксис регулярных выражений основан на использовании символов **<([{\^-=$!|]})?*+.>**, которые можно комбинировать с цифровыми и буквенными символами.

В зависимости от роли символы можно разделить на несколько групп:

- метасимволы для поиска совпадений границ строк или текста
- метасимволы для поиска символьных классов
- метасимволы для поиска символов редактирования текста
- метасимволы для группировки символов
- метасимволы для обозначения количества символов (квантификаторы), квантификатор всегда следует после символа или группы символов

Метасимволы для поиска совпадений границ строк или текста:

Метасимвол	Назначение
^	начало строки
$	конец строки
\b	граница слова
\B	не граница слова
\A	начало ввода
\G	конец предыдущего совпадения
\Z	конец ввода
\z	конец ввода

Метасимволы для поиска символьных классов:

Метасимвол	Назначение
\d	цифровой символ
\D	нецифровой символ
\s	символ пробела
\S	непробельный символ
\w	буквенно-цифровой символ или знак подчёркивания
\W	любой символ, кроме буквенного, цифрового или знака подчёркивания
.	любой символ

Метасимволы для поиска символов редактирования текста:

Метасимвол	Назначение
\t	символ табуляции
\n	символ новой строки
\r	символ возврата каретки
\f	переход на новую страницу
\u 0085	символ следующей строки
\u 2028	символ разделения строк
\u 2029	символ разделения абзацев

Метасимволы для группировки символов:

Метасимвол	Назначение
[абв]	любой из перечисленных (а, б, или в)
[^абв]	любой, кроме перечисленных (не а, б, в)
[a-zA-Z]	слияние диапазонов (латинские символы от a до z без учёта регистра)
[a-d[m-p]]	объединение символов (от a до d и от m до p)
[a-z&&[def]]	пересечение символов (символы d, e, f)
[a-z&&[^bc]]	вычитание символов (символы a, d-z)

Метасимволы для обозначения количества символов (квантификаторы):

Метасимвол	Назначение
?	один или отсутствует
*	ноль или более
+	один или более
{n}	n
{n,}	n и более
{n,m}	не менее n и не более m

Используемые порты и протоколы

IVA SBC автоматически открывает на серверах все необходимые для своей работы порты.

В зависимости от типа ролей, которые выполняет сервер проксирования, требования к открытию портов применяются для:

- сервера проксирования IVA SBC
- межсервисное общения сервера проксирования IVA SBC с сервером управления и конфигурации
- межсервисное общение сервера управления и конфигурации с сервером проксирования IVA SBC
- портов вспомогательных программ
- входящих портов всех серверов IVA SBC

где:
ANY – любой диапазон сетей (0.0.0.0/0) или портов в зависимости от контекста (колонки)
APNS_IP – диапазон адресов службы push-уведомлений Apple (17.0.0.0/8)
GCM_IP – диапазон адресов службы push-уведомлений Google (ANY)
dst ip range – диапазон IP-адресов назначения
dst ports range – диапазон портов назначения
HTTP Reverse Proxy Servers – IP-адрес, по которому доступен сервер обратного проксирования
IVA_MCU_IP – IP-адрес головного сервера IVA MCU
SBC_CFG_IP – IP-адрес, по которому доступен сервер управления и конфигурации IVA SBC
SBC_PROXY_IP – IP-адрес, по которому доступен сервер проксирования IVA SBC
src ip range – диапазон исходящих IP-адресов
src ports range – диапазон исходящих портов
ZABBIX HOST – IP-адрес Zabbix-сервера

Сервер проксирования IVA SBC

- SIP-порты

> Если для SIP-звонков настроено RTP-проксирование, то используются также сетевые порты и протоколы для проксирования RTP-трафика

  - Входящие SIP-порты:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
ANY	ANY	SBC_PROXY_IP	5060	TCP	SIP	SIP-сигнализация (входящая): входящие SIP-звонки
ANY	ANY	SBC_PROXY_IP	5061	TLS / TCP	SIP	
ANY	ANY	SBC_PROXY_IP	5060	UDP	SIP	SIP-сигнализация (входящая): входящие / исходящие SIP-звонки
ANY	ANY	SBC_PROXY_IP	5061	DTLS / UDP	SIP	

- Исходящие SIP-порты (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	5060	ANY	5060 (возможен любой порт)	TCP	SIP	SIP-сигнализация (исходящая): исходящие SIP-звонки
SBC_PROXY_IP	5061	ANY (для внутренней сети можно ограничить допустимые в рамках решения IP-адреса)	5061 (возможен любой порт)	TLS / TCP	SIP	
SBC_PROXY_IP	5060	ANY (для внутренней сети можно ограничить допустимые в рамках решения IP-адреса)	5060 (возможен любой порт)	UDP	SIP	SIP-сигнализация (исходящая): входящие / исходящие SIP-звонки
SBC_PROXY_IP	5061	ANY (для внутренней сети можно ограничить допустимые в рамках решения IP-адреса)	5061 (возможен любой порт)	DTLS / UDP	SIP	

- H.323-порты

> Если для H.323-звонков настроено RTP-проксирование, то используются также сетевые порты и протоколы для проксирования RTP-трафика

  - Входящие H.323-порты:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
IVA_MCU_IP	ANY	SBC_PROXY_IP	1720	TCP	H.323, H.245	H.323-сигнализация (входящая): входящие H.323-звонки со стороны IVA MCU
ANY	ANY	SBC_PROXY_IP	1720	TCP	H.323	H.323-сигнализация (входящая): входящие H.323-звонки
ANY	ANY	SBC_PROXY_IP	30000-38000	TCP	H.323	H.323-сигнализация (входящая): входящие H.323-звонки. H.245-канал. Необходимо открывать, если удалённый терминал не поддерживает H.245 внутри H.323
ANY	ANY	SBC_PROXY_IP	1719	UDP	H.323	H.323 RAS-протокол (регистрация абонентов). Для внутренней сети могут быть ограничения в соответствии с решением

ANY	ANY	SBC_PROXY_IP	1718	UDP	H.323	H.323 RAS multicast (для работы с H.323 Neiborhood). Для внутренней сети могут быть ограничения в соответствии с решением

- Исходящие H.323-порты (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	ANY	IVA_MCU_IP	1720	TCP	H.323, H.245	H.323-сигнализация (исходящая): исходящие H.323-звонки в сторону IVA MCU
SBC_PROXY_IP	1720 / ANY	ANY	1720	TCP	H.323	H.323-сигнализация (исходящая): исходящие H.323-звонки
SBC_PROXY_IP	ANY	ANY	ANY (для создания H.245-канала, если удалённый терминал не поддерживает H.323)	TCP	H.323	H.323-сигнализация (исходящая): исходящие H.323-звонки. H.245 канал. Необходимо открывать, если удалённый терминал не поддерживает H.245 внутри H.323
SBC_PROXY_IP	1719	ANY	ANY	UDP	H.323	H.323 RAS-протокол (регистрация абонентов)

- RTP-порты (используются в случае, если применяется проксирование RTP-трафика для VVoIP (SIP и H.323)
  - Входящие сетевые порты и протоколы:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
ANY	ANY	SBC_PROXY_IP	30000-39999	UDP	RTP ICE BFCP-UDP	Входящие пакеты RTP-трафика для VVoIP-звонков
ANY	ANY	SBC_PROXY_IP	38000-39999	TCP	BFCP-TCP	Протокол BFCP-TCP для SIP-соединений

  - Исходящие сетевые порты и протоколы (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	30000-39999	ANY	ANY	UDP	RTP ICE BFCP-UDP	Исходящие RTP-пакеты для VVoIP-звонков
SBC_PROXY_IP	38000-39999	ANY	ANY	TCP	BFCP-TCP	Протокол BFCP-TCP для SIP-соединений с поддержкой TCP-BFCP

- TURN-порты (необходимы в случае, если применяется TURN Proxy для WebRTC)
  - Входящие TURN-порты:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
ANY	ANY	SBC_PROXY_IP	3478 5349	UDP	TURN ICE-STUN	TURN-соединение для WebRTC-подключений. Если внутренние пользователи не могут использовать TURN, то данные порты можно закрыть для внутренней сети
ANY	ANY	SBC_PROXY_IP	3478 5349	TCP	TURN ICE-STUN	
ANY	ANY	SBC_PROXY_IP	50000-60000	UDP	RTP	Назначение зависит от списка добавленных разрешённых IP-адресов в администрировании

  - Исходящие TURN-порты (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	3478 5349	ANY	ANY	UDP	TURN	TURN-соединение для WebRTC-подключений. Доступ можно ограничить только портами, разрешенными в рамках решения (например, к определенным внутренним приемникам RTP)
SBC_PROXY_IP	50000-60000	ANY	ANY	UDP	RTP	Назначение зависит от списка добавленных разрешённых IP-адресов в администрировании

- HTTP Reverse-порты
  - Входящие порты HTTP Reverse:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
ANY	ANY	SBC_PROXY_IP	443	TCP	HTTPS	HTTPS-подключения из внешней сети к внутреннему серверу

  - Исходящие порты HTTP Reverse (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	ANY	HTTP Reverse Proxy Servers	HTTP Reverse Proxy Servers Ports	TCP	HTTPS	HTTPS-подключение к внешнему серверу. Можно ограничить только тем сервером, к которому должен быть доступ

- HTTP Proxy-порты
  - Входящие порты HTTP Proxy:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
IVA_MCU_IP	ANY	SBC_PROXY_IP	3128	TCP	HTTP, HTTPS	Подключение к HTTP Proxy для выполнения запросов в Интернет из внутренней сети (например, отправка push-уведомлений на внешние сервера)

- Исходящие порты HTTP Proxy (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	ANY	Зависит от назначения. Например: APNS_IP GCM_IP	Зависит от назначения. Например: 443, 2197	TCP	HTTP, HTTPS	Подключение к HTTP Proxy для выполнения запросов в Интернет из внутренней сети (например, отправка push-уведомлений на внешние сервера)

Межсервисное общение сервера проксирования IVA SBC с сервером управления и конфигурации

- Межсервисные входящие порты:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_CFG_IP	ANY	SBC_PROXY_IP	11600	TCP	REST API	Доступ к сервису monitoring от сервера управления и конфигурации
SBC_CFG_IP	ANY	SBC_PROXY_IP	11612	TCP	REST API	Доступ к сервису monitoring от сервера управления и конфигурации
SBC_PROXY_IP	ANY	SBC_PROXY_IP2	11600	TCP	Internal	Доступ к проверке ping от одного сервера проксирования до другого (не обязательно)

SBC_PROXY_IP	ANY	SBC_PROXY_IP2	11901	TCP	Internal	Доступ к возможности обработки команд, если локальный SBC контроллер VVoIP не отвечает (не обязательно)

- Межсервисные исходящие порты (установленные TCP-соединения считаются действительными):

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	ANY	SBC_CFG_IP	11950	TCP	Internal	Запрос конфигурации сервера и отправка различных trap-сообщений
SBC_PROXY_IP	ANY	SBC_CFG_IP	11100	TCP	Internal	Работа с системой Zookeeper
SBC_PROXY_IP	ANY	SBC_CFG_IP	11954	TCP	Internal	Информирование сервера управления и конфигурации о системных событиях
SBC_PROXY_IP	ANY	SBC_CFG_IP	11600	TCP	Internal	Доступ к проверке ping от одного сервера проксирования до другого (не обязательно)
SBC_PROXY_IP	ANY	SBC_PROXY_IP2	11600	TCP	Internal	Доступ к проверке ping от одного сервера проксирования до другого (не обязательно)
SBC_PROXY_IP	ANY	SBC_PROXY_IP2	11901	TCP	Internal	Доступ к возможности обработки команд, если локальный SBC контроллер VVoIP не отвечает (не обязательно)

Межсервисное общение сервера управления и конфигурации с сервером проксирования IVA SBC

- Межсервисные входящие порты:

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
SBC_PROXY_IP	11100	SBC_CFG_IP	11100	TCP	Internal	Регистрация сервера проксирования в системе Zookeeper
SBC_PROXY_IP	11950	SBC_CFG_IP	11950	TCP	Internal	Запрос конфигурации сервера проксирования и приём различных trap-сообщений
SBC_PROXY_IP	11600	SBC_CFG_IP	11600	TCP	Internal	Доступ к проверке ping от сервера проксирования (не обязательно)
SBC_PROXY_IP	11954	SBC_CFG_IP	11954	TCP	Internal	Monitoring callback от сервера проксирования для загрузки серверных настроек: • настройки сети • DNS-серверов • событий аудита и т. д.

Межсервисное общение между серверами проксирования IVA SBC

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L3 protocol(s)	Примечания
SBC_PROXY_IP (1)	ANY	SBC_PROXY_IP (N)	ANY	VRRP	Поддержка плавающего IP-адреса отказоустойчивого кластера на основе сервиса keepalived. Связность обеспечивается только между серверами одной группы кластера

Входящие порты вспомогательных программ

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
ANY	ANY	SBC_PROXY_IP	10500	TCP	zabbix-agent	Пассивный агент Zabbix
192.168.0.0/16 172.16.0.0/12 10.0.0.0/8	ANY	SBC_PROXY_IP	161	UDP	SNMP	Доступ для внешних систем мониторинга по протоколу SNMP

Входящие порты для всех серверов IVA SBC

src_ip_range	src_ports_range	dst_ip_range	dst_ports_range	L4 protocol(s)	L7 protocol(s)	Примечания
192.168.0.0/16 172.16.0.0/12 10.0.0.0/8	ANY	SBC_PROXY_IP	161	UDP	SNMP	SNMP-управление
ANY	ANY	SBC_PROXY_IP	22	TCP	SSH	Доступ к консоли сервера управления и конфигурации. Ограничивается для безопасности и открывается только для хостов, использование которых является необходимым
ZABBIX HOST	1024-65535	SBC_PROXY_IP	10500	TCP	zabbix-agent	Доступ для внешней системы мониторинга Zabbix (если используется)
–	–	–	–	–	ICMP	Передача сообщений об ошибках и т. д. при передаче данных

Логи системы

Это приложение содержит информацию о логах, создаваемых системой IVA SBC, их ротации и занимаемом ими пространстве.

Общие логи

Общие логи создаются для сервера проксирования и сервера управления и конфигурации. К общим логам относятся:

- системные логи
- логи утилиты iva-cli
- логи модуля monitoring
- логи модуля Zabbix
- логи модуля VictoriaMetrics

- Системные логи

Системные логи создаются стандартными процессами системы.
Хранятся в **/var/log/**.

Имя файла	Назначение	Где хранятся настройки	Ротирование	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
alternatives.log	Логи команды update-alternatives	/etc/logrotate.d/alternatives	По размеру	100 МБ	5	150 МБ
auth.log	Логи авторизации пользователей	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ

Имя файла	Назначение	Где хранятся настройки	Ротирование	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
btmp	Логи записей неудачных попыток входа в систему	/etc/logrotate.d/btmp	По размеру	100 МБ	5	150 МБ
daemon.log	Логи утилиты systemd	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ
debug	Отладочная информация	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ
dpkg.log	Логи утилиты dpkg	/etc/logrotate.d/dpkg	По размеру	100 МБ	5	150 МБ
fail2ban.log	Логи утилиты fail2ban	/etc/logrotate.d/fail2ban	По размеру	100 МБ	5	150 МБ
kern.log	Логи сообщений ядра ОС	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ
messages	Логи сообщений с момента запуска системы от ядра Linux, различных служб, обнаруженных устройств, сетевых интерфейсов	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ
syslog	Логи сообщений с момента запуска системы от ядра Linux, различных служб, обнаруженных устройств, сетевых интерфейсов	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ

Имя файла	Назначение	Где хранятся настройки	Ротирование	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
user.log	Системный лог от служб уровня пользователей ОС	/etc/logrotate.d/rsyslog	По размеру	100 МБ	5	150 МБ
wtmp	Лог записей входа пользователей в систему	/etc/logrotate.d/wtmp	По размеру	100 МБ	5	150 МБ
faillog	Логи неудачных попыток входа в систему	/var/log/faillog	Не задано	—	—	Количество пользователей × 44 байта. В среднем 2 КБ
lastlog	Логи последних сессий пользователей	/var/log/lastlog	Не задано	—	—	Количество пользователей × 300 байт. В среднем 10 КБ
vmware-network.log	Лог инструментария VMWare	/etc/vmware-tools/scripts/vmware/network	При каждом запуске	—	9	10 МБ
vmware-vmsvc-root.log	Лог инструментария VMWare	/etc/vmware-tools/tools.conf	По размеру	1 МБ	3	4 МБ
vmware-vmtoolsd-root.log	Лог инструментария VMWare	/etc/vmware-tools/tools.conf	По размеру	1 МБ	3	4 МБ
						Итого: до 2 ГБ

- Логи утилиты iva-cli

Хранятся в **/var/log**.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
iva-cli.log	Логи выполнения команды iva-cli	100 МБ	5	до 150 МБ

- Логи модуля monitoring

Хранятся в **/var/log/monitoring**.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
monitoring.log	Логи работы модуля monitoring	100 МБ	5	150 МБ
audit.log	Логи событий аудита модуля monitoring	100 МБ	5	150 МБ
gc.log	Логи сборщика мусора JVM	100 МБ	5	30 МБ
monitoring.output	Логи JVM	100 МБ	5	150 МБ
				Итого: до 500 МБ

- Логи модуля Zabbix

Создаются только после ручной установки Zabbix.
Хранятся в /etc/logrotate.d/zabbix-agent.
Ротируются еженедельно.

Имя файла	Назначение	Количество архивных логов	Средний объём всех логов
zabbix_agentd.log	Логи работы процесса zabbix	7	до 50 МБ

- Логи модуля VictoriaMetrics

Логи модуля VictoriaMetrics записываются в системный лог /var/log/syslog.

Расчёт объёма общих логов

Тип логов	Размер
Системные логи	2 ГБ
Логи утилиты iva-cli	150 МБ
Логи модуля monitoring	500 МБ
Логи модуля Zabbix	50 МБ
	Итого: 2,7 ГБ

Логи модулей сервера проксирования

К логам модулей сервера проксирования относятся:

- логи модуля voip-signalling-gateway
- логи модуля sbc

- Логи модуля voip-signalling-gateway

Хранятся в /var/log/voip-signalling-gateway.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
voip-signalling-gateway.log	Логи работы модуля voip-signalling-gateway	100 МБ	5	150 МБ
auth.log	Логи событий VoIP-аутентификации модуля voip-signalling-gateway	100 МБ	5	150 МБ
gc.log	Логи сборщика мусора JVM	20 МБ	5	30 МБ
voip-signalling-gateway.output	Логи JVM	100 МБ	5	150 МБ
sip.log	Логи SIP-сигнализации модуля voip-signalling-gateway	100 МБ	5	150 МБ
				Итого: до 630 МБ

- Логи модуля sbc

Хранятся в **/var/log/sbc/**.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
sbc.log	Общие логи сервиса SBC	100 МБ	5	150 МБ
sbc.output	Логи JVM	100 МБ	5	150 МБ
gc.log	Логи сборщика мусора JVM	20 МБ	5	30 МБ
reverse_proxy.log	Логи модуля HTTP Reverse Proxy	100 МБ	5	150 МБ
http_proxy.log	Логи модуля HTTP Proxy	100 МБ	5	150 МБ
turn_error.log	Логи модуля TURN. Ошибки аутентификации и доступа к запрещённым адресам	100 МБ	5	150 МБ
turn_relay.log	Логи модуля TURN. Открытие/закрытие релея со статистикой по переданным данным	100 МБ	5	150 МБ
				Итого: до 1 ГБ

Расчёт объёма логов модулей сервера проксирования

Тип логов	Размер
Логи voip-singalling-gateway	630 МБ
Логи sbc	1 ГБ
	Итого: 1,7 ГБ

Логи модулей сервера управления и конфигурации

К логам модулей сервера управления и конфигурации относятся:

- логи модуля registry
- логи модуля postgres
- логи модуля nginx
- логи модуля sbc-cfg-server

- **Логи модуля registry**

Хранятся в **/var/log/registry/**.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
registry.log	Логи работы процесса registry	150 МБ	5	150 МБ
registry.output	Логи JVM	150 МБ	5	150 МБ

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
gc.log	Логи сборщика мусора JVM	20 МБ	5	30 МБ
				Итого: до 330 МБ

- Логи модуля postgres

Хранятся в **/var/log/postgresql/**.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
postgresql-13-main.log	Логи работы процесса postgresql	100 МБ	5	до 150 МБ

- Логи модуля nginx

Хранятся в **/var/log/nginx/**.
Ротируются по размеру.

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
access.log	Логи клиентских запросов к nginx	100 МБ	10	200 МБ
error.log	Логи с ошибками при работе сервиса nginx	100 МБ	10	200 МБ
sbc-cfg-server.https.access.log	Логи клиентских запросов к модулю sbc-cfg-server через nginx	100 МБ	10	200 МБ

Имя файла	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
sbc-cfg-server.https.error.log	Логи ошибок клиентских запросов к модулю sbc-cfg-server через nginx	100 МБ	10	200 МБ
				Итого: 800 МБ

- Логи модуля sbc-cfg-server

Хранятся в **/var/log/sbc-cfg-server/**.
Ротируются по размеру.

Имя	Назначение	Максимальный размер активного лога	Количество архивных логов	Средний объём всех логов
gc.log	Логи сборщика мусора JVM	20 МБ	5	30 МБ
sbc-cfg-server.log	Общие логи сервиса sbc-cfg-server	100 МБ	5	150 МБ
sbc-cfg-server.output	Логи JVM	100 МБ	5	150 МБ
				Итого: 330 МБ

Расчёт объёма логов модулей сервера управления и конфигурации

Тип логов	Размер
Логи registry	330 МБ
Логи postgres	150 МБ
Логи nginx	800 МБ
Логи sbc-cfg-server	330 МБ
	Итого: 1,61 ГБ

Установка Kaspersky Endpoint Security

IVA SBC поддерживает установку на серверы системы антивирусного программного обеспечения Kaspersky Endpoint Security, а также Агента администрирования, обеспечивающего взаимодействие между сервером администрирования Kaspersky Security Center и Kaspersky Endpoint Security.

> Установка Kaspersky Endpoint Security и Агента администрирования выполняется исходя из требований проекта или заказчика к информационной безопасности

Перед установкой программного обеспечения рекомендуется ознакомиться со следующей документацией от производителя:

- официальная документация Kaspersky Endpoint Security для Linux
- требования к портам, используемым в Kaspersky Security Center
- сетевые параметры для взаимодействия с внешними службами

Установка Kaspersky Endpoint Security

Для установки Kaspersky Endpoint Security необходимо в командной строке (консоли) сервера выполнить следующие действия:

1 загрузить инсталлятор kesl_<версия>_amd64.deb на сервер через scp, где <версия> – версия соответствующего программного компонента

> Загружать файл инсталлятора рекомендуется с официального сайта

2 разрешить установку, выполнив команду:

```
sudo iva-cli kesl prepare
```

3 выполнить установку пакета kesl с помощью команды:

```
sudo dpkg -i kesl_<версия>_amd64.deb
```

4 выполнить первоначальную настройку командой:

```
sudo /opt/kaspersky/kesl/bin/kesl-setup.pl
```

В процессе первоначальной настройки необходимо:

- принять лицензионное соглашение
- указать адрес сервера для загрузки обновлений (опционально)
- выполнить первоначальную загрузку обновлений (рекомендуется для обеспечения полнофункциональной защиты)
- включить автоматическую загрузку обновлений (опционально)
- указать ключ лицензии (опционально, по умолчанию будет использоваться временный ключ (trial key)

5 сохранить изменения, выполнив команду:

```
sudo iva-cli live save-changes -q
```

Ошибка загрузки обновлений при первоначальной настройке Kaspersky Endpoint Security

После запуска скрипта первоначальной настройки Kaspersky Endpoint Security kesl-setup.pl в консоли отображается следующее предупреждение:

```
Downloading the latest application databases

Task progress:
[##################################################]100%

Warning: Failed to update.
```

Данное предупреждение наблюдается при установке Kaspersky Endpoint Security версии 11.4.0–1096 и связано с преждевременной проверкой ключа лицензии. Проблему можно игнорировать, но после завершения первоначальной настройки требуется вручную запустить задачу на загрузку антивирусных баз, выполнив команду:

```
sudo kesl-control --start-task 6
```

Установка Агента администрирования

> Установка Агента администрирования выполняется при необходимости интеграции Kaspersky Endpoint Security с Kaspersky Security Center

Для установки Агента администрирования необходимо в командной строке (консоли) сервера, на котором установлен Kaspersky Endpoint Security, выполнить следующие действия:

1 загрузить инсталлятор klnagent64_<версия>_amd64.deb на сервер через scp, где <версия> – версия соответствующего программного компонента

2 разрешить установку, выполнив команду:

```
sudo iva-cli kesl prepare
```

3 выполнить установку пакета klnagent64 с помощью команды:

```
sudo dpkg -i klnagent64_<версия>_amd64.deb
```

4 выполнить первоначальную настройку командой:

```
sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

> В процессе первоначальной настройки необходимо принять лицензионное соглашение и указать адрес Kaspersky Security Center – хост, порт и т. д.

5 сохранить изменения, выполнив команду:

```
sudo iva-cli live save-changes -q
```

Мониторинг

Выполнение команд для мониторинга производится в командной строке (консоли) сервера, на котором установлен Kaspersky Endpoint Security.

> Команды мониторинга Kaspersky Endpoint Security относятся к использованию антивируса в режиме standalone (без использования Kaspersky Security Center и Агента администрирования)

Для отслеживания событий, происходящих в Kaspersky Endpoint Security, необходимо выполнить команду:

```
sudo kesl-control -W
```

Для проверки файла или директории на наличие вредоносного программного обеспечения необходимо выполнить команду:

```
sudo kesl-control --scan-file <путь к файлу>
```

Для просмотра общей информации о состоянии Kaspersky Endpoint Security необходимо выполнить команду:

```
sudo kesl-control --app-info
```

Удаление Kaspersky Endpoint Security и Агента администрирования

Для удаления Kaspersky Endpoint Security и Агента администрирования необходимо в командной строке (консоли) сервера, на котором установлено данное программное обеспечение, выполнить следующий скрипт:

```
sudo systemctl stop kesl
sudo systemctl disable kesl
sudo systemctl stop klnagent64
sudo systemctl disable klnagent64
sudo rm -rf /opt/kaspersky/* \
     /var/opt/kaspersky/* \
     /etc/opt/kaspersky/* \
     /etc/init.d/klnagent64 \
     /usr/lib/systemd/system/kesl.service \
     /etc/rc0.d/K01klnagent64 \
     /etc/rc1.d/K01klnagent64 \
     /etc/rc2.d/S01klnagent64 \
     /etc/rc3.d/S01klnagent64 \
     /etc/rc4.d/S01klnagent64 \
     /etc/rc5.d/S01klnagent64 \
     /etc/rc6.d/K01klnagent64 \

/etc/ssl/certs/Kaspersky_Anti_Virus_Personal_Root_Certificate_176929
93.pem \
     /etc/systemd/system/kesl.service \
     /etc/systemd/system/multi-user.target.wants/kesl.service \
     /usr/lib/systemd/system/kesl.service \     /usr/local/share/ca-
certificates/Kaspersky_Anti_Virus_Personal_Root_Certificate_17692993
.crt
```

IVA
TECHNOLOGIES

Learn more

https://iva.ru/
+7 495 134-66-77
info@iva.ru