СЕРВИСНЫЙ МАРШРУТИЗАТОР СЕРИИ ISN415
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СЕРВИСНОГО МАРШРУТИЗАТОРА CS
ИНСТРУКЦИЯ ПО НАСТРОЙКЕ С ПОМОЩЬЮ WEB-СЕРВЕРА
ВЕРСИЯ ПО 3.25.01

2026

СОДЕРЖАНИЕ

История изменений документа

Версия документа	Дата выпуска	Внесены изменения	Версия ПО

1 Подготовка сервисного маршрутизатора к работе с web-интерфейсом

Перед началом работы с web-интерфейсом на сервисном маршрутизаторе необходимо включить web-сервер. Далее приведен пример настройки сервисного маршрутизатора.

1.1 Описание настройки

В качестве основного устройства выбран сервисный маршрутизатор - RouterA (рисунок 1).

На RouterA настроен интерфейс vlan1 с IP-адресом 192.168.0.1/24. Также на данном маршрутизаторе настраивается web-сервер, который обеспечивает доступ к web-интерфейсу.

К сервисному маршрутизатору подключен PC на котором настроен IP-адрес 192.168.0.2/24. Это позволяет PC и RouterA находится в одной локальной сети, а также пользователь может получать доступ к web-ресурсам.

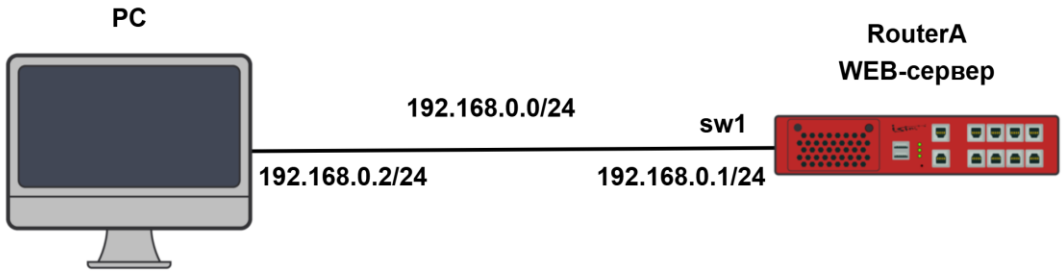


Рисунок 1 – Схема настройки web-сервера

1.2 Этапы настройки сети

1.2.1 Настройте IP-адрес 192.168.0.2/24 на PC

1.2.2 Войдите в режим глобальной конфигурации на устройствах перед настройкой

Конфигурационный режим - это один из режимов командной строки. В конфигурационном режиме можно изменять настройки интерфейсов, маршрутизацию, безопасность и другие параметры устройств.

ⓘ Напоминание

Router#configure terminal

1.2.3 Настройте RouterA

1.2.3.1 Настройте web-сервер на устройстве

```
RouterA(config)#web-server
RouterA(config-if-[eth1])#authentication basic
RouterA(config-if-[eth1])#on
RouterA(config-if-[eth1])#end
```

1.2.4 Сохраните настройки

Используйте команду **write <name>** для сохранения настроек на устройствах

ⓘ Напоминание

Router#write <name>

1.3 Проверка настроек

1.3.1 Выполните команду ping 192.168.0.1 на PC для проверки связности с RouterA

```
C:\Users\Conference>ping 192.168.0.1
```

```
Обмен пакетами с 192.168.0.1 по с 32 байтами данных:
Ответ от 192.168.0.1 число байт=32 время<1мс TTL=64
Ответ от 192.168.0.1 число байт=32 время<1мс TTL=64
Ответ от 192.168.0.1 число байт=32 время<1мс TTL=64
Ответ от 192.168.0.1 число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее =  0 мсек
```

1.3.2 Выполните команду show web-server для проверки конфигурации сервера

```
WebServer configuration

Status: enabled and running
VRF: default
Port: 443
Protocol: https
Host: any
Authentication: basic
SSL certificate: istok (OK)
```

1.3.3 Чтобы получить доступ к управлению маршрутизатором через веб-интерфейс, откройте браузер на PC и введите адрес https://192.168.0.1

1.4 Конфигурационный файл

Конфигурационный файл RouterA

```
configure terminal
web-server
authentication basic
on
end
write name
```

2 Первичная настройка сервисного маршрутизатора

ⓘ Напоминание

Для создания локальной сети с помощью сервисного маршрутизатора и подключения к внешней сети рекомендуется выполнить настройки описанные в данном разделе

2.1 Изменение пароля пользователя admin

⚠ Внимание!

Если на сервисном маршрутизаторе установлен логин и пароль по умолчанию "admin", "admin" обязательно смените пароль пользователя "admin"

Откройте вкладку "Управление пользователями" (рисунок 2).

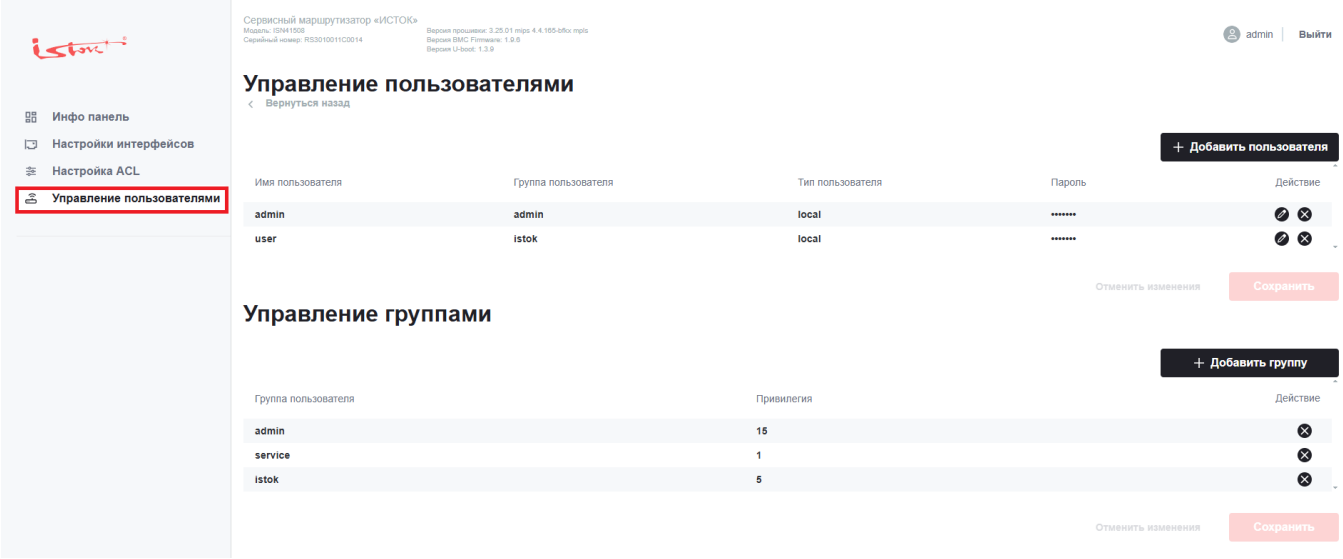


Рисунок 2 – Вкладка Настройки ACL

В разделе "Управление пользователями" нажмите пиктограмму "Изменить" (рисунок 3).

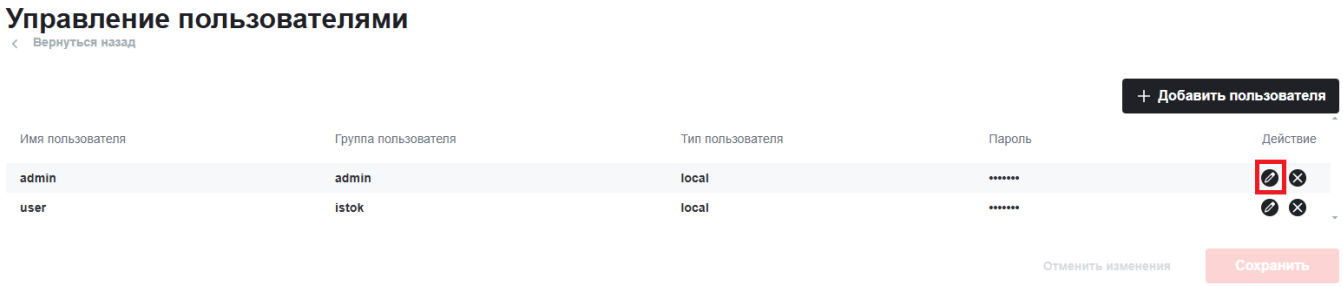


Рисунок 3 – Корректировка пользователя admin

В столбце "Пароль" задайте новый пароль для пользователя "admin". Обратите внимание, что пароль должен содержать не менее 9 символов и включать как минимум одну цифру и одну букву (рисунок 4).

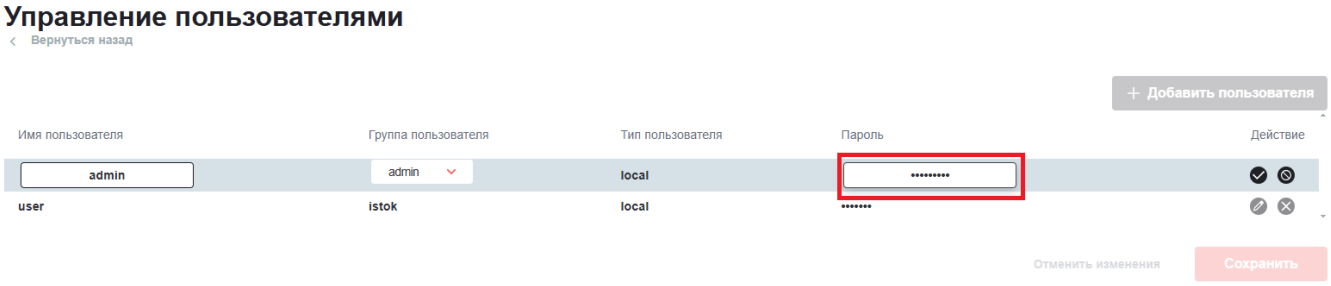


Рисунок 4 – Установка пароля

В столбце "Действие" нажмите на пиктограмму "Подтвердить" (рисунок 5).

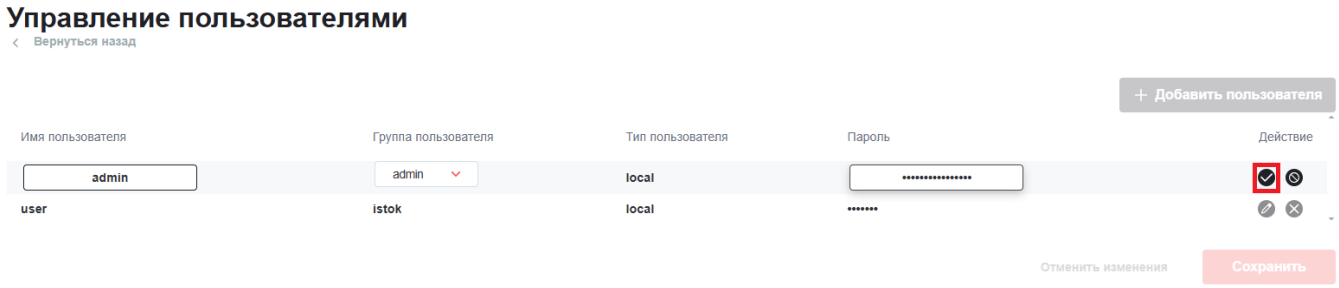


Рисунок 5 – Подтверждение изменений

Затем нажмите клавишу "Сохранить" (рисунок 6).

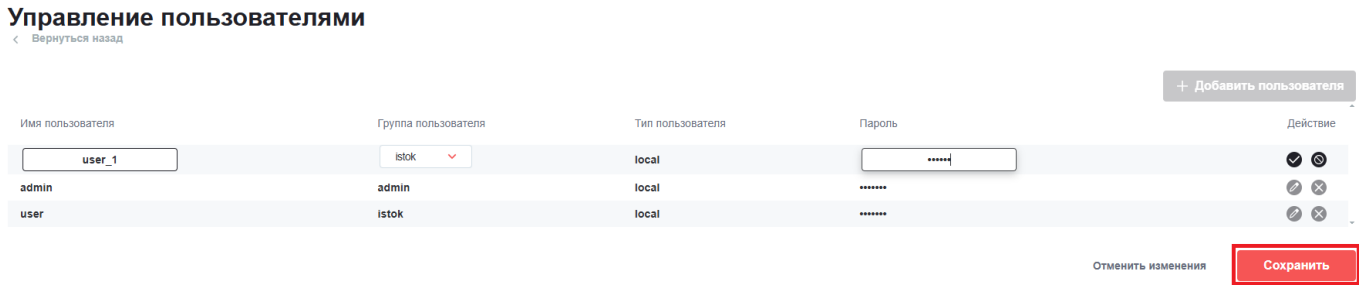


Рисунок 6 – Сохранение нового пароля

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 7).

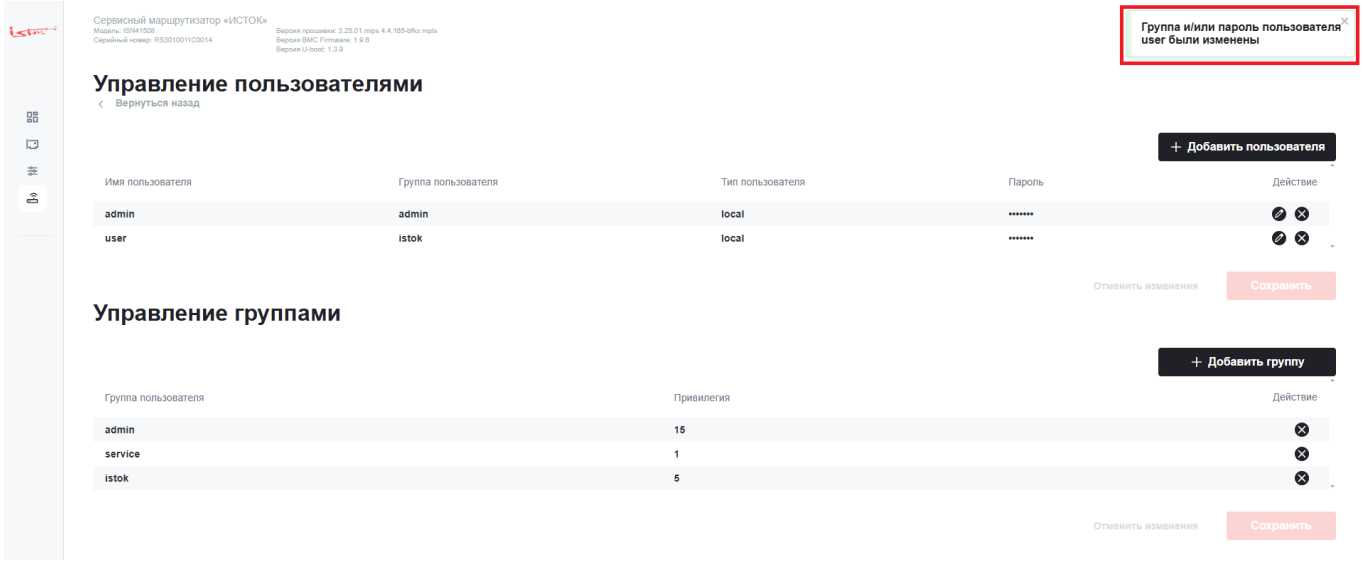


Рисунок 7 – Подтверждение сохранения

2.2 Настройка NAT masquerade

В данной настройке описывается пример перемаркировки пакетов на сервисном маршрутизаторе.

Откройте вкладку "Настройка ACL" (рисунок 8).

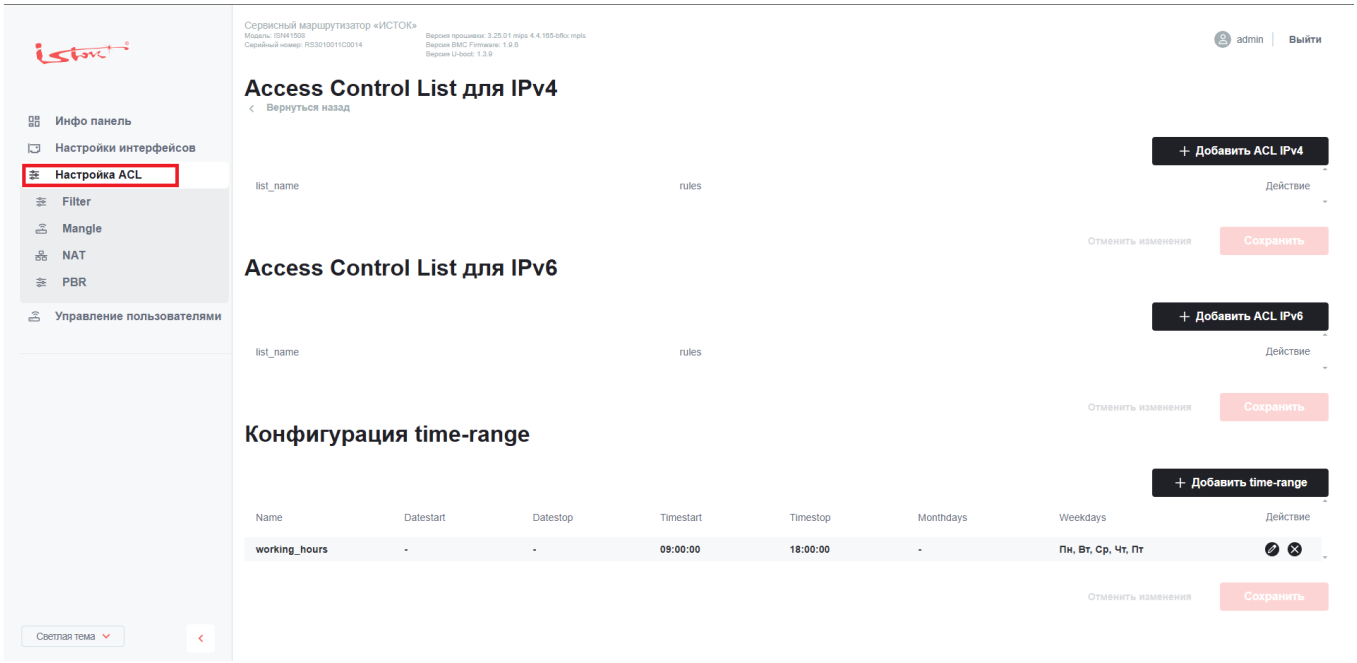


Рисунок 8 – Вкладка Настройки ACL

Создайте лист контроля доступа, нажмите кнопку "+Добавить ACL IPv4" (рисунок 9).

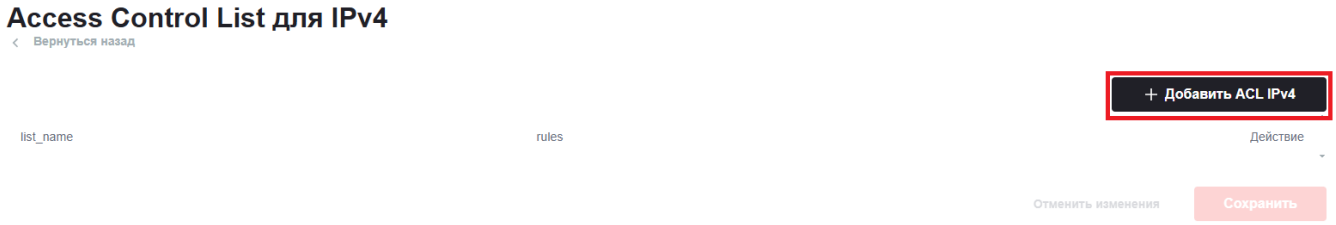


Рисунок 9 – Добавление списком управления доступом

В поле столбца "list_name" введите наименование листа без пробелов "nat_masquerade". В поле столбца "rules" выберите из выпадающего списка правило "outinterface" (рисунок 10).

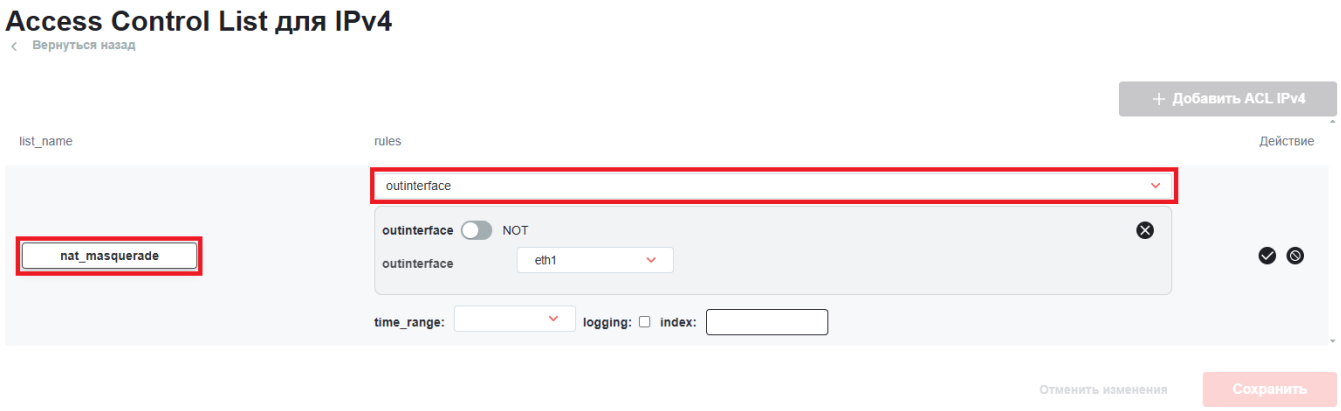


Рисунок 10 – Выбор правила

После добавления правила "outinterface" отобразится блок с настройками правила (рисунок 11).

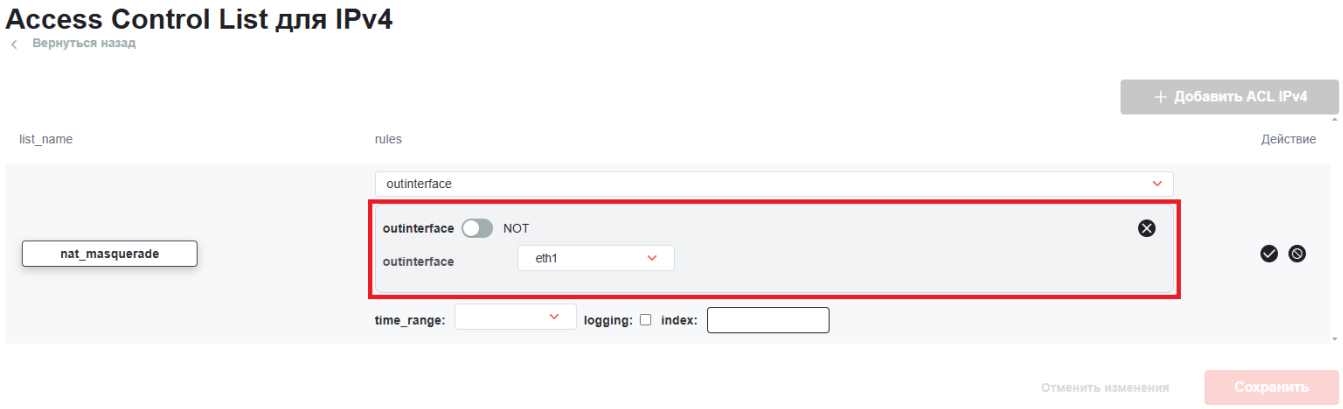


Рисунок 11 – Блок настройки правила

В поле "outinterface" выберите из выпадающего списка протокол "eth1" (рисунок 12).

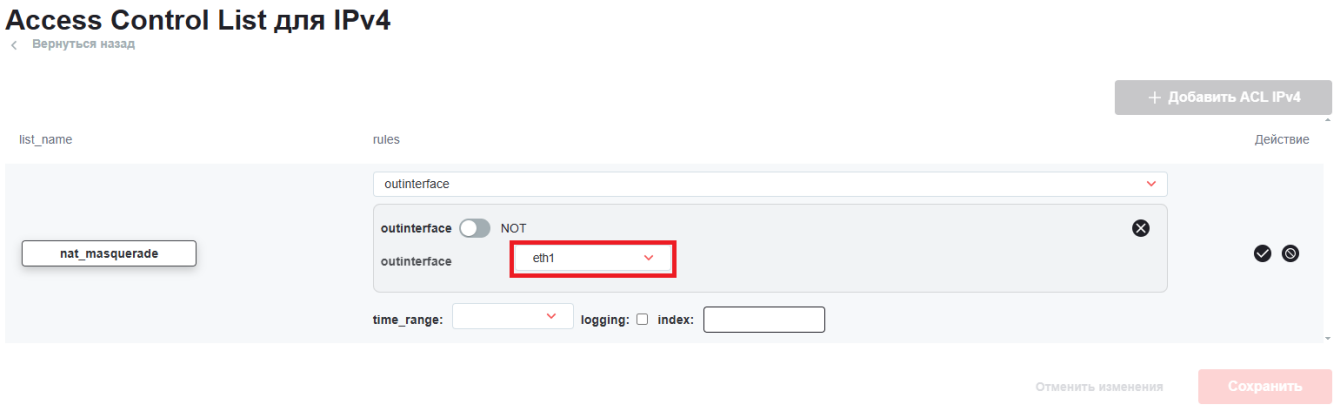


Рисунок 12 – Выбор протокола

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 13).

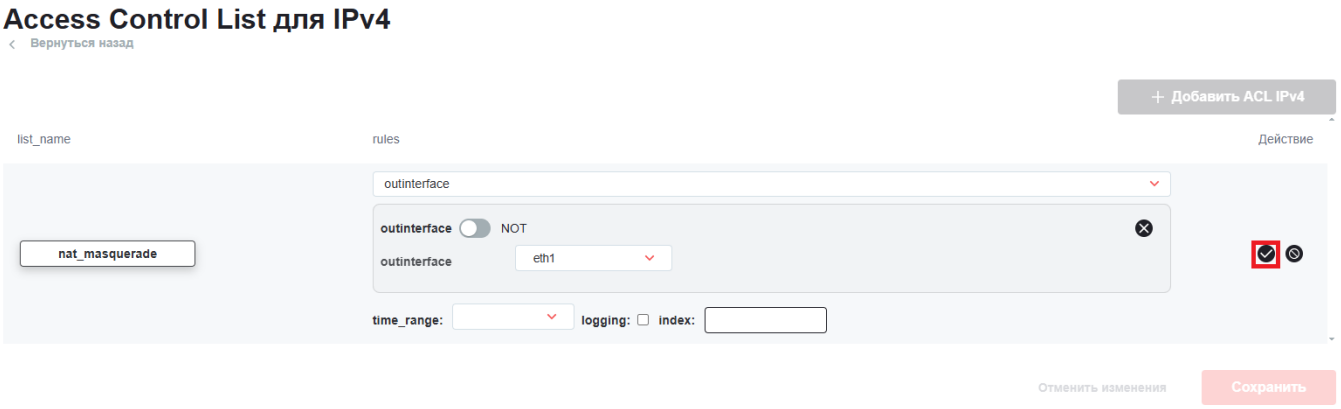


Рисунок 13 – Подтверждение создания списка

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 14).

Рисунок 14 – Сохранение списка

Для перемаркировки пакетов по правилу листа контроля доступа необходимо добавить листу NAT. Откройте вкладку "NAT" (рисунок 15).

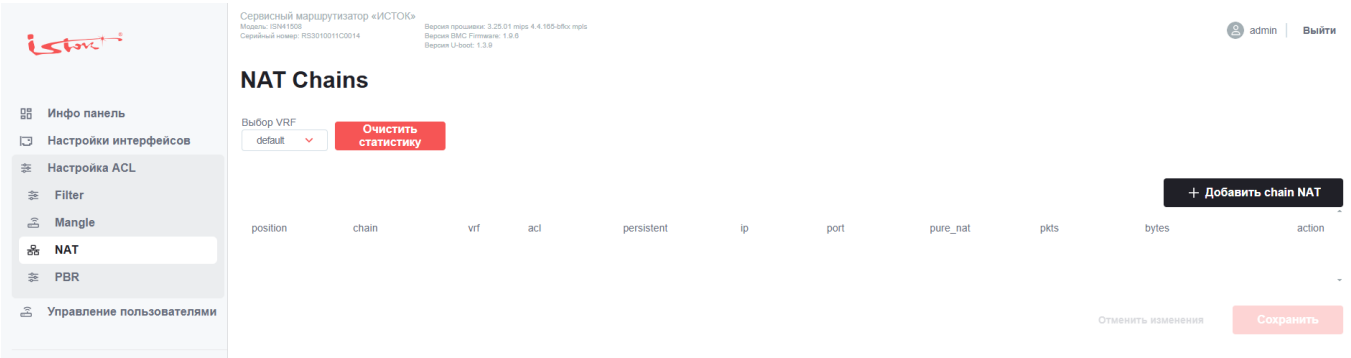


Рисунок 15 – Вкладка Filter

Нажмите кнопку "+Добавить chain NAT" (рисунок 16).

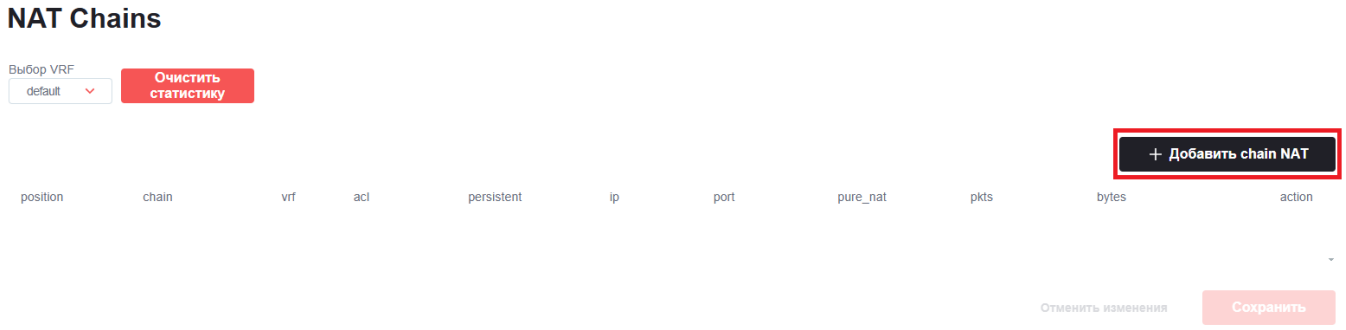


Рисунок 16 – Добавление NAT

Настройте NAT выполнив следующие действия (рисунок 17):

- в поле столбца "position" введите "1";
- в столбце "chain" выберите из выпадающего списка "postrouting";
- в столбце "acl" выберите из выпадающего списка "port_blocking" (наименование созданного ACL);
- в столбце "pure_nat" включите кнопку-переключатель.

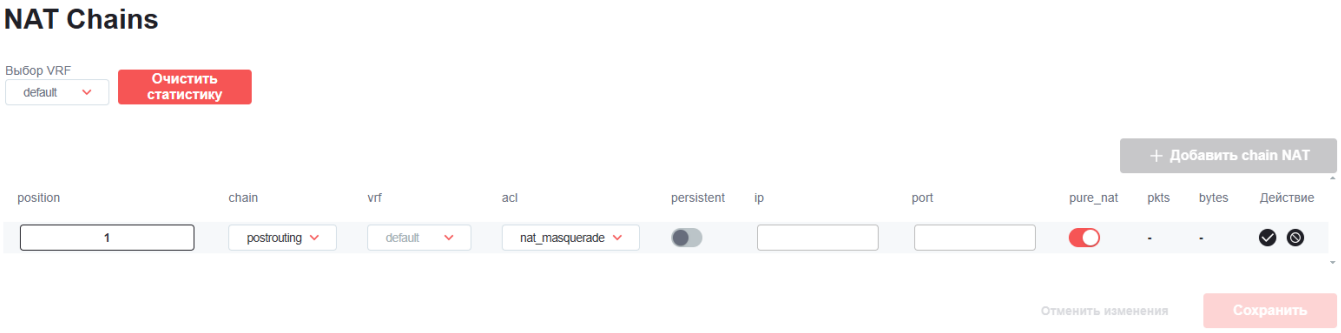


Рисунок 17 – Настройка NAT

Подтвердите создание NAT, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 18).

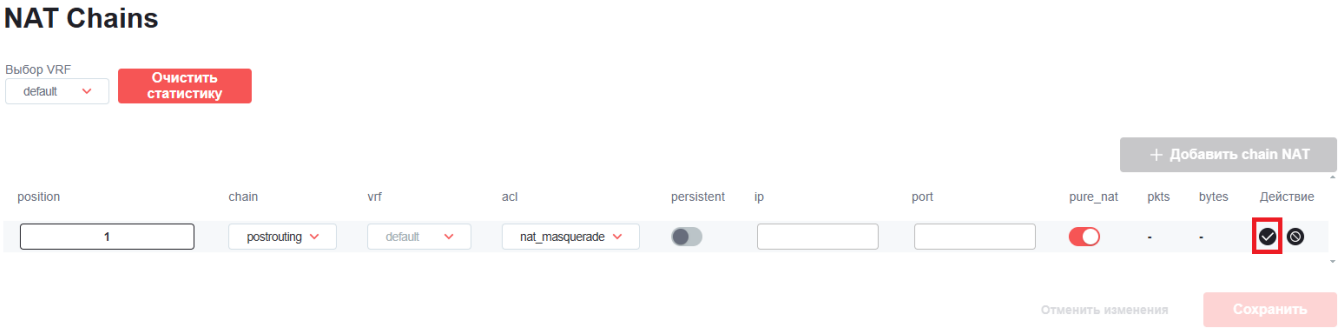


Рисунок 18 – Подтверждение создания NAT

Затем нажмите клавишу "Сохранить" (рисунок 19).

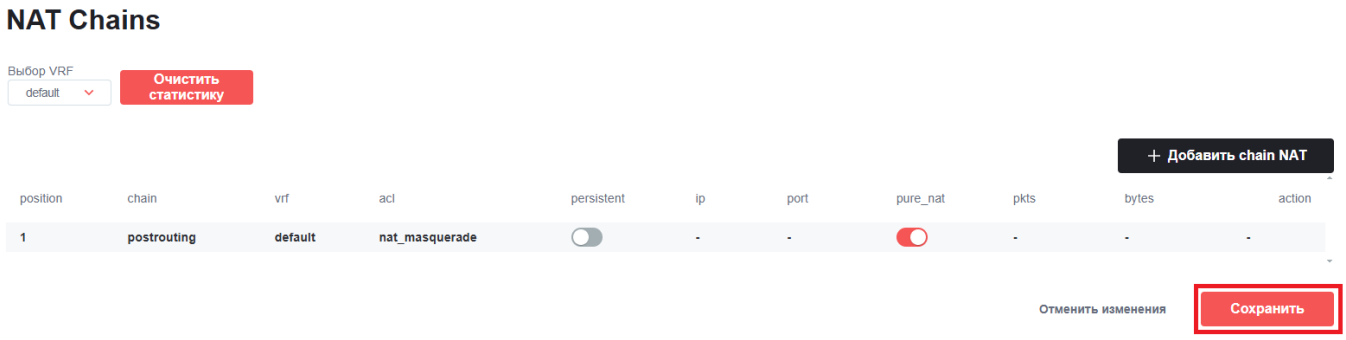


Рисунок 19 – Сохранение фильтра

Успешно добавленный NAT будет иметь следующий вид (рисунок 20).

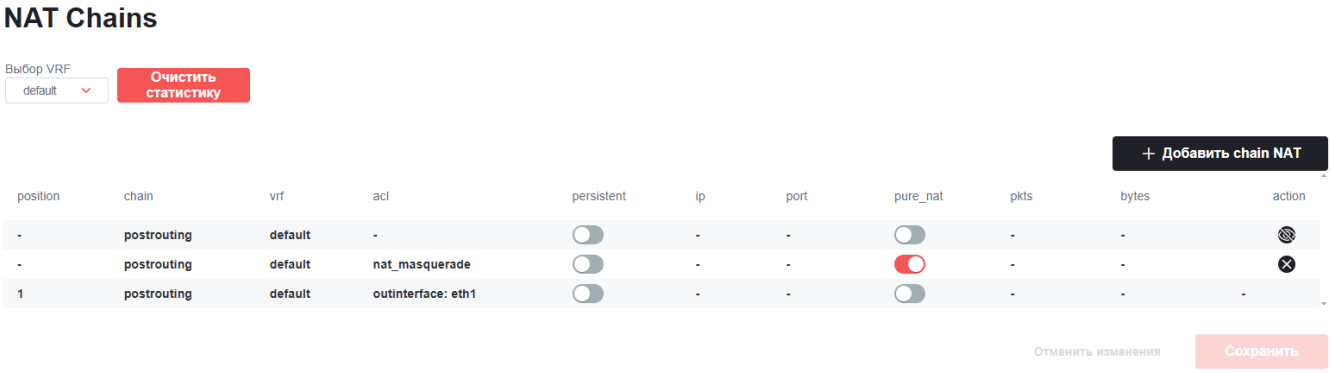


Рисунок 20 – Отображение NAT

После этого настройка считается завершенной.

2.3 Настройка ограничения доступа по номеру порта

В данной настройке ограничим доступ к сервисному маршрутизатору по номеру порта входящего трафика.

Откройте вкладку "Настройка ACL" (рисунок 21).

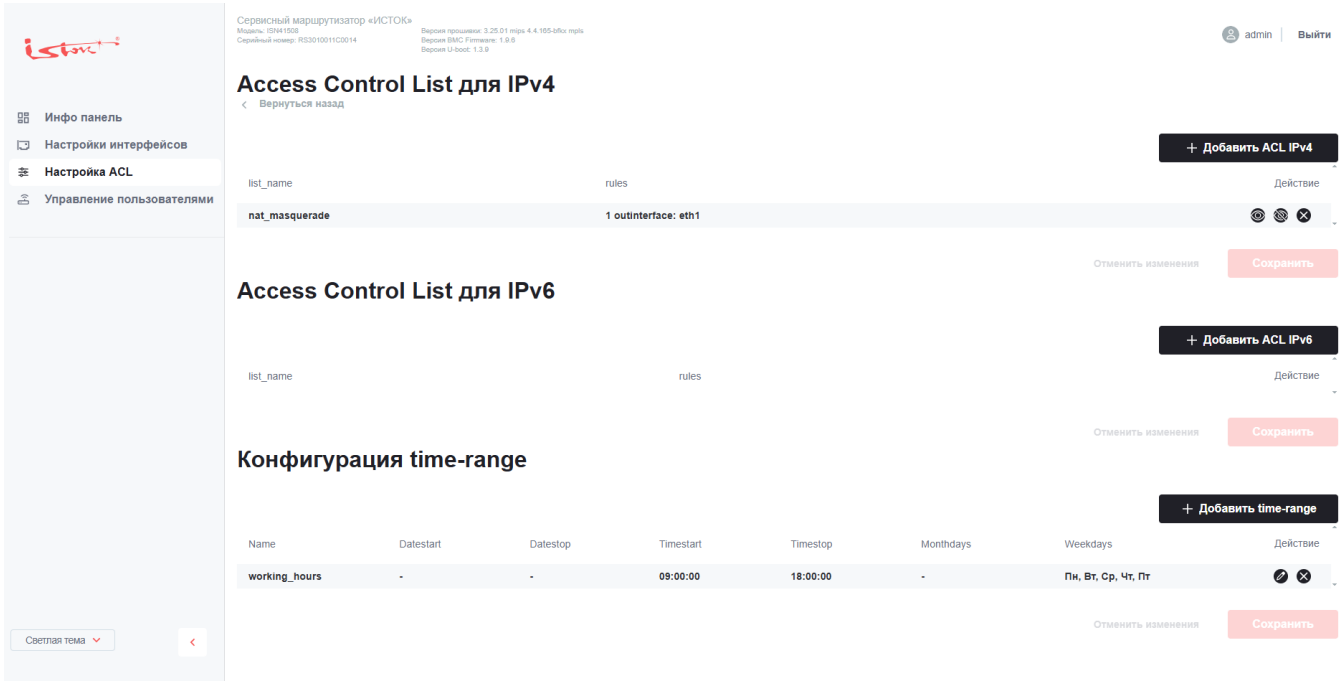


Рисунок 21 – Вкладка Настройки ACL

Создайте лист контроля доступа, нажмите кнопку "+Добавить ACL IPv4" (рисунок 22).

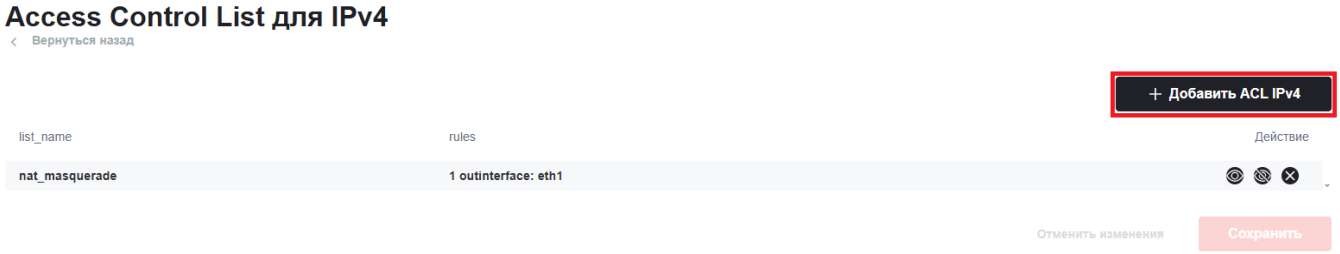


Рисунок 22 – Добавление списком управления доступом

В поле столбца "list_name" введите наименование листа без пробелов "port_blocking". В поле столбца "rules" выберите из выпадающего списка правило "protocol" (рисунок 23).

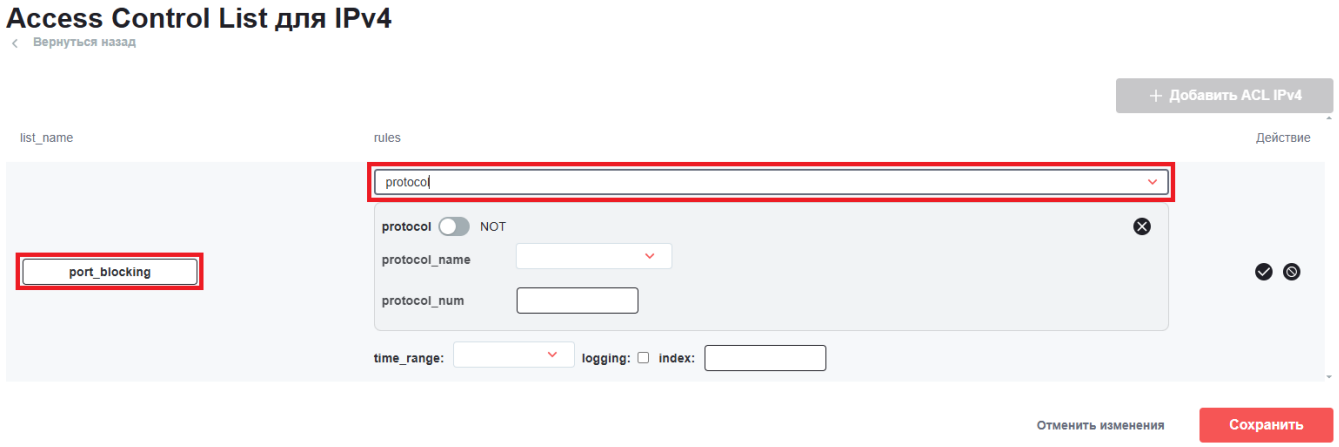


Рисунок 23 – Выбор правила

После добавления правила "protocol" отобразится блок с настройками правила (рисунок 24).

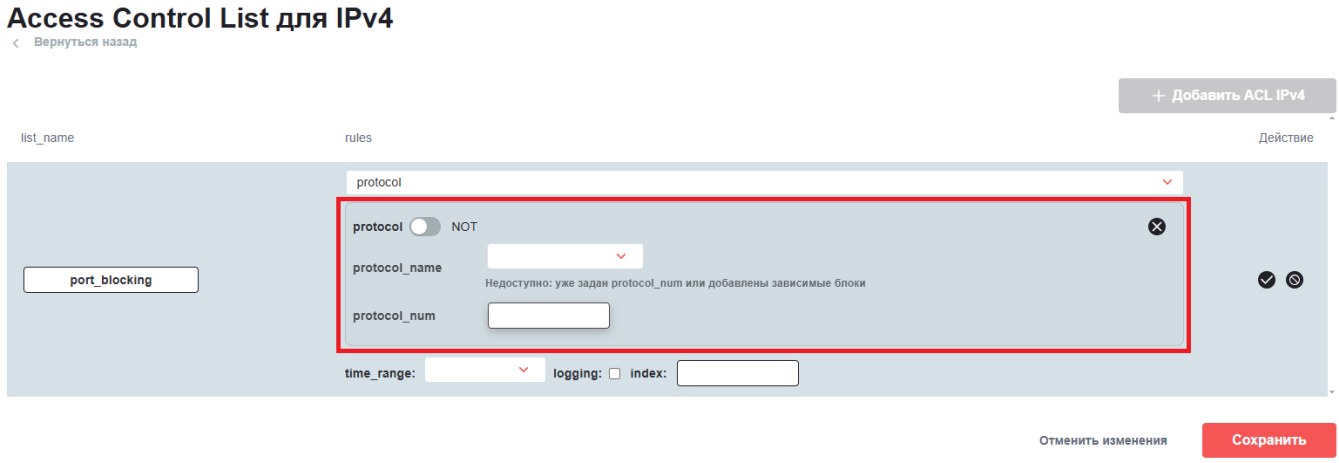


Рисунок 24 – Блок настройки правила

В поле "protocol_name" выберите из выпадающего списка протокол "tcp" (рисунок 25).

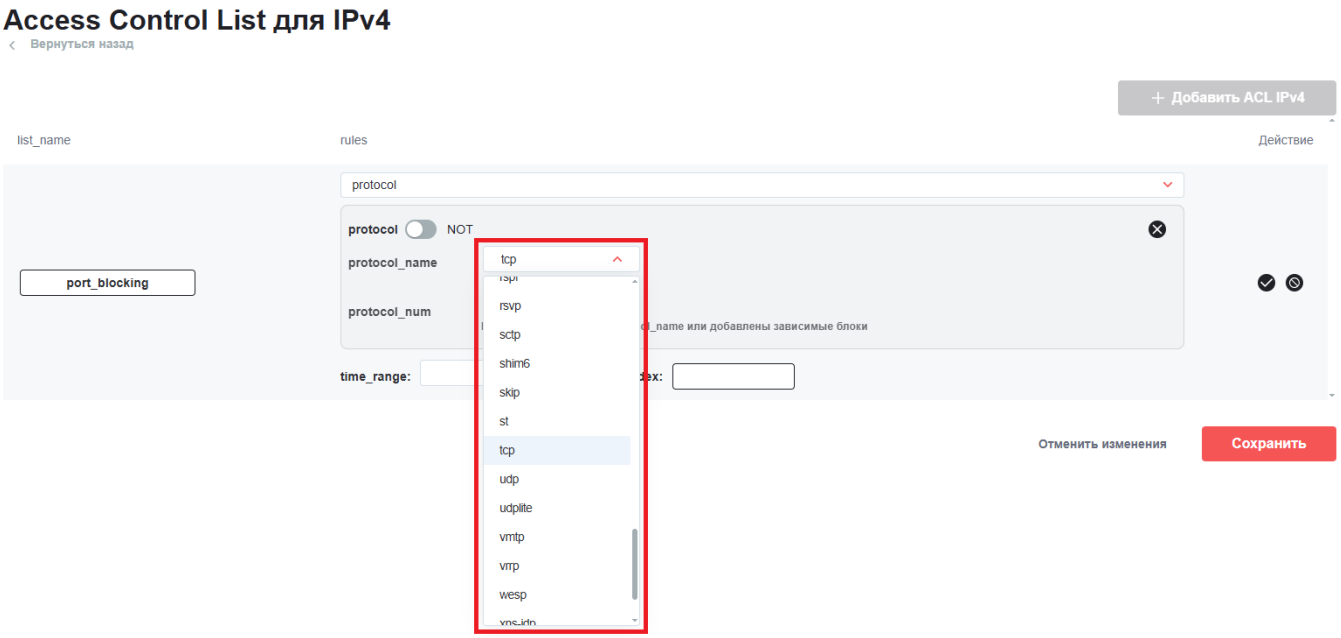


Рисунок 25 – Выбор протокола

Не завершая настройку листа контроля доступом выберите в столбце "rules" из выпадающего списка правило "destinationports" (рисунок 26).

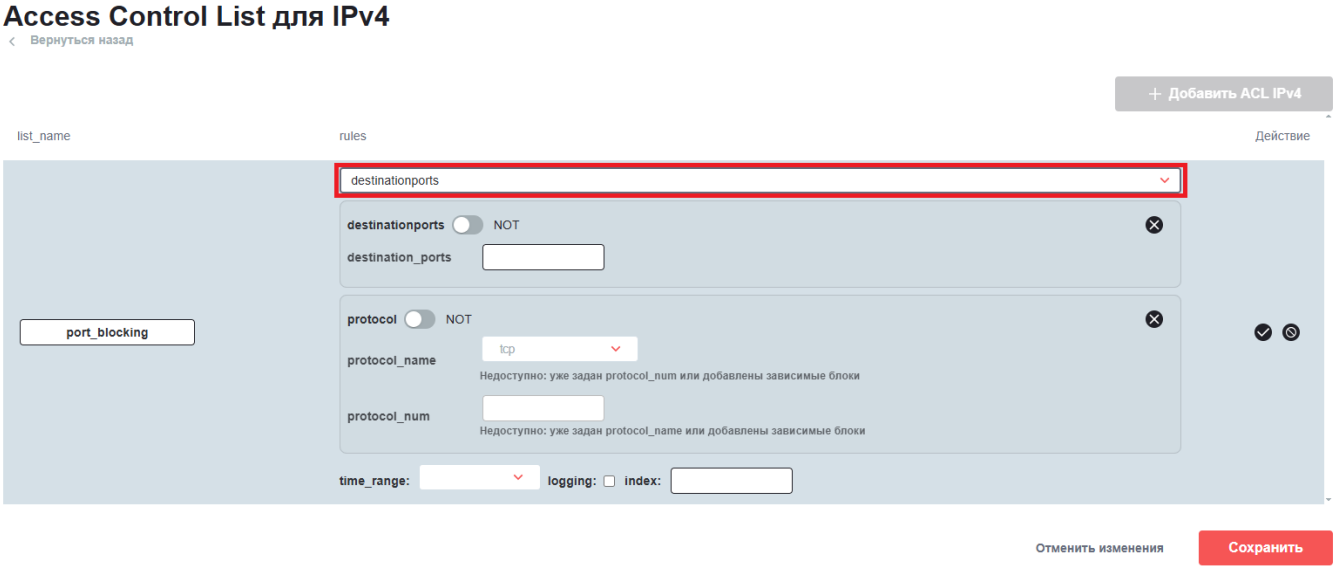


Рисунок 26 – Выбор занесения срабатывания правила в лог

После добавления правила "destinationports" отобразится блок с настройками правила (рисунок 27).

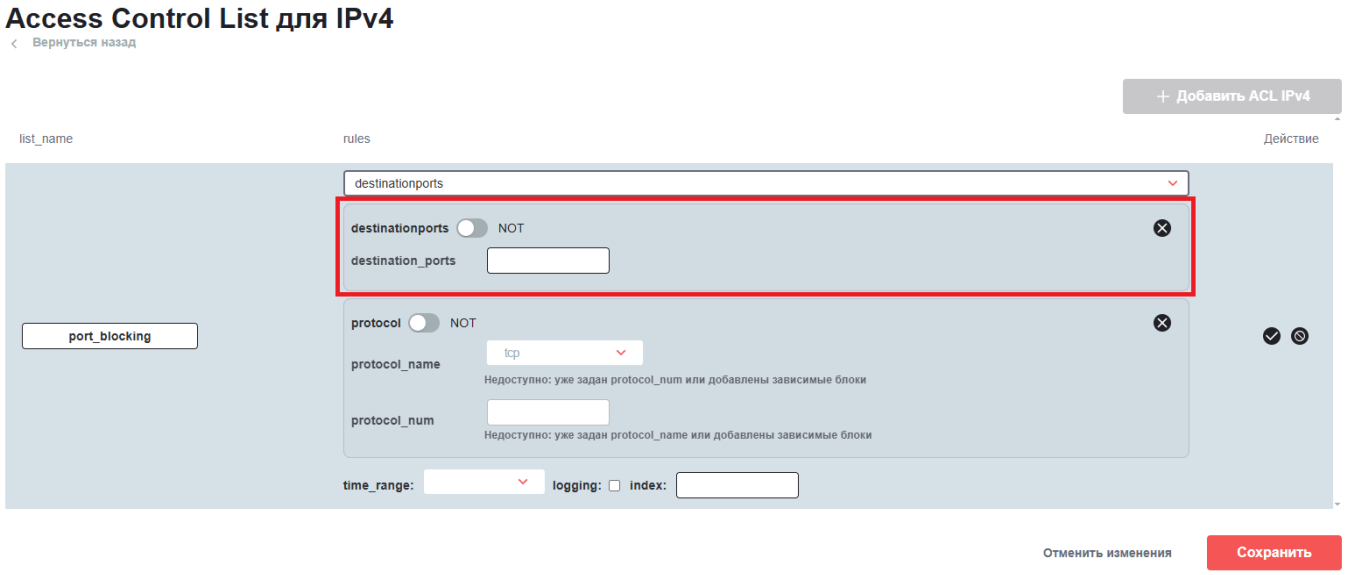


Рисунок 27 – Блок настройки правила

В поле "destination_ports" введите номера портов "80,8080,443,8082" (рисунок 28).

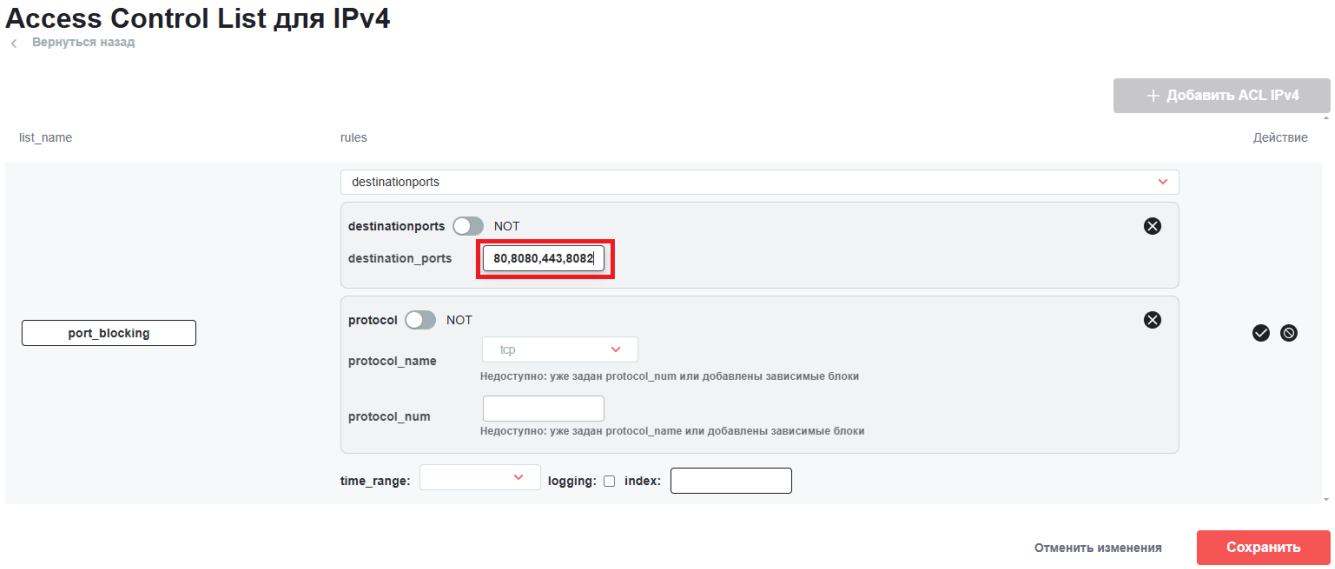


Рисунок 28 – Выбор портов

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 29).

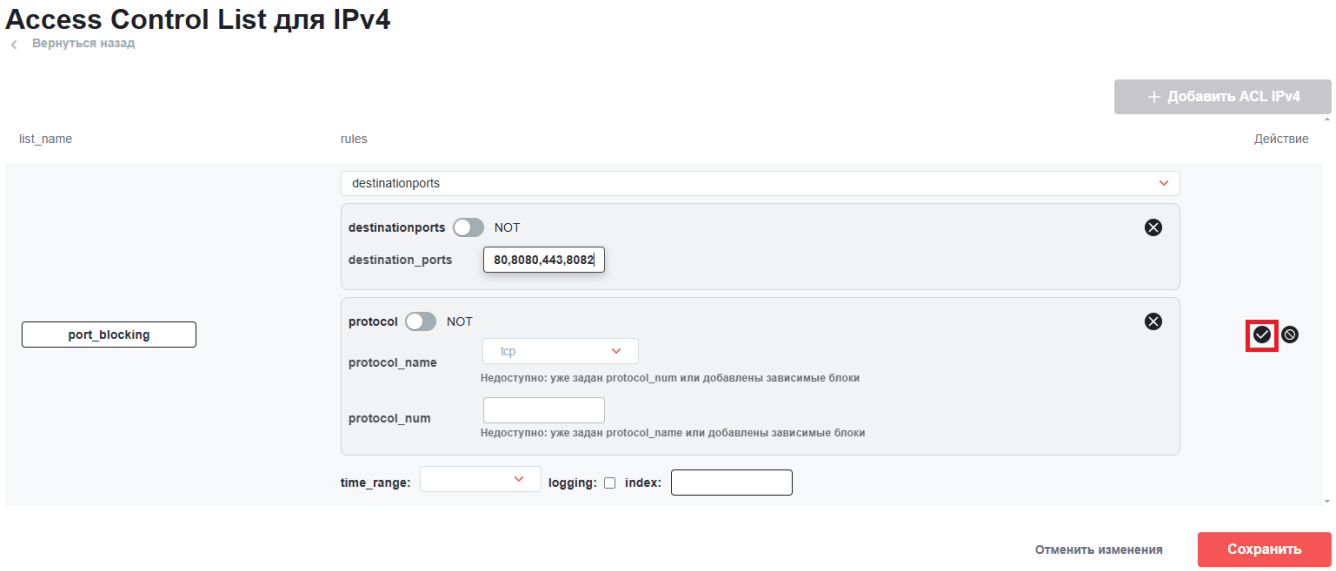


Рисунок 29 – Подтверждение создания списка

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 30).

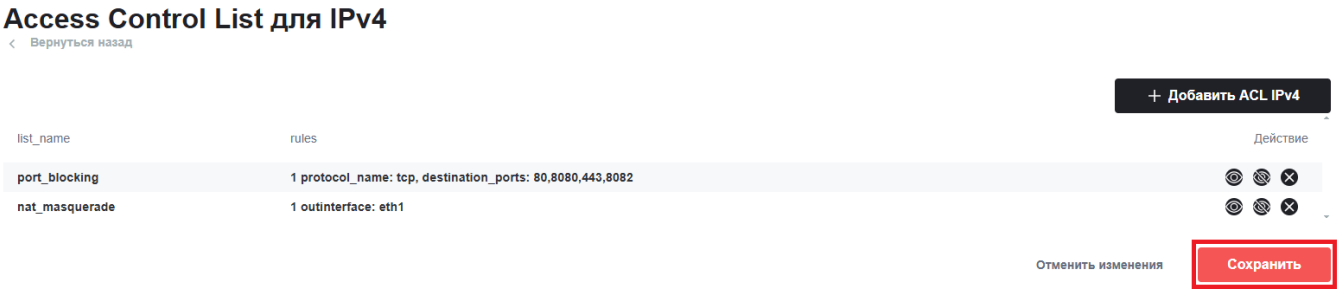


Рисунок 30 – Сохранение списка

Создайте еще один лист контроля доступа, нажмите кнопку "+Добавить ACL IPv4". В поле столбца "list_name" введите наименование листа без пробелов "allowed_ip_addresses4ports". В поле столбца "rules" выберите из выпадающего списка правило "protocol" (рисунок 31).

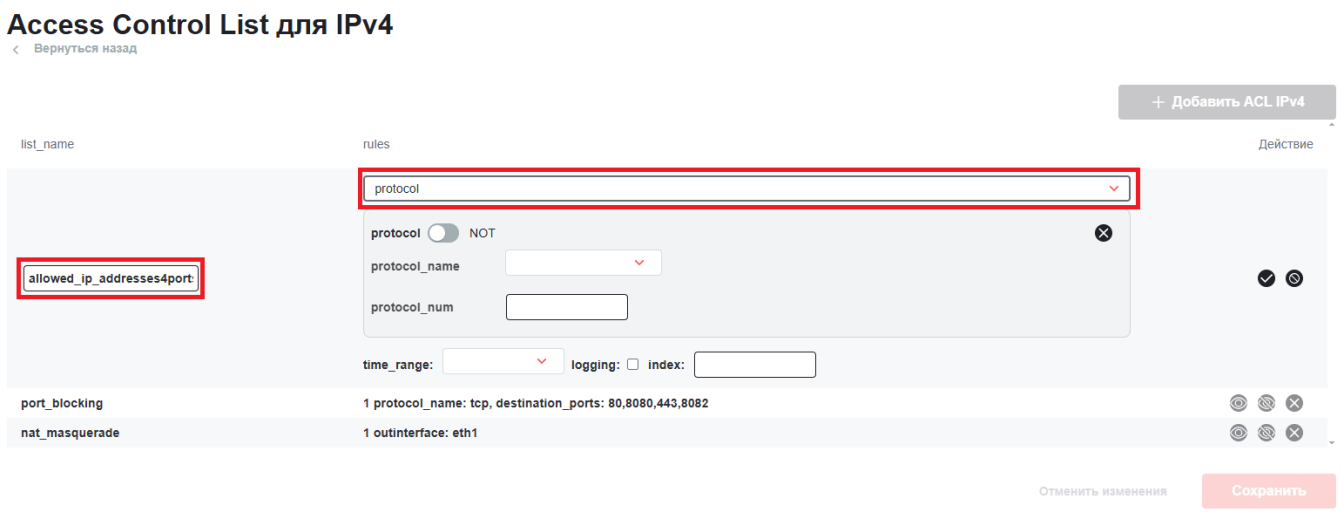


Рисунок 31 – Выбор правила

В поле "protocol_name" выберите из выпадающего списка протокол "tcp" (рисунок 32).

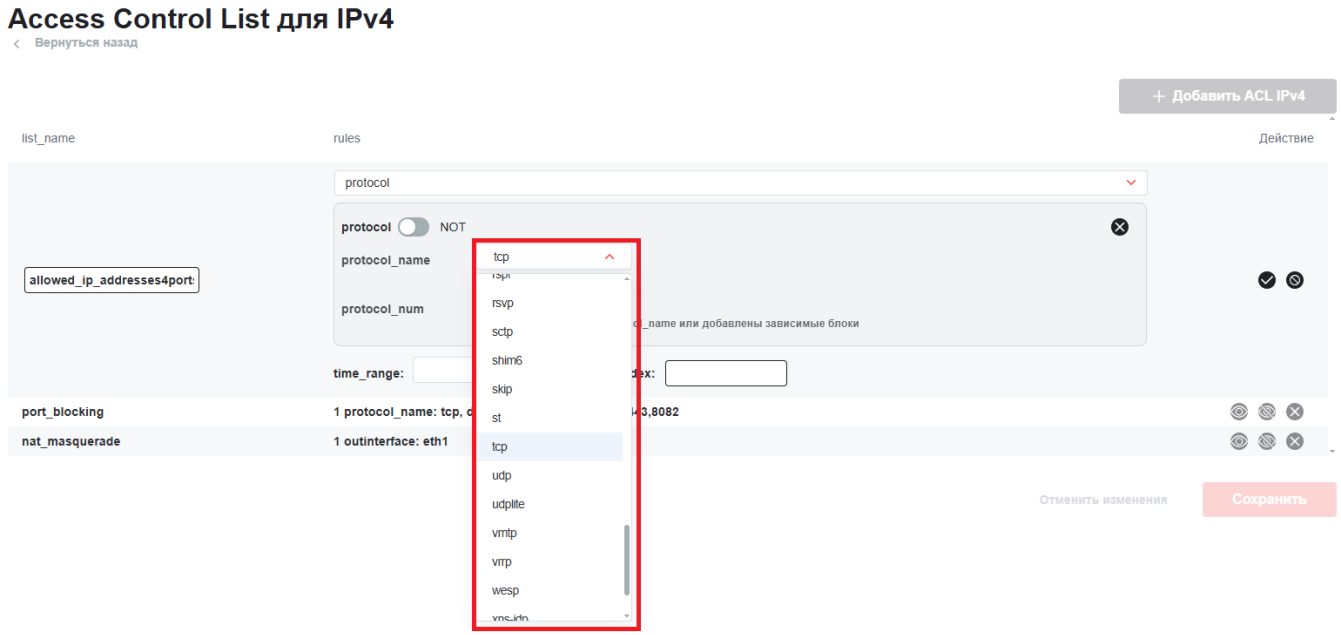


Рисунок 32 – Выбор протокола

Не завершая настройку листа контроля доступом выберите в столбце "rules" из выпадающего списка правило "destinationports" и "sourceip". После добавления правил отобразятся блоки с настройками правил (рисунок 33).

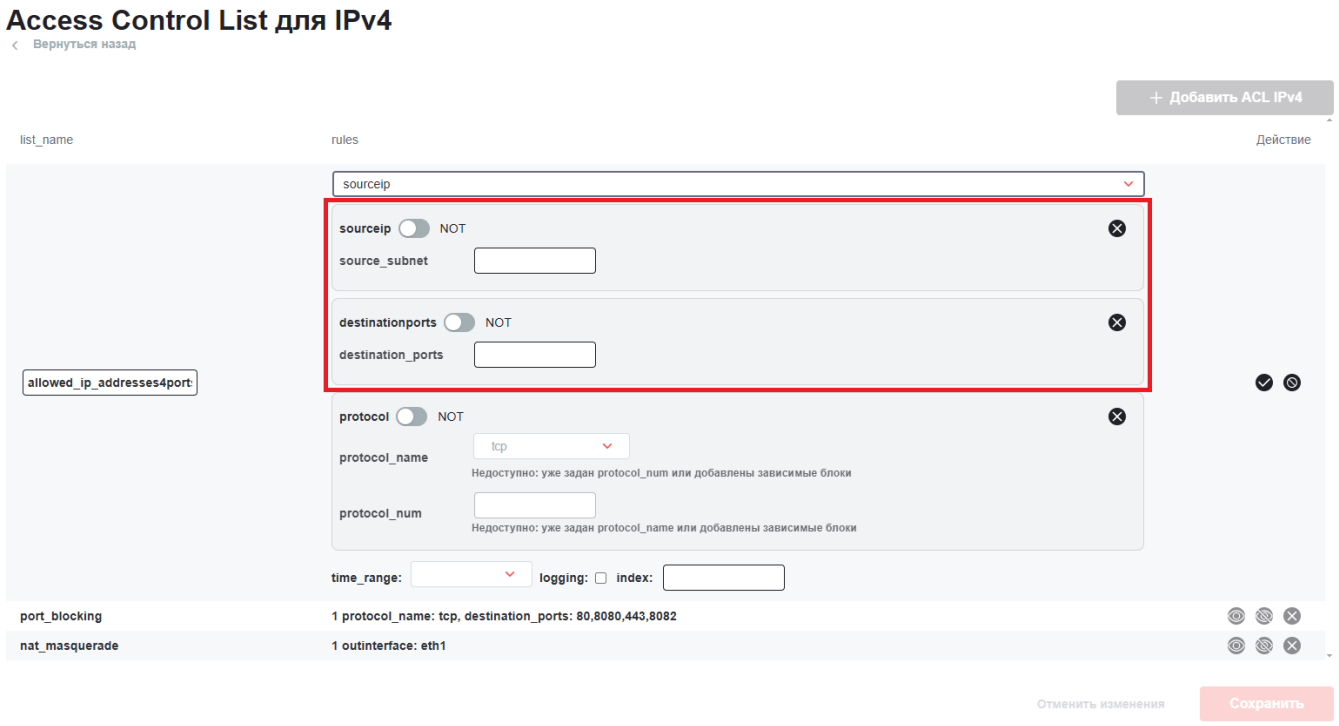


Рисунок 33 – Блок настройки правила

В поле "source_subnet" введите ip-адрес и маску "192.168.0.1/24". В поле "destination_ports" введите номера портов "80,8080,443,8082". (рисунок 28).

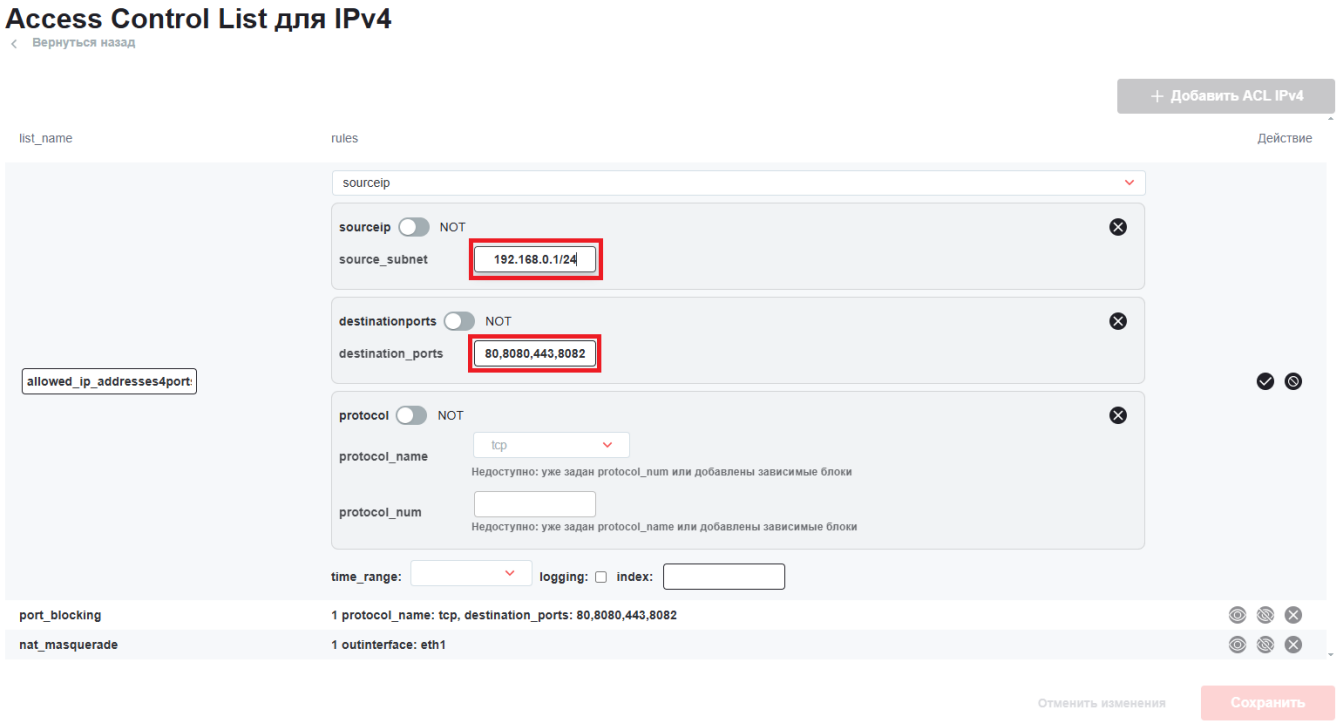


Рисунок 34 – Выбор портов

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие". Сохраните список управления доступом, нажав кнопку "Сохранить". Успешно добавленные списки контроля доступом будет иметь следующий вид (рисунок 35).

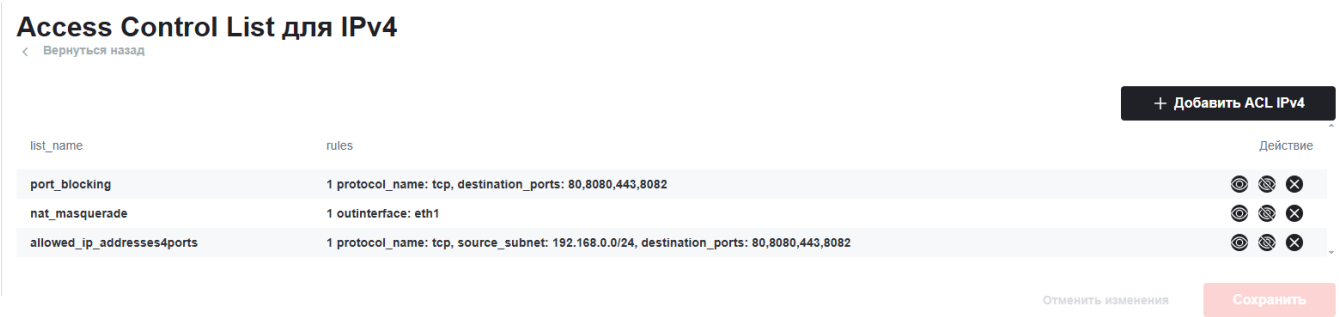


Рисунок 35 – Отображение списков контроля доступом

Для срабатывания правил листа контроля доступа необходимо добавить лист фильтру. Откройте вкладку "Filter" (рисунок 36).

Рисунок 36 – Вкладка Filter

Добавьте фильтр обеспечивающий доступ к VLAN-интерфейсу 192.168.0.1. Для этого нажмите кнопку "+Добавить ACL Filter IPv4" (рисунок 37).

Рисунок 37 – Добавление фильтра

Настройте фильтр выполнив следующие действия (рисунок 38):

- в поле столбца "index" введите "1" (очередность срабатывания фильтров);
- в столбце "chain" выберите из выпадающего списка "input" (применять к входящим пакетам);
- в столбце "acl" выберите из выпадающего списка "allowed_ip_addresses4ports" (наименование созданного ACL);
- в столбце "action" выберите из выпадающего списка "permit" (разрешить пакет).

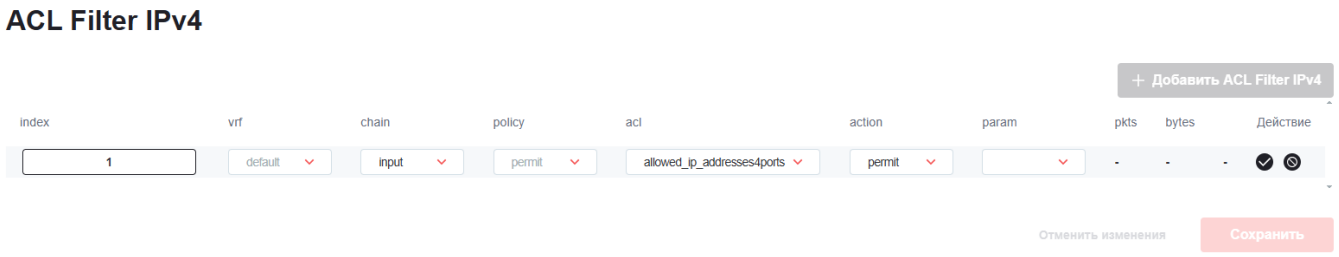


Рисунок 38 – Настройка фильтра

Подтвердите создание фильтра, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 39).

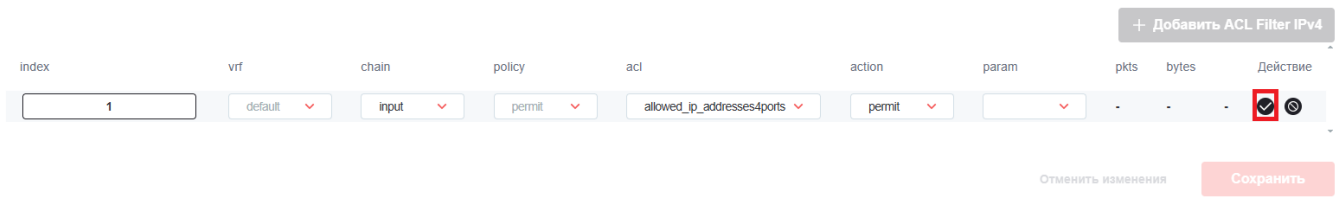


Рисунок 39 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 40).

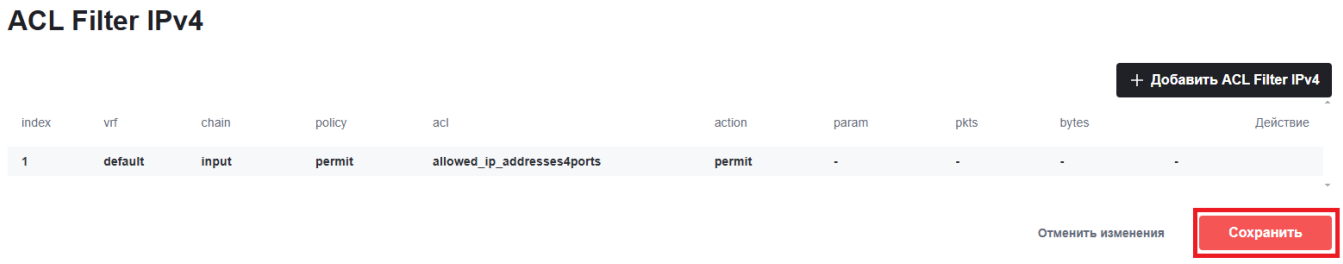


Рисунок 40 – Сохранение фильтра

Добавьте фильтр ограничивающий доступ к портам сервисного маршрутизатора. Нажмите кнопку "+Добавить ACL Filter IPv4".

Настройте фильтр выполнив следующие действия (рисунок 41):

- в поле столбца "index" введите "2" (очередность срабатывания фильтров);
- в столбце "chain" выберите из выпадающего списка "input" (применять к входящим пакетам);
- в столбце "acl" выберите из выпадающего списка "port_blocking" (наименование созданного ACL);
- в столбце "action" выберите из выпадающего списка "deny" (блокировать пакет).

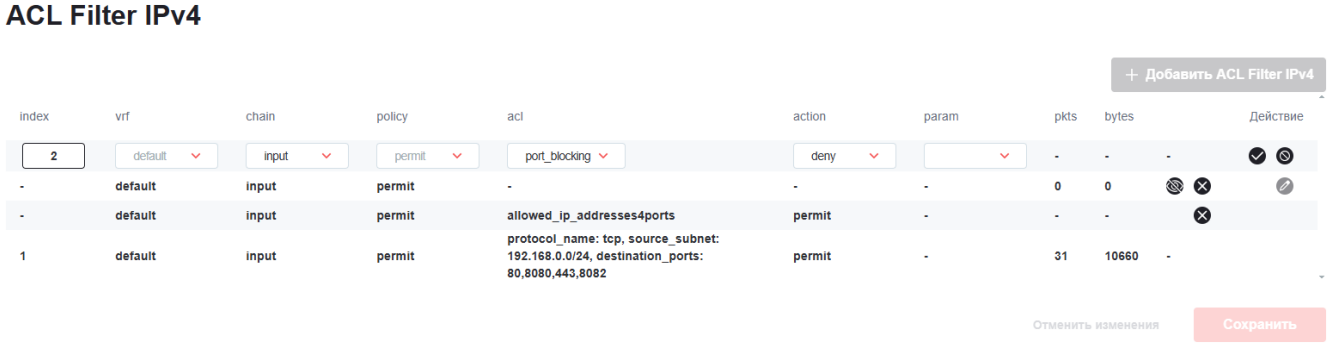


Рисунок 41 – Настройка фильтра

Подтвердите создание фильтра, нажав на пиктограмму "Подтвердить" в столбце "Действие". Затем нажмите клавишу "Сохранить". Успешно добавленный фильтр будет иметь следующий вид (рисунок 42).

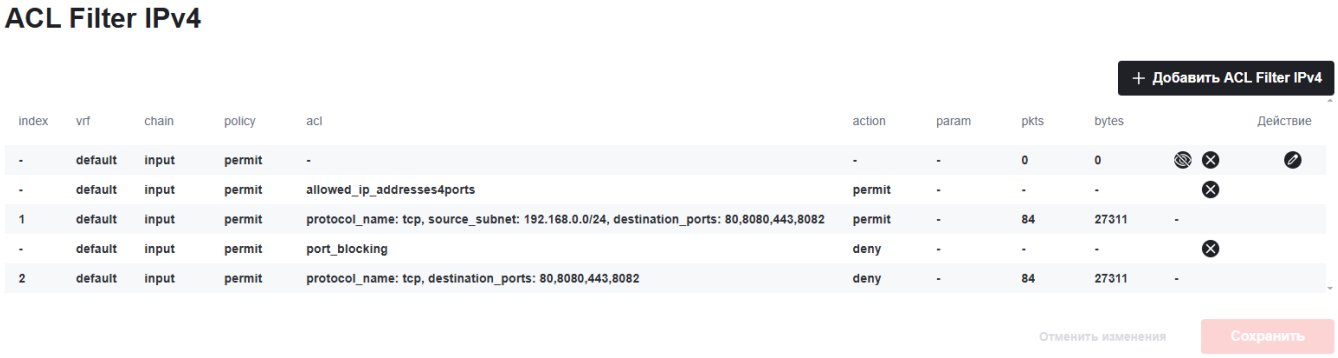


Рисунок 42 – Отображение фильтра

После этого настройка считается завершенной.

3 Авторизация

После перехода на веб-страницу https://192.168.0.1 вы можете выполнить авторизацию в системе (рисунок 43).

Рисунок 43 – Авторизация

Примечание

По умолчанию имя пользователя и пароль установлены как "admin".

Для этого введите в соответствующие поля имя пользователя и пароль, затем нажмите кнопку "Войти" (рисунок 44).

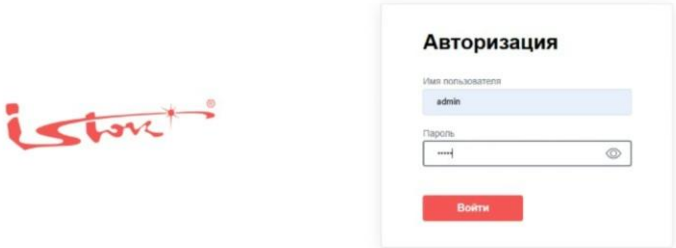


Рисунок 44 – Ввод логина и пароля

В случае успешной авторизации на экране появится уведомляющее окно, подтверждающее успешный вход в систему (рисунок 45).

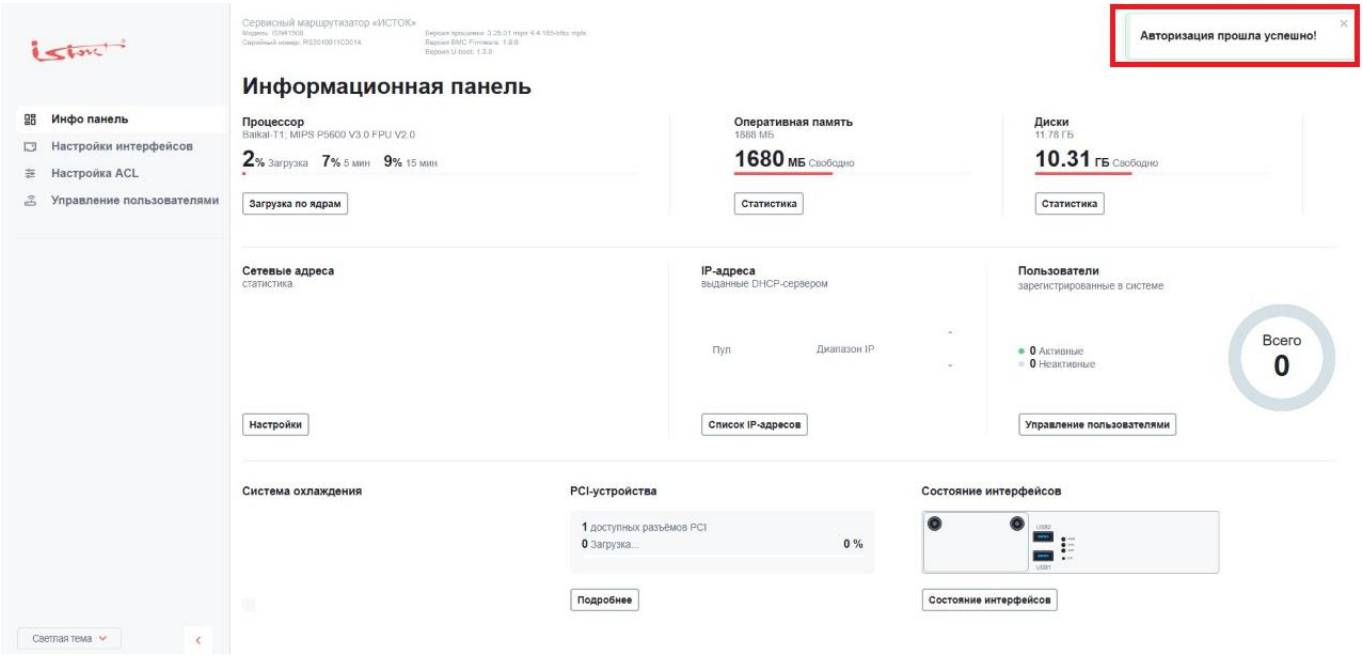


Рисунок 45 – Уведомление об успешной авторизации

После авторизации в верхнем углу страницы будет отображаться информация о вашем профиле, а также будет предоставлена возможность выхода из системы (рисунок 46).

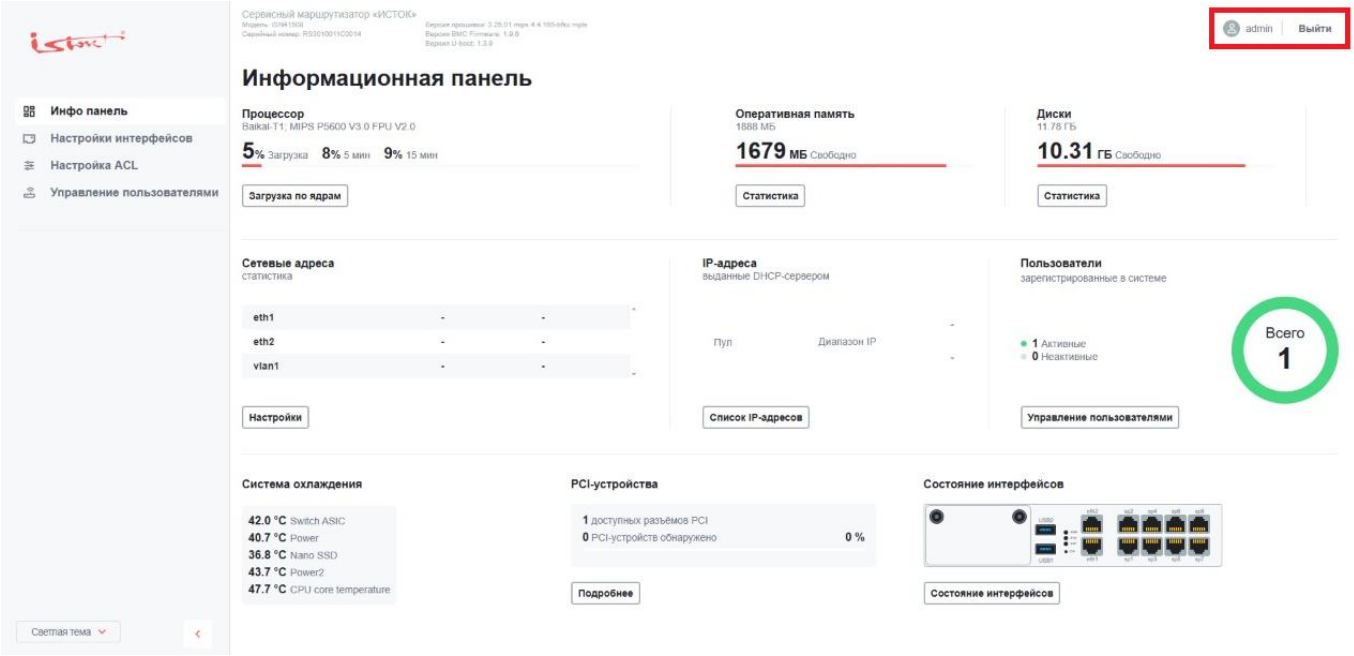


Рисунок 46 – Профиль

4 Информационная панель

Примечание

Чтобы получить доступ к управлению маршрутизатором через веб-интерфейс, откройте браузер и введите в адресной строке адрес - 10.0.0.1. В окне отобразиться главная страница - Информационная панель.

Информационная панель обеспечивает оперативный обзор состояния аппаратных компонентов и служб, включая загрузку процессора (CPU), использование оперативной и дисковой памяти, состояние сетевых интерфейсов, IP-адресацию, активных пользователей, данные температурных датчиков, информацию о обнаруженных устройствах PCI, а также статус портов (рисунок 47). В верхней части информационной панели отображаются основные сведения об устройстве такие как название устройства, модель, серийный номер, версия прошивки, версия BMC Firmware и версия U-boot.

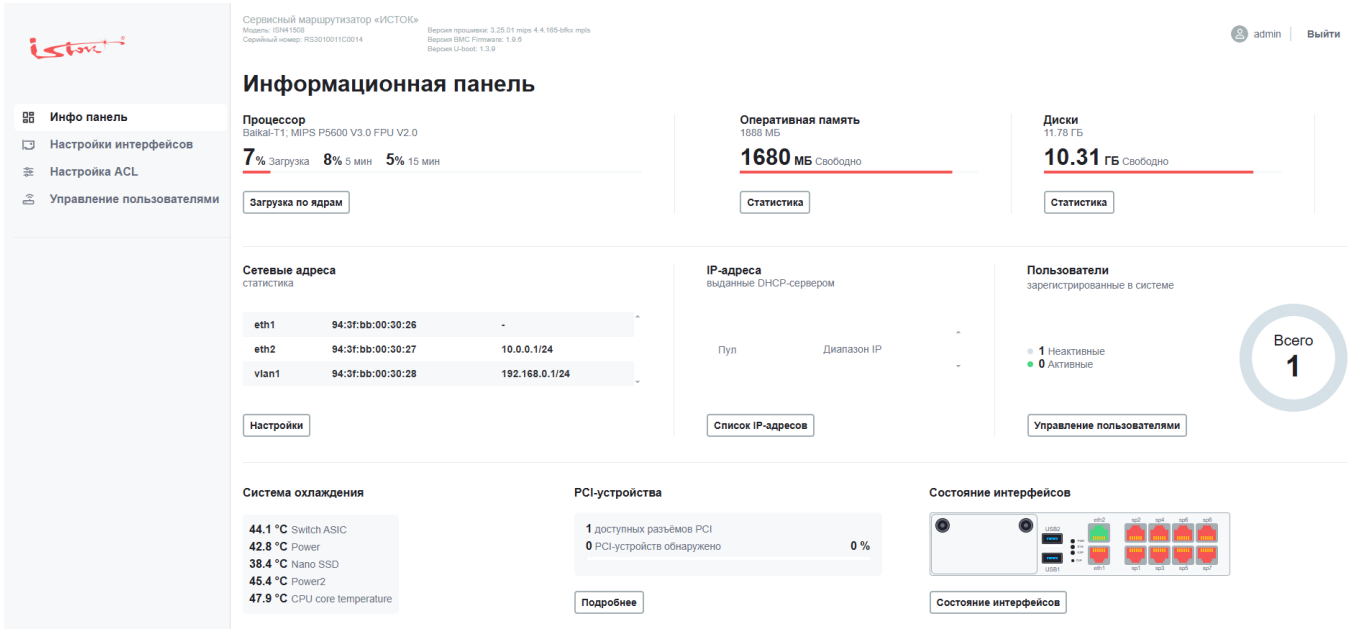


Рисунок 47 – Информационная панель

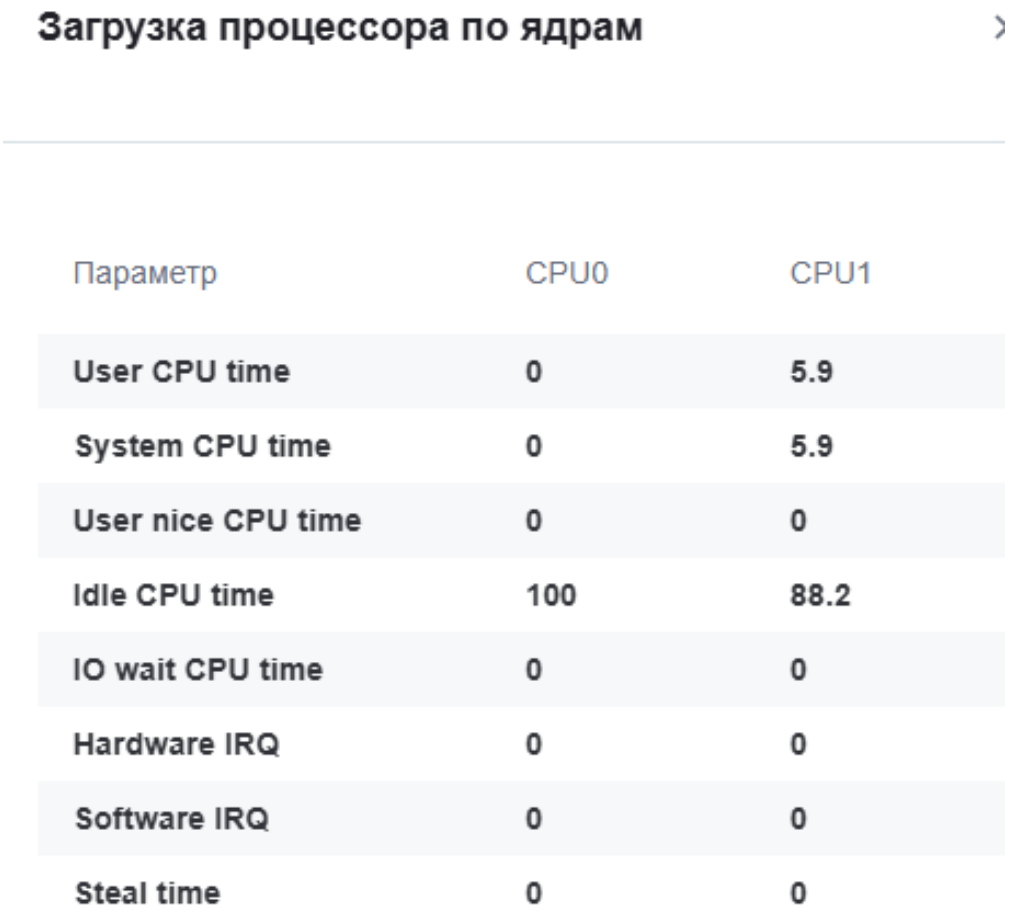
4.1 Процессор

В части информационной панели "Процессоры" отображается информация о модели процессора, текущей загрузке в процентах, а также средние значения загрузки в

процентах за последние 5 и 15 минут. Также представлена визуальная индикация уровня загрузки (рисунок 48).

Рисунок 48 – Блок "Процессор"

Нажав на клавишу "Загрузка процессора по ядрам" отображается таблица с параметрами загрузки для каждого ядра и процентными значениями для CPU0 и CPU1 (рисунок 49).



Загрузка процессора по ядрам

Параметр	CPU0	CPU1
User CPU time	0	5.9
System CPU time	0	5.9
User nice CPU time	0	0
Idle CPU time	100	88.2
IO wait CPU time	0	0
Hardware IRQ	0	0
Software IRQ	0	0
Steal time	0	0

Рисунок 49 – Загрузка по ядрам

Значения представлены в процентах времени, распределенные по следующим категориям:

- User CPU time - процент времени, в течение которого процессор выполнял пользовательские процессы, то есть программы, запущенные от имени пользователя;
- System CPU time - процент времени, в течение которого процессор обрабатывал системные процессы;
- User nice CPU time - процент времени, в течение которого процессор обрабатывал пользовательские процессы с пониженным приоритетом (приоритет "nice");
- Idle CPU time - процент времени, в течение которого процессор находился в состоянии простоя и не выполнял никаких задач;

- IO wait CPU time - процент времени, в течение которого процессор ожидал завершения операций ввода/вывода;
- Hardware IRQ - процент времени, в течение которого процессор обрабатывал аппаратные прерывания;
- Software IRQ - процент времени, в течение которого процессор обрабатывал программные прерывания;
- Steal time - процент времени, в течение которого процессор ожидал выделения ресурсов от гипервизора.

4.2 Оперативная память

В части информационной панели "Оперативная память" отображается информация об общем объёме в мегабайтах и объёме свободной памяти в мегабайтах. Также представлена визуальная индикация уровня загрузки (рисунок 50).

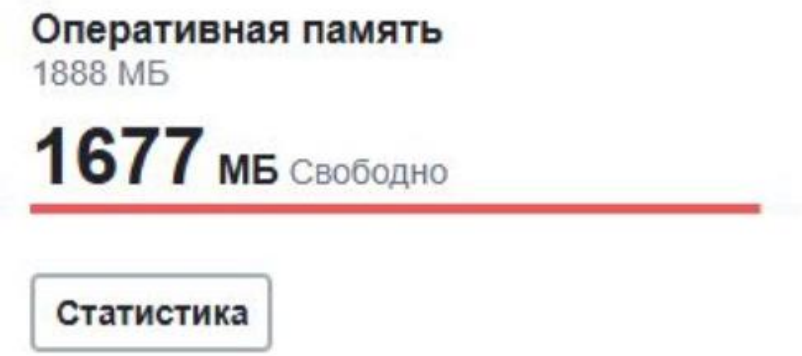


Рисунок 50 – Блок "Оперативная память"

Нажав на клавишу "Статистика" отображается таблица использования оперативной памяти с перечислением параметров и значений в МБ (рисунок 51).

Рисунок 51 – Статистика оперативной памяти

4.3 Диски

В части информационной панели "Диски" отображается информация об общем объёме в гигабайтах и свободном объёме в гигабайтах (рисунок 52).

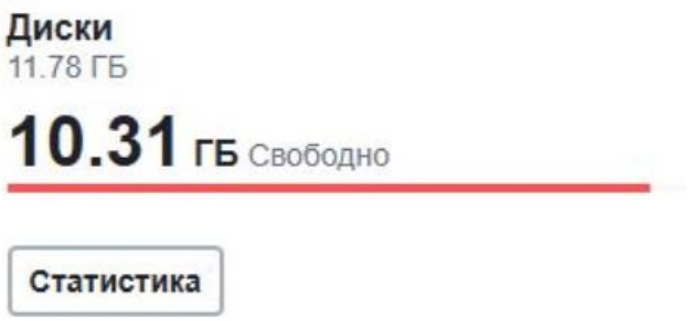


Рисунок 52 – Блок "Диски"

Нажав на клавишу "Статистика" отображается окно "Подключенные диски" с таблицей, где указаны файловые системы с их объёмами в ГБ и процентом заполнения (рисунок 53).

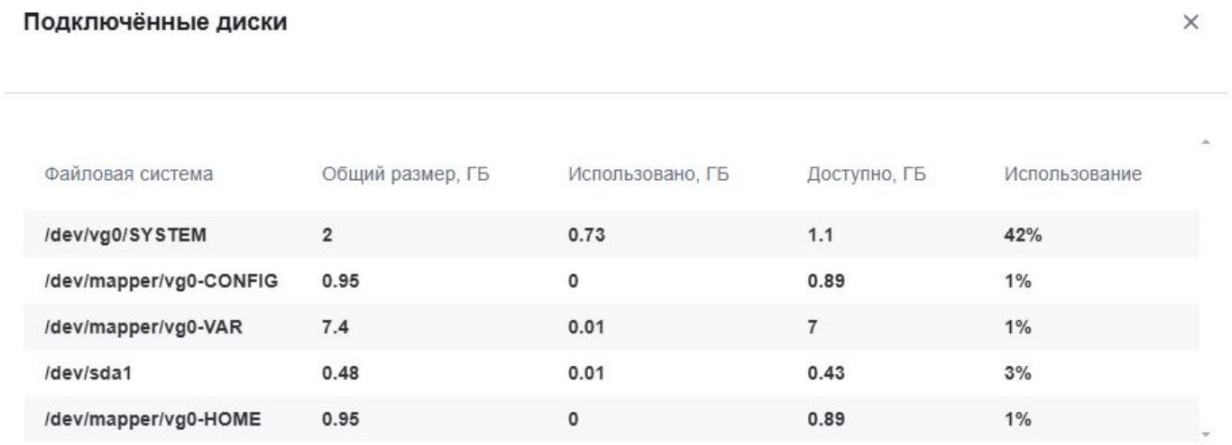


Рисунок 53 – Статистика дискового пространства

4.4 Сетевые адреса

В части информационной панели "Сетевые адреса" отображается информация об интерфейсах, MAC-адресах и IP-адресах (рисунок 54).

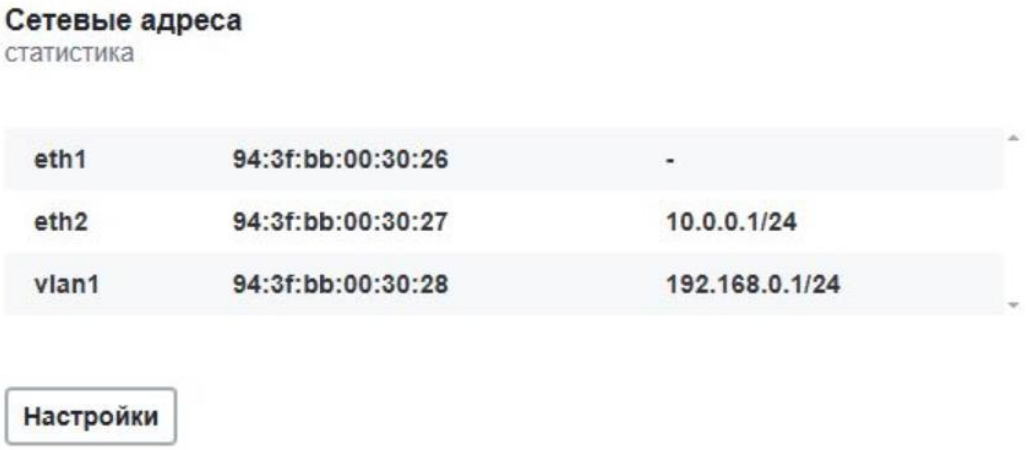


Рисунок 54 – Блок "Сетевые адреса"

Нажав на клавишу "Настройка" отображается окно конфигурации интерфейсов. Более детальную информацию о доступных действиях можно найти в разделе Настройка интерфейсов.

4.5 IP- адреса, выданные DHCP-сервером

В части информационной панели "IP-адреса" отображается информация о пулах и диапазонах IP-адресов (рисунок 55).

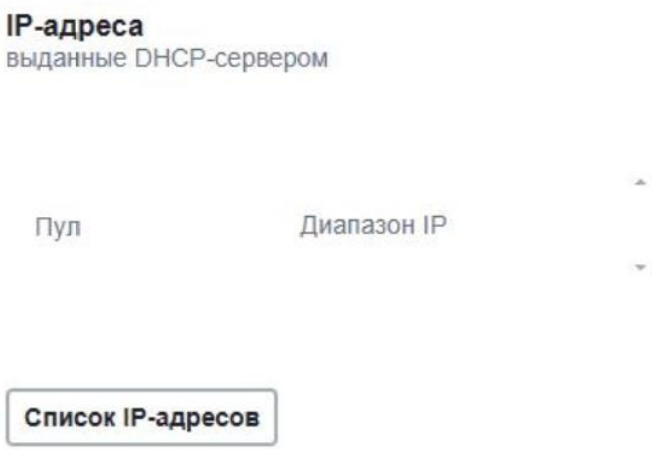


Рисунок 55 – Блок "IP-адреса"

Нажав на клавишу "Список IP-адресов" отображается окно со списком активных адресов (рисунок 56).

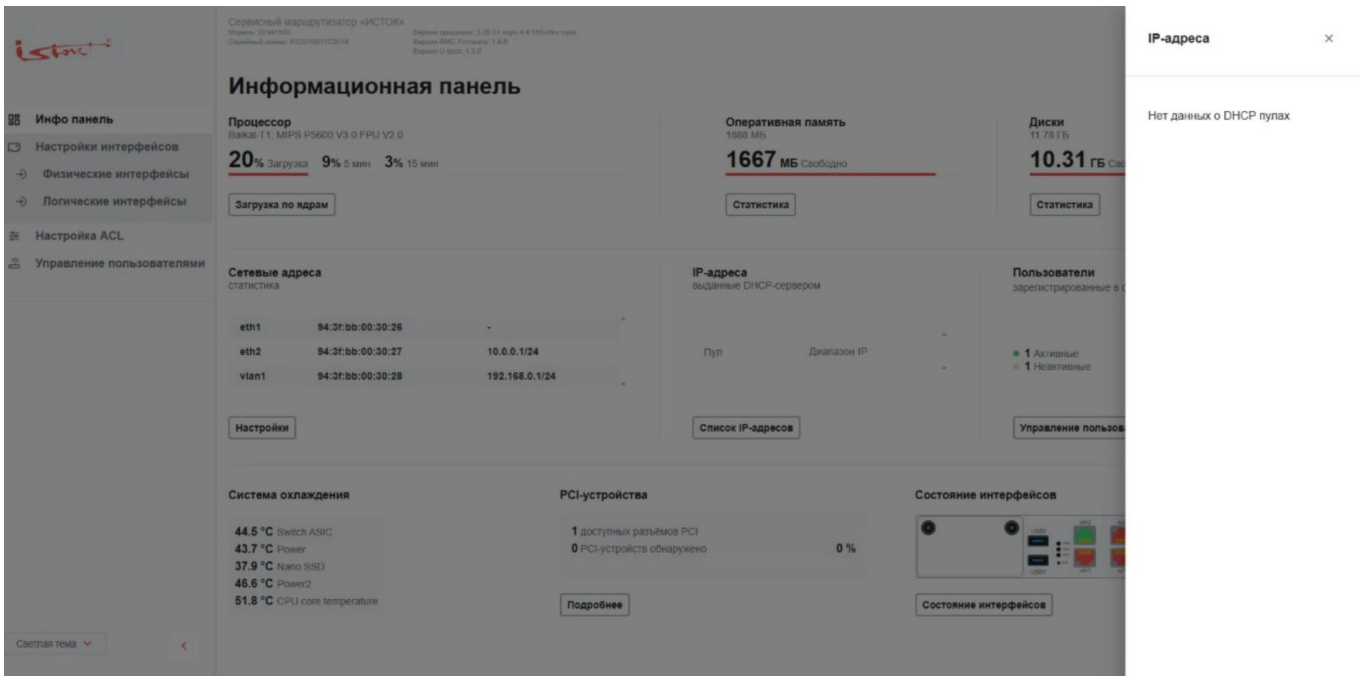


Рисунок 56 – Список IP-адресов

4.6 Пользователи

В части информационной панели "Пользователи" отображается информация о количестве зарегистрированных и активных сессий (рисунок 57).

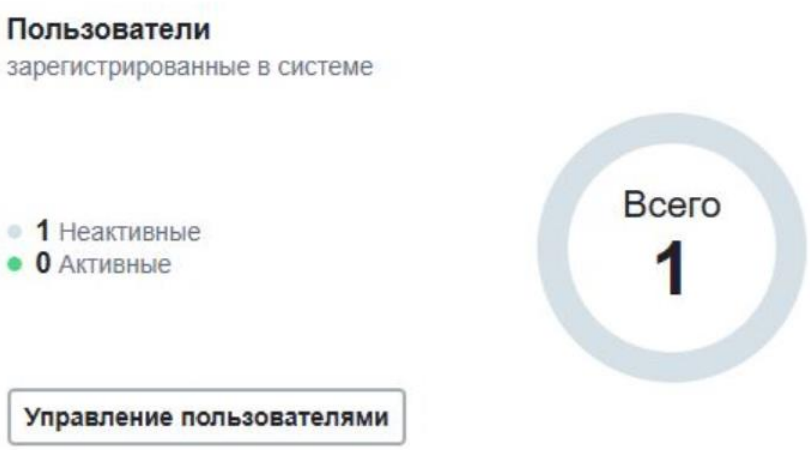


Рисунок 57 – Блок "Пользователи"

Нажав на клавишу "Управление пользователями" отображается окно, которое позволяет создавать, удалять, редактировать, настраивать тип пользователей и групп. Более детальную информацию о доступных действиях можно найти в разделе Управление пользователями.

4.7 Система охлаждения

В части информационной панели "Система охлаждения" отображается перечень сенсоров и текущие температуры (°C) (рисунок 58).

Рисунок 58 – Блок "Система охлаждения"

4.8 PCI- устройства

В части информационной панели "PCI-устройства" отображается информация о количестве доступных слотов, обнаруженных устройствах, визуальная индикация уровня использования ресурсов, а также процентное соотношение использования (рисунок 59).

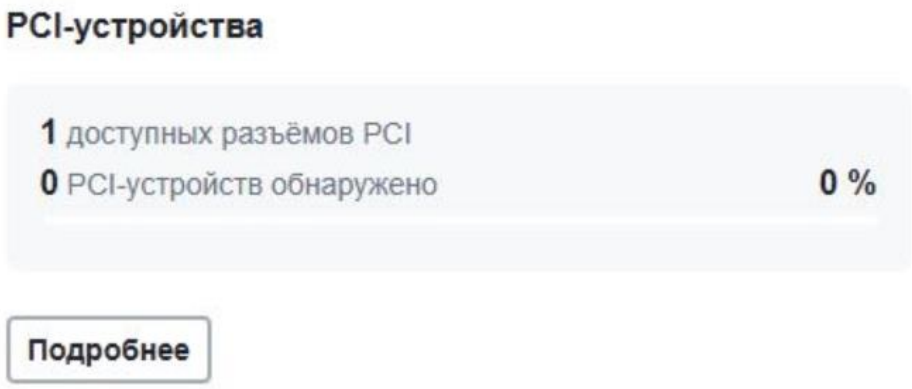


Рисунок 59 – Блок "PCI-устройства"

Нажав на клавишу "Подробнее" отображается окно со списком активных PCI-устройств (рисунок 60).

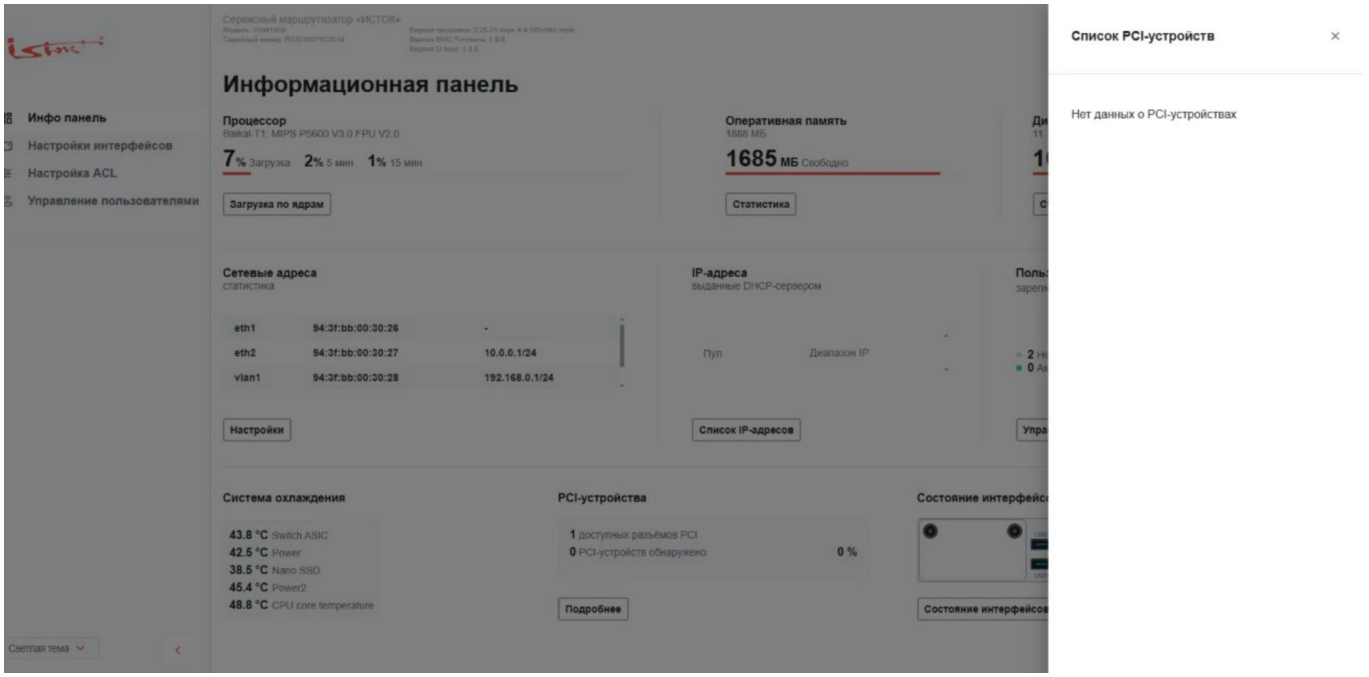


Рисунок 60 – PCI-устройства

4.9 Состояние интерфейсов

В части информационной панели "Состояние интерфейсов" отображается схема устройства с отображением портов и цветовой индикацией состояния каждого порта: зеленый (link), красный (down), оранжевый (errors) (рисунок 61).

Рисунок 61 – Блок "Состояние интерфейсов"

Нажав на клавишу "Состояние интерфейсов" отображается окно для более подробной информации и настройки интерфейсов (См. раздел Настройка интерфейсов).

5 Настройка интерфейсов

На вкладке "Настройки интерфейсов" отображается таблица с текущими настройками интерфейсов (рисунок 62).

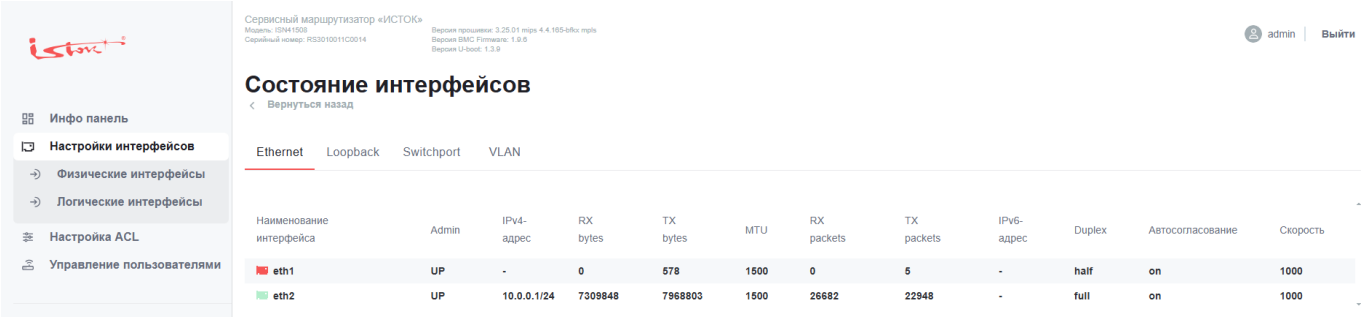


Рисунок 62 – Информация о состоянии интерфейсов

Переключая вкладки можно просматривать все физические и логические интерфейсы (рисунок 63).

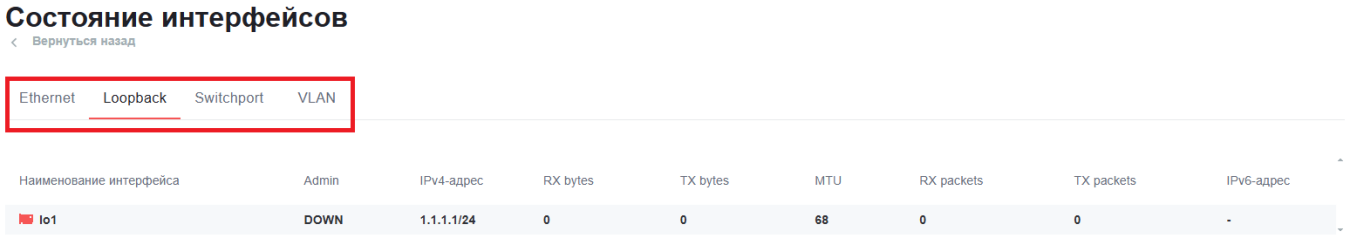


Рисунок 63 – Вкладки с просмотром настроек

5.1 Настройка Ethernet интерфейса

Выберите пункт "Физические интерфейсы" из выпадающей вкладки "Настройки интерфейсов" в левом меню (рисунок 64).

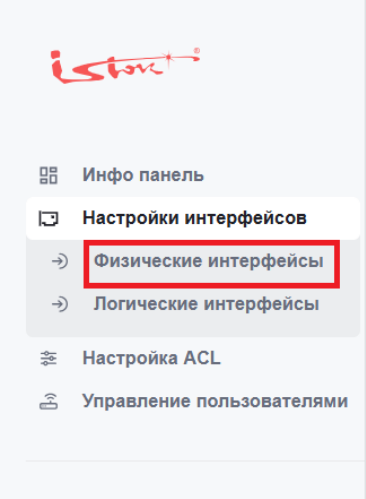


Рисунок 64 – Выбор пункта "Физические интерфейсы"

Переключитесь на вкладку "Ethernet" для отображения соответствующей таблицы интерфейсов (рисунок 65).

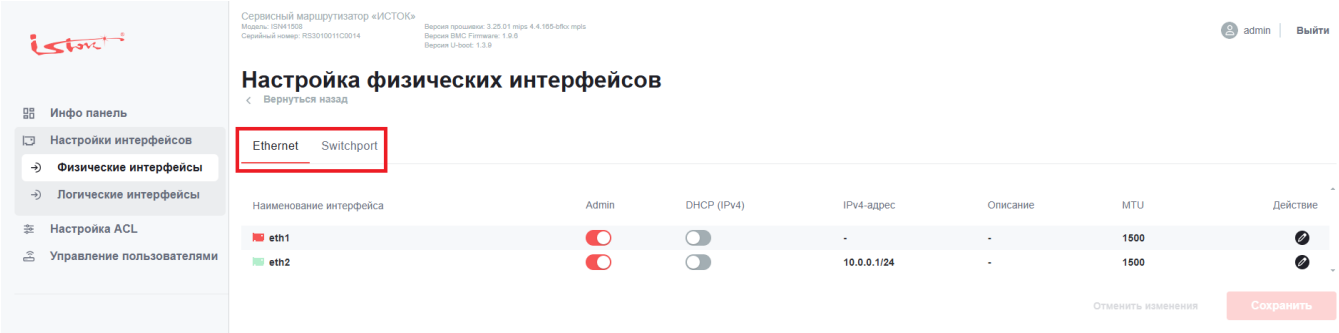


Рисунок 65 – Выбор типа физического интерфейса

В столбце "Наименование интерфейса" указаны наименования интерфейсов (рисунок 66).

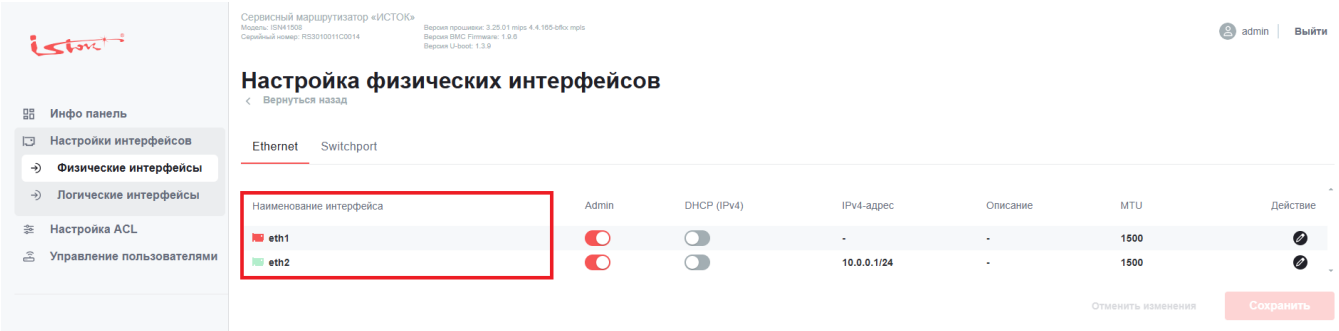


Рисунок 66 – Наименование интерфейсов

В столбце "Действие" нажмите на пиктограмму "Изменить" чтобы начать корректировку Ethernet интерфейса (рисунок 67).

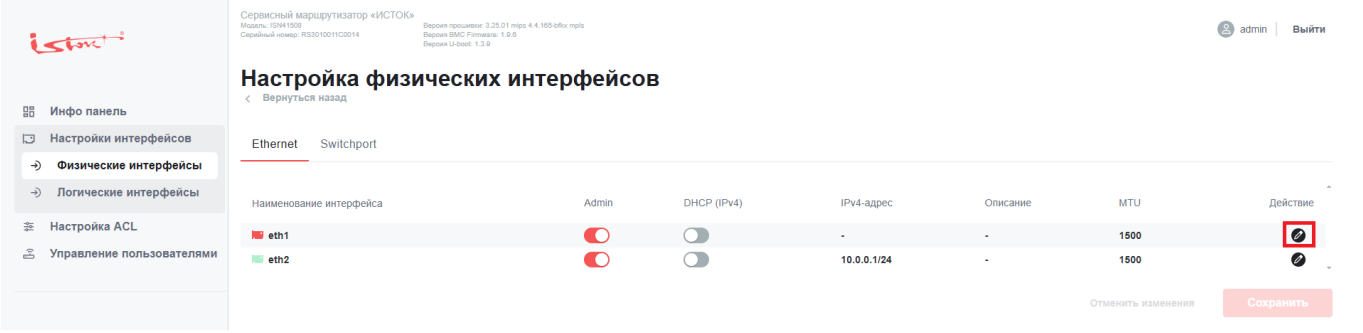


Рисунок 67 – Ethernet интерфейс пиктограмма изменить

Используйте кнопку-переключатель в столбце "Admin" для изменения административного статуса интерфейса (Administrative status: UP/DOWN) (рисунок 68).

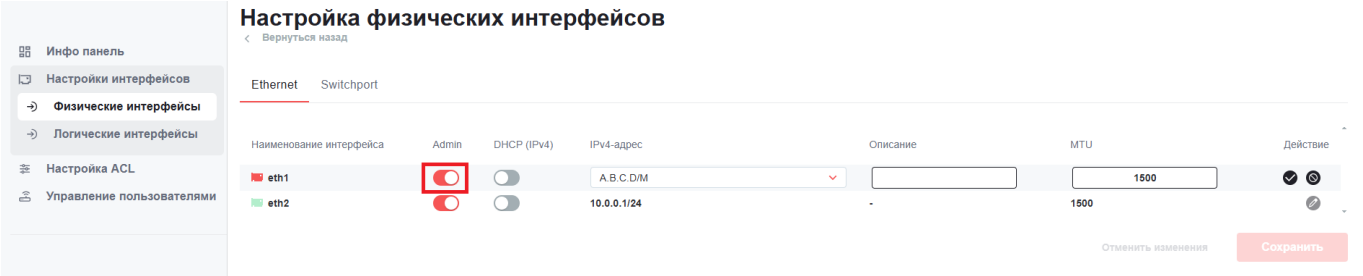


Рисунок 68 – Изменение административного статуса интерфейса

Используйте кнопку-переключатель в столбце "DHCP (IPv4)" для перехода интерфейса в режим DHCP-клиента (DHCP client: ON/OFF) (рисунок 69).

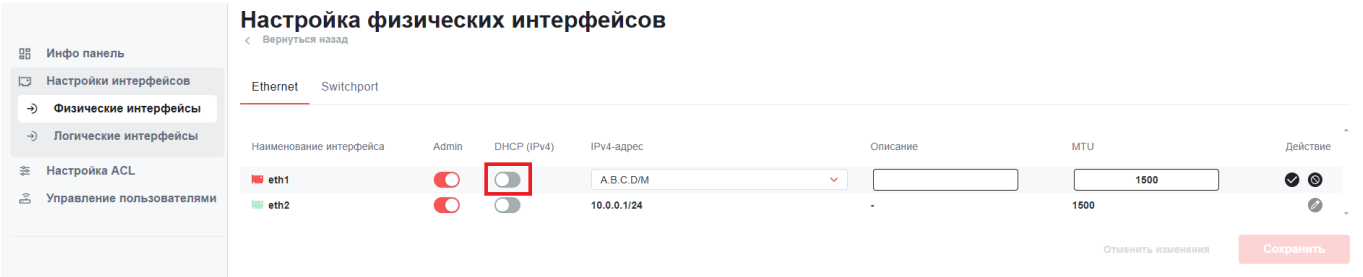


Рисунок 69 – Настройка DHCP клиента

Введите IP-адрес и маску в поле столбца "IPv4-адрес", затем нажмите на поле "Добавить" или клавишу "Enter" для добавления IP-адреса (рисунок 70).

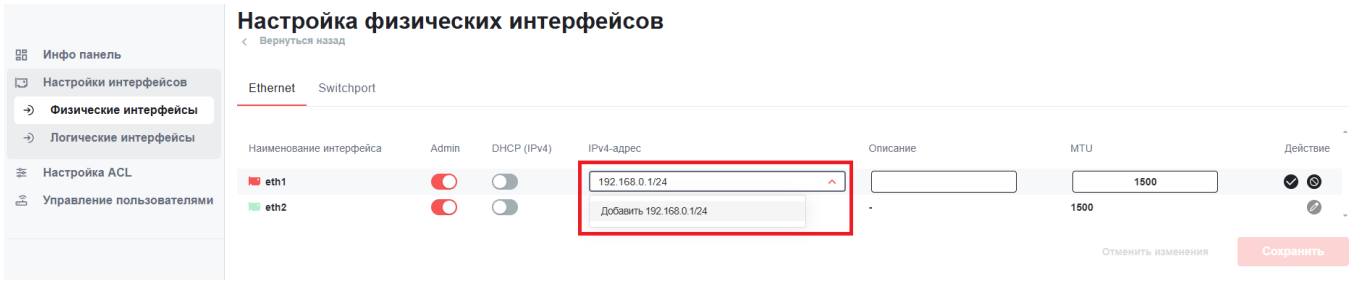


Рисунок 70 – Добавление IP-адреса

Сервисный маршрутизатор позволяет назначать несколько IP-адресов одному интерфейсу. Для просмотра всех назначенных IP-адресов на интерфейсе нажмите на пиктограмму, расположенную в правой части поля ввода IP-адрес (рисунок 71).

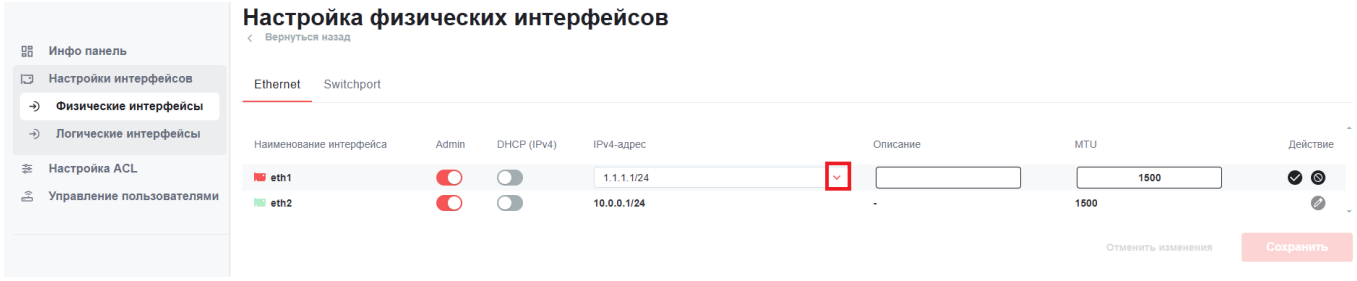


Рисунок 71 – Просмотр IP-адресов на интерфейсе

Для удаления ненужных IP-адресов нажмите по ним левой клавишей мыши или удалить все адреса (рисунок 72).

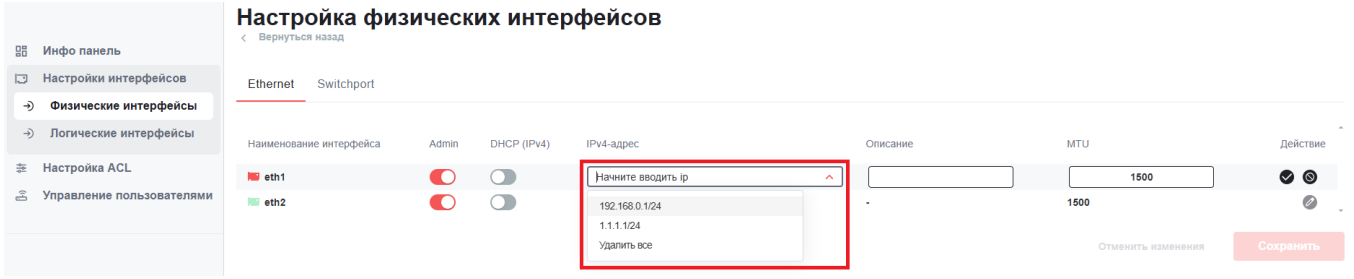


Рисунок 72 – Удаление IP-адресов

В столбце "Описание" есть возможность добавить краткое описание интерфейса (рисунок 73).

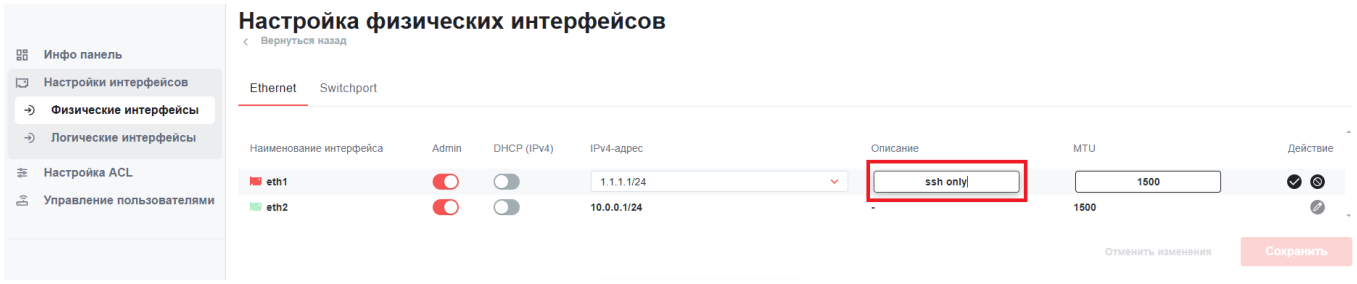


Рисунок 73 – Добавление описания интерфейсу

В столбце MTU укажите максимальный размер блока данных (в байтах, от 68 до 65535) (рисунок 74).

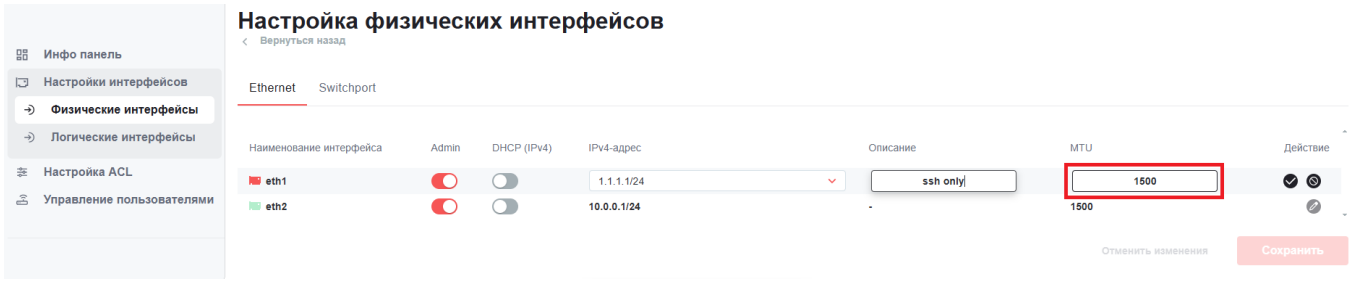


Рисунок 74 – Настройка MTU

Для сохранения настроек необходимо сначала подтвердить изменения, нажав соответствующую пиктограмму в столбце "Действие" (рисунок 75).

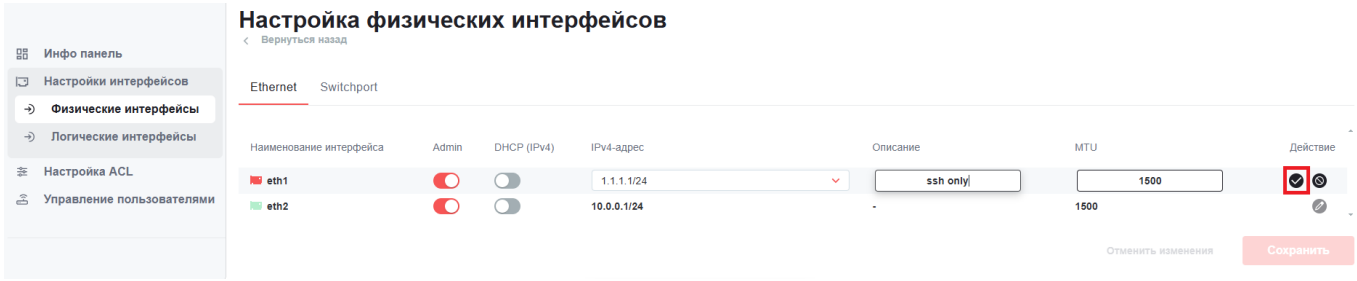


Рисунок 75 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 76).

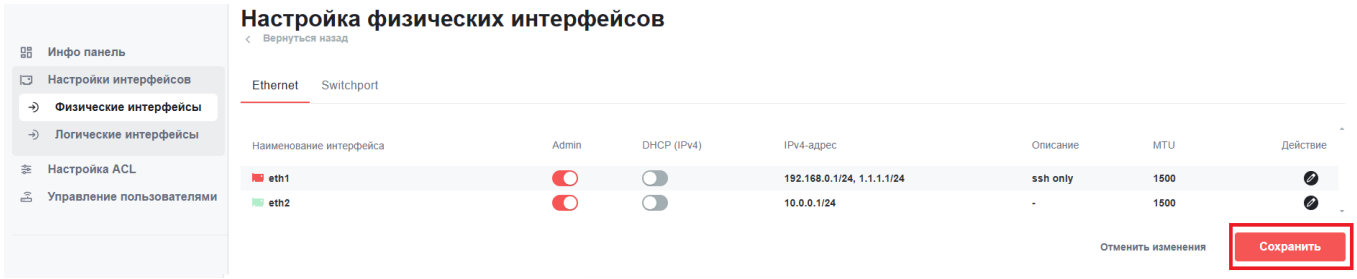


Рисунок 76 – Сохранение настроек

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 77).

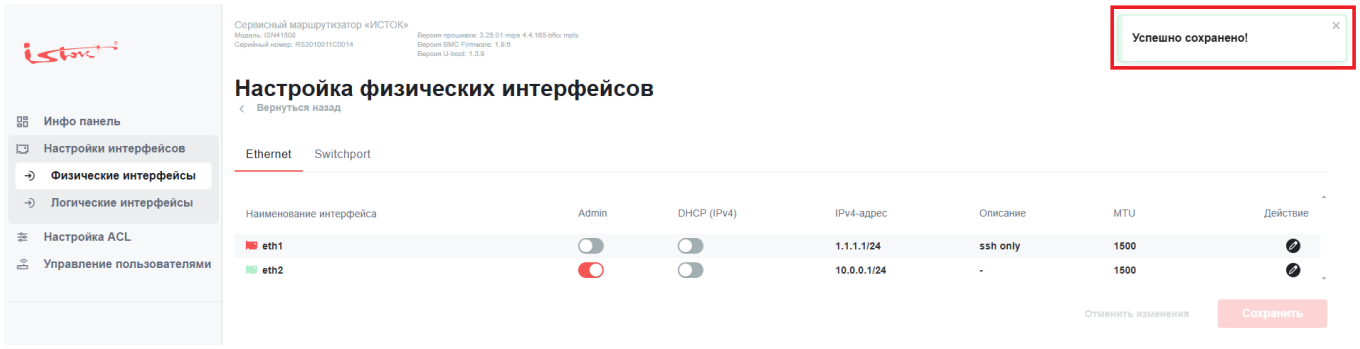


Рисунок 77 – Подтверждение сохранения

5.2 Настройка Switchport интерфейса

Выберите пункт "Физические интерфейсы" из выпадающей вкладки "Настройки интерфейсов" в левом меню (рисунок 78).

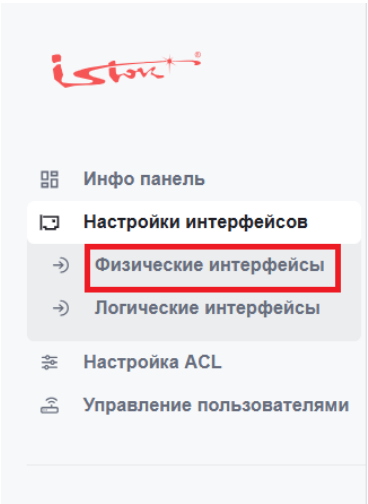


Рисунок 78 – Выбор пункта "Физические интерфейсы"

Переключитесь на вкладку "Switchport" для отображения соответствующей таблицы интерфейсов (рисунок 79).

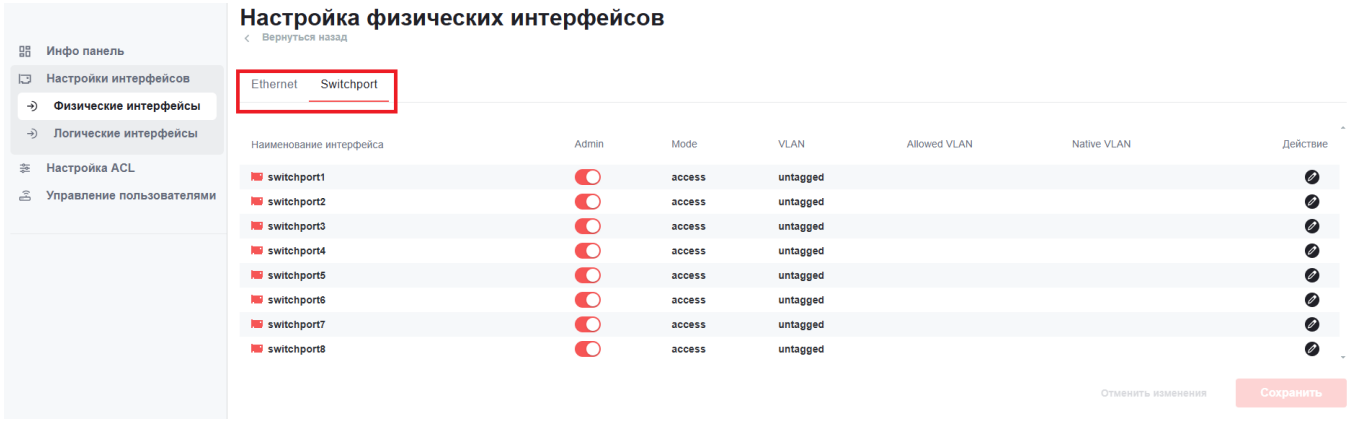


Рисунок 79 – Выбор типа физического интерфейса

В столбце "Наименование интерфейса" указаны наименования интерфейсов (рисунок 80).

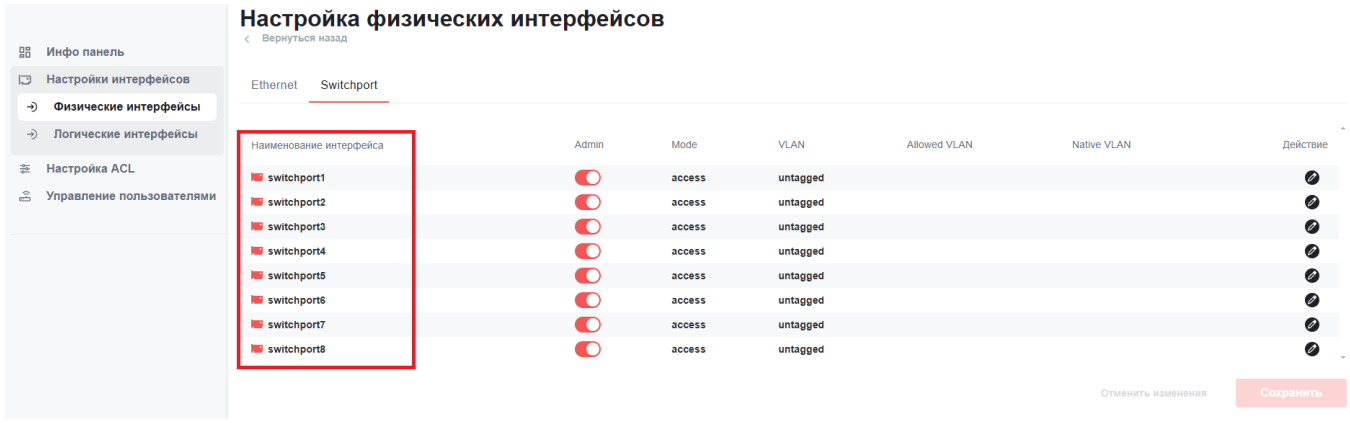


Рисунок 80 – Наименование интерфейсов

В столбце "Действие" нажмите на пиктограмму "Изменить", чтобы начать корректировку Ethernet-интерфейса (рисунок 81).

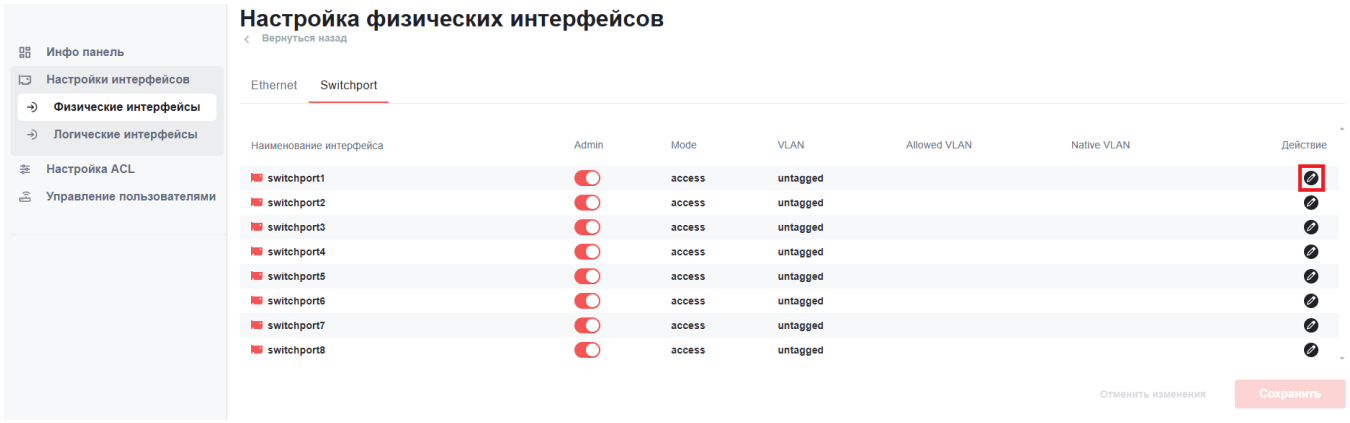


Рисунок 81 – Switchport интерфейс пиктограмма изменить

Используйте кнопку-переключатель в столбце "Admin" для изменения административного статуса интерфейса (Administrative status: UP/DOWN) (рисунок 82).

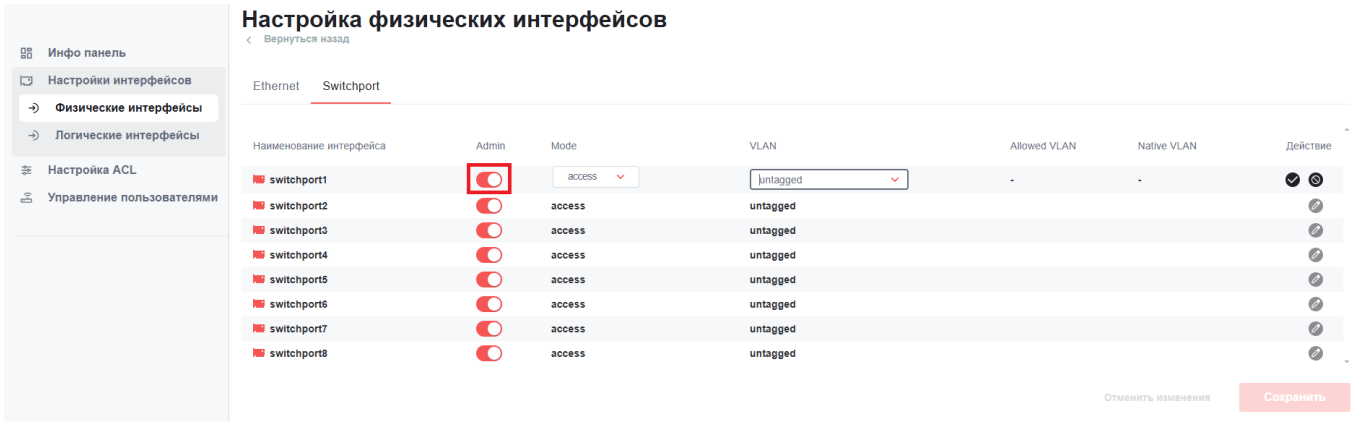


Рисунок 82 – Изменение административного статуса интерфейса

Используйте выпадающий список в столбце "Mode" для выбора режима работы VLAN (рисунок 83).

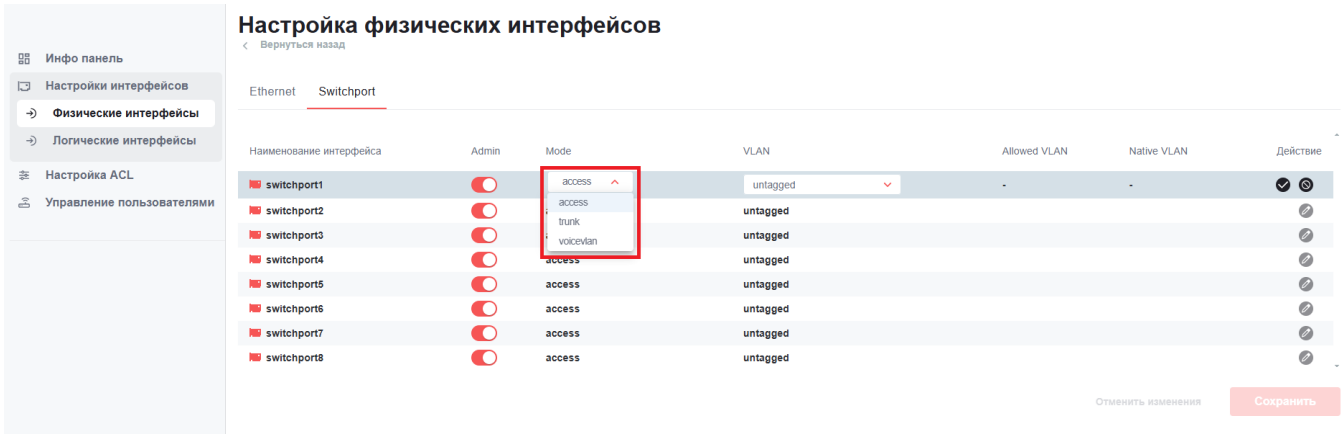


Рисунок 83 – Настройка работы VLAN

В столбце "VLAN" укажите номер VLAN интерфейса который будет назначен switchport'y, нажмите на поле "Добавить" или клавишу "Enter" (untagged - это vlan1, VLAN интерфейс по умолчанию). Данный параметр настраивается только при access mod (рисунок 84).

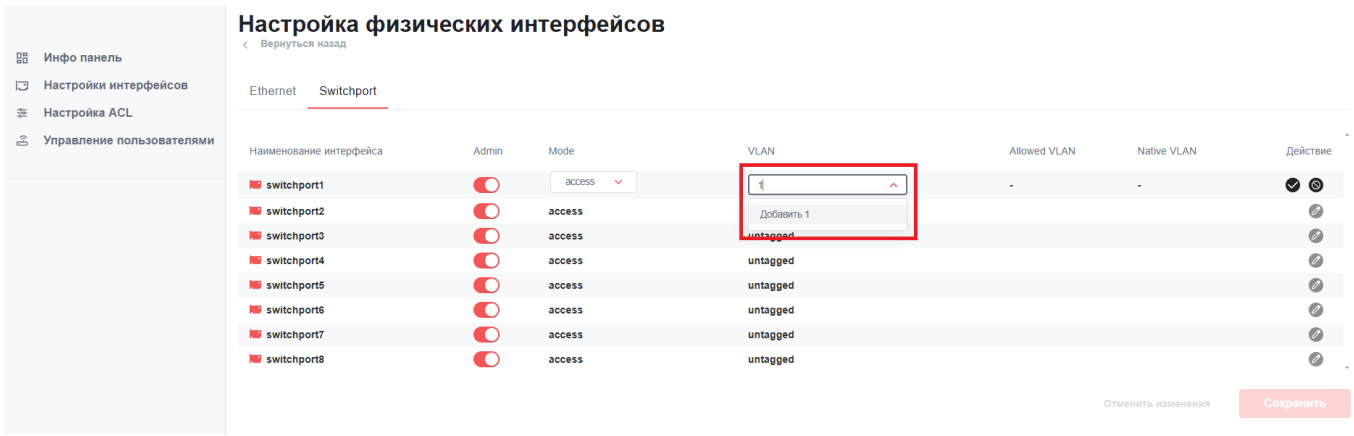


Рисунок 84 – Назначение VLAN интерфейса

В столбце "Allowed VLAN" выберите VLAN, которые будут проходить через данный канал, укажите один из следующих параметров all, none или VLAN ID, где VLAN ID - id-номер VLAN, затем нажмите на поле "Добавить" или клавишу "Enter". Данный параметр настраивается только при trunk mod и voicevlan (рисунок 85).

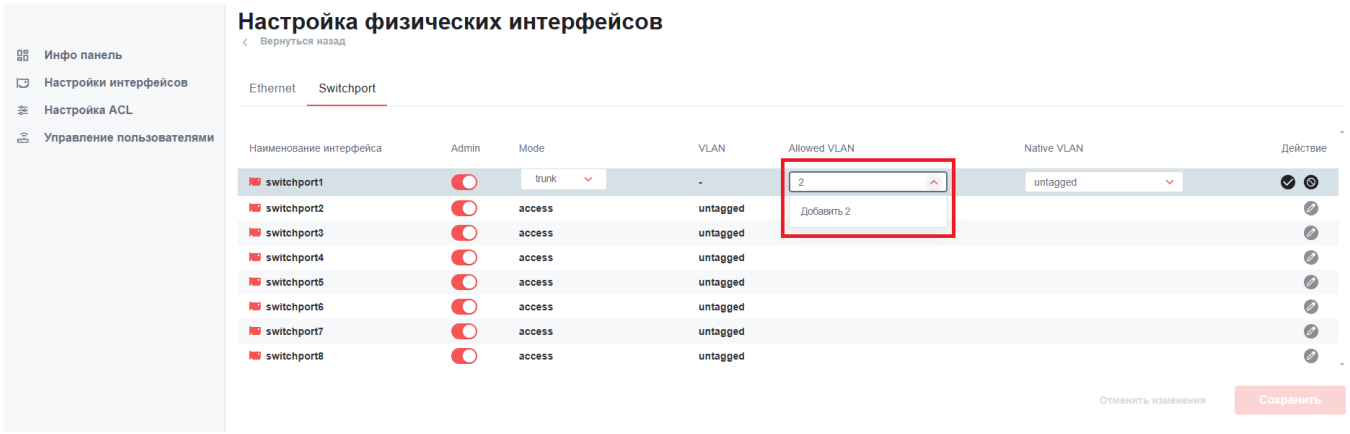


Рисунок 85 – Настройка транкового порта

В столбце "Native VLAN" укажите к какой сети относить кадры приходящие без тега, затем нажмите на поле "Добавить" или клавишу "Enter" (untagged - это vlan1, VLAN интерфейс по умолчанию) (рисунок 86).

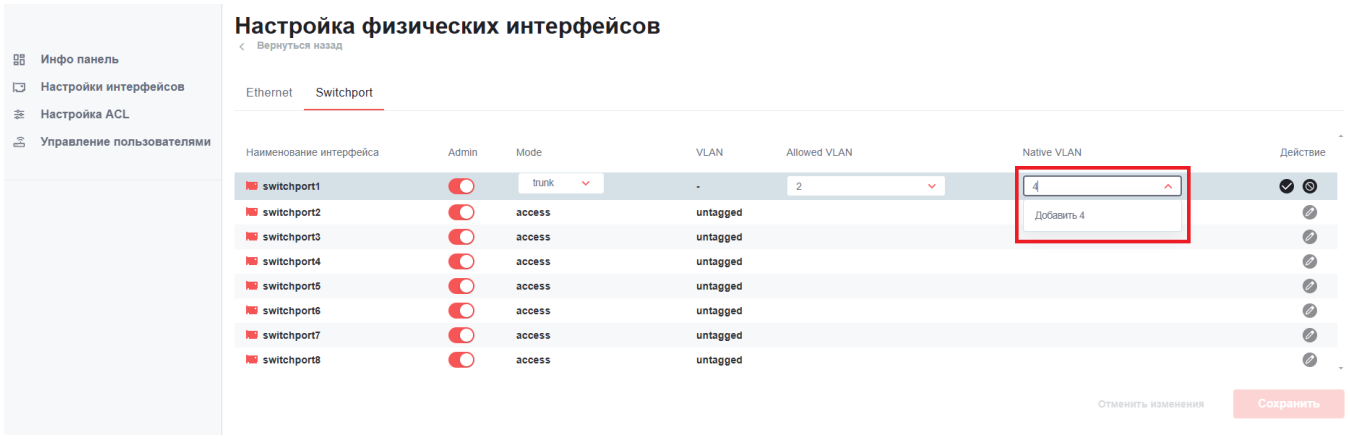


Рисунок 86 – Настройка Native VLAN

Для сохранения настроек необходимо сначала подтвердить изменения, нажав соответствующую пиктограмму в столбце "Действие" (рисунок 87).

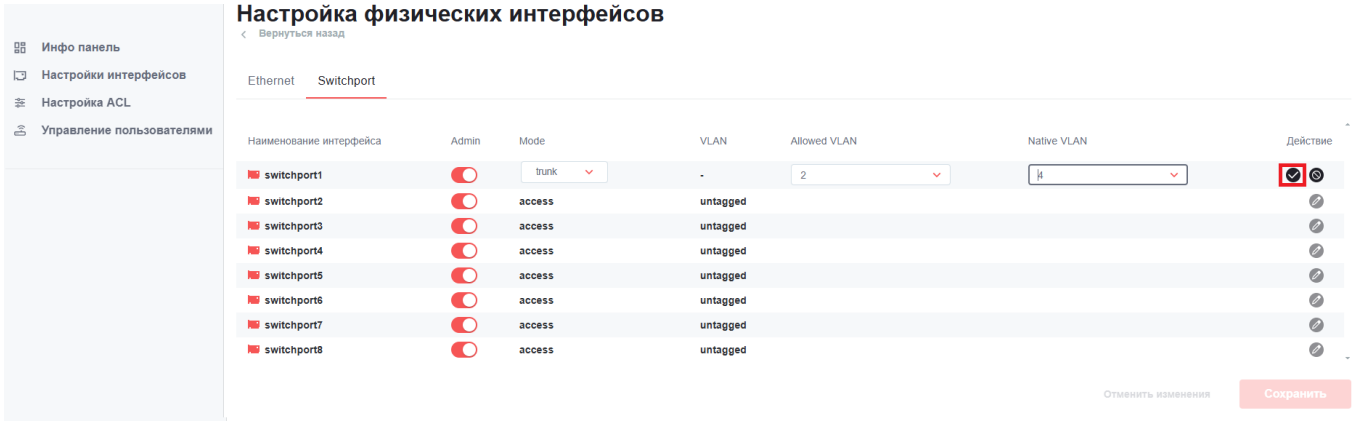


Рисунок 87 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 88).

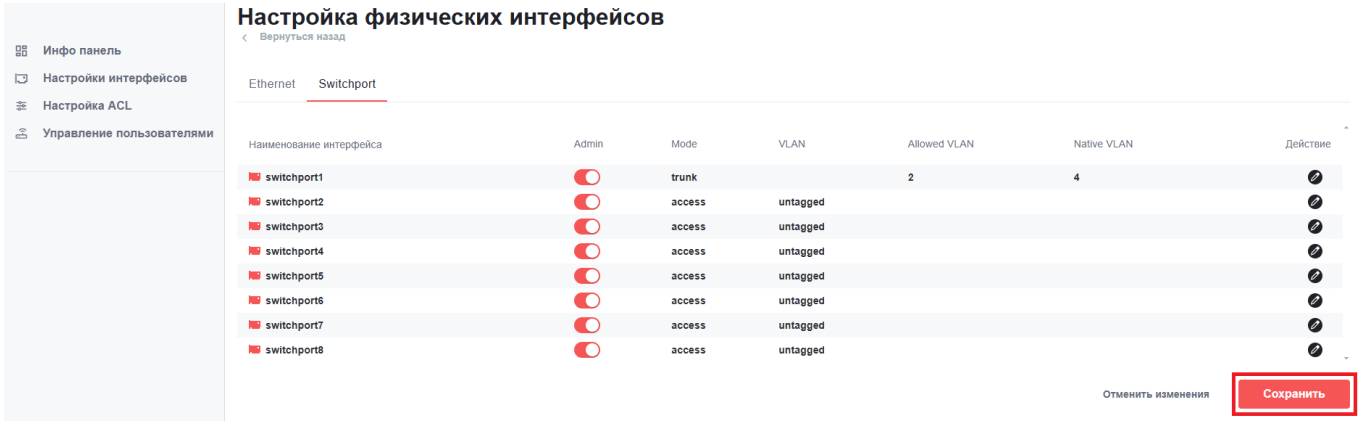


Рисунок 88 – Сохранение настроек

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 89).

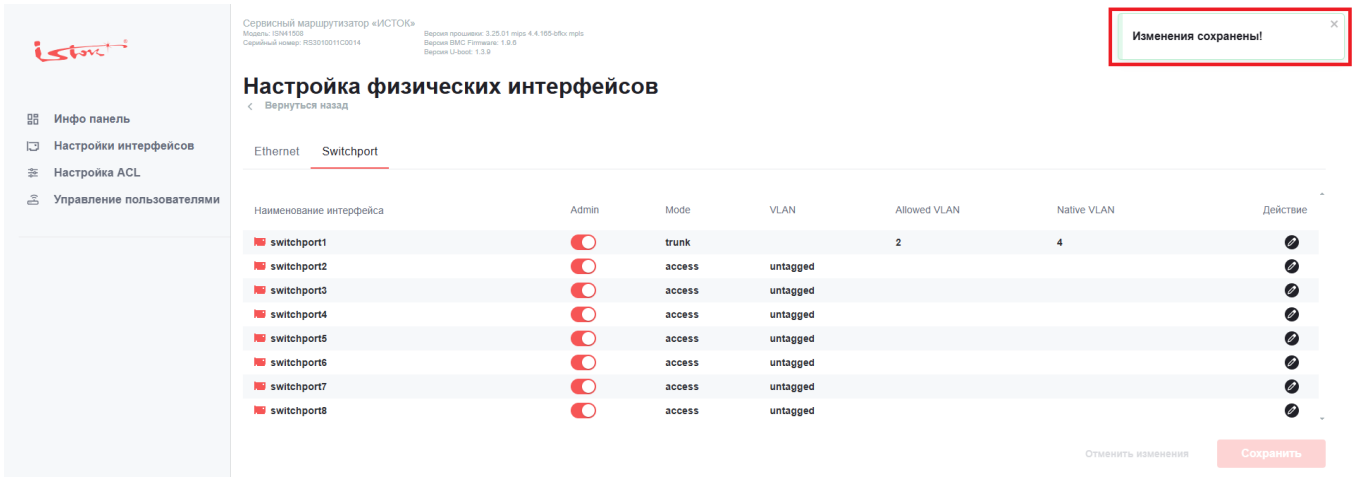


Рисунок 89 – Подтверждение сохранения

5.3 Настройка логических интерфейсов

Выберите пункт "Логические интерфейсы" из выпадающей вкладки "Настройки интерфейсов" в левом меню (рисунок 90).

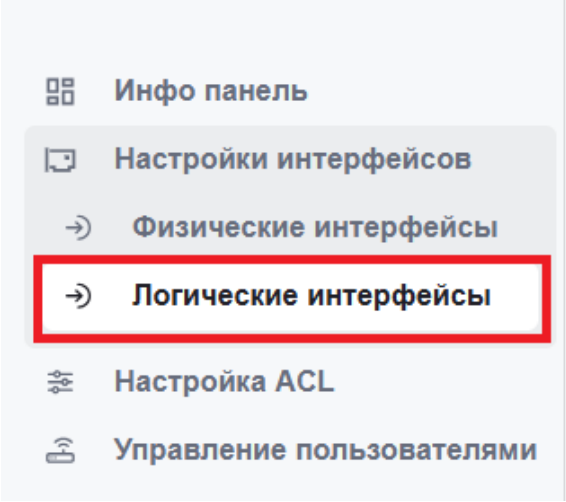


Рисунок 90 – Выбор пункта "Физические интерфейсы"

В столбце "Наименование интерфейса" представлены наименования интерфейсов созданных на сервисном маршрутизаторе (рисунок 91).

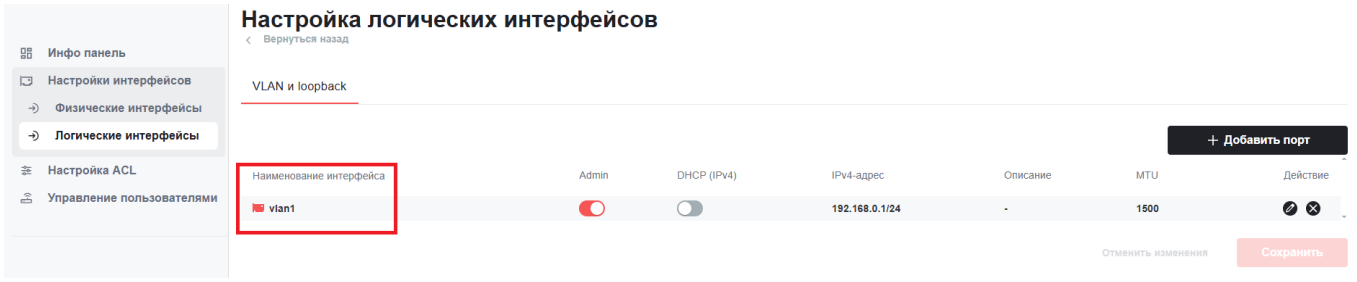


Рисунок 91 – Наименование интерфейсов

Для создания нового интерфейса нажмите кнопку "+Добавить порт" (рисунок 92) или отредактируйте текущий, нажав на пиктограмму "Изменить" в столбце "Действие" (рисунок 93).

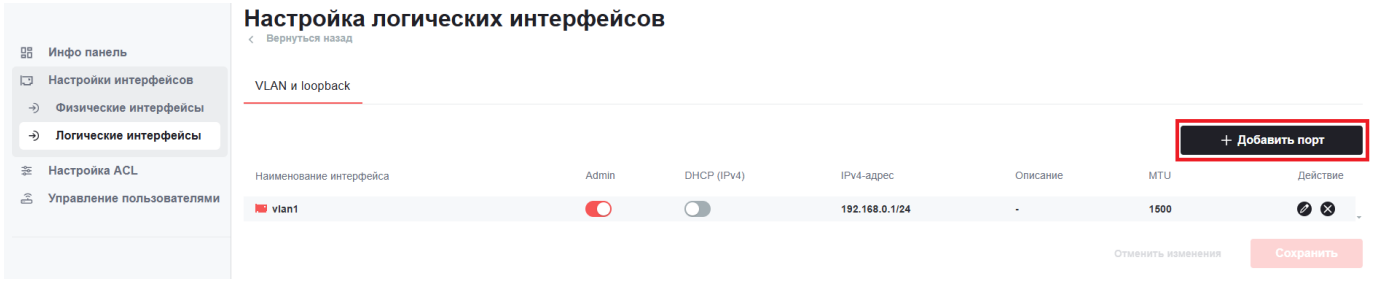


Рисунок 92 – Наименование интерфейсов

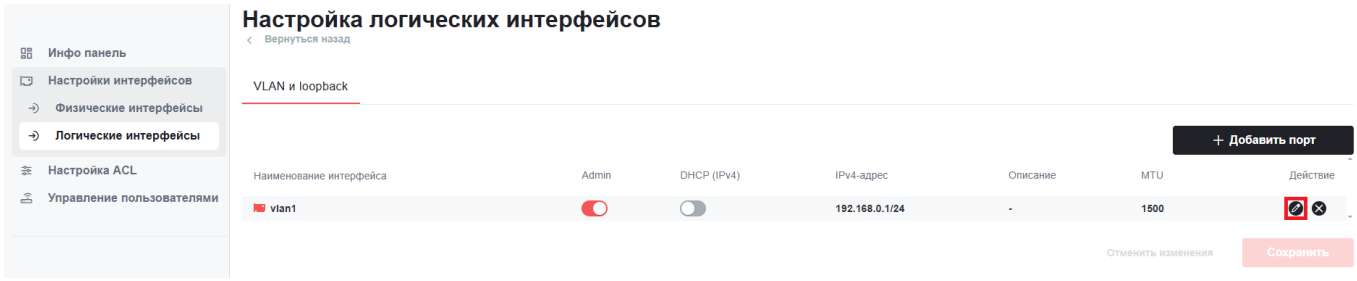


Рисунок 93 – Логический интерфейс пиктограмма изменить

Введите название нового интерфейса в формате <TYPE><ID>, где <TYPE> - тип интерфейса vlan - VLAN интерфейс, lo - loopback интерфейс; <ID> - идентификационный номер интерфейса (рисунок 94).

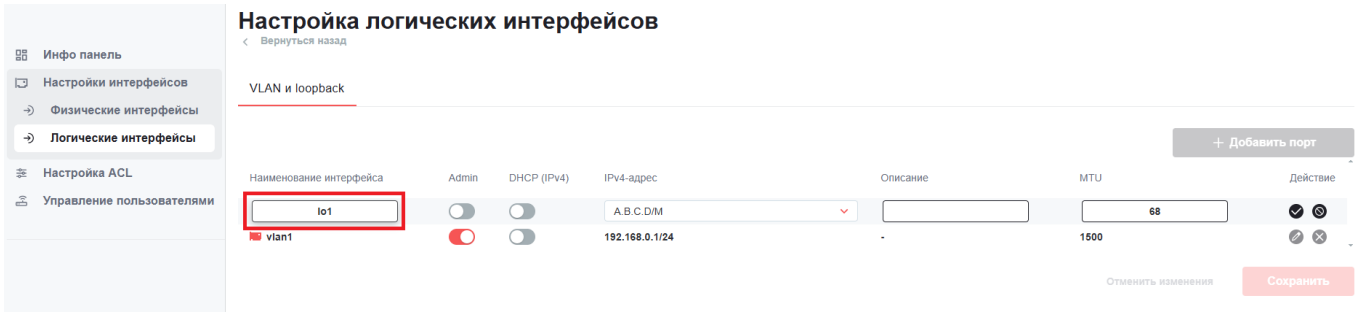


Рисунок 94 – Заполнение наименования интерфейса

Используйте кнопку-переключатель в столбце "Admin" для изменения административного статуса интерфейса (Administrative status: UP/DOWN) (рисунок 95).

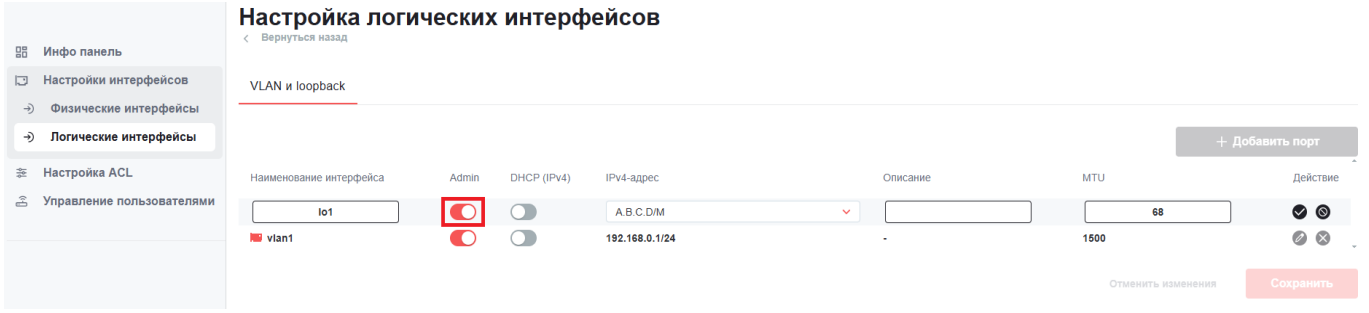


Рисунок 95 – Изменение административного статуса интерфейса

Используйте кнопку-переключатель в столбце "DHCP (IPv4)" для перехода интерфейса в режим DHCP-клиента (DHCP client: ON/OFF) (рисунок 96).

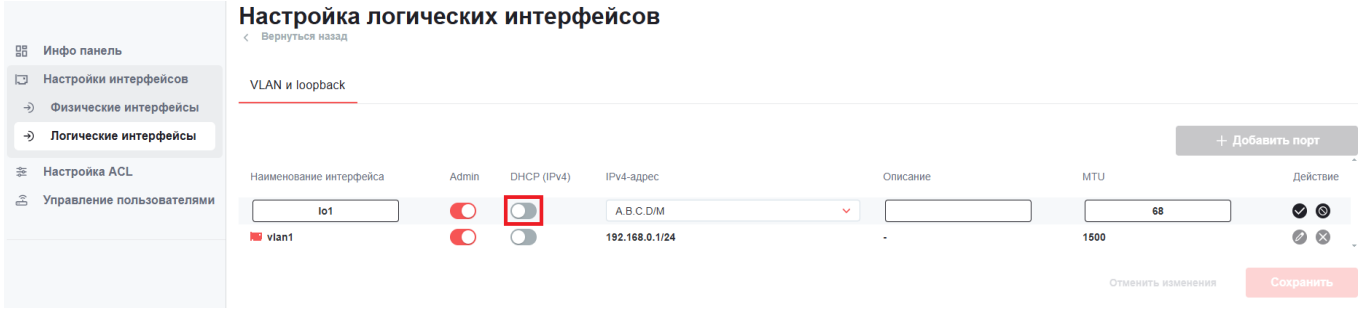


Рисунок 96 – Настройка DHCP клиента

Введите IP-адрес и маску в поле столбца "IPv4-адрес", затем нажмите на поле "Добавить" или клавишу "Enter" для добавления IP-адреса (рисунок 97).

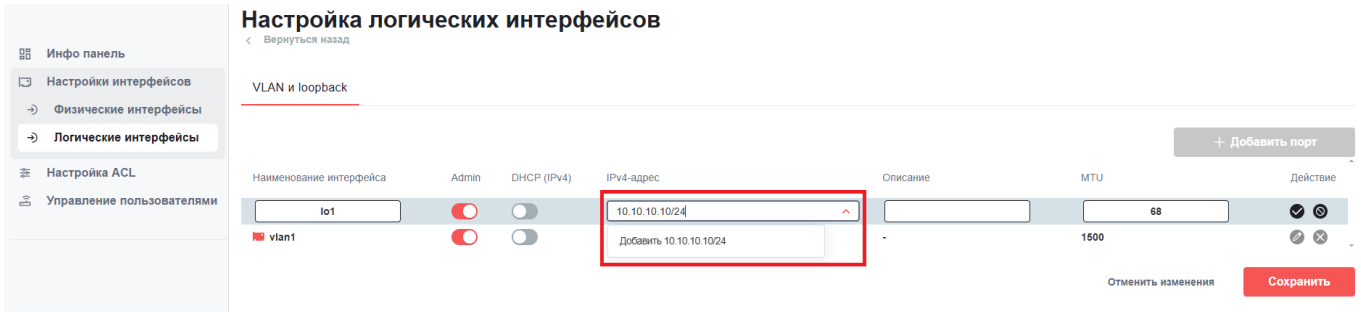


Рисунок 97 – Добавление IP-адреса

Сервисный маршрутизатор позволяет назначать несколько IP-адресов одному интерфейсу. Для просмотра всех назначенных IP-адресов на интерфейсе нажмите на пиктограмму, расположенную в правой части поля ввода IP-адрес (рисунок 98).

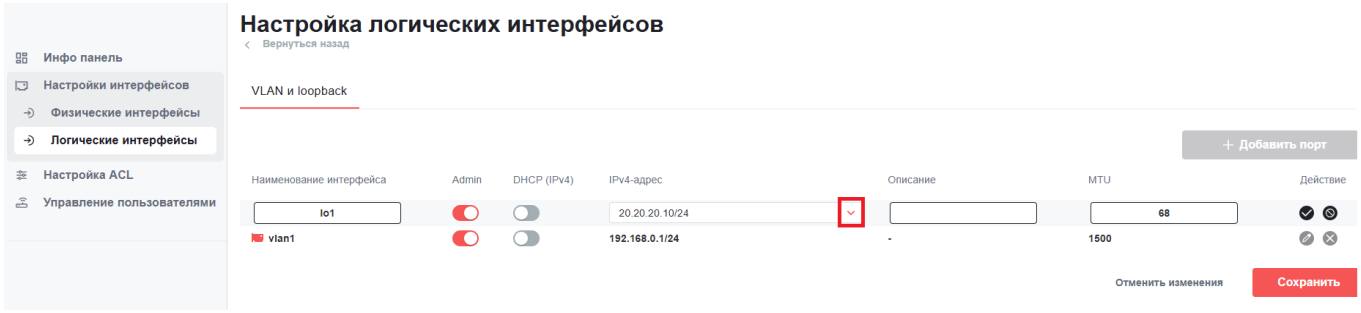


Рисунок 98 – Просмотр IP-адресов на интерфейсе

Для удаления ненужных IP-адресов нажмите по ним левой клавишей мыши или удалить все адреса (рисунок 99).

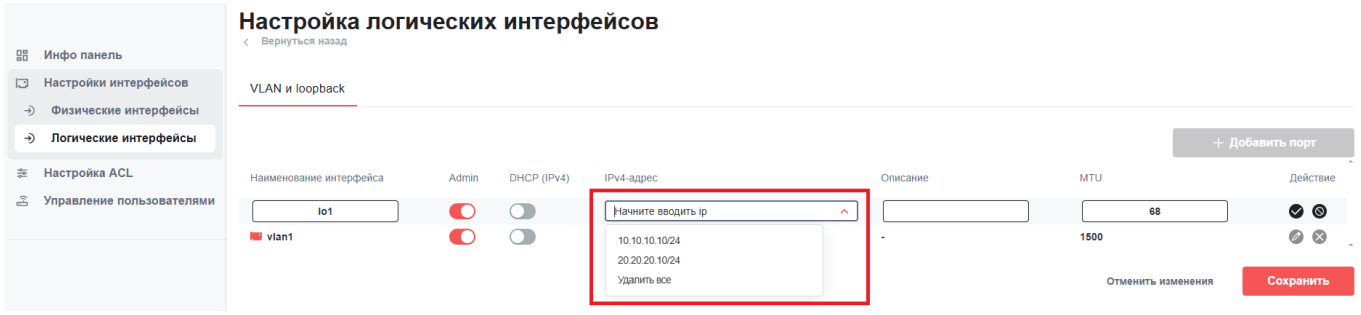


Рисунок 99 – Удаление IP-адресов

В столбце "Описание" есть возможность добавить краткое описание интерфейса (рисунок 100).

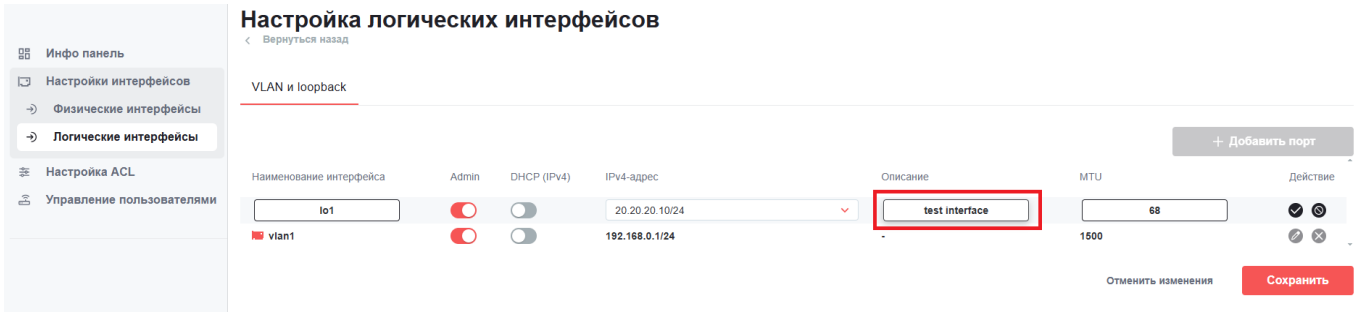


Рисунок 100 – Добавление описания интерфейсу

В столбце MTU укажите максимальный размер блока данных (в байтах, от 68 до 65535) (рисунок 101).

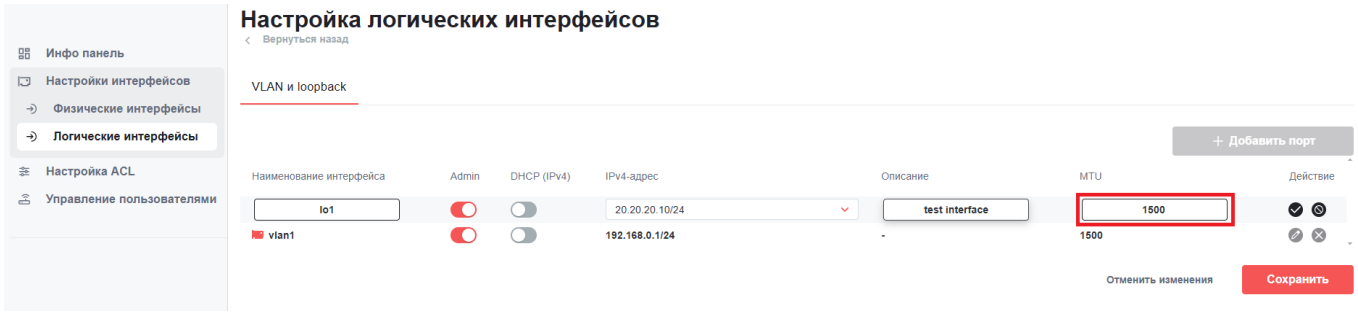


Рисунок 101 – Настройка MTU

Для сохранения настроек необходимо сначала подтвердить изменения, нажав соответствующую пиктограмму в столбце "Действие" (рисунок 102).

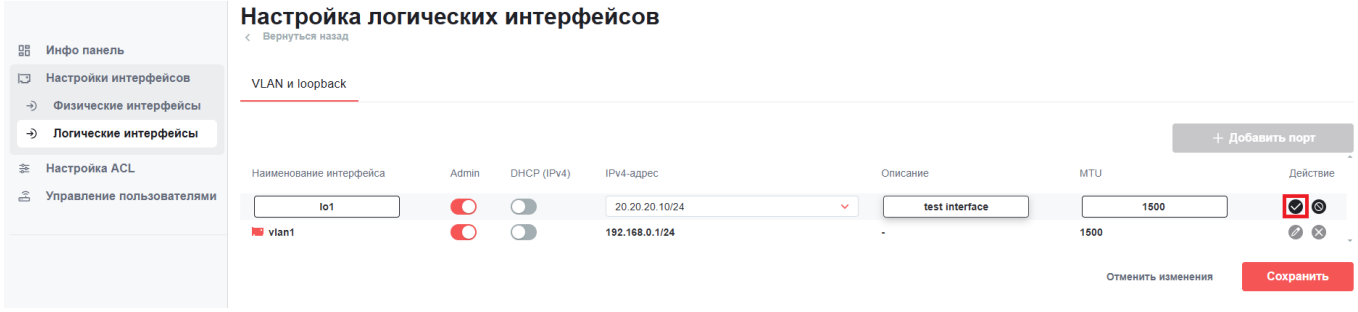


Рисунок 102 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 103).

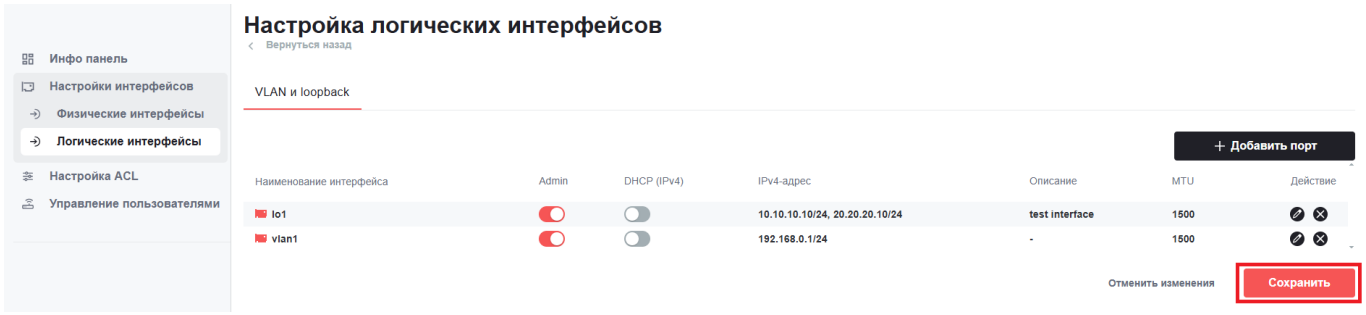


Рисунок 103 – Сохранение настроек

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 104).

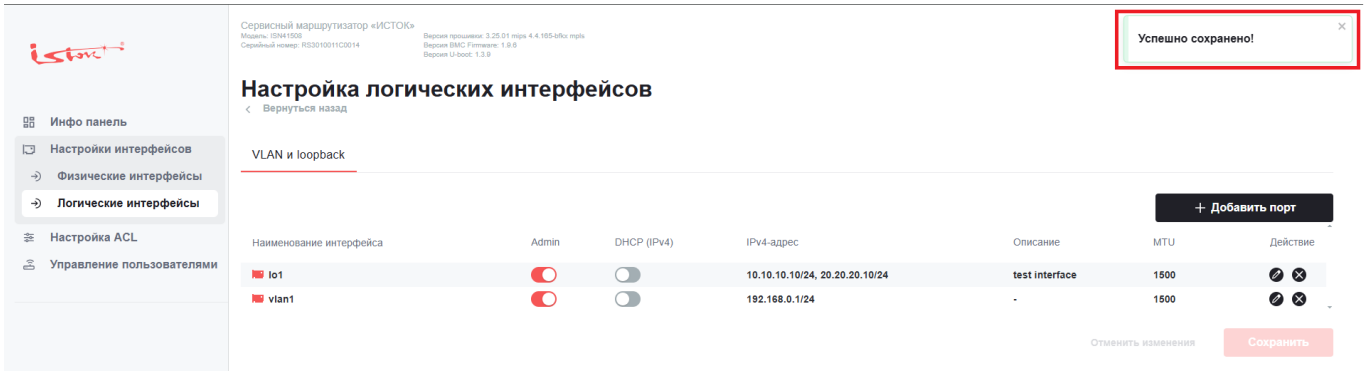


Рисунок 104 – Подтверждение сохранения

Для удаления интерфейса в столбце "Действие" нажмите пиктограмму "Удалить" (рисунок 105), затем кнопку "Сохранить" (рисунок 106).

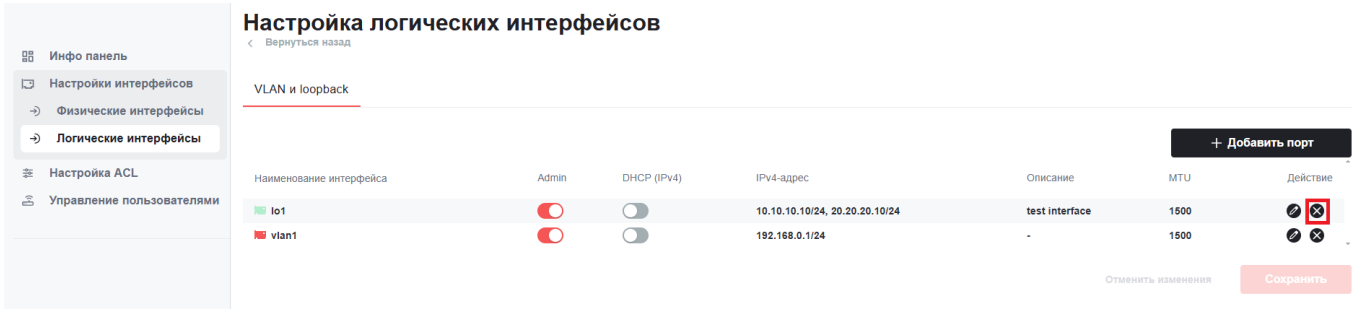


Рисунок 105 – Удаление интерфейса

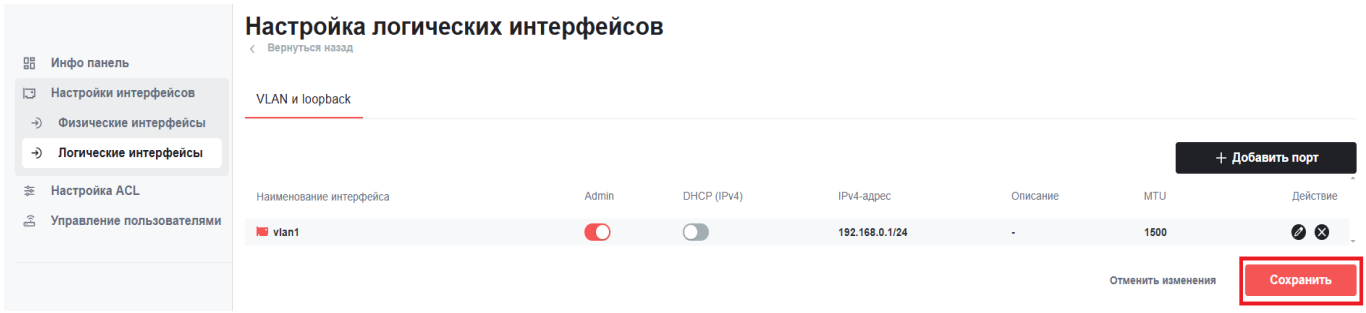


Рисунок 106 – Сохранение настроек

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 107).

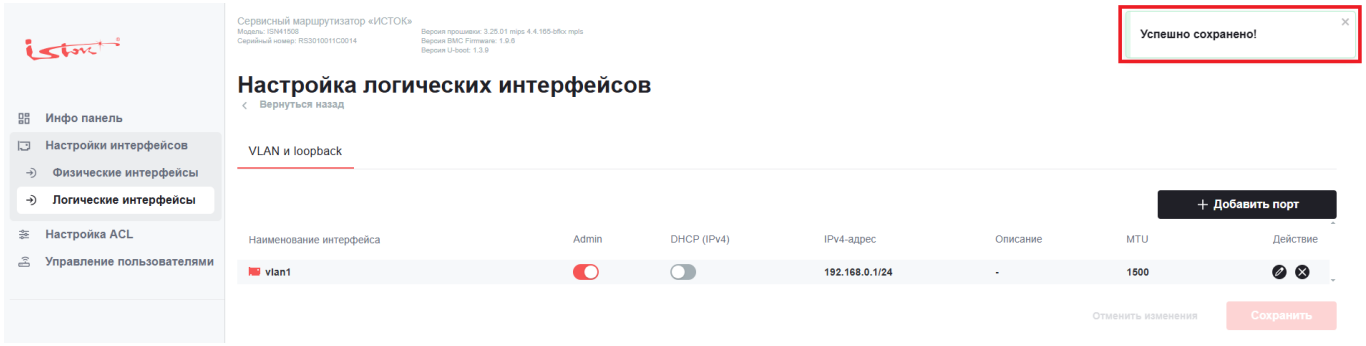


Рисунок 107 – Подтверждение сохранения

6 Настройка ACL

Внимание!

Для выполнения настроек сервисным маршрутизатором, список управления доступом (Access Control List) должен быть назначен:

фильтру (настройка ACL Filter);

списку маркировки пакетов (настройка ACL Mangle);

списку подмены ip-адресов (настройка ACL NAT);

списку политик (настройка ACL PBR).

Примечание

Более подробное описание для каждого правила смотрите в примерах настроек

На вкладке "Настройка ACL" отображаются таблицы с активными списками управления доступом (рисунок 108).

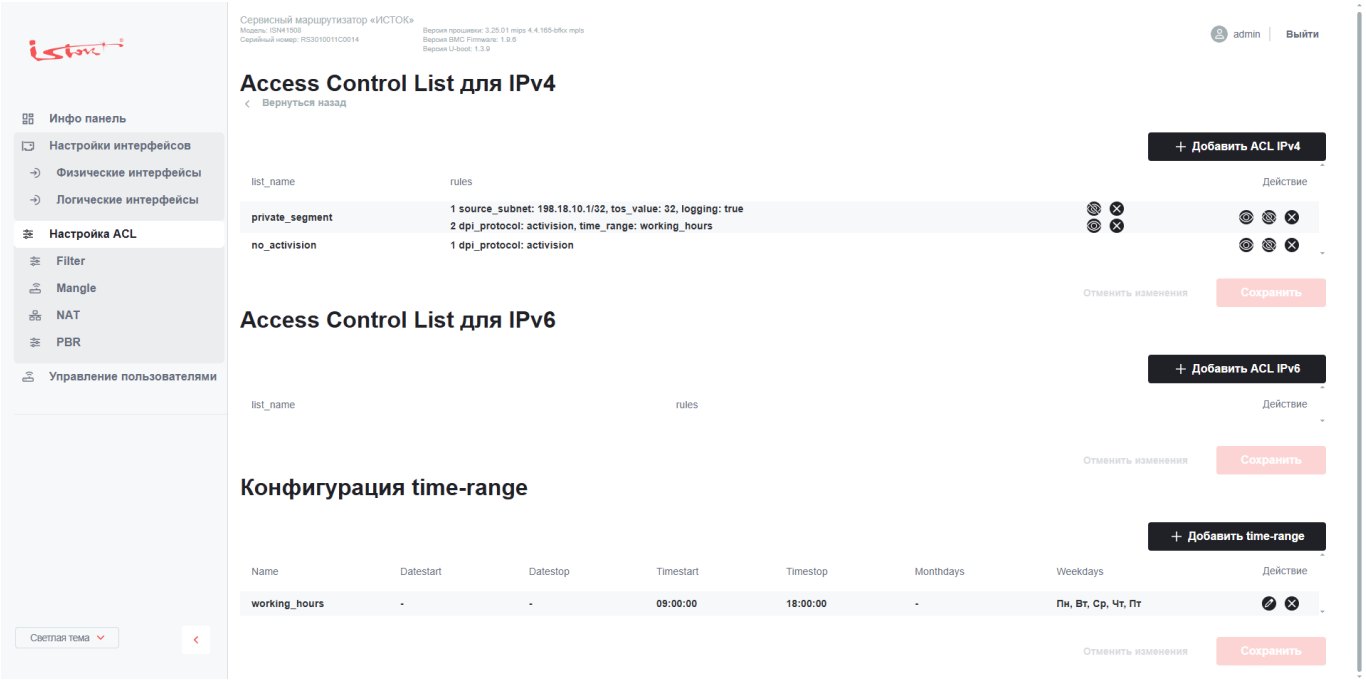


Рисунок 108 – Внешний вид вкладки "Настройка ACL"

6.1 Настройка Access Control List

Внимание!

Web-интерфейс не дает возможности редактировать правила в списке управления доступом. Убедитесь в корректном заполнении всех полей и расписании (настройка time-range) перед сохранением списка управлением доступа

Примечание

Для добавления правил (rules) существующему списку управления доступом, создайте новый список управления доступом с таким-же наименованием. После сохранения списки будут объединены.

Используйте кнопки "+Добавить ACL IPv4", "+Добавить ACL IPv6" для добавления соответствующего списка управления доступом (рисунок 109).

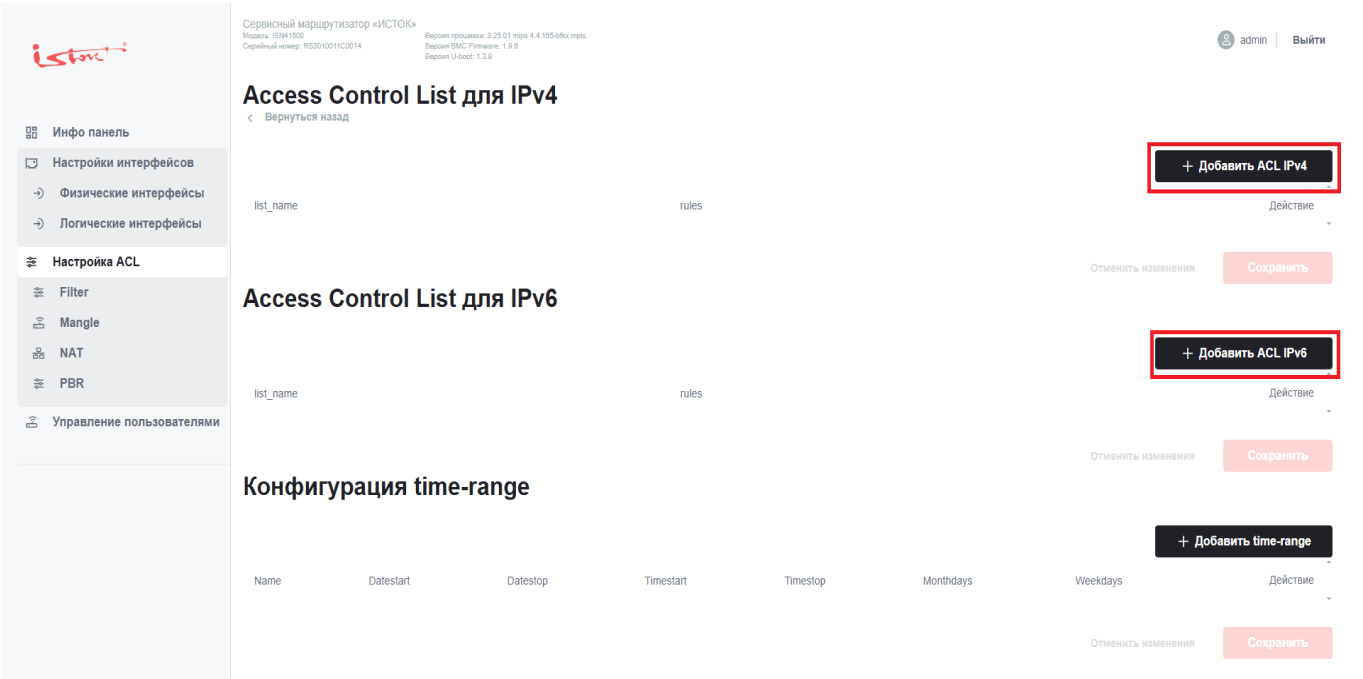


Рисунок 109 – Добавление списка управления доступом

В столбце "list_name" введите наименование списка управления доступом (рисунок 110).

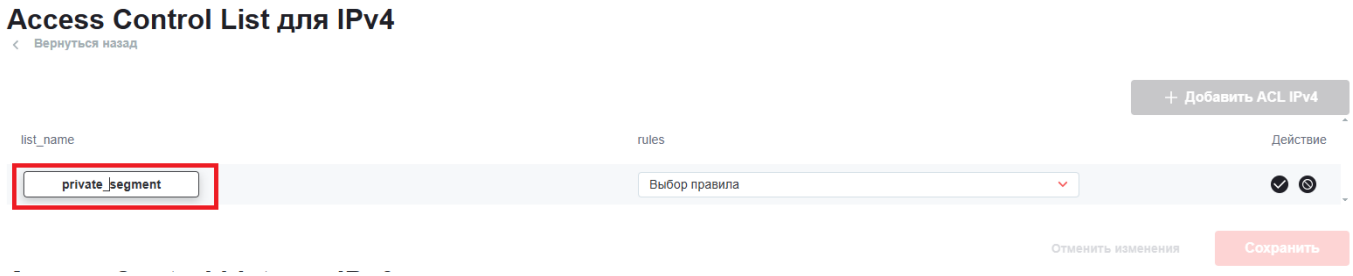


Рисунок 110 – Наименование списка контроля доступом

В столбце "rules" выберите одно или несколько правил, по которым будет осуществляться управление доступом на сервисном маршрутизаторе (рисунок 111).

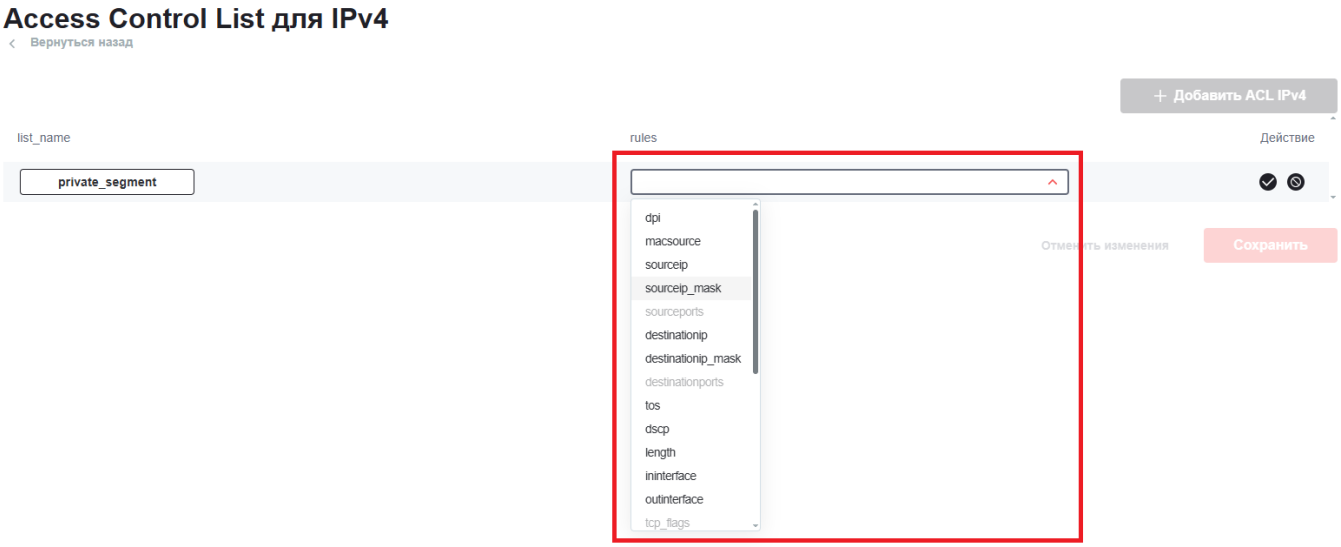


Рисунок 111 – Выбор правил

С каждым добавляемым правилом будет отображаться панель настройки добавленного правила (рисунок 112).

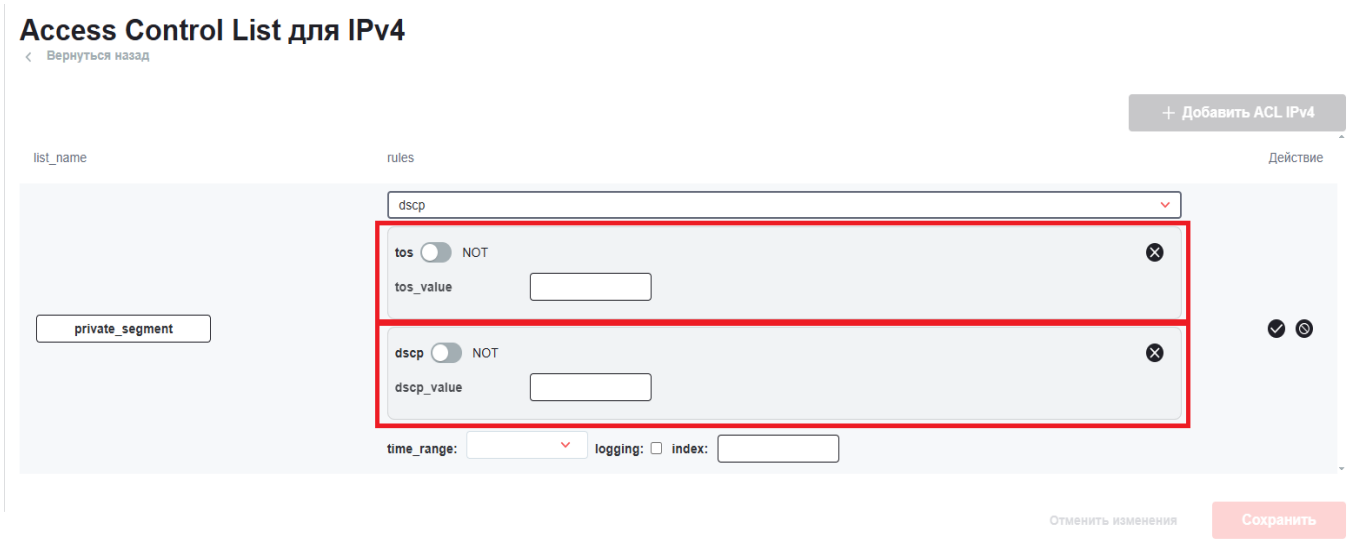


Рисунок 112 – Настройки правила

Примечание

Более подробное описание для каждого правила смотрите в примерах настроек

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 113).

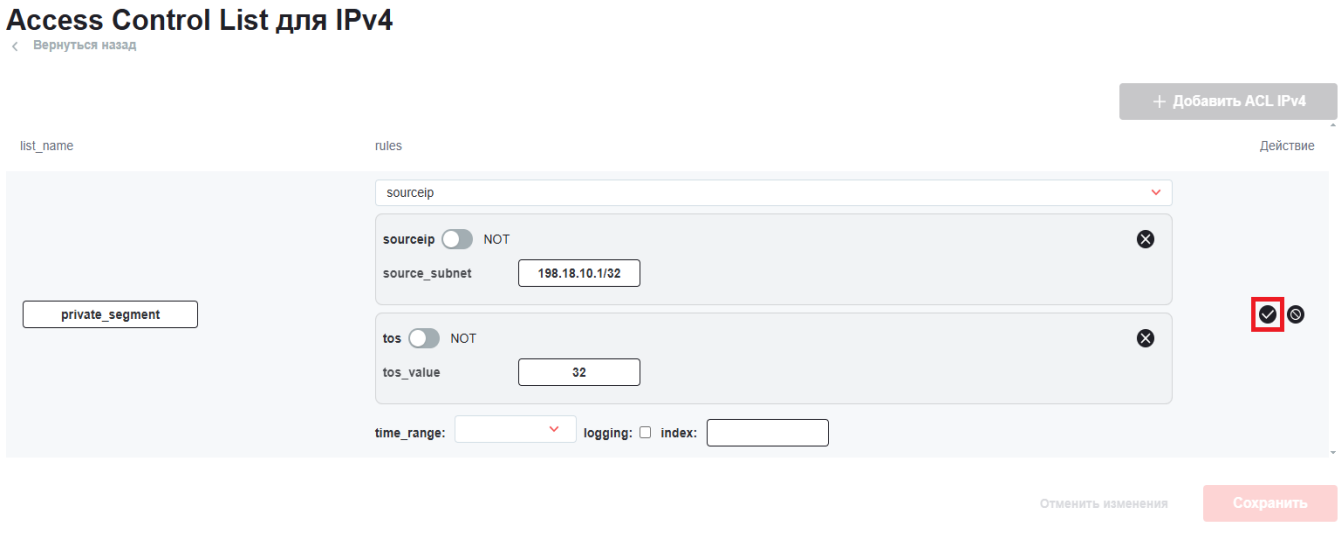


Рисунок 113 – Подтверждение создания списка

Настройте отображение сообщения о срабатывания правила в логе выбрав соответствующую пиктограмму (- отображать срабатывание правил списка управления доступом в логе, - не отображать срабатывание правил списка управления доступом в логе) (рисунок 114).

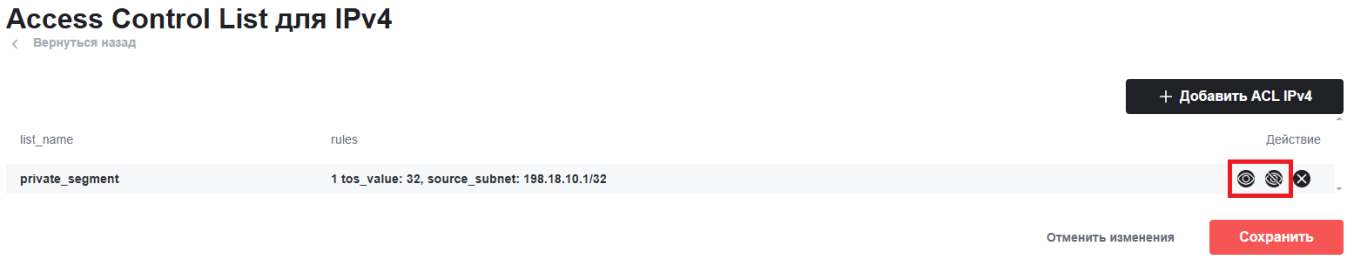


Рисунок 114 – Выбор занесения срабатывания правила в лог

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 115).

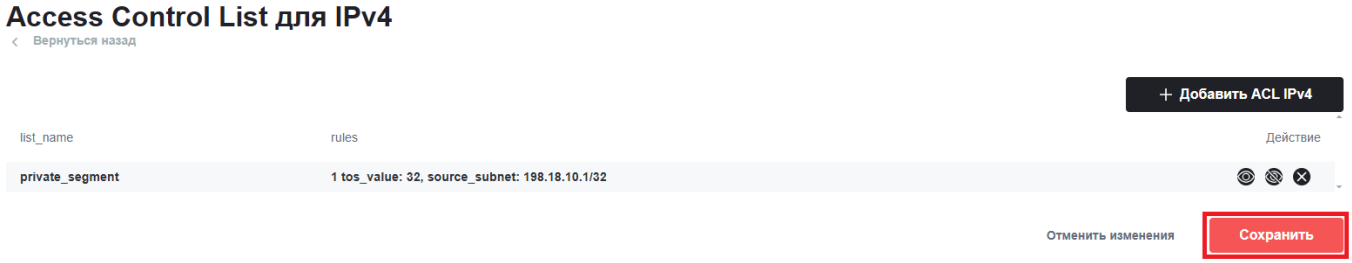


Рисунок 115 – Сохранение списка

Для удаления списка управления доступом в столбце "Действие" нажмите пиктограмму "Удалить" (рисунок 116), затем кнопку "Сохранить" (рисунок 117).

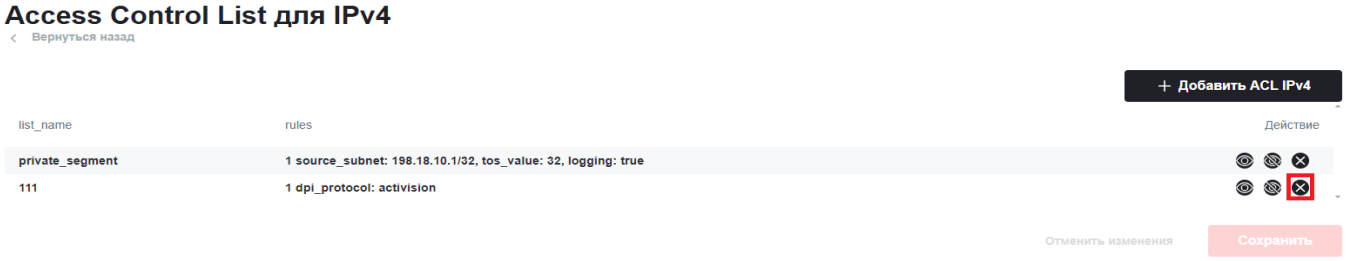


Рисунок 116 – Удаление списка управления доступом

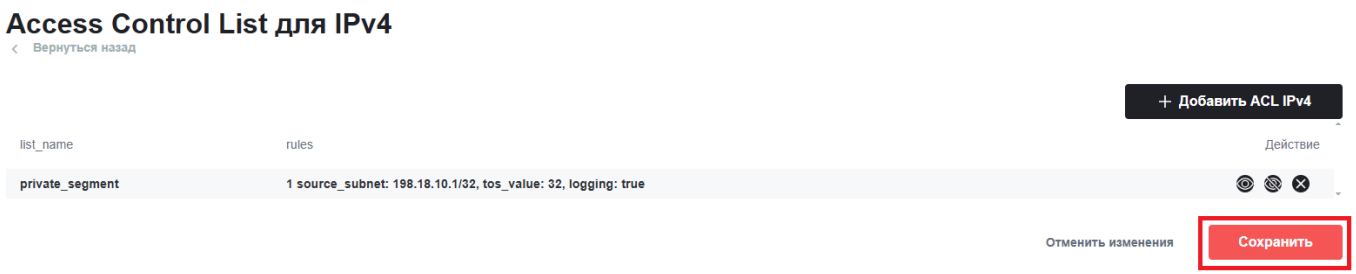


Рисунок 117 – Сохранение настроек

6.2 Настройка конфигурации time-range

Используйте кнопку "+Добавить time-range" для добавления расписания списку управления доступом (рисунок 118).

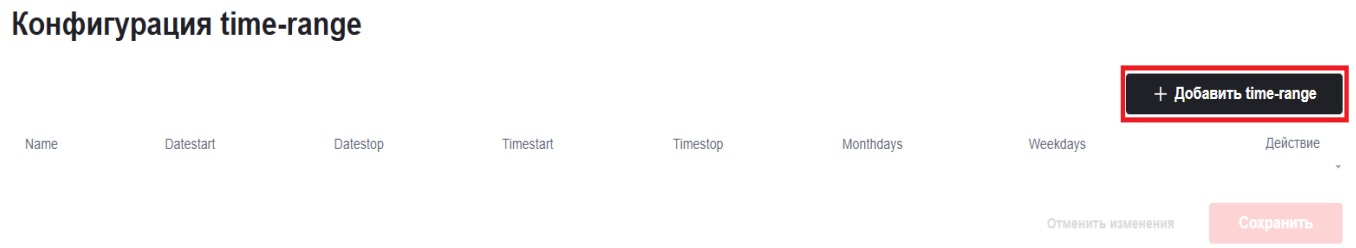


Рисунок 118 – Добавление списка управления доступом

В столбце "Name" введите наименование расписания списка управления доступом (рисунок 119).

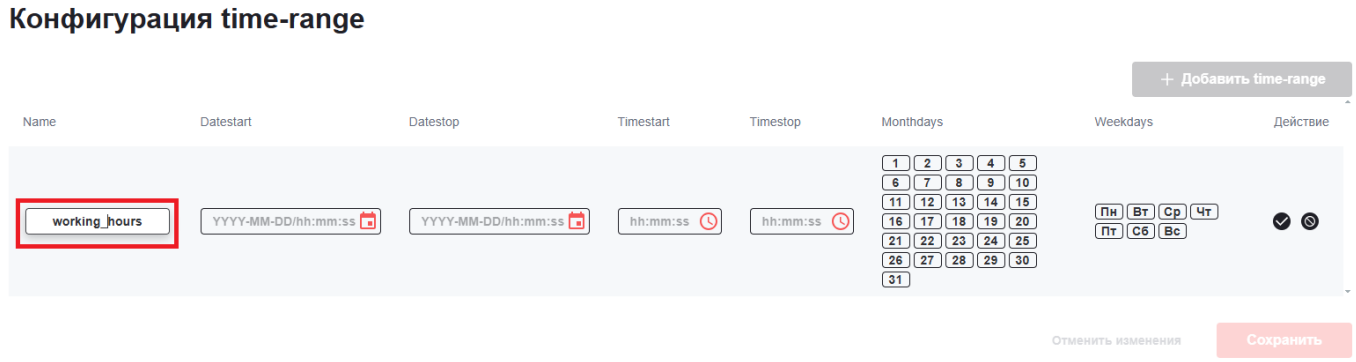


Рисунок 119 – Наименование списка контроля доступом

В столбцах со второго по седьмой задаются параметры работы расписания (рисунок 120), незаполненные поля считаются выполняющимися постоянно (например: если указать

время в Timestart и Timestop, но не указывать дни недели в Weekdays расписание будет срабатывать в указанное время в каждый день недели).

- Datestart - указывает дату и время начала работы;
- Datestop - указывает дату и время окончания работы;
- Timestart - указывает время начала работы;
- Timestop - указывает время окончания работы;
- Monthdays - указать в какие дни месяца будет срабатывать расписание;
- Weekdays - указать в какие дни недели будет срабатывать расписание.

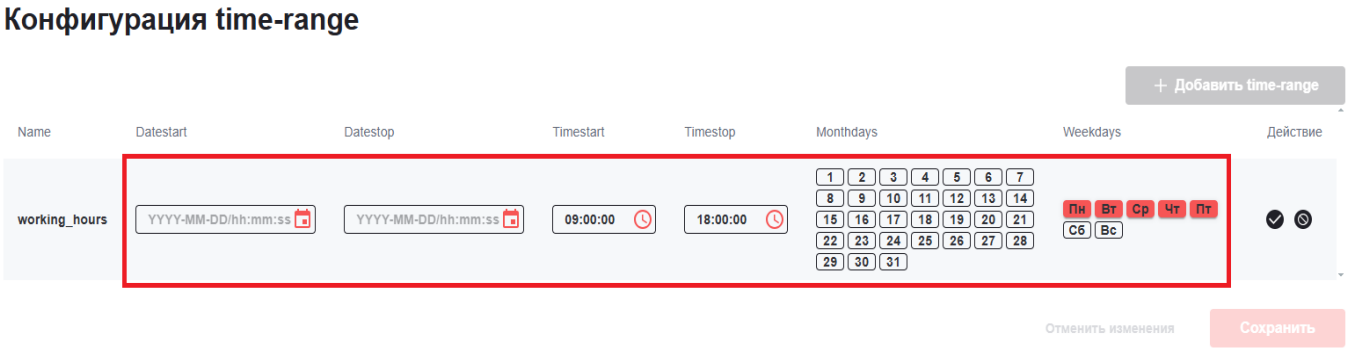


Рисунок 120 – Настройка временного диапазона

Подтвердите создание расписания, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 121).

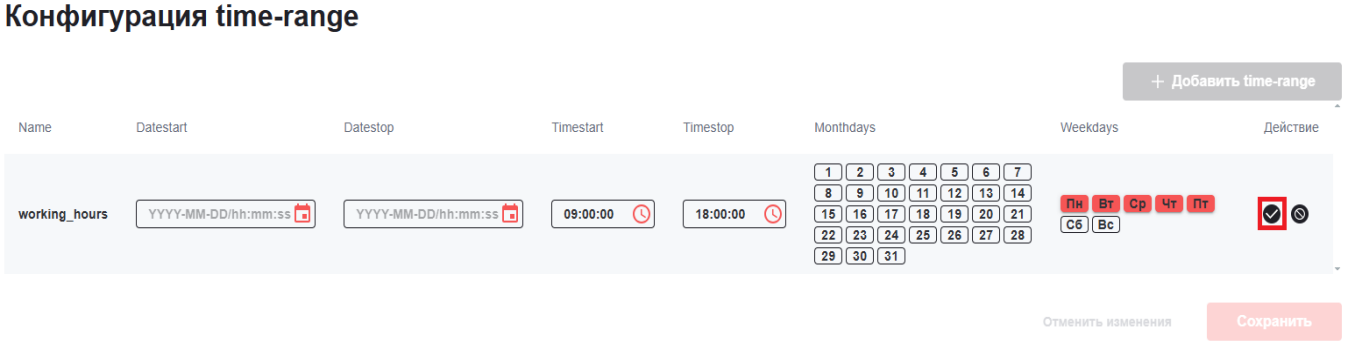


Рисунок 121 – Подтверждение создания списка

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 122).

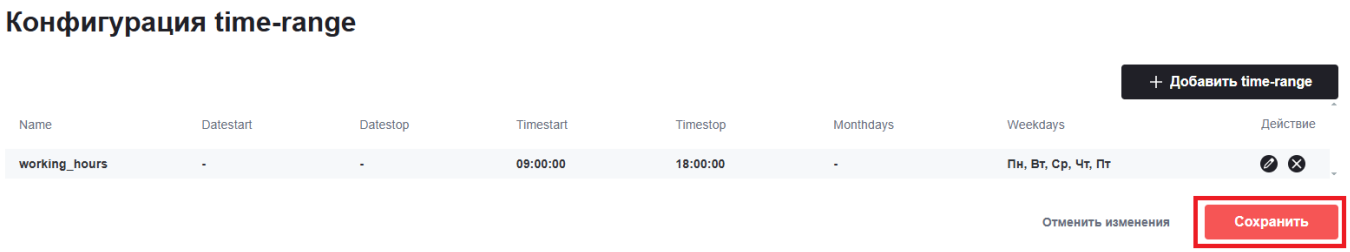


Рисунок 122 – Сохранение списка

Для удаления расписания в столбце "Действие" нажмите пиктограмму "Удалить" (рисунок 123), затем кнопку "Сохранить" (рисунок 124).

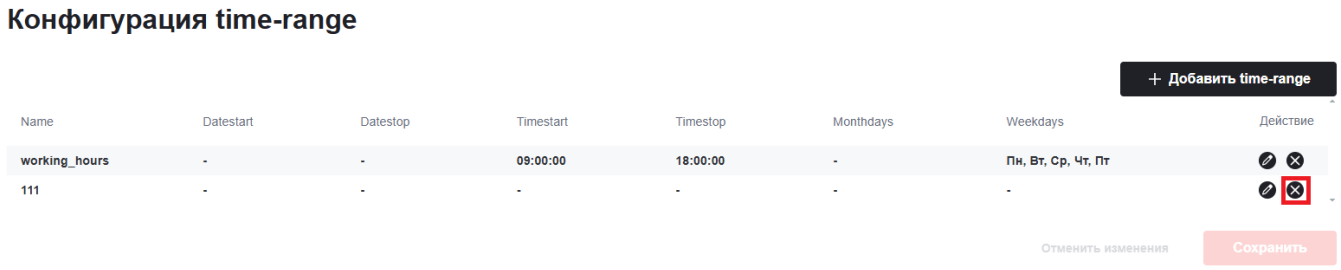


Рисунок 123 – Удаление расписания

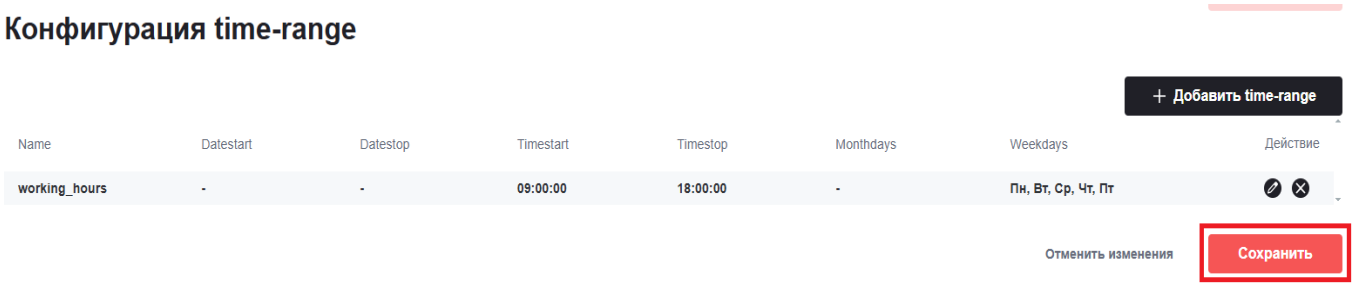


Рисунок 124 – Сохранение настроек

6.3 Настройка ACL Filter

На вкладке "Настройка ACL Filter" отображаются таблицы с активными фильтрами доступа (рисунок 125). В столбце "pkts" отображается количество пакетов, для которых сработал фильтр, а в столбце "bytes" объём данных в байтах, который они обработали.

Рисунок 125 – Внешний вид вкладки "Filter"

Для сброса статистики нажмите на пиктограмму "Сброс" в столбце "Действия" (рисунок 126).

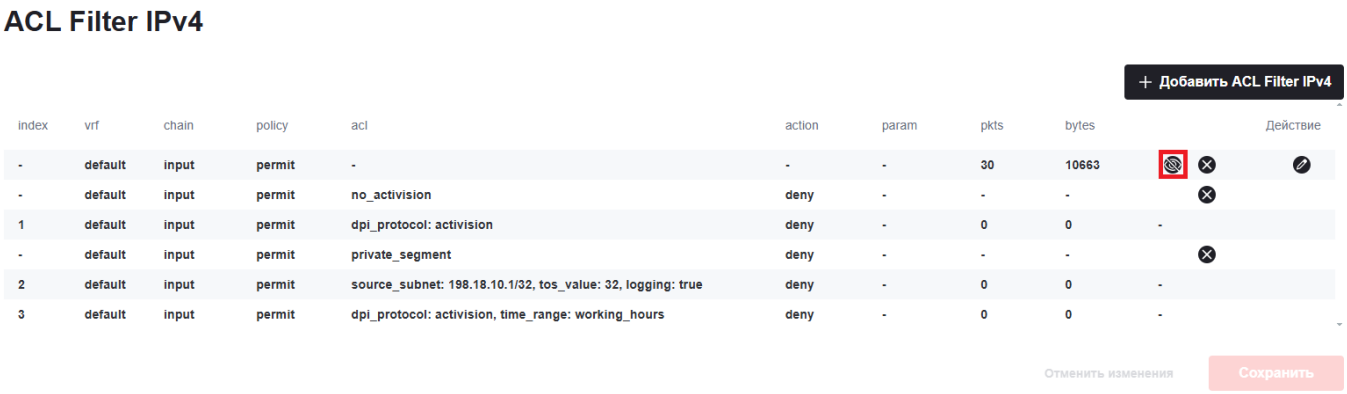


Рисунок 126 – Сброс статистики

Используйте кнопки "+Добавить ACL Filter IPv4", "+Добавить ACL Filter IPv6" для добавления соответствующего фильтра доступа (рисунок 127).

Рисунок 127 – Добавление списка управления доступом

В столбце "index" укажите индекс фильтра, который определят порядок срабатывания правил (чем меньше индекс, тем раньше будет применено правило) (рисунок 128).

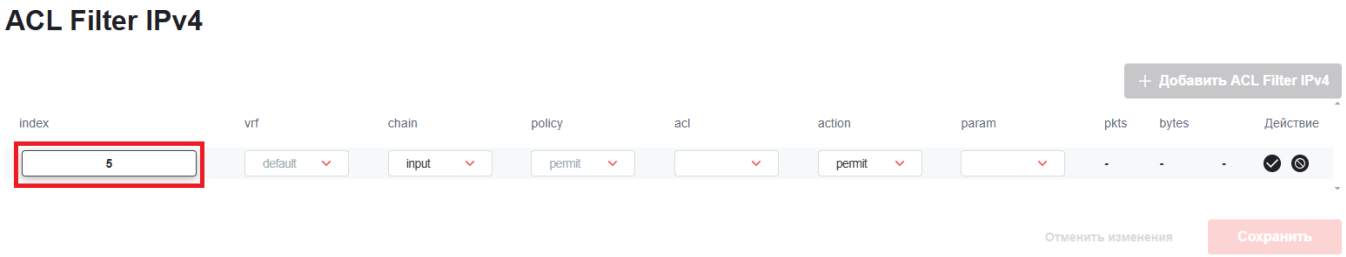


Рисунок 128 – Индекс ACL Filter

В столбце "chain" выберите тип пакетов для которых будет применен фильтр (рисунок 129):

- forward - применять к пакетам проходящим через сервисный маршрутизатор;
- input - применять к пакетам, поступающим на сервисный маршрутизатор (фильтр применяется к пакетам, адреса которых совпадают с адресом интерфейса сервисного маршрутизатора, на который эти пакеты поступили);
- output - применять к пакетам, созданным сервисным маршрутизатором.

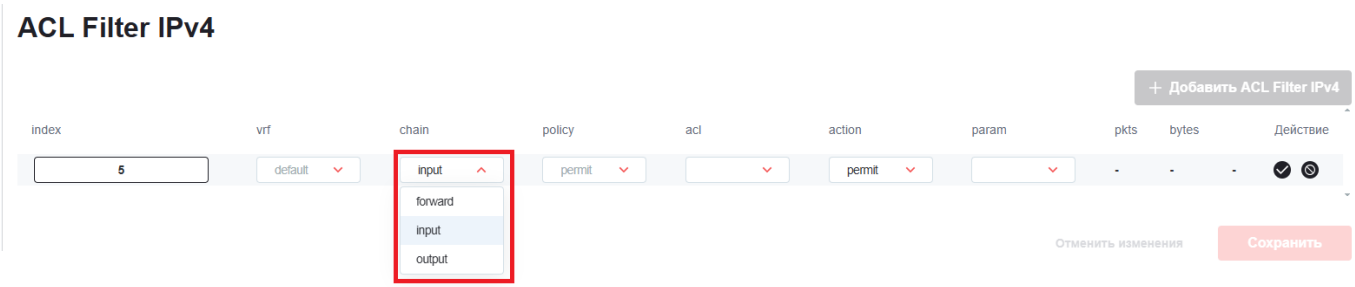


Рисунок 129 – Выбор типа пакетов

Примечание

Пакеты, проходящие через маршрутизатор не подлежат действию правил input, output

В столбце "acl" выберите один из списков контроля доступом, по которому будет осуществляться фильтрация (рисунок 130).

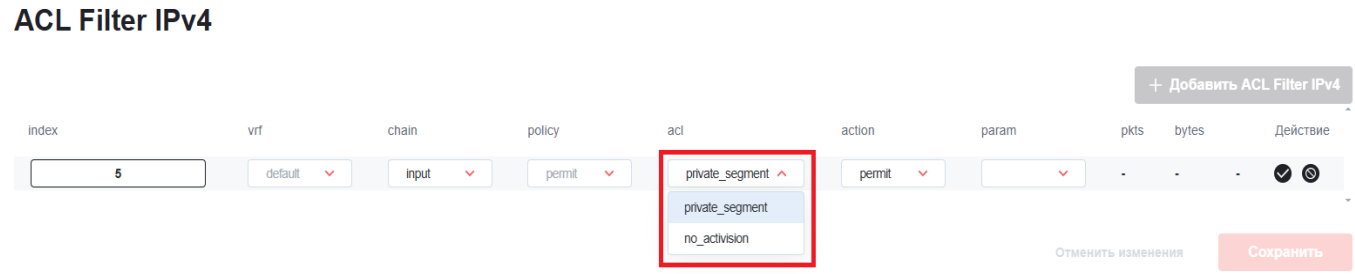


Рисунок 130 – Выбор списка контроля доступом

В столбце "action" выберите действие, которое будет выполнено при срабатывании правила (рисунок 131):

- deny - отбросить пакет;
- permit - пропустить пакет (правила из последующих фильтров не будут применяться к данному пакету);
- reject - отбросить пакет и послать сообщение ICMP reject.

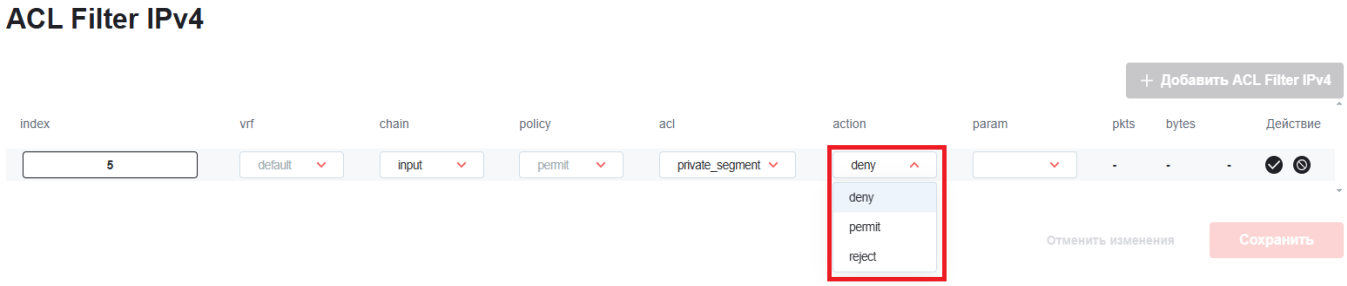


Рисунок 131 – Действия при срабатывании правила

Примечание

Для действий типа reject выберите тип ICMP ответа из поля в столбце "param"

Подтвердите создание фильтра, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 132).

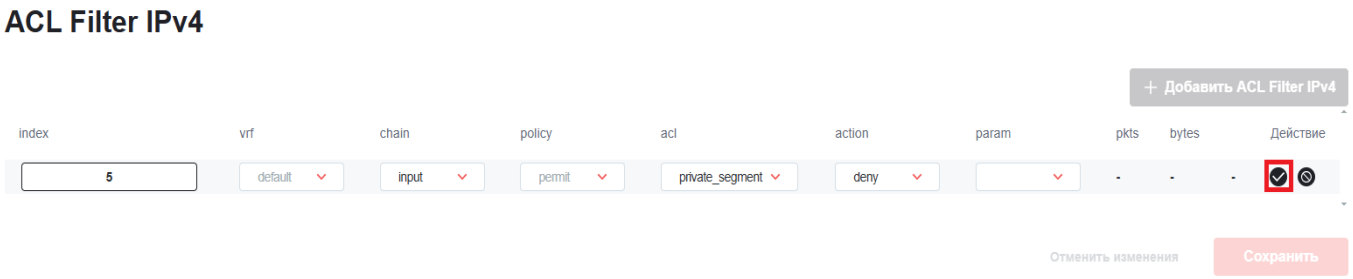


Рисунок 132 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 133).

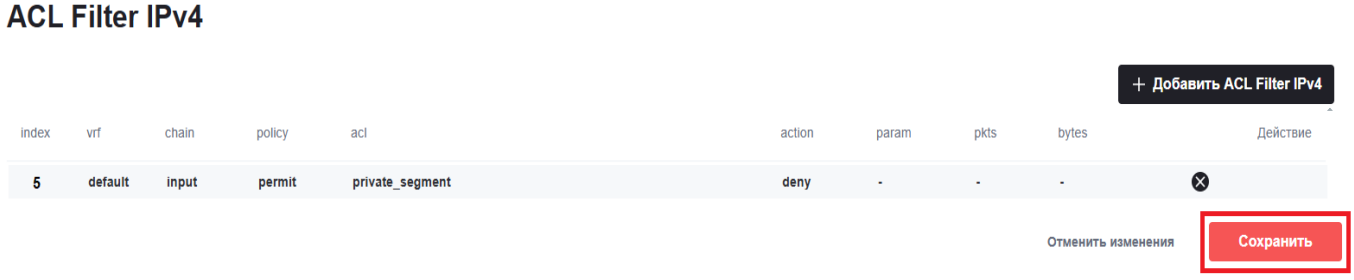


Рисунок 133 – Сохранение фильтра

После сохранения в таблице отобразится новый фильтр доступа, а все применимые правила будут записаны в следующих строках с собственным индексом в порядке их применения (рисунок 134).

Рисунок 134 – Список фильтров

Для удаления фильтра доступа нажмите на пиктограмму "Удалить" в столбце "Действие" (рисунок 135).

Рисунок 135 – Удаление фильтра доступа

6.4 Настройка ACL Mangle (Маркировки пакетов)

Примечание

Более подробное описание для каждого типа действия с пакетом смотрите в примерах настроек

На вкладке "Настройка ACL Mangle" отображаются таблицы с активными списками маркировки пакетов (рисунок 136). В столбце "pkts" записывается количество пакетов для

которых сработал фильтр, а в столбце "bytes" записывается объём данных в байтах , который они обработали.

Рисунок 136 – Внешний вид вкладки "Filter"

Для сброса статистики нажмите на пиктограмму "Сброс" в столбце "Действия" (рисунок 137).

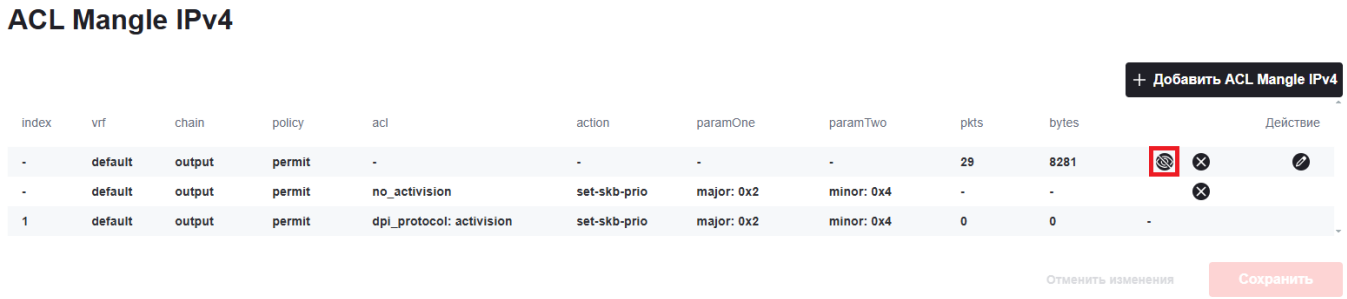


Рисунок 137 – Сброс статистики

Для добавления нового списка маркировки пакетов используйте кнопки "+Добавить ACL Mangle IPv4" и "+Добавить ACL Mangle IPv6" (рисунок 138).

Рисунок 138 – Добавление списка управления доступом

В столбце "index" укажите индекс списка, который определят порядок срабатывания правил (чем меньше значение индекса, тем раньше будет применено правило, и последующие правила не будут действовать на данный пакет) (рисунок 139).

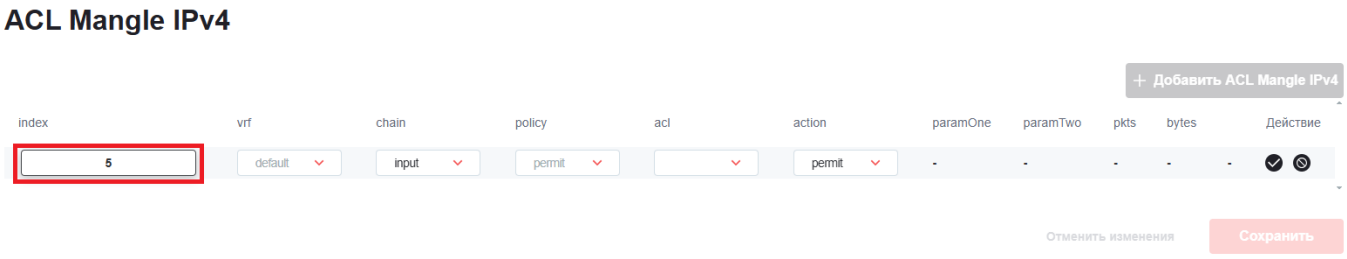


Рисунок 139 – Индекс ACL Mangle

В столбце "chain" выберите тип пакетов, к которым будет применяться маркировка (рисунок 140):

- forward - применять к пакетам, проходящим через сервисный маршрутизатор;
- input - применять к пакетам, поступающим на сервисный маршрутизатор (фильтр применяется к пакетам, адреса которых совпадают с адресом интерфейса сервисного маршрутизатора, на который эти пакеты поступают);
- output - применять к пакетам созданным сервисным маршрутизатором;
- postrouting - применять к пакетам после их маршрутизации;
- prerouting - применять к пакетам до их маршрутизации.

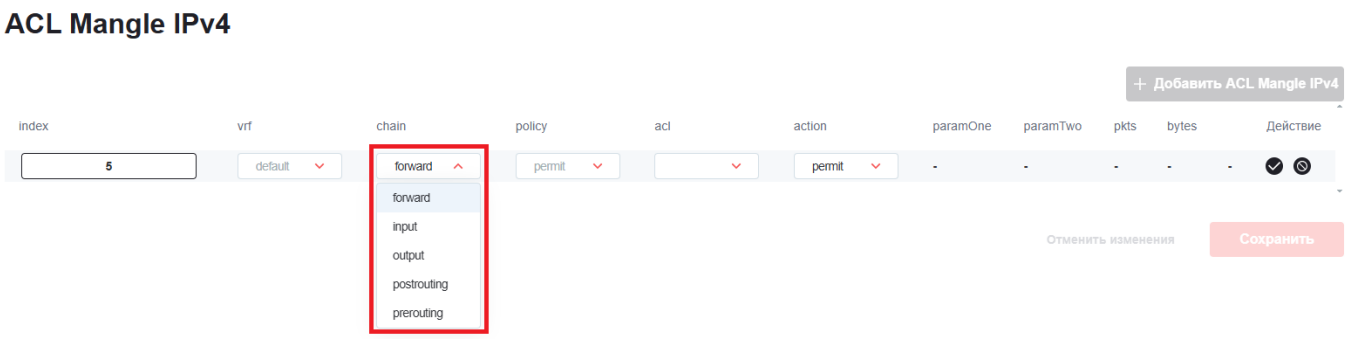


Рисунок 140 – Выбор типа пакетов

Примечание

Пакеты, проходящие через маршрутизатор не попадают под действие правил input, output

В столбце "acl" выберите один из списков контроля доступом, по которому будет осуществляться маркировка (рисунок 141).

Рисунок 141 – Выбор списка контроля доступом

В столбце "action" выберите действие, которое будет выполнено при срабатывании правила (рисунок 142):

- clone - клонировать пакет;
- deny - отбросить пакет;
- permit - пропустить пакет (правила из последующих фильтров не будут применяться к данному пакету);
- set-clamp-mss - установить MSS равным MTU исходящего интерфейса;
- set-mark - установить метку;

- set-mss - установить значение MSS в заголовке TCP;
- set-skb-prio - установить приоритет пакета;
- set-tos - установить значение TOS.

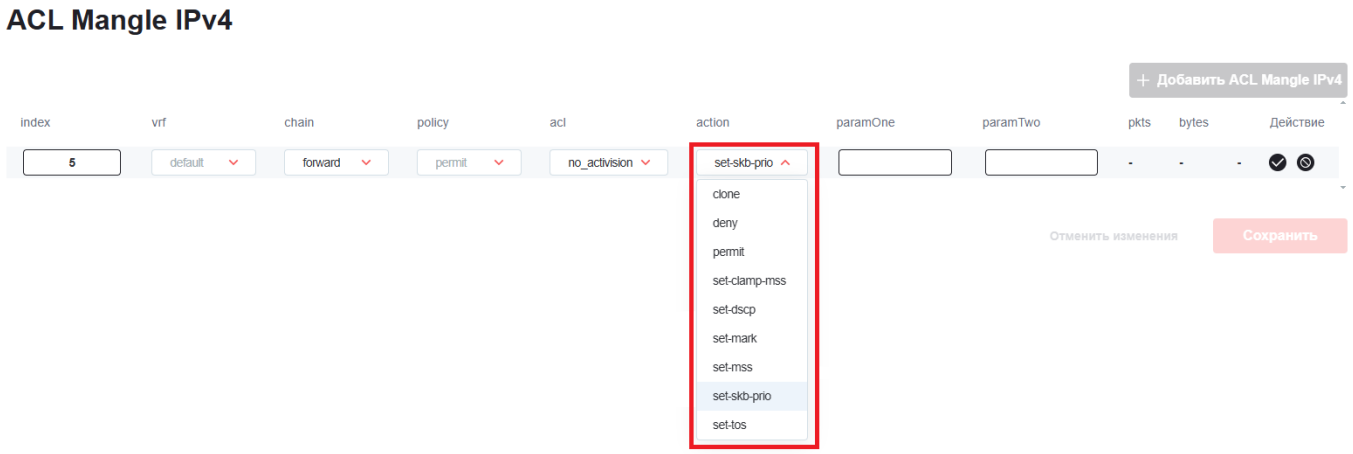


Рисунок 142 – Действия при срабатывании правила

Примечание

Более подробное описание для каждого типа действия с пакетом смотрите в примерах настроек

В столбцах параметров "paramOne" и "paramTwo" введите необходимые параметры маркировки пакетов (рисунок 143).

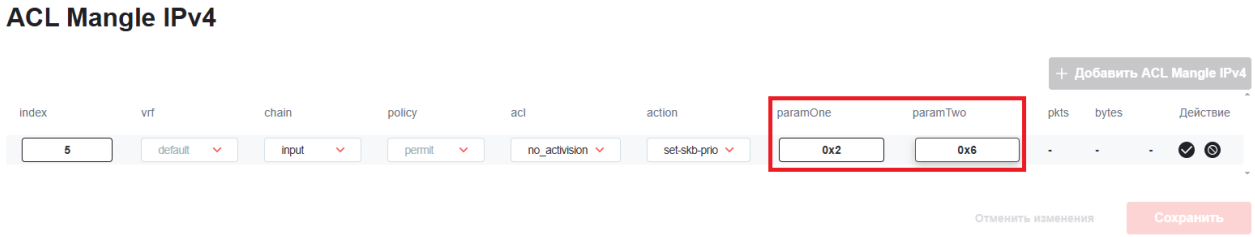


Рисунок 143 – Заполнение параметров маркировки

Подтвердите создание списка маркировки, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 144).

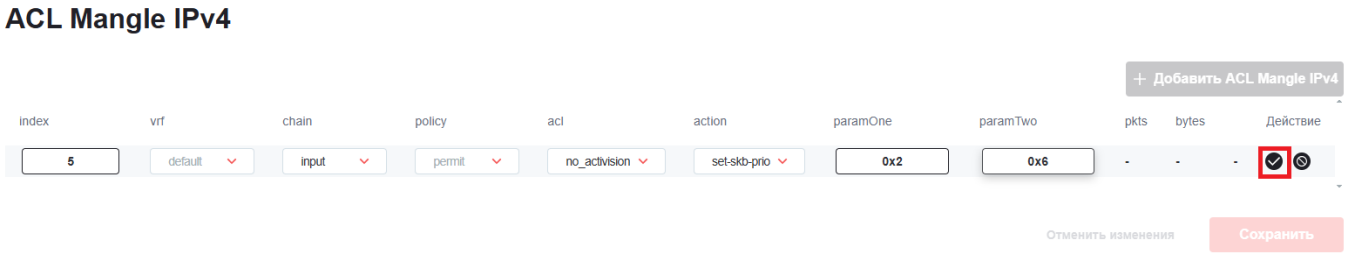


Рисунок 144 – Подтверждение создания списка маркировки

Затем нажмите клавишу "Сохранить" (рисунок 145).

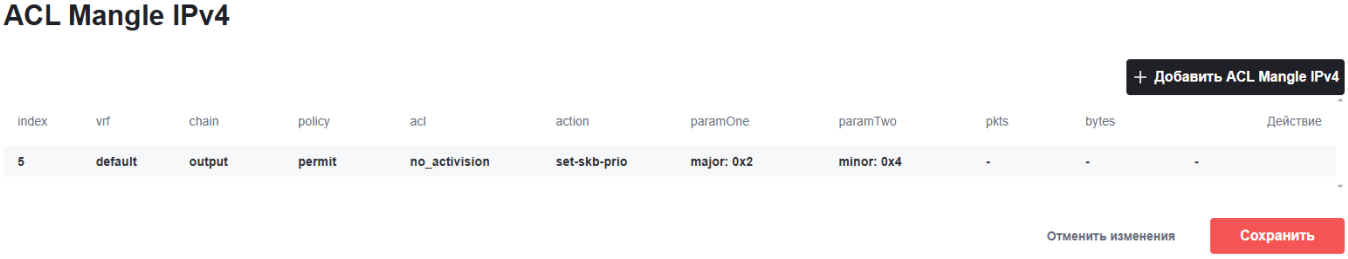


Рисунок 145 – Сохранение фильтра

После сохранения в таблице отобразится новый список маркировки, а все применимые правила будут записаны в следующих строках с собственным индексом в порядке их применения (рисунок 146).

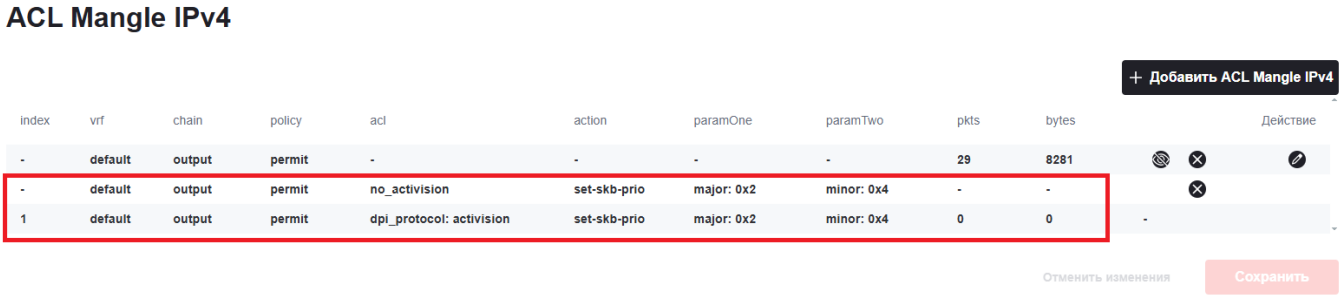


Рисунок 146 – Списки маркировки

Для удаления списка маркировки нажмите на пиктограмму "Удалить" в столбце "Действие" (рисунок 147).

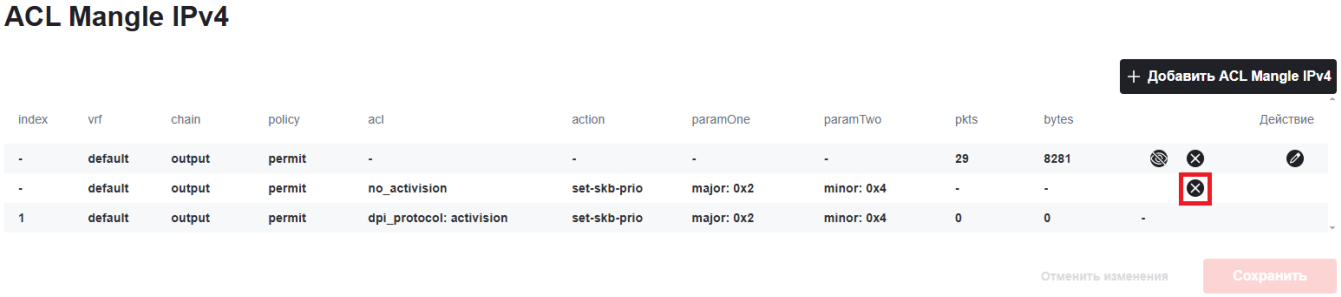


Рисунок 147 – Удаление фильтра доступа

6.5 Настройка ACL NAT (подмены ip-адресов)

Примечание

Более подробное описание для каждого типа действия с пакетом смотрите в примерах настроек

На вкладке "Настройка ACL NAT" отображаются таблицы с активными списками подмены ip-адресов (рисунок 148). В столбце "pkts" отображается количество пакетов, для которых сработал фильтр, а в столбце "bytes" объём данных в байтах, который они обработали.

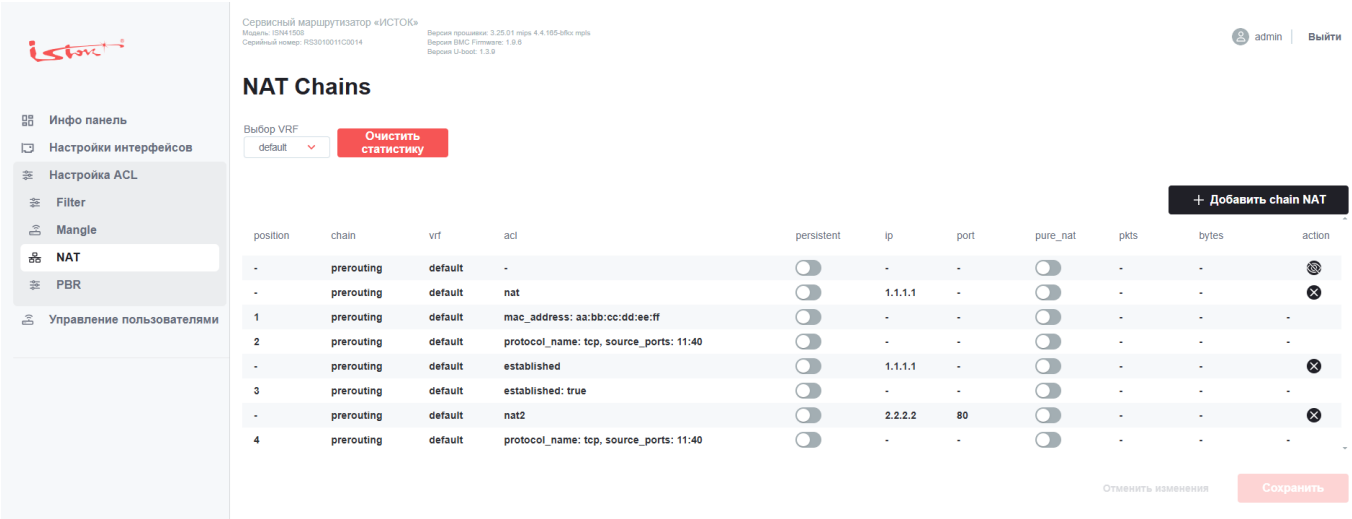


Рисунок 148 – Внешний вид вкладки "NAT"

Для добавления нового списка подмены IP-адресов нажмите кнопку "+Добавить chain NAT" (рисунок 149).

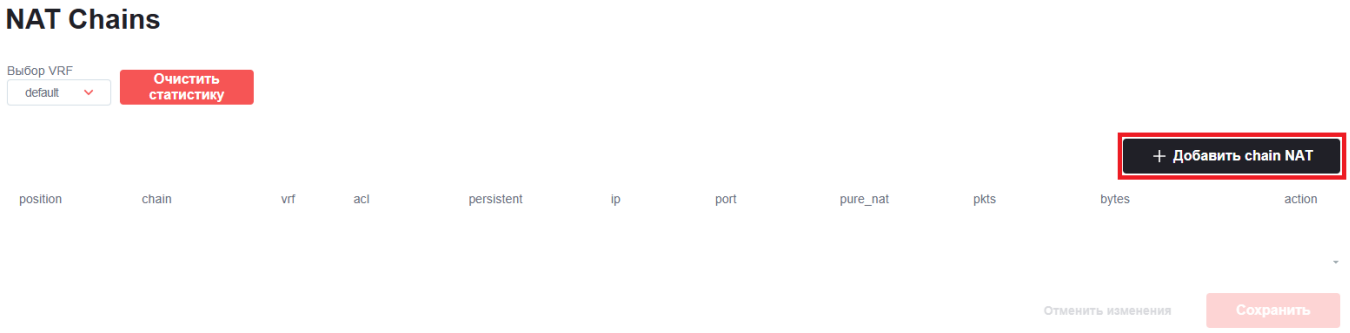


Рисунок 149 – Добавить списка подмены ip-адресов

В столбце "position" укажите позицию фильтра, которая определят порядок срабатывания правил (чем позиция меньше, тем раньше будет применено правило) (рисунок 150).

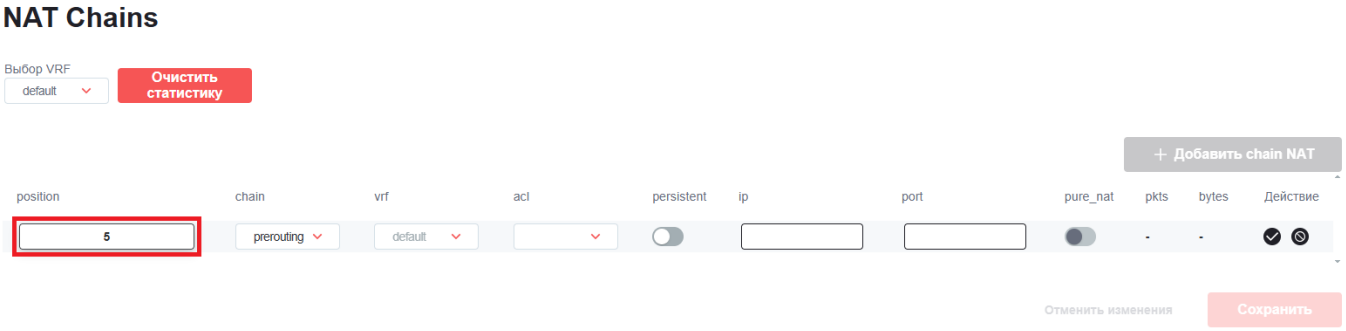


Рисунок 150 – Позиция ACL NAT

В столбце "chain" выберите тип пакетов для которых будет применен фильтр (рисунок 151):

- output - применять к пакетам созданным сервисным маршрутизатором;
- postrouting - применять к пакетам после их маршрутизации;
- prerouting - применять к пакетам до их маршрутизации.

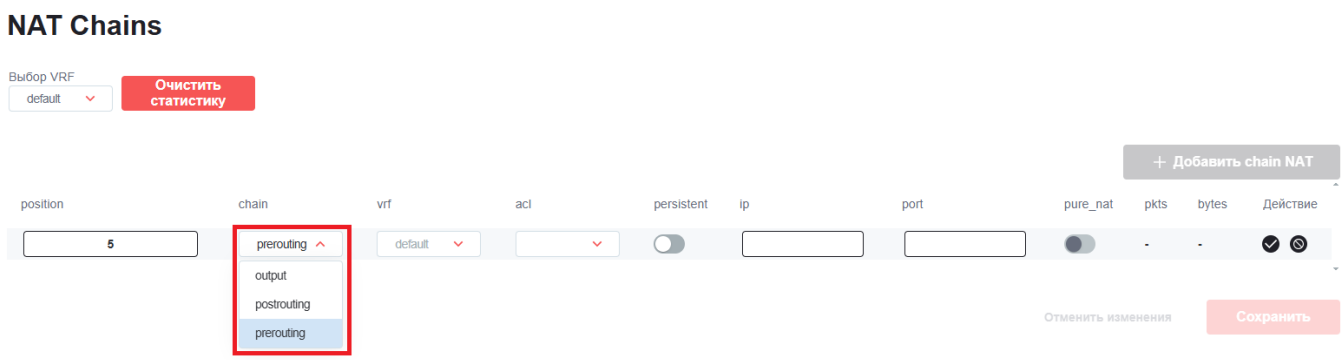


Рисунок 151 – Выбор типа пакетов

В столбце "acl" выберите один из списков контроля доступом, по которому будет осуществляться подмена IP-адреса (рисунок 152).

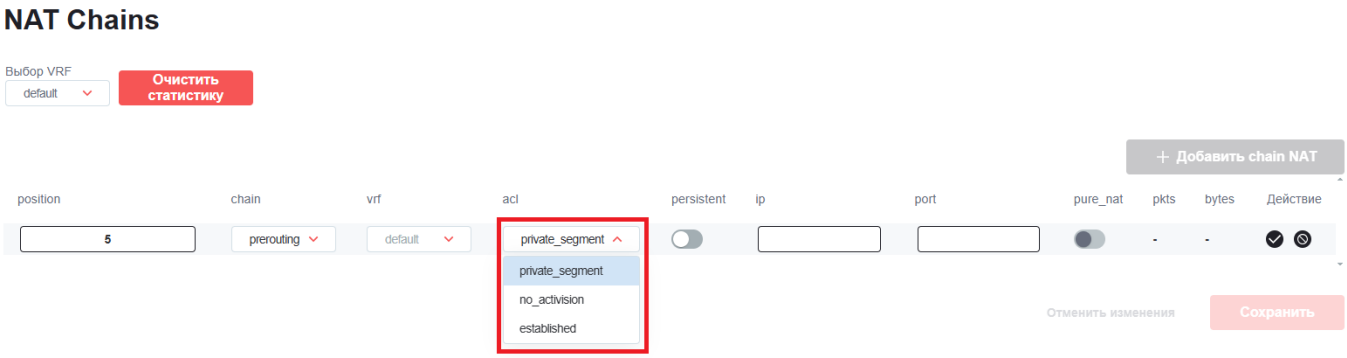


Рисунок 152 – Выбор списка контроля доступом

Используйте кнопку-переключатель в столбце "persisten" для изменения статуса persistent (активный статус persistent гарантирует, что внутренний IP-адрес и порт всегда сопоставляются с одним и тем же публичным адресом и портом) (рисунок 153).

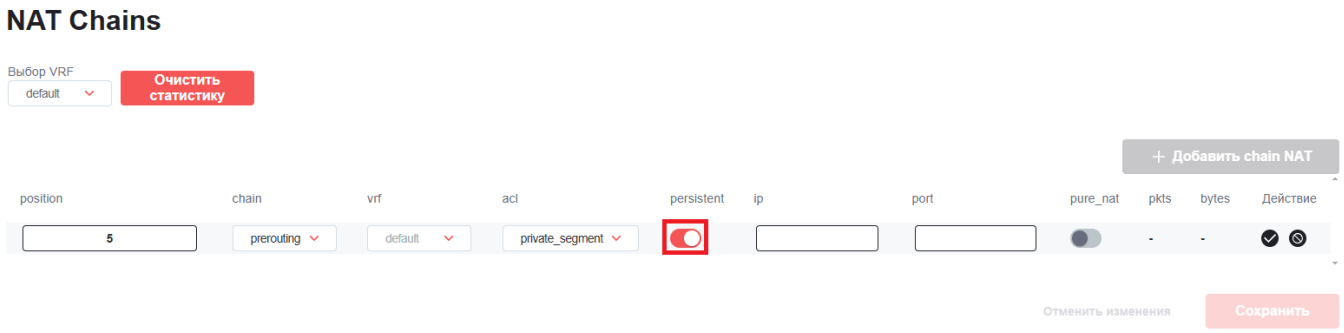


Рисунок 153 – Изменение статуса persisten

Введите IP-адрес или пул IP-адресов, используемых для подмены в поле столбца "ip" (рисунок 154).

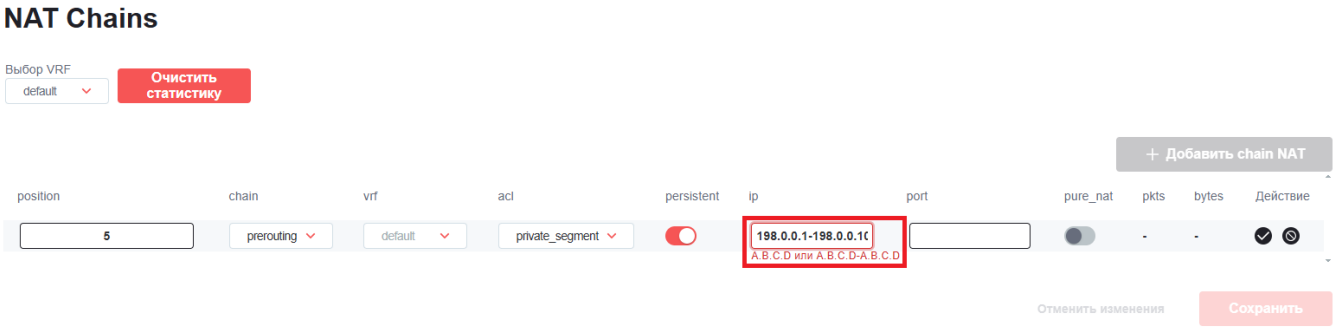


Рисунок 154 – Добавление IP-адреса

Укажите порт, используемый для подмены, в поле столбца "port" (рисунок 155).

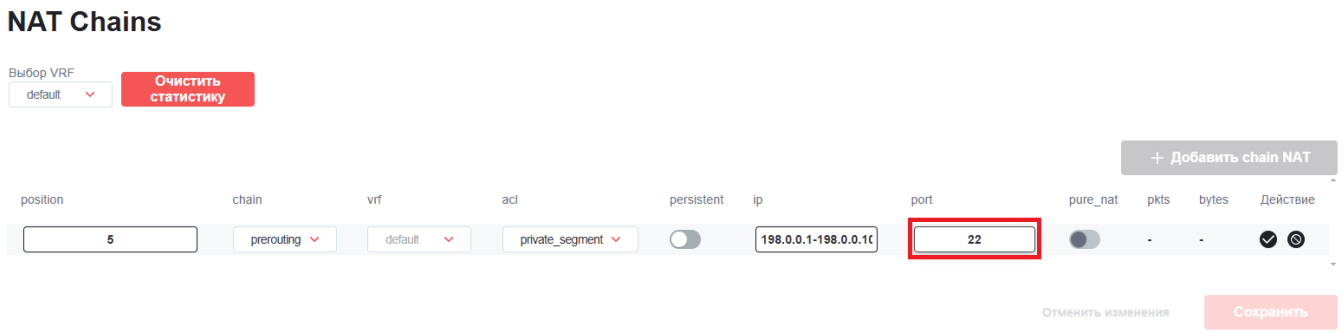


Рисунок 155 – Добавление порта

Используйте кнопку-переключатель в столбце "pure_nat" для изменения статуса данного параметра (активный статус pure_nat позволяет устройствам внутри локальной сети обращаться к серверам в этой же сети, используя их публичный IP-адрес или доменное имя) (рисунок 156).

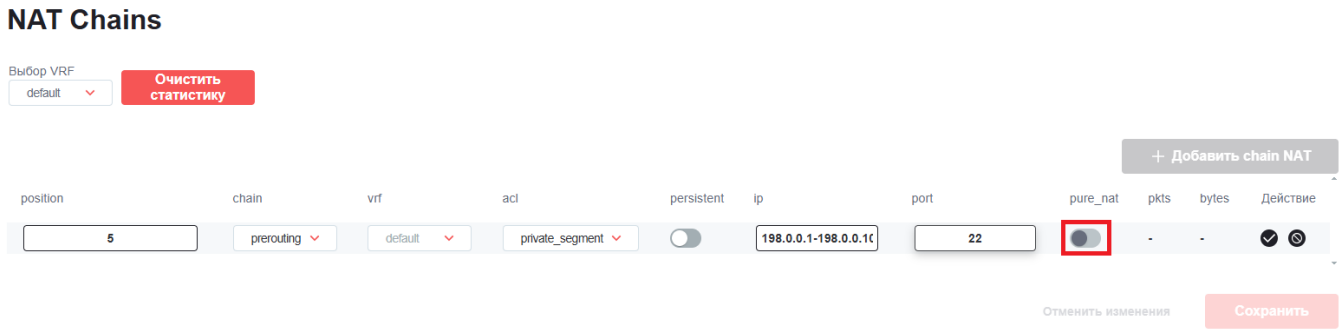


Рисунок 156 – Изменение статуса pure_nat

Для сохранения настроек необходимо сначала подтвердить изменения, нажав соответствующую пиктограмму в столбце "Действие" (рисунок 157).

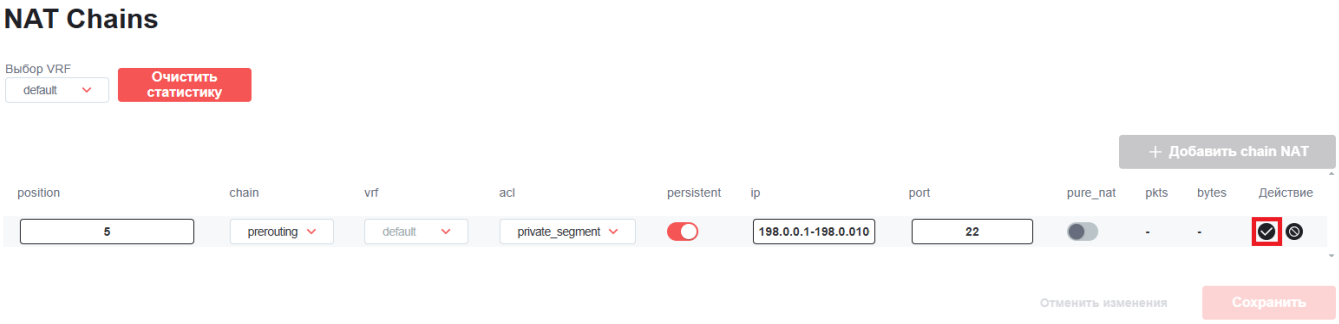


Рисунок 157 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 158).

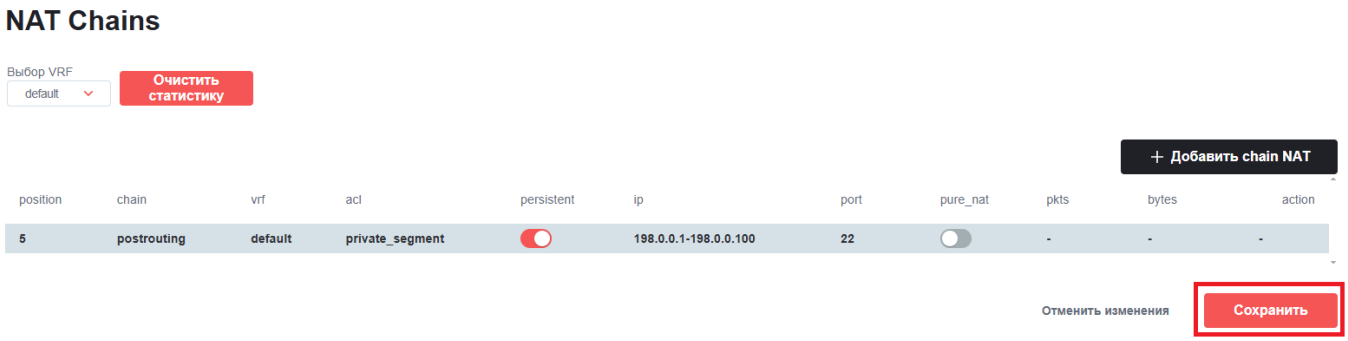


Рисунок 158 – Сохранение настроек

6.6 Настройка ACL PBR (политик)

Примечание

Более подробное описание для каждого типа действия с пакетом смотрите в примерах настроек

На вкладке "Настройка ACL PBR" отображаются таблицы с маршрутизацией на основе политик (рисунок 159).

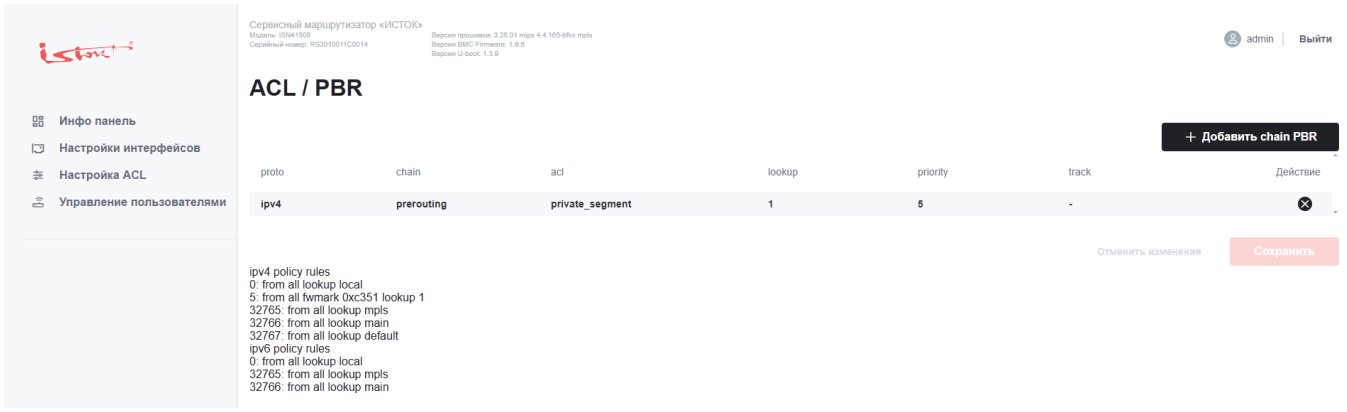


Рисунок 159 – Внешний вид вкладки "PBR"

Для добавления новой политики нажмите кнопку "+Добавить chain PBR" (рисунок 160).

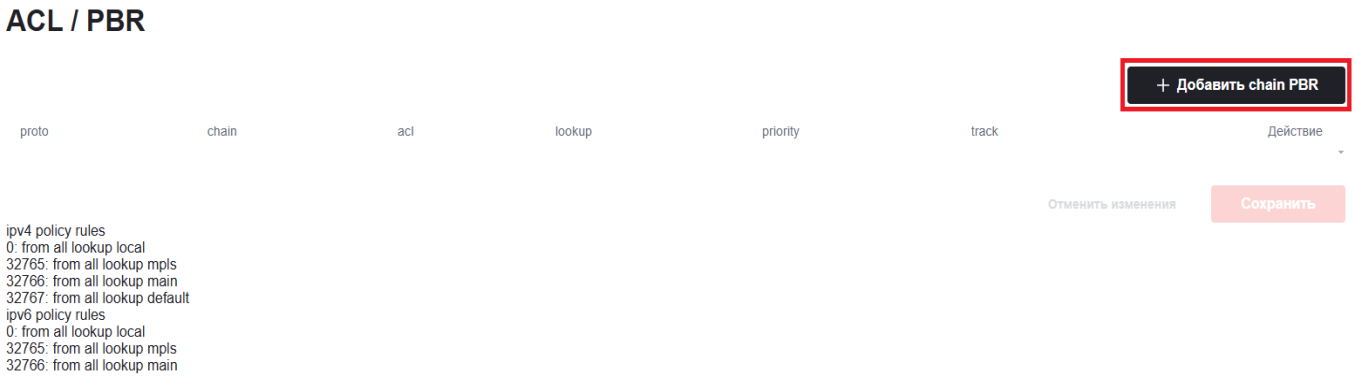


Рисунок 160 – Добавить политику маршрутизации

В столбце "proto" выберите протокол (IPv4/IPv6) на котором будет работать политика маршрутизации (рисунок 161).

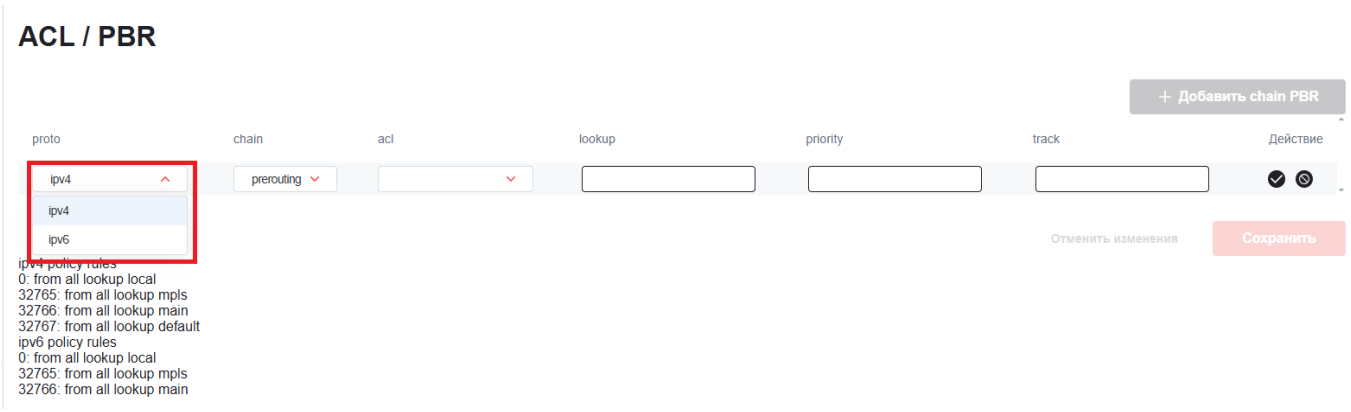


Рисунок 161 – Выбор протокола

В столбце "chain" выберите тип пакетов для которых будет применен фильтр (рисунок 162):

- forward - применять к пакетам, проходящим через сервисный маршрутизатор;
- input - применять к пакетам, поступающим на сервисный маршрутизатор (фильтр применяется к пакетам, адреса которых совпадают с адресом интерфейса сервисного маршрутизатора, на который эти пакеты поступают);
- output - применять к пакетам созданным сервисным маршрутизатором;
- postrouting - применять к пакетам после их маршрутизации;
- prerouting - применять к пакетам до их маршрутизации.

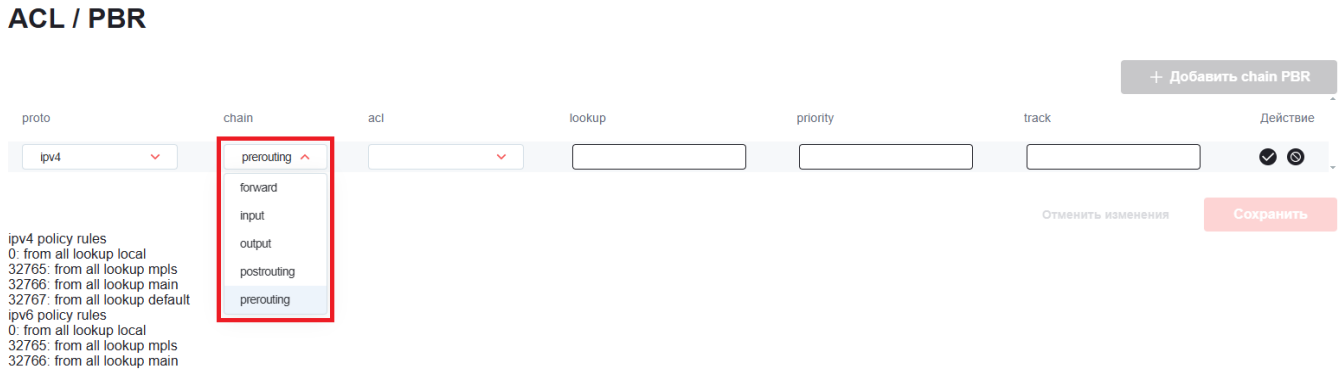


Рисунок 162 – Выбор типа пакетов

В столбце "acl" выберите один из списков контроля доступом, по которому будет осуществляться политика маршрутизации (рисунок 163).

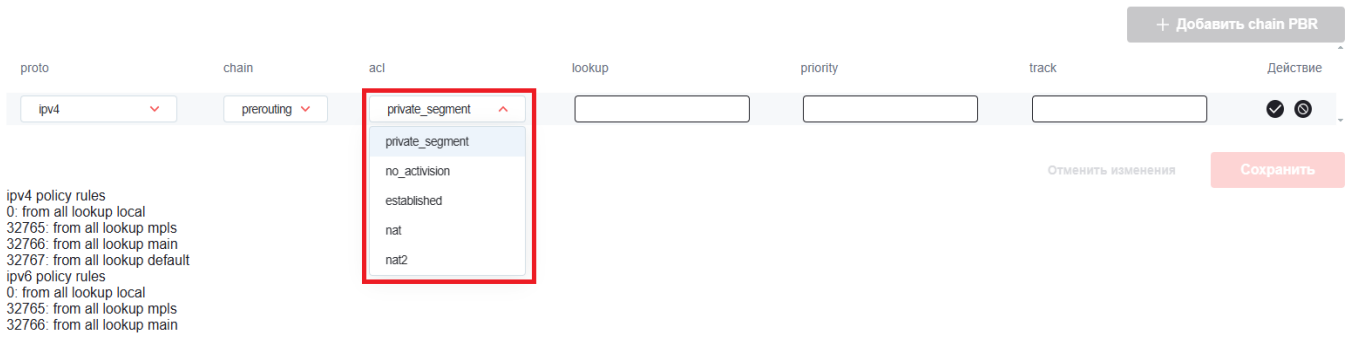


Рисунок 163 – Выбор списка контроля доступом

В столбце "lookup" введите id-номер таблице по которой будет осуществляться маршрутизация (рисунок 164).

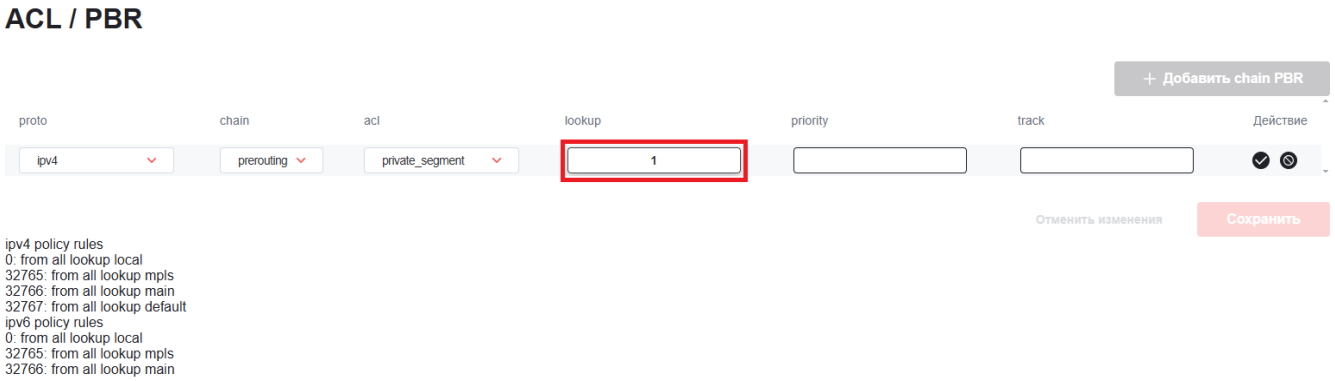


Рисунок 164 – Указание id-номера таблицы маршрутизации

В столбце "priority" укажите приоритет политики (чем значение приоритета меньше, тем раньше будет применено правило) (рисунок 165).

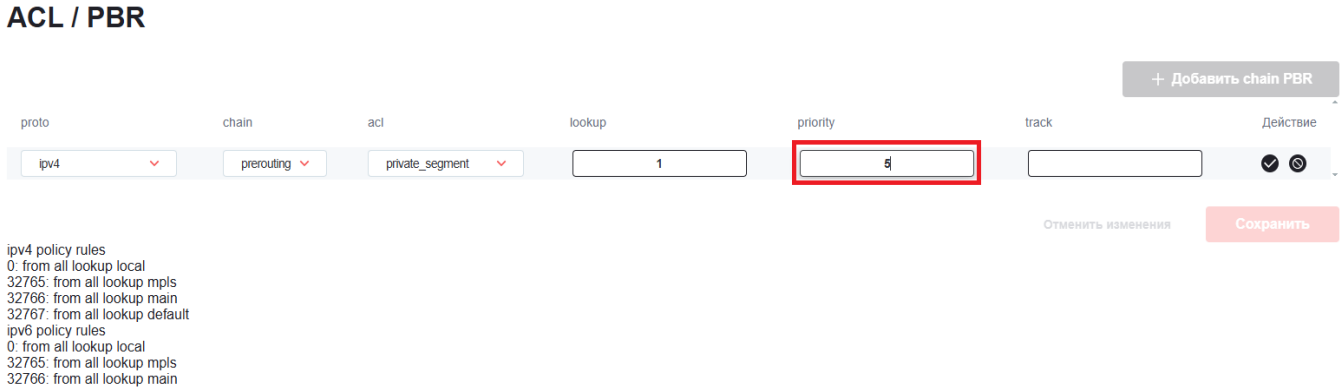


Рисунок 165 – Позиция ACL NAT

При необходимости укажите трекер IP SLA (рисунок 166).

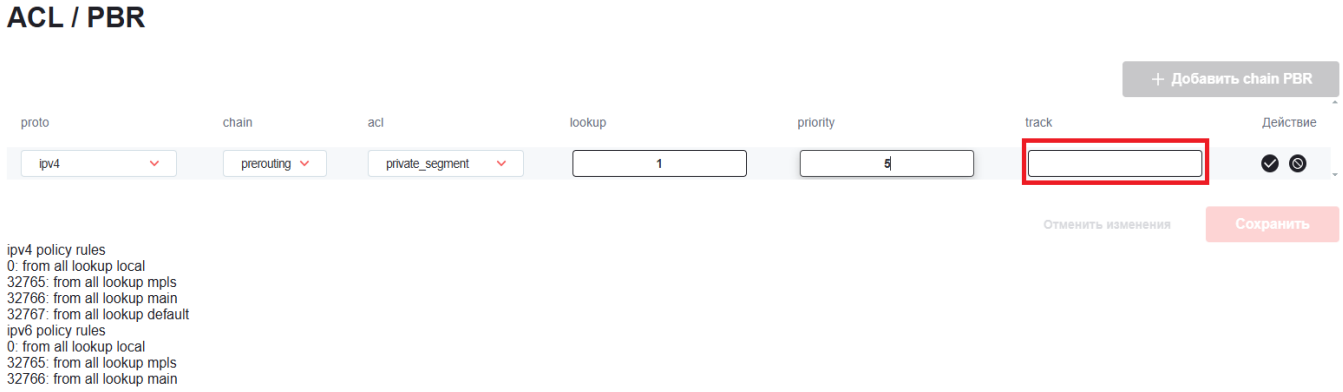


Рисунок 166 – Добавление порта

Для сохранения настроек необходимо сначала подтвердить изменения, нажав соответствующую пиктограмму в столбце "Действие" (рисунок 167).

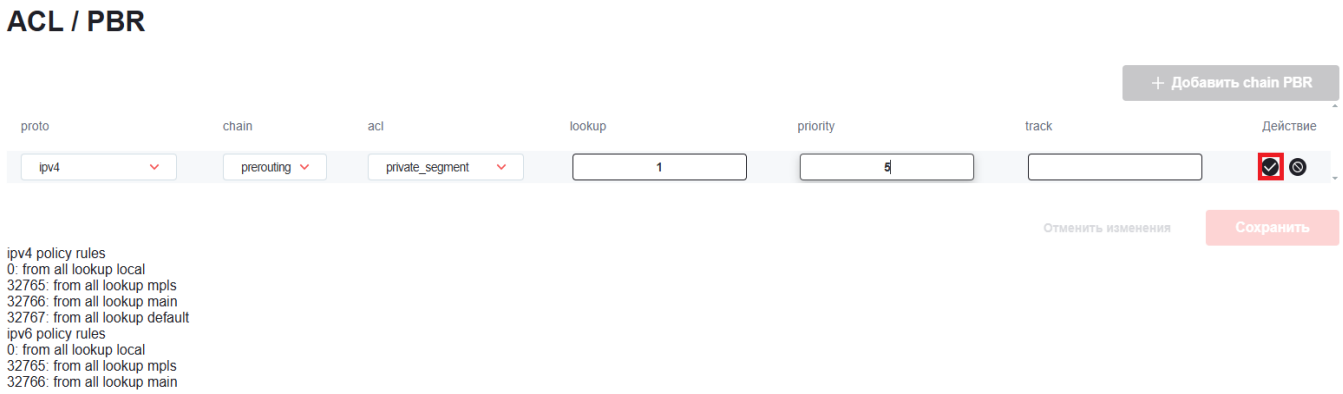


Рисунок 167 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 168).

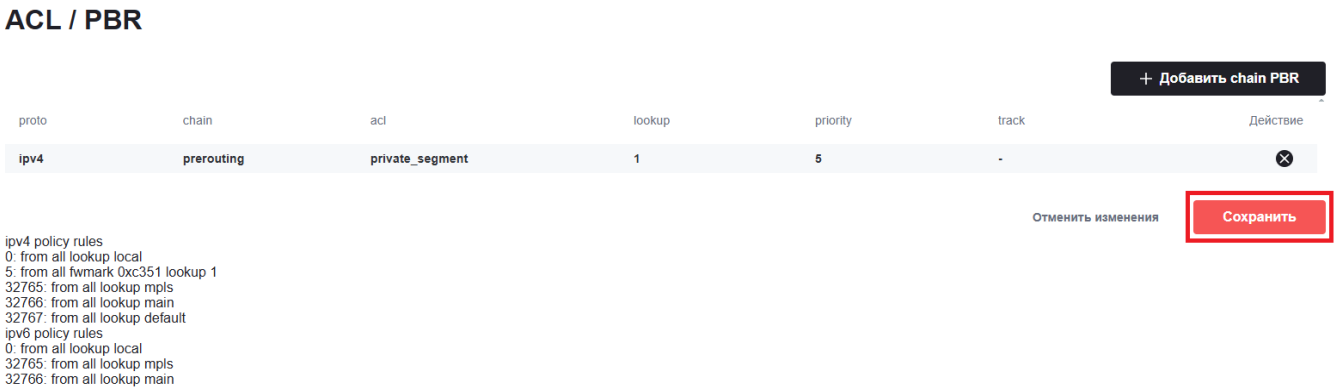


Рисунок 168 – Сохранение настроек

6.7 Примеры настроек

6.7.1 Настройка фильтрации на основе IP-адреса источника

В данном примере настройки будет показано как ограничить получение пакетов проходящих через сервисный маршрутизатор с помощью IP-адреса интерфейса источника.

Откройте вкладку "Настройка ACL" (рисунок 169).

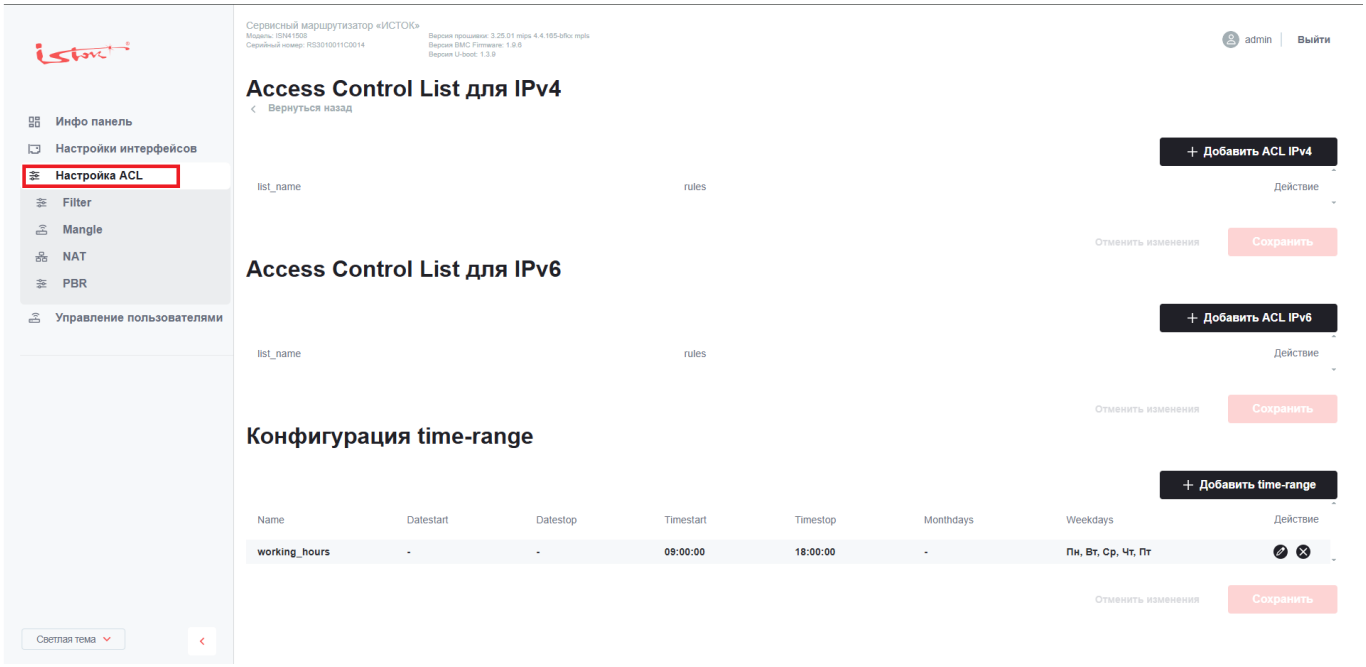


Рисунок 169 – Вкладка Настройки ACL

Нажмите кнопку "+Добавить ACL IPv4" (рисунок 170).

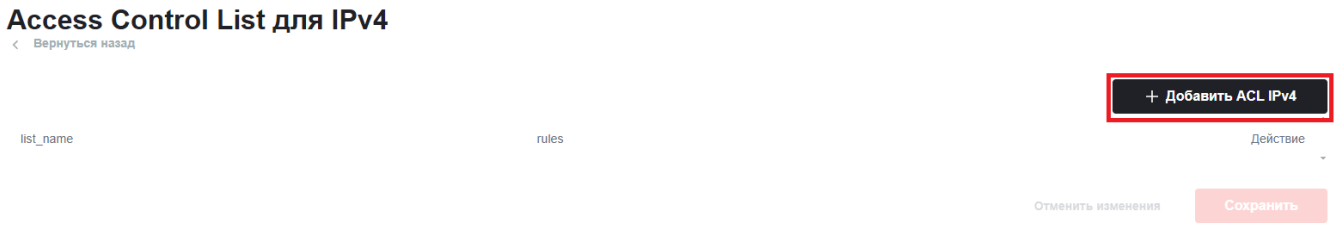


Рисунок 170 – Добавление списком управления доступом

В поле столбца "list_name" введите наименование листа без пробелов, наименование должно позволять пользователю безошибочно понимать набор правил в листе. В примере будет блокироваться трафик приходящий с определенного ip-адреса, поэтому составим наименование листа как "ip_router_a1". В поле столбца "rules" выберите из выпадающего списка правило "sourceip" (рисунок 171).

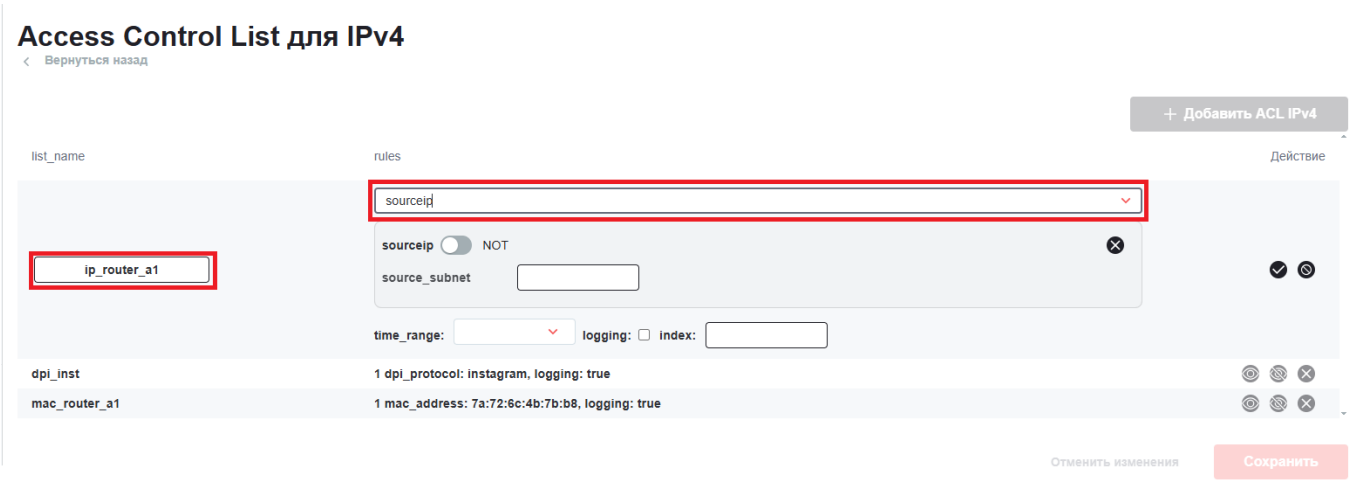


Рисунок 171 – Выбор правила

После добавления правила "sourceip" отобразится блок с настройками правила (рисунок 172).

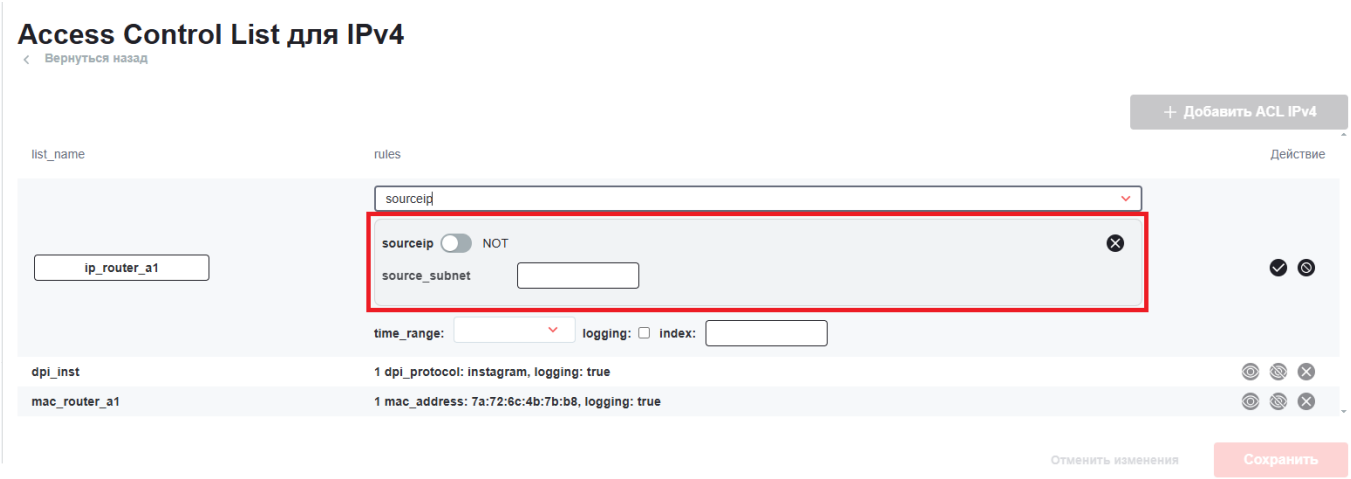


Рисунок 172 – Блок настройки правила

Впишите в поле "source_subnet" ip-адрес и маску интерфейса трафик с которого необходимо заблокировать (с помощью маски можно заблокировать как конкретный ip-адрес, так и группу ip-адресов, так и целую подсеть. В примере будет использован ip-адрес и маска "198.0.0.1/24") (рисунок 173).

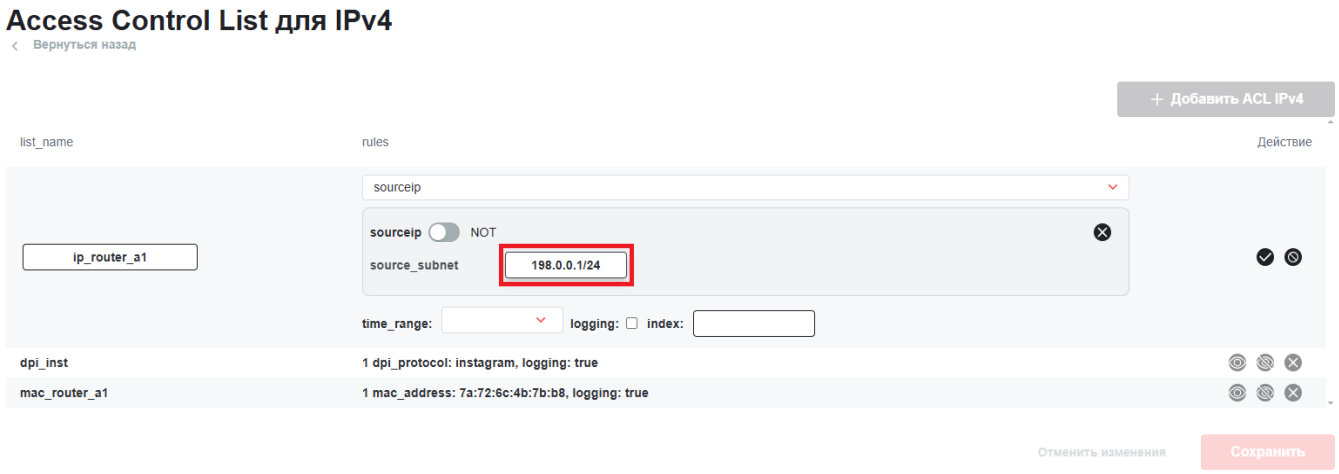


Рисунок 173 – Ввод IP-адреса

Примечание

Кнопка-переключатель "sourceip NOT" инвертирует правило, оставьте ее в выключенном состоянии

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 174).

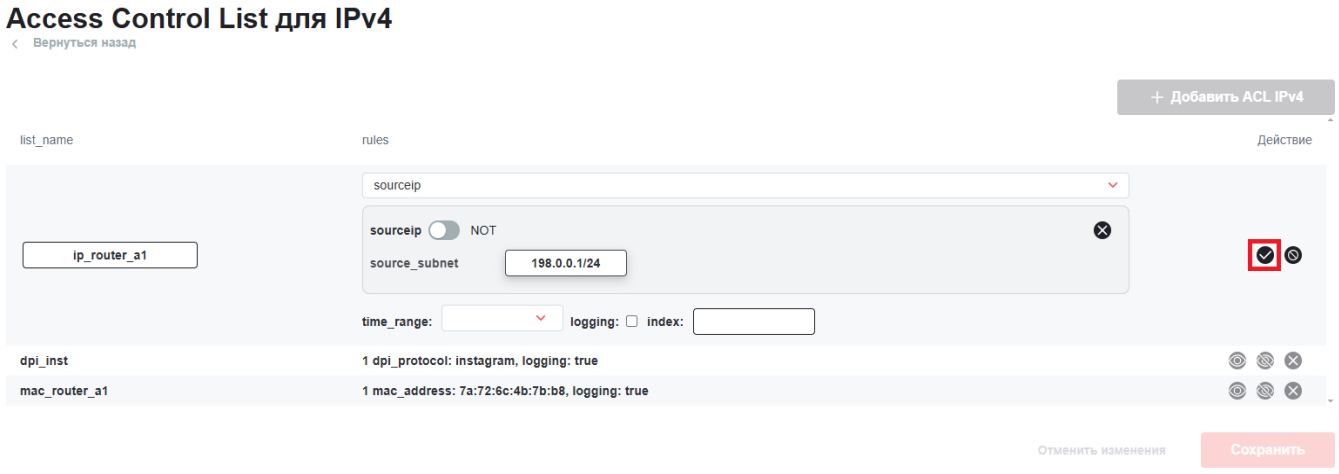


Рисунок 174 – Подтверждение создания списка

Включите отображение сообщения о срабатывания правила в логе выбрав в столбце "Действие" пиктограмму (рисунок 175).

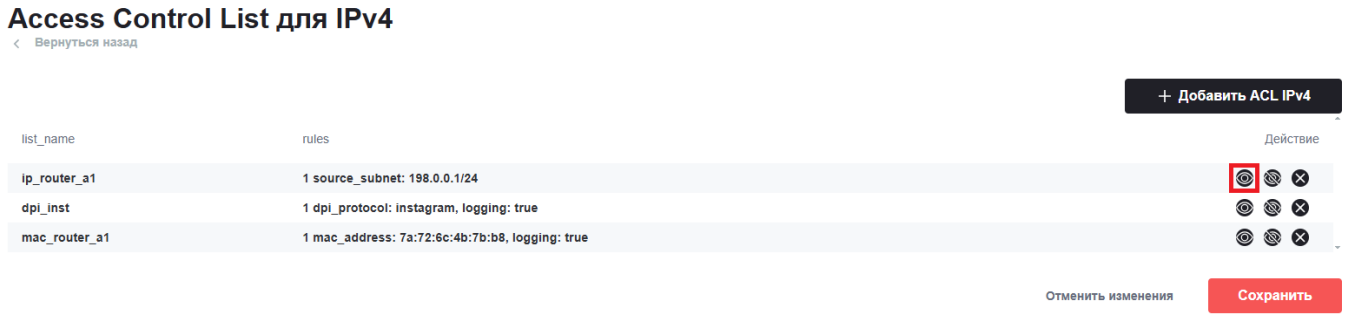


Рисунок 175 – Выбор занесения срабатывания правила в лог

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 176).

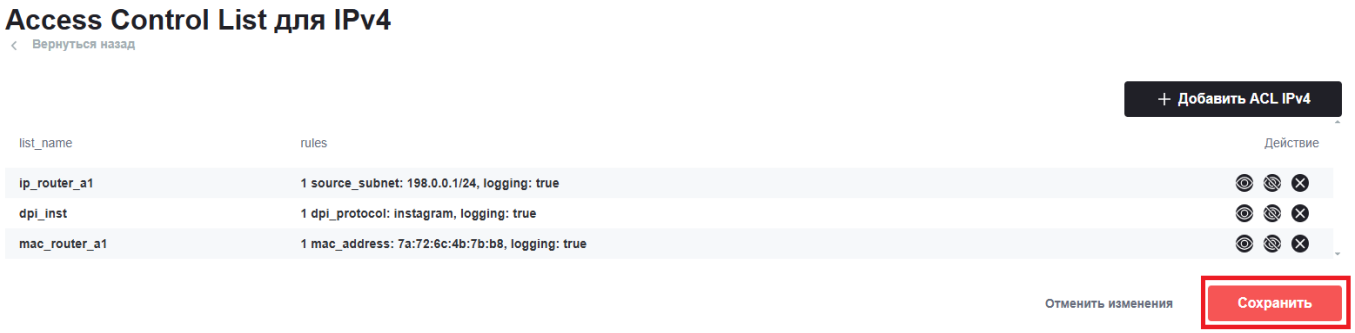


Рисунок 176 – Сохранение списка

Успешно добавленный лист контроля доступом будет иметь следующий вид (рисунок 177).

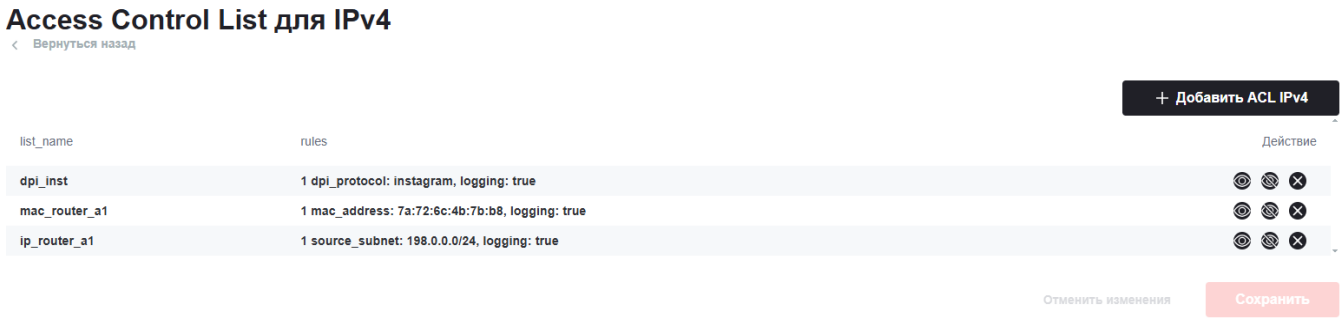


Рисунок 177 – Отображения листа контроля доступом

Для срабатывания правил листа контроля доступа необходимо добавить лист фильтру. Откройте вкладку "Filter" (рисунок 178).

Рисунок 178 – Вкладка Filter

Нажмите кнопку "+Добавить ACL Filter IPv4" (рисунок 179).

Рисунок 179 – Добавление фильтра

Настройте фильтр выполнив следующие действия (рисунок 180):

- в поле столбца "index" введите "1" (очередность срабатывания фильтров);
- в столбце "chain" выберите из выпадающего списка "forwatd" (тип пакета);
- в столбце "acl" выберите из выпадающего списка "ip_router_a1" (наименование созданного ACL);
- в столбце "action" выберите из выпадающего списка "deny" (отбрасывать пакеты).

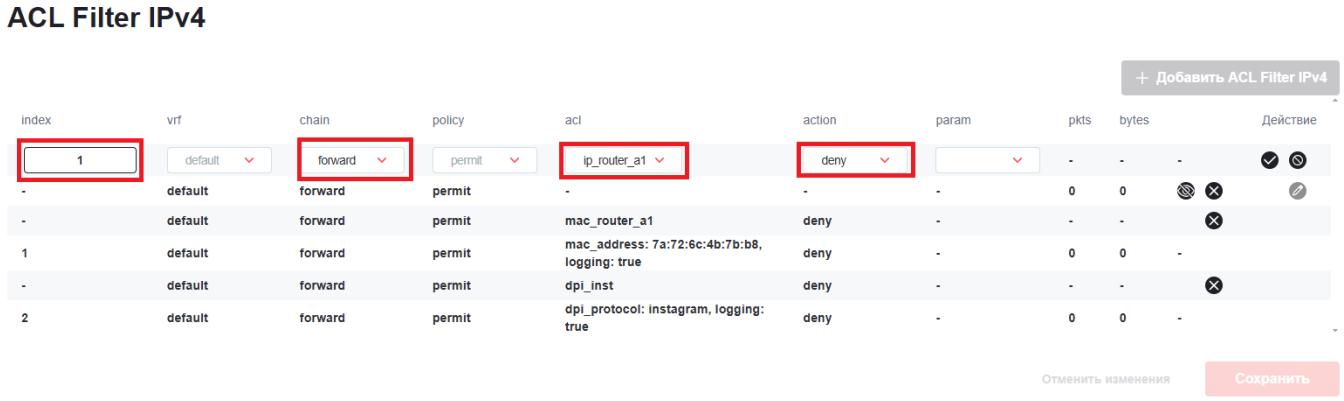


Рисунок 180 – Настройка фильтра

Подтвердите создание фильтра, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 181).

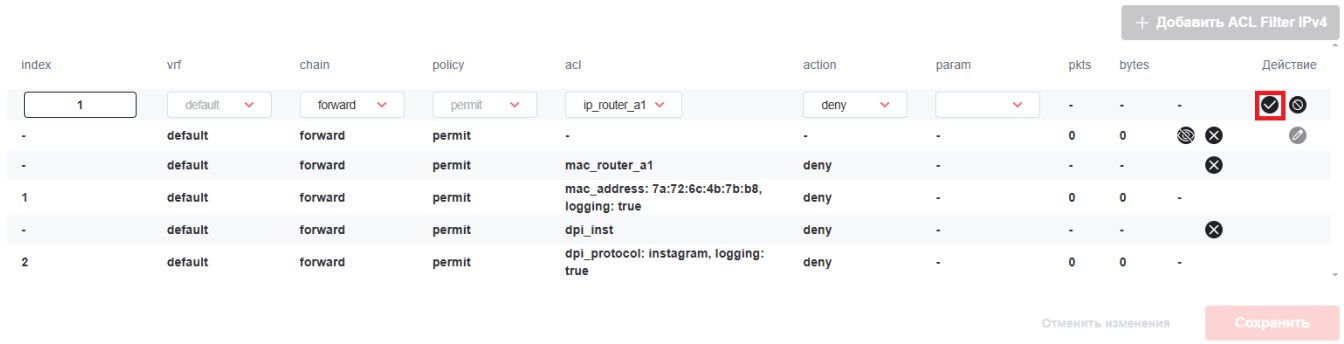


Рисунок 181 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 176).

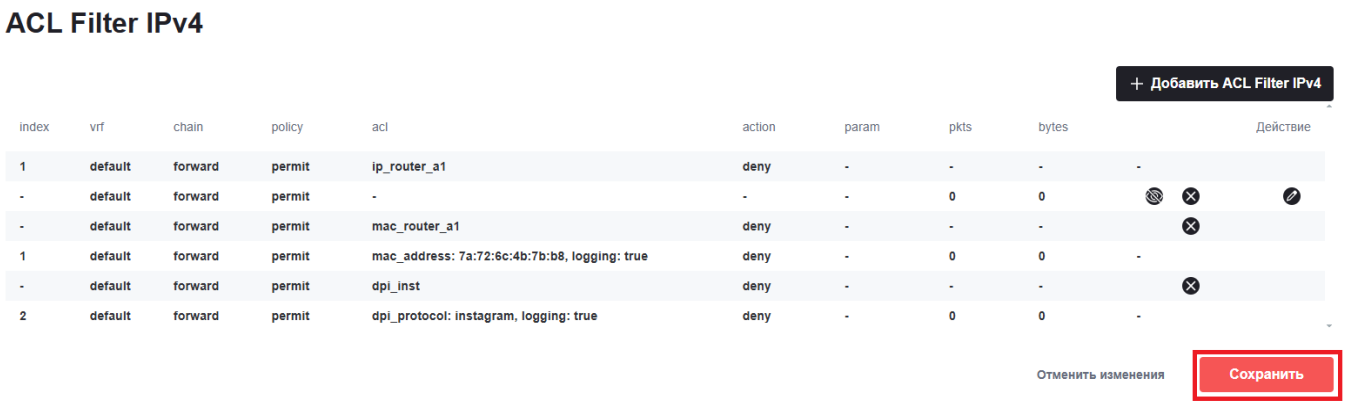


Рисунок 182 – Сохранение фильтра

Успешно добавленный фильтр будет иметь следующий вид (рисунок 183).

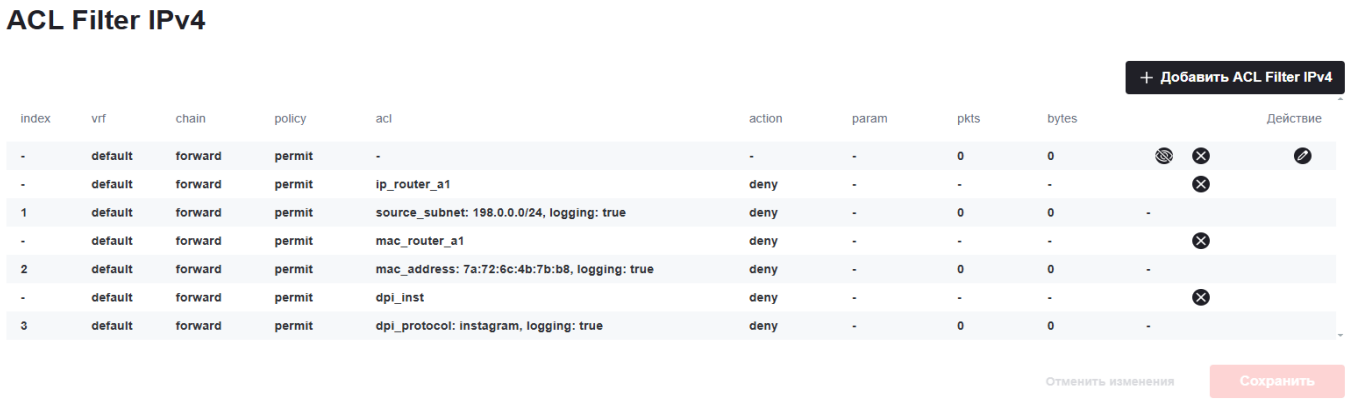


Рисунок 183 – Отображение фильтра

После этого настройка считается завершенной.

6.7.2 Настройка фильтрации на основе MAC-адреса отправителя

В данном примере настройки будет показано как ограничить получение пакетов проходящих через сервисный маршрутизатор с помощью MAC-адреса интерфейса отправителя.

Откройте вкладку "Настройка ACL" (рисунок 184).

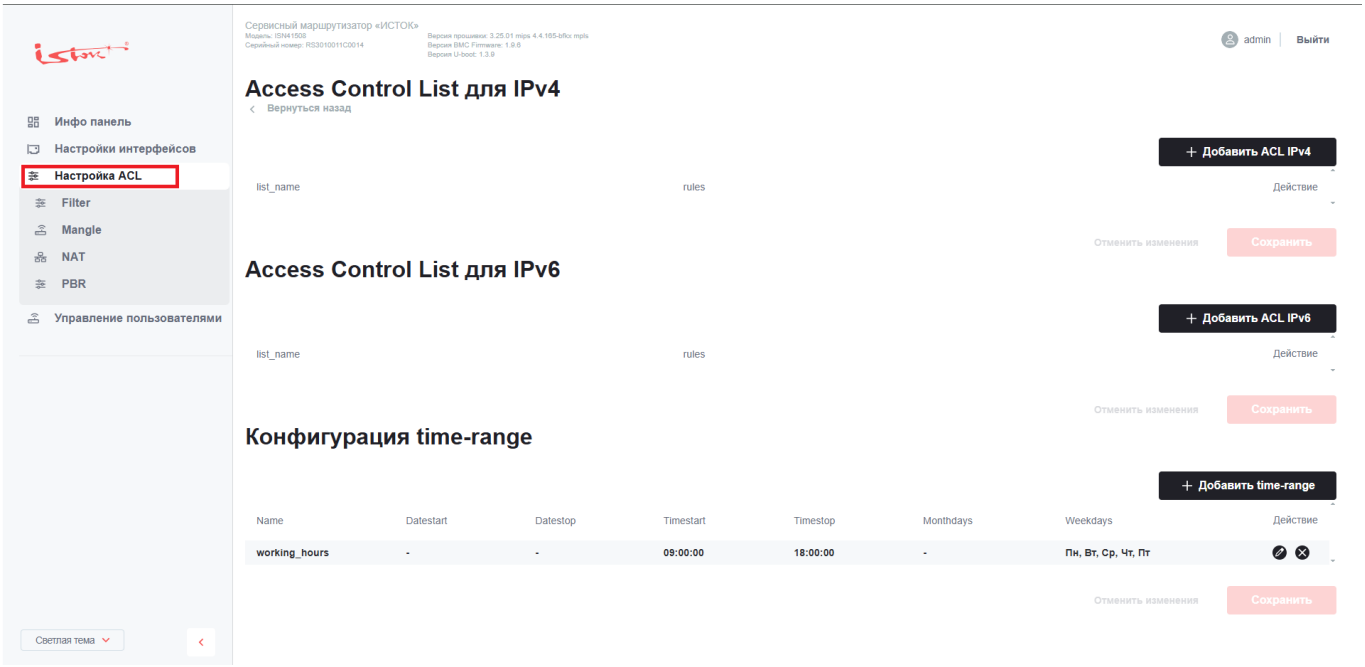


Рисунок 184 – Вкладка Настройки ACL

Нажмите кнопку "+Добавить ACL IPv4" (рисунок 185).

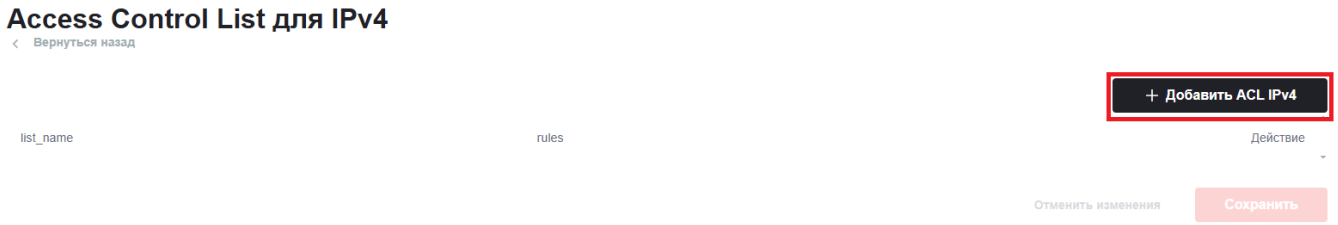


Рисунок 185 – Добавление списком управления доступом

В поле столбца "list_name" введите наименование листа без пробелов, наименование должно позволять пользователю безошибочно понимать набор правил в листе. В примере будет блокироваться трафик приходящий с определенного mac-адреса, поэтому составим наименование листа как "mac_router_a1". В поле столбца "rules" выберите из выпадающего списка правило "macsource" (рисунок 186).

Рисунок 186 – Выбор правила

После добавления правила "macsource" отобразится блок с настройками правила (рисунок 187).

Рисунок 187 – Блок настройки правила

Впишите в поле "mac_address" mac-адрес интерфейса трафик с которого необходимо заблокировать (в примере будет использован mac-адрес "7a:72:6c:4b:7b:b8") (рисунок 188).

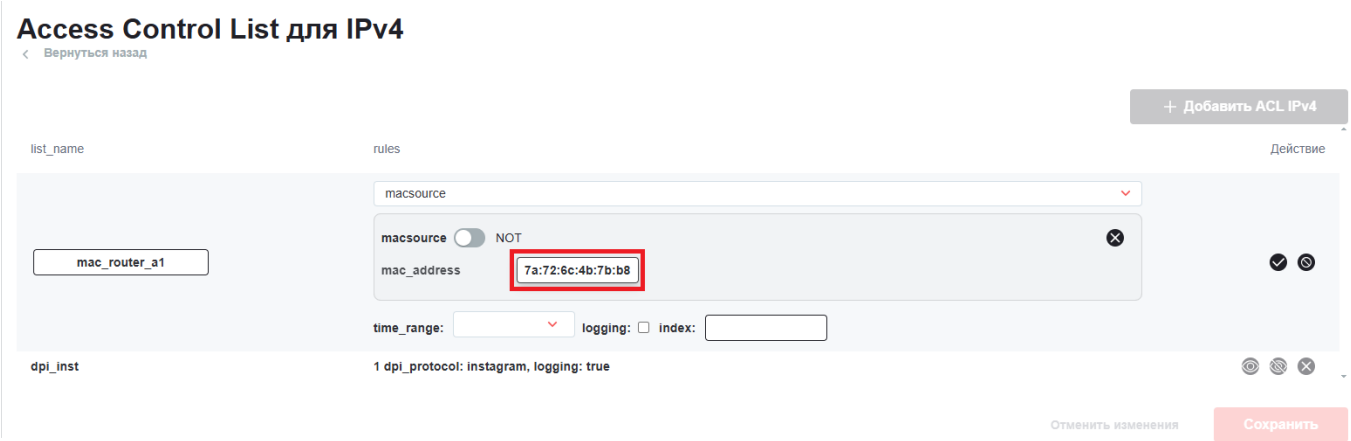


Рисунок 188 – Ввод mac-адреса

Примечание

Кнопка-переключатель "macsource NOT" инвертирует правило, оставьте ее в выключенном состоянии

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 189).

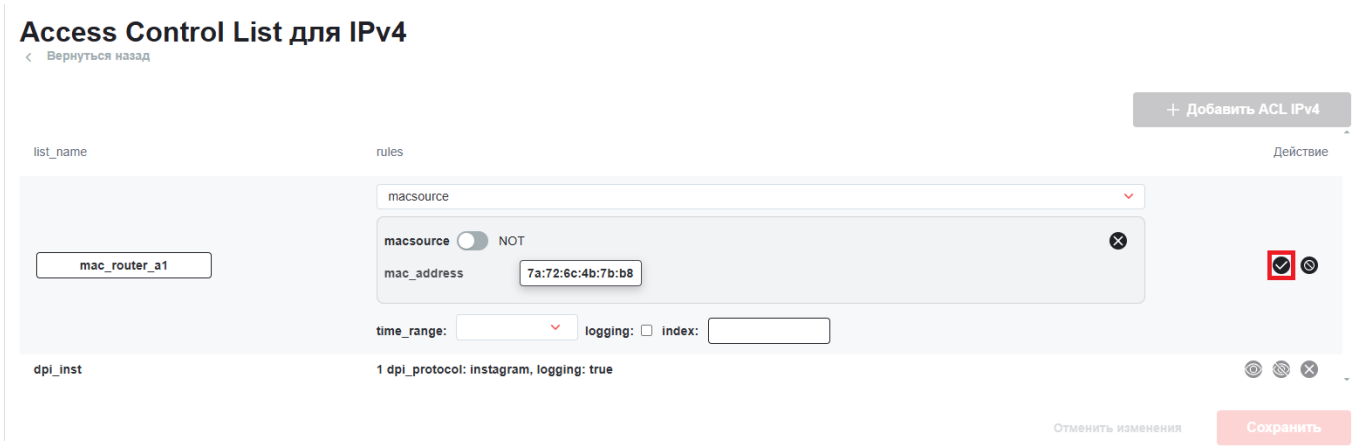


Рисунок 189 – Подтверждение создания списка

Включите отображение сообщения о срабатывания правила в логе выбрав в столбце "Действие" пиктограмму (рисунок 190).

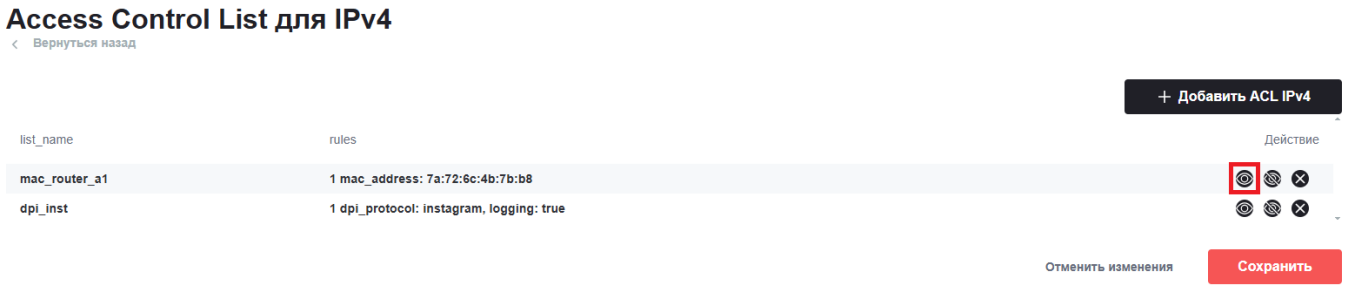


Рисунок 190 – Выбор занесения срабатывания правила в лог

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 191).

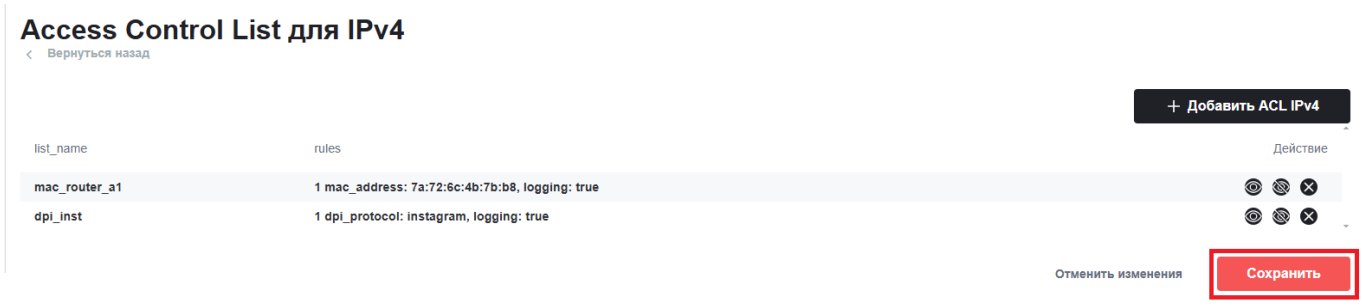


Рисунок 191 – Сохранение списка

Успешно добавленный лист контроля доступом будет иметь следующий вид (рисунок 192).

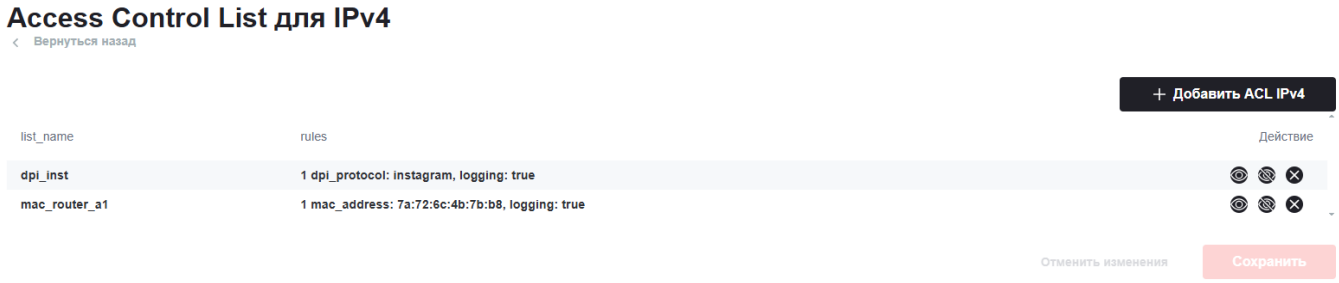


Рисунок 192 – Отображения листа контроля доступом

Для срабатывания правил листа контроля доступа необходимо добавить лист фильтру. Откройте вкладку "Filter" (рисунок 193).

Рисунок 193 – Вкладка Filter

Нажмите кнопку "+Добавить ACL Filter IPv4" (рисунок 194).

Рисунок 194 – Добавление фильтра

Настройте фильтр выполнив следующие действия (рисунок 195):

- в поле столбца "index" введите "1" (очередность срабатывания фильтров);

- в столбце "chain" выберите из выпадающего списка "forwatd" (тип пакета);
- в столбце "acl" выберите из выпадающего списка "mac_router_a1" (наименование созданного ACL);
- в столбце "action" выберите из выпадающего списка "deny" (отбрасывать пакеты).

Рисунок 195 – Настройка фильтра

Подтвердите создание фильтра, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 196).

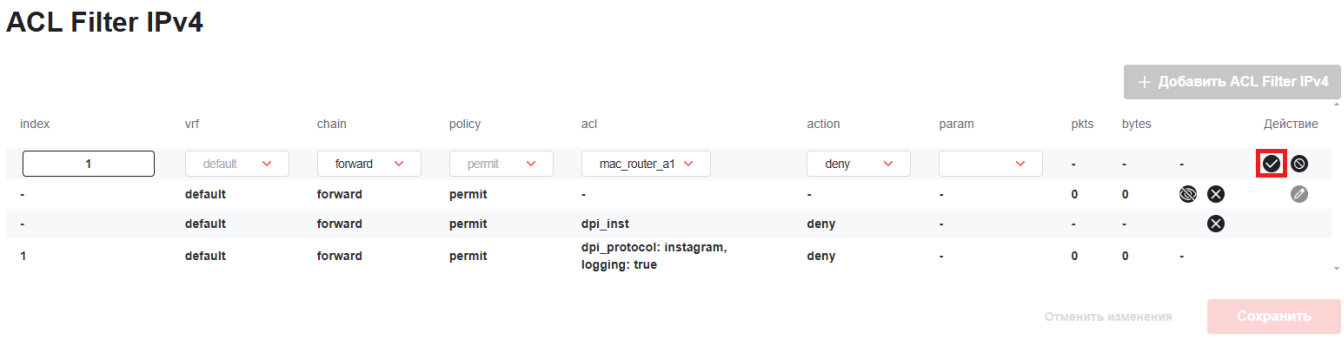


Рисунок 196 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 191).

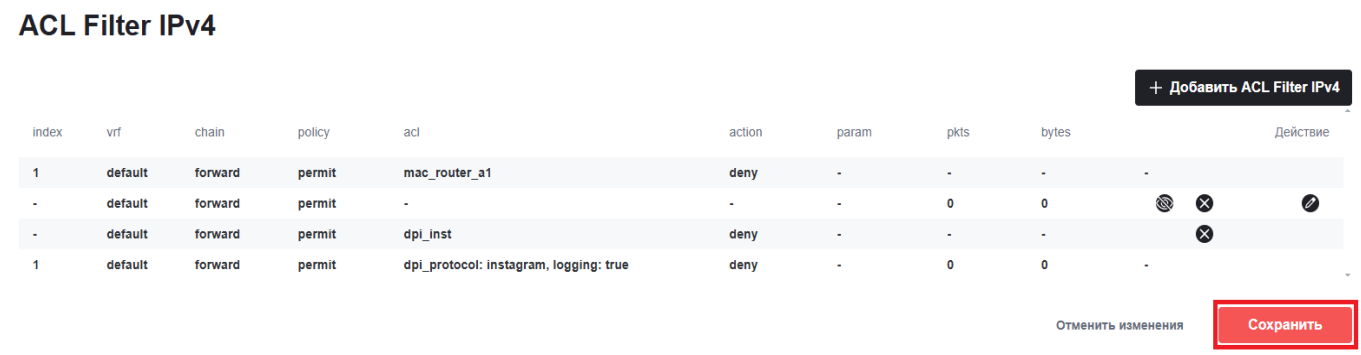


Рисунок 197 – Сохранение фильтра

Успешно добавленный фильтр будет иметь следующий вид (рисунок 198).

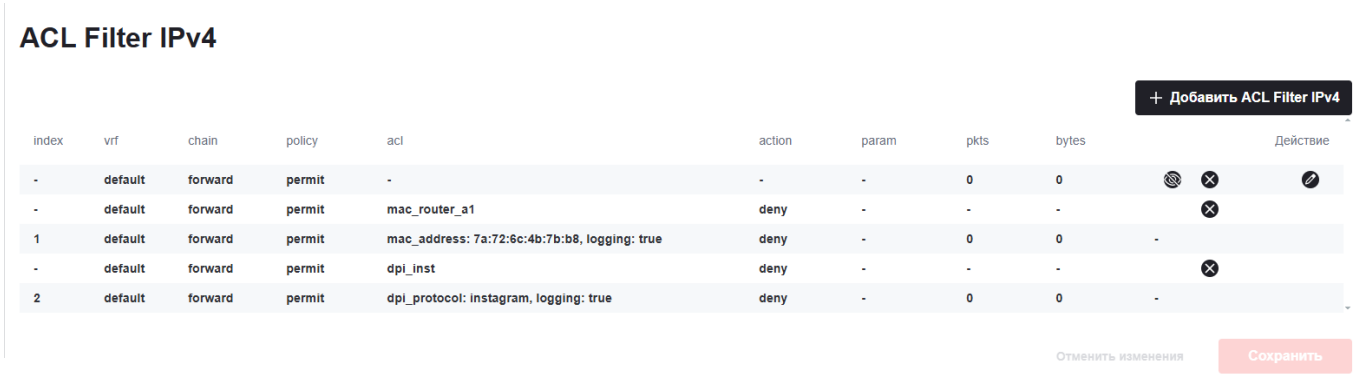


Рисунок 198 – Отображение фильтра

После этого настройка считается завершенной.

6.7.3 Настройка фильтрации по DPI

В данном примере настройки будет показано как ограничить получение пакетов от сайта/приложения instagram проходящих через сервисный маршрутизатор с помощью DPI.

Откройте вкладку "Настройка ACL" (рисунок 199).

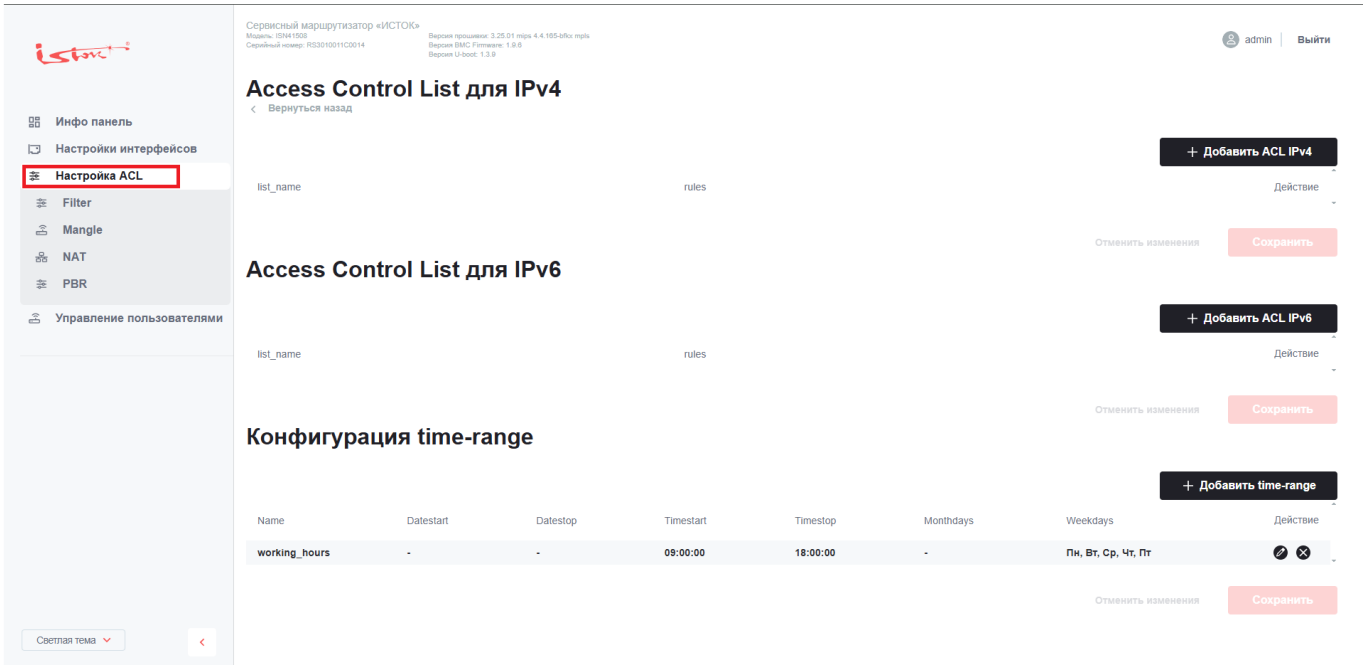


Рисунок 199 – Вкладка Настройки ACL

Нажмите кнопку "+Добавить ACL IPv4" (рисунок 200).

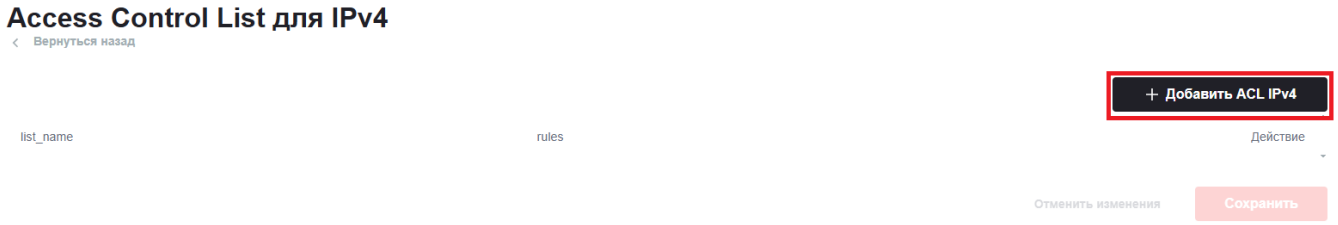


Рисунок 200 – Добавление списком управления доступом

В поле столбца "list_name" введите наименование листа без пробелов, наименование должно позволять пользователю безошибочно понимать набор правил в листе. В примере будет блокироваться трафик сайта/приложения instagramm, поэтому составим наименование листа как "dpi_inst". В поле столбца "rules" выберите из выпадающего списка правило "dpi" (рисунок 201).

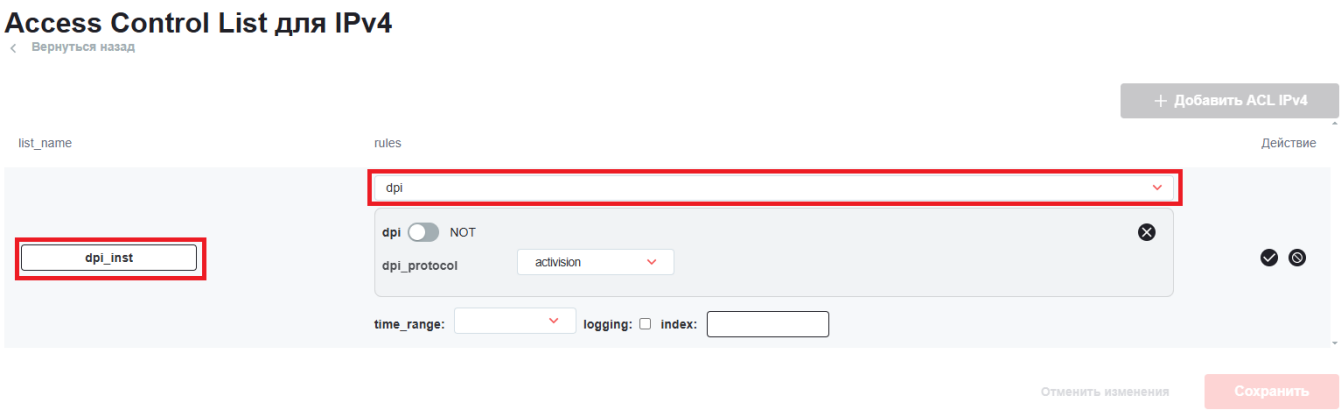


Рисунок 201 – Выбор правила

После добавления правила "dpi" отобразится блок с настройками правила (рисунок 202).

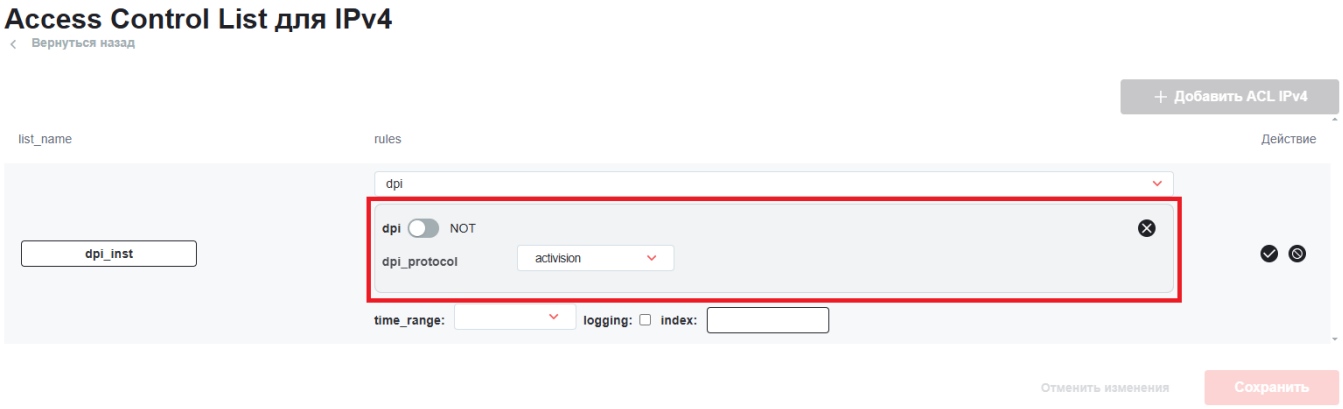


Рисунок 202 – Блок настройки правила

Из выпадающего списка поля "dpi_protocol" выберите пакеты сайта/приложения "instagramm" (рисунок 203).

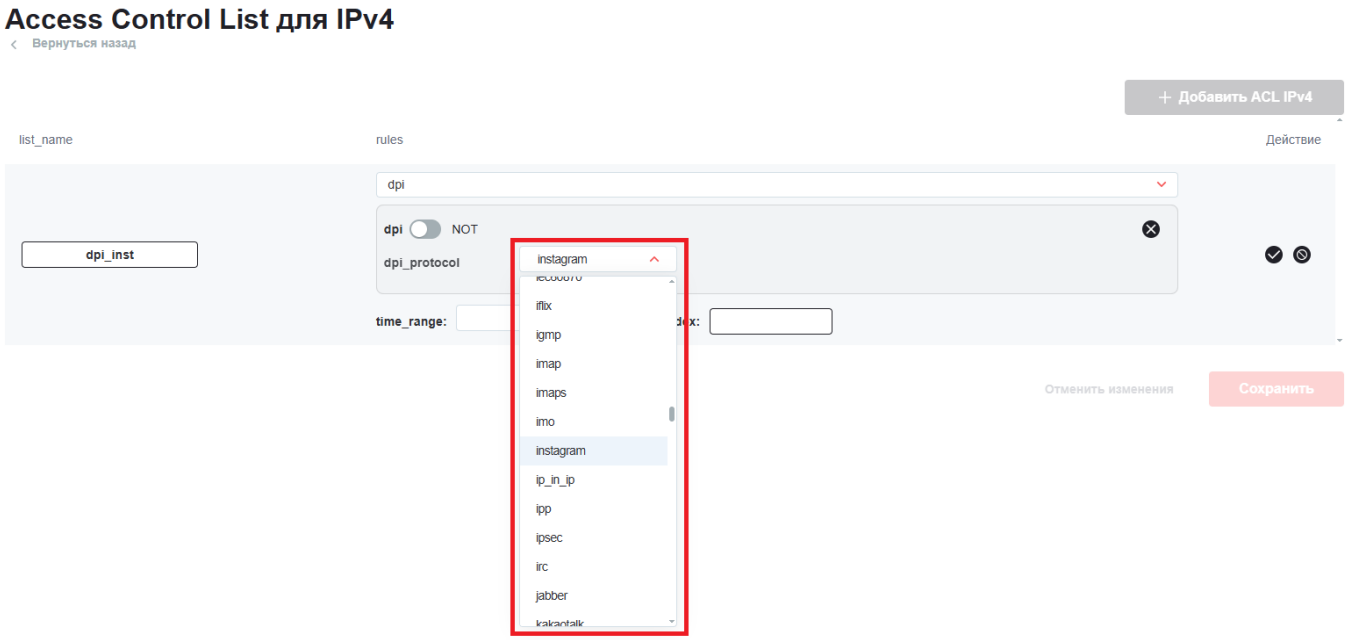


Рисунок 203 – Выбор сайта/приложения

Примечание

Кнопка-переключатель "dpi NOT" инвертирует правило, оставьте ее в выключенном состоянии

Подтвердите создание списка управления доступом, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 204).

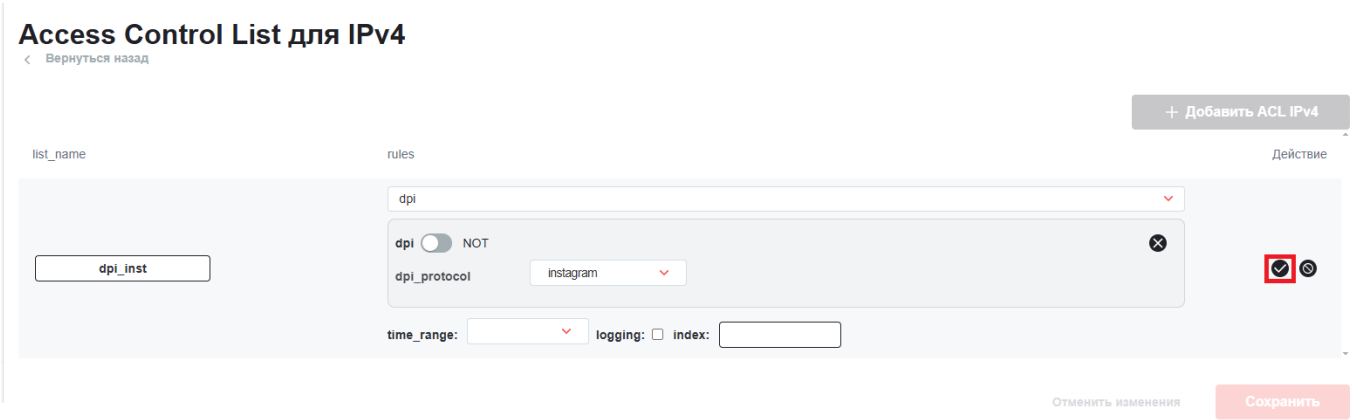


Рисунок 204 – Подтверждение создания списка

Включите отображение сообщения о срабатывания правила в логе выбрав в столбце "Действие" пиктограмму (рисунок 205).

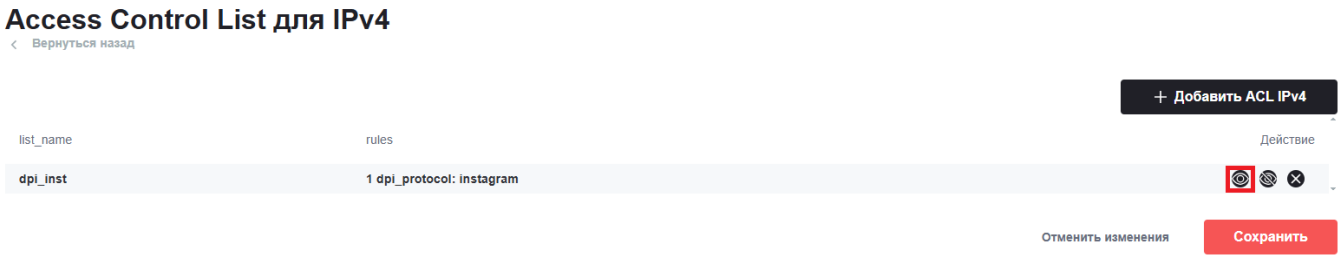


Рисунок 205 – Выбор занесения срабатывания правила в лог

Сохраните список управления доступом, нажав кнопку "Сохранить" (рисунок 206).

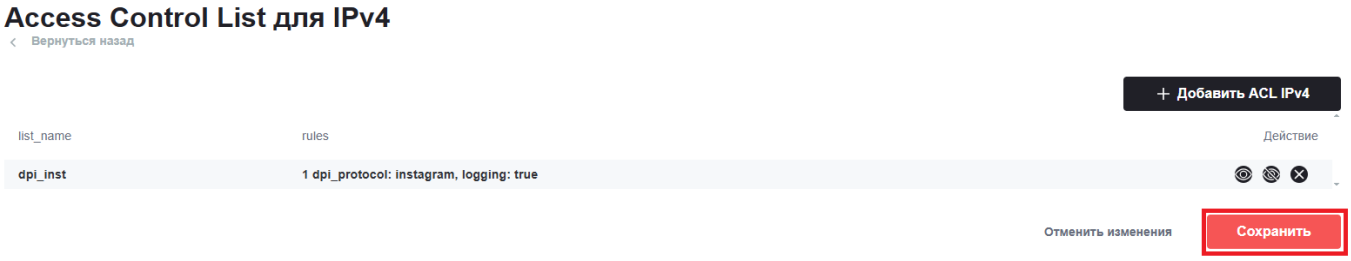


Рисунок 206 – Сохранение списка

Успешно добавленный лист контроля доступом будет иметь следующий вид (рисунок 207).

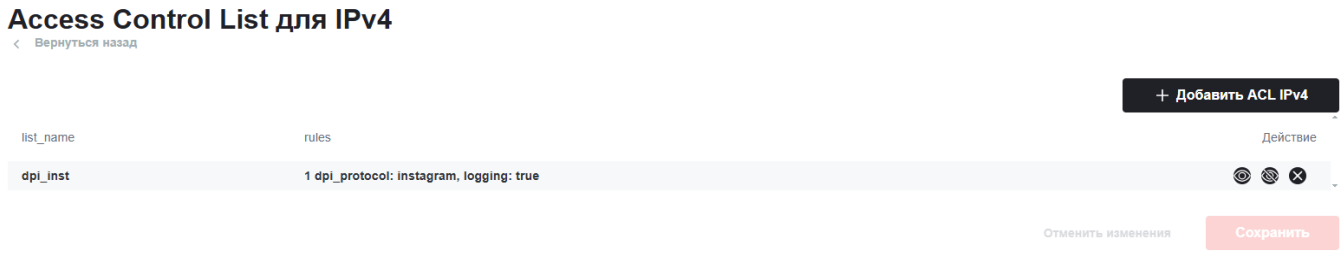


Рисунок 207 – Отображения листа контроля доступом

Для срабатывания правил листа контроля доступа необходимо добавить лист фильтру. Откройте вкладку "Filter" (рисунок 208).

Рисунок 208 – Вкладка Filter

Нажмите кнопку "+Добавить ACL Filter IPv4" (рисунок 209).

Рисунок 209 – Добавление фильтра

Настройте фильтр выполнив следующие действия (рисунок 210):

- в поле столбца "index" введите "1" (очередность срабатывания фильтров);
- в столбце "chain" выберите из выпадающего списка "forward" (тип пакета);
- в столбце "acl" выберите из выпадающего списка "dpi_inst" (наименование созданного ACL);
- в столбце "action" выберите из выпадающего списка "deny" (отбрасывать пакеты).

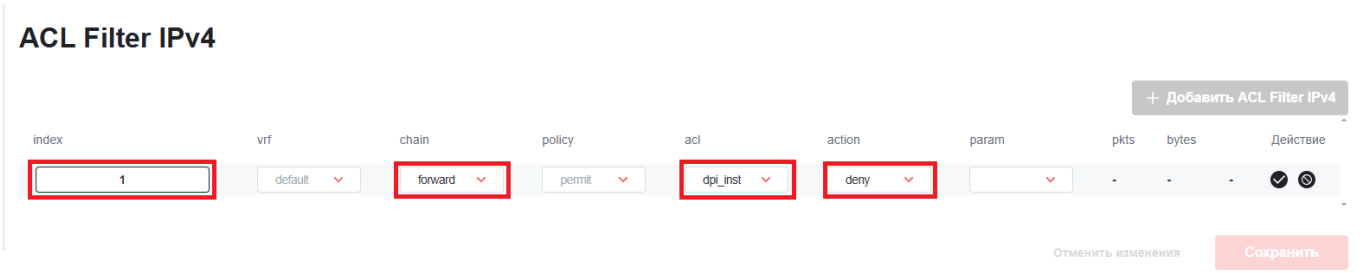


Рисунок 210 – Настройка фильтра

Подтвердите создание фильтра, нажав на пиктограмму "Подтвердить" в столбце "Действие" (рисунок 211).

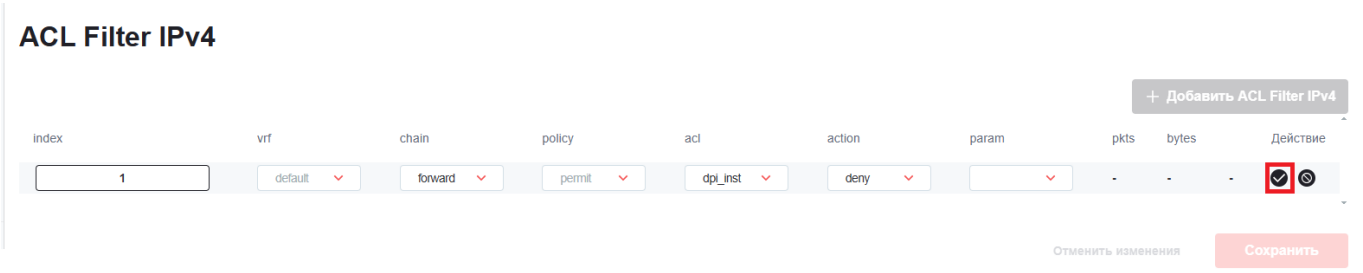


Рисунок 211 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 212).

Рисунок 212 – Сохранение фильтра

Успешно добавленный фильтр будет иметь следующий вид (рисунок 213).

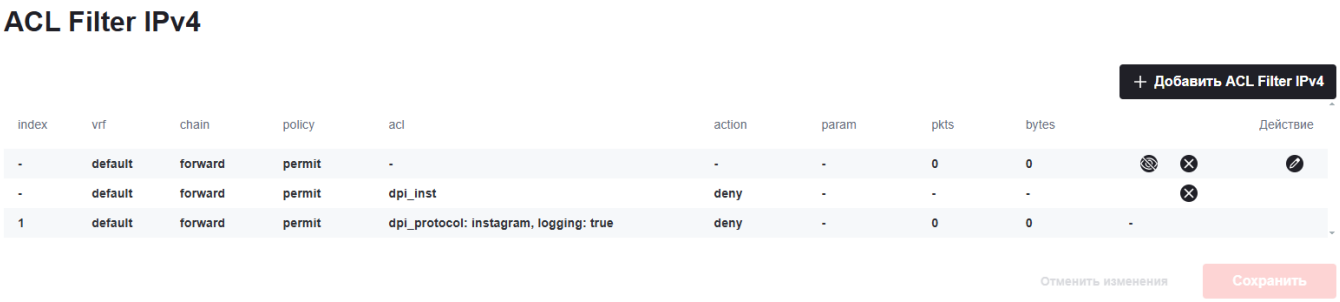


Рисунок 213 – Отображение фильтра

После этого настройка считается завершенной.

7 Управление пользователями

В данном окне предусмотрена возможность добавления, редактирования, удаления пользователей и групп (рисунок 214).

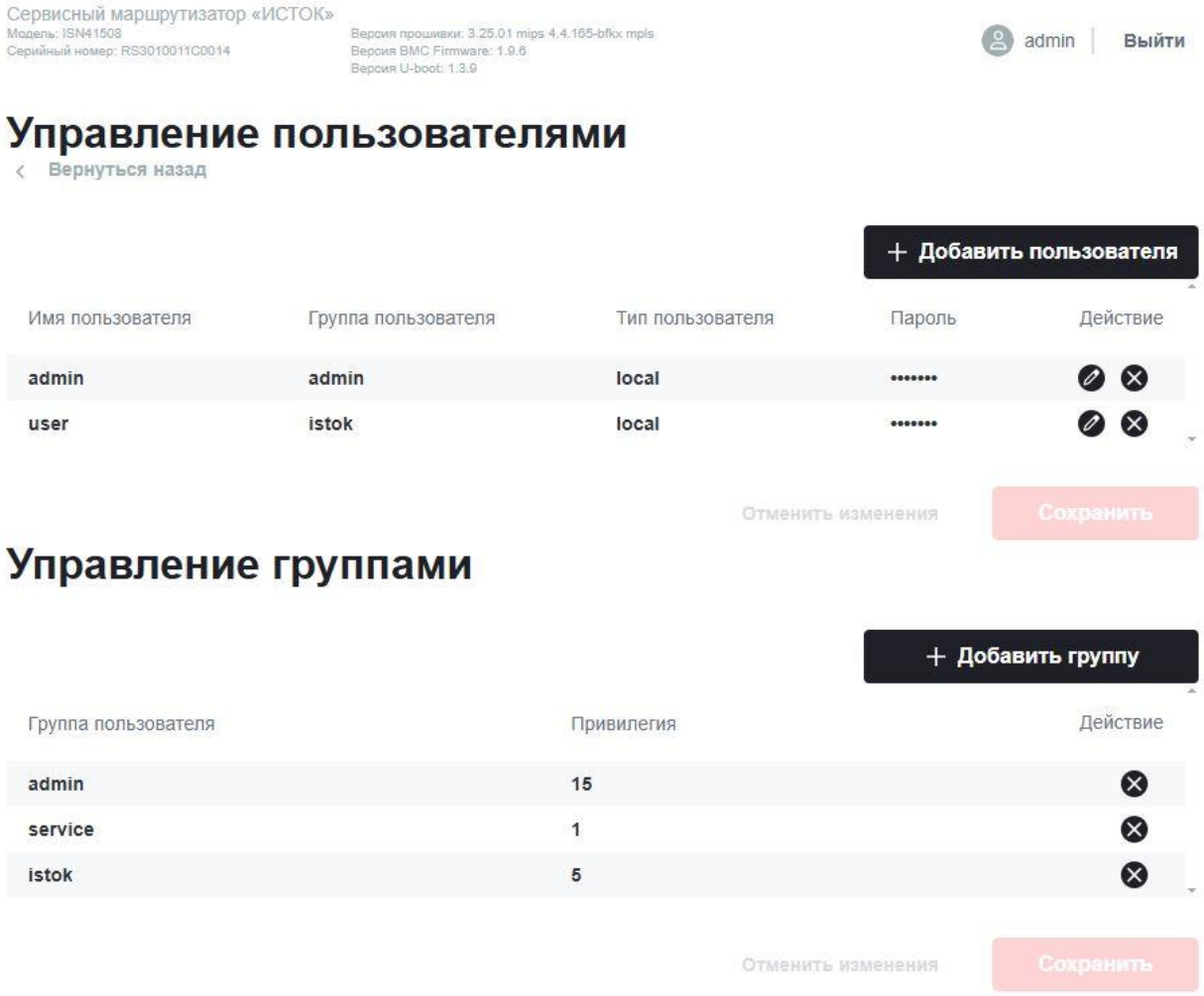


Рисунок 214 – Управление пользователями и группами

7.1 Управление пользователями

Для добавления нового пользователя нажмите на клавишу "Добавить пользователя" (рисунок 215).

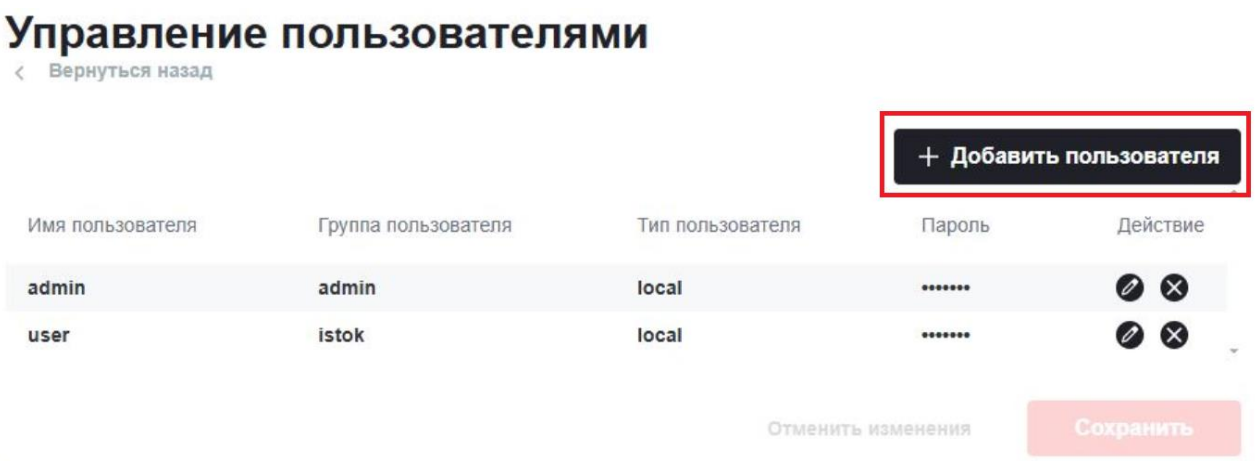


Рисунок 215 – Добавление пользователя

В соответствующем поле введите имя нового пользователя (рисунок 216).

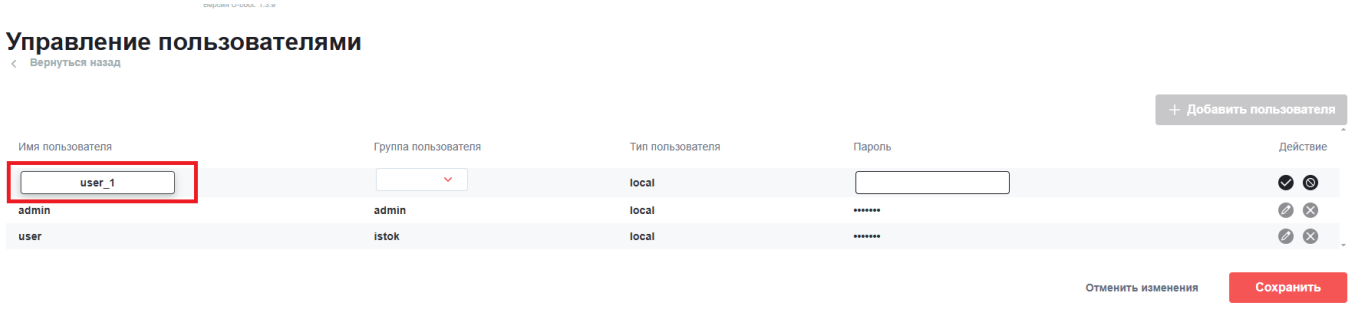


Рисунок 216 – Имя пользователя

В столбце "Группа пользователя" нажмите на стрелку вниз и выберите необходимую группу из выпадающего списка: admin, istok, service (рисунок 217).

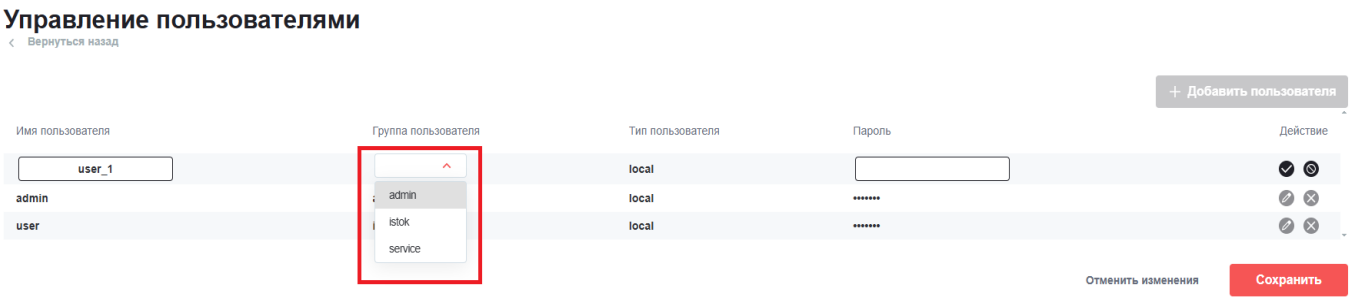


Рисунок 217 – Группа пользователя

Тип пользователя по умолчанию установлен как "local" (рисунок 218).

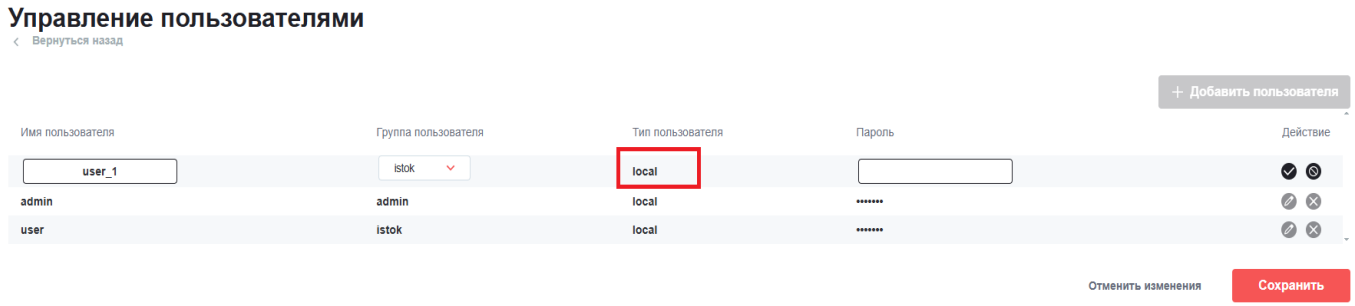


Рисунок 218 – Тип пользователя

В столбце "Пароль" задайте пароль для нового пользователя. Обратите внимание, что пароль должен содержать не менее 9 символов и включать как минимум одну цифру и одну букву (рисунок 219).

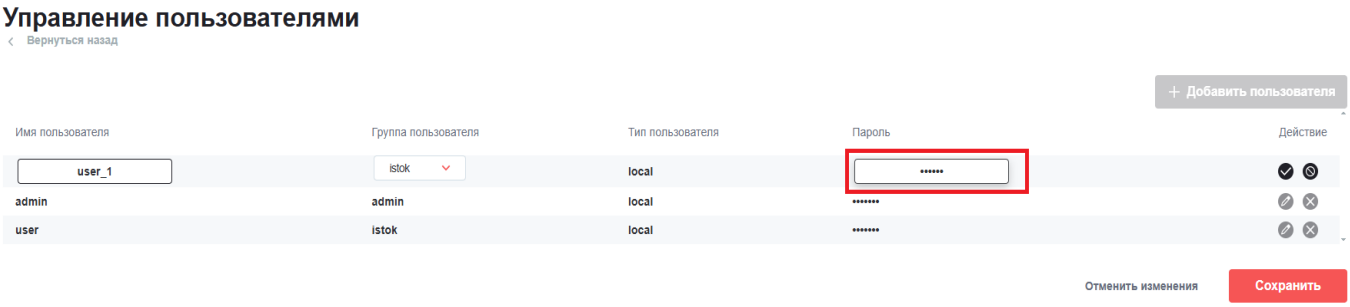


Рисунок 219 – Установка пароля

В столбце "Действие" нажмите на пиктограмму "Подтвердить" (рисунок 220).

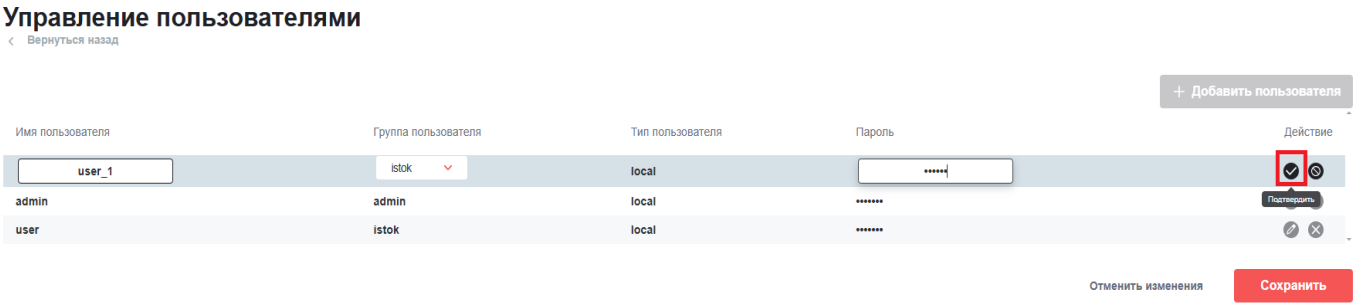


Рисунок 220 – Подтверждение действия

Если необходимо отменить создание пользователя до его сохранения в системе, используйте пиктограмму "Отменить", расположенную в столбце "Действие" (рисунок 221) или нажмите на клавишу "Отменить изменения" (рисунок 222).

Рисунок 221 – Пиктограмма "Отменить"

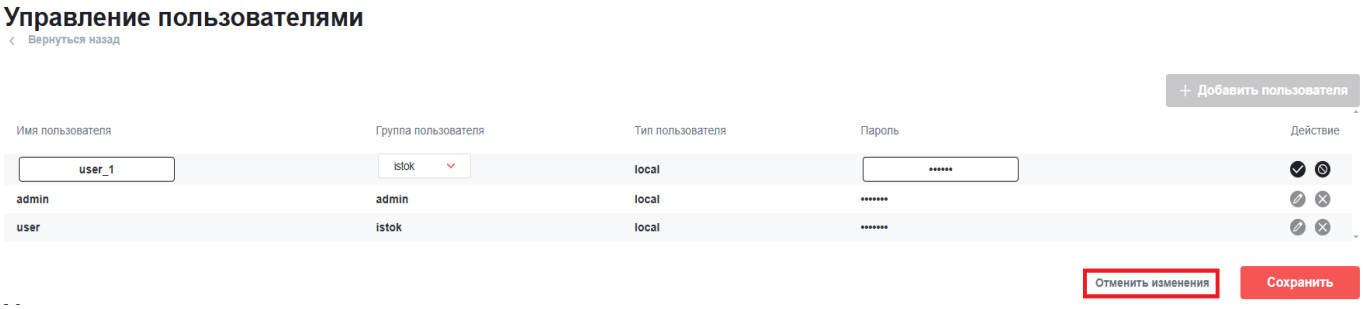


Рисунок 222 – Отмена изменений

Если Вы не хотите отменять процесс создания пользователя, то нажмите клавишу "Сохранить" (рисунок 223).

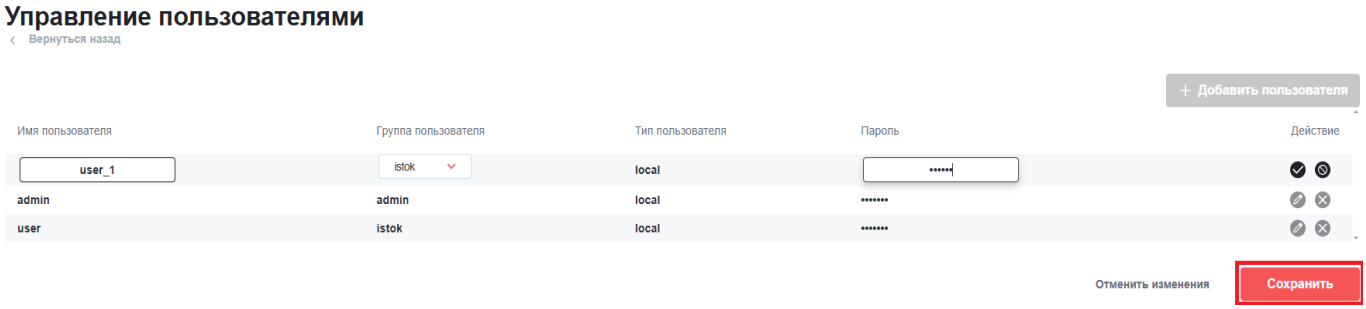


Рисунок 223 – Сохранение пользователя

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 224).

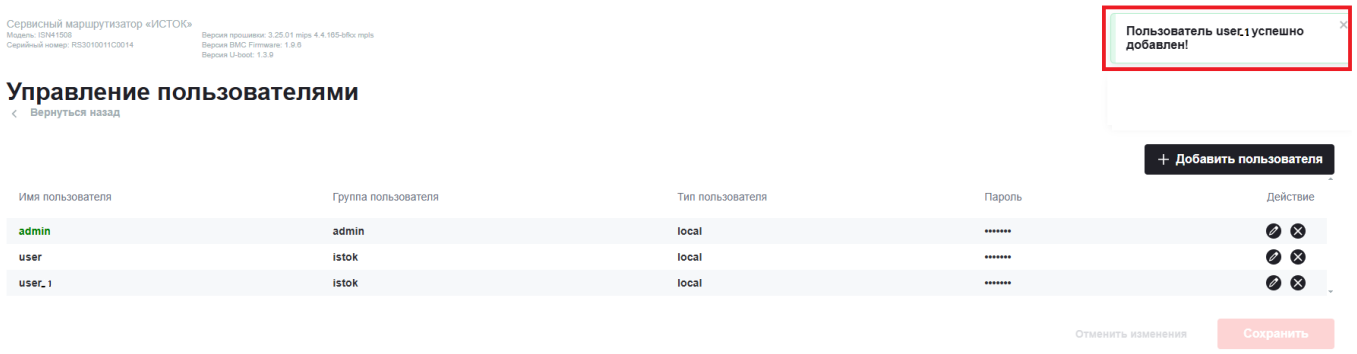


Рисунок 224 – Уведомляющее окно

Для удаления пользователя нажмите на пиктограмму "Удалить", расположенную в столбце "Действие" (рисунок 225).

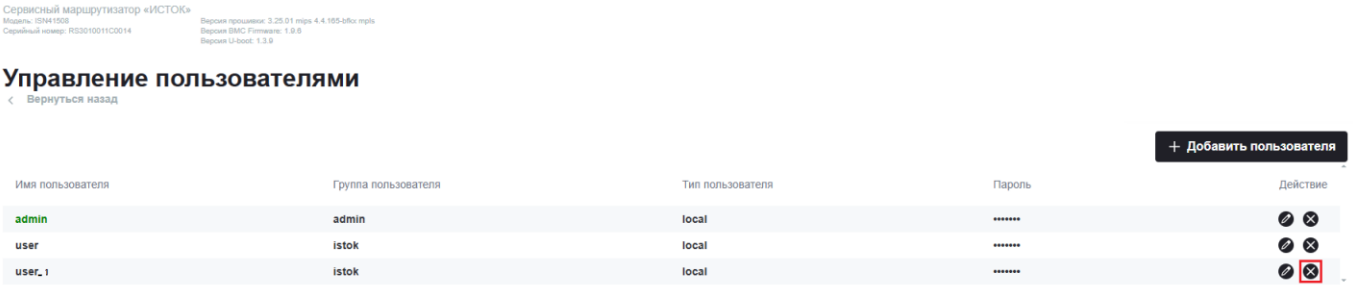


Рисунок 225 – Удаление пользователя

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 226).

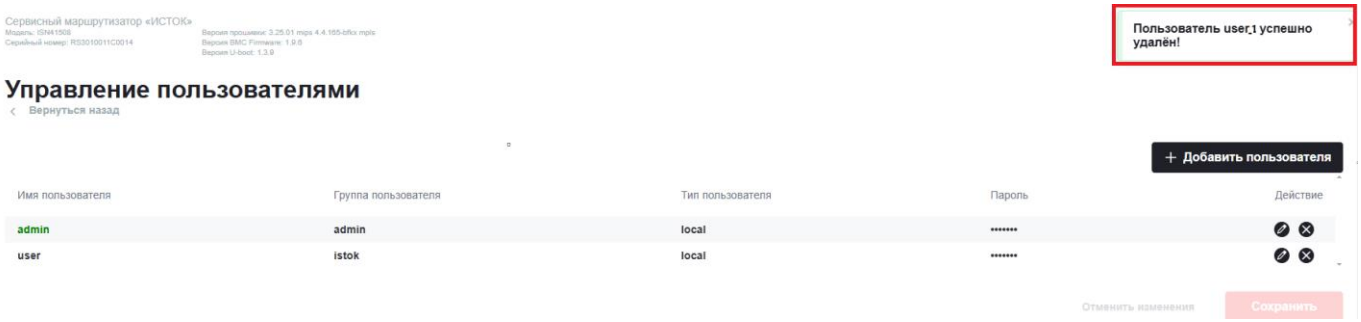


Рисунок 226 – Уведомляющее окно

7.2 Управление группами

Для добавления группы нажмите на клавишу "Добавить группу" (рисунок 227).

Рисунок 227 – Добавление группы

В соответствующем поле введите название новой группы (рисунок 228).

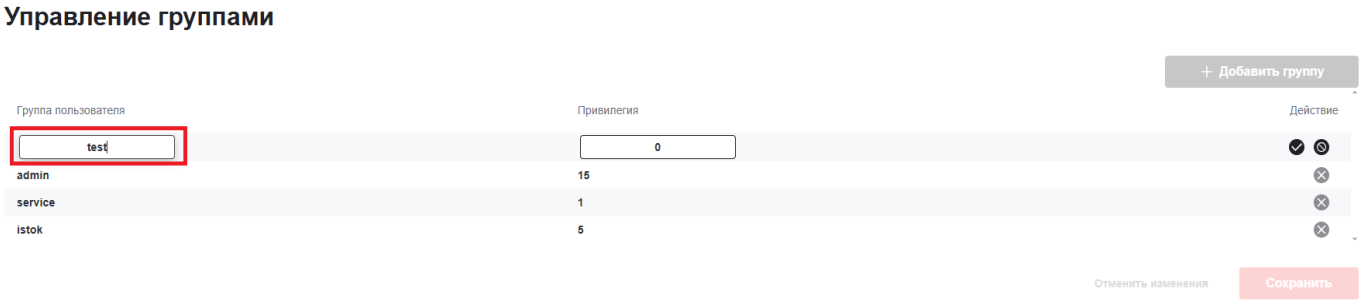


Рисунок 228 – Ввод названия группы

В столбце "Привилегия" введите номер привилегий к которому будет относится данная группа (рисунок 229).

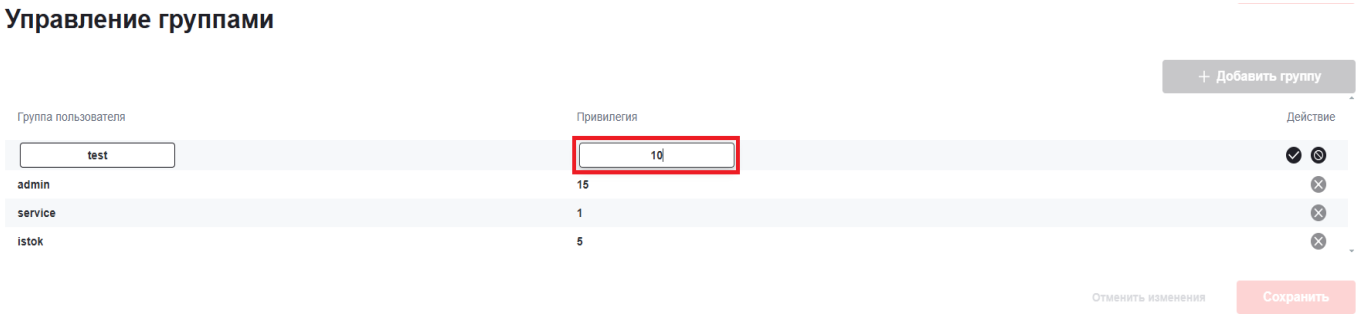


Рисунок 229 – Установка привелегии группы

В столбце "Действие" нажмите на пиктограмму "Подтвердить" (рисунок 230).

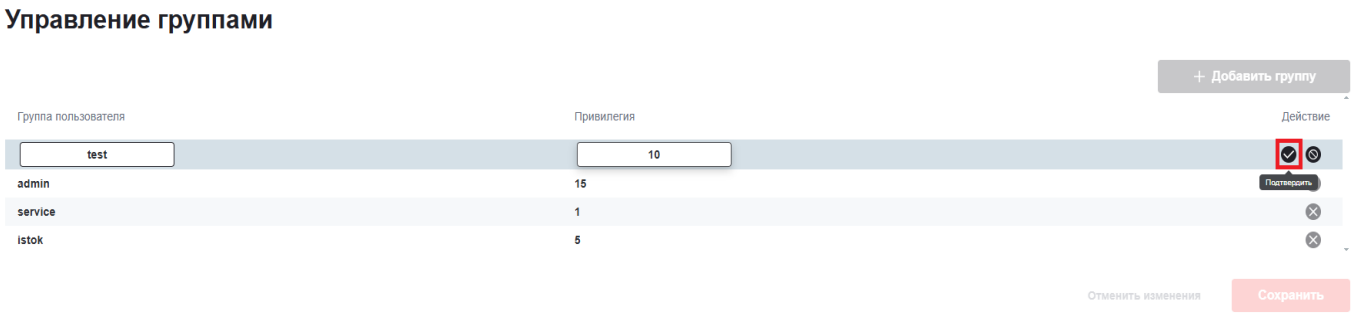


Рисунок 230 – Подтверждение действия

Если необходимо отменить создание группы до его сохранения в системе, используйте пиктограмму "Отменить", расположенную в столбце "Действие" (рисунок 231) или нажмите на клавишу "Отменить изменения" (рисунок 232).

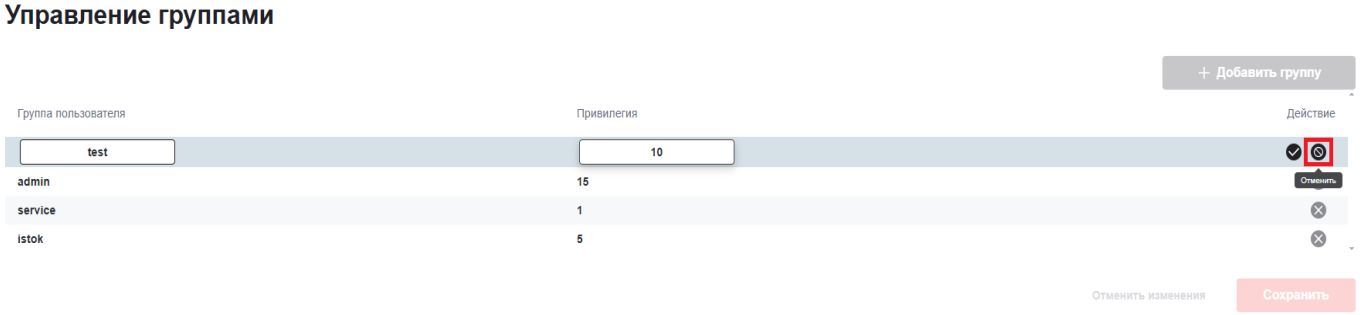


Рисунок 231 – Отмена действия

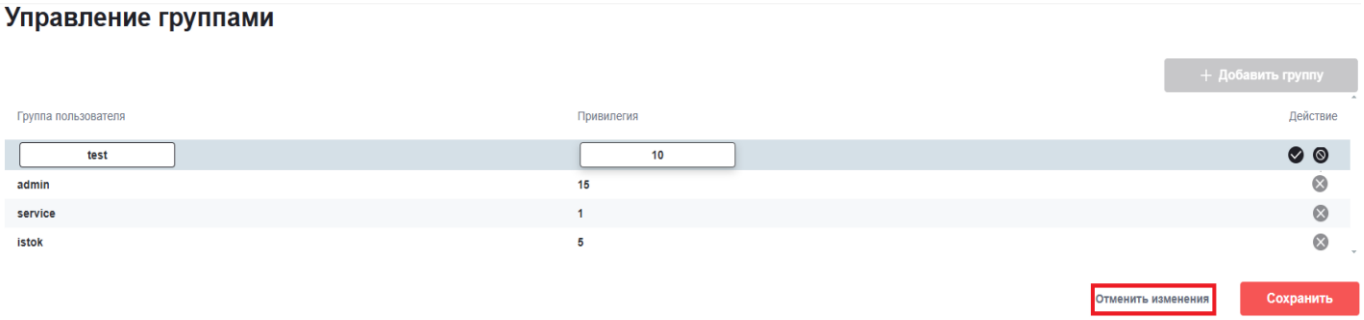


Рисунок 232 – Отмена изменений

Если Вы не хотите отменять процесс создания группы, то нажмите клавишу "Сохранить" (рисунок 233).

Рисунок 233 – Сохранение группы

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 234).

Рисунок 234 – Уведомляющее окно

Для удаления группы нажмите на пиктограмму "Удалить", расположенную в столбце "Действие" (рисунок 235).

Рисунок 235 – Удаление группы

В случае успешного сохранения появится соответствующее уведомление в правом верхнем углу экрана (рисунок 236).

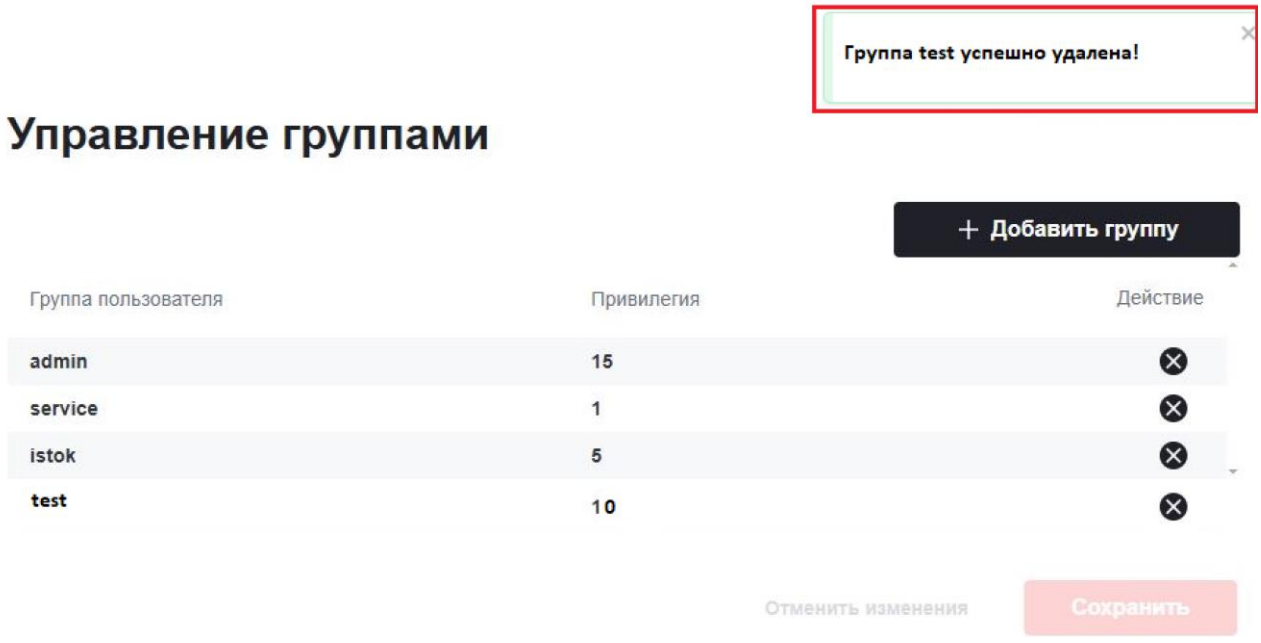


Рисунок 236 – Уведомляющее окно

Техническая поддержка

Официальный сайт компании: https://istokmw.ru/

Документацию и программное обеспечение на изделия можно скачать в разделе «Документация и Программное обеспечение» на странице https://istokmw.ru/service-router/

Базовая техническая поддержка осуществляется
5 дней в неделю по будням с 8:00 до 17:00 (время Московское)
тел: +7 (495) 465-86-48
e-mail: support@istokmw.ru
web: https://istokmw.ru/support/

Личный кабинет технической поддержки по функционированию продуктов
https://helpdesk.istokmw.ru/