

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

СОДЕРЖАНИЕ

История изменений документа.....	4
1 Подготовка сервисного маршрутизатора к работе с web-интерфейсом.....	5
2 Первичная настройка сервисного маршрутизатора.....	8
2.1 Изменение пароля пользователя admin	8
2.2 Настройка NAT masquerade.....	10
2.3 Настройка ограничения доступа по номеру порта.....	16
3 Авторизация.....	27
4 Информационная панель.....	30
4.1 Процессор.....	30
4.2 Оперативная память	33
4.3 Диски	34
4.4 Сетевые адреса	35
4.5 IP-адреса, выданные DHCP-сервером	36
4.6 Пользователи.....	37
4.7 Система охлаждения.....	37
4.8 PCI-устройства	38
4.9 Состояние интерфейсов	39
5 Настройка интерфейсов	41
5.1 Настройка Ethernet интерфейса	41
5.2 Настройка Switchport интерфейса	46
5.3 Настройка логических интерфейсов.....	52
6 Настройка ACL.....	59
6.1 Настройка Access Control List	60
6.2 Настройка конфигурации time-range	64
6.3 Настройка ACL Filter.....	66
6.4 Настройка ACL Mangle (Маркировки пакетов)	71
6.5 Настройка ACL NAT (подмены ip-адресов).....	77
6.6 Настройка ACL PBR (политик)	81
6.7 Примеры настроек.....	86
6.7.1 Настройка фильтрации на основе IP-адреса источника	86
6.7.2 Настройка фильтрации на основе MAC-адреса отправителя.....	92

6.7.3	Настройка фильтрации по DPI.....	98
7	Управление пользователями	106
7.1	Управление пользователями	106
7.2	Управление группами	110

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.

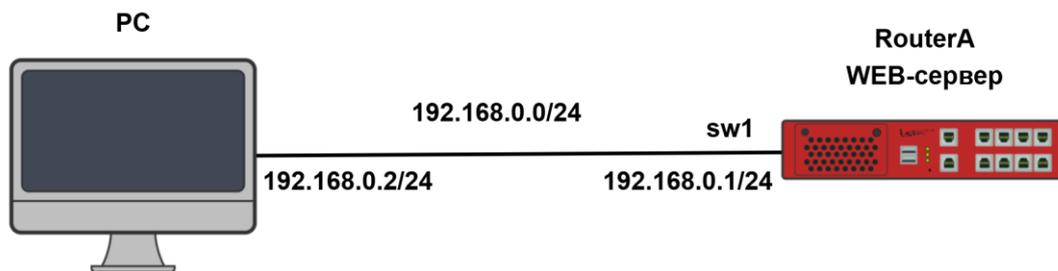


Рисунок 1 – Схема настройки web-сервера

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

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).

Сервисный маршрутизатор «ИСТОК»
Модель: ISM1508
Серийный номер: RS3010011C0014
Версия прошивки: 3.25.01 (стр: 4.4, 105-106) rps
Версия BMC: Firmware: 1.0.0
Версия Linux: 3.2.9

admin | Выйти

Управление пользователями

< Вернуться назад

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
admin	admin	local	*****	✎ ✕
user	istok	local	*****	✎ ✕

Отменить изменения Сохранить

Управление группами

Группа пользователя	Привилегия	Действие
admin	15	✕
service	1	✕
istok	5	✕

Отменить изменения Сохранить

Рисунок 2 – Вкладка Настройки ACL

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

Управление пользователями

< Вернуться назад



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).

Управление пользователями

< Вернуться назад



Рисунок 4 – Установка пароля

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

Управление пользователями

< Вернуться назад

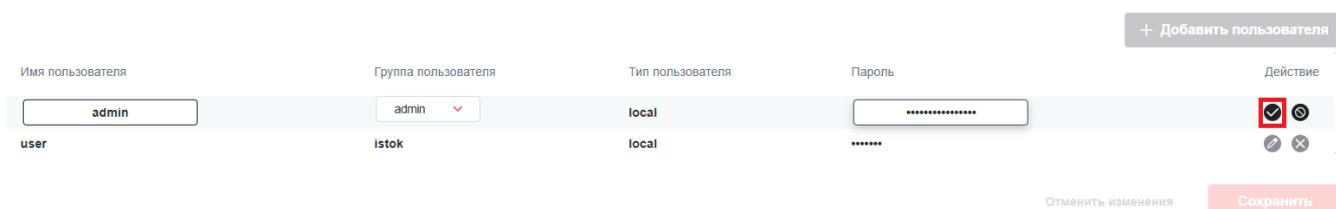


Рисунок 5 – Подтверждение изменений

Затем нажмите клавишу "Сохранить" (рисунок 6).

Управление пользователями

< Вернуться назад

+ Добавить пользователя

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="password" value="*****"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>

Отменить изменения

Сохранить

Рисунок 6 – Сохранение нового пароля

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

Сервисный маршрутизатор «ИСТОК»
 Модель: ISN4150B
 Серийный номер: RS2010011C2014

Версия прошивки: 3.25.01 (стр. 4, 4:195-68х, rpl)
 Версия BMC: Firmware: 1.9.0
 Версия U-boot: 1.3.9

Группа и/или пароль пользователя user были изменены

Управление пользователями

< Вернуться назад

+ Добавить пользователя

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
admin	admin	local	*****	<input checked="" type="checkbox"/> <input type="checkbox"/>
user	istok	local	*****	<input checked="" type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

Управление группами

+ Добавить группу

Группа пользователя	Привилегия	Действие
admin	15	<input checked="" type="checkbox"/> <input type="checkbox"/>
service	1	<input type="checkbox"/> <input checked="" type="checkbox"/>
istok	5	<input type="checkbox"/> <input checked="" type="checkbox"/>

Отменить изменения Сохранить

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).

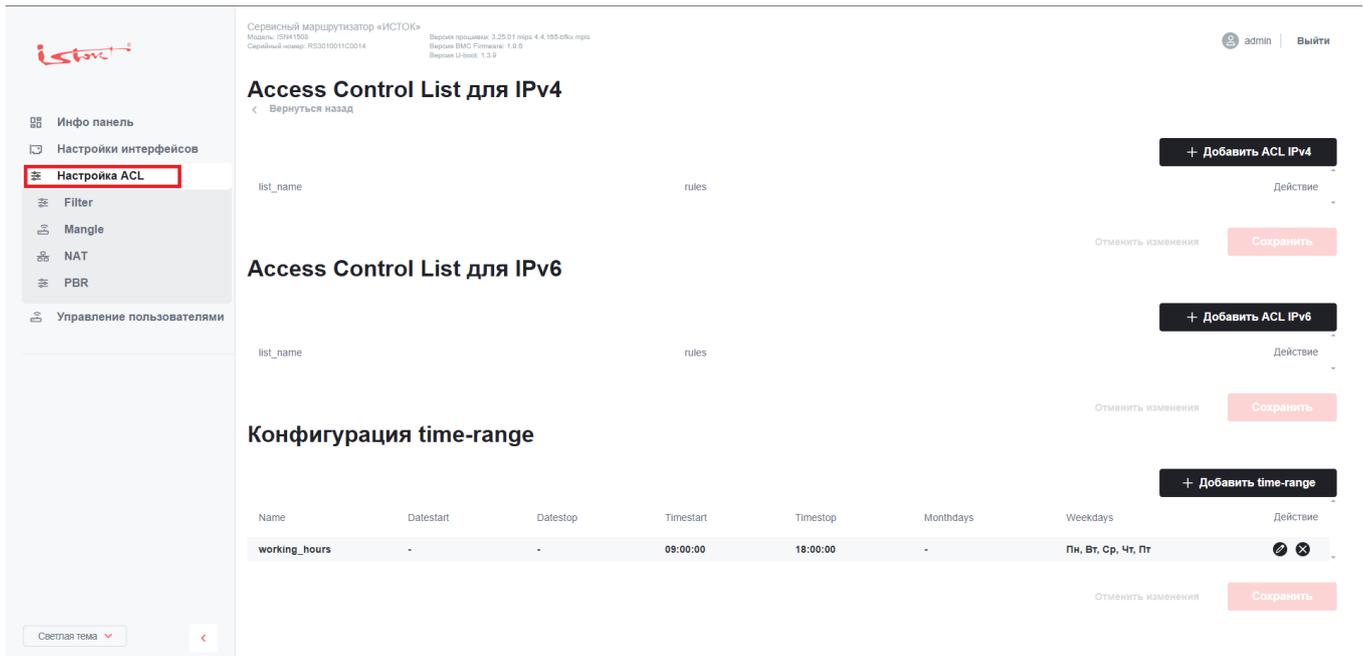


Рисунок 8 – Вкладка Настройки ACL

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

Access Control List для IPv4



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).

Access Control List для IPv4

[← Вернуться назад](#)

The screenshot shows the 'Access Control List для IPv4' configuration page. On the left, a list of rules is shown with 'nat_masquerade' selected. On the right, the configuration for the selected rule is displayed. The 'rules' section has a dropdown menu set to 'outinterface', which is highlighted with a red box. Below it, there is a toggle for 'outinterface' (currently 'NOT'), a dropdown for 'outinterface' set to 'eth1', and fields for 'time_range', 'logging', and 'index'. At the bottom right, there are buttons for 'Отменить изменения' and 'Сохранить'.

Рисунок 10 – Выбор правила

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

Access Control List для IPv4

[← Вернуться назад](#)

This screenshot is similar to Figure 10, but the configuration block for the 'outinterface' rule is highlighted with a red box. The 'outinterface' dropdown menu is now set to 'eth1'. The rest of the interface, including the rule list on the left and the 'Сохранить' button at the bottom right, remains the same.

Рисунок 11 – Блок настройки правила

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

Access Control List для IPv4

[← Вернуться назад](#)

This screenshot is similar to Figure 11, but the 'eth1' option in the 'outinterface' dropdown menu is highlighted with a red box. The rest of the interface, including the rule list on the left and the 'Сохранить' button at the bottom right, remains the same.

Рисунок 12 – Выбор протокола

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

Access Control List для IPv4

< Вернуться назад

list_name: nat_masquerade

rules:

- outinterface: [dropdown menu]
- outinterface: NOT
- outinterface: eth1
- time_range: [dropdown menu]
- logging: index: [input field]

Действие: [Red checkmark icon]

Отменить изменения | Сохранить

Рисунок 13 – Подтверждение создания списка

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

Access Control List для IPv4

< Вернуться назад

list_name: nat_masquerade

rules: 1 outinterface: eth1

Действие: [Red checkmark icon], [Lock icon], [Close icon]

Отменить изменения | Сохранить

Рисунок 14 – Сохранение списка

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

Сервисный маршрутизатор «ИСТОК»

Модель: ISM1009
Серийный номер: R53010011C0014

Версия прошивки: 3.25.01 ipso 4.4.105-0bxc-mpis
Фирменная ОС: Firmaware: 1.0.0
Версия U-boot: 1.3.0

admin | Выйти

NAT Chains

Выбор VRF: default [Очистить статистику]

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	action
----------	-------	-----	-----	------------	----	------	----------	------	-------	--------

Отменить изменения | Сохранить

Рисунок 15 – Вкладка Filter

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

NAT Chains



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.

NAT Chains



Рисунок 17 – Настройка NAT

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

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	Действие
1	postrouting	default	nat_masquerade	<input type="checkbox"/>			<input checked="" type="checkbox"/>	-	-	<input checked="" type="checkbox"/>

Отменить изменения Сохранить

Рисунок 18 – Подтверждение создания NAT

Затем нажмите клавишу "Сохранить" (рисунок 19).

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	action
1	postrouting	default	nat_masquerade	<input type="checkbox"/>	-	-	<input checked="" type="checkbox"/>	-	-	-

Отменить изменения Сохранить

Рисунок 19 – Сохранение фильтра

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

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	action
-	postrouting	default	-	<input type="checkbox"/>	-	-	<input checked="" type="checkbox"/>	-	-	
-	postrouting	default	nat_masquerade	<input type="checkbox"/>	-	-	<input checked="" type="checkbox"/>	-	-	
1	postrouting	default	outinterface: eth1	<input type="checkbox"/>	-	-	<input type="checkbox"/>	-	-	-

Отменить изменения Сохранить

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).

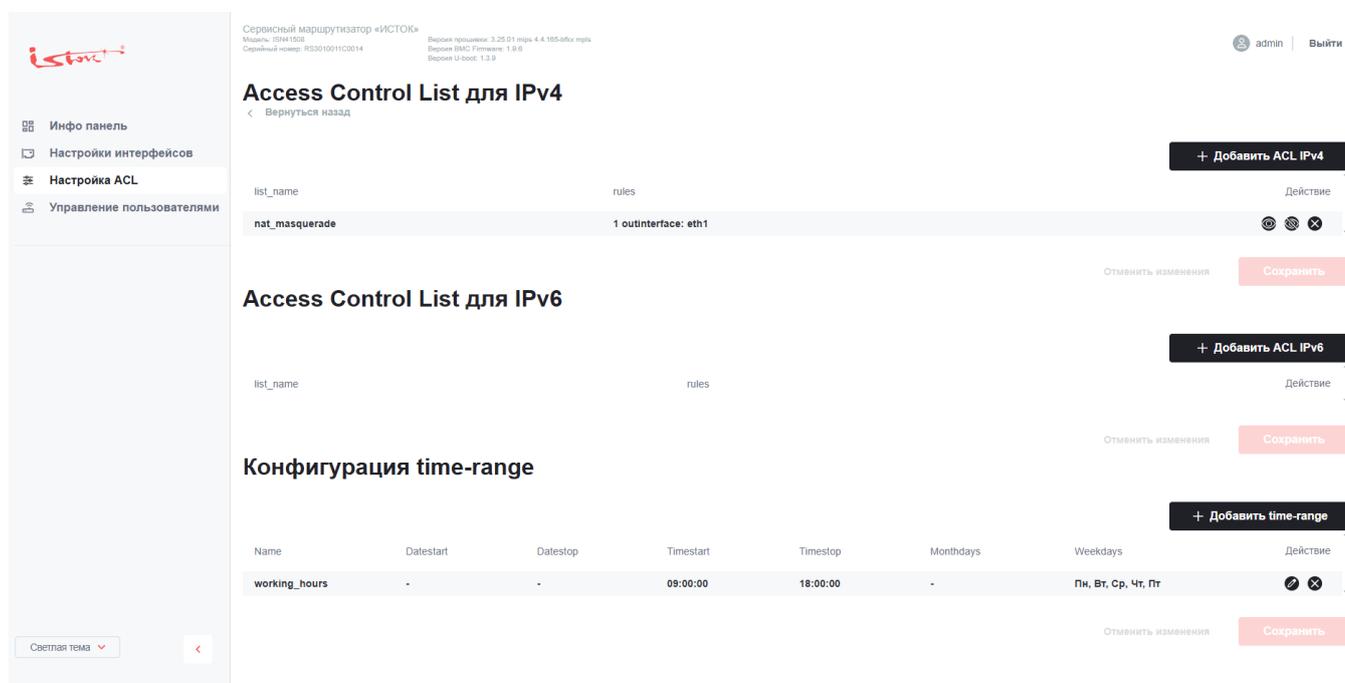


Рисунок 21 – Вкладка Настройки ACL

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

Access Control List для IPv4

< Вернуться назад

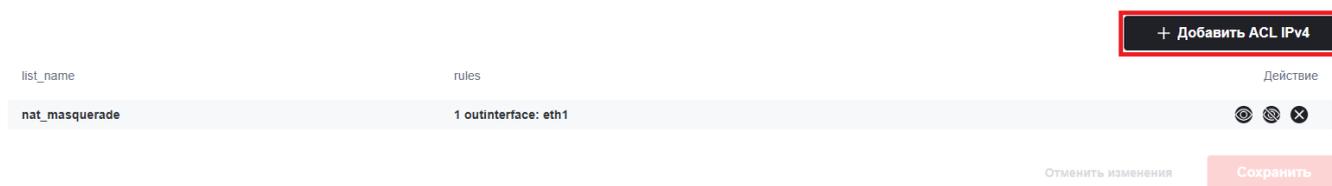


Рисунок 22 – Добавление списком управления доступом

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

Access Control List для IPv4

[← Вернуться назад](#)

The screenshot shows the 'Access Control List для IPv4' configuration page. In the 'rules' section, a dropdown menu is open, showing 'protocol' as the selected option. This dropdown is highlighted with a red border. To the left of the main configuration area, there is a button labeled 'port_blocking', also highlighted with a red border. Below the dropdown, there are fields for 'protocol' (with a toggle and 'NOT' label), 'protocol_name', and 'protocol_num'. At the bottom of the rule configuration, there are fields for 'time_range', 'logging' (checkbox), and 'index'. On the right side, there are 'Отменить изменения' and 'Сохранить' buttons.

Рисунок 23 – Выбор правила

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

Access Control List для IPv4

[← Вернуться назад](#)

This screenshot shows the same ACL configuration page as Figure 23, but now the configuration block for the 'protocol' rule is highlighted with a red border. The 'protocol_name' field is disabled and displays the message: 'Недоступно: уже задан protocol_num или добавлены зависимые блоки'. The 'port_blocking' button is still visible on the left. The 'Отменить изменения' and 'Сохранить' buttons are at the bottom right.

Рисунок 24 – Блок настройки правила

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

Access Control List для IPv4

< Вернуться назад

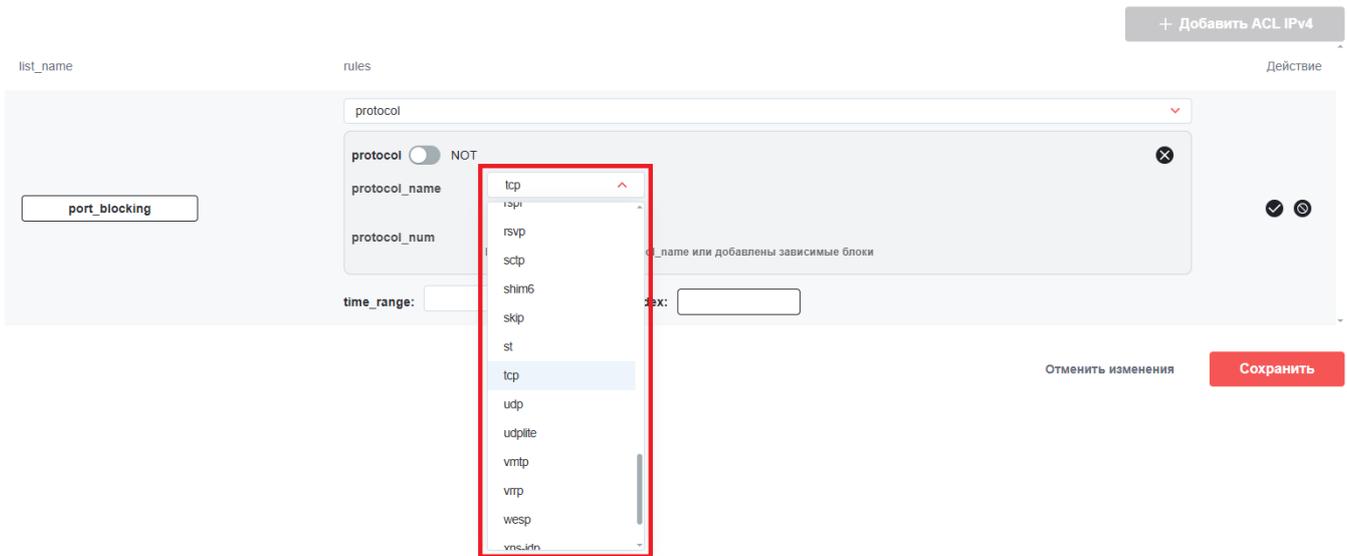


Рисунок 25 – Выбор протокола

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

Access Control List для IPv4

< Вернуться назад

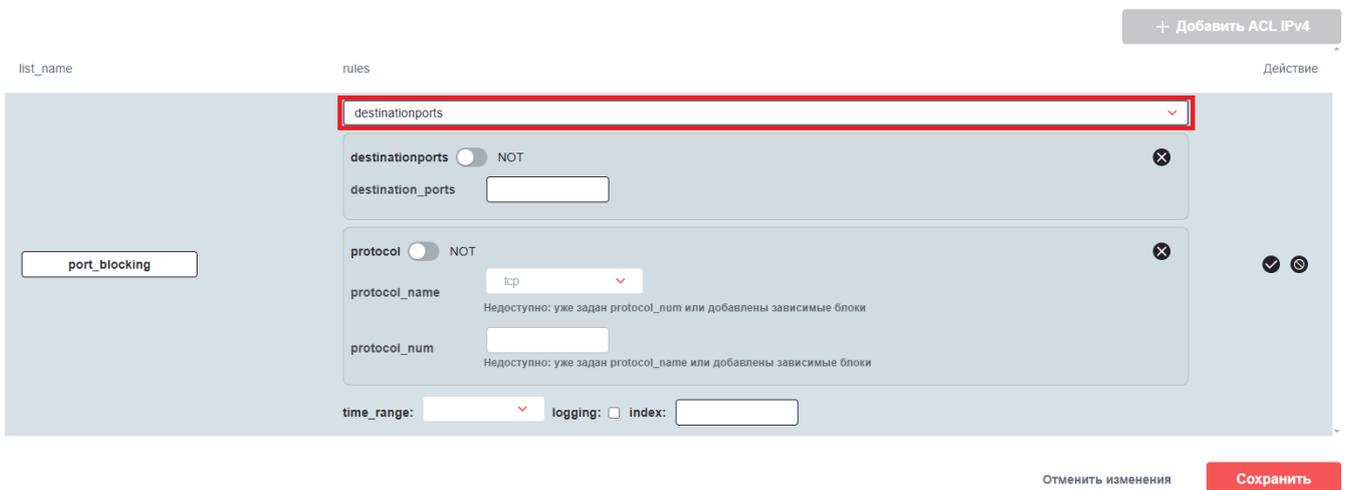


Рисунок 26 – Выбор занесения срабатывания правила в лог

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

Access Control List для IPv4

[← Вернуться назад](#)

The screenshot shows the configuration page for an IPv4 Access Control List. At the top right, there is a button '+ Добавить ACL IPv4'. Below it, a table with columns 'list_name', 'rules', and 'Действие' is visible. The 'rules' column contains a configuration form for a rule named 'destinationports'. This form is highlighted with a red rectangular box. The form includes a 'destinationports' dropdown menu, a 'destinationports' toggle switch set to 'NOT', and a 'destination_ports' text input field. Below this, there is a 'protocol' toggle switch set to 'NOT', a 'protocol_name' dropdown menu set to 'tcp', and a 'protocol_num' text input field. At the bottom of the form, there are 'time_range' and 'index' dropdown menus, and a 'logging' checkbox. To the left of the form is a 'port_blocking' button. To the right, in the 'Действие' column, there are two icons: a checkmark and a cross. At the bottom right of the page, there are two buttons: 'Отменить изменения' and 'Сохранить'.

Рисунок 27 – Блок настройки правила

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

Access Control List для IPv4

[← Вернуться назад](#)

This screenshot is similar to the previous one, showing the same ACL configuration page. However, the 'destination_ports' text input field is now filled with the value '80,8080,443,8082'. This field is highlighted with a red rectangular box. All other elements of the interface, including the 'protocol' settings and the 'Сохранить' button, remain the same as in the previous screenshot.

Рисунок 28 – Выбор портов

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

Access Control List для IPv4

[← Вернуться назад](#)

+ Добавить ACL IPv4

list_name	rules	Действие
port_blocking	destinationports destinationports <input type="checkbox"/> NOT destination_ports <input type="text" value="80,8080,443,8082"/> protocol <input type="checkbox"/> NOT protocol_name <input type="text" value="tcp"/> <small>Недоступно: уже задан protocol_num или добавлены зависимые блоки</small> protocol_num <input type="text"/> <small>Недоступно: уже задан protocol_name или добавлены зависимые блоки</small> time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

Рисунок 29 – Подтверждение создания списка

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

Access Control List для IPv4

[← Вернуться назад](#)

+ Добавить ACL IPv4

list_name	rules	Действие
port_blocking	1 protocol_name: tcp, destination_ports: 80,8080,443,8082	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
nat_masquerade	1 outinterface: eth1	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Отменить изменения Сохранить

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).

Access Control List для IPv4

< Вернуться назад

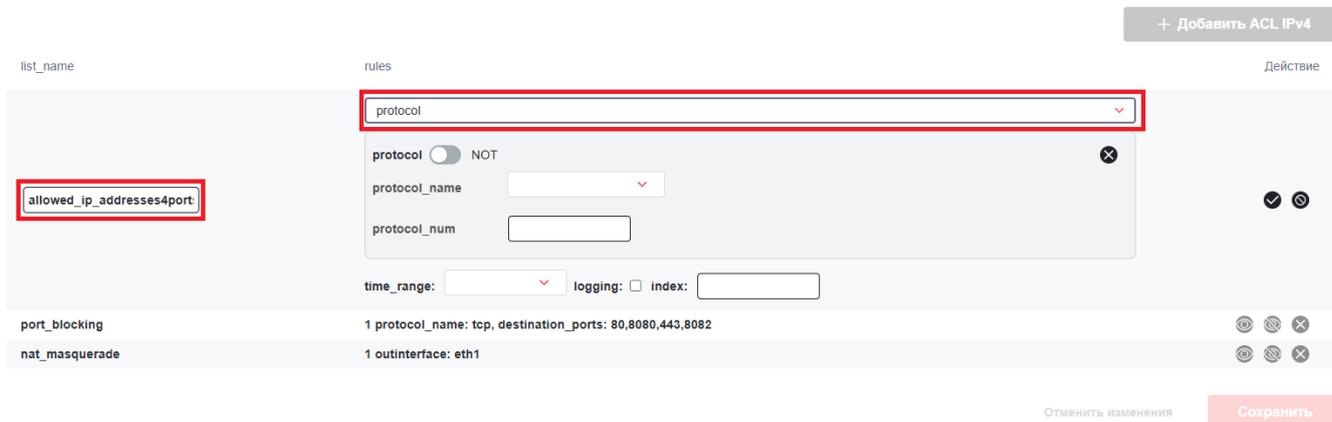


Рисунок 31 – Выбор правила

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

Access Control List для IPv4

< Вернуться назад

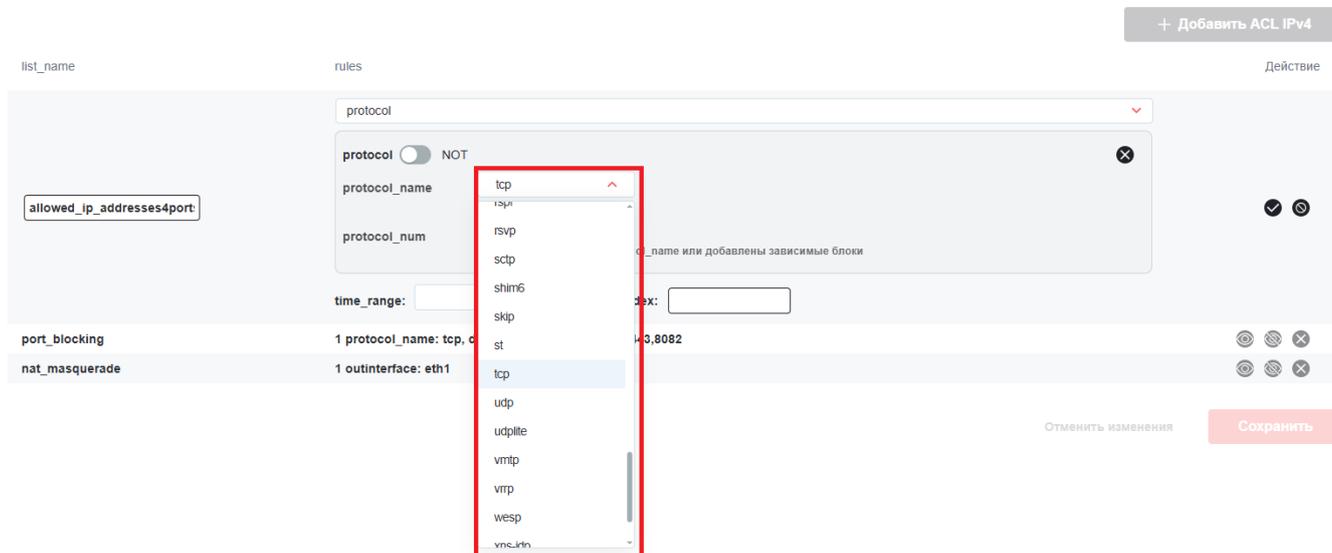


Рисунок 32 – Выбор протокола

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).

Access Control List для IPv4

[← Вернуться назад](#)

+ Добавить ACL IPv4

list_name	rules	Действие
<div style="border: 1px solid #ccc; padding: 5px; width: fit-content;">allowed_ip_addresses4port:</div>	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> sourceip </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> sourceip <input type="checkbox"/> NOT ✕ </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> source_subnet <input type="text"/> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> destinationports <input type="checkbox"/> NOT ✕ </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> destination_ports <input type="text"/> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> protocol <input type="checkbox"/> NOT ✕ </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> protocol_name <input type="text" value="tcp"/> <small>Недоступно: уже задан protocol_num или добавлены зависимые блоки</small> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> protocol_num <input type="text"/> <small>Недоступно: уже задан protocol_name или добавлены зависимые блоки</small> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/> </div> </div>	✔ 🔄
	port_blocking 1 protocol_name: tcp, destination_ports: 80,8080,443,8082 👁️ 🔄 ✕	
	nat_masquerade 1 outinterface: eth1 👁️ 🔄 ✕	
	Отменить изменения Сохранить	

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).

Access Control List для IPv4

[← Вернуться назад](#)

+ Добавить ACL IPv4

list_name	rules	Действие
<div style="border: 1px solid #ccc; padding: 5px; width: fit-content;">allowed_ip_addresses4port:</div>	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> sourceip </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> sourceip <input type="checkbox"/> NOT ✕ </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> source_subnet <input style="border: 2px solid red;" type="text" value="192.168.0.1/24"/> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> destinationports <input type="checkbox"/> NOT ✕ </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> destination_ports <input style="border: 2px solid red;" type="text" value="80,8080,443,8082"/> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> protocol <input type="checkbox"/> NOT ✕ </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> protocol_name <input type="text" value="tcp"/> <small>Недоступно: уже задан protocol_num или добавлены зависимые блоки</small> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> protocol_num <input type="text"/> <small>Недоступно: уже задан protocol_name или добавлены зависимые блоки</small> </div> <div style="border-bottom: 1px solid #ccc; margin-bottom: 5px;"> time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/> </div> </div>	✔ 🔄
	port_blocking 1 protocol_name: tcp, destination_ports: 80,8080,443,8082 👁️ 🔄 ✕	
	nat_masquerade 1 outinterface: eth1 👁️ 🔄 ✕	
	Отменить изменения Сохранить	

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).

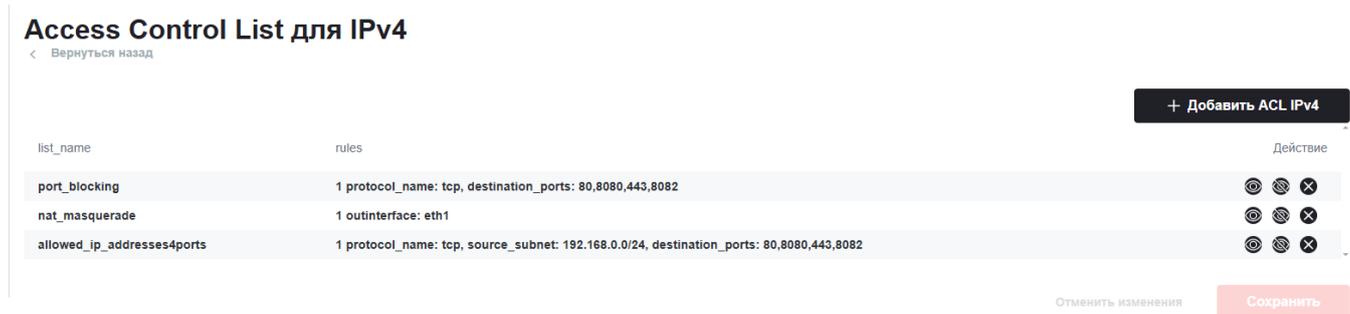


Рисунок 35 – Отображение списков контроля доступом

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).

ACL Filter IPv4



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).

ACL Filter IPv4



Рисунок 38 – Настройка фильтра

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

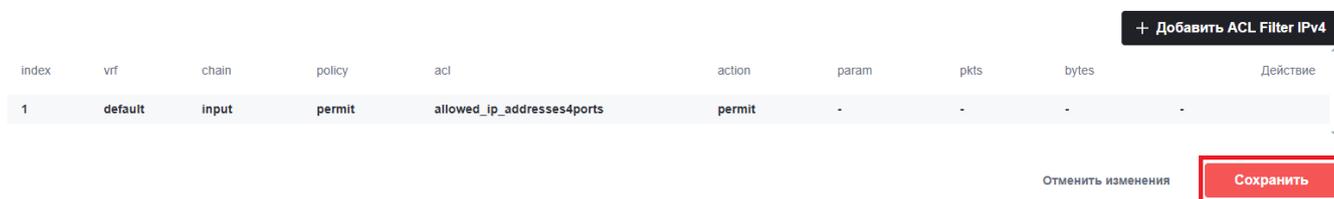
ACL Filter IPv4



Рисунок 39 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 40).

ACL Filter IPv4



index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	input	permit	allowed_ip_addresses4ports	permit	-	-	-	

[+ Добавить ACL Filter IPv4](#)
[Отменить изменения](#) [Сохранить](#)

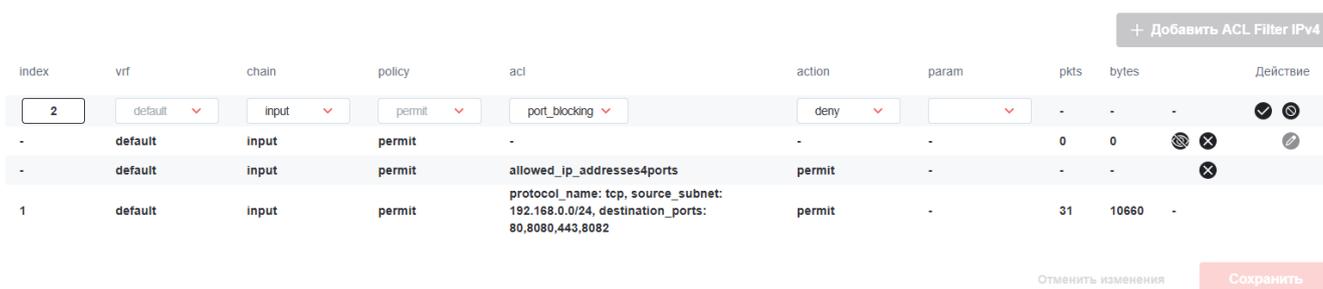
Рисунок 40 – Сохранение фильтра

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).

ACL Filter IPv4



index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
2	default	input	permit	port_blocking	deny		-	-	✓
-	default	input	permit	allowed_ip_addresses4ports	permit	-	0	0	✗
1	default	input	permit	protocol_name: tcp, source_subnet: 192.168.0.0/24, destination_ports: 80,8080,443,8082	permit	-	31	10660	

[+ Добавить ACL Filter IPv4](#)
[Отменить изменения](#) [Сохранить](#)

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).

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
-	default	input	permit	-	-	-	0	0	  
-	default	input	permit	allowed_ip_addresses4ports	permit	-	-	-	
1	default	input	permit	protocol_name: tcp, source_subnet: 192.168.0.0/24, destination_ports: 80,8080,443,8082	permit	-	84	27311	-
-	default	input	permit	port_blocking	deny	-	-	-	
2	default	input	permit	protocol_name: tcp, destination_ports: 80,8080,443,8082	deny	-	84	27311	-

Отменить изменения Сохранить

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).

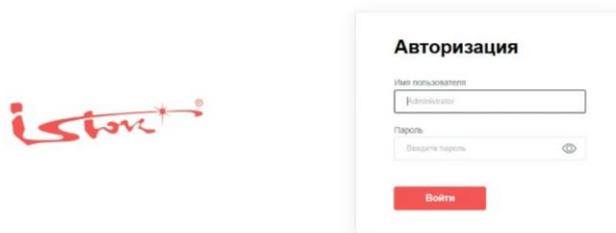


Рисунок 43 – Авторизация

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).

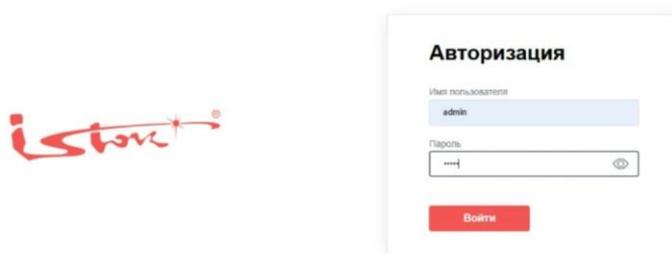


Рисунок 44 – Ввод логина и пароля

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

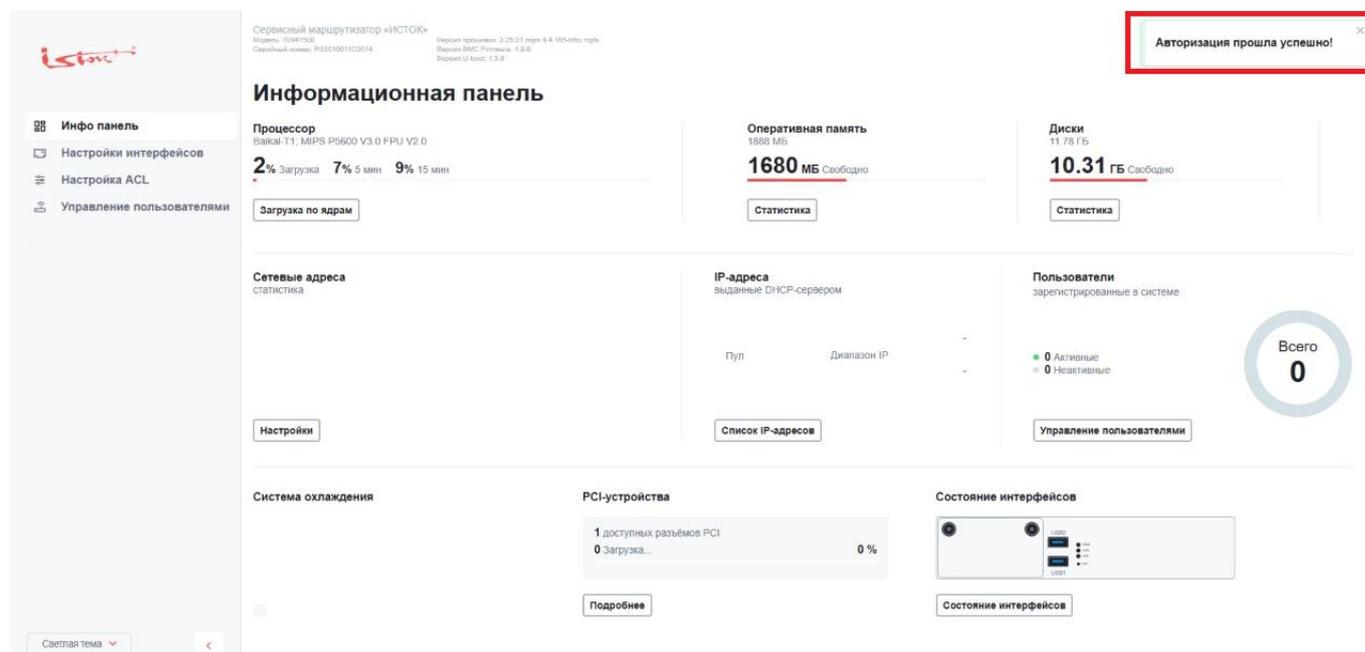


Рисунок 45 – Уведомление об успешной авторизации

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

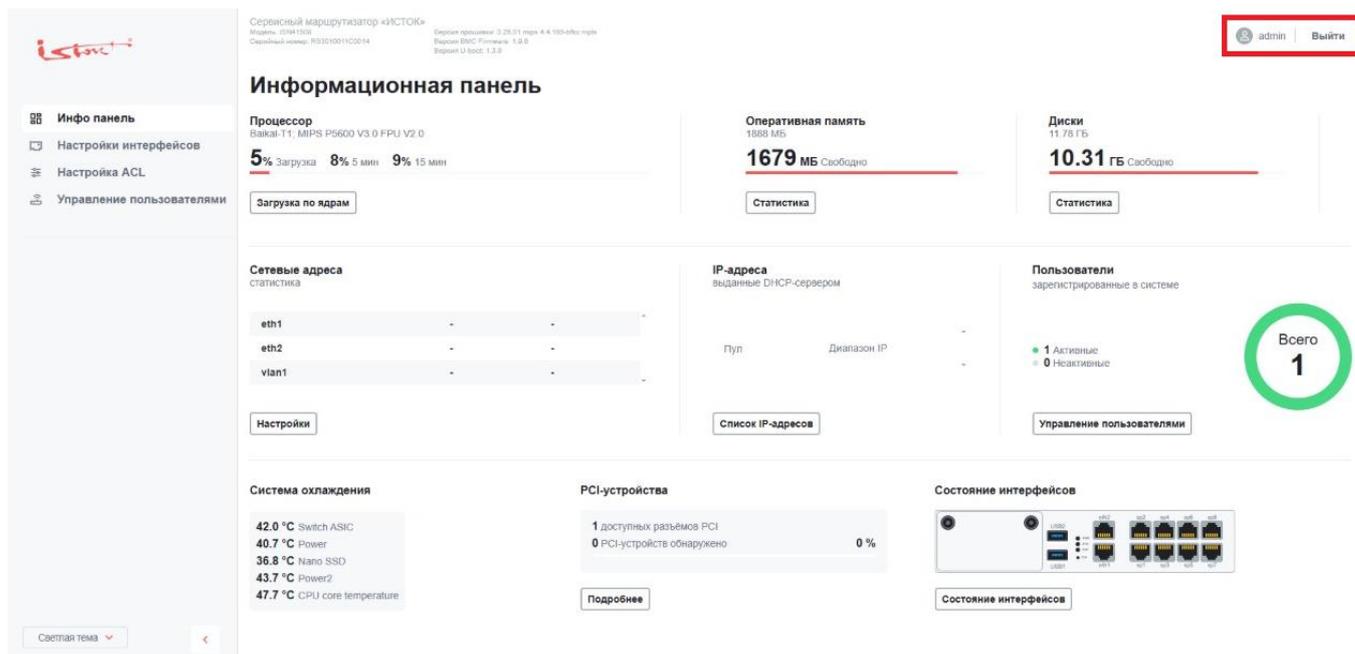


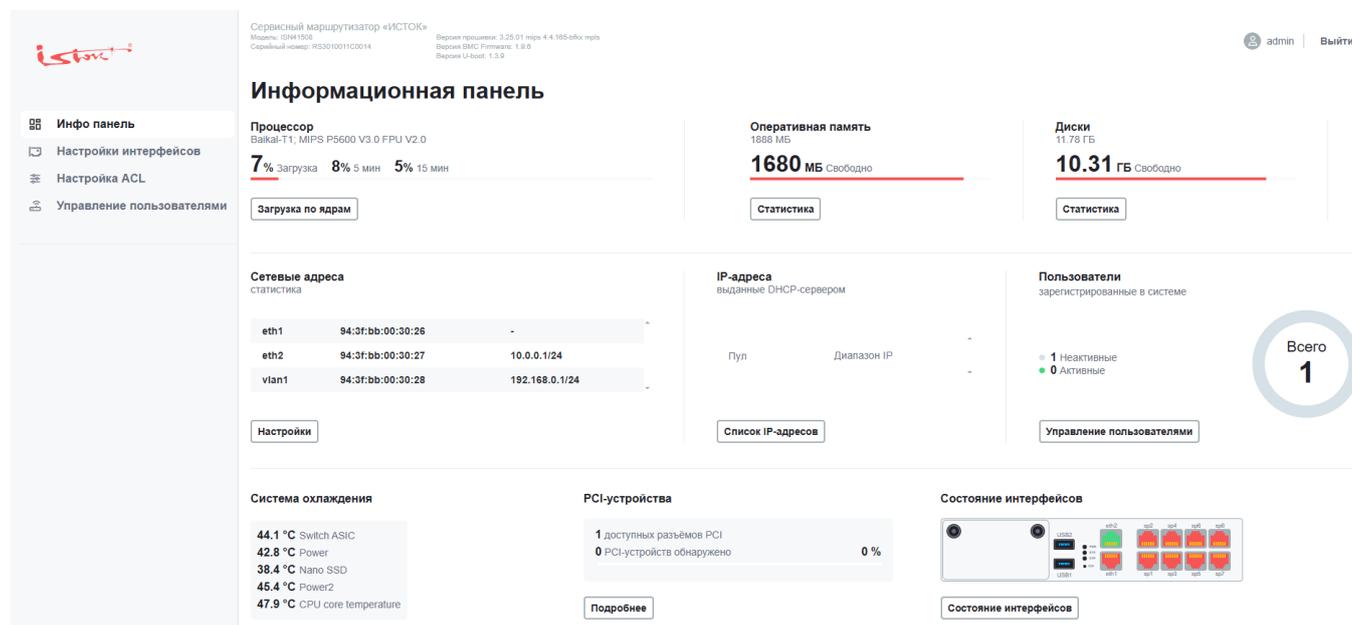
Рисунок 46 – Профиль

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 отобразится 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.



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

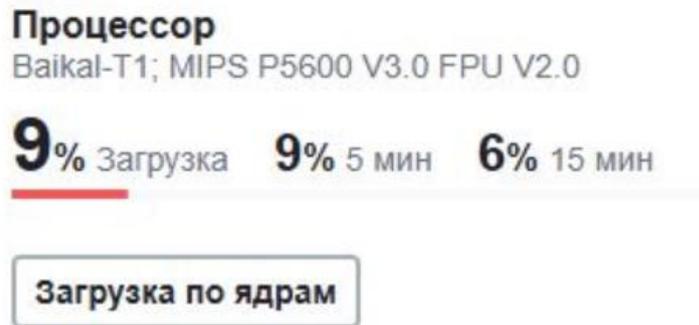


Рисунок 48 – Блок "Процессор"

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).

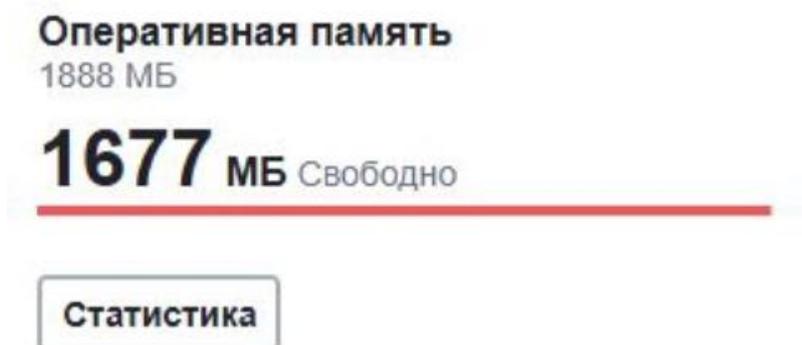


Рисунок 50 – Блок "Оперативная память"

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

Статистика использования оперативной памяти ×

Параметр	Память, МБ
Физическая память всего	1888
Свободная физическая память	1660
Используемая физическая память	119
Совместно используемая физическая память	0
Память файла подкачки, всего	51
Свободная память файла подкачки	51
Используемая память файла подкачки	0
Кешировано	108
Доступно	1682

Рисунок 51 – Статистика оперативной памяти

4.3 Диски

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

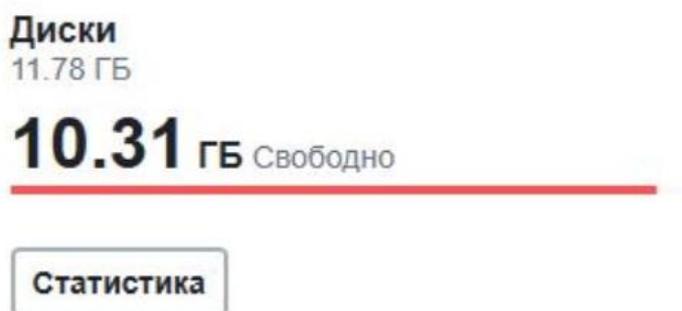
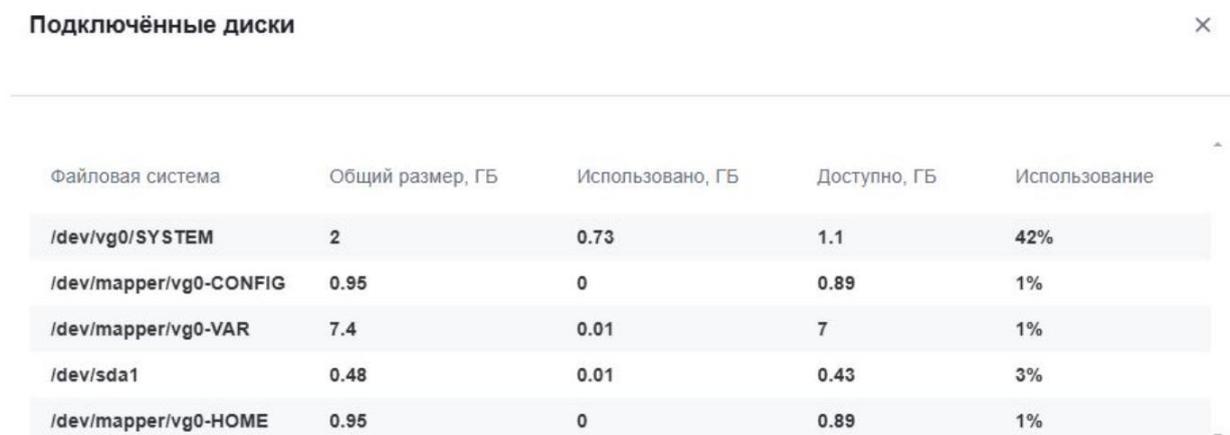


Рисунок 52 – Блок "Диски"

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



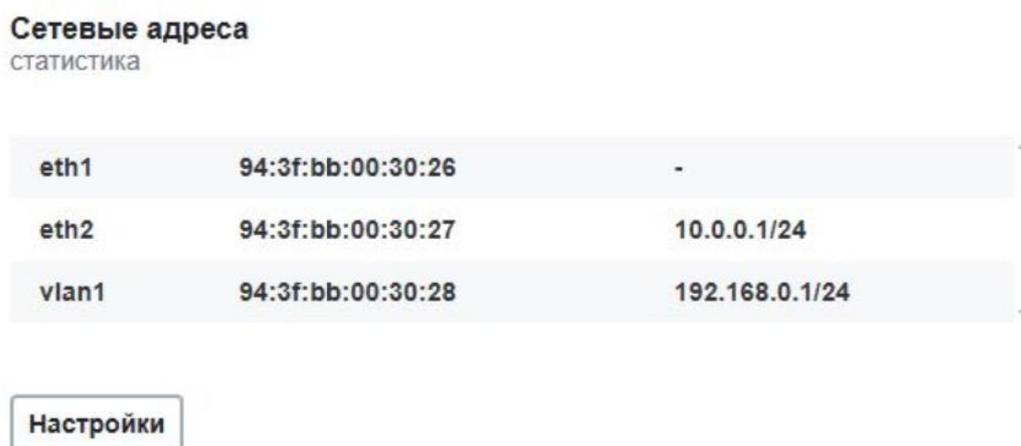
Подключенные диски

Файловая система	Общий размер, ГБ	Использовано, ГБ	Доступно, ГБ	Использование
/dev/vg0/SYSTEM	2	0.73	1.1	42%
/dev/mapper/vg0-CONFIG	0.95	0	0.89	1%
/dev/mapper/vg0-VAR	7.4	0.01	7	1%
/dev/sda1	0.48	0.01	0.43	3%
/dev/mapper/vg0-HOME	0.95	0	0.89	1%

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).



Сетевые адреса
статистика

eth1	94:3f:bb:00:30:26	-
eth2	94:3f:bb:00:30:27	10.0.0.1/24
vlan1	94:3f:bb:00:30:28	192.168.0.1/24

Настройки

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).

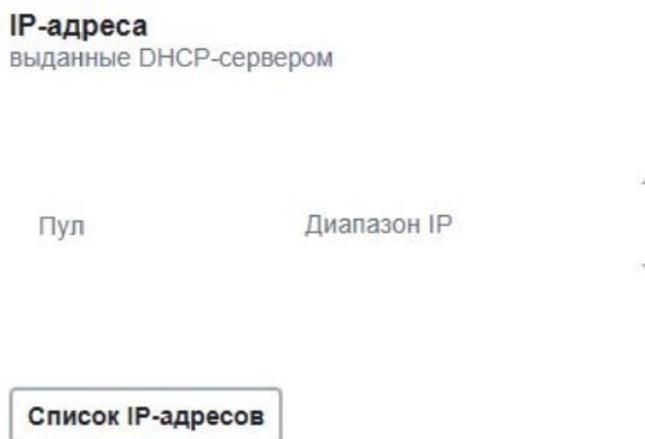


Рисунок 55 – Блок "IP-адреса"

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

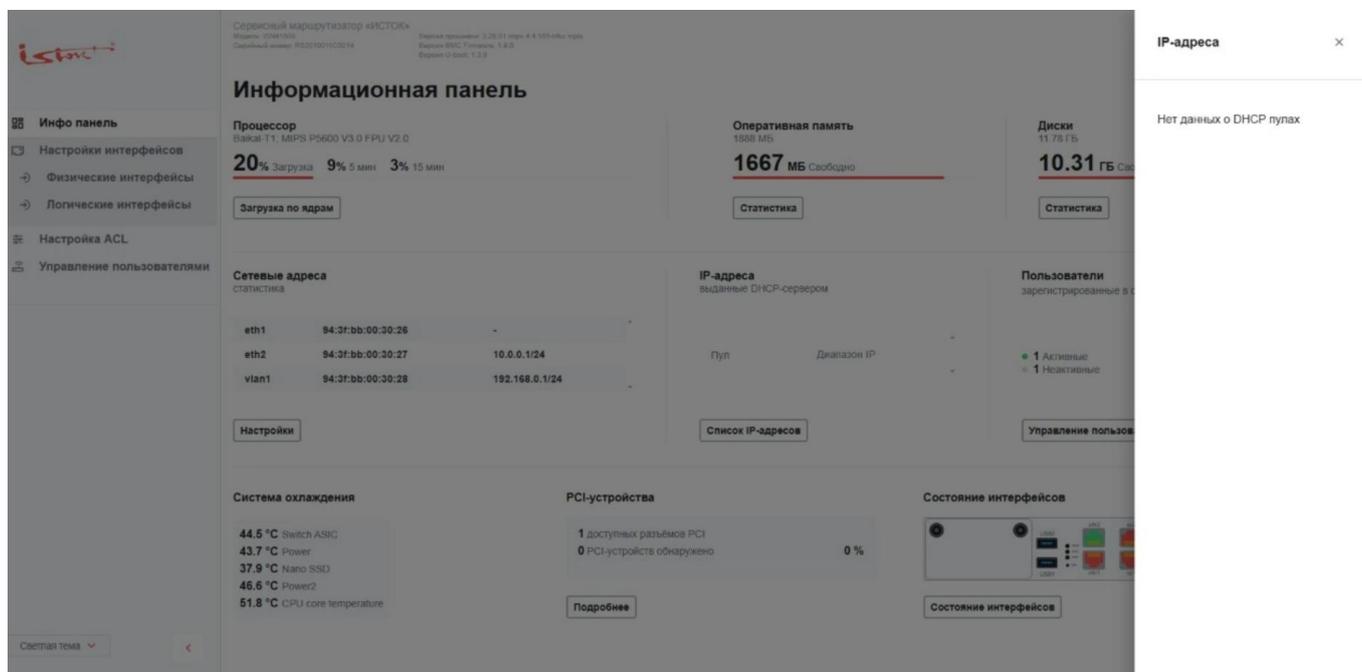


Рисунок 56 – Список IP-адресов

4.6 Пользователи

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

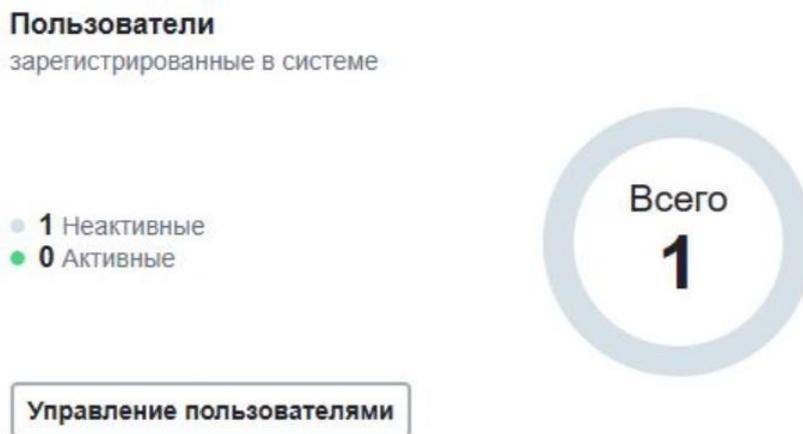


Рисунок 57 – Блок "Пользователи"

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).

Система охлаждения



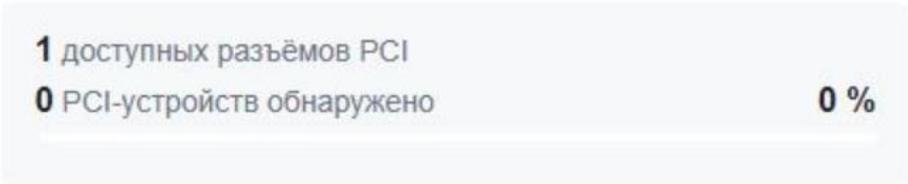
46.7 °C Switch ASIC
45.3 °C Power
40.0 °C Nano SSD
48.3 °C Power2
51.2 °C CPU core temperature

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).

PCI-устройства



1 доступных разъёмов PCI
0 PCI-устройств обнаружено 0 %

[Подробнее](#)

Рисунок 59 – Блок "PCI-устройства"

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

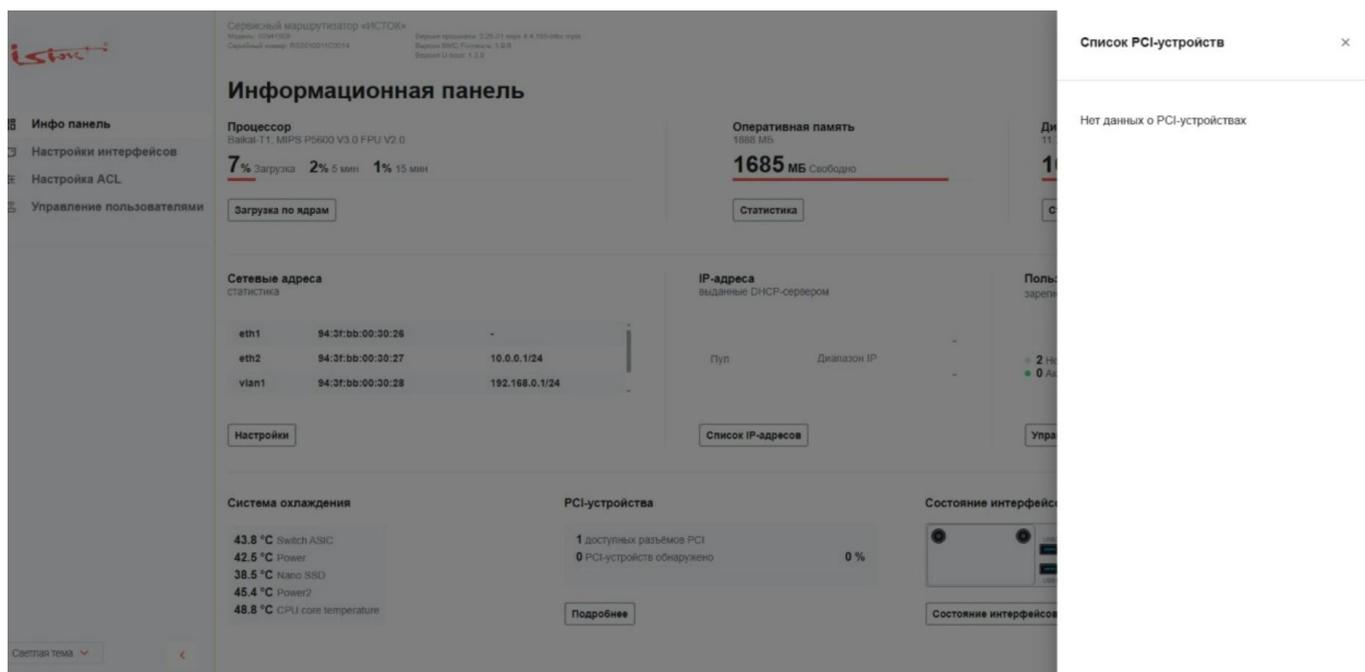


Рисунок 60 – PCI-устройства

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).

Наименование интерфейса	Admin	IPv4-адрес	RX bytes	TX bytes	MTU	RX packets	TX packets	IPv6-адрес	Duplex	Автосогласование	Скорость
eth1	UP	-	0	578	1500	0	5	-	half	on	1000
eth2	UP	10.0.0.1/24	7309848	7968803	1500	26682	22948	-	full	on	1000

Рисунок 62 – Информация о состоянии интерфейсов

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

Состояние интерфейсов

[Вернуться назад](#)

Ethernet **Loopback** Switchport VLAN

Наименование интерфейса	Admin	IPv4-адрес	RX bytes	TX bytes	MTU	RX packets	TX packets	IPv6-адрес
lo1	DOWN	1.1.1.1/24	0	0	68	0	0	-

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).

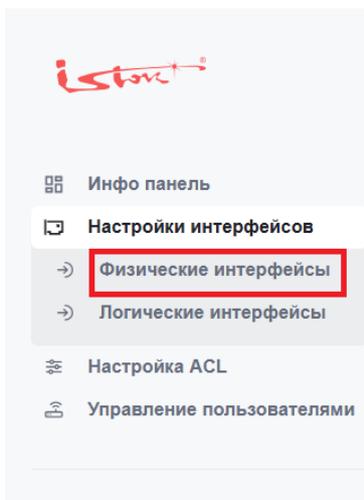


Рисунок 64 – Выбор пункта "Физические интерфейсы"

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

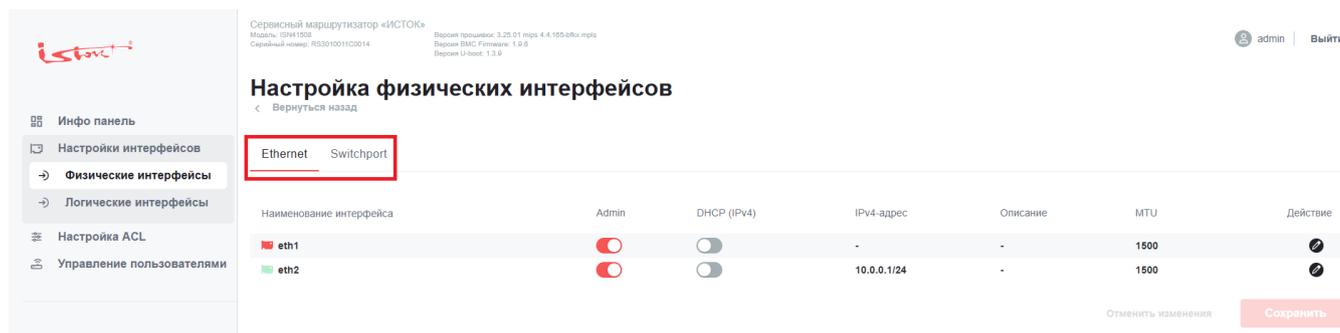


Рисунок 65 – Выбор типа физического интерфейса

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

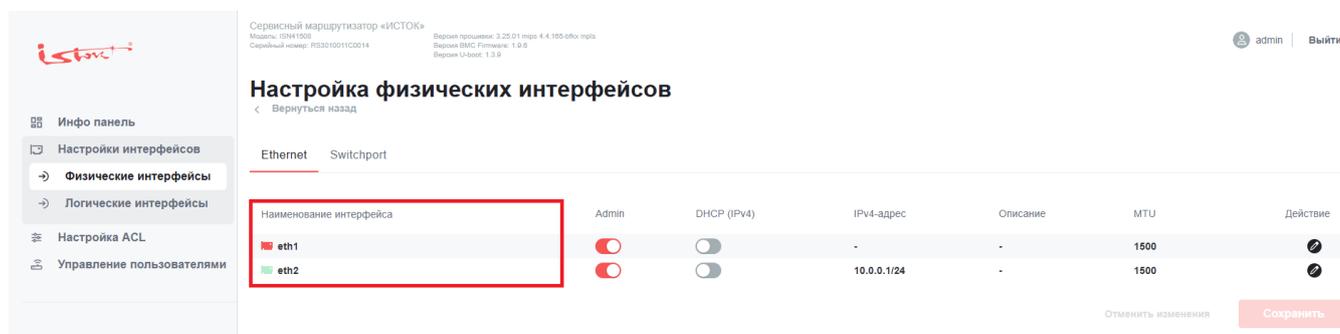


Рисунок 66 – Наименование интерфейсов

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

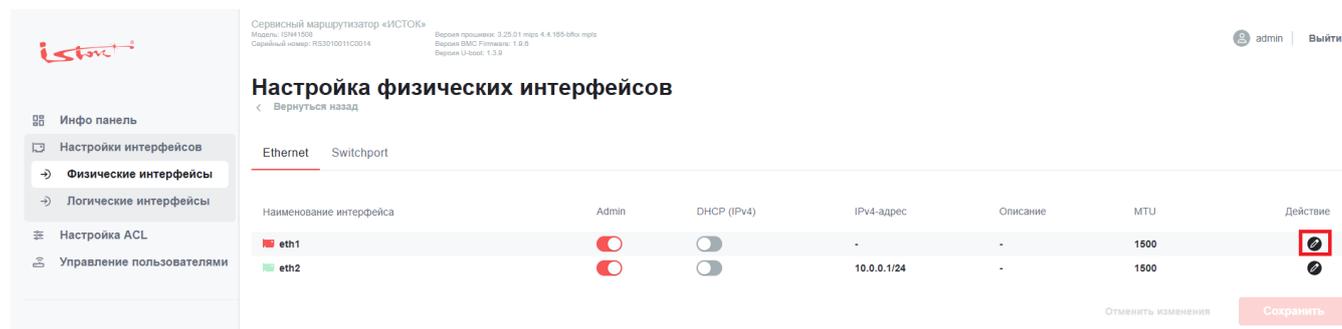


Рисунок 67 – Ethernet интерфейс пиктограмма изменить

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

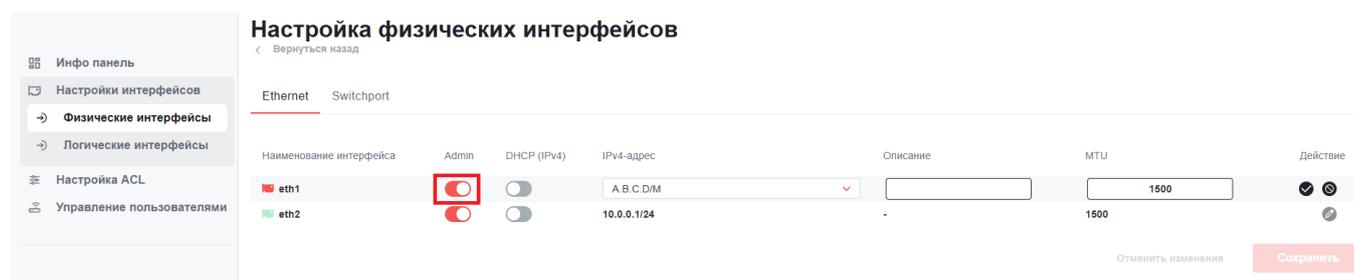


Рисунок 68 – Изменение административного статуса интерфейса

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

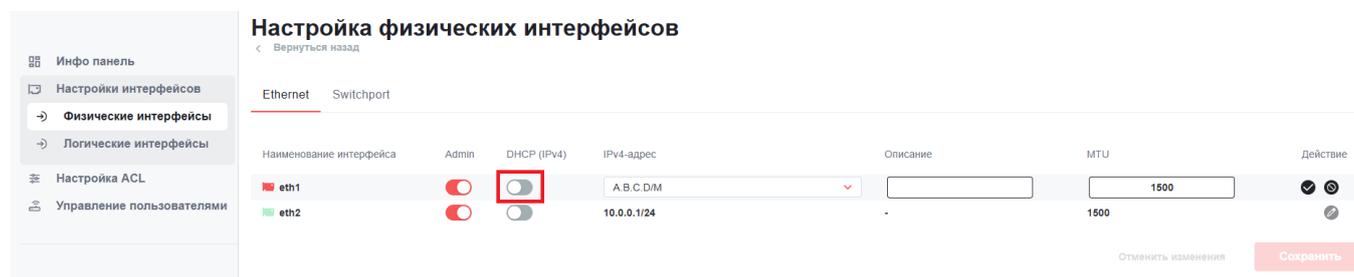


Рисунок 69 – Настройка DHCP клиента

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

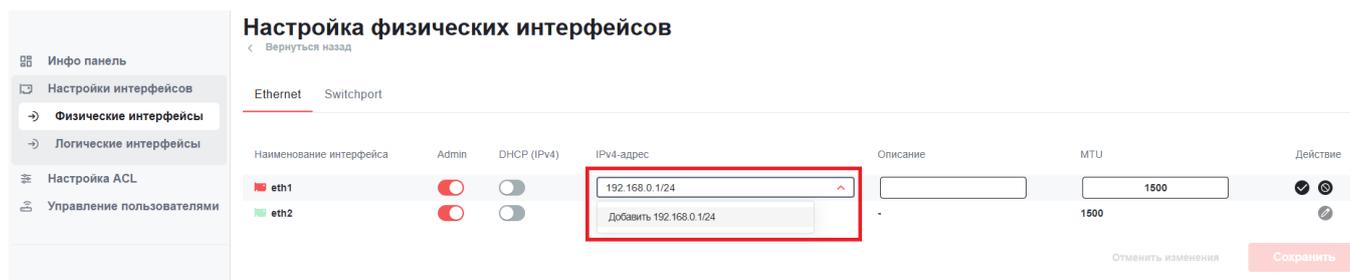


Рисунок 70 – Добавление IP-адреса

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).

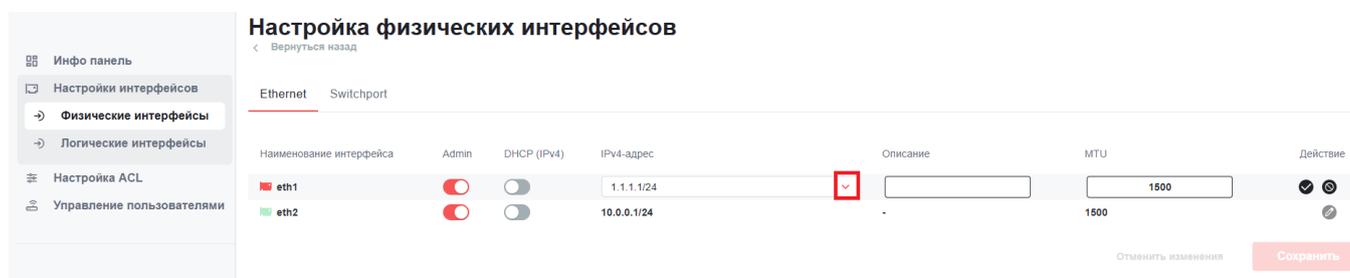


Рисунок 71 – Просмотр IP-адресов на интерфейсе

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

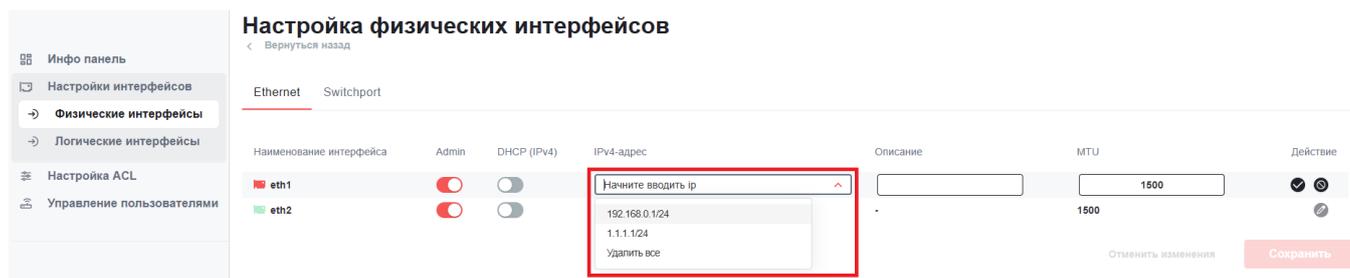


Рисунок 72 – Удаление IP-адресов

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

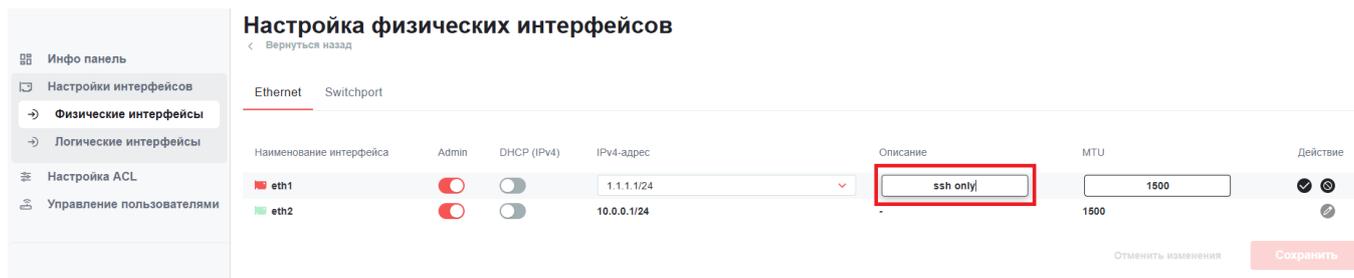


Рисунок 73 – Добавление описания интерфейсу

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

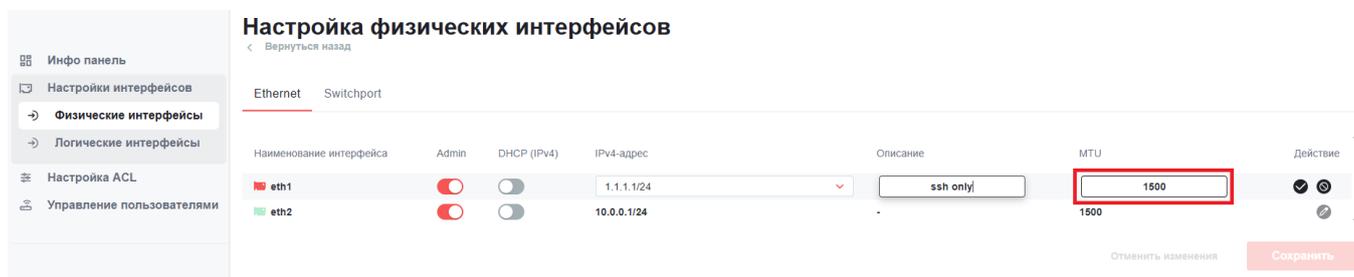


Рисунок 74 – Настройка MTU

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

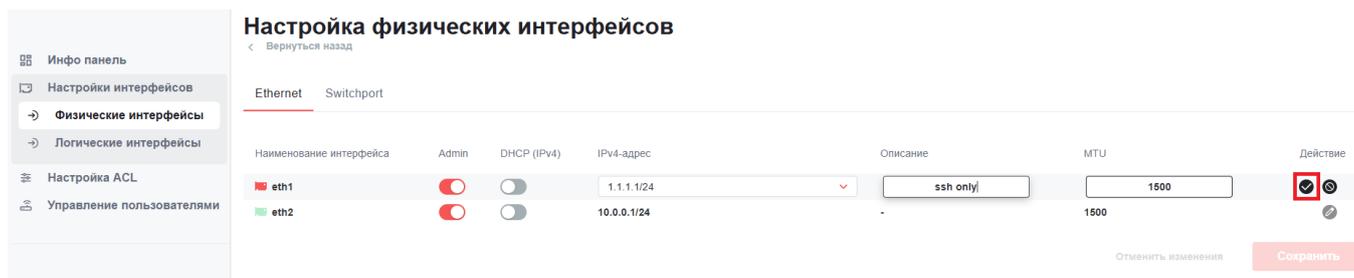


Рисунок 75 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 76).

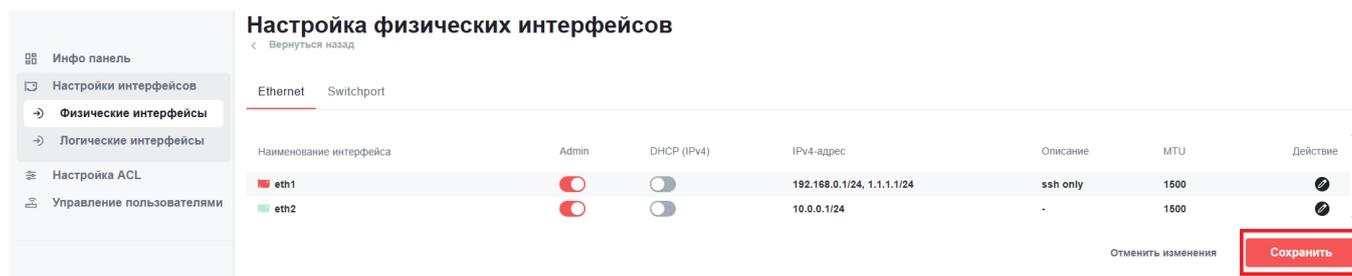


Рисунок 76 – Сохранение настроек

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

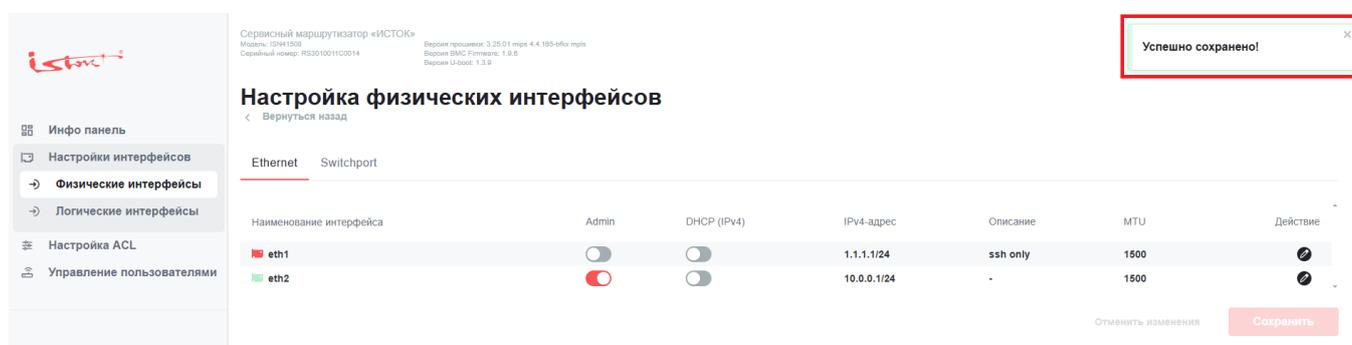


Рисунок 77 – Подтверждение сохранения

5.2 Настройка Switchport интерфейса

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

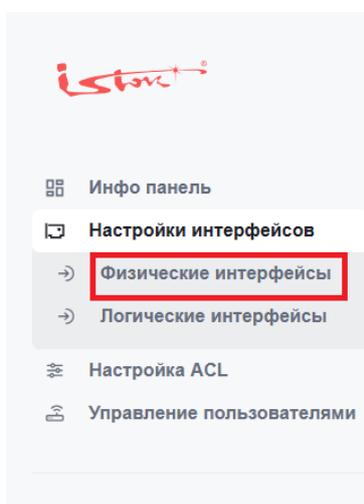


Рисунок 78 – Выбор пункта "Физические интерфейсы"

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

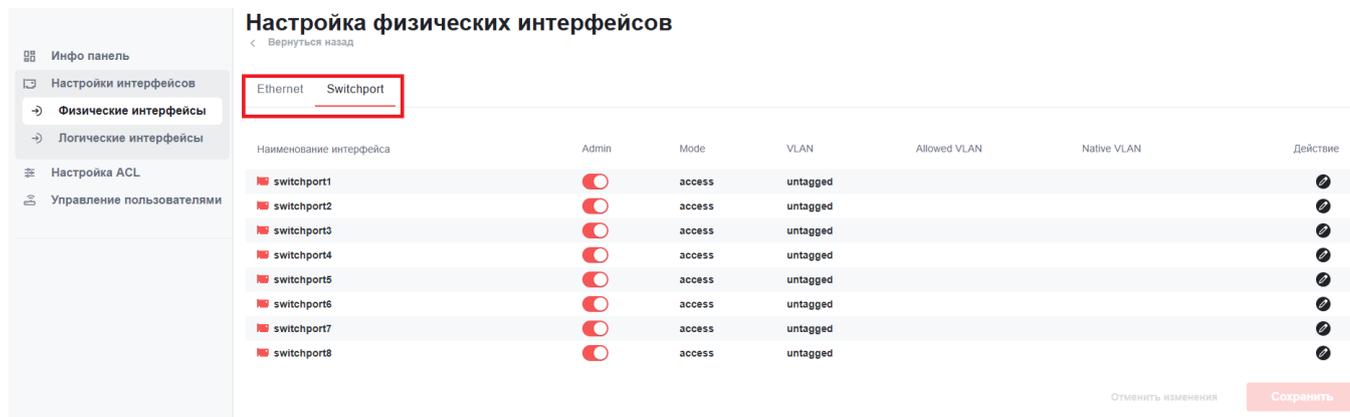


Рисунок 79 – Выбор типа физического интерфейса

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

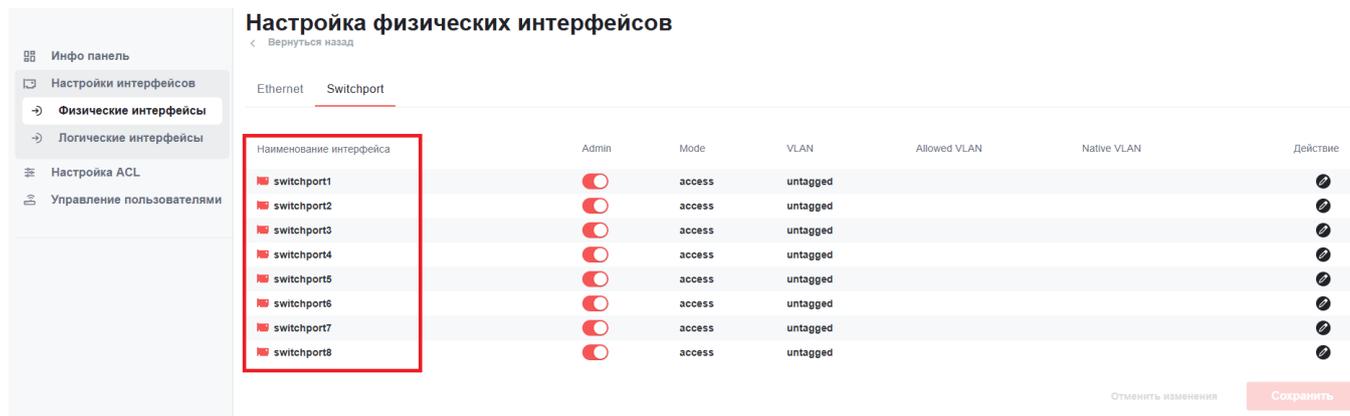


Рисунок 80 – Наименование интерфейсов

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

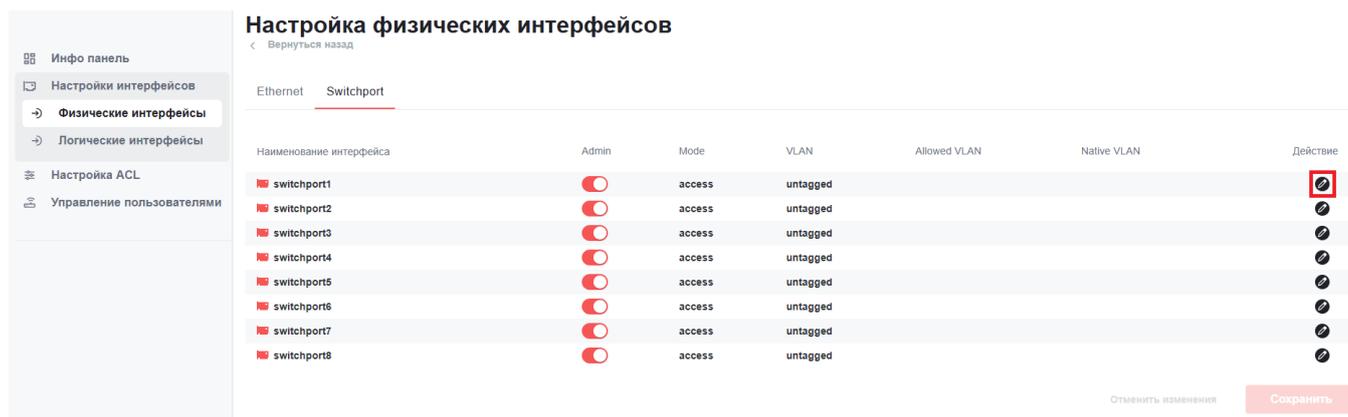


Рисунок 81 – Switchport интерфейс пиктограмма изменить

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

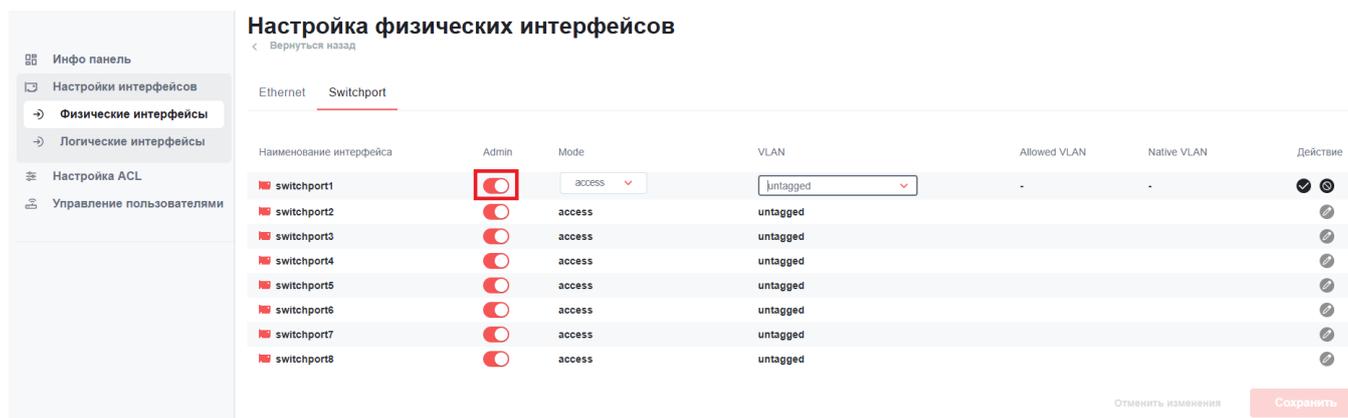


Рисунок 82 – Изменение административного статуса интерфейса

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

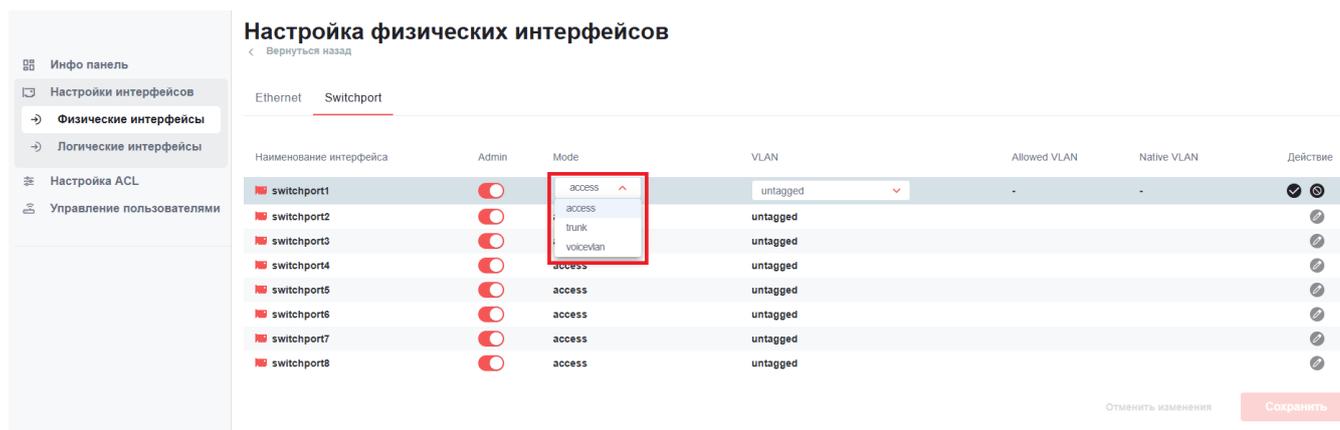


Рисунок 83 – Настройка работы VLAN

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

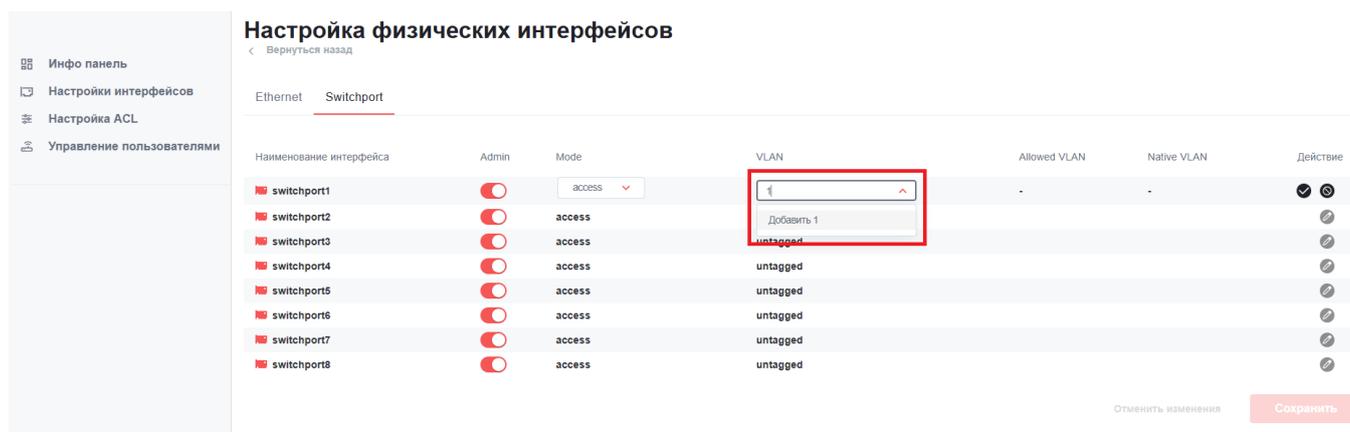


Рисунок 84 – Назначение VLAN интерфейса

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).

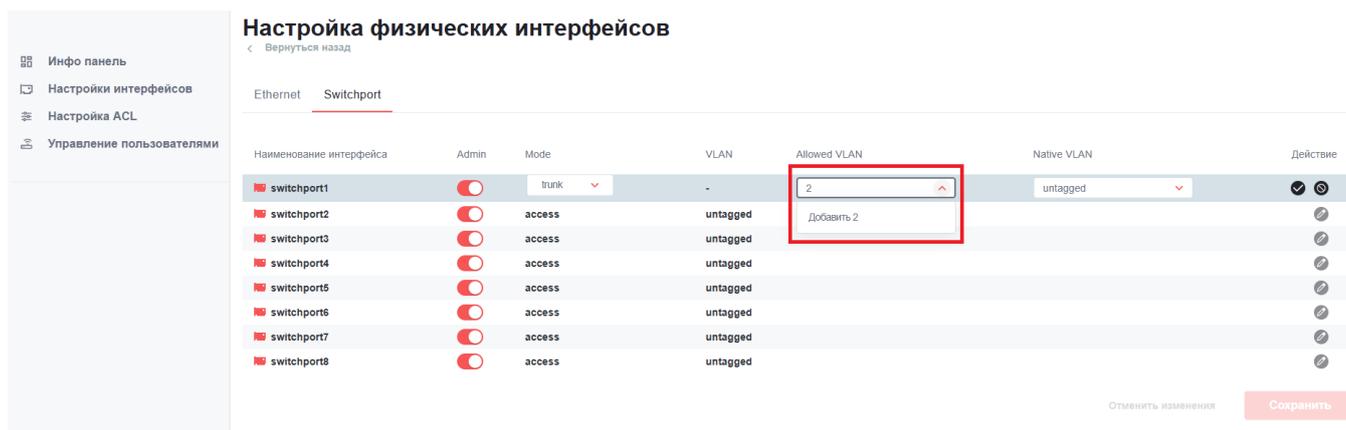


Рисунок 85 – Настройка транкового порта

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

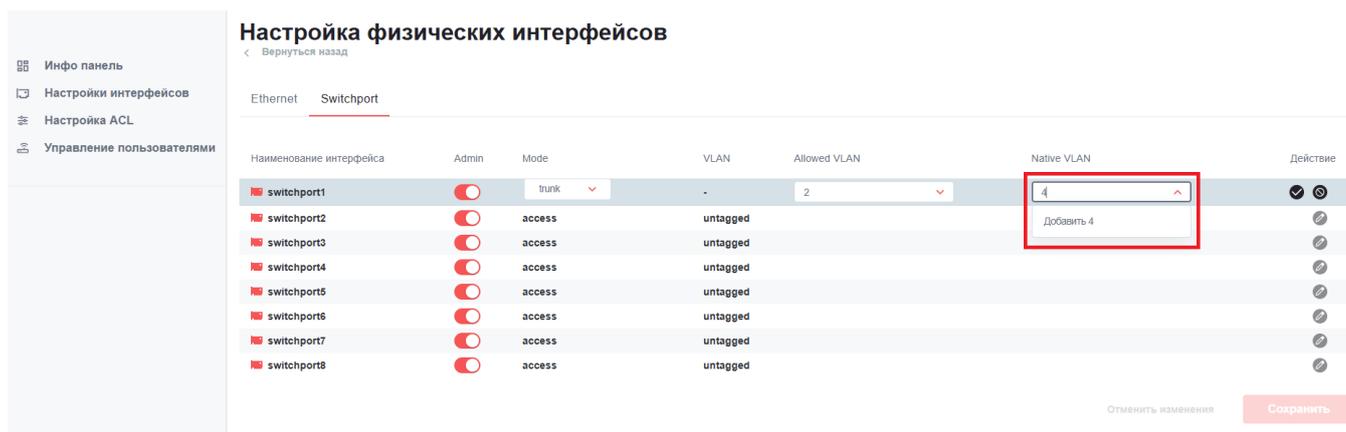


Рисунок 86 – Настройка Native VLAN

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

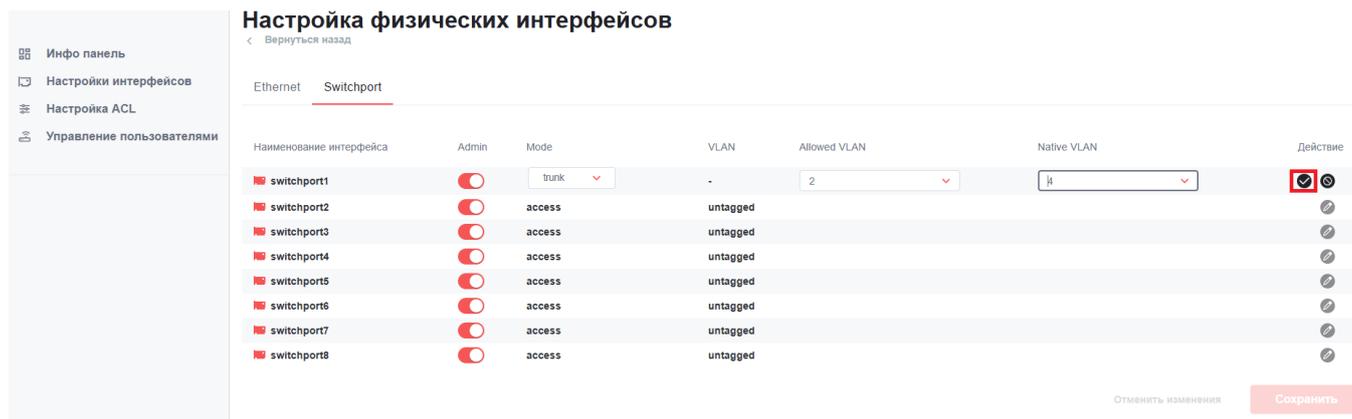


Рисунок 87 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 88).

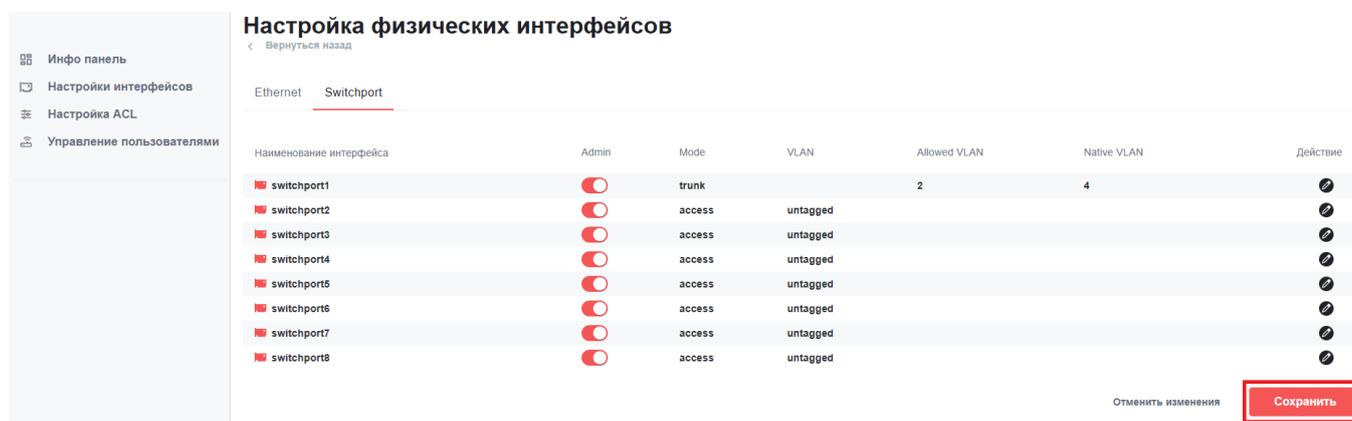


Рисунок 88 – Сохранение настроек

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

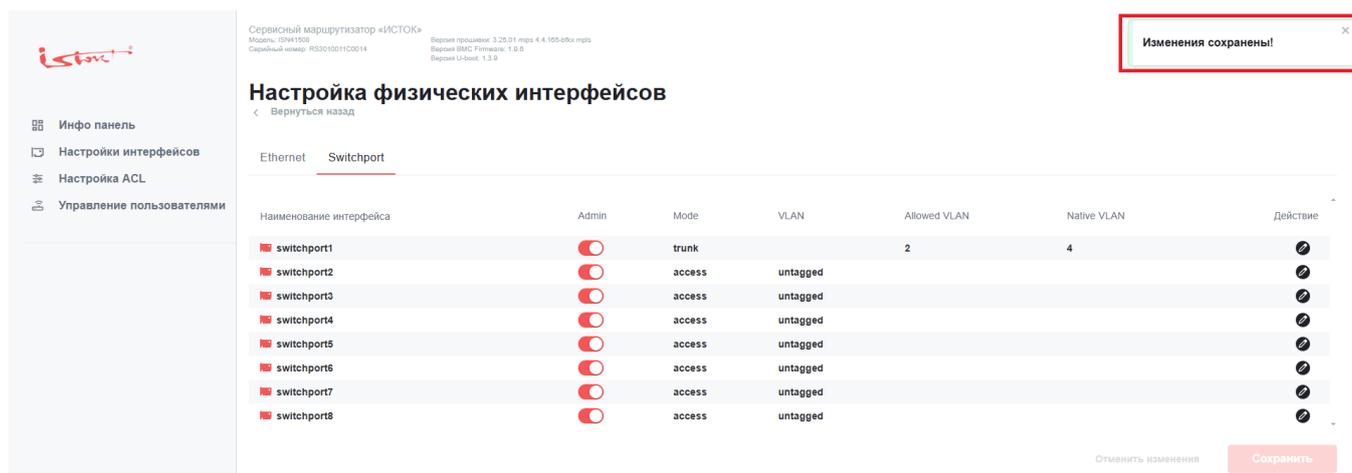


Рисунок 89 – Подтверждение сохранения

5.3 Настройка логических интерфейсов

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

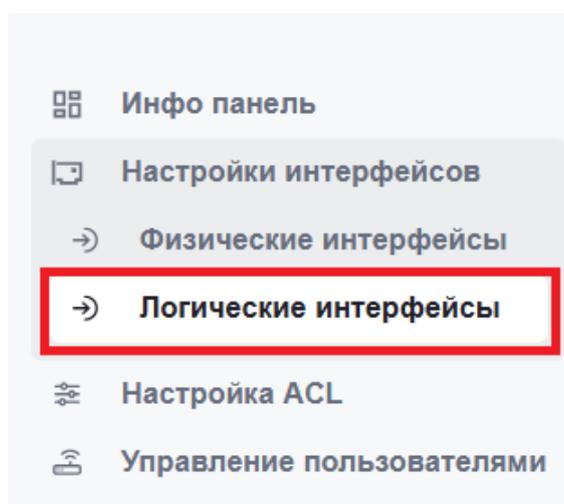


Рисунок 90 – Выбор пункта "Физические интерфейсы"

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

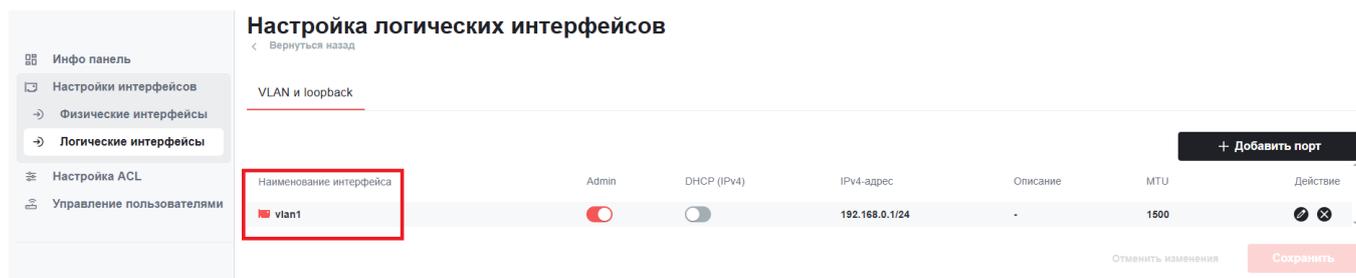


Рисунок 91 – Наименование интерфейсов

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

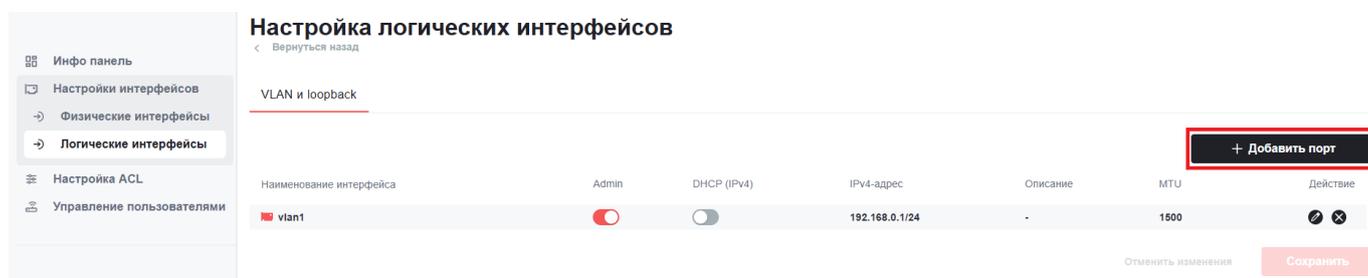


Рисунок 92 – Наименование интерфейсов

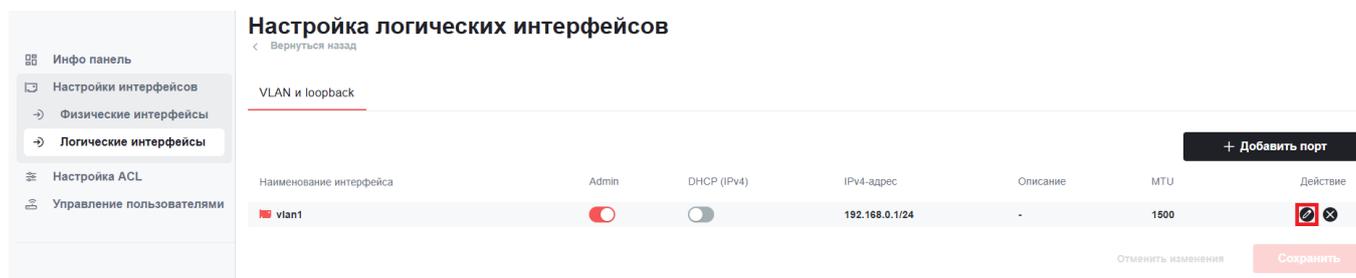


Рисунок 93 – Логический интерфейс пиктограмма изменить

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

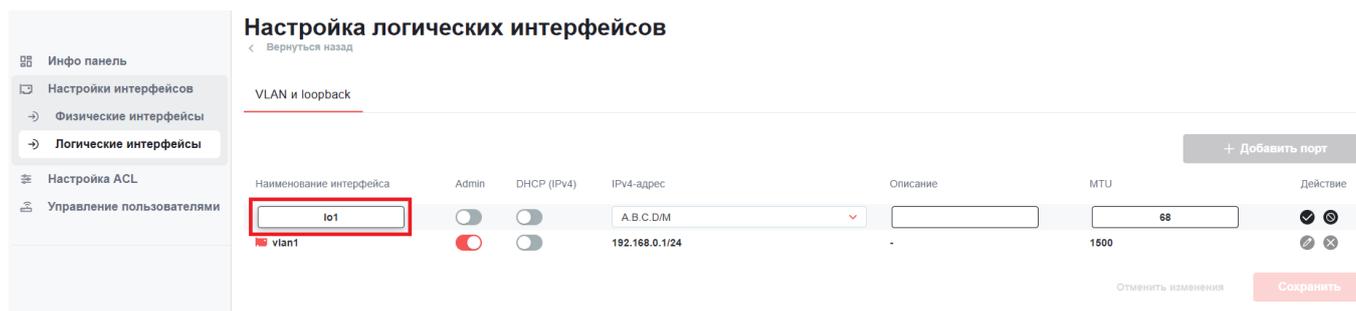


Рисунок 94 – Заполнение наименования интерфейса

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

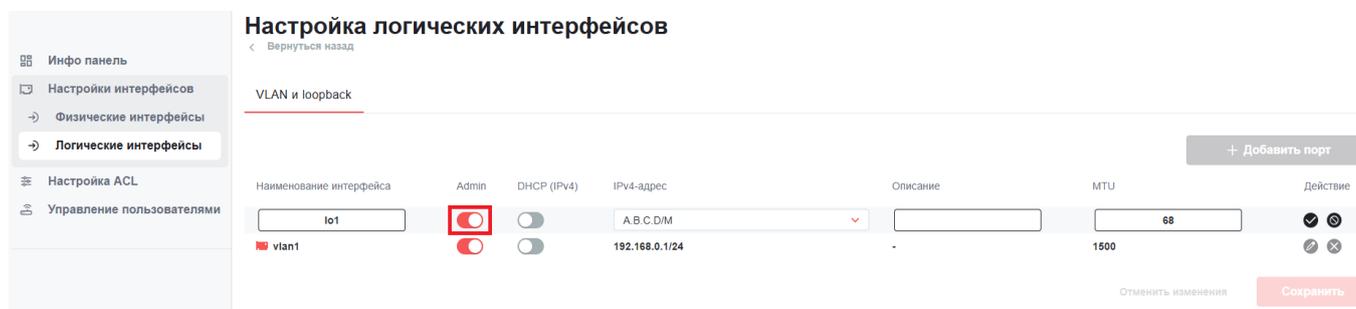


Рисунок 95 – Изменение административного статуса интерфейса

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

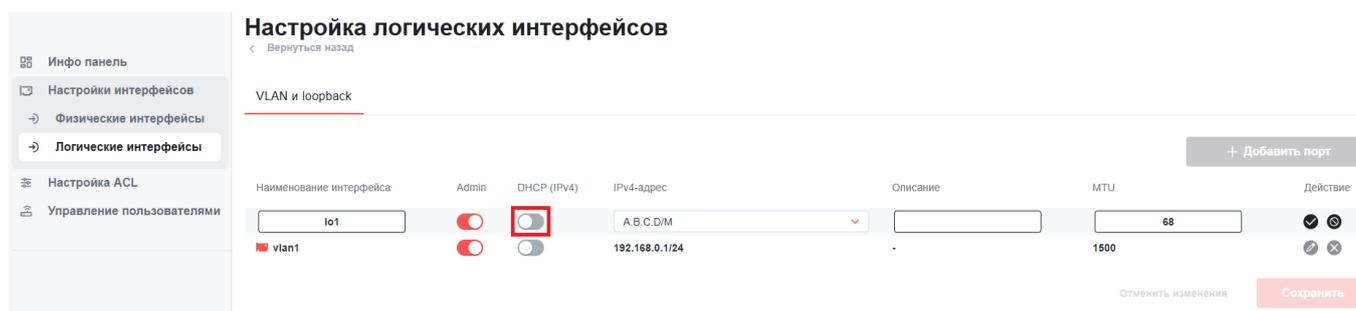


Рисунок 96 – Настройка DHCP клиента

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

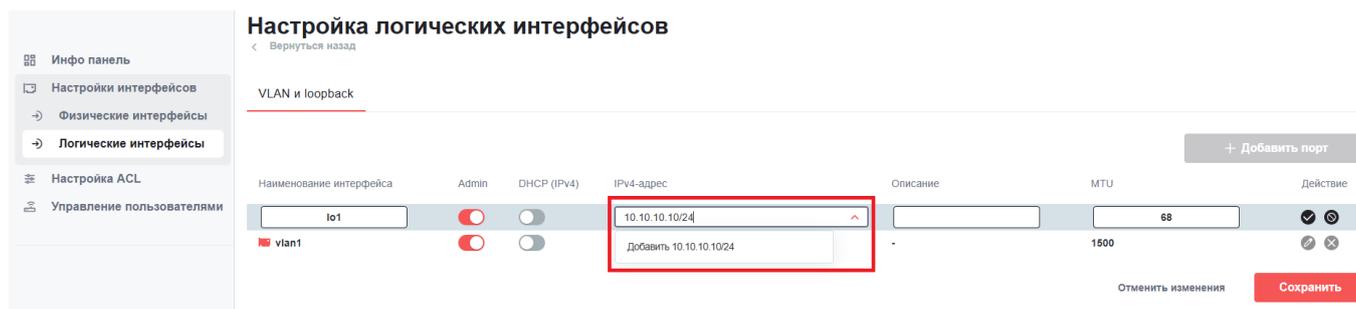


Рисунок 97 – Добавление IP-адреса

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).

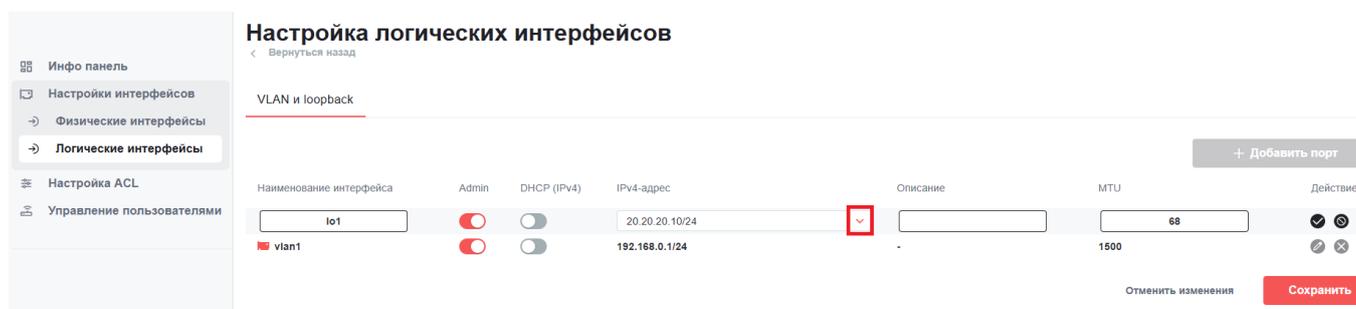


Рисунок 98 – Просмотр IP-адресов на интерфейсе

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

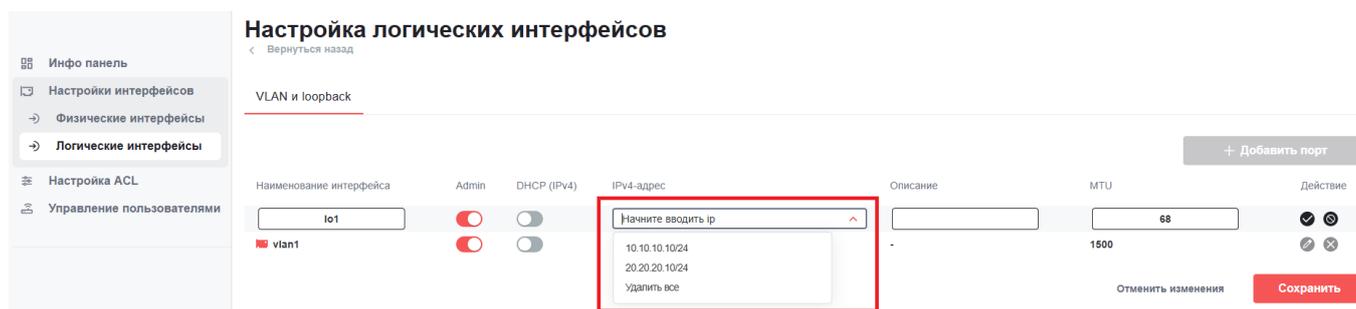


Рисунок 99 – Удаление IP-адресов

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

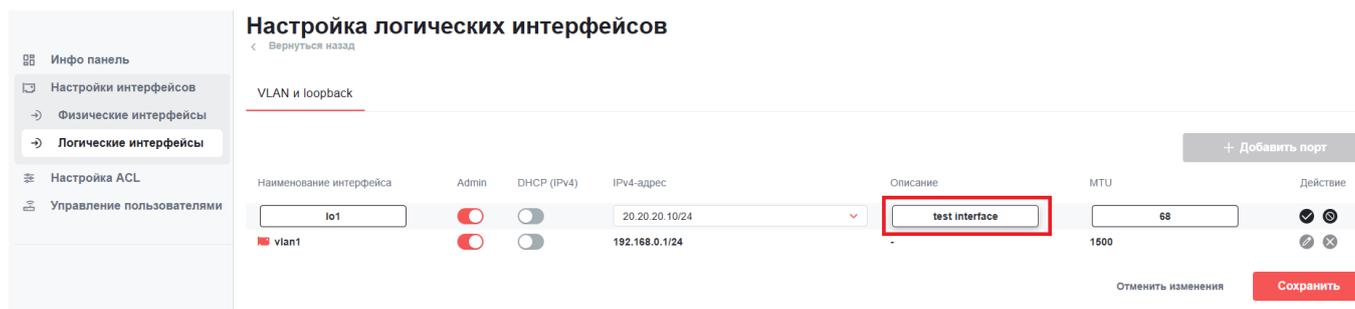


Рисунок 100 – Добавление описания интерфейсу

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

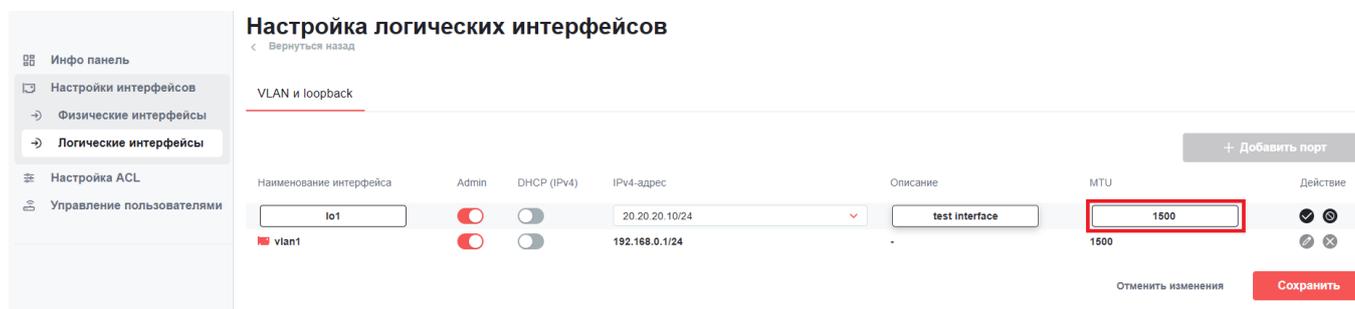


Рисунок 101 – Настройка MTU

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

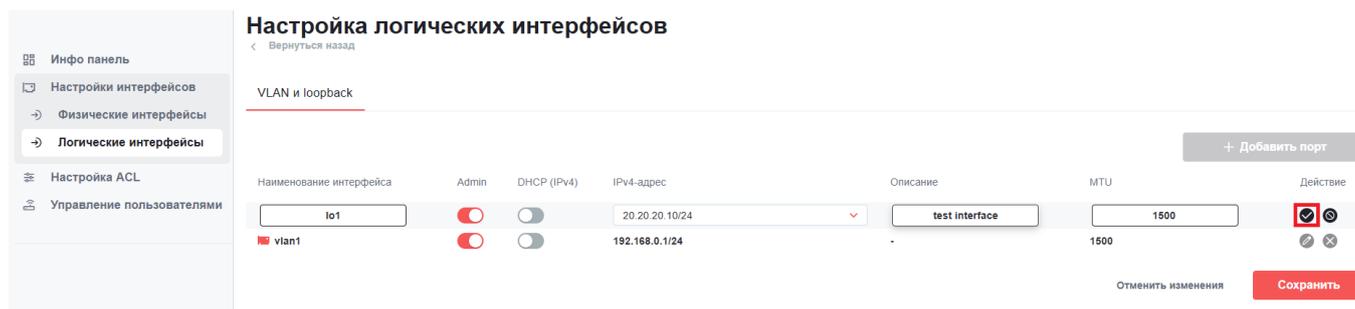


Рисунок 102 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 103).

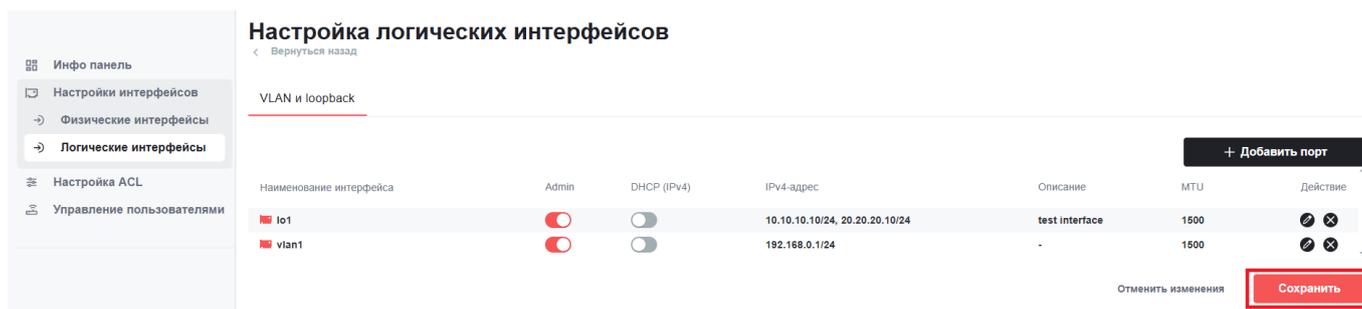


Рисунок 103 – Сохранение настроек

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

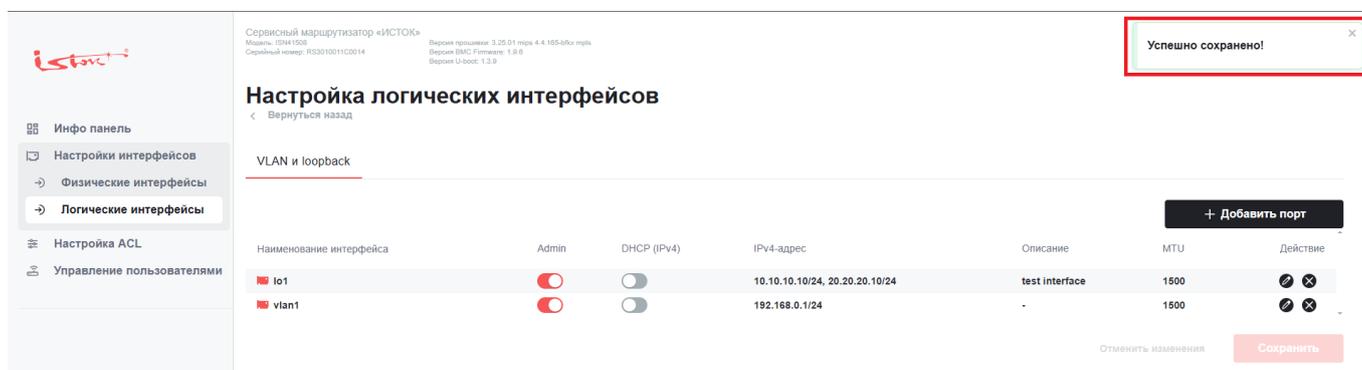


Рисунок 104 – Подтверждение сохранения

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

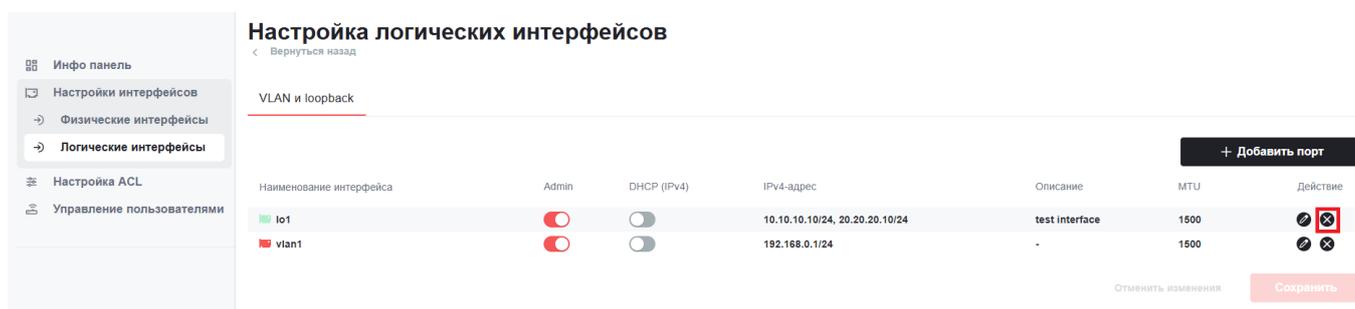


Рисунок 105 – Удаление интерфейса

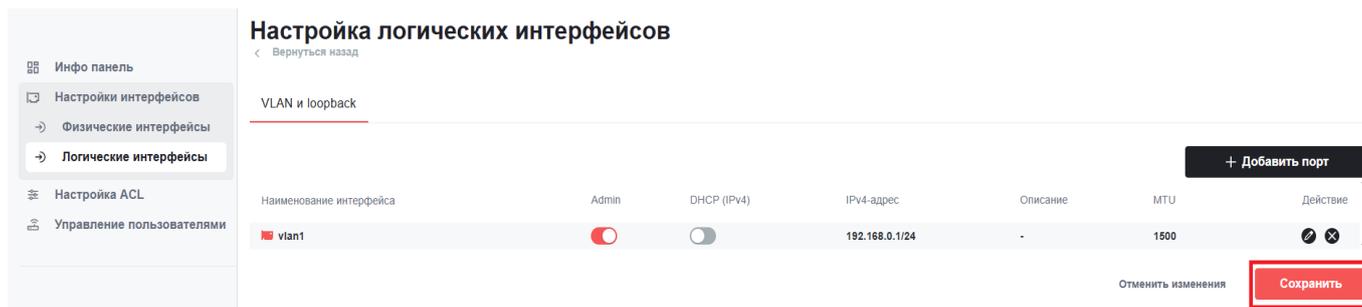


Рисунок 106 – Сохранение настроек

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

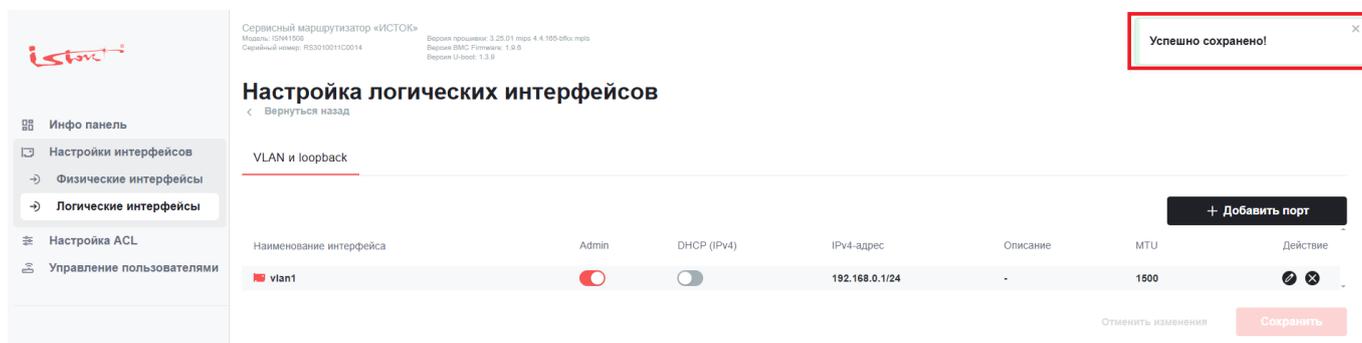


Рисунок 107 – Подтверждение сохранения

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).

Службный маршрутизатор «ИСТОК»
Модель: ISM1508
Серийный номер: R53010011C0014
Версия прошивки: 3.25.01 mips 4.4.165-bfco mips
Версия BMC Firmware: 1.0.0
Версия UI-Shell: 1.3.0

admin | Выйти

Access Control List для IPv4

list_name	rules	Действие
private_segment	1 source_subnet: 188.18.10.1/32, tos_value: 32, logging: true 2 dpi_protocol: activation, time_range: working_hours	⊗ ⊗ ⊗ ⊗
no_activation	1 dpi_protocol: activation	⊗ ⊗ ⊗ ⊗

Отменить изменения | Сохранить

Access Control List для IPv6

list_name	rules	Действие
-----------	-------	----------

Отменить изменения | Сохранить

Конфигурация time-range

Name	Datstart	Datestop	Timestart	Timetop	Monthdays	Weekdays	Действие
working_hours	-	-	09:00:00	18:00:00	-	Пн, Вт, Ср, Чт, Пт	⊗ ⊗

Отменить изменения | Сохранить

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).

The screenshot displays the Mikrotik web interface for configuring ACLs. On the left is a sidebar with a menu including 'Инфо панель', 'Настройки интерфейсов', 'Настройка ACL' (with sub-items: Filter, Mangle, NAT, PBR), and 'Управление пользователями'. The main area is divided into three sections:

- Access Control List для IPv4:** A table with columns 'list_name' and 'rules'. A red box highlights the '+ Добавить ACL IPv4' button. Below the table are 'Отменить изменения' and 'Сохранить' buttons.
- Access Control List для IPv6:** A table with columns 'list_name' and 'rules'. A red box highlights the '+ Добавить ACL IPv6' button. Below the table are 'Отменить изменения' and 'Сохранить' buttons.
- Конфигурация time-range:** A table with columns: Name, Datestart, Datestop, Timestart, Timestop, Monthdays, Weekdays, and Действие. A red box highlights the '+ Добавить time-range' button. Below the table are 'Отменить изменения' and 'Сохранить' buttons.

Рисунок 109 – Добавление списка управления доступом

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

Access Control List для IPv4

< Вернуться назад

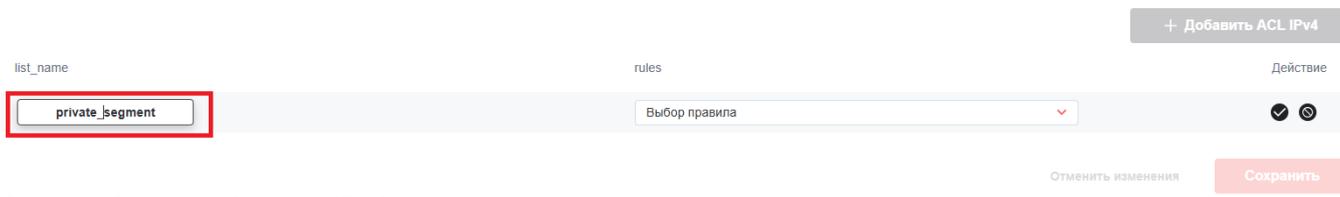


Рисунок 110 – Наименование списка контроля доступа

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

Access Control List для IPv4

< Вернуться назад

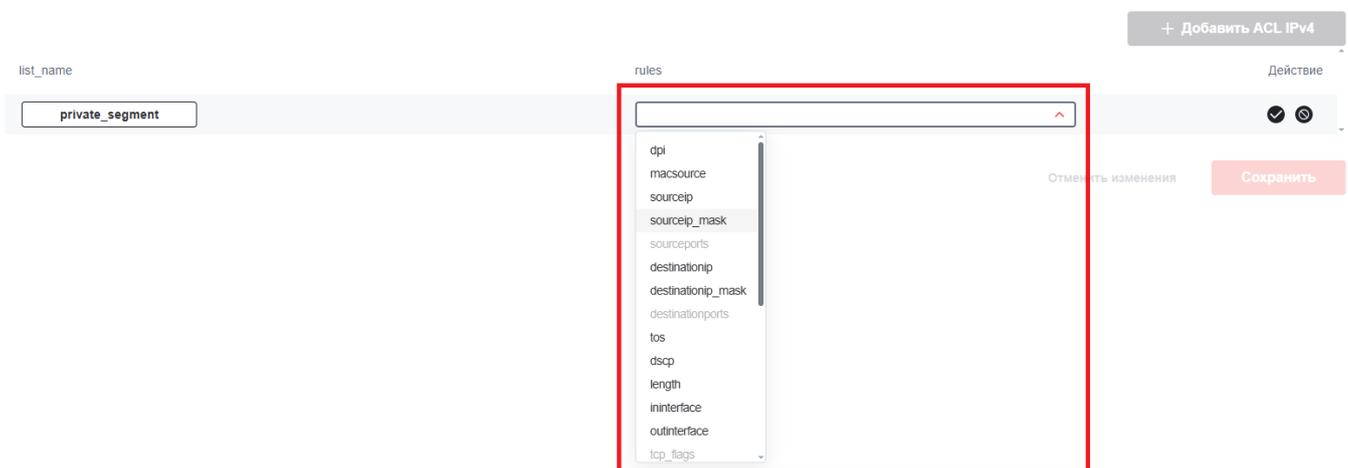


Рисунок 111 – Выбор правил

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

Access Control List для IPv4

< Вернуться назад

+ Добавить ACL IPv4

list_name	rules	Действие
private_segment	dscp tos <input type="checkbox"/> NOT tos_value <input type="text"/> dscp <input type="checkbox"/> NOT dscp_value <input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
	time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/>	

Отменить изменения Сохранить

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).

Access Control List для IPv4

< Вернуться назад

+ Добавить ACL IPv4

list_name	rules	Действие
private_segment	sourceip sourceip <input type="checkbox"/> NOT source_subnet 198.18.10.1/32 tos <input type="checkbox"/> NOT tos_value 32	<input checked="" type="checkbox"/> <input type="checkbox"/>
	time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/>	

Отменить изменения Сохранить

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).

Access Control List для IPv4

< Вернуться назад

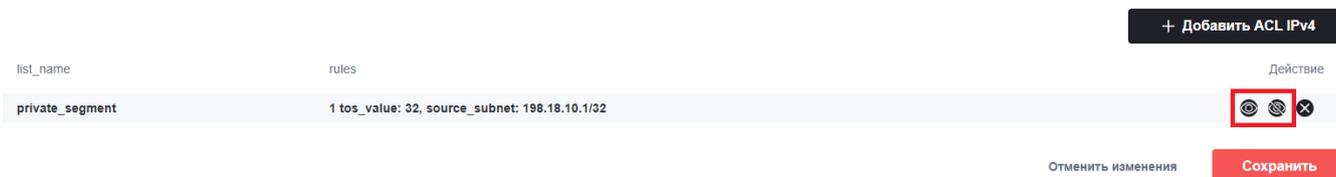


Рисунок 114 – Выбор занесения срабатывания правила в лог

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

Access Control List для IPv4

< Вернуться назад

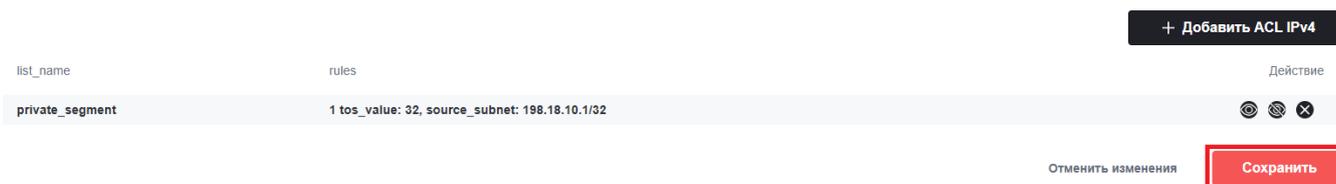


Рисунок 115 – Сохранение списка

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

Access Control List для IPv4

< Вернуться назад

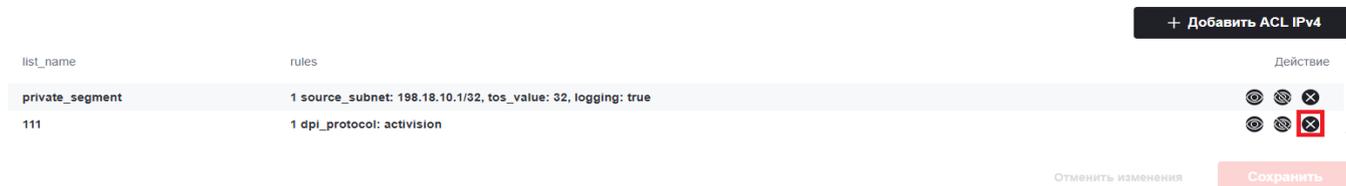


Рисунок 116 – Удаление списка управления доступом

Access Control List для IPv4

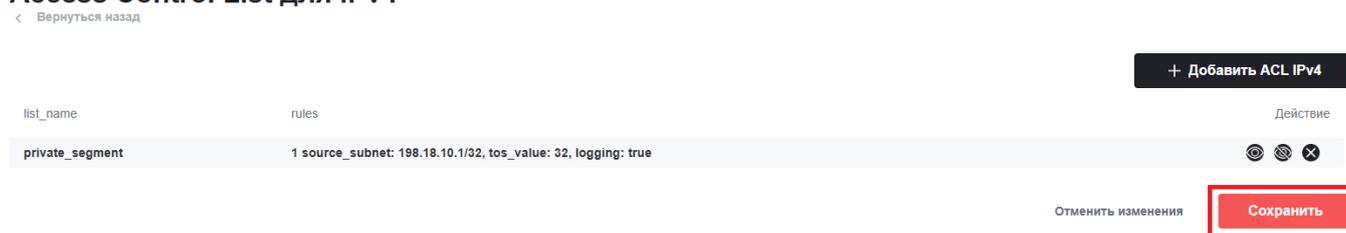


Рисунок 117 – Сохранение настроек

6.2 Настройка конфигурации time-range

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

Конфигурация time-range

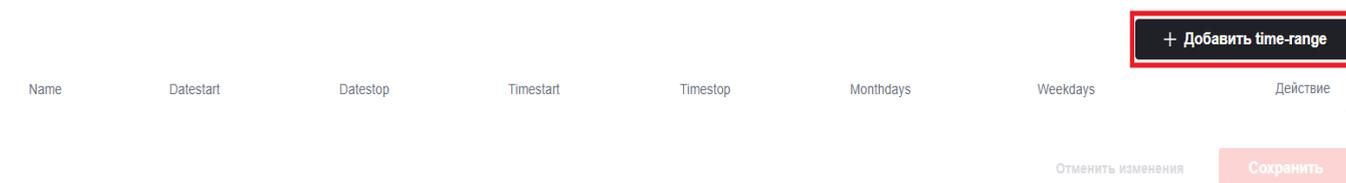


Рисунок 118 – Добавление списка управления доступом

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

Конфигурация time-range

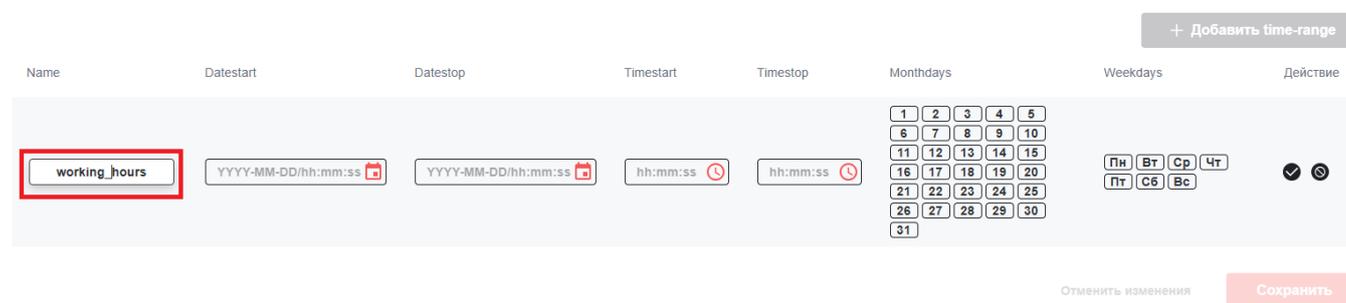


Рисунок 119 – Наименование списка контроля доступом

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.

Конфигурация time-range

Рисунок 120 – Настройка временного диапазона

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

Конфигурация time-range

Рисунок 121 – Подтверждение создания списка

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

Конфигурация time-range

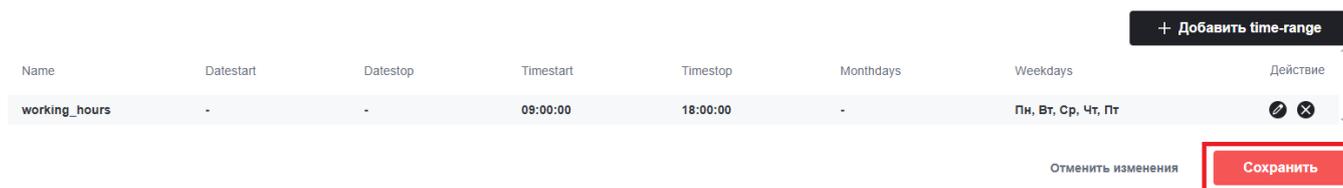


Рисунок 122 – Сохранение списка

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

Конфигурация time-range

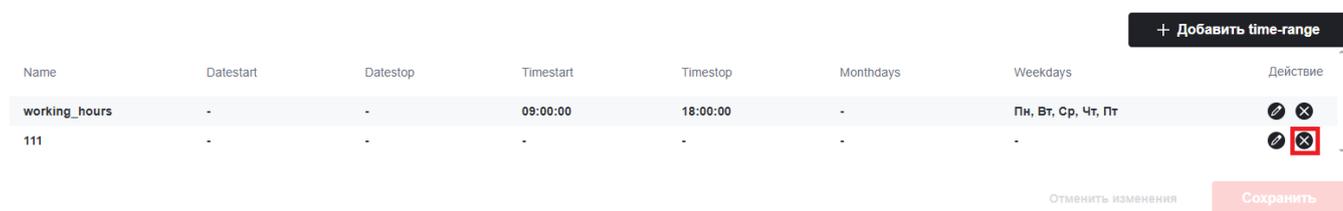


Рисунок 123 – Удаление расписания

Конфигурация time-range

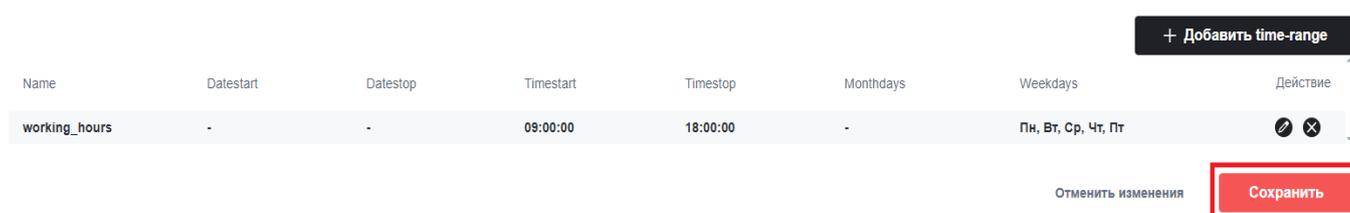


Рисунок 124 – Сохранение настроек

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.

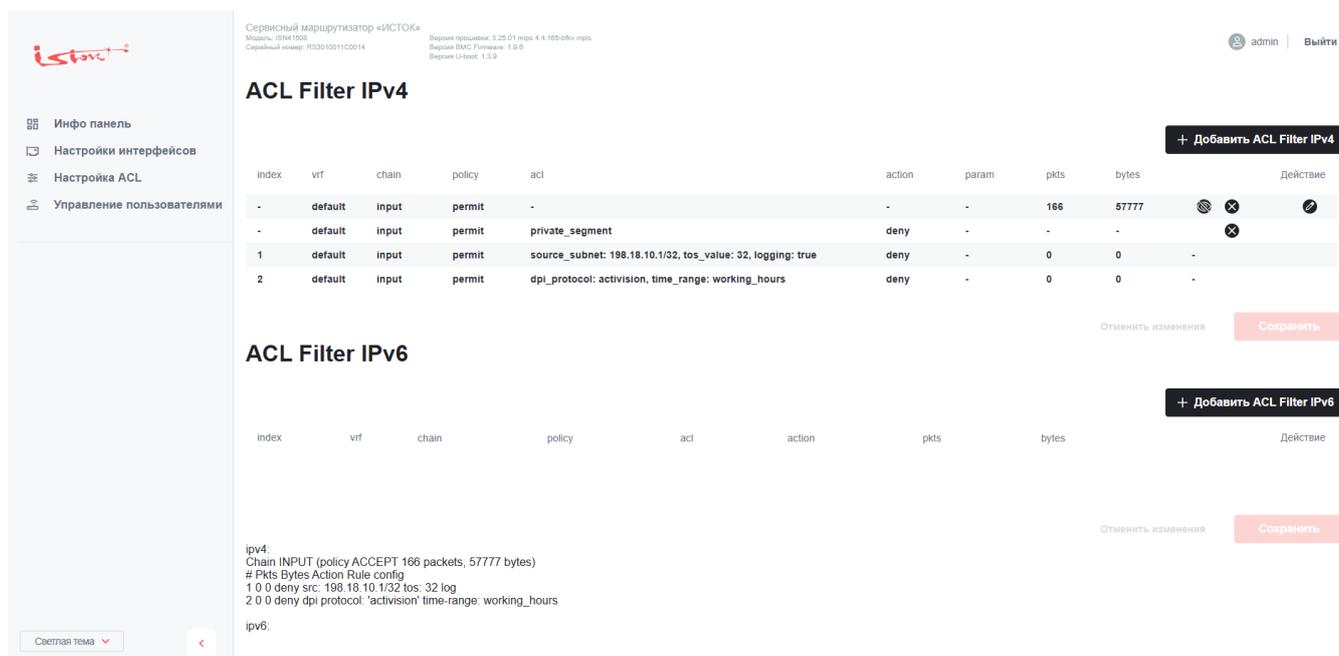


Рисунок 125 – Внешний вид вкладки "Filter"

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

ACL Filter IPv4

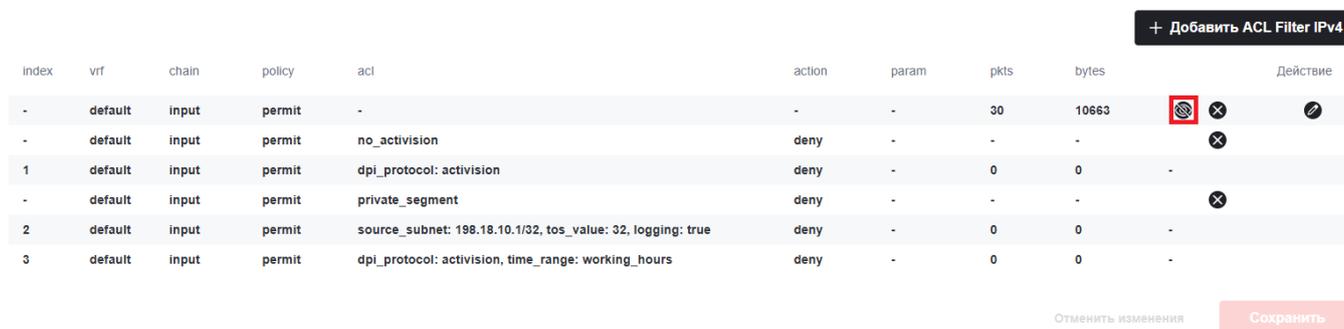


Рисунок 126 – Сброс статистики

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

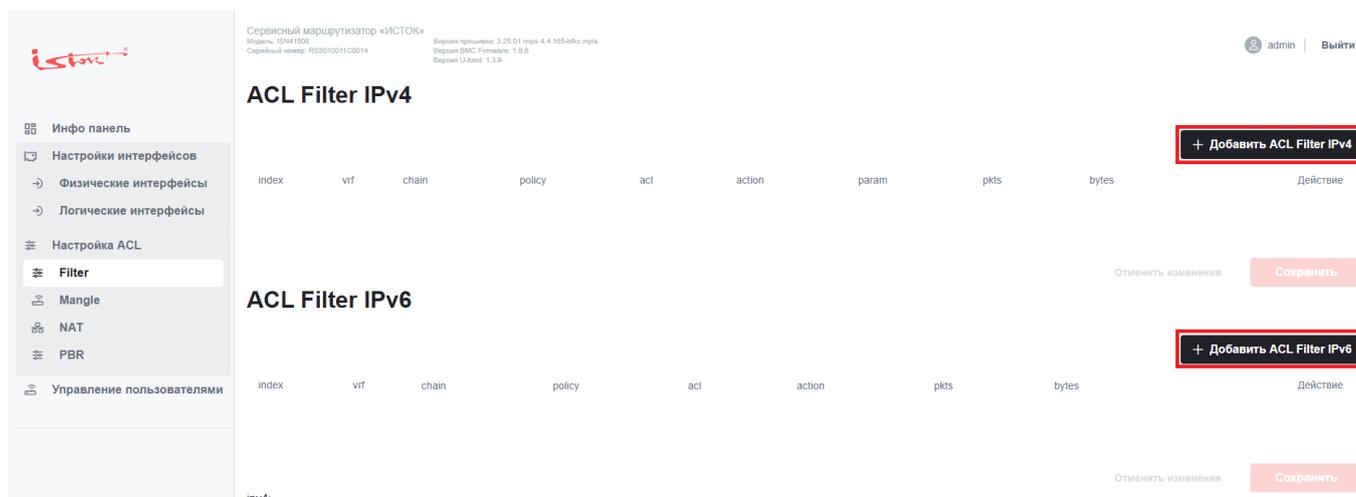


Рисунок 127 – Добавление списка управления доступом

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

ACL Filter IPv4

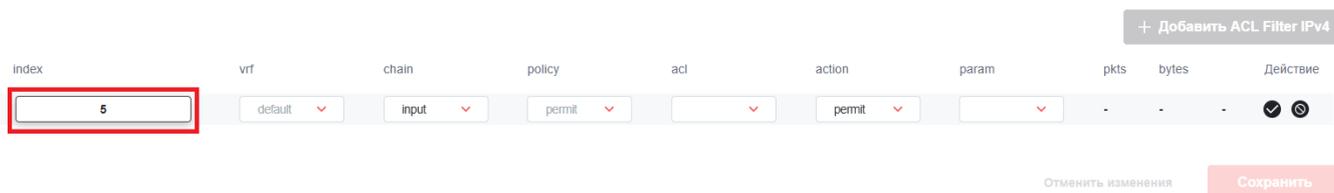


Рисунок 128 – Индекс ACL Filter

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.

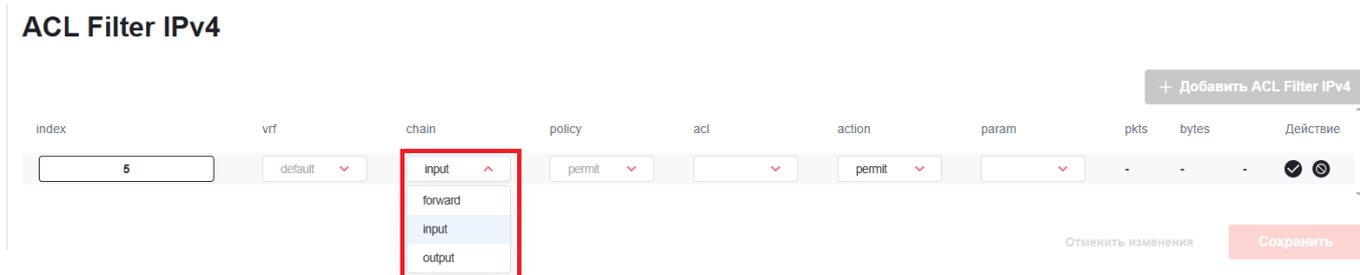


Рисунок 129 – Выбор типа пакетов

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).

ACL Filter IPv4



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.

ACL Filter IPv4

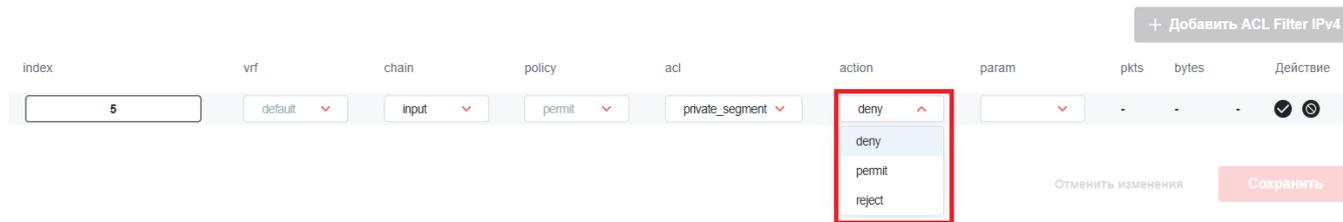


Рисунок 131 – Действия при срабатывании правила

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).

ACL Filter IPv4



Рисунок 132 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 133).

ACL Filter IPv4

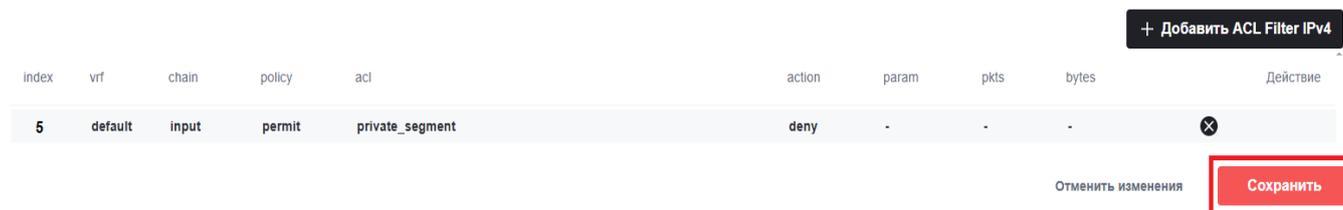


Рисунок 133 – Сохранение фильтра

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).

ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
-	default	input	permit	-	-	-	166	57777	
-	default	input	permit	private_segment	deny	-	-	-	
1	default	input	permit	source_subnet: 198.18.10.1/32, tos_value: 32, logging: true	deny	-	0	0	-
2	default	input	permit	dpi_protocol: activision, time_range: working_hours	deny	-	0	0	-

Отменить изменения Сохранить

Рисунок 134 – Список фильтров

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

ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
-	default	input	permit	-	-	-	30	10663	
-	default	input	permit	no_activision	deny	-	-	-	
1	default	input	permit	dpi_protocol: activision	deny	-	0	0	-
-	default	input	permit	private_segment	deny	-	-	-	
2	default	input	permit	source_subnet: 198.18.10.1/32, tos_value: 32, logging: true	deny	-	0	0	-
3	default	input	permit	dpi_protocol: activision, time_range: working_hours	deny	-	0	0	-

Отменить изменения Сохранить

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).

ACL Mangle IPv4



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 определяют порядок срабатывания правил (чем меньше значение индекса, тем раньше будет применено правило, и последующие правила не будут действовать на данный пакет) (рисунок 139).

ACL Mangle IPv4



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.

ACL Mangle IPv4

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).

ACL Mangle IPv4

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.

ACL Mangle IPv4

The screenshot shows the configuration interface for ACL Mangle IPv4. The 'action' dropdown menu is open, displaying a list of actions: clone, deny, permit, set-clamp-mss, set-dscp, set-mark, set-mss, set-skb-prio (highlighted with a red box), and set-tos. The 'index' field is set to 5, 'vrf' is default, 'chain' is forward, 'policy' is permit, and 'acl' is no_activation. The 'paramOne' and 'paramTwo' fields are empty. The 'Action' column shows a checkmark and a refresh icon. Buttons for 'Отменить изменения' and 'Сохранить' are visible at the bottom right.

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).

ACL Mangle IPv4

The screenshot shows the configuration interface for ACL Mangle IPv4. The 'paramOne' and 'paramTwo' input fields are highlighted with a red box and contain the values '0x2' and '0x6' respectively. The 'action' dropdown is set to 'set-skb-prio'. The 'index' field is set to 5, 'vrf' is default, 'chain' is input, 'policy' is permit, and 'acl' is no_activation. The 'Action' column shows a checkmark and a refresh icon. Buttons for 'Отменить изменения' and 'Сохранить' are visible at the bottom right.

Рисунок 143 – Заполнение параметров маркировки

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

ACL Mangle IPv4

+ Добавить ACL Mangle IPv4

index	vrf	chain	policy	acl	action	paramOne	paramTwo	pkts	bytes	Действие
5	default	input	permit	no_activision	set-skb-prio	0x2	0x6	-	-	

Отменить изменения Сохранить

Рисунок 144 – Подтверждение создания списка маркировки

Затем нажмите клавишу "Сохранить" (рисунок 145).

ACL Mangle IPv4

+ Добавить ACL Mangle IPv4

index	vrf	chain	policy	acl	action	paramOne	paramTwo	pkts	bytes	Действие
5	default	output	permit	no_activision	set-skb-prio	major: 0x2	minor: 0x4	-	-	-

Отменить изменения Сохранить

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).

ACL Mangle IPv4

+ Добавить ACL Mangle IPv4

index	vrf	chain	policy	acl	action	paramOne	paramTwo	pkts	bytes	Действие
-	default	output	permit	-	-	-	-	29	8281	  
-	default	output	permit	no_activision	set-skb-prio	major: 0x2	minor: 0x4	-	-	
1	default	output	permit	dpi_protocol: activision	set-skb-prio	major: 0x2	minor: 0x4	0	0	-

Отменить изменения Сохранить

Рисунок 146 – Списки маркировки

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

ACL Mangle IPv4

index	vrf	chain	policy	acl	action	paramOne	paramTwo	pkts	bytes	Действие
-	default	output	permit	-	-	-	-	29	8281	
-	default	output	permit	no_activision	set-skb-prio	major: 0x2	minor: 0x4	-	-	
1	default	output	permit	dpi_protocol: activision	set-skb-prio	major: 0x2	minor: 0x4	0	0	

[+ Добавить ACL Mangle IPv4](#)
[Отменить изменения](#) [Сохранить](#)

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.

Сервисный маршрутизатор «ИСТОК»
Модель: ISM41520
Серийный номер: RS3010011C0014

Версия прошивки: 3.25.01 ipra 4.4.155-8bfa ipra
Версия BMC Firmware: 1.9.9
Версия UI/Boot: 1.3.9

admin | Выйти

NAT Chains

Выбор VRF: default [Очистить статистику](#)

[+ Добавить chain NAT](#)

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	action
-	prerouting	default	-	<input type="checkbox"/>	-	-	<input type="checkbox"/>	-	-	
-	prerouting	default	nat	<input type="checkbox"/>	1.1.1.1	-	<input type="checkbox"/>	-	-	
1	prerouting	default	mac_address: aa:bb:cc:dd:ee:ff	<input type="checkbox"/>	-	-	<input type="checkbox"/>	-	-	-
2	prerouting	default	protocol_name: tcp, source_ports: 11:40	<input type="checkbox"/>	-	-	<input type="checkbox"/>	-	-	-
-	prerouting	default	established	<input type="checkbox"/>	1.1.1.1	-	<input type="checkbox"/>	-	-	
3	prerouting	default	established: true	<input type="checkbox"/>	-	-	<input type="checkbox"/>	-	-	-
-	prerouting	default	nat2	<input type="checkbox"/>	2.2.2.2	80	<input type="checkbox"/>	-	-	
4	prerouting	default	protocol_name: tcp, source_ports: 11:40	<input type="checkbox"/>	-	-	<input type="checkbox"/>	-	-	-

[Отменить изменения](#) [Сохранить](#)

Рисунок 148 – Внешний вид вкладки "NAT"

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

NAT Chains



Рисунок 149 – Добавить списка подмены ip-адресов

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

NAT Chains

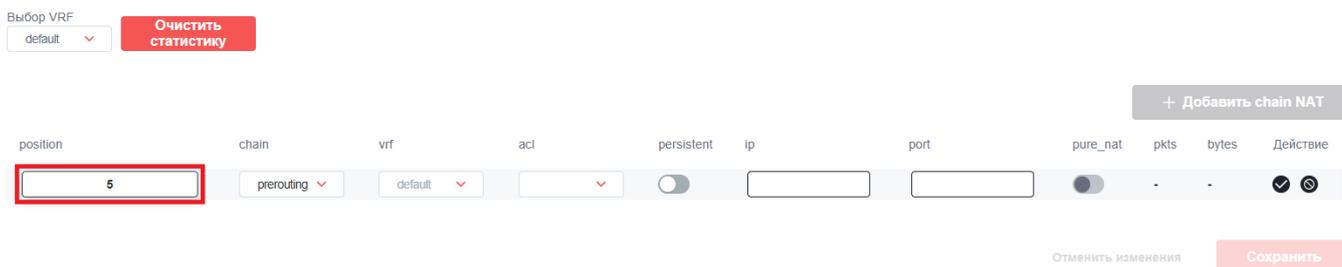


Рисунок 150 – Позиция ACL NAT

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.

NAT Chains

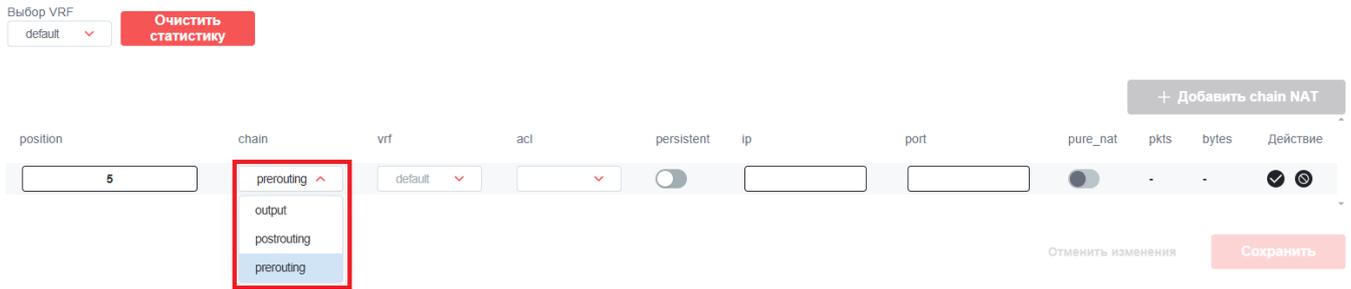


Рисунок 151 – Выбор типа пакетов

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

NAT Chains

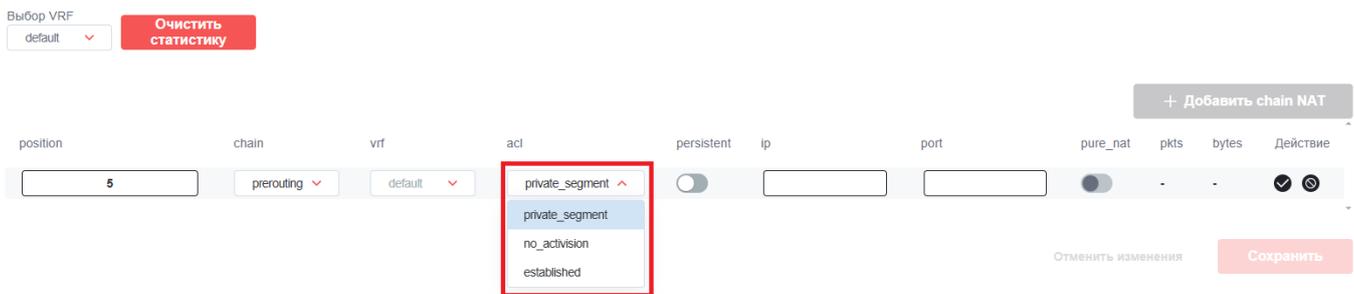


Рисунок 152 – Выбор списка контроля доступом

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).

NAT Chains

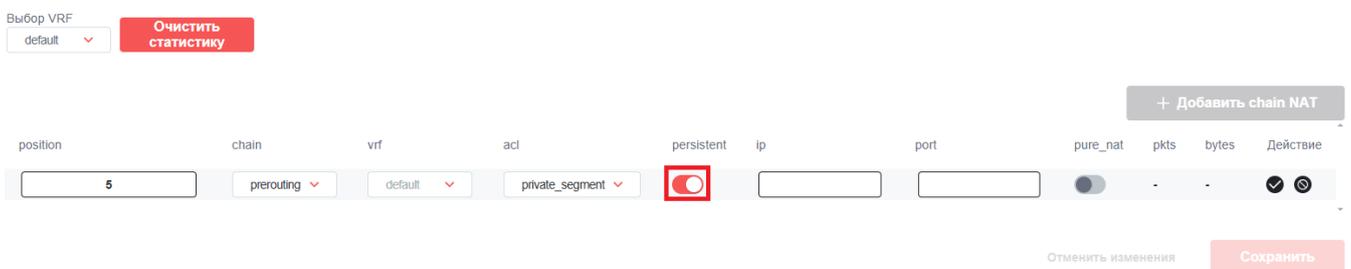


Рисунок 153 – Изменение статуса persisten

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

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	Действие
5	prerouting	default	private_segment	<input checked="" type="checkbox"/>	198.0.0.1-198.0.0.10 A.B.C.D или A.B.C.D-A.B.C.D		<input type="checkbox"/>	-	-	<input checked="" type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

Рисунок 154 – Добавление IP-адреса

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

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	Действие
5	prerouting	default	private_segment	<input type="checkbox"/>	198.0.0.1-198.0.0.10	22	<input type="checkbox"/>	-	-	<input checked="" type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

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).

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	Действие
5	prerouting	default	private_segment	<input type="checkbox"/>	198.0.0.1-198.0.0.10	22	<input checked="" type="checkbox"/>	-	-	<input checked="" type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

Рисунок 156 – Изменение статуса pure_nat

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

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	Действие
5	prerouting	default	private_segment	<input type="checkbox"/>	198.0.0.1-198.0.0.10	22	<input type="checkbox"/>	-	-	<input checked="" type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

Рисунок 157 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 158).

NAT Chains

Выбор VRF: default Очистить статистику

+ Добавить chain NAT

position	chain	vrf	acl	persistent	ip	port	pure_nat	pkts	bytes	action
5	postrouting	default	private_segment	<input type="checkbox"/>	198.0.0.1-198.0.0.100	22	<input type="checkbox"/>	-	-	-

Отменить изменения Сохранить

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).

ACL / PBR

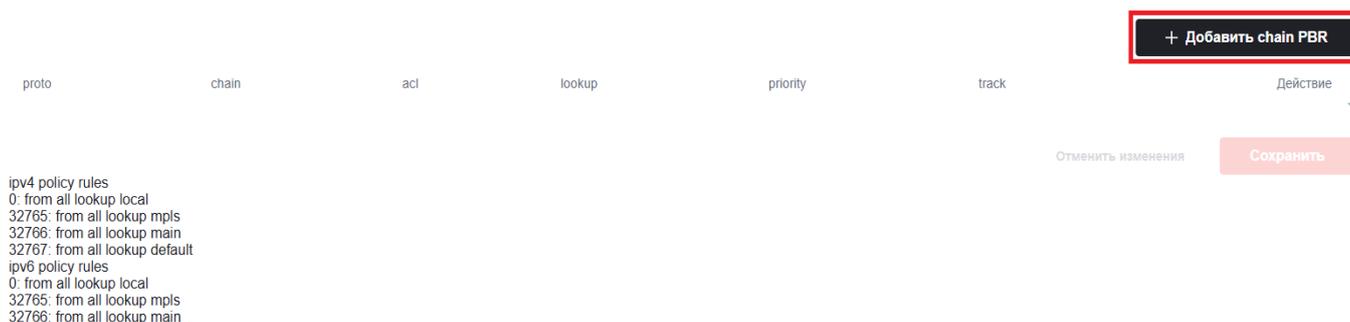


Рисунок 160 – Добавить политику маршрутизации

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

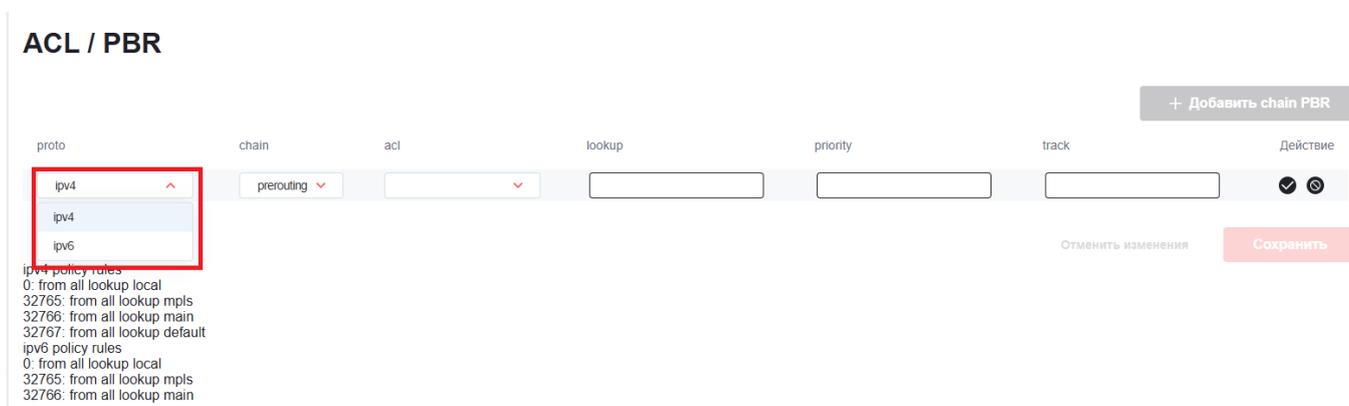


Рисунок 161 – Выбор протокола

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.

ACL / PBR

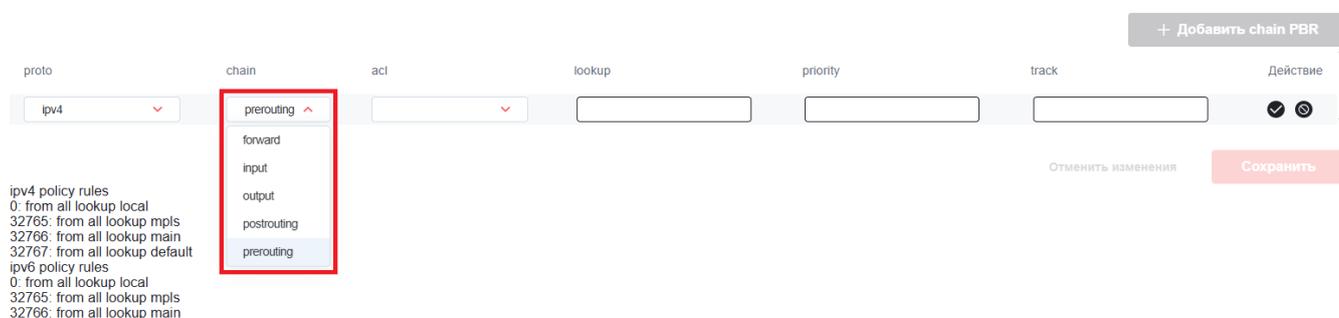


Рисунок 162 – Выбор типа пакетов

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

ACL / PBR

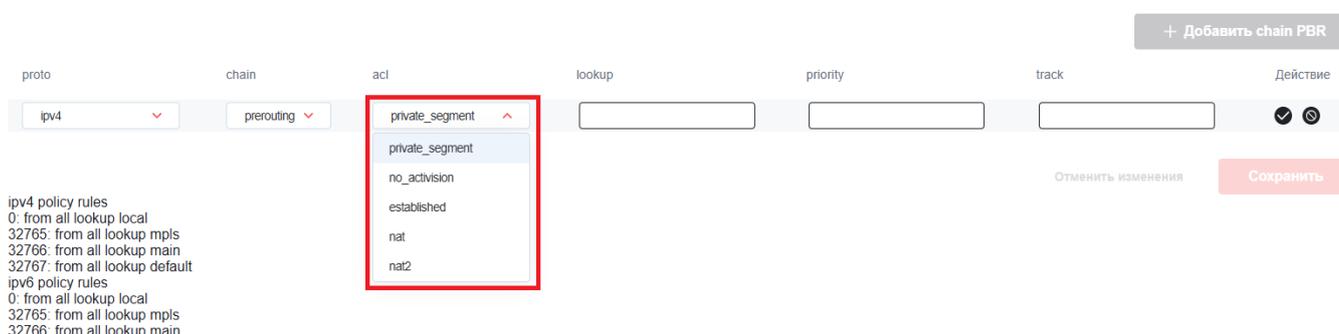


Рисунок 163 – Выбор списка контроля доступом

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

ACL / PBR

The screenshot shows a configuration form for ACL/PBR. The fields are: proto (ipv4), chain (prerouting), acl (private_segment), lookup (1), priority (empty), and track (empty). The 'lookup' field is highlighted with a red box. Below the form, there are buttons for 'Отменить изменения' and 'Сохранить', and a '+ Добавить chain PBR' button. A list of policy rules is visible on the left side of the form.

Рисунок 164 – Указание id-номера таблицы маршрутизации

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

ACL / PBR

The screenshot shows the same configuration form as in Figure 164, but now the 'priority' field is highlighted with a red box and contains the value '5'. The 'lookup' field still contains '1'. The rest of the interface remains the same.

Рисунок 165 – Позиция ACL NAT

При необходимости укажите трекер IP SLA (рисунок 166).

ACL / PBR

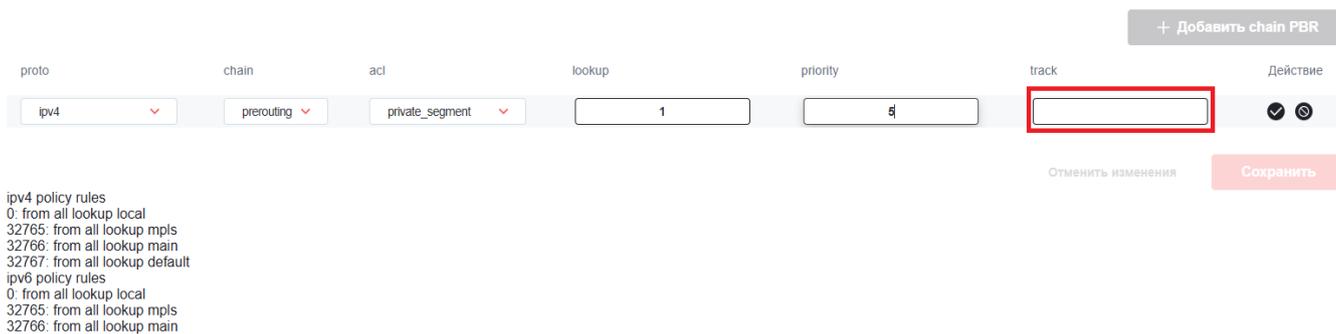


Рисунок 166 – Добавление порта

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

ACL / PBR



Рисунок 167 – Подтверждение настроек

Затем нажмите кнопку "Сохранить" (рисунок 168).

ACL / PBR

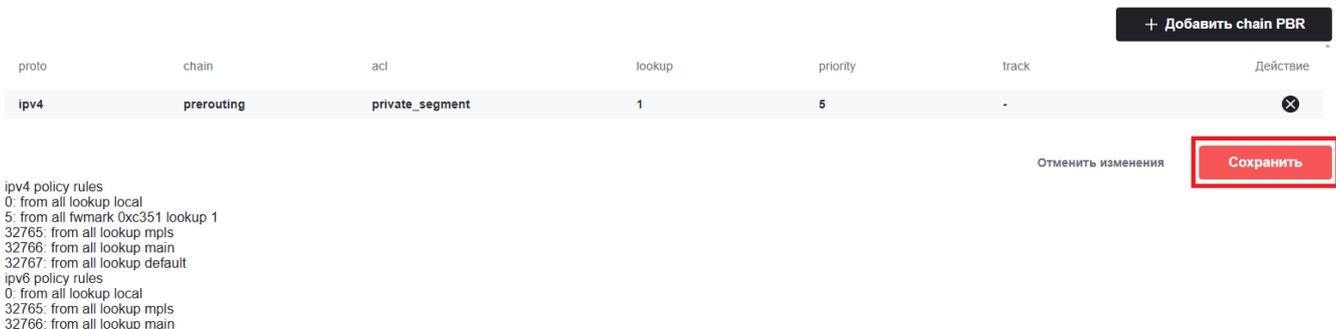


Рисунок 168 – Сохранение настроек

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).

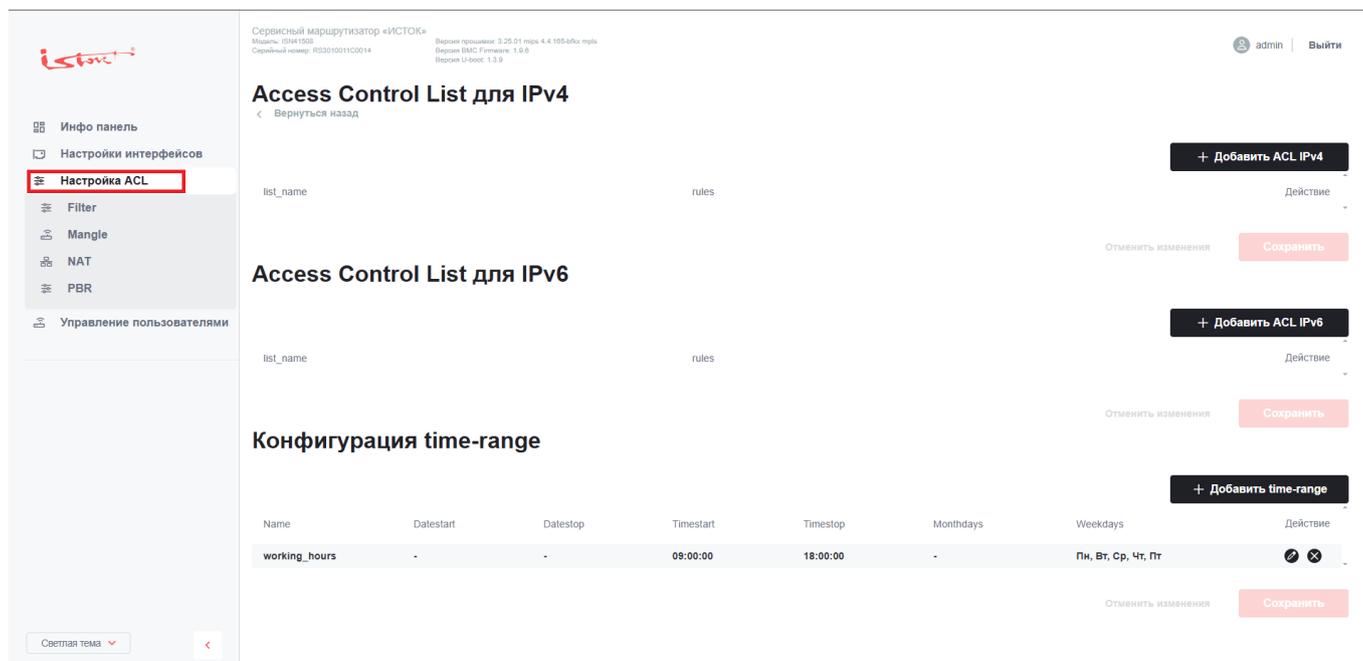


Рисунок 169 – Вкладка Настройки ACL

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

Access Control List для IPv4



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).

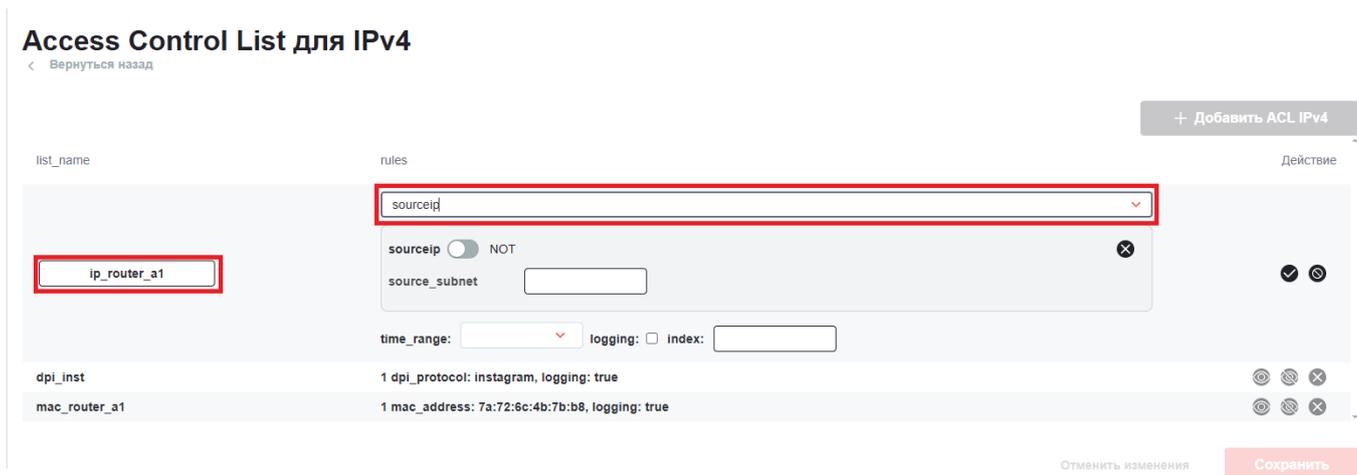


Рисунок 171 – Выбор правила

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

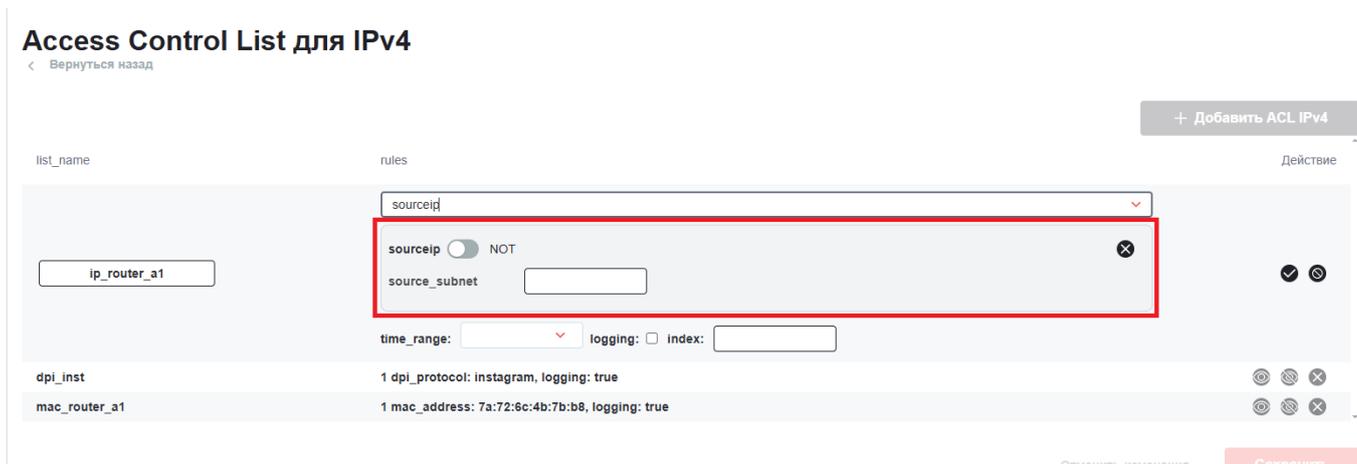


Рисунок 172 – Блок настройки правила

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).

Access Control List для IPv4

< Вернуться назад

+ Добавить ACL IPv4

list_name	rules	Действие
ip_router_a1	sourceip sourceip <input type="checkbox"/> NOT source_subnet 198.0.0.1/24 time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
mac_router_a1	1 mac_address: 7a:72:6c:4b:7b:b8, logging: true	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

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).

Access Control List для IPv4

< Вернуться назад

+ Добавить ACL IPv4

list_name	rules	Действие
ip_router_a1	sourceip sourceip <input type="checkbox"/> NOT source_subnet <input type="text" value="198.0.0.1/24"/> time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
mac_router_a1	1 mac_address: 7a:72:6c:4b:7b:b8, logging: true	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Отменить изменения Сохранить

Рисунок 174 – Подтверждение создания списка

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

Access Control List для IPv4

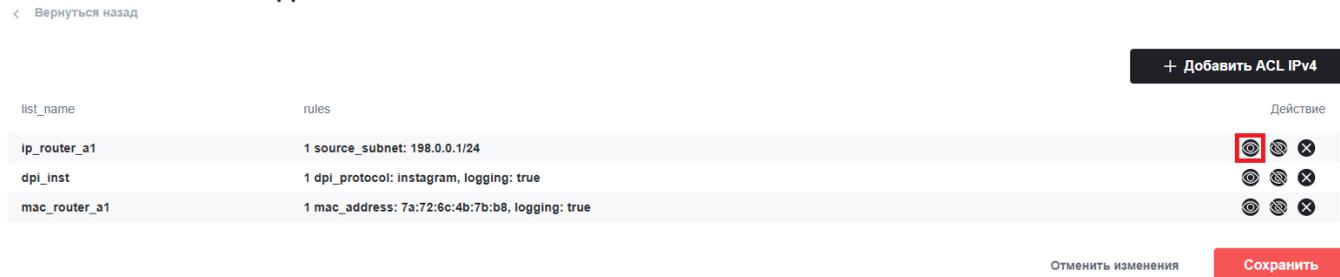


Рисунок 175 – Выбор занесения срабатывания правила в лог

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

Access Control List для IPv4

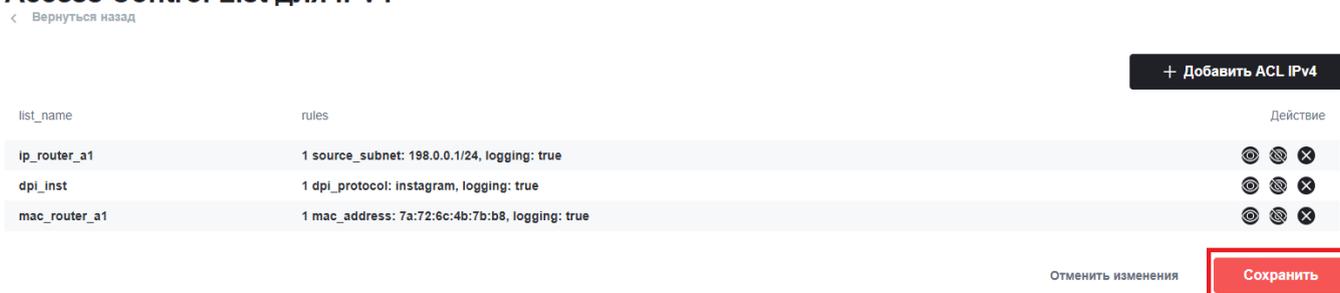


Рисунок 176 – Сохранение списка

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

Access Control List для IPv4



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).

ACL Filter IPv4



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).

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	ip_router_a1	deny		-	-	✓
-	default	forward	permit	-	-	-	0	0	⊗
-	default	forward	permit	mac_router_a1	deny	-	-	-	⊗
1	default	forward	permit	mac_address: 7a:72:6c:4b:7b:b8, logging: true	deny	-	0	0	-
-	default	forward	permit	dpi_inst	deny	-	-	-	⊗
2	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	-

Отменить изменения Сохранить

Рисунок 180 – Настройка фильтра

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

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	ip_router_a1	deny		-	-	✓
-	default	forward	permit	-	-	-	0	0	⊗
-	default	forward	permit	mac_router_a1	deny	-	-	-	⊗
1	default	forward	permit	mac_address: 7a:72:6c:4b:7b:b8, logging: true	deny	-	0	0	-
-	default	forward	permit	dpi_inst	deny	-	-	-	⊗
2	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	-

Отменить изменения Сохранить

Рисунок 181 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 176).

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	ip_router_a1	deny	-	-	-	✓
-	default	forward	permit	-	-	-	0	0	⊗
-	default	forward	permit	mac_router_a1	deny	-	-	-	⊗
1	default	forward	permit	mac_address: 7a:72:6c:4b:7b:b8, logging: true	deny	-	0	0	-
-	default	forward	permit	dpi_inst	deny	-	-	-	⊗
2	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	-

Отменить изменения Сохранить

Рисунок 182 – Сохранение фильтра

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

ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
-	default	forward	permit	-	-	-	0	0	
-	default	forward	permit	ip_router_a1	deny	-	-	-	
1	default	forward	permit	source_subnet: 198.0.0.0/24, logging: true	deny	-	0	0	
-	default	forward	permit	mac_router_a1	deny	-	-	-	
2	default	forward	permit	mac_address: 7a:72:6c:4b:7b:b8, logging: true	deny	-	0	0	
-	default	forward	permit	dpi_inst	deny	-	-	-	
3	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	

[Отменить изменения](#)
[Сохранить](#)

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).

The screenshot shows the Mikrotik WinBox interface for configuring ACLs. The left sidebar has 'Настройка ACL' highlighted. The main area is divided into three sections:

- Access Control List для IPv4:** Shows a table with columns 'list_name' and 'rules'. A '+ Добавить ACL IPv4' button is at the top right. Below the table are 'Отменить изменения' and 'Сохранить' buttons.
- Access Control List для IPv6:** Similar to the IPv4 section, with a '+ Добавить ACL IPv6' button and 'Отменить изменения'/'Сохранить' buttons.
- Конфигурация time-range:** Shows a table with columns: Name, Datestart, Datestop, Timestart, Timestop, Monthdays, Weekdays, and Действие. A row is visible for 'working_hours' with values: -, -, 09:00:00, 18:00:00, -, Пн, Вт, Ср, Чт, Пт. A '+ Добавить time-range' button is at the top right. Below the table are 'Отменить изменения' and 'Сохранить' buttons.

Рисунок 184 – Вкладка Настройки ACL

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

Access Control List для IPv4

< Вернуться назад



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).

Access Control List для IPv4

< Вернуться назад



Рисунок 186 – Выбор правила

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

Access Control List для IPv4

< Вернуться назад

The screenshot shows the configuration page for an IPv4 Access Control List. On the left, there is a dropdown menu for 'list_name' with 'mac_router_a1' selected. The main area is titled 'rules' and contains a configuration block for a rule named 'macsource'. This block is highlighted with a red border and includes a toggle switch for 'macsource' set to 'NOT', a text input field for 'mac_address', and a close button. Below the rule configuration, there are fields for 'time_range', 'logging' (checkbox), and 'index'. At the bottom, it shows '1 dpi_protocol: instagram, logging: true'. On the right side, there are icons for actions and a 'Сохранить' (Save) button.

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).

Access Control List для IPv4

< Вернуться назад

This screenshot is similar to the previous one, but the 'mac_address' field in the rule configuration block is now filled with the hexadecimal value '7a:72:6c:4b:7b:b8'. The 'macsource' toggle remains in the 'NOT' position. The rest of the interface, including the 'list_name' dropdown, 'time_range', 'logging' options, and the 'Сохранить' button, is identical to the previous screenshot.

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).

Access Control List для IPv4

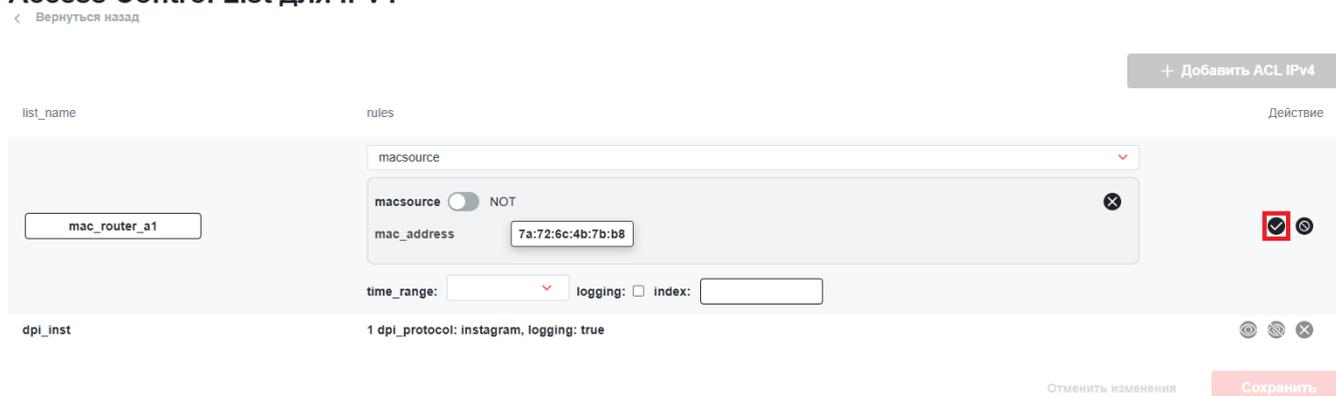


Рисунок 189 – Подтверждение создания списка

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

Access Control List для IPv4



Рисунок 190 – Выбор занесения срабатывания правила в лог

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

Access Control List для IPv4



Рисунок 191 – Сохранение списка

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

Access Control List для IPv4

< Вернуться назад

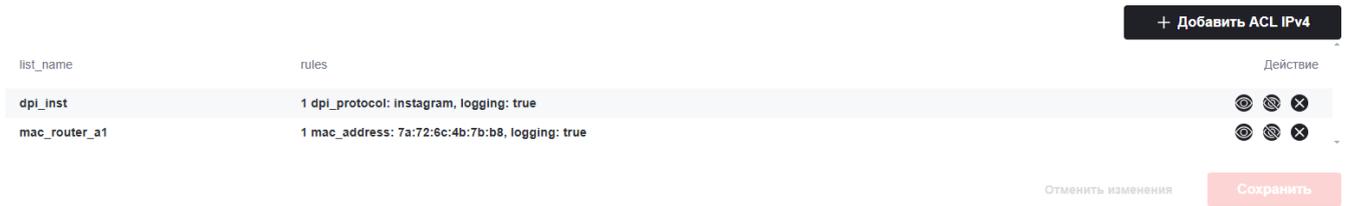


Рисунок 192 – Отображения листа контроля доступом

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).

ACL Filter IPv4



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 "forward" (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).

ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	mac_router_a1	deny		-	-	✓
-	default	forward	permit	-	-	-	0	0	✗
-	default	forward	permit	dpi_inst	deny	-	-	-	✗
1	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	-

Рисунок 195 – Настройка фильтра

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

ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	mac_router_a1	deny		-	-	✓
-	default	forward	permit	-	-	-	0	0	✗
-	default	forward	permit	dpi_inst	deny	-	-	-	✗
1	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	-

Рисунок 196 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 191).

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	mac_router_a1	deny	-	-	-	
-	default	forward	permit	-	-	-	0	0	
-	default	forward	permit	dpi_inst	deny	-	-	-	
1	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	

Отменить изменения
Сохранить

Рисунок 197 – Сохранение фильтра

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

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
-	default	forward	permit	-	-	-	0	0	
-	default	forward	permit	mac_router_a1	deny	-	-	-	
1	default	forward	permit	mac_address: 7a:72:6c:4b:7b:b8, logging: true	deny	-	0	0	
-	default	forward	permit	dpi_inst	deny	-	-	-	
2	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	

Отменить изменения
Сохранить

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).

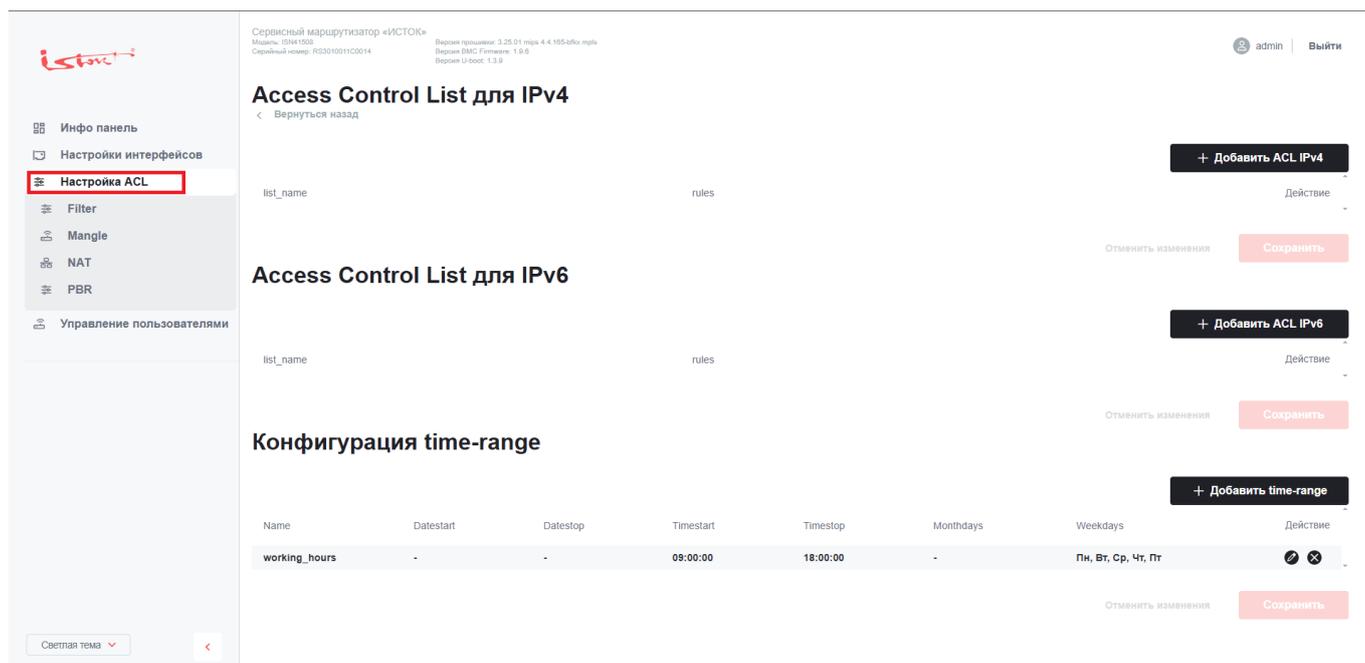


Рисунок 199 – Вкладка Настройки ACL

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

Access Control List для IPv4



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).

Access Control List для IPv4

[← Вернуться назад](#)

The screenshot shows the configuration page for an IPv4 ACL. At the top right, there is a button labeled "+ Добавить ACL IPv4". Below this, the interface is divided into three columns: "list_name", "rules", and "Действие". In the "list_name" column, a text input field contains "dpi_inst". In the "rules" column, a dropdown menu is open, showing "dpi" as the selected option. Below the dropdown, there is a configuration block for the "dpi" rule, which includes a toggle switch for "dpi" (currently off), a "NOT" checkbox, a "dpi_protocol" dropdown menu set to "activision", and a "time_range" dropdown menu. At the bottom of this block, there are checkboxes for "logging" and an "index" input field. In the "Действие" column, there are two circular icons: a checkmark and a refresh icon. At the bottom right of the interface, there are two buttons: "Отменить изменения" and "Сохранить".

Рисунок 201 – Выбор правила

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

Access Control List для IPv4

[← Вернуться назад](#)

This screenshot is similar to the previous one, but the configuration block for the "dpi" rule is now highlighted with a red border. The "dpi" toggle switch is still off, and the "dpi_protocol" dropdown menu is set to "activision". The "time_range" dropdown menu is also visible. The "Действие" column shows the checkmark and refresh icons. The "Сохранить" button is highlighted in red.

Рисунок 202 – Блок настройки правила

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

Access Control List для IPv4

[← Вернуться назад](#)

+ Добавить ACL IPv4

list_name	rules	Действие
<input type="text" value="dpi_inst"/>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>rules: dpi</p> <p> <input type="checkbox"/> dpi NOT </p> <p> dpi_protocol: instagram </p> <p>time_range: <input type="text"/> index: <input type="text"/></p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p> <input checked="" type="checkbox"/> <input type="checkbox"/> </p> <p>Отменить изменения Сохранить</p> </div>

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).

Access Control List для IPv4

[← Вернуться назад](#)

+ Добавить ACL IPv4

list_name	rules	Действие
<input type="text" value="dpi_inst"/>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>rules: dpi</p> <p> <input type="checkbox"/> dpi NOT </p> <p> dpi_protocol: instagram </p> <p>time_range: <input type="text"/> logging: <input type="checkbox"/> index: <input type="text"/></p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p> <input checked="" type="checkbox"/> <input type="checkbox"/> </p> <p>Отменить изменения Сохранить</p> </div>

Рисунок 204 – Подтверждение создания списка

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

Access Control List для IPv4

[← Вернуться назад](#)

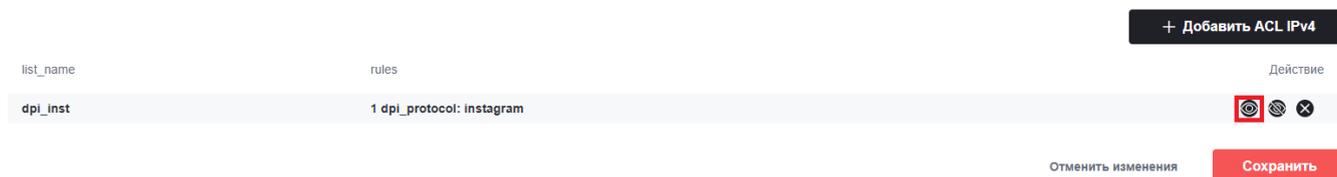


Рисунок 205 – Выбор занесения срабатывания правила в лог

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

Access Control List для IPv4

[← Вернуться назад](#)

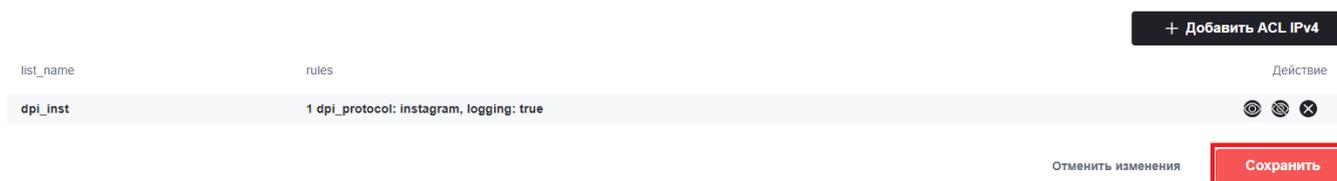


Рисунок 206 – Сохранение списка

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

Access Control List для IPv4

[← Вернуться назад](#)

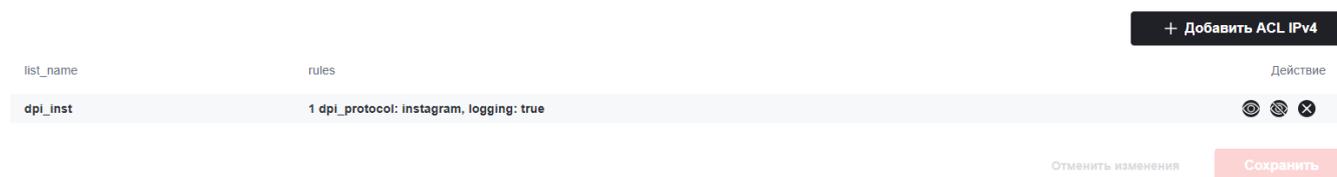


Рисунок 207 – Отображения листа контроля доступом

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).

ACL Filter IPv4

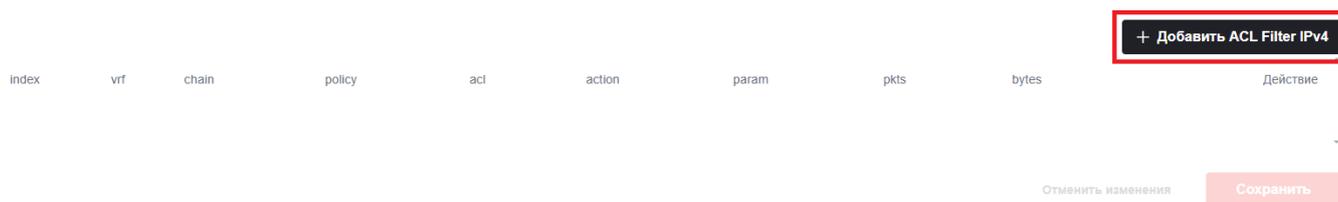


Рисунок 209 – Добавление фильтра

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).

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	dpi_inst	deny		-	-	⏏

Отменить изменения Сохранить

Рисунок 210 – Настройка фильтра

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

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	dpi_inst	deny		-	-	⏏

Отменить изменения Сохранить

Рисунок 211 – Подтверждение создания фильтра

Затем нажмите клавишу "Сохранить" (рисунок 212).

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
1	default	forward	permit	dpi_inst	deny	-	-	-	

Отменить изменения Сохранить

Рисунок 212 – Сохранение фильтра

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

ACL Filter IPv4

+ Добавить ACL Filter IPv4

index	vrf	chain	policy	acl	action	param	pkts	bytes	Действие
-	default	forward	permit	-	-	-	0	0	  
-	default	forward	permit	dpi_inst	deny	-	-	-	
1	default	forward	permit	dpi_protocol: instagram, logging: true	deny	-	0	0	

Отменить изменения Сохранить

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).

Сервисный маршрутизатор «ИСТОК»
Модель: ISN41508
Серийный номер: RS3010011C0014

Версия прошивки: 3.25.01 mips 4.4.165-bfix mpls
Версия BMC Firmware: 1.8.6
Версия U-boot: 1.3.9

admin | Выйти

Управление пользователями

[← Вернуться назад](#)

+ Добавить пользователя

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
admin	admin	local	 
user	istok	local	 

[Отменить изменения](#) [Сохранить](#)

Управление группами

+ Добавить группу

Группа пользователя	Привилегия	Действие
admin	15	
service	1	
istok	5	

[Отменить изменения](#) [Сохранить](#)

Рисунок 214 – Управление пользователями и группами

7.1 Управление пользователями

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

Управление пользователями

[← Вернуться назад](#)

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
admin	admin	local	*****	
user	istok	local	*****	

[Отменить изменения](#) [Сохранить](#)

Рисунок 215 – Добавление пользователя

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

Управление пользователями

[← Вернуться назад](#)

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	admin	local	<input type="text"/>	
admin	admin	local	*****	
user	istok	local	*****	

[Отменить изменения](#) [Сохранить](#)

Рисунок 216 – Имя пользователя

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

Управление пользователями

[← Вернуться назад](#)

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	<ul style="list-style-type: none">administokservice	local	<input type="text"/>	
admin	admin	local	*****	
user	istok	local	*****	

[Отменить изменения](#) [Сохранить](#)

Рисунок 217 – Группа пользователя

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

Управление пользователями

[< Вернуться назад](#)

[+ Добавить пользователя](#)

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>

[Отменить изменения](#) [Сохранить](#)

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).

Управление пользователями

[< Вернуться назад](#)

[+ Добавить пользователя](#)

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="password" value="*****"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>

[Отменить изменения](#) [Сохранить](#)

Рисунок 219 – Установка пароля

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

Управление пользователями

[< Вернуться назад](#)

[+ Добавить пользователя](#)

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="password" value="*****"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input checked="" type="checkbox"/>

[Отменить изменения](#) [Сохранить](#)

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).

Управление пользователями

[Вернуться назад](#)

+ Добавить пользователя

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="password" value="*****"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input type="checkbox"/>

[Отменить изменения](#) [Сохранить](#)

Рисунок 221 – Пиктограмма "Отменить"

Управление пользователями

[Вернуться назад](#)

+ Добавить пользователя

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="password" value="*****"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input type="checkbox"/>

[Отменить изменения](#) [Сохранить](#)

Рисунок 222 – Отмена изменений

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

Управление пользователями

[Вернуться назад](#)

+ Добавить пользователя

Имя пользователя	Группа пользователя	Тип пользователя	Пароль	Действие
<input type="text" value="user_1"/>	istok	local	<input type="password" value="*****"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
admin	admin	local	*****	<input type="checkbox"/> <input type="checkbox"/>
user	istok	local	*****	<input type="checkbox"/> <input type="checkbox"/>

[Отменить изменения](#) [Сохранить](#)

Рисунок 223 – Сохранение пользователя

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

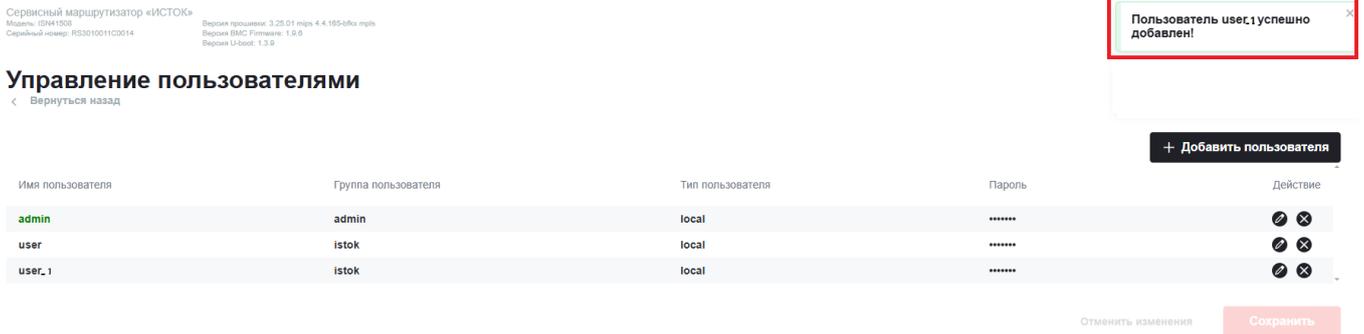


Рисунок 224 – Уведомляющее окно

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

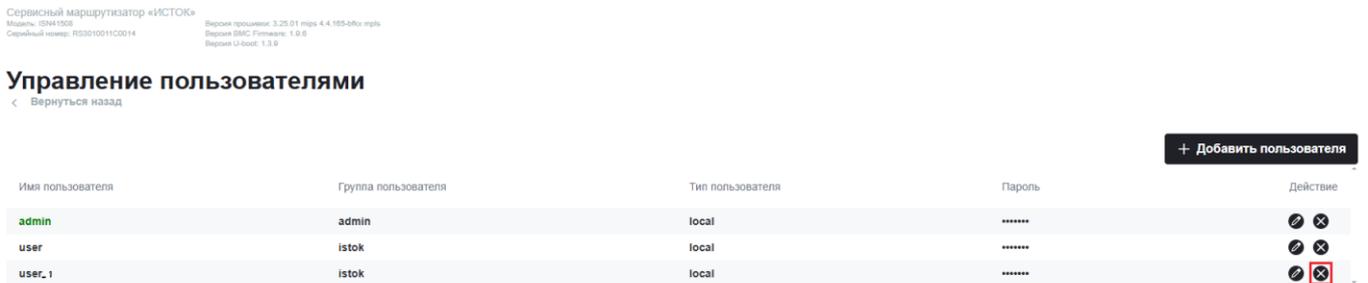


Рисунок 225 – Удаление пользователя

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

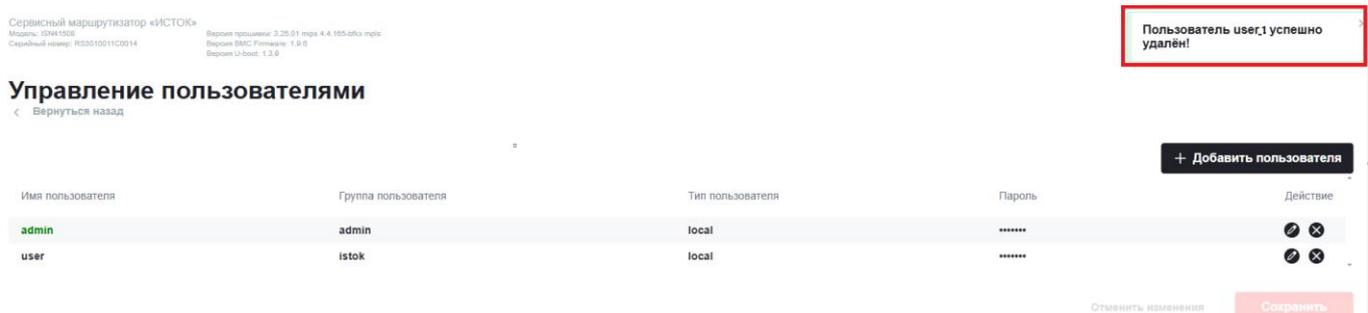


Рисунок 226 – Уведомляющее окно

7.2 Управление группами

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

Управление группами



Рисунок 227 – Добавление группы

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

Управление группами



Рисунок 228 – Ввод названия группы

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

Управление группами



Рисунок 229 – Установка привелегии группы

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

Управление группами



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).

Управление группами

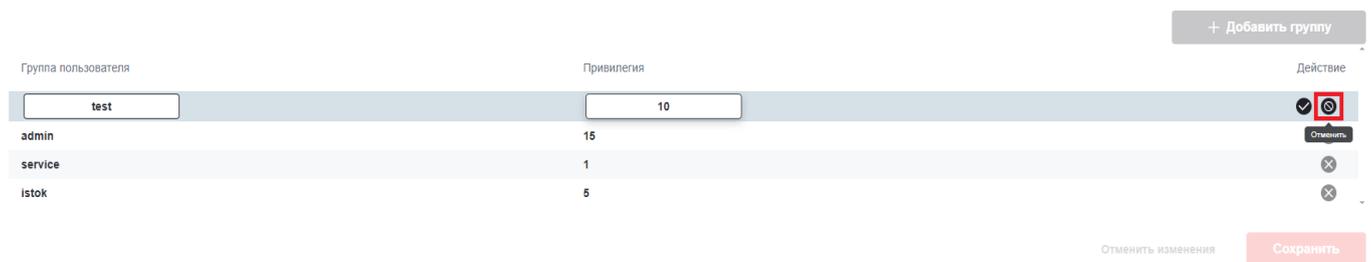


Рисунок 231 – Отмена действия

Управление группами



Рисунок 232 – Отмена изменений

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

Управление группами

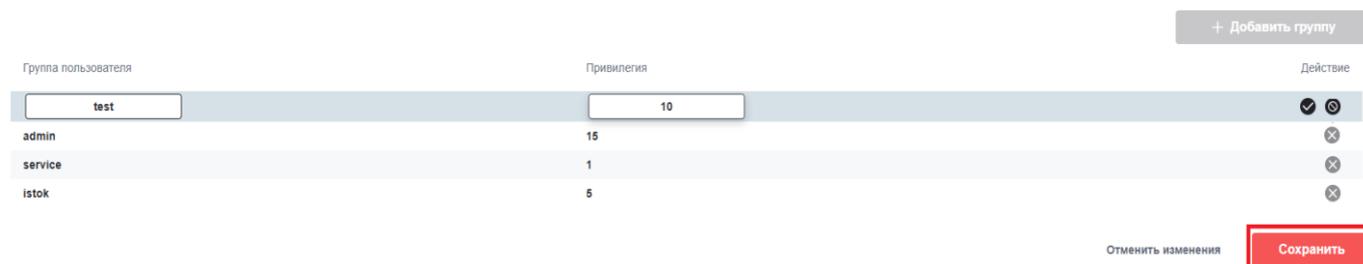


Рисунок 233 – Сохранение группы

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).

Управление группами



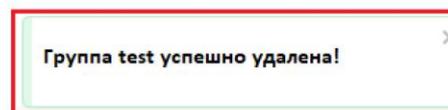
The screenshot shows a table with three columns: 'Группа пользователя' (User Group), 'Привилегия' (Privilege), and 'Действие' (Action). The 'test' group is highlighted, and its delete icon (a circle with an 'X') is enclosed in a red box. Below the table are two buttons: 'Отменить изменения' (Cancel changes) and 'Сохранить' (Save).

Группа пользователя	Привилегия	Действие
admin	15	⊗
service	1	⊗
istok	5	⊗
test	10	⊗

Отменить изменения Сохранить

Рисунок 235 – Удаление группы

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



Управление группами



The screenshot shows the same table as in Figure 235, but now all four groups (admin, service, istok, test) are visible. The 'test' group's delete icon is no longer highlighted. The 'Сохранить' (Save) button is now active.

Группа пользователя	Привилегия	Действие
admin	15	⊗
service	1	⊗
istok	5	⊗
test	10	⊗

Отменить изменения Сохранить

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/>