INFOWATCH

ARMA | NEXT GENERATION FIREWALL

ПРОГРАММНЫЙ КОМПЛЕКС
INFOWATCH ARMA СТЕНА

Межсетевой экран нового поколения
для промышленных и корпоративных сетей

Руководство по настройке «ARMA Стена» в веб-интерфейсе

Версия 2 ред. от 09.02.2026

Листов 287

СОДЕРЖАНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем руководстве использованы определения, представленные в таблице (см. Таблица «Термины и сокращения»).

Таблица «Термины и сокращения»

Термины и сокращения	Значение
ИБ	Информационная безопасность
МЭ	Межсетевой экран
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
УЗ	Учётная запись
ЦП	Центральный процессор
ARMA Стена	InfoWatch ARMA Стена
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
DVI	Digital Visual Interface – цифровой видеоинтерфейс
FTP	File Transfer Protocol – протокол передачи файлов по сети
FQDN	Fully Qualified Domain Name, полностью определённое имя домена – имя домена, не имеющее неоднозначностей в определении
HTTP	HyperText Transfer Protocol, протокол передачи гипертекста – протокол прикладного уровня передачи данных
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
LAN	Local Area Network – локальная вычислительная сеть

Термины и сокращения	Значение
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
SSD	Solid-State Drive – твердотельный накопитель
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
STP	Spanning Tree Protocol, протокол основного дерева – канальный протокол, предназначенный для устранения петель в топологии сети Ethernet
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
USB	Universal Serial Bus – универсальная последовательная шина
VRRP	Virtual Router Redundancy Protocol, протокол резервирования виртуального маршрутизатора – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
WAN	Wide Area Network – глобальная вычислительная сеть
Zabbix	Свободная система мониторинга статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования

В настоящем руководстве использованы ссылки на документы, представленные в таблице (см. Таблица «Смежные документы»).

Таблица «Смежные документы»

Сокращённое наименование	Полное наименование
Руководство по настройке **ARMA Стена** в CLI	Руководство по настройке **InfoWatch ARMA Стена** в CLI

АННОТАЦИЯ

Настоящее руководство предназначено для пользователей, производящих установку, запуск и первоначальную настройку конфигурации работы **InfoWatch ARMA Стена v.4.8**.

Роль пользователя и администратора может выполнять один сотрудник предприятия.

1 УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ

В настоящем разделе представлено описание лицензирования продукта, предусматривающего механизм управления лицензией, который позволяет:

- активировать новую лицензию:
  - автоматическим способом;
  - ручным способом.
- просматривать информацию о действующей лицензии.

Примечание:

Управление лицензией доступно только пользователям, у которых имеются права на использование команды **license** (см. раздел **«Управление доступом» руководства по настройке ARMA Стена в CLI**).

1.1 Активация системы ARMA Стена

Активация – это процедура введения в действие лицензии, дающей право на использование полнофункциональной версии системы **ARMA Стена** в течение срока действия лицензии.

При первоначальной загрузке системы **ARMA Стена** необходимо произвести активацию лицензии. Активация лицензии осуществляется двумя сценариями:

- автоматическая активация через интернет;
- ручная активация без подключения к сети Интернет.

Примечание:

Лицензионный ключ предоставляется согласно условиям в договоре поставки.

В системе **ARMA Стена** при отсутствии активной лицензии доступ к веб-интерфейсу **блокируется**. В таком состоянии минимальная конфигурация системы осуществляется исключительно через интерфейс **CLI** (см. раздел **«Управление лицензией» руководства по настройке ARMA Стена в CLI**).

В случае удаления лицензионного файла из системы, находящейся в активированном состоянии, **ARMA Стена** осуществит блокировку доступа к веб-интерфейсу. При этом текущая конфигурация системы сохраняется, и её сетевые функции продолжают выполняться в обычном режиме.

Для восстановления доступа к веб-интерфейсу необходимо выполнить повторную активацию системы или вручную восстановить лицензионный файл в каталоге /config/ из ранее сохранённой резервной копии, если таковая имеется (см. раздел **«Ручная активация лицензии» руководства по настройке ARMA Стена в CLI**).

Перед активацией лицензии необходимо выполнить следующие подготовительные шаги:

1. Настроить сетевой интерфейс устройства для обеспечения доступа к сети интернет через интерфейс CLI. Подробная информация приведена в разделе **«Настройка интерфейсов» руководства по настройке ARMA Стена в CLI**.
2. Добавить активируемое устройство в состав источников системы **ARMA MC**. Порядок выполнения указан в разделе **«Веб-интерфейс» руководства по настройке ARMA Стена в CLI**.

1.1.1 Автоматическая активация лицензии

Для автоматической активации лицензии на устройстве **ARMA Стена** необходимо выполнить следующие действия:

1. В списке источников **ARMA MC** открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника **«NGFW»** нажать **кнопку «Активировать лицензию»** (см. Рисунок – Блок активации лицензии).

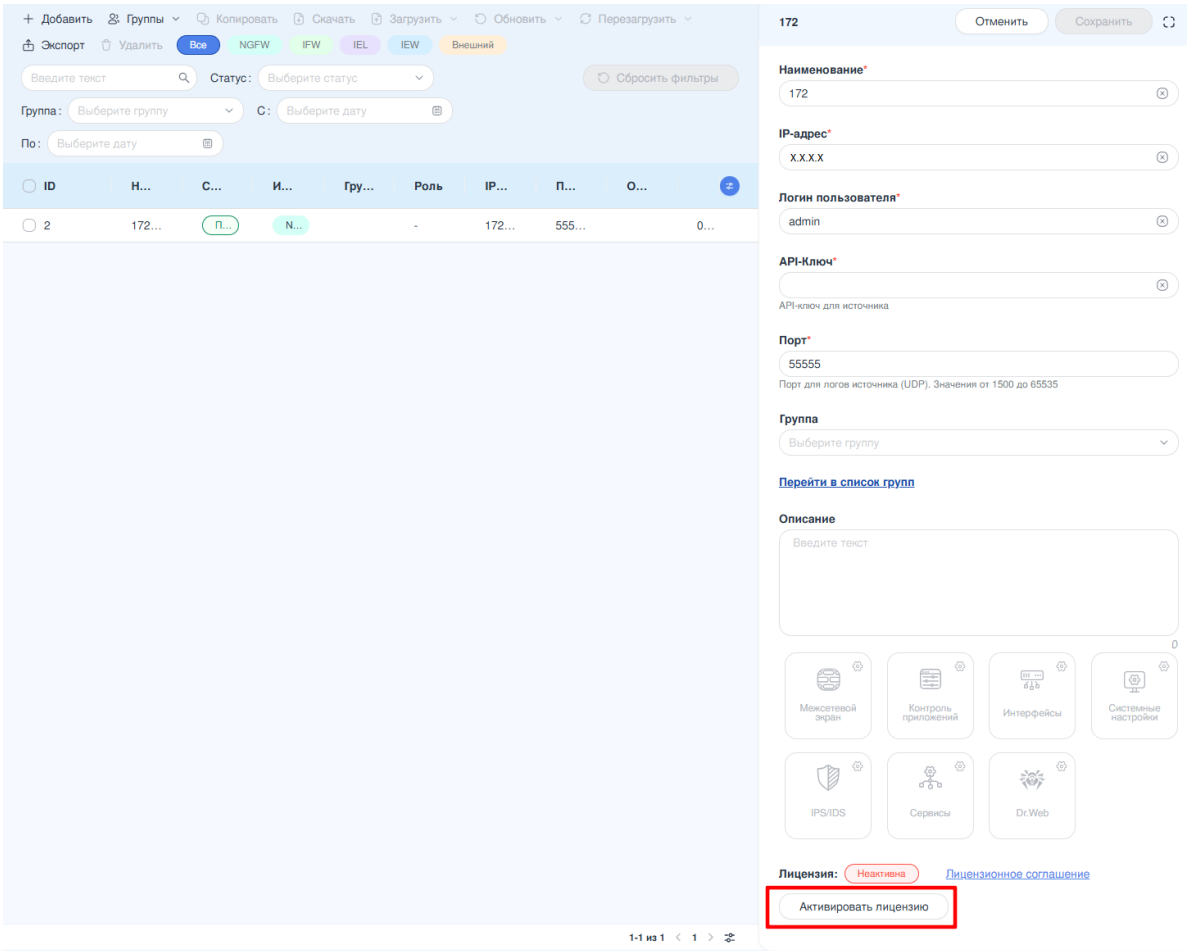


Рисунок – Блок активации лицензии

3. В открывшемся боковом окне **«Активировать лицензию»** необходимо выбрать способ активации **«Автоматическая»**.
4. В поле **«Лицензионный ключ продукта»** ввести предоставленный лицензионный ключ продукта и нажать **кнопку «Активировать»** (см. Рисунок – Автоматическая активация ARMA Стена).

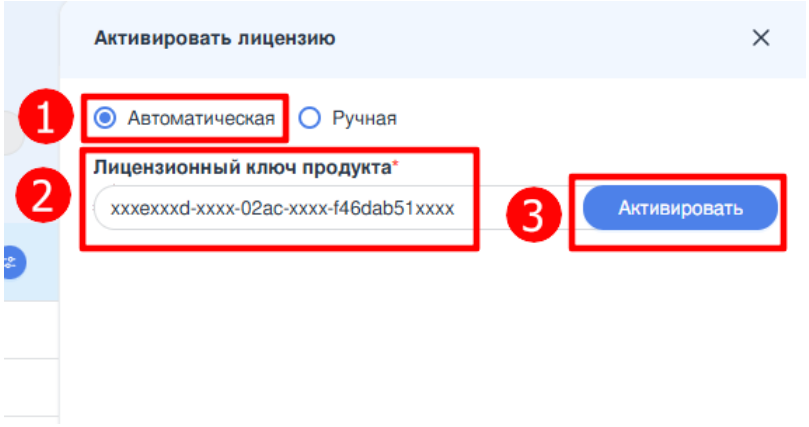


Рисунок – Автоматическая активация ARMA Стена

5. В правом нижнем углу экрана появится уведомление об успешной активации лицензии.

1.1.2 Ручная активация лицензии

Для ручной активации лицензии необходимо выполнить следующие действия:

1. В списке источников **ARMA MC** открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника **«NGFW»** нажать **кнопку «Активировать лицензию»** (см. Рисунок – Блок активации лицензии).
3. В открывшемся боковом окне **«Активировать лицензию»** необходимо выбрать способ активации **«Ручная»**.
4. В поле **«Лицензионный ключ продукта»** ввести предоставленный лицензионный ключ продукта и нажать **кнопку «Получить токен»**.
5. Система сгенерирует токен, который отобразится в поле **«Токен»** (см. Рисунок – Ручная активация системы ARMA Стена).

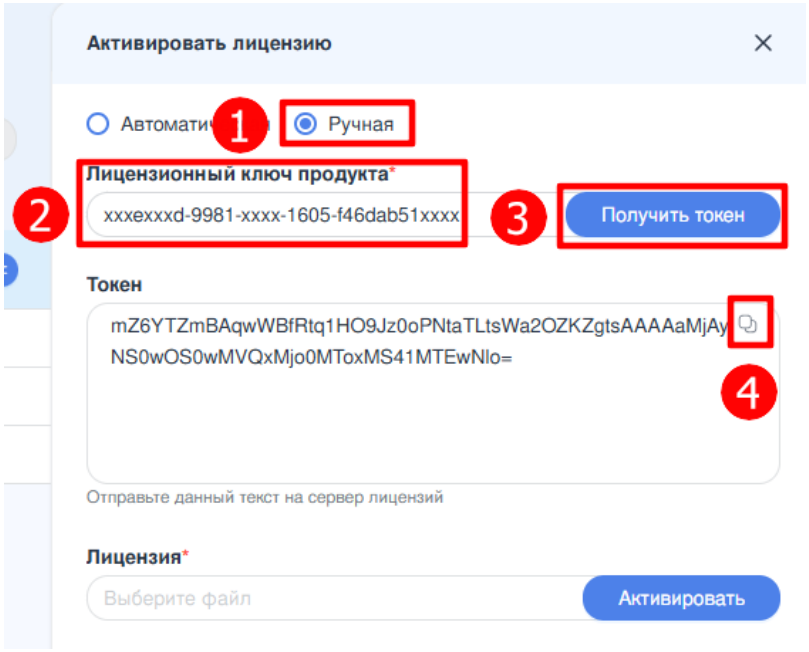


Рисунок – Ручная активация системы ARMA Стена

6. Полученный токен необходимо направить в техническую поддержку ООО **«ИнфоВотч АРМА»**.

   Примечание:

   Окно активации лицензии может быть закрыто на время ожидания получения лицензионного файла.

   Специалист ООО **«ИнфоВотч АРМА»** предоставит файл лицензии в формате **bin**, который необходимо загрузить в систему **ARMA Стена**.

7. В списке источников **ARMA MC** открыть активируемый источник **«NGFW»**.
8. В открывшемся боковом окне **«Активировать лицензию»** необходимо выбрать способ активации **«Ручная»**.
9. Нажать **кнопку «Активировать»**, после чего в открывшемся окне проводника выбрать полученный лицензионный файл (см. Рисунок – Загрузка лицензионного файла).

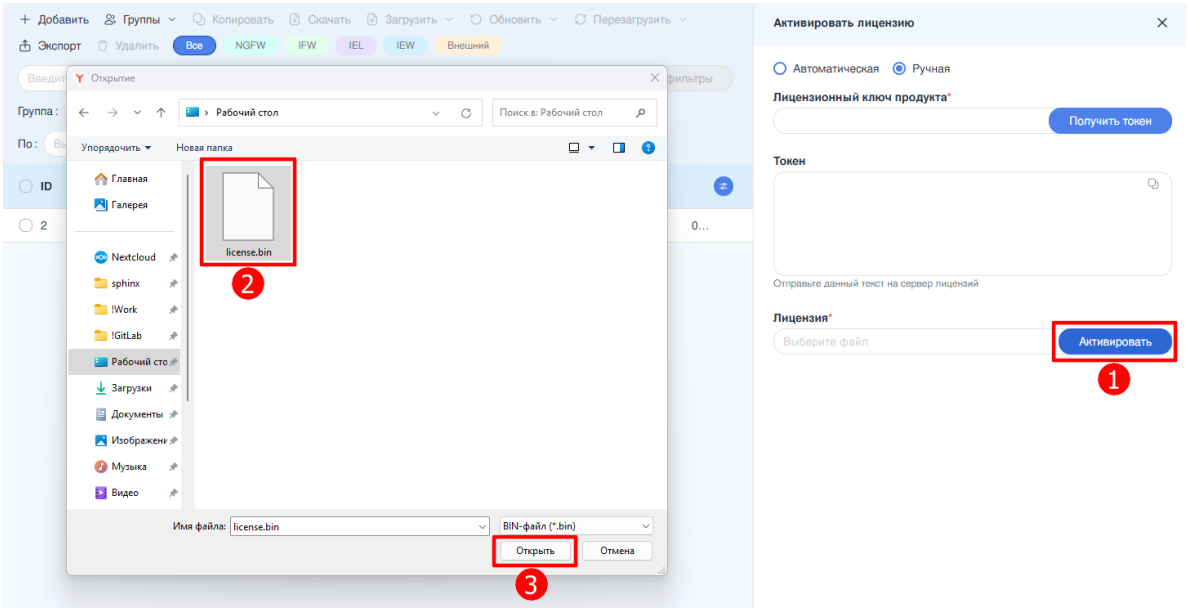


Рисунок – Загрузка лицензионного файла

10. Выбранный лицензионный файл отобразится в поле **«Лицензия»**. Повторно нажать **кнопку «Активировать»**. В правом нижнем углу экрана отобразится уведомление об успешной загрузке лицензионного файла.

11. Активация лицензии выполнена.

> **Примечание:**
>
> В случае, если загружаемый лицензионный файл является некорректным (например, повреждённым или предназначенным для другой версии продукта), система отобразит сообщение о том, что лицензия успешно загружена, однако устройство останется в неактивированном состоянии.

1.2 Информация о текущей лицензии

Информация о текущей лицензии доступна в карточке источника **«NGFW»** (см. Рисунок – Информация о текущей лицензии).

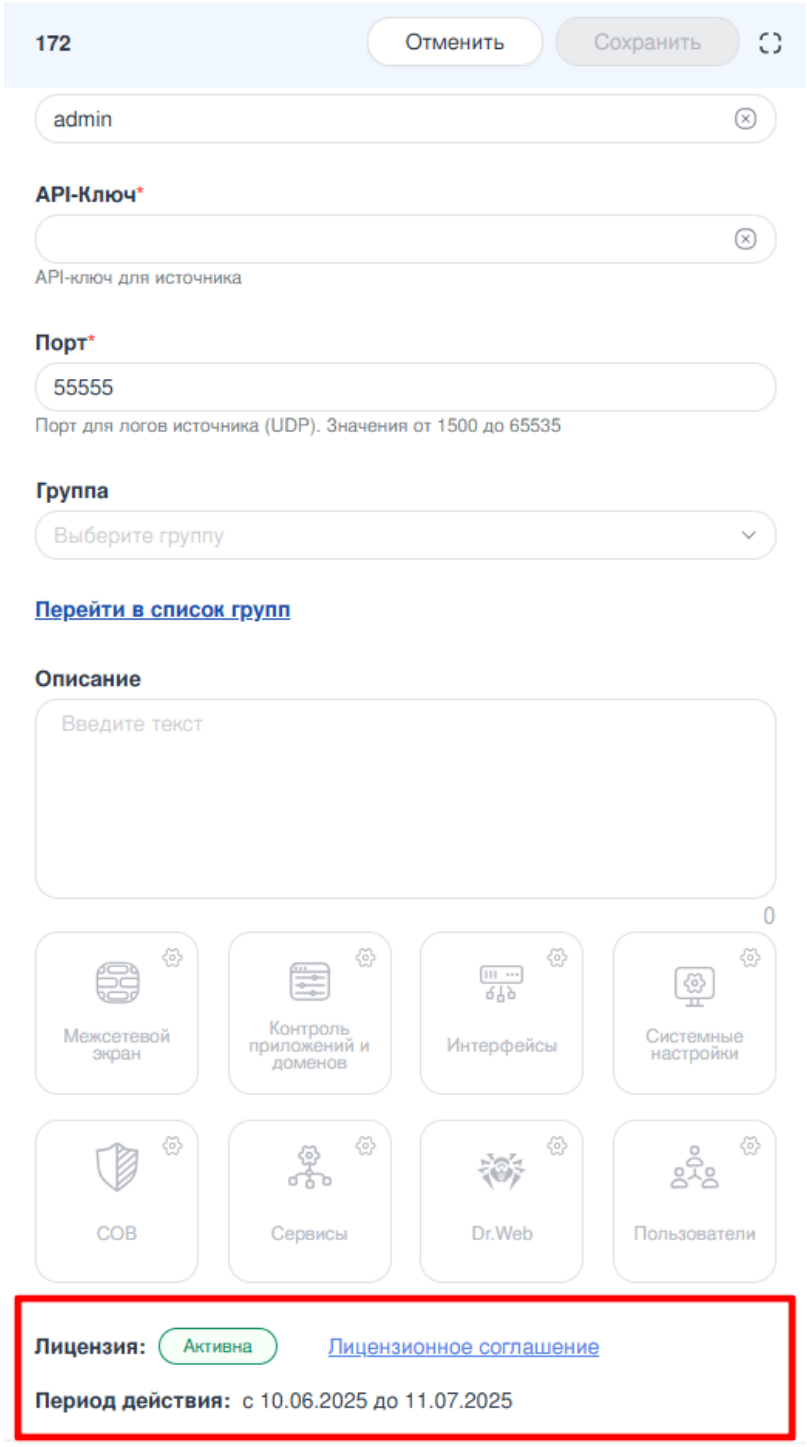


Рисунок – Информация о текущей лицензии

Для ознакомления с пользовательским лицензионным соглашением необходимо в карточке источника **«NGFW»** выбрать ссылку **«Лицензионное соглашение»** (см. Рисунок – Лицензионное соглашение).

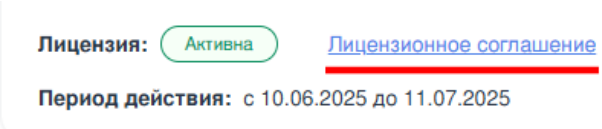


Рисунок – Лицензионное соглашение

2 УПРАВЛЕНИЕ ДОСТУПОМ

В настоящем разделе представлено описание раздела меню **«Пользователи»**, предусматривающего механизм управления следующими функциями:

- права доступа к разделам веб-интерфейса;
- управление активными сессиями пользователей;
- операции блокировки и разблокировки учётных записей.

2.1 Права доступа

Права доступа к разделам веб-интерфейса определяются набором **CLI**-команд, разрешённых для класса пользователя. Доступ реализуется на основе проверки наличия необходимых привилегий на выполнение соответствующих команд в конфигурационном или эксплуатационном режиме. Подробная информация о классах пользователей и назначении прав доступа в CLI приведена в **руководстве по настройке ARMA Стена в CLI**, раздел **«Назначение прав доступа пользовательским учётным записям»**.

Основные тезисы предоставления доступа:

- Просмотр раздела возможен при наличии у пользователя прав на выполнение всех команд, требуемых для отображения информации в данном разделе.
- Редактирование (добавление, изменение, удаление конфигураций раздела) допускается только при условии:
    - наличия прав на просмотр всего раздела;
    - наличия прав на модификацию параметров (команды **set**, **delete**);
    - наличия прав на доступ к смежным зависимым разделам.

Каждый раздел веб-интерфейса связан с определённым минимальным набором **CLI**-команд, необходимых для реализации функций просмотра и редактирования. Перечень этих команд приведён в таблице «Соответствие прав доступа в веб-интерфейсе CLI-командам».

Примечание:

Для получения доступа к веб-интерфейсу система требует, чтобы учётная запись пользователя имела права на чтение лицензии и лицензионного соглашения. Указанные права являются обязательными и проверяются на этапе аутентификации при попытке входа в веб-интерфейс.

Доступ к веб-интерфейсу предоставляется только в случае, если в классе привилегий пользователя предусмотрено разрешение на выполнение следующих команд эксплуатационного режима:

- **show version** — команда, отображающая информацию о версии программного обеспечения;
- **show license** — команда, выводящая текст лицензионного соглашения.

Отсутствие хотя бы одной из указанных команд в списке разрешённых для класса пользователя приводит к блокировке доступа к веб-интерфейсу.

Таблица «Соответствие прав доступа в веб-интерфейсе CLI-командам»

Раздел	Права на просмотр	Права на редактирование
1. Межсетевой экран		
1.1 Глобальные настройки	*Команды конфигурационного режима:* • show firewall global-options	*Команды конфигурационного режима:* • set firewall global-options • delete firewall global-options • show firewall global-options
1.2 Группы	*Команды конфигурационного режима:* • show firewall group	*Команды конфигурационного режима:* • set firewall group • delete firewall group • show firewall group • show interfaces
1.3 Правила межсетевого экрана	*Команды конфигурационного режима:* • show firewall zone • show firewall group • show firewall ipv4 • show firewall ipv6 • show firewall bridge • show interfaces	*Команды конфигурационного режима:* • show interfaces • show firewall group • show firewall zone • show firewall ipv4 • show firewall ipv6 • show firewall bridge

Раздел	Права на просмотр	Права на редактирование
		• set firewall ipv4 • set firewall ipv6 • set firewall bridge • delete firewall ipv4 • delete firewall ipv6 • delete firewall bridge
1.4 Зоны сети	*Команды конфигурационного режима:* • show firewall zone • show interfaces	*Команды конфигурационного режима:* • set firewall zone • delete firewall zone • show firewall zone • show interfaces
1.5 Назначения на направления трафика между зонами сети	*Команды конфигурационного режима:* • show firewall zone • show firewall group • show firewall ipv4 • show firewall ipv6 • show firewall bridge • show interfaces	*Команды конфигурационного режима:* • show firewall group • show interfaces • show firewall zone • show firewall ipv4 • show firewall ipv6 • show firewall bridge • set firewall zone • set firewall ipv4 • set firewall ipv6 • set firewall bridge • delete firewall zone • delete firewall ipv4 • delete firewall ipv6 • delete firewall bridge

Раздел	Права на просмотр	Права на редактирование
1.6 Логи межсетевого экрана	*Команды эксплуатационного режима:* • show logging firewall или • show logging all	-
1.7 NAT	*Команды конфигурационного режима:* • show nat • show firewall group • show interfaces	*Команды конфигурационного режима:* • set nat • delete nat • show nat • show firewall group • show interfaces
2. Контроль приложений	*Команды конфигурационного режима:* • show app-control *Команды эксплуатационного режима:* • show app-control	*Команды конфигурационного режима:* • set app-control • delete app-control • show app-control *Команды эксплуатационного режима:* • show app-control
3. Интерфейсы		
3.1 Настройки интерфейсов	*Команды конфигурационного режима:* • show interfaces *Команды эксплуатационного режима:* • show interfaces	*Команды конфигурационного режима:* • set interfaces • delete interfaces • show interfaces *Команды эксплуатационного режима:*

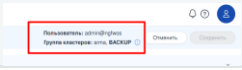
Раздел	Права на просмотр	Права на редактирование
		• show interfaces
3.2 Балансировка нагрузки на WAN-интерфейсах	*Команды конфигурационного режима:* • show load-balancing wan • show interfaces *Команды эксплуатационного режима:* • show wan-load-balance	*Команды конфигурационного режима:* • show load-balancing wan • show interfaces • set load-balancing wan • delete load-balancing wan *Команды эксплуатационного режима:* • show wan-load-balance
3.3 Обратный прокси	*Команды конфигурационного режима:* • show load-balancing reverse-proxy	*Команды конфигурационного режима:* • show load-balancing reverse-proxy • set load-balancing reverse-proxy • delete load-balancing reverse-proxy
4. Системные настройки		
4.1 Системный DNS	*Команды конфигурационного режима:* • show system domain-search • show system name-server • show interfaces	*Команды конфигурационного режима:* • show system domain-search • show system name-server • show interfaces • set system domain-search • set system name-server • delete system domain-search

Раздел	Права на просмотр	Права на редактирование
		• delete system name-server
4.2 Системный Прокси	*Команды конфигурационного режима:* • show system proxy	*Команды конфигурационного режима:* • show system proxy • set system proxy • delete system proxy
4.3 Логирование	*Команды конфигурационного режима:* • show system logging global • show system logging file • show system logging host	*Команды конфигурационного режима:* • show system logging global • show system logging file • show system logging host • set system logging global • set system logging file • set system logging host • delete system logging global • delete system logging file • delete system logging host
4.4 Шлюз по умолчанию	*Команды конфигурационного режима:* • show protocols static route	*Команды конфигурационного режима:* • show protocols static route • set protocols static route • delete protocols static route
4.5 Управление конфигурацией	*Команды конфигурационного*	*Команды конфигурационного*

Раздел	Права на просмотр	Права на редактирование
	режима: ● show system config-management ● compare *Команды эксплуатационного режима:* ● show configuration ● show system commit	*режима:* ● show system config-management ● set system config-management ● delete system config-management ● load ● delete commit *Команды эксплуатационного режима:* ● show configuration ● delete commit ● show system commit
4.6 Мониторинг аппаратной платформы	*Команды эксплуатационного режима:* ● show health psu ● show health all ● show health json	-
4.7 Мониторинг процессов	*Команды эксплуатационного режима:* ● show system processes	-
4.8 Отказоустойчивая маршрутизация	*Команды конфигурационного режима:* ● show protocols failover ● show interfaces	*Команды конфигурационного режима:* ● show protocols failover ● show interfaces ● set protocols failover ● delete protocols failover
5. СОВ	*Команды конфигурационного режима:*	*Команды конфигурационного режима:*

Раздел	Права на просмотр	Права на редактирование
	• show suricata • show interfaces *Команды эксплуатационного режима:* • suricata • show idps	• show suricata • show interfaces • set suricata • delete suricata *Команды эксплуатационного режима:* • suricata • show idps
6. Сервисы		
6.1 Ретрансляция DHCPv4	*Команды конфигурационного режима:* • show service dhcp-relay • show interfaces	*Команды конфигурационного режима:* • show service dhcp-relay • show interfaces • set service dhcp-relay • delete service dhcp-relay
6.2 Ретрансляция DHCPv6	*Команды конфигурационного режима:* • show service dhcpv6-relay • show interfaces	*Команды конфигурационного режима:* • show service dhcpv6-relay • show interfaces • set service dhcpv6-relay • delete service dhcpv6-relay
6.3 Веб-прокси	*Команды конфигурационного режима:* • show service webproxy	*Команды конфигурационного режима:* • show service webproxy • set service webproxy • delete service webproxy
7. DrWEB	*Команды конфигурационного*	*Команды конфигурационного*

Раздел	Права на просмотр	Права на редактирование
	режима: • show third-party service drweb gss *Команды эксплуатационного режима:* • show third-party drweb gss • show logging third-party service drweb	*режима:* • show third-party service drweb gss • set third-party service drweb gss • delete third-party service drweb gss *Команды эксплуатационного режима:* • show third-party drweb gss • show logging third-party service drweb • third-party drweb gss update
8. Пользователи	*Команды конфигурационного режима:* • show system login *Команды эксплуатационного режима:* • show users recent • show users sessions • show system login users	*Команды конфигурационного режима:* • show lock ip • show lock users • show lock all • show system login • set system login users • delete system login users *Команды эксплуатационного режима:* • clear lock user • clear lock ip-address • reset sessions • show users recent • show users sessions

Раздел	Права на просмотр	Права на редактирование
9. Обзорная панель		
9.1 Мониторинг аппаратной платформы	*Команды эксплуатационного режима:* ● show health	-
9.2 Мониторинг процессов	*Команды эксплуатационного режима:* ● show system processes	-
9.3 Трафик экрана	*Команды эксплуатационного режима:* ● show interfaces	-
10. Информация о статусе кластера		
10.1. Отображение статуса кластера в хедере страницы источника NGFW 	*Команды эксплуатационного режима:* ● show vrrp ● show host name	-
10.2. Отображение статуса кластера в списках источников ARMA MC 	*Команды конфигурационного режима:* ● show high-availability *Команды эксплуатационного режима:* ● show vrrp	-

Примечание:

Наличие у пользователя прав на выполнение команд более высокого уровня иерархии автоматически предоставляет доступ к соответствующему разделу веб-интерфейса. Например, если пользователь имеет право на выполнение команды *show firewall*, ему предоставляется доступ ко всем подразделам группы «Межсетевой экран», включая, например, «Зоны сети», даже если права на *show firewall zone* не указаны явно.

Просмотр прав доступа

Для просмотра прав доступа текущей учётной записи в веб-интерфейсе необходимо в карточке источника событий **NGFW** выбрать ссылку **«Права доступа»** (см. Рисунок – Ссылка на просмотр прав доступа).

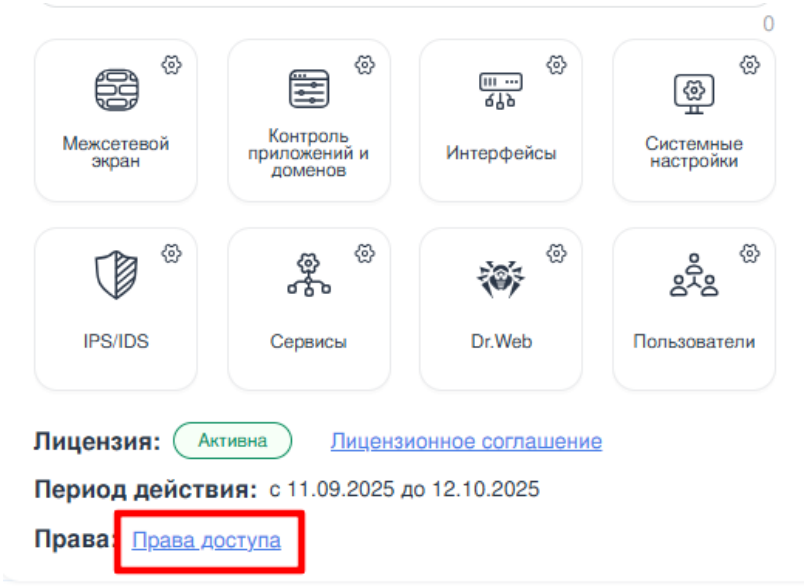


Рисунок – Ссылка на просмотр прав доступа

После перехода по указанной ссылке открывается окно **«Права доступа <имя_текущей_УЗ>»**. Окно содержит две основные секции: таблицу разрешений на доступ к разделам веб-интерфейса и список доступных CLI-команд.

Таблица «Разрешения»

Таблица **«Разрешения»** включает полный перечень всех разделов веб-интерфейса **NGFW** (см. Рисунок – Просмотр прав доступа).

Для каждого раздела в таблице предусмотрены две колонки:

- **«Просмотр»** — указывает, имеет ли текущий пользователь право на отображение информации в данном разделе.
- **«Редактирование»** — отражает наличие прав у текущего пользователя на изменение конфигурации (добавление, редактирование, удаление параметров).

Статус прав визуализируется с помощью графических индикаторов:

— указывает на наличие разрешения;

— указывает на отсутствие соответствующего права.

Права доступа test

Разрешения

Раздел	Просмотр	Редактирование
Интерфейсы		
Настройка интерфейсов	✗	✗
Балансировка нагрузки на WAN-интерфейсах	✗	✗
Обратный прокси	✓	✗
Системные настройки		
Системный DNS	✓	✗
Системный Прокси	✓	✗
Логирование	✓	✗
Шлюз по умолчанию	✓	✗
Управление конфигурацией	✗	✗
Мониторинг аппаратной платформы	✗	
Отказоустойчивая маршрутизация	✓	✗
Межсетевой экран		
Глобальные настройки	✓	✗
Группы	✓	✗
Правила межсетевого экрана	✓	✗
Зоны сети	✓	✗
Назначения на направления трафика между зонами сети	✓	✗
Логи межсетевого экрана	✗	

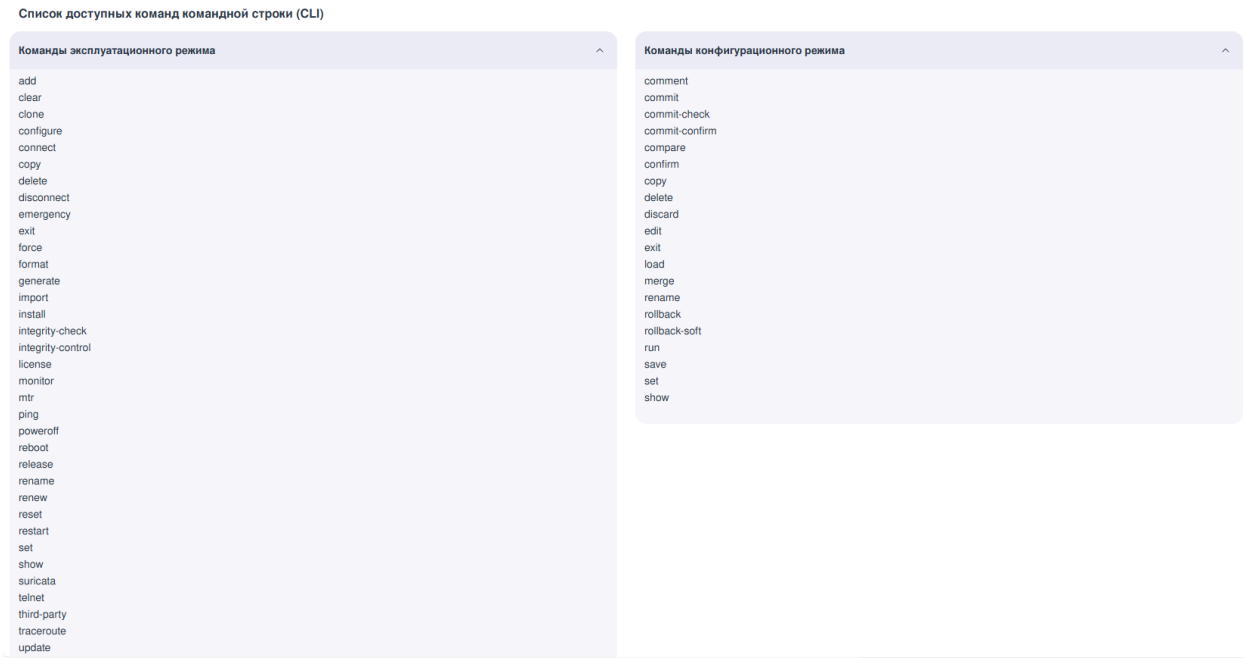
Рисунок – Просмотр прав доступа

Блок «Список доступных команд командной строки (CLI)»

В дополнение к веб-правам предоставляется информация о CLI-привилегиях пользователя. Данный блок содержит два упорядоченных списка команд:

- **Команды конфигурационного режима**
- **Команды эксплуатационного режима**

Перечень отражает только те команды, которые включены в класс привилегий текущей учётной записи (см. Рисунок – Список доступных команд командной строки (CLI)).



Список доступных команд командной строки (CLI)

Команды эксплуатационного режима

add
clear
clone
configure
connect
copy
delete
disconnect
emergency
exit
force
format
generate
import
install
integrity-check
integrity-control
license
monitor
mtr
ping
poweroff
reboot
release
rename
renew
reset
restart
set
show
suricata
telnet
third-party
traceroute
update

Команды конфигурационного режима

comment
commit
commit-check
commit-confirm
compare
confirm
copy
delete
discard
edit
exit
load
merge
rename
rollback
rollback-soft
run
save
set
show

Рисунок – Список доступных команд командной строки (CLI)

Пример назначения прав доступа для учётной записи

Рассмотрим сценарий настройки класса привилегий для учётной записи с именем **test**, предназначенной исключительно для просмотра конфигурационных данных межсетевого экрана в веб-интерфейсе. Учётная запись наделяется правами только на чтение; редактирование конфигурации во всех разделах системы запрещено. Доступ к подразделу **«NAT»** в составе раздела «Межсетевой экран» не предоставляется.

Учётная запись **test** ассоциирована с пользовательским классом привилегий, которому разрешено выполнение следующих CLI-команд:

- Команды конфигурационного режима:
    - show firewall global-options
    - show firewall zone
    - show firewall group
    - show firewall ipv4
    - show firewall ipv6
    - show firewall bridge
    - show interfaces
- Команды эксплуатационного режима:
    - show version
    - show license
    - show logging firewall

В результате пользователь **test** имеет возможность:

- просматривать текущую конфигурацию межсетевого экрана, включая глобальные параметры, зоны безопасности, группы объектов, правила фильтрации;
- получать информацию о версии системы, лицензировании и состоянии журналов событий межсетевого экрана.

Доступ к разделу «NAT» и ко всем остальным разделам веб-интерфейса блокируется на уровне прав доступа.

Для проверки корректности назначенных прав необходимо выполнить следующие действия:

1. В карточке источника событий NGFW указать учётные данные пользователя **test** в поле авторизации и сохранить изменения.
2. Повторно открыть данную карточку и перейти по ссылке **«Права доступа»**.

3. В открывшемся окне убедиться, что список доступных разделов веб-интерфейса и разрешённых CLI-команд соответствует заданной политике (см. Рисунок – Права доступа для УЗ test).

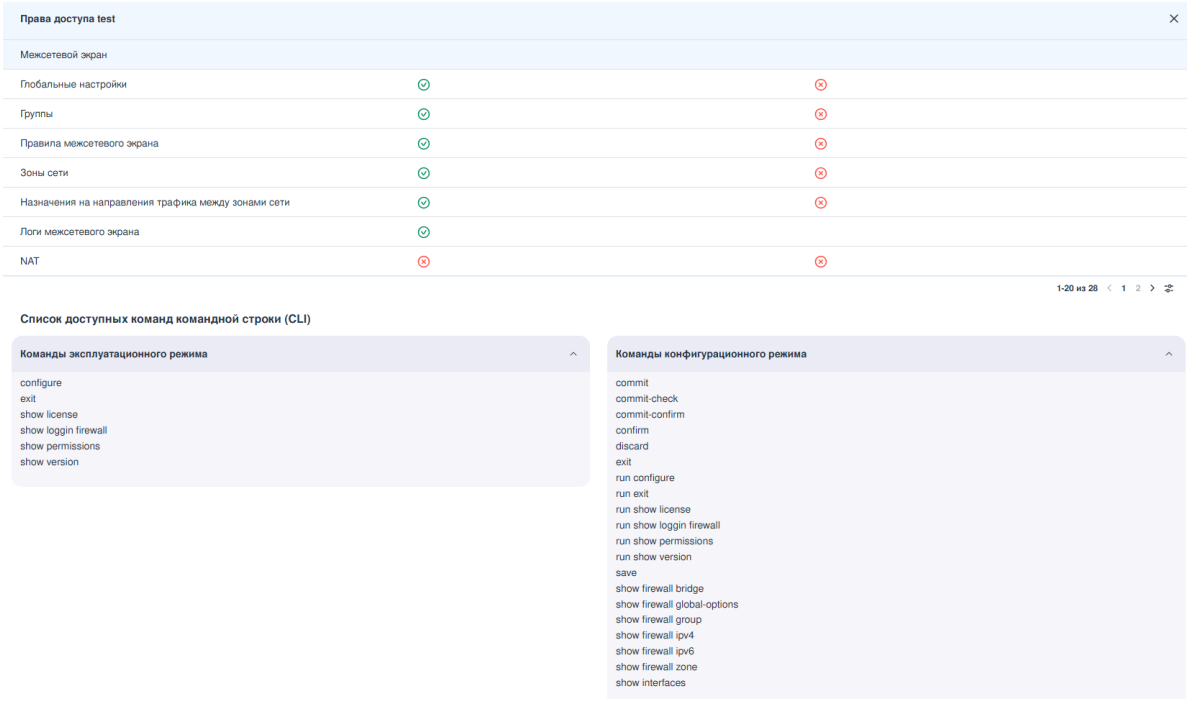


Рисунок – Права доступа для УЗ test

В блоке отображения доступных модулей веб-интерфейса карточки источника должен присутствовать только модуль **«Межсетевой экран»** (см. Рисунок – Доступные модули для УЗ test).

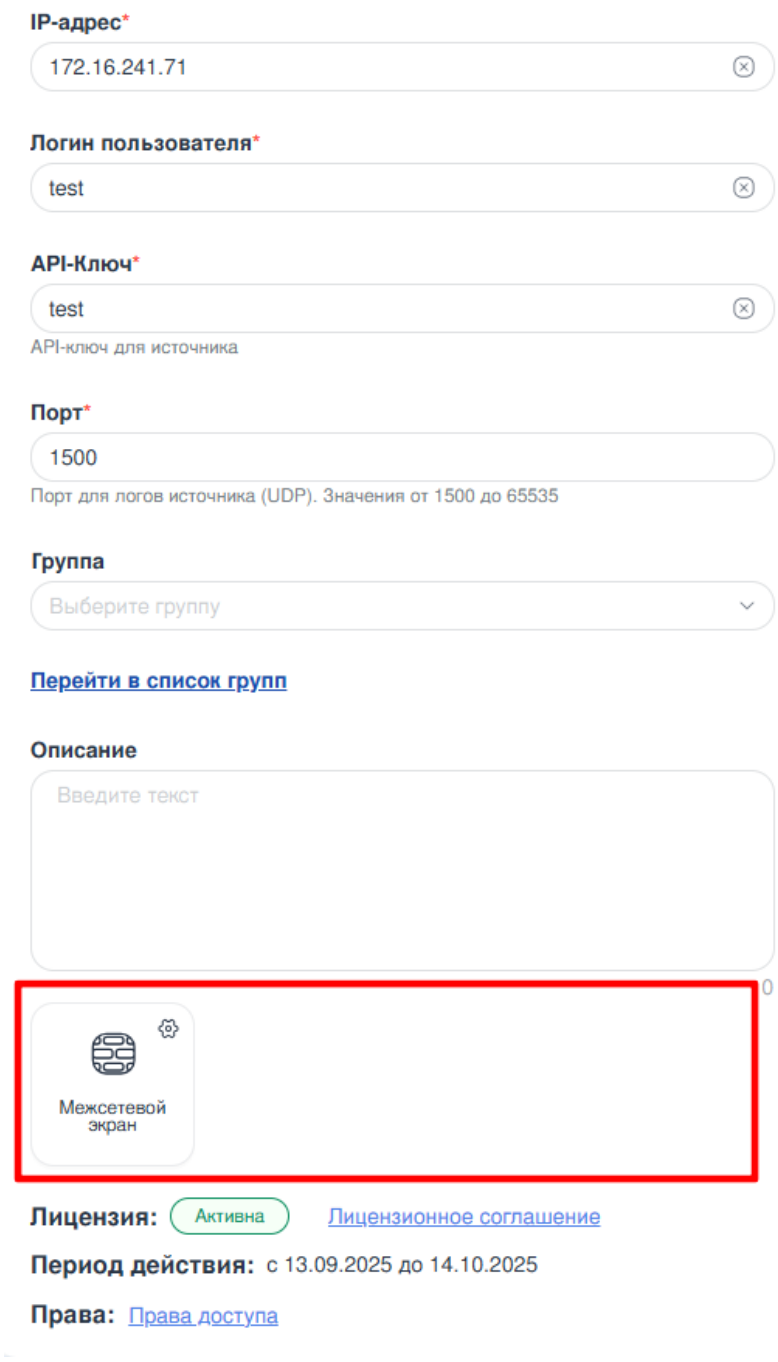


Рисунок – Доступные модули для УЗ test

2.2 Управление пользователями

В системе ARMA Стена реализовано централизованное администрирование пользовательских учётных записей. Функционал включает контроль доступа, управление состоянием учётных записей, а также оперативное принудительное завершение активных сессий.

Поддерживаются следующие типы сессий:

- SSH-сессии;
- терминальные сессии;

Администратор имеет возможность:

- просматривать список активных сессий;
- блокировать и разблокировать учётные записи;
- инициировать принудительное завершение одной или нескольких сессий.

2.2.1 Просмотр списка активных сессий

Для управления пользовательскими учётными записями необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«Пользователи»** и перейти в раздел **«Управление пользователями»** (см. Рисунок – Управление пользователями).

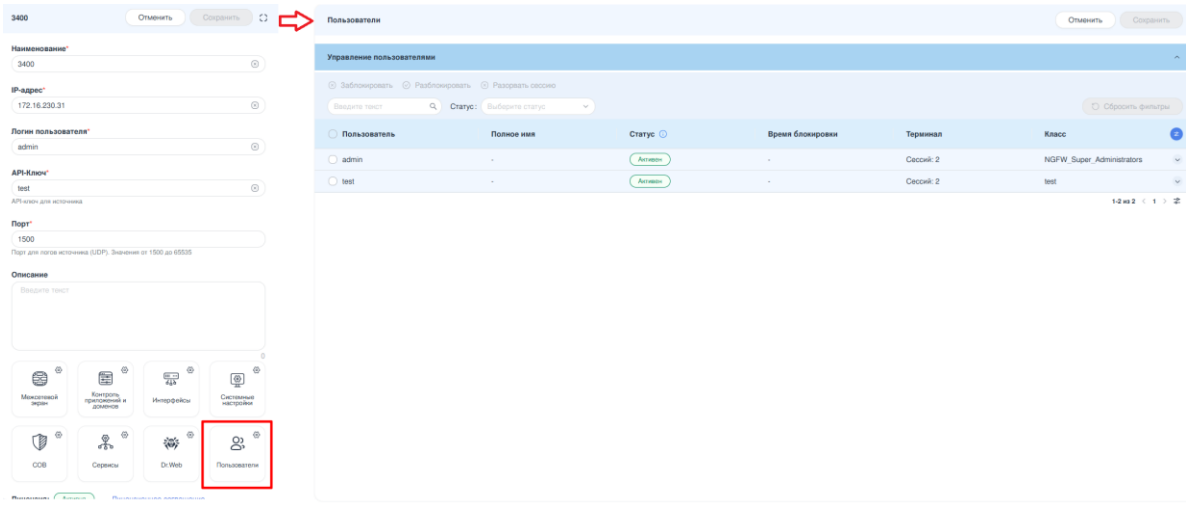


Рисунок – Управление пользователями

Раздел меню позволяет просматривать сессии пользователей в формате таблицы, состоящей из следующих столбцов:

- **Пользователь** - логин учётной записи;
- **Полное имя** - полное имя пользовательской учётной записи;
- **Статус** - текущее состояние учётной записи:
  - Активен;
  - Заблокирован;
  - Временно заблокирован (по причине превышения допустимого количества неудачных попыток авторизации).

  Данные обновляются раз в 30 секунд.
- **Время блокировки** - отображает дату и время временного промежутка на который заблокирована УЗ пользователя.
- **Терминал** - отображает количество активных сессий пользователя.

- **Класс** - наименование класса, к которому относится учётная запись.

Для пользователей, имеющих активные сессии, в соответствующей строке таблицы отображается кнопка , раскрывающая детализированный список активных сессий.

Примечание:

Сессии, для которых значение поля **«Терминал»** не указано, являются фоновыми. Как правило, такие сессии создаются системными процессами и не связаны с интерактивным входом пользователя в систему.

2.2.2 Блокировка и разблокировка учётной записи

В системе **ARMA Стена** реализована функция управления доступом пользователей, включающая возможность блокировки и разблокировки учётных записей с гибкими параметрами по времени и сессиям.

Примечание:

Блокировка встроенной учётной записи **«admin»** запрещена на уровне системы. Допускается исключительно принудительное завершение активных сессий данной учётной записи.

Блокировка учётной записи

Блокировка одной или нескольких пользовательских учётных записей может быть выполнена двумя способами.

Способ 1: Групповая блокировка через контекстное меню:

1. В таблице раздела **«Управление пользователями»** выбрать требуемую УЗ, установив флажок в левом столбце напротив логина. Поддерживается множественный выбор для одновременной обработки нескольких учётных записей.
2. Нажать **кнопку «Заблокировать»**. Откроется диалоговое окно **«Блокировка пользователей»**, в котором доступны следующие режимы:
    - **Заблокировать** — немедленное применение постоянной блокировки учётной записи.
    - **Заблокировать на время** — возможность задать временные параметры блокировки:
        - **Активация блокировки в заданное время** — позволяет назначить дату и время начала блокировки без указания её окончания. Для этого следует выбрать тип **«Заблокировать на время»**, в поле **«С»** указать требуемую дату и время начала

действия блокировки, а поле **«По»** оставить пустым. Учётная запись будет заблокирована автоматически в указанное время.

- **Блокировка в указанный период** — задание интервала действия блокировки. Необходимо заполнить оба поля: **«С»** (дата и время начала) и **«По»** (дата и время окончания). Блокировка будет активна только в пределах указанного периода.

3. При необходимости принудительного завершения активных сессий пользователя следует установить флажок в поле **«Разорвать сессию»**. Это приведёт к немедленному завершению всех текущих сессий выбранного пользователя в момент активации блокировки.
4. Подтвердить операцию, нажав **кнопку «Заблокировать»** (см. Рисунок – Блокировка учётной записи).

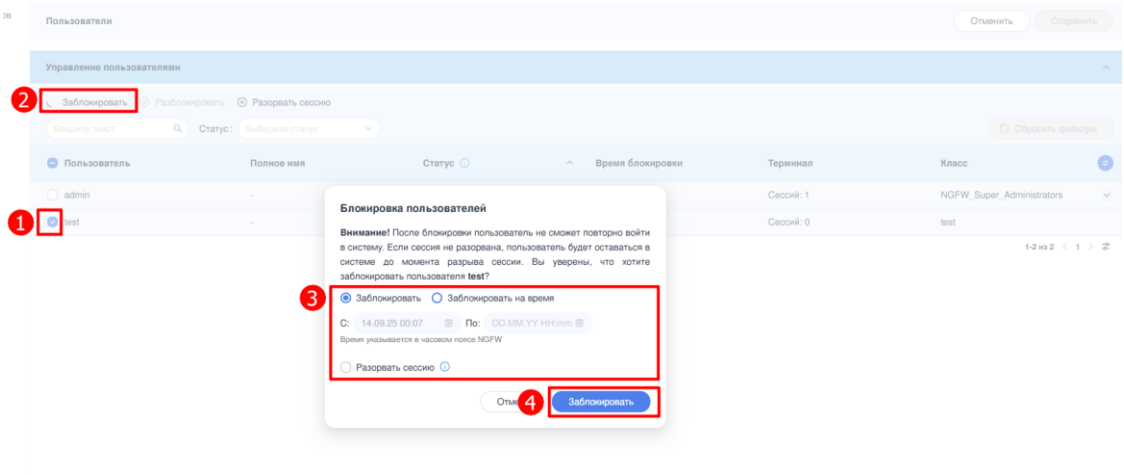


Рисунок – Блокировка учётной записи.

5. Для применения и сохранения настроек нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Пользователи»** (см. Рисунок – Применение и сохранение настроек блокировки).

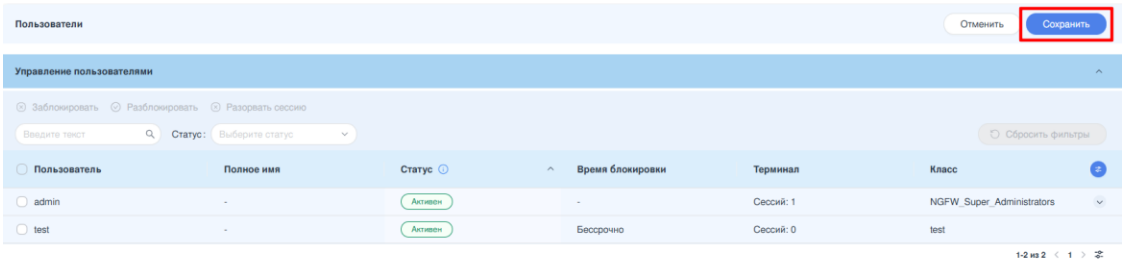


Рисунок – Применение и сохранение настроек блокировки.

Способ 2: Индивидуальная блокировка через боковую панель:

1. В таблице **«Управление пользователями»** щёлкнуть по строке нужной учётной записи.
2. В открывшемся боковом окне **«Пользователь <имя_УЗ>»** перевести переключатель **«Заблокировать»** в положение «Включено».
3. Выбрать тип блокировки (постоянная или временная) и при необходимости отметить опцию «Разорвать сессию».
4. Нажать **кнопку «Изменить»**.
5. Применить изменения, нажав **кнопку «Сохранить»** в правом верхнем углу раздела (см. Рисунок – Разблокировка учётной записи).

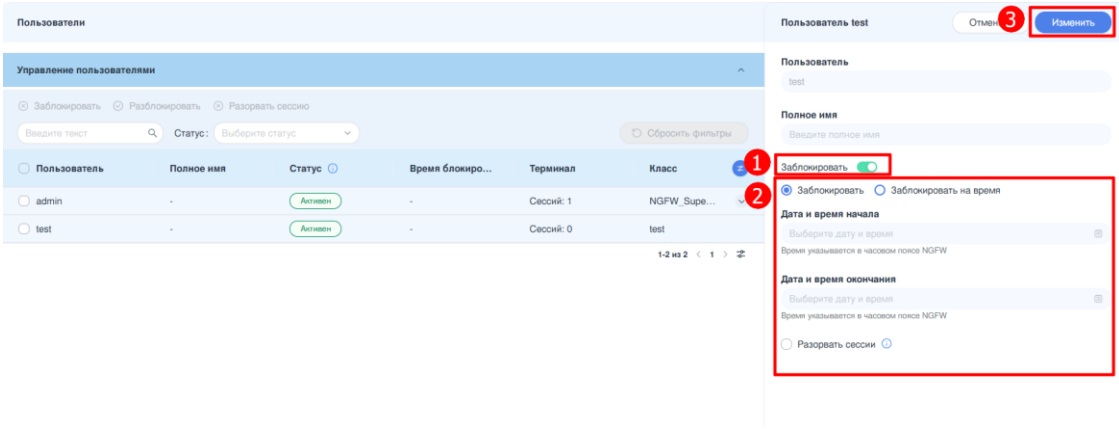


Рисунок – Разблокировка учётной записи.

Если при выполнении блокировки учётной записи не был выбран параметр **«Разорвать сессию»**, и пользователь к моменту активации блокировки уже авторизован в системе, то его активные сессии не прерываются автоматически. Пользователь сохраняет возможность продолжать работу в рамках существующих сессий до их естественного завершения — в результате ручного выхода, истечения времени бездействия или принудительного завершения администратором. Для обеспечения немедленного прекращения доступа рекомендуется совмещать блокировку учётной записи с опцией принудительного разрыва активных сессий.

Примечание:

При блокировке учётной записи доступ к веб-интерфейсу прекращается немедленно, независимо от того, был ли установлен флаг **«Разорвать сессию»**.

Если на момент блокировки пользователь находился в веб-интерфейсе, текущая страница остаётся открытой, однако возможность вносить изменения в конфигурацию становится недоступной. Любая попытка сохранить изменения приведёт к выводу системной ошибки, после которой отображается сообщение о недостаточности прав.

Источник **«NGFW»** в **ARMA MC**, в настройках которого используются учётные данные заблокированной учётной записи, автоматически переходит в статус **«Ошибка»**.

Разблокировка учётной записи

Для снятия блокировки с одной или нескольких пользовательских учётных записей предусмотрены два способа.

Способ 1: Групповая разблокировка через контекстное меню:

1. В таблице раздела **«Управление пользователями»** выбрать одну или несколько заблокированных УЗ, установив соответствующие флажки.
2. Нажать **кнопку «Разблокировать»**.
3. В открывшемся диалоговом окне подтвердить операцию, нажав **кнопку «Разблокировать»** (см. Рисунок – Разблокировка учётных записей).
4. Для применения и сохранения настроект нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Пользователи»**.

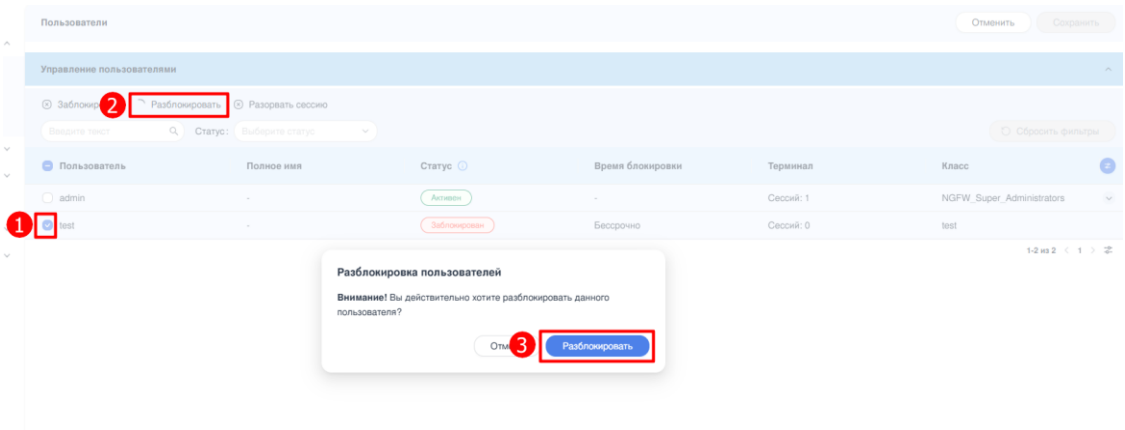


Рисунок – Разблокировка учётных записей.

Способ 2: Индивидуальная разблокировка через боковую панель:

1. В таблице **«Управление пользователями»** щёлкнуть по строке нужной учётной записи.
2. В открывшемся боковом окне **«Пользователь <имя_УЗ>»** перевести переключатель **«Заблокировать»** в положение «Выключено».
3. Нажать **кнопку «Изменить»**.
4. Применить изменения, нажав **кнопку «Сохранить»** в правом верхнем углу раздела (см. Рисунок – Разблокировка учётной записи).

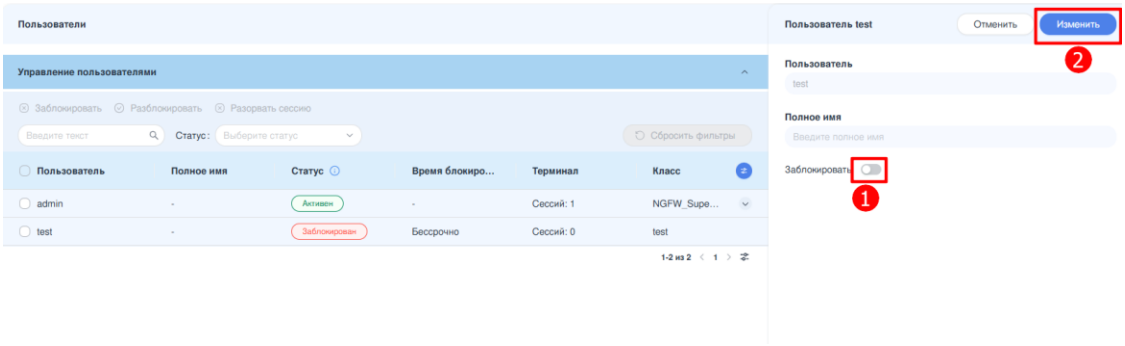


Рисунок – Разблокировка учётной записи.

После успешного выполнения операции статус учётной записи изменяется на **«Активен»**, и пользователь получает возможность авторизоваться в системе в соответствии с установленными политиками доступа.

Примечание:

Для повторной авторизации в веб-интерфейсе после разблокировки УЗ необходимо перезагрузить страницу веб-интерфейса.

2.2.3 Принудительное завершение сессий

Система **ARMA Стена** предоставляет функционал принудительного завершения активных сессий, реализованный по двум критериям: по идентификатору отдельной сессии или по имени пользователя (учётной записи).

Завершение сессии по идентификатору

Одна учётная запись может иметь несколько активных сессий одновременно. Для завершения конкретной сессии необходимо выполнить следующие действия:

1. В таблице **«Управление пользователями»** раскрыть список активных сессий требуемой учётной записи с помощью кнопки в соответствующей строке.
2. Выбрать нужную сессию, установив флажок рядом с её идентификатором.
3. Нажать **кнопку «Разорвать сессии»**.
4. В появившемся диалоговом окне подтвердить действие, нажав **кнопку «Разорвать»** (см. Рисунок – Завершение сессии по идентификатору).

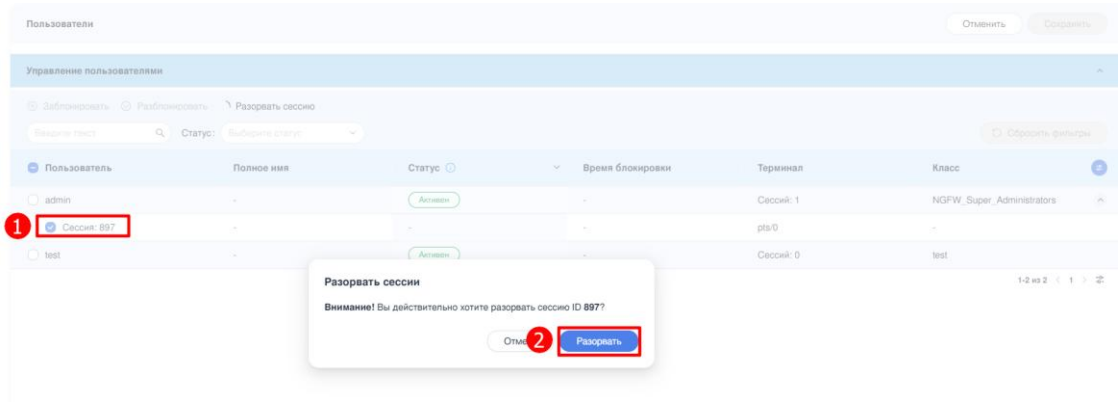


Рисунок – Завершение сессии по идентификатору.

После подтверждения выбранная сессия будет немедленно завершена. Пользователь теряет доступ в рамках данного сеанса.

Завершение всех сессий пользователя

Для завершения всех активных сессий выбранного пользователя необходимо выполнить следующие действия:

1. В таблице **«Управление пользователями»** выбрать учётную запись, установив флажок слева от логина. Поддерживается выбор нескольких пользователей для массового завершения сессий.
2. Нажать **кнопку «Разорвать сессии»**.
3. В открывшемся диалоговом окне подтвердить операцию, нажав **кнопку «Разорвать»** (см. Рисунок – Завершение всех сессий пользователя).

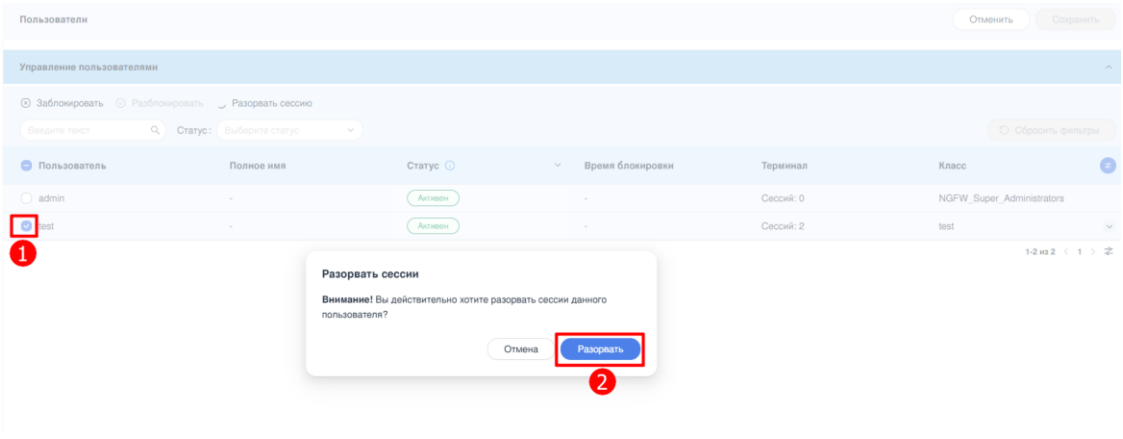


Рисунок – Завершение всех сессий пользователя.

Все активные сессии выбранных пользователей будут немедленно завершены. Фоновые сессии (например, системные) также подлежат завершению.

Примечание:

Сессии пользователей веб-интерфейса не отображаются в таблице **«Управление пользователями»** и не подлежат принудительному завершению через данный интерфейс. Для разрыва таких сессий требуется выполнить блокировку

соответствующей учётной записи. Данная операция недоступна для встроенной учётной записи **«admin»**.

3 ИНТЕРФЕЙСЫ

ARMA Стена поддерживает множество типов интерфейсов, используя как сетевые интерфейсы, так и различные сетевые протоколы.

Для просмотра всех интерфейсов системы, их настройки и создания новых необходимо перейти в раздел **«Настройки интерфейсов»** (см. Рисунок – Панель настройки интерфейсов).

Рисунок – Панель настройки интерфейсов

Примечание:

В веб-интерфейсе реализована функциональность конфигурирования только физических интерфейсов и сетевого моста. Для настройки всех остальных сетевых интерфейсов необходимо использовать интерфейс командной строки (**CLI**).

Примечание:

Перед удалением сетевых интерфейсов требуется обязательно исключить их из состава всех сервисов и служб, в которых они используются. К таким службам могут относиться маршрутизация, NAT, МЭ, балансировка нагрузки, VPN-туннели, СОВ и др. Невыполнение данного шага может привести к нарушению сетевой связности, сбоям в работе сервисов или ошибкам в конфигурации. Рекомендуется проверить все зависимости перед выполнением операции удаления интерфейса.

3.1 Физический интерфейс

Физические интерфейсы получают имена в формате **«ethN»**, где **«N»** — идентификатор, присвоенный интерфейсу.

3.1.1 Настройки физического интерфейса

Настройка физического интерфейса осуществляется в боковой панели **«Редактирование интерфейса»**, которая вызывается щелчком **ЛКМ** на нужном интерфейсе (см. Рисунок – Редактирование интерфейса).

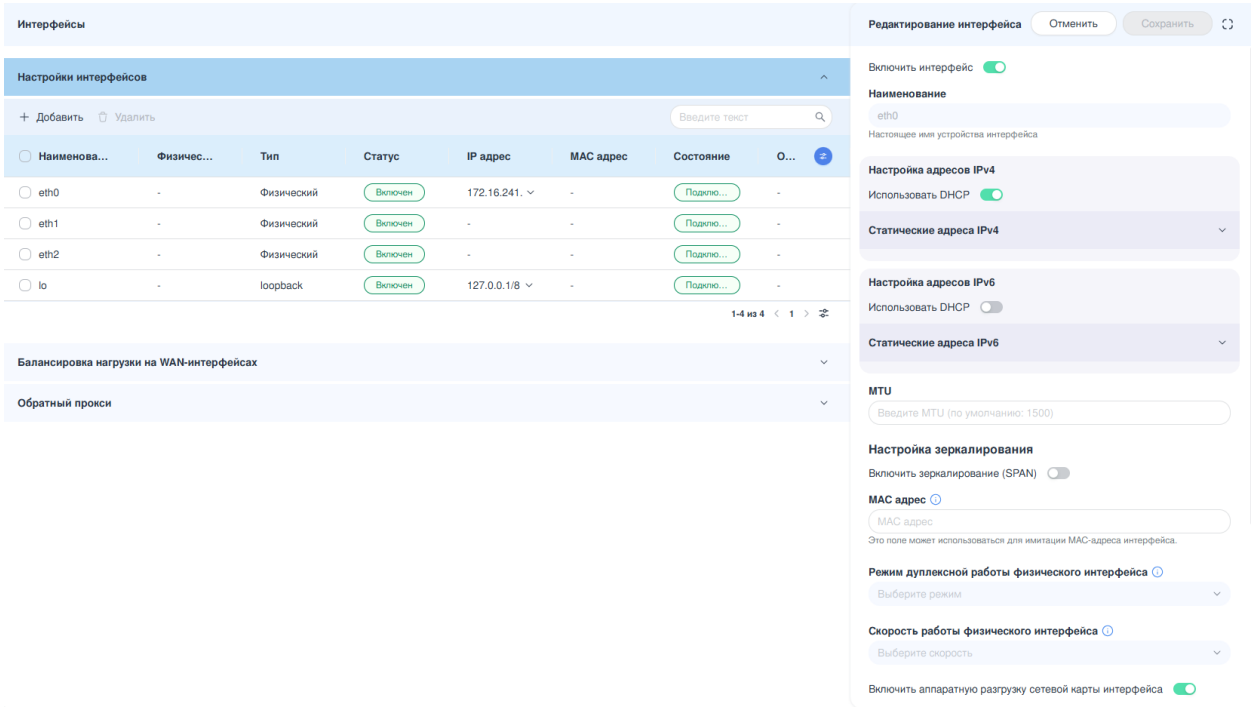


Рисунок – Редактирование интерфейса

Параметры интерфейса:

- **«Включить интерфейс»** - включение/выключение физического интерфейса.
- **«Настройка адресов IPv4»** - блок параметров для конфигурации IPv4-адресов. Поддерживается установка нескольких IPv4-адресов для одного интерфейса. Для автоматического получения адреса по протоколу DHCP необходимо перевести переключатель **«Использовать DHCP»** в активное состояние. Для ручного назначения статических адресов требуется раскрыть опцию **«Статические адреса IPv4»**, нажать **кнопку «+ Добавить»**, и ввести IPv4-адрес и маску подсети. **Кнопки «Добавить»** и **«Удалить»** позволяют добавлять новые строки с адресами или удалять существующие.
- **«Настройка адресов IPv6»** - блок параметров для конфигурации IPv6-адресов. Поддерживается установка нескольких IPv6-адресов для одного интерфейса. Для автоматического получения адреса по протоколу DHCP необходимо перевести переключатель **«Использовать DHCP»** в активное состояние. Для ручного назначения статических адресов требуется раскрыть опцию **«Статические адреса IPv6»**, нажать **кнопку «+ Добавить»**, и ввести IPv6-адрес и маску подсети. **Кнопки «Добавить»** и **«Удалить»** позволяют добавлять новые строки с адресами или удалять существующие.
- **«MTU»** - значение MTU. Возможно указать значение в диапазоне от «1280» до «9190». По умолчанию используется значение «1500». Значение MTU не может быть меньше значения MTU дочернего VLAN интерфейса.
- **«Включить зеркалирование (SPAN)»** - настройка копирование входящего/исходящего трафика:

- **«Входящий трафик»** - выбор интерфейса, на который будет выполняться зеркалирование входящего трафика;
- **«Исходящий трафик»** - выбор интерфейса, на который будет выполняться зеркалирование исходящего трафика.

Примечание:

Невозможно назначить сетевой мост для зеркалирования трафика сетевого интерфейса, если данный интерфейс является участником этого сетевого моста.

Примечание:

Зеркалирование трафика на субинтерфейс VLAN сетевого интерфейса не может быть реализован даже при применении промежуточных этапов перенаправления трафика.

- **«MAC-адрес»** - пользовательский MAC-адрес. Имитацию MAC-адреса интерфейса возможно использовать, например, при определённых кабельных соединениях WAN интерфейса. Формат ввода значения MAC-адреса «xx:xx:xx:xx:xx:xx».
- **«Режим дуплексной работы физического интерфейса»** - настройка параметров дуплексного режима работы физического интерфейса. Возможный выбор значений:
  - **«auto»** - настройка двустороннего режима интерфейса согласовывается автоматически;
  - **«full»** - использовать полнодуплексный режим;
  - **«half»** - использовать полудуплекс.

  Для каждой сетевой карты отображается свой список допустимых значений. Недоступно для редактирования в сетевой карте, использующей один из драйверов: «vmxnet3», «virtio_net», «xen_netfront», «iavf», «ice», «i40e», «veth».
- **«Скорость работы физического интерфейса»** - установка скорости работы интерфейса. Недоступно для редактирования в сетевой карте, использующей один из драйверов: «vmxnet3», «virtio_net», «xen_netfront», «iavf», «ice», «i40e», «veth».
- **«Включить аппаратную разгрузку сетевой карты интерфейса»** - позволяет снизить нагрузку на ЦП.
  - **«Тип аппаратной разгрузки сетевой карты интерфейса»** - выбор метода разгрузки обработки стека TCP/IP.
- **«Отключить контроль потоков (IEEE 802.3x)»** - механизм временной остановки передачи данных в компьютерных сетях. Целью этого механизма

является обеспечение нулевой потери пакетов при перегрузке сети. Недоступно для редактирования в сетевой карте, использующей один из драйверов: «vmxnet3», «virtio_net», «xen_netfront», «iavf», «ice», «i40e», «veth».

- **«Отключить мониторинг состояния интерфейса (link-detect)»** - отключить контроль физических состояний интерфейса, например, при отключении кабеля.
- **«Описание»** - краткое текстовое описание. Допускается использование символов кириллического и латинского алфавитов. Описание не должно начинаться с последовательности «//». Запрещено использование символов «"», «'» и перенос строки. Максимальная длина значения — «127» символов.

Для применения и сохранения настроек в конфигурационный файл необходимо нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»** (см. Рисунок – Применить и сохранить новые настройки в конфигурационный файл).

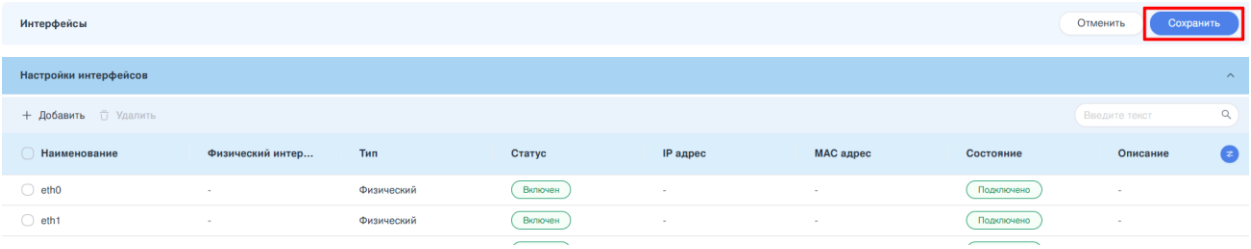


Рисунок – Применить и сохранить новые настройки в конфигурационный файл

3.1.2 Виртуальный интерфейс

Виртуальные интерфейсы имеют имена в формате **«ethN.M»**, где **«M»** — значение VLAN-тега, указанное при создании виртуального интерфейса.

Для создания виртуального интерфейса необходимо выполнить следующие действия:

1. В окне **«Настройка интерфейсов»** нажать **кнопку «+Добавить»**.
2. В открывшейся боковой панели выбрать создаваемый объект **«Виртуальный интерфейс»** и заполнить параметры:
   - **«Наименование»** - наименование VLAN. Назначается автоматически на основе имени физического интерфейса и VLAN-тег;
   - **«Включить интерфейс»** - включение/выключение виртуального интерфейса;
   - **«Физический интерфейс»** - выбор физического интерфейса, на котором будет создан сегмент виртуальной сети;
   - **«VLAN-тег»** - метка виртуальной сети. Возможно указать значение в диапазоне от «0» до «4094»;

- **«Тип конфигурации IPv4»** - выбор настройки IP-адреса: «отключён», «ручная настройка», «DHCPv4»;
- **«Тип конфигурации IPv6»** - выбор настройки IP-адреса: «отключён», «ручная настройка», «DHCPv6»;
- **«MTU»** - значение MTU. Возможно указать значение в диапазоне от «1280» до «9190». По умолчанию используется значение «1500». Значение MTU должно быть меньшим или равным значению MTU родительского интерфейса;
- **«MAC-адрес»** - пользовательский MAC-адрес. Формат ввода значения MAC-адреса «xx:xx:xx:xx:xx:xx»;
- **«Отключить мониторинг состояния интерфейса (link-detect)»** - отключить контроль физических состояний интерфейса, например, при отключении кабеля.
- **«Описание»** - краткое текстовое описание. Допускается использование символов кириллического и латинского алфавитов. Описание не должно начинаться с последовательности «//». Запрещено использование символов «"», «'» и перенос строки. Максимальная длина значения — «127» символов.

3. По завершению нажать **кнопку «Сохранить»** (см. Рисунок – Добавление виртуального интерфейса).

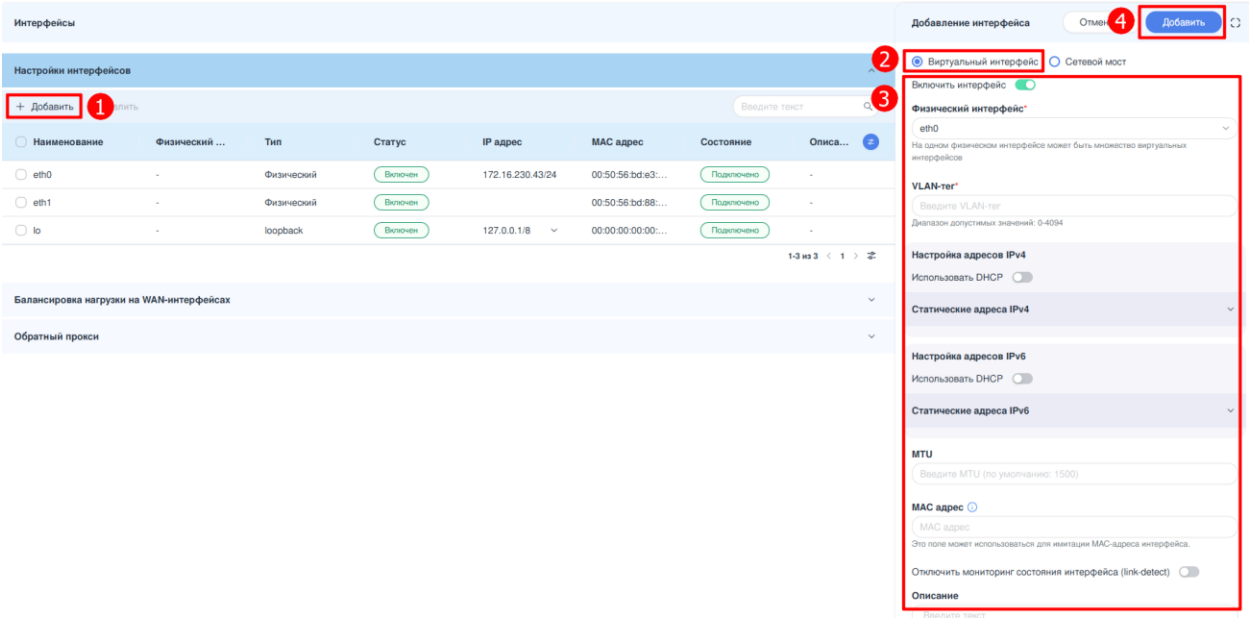


Рисунок – Добавление виртуального интерфейса

4. Нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»** для применения и сохранения новых настроек в конфигурационный файл.

Примечание:

Невозможно создать виртуальные интерфейсы для физического интерфейса, который участвует в сетевом мосте с поддержкой VLAN.

3.1.3 Редактирование интерфейса

Для редактирования интерфейса необходимо выполнить следующие действия:

1. Нажать **ЛКМ** на нужном интерфейсе в окне **«Настройка интерфейсов»**.
2. В открывшейся боковой панели **«Редактирование интерфейса»** внести необходимые изменения и нажать **кнопку «Сохранить»**.
3. Нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»**.

Примечание:

Если сетевой интерфейс является частью сетевого моста, то настройка адреса будет невозможна.

Примечание:

В случае добавления интерфейса в список прослушиваемых интерфейсов ретрансляции DHCP, на нём требуется наличие как минимум одного статически назначенного IP-адреса. Удаление всех IP-адресов с такого интерфейса запрещено и приведёт к нарушению функционирования сервиса ретрансляции DHCP.

3.1.4 Удаление интерфейса

Для удаления виртуальных интерфейсов необходимо выполнить следующие действия:

1. Выбрать один или несколько интерфейсов для удаления, установив флажок в чек-боксе слева от наименования интерфейса, и нажать **кнопку «Удалить»**.
2. Подтвердить удаление нажатием **кнопки «Удалить»** в открывшемся окне (см. Рисунок – Удаление виртуального интерфейса).
3. Нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»**.

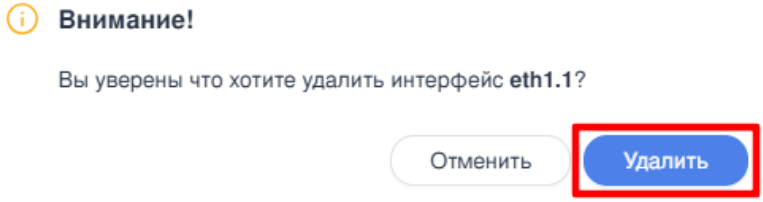


Рисунок – Удаление виртуального интерфейса

Примечание:

Физические интерфейсы не подлежат удалению. При одновременном выборе физических и виртуальных интерфейсов **кнопка «Удалить»** блокируется в интерфейсе управления.

Примечание:

Удаление интерфейсов, задействованных в процессе ретрансляции DHCP, не допускается.

Примечание:

Если сетевой интерфейс включён в состав сетевого моста, операция его удаления будет заблокирована, и система выдаст соответствующее предупреждение (см. Рисунок – Удаление невозможно).

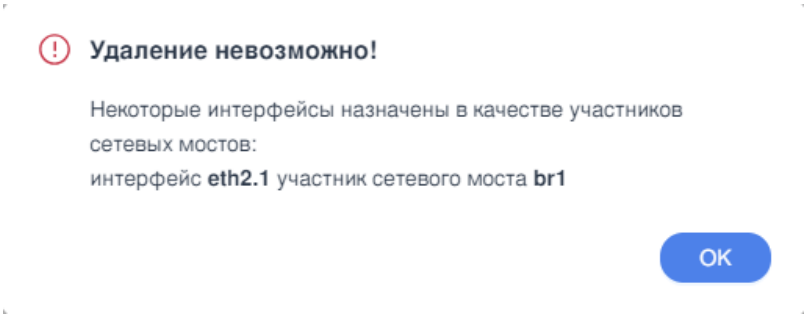


Рисунок – Удаление невозможно

3.2 Сетевой мост

Сетевой мост - это сетевое устройство, предназначенное для объединения сегментов сети передачи данных в единую сеть. Он функционирует на канальном уровне модели OSI, обеспечивая прозрачное прохождение протоколов через него.

Примечание:

Протокол **STP** по умолчанию не активирован в системе **ARMA Стена**. Однако его возможно активировать в процессе настройки сетевого моста.

В **ARMA Стена** добавление и настройка сетевых мостов производится в разделе **«Настройки интерфейсов»** (см. Рисунок – Панель настройки интерфейсов).

При создании сетевого моста формируется новый сетевой интерфейс, который получает имя **«brN»**, где **«N»** — порядковый номер. На сетевом интерфейсе не должно быть настроек конфигурации IP-адреса перед добавлением его в сетевой мост. В составе сетевого моста поддерживаются следующие типы сетевых интерфейсов: Ethernet, Bond/Link Aggregation, L2TPv3, OpenVPN, VXLAN, WLAN/WIFI - Wireless LAN, Tunnel, GENEVE.

3.2.1 Создание сетевого моста

Для создания сетевого моста необходимо выполнить следующие действия:

1. В окне «Настройка интерфейсов» нажать **кнопку «+Добавить»**.
2. В открывшейся боковой панели «Добавление интерфейса» выбрать создаваемый объект **«Сетевой мост»** и заполнить параметры:
   - **«Включить интерфейс»** - позволяет включить или отключить сетевой мост. Отключение мостовой группы сохраняет текущие настройки. После отключения интерфейс переходит в состояние административного отключения (A/D).
   - **«Наименование»** - имя сетевого моста. Оно должно иметь вид «brN», где N представляет собой уникальный идентификатор сетевого моста, начинающийся с «0». Длина наименования не должна превышать «15» символов.
   - **«Участники»** - блок добавления сетевых интерфейсов в состав сетевого моста. **Кнопки «+Добавить»** и **«Удалить»** позволяют добавлять или удалять сетевые интерфейсы. На сетевом интерфейсе не должно быть настроек конфигурации IP-адреса перед добавлением его в сетевой мост.

     Примечание:

     Один и тот же сетевой интерфейс может быть участником только одного сетевого моста.

     Примечание:

     Нельзя назначить сетевой интерфейс на сетевой мост, если данный интерфейс настроен на зеркалирование трафика на этот сетевой мост.

     Дополнительные параметры:

     - **«Приоритет участника»** - приоритет для интерфейса, входящего в состав сетевого моста. Возможно указать значение в диапазоне от «1» до «63».
     - **«Разрешенные VLAN»** - идентификатор VLAN. Позволить указанным идентификаторам VLAN проходить через интерфейс сетевого моста. Возможно указать значение в диапазоне от «1» до «4094». Допускается указывать как один идентификатор VLAN, так и группу идентификаторов, разделённых дефисом (X-Y). **Кнопки «+Добавить»** и **«Удалить»** позволяют добавлять или удалять идентификатор VLAN. Невозможно использовать параметр «Разрешенные VLAN» на сетевом мосту, если не активирована опция «Поддержка VLAN».

- **«Цена (cost для STP)»** - стоимость пути для интерфейса, входящего в состав сетевого моста. Более быстрый интерфейс должен иметь более низкую стоимость. Возможно указать значение в диапазоне от «1» до «65535». Значение по умолчанию для стоимости пути рассчитывается исходя из пропускной способности канала (см. Таблица «Соответствия пропускной способности и назначаемой по умолчанию стоимости пути»).

Таблица «Соответствия пропускной способности и назначаемой по умолчанию стоимости пути»

Пропускная способность канала	Стоимость пути протокола STP для интерфейса
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

- **«Изолировать порт»** - при включении изолированный порт в частной виртуальной локальной сети (PVLAN) изолируется на втором уровне от любых других коммутаторов, кроме тех, которые настроены на режим promiscuous.
- **«Собственный VLAN ID (native-vlan)»** - указать идентификатор VLAN, который должен присутствовать на канале. Возможно указать значение в диапазоне от «1» до «4094». При поступлении пакета данных без тега VLAN на порт, пакет данных будет вынужден получить тег с определённым идентификатором VLAN. При выходе флага идентификатора VLAN из порта, тег идентификатора VLAN будет удалён. Невозможно использовать параметр «Собственный VLAN ID (native-vlan)» на сетевом мосту, если не активирована опция «Поддержка VLAN».

- **«Тип конфигурации IPv4»** - выбрать тип конфигурирования IPv4-адреса. При выборе «Ручная настройка» открываются дополнительные поля для указания IPv4-адреса. **Кнопки «+Добавить»** и **«Удалить»** позволяют добавлять или удалять IPv4-адреса.
- **«Тип конфигурации IPv6»** - выбрать тип конфигурирования IPv6-адреса. При выборе «Ручная настройка» открываются дополнительные поля для

указания IPv6-адреса. **Кнопки «+Добавить»** и **«Удалить»** позволяют добавлять или удалять IPv6-адреса.

- **«Включить зеркалирование (SPAN)»** - функция SPAN позволяет дублировать входящий и исходящий трафик, проходящий через сетевой мост на указанный интерфейс. Обычно данный интерфейс подключается к специализированному оборудованию, такому как системы контроля поведения и обнаружения вторжений. Преимущество функции SPAN состоит в том, что она позволяет отделить приложение от основного трафика, что предотвращает влияние приложения на общий поток данных и производительность системы. При включении SPAN необходимо указать дополнительные параметры:
    - **«Входящий трафик»** - выбрать интерфейс, на который будет дублироваться весь входящий трафик сетевого моста;
    - **«Исходящий трафик»** - выбрать интерфейс, на который будет дублироваться весь исходящий трафик сетевого моста;
- **«Приоритет»** - указать приоритет пересылки сетевого моста в рамках связующего дерева. Значение приоритета учитывается при выборе корневого элемента связующего дерева. Чем меньше значение, присвоенное сетевому мосту, тем выше его приоритет и тем больше вероятность того, что данный сетевой мост будет выбран в качестве корневого элемента связующего дерева. Возможно указать значение в диапазоне от «0» до «65535». По умолчанию используется значение «32768».
- **«MTU»** - значение MTU. Возможно указать значение в диапазоне от «1280» до «16000». По умолчанию используется значение «1500».
- **«MAC адрес»** - данное поле возможно использовать для имитации MAC-адреса интерфейса. В поле необходимо ввести MAC-адрес в формате XX:XX:XX:XX:XX:XX или оставить поле пустым. Эта операция может потребоваться, например, при определённых типах кабельных соединений WAN-интерфейса.
- **«Отключить мониторинг состояния интерфейса (link-detect)»** - система не будет отслеживать изменения физического состояния канала связи, например, в случае отсоединения кабеля.
- **«Поддержка VLAN»** - включить поддержку VLAN на данном сетевом мосту.

Примечание:

В случае если интерфейсы, участвующие в сетевом мосту, имеют дочерние VLAN-интерфейсы, то функция поддержки VLAN на этом мосту будет недоступна.

- **«Протокол связующего дерева (STP)»** - включить протокол STP на сетевом мосту.
- **«Задержка пересылки STP»** - значение времени задержки пересылки в секундах. Время задержки пересылки — это время, в течение которого устройство находится в состоянии прослушивания и обучения перед переходом в состояние пересылки. Это время необходимо для того, чтобы новое устройство, подключённое к загруженной сети, могло проанализировать трафик перед началом работы. Возможно указать значение в диапазоне от «2» до «30». По умолчанию используется значение «14».
- **«Интервал приветствий STP»** - значение интервала времени в секундах. Возможно указать значение в диапазоне от «1» до «10». По умолчанию используется значение «2». Параметр используется для настройки интервала времени, через который мостовая группа отправляет пакеты «hello». Пакеты «hello» представляют собой блоки BPDU (Bridge Protocol Data Units), которые используются для передачи информации о структуре топологии сети.
- **«Время хранения MAC-адреса»** - интервал времени хранения, в секундах, по истечении которого MAC-адрес удаляется из таблицы пересылки. Возможно указать значение в диапазоне от «10» до «1000000». По умолчанию используется значение «300». При значении «0» функция MAC-адресного обучения отключается (всегда используется широковещательная передача).
- **«Время жизни других коммутаторов (max-age)»** - значение интервала времени, в секундах, в течение которого сетевой мост ожидает получения пакета «hello» перед перевычислением топологии связующего дерева. Возможно указать значение в диапазоне от «6» до «40». По умолчанию используется значение «20».
- **«Включить IGMP»** - включить IGMP/MLD querier.

3. По завершению нажать **кнопку «Сохранить»** (см. Рисунок – Добавление сетевого моста).
4. Нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»**.

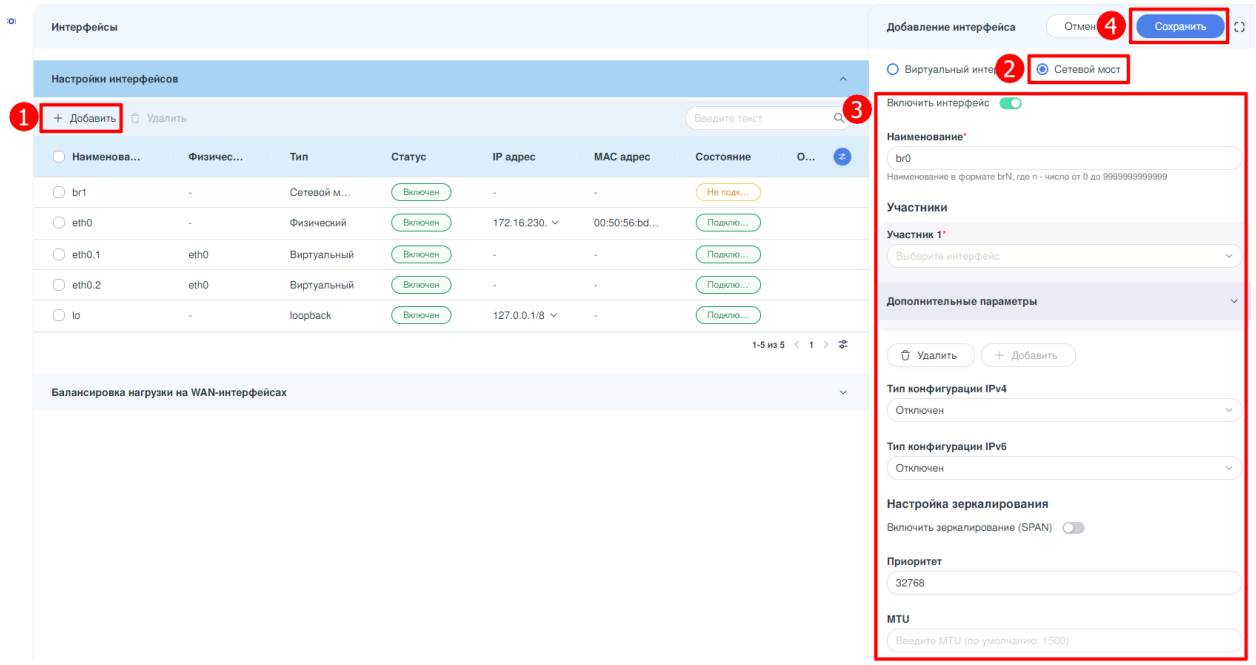


Рисунок – Добавление сетевого моста

3.2.2 Редактирование сетевого моста

Для редактирования сетевого моста необходимо выполнить следующие действия:

1. Нажать **ЛКМ** на нужном интерфейсе сетевого моста в окне **«Настройка интерфейсов»**.
2. В открывшейся боковой панели «Редактирование интерфейса» внести необходимые изменения и нажать **кнопку «Сохранить»**.
3. Нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»**.

> **Примечание:**
>
> При изменении участников сетевого моста с включённой поддержкой VLAN не допускается указывать интерфейсы, которые имеют дочерние VLAN.

3.2.3 Удаление сетевого моста

Для удаления сетевого моста необходимо выполнить следующие действия:

1. Выбрать один или несколько сетевых мостов для удаления, установив флажок в чек-боксе слева от наименования интерфейса, и нажать **кнопку «Удалить»**.
2. Подтвердить удаление нажатием **кнопки «Удалить»** в открывшемся окне (см. Рисунок – Удаление сетевого моста).

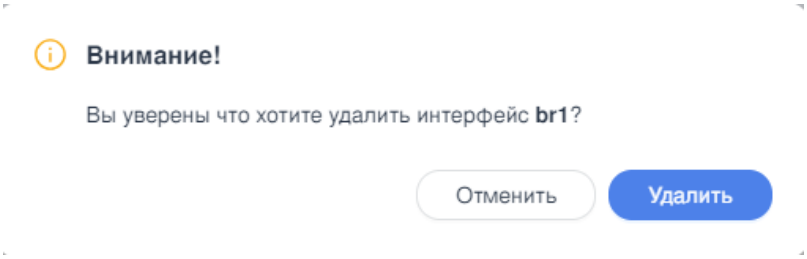


Рисунок – Удаление сетевого моста

3. Нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«Интерфейсы»**.

4 СИСТЕМНЫЕ НАСТРОЙКИ

В настоящем разделе представлено описание раздела меню **«Системные настройки»**, предусматривающего механизм управления следующими функциями:

- настройка системного DNS;
- настройка системного прокси;
- настройка шлюза по умолчанию;
- управление версиями конфигурации системы;
- мониторинг текущего состояния аппаратной платформы.

Для перехода в раздел **«Системные настройки»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«Системные настройки»** (см. Рисунок – Системные настройки).

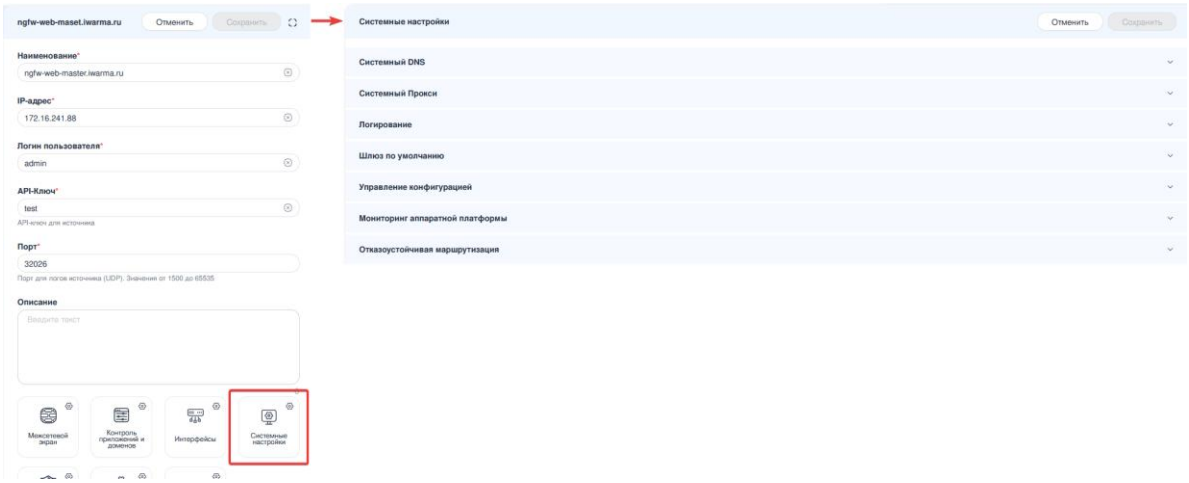


Рисунок – Системные настройки

Применение и сохранение системных настроек

После завершения настройки всех необходимых параметров в подразделах раздела **«Системные настройки»** необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Системные настройки»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**, в котором отображается список подразделов, затронутых внесёнными изменениями. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

Только после успешного подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

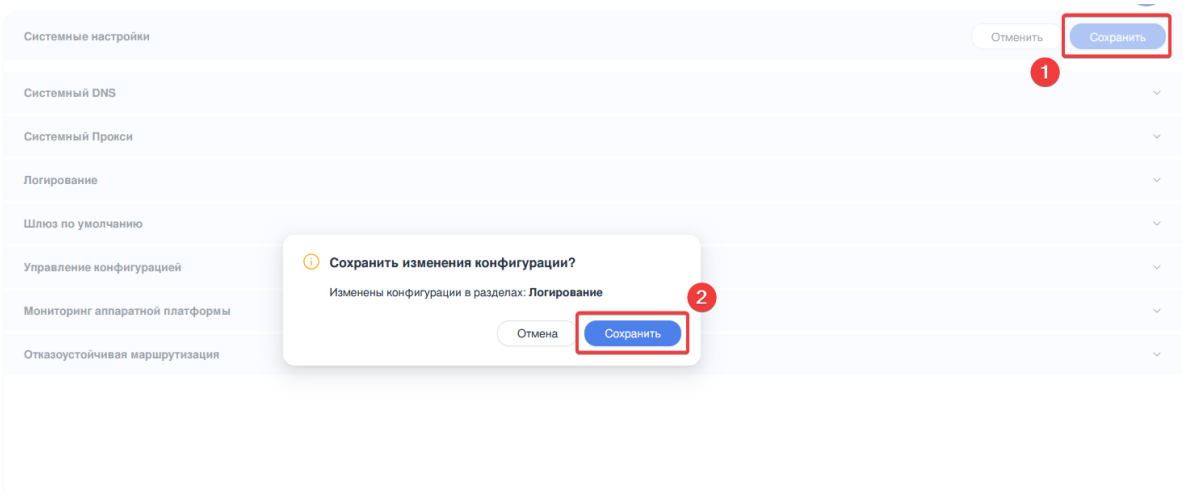


Рисунок – Применение и сохранение настроек

При необходимости отменить все неприменённые настройки следует нажать **кнопку «Отмена»**, расположенную в верхнем правом углу заголовка раздела **«Системные настройки»**. В этом случае конфигурация раздела **«Системные настройки»** будет откатана к последнему сохранённому состоянию.

Примечание:

Для подраздела **«Шлюз по умолчанию»** общий механизм сохранения и применения настроек не используется. Изменения в этом подразделе применяются отдельно — сразу после нажатия **кнопки «Сохранить»** в соответствующем окне настроек шлюза.

4.1 Системный DNS

Данный раздел содержит настройки DNS сервисов, использующиеся для обработки DNS-запросов.

4.1.1 Адреса серверов

Для добавления адреса сервера DNS необходимо выполнить следующие действия:

1. В разделе **«Системные настройки»** выбрать подраздел **«Системный DNS»**. В блоке **«Адреса серверов»** нажать **кнопку «+Добавить»**.
2. В открывшейся боковой панели выбрать тип:
   - **IPv4** — для указания IPv4-адреса;
   - **IPv6** — для указания IPv6-адреса;
   - **Интерфейс** — для привязки к сетевому интерфейсу.
3. При выборе типа **IPv4** или **IPv6** ввести соответствующий IP-адрес в поле **«IPv4 | IPv6 адрес сервера»**. При выборе типа **«Интерфейс»** указать в поле **«Интерфейс»** имя требуемого сетевого интерфейса из выпадающего списка.

4. Нажать **кнопку «Сохранить»**. В левой нижней части окна отобразится уведомление об успешном добавлении адреса DNS-сервера (см. Рисунок – Добавление адреса DNS сервера).

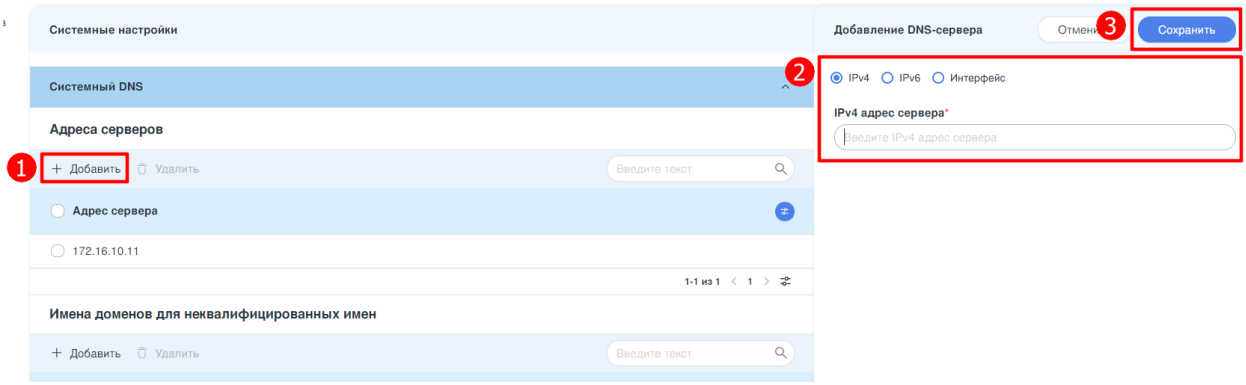


Рисунок – Добавление адреса DNS сервера

Для изменения параметров существующего адреса DNS-сервера необходимо нажать **ЛКМ** на строке редактируемого адреса и в открывшейся боковой панели внести корректировки. По завершению нажать **кнопку «Сохранить»**.

Для удаления одного или нескольких адресов DNS-серверов необходимо установить флажок в чек-боксе слева от адреса сервера и нажать **кнопку «Удалить»**. Подтвердить удаление в открывшемся окне нажатием **кнопки «Удалить»**.

4.1.2 Имена доменов для неквалифицированных имён

Для добавления домена необходимо в блоке **«Имена доменов для неквалифицированных имён»** нажать **кнопку «+Добавить»**. В открывшемся окне **«Добавить доменное имя»** ввести требуемое доменное имя (см. Рисунок – Добавление доменного имени) и нажать **кнопку «Сохранить»**.

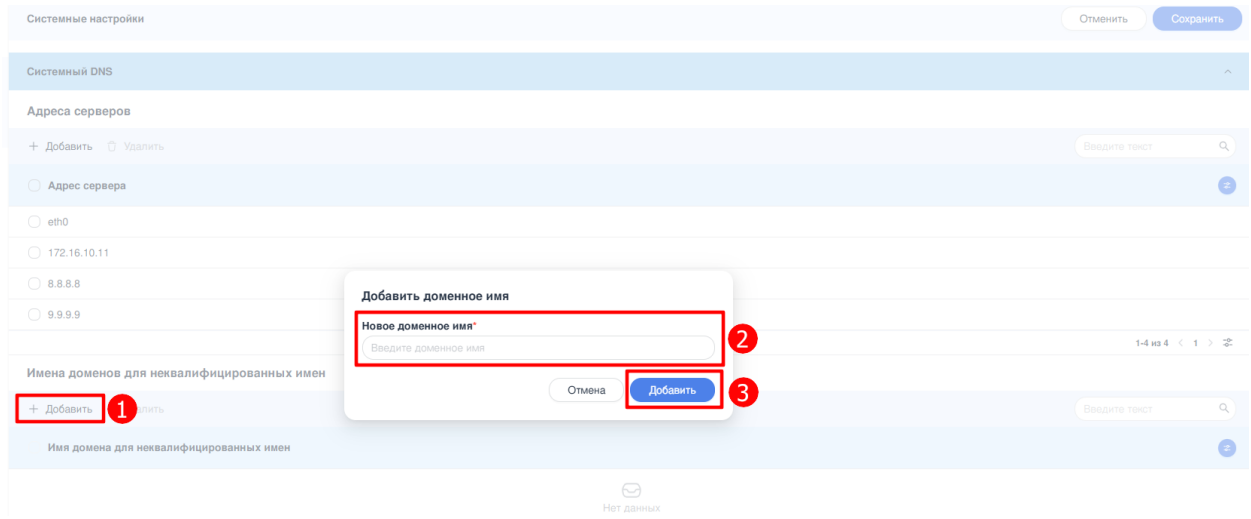


Рисунок – Добавление доменного имени

Для редактирования настроек домена необходимо нажать **ЛКМ** на строке редактируемого домена и в открывшемся окне внести изменения. По завершению нажать **кнопку «Сохранить»**.

Для удаления домена необходимо установить флажок в чек-боксе слева от имени домена и нажать **кнопку «Удалить»**. Подтвердить удаление в открывшемся окне нажатием **кнопки «Удалить»**.

4.2 Системный Прокси

В некоторых IT-средах для подключения к сети Интернет необходимо использовать прокси-сервер.

Для настройки системного прокси необходимо выполнить следующие действия:

1. В разделе **«Системные настройки»** выбрать подраздел **«Системный Прокси»**.
2. В поле **«Адрес прокси (url)»** ввести url-адрес прокси-сервера. Адрес должен начинаться с **«http://»** или с **«https://»**.
3. В поле **«Порт»** указать порт подключения к прокси. Возможно указать значение в диапазоне от **«1»** до **«65535»**.
4. В случае необходимости, ввести имя пользователя и пароль в соответствующие поля. Допускается использование латинских букв (a–z, A–Z), цифр (0–9) и специальных символов, за исключением символов «"» и «'». Имя пользователя должно иметь длину не более 128 символов.

   Примечание:

   Имя пользователя и пароль не должны начинаться со спецсимвола «//» или пробела.

5. Завершить настройку, нажав **кнопку «Сохранить»** (см. Рисунок – Настройка системного прокси).

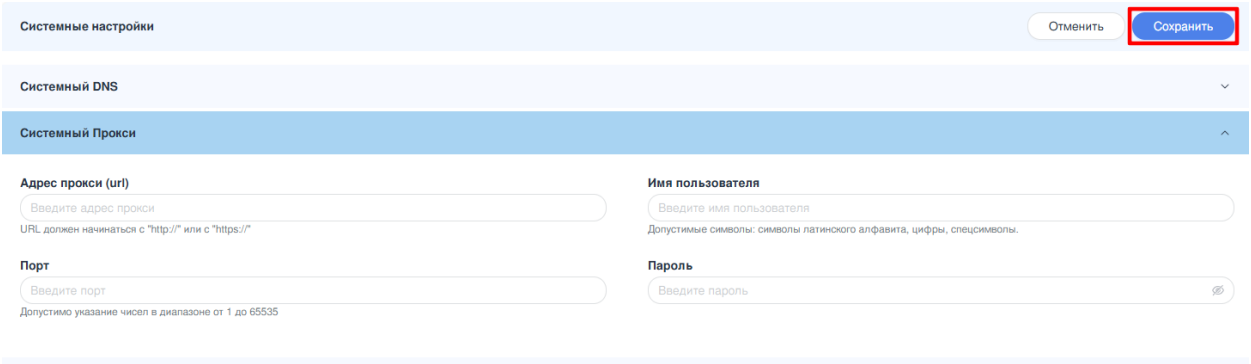


Рисунок – Настройка системного прокси

4.3 Шлюз по умолчанию

Для настройки шлюза по умолчанию необходимо в разделе **«Системные настройки»** выбрать подраздел **«Шлюз по умолчанию»**. В поле «IPv4-адрес шлюза по умолчанию» следует указать IPv4-адрес шлюза. После этого необходимо нажать кнопку «Сохранить» (см. Рисунок – Настройка шлюза по умолчанию). Допускается указание только одного шлюза.

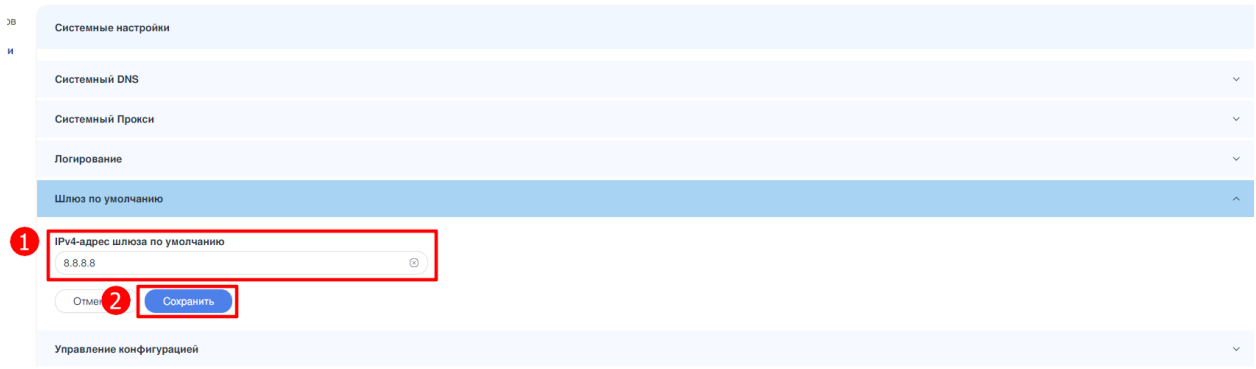


Рисунок – Настройка шлюза по умолчанию

4.4 Управление конфигурацией

ARMA Стена имеет встроенную систему управления версиями конфигурации. Она автоматически создаёт резервные копии всех предыдущих конфигураций, сохранённых в системе. Конфигурации хранятся в локальных версиях для быстрого восстановления при необходимости, а также могут быть сохранены на удалённом хосте для архивирования и резервного копирования.

ARMA Стена использует единый конфигурационный файл для всей системы — **/config/config.boot**. Это позволяет легко создавать шаблоны, делать резервные копии и тиражировать конфигурацию системы.

Для просмотра и управления архивами конфигурации системы необходимо в разделе **«Системные настройки»** выбрать подраздел **«Управление конфигурацией»** (см. Рисунок – Управление конфигурацией).

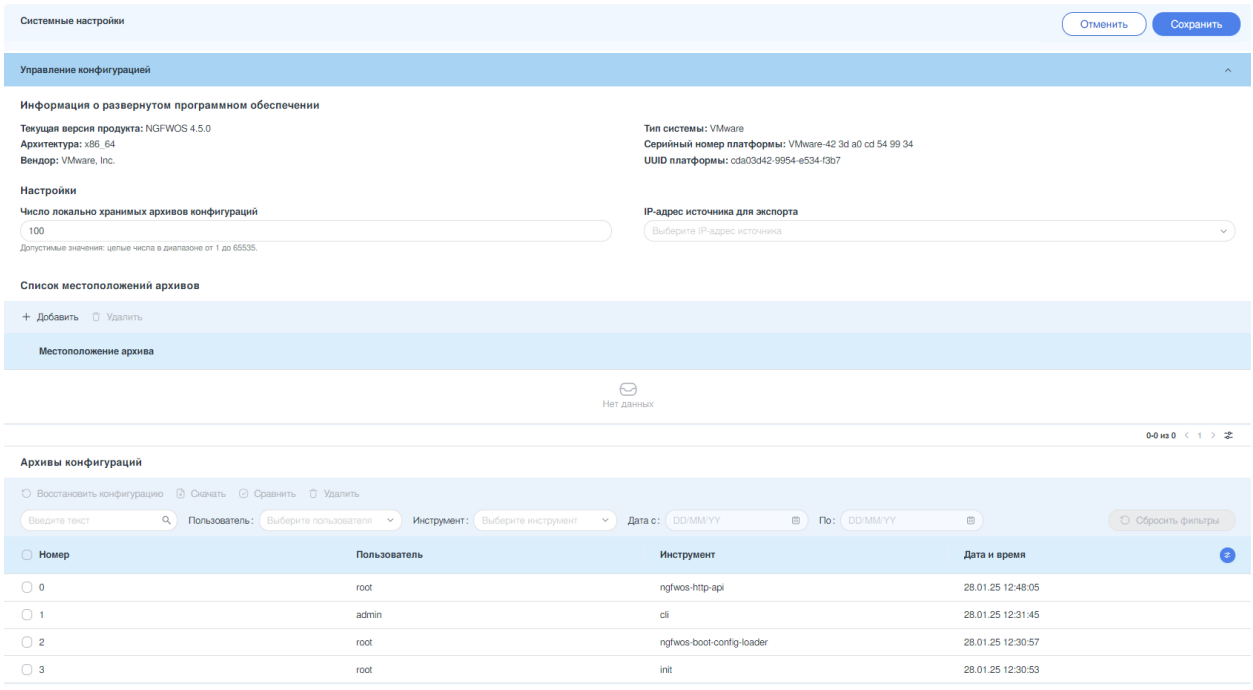


Рисунок – Управление конфигурацией

Примечание:

Конфигурация с меткой **«init»** в столбце **«Инструмент»** таблицы **«Архивы конфигураций»** заблокирована для просмотра, восстановления и скачивания. Это связано с тем, что указанная конфигурация не содержит настроек системы, и любые манипуляции с этой конфигурацией могут привести к нарушению стабильной работы устройства.

При осуществлении множественного выбора архивов, включающего конфигурацию с меткой **«init»**, функционал управления архивами становится недоступным. Для обеспечения возможности выполнения операций с другими архивами необходимо исключить конфигурацию с меткой «init» из списка выбранных объектов.

В верхней части окна подраздела **«Управление конфигурацией»** отображается краткая информация о программном обеспечении (см. Рисунок – Информация о развёрнутом программном обеспечении).

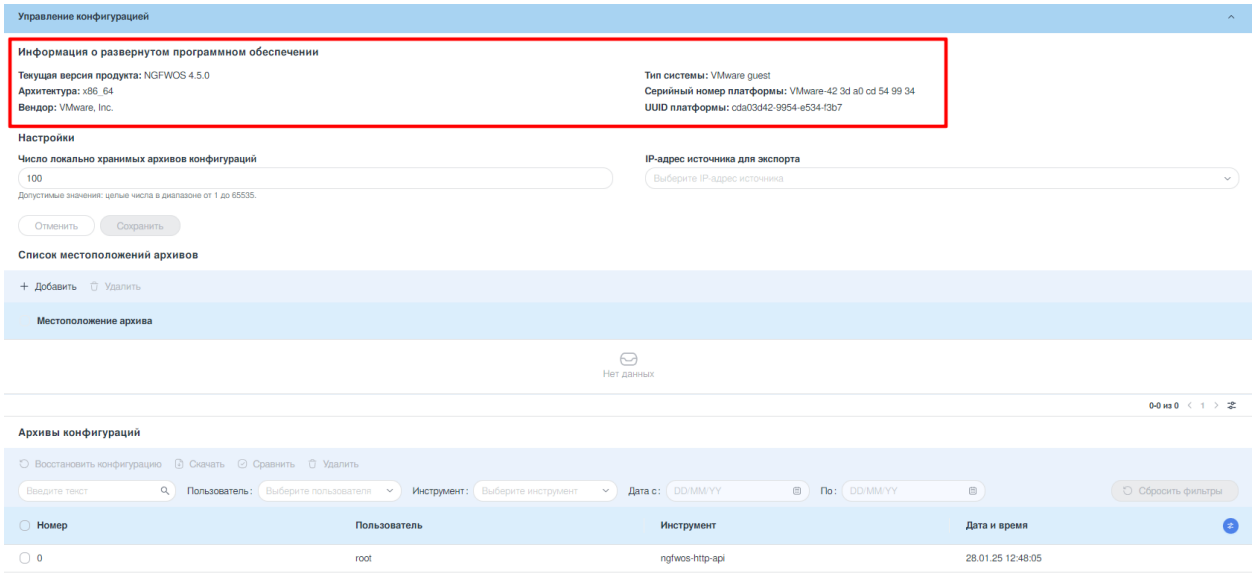


Рисунок – Информация о развёрнутом программном обеспечении

4.4.1 Настройки архива конфигурации

Блок **«Настройки»** позволяет настраивать параметры архивации конфигурации системы **ARMA Стена**.

В данном блоке существует возможность задать количество локально хранимых архивов конфигураций, а также настроить резервное копирование и архивирование конфигураций на удалённые хосты. Дополнительно предусмотрена возможность указания IP-адреса источника для экспорта конфигураций.

Для применения изменённых параметров необходимо нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу раздела **«Системные настройки»** (см. Рисунок – Настройки архива конфигураций).

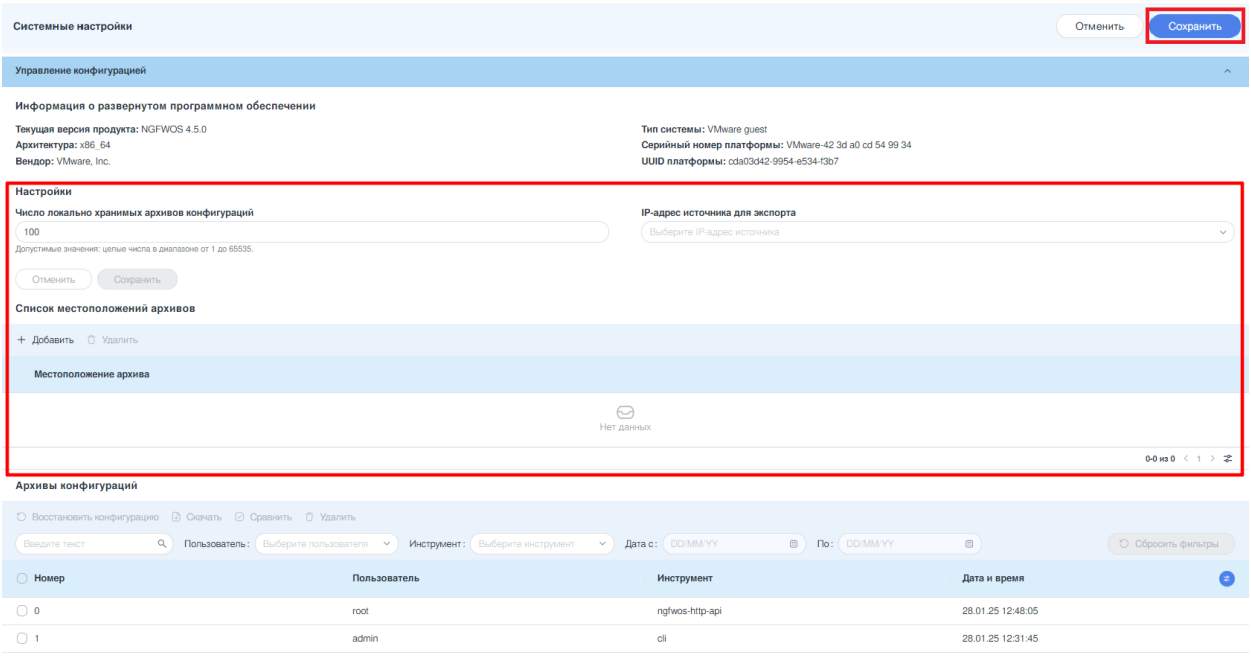


Рисунок – Настройки архива конфигураций

Настройки локальных версий конфигурации.

Для определения максимального количества локальных версий конфигурации необходимо указать в поле **«Число локально хранимых архивов конфигураций»** количество архивов в диапазоне от «1» до «65535» и нажать **кнопку «Сохранить»**. По умолчанию система сохраняет «100» копий архива конфигураций. В случае достижения установленного лимита хранящихся версий, произойдёт перезапись самой ранней сохранённой версии.

IP-адрес источника для экспорта.

Данный параметр позволяет задать IP-адрес, с которого будет производиться подключение к удалённому хосту. IP-адрес источника для экспорта выбирается из выпадающего списка, который включает IPv4- и IPv6-адреса всех интерфейсов системы.

Добавление удалённого расположения архива.

Для настройки резервного копирования и архивации конфигураций на удалённый хост необходимо выполнить следующие действия (см. Рисунок – Добавление удалённого расположения архива):

1. В таблице **«Список местоположений архивов»** нажать **кнопку «+Добавить»**.
2. В открывшемся окне в поле **«Адрес месторасположения архива»** ввести параметры удалённого хоста в формате **«URL»**. Поле может содержать не более 1024 символов. Для удалённого расположения архива конфигурации возможно использование следующих шаблонов **«URI»**:
   - **http://<user>:<passwd>@<host>:/<dir>**

- **https://<user>:<passwd>@<host>:/<dir>**
- **ftp://<user>:<passwd>@<host>/<dir>**
- **sftp://<user>:<passwd>@<host>/<dir>**
- **scp://<user>:<passwd>@<host>/<dir>**
- **tftp://<host>/<dir>**
- **git+https://<user>:<passwd>@<host>/<path>**

где:

- **<user>** – имя УЗ;
- **<passwd>** – пароль УЗ;
- **<host>** – адрес компьютера;
- **<dir>** – директория для сохранения файла конфигурации.

3. Нажать **кнопку «Добавить»**. В случае успешного добавления удалённого расположения архива появится соответствующее уведомление.

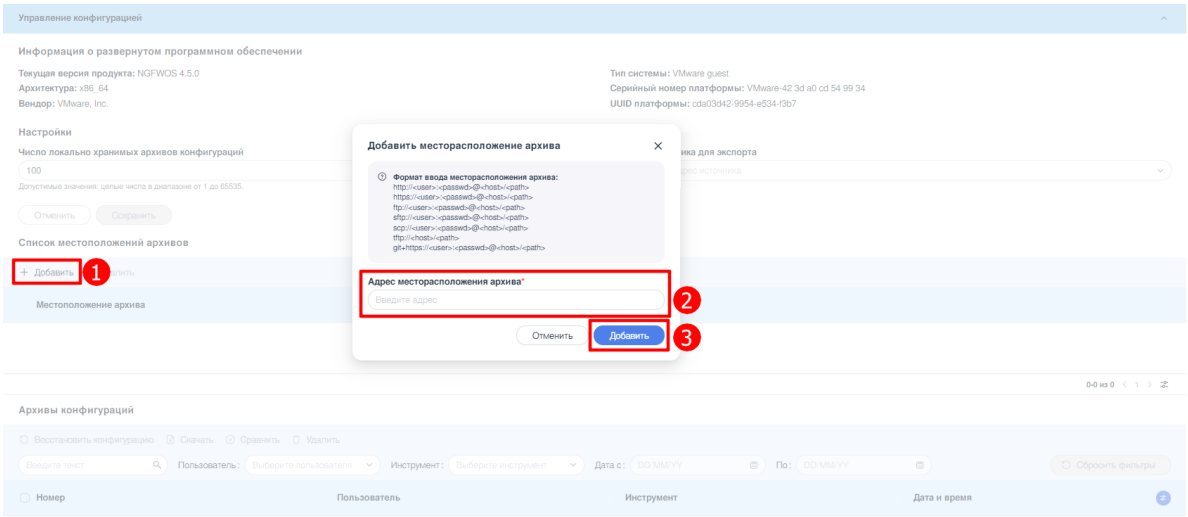


Рисунок – Добавление удалённого расположения архива

Система **ARMA Стена** будет экспортировать конфигурацию на удалённый сервер каждый раз при применении и сохранении изменений в конфигурации.

Удаление настроек удалённого расположения архива.

Для удаления настроек удалённого расположения архива необходимо выполнить следующие действия (см. Рисунок – Удаление настроек удалённого расположения архива):

1. Выбрать необходимые удалённые хосты, установив флажок слева от значений столбца **«Местоположение архива»**.
2. На панели инструментов нажать **кнопку «Удалить»**.
3. Подтвердить удаление, нажав **кнопку «Удалить»** в открывшемся окне.

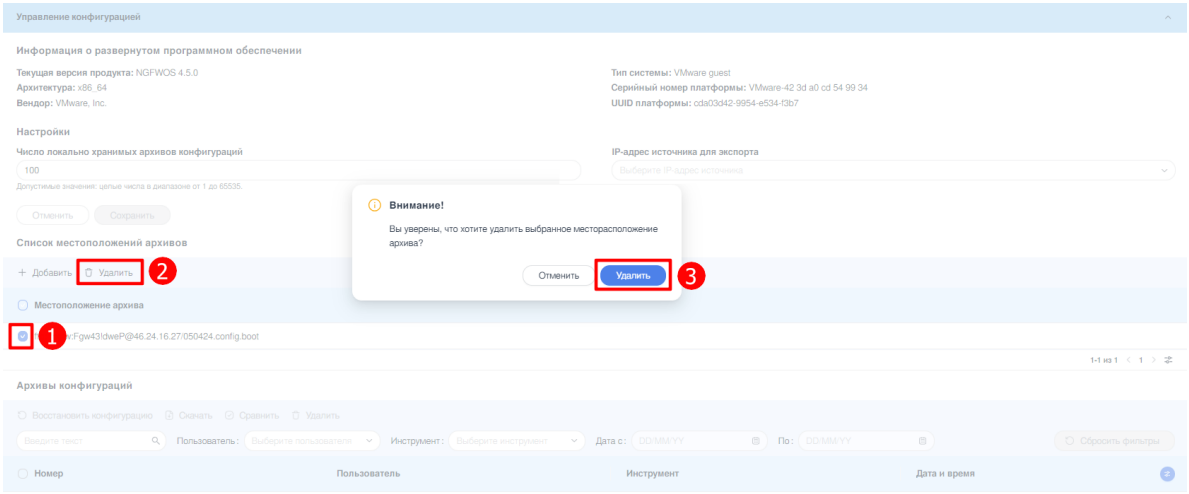


Рисунок – Удаление настроек удалённого расположения архива

4.4.2 Просмотр конфигурации

Для просмотра настроек архивной конфигурации необходимо нажать **ЛКМ** на архив конфигурации. В результате будет отображена карточка **«Конфигурация [номер]»** в виде интерфейсного маркерного представления (см. Рисунок – Просмотр конфигурации):

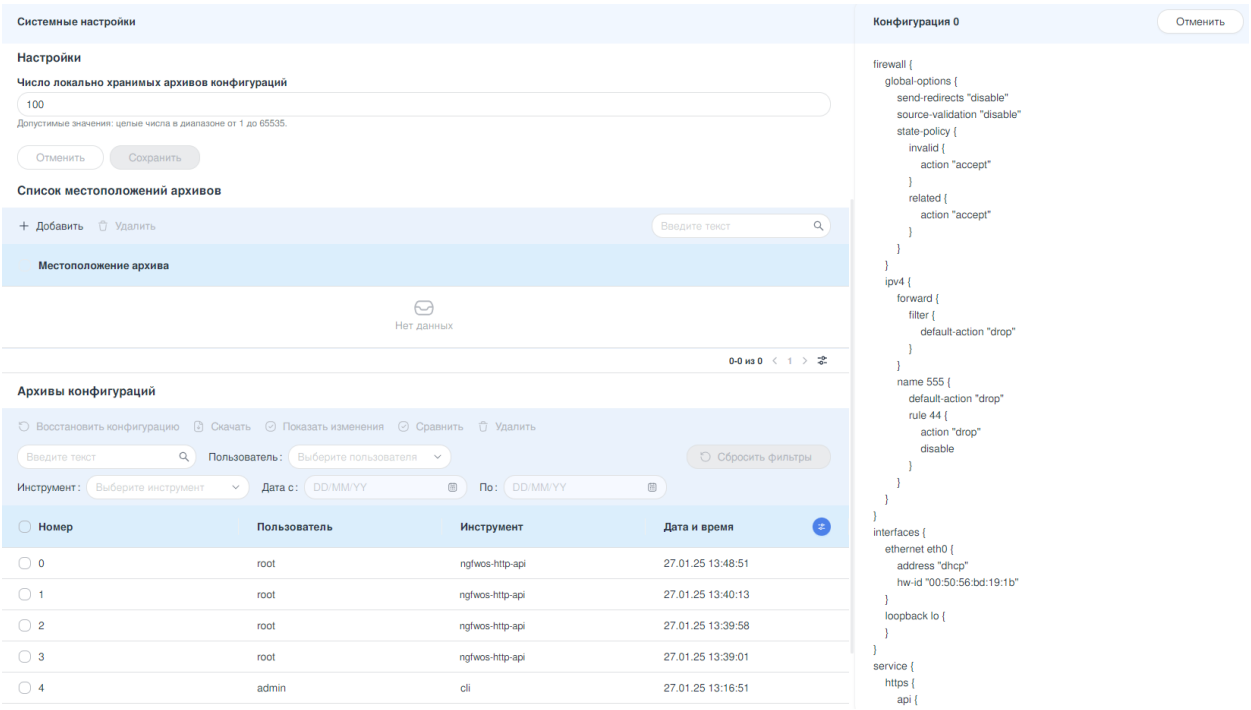


Рисунок – Просмотр конфигурации

Поиск и фильтрация

Блок фильтрации предоставляет возможность сортировки и фильтрации данных в таблице **«Архивы конфигураций»** по всем столбцам в списке (см. Рисунок – Панель поиск и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Пользователь»**;

- **«Инструмент»**;
- **«С»**;
- **«По»**;
- **кнопка «Сбросить фильтры»**.

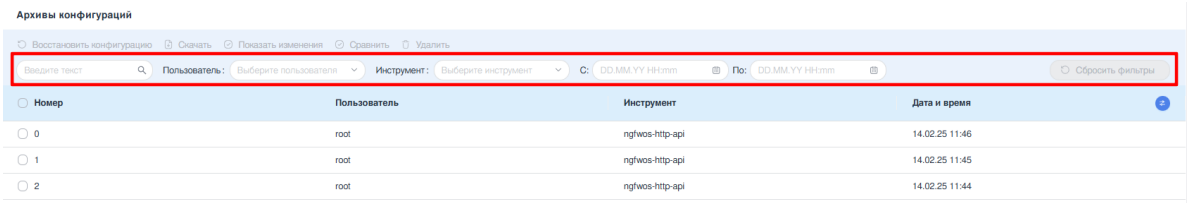


Рисунок – Панель поиск и фильтрации

Сквозной поиск по полям таблицы **«Архивы конфигураций»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам «Номер», «Пользователь» и «Инструмент».

Фильтрация по полю **«Пользователь»** позволяет осуществлять отбор данных на основе имени учётной записи пользователя, создавшего архив конфигурации.

Фильтрация по полю **«Инструмент»** позволяет отфильтровать архивы в зависимости от типа инструмента, который использовался для их создания.

Фильтрация по полю **«С»** позволяет отфильтровать архивы по дате создания и задаёт начальную дату диапазона. После ввода даты в таблице отобразятся лишь те действия, где «Дата» совпадает или больше введённой в фильтр.

Фильтрация по полю **«По»** позволяет отфильтровать архивы по дате создания и задаёт конечную дату диапазона. После ввода даты в таблице отобразятся лишь те действия, где «Дата» совпадает или меньше введённой в фильтр.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

4.4.3 Скачивание конфигурации

Для скачивания архивных файлов конфигурации необходимо выполнить следующие действия:

1. В таблице **«Архивы конфигураций»** следует выбрать одну или несколько архивных конфигураций, установив флажок в соответствующем чек-боксе слева от номера архива.
2. Нажать **кнопку «Скачать»** и в открывшемся окне указать имя архива, выбрать директорию сохранения архива и нажать **кнопку «Сохранить»** (см. Рисунок – Скачивание конфигурации).

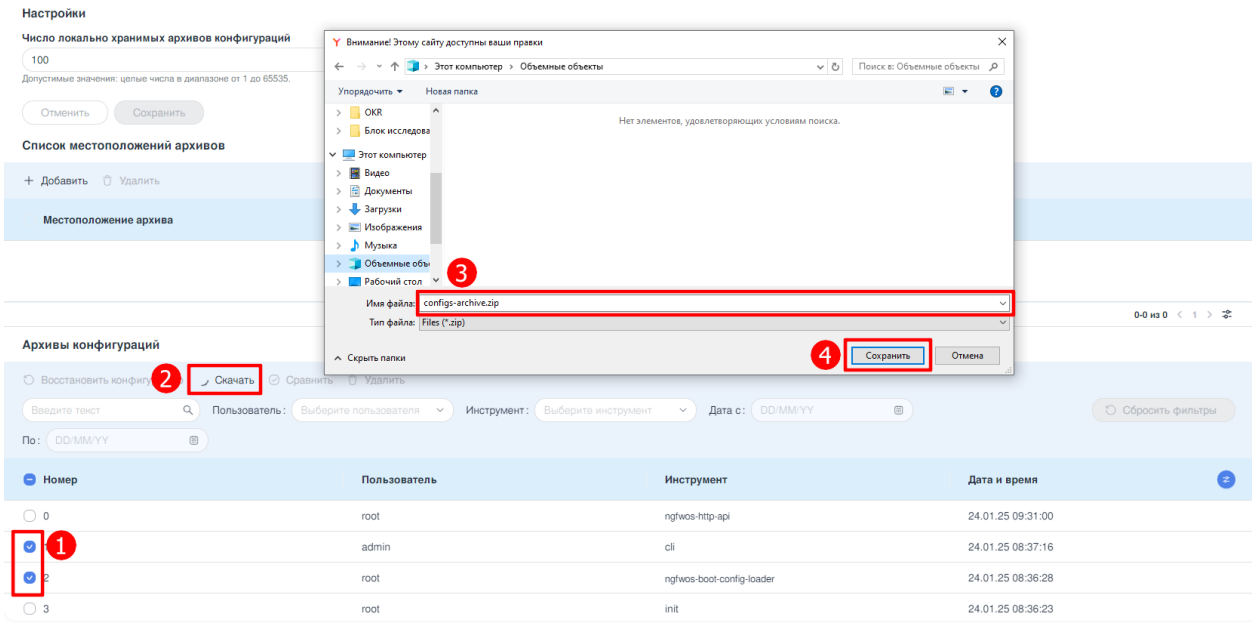


Рисунок – Скачивание конфигурации

4.4.4 Восстановление конфигурации

Для восстановления конфигурации к какой-либо версии активной конфигурации необходимо выполнить следующие действия:

1. В таблице **«Архивы конфигураций»** следует выбрать архивную конфигурацию, установив флажок в соответствующем чек-боксе слева от номера архива.
2. Нажать **кнопку «Восстановить конфигурацию»** и в открывшемся окне подтвердить восстановление нажатием **кнопки «Восстановить»** (см. Рисунок – Восстановление конфигурации).

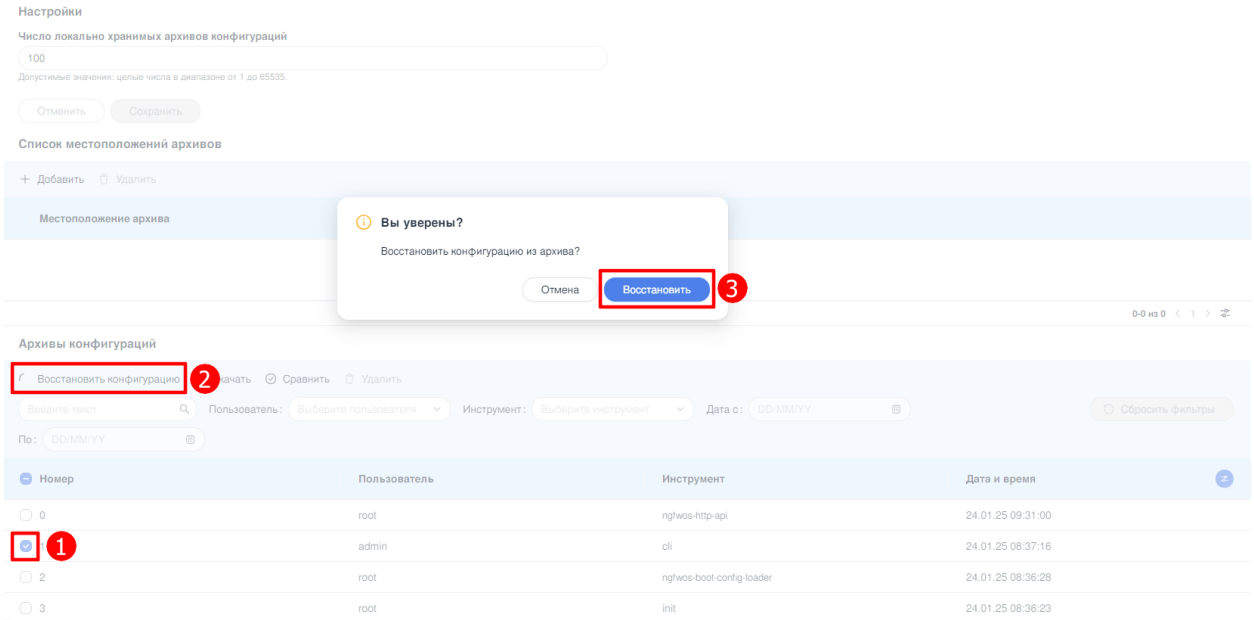


Рисунок – Восстановление конфигурации

3. По завершении процесса восстановления конфигурации в нижнем левом углу экрана будет отображено всплывающее окно с уведомлением об успешном восстановлении (см. Рисунок – Архив конфигурации восстановлен).

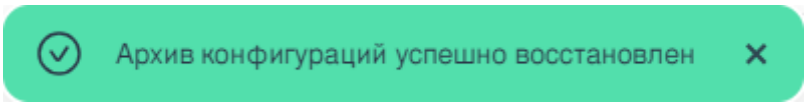


Рисунок – Архив конфигурации восстановлен

4.4.5 Сравнение архивных конфигураций

В системе **ARMA Стена** реализовано два механизма сравнение архивных конфигураций:

- **сравнение с предыдущим архивом**;
- **произвольное сравнение**.

Сравнение с предыдущим архивом

Данный механизм позволяет выполнить сравнение выбранной архивной конфигурации с предыдущим архивом по алгоритму **«<N> сравнить с <N+1>»**, где <N> — номер выбранного архива. Для этого необходимо выполнить следующие действия:

1. В таблице **«Архив конфигураций»** выбрать нужный архив, установив флажок в соответствующей строке слева от номера архива.
2. В панели инструментов таблицы нажать **кнопку «Показать изменения»**.
3. После активации кнопки откроется модальное окно **«Изменения конфигурации <N>»**, в котором будет отображён список параметров, отличающихся между выбранной конфигурацией <N> и предыдущей <N+1>. Добавленные параметры будут помечены символом **«+»**, удалённые — символом **«–»**.

Например, если выбрать архив конфигурации с номером «2» и нажать кнопку «Показать изменения» , система выполнит сравнение с предыдущей версией — архивом с номером «3» (N+1) — и выведет перечень изменений относительно архива «3». (см. Рисунок – Отображение изменений архивной конфигурации с номером «2»).

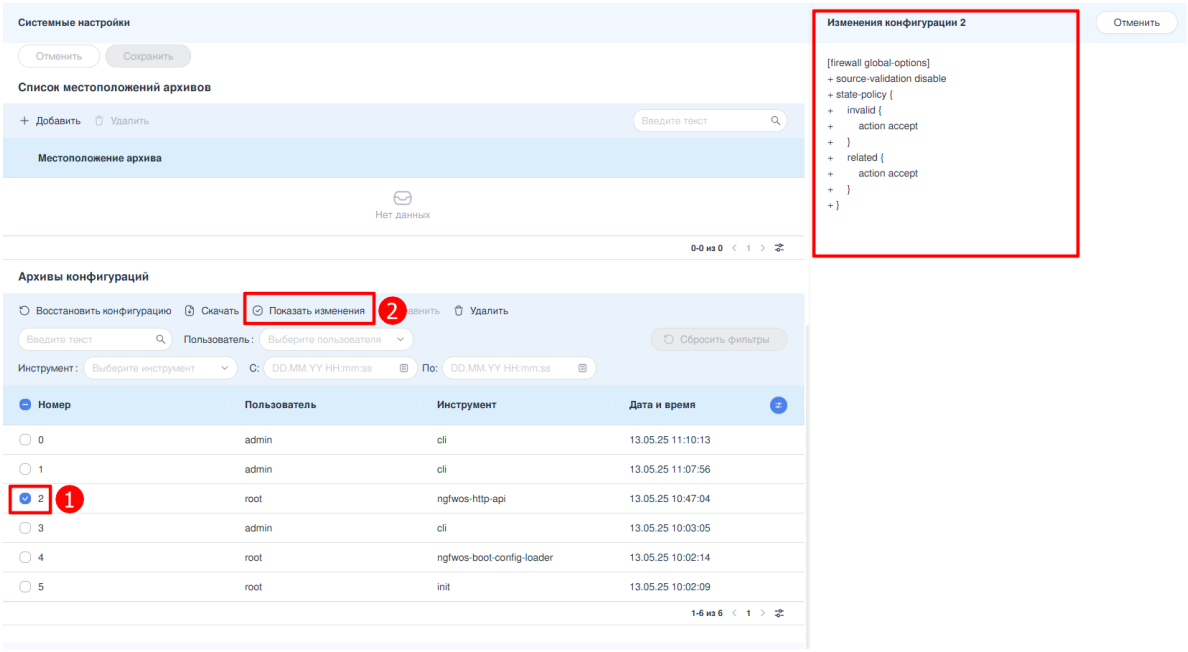


Рисунок – Отображение изменений архивной конфигурации с номером «2»

Произвольное сравнение

Данный механизм предназначен для сравнения конфигурационных настроек между двумя выбранными архивами. Для выполнения операции сравнения необходимо выполнить следующие действия:

1. В таблице **«Архив конфигураций»** выбрать два архива, установив флажки в соответствующих строках слева от номеров архивов.
2. В панели инструментов таблицы нажать **кнопку «Сравнить»**.
3. В открывшемся модальном окне **«Сравнение конфигураций <N> и <M>»** отображается список параметров, в которых зафиксированы различия между двумя выбранными конфигурациями. Параметры, добавленные в более новой конфигурации, помечаются символом **«+»**, а удалённые — символом **«–»**.

Сравнение выполняется таким образом, что отражает изменения относительно более старого из выбранных архивов по сравнению с более новым. Например, если для сравнения выбраны архивы с номерами «4» и «1», то будет показано, какие параметры были добавлены или удалены в конфигурации архива «1» по сравнению с архивом «4» (см. Рисунок – Сравнение архивов с номерами «4» и «1»).

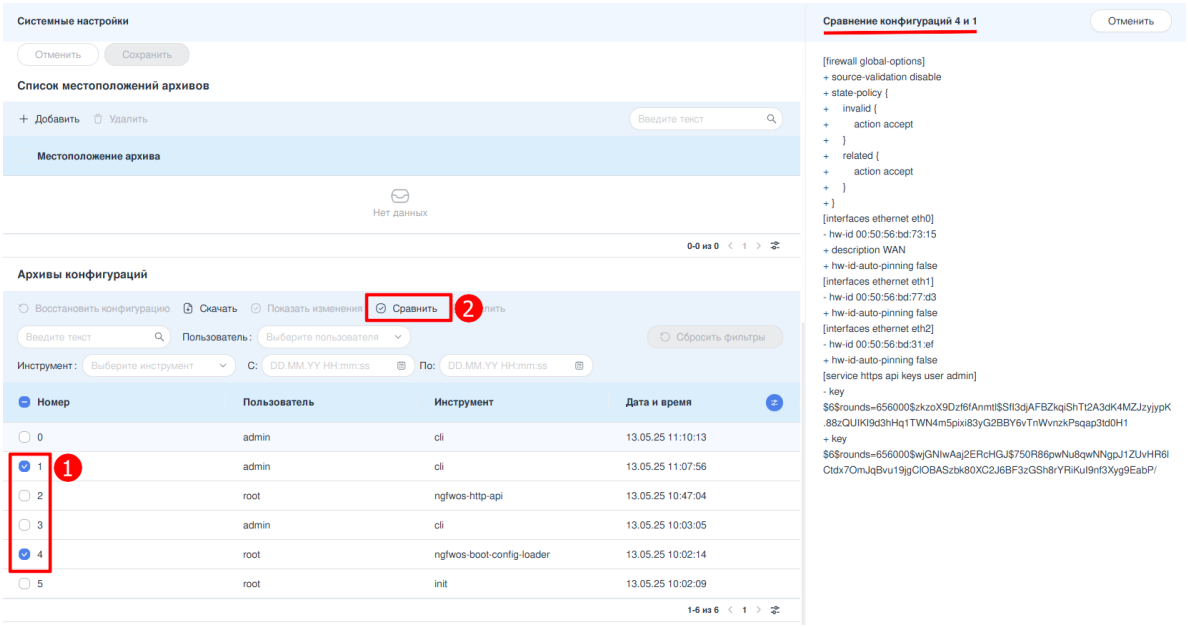


Рисунок – Сравнение архивов с номерами «4» и «1»

4.4.6 Удаление архивной конфигурации

Для удаления архивных конфигураций необходимо выполнить следующую последовательность действий:

1. В таблице **«Архивы конфигураций»** выбрать одну или несколько записей, установив флажок в соответствующем чек-боксе слева от номера архива.
2. Нажать **кнопку «Удалить»**, расположенную на панели инструментов таблицы **«Архивы конфигураций»**.
3. В открывшемся диалоговом окне подтвердить выполнение операции удаления, нажав на **кнопку «Удалить»**.

5 МАРШРУТИЗАЦИЯ

5.1 Отказоустойчивая маршрутизация

В системе **ARMA Стена** возможна настройка отказоустойчивой маршрутизации. Это технология, которая обеспечивает непрерывность работы сети при выходе из строя одного или нескольких маршрутизаторов. Непрерывность достигается за счёт резервирования маршрутов и автоматического переключения на резервные пути в случае сбоя, что минимизирует время простоя и поддерживает доступность сети.

Для перехода в подраздел **«Отказоустойчивая маршрутизация»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника «NGFW».
2. В карточке источника выбрать модуль **«Системные настройки»**.
3. В разделе **«Системные настройки»** перейти в подраздел **«Отказоустойчивая маршрутизация»** (см. Рисунок – подраздел «Отказоустойчивая маршрутизация»).

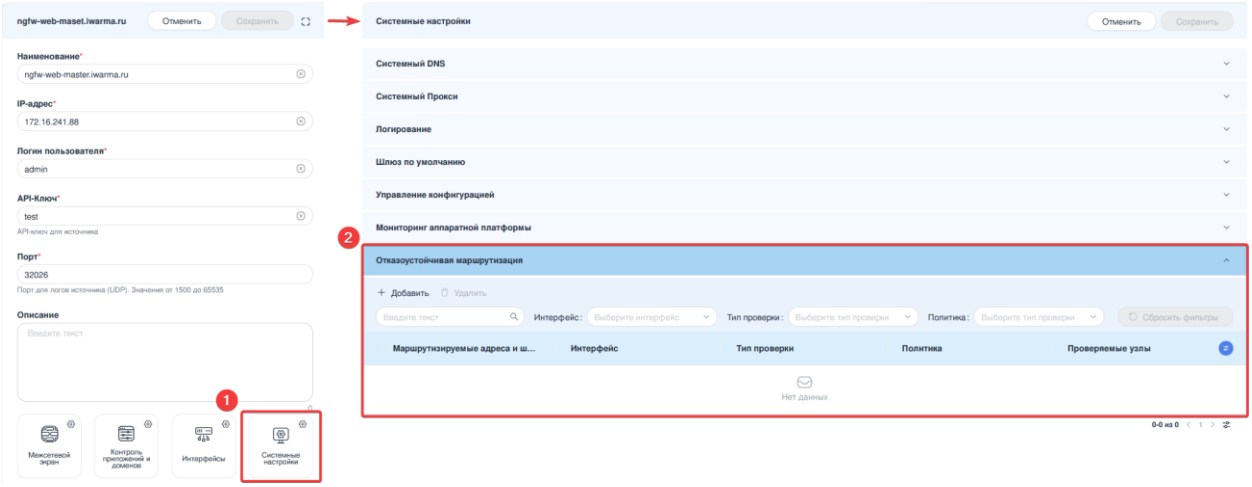


Рисунок – подраздел «Отказоустойчивая маршрутизация»

Применение и сохранение настроек маршрутизации

После завершения настройки всех необходимых параметров в подразделе **«Отказоустойчивая маршрутизация»** необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Системные настройки»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**, в котором отображается список подразделов, затронутых внесёнными изменениями. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

Только после успешного подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

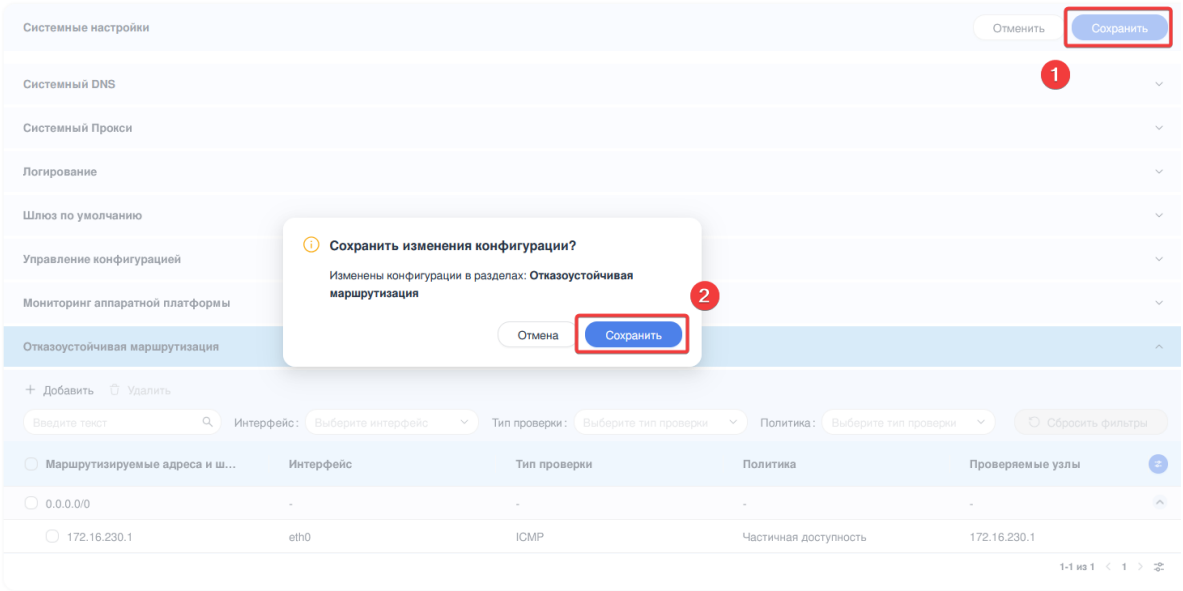


Рисунок – Применение и сохранение настроек

При необходимости отменить все неприменённые настройки следует нажать **кнопку «Отмена»**, расположенную в верхнем правом углу заголовка раздела **«Системные настройки»**. В этом случае конфигурация подраздела **«Отказоустойчивая маршрутизация»** будет откатана к последнему сохранённому состоянию.

5.1.1 Добавление маршрутов

Для добавления маршрута необходимо выполнить следующие действия (см. Рисунок - Добавление маршрута):

1. В таблице подраздела **«Отказоустойчивая маршрутизация»** нажать кнопку **«+Добавить»**.
2. В открывшейся боковой панели задать следующие настройки:
   - **«Маршрутизируемый адрес»** — указать адрес для маршрутизации. Допускается указание IPv4-адреса и маски сети в формате **x.x.x.x/y**, где **x** - положительное число в диапазоне от 0 до 255, **y** - положительное число в диапазоне от 1 до 32.
   - **«Шлюз»** - указать IP-адрес шлюза в формате IPv4.
   - **«Интерфейс»** — выбрать интерфейс из выпадающего списка.
   - Флаг **«Onlink»** — флаг для указания, что шлюз находится в прямой досягаемости.
   - **«Метрика»** — задать приоритет маршрута. Допускаются целые положительные числа в диапазоне от 1 до 255.

     Примечание:

     Если метрика шлюзов одинаковая, то маршрутизация будет выполняться в режиме балансировки. Если метрика шлюзов разная,

то маршрутизация будет выполняться в режиме резервирования - чем выше метрика, тем приоритетней маршрут.

- **«Тип проверки»** — выбрать тип проверки доступности узла.

  Возможно указать следующие типы:

  - arp;
  - icmp;
  - tcp.

- **«Политика»** — выбрать политику проверки доступности узлов.

  Возможно указать следующие политики:

  - Доступен каждый узел.
  - Доступен хотя бы один узел.

- **«Порт»** — указать порт узла. Обязательно для заполнения, если в поле **«Тип проверки»** выбрано значение **tcp**. Допускаются целые положительные числа в диапазоне от 1 до 65535.
- **«Частота проверки»** — задать частоту проверки доступности узлов в секундах. Допускаются целые положительные числа от 1 до 300.
- **«IPv4-адрес»** — указать адрес проверяемого узла. Возможно добавить несколько адресов, используя **кнопку «+Добавить»**.

3. Нажать **кнопку «Добавить»**. В левой нижней части окна отобразится уведомление об успешном добавлении маршрута (см. Рисунок - Добавление маршрута).

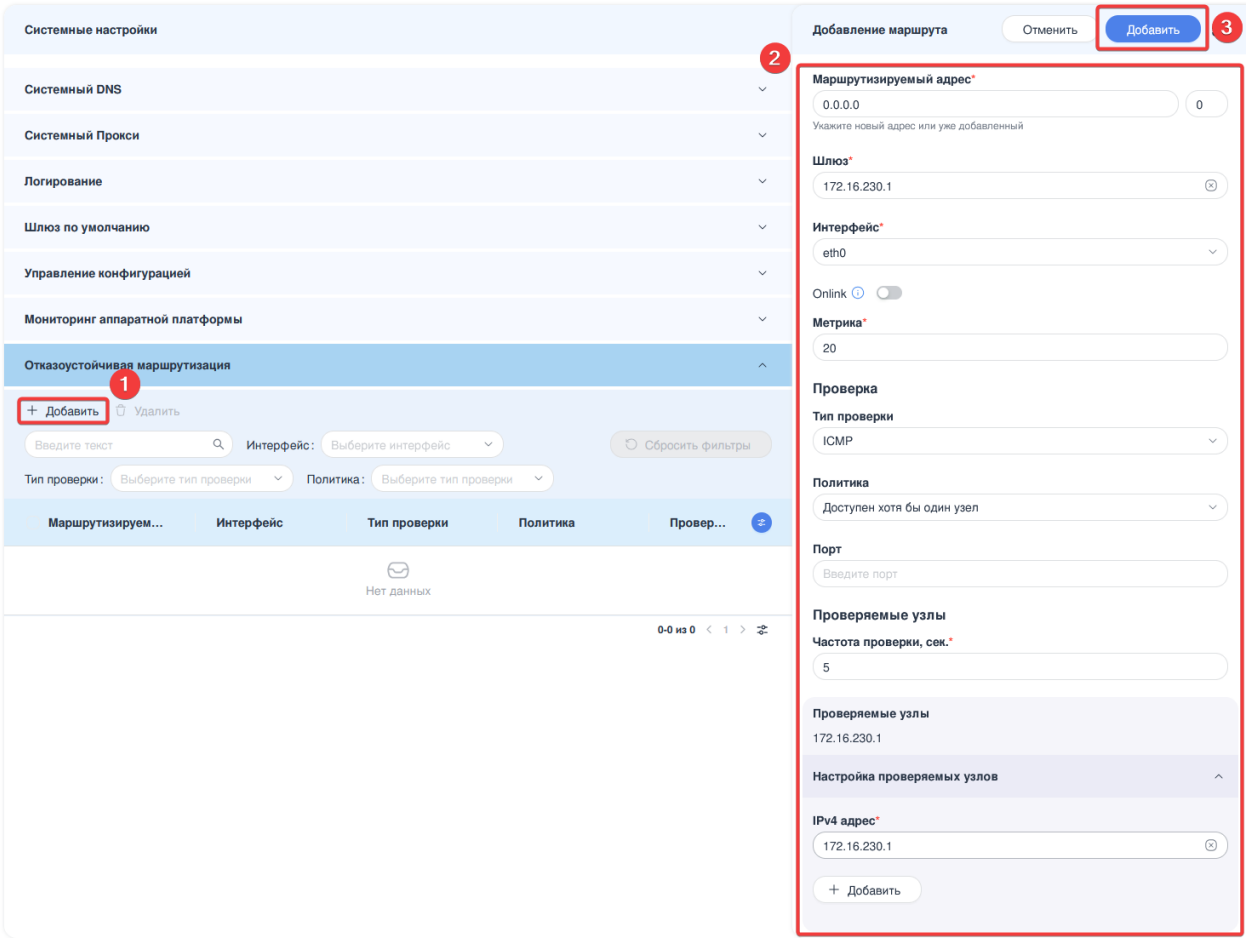


Рисунок – Добавление маршрута

5.1.2 Просмотр и редактирование маршрутов

Для просмотра и редактирования параметров маршрута необходимо нажать **ЛКМ** на строке маршрута в таблице. В результате откроется боковая панель «Редактирование маршрута» (см. Рисунок – Редактирование маршрута):

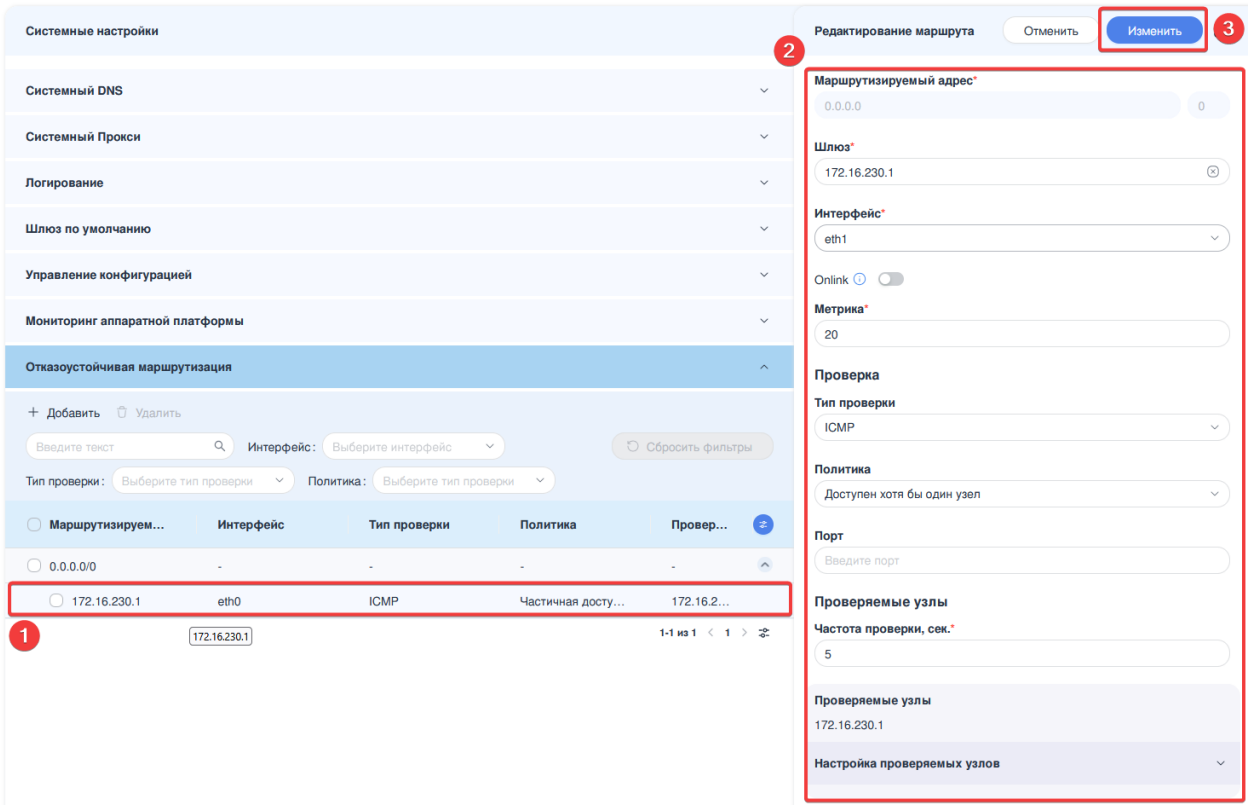


Рисунок – Редактирование маршрута

Для сохранения изменений после редактирования необходимо нажать **кнопку «Изменить»**.

5.1.3 Удаление маршрутов

Для удаления маршрутов и шлюзов необходимо выполнить следующую последовательность действий:

1. В таблице подраздела **«Отказоустойчивая маршрутизация»** выбрать одну или несколько записей, установив флажок в соответствующем чек-боксе слева от маршрута или шлюза.
2. Нажать **кнопку «Удалить»**, расположенную на панели инструментов таблицы.
3. В открывшемся диалоговом окне подтвердить выполнение операции удаления, нажав на **кнопку «Удалить»**.

> **Примечание:**
>
> Удаление последнего маршрутизируемого адреса шлюза также приведёт к удалению самого шлюза.

5.1.4 Поиск и фильтрация

Блок фильтрации предоставляет возможность сортировки и фильтрации данных в таблице подраздела **«Отказоустойчивая маршрутизация»** по всем столбцам

в списке (см. Рисунок – Панель поиска и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Интерфейс»**;
- **«Тип проверки»**;
- **«Политика»**;
- **кнопка «Сбросить фильтры»**.

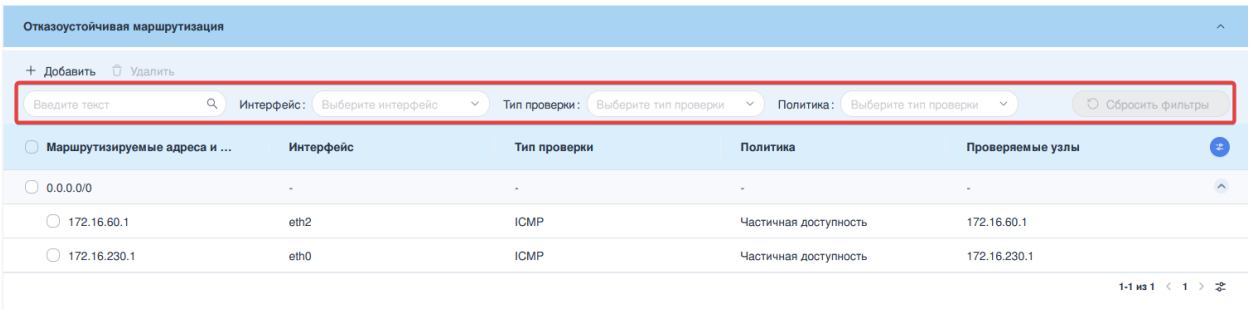


Рисунок – Панель поиска и фильтрации

Сквозной поиск по полям таблицы подраздела **«Отказоустойчивая маршрутизация»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцу «Маршрутизируемые адреса и шлюзы».

Фильтрация по полю **«Интерфейс»** позволяет отфильтровать маршруты в зависимости от выбранного сетевого интерфейса.

Фильтрация по полю **«Тип проверки»** позволяет выбрать данные на основании указанного типа проверки доступности узла.

Фильтрация по полю **«Политика»** позволяет отфильтровать маршруты в зависимости от выбранной политики проверки доступности узлов.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

6 МЕЖСЕТЕВОЙ ЭКРАН

Одной из основных функций **ARMA Стена** является фильтрация трафика с помощью встроенного межсетевого экрана. С помощью **МЭ** возможно установить правила для блокировки, отклонения или разрешения входящего, исходящего и локального трафика.

Для перехода в раздел «Межсетевой экран» необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«Межсетевой экран»** (см. Рисунок – Межсетевой экран):

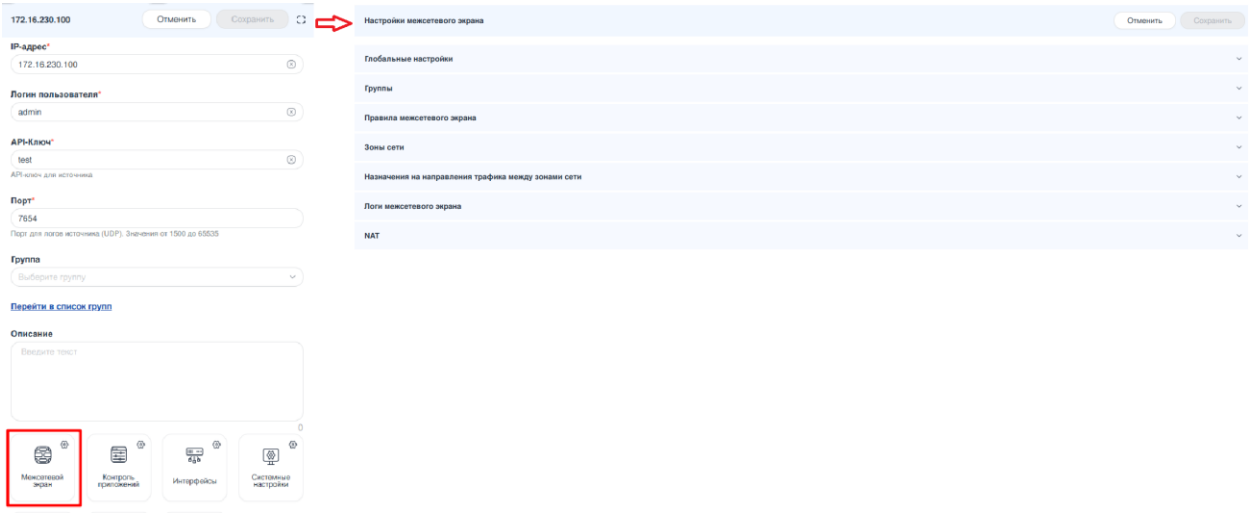


Рисунок – Межсетевой экран

В **МЭ** реализованы две политики фильтрации сетевого трафика:

1. **Стандартная политика на основе системных наборов правил.**

   Системные наборы правил представляют собой предопределённые пакеты правил, входящие в состав **МЭ**. В зависимости от направления и назначения сетевого трафика, применяются следующие системные наборы правил:

   - **«Input»** - набор правил для фильтрации входящего IPv4/IPv6-трафика, адресованного самой системе **ARMA Стена**.
   - **«Output»** - набор правил для фильтрации исходящего IPv4/IPv6-трафика, инициированного самой системой **ARMA Стена**, например, ответы на внешние запросы (SSH, ICMP и др.).
   - **«Forward»** - набор правил для фильтрации транзитного IPv4/IPv6-трафика, проходящего через устройство **ARMA Стена**.

2. **Политика на основе зон сети.**

   В рамках архитектуры, основанной на зонах безопасности, сетевые интерфейсы объединяются в логические группы — зоны, в соответствии с

их функциональным или сегментационным назначением. Правила фильтрации трафика между зонами определяются кастомными наборами правил, назначенными для каждой пары взаимодействующих зон. Такой подход обеспечивает гибкое и детализированное управление доступом, позволяя задавать различные уровни разрешений и политик безопасности для каждой конкретной зоны и межзонового взаимодействия.

Примечание:

Стандартная политика фильтрации трафика имеет приоритет над политикой на основе зон сети и применяется по умолчанию.

По умолчанию сетевой трафик сначала обрабатывается на уровне системных наборов правил. Для использования исключительно политики на основе зон необходимо разрешить весь трафик на уровне системных наборов правил. Это осуществляется путём установки параметра **«Действие по умолчанию»** в значение **«Разрешить (accept)»** и удаления (или отключения) всех правил в каждом из системных наборов **Input, Output** и **Forward**.

При конфигурации **МЭ** требуется обеспечить доступность определённого набора сетевых портов, необходимых для стабильного функционирования системных сервисов и взаимодействия с другими компонентами инфраструктуры. Перечень используемых портов приведён в таблице «Служебные порты системы ARMA Стена».

*Таблица «Служебные порты системы **ARMA Стена**»*

Порт	Протокол	Описание
22	TCP	Порт для удалённого доступа к системе по протоколу SSH
123	UDP	Порт службы синхронизации времени NTP
443	TCP	Порт, используемый для онлайн-активации системы и получения обновлений правил СОВ
3128	TCP	Порт прокси-сервера для обработки HTTP-запросов
3129	TCP	Порт прокси-сервера для обработки HTTPS-запросов

Порт	Протокол	Описание
5000	TCP	Порт взаимодействия системы **ARMA Стена** с **ARMA MC**
8082	TCP	Порт, предназначенный для синхронизации конфигураций и служебного взаимодействия с **ARMA MC**

Примечание:

Рекомендуется применять строгую политику фильтрации сетевого трафика на уровне межсетевого экрана, предполагающую по умолчанию запрет всего входящего, исходящего и транзитного трафика. Доступ должен быть разрешён только на основании принципа минимальных привилегий.

6.1 Глобальные настройки

Некоторые настройки **МЭ** являются глобальными и влияют на всю систему. Для настройки глобальных параметров необходимо перейти в подраздел **«Настройки межсетевого экрана» - «Глобальные настройки»** (см. Рисунок – Глобальные настройки).

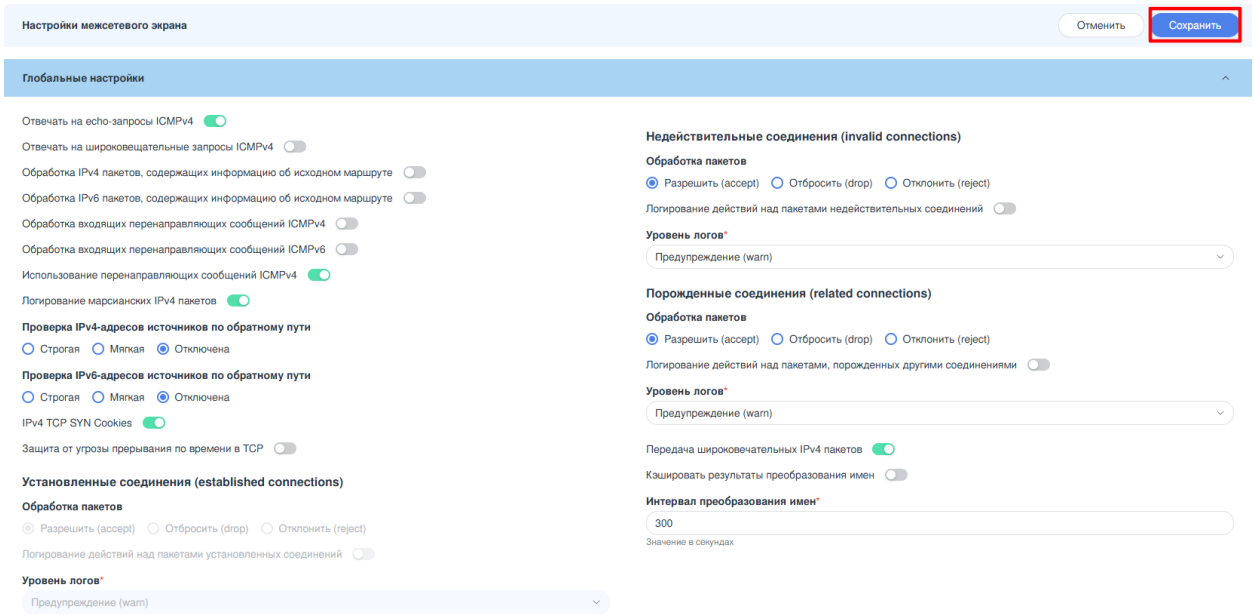


Рисунок – Глобальные настройки

Список глобальных настроек **МЭ**:

- **Отвечать на echo-запросы ICMPv4** - разрешить или запретить приём ICMP-запросов (ping) на входящие соединения на устройстве **ARMA Стена**. По умолчанию устройство отвечает на все виды ICMP-запросов.
- **Отвечать на широковещательные запросы ICMPv4** - разрешить или запретить ответы на широковещательные ICMP сообщения. По умолчанию ответы на широковещательные ICMP сообщения запрещены.
- **Обработка IPv4 пакетов, содержащих информацию об исходном маршруте** - принимать или игнорировать IPv4-пакеты, в которых заданы параметры маршрутизации источника (например, LSRR — Loose Source and Record Route или SSRR — Strict Source and Record Route). Эти параметры позволяют отправителю указать конкретный маршрут, по которому должны проходить пакеты через сеть. Это может быть использовано в контексте атак типа «man-in-the-middle», когда злоумышленник пытается перехватить трафик, перенаправляя его через свой узел. По умолчанию такие пакеты игнорируются.
- **Обработка IPv6 пакетов, содержащих информацию об исходном маршруте** - принимать или игнорировать IPv6-пакеты, в которых заданы параметры маршрутизации источника. По умолчанию такие пакеты игнорируются.
- **Обработка входящих перенаправляющих сообщений ICMPv4** - разрешить или запретить возможность приёма сообщений ICMPv4 Redirect. ICMPv4 Redirect представляет собой протокол сетевого уровня, используемый для передачи информации о более эффективных маршрутах к целевым узлам. Маршрутизатор может отправить такое сообщение хосту, чтобы указать на более оптимальный путь для достижения конечной точки. Эта функция может быть полезна для оптимизации маршрутизации в некоторых сетевых конфигурациях. Однако, с точки зрения информационной безопасности, ICMP Redirect-сообщения могут представлять угрозу, так как они могут быть использованы злоумышленниками для модификации таблицы маршрутизации клиента. По умолчанию приём ICMPv4 Redirect-сообщений отключён.
- **Обработка входящих перенаправляющих сообщений ICMPv6** - разрешить или запретить возможность приёма сообщений ICMPv6 Redirect. По умолчанию приём ICMPv6 Redirect-сообщений отключён.
- **Использование перенаправляющих сообщений ICMPv4** - разрешить или запретить возможность отправки ICMP Redirect-сообщений через IPv4. По умолчанию устройство отправляет ICMP Redirect-сообщения другим хостам, если обнаружит более оптимальный путь.

- **Логирование марсианских IPv4 пакетов** - включить или отключить регистрацию пакетов с некорректными или подозрительными IP-адресами источника или назначения, известных как «марсианские» пакеты (martian packets). По умолчанию логирование включено.
- **Проверка IPv4-адресов источников по обратному пути** - включить или отключить проверку источников по обратному пути. Возможно указать следующие варианты проверок:
    - **Строгая** - осуществляется проверку того, что маршрут до исходного IPv4-адреса проходит через тот же сетевой интерфейс, с которого был получен пакет;
    - **Мягкая** - проверяется наличие маршрута до исходного IPv4-адреса, независимо от его соответствия интерфейсу, через который поступил пакет;
    - **Отключена** - Проверка отключена. Используется по умолчанию.
- **Проверка IPv6-адресов источников по обратному пути** - включить или отключить проверку источников по обратному пути. Возможно указать следующие варианты проверок:
    - **Строгая** - осуществляется проверку того, что маршрут до исходного IPv6-адреса проходит через тот же сетевой интерфейс, с которого был получен пакет;
    - **Мягкая** - проверяется наличие маршрута до исходного IPv6-адреса, независимо от его соответствия интерфейсу, через который поступил пакет;
    - **Отключена** - Проверка отключена. Используется по умолчанию.
- **IPv4 TCP SYN Cookies** - включить или отключить механизм SYN-cookies в **МЭ**. Механизм SYN-cookies представляет собой метод защиты от атак типа «SYN flood», при которых злоумышленник отправляет значительное количество SYN-пакетов с целью исчерпания ресурсов сервера. По умолчанию данный механизм активирован.
- **Защита от угрозы прерывания по времени в TCP** - включить или отключить защиту от угроз, связанных с Time-Wait Assault (TWA). По умолчанию отключено.
-

  Установленные соединения (established connections) - блок настройки политики обработки уже установленных соединений в МЭ:
    - **Обработка пакетов** - определяет, как система должна обрабатывать входящий трафик, который является частью уже

установленного и разрешённого TCP/IP-соединения. Возможно выбрать следующие значения:

- **Разрешить (accept)** - принимать весь трафик, относящийся к установленным соединениям. Используется по умолчанию.
- **Отбросить (drop)** - отбрасывать установленные соединения без отправки какого-либо ответа.
- **Отклонить (reject)** - отбрасывать трафик с отправкой ICMP или TCP RST сообщения.

Примечание:

При выборе значения «Отбросить (drop)» или «Отклонить (reject)» управление данным устройством станет недоступным.

- **Логирование действий над пакетами установленных соединений** - определяет, будут ли записываться в журнал событий все пакеты, принадлежащие уже существующим, установленным соединениям. По умолчанию логирование отключено.
- **Уровень логов** - настроить уровень детализации логирования установленных соединений в **МЭ**. Возможно выбрать следующие значения:
  - **Аварийный (emerg)**;
  - **Тревожный (alert)**;
  - **Критический (crit)**;
  - **Ошибка (err)**;
  - **Предупреждение (warn)** - используется по умолчанию;
  - **Уведомление (notice)**;
  - **Информация (info)**;
  - **Отладка (debug)**.

Примечание:

Блок **«Установленные соединения (established connections)»** доступен только для просмотра и не поддерживает редактирование через графический интерфейс. Настройка параметров данного блока возможна исключительно с использованием командной строки (**CLI**).

- **Недействительные соединения (invalid connections)** - блок настройки обработки недопустимых (invalid) сетевых пакетов в **МЭ**. Конфигурация этого раздела аналогична параметрам, применяемым к политике обработки уже установленных соединений.
- **Порождённые соединения (related connections)** - блок настройки обработки связанных (related) сетевых соединений в **МЭ**. Конфигурация этого раздела аналогична параметрам, применяемым к политике обработки уже установленных соединений.
- **Передача широковещательных IPv4 пакетов** - включить или отключить обработку направленных широковещательных пакетов (directed broadcast) в **МЭ**. По умолчанию обработка широковещательных пакетов включена.
- **Кэшировать результаты преобразования имён** - включить или отключить кэширование результатов преобразования DNS-имён, используемых при работе с правилами **МЭ**, содержащими доменные имена. По умолчанию кэширование отключено.
- **Интервал преобразования имён** - установить значения интервала в секундах для обновления разрешения DNS-имён. Возможно указание значения в диапазоне от «10» до «3600». При использовании FQDN в группах «Домены» или правилах **МЭ** функция разрешения доменных имён будет выполняться с указанной периодичностью для актуализации связанных IP-адресов, при этом результаты могут кэшироваться, если включена глобальная опция «Кэшировать результаты преобразования имен».

Для сохранения внесённых изменений в глобальные настройки **МЭ** необходимо нажать **кнопку «Сохранить»** (см. Рисунок – Глобальные настройки).

6.2 Группы

Группы представляют собой удобный инструмент для объединения множества сетей, хостов и портов с целью их дальнейшего использования в правилах межсетевого экрана (МЭ) и других настройках **ARMA Стена**. Применение групп позволяет улучшить читаемость правил **МЭ**, а также ускорить процесс добавления новых или изменения существующих правил.

Для просмотра списка назначенных групп необходимо выполнить следующие действия:

1. открыть карточку соответствующего источника «NGFW»;
2. выбрать модуль **«Межсетевой экран»**;
3. перейти в меню **«Настройки межсетевого экрана»**;
4. открыть раздел **«Группы»**.

6.2.1 Добавление группы

Для добавления группы необходимо выполнить следующие действия:

1. Перейти в раздел управления группами и нажать **кнопку «+ Добавить»**.
2. В открывшейся боковой панели указать необходимые параметры (см. Рисунок – Добавление группы):
   - **«Наименование»** - должно быть уникальным в рамках своего типа, не превышать «31» символа, начинаться только с латинской буквы или цифры, не может начинаться с символов «-» или «!», и не должно содержать символы «|», «;», «:», «&», «$», «<», «>»;
   - **«Тип»** - тип группы. Возможно выбрать из списка: **«IPv4 адреса», «IPv4 сети», «IPv6 адреса», «IPv6 сети», «Порты», «Домены», «MAC-адреса», «Интерфейсы», «Динамические группы»**. В зависимости от выбранного типа в окне откроются дополнительные поля для ввода параметров;

     Примечание:

     Настройка наполнения элементами в динамической группе осуществляется через правила **МЭ**.

   - **Группы <тип_группы>** - позволяет выбрать одну или несколько существующих групп аналогичного типа из выпадающего списка. Данная функция позволяет вложить одну группу в другую для удобной организации правил фильтрации трафика. Параметр не доступен для типов групп «Домены» и «Динамические группы».
   - **«Описание»** - максимально допустимая длина значения поля «127» символов.
3. По завершению нажать **кнопку «Сохранить»**.

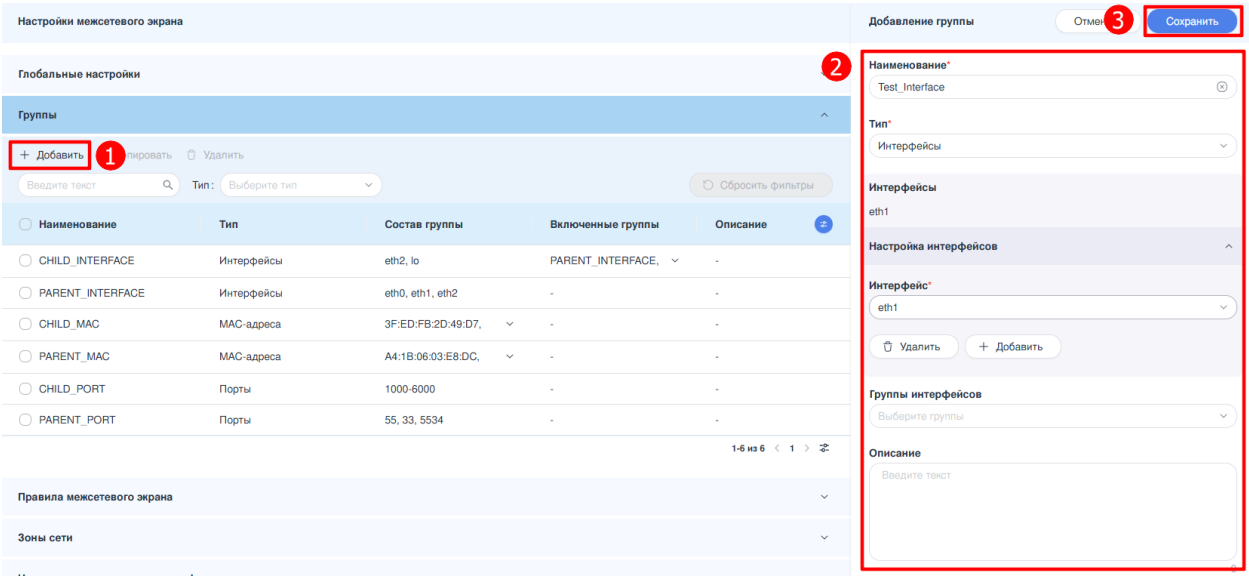


Рисунок – Добавление группы

6.2.2 Редактирование группы

Для внесения изменений в псевдоним необходимо выполнить следующие действия:

1. Нажать **ЛКМ** на строке нужной группы.
2. В открывшейся боковой панели внести допустимые корректировки.
3. По завершению редактирования, нажать **кнопку «Сохранить»**.

6.2.3 Копирование группы

Для копирования группы необходимо выполнить следующие действия:

1. Выбрать одну группу, установив флажок в чек-боксе слева от наименования группы, и нажать **кнопку «Копировать»**.
2. В открывшейся боковой панели **«Копирование группы»** ввести новое наименование группы. Значение поля **«Тип»** наследуется от копируемого группы и недоступно для изменений.
3. Нажать **кнопку «Копировать»** (см. Рисунок – Копирование группы).

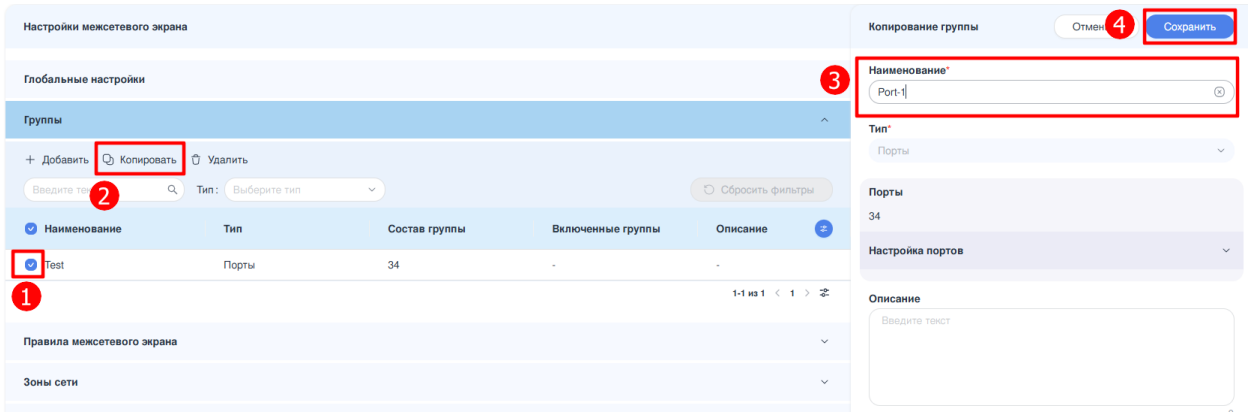


Рисунок – Копирование группы

6.2.4 Удаление группы

Для удаления группы необходимо выполнить следующие действия:

1. Выбрать одну или несколько групп установив флажок в чек-боксе слева от наименования группы и нажать **кнопку «Удалить»**.
2. В открывшемся окне подтвердить удаление нажатием **кнопки «Удалить»** (см. Рисунок – Подтверждение удаление группы).

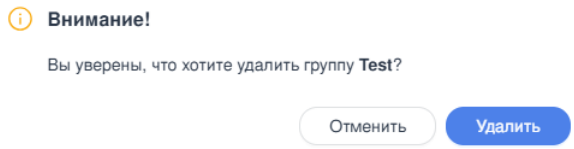


Рисунок – Подтверждение удаление группы

Примечание:

При попытке удаления группы, используемой в правилах NAT или **МЭ**, отобразится предупреждение о невозможности её удаления (см. Рисунок – Удаление группы невозможно).

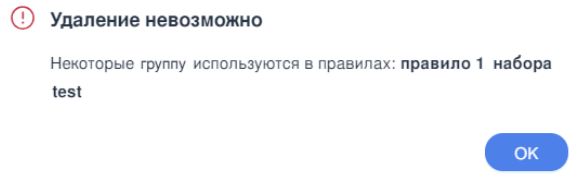


Рисунок – Удаление группы невозможно

6.3 Стандартная политика на основе системных наборов правил

6.3.1 Набор правил

Набор правил - это именованный пакет правил **МЭ**.

В зависимости от принадлежности трафика существуют следующие наборы правил:

1. **«Input»** - набор правил для фильтрации IPv4 и IPv6 трафика, предназначенного для самой **ARMA Стена**, и используется для её защиты.
2. **«Output»** - набор правил для фильтрации IPv4 и IPv6 трафика, исходящего от самой **ARMA Стена**. Например, ответ на попытку входа по SSH в **ARMA Стену**.
3. **«Forward»** - набор правил для фильтрации IPv4, IPv6 и сетевого моста (Bridge) трафика, проходящего транзитом через **ARMA Стена**.
4. **«Name»** - кастомный набор правил. Используется во всех вариантах работы **МЭ**, включая системные наборы **«Input»**, **«Output»** и **«Forward»**, реализуемый через действия правила **«Перейти (jump)»**.

ARMA Стена по умолчанию содержит семь системных наборов правил: три набора **«Input»**, **«Output»** и **«Forward»** для фильтрации IPv4 трафика, три набора **«Input»**, **«Output»** и **«Forward»** для фильтрации IPv6 трафика и один набор **«Forward»** для сетевого моста.

Набор правил содержит действие по умолчанию, которое применяется к сетевому пакету, если ни одно из правил в наборе не сработало.

Для системных наборов правил **«Input»**, **«Output»** и **«Forward»** возможно установить следующие значения действия по умолчанию:

- **«Разрешить (accept)»** - значение по умолчанию;
- **«Отбросить (drop)»**.

Для кастомных наборов правил возможно установить следующие значения действия по умолчанию:

- **«Отбросить (drop)»** - значение по умолчанию;
- **«Перейти (jump)»**;
- **«Отклонить (reject)»**;
- **«Вернуться (return)»**;
- **«Разрешить (accept)»**;
- **«Продолжить (continue)»**.

6.3.1.1 Добавление кастомного набора правил

Для добавления кастомного набора правил необходимо выполнить следующие действия:

1. Перейти в раздел **«Правила межсетевого экрана»** меню **«Настройки межсетевого экрана»** и нажать **кнопку «+Добавить»**.
2. В открывшейся боковой панели выбрать создаваемую сущность **«Набор»** (см. Рисунок – Добавление набора правил).

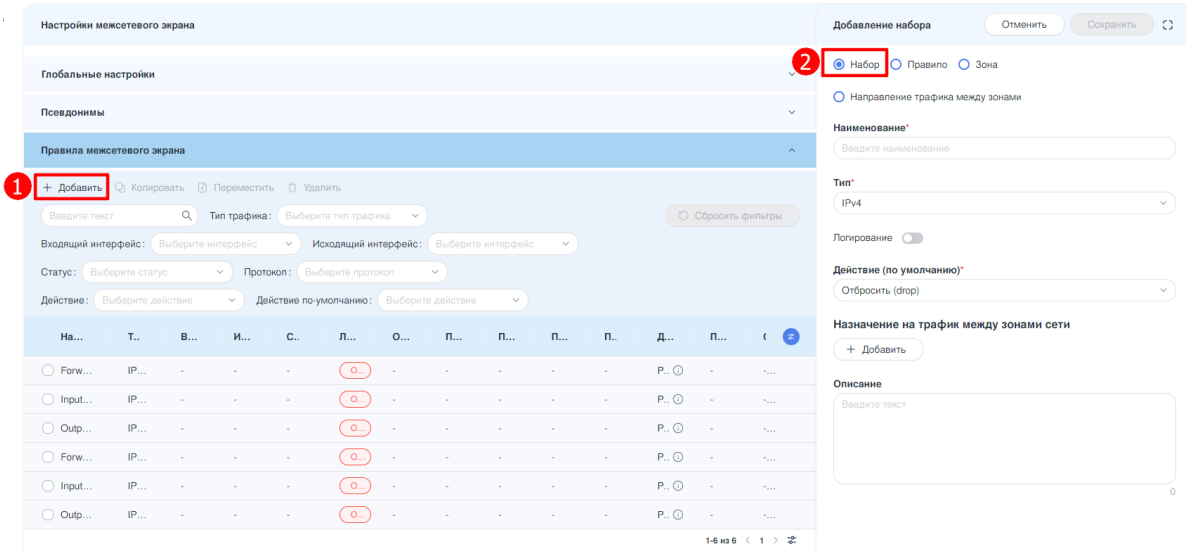


Рисунок – Добавление набора правил

3. Внести/скорректировать значения в полях:

   - **«Наименование»** - максимально допустимая длина значения «28» символов. Допускается использование только латинских букв (A–Z, a–z), цифр (0–9) и специальных символов: подчёркивание («_») и точка («.»). Значение должно начинаться с латинской буквы или цифры;
   - **«Тип»** - выбор типа трафика **«IPv4»**, **«IPv6»** или **«Сетевой мост»**. При дальнейшем редактировании или копировании значение поля не подлежит изменению;
   - **«Логирование»** - включение/отключение журналирования;
   - **«Действие по умолчанию»** - действие применится в случае, если ни одно из установленных правил в наборе не было применено.

     Примечание:

     При использовании действия **«Перейти (jump)»** не допускается создание бесконечных циклов, когда набор перенаправляет сам на себя или через несколько переходов возвращается к себе.

4. Для назначения кастомного набора правил типа **«IPv4»** или **«IPv6»** на трафик между зонами сети необходимо нажать **кнопку «+Добавить»** в блоке **«Назначение на трафик между зонами сети»** и заполнить необходимые поля (см. Рисунок – Назначение на трафик между зонами сети):

   - **«Зона отправителя»** - выбор из списка зоны отправителя;
   - **«Интерфейсы зоны отправителя»** - поле отображает интерфейсы, входящие в выбранную зону отправителя. Поле заблокировано для редактирования;
   - **«Зона получателя»** - выбор из списка зоны получателя;

- **«Интерфейсы зоны отправителя»** - поле отображает интерфейсы, входящие в выбранную зону получателя. Поле заблокировано для редактирования.

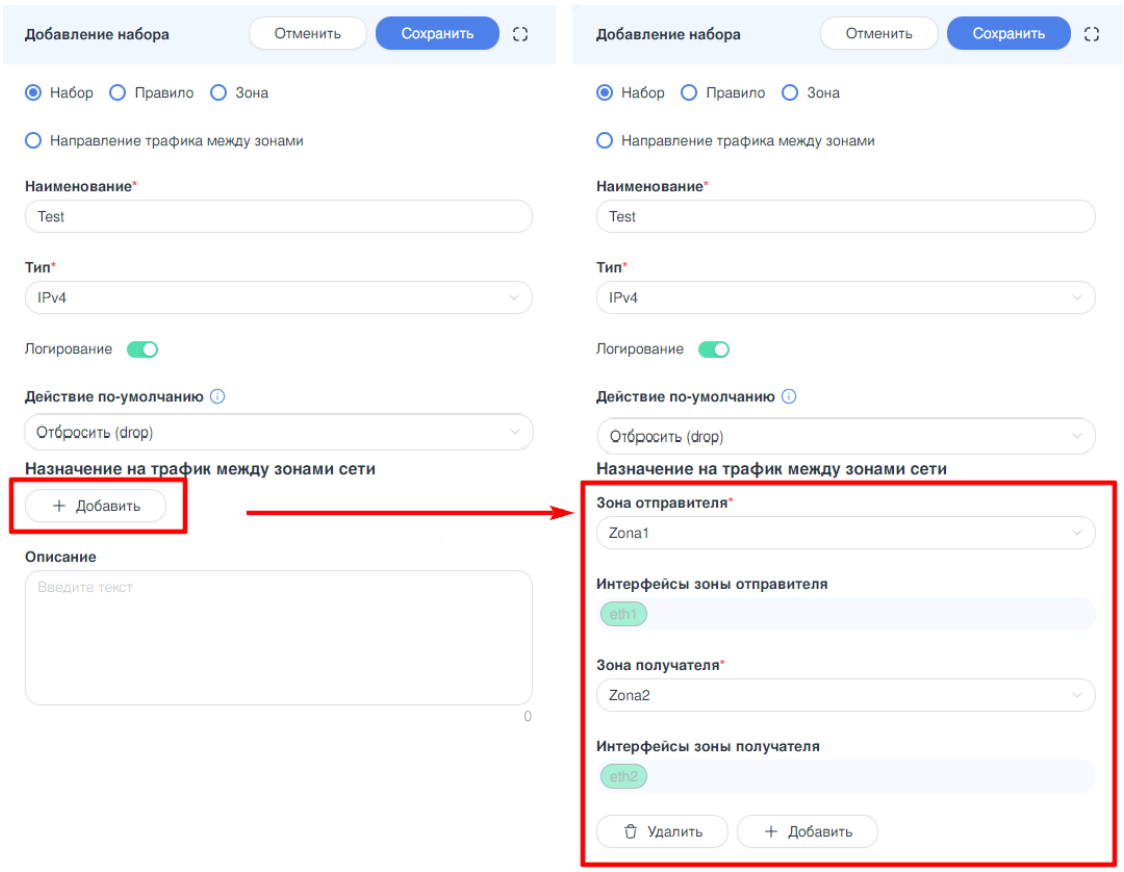


Рисунок – Назначение на трафик между зонами сети

5. По завершению нажать **кнопку «Сохранить»**.

6.3.1.2 Редактирование набора правил

Для редактирования набора правил необходимо нажать **ЛКМ** на строку с нужным набором и в открывшейся боковой панели внести корректировки. По завершению нажать **кнопку «Сохранить»**.

6.3.1.3 Копирование кастомных наборов правил

Для копирования кастомных наборов правил необходимо выполнить следующие действия:

1. Выбрать один или несколько кастомных наборов правил, установив флажок в чек-боксе слева от наименования набора, и нажать **кнопку «Копировать»**.
2. В открывшейся боковой панели **«Копирование набора»** предусмотрена возможность изменения имени нового набора. По умолчанию имя копии формируется на основе имени исходного набора с добавлением суффикса «_copy». Параметр «Тип» автоматически наследуется от оригинального набора и не подлежит редактированию.

3. Нажать **кнопку «Копировать»** (см. Рисунок – Копирование набора правил).

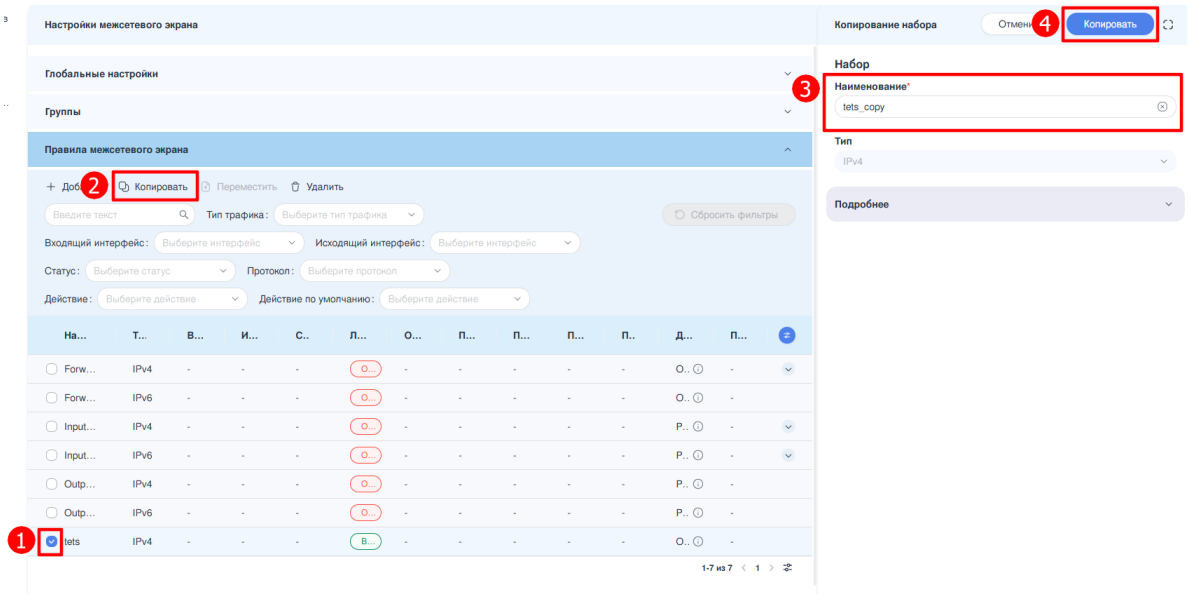


Рисунок – Копирование набора правил

6.3.1.4 Удаление набора правил

Для удаления наборов правил необходимо:

1. Выбрать один или несколько наборов правил, установив флажок в чек-боксе слева от наименования набора правил, и нажать **кнопку «Удалить»**.
2. Подтвердить удаление набора правил нажатием **кнопки «Удалить»** в открывшемся окне (см. Рисунок – Подтверждение удаление набора).

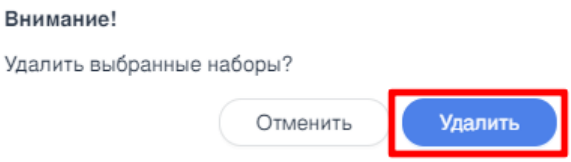


Рисунок – Подтверждение удаление набора

Примечание:

При удалении системного набора правил удаляются только правила, входящие в состав этого набора; сам набор из списка не удаляется.

Примечание:

Если удаляемый кастомный набор правил назначен на направление трафика между зонами сети или используется в других наборах и правилах для переадресации на них, то появится предупреждающее окно с запретом на удаление (см. Рисунок – Удаление невозможно).

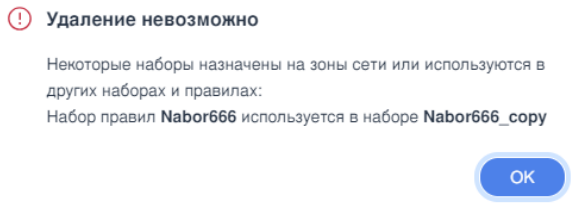


Рисунок – Удаление невозможно

6.3.2 Правила МЭ

Фильтрация трафика происходит с помощью правил **МЭ**. Каждое правило пронумеровано, имеет действие, которое следует применить, если правило соответствует, и критерии соответствия. Пакеты данных проходят по правилам от «1» до «999999», при первом совпадении будет выполнено действие правила, далее обработка пакета не производится.

Правилами **МЭ** предусмотрены следующие действия над сетевыми пакетами:

- **«Отбросить (drop)»** - отбросить пакет.
- **«Перейти (jump)»** - перейти к кастомному набору правил.
- **«Вернуться (return)»** - вернуться из кастомного набора правил и перейти к следующему правилу.
- **«Отклонить (reject)»** - отклонить пакет.
- **«Разрешить (accept)»** - разрешить пакет.
- **«Продолжить (continue)»** - продолжить проверку следующего правила.
- **«В очередь (queue)»** - отправляет пакет в пользовательское пространство для дальнейшей обработки.

  Данный оператор отправляет пакет в пространство пользователя с использованием функции nfnetlink_queue. Пакет помещается в очередь, идентифицируемую по 16-разрядному номеру. Пользовательское пространство может при необходимости просмотреть и изменить пакет. Затем пользовательское пространство должно удалить пакет или повторно отправить его в ядро. Также предусмотрена возможность активации опции обхода, которая позволит не выполнять операцию записи пакета в пользовательское пространство, если в очереди нет приложений, ожидающих обработки пакета. В таком случае правило будет действовать аналогично действию «Разрешить (accept)», если не обнаружено приложений, ожидающих пакет.

- **«Разгрузить (offload)»** - определяет, какие потоки добавляются в таблицу потоков.

  Таблицы потоков позволяют ускорить передачу пакетов в программном обеспечении (и в аппаратном обеспечении, если

сетевой адаптер поддерживает эту функцию) за счёт обхода сетевого стека на основе conntrack. Записи представляются в виде кортежа, состоящего из входного интерфейса, адреса источника и назначения, порта источника и назначения, а также протоколов уровня 3/4. Каждая запись также кэширует информацию об интерфейсе назначения и адресе шлюза (для обновления адреса назначения на канальном уровне) с целью пересылки пакетов. Поля TTL и hoplimit также декрементируются. Таким образом, таблицы потоков обеспечивают альтернативный путь, позволяющий пакетам обойти классический путь пересылки. После установления состояния потоки разгружаются. Это означает, что первый ответный пакет обычно создаёт запись в таблице потоков. Для приёма исходного трафика требуется правило межсетевого экрана. Выражение потока в прямой цепочке должно соответствовать обратному трафику из исходного соединения. Следует иметь в виду, что обратный маршрут определяется на основе пакета, который создаёт запись в таблице потоков. Если используются определённые правила IP, необходимо убедиться, что они соответствуют как трафику ответного пакета, так и исходному трафику.

- **«Synproxy»** - соединения synproxy.

  Сетевой фильтр Synproxy перехватывает новые TCP-соединения и обрабатывает начальное трёхстороннее подтверждение связи по протоколу TCP, используя syncookies вместо conntrack для установления соединения. Таким образом, запуск SynProxy на порту прослушивающего сервера предотвращает использование ограниченных ресурсов conntrack при атаках типов SYN, SYN-ACK, ACK Flood на этот порт, при которых сервер подвергается воздействию большого количества syn-пакетов. Данное действие требует отслеживания соединения, поскольку необходимо передать порядковые номера. Принцип работы: сервер вычисляет значение на основе текущего состояния и отправляет его в SYN+ACK-пакете. Когда клиент возвращает ACK-пакет, сервер извлекает значение для аутентификации. Если значение верно, соединение считается установленным.

Примечание:

Каждое правило **МЭ** должно принадлежать какому-либо набору правил.

6.3.2.1 Добавление правила МЭ

Создание правила МЭ типа Ipv4 и IPv6

Для добавления правила **МЭ** необходимо выполнить следующие действия:

1. Перейти в подраздел **«Межсетевой экран» - «Настройки межсетевого экрана» - «Правила межсетевого экрана»** и нажать **кнопку «+Добавить»**.
2. В открывшейся боковой панели выбрать создаваемую сущность **«Правило»** (см. Рисунок – Добавление правила).

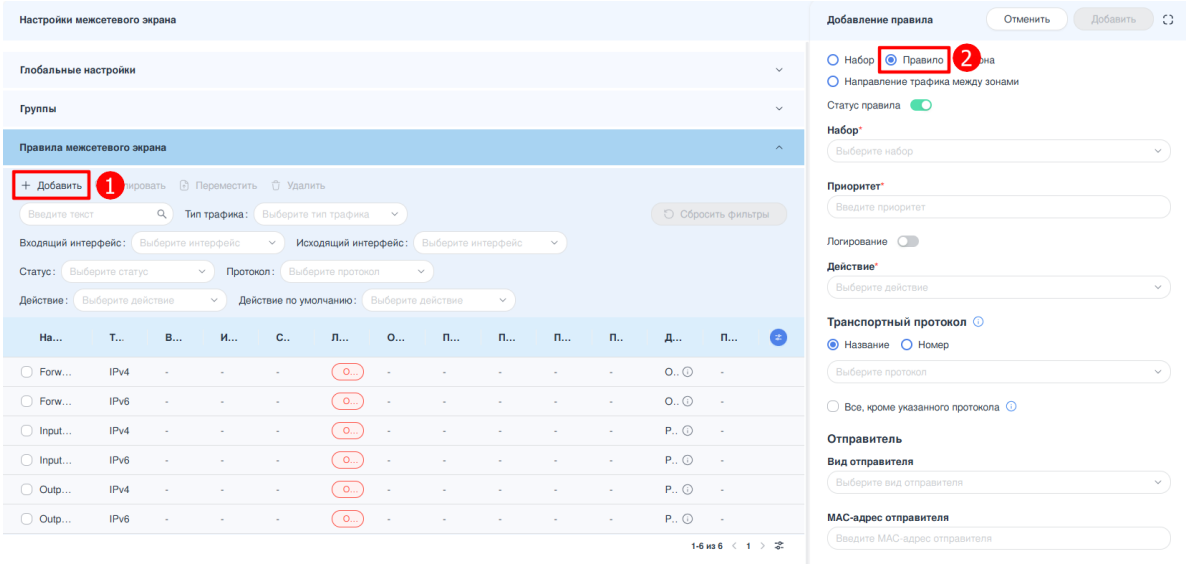


Рисунок – Добавление правила

3. Внести/скорректировать значение в полях (см. Рисунок – Параметры правила):

   - **«Статус правила»** - включение/отключение правила, по умолчанию правило включено.
   - **«Набор»** - набор правил, к которому будет принадлежать создаваемое правило. Справа от имени набора в скобках указан тип набора: IPv4 или IPv6. В зависимости от выбранного набора правил откроются дополнительные поля настройки.
   - **«Приоритет»** - номер приоритета правила. Возможно указать значение в диапазоне от «1» до «999999». Параметр должен быть уникальным в рамках выбранного набора правил и определяет последовательность выполнения правил.
   - **«Логирование»** - включение/отключение журналирования действий, по умолчанию логирование правила отключено.
   - **«Действие»** - выбор действия над сетевым пакетом.

     При выборе действия **«Разгрузить (offload)»** требуется указать целевую таблицу потоков для экспорта. Для этого в поле **«Потоковая таблица»** необходимо выбрать соответствующую таблицу из выпадающего списка. Действие **«Разгрузить (offload)»** недоступно для наборов типа **Input** и **Output**.

В случае выбора действия **«Synproxy»** необходимо дополнительно указать следующие параметры:

- **MSS** - максимальный размер полезного блока данных в байтах для TCP-пакета (сегмента). Возможно указать значение в диапазоне от «501» до «65535».
- **Коэффициент масштабирования окна** - коэффициент масштабирования окна для TCP-соединения. Возможно указать значение в диапазоне от «1» до «14».

Примечание:

Для действия **«Synproxy»** необходимо выбрать протокол **«TCP»**.

При выборе действия **«Перейти (jump)»** последующая проверка пакета осуществляется в кастомном наборе, указанном в дополнительном поле **«Переадресация»**.

Примечание:

При использовании действия **«Перейти (jump)»** не допускается создание бесконечных циклов, когда набор перенаправляет сам на себя или через несколько переходов возвращается к себе.

В случае выбора действия **«В очередь (queue)»** необходимо дополнительно указать следующие параметры:

- **Очередь** - номер очереди, в которую будут направлены пакеты, соответствующие заданному правилу. Возможно указать значение в диапазоне от «0» до «65535» или диапазон значений через дефис в формате X-Y.
- **Исключать из очереди** - исключать пакеты из очереди и пропускать их через **МЭ**, если ни одно приложение в пользовательском пространстве не подключено к данной очереди.
- **Распределение** - распределять пакеты между несколькими очередями. Распределение возможно включить, только если указан диапазон очередей.

- **«Входящий интерфейс»** - предназначено для указания одного или группы входящих интерфейсов. При выборе значения **«Интерфейсы»** требуется задать имя физического или виртуального интерфейса **«ARMA Стена»**. Допускается использование подстановочного знака «*» для группового выбора интерфейсов (например, значение «eth*» позволяет охватить все интерфейсы типа Ethernet). Поддерживается указание входящего интерфейса в качестве критерия соответствия для

наборов правил: **«name»**, **«input»**, **«forward»**. Для инверсии условия соответствия доступна опция «Все, кроме указанного интерфейса» — при активации соответствующего чекбокса правило применяется ко всем интерфейсам, за исключением указанных.

- **«Исходящий интерфейс»** - назначить исходящий интерфейс или группу интерфейсов. При выборе значения **«Интерфейсы»** требуется задать имя физического или виртуального интерфейса **«ARMA Стена»**. Допускается использование подстановочного знака «*» для группового выбора интерфейсов. Поддерживается указание исходящего интерфейса в качестве критерия соответствия для наборов правил: **«name»**, **«output»**, **«forward»**. Для инверсии условия соответствия доступна опция «Все, кроме указанного интерфейса» — при активации соответствующего чекбокса правило применяется ко всем интерфейсам, за исключением указанных.
- **«Транспортный протокол»** - значение транспортного протокола. Возможно указать значение номером или именем протокола:
  - **«Номер»** - номер протокола в соответствии с документом IANA. Возможно указать значение в диапазоне от «0» до «255».
  - **«Название»** - выбор транспортного протокола из выпадающего списка. Для инверсии условия соответствия доступна опция «Все, кроме указанного протоколов».
- **«Вид отправителя»** - выбор отправителя из списка:
    - **«Адрес»** - указание IP-адреса отправителя в формате IPv4 или IPv6 в зависимости от типа набора правил.
    - **«Диапазон адресов»** - задание диапазона IP-адресов отправителя в соответствующих полях.
    - **«Сеть»** - указание сети отправителя с использованием IP-адреса и маски подсети.
    - **«Группа адресов»** - выбрать группу адресов из списка.
    - **«Группа сетей»** - выбрать группу сетей из списка.
    - **«Группа доменов»** - выбрать группу доменов из списка.
    - **«Полное доменное имя»** - предназначено для указания доменного имени в формате FQDN в поле **«Доменное имя»**. Требования к формату ввода:
        - общая длина значения не должна превышать 242 символа;

- имя должно начинаться и заканчиваться латинской буквой (A–Z, a–z) или цифрой (0–9);
- не допускается начало или окончание имени символами «.» или «-»;
- разрешены только следующие символы: латинские буквы (A–Z, a–z), цифры (0–9), а также символы «.» (точка) и «-» (дефис);
- каждая доменная метка (группа между точками) не должна превышать «63» символа и не может быть пустой;
- максимальное количество доменных меток, разделённых точками, — «127».

- **«Код страны (DB-IP.com)»** - выбор страны, определяемой по геоинформационной базе DB-IP.com, как критерия источника трафика.

Для инверсии условия соответствия доступна опция «Все, кроме указанного отправителя». Доступна для следующих отправителей: «Адрес», «Диапазон адресов», «Сеть», «Код страны (DB-IP.com)».

- **«MAC-адрес отправителя»** - ввести MAC-адрес отправителя. Для инверсии условия соответствия доступна опция «Все, кроме указанного MAC-адреса».
- **«Группа MAC-адресов»** - выбрать группу MAC-адресов из списка.
- **«Динамическая группа отправителя»** - выбрать динамическую группу из списка.
- **«Порт отправителя»** - указать порт отправителя вручную или выбрать группу. Для ручного ввода порта необходимо выбрать значение «Порты», после чего станут доступны следующие варианты указания порта: «Номер порта», «Диапазон портов», «Протокол». Поле становится доступным, если в блоке **«Транспортный протокол»** указано одно из значений: имя **«TCP»**, имя **«TCP и UDP»**, имя **«UDP»**.
- **«Вид получателя»** - выбор получателя из списка:
  - **«Адрес»** - указание IP-адреса получателя в формате IPv4 или IPv6 в зависимости от типа набора правил.
  - **«Диапазон адресов»** - задание диапазона IP-адресов получателя в соответствующих полях.
  - **«Сеть»** - указание сети получателя с использованием IP-адреса и маски подсети.

- **«Группа адресов»** - выбрать группу адресов из списка.
- **«Группа сетей»** - выбрать группу сетей из списка.
- **«Группа доменов»** - выбрать группу доменов из списка.
- **«Полное доменное имя»** - предназначено для указания доменного имени в формате FQDN в поле **«Доменное имя»**. Требования к формату ввода:
    - общая длина значения не должна превышать 242 символа;
    - имя должно начинаться и заканчиваться латинской буквой (A–Z, a–z) или цифрой (0–9);
    - не допускается начало или окончание имени символами «.» или «-»;
    - разрешены только следующие символы: латинские буквы (A–Z, a–z), цифры (0–9), а также символы «.» (точка) и «-» (дефис);
    - каждая доменная метка (группа между точками) не должна превышать «63» символа и не может быть пустой;
    - максимальное количество доменных меток, разделённых точками, — «127».
- **«Код страны (DB-IP.com)»** - выбор страны, определяемой по геоинформационной базе DB-IP.com, как критерия источника трафика.

Для инверсии условия соответствия доступна опция «Все, кроме указанного получателя». Доступна для следующих отправителей: «Адрес», «Диапазон адресов», «Сеть», «Код страны (DB-IP.com)».

- **«MAC-адрес получателя»** - ввести MAC-адрес получателя. Для инверсии условия соответствия доступна опция «Все, кроме указанного MAC-адреса».
- **«Группа MAC-адресов»** - выбрать группу MAC-адресов из списка.
- **«Динамическая группа получателя»** - выбрать динамическую группу из списка.
- **«Порт получателя»** - указать порт получателя вручную или выбрать псевдоним. Для ручного ввода порта необходимо выбрать значение «Порты», после чего станут доступны следующие варианты указания порта: «Номер порта», «Диапазон портов», «Протокол». Поле

становится доступным, если в блоке **«Транспортный протокол»** указано одно из значений: имя **«TCP»**, имя **«TCP и UDP»**, имя **«UDP»**.

- **«Добавление адресов в динамическую группу»** - раздел настроек, предназначенный для добавления IP-адресов отправителя и получателя в динамические группы:
    - **«Динамическая группа отправителя»** - выбор из выпадающего списка динамической группы, в которую добавляется IP-адрес отправителя;
    - **«Единица времени действия правила»** - выбор единицы измерения длительности пребывания адреса в динамической группе;
    - **«Значение (<выбранная единица времени>)»** - указание продолжительности пребывания адреса отправителя в динамической группе. Допустимые диапазоны значений в зависимости от выбранной единицы времени:
        - **секунды** - от «0» до «99 999 999»;
        - **минуты** - от «0» до «99 999 999»;
        - **часы** - от «0» до «5 124 095»;
        - **дни** - от «0» до «213 503».
    - **«Динамическая группа получателя»** - выбор из выпадающего списка динамической группы, в которую добавляется IP-адрес получателя;
    - **«Единица времени действия правила»** - выбор единицы измерения длительности пребывания адреса в динамической группе;
    - **«Значение (<выбранная единица времени>)»** - указание продолжительности пребывания адреса получателя в динамической группе. Допустимые диапазоны значений в зависимости от выбранной единицы времени:
        - **секунды** - от «0» до «99 999 999»;
        - **минуты** - от «0» до «99 999 999»;
        - **часы** - от «0» до «5 124 095»;
        - **дни** - от «0» до «213 503».
- **«Сообщения ICMP»** - компонент доступен для заполнения только при условии, что в блоке **«Транспортный протокол»** указано имя **«ICMP»** / номер **«1»** для IPv4 или имя **«IPv6-ICMP»** / номер **«58»** для IPv6.

- **«Тип»** - номер типа ICMP в диапазоне от «0» до «255».
- **«Код»** - номер кода ICMP в диапазоне от «0» до «255».
- **«Имя»** - имя типа ICMP, выбор из выпадающего списка.

- **«Анализ фрагментов IP»** - сопоставление пакетов на основе критерия фрагмента IP.
- **«IPsec»** - соответствие пакетов на основе критериев IPsec. В системном наборе правил **«output»** фильтрация пакетов на основе IPsec не применяется.
- **«Ограничение скорости»** - блок параметров, определяющий частоту срабатывания правила. Правило продолжает проверяться до достижения заданного лимита пакетов.
  - **«Количество пакетов»** - целое положительное число, начиная с «1». Максимально допустимое значение зависит от выбранной единицы времени:
    - для секунды — от «1» до «10 000»;
    - для минуты — от «1» до «600 000»;
    - для часа — от «1» до «36 000 000»;
    - для суток — от «1» до «864 000 000».

    При активации параметра **«Допустимое превышение лимита»** минимальные значения диапазона устанавливаются следующим образом:
    - для секунды — от «1» до «10 000»;
    - для минуты — от «14» до «600 000»;
    - для часа — от «839» до «36 000 000»;
    - для суток — от «20 117» до «864 000 000».
  - **«Единица времени»** - выбор единицы измерения временного интервала из предопределённого списка.
  - **«Допустимое превышение лимита»** - максимальное количество пакетов, разрешаемое при превышении скорости. Возможно указать значение в диапазоне от «1» до «4294967295».
- **«Сопоставление отправителей пакетов»** - блок компонентов для настройки критерия срабатывания правила на основании частоты принимаемых пакетов от одного отправителя.

- **«Количество»** - число последних пакетов от одного отправителя. Возможно указать значение в диапазоне от «1» до «255».
- **«Время»** - указать единицу измерения: минута, час, секунда.

- **«Типы соединений»** - правило проверяется только на указанные состояния соединений.
- **«Число прыжков»** - блок и его дочерние компоненты доступны для заполнения только при условии, что правило относится к типу «IPv6». Дополнительные поля для настройки:
  - **«Знак сравнения»** - возможно выбрать следующие знаки сравнения: равно, больше или равно, меньше или равно.
  - **«Число прыжков»** - возможно ввести целочисленное значение в диапазоне от «0» до «255».
- **«Максимальный размер сегмента (MSS)»** - параметр доступен если указан транспортный протокол «tcp». Возможно указать значения в диапазоне от «1» до «16384». Возможно ввести диапазон значений в формате «X-Y».
- **«Флаги TCP»** - правило будет проверять только те TCP-пакеты, значения проверяемых флагов которых, совпадают с настроенным. Блок и его дочерние компоненты доступны при условии, что в блоке **«Транспортный протокол»** выбрано имя **«TCP»**.
- **«Расписание»** - блок предназначен для определения временных интервалов активности правила в соответствии с системным временем устройства **ARMA Стена**.

4. По завершению нажать **кнопку «Добавить»**.

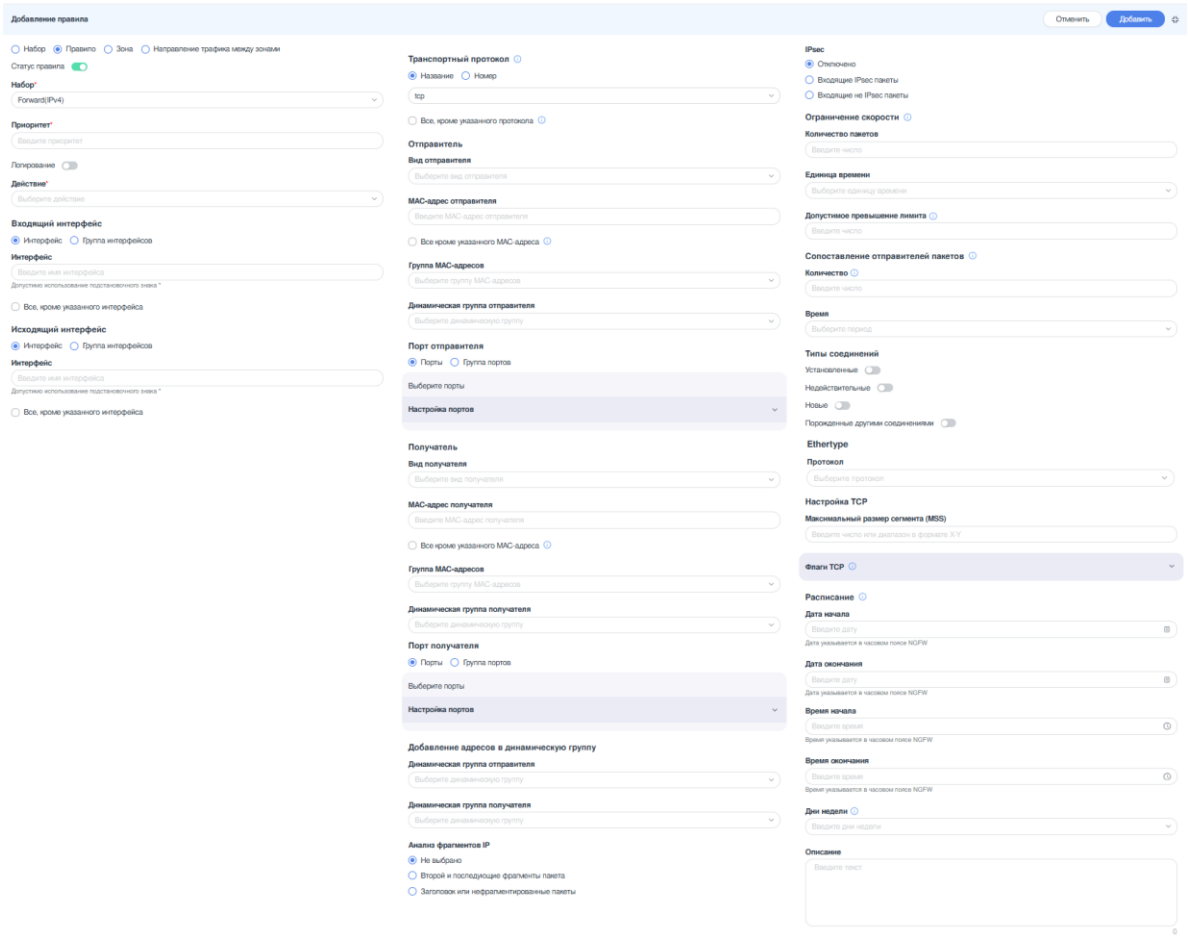


Рисунок – Параметры правила

Создание правила МЭ для наборов правил сетевого моста

Для создания правила **МЭ** необходимо выполнить следующие действия:

1. Перейти в подраздел **«Межсетевой экран» - «Настройки межсетевого экрана» - «Правила межсетевого экрана»** и нажать **кнопку «+Добавить»**.
2. В открывшейся боковой панели выбрать создаваемую сущность **«Правило»**.
3. Задать или скорректировать значения параметров правила (см. Рисунок – Параметры правила для сетевого мосат):
   - **«Статус правила»** - определяет состояние правила: включено или отключено. По умолчанию правило включено.
   - **«Набор»** - выбор набора сетевого моста, к которому будет отнесено правило.
   - **«Приоритет»** - числовое значение приоритета в диапазоне от «1» до «999999». Значение должно быть уникальным в пределах выбранного набора и определяет порядок обработки правил.

- **«Логирование»** - включение или отключение журналирования событий, соответствующих данному правилу. По умолчанию логирование отключено.
- **«Действие»** - определяет обработку сетевого пакета при соответствии условиям правила. Доступны следующие варианты:
    - **«Разрешить (accept)»** - разрешить пакет;
    - **«Отбросить (drop)»** - отбросить пакет (по умолчанию);
    - **«Вернуться (return)»** - вернуться из кастомного набора правил и перейти к следующему правилу;
    - **«Перейти (jump)»** - перейти к кастомному набору правил;
    - **«Продолжить (continue)»** - продолжить проверку следующего правила;
    - **«В очередь (queue)»** - отправляет пакет в пользовательское пространство для дальнейшей обработки.

  При выборе действия **«Перейти (jump)»** последующая проверка пакета осуществляется в кастомном наборе, указанном в дополнительном поле **«Переадресация»**.

  Примечание:

  При использовании действия **«Перейти (jump)»** не допускается создание бесконечных циклов, когда набор перенаправляет сам на себя или через несколько переходов возвращается к себе.

  В случае выбора действия **«В очередь (queue)»** необходимо дополнительно указать следующие параметры:

    - **Очередь** - номер очереди, в которую будут направлены пакеты, соответствующие заданному правилу. Возможно указать значение в диапазоне от «0» до «65535» или диапазон значений через дефис в формате X-Y.
    - **Исключать из очереди** - исключать пакеты из очереди и пропускать их через **МЭ**, если ни одно приложение в пользовательском пространстве не подключено к данной очереди.
    - **Распределение** - распределять пакеты между несколькими очередями. Распределение возможно включить, только если указан диапазон очередей.
- **«Входящий интерфейс»** - предназначено для указания одного или группы входящих интерфейсов. При выборе значения **«Интерфейсы»**

требуется задать имя физического или виртуального интерфейса **«ARMA Стена»**. Допускается использование подстановочного знака «*» для группового выбора интерфейсов (например, значение «eth*» позволяет охватить все интерфейсы типа Ethernet). Для инверсии условия соответствия доступна опция «Все, кроме указанного интерфейса» — при активации соответствующего чекбокса правило применяется ко всем интерфейсам, за исключением указанных.

- **«Исходящий интерфейс»** - назначить исходящий интерфейс или группу интерфейсов. При выборе значения **«Интерфейсы»** требуется задать имя физического или виртуального интерфейса **«ARMA Стена»**. Допускается использование подстановочного знака «*» для группового выбора интерфейсов. Для инверсии условия соответствия доступна опция «Все, кроме указанного интерфейса» — при активации соответствующего чекбокса правило применяется ко всем интерфейсам, за исключением указанных.
- **«MAC-адрес отправителя»** - задание MAC-адреса источника. Поддерживается инверсия условия с помощью опции «Все, кроме указанного MAC-адреса»;
- **«MAC-адрес получателя»** - задание MAC-адреса назначения. Поддерживается инверсия условия с помощью опции «Все, кроме указанного MAC-адреса»;
- **«Ethertype»** - блок параметров настройки фильтрации сетевого трафика по значению поля EtherType в заголовке Ethernet-кадра. Позволяет осуществлять точную сегментацию пакетов и обрабатывать только кадры требуемых типов, включая ARP, VLAN, IPv6 и другие.
    - **«Протокол»** - содержит перечень наиболее часто используемых значений EtherType:
        - **802.1q** — соответствует 0x8100 (VLAN Tagged Frame);
        - **802.1ad** — соответствует 0x88A8 (Provider Bridging);
        - **arp** — соответствует 0x0806 (Address Resolution Protocol);
        - **ipv4** — соответствует 0x0800;
        - **ipv6** — соответствует 0x86DD;
        - **ethercat** — соответствует 0x88A4;
        - **Другое (0xXXXX)** - опция для задания произвольного значения EtherType. При выборе

данной опции становится доступным дополнительное поле **«Значение»**, в которое необходимо ввести двухбайтовое шестнадцатеричное число в формате 0xXXXX.

- **«Фильтрация по VLAN»** - блок параметров, применяемый при анализе EtherType в заголовке, расположенном после тега VLAN (внутренний EtherType).
    - **«Ethertype внутри VLAN»** - список предопределённых значений EtherType для внутреннего заголовка:
        - **802.1q** — 0x8100;
        - **802.1ad** — 0x88A8;
        - **arp** — 0x0806;
        - **ipv4** — 0x0800;
        - **ipv6** — 0x86DD;
        - **ethercat** — 0x88A4;
        - **Другое (0xXXXX)** - опция для задания произвольного значения EtherType. При выборе данной опции становится доступным дополнительное поле **«Значение»**, в которое необходимо ввести двухбайтовое шестнадцатеричное число в формате 0xXXXX.
    - **«VLAN ID»** - идентификатор VLAN (диапазон от «0» до «4095») или диапазон в формате «X-Y».
    - **«Приоритет»** - значение поля приоритета 802.1p (диапазон от «0» до «7») или диапазон в формате «X-Y».

4. По завершению конфигурации нажать **кнопку «Добавить»**.

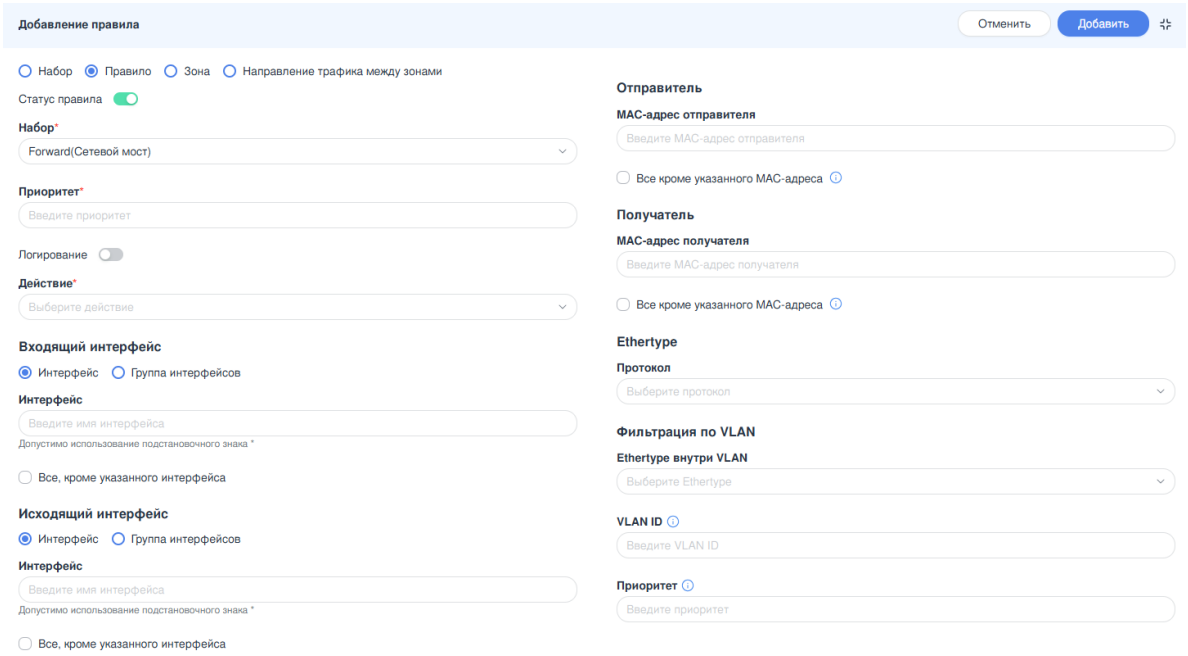


Рисунок – Параметры правила для сетевого моста

При указании в одном правиле нескольких критериев соответствия применяется логическое условие **И (AND)**: правило срабатывает только в случае одновременного совпадения всех заданных критериев.

Это требует особого внимания при проектировании правил. Например, если в одном правиле в качестве домена источника и домена назначения указан один и тот же адрес — например, example.com — и для правила задано действие drop, то блокировка применена не будет к обычному трафику пользователей, направленному к example.com. Правило в данном случае будет соответствовать только тем сетевым соединениям, у которых и источник, и получатель принадлежат домену example.com, что в типовой сетевой инфраструктуре маловероятно.

6.3.2.2 Редактирование правила

Для редактирования правила необходимо нажать **ЛКМ** на строке с нужным правилом и в открывшейся боковой панели внести корректировки в атрибуты правила. По завершению нажать **кнопку «Сохранить»**.

6.3.2.3 Копирование правила

Копирование правил допускается исключительно в набор правил, идентичный по типу исходному набору, в котором находятся копируемые правила.

Для копирования правила необходимо выполнить следующие действия:

1. Выбрать правило, установив флажок в чек-боксе слева от наименования правила, и нажать **кнопку «Копировать»**.
2. В появившейся боковой панели **«Копирование правила»** выбрать целевой набор правил, в который будет скопировано правило. Система автоматически проверяет наличие конфликта по значению приоритета в

целевом наборе. Если значение приоритета уже используется, система назначает ближайшее доступное значение, увеличивая исходный приоритет на единицу или более, в зависимости от свободных позиций в последовательности. При необходимости возможно изменить параметры правила, включая значение приоритета.

3. Нажать **кнопку «Копировать»** (см. Рисунок – Копирование правила).

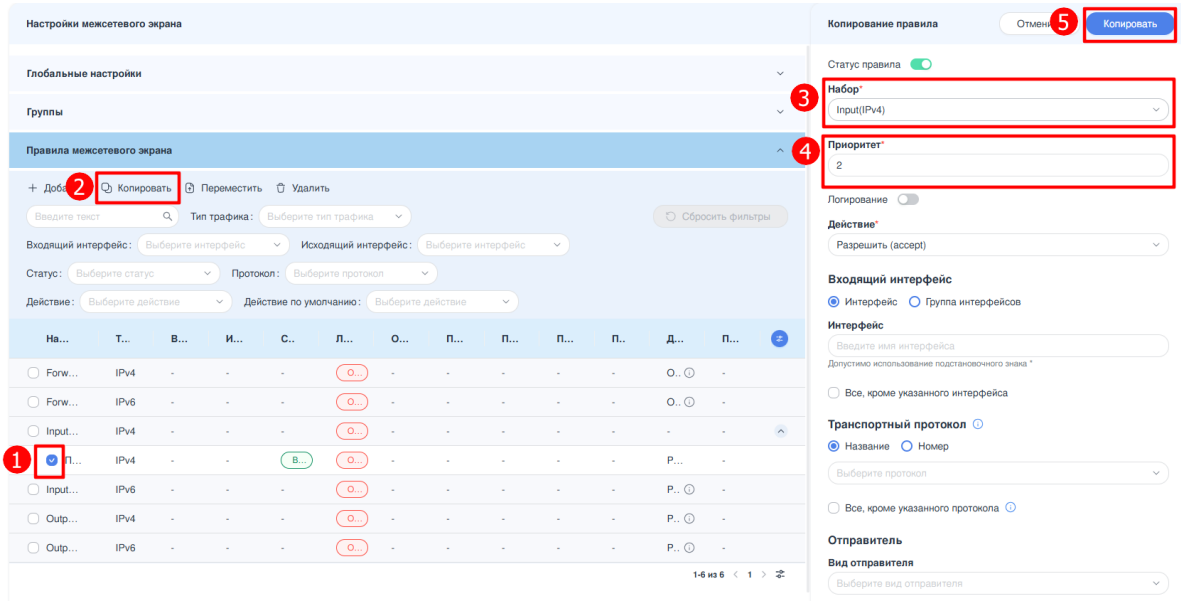


Рисунок – Копирование правила

При копировании нескольких правил одновременно в окне **«Копирование правил»** необходимо выбрать целевой набор и задать начальный приоритет. Приоритеты будут назначены последовательно, начиная с указанного значения.

Копирование правил в наборы, на которые осуществляется переход с помощью действия **«Перейти (jump)»**, указанного в самих правилах, запрещено. При попытке выполнить такое копирование система выводит предупреждение о невозможности копирования правила, осуществляющего переход в целевой набор.

Данное ограничение введено с целью предотвращения формирования циклических (петлевых) цепочек правил, способных привести к нарушению обработки трафика и неопределённому поведению политик фильтрации.

6.3.2.4 Перемещение правила

Перемещение правил допускается только в набор правил того же типа, что и исходный набор, в котором они находятся в текущий момент.

Для перемещения правила необходимо выполнить следующие действия:

1. Выбрать правило, установив флажок в чек-боксе слева от наименования правила, и нажать **кнопку «Переместить»**.
2. В открывшейся боковой панели **«Перемещение правила»** указать целевой набор правил, в который будет перемещено выбранное правило.

Система автоматически проверяет наличие конфликта по значению приоритета в целевом наборе. Если значение приоритета уже используется, система назначает ближайшее доступное значение, увеличивая исходный приоритет на единицу или более, в зависимости от свободных позиций в последовательности. При необходимости возможно изменить параметры правила, включая значение приоритета.

3. Нажать **кнопку «Переместить»** (см. Рисунок – Копирование правила).

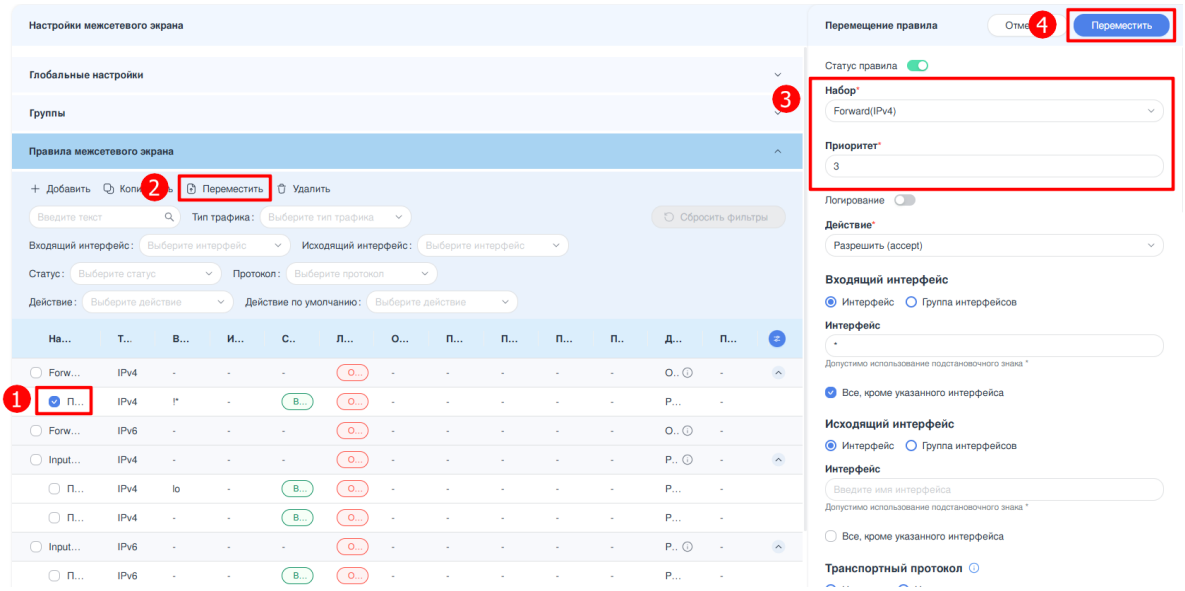


Рисунок – Копирование правила

При перемещении нескольких правил одновременно в окне **«Перемещение правил»** необходимо выбрать целевой набор и задать начальный приоритет. Приоритеты будут назначены последовательно, начиная с указанного значения.

Перемещение правил в наборы, на которые осуществляется переход с помощью действия **«Перейти (jump)»**, указанного в самих правилах, запрещено. При попытке выполнить такое перемещение система выводит предупреждение о невозможности переместить правила, осуществляющего переход в целевой набор.

6.3.2.5 Удаление правила

Для удаления правила необходимо выбрать одно или несколько правил, установив флажки слева от их наименований, нажать **кнопку «Удалить»** и подтвердить действие в появившемся диалоговом окне.

6.3.3 Поиск и фильтрация правил

Блок фильтрации предназначен для отбора событий **МЭ** в соответствии с заданными пользователем критериями. По умолчанию блок фильтрации содержит следующие поля (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **«Тип трафика»**;

- **«Входящий интерфейс»**;
- **«Исходящий интерфейс»**;
- **«Статус»**;
- **«Протокол»**;
- **«Действие»**;
- **«Действие по умолчанию»**;
- **кнопка «Сбросить фильтры»»**.

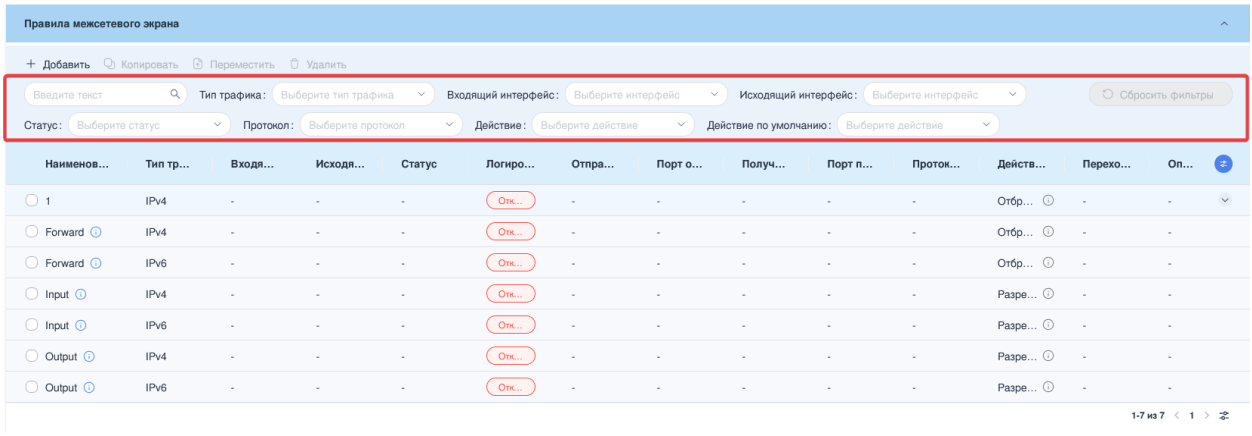


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем столбцам таблицы.

Фильтрация по полю **«Тип трафика»** позволяет отфильтровать правила **МЭ** по версии IP-протокола.

Фильтрация по полю **«Входящий интерфейс»** позволяет отфильтровать правила по входящему интерфейсу.

Фильтрация по полю **«Исходящий интерфейс»** позволяет отфильтровать правила **МЭ** по исходящему интерфейсу.

Фильтрация по полю **«Статус»** позволяет отфильтровать правила **МЭ** по текущему статусу правила.

Фильтрация по полю **«Протокол»** позволяет отфильтровать правила **МЭ** по протоколу, в контексте которого будет применено правило обработки пакета.

Фильтрация по полю **«Действие»** позволяет отфильтровать правила **МЭ** по виду действия, применяемому к пакету данных.

Фильтрация по полю **«Действие по умолчанию»** позволяет отфильтровать правила **МЭ** по виду действия по умолчанию, применяемому к пакету данных.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

6.4 Политика на основе зон сети

6.4.1 Зоны сети

В архитектуре безопасности, основанной на зонах, сетевые интерфейсы группируются в зоны, которые определяются на основе их функционального или логического сходства. Трафик, проходящий через зону, регулируется назначенными кастомными наборами правил. Данный подход обеспечивает более детальный и целенаправленный контроль над сетевым трафиком, позволяя применять различные уровни доступа и защиты в зависимости от конкретных требований каждой зоны.

В **МЭ** на основе зон реализована новая концепция, дополнительно к стандартным входящим и исходящим потокам трафика был добавлен локальный поток. Он предназначен для входящего и исходящего трафика **ARMA Стена** (см. Рисунок – Схема направления трафика в зонах сети **МЭ**). Это предоставляет возможность установить дополнительные правила **МЭ**, которые будут защищать сам брандмауэр от внешних угроз сети, дополняя уже существующие входящие и исходящие правила **МЭ**.

Рисунок – Схема направления трафика в зонах сети МЭ

Примечание:

Создать локальную зону возможно исключительно через интерфейс командной строки.

Основные тезисы:

- интерфейс может быть назначен только одной зоне;
- в пределах зоны разрешён весь входящий и исходящий трафик интерфейса;
- трафик между зонами зависит от существующих политик;
- трафик не может передаваться между интерфейсом-участником зоны и любым интерфейсом, который не является участником этой зоны;
- для каждого направления трафика необходимо задать отдельную политику.

В общем случае алгоритм настройки работы **МЭ** на основе зон сети выглядит следующим образом:

1. Создать **кастомные наборы правил МЭ**, в которых будут содержаться правила.

2. Создать **правила МЭ**, указать в них критерии соответствия, действия с сетевыми пакетами и привязать эти правила к кастомным наборам.
3. Объединить интерфейсы в **зоны**.
4. Создать два **направления трафика между зонами сети** (входящий и исходящий трафик) и назначить на них созданные кастомные наборы правил.

Для просмотра и настройки зоны сети необходимо перейти в раздел **«Зоны сети»** меню **«Настройки межсетевого экрана»** (см. Рисунок – Зоны сети).

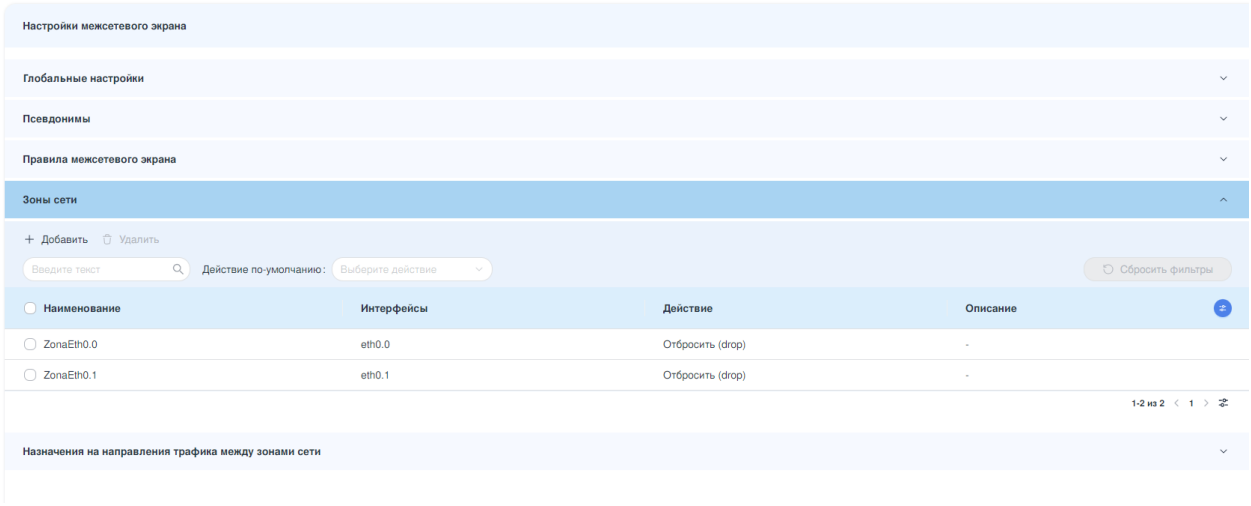


Рисунок – Зоны сети

6.4.1.1 Добавление зоны сети

Для создания новой зоны необходимо нажать **кнопку «+Добавить»** в таблице **«Зоны сети»** и в открывшейся боковой панели внести значения в поля (см. Рисунок – Добавление зоны сети):

- **«Наименование»** - максимальная длина значения - «18» символов. Допускается использование только латинских букв (A–Z, a–z), цифр (0–9) и специальных символов: подчёркивание («_») и точка («.»). Значение должно начинаться с латинской буквы или цифры;
- **«Действие по умолчанию»** - действие по умолчанию для входящего трафика: «Отбросить (drop)» (по умолчанию) или «Отклонить (reject)»;
- **«Логирование»** - включить запись событий в глобальный журнал;
- **«Интерфейс»** - выбор физических и виртуальных интерфейсов. Список отображает только те интерфейсы, которые в текущий момент не принадлежат ни одной зоне;
- **«Описание»** - максимально допустимая длина значения поля «127» символов.

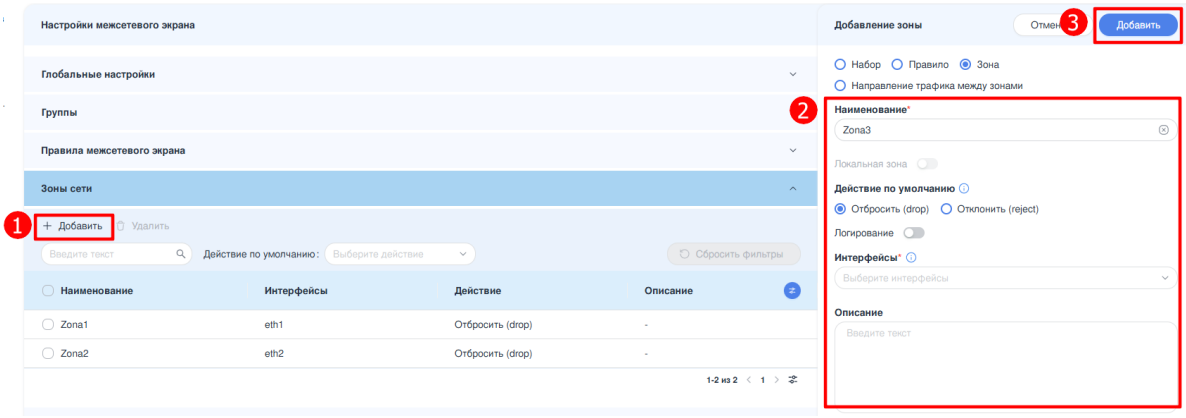


Рисунок – Добавление зоны сети

Примечание:

При добавлении зоны на интерфейс происходит полное блокирование всего транзитного трафика, проходящего через этот интерфейс, в соответствии с политикой действий по умолчанию.

6.4.1.2 Редактирование зоны сети

Для редактирования параметров зоны сети необходимо нажать **ЛКМ** по строке с наименованием требуемой зоны. После открытия боковой панели редактирования допускается внесение изменений в доступные поля конфигурации.

Изменение наименования зоны сети не поддерживается, поле **«Наименование»** заблокировано для редактирования.

После внесения необходимых корректировок следует нажать **кнопку «Изменить»**.

6.4.1.3 Удаление зоны сети

Для удаления зон сети необходимо выбрать одну или несколько зон, установив флажок в чек-боксе слева от наименования зоны, и нажать **кнопку «Удалить»**. В появившемся диалоговом окне подтвердить операцию, нажав **кнопки «Удалить»**.

Если зона назначена в качестве зоны отправителя, система отобразит уведомление о невозможности удаления этой зоны. Удаление становится доступным только после снятия соответствующих назначений.

6.4.2 Назначения на направления трафика между зонами сети

Для добавления направления трафика между зонами сети необходимо выполнить следующие действия:

1. Перейти в подраздел **«Межсетевой экран» - «Настройки межсетевого экрана» - «Назначения на направления трафика между зонами сети»** и нажать **кнопку «+Добавить»**
2. В открывшейся боковой панели внести значения в поля:
   - **«Зона отправителя»** - выбор из списка зоны отправителя;

- **«Интерфейсы зоны отправителя»** - отображает интерфейсы, входящие в выбранную зону отправителя. Поле заблокировано для редактирования;
- **«Зона получателя»** - выбор из списка зоны получателя;
- **«Интерфейсы зоны получателя»** - отображает интерфейсы, входящие в выбранную зону получателя. Поле заблокировано для редактирования;
- **«Действие по умолчанию»** - значение наследуется из настройки зоны получателя;
- **«Набор IPv4»** - выбор из списка набора правил с типом IPv4;
- **«Перейти к списку наборов»** - открывает окно выбора набора правил IPv4 с возможностью просмотра и редактирования входящих в них правил (см. Рисунок – Выбор набора правил);
- **«Набор IPv6»** - выбор из списка набора правил с типом IPv6;
- **«Перейти к списку наборов»** - открывает окно выбора набора правил IPv6 с возможностью просмотра и редактирования входящих в них правил.

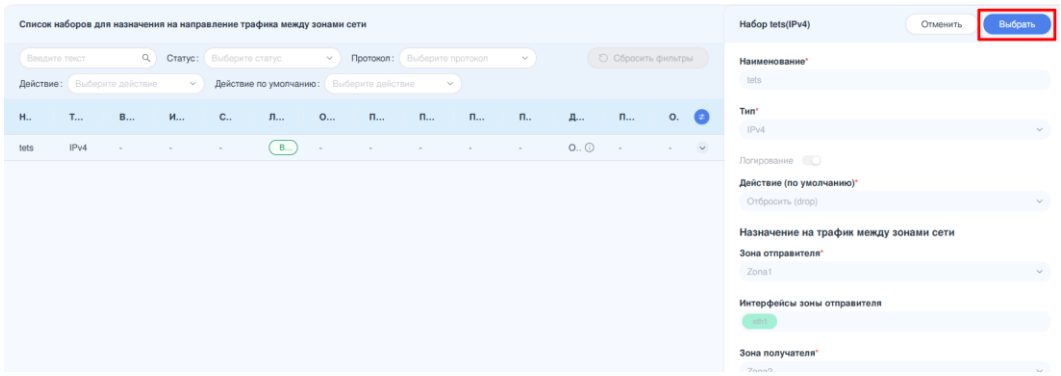


Рисунок – Выбор набора правил

3. По завершению нажать **кнопку «Добавить»** (см. Рисунок – Добавление направления трафика между зонами)

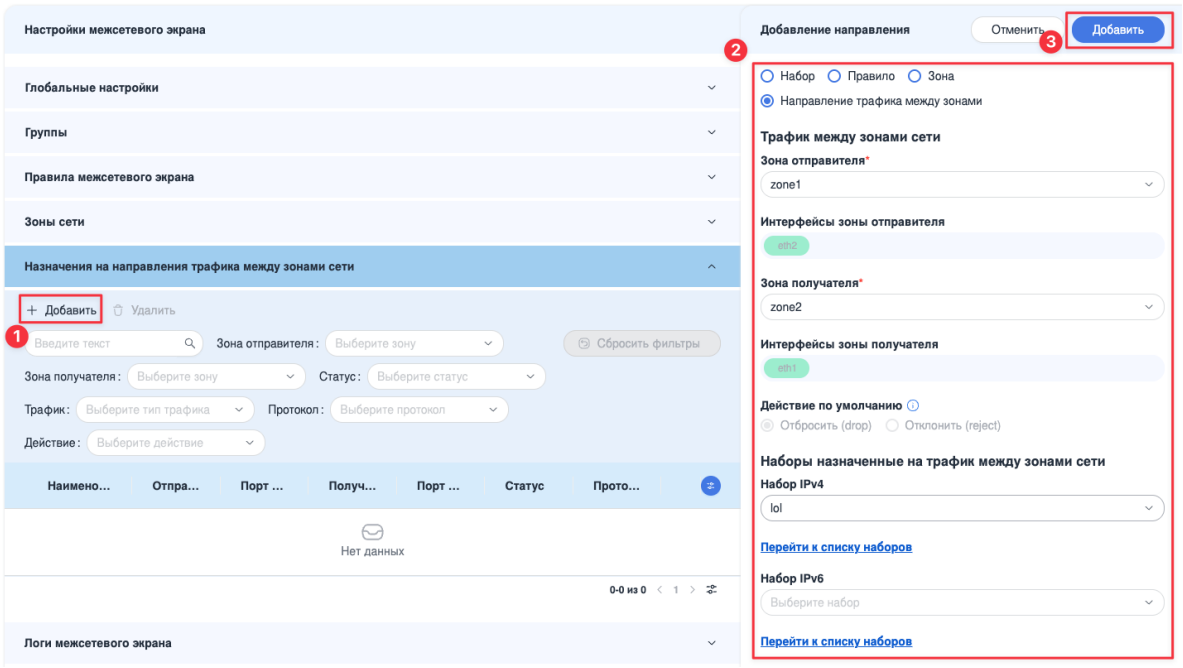


Рисунок – Добавление направления трафика между зонами

Для редактирования направления трафика между зонами сети необходимо нажать **ЛКМ** на строку с нужным набором и в открывшейся боковой панели внести корректировки. По завершению нажать **кнопку «Сохранить»**.

Для удаления направления необходимо выбрать одно или несколько направлений, установив флажок в чек-боксе слева от наименования направления, и нажать **кнопку «Удалить»**. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

Поиск и фильтрация по таблице назначений на направления осуществляется по следующим полям:

- **«Зона отправителя»**;
- **«Зона получателя»**;
- **«Статус»**;
- **«Трафик»**;
- **«Протокол»**;
- **«Действие»**.

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем столбцам таблицы.

Фильтрация по полю **«Зона отправителя»** позволяет отфильтровать назначения на направления трафика по версии зоне отправителя.

Фильтрация по полю **«Зона получателя»** позволяет отфильтровать назначения на направления трафика по зоне получателя.

Фильтрация по полю **«Статус»** позволяет отфильтровать назначения на направления трафика по текущему статусу назначения.

Фильтрация по полю **«Трафик»** позволяет отфильтровать назначения на направления трафика по версии IP-протокола.

Фильтрация по полю **«Протокол»** позволяет отфильтровать назначения на направления трафика по протоколу, в контексте которого будет применено правило обработки трафика.

Фильтрация по полю **«Действие»** позволяет отфильтровать назначения на направления трафика по виду действия.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

6.5 Журнал МЭ

В настоящем разделе представлено описание раздела меню **«Логи межсетевого экрана»**, предназначенного для просмотра и фильтрации событий, связанных со срабатыванием правил **МЭ**.

Для доступа к журналу событий **МЭ** необходимо выполнить переход в подраздел **«Логи межсетевого экрана»** из раздела **«Настройки межсетевого экрана»** (см. Рисунок – Журнал событий МЭ)

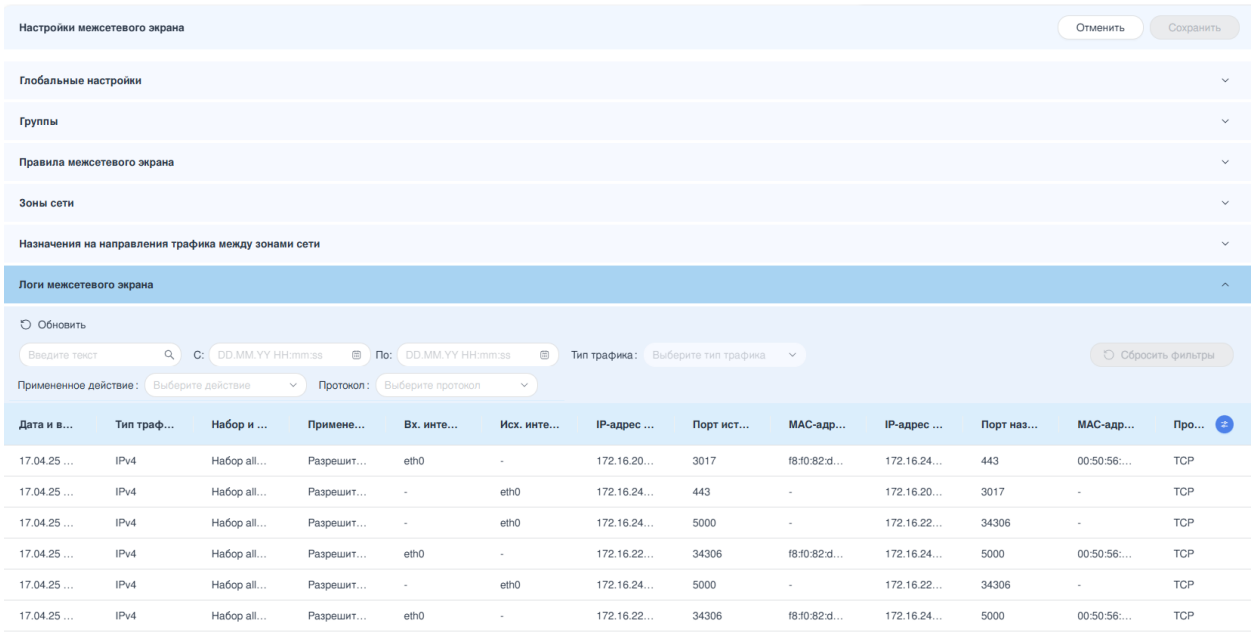


Рисунок – Журнал событий МЭ

Подраздел меню позволяет просматривать события в формате таблицы, состоящей из следующих столбцов:

- **«Дата и время»** - временная метка события, соответствующая моменту срабатывания правила.
- **«Тип трафика»** - версия IP-протокола: IPv4 или IPv6.

- **«Набор и правило»** - содержит наименование набора правил и приоритетного номера правила, которые были использованы для создания соответствующей записи. В случае отсутствия приоритетного номера правила, запись формируется на основе действия, назначенного по умолчанию для указанного набора правил.
- **«Примененное действие»** - действие, применённое к пакету данных.
- **«Вх. интерфейс»** - наименование сетевого интерфейса, через который был получен пакет. При наличии настроенных политик зон дополнительно указывается принадлежность интерфейса к определённой зоне.
- **«Исх. интерфейс»** - наименование сетевого интерфейса, через который был отправлен пакет. При наличии настроенных политик зон дополнительно указывается принадлежность интерфейса к определённой зоне.
- **«IP-адрес источника»** - IP-адрес хоста, являющегося отправителем пакета.
- **«Порт источника»** - номер порта отправителя пакета.
- **«MAC-адрес источника»** - MAC-адрес сетевого интерфейса отправителя.
- **«IP-адрес назначения»** - IP-адрес хоста, являющегося получателем пакета.
- **«Порт назначения»** - номер порта получателя пакета
- **«MAC-адрес назначения»** - MAC-адрес сетевого интерфейса получателя.
- **«Протокол»** - протокол, в контексте которого было применено правило обработки пакета.

Подраздел меню позволяет настроить отображение столбцов таблицы. Для настройки отображения столбцов необходимо нажать **кнопку «Настройка столбцов»**  и выбрать в выпадающем списке необходимые столбцы. По умолчанию в таблице отображаются все столбцы.

Обновление списка событий может выполняться двумя способами:

- **вручную**, с помощью соответствующей кнопки на панели инструментов таблицы;
- **автоматически**, с установленной периодичностью — 1 раз в 10 секунд.

При включении режима автоматического обновления ручное обновление становится недоступным. Кнопки управления обновлением находятся на панели инструментов таблицы **«Журнал»** (см. Рисунок – Обновление списка событий).

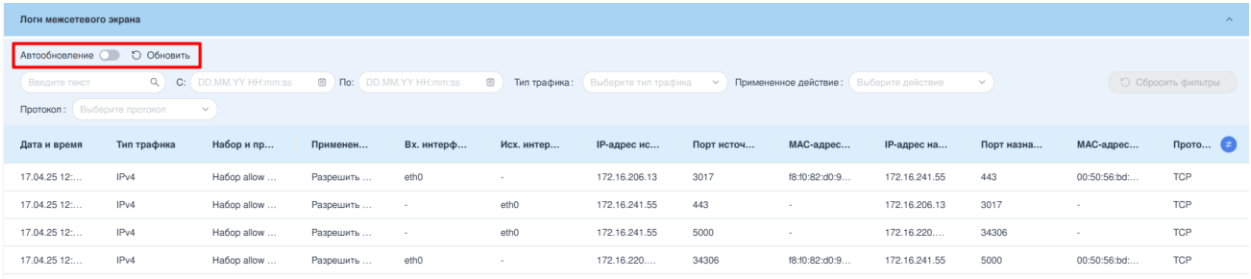


Рисунок – Обновление списка событий

Примечание:

В веб-интерфейсе установлено ограничение на выгрузку событий журнала **МЭ** — не более 10 000 записей.

6.5.1 Просмотр детализированной информации о событии

Для получения подробной информации о выбранном событии **МЭ** необходимо в таблице **«Логи межсетевого экрана»** нажать **ЛКН** на строке , соответствующей данному событию. После нажатия откроется боковое окно **«Запись лога»**, содержащее развёрнутую информацию о событии (см. Рисунок – Просмотр детализированной информации о событии).

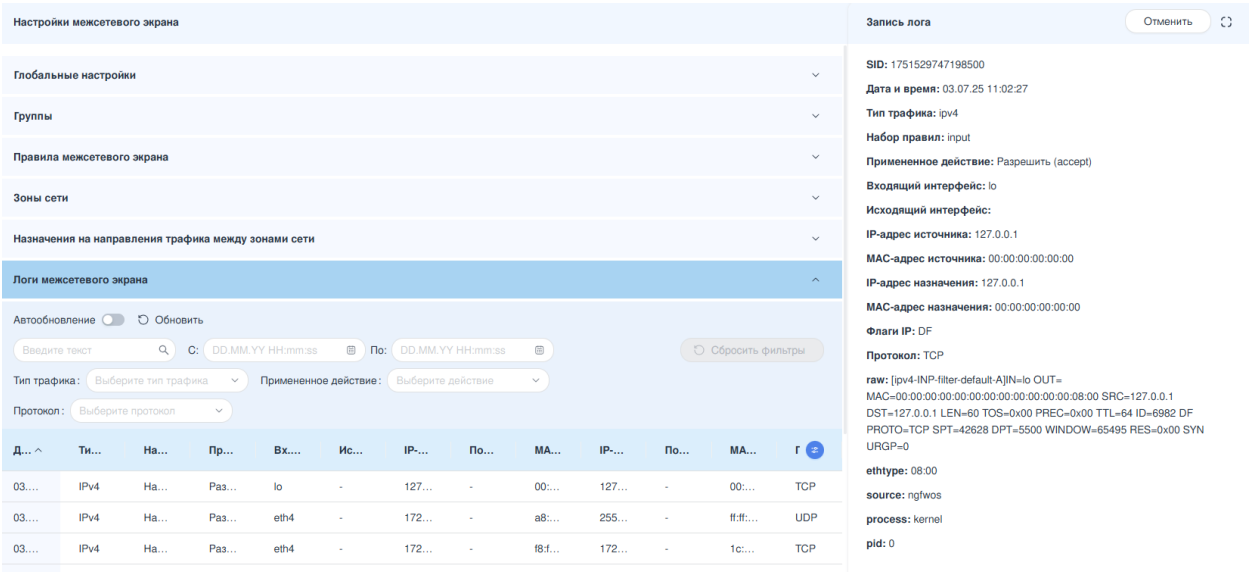


Рисунок – Просмотр детализированной информации о событии

6.5.2 Поиск и фильтрация

Блок фильтрации предназначен для отбора событий **МЭ** в соответствии с заданными пользователем критериями. По умолчанию блок фильтрации содержит следующие поля (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **«С»**;
- **«По»**;

- **«Тип трафика»**;
- **«Примененное действие»**;
- **«Протокол»**;
- **кнопка «Сбросить фильтры»»**.

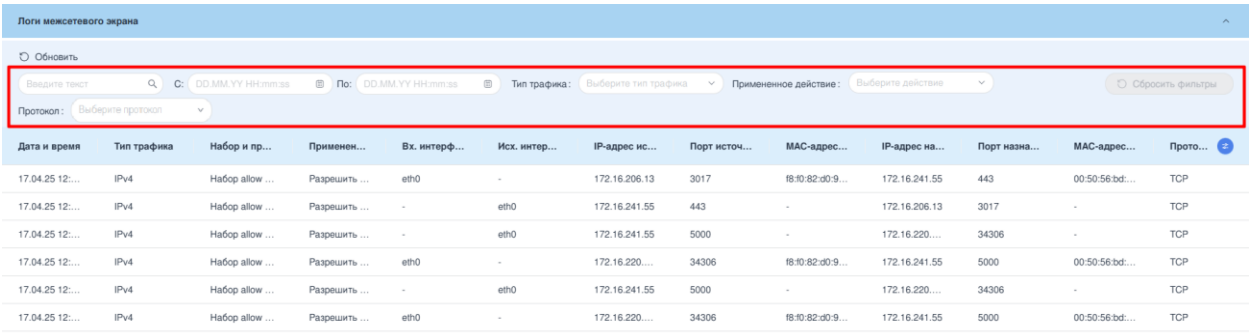


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем столбцам таблицы. Регистр вводимых символов учитывается при выполнении поиска.

Фильтрация по полю **«С»** позволяет отфильтровать записи по дате и времени события и задаёт начальный временной диапазон. После ввода даты и времени в таблице отобразятся лишь те события, где «Дата и время» совпадает или больше введённых в фильтр.

Фильтрация по полю **«По»** позволяет отфильтровать записи по дате и времени события и задаёт конечный временной диапазон. После ввода даты и времени в таблице отобразятся лишь те события, где «Дата и время» совпадает или меньше введённых в фильтр.

Фильтрация по полю **«Тип трафика»** позволяет отфильтровать записи событий **МЭ** по версии IP-протокола.

Фильтрация по полю **«Примененное действие»** позволяет отфильтровать записи событий **МЭ** по виду действия, применённого к пакету данных.

Фильтрация по полю **«Протокол»** позволяет отфильтровать записи событий **МЭ** по протоколу, в контексте которого было применено правило обработки пакета.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

Примечание:

Сбор логов осуществляется в обратном порядке, начиная с самых новых записей. При наличии фильтра по дате и времени, сбор логов производится начиная с указанного момента, до достижения заданного количества записей или максимального предела в 10 000 записей.

7 СОВ (IDS/IPS)

Функциональность системы обнаружения и предотвращения вторжений (**СОВ**) в **ARMA Стена** реализуется посредством ПО с открытым исходным кодом **«Suricata»** и использованием метода захвата пакетов **«NetMap»** для повышения производительности и минимизации загрузки ЦП.

Система обнаружения и предотвращения вторжений в **ARMA Стена** позволяет решать следующие задачи:

- обнаружение и предотвращение использования эксплойтов и уязвимостей сетевых приложений;
- обнаружение и предотвращение эксплуатации уязвимостей в поддерживаемых протоколах;
- обнаружение и предотвращение сетевого сканирования;
- обнаружение и фильтрация трафика от скомпрометированных хостов;
- обнаружение и фильтрация трафика от хостов, заражённых троянским ПО и сетевыми червями;
- обнаружение и предотвращение DOS-атак.

Для перехода в раздел **«СОВ»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«СОВ»** (см. Рисунок – СОВ (IDS/IPS)).

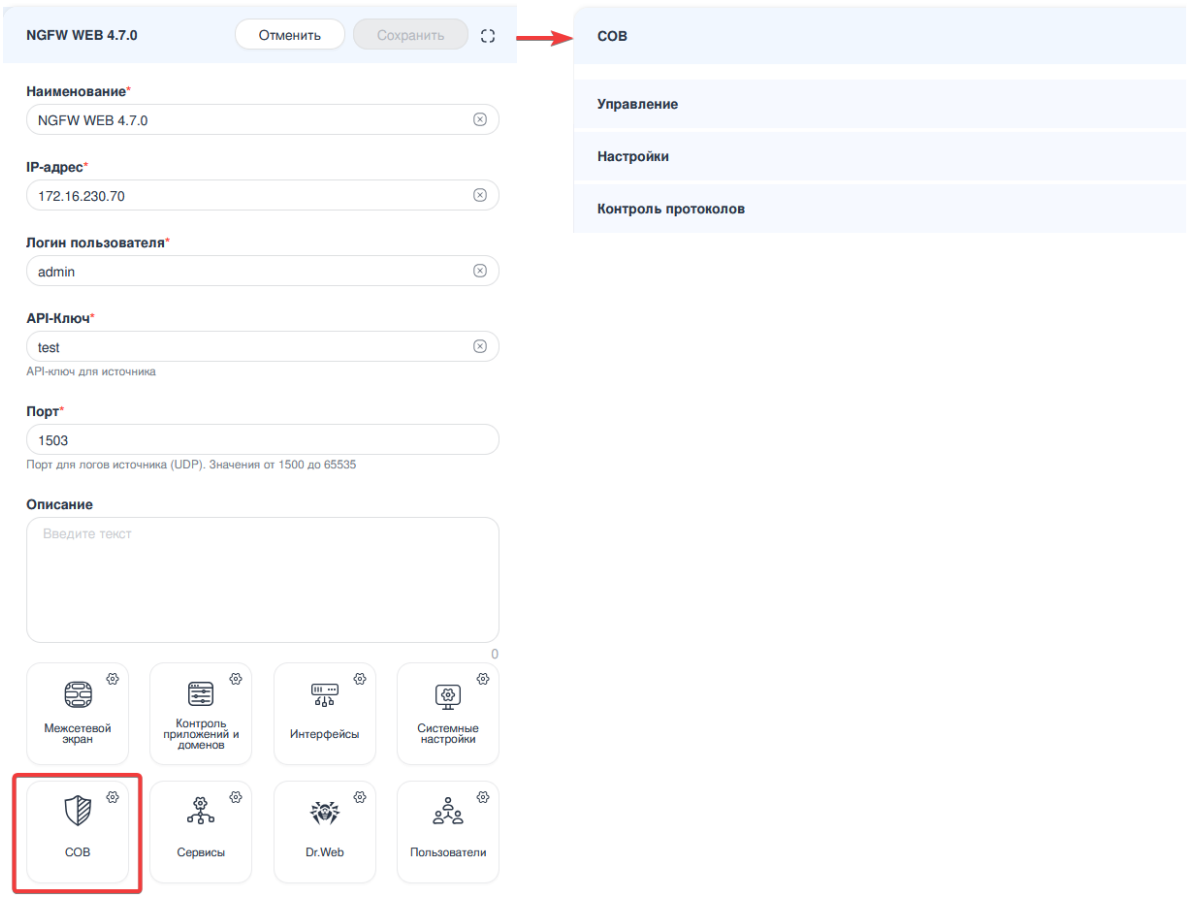


Рисунок – СОВ (IDS/IPS)

Применение и сохранение конфигурации СОВ (IDS/IPS)

После завершения настройки всех необходимых параметров в подразделах раздела **«СОВ»** необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«СОВ»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

Только после успешного подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

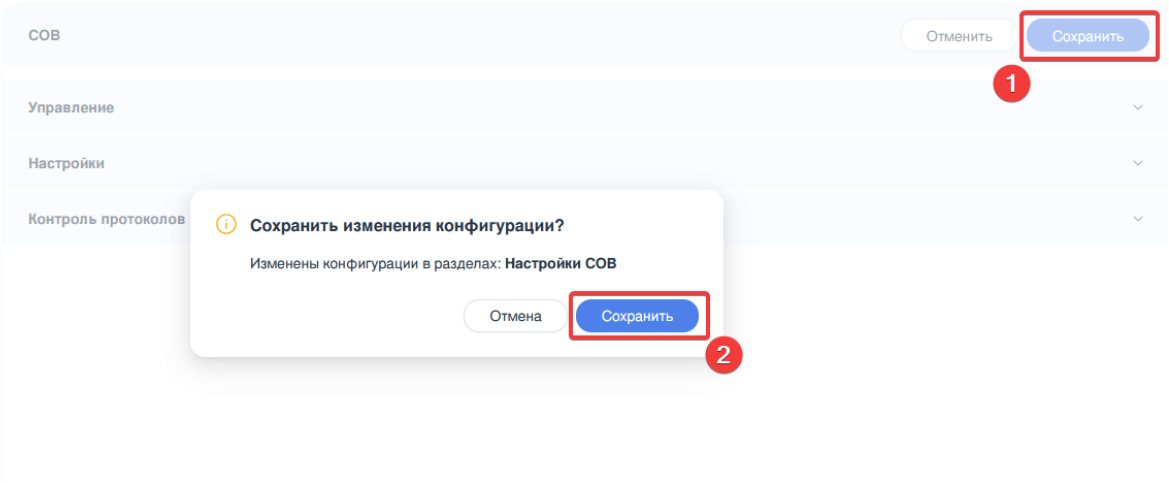


Рисунок – Применение и сохранение настроек

Примечание:

Если доступ к веб-интерфейсу осуществляется через сетевой интерфейс, на котором Suricata включена в режиме IPS, сохранение конфигурации СОВ приводит к кратковременному разрыву активных сетевых сессий на этом интерфейсе. В результате текущая сессия пользователя в веб-интерфейсе может быть прервана, и в браузере отобразится сообщение об ошибке. При этом все внесённые настройки сохраняются корректно. Для отображения обновлённой конфигурации необходимо обновить страницу вручную.

7.1 Настройки СОВ

Настройка СОВ осуществляется в подразделе **«Настройки»** меню **«СОВ»**. Данный раздел включает следующие блоки:

1. общие настройки;
2. настройки логирования;
3. источники обновлений правил;
4. настройки NetMap;
5. создание дампов трафика.

Примечание:

При работе Suricata в режиме IPS с использованием драйвера netmap перезагрузка конфигурации приводит к кратковременному разрыву активных сетевых сессий на интерфейсах, где включён IPS-режим.

Это обусловлено архитектурными особенностями IPS: Suricata располагается непосредственно на пути прохождения трафика на таких интерфейсах, обеспечивая его прямую обработку и пересылку. В ходе перезагрузки конфигурации сетевые интерфейсы с активированным IPS временно отключаются, передача трафика приостанавливается, а состояние активных

соединений (connection tracking) сбрасывается. В результате TCP- и UDP-сессии, проходящие через эти интерфейсы, могут быть прерваны.

В режиме IDS (TAB) Suricata анализирует лишь копию трафика и не участвует в его пересылке. Следовательно, перезагрузка конфигурации не оказывает влияния на стабильность сетевых соединений на интерфейсах, работающих в этом режиме.

В системах, где на отдельных интерфейсах включён IPS-режим, рекомендуется избегать частых перезагрузок Suricata. Обновление конфигурации следует выполнять в периоды минимальной сетевой нагрузки с целью минимизации воздействия на пользовательские сессии и критически важные сервисы, трафик которых проходит через указанные интерфейсы.

Обновление правил СОВ не приводит к перезапуску службы Suricata, однако инициирует внутреннюю перезагрузку правил в рамках работающего процесса. В момент перезагрузки правил возможна кратковременная несогласованность между текущим состоянием фильтрации и новым набором правил, что может повлиять на корректность обработки активных сессий. Рекомендуется учитывать этот фактор при планировании обновлений правил в высоконагруженных или критически важных сегментах сети.

7.1.1 Общие настройки

1. **Режим захвата** - выбрать режим захвата сетевого трафика для Suricata. Возможно указать следующие режимы:
    - **NetMap** - высокопроизводительный фреймворк для захвата и обработки сетевых пакетов, который минимизирует задержки и потери данных, обеспечивая максимальную эффективность на высокоскоростных сетях. Установлен по умолчанию.
    - **af-packet** - режим перехвата трафика в Suricata, который требует наличия нескольких сетевых интерфейсов и работает в режиме шлюза. Настройка данного режима недоступна через веб-интерфейс. Конфигурация режима осуществляется исключительно с использованием командной строки (CLI).
2. **Путь к файлам с правилами** - указать новый каталог, используемый по умолчанию для хранения правил Suricata. По умолчанию используется каталог **«/config/files/configuration/suricata/rule-files/»**. Максимальная длина — «255» символов. Не допускается использование символов «"» и «'».
3. **Файлы с правилами** - выпадающий список, позволяющий выбрать файлы с правилами, которые будут использоваться системой **Suricata** для анализа сетевого трафика и выявления потенциальных угроз. Список отображает только те файлы с расширением «.rules», которые находятся непосредственно в

каталоге, заданном в поле **«Путь к файлам с правилами»**. Возможно установить значение **«*.rules»**, при котором **Suricata** загружает все файлы с расширением «.rules» из каталога по умолчанию: **«/config/files/configuration/suricata/rule-files/»**. Файлы, расположенные в подкаталогах указанного пути, не учитываются.

Примечание:

При изменении каталога в поле **«Путь к файлам с правилами»** все ранее выбранные файлы, которые отсутствуют в новом указанном каталоге, будут выделены красным цветом. При этом отображается предупреждение о том, что данные файлы не будут использоваться системой **Suricata** (после её перезапуска), поскольку они не находятся в текущем каталоге.

В случае необходимости использования файла с правилами, находящегося в директории, отличной от текущей, возможно применить один из следующих методов:

1. Перенести требуемый файл в текущий каталог, указанный в поле **«Путь к файлам с правилами»**.
2. Задать полный путь к файлу посредством командной строки (CLI). Например:

```
admin@ngfwos# set suricata rule-files file-name /config/files/configuration/rule-files/test.rules
```

Во втором случае система выделит имя файла красным цветом, сигнализируя о его нахождении вне текущего каталога, однако **Suricata** будет корректно использовать данный файл для анализа сетевого трафика, так как указан полный путь к ресурсу (см. Рисунок – Файлы с правилами).

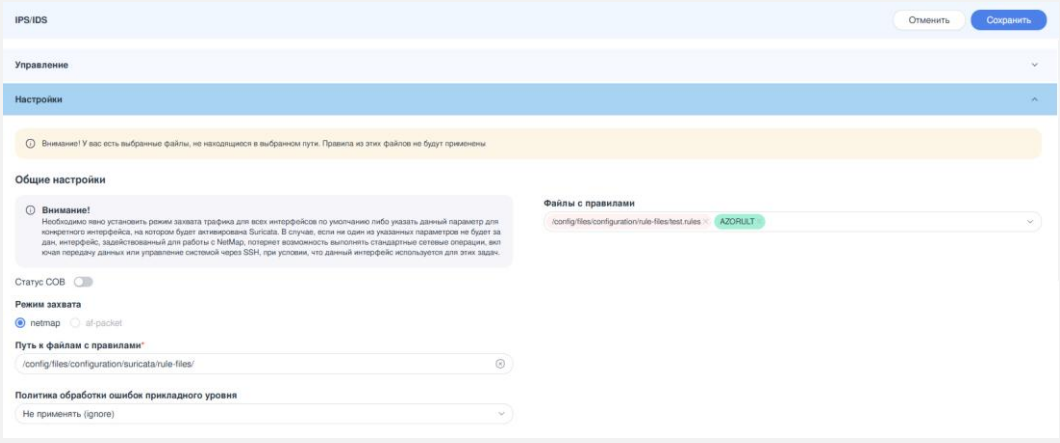


Рисунок – Файлы с правилами

4. **Политика обработки ошибок прикладного уровня** - выбрать политику обработки ошибок, возникающих на уровне приложений в Suricata. Возможно выбрать следующие политики:

- **Отбросить пакет (drop-packet)** - отбрасывает только текущий пакет, вызвавший ошибку.
- **Отбросить поток (drop-flow)** - отключает проверку для всего потока (flow), включая пакеты, полезную нагрузку и протоколы прикладного уровня. Отбрасывает текущий пакет и все последующие пакеты в этом потоке. Применяется в ситуациях, требующих обеспечения высокого уровня защиты и оперативного блокирования потенциально вредоносного трафика.
- **Отклонить (reject)** - аналогично drop-flow, но также отправляет TCP-сброс (RST) или ICMP-сообщение об ошибке для завершения соединения. Уведомляет участников соединения о блокировке.
- **В обход (bypass)** - обходит (игнорирует) весь поток, отключая дальнейшую проверку. Используется для минимизации влияния ошибок на производительность, но может снижать безопасность.
- **Пропустить пакет (pass-packet)** - отключает детектирование для текущего пакета, но продолжает обновление потока и анализ прикладного уровня (в зависимости от того, какая политика была активирована). Позволяет изолировать ошибку, не затрагивая остальной трафик.
- **Пропустить пакет (pass-flow)** - отключает проверку полезной нагрузки и пакетов, но продолжает выполнять сборку потока (stream reassembly), анализ прикладного уровня (app-layer parsing) и логирование.
- **Не применять (ignore)** - игнорировать ошибку в приложении и продолжать обработку данных. Значение используется по умолчанию.

7.1.2 Настройки логирования

1. **Уровень журналирования системных событий** - выбор уровня ведения журнала. Возможно выбрать следующие значения:
   - **«Ошибка (error)»** - уровень ошибок, которые могут оказать влияние на работу системы;
   - **«Предупреждение (warning)»** - уровень предупреждений о потенциальных проблемах;
   - **«Уведомление (notice)»** - уровень для общих уведомлений о важных событиях;
   - **«Инфо (info)»** - уровень для информационных сообщений;
   - **«Производительность (perf)»** - уровень для сообщений и событий, связанных с производительностью и работой системы Suricata;

- **«Конфигурирование (config)»** - уровень конфигурации Suricata;
- **«Отладка (debug)»** - уровень для отладочной информации.

По умолчанию используется уровень «Уведомление (notice)».

2. **Syslog** - включить логирование системных событий работы **Suricata** в глобальный журнал системы **ARMA Стена**. По умолчанию логирование включено.
3. **Логирование срабатываний правил (syslog)** - включить логирование событий и предупреждений IDS/IPS в глобальный журнал системы ARMA Стена. По умолчанию запись событий и предупреждений IDS/IPS в глобальный журнал включена.

7.1.3 Настройки NetMap

В разделе **«Настройки NetMap»** осуществляется конфигурация параметров захвата сетевого трафика с использованием высокопроизводительного метода **NetMap** в системе **Suricata**. Доступны настройки драйвера, режимов работы (IDS/IPS), политик исключений, проверки контрольных сумм и параметров параллельной обработки (см. Рисунок – Настройки NetMap):

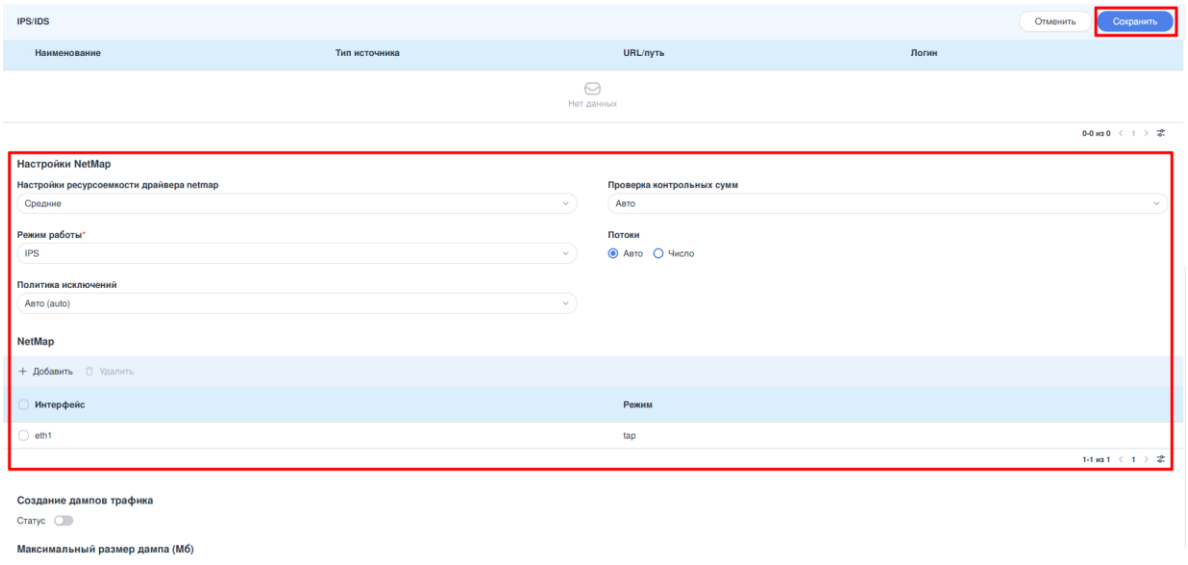


Рисунок – Настройки NetMap

1. **Настройки ресурсоемкости драйвера NetMap** - позволяет задать параметры драйвера сетевой карты при использовании технологии **NetMap**. Определяет баланс между производительностью и потреблением аппаратных ресурсов. Возможно выбрать следующие значения:
   - **экономичные** - подходит для сетей с низкой нагрузкой или ограниченными ресурсами оборудования. Минимизирует использование оперативной памяти и CPU:
     - **if_num = 100** - количество интерфейсов, которые могут быть обработаны одновременно;

- **buf_num = 163840** - общее количество буферов для хранения пакетов;
- **if_size = 1024** -размер кольцевого буфера (ring buffer) для каждого интерфейса.

- **средние** (по умолчанию)- оптимальное решение для большинства сценариев, особенно при использовании сетей средней пропускной способности (до 10 Гбит/с):
  - **if_num = 500** - увеличенное количество интерфейсов для обработки большего числа потоков данных;
  - **buf_num = 491520** - увеличение объёма буферов для временного хранения пакетов;
  - **if_size = 2048** -увеличенный размер кольцевого буфера для каждого интерфейса, снижая вероятность потери пакетов.
- **высокие** - рекомендовано для использования в высокоскоростных сетях со скоростью передачи данных 10 Гбит/с и выше, где требуется максимальная пропускная способность и минимальные потери данных:
  - **if_num = 1000** - максимальное количество интерфейсов, которые могут быть обработаны одновременно;
  - **buf_num = 983040** - увеличение объёма буферов для минимизации потерь пакетов при высокой нагрузке;
  - **if_size = 4096** -максимальный размер кольцевого буфера, обеспечивающий минимальные задержки и максимальную пропускную способность.

2. **Режим работы** - позволяет выбрать режим захвата трафика по умолчанию для сетевых интерфейсов, на которых режим не задан в явном виде, но активирована служба **Suricata**. Возможно выбрать следующие режимы:
   - **IDS** - пассивный режим анализа трафика. Обнаруженные инциденты регистрируются без вмешательства в поток данных.
   - **IPS** - активный режим. Система может блокировать или модифицировать трафик в реальном времени для предотвращения атак.
3. **Политика исключений** - глобальная конфигурация действий с пакетами и потоками, возникающими в процессе работы **Suricata** (нехватка памяти, неподдерживаемый протокол, разрыв соединения и т.д.). Может быть переопределена локальными настройками политики. Параметр доступен для редактирования только после выбора режима работы NetMap. Возможно выбрать следующие политики:

- **Авто (auto)**;
- **Отбросить пакет (drop-packet)**;
- **Отбросить поток (drop-flow)**;
- **Отклонить (reject)**;
- **В обход (bypass)**;
- **Пропустить пакет (pass-packet)**;
- **Пропустить пакет (pass-flow)**;
- **Не применять (ignore)**.

По умолчанию для режима NetMap **«IDS»** применяется политика исключений **«Не применять (ignore)»**, а для режима NetMap **«IPS»** — **«Авто (auto)»**.

4. **Проверка контрольных сумм** - определяет необходимость проверки контрольных сумм TCP/IP-пакетов при обработке трафика. Возможно указать следующие значения:
   - **Включена** - включает проверку контрольных сумм (надёжность, но ниже производительность). Проверка контрольных сумм TCP-пакетов оказывает значительное влияние на производительность системы;
   - **Выключена** - отключает проверку (высокая производительность, но возможны ошибки);
   - **Авто** - автоматический выбор, основанный на конфигурации системы и аппаратного обеспечения. Используется по умолчанию.
5. **Потоки** - указать количество потоков, используемых **Suricata** для обработки трафика. Возможно выбрать значение «auto» или «Число». По умолчанию используется значение «auto». При выборе значения «Число», появится дополнительное поле «Число потоков». В это поле возможно ввести количество потоков в диапазоне от «1» до «9999». Рекомендуется устанавливать значение, равное числу RSS-очередей на интерфейсе. Несоответствие указанного числа фактическому может привести к нестабильной работе Suricata.

Таблица **«NetMap»** содержит список сетевых интерфейсов, на которых активирован захват пакетов с использованием **NetMap**, а также указан режим захвата для каждого из интерфейсов.

Для включения захват пакетов с помощью **NetMap** на определённом интерфейсе необходимо выполнить следующие действия:

1. Нажать **кнопку «+ Добавить»** на панели инструментов таблицы **«NetMap»**.
2. В открывшемся окне **«Добавить Netmap»** указать следующие параметры:

- **Интерфейс** - выбрать из выпадающего списка необходимый сетевой интерфейс системы **ARMA Стена**, на котором будет осуществляться фильтрация трафика с помощью **Suricata**.
- **Режим работы** - укажите режим работы **Suricata** для данного интерфейса.

> **Примечание:**
>
> Если поле **«Режим работы»** оставлено незаполненным, система автоматически применит режим, заданный по умолчанию в общих настройках **СОВ**.
>
> Необходимо явно указывать режим захвата трафика либо глобально (в общих настройках), либо для каждого конкретного интерфейса, на котором активирована Suricata.

3. Нажать **кнопку «Добавить»** для сохранения параметров (см. Рисунок – Добавление сетевого интерфейса в СОВ).

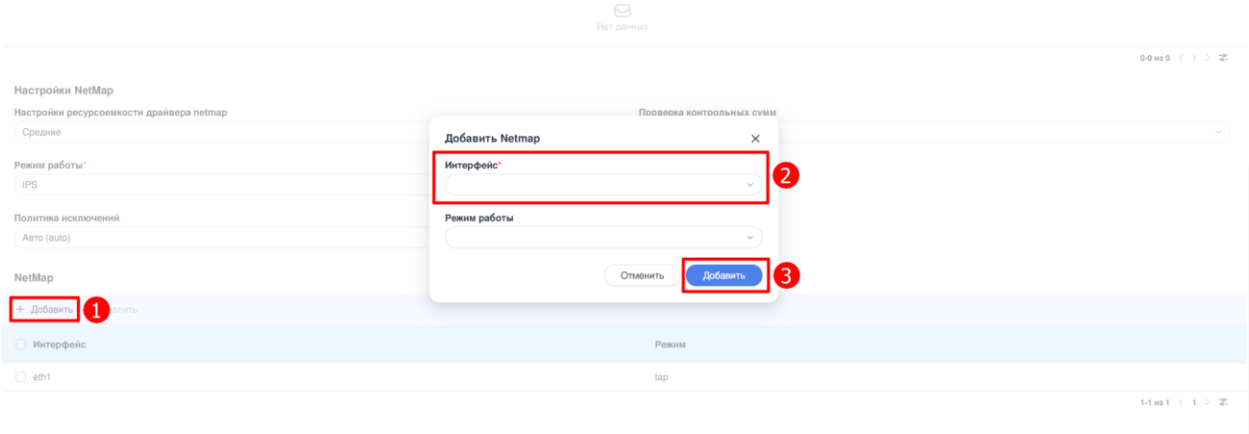


Рисунок – Добавление сетевого интерфейса в СОВ

После добавления интерфейс отобразится в таблице **«NetMap»** с указанием назначенного режима работы. Захват трафика начнётся немедленно при условии, что служба **СОВ** активна.

Для применения настроек **NetMap** необходимо нажать **кнопку «Сохранить»** в верхнем правом углу заголовка раздела **«IPS/IDS»**, а затем подтвердите действие в открывшемся окне **«Сохранить изменения конфигурации»**, нажав **кнопку «Сохранить»**.

7.1.4 Создание дампов трафика

Создание дампа трафика в **Suricata** необходимо для анализа инцидентов, отладки правил и расследования угроз. Трафик записывается в файл формата **pcap**.

Для включения записи дампов трафика в файл формата **pcap** необходимо перевести переключатель **«Статус»** в активное состояние и нажать **кнопку «Сохранить»** (см. Рисунок – Включение записи дампов трафика в файл).

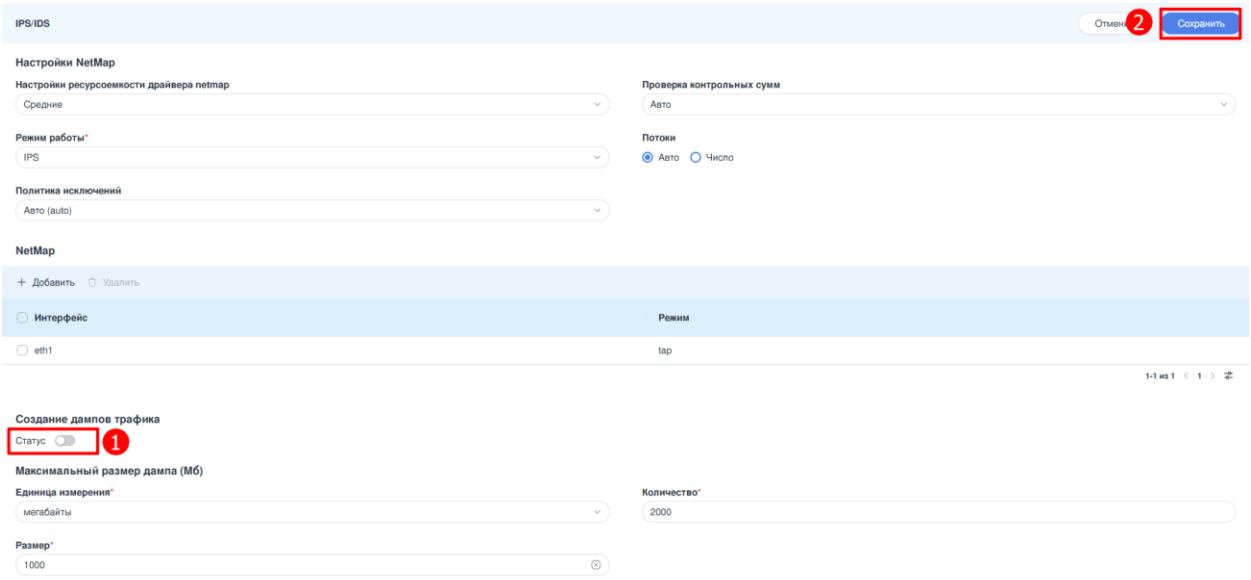


Рисунок – Включение записи дампов трафика в файл

Примечание:

Дамп сетевого трафика будет записываться в файл **«log.pcap»**, который создаётся при включении функции записи в каталоге **/var/log/suricata/**.

Блок настроек **«Максимальный размер дампа (Мб)»** предназначен для ограничения объёма записываемых дампов трафика с целью предотвращения переполнения накопителей данных. Блок включает следующие параметры:

1. **Единица измерения** - позволяет задать единицу измерения размера одного файла **pcap**. Возможно выбрать следующие значения:
   - **байты**;
   - **килобайты**;
   - **мегабайты** - используется по умолчанию;
   - **гигабайты**.
2. **Размер** - определяет максимальный объём одного файла **pcap** в указанной единице измерения. Возможно указать следующие значения в зависимости от единицы измерения:
   - от «0» до «18446744073709553664» - в байтах;
   - от «0» до «18014398509481986» - в килобайтах;
   - от «0» до «17592186044416» - в мегабайтах;
   - от «0» до «17179869184» - в гигабайтах.

   По умолчанию размер одного файла **pcap** установлен равным *1000 мегабайтах*.

3. **Количество** - указывает максимальное количество файлов **pcap**, которые могут быть созданы для одного потока. Возможно указать значение в диапазоне от «1» до «4294967295». По умолчанию используется значение «2000».

Для сохранения внесённых изменений необходимо нажать **кнопку «Сохранить»**, расположенную в верхнем правом углу заголовка раздела **«IPS/IDS»** (см. Рисунок – Включение записи дампов трафика в файл).

Примечание:

Блок настроек **«Максимальный размер дампа (Мб)»** применяются на каждый отдельный поток. Таким образом, ограничение объёма для восьми потоков с 2000 файлами с размером 1000 мегабайт каждый составит 16 терабайт.

7.2 Включение СОВ

Для обеспечения корректной работы **СОВ** необходимо выполнить следующие минимальные настройки **Suricata**:

1. указать интерфейс, на котором будет включён захват пакетов;
2. определить режим захвата, который будет применяться по умолчанию для всех интерфейсов системы **ARMA Стена**;
3. указать файл с правилами Suricata.

Для включения **СОВ** после выполнения минимальных настроек **Suricata**, необходимо перевести переключатель **«Статус СОВ»** в активное состояние и нажать **кнопку «Сохранить»** (см. Рисунок – Включение СОВ).

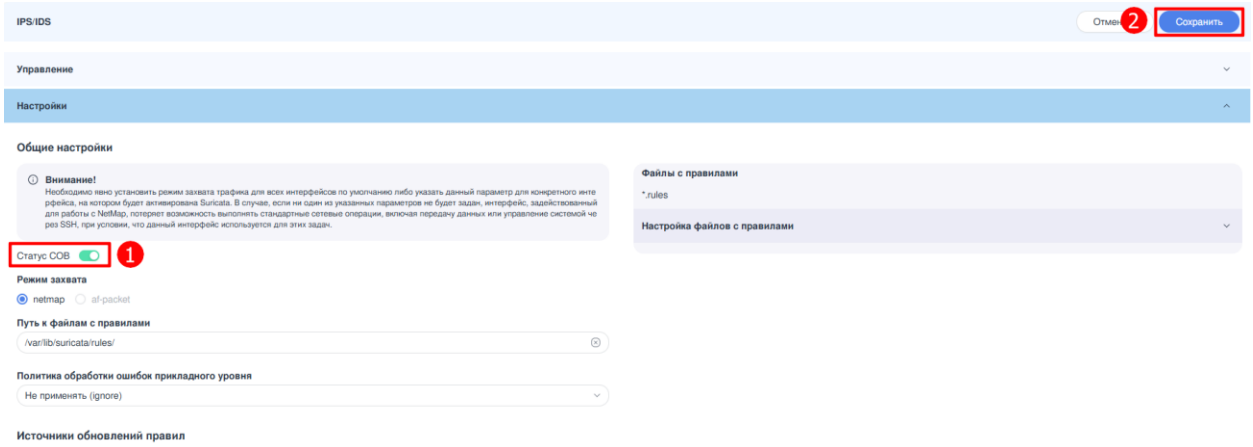


Рисунок – Включение СОВ

7.3 Правила СОВ

7.3.1 Создание пользовательских правил СОВ

Для создание пользовательского правила **СОВ** необходимо перейти в раздел **«Управление»** меню **«СОВ»** и нажать **кнопку «Добавить правило»**. В появившейся форме требуется заполнить следующие поля:

- **Путь к файлу** - указывается полное имя файла, в который будет сохранено правило. По умолчанию предлагается размещение в каталоге **/config/files/configuration/suricata/rule-files/**. Изменение пути не рекомендуется, поскольку при обновлении программного обеспечения файлы, находящиеся вне директории **config**, будут утеряны. Если указанный файл отсутствует в целевом каталоге, он будет создан автоматически при сохранении правила. При наличии файла с таким именем новое правило добавляется в конец существующего содержимого.

  Примечание:

  Файл, содержащий пользовательские правила, должен быть прописан в настройках **Suricata** в параметре **«Файлы с правилами»** раздела **«Настройки»** меню **«СОВ»**. В случае отсутствия этой конфигурации, несмотря на успешное сохранение правил в системе, они не будут применяться при анализе сетевого трафика.

- **SID** - уникальный идентификатор правила. Для оптимизации процесса рекомендуется оставить данное поле незаполненным, что позволит системе автоматически назначить свободный **SID**. В случае ручного ввода **SID** необходимо обеспечить его уникальность в пределах текущего файла правил. Несоблюдение данного требования приведет к возникновению ошибки при сохранении: *«Error: Rules added with some conflicts. DUPLICATED_SIDS: [1]»* — правило не будет добавлено. Также следует избегать использования **SID**, которые уже применяются в других файлах правил, поскольку это может привести к некорректной работе системы. При загрузке правил **Suricata** игнорирует дублирующиеся **SID**, что может привести к тому, что правило будет сохранено, но не будет участвовать в фильтрации трафика.
- **Сигнатура** - текст правила, соответствующий синтаксису **Suricata**. Требуется строгое соблюдение формата. Любое отклонение от синтаксиса (например, пропущенная точка с запятой, неверная последовательность опций или некорректные ссылки на переменные) приводит к ошибке валидации, и правило не будет сохранено.

После заполнения всех обязательных полей необходимо подтвердить ввод, нажав **кнопку «Сохранить»** (см. Рисунок – Создание пользовательских правил СОВ).

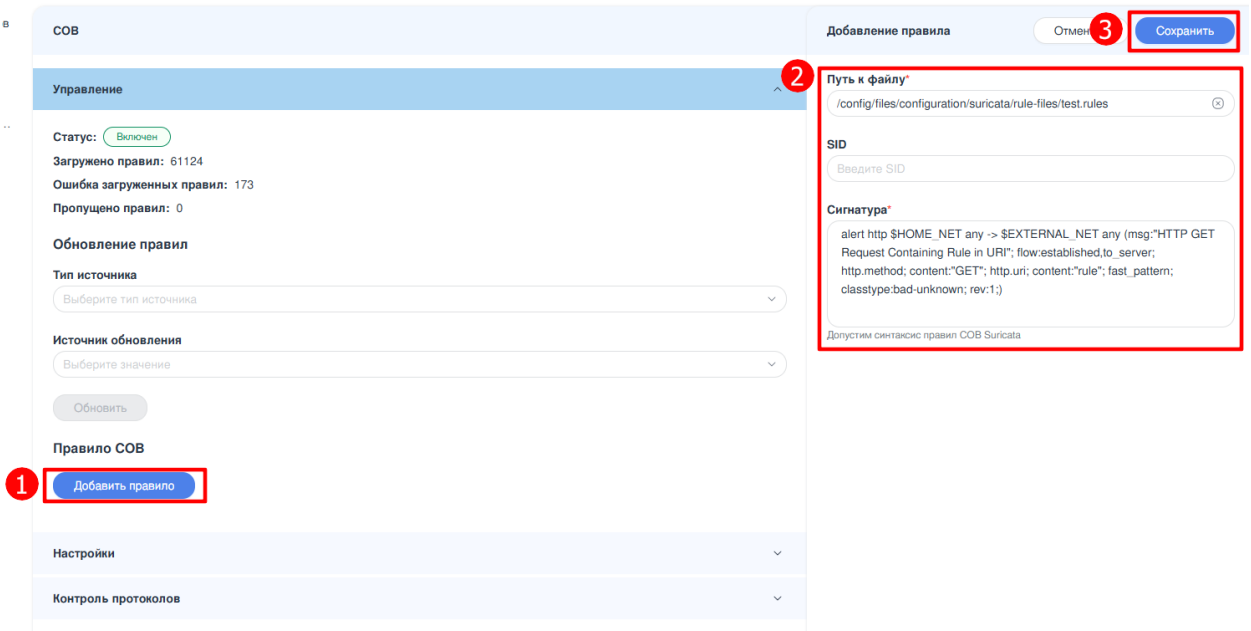


Рисунок – Создание пользовательских правил СОВ

При активированной службе **СОВ** после сохранения правила выполняется перезагрузка правил **Suricata** без полного перезапуска службы. Новое правило становится доступным для анализа трафика немедленно.

Примечание:

Существует вероятность неполного применения правил системы **Suricata** к процессу активной фильтрации сетевого трафика в момент перезапуска правил.

Если служба **СОВ** отключена, правило сохраняется в файловой системе, но применяется только после включения службы.

Переменные в правилах СОВ

В системе **ARMA Стена** предусмотрена возможность использования переменных при работе с правилами **СОВ**, на основе **Suricata**. Эта функциональность позволяет гибко задавать диапазоны IP-адресов, на которые распространяются правила, исключая необходимость вручную указывать адреса в каждом правиле. Это способствует повышению эффективности фильтрации сетевого трафика и оптимизации процесса управления безопасностью.

Переменные используются в правилах **Suricata** для указания источников, назначений и зон анализа (например, внутренние сети, внешние хосты). Это обеспечивает масштабируемость конфигурации и снижает нагрузку на систему за счёт ограничения области действия правил только релевантными сетевыми сегментами.

На текущий момент в **ARMA Стена** поддерживаются две основные переменные:

- **HOME_NET** - определяет доверенную внутреннюю сеть организации. Правила, ссылающиеся на **HOME_NET**, будут применяться только к трафику, проходящему через указанные подсети. Допустимые значения: IPv4-адреса и сети в формате CIDR, перечисленные через запятую; допускается использование специальных символов. Для задания значений переменных разрешены: цифры (0–9), буквы латинского алфавита (a–z, A–Z), специальные символы «/», «$», «!», «,», «.». Значение по умолчанию «192.168.0.0/16,10.0.0.0/8,172.16.0.0/12».
- **EXTERNAL_NET** - задаёт внешние сети, находящиеся за пределами доверенной зоны. Для задания значений переменных разрешены: цифры (0–9), буквы латинского алфавита (a–z, A–Z), специальные символы «/», «$», «!», «,», «.». Значение по умолчанию «!$HOME_NET» - все IP-адреса, кроме тех, что входят в **HOME_NET**.

Для изменения значений переменных необходимо перейти в раздел **«Настройки»** меню **«СОВ»**, где в блоке **«Переменные»** следует указать требуемые параметры (см. Рисунок – Переменные группы адресов). После ввода значений конфигурация сохраняется нажатием **кнопки «Сохранить»**, расположенной в правом верхнем углу заголовка раздела **«СОВ»**.

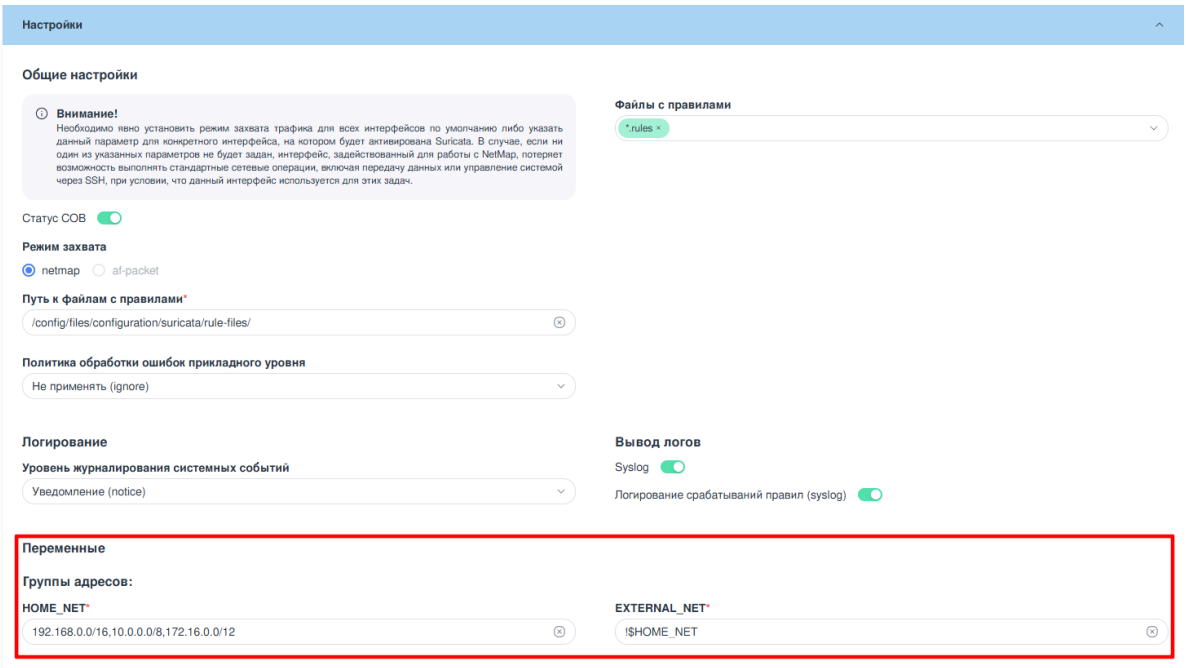


Рисунок – Переменные группы адресов

Изменения в переменных затрагивают все правила — как стандартные, так и пользовательские, — в которых используются ссылки на **HOME_NET** и **EXTERNAL_NET**.

7.3.2 Обновление правил СОВ

Для обеспечения высокой степени защиты сети система **ARMA Стена** поддерживает обновление правил Suricata. Обновления правил могут осуществляться из

локальных и внешних источников, что обеспечивает гибкость настройки в зависимости от условий эксплуатации — как в изолированных сетях, так и в средах с выходом во внешние сети.

7.3.2.1 Источники обновлений правил

Система **ARMA Стена** позволяет использовать два источника обновления правил **Suricata**:

- **локальный источник** - файлы с правилами, размещённые непосредственно на устройстве;
- **внешний источник** - удалённый ресурс, предоставляющий актуальные версии правил.

Локальный источник

Для добавления локального источника обновлений правил **Suricata** необходимо выполнить следующие действия (см. Рисунок – Добавление локального источника обновления правил):

1. Перейти в подраздел **«Настройки»** раздела **«IPS/IDS»**.
2. В таблице **«Источники обновлений правил»** нажать **кнопку «+ Добавить»** в панели инструментов.
3. В открывшемся боковом окне **«Источник обновлений правил»** выбрать создаваемую сущность **«Локальный»** и указать следующие параметры:
    - **Наименование** - пользовательское имя создаваемого локального источника обновлений правил. Значение не может содержать двойные («"») или одинарные («'») кавычки и знак вопроса («?»). Максимальная длина — «256» символов.
    - **Путь** - полный путь к файлу обновления с правилами **Suricata**, который расположен в системе **ARMA Стена**. Максимальная длина — «2000» символов.

      Для переноса файла обновления в систему **ARMA Стена** возможно использовать программное обеспечение, поддерживающее передачу файлов по протоколам SFTP или SCP (например, WinSCP для операционной системы Windows), либо воспользоваться командой «scp» через интерфейс командной строки. Возможны также альтернативные способы передачи данных.

      Пример использования команды «scp»:

```
«C:\Users\test>scp c:\Users\test\Desktop\user.rules
admin@172.16.20.76:/config/files/configuration/suricata/rule
-files/»
```

Команда выполнит копирование файла обновления правил СОВ «user.rules» в каталог «/config/files/configuration/suricata/rule-files/» на системе **ARMA Стена**, доступной по IP-адресу 172.16.20.105.

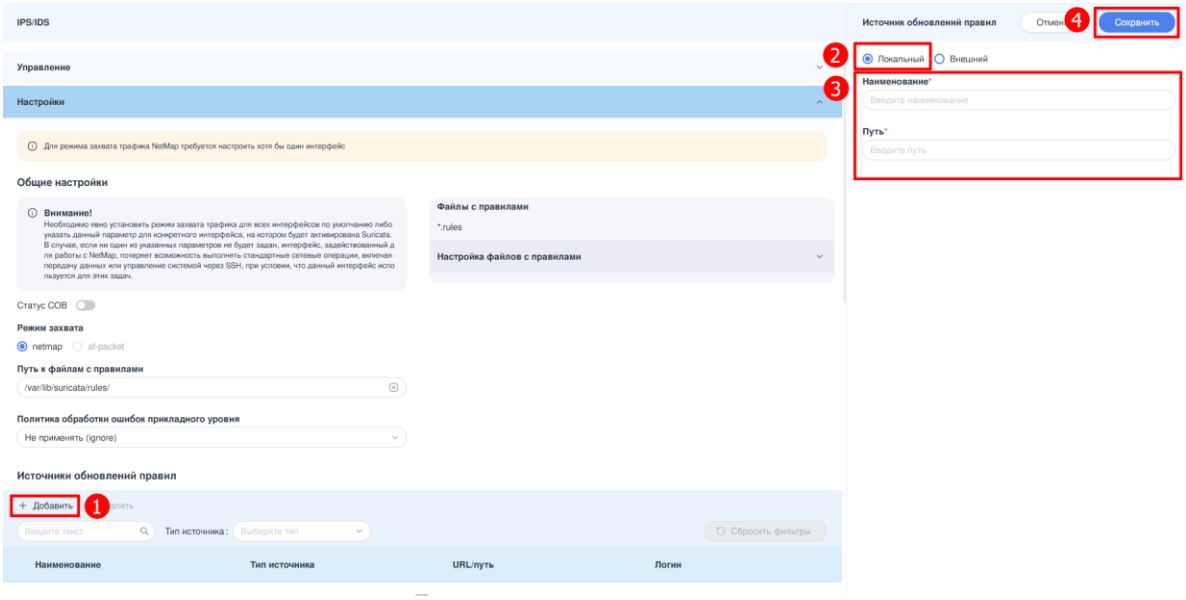


Рисунок – Добавление локального источника обновления правил

Внешний источник

Для добавления внешнего источника обновлений правил **Suricata** необходимо выполнить следующие действия (см. Рисунок – Добавление внешнего источника обновления правил):

1. Перейти в подраздел **«Настройки»** раздела **«IPS/IDS»**.
2. В таблице **«Источники обновлений правил»** нажать **кнопку «+ Добавить»** в панели инструментов.
3. В открывшемся боковом окне **«Источник обновлений правил»** выбрать создаваемую сущность **«Внешний»** и указать следующие параметры:
   - **Наименование** - пользовательское имя создаваемого источника обновлений правил. Значение не может содержать двойные («"») или одинарные («'») кавычки и знак вопроса («?»). Максимальная длина — «256» символов.
   - **URL** - URL-адрес внешнего источника обновлений правил. Значение не может содержать двойные («"») или одинарные («'») кавычки и знак вопроса («?»). По умолчанию поле

содержит URL-адрес сервера обновлений правил **Suricata** компании ООО **«ИнфоВотч АРМА»** - «https://update.iwarma.ru/ngfw/ids_ips». Максимальная длина — «2000» символов.

- **Логин** - имя УЗ, имеющей доступ к внешнему источнику обновлений правил. Значение не может содержать двойные («"») или одинарные («'») кавычки и знак вопроса («?»). Максимальная длина — «256» символов.
- **Пароль** - пароль УЗ. Значение не может содержать двойные («"») или одинарные («'») кавычки и знак вопроса («?»). Максимальная длина — «256» символов.

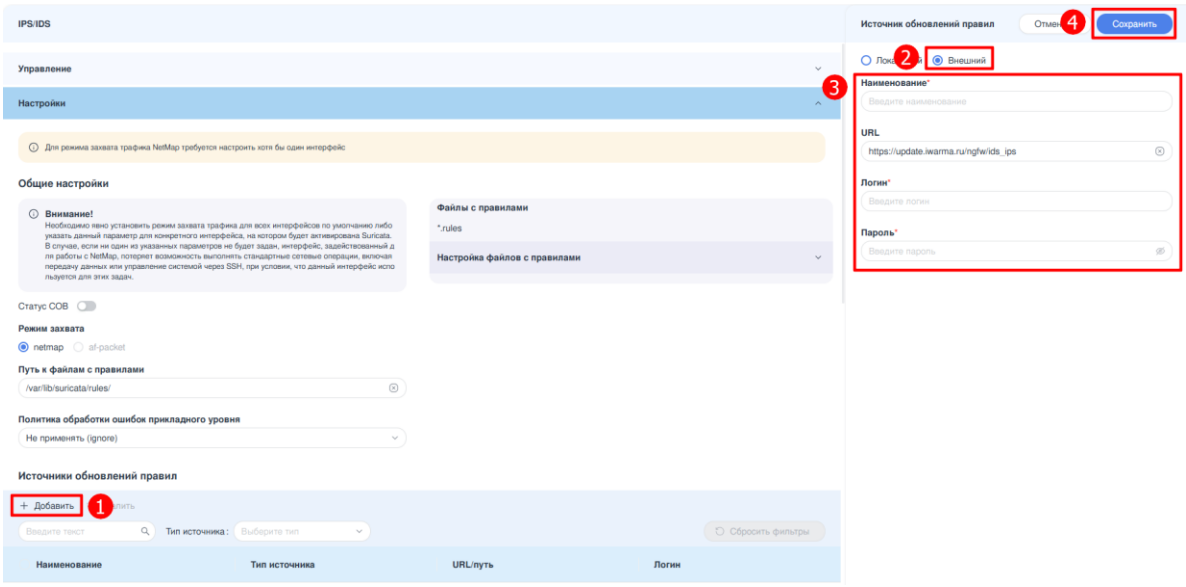


Рисунок – Добавление внешнего источника обновления правил

Для модификации источника обновлений правил следует осуществить выбор соответствующей записи в таблице **«Источники обновлений правил»** посредством нажатия **ЛКМ**. В открывшемся окне необходимо произвести требуемые изменения. Поле **«Наименование»** не подлежит редактированию. По завершении процесса модификации следует нажать **кнопку «Сохранить»**.

Для удаления источника обновлений правил необходимо выбрать одну или несколько соответствующих записей в таблице **«Источники обновлений правил»**, установив флажок в чек-боксе слева от наименования источника, и нажать **кнопку «Удалить»** на панели инструментов. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

7.3.2.2 Порядок выполнения обновления

1. Настроить источник обновления правил (см. Источники обновлений правил).
2. В разделе **«IPS/IDS»** перейти в подраздел **«Управление»**.

3. В поле **«Тип источника»** выбрать тип источника обновления внешний или локальный.
4. В поле **«Источник обновления»** выбрать из списка ранее настроенный источник, соответствующий указанному типу. При выборе значения **«все»** обновление будет выполнено со всех доступных источников данного типа.
5. Нажать **кнопку «Обновить»** (см. Рисунок – Обновление правил Suricata).

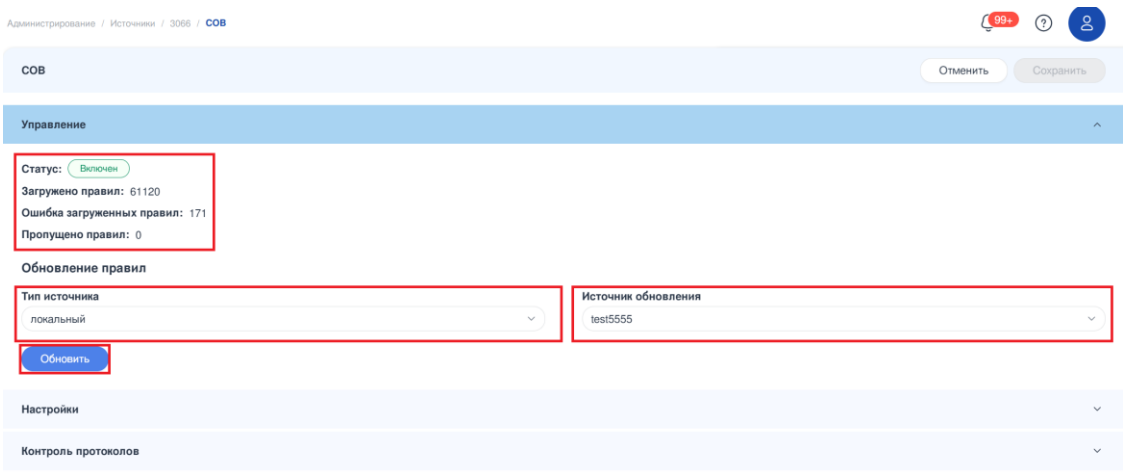


Рисунок – Обновление правил Suricata

Примечание:

Верхняя область окна, показанного на рисунке, отображает статус службы СОВ, количество загруженных правил, а также наличие ошибок и пропущенных правил. Эти данные автоматически обновятся после обновления правил.

6. По завершении процесса система отобразит информационное сообщение о результате выполненного обновления (см. Рисунок – Результат обновления правил Suricata).

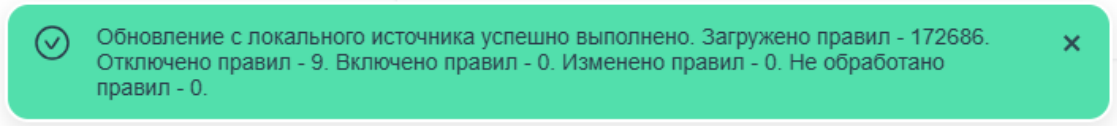


Рисунок – Результат обновления правил Suricata

7.4 Контроль протоколов

Функционал контроля протоколов в системе **ARMA Стена** основан на сигнатурном методе обнаружения и обеспечивает интеллектуальное распознавание сетевых протоколов в реальном времени. Обнаружение и классификация трафика осуществляются с использованием правил системы **Suricata**, что позволяет эффективно выявлять несанкционированное использование протоколов, а также потенциально вредоносную активность, связанную с ними.

Примечание:

Для работы правил фильтрации протоколов необходимо настроить и активировать службу **«СОВ»** (см. Включение СОВ).

Все правила контроля протоколов сохраняются в файл **/config/files/configuration/protocols/rule-files/protocols.rules**.

При добавлении новых правил, внесении изменений в существующие или при включении/отключении парсеров протоколов применение обновлённой конфигурации к процессу фильтрации трафика выполняется после нажатия **кнопки «Сохранить»** на панели инструментов раздела **«СОВ»** (см. Рисунок – Применение и сохранение настроек). Данное действие инициирует перезагрузку правил службы СОВ без полного перезапуска движка **Suricata**.

Примечание:

В момент перезагрузки правил существует вероятность неполного применения обновлённых правил к активному сетевому трафику.

7.4.1 Включение/отключение парсеров протоколов

Служба **СОВ** включает набор парсеров, отвечающих за анализ (декодирование) сетевых протоколов или форматов данных с целью извлечения структурированной информации. Эта информация используется механизмами обнаружения (на основе правил **Suricata**) для выявления аномалий и угроз.

Анализ трафика в **Suricata** реализован по многоуровневой архитектуре, соответствующей стеку сетевых протоколов:

- *Парсеры канального уровня (L2 / Decode Layer)* - обрабатывают заголовки канального уровня (Ethernet, 802.1Q VLAN, PPP, SLL и др.), извлекая MAC-адреса, теги.
- *Сетевые парсеры (L3 / IP Layer)* - анализируют заголовки IPv4, IPv6, ICMP, ICMPv6, GRE и обеспечивают дефрагментацию IP-пакетов.
- *Парсеры прикладного уровня (App-Layer)* - выполняют глубокий анализ (DPI) протоколов прикладного уровня (HTTP, TLS, DNS, SSH, Modbus, DNP3 и др.), реконструируют сессии и предоставляют структурированные метаданные для механизмов обнаружения.

Совместная работа этих уровней под управлением единого движка правил обеспечивает сквозную видимость трафика и эффективное обнаружение угроз на всех уровнях сетевого стека.

Для включения или отключения парсеров прикладного уровня необходимо выполнить следующие действия (см. Рисунок – Включение/отключение парсеров протоколов):

1. Перейти в раздел **«Контроль протоколов»** меню **«СОВ»**.
2. Установить или снять флажки напротив требуемых протоколов.
3. Нажать **кнопку «Сохранить»**.

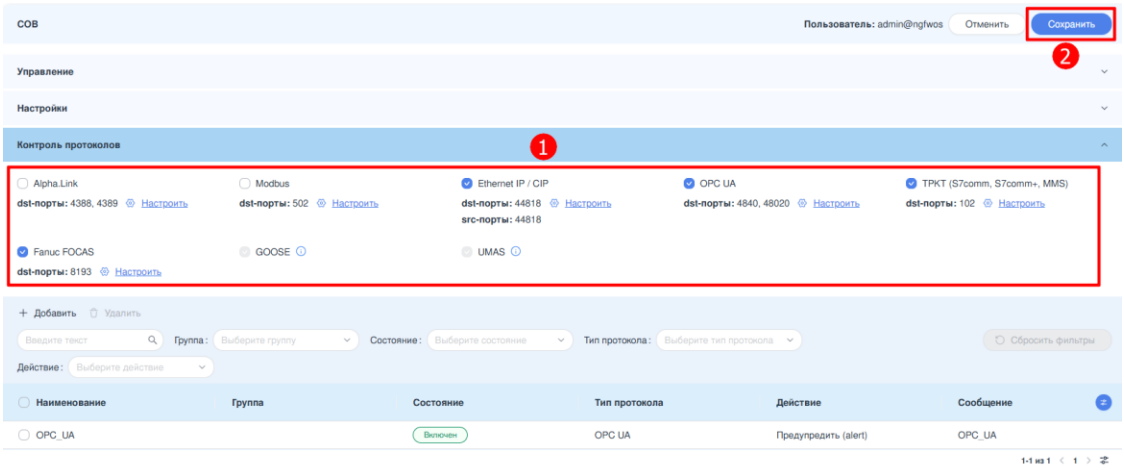


Рисунок – Включение/отключение парсеров протоколов

Парсеры канального и сетевого уровней всегда включены и не подлежат отключению.

Правила, относящиеся к отключённым протоколам, не применяются к анализу трафика. В журналах службы **СОВ** фиксируется сообщение о невозможности применения таких правил из-за отсутствия соответствующего парсера.

Система **ARMA Стена** поддерживает следующие парсеры протоколов:

- **ADS** - включён по умолчанию;
- **Alpha.Link** - отключён по умолчанию;
- **AoE (ADS over EtherCAT)** - включён;
- **Bittorrent-DHT** - включён по умолчанию;
- **DCERPC** - включён по умолчанию;
- **DHCP** - включён по умолчанию;
- **DNP3** - включён по умолчанию;
- **DNS** - включён по умолчанию;
- **ENIP/CIP** - включён по умолчанию;
- **EtherCAT** - включён;
- **Fanuc FOCAS** - включён по умолчанию;
- **FTP** - включён;
- **GOOSE** - включён;

- **HTTP** - включён по умолчанию;
- **HTTP2** - включён по умолчанию;
- **IEC 60870-5-104 (IEC-104)** - включён по умолчанию;
- **IKE** - включён по умолчанию;
- **IMAP** - включён по умолчанию;
- **KRB5** - включён по умолчанию;
- **KRUG** - включён;
- **Modbus** - отключён по умолчанию;
- **MQTT** - включён по умолчанию;
- **NFS** - включён по умолчанию;
- **NTP** - включён по умолчанию;
- **OPC DA (только L3/IP Layer)** - включён;
- **OPC UA** - включён по умолчанию;
- **PgSQL** - включён по умолчанию;
- **QUIC** - включён по умолчанию;
- **RDP** - включён по умолчанию;
- **RFB** - включён по умолчанию;
- **SIP** - включён по умолчанию;
- **SMB** - включён по умолчанию;
- **SMTP** - включён по умолчанию;
- **SNMP** - включён по умолчанию;
- **SSH** - включён по умолчанию;
- **Telnet** - включён по умолчанию;
- **TFTP** - включён по умолчанию;
- **TLS/SSL** - включён по умолчанию;
- **TPKT (S7COMM, S7COMM Plus, MMS)** - включён по умолчанию;
- **UMAS** - включён;
- **UNET 2** - отключён по умолчанию.

На текущий момент в веб-интерфейсе доступны функции включения/отключения парсеров и создания шаблонов правил только для следующих протоколов:

- **«Alpha.Link»**;
- **«Ethernet IP / CIP»**;
- **«Modbus»**;
- **«OPC UA»**;
- **«TPKT (S7COMM, S7COMM Plus, MMS)»**;
- **«GOOSE»**;
- **«UMAS»**;
- **«Fanuc FOCAS»**.

Поддержка остальных протоколов реализована исключительно через **CLI-интерфейс**. В последующих версиях системы планируется расширение функционала веб-интерфейса за счёт добавления шаблонов и управления для дополнительных парсеров.

7.4.2 Настройка портов для анализа протоколов

Для определённых парсеров протоколов в системе **ARMA Стена** по умолчанию заданы порты назначения (**dst-port**) и порты источника (**src-port**), используемые **Suricata** для идентификации трафика соответствующего протокола.

Изменение списка портов выполняется следующим образом:

1. В разделе **«Контроль протоколов»** нажать **кнопку «** **Настроить»**, расположенную под названием требуемого протокола.
2. В открывшемся боковом окне:
   - отредактировать существующий порт по умолчанию;
   - при необходимости добавить новый порт, нажав **кнопку «Добавить»** в соответствующем разделе:
     - **«dst-порты протокола <Имя протокола>»** — для портов назначения;
     - **«src-порты протокола <Имя протокола>»** — для портов источника (если поддерживается).
3. После внесения изменений нажать **кнопку «Изменить»** в боковом окне (см. Рисунок – Редактирование портов для анализа протоколов).
4. Для сохранения и применения обновлённой конфигурации нажать **кнопку «Сохранить»** на панели инструментов раздела **«СОВ»** (см. Рисунок – Применение и сохранение настроек).

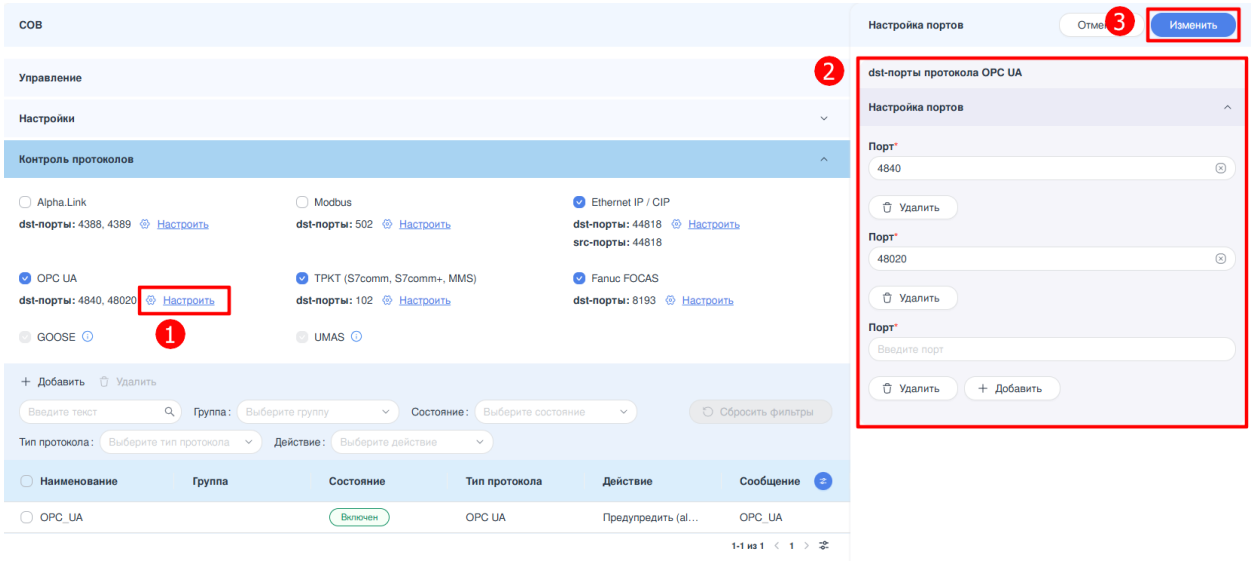


Рисунок – Редактирование портов для анализа протоколов

По умолчанию заданы следующие порты назначения (**dst-port**):

- **«Alpha.Link»** – «4388», «4389»;
- **«Ethernet IP / CIP»** – «44818»;
- **«Modbus»** – «502»;
- **«OPC UA»** – «53»;
- **«TPKT (S7comm, S7comm+, MMS)»** – «102»;
- **«Fanuc FOCAS»** – «8193».

По умолчанию задан следующий порт источника (**src-port**):

- **«Ethernet IP / CIP»** – «44818».

Указание дополнительных портов позволяет расширить охват анализа трафика в случаях, когда протокол используется на нестандартных портах.

7.4.3 Создание правил фильтрации протоколов на основе шаблонов

Для упрощения настройки правил фильтрации протоколов в системе **«ARMA Стена»** реализован механизм создания правил **СОВ** с использованием шаблонов.

Для создания правила на основе шаблона необходимо перейти в раздел **«Контроль протоколов»** меню **«СОВ»** и выполнить следующие действия (см. Рисунок – Создание правил СОВ на основе шаблонов протоколов):

1. Нажать **кнопку «Добавить»** на панели инструментов таблицы **«Контроль протоколов**.
2. В открывшемся окне **«Добавление правила»** заполнить следующие общие параметры:

- **Статус** - определяет активность правила. При значении «Включено» правило участвует в фильтрации трафика. По умолчанию правило создаётся с состоянием «Выключено».
- **Наименование** - уникальное имя правила, используемое для идентификации в таблице. Максимальная длина — «255» символов.
- **Группа** - название группы, к которой относится правило. Позволяет организовать правила в логические группы. Допускается выбор из существующего списка или ввод нового имени. Максимальная длина — «255» символов.
- **Тип протокола** - выбор протокола из доступного списка.
- **Действие** - действие, применяемое к пакету при срабатывании правила. Доступны следующие значения:
    - **«Предупредить (Alert)»** – генерация оповещения без блокировки пакета (значение по умолчанию);
    - **«Отклонить (Reject)»** – блокировка пакета с отправкой уведомления источнику;
    - **«Отбросить (Drop)»** – блокировка пакета без уведомления источника;
    - **«Разрешить (Pass)»** – пропуск пакета без ограничений.
- **Адреса отправителя** - указываются IPv4-адреса или подсети. Если поле не заполнено, правило применяется ко всем адресам источника.
- **Порты отправителя** - указывается один или несколько портов в диапазоне от «1» до «65535».
- **Направление** - определяет направление трафика, к которому применяется правило:
    - **Прямое** - трафик от источника к получателю;
    - **Прямое и обратное** - трафик в обоих направлениях (источник ↔ получатель).
- **Адреса получателя** - указываются IPv4-адреса или подсети.
- **Порты получателя** - указывается один или несколько портов в диапазоне от «1» до «65535».

  Для протоколов используются следующие порты получателя по умолчанию:
    - **«Ethernet IP / CIP»** - 2222, 44818;
    - **«Modbus»**, **UMAS**. - 502;

- **«OPC UA»** - 4840, 48020;
- **«S7 Communication»**, **«S7 Communication Plus»**, **«MMS»** - 102;
- **«Fanuc FOCAS»** - 8193.

Примечание:

При конфигурировании правила порты получателя и отправителя должны находиться в пределах диапазонов, определённых в настройках протокола по умолчанию:

- **dst-порты** (порты получателя) — должны соответствовать значениям, указанным в списке портов назначения для выбранного протокола;
- **src-порты** (порты отправителя) — должны соответствовать значениям, указанным в списке портов источника (если таковые определены).

Если поля **«Порты отправителя»** и **«Порты получателя»** не заполнены, анализ трафика выполняется на всех портах, указанных в настройках протокола по умолчанию (**dst-port** и **src-port**). Указание портов за пределами этих диапазонов может привести к игнорированию трафика и, как следствие, к несрабатыванию правила.

- **Фильтрация на основе протокола** - позволяет задать специфичные для выбранного протокола параметры фильтрации.
- **Сетевой уровень** - позволяет задать сетевой уровень фильтрации:
  - уровень приложения;
  - уровень IP.

Примечание:

Поле доступно только при выборе протокола **«Alpha.Link»**.

- **Счетчик** - позволяет задать числа для декодирования пакетов. Принимает значения целых чисел в диапазоне от «0» до «255».

Примечание:

Поле доступно только при выборе протокола **«Alpha.Link»**.

- **Сообщение** - текстовое описание события, которое будет записано в журнал при срабатывании правила. Максимальная длина — «512» символов.

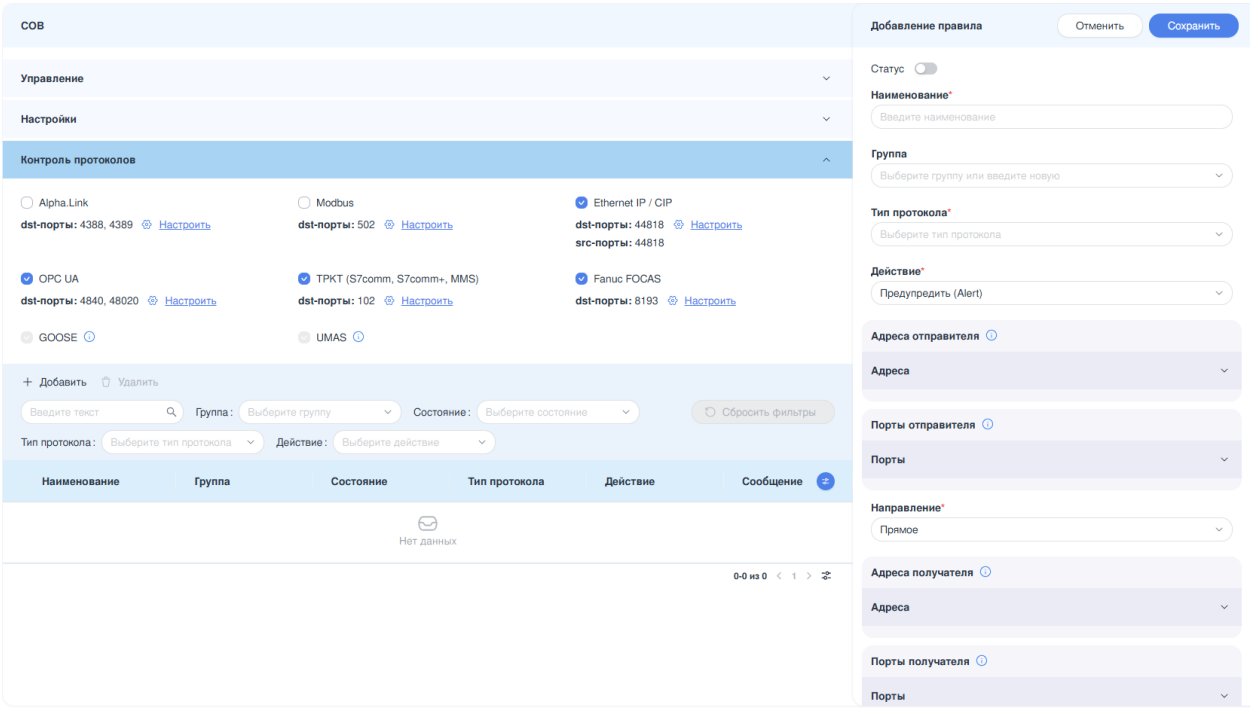


Рисунок – Создание правил СОВ на основе шаблонов протоколов

На текущий момент в веб-интерфейсе доступны шаблоны для настройки правил фильтрации следующих протоколов:

- **«Alpha.Link»**;
- **«Ethernet IP / CIP»**;
- **«Modbus»**;
- **«OPC UA»**;
- **«S7 Communication»**;
- **«S7 Communication Plus»**;
- **«MMS»**;
- **«GOOSE»**;
- **«UMAS»**;
- **«Fanuc FOCAS»**.

Поддержка других протоколов реализована исключительно через CLI-интерфейс. В последующих версиях системы планируется расширение функционала веб-интерфейса за счёт добавления шаблонов для других протоколов.

7.4.3.1 Шаблон протокола Alpha.Link

Для создания пользовательского правила на основе шаблона протокола **«Alpha.Link»** необходимо в поле **«Тип протокола»** выбрать значение **«Alpha.Link»**, а в поле **«Фильтрация на основе протокола»** - установить параметр **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появятся параметры **«Команда»**, **«Тип команды»**.

В поле параметра **«Команда»** возможен выбор следующих значений:

- **«CMD_LIST_NODES»**;
- **«RES_LIST_NODES»**;
- **«CMD_GET_PROPS»**;
- **«RES_GET_PROPS»**;
- **«CMD_SET_PROP»**;
- **«RES_SET_PROP»**;
- **«CMD_GET_PROP»**;
- **«RES_GET_PROP»**;
- **«CMD_CREATE_NODE»**;
- **«RES_CREATE_NODE»**;
- **«CMD_DELETE_NODE»**;
- **«RES_DELETE_NODE»**;
- **«CMD_RENAME_NODE»**;
- **«RES_RENAME_NODE»**;
- **«CMD_DELETE_PROP»**;
- **«RES_DELETE_PROP»**;
- **«CMD_SET_PROPS»**;
- **«RES_SET_PROPS»**;
- **«CMD_CREATE_NODE_EX»**;
- **«RES_CREATE_NODE_EX»**;
- **«CMD_COPY_NODE»**;
- **«RES_COPY_NODE»**;
- **«CMD_LOCK_NODE»**;
- **«RES_LOCK_NODE»**;
- **«CMD_UNLOCK_NODE»**;
- **«RES_UNLOCK_NODE»**;
- **«CMD_LOCK_BRANCH»**;
- **«RES_LOCK_BRANCH»**;

- **«CMD_UNLOCK_BRANCH»**;
- **«RES_UNLOCK_BRANCH»**;
- **«CMD_GET_PROP_DESCRIPTIONS»**;
- **«RES_GET_PROP_DESCRIPTIONS»**;
- **«CMD_ON_CHANGE_CONFIG»**;
- **«CMD_ON_LOCK»**;
- **«CMD_SET_USER_INFO»**;
- **«CMD_GET_LOCKINGS»**;
- **«RES_GET_LOCKINGS»**;
- **«CMD_BACKUP»**;
- **«RES_BACKUP»**;
- **«CMD_FIND_NODE»**;
- **«RES_FIND_NODE»**;
- **«CMD_GET_CONFIG_TREE»**;
- **«RES_GET_CONFIG_TREE»**;
- **«CMD_GET_SERVER_PARAM»**;
- **«RES_GET_SERVER_PARAM»**;
- **«CMD_CREATE_NODES»**;
- **«RES_CREATE_NODES»**;
- **«CMD_CREATE_NODES_BY_ID»**;
- **«RES_CREATE_NODES_BY_ID»**;
- **«CMD_GET_FREE_ID»**;
- **«RES_GET_FREE_ID»**;
- **«CMD_GET_ID_BY_NAME»**;
- **«RES_GET_ID_BY_NAME»**;
- **«CMD_CREATE_NODE_BY_ID»**;
- **«RES_CREATE_NODE_BY_ID»**;
- **«CMD_GET_CONFIG_ID»**;
- **«RES_GET_CONFIG_ID»**;
- **«CMD_SET_CONFIG_ID»**;
- **«RES_SET_CONFIG_ID»**;

- **«CMD_GET_CONFIG_NODE_STREAM»**;
- **«RES_GET_CONFIG_NODE_STREAM»**;
- **«CMD_SEND_DATA_STREAM»**;
- **«RES_SEND_DATA_STREAM»**;
- **«CMD_DATA_STREAM_CONTROL»**;
- **«RES_DATA_STREAM_CONTROL»**;
- **«CMD_AUTHORIZE_WITH_PASSWORD»**;
- **«RES_AUTHORIZE_WITH_PASSWORD»**;
- **«CMD_SET_MASTER_PASSWORD»**;
- **«RES_SET_MASTER_PASSWORD»**;
- **«CMD_KICKED_FROM_SERVER»**;
- **«CMD_CREATE_OR_UPDATE_NODES»**;
- **«RES_CREATE_OR_UPDATE_NODES»**;
- **«CMD_GET_BACKUP»**;
- **«RES_GET_BACKUP»**;
- **«CMD_SET_BACKUP»**;
- **«RES_SET_BACKUP»**;
- **«CMD_GET_EXTOBJECTS»**;
- **«RES_GET_EXTOBJECTS»**;
- **«CMD_SET_EXTOBJECTS»**;
- **«RES_SET_EXTOBJECTS»**;
- **«CMD_GET_SNAPSHOT»**;
- **«RES_GET_SNAPSHOT»**;
- **«CMD_UPLOAD_SNAPSHOT»**;
- **«RES_UPLOAD_SNAPSHOT»**;
- **«Настроенное пользователем»**.

При выборе команд, за исключением «Настроенное пользователем», дополнительно появится параметр **«Тип команды»**.

Перечень доступных к выбору значений в полях параметров **«Команда»** и **«Тип команды»** приведён в таблице (см. Таблица «Доступные типы команд»).

Таблица «Доступные типы команд»

Команда	Тип команды
• CMD_BACKUP • CMD_GET_FREE_ID • CMD_GET_ID_BY_NAME • CMD_GET_LOCKINGS • CMD_GET_PROP_DESCRIPTIONS	• vt_uint32
• CMD_COPY_NODE	• vt_CFG_COPY_NODE
• CMD_CREATE_NODE	• vt_CFG_CREATE_NODE
• CMD_CREATE_NODE_BY_ID	• vt_CFG_CREATE_NODE_BY_ID
• CMD_CREATE_NODE_EX	• vt_CFG_CREATE_NODE_EX
• CMD_CREATE_NODES	• vt_CFG_CREATE_NODES
• CMD_CREATE_NODES_BY_ID	• vt_CFG_CREATE_NODES_BY_ID
• CMD_CREATE_OR_UPDATE_NODES	• vt_CFG_CREATE_OR_UPDATE_NODES
• CMD_DATA_STREAM_CONTROL	• vt_DATA_STREAM_CONTROL_ID
• CMD_DELETE_NODE	• vt_CFG_DELETE_NODE
• CMD_DELETE_PROP	• vt_CFG_DELETE_PROP
• CMD_FIND_NODE • CMD_GET_CONFIG_TREE • CMD_GET_PROPS • CMD_LIST_NODES • CMD_LOCK_BRANCH • CMD_LOCK_NODE	• vt_wstring
• CMD_GET_CONFIG_NODE_STREAM	• vt_CFG_GET_NODE_STREAM
• CMD_GET_PROP	• vt_CFG_GET_PROP
• CMD_GET_SERVER_PARAM	• vt_CFG_SERVER_PARAM
• CMD_ON_CHANGE_CONFIG	• vt_CFG_ON_CHANGE_CONFIG
• CMD_ON_LOCK	• vt_CFG_ON_LOCK
• CMD_RENAME_NODE	• vt_CFG_RENAME_NODE
• CMD_SEND_DATA_STREAM	• vt_DATA_STREAM_CONTAINER_ID

Команда	Тип команды
	• vt_CFG_NODE_ID • vt_CFG_NODE_ID_LIST
• CMD_SET_CONFIG_ID	• vt_CFG_CONFIG_ID
• CMD_SET_MASTER_PASSWORD	• vt_MASTER_PASSWORD_CHANGE_ID
• CMD_SET_PROP	• vt_CFG_SET_PROP
• CMD_SET_PROPS	• vt_CFG_SET_PROPS
• CMD_SET_USER_INFO	• vt_CFG_USER_INFO • vt_CFG_USER_INFO2
• CMD_UNLOCK_BRANCH	• vt_CFG_UNLOCK_NODE
• CMD_UNLOCK_NODE	• vt_CFG_UNLOCK_NODE
• CMD_UPLOAD_SNAPSHOT	• vt_UPLOAD_SNAPSHOT_ID
• RES_BACKUP • RES_COPY_NODE • RES_CREATE_NODE • RES_CREATE_NODE_BY_ID • RES_CREATE_NODE_EX • RES_CREATE_NODES • RES_CREATE_NODES_BY_ID • RES_DATA_STREAM_CONTROL • RES_DELETE_NODE • RES_DELETE_PROP • RES_FIND_NODE • RES_GET_FREE_ID • RES_GET_ID_BY_NAME • RES_LOCK_BRANCH • RES_LOCK_NODE • RES_RENAME_NODE • RES_SEND_DATA_STREAM • RES_SET_CONFIG_ID	• vt_uint32 • vt_wstring

Команда	Тип команды
• RES_SET_MASTER_PASSWORD • RES_SET_PROP • RES_SET_PROPS • RES_UNLOCK_BRANCH • RES_UNLOCK_NODE	
• RES_GET_CONFIG_ID	• vt_CFG_CONFIG_ID
• RES_GET_CONFIG_NODE_STREAM	• vt_CFG_RES_NODE_STREAM • vt_wstring
• RES_GET_CONFIG_TREE	• vt_CFG_TREE_ITEM
• RES_GET_LOCKINGS	• vt_CFG_GET_LOCKINGS
• RES_GET_PROP	• vt_CFG_RES_GET_PROP • vt_wstring
• RES_GET_PROP_DESCRIPTIONS	• vt_CFG_GET_PROP_DESC • vt_wstring
• RES_GET_PROPS	• vt_CFG_PROP_LIST • vt_wstring
• RES_GET_SERVER_PARAM	• vt_CFG_SERVER_PARAM • vt_wstring
• RES_LIST_NODES	• vt_CFG_NODE_LIST • vt_wstring

В зависимости от выбранного типа команды могут появляться следующие дополнительные параметры:

- **«COMPUTER_NAME»**, **«DST_FULL_NAME»**, **«ERROR»**, **«FULL_NAME»**, **«LOCAL_IP»**, **«NAME»**, **«NODE_FULL_NAME»**, **«NODE_NAME»**, **«NEW_NAME»**, **«PARAM»**, **«PATH»**, **«REMOTE_IP»**, **«USER_NAME»**, **«VERSION»** - поля параметров принимают данные в шестнадцатеричном формате, где символ занимает два байта, например, «4400 6500 6D00 6F00 2E00 5300 6500 7400»;
- **«CONFIG_ID»** - поле параметра принимает значение GUID;

- **«CUR_PASS_CIPHER»**, **«NEW_PASS_CIPHER»** - поля параметров принимают числа в шестнадцатеричной системе счисления, где символ занимает один байт, например, «44 65 6D 6F 2E 53 65 74»;
- **«DAY»** - поле параметра принимает число от «0» до «31» или диапазон чисел при установке флажка напротив параметра;
- **«DOW»** - номер дня в неделе, поле параметра принимает число от «1» до «7» или диапазон чисел при установке флажка напротив параметра;
- **«DST»** - поле параметра принимает число от «-1» до «1» или диапазон чисел при установке флажка напротив параметра;
- **«HOUR»** - час, поле параметра принимает число от «0» до «23» или диапазон чисел при установке флажка напротив параметра;
- **«ACTION»**, **«ID»**, **«LOCK_ID»**, **«NODE_ID»**, **«NUM»**, **«OPERATION»**, **«PARENT_ID»**, **«PROP_ID»**, **«QUALITY»**, **«STREAM_ID»**, **«TYPE»**, **«VER»** - возможно указать число от «-9223372036854775808» до «9223372036854775807» или диапазон чисел при установке флажка напротив параметра;
- **«IS_LAST_PART»**;
- **«IS_MY_CHANGE»**;
- **«TERMINATE»**;
- **«Все, кроме указанного значения»**;
- **«MIN»** - минута, поле параметра принимает число от «0» до «59» или диапазон чисел при установке флажка напротив параметра;
- **«MONTH»** - месяц, поле параметра принимает число от «1» до «12» или диапазон чисел при установке флажка напротив параметра;
- **«PROP_VALUE»** - в зависимости от выбранного значения параметра **«Тип PROP_VALUE»**, поле параметра принимает числа в десятичной системе счисления в различных диапазонах или числа в шестнадцатеричной системе счисления, где символ занимает один байт, например, «44 65 6D 6F 2E 53 65 74» либо два байта, например, «4400 6500 6D00 6F00 2E00 5300 6500 7400», а также принимает значения GUID;
- **«SEC»** - секунда, поле параметра принимает число от «0» до «59» или диапазон чисел при установке флажка напротив параметра;
- **«VALUE»** - в зависимости от выбранного значения параметра **«Тип VALUE»**, поле параметра принимает числа в десятичной системе счисления в различных диапазонах или числа в шестнадцатеричной системе счисления, где символ занимает один байт, например, «44 65 6D 6F 2E 53 65 74», либо

два байта, например, «4400 6500 6D00 6F00 2E00 5300 6500 7400», а также принимает значения GUID;

- **«YEAR»** - год, поле параметра принимает число от «0» до «9223372036854775807» или диапазон чисел при установке флажка напротив параметра;
- **«Тип PROP_VALUE»**, **«Тип VALUE»** - доступен выбор следующих значений: «Отсутствует», «BOOL», «UINT8», «INT8», «UINT16», «INT16», «UINT32», «INT32», «UINT64», «INT64», «FLOAT32», «STRING», «WSTRING», «GUID».

В поле параметра **«Команда»** при выборе значения «Настроенное пользователем» дополнительно появятся параметры:

- **«Пользовательская команда»** - возможно указать число от «0» до «4294967295» или диапазон чисел при установке флажка напротив параметра;
- **«Пользовательский тип команды»** - возможно указать число от «0» до «4294967295» или диапазон чисел при установке флажка напротив параметра.

7.4.3.2 Шаблон протокола Ethernet IP / CIP

Для создания пользовательского правила на основе шаблона протокола **«Ethernet IP / CIP»** необходимо в поле **«Тип протокола»** выбрать значение **«Ethernet IP / CIP»**, а в поле **«Фильтрация на основе протокола»** - установить параметр **«Указать дополнительные параметры»**.

После этого становится доступным поле **«Совпадение по»**, в котором можно выбрать один из следующих вариантов:

- **«Протокол ENIP»** - правило применяется к трафику, содержащему заголовки протокола Ethernet/IP (ENIP), используемого для инкапсуляции CIP-команд в IP-пакеты;
- **«Протокол CIP»** - правило применяется к трафику, содержащему данные протокола Common Industrial Protocol (CIP), используемого для обмена информацией между промышленными устройствами;
- **«Протокол ENIP, Протокол CIP»** - правило срабатывает при наличии как ENIP-заголовков, так и CIP-данных в пакете. Условие считается выполненным при совпадении по обоим уровням протокола.

Параметры при выборе «Протокол ENIP»

- **Команда ENIP** — указывает тип команды в заголовке ENIP. Каждая команда соответствует определённому типу запроса или ответа (например, List Identity, Send RR Data, Register Session и др.). Допустимые значения — целые числа в диапазоне от «1» до «65535».

Пример: Значение 111 соответствует команде Send RR Data (0x006F), использующейся для обмена запросами и ответами между клиентом и сервером.

Параметры при выборе «Протокол CIP»

- **Сервис** — определяет тип операции в CIP-запросе или ответе. Значение указывается как числовой код сервиса в диапазоне от «0» до «127».

  Примеры: 78 - Get Attribute Single (0x4E) — чтение значения атрибута объекта.

  Указание сервиса позволяет фильтровать конкретные типы операций, например, блокировать попытки записи данных.

- **Использовать класс** — активация параметра позволяет задать фильтрацию по классу CIP-объекта. Фильтрация по классам доступно только для сервисов: «3» - Get Attribute List (0x03), «4» - Set Attribute List (0x04), «14» - Get Attribute Single (0x0E), «16» - Set Attribute Single (0x10).

  - **Класс** — числовое значение в диапазоне от «1» до «65535», определяющее тип объекта (например, «4» - Assembly (0x04), «6» - Connection Manager (0x06)).

  При активации вложенного параметра **«Использовать атрибут»** становится доступным:

  - **Атрибут** — числовое значение от «0» до «65535», указывающее конкретный атрибут внутри класса. Например, атрибут «3» в классе Assembly может содержать данные конфигурации.

- **Часть адреса** — определяет тип адресной информации, используемой в CIP-маршруте. Допустимые значения:

  - **Отсутствует** — маршрут не содержит дополнительных адресных сегментов;
  - **ANSI сегмент** — маршрут включает сегмент, совместимый с ANSI/ISA-88. Указывается в поле **«ANSI сегмент»** в виде строки длиной до «50» символов;
  - **Порт** — маршрут включает сетевой порт. При выборе данного значения доступны следующие параметры:
    - **Порт** — конкретный порт в диапазоне от «0» до «65535». При активации чекбокса **«Все, кроме указанного порта»** правило применяется ко всем портам, кроме указанного (инверсия условия);
    - **Диапазон** — позволяет задать интервал портов:

- **Начальный порт** — минимальное значение порта в диапазоне от «0» до «65535»;
- **Конечный порт** — максимальное значение порта в диапазоне от «0» до «65535».

Начальный порт должен быть меньше конечного.

7.4.3.3 Шаблон протокола Modbus

Для создания пользовательского правила на основе шаблона протокола **«Modbus»** необходимо в поле **«Тип протокола»** выбрать значение **«Modbus»**, а в поле **«Фильтрация на основе протокола»** - установить параметр **«Указать дополнительные параметры»**.

После этого становится доступным поле **«Совпадение по»**, в котором можно выбрать один из следующих вариантов:

- **«Функции»**;
- **«Данные»**.

Параметры при выборе совпадения по «Функции»

При выборе опции **«Функции»** появится параметр **«Код функции»** — указывает код или категорию функции, по которым будет происходить фильтрация.

В поле параметра **«Код функции»** возможен выбор следующих значений:

- **«01:Read Coils»**;
- **«02:Read Discrete Inputs»**;
- **«03:Read Holding Register»**;
- **«04:Read Input Register»**;
- **«05:Write Single Coil»**;
- **«07:Read Exception Status»**;
- **«08:Diagnostic»**;
- **«0B:Get Com event counter»**;
- **«0C:Get Com Event Log»**;
- **«0F:Write Multiple Coils»**;
- **«10:Write Multiple Registers»**;
- **«11:Report Server ID»**;
- **«14:Read File record»**;
- **«15:Write File record»**;
- **«16:Mask Write Register»**;

- **«17:Read/Write Multiple Registers»**;
- **«18:Read FIFO queue»**.

Параметры при выборе совпадения по «Данные»

При выборе опции **«Данные»** появятся параметры **«Идентификатор устройства»**, **«Код функции»**, **«Отсчёт адреса»**, **«Адрес»** и **«Значение»**, доступные для указания значения или диапазона значений:

- **«Идентификатор устройства»** – от «0» до «255»;
- **«Код функции»** – от «0» до «255»;
- **«Отсчёт адреса»** – «С единицы» или «С нуля»;
- **«Адрес»** – от «0» до «65535»;
- **«Значение»** – от «0» до «65535».

7.4.3.4 Шаблон протокола OPC UA

Для создания пользовательского правила на основе шаблона протокола **«OPC UA»** необходимо в поле «Тип протокола» выбрать значение **«OPC UA»**, а в поле **«Фильтрация на основе протокола»** - установить параметр **«Указать дополнительные параметры»**.

После этого становится доступным поле **«Тип сообщения»**, в котором можно выбрать один из следующих вариантов:

- **«HELLO»** - маркер начала передачи данных между клиентом и сервером;
- **«ACKNOWLEDGE»** - ответ на сообщение типа HELLO;
- **«OPEN»** - открытие канала передачи данных с предложенным методом шифрования данных;
- **«MESSAGE»** - передаваемое сообщение;
- **«CLOSE»** - конец сессии.

Параметры при выборе «OPEN»

При выборе типа сообщения **«OPEN»** появится параметр **«Политика безопасности»**, в котором доступны следующие политики безопасности:

- **«NONE»**;
- **«BASIC128RSA15»**;
- **«BASIC256»**;
- **«BASIC256SHA256»**;
- **«AES128_SHA256_RSAOAEP»**;
- **«PUBSUB_AES128_CTR»**;

- **«PUBSUB_AES256_CTR»**.

Параметры при выборе «MESSAGE»

При выборе типа сообщения **«MESSAGE»** появится параметр **«Тип запроса»**, в котором доступны типы запросов:

- **«FINDSERVERS»** - запрос известных серверов;
- **«FINDSERVERSONNETWORK»** - запрос известных работающих серверов;
- **«GETENDPOINTS»** - запрос на поддерживаемые сервером конечные точки;
- **«REGISTERSERVER»** - запрос на регистрацию сервера;
- **«REGISTERSERVER2»** - запрос на регистрацию сервера с дополнительной информацией для FINDSERVERSONNETWORK;
- **«CREATESESSION»** - запрос на создание сессии;
- **«ACTIVATESESSION»** - запрос на создание сессии (передача идентификационных данных клиента);
- **«CLOSESESSION»** - запрос на завершение сессии;
- **«CANCEL»** - запрос отмены невыполненных запросов на обслуживание;
- **«ADDNODES»** - запрос на добавление узла как дочерний в адресное пространство;
- **«ADDREFERENCES»** - запрос на добавление ссылки на узел;
- **«DELETENODES»** - запрос на удаление узла из адресного пространства;
- **«DELETEREFERENCES»** - запрос на удаление ссылки узла;
- **«BROWSE»** - запрос на просмотр узлов;
- **«BROWSENEXT»** - запрос на продолжение просмотра результата запроса BROWSE, если результат этого запроса превышает максимальное значение;
- **«TRANSLATEBROWSEPATHSTONODEIDS»** - запрос на преобразование пути узла в идентификатор узла;
- **«REGISTERNODES»** - запрос на регистрацию узла, например, узла, информация о котором пользователю известна;
- **«UNREGISTERNODES»** - запрос на отмену регистрации узла;
- **«QUERYFIRST»** - запрос просмотр данных из определённого экземпляра;
- **«QUERYNEXT»** - запрос на продолжение просмотра результата запроса QUERYFIRST, если результат этого запроса превышает максимальное значение;
- **«READ»** - запрос на чтение данных;
- **«HISTORYREAD»** - запрос на просмотр значений или событий узлов;

- **«WRITE»** - запрос на изменение узла;
- **«HISTORYUPDATE»** - запрос на обновление значений или событий узлов;
- **«CALLMETHOD»** - запрос на получение результатов вызова удалённой процедуры;
- **«CALL»** - запрос на вызов удалённой процедуры;
- **«MONITOREDITEMCREATE»** - запрос на начало подписки на событие;
- **«CREATEMONITOREDITEMS»** - запрос на подписку на событие;
- **«MONITOREDITEMMODIFY»** - запрос на изменение параметров подписки на события;
- **«MODIFYMONITOREDITEMS»** - запрос на изменение подписки;
- **«SETMONITORINGMODE»** - запрос на установку режима подписки;
- **«SETTRIGGERING»** - запрос на создание связи между событием и узлом;
- **«DELETEMONITOREDITEMS»** - запрос на завершение подписки;
- **«CREATESUBSCRIPTION»** - запрос на создание подписки на событие;
- **«MODIFYSUBSCRIPTION»** - запрос на изменение подписки на событие;
- **«SETPUBLISHINGMODE»** - запрос на включение отправки уведомлений по подпискам на событие;
- **«PUBLISH»** - запрос на подтверждение получения уведомлений по подпискам на события;
- **«REPUBLISH»** - запрос на повторную отправку уведомлений по подпискам на события;
- **«TRANSFERSUBSCRIPTIONS»** - запрос на передачу подписки на событие из одной сессии в другую;
- **«DELETESUBSCRIPTIONS»** - запрос на удаление подписки на событие.

При выборе типа запросов **«BROWSE»** и **«READ»** появятся параметры:

- **«Идентификатор пространства имен»**;
- **«Тип идентификатора узла»**.

При выборе типа запросов **«WRITE»** появятся параметры:

- **«Идентификатор пространства имен»**;
- **«Тип идентификатора узла»**;
- **«Тип значений»**.

При выборе типа запроса **«CALL»** появятся параметры:

- **«Тип идентификатора узла вызываемого объекта»**;

- **«Тип идентификатора узла вызываемого метода»**.

7.4.3.5 Шаблон протокола S7 Communication

При создании пользовательского правила на основе шаблона промышленного протокола **S7 Communication** необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появится параметр **«Тип сообщения»**, в котором доступно четыре типа сообщений:

- **«JOBREQUEST»** - пакет с запросом на выполнение функции;
- **«ACK»** - пакет с результатом выполнения операции;
- **«ACKDATA»** - пакет с ответом на запрос;
- **«USERDATA»** - пакет с данными пользователя.

При выборе типа сообщения «JOBREQUEST» появится параметр **«Функция»**, в котором доступны следующие функции:

- **«CPUSERVICE»** - сервисы ЦП;
- **«SETUPCOMM»** - запрос на подключение к ПЛК;
- **«READVAR»** - запрос на чтение;
- **«WRITEVAR»** - запрос на запись;
- **«REQUESTDOWNLOAD»** - запрос на загрузку прошивки;
- **«DOWNLOADBLOCK»** - загрузка прошивки на ПЛК;
- **«DOWNLOADEND»** - запрос на завершение загрузки прошивки на ПЛК;
- **«STARTUPLOAD»** - запрос на выгрузку прошивки;
- **«UPLOAD»** - выгрузка прошивки с ПЛК;
- **«ENDUPLOAD»** - окончание выгрузки прошивки с ПЛК;
- **«PLCCONTROL»** - управление ПЛК;
- **«PLCSTOP»** - остановка ПЛК;
- **«Любой»**.

При выборе функции «READVAR» или «WRITEVAR» появится параметр **«Тип области»**, в котором доступны типы области чтения, указанные в таблице (см. Таблица «Типы области»).

Таблица «Типы области»

Тип области	Описание
Любой	Любая область чтения

Тип области	Описание
SI (System info)	Системная информация
SF (System flags)	Системные флаги
AI (Аналоговые входы)	Аналоговые вводы
AO (Аналоговые выводы)	Аналоговые выводы
C (Counters)	Счётчики
T (Timers)	Таймеры
IC (IEC Counters)	Счётчики IEC
IT (IEC Timers)	Таймеры IEC
P (Directp peripheral access)	Прямой доступ к периферии
I (Inputs)	Ввод
Q (Outputs)	Вывод
M (Flags)	Флаги
DB (Data blocks)	Блоки данных
DI (Instance data blocks)	Блоки данных экземпляра
LV (Local data)	Локальные данные

При выборе в поле параметра **«Тип области»** любого значения, кроме значения «Любой», появятся поля:

- **«Имя области»**;
- **«Тип данных»**;
- **«Количество данных»**;
- **«Смещение данных»**.

Поле параметра **«Имя области»** принимает значения от «0» до «65535».

В поле параметра **«Тип данных»** доступны следующие типы данных, представленные в таблице (см. Таблица «Доступные типы данных»).

Таблица «Доступные типы данных»

Значение	Значение	Значение
BIT	DINT	DATETIME
BYTE	REAL	COUNTER
CHAR	DATE	TIMER
WORD	TOD	IECTIMER

Значение	Значение	Значение
INT	TIME	IECCOUNTER
DWORD	S5TIME	HSCOUNTER

Поле параметра **«Количество данных»** принимает значения от «0» до «65535».

Поле параметра **«Смещение данных»** принимает целочисленное значение в шестнадцатеричной системе счисления в формате «0x000000».

При выборе функции «WRITEVAR» и любого значения в поле параметра **«Тип области»**, кроме значения «Любой», появятся дополнительные параметры:

- **«Тип передаваемого значения»**;
- **«Количество передаваемых данных»**;
- **«Список значений данных»**.

В поле параметра **«Тип передаваемого значения»** доступны следующие типы значений:

- **«NULL»** - не выбрано;
- **«BIT»** - значение в битах;
- **«BYTE»** - значение в байтах;
- **«INT»** - целочисленное значение;
- **«REAL»** - вещественное;
- **«STR»** - строковое значение.

Поле параметра **«Список значений данных»** принимает список значений в шестнадцатеричной системе счисления.

При выборе функций «REQUESTDOWNLOAD», «DOWNLOADBLOCK», «STARTUPLOAD» появится параметр **«Тип блока»**, в котором доступны следующие типы блока скачивания:

- **«OB»** - организационный блок, хранит главные программы;
- **«DB»** - блок данных, хранит необходимые для ПЛК программ данные;
- **«SDB»** - блок данных системы, хранит необходимые для ПЛК программ данные;
- **«FC»** - функция, функции без состояния - не имеют собственной памяти, могут быть запущены из других программ;
- **«SFC»** - системная функция, функции без состояния - не имеют собственной памяти, могут быть вызваны из других программ;

- **«FB»** - блок функции, функции с состоянием, обычно имеют ассоциированный SDB;
- **«SFB»** - блок системной функции, функции с состоянием, обычно имеют ассоциированный SDB;
- **«Любой»**.

При выборе в поле параметра **«Тип блока»** любого значения, кроме значения «Любой», появятся параметры **«Номер блока»** и **«Целевая файловая система»**. Параметры **«Номер блока»** принимает значения от «0» до «99999».

В поле параметра **«Целевая файловая система»** доступны две опции:

- **«P»** - пассивная, блок требует активации после скачивания;
- **«A»** - активная, блок будет активизирован после скачивания.

При выборе функции «PLCCONTROL» появится параметр **«Функция»**, в котором доступны следующие функции управления ПЛК:

- **«Любой»**;
- **«INSE»** - активация скачанного блока, параметром выступает имя блока;
- **«DELE»** - удаление блока, параметром выступает имя блока;
- **«PPROGRAM»** - запуск программы, параметром выступает имя программы;
- **«GARB»** - сжатие памяти;
- **«MODU»** - копирование RAM в ROM, параметр содержит идентификаторы файловой системы A/E/P;
- **«OFF»** - выключение ПЛК;
- **«ON»** - включение ПЛК.

7.4.3.6 Шаблон протокола S7 Communication Plus

При создании пользовательского правила на основе шаблона промышленного протокола **S7 Communication Plus** необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появятся следующие параметры:

- **«Тип сообщения»**;
- **«Тип»**;
- **«Функция»**.

Параметр **«Тип сообщения»** содержит выпадающий список со значениями:

- **«REQUEST»** - запрос на выполнение операции;

- **«RESPONSE»** - ответ на запрос;
- **«NOTIFY»** - асинхронное уведомление;
- **«RESPONSE2»** - расширенный ответ.

Параметр **«Тип»** - содержит выпадающий список со значениями:

- **«CONNECT»** - установка соединения;
- **«DATA»** - передача данных;
- **«DATAW1_5»** - передача данных протокола версии 1.5;
- **«KEEPALIVE»** - проверка активности соединения;
- **«EXT_KEEPALIVE»** - расширенный **«KEEPALIVE»**.

Параметр **«Функция»** - содержит выпадающий список со значениями:

- **«Отсутствует»**;
- **«EXPLORE»** - поиск и перечесление доступных объектов;
- **«CREATEOBJECT»** - создание нового объекта;
- **«DELETEOBJECT»** - удаление объекта;
- **«SETVARIABLE»** - запись значения одной переменной;
- **«GETLINK»** - получение ссылки на объект;
- **«SETMULTIVAR»** - запись значений нескольких переменных;
- **«GETMULTIVAR»** - чтение значений нескольких переменных;
- **«BEGINSEQUENCE»** - начало группы операций;
- **«ENDSEQUENCE»** - завершение группы операций;
- **«INVOKE»** - вызов метода объекта;
- **«GETVARSUBSTR»** - чтение части переменной.

При выборе опций «EXPLORE», «CREATEOBJECT», «DELETEOBJECT», «GETLINK», «SETMULTIVAR», «GETMULTIVAR», и «GETVARSUBSTR» появятся параметры для указания значений функции.

7.4.3.7 Шаблон протокола MMS

При создании пользовательского правила на основе шаблона промышленного протокола **MMS** необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появится параметр **«Тип сообщения»**, в котором доступны следующие типы сообщений:

- **«CANCEL_REQUEST»**;

- **«CANCEL_RESPONSE»**;
- **«CANCEL_ERROR»**;
- **«CONFIRMED_REQUEST»**;
- **«CONFIRMED_RESPONSE»**;
- **«CONFIRMED_ERROR»**;
- **«UNCONFIRMED»**;
- **«REJECT»**;
- **«INITIATE_REQUEST»**;
- **«INITIATE_RESPONSE»**;
- **«INITIATE_ERROR»**;
- **«CONCLUDE_REQUEST»**;
- **«CONCLUDE_RESPONSE»**;
- **«CONCLUDE_ERROR»**.

При выборе типа сообщения «CONFIRMED_REQUEST» появится параметр **«Тип службы»**, в котором доступны следующие типы используемых служб:

Перечень доступных к выбору значений в поле параметра **«Тип службы»** приведён в таблице (см. Таблица «Доступные типы служб»).

Таблица «Доступные типы служб»

Значение	Значение
STATUS	KILL
GETNAMELIST	GETPROGRAMINVOCATIONATTRIBUTES
IDENTIFY	OBTAINFILE
RENAME	DEFINEEVENTCONDITION
READ	DELETEEVENTCONDITION
WRITE	GETEVENTCONDITIONATTRIBUTES
GETVARIABLEACCESSATTRIBUTES	REPORTEVENTCONDITIONSTATUS
DEFINENAMEDVARIABLE	ALTEREVENTCONDITIONMONITORING
DEFINESCATTEREDACCESS	TRIGGEREVENT
GETSCATTEREDACCESSATTRIBUTES	DEFINEEVENTACTION
DELETEVARIABLEACCESS	DELETEEVENTACTION
DEFINENAMEDVARIABLELIST	GETEVENTACTIONATTRIBUTES
GETNAMEDVARIABLELISTATTRIBUTES	REPORTEVENTACTIONSTATUS

Значение	Значение
DELETENAMEDVARIABLELIST	DEFINEEVENTENROLLMENT
DEFINENAMEDTYPE	DELETEEVENTENROLLMENT
GETNAMEDTYPEATTRIBUTES	ALTEREVENTENROLLMENT
DELETENAMEDTYPE	REPORTEVENTENROLLMENTSTATUS
INPUT	GETEVENTENROLLMENTATTRIBUTES
OUTPUT	ACKNOWLEDGEEVENTNOTIFICATION
TAKECONTROL	GETALARMSUMMARY
RELINQUISHCONTROL	GETALARMENROLLMENTSUMMARY
DEFINESEMAPHORE	READJOURNAL
DELETESEMAPHORE	WRITEJOURNAL
REPORTSEMAPHORESTATUS	INITIALIZEJOURNAL
REPORTPOOLSEMAPHORESTATUS	REPORTJOURNALSTATUS
REPORTSEMAPHOREENTRYSTATUS	CREATEJOURNAL
INITIATEDOWNLOADSEQUENCE	DELETEJOURNAL
DOWNLOADSEGMENT	GETCAPABILITYLIST
TERMINATEDOWNLOADSEQUENCE	FILEOPEN
INITIATEUPLOADSEQUENCE	FILEREAD
UPLOADSEGMENT	FILECLOSE
TERMINATEUPLOADSEQUENCE	FILERENAME
REQUESTDOMAINDOWNLOAD	FILEDELETE
REQUESTDOMAINUPLOAD	FILEDIRECTORY
LOADDOMAINCONTENT	ADDITIONALSERVICE
STOREDOMAINCONTENT	GETDATAEXCHANGEATTRIBUTES
DELETEDOMAIN	EXCHANGEDATA
GETDOMAINATTRIBUTES	DEFINEACCESSCONTROLLIST
CREATEPROGRAMINVOCATION	GETACCESSCONTROLLISTATTRIBUTES
DELETEPROGRAMINVOCATION	REPORTACCESSCONTROLLEDOBJECTS
START	DELETEACCESSCONTROLLIST
STOP	CHANGEACCESSCONTROL
RESUME	RECONFIGUREPROGRAMINVOCATION

Значение	Значение
RESET	

При выборе типа службы «ADDITIONALSERVICE» появится параметр **«Дополнительный тип сервиса»**, в котором доступны следующие типы дополнительного сервиса, представленные в таблице (см. Таблица «Типы дополнительного сервиса»).

Таблица «Типы дополнительного сервиса»

Значение	Значение
VMDSTOP	GETUCATTRIBUTES
VMDRESET	LOADUCFROMFILE
SELECT	STOREUCTOFILE
ALTERPI	DELETEUC
INITIATEUCLOAD	DEFINEECL
UCLOAD	DELETEECL
UCUPLOAD	ADDECLREFERENCE
STARTUC	REMOVEECLREFERENCE
STOPUC	GETECLATTRIBUTES
CREATEUC	REPORTECLSTATUS
ADDTOUC	ALTERECLMONITORING
REMOVEFROMUC	

При выборе типа службы «READ» появятся параметры:

- **«Item ID запроса чтения»**. Максимальное количество символов - «32».
- **«Domain ID запроса чтения»**. Максимальное количество символов - «32».
- **«Адрес запроса чтения»**. Максимальное количество символов - «32».

При выборе типа службы «WRITE» появятся параметры:

- **«Item ID запроса записи»**. Максимальное количество символов - «32».
- **«Domain ID запроса записи»**. Максимальное количество символов - «32».

7.4.3.8 Шаблон протокола GOOSE

При создании пользовательского правила на основе шаблона промышленного протокола **GOOSE** необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появятся следующие параметры, значения которых должны содержать не более 150 символов:

- **«APPID»** - уникальный идентификатор приложения. Принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра.
- **«Dataset»** - ссылка на набор данных.
- **«GoCBRef»** - полная ссылка на блок управления GOOSE.
- **«GoID»** - идентификатор GOOSE-сообщения.
- **«Дельта секунд»** - разница времени в секундах между моментом формирования GOOSE-сообщения и некоторым базовым временем.
- **«Дельта наносекунд»** - разница времени в наносекундах между моментом формирования GOOSE-сообщения и базовым временем.
- **«Предустановленная дата и время»** - базовое системное время, относительно которого вычисляются **«Дельта секунд»** и **«Дельта наносекунд»**.
- **«Предустановленные наносекунды»** - фиксированные начальные базового системного времени, к которым потом прибавляются дельты.

Примечание:

Для включения записи событий срабатывания правил **COB** по протоколу **GOOSE** необходимо включить соответствующий параметр журналирования через интерфейс командной строки. Это осуществляется посредством выполнения следующей команды в конфигурационном режиме (см. раздел «Команды настройки Suricata» Руководства по настройке ARMA Стена в CLI):

```
set suricata outputs eve-log enabled yes
```

7.4.3.9 Шаблон протокола UMAS

При создании пользовательского правила на основе шаблона промышленного протокола **UMAS** необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появятся параметры **«Функция»**, **«Информация о проекте»** и **«Тип сообщения»**.

В поле параметра **«Функция»** доступны следующие функции:

- **«INIT_COMM»** - инициализация UMAS сессии;
- **«READ_ID»** - запрос ПЛК ID;

- **«READ_PROJECT_INFO»** - чтение информации о проекте;
- **«READ_PLC_INFO»** - чтение внутренней информации ПЛК;
- **«READ_CARD_INFO»** - чтение информации о внутренней SD карты ПЛК;
- **«REPEAT»** - отправить информацию обратно ПЛК. Используется для синхронизации;
- **«TAKE_PLC_RESERVATION»** - назначить ПЛК владельца;
- **«RELEASE_PLC_RESERVATION»** - снять владельца ПЛК;
- **«KEEP_ALIVE»** - поддержка активного соединения;
- **«READ_MEMORY_BLOCK»** - чтение блока памяти с ПЛК;
- **«READ_VARIABLES»** - чтение системных битов, системных слов и переменных;
- **«WRITE_VARIABLES»** - запись системных битов, системных слов и переменных;
- **«READ_COILS_REGISTERS»** - чтение coils и регистров с ПЛК;
- **«WRITE_COILS_REGISTERS»** - запись катушек и регистров в ПЛК;
- **«INITIALIZE_UPLOAD»** - инициализация загрузки (копирования с инженерного ПК на ПЛК);
- **«UPLOAD_BLOCK»** - загрузка блока данных с инженерного ПК на ПЛК;
- **«END_STRATEGY_UPLOAD»** - завершение загрузки (копирования с инженерного ПК на ПЛК);
- **«INITIALIZE_DOWNLOAD»** - инициализация скачивания (копирования с ПЛК на инженерный ПК);
- **«DOWNLOAD_BLOCK»** - скачивание блока данных с ПЛК на инженерный ПК;
- **«END_STRATEGY_DOWNLOAD»** - конец скачивания (копирования с ПЛК на инженерный ПК);
- **«READ_ETH_MASTER_DATA»** - чтение Ethernet Master Data;
- **«START_PLC»** - включение ПЛК;
- **«STOP_PLC»** - выключение ПЛК;
- **«MONITOR_PLC»** - мониторинг системных битов, системных слов и переменных;
- **«CHECK_PLC»** - проверка статуса подключения ПЛК;
- **«READ_IO_OBJECT»** - чтение IO объекта;
- **«WRITE_IO_OBJECT»** - запись IO объекта;

- **«GET_STATUS_MODULE»** - получение статуса модуля.

Параметр **«Информация о проекте»** принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра.

В поле параметра **«Тип сообщения»** доступны два типа сообщений:

- **«REQ»** - запрос;
- **«RES»** - ответ.

При выборе функции «READ_MEMORY_BLOCK» появятся параметры:

- **«Номер блока»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра;
- **«Количество данных»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра;
- **«Смещение»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра.

При выборе функции «READ_VARIABLES» появятся параметры:

- **«Базовое смещение»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра;
- **«Относительное смещение»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра;
- **«Номер блока»**;
- **«Количество значений»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра;
- **«Тип значений»**.

В поле параметра **«Тип значений»** доступны три типа значений:

- **«BIT»**;
- **«WORD»**;
- **«DWORD»**.

При выборе функции «WRITE_VARIABLES» появятся параметры:

- **«Номер блока»**;
- **«Смещение»**;
- **«Тип значений»**;
- **«Значение»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра.

При выборе функций «READ_COILS_REGISTERS» и «WRITE_COILS_REGISTERS» появятся параметры:

- **«Условие (значение)»** - только для «WRITE_COILS_REGISTERS»;
- **«Номер регистров флагов (Coils)»** - принимает значения от «0» до «65535» или диапазон значений при установке флажка напротив параметра;
- **«Смещение»**;
- **«Тип значений»**.

В поле параметра **«Условие (значение)»** доступны следующие условия:

- **«отсутствует»**;
- **«больше чем»**;
- **«меньше чем»**;
- **«равно»**;
- **«отрицание»**.

В поле параметра **«Тип значений»** доступны три типа значений:

- **«регистр»**;
- **«регистр флага (Coil)»**;
- **«отсутствует»**.

7.4.3.10 Шаблон протокола FOCAS

При создании пользовательского правила на основе шаблона протокола **Fanuc FOCAS** необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение **«Указать дополнительные параметры»**.

При выборе опции **«Указать дополнительные параметры»** появится параметр **«Тип сообщения»**.

В поле параметра **«Тип сообщения»** возможно выбрать следующие значения:

- **«Отсутствует»**;
- **«Запрос»**;
- **«Ответ»**;
- **«Команда»**.

В поле параметра **«Тип сообщения»** при выборе значения «Запрос» дополнительно появятся следующие параметры:

- **«Тип запроса»**;
- **«Добавить команду»**;
- **«Значение ARG1»**;

- **«Значение ARG2»**;
- **«Значение ARG3»**;
- **«Значение ARG4»**;
- **«Значение ARG5»**.

В полях параметров **«Значение ARG1»**, **«Значение ARG2»**, **«Значение ARG3»**, **«Значение ARG4»**, **«Значение ARG5»** возможно указать число от «0» до «4294967295» либо указать диапазон чисел при установке флажка напротив параметра.

В поле параметра **«Тип запроса»** возможно выбрать следующие значения:

- **«Любой»**;
- **«Загрузить программу»**;
- **«Настроенное пользователем»**.

При выборе в поле параметра **«Тип запроса»** значения «Загрузить программу» дополнительно появятся следующие параметры:

- **«Тип загружаемой программы»**;
- **«Путь к программе»**.

В полях параметров **«Тип загружаемой программы»**, **«Значение запроса»**, **«Значение команды»**, **«Тип скачиваемой программы»**, **«Значение ответа»**, **«Начальное значение диагностических данных»**, **«Конечное значение диагностических данных»**, **«Осевое значение диагностических данных»**, **«Начало чтения регистра»**, **«Конец чтения регистра»**, **«Тип памяти чтения регистра»**, **«Тип данных чтения регистра»** возможно указать число от «0» до «4294967295» либо указать диапазон чисел при установке флажка напротив параметра.

Примечание:

Рекомендуется использовать значения, соответствующие указанным в библиотеках Fanuc FOCAS.

В поле параметра **«Тип запроса»** при выборе значения «Настроенное пользователем» дополнительно появится параметр **«Значение запроса»**.

При установке флажка для параметра **«Добавить команду»** дополнительно появятся следующие параметры:

- **«Тип команды»**;
- **«Путь до удаляемых файлов»**.

В поле параметра **«Тип команды»** возможно выбрать следующие значения:

- **«Отсутствует»**;

- **«Диагностические данные»**;
- **«Список программ или файлов»**;
- **«Удалить файл, папку или программу»**;
- **«Чтение регистра»**;
- **«Настроенное пользователем»**.

В поле параметра **«Тип команды»** при выборе значения «Диагностические данные» дополнительно появятся следующие параметры:

- **«Начальное значение диагностических данных»**;
- **«Конечное значение диагностических данных»**;
- **«Осевое значение диагностических данных»**.

В поле параметра **«Тип команды»** при выборе значения «Список программ или файлов» дополнительно появится параметр **«Путь до читаемого каталога»**.

В поле параметра **«Тип команды»** при выборе значения «Удалить файл, папку или программу» дополнительно появится параметр **«Путь до удаляемых файлов»**.

В поле параметра **«Тип команды»** при выборе значения «Чтение регистра» дополнительно появятся следующие параметры:

- **«Начало чтения регистра»**;
- **«Конец чтения регистра»**;
- **«Тип памяти чтения регистра»**;
- **«Тип данных чтения регистра»**.

В поле параметра **«Тип команды»** при выборе значения «Настроенное пользователем» дополнительно появится параметр **«Значение команды»**.

В поле параметра **«Тип сообщения»** при выборе значения «Ответ» дополнительно появится параметр **«Тип ответа»**.

В поле параметра **«Тип ответа»** возможно выбрать следующие значения:

- **«Любой»**;
- **«Скачать программу»**;
- **«Настроенное пользователем»**.

В поле параметра **«Тип ответа»** при выборе значения «Скачать программу» дополнительно появятся следующие параметры:

- **«Тип скачиваемой программы»**;
- **«Путь к программе»**.

В поле параметра **«Тип ответа»** при выборе значения «Настроенное пользователем» дополнительно появится параметр **«Значение ответа»**.

В поле параметра **«Тип сообщения»** при выборе значения «Команда» дополнительно появятся следующие параметры:

- **«Тип команды»**;
- **«Значение команды»**.

7.4.4 Поиск и фильтрация

Блок фильтрации предоставляет возможность сортировки и фильтрации данных в таблице подраздела **«Контроль протоколов»** по всем столбцам в списке (см. Рисунок – Панель поиск и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Группа»**;
- **«Состояние»**;
- **«Тип протокола»**;
- **«Действие»**;
- **кнопка «Сбросить фильтры»**.

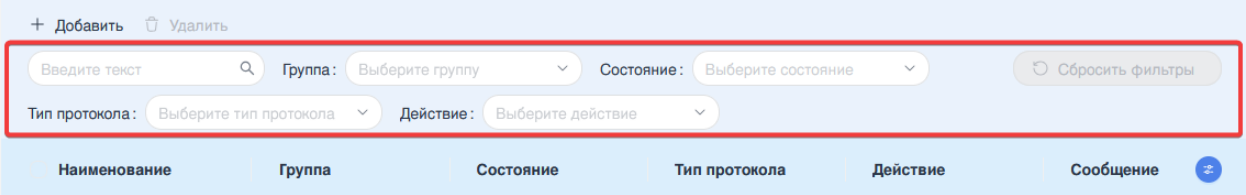


Рисунок – Панель поиск и фильтрации

Фильтрация по полю **«Группа»** позволяет осуществлять отбор данных на основе группы. В данном поле представлен раскрывающийся список с наименованиями групп, к которым относятся правила.

Фильтрация по полю **«Состояние»** позволяет отфильтровать список по статусу правила: *«Включен»*, *«Выключен»*.

Фильтрация по полю **«Тип протокола»** позволяет отфильтровать список по типу протокола. Поле содержит выпадающий список и предоставляет выбор из протоколов, которые доступны на текущий момент.

Фильтрация по полю **«Действие»** позволяет отфильтровать список по действию, которое задано в правиле. Поле содержит выпадающий список и предоставляет выбор из следующих вариантов значений: *«Предупредить (Alert)»*, *«Отклонить (Reject)»*, *«Отбросить (Drop)»*, *«Разрешить (Pass)»*.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

Сквозной поиск по таблице подраздела **«Контроль протоколов»** осуществляется с помощью ввода искомого значения или его фрагмента в поле **«Поиск»**, расположенное в левом углу заголовка таблицы.

8 КОНТРОЛЬ ПРИЛОЖЕНИЙ И ДОМЕНОВ

Для перехода в раздел **«Контроль приложений и доменов»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«Контроль приложений и доменов»** (см. Рисунок – Окно настроек службы «Контроль приложений и доменов»).

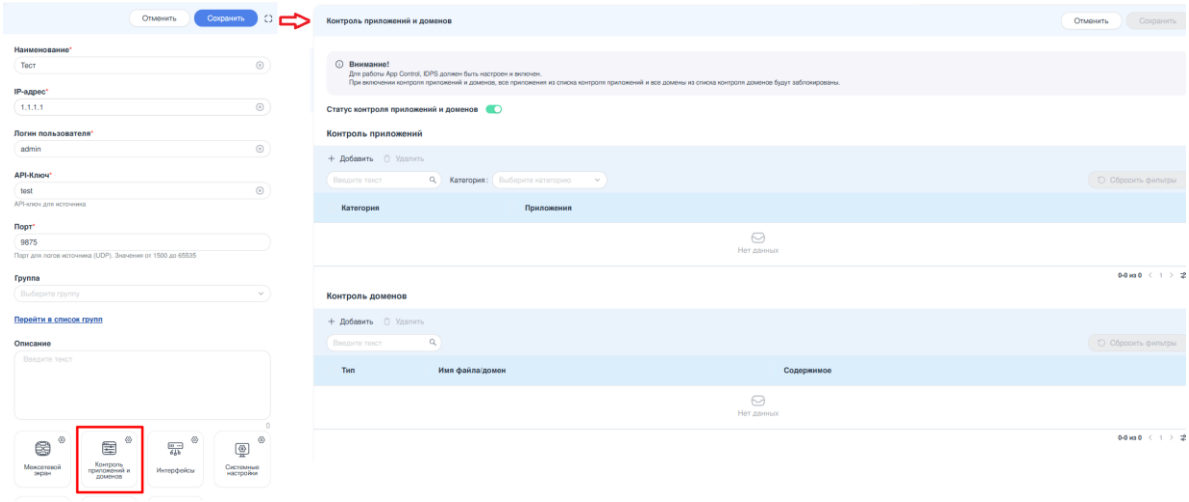


Рисунок – Окно настроек службы «Контроль приложений и доменов»

Применение и сохранение настроек

После завершения настройки всех необходимых параметров в разделе **«Контроль приложений и доменов»** необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Контроль приложений и доменов»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

Только после успешного подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

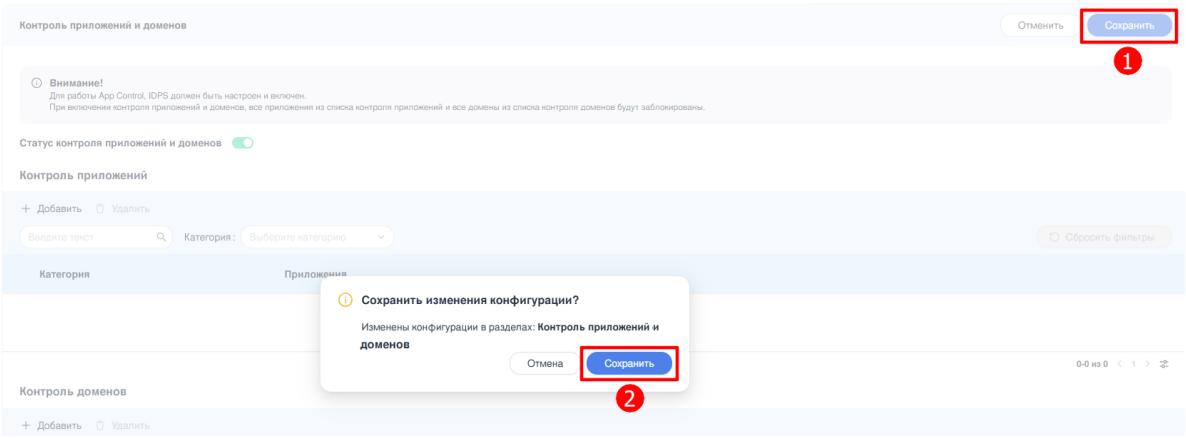


Рисунок – Применение и сохранение настроек

При необходимости отменить все неприменённые настройки следует нажать **кнопку «Отмена»**, расположенную в верхнем правом углу заголовка раздела **«Контроль приложений и доменов»**. В этом случае конфигурация раздела **«Контроль приложений и доменов»** будет откатана к последнему сохранённому состоянию.

8.1 Контроль приложений

Служба **«Контроль приложений»** предназначена для идентификации и ограничения использования сетевых приложений в трафике, проходящем через систему **ARMA Стена**. Реализована возможность блокировки приложений по категориям, включая мессенджеры, социальные сети, облачные сервисы, игровые платформы и другие, на основе предопределённых правил фильтрации.

Поддерживаемые приложения приведены в таблице «Список приложений».

Таблица «Список приложений»

Категория	Приложение
Искусственный интеллект	deepseek
Букмекерские конторы	winline
Облачные ресурсы	digital-ocean
CRM-системы	bitrix24
Критптобиржи и кошельки	mining
Файлообменники	1337x.tw 4shared Internxt-drive adrive bit-comet bit-torrent box-com

Категория	Приложение
	dropsend e-donkey falcobrowser filecloud fileden filefactory filepost firestorage flash-get fotolub gnutella google-drive hightail jottacloud media-fire media-get mega my-files one-drive p-cloud sendanywhere sendspace smartfile soul-seek source-forge spider-oak sync-com transferbigfiles transferxl transfiles.ru vuze yandex-disk yunpan zona
Форумы и блоги	geeksforgeeks pikabu
Онлайнг-гемблинг	casino stoloto
Игровые платформы	battle-net ea epic fortnite

Категория	Приложение
	gameasy gog riot rockstar steam ubi xbox
Системы управления версиями	github gitlab
Почтовые сервисы	outlook yandex-mail
Карты и навигация	2-gis google-maps
Маркетплейсы	aliexpress wildberries
Мессенджеры	amazon-chime amo bop-up-messenger express-messenger ice-chat icq imoim rocket-chat skype tada-team tamtam tango team-speak telegram viber whatsapp xchat yandex-messenger zulip
Музыкальные стриминговые сервисы	spotify
Новостные ресурсы	abcnews new-york-post
Офисные приложения	google-docs

Категория	Приложение
Прочие приложения	ads anonymizer anonymox archive-org astrology avira-update bootsnipp botnets c2c codesandbox croxyproxy delivery-club dodopizza dr-web-update edadeal elma365 fasts-tunnel free-proxy-list freemybrowser from-doc-to-pdf ghostery gismeteo gosuslugi hi-ru howtogeek ideone jsbin jsfiddle kaspersky-update kproxy kraken local-xpose microsoft-store miro nalog news ngrok npr online-video-converter packetriot page-kite pastebin pdf-drive

Категория	Приложение
	phishing polycom portable-apps raketu smallpdf softonic speedify star-force stealthy-com symantec-update talk-me tapin-radio teletype trend-micro-update vexacion vpn-proxy-site w3schools ways-online word-press yandex-taxi yoomoney zerotier
Протоколы связи	ip-6-to-4 quic smb smtp syslog tftp xmpp
Удалённое управление	1c-connect aeroadmin alpemix ammyy-admin anydesk get-screen jump-desktop log-me-in radmin simple-help sunlogin teleconsole ultra-viewer

Категория	Приложение
Поисковые системы	onion-search-engine rambler
Социальные сети	camfrog dating discord facebook fandom flickr g-mail-chat imgur intranetus mirapolis-virtual-room my-own-conference odnoklassniki tik-tok tumblr vkontakte whereby
Видеосвязь	clickmeeting free-conference-call go-meet-now google-meet mts-link true-conf video-grace web-ex yandex-telemost
Видеохостинги	adults-18 amediateka ivi megomult msn-video okko real-player rutube twitch y-2-mate youtube
VPN	123-vpn 1clickvpn beepass-vpn

Категория	Приложение
	best-vpn-ssh browsec continent-ap cyber-ghost-vpn dot-vpn droid-vpn fly-vpn free-open-vpn hide-my-ip hola-vpn hoxx i-top-vpn openvpnssh systweak-vpn tcp-vpn thunder-vpn touch-vpn tuxler-vpn u-vpn ultra-vpn vpn-book vpn-city vpn-jantlt vpn-ki vpn-professional vpn-udp wireguard your-freedom-vpn
Сканеры уязвимостей	metasploit nmap

Функционал службы реализован с использованием системы **СОВ**, которая анализирует сетевой трафик и классифицирует типы используемых приложений на основе сигнатур и поведенческих шаблонов.

Фильтрация трафика с применением службы **«Контроль приложений»** выполняется только на тех сетевых интерфейсах, которые указаны в конфигурации **СОВ** и для которых установлен режим захвата трафика **IPS**.

Примечание:

Перед включением службы **«Контроль приложений»** необходимо выполнить предварительную настройку **СОВ**, указав используемые сетевые интерфейсы и установив режим захвата трафика в значение **IPS**.

На интерфейсах, где в **СОВ** установлен режим **IDS**, фильтрация трафика по службе **«Контроль приложений» не применяется**.

Добавление приложения к списку блокировки

Для добавления приложений в список блокируемых необходимо выполнить следующие действия:

1. Нажать **кнопку «+ Добавить»** в таблице **«Контроль приложений»**.
2. В открывшемся боковом окне **«Добавление категории»** указать следующие параметры:
   - в поле **«Категория»** выбрать необходимую категорию приложений из выпадающего списка;
   - в поле **«Приложения»** отметить одно или несколько приложений, подлежащих блокировке. Для включения в список всех приложений выбранной категории необходимо установить флажок в чек-боксе **«Заблокировать все приложения»**.
3. Нажать **кнопку «Добавить»**, чтобы включить выбранные приложения в список блокировки (см. Рисунок – Добавление приложений в список блокировки).

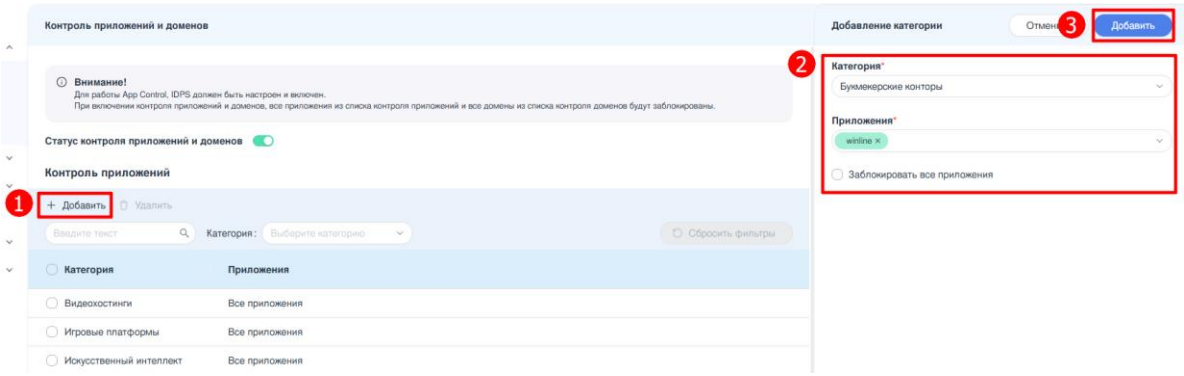


Рисунок – Добавление приложений в список блокировки

При необходимости повторить действия для добавления всех требуемых приложений.

Редактирование списка приложений

Для редактирования списка приложений в определённой категории необходимо нажать **ЛКМ** на строку с нужной категорией и в открывшейся боковой панели внести корректировки. По завершению нажать **кнопку «Изменить»**.

Удаление приложений из списка блокировки

Для удаления одной или нескольких категорий приложений из списка блокировки необходимо отметить их флажками в чек-боксах слева от

наименования и нажать **кнопку «Удалить»**. В открывшемся окне, подтвердить удаление.

Примечание:

При удалении всех приложений из списка блокировки, фильтрация трафика с помощью службы **«Контроль приложений»** становится невозможной.

Активация службы «Контроль приложений»

Для включения службы **«Контроль приложений»** требуется:

1. Включить и настроить **СОВ** в соответствии с заданными требованиями.
2. Добавить приложения, подлежащие блокировке, и перевести переключатель **«Статус контроля приложений и доменов»** в положение «Включено» (см. Рисунок – Включение службы «Контроль приложений» и сохранение настроек).

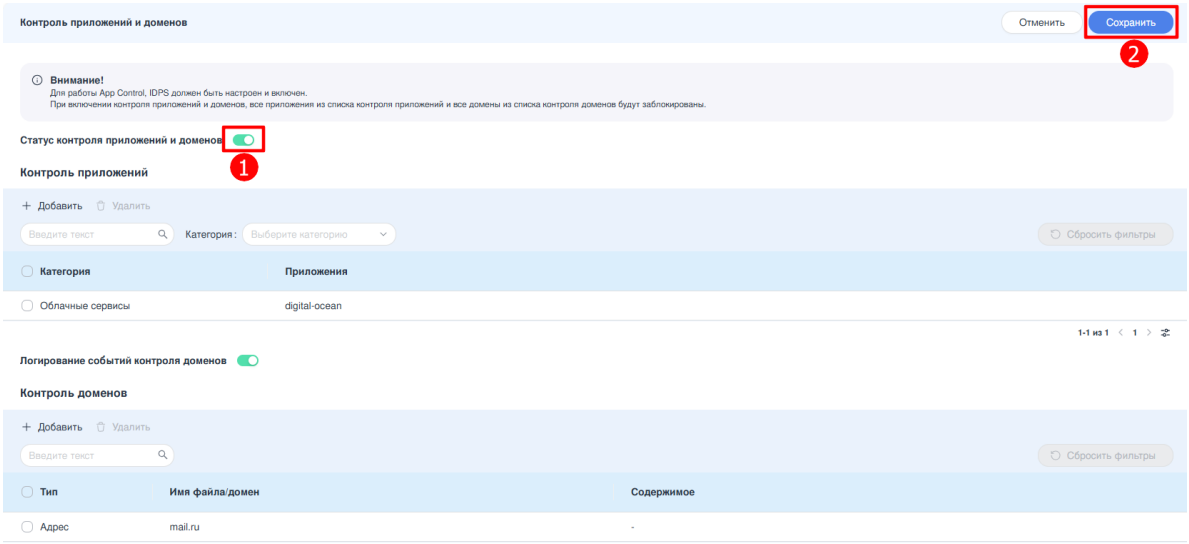


Рисунок – Включение службы «Контроль приложений»

После активации служба начинает обработку трафика согласно заданной политике.

8.2 Контроль доменов

Служба **«Контроль доменов»** предназначена для фильтрации сетевого трафика на основе доменных имён. Механизм блокировки реализован с использованием политик **МЭ**. Поддерживается добавление доменов как по одному, так и группами через загрузку текстового файла.

Служба **«Контроль доменов»** обладает более высоким приоритетом по сравнению с правилами **МЭ**. Если домен включён в список блокировки, доступ к нему запрещается даже при наличии разрешающего правила **МЭ**.

Добавление доменов в список блокировки

Для добавления доменов в список блокируемых необходимо выполнить следующие действия:

1. Нажать **кнопку «+Добавить»** в таблице **«Контроль доменов»**.
2. В открывшемся боковом окне **«Добавление домена»** выбрать способ добавления:
   - **Адрес** - указать имя блокируемого домена в поле **«Введите домен»**. Для добавления нескольких доменов следует последовательно нажимать **кнопку «Добавить»**, расположенную под полем ввода, и вводить каждое доменное имя отдельно.
   - **Файл** - загрузить список блокируемых доменов из текстового файла. Требования к файлу:
     - максимальный размер - 512 Кбайт;
     - файл должен иметь расширение «*.txt»;
     - каждый домен указывается в отдельной строке;
     - не допускается указывать протокол (http://, https://).

     Пример содержимого файла:

     ```
     ya.ru
     mail.ru
     vk.ru
     ```

     Загружаемые файлы сохраняются в директории **/config/files/configuration/app-control/domains/**.
3. После завершения ввода или загрузки данных нажать **кнопку «Добавить»** (см. Рисунок – Добавление доменов в список блокируемых).

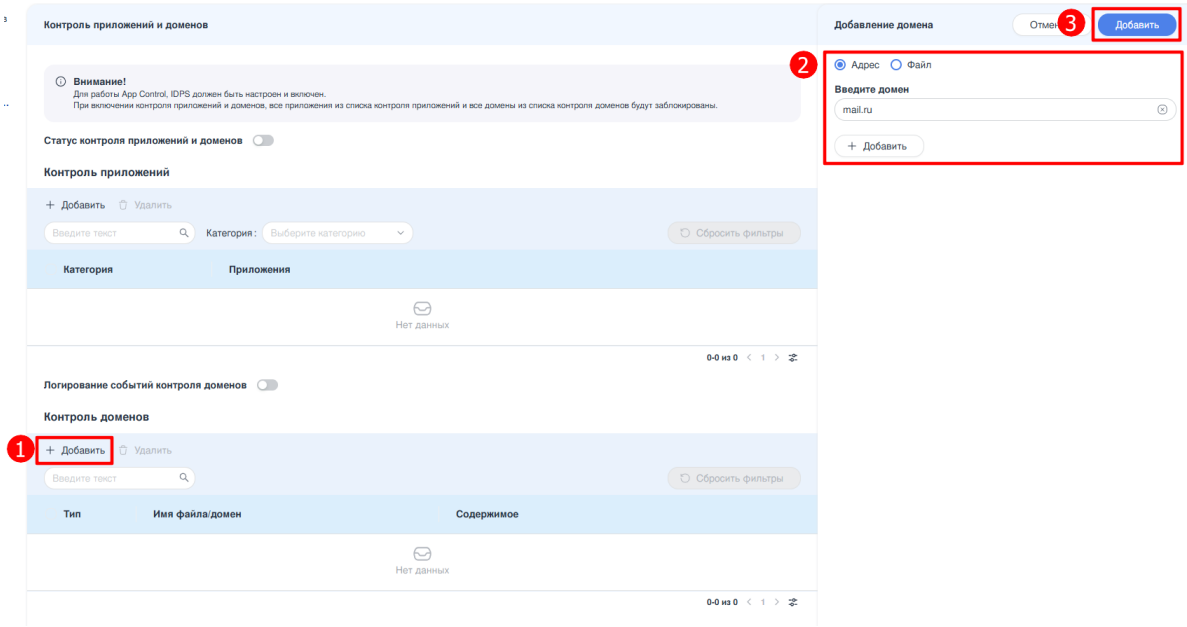


Рисунок – Добавление доменов в список блокируемых

Примечание:

Если DNS-сервер, используемый клиентом, расположенным за системой **ARMA Стена**, отличается от DNS-сервера, применяемого самой системой, то блокировка по всем IP-адресам домена не гарантируется. В этом случае часть ресурсов, связанных с доменом, может оставаться доступной, поскольку не подпадает под действие фильтрационной политики.

Удаление доменов из списка блокировки

Для удаления одного или нескольких доменов из списка блокировки требуется в таблице **«Контроль доменов»** установить флажки в чек-боксах слева от соответствующих записей (доменов или файлов со списками доменов) и нажать **кнопку «Удалить»**. В появившемся диалоговом окне подтвердить операцию.

Удалению подлежат только записи в конфигурационном файле. Загруженные текстовые файлы с доменами остаются в системе.

Активация службы «Контроль доменов»

Для включения службы **«Контроль доменов»** требуется:

1. Добавить домены, доступ к которым должен быть ограничен, в список блокируемых.
2. Установить переключатель **«Статус контроля приложений и доменов»** в положение «Включено» (см. Рисунок – Включение службы «Контроль приложений» и «Контроль доменов»).

После выполнения указанных действий служба начинает обработку трафика согласно политике фильтрации доменных имён.

Логирование событий

По умолчанию логирование событий, связанных с блокировкой доменов, отключено. Для его активации необходимо перевести переключатель **«Логирование событий контроля доменов»** в положение «Включено» и нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Контроль приложений и доменов»**.(см. Рисунок – Включение логирования событий контроля доменов).

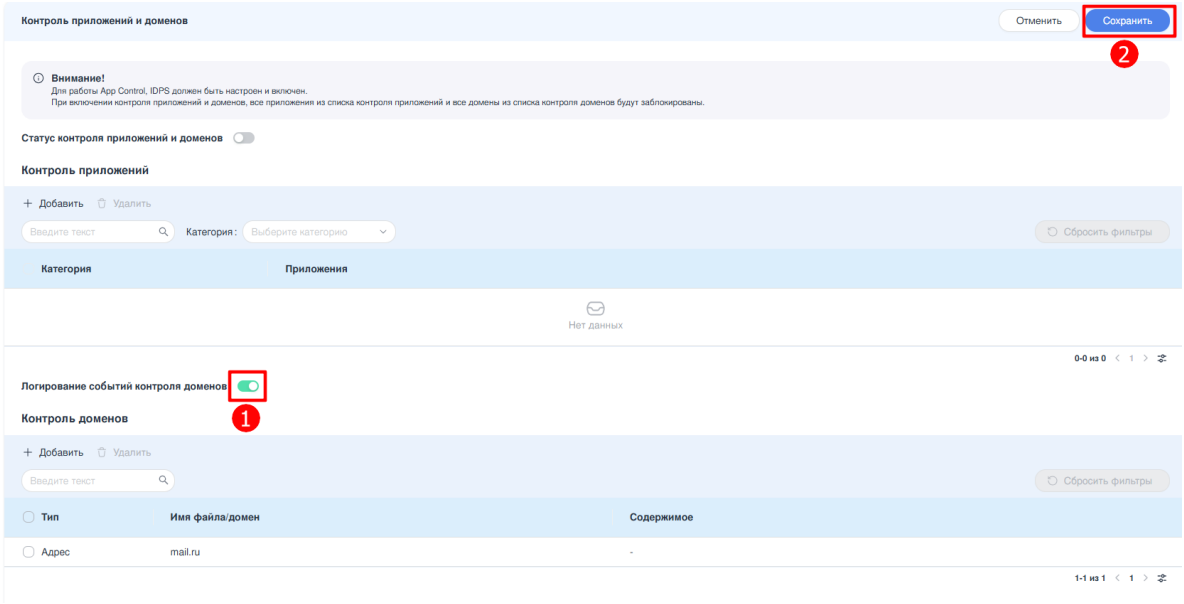


Рисунок – Включение логирования событий контроля доменов

После включения параметра все события, возникающие при попытках доступа к заблокированным доменам, фиксируются в глобальном журнале системы.

Для просмотра записей необходимо перейти в подраздел **«Логи межсетевого экрана»** раздела **«Настройки межсетевого экрана»**.

9 DR.WEB

Сервис Dr.Web позволяет с помощью веб-прокси осуществлять захват и сканирование проксируемого трафика HTTP и HTTPS на предмет наличия вирусов, вредоносного программного обеспечения и других угроз. Дополнительно сервис обеспечивает фильтрацию трафика в соответствии с базами данных нежелательных вредоносных ресурсов и тематических категорий, а также в соответствии с пользовательскими правилами, реализуемыми посредством модуля ICAPD.

Сервис Dr.Web интегрирован в систему **ARMA Стена**.

Примечание:

Для функционирования сервиса Dr.Web требуется ключ активации лицензии.

Для перехода в раздел «Dr.Web» необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«Dr.WEB»** (см. Рисунок – Окно настроек сервиса Dr.Web).

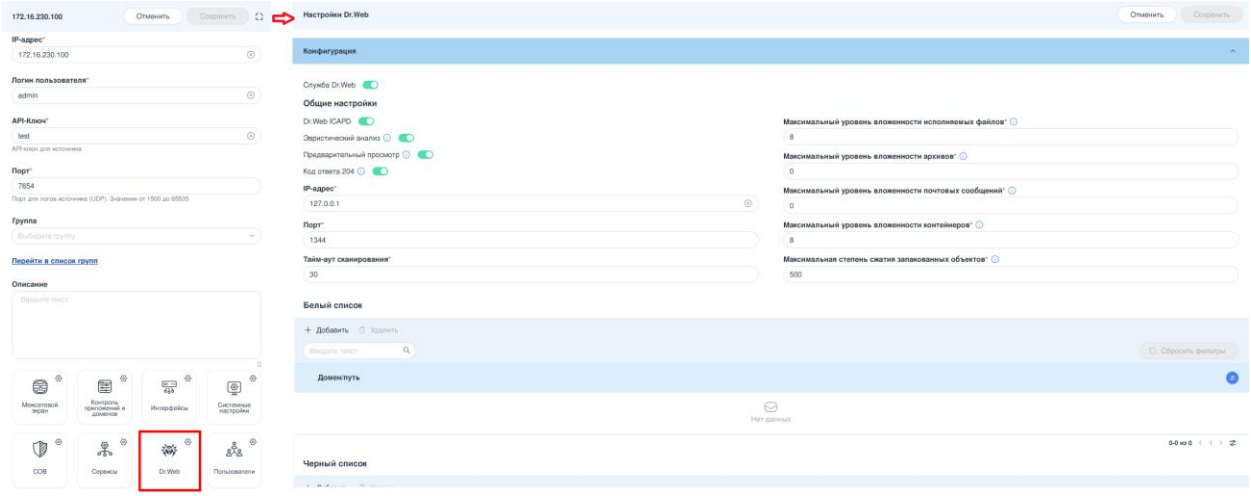


Рисунок – Окно настроек сервиса Dr.Web

Применение и сохранение настроек Dr.Web

После завершения настройки всех необходимых параметров в подразделах раздела **«Настройки Dr.Web»** необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Настройки Dr.Web»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

Только после успешного подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

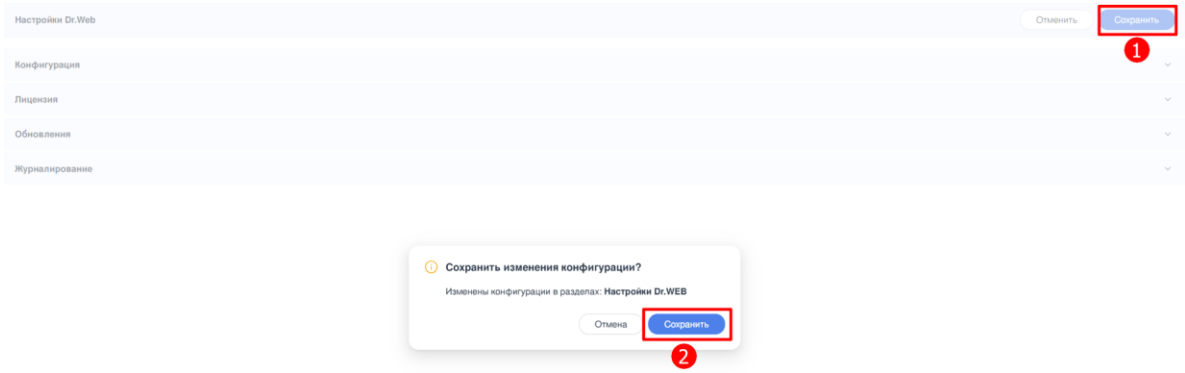


Рисунок – Применение и сохранение настроек

При необходимости отменить все неприменённые настройки следует нажать **кнопку «Отмена»**, расположенную в верхнем правом углу заголовка раздела **«Настройки Dr.Web»**. В этом случае конфигурация раздела **«Настройки Dr.Web»** будет откатана к последнему сохранённому состоянию.

9.1 Включение Dr.Web

Для включения сервиса Dr.Web необходимо выполнить следующие действия:

1. Настроить прокси-сервера в любой из доступных режимов (см. раздел **«Прокси-сервер»** руководства пользователя **ARMA Стена** CLI-интерфейс).
2. Выполнить настройку ICAP через CLI-интерфейс (см. раздел **«Параметры ICAP-клиента»** руководства пользователя **ARMA Стена** CLI-интерфейс):

```
# Пример настройки:
set service webproxy icap-client enable
set service webproxy icap-client remote-address 127.0.0.1
set service webproxy icap-client remote-port 1344
set service webproxy icap-client request location reqmod
set service webproxy icap-client response location respmod
# Применить и сохранить конфигурацию:
commit
save
```

3. В разделе **«Настройки Dr.Web»** веб-интерфейса перейти в подраздел **«Конфигурация»**.
4. Перевести переключатель **«Служба Dr.Web»** в активное состояние. Переключение параметра **«Dr.Web ICAPD»** выполняется автоматически в соответствии с состоянием переключателя **«Служба Dr.Web»**.

5. Нажать **кнопку «Сохранить»**, чтобы применить изменения и сохранить настройки (см. Рисунок – Включение сервиса Dr.Web и компонента Dr.Web ICAPD).

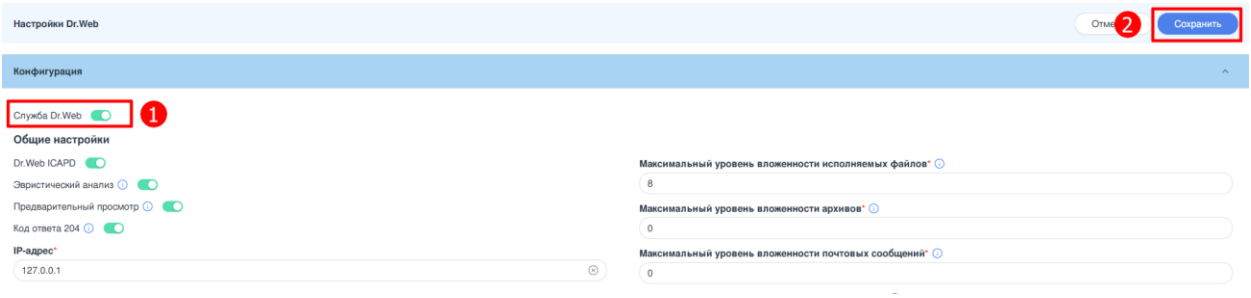


Рисунок – Включение сервиса Dr.Web и компонента Dr.Web ICAPD

9.2 Лицензирование Dr.Web

Примечание:

Перед активацией продукта **Dr.Web Gateway Security Suite** необходимо включить службу Dr.Web.

Права пользователя на использование копии **Dr.Web Gateway Security Suite** подтверждаются и регулируются лицензией, приобретённой пользователем у компании «Доктор Веб» или её партнёров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. https://license.drweb.com/agreement/), условия которого принимаются пользователем при активации **Dr.Web Gateway Security Suite** в системе **ARMA Стена**.

Имеется также возможность активировать для приобретённой копии **Dr.Web Gateway Security Suite** демонстрационный период. В этом случае, если не нарушены условия активации демонстрационного периода, пользователь получает право на полноценное использование **Dr.Web Gateway Security Suite** в течение демонстрационного периода.

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а в системе **ARMA Стена** с лицензией связывается специальный файл, регулирующий работу компонентов в соответствии с параметрами лицензии. Он называется лицензионным ключевым файлом. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый демонстрационным.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов **Dr.Web Gateway Security Suite** блокируются, кроме того, недоступен сервис регулярных обновлений вирусных баз с серверов обновлений компании «Доктор Веб».

После получения лицензионного ключевого файла для продукта **Dr.Web Gateway Security Suite** необходимо перенести его в систему **ARMA Стена**. Для этого следует выполнить следующие действия:

1. В разделе **«Настройки DrWEB»** перейти в подраздел **«Лицензия»**.
2. В поле **«Файл ключа лицензии:»** нажать **кнопку «Загрузить»**.
3. В открывшемся окне выбрать лицензионный ключевой файл Dr.Web и нажать в окне **кнопку «Открыть»** (см. Рисунок – Лицензирования Dr.Web)

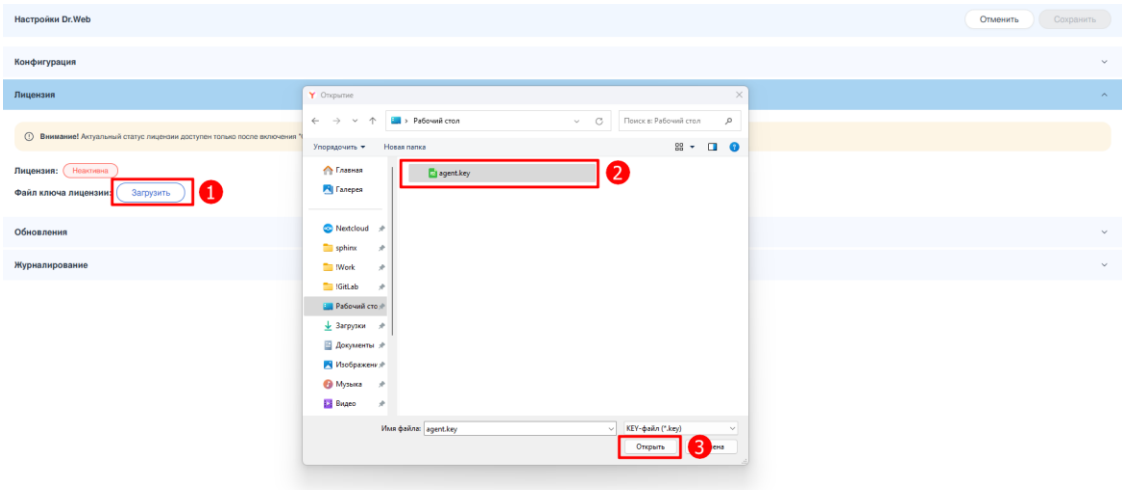


Рисунок – Лицензирования Dr.Web

4. После успешной загрузки ключевого файла статус лицензии в поле **«Лицензия»** изменится на **«Активна»**, и будет отображена информация о сроке действия лицензии (см. Рисунок – Период действия лицензии Dr.Web).

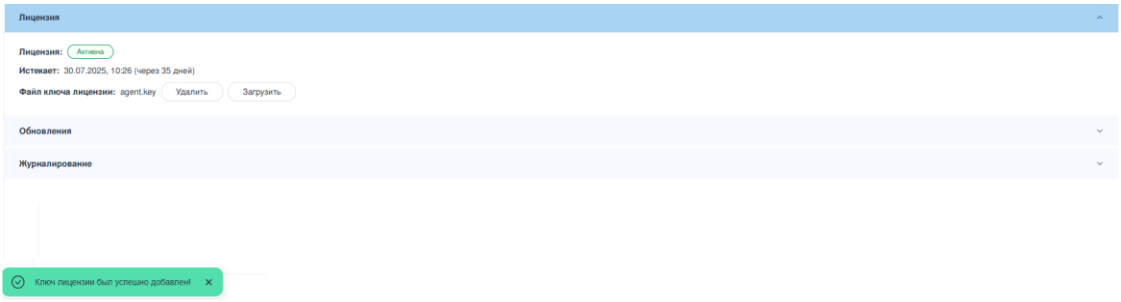


Рисунок – Период действия лицензии Dr.Web

Примечание:

Ключевой файл Dr.Web хранится в каталоге **/config/files/configuration/third-party/service/drweb/gss/license/**.

Удаление лицензии Dr.Web

При необходимости удаления лицензии Dr.Web следует перейти в подраздел **«Лицензия»** и нажать **кнопку «Удалить»** в поле **«Файл ключа лицензии»**. В появившемся диалоговом окне подтвердить удаление лицензии, нажав **кнопку «Удалить»** (см. Рисунок – Удаление лицензии Dr.Web). После выполнения

данной операции лицензия Dr.Web будет деактивирована, а ключевой файл физически удалён из системы **ARMA Стена**.

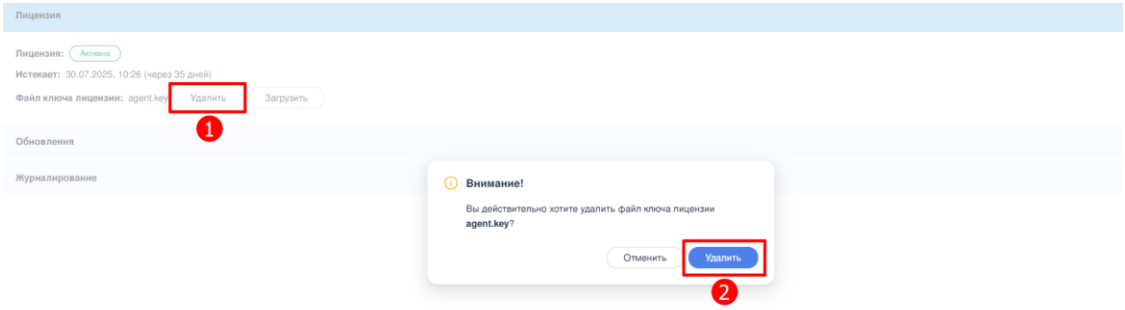


Рисунок – Удаление лицензии Dr.Web

9.3 Конфигурация Dr.Web ICAPD

Компонент Dr.Web ICAPD использует протокол ICAP (Internet Content Adaptation Protocol, RFC 3507) для взаимодействия с внешним по отношению к Dr.Web прокси-сервером, обслуживающим соединения узлов локальной сети с веб-серверами по протоколу HTTP/HTTPS.

Компонент Dr.Web ICAPD предназначен для подключения по протоколу ICAP к прокси-серверу системы **ARMA Стена**, установленному на шлюзе, через который пользователи локальной сети осуществляют выход в интернет. Прокси-сервер использует Dr.Web ICAPD в качестве внешнего фильтра, передавая ему на анализ как HTTP-запросы пользователей, так и ответы от удалённых веб-серверов.

Если доступ к ресурсу во внешней сети должен быть запрещён, либо передаваемые данные (запрос или ответ) содержат угрозу либо не могут быть проверены по причине возникшей ошибки, Dr.Web ICAPD инициирует возврат прокси-сервером пользователю HTML-страницы с информацией о блокировке.

Для настройки параметров компонента Dr.Web ICAPD необходимо в разделе **«Настройки DrWEB»** перейти в подраздел **«Конфигурация»** (см. Рисунок – Окно конфигурации Dr.Web ICAPD):

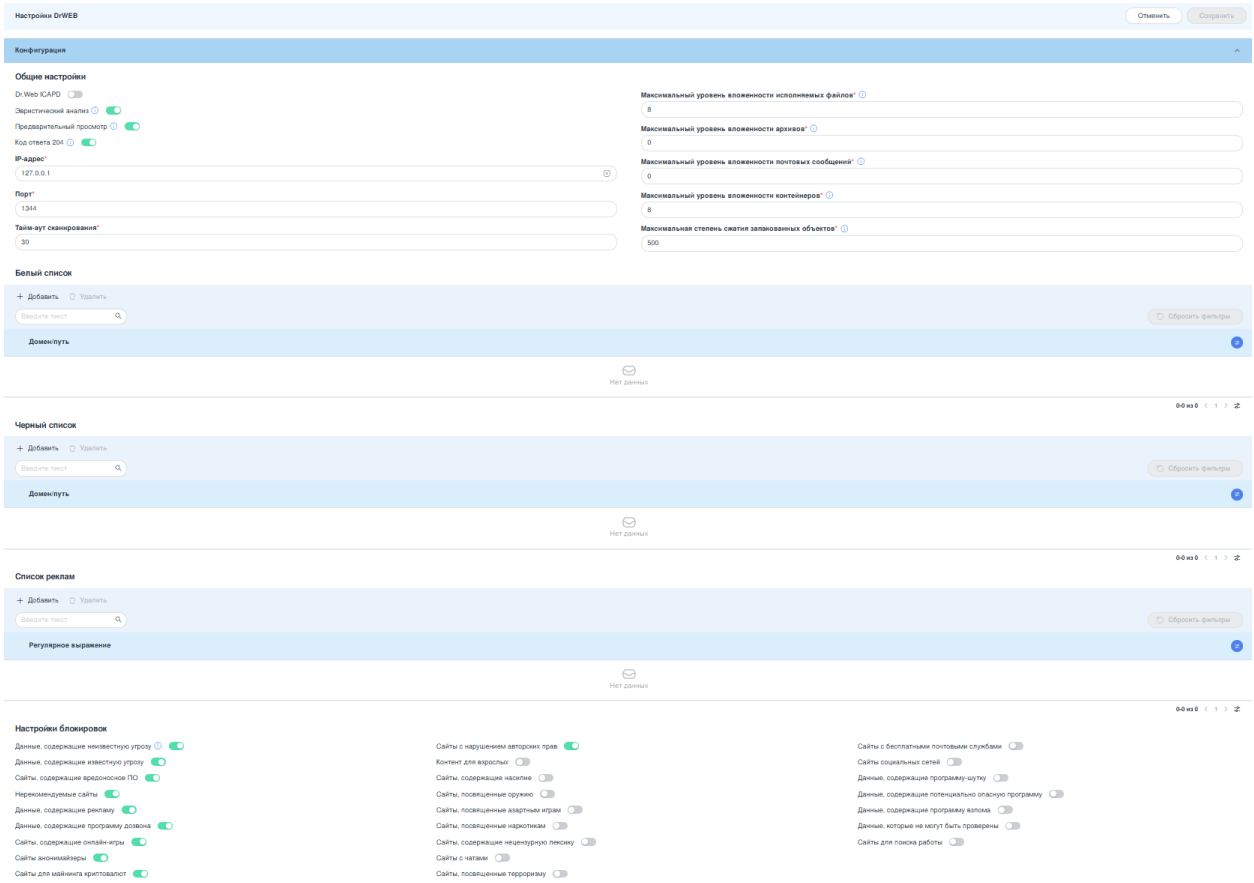


Рисунок – Окно конфигурации Dr.Web ICAPD

Подраздел **«Конфигурация»** состоит из следующих блоков:

- **«Общие настройки»**;
- **«Белый список»**;
- **«Чёрный список»**;
- **«Список реклам»**;
- **«Настройки блокировок»**;

9.3.1 Общие настройки

Блок настроек **«Общие настройки»** включает основные параметры конфигурации компонента Dr.Web ICAPD (см. Рисунок – Общие настройки Dr.Web ICAPD):

- **«Dr.Web ICAPD»** - включение или отключение компонента Dr.Web ICAPD. По умолчанию компонент отключён.
- **«Эвристический анализ»** - использовать или не использовать эвристический анализ для поиска неизвестных угроз. По умолчанию эвристический анализ включён.
- **«Предварительный просмотр»** - включить или отключить режим ICAP preview для Dr.Web ICAPD. Предварительный просмотр позволяет антивирусу быстро оценить содержимое файла без выполнения полного анализа. Основная цель — оптимизация производительности. Если файл

явно безопасен или не представляет интереса для детального анализа, антивирус может пропустить его полную проверку. По умолчанию предварительный просмотр включён.

- **«Код ответа 204»** - возвращать код ответа 204 не только в режиме ICAP preview. Параметр позволяет оптимизировать взаимодействие между прокси-сервером и Dr.Web ICAPD, избегая ненужной передачи данных, если файл или трафик признан безопасным. По умолчанию параметр включён.
- **«IP-адрес»** - IP-адрес в формате <x.x.x.x>, прослушиваемый Dr.Web ICAPD в ожидании подключений от прокси-серверов HTTP. По умолчанию используется IP-адрес «127.0.0.1».
- **«Порт»** - порт, прослушиваемый Dr.Web ICAPD в ожидании подключений от прокси-серверов HTTP. Возможно указать значение в диапазоне от «1» до «65535». По умолчанию используется порт «1344».
- **«Тайм-аут сканирования»** - значение тайм-аута в секундах на проверку одного файла по запросу Dr.Web ICAPD. Возможно указать значение в диапазоне от «1» до «3600». По умолчанию используется значение «30».
- **«Максимальный уровень вложенности исполняемых файлов»** - возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «8». Значение «0» указывает, что вложенные объекты не проверяются. Под запакованным объектом понимается исполняемый код, сжатый при помощи специализированных инструментов (UPX, PELock, PECompact, Petite, ASPack, Morphine и др.). Такие объекты могут включать другие запакованные объекты, в состав которых также могут входить другие запакованные объекты, и т. д. Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого объекты внутри объектов не будут проверяться.
- **«Максимальный уровень вложенности архивов»** - возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «0». Значение этого параметра устанавливает предельный уровень иерархии вложенности, после которого архивы внутри архивов не будут проверяться.

  Примечание:

  При значении параметра **«Максимальный уровень вложенности архивов»** равном **«0»** содержимое архивов не проверяется.

- **«Максимальный уровень вложенности почтовых сообщений»** - возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «0».

- **«Максимальный уровень вложенности контейнеров»** - значение максимального уровня вложенности для других типов объектов с вложениями (например, страницы HTML, файлы .jar и др.). Возможно указать значение в диапазоне от «0» до «1000». По умолчанию используется значение «8».
- **«Максимальная степень сжатия запакованных объектов»** - возможно указать значение в диапазоне от «2» до «10000». По умолчанию используется значение «500». Если степень сжатия объекта превысит указанную величину, он будет пропущен при проверке данных, инициированной по запросу Dr.Web ICAPD.

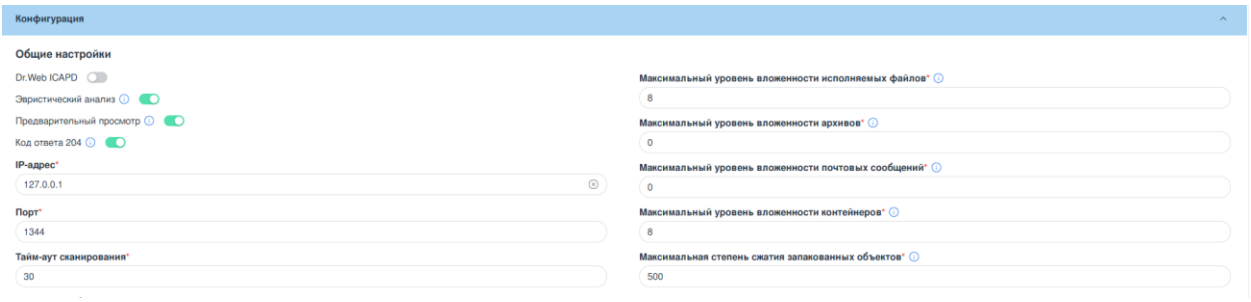


Рисунок – Общие настройки Dr.Web ICAPD

9.3.2 Белый список

Все домены, добавленные в белый список, будут доступны для пользователей без ограничений, независимо от их принадлежности к категориям нежелательных веб-ресурсов. Доступ распространяется также на все поддомены указанных доменов.

Для добавления домена в белый список необходимо выполнить следующие действия:

1. В панели инструментов блока **«Белый список»** нажать **кнопку «+ Добавить»**.
2. В открывшемся окне **«Добавить ресурс белого списка»** в поле **«Домен/путь»** ввести URL-адрес или путь к ресурсу. URL-адрес может содержать символы кириллического и латинского алфавитов, а также цифры. В пути допускается использование следующих символов: & - = ! " № ; % : ? * ( ) _ + < > [ ] { } / \ | , . ' @ # $ ^ ~ `.
3. Нажать **кнопку «Добавить»** для сохранения нового ресурса в список (см. Рисунок – Добавление домена в белый список).

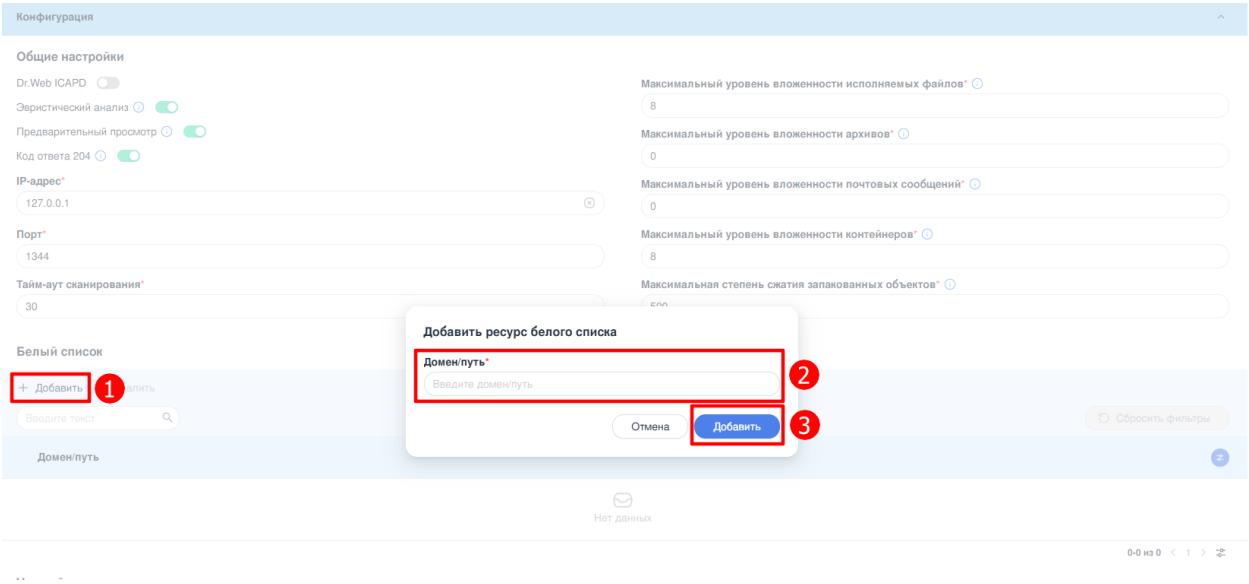


Рисунок – Добавление домена в белый список

Примечание:

Использование белого списка, определяется правилами управления доступом к веб-ресурсам, настроенными для **Dr.Web ICAPD**.

В правилах, заданных по умолчанию, обеспечивается предоставление доступа к доменам и их поддоменам, включённым в белый список, независимо от их принадлежности к блокируемым категориям веб-ресурсов, определённых в блоке **«Настройки блокировок»**. Кроме того, правила по умолчанию обеспечивают проверку данных, загружаемых с доменов из белого списка, на наличие потенциальных угроз.

Для редактирования домена в белом списке необходимо выбрать соответствующую запись, щёлкнув по ней **ЛКМ**. В открывшемся окне **«Изменить ресурс белого списка»** внести изменения в URL-адресе или пути к ресурсу. По завершению редактирования нажать **кнопку «Изменить»**.

Для удаления домена из белого списка необходимо выбрать одну или несколько соответствующих записей, установив флажок в чек-боксе слева от значения домена, и нажать **кнопку «Удалить»** на панели инструментов. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

9.3.3 Чёрный список

Все домены, добавленные в чёрный список, будут недоступны для пользователей, независимо от их классификации в рамках категорий нежелательных веб-ресурсов. Блокировка распространяется также на все поддомены указанных доменов.

Для добавления домена в чёрный список необходимо выполнить следующие действия:

1. В панели инструментов блока **«Чёрный список»** нажать **кнопку «+ Добавить»**.

2. В открывшемся окне **«Добавить ресурс чёрного списка»** в поле **«Домен/путь»** ввести URL-адрес или путь к ресурсу. URL-адрес может содержать символы кириллического и латинского алфавитов, а также цифры. В пути допускается использование следующих символов: & - = ! " № ; % : ? * ( ) _ + < > [ ] { } / \ | , . ' @ # $ ^ ~ `.
3. Нажать **кнопку «Добавить»** для сохранения нового ресурса в список (см. Рисунок – Добавление домена в чёрный список).

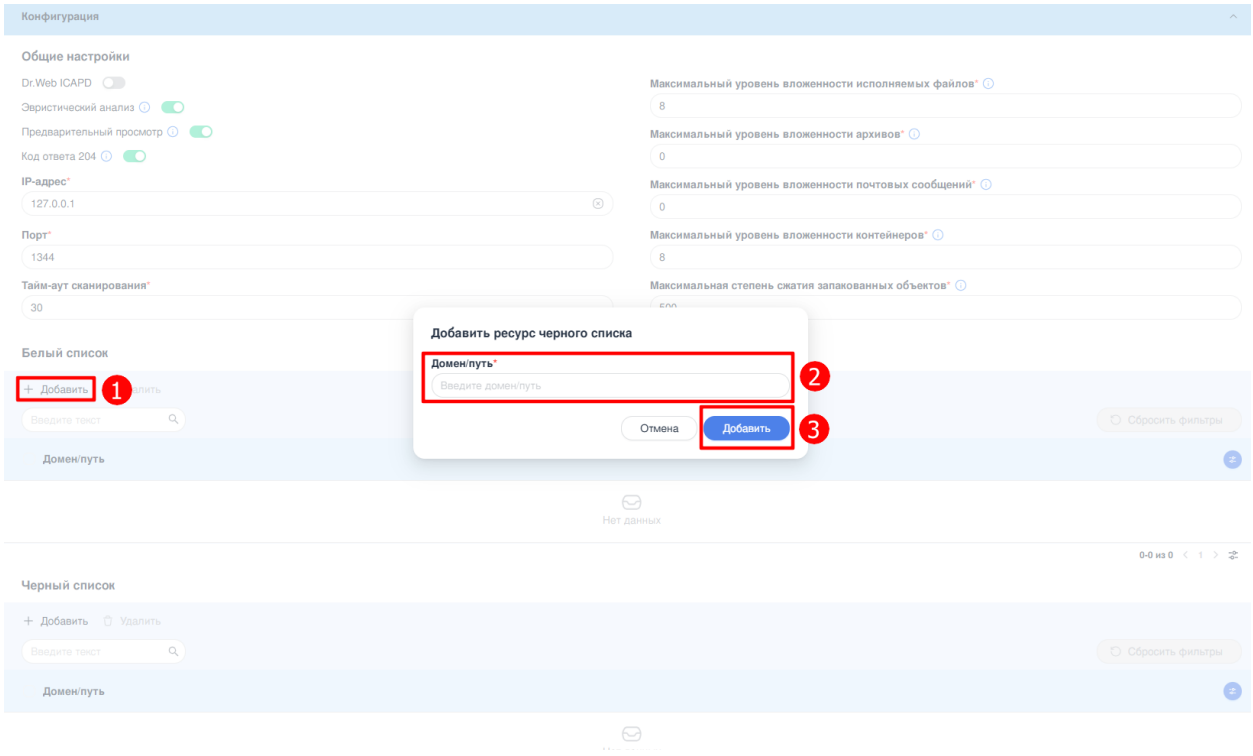


Рисунок – Добавление домена в чёрный список

Примечание:

Использование чёрного списка, определяется правилами управления доступом к веб-ресурсам, настроенными для **Dr.Web ICAPD**.

В соответствии с правилами, заданными по умолчанию, доступ к доменам и их поддоменам, указанным в чёрном списке, блокируется. В случае, если один и тот же домен фигурирует как в белом, так и в чёрном списке, применяется правило блокировки, и доступ к домену ограничивается.

Для редактирования домена в чёрном списке необходимо выбрать соответствующую запись, щёлкнув по ней **ЛКМ**. В открывшемся окне **«Изменить ресурс чёрного списка»** внести изменения в URL-адресе или пути к ресурсу. По завершению редактирования нажать **кнопку «Изменить»**.

Для удаления домена из чёрного списка необходимо выбрать одну или несколько соответствующих записей, установив флажок в чек-боксе слева от значения домена, и нажать **кнопку «Удалить»** на панели инструментов. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

9.3.4 Список реклам

Список регулярных выражений для описания веб-сайтов. URL, соответствующий любому из регулярных выражений, указанных в данном списке, классифицируется как рекламный.

Для добавления регулярных выражений в список реклам необходимо выполнить следующие действия:

1. В панели инструментов блока **«Список реклам»** нажать **кнопку «+ Добавить»**.
2. В открывшемся окне **«Добавить ресурс списка реклам»** в поле **«Регулярное выражение»** ввести значение регулярного выражения.
3. Нажать **кнопку «Добавить»** для сохранения нового регулярного выражения в список (см. Рисунок – Добавление домена в белый список).

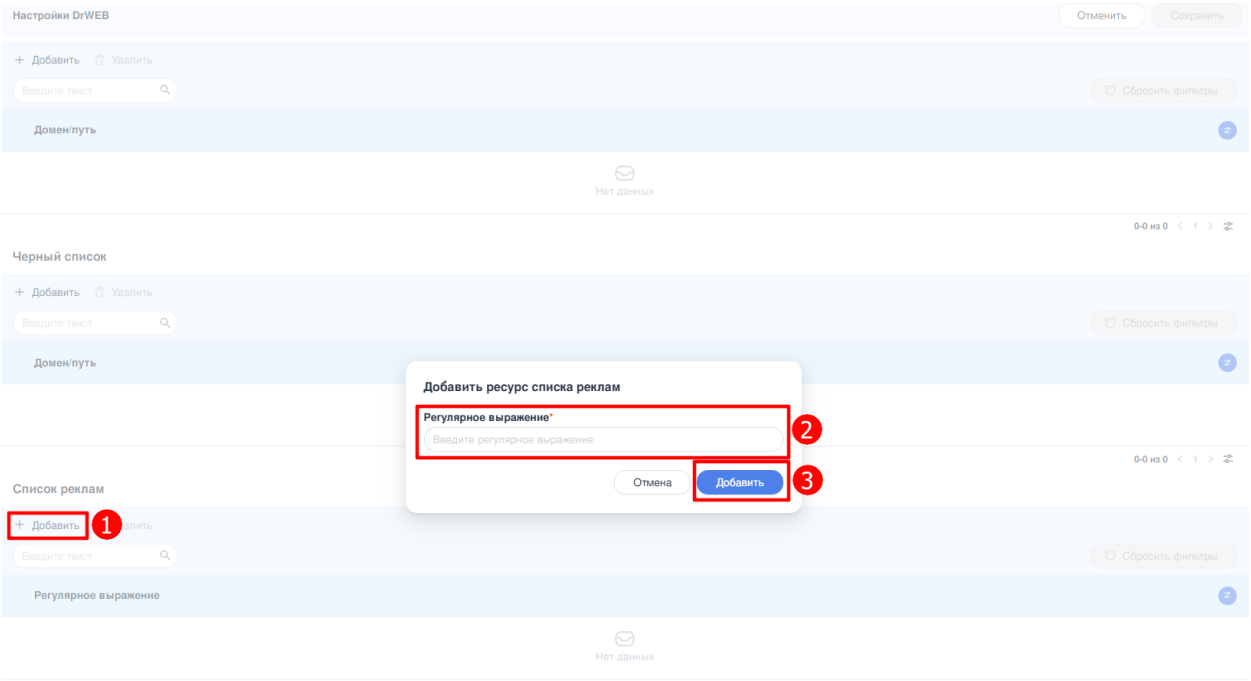


Рисунок – Добавление домена в белый список

Примечание:

Использование списка реклам определяется правилами управления доступом к веб-ресурсам, настроенными для **Dr.Web ICAPD**.

В правилах, заданных по умолчанию, доступ к URL из данного списка запрещается только в случае, если домены, на которые ссылаются эти URL, не добавлены в белый список.

Для редактирования регулярного выражения необходимо выбрать соответствующую запись, щёлкнув по ней **ЛКМ**. В открывшемся окне **«Изменить ресурс списка реклам»** внести изменения в поле **«Регулярное выражение»**. По завершению редактирования нажать **кнопку «Изменить»**.

Для удаления регулярного выражения из списка реклам необходимо выбрать одну или несколько соответствующих записей, установив флажок в чек-боксе слева от значения регулярного выражения, и нажать **кнопку «Удалить»** на панели инструментов. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

9.3.5 Настройки блокировок

Блок **«Настройки блокировок»** позволяет настроить запрет доступа к ресурсам по следующим критериям (см. Рисунок – Настройки блокировок Dr.Web ICAPD):

- **«Данные, содержащие неизвестную угрозу»** - по умолчанию включено;
- **«Данные, содержащие известную угрозу»** - по умолчанию включено;
- **«Сайты, содержащие вредоносное ПО»** - по умолчанию включено;
- **«Нерекомендуемые сайты»** - по умолчанию включено;
- **«Данные, содержащие рекламу»** - по умолчанию включено;
- **«Данные, содержащие программу дозвона»** - по умолчанию включено;
- **«Сайты, содержащие онлайн-игры»** - по умолчанию включено;
- **«Сайты анонимайзеры»** - по умолчанию включено;
- **«Сайты для майнинга криптовалют»** - по умолчанию включено;
- **«Контент для взрослых»** - по умолчанию отключено;
- **«Сайты, содержащие насилие»** - по умолчанию отключено;
- **«Сайты, посвященные оружию»** - по умолчанию отключено;
- **«Сайты, посвященные азартным играм»** - по умолчанию отключено;
- **«Сайты, посвященные наркотикам»** - по умолчанию отключено;
- **«Сайты, содержащие нецензурную лексику»** - по умолчанию отключено;
- **«Сайты с чатами»** - по умолчанию отключено;
- **«Сайты, посвященные терроризму»** - по умолчанию отключено;
- **«Сайты с бесплатными почтовыми службами»** - по умолчанию отключено;
- **«Сайты социальных сетей»** - по умолчанию отключено;
- **«Сайты с нарушением авторских прав»** - по умолчанию включено;
- **«Данные, содержащие программу-шутку»** - по умолчанию отключено;
- **«Данные, содержащие потенциально опасную программу»** - по умолчанию отключено;

- **«Данные, содержащие программу взлома»** - по умолчанию отключено;
- **«Данные, которые не могут быть проверены»** - по умолчанию отключено;
- **«Сайты для поиска работы»** - по умолчанию отключено;

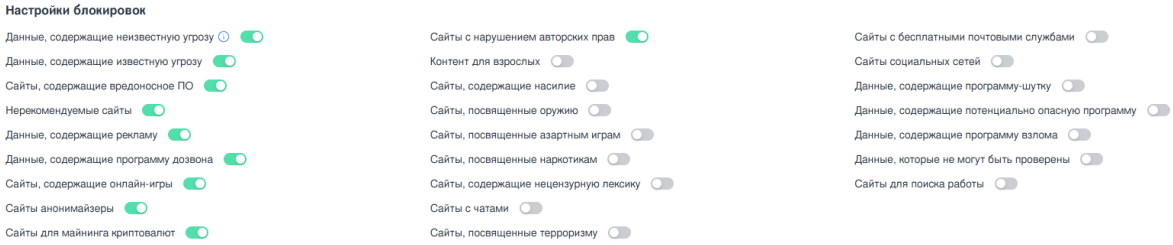


Рисунок – Настройки блокировок Dr.Web ICAPD

Примечание:

В случае исключения ресурса из списка блокируемых **Dr.Web**, при котором доступ к указанному ресурсу не восстанавливается, требуется выполнить перезапуск компонента **DrWeb ICAPD**. Для этого необходимо вручную отключить, а затем вновь включить компонент **DrWeb ICAPD**. Только после завершения данного действия обеспечивается корректное применение изменений в политике фильтрации и восстановление доступа к ресурсу.

9.4 Обновление Dr.Web

Служба обновления Dr.Web предназначен для получения обновлений вирусных баз и антивирусного ядра Dr.Web Virus-Finding Engine, базы категорий веб-ресурсов, а так же компонентов **Dr.Web Gateway Security Suite** с серверов обновлений компании «Доктор Веб».

В зависимости от наличия подключения к сети Интернет доступны следующие методы обновления:

- **обновление через сеть Интернет** — автоматическое получение и установка актуальных версий компонентов Dr.Web с использованием интернет-соединения;
- **ручное обновление без доступа к сети Интернет** — выполнение обновления путём импорта архива обновлений в систему **ARMA Стена**.

Для включения, настройки параметров и просмотра информации о последнем обновлении и текущей версии Dr.Web необходимо перейти в раздел **«Настройки Dr.Web»** и выбрать подраздел **«Обновления»** (см. Рисунок – Обновление Dr.Web).

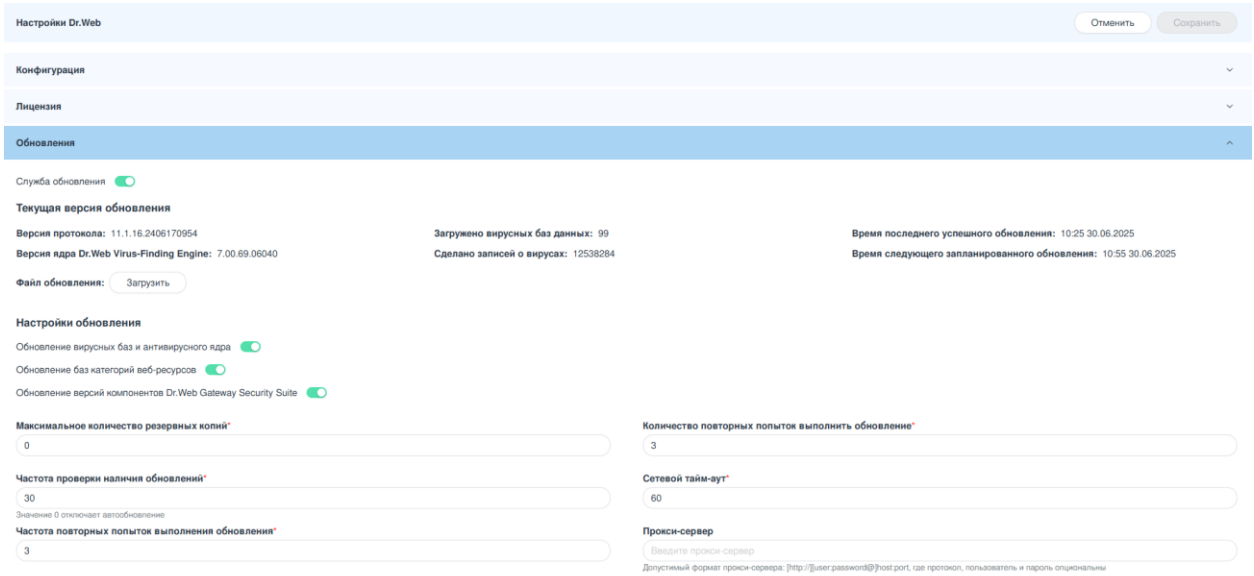


Рисунок – Обновление Dr.Web

По умолчанию служба обновления Dr.Web включена. При наличии активной лицензии и запущенной службы Dr.Web, компоненты антивируса обновляются автоматически каждые 30 минут, при условии доступности подключения к интернету. Для её отключения необходимо перевести переключать **«Служба обновления»** в неактивное состояние.

Предусмотрена возможность выборочного управления обновлениями, которая позволяет определить, какие компоненты Dr.Web будут включены в процесс обновления, а какие — исключены. Доступны следующие параметры обновления (см. Рисунок – Компоненты обновления Dr.Web):

- **Обновление вирусных баз и антивирусного ядра**
- **Обновление баз категорий веб-ресурсов**
- **Обновление версий компонентов Dr.Web Gateway Security Suite**

По умолчанию обновление всех перечисленных компонентов включено.

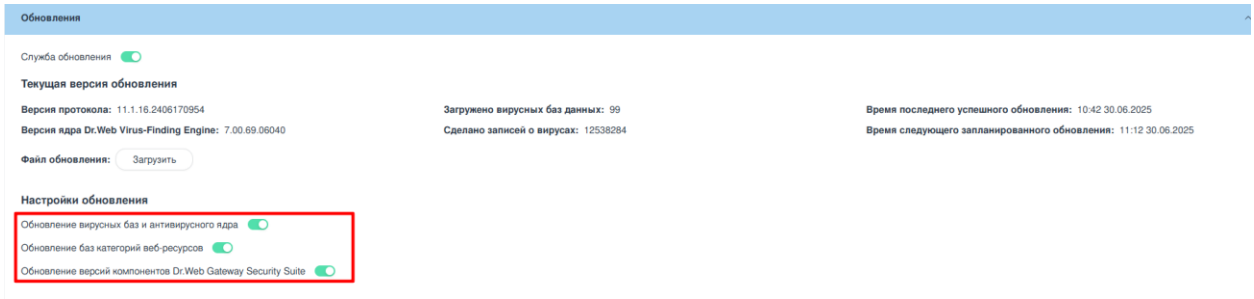


Рисунок – Компоненты обновления Dr.Web

В блоке **«Текущая версия обновления»** подраздела **«Обновления»** отображается информация о версиях установленных компонентов Dr.Web, а также указаны дата и время последнего и следующего обновления (см. Рисунок – Информация о версии и обновлениях Dr.Web).

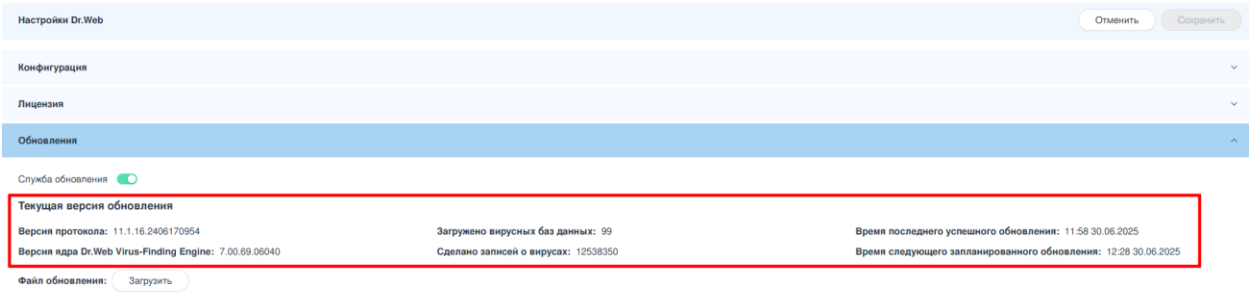


Рисунок – Информация о версии и обновлениях Dr.Web

9.4.1 Обновление Dr.Web через сеть Интернет

После включения и активации службы Dr.Web на устройстве **ARMA Стена** автоматически запускается процесс проверки и загрузки актуальных обновлений с установленным по умолчанию интервалом в 30 минут.

По умолчанию служба обновления Dr.Web использует следующий URL-адрес сервера обновлений: **url=http://update.geo.drweb.com/unix/1110/dws**.

Актуальный список URL-адресов серверов обновлений Dr.Web указан в файле **«update.drl»**, расположенном в каталоге **/var/opt/drweb.com/drl/dws/**.

Служба автоматического обновления Dr.Web поддерживает следующие параметры настройки (см. Рисунок – Настройки автоматического обновления Dr.Web):

1. **Максимальное количество резервных копий** - максимальное количество сохраняемых предыдущих версий обновляемых файлов. При превышении этой величины самая старая копия удаляется при очередном обновлении. Возможно указать значение в диапазоне от «0» до «9». Если значение параметра — «0», то предыдущие версии файлов для восстановления не сохраняются. По умолчанию используется значение «0».
2. **Частота проверки наличия обновлений** - значение частоты проверки наличия обновлений в минутах, т. е. период времени, который должен пройти от предыдущей успешной попытки подключения к серверам обновления до следующей попытки выполнить обновление. Возможно указание значения в диапазоне от «0» до «100». По умолчанию используется значение «30».

   Примечание:

   Значения «0» отключает автоматическое обновление компонентов службы Dr.Web через интернет.

3. **Частота повторных попыток выполнения обновления** - значение частоты повторных попыток выполнить обновление в минутах. Возможно указание значения в диапазоне от «1» до «30». По умолчанию используется значение «3».

4. **Количество повторных попыток выполнить обновление** - количество повторных попыток выполнить обновление с серверов обновления Dr.Web (предпринимаемых через промежутки времени, указанные в параметре **«Частота повторных попыток выполнения обновления»**), если предыдущая попытка обновления закончилась неудачей. Возможно указание значения в диапазоне от «0» до «9». Если значение параметра — «0», то повторные попытки выполнить неудавшееся обновление не производятся (следующее обновление будет производиться через период времени, указанный в параметре **«Частота повторных попыток выполнения обновления»**). По умолчанию используется значение «3».
5. **Сетевой тайм-аут** - тайм-аут на сетевые операции компонента при выполнении обновлений с серверов Dr.Web в секундах. Возможно указание значения в диапазоне от «5» до «75». Используется для ожидания продолжения обновления в случае временного обрыва соединения. Если оборванное сетевое соединение будет восстановлено до истечения тайм-аута, то обновление будет продолжено. По умолчанию используется значение «60».
6. **Прокси-сервер** - параметры подключения к прокси-серверу, который используется службой обновления Dr.Web для подключения к серверам обновлений Dr.Web (например, если непосредственное подключение к внешним серверам запрещено политиками безопасности сети).

   URL подключение к прокси-серверу имеет следующий формат:

   [<протокол>://][<пользователь>:<пароль>@]<хост>:<порт>

   где:

   - **<протокол>** — тип используемого протокола (в текущей версии доступен только http);
   - **<пользователь>** — имя пользователя для подключения к прокси-серверу;
   - **<пароль>** — пароль для подключения к прокси-серверу;
   - **<хост>** — адрес узла, на котором работает прокси-сервер (IP-адрес или имя домена, т. е. FQDN);
   - **<порт>** — используемый порт.

   Части URL **<протокол>** и **<пользователь>:<пароль>** могут отсутствовать. Адрес прокси-сервера **<хост>:<порт>** является обязательным. Если имя пользователя или пароль содержат символы **«@»**, **«%»** или **«:»**, то их следует заменить на соответствующие HEX-коды: *«@» - «%40»*, *«%» - «%25»* и *«:» - «%3A»*.

   Пример:

Настройка подключения к прокси-серверу, расположенному по адресу *10.26.127.0:3336*, с использованием учётной записи *«user@company.com»* и пароля *«passw%123:»*:

user%40company.com:passw%25123%3A@10.26.127.0:3336

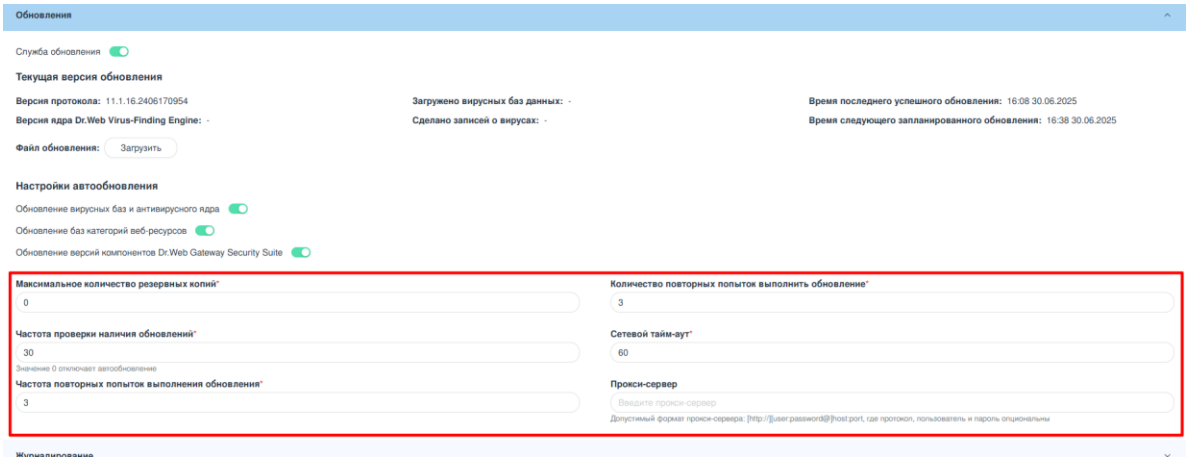


Рисунок – Настройки автоматического обновления Dr.Web

9.4.2 Ручное обновление Dr.Web без доступа к сети Интернет

Примечание:

Ручное обновление **Dr.Web** будет доступно в **ARMA MC** начиная с версии **2.0**. В версиях программного обеспечения **1.8** и **ниже** для выполнения ручного обновления **Dr.Web** без доступа к сети Интернет необходимо использовать интерфейс командной строки (**CLI**) непосредственно на устройстве **ARMA Стена**.

В случае недоступности подключения к сети Интернет обновление антивирусных компонентов Dr.Web возможно выполнить вручную с использованием архивного файла обновлений. Для этого необходимо выполнить следующие действия:

1. В подразделе **«Обновления»** в поле **«Файл обновления»** нажать **кнопку «Загрузить»**.
2. В открывшемся окне проводника выбрать необходимый архив обновления (см. Рисунок – Ручное обновление Dr.Web).

   Примечание:

   Поддерживаются только архивы форматов **tar** и **zip**.

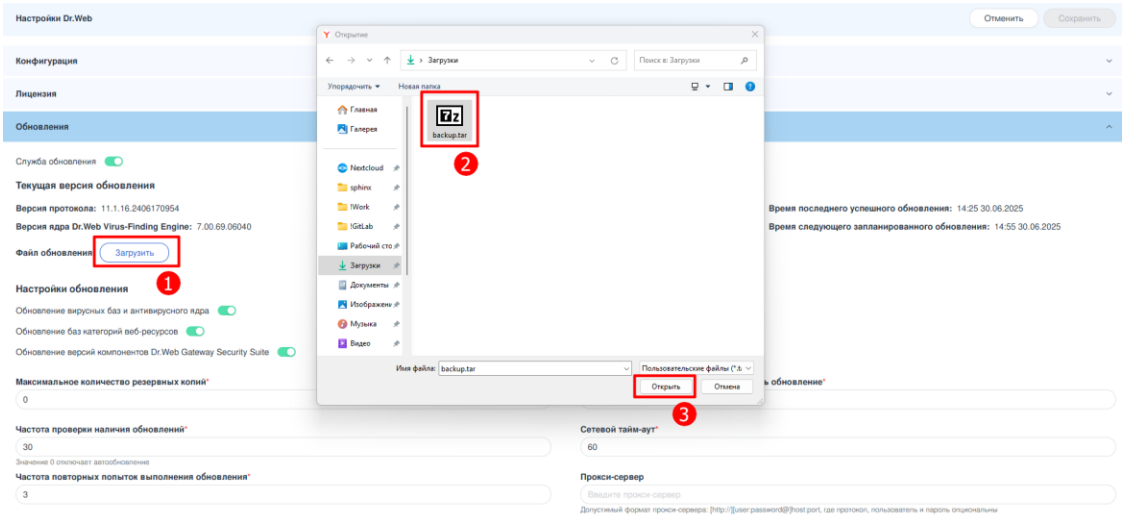


Рисунок – Ручное обновление Dr.Web

3. После выбора архива система автоматически разархивирует его и применит обновления. О начале процесса будет сообщено соответствующее уведомление в нижней левой части интерфейса: **«Загрузка обновления Dr.Web...»**.

4. По завершении обновления отобразится уведомление: **«Обновление Dr.Web успешно загружено»**.

9.5 Журналирование Dr.Web

Для настройки и просмотра событий, генерируемых сервисом Dr.Web, необходимо в разделе **«Настройки Dr.Web»** выбрать подраздел **«Журналирование»** (см. Рисунок – Журналирование Dr.Web).

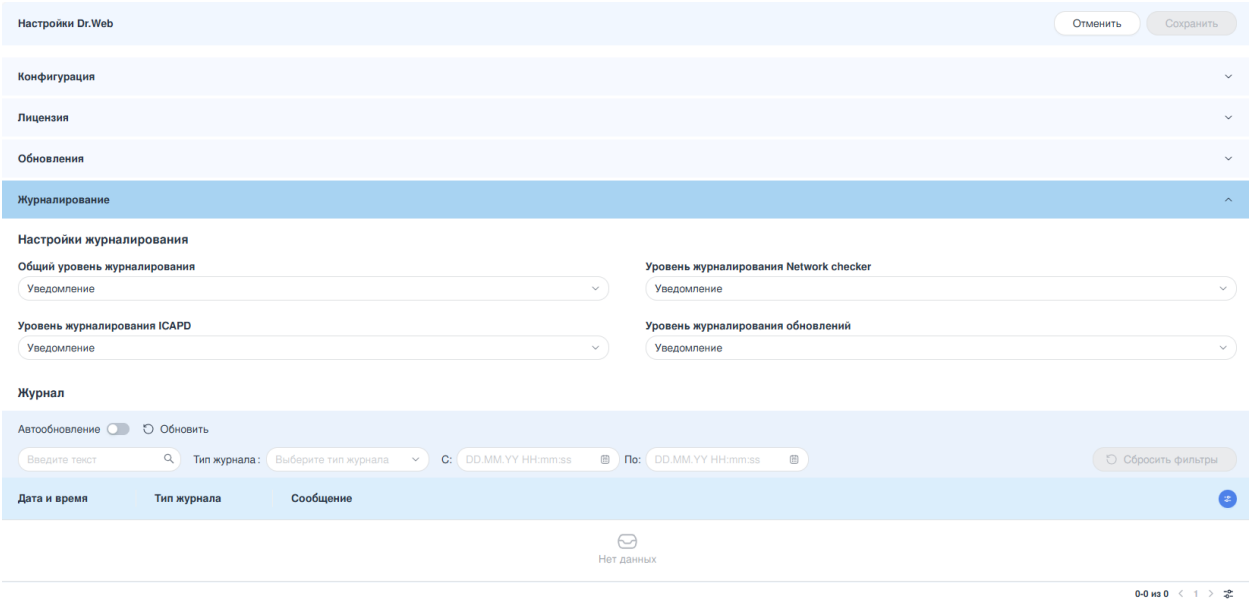


Рисунок – Журналирование Dr.Web

Блок **«Настройки журналирования»** позволяет настроить уровень детализации записей, сохраняемых в журнале, для следующих компонентов Dr.Web (см. Рисунок – Настройки журналирования Dr.Web):

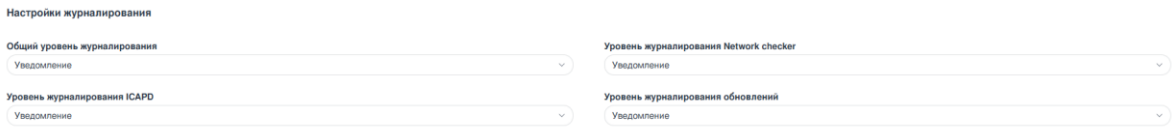


Рисунок – Настройки журналирования Dr.Web

- **«Общий уровень журналирования»** - значение уровня детализации записей для всех компонентов Dr.Web, если для конкретного компонента не указан собственный уровень журналирования. Возможно выбрать из выдающего списка следующие значения:
  - **Отладка** - самый подробный (отладочный) уровень. Выводятся все сообщения, а также отладочная информация;
  - **Информация** - выводятся все сообщения;
  - **Уведомления** - выводятся сообщения об ошибках, предупреждения, уведомления. *Значение используется по умолчанию*;
  - **Предупреждения** - выводятся сообщения об ошибках и предупреждения;
  - **Ошибка** - выводятся только сообщения об ошибках.
- **«Уровень журналирования ICAPD»** - значение уровня детализации записей событий связанных с работой компонента ICAPD (например, проверка трафика, блокировка доступа к сайтам, обработка запросов). Возможно выбрать из выдающего списка следующие значения:
  - **Отладка**;
  - **Информация**;
  - **Уведомления** - *используется по умолчанию*;
  - **Предупреждения**;
  - **Ошибка**.
- **«Уровень журналирования Network checker»** - значение уровня детализации записей событий связанных с проверкой сетевых подключений и трафика. Этот компонент отвечает за мониторинг сетевой активности, выявление подозрительных или потенциально опасных соединений и блокировку доступа к небезопасным ресурсам. Возможно выбрать из выдающего списка следующие значения:
  - **Отладка**;

- **Информация**;
- **Уведомления** - *используется по умолчанию*;
- **Предупреждения**;
- **Ошибка**.

- **«Уровень журналирования обновлений»** - значение уровня детализации записей событий связанных с работой компонента обновлений Dr.Web. Возможно выбрать из выдающего списка следующие значения:
  - **Отладка**;
  - **Информация**;
  - **Уведомления** - *используется по умолчанию*;
  - **Предупреждения**;
  - **Ошибка**.

Просмотр событий сервиса Dr.Web осуществляется в формате таблицы, состоящей из следующих столбцов:

- **«Дата и время»** - временная метка события.
- **«Тип журнала»** - отображает тип дополнительного фильтра, к которому относится данное событие.
- **«Сообщение»** - содержит описание произошедшего события.

В таблице **«Журнал» возможно настроить отображение столбцов. Для настройки отображения столбцов необходимо нажать **кнопку «Настройка столбцов»**  и выбрать требуемые столбцы из выпадающего списка. По умолчанию отображаются все доступные столбцы.

Обновление списка событий может выполняться двумя способами:

- **вручную**, с помощью соответствующей кнопки на панели инструментов таблицы;
- **автоматически**, с установленной периодичностью — 1 раз в 10 секунд.

При включении режима автоматического обновления ручное обновление становится недоступным. Кнопки управления обновлением находятся на панели инструментов таблицы **«Журнал»** (см. Рисунок – Обновление списка событий).

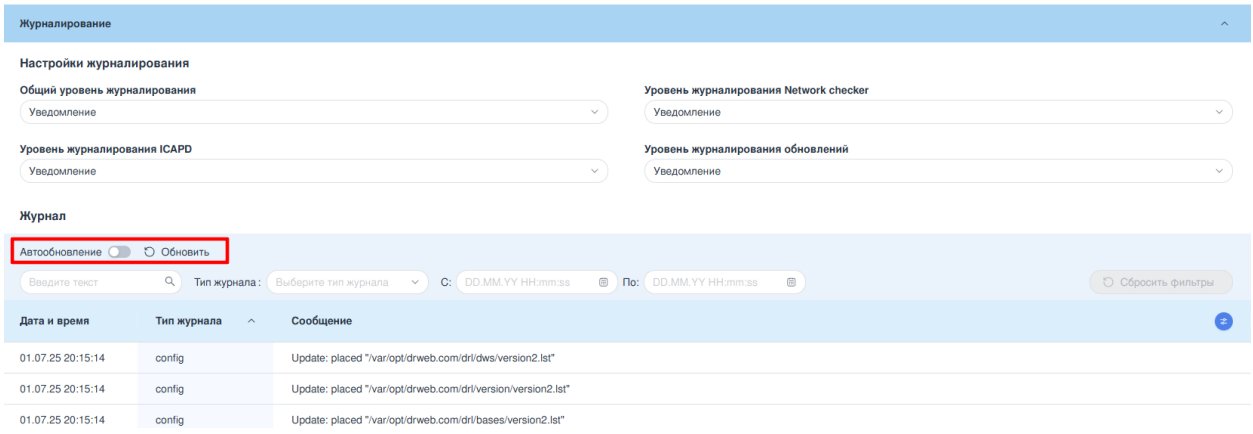


Рисунок – Обновление списка событий

Поиск и фильтрация

Блок фильтрации предназначен для отбора событий Dr.Web в соответствии с заданными пользователем критериями. По умолчанию блок фильтрации содержит следующие поля (см. Рисунок – Блок фильтрации):

- **«Поиск»**;
- **«Тип журнала»**;
- **«С»**;
- **«По»**;
- **кнопка «Сбросить фильтры»»**.

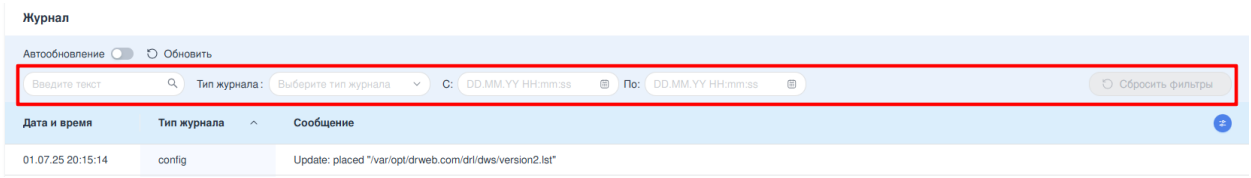


Рисунок – Блок фильтрации

Сквозной поиск по полям таблицы осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по всем столбцам таблицы.

Фильтрация по полю **«Тип журнала»** предназначено для выборки записей журналирования Dr.Web по типу события. Фильтрация позволяет выделить события, относящиеся к следующим типам:

- **config** - события, связанные с конфигурацией Dr.Web;
- **http** - события, связанные с обработкой HTTP-запросов/ответов через Dr.Web;
- **icapd** - события компонента Dr.Web ICAPD;
- **netcheck** - события сетевых проверок, например, соединений с серверами обновлений;

- **scan-engine** - события о работе сканирующего движка Dr.Web;
- **update** - события, связанные с обновлением Dr.Web;
- **url-check** - события проверки URL-адресов на предмет вредоносного содержимого.

Фильтрация по полю **«С»** позволяет отфильтровать записи по дате и времени события и задаёт начальный временной диапазон. После ввода даты и времени в таблице отобразятся лишь те события, где «Дата и время» совпадает или больше введённых в фильтр.

Фильтрация по полю **«По»** позволяет отфильтровать записи по дате и времени события и задаёт конечный временной диапазон. После ввода даты и времени в таблице отобразятся лишь те события, где «Дата и время» совпадает или меньше введённых в фильтр.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

Примечание:

В веб-интерфейсе установлено ограничение на выгрузку событий журнала Dr.Web — **не более 10 000 записей**.

Сбор логов осуществляется в обратном порядке, начиная с самых новых записей. При наличии фильтра по дате и времени, сбор логов производится начиная с указанного момента, до достижения заданного количества записей или максимального предела в 10 000 записей.

10 СЕРВИСЫ

10.1 Ретрансляция DHCP

Ретрансляция DHCP применяется в ситуациях, когда у клиента DHCP нет возможности напрямую обратиться к серверу DHCP, например, если они находятся в разных широковещательных доменах. В таких случаях ретрансляция DHCP позволяет избежать необходимости установки и запуска DHCP-сервера в каждом широковещательном домене.

ARMA Стена возможно сконфигурировать для работы в качестве DHCP-ретранслятора. После настройки агента ретрансляции DHCP он начинает перенаправлять DHCP-запросы на внешний DHCP-сервер. Агент ретрансляции DHCP поддерживает работу с адресами IPv4 и IPv6.

На всех интерфейсах, используемых для ретрансляции DHCP, должны быть настроены IP-адреса.

Применение и сохранение настроек ретрансляции DHCP

После настройки параметров необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»** в правом верхнем углу заголовка раздела **«Сервисы»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

После подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

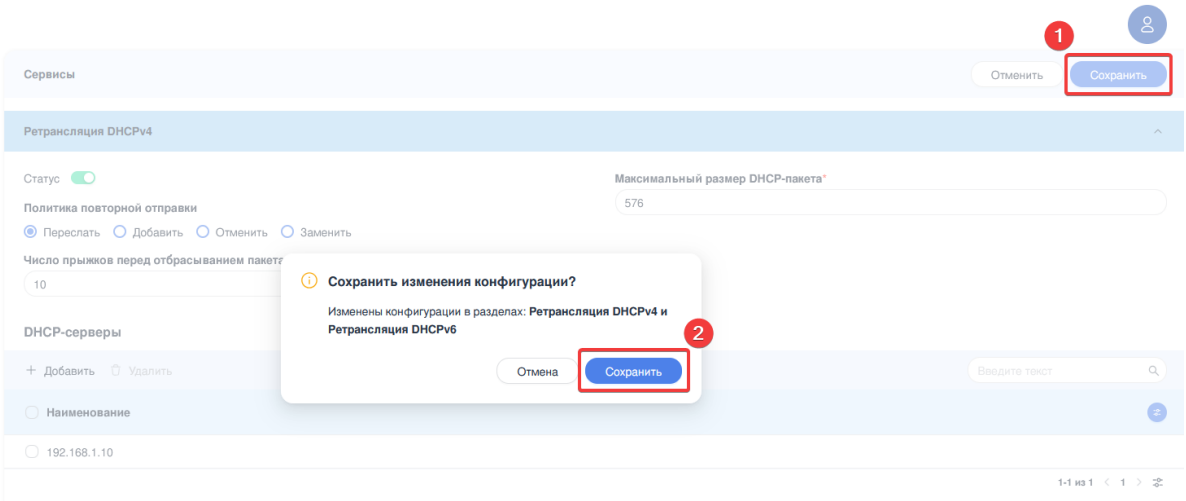


Рисунок – Применение и сохранение настроек

Для отмены всех неприменённых настроек необходимо нажать **кнопку «Отмена»** в верхнем правом углу заголовка раздела **«Сервисы»**. В этом случае

конфигурация раздела **«Сервисы»** вернется к последнему сохранённому состоянию.

10.1.1 Ретрансляция DHCPv4

Для настройки параметров ретрансляции DHCPv4 необходимо перейти в раздел **«Ретрансляция DHCPv4»**, расположенный в меню **«Сервисы» — «Ретрансляция DHCPv4»** (см. Рисунок – Ретрансляция DHCPv4).

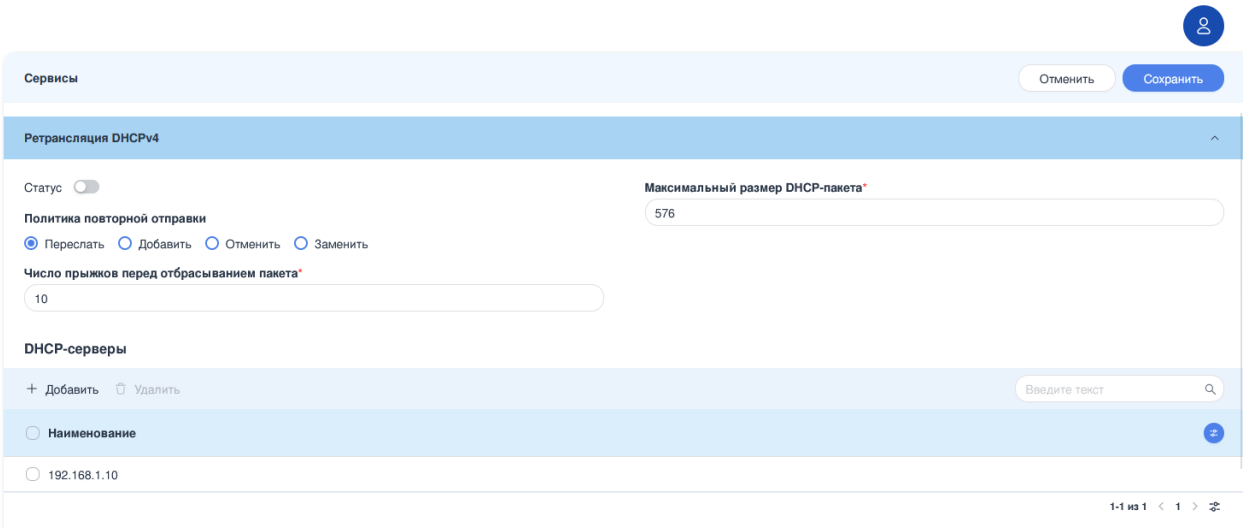


Рисунок – Ретрансляция DHCPv4

10.1.1.1 Основные настройки

Перед запуском службы ретрансляции DHCP необходимо предварительно указать следующие настройки:

- **IP-адрес** DHCP-сервера;
- **прослушиваемый интерфейс**, на котором будут прослушиваться DHCP-запросы;
- **upstream-интерфейс**, через который DHCP-запросы от клиентов будут передаваться на DHCP-сервер.

DHCP-сервера

Для добавления **DHCP-сервера** необходимо в разделе **«Ретрансляция DHCPv4»** нажать **кнопку «+Добавить»** и в открывшемся окне «Добавление DHCP-сервера» ввести IP-адрес DHCP-сервера в формате IPv4. (см. Рисунок – Добавление DHCP-сервера).

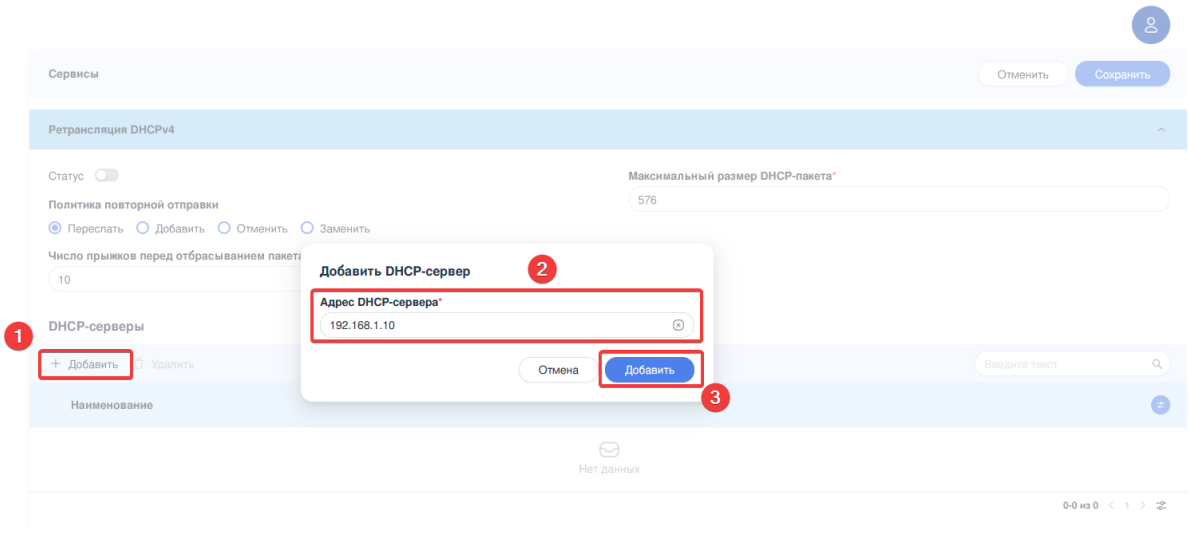


Рисунок – Добавление DHCP-сервера

Для удаления DHCP-сервера необходимо выбрать один или несколько DHCP-серверов, установив флажок в чек-боксе слева от IP-адреса DHCP-сервера, и нажать **кнопку «Удалить»**. В открывшемся окне необходимо подтвердить удаление, нажав **кнопку «Удалить»** (см. Рисунок – Удаление DHCP сервера).

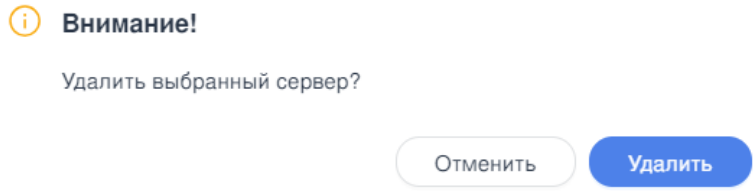


Рисунок – Удаление DHCP сервера

В случае если после удаления DHCP-сервера не останется ни одного сервера, а служба ретрансляции DHCP будет включена, программа выдаст предупреждающее сообщение об отключении данной службы (см. Рисунок – Предупреждение об отключении службы ретрансляции DHCP). Нажатие **кнопки «Удалить»** приведёт к деактивации службы ретрансляции DHCP.

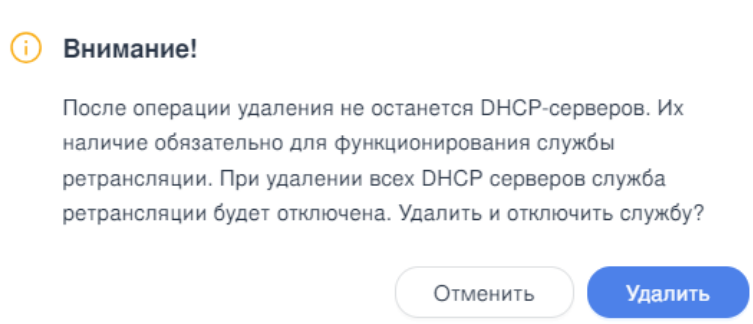


Рисунок – Предупреждение об отключении службы ретрансляции DHCP

Настройки прослушиваемого/upstream интерфейса

Для добавления интерфейсов ретрансляции DHCP-сообщений необходимо в разделе **«Интерфейсы ретрансляции DHCP-сообщений»** нажать **кнопку**

«+Добавить» и в открывшемся боковом окне выбрать из списка интерфейс и назначить ему роль (см. Рисунок – Добавления интерфейсов ретрансляции DHCP-сообщений).

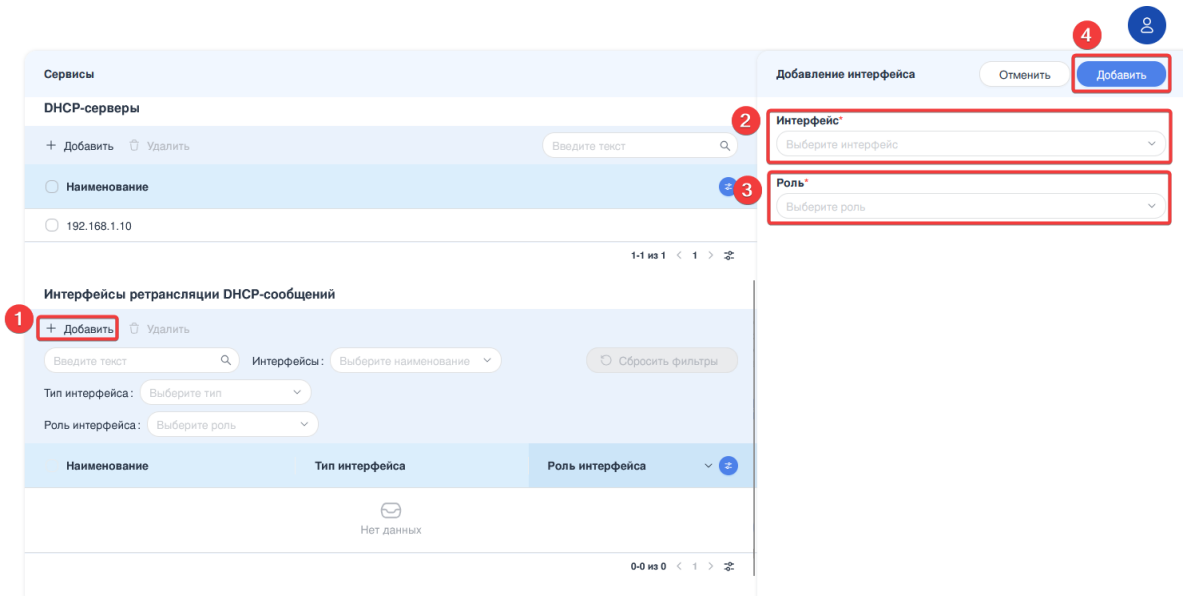


Рисунок – Добавления интерфейсов ретрансляции DHCP-сообщений

Для удаления интерфейсов ретрансляции DHCP-сообщений необходимо выбрать один или несколько интерфейсов в разделе **«Интерфейсы ретрансляции DHCP-сообщений»**, установив флажок в чек-боксе слева от имени интерфейса, и нажать **кнопку «Удалить»**. В открывшемся окне необходимо подтвердить удаление, нажав **кнопку «Удалить»**.

Примечание:

В случае, если после удаления все оставшиеся интерфейсы будут выполнять одну и ту же функцию (либо только «Прослушиваемый интерфейс», либо только «Upstream-интерфейс»), и при этом будет включена ретрансляция, система выдаст предупреждение об отключении службы ретрансляции (см. Рисунок – Подтвердить удаление интерфейса и отключение службы ретрансляции):

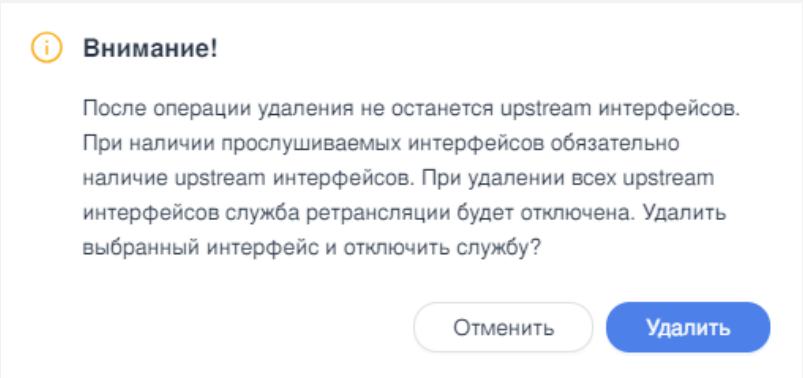


Рисунок – Подтвердить удаление интерфейса и отключение службы ретрансляции

Запуск службы ретрансляции DHCP.

Для запуска службы ретрансляции DHCP необходимо перевести **переключатель «Статус»** в положение включено и нажать **кнопку «Сохранить»** (см. Рисунок – Включение службы ретрансляции DHCP).

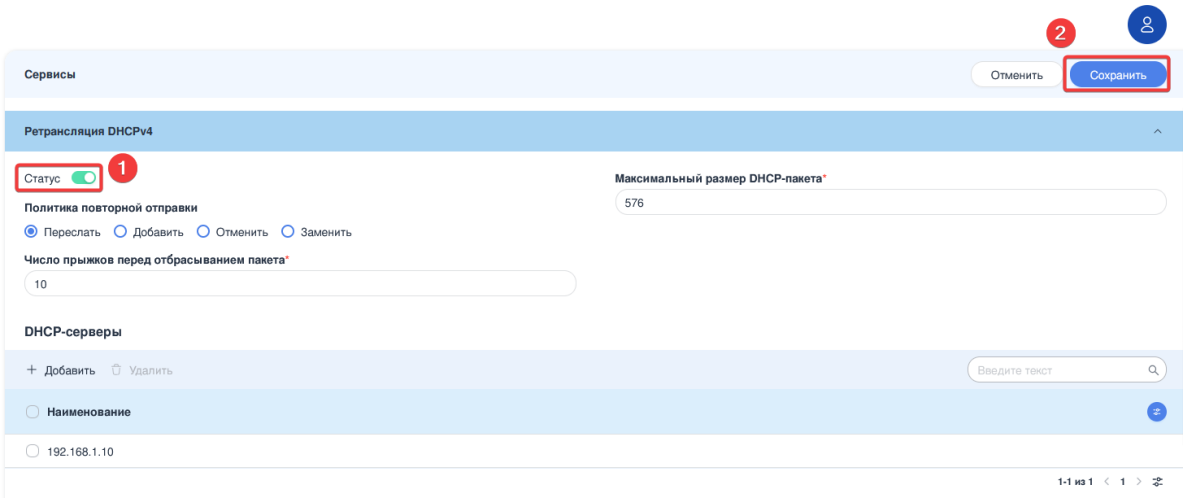


Рисунок – Включение службы ретрансляции DHCP

В случае невыполнения минимальных требований для запуска службы в левом нижнем углу экрана отобразится сообщение о невозможности запуска службы ретрансляции DHCP. Для обеспечения включения службы ретрансляции DHCP в соответствии с минимальными требованиями необходимо указать IP-адрес DHCP-сервера.

10.1.1.2 Дополнительные настройки

Дополнительные настройки ретрансляция DHCPv4 (см. Рисунок – Дополнительные настройки ретрансляции DHCPv4):

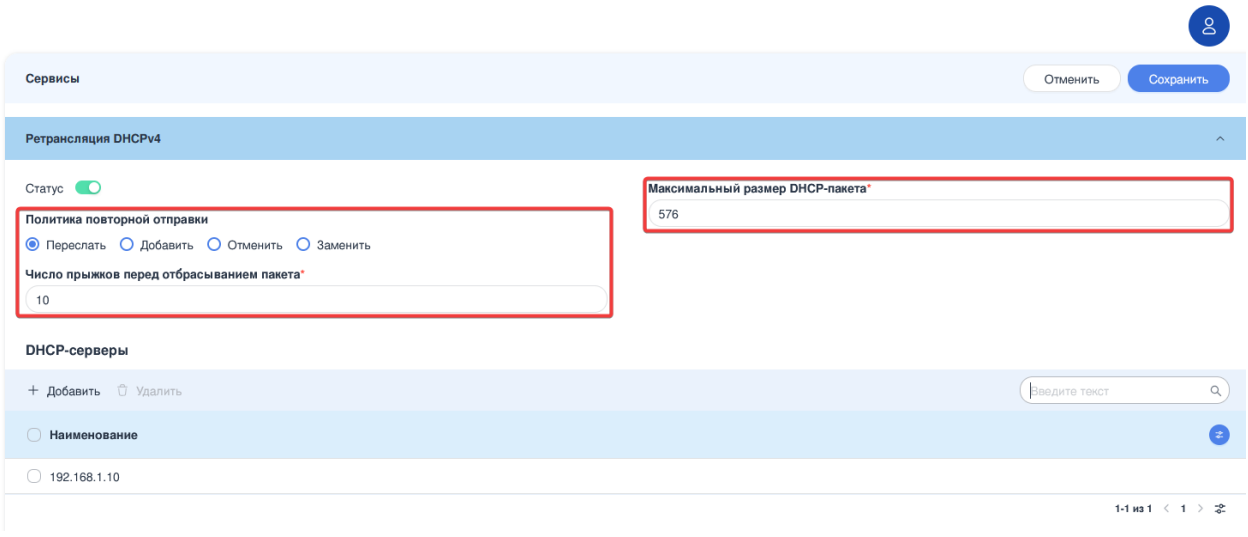


Рисунок – Дополнительные настройки ретрансляции DHCPv4

1. **Политика повторной отправки** - позволяет выбрать политику для повторной пересылки DHCP-пакетов. Возможно указать следующие политики:

- **«Переслать»** - все пакеты будут перенаправлены, а имеющаяся информация о ретрансляции будет проигнорирована;
- **«Добавить»** - ретранслятору разрешено добавлять в полученный DHCP-пакет собственную информацию о ретрансляции, при этом игнорируя информацию о ретрансляции, которая уже содержится в пакете;
- **«Отменить»** - принятые пакеты, которые уже содержат информацию о ретрансляции, будут отброшены;
- **«Заменить»** - информация о ретрансляции, которая уже присутствует в пакете, удаляется, и вместо неё вставляется собственный набор данных о ретрансляции маршрутизатора.

По умолчанию используется политика повторной отправки **«Переслать»**.

2. **Число прыжков перед отбрасыванием пакета** - определяет максимальное количество устройств DHCP-ретрансляции, которые может пройти пакет, прежде чем он будет отброшен. Возможно указать значение в диапазоне от **«1»** до **«255»**. По умолчанию используется значение **«10»**.
3. **Максимальный размер DHCP-пакета** - определяет максимальный размер DHCP-пакета в байтах, содержащий информацию об агенте ретрансляции. Если размер DHCP-пакета превышает установленное значение, он будет передан без включения информации об агенте ретрансляции. Возможно указать значение в диапазоне от **«64»** до **«1400»**. По умолчанию используется значение **«576»**.

10.1.1.3 Поиск и фильтрация

Блок фильтрации предоставляет возможность сортировки и фильтрации данных в таблице **«Интерфейсы ретрансляции DHCP-сообщений»** по всем столбцам в списке (см. Рисунок – Панель поиск и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Наименование»**;
- **«Тип интерфейса»**;
- **«Роль интерфейса»**;
- **кнопка «Сбросить фильтры»**.

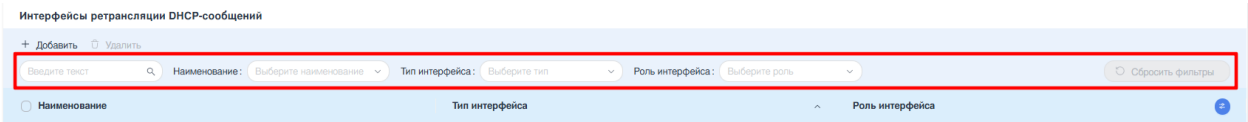


Рисунок – Панель поиск и фильтрации

Сквозной поиск по полям таблицы **«Интерфейсы ретрансляции DHCP-сообщений»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцу «Наименование».

Фильтрация по полю **«Наименование»** позволяет осуществлять отбор данных на основе указанного сетевого интерфейса. В данном поле представлен раскрывающийся список с именами интерфейсов, добавленных в таблицу **«Интерфейсы ретрансляции DHCP-сообщений»**.

Фильтрация по полю **«Тип интерфейса»** позволяет отфильтровать список по типу интерфейса.

Фильтрация по полю **«Роль интерфейса»** позволяет отфильтровать список по роли интерфейса. Поле содержит выпадающий список и предоставляет выбор из следующих вариантов значений: *«Прослушиваемый интерфейс»*, *«Upstream-интерфейс»*.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

Сквозной поиск по таблице **«DHCP-сервера»** осуществляется с помощью ввода искомого значения IP-адреса или его фрагмента в поле **«Поиск»**, расположенное в правом углу заголовка таблицы (см. Рисунок – Панель поиска).

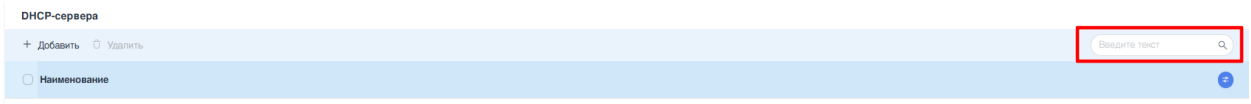


Рисунок – Панель поиска

10.1.2 Ретрансляция DHCPv6

Для настройки параметров ретрансляции DHCPv6 необходимо перейти в раздел **«Ретрансляция DHCPv6»**, расположенный в меню **«Сервисы» — «Ретрансляция DHCPv6»** (см. Рисунок – Ретрансляция DHCPv6).

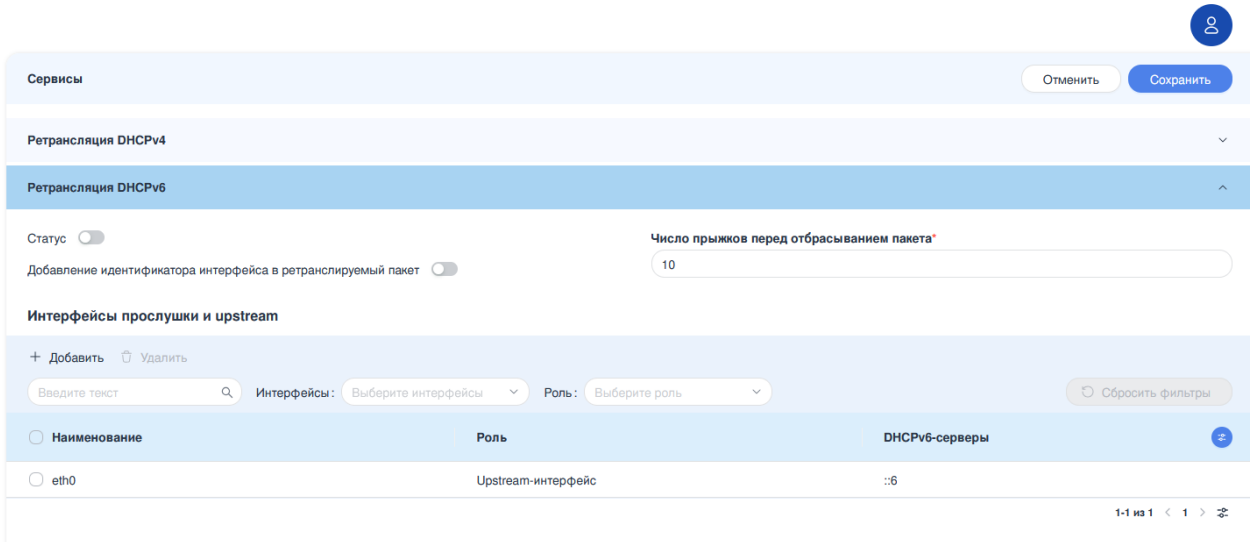


Рисунок – Ретрансляция DHCPv6

10.1.2.1 Основные настройки

Перед запуском службы ретрансляции DHCPv6 необходимо предварительно указать следующие настройки:

- **прослушиваемый интерфейс**, на котором будут прослушиваться DHCPv6-запросы;
- **upstream-интерфейс**, через который DHCPv6-запросы от клиентов будут передаваться на DHCPv6-сервер.

Настройки прослушиваемого/upstream интерфейса

Для добавления интерфейсов ретрансляции DHCPv6-сообщений необходимо в подразделе **«Интерфейсы прослушки и upstream»** раздела «Ретрансляция DHCPv6» нажать **кнопку «+Добавить»** и в открывшемся боковом окне внести следующие параметры (см. Рисунок – Добавления интерфейсов ретрансляции DHCPv6-сообщений):

- **Роль интерфейса** - указать, какую роль будет играть добавляемый интерфейс: прослушиваемый или upstream;
- **Интерфейс** - выбрать интерфейс из выпадающего списка;
- **Адрес** - ввести IPv6-адрес DHCPv6-сервера. Для upstream-интерфейса возможно добавить несколько IPv6-адресов, используя **кнопку «+Добавить»**.

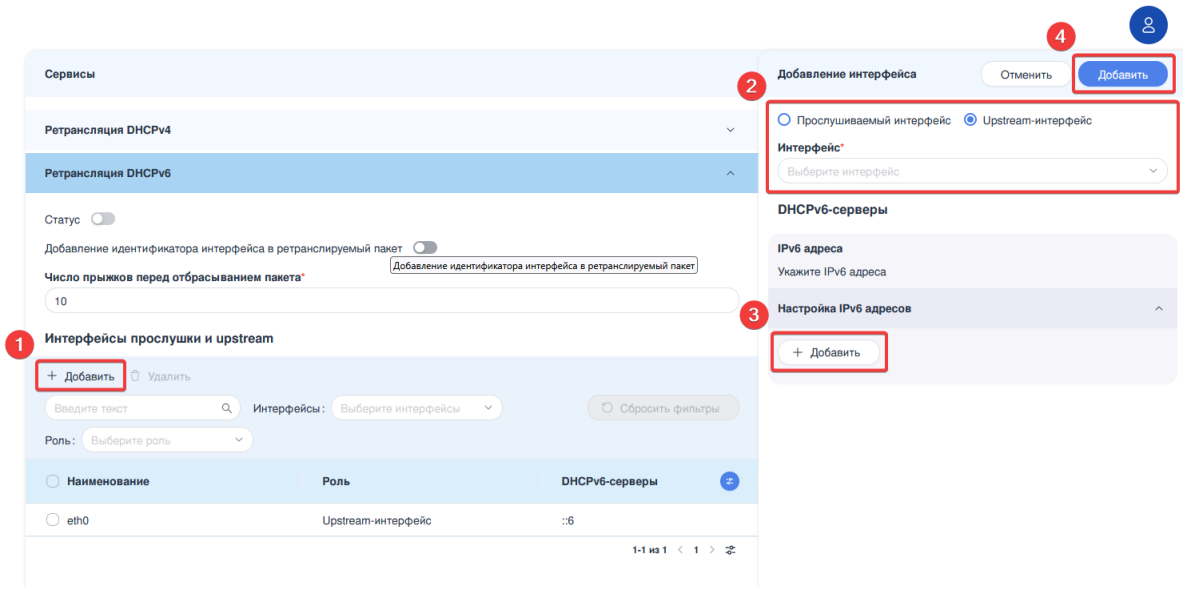


Рисунок – Добавления интерфейсов ретрансляции DHCPv6-сообщений

Для изменения IP-адреса DHCPv6-сервера в настроенном интерфейсе ретрансляции DHCPv6-сообщений необходимо нажать **ЛКМ** на строке с нужным интерфейсом и в открывшемся боковом окне внести корректировки. По завершению нажать **кнопку «Изменить»**.

Для удаления интерфейсов ретрансляции DHCPv6-сообщений необходимо выбрать один или несколько интерфейсов в разделе **«Интерфейсы прослушки и upstream»**, установив флажок в чек-боксе слева от имени интерфейса, и нажать **кнопку «Удалить»**. В открывшемся окне необходимо подтвердить удаление, нажав **кнопку «Удалить»**.

Примечание:

В случае, если после удаления все оставшиеся интерфейсы будут выполнять одну и ту же роль (либо только «Прослушиваемый интерфейс», либо только «Upstream-интерфейс»), и при этом будет включена ретрансляция, система выдаст предупреждение об отключении службы ретрансляции в случае подтверждения удаления.

Запуск службы ретрансляции DHCPv6

Для запуска службы ретрансляции DHCPv6 необходимо перевести **переключатель «Статус»** в положение включено и нажать **кнопку «Сохранить»** (см. Рисунок – Включение службы ретрансляции DHCPv6).

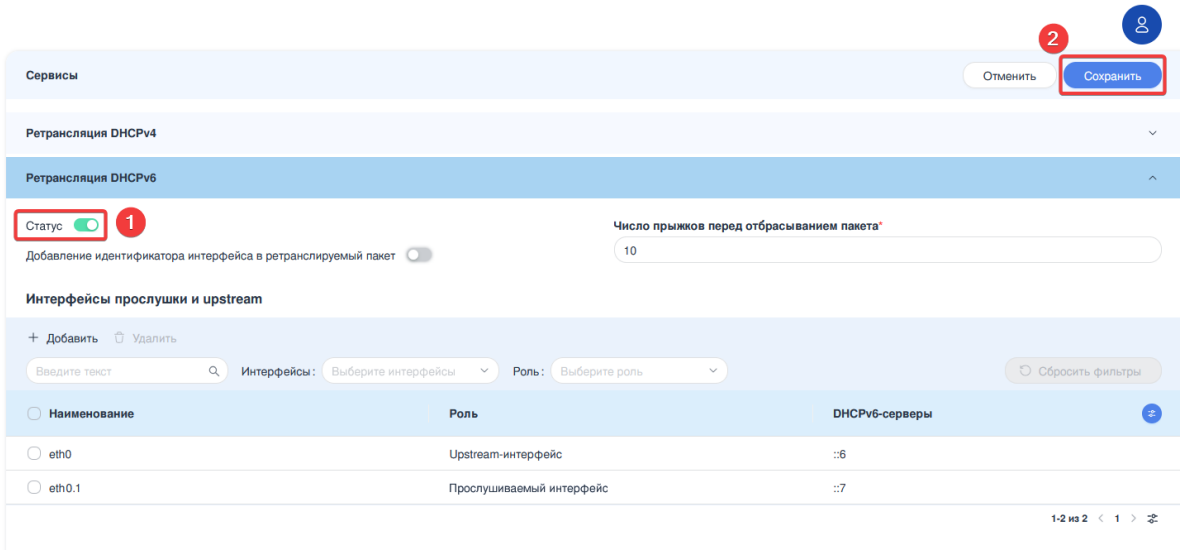


Рисунок – Включение службы ретрансляции DHCPv6

В случае невыполнения минимальных требований для запуска службы в левом нижнем углу экрана отобразится сообщение о невозможности запуска службы ретрансляции DHCPv6.

10.1.2.2 Дополнительные настройки

Дополнительные настройки ретрансляция DHCPv6 (см. Рисунок – Дополнительные настройки ретрансляции DHCPv6):

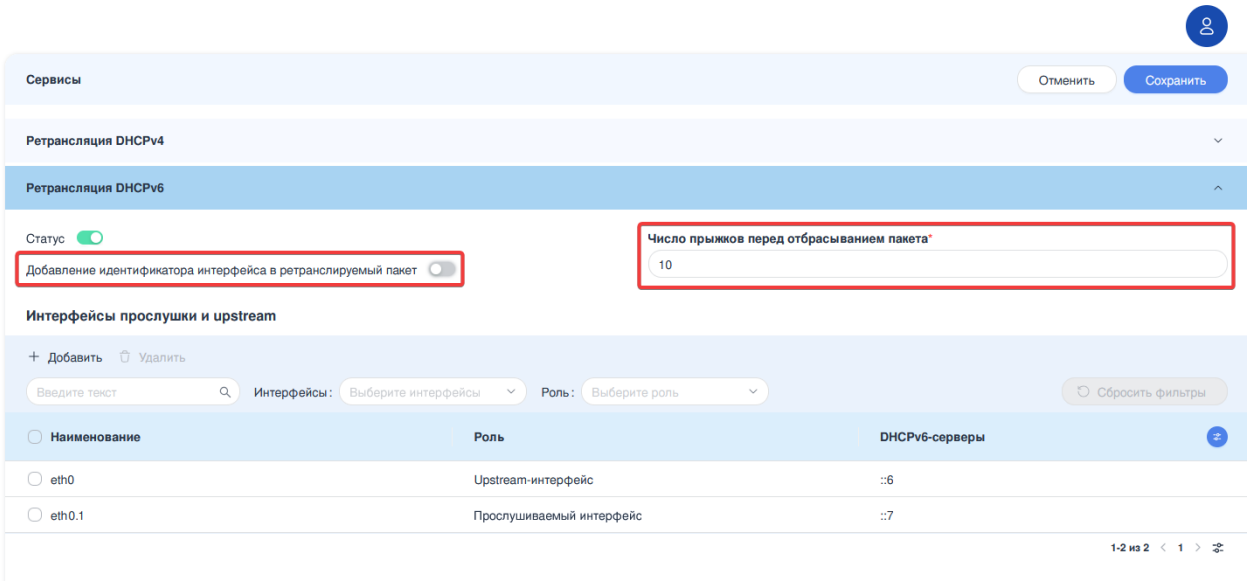


Рисунок – Дополнительные настройки ретрансляции DHCPv6

1. **Добавление идентификатора интерфейса в ретранслируемый пакет** - если параметр активирован, агент ретрансляции будет включать идентификатор интерфейса. Данный параметр активируется автоматически при использовании более одного прослушивающего интерфейса. В случае, если в запросе на ретрансляцию DHCPv6 присутствует значение идентификатора интерфейса, сервер копирует его в ответное сообщение. Идентификатор интерфейса позволяет определить, с какого интерфейса был получен запрос DHCPv6. Этот параметр следует использовать, когда IPv6-адрес интерфейса, на котором выполняется ретрансляция DHCPv6, не может быть однозначно идентифицирован.
2. **Число прыжков перед отбрасыванием пакета** - определяет максимальное количество устройств DHCP-ретрансляции, которые может пройти пакет, прежде чем он будет отброшен. Возможно указать значение в диапазоне от **«1»** до **«255»**. По умолчанию используется значение **«10»**.

10.1.2.3 Поиск и фильтрация

Блок фильтрации предоставляет возможность сортировки и фильтрации данных в таблице **«Интерфейсы прослушки и upstream»** по всем столбцам списка (см. Рисунок – Панель поиск и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Интерфейсы»**;
- **«Роль»**;
- **кнопка «Сбросить фильтры»**.

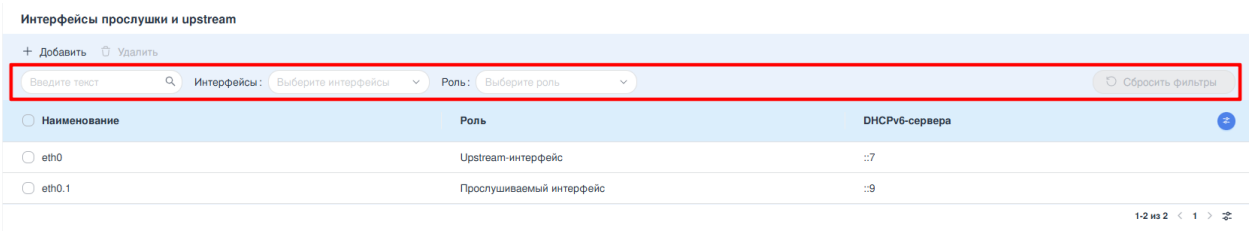


Рисунок – Панель поиск и фильтрации

Сквозной поиск по полям таблицы **«Интерфейсы прослушки и upstream»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам «Наименование» и «DHCPv6-сервера».

Фильтрация по полю **«Интерфейсы»** позволяет осуществлять отбор данных на основе указанного сетевого интерфейса. В данном поле представлен раскрывающийся список с именами интерфейсов, добавленных в таблицу **«Интерфейсы прослушки и upstream»**.

Фильтрация по полю **«Роль»** позволяет отфильтровать список по роли интерфейса. Поле содержит выпадающий список и предоставляет выбор из следующих вариантов значений: *«Прослушиваемый интерфейс», «Upstream-интерфейс»*.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

10.2 Веб-прокси

Для настройки параметров веб-прокси необходимо перейти в раздел **«Веб-прокси»**, расположенный в меню **«Сервисы»** (см. Рисунок – Веб-прокси).

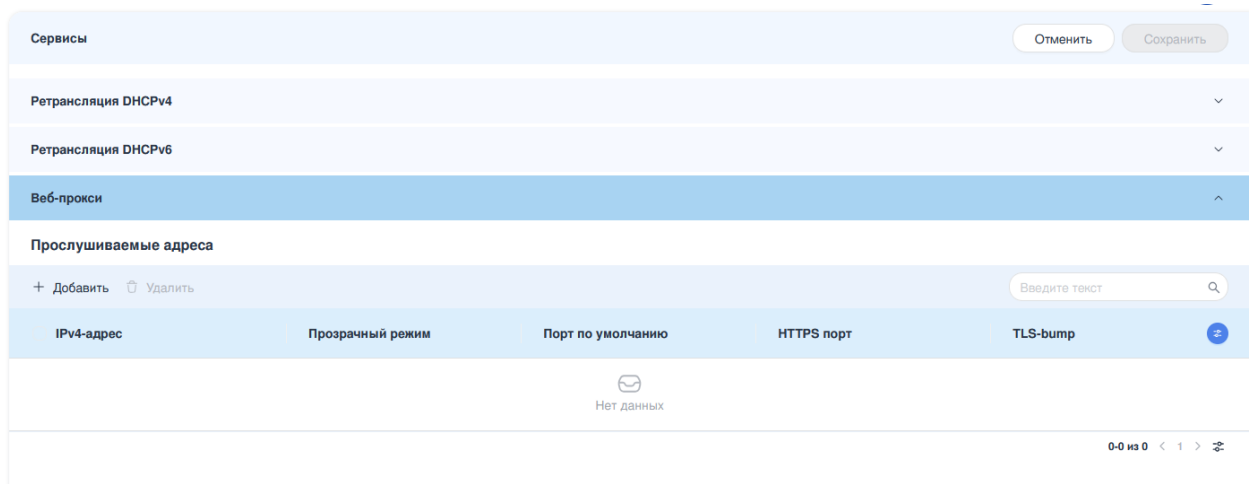


Рисунок – раздел «Веб-прокси»

10.2.1 Добавление прослушиваемых адресов

Для добавления прослушиваемого адреса необходимо выполнить следующие действия (см. Рисунок – Добавление прослушиваемого адреса):

1. В разделе **«Веб-прокси»** нажать **кнопку «+Добавить»**.
2. В открывшемся окне «Добавление адреса» задать следующие настройки:

- **«Прослушиваемый адрес»** — указать прослушиваемый адрес в формате IPv4.
- Флаг **«Прозрачный режим»** — флаг для указания, что трафик перенаправляется на прокси-сервер автоматически.
- **«Порт по умолчанию»** — задайте порт по умолчанию, на котором прокси-сервер будет прослушивать запросы. Допускаются целые положительные числа в диапазоне от **«1025»** до **«65535»**.
- **«HTTPS порт»** — задайте порт, отличный от значения по умолчанию, для указанного IPv4-адреса прокси, используемого для HTTPS трафика в прозрачном режиме работы прокси-сервера. Разрешён ввод целых положительных чисел в диапазоне от **«1025»** до **«65535»**.
- Флаг **«Статус»** — флаг для включения подмены сертификата TLS-Bump.
- **«Сертификат ЦС»** — укажите сертификат для работы TLS-bump.

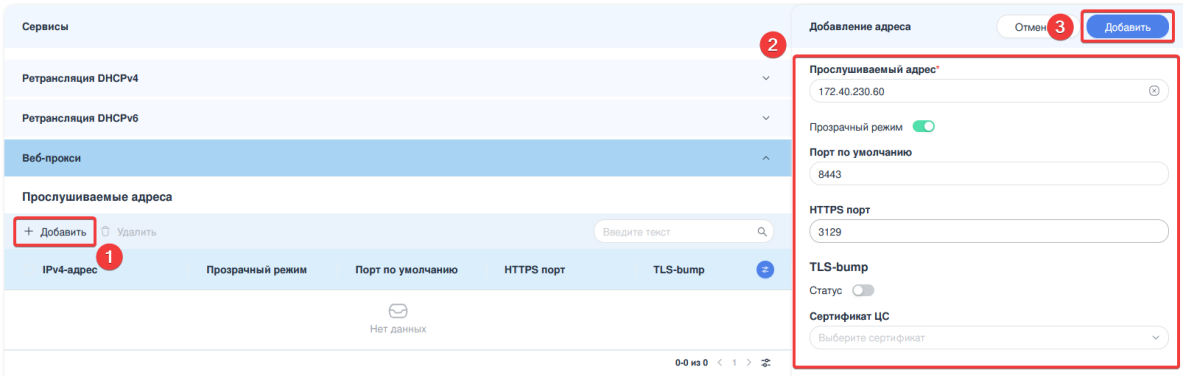


Рисунок – Добавление прослушиваемого адреса

Для удаления прослушиваемого адреса необходимо выбрать один или несколько адресов в таблице, установив флажок в чек-боксе слева от IP-адреса, и нажать **кнопку «Удалить»**. В открывшемся окне необходимо подтвердить удаление, нажав **кнопку «Удалить»** (см. Рисунок – Удаление прослушиваемого адреса).

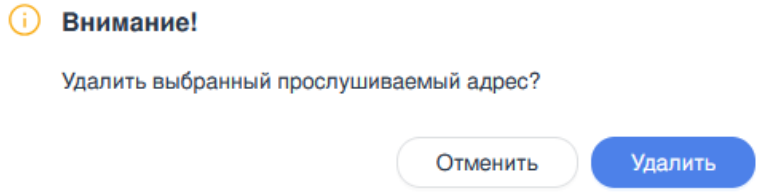


Рисунок – Удаление прослушиваемого адреса

В случае, если были удалены все прослушиваемые адреса, при сохранении настроек система выдаст ошибку (см. Рисунок – Ошибка при сохранении настроек после удаления всех прослушиваемых адресов):

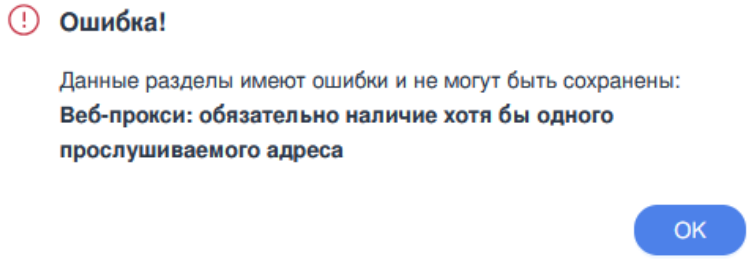


Рисунок – Ошибка при сохранении настроек после удаления всех прослушиваемых адресов

10.2.2 Редактирование прослушиваемых адресов

Для просмотра и редактирования параметров прослушиваемого адреса необходимо нажать **ЛКМ** на строке адреса в таблице **«Прослушиваемые адреса»**. В результате откроется боковая панель «Редактирование адреса» (см. Рисунок – Редактирование параметров прослушиваемого адреса).

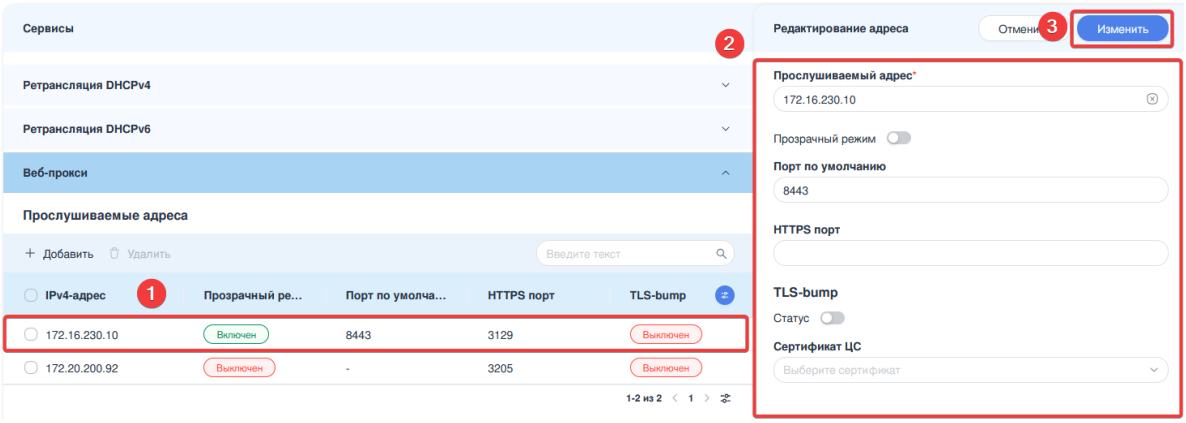


Рисунок – Редактирование параметров прослушиваемого адреса

10.2.3 Поиск и фильтрация

Сквозной поиск по полям таблицы **«Прослушиваемые адреса»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцу «IPv4-адрес». (см. Рисунок – Панель поиска).

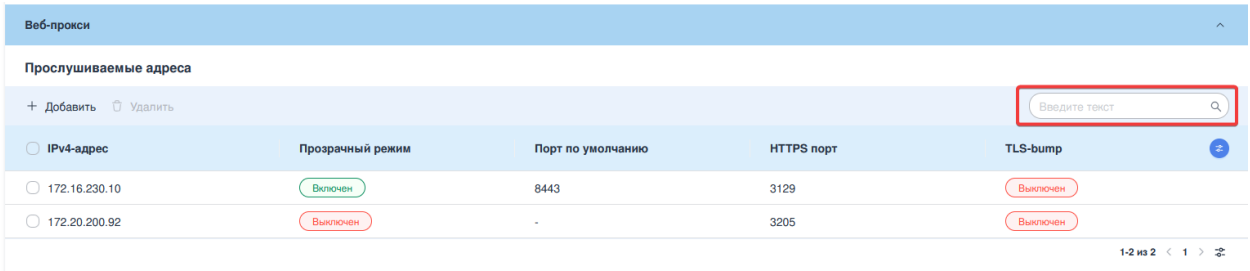


Рисунок – Панель поиска

10.2.4 Аутентификация пользователей

Аутентификация – это процесс проверки подлинности введённых пользователем имени и пароля. В ARMA Стена возможна аутентификация с использованием

локальной или внешней БД пользователей. В качестве внешней БД служат различные внешние серверы авторизации.

Общие настройки аутентификации

В блоке общих настроек аутентификации для сервиса веб-прокси можно задать следующие настройки (см. Рисунок – Общие настройки аутентификации):

- флаг **«Аутентификация»** - флаг для включения дополнительной аутентификации пользователей при работе с веб-прокси;
- **«Количество запросов»** — количество процессов единовременной аутентификации на веб-прокси. Определяет, сколько запросов на аутентификацию может обрабатываться одновременно. Возможно указать значение в диапазоне от **«1»** до **«500»**. По умолчанию используется значение **«5»**.

> **Примечание:**
>
> Использование дополнительной аутентификации невозможно при наличии прослушиваемых адресов в прозрачном режиме.

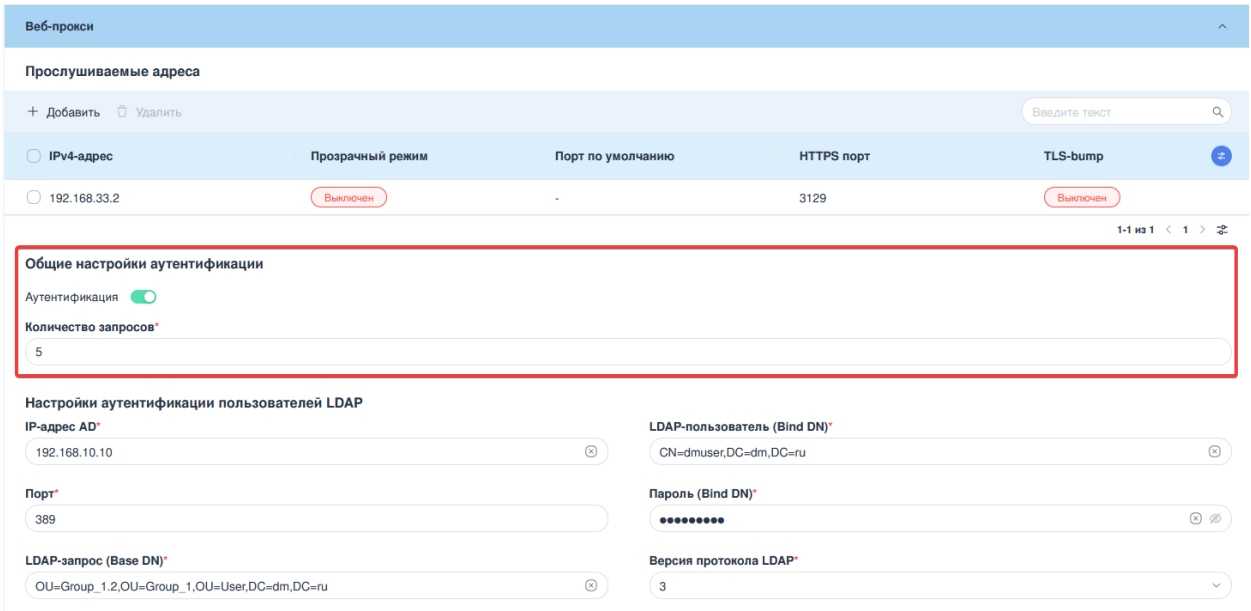


Рисунок – Общие настройки аутентификации

Настройки аутентификации пользователей LDAP

> **Примечание:**
>
> Для аутентификации пользователей с использованием LDAP необходимо предварительно указать адрес DNS-сервера, который обслуживает домен Active Directory, в разделе **«Системные настройки»** > **«Системный DNS»** (см. Системный DNS).

Для использования LDAP при работе с внешним сервером авторизации необходимо задать следующие параметры (см. Рисунок – Настройки аутентификации пользователей LDAP):

- **«IP-адрес AD»** - указать адрес сервера Active Directory в формате IPv4.
- **«Порт»** - указать порт для обращения серверу Active Directory. Допускаются целые положительные числа в диапазоне от **«1»** до **«65535»**. Значение по умолчанию - **«389»**
- **«LDAP-запрос (Base DN)»** - задать Distinguished Name (DN) каталога LDAP, с которого начинается поиск пользователей. Допустимо использование букв латинского и русского алфавитов и цифр. Не допускается использование следующих символов: пробел, **«/»**, **«\»**, **«:»**, **«;»**, **«,»**, **«+»**, **«*»**, **«?»**, **«<»**, **«>»**, **«@»**, **«[»**, **«]»**. Значение не должно начинаться или заканчиваться специальными символами. Максимально допустимое значение - «250» символов

  Примечание:

  Атрибуты фильтрации должны содержать доменную часть, УЗ, либо контейнер. Пример: *CN=<имя_группы>,DC=example,DC=com*.

- **«LDAP-пользователь (Bind DN)»** - задать Bind DN, который используется для подключения к серверу Active Directory. Допустимо использование букв латинского и русского алфавитов и цифр. Не допускается использование следующих символов: пробел, **«/»**, **«\»**, **«:»**, **«;»**, **«,»**, **«+»**, **«*»**, **«?»**, **«<»**, **«>»**, **«@»**, **«[»**, **«]»**. Значение не должно начинаться или заканчиваться специальными символами. Максимально допустимое значение - «250» символов.

  Примечание:

  Атрибуты фильтрации должны содержать доменную часть, УЗ, либо контейнер. Пример: *CN=admin, DC=example,DC=com*.

- **«Пароль (Bind DN)»** - указать пароль для Bind DN. Допустимо использование букв латинского алфавита, цифр и специальных символов. Не допускается использование пробела. Максимально допустимое значение - «32» символа.
- **«Версия протокола LDAP»** - указать версию протокола LDAP. Допустимые значения: **«2»** и **«3»**.

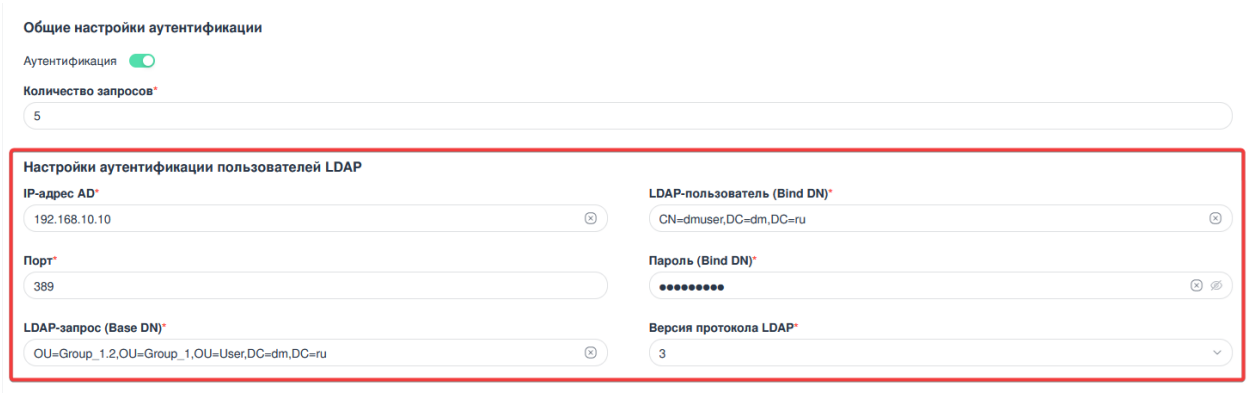


Рисунок – Настройки аутентификации пользователей LDAP

10.3 LLDP

Служба LLDP – это демон, позволяющий **ARMA Стена** посредством протокола LLDP идентифицировать устройства локальной сети и обмениваться информацией о своих характеристиках.

К информации, которую можно получить, относятся:

- Имя и описание системы.
- Имя и описание порта.
- Имя VLAN.
- IP-адрес управления.
- Возможности системы (коммутация, маршрутизация и т. д.).
- Информация о MAC/PHY.
- Питание по MDI (Power over Ethernet).
- Агрегация каналов (Link aggregation).

> **Примечание:**
>
> LLDP не использует шифрование и работает на канальном уровне. Он не может использоваться в публичных сетях и должен быть отключен для интерфейсов, на которых он не используется.

Для настройки параметров сервиса LLDP необходимо перейти в раздел **«LLDP»**, расположенный в меню **«Сервисы»** (см. Рисунок – Раздел «LLDP»).

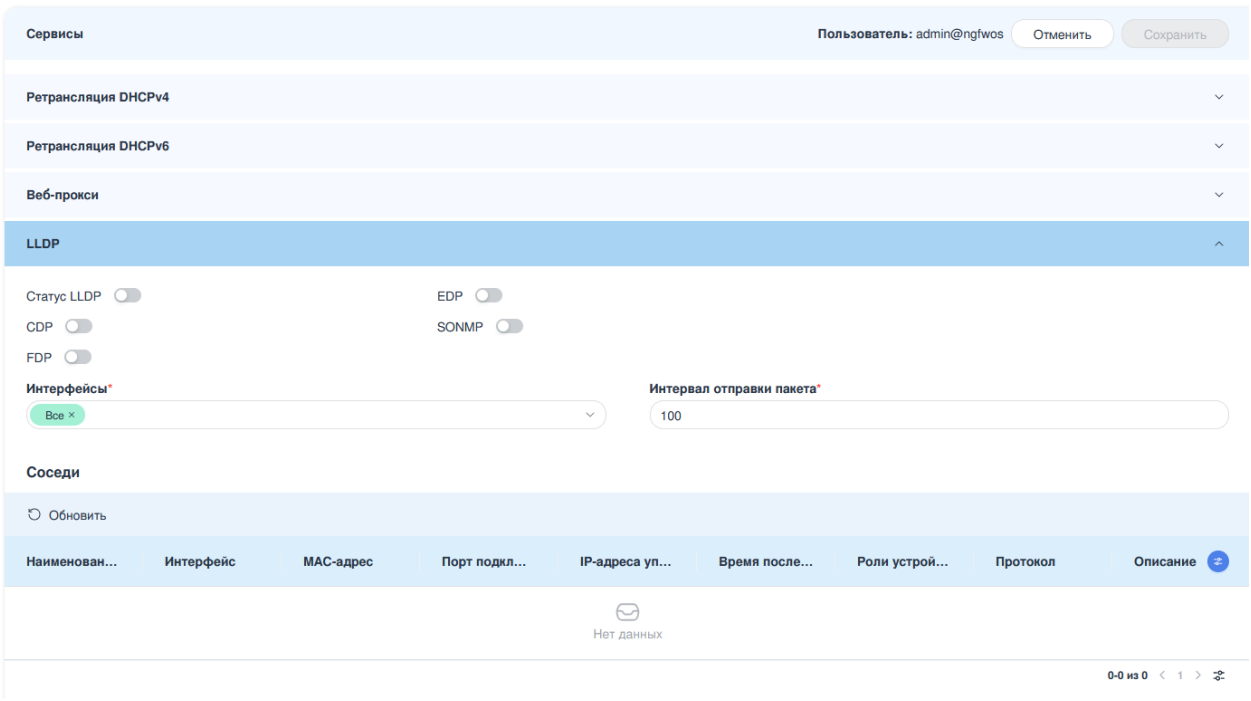


Рисунок – раздел «LLDP»

10.3.1 Общие настройки LLDP

В блоке общих настроек для сервиса LLDP можно задать следующие настройки (см. Рисунок – Общие настройки LLDP):

- флаг **«Статус LLDP»** - флаг для включения сервиса LLDP;
- флаг **«EDP»** - флаг для использования протокола Extreme Discovery;
- флаг **«CDP»** - флаг для использования протокола Cisco Discovery;
- флаг **«SONMP»** - флаг для использования протокола Nortel/SynOptics Network Management;
- флаг **«FDP»** - флаг для использования протокола Foundry Discovery;
- **«Интерфейсы»** - выбрать из выпадающего списка интерфейс, который будет использоваться при работе сервиса LLDP.
- **«Интервал отправки пакета»** - задать интервал для отправки LLDP-пакетов. Возможно указание значения в диапазоне от **«30»** до **«300»**. По умолчанию используется значение **«30»**.

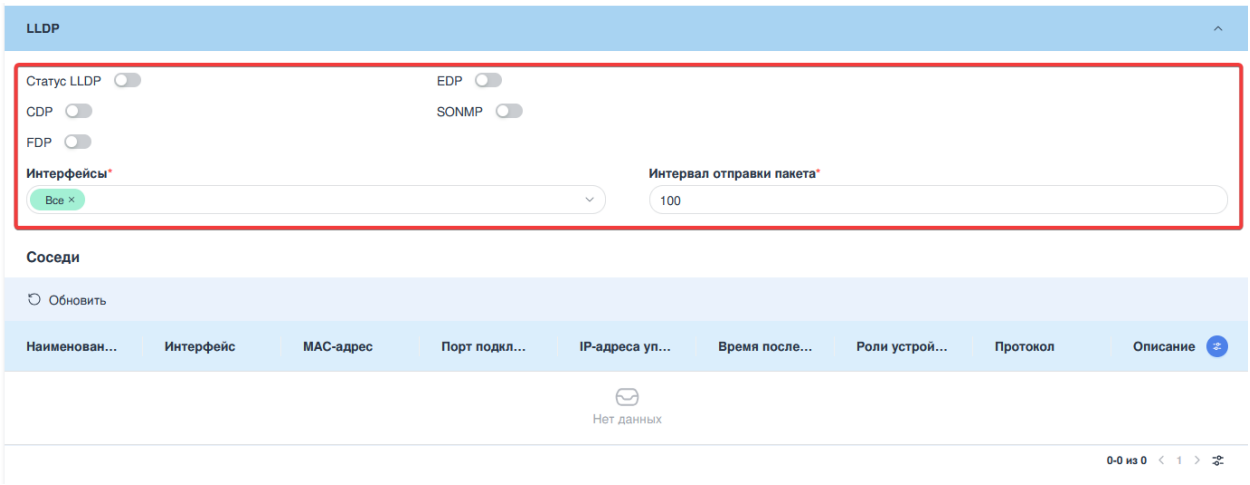


Рисунок – Общие настройки LLDP

10.3.2 Соседи

Таблица «Соседи» отображает устройства, которые доступны для обнаружения по LLDP. Для обновления списка необходимо нажать **кнопку «Обновить»** (см. Рисунок – Таблица «Соседи»):

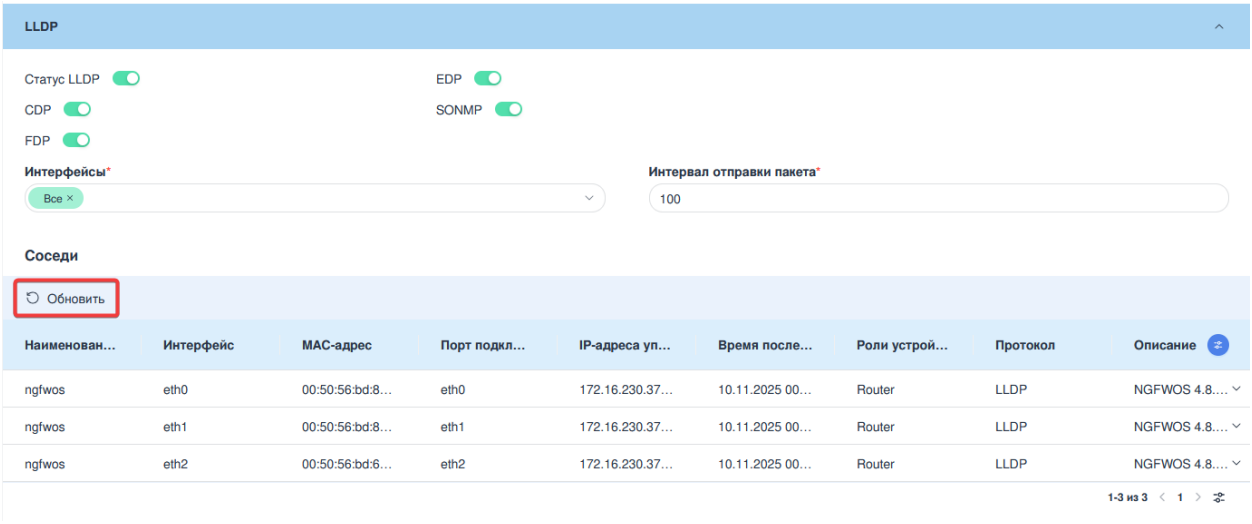


Рисунок – таблица «Соседи»

Для просмотра дополнительных сведений об устройстве-соседе необходимо нажать **ЛКМ** на строке в таблице **«Соседи»**. В результате откроется боковая панель «LLDP-сосед» (см. Рисунок – Просмотр сведений о соседе):

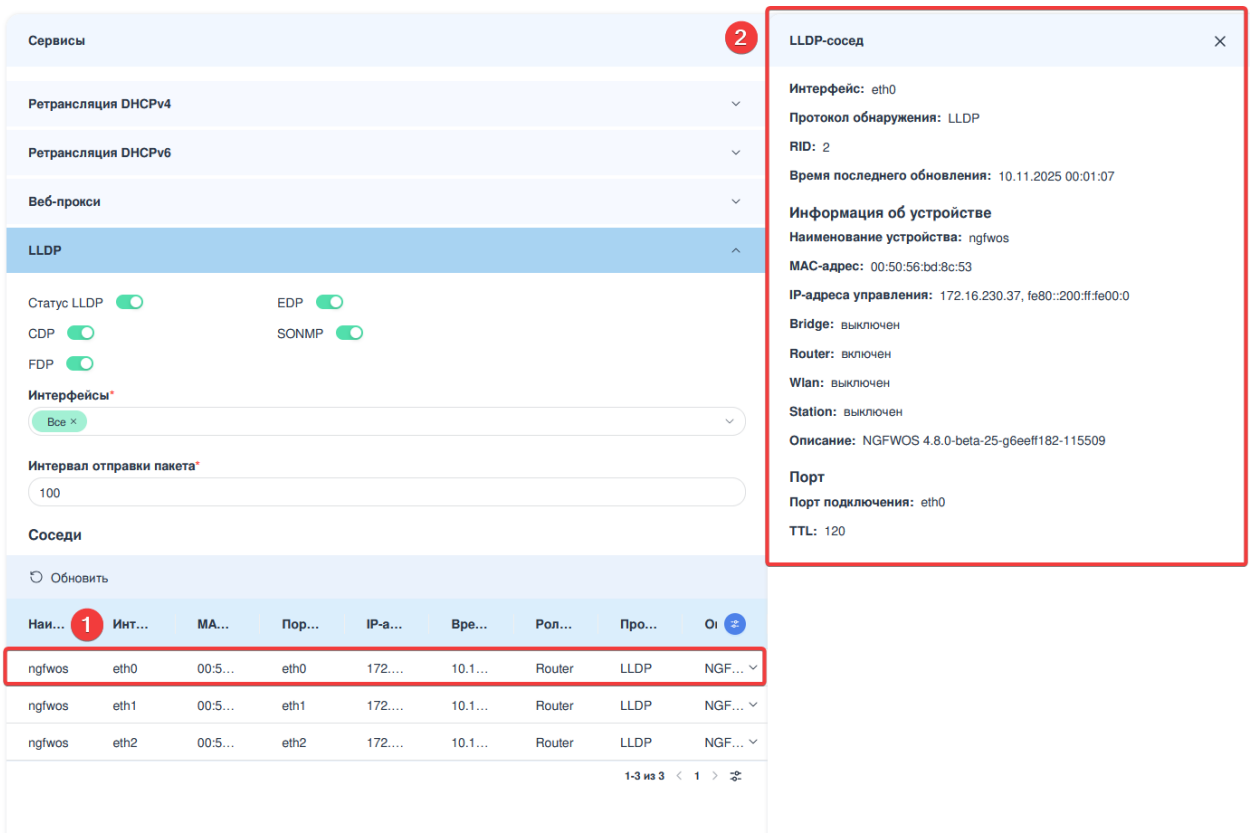


Рисунок – Просмотр сведений о соседе

11 NAT

NAT (Network Address Translation) — это механизм сетевой адресации, обеспечивающий преобразование внутренних (частных) IP-адресов в публичные и наоборот для обеспечения доступа узлов локальной сети к внешним ресурсам. Технология функционирует на уровне сетевого шлюза или межсетевого экрана, осуществляя прозрачную трансляцию адресных пространств с возможностью статического или динамического сопоставления, а также с использованием технологии множественной адресации портов (PAT) для оптимизации использования публичных IP-адресов.

В системе **ARMA Стена** реализованы следующие способы трансляции сетевых адресов:

- **DNAT** – позволяет получить доступ из внешней сети во внутреннюю сеть с перенаправлением на конкретный адрес и порт;
- **SNAT, Masquerading** – позволяет множеству устройств, находящихся за NAT, выходить в сеть через один внешний IP-адрес. Скрывает структуру сети от внешнего мира;
- **Статический NAT, «Один-к-одному»** – позволяет каждому внутреннему IP-адресу присваивать уникальный внешний IP-адрес.

IP Masquerading - технология трансляции адресов, которая обеспечивает инкапсуляцию приватного IP-пространства за единственным публичным IP-адресом. В процессе обработки исходящего трафика механизм подменяет исходные адреса узлов локальной сети на внешний адрес маршрутизирующего устройства, создавая иллюзию непосредственного источника пакетов. Данный метод стал де-факто стандартом для оптимизации использования дефицитного адресного пространства IPv4, в результате чего термины NAT и IP Masquerading часто используются как взаимозаменяемые.

11.1 Правила NAT

NAT функционирует на основе конфигурации, состоящей из упорядоченного набора правил трансляции адресов. Каждое правило содержит набор параметров, определяющих алгоритм преобразования сетевых заголовков. Правила идентифицируются уникальными номерами и обрабатываются в строгой последовательности. Важно отметить, что идентификатор правила NAT является статичным атрибутом и не подлежит модификации после создания. Изменение порядкового номера правила требует его полного удаления из конфигурации с последующей реитерацией и присвоением нового идентификатора.

В связи с этим рекомендуется присваивать правилам NAT последовательные номера с интервалами между ними. Например, можно создать набор правил NAT с номерами 10, 20, 30 и 40. В случае необходимости добавления нового правила в

определённое место последовательности, это можно будет сделать без изменения текущего набора правил.

Примечание:

Изменения, внесённые в конфигурацию NAT, будут действовать только для новых соединений. Ранее установленные соединения останутся неизменными.

Для создания, просмотра или изменения правил NAT необходимо перейти в раздел **«Межсетевой экран» - «NAT»** (см. Рисунок – Правила NAT):

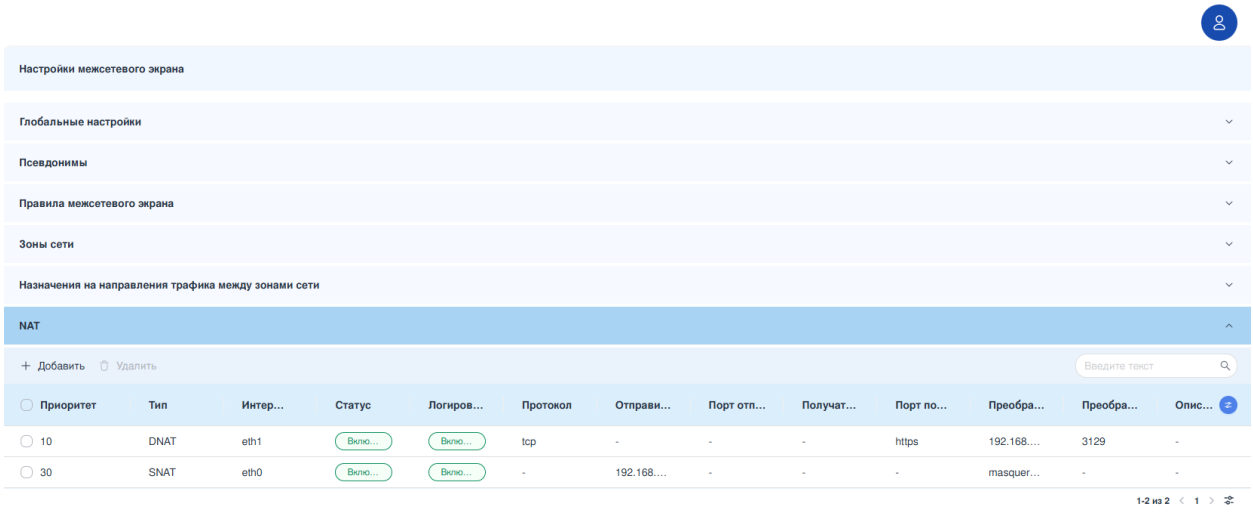


Рисунок – Правила NAT

Поиск и фильтрация данных в таблице NAT.

В таблице с правилами NAT реализован блок фильтрации, который позволяет сортировать и искать данные по всем столбцам в списке (см. Рисунок – Панель поиск и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Тип»**;
- **«Интерфейс»**;
- **«Статус»**;
- **«Логирование»**;
- **«Протокол»**;
- **кнопка «Сбросить фильтры»**.

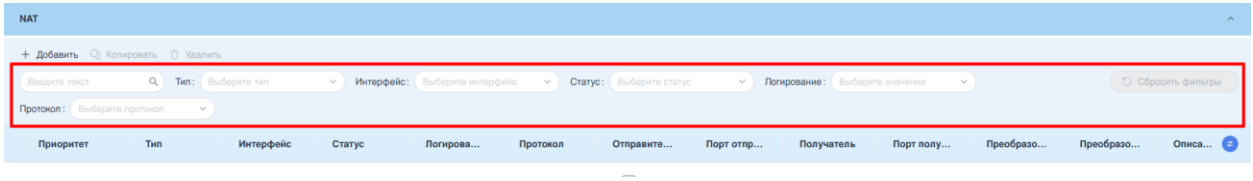


Рисунок – Панель поиск и фильтрации

Сквозной поиск по полям таблицы **«NAT»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск производится без учёта регистра вводимых символов. Поиск производится по всем строкам таблицы согласно их сохранённым значениям в конфигурационном файле. Например, если ввести в поиске текст «destination», в таблице отобразятся все правила DNAT, поскольку в конфигурационном файле правила DNAT сохранены как destination.

С помощью фильтров «Тип», «Интерфейс», «Статус», «Логирование» и «Протокол» возможно осуществить отбор данных в соответствии с заданными параметрами.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

11.2 Создание правила DNAT

Для создания правила **DNAT** необходимо выполнить следующие действия:

1. Нажать кнопку «+Добавить» в разделе **«NAT»**.
2. В открывшейся боковой панели выбрать создаваемую сущность «DNAT» (см. Рисунок – Создание правила DNAT):

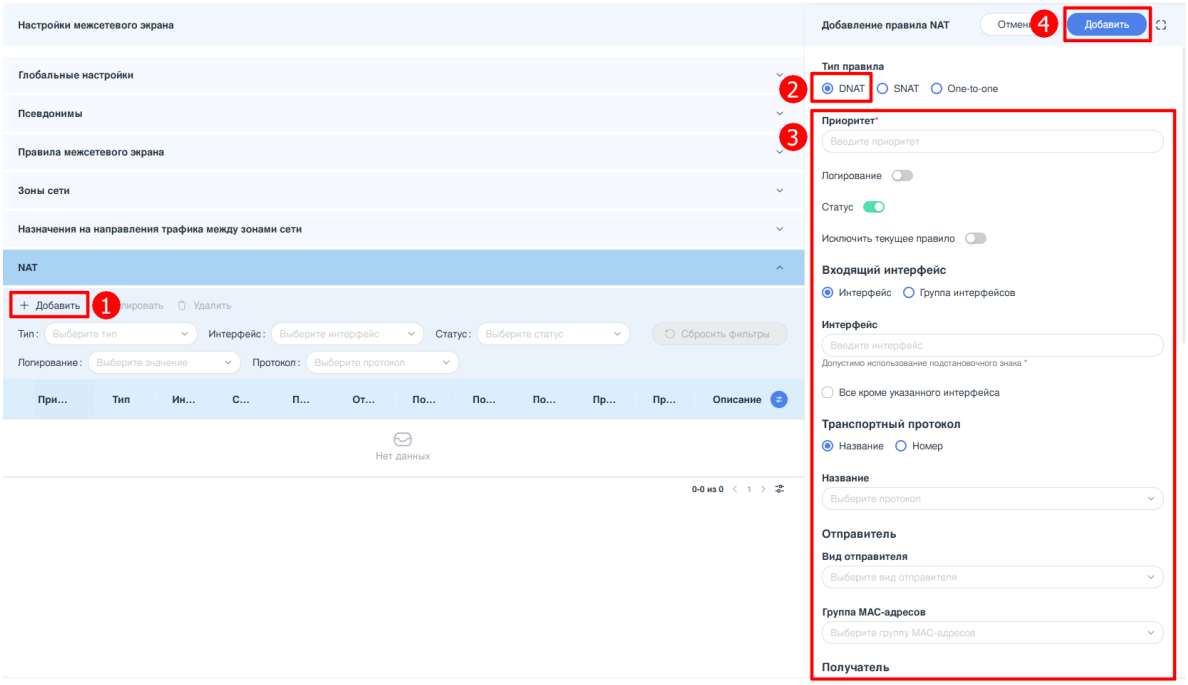


Рисунок – Создание правила DNAT

3. Внести/скорректировать значение в полях:
   - **Приоритет** - номер приоритета правила DNAT. Возможно указать значение в диапазоне от «1» до «999999». Параметр должен быть уникальным в рамках выбранного набора правил и определяет последовательность выполнения правил от 1 к 999999.

Примечание:

Рекомендуется присваивать правилам NAT последовательные номера с интервалами между ними, оставляя свободные номера для новых правил.

- **Логирование** - включение/отключение журналирование действий.
- **Статус** - отключение правила преобразования сетевых адресов.
- **Исключить текущее правило** - с помощью «исключающих» правил можно определить сетевые пакеты, для которых не будет выполняться преобразование сетевых адресов. Это особенно полезно в случаях, когда для некоторых видов трафика, например, для VPN-трафика, требуется исключить преобразование адресов.
- **Входящий интерфейс** - указание входного интерфейса, на котором будет выполняться правило DNAT. Преобразование сетевого адреса получателя (DNAT) будет осуществляться для трафика, принятого на указанном интерфейсе. Возможно указать следующие значения:
    - **Интерфейс** - ввести наименование сетевого интерфейса. В этом поле возможно использовать следующие символы: *символы латинского алфавита; цифры; подстановочный знак* **«*»** (например, «eth1*» — все интерфейсы, имена которых начинаются с «eth1»); **«any»** (система будет обрабатывать весь входящий трафик независимо от того, через какой интерфейс он пришёл). Имя интерфейса должно начинаться с латинской буквы, иметь длину не более 14 символов, подстановочный знак должен располагаться в конце.
    - **Группа интерфейсов** - выбор из предложенного списка название ранее созданной группы интерфейсов.

  При установке флажка в чек-боксе **«Все кроме указанного интерфейса»** правило будет срабатывать на всех интерфейсах, кроме указанного.
- **«Транспортный протокол»** - указание протоколов, для которых осуществляется преобразование сетевых адресов. Возможно указать значение номером или именем протокола:
    - **«Название»** - выбор транспортного протокола из выпадающего списка;

- **«Номер»** - номер протокола в соответствии с документом IANA. Возможно указать значение в диапазоне от «0» до «255».

- **Отправитель** - указать параметры отправителя, на основе которых будет осуществляться сопоставление в правиле NAT:
  - **«Вид отправителя»** - выбор вида отправителя из списка, который будет использоваться для проверки соответствия сетевого пакета правилу NAT:
    - **«Адрес»** - IPv4-адрес отправителя для проверки соответствия в формате <x.x.x.x>;
    - **«Сеть»** - IPv4-сеть отправителя для проверки соответствия в формате <x.x.x.x/x>;
    - **«Диапазон адресов»** - указать диапазон IPv4-адресов отправителя в соответствующих полях;
    - **«Группа адресов»** - выбрать группу адресов из списка;
    - **«Группа сетей»** - выбрать группу сетей из списка;
    - **«Группа доменов»** - выбрать группу доменов из списка.

    Для типов отправителей **«Адрес»**, **«Сеть»** и **«Диапазон адресов»** доступна функция инверсии значений. Для её активации необходимо установить флажок в чекбоксе **«Все кроме указанного отправителя»**. В этом случае правило будет применяться ко всем адресам, за исключением указанных.

    При выборе одной из **групп** предусмотрена возможность указать дополнительные категории групп: **«Группа MAC-адресов»** и **«Группа портов»** (группа портов доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP).
  - **«Группа MAC-адресов»** - указать группу MAC-адресов отправителя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
  - **«Порт отправителя»** - секция параметров доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP. Возможно настроить следующие параметры:

- **«Группа портов»** - указать группу портов отправителя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
- **«Порты»** - указать порт отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу NAT. Для конфигурации портов необходимо нажать **кнопку** « » справа от поля **«Настройка портов»** и в раскрывшемся поле нажать **кнопку «+Добавить»**. Доступны следующие параметры:
  - **«Номер порта»** - в поле **«Порт»** ввести номер порта в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - указать диапазон портов в соответствующих полях;
  - **«Протокол»** - выбрать протокол из списка.

  Кнопки «+Добавить» и «**Удалить»** позволяют добавлять или удалять порты отправителя.

  При установке флажка в чекбоксе **«Все кроме указанных портов»** правило будет применяться ко всем портам, за исключением указанных.

- **Получатель** - указать параметры получателя, на основе которых будет осуществляться сопоставление в правиле NAT:
  - **«Вид получателя»** - выбор вида получателя из списка, который будет использоваться для проверки соответствия сетевого пакета правилу NAT:
    - **«Адрес»** - IPv4-адрес получателя для проверки соответствия в формате <x.x.x.x>;
    - **«Сеть»** - IPv4-сеть получателя для проверки соответствия в формате <x.x.x.x/x>;
    - **«Диапазон адресов»** - указать диапазон IPv4-адресов получателя в соответствующих полях;

- **«Группа адресов»** - выбрать группу адресов из списка;
- **«Группа сетей»** - выбрать группу сетей из списка;
- **«Группа доменов»** - выбрать группу доменов из списка.

Для типов получателя **«Адрес»**, **«Сеть»** и **«Диапазон адресов»** доступна функция инверсии значений. Для её активации необходимо установить флажок в чекбоксе **«Все кроме указанного получателя»**. В этом случае правило будет применяться ко всем адресам, за исключением указанных.

При выборе одной из **групп** предусмотрена возможность указать дополнительные категории групп: **«Группа MAC-адресов»** и **«Группа портов»** (группа портов доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP).

- **«Группа MAC-адресов»** - указать группу MAC-адресов получателя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
- **«Порт получателя»** - секция параметров доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP. Возможно настроить следующие параметры:
  - **«Группа портов»** - указать группу портов получателя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
  - **«Порты»** - указать порт получателя, который будет использоваться для проверки соответствия сетевого пакета правилу NAT. Для конфигурации портов необходимо нажать **кнопку** « » справа от поля **«Настройка портов»** и в раскрывшемся поле нажать **кнопку «+Добавить»**. Доступны следующие параметры:
    - **«Номер порта»** - в поле **«Порт»** ввести номер порта в диапазоне от «1» до «65535»;
    - **«Диапазон портов»** - указать диапазон портов в соответствующих полях;

- **«Протокол»** - выбрать протокол из списка.

Кнопки «+Добавить» и «**Удалить»** позволяют добавлять или удалять порты получателя.

При установке флажка в чекбоксе **«Все кроме указанных портов»** правило будет применяться ко всем портам, за исключением указанных.

- **«Преобразованный адрес»** - указать адрес, на который будет заменён исходный адрес назначения пакетов. Возможен выбор следующих значений:
  - **«Адрес»** - IP-адрес в формате IPv4;
  - **«Диапазон адресов»** - указать диапазон IP-адресов в соответствующих полях;
  - **«Сеть»** - указать сеть: IP-адрес и маску подсети.
- **«Преобразованный порт»** - указать порт для трансляции. Возможен выбор следующих значений:
  - **«Номер порта»** - ввести номер порта в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - указать диапазон портов в соответствующих полях.
- **«Перенаправление трафика»** - указать порт, на который будет перенаправляться входящий трафик. Возможен выбор следующих значений:
  - **«Номер порта»** - ввести номер порта в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - указать диапазон портов в соответствующих полях.
- **«Дополнительные параметры NAT преобразованного адреса»** - секция настроек дополнительных параметров NAT:
  - **«Назначение IP-адреса»** - определить тип механизма сопоставления адресов для трансляции в правиле NAT:
    - **«Случайный IP»** (random) - случайное распределение адресов отправителя или получателя для каждого соединения. Используется по умолчанию.

- **«Постоянный IP»** (persistent)- пользователь получает один и тот же адрес отправителя или получателя для каждого соединения.

- **«Назначение порта»** - определить метода сопоставления портов при трансляции адресов в правилах NAT:
  - **«Порт без изменений»** (none) - отключает динамическое сопоставление портов, использует исходный порт исходного пакета. Используется по умолчанию.
  - **«Случайный порт»** (random)- выбирает случайный доступный порт из диапазона трансляции.

- **«Балансировка»**

  В рамках одного правила возможно определить несколько транслируемых адресов, чтобы NAT мог сбалансировать трансляцию между ними. Алгоритм балансировки использует хэш для распределения нагрузки. При определении транслируемых адресов, называемых бэкендами, необходимо настроить вес. Это позволяет пользователю самостоятельно определить распределение нагрузки в соответствии с его предпочтениями.

  Параметры настройки балансировки:

  - **«Метод распределения»** - выбрать алгоритм генерации хэша. Возможен множественный выбор следующих значений: «Случайное», «По IP-адресу отправителя», «По IP-адресу получателя», «По порту отправителя», «По порту получателя». Выбор значений «По порту отправителя» и «По порту получателя» допускается при указанном для параметра **«Транспортный протокол»** значении «tcp», «udp» или «tcp/udp». По умолчанию хэш генерируется случайным образом - метод **«Случайное»**.
  - **«Настройка преобразованных IP-адресов»** - возможно указание преобразованных IP-адресов и веса для каждого бэкенда. Сумма всех весов, присвоенных бэкендам, должна составлять **«100»**. Иными словами, вес, присвоенный конкретному бэкенду, представляет собой процент соединений, которые будут направлены на этот бэкенд.

- **«Тип пакета»** - настроить правило соответствия на основе типа пакета. Возможно указание следующих типов: «Широковещательный пакет», «Одиночный пакет», «Пакеты для группы устройств», «Другие типы».

4. По завершении нажать **кнопку «Сохранить»**.
5. После сохранения нового правила NAT необходимо нажать **кнопку «Сохранить»** в правом верхнем углу формы **«Настройки межсетевого экрана»** для сохранения и применения новых настроек в системе **ARMA Стена** (см. Рисунок – Кнопка сохранения и применения новых настроек системы).

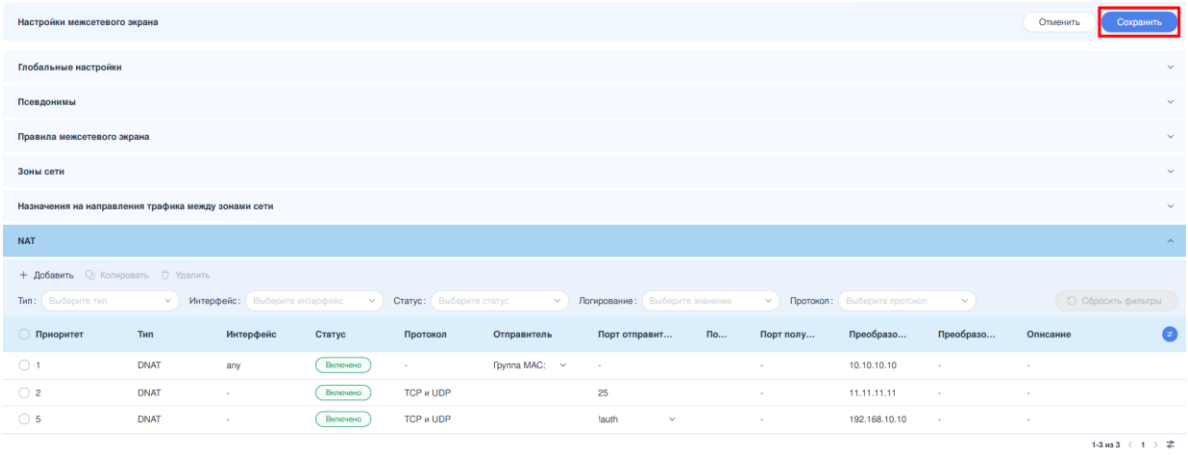


Рисунок – Кнопка сохранения и применения новых настроек системы.

11.3 Создание правила SNAT

Для создания правила **SNAT** необходимо выполнить следующие действия:

1. Нажать **кнопку «+Добавить»** в разделе **«NAT»**.
2. В открывшейся боковой панели выбрать создаваемую сущность «SNAT» (см. Рисунок – Создание правила DNAT):

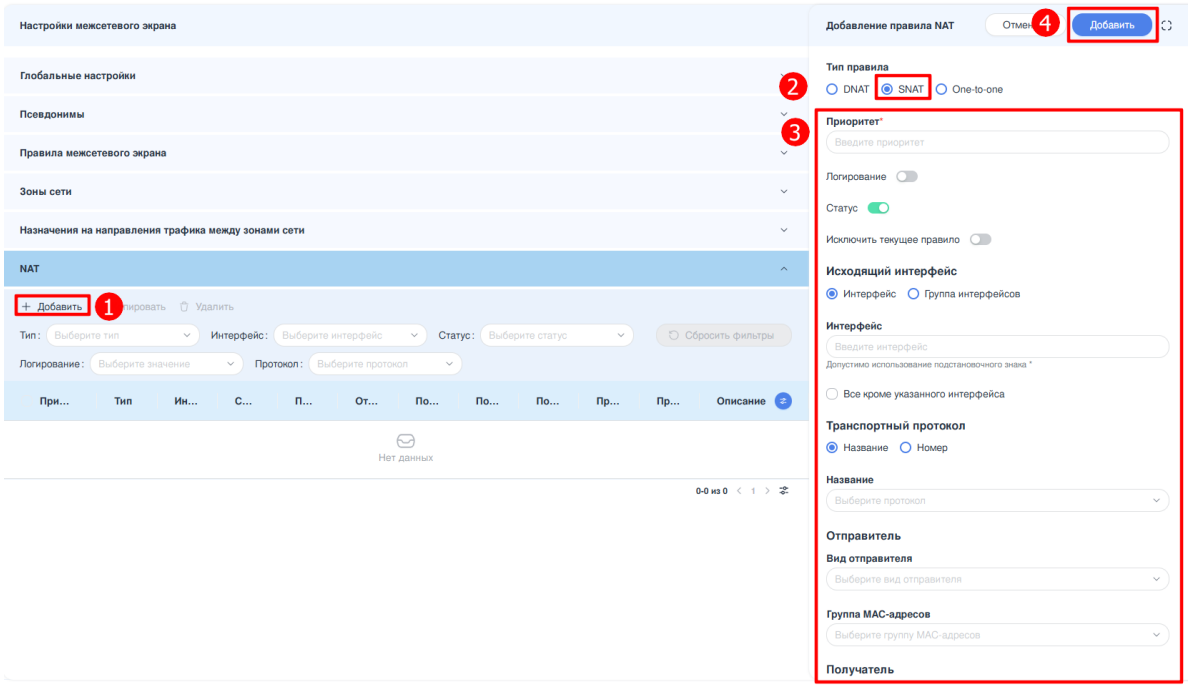


Рисунок – Создание правила SNAT

3. Внести/скорректировать значение в полях:

- **Приоритет** - номер приоритета правила SNAT. Возможно указать значение в диапазоне от «1» до «999999». Параметр должен быть уникальным в рамках выбранного набора правил и определяет последовательность выполнения правил от 1 к 999999.

  Примечание:

  Рекомендуется присваивать правилам NAT последовательные номера с интервалами между ними, оставляя свободные номера для новых правил.

- **Логирование** - включение/отключение журналирование действий.
- **Статус** - отключение правила преобразования сетевых адресов.
- **Исключить текущее правило** - с помощью «исключающих» правил можно определить сетевые пакеты, для которых не будет выполняться преобразование сетевых адресов. Это особенно полезно в случаях, когда для некоторых видов трафика, например, для VPN-трафика, требуется исключить преобразование адресов.
- **Исходящий интерфейс** - указание интерфейса, на который будет передаваться исходящий трафик для правил преобразования адресов отправителя (SNAT) и правил «маскировки» (masquerade). Возможно указать следующие значения:
  - **Интерфейс** - ввести наименование сетевого интерфейса. В этом поле возможно использовать следующие символы:

символы латинского алфавита; цифры; подстановочный знак **«*»** (например, «eth1*» — все интерфейсы, имена которых начинаются с «eth1»); **«any»** (система будет обрабатывать весь входящий трафик независимо от того, через какой интерфейс он пришёл). Имя интерфейса должно начинаться с латинской буквы, иметь длину не более 14 символов, подстановочный знак должен располагаться в конце.

- **Группа интерфейсов** - выбор из предложенного списка название ранее созданной группы интерфейсов.

При установке флажка в чек-боксе **«Все кроме указанного интерфейса»** правило будет срабатывать на всех интерфейсах, кроме указанного.

- **«Транспортный протокол»** - указание протоколов, для которых осуществляется преобразование сетевых адресов. Возможно указать значение номером или именем протокола:
  - **«Название»** - выбор транспортного протокола из выпадающего списка;
  - **«Номер»** - номер протокола в соответствии с документом IANA. Возможно указать значение в диапазоне от «0» до «255».
- **Отправитель** - указать параметры отправителя, на основе которых будет осуществляться сопоставление в правиле NAT:
  - **«Вид отправителя»** - выбор вида отправителя из списка, который будет использоваться для проверки соответствия сетевого пакета правилу NAT:
    - **«Адрес»** - IPv4-адрес отправителя для проверки соответствия в формате <x.x.x.x>;
    - **«Сеть»** - IPv4-сеть отправителя для проверки соответствия в формате <x.x.x.x/x>;
    - **«Диапазон адресов»** - указать диапазон IPv4-адресов отправителя в соответствующих полях;
    - **«Группа адресов»** - выбрать группу адресов из списка;
    - **«Группа сетей»** - выбрать группу сетей из списка;
    - **«Группа доменов»** - выбрать группу доменов из списка.

Для типов отправителей **«Адрес»**, **«Сеть»** и **«Диапазон адресов»** доступна функция инверсии значений. Для её активации необходимо установить флажок в чекбоксе **«Все кроме указанного отправителя»**. В этом случае правило будет применяться ко всем адресам, за исключением указанных.

При выборе одной из **групп** предусмотрена возможность указать дополнительные категории групп: **«Группа MAC-адресов»** и **«Группа портов»** (группа портов доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP).

- **«Группа MAC-адресов»** - указать группу MAC-адресов отправителя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
- **«Порт отправителя»** - секция параметров доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP. Возможно настроить следующие параметры:
  - **«Группа портов»** - указать группу портов отправителя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
  - **«Порты»** - указать порт отправителя, который будет использоваться для проверки соответствия сетевого пакета правилу NAT. Для конфигурации портов необходимо нажать **кнопку** « » справа от поля **«Настройка портов»** и в раскрывшемся поле нажать **кнопку «+Добавить»**. Доступны следующие параметры:
    - **«Номер порта»** - в поле **«Порт»** ввести номер порта в диапазоне от «1» до «65535»;
    - **«Диапазон портов»** - указать диапазон портов в соответствующих полях;
    - **«Протокол»** - выбрать протокол из списка.

    Кнопки «+Добавить» и «**Удалить»** позволяют добавлять или удалять порты отправителя.

При установке флажка в чекбоксе **«Все кроме указанных портов»** правило будет применяться ко всем портам, за исключением указанных.

- **Получатель** - указать параметры получателя, на основе которых будет осуществляться сопоставление в правиле NAT:
  - **«Вид получателя»** - выбор вида получателя из списка, который будет использоваться для проверки соответствия сетевого пакета правилу NAT:
    - **«Адрес»** - IPv4-адрес получателя для проверки соответствия в формате <x.x.x.x>;
    - **«Сеть»** - IPv4-сеть получателя для проверки соответствия в формате <x.x.x.x/x>;
    - **«Диапазон адресов»** - указать диапазон IPv4-адресов получателя в соответствующих полях;
    - **«Группа адресов»** - выбрать группу адресов из списка;
    - **«Группа сетей»** - выбрать группу сетей из списка;
    - **«Группа доменов»** - выбрать группу доменов из списка.

    Для типов получателя **«Адрес»**, **«Сеть»** и **«Диапазон адресов»** доступна функция инверсии значений. Для её активации необходимо установить флажок в чекбоксе **«Все кроме указанного получателя»**. В этом случае правило будет применяться ко всем адресам, за исключением указанных.

    При выборе одной из **групп** предусмотрена возможность указать дополнительные категории групп: **«Группа MAC-адресов»** и **«Группа портов»** (группа портов доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP).
  - **«Группа MAC-адресов»** - указать группу MAC-адресов получателя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
  - **«Порт получателя»** - секция параметров доступна при условии выбора транспортного протокола типа TCP, UDP или TCP/UDP. Возможно настроить следующие параметры:

- **«Группа портов»** - указать группу портов получателя, которые будут использоваться для проверки соответствия сетевых пакетов правилу NAT.
- **«Порты»** - указать порт получателя, который будет использоваться для проверки соответствия сетевого пакета правилу NAT. Для конфигурации портов необходимо нажать **кнопку** « » справа от поля **«Настройка портов»** и в раскрывшемся поле нажать **кнопку «+Добавить»**. Доступны следующие параметры:
  - **«Номер порта»** - в поле **«Порт»** ввести номер порта в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - указать диапазон портов в соответствующих полях;
  - **«Протокол»** - выбрать протокол из списка.

  Кнопки «+Добавить» и «**Удалить»** позволяют добавлять или удалять порты получателя.

  При установке флажка в чекбоксе **«Все кроме указанных портов»** правило будет применяться ко всем портам, за исключением указанных.

- **«Преобразованный адрес»** - указать адрес, на который будет заменён исходный адрес назначения пакетов. Возможен выбор следующих значений:
  - **«Адрес»** - IP-адрес в формате IPv4;
  - **«Диапазон адресов»** - указать диапазон IP-адресов в соответствующих полях;
  - **«Сеть»** - указать сеть: IP-адрес и маску подсети.
- **«Преобразованный порт»** - указать порт для трансляции. Возможен выбор следующих значений:
  - **«Номер порта»** - ввести номер порта в диапазоне от «1» до «65535»;

- **«Диапазон портов»** - указать диапазон портов в соответствующих полях.

- **«Перенаправление трафика»** - указать порт, на который будет перенаправляться входящий трафик. Возможен выбор следующих значений:
  - **«Номер порта»** - ввести номер порта в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - указать диапазон портов в соответствующих полях.
- **«Дополнительные параметры NAT преобразованного адреса»** - секция настроек дополнительных параметров NAT:
  - **«Назначение IP-адреса»** - определить тип механизма сопоставления адресов для трансляции в правиле NAT:
    - **«Случайный IP»** (random) - случайное распределение адресов отправителя или получателя для каждого соединения. Используется по умолчанию.
    - **«Постоянный IP»** (persistent)- пользователь получает один и тот же адрес отправителя или получателя для каждого соединения.
  - **«Назначение порта»** - определить метода сопоставления портов при трансляции адресов в правилах NAT:
    - **«Порт без изменений»** (none) - отключает динамическое сопоставление портов, использует исходный порт исходного пакета. Используется по умолчанию.
    - **«Случайный порт»** (random)- выбирает случайный доступный порт из диапазона трансляции.
- **«Балансировка»**

  В рамках одного правила возможно определить несколько транслируемых адресов, чтобы NAT мог сбалансировать трансляцию между ними. Алгоритм балансировки использует хэш для распределения нагрузки. При определении транслируемых адресов, называемых бэкендами, необходимо настроить вес. Это позволяет пользователю самостоятельно определить распределение нагрузки в соответствии с его предпочтениями.

Параметры настройки балансировки:

- **«Метод распределения»** - выбрать алгоритм генерации хэша. Возможен множественный выбор следующих значений: «Случайное», «По IP-адресу отправителя», «По IP-адресу получателя», «По порту отправителя», «По порту получателя». Выбор значений «По порту отправителя» и «По порту получателя» допускается при указанном для параметра **«Транспортный протокол»** значении «tcp», «udp» или «tcp/udp». По умолчанию хэш генерируется случайным образом - метод **«Случайное»**.
- **«Настройка преобразованных IP-адресов»** - возможно указание преобразованных IP-адресов и веса для каждого бэкенда. Сумма всех весов, присвоенных бэкендам, должна составлять **«100»**. Иными словами, вес, присвоенный конкретному бэкенду, представляет собой процент соединений, которые будут направлены на этот бэкенд.

- **«Тип пакета»** - настроить правило соответствия на основе типа пакета. Возможно указание следующих типов: «Широковещательный пакет», «Одиночный пакет», «Пакеты для группы устройств», «Другие типы».

4. По завершении нажать **кнопку «Сохранить»**.
5. После сохранения нового правила NAT необходимо нажать **кнопку «Сохранить»** в правом верхнем углу формы **«Настройки межсетевого экрана»** для сохранения и применения новых настроек в системе **ARMA Стена** (см. Рисунок – Кнопка сохранения и применения новых настроек системы).

11.4 Создание правила One-to-one

Для создания правила **One-to-one** необходимо выполнить следующие действия:

1. Нажать **кнопку «+Добавить»** в разделе **«One-to-one»**.
2. В открывшейся боковой панели выбрать создаваемую сущность «One-to-one» (см. Рисунок – Создание правила One-to-one):

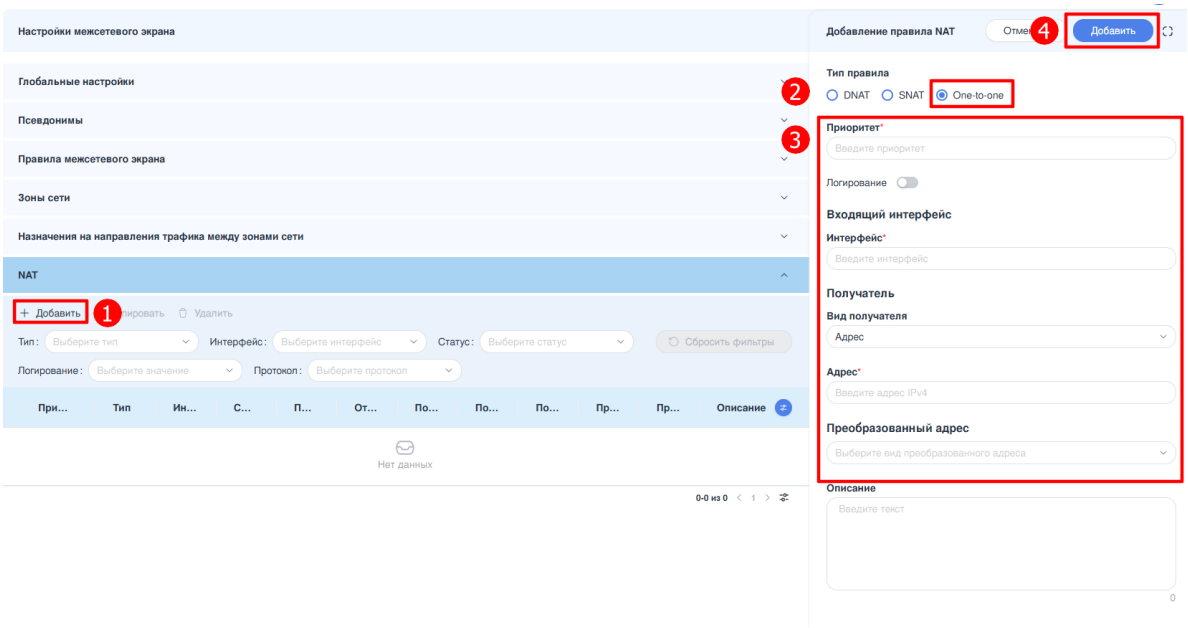


Рисунок – Создание правила One-to-one

3. Внести/скорректировать значение в полях:

- **Приоритет** - номер приоритета правила One-to-one. Возможно указать значение в диапазоне от «1» до «999999». Параметр должен быть уникальным в рамках выбранного набора правил и определяет последовательность выполнения правил от 1 к 999999.

  Примечание:

  Рекомендуется присваивать правилам NAT последовательные номера с интервалами между ними, оставляя свободные номера для новых правил.

- **Логирование** - включение/отключение журналирование действий.
- **Статус** - отключение правила преобразования сетевых адресов.
- **Входящий интерфейс** - указание входного интерфейса системы, на котором будет выполняться правило One-to-one. Допускается указать значение **«any»** - система будет обрабатывать весь входящий трафик независимо от того, через какой интерфейс он пришёл.
- **«Вид получателя»** - выбор вида получателя из списка:
  - **«Адрес»** - IP-адрес получателя в формате IPv4;
  - **«Сеть»** - указать сеть получателя: IP-адрес и маску подсети.
- **«Преобразованный адрес»** - указание преобразованного адреса. Возможен выбор следующих значений:
  - **«Адрес»** - IP-адрес в формате IPv4;
  - **«Сеть»** - указать сеть: IP-адрес и маску подсети.

4. По завершении нажать **кнопку «Сохранить»**.
5. После сохранения нового правила NAT необходимо нажать **кнопку «Сохранить»** в правом верхнем углу формы **«Настройки межсетевого экрана»** для сохранения и применения новых настроек в системе **ARMA Стена** (см. Рисунок – Кнопка сохранения и применения новых настроек системы).

11.5 Копирование правила NAT

Для копирования правила NAT необходимо выполнить следующие действия:

1. Выбрать правило, установив флажок в чек-боксе слева от наименования правила, и нажать **кнопку «Копировать»**.
2. В открывшейся боковой панели **«Копирование правила»** установить уникальное значение приоритета и внести необходимые корректировки.
3. Нажать **кнопку «Копировать»** (см. Рисунок – Копирование правила NAT).

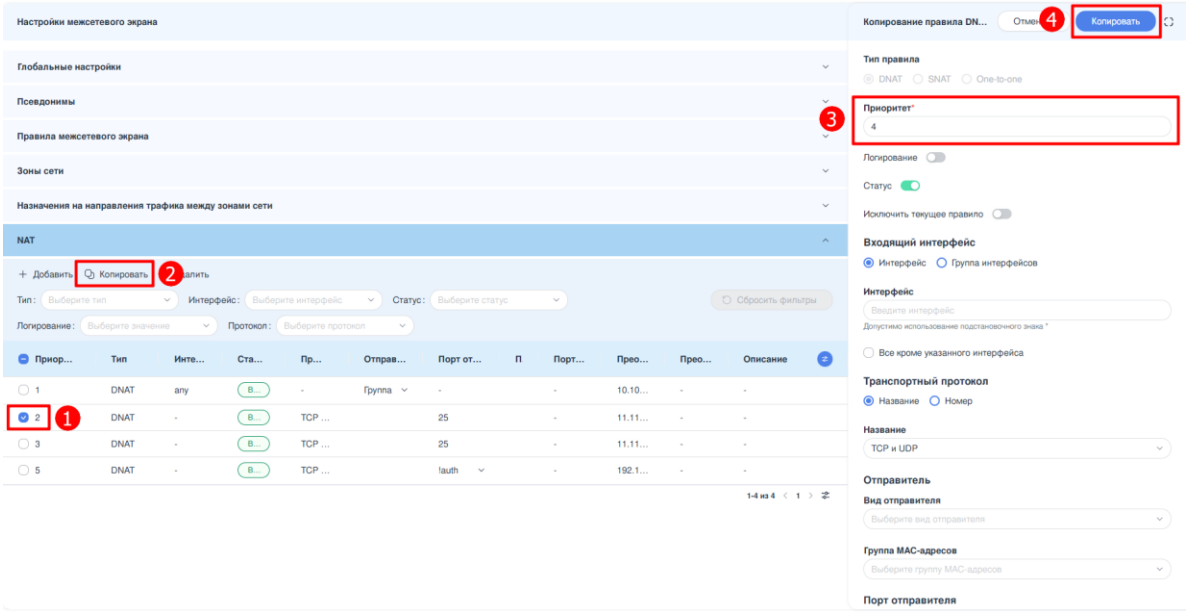


Рисунок – Копирование правила NAT

11.6 Редактирование правила NAT

Для редактирования правила NAT необходимо нажать **ЛКМ** на строке с нужным правилом и в открывшейся боковой панели внести корректировки в атрибуты правила. По завершении нажать **кнопку «Сохранить»**.

11.7 Удаление правила NAT

Для удаления правила NAT необходимо выполнить следующие действия:

1. Выбрать одно или несколько правил, установив флажок в чек-боксе слева от наименования правила, и нажать **кнопку «Удалить»**.

2. Подтвердить удаление правила нажатием **кнопки «Удалить»** в открывшемся окне (см. Рисунок – Подтверждение удаления правила NAT).

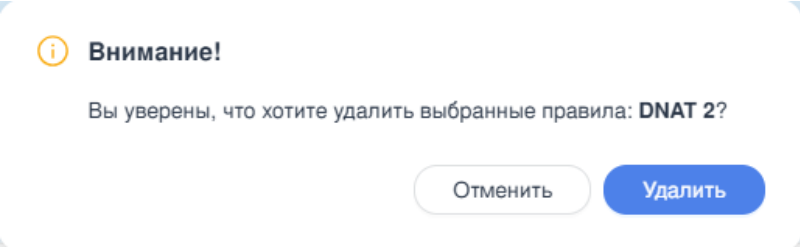


Рисунок – Подтверждение удаления правила NAT

12 БАЛАНСИРОВКА НАГРУЗКИ

12.1 Балансировка нагрузки на WAN-интерфейсах

Подсистема балансировки нагрузки автоматически добавляет маршруты для каждого пути в таблицу маршрутизации и балансирует трафик между настроенными интерфейсами в зависимости от работоспособности и веса интерфейса.

Минимально необходимая конфигурация для балансировки WAN-интерфейса должна включать в себя следующие элементы:

- требуется добавить как минимум один сетевой интерфейс маршрутизатора с заданным адресом и адресом следующего узла;
- необходимо добавить хотя бы одно правило с балансируемыми интерфейсами.

> **Примечание:**
>
> Балансировка нагрузки не используется совместно с динамической маршрутизацией. Сервис создаёт настраиваемые таблицы маршрутизации и правила брандмауэра, что делает его несовместимым с протоколами динамической маршрутизации.

Для настройки балансировочной нагрузки необходимо перейти в раздел **«Балансировка нагрузки на WAN-интерфейсах»** (**«Настройка интерфейсов» - «Балансировка нагрузки на WAN-интерфейсах»**) (см. Рисунок – Балансировка нагрузки на WAN-интерфейсах).

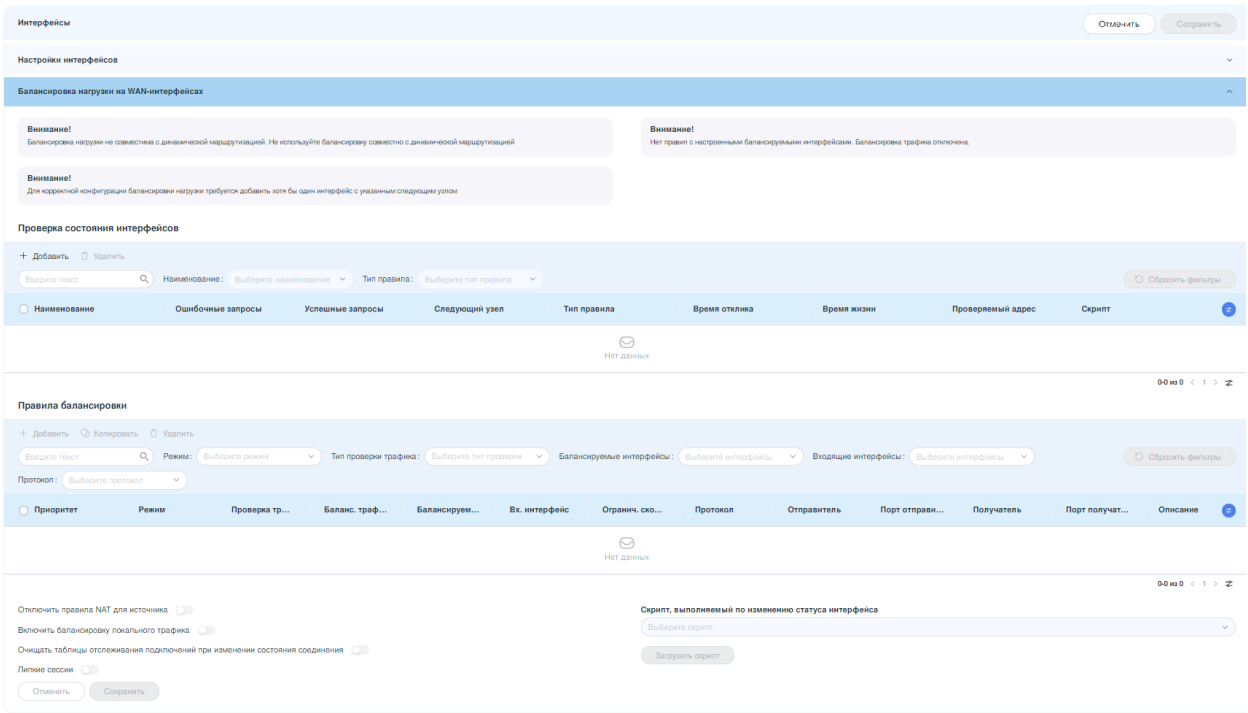


Рисунок – Балансировка нагрузки на WAN-интерфейсах

Применение и сохранение настроек подсистемы балансировки нагрузки на WAN-интерфейсах

Для применения и сохранения настроек после завершения конфигурации подсистемы балансировки нагрузки необходимо нажать **кнопку «Сохранить»**, расположенную в верхнем правом углу заголовка раздела **«Интерфейсы»** (см. Рисунок – Применение и сохранение настроек). Далее следует подтвердить действие в появившемся окне **«Сохранить изменения конфигурации»**, нажав **кнопку «Сохранить»**.

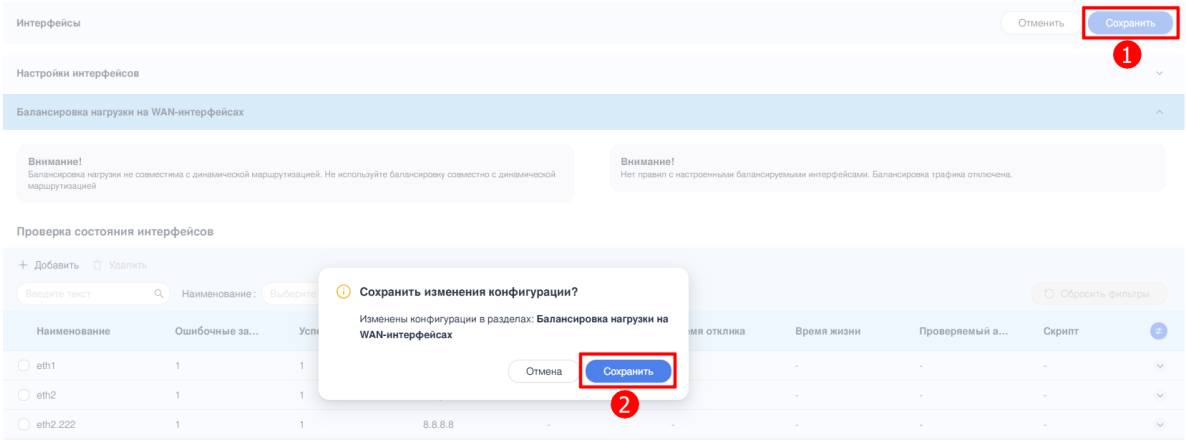


Рисунок – Применение и сохранение настроек

При необходимости отменить все неприменённые настройки следует нажать **кнопку «Отмена»**, расположенную в верхнем правом углу заголовка раздела **«Интерфейсы»**. В этом случае конфигурация подсистемы балансировки нагрузки будет откатана к последнему сохранённому состоянию.

12.1.1 Проверка состояния интерфейсов

Работоспособность WAN-каналов, используемых сервисом балансировки, периодически проверяется несколькими способами:

1. Отправка сообщения ICMP Echo Request на удалённые хосты.
2. Мониторинг времени жизни сетевого пакета (TTL).
3. Выполнение специального пользовательского скрипта.

Если канал не проходит проверку, он исключается из списка используемых сервисом балансировки.

12.1.1.1 Проверяемый интерфейс

Для добавления проверяемого интерфейса необходимо выполнить следующие действия:

1. Перейти в раздел **«Балансировка нагрузки на WAN-интерфейсах»** и нажать **кнопку «+ Добавить»** в подразделе **«Проверка состояния интерфейсов»**.

2. В открывшейся боковой панели выбрать создаваемый объект **«Проверяемый интерфейс»** и ввести необходимые параметры (см. Рисунок – Добавление проверяемого интерфейса):

   - **«Наименование»** - выбирать сетевой интерфейс из предложенного списка для активации на нём проверки WAN-канала;
   - **«Количество ошибок»** - указать количество неудачных проверок, после которых WAN-канал будет считаться недоступным. Возможно указать значение в диапазоне от «1» до «10»;
   - **«Количество успешных запросов»** - указать количество успешных проверок, после которых WAN-канал будет отмечен как доступный. Возможно указать значение в диапазоне от «1» до «10»;
   - **«Следующий узел»** - адрес узла, через который будет осуществляться доступ к хосту-получателю. Возможно указать **«IPv4-адрес»** или **«DHCP»**.

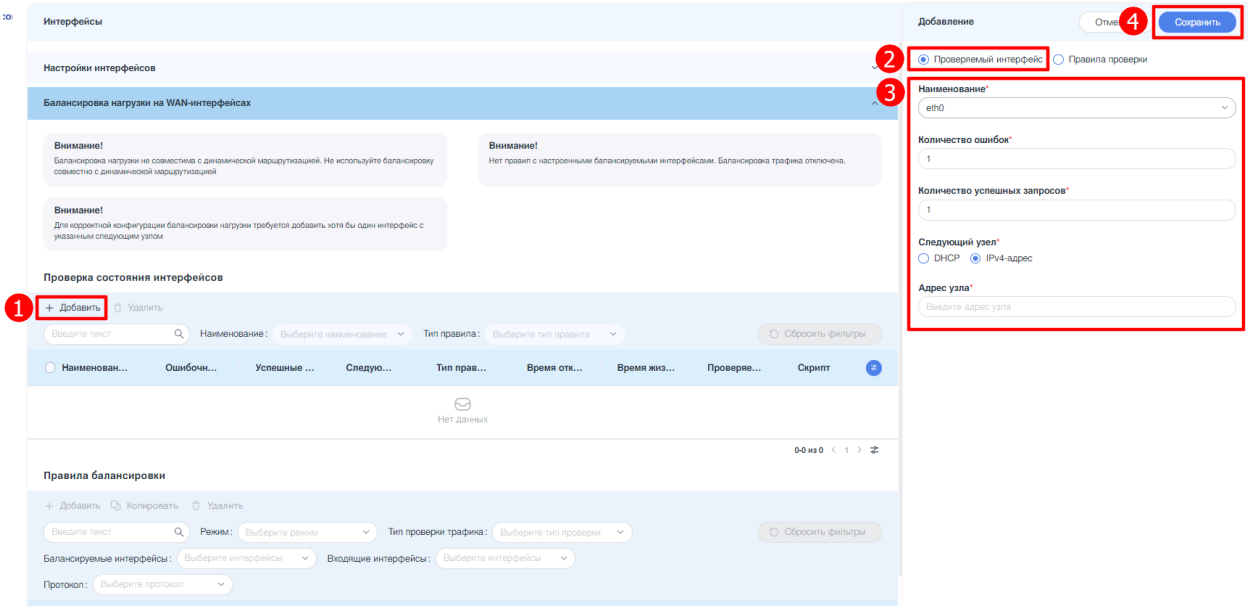


Рисунок – Добавление проверяемого интерфейса

Примечание:

Для корректной работы проверки состояния необходимо с помощью CLI-интерфейса ARMA Стена задать статический маршрут до следующего узла для каждого из проверяемых интерфейсов (см. раздел «Настройка статического маршрута» Руководства по настройке ARMA Стена в CLI).

Пример команды для настройки статического маршрута:

```
set protocols static route 8.8.8.8/32 next-hop 192.168.43.100 interface eth1
```

Для редактирования настроек проверяемого интерфейса необходимо нажать **ЛКМ** на строке с нужным интерфейсом и в открывшейся боковой панели внести корректировки. По завершению нажать **кнопку «Сохранить»**.

Для удаления проверяемого интерфейса необходимо выбрать один или несколько интерфейсов, установив флажок в чек-боксе слева от наименования интерфейса, и нажать **кнопку «Удалить»**. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

Примечание:

В случае удаления последнего проверяемого интерфейса или всех проверяемых интерфейсов система предупредит о том, что все правила и основные параметры балансировки будут удалены. Для продолжения необходимо подтвердить удаление (см. Рисунок – Удаление проверяемого интерфейса):

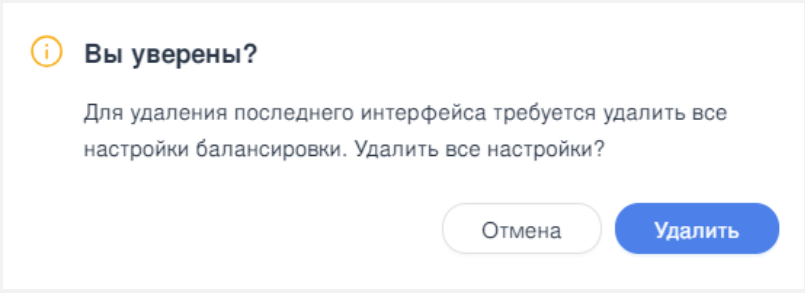


Рисунок – Удаление проверяемого интерфейса

12.1.1.2 Правила проверки

Каждая проверка настраивается для отдельного хоста-получателя и предполагает выполнение соответствующего теста. В случае необходимости проверки нескольких хостов-получателей необходимо настроить несколько тестов, каждый из которых будет выполняться в определённом порядке.

Для добавления правил проверки интерфейса необходимо выполнить следующие действия:

1. Перейти в раздел **«Балансировка нагрузки на WAN-интерфейсах»** и нажать **кнопку «+ Добавить»** в подразделе **«Проверка состояния интерфейсов»**.
2. В открывшейся боковой панели выбрать создаваемый объект **«Правила проверки»** и ввести необходимые параметры (см. Рисунок – Добавление правил проверки):
   - **«Интерфейс»** - указать из списка проверяемый интерфейс;
   - **«Приоритет»** - указать номер правила в соответствии с его очерёдностью. Возможно указать значение в диапазоне от «0» до «4294967295»;
   - **«Тип»** - указать тип теста. Возможно указать следующие значения:
     - **«ping»**;
     - **«TTL»**;
     - **«Пользовательский»** - указать пользовательский скрипт, описывающий характер проверки.

Для загрузки скрипта необходимо нажать **кнопку «Загрузить скрипт»** и в открывшемся окне проводника выбрать необходимый скрипт (см. Рисунок –Загрузка пользовательского скрипта):

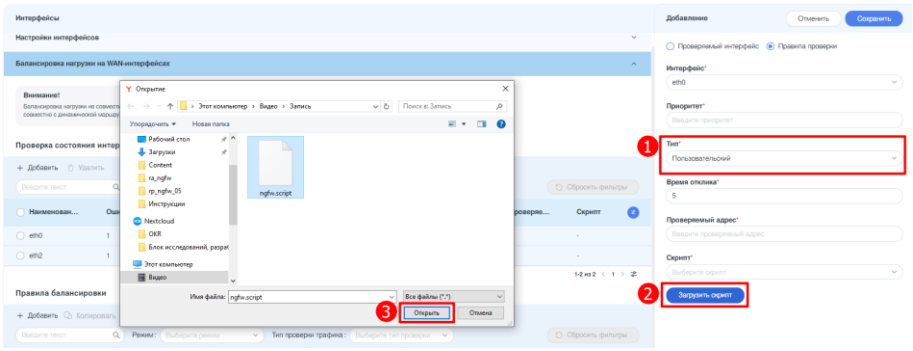


Рисунок – Загрузка пользовательского скрипта

Примечание:

Скрипт должен возвращать «0» для обозначения успешного результата и значение отличное от «0» - для неудачных результатов. Система перестанет отвечать на запросы, если выполнение скрипта не завершится!

Примечание:

Скрипт сохраняется в каталоге **/config/scripts**.

- **«Время отклика»** - указать значение максимального времени ожидания ответа на сообщение ICMP в секундах. Возможно указать значение в диапазоне от «1» до «30». По умолчанию используется значение «5».
- **«Предельное время жизни (число узлов)»** - параметр, который определяет количество переходов между каждой парой шлюзов на пути к хосту-получателю. Он используется для тестирования с протоколом UDP, когда выбирается тип тестирования **«TTL»**. Успешным результатом является получение в ответ сообщения ICMP Time Expired.
- **«Проверяемый адрес»** - указать IPv4-адрес хоста-получателя, на который будут отправляться сообщения ICMP Echo Request.

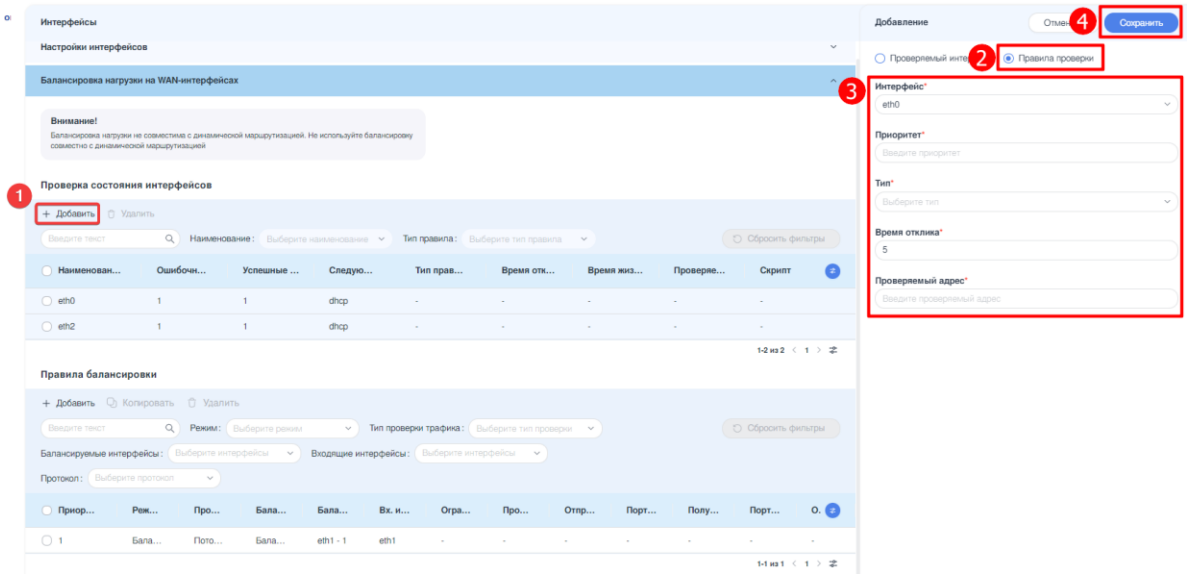


Рисунок – Добавление правил проверки

Для изменения настроек правил проверки интерфейса необходимо нажать **ЛКМ** на **кнопку** « » в правом углу строки с нужным интерфейсом в таблице **«Проверка состояния интерфейсов»**. В открывшемся списке правил необходимо выбрать нужное правило, также нажав на него **ЛКМ**. В боковой панели внести необходимые изменения. По завершению нажать **кнопку «Сохранить»**.

Для удаления правил проверки интерфейса необходимо выбрать одно или несколько правил проверки интерфейсов, установив флажок в чек-боксе слева от наименования правила, и нажать **кнопку «Удалить»**. В открывшемся окне подтвердить удаление нажатием **кнопки «Удалить»**.

12.1.1.3 Поиск и фильтрация

Блок фильтрации предоставляет возможность сортировки и фильтрации данных из таблицы **«Проверка состояния интерфейсов»** по всем столбцам в списке (см. Рисунок – Панель поиск и фильтрации). Он включает в себя следующие поля:

- **«Поиск»**;
- **«Наименование»**;
- **«Тип правила»**;
- **кнопка «Сбросить фильтры»**.

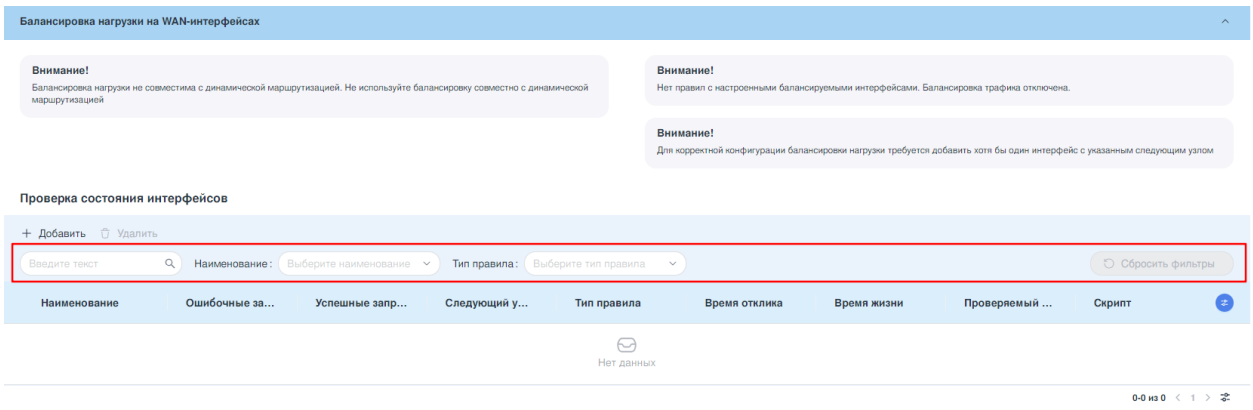


Рисунок – Панель поиск и фильтрации

Сквозной поиск по полям таблицы **«Проверка состояния интерфейсов»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск производится по наименованию сетевого интерфейса и номеру правил.

Фильтрация по полю **«Наименование»** позволяет осуществлять отбор данных на основе названий сетевых интерфейсов. В данном поле представлен раскрывающийся список с именами интерфейсов, добавленных в таблицу **«Проверка состояния интерфейсов»**.

Фильтрация по полю **«Тип правила»** позволяет отфильтровать правила по типу теста. Поле содержит выпадающий список и предоставляет выбор из следующих вариантов значений: *«ping», «TTL», «Пользовательский»*.

Сброс всех установленных фильтров осуществляется нажатием **кнопки «Сбросить фильтры»**.

12.1.2 Правила балансировки

Балансировка нагрузки представляет собой совокупность правил, определяющих тип трафика, подлежащего распределению, а также перечень таблиц маршрутизации и их значимости.

Каждое правило включает в себя критерии соответствия и таблицы маршрутизации с присвоенной значимостью. Правила пронумерованы и выполняются в установленном порядке, начиная с «1» и заканчивая «9999».

Важно отметить, что номер правила является уникальным идентификатором, который не может быть изменён. Для изменения номера правила необходимо удалить его и создать заново с новым номером. Рекомендуется назначать номера правил балансировки нагрузки, оставляя свободные интервалы. Например, возможно создать набор правил с номерами 10, 20, 30 и т. д. Это позволит в случае необходимости добавить новое правило в определённое место в текущей последовательности без удаления текущего набора правил.

12.1.2.1 Добавление правил балансировки

Для добавления правила балансировки необходимо выполнить следующие действия:

1. Перейти в раздел **«Балансировка нагрузки на WAN-интерфейсах»** и нажать **кнопку «+ Добавить»** в подразделе **«Правила балансировки»**.
2. В открывшейся боковой панели ввести необходимые параметры правила (см. Рисунок – Добавление правила балансировки):
   - **«Приоритет»** - уникальный номер приоритета правила балансировки трафика. Возможно указать номер приоритета в диапазоне от «1» до «9999».
   - **«Режим»** - режим работы правила:
     - **«Балансировка трафика»** - выполняется распределение трафика пропорционально отношению значимости интерфейса.
     - **«Резервирование канала»** - весь трафик идёт через основной интерфейс, а в случае его отказа - через резервный. В этом случае вместо балансировки трафика между всеми работоспособными WAN каналами трафик передаётся только по активному. В случае отказа активного WAN канала на эту роль выбирается другой из списка резервных на основе состояния и значимости интерфейса. Оставшиеся WAN каналы становятся резервными по отношению к новому активному.

     Роли WAN-каналов и соответствующих им интерфейсов могут быть выбраны на основе порядка правил балансировки. В связи с тем, что автоматическое перераспределение установленных ранее сессий между активными и резервными каналами WAN не осуществляется, необходимо включить параметр **«Очищать таблицы отслеживания подключений при изменении состояния соединения»**.
   - **«Тип проверки трафика»** - тип проверки трафика правилом:
     - **«Потоковый»** - для исходящего трафика по умолчанию применяется балансировка потоков в полном объёме. Для функционирования в данном режиме используется механизм отслеживания соединений на основе IP-адресов отправителя и получателя, а также номеров портов отправителя и получателя. Каждый поток связывается с определённым сетевым интерфейсом в соответствии с установленными правилами балансировки, в результате чего все сетевые пакеты, относящиеся к данному потоку, перенаправляются через этот интерфейс. Преимуществом данного режима работы является сохранение

последовательности пакетов при использовании различных скоростей передачи данных для различных подключений.

- **«Пакетный»** - балансировка пакетов для исходящего трафика позволяет достичь лучших показателей, но только при условии, что нарушение порядка пакетов не повлияет на функционирование сетевой инфраструктуры.

- **«Небалансируемый трафик»** - трафик, который соответствует правилу, не балансируется, а маршрутизируется в соответствии с записями в системной таблице маршрутизации. Параметр доступен при выборе режима «Балансировка трафика».
- **«Балансируемые интерфейсы»**:
  - **«Интерфейс»** - выбор из списка внешнего WAN-интерфейса для правила балансировки.
  - **«Значимость»** - отношение значимостей интерфейсов будет применяться с помощью алгоритма взвешенного случайного распределения в балансировке трафика. Пример, значимости 2 и 1 балансируемых интерфейсов означают, что через первый пойдёт 66% трафика, а через второй - 33%.

  Кнопки «+ Добавить» и «Удалить» позволяют добавлять или удалять балансируемые интерфейсы.
- **«Входящий интерфейс»** - выбор из списка внутреннего интерфейса для правила балансировки.
- **«Ограничение скорости»** - для правила возможно установить ограничение скорости передачи пакетов, чтобы применять правило к трафику выше или ниже заданного порога. Если в поле «Небалансируемый трафик» установлен флажок, то блок компонентов не отображается. Блок содержит следующие параметры:
  - **«Порог»** - выбор варианта сравнения, «Выше» или «Ниже» заданного лимита скорости.
  - **«Количество пакетов»** - количество сетевых пакетов. Возможно указать значение в диапазоне от «0» до «4294967295».
  - **«Период»** - период времени, в течение которого производится расчёт скорости.
  - **«Допустимое превышение лимита»** - количество пакетов, допустимое для превышения лимита в течение указанного периода времени. Возможно указать значение в диапазоне от «0» до «4294967295».

- **«Транспортный протокол»** - блок настройки протокола транспортного уровня инкапсулируемый в IP протокол. Возможно выбрать один из следующих вариантов:
  - **«Номер»** - ввести номер протокола в соответствии с документом IANA;

    Примечание:

    В случае необходимости выбора протоколов TCP или UDP, следует выбирать их из списка, представленного в поле «Название», а не указывать их числовое обозначение (6 - TCP, 17 - UDP) в поле «Номер». Указание протоколов TCP или UDP через числовое обозначение приводит к некорректной работе правила.

  - **«Название»** - выбор протокола из выпадающего списка.

  При установке флажка в чек-боксе «Все, кроме указанного протокола» правило будет срабатывать на трафик всех протоколов, кроме указанного.
- **«Отправитель»** - блок, в котором возможно настроить параметры правил в зависимости от источника трафика. Возможно выбрать один из следующих вариантов:
  - **«IP-адрес»** - ввести IPv4-адрес отправителя в поле «Адрес»;
  - **«Диапазон адресов»** - указать начальный и конечный IPv4-адрес отправителя в соответствующих полях;
  - **«Сеть»** - ввести IPv4-сеть отправителя в формате «x.x.x.x/x» в поле «Сеть».

    Если установить флажок в чек-боксе «Все, кроме указанного отправителя», то правило будет срабатывать для всех адресов, кроме заданных.
- **«Порт отправителя»** - блок настроек доступен, если в блоке «Транспортный протокол» в поле «Название» указано одно из следующих значений: **«tcp»** или **«udp»**. Указать порт возможно одним из следующих способов:
  - **«Номер порта»** - возможно указать значение в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - позволяет задать интервал портов в диапазоне от «1» до «65535»;
  - **«Протокол»** - выбор протокола из выпадающего списка.

При установке флажка в чек-боксе «Все, кроме указанных портов» правило будет срабатывать на все порты, кроме указанных. **Кнопки «+ Добавить» и «Удалить»** позволяют добавлять или удалять порты отправителя.

- **«Получатель»** - блок, в котором настраиваются параметры правил в зависимости от адресата трафика. Возможно выбрать один из следующих вариантов:
  - **«IP-адрес»** - ввести IPv4-адрес получателя в поле «Адрес»;
  - **«Диапазон адресов»** - указать начальный и конечный IPv4-адрес получателя в соответствующих полях;
  - **«Сеть»** - ввести IPv4-сеть получателя в формате «x.x.x.x/x» в поле «Сеть».

  Если установить флажок в чек-боксе «Все, кроме указанного получателя», правило будет действовать на все адреса, кроме заданных.
- **«Порт получателя»** - блок настроек доступен, если в блоке «Транспортный протокол» в поле «Название» указано одно из следующих значений: **«tcp»** или **«udp»**. Указать порт возможно одним из следующих способов:
  - **«Номер порта»** - возможно указать значение в диапазоне от «1» до «65535»;
  - **«Диапазон портов»** - позволяет задать интервал портов в диапазоне от «1» до «65535»;
  - **«Протокол»** - выбор протокола из выпадающего списка.

  При установке флажка в чек-боксе «Все, кроме указанных портов» правило будет срабатывать на все порты, кроме указанных. **Кнопки «+ Добавить» и «Удалить»** позволяют добавлять или удалять порты получателя.

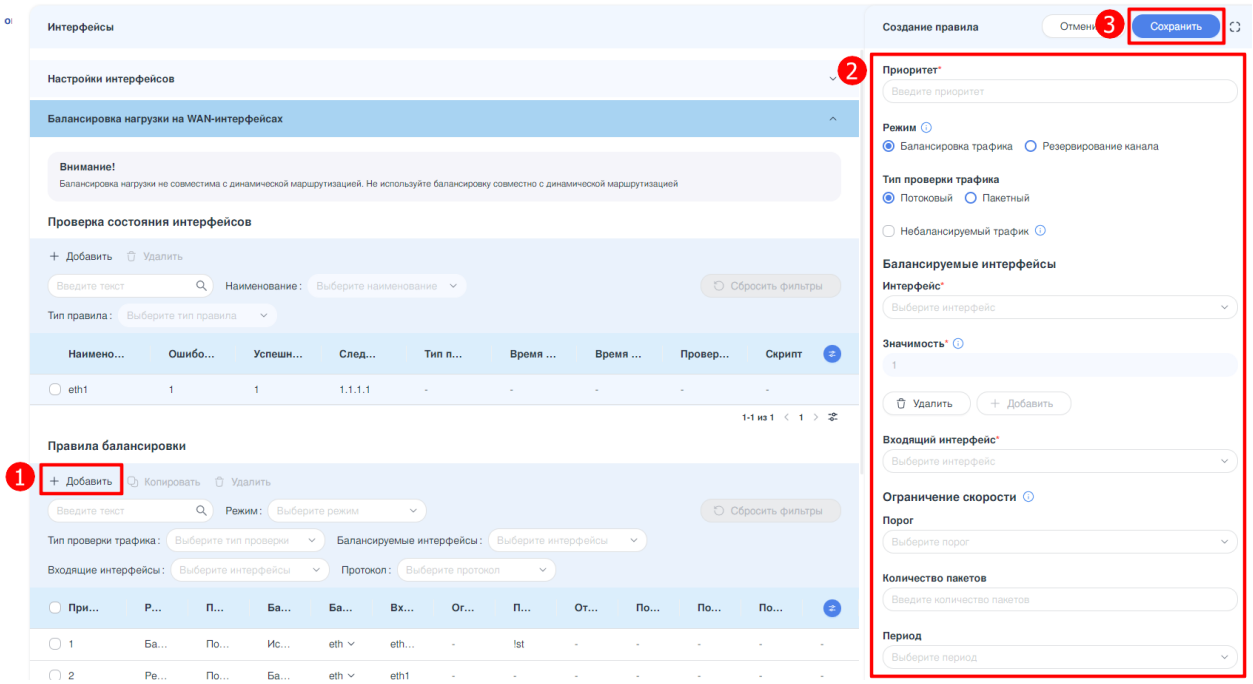


Рисунок – Добавление правила балансировки

12.1.2.2 Редактирование правил балансировки

Для редактирования правила балансировки необходимо нажать **ЛКМ** на строке с нужным правилом и в открывшейся боковой панели внести корректировки в атрибуты правила. По завершению нажать **кнопку «Сохранить»**.

12.1.2.3 Копирование правила балансировки

Для копирования правила балансировки необходимо выполнить следующие действия:

1. Выбрать правило, установив флажок в чек-боксе слева от приоритета правила, и нажать **кнопку «Копировать»**.
2. В открывшейся боковой панели «Копирование правила» установить приоритет и при необходимости внести изменения в параметры правила.
3. Нажать **кнопку «Сохранить»**, чтобы сохранить копию правила (см. Рисунок – Копирование правила балансировки).

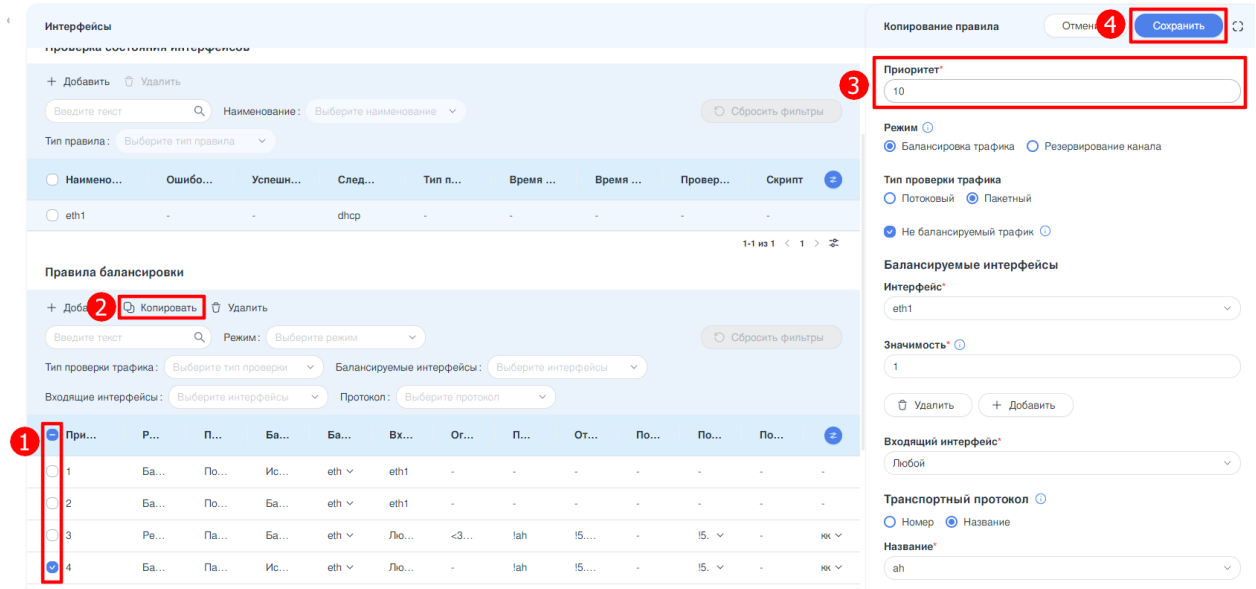


Рисунок – Копирование правила балансировки

12.1.2.4 Удаление правил балансировки

Для удаления правила балансировки необходимо выбрать одно или несколько правил, установив флажок в чек-боксе слева от приоритета правила, и нажать **кнопку «Удалить»**. В открывшемся окне, подтвердить удаление нажатием **кнопки «Удалить»**.

Примечание:

В случае удаления последнего правила балансировки система выдаст предупреждение о том, что служба балансировки перестанет функционировать. Будет предложено подтвердить удаление правила (см. Рисунок – Подтверждения удаления последнего правила балансировки):

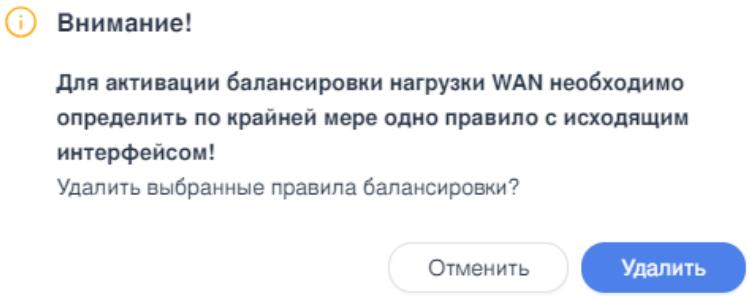


Рисунок – Подтверждения удаления последнего правила балансировки

12.1.3 Общие настройки балансировочной нагрузки

Примечание:

Общие параметры балансировки нагрузки недоступны для редактирования, если в таблице «Проверка состояний интерфейсов» не указан хотя бы один интерфейс.

1. **«Отключить правила NAT для источника»** - отключение механизма автоматической генерации правил SNAT.

   По умолчанию интерфейсы, используемые в пуле балансировки нагрузки, заменяют IP-адрес источника исходящего пакета на свой собственный адрес, что гарантирует поступление ответов на один и тот же интерфейс. Это работает с помощью автоматически сгенерированных правил SNAT, которые применяются только к сбалансированному трафику. В тех случаях, когда такое поведение нежелательно, автоматическую генерацию правил SNAT возможно отключить.

2. **«Включить балансировку локального трафика»** - включение балансировки нагрузки WAN для локального трафика.

3. **«Очищать таблицы отслеживания подключений при изменении состояния соединения»** - очистка таблицы соединений при изменении состояния активного WAN-канала.

   Примечание:

   Очистка таблицы соединений приведёт к тому, что будет выполняться балансировка пакетов вместо балансировки потоков до момента повторного установления соединений.

4. **«Липкие сессии»** - включение возможности отправки ответных пакетов с сетевого интерфейса, входящего в группу балансировочных интерфейсов, откуда поступил запрос.

5. **«Скрипт, выполняемый по изменению статуса интерфейса»** - выбор пользовательского скрипта, который будет запускаться при изменении состояния балансируемого интерфейса.

   Для загрузки пользовательского скрипта в систему **ARMA Стена** необходимо нажать **кнопку «Загрузить скрипт»** (см. Рисунок – Загрузка пользовательского скрипта). В появившемся диалоговом окне следует выбрать файл скрипта, располагающийся на локальном устройстве пользователя. Скрипты загружаются в директорию **/config/scripts**.

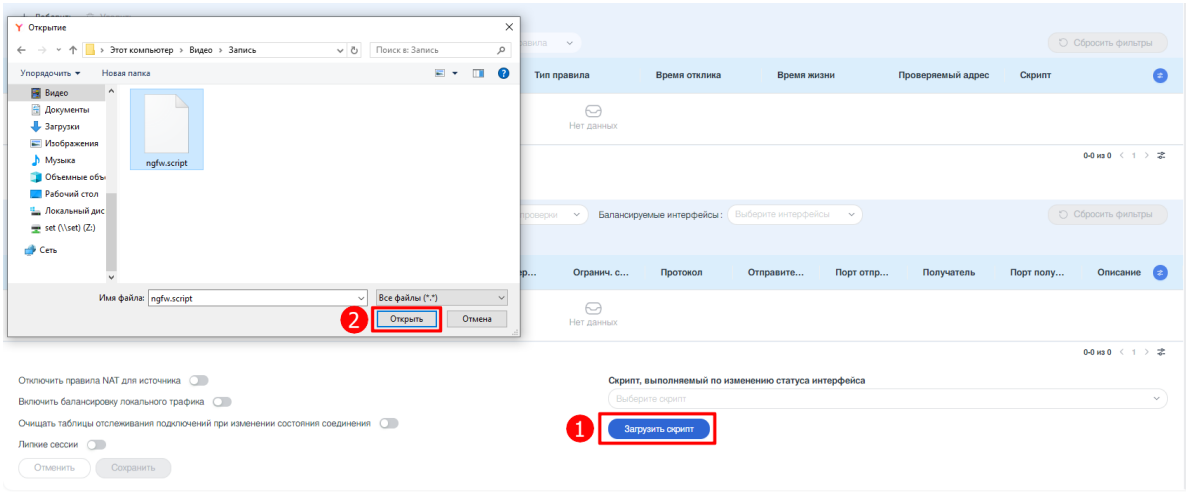


Рисунок – Загрузка пользовательского скрипта

Примечание:

В названии файла скрипта недопустимо использовать символы: пробел, «”», «\». Максимальный размер файла не более 1 мегабайта.

Примечание:

Скрипт должен возвращать «0» для обозначения успешного результата и значение отличное от «0» - для неудачных результатов. Система перестанет отвечать на запросы, если выполнение скрипта не завершится!

Для сохранения изменений в общих настройках балансировочной нагрузки необходимо нажать **кнопку «Сохранить** (см. Рисунок – Сохранение настроек).

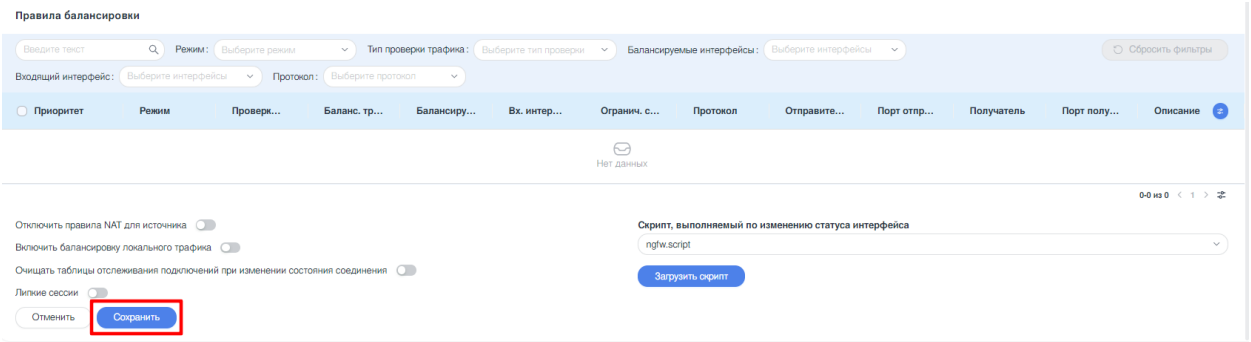


Рисунок – Сохранение настроек

Примечание:

Если минимально необходимые настройки балансировки не будут соблюдены, при попытке сохранить изменения система выдаст предупреждение о невозможности обновления настроек балансировки нагрузки на WAN-интерфейсах.

12.2 Обратный прокси

ARMA Стена включает в себя функциональность обратного прокси-сервера, обеспечивающего высокую доступность, распределение нагрузки и проксирование для приложений на основе TCP (уровень 4) и HTTP (уровень 7).

Для настройки обратного прокси необходимо перейти в раздел **«Интерфейсы»** затем в подраздел **«Обратный прокси»** (см. Рисунок – Обратный прокси).

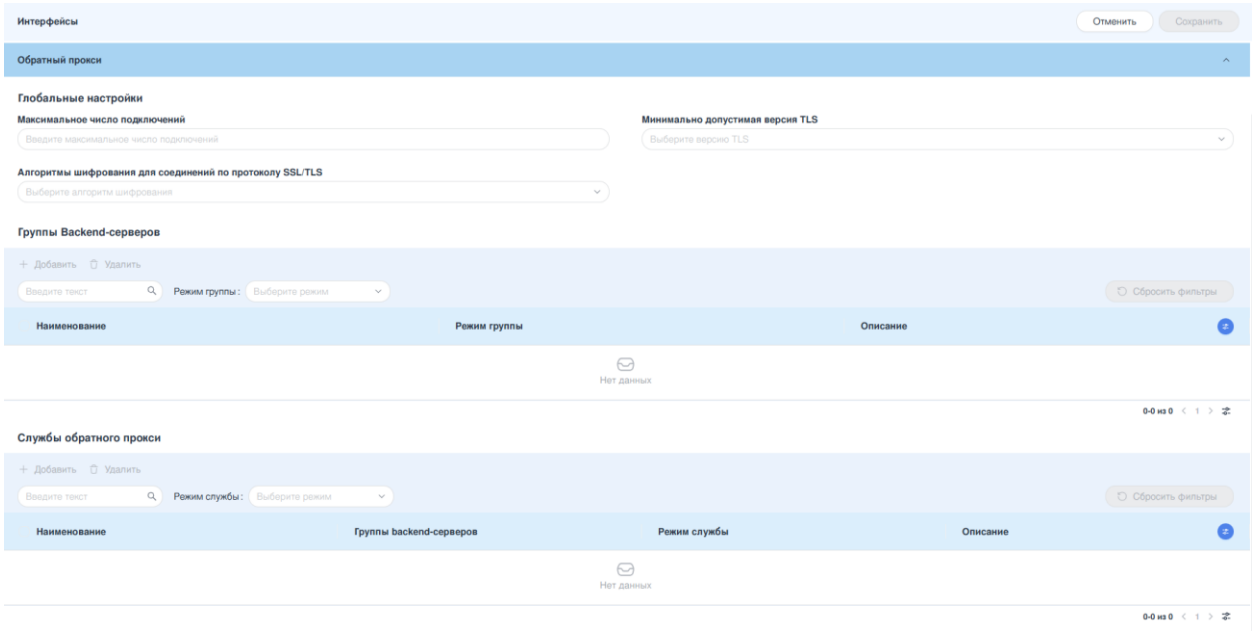


Рисунок – Обратный прокси

Минимально необходимая конфигурация для реализации обратного прокси должна включать в себя следующие элементы:

- добавлен минимум один backend-сервер (таблица **«Группы Backend-серверов»**), с хотя бы одним добавленным сервером (таблица **«Сервер»**);
- добавлена минимум одна служба обратного прокси (таблица «**Службы обратного прокси»**) с указанием следующих параметров: **«Порт, используемый для соединения»**, **«Группа Backend-серверов»**.

12.2.1 Глобальные настройки

1. **«Максимальное число подключений»** - используется для настройки максимального количества одновременных подключений для обратного прокси-сервера с балансировкой нагрузки. Позволяет ограничивать количество одновременных подключений к серверу с целью предотвращения его перегрузки, обеспечения стабильной работы при высоких нагрузках и эффективного управления ресурсами. Возможно указать значение в диапазоне от «1» до «2000000».
2. **«Алгоритмы шифрования для соединений по протоколу SSL/TLS»** - используется для настройки списка шифров, которые будут использоваться при

установлении SSL/TLS соединений через обратный прокси-сервер. Возможен множественный выбор.

3. **«Минимально допустимая версия TLS»** - указать минимальную поддерживаемую версию протокола TLS для всех SSL/TLS соединений через обратный прокси-сервер с балансировкой нагрузки. Возможно выбрать версию протокола TLS: 1.2 или 1.3. По умолчанию используется версия 1.3.

12.2.2 Группы Backend-серверов

Блок **«Группы Backend-серверов»** предназначен для конфигурации групп серверов, известных как бэкенд-серверы, которые обрабатывают входящие запросы, поступающие через обратный прокси-сервер. Основная функция данного блока заключается в реализации внутренней логики распределения трафика между серверами.

Для добавления группы backend-серверов необходимо выполнить следующие действия:

1. Нажать **кнопку «+ Добавить»** в таблице **«Группы Backend-серверов»** и в открывшемся окне **«Добавление группы Backend-серверов»** внести следующие параметры:

   - **Наименование** - уникальное имя группы. Допускается использование следующих символов: буквы латинского алфавита, цифры, дефис («-») и нижнее подчёркивание («_»).
   - **Режим группы backend-серверов** - режим определяет, какой протокол будет использоваться для взаимодействия с серверами бэкенда: **HTTP** или **TCP**. При выборе режима **HTTP** отобразится таблица **«Заголовки HTTP ответа»** для просмотра HTTP-заголовков ответов, которые был настроен для группы backend-серверов. Таблица предназначена для верификации установленных значений определённых заголовков и подтверждения соответствия конфигурации заданным параметрам.
   - **Алгоритм балансировки** - алгоритм балансировки нагрузки, который будет использоваться для распределения запросов между доступными серверами. Возможно указать следующие алгоритмы:
     - **source-address** - распределяет запросы на основе исходного IP-адреса клиента;
     - **round-robin** - распределяет запросы циклическим образом, последовательно отправляя каждый запрос следующему в очереди серверу. Используется по умолчанию;
     - **least-connection** - распределяет запросы на сервер с наименьшим количеством активных подключений.

- **Проверка состояния узла (без HTTP)** - выбрать протокол проверки состояния серверов, входящих в группу backend-серверов. Доступно при выборе режима группы backend-серверов - **«tcp»**. Данный параметр обеспечивает автоматическое отслеживание доступности серверов и исключение из пула недоступных экземпляров, что способствует повышению отказоустойчивости системы. Возможно выбрать следующие протоколы проверок:
    - **ldap** - проверка состояния сервера через протокол LDAP;
    - **mysql** - проверка состояния сервера через протокол MySQL;
    - **redis** - проверка состояния сервера через протокол Redis;
    - **pgsql** - проверка состояния сервера через протокол PostgreSQL;
    - **smtp** - проверка состояния сервера через протокол SMTP.
- **HTTP-проверка состояния узла** - блок компонентов, предназначенный для настройки и проведения оценки доступности веб-приложений, осуществляющих предоставление информации о своём состоянии через HTTP-запросы. Данный блок обеспечивает мониторинг работоспособности серверов в составе группы посредством инициации HTTP-запросов и последующего анализа полученных ответов.
    - **URI** - задать конечную точку, которая будет использоваться для проверки работоспособности сервера. URL должен начинаться с символа «/» и не должен содержать символ «#» или пробел.
    - **Метод** - выбрать используемый HTTP-метод проверки работоспособности сервера. Возможно выбрать следующие методы:
        - **options** - используется для запроса метаданных о поддерживаемых HTTP-методах на сервере;
        - **get** - запрашивает ресурс с сервера, включая заголовки и тело ответа;
        - **head** - аналогичен GET, но возвращает только заголовки ответа без тела;
        - **post** - отправляет данные на сервер для обработки;
        - **put** - используется для обновления ресурса на сервере.

- **Проверяемый атрибут ответа** - блок настройки условия, которое должно выполняться для того, чтобы сервер считался доступным в процессе проверки состояния. Условие может быть основано на HTTP-статусе ответа - **«Код ответа»** или содержимом тела ответа - **«Тело»**.
    - **Код ответа** - ожидаемый HTTP-статус ответа, который должен быть возвращён сервером для успешного прохождения health check. Возможно указать значение в диапазоне от «200» до «399». Поле становится доступным для ввода при условии, что значение компонента «Проверяемый атрибут ответа» установлено как «Код ответа».
    - **Содержимое тела ответа** - содержимое строки в теле HTTP-ответа. Если указанная строка присутствует в теле ответа, сервер считается доступным. Поле становится доступным для ввода при условии, что значение компонента «Проверяемый атрибут ответа» установлено как «Тело». Значение не должно начинаться с пробела или двойной косой черты «//». Максимально допустимое значение - «10000» символов.

- **Заголовки HTTP ответа** - блок настройки HTTP-заголовков, которые будут добавлены к ответам, отправляемых через обратный прокси-сервер. Настройки доступны при выборе режима группы backend-серверов - «http». Для добавления заголовков необходимо нажать **кнопку «+ Добавить»** и в открывшемся окне **«Добавить заголовок HTTP ответа»** внести следующие параметры:
    - **Наименование** - указать уникальное имя заголовка. Допускается использование следующих символов: буквы латинского алфавита в верхнем и нижнем регистре, дефис («-»).
    - **Значение** - значение заголовка HTTP-ответа. Допускается использование только латинские буквы, цифры и символы ASCII, за исключением «'», «"». Значение не должно начинаться с пробела или спецсимволов: «//», «-».
- **Серверы** - таблица настроек серверов в группе. Для добавления сервера необходимо нажать **кнопку «+ Добавить»** и в открывшемся окне **«Добавление сервера»** внести следующие параметры:

- **Наименование сервера** - указать уникальный идентификатор сервера. Допускается использование следующих символов: буквы латинского алфавита, цифры, дефис («-») и нижнее подчёркивание («_»). Максимально допустимое значение - «247» символов.
- **Адрес** - IP-адрес сервера в формате IPv4 <x.x.x.x> или IPv6 <h:h:h:h:h:h:h:h:>.
- **Порт** - номер порта. Возможно указать значение в диапазоне от «1» до «65535».
- **Проверка состояния сервера** - включение проверки состояние сервера. Если проверка включена, то сервер будет периодически проверяться на доступность. Сервер, не прошедший проверку, автоматически исключается из пула бэкенда.
- **Использовать как резервный сервер** - указать сервер в группе бэкэнда как резервный. Резервные серверы используются только в случае, если все основные серверы в пуле недоступны (например, не прошли health check или отключены). Это позволяет настроить отказоустойчивость системы, обеспечивая резервную обработку запросов.
- **Отправка заголовка прокси-протокола** - настроить передачу информации о клиенте (IP-адрес, порт) от reverse proxy к серверу бэкенда для обеспечения более точного логирования и анализа трафика. Возможно выбрать следующие значения:
    - **Версия 1 (текстовый формат)** - данные передаются в виде текстовой строки;
    - **Версия 2 (бинарный формат)** - данные передаются в виде бинарных блоков;
    - **Отключено** - информация не передаётся.

Для сохранения настроек сервера необходимо нажать **кнопку «Добавить»** (см. Рисунок – Добавление сервера в группу backend-серверов).

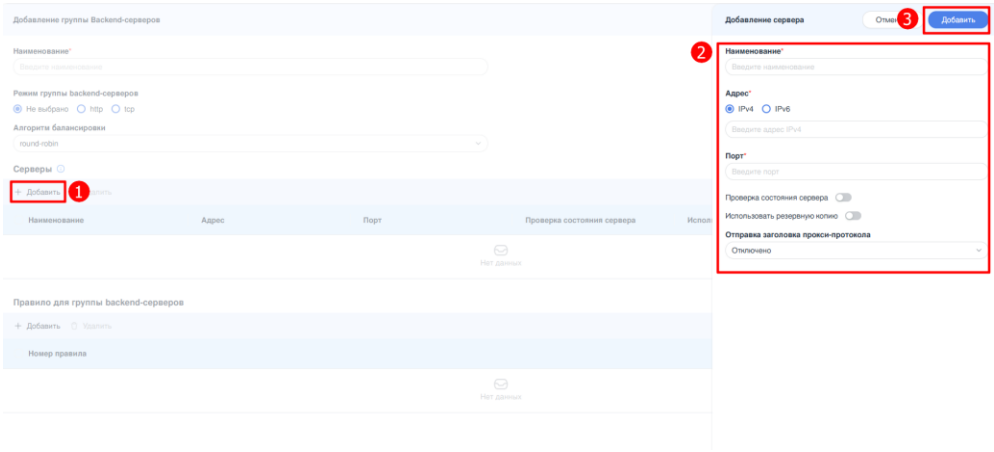


Рисунок – Добавление сервера в группу backend-серверов

- **SSL-шифрование и проверка подлинности** - настроить проверку подлинности SSL-сертификата. Возможно выбрать следующие значения из списка:
    - **Корневой сертификат SSL** - проверки подлинности SSL-сертификата backend-сервера с использованием указанного CA-сертификата. При выборе данного параметра откроется дополнительное поле **«Корневой сертификат SSL»**, предназначенное для выбора SSL-сертификата из списка сертификатов, уже установленных в системе.
    - **Без проверки сертификата сервера** - отключить проверку подлинности SSL-сертификата backend-сервера.
- **Таймаут проверки установки соединения** - установить таймаут ожидания ответа от backend-сервера при выполнении проверки работоспособности. Если ответ не получен в течение указанного времени, backend-сервер считается недоступным. Возможно указать значение в диапазоне от «1» до «3600» секунд.
- **Таймаут ожидания успешной попытки подключения к серверу** - установить максимальное время ожидания для установления соединения с backend-сервером. Если соединение не будет установлено за указанное время, попытка считается неудачной. Возможно указать значение в диапазоне от «1» до «3600» секунд.
- **Таймаут бездействия на стороне сервера** - установить максимальное время, в течение которого соединение с backend-сервером остаётся неактивным. Если за это время не происходит никакой активности, соединение закрывается. Возможно указать значение в диапазоне от «1» до «3600» секунд.

2. По завершению настроек нажать **кнопку «Добавить»** (см. Рисунок – Добавление группы backend-серверов).

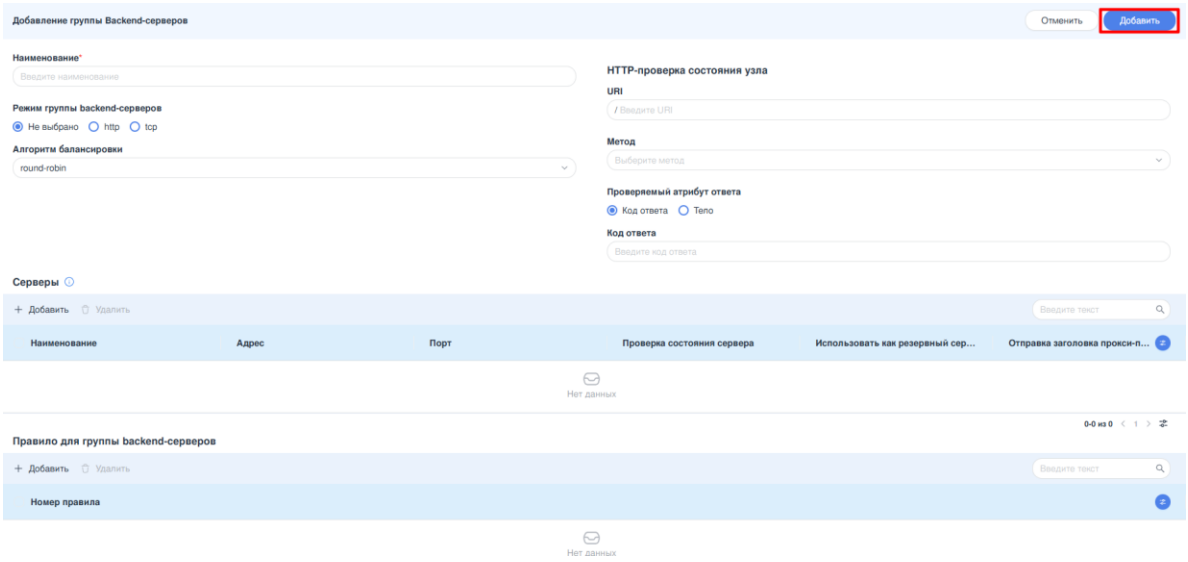


Рисунок – Добавление группы backend-серверов

12.2.2.1 Правило для группы backend-серверов

Для управления распределением трафика между серверами группы backend-серверов используются правила. Правила предоставляют функционал для гибкой и контролируемой маршрутизации запросов, что является особенно важным в сложных системах с большим количеством серверов и сервисов. Они предоставляют возможность разработки сложных алгоритмов маршрутизации, основанных на параметрах запроса таких как URL-путь, доменное имя или использование SSL/TLS. Каждое правило определяет условия, при которых запросы перенаправляются на соответствующие серверы.

Для создания правил в группе backend-серверов необходимо выполнить следующие действия:

1. В таблице **«Группы Backend-серверов»** выбрать нужную группу, нажав **ЛКМ** по соответствующей строке.
2. В открывшемся окне **«Группа Backend-серверов <имя_группы>»** нажать **кнопку «+ Добавить»** в таблице **«Правило для группы backend-серверов»**.
3. В окне **«Добавление правила группы backend-серверов»** внести необходимые параметры:
   - **Номер правила** - уникальный идентификатор правила. Возможно указать значение в диапазоне от «1» до «10000».
   - **Шаблоны поиска совпадений в пути URL** - таблица шаблонов поиска в URL. Для добавления шаблона необходимо нажать **кнопку «+ Добавить»** и в открывшемся окне **«Добавить шаблон поиска в URL»** указать следующие обязательные параметры (см. Рисунок – Добавление шаблона поиска в URL):

- **Режим поиска** - позволяет настроить условия правила для маршрутизации запросов на основе URL-пути. Возможно выбрать следующие значения:
    - **begin - Совпадение в начале** - запрос соответствует правилу, если URL начинается с указанного значения;
    - **end - Совпадение в конце** - запрос соответствует правилу, если URL заканчивается на указанное значение;
    - **exact - Полное совпадение** - запрос соответствует правилу, если URL полностью совпадает с указанным значением.
- **Содержимое шаблона поиска в URL** - значение URL-пути, используемое для сопоставления. Значение должно начинаться с символа «/». Допустимо использование букв латинского алфавита и цифр. В строке могут присутствовать следующие символы: «.», «-», «/», «-».

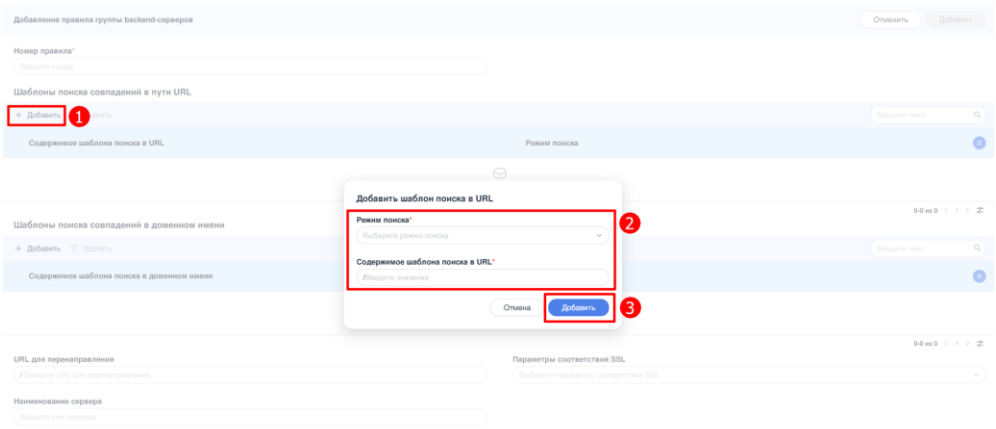


Рисунок – Добавление шаблона поиска в URL

- **Шаблоны поиска совпадения в доменном имени** - таблица шаблонов поиска в доменном имени. Для добавления шаблона необходимо нажать **кнопку «+ Добавить»**. В открывшемся окне **«Добавить шаблон поиска в доменном имени»** указать в поле **«Содержимое шаблона поиска в доменном имени»** значение доменного имени, используемое для сопоставления (см. Рисунок – Добавление шаблона поиска совпадения в доменном имени). Максимальная длина доменного имени не должна превышать 242 символов. В составе доменного имени разрешены точка и дефис, при условии, что они не находятся на первой и последней позициях. Длина каждой доменной группы не должна превышать 63 символов.

Количество доменных групп, разделённых точками, не должно превышать 127.

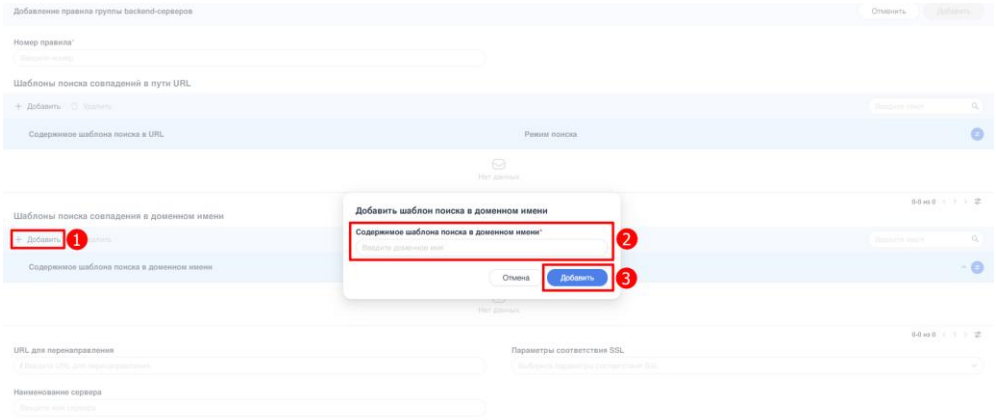


Рисунок – Добавление шаблона поиска совпадения в доменном имени

- **URL для перенаправления** - перенаправление (редирект) запросов на указанный URL. Данная функция позволяет эффективно управлять миграцией доменных имён, обновлением API, принудительным переходом на протокол HTTPS и другими сценариями, требующими изменения адреса запроса. Значение должно начинаться с символа «/». Допустимо использование букв латинского алфавита и цифр. В строке могут присутствовать следующие символы: «.», «-», «/», «-». Максимальная длина значения не должна превышать 242 символов.
- **Наименование сервера** - имя сервера, на который будет направлен трафик соответствующий данному правилу. Допускается использование следующих символов: буквы латинского алфавита, цифры, дефис («-») и нижнее подчёркивание («_»).
- **Параметры соответствия SSL** - настроить условия правила для маршрутизации запросов на основе SSL/TLS и связанных с ним параметр Server Name Indication (SNI). SNI — это расширение протокола TLS, которое позволяет клиенту указать имя домена в начале SSL-соединения. Данная функция особенно актуальна для работы с несколькими доменами на одном IP-адресе. Возможно выбрать следующие параметры сопоставления данных:
    - **req-ssl-sni** - сопоставление SNI из запроса клиента;
    - **ssl-fc-sni** - сопоставляет значение SNI, извлечённое из фронтенд-соединения (frontend connection) SSL/TLS. Используется для проверки SNI на уровне входящего соединения;

- **ssl-fc-sni-end** - сопоставляет значение SNI в конце фронтенд-соединения SSL/TLS. Используется в редких случаях, когда SNI проверяется в конце соединения.

4. По завершению настроек нажать **кнопку «Добавить»** (см. Рисунок – Добавление правила для группы backend-серверов).

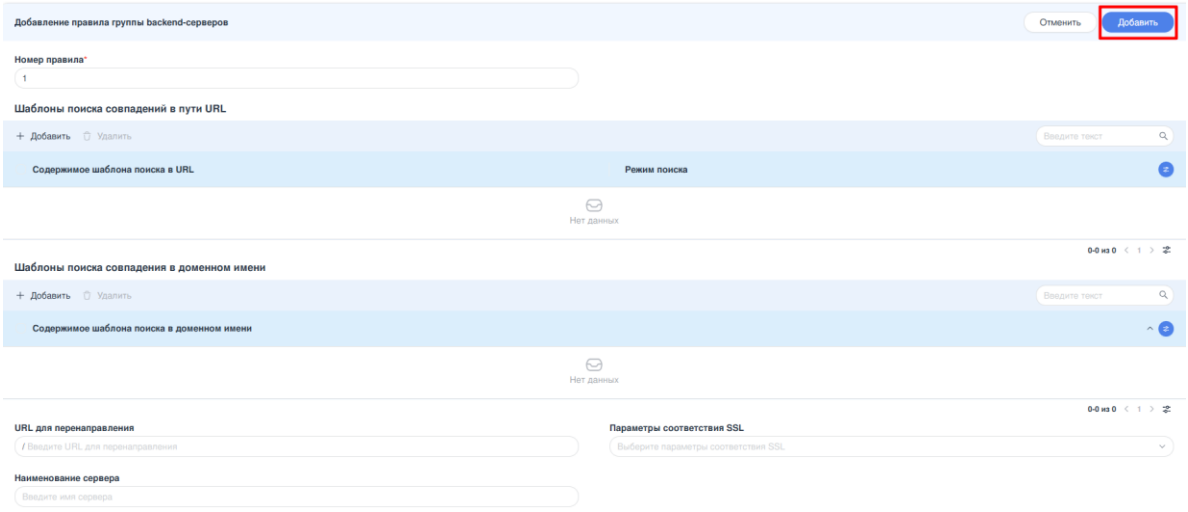


Рисунок – Добавление правила для группы backend-серверов

12.2.3 Службы обратного прокси

Раздел **«Службы обратного прокси»** отвечает за определение параметров точек входа для внешнего сетевого трафика. Она включает указание IP-адреса и порта, на которых будет осуществляться мониторинг входящих соединений, а также выбор протоколов. Конфигурация также определяет параметры обработки SSL/TLS для обеспечения защищённого взаимодействия с клиентами. Дополнительно она включает правила маршрутизации, такие как сопоставление доменных имён или путей запросов с соответствующими backend-серверами.

Для добавления службы обратного прокси необходимо выполнить следующие действия:

1. Нажать **кнопку «+ Добавить»** в таблице **«Службы обратного прокси»** и в открывшемся окне **«Добавление службы обратного прокси»** внести следующие параметры (см. Рисунок – Добавление службы обратного прокси):

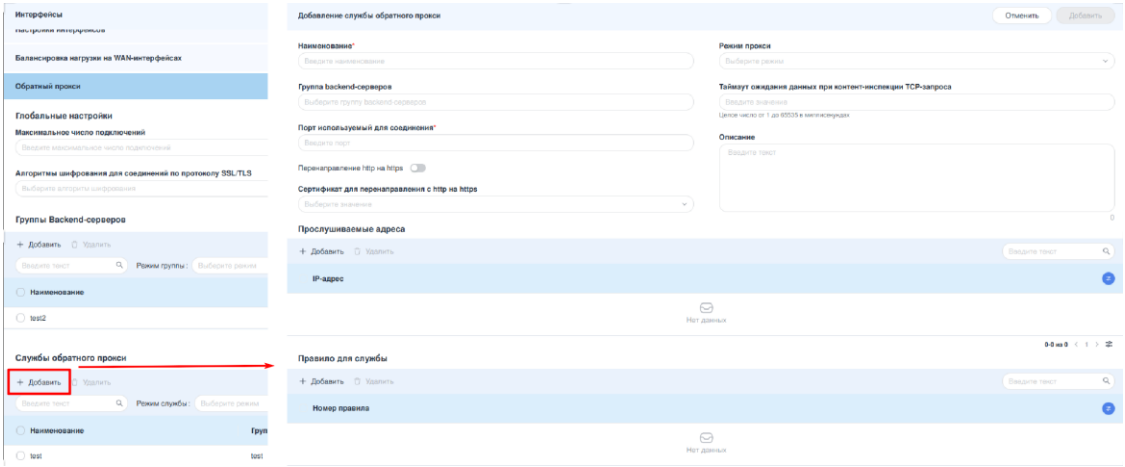


Рисунок – Добавление службы обратного прокси

- **Наименование** - уникальное имя службы. Допускается использование следующих символов: буквы латинского алфавита, цифры, дефис («-») и нижнее подчёркивание («_»).
- **Группа backend-серверов** - выбор группы backend-серверов, которая будет обрабатывать запросы.
- **Порт используемый для соединения** - номер порта, на котором обратный прокси будет принимать входящие подключения для указанного сервиса. Возможно указать значение в диапазоне от «1» до «65535».
- **Перенаправлять http на https** - включает автоматическое перенаправление HTTP-запросов на HTTPS.
- **Сертификат для перенаправления с http на https** - выбрать сертификат(ы), который будет использоваться для шифрования трафика.
- **Режим прокси** - выбрать режим работы сервиса (**http** или **tcp**) для обратного прокси, влияющий на тип обрабатываемого трафика.
- **Таймаут ожидания данных при контент-инспекции TCP-запроса** - время ожидания (в миллисекундах) данных от клиента при анализе TCP-соединений. Параметр определяет сколько времени балансировщик будет ждать данные от клиента, прежде чем закрыть соединение. Возможно указать значение в диапазоне от «1» до «65535».
- **Заголовки HTTP ответа** - таблица **«Заголовки HTTP ответа»** становится доступном для конфигурирования при выборе режима прокси «http». Для добавления заголовка HTTP ответа необходимо нажать **кнопку «+ Добавить»** на панели инструментов таблицы. В открывшемся окне **«Добавить заголовок HTTP ответа»** внести значения в следующие поля (см. Рисунок – Добавление заголовка HTTP ответа):

- **Наименование** - допускается использование только латинские буквы и символ дефиса («-»). Длина значения не должна превышать 64 символов.
- **Значение** - допускается использование только латинские буквы, цифры и символы ASCII, за исключением «'», «"». Значение не должно начинаться с пробела или спецсимволов: «//», «-».

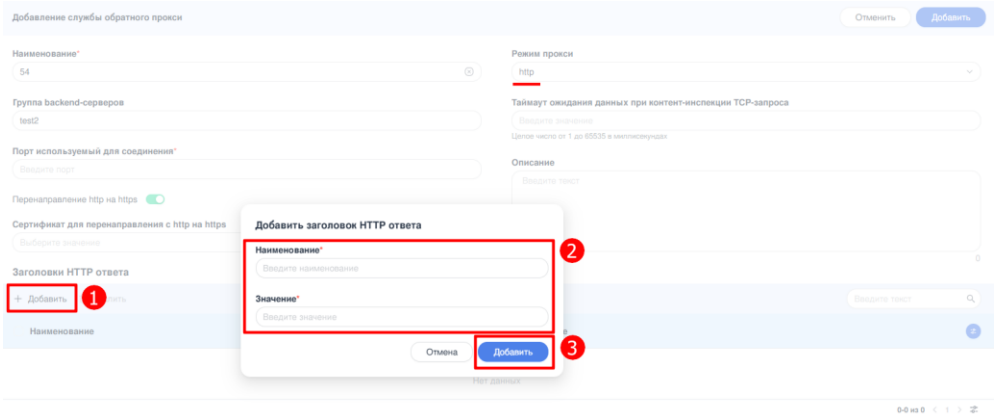


Рисунок – Добавление заголовка HTTP ответа

- **Прослушиваемые адреса** - локальный IP-адрес интерфейса, на котором обратный прокси будет принимать клиентские запросы. Для добавления IP-адрес необходимо нажать **кнопку «+ Добавить»** на панели инструментов. В открывшемся окне **«Добавить прослушиваемый адрес»** следует выбрать тип IP-адреса (IPv4 или IPv6) и указать соответствующий адрес (см. Рисунок – Добавление прослушиваемого адреса).

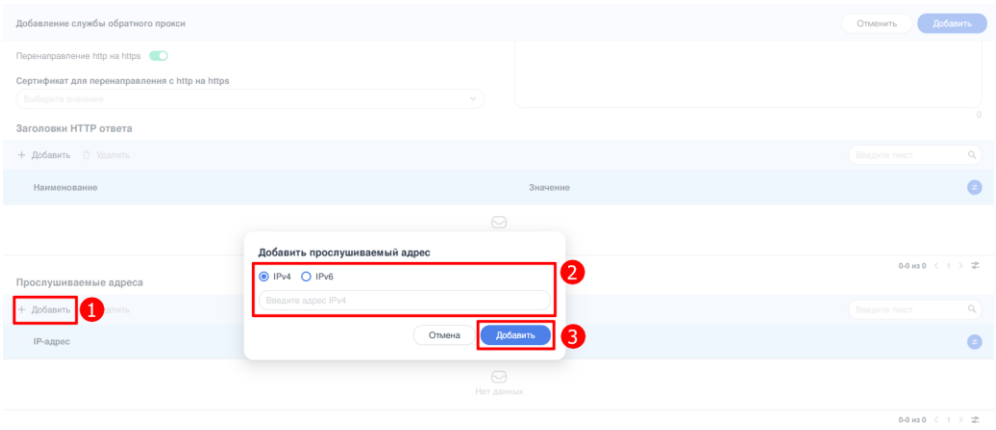


Рисунок – Добавление прослушиваемого адреса

2. По завершению настроек нажать **кнопку «Добавить»** (см. Рисунок – Сохранение конфигурации службы обратного прокси).

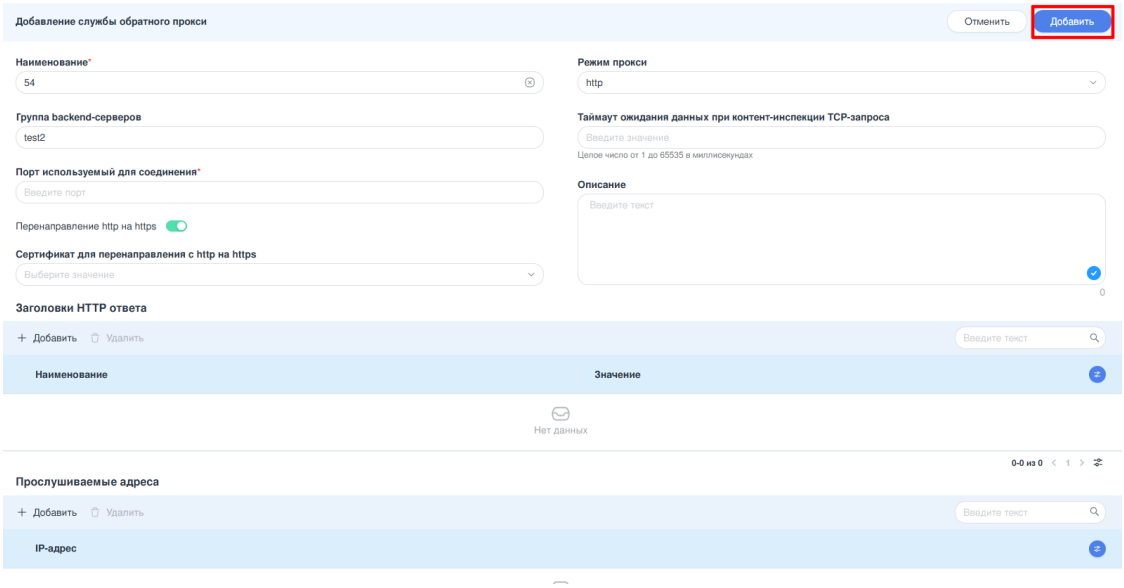


Рисунок – Сохранение конфигурации службы обратного прокси

12.2.3.1 Правило для службы

Правила служб обратного прокси используются для определения условий маршрутизации и обработки входящего трафика в рамках указанного сервиса.

Для создания правил служб необходимо выполнить следующие действия:

1. В таблице **«Службы обратного прокси»** выбрать нужную группу, нажав **ЛКМ** по соответствующей строке.
2. В открывшемся окне **«Служба <имя_группы>»** нажать **кнопку «+ Добавить»** в таблице **«Правило для службы»**.
3. В окне **«Добавление правила службы»** внести необходимые параметры:
   - **Номер правила** - уникальный идентификатор правила. Возможно указать значение в диапазоне от «1» до «10000».
   - **Шаблоны поиска совпадений в пути URL** - таблица шаблонов поиска в URL. Для добавления шаблона необходимо нажать **кнопку «+ Добавить»** и в открывшемся окне **«Добавить шаблон поиска в URL»** указать следующие обязательные параметры (см. Рисунок – Добавление шаблона поиска в URL):
     - **Режим поиска** - позволяет настроить условия правила для маршрутизации запросов на основе URL-пути. Возможно выбрать следующие значения:
       - **begin - Совпадение в начале** - запрос соответствует правилу, если URL начинается с указанного значения;

- **end - Совпадение в конце** - запрос соответствует правилу, если URL заканчивается на указанное значение;
- **exact - Полное совпадение** - запрос соответствует правилу, если URL полностью совпадает с указанным значением.

- **Содержимое шаблона поиска в URL** - значение URL-пути, используемое для сопоставления. Значение должно начинаться с символа «/». Допустимо использование букв латинского алфавита и цифр. В строке могут присутствовать следующие символы: «.», «-», «/», «-».

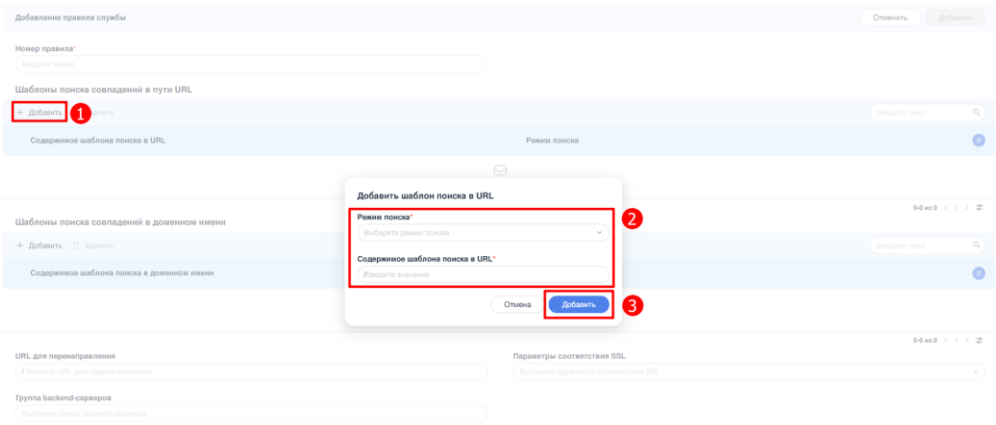


Рисунок – Добавление шаблона поиска в URL

- **Шаблоны поиска совпадения в доменном имени** - таблица шаблонов поиска в доменном имени. Для добавления шаблона необходимо нажать **кнопку «+ Добавить»**. В открывшемся окне **«Добавить шаблон поиска в доменном имени»** указать в поле **«Содержимое шаблона поиска в доменном имени»** значение доменного имени, используемое для сопоставления (см. Рисунок – Добавление шаблона поиска совпадения в доменном имени). Максимальная длина доменного имени не должна превышать 242 символов. В составе доменного имени разрешены точка и дефис, при условии, что они не находятся на первой и последней позициях. Длина каждой доменной группы не должна превышать 63 символов. Количество доменных групп, разделённых точками, не должно превышать 127.

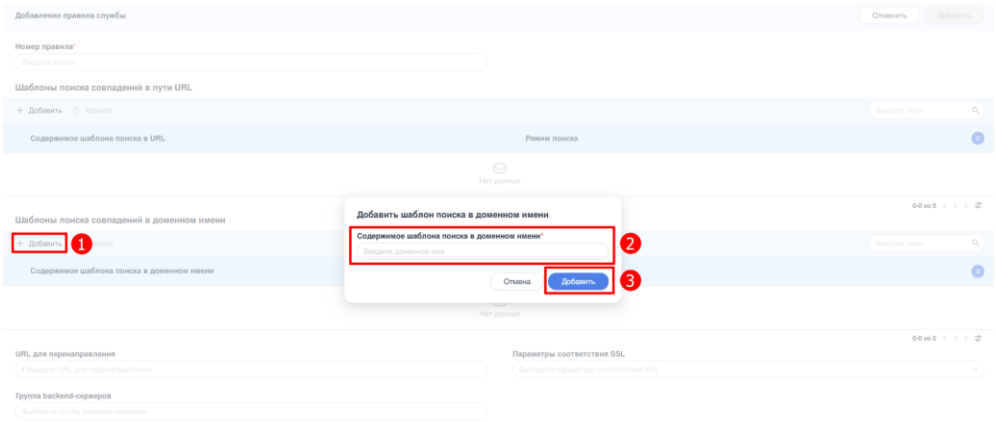


Рисунок – Добавление шаблона поиска совпадения в доменном имени

- **URL для перенаправления** - перенаправление (редирект) запросов на указанный URL. Значение должно начинаться с символа «/». Допустимо использование букв латинского алфавита и цифр. В строке могут присутствовать следующие символы: «.», «-», «/», «-». Максимальная длина значения не должна превышать 242 символов.
- **Группа backend-серверов** - выбор из списка группы backend-серверов. Определяет какая группа backend-серверов будет обрабатывать входящие запросы, поступающие на данный сервис.
- **Параметры соответствия SSL** - настроить условия правила для маршрутизации запросов на основе SSL/TLS и связанных с ним параметр Server Name Indication (SNI). SNI — это расширение протокола TLS, которое позволяет клиенту указать имя домена в начале SSL-соединения. Данная функция особенно актуальна для работы с несколькими доменами на одном IP-адресе. Возможно выбрать следующие параметры сопоставления данных:
    - **req-ssl-sni** - сопоставление SNI из запроса клиента;
    - **ssl-fc-sni** - сопоставляет значение SNI, извлечённое из фронтенд-соединения (frontend connection) SSL/TLS. Используется для проверки SNI на уровне входящего соединения;
    - **ssl-fc-sni-end** - сопоставляет значение SNI в конце фронтенд-соединения SSL/TLS. Используется в редких случаях, когда SNI проверяется в конце соединения.

4. По завершению настроек нажать **кнопку «Добавить»** (см. Рисунок – Добавление правила службы).

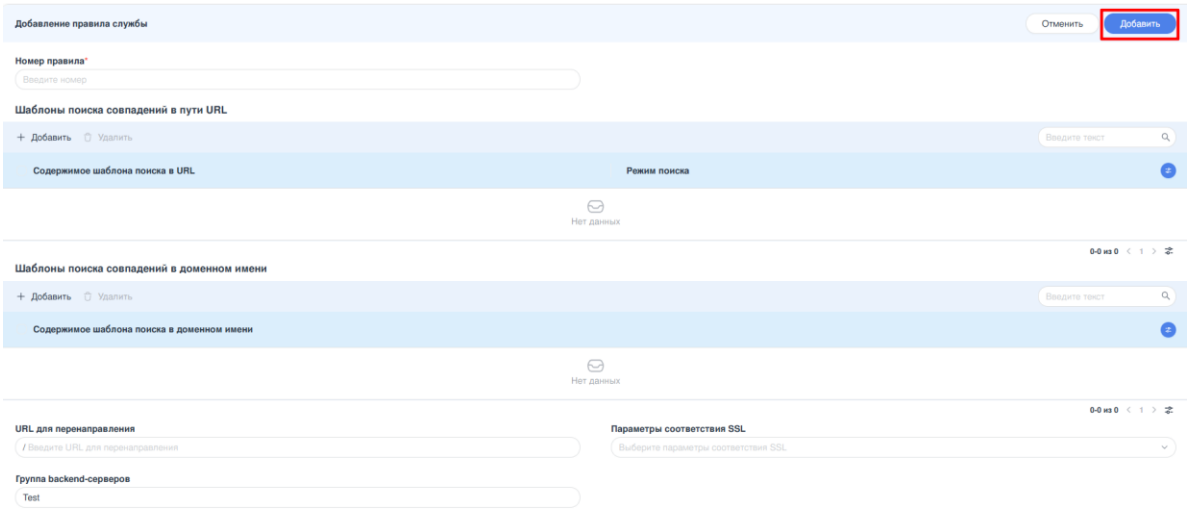


Рисунок – Добавление правила службы

12.2.4 Применение и сохранение настроек обратного прокси

Примечание:

Для применения настроек требуется минимальная рабочая конфигурация сервиса обратного прокси.

Для применения и сохранения конфигурации обратного прокси необходимо нажать **кнопку «Сохранить»** в шапке раздела **«Интерфейсы»** (см. Рисунок – Сохранение конфигурации обратного прокси).

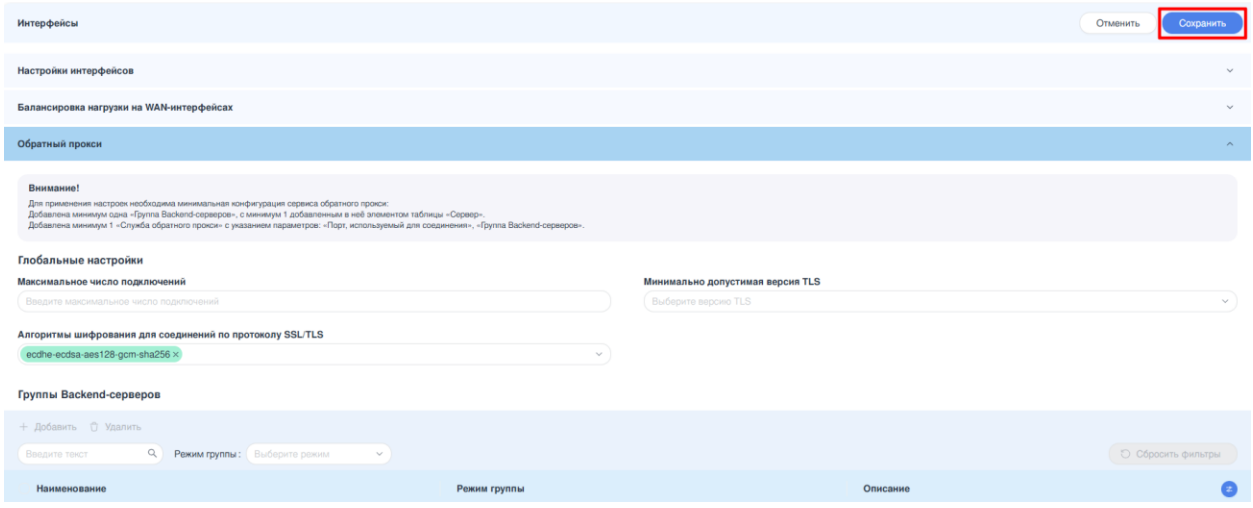


Рисунок – Сохранение конфигурации обратного прокси

В случае несоблюдения минимальных настроек прокси-сервера система выдаст предупреждение о невозможности сохранения конфигурации (см. Рисунок – Сообщение об ошибке несоблюдения минимальной конфигурации).

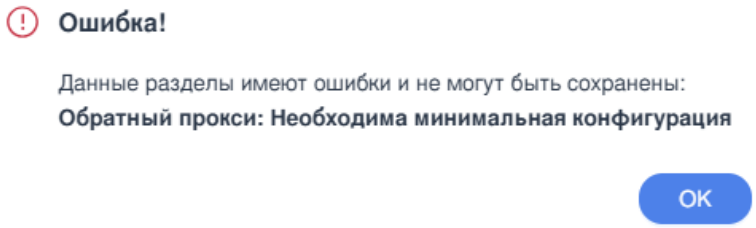


Рисунок – Сообщение об ошибке несоблюдения минимальной конфигурации

13 ОБЗОРНАЯ ПАНЕЛЬ

13.1 Трафик

Раздел **«Трафик»** предназначен для мониторинга текущей загрузки сетевых интерфейсов и отображения статистики передачи и приёма данных в системе **ARMA Стена** (см. Рисунок – Мониторинг трафика).

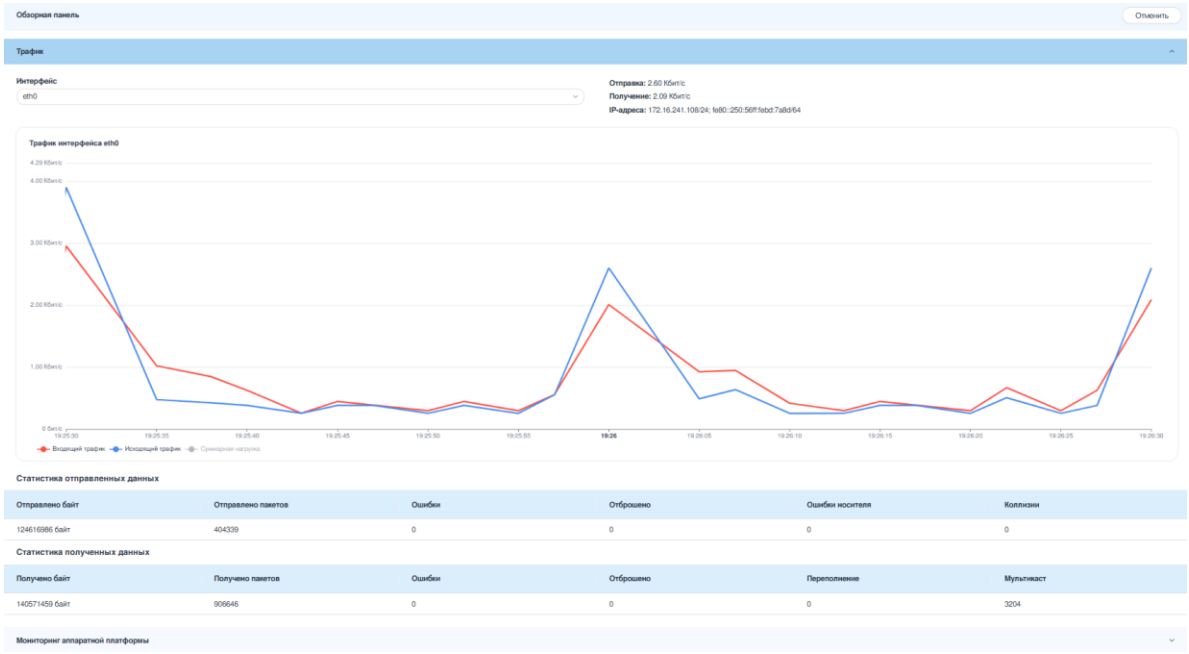


Рисунок – Мониторинг трафика

Для выбора интерфейса используется выпадающий список **«Интерфейс»**, содержащий имена всех доступных физических и виртуальных интерфейсов системы. По умолчанию интерфейс не выбран. Выбор интерфейса инициирует обновление всех компонентов раздела.

Информационный блок

Информационный блок включает набор недоступных для редактирования элементов, отображающих текущее состояние и статистику выбранного интерфейса:

- **Отправка** - текущая скорость исходящего трафика (TX) через выбранный интерфейс, измеряемая в единицах объёма данных в секунду. Значение обновляется с интервалом 2,5 секунды.
- **Получение** - текущая скорость входящего трафика (RX) через выбранный интерфейс, измеряемая в единицах объёма данных в секунду. Значение обновляется с интервалом 2,5 секунды.
- **IP-адреса** - перечень IPv4- и IPv6-адресов, назначенных выбранному интерфейсу.

График загрузки интерфейса

Отображается линейный график, отражающий динамику входящего и исходящего трафика на выбранном интерфейсе.

По **оси X** представлена временная шкала с глубиной хранения данных 60 секунд.

По **оси Y** указана скорость трафика в бит/с, кбит/с, Мбит/с или Гбит/с. Единица измерения определяется автоматически в зависимости от текущей интенсивности трафика.

График обновляется каждые 2,5 секунды и включает два временных ряда:

- входящий трафик — красная линия;
- исходящий трафик — синяя линия.

Статистика отправленных данных

Статистика исходящего трафика представлена в табличной форме со следующими полями:

- **Отправлено байт** - общий объём данных, переданных через интерфейс (в байтах);
- **Отправлено пакетов** - общее количество переданных сетевых пакетов;
- **Ошибки** - число неудачных попыток передачи из-за аппаратных или программных сбоев;
- **Отброшено** - количество пакетов, отменённых перед отправкой (например, из-за нехватки ресурсов);
- **Ошибки носителя** - сбои на физическом уровне (например, проблемы с кабелем или дуплексом);
- **Коллизии** - количество конфликтов при передаче в сетях с разделяемой средой.

Статистика полученных данных

Статистика входящего трафика представлена в табличной форме со следующими полями:

- **Получено байт** - общий объём данных, принятых через интерфейс (в байтах);
- **Получено пакетов** - общее количество принятых сетевых пакетов;
- **Ошибки** - число повреждённых или некорректно принятых пакетов;
- **Отброшено** - количество пакетов, отклонённых при приёме;
- **Переполнение** - количество пакетов, потерянных вследствие переполнения входного буфера;

- **Мультикаст** - количество принятых пакетов, адресованных группе получателей (мультикаст-трафик).

13.2 Мониторинг аппаратной платформы

В системе **ARMA Стена** возможен мониторинг текущего состояния компонентов устройства, включая систему питания и охлаждения. Это позволяет предотвратить возможные аварийные ситуации, связанные с оборудованием.

Для просмотра состояния аппаратной платформы системы необходимо в меню **«Обзорная панель»** выбрать раздел **«Мониторинг аппаратной платформы»** (см. Рисунок – Мониторинг аппаратной платформы).

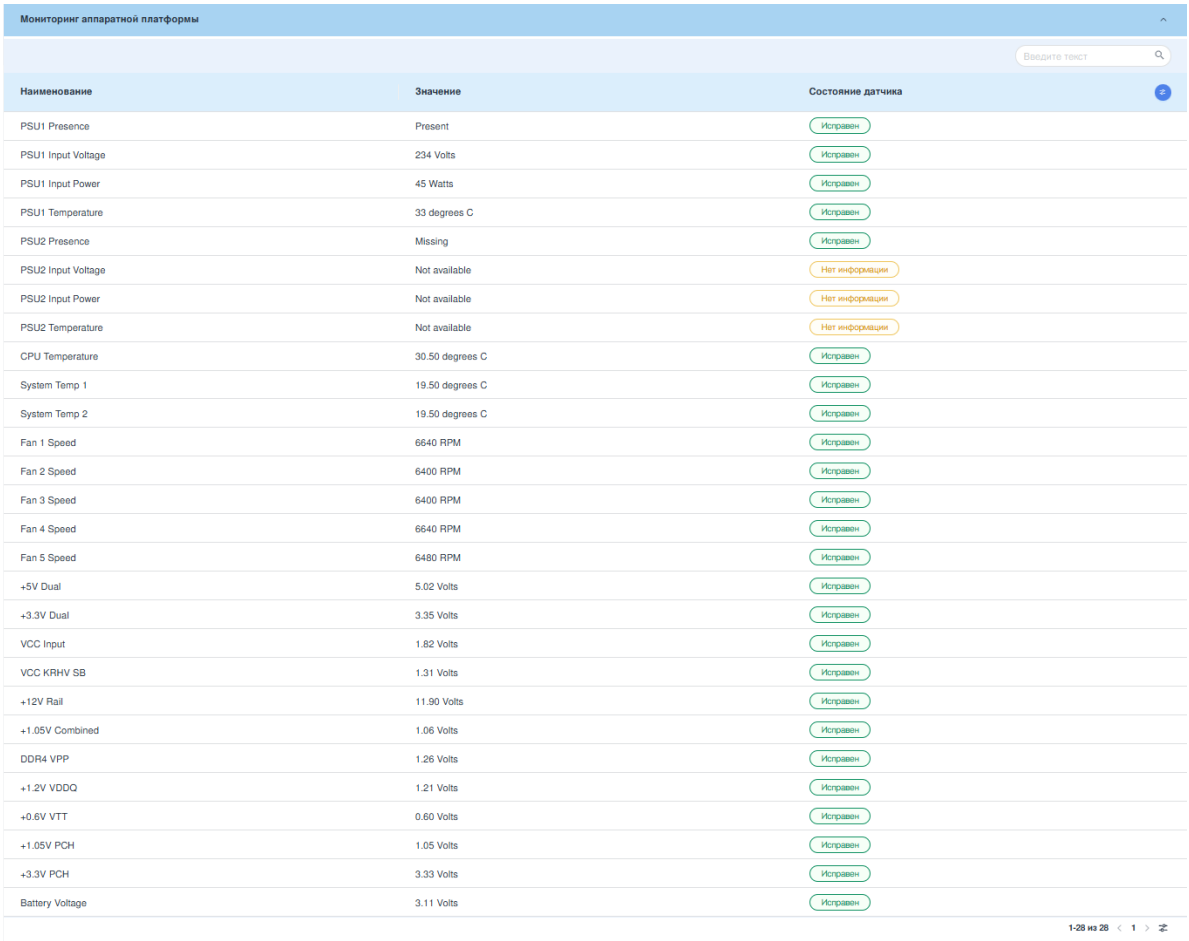


Рисунок – Мониторинг аппаратной платформы

Столбец **«Состояние датчика»** таблицы **«Мониторинг аппаратной платформы»** отображает текущее состояние датчика. Допустимые значения:

- **Исправлен** - датчик функционирует корректно и предоставляет данные;
- **Нет информации** - датчик отсутствует, не отвечает или неисправен, данные от него не поступают.

> **Примечание:**
>
> Для обеспечения мониторинга аппаратной платформы требуется активировать поддержку **BMC** в настройках **BIOS**. Если функция **BMC**

отключена, система отобразит следующее сообщение: *«Мониторинг аппаратной платформы недоступен. Проверьте настройки BIOS»*.

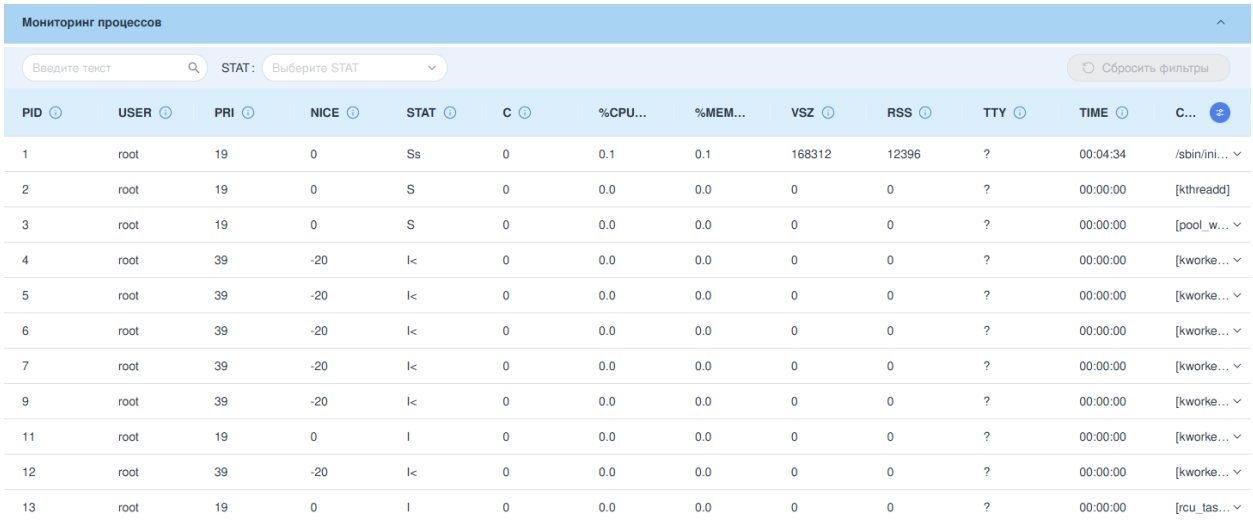
Примечание:

В случае отключения резервного блока питания (PSU) во время работы устройства, в интерфейсе мониторинга сохранятся все поля, связанные с данным блоком питания. При этом их статус будет отображён как **«Not available»**, а значение поля **«PSU<номер_БП> Presence»** изменится на **«Missing»**.

Если устройство было предварительно выключено, и только после этого был отключен блок питания, в интерфейсе останется отображаться исключительно строка **«PSU<номер_БП> Presence»** с указанием значения **«Missing»**. Все остальные параметры, относящиеся к данному блоку питания, отображаться не будут.

13.3 Мониторинг процессов

Раздел **«Мониторинг процессов»** предназначен для отображения текущего состояния системных и пользовательских процессов, активных на устройстве. Информация представлена в табличном виде и автоматически обновляется с периодичностью 5 секунд. Для доступа к разделу необходимо перейти по пути: **«Обзорная панель»** - **«Мониторинг процессов»** (см. Рисунок – Мониторинг процессов).



PID	USER	PRI	NICE	STAT	C	%CPU...	%MEM...	VSZ	RSS	TTY	TIME	C...
1	root	19	0	Ss	0	0.1	0.1	168312	12396	?	00:04:34	/sbin/ini...
2	root	19	0	S	0	0.0	0.0	0	0	?	00:00:00	[kthreadd]
3	root	19	0	S	0	0.0	0.0	0	0	?	00:00:00	[pool_w...
4	root	39	-20	I<	0	0.0	0.0	0	0	?	00:00:00	[kworke...
5	root	39	-20	I<	0	0.0	0.0	0	0	?	00:00:00	[kworke...
6	root	39	-20	I<	0	0.0	0.0	0	0	?	00:00:00	[kworke...
7	root	39	-20	I<	0	0.0	0.0	0	0	?	00:00:00	[kworke...
9	root	39	-20	I<	0	0.0	0.0	0	0	?	00:00:00	[kworke...
11	root	19	0	I	0	0.0	0.0	0	0	?	00:00:00	[kworke...
12	root	39	-20	I<	0	0.0	0.0	0	0	?	00:00:00	[kworke...
13	root	19	0	I	0	0.0	0.0	0	0	?	00:00:00	[rcu_tas...

Рисунок – Мониторинг процессов

Описание полей таблицы:

- **PID** - уникальный числовой идентификатор процесса, присваиваемый ядром операционной системы при его запуске;
- **USER** - имя пользователя, от имени которого выполняется процесс. Для системных процессов указано значение root. При наличии у текущей учётной записи прав на просмотр информации о пользователе (право

выполнения команды show permissions user <имя_УЗ>), нажатие на имя УЗ инициирует открытие окна «Права доступа <имя_УЗ>», содержащего права пользователя в веб-интерфейсе и перечень разрешённых CLI-команд;

- **PRI** - приоритет планирования процесса (значение динамического приоритета), определяемое на основе параметра NICE и внутренней логики планировщика;
- **NICE** - статический параметр корректировки приоритета процесса; допустимые значения находятся в диапазоне от «-20» до «19». Процессы с меньшим значением nice получают больше CPU-времени;
- **STAT** - состояние процесса согласно классификации ядра Linux:
    - **R** - процесс выполняется в текущий момент;
    - **S** - процесс находится в состоянии ожидания (прерываемый сон);
    - **D** - процесс заблокирован в непрерываемом режиме (например, ожидание операций ввода-вывода);
    - **Z** - завершённый процесс (zombie или defunct), не получивший сигнала от родительского процесса;
    - **T** - процесс приостановлен (остановлен сигналом);
    - **W** - процесс находится в состоянии свопа;
    - **<** - процесс имеет повышенный приоритет (запущен с приоритетом real-time);
    - **N** - процесс выполняется с пониженным приоритетом;
    - **L** - процесс имеет страницы памяти, заблокированные в RAM (обычно указывает на использование real-time планирования);
    - **I** - поток ядра в режиме бездействия (idle), не имеющий активного выполнения.
- **C** - индикатор загрузки процессора;
- **%CPU** - доля использования центрального процессора данным процессом за последний интервал измерения;
- **%MEM** - процент использования оперативной памяти относительно общего объёма RAM;
- **VSZ** - объём виртуальной памяти, занимаемой процессом (в килобайтах);
- **RSS** - объём резидентной памяти (физической памяти, используемой процессом без учёта свопа), в килобайтах;
- **TTY** - терминал, связанный с процессом. Для фоновых и системных процессов значение — «?»;

- **TIME** - суммарное время CPU, затраченное на выполнение процесса, отображается в формате ЧЧ:ММ:СС;
- **COMMAND** - имя исполняемого файла или команды, запустившей процесс. Для потоков ядра указано название в квадратных скобках (например, [kthreadd]).

14 ЛОГИРОВАНИЕ

В настоящем разделе представлено описание подраздела **«Логирование»**, предусматривающего механизм управления следующими функциями:

- настройка глобального журнала;
- экспорт логов в файл;
- экспорт логов на удалённый сервер (syslog).

Для перехода в подраздел **«Логирование»** необходимо выполнить следующие действия:

1. В списке источников открыть карточку необходимого источника **«NGFW»**.
2. В карточке источника выбрать модуль **«Системные настройки»**.
3. В разделе **«Системные настройки»** перейти в подраздел **«Логирование»** (см. Рисунок – Системные настройки).

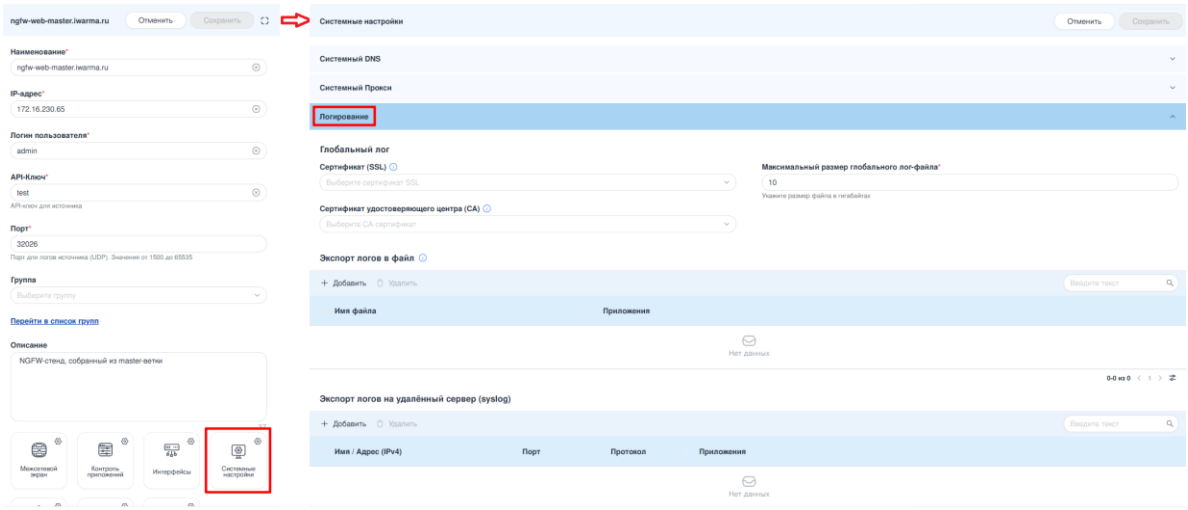


Рисунок – Системные настройки

Применение и сохранение настроек логирования

После завершения настройки всех необходимых параметров в подразделе **«Логирование»** необходимо сохранить внесённые изменения. Для этого следует нажать **кнопку «Сохранить»**, расположенную в правом верхнем углу заголовка раздела **«Системные настройки»**.

После нажатия кнопки откроется окно подтверждения **«Сохранить изменения конфигурации»**, в котором отображается список подразделов, затронутых внесёнными изменениями. Для продолжения и применения настроек необходимо подтвердить действие, нажав **кнопку «Сохранить»** в данном окне (см. Рисунок – Применение и сохранение настроек).

Только после успешного подтверждения все изменения будут сохранены и активированы в текущей конфигурации системы **ARMA Стена**.

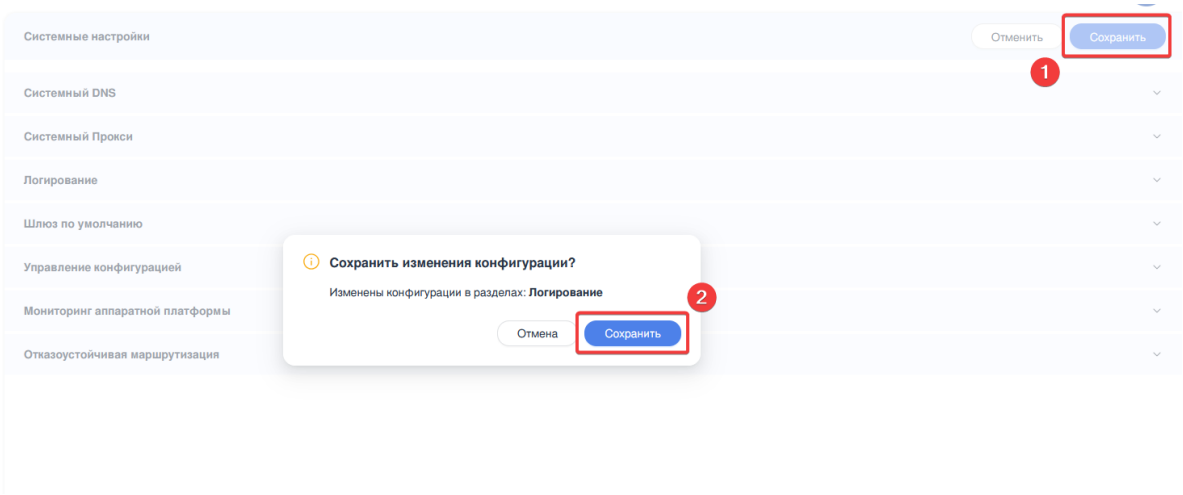


Рисунок – Применение и сохранение настроек

При необходимости отменить все неприменённые настройки следует нажать **кнопку «Отмена»**, расположенную в верхнем правом углу заголовка раздела **«Системные настройки»**. В этом случае конфигурация подраздела **«Логирование»** будет откатана к последнему сохранённому состоянию.

14.1 Настройки глобального журнала

В блоке **«Глобальный лог»** представлены параметры конфигурации глобального журнала (см. Рисунок – Настройки глобального журнала):

- **Максимальный размер глобального лог-файла** - задаёт максимальный объём дискового пространства, выделяемого для хранения всех лог-файлов в локальном хранилище, в гигабайтах. Возможно указать значение в диапазоне от «1» до «100». По умолчанию используется значение «10» Гб.
- **Сертификат (SSL)** - позволяет выбрать клиентский SSL-сертификат из числа установленных в системе **ARMA Стена**, который будет использоваться для шифрования трафика при удалённой передаче логов по протоколу TLS.
- **Сертификат удостоверяющего центра (CA)** - предоставляет возможность выбора CA-сертификата из числа установленных в системе **ARMA Стена**, который применяется для проверки подлинности сервера, принимающего логи по защищённому SSL-соединению.

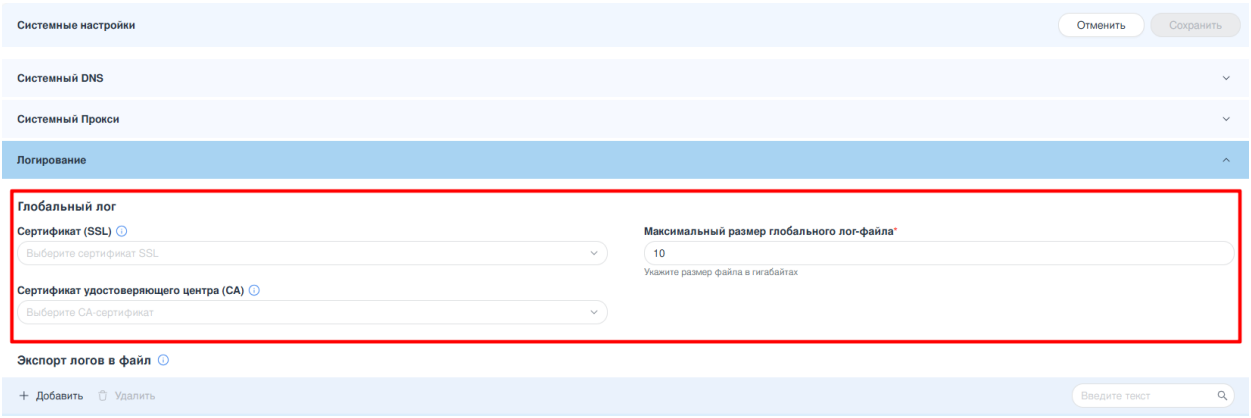


Рисунок – Настройки глобального журнала

14.2 Экспорт логов в файл

Для настройки экспорта логов в файл необходимо выполнить следующую последовательность действий:

1. Нажать **кнопку «+ Добавить»** в таблице **«Экспорт логов в файл»** (см. Рисунок – Экспорт логов в файл).
2. В появившейся боковой панели **«Добавление файла экспорта логов»** указать имя файла. Имя файла должно соответствовать следующим требованиям:
   - максимальная длина — 247 символов;
   - допустимые символы: латинские буквы, цифры, а также символы «-», «.», «_»;
   - имя не может начинаться с символов «-» или «.».
3. В блоке **«Логируемые приложения»** выбрать одно или несколько приложений, события которых подлежат экспорту в указанный файл. Выбор приложения осуществляется из выпадающего списка **«Приложение»**. После выбора приложения становятся доступны дополнительные поля конфигурации, позволяющие задать параметры фильтрации событий (например, по типу события, уровню логирования и другим атрибутам). Это обеспечивает возможность тонкой настройки состава экспортируемых данных. Для добавления дополнительного приложения требуется повторно нажать **кнопку «+ Добавить»**. Перечень поддерживаемых приложений приведён в таблице «Экспортируемые приложения». Если уровень логирования для выбранного приложения не задан явно, в файл будут записываться все события данного приложения в соответствии с текущими системными настройками уровня логирования.

Таблица «Экспортируемые приложения»

Приложение	Уровень логирования по умолчанию
arma-endpoint	informational

Приложение	Уровень логирования по умолчанию
conntrack	informational
conntrack-sync	informational
console-server	informational
dhcp: client	informational
dhcp: server	informational
dhcpv6: client	informational
dhcpv6: server	informational
dns: dynamic	informational
dns: forwarding	informational
drweb: config	notice
drweb: http	notice
drweb: icapd	notice
drweb: netcheck	notice
drweb: scan-engine	notice
drweb: update	notice
drweb: url-check	notice
firewall	-
http-api	informational
https	notice
idps: engine	notice
idps: rules	notice
idps: server	notice
idps: update-rules	notice
ipoe-server	informational
kernel	-
lldp	informational
login	informational
nat	-
ntp	informational
pppoe	debug

Приложение	Уровень логирования по умолчанию
pppoe-server	informational
snmp	warning
ssh	debug
systemd	informational
users	-
vpn: ipsec	informational
vpn: l2tp	informational
vpn: openconnect	informational
vpn: openvpn	informational
vpn: pptp	informational
vpn: sstp	informational
vpn: wireguard	informational
vrrp	informational
webproxy	informational

4. Настроить ротацию файлов установив следующие параметры:
   - **Максимальный размер файла** - указать максимальный размер файла в мегабайтах. Возможно указать значение в диапазоне от «1» до «1024». По умолчанию значение установлено на 5 мегабайт.
   - **Количество сохраняемых файлов** - указать максимальное количество файлов. Возможно указать значение в диапазоне от «1» до «100». По умолчанию значение равно «5».

   При достижении указанного максимального размера текущего файла создаётся новый файл для записи. При превышении заданного количества файлов ротация продолжается с перезаписью наиболее старых файлов.
5. По завершению настроек нажать **кнопку «Сохранить»**.

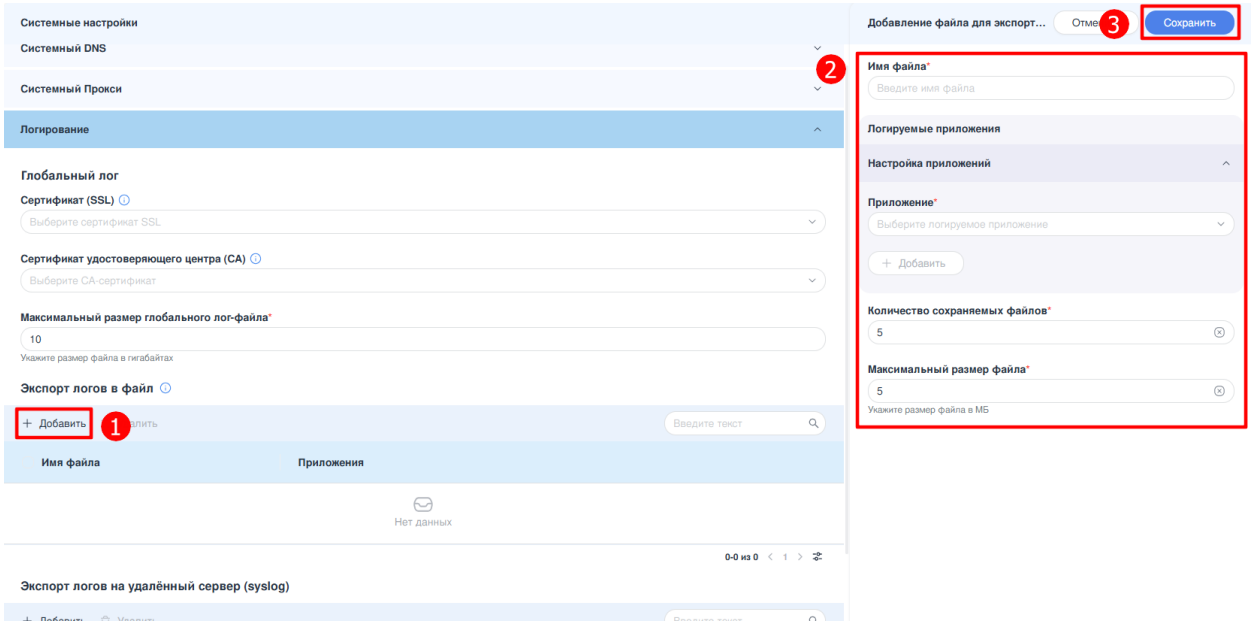


Рисунок – Экспорт логов в файл

Примечание:

Log-файлы сохраняются в каталоге **/var/log/user/**.

Примечание:

Возможно создать не более 64 файлов логирования.

Для редактирования настроек необходимо нажать **ЛКМ** на нужном файле в разделе **«Экспорт логов в файл»** и в открывшейся боковой панели внести изменения. По завершению изменений нажать **кнопку «Сохранить»**.

Для удаления настроек необходимо выбрать один или несколько файлов, установив флажок в чек-боксе слева от имени файла, и нажать **кнопку «Удалить»**. В открывшемся диалоговом окне подтвердить удаление нажатием **кнопки «Удалить»** (см. Рисунок – Подтверждение удаление файла).

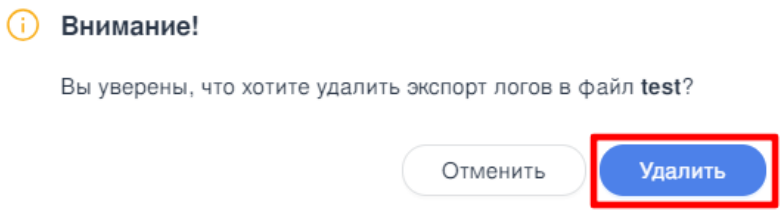


Рисунок – Подтверждение удаление файла

Поддерживается сквозной поиск по всем полям таблицы **«Экспорт логов в файл»**. Для выполнения поиска необходимо ввести искомое значение в поле **«Поиск»**. Поиск осуществляется по содержимому всех столбцов таблицы.

14.3 Экспорт логов на удалённый сервер (syslog)

Система **ARMA Стена** предоставляет возможность настройки передачи выбранных журналов событий на удалённый сервер регистрации с использованием протокола Syslog.

Для настройки экспорта логов необходимо выполнить следующие действия:

1. В таблице **«Экспорт логов на удалённый сервер (syslog)»** нажмите **кнопку «+ Добавить»**.
2. В открывшемся окне необходимо указать параметры подключения к серверу и настроить фильтрацию экспортируемых событий (см. Рисунок – Добавление удалённого сервера для экспорта логов):

- **«Имя / Адрес (IPv4) сервера»** - идентификатор удалённого сервера. Указывается в виде IPv4-адреса в формате «x.x.x.x» или имени хоста. Максимальная длина строки — 63 символа. Имя хоста должно содержать только латинские буквы, цифры, а также символы точка «.» и дефис «-». Не допускается начинать имя с символов «-» и «.».
- **«Порт»** - номер TCP/UDP-порта, используемого сервером для приёма сообщений. Возможно указать значение в диапазоне от **«1»** до **«65535»**. По умолчанию используется значение **«514»**.
- **«Протокол»** - тип транспортного протокола для передачи данных. Возможно указать значение: **«UDP»** или **«TCP»**. По умолчанию используется протокол **«TCP»**.
- **«Использовать шифрование TLS»** - флаг, определяющий необходимость использования защищённого канала передачи данных.
- **«Формат сообщений журнала (syslog)»** - формат представления логируемых записей. Поддерживаются значения: **«RFC 3164»**, **«CEF»**.
- **«Режим аутентификации»** - способ проверки подлинности клиента. Поддерживаемые режимы: **«Анонимная»** — без проверки подлинности, **«По сертификату x509-name»** — с использованием клиентского X.509 сертификата.
- **«Логируемые приложения»** - блок, предназначенный для выбора приложений, события которых будут передаваться на удалённый сервер. Для добавления приложения необходимо выбрать нужное значение из выпадающего списка **«Приложение»**. После выбора приложения становятся доступны дополнительные поля, позволяющие задать параметры фильтрации событий данного приложения. Это позволяет настроить более узкий диапазон экспортируемых событий (например, по типу события, уровню серьёзности и другим характеристикам). При необходимости добавить ещё одно приложение требуется нажать **кнопку «+ Добавить»**. Список доступных приложений представлен в таблице «Экспортируемые приложения».

3. По завершению нажать **кнопку «Сохранить»**.

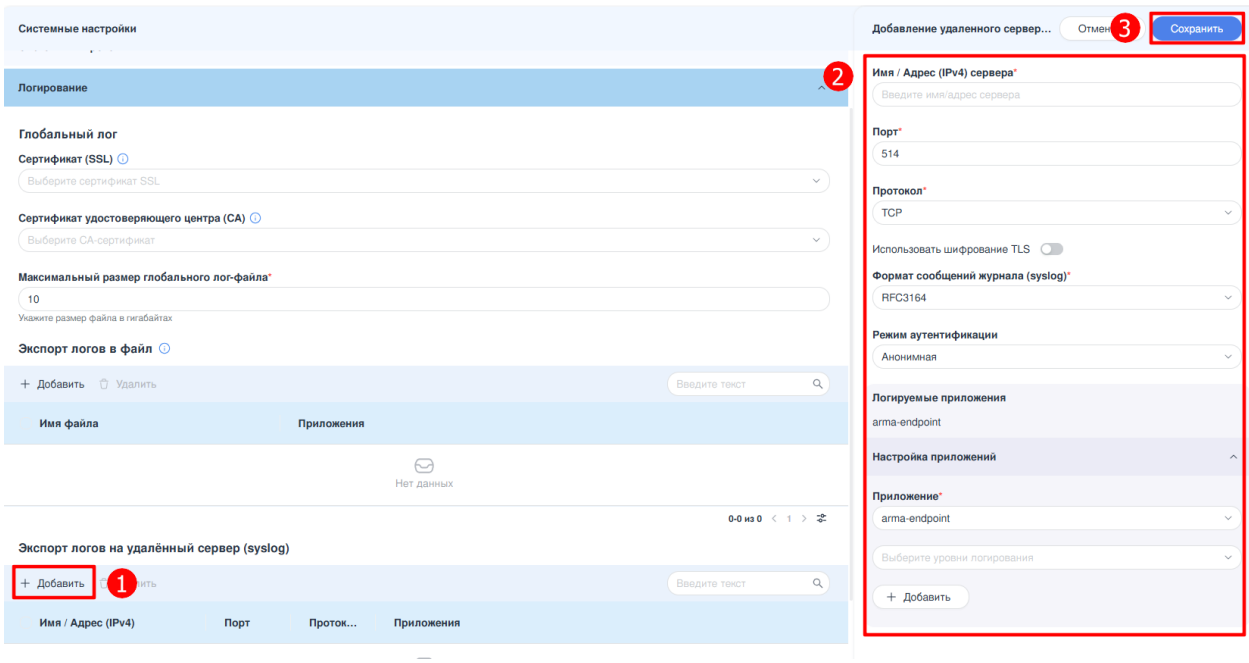


Рисунок – Добавление удалённого сервера для экспорта логов

Для редактирования настроек необходимо нажать **ЛКМ** на нужном сервере в разделе **«Экспорт логов на удалённый сервер (syslog)»** и в открывшейся боковой панели внести изменения. По завершению изменений нажать **кнопку «Сохранить»**.

Для удаления настроек необходимо выбрать один или несколько серверов, установив флажок в чек-боксе слева от имени сервера, и нажать **кнопку «Удалить»**. В открывшемся диалоговом окне подтвердить удаление нажатием **кнопки «Удалить»**.

Сквозной поиск по полям таблицы **«Экспорт логов на удалённый сервер (syslog)»** осуществляется с помощью ввода искомого значения в поле параметра **«Поиск»**. Поиск осуществляется по столбцам **«Имя / Адрес (IPv4)»** и **«Приложения»**.