Руководство пользователя по эксплуатации

версия 76 ред. от 27.11.2024

Листов 485

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
АС	Автономные системы
АСУ ТП	Автоматизированная система управления технологическим процессом
ДСЧ	Датчик случайных чисел
ИБ	Информационная безопасность
ЛКМ	Левая кнопка мыши
МП	Материнская плата
МЭ	Межсетевой экран
ПК	Персональный компьютер
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
СПВ	Система предотвращения вторжений
УЗ	Учётная запись
ЦП	Центральный процессор
ЧПУ	Числовое программное управление
ABR	Area Border Router, пограничный маршрутизатор области – роутер, соединяющий одну или несколько OSPF-областей с магистральной зоной
ADS	Automation Device Specification – протокол взаимодействия устройств между собой, не зависящий от оборудования, с помощью которого эти устройства передают информацию
API	Application Programming Interface – программный интерфейс приложения
ARMA FW	InfoWatch ARMA Firewall
ARMA MC	InfoWatch ARMA Management Console

Термины и сокращения	Значение
ARP	Address Resolution protocol, протокол определения адреса – протокол, предназначенный для определения MAC-адреса другого компьютера по известному IP-адресу
AS	Autonomous system – Автономные системы
ASBR	Autonomus System Boundary Router, пограничный маршрутизатор автономной системы – обменивается информацией с роутерами, принадлежащим другим автономным системам
Blacklists UT1	Список ограничения доступа к URL-адресам
BGP	Border Gateway Protocol – протокол граничного шлюза
CA	Certification authority – центр сертификации
CARP	Common Address Redundancy Protocol – протокол дупликации общего адреса
CDP	Cisco Discovery Protocol, Протокол обнаружения Cisco – проприетарный протокол второго уровня, разработанный компанией Cisco Systems, позволяющий обнаруживать подключённое сетевое оборудование Cisco, его название, версию ПО и IP-адреса
CEF	Common Event Format – открытый формат журнала событий
CIDR	Classless Inter-Domain Routing – бесклассовая междоменная маршрутизация
CIP	Common Industrial Protocol, Общий промышленный протокол – протокол для приложений промышленной автоматизации
DCERPC	Distributed Computing Environment/Remote Procedure Calls, распределённая вычислительная среда/удалённые вызовы процедур – система удалённого вызова процедур, разработанная для Distributed Computing Environment
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла

Термины и сокращения	Значение
DNP3	Distributed Network Protocol – протокол передачи данных, используемый для связи между компонентами АСУ ТП
DNS	Domain Name System, система доменных имён – компьютерная распределённая система для получения информации о доменах
Dr.Web	Доктор Веб – общее название семейства антивирусного ПО для различных платформ, разрабатываемое компанией «Доктор Веб»
DUID	Уникальный идентификатор DHCP
EDP	Extreme Discovery Protocol, Протокол обнаружения Extreme – протокол, используемый для сбора информации о соседних устройствах Extreme Networks
ENIP	EtherNet/Industrial Protocol – промышленный сетевой протокол, разработанный для адаптации протокола CIP под сеть Ethernet
EtherCAT	Ethernet for Control Automation Technology – высокопроизводительный промышленный протокол связи на основе Ethernet, используемый для управления в режиме реального времени
FDP	Foundry Discovery Protocol, Протокол обнаружения Foundry – протокол, используемый для сбора информации о соседних устройствах Brocade
FOCAS	Factory Automation Computer Aided Engineering Support – протокол для обмена данными со станками с ЧПУ производства компании Fanuc
FQDN	Fully Qualified Domain Name, полностью определённое имя домена – имя домена, не имеющее неоднозначностей в определении
FRR	Free Range Routing – свободное ПО, разработанное с целью реализации сетевой маршрутизации на Unix-подобных системах
FTP	File Transfer Protocol – протокол передачи файлов по сети
GOOSE	Generic Object Oriented Substation Event – протокол передачи данных о событиях на подстанции

Термины и сокращения	Значение
GRE	Generic Routing Encapsulation, общая инкапсуляция маршрутов – протокол туннелирования, предназначенный для инкапсуляции пакетов сетевого уровня в IP-пакеты
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
ICAP	Internet Content Adaptation Protocol – протокол адаптации интернет-контента
ICMP	Internet Control Message Protocol, протокол межсетевых управляющих сообщений – сетевой протокол, входящий в стек протоколов TCP/IP
ID	Идентификатор
IEC 60870-5-104	Стандарт, определяющий набор протоколов для контроля и управления с использованием постоянного соединения
IGMP	Internet Group Management Protocol – протокол управления групповой передачей данных в сетях, основанных на протоколе IP
IMAP	Internet Message Access Protocol – протокол прикладного уровня для доступа к электронной почте
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP
IPS	Intrusion Prevention System, система предотвращения вторжений – система сетевой безопасности, предназначенная для обнаружения несанкционированных действий и атак, а также автоматизированного противодействия им
IPsec	IP Security – набор протоколов для обеспечения защиты данных
LAGG	Link aggregation interface – интерфейс агрегированного канала

Термины и сокращения	Значение
LAN	Local Area Network – локальная вычислительная сеть
LDAP	Lightweight Directory Access Protocol – легковесный протокол доступа к каталогам
LLDP	Link Layer Discovery Protocol, Протокол обнаружения канального уровня – протокол, позволяющий сетевому оборудованию, работающему в локальной сети, обмениваться информацией о своём существовании и своих характеристиках
LSA	Link State Advertisement – объявление о состоянии канала или маршрутизатора
MIB	Management Information Base, база управляющей информации – виртуальная база данных, используемая для управления объектами в сети связи
MMS	Протокол передачи данных реального времени и команд диспетчерского управления между сетевыми устройствами и/или программными приложениями
Modbus TCP	Открытый коммуникационный протокол, основанный на архитектуре ведущий – ведомый, используемый для передачи данных через сети TCP/IP
MS Active Directory	Служба каталогов корпорации Microsoft для операционных систем семейства Windows Server
NAT	Network Address Translation, преобразование сетевых адресов – механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов
NDP	Nortel Discovery Protocol, Протокол обнаружения Nortel – протокол канального уровня, используемый для обнаружения сетевых устройств Nortel, а также некоторых продуктов Avaya и Ciena
NetBIOS	Network Basic Input/Output System – протокол для работы в локальных сетях на персональных ЭВМ типа IBM/PC, разработан в виде интерфейса, который не зависит от фирмы-производителя
Netflow	Сетевой протокол, предназначенный для учёта сетевого трафика
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов

Термины и сокращения	Значение
	компьютера с использованием сетей с переменной латентностью
OID	Идентификатор объектов MIB
OPC	Open Platform Communications – семейство программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами
OPC DA	Open Platform Communications Data Access – стандарт OPC
OPC UA	Open Platform Communications Unified Architecture – стандарт OPC
OpenSSL	Криптографическая библиотека с открытым исходным кодом
OSPF	Open Shortest Path First – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры
PAC	Proxy Auto Configuration, автоматическая настройка прокси-сервера
POP3	Post Office Protocol Version 3, протокол почтового отделения, версия 3 – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению
Proxy ARP	Техника, с помощью которой маршрутизатор в данной сети отвечает на запросы протокола ARP для IP-адреса, который не находится в этой сети
RFC	Request for Comments, рабочее предложение – документ из серии пронумерованных информационных документов Интернета
RIP	Routing Information Protocol – протокол маршрутной информации
RRD	Round-robin Database, циклическая база данных – база данных, объём хранимых данных которой не меняется со временем, поскольку количество записей постоянно, в

Термины и сокращения	Значение
	процессе сохранения данных они используются циклически
RSPAN	Remote Switched Port Analyzer – дублирование пакетов порта удалённого коммутатора на порту другого коммутатора
S7comm	Протокол, предназначенный для обмена данными с контроллерами Siemens S7 и любым другим оборудованием, поддерживающим данный протокол
S7comm Plus	Протокол, предназначенный для обмена данными с оборудованием серий Siemens SIMATIC S7-1200 и S7-1500 и любым другим оборудованием, поддерживающим данный протокол
SDB	Подлежащие загрузке блоки
SMB	Server Message Block – сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDPB
SONMP	SynOptics Network Management Protocol, Протокол управления сетью SynOptics. Протокол был переименован в Nortel Discovery Protocol
SPAN	Switched Port Analyzer, анализатор коммутируемых портов – дублирование пакетов одного порта сетевого коммутатора на другом порту
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	Secure Sockets Layer, уровень защищённых сокетов – криптографический протокол
SSO	Single Sign-On – технология единого входа

Термины и сокращения	Значение
TCP	Transmission Control Protocol, протокол управления передачей – один из основных протоколов передачи данных интернета
TFTP	Trivial File Transfer Protocol, простой протокол передачи файлов – используется главным образом для первоначальной загрузки бездисковых рабочих станций
TLS	Transport layer security – протокол защиты транспортного уровня
Tshark	Анализатор сетевого трафика
TUN/TAP	Виртуальные сетевые драйверы ядра системы
UDP	User Datagram Protocol, протокол пользовательских датаграмм – один из ключевых элементов набора сетевых протоколов для Интернета
UMAS	Собственный протокол Schneider Electric, который может интерпретироваться только процессором и некоторыми коммуникационными модулями
URL	Uniform Resource Locator, Унифицированный указатель ресурса – система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса
UUID	Universally unique identifier, универсальный уникальный идентификатор – стандарт идентификации, используемый в создании ПО
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
VOIP	Voice over Internet Protocol – телефонная связь по протоколу IP
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети
VXLAN	Virtual Extensible Local Area Network – технология сетевой виртуализации, созданной для решения проблем масштабируемости
WAN	Wide Area Network – глобальная вычислительная сеть

Термины и сокращения	Значение
WPAD	Web Proxy Autodiscovery Protocol – протокол автоматической настройки прокси

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

Таблица «Смежные документы»

Сокращённое наименование	Полное наименование
Руководство администратора ARMA FW	Руководство администратора InfoWatch ARMA Firewall
Руководство пользователя ARMA MC	Руководство пользователя по эксплуатации InfoWatch ARMA Management Console

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Firewall v.3.13**.

Руководство пользователя по эксплуатации описывает принципы работы с **ARMA FW**, доступные функции, их подробное описание, настройку и использование.

Пользователю **ARMA FW** необходимо изучить настоящее руководство перед эксплуатацией.

1 МЕЖСЕТЕВОЙ ЭКРАН

Одной из основных функций **ARMA FW** является фильтрация трафика с помощью встроенного межсетевого экрана.

На рисунке (см. Рисунок – Пример использования МЭ) представлен стенд, в рамках которого будут создаваться правила МЭ. Необходимо получить доступ с ПК **«Admin»** к веб-серверу **«WebServer»** по протоколам HTTP и HTTPS.

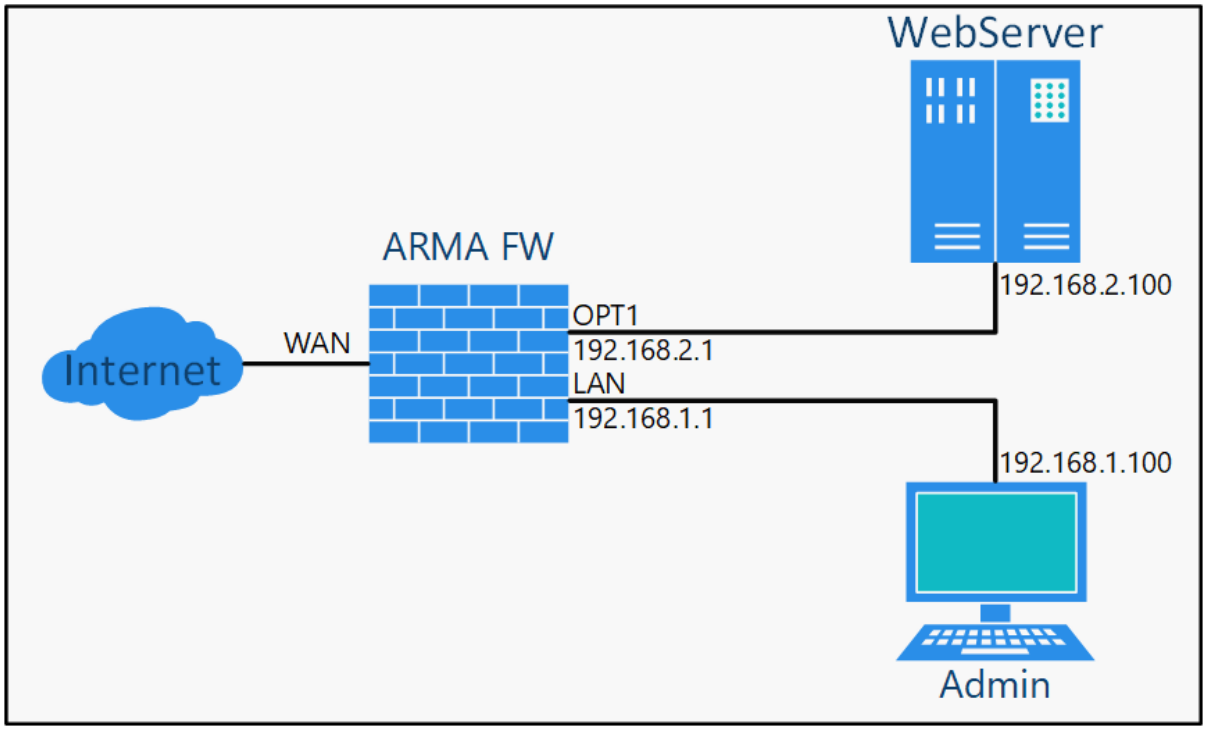


Рисунок – Пример использования МЭ

Для получения доступа необходимо выполнить следующие шаги:

1. Убедиться в отсутствии доступа с ПК **«Admin»** к веб-серверу **«WebServer»**.
2. Понять общую последовательность работы правил МЭ (см. Настройка правил МЭ).
3. Создать правила МЭ для каждого из указанных протоколов (см. Создание правил межсетевого экранирования).
4. Убедиться в наличии доступа с ПК **«Admin»** к веб-серверу **«WebServer»** (см. Проверка созданных правил МЭ).

Для проверки доступа необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «192.168.2.100» и нажать **клавишу «Enter»**. В результате откроется страница, указывающая на отсутствие доступа к веб-серверу (см. Рисунок – Недоступность веб-сервера).

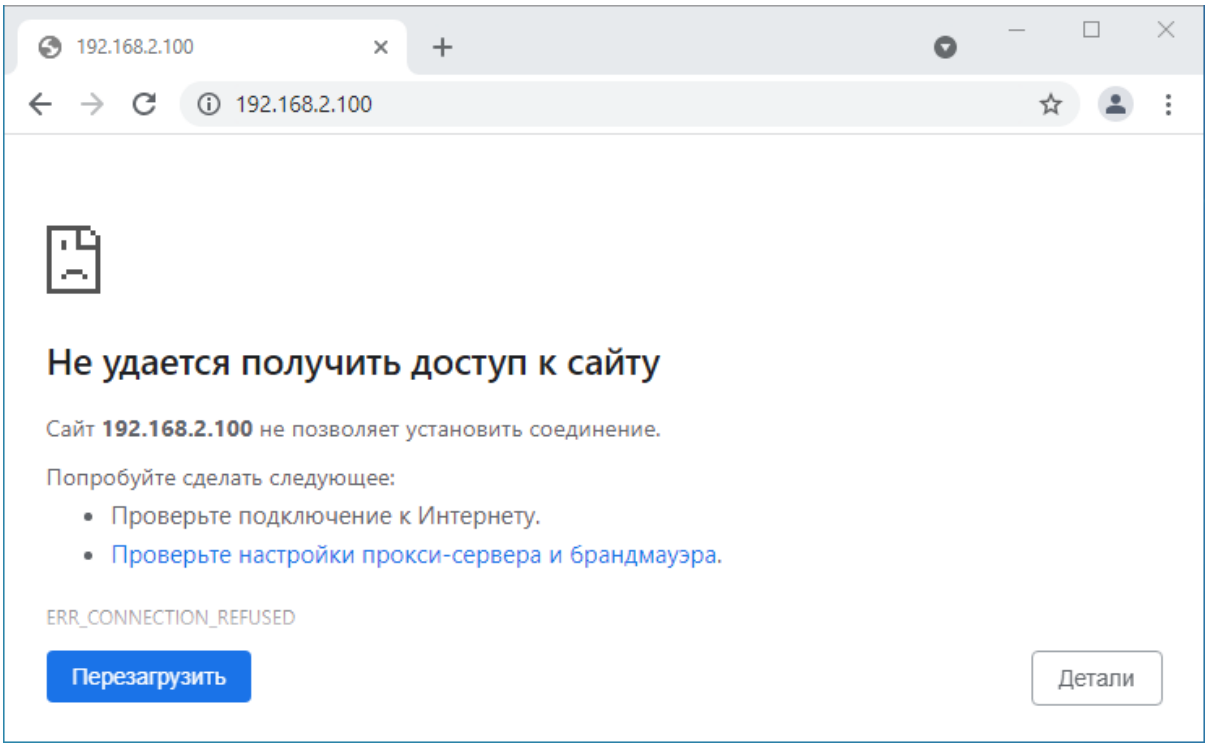


Рисунок – Недоступность веб-сервера

1.1 Настройка правил МЭ

Перед созданием правил МЭ важно понимать алгоритм их работы.

Правила МЭ задаются отдельно для каждого сетевого интерфейса и располагаются в виде списка (см. Рисунок – Список правил). По умолчанию предусмотрены автоматически сгенерированные правила. Для их просмотра необходимо нажать **кнопку** «14» в верхней правой части страницы. Перечень сгенерированных правил представлен в списке (см. Перечень автоматически сгенерированных правил).

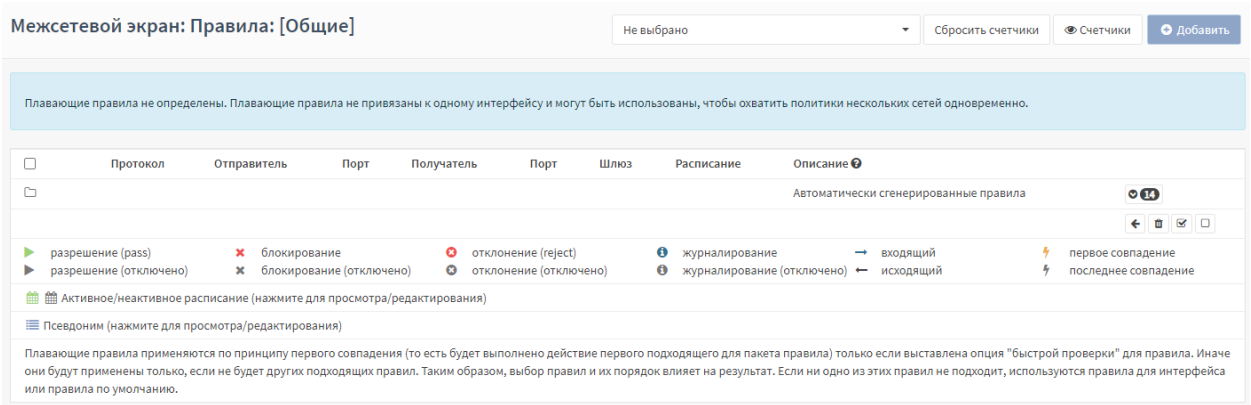


Рисунок – Список правил

Порядок правил в списке имеет значение и им можно управлять с помощью **кнопки** « » напротив каждого из созданных правил. Сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз.

Возможны два принципа совпадения:

- **первого совпадения** – сразу происходит действие, указанное в первом совпавшем правиле, далее обработка сетевого пакета не производится;
- **последнего совпадения** – производится действие, указанное в последнем совпавшем правиле, далее обработка сетевого пакета не производится.

Принципы совпадения задаются в параметре правила **«Быстрая проверка»** (см. Рисунок – Включение принципа первого совпадения) и отмечаются иконкой молнии в списке правил (см. Рисунок – Список правил):

- **жёлтая молния** « » – принцип первого совпадения;
- **серая молния** « » – принцип последнего совпадения.

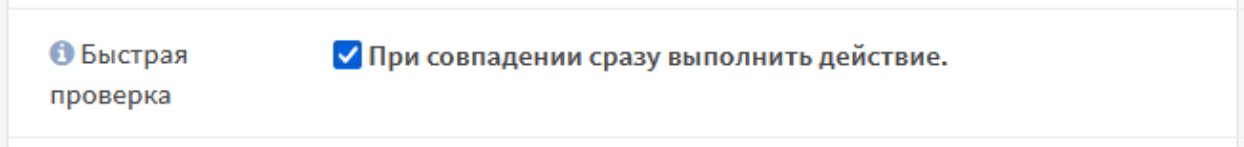


Рисунок – Включение принципа первого совпадения

Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется.

Для интерфейсов правила проверяются в порядке, представленном на рисунке (см. Рисунок – Порядок применения правил для интерфейсов).

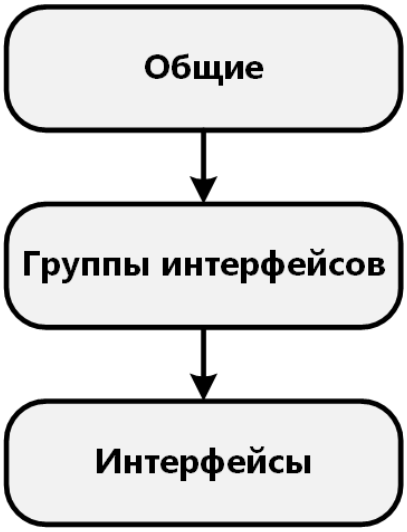


Рисунок – Порядок применения правил для интерфейсов

По умолчанию во всех создаваемых правилах параметр **«Направление»** содержит значение **«Вх.»** – «Входящий трафик». Следует понимать, что это значение для интерфейса, первоначально принимающего трафик. Применение правил МЭ для исходящего трафика используется редко и для специфических целей.

В правиле возможны три действия над пакетом трафика:

- разрешить, **«Pass»** – разрешить движение пакета;
- блокировать, **«Drop»** – отбросить пакет;
- отклонить, **«Reject»** – отбросить пакет и отправить уведомление отправителю.

При выборе в поле параметра **«Действие»** значения **«Блокирование (Drop)»** или **«Отклонить (Reject)»** дополнительно появится параметр **«Сбрасывать установленные состояния»**.

В случае установки флажка для параметра **«Сбрасывать установленные состояния»** созданное правило будет срабатывать даже в условиях непрерывного трафика. При этом произойдёт сброс всех записей в таблице состояний, относящихся к хосту, с которого был отправлен запрещённый пакет.

Перечень автоматически сгенерированных правил МЭ. Раздел [Общие]:

- 1 – **«Default deny rule»** – Правило отбрасывает трафик, если для него не сработало ни одно из разрешающих правил. Правило работает по принципу «последнее совпадение». То есть, если правила №13 и №14, находящиеся ниже в таблице и тоже работают по принципу «последнее совпадение», или любое из «мгновенно применяемых правил» сработают, то такой трафик не будет отброшен. Во всех остальных случаях будет использовано это правило;
- 2, 3, 4, 5, 6 – **«IPv6 requirements (ICMP)»** – Правила разрешают отправлять трафик по протоколу IPv6-ICMP с **ARMA FW** в локальную сеть «fe80::/10» и для групповой рассылки на адрес «ff02::/16» (правило №3) и в обратном направлении (все кроме, правила №3);
- 7 – **«Block all targetting from port 0»** – Правило блокирует все соединения с портом отправителя 0;
- 8 – **«Block all targetting to port 0»** – Правило блокирует все соединения с портом получателя 0;
- 9 – **«Allow CARP connection»** – Правило разрешает весь трафик CARP в двух направлениях. Правило не сработает, если CARP на устройстве выключен, так как сработает правило №9;
- 10 – **«sshlockout»** – Правила блокируют списки адресов/сетей из псевдонимов: «sshlockout», «webConfiguratorlockout», «virusprot». Для срабатывания необходимо в разделе псевдонимов создать соответствующий псевдоним, например, «virusprot» и заполнить поля таблицы в pfTabl (**«Межсетевой экран» - «Диагностика» - «pfTables»**);

- 11 – **«WebConfiguratorlockout»** – Правила блокируют списки адресов/сетей из псевдонимов: «sshlockout», «webConfiguratorlockout», «virusprot». Для срабатывания необходимо в разделе псевдонимов создать соответствующий псевдоним, например, «virusprot» и заполнить поля таблицы в pfTabl (**«Межсетевой экран» - «Диагностика» - «pfTables»**);
- 12 – **«virusprot overload table** – Правила блокируют списки адресов/сетей из псевдонимов: «sshlockout», vwebConfiguratorlockout», «virusprot». Для срабатывания необходимо в разделе псевдонимов создать соответствующий псевдоним, например, «virusprot» и заполнить поля таблицы в pfTabl (**«Межсетевой экран» - «Диагностика» - «pfTables»**);
- 13 – **«Let out anything from firewall host itself»** – Правило разрешает исходящий с **ARMA FW** трафик;
- 14 – **«Let out anything from firewall host itself (force gw)»** – Правило разрешает исходящий с **ARMA FW** трафик (принудительно для WAN-шлюза).

Автоматически сгенерированное правило МЭ. Раздел [LAN]:

- 1 – **«Anti-lockout rule»** – Правило разрешает доступ к **ARMA FW** по HTTP(S) и SSH соединению.

Перечень автоматически сгенерированных правил МЭ. Раздел [WAN]:

- 1,2 – **«Allow dhcpv6 client in WAN»** – Правила разрешают входящий трафик по протоколу DHCP;
- 3 – **«Allow dhcpv6 client out WAN»** – Правило разрешает исходящий трафик по протоколу DHCP;
- 4 – **«Block bogon IPv4 networks from WAN»** – Правило блокирует IP-адреса Bogon-сетей IPv4;
- 5 – **«Block bogon IPv6 networks from WAN»** – Правило блокирует IP-адреса Bogon-сетей IPv6;
- 6,7 – **«Block private networks from WAN»** – Правила блокируют трафик, если адрес отправителя из локального сегмента адресов IPv4/IPv6;
- 8,9 – **«Allow DHCP client on WAN»** – Правила разрешают двусторонний обмен пакетами протокола DHCP для IPv4 сетей.

Примечание:

Количество автоматически сгенерированных правил может отличаться в зависимости от конфигурации **ARMA FW**. Например, при настройке **ARMA FW** в режиме отказоустойчивого кластера появятся автоматически сгенерированные правила в списке подраздела «[PFsync]» правил МЭ.

Примечание:

Помимо правил МЭ в **ARMA FW** присутствуют другие механизмы ограничения трафика, работающие в следующем порядке:

1. Правила ограничения трафика (см. Настройки ограничения трафика).
2. Правила NAT (см. NAT).
3. Правила МЭ (см. Межсетевой экран).
4. Правила СОВ (см. Система обнаружения и предотвращения вторжений).
5. Ограничения портала авторизации (см. Портал авторизации).

1.1.1 Создание правил межсетевого экранирования

Параметры создаваемого правила указаны в таблице (см. Таблица «Параметры создаваемого правила»).

Таблица «Параметры создаваемого правила»

Параметр	Значение
Действие	Разрешить (Pass)
Быстрая проверка	Да
Интерфейс	LAN
Направление	Вх.
Протокол	TCP
Отправитель	LAN сеть
IP-адрес назначения	Единственный хост или сеть 192.168.2.100/32
Диапазон портов назначения	HTTP - HTTP
Описание	Доступ к веб-серверу

Для параметров **«Отправитель»** и **«IP-адрес назначения»** существуют чек-боксы **«Инвертировать отправителя»** и **«Инвертировать получателя»** соответственно.

При установке флажка в данных чек-боксах правило будет применено для всех отправителей/получателей, кроме значений, указанных в полях параметров **«Отправитель»/«IP-адрес назначения»**.

Для создания правила МЭ необходимо выполнить следующие действия:

1. Перейти в подраздел общих правил МЭ (**«Межсетевой экран» - «Правила» - «[Общие]»**) (см. Рисунок – Подраздел «Общие»).

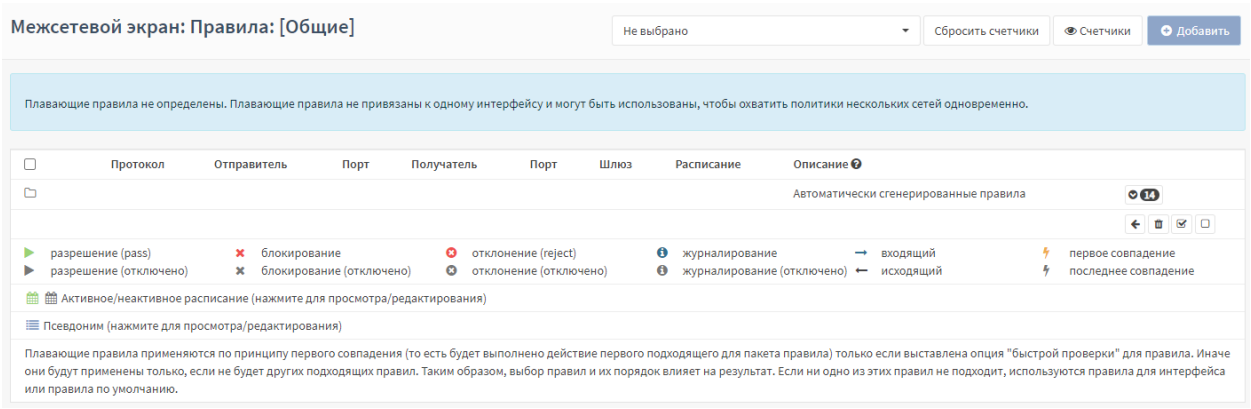


Рисунок – Подраздел «Общие»

2. Нажать **кнопку «+Добавить»** и в открывшейся форме (см. Рисунок – Создание правила МЭ) указать параметры из таблицы (см. Таблица «Параметры создаваемого правила»). Остальные параметры оставить без изменения.

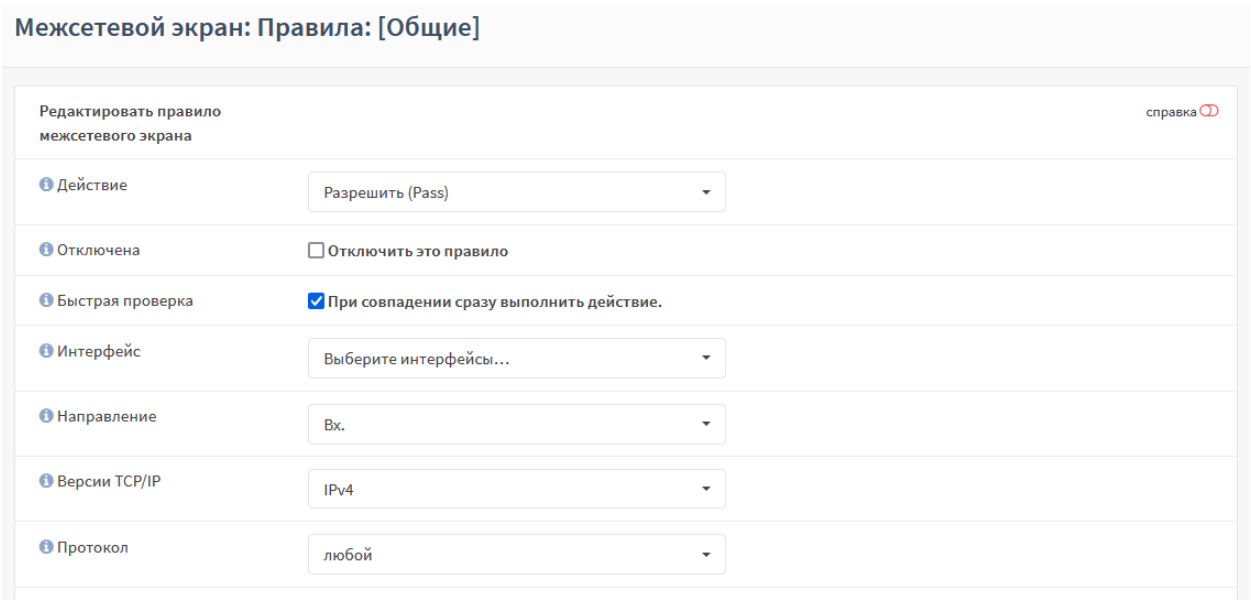


Рисунок – Создание правила МЭ

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»** (см. Рисунок – Принятие изменений).

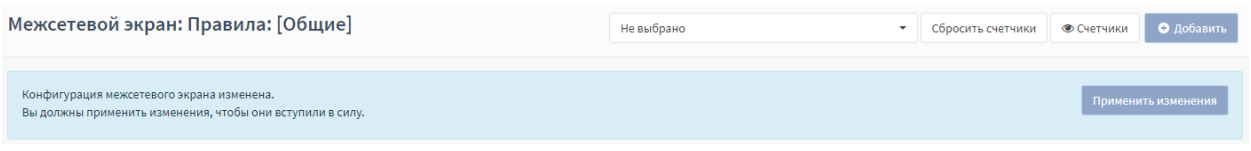


Рисунок – Принятие изменений

4. В результате правило будет применено и отображено в списке правил (см. Рисунок – Созданное правило в списке правил).

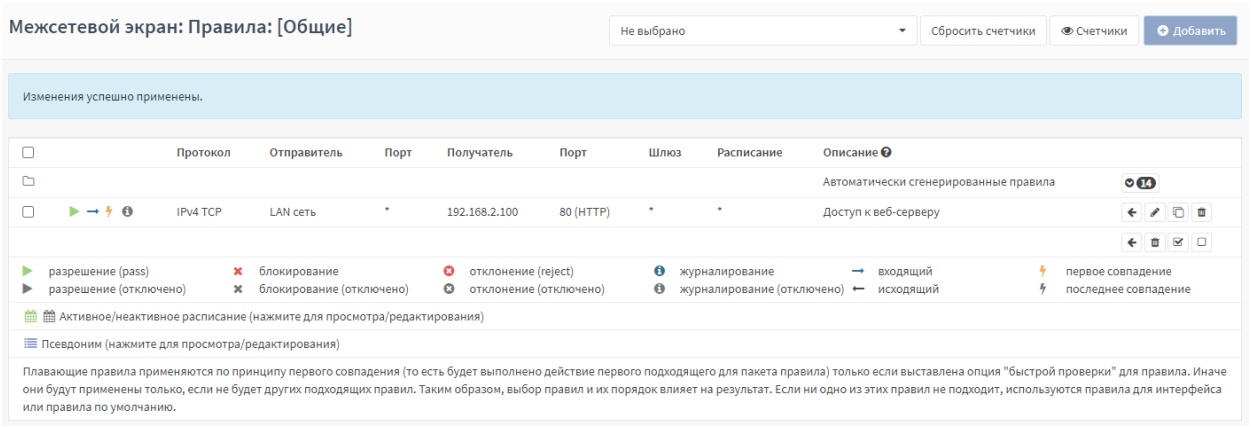


Рисунок – Созданное правило в списке правил

Для копирования правила, например, для разрешения HTTPS-трафика, необходимо выполнить следующие действия:

1. Нажать **кнопку** «  » и в открывшейся форме изменить порт с HTTP на HTTPS (см. Рисунок – Изменение диапазона портов).

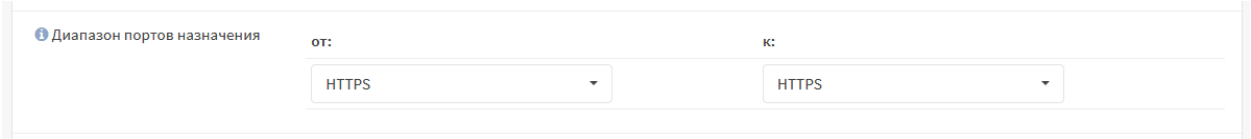


Рисунок – Изменение диапазона портов

2. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.
3. В результате правило будет применено и отображено в списке правил.

В примере не используются дополнительные возможности правил МЭ и дополнительные параметры, доступные при нажатии **кнопки «Показать/скрыть»** (см. Рисунок – Дополнительные возможности правил МЭ). Данные возможности и параметры необходимы для более тонкой настройки правил МЭ.

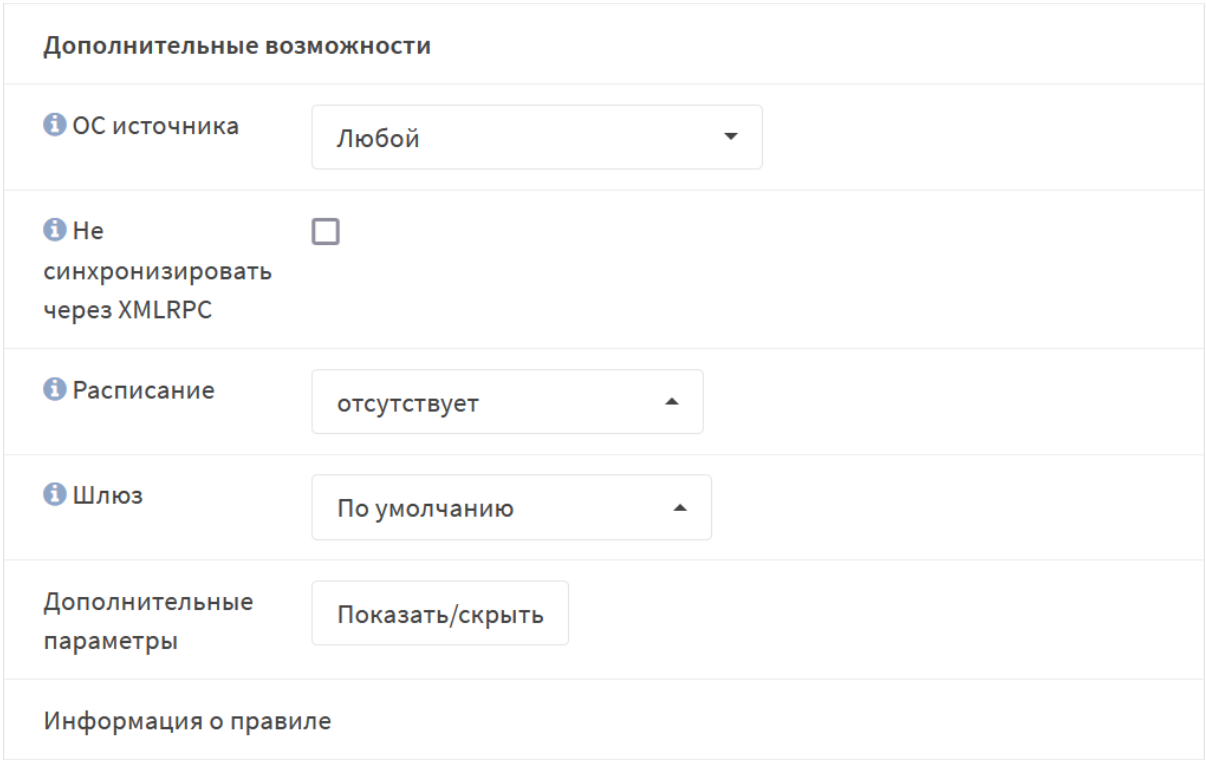


Рисунок – Дополнительные возможности правил МЭ

1.1.2 Проверка созданных правил МЭ

Для проверки работы правил МЭ необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «192.168.2.100» и нажать **клавишу «Enter»**. В результате отобразится стартовая страница веб-сервера (см. Рисунок – Стартовая страница веб-сервера).

Рисунок – Стартовая страница веб-сервера

1.1.3 Создание псевдонимов

Псевдонимы – удобный инструмент объединения множества сетей, хостов и портов с целью дальнейшего использования в правилах МЭ, NAT, переадресации портов и других настройках **ARMA FW**.

Правильное использование псевдонимов улучшает читаемость правил МЭ и ускоряет добавление новых или изменение действующих правил.

Для создания псевдонима необходимо выполнить следующие действия:

1. Перейти в подраздел управления псевдонимами (**«Межсетевой экран» - «Псевдонимы»**) и нажать **кнопку** « + » (см. Рисунок – Псевдонимы).

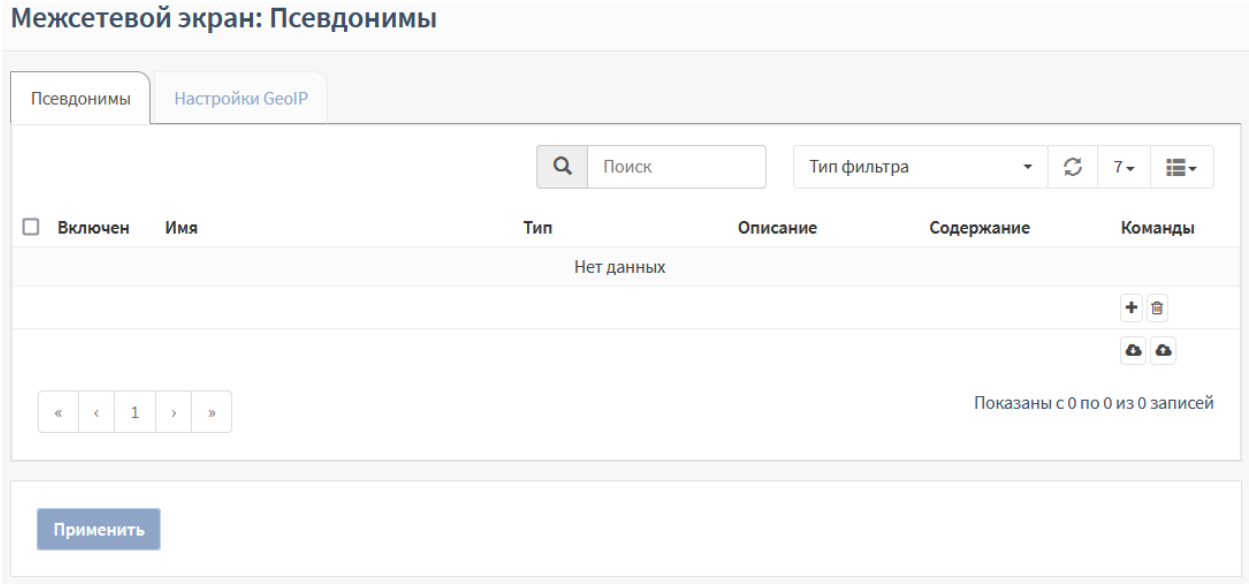


Рисунок – Псевдонимы

2. В открывшейся форме (см. Рисунок – Изменить псевдоним) указать параметры и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить»**.

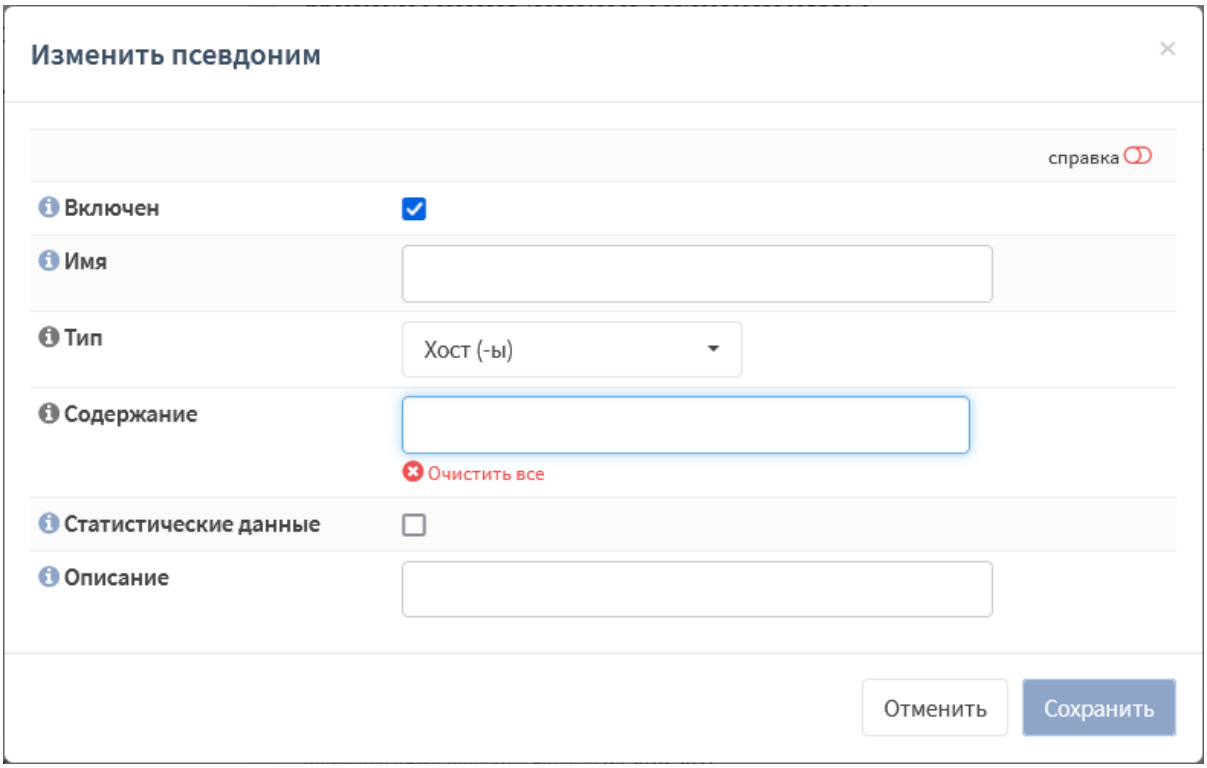


Рисунок – Изменить псевдоним

Обязательными для создания псевдонима являются поля **«Имя»** и **«Тип»**.

Типы псевдонимов, используемые в **ARMA FW**, и их краткое описание:

- **«Хост(-ы)»** – один или более хостов указываются по IP-адресам или FQDN;
- **«Сеть(-и)»** – одна или более сетей указываются в формате CIDR;
- **«Порт(-ы)»** – один или более портов протоколов TCP и UDP указываются в форме списка или диапазона;
- **«URL (IP-адреса)»** – URL размещённого на каком-то web-ресурсе списка IP-адресов. Список загружается один раз;
- **«Таблица URL (IP-адреса)»** – URL размещённого на каком-то web-ресурсе списка IP-адресов и периодичность обновления информации из списка. Список загружается с установленной периодичностью;
- **«GeoIP»** – одна или более стран и регионов;
- **«Сетевая группа»** – один или более псевдонимов типа **«Сеть(-и)»**;
- **«Внешний (расширенный)»** – внешний псевдоним (только объявление).

Каждый псевдоним может содержать от одного до нескольких значений (см. Рисунок – Несколько значений в псевдониме).

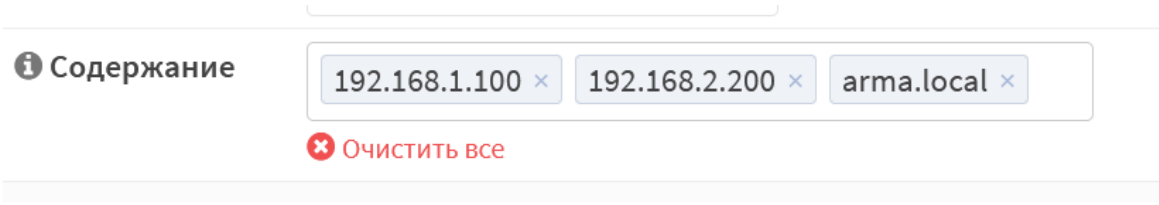


Рисунок – Несколько значений в псевдониме

Большинство псевдонимов могут быть вложены в другие псевдонимы. Например, псевдоним, содержащий веб-серверы, и псевдоним, содержащий почтовые серверы, могут вместе входить в один более крупный псевдоним, содержащий все серверы.

1.1.3.1 Хост (-ы)

В содержании псевдонима данного типа возможно указать один или более хостов. Хосты задаются списком IP-адресов или полностью определённым доменным именем FQDN.

В случае использования доменного имени для определения IP-адресов будет использоваться ответ DNS-сервера, опрос которого производится каждые 300 секунд. Интервал задаётся в параметре **«Интервал разрешения псевдонимов»** подраздела дополнительных настроек МЭ (**«Межсетевой экран» - «Настройки» - «Дополнительно»**).

1.1.3.2 Сеть (-и)

В содержании псевдонима данного типа возможно указать одну или более сетей IPv4 или IPv6.

Сети указываются в формате CIDR:

- <Адрес сети></><маска сети>, например, «192.168.1.0/24».

Используются списки сетей IPv4 и IPv6. Сети с масками «/32» для IPv4 и «/128» для IPv6 соответствуют одиночным хостам.

1.1.3.3 Порт (-ы)

В содержании псевдонима данного типа возможно указать один или более портов. Перечисляются одиночные порты, либо диапазоны портов, разделённые знаком «двоеточие».

Например, «420:500» будет соответствовать диапазону портов от 420 до 500.

1.1.3.4 URL (IP-адреса)

В содержании псевдонима данного типа возможно указать один или более URL со списком IP-адресов.

Список IP-адресов должен содержаться в текстовом файле, в котором каждый элемент списка (адрес отдельного хоста или сети) представлен отдельной строкой.

В списке IP-адресов могут быть указаны как отдельные IP-адреса, так и сети в формате CIDR.

URL задаются в следующей форме:

- <протокол><://><FQDN или IP-адрес хоста><путь к файлу списка>, например:
  - «https://www.spamhaus.org/drop/drop.txt»;
  - «http://192.168.252.130/ip_list.txt».

После создания данного псевдонима список IP-адресов загружается однократно, после этого обновление списка не происходит.

1.1.3.5 Таблицы URL (IP-адреса)

В содержании псевдонима данного типа возможно указать один или более URL списком IP-адресов и периодичность обновления информации из указанного списка.

Параметры списков и URL идентичны параметрам псевдонима типа **«URL (IP-адреса)»** (см. URL (IP-адреса)).

Периодичность обновления информации из списка задаётся в форме количества дней и количества часов в полях **«Д»** и **«Ч»** соответственно. По истечении указанного периода времени будет произведена загрузка файла заново.

В состав псевдонима типа **«Таблица URL (IP-адреса)»** нельзя вложить никакой псевдоним. Псевдоним типа **«Таблица URL (IP-адреса)»** также не может быть вложен ни в один другой псевдоним.

1.1.3.6 GeoIP

В содержании псевдонима данного типа указывается одна или более стран и/или регионов. Задание значений псевдонима осуществляется выбором соответствующего пункта из выпадающих меню.

После настройки псевдонима необходимо добавить правило МЭ и указать следующие параметры:

- **«Действие»** – требуемое действие;
- **«Направление»** – «Любой»;
- **«Отправитель»** – имя соответствующего псевдонима GeoIP;
- **«Описание»** – краткое описание.

1.1.3.6.1 Обновление локальной базы IP-адресов

Для настройки обновления локальной базы IP-адресов с сервера **InfoWatch ARMA** необходимо перейти во вкладку **«Настройки GeoIP»** подраздела настройки

псевдонимов (**«Межсетевой экран» - «Псевдонимы»**), ввести в полях параметров **«Имя пользователя»** и **«Пароль»** значения, предоставляемые вендором, и нажать **кнопку «Применить»** (см. Рисунок – Настройки GeoIP).

Примечание:

Для успешного импорта базы IP-адресов с сервера обновлений требуется доступ к сети Интернет.

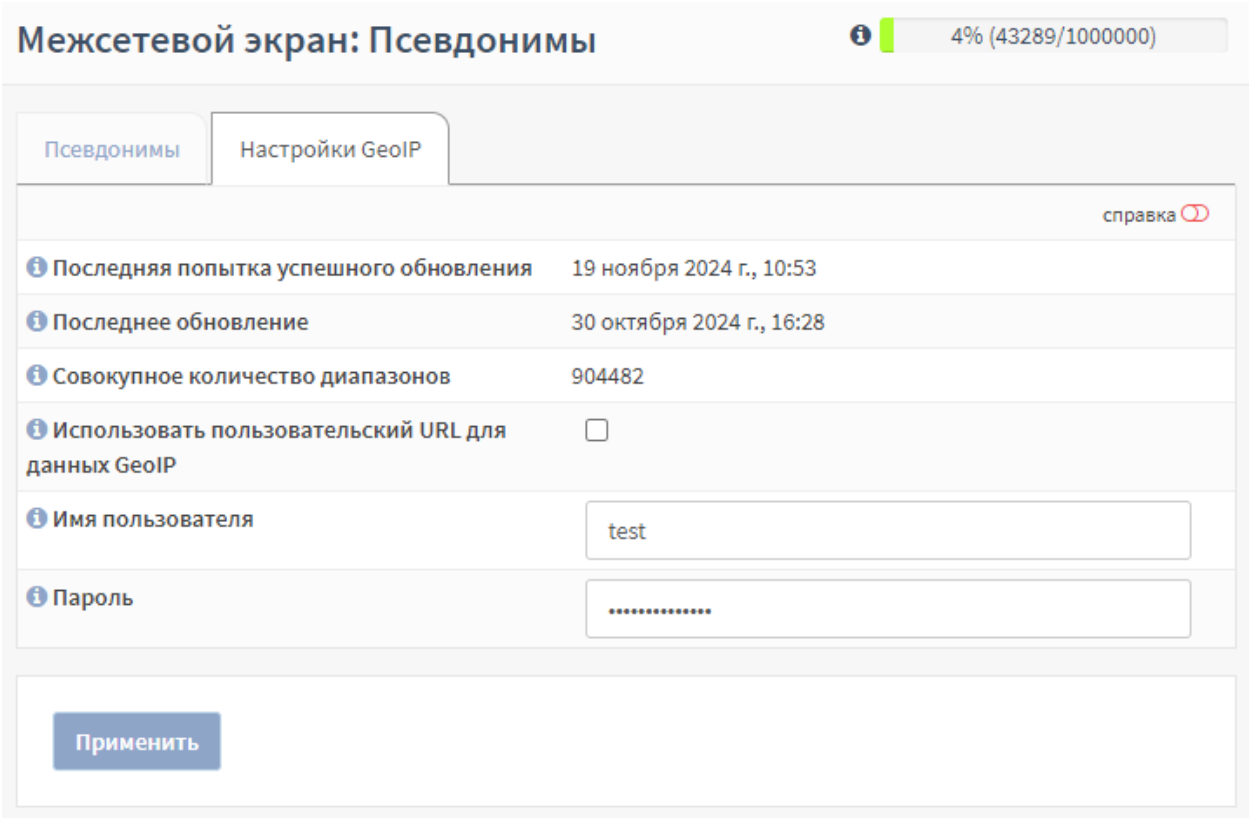


Рисунок – Настройки GeoIP

При корректно введённых значениях, отобразятся актуальные сведения о дате и времени создания данных на сервере обновлений, а также о совокупном количестве диапазонов.

В случае необходимости импорта диапазонов с определённого ресурса в сети Интернет следует установить флажок для параметра **«Использовать пользовательский URL для данных GeoIP»**, указать адрес в поле параметра **«URL»** и нажать **кнопку «Применить»** (см. Рисунок – Пользовательский URL для данных GeoIP).

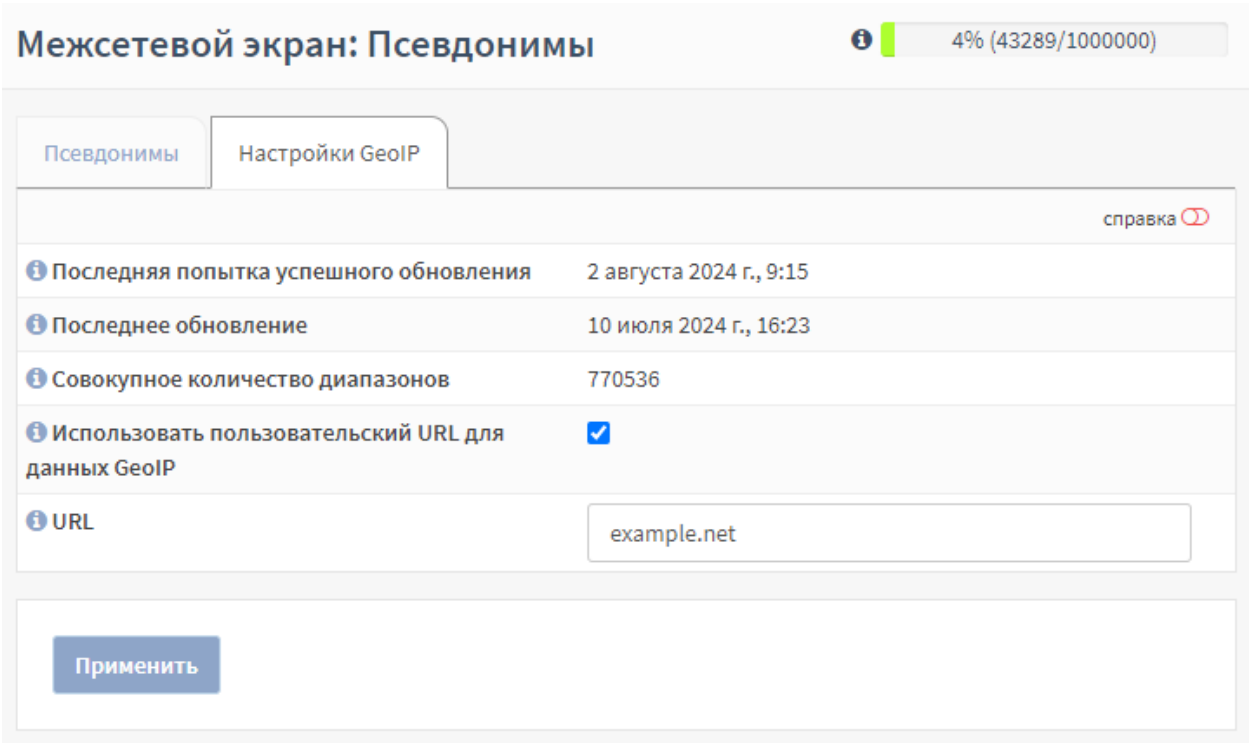


Рисунок – Пользовательский URL для данных GeoIP

1.1.3.7 Сетевая группа

В содержании псевдонима данного типа указывается один или более существующих псевдонимов типа **«Сеть (-и)»** и/или **«Хост (-ы)»**. Функционально псевдоним выполняет ту же роль, что и псевдоним типа **«Сеть (-и)»**, но использует другой подход к отображению содержания псевдонима, что может упростить управление большим количеством псевдонимов типа **«Сеть (-и)»**.

1.1.3.8 Внешний (расширенный)

Содержание псевдонима данного типа нельзя указать средствами веб-интерфейса. В подразделе управления псевдонимами (**«Межсетевой экран» - «Псевдонимы»**) выполняется только объявление псевдонима для дальнейшего использования его в правилах межсетевого экрана. Содержание псевдонима управляется отдельными плагинами к **ARMA FW**, к функциональности которых относится псевдоним.

1.1.4 Создание групп интерфейсов

Данная функция позволяет создавать правила, применяемые к нескольким интерфейсам без дублирования правил (см. Рисунок – Создание групп интерфейсов).

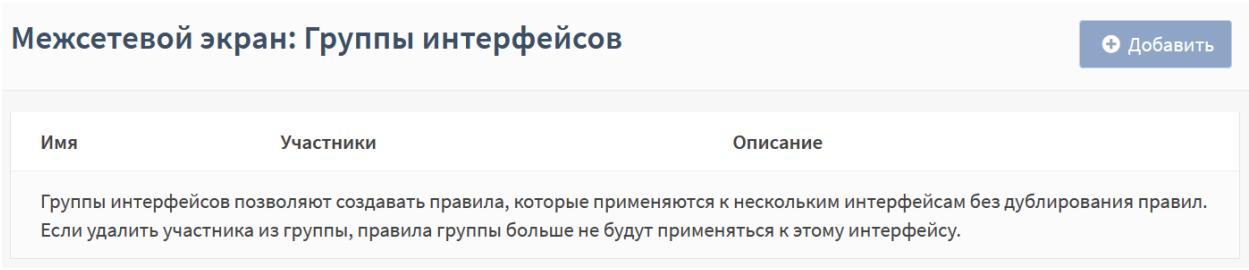


Рисунок – Создание групп интерфейсов

В качестве примера использования групп интерфейсов подходит следующая задача:

- разрешить прохождение трафика ICMP по всем внутренним сетям согласно схеме стенда, представленного на рисунке (см. Рисунок – Пример использования МЭ).

Для выполнения такой задачи необходимо объединить внутренние интерфейсы «OPT1» и «LAN» в группу и создать соответствующее правило.

Для создания группы интерфейсов необходимо выполнить следующие действия:

1. Перейти в подраздел настроек групп интерфейсов (**«Межсетевой экран» - «Группы интерфейсов»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Редактирование группы интерфейсов) указать следующие параметры:
   - поле **«Имя»** – «OPT1_LAN»;
   - поле **«Описание»** – «Внутренние интерфейсы»;
   - в списке **«Участники»** – «LAN» и «OPT1».

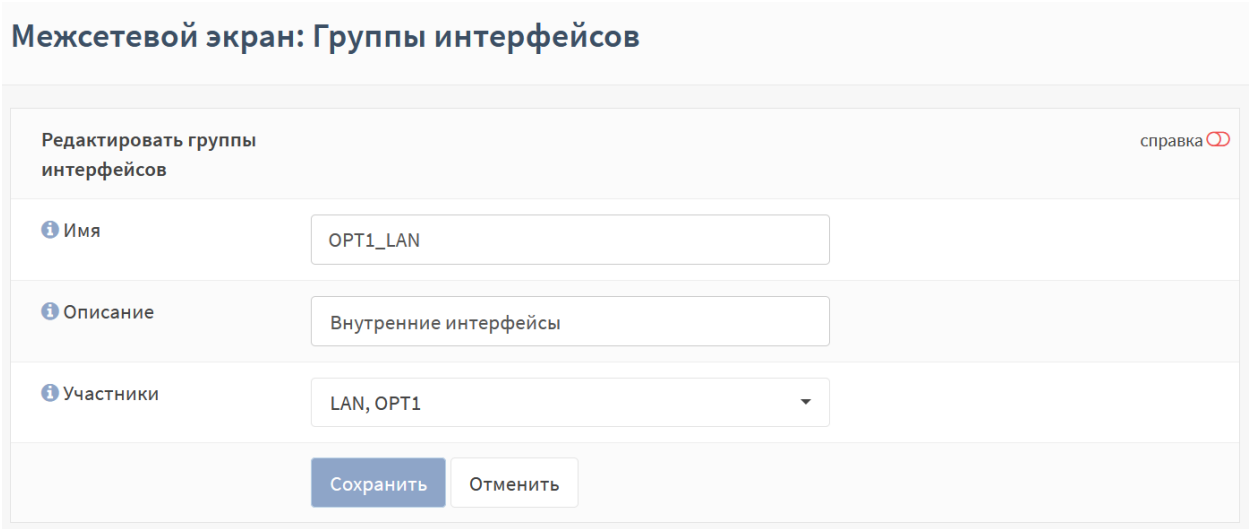


Рисунок – Редактирование группы интерфейсов

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

4. В результате созданная группа интерфейсов появится в подразделе **«Правила»** (см. Рисунок – Созданная группа интерфейсов).

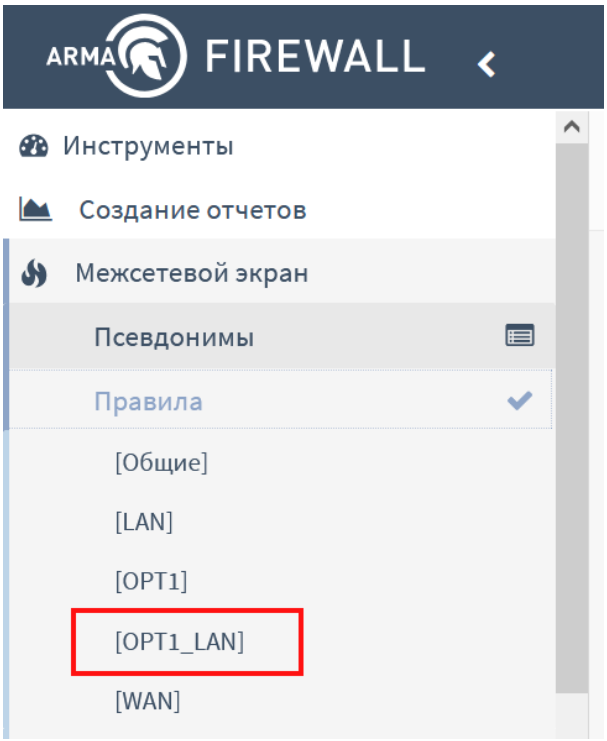


Рисунок – Созданная группа интерфейсов

После этого необходимо создать правило (см. раздел Создание правил межсетевого экранирования) для этой группы интерфейсов с параметрами, указанными в таблице (см. Таблица «Значения параметров правила для группы интерфейсов»).

Таблица «Значения параметров правила для группы интерфейсов»

Параметр	Значение
Действие	Разрешить (Pass)
Интерфейс	OPT1_LAN
Направление	Любой
Протокол	ICMP

После сохранения и применения правила трафик ICMP будет доступен на внутренних интерфейсах (см. Рисунок – Результат работы команды «Ping»).

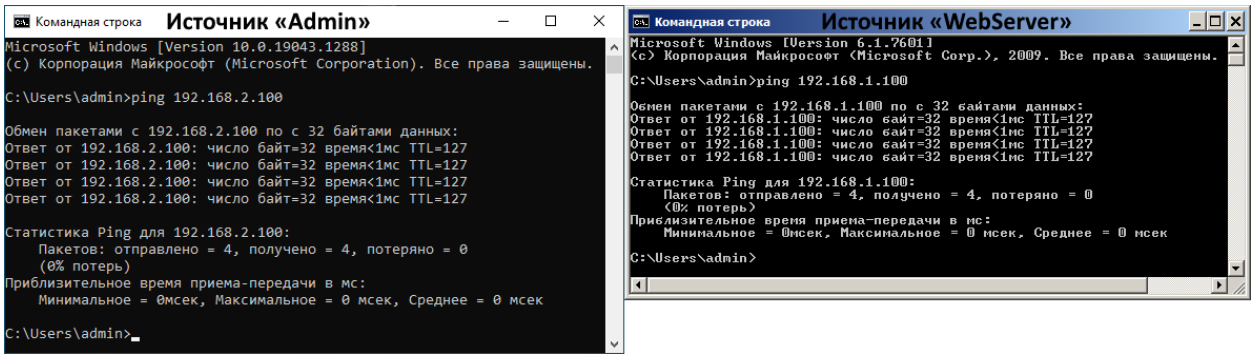


Рисунок – Результат работы команды «Ping»

1.1.5 Создание расписания срабатывания правил

В некоторых случаях необходимо указать расписание работы правил МЭ. Например, требуется разрешить доступ к веб-серверу (см. Рисунок – Пример использования МЭ) только на рабочую неделю – с 21 по 25 октября 2024 года.

Для решения данной задачи необходимо создать расписание и изменить созданные ранее правила МЭ.

Для создания расписания необходимо выполнить следующие действия:

1. Перейти в подраздел управления расписаниями (**«Межсетевой экран» - «Настройки» - «Расписания»**) (см. Рисунок – Расписания для правил МЭ) и нажать **кнопку «+Добавить»**.

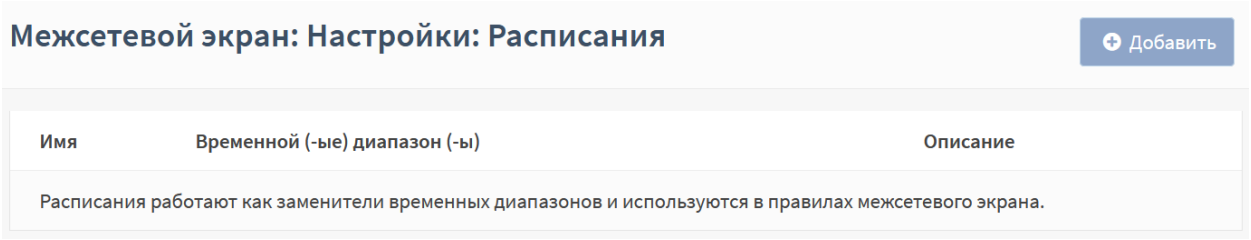


Рисунок – Расписания для правил МЭ

2. В открывшейся форме (см. Рисунок – Создание расписания для правил МЭ) выполнить следующие действия:
   - в поле **«Имя»** указать значение «WebServer_Week»;
   - в списке **«Месяц»** выбрать «Октябрь 2024»;
   - нажать левой кнопкой мыши на все числа в диапазоне от 21 до 25 включительно;
   - в поле **«Конечное время»** указать «23:59»;
   - нажать **кнопку «Добавить время»**.

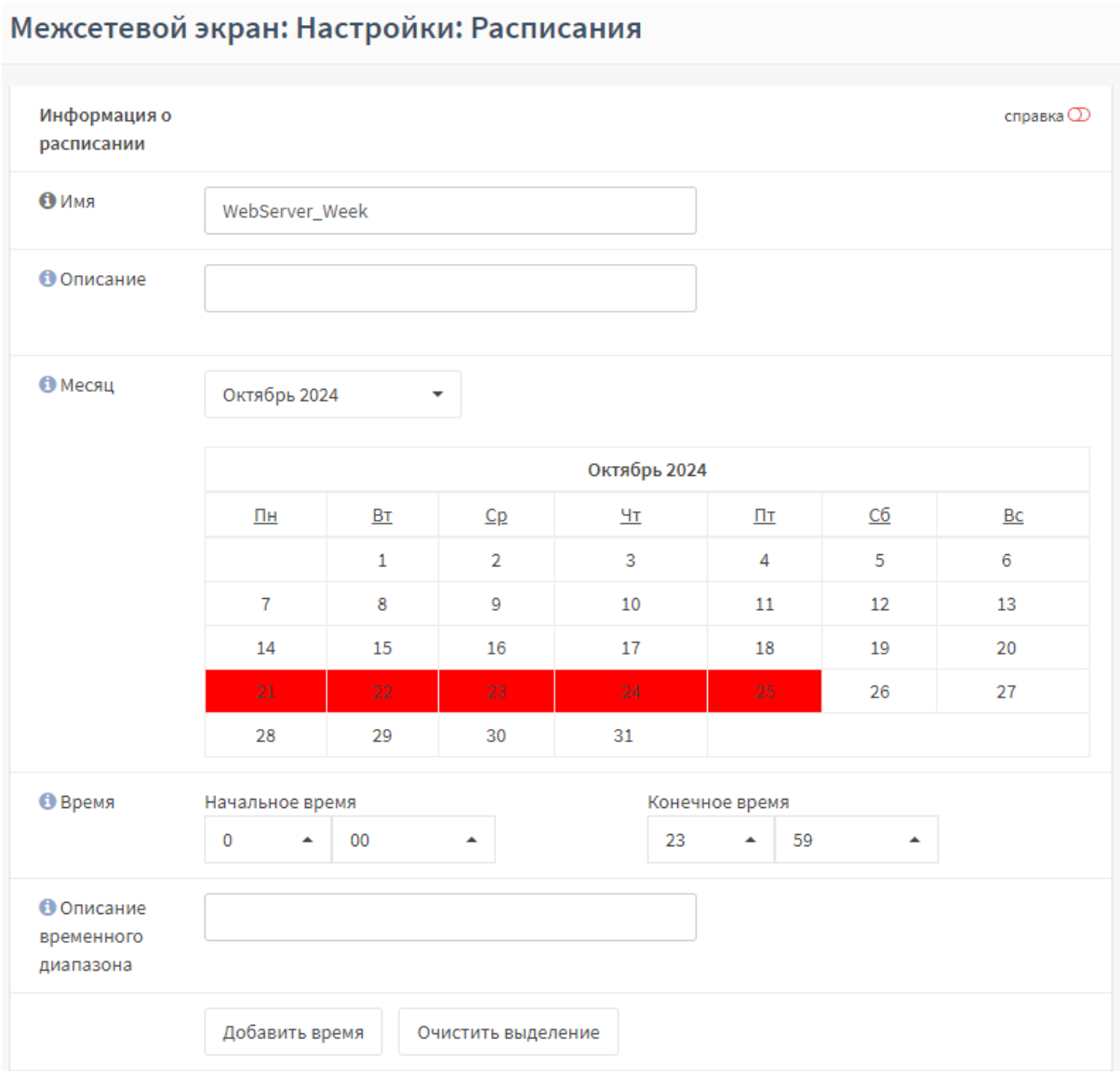


Рисунок – Создание расписания для правил МЭ

3. В результате в блоке **«Повторение расписание»** формы будет отображено выбранное время (см. Рисунок – Настроенные диапазоны).

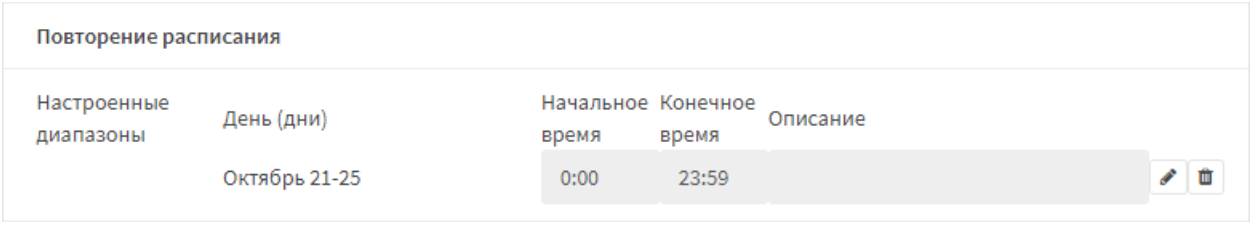


Рисунок – Настроенные диапазоны

4. Нажать **кнопку «Сохранить»**.
5. В результате созданное расписание будет отображено в списке (см. Рисунок – Созданное расписание для правил МЭ).

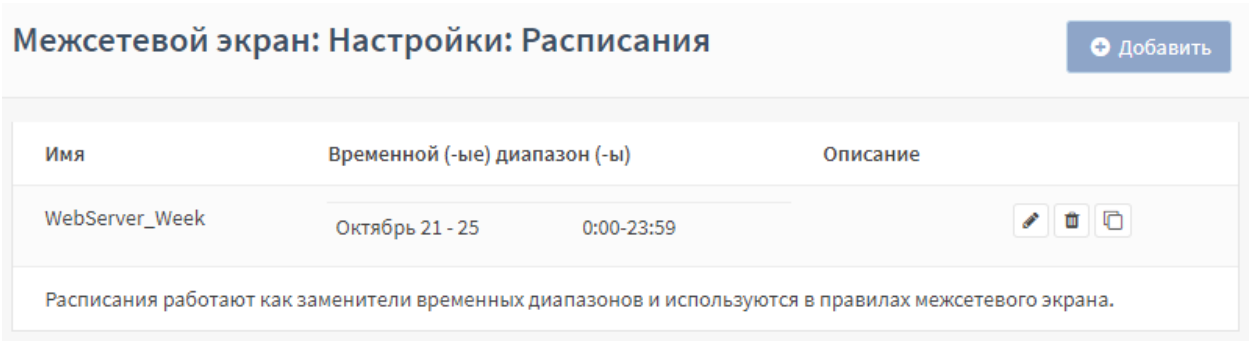


Рисунок – Созданное расписание для правил МЭ

После создания расписания необходимо изменить правила МЭ для ограничения доступа к веб-серверу, выполнив следующие действия:

1. Перейти в подраздел общих правил МЭ (**«Межсетевой экран» - «Правила» - «[Общие]»**) (см. Рисунок – Подраздел «Общие») и нажать **кнопку** « » напротив соответствующего правила.
2. В открывшейся форме (см. Рисунок – Создание правила МЭ) в поле **«Расписание»** выбрать значение **«WebServer_Week»** (см. Рисунок – Выбор расписания в правилах МЭ).

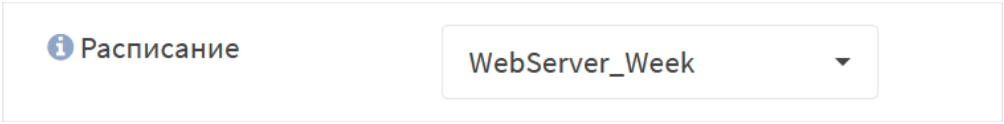


Рисунок – Выбор расписания в правилах МЭ

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.
4. В результате расписание будет применено к правилу и будет отображено в столбце **«Расписание»** в списке правил (см. Рисунок – Правила МЭ с расписанием).

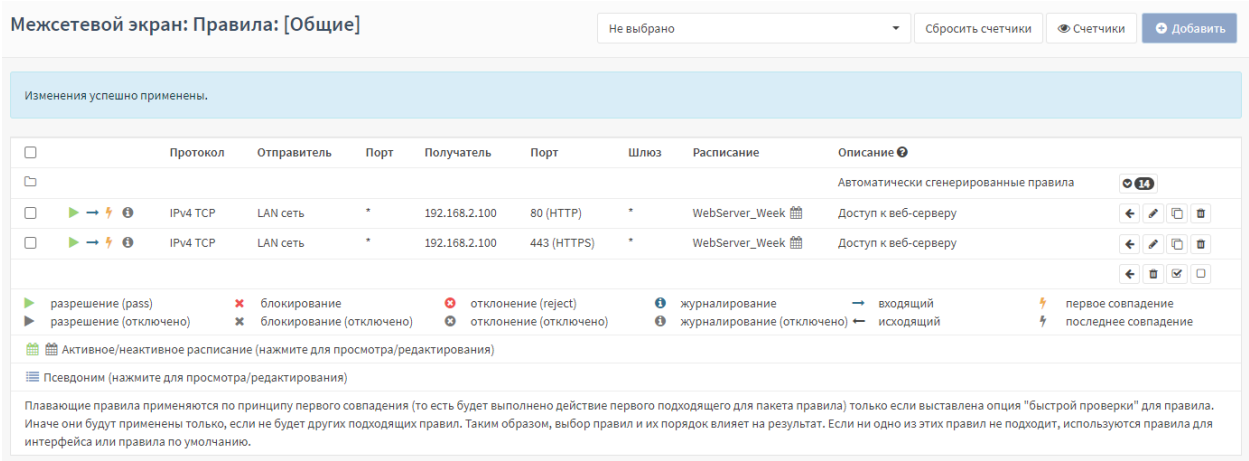


Рисунок – Правила МЭ с расписанием

1.1.6 Создание правил API

Для управления извне **ARMA FW** необходимо создать соответствующие правила МЭ в подразделе управления правил API (**«Межсетевой экран» - «API правила»**).

Правила создаются по аналогии с другими правилами МЭ (см. Создание правил межсетевого экранирования).

Для создания правила API необходимо выполнить следующие действия:

1. Перейти в подраздел управления правил API (**«Межсетевой экран» - «API правила»**) и нажать **кнопку** « + ».
2. В открывшейся форме (см. Рисунок – Создание правила API) задать параметры правила и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

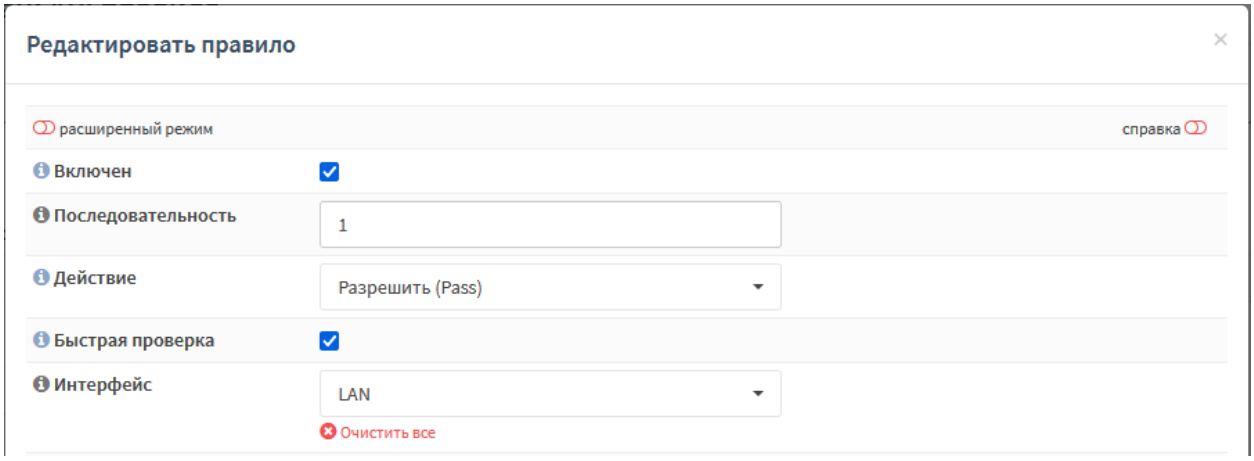


Рисунок – Создание правила API

1.1.7 Мониторинг срабатывания правил

ARMA FW позволяет отслеживать количество срабатываний правил.

Для отображения таблицы мониторинга срабатывания правил следует в разделе правил МЭ (**«Межсетевой экран» - «Правила»**) перейти в необходимый подраздел, например **«[LAN]»**, и нажать **кнопку «Счетчики»** (см. Рисунок – Мониторинг срабатывания правил).

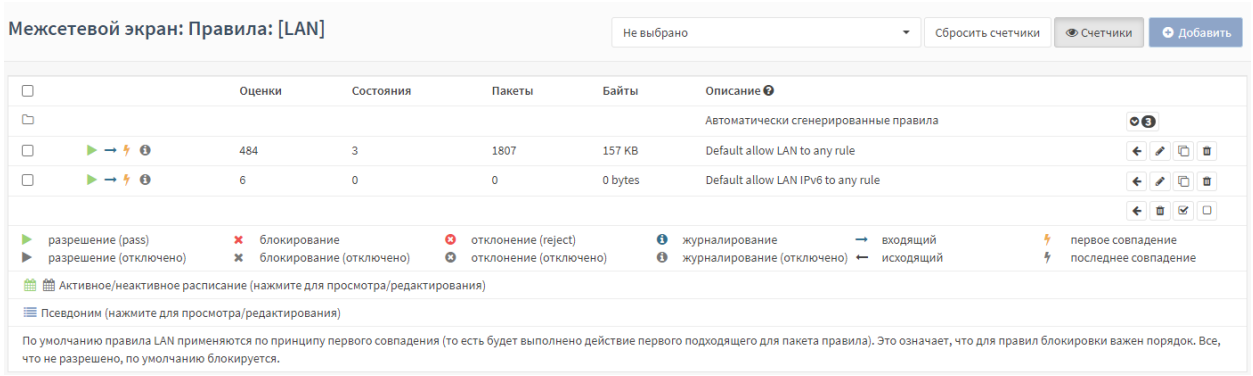


Рисунок – Мониторинг срабатывания правил

Таблица мониторинга срабатывания правил содержит следующие показатели:

- **«Оценки»** - количество выполненных сравнений правила;
- **«Состояния»** - количество срабатываний правила;
- **«Пакеты»** - количество перехваченных пакетов;
- **«Байты»** - общий размер перехваченных пакетов;
- **«Описание»** - описание правила.

Подсчёт срабатывания правила ведётся с момента его создания или с последнего обнуления счётчика, осуществляемого нажатием **кнопки «Сбросить счётчики»**.

2 NAT

Трансляция сетевых адресов, сокращённо NAT – это технология преобразования IP-адресов внутренней сети «LAN» в IP-адреса внешней сети «WAN». Существуют следующие способы трансляции сетевых адресов:

- **переадресация портов** – позволяет получить доступ из внешней сети во внутреннюю сеть с перенаправлением на конкретный адрес и порт;
- **статический NAT, «Один-к-одному»** – позволяет каждому внутреннему IP-адресу присваивать уникальный внешний IP-адрес;
- **исходящий NAT, «Маскарадинг»** – позволяет множеству устройств, находящихся за NAT, выходить в сеть через один внешний IP-адрес. Скрывает структуру сети от внешнего мира.

Правила NAT задаются отдельно для каждого способа и располагаются в виде списка.

Порядок правил в списке имеет значение и им можно управлять с помощью **кнопки** « » напротив каждого из созданных правил. Сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз, по следующему принципу:

- **последнего совпадения** – производится действие, указанное в последнем совпавшем правиле, далее обработка сетевого пакета не производится.

2.1 Создание правила NAT «Переадресация портов»

Переадресация портов позволяет указать, что все запросы, приходящие на конкретный внешний адрес и конкретный порт маршрутизатора, должны быть перенаправлены на конкретный внутренний адрес и порт получателя.

Пример использования NAT «Переадресация портов» приведён на рисунке (см. Рисунок – NAT «Переадресация портов») все обращения на порт 8080 интерфейса «WAN» переадресовываются на порт 80 веб-сервера «WebServer».

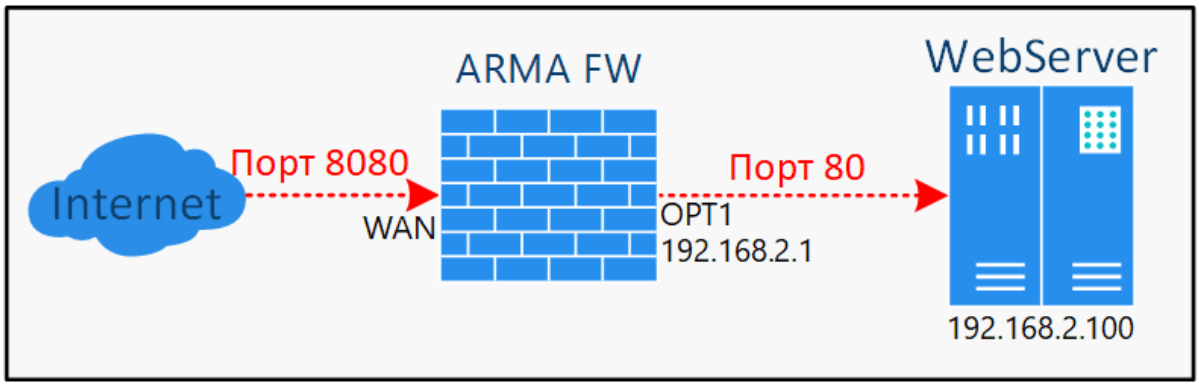


Рисунок – NAT «Переадресация портов»

Для настройки переадресации портов необходимо выполнить следующие действия:

1. Перейти в подраздел управления переадресацией портов (**«Межсетевой экран» - «NAT» - «Переадресация портов»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Создание правила NAT «Переадресация портов») указать следующие значения:
   - **«Интерфейс»** – «WAN»;
   - **«Версии TCP/IP»** – «IPv4»;
   - **«Протокол»** – «TCP»;
   - **«Отправитель»** – «любой»;
   - **«Диапазон портов источника»** – «любой»;
   - **«IP-адрес назначения»** – «WAN адрес»;
   - **«Диапазон портов назначения»** – «от: (другое), 8080», «к: (другое), 8080»;
   - **«Целевой IP-адрес»** – «192.168.2.100»;
   - **«Целевой порт перенаправления»** – «HTTP».
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

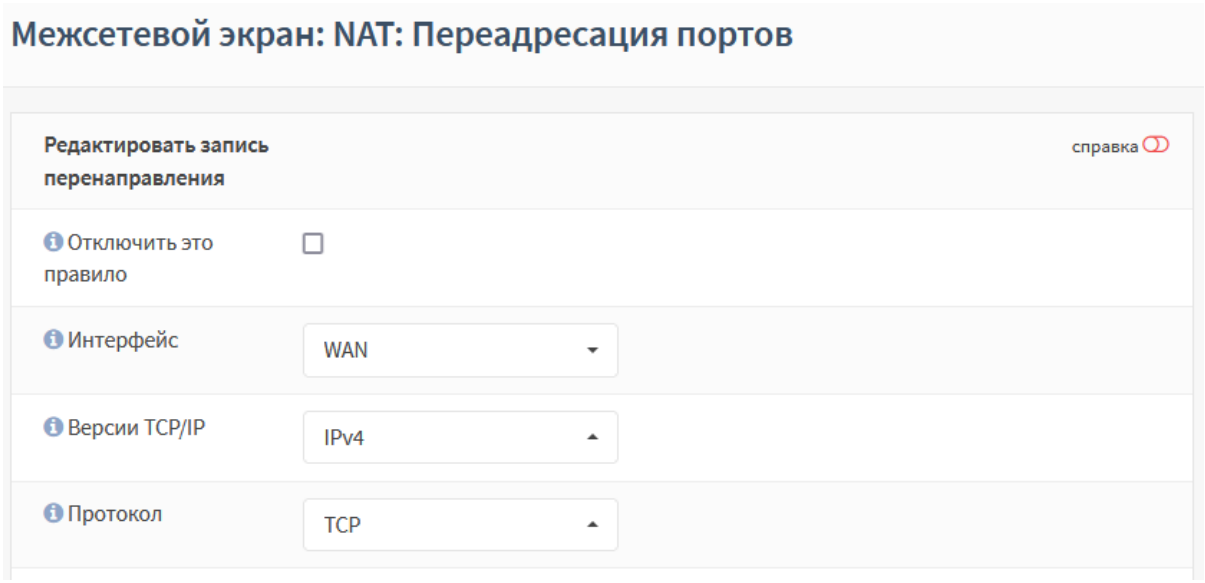


Рисунок – Создание правила NAT «Переадресация портов»

2.1.1 Дополнительные параметры правила NAT «Переадресация портов»

Для параметров **«Отправитель»** и **«IP-адрес назначения»** существуют чек-боксы **«Инвертировать отправителя»** и **«Инвертировать получателя»** соответственно. При установке флажка в данных чек-боксах правило будет применено для всех отправителей/получателей, кроме значений, указанных в полях параметров **«Отправитель»/«IP-адрес назначения»**.

Параметр **«Режим работы с сетью»** предназначен для выбора режима работы в случае использования конкретной сети в качестве целевого IP-адреса. По умолчанию используется циклический перебор транслируемых IP-адресов.

Поле **«Установить локальный тег»** предназначено для добавления внутреннего тэга пакетам, соответствующим критериям правила. Данный тэг могут проверять другие правила и фильтры NAT. Включение проверки тега осуществляется в поле **«Проверка на соответствие локального тега»**.

Параметр **«Не синхронизировать через XMLRPC»** предназначен для предотвращения передачи информации о записях состояния соединений другим участникам кластера межсетевых экранов.

Параметр **«Зеркальный NAT»** предназначен для включения/выключения возможности получить доступ к внешнему сервису из внутренней сети по публичному IP-адресу.

Параметр **«Ассоциация правила фильтрации»** необходим для создания правила МЭ разрешающего прохождение трафика перенаправления NAT. По умолчанию для параметра задано значение **«Rule»**, создающее правило МЭ, связанное с настраиваемым правилом NAT.

Также доступны следующие параметры:

- **«отсутствует»** – правило МЭ создаваться не будет;
- **«добавить ассоциированное правило фильтрации»** – создастся правило МЭ, связанное с правилом NAT;
- **«добавить неассоциированное правило фильтрации»** – создастся правило МЭ, несвязанное с правилом NAT. При этом изменения, внесённые в правило NAT, необходимо будет вручную вносить в правило МЭ;
- **«разрешить (Pass)»** – разрешает прохождение трафика без правила МЭ.

2.2 Создание правила NAT «Один-к-одному»

Статический NAT «Один-к-одному» сопоставляет один внешний IP-адрес, в большинстве случаев общедоступный, с одним внутренним IP-адресом, в большинстве случаев частным.

В **ARMA FW** предусмотрена настройка статического NAT двух типов:

- **«NAT»** – позволяет организовать связь между сетями одного размера, то есть применяется только в одном направлении;
- **«BINAT»** – позволяет организовать связь между разными подсетями без указания основного шлюза в настройках сетевого адаптера, то есть

определяет двунаправленное отображение между внешней и внутренней сетями и может быть использован в обоих направлениях.

Пример использования NAT «Один-к-одному» приведён на рисунке (см. Рисунок – NAT «Один-к-одному»). Все обращения на IP-адрес интерфейса «WAN» переадресовываются на IP-адрес ПК «WebServer».

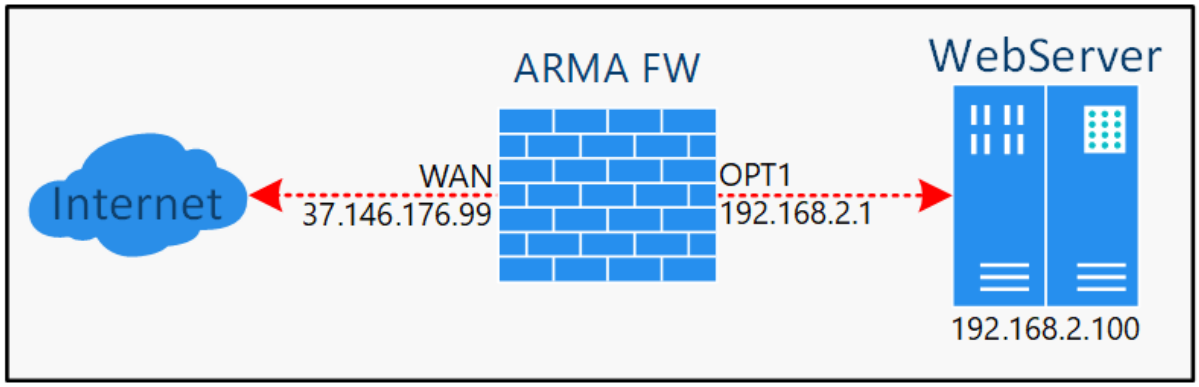


Рисунок – NAT «Один-к-одному»

Для настройки статического NAT необходимо выполнить следующие действия:

1. Перейти в подраздел настроек NAT один-к-одному (**«Межсетевой экран» - «NAT» - «Один-к-одному»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Создание правила NAT «Один-к-одному») указать следующие значения:
   - **«Интерфейс»** – «WAN»;
   - **«Тип»** – «BINAT»;
   - **«Внешняя подсеть»** – «37.146.176.0»;
   - **«IP-адрес источника»** – «Единственный хост или сеть, 192.168.2.100/32».
3. Остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

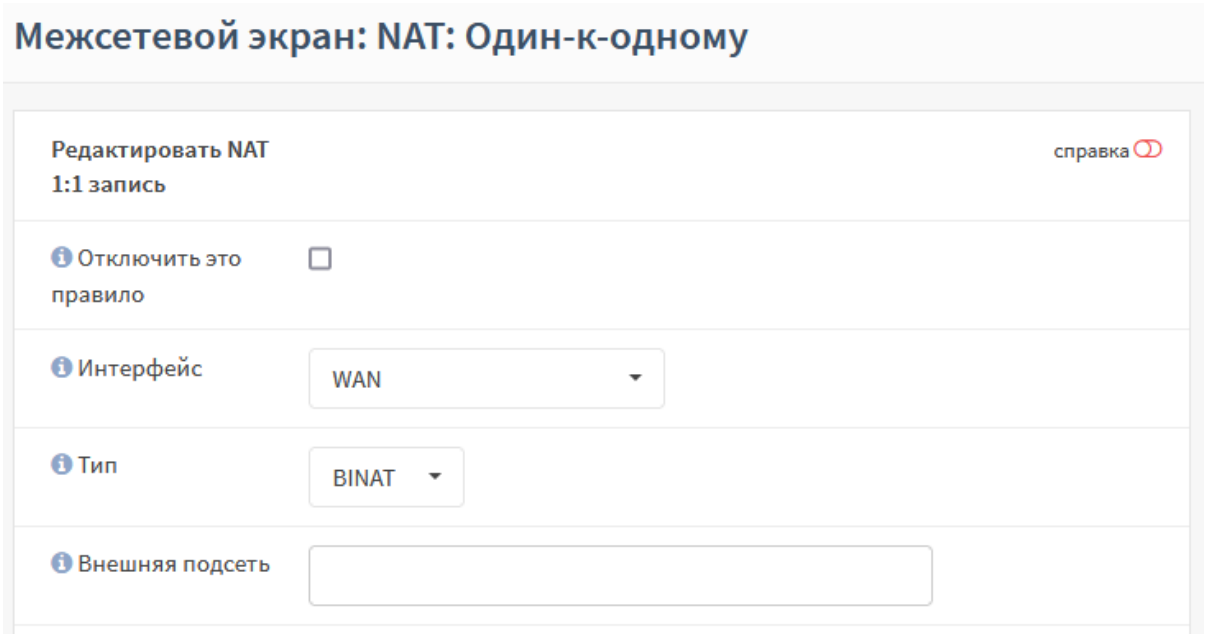


Рисунок – Создание правила NAT «Один-к-одному»

2.3 Создание правила NAT «Исходящий»

В **ARMA FW** представлены четыре режима работы исходящего NAT:

- **«автоматическое создание правил исходящего NAT»** – запрет использования созданных вручную правил;
- **«ручное создание правил исходящего NAT»** – правила не будут созданы автоматически;
- **«смешанное создание правил исходящего NAT»** – автоматически созданные правила применяются после созданных вручную правил;
- **«отключить создание правил исходящего NAT»** – исходящий NAT отключён.

По умолчанию в **ARMA FW** используется режим **«Автоматическое создание правил исходящего NAT»**.

2.3.1 Автоматическое создание правил исходящего NAT

В режиме автоматического создания правил исходящего NAT система автоматически добавляет правила NAT, которые обеспечивают соединение между сетью «WAN» и внутренней сетью «LAN» (см. Рисунок – Автоматический режим создания правил исходящего NAT).

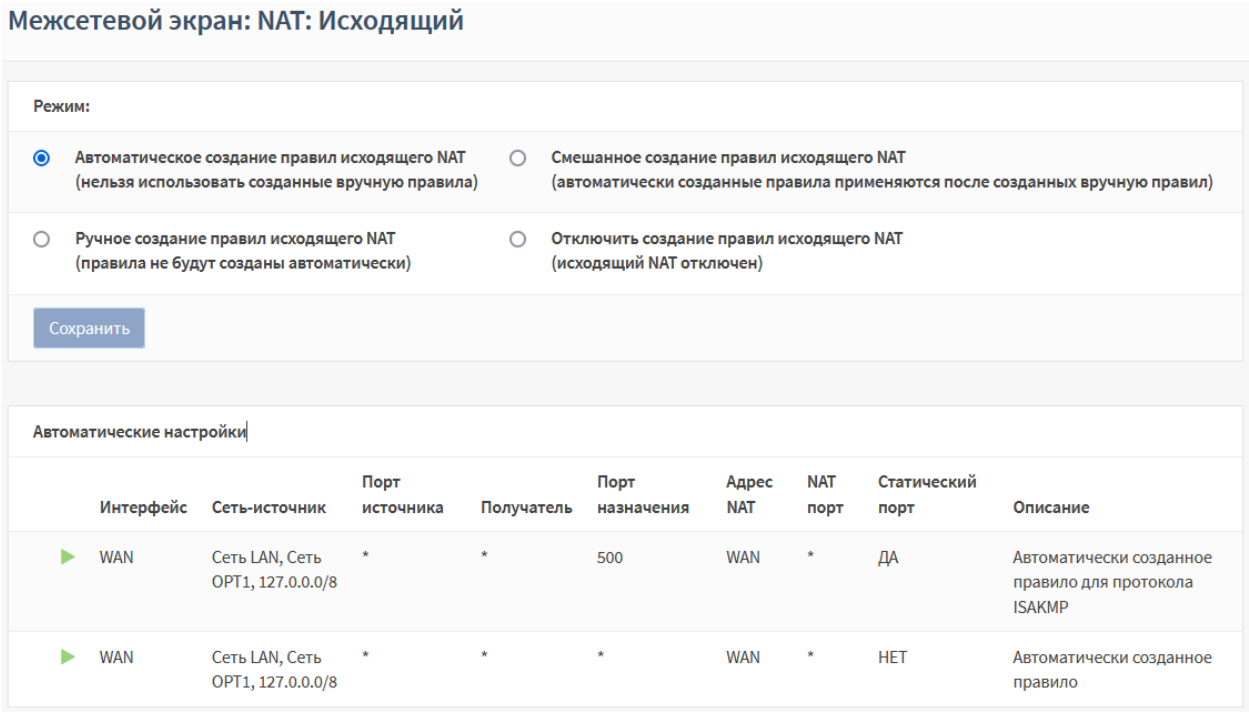


Рисунок – Автоматический режим создания правил исходящего NAT

2.3.2 Ручное создание правил исходящего NAT

Режим ручного создания правил исходящего NAT позволяет вручную создавать правила исходящего NAT. Правила контролируют, как **ARMA FW** будет преобразовывать адрес источника и порты трафика, выходящего из интерфейса.

Для возможности создания правил необходимо выбрать режим ручного создания правил исходящего NAT в подразделе настроек исходящего NAT (**«Межсетевой экран» - «NAT» - «Исходящий»**) нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**. После этого появится **кнопка «+Добавить»** в правом верхнем углу страницы.

Для проверки работы созданных вручную правил исходящего NAT необходимо выполнить следующие шаги:

1. С помощью веб-браузера на ПК **«Admin»** (см. Рисунок – Стенд для проверки созданных правил исходящего NAT) проверить доступность сайта «yandex.ru/internet».
2. Создать правило NAT со следующими основными параметрами:
   - **«Интерфейс»** – «WAN»;
   - **«IP-адрес источника»** – «LAN-сеть»;
   - **«Транслируемый IP-адрес/целевой IP-адрес»** – «WAN-адрес».

3. С помощью браузера на ПК **«Admin»** (см. Рисунок – Стенд для проверки созданных правил исходящего NAT) проверить доступность сайта «yandex.ru/internet».

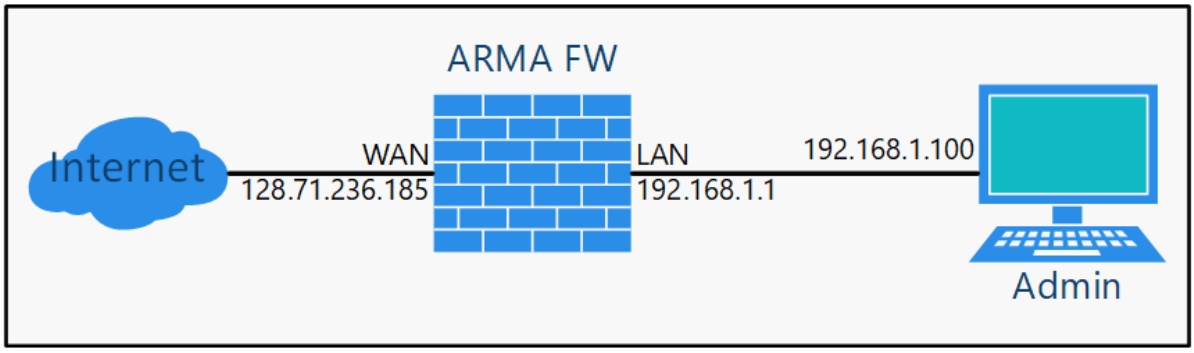


Рисунок – Стенд для проверки созданных правил исходящего NAT

2.3.2.1 Проверка доступности сайта

В режиме ручного создания правил исходящего NAT правила исходящего NAT отсутствуют.

Для проверки доступности сайта необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «yandex.ru/internet» и нажать **клавишу «Enter»**. В результате откроется страница, указывающая на отсутствие доступа к сайту (см. Рисунок – Недоступность сайта).

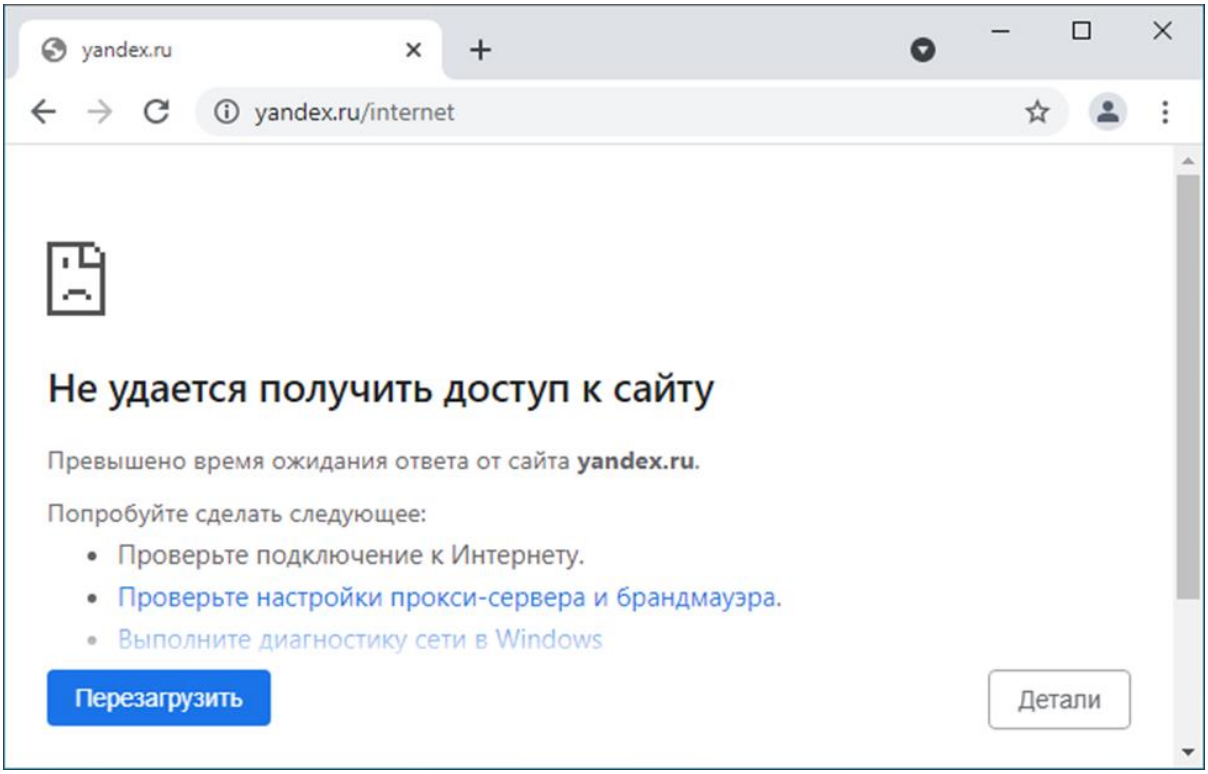


Рисунок – Недоступность сайта

2.3.2.2 Создание правила NAT

Для создания правила необходимо выполнить следующие действия:

1. Перейти в подраздел настроек исходящего NAT (**«Межсетевой экран» - «NAT» - «Исходящий»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Форма редактирования правил NAT) указать основные параметры указанные в примере (см. Ручное создание правил исходящего NAT), нажать **кнопку «Сохранить»** и затем нажать **кнопку «Применить изменения»**.

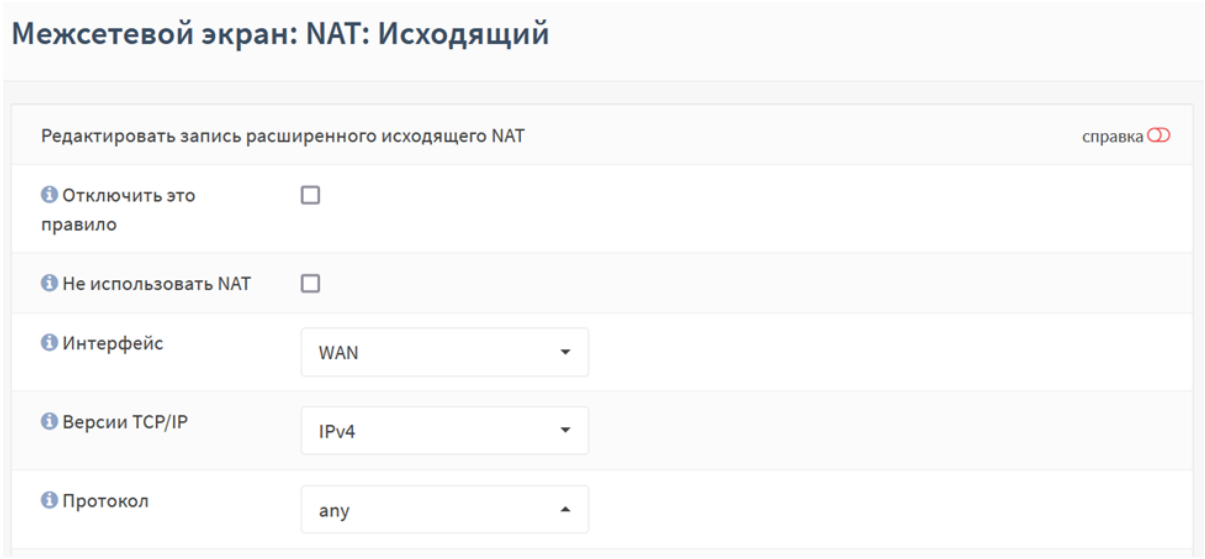


Рисунок – Форма редактирования правил NAT

В результате правило исходящего NAT будет создано и отобразится в списке правил (см. Рисунок – Список правил исходящего NAT).

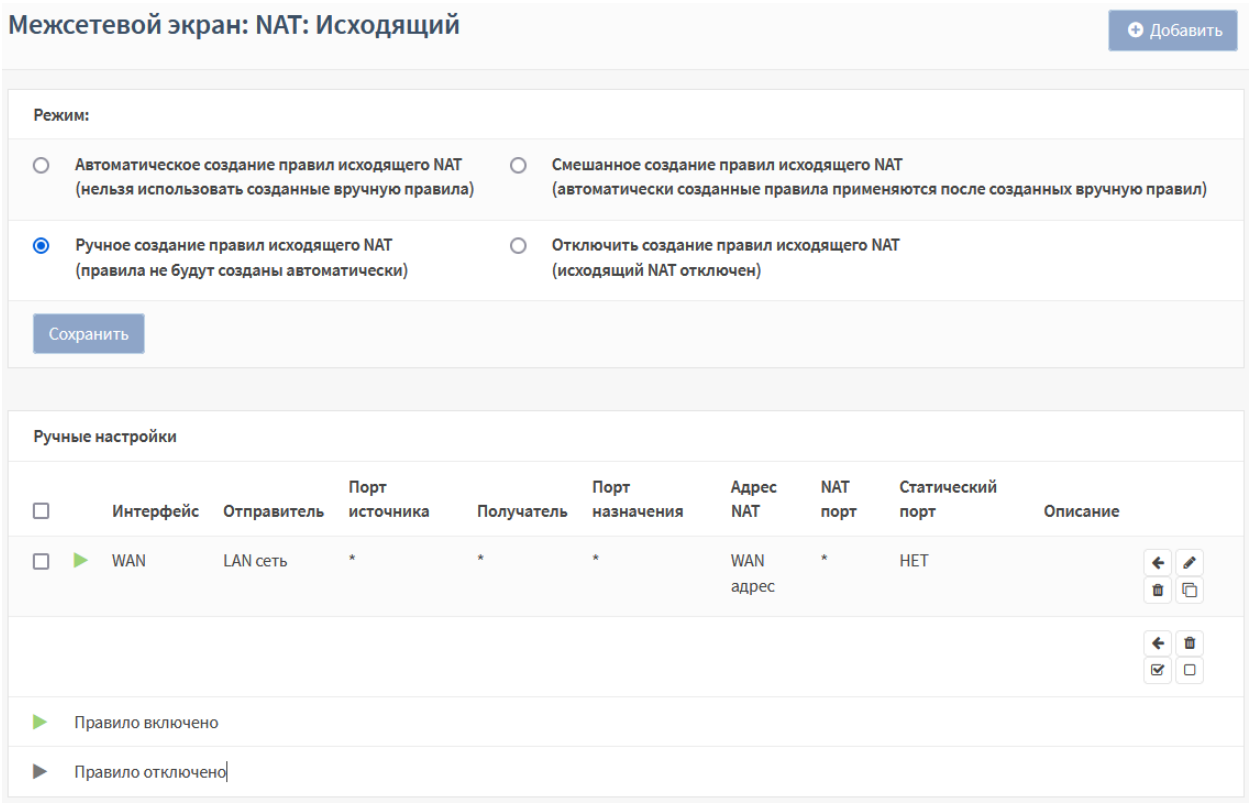


Рисунок – Список правил исходящего NAT

В примере рассматриваются только основные настройки исходящего правила NAT. Остальные параметры необходимы для более тонкой настройки правил.

Порядок правил в списке имеет значение и им можно управлять с помощью кнопки «  » напротив каждого из созданных правил. Правила обрабатываются, начиная с самого верхнего и далее вниз по списку.

2.3.2.3 Проверка доступности сайта

В веб-браузере на ПК **«Admin»** ввести в адресной строке «yandex.ru/internet» и нажать **клавишу «Enter»**. В результате откроется страница с данными о внешнем IP-адресе интерфейса «WAN» (см. Рисунок – Работа исходящего NAT).

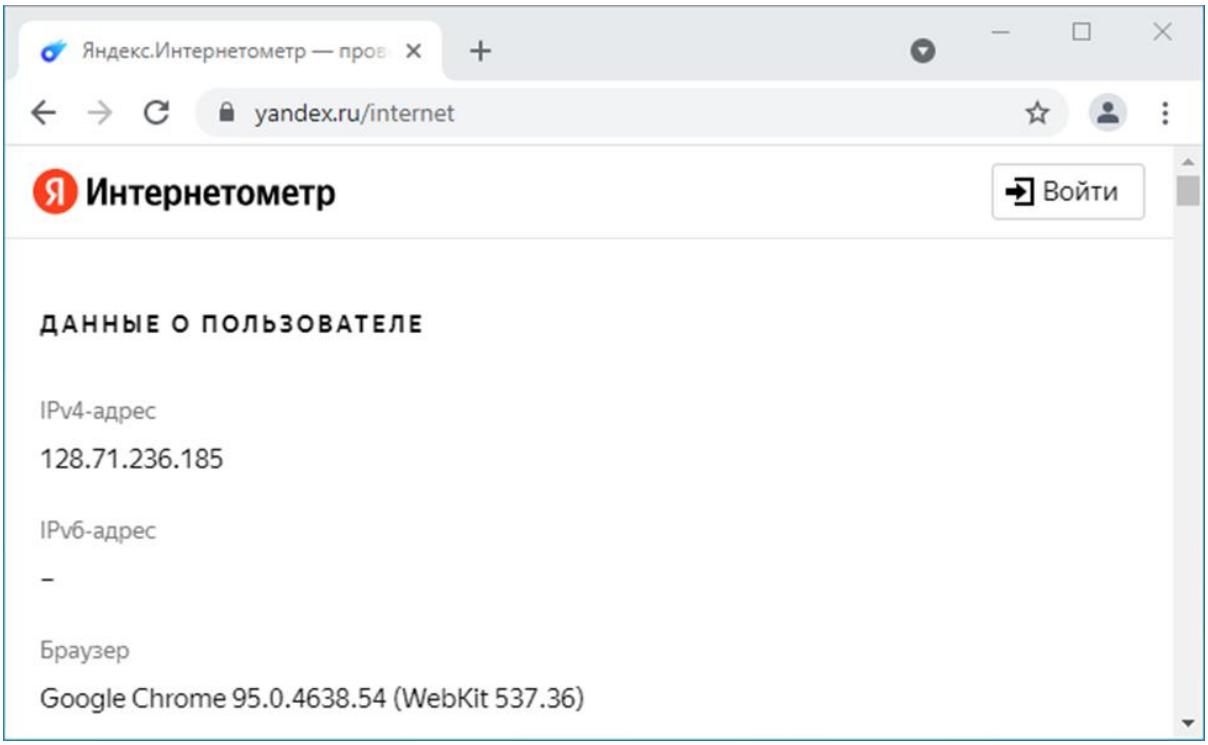


Рисунок – Работа исходящего NAT

2.3.3 Смешанное создание правил исходящего NAT

Режим смешанного создания правил исходящего NAT позволяет создавать правила исходящего NAT, но также присутствуют автоматические правила исходящего NAT.

2.3.4 Отключить создание правил исходящего NAT

Режим отключения создания правил исходящего NAT отключает все правила исходящего NAT.

3 НАСТРОЙКИ ОГРАНИЧЕНИЯ ТРАФИКА

Функция ограничения трафика позволяет гибко настраивать пропускную способность канала, управлять приоритетом трафика для сетей, хостов и приложений с целью обеспечения непрерывности критичных сетевых сервисов, в том числе в моменты пиковой сетевой нагрузки.

Примеры использования ограничения трафика:

- ограничение скорости входящего и исходящего соединений;
- ограничение максимальной пропускной способности на интерфейсе;
- приоритизация одного вида трафика перед другим.

В качестве примера настройки будет использоваться следующее ограничение трафика:

- **сегмент «LAN»** – 192.168.1.0/24, хост сегмента 192.168.1.100;
- **сегмент «WAN»** – 192.168.2.0/24, хост сегмента 192.168.2.100;
- **скорость входящего соединения** – 10 Мбит/с, из сегмента «WAN» в сегмент «LAN»;
- **скорость исходящего соединения** – 1 Мбит/с, из сегмента «LAN» в сегмент «WAN»;
- **равномерное распределение скорости** – между всеми хостами сегмента «LAN».

Для проверки корректности настройки будет использоваться утилита командной строки «iperf», не входящая в состав **ARMA FW**.

До момента настройки ограничений пропускная способность равна 431 Мбит/с и 456 Мбит/с для исходящего и входящего соединений соответственно (см. Рисунок – Результат работы утилиты «iperf»).

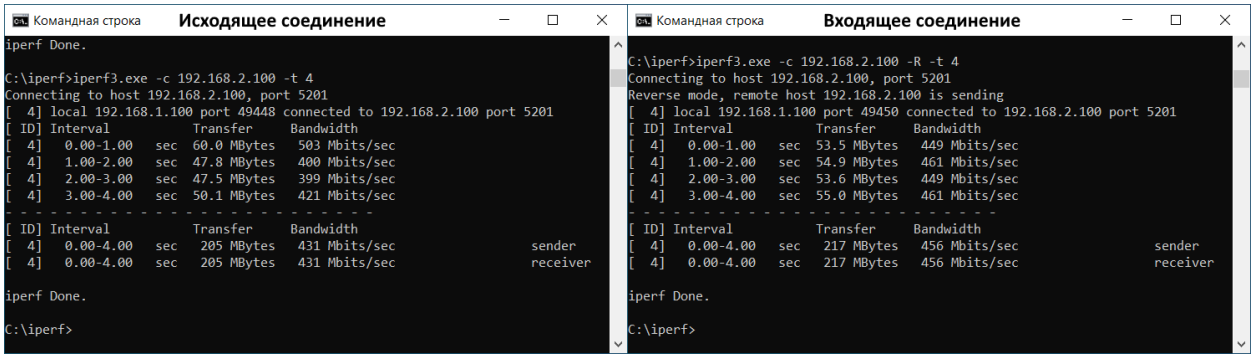


Рисунок – Результат работы утилиты «iperf»

Утилита «iperf» запущена со следующими параметрами:

- в качестве сервера на хосте, находящемся в сети интерфейса «WAN»;

- в режиме измерения пропускной способности на хосте, находящемся в сети интерфейса «LAN».

3.1 Ограничение трафика

Подраздел ограничения трафика (**«Межсетевой экран» - «Ограничение трафика»**) содержит три вкладки (см. Рисунок – Функция «Ограничение трафика»):

- **«Каналы»** – настраиваются ограничения пропускной способности;
- **«Очереди»** – настраивается пропускная способность внутри канала и приоритет пропускной способности определённым приложениям;
- **«Правила»** – задаются правила, согласно которым будут применены ограничения трафика.

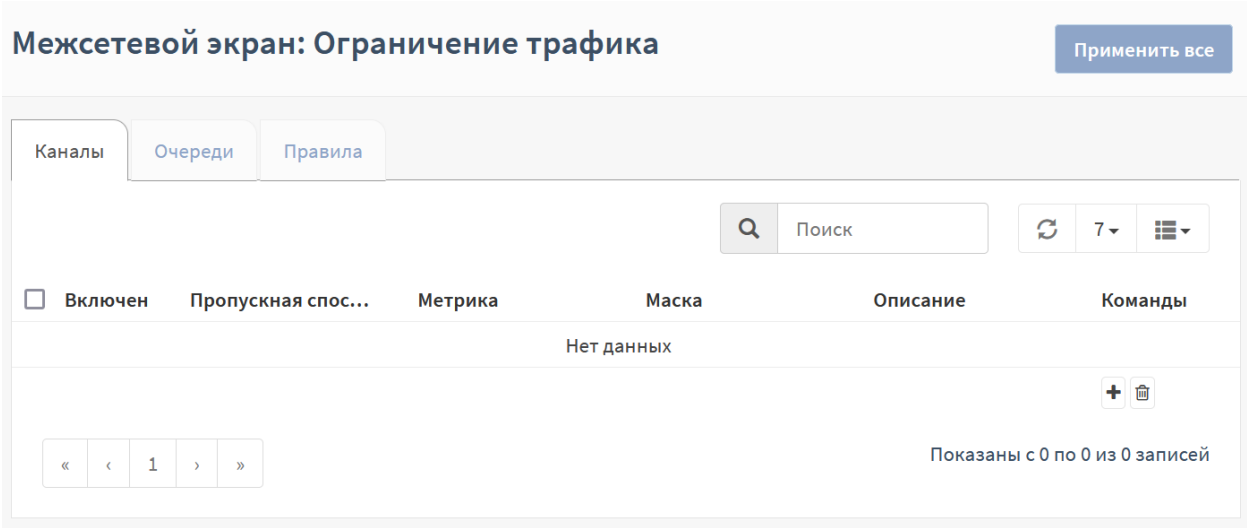


Рисунок – Функция «Ограничение трафика»

3.1.1 Вкладка «Каналы»

Во вкладке настраиваются ограничения пропускной способности.

В данной вкладке необходимо создать два канала со следующими параметрами (см. Таблица «Значения параметров каналов»):

Таблица «Значения параметров каналов»

Параметр	Исходящий канал	Входящий канал
Пропускная способность	1	10
Единицы измерения пропускной способности	Мбит/с	Мбит/с
Описание	1Mbps_UP	10Mbps_Down

Для добавления канала необходимо выполнить следующие действия:

1. Нажать **кнопку** « » в правой части формы.
2. В открывшейся форме (см. Рисунок – Редактирование канала) указать параметры (см. Таблица «Значения параметров каналов»).

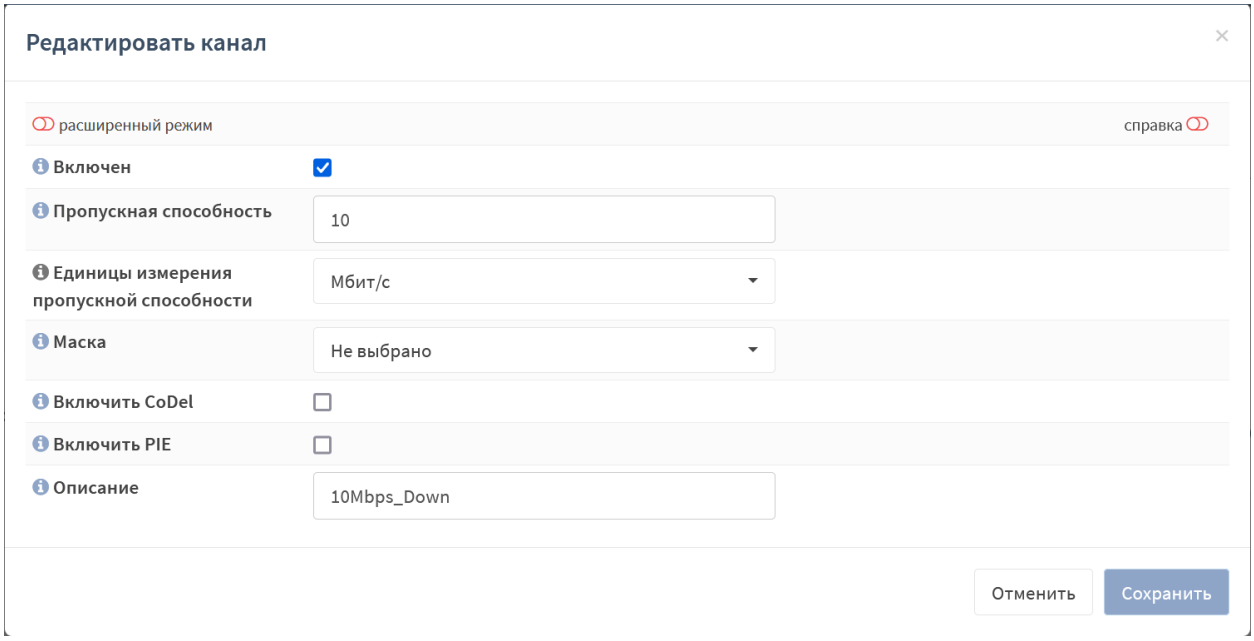


Рисунок – Редактирование канала

3. Нажать **кнопку «Сохранить»**.
4. В результате канал будет добавлен в список (см. Рисунок – Список каналов).

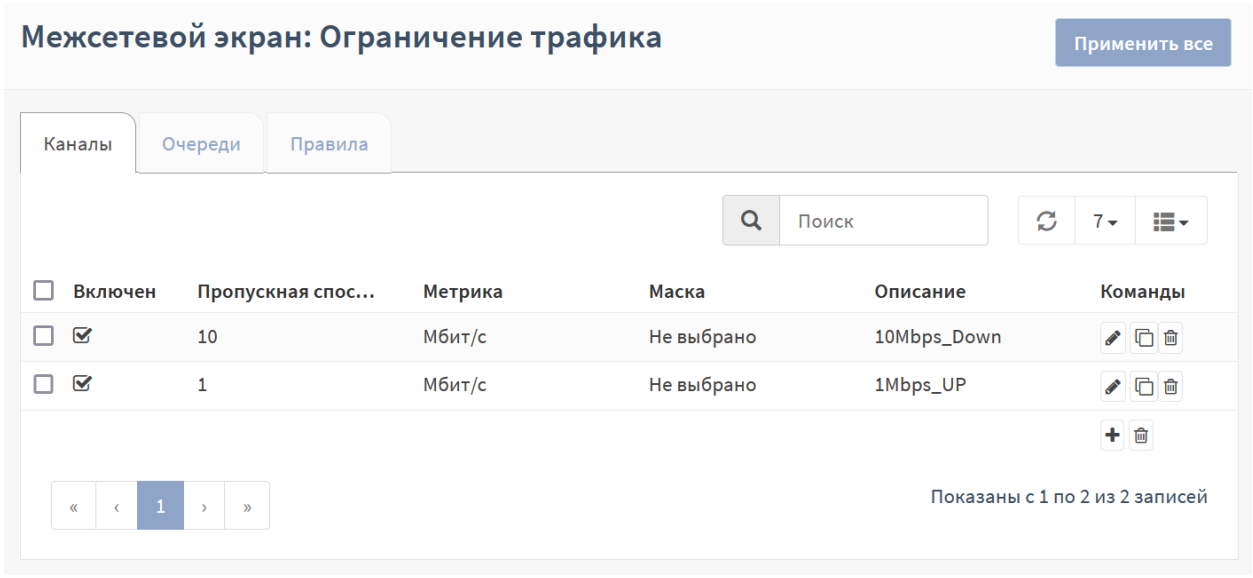


Рисунок – Список каналов

При переключении выключателя **«расширенный режим»** (см. Рисунок – Редактирование канала) в верхней левой части формы будут доступны дополнительные параметры для более тонкой настройки ограничений трафика:

- **«Очередь»**;

- **«Buckets»**;
- **«Тип планировщика»**;
- **«(FQ-)CoDel target»**;
- **«(FQ-)CoDel интервал»**;
- **«(FQ-)CoDel ECN»**;
- **«FQ-CoDel quantum»**;
- **«FQ-CoDel ограничение»**;
- **«FQ-CoDel потоки»**;
- **«Задержка»**.

3.1.2 Вкладка «Очереди»

В данной вкладке необходимо создать две очереди со следующими параметрами (см. Таблица «Значения параметров очереди»):

Таблица «Значения параметров очереди»

Параметр	Исходящий канал	Входящий канал
Канал	1Mbps_UP	10Mbps_Down
Весовой коэффициент	100	100
Описание	Queue_UP	Queue_Down

Для добавления очереди необходимо выполнить следующие действия:

1. Нажать **кнопку** « + » в правой части формы.
2. В открывшейся форме (см. Рисунок – Редактирование очереди) указать параметры (см. Таблица «Значения параметров очереди»).

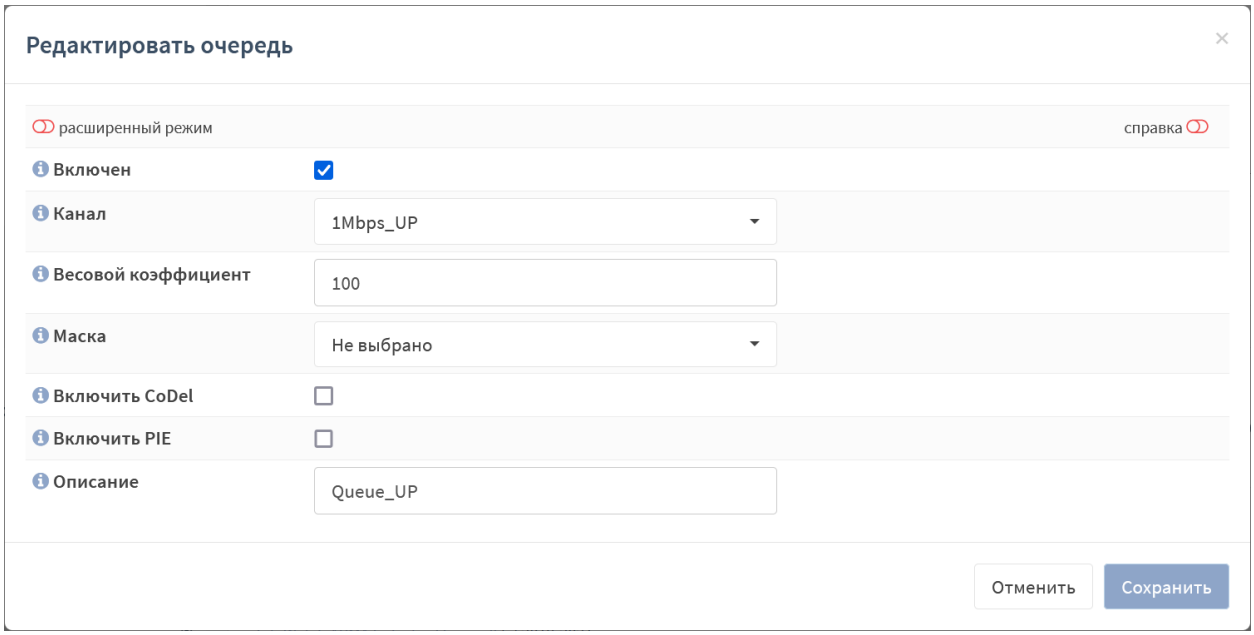


Рисунок – Редактирование очереди

3. Нажать **кнопку «Сохранить»**.
4. В результате очередь будет добавлена в список (см. Рисунок – Список очередей).

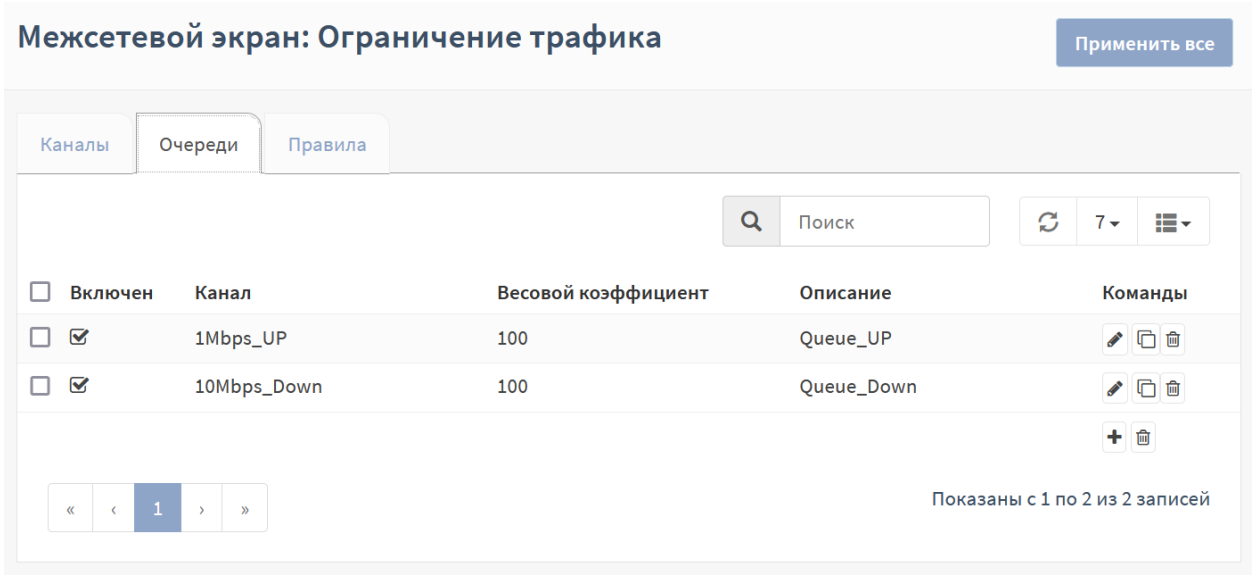


Рисунок – Список очередей

При переключении выключателя **«расширенный режим»** (см. Рисунок – Редактирование очереди) в верхней левой части формы будут доступны дополнительные параметры очереди для более тонкой настройки ограничений трафика:

- **«Очередь»**;
- **«Buckets»**;
- **«Тип планировщика»**;

- **«(FQ-)CoDel target»**;
- **«(FQ-)CoDel интервал»**;
- **«(FQ-)CoDel ECN»**.

3.1.3 Вкладка «Правила»

В данной вкладке необходимо создать два правила со следующими параметрами (см. Таблица «Значения параметров правила»).

Таблица «Значения параметров правила»

Параметр	Исходящий канал	Входящий канал
Интерфейс	WAN	WAN
Протокол	IP	IP
Отправитель	192.168.1.0/24	any
Порт источника	any	any
Получатель	any	192.168.1.0/24
Порт назначения	any	any
Канал/очередь	Queue_UP	Queue_Down
Описание	Upload	Download

Для добавления правила необходимо выполнить следующие действия:

1. Нажать **кнопку** « + » в правой части формы.
2. В открывшейся форме (см. Рисунок – Редактирование правила) указать параметры (см. Таблица «Значения параметров правила»).

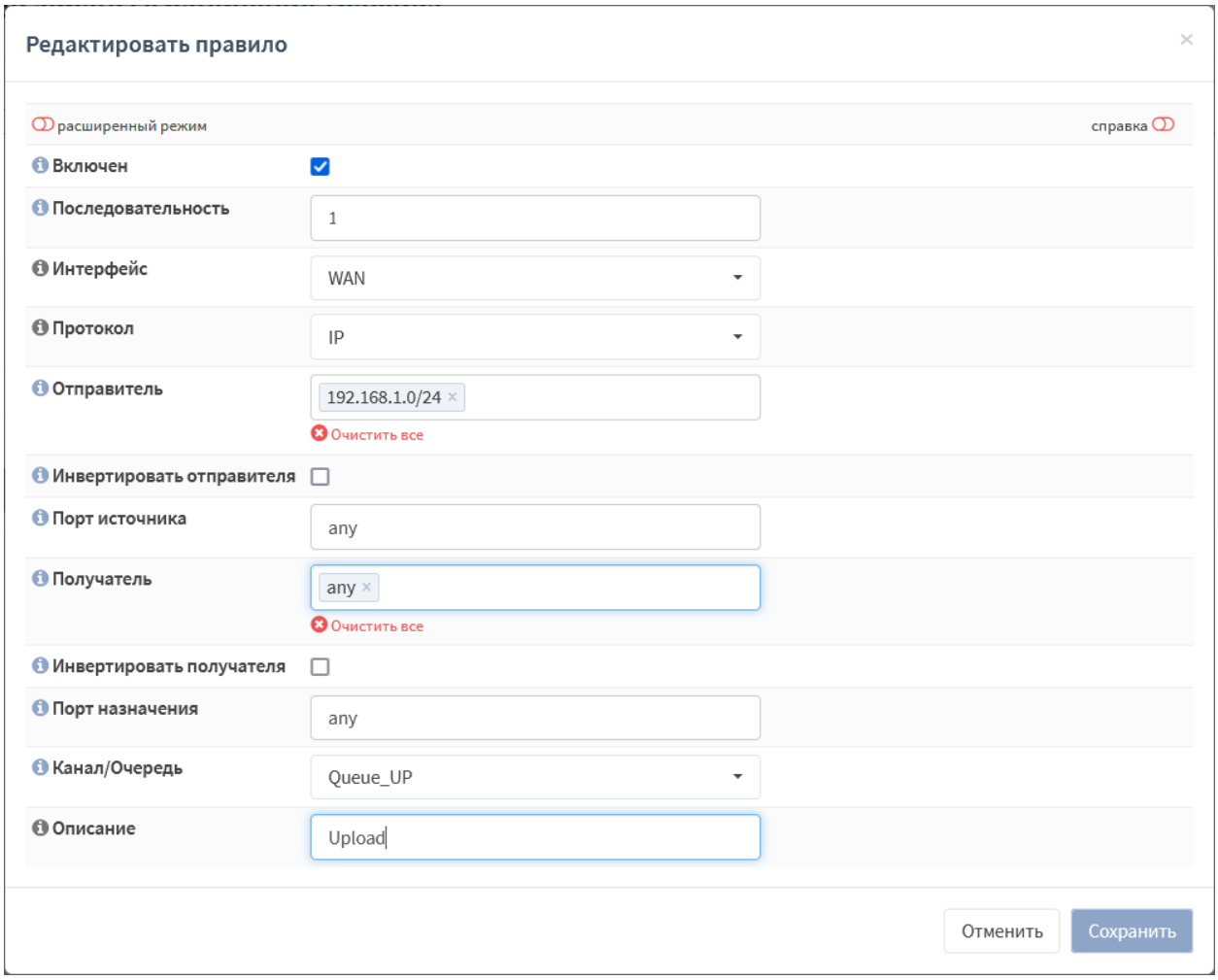


Рисунок – Редактирование правила

3. Нажать **кнопку «Сохранить»**. В результате очередь будет добавлена в список (см. Рисунок – Список правил).

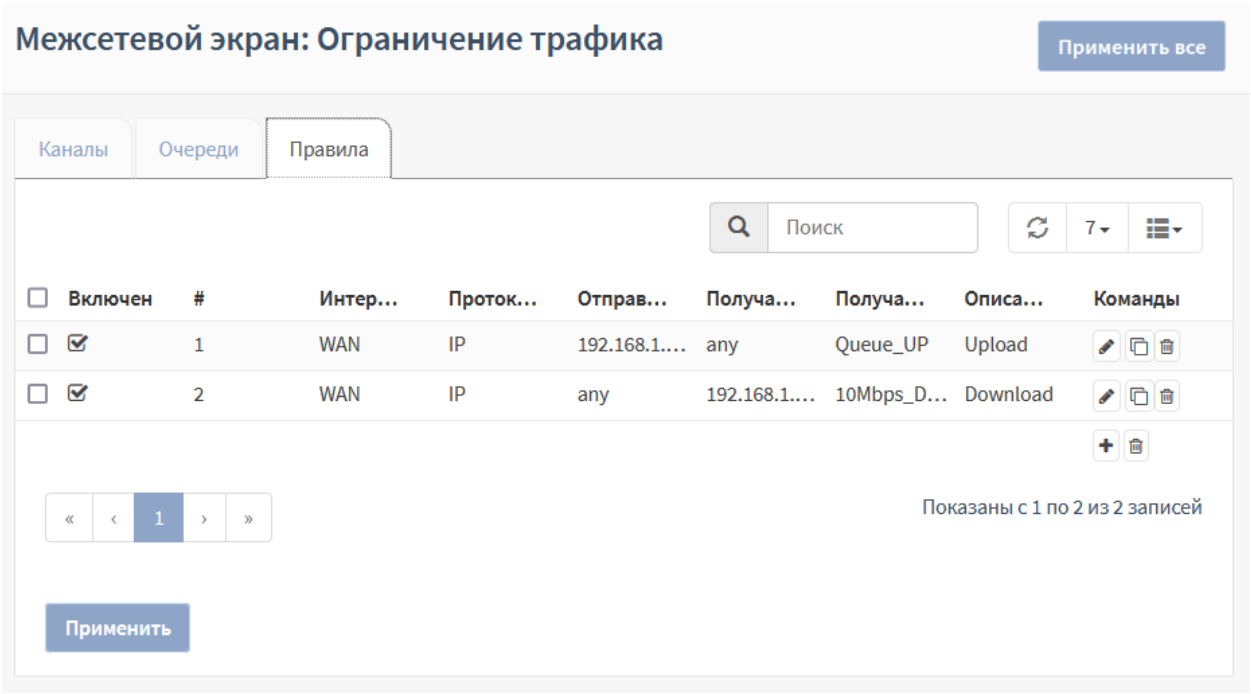


Рисунок – Список правил

4. Нажать **кнопку «Применить все»** для применения ограничений.

При переключении выключателя **«расширенный режим»** (см. Рисунок – Редактирование правила) в верхней левой части формы будут доступны дополнительные параметры правила для более тонкой настройки ограничений трафика:

- **«Интерфейс 2»**;
- **«DSCP»**;
- **«Направление»**.

3.1.4 Проверка ограничения трафика

Для проверки корректности настройки используется утилита командной строки «iperf», не входящая в состав **ARMA FW**.

После настройки и применения ограничений пропускная способность равна 1 Мбит/с и 10 Мбит/с для исходящего и входящего соединений соответственно (см. Рисунок – Результат работы утилиты «iperf»).

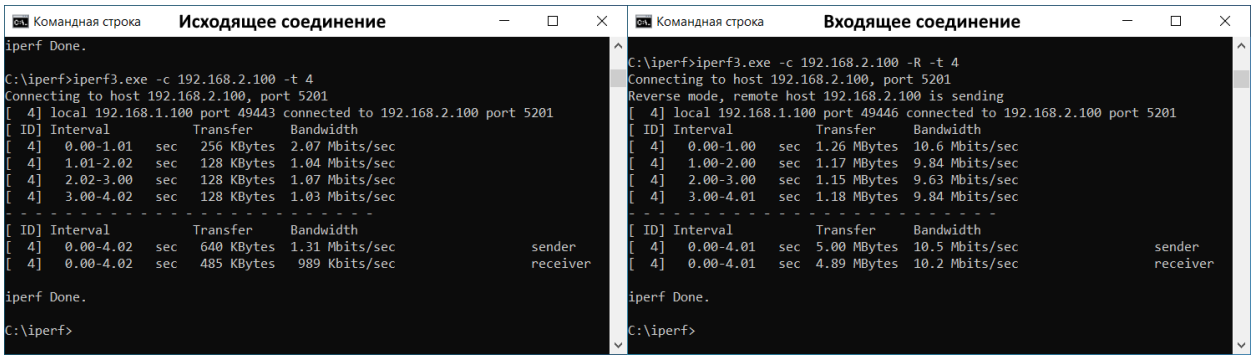


Рисунок – Результат работы утилиты «iperf»

3.2 Статус

В подразделе отображаются настроенные ограничения и результаты их работы (см. Рисунок – Текущие ограничения трафика).

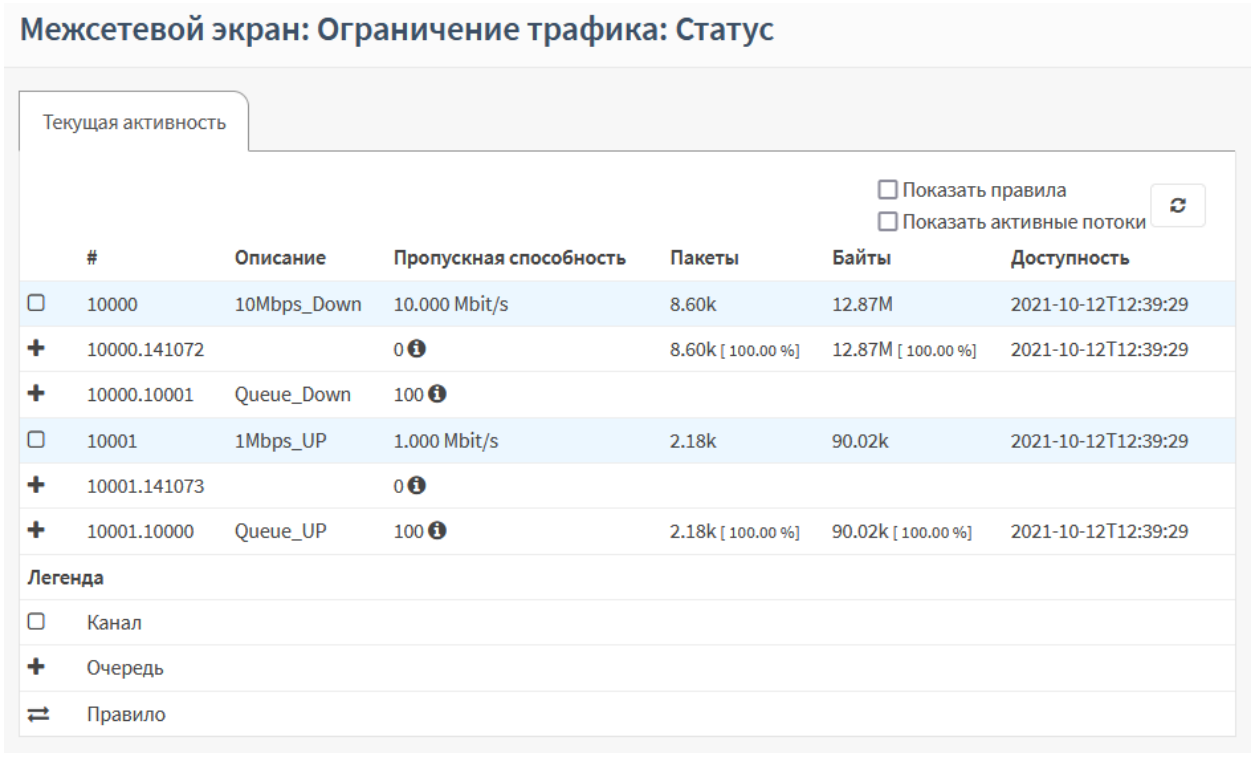


Рисунок – Текущие ограничения трафика

При необходимости отобразить правила или активные потоки требуется установить флажок напротив соответствующего значения в верхней правой части формы.

4 НАСТРОЙКА ОТКАЗОУСТОЙЧИВОГО КЛАСТЕРА

Кластер – это логическое и физическое объединение нескольких объектов со схожими функциями в одну группу с целью повышения эффективности.

В случае объединения двух **ARMA FW** в каждый момент времени только одно устройство **ARMA FW** в кластере обрабатывает весь трафик, такое устройство считается ведущим. Подчинённые, резервные устройства постоянно синхронизируют своё состояние с ведущим устройством. В случае выхода из строя ведущего устройства его подменяет одно из резервных устройств, которое само становится ведущим и начинает обрабатывать трафик. В случае если «старое» ведущее устройство вновь переходит в рабочее состояние, то текущее ведущее устройство возвращается в статус подчинённого резервного устройства.

Примечание:

Для корректной работы отказоустойчивого кластера, версии ведущего и резервного **ARMA FW** должны быть идентичными.

Для настройки работы **ARMA FW** в режиме отказоустойчивого кластера используется схема, представленная на рисунке (см. Рисунок – Схема стенда для настройки режима отказоустойчивого кластера). Оба **ARMA FW** подключены к одним и тем же коммутаторам для обеспечения работы в режиме отказоустойчивого кластера, а также между собой **ARMA FW** соединены сетевым кабелем для обеспечения передачи состояния устройств.

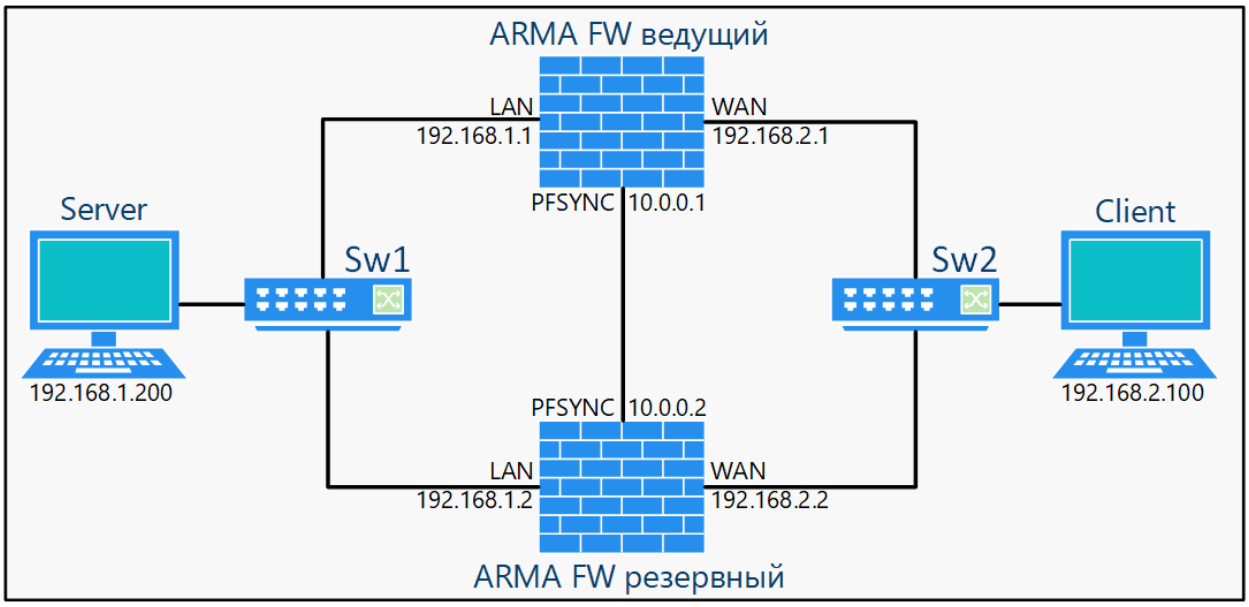


Рисунок – Схема стенда для настройки режима отказоустойчивого кластера

Примечание:

Для корректной работы СОВ с пакетами промышленных протоколов на **ARMA FW**, настроенных в режиме отказоустойчивого кластера,

необходимо перейти в подраздел администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**), на вкладке **«Настройки»** включить переключатель **«расширенный режим»** и установить флажок для параметра **«Режим midstream»**.

Для корректной работы СОВ на **ARMA FW**, настроенных в режиме отказоустойчивого кластера, необходимо предварительно загрузить правила и выполнить настройку СОВ на каждом **ARMA FW**, входящем в состав кластера.

Примечание:

При настройке **ARMA FW** в режиме отказоустойчивого кластера и использовании агрегации каналов необходимо перейти в подраздел параметров **ARMA FW** (**«Система» - «Настройки» - «Параметры»**). Убедиться, что для параметров **«net.inet.carp.senderr_demotion_factor»** и **«net.pfsync.carp_demotion_factor»** установлены значения «0».

Примечание:

В случае необходимости использования VLAN на **ARMA FW**, настроенных в режиме отказоустойчивого кластера, требуется предварительно создать и настроить идентично именованные VLAN-интерфейсы на каждом **ARMA FW**, входящем в состав кластера.

Настройка и проверка работы **ARMA FW** в режиме отказоустойчивого кластера состоит из следующих этапов:

1. Добавить на ведущем устройстве виртуальные IP-адреса для сегментов сети.
2. Настроить режим отказоустойчивого кластера на резервном устройстве.
3. Настроить режим отказоустойчивого кластера на ведущем устройстве.
4. Настроить перезапуск службы «Suricata» на ведущем устройстве (см. Настройка перезапуска службы «Suricata» на ведущем устройстве отказоустойчивого кластера).
5. Выполнить проверку корректной работы устройств.

В примере у каждого экземпляра **ARMA FW** используются три сетевых интерфейса: «LAN», «WAN» и «PFSYNC». Каждый из интерфейсов имеет базовые настройки. В случае использования ВМ необходимо в настройках гипервизора включить режим **«Promiscuous mode»** на виртуальных сетевых интерфейсах для корректной работы кластера.

Сетевым интерфейсам необходимо назначить IP-адреса, указанные в таблице (см. Таблица «IP-адреса для интерфейсов МЭ»). Настройка IP-адресов производится в разделе **«Интерфейсы»** (см. Настройка сетевых интерфейсов).

Таблица «IP-адреса для интерфейсов МЭ»

Интерфейс	Ведущий ARMA FW	Резервный ARMA FW
LAN	192.168.1.1/24	192.168.1.2/24
WAN	192.168.2.1/24	192.168.2.2/24
PFSYNC	10.0.0.1/24	10.0.0.2/24

4.1 Настройка устройств кластера

4.1.1 Добавление виртуальных IP-адресов на ведущем устройстве

Для добавления IP-адресов на ведущем устройстве необходимо выполнить следующие действия:

1. Перейти в подраздел настроек виртуальных адресов (**«Межсетевой экран» - «Виртуальные IP-адреса» - «Настройки»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Форма создания виртуального IP-адреса) указать параметры IP-адреса для LAN-интерфейса и нажать **кнопку «Сохранить»**.
3. Нажать **кнопку «+Добавить»**, указать параметры IP-адреса для WAN-интерфейса, нажать **кнопку «Сохранить»** и **кнопку «Применить изменения»**. Данные для IP-адресов указаны в таблице (см. Таблица «Параметры виртуальных IP-адресов»).

   Примечание:

   В случае, когда **ARMA FW** используется в сети в качестве шлюза по умолчанию, необходимо изменить для клиентов шлюз по умолчанию на созданный виртуальный IP-адрес.

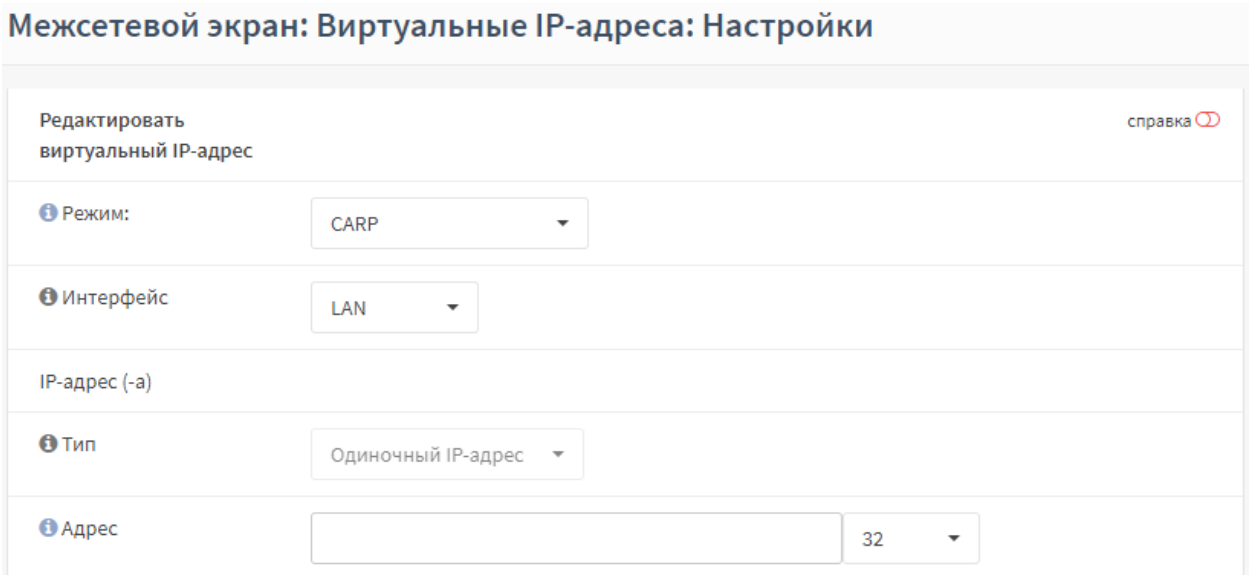


Рисунок – Форма создания виртуального IP-адреса

Таблица «Параметры виртуальных IP-адресов»

Параметр	Значение для IP-адреса для LAN-интерфейса	Значение для IP-адреса для WAN-интерфейса
Режим	CARP	CARP
Интерфейс	LAN	WAN
Адрес	192.168.1.254/24	192.168.2.254/24
[1] Пароль	1234	1234
[2] Группа VHID	1	2
Описание	Виртуальный IP-адрес на LAN стороне	Виртуальный IP-адрес на WAN стороне

4.1.2 Порядок настройки резервного устройства

Для настройки режима работы **ARMA FW** в режиме отказоустойчивого кластера на резервном устройстве необходимо выполнить следующие действия:

1. Перейти в подраздел настроек синхронизации состояния (**«Система» - «Высокий уровень доступности» - «Настройки»**) и включить синхронизацию состояния, установив флажок в параметре **«Синхронизировать состояния»** (см. Рисунок – Настройка синхронизации).

[1] Значение параметра **«Пароль»** указано в качестве примера.

[2] Параметр **«Группа VHID»** должен отличаться для каждого интерфейса.

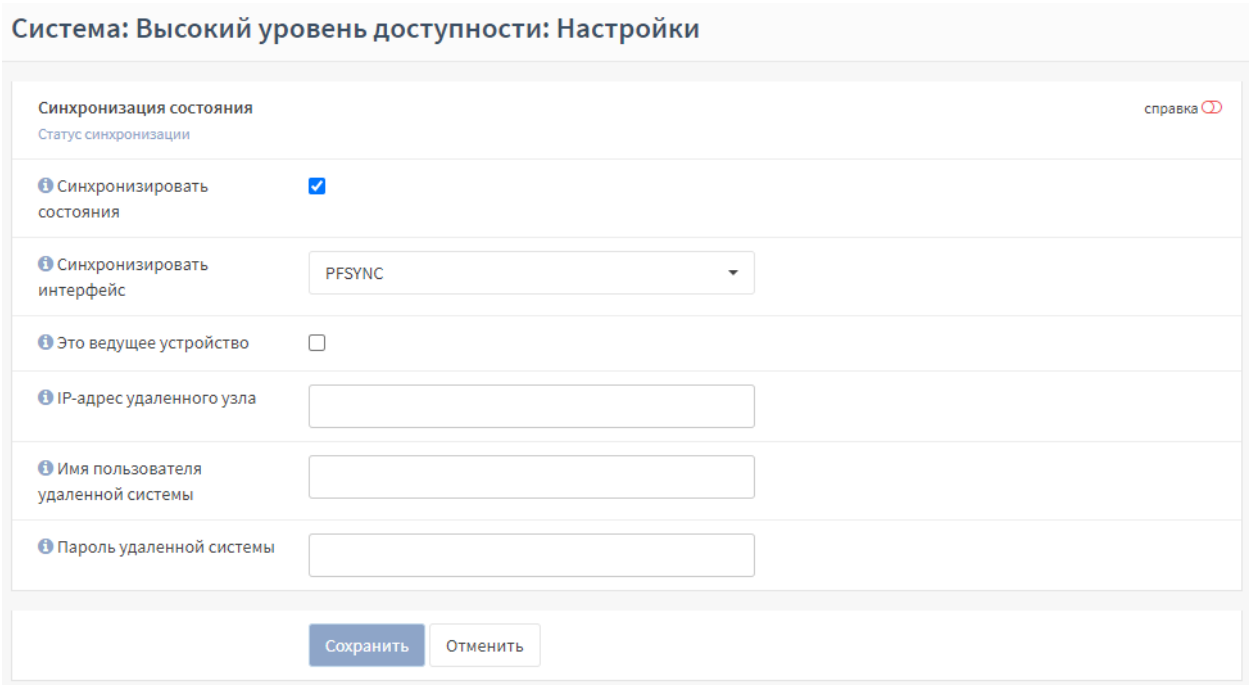


Рисунок – Настройка синхронизации

2. Указать интерфейс синхронизации – **«PFSYNC»**.
3. Указать данные резервного устройства:
   - **«IP-адрес удаленного узла»** – «10.0.0.1»;
   - **«Имя пользователя удаленной системы»** – «root», значение по умолчанию;
   - **«Пароль удаленной системы»** – «root», значение по умолчанию.
4. Нажать **кнопку «Сохранить»**.

4.1.3 Порядок настройки ведущего устройства

Для настройки режима работы **ARMA FW** в режиме отказоустойчивого кластера на ведущем устройстве необходимо выполнить следующие действия:

1. Перейти в подраздел настроек синхронизации состояния (**«Система» - «Высокий уровень доступности» - «Настройки»**) и включить синхронизацию состояния, установив флажок в параметре **«Синхронизировать состояния»** (см. Рисунок – Настройка синхронизации).
2. Указать интерфейс синхронизации – **«PFSYNC»** и установить флажок в параметре **«Это ведущее устройство»**.
3. Указать данные резервного устройства:
   - **«IP-адрес удаленного узла»** – «10.0.0.2»;
   - **«Имя пользователя удаленной системы»** – «root», значение по умолчанию;

- **«Пароль удаленной системы»** – «root», значение по умолчанию.

4. Нажать **кнопку «Сохранить»**.

После применения изменений в подразделе настроек виртуальных адресов на резервном устройстве (**«Межсетевой экран» - «Виртуальные IP-адреса» - «Настройки»**) появятся виртуальные IP-адреса, созданные на ведущем устройстве (см. Рисунок – Синхронизированные виртуальные IP-адреса).

Рисунок – Синхронизированные виртуальные IP-адреса

Примечание:

В случае необходимости переключения шлюза по умолчанию, следует в подразделе общих настроек ведущего **ARMA FW** (**«Система» - «Настройки» - «Общие настройки»**) установить флажок напротив параметра **«Переключение шлюзов»**.

4.2 Проверка работы отказоустойчивого кластера

Статус работы кластера отображается в подразделе статуса виртуальных IP-адресов (**«Межсетевой экран» - «Виртуальные IP-адреса» - «Статус»**) (см. Рисунок – Статус работы кластера на ведущем устройстве и Рисунок – Статус работы кластера на резервном устройстве).

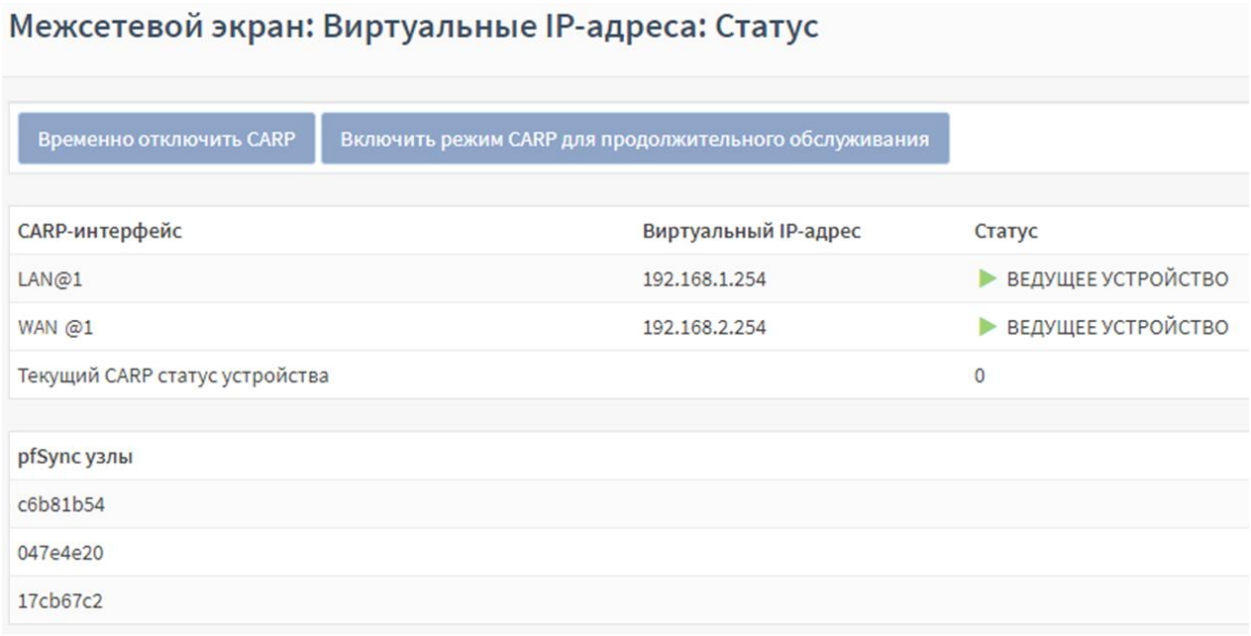


Рисунок – Статус работы кластера на ведущем устройстве

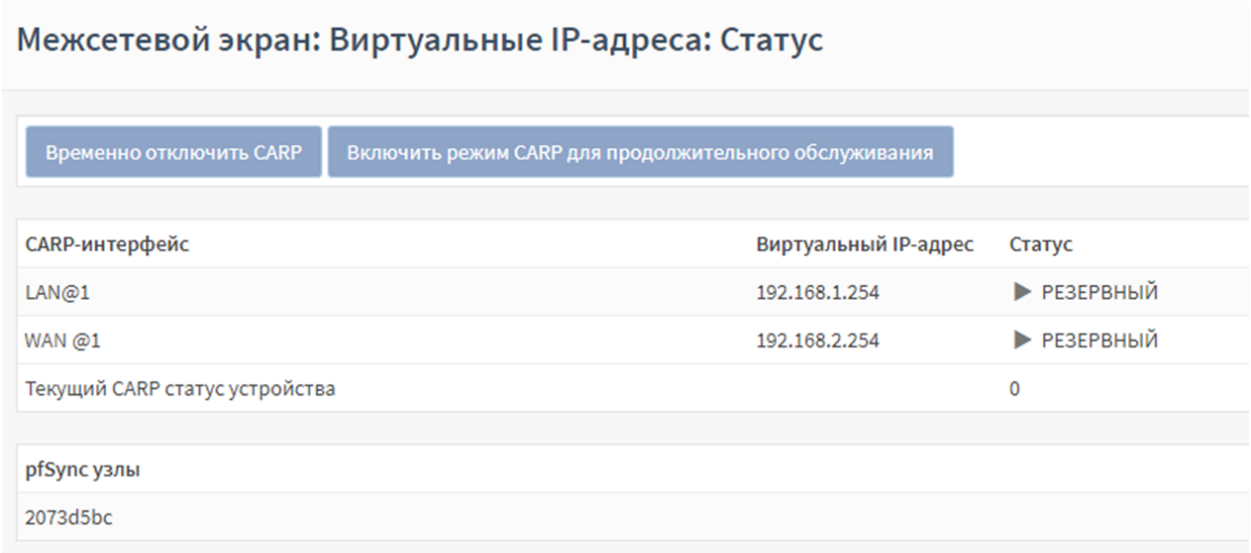


Рисунок – Статус работы кластера на резервном устройстве

Проверка режима отказоустойчивого кластера считается успешно пройденной, когда после выключения ведущего устройства, значение статуса работы кластера резервного устройства изменится с **«РЕЗЕРВНЫЙ»** на **«ВЕДУЩЕЕ УСТРОЙСТВО»**.

При переключении устройства возможен обрыв соединения продолжительностью примерно одна секунда.

Примечание:

В случае отключения интерфейса ведущего устройства путём снятия флажка в параметре **«Включен»** подраздела настройки интерфейса (**«Интерфейсы» - «[Название интерфейса]»**) (например, **«[WAN]»**) переключение устройств не произойдёт.

4.3 Синхронизация состояний

ARMA FW поддерживает возможность синхронизации состояний.

Настройка синхронизации состояний **ARMA FW** выполняется аналогично настройке **ARMA FW** в составе отказоустойчивого кластера, учитывая следующие особенности:

- не требуется настройка виртуальных IP-адресов;
- в подразделе настроек синхронизации состояния (**«Система» - «Высокий уровень доступности» - «Настройки»**) следует оставить пустыми поля для параметров **«IP-адрес удаленного узла»**, **«Имя пользователя удаленной системы»**, **«Пароль удаленной системы»**;
- не требуется перезапуск службы «Suricata» на ведущем устройстве.

4.3.1 Проверка синхронизации состояний

Для проверки необходимо на резервном **ARMA FW** перейти в подраздел снимка состояний (**«Межсетевой экран» - «Диагностика» - «Снимок состояний»**) и убедиться в наличии синхронизации сессии ПК **«Server»** с ведущим **ARMA FW** (см. Рисунок – Снимок состояний).

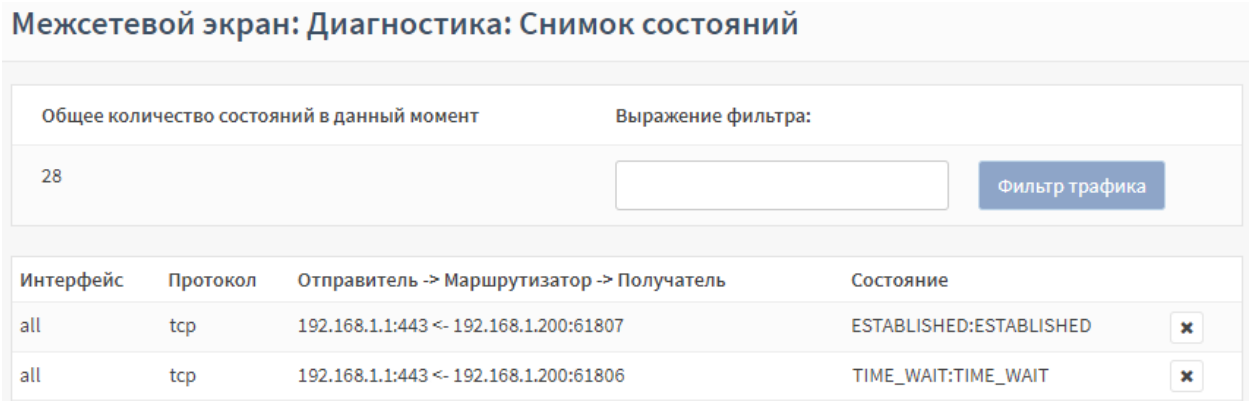


Рисунок – Снимок состояний

5 СИСТЕМА ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

Функциональность системы обнаружения и предотвращения вторжений в **ARMA FW** 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 FW** позволяет решать следующие задачи:

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

Примечание:

Фильтрация трафика производится только при включённом режиме СПВ. При выключенном режиме СПВ производятся только уведомления о срабатывании правил СОВ.

Правила СОВ отображаются во вкладке **«Правила»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**).

Правила обрабатываются в порядке, зависящем от действия над пакетом трафика:

1. **«Pass»** – разрешить движение пакета;
2. **«Drop»** – отбросить пакет;
3. **«Reject»** – отклонить пакет;
4. **«Alert»** – уведомить о пакете.

5.1 Основные настройки СОВ

Перед использованием СОВ необходимо убедиться, что отключён режим «Hardware Offloading». Для выключения данного режима необходимо перейти в подраздел настройки интерфейсов (**«Интерфейсы» - «Настройки»**), установить флажки напротив параметров:

- **«CRC аппаратного обеспечения»**;

- **«TSO аппаратного обеспечения»**;
- **«LRO аппаратного обеспечения»**;

и нажать **кнопку «Сохранить»** внизу страницы (см. Рисунок – Отключение режима Hardware Offloading).

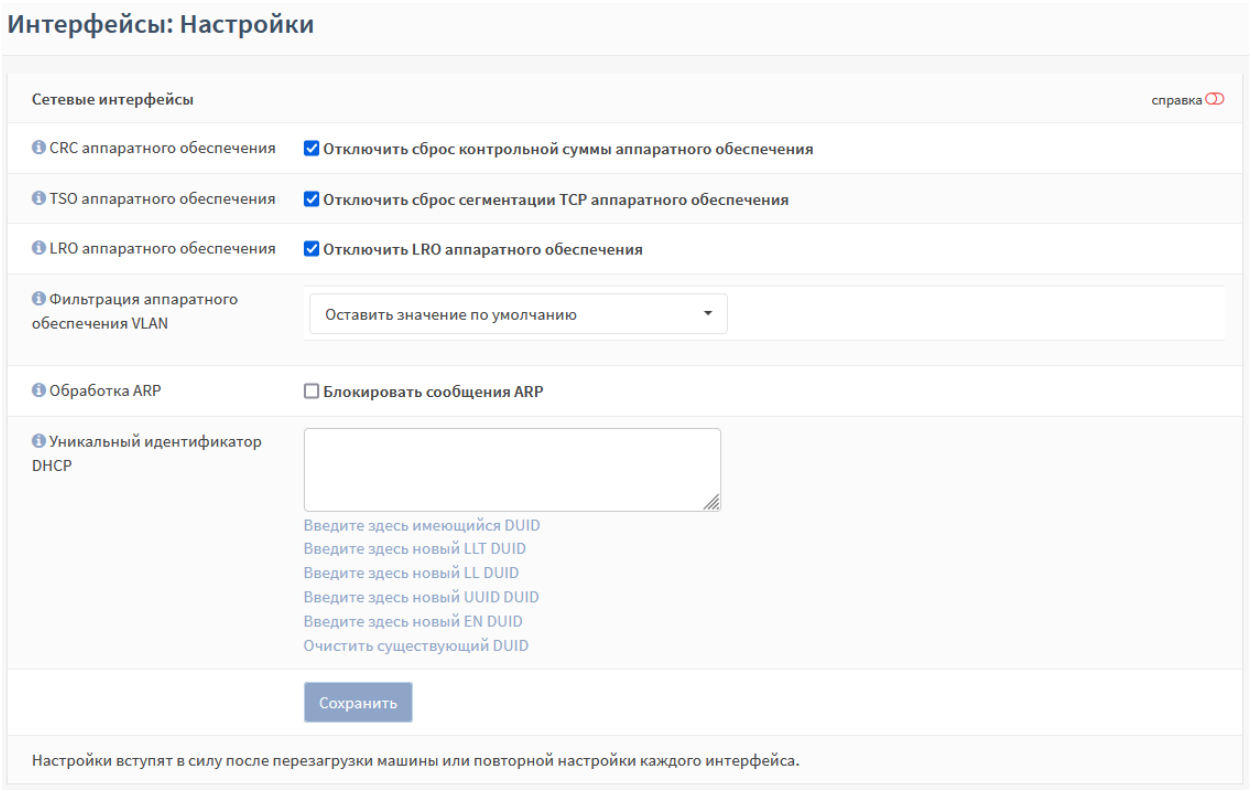


Рисунок – Отключение режима Hardware Offloading

Для включения СОВ необходимо выполнить следующие действия:

1. Перейти в подраздел администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**) и на вкладке **«Настройки»** установить флажок для параметра **«Включен»** (см. Рисунок – Включение СОВ).
2. Выбрать все интерфейсы, которые необходимо будет защищать в параметре **«Интерфейсы»**.
3. Включить переключатель **«расширенный режим»**, указать значения используемых локальных сетей в поле **«Домашние сети ($HOME_NET)»** и нажать **кнопку «Применить»**.

   Примечание:

   Для включения режима СПВ необходимо установить флажок для параметра **«Режим IPS»**.

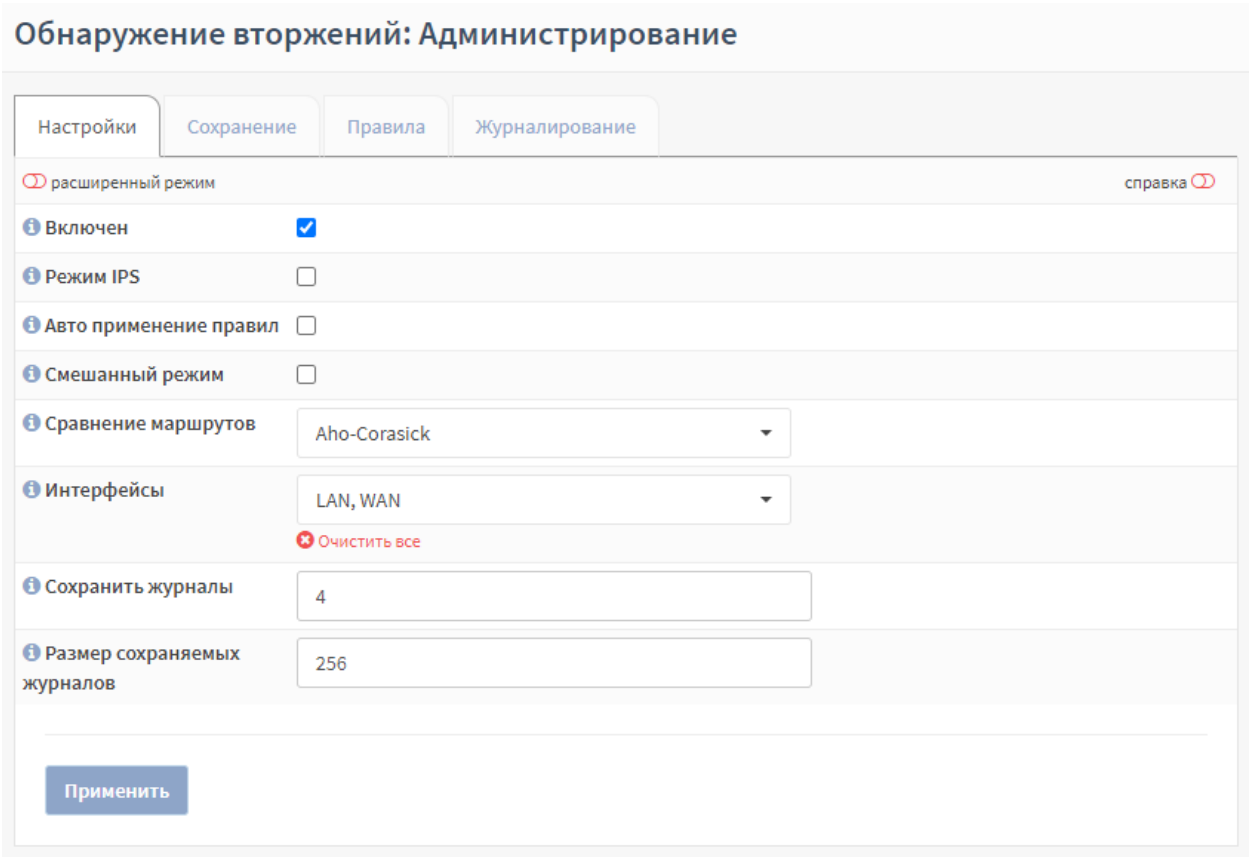


Рисунок – Включение СОВ

После включения СОВ возможно просмотреть пакеты трафика, прошедшие через **ARMA FW** (см. Анализ дампа трафика).

Работу СОВ возможно проверить, настроив правило из раздела Создание правила СОВ настоящего руководства.

5.1.1 Дополнительные настройки СОВ

Часть дополнительных параметров доступна при включённом переключателе **«расширенный режим»**.

Параметр **«Авто применение правил»** – включает автоматическое применение правил после их изменения.

Параметр **«Смешанный режим»** включает режим неразборчивого захвата – «Promiscuous Mode», например, при использовании СОВ на конфигурации с VLAN.

В параметре **«Сравнение маршрутов»** выбирается один из алгоритмов поиска подстроки при обработке пакетов:

- **«Aho-Corasick»** – алгоритм сопоставления «со словарём», находящий подстроки из «словаря» в пакетах. Используется по умолчанию;
- **«Hyperscan»** – высокопроизводительная библиотека сопоставления регулярных выражений от корпорации «Intel».

В параметрах **«Домашние сети ($HOME_NET)»** и **«Внешние сети ($EXTERNAL_NET)»** задаются диапазоны адресов домашней сети и не относящихся к домашней сети соответственно.

В параметрах **«HTTP Сервера ($HTTP_SERVERS)»**, **«SMTP Сервера ($SMTP_SERVERS)»**, **«SQL Сервера ($SQL_SERVERS)»**, **«DNS Сервера ($DNS_SERVERS)»**, **«Telnet Сервера ($TELNET_SERVERS)»**, **«DC Сервера ($DC_SERVERS)»**, **«DNP3 Сервера ($DNP3_SERVER)»**, **«DNP3 Клиенты ($DNP3_CLIENT)»**, **«Modbus Клиенты ($MODBUS_CLIENT)»**, **«Modbus Серверы ($MODBUS_SERVER)»**, **«EnIP Client ($ENIP_CLIENT)»**, **«EnIP Серверы»** задаются адреса устройств, передающих пакеты по соответствующим протоколам.

В параметрах **«HTTP Порты ($HTTP_PORTS)»**, **«Oracle Порты ($ORACLE_PORTS)»**, **«SSH Порты ($SSH_PORTS)»**, **«DNP3 Порты ($DNP3_PORTS)»**, **«Modbus Порты ($MODBUS_PORTS)»**, **«Порты Файловых Данных ($FILE_DATA_PORTS)»**, **«FTP Порты ($FTP_PORTS)»** задаются порты, обрабатывающие трафик по соответствующим протоколам.

В параметре **«Shell Code Порты ($SHELLCODE_PORTS)»** задаются порты, трафик с которых необходимо проверить на наличие двоичного исполняемого кода.

> **Примечание:**
>
> Указание широкого диапазона портов в поле параметра **«Shell Code Порты ($SHELLCODE_PORTS)»** может снижать производительность системы.

Параметр **«Размер пакета по умолчанию»** – задаёт размер сетевых пакетов по умолчанию.

Параметры **«Сохранить журналы»**, **«Размер сохраняемых журналов»** отвечают за ведение журнала работы СОВ. В поле параметра **«Сохранить журналы»** указывается значение, не превышающее «1000». По умолчанию используется значение «4». В поле параметра **«Размер сохраняемых журналов»** указывается значение в диапазоне от «8» до «512» Мбайт. По умолчанию используется значение «256» Мбайт.

Параметры **«Содержимое пакета для журнала»** и **«Журналировать пакет»** отвечают за полноту информации о трафике, содержащейся в журнале работы СОВ.

Параметр **«Режим midstream»** отвечает за детектирование на уровне приложения в середине TCP-потока без предварительного обнаружения «трёхсторонних рукопожатий».

В параметрах **«Уровень приложения: Modbus порт(-ы)»**, **«Уровень приложения: DNP3 порт(-ы)»**, **«Уровень приложения: TPKT порт(-ы)»**, **«Уровень приложения: OPC UA порт(-ы)»**, **«Уровень приложения: IEC104 порт(-ы)»**,

«Уровень приложения: ADS порт(-ы)», **«Уровень приложения: ENIP/CIP порт(-ы)»** и **«Уровень приложения: Fanuc FOCAS порт(-ы)»** задаются значения портов, на которых производится детектирование соответствующих протоколов.

5.2 Загрузка и включение наборов правил

Во вкладке **«Сохранение»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**) (см. Рисунок – Настройка импорта правил) возможны следующие действия с локальными наборами правил:

- **«Включить выбранные»** – включение набора правил;
- **«Включить (фильтр отбрасывания)»** – включение набора правил с применением отбрасывания пакета;
- **«Включить (без фильтра действия)»** – включение набора правил применением действий по умолчанию;
- **«Отключить выбранные»** – отключение набора правил без изменения порядка обработки пакетов;
- **«Удалить выбранные»** – удаление набора и правил его составляющих;
- **«Загрузить новый локальный набор правил»** – импорт файла с правилами.

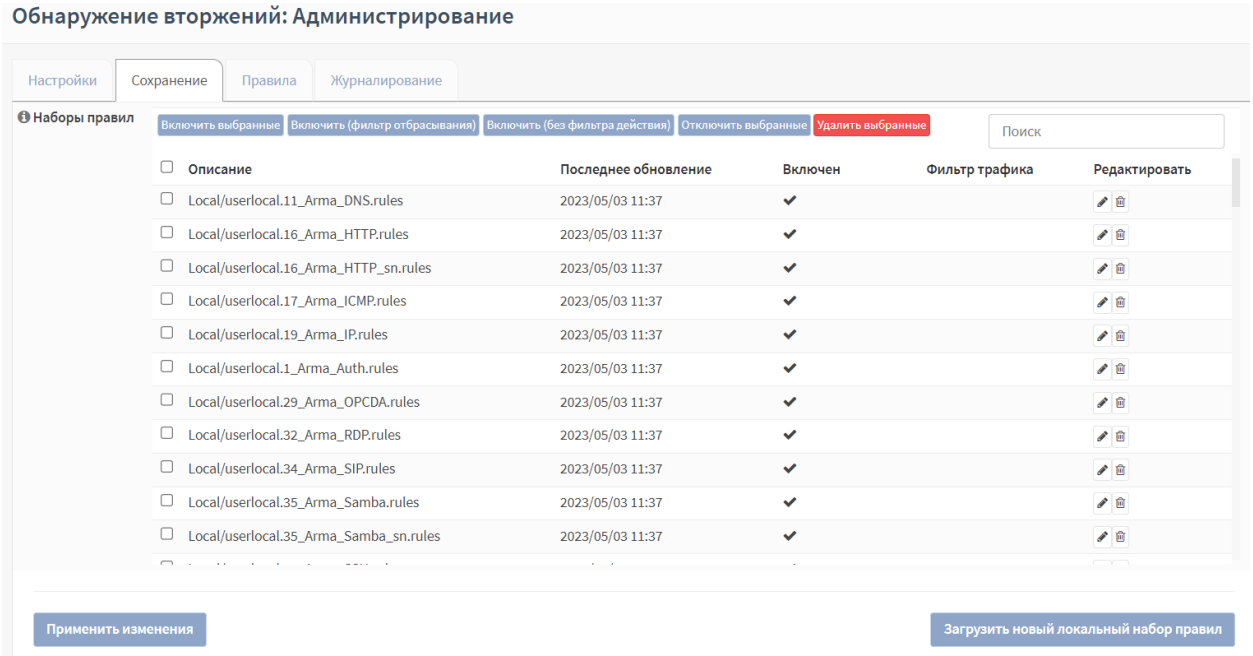


Рисунок – Настройка импорта правил

Примечание:

В случае сброса **ARMA FW** к значениям по умолчанию, загруженные ранее правила сохраняются.

При удалении наборов правил СОВ **кнопка «Применить изменения»** становится неактивной на период выполнения процесса удаления.

Возможна настройка автоматического обновления и перезагрузки правил СОВ с помощью планировщика задач Cron (см. Cron). При создании задачи необходимо выбрать **«Обновить и перезагрузить правила обнаружения вторжений»** в параметре **«Команда»**.

Примечание:

В случае работы СОВ в режиме СПВ, при выполнении расписания автоматического обновления и перезагрузки правил обнаружения вторжений, возможен временный разрыв соединений.

5.2.1 Обновление правил СОВ с внешнего сервера

ARMA FW поддерживает возможность обновления правил СОВ с внешнего сервера.

Примечание:

В случае предварительного удаления набора правил СОВ и последующего обновления правил, удалённый набор не появится в списке наборов правил, отображаемом во вкладке **«Сохранение»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**).

При необходимости импорт набора правил СОВ следует выполнять посредством **кнопки «Загрузить новый локальный набор правил»**.

Для обновления правил СОВ с внешнего сервера необходимо выполнить следующие действия:

1. Перейти во вкладку **«Настройки»** подраздела настроек обновления (**«Система» - «Прошивка» - «Обновления»**), ввести значения в полях параметров **«Имя пользователя»** и **«Пароль»**, предоставляемые вендором, и нажать **кнопку «Сохранить»**.
2. Перейти во вкладку **«СОВ»** и нажать **кнопку «Проверить наличие обновлений»** (см. Рисунок – Проверка наличия обновлений).

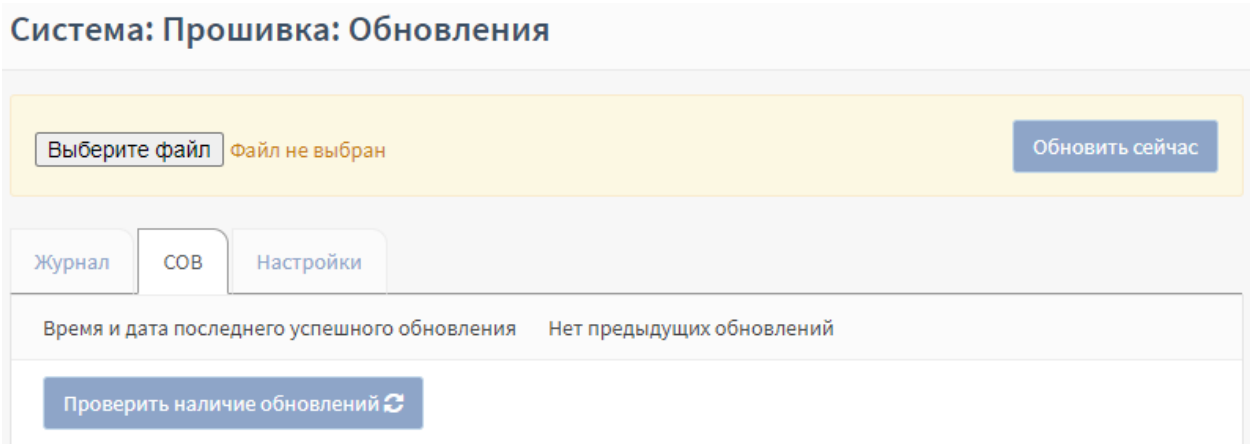


Рисунок – Проверка наличия обновлений

3. Нажать **кнопку «Обновить»** в случае появления окна с сообщением о найденных доступных обновлениях (см. Рисунок – Найдены доступные обновления).

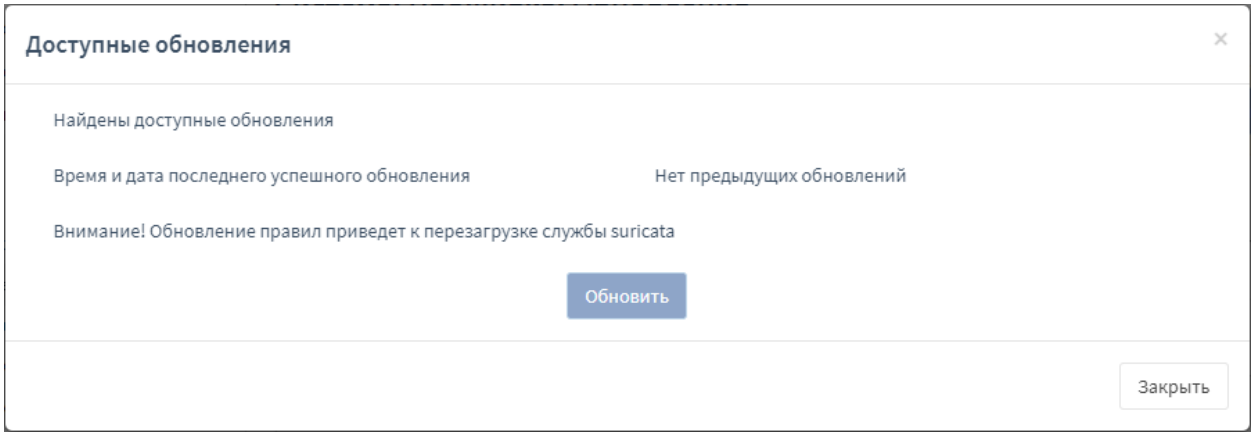


Рисунок – Найдены доступные обновления

4. Дождаться окончания процесса обновления, после которого будет отображена информация о дате и времени загрузки правил.

Загруженные правила будут отображены в списке во вкладке **«Правила»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**).

Возможна настройка автоматической проверки наличия обновления с помощью планировщика задач Cron (см. Cron). При создании задачи необходимо выбрать **«Проверить обновления правил suricata»** в параметре **«Команда»**. После результативного выполнения задачи планировщиком, при наличии доступного обновления будет выведено соответствующее уведомление.

5.2.2 Пример импорта пользовательских решающих правил

Обновление базы правил может осуществляться путём импорта файла с правилами в формате «Suricata» с помощью веб-интерфейса.

В качестве примера будет использован файл набора правил «scan.rules», содержащий в себе правило, рассчитанное на обнаружение сетевого сканирования.

Для импорта пользовательских решающих правил необходимо выполнить следующие действия:

1. Во вкладке **«Сохранение»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**) нажать **кнопку «Загрузить новый локальный набор правил»**, в открывшейся форме выбрать файл «scan.rules» и нажать **кнопку «Открыть»**.
2. После успешной загрузки правил (см. Рисунок – Успешный импорт правил) необходимо нажать **кнопку «Закрыть»**, а затем **кнопку «Скачать и обновить правила»** чтобы изменения вступили в силу.

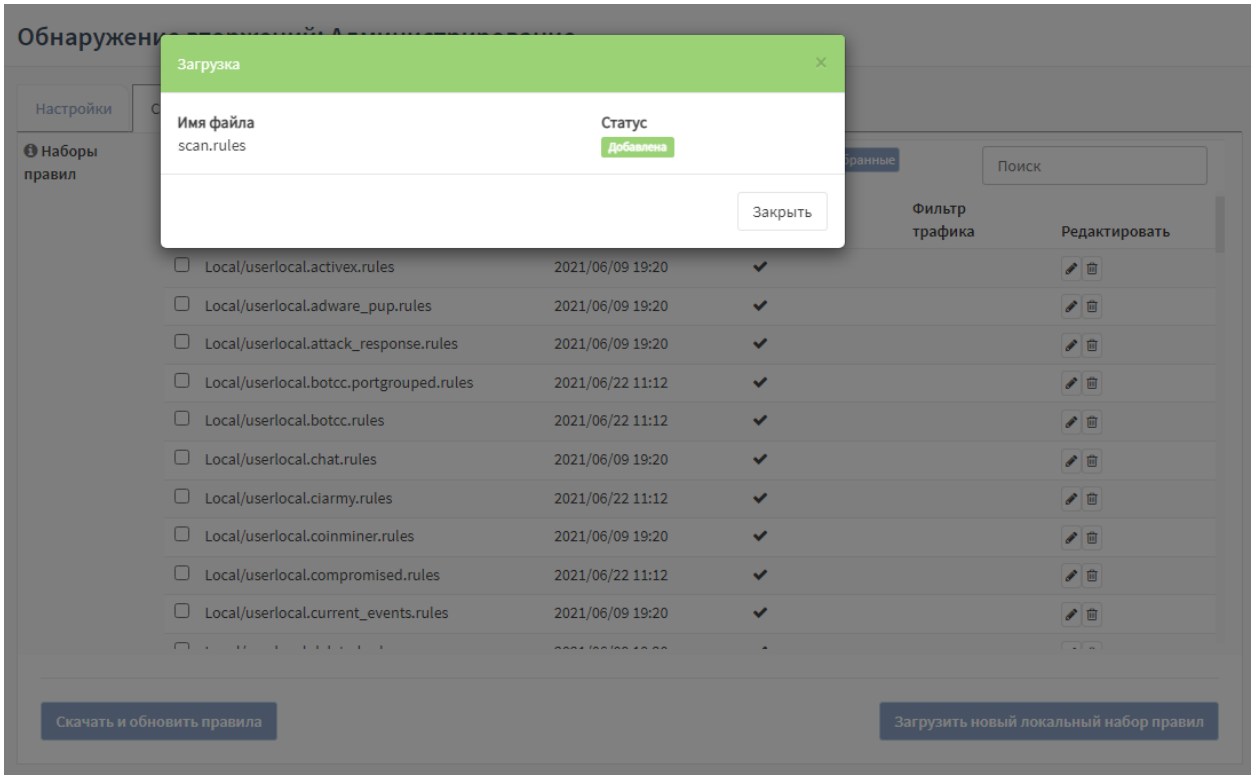


Рисунок – Успешный импорт правил

3. Перейти во вкладку **«Правила»**, ввести в строку поиска **«NMAP –sS»**, установить флажок справа от **кнопки** « » для включения правил (см. Рисунок – Включение правил) и нажать **кнопку «Применить»**.

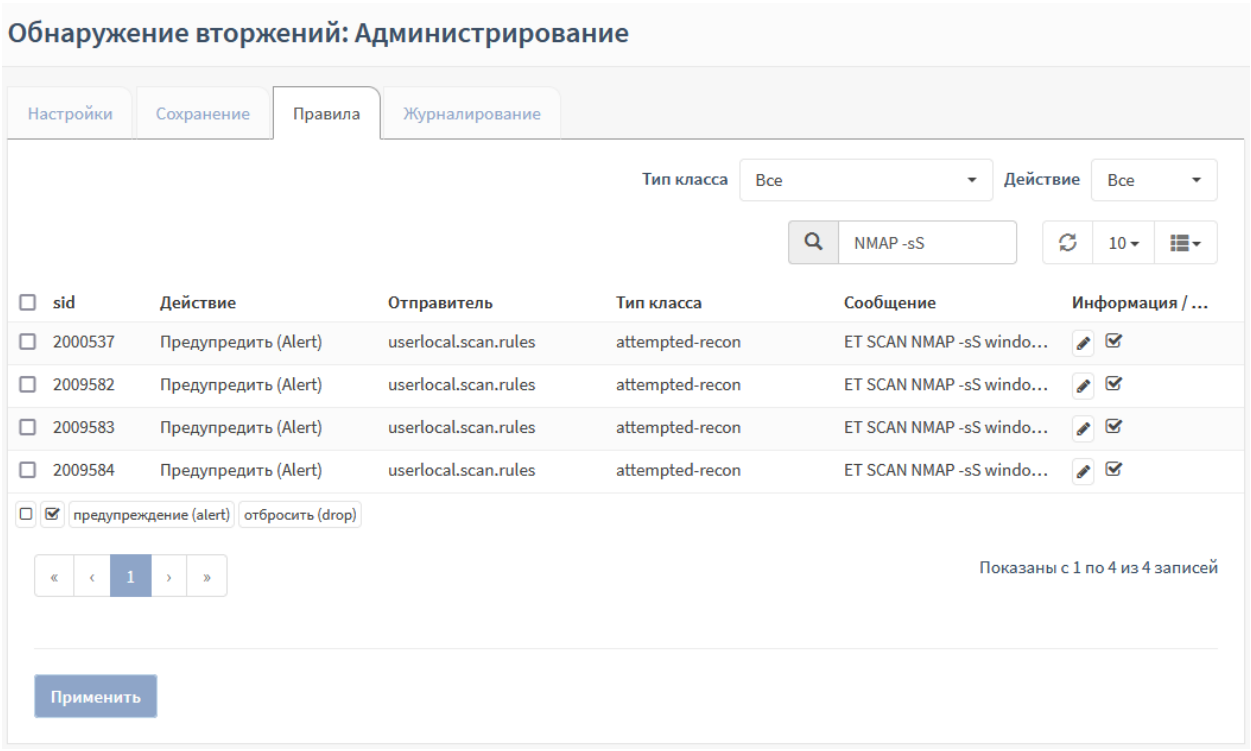


Рисунок – Включение правил

5.2.3 Проверка загруженного набора правил

Для проверки срабатывания правил СОВ используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для проверки срабатывания правил СОВ). На ПК **«Server»** установлено ПО «Zenmap».

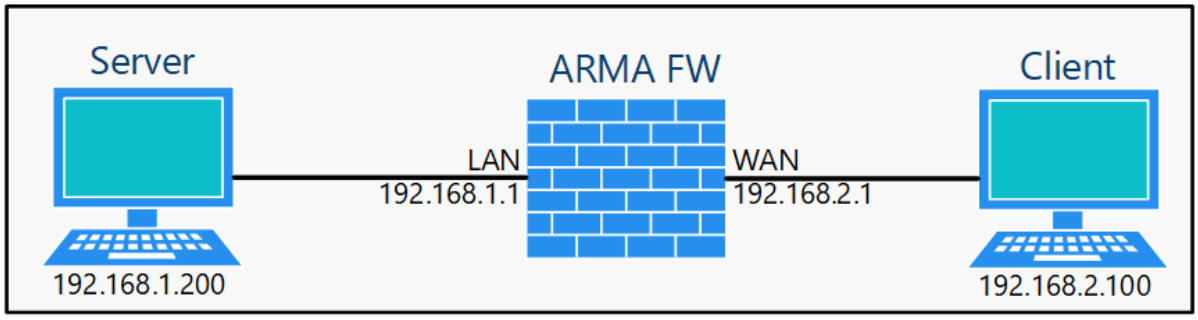


Рисунок – Схема стенда для проверки срабатывания правил СОВ

Порядок проверки срабатывания загруженного набора правил:

1. В ПО «Zenmap» в поле **«Команда»** ввести строку **«nmap -sS 192.168.2.100»** и нажать **кнопку «Сканирование»** (см. Рисунок – Запуск сканирования с помощью программы Zenmap).

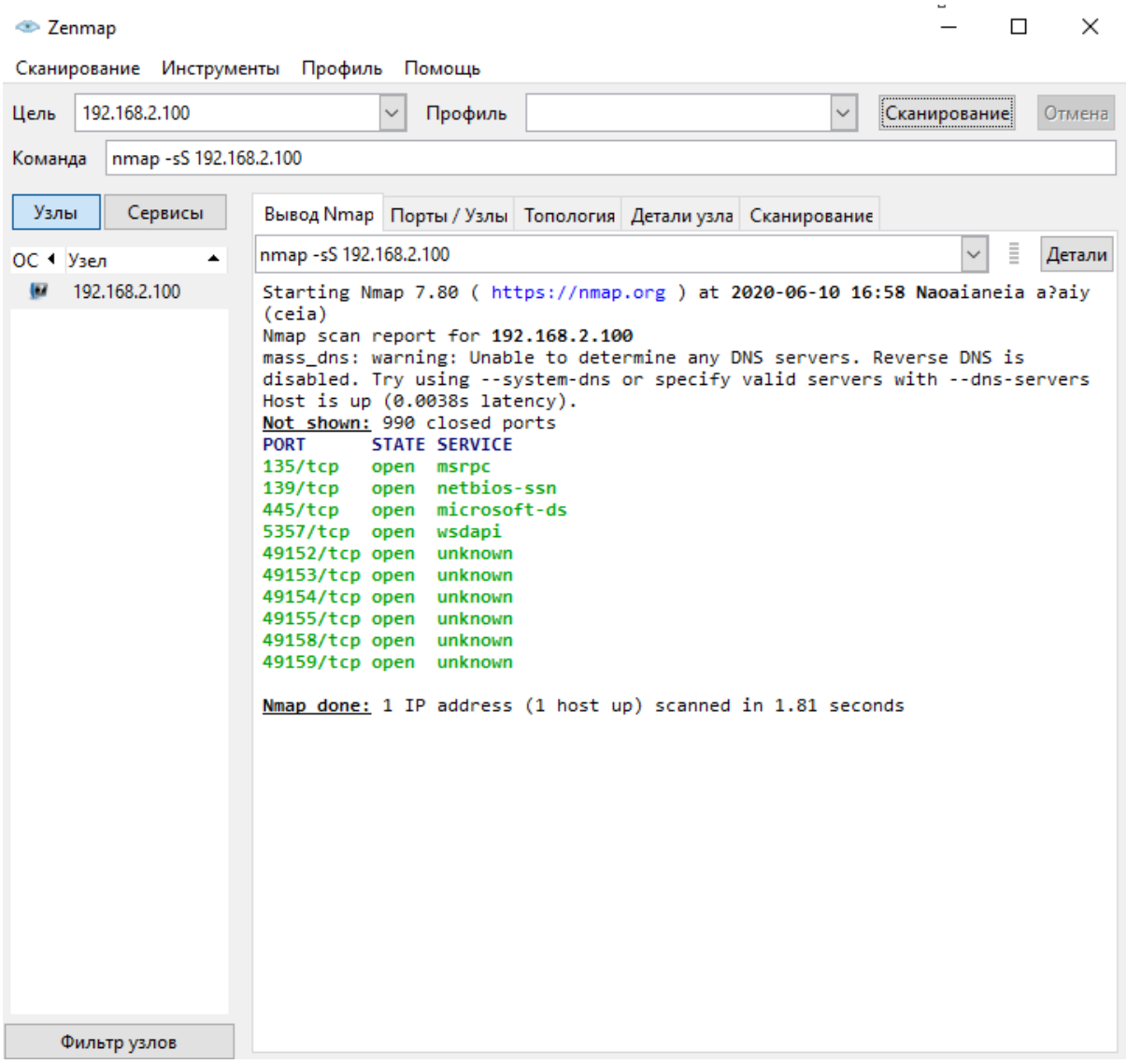


Рисунок – Запуск сканирования с помощью программы Zenmap

2. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

   - «ET SCAN NMAP» (см. Рисунок – Результаты сканирования).

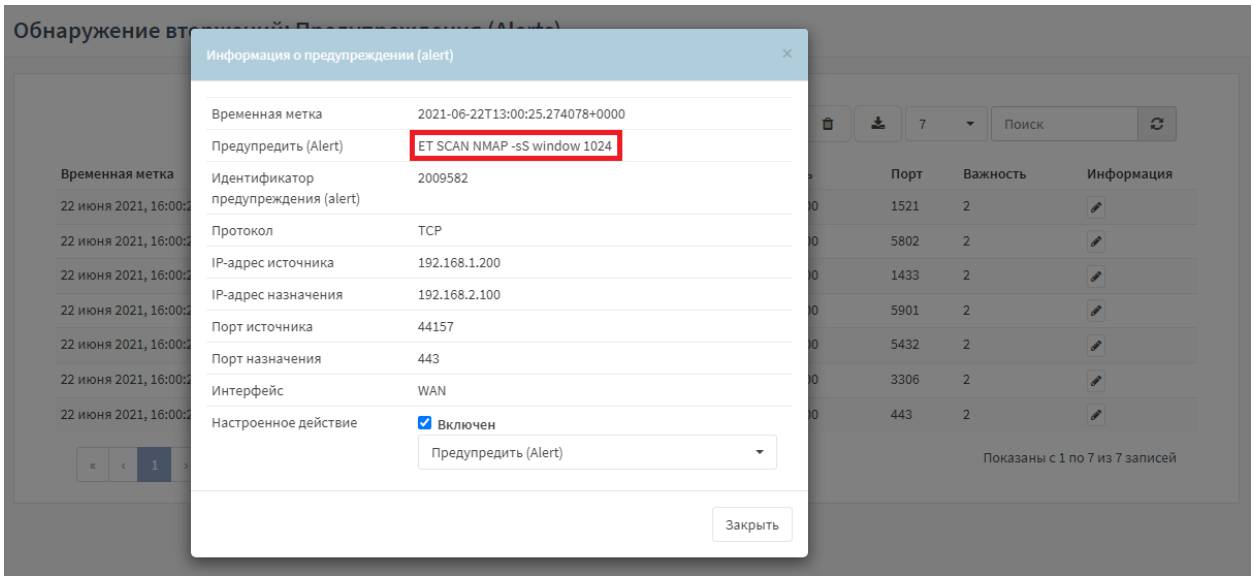


Рисунок – Результаты сканирования

5.2.4 Управление группой правил СОВ

«ARMA FW» поддерживает выполнение определённых действий над группой выбранных правил СОВ нажатием на следующие **кнопки**:

- «☐» – отключение правил;
- «☑» – включение правил;
- «предупреждение (alert)» – назначение действия «Предупредить (Alert)»;
- «отбросить (drop)» – назначение действия «Отбросить (Drop)».

Для управления группой выбранных правил СОВ необходимо выполнить следующие действия:

1. Перейти во вкладку **«Правила»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**).
2. Установить в столбце слева флажки напротив интересующих правил.
3. Нажать **кнопку**, соответствующую необходимому действию.
4. Нажать **кнопку «Применить»**.

5.3 Настройка импорта правил

Импорт правил СОВ возможен с удалённых FTP/SMB-серверов.

ARMA FW поддерживает передачу данных по протоколу SMB 3.1.1.

При импорте используется архив **«tar.gz»**, содержащий файлы наборов правил. Название архива должно соответствовать следующему формату:

- **«rulesets_[версия ARMA FW]_[версия правил].tar.gz»**, например «rulesets_3.7.1_1.0.6.tar.gz»,

файлы наборов правил должны иметь расширение **«rules»**, например, «scan.rules».

В процессе импорта выбирается архив с наиболее новой версией правил.

Архив, содержащий файлы наборов правил, должен находиться в каталоге с названием, соответствующим следующему формату:

- **«armaif_[версия ARMA FW]»**, например «armaif_3.7.1».

Для настройки импорта правил необходимо выполнить следующие действия:

1. Перейти в подраздел настроек импорта правил (**«Обнаружение вторжений» - «Настройки импорта правил»**).
2. Установить флажок в параметре **«Включен»** и указать настройки импорта для требуемого протокола:
   - Значение для **FTP**:
     - **«Протокол»** – «FTP»;
     - **«Адрес»** – Адрес сервера: IP-адрес, хост, доменное имя;
     - **«Имя пользователя»** – Учётные данные;
     - **«Пароль»** – Учётные данные;
     - **«Путь к корневой папке»** – Путь к каталогу с архивом правил. Путь должен начинаться с символа **«/»**. Если каталог с архивом находится в корневой директории, необходимо оставить только символ **«/»**;
     - **«Интервал»** – Интервал ожидания в случае неудачной попытки, задаётся в секундах;
   - Значение для **SMB**:
     - **«Протокол»** – «SMB»;
     - **«Адрес»** – Адрес сервера: IP-адрес, хост, доменное имя;
     - **«Общедоступный ресурс Samba»** – Имя общедоступного ресурса Samba;
     - **«Имя пользователя»** – Учётные данные;
     - **«Пароль»** – Учётные данные;
     - **«Путь к корневой папке»** – Путь к каталогу с архивом правил. Путь должен начинаться с символа **«/»**. Если каталог с архивом находится в корневой директории, необходимо оставить только символ **«/»**;

- **«Интервал»** – Интервал ожидания в случае неудачной попытки, задаётся в секундах.

3. Для сохранения настроек необходимо нажать **кнопку «Сохранить»**, а для сохранения настроек и импорта нажать **кнопку «Сохранить и импортировать»**.

Результатом успешного импорта правил СОВ будет запись в журнале syslog (**«Система» - «Журналы» - «Журнал Syslog»**) (см. Рисунок – Сообщения об успешном импорте правил СОВ) и появление импортированных правил в подразделе СОВ (**«Обнаружение вторжений» - «Администрирование» - «Сохранение»**) (см. Рисунок – Настройка импорта правил).

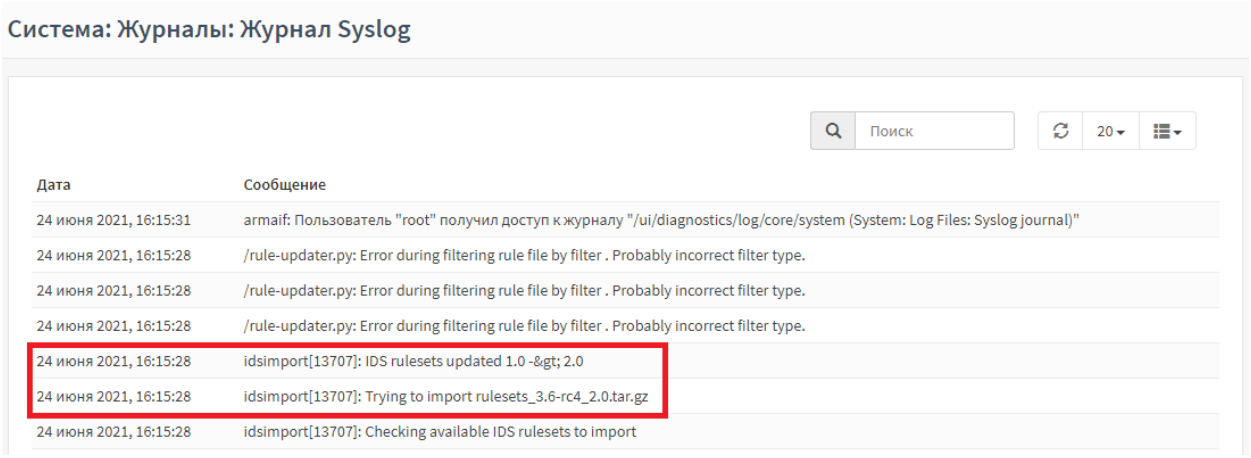


Рисунок – Сообщения об успешном импорте правил СОВ

Для настроенного импорта возможно задать расписание выполнения с помощью планировщика задач Cron (см. Cron). При создании задачи необходимо выбрать «Импорт правил СОВ» в параметре **«Команда»**.

5.4 Экспорт наборов правил СОВ

Существует возможность экспортировать наборы правил СОВ, загруженных ранее.

Для этого необходимо перейти в подраздел резервного копирования (**«Система» - «Конфигурация» - «Резервные копии»**) и в блоке **«Скачать наборы правил СОВ»** (см. Рисунок – Экспорт наборов правил СОВ) нажать **кнопку «Экспорт»**. Наборы правил СОВ будут скачаны архивом формата **«tar.gz»**, название архива будет иметь следующий формат:

- «localrulesets-[полное доменное имя ARMA FW]-[Дата экспорта][Время экспорта].tar.gz».

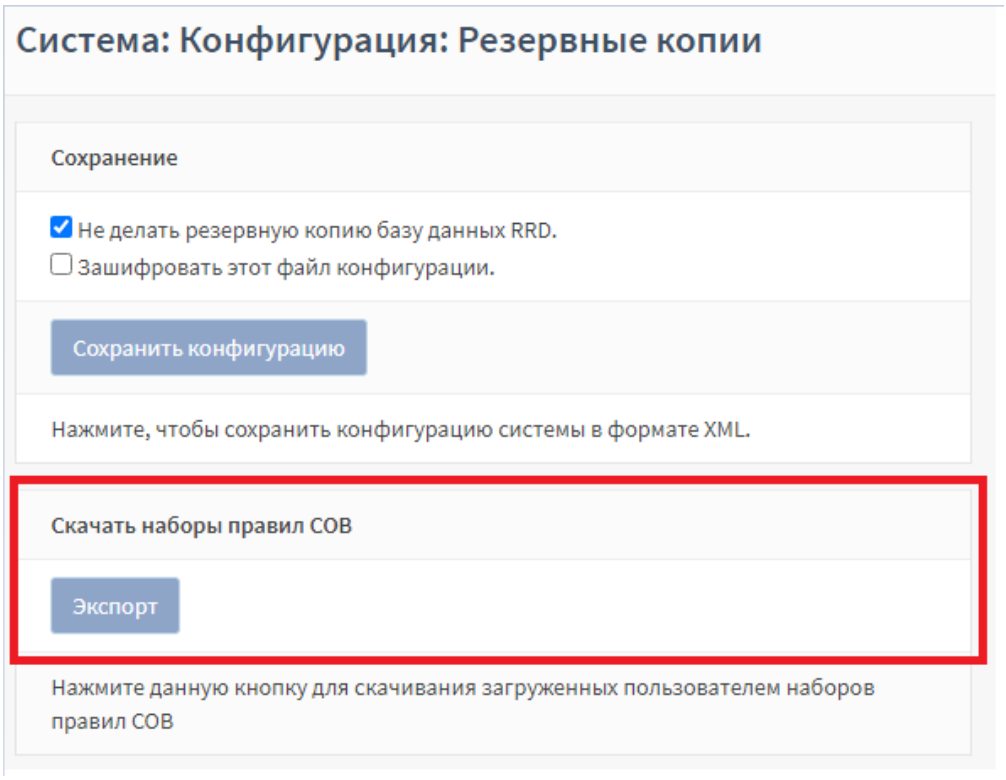


Рисунок – Экспорт наборов правил СОВ

5.5 Подсистема «Контроль промышленных протоколов»

Подсистема контроля промышленных протоколов модуля СОВ реализована на базе технологии глубокой инспекции пакетов протоколов прикладного уровня, включая промышленные протоколы.

Функциональность подсистемы контроля промышленных протоколов обеспечивает интеллектуальное распознавание протоколов прикладного уровня за счёт сигнатурного анализа.

Шаблоны промышленных протоколов позволяют создавать пользовательские правила для обеспечения дополнительной фильтрации или уведомления об определённых сетевых событиях.

Ниже приведён список поддерживаемых протоколов, для которых представлены шаблоны форм правил, и степень их разбора:

1. **ADS**.

   Стандарт – Automation Device Specification.

   Сообщения по протоколу ADS разделяются по типу транспорта:

   - TCP;
   - UDP.

Для сообщений по протоколу ADS возможно задать правило обнаружения по признакам:

- AMS NetId – идентификатор устройства, для которого предназначен пакет;
- AMS порт – порт устройства, для которого предназначен пакет;
- команды ADS;
- тип сообщения – запрос или ответ.

При обнаружении по командам **«ADS Read»**, **«ADS Write»**, **«ADS Add Device Notification»**, **«ADS Read Write»** возможно задать параметры для следующих запросов:

- ADS индекс группы;
- ADS индекс смещения.

При обнаружении по команде **«ADS Write Control»** возможно задать параметры для следующих запросов:

- состояние ADS;
- состояние устройства.

При обнаружении по команде **«ADS Add Device Notification»** возможно задать параметры для запроса:

- режим передачи.

2. **DNP3**.

   Сообщения по протоколу DNP3 разделяются по:

   - функции;
   - объекту, с указанием группы и вариации;
   - внутренней индикации;
   - контенту, с указанием шестнадцатеричного потока.

3. **ENIP/CIP**.

   Сообщения по протоколу ENIP обнаруживаются по команде.

   Сообщения по протоколу CIP обнаруживаются по:

   - сервису;
   - сервису и классу;
   - сервису, классу и атрибуту.

Сообщения по протоколу CIP обнаруживаются по классу и атрибуту для сервисов: «3», «4», «14», «16».

4. **EtherCAT**.

   Стандарт – IEC/PAS 62407(2005).

   Сообщения по протоколу EtherCAT обнаруживаются по:

   - команде – CMD;
   - логическому адресу – ADDR;
   - составному адресу – SLAVE, OFFSET;
   - значению поля **данные** – DATA;
   - регистрам – 120, 130, 200, 300, 502, 504-50E.

5. **Fanuc FOCAS**.

   Сообщения по протоколу EtherCAT обнаруживаются по:

   - запросу;
   - ответу;
   - команде;
   - аргументам.

6. **GOOSE**.

   Стандарт – IEC 61850-8-1.

   Сообщения по протоколу GOOSE разделяются по:

   - идентификатору приложения;
   - значению поля **«Dataset»**;
   - значению поля **«GoCBRef»**;
   - значению поля **«GoID»**;
   - значению поля **«Дельта секунд»**;
   - значению поля **«Дельта наносекунд»**;
   - значению поля **«Предустановленная дата и время»**;
   - значению поля **«Предустановленные наносекунды»**.

7. **IEC 60870-5-104**.

   Стандарт – ГОСТ Р МЭК 60870-5-104-2004.

   Сообщения по протоколу IEC 60870-5-104 могут быть определены по типу пакета:

- полный APDU;
- для целей управления – только поля APCI.

При классификации по типу пакета APCI возможен выбор формата пакета:

- **любой**;
- **«U-format (unnumbered control functions)»** – функции управления без нумерации;
- **«S-format (numbered supervisory functions)»** – функции контроля с нумерацией.

При классификации по типу пакета ASDU возможно задание:

- диапазона разрешённых входящих пакетов (RX);
- диапазона разрешённых исходящих пакетов (TX);
- типа данных ASDU;
- COT (Cause of Transmission) – причины передачи;
- AD – ASDU адреса (условие).

Возможно задать правила для полей объектов информации:

- **IOA** – адрес (диапазон);
- **IOA_V** – значение (целые числа) (условие);
- **VALUE** – значение (целые и дробные числа) (условие и диапазон);
- **QDS**, **SP_QDS**, **DP_QDS** – описатели качества;
- **SINGLE_CMD**, **DOUBLE_CMD** – одиночная команда, двойная команда;
- **QLF**, **QLF_COUNTER**, **QLF_MEASURED** – квалификатор;
- **CP16TIME**, **CP24TIME**, **CP56TIME**, **CP56TIME_BEGIN**, **CP56TIME_END** – метки времени;
- **FILE** – для файловых типов данных;
- **COI** – причина инициализации;
- **VTI** – значение с индикацией переходного состояния (с поддержкой отрицательных чисел);
- **SEP_SINGLE** – одиночное событие релейной защиты.

8. **KRUG**.

   Круг ПК-контроллер.

   Сообщения по протоколу KRUG разделяются по:

- значению поля **«COMMAND»**;
- значению поля **«CMD»**;
- значению поля **«PORT»**;
- значению поля **«ACCESS»**;
- значению поля **«MODE»**;
- значению поля **«ERRCODE»**.

9. **MMS**.

   Стандарт – IEC 61850-8-1.

   Сообщения по протоколу MMS разделяются по типу сообщения.

   Для типа сообщения **«CONFIRMED_REQUEST»** возможен выбор типа служб.

   Для службы **«READ»** возможен ввод имени переменной и адреса переменной для функции чтения.

   Для службы **«WRITE»** возможен ввод имени переменной для функции записи.

10. **Modbus TCP**.

    Стандарт – MODBUS Application Protocol Specification V1.1b3.

    Для сообщений по протоколу Modbus TCP можно задать правило обнаружения на основе признака совпадения:

    - свойство функции – код или категория функции;
    - тип доступа к данным – тип доступа и основная модель данных;
    - диапазон функции – ввод кода функции, адреса и значения переменной вручную.

    При обнаружении по свойству функции возможно задать дополнительные опции:

    - используемую функцию, подфункцию;
    - категорию кодов функции.

    Категории кодов функции:

    - назначенная – коды функций, которые определены в Modbus спецификации;
    - неназначенная – общедоступная, стандартные и организационные коды;
    - пользовательская – два диапазона кодов, для которых возможно назначить произвольную функцию;

- зарезервированная – коды функций, не являющимися стандартными;
- все категории.

При классификации по доступу к данным возможно задать следующие дополнительные опции:

- тип доступа к данным – записать или считать;

Модель данных:

- **«Регистры флагов (Coils)»** – битовые данные, доступ чтение/запись;
- **«Регистры хранения (Holding Registers)»** – 16 битовые данные, доступ чтение/запись;
- **«Дискретные входы (Discrete Inputs)»** – битовые данные, доступ чтение;
- **«Регистры ввода (Input Registers)»** – 16 битовые данные, доступ чтение.

11. **OPC DA**.

Стандарт – OLE for Process Control Data Access Automation Interface Standard v.2.0.

Сообщения по протоколу OPC DA разделяются по типу сообщения:

- REQUEST;
- PING;
- RESPONSE;
- FAULT;
- WORKING;
- NOCALL;
- REJECT;
- ACK;
- CI_CANCEL;
- FACK;
- CANCEL_ACK;
- BIND;
- BIND_ACK;
- BIND_NACK;
- ALTER_CONTEXT;

- ALTER_CONTEXT_RESP;
- SHUTDOWN;
- AUTH3;
- CO_CANCEL;
- ORPHANED.

При выборе **«REQUEST»** в поле появятся поля ввода идентификатора вызываемого объекта и ввода номера вызываемой функции объекта.

12. **OPC UA**.

Стандарт – IEC 62541.

Сообщения по протоколу OPC UA разделяются по типу сообщения:

- **«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.

При выборе **«OPEN»** появится поле выбора политики безопасности.

При выборе **«MESSAGE»** появится поле выбора типа запроса.

При выборе **«BROWSE»** в поле **«Тип запроса»** появятся поле выбора типа идентификатора узла и поле ввода значения, и поле ввода идентификатора пространства имен.

При выборе **«READ»** в поле **«Тип запроса»** появятся поле выбора типа идентификатора узла и поле ввода значения, поле ввода идентификатора пространства имен.

При выборе **«WRITE»** в поле **«Тип запроса»** появятся поле ввода идентификатора пространства имен, поле ввода значения, поле выбора типа идентификатора узла и поле выбора типа значений.

При выборе **«CALL»** в поле **«Тип запроса»** появятся поле выбора типа идентификатора узла, вызываемого объекта, и поле выбора типа идентификатора узла, вызываемого метода.

13. **RDP**.

Стандарт – T.120.

Сообщения по протоколу RDP фильтруются по значению поля «Значение RDP Cookie».

14. **S7comm**.

    Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-300/400.

    Сообщения по протоколу S7comm разделяются по функции:

    - CPUSERVICE;
    - SETUPCOMM;
    - READVAR;
    - WRITEVAR;
    - REQUESTDOWNLOAD;
    - DOWNLOADBLOCK;
    - DOWNLOADENDED;
    - STARTUPLOAD;
    - UPLOAD;
    - ENDUPLOAD;
    - PLCCONTROL;
    - PLCSTOP.

    При выборе в поле **«Функция»** функции **«READVAR»** необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных.

    При выборе в поле **«Функция»** функции **«WRITEVAR»** необходимо выбрать тип области чтения и поля ввода имени области, типа данных, количества данных и смещения данных, типа передаваемого значения, количество передаваемых данных, список значений данных.

    При выборе в поле **«Функция»** функции **«REQUESTDOWNLOAD»** появятся поля выбора типа блока, номера блока и целевой файловой системы.

    При выборе в поле **«Функция»** функции **«DOWNLOADBLOCK»** появятся поля выбора типа блока, номера блока и целевой файловой системы.

    При выборе в поле **«Функция»** функции **«STARTUPLOAD»** появятся поля выбора типа блока, номера блока и целевой файловой системы.

    При выборе в поле **«Функция»** функции **«PLCCONTROL»** появится поле выбора функции управления ПЛК:

- «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 идентификатор файловой системы A/E/P)»;
- «OFF (Выключение ПЛК)»;
- «ON (Включение ПЛК)».

15. **S7comm Plus**.

Стандарт протокола связи коммуникационных модулей серий Siemens SIMATIC S7-1200 и S7-1500.

Сообщения по протоколу S7comm Plus разделяются по типу сообщения:

- REQUEST;
- RESPONSE;
- NOTIFY;
- RESPONSE2.

По типу взаимодействия:

- CONNECT;
- DATA;
- DATAFW1_5;
- KEEPALIVE;
- EXT_KEEPALIVE.

По функции:

- EXPLORE;
- CREATEOBJECT;
- DELETEOBJECT;
- SETVARIABLE;
- GETLINK;
- SETMULTIVAR;

- GETMULTIVAR;
- BEGINSEQUENCE;
- ENDSEQUENCE;
- INVOKE;
- GETVARSUBSTR.

При выборе в поле **«Функция»** функции **«EXPLORE»** возможно выбрать диапазоны для параметров EXPLORE_AREA и EXPLORE_ATTR_ID.

При выборе в поле **«Функция»** функции **«CREATEOBJECT»** возможно выбрать диапазон для параметра CREATEOBJECT_ATTR_ID.

При выборе в поле **«Функция»** функции **«DELETEOBJECT»** возможно выбрать диапазоны для параметров DELETEOBJECT_OBJ_ID и DELETEOBJECT_ATTR_ID.

При выборе в поле **«Функция»** функции **«GETLINK»** возможно выбрать диапазон для параметра GETLINK_ATTR_ID.

При выборе в поле **«Функция»** функции **«SETMULTIVAR»** возможно выбрать диапазон для параметра SETMULTIVAR_ATTR_ID.

При выборе в поле **«Функция»** функции **«GETMULTIVAR»** возможно выбрать диапазон для параметра GETMULTIVAR_ATTR_ID.

При выборе в поле **«Функция»** функции **«GETVARSUBSTR»** возможно выбрать диапазон для параметра GETVARSUBSTR_ATTR_ID.

16. **Telnet**.

    Стандарт – RFC 854.

    Сообщения по протоколу Telnet фильтруются по значению поля «Значение Telnet login».

17. **UMAS**.

    Основан на протоколе Xway Unite. Протокол Umas используется для настройки и мониторинга ПЛК Schneider-Electric.

    Сообщения по протоколу UMAS разделяются по функциям:

    - инициализация UMAS сессии;
    - чтение информации о проекте;
    - чтение внутренней информации ПЛК;
    - назначение ПЛК владельца;
    - инициализация загрузки – копирование с инженерного ПК на ПЛК;
    - завершение загрузки – копирования с инженерного ПК на ПЛК;

- инициализация скачивания – копирование с ПЛК на инженерный ПК;
- конец скачивания – копирования с ПЛК на инженерный ПК;
- включение ПЛК;
- выключение ПЛК.

Поддержка правил по протоколам:

- ADS;
- IEC104;
- MMS;
- Modbus;
- OPC DA;
- OPC UA;
- S7comm;
- S7comm Plus;

реализована на уровне приложений. Данные протоколы будут анализироваться и обнаруживаться **ARMA FW** только в случае, если подсистема СОВ была запущена до момента установления сессии по данным протоколам.

В случае, если установление сессии произошло до запуска подсистемы СОВ, пакеты данных сессий при анализе использованы не будут.

При использовании нестандартных портов для протоколов:

- Modbus;
- DNP3;
- OPC UA;
- S7comm, TPKT;
- S7comm Plus, TPKT;
- MMS, TPKT;
- IEC104;
- ADS;
- ENIP/CIP;
- Fanuc FOCAS;

следует указать порты с помощью параметров **«Уровень приложения: Modbus порт(-ы)»**, **«Уровень приложения: DNP3 порт(-ы)»**, **«Уровень приложения: TPKT порт(-ы)»**, **«Уровень приложения: OPC UA порт(-ы)»**,

«Уровень приложения: IEC104 порт(-ы)», **«Уровень приложения: ADS порт(-ы)»**, **«Уровень приложения: ENIP/CIP порт(-ы)»** и **«Уровень приложения: Fanuc FOCAS порт(-ы)»** (см. Дополнительные настройки СОВ).

5.5.1 Создание правила СОВ

Для создания пользовательских правил необходимо перейти в подраздел настроек правил (**«Обнаружение вторжений» - «Контроль промышленных протоколов»**) и нажать **кнопку** « », в открывшейся форме (см. Рисунок – Форма редактирования правила СОВ) указать параметры правила и нажать **кнопку «Сохранить»**.

Для редактирования существующих правил необходимо перейти в подраздел настроек правил (**«Обнаружение вторжений» - «Контроль промышленных протоколов»**) и нажать **кнопку** « » напротив существующего правила, в открывшейся форме (см. Рисунок – Форма редактирования правила СОВ) изменить параметры правила и нажать **кнопку «Сохранить»**.

Поля параметров **«Заголовок»** и **«Сообщение»** обязательны для заполнения.

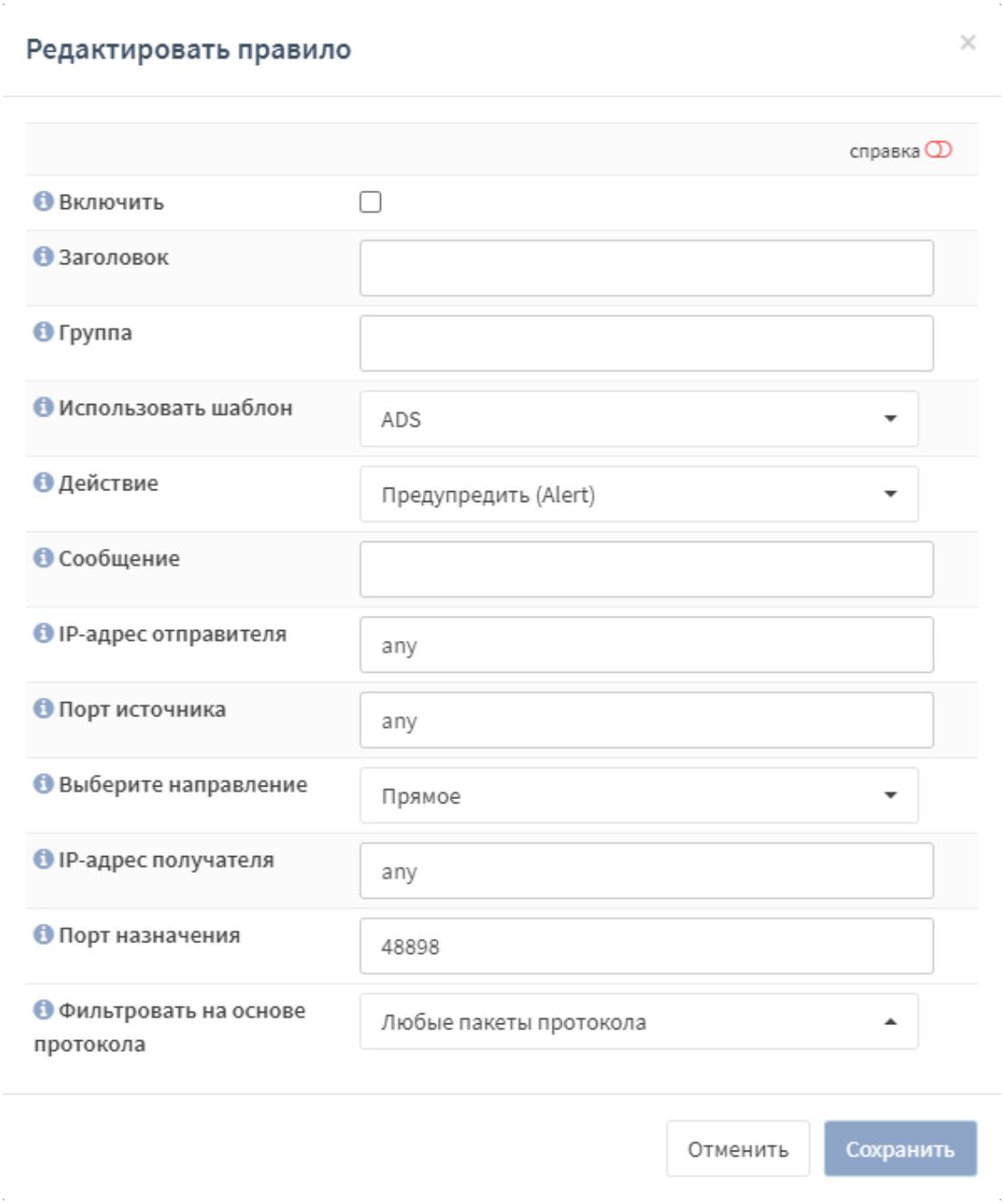


Рисунок – Форма редактирования правила СОВ

При создании пользовательских правил доступны следующие варианты действий:

- **«Предупредить (Alert)»** –оповещение при срабатывании правила;
- **«Отклонить (Reject)»** – блокировка пакета при срабатывании правила и оповещение о блокировке отправителя;
- **«Отбросить (Drop)»** – блокировка пакета при срабатывании правила без уведомления о блокировке отправителя;
- **«Разрешить (Pass)»** – разрешение прохождения пакета при срабатывании правила.

Примечание:

При проверке срабатывания пользовательских правил необходимо убедиться, что СОВ включена (см. Основные настройки СОВ).

5.5.2 Создание пользовательских правил на основе собственного шаблона

В качестве примера работы правила СОВ будет рассмотрена имитация DOS-атаки. Схема стенда представлена на рисунке (см. Рисунок – Схема стенда для проверки срабатывания пользовательского правила на DOS-атаку). На ПК **«Kali Linux»** установлено ОС Kali Linux.

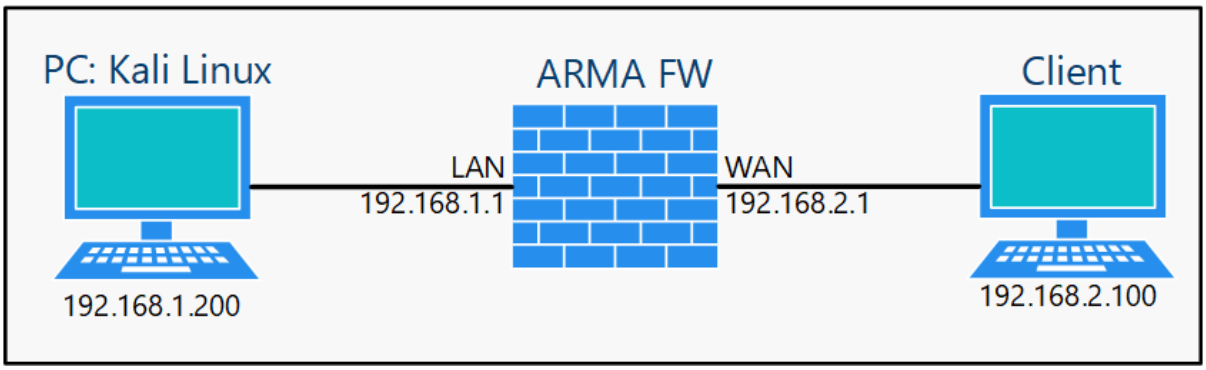


Рисунок – Схема стенда для проверки срабатывания пользовательского правила на DOS-атаку

5.5.2.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Создание правила СОВ) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «DOS-attack»;
- **«Использовать шаблон»** – «Настроенное пользователем»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «DOS-attack»;
- **«Протокол»** – «TCP»;
- **«Специфичная часть правила»** – «flow: stateless; threshold: type both, track by_dst, count 200, seconds 1;».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

Параметр **«Специфичная часть правила»** сконфигурирован в соответствии с форматом написания правил ПО «Suricata», дополнительные сведения представлены на официальном сайте ПО «Suricata» (см. https://docs.suricata.io/en/suricata-6.0.20/rules/intro.html).

5.5.2.2 Проверка созданного правила СОВ

Для проверки правила СОВ необходимо выполнить следующие действия:

1. На ПК «Kali Linux» запустить терминал и выполнить команду:

```
hping3 -S --flood 192.168.2.100
```

2. Через 10 секунд остановить команду комбинацией **клавиш «Ctrl»** + **«C»**.
3. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
   - «DOS-attack» (см. Рисунок – Детальная информация. DOS-атака).

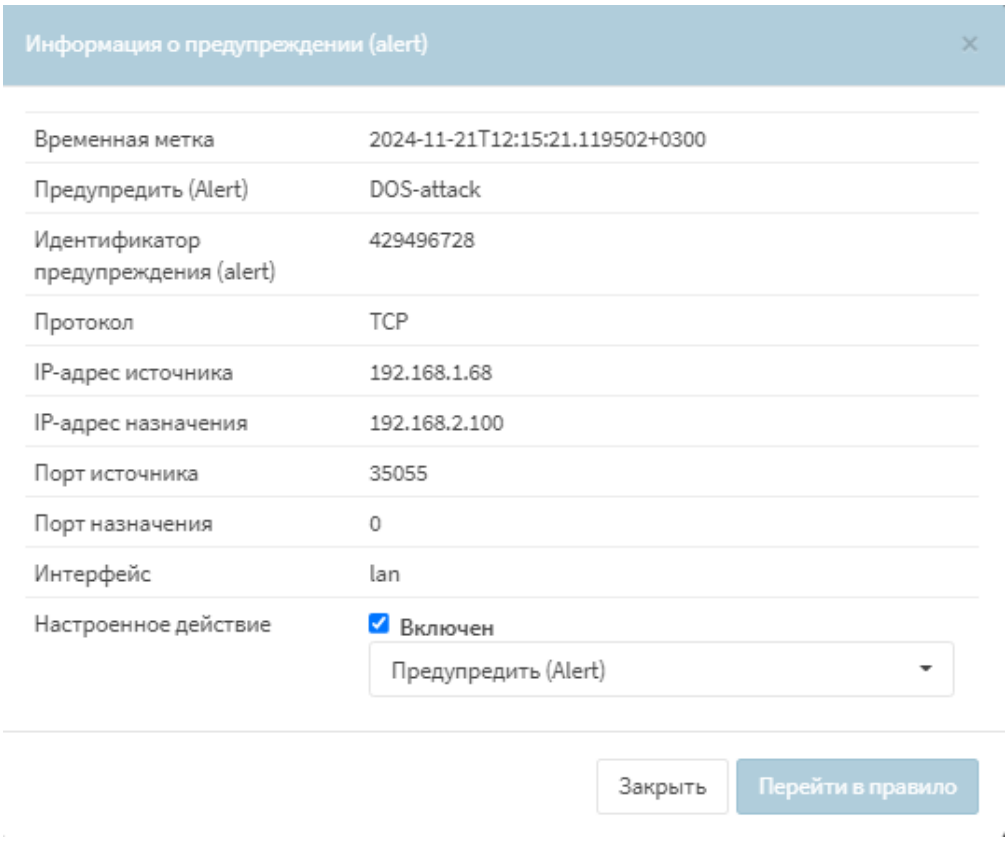


Рисунок – Детальная информация. DOS-атака

5.5.3 Создание пользовательских правил СОВ на основе шаблонов промышленных протоколов

Для проверки срабатывания пользовательских правил СОВ на основе шаблонов промышленных протоколов используется стандартная схема стенда (см. Рисунок – Схема стенда для срабатывания пользовательских правил СОВ на основе шаблонов промышленных протоколов).

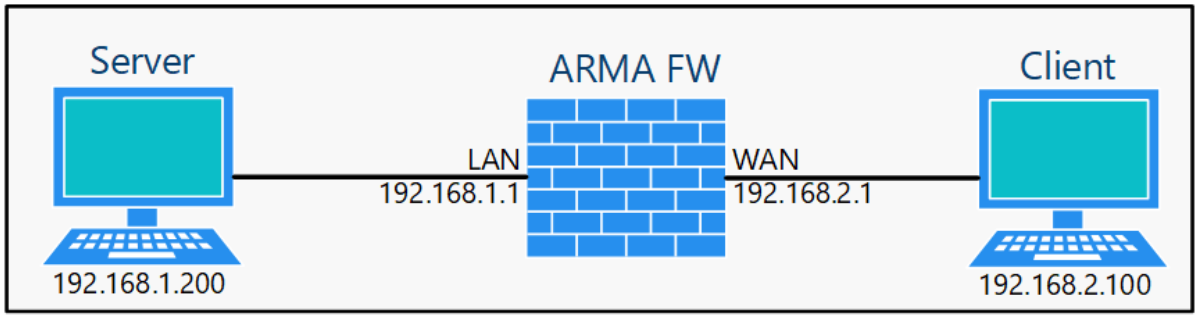


Рисунок – Схема стенда для срабатывания пользовательских правил СОВ на основе шаблонов промышленных протоколов

Для некоторых промышленных протоколов доступно значение «Любые кроме пакета протокола» в параметре **«Фильтровать на основе протокола»**. При выборе данной опции при создании правила для указанного протокола все пакеты, не определённые как пакеты указанного протокола, вызовут срабатывания правила.

Примечание:

При проверке срабатывания пользовательских правил на основе шаблонов промышленных протоколов необходимо убедиться, что создано соответствующее разрешающее правило МЭ (см. Создание правил межсетевого экранирования) и включена СОВ (см. Основные настройки СОВ). Основные параметры правил для протоколов приведены в списке (см. Основные параметры правил для протоколов).

Основные параметры правил для протоколов:

- **«Действие»** – Разрешить (Pass);
- **«Интерфейс»** – WAN;
- **«Протокол»** – TCP;
- **«IP-адрес назначения»** – Единственный хост или сеть, 192.168.1.200/32;
- **«Диапазон портов назначения»** – Указывается в зависимости от протокола (см. Таблица «Значения портов по умолчанию для промышленных протоколов»).

Таблица «Значения портов по умолчанию для промышленных протоколов»

Протокол	Порт по умолчанию
ADS	48898
DNP3	20000
ENIP/CIP	2222, 44818
Fanuc FOCAS	8193
GOOSE	Не используется

Протокол	Порт по умолчанию
IEC 104	2404
KRUG	2100/UDP
MMS	102
Modbus	502
OPC DA	135
OPC UA	4840, 48020
RDP	3389
S7comm	102
S7comm Plus	102
Telnet	23
UMAS	502

Примечание:

Для протокола GOOSE рекомендуется использовать белые списки для интерфейса (см. Блок «Контроль доступа устройств»).

5.5.3.1 Шаблон протокола Modbus

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

При выборе «Указать дополнительные параметры» появятся параметры **«Совпадение по»** и **«Код функции»**.

В поле параметра **«Совпадение по»** доступно два признака совпадения правила:

- **«Функции»** – код или категория функции;
- **«Данные»** – тип доступа и основная таблица.

При выборе опции **«Функции»** появится параметр **«Код функции»**, в котором необходимо выбрать код или категорию функции.

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».

5.5.3.1.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Создание правила СОВ) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «Modbus»;
- **«Использовать шаблон»** – «Modbus»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «Modbus»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Совпадение по»** – «Функции»;
- **«Код функции»** – «06:Write Single Register».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.1.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола Modbus на ПК **«Server»** должно быть установлено ПО «ModbusPal», а на ПК **«Client»** – ПО «qModMaster».

Для проверки правила СОВ необходимо выполнить следующие действия:

1. В ПО «ModbusPal» запустить сервис, нажав **кнопку «Run»**, затем в блоке **«Modbus slaves»** нажать **кнопку «Add»**, выбрать **«1»** и снова нажать **кнопку «Add»**.

2. Нажать **кнопку** «  » и путём нажатия **кнопки «Add»** добавить строки от «1» до «10» (см. Рисунок – Настройка ПО «ModbusPal») для добавления десяти регистров со значениями «0».

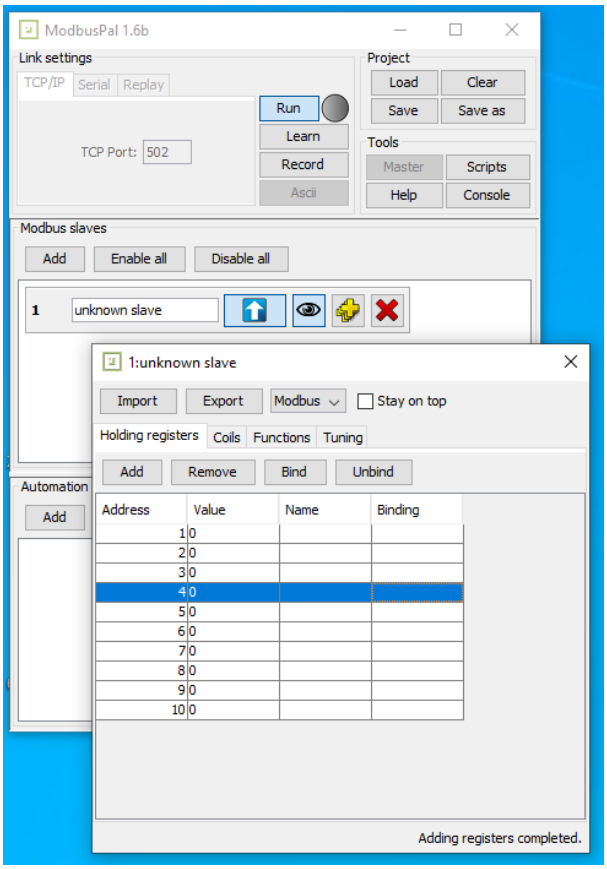


Рисунок – Настройка ПО «ModbusPal»

3. В ПО «qModMaster» выполнить соединение с ПО «ModbusPal», для этого нажать **кнопку** « », ввести «192.168.1.100» и нажать **кнопку** « » (**«Connect»**) для подключения к ПК **«Server»**.
4. Выбрать следующие значения в полях:
   - **«Modbus Mode»** – «TCP»;
   - **«Function code»** – «Write Single Register»;
   - **«Start Address»** – «7».
5. Выполнить функцию чтения/записи нажав **кнопку** « » – **«Read/Write»**.

   Примечание:

   Внесённые данные в строку, указанную в поле **«Start Address»**, фактически будут отображаться со смещением на одну строку – то есть при внесении изменения в 7 строку данные появятся в 8.

6. В ПО «ModbusPal» убедиться, что внесённые данные отобразились (см. Рисунок – Запись данных).

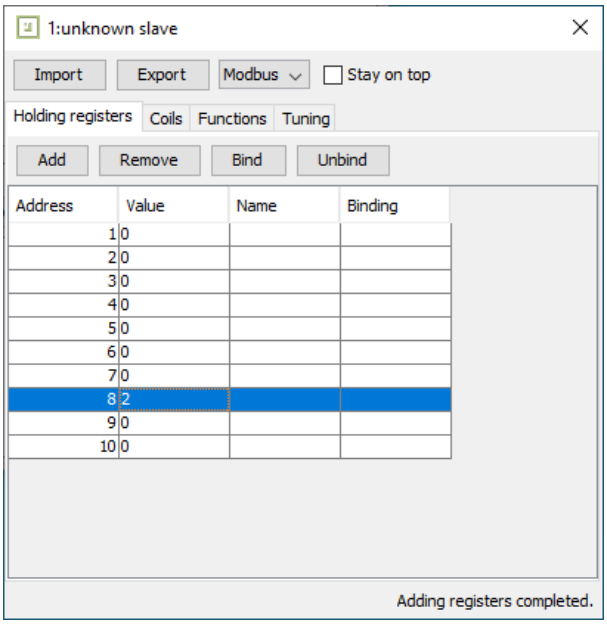


Рисунок – Запись данных

7. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

   - «Modbus» (см. Рисунок – Детальная информация, протокол Modbus).

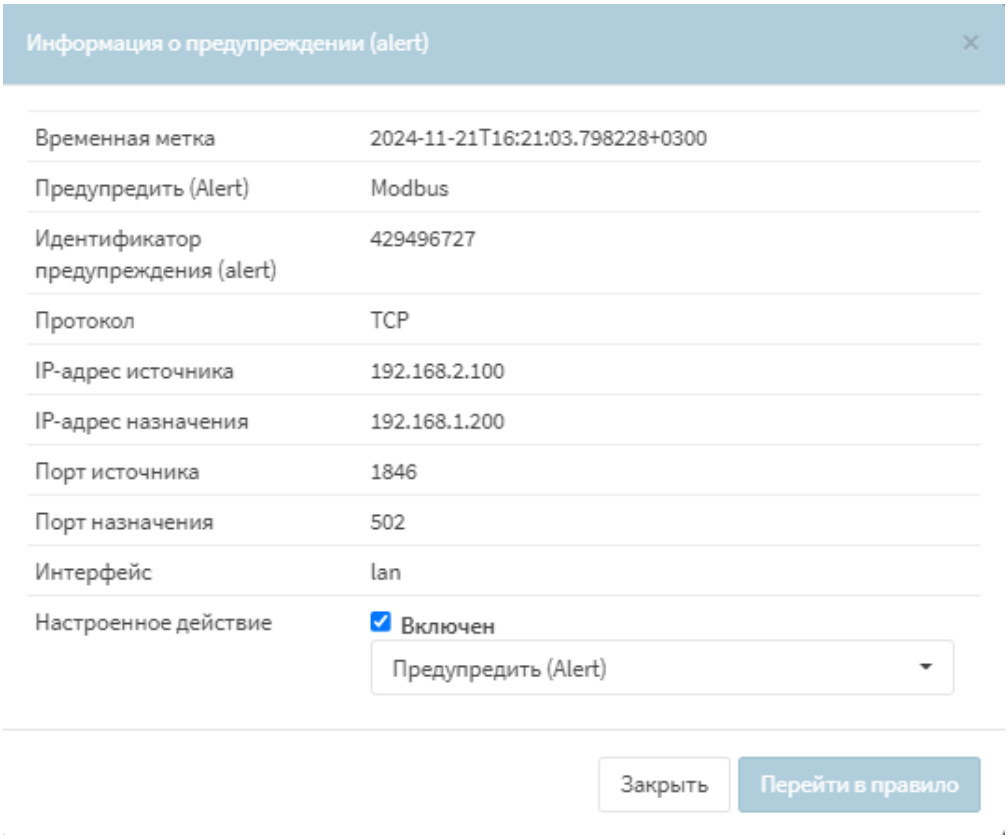


Рисунок – Детальная информация, протокол Modbus

5.5.3.2 Шаблон протокола IEC 104

При создании пользовательского правила на основе шаблона промышленного протокола IEC 104 необходимо задать параметры протокола, выбрав в поле параметра **«Фильтровать на основе протокола»** значение «Указать дополнительные параметры».

При выборе опции «Указать дополнительные параметры» появится параметр **«Функция приложения»**, в котором доступно два типа пакета:

- **«ASDU»** – блок данных прикладного уровня;
- **«APCI»** – управляющая информация прикладного уровня, включающий в каждый заголовок APCI такие маркировочные элементы, как стартовый символ и указание длины ASDU вместе с полем управления.

При выборе опции **«ASDU (блок данных прикладного уровня)»** появятся следующие параметры:

- **«RX»**;
- **«TX»**;
- **«Тип ASDU»**;
- **«ASDU COT (причина передачи)»**;
- **«AD условие»**;
- **«AD (ASDU адрес)»**;
- **«IOA (адрес объекта информации)»**;
- **«Тип объекта»**;
- **«Инвертировать IOA значение»**;
- **«IOA значение»**;
- **«Тип проверки»**.

Диапазон разрешённых входящих и исходящих пакетов необходимо указать в полях параметров **«RX»** и **«TX»** соответственно.

В поле параметра **«Тип ASDU»** доступны следующие типы ASDU:

- **«Любой»**;
- **«1: M_SP_NA_1 (Single-point information)»** – одноэлементная информация;
- **«2: M_SP_TA_1 (Single-point information with time tag)»** – одноэлементная информация с меткой времени;

- **«3: M_DP_NA_1 (Double-point information)»** – двухэлементная информация;
- **«4: M_DP_TA_1 (Double-point information with time tag)»** – двухэлементная информация с меткой времени;
- **«5: M_ST_NA_1 (Step position information)»** – информация о положении отпаек;
- **«6: M_ST_TA_1 (Step position information with time tag)»** – информация о положении отпаек с меткой времени;
- **«7: M_BO_NA_1 (Bitstring of 32 bit)»** – строка из 32 битов;
- **«8: M_BO_TA_1 (Bitstring of 32 bit with time tag)»** – строка из 32 битов с меткой времени;
- **«9: M_ME_NA_1 (Measured value, normalised value)»** – значение измеряемой величины, нормализованное значение;
- **«10: M_ME_TA_1 (Measured value, normalised value with time tag)»** – значение измеряемой величины, нормализованное значение с меткой времени;
- **«11: M_ME_NB_1 (Measured value, scaled value)»** – значение измеряемой величины, масштабированное значение;
- **«12: M_ME_TB_1 (Measured value, scaled value with time tag)»** – значение измеряемой величины, масштабированное значение с меткой времени;
- **«13: M_ME_NC_1 (Measured value, short floating point number)»** – значение измеряемой величины, короткий формат с плавающей запятой;
- **«14: M_ME_TC_1 (Measured value, short floating point number with time tag)»** – значение измеряемой величины, короткий формат с плавающей запятой, с меткой времени;
- **«15: M_IT_NA_1 (Integrated totals)»** – интегральные суммы;
- **«16: M_IT_TA_1 (Integrated totals with time tag)»** – интегральные суммы с меткой времени;
- **«17: M_EP_TA_1 (Event of protection equipment with time tag)»** – информация о работе релейной защиты с меткой времени;
- **«18: M_EP_TB_1 (Packed start events of protection equipment with time tag)»** – упакованная информация о срабатывании пусковых органов защиты с меткой времени;

- **«19: M_EP_TC_1 (Packed output circuit information of protection equipment with time tag)»** – упакованная информация о срабатывании выходных цепей защиты с меткой времени;
- **«20: M_PS_NA_1 (Packed single point information with status change detection)»** – упакованная одноэлементная информация с определением изменения состояния;
- **«21: M_ME_ND_1 (Measured value, normalized value without quality descriptor)»** – значение измеряемой величины, нормализованное значение без описателя качества;
- **«30: M_SP_TB_1 (Single-point information with time tag CP56Time2a)»** – одноэлементная информация с меткой времени CP56time2a;
- **«31: M_DP_TB_1 (Double-point information with time tag CP56Time2a)»** – двухэлементная информация с меткой времени CP56time2a;
- **«32: M_ST_TB_1 (Step position information with time tag CP56Time2a)»** – информация о положении отпаек с меткой времени CP56time2a;
- **«33: M_BO_TB_1 (Bitstring of 32 bit with time tag CP56Time2a)»** – строка из 32 битов с меткой времени CP56time2a;
- **«34: M_ME_TD_1 (Measured value, normalized value with tag CP56Time2a)»** – значение измеряемой величины, нормализованное значение с меткой времени CP56time2a;
- **«35: M_ME_TE_1 (Measured value, scaled value with tag CP56Time2a)»** – значение измеряемой величины, масштабированное значение с меткой времени CP56time2a;
- **«36: M_ME_TF_1 (Measured value, short floating point number with time tag CP56Time2a)»** – значение измеряемой величины, короткий формат с плавающей запятой с меткой времени CP56time2a;
- **«37: M_IT_TB 1 (Integrated totals with time tag CP56Time2a)»** – интегральная сумма с меткой времени CP56time2a;
- **«38: M_EP_TD_1 (Event of protection equipment with time tag CP56Time2a)»** – информация о работе релейной защиты с меткой времени CP56time2a;
- **«39: M_EP_TE_1 (Packed start events of protection equipment with time tag CP56Time2a)»** – упакованная информация о срабатывании пусковых органов защиты с меткой времени CP56time2a;

- **«40: M_EP_TF_1 (Packed output circuit information of protection equipment with time tag CP56Time2a)»** – упакованная информация о срабатывании выходных цепей защиты с меткой времени CP56time2a;
- **«45: C_SC_NA_1 (Single command)»** – одноэлементная команда;
- **«46: C_DC_NA_1 (Double command)»** – двухэлементная команда;
- **«47: C_RC_NA_1 (Regulating step command)»** – команда пошагового регулирования;
- **«48: C_SE_NA_1 (Set-point Command, normalized value)»** – команда установки, нормализованное значение;
- **«49: C_SE_NB_1 (Set-point Command, scaled value)»** – команда установки, масштабированное значение;
- **«50: C_SE_NC_1 (Set-point Command, short floating point number)»** – команда установки, короткое число с плавающей запятой;
- **«51: C_BO_NA_1 (Bitstring 32 bit command)»** – строка из 32 битов;
- **«58: C_SC_TA_1 (Single command with tag CP56Time2a)»** – одноэлементная команда с меткой времени CP56time2a;
- **«59: C_DC_TA_1 (Double command with tag CP56Time2a)»** – двухэлементная команда с меткой времени CP56time2a;
- **«60: C_RC_TA_1 (Regulating step command with tag CP56Time2a)»** – команда пошагового регулирования с меткой времени CP56time2a;
- **«61: C_SE_TA_1 (Measured value, normalized value command with tag CP56Time2a)»** – команда установки, нормализованное значение с меткой времени CP56time2a;
- **«62: C_SE_TB_1 (Measured value, scaled value command with tag CP56Time2a)»** – команда установки, масштабированное значение с меткой времени CP56time2a;
- **«63: C_SE_TC_1 (Measured value, short floating point number command with time tag CP56Time2a)»** – команда установки, короткое число с плавающей запятой с меткой времени CP56time2a;
- **«64: C_BO_TA_1 (Bitstring 32 bit command with time tag CP56Time2a)»** – строка из 32 битов с меткой времени CP56time2a;
- **«70: M_EI_NA_1 (End of initialisation)»** – конец инициализации;
- **«100: C_IC_NA_1 (Interrogation command)»** – команда опроса;
- **«101: C_CI_NA_1 (Counter interrogation command)»** – команда опроса счётчика;

- **«102: C_RD_NA_1 (Read command)»** – команда считывания;
- **«103: C_CS_NA 1 (Clock synchronisation command)»** – команда синхронизации времени;
- **«104: C_TS_NA_1 (Test command)»** – команда тестирования;
- **«105: C_RP_NA_1 (Reset process command)»** – команда установки процесса в исходное состояние;
- **«106: C_CD_NA_1 (C_CD_NA_1 Delay acquisition command)»** – команда задержки получения;
- **«107: C_TS_TA_1 (Test command with time tag CP56Time2a)»** – команда тестирования с меткой времени CP56time2a;
- **«110: P_ME_NA_1 (Parameter of measured values, normalized value)»** – параметр измеряемой величины, нормализованное значение;
- **«111: P_ME_NB_1 (Parameter of measured values, scaled value»** – параметр измеряемой величины, масштабированное значение;
- **«112: P_ME_NC_1 (Parameter of measured value, short floating point number)»** – параметр измеряемой величины, короткий формат с плавающей запятой;
- **«113: P_AC_NA_1 (Parameter activation)»** – параметр активации;
- **«120: F_FR_NA_1 (File ready)»** – файл готов;
- **«121: F_SR_NA_1 (Section ready)»** – секция готова;
- **«122: F_SC_NA_1 (Call directory, select file, call file, call section)»** – вызов директории, выбор файла, вызов файла, вызов секции;
- **«123: F_LS_NA_1 (Last section, last segment)»** – последняя секция, последний сегмент;
- **«124: F_AF_NA_1 (ACK file, ACK section)»** – подтверждение файла, подтверждение секции;
- **«125: F_SG_NA_1 (Segment)»** – сегмент;
- **«126: F_DR_TA_1 (Directory)»** – директория;
- **«127: F_SC_NB_1 (QueryLog, request archive file)»** – архив запросов.

В поле параметра **«ASDU COT (причина передачи)»** доступны следующие причины передачи:

- **«Любой»**;
- **«1:COT_CYCLIC (Cyclic data)»**;

- **«2:COT_BACKGROUND (Background scan:)»**;
- **«3:COT_SPONTAN (Spontaneous data)»**;
- **«4:COT_INIT (End of initialization)»**;
- **«5:COT_REQ (Read request)»**;
- **«6:COT_ACT (Command activation)»**;
- **«7:COT_ACT_CON (Confirmation of command activation)»**;
- **«8:COT_DEACT (Command abortion)»**;
- **«9:COT_DEACT_CON (Confirmation of command abortion)»**;
- **«10:COT_ACT_TERM (Termination of command activation)»**;
- **«11:COT_RETREM (Response due to remote command)»**;
- **«12:COT_RETLOC (Response due to local command)»**;
- **«13:COT_FILE (File access)»**;
- **«14:COT_14»**;
- **«15:COT_15»**;
- **«16:COT_16»**;
- **«17:COT_17»**;
- **«18:COT_18»**;
- **«19:COT_19»**;
- **«20:COT_INROGEN (Station query (general))»**;
- **«21:COT_INRO1 (Station query for group 1)»**;
- **«22:COT_INRO2 (Station query for group 2)»**;
- **«23:COT_INRO3 (Station query for group 3)»**;
- **«24:COT_INRO4 (Station query for group 4)»**;
- **«25:COT_INRO5 (Station query for group 5)»**;
- **«26:COT_INRO6 (Station query for group 6)»**;
- **«27:COT_INRO7 (Station query for group 7)»**;
- **«28:COT_INRO8 (Station query for group 8)»**;
- **«29:COT_INRO9 (Station query for group 9)»**;
- **«30:COT_INRO10 (Station query for group 10)»**;
- **«31:COT_INRO11 (Station query for group 11)»**;

- **«32:COT_INRO12 (Station query for group 12)»**;
- **«33:COT_INRO13 (Station query for group 13)»**;
- **«34:COT_INRO14 (Station query for group 14)»**;
- **«35:COT_INRO15 (Station query for group 15)»**;
- **«36:COT_INRO16 (Station query for group 16)»**;
- **«37:COT_REQCOGEN (Counter query (general))»**;
- **«38:COT_REQCO1 (Counter query for group 1)»**;
- **«39:COT_REQCO2 (Counter query for group 2)»**;
- **«40:COT_REQCO3 (Counter query for group 3)»**;
- **«41:COT_REQCO4 (Counter query for group 4)»**;
- **«42:COT_42»**;
- **«43:COT_43»**;
- **«44:COT_UNKNOWN_TYPE (Unknown type)»**;
- **«45:COT_UNKNOWN_CAUSE (Unknown cause of transfer)»**;
- **«46:COT_UNKNOWN_ASDU_ADDRESS (Unknown common ASDU address)»**;
- **«47:COT_UNKNOWN_OBJECT_ADDRESS (Unknown object address)»**;
- **«48:COT_48»**;
- **«49:COT_49»**;
- **«50:COT_50»**;
- **«51:COT_51»**;
- **«52:COT_52»**;
- **«53:COT_53»**;
- **«54:COT_54»**;
- **«55:COT_55»**;
- **«56:COT_56»**;
- **«57:COT_57»**;
- **«58:COT_58»**;
- **«59:COT_59»**;
- **«60:COT_60»**;
- **«61:COT_61»**;

- **«62:COT_62»**;
- **«63:COT_63»**.

В поле параметра **«AD условие»** доступны следующие условия:

- **«Равно»**;
- **«Больше чем»**;
- **«Меньше чем»**;
- **«Отрицание»**;
- **«Побитовое И»**.

В поле параметра **«AD (ASDU адрес)»** возможно указание значения в диапазоне от «0» до «65535».

В поле параметра **«IOA (адрес объекта информации)»** возможно указание отрицательных или положительных значений.

В поле параметра **«Тип объекта»** доступны следующие значения:

- **«Нетипизированный»**;
- **«Типизированный»**.

При установке флажка для параметра **«Инвертировать IOA значение»** дополнительно появится параметр **«Инвертируемое IOA значение»**.

В поле параметра **«Инвертируемое IOA значение»** возможно указание отрицательного или положительного значения.

При выборе в поле параметра **«Тип ASDU»** значений «9: M_ME_NA_1 (Measured value, normalised value)», «10: M_ME_TA_1 (Measured value, normalised value with time tag)», «13: M_ME_NC_1 (Measured value, short floating point number)», «14: M_ME_TC_1 (Measured value, short floating point number with time tag)», «34: M_ME_TD_1 (Measured value, normalized value with tag CP56Time2a)», «36: M_ME_TF_1 (Measured value, short floating point number with time tag CP56Time2a)», «48: C_SE_NA_1 (Set-point Command, normalized value)», «50: C_SE_NC_1 (Set-point Command, short floating point number)», «61: C_SE_TA_1 (Measured value, normalized value command with tag CP56Time2a)», «63: C_SE_TC_1 (Measured value, short floating point number command with time tag CP56Time2a)», «110: P_ME_NA_1 (Parameter of measured values, normalized value)», «112: P_ME_NC_1 (Parameter of measured value, short floating point number)» и выборе в поле параметра **«Тип объекта»** значения «Нетипизированный» дополнительно появится параметр **«Вещественное IOA значение»**, а в случае установленного флажка для параметра **«Инвертировать IOA значение»** появится параметр **«Вещественное инвертируемое IOA значение»**.

В поле параметра **«Тип проверки»** доступны следующие значения:

- **«Отсутствует»**;
- **«CHECK_ANY (по крайней мере один из пакетов IEC соответствует сигнатуре)»**;
- **«CHECK_ONLY (все пакеты IEC соответствуют сигнатуре)»**.

При выборе значения «Типизированный» в поле параметра **«Тип объекта»** появится параметр **«Тип»**.

В поле параметра **«Тип»** доступны следующие значения:

- **«SIQ - Одноэлементная информация с описателем качества»**;
- **«QDS - Описатель качества (отдельный байт)»**;
- **«SP_QDS - Фильтрует SIQ»**;
- **«DP_QDS - Фильтрует DIQ»**;
- **«QDP - Описатель качества для сообщения о работе релейной защиты»**;
- **«SEP - Одиночное событие релейной защиты»**;
- **«OCI - Информация о выходных цепях»**;
- **«SINGLE_CMD - Фильтрует SCO»**;
- **«DOUBLE_CMD - Фильтрует DCO, RCO»**;
- **«QLF - Фильтрует QOS»**;
- **«QLF_COUNTER - Фильтрует QCC»**;
- **«QLF_MEASURED - Фильтрует QPB»**;
- **«CP16TIME - Фильтрует time_elapsed, delay»**;
- **«CP24TIME - Фильтрует time»**;
- **«CP56TIME - Фильтрует time»**;
- **«CP56TIME_BEGIN - Фильтрует time_begin»**;
- **«CP56TIME_END - Фильтрует time_end»**;
- **«VTI - Фильтрует VTI»**;
- **«COI - Фильтрует COI»**;
- **«FILE - Фильтрует NOF, section_name, SOF, CHS, FRQ, SRQ, SCQ, LSQ, AFQ»**;
- **«SEP_SINGLE - Фильтрует SEP»**.

При выборе в поле параметра **«Тип»** значения «SIQ - Одноэлементная информация с описателем качества» дополнительно появятся параметры **«SIQ условие»** и **«SIQ значение»**.

В полях параметров **«SIQ условие»**, **«QDP условие»**, **«SEP условие»**, **«OCI условие»** доступны следующие значения:

- **«Равно»**;
- **«Больше чем»**;
- **«Меньше чем»**;
- **«Отрицание»**;
- **«Побитовое И»**.

В поле параметра **«SIQ значение»** доступны следующие значения:

- **«SPI»**;
- **«BL»**;
- **«SB»**;
- **«NT»**;
- **«IV»**.

При выборе в поле параметра **«Тип»** значений «QDS - Описатель качества (отдельный байт)» дополнительно появится параметр **«QDS значение»**.

В поле параметра **«QDS значение»** доступны следующие значения:

- **«OV»**;
- **«BL»**;
- **«SB»**;
- **«NT»**;
- **«IV»**.

При выборе в поле параметра **«Тип»** значений «SP_QDS - Фильтрует SIQ» дополнительно появится параметр **«SP_QDS значение»**.

В поле параметра **«SP_QDS значение»** доступны следующие значения:

- **«SP»**;
- **«BL»**;
- **«SB»**;
- **«NT»**;
- **«IV»**.

При выборе в поле параметра **«Тип»** значения «DP_QDS - Фильтрует DIQ» дополнительно появятся параметры **«DP_QDS значение»** и **«DP_QDS DP значение»**.

В поле параметра **«DP_QDS значение»** доступны следующие значения:

- **«BL»**;
- **«SB»**;
- **«NT»**;
- **«IV»**.

В поле параметра **«DP_QDS DP значение»** возможно указать число от «0» до «3» или диапазон чисел от «0» до «3» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «QDP - Описатель качества для сообщения о работе релейной защиты» дополнительно появятся параметры **«QDP условие»** и **«QDP значение»**.

В полях параметров **«QDP значение»** и **«SEP значение»** доступны следующие значения:

- **«EI»**;
- **«BL»**;
- **«SB»**;
- **«NT»**;
- **«IV»**.

При выборе в поле параметра **«Тип»** значения «SEP - Одиночное событие релейной защиты» дополнительно появятся параметры **«SEP условие»**, **«SEP ES»** и **«SEP значение»**.

В поле параметра **«SEP ES»** доступны следующие значения:

- **«0 - not used»**;
- **«1 - disabled»**;
- **«2 - enabled»**;
- **«3 - not used»**.

При выборе в поле параметра **«Тип»** значения «OCI - Информация о выходных цепях» дополнительно появятся параметры **«OCI условие»** и **«OCI значение»**.

В поле параметра **«OCI значение»** доступны следующие значения:

- **«CL3»**;
- **«CL2»**;

- **«CL1»**;
- **«GC»**.

При выборе в поле параметра **«Тип»** значения «SINGLE_CMD - Фильтрует SCO» дополнительно появятся параметры **«SINGLE_CMD ST значение»**, **«SINGLE_CMD QL значение»** и **«SINGLE_CMD значение»**.

В поле параметра **«SINGLE_CMD ST значение»** возможно указать число от «0» до «3» или диапазон чисел от «0» до «3» при установке флажка напротив параметра.

В поле параметра **«SINGLE_CMD QL значение»** возможно указать число от «0» до «31» или диапазон чисел от «0» до «31» при установке флажка напротив параметра.

В полях параметров **«SINGLE_CMD значение»**, **«DOUBLE_CMD значение»**, **«QLF значение»** доступны следующие значения:

- **«Отсутствует»**;
- **«SE»**.

При выборе в поле параметра **«Тип»** значения «DOUBLE_CMD - Фильтрует DCO, RCO» дополнительно появятся параметры **«DOUBLE_CMD ST значение»**, **«DOUBLE_CMD QL значение»** и **«DOUBLE_CMD значение»**.

В поле параметра **«DOUBLE_CMD ST значение»** возможно указать число от «0» до «3» или диапазон чисел от «0» до «3» при установке флажка напротив параметра.

В поле параметра **«DOUBLE_CMD QL значение»** возможно указать число от «0» до «31» или диапазон чисел от «0» до «31» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «QLF - Фильтрует QOS» дополнительно появятся параметры **«QLF QL значение»** и **«QLF значение»**.

В поле параметра **«QLF QL значение»** возможно указать число от «0» до «127» или диапазон чисел от «0» до «127» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «QLF_COUNTER - Фильтрует QCC» дополнительно появятся параметры **«QLF_COUNTER QL значение»** и **«QLF_COUNTER FR значение»**.

В поле параметра **«QLF_COUNTER QL значение»** возможно указать число от «0» до «63» или диапазон чисел от «0» до «63» при установке флажка напротив параметра.

В поле параметра **«QLF_COUNTER FR значение»** возможно указать число от «0» до «3» или диапазон чисел от «0» до «3» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «QLF_MEASURED - Фильтрует QPB» дополнительно появятся параметры **«QLF_MEASURED значение»** и **«QLF_MEASURED KIND значение»**.

В поле параметра **«QLF_MEASURED значение»** доступны следующие значения:

- **«LPC»**;
- **«POP»**.

В поле параметра **«QLF_MEASURED KIND значение»** возможно указать число от «0» до «63» или диапазон чисел от «0» до «63» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «CP16TIME - Фильтрует time_elapsed, delay» дополнительно появится параметр **«CP16TIME MS значение»**.

В полях параметров **«CP16TIME MS значение»**, **«CP24TIME MS значение»**, **«CP56TIME MS значение»** возможно указать число от «0» до «59999» или диапазон чисел от «0» до «59999» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «CP24TIME - Фильтрует time» дополнительно появятся параметры **«CP24TIME MS значение»** и **«CP24TIME MIN значение»**.

В полях параметров **«CP24TIME MIN значение»**, **«CP56TIME MIN значение»** возможно указать число от «0» до «59» или диапазон чисел от «0» до «59» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «CP56TIME - Фильтрует time» дополнительно появятся параметры **«CP56TIME MS значение»**, **«CP56TIME MIN значение»**, **«CP56TIME HOUR значение»**, **«CP56TIME значение»**, **«CP56TIME DAY значение»**, **«CP56TIME DOW значение»**, **«CP56TIME MONTH значение»** и **«CP56TIME YEAR значение»**.

В полях параметров **«CP56TIME HOUR значение»**, **«CP56TIME MIN значение»** возможно указать число от «0» до «23» или диапазон чисел от «0» до «23» при установке флажка напротив параметра.

В полях параметров **«CP56TIME значение»**, **«CP56TIME_BEGIN значение»** доступны следующие значения:

- **«Отсутствует»**;
- **«SU»**.

В полях параметров **«CP56TIME DAY значение»**, **«CP56TIME_BEGIN DAY значение»**, **«CP56TIME_END DAY значение»** возможно указать число от «0» до «31» или диапазон чисел от «0» до «31» при установке флажка напротив параметра.

В полях параметров **«CP56TIME DOW значение»**, **«CP56TIME_BEGIN DOW значение»**, **«CP56TIME_END DOW значение»** возможно указать число от «0» до «7» или диапазон чисел от «0» до «7» при установке флажка напротив параметра.

В полях параметров **«CP56TIME MONTH значение»**, **«CP56TIME_BEGIN MONTH значение»**, **«CP56TIME_END MONTH значение»** возможно указать число от «0» до «12» или диапазон чисел от «0» до «12» при установке флажка напротив параметра.

В полях параметров **«CP56TIME YEAR значение»**, **«CP56TIME_BEGIN YEAR значение»**, **«CP56TIME_END YEAR значение»** возможно указать число от «0» до «99» или диапазон чисел от «0» до «99» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «CP56TIME_BEGIN - Фильтрует time_begin» дополнительно появятся параметры **«CP56TIME_BEGIN MS значение»**, **«CP56TIME_BEGIN MIN значение»**, **«CP56TIME_BEGIN HOUR значение»**, **«CP56TIME_BEGIN значение»**, **«CP56TIME_BEGIN DAY значение»**, **«CP56TIME_BEGIN DOW значение»**, **«CP56TIME_BEGIN MONTH значение»** и **«CP56TIME_BEGIN YEAR значение»**.

В полях параметров **«CP56TIME_BEGIN MS значение»**, **«CP56TIME_END MS значение»** возможно указать число от «0» до «59999» или диапазон чисел от «0» до «59999» при установке флажка напротив параметра.

В полях параметров **«CP56TIME_BEGIN MIN значение»**, **«CP56TIME_END MIN значение»** возможно указать число от «0» до «59» или диапазон чисел от «0» до «59» при установке флажка напротив параметра.

В полях параметров **«CP56TIME_BEGIN HOUR значение»**, **«CP56TIME_END HOUR значение»** возможно указать число от «0» до «23» или диапазон чисел от «0» до «23» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «CP56TIME_END - Фильтрует time_end» дополнительно появятся параметры **«CP56TIME_END MS значение»**, **«CP56TIME_END HOUR значение»**, **«CP56TIME_END значение»**, **«CP56TIME_END DAY значение»**, **«CP56TIME_END DOW значение»**, **«CP56TIME_END MONTH значение»** и **«CP56TIME_END YEAR значение»**.

При выборе в поле параметра **«Тип»** значения «VTI - Фильтрует VTI» дополнительно появятся параметры **«VTI значение»** и **«VTI VAL значение»**.

В поле параметра **«VTI значение»** доступны следующие значения:

- **«Отсутствует»**;
- **«T»**.

В поле параметра **«VTI VAL значение»** возможно указать отрицательное или положительное число от «-64» до «63» или диапазон чисел от «-64» до «63» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «COI - Фильтрует COI» дополнительно появятся параметры **«COI значение»** и **«COI CAUSE значение»**.

В поле параметра **«COI значение»** доступны следующие значения:

- **«Отсутствует»**;
- **«CHANGED»**.

В поле параметра **«COI CAUSE значение»** возможно указать число от «0» до «127» или диапазон чисел от «0» до «127» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «FILE - Фильтрует NOF, section_name, SOF, CHS, FRQ, SRQ, SCQ, LSQ, AFQ» дополнительно появятся следующие параметры:

- **«FILE NAME значение»**;
- **«FILE SECTION_NAME значение»**;
- **«FILE STATE значение»**;
- **«FILE CHECKSUM значение»**;
- **«FILE QL значение»**.

В поле параметра **«FILE NAME значение»** возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

В полях параметров **«FILE SECTION_NAME значение»**, **«FILE STATE значение»**, **«FILE CHECKSUM значение»**, **«FILE QL значение»** возможно указать число от «0» до «255» или диапазон чисел от «0» до «255» при установке флажка напротив параметра.

При выборе в поле параметра **«Тип»** значения «SEP_SINGLE - Фильтрует SEP» дополнительно появятся параметры **«SEP_SINGLE значение»** и **«SEP_SINGLE ES значение»**.

В поле параметра **«SEP_SINGLE значение»** доступны следующие значения:

- **«EL»**;
- **«BL»**;
- **«SB»**;
- **«NT»**;
- **«IV»**.

В поле параметра **«SEP_SINGLE ES значение»** возможно указать число от «0» до «3» или диапазон чисел от «0» до «3» при установке флажка напротив параметра.

При выборе опции **«APCI (управляющая информация прикладного уровня)»** появится параметр **«Формат»**, в котором доступны следующие значения:

- **«Любой»**;

- **«U-format (ненумерованные функции управления)»** – функции управления без нумерации;
- **«S-format (пронумерованные надзорные функции)»** – функции контроля с нумерацией.

При выборе в поле параметра **«Формат»** значения «U-format (ненумерованные функции управления)» дополнительно появятся параметры **«Функция U-формата»** и **«Статус функции U-формата»**.

В поле параметра **«Функция U-формата»** доступны следующие значения:

- **«Любая U-формат функция»**;
- **«TESTFR (тестовый блок)»**;
- **«старт передачи данных»**;
- **«STOPDT (прекращение передачи данных)»**.

В поле параметра **«Статус функции U-формата»** доступны следующие значения:

- **«act (активация)»**;
- **«con (подтверждение)»**.

При выборе в поле параметра **«Формат»** значения «S-format (пронумерованные надзорные функции)» дополнительно появится параметр **«RX»**.

В поле параметра **«RX»** возможно указать число от «0» до «65534» или диапазон чисел от «0» до «65534» при установке флажка напротив параметра.

5.5.3.2.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Создание правила СОВ) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «IEC 104»;
- **«Использовать шаблон»** – «IEC 104»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «IEC 104»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»;
- **«Функция приложения»** – «ASDU (блок данных прикладного уровня)»;
- **«Тип ASDU»** – «45:C_SC_NA_1 (Single command)»;
- **«IOA (адрес объекта информации)»** – установить флажок, «от 1 до 1».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.2.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола IEC 104 на ПК **«Server»** должен быть установлен эмулятор протокола IEC 104 – ПО «IECServer», а на ПК **«Client»** – ПО «QTester104». Для проверки правила СОВ необходимо выполнить следующие действия:

1. Запустить ПО «IECServer».
2. В выпадающем списке выбрать «C_SC_NA» и дважды нажать **кнопку «Add»**, а затем нажать **кнопку «StartServer»** (см. Рисунок – Запуск IECServer).

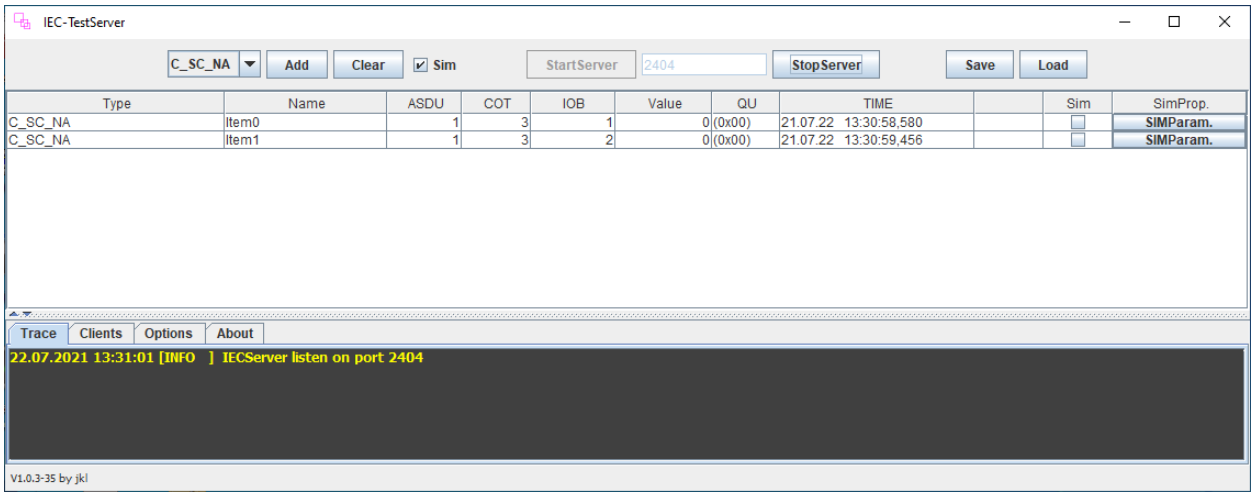


Рисунок – Запуск IECServer

3. Запустить ПО «QTester104», указать в поле **«Remote IP Address»** значение «192.168.1.200» и нажать **кнопку «Connect»** для подключения к ПО «IECServer» (см. Рисунок – Подключение к серверу в QTester104).

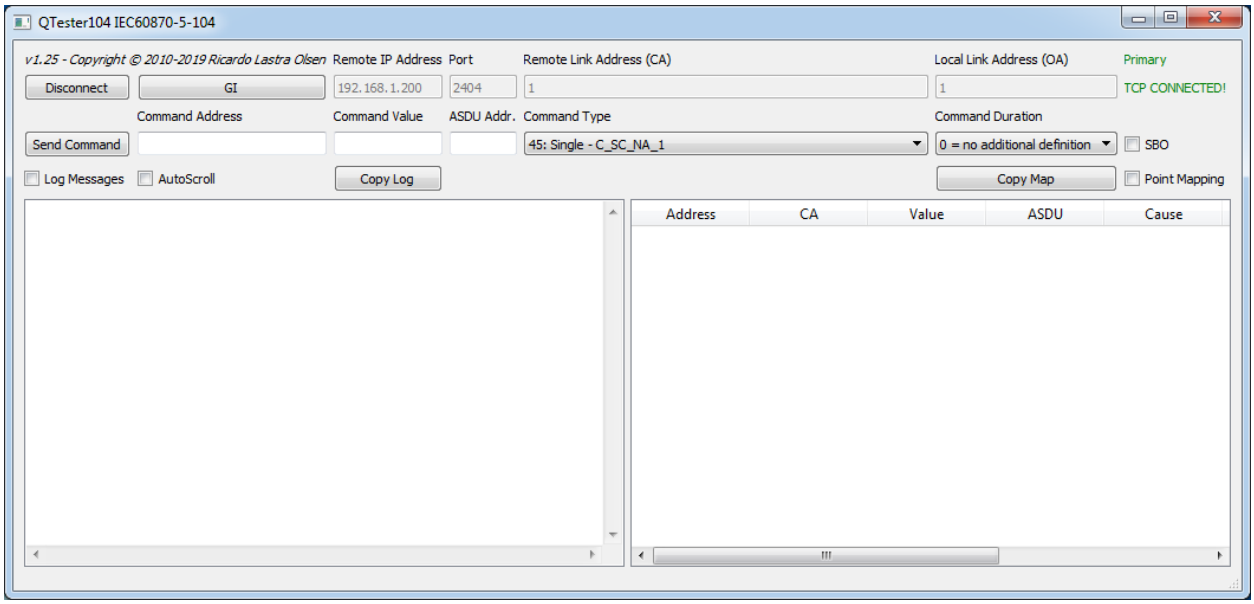


Рисунок – Подключение к серверу в QTester104

4. Задать следующие значения в полях (см. Рисунок – Настройка значений в QTester104):
   - **«Command Address»** – 1;
   - **«Command Value»** – 2;
   - **«ASDU Addr.»** – 1.
5. Нажать **кнопку «Send Command»** для отправки команды на сервер.

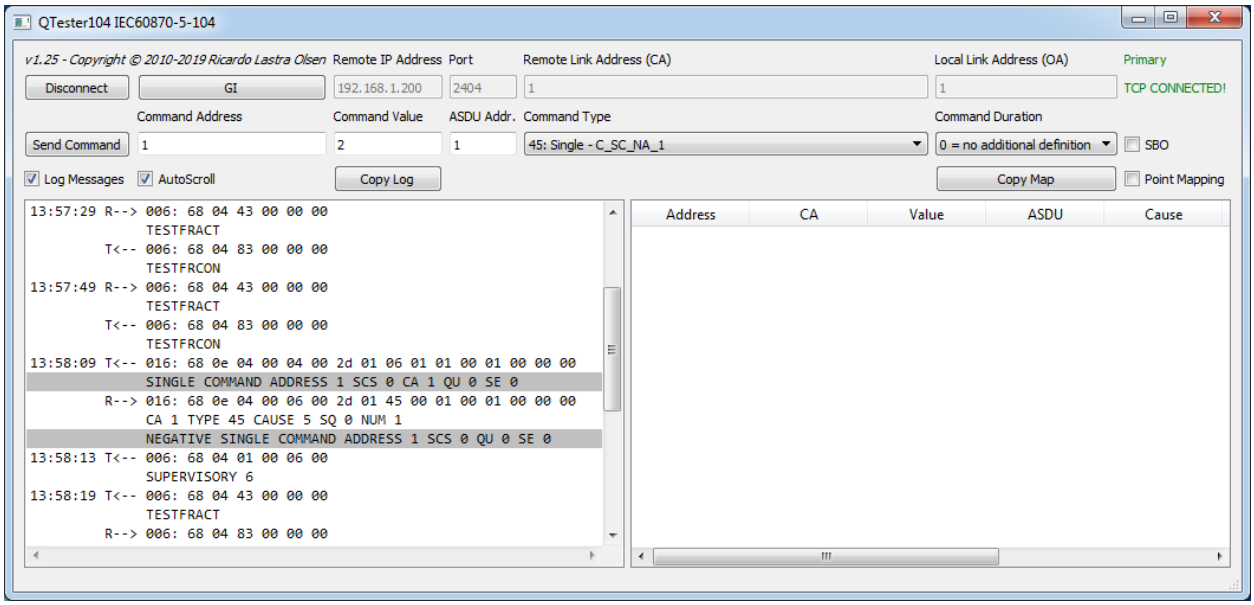


Рисунок – Настройка значений в QTester104

6. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

- «IEC 104» (см. Рисунок – Детальная информация, протокол IEC 104).

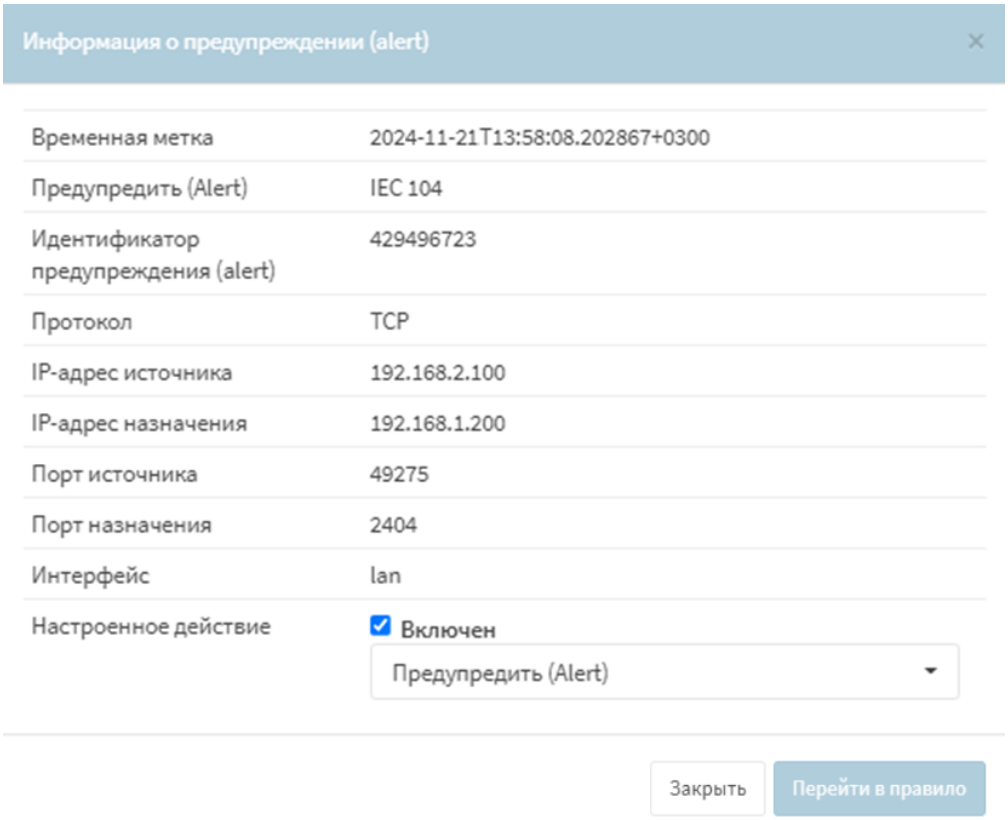


Рисунок – Детальная информация, протокол IEC 104

5.5.3.3 Шаблон протокола S7comm

При создании пользовательского правила на основе шаблона промышленного протокола S7comm 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.

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
SI (System info)	Системная информация
SF (System flags)	Системные флаги
AI (Analog inputs)	Аналоговый ввод
AO (Analog outputs)	Аналоговый вывод
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:

- **«BIT»**;
- **«BYTE»**;
- **«CHAR»**;
- **«WORD»**;
- **«INT»**;
- **«DWORD»**;
- **«DINT»**;
- **«REAL»**;
- **«DATE»**;
- **«TOD»**;
- **«TIME»**;
- **«S5TIME»**;
- **«DATETIME»**;
- **«COUNTER»**;
- **«TIMER»**;
- **«IECTIMER»**;
- **«IECCOUNTER»**;
- **«HSCOUNTER»**.

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 целочисленное значение в шестнадцатеричной системе счисления в формате «0x000000».

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.

При выборе в поле параметра **«Тип блока»** любого значения, кроме значения «Любой», появятся параметры **«Номер блока»** и **«Целевая файловая система»**.

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:

- **«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.

5.5.3.3.1 Пример создания правила COB

Необходимо создать пользовательское правило (см. Создание правила COB) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «S7comm»;
- **«Использовать шаблон»** – «S7comm»;
- **«Действие»** – «Отклонить (Reject)»;
- **«Сообщение»** – «S7comm»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»
- **«Тип сообщения»** – «JOBREQUEST»;
- **«Функция»** – «PLCSTOP».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.3.2 Проверка созданного правила COB

Для проверки срабатывания пользовательского правила на основе шаблона протокола S7comm на ПК **«Server»** должно быть установлено ПО «Snap7 Server Demo», а на ПК **«Client»** – ПО «Snap7 Client Demo».

Для проверки правила COB необходимо выполнить следующие действия:

1. В ПО «Snap7 Server Demo», в поле **«Local Address»** ввести «192.168.1.200» и нажать **кнопку «Start»** (см. Рисунок – Запуск ПО «Snap7 Server Demo») для локального запуска сервиса.

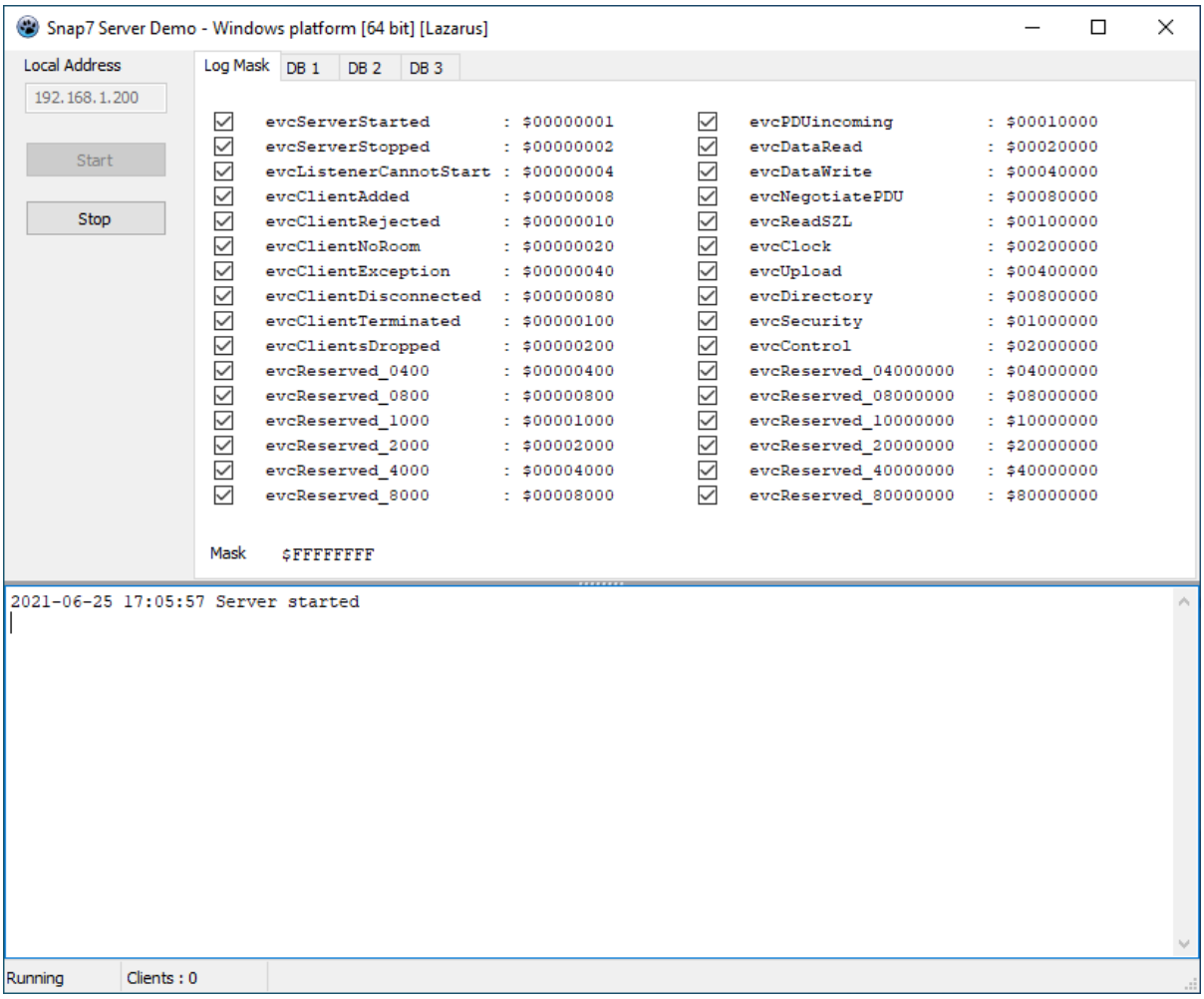


Рисунок – Запуск ПО «Snap7 Server Demo»

2. Запустить ПО «Snap7 Client Demo», в поле **«IP»** ввести «192.168.1.200» и нажать **кнопку «Connect»** для подключения к «Snap7 Server Demo».
3. Убедиться, что во вкладке **«System info»** отображается информация о контроллере (см. Рисунок – Запуск ПО «Snap7 Client Demo»).

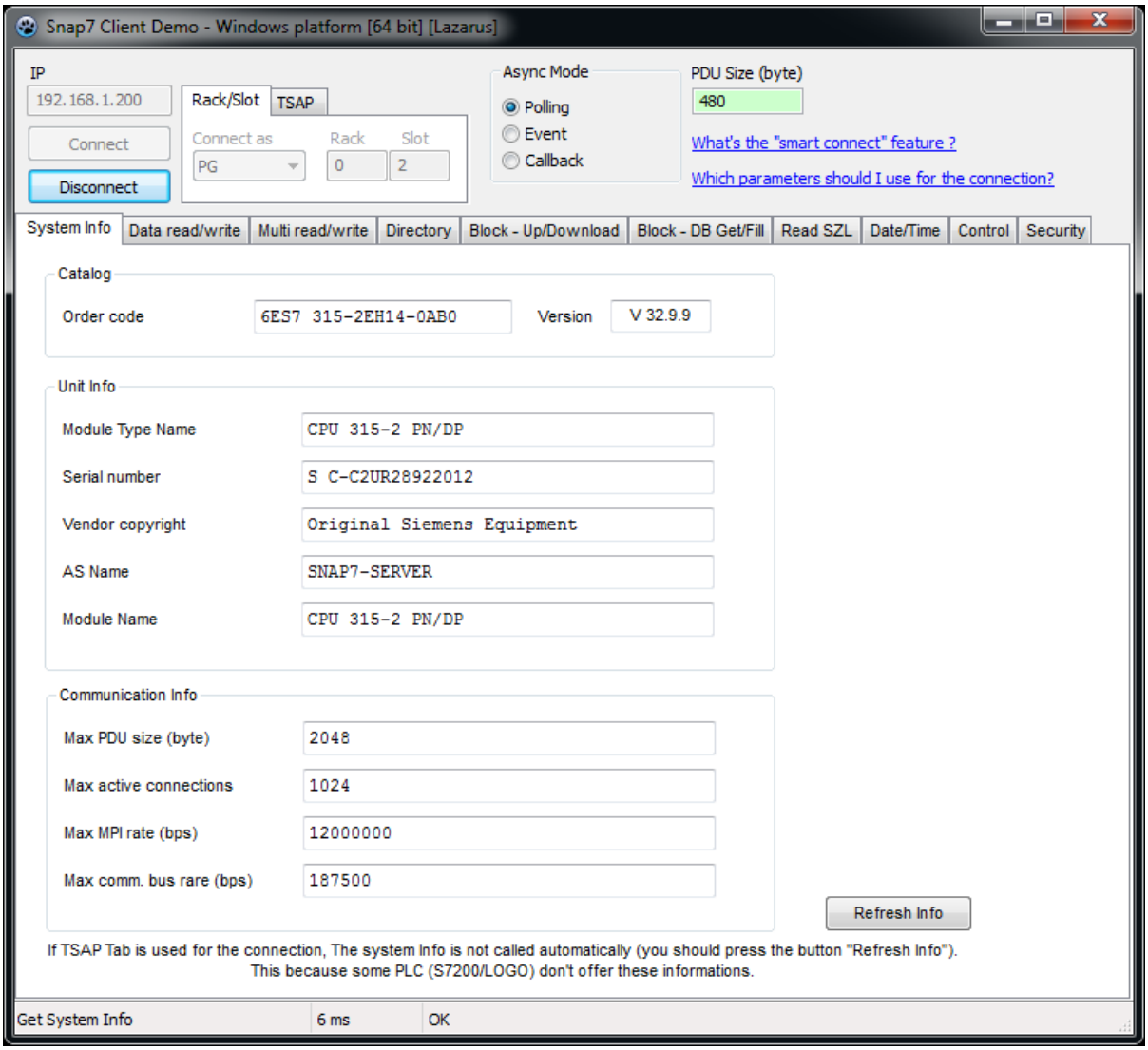


Рисунок – Запуск ПО «Snap7 Client Demo»

4. Произвести запись в регистр, для этого перейти во вкладку **«Data read/write»**, ввести в регистр «0000/00» значение «1» и нажать **кнопку «Write»** (см. Рисунок – Запись в регистр «0000/00»).

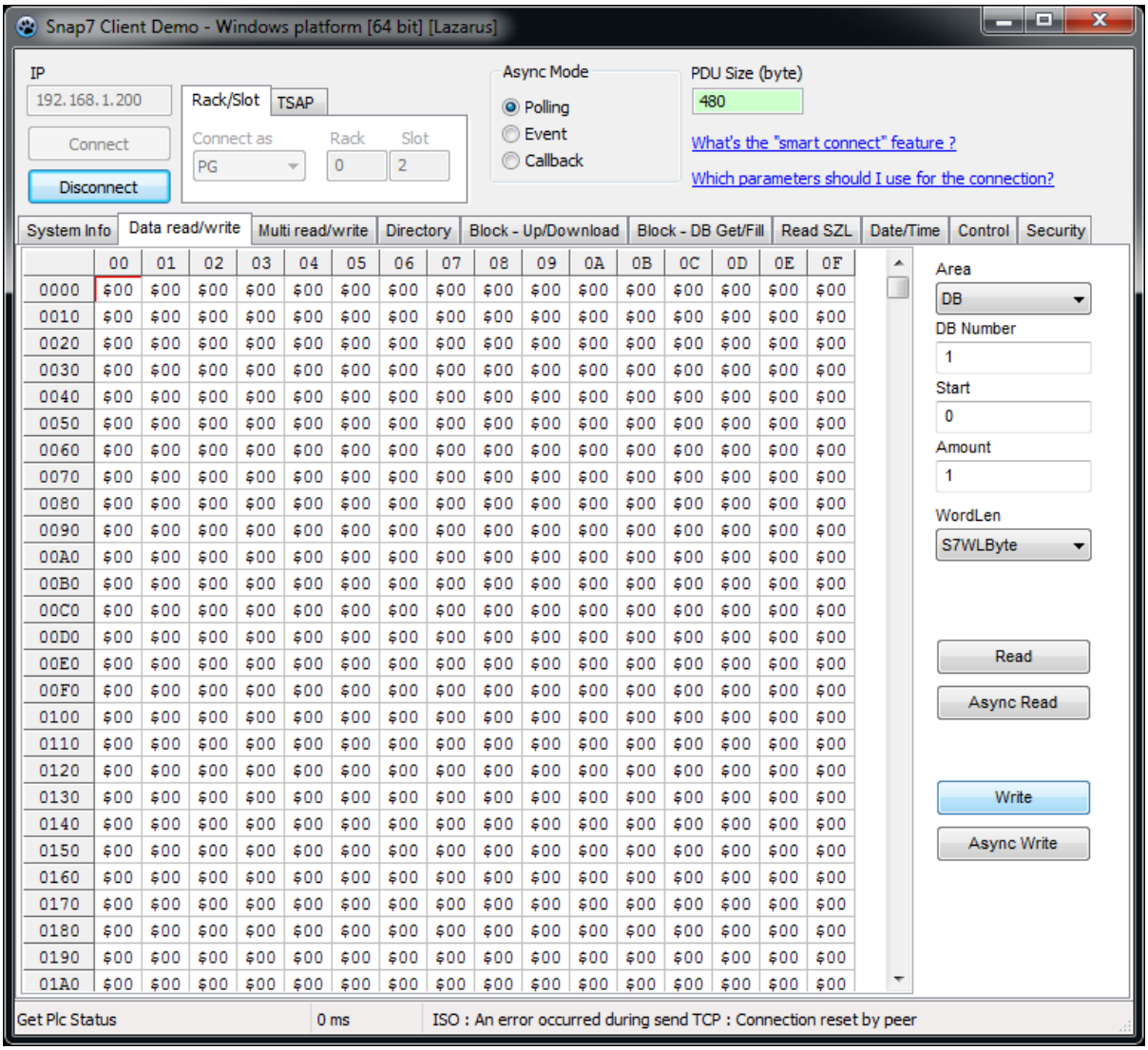


Рисунок – Запись в регистр «0000/00»

5. Перейти во вкладку **«Control»**, нажать **кнопку «Stop»** для остановки работы контроллера и убедиться в изменении индикации с «RUN» на «Unknown» и недоступности **кнопки «Get status»** (см. Рисунок – Отключение контроллера).

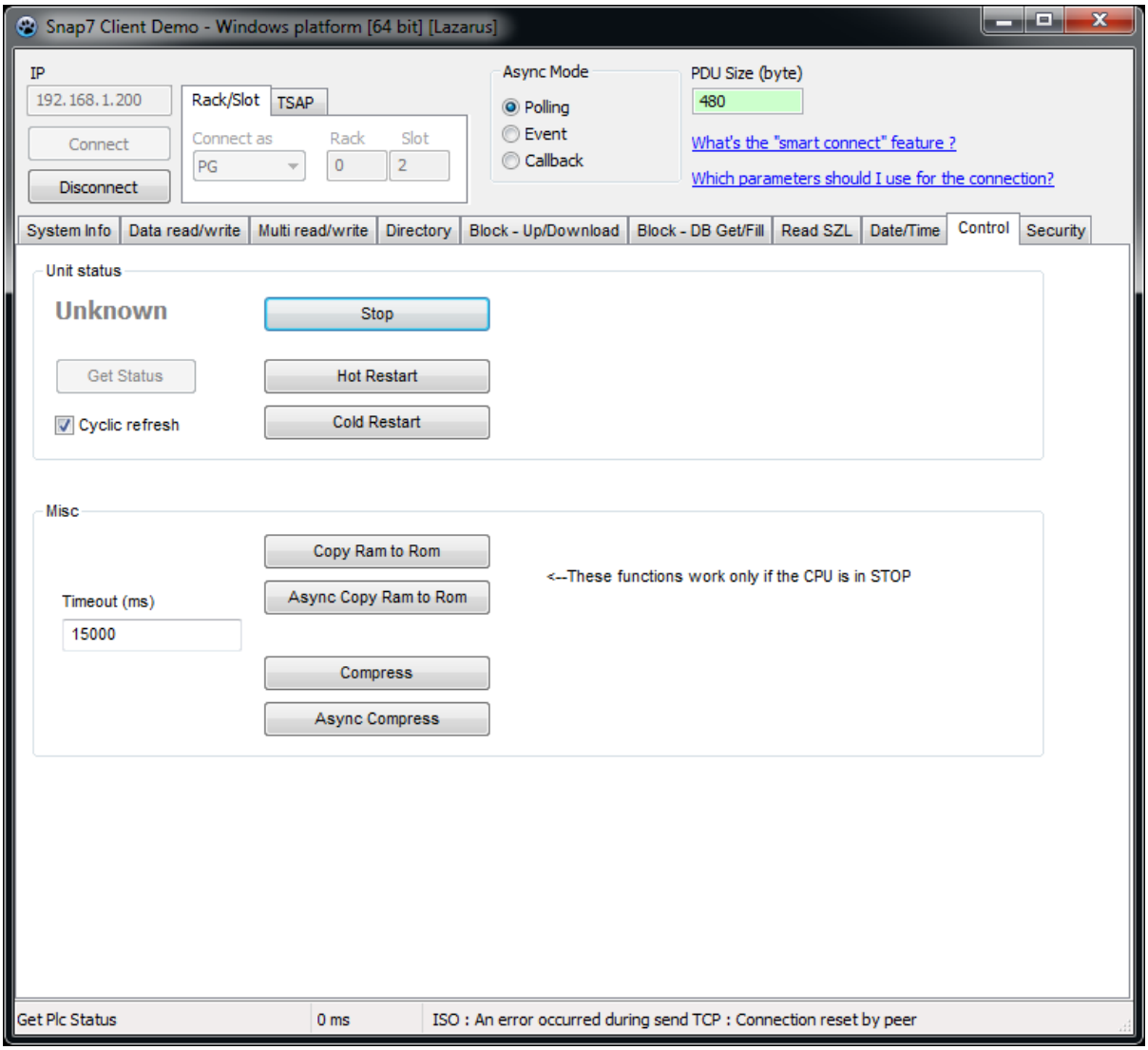


Рисунок – Отключение контроллера

6. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
   - «S7Comm» (см. Рисунок – Детальная информация, протокол S7comm).

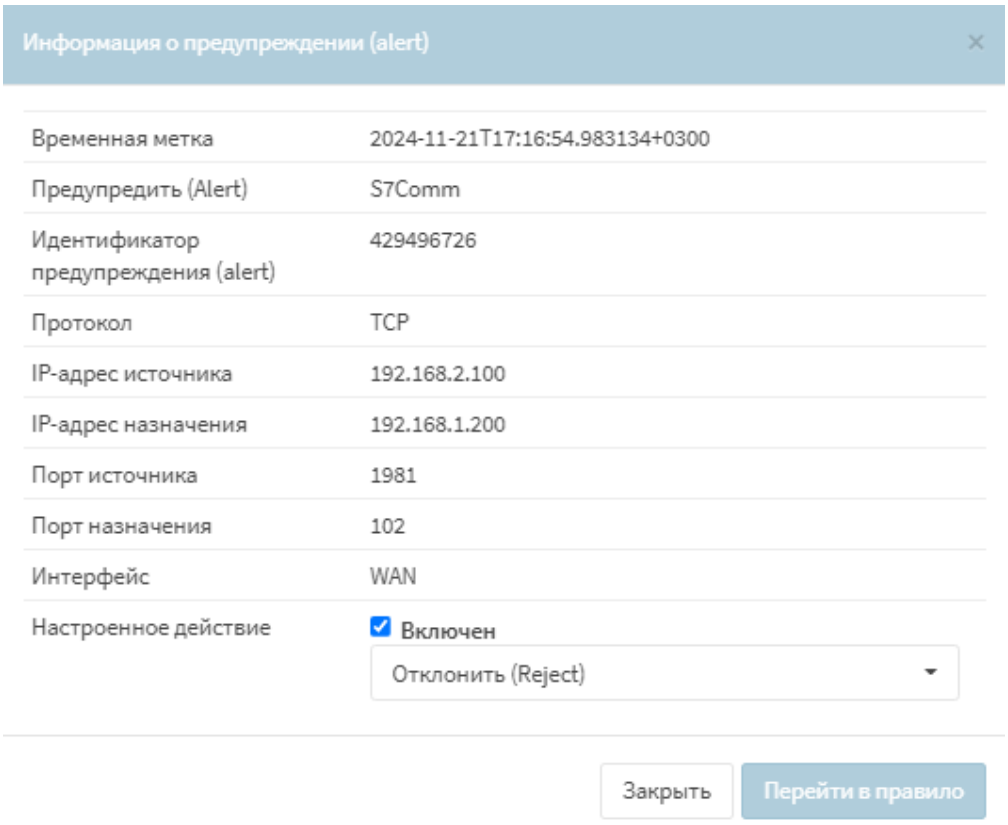


Рисунок – Детальная информация, протокол S7comm

5.5.3.4 Шаблон протокола S7comm Plus

При создании пользовательского правила на основе шаблона промышленного протокола S7comm 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»**;
- **«RESPONSE»**;
- **«NOTIFY»**;
- **«RESPONSE2»**.

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

- **«CONNECT»**;

- **«DATA»**;
- **«DATAW1_5»**;
- **«KEEPALIVE»**;
- **«EXT_KEEPALIVE»**.

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

- **«Отсутствует»**;
- **«EXPLORE»**;
- **«CREATEOBJECT»**;
- **«DELETEOBJECT»**;
- **«SETVARIABLE»**;
- **«GETLINK»**;
- **«SETMULTIVAR»**;
- **«GETMULTIVAR»**;
- **«BEGINSEQUENCE»**;
- **«ENDSEQUENCE»**;
- **«INVOKE»**;
- **«GETVARSUBSTR»**.

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

5.5.3.5 Шаблон протокола OPC DA

При создании пользовательского правила на основе шаблона промышленного протокола OPC DA 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 типы сообщений, указанных в таблице (см. Таблица «Типы сообщений OPC DA»).

Таблица «Типы сообщений OPC DA»

Тип сообщения	Описание
REQUEST	Сообщение запроса на операцию
PING	Сообщение запроса обратного вызова

Тип сообщения	Описание
RESPONSE	Сообщение ответа
FAULT	Сообщение сбоя
WORKING	Сообщение подтверждающее, что все исходящие пакеты получены
NOCALL	Ответ на команду PING
REJECT	Сообщение отклонения пакета
ACK	Подтверждение получения ответа
CI_CANCEL	Отмена операции
FACK	Если состояние вызова не STATE_SEND_FRAGS, отбросить пакет
CANCEL_ACK	Подтверждение отмены операции
BIND	Установка сессии
BIND_ACK	Подтверждение установки сессии
BIND_NACK	Отказ в установке сессии с выбранными параметрами
ALTER_CONTEXT	Изменение параметров сессии
ALTER_CONTEXT_RESP	Подтверждение изменения параметров сессии
SHUTDOWN	Сброс соединения
AUTH3	Обновление авторизации пользователя
CO_CANCEL	Передача команды отмены
ORPHANED	Флаг невозможности отмены операции

При выборе типа сообщения «REQUEST» появятся параметры **«Идентификатор вызываемого интерфейса»** и **«Номер вызываемой функции объекта»**.

Пользовательские правила для протокола OPC DA возможно создать для действий над тегами и для заранее определённого UUID.

Набор заранее определённых UUID конечен и добавлен в **ARMA FW** в соответствии со спецификацией протокола OPC DA.

При выборе в параметре **«Фильтровать на основе протокола»** опции «Операция над тегом» появятся следующие параметры:

- **«Операция над тегом»**;
- **«Полный путь к тегу(-ам)»**.

Параметр **«Операция над тегом»** содержит выпадающий список со значениями:

- **«Считать»**;
- **«Записать»**.

5.5.3.5.1 Пример создания правила СОВ

В качестве примера будет рассмотрено детектирование чтения тега «Integer_1» и выполнение функции номер «3» UUID «IOPCItemMgt».

Необходимо создать пользовательские правила (см. Создание правила СОВ) для детектирования действия над тегом и детектирования выполнения функции с заданным UUID.

Для детектирования действия над тегом при создании правила необходимо указать следующие параметры правила:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «Test.Folder.Integer_1 Read»;
- **«Использовать шаблон»** – «OPC DA»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «Test.Folder.Integer_1 Read»;
- **«Фильтровать на основе протокола»** – «Операция над тегом»;
- **«Операция над тегом»** – «Считать»;
- **«Полный путь к тегу(-ам)»** – «Test.Folder.Integer_1». Данный параметр содержит в себе имя тега и все каталоги по пути к нему, разделённые точками.

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**.

Для детектирования выполнения функции UUID при создании правила необходимо указать следующие параметры правила:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «OPC DA IOPCItemMgt»;
- **«Использовать шаблон»** – «OPC DA»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «OPC DA IOPCItemMgt»;
- **«Фильтровать на основе протокола»** – «Дополнительные параметры»;
- **«Тип сообщения»** – «REQUEST»;

- **«Идентификатор вызываемого интерфейса»** – «[OPC DA] IOPCItemMgt»;
- **«Номер вызываемой функции объекта»** – «3». В случае, если данный параметр оставить пустым предупреждение будет сформировано для любой вызываемой функции UUID.

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.5.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательских правила на основе шаблона протокола OPC DA на ПК **«Server»** должен быть установлен и запущен эмулятор протокола OPC DA – «OPC DA Server», на ПК **«Client»** – «OPCtools».

Порядок проверки срабатывания пользовательских правил:

1. Запустить ПО «OPCtools» и выполнить подключение к серверу «OPC DA».
2. Выполнить чтение тега «Integer_1» (см. Рисунок – Чтение тега «Integer_1» в ПО «OPCtools»).

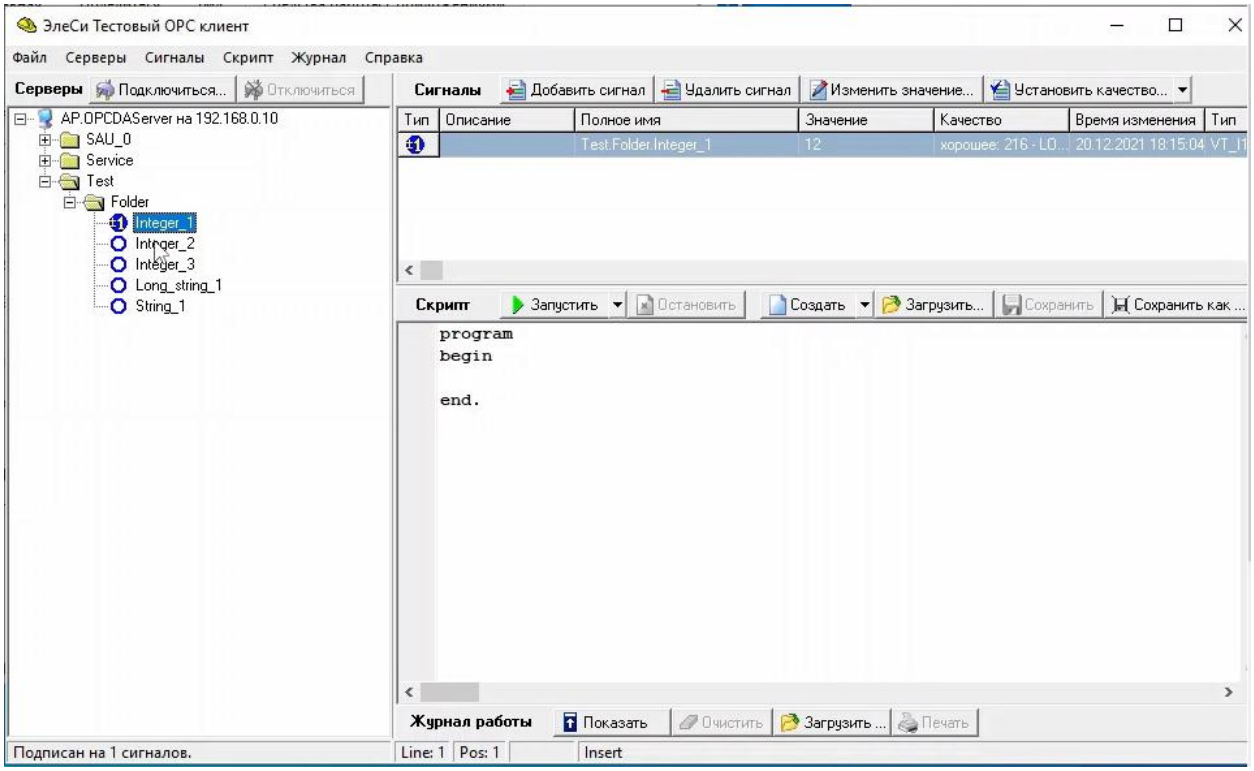


Рисунок – Чтение тега «Integer_1» в ПО «OPCtools»

3. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

- **«Test.Folder.Integer_1 Read»** – для действия с тегом (см. Рисунок – Детальная информация, протокол OPC DA – чтение тега);
- **«OPC DA IOPCItemMgt»** – для вызова функции UUID. (см. Рисунок – Детальная информация, протокол OPC DA – вызов функции).

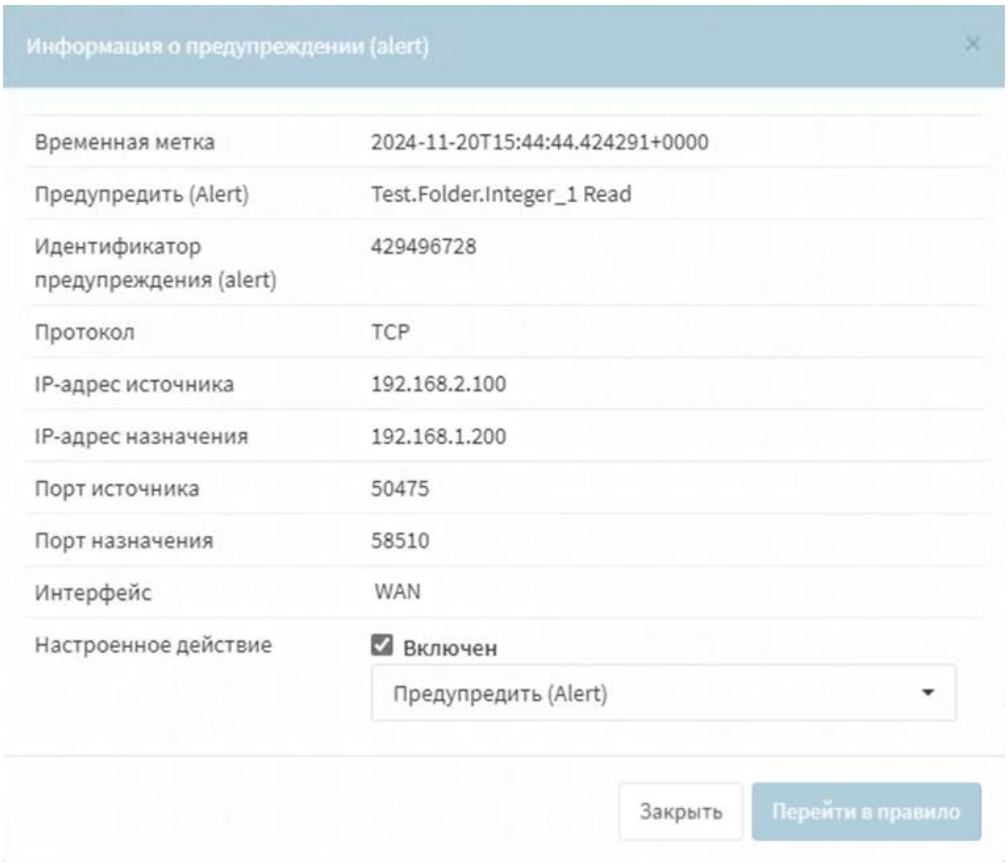


Рисунок – Детальная информация, протокол OPC DA – чтение тега

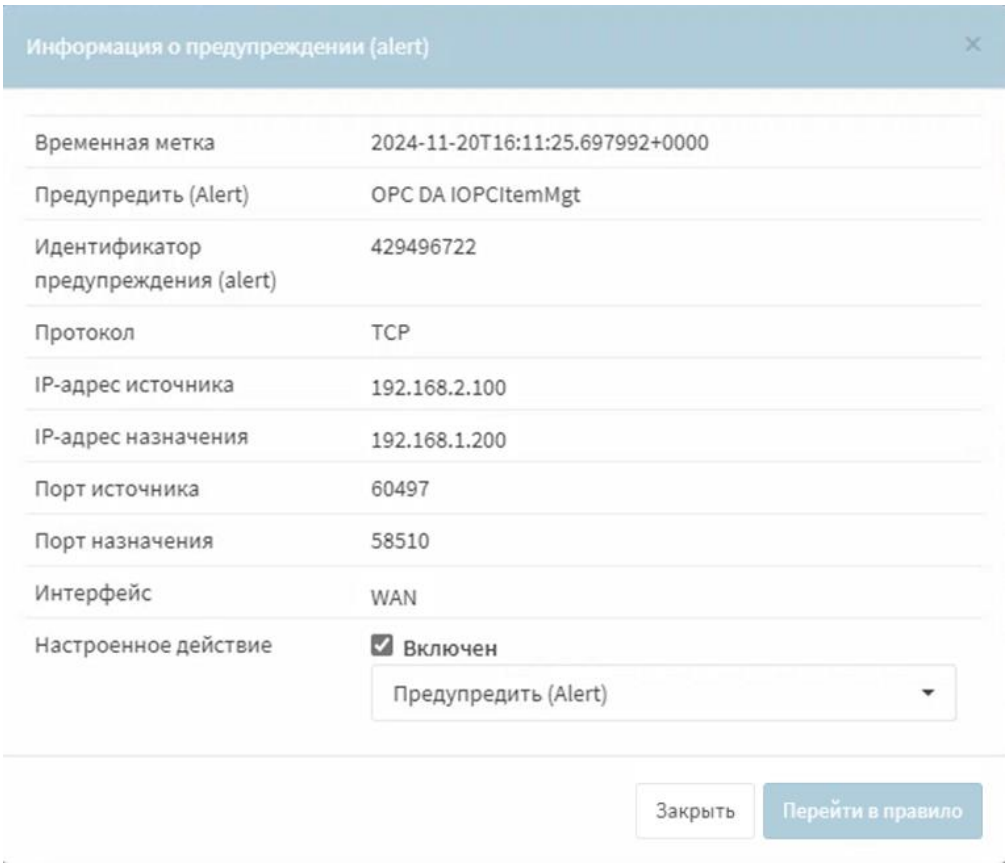


Рисунок – Детальная информация, протокол OPC DA – вызов функции

5.5.3.6 Шаблон протокола OPC UA

При создании пользовательского правила на основе шаблона промышленного протокола OPC UA 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»** доступны следующие типы сообщений:

- **«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.

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

- **«NONE»** – политика безопасности для конфигураций с самыми низкими требованиями безопасности, нет алгоритмов шифрования;
- **«BASIC128RSA15»** – политика безопасности для конфигураций со средними требованиями безопасности, такими как:
  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования SHA 1;
  - использование алгоритма шифрования AES 128 CBC;
  - использование алгоритма шифрования RSA-PKCS15-SHA1;
  - использование алгоритма шифрования RSA-PKCS15;
  - использование алгоритма получения ключа P-SHA1;
  - использование алгоритма подписи сертификата RSA-PKCS15-SHA1;
  - использование ограниченного алгоритма получения ключа RSA15;
- **«BASIC256»** – политика безопасности для конфигураций со средними требованиями безопасности, такими как:
  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования SHA 1;
  - использование алгоритма шифрования AES 128 CBC;
  - использование алгоритма шифрования RSA-PKCS15-SHA1;
  - использование алгоритма шифрования RSA-OAEP-SHA1;
  - использование алгоритма получения ключа P-SHA1;
  - использование алгоритма подписи сертификата RSA-PKCS15-SHA1;
  - использование ограниченного алгоритма получения ключа RSA15;
- **«BASIC256SHA256»** – политика безопасности для конфигураций со средними требованиями безопасности, такими как:
  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;

- использование алгоритма шифрования SHA 2;
- использование алгоритма шифрования AES 256 CBC;
- использование алгоритма шифрования RSA-PKCS15-SHA2-256;
- использование алгоритма шифрования RSA-OAEP-SHA1;
- использование алгоритма получения ключа P-SHA2-256;
- использование алгоритма подписи сертификата RSA-PKCS15-SHA2-256;
- использование ограниченного алгоритма получения ключа SHA2-256;

- **«AES128_SHA256_RSAOAEP»** – политика безопасности для конфигураций со средними требованиями безопасности, такими как:
  - проверка сертификата безопасности;
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования AES 128 SHA-256;
- **«PUBSUB_AES128_CTR»** – политика безопасности для конфигураций со средними требованиями безопасности, такими как:
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования AES 128 CTR;
- **«PUBSUB_AES256_CTR»** – политика безопасности для конфигураций со средними требованиями безопасности, такими как:
  - необходимо шифрование;
  - необходима безопасная подпись;
  - использование алгоритма шифрования AES 128 CTR.

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 информации 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 определенного 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 удаленной 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»**.

ARMA FW поддерживает отслеживание следующих типов идентификатора узла:

- числовой;
- строковый;
- GUID.

ARMA FW поддерживает отслеживание следующих типов значений:

- числовой;

- строковый.

5.5.3.6.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Создание правила СОВ) со следующими параметрами:

- **«Включить»** – флажок установлен;
- **«Заголовок»** – «OPC UA»;
- **«Использовать шаблон»** – «OPC UA»;
- **«Действие»** – «Отклонить (Reject)»;
- **«Сообщение»** – «OPC UA»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»;
- **«Тип сообщения»** – «MESSAGE»;
- **«Функция»** – «WRITE»;
- **«Тип идентификатора узла»** – «Числовой тип»;
- **«Значение»** – флажок установлен, «от 6257 до 6257».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.6.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола OPC UA на ПК **«Server»** должен быть установлен эмулятор протокола OPC UA – «OPC UA Server», на ПК **«Client»** – ПО «UaExpert».

Порядок проверки срабатывания пользовательских правил:

1. Запустить ПО «OPC UA Server» (см. Рисунок – Запуск OPC UA Server).

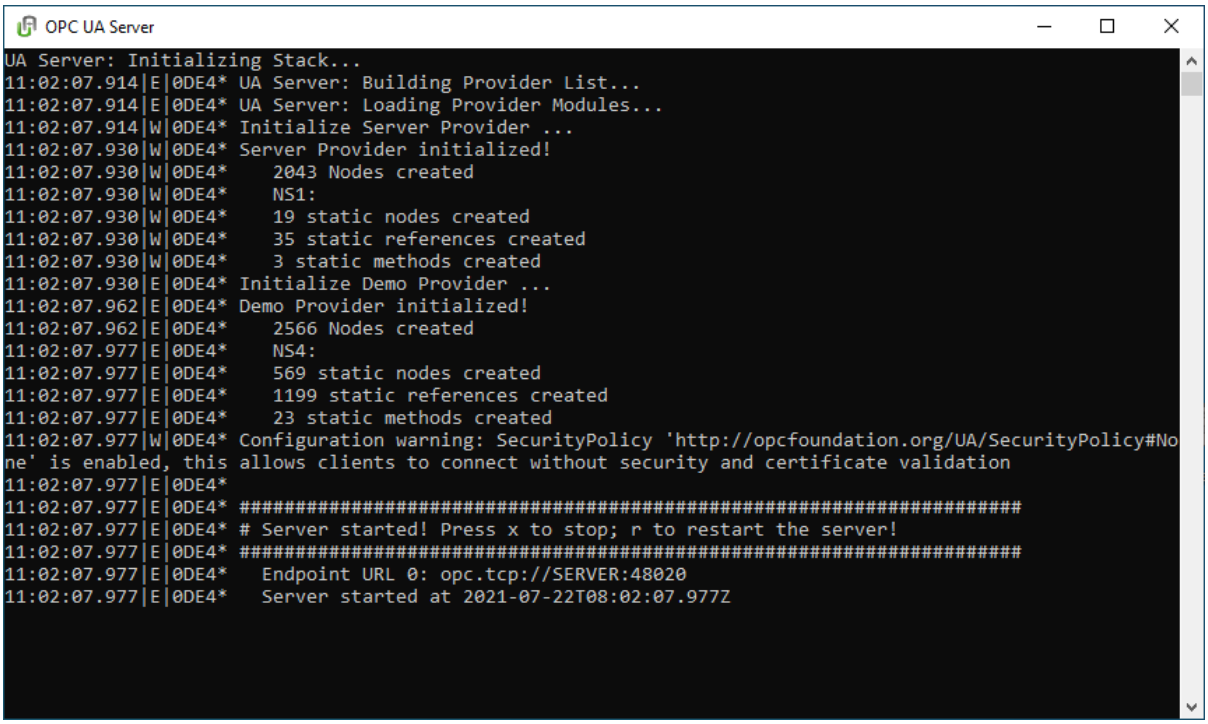


Рисунок – Запуск OPC UA Server

2. Запустить ПО «UaExpert». При первом запуске необходимо будет создать сертификат, указав стандартную информацию SSL-ключа (см. Рисунок – Создание сертификата в UaExpert).

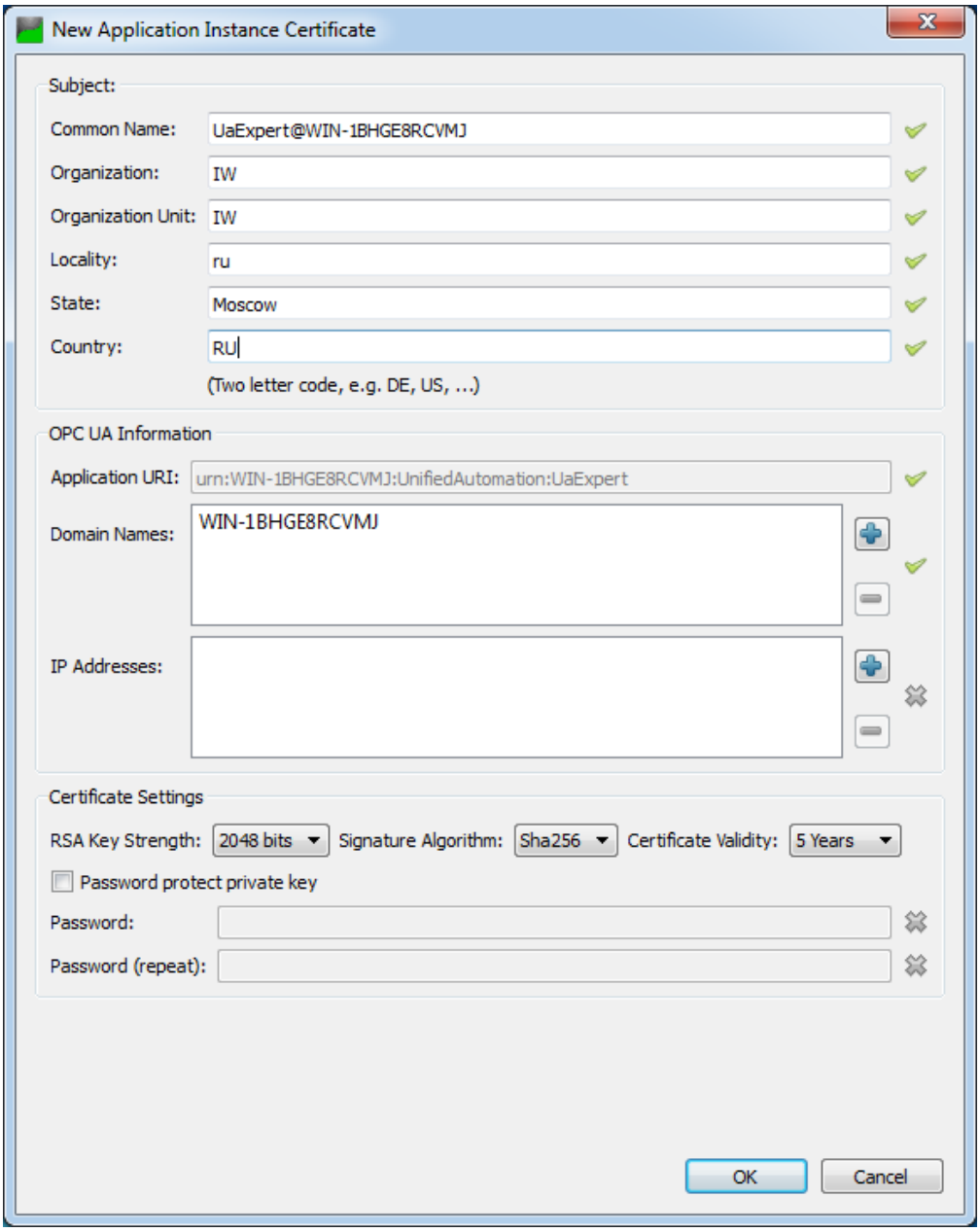


Рисунок – Создание сертификата в UaExpert

3. Нажать **кнопку** «  » и добавить подключение к серверу «OPC UA Server» (см. Рисунок – Добавление сервера в UaExpert).

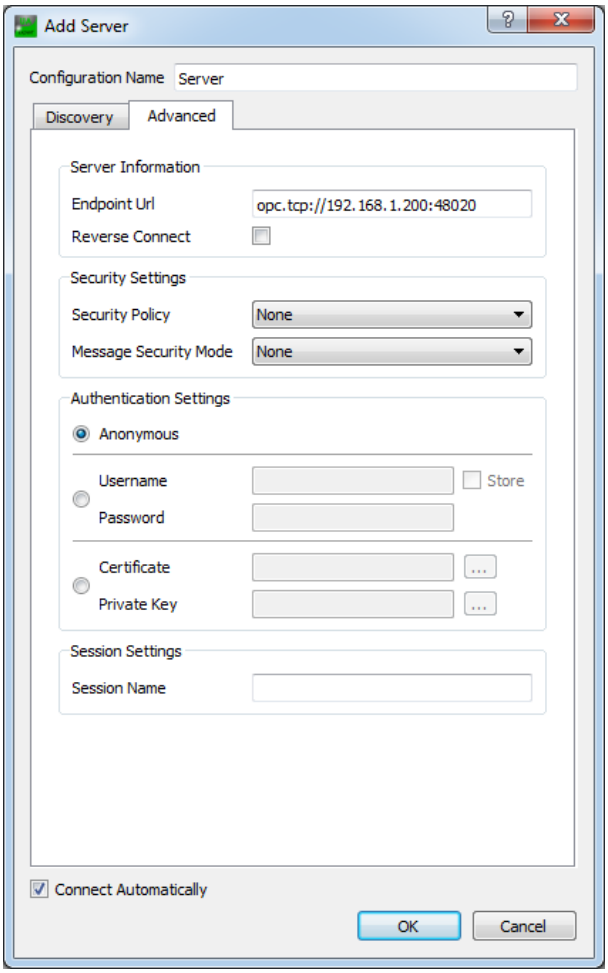


Рисунок – Добавление сервера в UaExpert

4. Перейти в каталог «Root/Server/Machine» и перетащить мышью строку «HeaterSwitch» в окно «Data Access View». Затем нажать два раза **левой кнопкой мыши** по значению поля **«Value»** для перехода в режим редактирования значения переменной (см. Рисунок – Редактирование значения переменной).

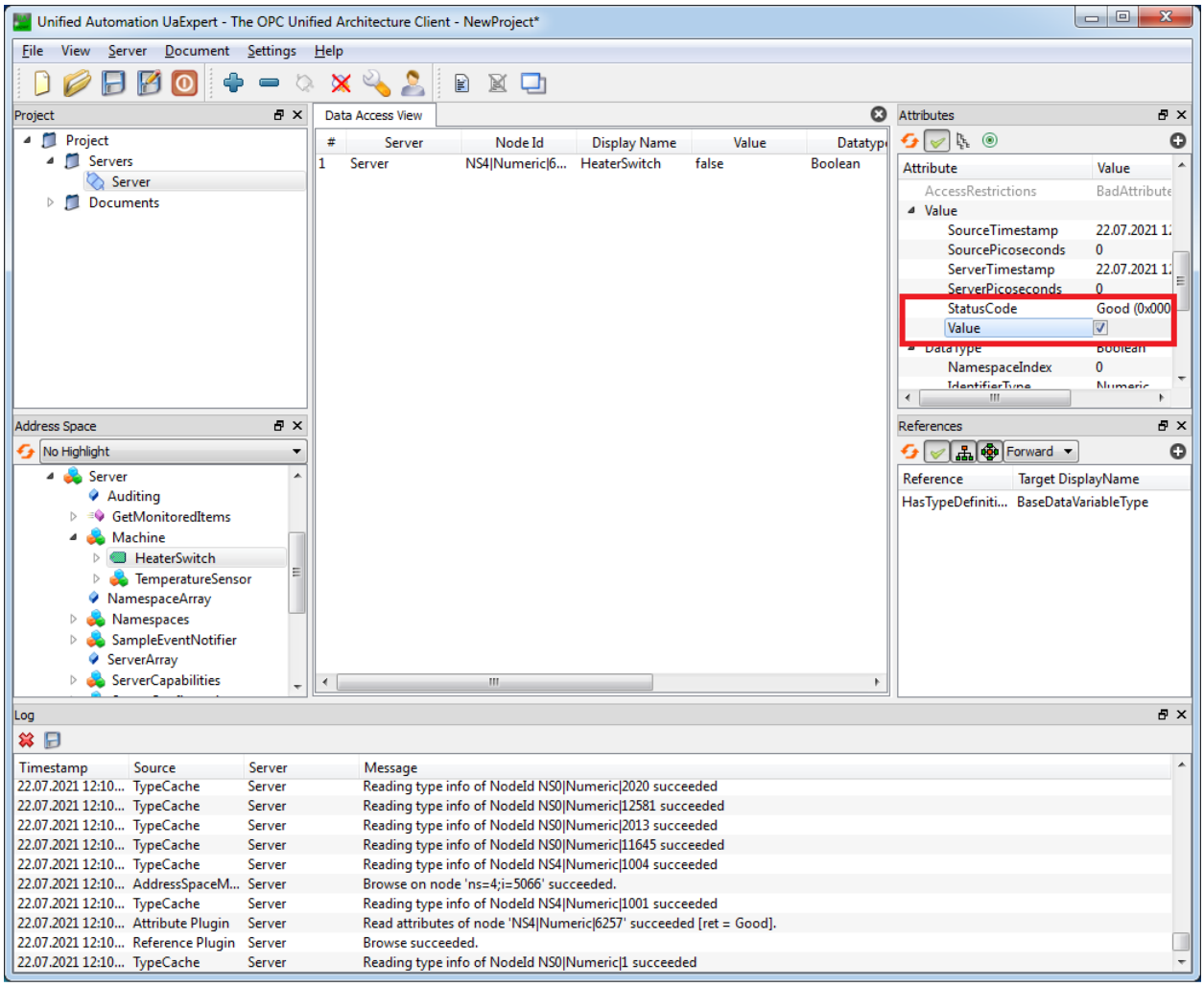


Рисунок – Редактирование значения переменной

5. В блоке **«Log»** появится информация о неуспешной записи (см. Рисунок – Сообщение о неуспешной записи).

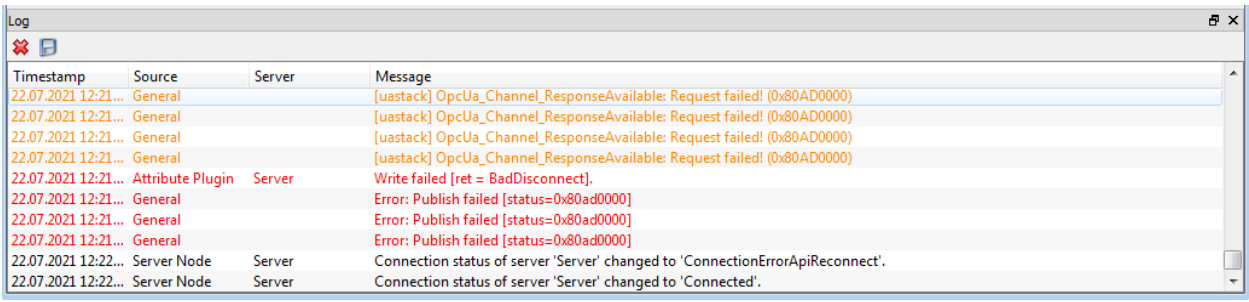


Рисунок – Сообщение о неуспешной записи

6. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

   - «OPC UA» (см. Рисунок – Детальная информация, протокол OPC UA).

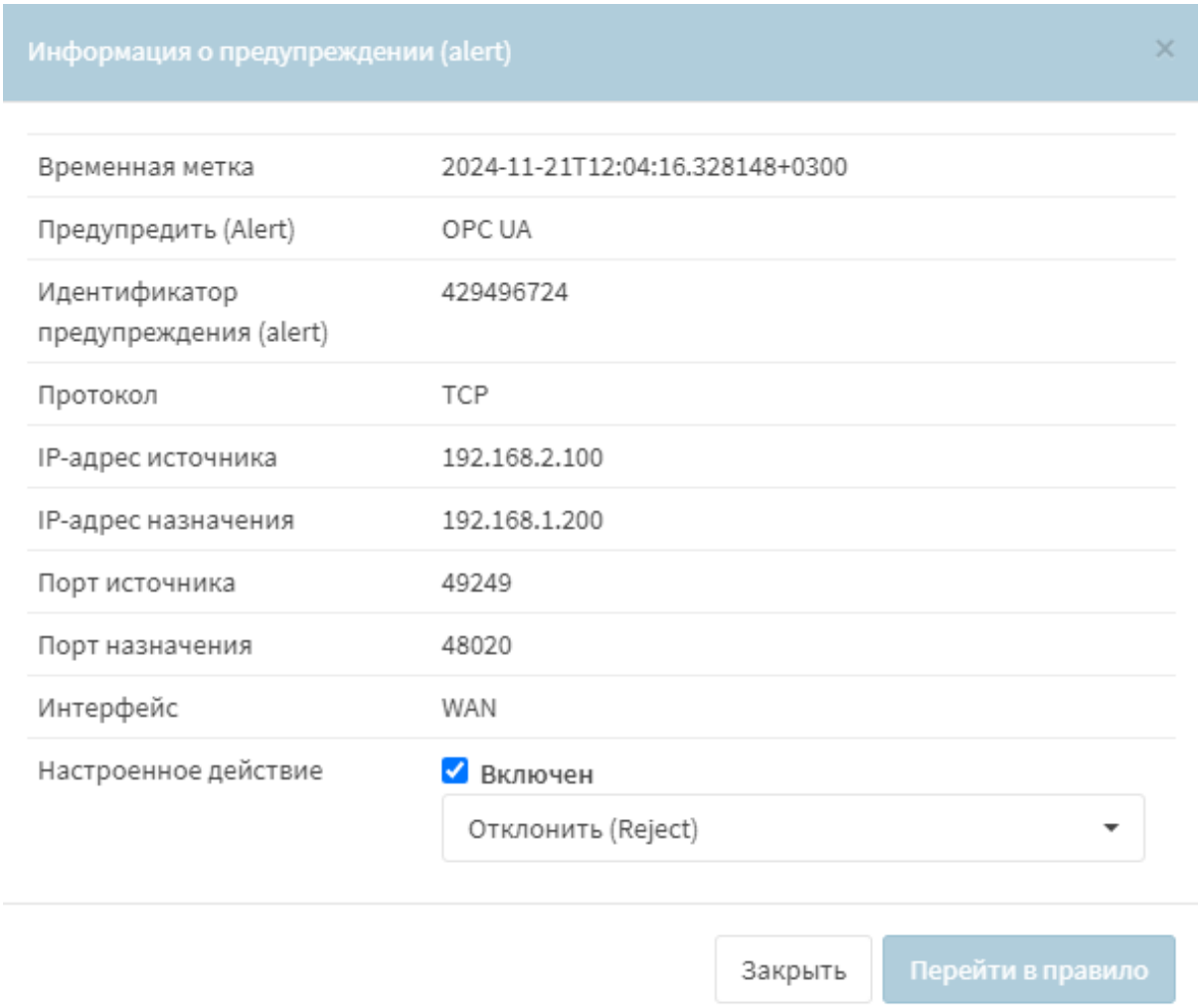


Рисунок – Детальная информация, протокол OPC UA

5.5.3.7 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» появится параметр **«Функция»**, в поле которого доступны функции:

- 0x01 – **INIT_COMM** – Инициализация UMAS сессии;
- 0x02 – **READ_ID** – Запрос ПЛК ID;
- 0x03 – **READ_PROJECT_INFO** – Чтение информации о проекте;
- 0x04 – **READ_PLC_INFO** – Чтение внутренней информации ПЛК;
- 0x06 – **READ_CARD_INFO** – Чтение информации о внутренней SD карты ПЛК;

- 0x0A – **REPEAT** – Отправить информацию обратно ПЛК. Используется для синхронизации;
- 0x10 – **TAKE_PLC_RESERVATION** – Назначить ПЛК владельца;
- 0x11 – **RELEASE_PLC_RESERVATION** – Снять владельца ПЛК;
- 0x12 – **KEEP_ALIVE** – Поддержка активного соединения;
- 0x20 – **READ_MEMORY_BLOCK** – Чтение блока памяти с ПЛК;
- 0x22 – **READ_VARIABLES** – Чтение системных битов, системных слов и переменных;
- 0x23 – **WRITE_VARIABLES** – Запись системных битов, системных слов и переменных;
- 0x24 – **READ_COILS_REGISTERS** – Чтение coils и регистров с ПЛК;
- 0x25 – **WRITE_COILS_REGISTERS** – Запись катушек и регистров в ПЛК;
- 0x30 – **INITIALIZE_UPLOAD** – Инициализация загрузки (копирование с инженерного ПК на ПЛК);
- 0x31 – **UPLOAD_BLOCK** – Загрузка блока данных с инженерного ПК на ПЛК;
- 0x32 – **END_STRATEGY_UPLOAD** – Завершение загрузки (копирования с инженерного ПК на ПЛК);
- 0x33 – **INITIALIZE_DOWNLOAD** – Инициализация скачивания (копирование с ПЛК на инженерный ПК);
- 0x34 – **DOWNLOAD_BLOCK** – Скачивание блока данных с ПЛК на инженерный ПК;
- 0x35 – **END_STRATEGY_DOWNLOAD** – Конец скачивания (копирования с ПЛК на инженерный ПК);
- 0x39 – **READ_ETH_MASTER_DATA** – Чтение Ethernet Master Data;
- 0x40 – **START_PLC** – Включение ПЛК;
- 0x41 – **STOP_PLC** – Выключение ПЛК;
- 0x50 – **MONITOR_PLC** – Мониторинг системных битов, системных слов и переменных;
- 0x58 – **CHECK_PLC** – Проверка статуса подключения ПЛК;
- 0x70 – **READ_IO_OBJECT** – Чтение IO объекта;
- 0x71 – **WRITE_IO_OBJECT** – Запись IO объекта;
- 0x73 – **GET_STATUS_MODULE** – Получение статуса модуля.

При выборе «INIT_COMM», «READ_ID», «READ_PROJECT_INFO», «READ_PLC_INFO», «READ_CARD_INFO», «REPEAT», «TAKE_PLC_RESERVATION», «RELEASE_PLC_RESERVATION», «KEEP_ALIVE», «INITIALIZE_UPLOAD», «UPLOAD_BLOCK», «END_STRATEGY_UPLOAD», «INITIALIZE_DOWNLOAD», «DOWNLOAD_BLOCK», «END_STRATEGY_DOWNLOAD», «READ_ETH_MASTER_DATA», «START_PLC», «STOP_PLC», «MONITOR_PLC», «CHECK_PLC», «READ_IO_OBJECT», «WRITE_IO_OBJECT», «GET_STATUS_MODULE» появятся параметры **«Информация о проекте»** и **«Тип сообщения»**.

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

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

При выборе функции «READ_MEMORY_BLOCK» появятся параметры:

- **«Номер блока»**;
- **«Количество данных»**;
- **«Смещение»**.

При выборе функции «READ_VARIABLES» появятся параметры:

- **«Базовое смещение»**;
- **«Относительное смещение»**;
- **«Номер блока»**;
- **«Количество значений»**;
- **«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»**.

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

- **«Условие (значение)»** – только для «WRITE_COILS_REGISTERS»;
- **«Номер регистров флагов (Coils)»**;
- **«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»**.

5.5.3.8 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:

- **«CONFIRMED_REQUEST»**;
- **«CONFIRMED_RESPONSE»**;
- **«CONFIRMED_ERROR»**;
- **«UNCONFIRMED»**;
- **«REJECT»**;
- **«CANCEL_REQUEST»**;
- **«CANCEL_RESPONSE»**;
- **«CANCEL_ERROR»**;
- **«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:

- **«STATUS»**;
- **«GETNAMELIST»**;
- **«IDENTIFY»**;
- **«RENAME»**;
- **«READ»**;
- **«WRITE»**;
- **«GETVARIABLEACCESSATTRIBUTES»**;
- **«DEFINENAMEDVARIABLE»**;
- **«DEFINESCATTEREDACCESS»**;
- **«GETSCATTEREDACCESSATTRIBUTES»**;
- **«DELETEVARIABLEACCESS»**;
- **«DEFINENAMEDVARIABLELIST»**;
- **«GETNAMEDVARIABLELISTATTRIBUTES»**;
- **«DELETENAMEDVARIABLELIST»**;
- **«DEFINENAMEDTYPE»**;
- **«GETNAMEDTYPEATTRIBUTES»**;
- **«DELETENAMEDTYPE»**;
- **«INPUT»**;
- **«OUTPUT»**;
- **«TAKECONTROL»**;
- **«RELINQUISHCONTROL»**;
- **«DEFINESEMAPHORE»**;
- **«DELETESEMAPHORE»**;
- **«REPORTSEMAPHORESTATUS»**;
- **«REPORTPOOLSEMAPHORESTATUS»**;

- **«REPORTSEMAPHOREENTRYSTATUS»**;
- **«INITIATEDOWNLOADSEQUENCE»**;
- **«DOWNLOADSEGMENT»**;
- **«TERMINATEDOWNLOADSEQUENCE»**;
- **«INITIATEUPLOADSEQUENCE»**;
- **«UPLOADSEGMENT»**;
- **«TERMINATEUPLOADSEQUENCE»**;
- **«REQUESTDOMAINDOWNLOAD»**;
- **«REQUESTDOMAINUPLOAD»**;
- **«LOADDOMAINCONTENT»**;
- **«STOREDOMAINCONTENT»**;
- **«DELETEDOMAIN»**;
- **«GETDOMAINATTRIBUTES»**;
- **«CREATEPROGRAMINVOCATION»**;
- **«DELETEPROGRAMINVOCATION»**;
- **«START»**;
- **«STOP»**;
- **«RESUME»**;
- **«RESET»**;
- **«KILL»**;
- **«GETPROGRAMINVOCATIONATTRIBUTES»**;
- **«OBTAINFILE»**;
- **«DEFINEEVENTCONDITION»**;
- **«DELETEEVENTCONDITION»**;
- **«GETEVENTCONDITIONATTRIBUTES»**;
- **«REPORTEVENTCONDITIONSTATUS»**;
- **«ALTEREVENTCONDITIONMONITORING»**;
- **«TRIGGEREVENT»**;
- **«DEFINEEVENTACTION»**;
- **«DELETEEVENTACTION»**;

- **«GETEVENTACTIONATTRIBUTES»**;
- **«REPORTEVENTACTIONSTATUS»**;
- **«DEFINEEVENTENROLLMENT»**;
- **«DELETEEVENTENROLLMENT»**;
- **«ALTEREVENTENROLLMENT»**;
- **«REPORTEVENTENROLLMENTSTATUS»**;
- **«GETEVENTENROLLMENTATTRIBUTES»**;
- **«ACKNOWLEDGEEVENTNOTIFICATION»**;
- **«GETALARMSUMMARY»**;
- **«GETALARMENROLLMENTSUMMARY»**;
- **«READJOURNAL»**;
- **«WRITEJOURNAL»**;
- **«INITIALIZEJOURNAL»**;
- **«REPORTJOURNALSTATUS»**;
- **«CREATEJOURNAL»**;
- **«DELETEJOURNAL»**;
- **«GETCAPABILITYLIST»**;
- **«FILEOPEN»**;
- **«FILEREAD»**;
- **«FILECLOSE»**;
- **«FILERENAME»**;
- **«FILEDELETE»**;
- **«FILEDIRECTORY»**;
- **«ADDITIONALSERVICE»**;
- **«GETDATAEXCHANGEATTRIBUTES»**;
- **«EXCHANGEDATA»**;
- **«DEFINEACCESSCONTROLLIST»**;
- **«GETACCESSCONTROLLISTATTRIBUTES»**;
- **«REPORTACCESSCONTROLLEDOBJECTS»**;
- **«DELETEACCESSCONTROLLIST»**;

- **«CHANGEACCESSCONTROL»**;
- **«RECONFIGUREPROGRAMINVOCATION»**.

При выборе типа службы «ADDITIONALSERVICE» появится параметр **«Дополнительный тип сервиса»**, в котором доступны следующие типы дополнительного сервиса:

- **«VMDSTOP»**;
- **«VMDRESET»**;
- **«SELECT»**;
- **«ALTERPI»**;
- **«INITIATEUCLOAD»**;
- **«UCLOAD»**;
- **«UCUPLOAD»**;
- **«STARTUC»**;
- **«STOPUC»**;
- **«CREATEUC»**;
- **«ADDTOUC»**;
- **«REMOVEFROMUC»**;
- **«GETUCATTRIBUTES»**;
- **«LOADUCFROMFILE»**;
- **«STOREUCTOFILE»**;
- **«DELETEUC»**;
- **«DEFINEECL»**;
- **«DELETEECL»**;
- **«ADDECLREFERENCE»**;
- **«REMOVEECLREFERENCE»**;
- **«GETECLATTRIBUTES»**;
- **«REPORTECLSTATUS»**;
- **«ALTERECLMONITORING»**.

При выборе типа службы «READ» появятся параметры:

- **«Item ID запроса чтения»**;
- **«Domain ID запроса чтения»**;

- **«Адрес запроса чтения»**.

При выборе типа службы «WRITE» появятся параметры **«Item ID запроса чтения»** и **«Domain ID запроса чтения»**.

5.5.3.8.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Создание правила СОВ) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «MMS»;
- **«Использовать шаблон»** – «MMS»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «MMS»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»;
- **«Тип сообщения»** – «CONFIRMED_REQUEST»;
- **«Тип службы»** – «WRITE».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.8.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола MMS на ПК **«Server»** должен быть установлен эмулятор протокола MMS, а на ПК **«Client»** – ПО «IEDExplorer».

Порядок проверки срабатывания пользовательских правил:

1. Запустить «IEDExplorer» и выполнить подключение к ПК **«Server»** (см. Рисунок – Подключение к ПК «Server» в ПО «IEDExplorer»).

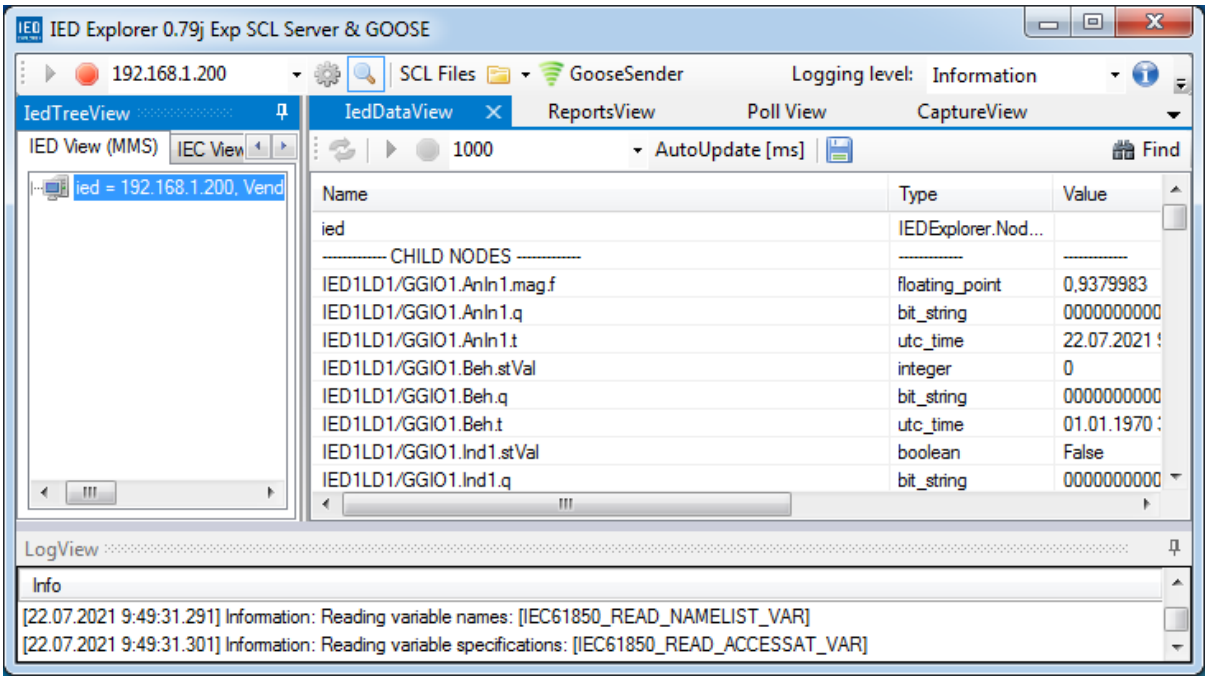


Рисунок – Подключение к ПК «Server» в ПО «IEDExplorer»

2. Выбрать файл по пути «IED1LD1/MMDC1/FC SV/Watt/SubMag/DA f», нажать **правой кнопкой мыши**, выбрать **«Write data»**, в поле **«New Value»** ввести значение «1» и нажать **кнопку «OK»** (см. Рисунок – Запись значения) для сохранения нового значения.

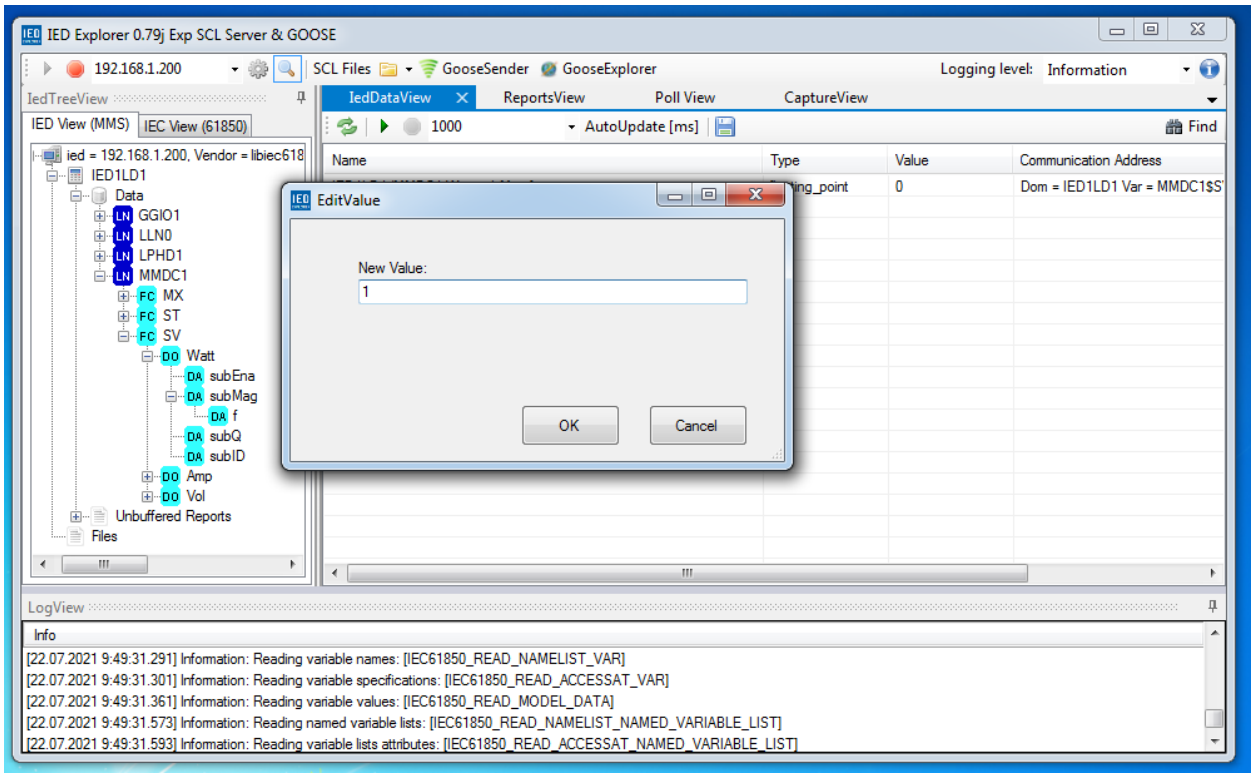


Рисунок – Запись значения

3. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» -**

«Предупреждения (Alerts)»), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:

- «MMS» (см. Рисунок – Детальная информация, протокол MMS).

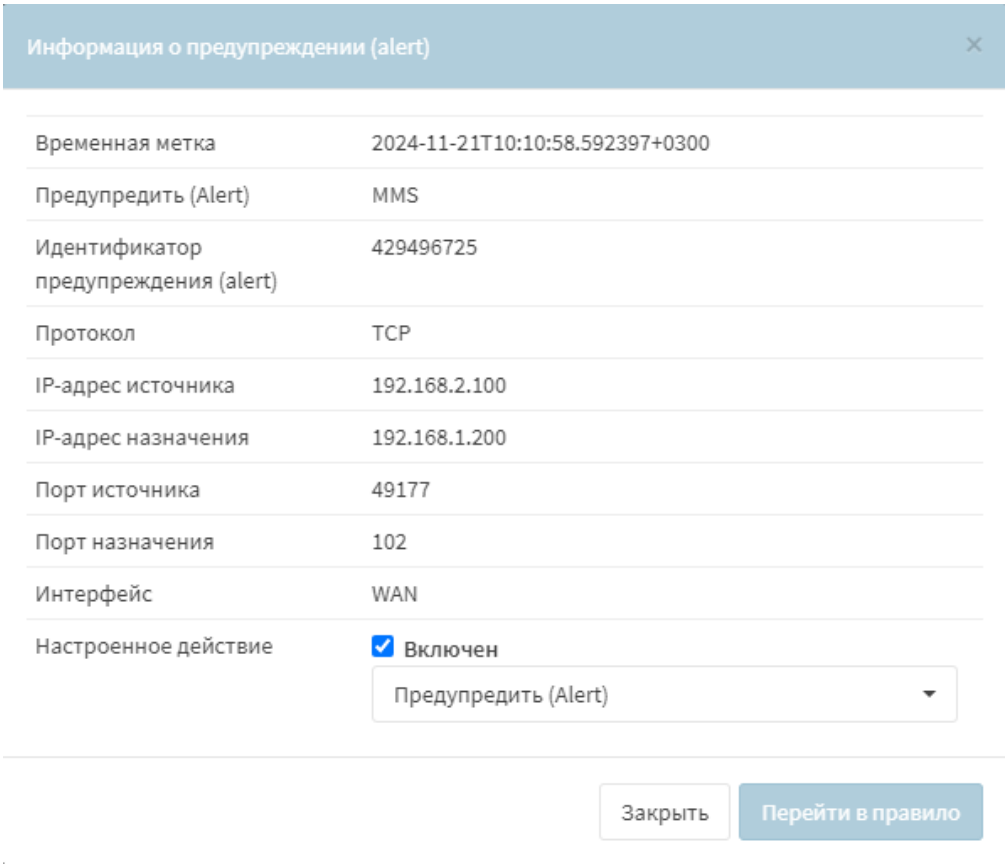


Рисунок – Детальная информация, протокол MMS

5.5.3.9 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»**;
- **«Dataset»**;
- **«GoCBRef»**;
- **«GoID»**;
- **«Дельта секунд»**;
- **«Дельта наносекунд»**;

- **«Предустановленная дата и время»**;
- **«Предустановленные наносекунды»**.

ARMA FW пропускает пакеты промышленного протокола GOOSE только в режиме сетевого моста, который необходимо настроить перед проверкой (см. Пример настройки сетевого моста).

5.5.3.9.1 Пример создания правила СОВ

Необходимо создать пользовательское правило (см. Создание правила СОВ) со следующими параметрами:

- **«Включить»** – установлен флажок;
- **«Заголовок»** – «DREADED CANADIAN GOOSE»;
- **«Использовать шаблон»** – «GOOSE»;
- **«Действие»** – «Предупредить (Alert)»;
- **«Сообщение»** – «DREADED CANADIAN GOOSE»;
- **«Фильтровать на основе протокола»** – «Указать дополнительные параметры»;
- **«Dataset»** – «[5:]».

Остальные параметры необходимо оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

5.5.3.9.2 Проверка созданного правила СОВ

Для проверки срабатывания пользовательского правила на основе шаблона протокола GOOSE на ПК **«Server»** и **«Client»** должно быть установлено ПО «IED Explorer».

Порядок проверки срабатывания пользовательских правил:

1. На ПК **«Client»** запустить ПО «IED Explorer» и выполнить подключение к ПК **«Server»**.
2. Нажать **кнопку «GooseExplorer»**, в выпадающем списке выбрать используемую сетевую карту и нажать **кнопку** « » (см. Рисунок – Настройка ПО «IED Explorer» на ПК «Client»).

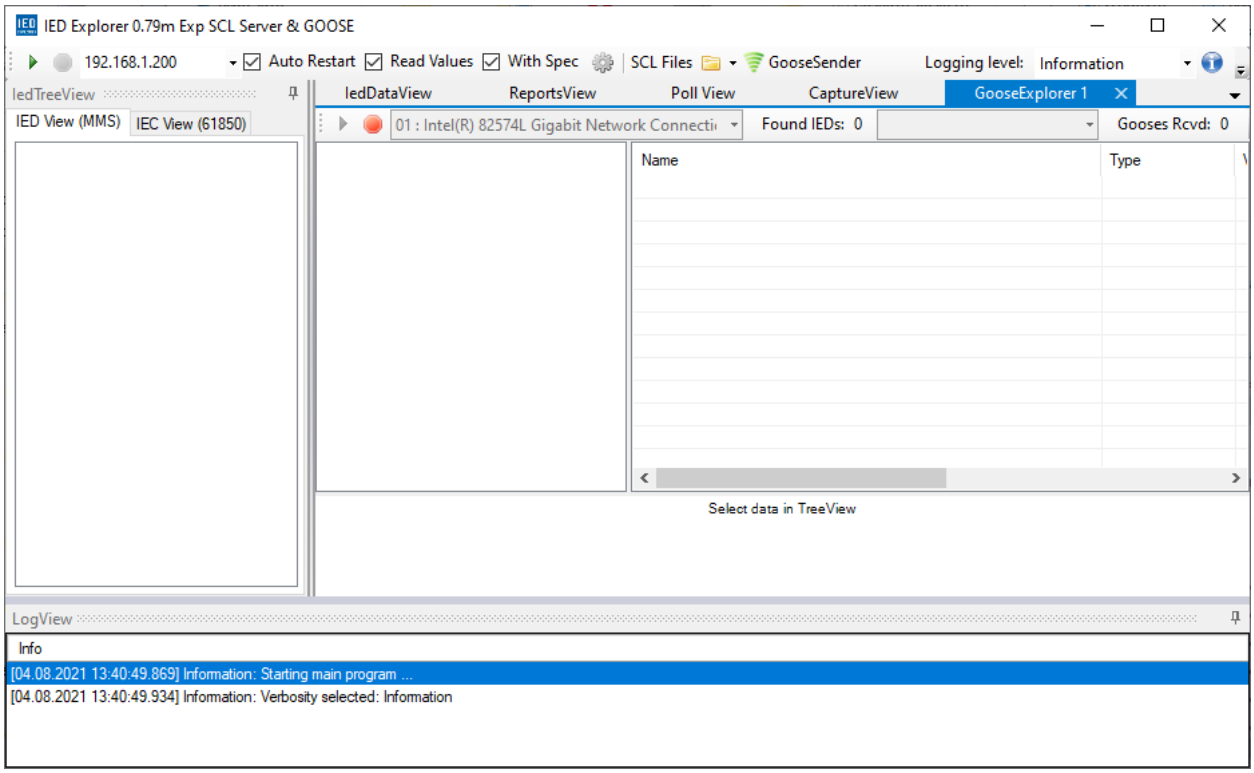


Рисунок – Настройка ПО «IED Explorer» на ПК «Client»

3. На ПК **«Server»** запустить ПО «IED Explorer» и нажать **кнопку «GooseSender»**, в выпадающем списке выбрать используемую сетевую карту и нажать **кнопку** «  ».

4. Нажать **кнопку** «  », в поле **«AppID»** поставить значение «5» и нажать **кнопку «Send 1x»** (см. Рисунок – Настройка ПО «IED Explorer» на ПК «Server»).

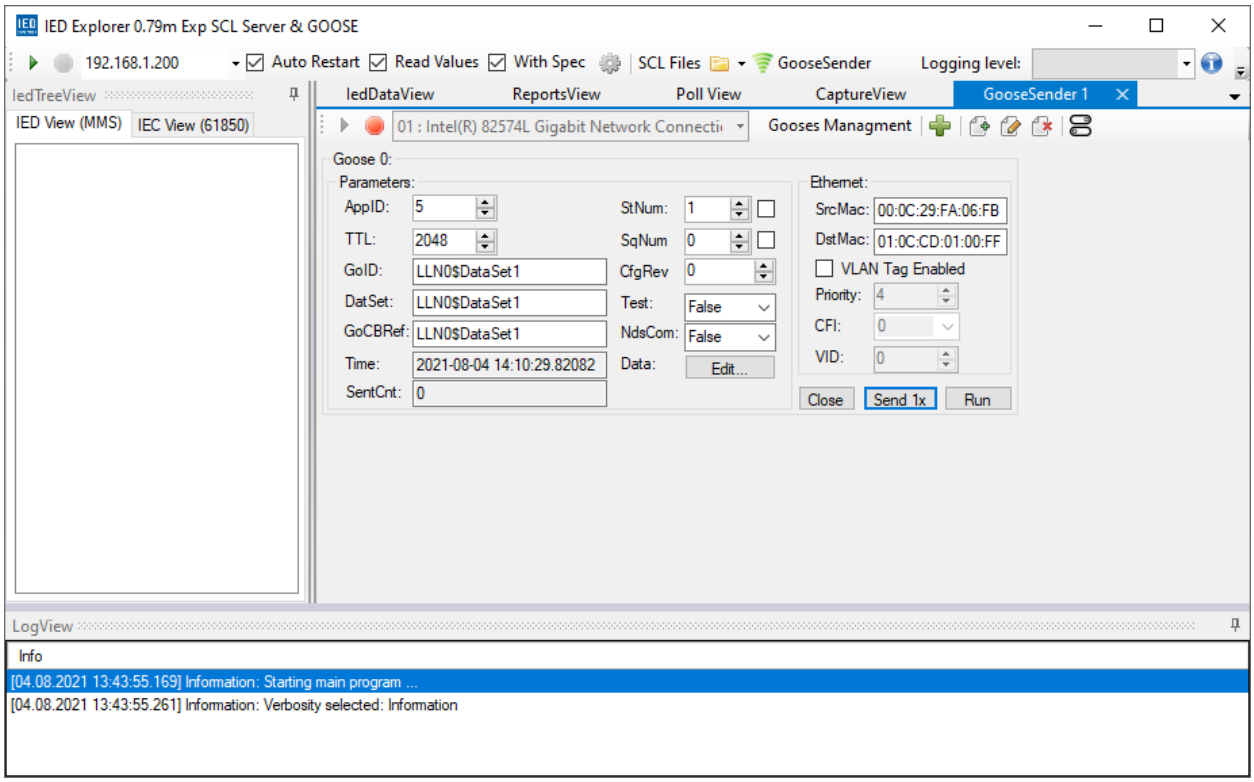


Рисунок – Настройка ПО «IED Explorer» на ПК «Server»

5. Результатом успешного срабатывания правила будет появление событий в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**), в детальной информации которых присутствует значение, указанное в параметре **«Заголовок»**:
   - «DREADED CANADIAN GOOSE» (см. Рисунок – Детальная информация. GOOSE).

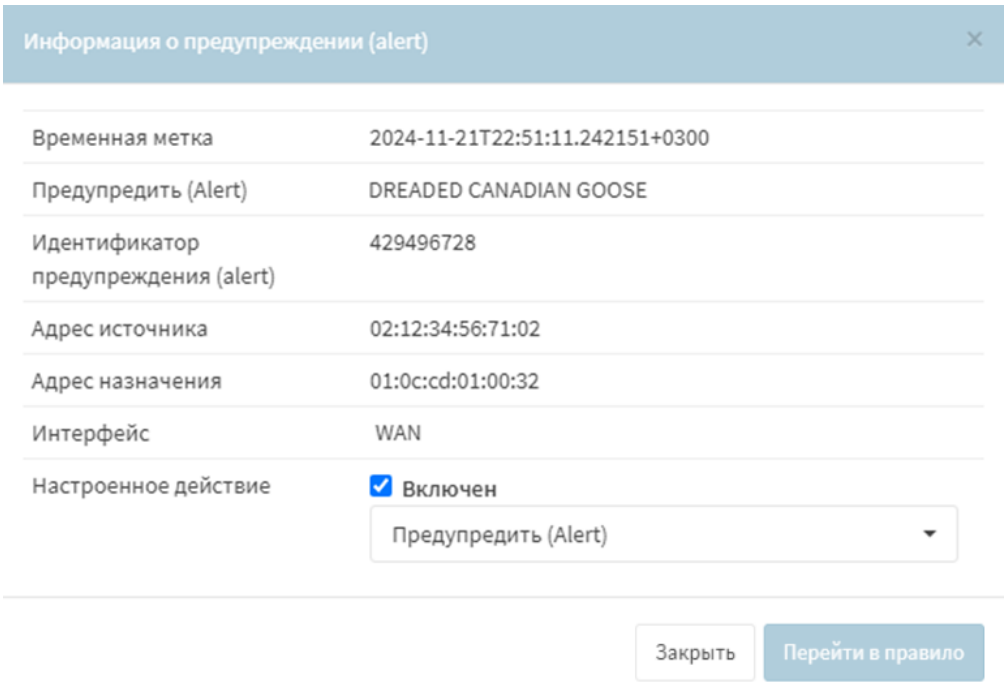


Рисунок – Детальная информация. GOOSE

5.5.3.10 Шаблон протокола KRUG

При создании пользовательского правила на основе шаблона промышленного протокола KRUG 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:

- **«COMMAND»** – используется для передачи номера команды запроса от станции оператора, возможно указать число или диапазон чисел от «0» до «255»;
- **«CMD»** – используется для передачи номера команды запроса от станции инжиниринга, за исключением значения «23» – номера команды от станции оператора на запрос протокола событий, возможно указать число или диапазон чисел от «0» до «255»;
- **«PORT»** – используется для передачи номера устройства, для которого послан пакет, возможно указать число или диапазон чисел от «0» до «65535»;
- **«ACCESS»** – используется для передачи атрибута файла в запросах станции инжиниринга при работе с файловой системой, возможно указать число или диапазон чисел от «0» до «65535»;

- **«MODE»** – используется для передачи кода «тип переменной» в запросах/ответах от станции оператора, возможно указать число или диапазон чисел от «0» до «65535»;
- **«ERRCODE»** – используется для передачи кода ошибки в запросах/ответах от станции оператора, возможно указать число или диапазон чисел от «0» до «65535».

5.5.3.11 Шаблон протокола EtherCAT

При создании пользовательского правила на основе шаблона промышленного протокола EtherCAT 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:

- **«Cmd»**;
- **«Тип адресации»**;
- **«Значение логического адреса»**;
- **«Поля регистра 0x120»**;
- **«Поля регистра 0x130»**;
- **«Поля регистра 0x200»**;
- **«Поля регистра 0x300»**;
- **«Поля регистра 0x502»**;
- **«Поля регистров 0x504-0x50E»**;
- **«Строка данных в шестнадцатеричном формате»**;
- **«Коммуникационный профиль»**.

В поле параметра **«Cmd»** возможно выбрать следующие значения:

- **«Любой»**;
- **«0: No operation»** – ведомое устройство игнорирует команду;
- **«1: Auto Increment Physical Read»** – ведомое устройство увеличивает значение адреса «Slave», записывает данные в датаграмму, если значение адреса «Slave» равно «0»;
- **«2: Auto Increment Physical Write»** – ведомое устройство увеличивает значение адреса «Slave», записывает данные себе, если значение адреса «Slave» равно «0»;

- **«3: Auto Increment Physical ReadWrite»** – ведомое устройство увеличивает значение адреса «Slave», записывает данные в датаграмму и себе, если значение адреса «Slave» равно «0»;
- **«4: Configured address Physical Read»** – ведомое устройство записывает данные в датаграмму, если значение адреса «Slave» датаграммы соответствует адресу/псевдониму этого устройства;
- **«5: Configured address Physical Write»** – ведомое устройство записывает данные себе, если значение адреса «Slave» датаграммы соответствует адресу/псевдониму этого устройства;
- **«6: Configured address Physical ReadWrite»** – ведомое устройство записывает данные в датаграмму и себе, если значение адреса «Slave» датаграммы соответствует адресу/псевдониму этого устройства;
- **«7: Broadcast Read»** – все ведомые устройства записывают в датаграмму «логическое или» данных своих и датаграммы, увеличивают значение адреса «Slave»;
- **«8: Broadcast Write»** – все ведомые устройства записывают данные себе, увеличивают значение адреса «Slave»;
- **«9: Broadcast ReadWrite»** – все ведомые устройства записывают в датаграмму «логическое или» данных своих и датаграммы, записывают данные себе, увеличивают значение адреса «Slave»;
- **«10: Logical Read»** – ведомое устройство записывает данные в датаграмму, если значение адреса датаграммы соответствует логическому адресу этого устройства;
- **«11: Logical Write»** – ведомое устройство записывает данные себе, если значение адреса датаграммы соответствует логическому адресу этого устройства;
- **«12: Logical ReadWrite»** – ведомое устройство записывает данные в датаграмму и себе, если значение адреса датаграммы соответствует логическому адресу этого устройства;
- **«13: Auto Increment Physical Read Multiple Write»** – ведомое устройство увеличивает значение адреса «Slave», записывает данные в датаграмму, если значение адреса «Slave» равно «0» и записывает данные себе, если значение адреса «Slave» не равно «0»;
- **«14: Configured address Physical Read Multiple Write»**;
- **«255: EXT»**;
- **«Настроенное пользователем»**.

В поле параметра **«Cmd»** при выборе значения «Настроенное пользователем» дополнительно появится параметр:

- **«Значение Cmd»** – возможно указать число от «0» до «255» или диапазон чисел от «0» до «255» при установке флажка напротив параметра.

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

- **«Логический»**;
- **«Составной»**.

В поле параметра **«Тип адресации»** при выборе значения «Составной» появятся следующие параметры:

- **«Значение адреса Slave»**;
- **«Значение адреса Offset»**;

в поле каждого из которых, возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

В поле параметра **«Значение логического адреса»** возможно указать число от «0» до «4294967295» или диапазон чисел от «0» до «4294967295» при установке флажка напротив параметра.

В полях параметров **«Поля регистра 0x120»**, **«Поля регистра 0x130»**, **«Поля регистра 0x200»**, **«Поля регистра 0x300»**, **«Поля регистра 0x502»** и **«Поля регистров 0x504-0x50E»** возможно выбрать следующие значения:

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

В поле параметра **«Поля регистра 0x120»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Регистр 0x120 значение Ctrl»**;
- **«Регистр 0x120 Error ACK»**;
- **«Регистр 0x120 Id»**.

В поле параметра **«Регистр 0x120 значение Ctrl»** возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

В полях параметров **«Регистр 0x120 Error ACK»** и **«Регистр 0x120 Id»** возможно выбрать следующие значения:

- **«Любой»**;
- **«True»**;

- **«False»**.

В поле параметра **«Поля регистра 0x130»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Регистр 0x130 значение Status»**;
- **«Регистр 0x130 Error»**;
- **«Регистр 0x130 Id»**.

В поле параметра **«Регистр 0x130 значение Status»** возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

В полях параметров **«Регистр 0x130 Error»** и **«Регистр 0x130 Id»** возможно выбрать следующие значения:

- **«Любой»**;
- **«True»**;
- **«False»**.

В поле параметра **«Поля регистра 0x200»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Регистр 0x200 Latch»**;
- **«Регистр 0x200 Esk Status»**;
- **«Регистр 0x200 Sm 0 IRQ»**;
- **«Регистр 0x200 Sm 1 IRQ»**;
- **«Регистр 0x200 Sm 2 IRQ»**;
- **«Регистр 0x200 Sm 3 IRQ»**;
- **«Регистр 0x200 Sm 4 IRQ»**;
- **«Регистр 0x200 Sm 5 IRQ»**;
- **«Регистр 0x200 Sm 6 IRQ»**;
- **«Регистр 0x200 Sm 7 IRQ»**;

в поле каждого из которых, возможно выбрать следующие значения:

- **«Любой»**;
- **«True»**;
- **«False»**.

В поле параметра **«Поля регистра 0x300»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Регистр 0x300 значение CRC 0 Inv Frame»**;
- **«Регистр 0x300 значение CRC 1 Inv Frame»**;
- **«Регистр 0x300 значение CRC 2 Inv Frame»**;
- **«Регистр 0x300 значение CRC 3 Inv Frame»**;
- **«Регистр 0x300 значение CRC 0 RX Error»**;
- **«Регистр 0x300 значение CRC 1 RX Error»**;
- **«Регистр 0x300 значение CRC 2 RX Error»**;
- **«Регистр 0x300 значение CRC 3 RX Error»**;

в поле каждого из которых, возможно указать число от «0» до «255» или диапазон чисел от «0» до «255» при установке флажка напротив параметра.

В поле параметра **«Поля регистра 0x502»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Регистр 0x502 Write Access 1»**;
- **«Регистр 0x502 EEPROM Emul»**;
- **«Регистр 0x502 8 B Access»**;
- **«Регистр 0x502 2 B Access»**;
- **«Регистр 0x502 Read Access»**;
- **«Регистр 0x502 Write Access 2»**;
- **«Регистр 0x502 Reload Access»**;
- **«Регистр 0x502 CRC Error»**;
- **«Регистр 0x502 Load Error»**;
- **«Регистр 0x502 Cmd Eror»**;
- **«Регистр 0x502 Write Error»**;
- **«Регистр 0x502 Busy»**;

в поле каждого из которых, возможно выбрать следующие значения:

- **«Любой»**;
- **«True»**;
- **«False»**.

В поле параметра **«Поля регистров 0x502-0x50E»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Значение регистра 0x504»**;

- **«Значение регистра 0x506»**;
- **«Значение регистра 0x508»**;
- **«Значение регистра 0x50A»**;
- **«Значение регистра 0x50C»**;
- **«Значение регистра 0x50E»**;

в поле каждого из которых, возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

В поле параметра **«Строка данных в шестнадцатеричном формате»** возможно указать данные в шестнадцатеричном формате, например «0A 94 FF C7».

В поле параметра **«Коммуникационный профиль»** возможно выбрать следующие параметры:

- **«Любой»**;
- **«ADS over EtherCAT»**.

В поле параметра **«Коммуникационный профиль»** при выборе значения «ADS over EtherCAT» дополнительно появится параметр **«Фильтровать на основе протокола»**.

В поле параметра **«Фильтровать на основе протокола»** возможно выбрать следующие параметры:

- **«Любые пакеты протокола»**;
- **«Указать дополнительные параметры»**.

Для ознакомления с описанием дополнительно появляющихся параметров см. Шаблон протокола ADS.

5.5.3.12 Шаблон протокола ADS

При создании пользовательского правила на основе шаблона промышленного протокола ADS 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:

- **«Любой»**;
- **«Запрос»**;
- **«Ответ»**.

При выборе значения «Запрос» в поле параметра **«Тип сообщения»** дополнительно появятся следующие параметры:

- **«Тип условия AMS Target Net Id»** – значение или диапазон;
- **«Значение AMS Target Net Id»** – целевой идентификатор;
- **«Значение AMS Target port»** – целевой порт;
- **«Тип условия AMS Source Net Id»** – значение или диапазон;
- **«Значение AMS Source Net Id»** – идентификатор источника;
- **«Значение AMS Source port»** – порт источника;
- **«CmdId»** – идентификатор команды.

В полях параметров **«Тип условия AMS Target Net Id»** и **«Тип условия AMS Source Net Id»** возможно выбрать:

- **«Значение»**;
- **«Диапазон»**.

При выборе значения «Диапазон» в поле параметра **«Тип условия AMS Target Net Id»** дополнительно появятся следующие параметры:

- **«Начало диапазона значения AMS Target Net Id»**;
- **«Конец диапазона значения AMS Target Net Id»**.

При выборе значения «Диапазон» в поле параметра **«Тип условия AMS Source Net Id»** дополнительно появятся следующие параметры:

- **«Начало диапазона значения AMS Source Net Id»**;
- **«Конец диапазона значения AMS Source Net Id»**.

В полях параметров **«Значение AMS Target Net Id»**, **«Значение AMS Source Net Id»**, **«Начало диапазона значения AMS Target Net Id»**, **«Конец диапазона значения AMS Target Net Id»**, **«Начало диапазона значения AMS Source Net Id»** и **«Конец диапазона значения AMS Source Net Id»** необходимо указать значение, состоящее из шести чисел от «0» до «255», разделённых знаком «точка», например «10.0.8.2.1.1».

В полях параметров **«Значение Target port»** и **«Значение AMS Source port»** возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

В поле параметра **«CmdId»** возможно выбрать следующие значения:

- **«Любой»**;
- **«1: ADS Read Device Info»**;

- **«2: ADS Read»**;
- **«3: ADS Write»**;
- **«4: ADS Read State»**;
- **«5: ADS Write Control»**;
- **«6: ADS Add Device Notification»**;
- **«7: ADS Delete Device Notification»**;
- **«8: ADS Device Notification»**;
- **«9: ADS Read Write»**;
- **«Настроенное пользователем»**.

В поле параметра **«CmdId»** при выборе значения «Настроенное пользователем» дополнительно появится параметр:

- **«Значение CmdId»** – возможно указать число от «1» до «10» или диапазон чисел от «1» до «10» при установке флажка напротив параметра.

В поле параметра **«CmdId»** при выборе значений «2: ADS Read», «3: ADS Write», «6: ADS Add Device Notification» и «9: ADS Read Write» дополнительно появятся следующие параметры:

- **«Значение IndexGroup»**;
- **«Значение IndexOffset»**.

В полях параметров **«Значение IndexGroup»** и **«Значение IndexOffset»** возможно указать число от «0» до «4294967295» или диапазон чисел от «0» до «4294967295» при установке флажка напротив параметра.

В поле параметра **«CmdId»** при выборе значения «5: ADS Write Control» дополнительно появятся следующие параметры:

- **«AdsState»**;
- **«DeviceState»**.

В полях параметров **«AdsState»** и **«DeviceState»** возможно выбрать следующие значения:

- **«Любой»**;
- **«1: INVALID»**;
- **«2: IDLE»**;
- **«3: RESET»**;
- **«4: INIT»**;

- **«5: RUN»**;
- **«6: STOP»**;
- **«7: SAVECFG»**;
- **«8: LOADCFG»**;
- **«9: POWERFAILURE»**;
- **«10: POWERGOOD»**;
- **«11: ERROR»**;
- **«12: SHUTDOWN»**;
- **«13: SUSPEND»**;
- **«14: RESUME»**;
- **«15: CONFIG»**;
- **«16: RECONFIG»**;
- **«Настроенное пользователем»**.

В полях параметров **«AdsState»** и **«DeviceState»** при выборе значения «Настроенное пользователем» дополнительно появятся следующие параметры:

- **«Значение AdsState»**;
- **«Значение DeviceState»**.

В полях параметров **«Значение AdsState»** и **«Значение DeviceState»** возможно указать число от «0» до «65535» или диапазон чисел от «0» до «65535» при установке флажка напротив параметра.

5.5.3.13 Шаблон протокола RDP

При создании пользовательского правила на основе шаблона протокола RDP 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:

- **«Инвертировать правило»**:
  - **«Нет»** – используется для фильтрации по указанному имени пользователя;
  - **«Да»** – используется для фильтрации по именам всех пользователей, кроме указанного имени.
- **«Значение RDP Cookie»** – используется для передачи имени подключённого пользователя.

Примечание:

Фильтрация согласно созданному правилу на основе шаблона протокола RDP не будет происходить в случае добавления имени ПК к имени пользователя (см. Рисунок – Добавление имени ПК к имени пользователя), в некоторых случаях ОС Windows может добавлять имя ПК автоматически. Для корректной фильтрации следует в используемом правиле указанное ранее имя пользователя, например «test_user», в поле параметра **«Значение RDP Cookie»** заменить 9-ю начальными символами имени ПК (см. Рисунок – Редактирование правила).

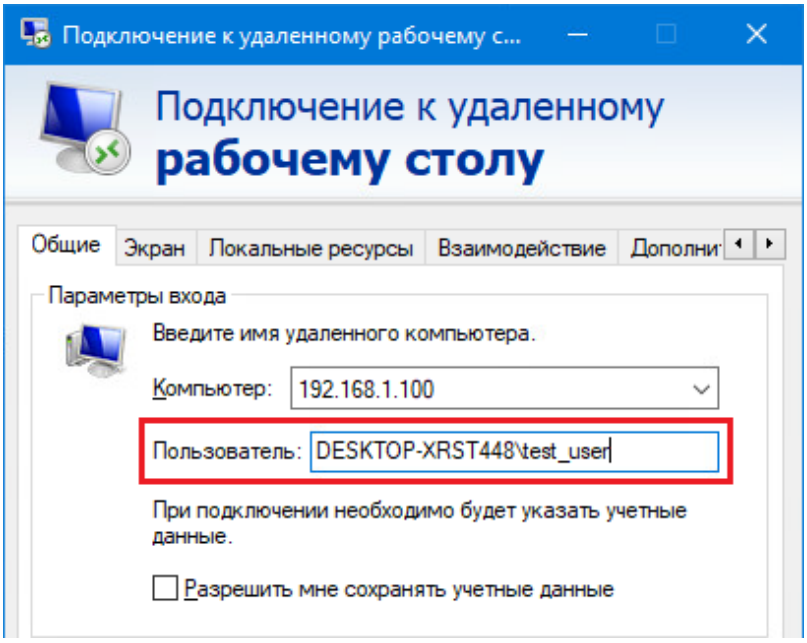


Рисунок – Добавление имени ПК к имени пользователя

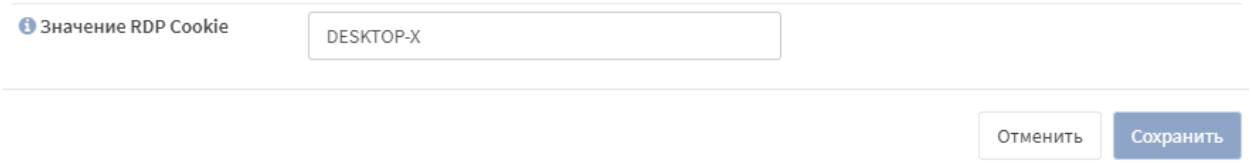


Рисунок – Редактирование правила

5.5.3.14 Шаблон протокола Telnet

При создании пользовательского правила на основе шаблона протокола Telnet необходимо задать значения следующих параметров:

- **«Уникальный Telnet Login поток»**;
- **«Значение Telnet login»** – используется для передачи имени пользователя.

Примечание:

В случае создания множества правил для разных логинов на один и тот же набор IP-адресов получателей и отправителей и портов, необходимо выбирать в поле параметра **«Уникальный Telnet Login поток»**:

- **«Да»** – только на первом правиле из этого множества или единственном правиле;
- **«Нет»** – на остальных правилах из этого множества.

5.5.3.15 Шаблон протокола DNP3

При создании пользовательского правила на основе шаблона протокола DNP3 необходимо задать следующие параметры:

- **«Функция DNP3»**;
- **«Группа объектов DNP3»**;
- **«Вариация объекта DNP3»**;
- **«Внутренняя индикация DNP3»**;
- **«Контент DNP3»**.

В поле параметра **«Функция DNP3»** возможно выбрать следующие значения:

- **«Отсутствует»**;
- **«0: confirm»**;
- **«1: read»**;
- **«2: write»**;
- **«3: select»**;
- **«4: operate»**;
- **«5: direct_operate»**;
- **«6: direct_operate_nr»**;
- **«7: immed_freeze»**;
- **«8: immed_freeze_nr»**;
- **«9: freeze_clear»**;
- **«10: freeze_clear_nr»**;
- **«11: freeze_at_time»**;
- **«12: freeze_at_time_nr»**;
- **«13: cold_restart»**;
- **«14: warm_restart»**;
- **«15: initialize_data»**;
- **«16: initialize_appl»**;

- **«17: start_appl»**;
- **«18: stop_appl»**;
- **«19: save_config»**;
- **«20: enable_unsolicited»**;
- **«21: disable_unsolicited»**;
- **«22: assign_class»**;
- **«23: delay_measure»**;
- **«24: record_current_time»**;
- **«25: open_file»**;
- **«26: close_file»**;
- **«27: delete_file»**;
- **«28: get_file_info»**;
- **«29: authenticate_file»**;
- **«30: abort_file»**;
- **«31: activate_config»**;
- **«32: authenticate_req»**;
- **«33: authenticate_err»**;
- **«129: response»**;
- **«130: unsolicited_response»**;
- **«131: authenticate_resp»**;
- **«Настроенное пользователем»**.

В поле параметра **«Функция DNP3»** при выборе значения «Настроенное пользователем» дополнительно появятся параметр **«Пользовательская функция DNP3»**.

В полях параметров **«Пользовательская функция DNP3»**, **«Группа объекта DNP3»**, **«Вариация объекта DNP3»** возможно указать число от «0» до «255».

В выпадающем списке параметра **«Внутренняя индикация DNP3»** возможно установить флажки для следующих значений:

- **«device_trouble»**;
- **«local_control»**;
- **«need_time»**;

- **«class_3_events»**;
- **«class_2_events»**;
- **«class_1_events»**;
- **«all_stations»**;
- **«reserved_1»**;
- **«reserved_2»**;
- **«config_corrupt»**;
- **«already_executing»**;
- **«event_buffer_overflow»**;
- **«parameter_error»**;
- **«object_unknown»**;
- **«no_func_code_support»**.

В поле параметра **«Контент DNP3»** возможно указать шестнадцатеричный поток, например «3c 02 06».

5.5.3.16 Шаблон протокола ENIP/CIP

При создании пользовательского правила на основе шаблона протокола ENIP/CIP необходимо задать параметр **«Совпадение по»**.

В поле параметра **«Совпадение по»** возможно выбрать следующие значения:

- **«ENIP команда»**;
- **«Сервис CIP»**;
- **«ENIP команда CIP сервис»**.

В поле параметра **«Команда»** возможно указать число от «0» до «65535».

В поле параметра **«Совпадение по»** при выборе значения «Сервис CIP» дополнительно появятся следующие параметры:

- **«Служба»**;
- **«Использовать класс»**.

В поле параметра **«Служба»** возможно указать число от «0» до «127».

При установке флажка для параметра **«Использовать класс»** дополнительно появятся следующие параметры:

- **«Класс»**;
- **«Использовать атрибут»**.

При установке флажка для параметра **«Использовать атрибут»** дополнительно появится параметр **«Атрибут»**.

В полях параметров **«Класс»** и **«Атрибут»** возможно указать число от «0» до «65535».

5.5.3.17 Шаблон протокола Fanuc 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» в десятичной системе или от «0» до «FFFFFFFF» в шестнадцатеричной системе либо указать диапазон чисел при установке флажка напротив параметра.

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

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

В поле параметра **«Тип запроса»** при выборе 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» в десятичной системе или от «0» до «FFFFFFFF» в шестнадцатеричной системе 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»**.

5.6 Контроль приложений

Функция «Контроль приложений» идентифицирует трафик от различных приложений в сети и позволяет блокировать их использование.

Для включения контроля приложений необходимо выполнить следующие действия:

1. Включить СОВ и СПВ (см. Основные настройки СОВ).
2. Перейти в подраздел управления политиками контроля приложений (**«Обнаружение вторжений» - «Контроль приложений»**) и нажать **кнопку** « » (см. Рисунок – Добавление политик контроля приложений).

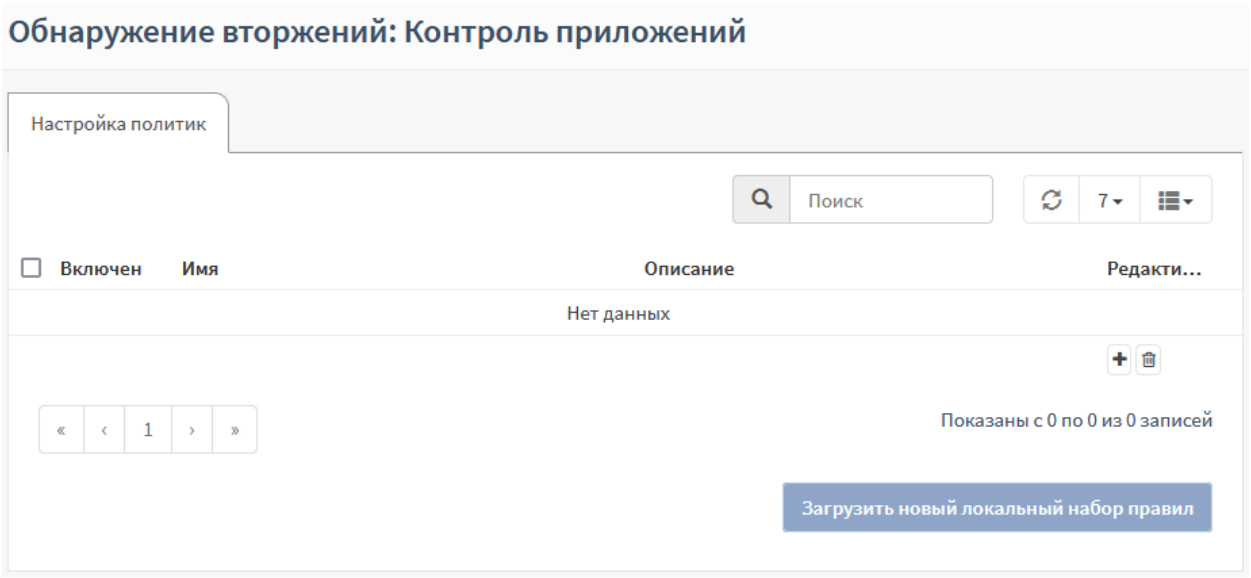


Рисунок – Добавление политик контроля приложений

3. В открывшейся форме (см. Рисунок – Настройка политики контроля приложений) отметить в списке правила для приложений, подлежащих блокировке, указать значения параметров **«Имя»** и **«Описание»**, нажать **кнопку «Сохранить»** и нажать **кнопку «Применить изменения»**.

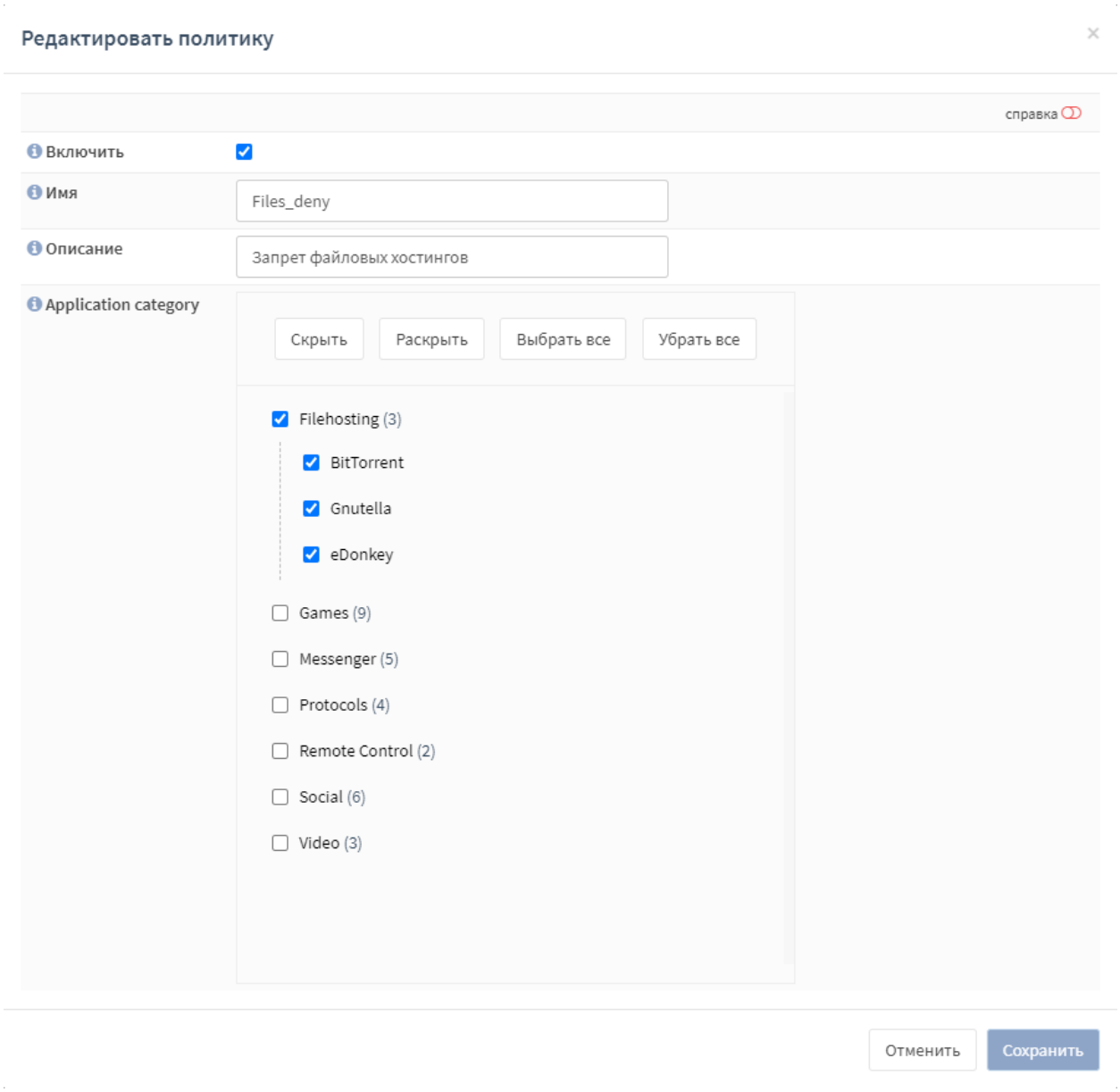


Рисунок – Настройка политики контроля приложений

5.6.1 Импорт набора правил контроля приложений

Для импорта набора правил контроля приложений необходимо выполнить следующие действия:

1. Перейти в подраздел указания политик контроля приложений (**«Обнаружение вторжений» - «Контроль приложений»**) и нажать **кнопку «Загрузить новый локальный набор правил»** (см. Рисунок – Добавление политик контроля приложений).
2. В открывшейся форме выбрать архив в формате **«tar.gz»**, содержащий набор правил контроля приложений, и нажать **кнопку «Открыть»**.

3. После успешной загрузки правил (см. Рисунок – Статус импорта правил) необходимо нажать **кнопку «Закрыть»**, а затем **кнопку «Применить изменения»** чтобы изменения вступили в силу.

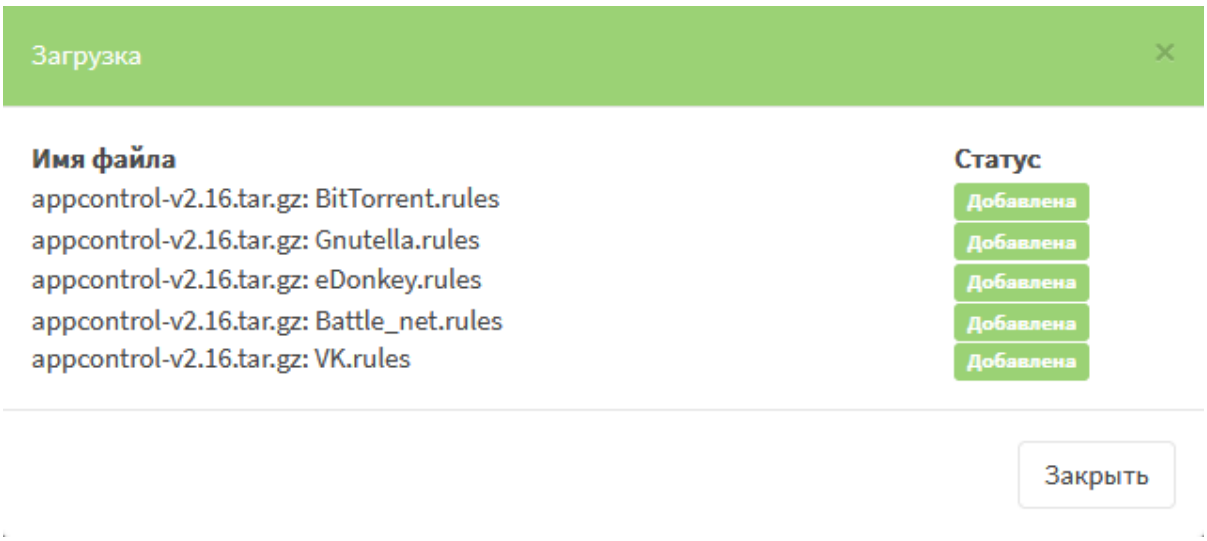


Рисунок – Статус импорта правил

6 ОБНАРУЖЕНИЕ УСТРОЙСТВ

Обнаружение устройств в **ARMA FW** выполняется с помощью сервиса «ARPwatch», отслеживающим появление в сети новых устройств, подмену IP/MAC-адресов и обнаруживает атаки на сетевом уровне – «ARP-spoofing».

6.1 Общие настройки

Для настройки сервиса необходимо перейти в подраздел настроек обнаружения устройств (**«Сеть» - «Обнаружение устройств» - «Общие настройки»**), включить сервис и указать прослушиваемые интерфейсы (см. Рисунок – Настройка сервиса «ARPwatch»).

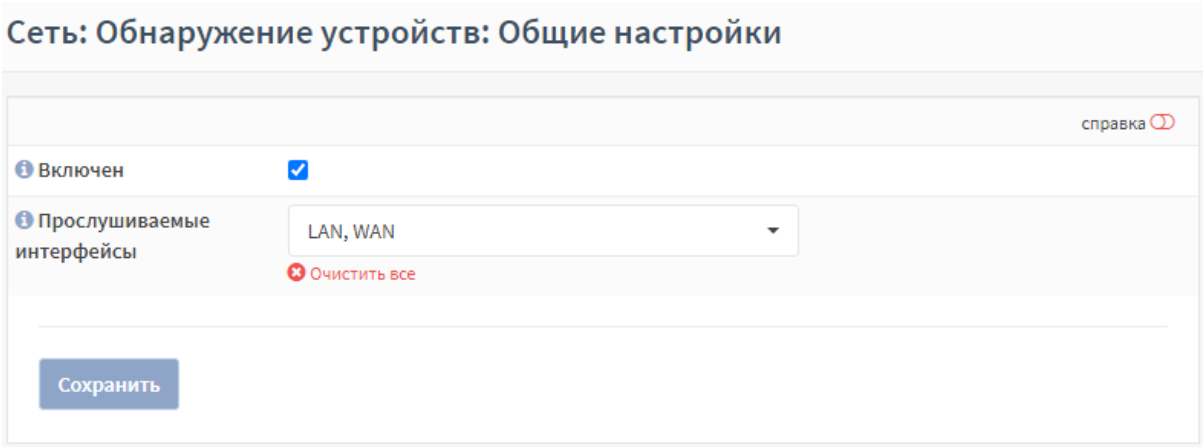


Рисунок – Настройка сервиса «ARPwatch»

Запуск сервиса будет отображён в журнале syslog (**«Система» - «Журналы» - «Syslog»**) (см. Рисунок – Сообщения от сервиса «ARPwatch» в журнале syslog).

6.2 Список устройств

Информация об обнаруженных устройствах отображается в подразделе обнаруженных хостов (**«Сеть» - «Обнаружение устройств» - «Хосты»**) (см. Рисунок – Список подключённых устройств).

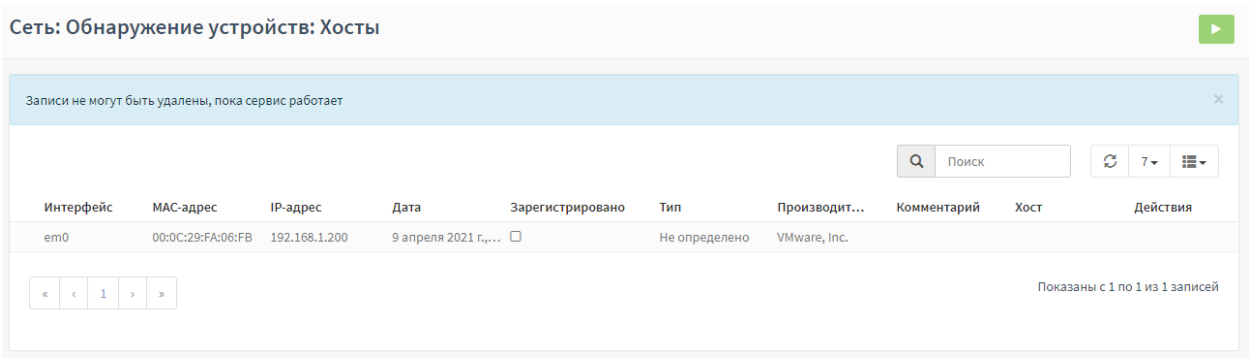


Рисунок – Список подключённых устройств

Дополнительно записи об обнаружении устройств отображаются в журнале syslog (**«Система» - «Журналы» - «Syslog»**) и в журнале событий безопасности

(**«Система» - «Журналы» - «Журнал событий безопасности»**) (см. Рисунок – Сообщения от сервиса «ARPwatch» в журнале syslog и Рисунок – Сообщения от сервиса «ARPwatch» в журнале событий безопасности).

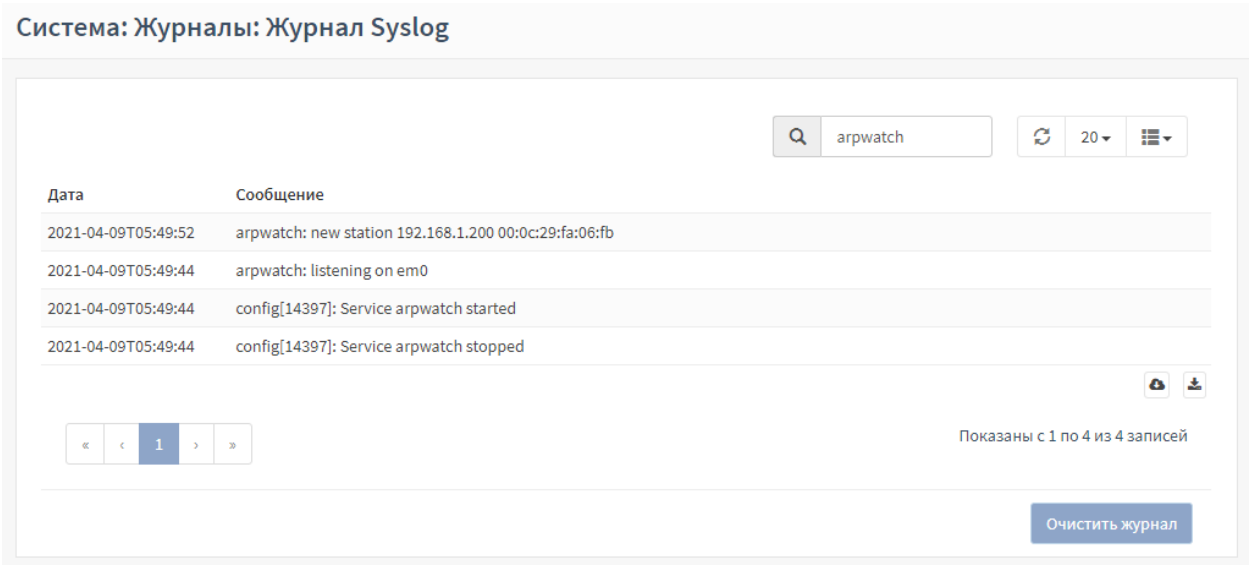


Рисунок – Сообщения от сервиса «ARPwatch» в журнале syslog

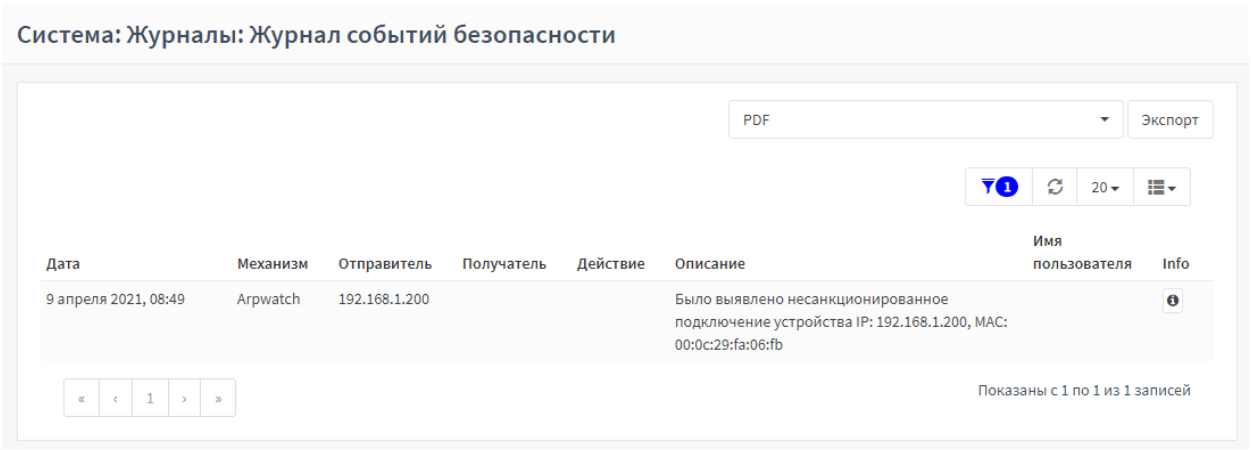


Рисунок – Сообщения от сервиса «ARPwatch» в журнале событий безопасности

7 PROXY ARP

ARMA FW поддерживает технику Proxy ARP, с помощью которой маршрутизатор в данной сети отвечает на запросы по протоколу ARP для IP-адреса, который не находится в этой сети.

В качестве примера настройки Proxy ARP будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки Proxy ARP).

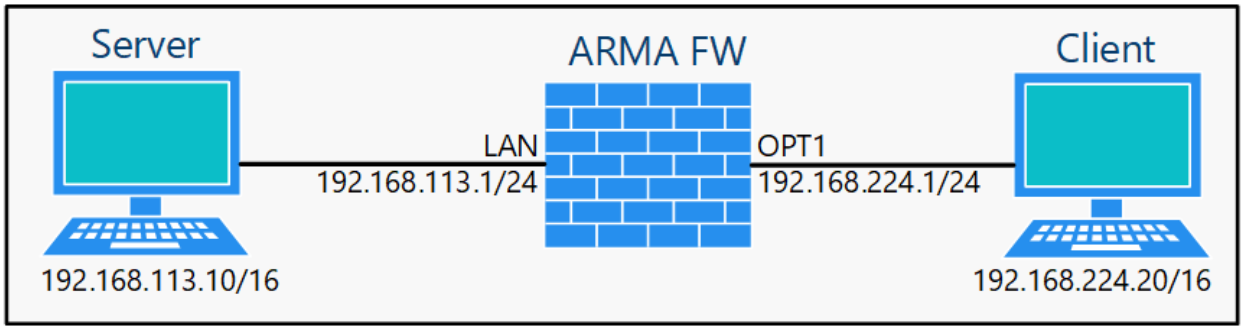


Рисунок – Схема стенда для настройки Proxy ARP

Для настройки Proxy ARP необходимо выполнить следующие действия:

1. Перейти в подраздел настроек виртуальных адресов (**«Межсетевой экран» - «Виртуальные IP-адреса» - «Настройки»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Форма создания виртуального IP-адреса Proxy ARP) указать для интерфейса «LAN» следующие параметры IP-адреса:
   - **«Режим»** – «Proxy ARP»;
   - **«Интерфейс»** – «LAN»;
   - **«Тип»** – «Сеть»;
   - **«Адрес»** – «192.168.0.0», «16»;

   и нажать **кнопку «Сохранить»**. Не указанные параметры оставить по умолчанию.

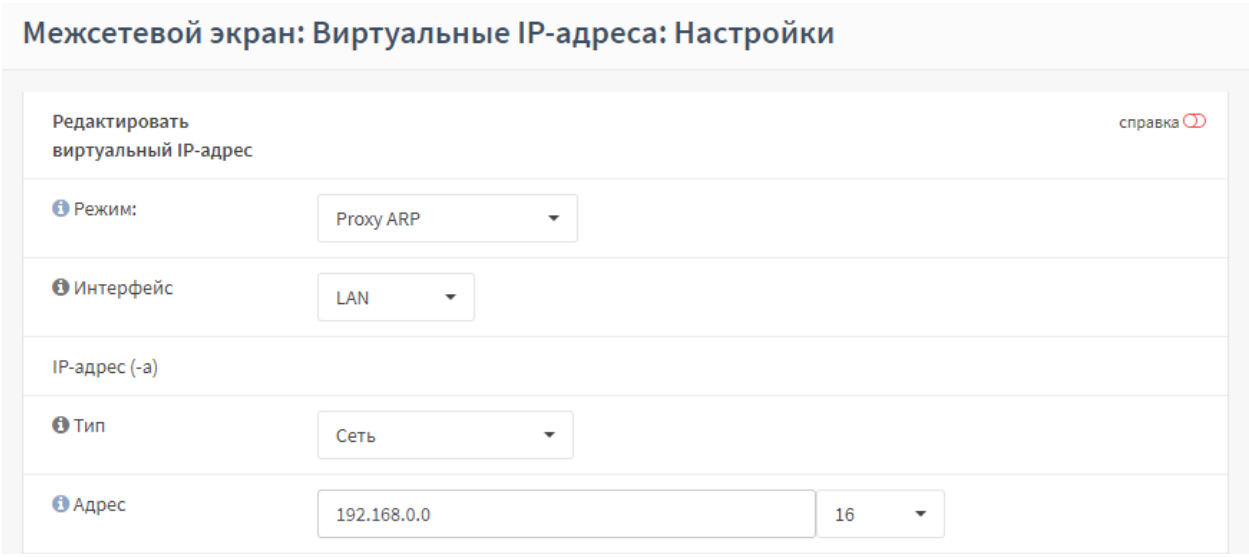


Рисунок – Форма создания виртуального IP-адреса

3. Нажать **кнопку** « » , напротив созданного виртуального IP-адреса.
4. В открывшейся форме указать в поле параметра **«Интерфейс»** значение «OPT1» и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»** (см. Рисунок – Виртуальные IP-адреса Proxy ARP).

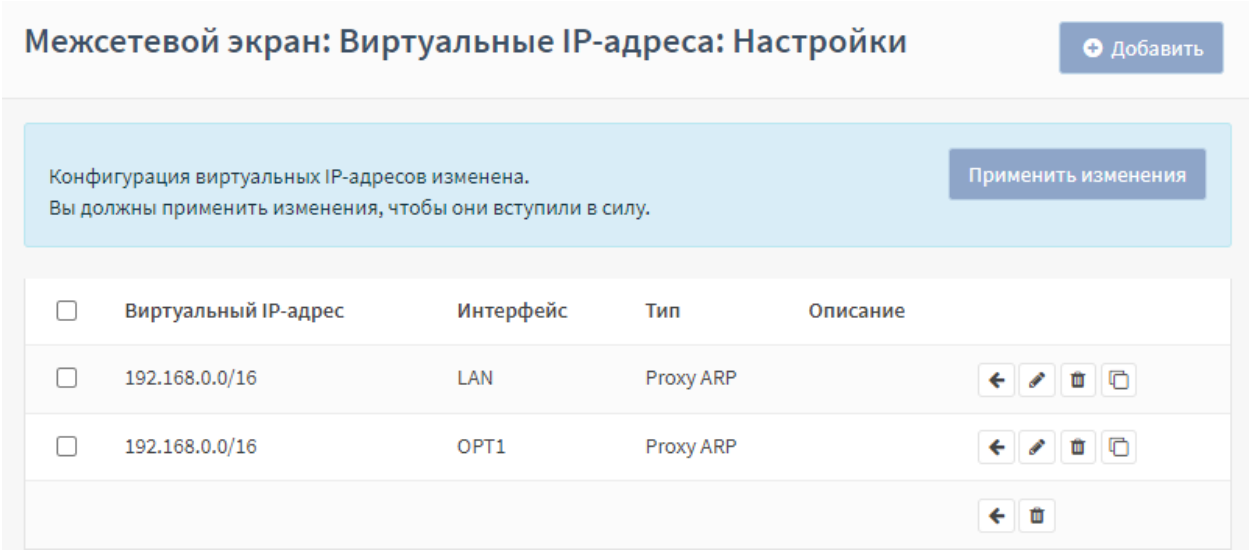


Рисунок – Виртуальные IP-адреса Proxy ARP

Для проверки Proxy ARP необходимо с ПК **«Client»** выполнить команду «ping» ПК **«Server»**. При правильной настройке команда выполнится успешно.

В случае необходимости прекращения использования Proxy ARP следует удалить назначенные виртуальные IP-адреса, а также ARP-записи на ПК **«Client»** и ПК **«Server»**.

8 LLDPD

Служба LLDPd – это демон, позволяющий **ARMA FW** посредством протокола LLDP идентифицировать устройства локальной сети и обмениваться информацией о своих характеристиках.

Для включения службы LLDPd необходимо выполнить следующие действия:

1. Перейти в подраздел настройки LLDPd (**«Службы» - «LLDPd»**) (см. Рисунок – Настройка LLDPd).

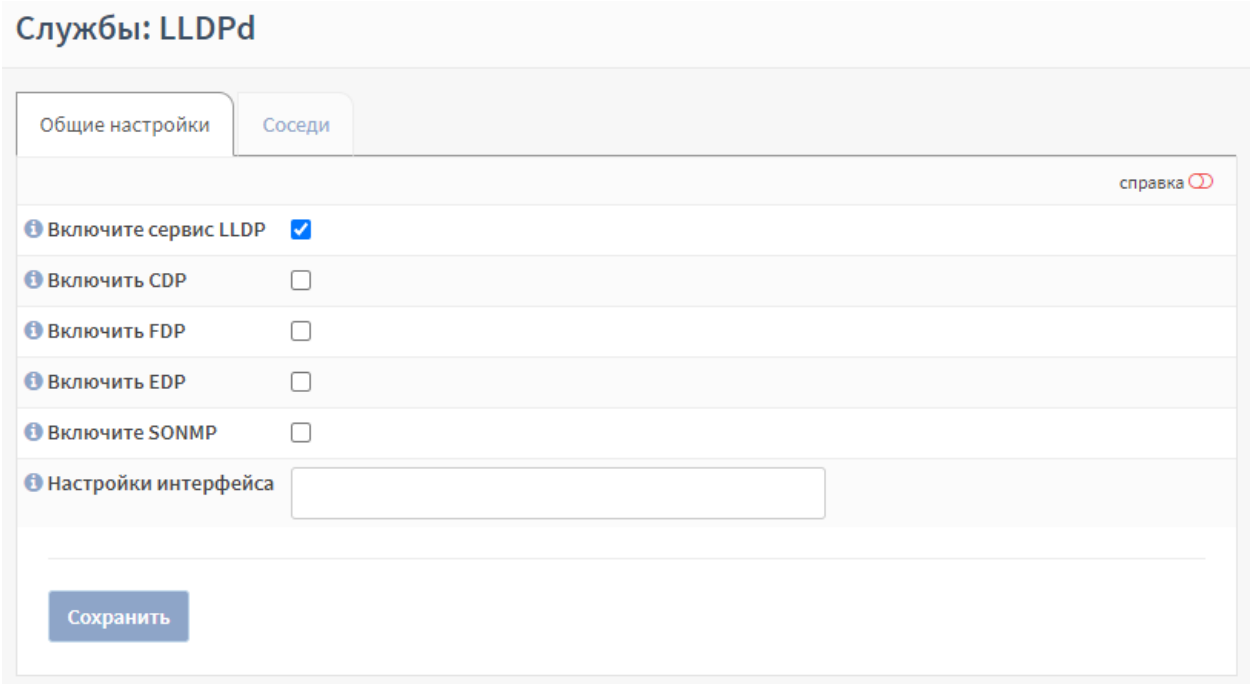


Рисунок – Настройка LLDPd

2. Установить флажок для параметра **«Включите сервис LLDP»**.
3. Нажать **кнопку «Сохранить»**.

Во вкладке **«Соседи»** подраздела настройки LLDPd (**«Службы» - «LLDPd»**) будет отображена информация об обнаруженных сетевых устройствах.

При необходимости существует возможность дополнительно настроить следующие параметры:

- **«Включить CDP»** – для использования протокола CDP;
- **«Включить FDP»** – для использования протокола FDP;
- **«Включить EDP»** – для использования протокола EDP;
- **«Включите SONMP»** – для использования протокола NDP;
- **«Настройки интерфейса»** – для указания физических имён интерфейсов **ARMA FW**, через которые будут передаваться данные об устройствах. По умолчанию используются все интерфейсы.

В поле параметра **«Настройки интерфейса»** возможно использование следующего синтаксиса:

- «em*» – для указания всех интерфейсов с именами, начинающимися на «em»;
- «!em0» – для указания всех интерфейсов, кроме «em0»;
- «em1,em2» – для указания списка интерфейсов, разделённых знаком «запятая».

Имена интерфейсов приведены в качестве примера.

9 SNMP

SNMP – простой протокол сетевого управления, позволяющий осуществлять удаленный мониторинг некоторых системных параметров **ARMA FW** с помощью различных систем мониторинга.

В зависимости от выбранных опций может выполняться мониторинг:

- общей системной информации – использование ЦП, памяти и диска;
- сведений об устройстве, сетевого трафика;
- сведений об интерфейсах, активных процессов и установленного ПО.

За реализацию SNMP в **ARMA FW** отвечает сервис «snmpd». **ARMA FW** поддерживает следующие версии SNMP:

- SNMP v.1, 2;
- SNMP v.3.

9.1 SNMP v.1, 2

Настройка SNMP v.1, 2 подразумевает аутентификацию на основе единой текстовой строки «Community String» – своеобразного пароля. Удалённая пользовательская программа SNMP и агент SNMP должны использовать одно и то же значение Community Strings.

9.1.1 Настройка SNMP v.1, 2

Для настройки удалённого мониторинга по протоколам SNMP v.1,2 необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек SNMP (**«Система» - «Настройки» - «SNMP» - «Общие настройки»**) и установить флажок в параметре **«Включить»**.
2. Задать значение в параметре **«Общая строка SNMP»** и нажать **кнопку «Сохранить»** (см. Рисунок – Настройка SNMP v.1, 2).

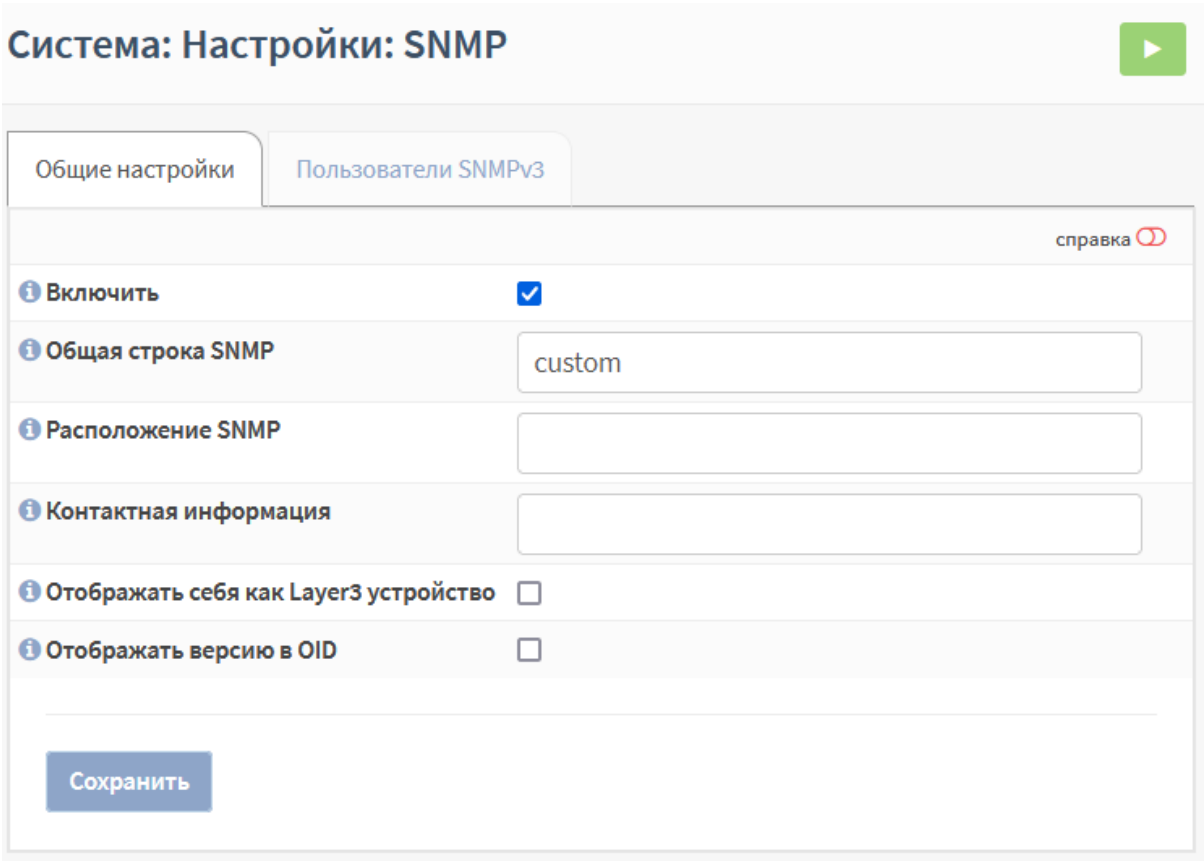


Рисунок – Настройка SNMP v.1, 2

Дополнительные параметры SNMP v.1, 2.

В качестве дополнительной информации возможно указать расположение **ARMA FW** и контактную информацию в полях **«Расположение SNMP»** и **«Контактная информация»** соответственно.

В случае установки флажка в параметре **«Отображать себя как Layer3 устройство»** устройство будет позиционировать себя, как устройство в сети на уровне L3, то есть устройство с IP-адресами на сетевом уровне модели OSI. По умолчанию **ARMA FW** работает в сети на уровне L2, то есть как устройство с MAC-адресом.

В случае установки флажка в параметре **«Отображать версию в OID»** будет передаваться OID устройства для идентификации поставщика данного устройства. Используется в случае, если по-другому получить информацию об установленной системе и других характеристиках устройства не получается через протокол SNMP.

9.1.2 Проверка работы SNMP v.1, 2

Для проверки работы SNMP будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для проверки SNMP). На ПК **«Admin»** установлено ПО мониторинга «PowerSNMP Free Manager».

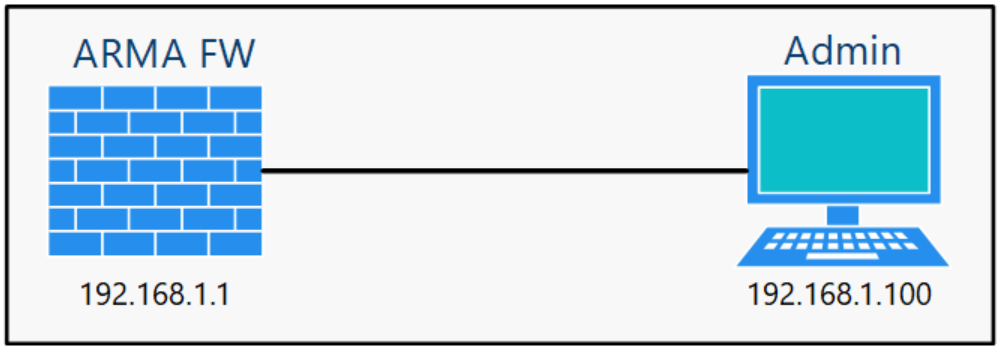


Рисунок – Схема стенда для проверки SNMP

Для проверки работы SNMP v.1, 2 необходимо выполнить следующие действия:

1. В ПО «PowerSNMP Free Manager» нажать **правой кнопкой мыши** на строку **«SNMP Agents»** и выбрать **«Add Agent»**.
2. В нижней части открывшегося окна нажать **кнопку «Add Agent»**, указать IP-адрес **ARMA FW**, в **«Community»** значение, указанное в настройках ранее (см. Настройка SNMP v.1, 2), выбрать версию протокола «1» или «2» и нажать **«OK»** (см. Рисунок – Добавление SNMP агента, SNMP v.1, 2).

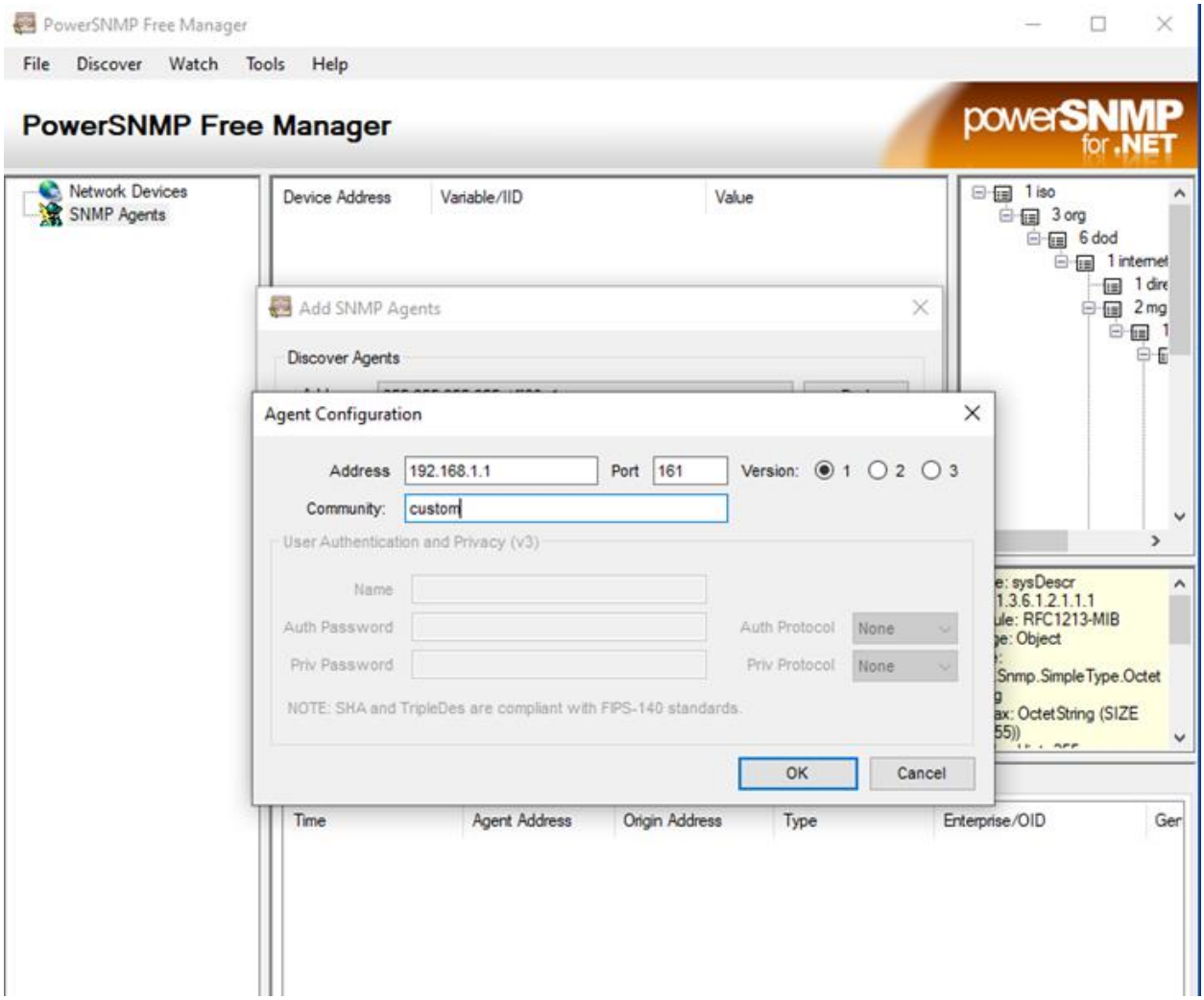


Рисунок – Добавление SNMP агента, SNMP v.1, 2

3. В правой области окна в дереве доступных данных выбрать поле **«1 sysDescr»**, нажать **правой кнопкой мыши** по IP-адресу **ARMA FW** и выбрать **«Query...»**. Результатом будет получение информации о значениях параметров **ARMA FW** (см. Рисунок – Информация о значениях параметров ARMA FW).

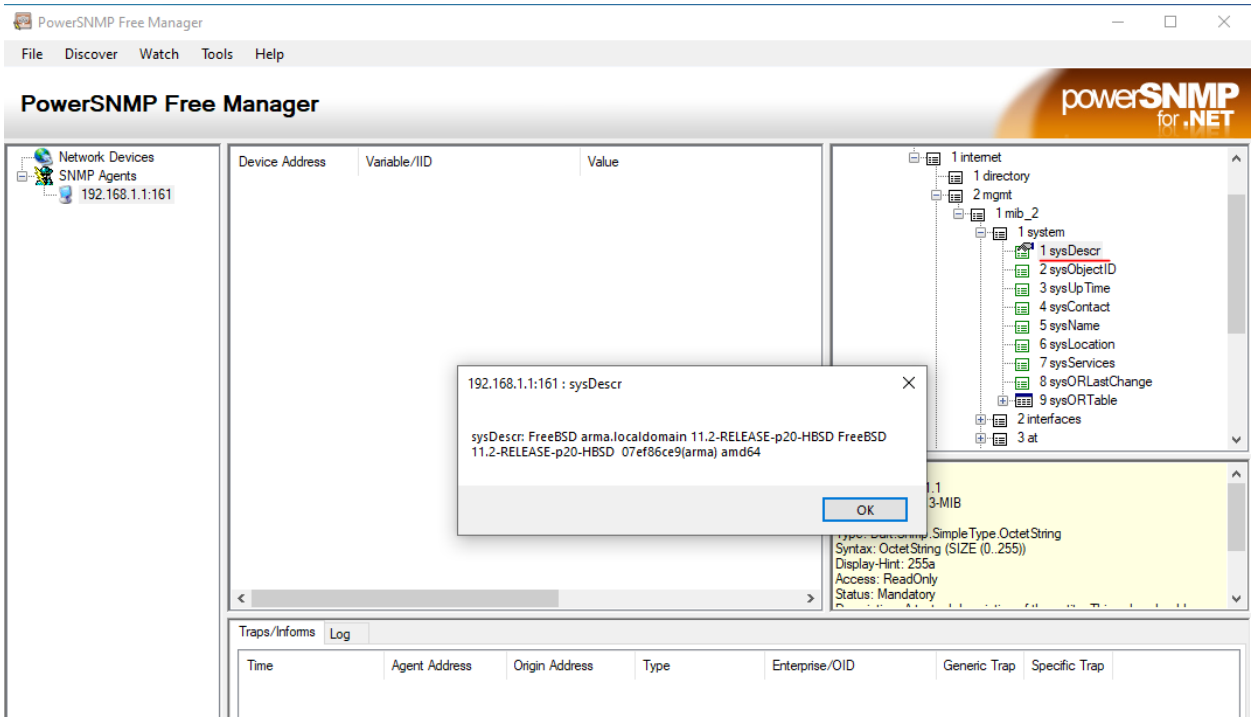


Рисунок – Информация о значениях параметров ARMA FW

9.2 SNMP v.3

Настройка SNMP v.3 подразумевает аутентификацию на основе имени пользователя и пароля, а также шифрование трафика.

9.2.1 Настройка SNMP v.3

Для настройки удалённого мониторинга по протоколу SNMP v.3 необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек SNMP (**«Система» - «Настройки» - «SNMP» - «Общие настройки»**) и установить флажок в параметре **«Включить»**.

2. Перейти во вкладку **«Пользователи SNMP v.3»** и нажать **кнопку** « + ».

3. В открывшейся форме (см. Рисунок – Добавление пользователя SNMP v.3) заполнить поля **«Имя пользователя»**, **«Пароль»**, **«Ключ шифрования»** и нажать **кнопку «Сохранить»**. Для возможности редактирования дерева MIB, созданным пользователем, необходимо установить флажок для параметра **«Разрешить запись»**. Параметры **«Алгоритм хеша»** и **«Тип шифрования»** меняются при необходимости.

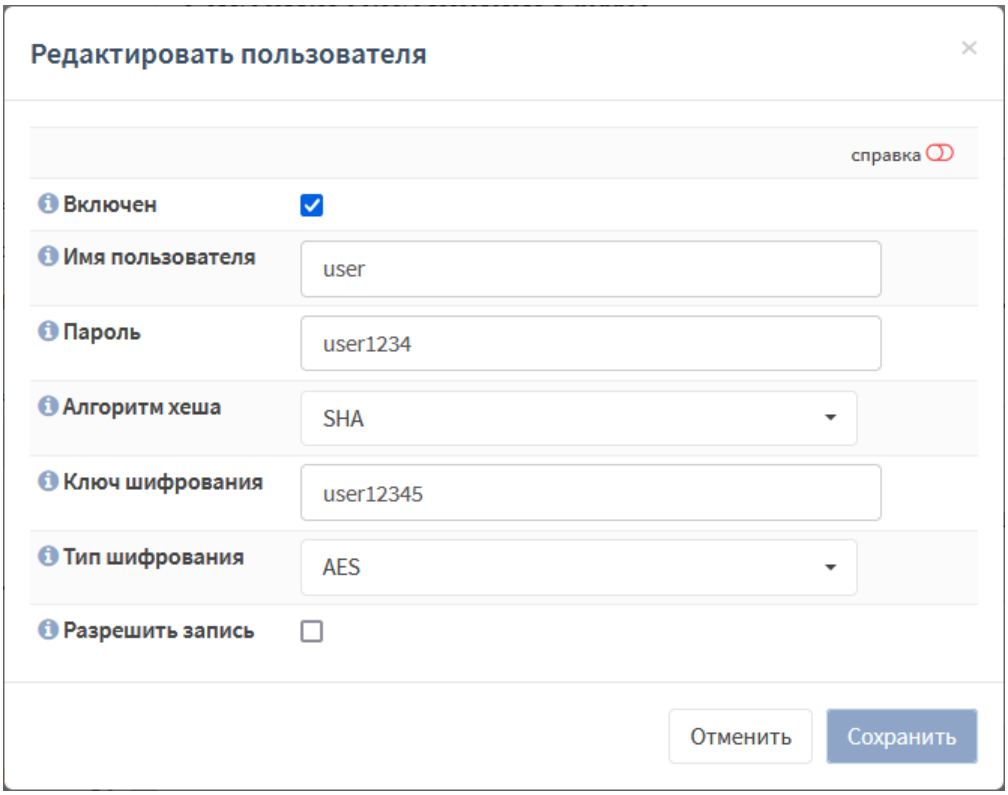


Рисунок – Добавление пользователя SNMP v.3

Примечание:

Пароль и ключ шифрования должен содержать от 8 до 64 символов. Допустимые символы:

```
0-9a-zA-Z._-!$%/()+#=
```

9.2.2 Проверка работы SNMP v.3

Для проверки работы SNMP будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для проверки SNMP). На ПК **«Admin»** установлено ПО мониторинга «PowerSNMP Free Manager».

Для проверки работы SNMP v.3 необходимо выполнить следующие действия:

1. В ПО «PowerSNMP Free Manager» нажать **правой кнопкой мыши** на строку **«SNMP Agents»** и выбрать **«Add Agent»**.
2. В нижней части открывшегося окна нажать **кнопку «Add Agent»**, указать IP-адрес **ARMA FW**, указать данные для аутентификации, заданные в настройках ранее (см. Настройка SNMP v.3), выбрать версию протокола «3» и нажать **«OK»** (см. Рисунок – Добавление SNMP агента (SNMP v.3)).

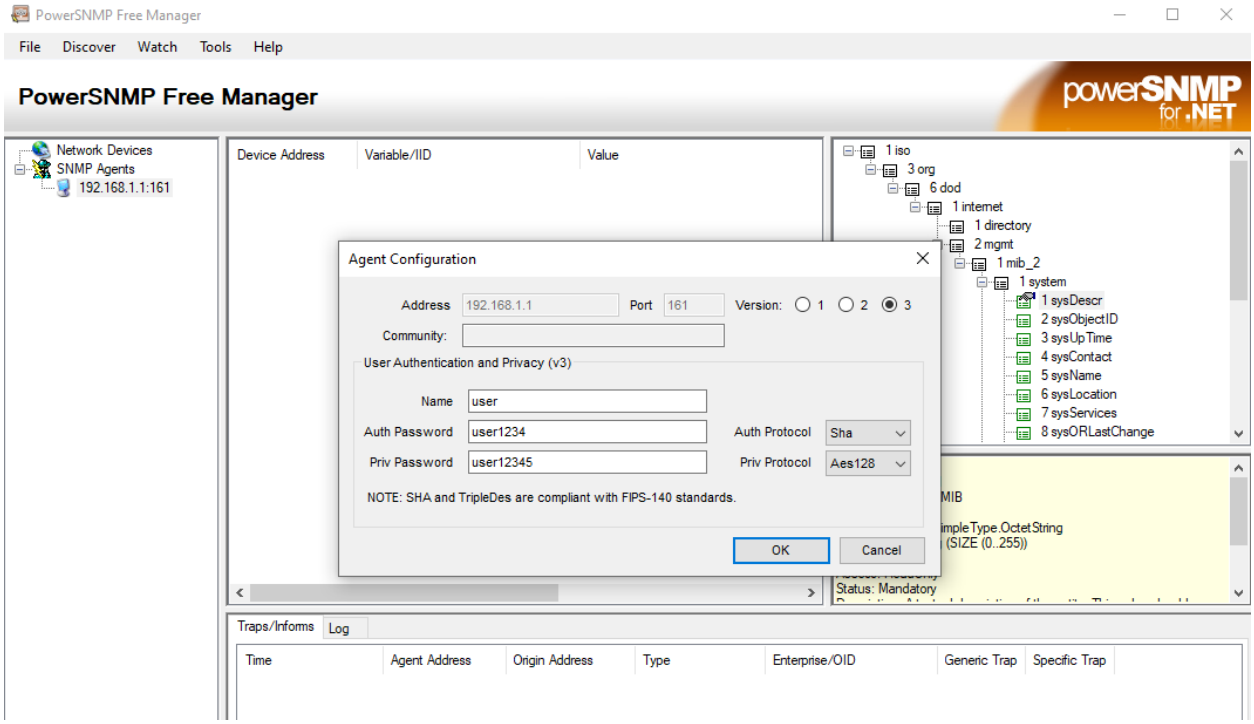


Рисунок – Добавление SNMP агента (SNMP v.3)

3. В правой области окна в дереве доступных данных выбрать поле **«1 sysDescr»**, нажать **правой кнопкой мыши** по IP-адресу **ARMA FW** и выбрать **«Query…»**. Результатом будет получение информации о значениях параметров **ARMA FW**.

10 СЕРВИС SYSLOG

Syslog – это стандарт отправки и регистрации сообщений о происходящих в системе событиях, используемый для удобства администрирования и обеспечения ИБ.

ARMA FW позволяет отправлять события безопасности модулей МЭ, СОВ, контроля промышленных протоколов, портала авторизации пользователей, а также системные события на внешний syslog-сервер или в SIEM-системы, а также в единый центр управления **ARMA MC**.

Процесс подключения **ARMA FW** к **ARMA MC** описан в разделе **«Подключение к ARMA MC»** Руководства администратора **ARMA FW**.

10.1 Настройка экспорта событий syslog

Для настройки экспорта событий необходимо выполнить следующие действия:

1. Перейти в настройки экспорта событий системы (**«Система» - «Настройки» - «Экспорт событий»**) и во вкладке **«Получатели»** нажать **кнопку** « + ».
2. В открывшейся форме (см. Рисунок – Добавление получателя внешнего syslog-сервера). установить флажок для параметра **«Включен»**.

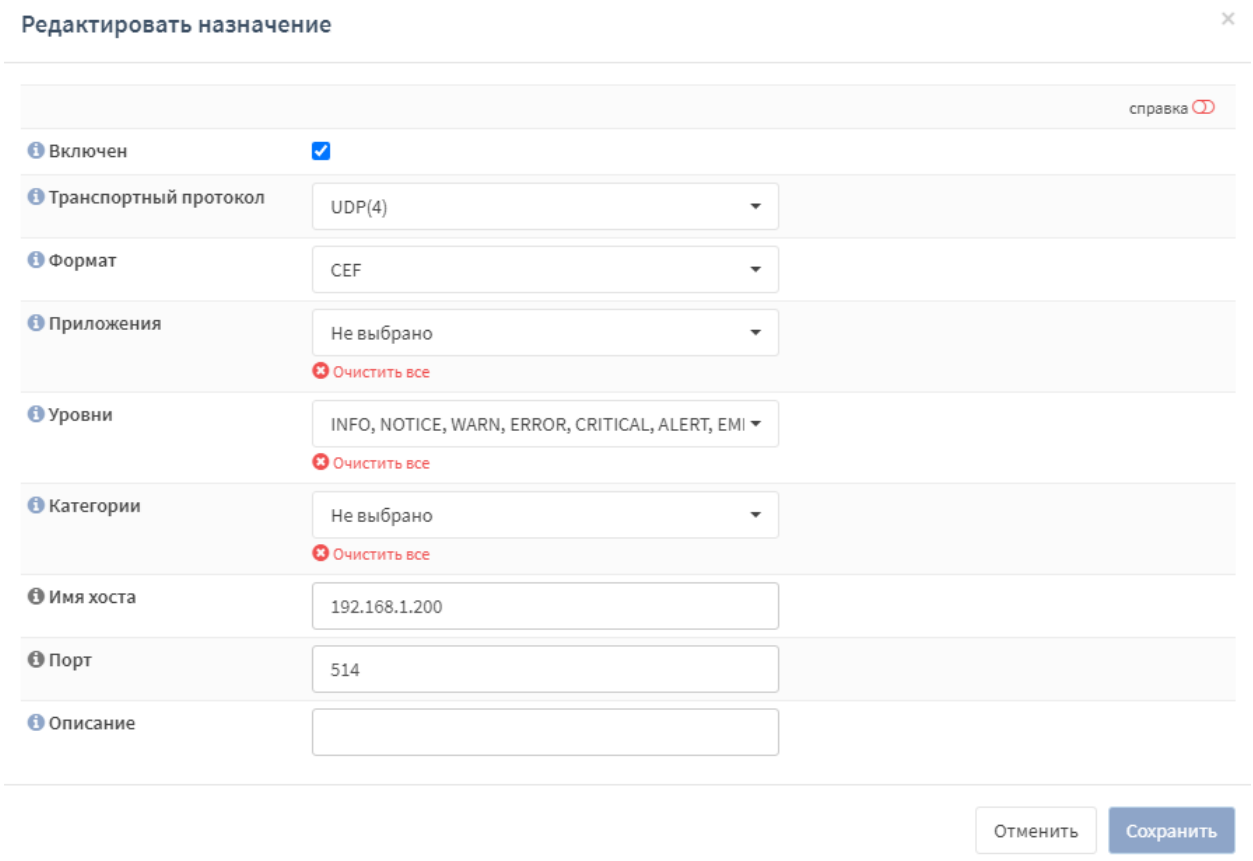


Рисунок – Добавление получателя внешнего syslog-сервера

3. Выбрать значения параметров:

- **«Формат»**;
- **«Транспортный протокол»**;
- **«Приложения»**;
- **«Уровни»**;
- **«Категории»**.

В параметрах **«Приложения»**, **«Уровни»** и **«Категории»** значение «Не выбрано» означает выбор всех значений.

4. Задать доменное имя и порт удалённого syslog-сервера в параметрах **«Имя хоста»** и **«Порт»** соответственно. Номер порта рекомендуется изменять только в тех случаях, когда отправка сообщений от **ARMA FW** будет происходить через порт, заданный в настройках удалённого syslog-сервера и отличный от стандартного 514.
5. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

10.2 Проверка экспорта событий syslog

Для проверки работы экспорта событий необходимо выполнить подключение к syslog-серверу и удостовериться в наличии событий от **ARMA FW**. В качестве syslog-сервера возможно использовать стороннее ПО, например, «Visual Syslog», в примере ниже будет описано подключение к продукту **ARMA MC**.

Настройка экспорта событий в единый центр управления **ARMA MC** описана в руководстве пользователя по эксплуатации **ARMA MC**. События от **ARMA FW** отображаются в журнале событий **ARMA MC** (**«Журналы» - «События»**) (см. Рисунок – Журнал событий ARMA Management Console).

В **ARMA FW** просмотр информации о переданных сообщениях осуществляется во вкладке **«Статические данные»** подраздела настройки экспорта событий (**«Система» - «Настройки» - «Экспорт событий»**) (см. Рисунок – Система: Настройки: Экспорт событий: Статистические данные).

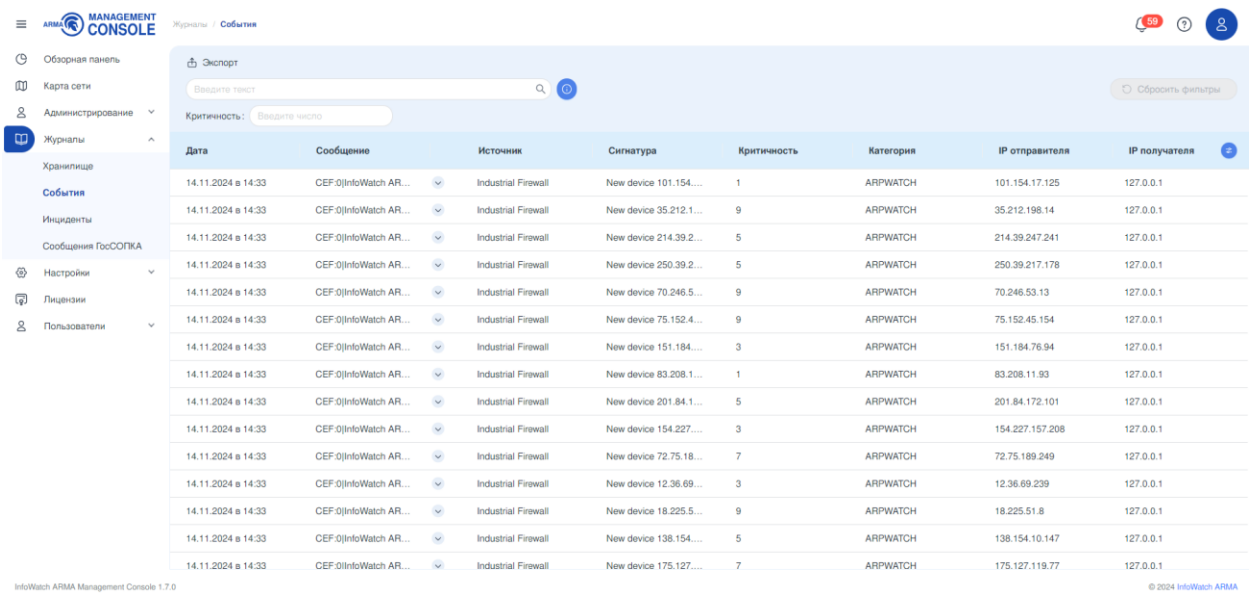


Рисунок – Журнал событий ARMA Management Console

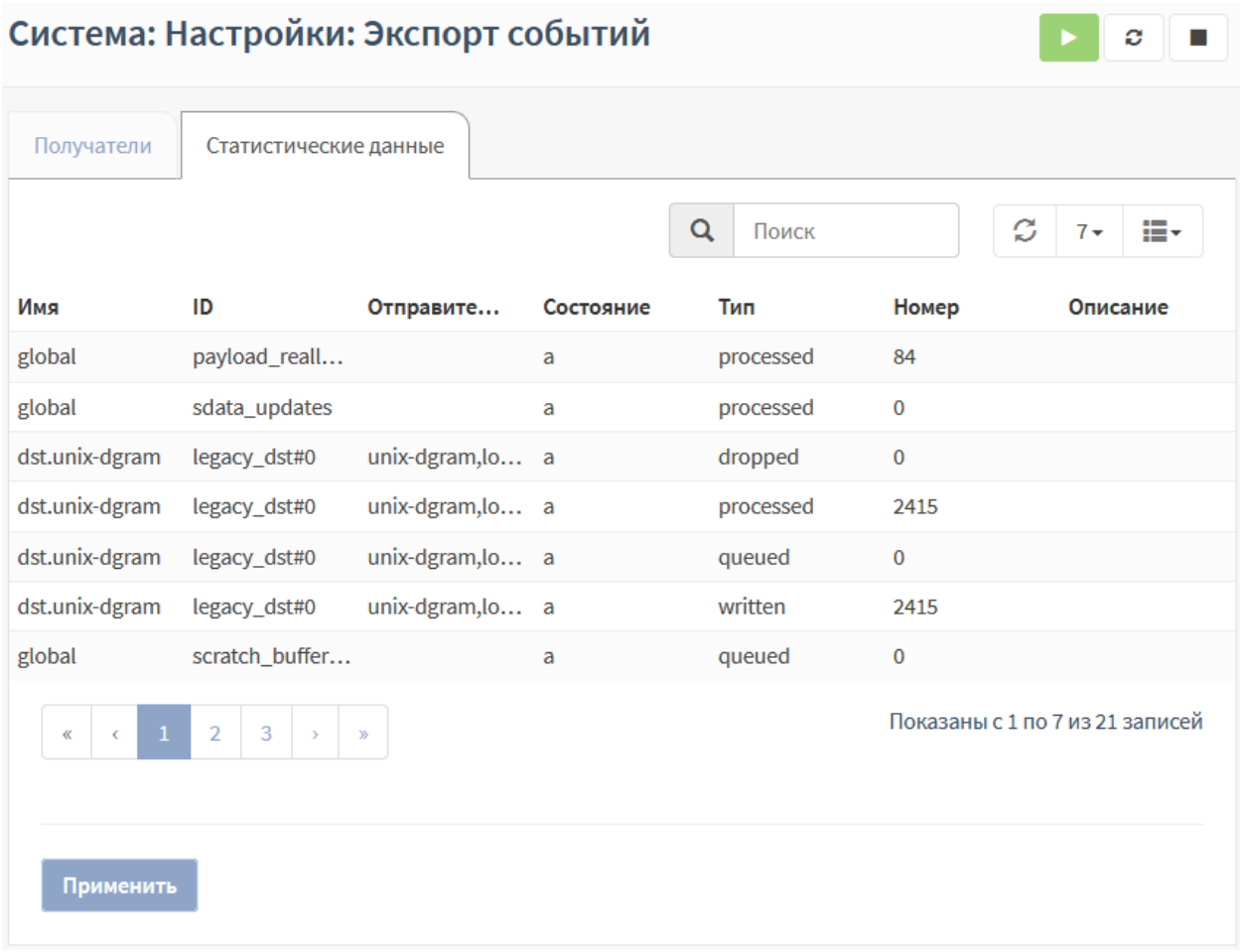


Рисунок – Система: Настройки: Экспорт событий: Статистические данные

11 SSH-СЕРВЕР

Сервер SSH обеспечивает безопасный удалённый доступ к управлению функциями локального, консольного интерфейса **ARMA FW**. По умолчанию используется порт 22.

Для подключения по протоколу SSH к **ARMA FW** возможно использовать различные SSH-клиенты, например:

- «OpenSSH» для UNIX-подобных ОС;
- «PuTTY» или «SecureCRT» для ОС Windows и Linux.

Для включения доступа по протоколу SSH необходимо перейти в подраздел настроек администрирования системы (**«Система» - «Настройки» - «Администрирование»**), в блоке настроек SSH установить флажок для параметра **«Включить безопасный shell»** (см. Рисунок – Включение SSH-сервера), при необходимости задать параметры доступа (см. Параметры доступа SSH) и нажать **кнопку «Сохранить»** внизу страницы.

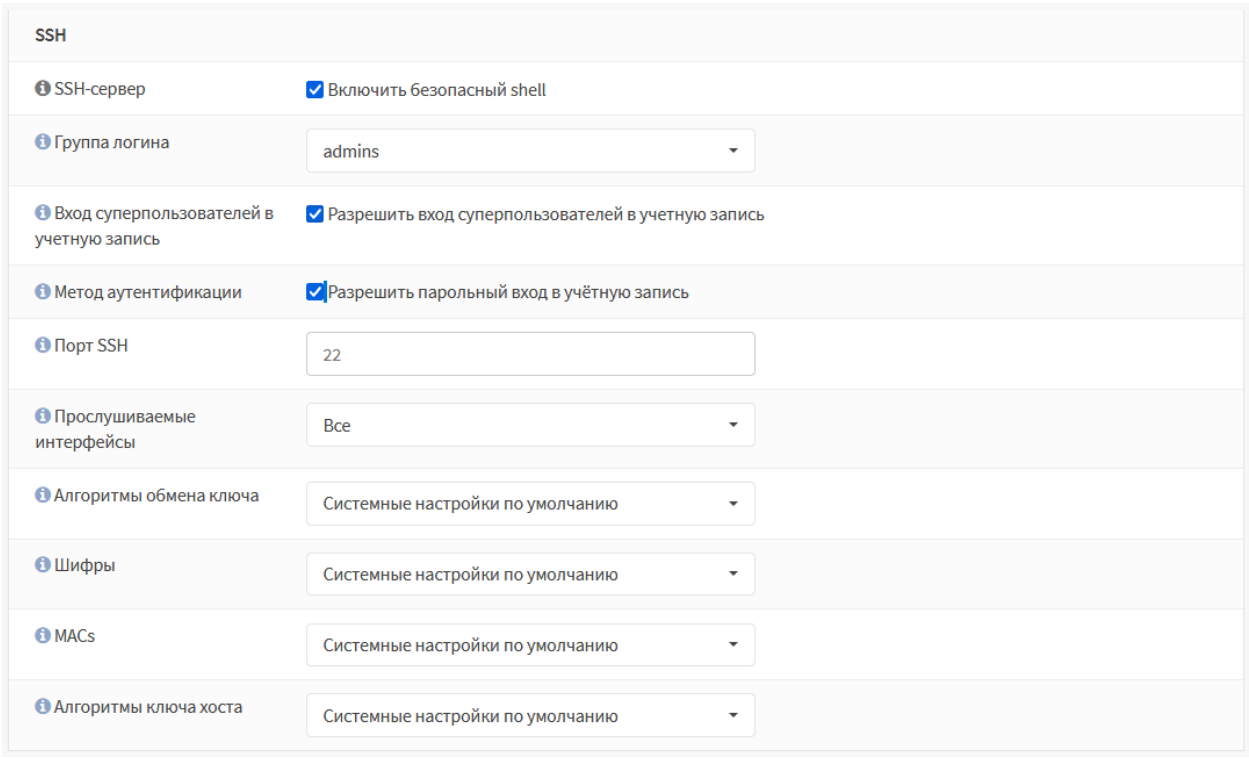


Рисунок – Включение SSH-сервера

Примечание:

Для возможности доступа должно быть создано разрешающее правило МЭ (см. Создание правил межсетевого экранирования) для заданного порта.

11.1 Параметры доступа SSH

В параметре **«Группа логина»** указывается группа пользователей, члены которой будут иметь доступ по протоколу SSH. Предоставление прав доступа по SSH отдельному пользователю описано в разделе Создание пользовательских учётных записей и их привилегий настоящего руководства.

При включённом значении «Разрешить вход суперпользователей в учетную запись» параметра **«Вход суперпользователей в учетную запись»** будет разрешён доступ с УЗ «root», рекомендуется не включать данное значение в целях безопасности.

При включённом значении «Разрешите парольный вход в учетную запись» для параметра **«Метод аутентификации»** будет задан метод аутентификации по паролю. При выключенном значении «Разрешите парольный вход в учетную запись» будет задан метод аутентификации по авторизированным ключам для каждого отдельного пользователя, которому предоставлен доступ по протоколу SSH. Генерация ключей в таком случае будет выполняться сторонним ПО.

Например, в случае использования для подключения ПО «PuTTY», генерацию ключей возможно выполнить с помощью ПО «PuTTYgen», по умолчанию устанавливаемым вместе с ПО «PuTTY». При генерации ключей будет создана пара ключей:

- **«Public key, открытый ключ»** – хранится в памяти приложения;
- **«Private key, закрытый ключ»** – необходимо указать в настройках определённого пользователя **ARMA FW** в поле параметра **«Авторизованные ключи»** формы редактирования УЗ (**«Система» - «Доступ» - «Пользователи»**) (см. Создание пользовательских учётных записей и их привилегий).

В параметре **«Прослушиваемые интерфейсы»** рекомендуется оставлять только внутренние интерфейсы.

Дополнительные параметры шифрования:

- **«Алгоритмы обмена ключа»**;
- **«Шифры»**;
- **«MACs»**;
- **«Алгоритмы ключа хоста»**;

рекомендуется изменять только при необходимости, так как некорректные значения указанных параметров могут привести к уменьшению уровня безопасности SSH-соединения или потере доступности SSH-сервиса для легитимных пользователей.

Настройка SSH-сервера считается успешной, в случае доступа к консольному интерфейсу **ARMA FW** после подключения (см. Рисунок – Доступ к консольному интерфейсу по протоколу SSH).

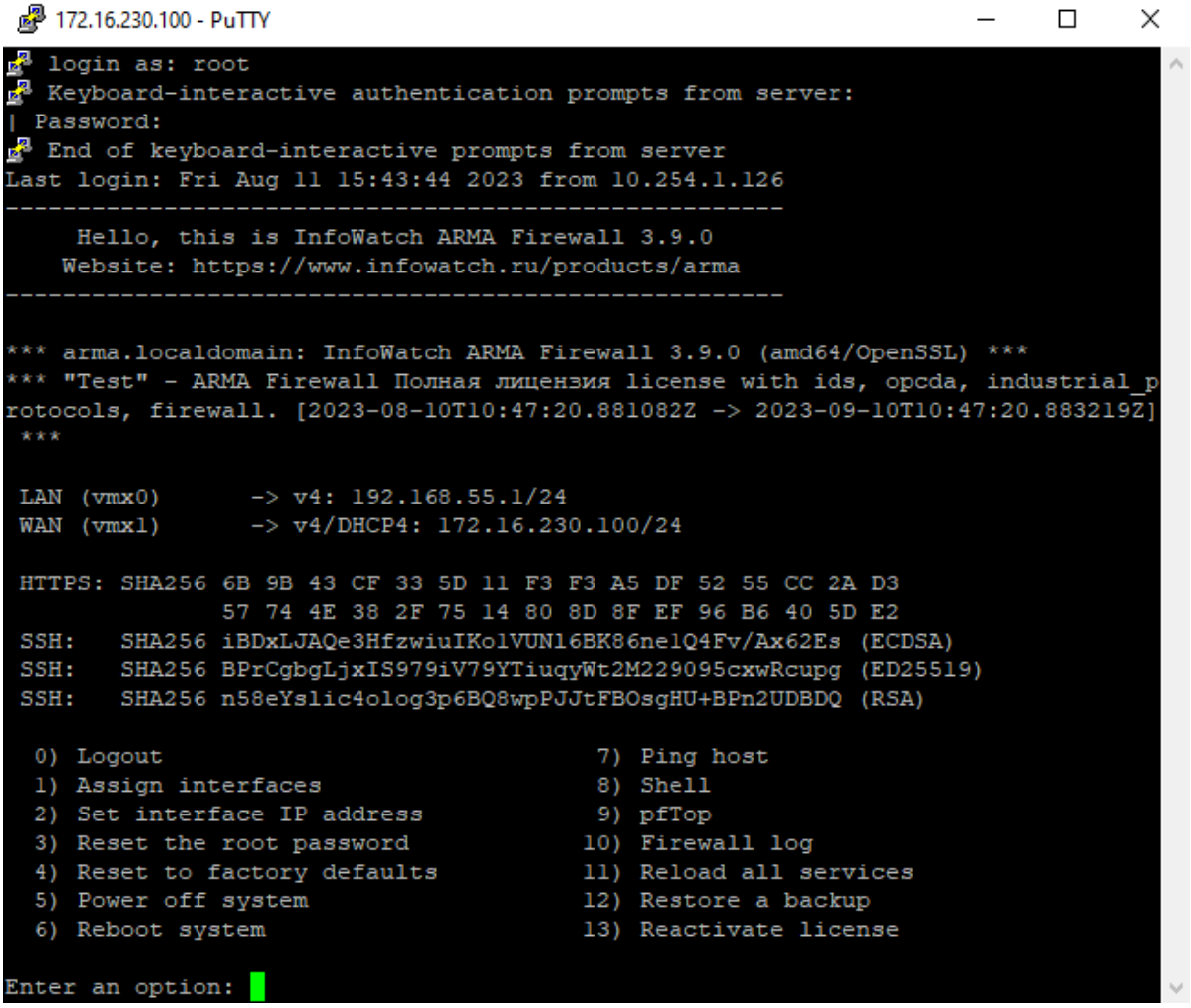


Рисунок – Доступ к консольному интерфейсу по протоколу SSH

12 СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Статическая маршрутизация – это запись маршрутизации, настроенная вручную, без применения протоколов маршрутизации. После установки статического маршрута пакет для заданного назначения будет перенаправлен на путь, указанный ранее. Данный тип маршрутизации применяется при взаимодействии сети с одной или двумя другими сетями.

Статические маршруты используются в случае, когда узлы или сети доступны через маршрутизатор, отличный от шлюза по умолчанию. Маршрутизаторы, через которые осуществляется доступ к другим сетям, предварительно необходимо добавить в качестве шлюзов.

12.1 Настройка шлюзов

Для добавления и настройки шлюза необходимо перейти в подраздел настройки единичных шлюзов (**«Система» - «Шлюзы» - «Единичный»**), нажать **кнопку «+Добавить»**, в открывшейся форме (см. Рисунок – Настройки шлюза) задать параметры шлюза, нажать **кнопку «Сохранить»** и нажать **кнопку «Применить изменения»**.

Параметры **«Имя»**, **«Интерфейс»**, **«Семейство адресов»** и **«IP-адрес»** являются необходимыми для заполнения.

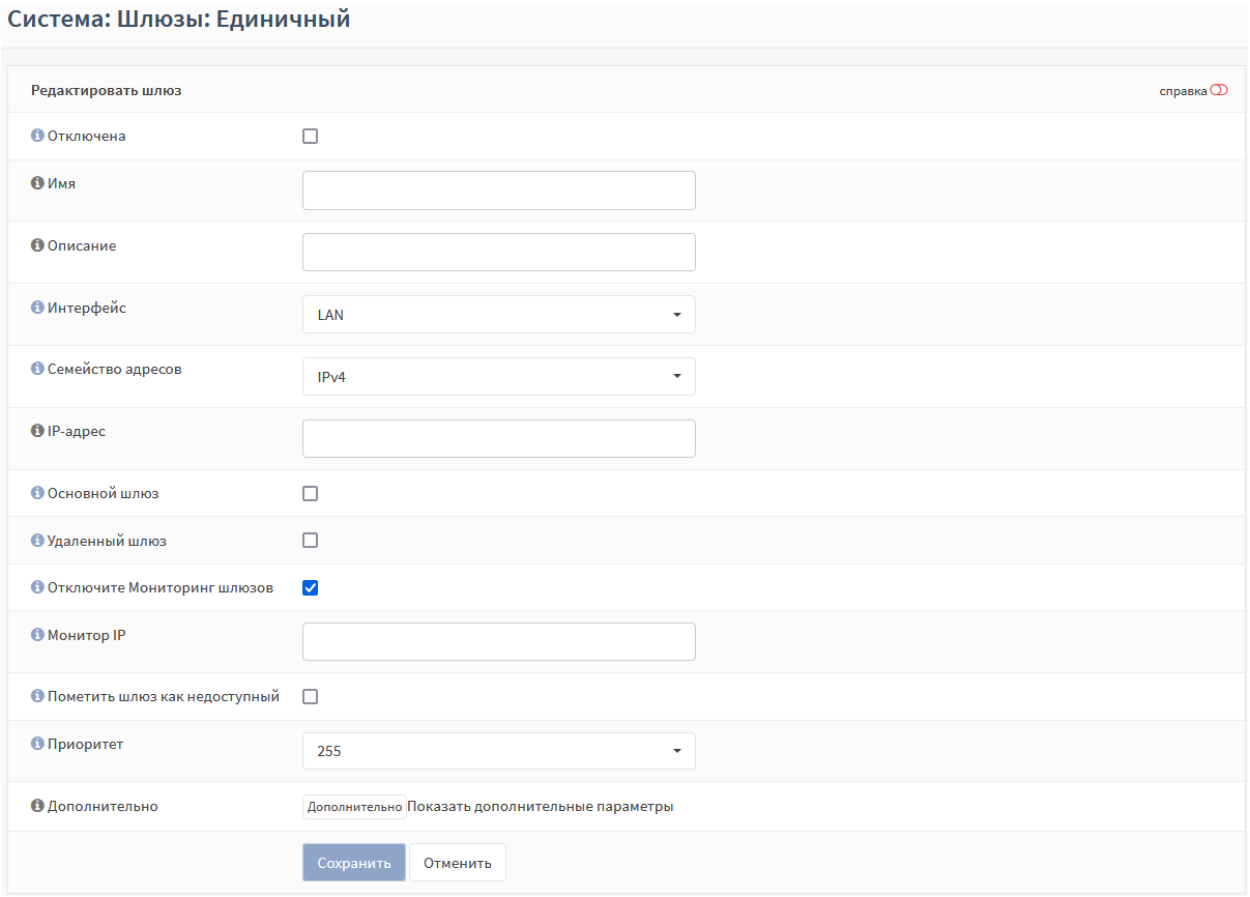


Рисунок – Настройки шлюза

Для указания шлюза по умолчанию необходимо установить флажок для параметра **«Основной шлюз»**.

Для разрешения существовать шлюзу за пределами подсети интерфейса необходимо установить флажок для параметра **«Удаленный шлюз»**.

По умолчанию демон мониторинга шлюза периодически проверяет связь с каждым шлюзом, чтобы отслеживать задержку и потерю пакетов для трафика на отслеживаемый IP-адрес. Эти данные используются для информации о состоянии шлюза, а также для построения графика RRD.

Для отключения мониторинга необходимо установить флажок для параметра **«Отключите Мониторинг шлюзов»**. Мониторинг используется для отслеживания задержки и потери пакетов трафика для отслеживаемого IP-адреса. Данные используются для получения статуса состояния шлюза и построения графика RRD.

Для принудительного обозначения шлюза в качестве недоступного необходимо установить флажок для параметра **«Пометить шлюз как недоступный»**. Данная функциональность может применяться в случае необходимости обеспечения возможности использования какого-либо иного маршрута по умолчанию, например, полученного по протоколу динамической маршрутизации.

Примечание:

Совместно с установкой флажка для параметра **«Пометить шлюз как недоступный»** необходимо снять флажок для параметра **«Основной шлюз»** (см. Рисунок – Обозначение шлюза в качестве недоступного).

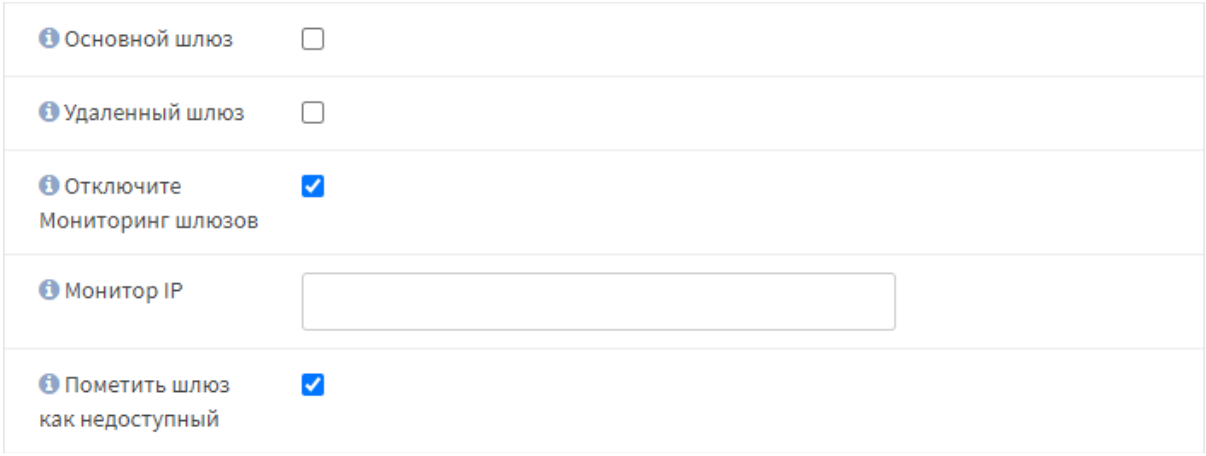


Рисунок – Обозначение шлюза в качестве недоступного

В случае необходимости настройки Multi-WAN – нескольких WAN, доступ к расширенным параметрам возможно получить, нажав **кнопку «Дополнительно»** (см. Рисунок – Расширенные параметры настройки шлюза).

Примечание:

В большинстве случаев эти параметры не подлежат изменению.

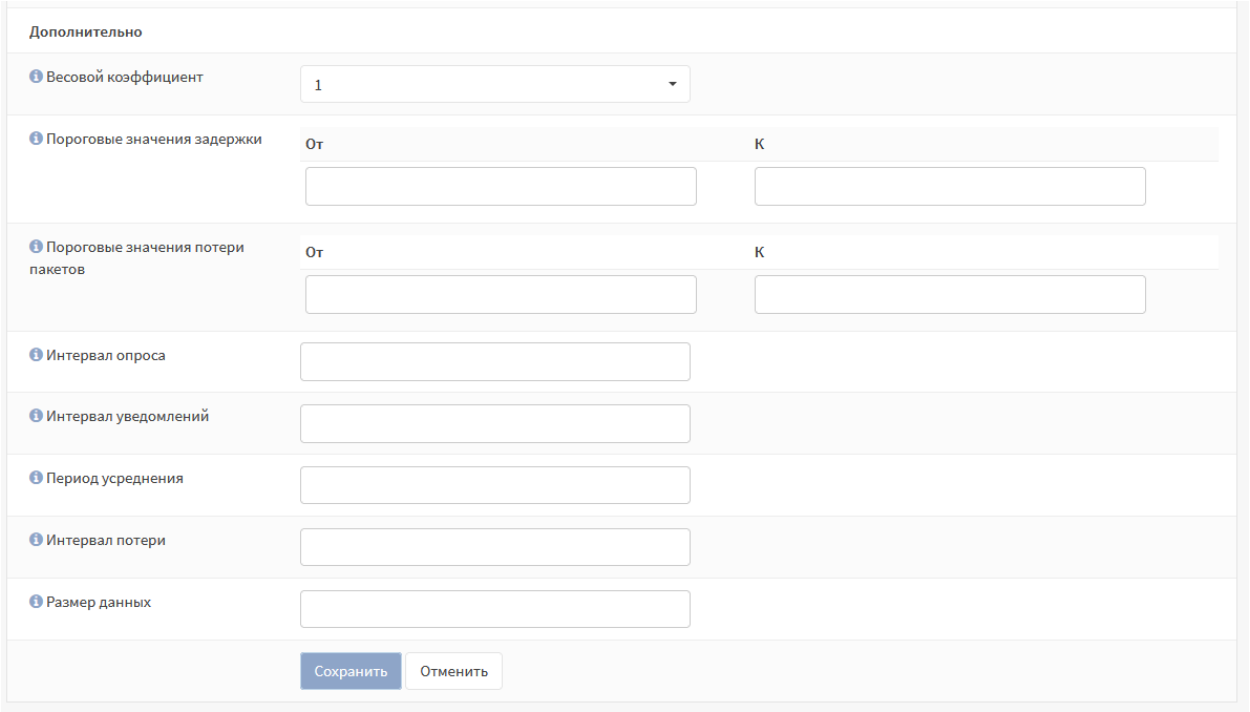


Рисунок – Расширенные параметры настройки шлюза

Для обеспечения балансировки нагрузки, аварийного переключения или маршрутизации, основанной на правилах, в **ARMA FW** предусмотрена возможность добавления группы шлюзов.

Для добавления и настройки группы шлюзов необходимо перейти в подраздел настройки группы шлюзов (**«Система» - «Шлюзы» - «Группы»**), нажать **кнопку «+Добавить»**, в открывшейся форме (см. Рисунок – Добавление группы шлюзов) задать параметры группы шлюзов и нажать **кнопку «Сохранить»**.

Параметры **«Имя группы»** и **«Приоритет шлюзов»** являются необходимыми для заполнения.

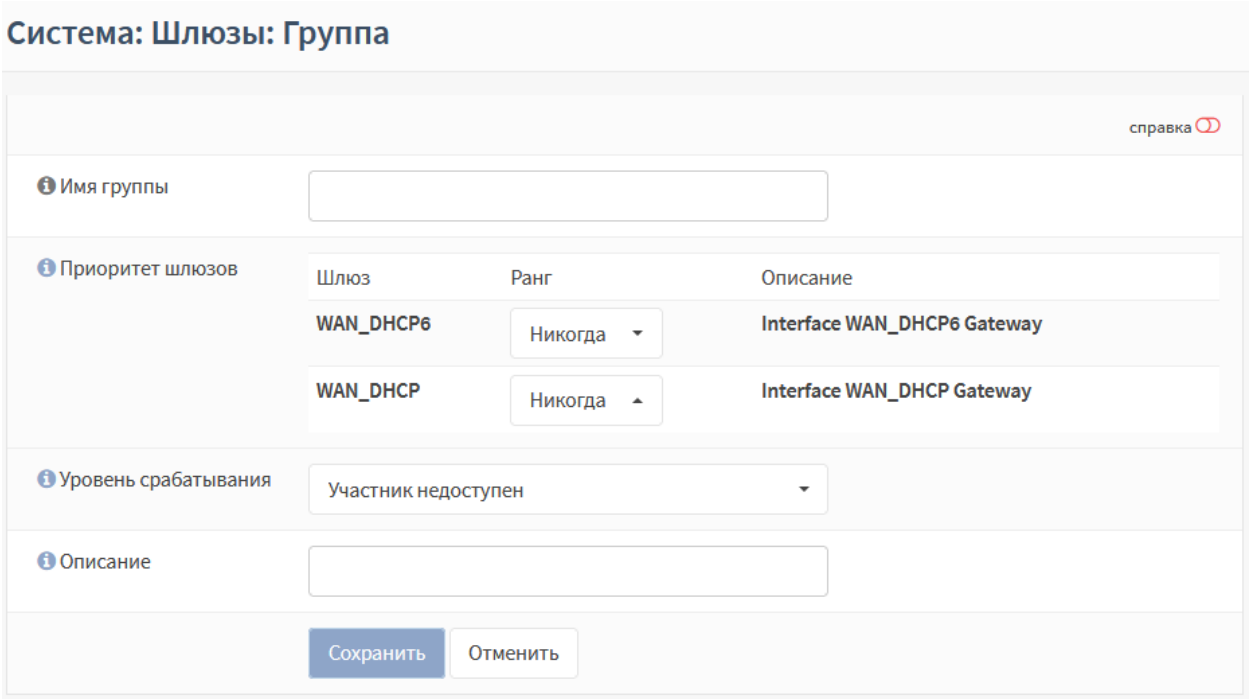


Рисунок – Добавление группы шлюзов

В блоке **«Приоритет шлюзов»** необходимо выбрать шлюзы, входящие в создаваемую группу, и определить для них уровень приоритета в столбце **«Ранг»**: от «1» до «5». Для исключения шлюза из создаваемой группы необходимо выбрать значение уровня приоритета «Никогда».

Примечание:

Более низкие значения имеют более высокий приоритет. Например, шлюзы уровня «Ранг 1» используются перед шлюзами уровня «Ранг 2» и т.д.

Параметр **«Уровень срабатывания»** отвечает за то, как **ARMA FW** будет управлять записями группы шлюзов при возникновении определённых событий. Доступны следующие уровни:

- **«Участник недоступен»** – отмечает шлюз как неработающий только тогда, когда он полностью отключён, превышая один или оба более высоких пороговых значения, настроенных для шлюза;
- **«Потеря пакетов»** – отмечает шлюз как неработающий, когда потеря пакетов превышает нижний порог оповещения;
- **«Высокая задержка»** – отмечает шлюз как неработающий, когда задержка превышает нижний порог оповещения;
- **«Потеря пакетов или высокая задержка»** – отмечает шлюз как неработающий для любого типа предупреждений.

12.2 Настройка статических маршрутов

Конфигурация статического маршрута осуществляется в подразделе настройки маршрутизации (**«Система» - «Маршруты» - «Конфигурация»**).

Для добавления маршрута необходимо нажать **кнопку** « + », указать адрес сети конечной точки маршрута и шлюз (см. Рисунок – Настройка конфигурации статического маршрута), при необходимости добавить описание маршрута, нажать **кнопку «Сохранить»** и нажать **кнопку «Применить»**.

Адрес сети задаётся в формате CIDR:

- [адрес сети]/[маска сети], например, «192.168.1.0/24».

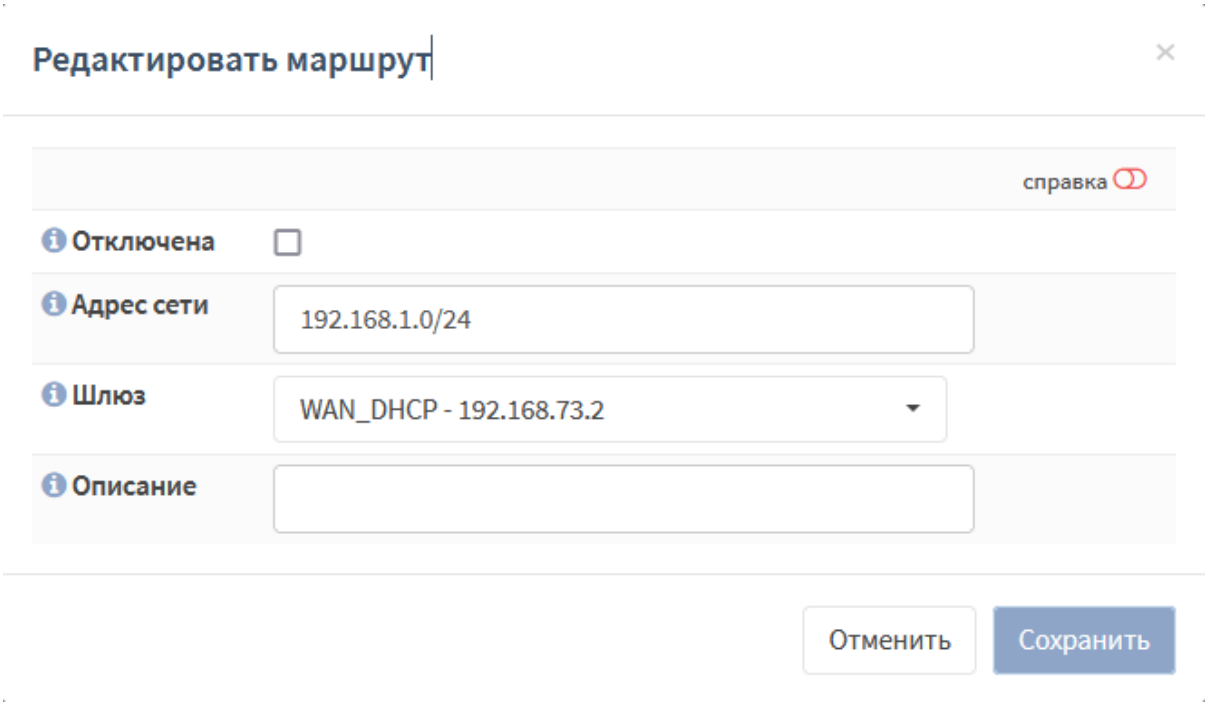


Рисунок – Настройка конфигурации статического маршрута

12.2.1 Пример реализации статического маршрута

В качестве примера работы статического маршрута будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки статического маршрута). Необходимо добиться прохождения трафика от ПК **«Server»** до ПК **«Client»**. На каждом **ARMA FW** предварительно должно быть создано правило МЭ (см. Создание правил межсетевого экранирования) для интерфейса **«[WAN]»**, разрешающее прохождение трафика по протоколу ICMP.

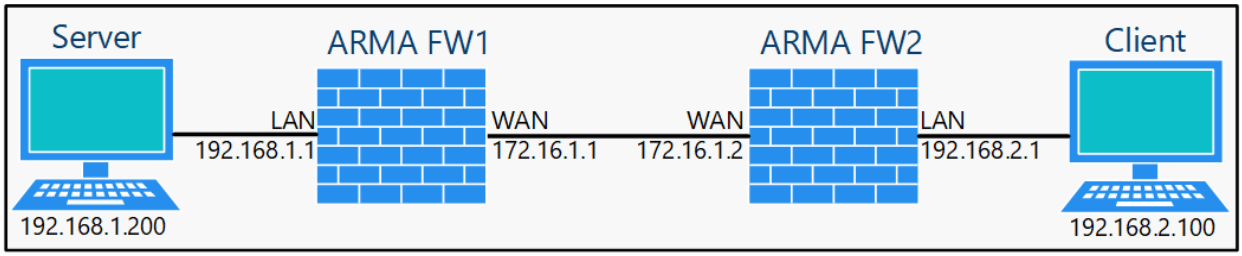


Рисунок – Схема стенда для настройки статического маршрута

Для реализации прохождения трафика необходимо выполнить следующие действия:

1. Добавить на каждом **ARMA FW** единичный шлюз.
2. Добавить на каждом **ARMA FW** статические маршруты.

Для каждого **ARMA FW** необходимо добавить единичный шлюз (см. Настройка шлюзов) с параметрами, указанными в таблице (см. Таблица «Значения параметров единичных шлюзов»).

Таблица «Значения параметров единичных шлюзов»

Параметр	ARMA FW1	ARMA FW2
Имя	GW_AFW1	GW_AFW2
Интерфейс	WAN	WAN
Семейство адресов	IPv4	IPv4
IP-адрес	172.16.1.2	172.16.1.1

Для связи сетей «192.168.1.0/24» и «192.168.2.0/24» необходимо добавить статические маршруты (см. Настройка статических маршрутов) с параметрами, указанными в таблице (см. Таблица «Значения параметров статических маршрутов»).

Таблица «Значения параметров статических маршрутов»

Параметр	ARMA FW1	ARMA FW2
Адрес сети	192.168.2.0/24	192.168.1.0/24
Шлюз	GW_AFW1 - 172.16.1.2	GW_AFW2 - 172.16.1.1

Для проверки работы статического маршрута необходимо на ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**. Успешным результатом выполнения команды является отображение маршрута трафика (см. Рисунок – Трассировка маршрута).

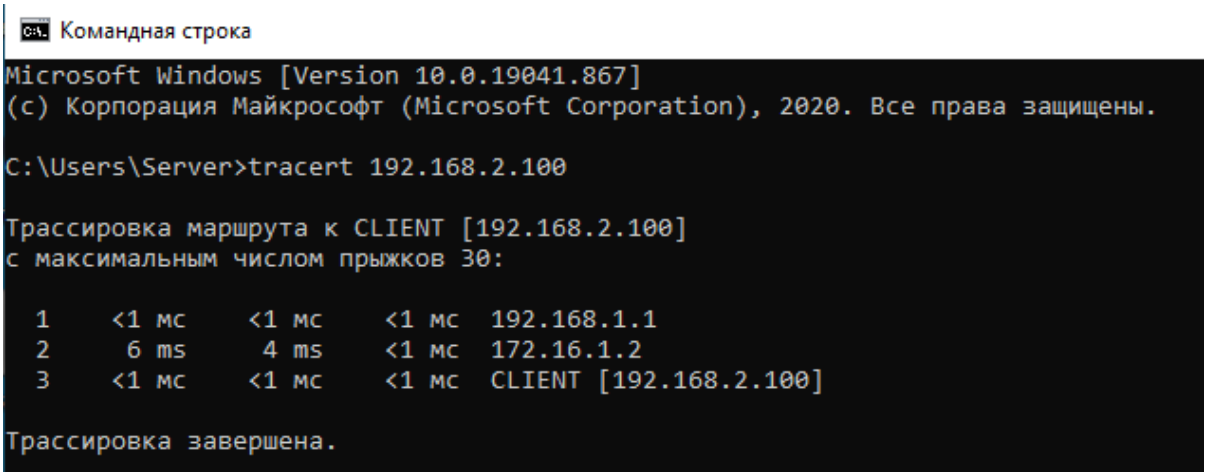


Рисунок – Трассировка маршрута

13 ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Динамическая маршрутизация – это вид маршрутизации, в котором отличительной особенностью является автоматический выбор оптимального маршрута при прохождении трафика между поддерживающими динамическую маршрутизацию сетевыми устройствами.

ARMA FW поддерживает динамическую маршрутизацию по протоколам RIP v.1 и v.2, OSPF, BGP.

13.1 RIP

Данный протокол применяется в небольших компьютерных сетях и позволяет маршрутизаторам динамически обновлять маршрутную информацию, получая её от соседних маршрутизаторов.

13.1.1 Настройка динамической маршрутизации RIP

В качестве примера приведена настройка динамической маршрутизации на трёх **ARMA FW** согласно схеме стенда, представленной на рисунке (см. Рисунок – Схема стенда для настройки динамической маршрутизации).

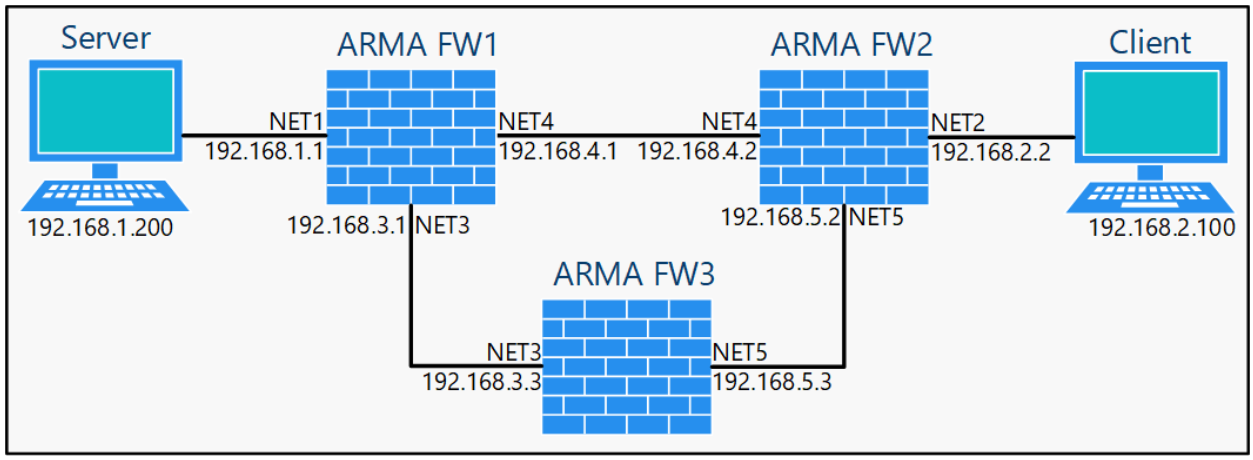


Рисунок – Схема стенда для настройки динамической маршрутизации

Перечень интерфейсов со значениями IP-адресов для каждого **ARMA FW** приведён в таблице (см. Таблица «Перечень интерфейсов»).

Таблица «Перечень интерфейсов»

Интерфейс	ARMA FW1	ARMA FW2	ARMA FW3
NET1	192.168.1.1/24	–	–
NET2	–	192.168.2.2/24	–
NET3	192.168.3.1/24	–	192.168.3.3/24
NET4	192.168.4.1/24	192.168.4.2/24	–
NET5	–	192.168.5.2/24	192.168.5.3/24

На каждом **ARMA FW** предварительно необходимо создать разрешающее правило МЭ (см. Создание правил межсетевого экранирования) на интерфейсах **[NETx]**, где «x» – порядковый номер интерфейса, с параметрами, указанными в таблице (см. Таблица «Значения параметров правила для интерфейсов»).

Таблица «Значения параметров правила для интерфейсов»

Параметр	Значение
Действие	Разрешить (Pass)
Интерфейс	NETx, где «x» – порядковый номер интерфейса
Направление	Любой
Протокол	ICMP

Для настройки динамической маршрутизации по протоколу RIP необходимо выполнить следующие действия:

1. На каждом **ARMA FW** перейти в подраздел общих настроек маршрутизации (**«Маршрутизация» - «Общие настройки»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Включение сервиса маршрутизации) для включения сервиса маршрутизации.

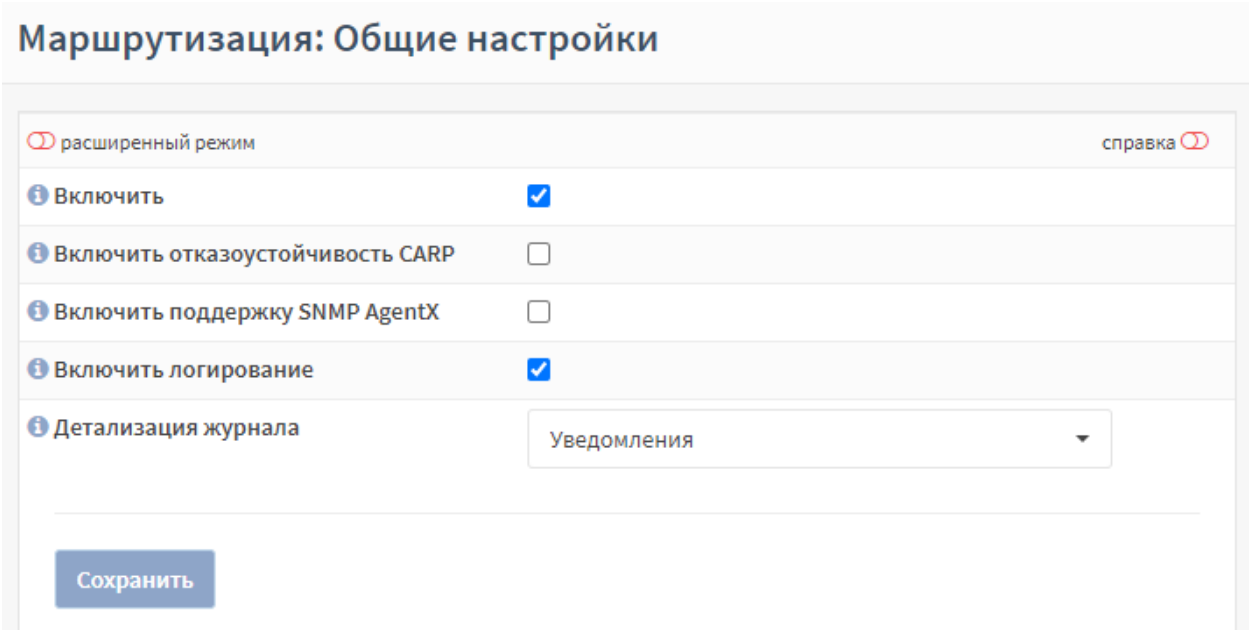


Рисунок – Включение сервиса маршрутизации

2. На каждом **ARMA FW** перейти в подраздел настроек маршрутизации RIP (**«Маршрутизация» - «RIP»**), установить флажок для параметра **«Включить»**, указать параметры маршрутизации:
   - **ARMA FW1**:

- **«Версия»** – «2»;
- **«Пассивные интерфейсы»** – «NET1»;
- **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)»;
- **«Сети»** – «192.168.3.0/24», «192.168.4.0/24»;

- **ARMA FW2**:
  - **«Версия»** – «2»;
  - **«Пассивные интерфейсы»** – «NET2»;
  - **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)»;
  - **«Сети»** – «192.168.4.0/24», «192.168.5.0/24»;
- **ARMA FW3**:
  - **«Версия»** – «2»;
  - **«Пассивные интерфейсы»** – «Не выбрано»;
  - **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)»;
  - **«Сети»** – «192.168.3.0/24», «192.168.5.0/24».

13.1.2 Проверка работы динамической маршрутизации RIP

Для проверки динамической маршрутизации необходимо выполнить следующие действия:

1. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, зафиксировать маршрут прохождения трафика (см. Рисунок – Результат выполнения команды трассировки).

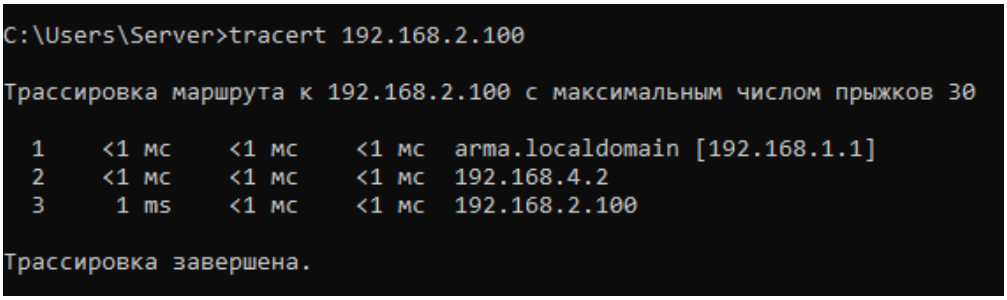


Рисунок – Результат выполнения команды трассировки

2. Отключить сетевой интерфейс NET4 на **ARMA FW1** и **ARMA FW2** и дождаться перестроения маршрутов – до 5 минут.

3. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, убедиться в смене маршрута (см. Рисунок – Результат выполнения команды трассировки).

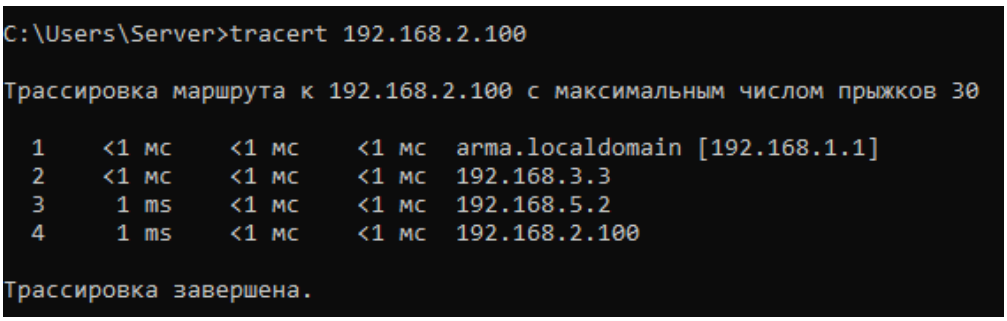


Рисунок – Результат выполнения команды трассировки

13.2 OSPF

Данный протокол основан на технологии отслеживания состояния канала – «link-state technology» и использующий алгоритм поиска кратчайшего пути. OSPF представляет собой протокол внутреннего шлюза и распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

13.2.1 Настройка динамической маршрутизации OSPF

В качестве примера приведена настройка динамической маршрутизации на трёх **ARMA FW** согласно схеме стенда, представленной на рисунке (см. Рисунок – Схема стенда для настройки динамической маршрутизации).

Перечень интерфейсов со значениями IP-адресов для каждого **ARMA FW** приведён в таблице (см. Таблица «Перечень интерфейсов»).

На каждом **ARMA FW** предварительно необходимо создать разрешающее правило МЭ (см. Создание правил межсетевого экранирования) на интерфейсах **[NETx]**, где «x» – порядковый номер интерфейса, с параметрами, указанными в таблице (см. Таблица «Значения параметров правила для интерфейсов»).

Для настройки динамической маршрутизации по протоколу OSPF необходимо выполнить следующие действия:

1. На каждом **ARMA FW** перейти в подраздел общих настроек маршрутизации (**«Маршрутизация» - «Общие настройки»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Включение сервиса маршрутизации) для включения сервиса маршрутизации.

   Примечание:

   В случае настройки маршрутизации OSPF на **ARMA FW**, используемых в режиме отказоустойчивого кластера, необходимо установить флажок для параметра **«Включить отказоустойчивость CARP»**.

2. На каждом **ARMA FW** перейти в подраздел настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), установить флажок для параметра **«Включить»**, указать параметры маршрутизации:
   - **ARMA FW1**:
     - **«Пассивные интерфейсы»** – «NET1»;
     - **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)»;
   - **ARMA FW2**:
     - **«Пассивные интерфейсы»** – «NET2»;
     - **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)»;
   - **ARMA FW3**:
     - **«Пассивные интерфейсы»** – «Не выбрано»;
     - **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)».
3. На каждом **ARMA FW** перейти во вкладку **«Сети»** подраздела настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), нажать **кнопку** « + », указать параметры сетей согласно таблице (см. Таблица «Параметры сетей для протокола OSPF») и нажать **кнопку «Сохранить»**. Действие выполнить для каждой сети в таблице.

Таблица «Параметры сетей для протокола OSPF»

Параметр	Сеть	ARMA FW1	ARMA FW2	ARMA FW3
Адрес сети	№1	192.168.3.0	192.168.4.0	192.168.3.0
Адрес сети	№2	192.168.4.0	192.168.5.0	192.168.5.0
Область	№1	0.0.0.0	0.0.0.0	0.0.0.0
Область	№2	0.0.0.0	0.0.0.0	0.0.0.0

13.2.2 Проверка работы динамической маршрутизации OSPF

Для проверки динамической маршрутизации необходимо выполнить следующие действия:

1. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, зафиксировать маршрут прохождения трафика (см. Рисунок – Результат выполнения команды трассировки).

```
C:\Users\Server>tracert 192.168.2.100

Трассировка маршрута к 192.168.2.100 с максимальным числом прыжков 30

  1    <1 мс    <1 мс    <1 мс  arma.localdomain [192.168.1.1]
  2    <1 мс    <1 мс    <1 мс  192.168.4.2
  3     1 ms    <1 мс    <1 мс  192.168.2.100

Трассировка завершена.
```

Рисунок – Результат выполнения команды трассировки

2. Отключить сетевой интерфейс NET4 на **ARMA FW1** и **ARMA FW2** и дождаться перестроения маршрутов – до 5 минут.
3. На ПК **«Server»** запустить командную строку и выполнить команду трассировки до ПК **«Client»**, убедиться в смене маршрута (см. Рисунок – Результат выполнения команды трассировки).

```
C:\Users\Server>tracert 192.168.2.100

Трассировка маршрута к 192.168.2.100 с максимальным числом прыжков 30

  1    <1 мс    <1 мс    <1 мс  arma.localdomain [192.168.1.1]
  2    <1 мс    <1 мс    <1 мс  192.168.3.3
  3     1 ms    <1 мс    <1 мс  192.168.5.2
  4     1 ms    <1 мс    <1 мс  192.168.2.100

Трассировка завершена.
```

Рисунок – Результат выполнения команды трассировки

13.2.3 Настройки области

При необходимости настройки области OSPF следует выполнить следующие действия:

1. Перейти во вкладку **«Настройки области»** подраздела настройки OSPF (**«Маршрутизация» - «OSPF»**) и нажать **кнопку** « » (см. Рисунок – Настройки области OSPF).

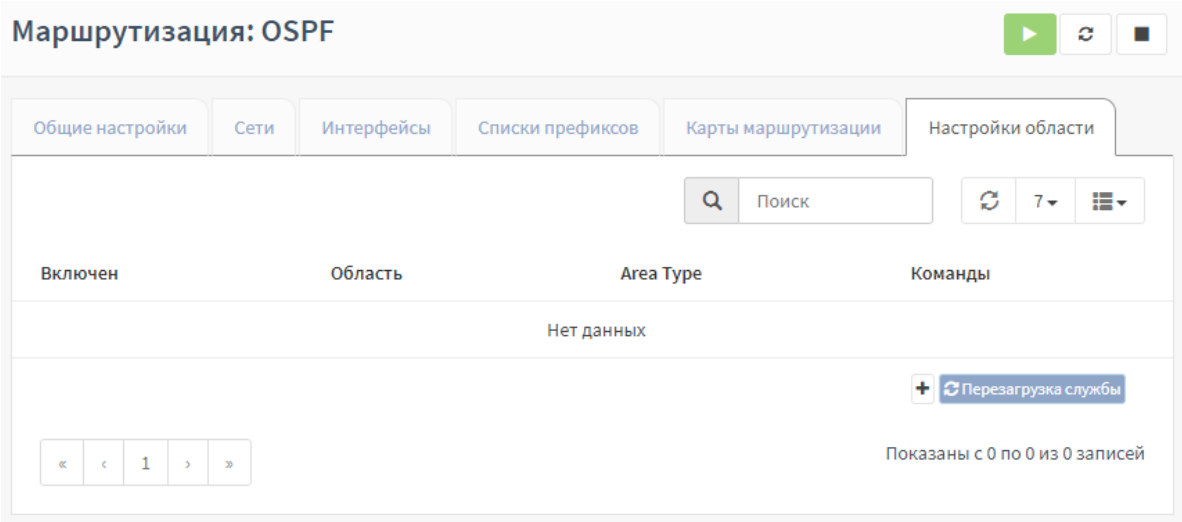


Рисунок – Настройки области OSPF

2. В открывшейся форме указать параметры **«Область»** и **«Тип области»**.

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

   - **«Default (по-умолчанию)»**;
   - **«Stub (тупиковая)»** – принимает маршруты из других зон, но не принимает информацию о внешних маршрутах для автономной системы;
   - **«NSSA (не совсем тупиковая область)»** – область, в которой может находиться ASBR.

   При выборе значения «Stub (тупиковая)» в поле параметра **«Тип области»** дополнительно появится параметр **«no-summary»**. При установке флажка для параметра **«no-summary»** типа области «Stub (тупиковая)» настраиваемая область будет соответствовать типу **«Totally stub»**.

   При выборе значения «NSSA (не совсем тупиковая область)» в поле параметра **«Тип области»** дополнительно появятся параметры **«NSSA»** и **«no-summary»**. При установке флажка для параметра **«no-summary»** типа области «NSSA (не совсем тупиковая область)» настраиваемая область будет соответствовать типу **«Totally NSSA»**.

   В поле параметра **«NSSA»** возможно выбрать следующие значения:

   - **«translate-candidate (по-умолчанию)»**;
   - **«translate-never»** – не будет выполняться трансляция LSA 7-го типа, конвертированных в LSA 5-го типа;
   - **«translate-always»** – независимо от состояния маршрутизатора будет выполняться трансляция LSA 7-го типа, конвертированных в LSA 5-го типа.

3. Нажать **кнопку «Сохранить»**.

13.2.4 Особенности настройки маршрутизации OSPF с туннелем OpenVPN

В качестве примера приведены особенности настройки маршрутизации OSPF на двух **ARMA FW**, предварительно подключённых с помощью технологии OpenVPN в режиме **«Пиринговая сеть (Общий ключ)»** или **«Пиринговая сеть (SSL/TLS)»**. Подробное описание настройки OpenVPN рассмотрено в разделе OpenVPN настоящего руководства.

Для корректной работы маршрутизации OSPF необходимо выполнить следующие действия:

1. Добавить обнаруженный интерфейс:
   - «ovpns1» на **ARMA FW**, настроенном в качестве сервера OpenVPN;
   - «ovpnc1» на **ARMA FW**, настроенном в качестве клиента OpenVPN.

   Подробная настройка интерфейсов рассмотрена в разделе Сетевые интерфейсы настоящего руководства.
2. Переименовать добавленный интерфейс с «OPT1» на «ovpns».
3. Создать разрешающие правила МЭ для интерфейса «[ovpns]».
4. Включить сервис маршрутизации (см. Рисунок – Включение сервиса маршрутизации).
5. Перейти во вкладку **«Общие настройки»** подраздела настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), установить флажок для параметра **«Включить»**, указать следующие параметры:
   - **«Пассивные интерфейсы»** – «LAN», «WAN»;
   - **«Перераспределение маршрута»** – «Подключенные маршруты (напрямую подключенная подсеть или хост)».
6. Перейти во вкладку **«Сети»** подраздела настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), нажать **кнопку** « + », указать следующие параметры:
   - **«Включен»** – флажок установлен;
   - **«Адрес сети»** – «10.0.8.0»;
   - **«Маска сети»** – «24»;
   - **«Область»** – «0.0.0.0»;

   и нажать **кнопку «Сохранить»**.

7. Перейти во вкладку **«Интерфейсы»** подраздела настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), нажать **кнопку** « + », указать следующие параметры:
   - **«Включен»** – флажок установлен;
   - **«Интерфейс»** – «ovpns»;
   - **«Область»** – «0.0.0.0»;

   и нажать **кнопку «Сохранить»**.
8. Перезапустить сервисы «frr» и «openvpn» в виджете **«Службы»** раздела **«Инструменты»**.

Указанные действия повторить на **ARMA FW**, настроенном в качестве клиента OpenVPN, указывая в полях параметров значение «ovpnc».

13.3 BGP

Данный протокол относится к классу протоколов маршрутизации внешнего шлюза и предназначен для обмена информацией о достижимости подсетей между АС. Вместе с информацией о сетях передаются различные атрибуты этих сетей, с помощью которых выбирается лучший маршрут и настраиваются политики маршрутизации.

13.3.1 Настройка динамической маршрутизации BGP

Основными настройками для BGP являются:

- **«Номер BGP AS»** – внутренний номер АС;
- **«Сеть»** – список сетей, объявляемых через BGP как принадлежащие локальной АС;
- **«Журналировать изменения соседей»** – журналирование изменения соседей;
- **«Перераспределение маршрута»** – дополнительные источники маршрутизации, передаваемые другим узлам.

При включении переключателя **«расширенный режим»** дополнительно станут доступны следующие параметры:

- **«ID роутера»** – идентификатор маршрутизатора, используемого для связи с другими узлами;
- **«Плавный перезапуск»** – продолжение перенаправления пакетов во время восстановления информации маршрутизации;

- **«Проверка сетевого импорта»** – объявление о сетях, присутствующих в таблицах маршрутизации маршрутизаторов. По умолчанию флажок установлен.

Более детальные настройки BGP задаются во вкладках:

- **«Соседи»** – указываются соседние связи;
- **«Списки AS путей»** – указываются пути АС;
- **«Списки префиксов»** – указываются списки префиксов;
- **«Списки community»** – указываются атрибуты для фильтрации маршрутов;
- **«Карты маршрутизации»** – указываются карты маршрутизации.

На каждом **ARMA FW** предварительно необходимо создать разрешающее правило МЭ (см. Создание правил межсетевого экранирования) на интерфейсе «[LAN]».

Для настройки динамической маршрутизации по протоколу BGP на каждом **ARMA FW** необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек маршрутизации (**«Маршрутизация» - «Общие настройки»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Включение сервиса маршрутизации) для включения сервиса маршрутизации.
2. Перейти в подраздел настроек маршрутизации BGP (**«Маршрутизация» - «BGP»**), установить флажок для параметра **«Включить»** (см. Рисунок – Включение BGP), указать следующие параметры:
   - на **ARMA FW1**:
     - **«Номер BGP AS»** – «1»;
     - **«Сеть»** – адрес локальной сети **ARMA FW1** в формате CIDR;
   - на **ARMA FW2**:
     - **«Номер BGP AS»** – «2»;
     - **«Сеть»** – адрес локальной сети **ARMA FW2** в формате CIDR;

   и нажать **кнопку «Сохранить»**.

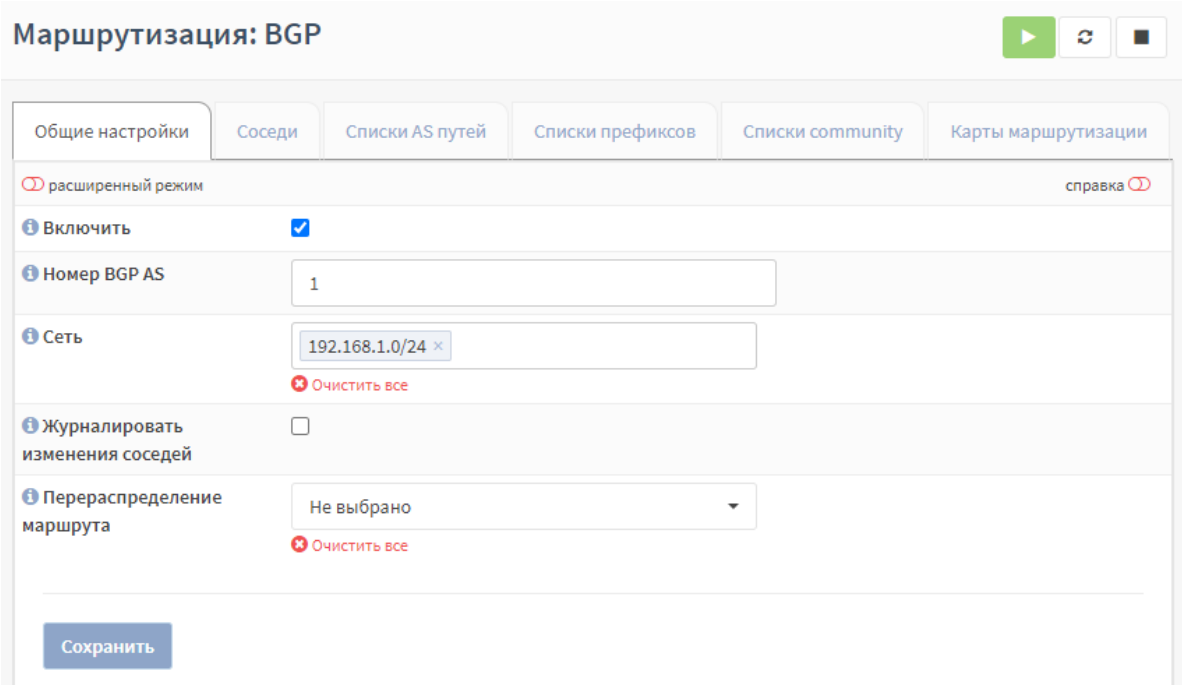


Рисунок – Включение BGP

3. Перейти во вкладку **«Соседи»**, нажать **кнопку** « + », указать следующие параметры:
   - на **ARMA FW1**:
     - **«Включен»** – флажок установлен;
     - **«IP пира»** – IP-адрес интерфейса «WAN» **ARMA FW2**;
     - **«Удалённый AS»** – «2»;
   - на **ARMA FW2**:
     - **«Включен»** – флажок установлен;
     - **«IP пира»** – IP-адрес интерфейса «WAN» **ARMA FW1**;
     - **«Удалённый AS»** – «1»;

   и нажать **кнопку «Сохранить»**.
4. Перезапустить сервис «frr» в виджете **«Службы»** раздела **«Инструменты»**.

13.3.2 Проверка работы динамической маршрутизации BGP

Для проверки динамической маршрутизации необходимо с ПК **«Client»** выполнить команду «ping» ПК **«Server»**. При правильной настройке команда выполнится успешно.

13.4 BFD

Данный протокол используется для обнаружения сбоев между маршрутизаторами, соединёнными каналом.

13.4.1 Настройка BFD при статической маршрутизации

В качестве примера приведена настройка BFD при статической маршрутизации на двух **ARMA FW** согласно схеме стенда, представленной на рисунке (см. Рисунок – Схема стенда для настройки BFD при статической маршрутизации).

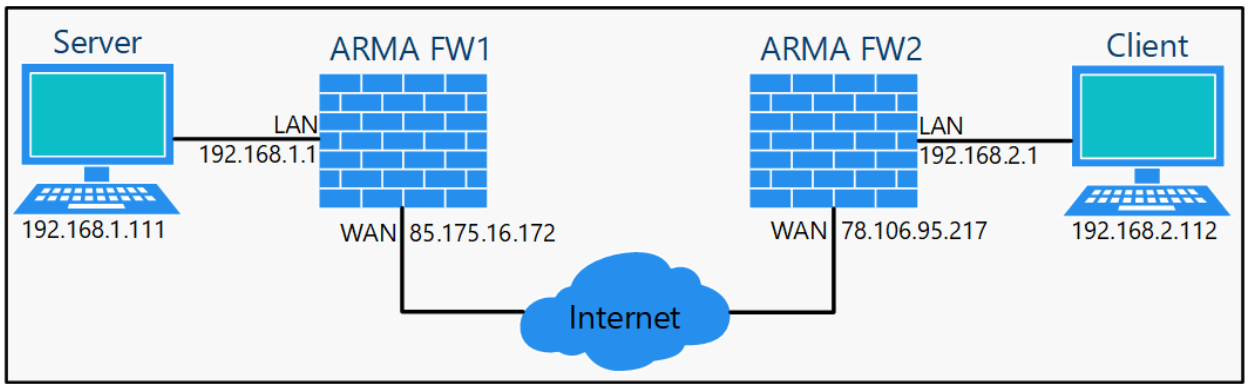


Рисунок – Схема стенда для настройки BFD при статической маршрутизации

Использованные IP-адреса на схеме стенда приведены в качестве примера и могут отличаться для каждой конкретной ситуации.

Для настройки BFD при статической маршрутизации необходимо выполнить следующие действия:

1. На каждом **ARMA FW** перейти в подраздел общих настроек маршрутизации (**«Маршрутизация» - «Общие настройки»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Включение сервиса маршрутизации) для включения сервиса маршрутизации.
2. На каждом **ARMA FW** перейти в подраздел настроек BFD (**«Маршрутизация» - «BFD»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**.
3. На **ARMA FW1** перейти во вкладку **«Статические маршруты»** подраздела настроек BFD, установить флажок для параметра **«Включить BFD для статической маршрутизации»**, нажать **кнопку «Сохранить»**, нажать **кнопку** « + », указать следующие параметры:
   - **«Включен»** – флажок установлен;
   - **«Описание»** – «stat route BFD»;
   - **«Адрес сети»** – адрес локальной сети **ARMA FW2** в формате CIDR, в примере «192.168.2.0/24»;
   - **«Шлюз»** – IP-адрес интерфейса «WAN» **ARMA FW2**, в примере «78.106.95.217»;

   и нажать **кнопку «Сохранить»**.

Перейти во вкладку **«Соседи»** подраздела диагностики BFD **ARMA FW1** (**«Маршрутизация» - «Диагностика» - «BFD»**) и убедиться в наличии информации о соседнем маршрутизаторе с отображением статуса «down».

4. На **ARMA FW2** перейти во вкладку **«Соседи»** подраздела настроек BFD (**«Маршрутизация» - «BFD»**), нажать **кнопку** « + », указать следующие параметры:
   - **«Включен»** – флажок установлен;
   - **«IP пира»** – IP-адрес интерфейса «WAN» **ARMA FW1**, в примере «85.175.16.172»;

   и нажать **кнопку «Сохранить»**.

13.4.1.1 Проверка настройки BFD при статической маршрутизации

Для проверки настройки BFD при статической маршрутизации необходимо выполнить следующие действия:

1. Перейти во вкладку **«Соседи»** подраздела диагностики BFD **ARMA FW1** (**«Маршрутизация» - «Диагностика» - «BFD»**) и убедиться в наличии информации о соседнем маршрутизаторе с отображением статуса «up».
2. С ПК **«Client»** выполнить команду «ping» ПК **«Server»**. При правильной настройке команда выполнится успешно.

13.4.2 Настройка BFD при маршрутизации OSPF

В качестве примера приведена настройка BFD и маршрутизации по протоколу OSPF на двух **ARMA FW**.

Для настройки BFD при маршрутизации OSPF необходимо на каждом **ARMA FW** выполнить следующие действия:

1. Перейти в подраздел общих настроек маршрутизации (**«Маршрутизация» - «Общие настройки»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Включение сервиса маршрутизации) для включения сервиса маршрутизации.
2. Перейти в подраздел настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**.
3. Перейти во вкладку **«Интерфейсы»** подраздела настроек маршрутизации OSPF (**«Маршрутизация» - «OSPF»**), нажать **кнопку** « + », указать следующие параметры:
   - **«Включен»** – флажок установлен;

- **«Интерфейс»** – «LAN»;
- **«Область»** – «0.0.0.0»;

и нажать **кнопку «Сохранить»**.

4. Нажать **кнопку** « + », указать следующие параметры:
   - **«Включен»** – флажок установлен;
   - **«Интерфейс»** – «WAN»;
   - **«Область»** – «0.0.0.0»;
   - **«BFD»** – флажок установлен;

   и нажать **кнопку «Сохранить»**.
5. Нажать **кнопку «Перезагрузка службы»**.
6. Перейти в подраздел настроек BFD (**«Маршрутизация» - «BFD»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**.

13.4.2.1 Проверка настройки BFD при маршрутизации OSPF

Для проверки настройки BFD при маршрутизации OSPF необходимо выполнить следующие действия:

1. Перейти во вкладку **«Маршруты IPv4»** подраздела диагностики маршрутизации (**«Маршрутизация» - «Диагностика» - «Общие настройки»**) и убедиться в наличии корректной информации о маршруте.
2. Перейти во вкладку **«Сводка»** подраздела диагностики BFD (**«Маршрутизация» - «Диагностика» - «BFD»**) и убедиться в отображении статуса «up».
3. Перейти во вкладку **«Счетчики»** подраздела диагностики BFD и убедиться в наличии корректной информации о соседнем маршрутизаторе.

13.4.3 Настройка BFD при маршрутизации BGP

В качестве примера приведены особенности настройки BFD при использовании маршрутизации по протоколу BGP на двух **ARMA FW**. Подробное описание процесса настройки маршрутизации по протоколу BGP приведено в разделе Настройка динамической маршрутизации BGP настоящего руководства.

Для настройки BFD при маршрутизации по протоколу BGP необходимо на каждом **ARMA FW** дополнительно установить флажок для параметра **«BFD»** во вкладке **«Соседи»** подраздела настроек маршрутизации BGP (**«Маршрутизация» - «BGP»**).

13.4.3.1 Проверка настройки BFD при маршрутизации BGP

Для проверки настройки BFD при маршрутизации BGP необходимо выполнить следующие действия:

1. Перейти во вкладку **«Маршруты IPv4»** подраздела диагностики маршрутизации (**«Маршрутизация» - «Диагностика» - «Общие настройки»**) и убедиться в наличии корректной информации о маршруте.
2. Перейти во вкладку **«Сводка»** подраздела диагностики BFD (**«Маршрутизация» - «Диагностика» - «BFD»**) и убедиться в отображении статуса «up».
3. Перейти во вкладку **«Соседи»** подраздела диагностики BFD и убедиться в наличии корректной информации о соседнем маршрутизаторе.

14 DHCP-СЕРВЕР

DHCP-сервер используется для автоматического предоставления клиентам IP-адреса и других параметров, необходимых для работы в сети TCP/IP. DHCP-сервер доступен как для клиентов IPv4, так и для IPv6, представленных в подразделах **«DHCPv4»** и **«DHCPv6»** раздела **«Службы»** соответственно.

14.1 DHCPv4

Подраздел содержит настройки DHCP-сервера для клиентов IPv4.

В качестве примера использования DHCP-сервера будет рассмотрено назначение IP-адресов хостам во внутренней сети интерфейса «LAN» из следующего диапазона:

- «192.168.1.100 – 192.168.1.199».

Результатом работы настроенного DHCP-сервера является назначение IP-адресов хостам, находящимся в сети интерфейса «LAN». Выданные IP-адреса представлены в подразделе аренды адресов (**«Службы» - «DHCPv4» - «Аренда адресов»**).

14.1.1 Настройка по имени интерфейса

Перечень параметров и процесс их настройки является идентичным для всех интерфейсов («LAN», «WAN», «OPT1» и т.д.).

Для того чтобы настроить DHCP-сервер, необходимо перейти в подраздел параметров DHCP-сервера настраиваемого интерфейса (**«Службы» - «DHCPv4» - «[LAN]»**), установить флажок **«Включить DHCP-сервер на LAN интерфейсе»**, задать параметры для работы в сети TCP/IP и нажать **кнопку «Сохранить»** внизу страницы.

Основные параметры (подсеть, маска подсети и доступный диапазон) будут заданы автоматически, на основании настроек интерфейса (см. Рисунок – Основные параметры DHCP).

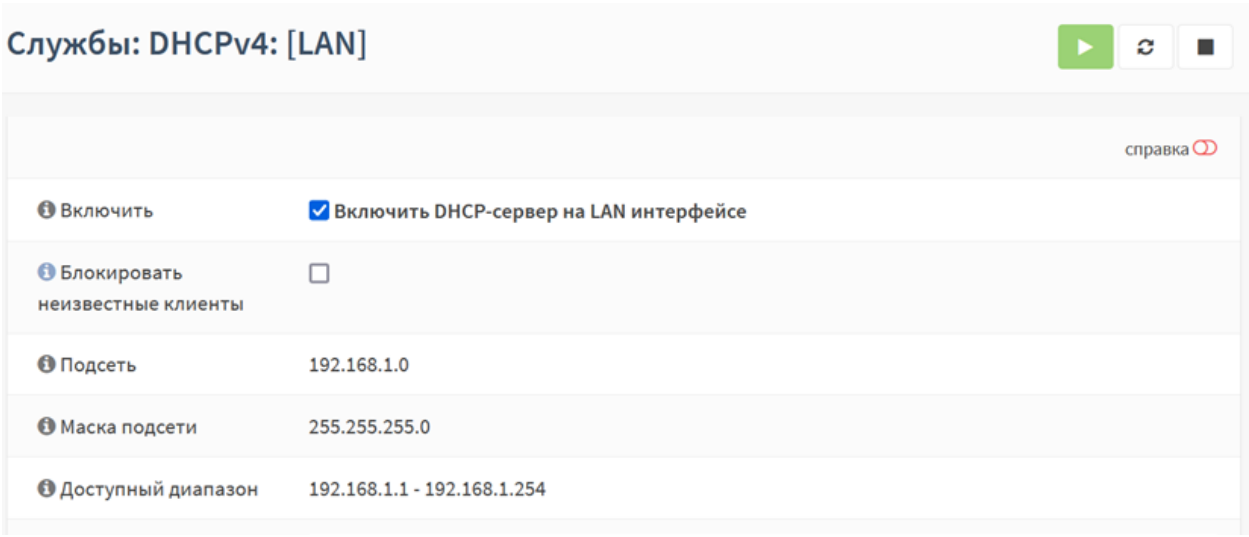


Рисунок – Основные параметры DHCP

14.1.1.1 Диапазон IP-адресов

Основной диапазон возможно скорректировать, указав значения в полях параметра **«Диапазон»** (см. Рисунок – Значение диапазона адресов).

Примечание:

В случае, если поля параметра **«Диапазон»** будут пустыми, выдача адресов не произойдёт.

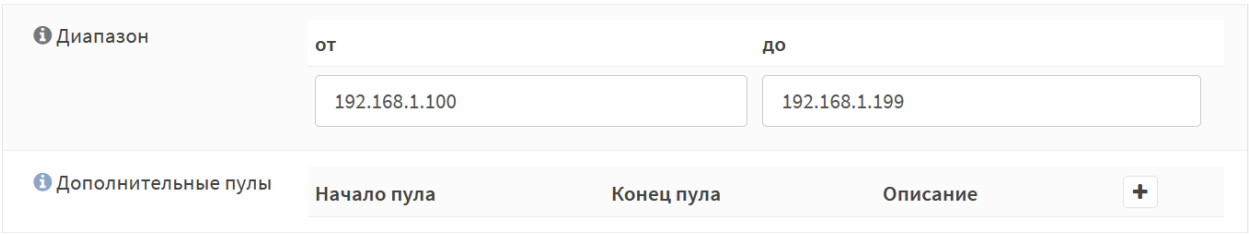


Рисунок – Значение диапазона адресов

Также существует возможность указать дополнительные диапазоны с заданными параметрами. Для этого необходимо нажать **кнопку** « + » в параметре **«Дополнительные пулы»** (см. Рисунок – Значение диапазона адресов) и, указав требуемые настройки в открывшемся интерфейсе, нажать **кнопку «Сохранить»**.

14.1.1.2 Параметры для работы в сети TCP/IP

В случае, когда требуется изменить дополнительные параметры работы в сети TCP/IP, необходимо выполнить одно или несколько из доступных действий:

1. Указать новые значения в соответствующих полях:
   - **«WINS-серверы»**;
   - **«DNS-серверы»**;
   - **«Шлюз»**;

- **«Имя домена»**;
- **«Список поиска доменов»**;
- **«Время аренды по умолчанию (секунд)»**;
- **«Максимальное время аренды (секунды)»**;
- **«MTU интерфейса»**;
- **«IP-адрес участника для аварийного переключения»**;
- **«Разделение аварийного переключения»**.

2. Установить флажок в чек-боксах:
   - **«Статический ARP – Включить статические записи ARP»**;
   - **«Изменить формат даты – Изменить отображение времени аренды DHCP с UTC на местное время»**.
3. Раскрыть дополнительные значения параметра для последующей настройки, нажав **кнопку «Дополнительно»** напротив параметра:
   - **«Динамический DNS»**;
   - **«Контроль доступа по MAC-адресам»**;
   - **«NTP-серверы»**;
   - **«TFTP-сервер»**;
   - **«LDAP URI»**;
   - **«Включить загрузку по сети»**;
   - **«Включить OMAPI»**;
   - **«Дополнительные параметры»**.

14.1.1.3 Статическая маршрутизация

Для закрепления связки **«IP-адрес – хост»** на основании MAC-адреса используется статическая маршрутизация.

Для сопоставления выделяемого IP-адреса заданному хосту необходимо нажать **кнопку** « + » в блоке **«Статическая маршрутизация через DHCP для этого интерфейса»** (см. Рисунок – Статическая маршрутизация через DHCP для этого интерфейса).

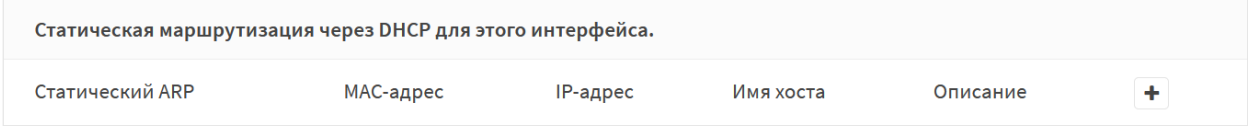


Рисунок – Статическая маршрутизация через DHCP для этого интерфейса

В открывшемся интерфейсе (см. Рисунок – Сопоставление MAC-адреса и IP-адреса) указать MAC-адрес хоста, за которым будет закреплён IP-адрес, непосредственно сам IP-адрес и нажать **кнопку «Сохранить»** внизу страницы. Дополнительные параметры вводятся при необходимости.

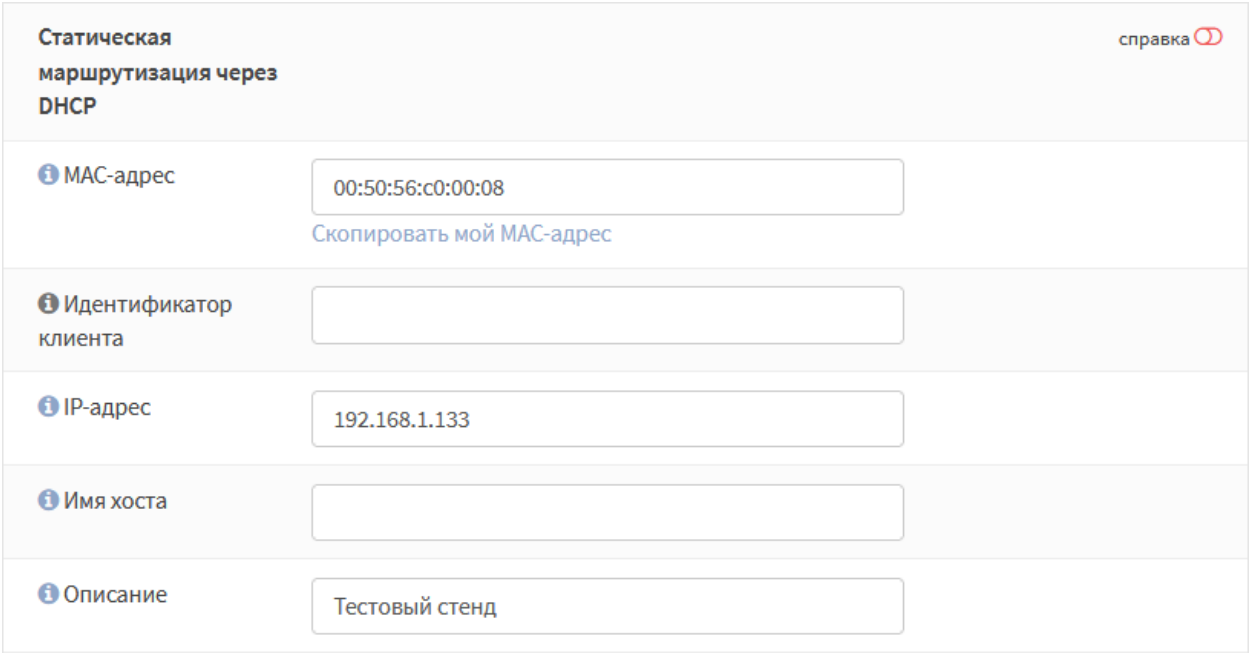


Рисунок – Сопоставление MAC-адреса и IP-адреса

14.1.2 Ретрансляция

DHCP-ретрансляция – это пересылка полученных DHCP-запросов на другой сервер. Настройки ретрансляции доступны только при выключенном DHCP-сервере.

Для настройки DHCP-ретрансляции необходимо задать интерфейсы ретрансляции и адреса внешних DHCP-серверов в подразделе конфигурации DHCP-ретрансляции (**«Службы» - «DHCPv4» - «Ретрансляция»**), установить флажок **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Настройка ретрансляции DHCP).

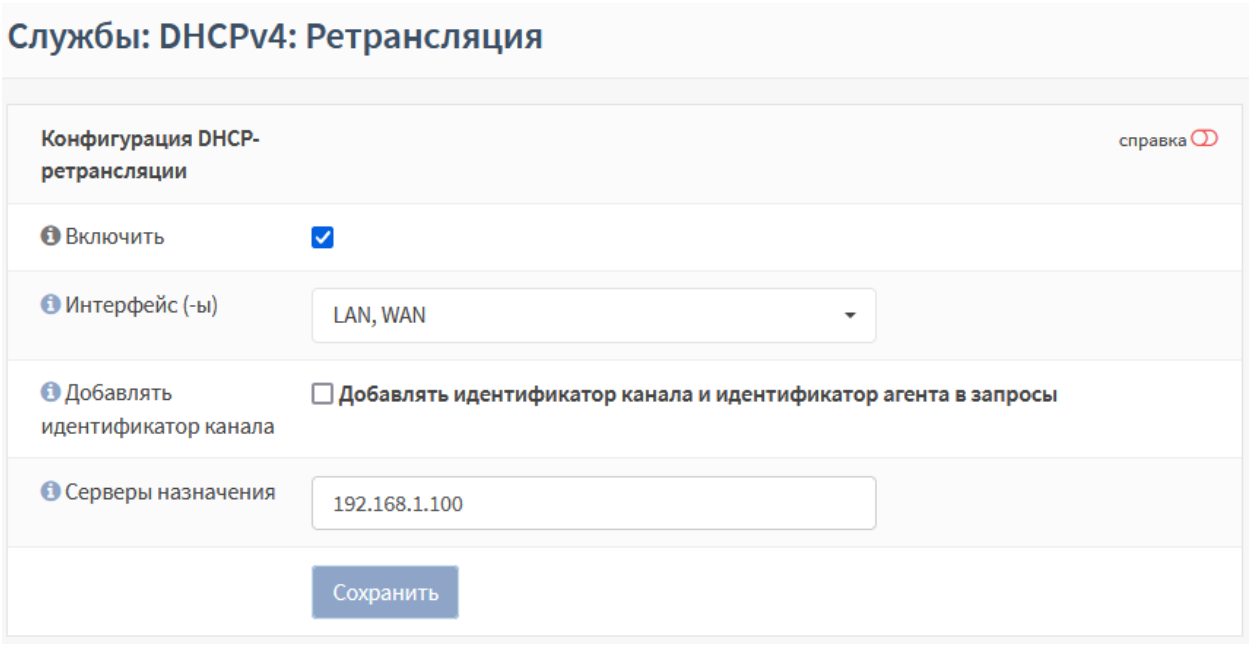


Рисунок – Настройка ретрансляции DHCP

14.1.3 Аренда адресов

В подразделе назначенных адресов (**«Службы» - «DHCPv4» - «Аренда адресов»**) отображается перечень арендованных адресов (см. Рисунок – Активные арендованные адреса). Наличие записей свидетельствует о правильно настроенном DHCP-сервере.

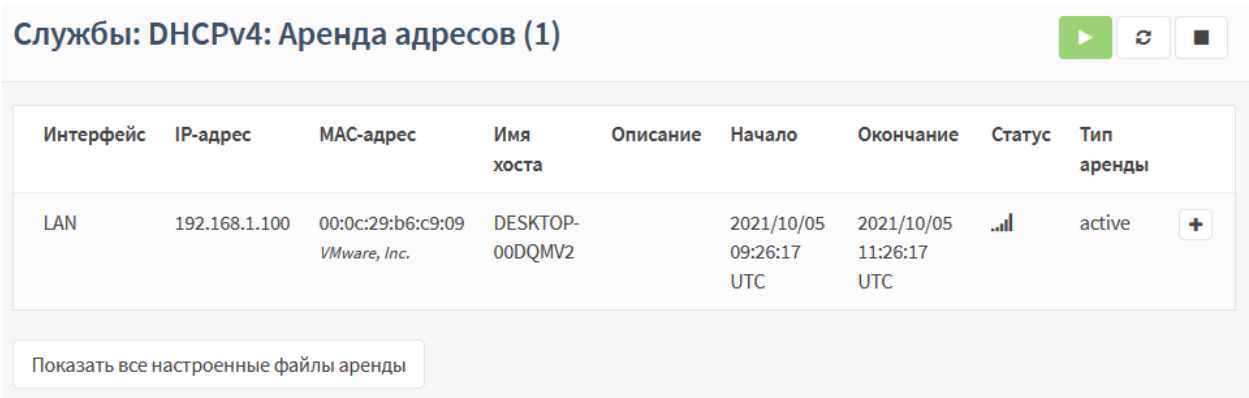


Рисунок – Активные арендованные адреса

При нажатии **кнопки** « + » напротив выбранного адреса – откроется форма статической маршрутизации для закрепления связки **«IP-адрес – хост»** (см. Рисунок – Сопоставление MAC-адреса и IP-адреса).

При нажатии **кнопки «Показать все настроенные файлы аренды»** будут отображены хосты с истекшим сроком аренды (см. Рисунок – Все настроенные файлы аренды).

Интерфейс	IP-адрес	MAC-адрес	Имя хоста	Описание	Начало	Окончание	Статус	Тип аренды	
LAN	192.168.1.100	00:0c:29:b6:c9:09 *VMware, Inc.*	DESKTOP-00DQMV2		2021/10/05 09:26:17 UTC	2021/10/05 11:26:17 UTC		active	+
LAN	192.168.1.101	00:0c:29:d4:28:2f *VMware, Inc.*			2021/09/29 14:41:00 UTC	2021/09/29 14:47:36 UTC	⊘	expired	+ 🗑

Рисунок – Все настроенные файлы аренды

14.2 DHCPv6

Подраздел содержит настройки DHCP-сервера для клиентов IPv6. По умолчанию для DHCPv6-сервера доступны только подразделы **«Ретрансляция»** и **«Аренда адресов»**.

Для того чтобы был доступен подраздел с настройками для каждого интерфейса («LAN», «WAN», «OPT1» и т.д.), необходимо произвести настройку протокола IPv6 для соответствующего интерфейса в разделе **«Интерфейсы»**.

Распространённым сценарием использования DHCPv6-сервера является назначение IPv6-адресов хостам во внутренней подсети интерфейса «LAN».

Далее будут приведены шаги настройки DHCPv6-сервера со следующими параметрами:

- Интерфейс – «LAN»;
- Подсеть – «0010:0000:0000:0000:0000:0000:0000:0000», сокращённо – «10::»;
- Длина префикса – «64».

14.2.1 Настройка по имени интерфейса

Процесс настройки DHCP-сервера для IPv6 аналогичен настройке для IPv4.

Необходимо перейти в подраздел параметров DHCP-сервера настраиваемого интерфейса (**«Службы» - «DHCPv6» - «[LAN]»**), установить флажок **«Включить DHCPv6-сервер на LAN интерфейсе»**, задать параметры для работы в сети TCP/IP и нажать **кнопку «Сохранить»** внизу страницы.

Основные параметры (подсеть, маска подсети и доступный диапазон) будут заданы автоматически, основываясь на настройках интерфейса (см. Рисунок – Основные настройки DHCPv6).

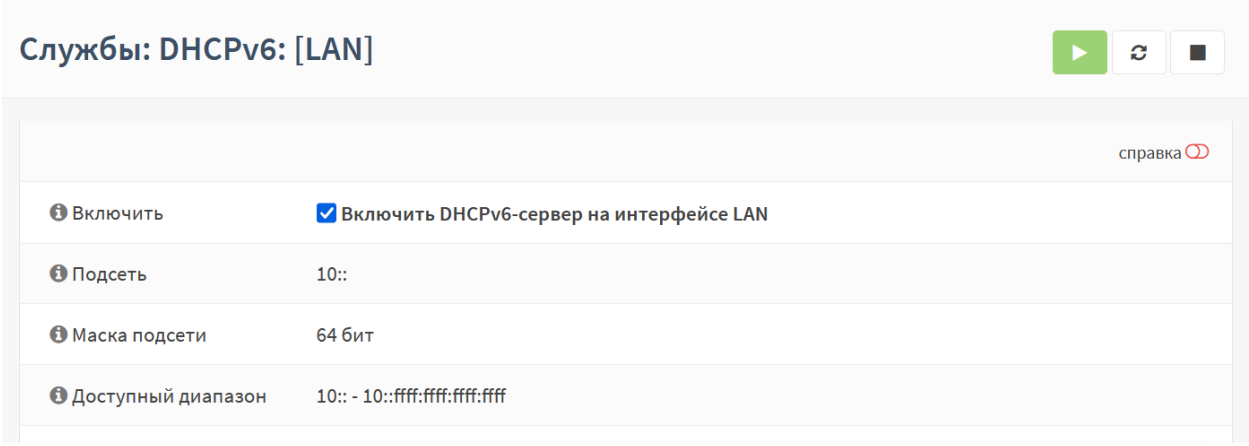


Рисунок – Основные настройки DHCPv6

14.2.1.1 Диапазон IP-адресов

Настройки диапазона задаются в параметрах **«Диапазон»** и **«Диапазон делегируемых префиксов»** (см. Рисунок – Дополнительные настройки диапазона адресов).

Примечание:

В случае, если поля параметра **«Диапазон»** будут пустыми, выдача адресов не произойдёт.

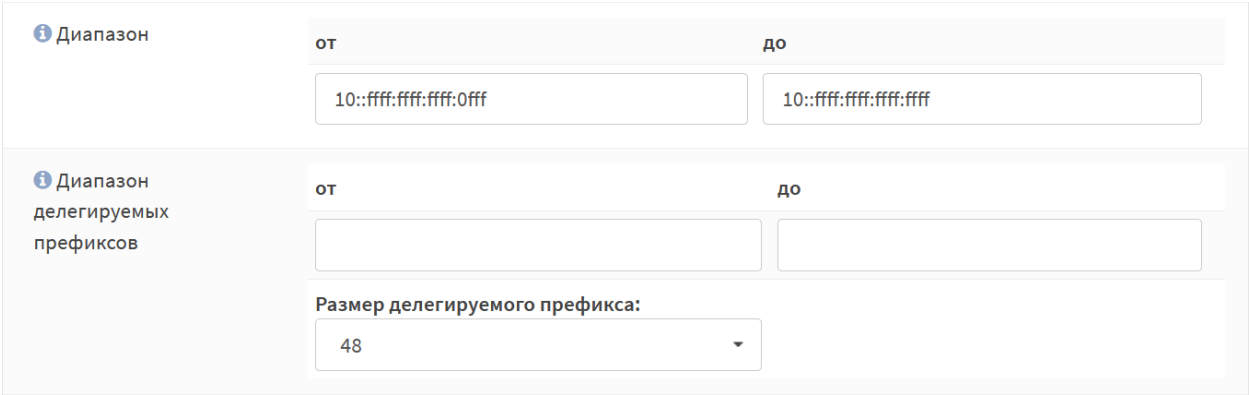


Рисунок – Дополнительные настройки диапазона адресов

14.2.1.2 Параметры для работы в сети TCP/IP

В случае, когда требуется изменить дополнительные параметры работы в сети TCP/IP, необходимо выполнить одно или несколько доступных действий:

1. Указать новые значения в соответствующих полях:
   - **«DNS-серверы»**;
   - **«Список поиска доменов»**;
   - **«Время аренды по умолчанию (секунды)»**;
   - **«Максимальное время аренды (секунды)»**.

2. Установить флажок в чек-боксе:
   - **«Изменить формат даты – Изменить отображение времени аренды DHCPv6 с UTC на местное время»**.
3. Раскрыть дополнительные значения параметра для последующей настройки, нажав **кнопку «Дополнительно»** напротив параметра:
   - **«Динамический DNS»**;
   - **«NTP-серверы»**;
   - **«Включить загрузку по сети»**;
   - **«Дополнительные параметры BOOTP/DHCP»**.

14.2.1.3 Статическая маршрутизация

Для закрепления связки **«IPv6-адрес – хостами»** на основании идентификатора участников DHCP (DUID) используется статическая маршрутизация.

Для сопоставления выделяемого IP-адреса заданному хосту необходимо нажать **кнопку** « + » в параметре **«Статическая маршрутизация через DHCPv6 для этого интерфейса»** (см. Рисунок – Статическая маршрутизация через DHCPv6 для этого интерфейса).

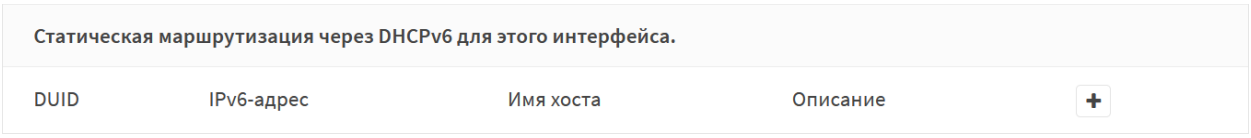


Рисунок – Статическая маршрутизация через DHCPv6 для этого интерфейса

В открывшемся интерфейсе (см. Рисунок – Сопоставление DUID и IPv6-адреса) указать DUID, за которым будет закреплён IPv6-адрес, непосредственно сам IPv6-адрес и нажать **кнопку «Сохранить»** внизу страницы. Дополнительные параметры вводятся при необходимости.

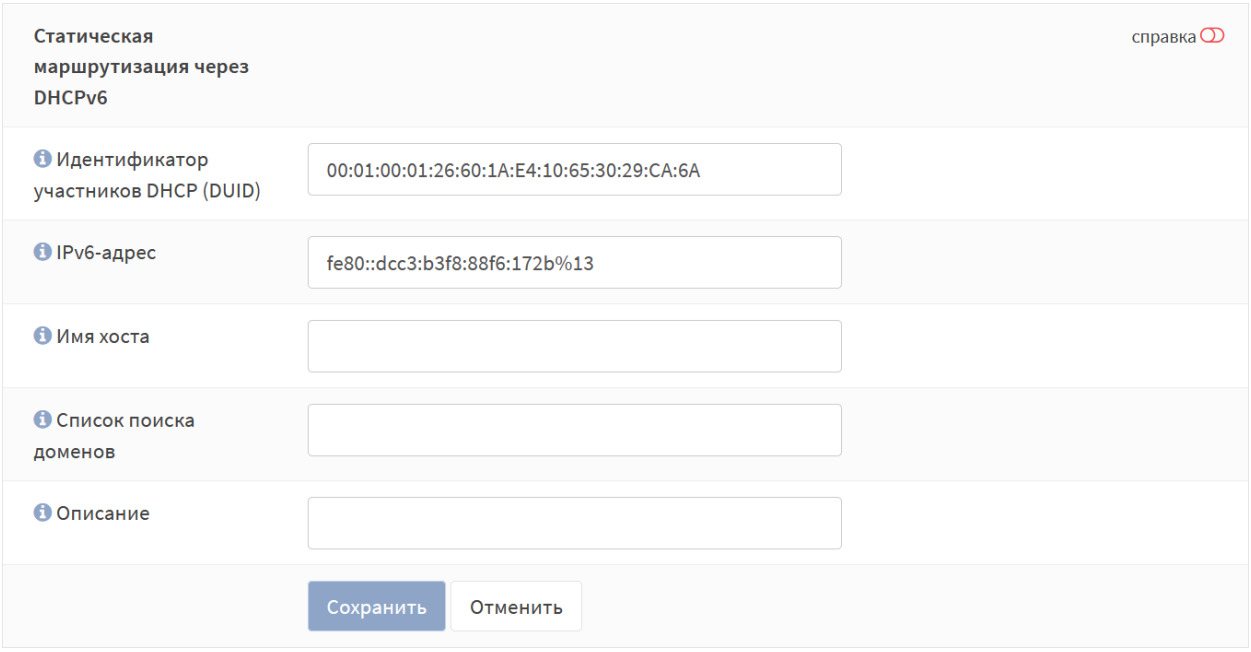


Рисунок – Сопоставление DUID и IPv6-адреса

14.2.2 Ретрансляция

Настройки ретрансляции доступны только при выключенном DHCPv6-сервере.

Для настройки DHCPv6-ретрансляции необходимо задать интерфейсы ретрансляции и адреса внешних DHCPv6-серверов в подразделе конфигурации DHCP-ретрансляции (**«Службы» - «DHCPv6» - «Ретрансляция»**), установить флажок **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Настройка ретрансляции DHCPv6). При необходимости установить флажок в параметре **«Добавлять идентификатор канала»**.

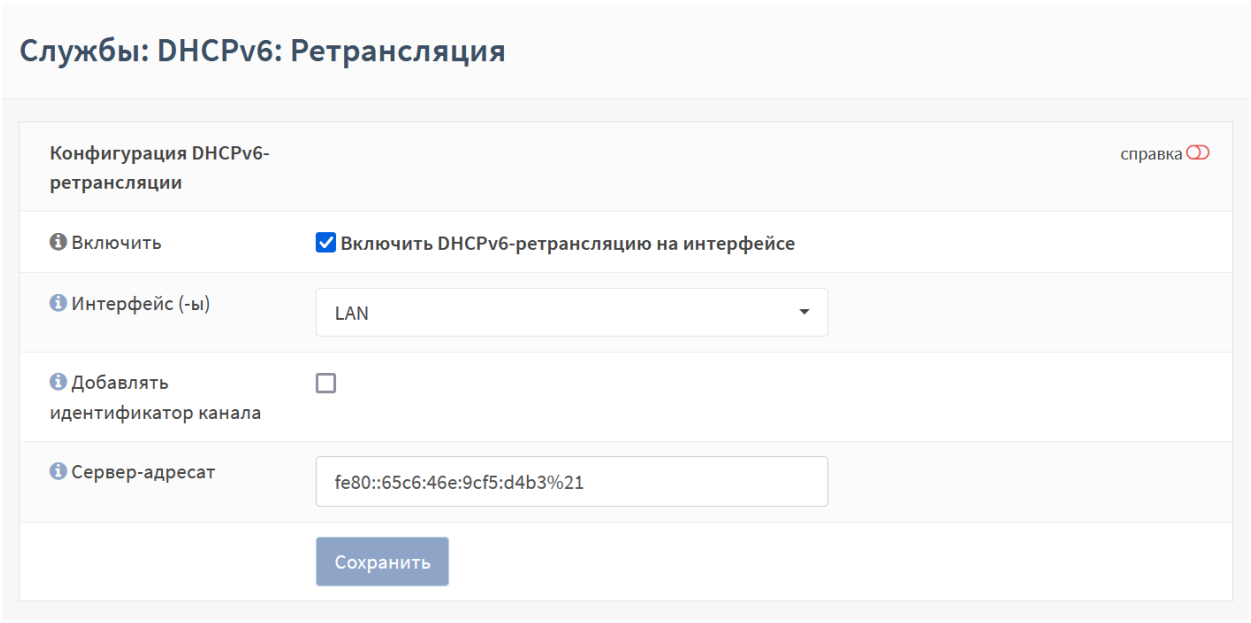


Рисунок – Настройка ретрансляции DHCPv6

14.2.3 Аренда адресов

В подразделе назначенных адресов (**«Службы» - «DHCPv6» - «Аренда адресов»**) отображается перечень арендованных адресов IPv6 (см. Рисунок – Активные арендованные адреса IPv6).

Наличие записей свидетельствует о правильно настроенном DHCPv6-сервере.

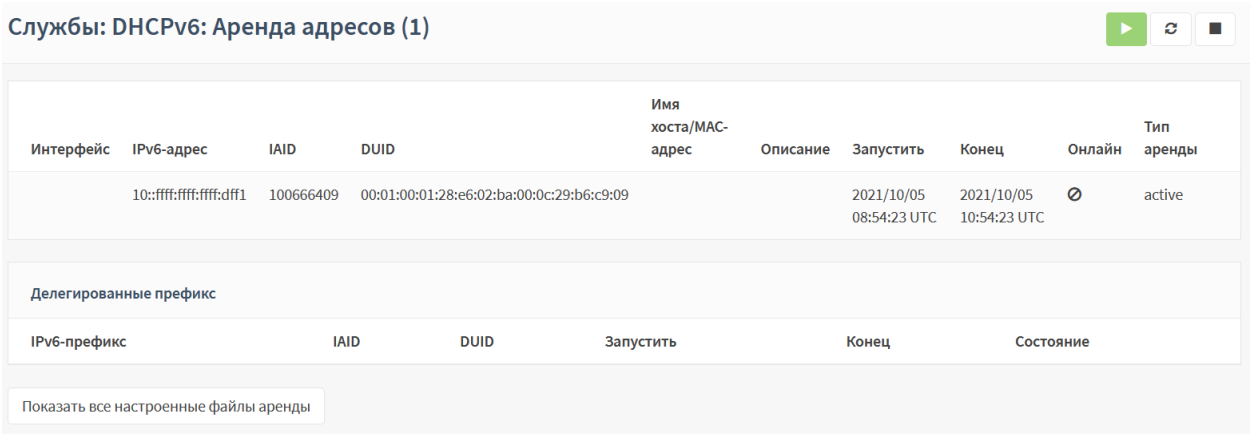


Рисунок – Активные арендованные адреса IPv6

При нажатии **кнопки «Показать все настроенные файлы аренды»** будут отображены хосты с истекшим сроком аренды.

15 КЭШИРУЮЩИЙ DNS-СЕРВЕР

Кэширующий DNS-сервер обслуживает запросы клиентов – получает рекурсивный запрос, выполняет его с помощью нерекурсивных запросов к авторитативным серверам или передаёт рекурсивный запрос вышестоящему DNS-серверу.

В качестве основного DNS-сервера в **ARMA FW** используется служба unbound, по умолчанию включённая после установки **ARMA FW**.

> **Примечание:**
>
> При включённой службе unbound возможна отправка запросов **ARMA FW** ко внешним серверам.

В большинстве случаев для корректной работы DNS-сервера достаточно настроек по умолчанию.

15.1 Общие принципы работы кэширующего DNS-сервера

Настройка DNS-сервера доступна в подразделе общих настроек кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Общие настройки»**).

В случае изменения настроек кэширующего DNS-сервера необходимо нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

При включённом DNS-сервере, DHCP-сервер для настроенных интерфейсов автоматически будет назначать **ARMA FW** в качестве DNS-сервера по умолчанию.

Кэширующий DNS-сервер использует в качестве вышестоящих следующие DNS-серверы:

- указанные в перечне **«DNS-серверы»** блока настроек **«Построение сетей»** подраздела общих настроек **ARMA FW** (**«Система» - «Настройки» - «Общие настройки»**) (см. Рисунок – Блок настроек «Построение сетей»);
- полученные в результате настройки сетевого интерфейса «WAN» посредством DHCP в случае установки флажка для параметра **«Позволить переопределить список DNS-серверов DHCP/PPP на WAN»** блока настроек **«Построение сетей»** подраздела общих настроек **ARMA FW** (**«Система» - «Настройки» - «Общие настройки»**) (см. Рисунок – Блок настроек «Построение сетей»).

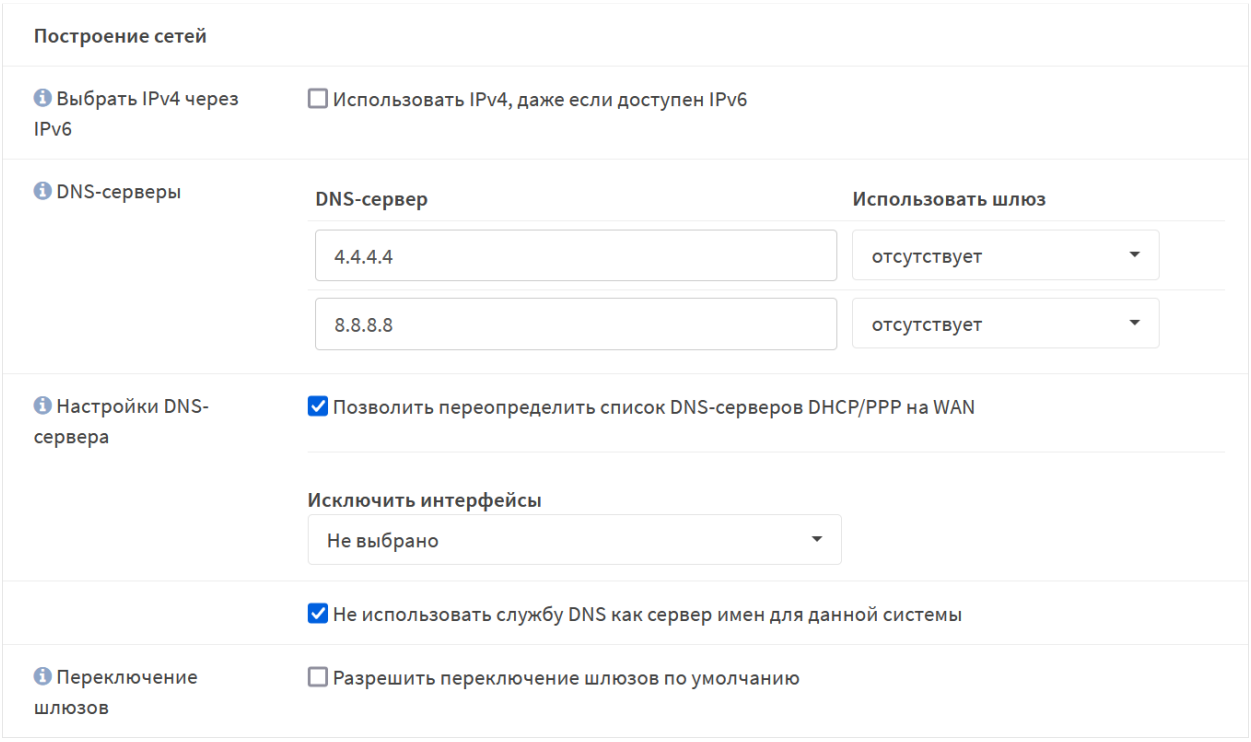


Рисунок – Блок настроек «Построение сетей»

15.2 Дополнительные параметры кэширующего DNS-сервера

Дополнительные параметры кэширующего DNS-сервера доступны в следующих подразделах:

- общих настроек кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Общие настройки»**) при нажатии **кнопки «Показать дополнительные параметры»** в нижней части раздела;
- дополнительных настроек кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Дополнительно»**).

При нажатии **кнопки «Показать дополнительные параметры»** будет доступен параметр **«Пользовательские настройки»** в поле которого указываются дополнительные параметры конфигурации службы unbound. Дополнительные сведения представлены на официальном сайте ПО «Unbound» (см. https://unbound.docs.nlnetlabs.nl).

Для параметров в разделе дополнительных настроек кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Дополнительно»**) доступно краткое описание при включении переключателя **«Справка»**. В случае изменения дополнительных настроек кэширующего DNS-сервера необходимо нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

15.3 Переопределения

В подразделе назначения переопределений (**«Службы» - «Кэширующий DNS-сервер» - «Переопределение»**) доступны следующие блоки настроек:

- **«Переопределение хоста»** – записи переопределяют отдельные результаты от перенаправляющих серверов;
- **«Переопределение домена»** – записи переопределяют домен, указывая полномочный DNS-сервер, запрашиваемый для этого домена.

Для создания переопределения необходимо выполнить следующие действия:

1. Нажать **кнопку** « » в блоке настроек, соответствующему создаваемой записи.
2. Указать параметры создаваемой записи:
   - для переопределения обязательными к заполнению полями являются поля параметров **«Домен»** и **«IP-адрес»**.
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

15.4 Списки доступа

Списки доступа определяют клиентов, имеющих разрешение направлять запросы кэширующему DNS-серверу.

Подраздел списков допуска кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Списки доступа»**) содержит перечень предопределённых списков доступа и имеет возможность добавления пользовательских списков доступа.

Для добавления пользовательского списка доступа необходимо выполнить следующие действия:

1. Нажать **кнопку «+Добавить»**.
2. В открывшейся форме указать значения параметров:
   - **«Имя списка доступа»** – описательное имя списка доступа, необязательный параметр;
   - **«Действие»** – действие из выпадающего списка;
   - **«Сеть»** – сеть, для которой будет выполняться действие.
3. При необходимости заполнить значения параметров **«Описание»** и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

   Перечень доступных действий для списков доступа:

   - **«Разрешить»** – разрешает запросы;

- **«Запретить»** – запрещает запросы;
- **«Отклонить»** – запрещает запросы и отправляет обратно сообщение об ошибке;
- **«Разрешить отслеживание»** – разрешает рекурсивный и нерекурсивный доступ и используется для отслеживания кэша;
- **«Отказ не локальный»** – разрешает только авторитетные запросы локальных данных и отправляет сообщение об ошибке для сообщений, которые запрещены;
- **«Запрет не локальный»** – разрешает только авторитетные запросы локальных данных и удаляет сообщения, которые запрещены.

15.5 Статистические данные

Подраздел статистики кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Статистические данные»**) предоставляет сведения о работающем DNS-сервере, такие как:

- количество выполненных запросов;
- использование кэша;
- время безотказной работы.

16 СЛУЖБА NTP

Служба NTP – это демон сетевого протокола времени, позволяющий устанавливать и поддерживать системное время, синхронизированное с серверами точного времени.

16.1 Настройка синхронизации времени по протоколу NTP

Первоначальная настройка синхронизации времени производится в мастере первоначальной настройки **ARMA FW**. Процесс настройки **ARMA FW** посредством мастера первоначальной настройки описан в разделе **«Мастер первоначальной настройки»** Руководства администратора **ARMA FW**.

Для изменения настроек синхронизации времени по протоколу NTP необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек NTP (**«Службы» - «Сетевое время» - «Общие настройки»**) (см. Рисунок – Настройка конфигурации NTP-сервера).
2. Выбрать интерфейс для использования NTP в параметре **«Интерфейс (-ы)»**. По умолчанию прослушиваются все настроенные интерфейсы.
3. В блоке настроек **«Серверы времени»** из списка серверов выбрать предпочитаемые серверы времени или отключить нежелательные. По умолчанию задано четыре сервера. Для добавления сервера необходимо нажать **кнопку** « + » и указать его параметры, а для удаления нажать **кнопку** « − » напротив записи.
4. Нажать **кнопку «Сохранить»**.

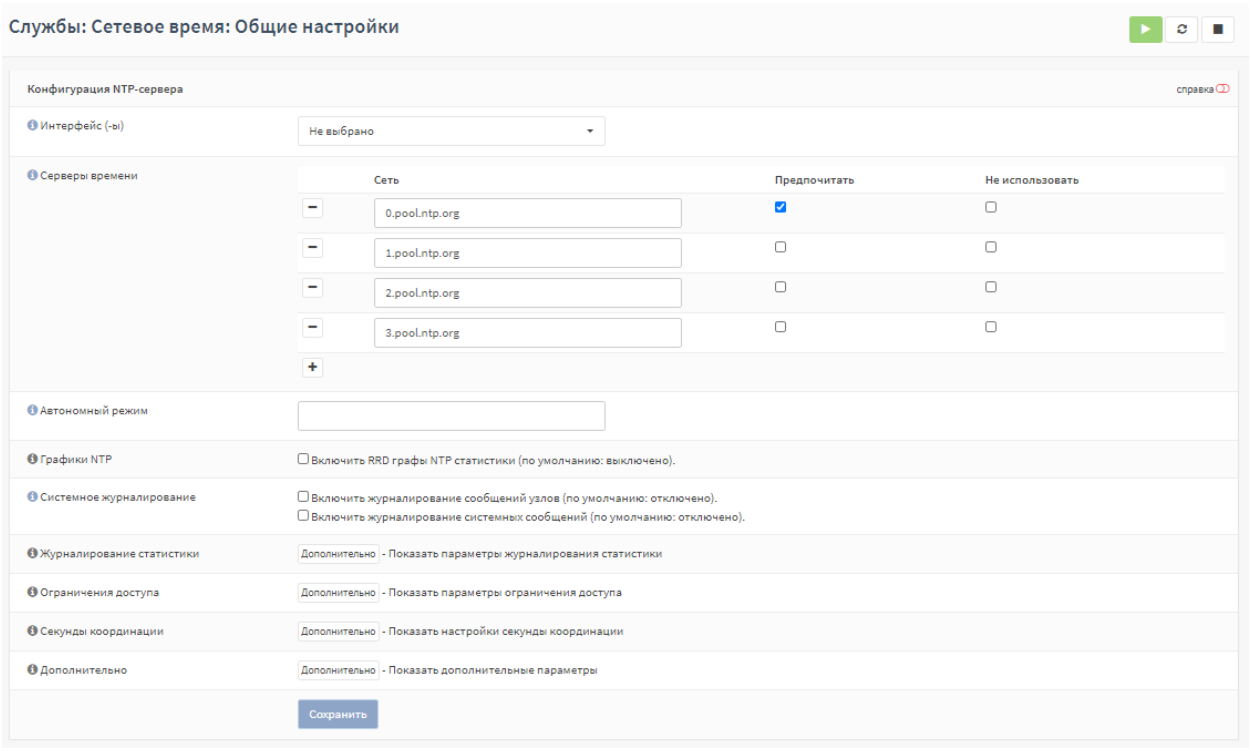


Рисунок – Настройка конфигурации NTP-сервера

При необходимости существует возможность настроить следующие параметры:

- **«Автономный режим»** – позволяет использовать системные часы при недоступности других вариантов;
- **«Графики NTP»** – включает RRD-графы NTP статистики;
- **«Системное журналирование»** – включает дополнительные сообщения NTP в системный журнал;
- **«Журналирование статистики»** – создает сохраняемые ежедневные журналы;
- **«Ограничения доступа»** – настраивает опции контроля доступа к NTP из WAN;
- **«Секунды координации»** – позволяет анонсировать демону NTP последующее добавление или вычитание секунды координации;
- **«Дополнительно»** – позволяет указать дополнительные параметры конфигурации.

Дополнительно существует возможность синхронизировать время по подключаемому GPS-приёмнику. Для этого необходимо задать настройки приёмника в соответствующем подразделе (**«Службы» - «Сетевое время» - «GPS-приемник»**).

17 СЕТЕВЫЕ ИНТЕРФЕЙСЫ

ARMA FW поддерживает множество типов интерфейсов используя как сетевые интерфейсы, так и различные сетевые протоколы. По умолчанию интерфейс «LAN» назначается сетевому интерфейсу «em0», а интерфейс «WAN» сетевому интерфейсу «em1». Для следующих по счёту сетевых интерфейсов по умолчанию применяется обозначение «OPT» – «OPT1» для «em2», «OPT2» для «em3» и так далее. Возможны другие варианты создаваемых интерфейсов, например:

- **«bridge»** – для сетевого моста (см. Сетевой мост);
- **«GRE»** – для интерфейса GRE (см. GRE);
- **«LAGG»** – для LAGG-интерфейса (см. LAGG);
- **«VLAN»** – для интерфейса VLAN (см. VLAN).

Назначение интерфейсов, изменение существующих и создание новых виртуальных интерфейсов осуществляется в разделе **«Интерфейсы»**.

17.1 Назначение портов

Все определённые и обнаруженные на текущий момент интерфейсы перечислены в подразделе назначения портов (**«Интерфейсы» - «Назначения портов»**) или в списке интерфейсов, доступных для назначения (см. Рисунок – Назначение портов).

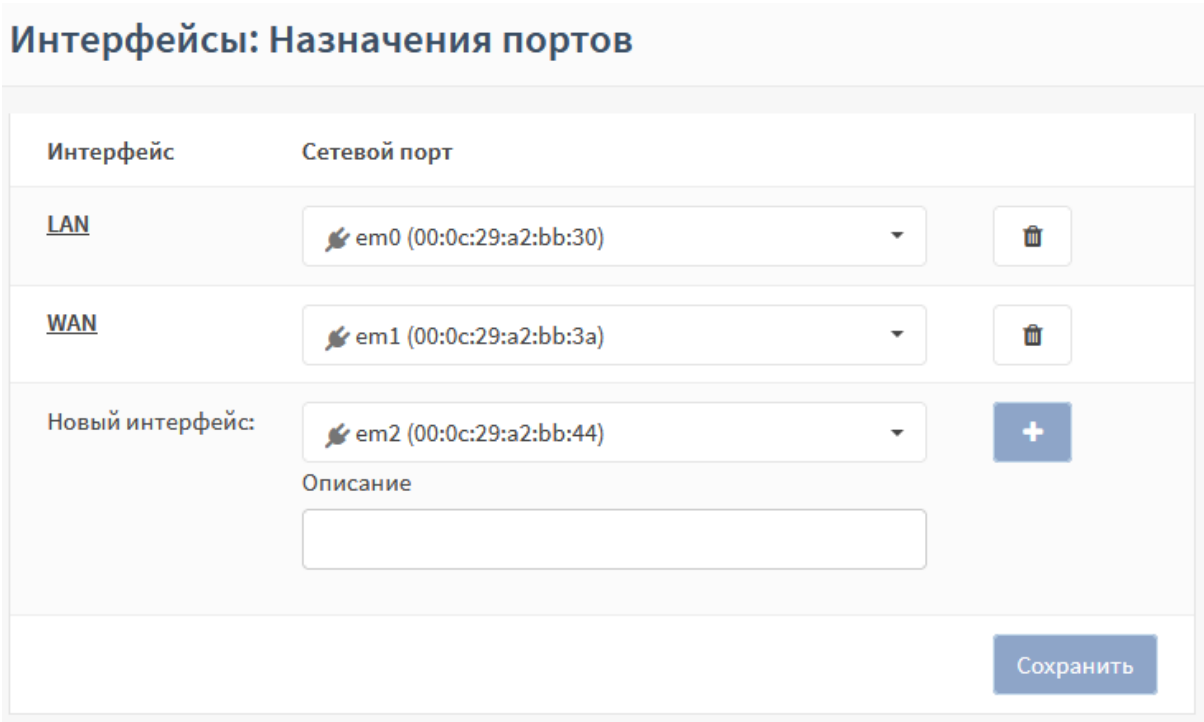


Рисунок – Назначение портов

Для добавления интерфейса необходимо нажать **кнопку** « + » напротив обнаруженного интерфейса, а затем **кнопку «Сохранить»**. Если не указать имя

создаваемого интерфейса в поле параметра **«Описание»**, то будет задано имя по умолчанию.

Для переназначения портов необходимо выбрать интерфейс и в выпадающем списке сетевых портов выбрать другой порт, затем нажать **кнопку «Сохранить»**. Сетевые порты имеют следующие индикаторы (см. Рисунок – Переназначение портов):

- **зелёный** – сетевое подключение установлено;
- **красный** – сетевое подключение отсутствует.

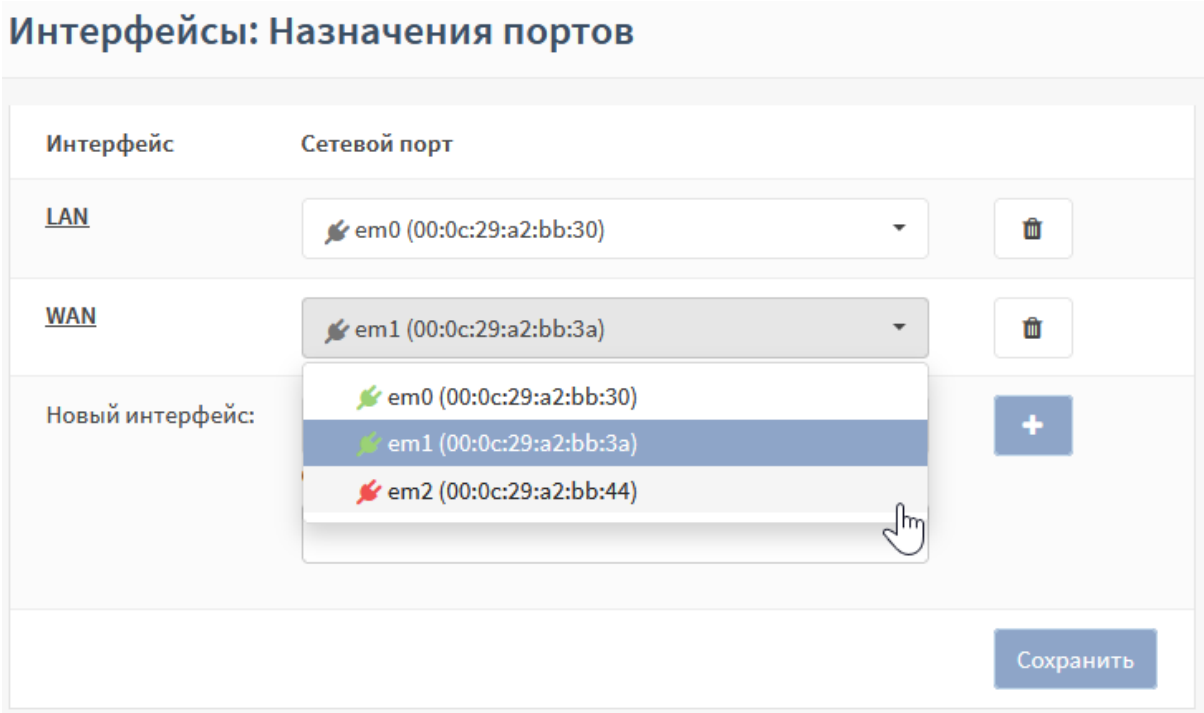


Рисунок – Переназначение портов

17.2 Настройка сетевых интерфейсов

Для перехода в подраздел настроек конкретного сетевого интерфейса существуют два способа:

- нажать **левой кнопкой мыши** на имя необходимого интерфейса в подразделе назначения портов (**«Интерфейсы» - «Назначения портов»**) (см. Рисунок – Назначение портов);
- выбрать необходимый интерфейс в списке раздела **«Интерфейсы»**.

При конфигурировании нового интерфейса или изменении существующего необходимо задать/изменить настройки в следующих блоках:

- **«Базовая конфигурация»**;
- **«Общая конфигурация»**;

- **«Контроль доступа устройств»**.

17.2.1 Блок «Базовая конфигурация»

В данном блоке (см. Рисунок – Настройка сетевого интерфейса. Базовая конфигурация) присутствуют следующие параметры:

- **«Включить»** – включает и выключает интерфейс;
- **«Включить физически»** – включает и выключает физический интерфейс;
- **«Блокировать»** – защищает от случайного удаления интерфейса;
- **«Устройство»** – отображает имя сетевого интерфейса;
- **«Описание»** – отображает имя интерфейса в **ARMA FW**.

Примечание:

Не рекомендуется без необходимости снимать флажок для параметра **«Включить физически»**.

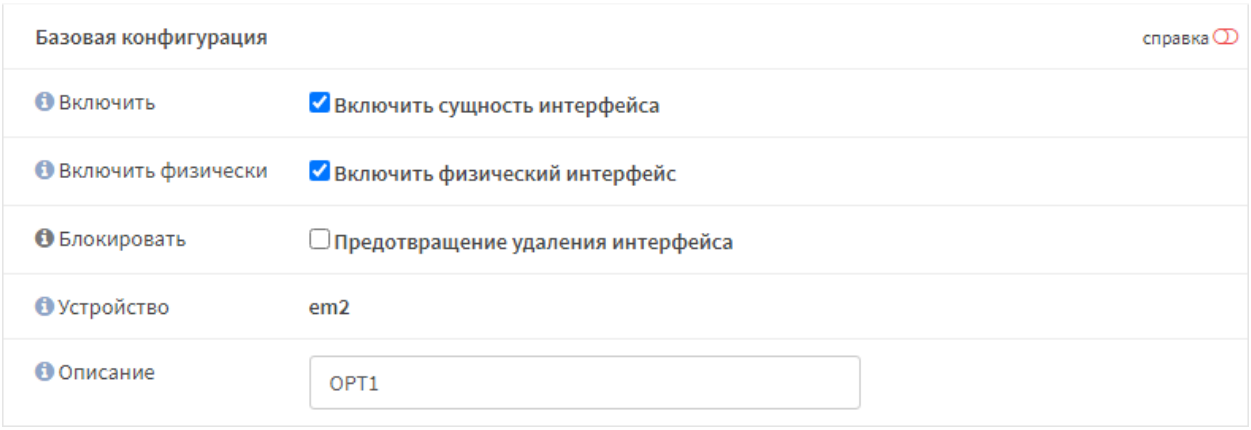


Рисунок – Настройка сетевого интерфейса. Базовая конфигурация

17.2.2 Блок «Общая конфигурация»

В данном блоке (см. Рисунок – Настройка сетевого интерфейса. Общая конфигурация) присутствуют следующие параметры:

- **«Блокировать частные сети»** – блокирует трафик с IP-адресов, зарезервированных для частных сетей: «10/8», «172.16/12», «192.168/16»; адреса обратной связи: «127/8», адреса NAT: «100.64/10»;
- **«Блокировать bogon сети»** – блокирует трафик с IP-адресов, которые не должны встречаться в таблицах маршрутизации в сети интернет или в качестве адреса отправителя получаемых пакетов;
- **«Блокировать трафик на SPAN порту»** – блокирует трафик от любого отправителя;

- **«Тип конфигурации IPv4»** – задаёт настройки конфигурации IPv4 (см. Конфигурация IPv4);
- **«Тип конфигурации IPv6»** – задаёт настройки конфигурации IPv6;
- **«MAC-адрес»** – имитирует заданный MAC-адрес для интерфейса;
- **«Максимальный размер кадра»** – задаёт максимальный размер кадра для сетевой карты;
- **«Максимальный размер сегмента»** – задаёт максимальный размер сегмента для TCP соединений;
- **«Скорость и двусторонний режим передачи данных»** – задаёт скорость и режим передачи для сетевой карты;
- **«Политика динамического шлюза»** – позволяет создавать динамические шлюзы без прямых адресов.

Примечание:

Параметры **«MAC-адрес»**, **«Максимальный размер кадра»**, **«Максимальный размер сегмента»**, **«Скорость и двусторонний режим передачи данных»**, **«Политика динамического шлюза»** стоит изменять только в случае необходимости, так как некорректные значения могут повлиять на работоспособность интерфейса.

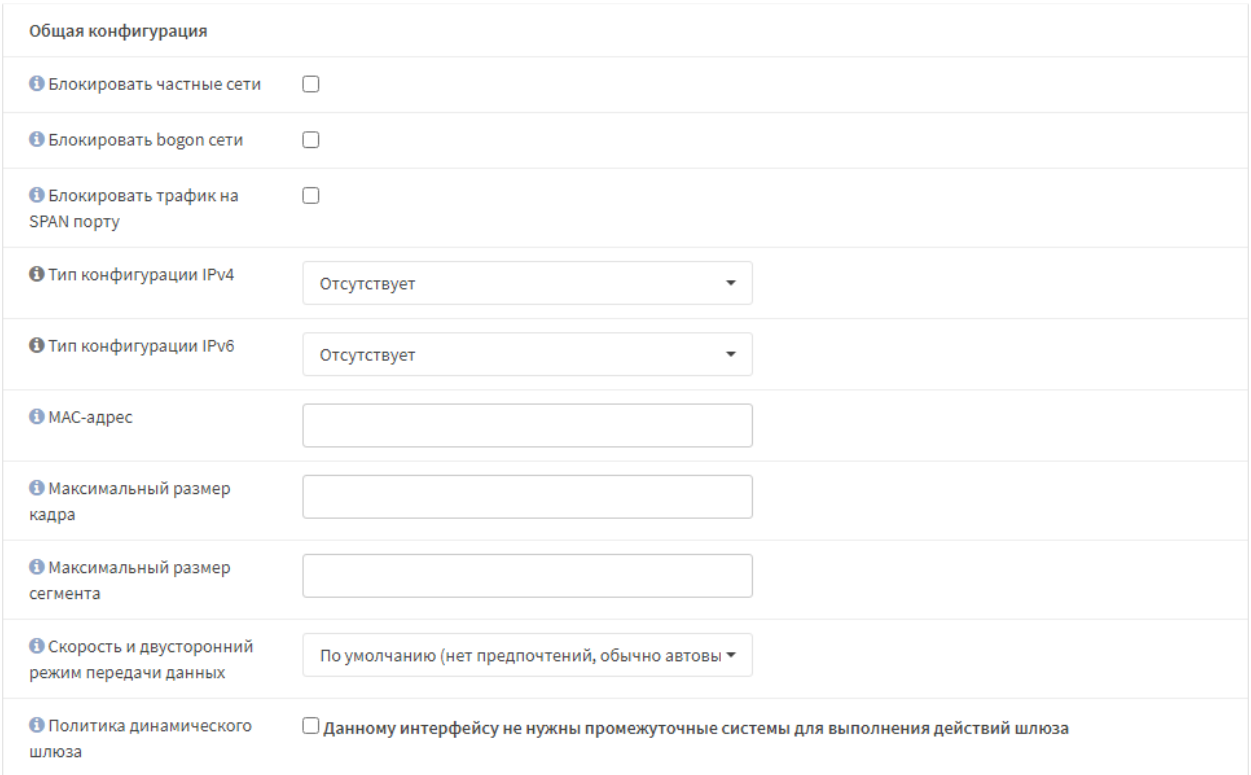


Рисунок – Настройка сетевого интерфейса. Общая конфигурация

17.2.2.1 Конфигурация IPv4

Параметр **«Тип конфигурации IPv4»** включает в себя следующие значения:

- **«Отсутствует»** – конфигурация не задана;
- **«Статический IPv4»** – ручное указание настроек IPv4;
- **«DHCP»** – автоматическая настройка IPv4 посредством DHCP;
- **«PPTP»** – конфигурации IPv4 по протоколу туннелирования PPTP;
- **«L2TP»** – конфигурации IPv4 по протоколу туннелирования L2TP.

При выборе значения «Статический IPv4» появится дополнительный блок настроек (см. Рисунок – Конфигурация статического IPv4-адреса), в котором указываются IP-адрес и маска сети, а также, при необходимости, задаются параметры публичного IP-адреса шлюза после нажатия **кнопки** « + ».

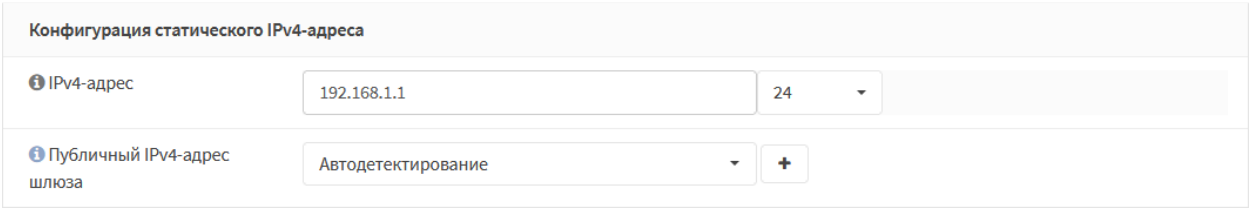


Рисунок – Конфигурация статического IPv4-адреса

При выборе значения «DHCP» **ARMA FW** выполнит автоматическую настройку интерфейса посредством DHCP. При этом появится дополнительный блок настроек (см. Рисунок – Конфигурация DHCP-клиента) для настройки конфигурации DHCP–клиента.

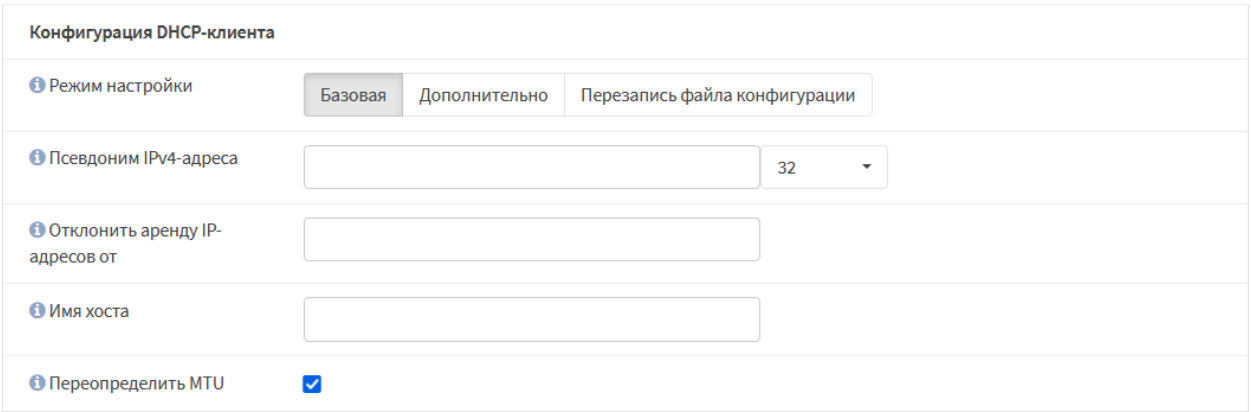


Рисунок – Конфигурация DHCP-клиента

Полученный по DHCP IP-адрес будет отображаться в виджете **«Интерфейсы»** раздела **«Инструменты»** (см. Мониторинг системы с помощью информационных виджетов).

При выборе значения «PPTP»/«L2TP» появится дополнительный блок конфигурации IPv4 по протоколам туннелирования (см. Рисунок – Настройка сетевого интерфейса. Конфигурация PPTP/L2TP).

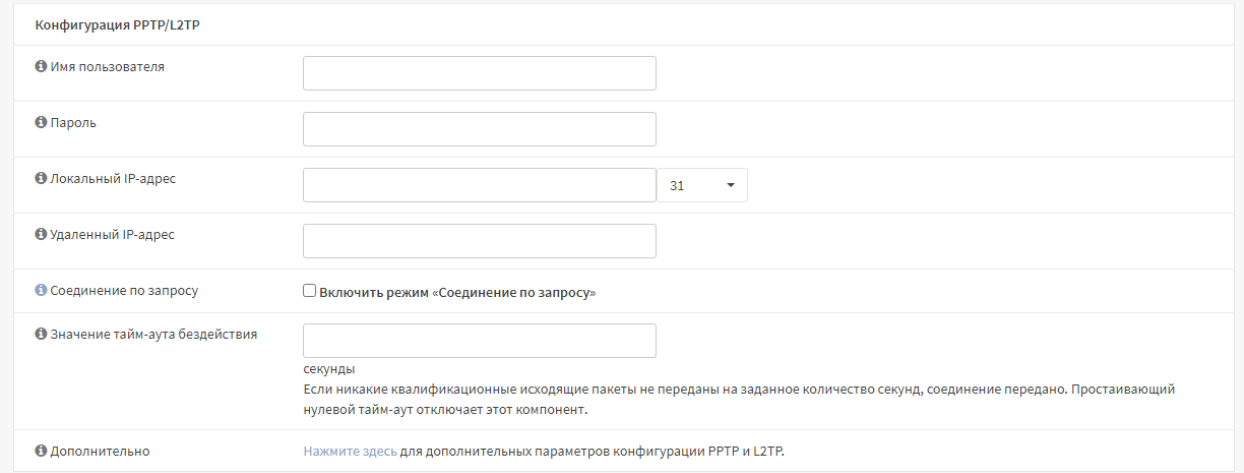


Рисунок – Настройка сетевого интерфейса. Конфигурация PPTP/L2TP

Примечание:

При настройке конфигурации IPv4 адресное пространство различных интерфейсов не должно совпадать. При необходимости использовать для **ARMA FW** более одного IP-адреса из одной сети необходимо воспользоваться подразделом настроек виртуальных адресов (**«Межсетевой экран» - «Виртуальные IP-адреса» - «Настройки»**).

17.2.2.2 Конфигурация IPv6

Параметр **«Тип конфигурации IPv6»** включает в себя следующие значения:

- **«Отсутствует»** – конфигурация не задана;
- **«Статический IPv6»** – ручное указание настроек IPv6;
- **«DHCPv6»** – автоматическая настройка IPv6 посредством DHCPv6;
- **«SLAAC»** – автоматическая настройка IPv6 посредством SLAAC;
- **«Туннель 6RD»** – автоматическая настройка IPv6 по протоколу 6RD;
- **«Туннель 6to4»** – автоматическая настройка IPv6 по протоколу 6to4;
- **«Отслеживать состояние интерфейсов»** – отслеживание настроек IPv6.

При выборе значения «Статический IPv6» появится дополнительный блок настроек (см. Рисунок – Конфигурация статического IPv6-адреса), в котором указываются IP-адрес и маска сети, а также, при необходимости, задаются параметры публичного IP-адреса шлюза после нажатия **кнопки** « + » и возможность использовать IPv4-подключение.

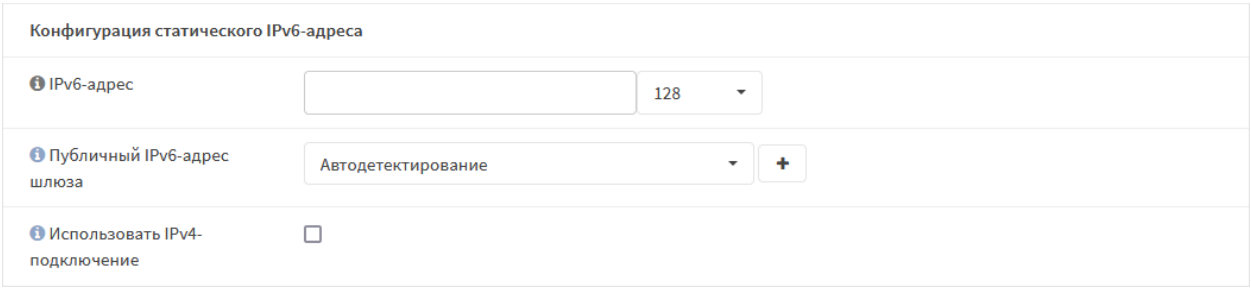


Рисунок – Конфигурация статического IPv6-адреса

При выборе значения «DHCPv6» **ARMA FW** выполнит автоматическую настройку интерфейса посредством DHCP. При этом появится дополнительный блок настроек (см. Рисунок – Конфигурация DHCPv6-клиента) для настройки конфигурации DHCP–клиента.

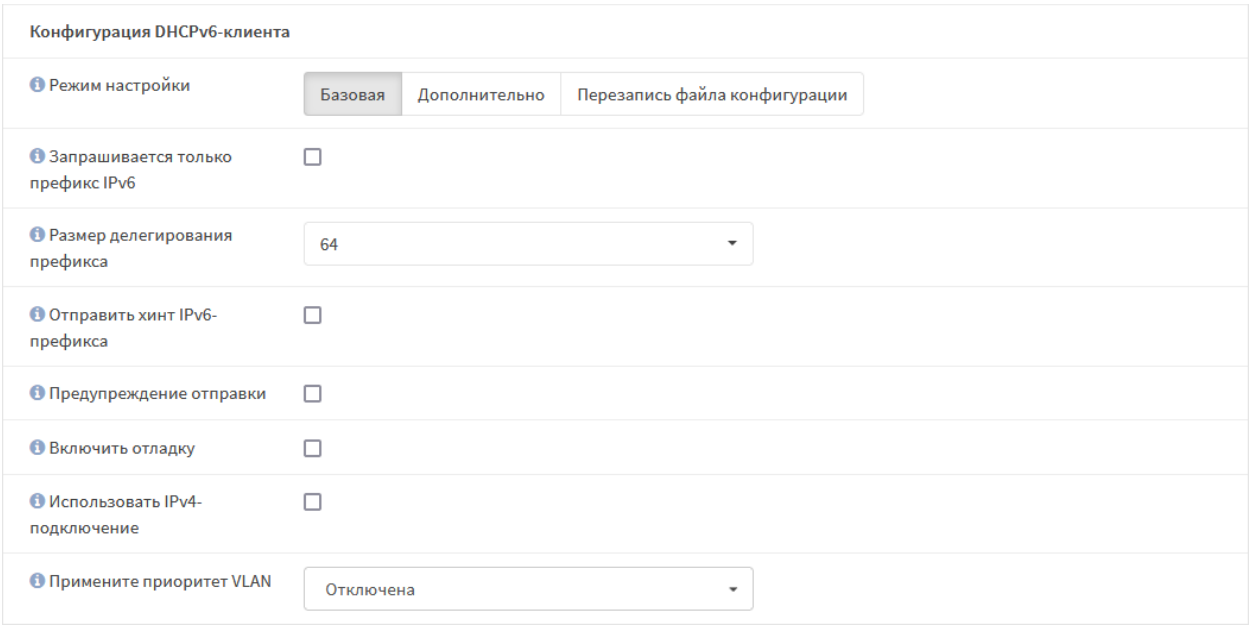


Рисунок – Конфигурация DHCPv6-клиента

При выборе значения «SLAAC» **ARMA FW** выполнит автоматическую настройку интерфейса посредством SLAAC без помощи DHCPv6-сервера. При этом появится дополнительный блок настроек (см. Рисунок – Конфигурация SLAAC) для настройки конфигурации DHCP–клиента.

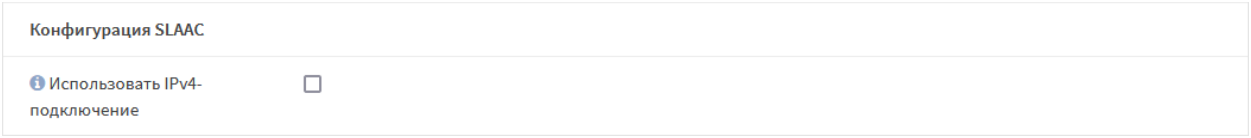


Рисунок – Конфигурация SLAAC

При выборе значения «Туннель 6RD» **ARMA FW** выполнит автоматическую настройку интерфейса по протоколу 6RD. При этом появится дополнительный блок настроек (см. Рисунок – Конфигурация протокола 6RD) для настройки конфигурации протокола 6RD.

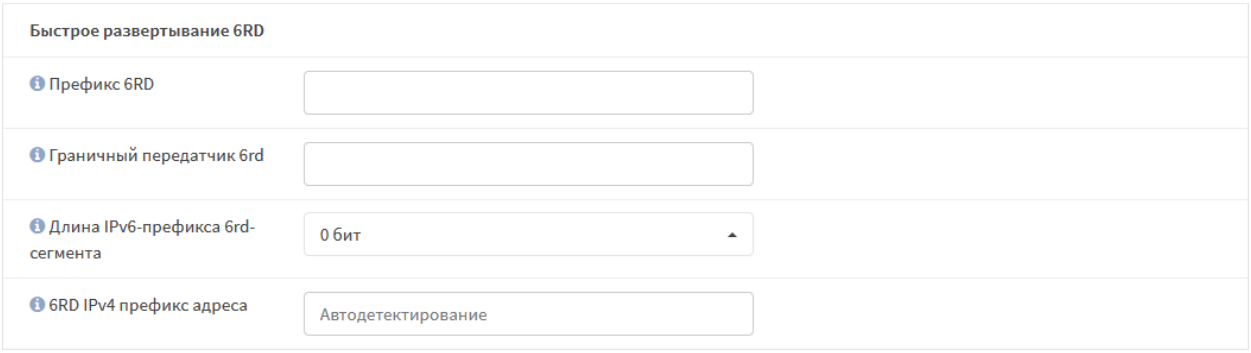


Рисунок – Конфигурация протокола 6RD

При выборе значения «Туннель 6to4» **ARMA FW** выполнит автоматическую настройку интерфейса по протоколу 6to4.

Примечание:

При настройке конфигурации IPv6 адресное пространство различных интерфейсов не должно совпадать.

17.2.3 Блок «Контроль доступа устройств»

В данном блоке (см. Рисунок – Настройка сетевого интерфейса. Контроль доступа устройств) возможно задать параметры контроля доступа устройств:

- **«Отключена»** – контроль доступа отключён;
- **«Белый список»** – доступ к настраиваемому интерфейсу имеют только указанные хосты;
- **«Черный список»** – доступ к настраиваемому интерфейсу имеют все, кроме указанных хостов.

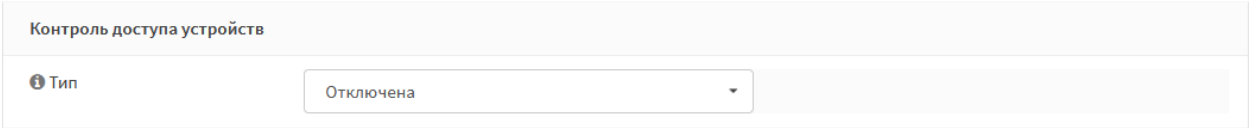


Рисунок – Настройка сетевого интерфейса. Контроль доступа устройств

При выборе значений «Белый список» или «Черный список» будет доступен параметр **«Список устройств»** с полем ввода значений MAC-адресов в виде списка, разделённых знаком «запятая».

17.3 Расширенные настройки

Для всех интерфейсов доступны расширенные настройки в подразделе настроек интерфейсов (**«Интерфейсы» - «Настройки»**) (см. Рисунок – Настройки интерфейсов).

Расширенные настройки требуются для использования определённых сценариев, например, при включении СОВ. В большинстве случаев настройки рекомендуется оставлять по умолчанию.

В случае выбора в параметре **«Фильтрация аппаратного обеспечения VLAN»** значения «Отключить фильтрацию аппаратного обеспечения внешних VLAN» появится дополнительное поле с выбором интерфейса, на котором будет отключена фильтрация. Отключение фильтрации для выбранного интерфейса позволяет успешно проходить тегированному трафику VLAN, созданных вне **ARMA FW**, при включённой IPS.

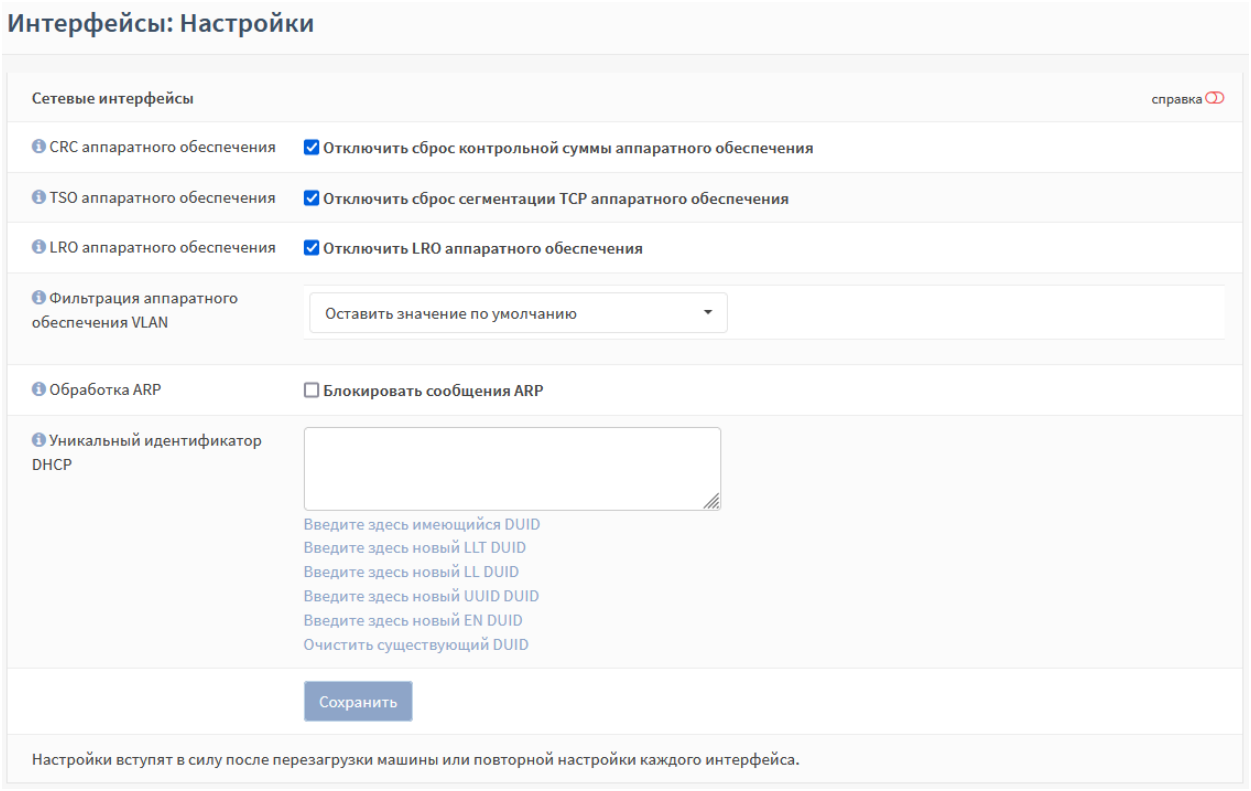


Рисунок – Настройки интерфейсов

18 GRE

Данный протокол используется для передачи пакетов сетевого уровня, инкапсулированных в пакеты транспортного уровня.

18.1 Пример настройки туннеля GRE

В качестве примера настройки туннеля GRE, используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки туннеля GRE).

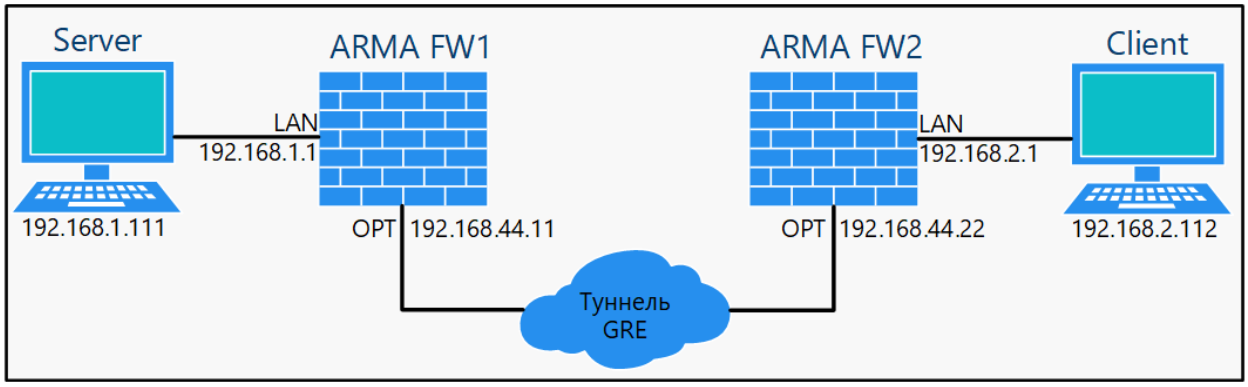


Рисунок – Схема стенда для настройки туннеля GRE

Используемые IP-адреса приведены в качестве примера.

Для настройки туннеля GRE необходимо выполнить следующие шаги:

1. Создать интерфейсы GRE.
2. Создать правила МЭ.
3. Проверить наличие добавленного шлюза.
4. Добавить маршрут.
5. Выполнить проверку.

18.1.1 Создание интерфейса GRE

Для создания интерфейса GRE на каждом **ARMA FW** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки GRE (**«Интерфейсы» - «Другие типы» - «GRE»**) и нажать **кнопку «+Добавить»** (см. Рисунок – Подраздел GRE).

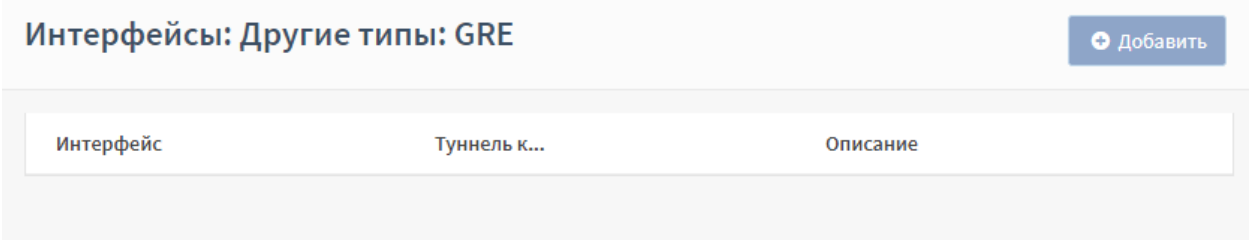


Рисунок – Подраздел GRE

2. В открывшейся форме (см. Рисунок – Конфигурация GRE) указать следующие параметры:
   - **ARMA FW1**:
     - **«Родительский интерфейс»** – «OPT1»;
     - **«Удаленный IP-адрес GRE»** – «192.168.44.22»;
     - **«Локальный IP-адрес GRE-туннеля»** – «10.0.0.1»;
     - **«Удаленный IP-адрес GRE-туннеля»** – «10.0.0.2», «24»;
     - **«Описание»** – «GRE FW 1»;
   - **ARMA FW2**:
     - **«Родительский интерфейс»** – «OPT1»;
     - **«Удаленный IP-адрес GRE»** – «192.168.44.11»;
     - **«Локальный IP-адрес GRE-туннеля»** – «10.0.0.2»;
     - **«Удаленный IP-адрес GRE-туннеля»** – «10.0.0.1», «24»;
     - **«Описание»** – «GRE FW 2»;

   и нажать **кнопку «Сохранить»**.

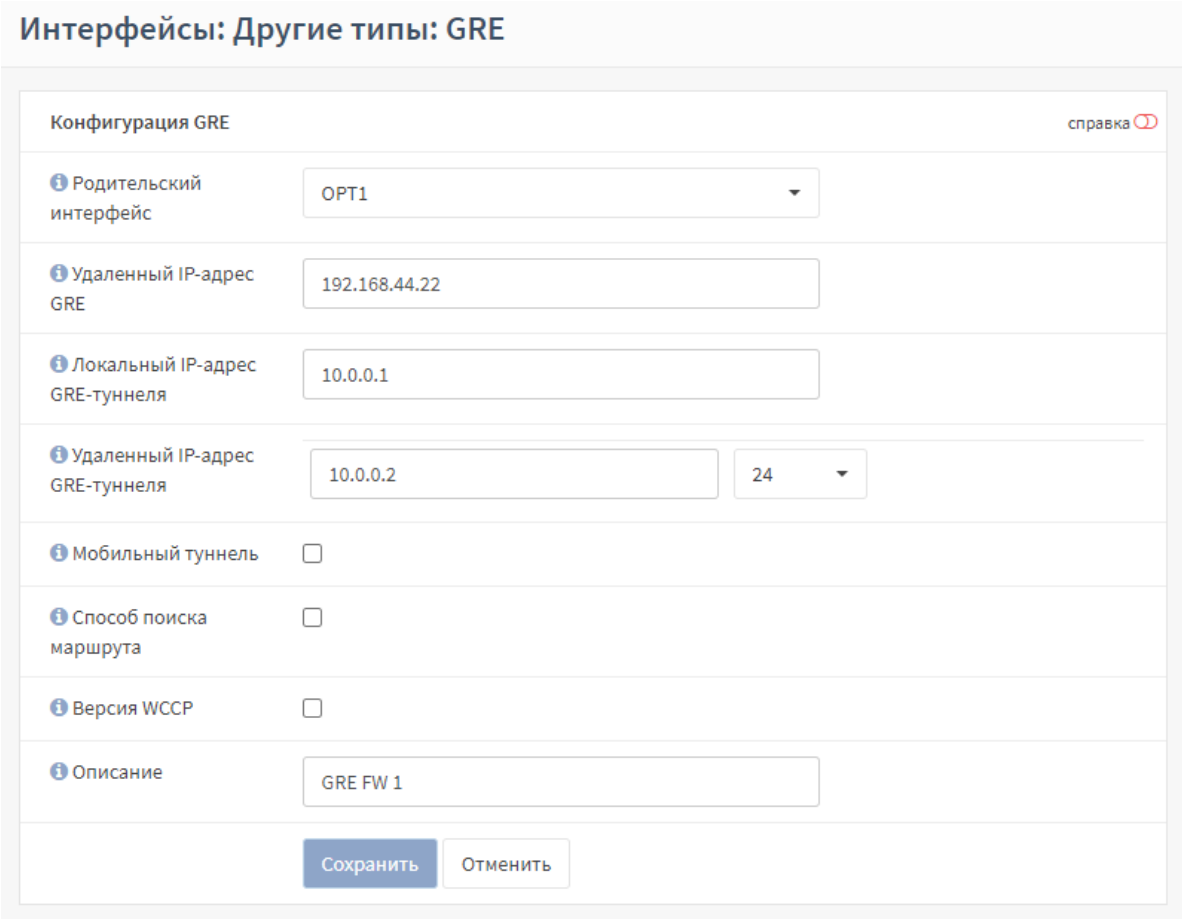


Рисунок – Конфигурация GRE

В результате, созданный GRE-интерфейс будет отображён в списке (см. Рисунок – Список созданных интерфейсов GRE).

Рисунок – Список созданных интерфейсов GRE

3. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**), ввести «GRE» в поле параметра **«Описание»** и нажать **кнопку** « + » напротив обнаруженного интерфейса, а затем нажать **кнопку «Сохранить»** (см. Рисунок – Назначение порта).

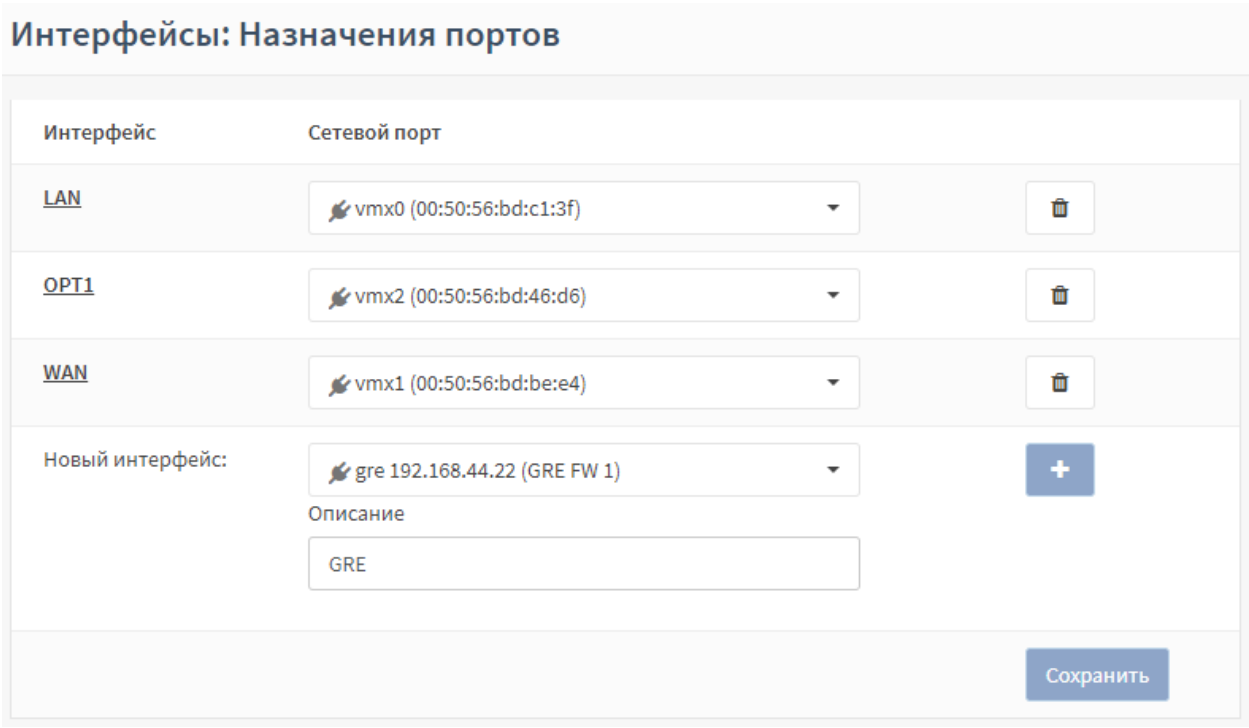


Рисунок – Назначение порта

4. Нажать на имя созданного интерфейса «GRE», в открывшемся окне установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**. Не указанные параметры оставить по умолчанию.

18.1.2 Создание правил МЭ

Для корректной работы GRE-туннеля, на каждом **ARMA FW** следует настроить правила МЭ.

Для создания правил МЭ необходимо выполнить следующие действия:

1. Перейти в подраздел настройки правил МЭ для интерфейса «[GRE]» (**«Межсетевой экран» - «Правила» - «[GRE]»**), нажать **кнопку «+Добавить»** и указать следующие параметры:
   - **«Действие»** – «Разрешить (Pass)»;
   - **«Направление»** – «Любой»;
   - **«Описание»** – «Allow GRE traffic»;

   и нажать **кнопку «Сохранить»**.

   Не указанные параметры следует оставить по умолчанию.
2. Перейти в подраздел настройки правил МЭ для интерфейса «[OPT1]» (**«Межсетевой экран» - «Правила» - «[OPT1]»**), нажать **кнопку «+Добавить»** и указать следующие параметры:

- **«Действие»** – «Разрешить (Pass)»;
- **«Направление»** – «Любой»;
- **«Описание»** – «Allow GRE»;

и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

Не указанные параметры следует оставить по умолчанию.

18.1.3 Проверка наличия добавленного шлюза

Для проверки наличия автоматически добавленного шлюза, на каждом **ARMA FW** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки шлюзов (**«Система» - «Шлюзы» - «Единичный»**).
2. Убедиться в наличии шлюза с именем «GRE_TUNNELV4» (см. Рисунок – Шлюзы).

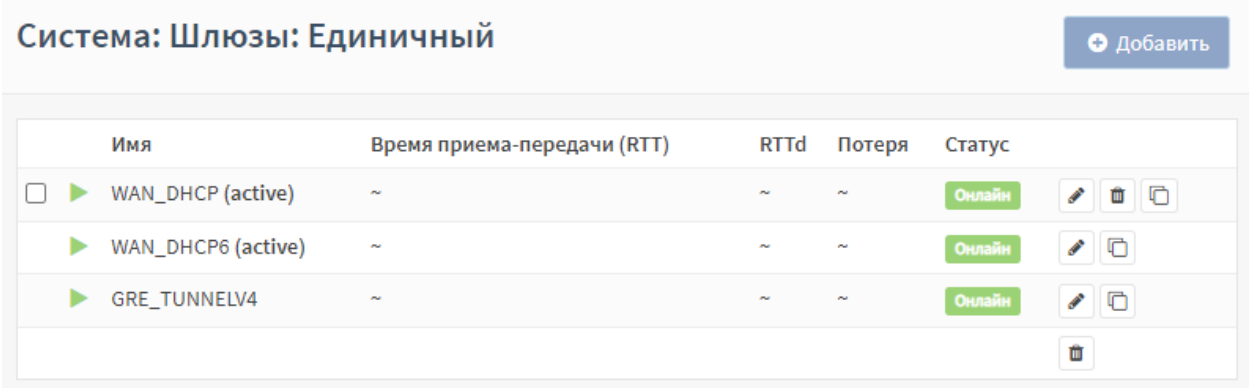


Рисунок – Шлюзы

В случае отсутствия шлюза с именем «GRE_TUNNELV4», следует нажать **кнопку «+Добавить»** и указать следующие параметры:

- **«Имя»** – «GRE_Gway»;
- **«Интерфейс»** – «GRE»;

и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

18.1.4 Добавление маршрута

Для добавления маршрута на каждом **ARMA FW** необходимо перейти в подраздел настройки маршрутов (**«Система» - «Маршруты» - «Конфигурация»**), нажать **кнопку** « + » и указать следующие параметры:

- **ARMA FW1**:
  - **«Адрес сети»** – «192.168.2.0/24»;

- **«Шлюз»** – «GRE_TUNNELV4 - 10.0.0.2»;
- **«Описание»** – «route»;

- **ARMA FW2**:
  - **«Адрес сети»** – «192.168.1.0/24»;
  - **«Шлюз»** – «GRE_TUNNELV4 - 10.0.0.1»;
  - **«Описание»** – «route»;

и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

18.1.5 Проверка работы

Для проверки работы необходимо с ПК **«Client»** выполнить команду «ping» ПК **«Server»**. При правильной настройке, команда выполнится успешно.

19 LAGG

Для повышения отказоустойчивости и пропускной способности интерфейсов используется функция агрегации каналов LAGG. Функция объединяет несколько физических интерфейсов в один логический интерфейс.

Создание LAGG-интерфейса возможно только из несконфигурированных интерфейсов.

Тестовый стенд имеет следующие параметры:

1. **ARMA FW** установлен на ВМ гипервизора VMware.
2. ВМ имеет три сетевых адаптера (см. Рисунок – Параметры виртуальной машины).
3. Первый и второй сетевые адаптеры подключены к виртуальной сети **«VMnet0»** в режиме **«Сетевой мост»** с сетевым адаптером гипервизора.
4. Третий сетевой адаптер используется для конфигурирования и доступа в Интернет **ARMA FW**.
5. Настройки сетевого адаптера гипервизора:
   - **Сеть** – «192.168.1.1/24»;
   - **IP-адрес** – назначается DHCP.
6. Сетевые адаптеры в **ARMA FW** «em0» и «em1» не сконфигурированы.

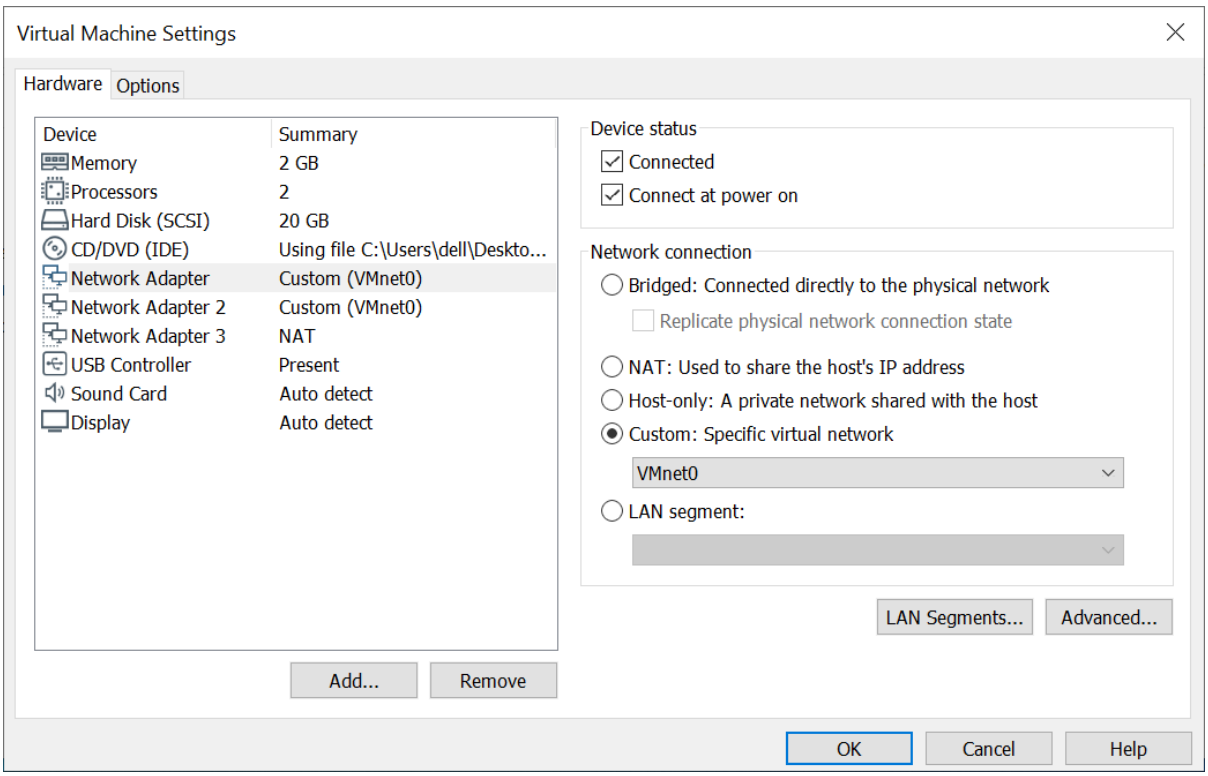


Рисунок – Параметры виртуальной машины

19.1 Создание LAGG-интерфейса

Для создания LAGG-интерфейса необходимо выполнить следующие действия:

1. Перейти в подраздел настройки LAGG (**«Интерфейсы» - «Другие типы» - «LAGG»**).
2. В подразделе (см. Рисунок – Подраздел LAGG) нажать **кнопку «+Добавить»**.

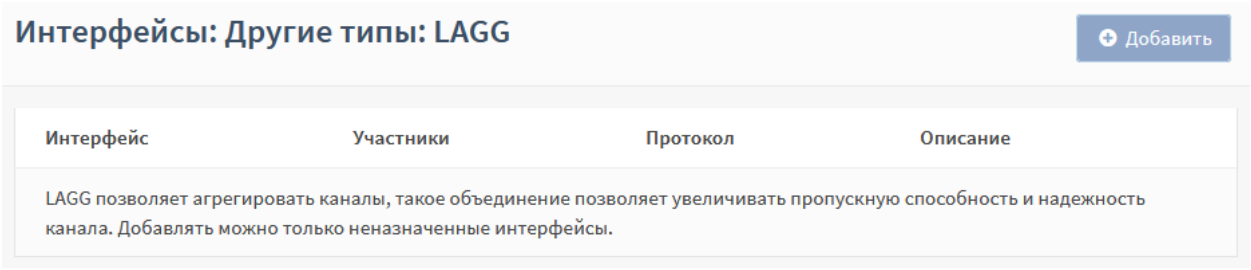


Рисунок – Подраздел LAGG

3. В открывшейся форме (см. Рисунок – Конфигурация LAGG) указать значения параметров:
   - **«Родительский интерфейс»** – «em0» и «em1»;
   - **«Протокол LAG»** – «FAILOVER», в данном режиме трафик проходит только через главный порт, указанный в интерфейсе первым. Если главный порт недоступен, используется следующий активный порт;
   - **«Описание»** – «Дублирование сетевых интерфейсов».

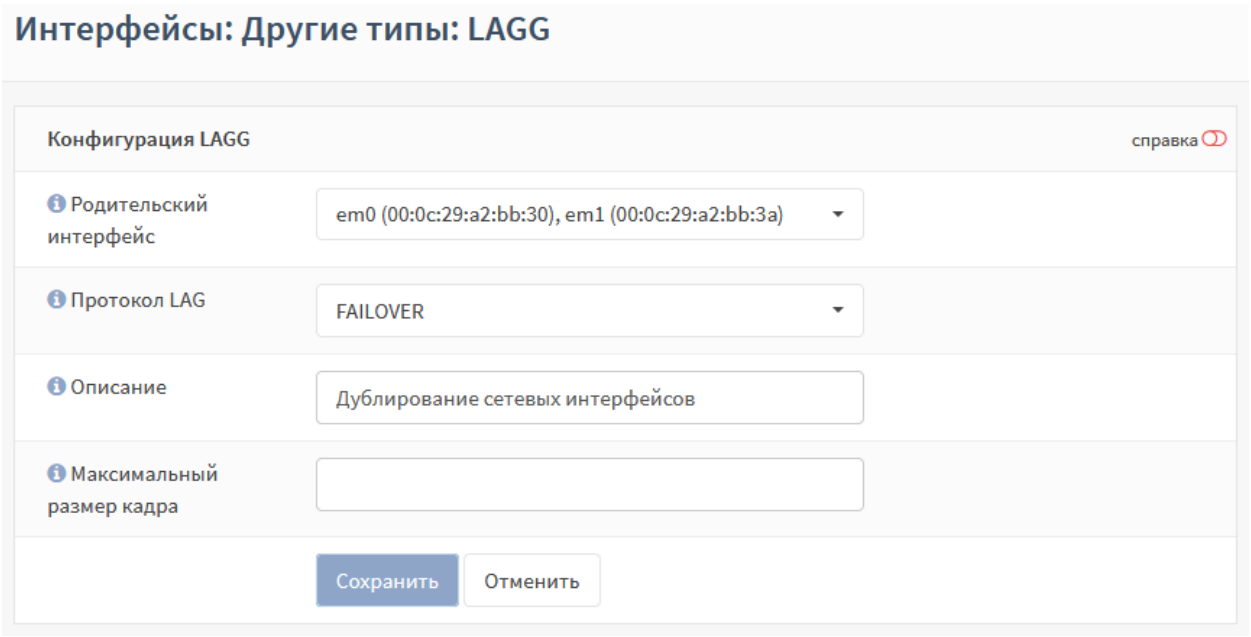


Рисунок – Конфигурация LAGG

4. Нажать **кнопку «Сохранить»**.
5. В результате созданный LAGG-интерфейс будет отображён в списке (см. Рисунок – Список созданных интерфейсов).

Рисунок – Список созданных интерфейсов

Примечание:

По умолчанию приём трафика осуществляется только через активный в данный момент интерфейс. Для того чтобы приём трафика осуществлялся всеми членами LAGG-интерфейса, необходимо добавить параметр **«net.link.lagg.failover_rx_all»**. Без добавления данного параметра переключение между интерфейсами будет происходить некорректно.

Для добавления параметра необходимо выполнить следующие действия:

1. Перейти в подраздел параметров **ARMA FW** (**«Система» - «Настройки» - «Параметры»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать:
   - **«Параметр»** – «net.link.lagg.failover_rx_all»;
   - **«Значение»** – «1».

19.2 Настройка LAGG-интерфейса

Настройка сетевых интерфейсов осуществляется в подразделах интерфейса **«Назначения портов»** (см. Назначение портов) и **«[имя интерфейса]»** (см. Настройка сетевых интерфейсов).

Для настройки созданного LAGG-интерфейса необходимо выполнить следующие действия:

1. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**).
2. Добавить новый интерфейс, нажав **кнопку** «+» и выбрав в списке сетевых портов «lagg0 (Агрегация сетевых интерфейсов)».
3. Нажать **кнопку «Сохранить»**.
4. Перейти в созданный интерфейс (**«Интерфейсы» - «[OPT2]»**).

5. Установить флажок **«Включить интерфейс»** и выбрать значение параметра **«Тип конфигурации IPv4» – «DHCP»**.
6. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.
7. Результат настройки интерфейса **«[OPT2]»** будет отображён в подразделе общей информации об интерфейсах (**«Интерфейсы» - «Обзор»**) (см. Рисунок – Настроенный интерфейс).

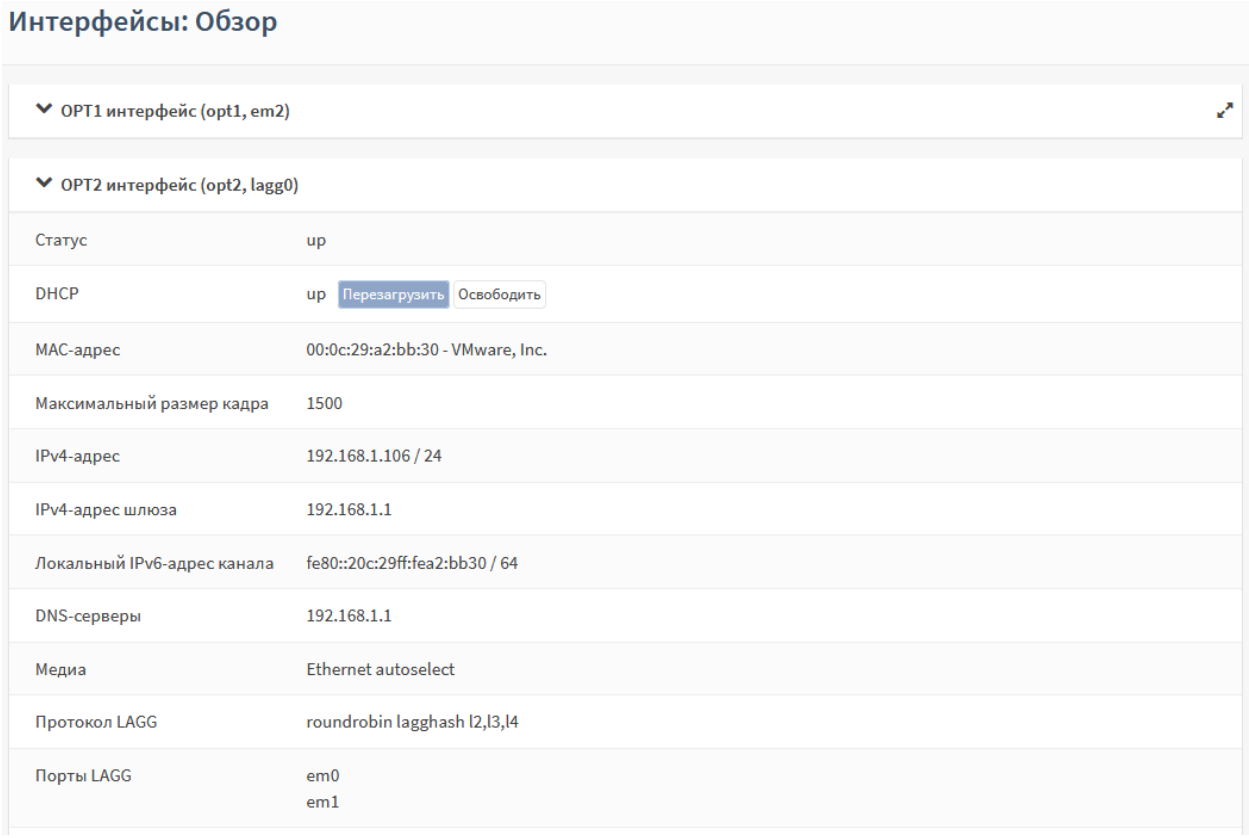


Рисунок – Настроенный интерфейс

19.3 Проверка работы LAGG-интерфейса

Для проверки работы LAGG-интерфейса будет использоваться функция ping **ARMA FW** (**«Интерфейсы» - «Диагностика» - «Ping»**) (см. Рисунок – Функция «Ping»).

Рисунок – Функция «Ping»

Порядок проверки работы LAGG-интерфейса:

1. В форме функции **«Ping»** (см. Рисунок – Функция «Ping») задать следующие параметры:
   - **«Хост»** – «8.8.8.8»;
   - **«Протокол»** – «IPv4»;
   - **«IP-адрес источника»** – «OPT2»;
   - **«Количество»** – «3».
2. Нажать **кнопку «Ping»** – результат внизу страницы (см. Рисунок – Результат работы утилиты «Ping») свидетельствует о корректности настройки LAGG-интерфейса.

```
# /sbin/ping -S '192.168.1.200' -c '3' '8.8.8.8'
PING 8.8.8.8 (8.8.8.8) from 192.168.1.200: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=46.217 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=47.309 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=53.642 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 46.217/49.056/53.642/3.273 ms
```

Рисунок – Результат работы утилиты «Ping»

3. В интерфейсе гипервизора отключить один из сетевых интерфейсов, входящих в LAGG-интерфейс (см. Рисунок – Выключение сетевого интерфейса).

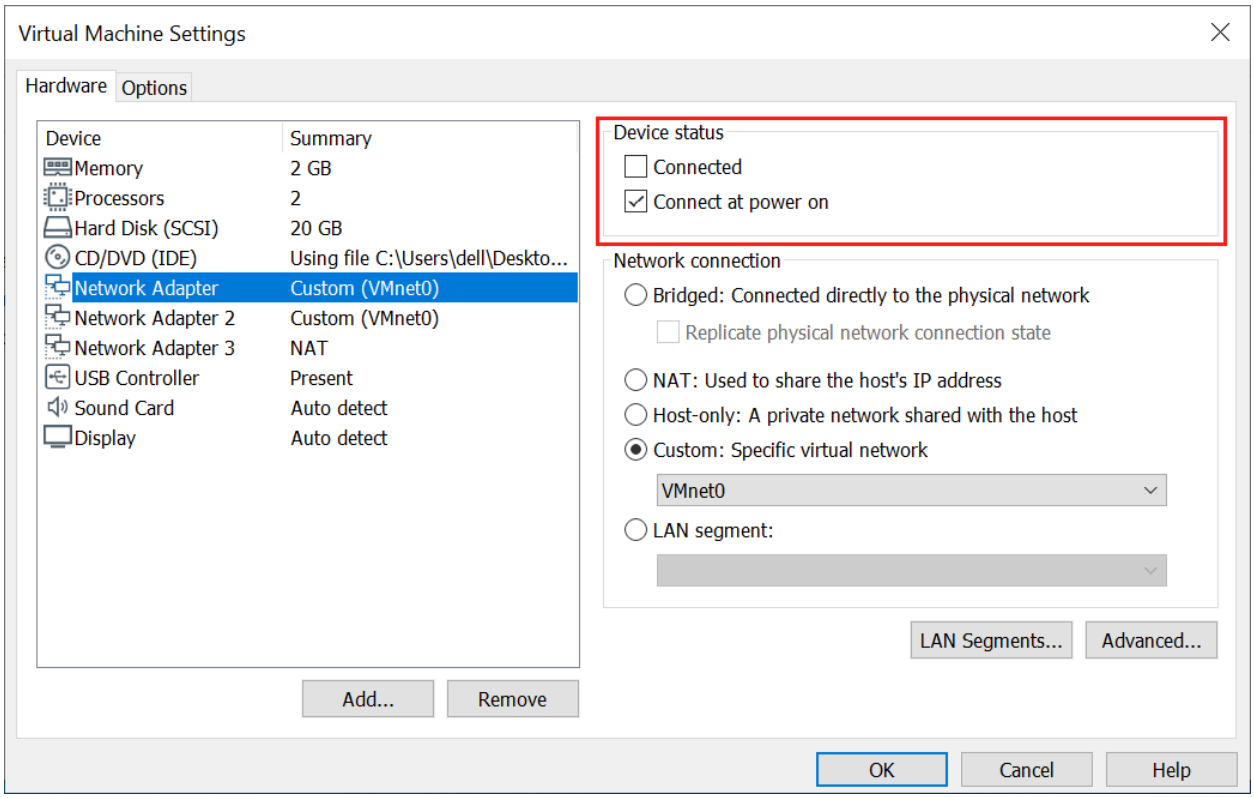


Рисунок – Выключение сетевого интерфейса

4. Повторно нажать **кнопку «Ping»** – результат внизу страницы (см. Рисунок – Результат работы утилиты «Ping») свидетельствует о корректности работы LAGG-интерфейса в случае отключения одного из физических интерфейсов, входящих в его состав.

```
# /sbin/ping -S '192.168.1.200' -c '3' '8.8.8.8'
PING 8.8.8.8 (8.8.8.8) from 192.168.1.200: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=46.217 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=47.309 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=53.642 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 46.217/49.056/53.642/3.273 ms
```

Рисунок – Результат работы утилиты «Ping»

20 СЕТЕВОЙ МОСТ

Сетевой мост – это объединение различных сегментов сети передачи данных в единую сеть.

В **ARMA FW** добавление и настройка сетевых мостов производится в подразделе интерфейсов (**«Интерфейсы» - «Другие типы» - «Сетевые мосты»**). При создании сетевого моста в веб-интерфейсе **ARMA FW** создаётся новый сетевой интерфейс в ОС с именем «bridge» и порядковым номером, начиная с «0».

20.1 Пример настройки сетевого моста

Перед настройкой и включением сетевого моста необходимо изменить значения системных параметров:

- **«net.link.bridge.pfil_bridge»** – установить значение «1»;
- **«net.link.bridge.pfil_member»** – установить значение «0».

Для изменения параметров необходимо выполнить следующие действия:

1. Перейти в подраздел параметров **ARMA FW** (**«Система» - «Настройки» - «Параметры»**).
2. Нажать **кнопку** « » напротив изменяемого параметра и задать значение в поле **«Значение»**.
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

20.1.1 Создание сетевого моста

Для настройки и проверки работоспособности сетевого моста используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки сетевого моста).

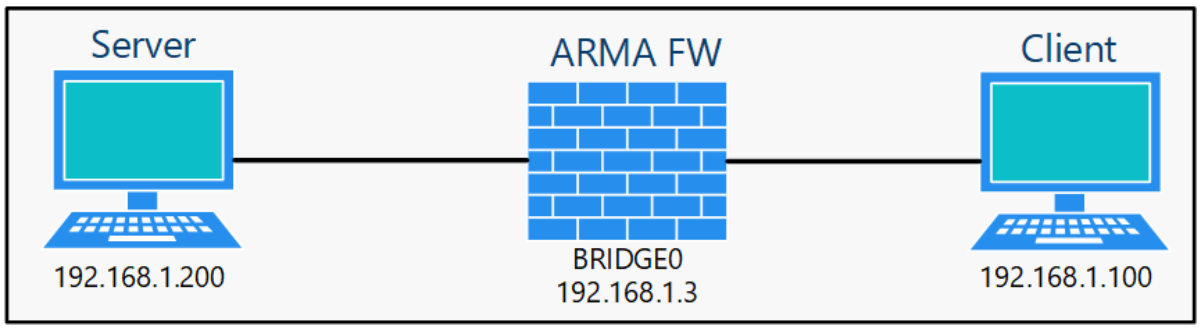


Рисунок – Схема стенда для настройки сетевого моста

Для добавления сетевого моста необходимо выполнить следующие действия:

1. Перейти в подраздел настройки сетевых мостов (**«Интерфейсы» - «Другие типы» - «Сетевой мост»**) и нажать **кнопку «+Добавить»**.

2. В поле параметра **«Интерфейсы-участники»** указать интерфейсы, соединяемые с помощью моста – «LAN» и «WAN», а затем нажать **кнопку «Сохранить»** (см. Рисунок – Добавление сетевого моста).

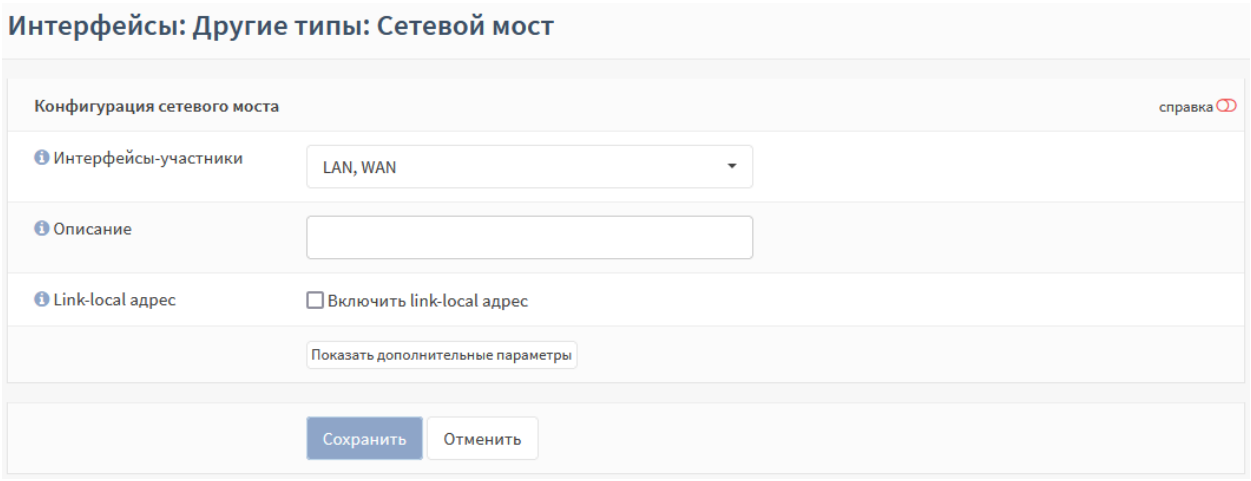


Рисунок – Добавление сетевого моста

3. Добавленный сетевой мост будет отображён в общей таблице (см. Рисунок – Перечень созданных сетевых мостов).

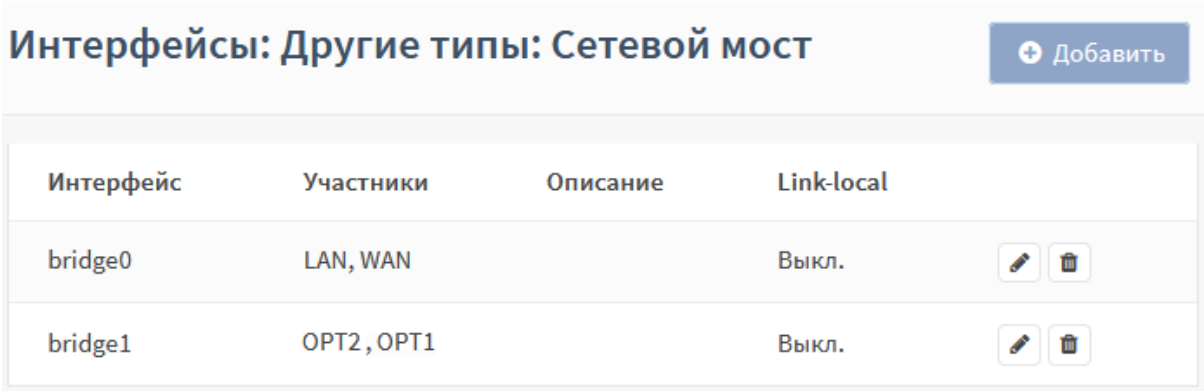


Рисунок – Перечень созданных сетевых мостов

4. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**), выбрать значение «bridge0» в параметре **«Новый интерфейс»**, ввести «BRIDGE0» в поле параметра **«Описание»** и нажать **кнопку** «+» для создания интерфейса (см. Назначение портов).

5. Перейти в настройки созданного сетевого интерфейса (**«Интерфейсы» - «[BRIDGE0]»**) и задать настройки согласно таблице (см. Таблица «Параметры интерфейса»).

Таблица «Параметры интерфейса»

Параметр	Значение
Включить	Значение установлено
Тип конфигурации IPv4	Статический IPv4

Параметр	Значение
Тип конфигурации IPv6	Отсутствует
IPv4-адрес	192.168.1.3/24

6. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

   Примечание:

   После настройки сетевого моста правила МЭ необходимо создавать для интерфейса сетевого моста. Правила МЭ для интерфейсов-участников сетевого моста будут игнорироваться.

20.1.2 Проверка настроенного сетевого моста

Перед проверкой настроенного моста необходимо добавить правило МЭ (см. Создание правил межсетевого экранирования) для интерфейса **«[BRIDGE0]»**, разрешающее прохождение трафика по протоколу ICMP.

Для проверки работоспособности необходимо выполнить следующие действия:

1. Перейти в настройки DHCP-сервера интерфейса «LAN» (**«Службы» - «DHCPv4» -«[LAN]»**) и выключить DHCP-сервер, убрав флажок с параметра **«Включить DHCP-сервер на LAN интерфейсе»**, а затем, нажав **кнопку «Сохранить»**.
2. На ПК **«Client»** открыть браузер, выполнить подключение к веб-интерфейсу **ARMA FW** по адресу сетевого интерфейса «BRIDGE0» – «https://192.168.1.3» и произвести аутентификацию в веб-интерфейсе.
3. Перейти в подраздел настроек LAN интерфейса (**«Интерфейсы» - «[LAN]»**), в поле **«Тип конфигурации IPv4»** выбрать **«Отсутствует»**, нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**. В подразделе настроек WAN (**«Интерфейсы» - «[WAN]»**) интерфейса повторить те же действия.
4. Перезагрузить **ARMA FW**. С ПК **«Client»** выполнить команду «ping» ПК **«Server»**. При правильной настройке сетевого моста команда выполнится успешно (см. Рисунок – Успешное выполнение команды ping).

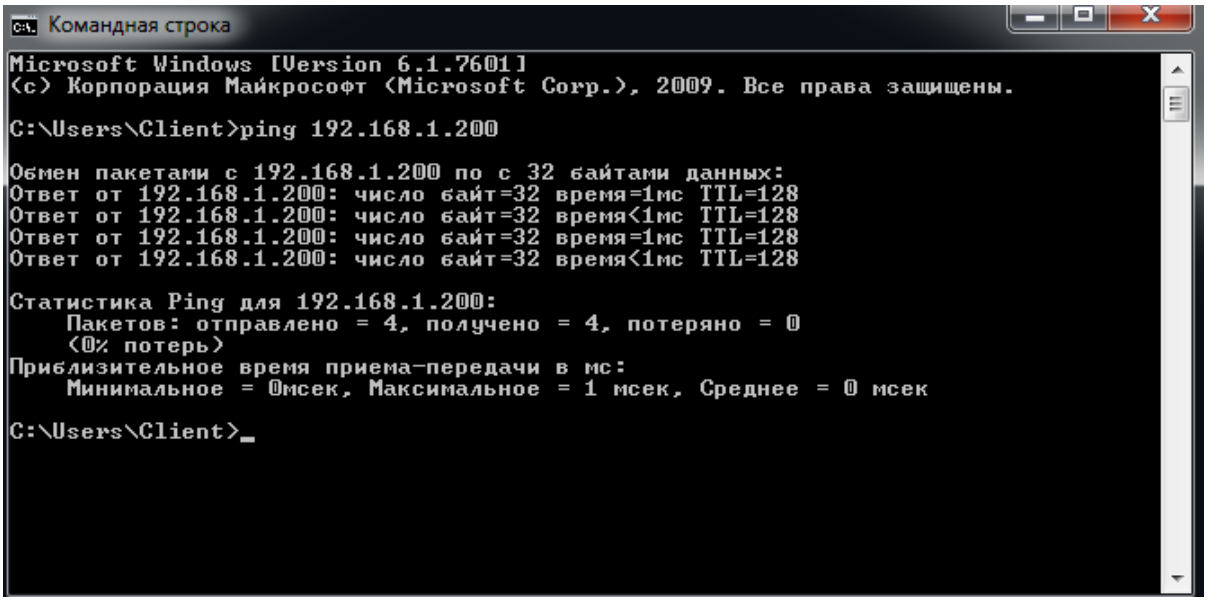


Рисунок – Успешное выполнение команды ping

При добавлении сетевого моста, нажав **кнопку «Показать дополнительные параметры»** (см. Рисунок – Добавление сетевого моста), будут доступны расширенные настройки, которые описаны в разделах Настройка RSTP/STP и Настройка SPAN настоящего руководства.

20.2 Настройка RSTP/STP

Функция RSTP/STP предназначена для устранения петель (бесконечных повторов передачи трафика) в топологии сети. Протокол автоматически блокирует соединения, являющиеся в данный момент для коммутаторов избыточными.

Для протокола RSTP/STP основными параметрами являются:

- **«Приоритет»** – используется для определения корневого коммутатора. Коммутатор с наименьшим значением параметра назначается корневым в топологии сети;
- **«Стоимость»** – используется для определения корневого порта коммутатора. Порт с наименьшим значением параметра назначается корневым. По умолчанию стоимость увеличивается с уменьшением скорости передачи порта.

Для проверки работоспособности протокола будет использоваться стенд с виртуальными машинами, представленный на рисунке (см. Рисунок – Стенд для проверки RSTP).

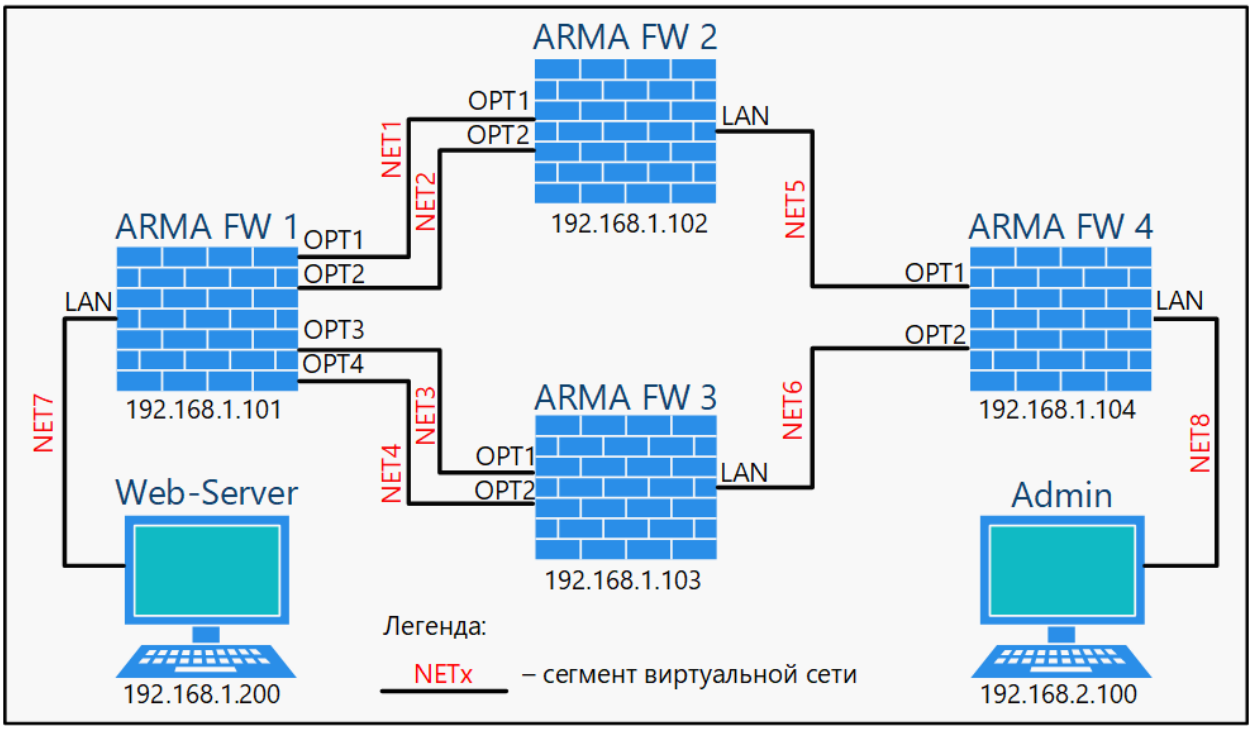


Рисунок – Стенд для проверки RSTP

Порты **«WAN»** каждой ВМ с **ARMA FW** подключены к гипервизору для возможности управления через веб-интерфейс. На ВМ **«Web-Server»** запущено приложение веб-сервера.

Для настройки протокола RSTP/STP необходимо выполнить следующие действия:

1. На каждой ВМ с **ARMA FW** включить необходимые интерфейсы.
2. На каждой ВМ с **ARMA FW** объединить включённые интерфейсы в сетевой мост с указанием параметров RSTP/STP.
3. Задать созданным сетевым мостам IP-адреса в соответствии со схемой стенда (см. Рисунок – Стенд для проверки RSTP).

Для проверки работоспособности протокола RSTP/STP будет использоваться утилита **«Wireshark»**, запущенная на ВМ **«Web-Server»**.

20.2.1 Включение интерфейсов

Для включения интерфейса требуется выполнить следующие действия:

1. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**), создать новый интерфейс (см. Назначение портов). Имя интерфейса выбирается в соответствии со схемой стенда (см. Рисунок – Стенд для проверки RSTP).
2. Перейти в раздел интерфейсов (**«Интерфейсы»**), выбрать созданный интерфейс, установить флажок **«Включить»** и, не изменяя другие параметры,

нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»** (см. Настройка сетевых интерфейсов).

3. Повторить пункты 1-2 для каждого интерфейса каждой ВМ **ARMA FW**, указанных на схеме стенда (см. Рисунок – Стенд для проверки RSTP).

20.2.2 Объединение интерфейсов в сетевой мост

Для настройки параметров RSTP/STP будут использоваться значения, указанные в таблице (см. Таблица «Параметры RSTP/STP»).

Таблица «Параметры RSTP/STP»

Параметр	ARMA FW 1	ARMA FW 2	ARMA FW 3	ARMA FW 4
Протокол	RSTP	RSTP	RSTP	RSTP
STP-интерфейсы	BRIDGE0	BRIDGE0	BRIDGE0	BRIDGE0
	LAN	LAN	LAN	LAN
	OPT1	OPT1	OPT1	OPT1
	OPT2	OPT1	OPT1	OPT1
	OPT3	OPT2	OPT2	OPT2
	OPT4	OPT2	OPT2	OPT2
Приоритет	4096	8192	12288	16384

Для объединения интерфейсов необходимо выполнить следующие действия:

1. Перейти в подраздел настройки сетевых мостов (**«Интерфейсы» - «Другие типы» - «Сетевой мост»**) и создать сетевой мост (см. Создание сетевого моста), указав в качестве интерфейсов-участников интерфейсы ВМ **ARMA FW** в соответствии со схемой стенда (см. Рисунок – Стенд для проверки RSTP). Для каждой ВМ **ARMA FW** указываются все перечисленные на схеме интерфейсы.
2. Нажать **кнопку «Показать дополнительные параметры»** и в открывшейся форме (см. Рисунок – Включение протокола RSTP/STP), в блоке **«Протокол основного дерева (RSTP/STP)»** установить флажок **«Включить»**, затем указать параметры RSTP/STP в соответствии с таблицей (см. Таблица «Параметры RSTP/STP») и нажать **кнопку «Сохранить»**.

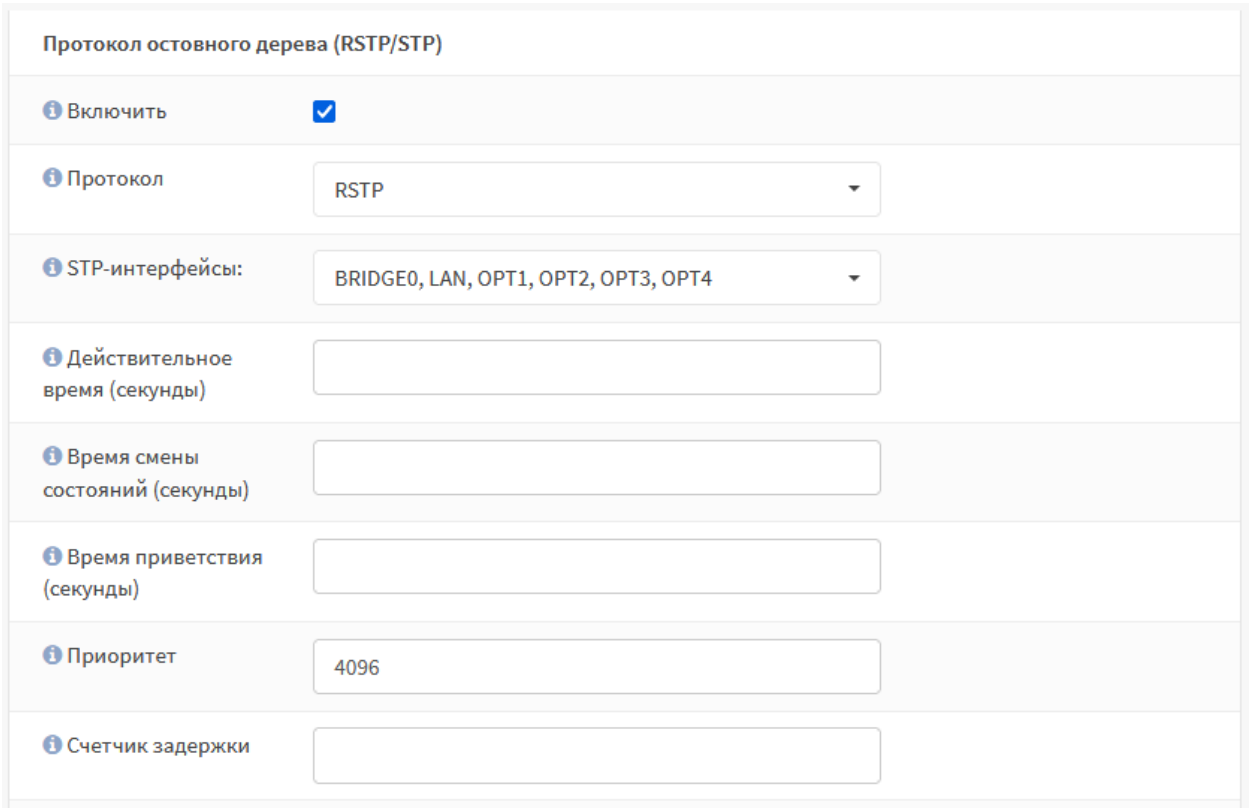


Рисунок – Включение протокола RSTP/STP

3. Для сетевого моста ВМ **«ARMA FW1»** дополнительно указать значения в полях каждого интерфейса для параметра **«Приоритет»** (см. Рисунок – Указание приоритета для сетевых интерфейсов):
   - **«LAN»** – 112;
   - **«OPT1»** – 96;
   - **«OPT2»** – 80;
   - **«OPT3»** – 48;
   - **«OPT4»** – 64.

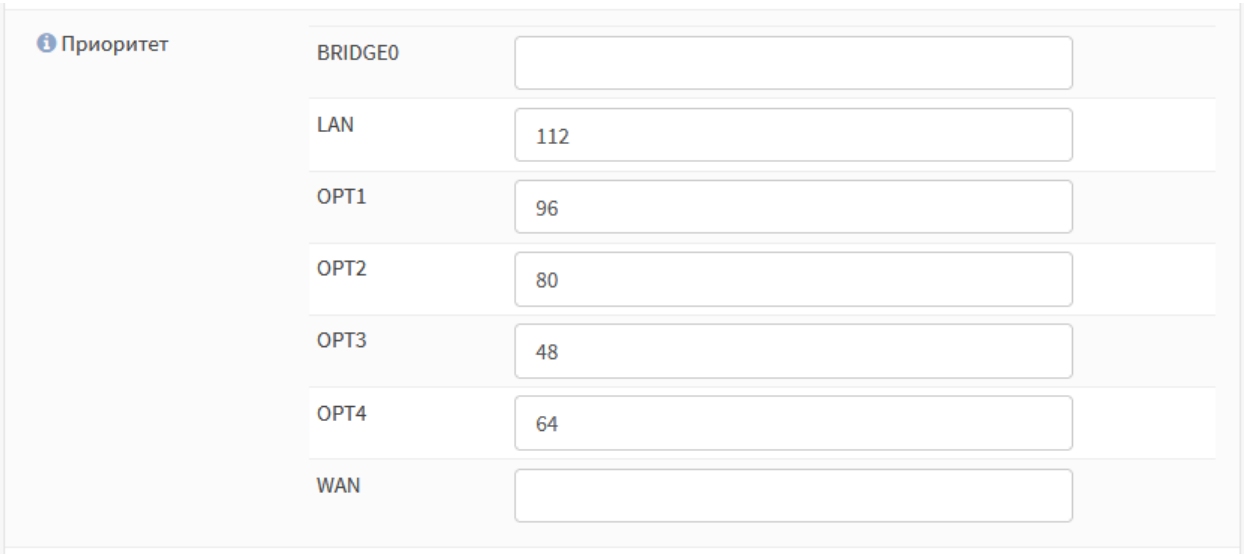


Рисунок – Указание приоритета для сетевых интерфейсов

4. Для сетевого моста ВМ **«ARMA FW4»** дополнительно указать значения в полях каждого интерфейса для параметра **«Приоритет»**:
   - **«OPT1»** – 16;
   - **«OPT2»** – 32.

20.2.3 Настройка сетевого моста

Созданные сетевые мосты необходимо настроить аналогично алгоритму, указанному в разделе Создание сетевого моста настоящего руководства.

IP-адреса для настройки представлены на схеме стенда (см. Рисунок – Стенд для проверки RSTP).

20.2.4 Проверка работы RSTP/STP

Для проверки работоспособности функции необходимо выполнить следующие действия:

1. На ВМ **«Admin»** запустить веб-браузер и перейти по адресу «192.168.1.200» (см. Рисунок – Доступ к веб-серверу с ПК администратора) – это позволит проверить правильность настройки стенда.

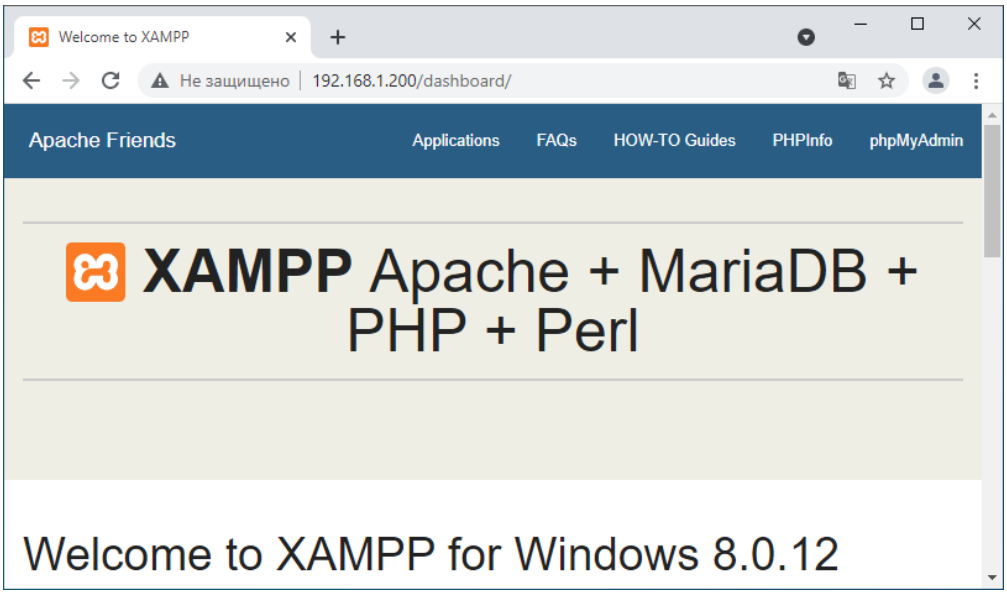


Рисунок – Доступ к веб-серверу с ПК администратора

2. На ВМ **«Web-Server»** запустить программу «Wireshark» и выполнить захват трафика на сетевом интерфейсе (см. Рисунок – Трафик с STP-пакетами). В списке захваченных пакетов будет присутствовать STP-трафик.

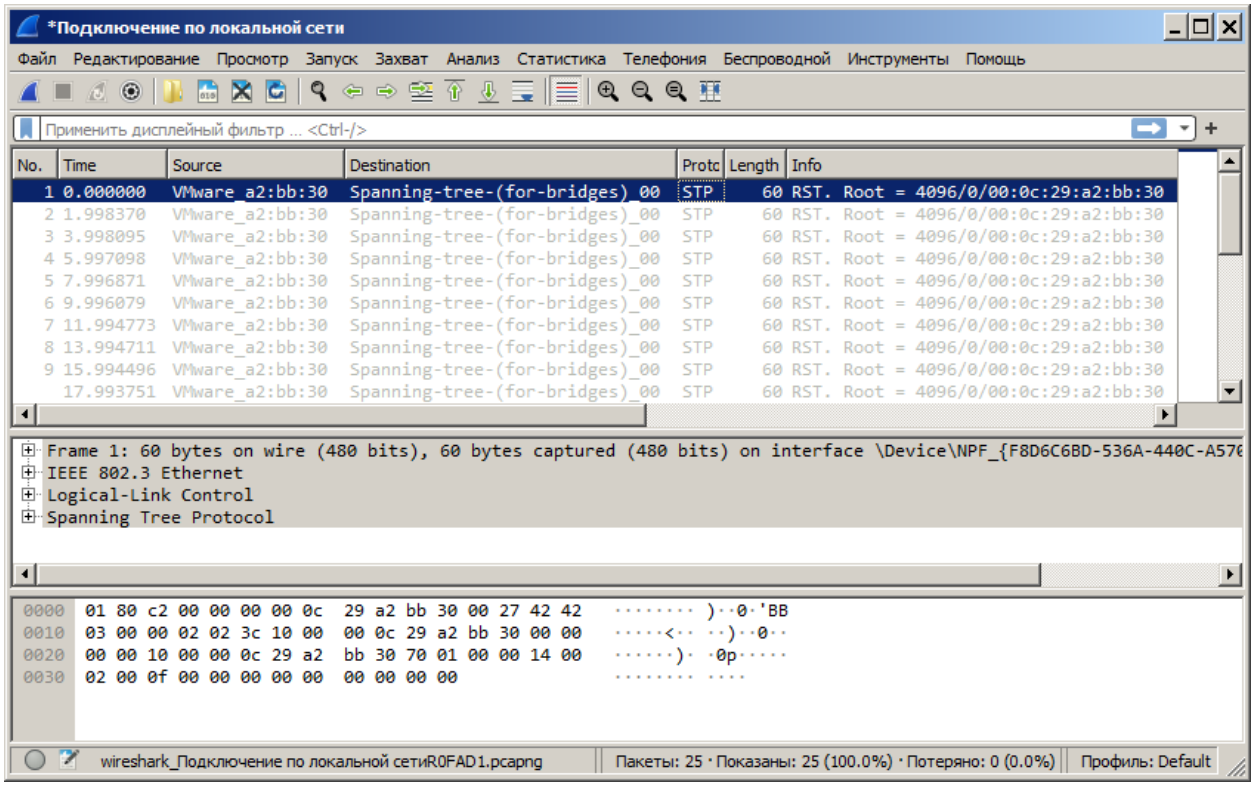


Рисунок – Трафик с STP-пакетами

3. На ВМ **«ARMA FW1»** перейти в настройки сетевого моста (**«Интерфейсы» - «Другие типы» - «Сетевой мост»**), нажать **кнопку «Дополнительные настройки»** и отключить функцию RSTP/STP, убрав соответствующий флажок.

4. На ВМ **«Web-Server»** запустить программу «Wireshark» и выполнить захват трафика на сетевом интерфейсе (см. Рисунок – Трафик широковещательной рассылки). В списке захваченных пакетов будет присутствовать постоянно растущий трафик широковещательной рассылки, указывающий на присутствие петли в топологии сети.

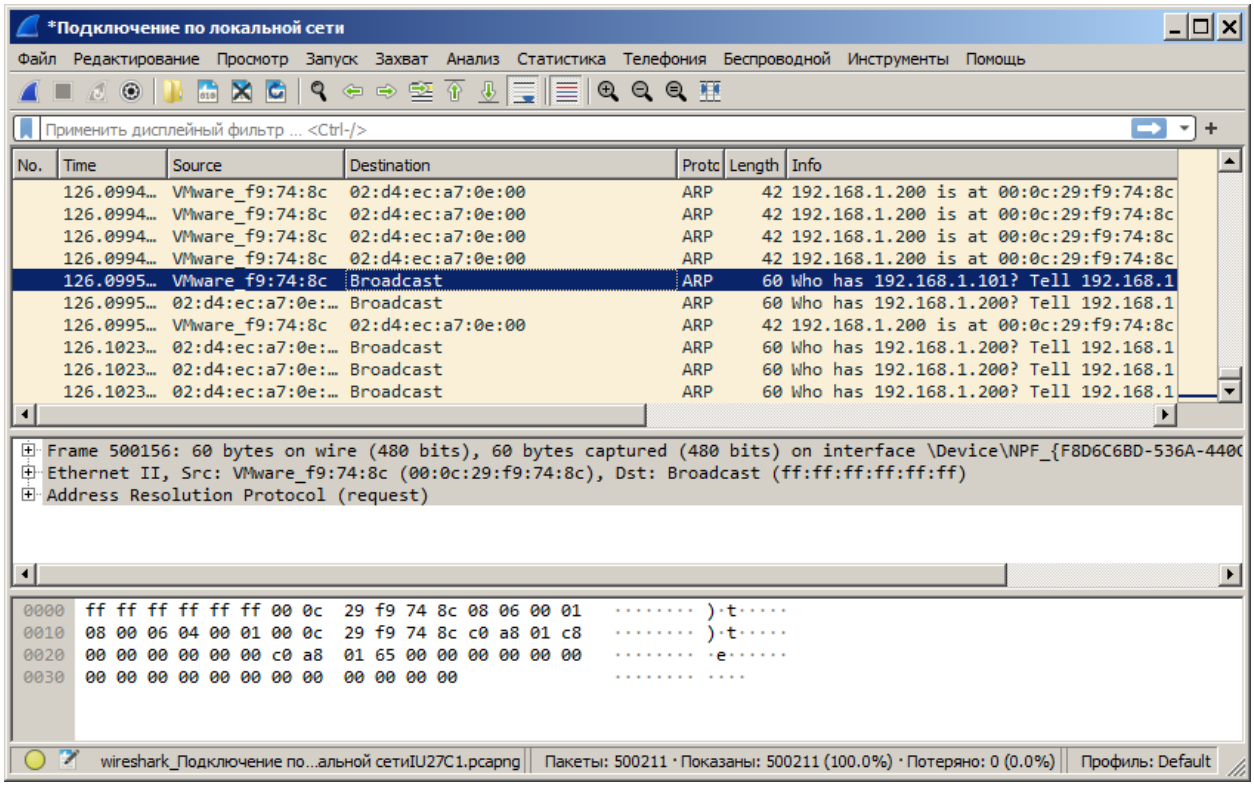


Рисунок – Трафик широковещательной рассылки

20.3 Настройка SPAN

Функция SPAN предназначена для зеркалирования трафика, проходящего через сетевой мост. Функция используется для анализа трафика и должна поддерживаться принимающим устройством, например, коммутатором.

В качестве примера настройки зеркалирования трафика будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Стенд для настройки зеркалирования трафика), со следующими параметрами:

- интерфейсы «OPT1» и «LAN» объединены в сетевой мост;
- интерфейс «OPT2» используется в качестве порта SPAN.

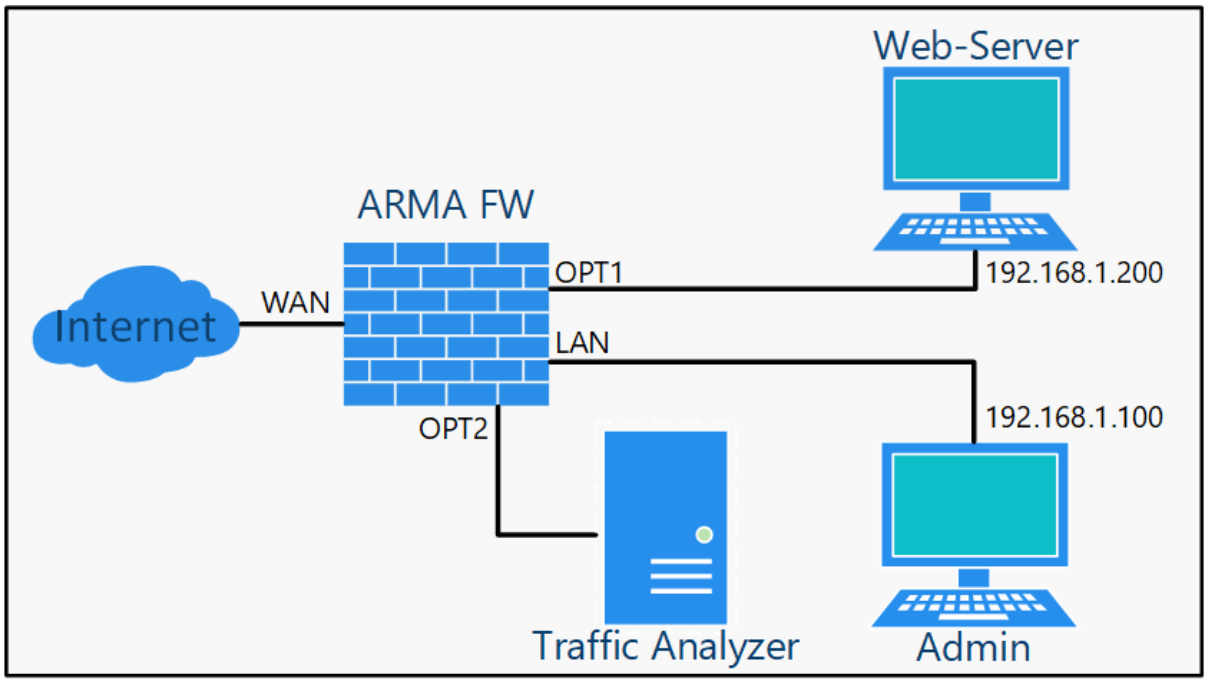


Рисунок – Стенд для настройки зеркалирования трафика

Для настройки зеркалирования необходимо выполнить следующие действия:

1. Включить интерфейс «OPT2».
2. Объединить интерфейсы «OPT1» и «LAN» в сетевой мост с указанием порта SPAN.
3. Настроить созданный сетевой мост.

Для проверки наличия трафика на интерфейсе «OPT2» будет использоваться утилита «Wireshark», запущенная на ПК **«Traffic Analyser»**.

20.3.1 Включение интерфейса «OPT2»

Для включения интерфейса необходимо выполнить следующие действия:

1. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**) и создать новый интерфейс с именем «OPT2» (см. Назначение портов).
2. В разделе интерфейсов (**«Интерфейсы»**) выбрать созданный интерфейс, установить флажки для параметров **«Включить»** и **«Блокировать трафик на SPAN порту»**, не изменяя другие параметры нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»** (см. Настройка сетевых интерфейсов).

20.3.2 Объединение интерфейсов «OPT1» и «LAN» в сетевой мост

Для объединения интерфейсов необходимо выполнить следующие действия:

1. Перейти в подраздел настройки сетевых мостов (**«Интерфейсы» - «Другие типы» - «Сетевой мост»**) и создать сетевой мост (см. Создание сетевого моста), указав в качестве интерфейсов-участников порты «OPT1» и «LAN».
2. Нажать **кнопку «Показать дополнительные параметры»** и в открывшейся форме указать «OPT2» в параметре **«Порт SPAN»** (см. Рисунок – Выбор порта SPAN), затем нажать **кнопку «Сохранить»**.

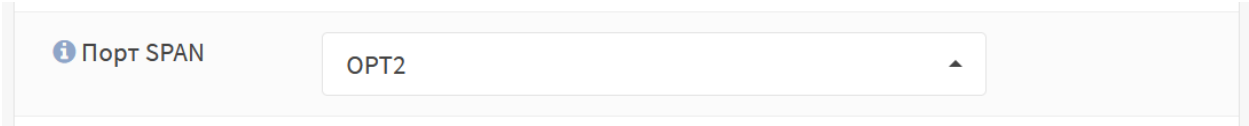


Рисунок – Выбор порта SPAN

Для корректной работы режима SPAN необходимо изменить значения следующих параметров (**«Система» - «Настройки» - «Параметры»**):

- **«net.link.bridge.pfil_member»** – «0»;
- **«net.link.bridge.pfil_bridge»** – «0».

Данные значения параметров отключают фильтрацию со стороны **ARMA FW** для коммутируемых кадров.

Для изменения параметров необходимо выполнить следующие действия:

1. Перейти в подраздел параметров **ARMA FW** (**«Система» - «Настройки» - «Параметры»**).
2. Нажать **кнопку** « » напротив изменяемого параметра и задать значение в поле **«Значение»**.
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.

20.3.3 Настройка сетевого моста

Созданный сетевой мост необходимо настроить аналогично алгоритму, указанному в разделе Создание сетевого моста настоящего руководства.

В результате настройки весь трафик, проходящий по созданному сетевому мосту, будет зеркалироваться на интерфейс «OPT2».

Настройка принимающего трафик устройства должна производиться согласно соответствующей инструкции и не описана в настоящем руководстве.

20.3.4 Проверка зеркалирования трафика

Для проверки зеркалирования трафика необходимо выполнить следующие действия:

1. На ПК **«Admin»** запустить веб-браузер и перейти по адресу «192.168.1.200» (см. Рисунок – Доступ к веб-серверу с ПК администратора).

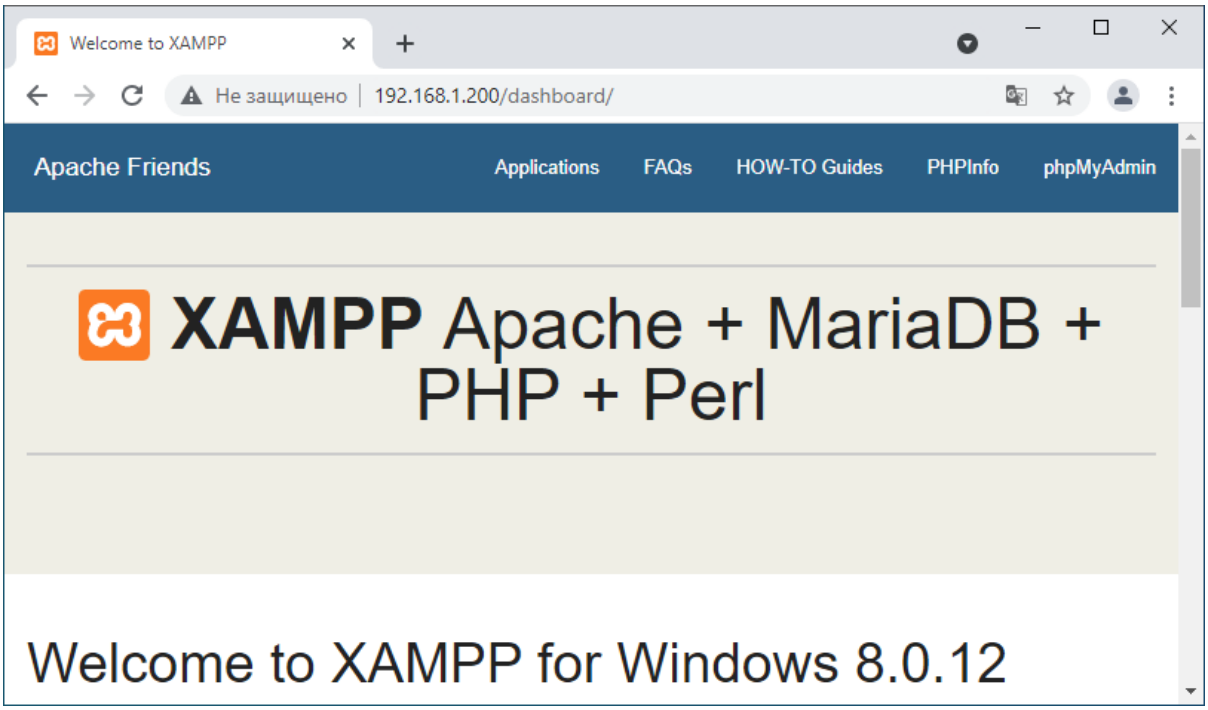


Рисунок – Доступ к веб-серверу с ПК администратора

2. На ПК **«Traffic Analyzer»** запустить программу «Wireshark» и выполнить анализ трафика с фильтром по IP (см. Рисунок – Зеркалированный трафик на интерфейсе «OPT2»).

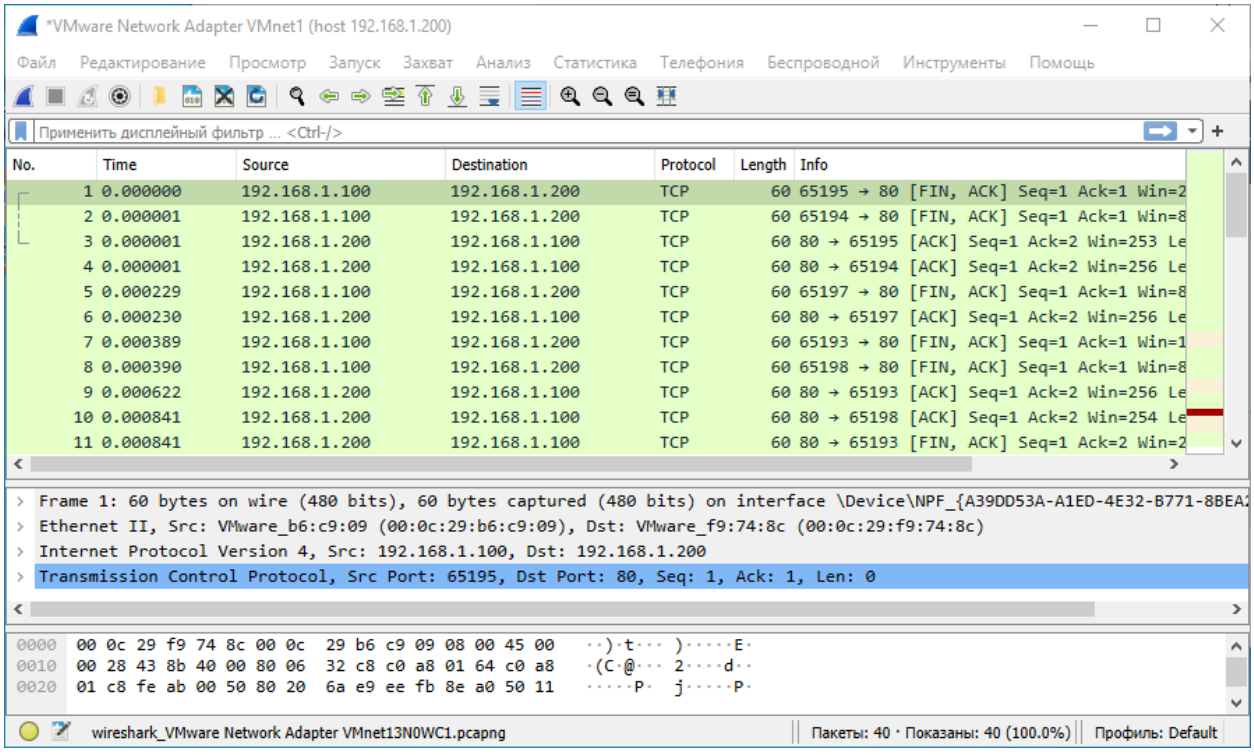


Рисунок – Зеркалированный трафик на интерфейсе «OPT2»

20.3.5 Особенности настройки ARMA FW для обработки СОВ зеркалированного трафика

В качестве примера приведён порядок настройки **ARMA FW** с предварительно подключённым интерфейсом «OPT2» к порту SPAN коммутатора.

Для корректной работы **ARMA FW** при обработке СОВ зеркалированного трафика необходимо выполнить следующие действия:

1. Перейти в подраздел настроек интерфейса «OPT2» (**«Интерфейсы» - «[OPT2]»**) и убедиться, что в полях для параметров **«Тип конфигурации IPv4»** и **«Тип конфигурации IPv6»** установлено значение «Отсутствует».

   Примечание:

   Для обработки СОВ трафика, поступающего из VLAN сети, необходимо отключить фильтрацию аппаратного обеспечения, указав интерфейс «OPT2» в дополнительно появившемся поле (см. Расширенные настройки).

2. Перейти в подраздел общих правил МЭ (**«Межсетевой экран» - «Правила» - «[Общие]»**) и создать правило, указав следующие параметры:

   - **«Действие»** – «Блокирование (Drop)»;
   - **«Интерфейс»** – «OPT2»;
   - **«Направление»** – «Любое».

   Не указанные параметры следует оставить по умолчанию. Создание правил МЭ описано в разделе Создание правил межсетевого экранирования настоящего руководства.

3. Перейти в подраздел администрирования СОВ (**«Обнаружение вторжений» – «Администрирование»**) и во вкладке **«Настройки»** ввести следующие параметры:

   - **«Включен»** – флажок установлен;
   - **«Смешанный режим»** – флажок установлен;
   - **«Интерфейсы»** – «OPT2».

   Настроить необходимые правила фильтрации трафика. Настройка правил СОВ описана в разделе Система обнаружения и предотвращения вторжений настоящего руководства.

Для проверки успешности подключения следует убедиться в присутствии трафика на интерфейсе «OPT2».

21 RSPAN

Функция RSPAN предназначена для дублирования пакетов порта удалённого коммутатора на порту другого коммутатора. Устройства, используемые по маршруту для передачи зеркалированного трафика, должны поддерживать RSPAN.

21.1 Пример настройки RSPAN

В качестве примера настройки RSPAN используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки RSPAN).

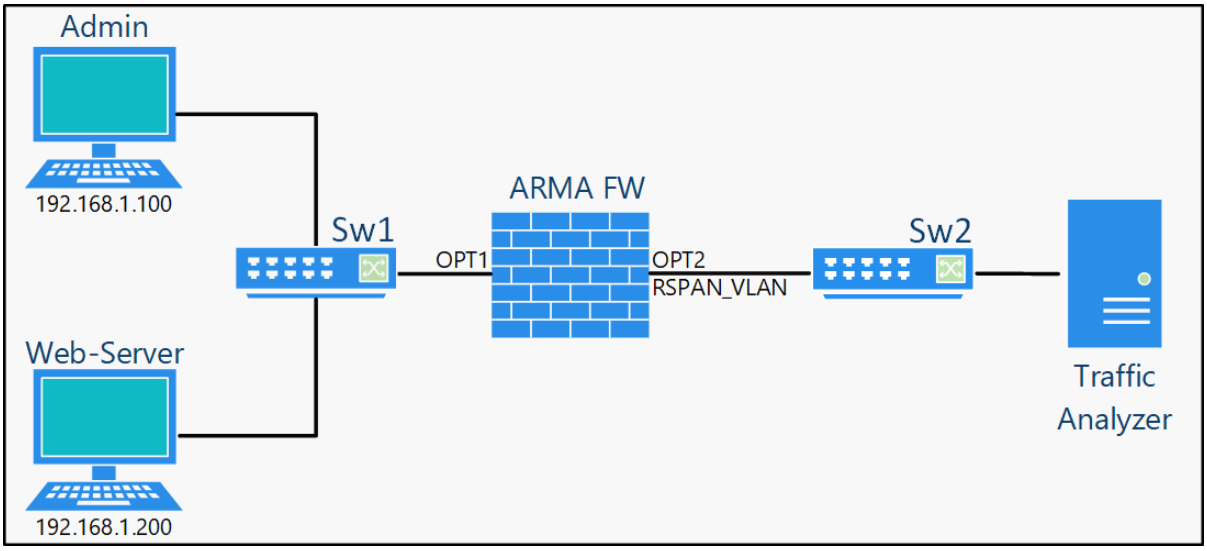


Рисунок – Схема стенда для настройки RSPAN

Для настройки RSPAN необходимо выполнить следующие действия:

1. Перейти в подраздел настройки интерфейса «OPT1» (**«Интерфейсы» - «[OPT1]»**), установить флажки для параметров **«Включить»** и **«Блокировать трафик на SPAN порту»**, выбрать значение «Отсутствует» для параметров **«Тип конфигурации IPv4»** и **«Тип конфигурации IPv6»**, не изменяя другие параметры нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»** (см. Настройка сетевых интерфейсов).
2. Перейти в подраздел настройки VLAN (**«Интерфейсы» - «Другие типы» - «VLAN»**), нажать **кнопку «+Добавить»** и указать следующие значения параметров:
   - **«Родительский интерфейс»** – «[OPT2]»;
   - **«Тег VLAN»** – «100»;
   - **«Описание»** – «RSPAN_VLAN».

   и нажать **кнопку «Сохранить»**.
3. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**), выбрать значение «виртуальная локальная сеть 100 на

em3(RSPAN_VLAN)» в поле параметра **«Новый интерфейс»**, ввести «RSPAN_VLAN100» в поле параметра **«Описание»** и нажать **кнопку** «+» для создания интерфейса.

4. Перейти в подраздел настройки интерфейса «RSPAN_VLAN100» (**«Интерфейсы» - «[RSPAN_VLAN100]»**), установить флажок для параметра **«Включить»** и, не изменяя другие параметры нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить изменения»**.
5. Создать разрешающее правило МЭ (см. Создание правил межсетевого экранирования) на интерфейсе «[RSPAN_VLAN100]», указав следующие параметры:
   - **«Действие»** – «Разрешить (Pass)»;
   - **«Интерфейс»** – «RSPAN_VLAN100»;
   - **«Направление»** – «любой»;
   - **«Описание»** – «Allow RSPAN».
6. Перейти во вкладку **«Общие настройки»** подраздела общих настроек RSPAN (**«Службы» - «RSPAN» - «Общие настройки»**), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»** (см. Рисунок – Включение RSPAN).

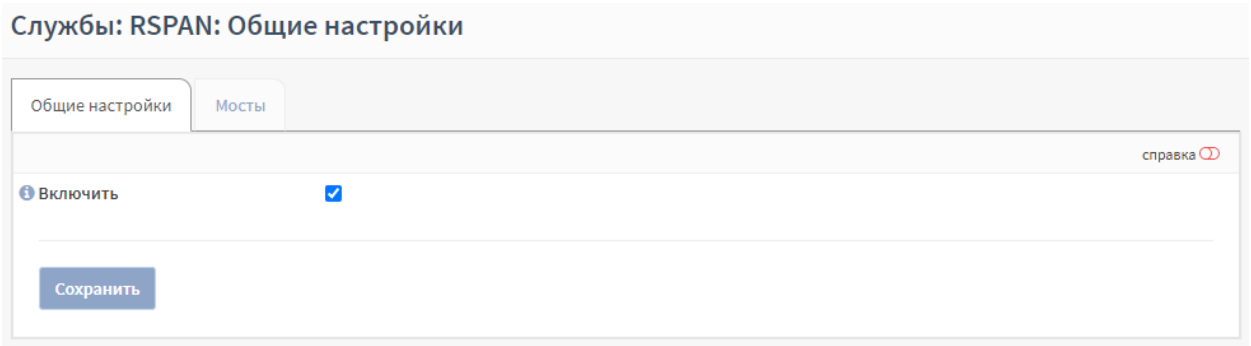


Рисунок – Включение RSPAN

7. Перейти во вкладку **«Мосты»** подраздела общих настроек RSPAN (**«Службы» - «RSPAN» - «Общие настройки»**), нажать **кнопку** «+», указать следующие значения параметров:
   - **«Имя»** – «RSPAN»;
   - **«Порты»** – «OPT1», «RSPAN_VLAN»;
   - **«Зеркала»** – «RSPAN_VLAN».

   и нажать **кнопку «Сохранить»** (см. Рисунок – Настройка моста RSPAN).

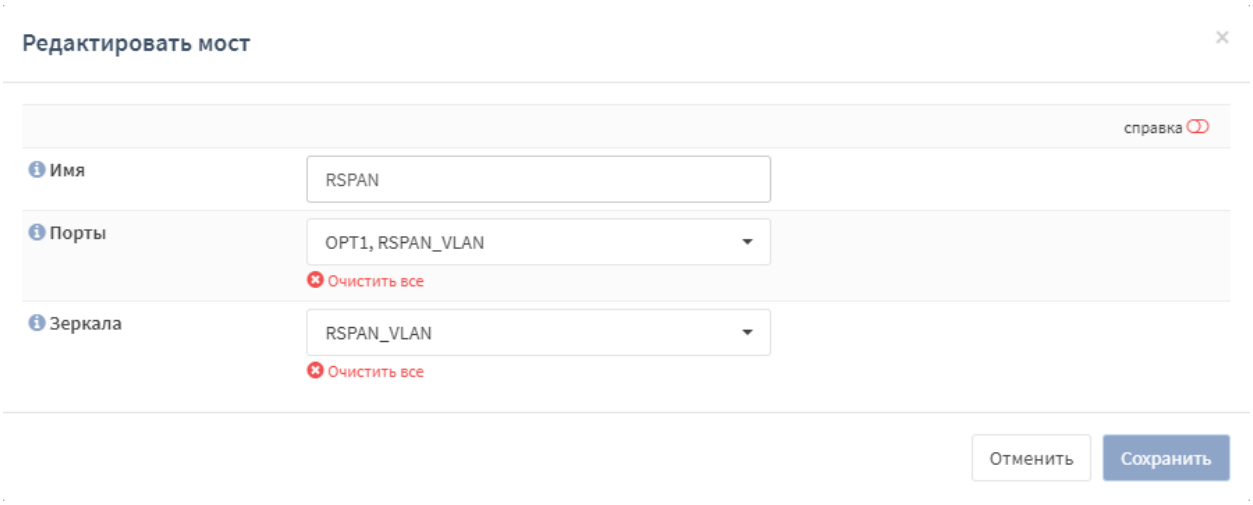


Рисунок – Настройка моста RSPAN

8. Нажать **кнопку** « Перезагрузка службы » (см. Рисунок – Перезагрузка RSPAN).

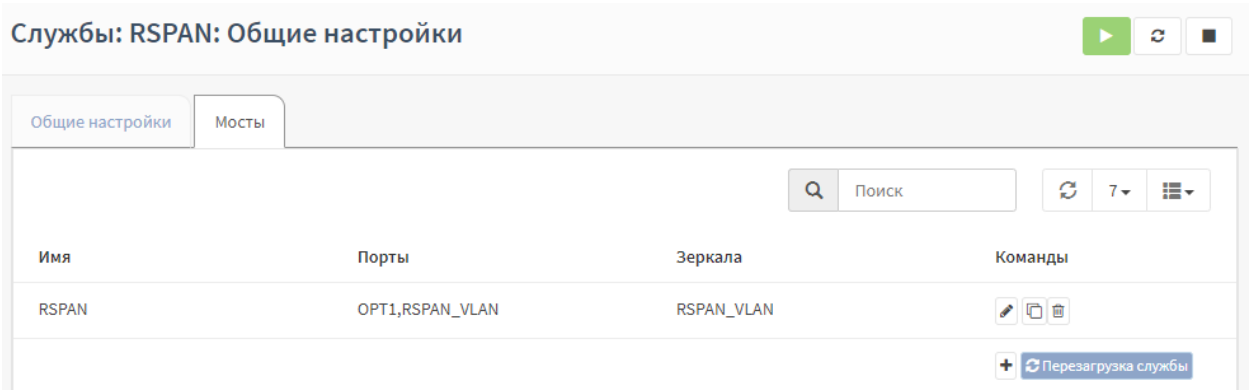


Рисунок – Перезагрузка RSPAN

21.2 Проверка RSPAN

Для проверки зеркалирования трафика необходимо выполнить следующие действия:

1. На ПК **«Admin»** запустить веб-браузер и перейти по адресу «192.168.1.200».
2. На ПК **«Traffic Analyzer»** запустить программу «Wireshark» и выполнить анализ трафика с фильтром по IP.

22 VLAN

VLAN – это технология, позволяющая строить виртуальные сети с независимой от физических устройств топологией.

ARMA FW поддерживает технологию VLAN по стандарту IEEE 802.1Q.

> **Примечание:**
>
> При использовании технологии VLAN коммутатор должен поддерживать стандарт IEEE 802.1Q и настроен соответствующим образом.

Для настройки и проверки работоспособности технологии VLAN используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки VLAN).

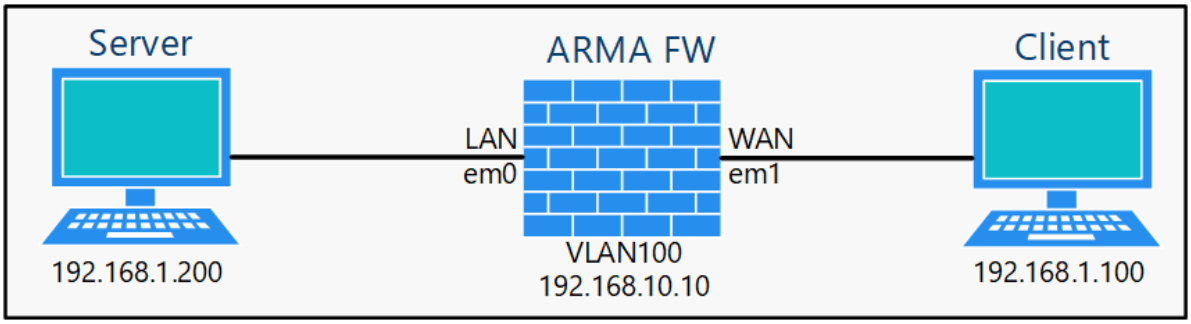


Рисунок – Схема стенда для настройки VLAN

22.1 Создание VLAN

Для создания интерфейса VLAN необходимо выполнить следующие действия:

1. Перейти в подраздел настройки VLAN (**«Интерфейсы» - «Другие типы» - «VLAN»**) и нажать **кнопку «+Добавить»**.
2. В параметре **«Родительский интерфейс»** выбрать сетевой интерфейс «em1», установить значение уникального идентификатора равным «100» в поле параметра **«Тег VLAN»**, оставить по умолчанию значение параметра **«Приоритет VLAN»** и нажать **кнопку «Сохранить»** (см. Рисунок – Создание интерфейса VLAN).

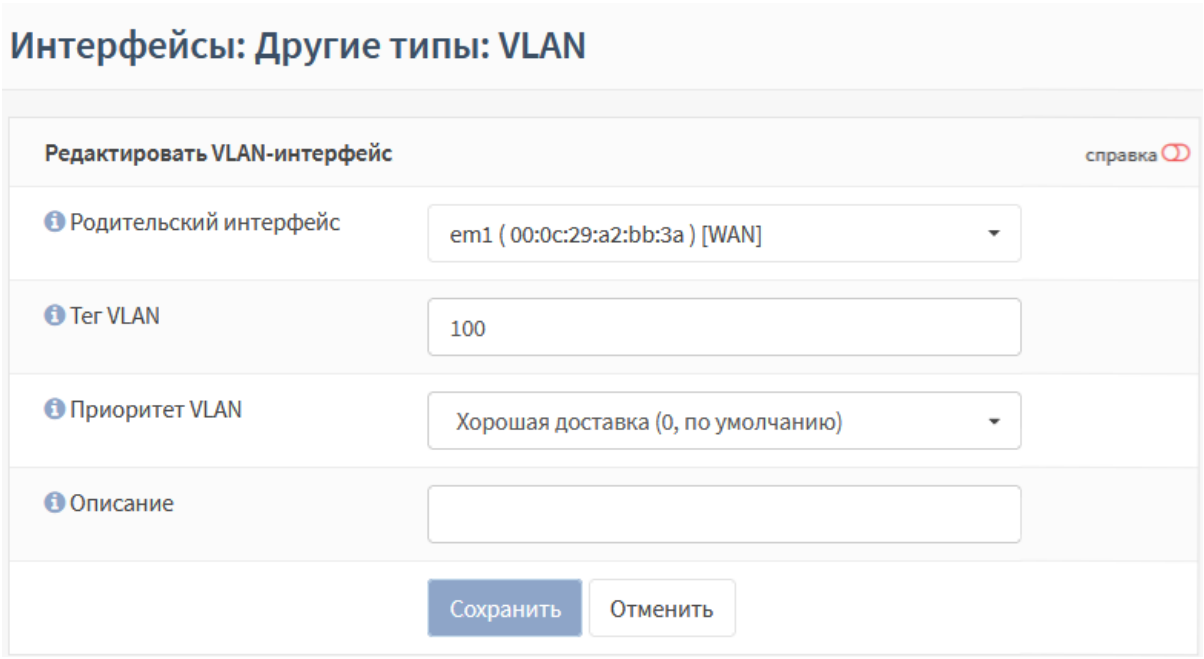


Рисунок – Создание интерфейса VLAN

3. Перейти в подраздел назначения портов (**«Интерфейсы» - «Назначения портов»**), выбрать значение «виртуальная локальная сеть 100 на em1()» в параметре **«Новый интерфейс»**, ввести «VLAN100» в поле параметра **«Описание»** и нажать **кнопку** « + » для создания интерфейса (см. Назначение портов).
4. Перейти в настройки созданного сетевого интерфейса (**«Интерфейсы» - «VLAN100»**) и задать настройки согласно таблице (см. Таблица «Параметры интерфейса»).

Таблица «Параметры интерфейса»

Параметр	Значение
Включить	Значение установлено
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
IPv4-адрес	192.168.10.10/24

5. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

22.2 Проверка работы созданного VLAN

Для проверки работоспособности настроенного интерфейса «VLAN100» необходимо выполнить следующие действия:

1. Перейти в подраздел диагностики захватом пакетов (**«Интерфейсы» - «Диагностика» - «Захват пакетов»**).

2. Изменить следующие параметры:
   - **«Интерфейс»** – «WAN»;
   - **«Смешанный режим»** – флажок установлен;
   - **«Количество»** – «0», для отключения предела захваченных пакетов;

   остальные параметры оставить без изменения и нажать **кнопку «Запустить»**.
3. На ПК **«Server»** выполнить команду «ping» до IP-адреса «192.168.10.100» – результат будет неуспешным.
4. Остановить захват пакетов, нажав **кнопку «Остановить»** в подразделе диагностики захватом пакетов (**«Интерфейсы» - «Диагностика» - «Захват пакетов»**) и скачать захваченные пакеты (см. Рисунок – Остановка захвата пакетов).
5. Скачать захваченные пакеты, нажав **левой кнопкой мыши** на имя файла внизу подраздела (см. Рисунок – Остановка захвата пакетов) и следуя указаниям веб-браузера.

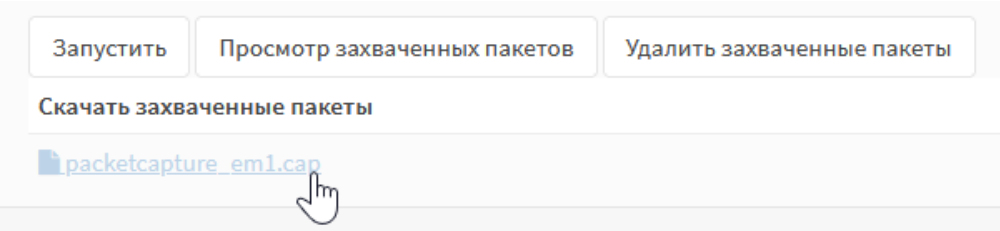


Рисунок – Остановка захвата пакетов

6. В ПО «Wireshark» открыть скачанный файл, в поле фильтра ввести – «vlan» и нажать **клавишу «Enter»**. В списке захваченных пакетов будут присутствовать пакеты с полем «802.1Q Virtual LAN, ID: 100».

22.3 VXLAN

VXLAN – это технология сетевой виртуализации, позволяющая наложения виртуализированных сетей 2 уровня на сети 3 уровня согласно rfc7348.

VXLAN имеет режимы работы «Unicast» и «Multicast».

Настроенные интерфейсы VXLAN отображены в подразделе настройки VXLAN (**«Интерфейсы» - «Другие типы» - «VXLAN»**) (см. Рисунок – Перечень VXLAN).

В подразделе доступны следующие команды:

- **кнопка** « + » – открывает форму «Редактировать VXLAN» (см. Рисунок – Форма редактирования VXLAN) для создания нового VXLAN;

- **кнопка** « » – открывает форму «Редактировать VXLAN» (см. Рисунок – Форма редактирования VXLAN) для редактированного ранее созданного VXLAN;
- **кнопка** « » – удаляет ранее созданный VXLAN;
- **кнопка** « » – открывает форму «Редактировать VXLAN» (см. Рисунок – Форма редактирования VXLAN) для создания нового VXLAN путём копирования раннее созданного.

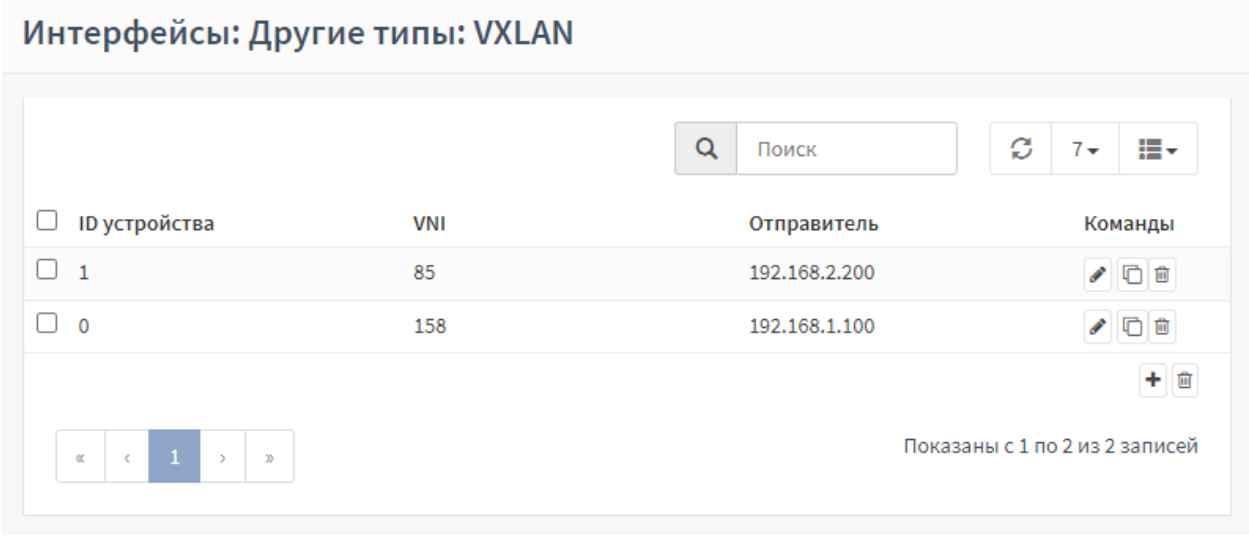


Рисунок – Перечень VXLAN

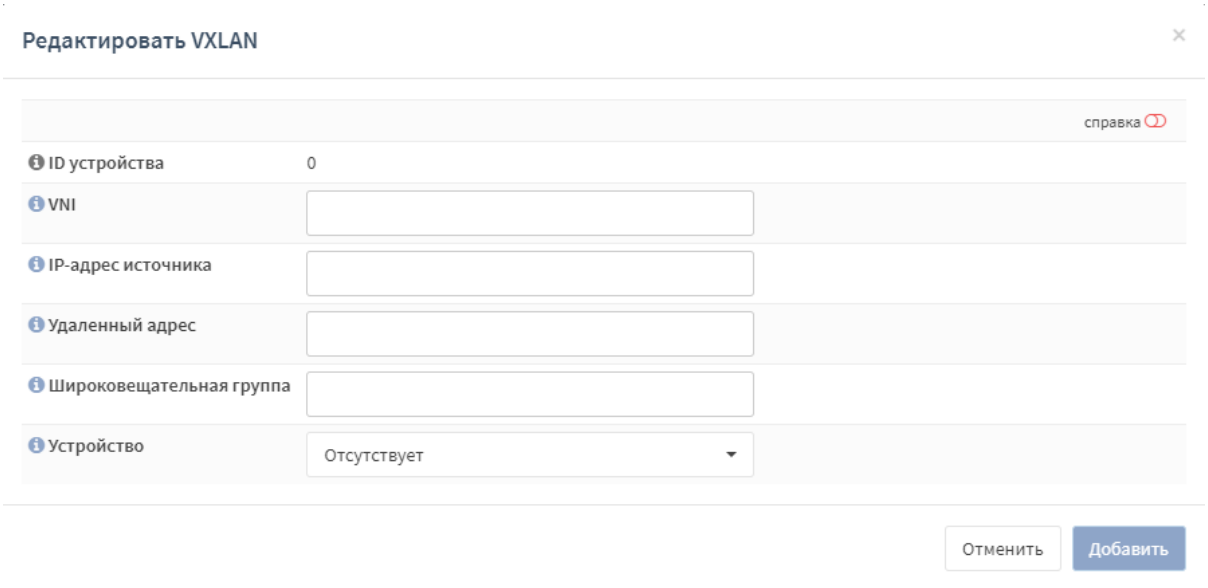


Рисунок – Форма редактирования VXLAN

23 ПРОКСИ

Прокси-сервер обеспечивает контролируемый доступ хостов локальной сети в сеть Интернет, а также защиту локальной сети от внешнего доступа.

В качестве примера настройки прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки прокси-сервера) со следующими параметрами прокси-сервера:

- интерфейс хостов локальной сети – «LAN», сеть 192.168.1.0/24;
- работа в прозрачном режиме для HTTP и HTTPS;
- кэширование данных включено;
- работает без аутентификации;
- номер порта для HTTP – «3128», номера порта для HTTPS – «3129»;
- ограничение доступа к ресурсам настроено для сайта «mail.ru» и согласно внешнему списку доступа «Blacklists UT1».

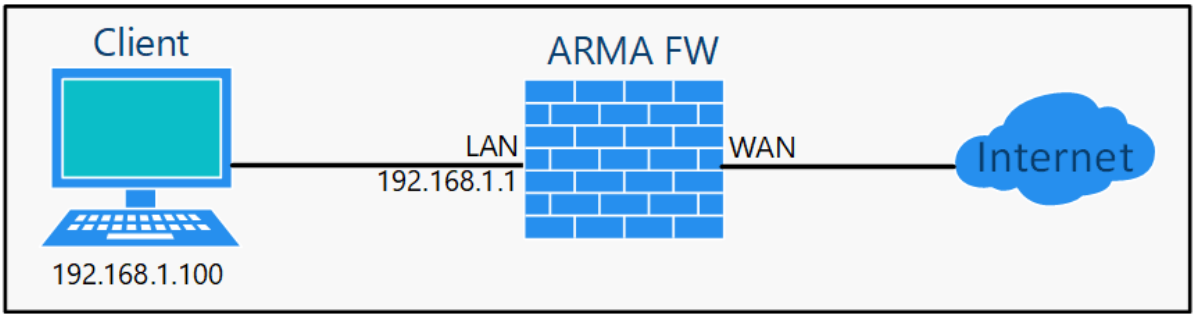


Рисунок – Схема стенда для настройки прокси-сервера

До момента настройки прокси-сервера подключение на ПК **«Client»** к сети Интернет отсутствует (см. Рисунок – Отсутствие подключения к сети Интернет).

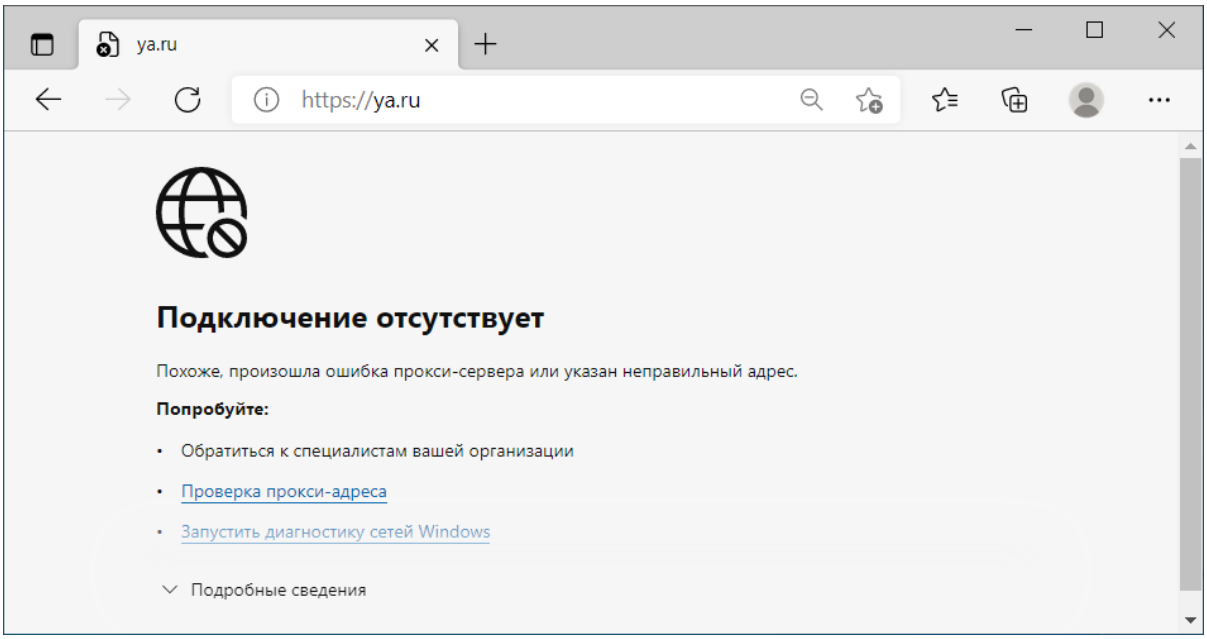


Рисунок – Отсутствие подключения к сети Интернет

23.1 Настройка кэширующего прокси-сервера

Для настройки кэширующего прокси-сервера необходимо выполнить следующие шаги:

1. Создать доверенный центр сертификации.
2. Настроить прокси-сервер.
3. Создать правила NAT для прокси-сервера.

23.1.1 Создание доверенного центра сертификации

Для корректной работы прокси-сервера с HTTPS-трафиком необходимо создать доверенный центр сертификации и добавить данный центр клиентам прокси-сервера.

В примере доверенный центр сертификации создается с параметрами, приведёнными в таблице (см. Таблица «Значения параметров центра сертификации»).

Таблица «Значения параметров центра сертификации»

Параметр	Значение
Описательное имя	ARMA CA
Метод	Создать внутренний центр сертификации
Длина ключа (бит)	2048
Алгоритм дайджеста	SHA256
Время существования (дни)	365

Параметр	Значение
Код страны	RU (Russia)
Область	MO
Город	Moscow
Организация	InfoWatch
Эл. почта	admin@infowatch.ru
Стандартное имя	arma-ca

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Эл. почта»**, **«Стандартное имя»** указаны справочно.

Для создания доверенного центра сертификации необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица «Значения параметров центра сертификации»).
4. Нажать **кнопку «Сохранить»**.

Для добавления доверенного центра сертификации клиентам прокси-сервера необходимо предварительно экспортировать сертификат созданного центра сертификации, нажав **кнопку «Экспортировать сертификат CA»** (см. Рисунок – Экспорт сертификата CA) в подразделе полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).

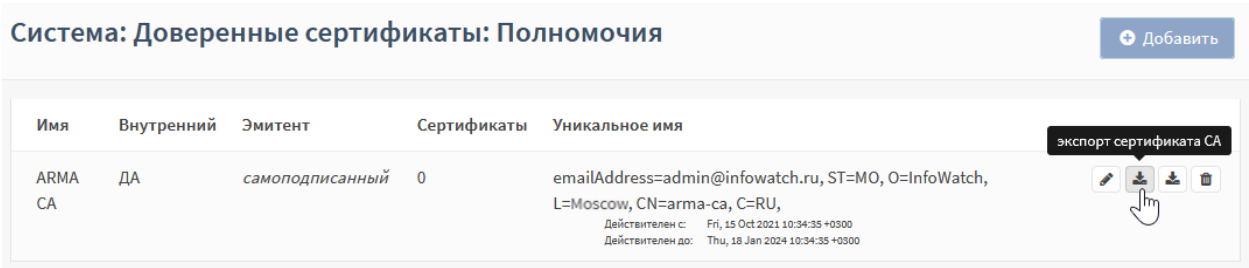


Рисунок – Экспорт сертификата CA

Установка сертификата клиентам прокси-сервера предполагается произвольным способом в зависимости от используемого оборудования – через групповые политики, с помощью браузера и т.д.

Примечание:

При использовании импортированного центра сертификации необходимо руководствоваться стандартом X.509, при этом длина серийного номера импортируемого центра сертификации не должна превышать 20 байт.

23.1.2 Настройка прокси-сервера

Для настройки прокси-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел администрирования прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**).
2. Установить флажок в параметре **«Включить прокси»** на вкладке **«Основные настройки»** (см. Рисунок – Основные настройки прокси) и нажать **кнопку «Применить»**.

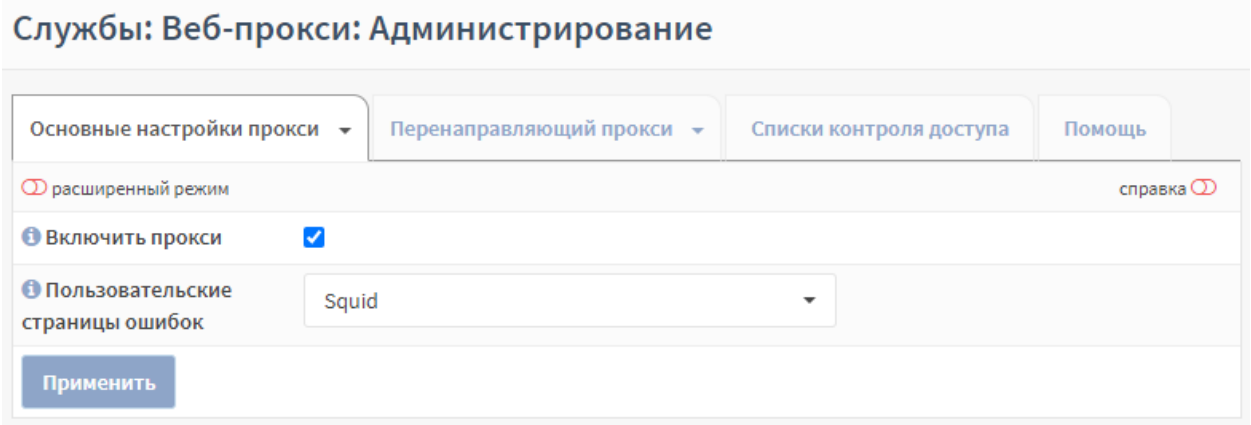


Рисунок – Основные настройки прокси

3. Раскрыть вкладку **«Основные настройки прокси»**, нажав **кнопку** « ▼ », и выбрать **«Настройки локального кэша»** (см. Рисунок – Выбор настроек прокси-сервера).

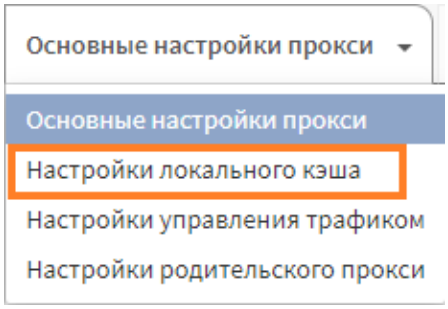


Рисунок – Выбор настроек прокси-сервера

4. В открывшейся форме (см. Рисунок – Настройки локального кэша) установить флажок для параметра **«Включите локальный кэш»** и нажать **кнопку «Применить»**.

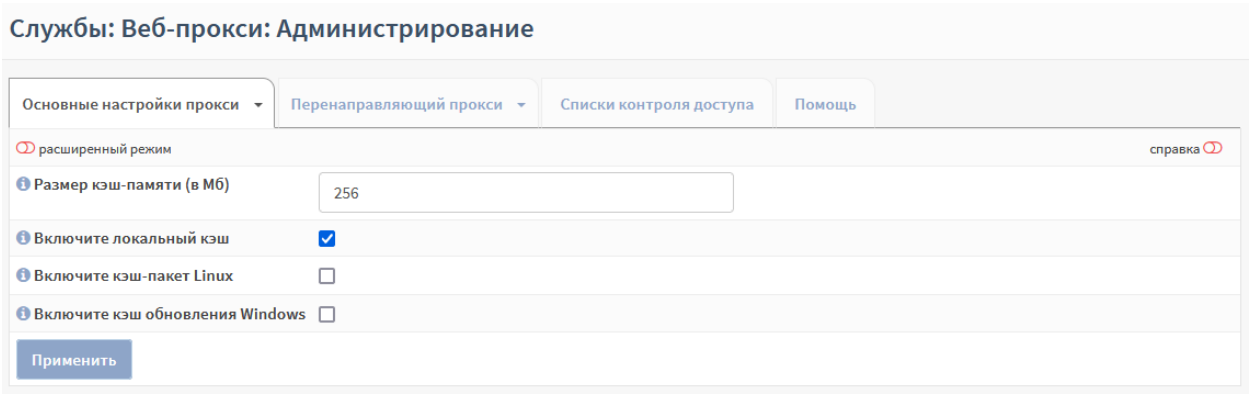


Рисунок – Настройки локального кэша

5. Перейти во вкладку **«Перенаправляющий прокси»** (см. Рисунок – Перенаправляющий прокси).

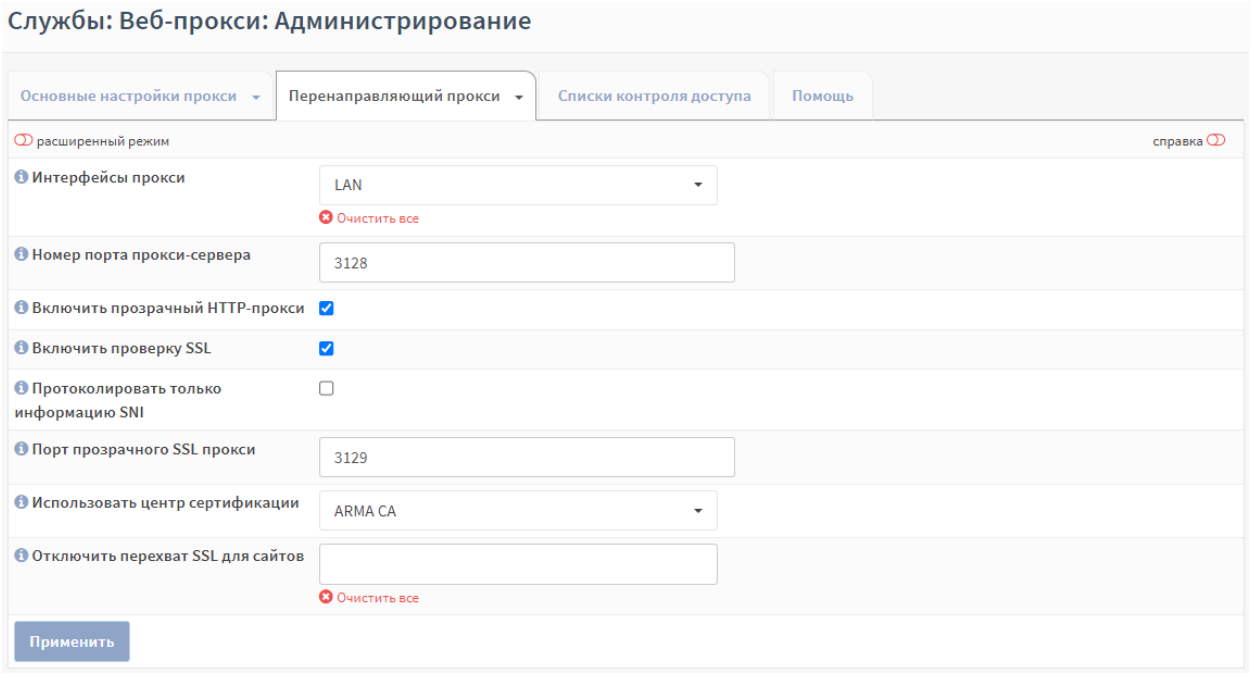


Рисунок – Перенаправляющий прокси

6. Проверить значение параметра **«Интерфейсы прокси»** – «LAN», выбрать значение «ARMA CA» в параметре **«Использовать центр сертификации»** и установить флажки для параметров:
   - **«Включить прозрачный HTTP-прокси»**;
   - **«Включить проверку SSL»**.
7. Нажать **кнопку «Применить»**.

Примечание:

В случае использования непрозрачного режима прокси-сервера при ручной настройке клиентов (см. Рисунок – Параметры прокси-сервера) необходимо указывать один порт для всех протоколов.

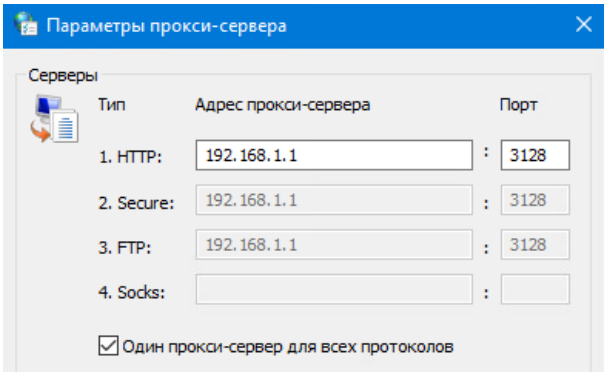


Рисунок – Параметры прокси-сервера

23.1.3 Создание правил NAT для прокси-сервера

Для работы прозрачного режима HTTP-прокси и HTTPS-прокси необходимо добавить правила NAT.

> **Примечание:**
>
> В случае использования непрозрачного прокси-сервера совместно с порталом авторизации (см. Портал авторизации) правила NAT необходимо отключать.

Создание правил NAT описано в разделе Создание правила NAT «Переадресация портов» настоящего руководства.

Необходимо создать правила с параметрами, указанными в таблице (см. Таблица «Значения параметров правил NAT»).

Таблица «Значения параметров правил NAT»

Параметр	HTTP	HTTPS
Интерфейс	LAN	LAN
Протокол	TCP	TCP
Отправитель	LAN сеть	LAN сеть
Диапазон портов источника	Любой-Любой	Любой-Любой
IP-адрес назначения	Любой	Любой
Диапазон портов назначения	HTTP-HTTP	HTTPS-HTTPS
Целевой IP-адрес	127.0.0.1	127.0.0.1
Целевой порт перенаправления	(другое), 3128	(другое), 3129
Описание	Трафик HTTP-прокси	Трафик HTTPS-прокси

Параметр	HTTP	HTTPS
Зеркальный NAT	Включить	Включить

После настройки NAT ПК **«Client»** имеет доступ к сети Интернет (см. Рисунок – Подключение к сети Интернет).

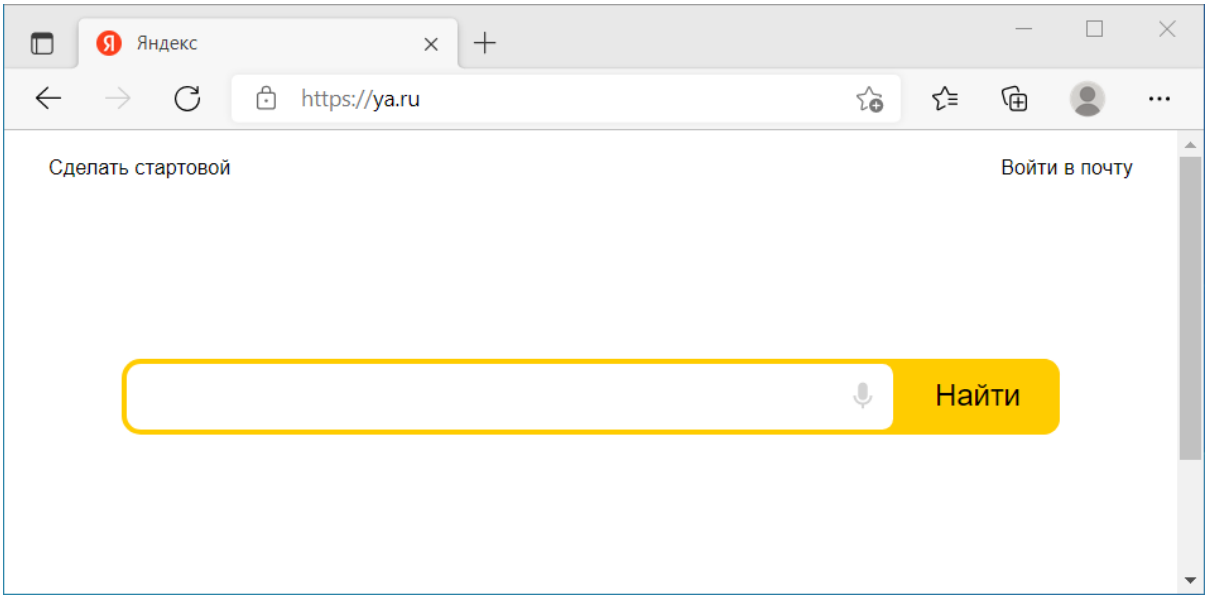


Рисунок – Подключение к сети Интернет

Примечание:

В случае отключения прокси-сервера созданное правило NAT продолжит работать.

23.1.4 Создание правил запрета обхода трафика на МЭ

Для рассматриваемого примера, настройка запрета обхода трафика не применяется.

В случае, когда прокси-сервер работает в режиме **«Непрозрачный прокси»**, для исключения доступа в сеть Интернет в обход прокси-сервера необходимо настроить правила блокировки HTTP и HTTPS трафика на МЭ.

Создание правил МЭ описано в разделе Создание правил межсетевого экранирования настоящего руководства.

Необходимо создать правила для интерфейса «LAN» с параметрами, указанными в таблице (см. Таблица «Значения параметров правил блокировки»).

Таблица «Значения параметров правил блокировки»

Параметр	HTTP	HTTPS
Действие	Блокирование (Drop)	Блокирование (Drop)
Интерфейс	LAN	LAN

Параметр	HTTP	HTTPS
Протокол	TCP	TCP
Отправитель	LAN сеть	LAN сеть
Диапазон портов назначения	HTTP	HTTPS
Описание	HTTP мимо Прокси	HTTPS мимо Прокси

Примечание:

В случае отключения прокси-сервера созданные правила МЭ продолжат работать.

23.2 Настройка веб-фильтрации

Данная функция предназначена для ограничения доступа к Интернет-ресурсам вредоносного или сомнительного содержания – фишинговые сайты, сайты с запрещённым контентом и т.д.

Для фильтрации трафика необходимо выполнить следующие действия:

1. Перейти во вкладку **«Перенаправляющий прокси»**.
2. Раскрыть вкладку **«Перенаправляющий прокси»**, нажав **кнопку** « ▼ », и выбрать **«Список управления доступом»** (см. Рисунок – Выбор настроек перенаправляющего прокси).

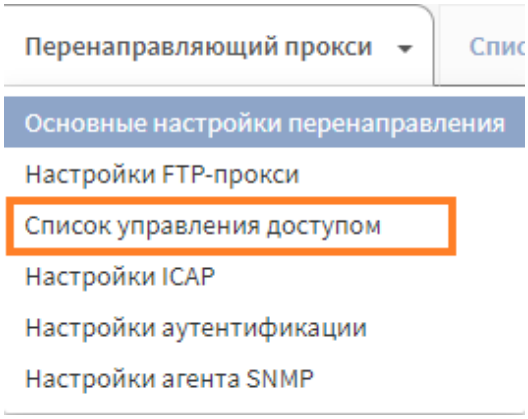


Рисунок – Выбор настроек перенаправляющего прокси

3. В открывшейся форме (см. Рисунок – Список управления доступом), в поле параметра **«Черный список»** указать список сайтов, подлежащих блокировке. В примере используется сайт «mail.ru».

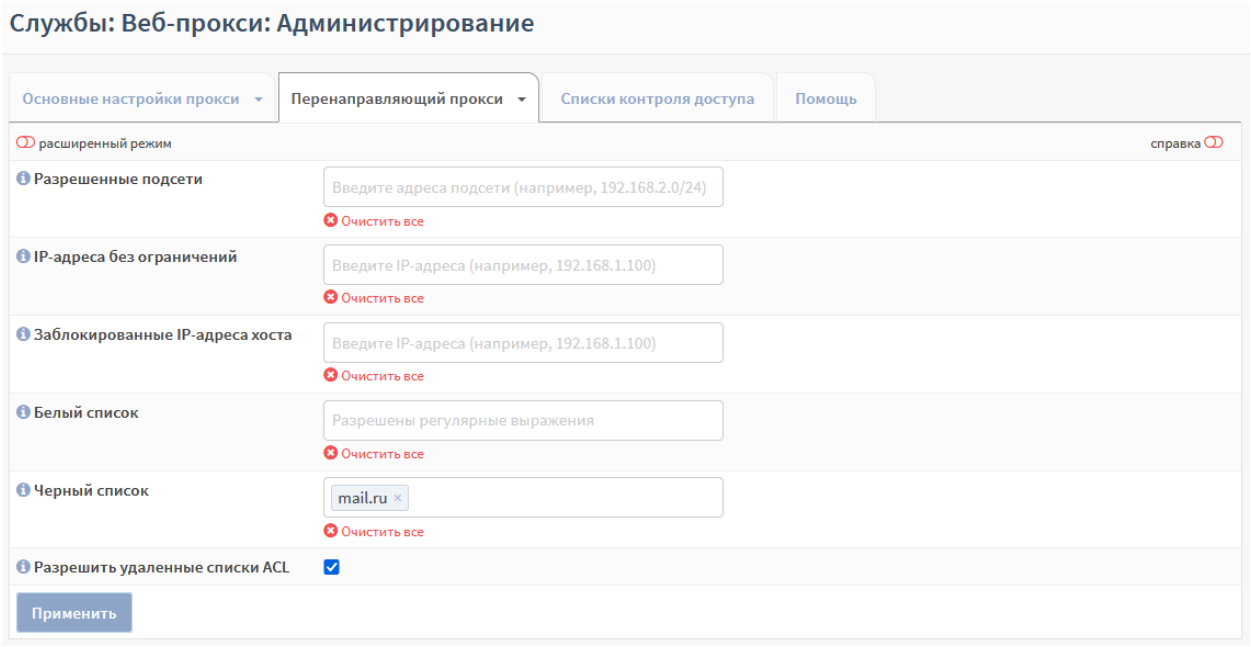


Рисунок – Список управления доступом

4. С целью разрешения загрузки удалённых списков доступа установить флажок для параметра **«Разрешить удаленные списки ACL»** и нажать **кнопку «Применить»**.
5. Перейти во вкладку **«Списки контроля доступа»** (см. Рисунок – Списки контроля доступа) и нажать **кнопку** « + » для добавления внешнего списка доступа.

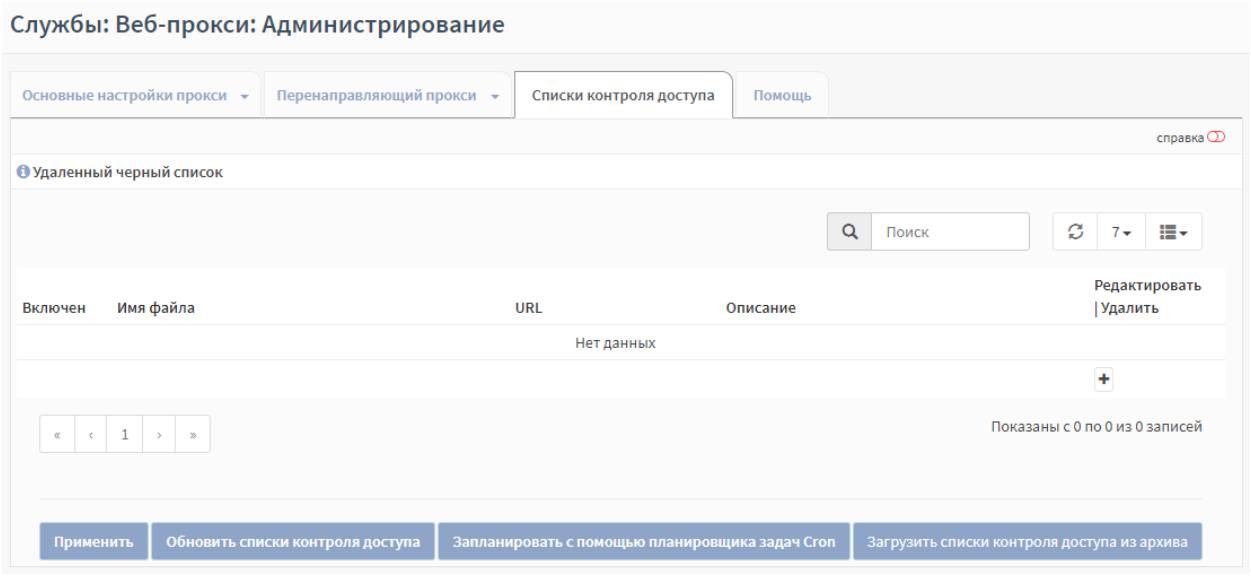


Рисунок – Списки контроля доступа

6. В открывшейся форме (см. Рисунок – Редактировать чёрный список) указать следующие параметры:
   - **«Имя файла»** – «UT1»;

- **«URL»** – «ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz»;
- **«Описание»** – «Блокировка UT1 web filter».

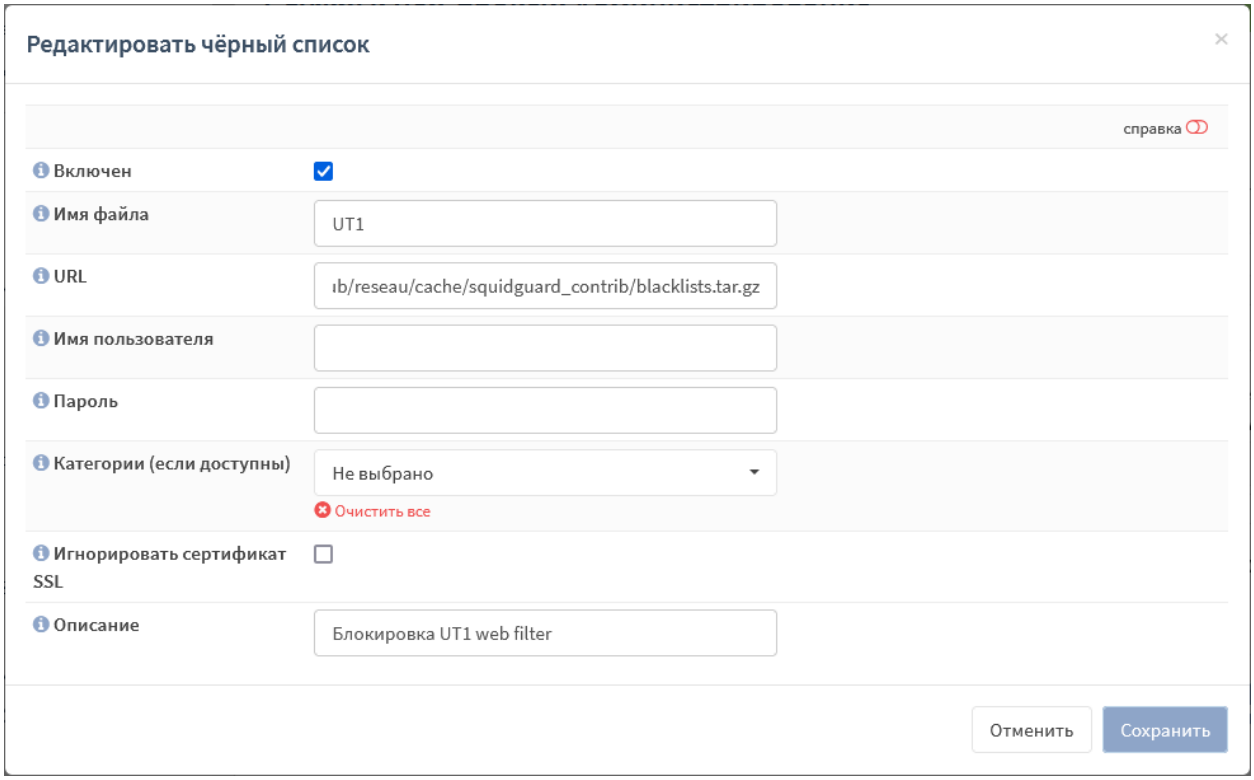


Рисунок – Редактировать чёрный список

7. Нажать **кнопку «Обновить списки контроля доступа»**, а затем нажать **кнопку «Применить»**.

   Примечание:

   При использовании внешних списков контроля доступа необходимо убедиться в их доступности.

В результате настройки сайт «mail.ru» будет заблокирован как включённый в чёрный список **ARMA FW**, а сайт «pornhub.com» будет заблокирован как включённый во внешний чёрный список (см. Рисунок – Заблокированные сайты).

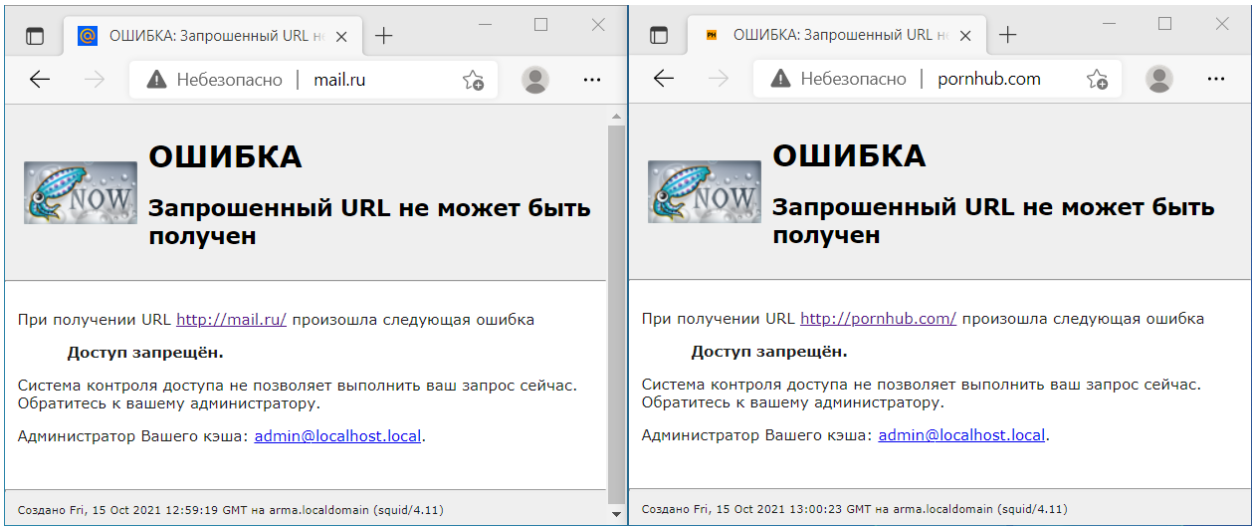


Рисунок – Заблокированные сайты

Порядок изменения текста уведомления при блокировке ресурса описан в разделе Редактирование шаблона уведомления настоящего руководства.

23.2.1 Расширенная веб-фильтрация

При использовании аутентификации на прокси-сервере доступно создание чёрных и белых списков доменов с привязкой к пользователям и группам пользователей.

Для создания списка доменов необходимо выполнить следующие действия:

1. Перейти во вкладку **«Перенаправляющий прокси»** подраздела администрирования прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**).

2. Раскрыть вкладку **«Перенаправляющий прокси»**, нажав **кнопку** « ▼ », и выбрать **«Настройки аутентификации»** (см. Рисунок – Настройки аутентификации).

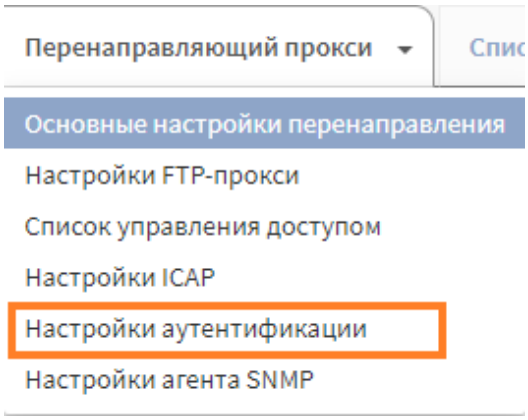


Рисунок – Настройки аутентификации

3. В открывшейся форме указать значение «Local Database» для параметра **«Метод аутентификации»** и нажать **кнопку «Применить»**.

4. Перейти в подраздел управления списками доменов (**«Службы» - «Веб-прокси» - «Группы и пользователи»**) и нажать **кнопку** « + ».
5. В открывшейся форме **«Редактирование групповых/пользовательских белых и черных журналов»** (см. Рисунок – Создание списка доменов) задать значения параметров:
   - **«Имя»** – имя пользователя или группы, в зависимости от выбранного значения параметра **«Группа/пользователь»**;
   - **«Приоритет»** – приоритет списка;
   - **«Группа/пользователь»** – тип записи;
   - **«Черный/белый»** – тип списка;
   - **«Домены»** – домен или перечень доменов.

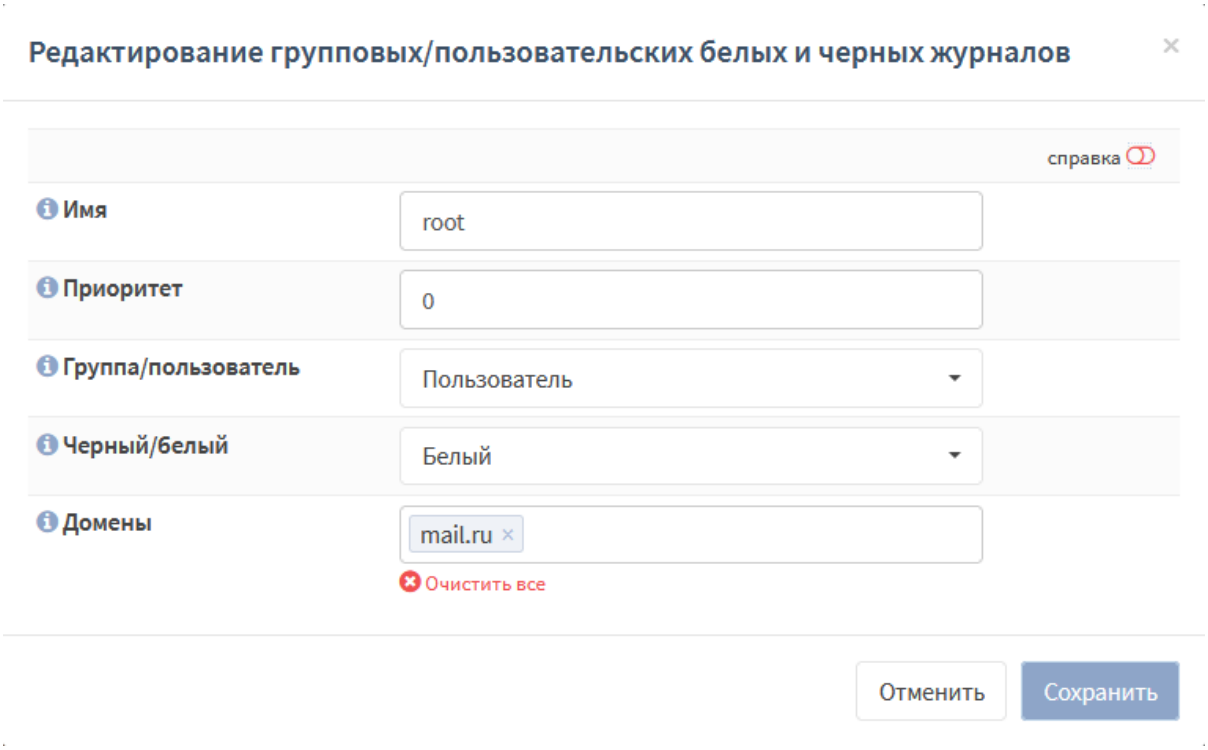


Рисунок – Создание списка доменов

6. Нажать **кнопку «Сохранить»** и нажать **кнопку «Применить»**.

В зависимости от выбранного типа параметра **«Черный/белый»** будет применяться следующее правило веб-фильтрации:

- **«Черный»** – доступ есть ко всем сайтам, кроме указанных в параметре **«Домены»**;
- **«Белый»** – доступ есть только к сайтам, указанным в параметре **«Домены»**.

23.3 ICAP

ICAP используется для настройки взаимодействия прокси-сервера с антивирусом или другими информационными системами, например, **InfoWatch Traffic Monitor**, в том числе, расположенными на внешнем хосте. Подробная настройка проверки веб-трафика с использованием службы Dr.Web в **ARMA FW** рассмотрена в разделе Dr.Web настоящего руководства.

ARMA FW поддерживает работу ICAP только с одним клиентом.

23.3.1 Интеграция по ICAP с InfoWatch Traffic Monitor

Для интеграции по ICAP с **InfoWatch Traffic Monitor** необходимо выполнить следующие шаги:

1. Настроить прокси-сервер (см. Настройка кэширующего прокси-сервера).
2. Включить ICAP.

   Для включения ICAP необходимо выполнить следующие действия:

   - перейти в подраздел настроек прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**);
   - раскрыть вкладку **«Перенаправляющий прокси»** нажатием **кнопки** « ▾ » и выбрать **«Настройки ICAP»** (см. Рисунок – Выбор настроек перенаправляющего прокси-сервера).

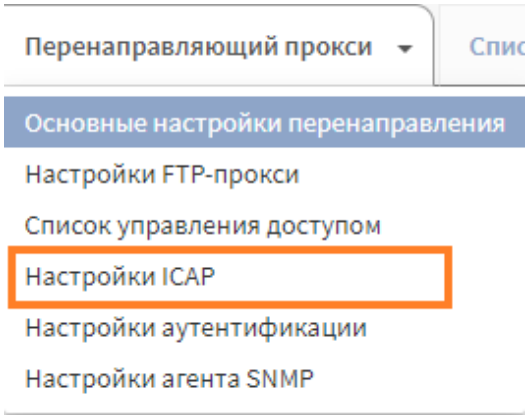


Рисунок – Выбор настроек перенаправляющего прокси-сервера

3. Установить флажок **«Включить ICAP»**, указав следующие значения параметров:
   - **«REQMOD URL»** – «icap://[IP_Traffic_Monitor]:1344/request», где «[IP_Traffic_Monitor]» – IP-адрес **InfoWatch Traffic Monitor**;
   - **«RESPMOD URL»** – поле параметра пустое;
   - **«Заголовок имени пользователя»** – «X-Authenticated-User»;
   - **«Отправить имя пользователя»** – флажок установлен;

- **«Закодировать имя пользователя»** – флажок установлен.

и нажать **кнопку «Применить»**.

Параметры **«Заголовок имени пользователя»**, **«Отправить имя пользователя»** и **«Закодировать имя пользователя»** доступны при включении переключателя **«расширенный режим»**.

23.4 Дополнительные настройки

В рамках выполнения сценария настройки прокси-сервера не используются некоторые вкладки и параметры, представленные в подразделе администрирования прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**):

1. Вкладка **«Основные настройки»**:
   - **«Настройка управления трафиком»** – задаёт максимальные значения пропускной способности и размеров скачиваемых/загружаемых файлов;
   - **«Настройка родительского прокси»** – задаёт настройки родительского (вышестоящего) прокси-сервера.
2. Вкладка **«Перенаправляющий прокси»**:
   - **«Настройки FTP-прокси»** – задаёт настройки для FTP-трафика;
   - **«Настройки аутентификации»** – задаёт настройки аутентификации;
   - **«Настройки агента SNMP»** – задаёт настройки для мониторинга работоспособности прокси-сервера.
3. Вкладка **«Помощь»** – позволяет очистить кэш-память прокси-сервера с последующей перезагрузкой.

Для некоторых вкладок подраздела доступны дополнительные настройки параметров. Их отображение включается переключателем **«расширенный режим»** в левой части формы (см. Рисунок – Переключатель «расширенный режим»).

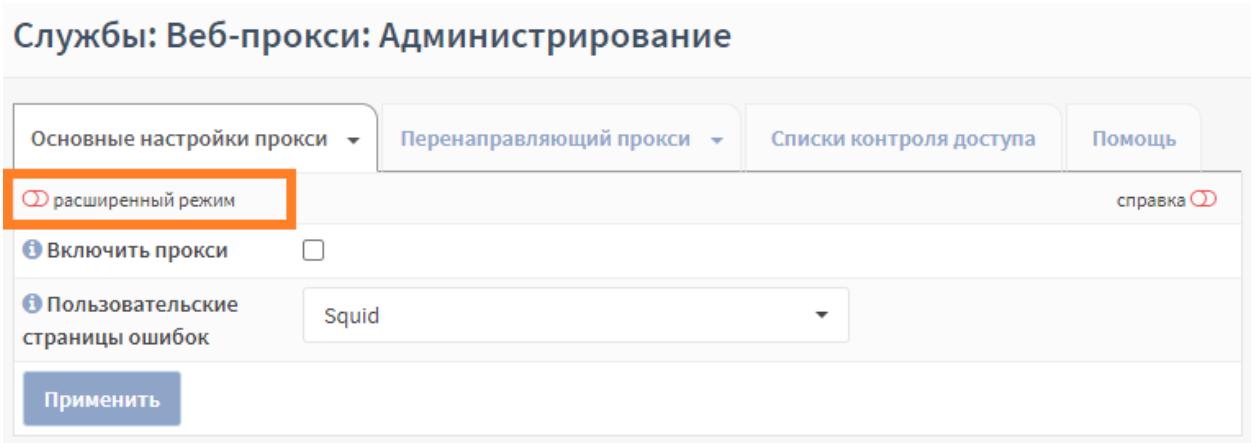


Рисунок – Переключатель «расширенный режим»

23.4.1 Редактирование шаблона уведомления

В **ARMA FW** реализована возможность редактирования шаблона уведомления при посещении сайтов, подлежащих блокировке. По умолчанию используется предустановленный шаблон уведомления.

Для редактирования шаблона уведомления необходимо выполнить следующие действия:

1. Перейти в подраздел администрирования прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**).
2. Выбрать значение «Настроенное пользователем» (см. Рисунок – Пользовательские страницы ошибок) в параметре **«Пользовательские страницы ошибок»**.

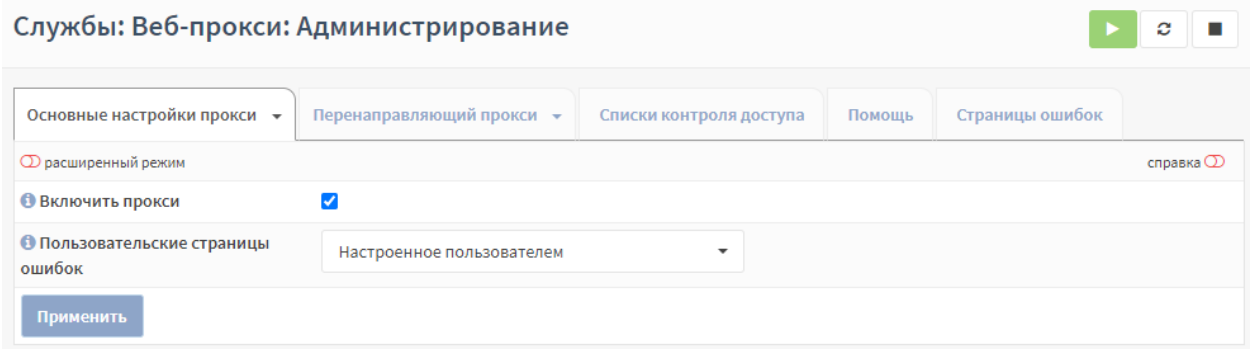


Рисунок – Пользовательские страницы ошибок

3. Перейти в появившуюся вкладку **«Страницы ошибок»**.
4. Нажать **кнопку** « » в результате чего будет загружен архив **«proxy_template.zip»**.
5. Распаковать загруженный архив и перейти в извлечённую директорию.
6. Открыть файл **«ERR_ACCESS_DENIED.html»** с помощью текстового редактора, например «Notepad++».
7. Изменить текст страницы в отмеченных строках (см. Рисунок – Редактирование уведомления) и сохранить файл.

```
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2020 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ОШИБКА: Запрошенный URL не может быть получен</title>
<!--EMBED:start-->
<!-- leave this block as is, our parser will convert links to inline content -->
<link rel="stylesheet" type="text/css" href="errorpage.css">
<!--EMBED:end -->
</head><body id="%c">
<div id="titles">

</div>
<hr>

<div id="content">
<h1>ОШИБКА</h1>
<h2>Запрошенный URL не может быть получен</h2>

```

Рисунок – Редактирование уведомления

8. Сжать директорию **«proxy_template»** в архив с расширением **«zip»**.
9. Нажать **кнопку** « » (folder), указать добавленный архив и нажать **кнопку «Открыть»**.
10. Нажать **кнопку** « » (upload), а затем **кнопку «Применить»** (см. Рисунок – Загрузка архива).

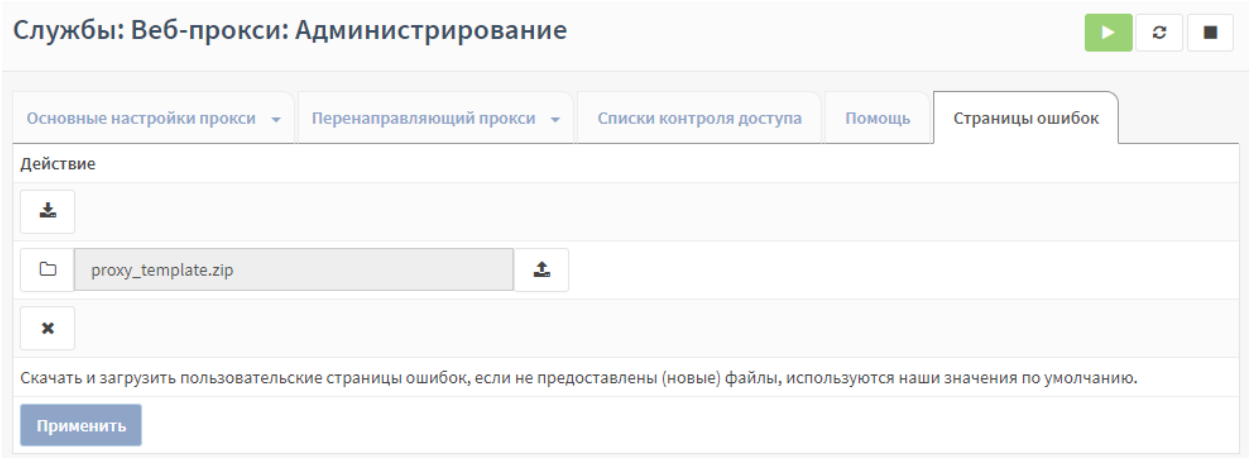


Рисунок – Загрузка архива

При необходимости сброса настроенного шаблона к значениям по умолчанию нажать **кнопку** « » (cancel), затем во всплывающем окне с предупреждением нажать **кнопку** « » (check) и **кнопку «Применить»**.

23.5 Технология единого входа

SSO используется для аутентификации пользователей на прокси-сервере через протокол Kerberos и позволяет исключить повторные запросы для прохождения аутентификации.

В качестве примера настройки SSO для прокси-сервера будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки SSO), со следующими параметрами:

- домен Active Directory – «test.local»;
- имя контроллера домена – «DC-01.test.local»;
- контроллер домена является DNS-сервером сети «LAN»;
- ПК **«Client»** введён в домен «test.local»;
- имя **ARMA FW** – «arma.test.local».

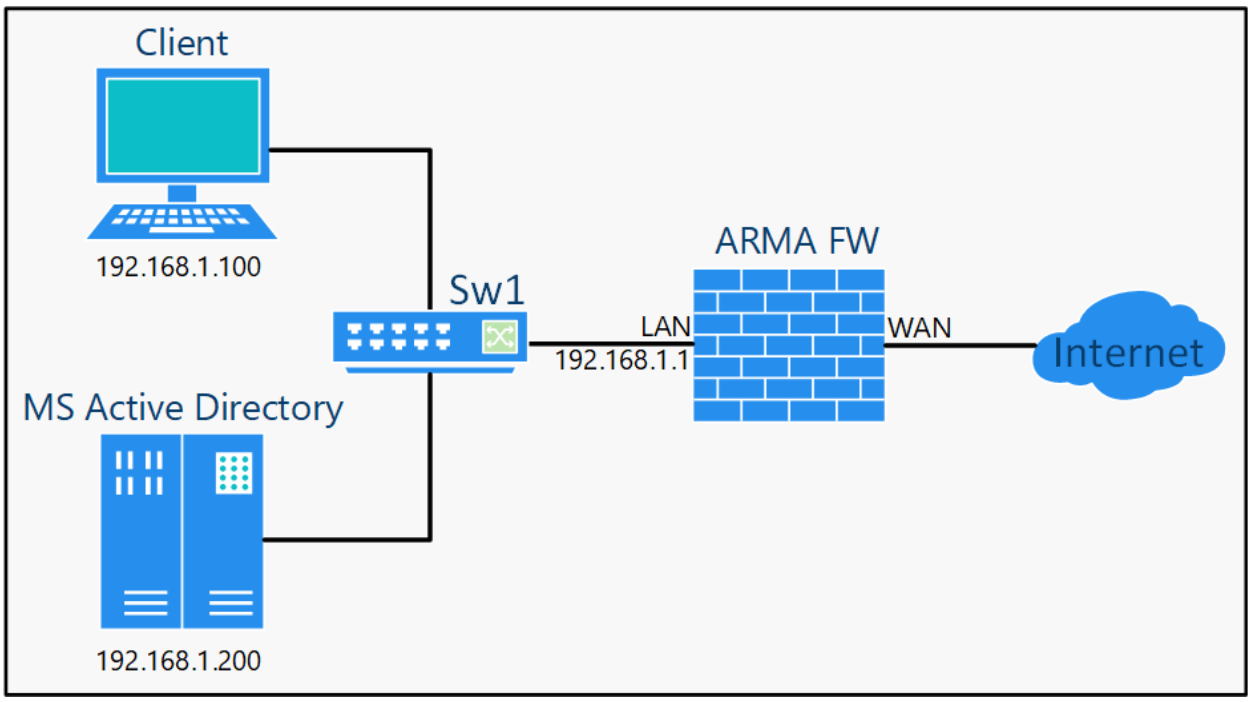


Рисунок – Схема стенда для настройки SSO

Для использования SSO на настроенном прокси-сервере необходимо выполнить следующие шаги:

1. Добавить DNS-записи на DNS-сервере.
2. Настроить **ARMA FW** для работы с Active Directory.
3. Настроить LDAP аутентификацию.
4. Настроить прокси-сервер.
5. Включить и настроить SSO.

23.5.1 Добавление DNS-записей

На DNS-сервере необходимо создать записи:

- **Запись 1**:
  - **«Зона»** – Прямого просмотра «test.local»;

- **«Тип записи»** – Узел (A);
- **«Узел»** – arma;
- **«IP-адрес»** – 192.168.1.1;
- **«Имя узла»** – –;

- **Запись 2**:
  - **«Зона»** – Прямого просмотра «test.local»;
  - **«Тип записи»** – Узел (A);
  - **«Узел»** – dc-01;
  - **«IP-адрес»** – 192.168.1.200;
  - **«Имя узла»** – –;
- **Запись 3**:
  - **«Зона»** – Обратного просмотра «1.168.192.in-addr.arpa»;
  - **«Тип записи»** – Указатель (PRT);
  - **«Узел»** – –;
  - **«IP-адрес»** – 192.168.1.1;
  - **«Имя узла»** – arma.test.local;
- **Запись 4**:
  - **«Зона»** – Обратного просмотра «1.168.192.in-addr.arpa»;
  - **«Тип записи»** – Указатель (PRT);
  - **«Узел»** – –;
  - **«IP-адрес»** – 192.168.1.200;
  - **«Имя узла»** – dc-01.test.local.

Записи создаются в соответствии с руководством пользователя используемого DNS-сервера.

23.5.2 Настройка ARMA FW для работы с Active Directory

Перед использованием SSO необходимо выполнить следующие шаги по настройке **ARMA FW**:

1. Указать домен.
2. Указать контроллер домена в качестве DNS-сервера.
3. Настроить синхронизацию времени с контролером домена.

23.5.2.1 Указание домена и DNS-сервера

Для указания домена **ARMA FW** и контроллера домена в качестве DNS-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел общих настроек **ARMA FW** (**«Система» - «Настройки» - «Общие настройки»**).
2. Указать имя домена **«test.local»** в поле параметра **«Домен»** (см. Рисунок – Указание домена).

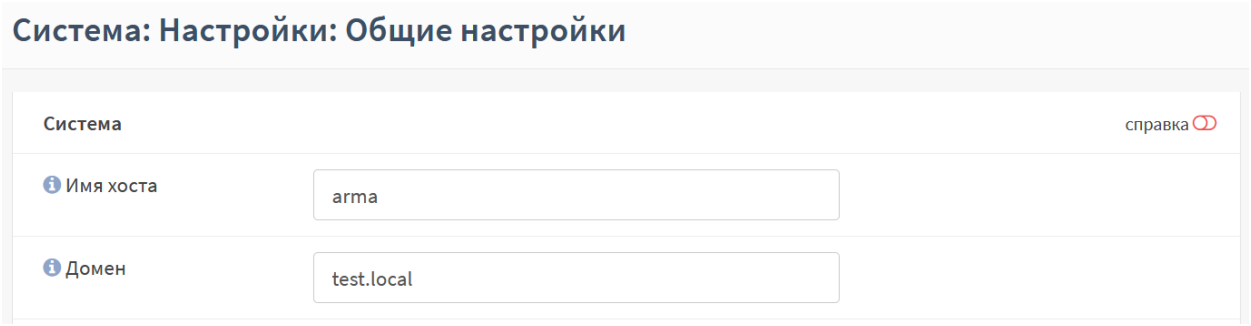


Рисунок – Указание домена

3. Указать IP-адрес контроллера домена в поле параметра **«DNS-сервер»** (см. Рисунок – Указание DNS-сервера).

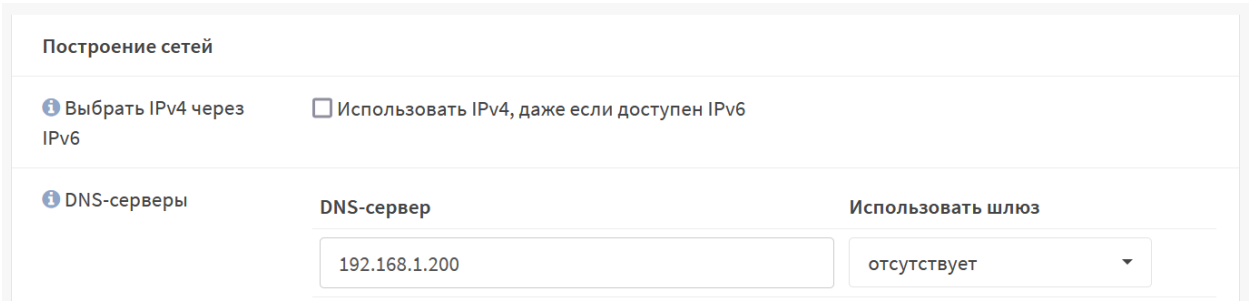


Рисунок – Указание DNS-сервера

4. Снять флажок для параметра **«Позволить переопределить список DNS-серверов DHCP/PPP на WAN»** и нажать **кнопку «Сохранить»**.

23.5.2.2 Настройка синхронизации времени с контроллером домена

Необходимо указать контроллер домена в качестве предпочтительного NTP-сервера. Подробная настройка синхронизации времени рассмотрена в разделе Настройка синхронизации времени по протоколу NTP настоящего руководства.

23.5.3 Настройка LDAP авторизации

Подробная настройка LDAP авторизации рассмотрена в разделе LDAP настоящего руководства.

23.5.4 Настройка прокси-сервера

Подробная настройка прокси-сервера рассмотрена в разделе Настройка кэширующего прокси-сервера настоящего руководства.

Для использования технологии единого входа на прокси-сервере необходимо выполнить следующие действия:

1. Отключить прозрачный прокси-сервер в случае его использования.

   Для этого необходимо перейти во вкладку **«Перенаправляющий прокси»** подраздела администрирования прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**), снять флажок для параметра **«Включить прозрачный HTTP-прокси»** и нажать **кнопку «Применить»**.

2. Указать добавленный LDAP-сервер в качестве метода аутентификации на прокси-сервере.

   Для этого необходимо раскрыть вкладку **«Перенаправляющий прокси»** подраздела администрирования прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**), выбрать **«Настройки аутентификации»**, выбрать добавленный LDAP-сервер в поле параметра **«Метод аутентификации»** и нажать **кнопку «Применить»**.

   Примечание:

   При отключённом прозрачном прокси-сервере настройки прокси-сервера на клиентах необходимо указывать явно – вручную, с помощью групповых политик и т.д. Адрес прокси-сервера указывается в виде полного доменного имени (см. Рисунок – Настройка прокси-сервера клиентам), **в случае указания IP-адреса технология единого входа работать не будет!**

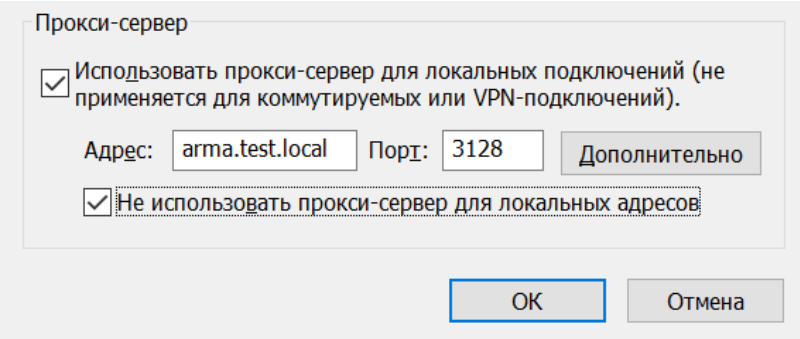


Рисунок – Настройка прокси-сервера клиентам

23.5.5 Включение и настройка SSO

Для включения SSO необходимо выполнить следующие действия:

1. Перейти в подраздел настроек единой точки входа (**«Службы» - «Веб-прокси» - «Единая точка входа»**) и установить флажок для параметра **«Включите единый вход»**.
2. Указать имя УЗ Kerberos **ARMA FW** (см. Рисунок – Включение SSO) и нажать **кнопку «Применить»**.

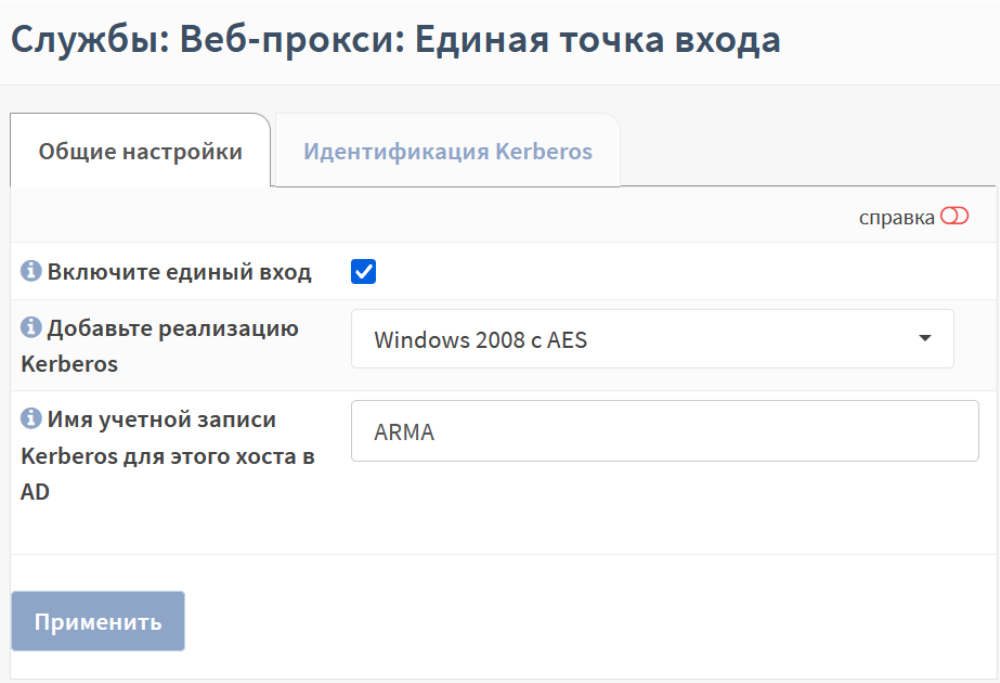


Рисунок – Включение SSO

Для настройки SSO необходимо выполнить следующие действия:

1. Перейти во вкладку **«Идентификация Kerberos»** подраздела настроек единой точки входа (**«Службы» - «Веб-прокси» - «Единая точка входа»**) и нажать **кнопку «Обновить»**.
2. Все пункты, за исключением **«Файл с таблицей ключей»**, должны быть отмечены зелёными флажками (см. Рисунок – Журнал проверок идентификации Kerberos).

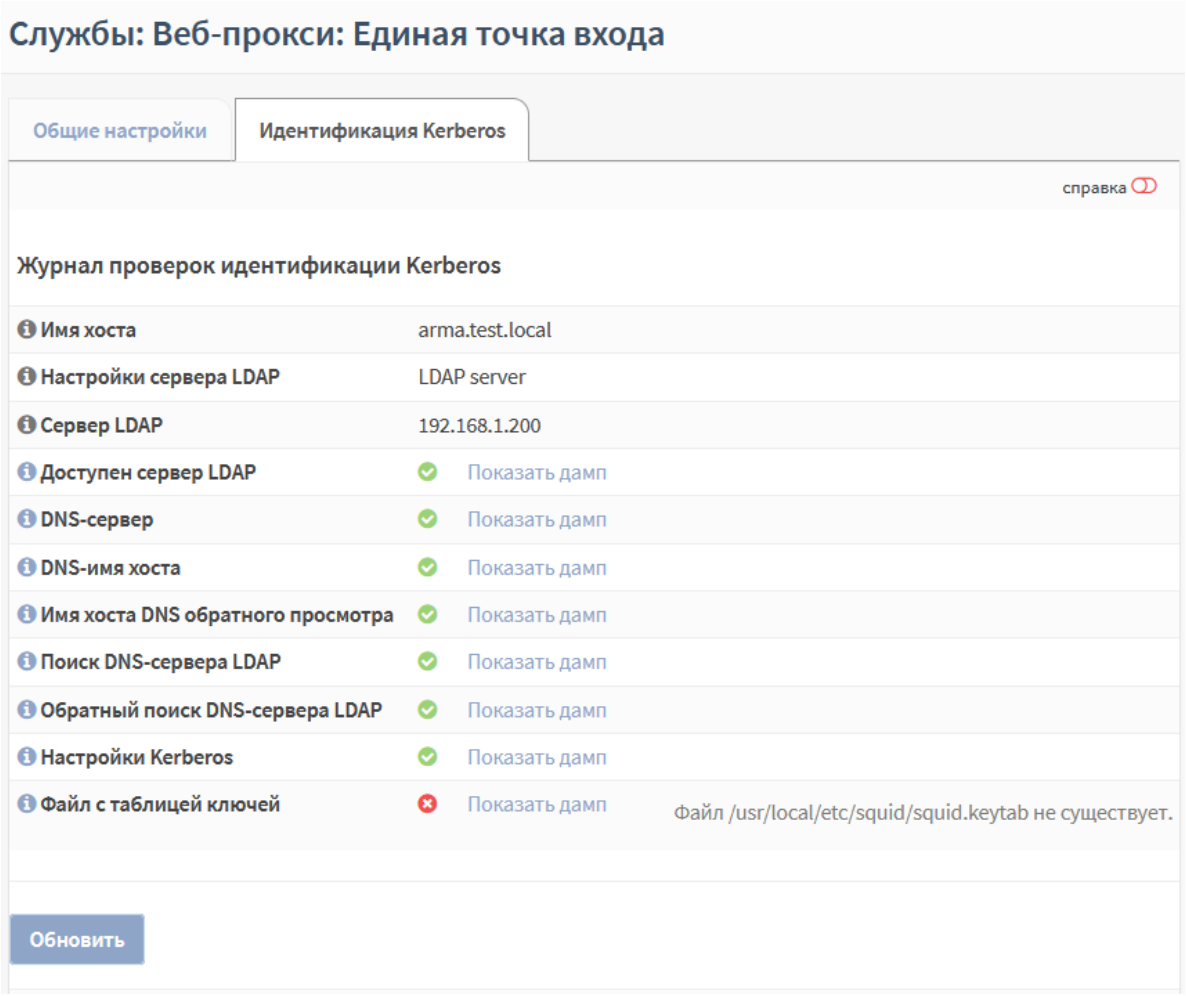


Рисунок – Журнал проверок идентификации Kerberos

В случае ошибок необходимо проверить выполненные ранее шаги.

3. Указать данные УЗ, имеющей привилегии администратора домена, в полях параметров **«Добавьте логин администратора»** и **«Добавьте пароль администратора»** и нажать **кнопку «Создать таблицу ключей»**.

   Примечание:

   При использовании контроллера домена уровня Windows Server 2003 перед созданием таблицы ключей необходимо удалить УЗ Kerberos **ARMA FW**.

4. Нажать **кнопку «Обновить»**. В случае успешного создания таблицы ключей пункт **«Файл с таблицей ключей»** будет отмечен зелёным флажком.
5. Перейти во вкладку **«Общие настройки»** и нажать **кнопку «Применить»**.

23.5.5.1 Проверка корректности настроек

Для проверки корректности настроек идентификации Kerberos необходимо выполнить следующие действия:

1. Перейти во вкладку **«Идентификация Kerberos»** подраздела настроек единой точки входа (**«Службы» - «Веб-прокси» - «Единая точка входа»**).
2. Указать учётные данные для подключения к внешнему LDAP серверу и нажать **кнопку «Проверка логина Kerberos»** (см. Рисунок – Проверка корректности настроек идентификации Kerberos).

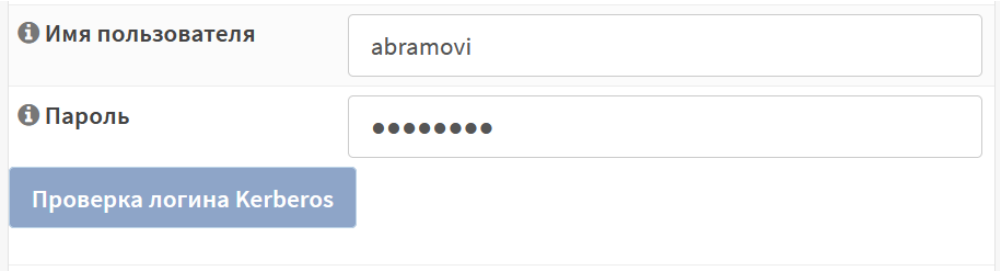


Рисунок – Проверка корректности настроек идентификации Kerberos

3. В случае успешной проверки в поле **«Выход»** отобразится результат, содержащий слово **«OK»** (см. Рисунок – Результат успешной проверки).

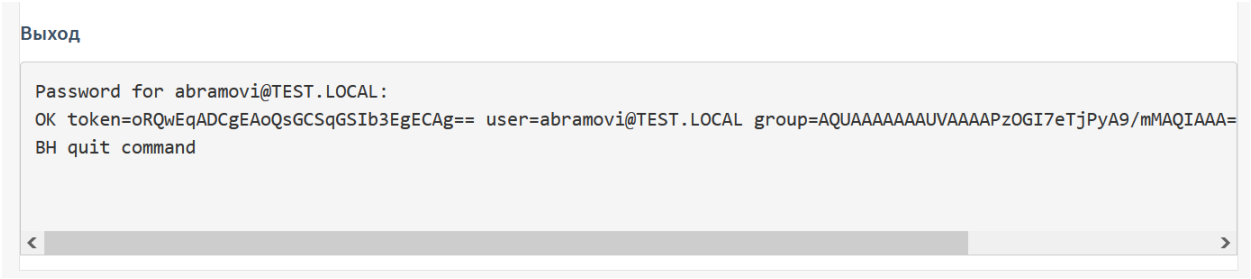
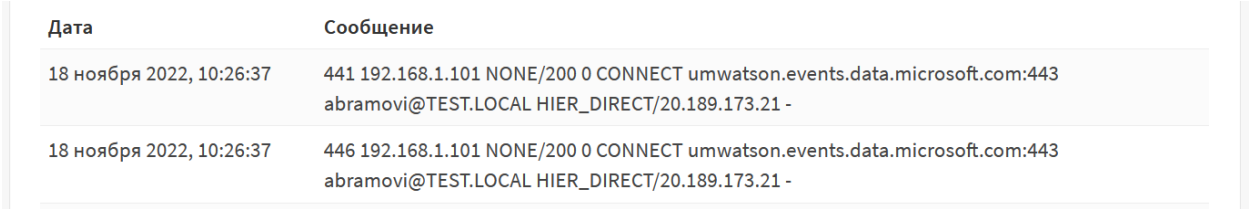


Рисунок – Результат успешной проверки

23.5.6 Проверка работы SSO

Для проверки работы технологии единого входа необходимо выполнить следующие действия:

1. Открыть настроенный веб-браузер на ПК **«Client»** и перейти на сайт «ya.ru» – сайт будет открыт без запроса учётных данных пользователя.
2. Перейти в подраздел журналирования прокси-сервера (**«Службы» - «Веб-прокси» - «Журнал доступа»**) и убедиться в наличии записей авторизации с УЗ пользователей домена «test.local» (см. Рисунок – Записи в журнале доступа).



Дата	Сообщение
18 ноября 2022, 10:26:37	441 192.168.1.101 NONE/200 0 CONNECT umwatson.events.data.microsoft.com:443 abramovi@TEST.LOCAL HIER_DIRECT/20.189.173.21 -
18 ноября 2022, 10:26:37	446 192.168.1.101 NONE/200 0 CONNECT umwatson.events.data.microsoft.com:443 abramovi@TEST.LOCAL HIER_DIRECT/20.189.173.21 -

Рисунок – Записи в журнале доступа

24 ОБРАТНЫЙ ПРОКСИ-СЕРВЕР И HTTP-СЕРВЕР

ARMA FW включает в себя функциональность обратного прокси-сервера и HTTP-сервера, основанного на ПО nginx.

Для включения службы nginx необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Установить флажок в параметре **«Включите nginx»** на вкладке **«Основные настройки»** (см. Рисунок – Включение nginx).

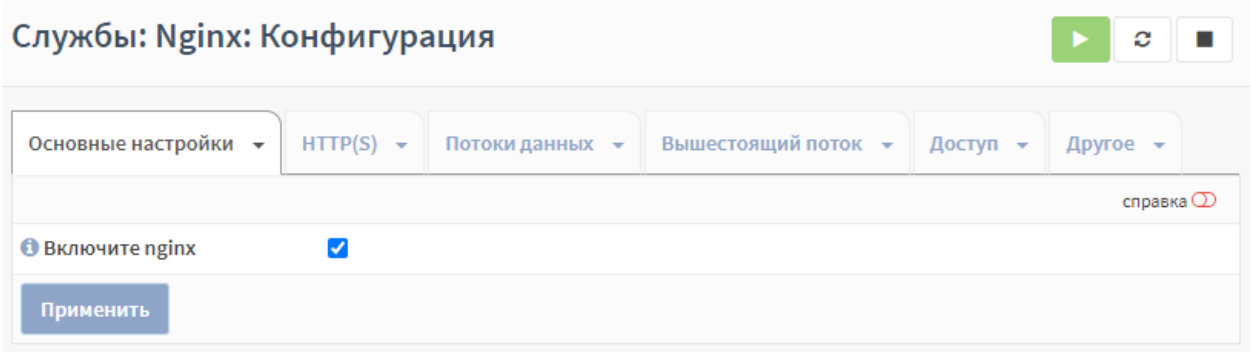


Рисунок – Включение nginx

3. Нажать **кнопку «Применить»**.

При раскрытии вкладки **«Основные настройки»** нажатием **кнопки** « ▼ » доступны дополнительные настройки nginx (см. Рисунок – Дополнительные настройки службы nginx):

- **«Общие настройки HTTP»**;
- **«Настройки веб-интерфейса»**.

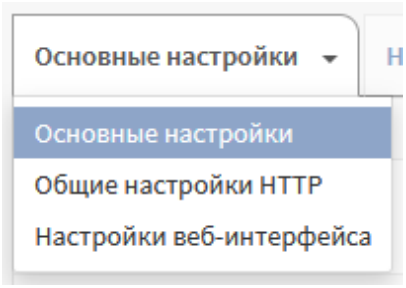


Рисунок – Дополнительные настройки службы nginx

В качестве примера настройки функций обратного прокси-сервера используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки функций обратного прокси-сервера). Доступ к веб-серверам осуществляется по порту «8080».

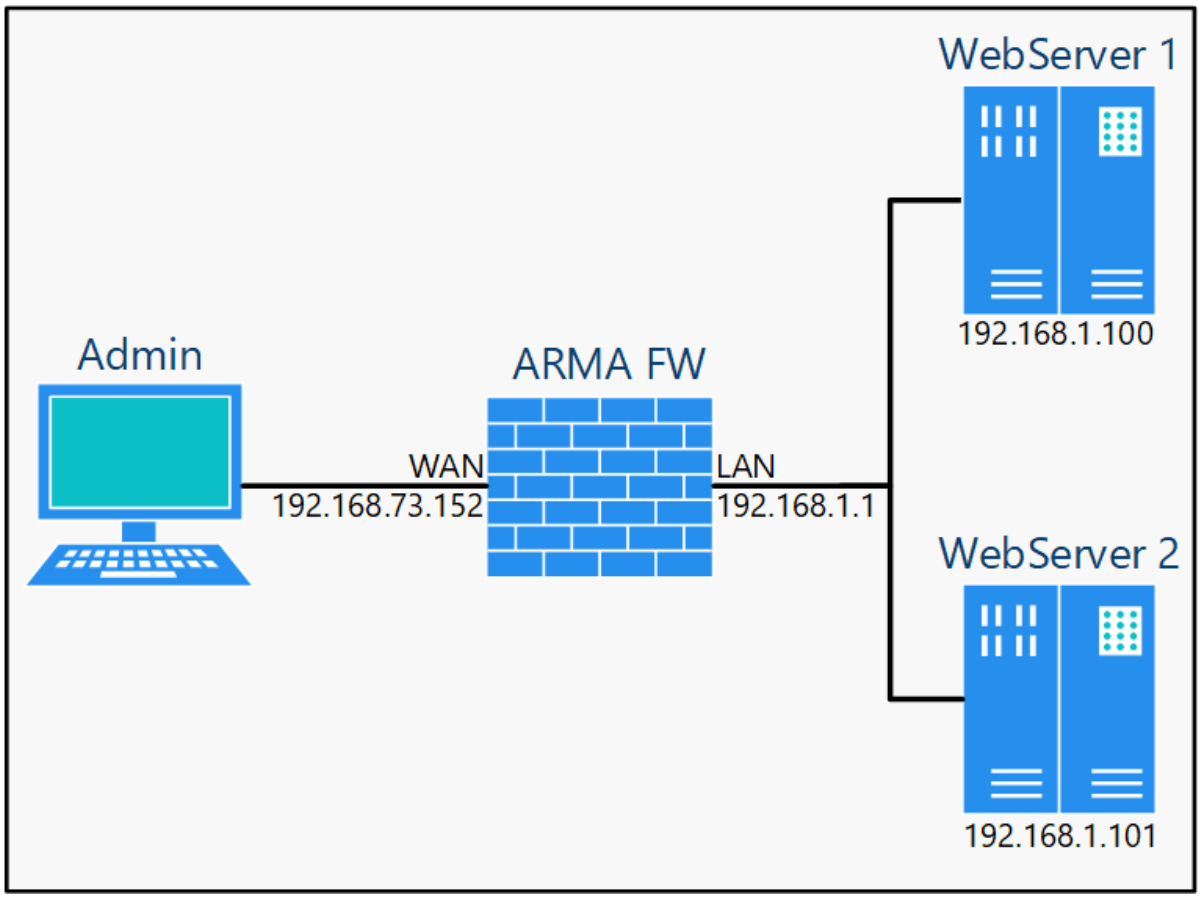


Рисунок – Схема стенда для настройки функций обратного прокси-сервера

24.1 Балансировка нагрузки

Для настройки балансировки необходимо выполнить следующие шаги:

1. Добавить веб-серверы.
2. Добавить группу серверов.
3. Добавить локацию.
4. Добавить HTTP-сервер.

Для прохождения трафика до веб-серверов необходимо выключить параметр **«Блокировать частные сети»** (см. Блок «Общая конфигурация») для интерфейса **«WAN»** и создать общее разрешающее правило МЭ (см. Создание правил межсетевого экранирования) со следующими параметрами:

- **«Действие»** – «Разрешить (Pass)»;
- **«Интерфейс»** – «WAN»;
- **«Протокол»** – «TCP»;
- **«IP-адрес назначения»** – «Этот межсетевой экран»;
- **«Диапазон портов назначения»** – «8080»;

- **«Описание»** – «Доступ к веб-серверам».

24.1.1 Добавление веб-серверов

Для добавления веб-серверов необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Перейти во вкладку **«Вышестоящий поток»** и нажать **кнопку** «  ».
3. В открывшейся форме (см. Рисунок – Добавление сервера) указать данные веб-сервера **«WebServer 1»**:
   - **«Описание»** – «WebServer 1»;
   - **«Сервер»** – «192.168.1.100»;
   - **«Порт»** – «8080»;
   - **«Приоритеты сервера»** – «10»;
   - **«Максимальное количество соединений»** – «100»;
   - **«Максимальное количество неудач»** – «10»;
   - **«Тайм-аут ошибки»** – «5»;

   и нажать **кнопку «Сохранить»**.

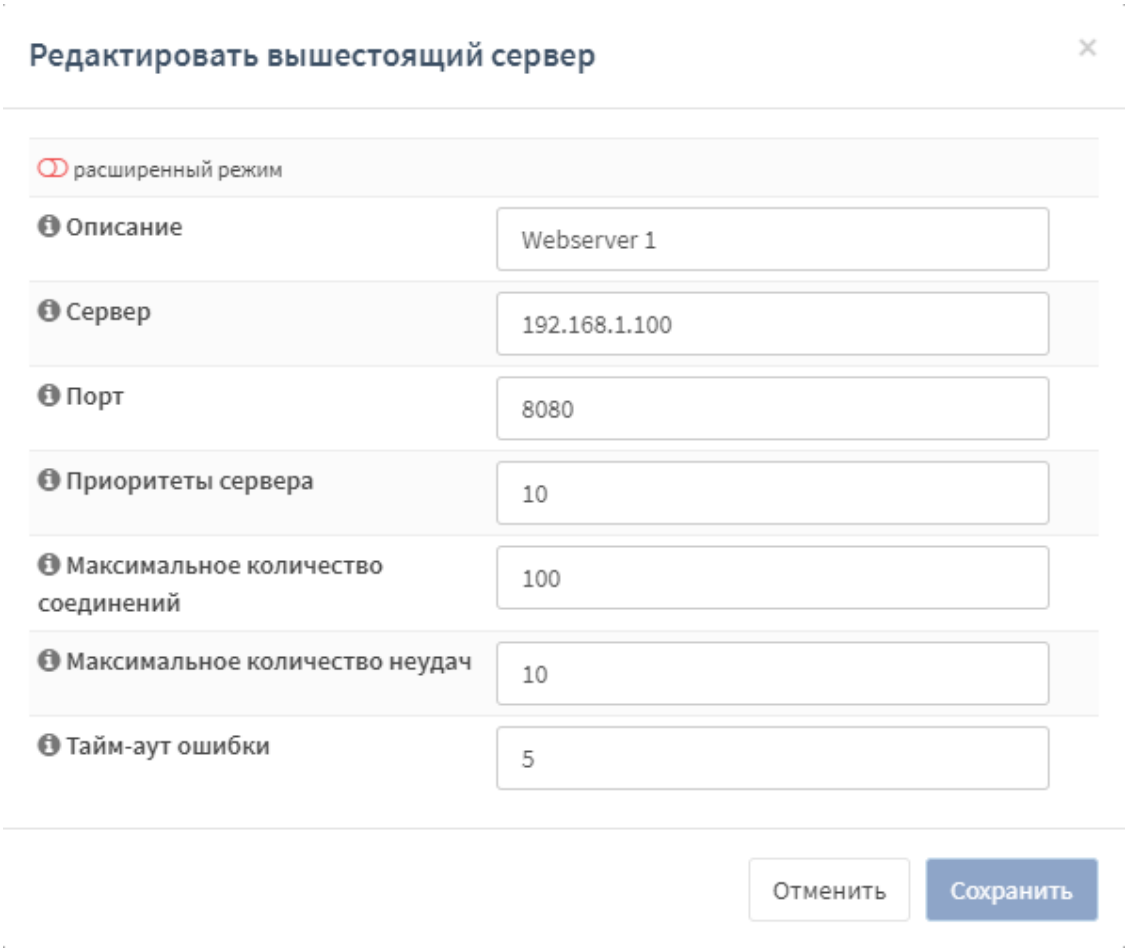


Рисунок – Добавление сервера

4. Повторить действия 1-3, указав данные веб-сервера **«WebServer 2»**:
   - **«Описание»** – «WebServer 2»;
   - **«Сервер»** – «192.168.1.101»;
   - **«Приоритеты сервера»** – «1».

24.1.2 Добавление группы серверов

Для добавления группы серверов необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«Вышестоящий поток»**, нажав **кнопку** « ▼ », выбрать **«Вышестоящий поток»** и нажать **кнопку** « + ».
3. В открывшейся форме (см. Рисунок – Добавление группы) добавить группу, указав следующие данные:
   - **«Описание»** – «web servers»;
   - **«Входы сервера»** – «WebServer 1, WebServer 2»;

остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

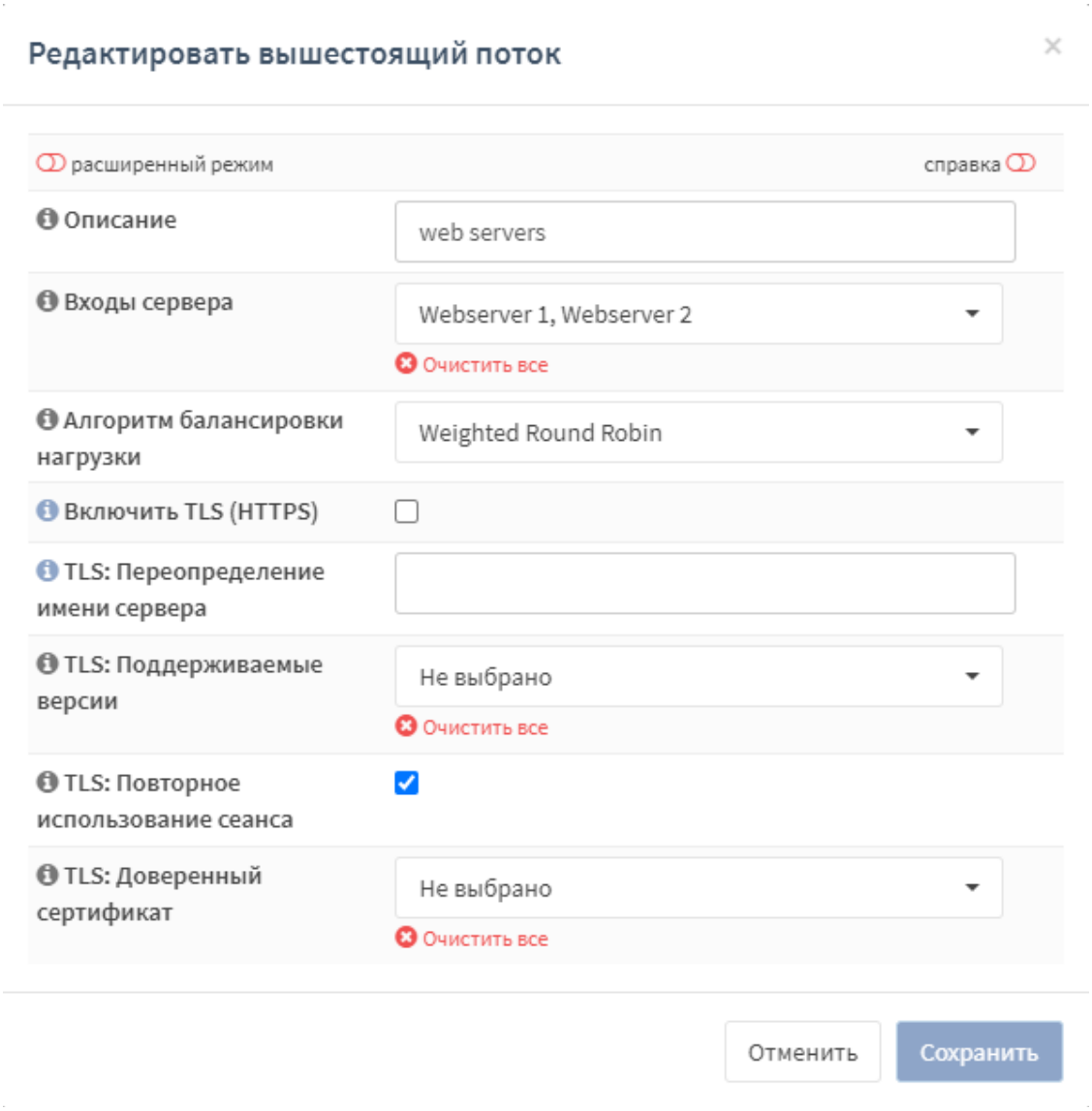


Рисунок – Добавление группы

24.1.3 Добавление локации

Для добавления локации необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Местоположение»** и нажать **кнопку** « + ».
3. В открывшейся форме (см. Рисунок – Добавление локации) добавить локацию, указав следующие данные:
   - **«Описание»** – «web location»;
   - **«Шаблон URL»** – «/»;

- **«Вышестоящие серверы»** – «web servers»;

остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

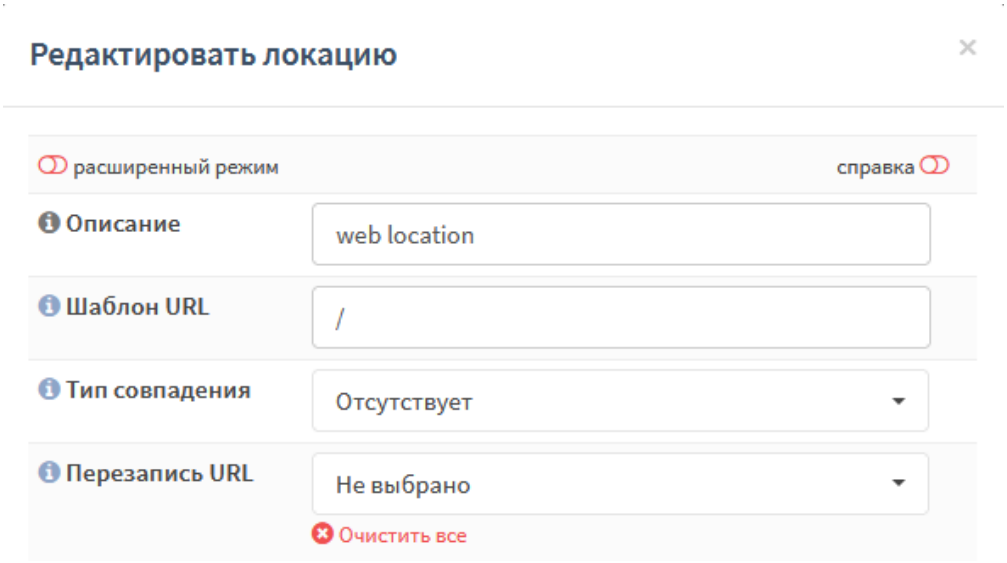


Рисунок – Добавление локации

24.1.4 Добавление HTTP-сервера

Для добавления HTTP-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Сервер HTTP»** и нажать **кнопку** « + ».
3. В открывшейся форме (см. Рисунок – Добавление HTTP-сервера) добавить HTTP-сервер, указав следующие данные:
   - **«Слушающий порт HTTP»** – «8080»;
   - **«Имя сервера»** – «arma.localdomain»;
   - **«Локации»** – «web location»;

   остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

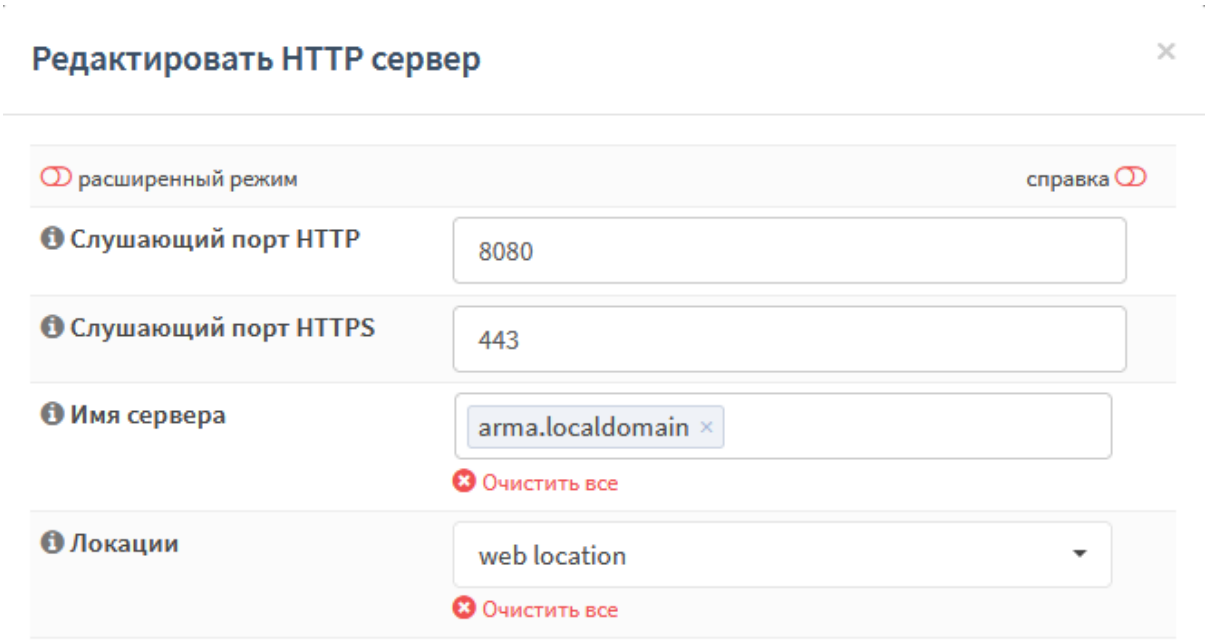


Рисунок – Добавление HTTP-сервера

24.1.5 Проверка работы

После завершения настроек необходимо перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**) и нажать **кнопку «Применить»**.

Для проверки работы балансировки нагрузки необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «http://192.168.73.152:8080» и нажать **клавишу «Enter»**. В результате отобразится стартовая страница веб-сервера «WebServer 1» (см. Рисунок – Стартовая страница веб-сервера «WebServer 1»).

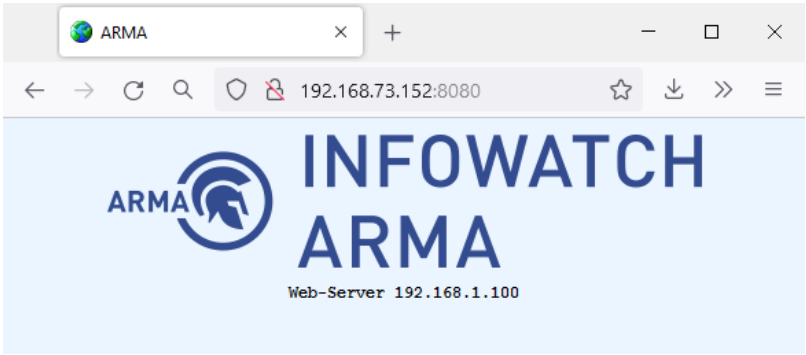


Рисунок – Стартовая страница веб-сервера «WebServer 1»

В случае отсутствия ответа веб-сервера **«WebServer 1»**, например, в результате превышения нагрузки или количества заданных сессий будет отображена стартовая страница веб-сервера **«WebServer 2»** (см. Рисунок – Стартовая страница веб-сервера «WebServer 2»).

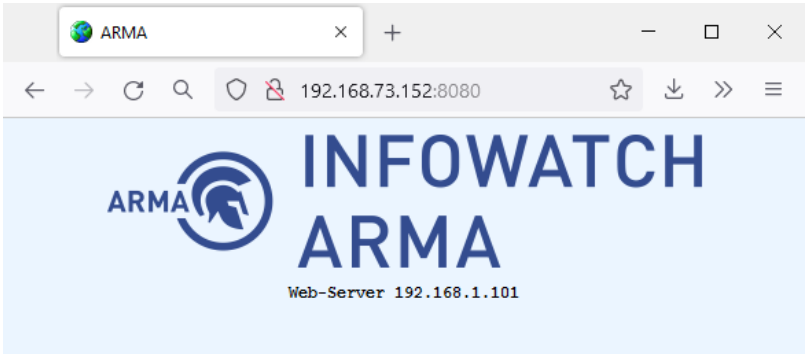


Рисунок – Стартовая страница веб-сервера «WebServer 2»

В подразделе статистики трафика nginx (**«Службы» - «Nginx» - «Статистика трафика»**) отображается статистика по распределению запросов между веб-серверами (см. Рисунок – Статистика запросов).

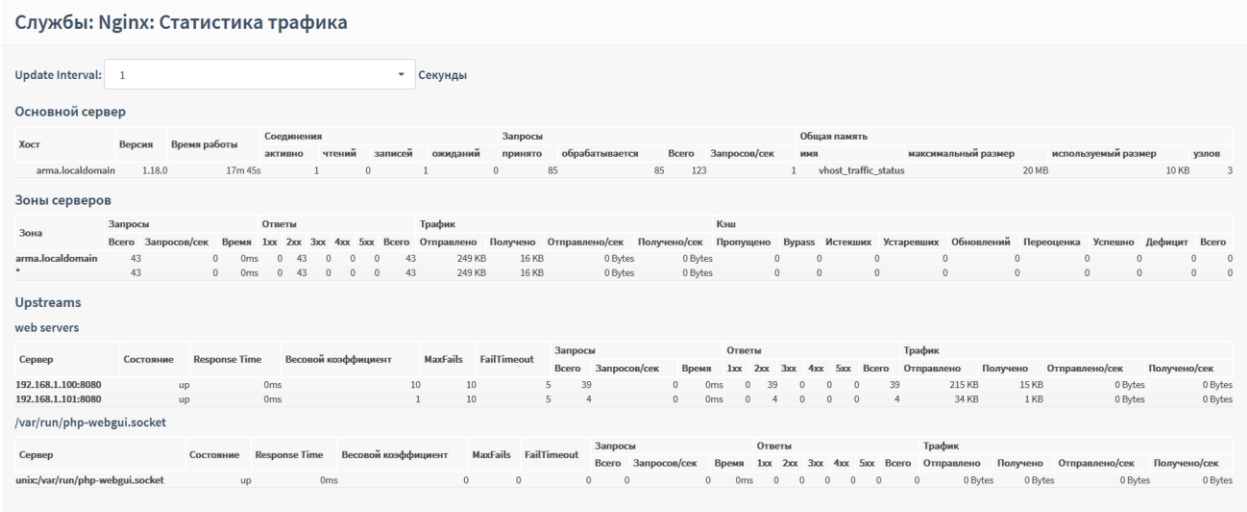


Рисунок – Статистика запросов

24.2 Настройки аутентификации

Для включения аутентификации для доступа к веб-серверам необходимо выполнить следующие шаги:

1. Добавить УЗ.
2. Добавить группу УЗ.
3. Изменить локацию.

24.2.1 Добавление УЗ

Для добавления УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Учетные данные»** и нажать **кнопку** « + ».

3. В открывшейся форме (см. Рисунок – Добавление пользователя) добавить пользователя, указав следующие данные:
   - **«Имя пользователя»** – «user»;
   - **«Пароль»** – произвольный пароль, в примере «12345»;

   и нажать **кнопку «Сохранить»**.

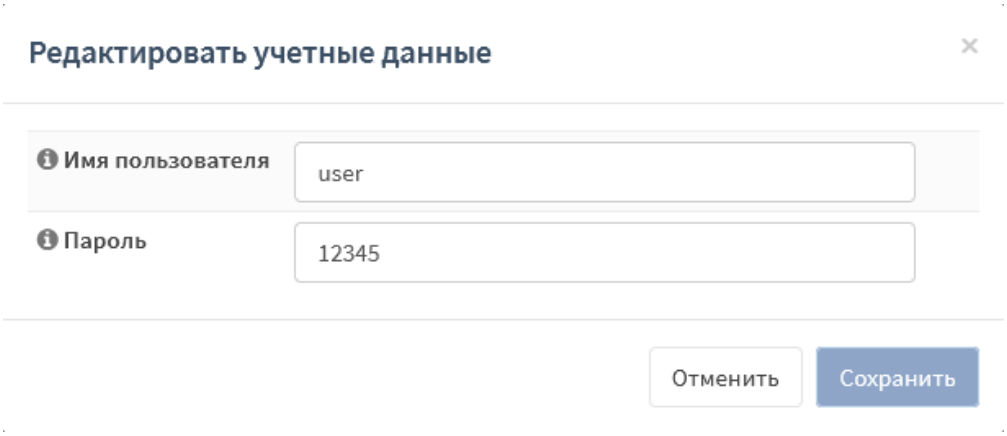


Рисунок – Добавление пользователя

4. Повторить действия 1-3, указав «admin» в поле параметра **«Имя пользователя»**.

24.2.2 Добавление группы УЗ

Для добавления группы УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Журнал пользователя»** и нажать **кнопку** « + ».
3. В открывшейся форме (см. Рисунок – Добавление группы УЗ) добавить группу, указав следующие данные:
   - **«Имя»** – «web-users»;
   - **«Пользователи»** – «admin», «user»;

   и нажать **кнопку «Сохранить»**.

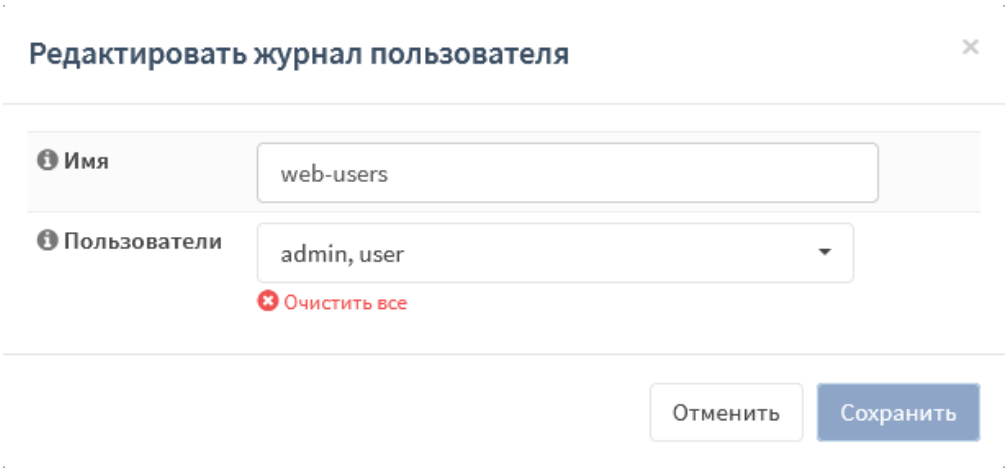


Рисунок – Добавление группы УЗ

24.2.3 Изменение локации

Для изменения локации необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Местоположение»** и нажать **кнопку** « ✎ » напротив ранее созданной локации (см. Добавление локации).
3. В открывшейся форме указать значения для следующих параметров:
   - **«Базовая идентификация»** – «web-area»;
   - **«Список основных учетных данных»** – «web-users»;

   остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

24.2.4 Проверка работы

После завершения настроек необходимо перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**) и нажать **кнопку «Применить»**.

Для проверки работы аутентификации необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «http://192.168.73.152:8080» и нажать **клавишу «Enter»**. В результате отобразится страница запроса имени пользователя и пароля (см. Рисунок – Запрос учётных данных для доступа).

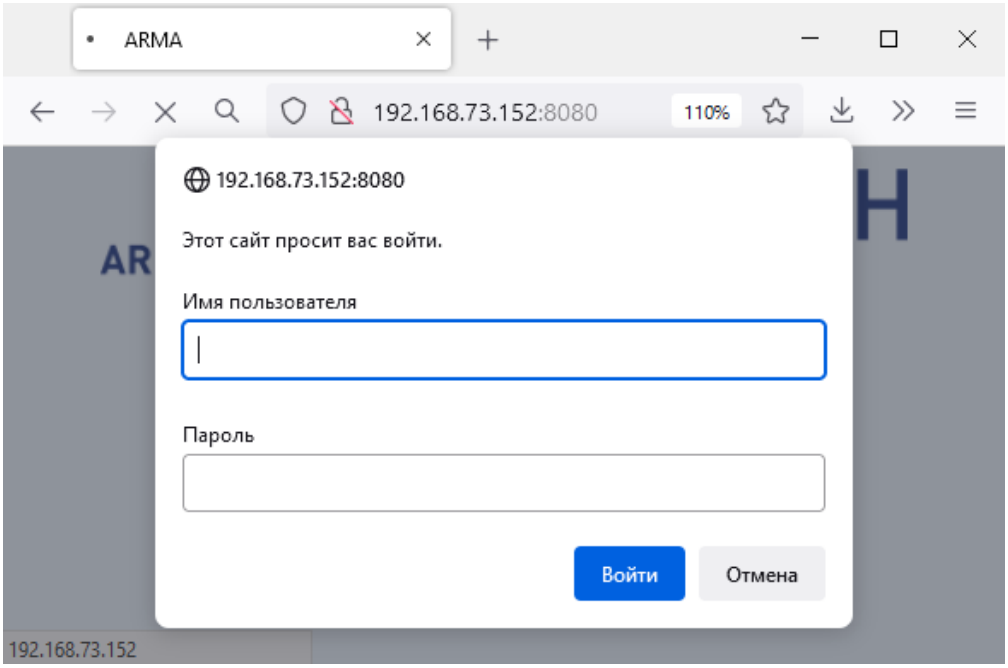


Рисунок – Запрос учётных данных для доступа

24.3 Управление доступом на основании IP-адресов

Для включения управления доступом на основании IP-адресов необходимо выполнить следующие шаги:

1. Добавить список IP-адресов.
2. Изменить локацию.

24.3.1 Добавление списка IP-адресов

Для добавления списка IP-адресов необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«Доступ»**, нажав **кнопку** « ▼ », выбрать **«IP ACLs»** и нажать **кнопку** « + ».
3. В открывшейся форме (см. Рисунок – Добавление списка IP-адресов) добавить пользователя, указав следующие данные:
   - **«Описание»** – «WAN net»;
   - **«Записи ACL»** – «192.168.73.0/24» и «Deny» для запрета доступа;

   остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

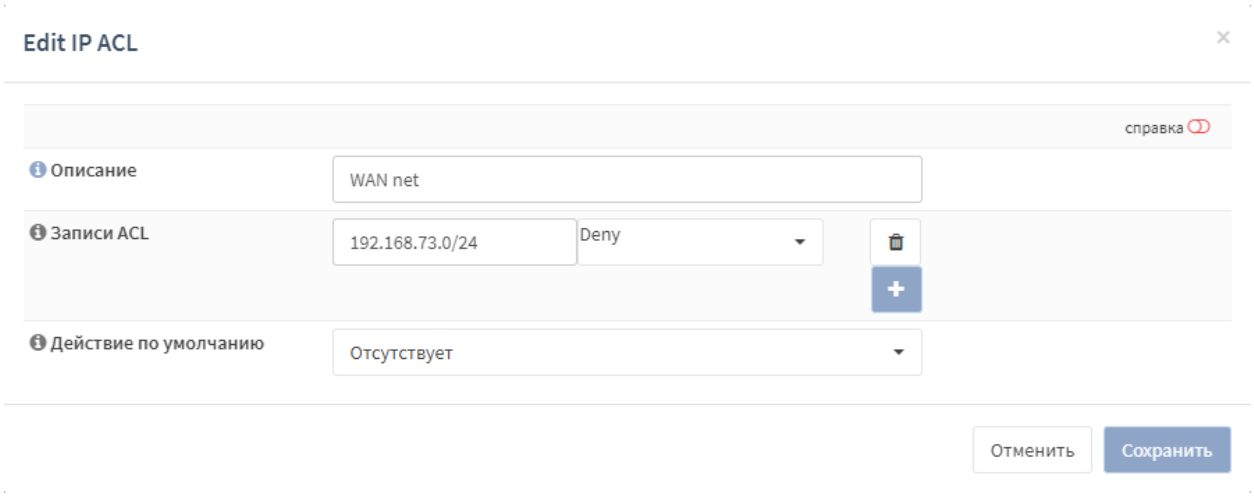


Рисунок – Добавление списка IP-адресов

24.3.2 Изменение локации

Для изменения локации необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Местоположение»** и нажать **кнопку** « ✎ » напротив ранее созданной локации (см. Добавление локации).
3. В открывшейся форме указать значения для следующих параметров:
   - **«Включить расширенные ACL»** – флажок установлен;
   - **«IP ACL»** – «WAN net»;

   остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

24.3.3 Проверка работы

После завершения настроек необходимо перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**) и нажать **кнопку «Применить»**.

Для проверки работы ограничения доступа по IP-адресам необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «http://192.168.73.152:8080» и нажать **клавишу «Enter»**. В результате отобразится страница с ошибкой доступа (см. Рисунок – Ошибка доступа).

Рисунок – Ошибка доступа

24.4 Межсетевой экран веб-приложений

Для защиты веб-приложений используется межсетевой экран веб-приложений – Naxsi WAF.

Для включения WAF необходимо выполнить следующие шаги:

1. Скачать основные правила NAXSI.
2. Изменить локацию.

24.4.1 Скачивание правил NAXSI

Скачивание правил NAXSI возможно только с доступом в Интернет. Для скачивания основных правил NAXSI выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Политика Naxsi WAF»** и нажать **кнопку «Сохранение»** (см. Рисунок – Отсутствие правил NAXSI).

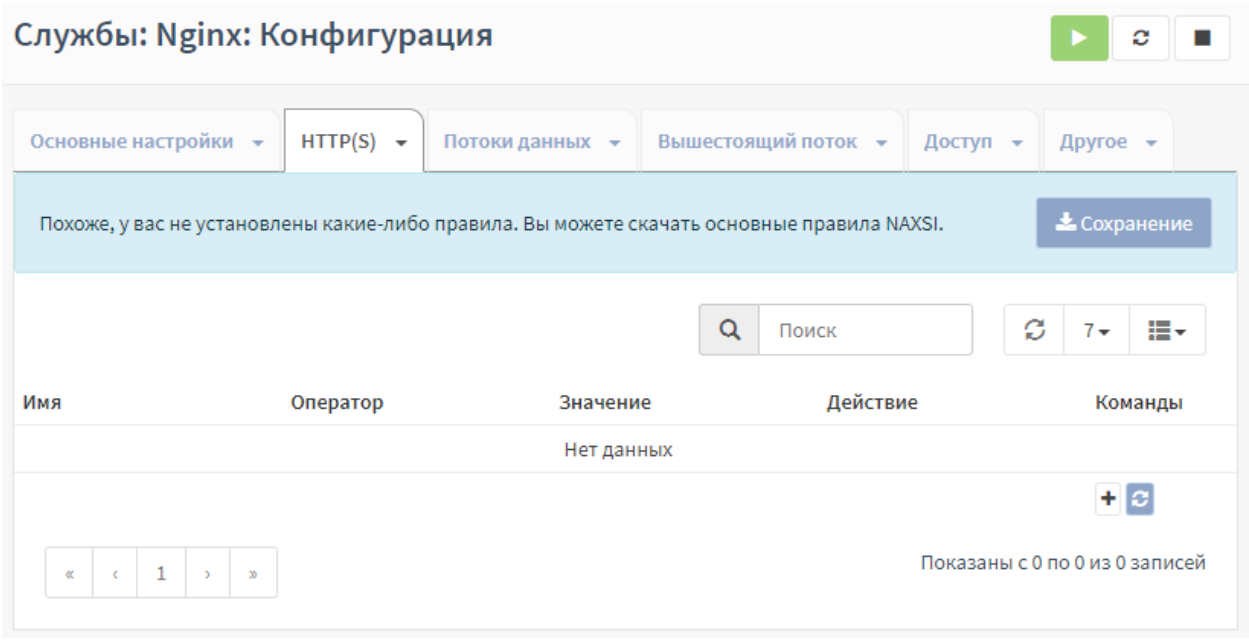


Рисунок – Отсутствие правил NAXSI

3. В открывшейся форме (см. Рисунок – Скачивание правил NAXSI) нажать **кнопку «Принять и скачать»**.

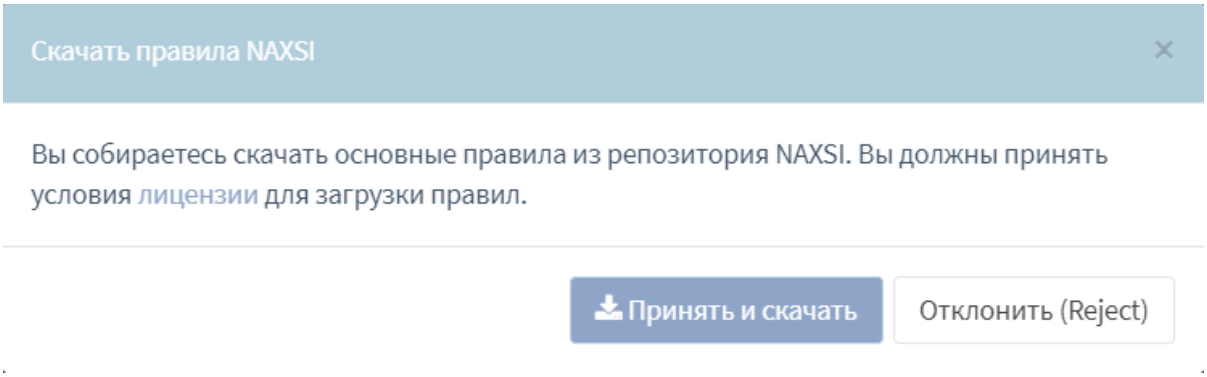


Рисунок – Скачивание правил NAXSI

В результате загрузки будут доступны правила WAF в разделе **«Правило Naxsi WAF»** вкладки **«HTTP(S)»**, правила группируются в политики в разделе **«Политика Naxsi WAF»** вкладки **«HTTP(S)»**.

Политика определяет выполняемое действие в случае выполнения условия.

24.4.2 Изменение локации

Для изменения локации необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Местоположение»** и нажать **кнопку** « ✎ » напротив ранее созданной локации (см. Добавление локации).

3. В открывшейся форме указать значения для следующих параметров:
   - **«Включите правила безопасности»** – флажок установлен;
   - **«Оценка блокирования XSS»** – «4»;
   - **«Оценка блокирования SQL-инъекций»** – «4»;
   - **«Пользовательская политика безопасности»** – все политики из списка;

   остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

В случае установки флажка для параметра **«Обучающий режим»** будет происходить только регистрация срабатывания политик без выполнения выбранного действия.

24.4.3 Проверка работы

После завершения настроек необходимо перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**) и нажать **кнопку «Применить»**.

Для проверки работы WAF необходимо открыть веб-браузер на ПК **«Admin»**, ввести в адресной строке «http://192.168.73.152:8080/hosts.php?a=select&b=union&c=from» и нажать **клавишу «Enter»**. В результате отобразится страница с предупреждением об ограничении доступа (см. Рисунок – Ограничение доступа).

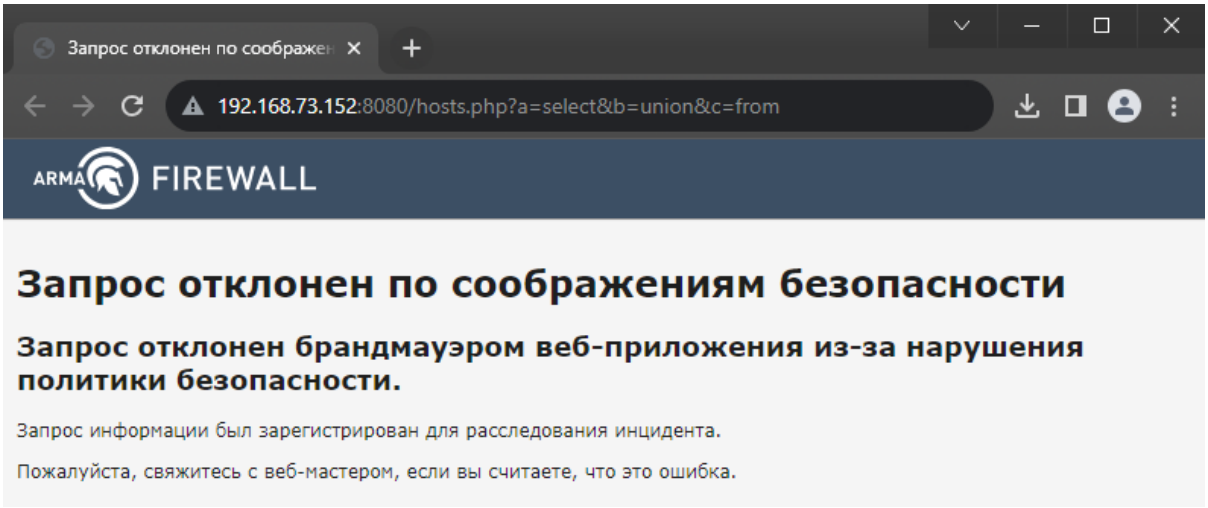


Рисунок – Ограничение доступа

24.5 Заголовки HTTP

Заголовки HTTP позволяют серверу и клиенту обмениваться дополнительной информацией HTTP запросом или ответом.

Существует возможность переопределять заголовки веб-сервера. Для этого необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).

2. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Заголовки безопасности»** и нажать **кнопку** « + ».
3. В открывшейся форме задать параметры политики и нажать **кнопку «Сохранить»**.
4. Раскрыть вкладку **«HTTP(S)»**, нажав **кнопку** « ▼ », выбрать **«Сервер HTTP»** и нажать **кнопку** « ✎ » для ранее созданного сервера (см. Добавление HTTP-сервера).
5. В открывшейся форме выбрать созданную политику в параметре **«Security Header»** и нажать **кнопку «Сохранить»**.
6. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**) и нажать **кнопку «Применить»**.

24.6 Проксирование TCP и UDP

Служба nginx также позволяет обрабатывать TCP и UDP трафик.

В качестве примера будет рассмотрен доступ к веб-серверу **«WebServer 2»** по протоколу RDP.

Для проброса порта необходимо выполнить следующие шаги:

1. Добавить сервер.
2. Добавить группу серверов.
3. Добавить потоковый сервер.

Для прохождения трафика до веб-сервера необходимо выключить параметр **«Блокировать частные сети»** (см. Блок «Общая конфигурация») для интерфейса **«WAN»** и создать общее разрешающее правило МЭ (см. Создание правил межсетевого экранирования) со следующими параметрами:

- **«Действие»** – «Разрешить (Pass)»;
- **«Интерфейс»** – «WAN»;
- **«Протокол»** – «TCP»;
- **«IP-адрес назначения»** – «Этот межсетевой экран»;
- **«Диапазон портов назначения»** – «MS RDP»;
- **«Описание»** – «Доступ по RDP».

24.6.1 Добавление сервера

Для добавления сервера необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Перейти во вкладку **«Вышестоящий поток»** и нажать **кнопку** « ».
3. В открывшейся форме указать данные веб-сервера **«WebServer 2»**:
   - **«Описание»** – «RDP WebServer 2»;
   - **«Сервер»** – «192.168.1.101»;
   - **«Порт»** – «3389»;
   - **«Приоритеты сервера»** – «1»;
   - **«Максимальное количество соединений»** – «10»;
   - **«Максимальное количество неудач»** – «5»;
   - **«Тайм-аут ошибки»** – «10»;

   и нажать **кнопку «Сохранить»**.

24.6.2 Добавление группы серверов

Для добавления группы серверов необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Раскрыть вкладку **«Вышестоящий поток»**, нажав **кнопку** « », выбрать **«Вышестоящий поток»** и нажать **кнопку** « ».
3. В открывшейся форме добавить группу, указав следующие данные:
   - **«Описание»** – «RDP servers»;
   - **«Входы сервера»** – «RDP WebServer 2»;
   - **«Алгоритм балансировки нагрузки»** – «IP Hash»;

   остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

24.6.3 Добавление потокового сервера

Для добавления потокового сервера необходимо выполнить следующие действия:

1. Перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**).
2. Перейти во вкладку **«Потоки данных»** и нажать **кнопку** « ».
3. В открывшейся форме указать данные потокового сервера:
   - **«Порт прослушивания»** – «3389»;

- **«Маршрутизировать с»** – «Вышестоящий поток»;
- **«Вышестоящие серверы»** – «RDP servers»;

остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

24.6.4 Проверка работы

После завершения настроек необходимо перейти в подраздел основных настроек nginx (**«Службы» - «Nginx» - «Конфигурация»**) и нажать **кнопку «Применить»**.

Для проверки работы доступа по протоколу RDP необходимо запустить на ПК **«Admin»** клиент удалённого рабочего стола, указать IP-адрес «192.168.73.152» и выполнить подключение.

25 VPN

VPN – это обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например сети Интернет.

ARMA FW поддерживает работу двух технологий VPN:

- **OpenVPN**;
- **IPsec**.

В **ARMA FW** реализована возможность просмотра конфигурации созданных серверов и клиентов при создании подключения OpenVPN или ГОСТ VPN (см. Диагностика RSPAN).

25.1 OpenVPN

OpenVPN – это реализация технологии VPN, использующая SSL/TLS для защиты туннелируемого трафика. В работе OpenVPN используется механизм TUN/TAP, реализованный в виде загружаемого драйвера ядра.

ARMA FW поддерживает работу OpenVPN в режимах **«сеть - сеть»** и **«узел - сеть»**.

При настройке подключения OpenVPN рекомендуется придерживаться следующих криптографических установок:

- **«Пиринговая сеть (Общий ключ)»**:
  - **«Алгоритм шифрования»** – «AES-256-CBC (256 bit key, 128 bit block)», «AES-128-CBC (128 bit key, 128 bit block)»;
  - **«Дайджест-алгоритм аутентификации»** – «SHA256 (256-bit)», «SHA512 (512-bit)»;
- **«Пиринговая сеть (SSL/TLS)»**:
  - **«Алгоритм шифрования»** – «AES-256-CBC (256 bit key, 128 bit block)»;
  - **«Дайджест-алгоритм аутентификации»** – «SHA256 (256-bit)», «SHA512 (512-bit)»;
- **«Удаленный доступ (SSL/TLS)»**:
  - **«Алгоритм шифрования»** – «AES-256-GCM (256 bit key, 128 bit block, TLS client/server mode only)»;
  - **«Дайджест-алгоритм аутентификации»** – «SHA256 (256-bit)»;
- **«Удаленный доступ (аутентификация пользователя)»**:
  - **«Алгоритм шифрования»** – «AES-256-GCM (256 bit key, 128 bit block, TLS client/server mode only)»;
  - **«Дайджест-алгоритм аутентификации»** – «SHA256 (256-bit)»;

- **«Удаленный доступ (SSL/TLS+аутентификация пользователя)»**:
  - **«Алгоритм шифрования»** – «AES-256-GCM (256 bit key, 128 bit block, TLS client/server mode only)»;
  - **«Дайджест-алгоритм аутентификации»** – «SHA256 (256-bit)».

Для режимов сервера **«Удаленный доступ (SSL/TLS)»**, **«Удаленный доступ (аутентификация пользователя)»** и **«Удаленный доступ (SSL/TLS+аутентификация пользователя)»** рекомендуется не включать сжатие туннельных пакетов.

25.1.1 Настройка OpenVPN в режиме «сеть - сеть»

В качестве примера настройки OpenVPN в режиме **«сеть - сеть»** будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки OpenVPN в режиме «сеть - сеть»).

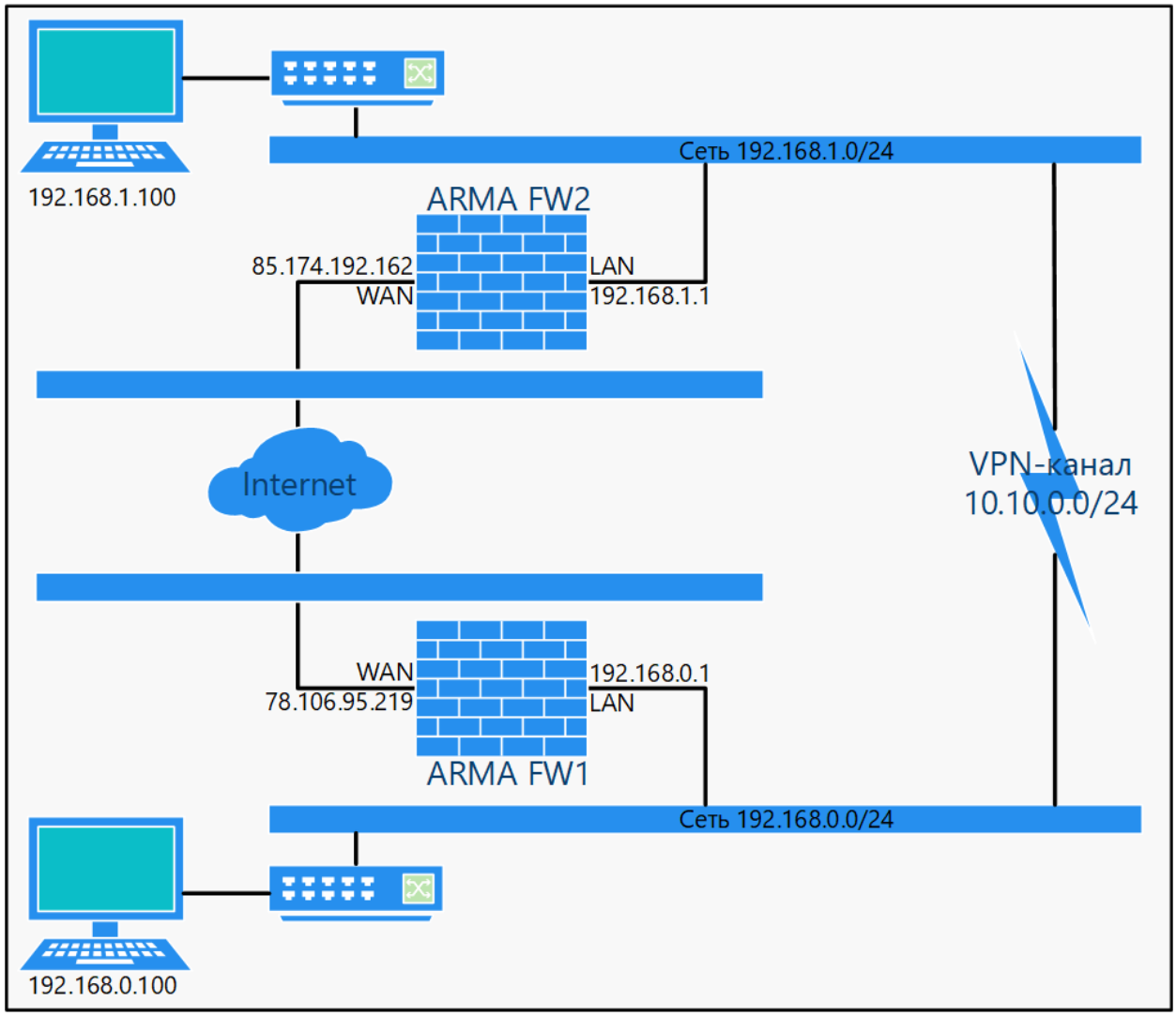


Рисунок – Схема стенда для настройки OpenVPN в режиме «сеть - сеть»

Перед началом настройки необходимо создать правила МЭ, разрешающие трафик ICMP, для интерфейсов **«[WAN]»** каждого **ARMA FW** (см. Создание правил межсетевого экранирования) и убедиться в следующем:

- интерфейсы «WAN» каждого **ARMA FW** используют IP-адреса доступные друг другу при команде «ping»;
- сегмент интерфейса «LAN» каждого **ARMA FW** использует уникальную сеть, в примере используются сети «192.168.0.0/24» и «192.168.1.0/24».

Примечание:

При использовании динамической маршрутизации OSPF в туннеле OpenVPN необходимо учитывать следующие особенности:

- при настройке сервера и клиента OpenVPN в режимах **«Пиринговая сеть (Общий ключ)»** или **«Пиринговая сеть (SSL/TLS)»** для параметра **«Режим работы устройства»** выбрать значение «tun», а поля параметров **«Локальная сеть IPv4»** и **«Удаленная сеть IPv4»** не должны быть заполнены;
- при настройке сервера OpenVPN в режиме **«Пиринговая сеть (SSL/TLS)»** в блоке **«Настройки клиента»** установить флажок для параметра **«Топология сети»**.

25.1.1.1 Настройка на ARMA FW1

Для настройки OpenVPN на **ARMA FW1** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN» - «OpenVPN» - «Серверы»**) и нажать **кнопку «+Добавить»** для добавления нового сервера.
2. В открывшейся форме указать параметры согласно таблице (см. Таблица «Параметры OpenVPN ARMA FW1») и нажать **кнопку «Сохранить»**. Не указанные в таблице параметры оставить по умолчанию.

Таблица «Параметры OpenVPN ARMA FW1»

Параметр	Значение параметра
Описание	OpenVPN peer 1
Режим сервера	Пиринговая сеть (Общий Ключ)
Интерфейс	WAN
Локальный порт	1194
Совместно использующийся ключ	Флажок установлен
Туннельная сеть IPv4	10.10.0.0/24

Параметр	Значение параметра
Локальная сеть IPv4	192.168.0.0/24
Удаленная сеть IPv4	192.168.1.0/24
Сжатие	Включено с использованием адаптивного сжатия

25.1.1.2 Копирование ключа

После создания сервера в параметре **«Совместно использующийся Ключ»** будет отображён сгенерированный ключ (см. Рисунок – Совместно используемый ключ OpenVPN).

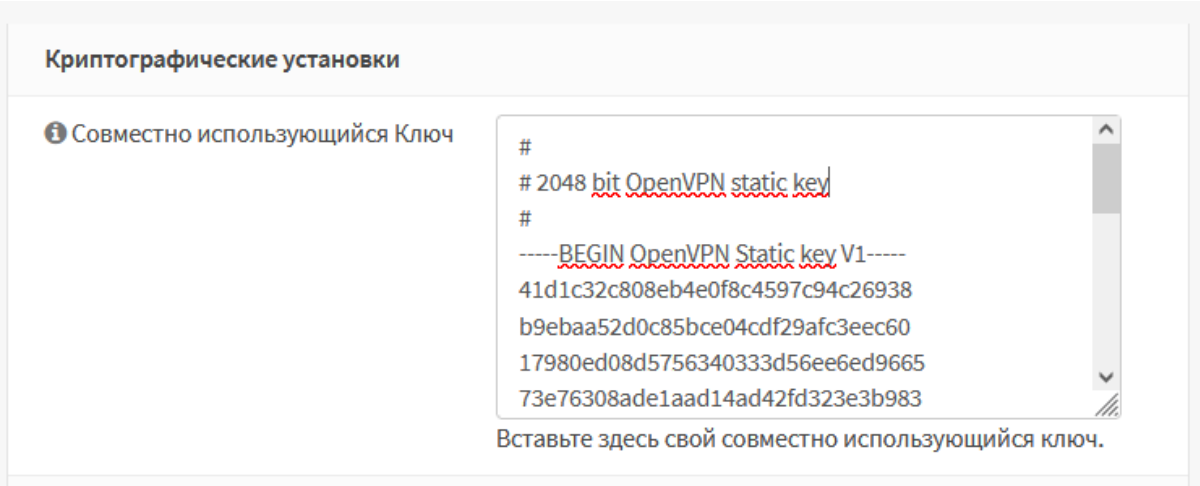


Рисунок – Совместно используемый ключ OpenVPN

Для копирования ключа необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN» - «OpenVPN» - «Серверы»**) и нажать **кнопку** « » напротив созданного сервера.
2. В открывшейся форме перейти в блок настроек **«Криптографические установки»** и скопировать в буфер обмена содержимое значения параметра **«Совместно использующийся Ключ»**.

25.1.1.3 Настройка на ARMA FW2

Для настройки OpenVPN на **ARMA FW2** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки клиента OpenVPN (**«VPN» - «OpenVPN» - «Клиенты»**) и нажать **кнопку «+Добавить»** для добавления нового клиента.
2. В открывшейся форме указать параметры согласно списку ниже и нажать **кнопку «Сохранить»**:
   - **«Описание»** – «OpenVPN peer 2»;

- **«Режим сервера»** – «Пиринговая сеть (Общий Ключ)»;
- **«Интерфейс»** – «WAN»;
- **«Удаленный сервер, Хост или адрес»** – «78.106.95.219»;
- **«Удаленный сервер, Порт»** – «1194»;
- **«Описание»** – «OpenVPN peer 2»;
- **«Совместно использующийся ключ»** – Флажок не установлен. Вставлено значение ранее скопированного ключа (см. раздел Копирование ключа);
- **«Туннельная сеть IPv4»** – «10.10.0.0/24»;
- **«Удаленная сеть IPv4»** – «192.168.0.0/24»;
- **«Сжатие»** – «Включено с использованием адаптивного сжатия».

Настройки, не указанные в списке оставить по умолчанию.

В результате настройки OpenVPN будет создан VPN-канал со следующими характеристиками:

- SSL/TLS используется;
- туннелируемый трафик инкапсулируется в UDP-пакеты;
- демон OpenVPN обрабатывает подключения только на IP-адрес, присвоенный WAN-адаптеру;
- сертификаты не используются;
- аутентификация по логину/паролю не используется;
- аутентификация TLS не используется;
- сжатие данных используется.

25.1.1.4 Создание правил МЭ

Для корректной работы VPN-туннеля необходимо настроить правила МЭ:

- на **ARMA FW1** правило для разрешения OpenVPN трафика и трафика из сети «192.168.1.0/24»;
- на **ARMA FW2** правило для разрешения трафика из сети «192.168.0.0/24».

Создание правил МЭ описано в разделе Создание правил межсетевого экранирования настоящего руководства, необходимо создать правила с параметрами, указанными в списке. Не указанные в списке параметры следует оставить по умолчанию.

- **ARMA FW1 (правило №1)**:
  - **«Интерфейс»** – «[WAN]»;

- **«Действие»** – «Разрешить (Pass)»;
- **«Быстрая проверка»** – «Включено»;
- **«Версии TCP/IP»** – «IPv4»;
- **«Протокол»** – «UDP»;
- **«Отправитель»** – «Единственный хост или сеть, 85.174.192.162»;
- **«Диапазон портов назначения»** – «OpenVPN»;
- **«Описание»** – «Allow VPN»;

- **ARMA FW1 (правило №2)**:
  - **«Интерфейс»** – «[OpenVPN]»;
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «Любой»;
  - **«Отправитель»** – «Единственный хост или сеть, 192.168.1.0/24»;
  - **«Диапазон портов назначения»** – «Любой»;
  - **«Описание** – «Allow VPN Traffic»;
- **ARMA FW2**:
  - **«Интерфейс»** – «[OpenVPN]»;
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка»** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «Любой»;
  - **«Отправитель»** – «Единственный хост или сеть, 192.168.0.0/24»;
  - **«Диапазон портов назначения»** – «Любой»;
  - **«Описание»** – «Allow VPN Traffic».

После применения правил МЭ необходимо убедиться в работе канала, для этого на любом из **ARMA FW** перейти в подраздел статусов соединения OpenVPN (**«VPN» - «OpenVPN» - «Статус соединения»**), значение столбца **«Статус»** должно быть «up» (см. Рисунок – Статус соединения OpenVPN).

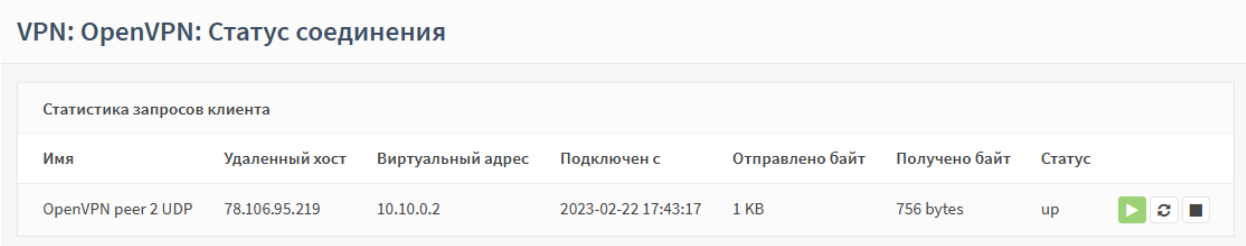


Рисунок – Статус соединения OpenVPN

25.1.2 Настройка OpenVPN в режиме «узел - сеть»

В качестве примера настройки OpenVPN в режиме **«узел - сеть»** будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки OpenVPN в режиме «клиент - сеть»), авторизация пользователей осуществляется согласно локальной БД **ARMA FW**.

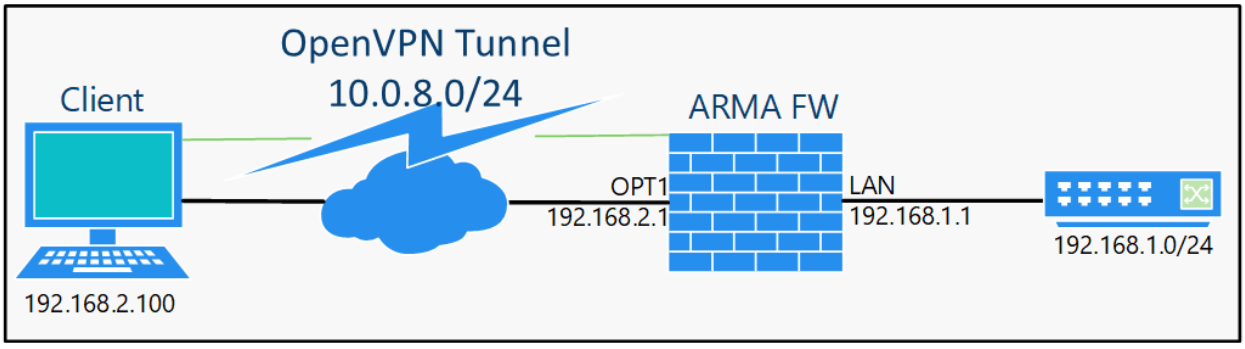


Рисунок – Схема стенда для настройки OpenVPN в режиме «клиент - сеть»

Для настройки OpenVPN в режиме **«узел - сеть»** необходимо выполнить следующие шаги:

1. Создать доверенный центр сертификации.
2. Создать сертификат сервера.
3. Создать пользовательскую УЗ и клиентский сертификат.
4. Настроить **ARMA FW** в качестве сервера OpenVPN.

25.1.2.1 Создание доверенного центра сертификации

Для создания доверенного центра сертификации необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица «Значения параметров центра сертификации»), не указанные параметры оставить по умолчанию.

4. Нажать **кнопку «Сохранить»**.

Таблица «Значения параметров центра сертификации»

Параметр	Значение
Описательное имя	ARMA CA
Метод	Создать внутренний центр сертификации
Время существования (дни)	365
Код страны	RU (Russia)
Область	Moscow
Город	Moscow
Организация	InfoWatch
Эл. почта	admin@infowatch.ru
Стандартное имя	ARMA CA

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Эл. почта»**, **«Стандартное имя»** указаны справочно.

25.1.2.2 Создание сертификата сервера

Для создания сертификата сервера необходимо выполнить следующие действия:

1. Перейти в подраздел сертификатов (**«Система» - «Доверенные сертификаты» - «Сертификаты»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица «Значения параметров сертификата»), не указанные параметры оставить по умолчанию.
4. Нажать **кнопку «Сохранить»**.

Таблица «Значения параметров сертификата»

Параметр	Значение
Метод	Создать внутренний сертификат
Описательное имя	OpenVPN cert
Центр сертификации	ARMA CA
Тип	Сертификат сервера
Стандартное имя	OpenVPN cert

Параметры **«Описательное имя»** и **«Стандартное имя»** указаны справочно.

25.1.2.3 Создание пользовательской УЗ и клиентского сертификата

Создание пользовательской УЗ описано в разделе Учётные записи и права доступа настоящего руководства.

Для создания пользовательского сертификата необходимо выполнить следующие действия:

1. Открыть форму создания сертификата:
   - при создании УЗ – установить флажок для параметра **«Сертификат»** и нажать **кнопку «Сохранить»**;
   - для созданной УЗ – нажать **кнопку** « + » в параметре **«Сертификаты пользователя»**.
2. В открывшейся форме выбрать:
   - в параметре **«Метод»** – **«Создать внутренний сертификат»**;
   - в параметре **«Центр сертификации»** – **«ARMA CA»**;

   и нажать **кнопку «Сохранить»**.
3. Нажать **кнопку «Сохранить»** в форме редактирования УЗ.

25.1.2.4 Настройка ARMA FW

Для настройки **ARMA FW** в качестве сервера OpenVPN необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов OpenVPN (**«VPN» - «OpenVPN» - «Серверы»**) и нажать **кнопку «+Добавить»** для добавления нового сервера.
2. В открывшейся форме указать параметры согласно списку и нажать **кнопку «Сохранить»**:
   - **«Описание»** – «OpenVPN Server»;
   - **«Режим сервера»** – «Удаленный доступ (SSL/TLS + аутентификация пользователя)»;
   - **«Сервер для аутентификации»** – «Локальная база данных»;
   - **«Интерфейс»** – «OPT1»;
   - **«Локальный порт»** – «1194»;
   - **«Центр сертификации пиров»** – «ARMA CA»;
   - **«Сертификат сервера»** – «OpenVPN cert (ARMA CA)»;
   - **«Туннельная сеть IPv4»** – «10.0.8.0/24»;
   - **«Локальная сеть IPv4»** – «192.168.1.0/24»;

- **«Сжатие»** – «Выключено Без сжатия»;
- **«DNS-серверы»** – Флажок установлен, указывается IP-адрес DNS сервера для локальной сети.

Настройки, не указанные в списке оставить по умолчанию.

После создания OpenVPN сервера необходимо создать правила МЭ для интерфейсов **«[OPT1]»** и **«[OpenVPN]»** с параметрами, указанными в списке ниже.

Создание правил МЭ описано в разделе Создание правил межсетевого экранирования настоящего руководства.

- **Правило для интерфейса [OPT1]**:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка»** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «UDP»;
  - **«Отправитель»** – «OPT 1 сеть»;
  - **«Диапазон портов назначения»** – «OpenVPN»;
  - **«Описание»** – «Allow VPN»;
- **Правило для интерфейса [OpenVPN]**:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка»** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «Любой»;
  - **«Отправитель»** – «OpenVPN сеть»;
  - **«Диапазон портов назначения»** – «Любой»;
  - **«Описание»** – «Allow VPN Traffic».

25.1.2.5 Настройка клиента

Для настройки клиента необходим конфигурационный файл OpenVPN.

Для создания конфигурационного файла необходимо выполнить следующие действия:

1. Перейти в подраздел экспорта настроек клиента (**«VPN» - «OpenVPN» - «Экспорт настроек клиента»**) (см. Рисунок – Экспорт настроек клиента).

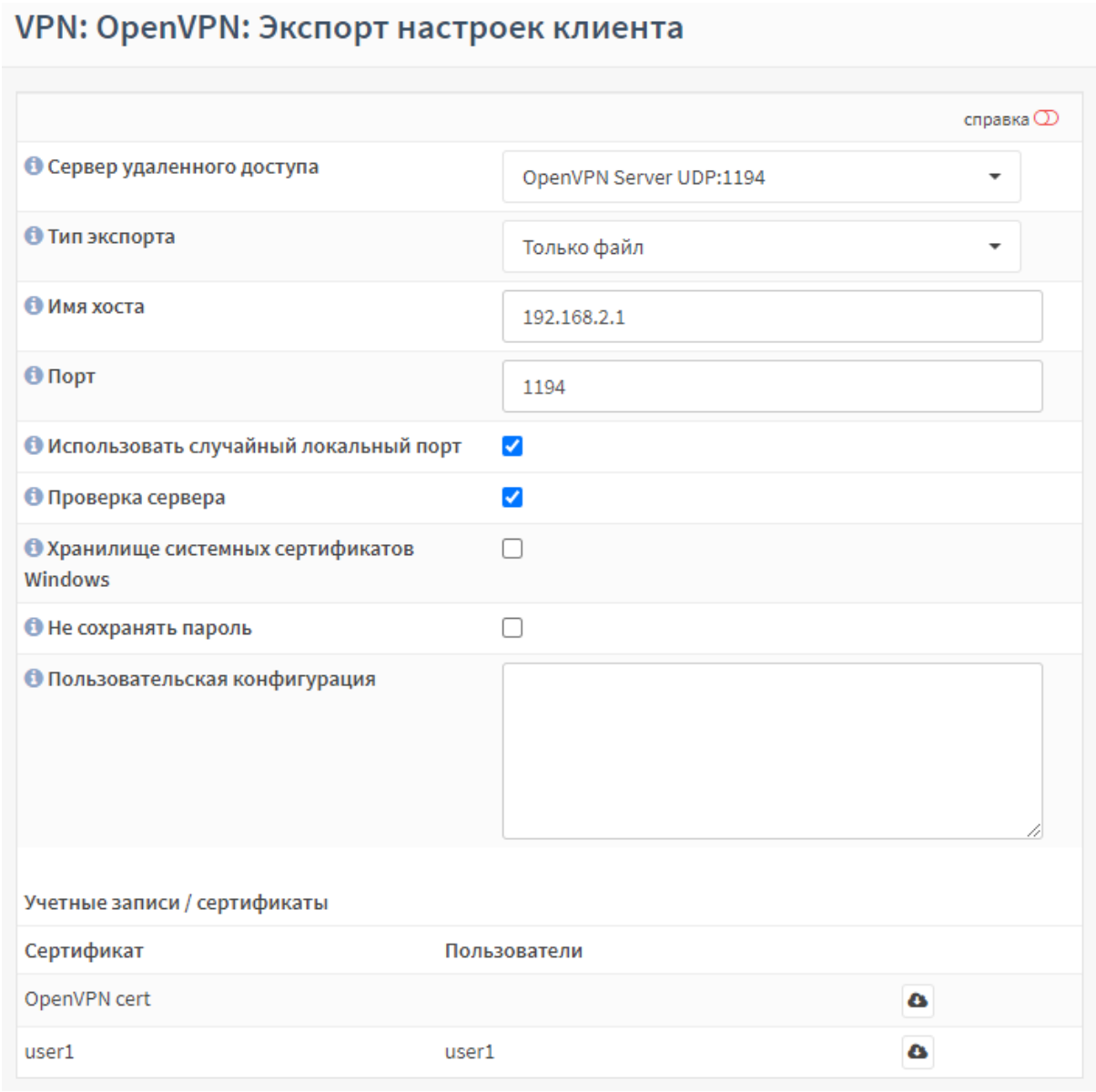


Рисунок – Экспорт настроек клиента

2. Задать параметры для экспорта:
   - **«Сервер удаленного доступа»** – созданный сервер;
   - **«Тип экспорта»** – «Только файл»;
   - **«Имя хоста»** – имя или IP-адрес сервера, в примере «192.168.2.1».
3. Остальные параметры оставить без изменения, нажать **кнопку** « » напротив имени пользователя внизу страницы и сохранить конфигурационный файл, следуя указаниям веб-браузера.

   Экспортированный конфигурационный файл необходимо импортировать в клиентскую часть ПО «OpenVPN» на ПК **«Client»** и выполнить подключение к созданному серверу на **ARMA FW**.

25.2 IPsec

IPsec – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.

ARMA FW поддерживает работу IPsec в режимах «сеть - сеть» и «узел - сеть».

В случае временного отключения и последующего подключения участника IPsec-туннеля, восстановление туннеля происходит автоматически.

> **Примечание:**
>
> При включении IPsec на виртуальных машинах возможны сбои в работе **ARMA FW**.

При настройке первой фазы туннеля IPsec возможно указать действие, выполняемое в случае потери связности с удалённым узлом:

- **«Отсутствует»** – отключает действие;
- **«Сброс»** – закрывает соединение без дальнейших действий;
- **«Удержание»** – перехватывает трафик и повторно инициирует согласование соединения по требованию;
- **«Перезапуск»** – немедленно инициирует согласование соединения.

> **Примечание:**
>
> Для параметра **«Действие закрытия»** следует установить значение «Отсутствует», если узел использует повторную аутентификацию или проверку уникальных идентификаторов.

При настройке фазы 1 туннеля в режиме динамической маршрутизации необходимо в блоке **«Дополнительные параметры»** снять флажок для параметра **«Политика установки»**.

25.2.1 Настройка IPsec в режиме «узел - сеть»

В качестве примера настройки IPsec в режиме **«узел - сеть»**, используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки IPsec в режиме «узел - сеть»).

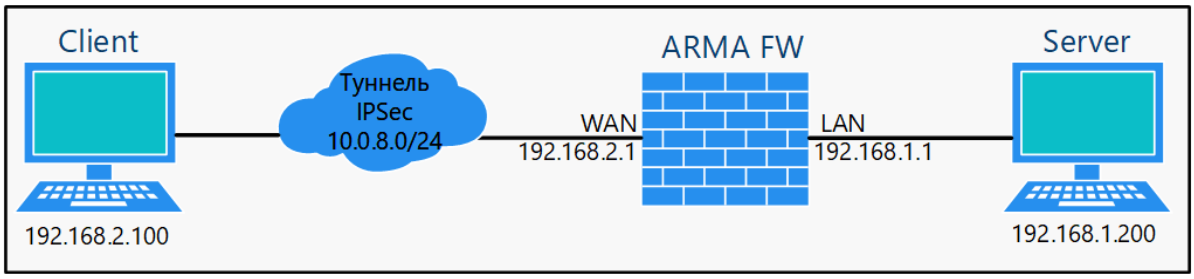


Рисунок – Схема стенда для настройки IPsec в режиме «узел - сеть»

Для настройки IPsec в режиме **«узел - сеть»** необходимо выполнить следующие шаги:

1. Создать внутренний центр сертификации.
2. Создать внутренний сертификат.
3. Настроить мобильный клиент и туннель IPsec.
4. Добавить ключ IPsec.
5. Импортировать сертификат клиенту.
6. Настроить новое сетевое подключение.

25.2.1.1 Шаг 1. Создание внутреннего центра сертификации

В примере доверенный центр сертификации создается с параметрами, приведёнными в таблице (см. Таблица «Значения параметров центра сертификации»), не указанные параметры необходимо оставить по умолчанию.

Таблица «Значения параметров центра сертификации»

Параметр	**Значение**
Описательное имя	ARMA CAF
Метод	Создать внутренний центр сертификации
Длина ключа (бит)	2048
Алгоритм дайджеста	SHA256
Время существования (дни)	365
Код страны	RU (Russia)
Область	MO
Город	Moscow
Организация	IWARMA
Эл. почта	info@infowatch.ru
Стандартное имя	internal-ca

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Эл. почта»**, **«Стандартное имя»** указаны справочно.

Для создания доверенного центра сертификации необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).
2. Нажать **кнопку «+Добавить»**.

3. В открывшейся форме указать параметры из таблицы (см. Таблица «Значения параметров центра сертификации»).
4. Нажать **кнопку «Сохранить»**.

Сертификат созданного центра сертификации необходимо экспортировать, нажав **кнопку «Экспортировать сертификат CA»** (см. Рисунок – Экспорт сертификата CA) в подразделе полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).

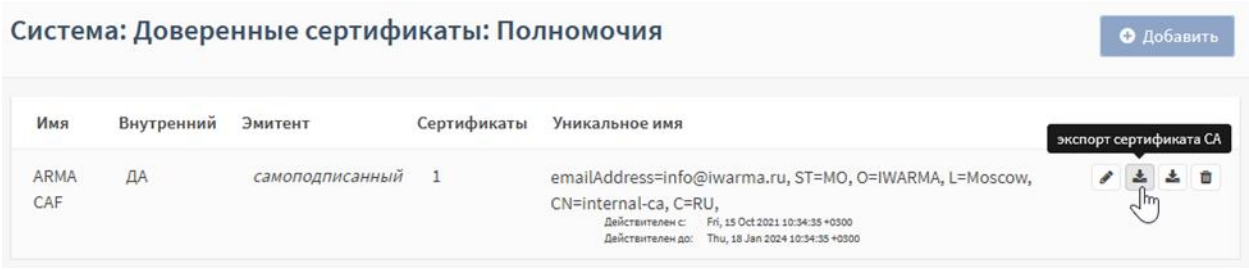


Рисунок – Экспорт сертификата CA

25.2.1.2 Шаг 2. Создать внутренний сертификат

В примере внутренний сертификат создается с параметрами, приведёнными в таблице (см. Таблица «Значения параметров сертификата»), не указанные параметры необходимо оставить по умолчанию.

Таблица «Значения параметров сертификата»

Параметр	Значение
Метод	Создать внутренний сертификат
Описательное имя	IKEv2 cert
Центр сертификации	ARMA CAF
Тип	Сертификат сервера
Время существования (дни)	365
Код страны	RU (Russia)
Область	MO
Город	Moscow
Организация	IWARMA
Эл. почта	info@infowatch.ru
Стандартное имя	IPsecCA
Альтернативные Имена, Тип	IP-адрес
Альтернативные Имена, Значение	IP-адрес WAN интерфейса **ARMA FW**, на схеме – 192.168.2.1

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Эл. почта»**, **«Стандартное имя»** указаны справочно.

Для создания внутреннего сертификата необходимо выполнить следующие действия:

1. Перейти в подраздел сертификатов (**«Система» - «Доверенные сертификаты» - «Сертификаты»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица «Значения параметров сертификата»).
4. Нажать **кнопку «Сохранить»**.

25.2.1.3 Шаг 3. Настройка мобильного клиента и туннеля IPsec

Для поддержки мобильных клиентов IPsec необходимо выполнить следующие действия:

1. Перейти в подраздел настроек мобильных клиентов IPsec (**«VPN» - «IPsec» - «Мобильные клиенты»**) (см. Рисунок – Настройка мобильного клиента IPsec).

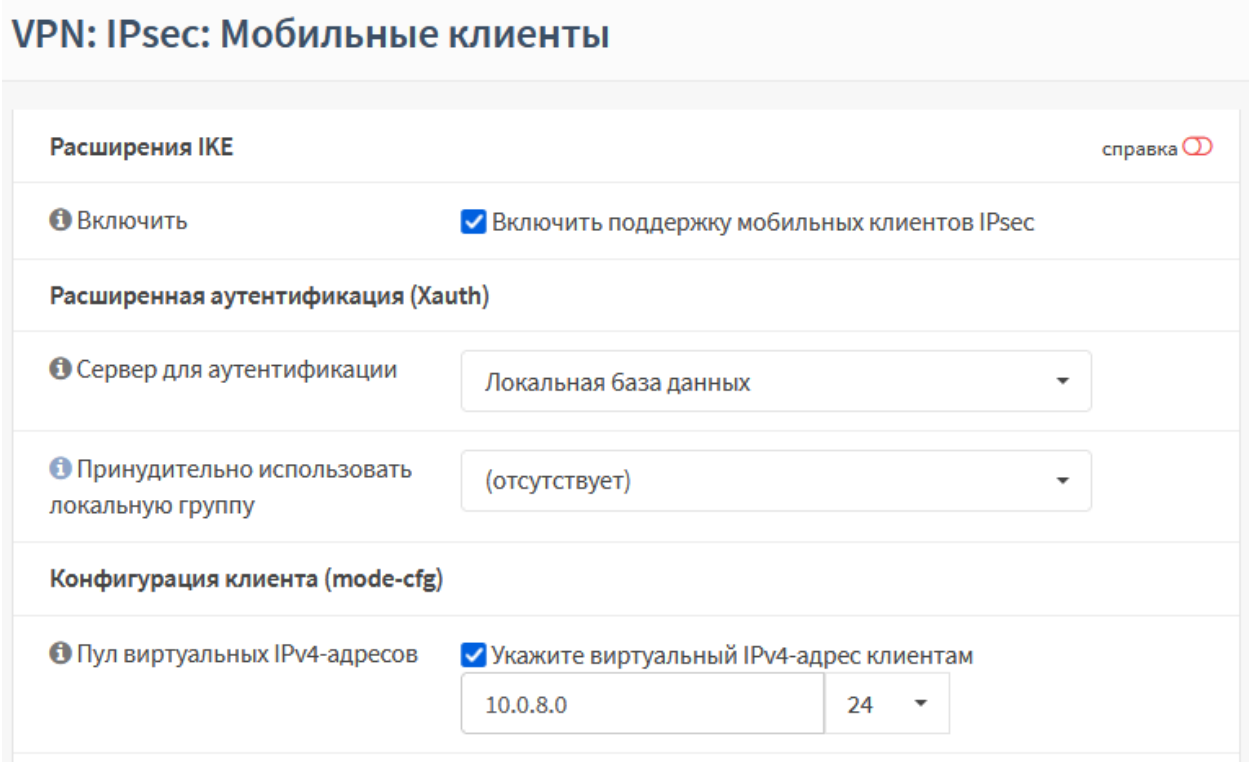


Рисунок – Настройка мобильного клиента IPsec

2. Указать следующие настройки:
   - **«Включить»** – флажок установлен;
   - **«Сервер для аутентификации»** – «Локальная база данных»;

- **«Пул виртуальных IPv4-адресов»** – флажок установлен и указано значение «10.0.8.0/24».

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**. Появится предупреждение о необходимости создания фазы 1 (см. Рисунок – Предупреждение о необходимости создания фазы 1).

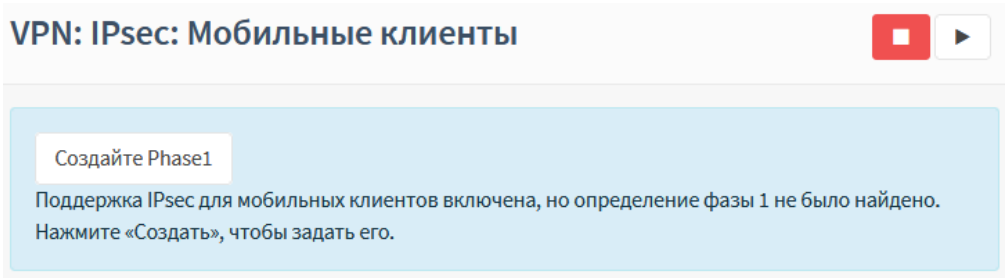


Рисунок – Предупреждение о необходимости создания фазы 1

4. Нажать **кнопку «Создайте Phase1»** и указать следующие настройки в открывшейся форме (см. Рисунок – Настройка фазы 1):

- **«Метод аутентификации»** – «EAP-MSCHAPV2»;
- **«Мой идентификатор»** – «Уникальное имя», «192.168.2.1»;
- **«Алгоритм шифрования»** – «AES, 256»;
- **«Группа ключей DH»** – «2 (1024 bits), 14 (2048 bits)».

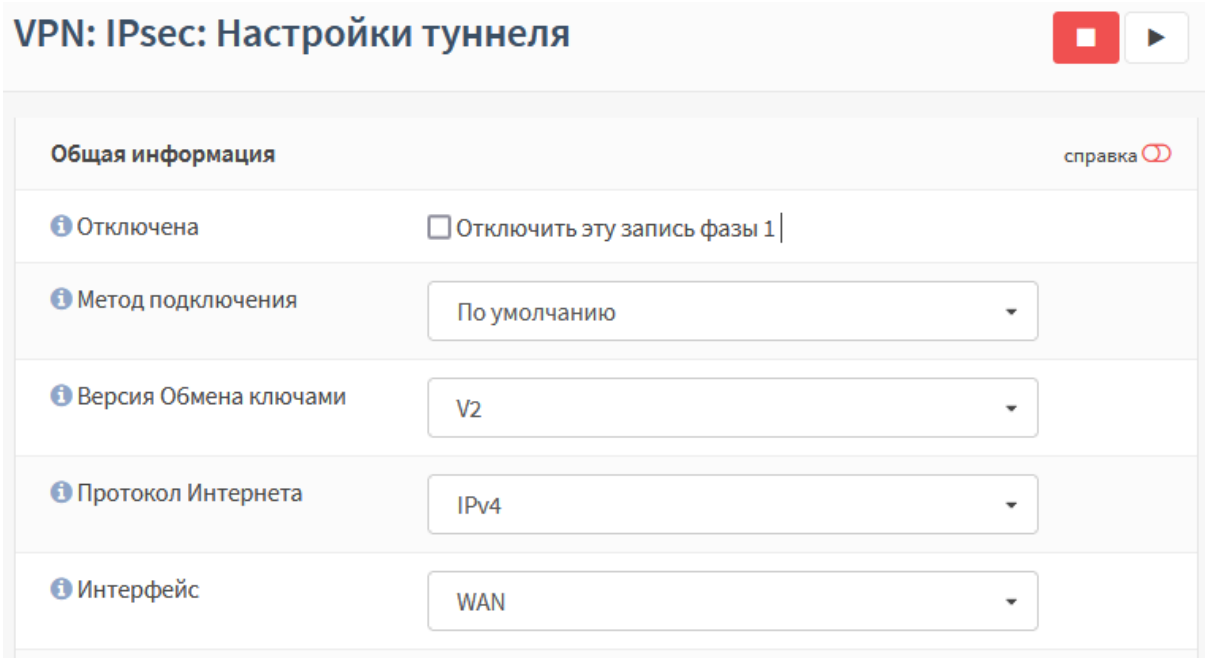


Рисунок – Настройка фазы 1

5. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

6. Для созданной записи нажать **кнопку** « + » (см. Рисунок – Добавление записи фазы 2) для добавления записи фазы 2.

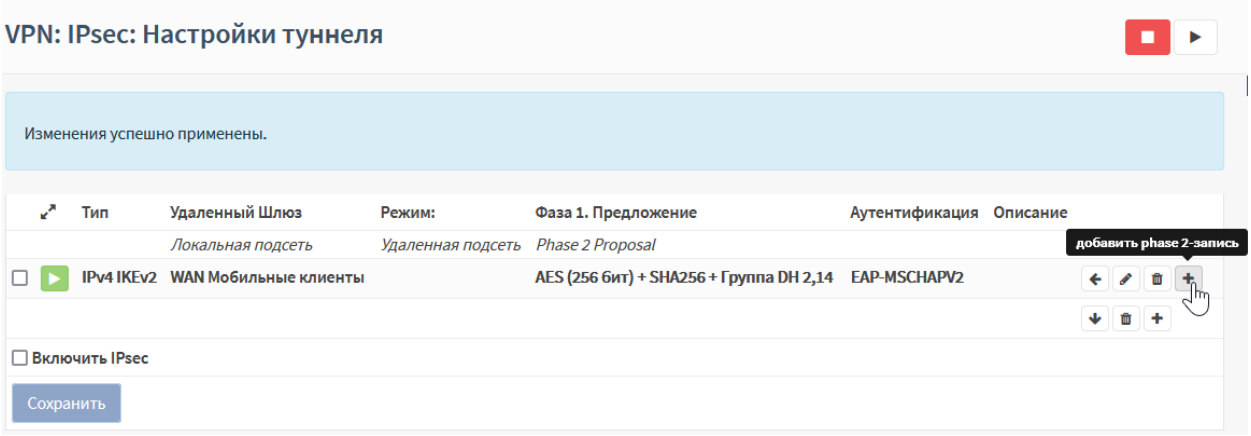


Рисунок – Добавление записи фазы 2

7. Указать следующие настройки в открывшейся форме (см. Рисунок – Настройка фазы 2):
   - **«Алгоритмы шифрования»** – флажки установлены на значениях «AES» и «3DES»;
   - **«Алгоритмы хеша»** – «SHA1».

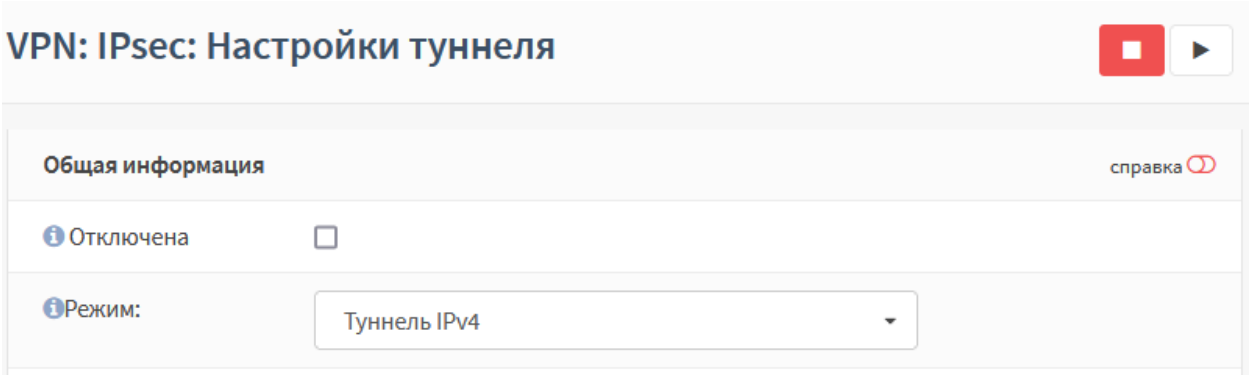


Рисунок – Настройка фазы 2

8. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
9. Установить флажок для параметра **«Включить IPsec»** и нажать **кнопку «Сохранить»**.

25.2.1.4 Шаг 4. Добавление ключа IPsec

Для добавления ключа IPsec необходимо выполнить следующие действия:

1. Перейти в подраздел предварительно выданных ключей (**«VPN» - «IPsec» - «Предварительно выданные ключи»**) и нажать **кнопку «+Добавить»**.

2. Указать следующие настройки в открывшейся форме (см. Рисунок – Добавление ключа IPsec):
   - **«Идентификатор»** – «User»;
   - **«Предварительно выданный ключ»** – «123»;
   - **«Тип»** – «EAP».

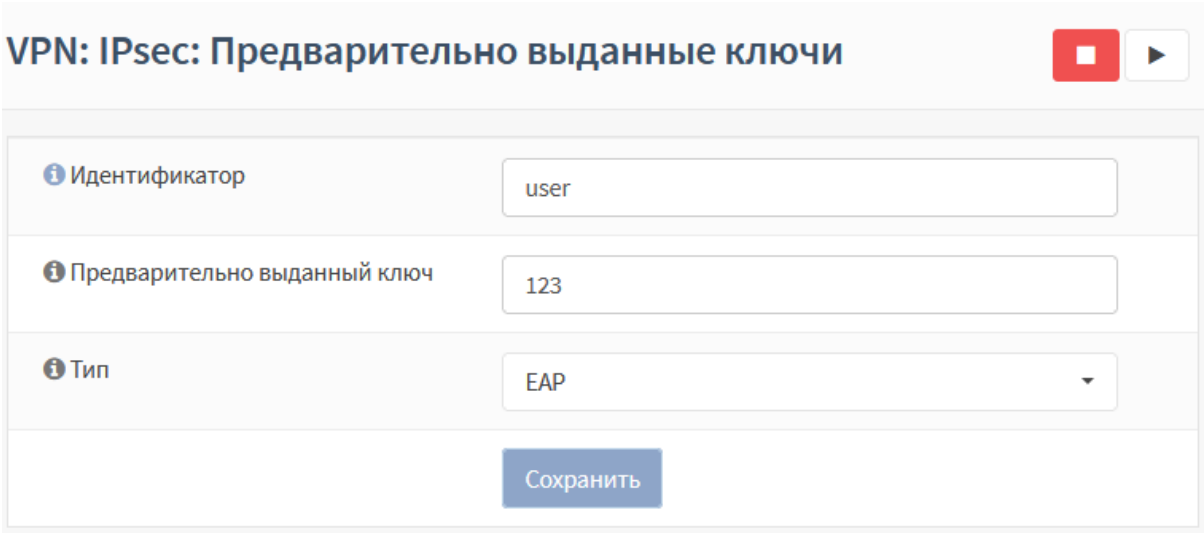


Рисунок – Добавление ключа IPsec

3. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

25.2.1.5 Шаг 5. Импорт сертификата клиенту

Перед началом импорта необходимо создать оснастку для работы с сертификатами, в качестве примера будет использоваться ОС «Windows».

Порядок создания оснастки для работы с сертификатами на ПК **«Client»** необходимо выполнить следующие действия:

1. Нажать **комбинацию клавиш «Win+R»** и в появившемся меню **«Выполнить»** ввести «mmc» и нажать **клавишу «Enter»** для запуска консоли управления.
2. В меню **«Файл»** открывшейся консоли управления выбрать **«Добавить или удалить оснастку...»**.
3. В открывшейся форме добавления и удаления оснасток из столбца **«Доступные оснастки»** выбрать **«Сертификаты»** и нажать **«+Добавить»**.
4. На первом шаге открывшейся оснастки выбрать значение **«Учетной записи компьютера»** и нажать **кнопку «Далее»**, в следующем шаге выбрать значение **«Локальным компьютером»** и нажать **кнопку «Готово»**.
5. Нажать **кнопку «ОК»** в форме добавления и удаления оснасток (см. Рисунок – Создание оснастки для работы с сертификатами на ПК «Client»).

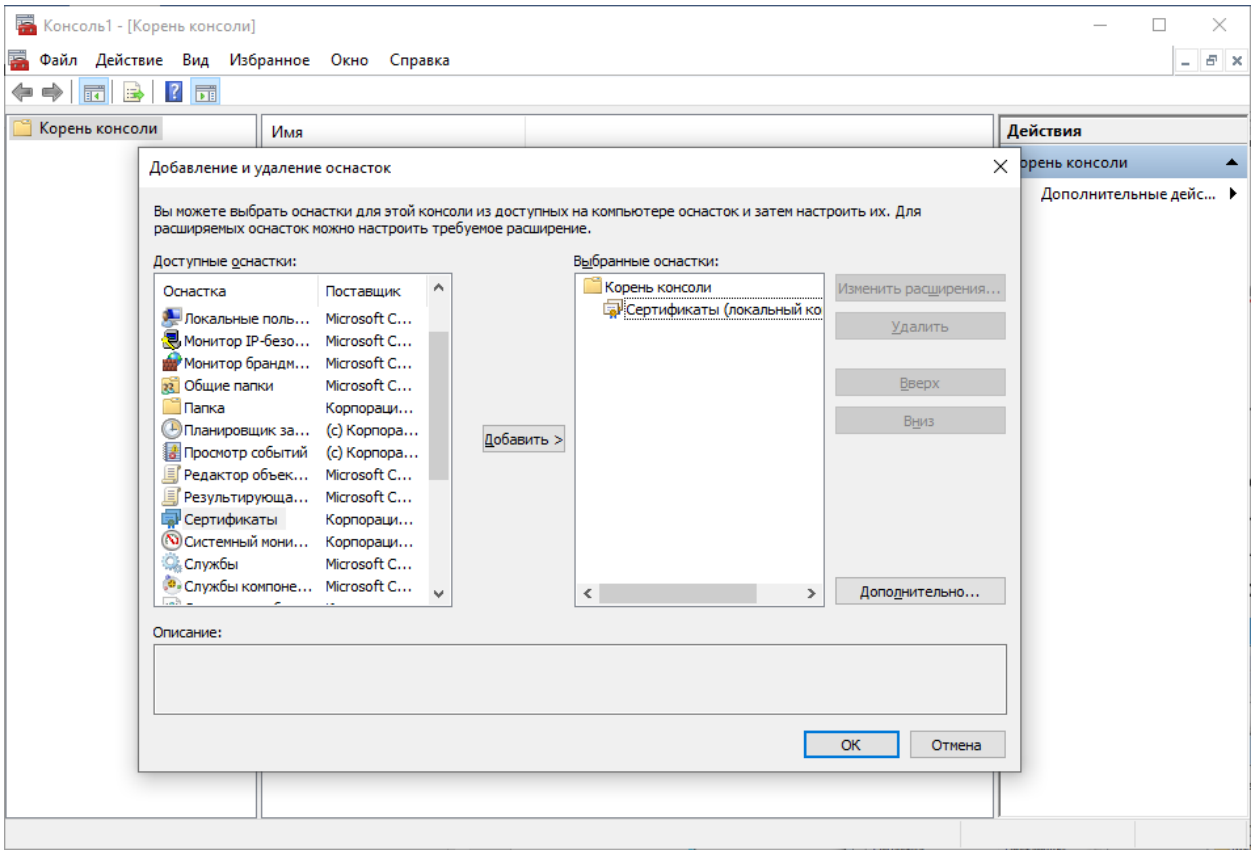


Рисунок – Создание оснастки для работы с сертификатами на ПК «Client»

6. При необходимости сохранить консоль – выбрать значение **«Сохранить»** или **«Сохранить как»** меню **«Файл»**. Рекомендуемое имя **«armacertmngr»**.

Для импорта сертификата, экспортированного на шаге 1 (см. Шаг 1. Создание внутреннего центра сертификации), необходимо выполнить следующие действия:

1. В оснастке для работы с сертификатами перейти в иерархии по пути:
   - **«Сертификаты (локальный компьютер)» - «Доверенные корневые центры сертификации» - «Сертификаты»**.
2. В меню **«Действие»** консоли управления выбрать **«Все задачи»**, а затем **«Импорт»**.
3. Следовать указаниям мастера импорта сертификатов, выбрав сертификат, экспортированный на шаге 1 (см. Шаг 1. Создание внутреннего центра сертификации).

25.2.1.6 Шаг 6. Настройка нового сетевого подключения.

В качестве примера настройки нового сетевого подключения будет использоваться создание и настройка подключения в ОС «Windows».

Для создания и настройки VPN подключения на ПК **«Client»** необходимо выполнить следующие действия:

1. Перейти в **«Панель управления»**, установить режим просмотра **«Мелкие значки»**, выбрать раздел **«Центр управления сетями и общим доступом»** и нажать **«Создание и настройка нового подключения или сети»**.
2. В открывшемся мастере выбрать **«Подключение к рабочему месту»** и нажать **кнопку «Далее»**.
3. На следующем шаге выбрать **«Использовать мое подключение к интернету (VPN)»**, а в следующем шаге задать настройки подключения (см. Рисунок – Настройка нового сетевого подключения):
   - **«Адрес в Интернете»** – «192.168.2.1»;
   - **«Имя объекта назначения»** – «VPN-подключение»;

   и нажать **кнопку «Создать»**.

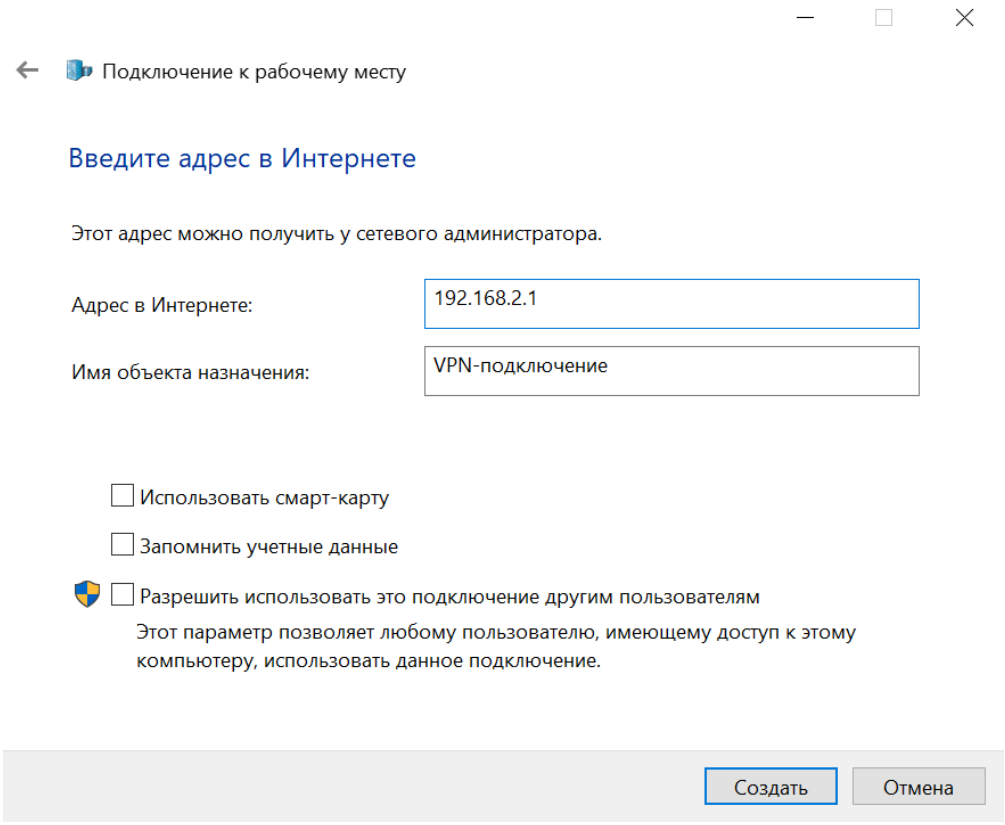


Рисунок – Настройка нового сетевого подключения

4. Перейти в **«Панель управления»**, установить режим просмотра **«Мелкие значки»**, выбрать раздел **«Центр управления сетями и общим доступом»**.
5. Выбрать **«Изменение параметров адаптера»**, нажать **правой кнопкой мыши** на созданное ранее подключение **«VPN-подключение»** и выбрать **«Свойства»**.
6. Перейти во вкладку **«Безопасность»** (см. Рисунок – Настройка параметров сетевого подключения) и указать следующие параметры:
   - **«Тип VPN»** – «IKEv2»;

- **«Шифрование данных»** – «обязательное (отключиться, если нет шифрования)»;
- **«Проверка подлинности»** – флажок установлен «Microsoft: защищённый пароль (EAP-MSCHAP v2) (шифрование включено)»;

и нажать **кнопку «ОК»**.

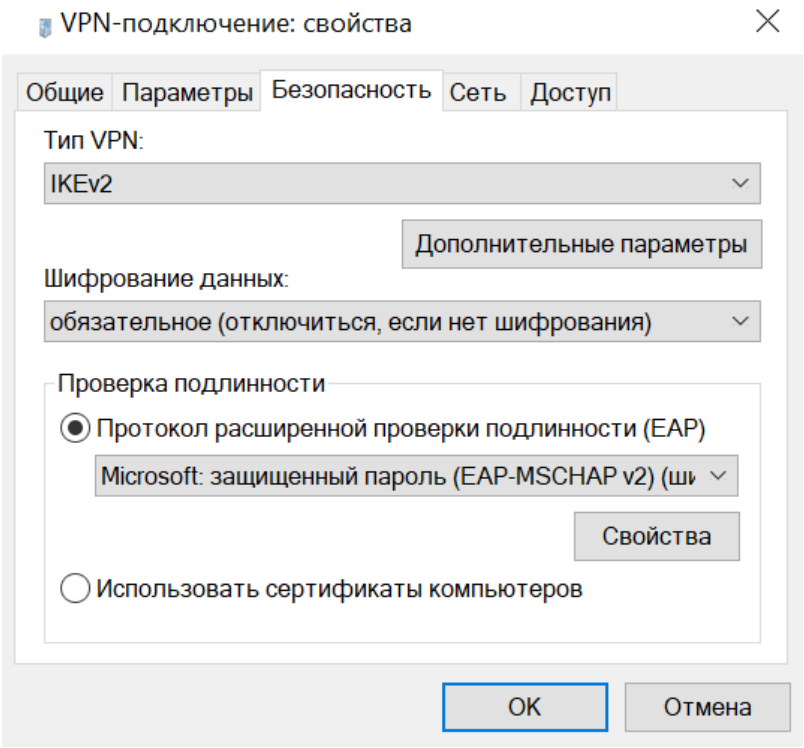


Рисунок – Настройка параметров сетевого подключения

Для подключения VPN соединения необходимо нажать **правой кнопкой мыши** на созданное ранее подключение **«VPN-подключение»** и выбрать **«Подключить»**. Ввести аутентификационные данные, созданные на шаге 4 (см. Шаг 4. Добавление ключа IPsec) и нажать **кнопку «ОК»** для подключения.

25.2.1.7 Проверка подключения

Для проверки успешного подключения необходимо убедиться в соответствующих записях в следующих подразделах:

1. Статуса аренды адресов (**«VPN» - «IPsec» - «Статус аренды адресов»**) (см. Рисунок – «VPN» - «IPsec» - «Статус аренды адресов»).

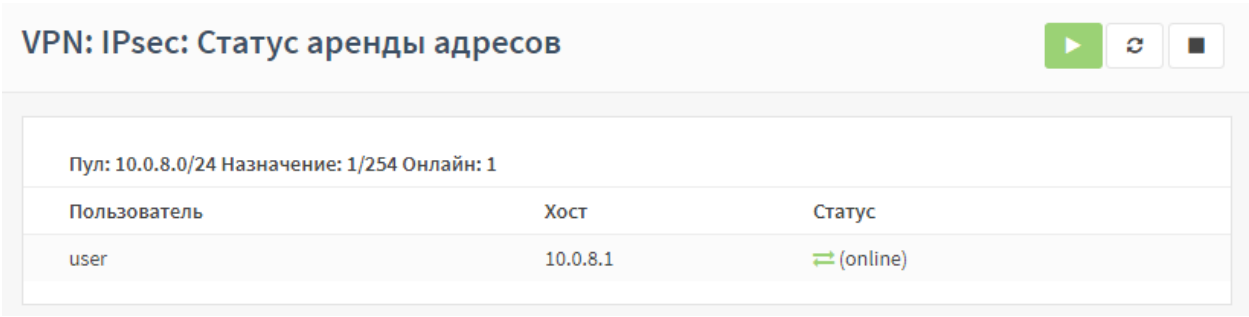


Рисунок – «VPN» - «IPsec» - «Статус аренды адресов»

2. Базы данных безопасных ассоциаций (**«VPN» - «IPsec» - «База данных безопасных ассоциаций (SAD)»**) (см. Рисунок – «VPN» - «IPsec» - «База данных безопасных ассоциаций (SAD)»).

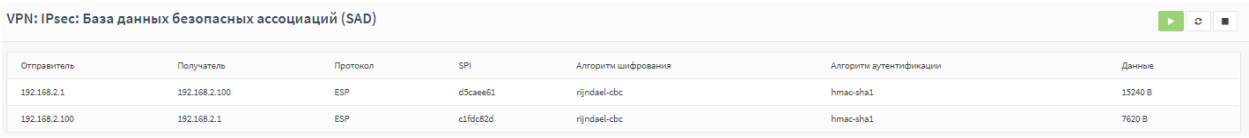


Рисунок – «VPN» - «IPsec» - «База данных безопасных ассоциаций (SAD)»

3. Базы данных политик безопасности (**«VPN» - «IPsec» - «База данных политик безопасности (SPD)»**) (см. Рисунок – «VPN» - «IPsec» - «База данных политик безопасности (SPD)»).

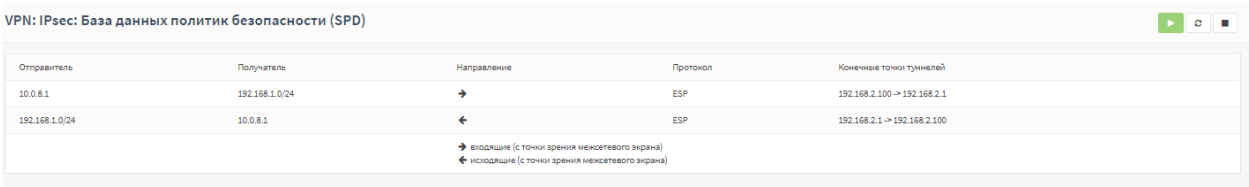


Рисунок – «VPN» - «IPsec» - «База данных политик безопасности (SPD)»

25.2.2 Настройка IPsec в режиме «сеть - сеть»

В качестве примера настройки IPsec в режиме **«сеть - сеть»**, используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки IPsec в режиме «сеть - сеть»).

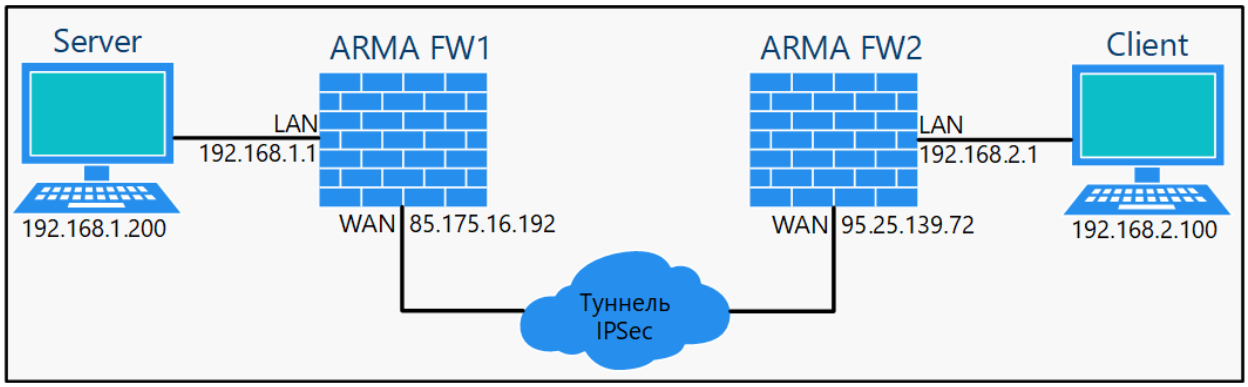


Рисунок – Схема стенда для настройки IPsec в режиме «сеть - сеть»

Для настройки IPsec в режиме **«сеть - сеть»** необходимо выполнить следующие шаги:

1. Добавить ключ IPsec.
2. Настроить туннель IPsec на **ARMA FW1**.
3. Настроить туннель IPsec на **ARMA FW2**.

Примечание:

В случае необходимости, при настройке записи фазы 2, в режимах «Туннель IPv4» или «Туннель IPv6», в блоке настроек **«Общая информация»** возможно выбрать протокол, трафик по которому будет направлен в туннель. При выборе протоколов «TCP» или «UDP» и типа сети «Адрес» или «Сеть» в блоках настроек **«Локальная сеть»** и **«Удаленная сеть»** дополнительно появятся параметры **«Диапазон портов источника»** и **«Диапазон портов назначения»** соответственно.

Примечание:

В случае перезагрузки одного из **ARMA FW** автоматически осуществится перезапуск IPsec на обоих **ARMA FW** для дальнейшей корректной работы.

25.2.2.1 Шаг 1. Добавление ключа IPsec

Для добавления ключа IPsec необходимо выполнить следующие действия:

1. На ПК **«Server»** в веб-интерфейсе **ARMA FW1** перейти в подраздел предварительно выданных ключей (**«VPN» - «IPsec» - «Предварительно выданные ключи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Добавление ключа IPsec) указать следующие параметры:
   - **«Идентификатор»** – «ANY»;
   - **«Предварительно выданный ключ»** – «12345»;
   - **«Тип»** – «PSK».

Рисунок – Добавление ключа IPsec

3. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

Параметры созданного ключа необходимо будет указать при настройке туннеля IPsec на **ARMA FW1** и **ARMA FW2**.

25.2.2.2 Шаг 2. Настройка туннеля IPsec на ARMA FW1

Для настройки туннеля IPsec **ARMA FW1** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки туннелей IPsec (**«VPN» - «IPsec» - «Настройки туннеля»**) и нажать **кнопку** « + » для создания фазы 1.
2. Указать следующие настройки в открывшейся форме (см. Рисунок – Настройка фазы 1 на ARMA FW1):
   - **«Удалённый шлюз»** – IP-адрес WAN интерфейса **ARMA FW2**, в примере «95.25.139.72»;
   - **«Описание»** – «peer 1»;
   - **«Предварительно выданный ключ»** – «12345»;
   - **«Алгоритм шифрования»** – «AES, 256»;
   - **«Группа ключей DH»** – «14 (2048 bits)»;
   - **«Отключить MOBIKE»** – флажок установлен;
   - **«Обнаружение недоступных пиров»** – флажок установлен.

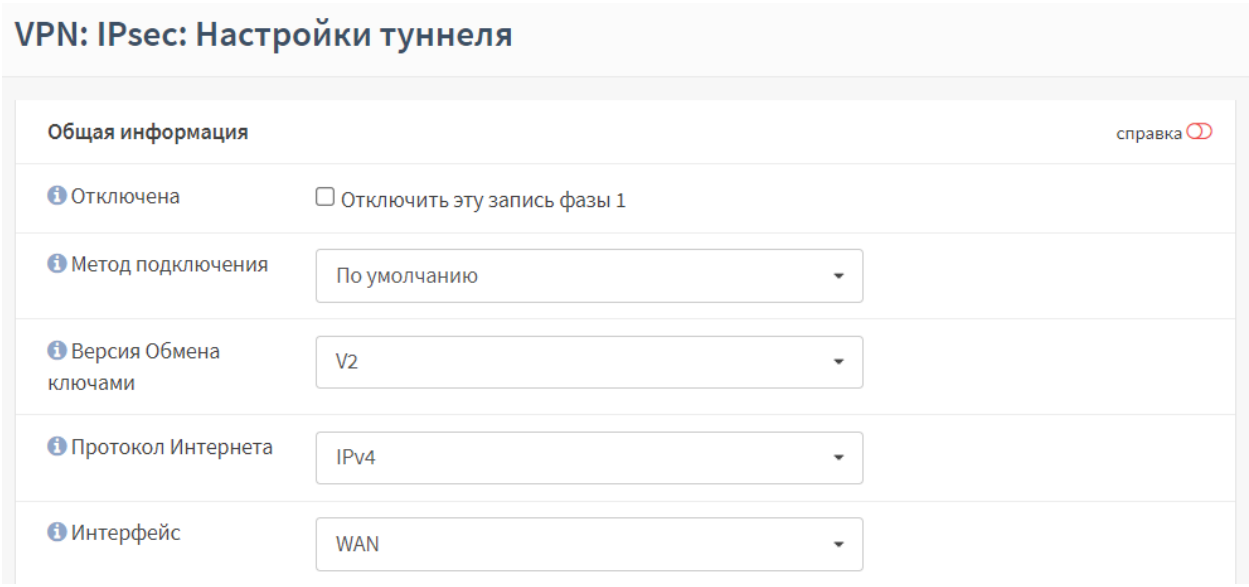


Рисунок – Настройка фазы 1 на ARMA FW1

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

4. Для созданной записи нажать **кнопку** « + » (см. Рисунок – Добавление записи фазы 2 на ARMA FW1) для добавления записи фазы 2.

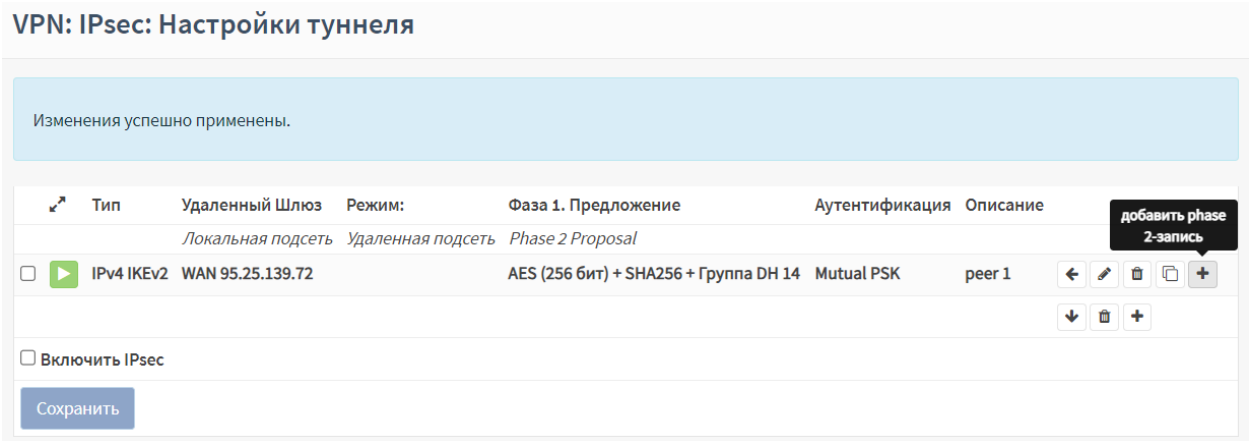


Рисунок – Добавление записи фазы 2 на ARMA FW1

5. Указать следующие настройки в открывшейся форме (см. Рисунок – Настройка фазы 2 на ARMA FW1):

   - **«Описание»** – «peer 1»;
   - **«Адрес»** (Удаленная сеть) – адрес локальной сети **ARMA FW2**, в примере «192.168.2.0», «24»;
   - **«Алгоритмы шифрования»** – флажок установлен для значения «aes256gcm16»;
   - **«Алгоритмы хеша»** – «SHA1»;

- **«Автоматически пингуйте хост»** – IP-адрес LAN интерфейса **ARMA FW2**, в примере «192.168.2.1».

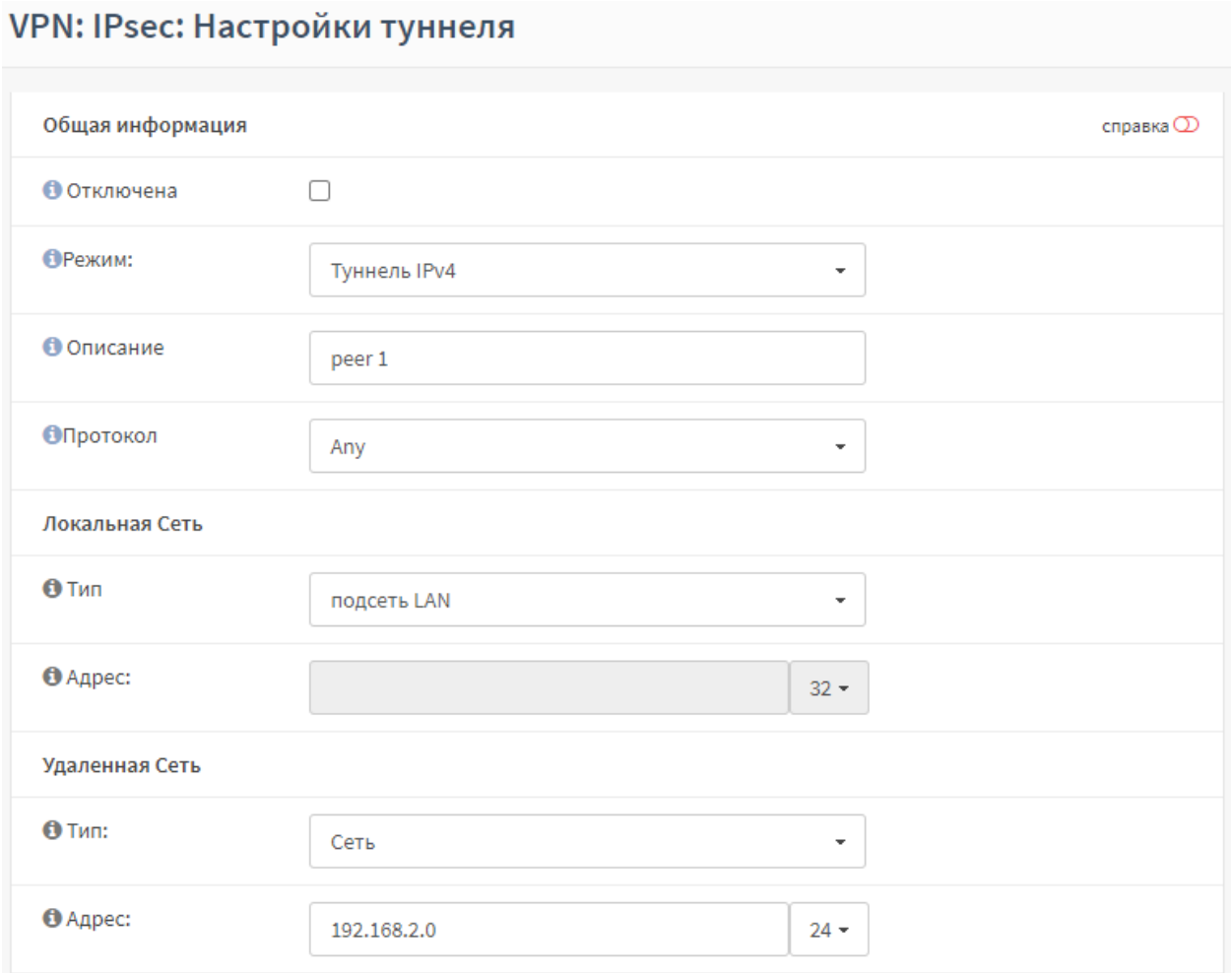


Рисунок – Настройка фазы 2 на ARMA FW1

Примечание:

В случае необходимости дополнительной настройки политик трафика, проходящего через интерфейс IPsec, следует ввести IP-адрес в формате CIDR в поле параметра **«Ручные записи SPD»**.

6. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
7. Установить флажок для параметра **«Включить IPsec»** и нажать **кнопку «Сохранить»**.

Для разрешения прохождения трафика в сеть LAN необходимо создать разрешающее правило МЭ (см. Создание правил межсетевого экранирования) для интерфейса **«[IPsec]»**, выбрав в параметре **«IP-адрес назначения»** «LAN-сеть».

25.2.2.3 Шаг 3. Настройка туннеля IPsec на ARMA FW2

Для настройки туннеля IPsec **ARMA FW2** необходимо выполнить следующие действия:

1. Перейти в подраздел настройки туннелей IPsec (**«VPN» - «IPsec» - «Настройки туннеля»**) и нажать **кнопку** « » для создания фазы 1.
2. Указать следующие настройки в открывшейся форме (см. Рисунок – Настройка фазы 1 на ARMA FW1):
   - **«Удалённый шлюз»** – IP-адрес WAN интерфейса **ARMA FW1**, в примере «85.175.16.192»;
   - **«Описание»** – «peer 2»;
   - **«Предварительно выданный ключ»** – «12345»;
   - **«Алгоритм шифрования»** – «AES, 256»;
   - **«Группа ключей DH»** – «14 (2048 bits)»;
   - **«Отключить MOBIKE»** – флажок установлен;
   - **«Обнаружение недоступных пиров»** – флажок установлен.
3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
4. Для созданной записи нажать **кнопку** « » для добавления записи фазы 2.
5. Указать следующие настройки в открывшейся форме:
   - **«Описание»** – «peer 2»;
   - **«Адрес»** (Удаленная сеть) – IP-адрес локальной сети **ARMA FW1**, в примере «192.168.1.0», «24»;
   - **«Алгоритмы шифрования»** – флажок установлен для значения **«aes256gcm16»**;
   - **«Алгоритмы хеша»** – «SHA1»;
   - **«Автоматически пингуйте хост»** – IP-адрес LAN интерфейса **ARMA FW1**, в примере «192.168.1.1».
6. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.
7. Установить флажок для параметра **«Включить IPsec»** и нажать **кнопку «Сохранить»**.

Для разрешения прохождения трафика в сеть LAN необходимо создать разрешающее правило МЭ (см. Создание правил межсетевого экранирования) для интерфейса **«[IPsec]»**, выбрав в параметре **«IP-адрес назначения»** «LAN-сеть».

25.2.2.4 Проверка подключения

Для проверки работоспособности подключения необходимо на одном из **ARMA FW** перейти в подраздел статуса IPsec (**«VPN» - «IPsec» - «Информация о статусе»**) и убедиться в наличии активного соединения (см. Рисунок – Информация о статусе IPsec VPN).

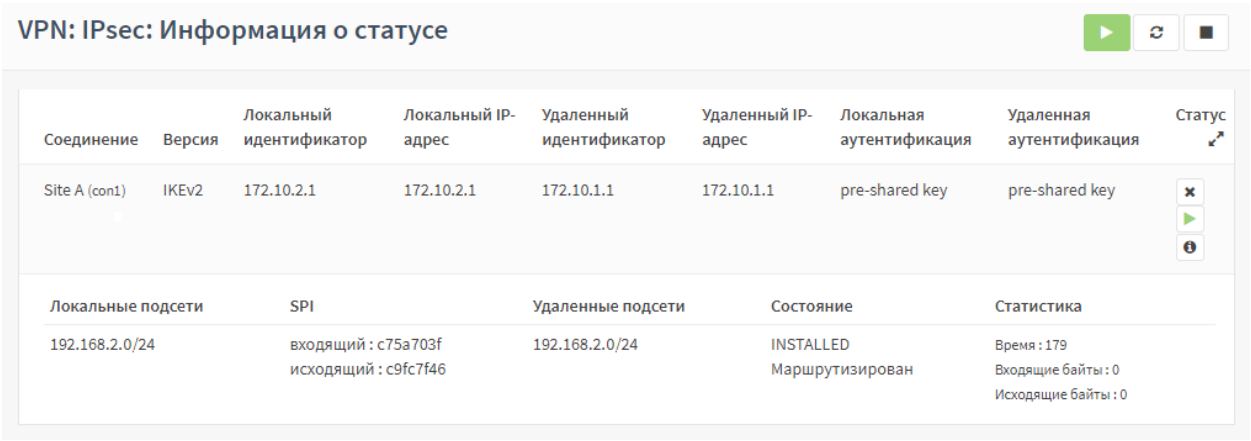


Рисунок – Информация о статусе IPsec VPN

25.2.3 Клонирование фазы IPsec

ARMA FW поддерживает возможность клонирования фазы IPsec.

Для клонирования какой-либо фазы IPsec необходимо выполнить следующие действия:

1. Перейти в подраздел настройки туннелей IPsec (**«VPN» - «IPsec» - «Настройки туннеля»**) и нажать **кнопку** « » напротив фазы, которую требуется клонировать.
2. При необходимости изменить параметры на открывшейся странице редактирования клонированной фазы.
3. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

Для одновременного клонирования фаз 1 и 2 следует выполнить следующие действия:

1. Инициировать процесс клонирования фазы 1 (см. Рисунок – Клонирование фазы 1).

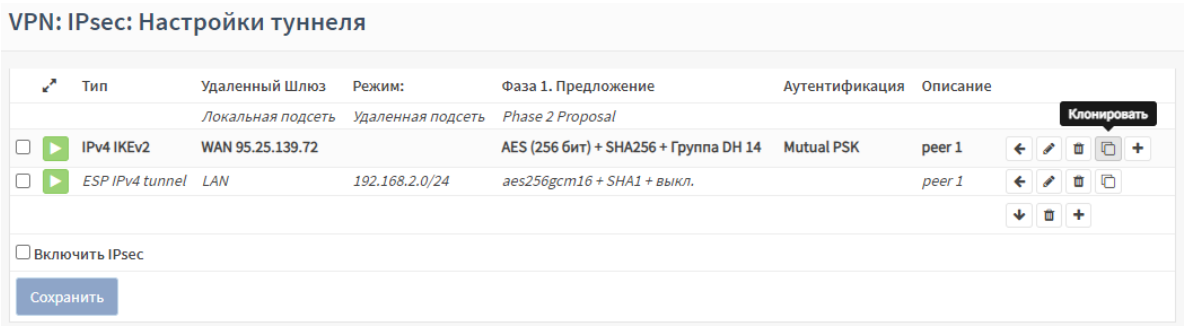


Рисунок – Клонирование фазы 1

2. Установить флажок для параметра **«Скопировать phase2»** на открывшейся странице редактирования клонированной фазы 1 (см. Рисунок – Клонирование фаз 1 и 2).

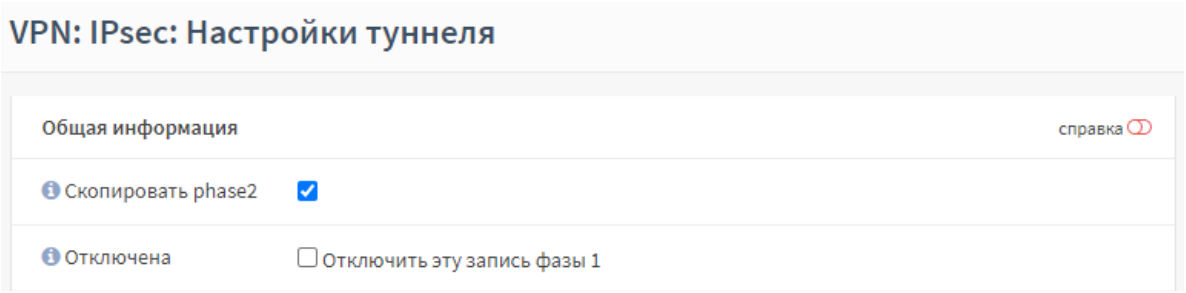


Рисунок – Клонирование фаз 1 и 2

3. Нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

Примечание:

Появляющаяся фаза 2 после одновременного клонирования фаз будет неактивна (см. Рисунок – Фазы IPsec). Для активации необходимо нажать **кнопку** « ▶ ».

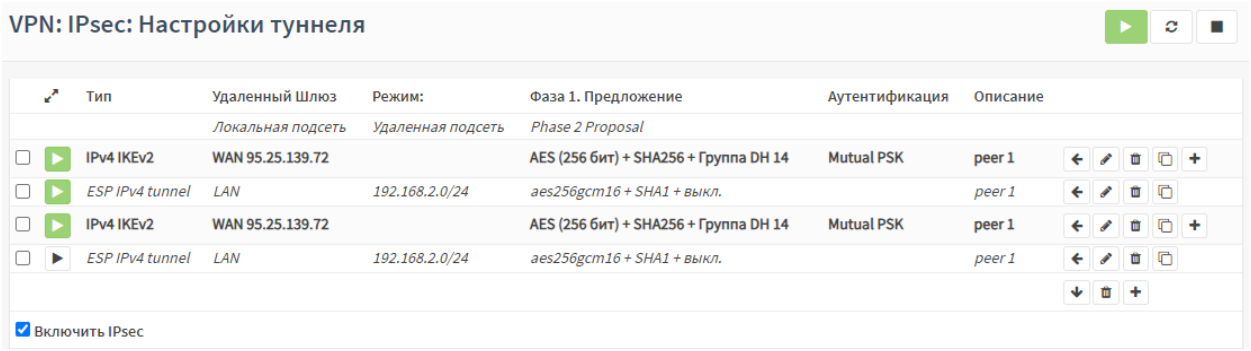


Рисунок – Фазы IPsec

25.3 ГОСТ VPN

ГОСТ VPN – это реализация OpenVPN, с применением алгоритмов шифрования, соответствующих ГОСТ и криптографических средств, прошедших процедуру оценки соответствия в ФСБ России.

ARMA FW поддерживает работу ГОСТ VPN в режимах **«сеть - сеть»** и **«узел - сеть»** с режимом работы устройства **«tun»** с настройками режима сервера, представленными в таблице (см. Таблица «Режимы работы сервера ГОСТ VPN»).

Таблица «Режимы работы сервера ГОСТ VPN»

Соединение «сеть - сеть»	Соединение «узел - сеть»
Пиринговая сеть (SSL/TLS)	Удаленный доступ (SSL/TLS)
	Удаленный доступ (аутентификация пользователя)
	Удаленный доступ (SSL/TLS+аутентификация пользователя)

Перед настройкой режимов подключения необходимо выполнить установку лицензии ГОСТ VPN.

Примечание:

Лицензия ГОСТ VPN не входит в комплект поставки **ARMA FW**. Для использования функциональности необходимо приобрести лицензию «OpenVPN-ГОСТ» у вендора или дистрибьюторов.

25.3.1 Информация о лицензии ГОСТ VPN

Установка и обновление лицензии ГОСТ VPN доступны только с доступом в Интернет. Лицензия продукта должна быть в виде текстового ключа, например:

- **«2JXC-4P5T-PAAH-NPFP»**.

Для ГОСТ VPN существуют следующие типы лицензии:

- **центрального шлюза** – позволяет настроить **ARMA FW** сервером, генерировать ключи и сертификаты;
- **шлюза филиала** – позволяет подключиться к центральному шлюзу и обеспечить защищённый канал с ним;
- **отдельного компьютера** – позволяет отдельному устройству подключиться к центральному шлюзу по зашифрованному каналу.

Для работы ГОСТ VPN в режиме **«сеть - сеть»** необходимо использовать следующие типы лицензии:

- центрального шлюза в качестве **серверной лицензии** – на **ARMA FW**, выполняющем роль сервера;
- шлюза филиала в качестве **клиентской лицензии** – на **ARMA FW**, выполняющем роль клиента.

Для работы ГОСТ VPN в режиме **«узел - сеть»** на **ARMA FW**, выполняющем роль сервера, необходимо использовать лицензию центрального шлюза в качестве **серверной лицензии**.

25.3.2 Установка или обновление лицензии ГОСТ VPN

Установка или обновление лицензии ГОСТ VPN осуществляется с помощью скрипта «openvpn-gost.sh».

Перед первой установкой лицензии необходимо сформировать файл инициализации ДСЧ. Для этого необходимо выполнить следующие действия:

1. Произвести аутентификацию в локальном консольном интерфейсе.
2. Нажать **клавишу «8»**, а затем **клавишу «Enter»** на клавиатуре для выбора пункта меню **«Shell»**.

   Для выведения справочной информации о доступных ключах к скрипту (см. Рисунок – Справочная информация) ввести команду **«openvpn-gost.sh -h»**.

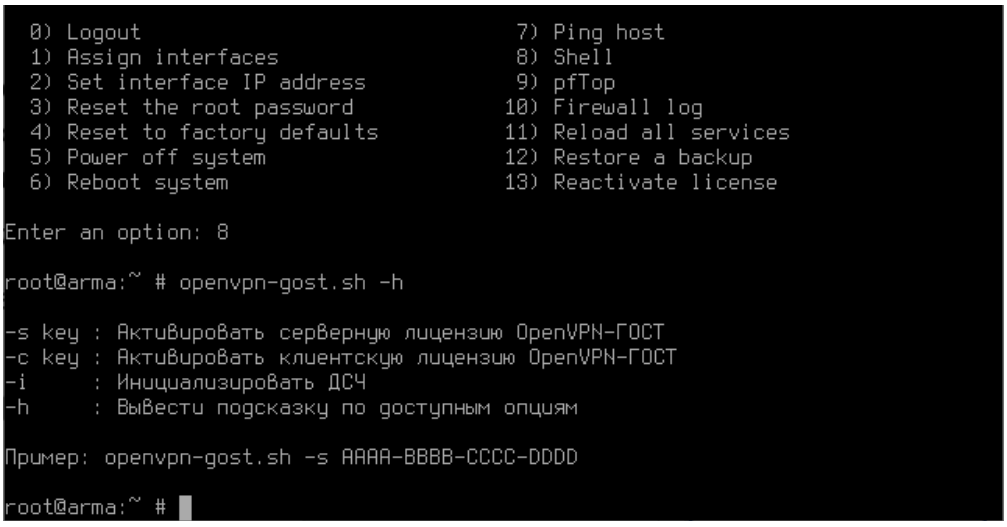


Рисунок – Справочная информация

3. В запущенной командной строке ввести команду:

   ```
   openvpn-gost.sh -i
   ```

   и нажать **клавишу «Enter»** для смены кодировки и корректного отображения выводимой информации и для запуска формирования файла инициализации программного ДСЧ. При обновлении лицензии запуск формирования файла инициализации программного ДСЧ не используется.

4. Последовательно нажимать на клавиатуре **клавиши**, соответствующие указанным в консоли символам (см. Рисунок – Запись файла инициализации ДСЧ). При правильном вводе будет произведена запись файла инициализации ДСЧ.

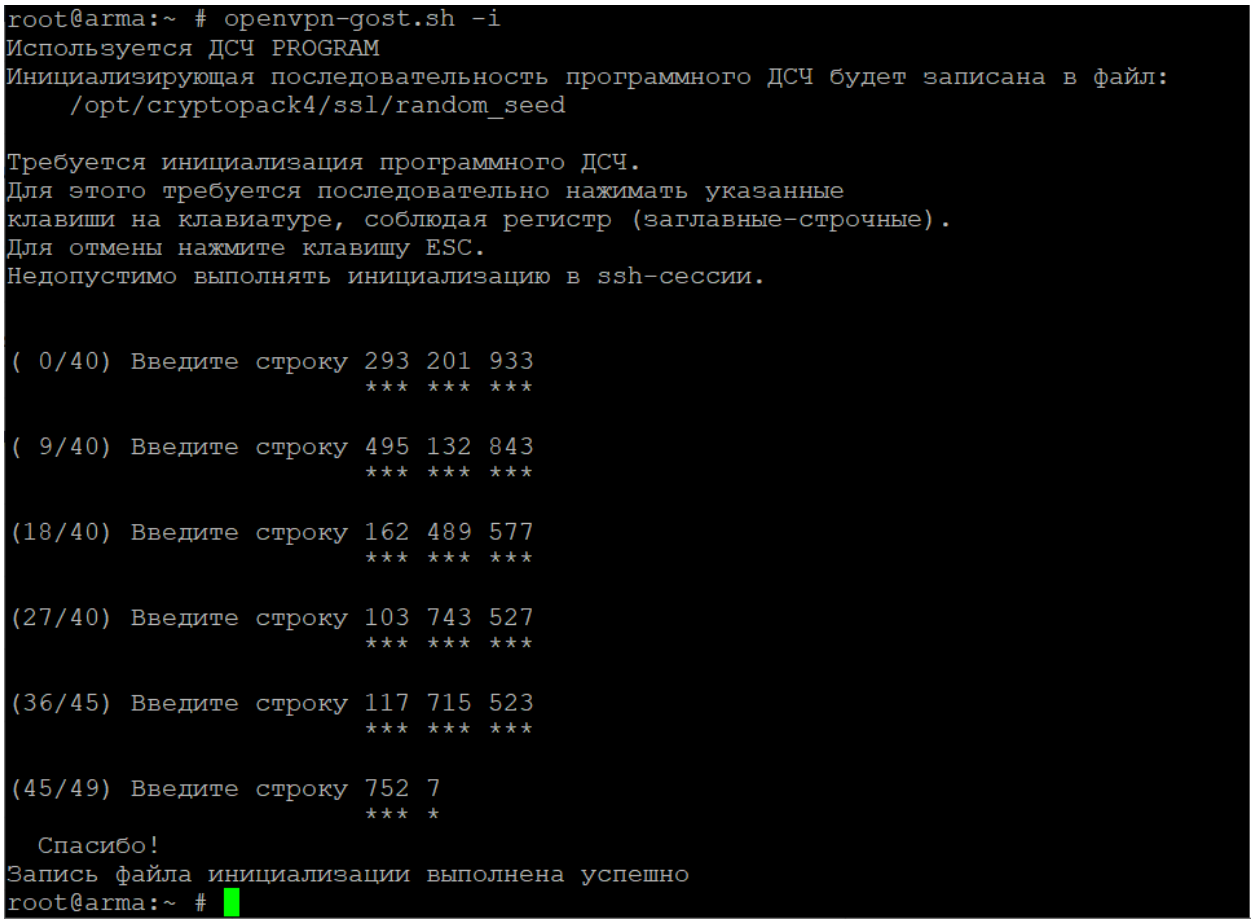


Рисунок – Запись файла инициализации ДСЧ

Для установки или обновления лицензии необходимо выполнить следующие действия:

1. Произвести аутентификацию в локальном консольном интерфейсе.
2. Нажать **клавишу «8»**, а затем **клавишу «Enter»** на клавиатуре для выбора пункта меню **«Shell»**.
3. Запустить процесс получения требуемой лицензии:
   - для **серверной лицензии** ввести команду:

     ```
     openvpn-gost.sh -s 4PJ2-DK5Y-ABTE-6T3W
     ```

     где «4PJ2-DK5Y-ABTE-6T3W» ключ лицензии для центрального шлюза, указан справочно;
   - для **клиентской лицензии** ввести команду:

     ```
     openvpn-gost.sh -c B9PZ-E7K8-3PC1-YGSE
     ```

     где «B9PZ-E7K8-3PC1-YGSE» ключ лицензии для шлюза филиала, указан справочно;

     и нажать **клавишу «Enter»**.

4. В случае успешного получения лицензии будет выведено сообщение:
   - для **серверной лицензии**:
     - «Получен файл лицензии. Лицензия успешно сохранена в файл /opt/cryptopack4/ssl/cryptocom_server.lic»;
   - для **клиентской лицензии**:
     - «Получен файл лицензии. Лицензия успешно сохранена в файл /opt/cryptopack4/ssl/cryptocom_client.lic».

25.3.3 Особенности настройки подключения ГОСТ VPN

При настройке подключения ГОСТ VPN необходимо придерживаться следующих криптографических установок:

- в режиме сервера **«Пиринговая сеть (SSL/TLS)»**:
  - **«Алгоритм шифрования»** – «magma-mgm (256 bit key, 64 bit blocks, TLS client/server mode only)»;
  - **«Дайджест-алгоритм аутентификации»** – «md_gost12_256 (256-bit)»; «md_gost12_512 (512-bit)»; «magma-mac(64-bit)»;
- в режимах сервера **«Удаленный доступ (SSL/TLS)»**, **«Удаленный доступ (аутентификация пользователя)»**, **«Удаленный доступ (SSL/TLS+аутентификация пользователя)»**:
  - **«Алгоритм шифрования»** – «magma-ctr (256 bit key, 64 bit blocks, TLS client/server mode only)»; «magma-mgm (256 bit key, 64 bit block, TLS client/server mode only)»;
  - **«Дайджест-алгоритм аутентификации»** – «md_gost12_256 (256-bit)»; «md_gost12_512 (512-bit)»; «magma-mac(64-bit)».

25.3.4 Настройка ГОСТ VPN в режиме «сеть – сеть»

В качестве примера приведено описание настройки ГОСТ VPN в режиме **«сеть – сеть»** без аутентификации TLS с использованием схемы стенда, представленной на рисунке (см. Рисунок – Схема стенда для настройки OpenVPN в режиме «сеть - сеть»).

Для настройки ГОСТ VPN в режиме **«сеть – сеть»** необходимо выполнить следующие шаги:

1. Создать доверенный центр сертификации ГОСТ на **ARMA FW1**. Экспортировать сертификат и секретный ключ для созданного центра сертификации.
2. Создать сертификаты сервера и клиента ГОСТ на **ARMA FW1**. Экспортировать пользовательские сертификат и ключ, созданного сертификата клиента.
3. Настроить сервер ГОСТ VPN на **ARMA FW1**.

4. Настроить правила МЭ на **ARMA FW1**.
5. Импортировать созданный центр сертификации на **ARMA FW2**.
6. Импортировать сертификат клиента ГОСТ на **ARMA FW2**.
7. Настроить клиент ГОСТ VPN на **ARMA FW2**.
8. Настроить правила МЭ на **ARMA FW2**.

25.3.4.1 Настройка ARMA FW1

25.3.4.1.1 Создание доверенного центра сертификации ГОСТ

Для создания доверенного центра сертификации необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры из таблицы (см. Таблица «Значение параметров центра сертификации ГОСТ»). Не указанные параметры оставить по умолчанию.

Таблица «Значение параметров центра сертификации ГОСТ»

Параметр	Значение
Описательное имя	GOST CA
Метод	Создать внутренний центр сертификации по ГОСТ
Код страны	RU (Russia)
Область	Moscow
Город	Moscow
Организация	InfoWatch
Email адрес	admin@infowatch.ru
Стандартное имя	GOST CA

Параметры **«Описательное имя»**, **«Код страны»**, **«Область»**, **«Город»**, **«Организация»**, **«Email адрес»**, **«Стандартное имя»** указаны справочно.

4. Нажать **кнопку «Сохранить»**.
5. Нажать **кнопки** напротив сертификата (см. Рисунок – Экспорт сертификата CA), для экспорта:
   - « » – сертификата CA (**1**);

- « » – ключа сертификата CA (**2**).

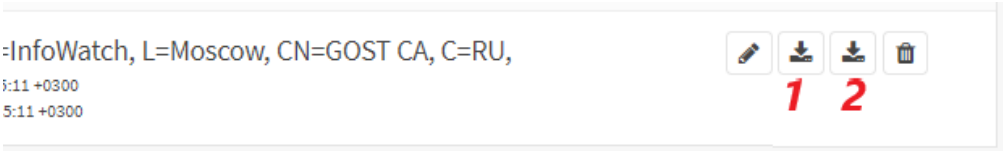


Рисунок – Экспорт сертификата CA

Просмотр и копирование содержимого экспортированных файлов возможны с помощью текстового редактора, например «Notepad++».

25.3.4.1.2 Создание сертификатов ГОСТ

Для создания сертификатов сервера и клиента ГОСТ необходимо выполнить следующие действия:

1. Перейти в подраздел сертификатов (**«Система» - «Доверенные сертификаты» - «Сертификаты»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры для создания сервера и нажать **кнопку «Сохранить»**. Не указанные параметры оставить по умолчанию.

   Примечание:

   Возможность создания внутреннего сертификата ГОСТ доступна только при активной лицензии ГОСТ VPN.

   Значения параметров сертификатов сервера ГОСТ:

   - **«Метод»** – «Создать внутренний сертификат по ГОСТ»;
   - **«Описательное имя»** – «GOST-server»;
   - **«Центр сертификации»** – «GOST CA»;
   - **«Тип»** – Сертификат сервера;
   - **«Время существования (дни)»** – «365»;
   - **«Стандартное имя»** – «GOST-server».
4. Нажать **кнопку «+Добавить»**.
5. В открывшейся форме для создания сертификата клиента указать параметры из списка ниже и нажать **кнопку «Сохранить»**. Не указанные параметры оставить по умолчанию.

   Значения параметров сертификатов клиента ГОСТ:

   - **«Метод»** – «Создать внутренний сертификат по ГОСТ»;
   - **«Описательное имя»** – «GOST-client»;

- **«Центр сертификации»** – «GOST CA»;
- **«Тип»** – Сертификат клиента;
- **«Время существования (дни)»** – «365»;
- **«Стандартное имя»** – «GOST-client».

6. Нажать **кнопки** напротив сертификата клиента (см. Рисунок – Экспорт сертификата клиента), для экспорта:
   - « » – пользовательского сертификата (**1**);
   - « » – пользовательского ключа сертификата (**2**).

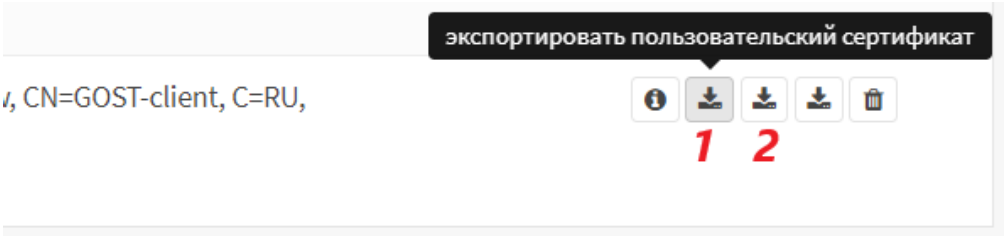


Рисунок – Экспорт сертификата клиента

Просмотр и копирование содержимого экспортированных файлов возможны с помощью текстового редактора, например «Notepad++».

25.3.4.1.3 Настройка сервера ГОСТ VPN

Для настройки сервера ГОСТ VPN необходимо выполнить следующие действия:

1. Перейти в подраздел настройки серверов (**«VPN» - «OpenVPN» - «Серверы»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры для сервера из списка ниже и нажать **кнопку «Сохранить»**. Не указанные параметры оставить по умолчанию.

   Значения параметров для сервера ГОСТ VPN:

   - **«Тип»** – «GostVPN»;
   - **«Описание»** – «GOST-server»;
   - **«Режим сервера»** – «Пиринговая сеть (SSL/TLS)»;
   - **«Интерфейс»** – «WAN»;
   - **«Локальный порт»** – «1194»;
   - **«Аутентификация TLS»** – Флажок не установлен;
   - **«Центр сертификации пиров»** – «GOST CA»;
   - **«Сертификат сервера»** – «GOST-server (GOST CA)»;

- **«Алгоритм шифрования»** – «magma-mgm (256 bit key, 64 bit blocks, TLS client/server mode only)»;
- **«Дайджест-алгоритм аутентификации»** – «md_gost12_256 (256-bit)»;
- **«Туннельная сеть IPv4»** – «10.10.0.0/24»;
- **«Локальная сеть IPv4»** – «192.168.0.0/24»;
- **«Удаленная сеть IPv4»** – «192.168.1.0/24»;
- **«Уровень детальности сообщений»** – «3 (рекомендуется)»;
- **«Принудительно принимать логин из переопределенных значений клиента»** – Флажок установлен.

25.3.4.1.4 Переопределение значений клиентов

Для режима сервера **«Пиринговая сеть (SSL/TLS)»** необходимо выполнить следующие настройки:

1. Перейти в настройки переопределения значений клиентов OpenVPN (**«VPN» - «OpenVPN» - «Переопределение значений для конкретного клиента»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме указать значения параметров:
   - **«Серверы»** – используемый сервер ГОСТ VPN;
   - **«Стандартное имя»** – имя сертификата клиента (см. Рисунок – Имя сертификата клиента);
   - **«Туннельная сеть IPv4»** – «10.10.0.0/24»;
   - **«Удаленная сеть IPv4»** – «192.168.1.0/24».

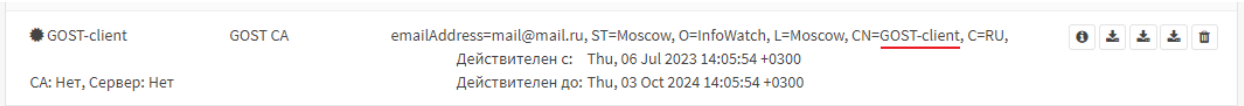


Рисунок – Имя сертификата клиента

Примечание:

При включённой аутентификации TLS в поле **«Стандартное имя»** следует указать «Root».

3. Нажать **кнопку «Сохранить»**.

25.3.4.1.5 Настройка правил МЭ

Для корректной работы VPN-туннеля необходимо настроить правила МЭ с параметрами, указанными в списке ниже. Не указанные в списке параметры оставить по умолчанию.

Создание правил МЭ описано в разделе Создание правил межсетевого экранирования настоящего руководства.

- **ARMA FW1 (правило №1)**:
  - **«Интерфейс»** – «[WAN]»;
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка»** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «UDP»;
  - **«IP-адрес назначения»** – «Любой»;
  - **«Диапазон портов назначения»** – «OpenVPN»;
  - **«Описание»** – «Allow VPN»;
- **ARMA FW1 (правило №2)**:
  - **«Интерфейс»** – «[OpenVPN]»;
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка»** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «Любой»;
  - **«Отправитель»** – «LAN сеть»;
  - **«Диапазон портов назначения»** – «Любой»;
  - **«Описание»** – «Allow VPN Traffic»;
- **ARMA FW2**:
  - **«Интерфейс»** – «[OpenVPN]»;
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Быстрая проверка»** – «Включено»;
  - **«Версии TCP/IP»** – «IPv4»;
  - **«Протокол»** – «Любой»;
  - **«Отправитель»** – «LAN сеть»;
  - **«Диапазон портов назначения»** – «Любой»;
  - **«Описание»** – «Allow VPN Traffic».

25.3.4.2 Настройка ARMA FW2

25.3.4.2.1 Импорт центра сертификации

Для импорта центра сертификации ГОСТ необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме (см. Рисунок – Импорт сертификата CA) указать значения параметров:
   - **«Описательное имя»** – «GOST CA», должно совпадать с именем созданного центра сертификации (см. Создание доверенного центра сертификации ГОСТ);
   - **«Метод»** – «Импортировать существующий центр сертификации по ГОСТ»;
   - **«Данные сертификата»** – скопированное значение из экспортированного файла сертификата CA (см. Создание доверенного центра сертификации ГОСТ);
   - **«Секретный ключ сертификата (необязательно)»** – скопированное значение из экспортированного файла секретного ключа CA.

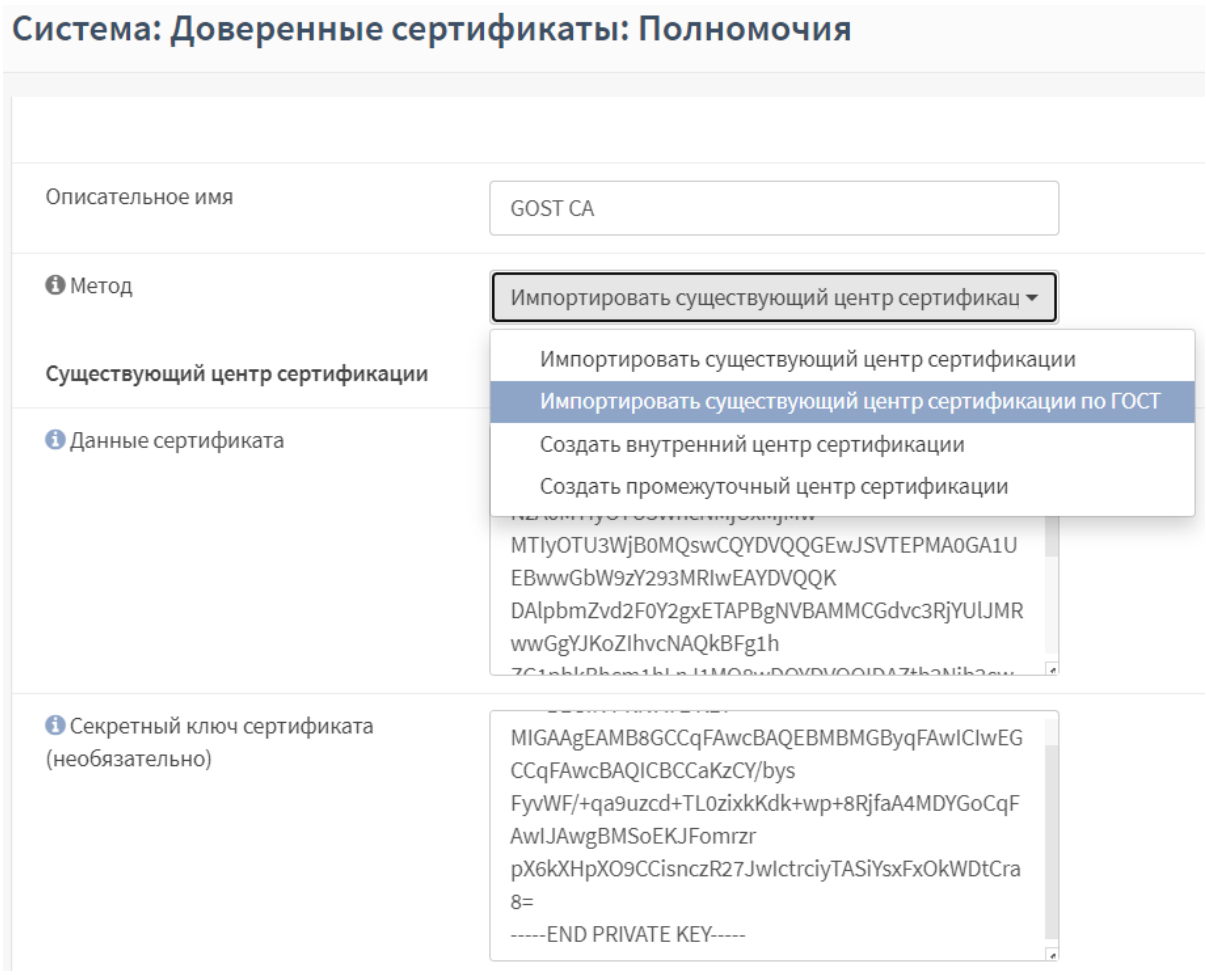


Рисунок – Импорт сертификата CA

4. Нажать **кнопку «Сохранить»**.

25.3.4.2.2 Импорт сертификата клиента

Для импорта сертификата клиента ГОСТ необходимо выполнить следующие действия:

1. Перейти в подраздел полномочий (**«Система» - «Доверенные сертификаты» - «Сертификаты»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать значения параметров:
   - **«Описательное имя»** – «GOST-client»;
   - **«Метод»** – «Импортировать существующий сертификат по ГОСТ»;
   - **«Данные сертификата»** – скопированное значение из экспортированного файла сертификата клиента (см. Создание сертификатов ГОСТ);
   - **«Данные секретного ключа»** – скопированное значение из экспортированного файла секретного ключа клиента.
4. Нажать **кнопку «Сохранить»**.

25.3.4.2.3 Настройка клиента ГОСТ VPN

Для настройки клиента ГОСТ VPN необходимо выполнить следующие действия:

1. Перейти в подраздел настройки клиентов (**«VPN» - «OpenVPN» - «Клиенты»**).
2. Нажать **кнопку «+Добавить»**.
3. В открывшейся форме указать параметры клиента из списка ниже. Не указанные параметры оставить по умолчанию.

   Значения параметров для клиента ГОСТ VPN:

   - **«Тип»** – «GostVPN»;
   - **«Описание»** – «GOST-client»;
   - **«Режим сервера»** – «Пиринговая сеть (SSL/TLS)»;
   - **«Интерфейс»** – «WAN»;
   - **«Удаленный сервер, Хост или адрес»** – «IP-адрес WAN интерфейса **ARMA FW1**»;
   - **«Удаленный сервер, Порт»** – «1194»;
   - **«Локальный порт»** – «1194»;
   - **«Аутентификация TLS»** – Флажок не установлен;
   - **«Центр сертификации пиров»** – «GOST CA»;
   - **«Сертификат клиента»** – «GOST-client»;
   - **«Алгоритм шифрования»** – «magma-mgm (256 bit key, 64 bit blocks, TLS client/server mode only)»;
   - **«Дайджест-алгоритм аутентификации»** – «magma-mac(64-bit)»;
   - **«Туннельная сеть»** – «10.10.0.0/24»;
   - **«Удаленная сеть»** – «192.168.0.0/24»;
   - **«Уровень детальности сообщений»** – «3».

4. Нажать **кнопку «Сохранить»**.

25.3.4.2.4 Настройка правил МЭ

Для корректной работы VPN-туннеля необходимо настроить правила МЭ с параметрами, указанными в Настройка правил МЭ. Не указанные параметры оставить по умолчанию.

После применения правил МЭ необходимо убедиться в работе канала, для этого на **ARMA FW2** перейти в подраздел статусов соединения OpenVPN (**«VPN» -**

«OpenVPN» - «Статус соединения»), значение в столбце **«Статус»** должно быть «up».

25.3.5 Особенности настройки ГОСТ VPN в режиме «узел - сеть»

При настройке ГОСТ VPN в режиме **«узел - сеть»** следует придерживаться принципа настройки OpenVPN в аналогичном режиме (см. Раздел Настройка OpenVPN в режиме «узел - сеть») за исключением следующих действий:

- создание доверенного центра сертификации – в подразделе полномочий (**«Система» - «Доверенные сертификаты» - «Полномочия»**) необходимо выбирать значение **«Создать внутренний центр сертификации по ГОСТ»** для параметра **«Метод»** в форме создания центра сертификации;
- создание сертификата – в подразделе сертификатов (**«Система» - «Доверенные сертификаты» - «Сертификаты»**) необходимо выбирать значение **«Создать внутренний сертификат по ГОСТ»** для параметра **«Метод»** в форме создания сертификата;
- настройка сервера – использовать криптографические установки указанные в разделе Особенности настройки подключения ГОСТ VPN.

26 ПОРТАЛ АВТОРИЗАЦИИ

26.1 Настройка портала авторизации

Портал авторизации – это веб-страница авторизации, на которую принудительно перенаправляются пользователи, подключившиеся к выделенной сети, перед тем как получить доступ к веб-ресурсам. Принцип работы портала авторизации заключается в перехвате HTTP/HTTPS-сессии подключившегося к выделенной сети пользователя и перенаправлении их на веб-сервер авторизации.

В качестве примера будет рассмотрен следующий сценарий использования портала авторизации (см. Рисунок – ARMA FW в качестве портала авторизации для OPT1):

1. Гостевая сеть на интерфейсе **«OPT1»**.
2. Аутентификация на портале через локальную базу данных **ARMA FW**.
3. Доступ к веб-серверу имеют только пользователи из группы **«guests»**.
4. Для ПК **«Guest2»** отключена необходимость авторизации.

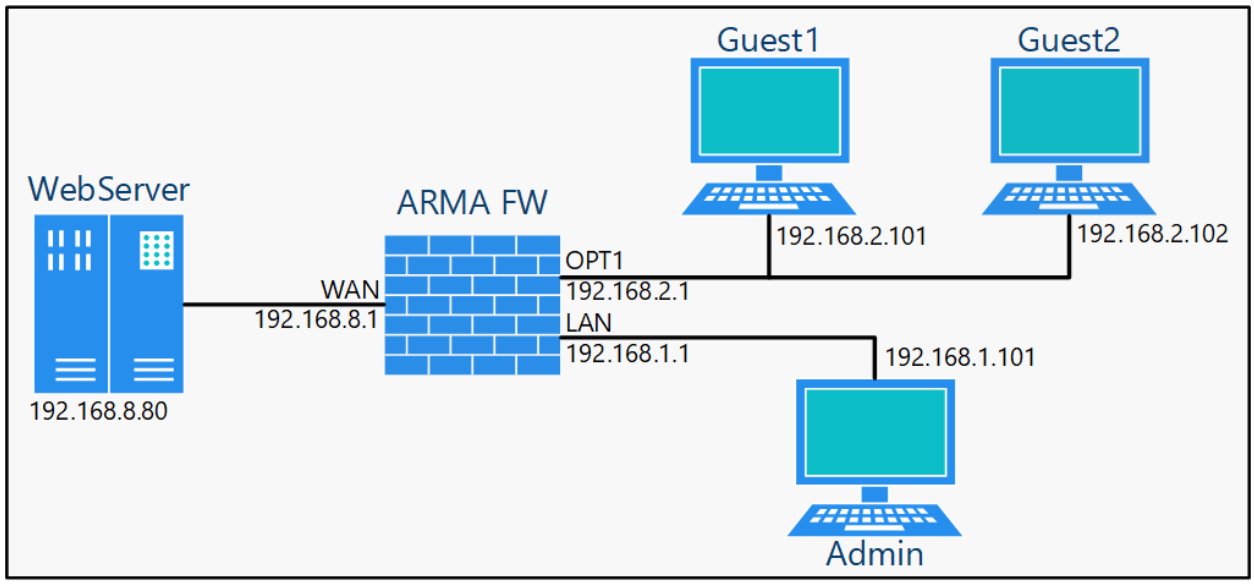


Рисунок – ARMA FW в качестве портала авторизации для OPT1

Для настройки портала авторизации необходимо выполнить следующие действия:

1. Создать для интерфейса «[OPT1]» правила МЭ (см. Создание правил межсетевого экранирования):
   - разрешающее доступ к порталу авторизации (к порту 8000);
   - разрешающие доступ к веб-серверу.
2. Создать портал авторизации на выбранном интерфейсе.

   Параметры правил представлены в списке:
   - Доступ к порталу авторизации:

- **«Действие»** – «Разрешить (Pass)»;
- **«Интерфейс»** – «OPT1»;
- **«Протокол»** – «TCP»;
- **«Отправитель»** – «OPT1 сеть»;
- **«IP-адрес назначения»** – «Этот межсетевой экран»;
- **«Диапазон портов назначения»** – «Другое/8000»;
- **«Описание»** – «Доступ к порталу авторизации»;

- Доступ к веб-серверу по HTTP:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Интерфейс»** – «OPT1»;
  - **«Протокол»** – «TCP»;
  - **«Отправитель»** – «OPT1 сеть»;
  - **«IP-адрес назначения»** – «192.168.8.80»;
  - **«Диапазон портов назначения»** – «HTTP»;
  - **«Описание»** – «Разрешающее правило HTTP»;
- Доступ к веб-серверу по HTTPS:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Интерфейс»** – «OPT1»;
  - **«Протокол»** – «TCP»;
  - **«Отправитель»** – «OPT1 сеть»;
  - **«IP-адрес назначения»** – «192.168.8.80»;
  - **«Диапазон портов назначения»** – «HTTPS»;
  - **«Описание»** – «Разрешающее правило HTTPS».

26.1.1 Добавление портала авторизации

Для добавления портала авторизации на выбранном интерфейсе необходимо перейти в подраздел зон портала авторизации (**«Службы» - «Портал авторизации» - «Администрирование» - вкладка «Зоны»**), нажать **кнопку** « + », заполнить поля в соответствии с таблицей (см. Таблица «Добавление зоны авторизации») и нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

Таблица «Добавление зоны авторизации»

Параметр	Значение
Включено	Выбрано
Интерфейсы	OPT1
Аутентификация через	Локальная база данных
Значение тайм-аута бездействия	0
Значение тайм-аута сеанса	0
Множественный вход пользователя в систему	Не выбрано
Сертификат SSL	Отсутствует
Имя хоста	(оставить пустым)
Разрешенные адреса	(оставить пустым)
Пользовательский шаблон	Интегрированный шаблон
Описание	Гостевой доступ

При создании или редактировании уже созданной зоны следует обратить внимание на данные параметры:

- **«Значение тайм-аута бездействия (в минутах)»** – в поле задаётся время, после которого клиенты будут отключены принудительно в случае бездействия;
- **«Значение тайм-аут сеанса (в минутах)»** – в поле задаётся время, после которого клиенты будут отключены принудительно;
- **«Множественный вход пользователя в систему»** – при включении данного параметра возможно выходить в сеть с одним логином с разных устройств одновременно;
- **«Прозрачный прокси (HTTP)»** – при включении данного параметра трафик будет перенаправлен на прозрачный прокси. Настройки прокси-сервера описаны в разделе Прокси настоящего руководства;
- **«Прозрачный прокси (HTTPS)»** – параметр аналогичен предыдущему.

26.1.2 Работа портала авторизации

Для авторизации в портале авторизации необходимо на ПК **«Guest1»** открыть веб-браузер и ввести IP-адрес веб-сервера, «192.168.8.80». При успешной настройке портала авторизации появится форма входа (см. Рисунок – Форма входа в портал авторизации).

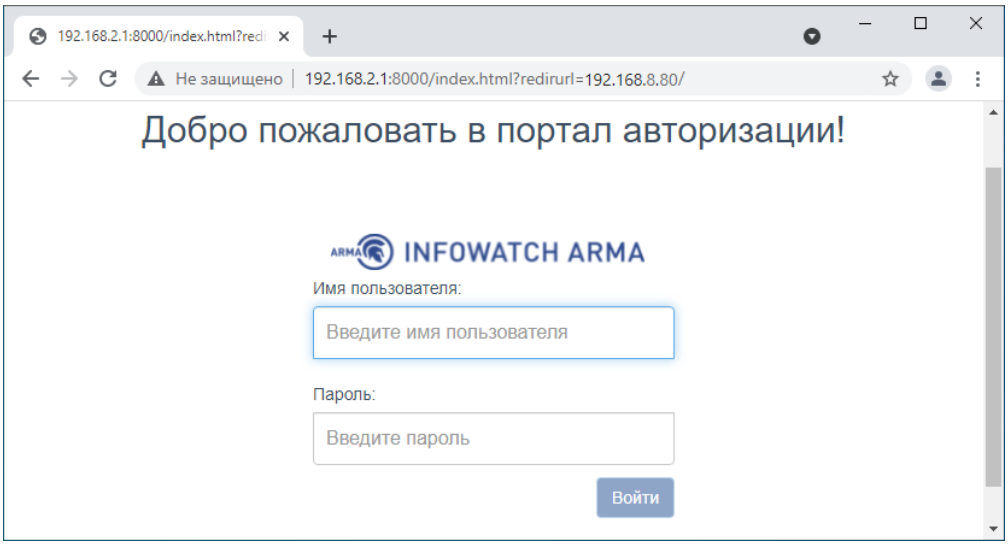


Рисунок – Форма входа в портал авторизации

Необходимо ввести аутентификационные данные и нажать **кнопку «Вход»**. При успешной авторизации отобразится запрашиваемая страница (см. Рисунок – Доступ к веб-серверу).

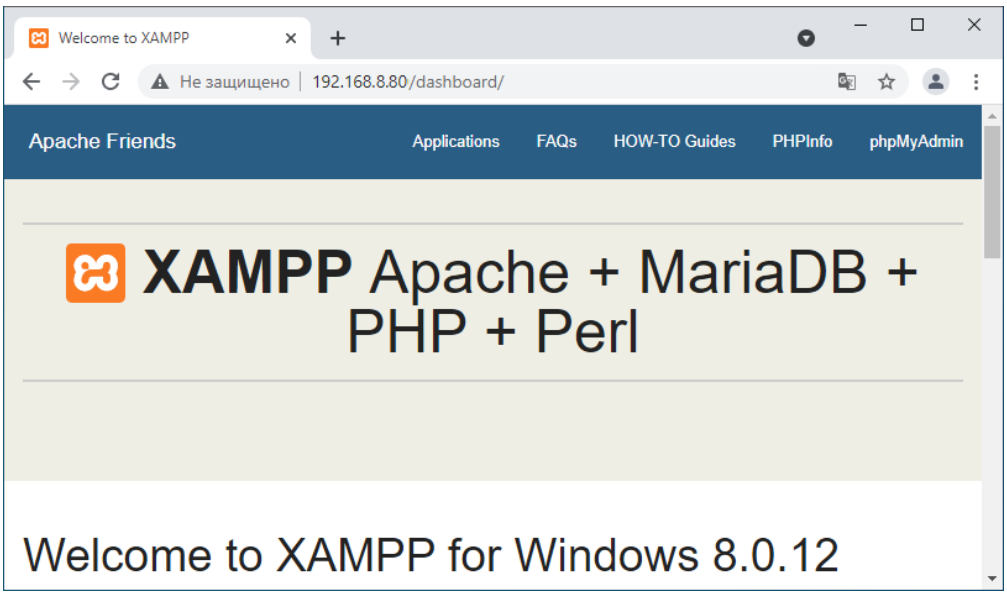


Рисунок – Доступ к веб-серверу

Для выхода из Портала авторизации необходимо перейти на страницу «192.168.2.1:8000» и нажать **кнопку «Выйти»** (см. Рисунок – Выход из Портала авторизации).

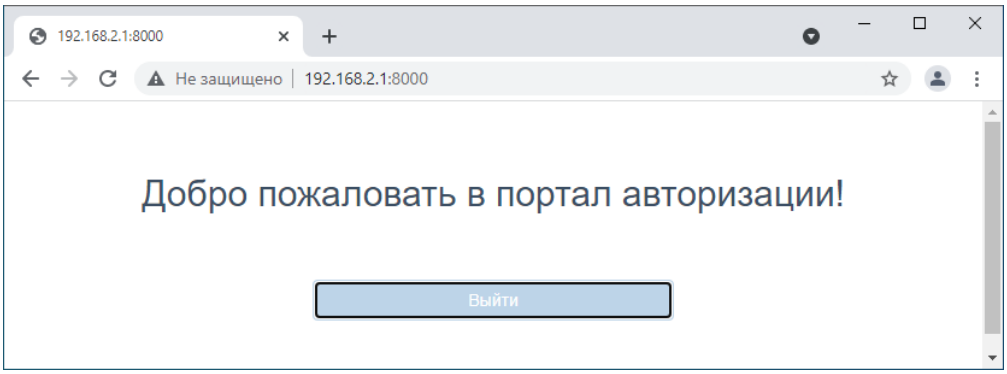


Рисунок – Выход из Портала авторизации

26.2 Доступ пользователей к порталу авторизации

Доступ пользователей возможно корректировать следующими параметрами:

- **«Принудительно использовать локальную группу»**;
- **«Разрешенные адреса»**;
- **«Разрешенные MAC-адреса»**.

26.2.1 Параметр «Принудительно использовать локальную группу»

При создании или редактировании уже созданной зоны доступен параметр **«Принудительно использовать локальную группу»** (см. Рисунок – Выбор группы для портала авторизации). Создание пользователей и групп пользователей для локальной БД описаны в разделе Учётные записи и права доступа настоящего руководства.

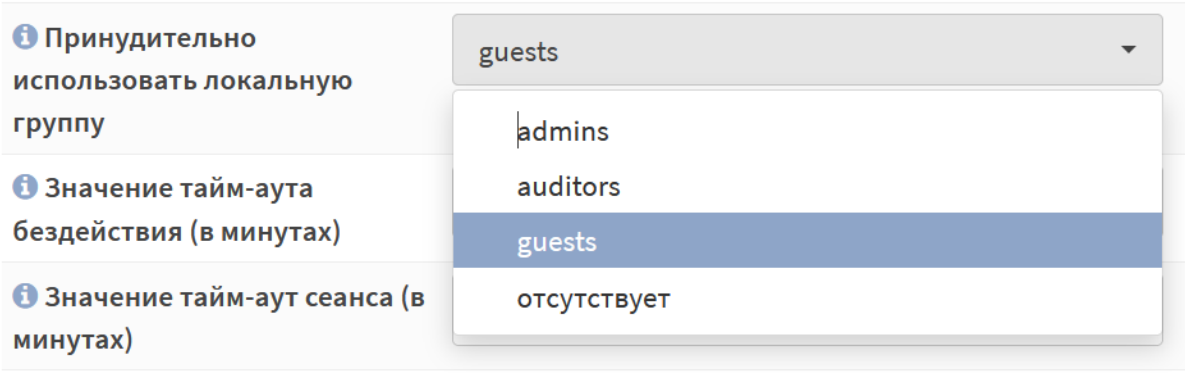


Рисунок – Выбор группы для портала авторизации

В случае выбора группы доступ будет только у пользователей данной группы.

Согласно примеру, в данном параметре необходимо выбрать значение **«guests»** и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить»** для вступления изменений в силу.

В случае, если пользователь не состоит в выбранной группе, при аутентификации будет выведена ошибка (см. Рисунок – Ошибка аутентификации).

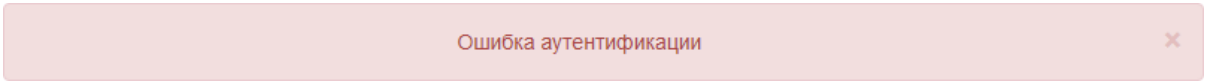


Рисунок – Ошибка аутентификации

26.2.2 Параметр «Разрешенные адреса»

При создании или редактировании уже созданной зоны доступен параметр **«Разрешенные адреса»** (см. Рисунок – Разрешенные адреса).

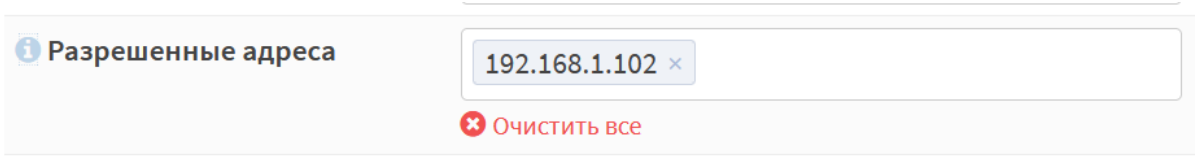


Рисунок – Разрешенные адреса

Для всех IP-адресов или сетей, указанных в поле данного параметра, доступ в сеть Интернет будет производиться без аутентификации на портале.

Согласно примеру, в данном параметре необходимо выбрать значение «192.168.2.102» и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить»** для вступления изменений в силу.

26.2.3 Параметр «Разрешенные MAC-адреса»

При создании или редактировании уже созданной зоны доступен параметр **«Разрешенные MAC-адреса»** (см. Рисунок – Разрешенные MAC-адреса). Данный параметр доступен только при взведении переключателя **«расширенный режим»** в верхней левой части формы.

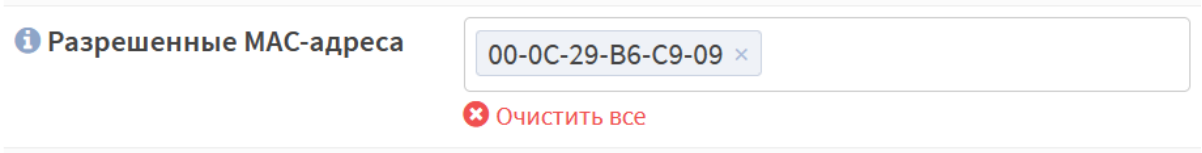


Рисунок – Разрешенные MAC-адреса

Для всех MAC-адресов, указанных в поле данного параметра, доступ к веб-серверу будет производиться без аутентификации на портале.

27 УЧЁТНЫЕ ЗАПИСИ И ПРАВА ДОСТУПА

Пользовательские УЗ и их привилегии позволяют контролировать доступ к подразделам и службам **ARMA FW**.

27.1 Создание пользовательских учётных записей и их привилегий

Для создания пользовательской УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система» - «Доступ» - «Пользователи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательные параметры **«Имя пользователя»** и **«Пароль»** (см. Рисунок – Создание пользовательской УЗ) и нажать **кнопку «Сохранить»**.

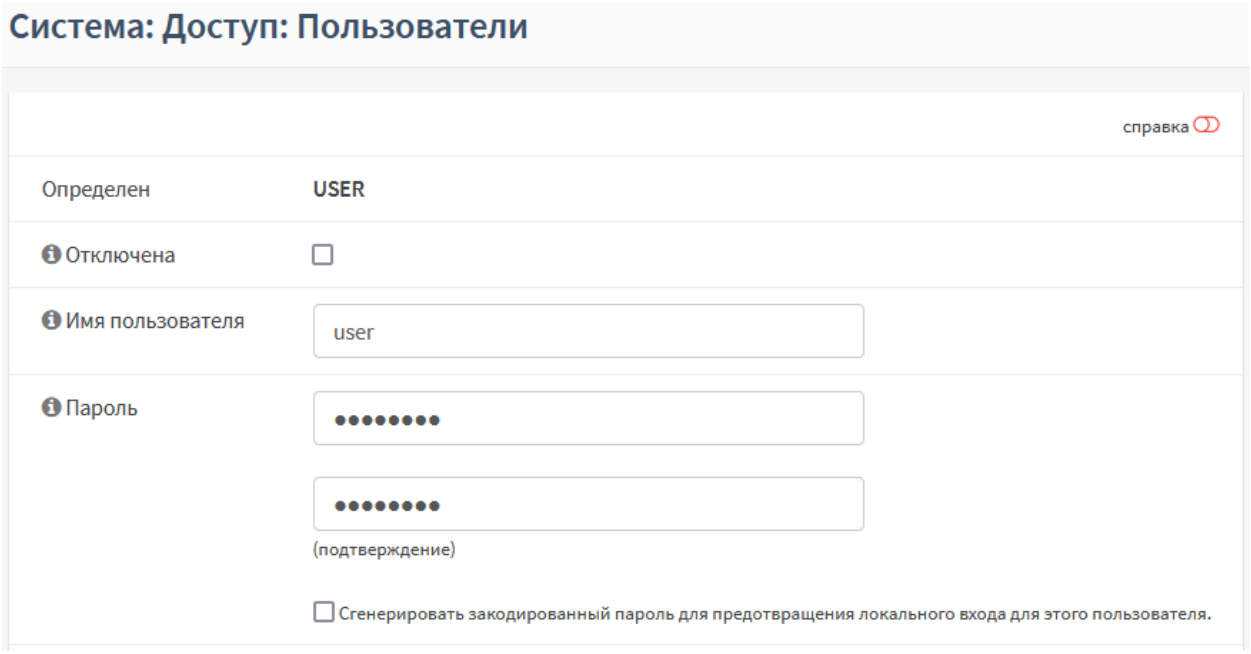


Рисунок – Создание пользовательской УЗ

Примечание:

Значение параметра **«Имя пользователя»** не может:

- содержать более 32 символов;
- начинаться с цифры;
- содержать символы, отличные от цифр **«0-9»**, **«A-Z»** верхнего и нижнего регистров и символов **«.-_»**.

27.1.1 Дополнительные параметры УЗ

Для более точной и полной информации о пользователе необходимо заполнить параметры **«Полное имя»**, **«Электронная почта»** и **«Комментарий»**.

Для создания временной пользовательской УЗ необходимо указать дату окончания срока действия в параметре **«Дата окончания срока действия»**. Пользователь будет иметь возможность авторизации по указанную дату включительно.

Для системной УЗ «root» отсутствует возможность ограничения срока действия УЗ.

Флажок **«Сгенерировать закодированный пароль для предотвращения локального входа для этого пользователя»** параметра **«Пароль»** может использоваться, например, для создания УЗ с SSH-ключом, но без доступа к веб-интерфейсу.

Для изменения стартовой страницы необходимо задать значение параметра **«Предпочтительная целевая страница»**, например, «ui/integritycontrol». По умолчанию при авторизации в веб-интерфейсе **ARMA FW** пользователю отображается страница инструментальной панели – информационные виджеты (см. Мониторинг системы с помощью информационных виджетов).

Для разрешения УЗ доступа к консольному интерфейсу **ARMA FW** необходимо установить флажок для параметра **«Доступ к консольному интерфейсу»**.

Для создания сертификата необходимо установить флажок для параметра **«Сертификат»**. Создание сертификатов используется **ARMA FW** для таких целей, как доступ к веб-интерфейсу через HTTPS, доступ к API, VPN, LDAP и т.д.

При настройке двухфакторной аутентификации в **ARMA FW** необходимо генерировать одноразовый пароль, установив флажок в **«Сгенерировать новый ключ (160 бит)»** параметра **«Выдача одноразовых паролей»**.

Для предоставления пользователю доступа к консольному интерфейсу **ARMA FW** по SSH (см. SSH-сервер) необходимо ввести сгенерированный ранее открытый ключ в поле параметра **«Авторизованные ключи»**.

Для подключения к настройке мобильного IPsec необходимо задать предварительный общий ключ в поле параметра **«Предварительно выданные ключи IPsec»**.

После сохранения УЗ доступно создание ключей API используемых, например, для подключения к **ARMA MC**. При нажатии **кнопки** « + » в параметре **«Ключи API»** будет создан ключ API для УЗ, а также скачан текстовый файл, содержащий значения **«key»** и **«secret»**.

27.1.2 Назначение привилегий пользовательской УЗ

Назначение привилегий пользовательской УЗ возможно двумя способами:

- добавление пользователя в определённую группу с уже заданными привилегиями;

- выбор привилегий из списка, установкой флажка напротив соответствующей привилегии в блоке настроек **«Системные привилегии»** (см. Рисунок – Установка системных привилегий).

Для удобства в блоке настроек **«Системные привилегии»** существует поле фильтра и функции множественного выбора:

- **«Веб-интерфейс: Все страницы»**;
- **«Функция: Очистить все журналы»**;
- **«Выбрать все (видимые)»**;
- **«Отменить выбор (видимые)»**.

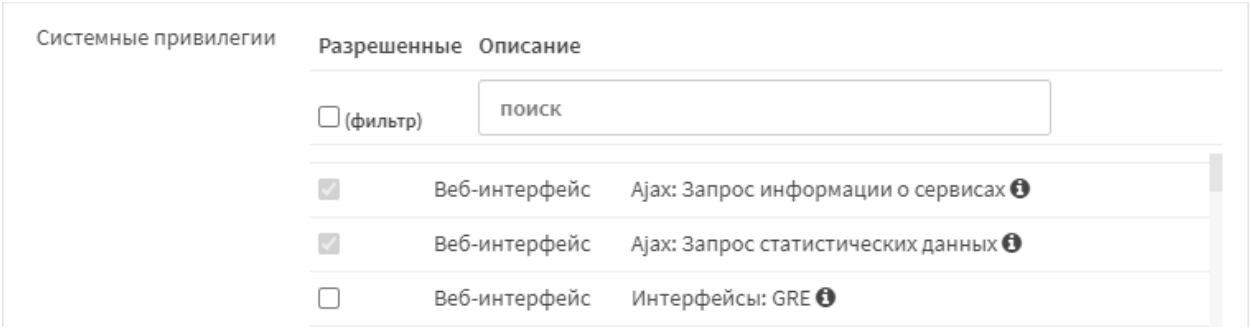


Рисунок – Установка системных привилегий

В случае необходимости назначения для УЗ пользователя возможности добавления или редактирования других УЗ, требуется в блоке **«Системные привилегии»** формы редактирования УЗ пользователя установить флажок для параметра **«Система Система: Изменить настройки»**.

Примечание:

Изменения привилегий УЗ пользователя вступят в силу, после завершения активной сессии пользователя.

В случае использования веб-прокси, для обеспечения актуального уровня доступа пользователя после изменения привилегий УЗ следует нажать **кнопку «Очистить»** во вкладке **«Помощь»** подраздела администрирования веб-прокси (см. Дополнительные настройки).

27.2 Создание группы и добавление им привилегий

Для удобства и простоты управления правами доступа существует возможность создания и редактирования групп. Каждую УЗ возможно включить в состав нескольких групп, в таком случае УЗ будет обладать совокупностью привилегий каждой из групп.

Для создания группы пользователей необходимо выполнить следующие действия:

1. Перейти в подраздел управления группами пользователей (**«Система» - «Доступ» - «Группы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательный параметр **«Имя группы»** (см. Рисунок – Создание группы пользователей) и нажать **кнопку «Сохранить»**.

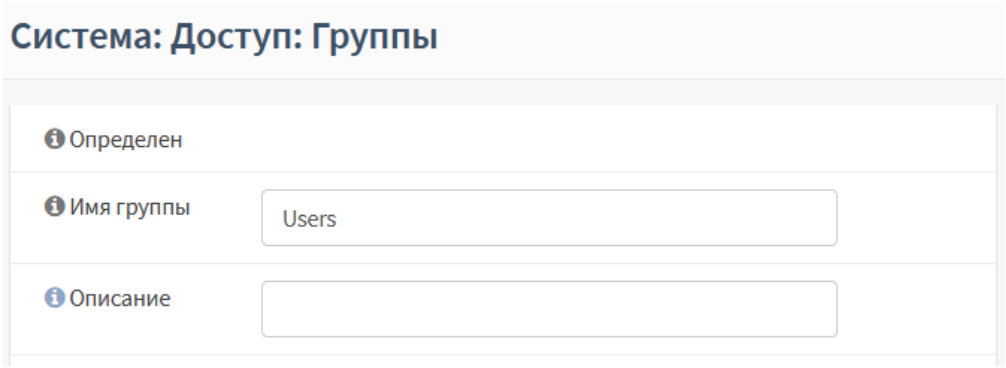


Рисунок – Создание группы пользователей

27.2.1 Дополнительные параметры групп

Для удобства использования групп необходимо добавить описание группы в поле параметра **«Описание»**.

Для добавления пользователей в создаваемую группу необходимо в блоке настроек **«Участники группы»** перенести имена пользователей из левой части в правую, нажав **кнопку** « » (см. Рисунок – Добавление участников в группу).

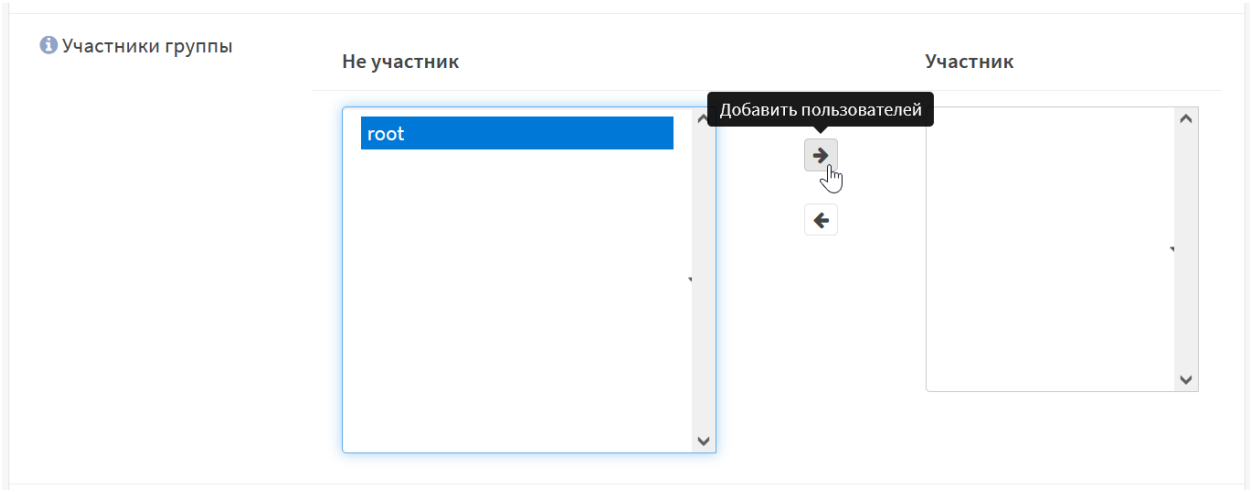


Рисунок – Добавление участников в группу

27.2.2 Назначение привилегий группе

Для назначения привилегий группе пользователей необходимо выбрать привилегии из списка, установив флажок напротив соответствующей привилегии в блоке настроек **«Системные привилегии»** аналогично назначению привилегий пользовательской УЗ (см. Назначение привилегий пользовательской УЗ).

27.3 Настройка парольной политики

Парольная политика – это набор правил при создании пароля, позволяющих повысить безопасность доступа к **ARMA FW**.

Для включения и настройки парольной политики необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система» - «Доступ» - «Серверы»**) и нажать **кнопку** « » напротив строки «Локальная база данных» для входа в режим редактирования.
2. В открывшейся форме установить флажок для параметра **«Включить ограничения политики паролей»**.
3. При необходимости задать значение в появившихся параметрах (см. Рисунок – Настройка парольной политики):
   - **«Срок действия»** – количество дней, в течение которых пароль остается действительным;
   - **«Длина»** – минимальная длина пароля;
   - **«Сложность»** – соответствие пароля требованиям сложности: пароль должен содержать цифры, прописные буквы, строчные буквы, специальные символы.

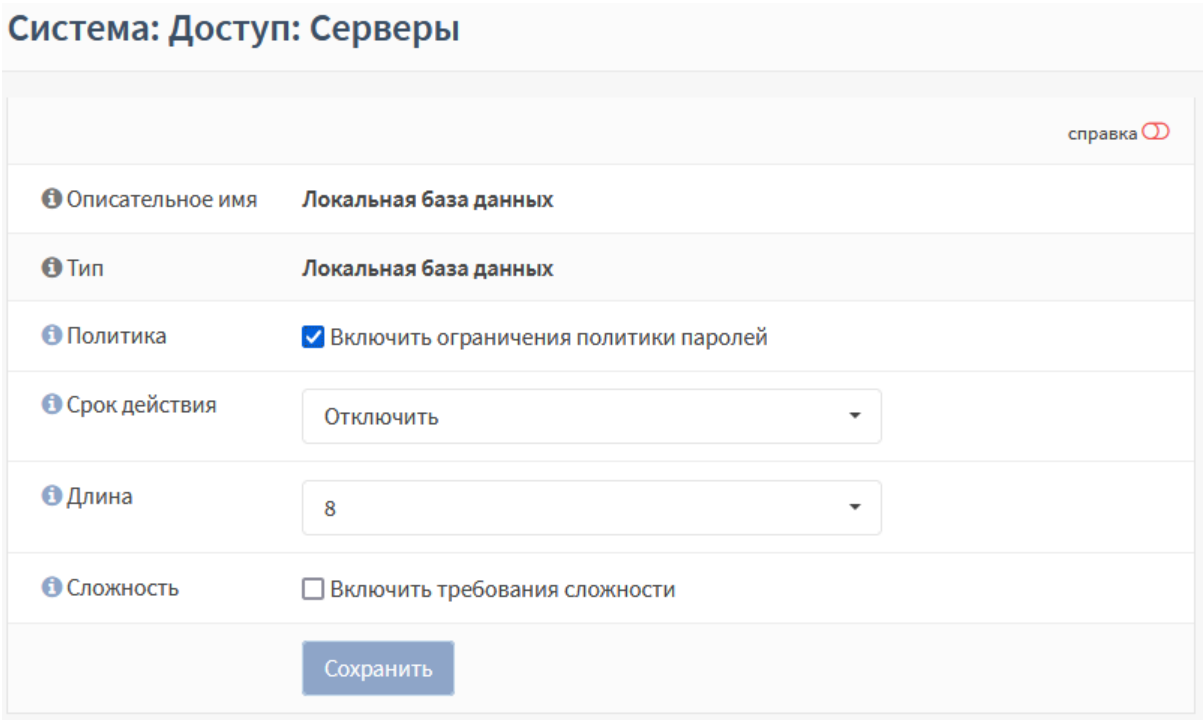


Рисунок – Настройка парольной политики

4. Нажать **кнопку «Сохранить»**.

После внесённых изменений при входе в систему с УЗ, пароль которой не отвечает установленным требованиям, будет предложено изменить пароль.

27.4 Аутентификация

Аутентификация – это процесс проверки подлинности введённого пользователем имени и пароля. В **ARMA FW** возможна аутентификация с использованием локальной или внешней БД пользователей. В качестве внешней БД служат различные внешние серверы авторизации. **ARMA FW** поддерживает работу со следующими внешними серверами:

- **«LDAP»** – OpenLDAP, MS Active Directory, Novell eDirectory;
- **«Radius»**.

По умолчанию в **ARMA FW** аутентификация осуществляется с использованием локальной БД пользователей. К дополнительным мерам защиты при аутентификации с использованием внутреннего сервера относится ваучер-сервер.

К дополнительным мерам защиты при аутентификации с использованием внешних серверов относится сервис двухфакторной аутентификации.

Для авторизации и предоставления соответствующих привилегий пользовательской УЗ, настроенной с помощью внешнего сервера, необходимо импортировать пользовательскую УЗ в локальную БД пользователей **ARMA FW**.

27.4.1 Ваучер-сервер

Ваучер-сервер используется для обеспечения аутентификации на портале авторизации в **ARMA FW**.

Ваучер – это запись с логином и паролем, которую **ARMA FW** генерирует по запросу. Ваучеры имеют настраиваемый срок действия, по истечении которого пользователю необходимо получить новый ваучер.

Для создания и настройки ваучер-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система» - «Доступ» - «Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме (см. Рисунок – Создание ваучер сервера), в параметре **«Тип»**, выбрать «Ваучер».
3. При необходимости установить флажок для параметра **«Использовать простые пароли (менее безопасные)»** и задать значения для параметров:
   - **«Описательное имя»**;
   - **«Длина имени пользователя»**;

- **«Длина пароля»**.

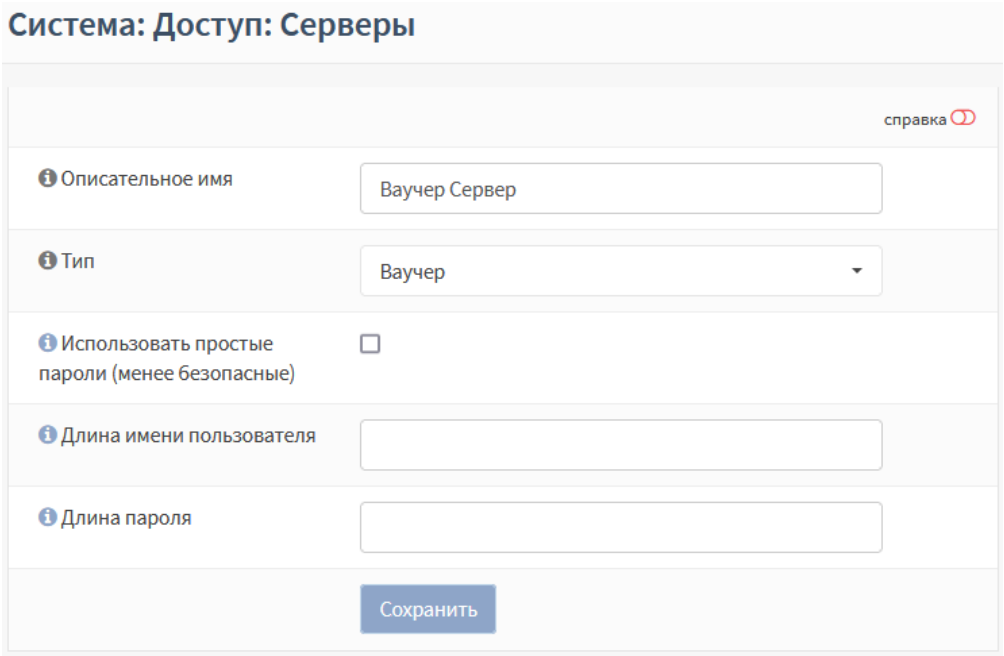


Рисунок – Создание ваучер сервера

4. Нажать **кнопку «Сохранить»**.

27.4.1.1 Использование ваучер-сервера для авторизации

Для использования ваучер-сервера на созданном портале авторизации необходимо выполнить следующие действия:

1. Перейти в подраздел зон портала авторизации (**«Службы» - «Портал авторизации» - «Администрирование» - «Зоны»**).
2. Нажать **кнопку** « » напротив созданной зоны и в открывшейся форме, в параметре **«Аутентификация через»** выбрать созданный ваучер сервер (см. Рисунок – Выбор метода аутентификации) и нажать **кнопку «Сохранить»**.

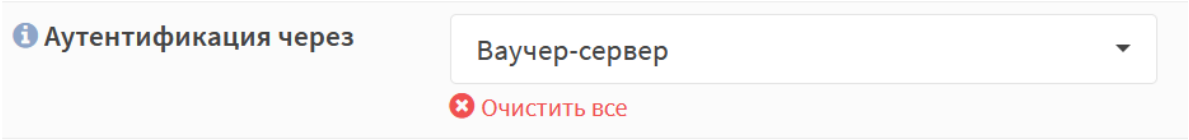


Рисунок – Выбор метода аутентификации

3. Перейти в подраздел управления ваучерами (**«Службы» - «Портал авторизации» - «Ваучеры»**) и нажать **кнопку «Создать ваучеры»**.
4. При необходимости в открывшейся форме задать значения для параметров:
   - **«Достоверность»**;
   - **«Истекает после»**;
   - **«Количество ваучеров»**;

- **«Имя группы»**;

и нажать **кнопку «Сгенерировать»**.

5. Созданный ваучер в формате **«CSV»** будет предложено скачать средствами используемого веб-браузера. Скачанный ваучер позволяет успешно аутентифицироваться через портал авторизации.

27.4.2 Двухфакторная аутентификация

Двухфакторная аутентификация в **ARMA FW** – это аутентификация, в процессе которой помимо постоянного пароля от локальной УЗ необходимо указать временный одноразовый пароль – «Time-based One-Time Password».

ARMA FW поддерживает RFC 6238. Для поддержки двухфакторной аутентификации используются мобильные приложения, совместимые с RFC 6238.

Для настройки двухфакторной аутентификации необходимо выполнить следующие шаги:

1. Добавить сервер аутентификации.
2. Добавить или настроить пользовательские УЗ.
3. Активировать одноразовый пароль.
4. Проверить токен.

27.4.2.1 Шаг 1 – Добавление сервера аутентификации

Для добавления сервера двухфакторной аутентификации необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система» - «Доступ» - «Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме задать настройки в соответствии с таблицей (см. Таблица «Настройки сервера аутентификации»). Значения параметров в таблице приведены справочно.

Таблица «Настройки сервера аутентификации»

Параметр	Значение
Описательное имя	Сервер TOTP
Тип	Локальный + Синхронизированный по времени одноразовый пароль

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**.

Дополнительные параметры:

- **«Длина токена»** – может быть изменён при необходимости;

- **«Интервал времени»** – может быть изменён при необходимости;
- **«Разрешенный период регистрации»** – используется для генерации нескольких различных токенов для разных периодов времени и сравнения их с токеном по передаваемому паролю;
- **«Обратный порядок токена»** – используется для установки требования пароля перед токеном.

27.4.2.2 Шаг 2 – Добавление или настройка пользовательской учётной записи

Для добавления пользовательской УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система» - «Доступ» - «Пользователи»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме заполнить обязательные параметры **«Имя пользователя»** и **«Пароль»**, установить флажок в значении **«Сгенерировать новый ключ (160 бит)»** параметра **«Выдача одноразовых паролей»** и нажать **кнопку «Сохранить»**.

27.4.2.3 Шаг 3 – Активация одноразового пароля

Для активации нового одноразового пароля необходимо выполнить следующие действия:

1. Нажать **кнопку** « » напротив созданной на шаге 2 УЗ (см. Шаг 2 – Добавление или настройка пользовательской учётной записи).
2. Нажать **кнопку «Нажмите, чтобы показать»** в параметре **«OTP QR код»** (см. Рисунок – Активация одноразового пароля).

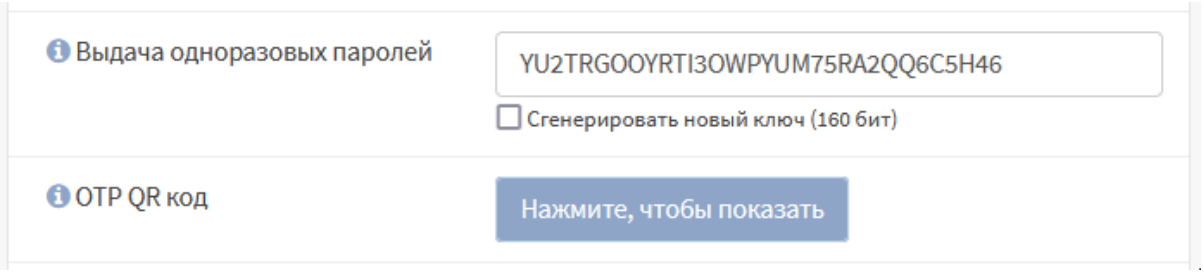


Рисунок – Активация одноразового пароля

3. Появившийся QR-код или содержимое значения параметра **«Выдача одноразовых паролей»** необходимо передать владельцу пользовательской УЗ.
4. Владельцу УЗ на мобильном устройстве открыть определённое администратором приложение, например, FreeOTP для ОС Android, и отсканировать полученный QR-код или ввести полученный одноразовый пароль. Подтвердить правильность сканирования QR-кода или ввода одноразового пароля и дождаться получения токена в приложении.

27.4.2.4 Шаг 4 – Проверка токена

Для тестирования аутентификации пользователя необходимо выполнить следующие действия:

1. Перейти в подраздел средств проверки (**«Система» - «Доступ» - «Средство проверки»**).
2. Указать значения параметров:
   - **«Сервер аутентификации»** – созданный на шаге 1 сервер (см. Шаг 1 – Добавление сервера аутентификации);
   - **«Имя пользователя»** –имя пользователя УЗ, созданной на шаге 2 (см. Шаг 2 – Добавление или настройка пользовательской учётной записи);
   - **«Пароль»** – данные в формате **«[Token][Password]»**, где:
     - **«[Token]»** – это значение токена из шага 3 (см. Шаг 3 – Активация одноразового пароля);
     - **«[Password]»** – это пароль УЗ, созданной на шаге 2 (см. Шаг 2 – Добавление или настройка пользовательской учётной записи);

   и нажать **кнопку «Проверка»**.
3. В случае правильной настройки сервера появится уведомление об успешной проверке (см. Рисунок – Успешная аутентификация). В случае указания некорректных данных появится уведомление об ошибке (см. Рисунок – Ошибка аутентификации).

При использовании двухфакторной аутентификации необходимо указывать данные в формате **«[Token][Password]»** в поле параметра **«Пароль»**.

27.4.3 LDAP

LDAP – протокол прикладного уровня для доступа к службе каталогов, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей.

Примечание:

ARMA FW не поддерживает аутентификацию LDAP в случае использования на внешнем LDAP-сервере двухфакторной авторизации. При добавлении нескольких LDAP-серверов для аутентификации будет использоваться только первый из списка.

Примечание:

Начиная с Microsoft Windows Server 2003 с пакетом обновления 1 (SP1), пользователи домена могут использовать предыдущий пароль для

доступа к сети в течение одного часа после смены пароля. Ознакомиться с описанием процесса изменения политики сетевой аутентификации NTLM возможно на сайте Microsoft Learn.

В качестве примера настройки LDAP будет описана настройка работы **ARMA FW** с MS Active Directory согласно схеме стенда, представленной на рисунке (см. Рисунок – Подключение внешнего сервера LDAP), имя домена LDAP – «test.local».

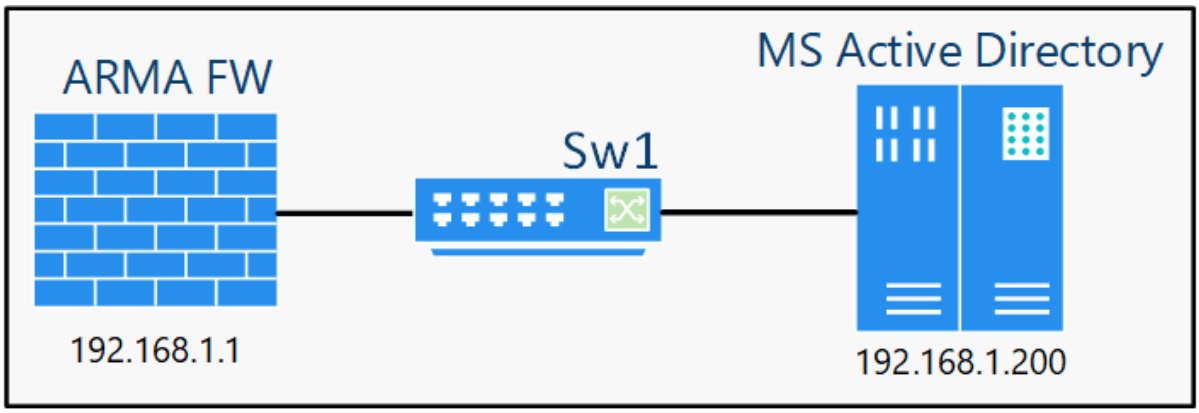


Рисунок – Подключение внешнего сервера LDAP

Перед началом настройки внешнего LDAP-сервера необходимо убедиться в наличии сетевого доступа к серверу Active Directory.

При использовании учётных записей LDAP-сервера для доступа к веб-интерфейсу **ARMA FW** необходимо определить привилегии УЗ, путём импорта пользовательских УЗ из LDAP-сервера.

Примечание:

При импорте пользовательских УЗ из LDAP-сервера принадлежность их к группам пользователей отобразится при первом входе в веб-интерфейс.

Для настройки внешнего сервера LDAP необходимо выполнить следующие шаги:

1. Добавить внешний сервер LDAP.
2. Протестировать соединение.
3. Обновить настройки доступа к системе.
4. Импортировать пользовательские УЗ.

27.4.3.1 Шаг 1 – Добавление сервера LDAP

Для добавления сервера LDAP необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система» - «Доступ» - «Серверы»**) и нажать **кнопку «+Добавить»**.

2. В открывшейся форме задать настройки в соответствии со списком ниже. Значения параметров в списке приведены справочно и зависят от настроек внешнего сервера Active Directory.
   - **«Описательное имя»** – «LDAP server»;
   - **«Тип»** – «LDAP»;
   - **«Имя хоста или IP-адрес»** – «192.168.1.200»;
   - **«Привязать параметры доступа»** – данные УЗ, имеющей роль администратора домена. В некоторых случаях необходимо указывать имя пользователя в формате: «имя_пользователя@имя_домена»;
   - **«Область поиска»** – «Целое поддерево»;
   - **«Базовый DN»** – «DC=test,DC=local»;
   - **«Контейнеры для аутентификации»** – нажать **кнопку «Выбрать»** и выбрать из доступного списка (см. Рисунок – Контейнеры для аутентификации);
   - **«Чтение свойств»** – флажок установлен;
   - **«Синхронизировать группы»** – флажок установлен. Присвоение пользователю группы произойдёт при первой авторизации в интерфейсе **ARMA FW**.

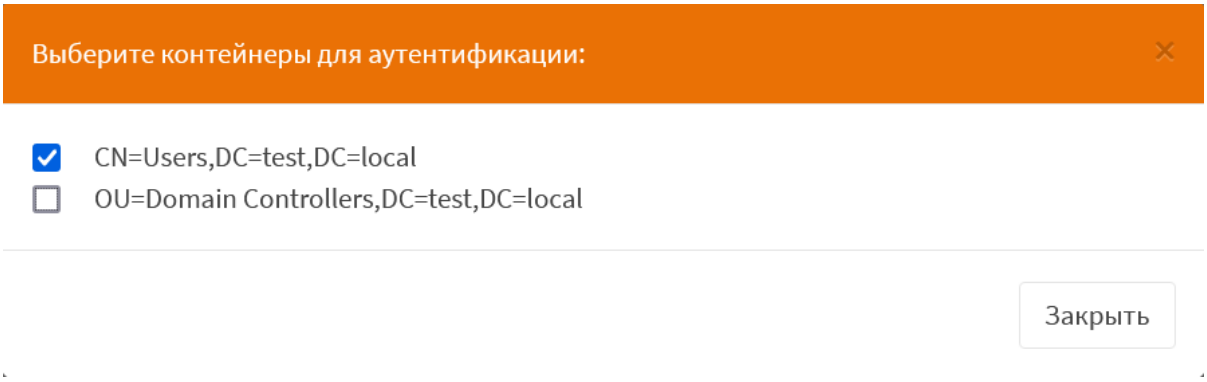


Рисунок – Контейнеры для аутентификации

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**.

Дополнительные параметры:

- **«Расширенный запрос»** – может быть использован для выбора пользователей, которые являются членами определённой группы;
- **«Ограничение групп»** – рекомендуется использовать только при необходимости.

27.4.3.2 Шаг 2 – Тест соединения

Для проверки правильности настройки сервера необходимо выполнить следующие действия:

1. Перейти в подраздел средств проверки (**«Система» - «Доступ» - «Средство проверки»**) (см. Рисунок – Проверка правильности настройки LDAP-сервера).

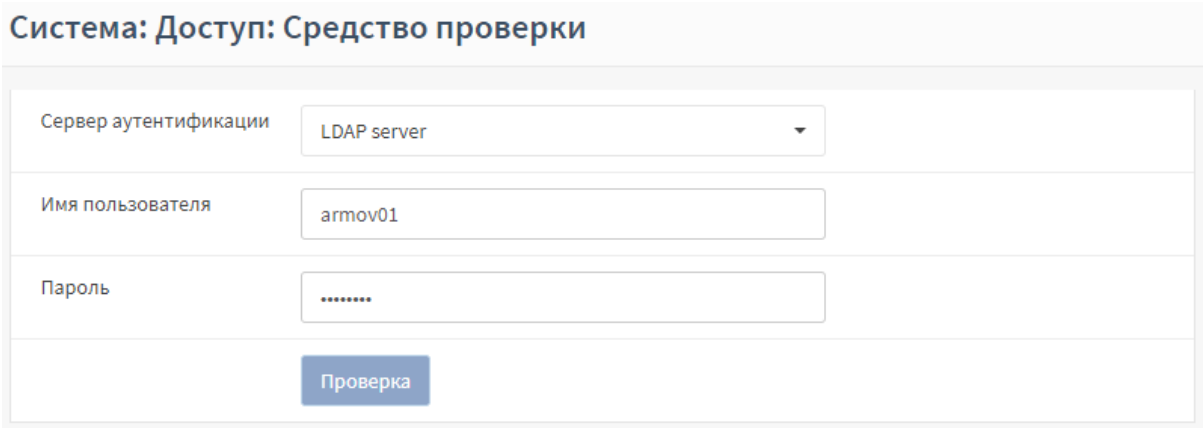


Рисунок – Проверка правильности настройки LDAP-сервера

2. В параметре **«Сервер аутентификации»** выбрать созданный на шаге 1 (см. Шаг 1 – Добавление сервера LDAP) LDAP-сервер, в параметрах **«Имя пользователя»** и **«Пароль»** ввести учётные данные для подключения к внешнему LDAP серверу и нажать **кнопку «Проверка»**.
3. В случае корректной настройки появится уведомление об успешной аутентификации (см. Рисунок – Успешная аутентификация).

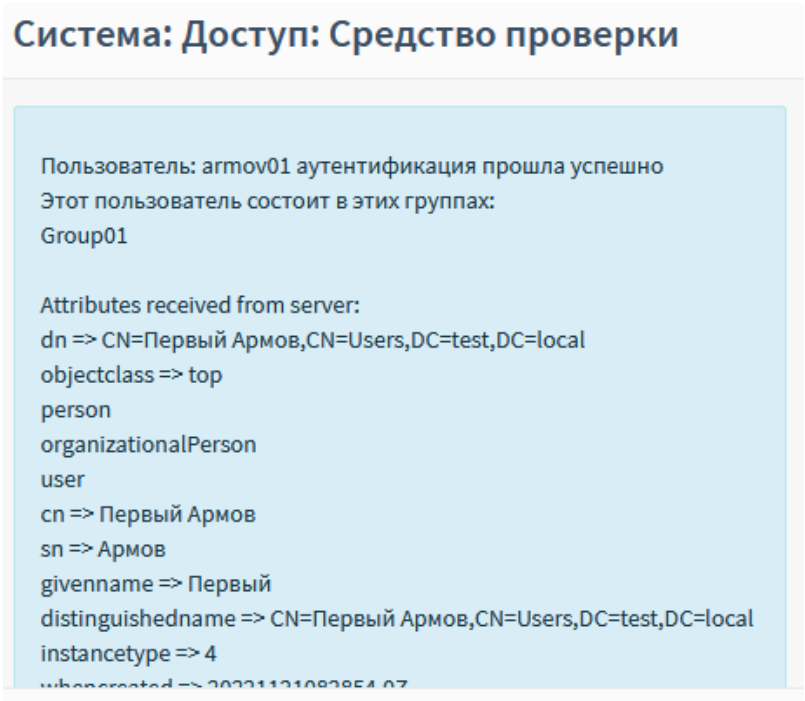


Рисунок – Успешная аутентификация

4. В случае некорректной настройки или ошибки в учётных данных будет отображена ошибка аутентификации (см. Рисунок – Ошибка аутентификации).

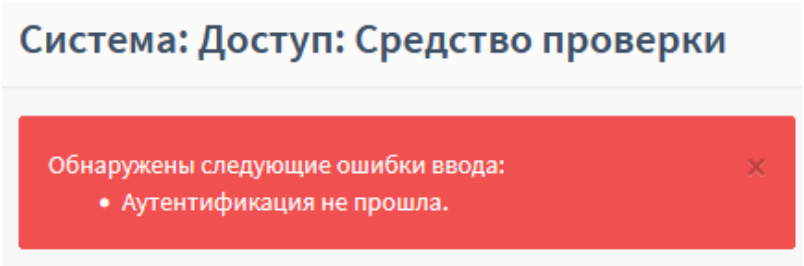


Рисунок – Ошибка аутентификации

27.4.3.3 Шаг 3 – Обновление настроек доступа к системе

На данном шаге необходимо изменить настройки по умолчанию, чтобы пользовательские УЗ LDAP получили доступ к **ARMA FW**.

Для обновления настроек доступа к системе необходимо выполнить следующие действия:

1. Перейти в подраздел настроек **ARMA FW** (**«Система» - «Настройки» - «Администрирование»**).
2. В блоке **«Аутентификация»** (см. Рисунок – Выбор сервера аутентификации) добавить сервер аутентификации «LDAP-сервер», созданный на шаге 1 (см. Шаг 1 – Добавление сервера LDAP), и нажать **кнопку «Сохранить»**.

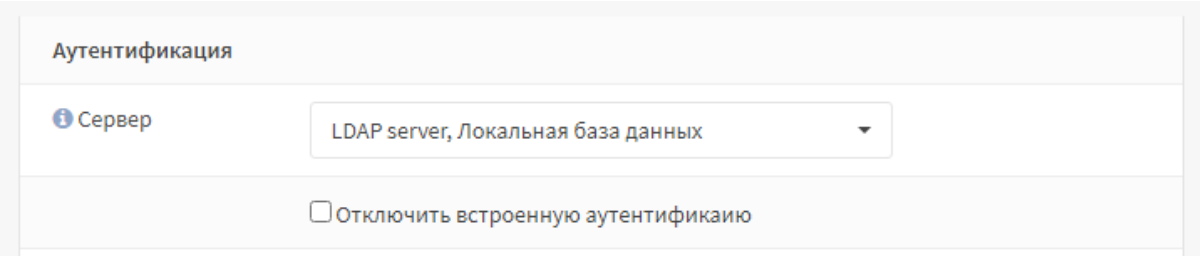


Рисунок – Выбор сервера аутентификации

27.4.3.4 Шаг 4 – Импорт пользовательских УЗ

Для предоставления доступа к веб-интерфейсу пользовательским УЗ внешнего LDAP-сервера, их необходимо импортировать в **ARMA FW**.

Для импорта УЗ необходимо выполнить следующие действия:

1. Перейти в подраздел управления пользователями (**«Система» - «Доступ» - «Пользователи»**) (см. Рисунок – Импорт пользовательских УЗ LDAP-сервера).

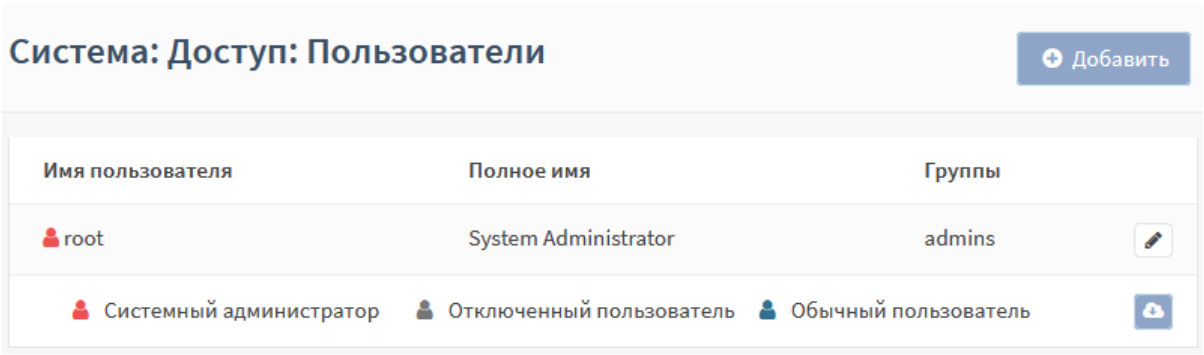


Рисунок – Импорт пользовательских УЗ LDAP-сервера

2. Нажать появившуюся **кнопку** « » в правом нижнем углу формы.
3. В открывшейся форме установить флажки для импортируемых пользовательских УЗ (см. Рисунок – Выбор импортируемых пользовательских УЗ) и нажать **кнопку «Сохранить»**. Импорт произведён успешно, если после нажатия кнопки не появились сообщения об ошибке и выбранные пользователи отображены в общем списке пользователей.

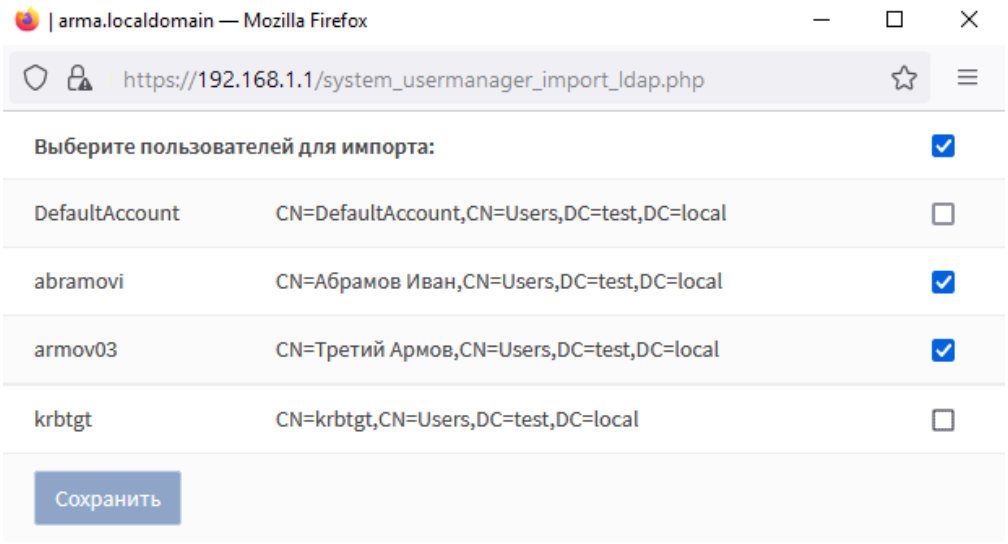


Рисунок – Выбор импортируемых пользовательских УЗ

Примечание:

УЗ, содержащие в имени пользователя символы кириллицы, не отображаются в форме и не подлежат импорту.

Примечание:

Невозможно импортировать из внешнего сервера аутентификации УЗ, имена пользователей которых совпадают с УЗ в локальной БД **ARMA FW**.

Возможно настроить синхронизацию пользователей с помощью планировщика задач Cron (см. Cron). В случае использования планировщика задач производится

автоматическое добавление новых и удаление отсутствующих УЗ внешнего сервера LDAP.

27.4.3.5 Импорт групп пользователей

Для использования пользовательских групп внешнего сервера LDAP требуется их предварительно импортировать, для этого необходимо выполнить следующие действия:

1. Перейти в подраздел управления группами (**«Система» - «Доступ» - «Группы»**) (см. Рисунок – Импорт пользовательских групп LDAP-сервера).

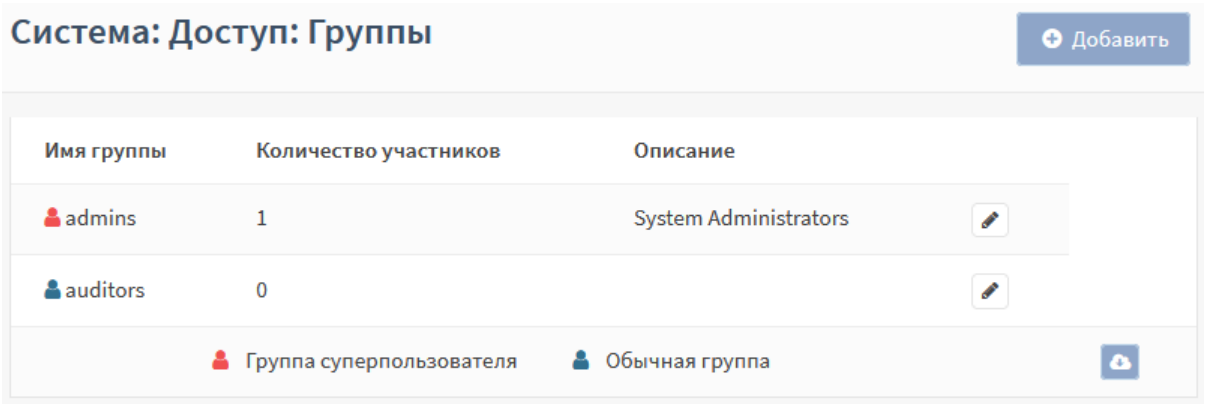


Рисунок – Импорт пользовательских групп LDAP-сервера

2. Нажать появившуюся **кнопку** « » в правом нижнем углу формы.
3. В открывшейся форме установить флажки для импортируемых пользовательских групп (см. Рисунок – Выбор импортируемых пользовательских групп) и нажать **кнопку «Сохранить»**. Импорт произведён успешно, если после нажатия кнопки не появились сообщения об ошибке и выбранные группы отображены в общем списке групп.

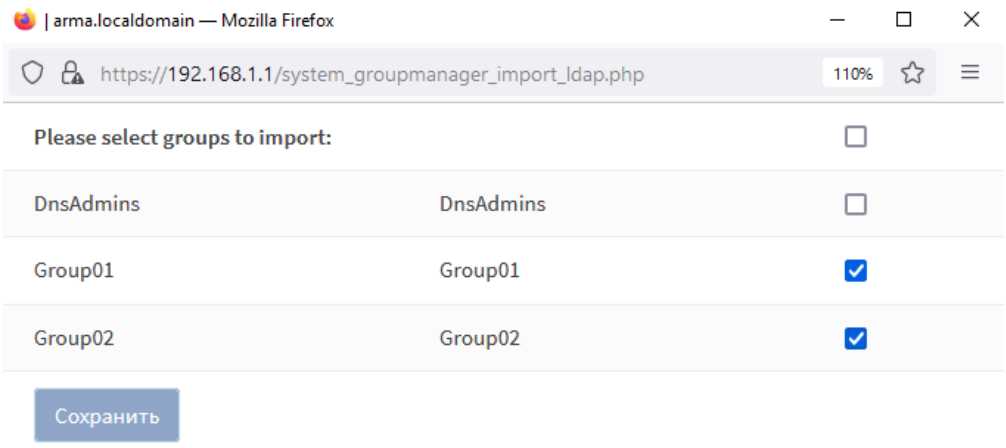


Рисунок – Выбор импортируемых пользовательских групп

Примечание:

Группы, содержащие в имени символы кириллицы, не отображаются в форме и не подлежат импорту.

Возможно настроить синхронизацию групп с помощью планировщика задач Cron (см. Cron). В случае использования планировщика задач производится автоматическое добавление новых и удаление отсутствующих групп внешнего сервера LDAP.

27.4.4 Radius

Radius – сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта пользователей, подключающихся к различным сетевым службам.

ARMA FW поддерживает использование внешнего Radius-сервера для аутентификации пользователей в сервисах VPN (см. VPN) и портала авторизации (см. Портал авторизации).

Перед началом настройки внешнего Radius-сервера необходимо убедиться в наличии сетевого доступа к данному серверу.

27.4.4.1 Добавление внешнего Radius-сервера

Для добавления внешнего Radius-сервера необходимо выполнить следующие действия:

1. Перейти в подраздел редактирования серверов авторизации (**«Система» - «Доступ» - «Серверы»**) и нажать **кнопку «+Добавить»**.
2. В открывшейся форме задать настройки в соответствии с таблицей (см. Таблица «Настройки Radius-сервера»). Значения параметров приведены справочно и зависят от настроек внешнего Radius-сервера.

Таблица «Настройки Radius-сервера»

Параметр	Значение
Описательное имя	Radius server
Тип	Radius
Имя хоста или IP-адрес	192.168.1.254
Общий секретный ключ	Указать секретный ключ сервера
Предложенные службы	Аутентификация и учёт

3. Остальные параметры оставить по умолчанию и нажать **кнопку «Сохранить»**.

27.4.4.2 Проверка работы внешнего Radius-сервера

Перед проверкой правильности настройки сервера необходимо создать две УЗ:

- **«user»** – с запретом доступа к **ARMA FW**;
- **«user1»** – с разрешением доступа к **ARMA FW**.

Для проверки правильности настройки сервера необходимо выполнить следующие действия:

1. Перейти в подраздел средств проверки (**«Система» - «Доступ» - «Средство проверки»**).
2. В параметре **«Сервер аутентификации»** выбрать созданный Radius-сервер, в параметрах **«Имя пользователя»** и **«Пароль»** ввести данные УЗ внешнего Radius-сервера и нажать **кнопку «Проверка»**:
   - УЗ **«user»** – не проходит аутентификацию с выводом соответствующего уведомления (см. Рисунок – Ошибка аутентификации);
   - УЗ **«user1»** – проходит аутентификацию с выводом соответствующего уведомления (см. Рисунок – Успешная аутентификация).

28 DR.WEB

Модуль Dr.Web позволяет с помощью веб-прокси осуществлять захват и сканирование проксируемого трафика HTTP и HTTPS на предмет вирусов, вредоносного ПО и пр., а также выполнять фильтрацию по базам нежелательных вредоносных или тематических ресурсов и в соответствии с пользовательскими правилами, реализуемыми модулем ICAPD.

Примечание:

Для функционирования службы Dr.Web требуется ключ активации лицензии.

Для настройки и тестирования функции антивирусной защиты используется схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки и тестирования функции антивирусной защиты).

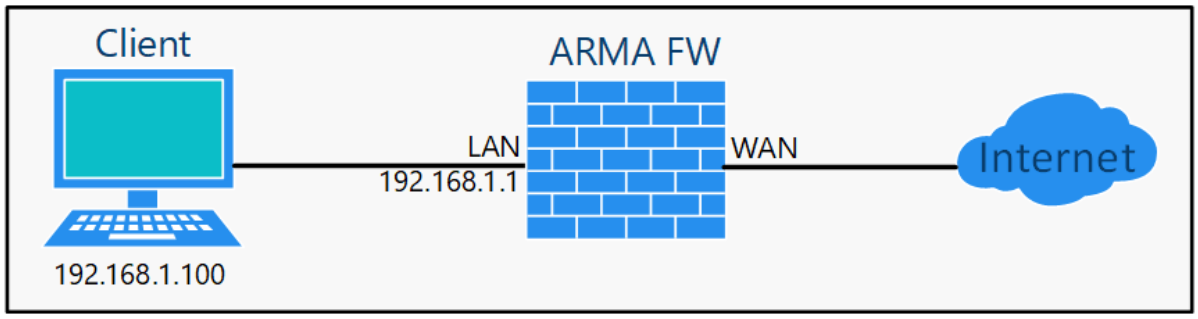


Рисунок – Схема стенда для настройки и тестирования функции антивирусной защиты

Для установки Dr.Web на **ARMA FW** необходимо выполнить следующие действия:

1. Скачать дистрибутив, предоставленный компанией «Доктор Веб».
2. Разместить файл-установщик Dr.Web в директории **«tmp» ARMA FW**.
3. Убедиться в наличии прав на исполнение файла-установщика и при необходимости обеспечить соответствующие права.
4. Установить пакет Dr.Web.

Для установки пакета Dr.Web на **ARMA FW** необходимо выполнить следующие действия:

- произвести аутентификацию в локальном консольном интерфейсе;
- нажать на клавиатуре **клавишу «8»**, а затем **клавишу «Enter»** для выбора пункта меню **«Shell»**;
- в запущенной командной строке ввести команду **«/tmp/drweb-11.1.4-av-igw-freebsd-amd64.run -- --non-interactive»** (см. Рисунок – Установка Dr.Web).

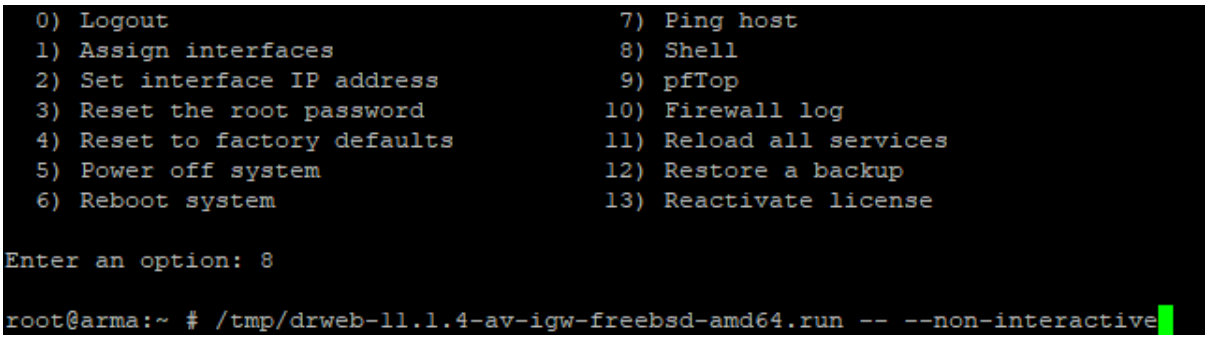


Рисунок – Установка Dr.Web

При успешном завершении установки пакета Dr.Web будет выведено соответствующее сообщение **«Nothing to do, exiting…Dr.Web packages repository is added to your repositories list.»**.

Перед настройкой антивирусной защиты необходимо настроить прокси-сервер (см. Настройка кэширующего прокси-сервера).

Для настройки функции антивирусной защиты необходимо выполнить следующие шаги:

1. Включить ICAP.
2. Настроить службу Dr.Web.
3. Проверить работу антивирусной защиты.

Необходимо убедиться в наличии разрешающих и отсутствии запрещающих правил МЭ для соединения по указанному адресу ICAP.

В случае использования адресов loopback следует убедиться в том, что loopback-интерфейсы включены и корректно настроены.

Примечание:

Включённая служба Dr.Web приводит к увеличению потребления ресурсов и повышает требования к аппаратному обеспечению. В случае нехватки ресурсов возможны сбои в работе **ARMA FW**.

28.1 Шаг 1. Включение ICAP

Для включения ICAP необходимо выполнить следующие действия:

1. Перейти в подраздел настроек прокси-сервера (**«Службы» - «Веб-прокси» - «Администрирование»**).
2. Раскрыть вкладку **«Перенаправляющий прокси»**, нажав **кнопку** « ▼ », и выбрать **«Настройки ICAP»** (см. Рисунок – Выбор настроек перенаправляющего прокси-сервера).

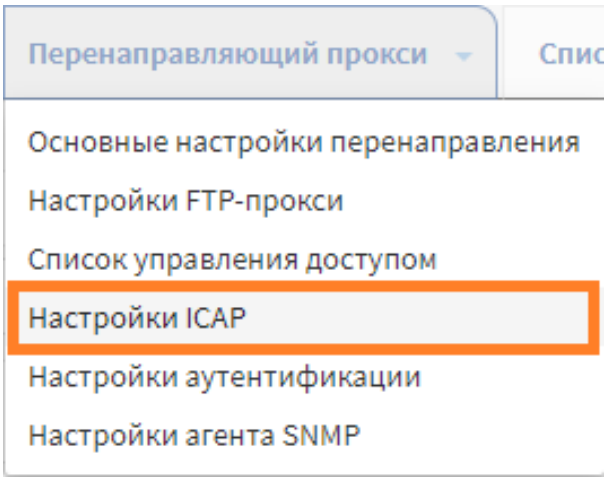


Рисунок – Выбор настроек перенаправляющего прокси-сервера

3. Установить флажок **«Включить ICAP»** и нажать **кнопку «Применить»** (см. Рисунок – Настройка ICAP).

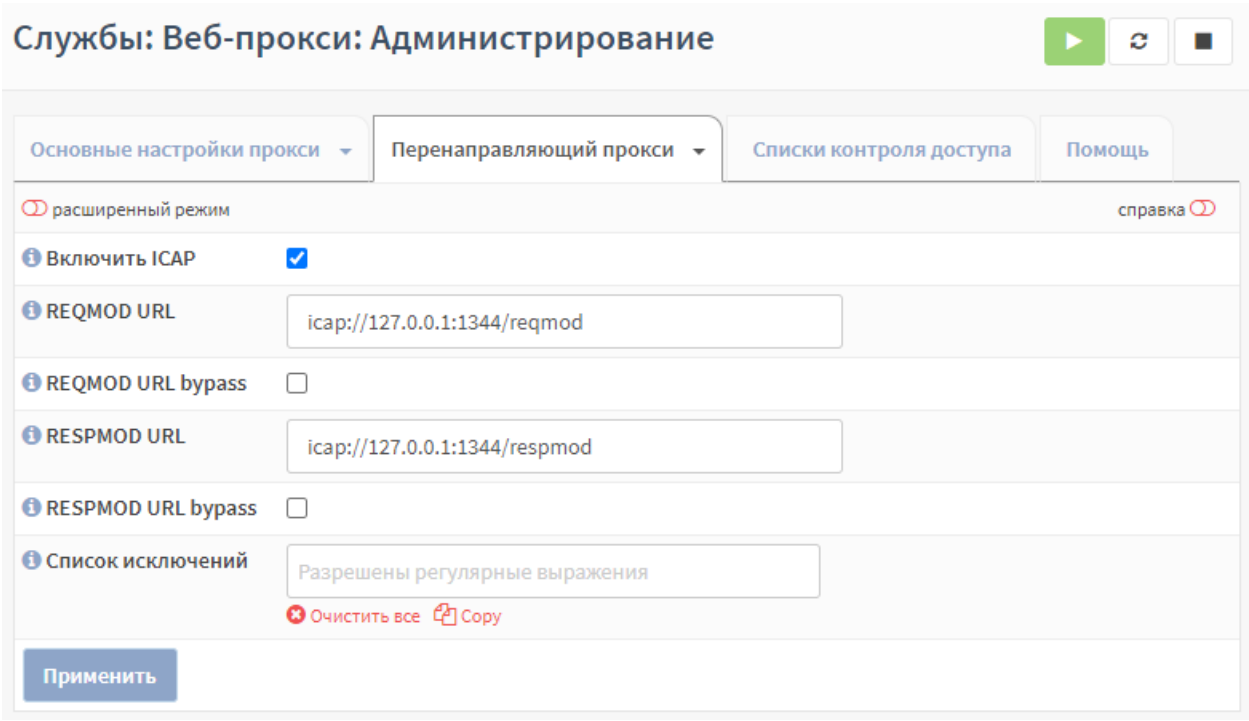


Рисунок – Настройка ICAP

В случае необходимости продолжения направления трафика прокси сервером при условии отсутствия доступности сервера ICAP следует установить флажки для параметров **«REQMOD URL bypass»** и **«RESPMOD URL bypass»**, затем применить изменения настроек.

28.2 Шаг 2. Настройка службы Dr.Web

Для настройки службы Dr.Web необходимо выполнить следующие действия:

1. Перейти в подраздел настройки Dr.Web (**«Службы» - «Dr.Web» - «Конфигурация»**) (см. Рисунок – Включение службы Dr.Web).

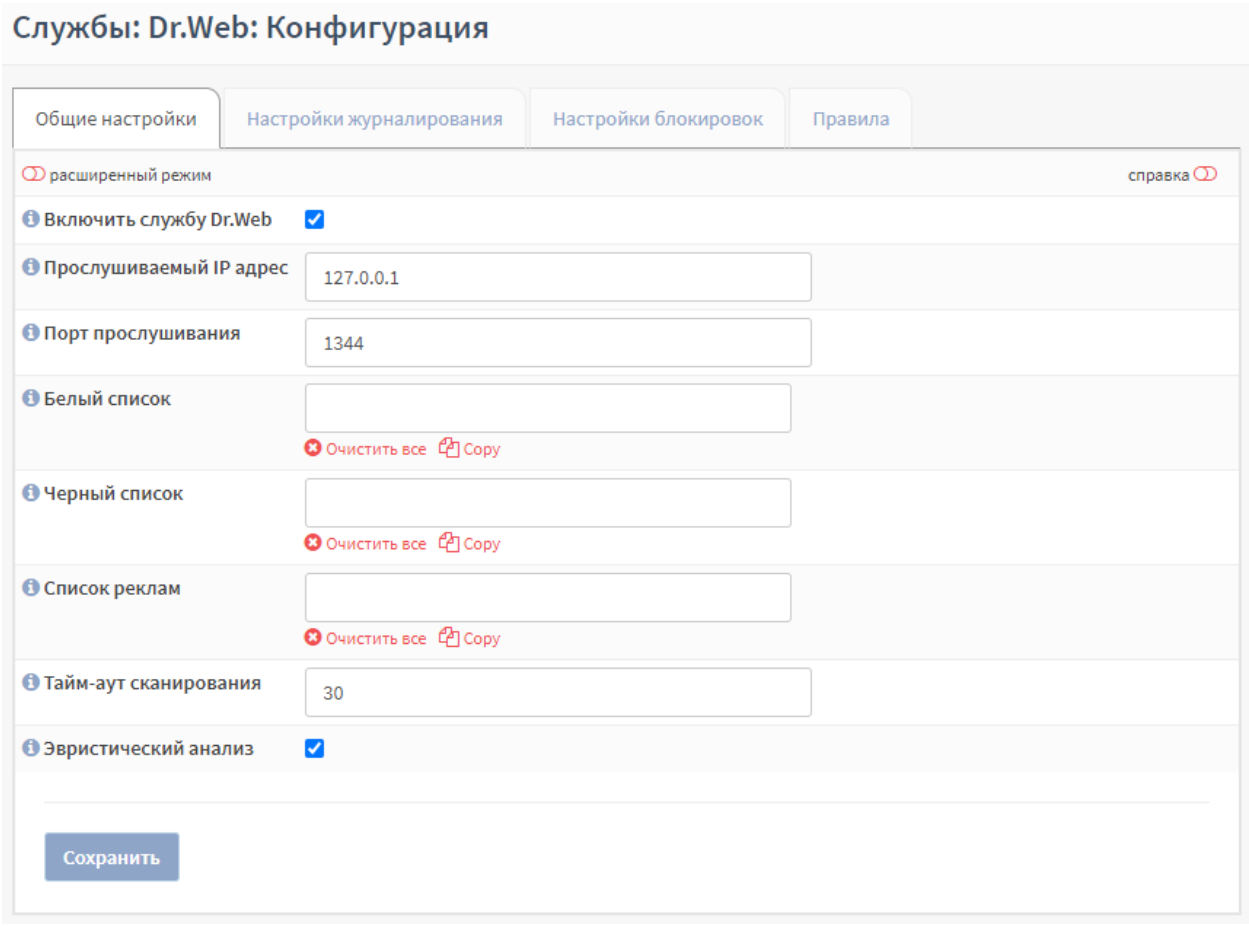


Рисунок – Включение службы Dr.Web

2. Установить флажок **«Включить службу Dr.Web»**, остальные параметры оставить без изменения и нажать **кнопку «Сохранить»**.

   Примечание:

   В случае отсутствия ключа активации лицензии Dr.Web, служба не будет запущена.

3. Перейти во вкладку **«Настройки журналирования»**, оставить параметры без изменения и нажать **кнопку «Сохранить»** (см. Рисунок – Настройки журналирования Dr.Web).

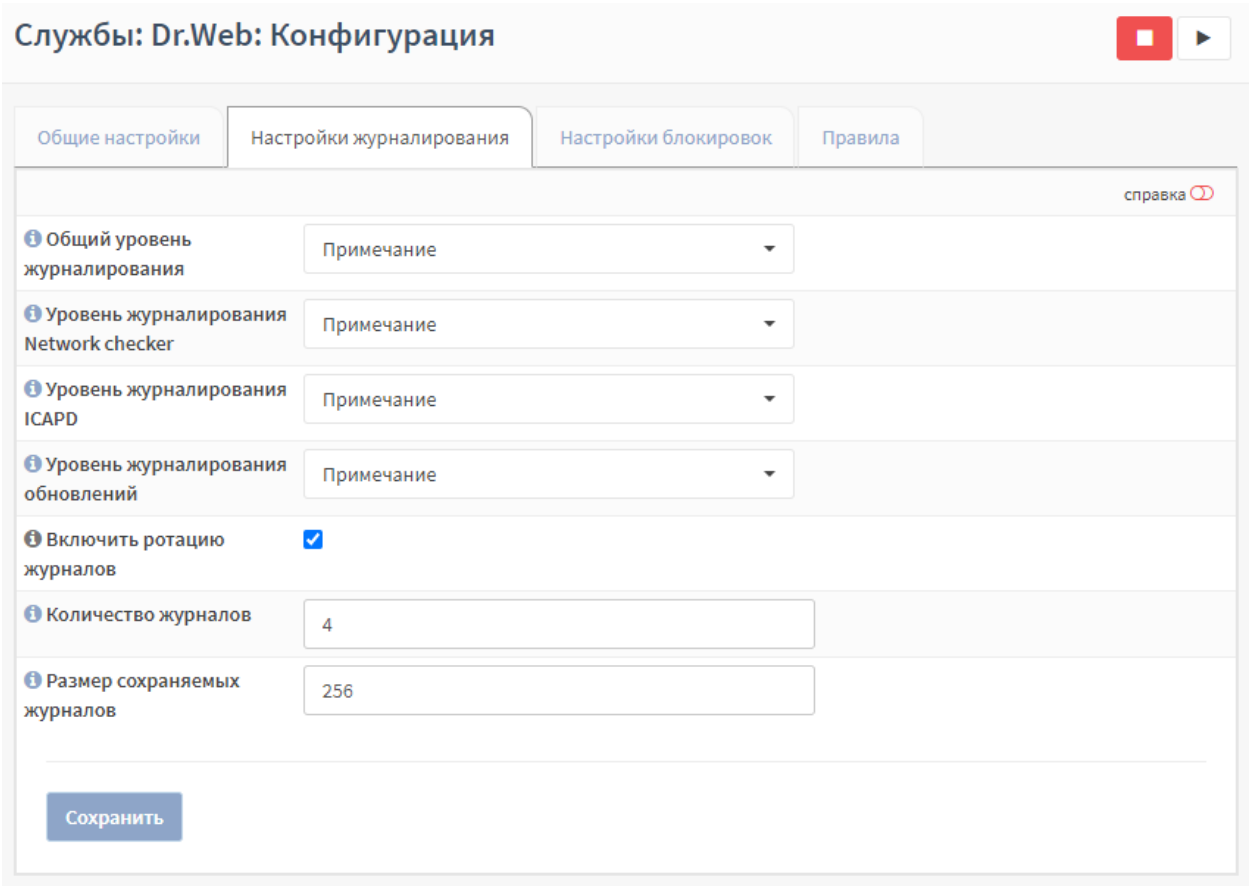


Рисунок – Настройки журналирования Dr.Web

4. Перейти в подраздел управления лицензией Dr.Web (**«Службы» - «Dr.Web» - «Лицензия»**) и нажать **кнопку «Выберите файл»** (см. Рисунок – Лицензия Dr.Web). В открывшемся окне проводника указать файл, содержащий ключ активации лицензии, предоставленный компанией «Доктор Веб», и нажать **кнопку «Открыть»**.

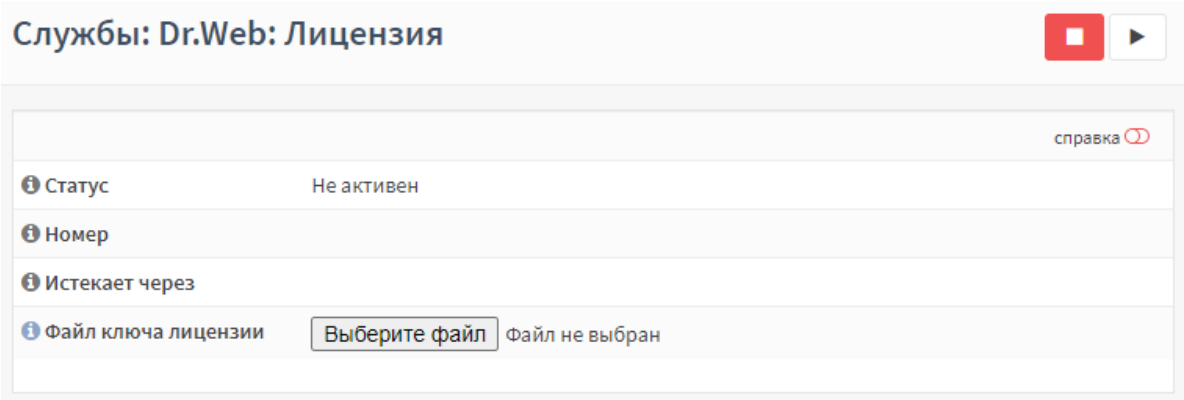


Рисунок – Лицензия Dr.Web

По истечении непродолжительного времени статус изменится на «Активный» и отобразится информация о номере, а также дате и времени окончания периода активации.

Примечание:

Для отображения актуального статуса состояния лицензии необходимо предварительно включить службу Dr.Web.

5. Нажать на **кнопку** « » для перезапуска службы Dr.Web.
6. Перейти во вкладку **«Настройки блокировок»** подраздела настройки Dr.Web (**«Службы» - «Dr.Web» - «Конфигурация»**), установить флажки напротив категорий, соответствующих тематике информации, подлежащей блокированию и нажать **кнопку «Сохранить»**.

28.2.1 Создание пользовательских правил

Модуль ICAPD в **ARMA FW** позволяет создавать пользовательские правила для фильтрации проксируемого трафика.

Для добавления пользовательского правила фильтрации проксируемого трафика необходимо выполнить следующие действия:

1. Перейти во вкладку **«Правила»** подраздела настройки Dr.Web (**«Службы» - «Dr.Web» - «Конфигурация»**) (см. Рисунок – Лицензия Dr.Web) и нажать **кнопку** « ».

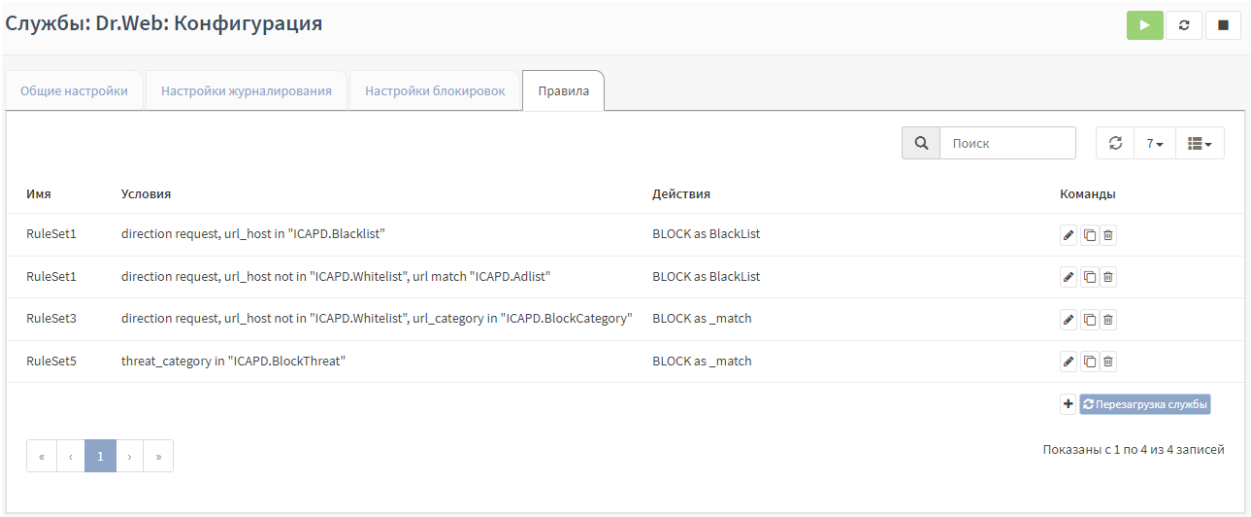


Рисунок – Правила Dr.Web

2. В открывшейся форме выбрать набор правил в поле параметра **«Имя»**, заполнить поля для параметров **«Условия»** и **«Действия»**, затем нажать **кнопку «Сохранить»**.

28.3 Шаг 3. Проверка антивирусной защиты

Для проверки работоспособности функции антивирусной защиты необходимо выполнить следующие действия:

1. На ПК **«Client»** запустить веб-браузер, перейти по ссылке:
   - «https://www.eicar.org/download-anti-malware-testfile/»

   и скачать файл **«eicar.txt»** (см. Рисунок – Скачивание файла eicar.txt).

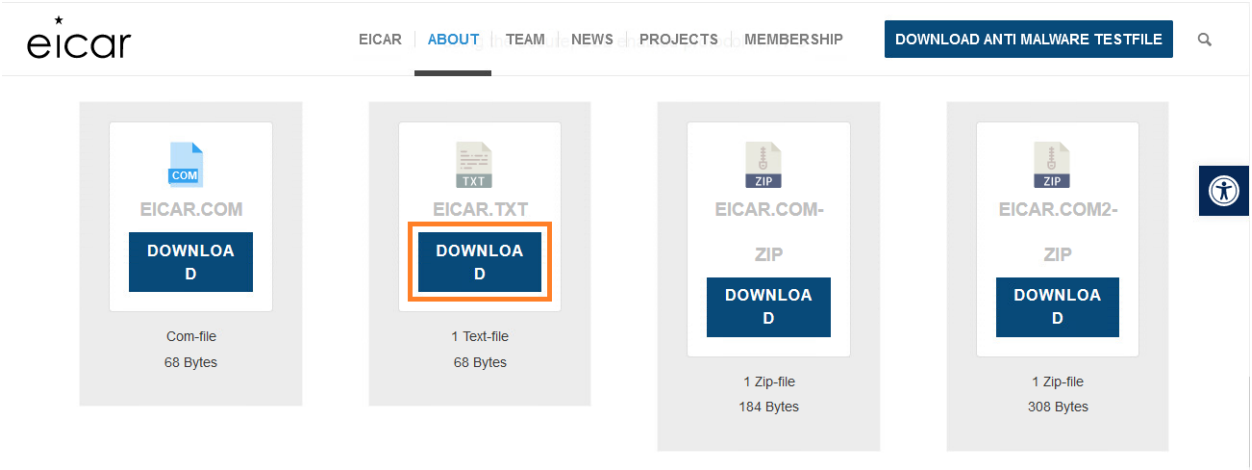


Рисунок – Скачивание файла eicar.txt

2. Убедиться в наличии уведомления в веб-браузере об обнаружении вредоносного ПО при скачивании файла (см. Рисунок – Уведомление антивируса об обнаружении вредоносного ПО).

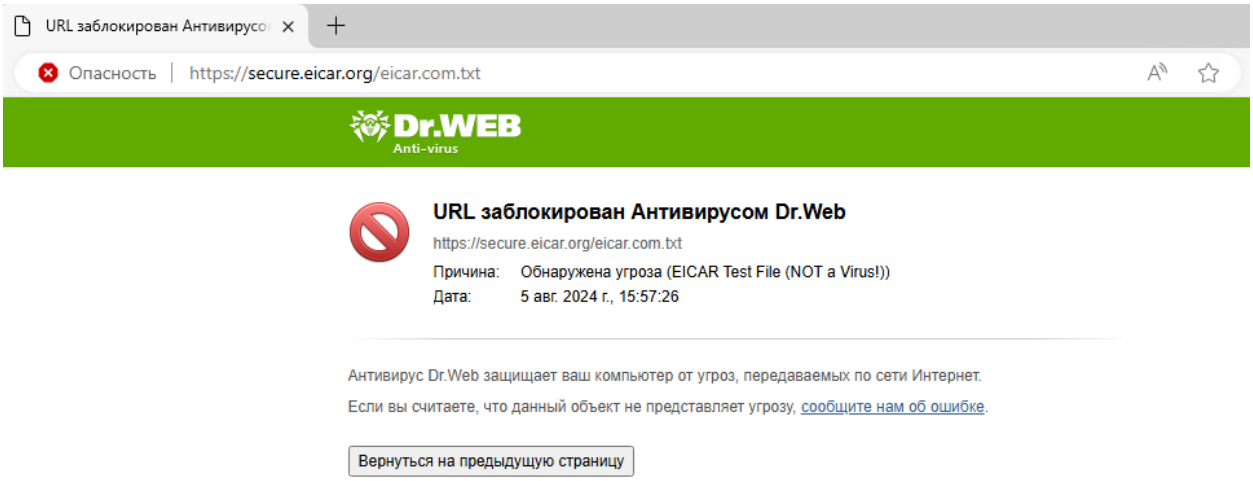


Рисунок – Уведомление антивируса об обнаружении вредоносного ПО

3. На **ARMA FW** убедиться в наличии записей в журнале ICAPD (**«Службы» - «Dr.Web» - «Журнал ICAPD»**) (см. Рисунок – Событие в журнале ICAPD).

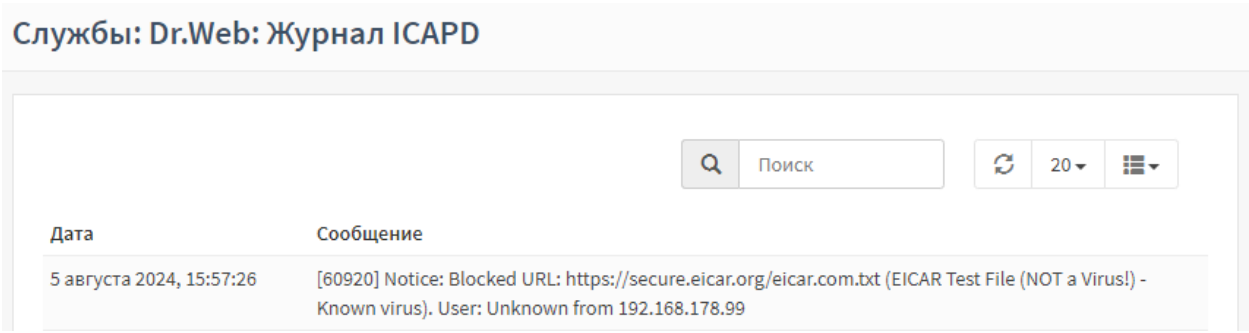


Рисунок – Событие в журнале ICAPD

29 DNSMASQ DNS

Dnsmasq – легковесный и быстроконфигурируемый проксирующий DNS-, DHCP- и TFTP-сервер, предназначенный для работы в небольших сетях.

В режиме DNS-сервера Dnsmasq обеспечивает доменными именами локальные хосты, не имеющие глобальных DNS-записей. DHCP-сервер интегрирован с DNS-сервером и назначает хостам с IP-адресом доменное имя, сконфигурированное ранее в конфигурационном файле, поддерживает привязку IP-адреса к хосту или автоматическую настройку IP-адресов из заданного диапазона и BOOTP для сетевой загрузки бездисковых машин.

В качестве примера настройки Dnsmasq будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда настройки Dnsmasq). На ПК **«Client»** установлена ОС Windows.

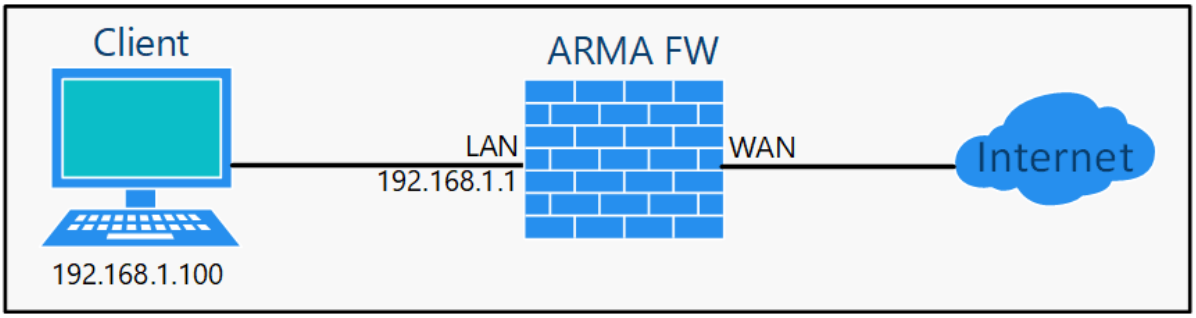


Рисунок – Схема стенда настройки Dnsmasq

29.1 Настройка Dnsmasq DNS

Для настройки Dnsmasq DNS необходимо выполнить следующие действия:

1. Перейти в подраздел настроек кэширующего DNS-сервера (**«Службы» - «Кэширующий DNS-сервер» - «Общие настройки»**) и убрать флажок для параметра **«Включить»**.
2. Перейти в подраздел настроек Dnsmasq DNS (**«Службы» - «Dnsmasq DNS» - «Настройки»**) (см. Рисунок – Включение Dnsmasq), установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**.

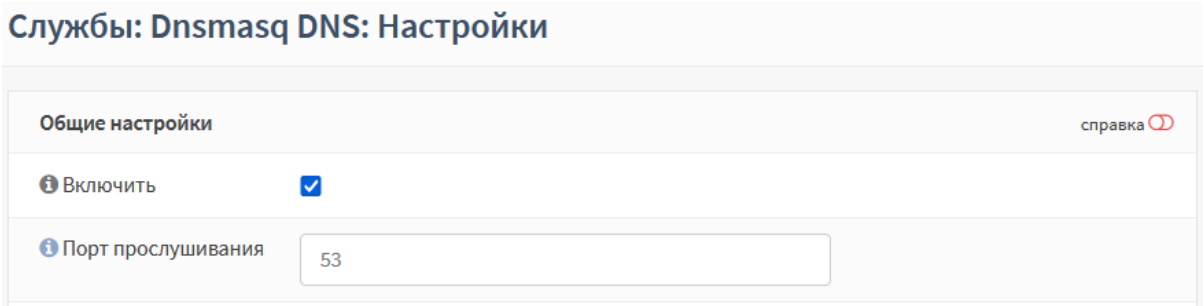


Рисунок – Включение Dnsmasq

Примечание:

При использовании динамических интерфейсов не рекомендуется привязываться к адресам из этих интерфейсов.

29.1.1 Дополнительные настройки Dnsmasq DNS

Параметр **«DNSSEC»** рекомендуется включать в целях минимизирования атак, связанных с подменой DNS-адреса при разрешении доменных имён.

Вариант **«Перенаправление запросов DNS»** параметра **«Переадресация DNS-запросов»** рекомендуется включать для опроса DNS-серверов по порядку, указанному в блоке настроек DNS-сервера (**«Система» - «Настройки» - «Общие настройки»**), вместо параллельного запроса всем указанным DNS-серверам.

Для создания отдельных записей определения хоста или домена необходимо нажать **кнопку** « + » в соответствующем блоке (см. Рисунок – Переопределение хоста или домена), задать значения в открывшейся форме и нажать **кнопку «Сохранить»**, а затем **кнопку «Применить изменения»**.

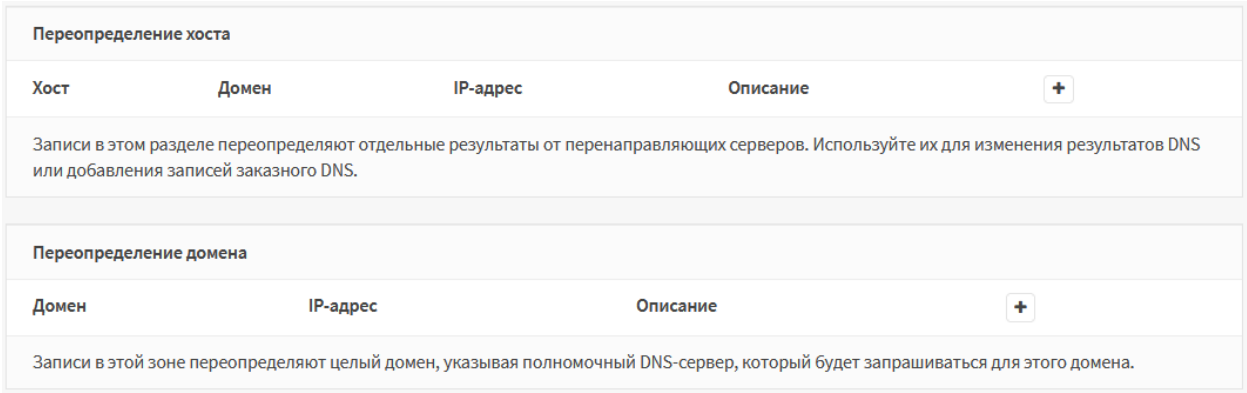


Рисунок – Переопределение хоста или домена

29.1.2 Фильтрация динамических поддоменов с помощью Dnsmasq

Dnsmasq предоставляет возможность ограничить доступ к определённым динамическим поддоменам.

В качестве примера рассмотрим блокировку доступа к домену «google.com» и к его динамическим поддоменам. Для этого необходимо выполнить следующие действия:

1. Создать псевдоним с именем **«google»** и типом **«Внешний (расширенный)»** (см. Создание псевдонимов).
2. Отключить **«Кеширующий DNS сервер»**.
3. Перейти в настройки **«Dnsmasq DNS»**.
4. Нажать **кнопку «Показать дополнительные параметры»** в пункте **«Дополнительно»** и ввести в открывшееся поле параметры фильтрации: **ipset=/google.com/google** (см. Рисунок – Настройка блокировки поддоменов).

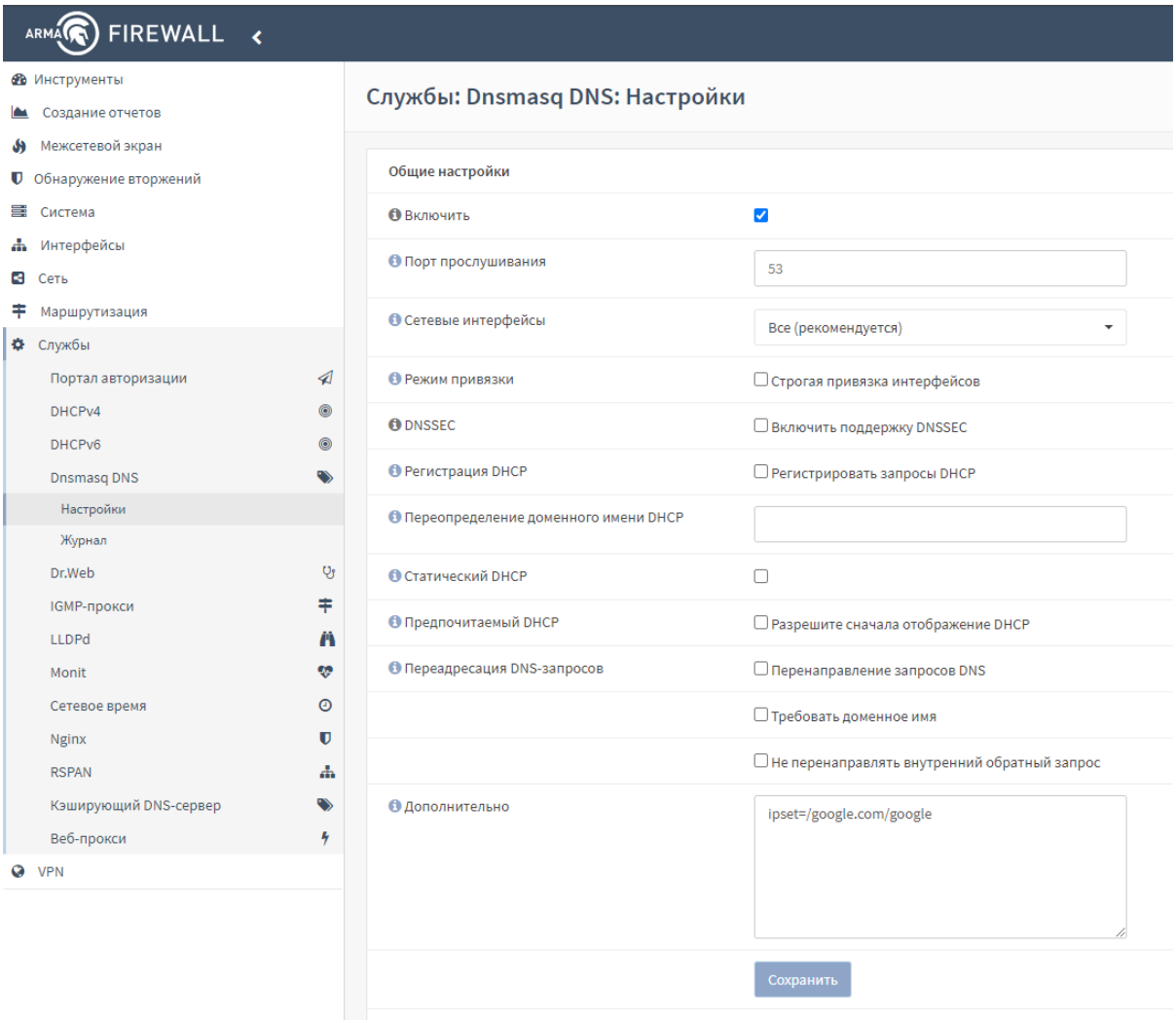


Рисунок – Настройка блокировки поддоменов

5. Установить флажок для параметра **«Включить»** и нажать **кнопку «Сохранить»**.
6. Создать на основе псевдонима **«google»** блокирующее правило МЭ (см. Создание правил межсетевого экранирования).
7. На клиентских компьютерах установить IFW в качестве основного DNS-сервера.

Если при создании блокирующего правила не был задан параметр **«Сбрасывать установленные состояния»**, то все соединения, установленные до применения правила, продолжат работать.

29.2 Проверка работы Dnsmasq DNS

Для проверки работы Dnsmasq DNS необходимо выполнить следующие действия:

1. На ПК **«Client»** указать для используемого сетевого подключения IP-адрес **ARMA FW** в качестве предпочитаемого DNS-сервера (см. Рисунок – Настройка параметров сети).

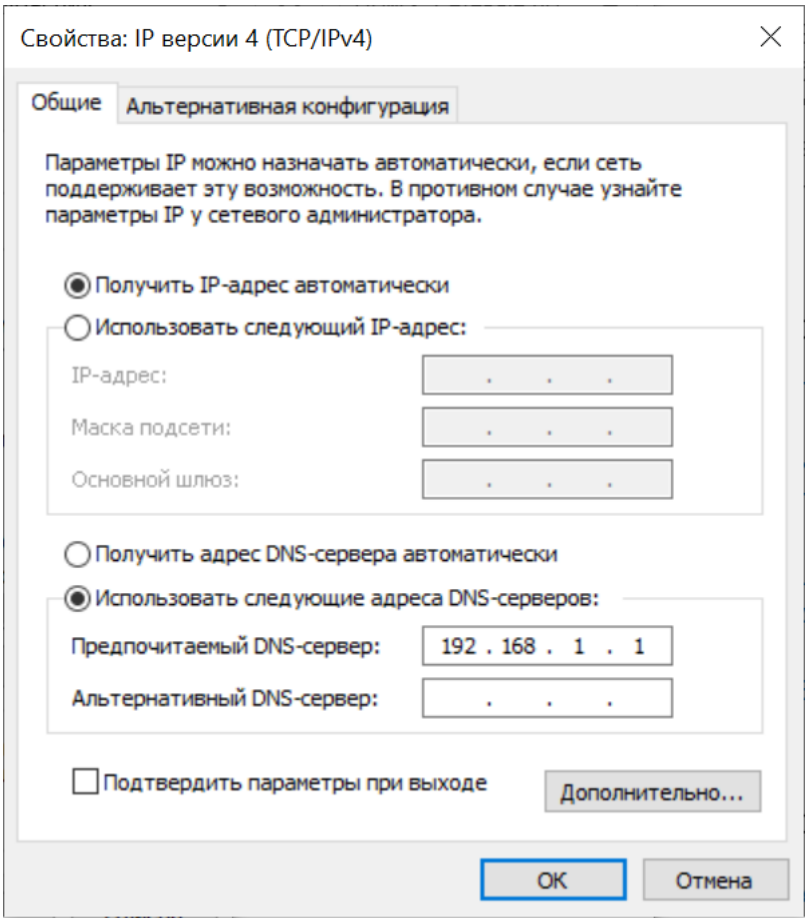


Рисунок – Настройка параметров сети

2. На ПК **«Client»** открыть веб-браузер и перейти на сайт «ya.ru». Работоспособность Dnsmasq DNS проверяется успешным подключением к сайту.

30 IGMP-ПРОКСИ

ARMA FW поддерживает групповую передачу данных с использованием протокола IGMP, в случае необходимости обеспечения многоадресного вещания.

В качестве примера настройки IGMP-прокси будет использоваться схема стенда, представленная на рисунке (см. Рисунок – Схема стенда для настройки IGMP-прокси).

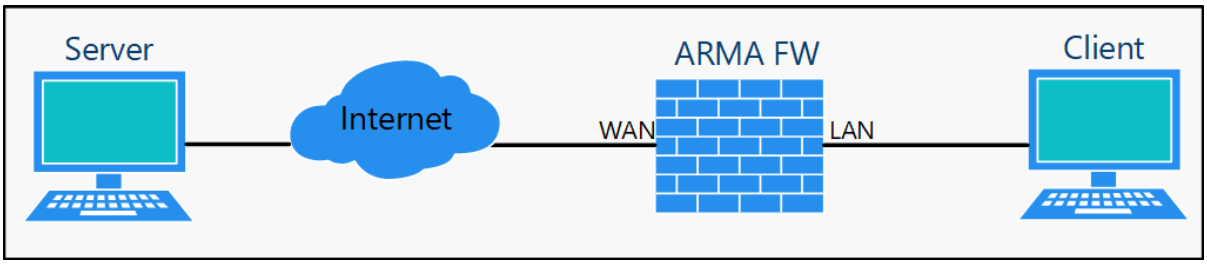


Рисунок – Схема стенда для настройки IGMP-прокси

30.1 Настройка IGMP-прокси

Для настройки IGMP-прокси необходимо выполнить следующие действия:

1. Перейти в подраздел настройки IGMP-прокси (**«Службы» - «IGMP-прокси»**).
2. Нажать **кнопку «+Добавить»**, ввести в открывшейся форме следующие параметры (см. Рисунок – Настройка IGMP-прокси):
   - **«Интерфейс»** – «WAN»;
   - **«Тип»** – «Публичный интерфейс»;
   - **«Сеть»** – адрес сети источника многоадресного вещания, например «198.51.100.0»;
   - **«CIDR»** – маска сети, например «24»;

   и нажать **кнопку «Сохранить»**.

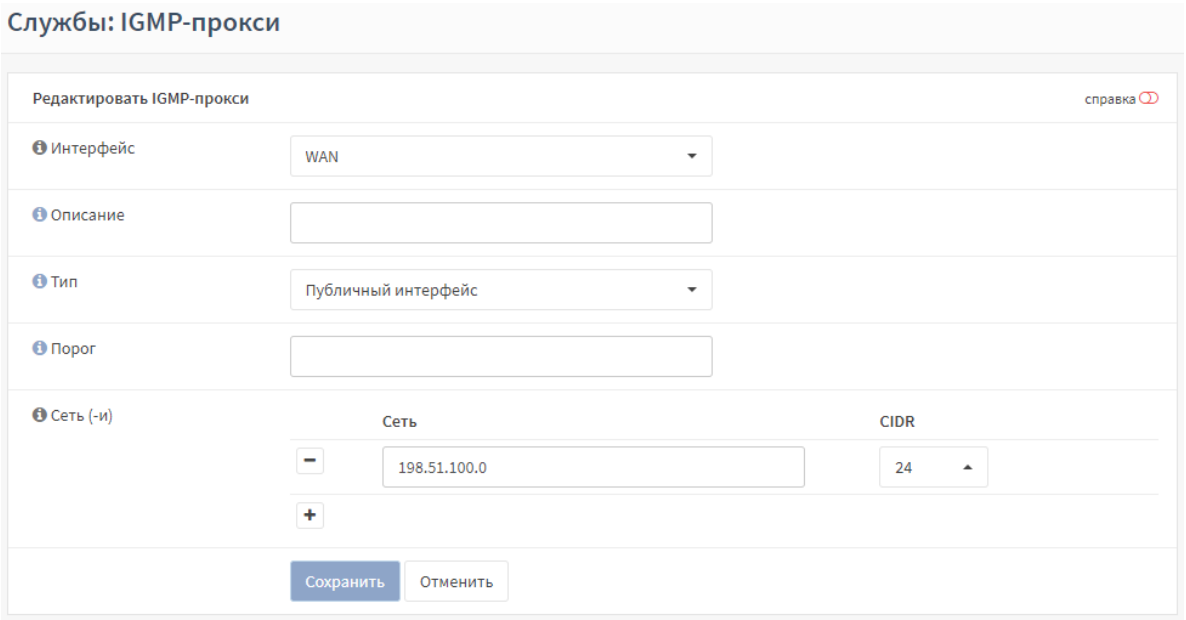


Рисунок – Настройка IGMP-прокси

3. Нажать **кнопку «+Добавить»**, ввести в открывшейся форме следующие параметры:

   - **«Интерфейс»** – «LAN»;
   - **«Описание»** – «multicast»;
   - **«Тип»** – «Внутренний интерфейс»;
   - **«Сеть»** – адрес сети назначения, например «192.168.7.0»;
   - **«CIDR»** – маска сети, например «24»;

   и нажать **кнопку «Сохранить»**.

   Примечание:

   Не следует добавлять несколько публичных интерфейсов (см. Рисунок – IGMP-прокси).

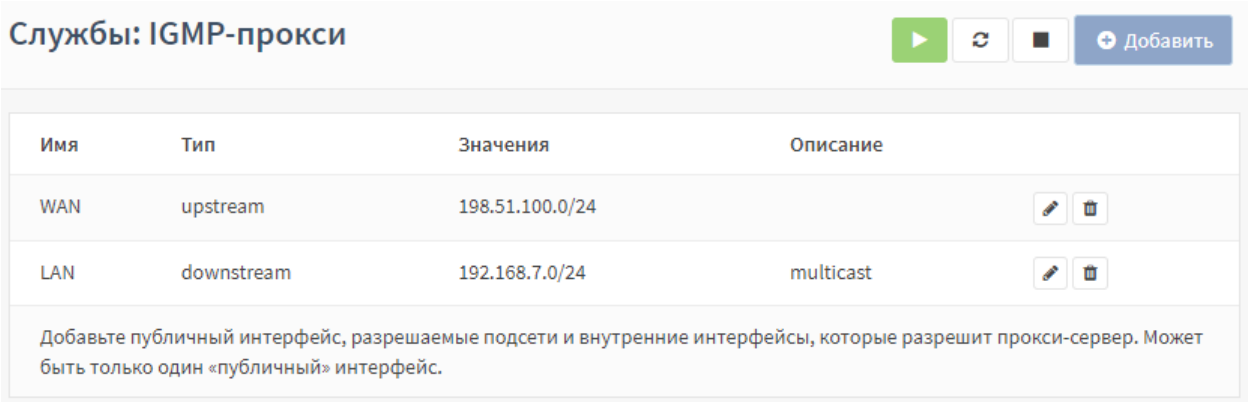


Рисунок – IGMP-прокси

Для обеспечения передачи трафика необходимо создать разрешающие правила МЭ (см. Создание правил межсетевого экранирования) со следующими параметрами:

- правило №1:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Интерфейс»** – «WAN»;
  - **«Направление»** – «Вх.»;
  - **«Протокол»** – «IGMP»;
  - **«Отправитель»** – «любой»;
  - **«IP-адрес назначения»** – «Единственный хост или сеть», «224.0.0.0», «4»;
  - **«Описание»** – «Allow IGMP»;
  - **«Дополнительные параметры»**:
    - **«Разрешить параметры»** – флажок установлен;
- правило №2:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Интерфейс»** – «WAN»;
  - **«Направление»** – «Вх.»;
  - **«Протокол»** – «UDP»;
  - **«Отправитель»** – «любой»;
  - **«IP-адрес назначения»** – «Единственный хост или сеть», «224.0.0.0», «4»;
  - **«Описание»** – «Allow UDP»;
  - **«Дополнительные параметры»**:
    - **«Разрешить параметры»** – флажок установлен;
- правило №3:
  - **«Действие»** – «Разрешить (Pass)»;
  - **«Интерфейс»** – «LAN»;
  - **«Направление»** – «Вх.»;
  - **«Отправитель»** – «LAN сеть»;
  - **«Дополнительные параметры»**:
    - **«Разрешить параметры»** – флажок установлен.

31 CRON

Cron – это служба, используемая в качестве планировщика задач в **ARMA FW**.

Планировщик задач позволяет выполнять различные задания в определённое время или с определённой периодичностью.

В качестве примера будет рассмотрен следующий сценарий использования планировщика заданий Cron:

- действие – перезагрузка **ARMA FW**;
- периодичность – каждую субботу;
- время перезагрузки – 18 часов 30 минут.

Для добавления задания необходимо выполнить следующие действия:

1. Перейти в подраздел планировщика задач (**«Система» - «Настройки» - «Планировщик задач Cron»**) и нажать **кнопку** « + ».
2. В появившейся форме (см. Рисунок – Редактирование задачи) указать следующие значения для параметров:
   - **«Мин»** – «30»;
   - **«Ч»** – «18»;
   - **«День недели»** – «6»;
   - **«Команда»** – «Выполнить перезагрузку»;
   - **«Описание»** – «Перезагрузка каждую субботу».

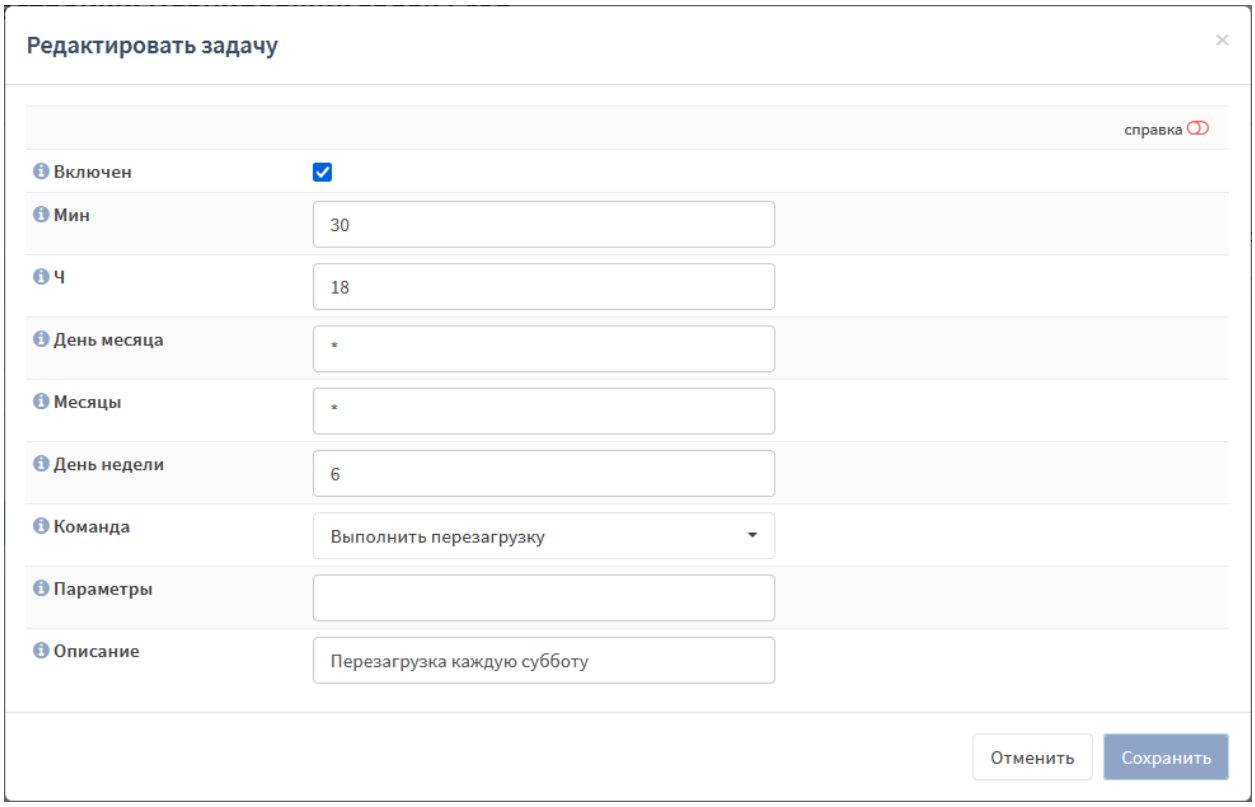


Рисунок – Редактирование задачи

3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

В результате новая задача будет добавлена в список (см. Рисунок – Список планировщика задач) и каждую субботу в 18:30 будет выполнена перезагрузка **ARMA FW**.

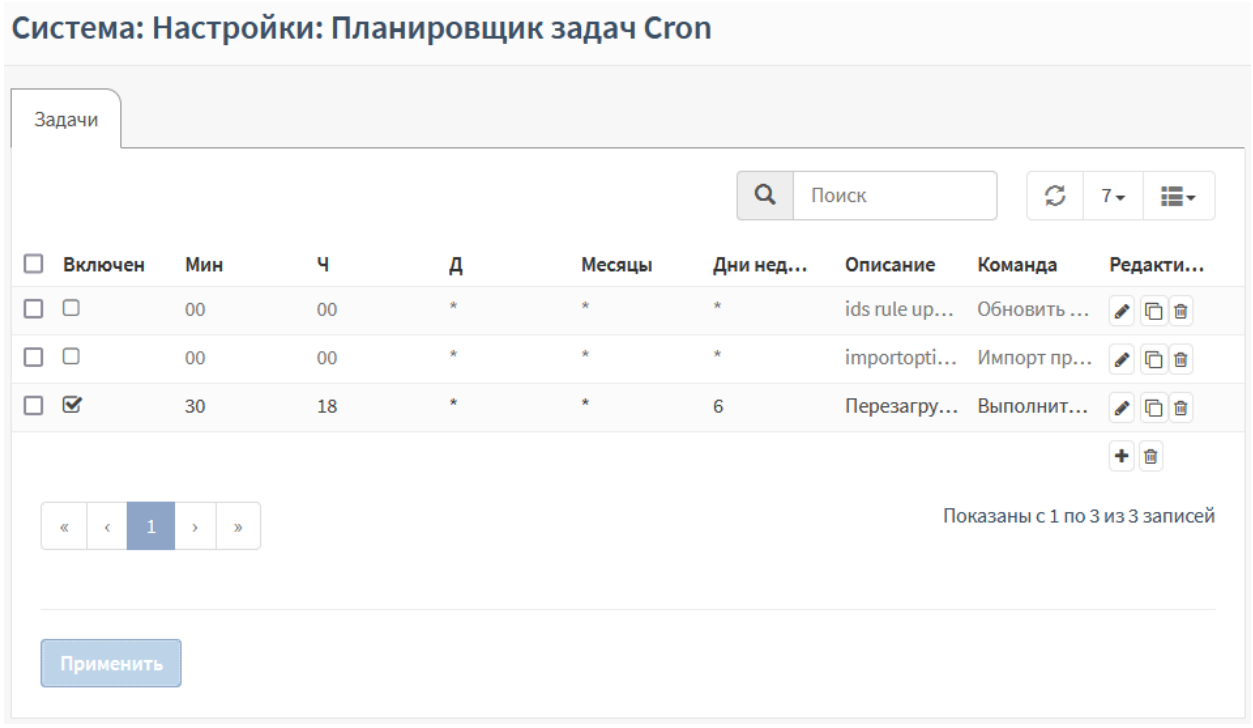


Рисунок – Список планировщика задач

Примечание:

По умолчанию в планировщике созданы две задачи СОВ, являющиеся системными и не подлежащие удалению.

31.1 Особенности параметров, используемых в задачах

Во всех полях временных параметров задачи возможно указать единичное значение, перечень значений, разделённых знаком «запятая», и диапазон значений, разделённых знаком «минус»:

- «4»;
- «1,3,6»;
- «2-7».

Значения разных параметров будут объединены, например, для параметров:

- **«Мин»** – «20,30»;
- **«Ч»** – «10,22»;
- **«Месяц»** – «1,3»;
- **«День недели»** – «1-5»;

задача будет выполняться с понедельника по пятницу, января и марта, в 10:20, 10:30, 22:20 и 22:30.

31.2 Задачи планировщика

Планировщик задач позволяет выполнять следующие задания:

- **«Автоматический бан для атакующих хостов»** – выполняет блокирование атакующих хостов;
- **«Восстановить DH параметры»** – генерирует DH параметры для введённой длины ключа, указанного в поле **«Параметры»**. Если длина ключа не указана, то параметры генерируются для следующих значений: «1024», «2048», «4096»;
- **«Выполнить перезагрузку»** – выполняет перезагрузку **ARMA FW**;
- **«Выполнять периодическое обновление интерфейса»** – обновляет настройки интерфейса (см. Сетевые интерфейсы), указанного в поле **«Параметры»**. Если интерфейс не указан, то выполняется обновление интерфейса «WAN»;
- **«Импорт правил СОВ»** – импортирует правила СОВ согласно настройкам, указанным в подразделе настройки импорта правил СОВ (**«Обнаружение вторжений» - «Настройка импорта правил»**);

- **«Обновить ACL с внешнего прокси»** – обновляет чёрный список веб-адресов прокси-сервера (см. Прокси) согласно спискам контроля доступа. Списки указываются в подразделе управления списками контроля доступа (**«Веб-прокси» - «Администрирование» - «Списки контроля доступа»**);
- **«Обновить ACL с внешнего прокси и перезагрузить сервис»** – дополнительно к **«Обновить ACL с внешнего прокси»** производит перезапуск службы, отвечающей за работу прокси-сервера в случае неудачной загрузки чёрного списка веб-адресов;
- **«Обновить GeoIP»** – выполняет обновление локальной базы IP-адресов (см. Обновление локальной базы IP-адресов);
- **«Обновить и перезагрузить правила обнаружения вторжений»** – добавляет импортированные правила в действующие правила СОВ и перезапускает службу, отвечающую за правила обнаружения вторжений (см. Система обнаружения и предотвращения вторжений);
- **«Обновить и перезагрузить псевдонимы и GeoIP межсетевого экрана»** – выполняет перезапуск службы, отвечающей за псевдонимы МЭ (см. Создание псевдонимов);
- **«Перезагрузить правила обнаружения вторжений»** – выполняет перезапуск службы, отвечающей за правила обнаружения вторжений (см. Система обнаружения и предотвращения вторжений);
- **«Перезапустить FRR»** – выполняет перезапуск сервиса маршрутизации FRR;
- **«Перезагрузить сервис IPsec»** – выполняет перезапуск службы, отвечающей за VLAN IPsec (см. VLAN);
- **«Перезапустить сервис портала авторизации»** – выполняет перезапуск службы, отвечающей за портал авторизации (см. Портал авторизации);
- **«Пересчитать все чек-суммы»** – выполняет проверку контроля целостности системы, процесс запуска проверки контроля целостности описан в разделе **«Контроль целостности»** Руководства администратора **ARMA FW**;
- **«Проверить обновления правил suricata»** – выполняет проверку наличия обновлений правил СОВ на внешнем сервере (см. Обновление правил СОВ с внешнего сервера);
- **«Синхронизация LDAP групп»** – выполняет синхронизацию групп LDAP (см. LDAP), при настроенном сервере LDAP, отличным от Active Directory, возможно отсутствие разделения импортируемых групп и пользователей;

- **«Синхронизация LDAP пользователей»** – выполняет синхронизацию пользователей LDAP (см. LDAP), при настроенном сервере LDAP, отличным от Active Directory, возможно отсутствие разделения импортируемых групп и пользователей;
- **«Экспорт конфигурации»** – выполняет экспорт конфигурации на удалённый сервер, процесс экспорта конфигурации описан в разделе **«Экспорт конфигурации на удалённый FTP/SMB-сервер»** Руководства администратора **ARMA FW**.

32 МОНИТОРИНГ, СТАТИСТИКА, ДИАГНОСТИКА

32.1 Мониторинг системы с помощью информационных виджетов

ARMA FW позволяет производить мониторинг текущего состояния с помощью различных виджетов.

Панель виджетов доступна в разделе **«Инструменты»**, являющимся по умолчанию стартовым разделом после аутентификации в **ARMA FW** (см. Рисунок – Панель виджетов).

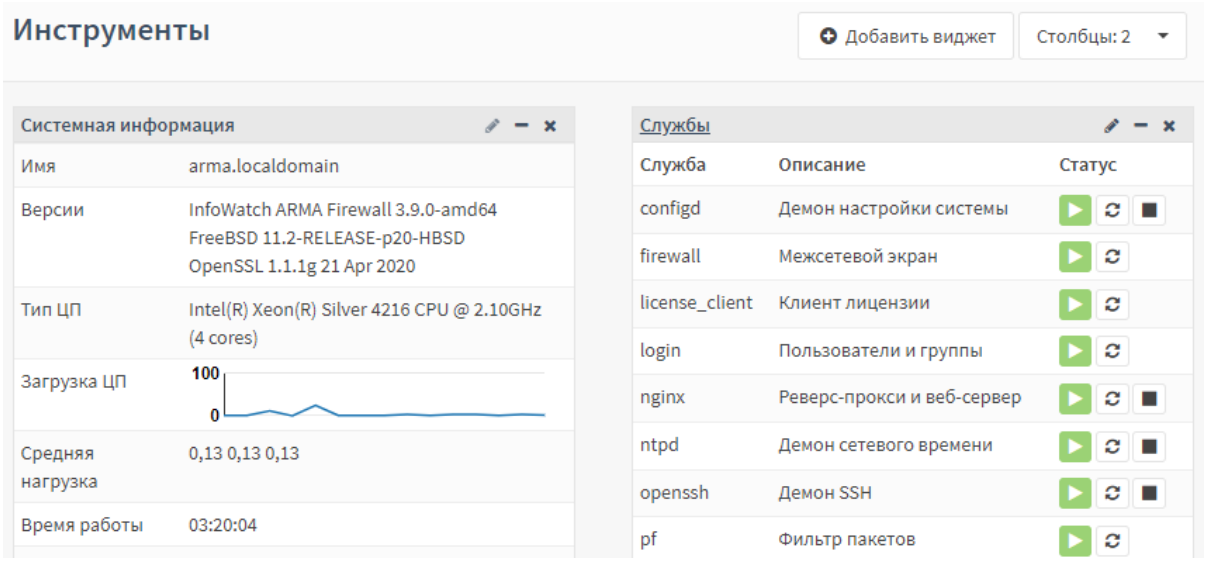


Рисунок – Панель виджетов

Существует возможность перемещения виджетов с помощью мыши. Для этого необходимо навести курсор мыши на заголовок виджета, зажать **левую кнопку мыши**, переместить виджет в требуемое положение и отпустить **левую кнопку мыши**.

Количество отображаемых столбцов выбирается с помощью выпадающего списка **«Столбцы»** в верхней правой части раздела.

Для сохранения местоположения виджетов и количества столбцов необходимо нажать **кнопку «Сохранить настройки»**.

32.1.1 Добавление виджетов

Для добавления виджета необходимо выполнить следующие действия:

1. Нажать **кнопку «+Добавить виджет»** и выбрать требуемый виджет в открывшейся форме доступных виджетов (см. Рисунок – Добавление виджетов). За один раз возможно выбрать несколько виджетов.
2. Нажать **кнопку «Закрыть»**, а затем нажать **кнопку «Сохранить настройки»**.

Рисунок – Добавление виджетов

В **ARMA FW** доступны следующие виджеты для мониторинга текущего состояния:

- **«CARP»** – отображает статус устройства в режиме работы кластера;
- **«Использование ЦП»** – отображает график загрузки ЦП в режиме реального времени;
- **«Шлюзы»** – отображает статус работы настроенных шлюзов, время приёма-передачи и процент потерь;
- **«Интерфейсы»** – отображает включённые сетевые интерфейсы и их основные параметры: имя, скорость и режим передачи, IP-адрес;
- **«Статистика интерфейса»** – отображает сводную таблицу по всем настроенным интерфейсам в режиме реального времени;
- **«IPsec»** – отображает настроенные IPsec туннели;
- **«Информация о лицензии»** – отображает информацию о лицензии;
- **«Журнал межсетевого экрана»** – отображает таблицу событий МЭ в режиме реального времени;
- **«Monit»** – отображает состояния почтовых серверов, доступность различных сервисов и ресурсов, состояние сетевых сервисов;
- **«Сетевое время»** – отображает текущее время системы, а также информацию о сервере синхронизации времени;
- **«OpenVPN»** – отображает настроенные OpenVPN серверы;
- **«Службы»** – отображает статус работы настроенных служб и позволяет остановить/запустить/перезапустить выбранную службу;
- **«Системная информация»** – отображает основную информацию о системе;

- **«Журнал Syslog»** – отображает таблицу журнала Syslog в режиме реального времени;
- **«Тепловые датчики»** – отображает по данным ACPI температуру ЦП, МП, позволяет задавать различные пороговые значения температуры;
- **«Графики трафика»** – отображает график входящего/исходящего трафика в режиме реального времени.

32.2 Сбор и статистика Netflow

NetFlow – сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems. Протокол захватывает полные потоки пакетов, включая источник, IP-адрес назначения и номер порта.

ARMA FW позволяет собирать данные NetFlow, проходящие через МЭ для последующего анализа, а также экспортировать эти данные для анализа сторонним ПО.

32.2.1 Настройка NetFlow

Для настройки NetFlow необходимо выполнить следующие действия:

1. Перейти в подраздел настройки NetFlow (**«Создание отчетов» - «NetFlow»**) (см. Рисунок – Параметры работы NetFlow).

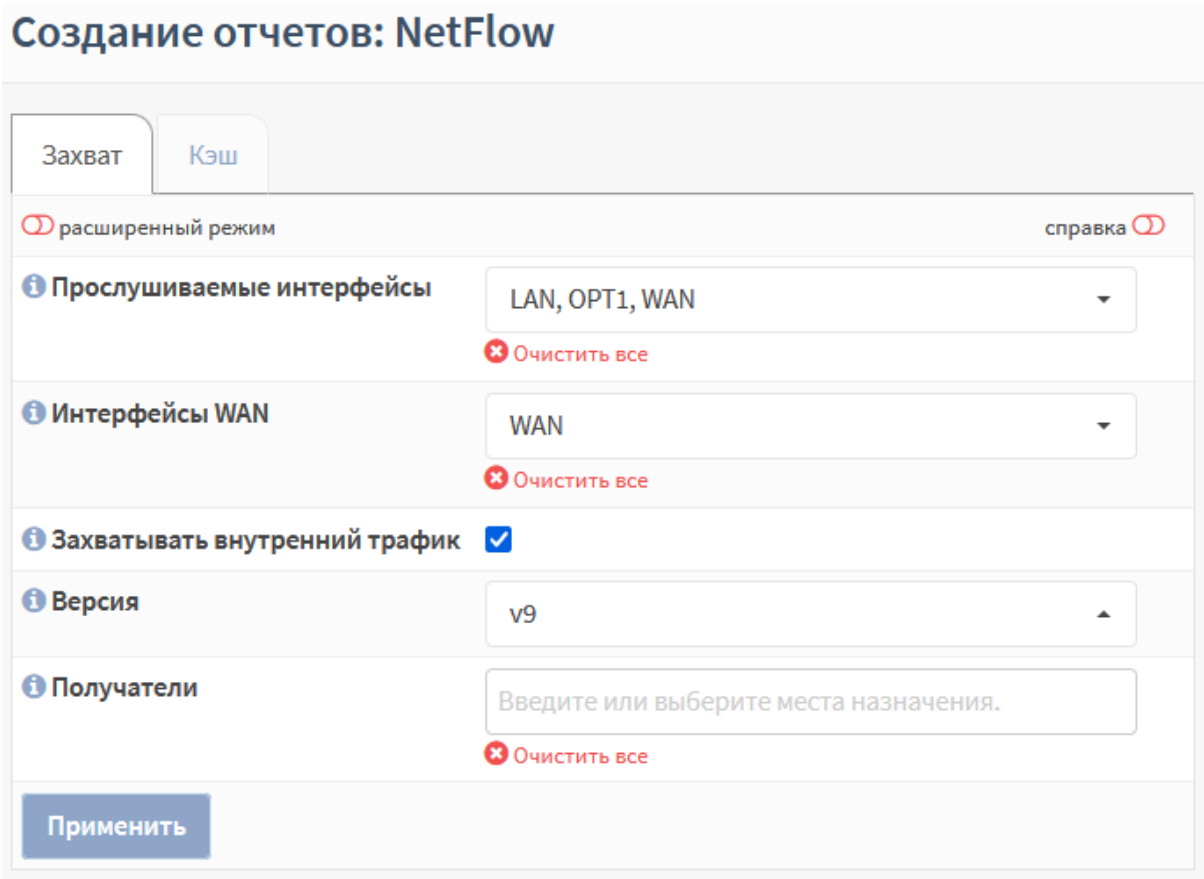


Рисунок – Параметры работы NetFlow

2. Указать интерфейсы, для которых необходимо собирать данные NetFlow.
3. Указать интерфейс, используемый в качестве выхода в глобальную сеть – WAN.
4. Установить флажок для параметра **«Захватывать внутренний трафик»** для сбора локальных данных на **ARMA FW**. Локальный кэш хранит только последние 100 Мбайт данных.
5. При необходимости выбрать версию NetFlow, по умолчанию выбрано значение «v9».
6. В параметре **«Получатели»** указать адреса получателей данных, если поле оставить пустым – будет осуществляться только локальный сбор данных.

   Формат заполнения:

   - «IP-адрес:номер порта», например «192.168.1.100:2550».
7. Нажать **кнопку «Применить»**.

   Примечание:

   При использовании стороннего сборщика данных NetFlow, в большинстве случаев, необходимо настроить передачу SNMP (см. SNMP) и создать правило МЭ (см. Создание правил межсетевого экранирования), разрешающее трафик SNMP на выбранном интерфейсе.

В случае сбора локальных данных на вкладке **«Кэш»** подраздела **«NetFlow»** будет отображено количество собранных пакетов на различных интерфейсах (см. Рисунок – Данные кэша NetFlow).

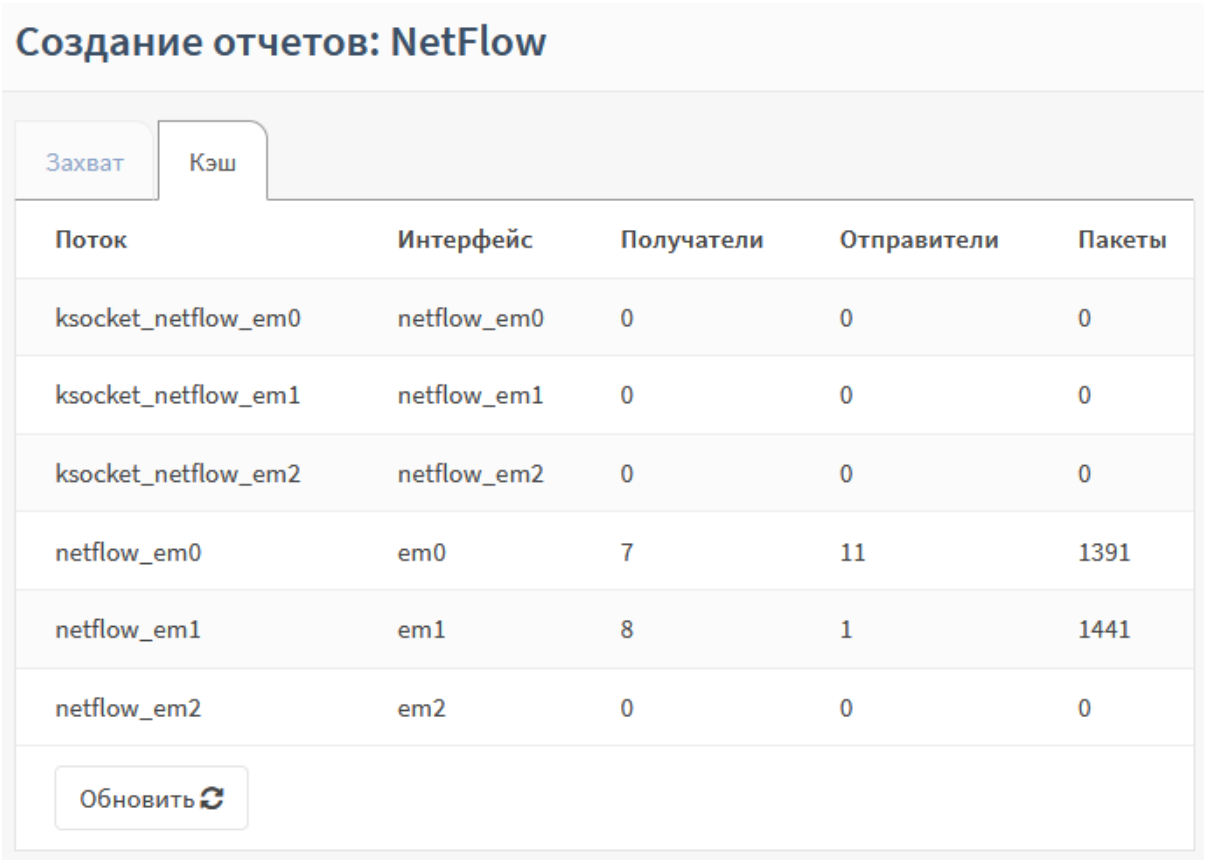


Рисунок – Данные кэша NetFlow

При настройке NetFlow доступны дополнительные параметры при включении переключателя **«расширенный режим»** в левой части формы:

- **«Тайм-аут активности»** – дробление длительных потоков на короткие;
- **«Тайм-аут неактивности»** – разрыв неактивных потоков;
- **«Время ротации flowd.log»** – время ротации создаваемого файла с данными, диапазон доступных значений от 10 до 120 секунд.

32.2.2 Анализ данных Netflow

В случае успешной настройки NetFlow (см. Настройка NetFlow) в подразделе анализа трафика (**«Создание отчетов» - «Анализ»**) будет отображена информация о трафике (см. Рисунок – Сводная информация на основании данных NetFlow).

В верхней части страницы существует возможность выбора временного промежутка представления из выпадающего списка.

При выборе значения на диаграмме будет произведён переход на вкладку **«Подробности»** для более детального представления данных.

На вкладке **«Экспорт»** подраздела **«Анализ»** возможно произвести экспорт данных NetFlow. Для этого необходимо выбрать требуемые значения в выпадающих списках и нажать **кнопку «Экспорт»**.

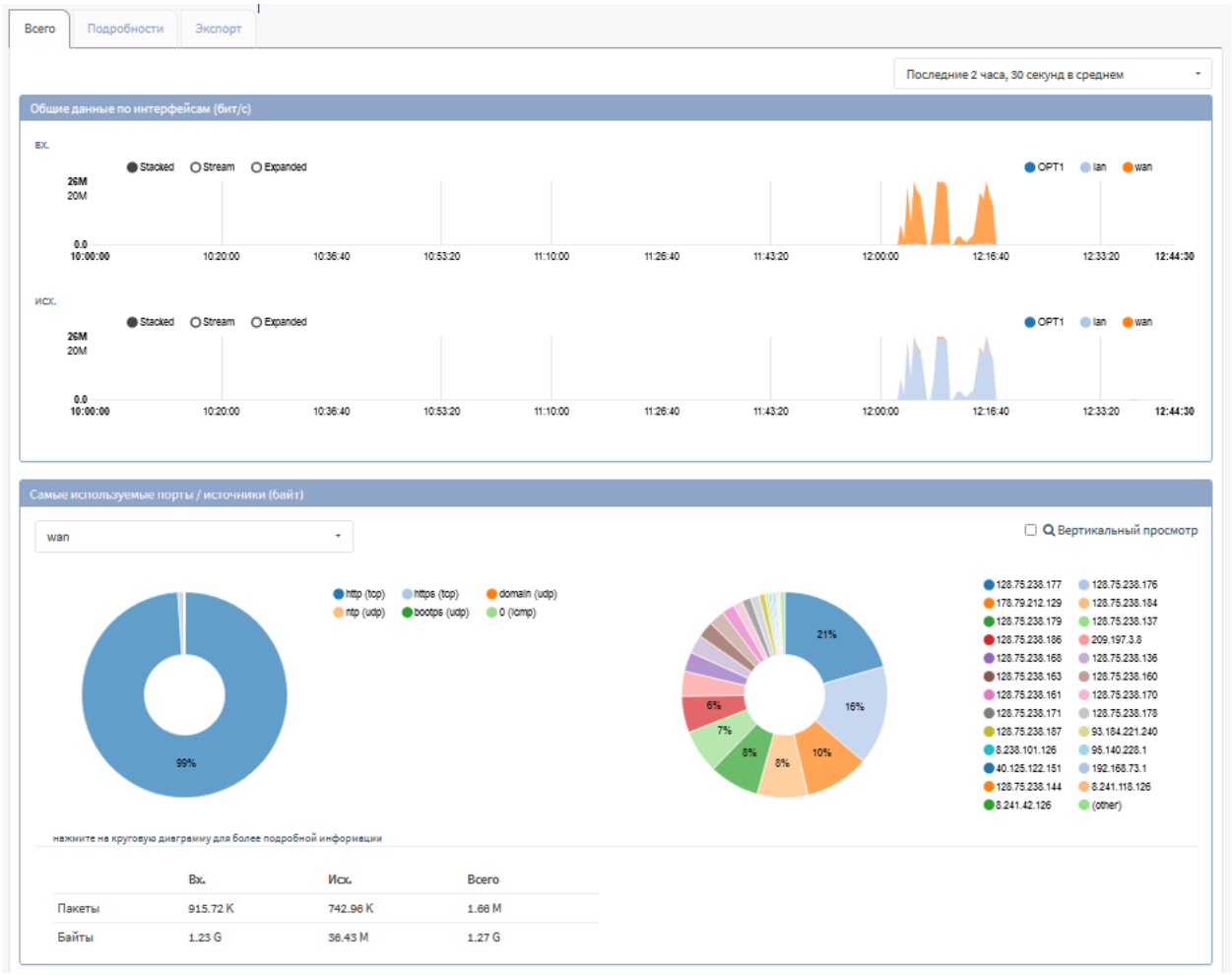


Рисунок – Сводная информация на основании данных NetFlow

32.3 Диагностика МЭ

Диагностика МЭ позволяет просматривать общую информацию и статистику МЭ, активные в текущее время маршруты, IP-адреса, записанные как псевдонимы, прослушивающие сокеты для IPv4 и IPv6, активные состояния, отсортированные состояния по различным критериям. Помимо просмотра информации имеется возможность удаления активных состояний и отслеживания источника.

32.3.1 Диагностика pfInfo

Для просмотра общей информации об МЭ необходимо перейти в подраздел диагностики pfInfo (**«Межсетевой экран» - «Диагностика» - «pfInfo»**) (см. Рисунок – Диагностика pfinfo).

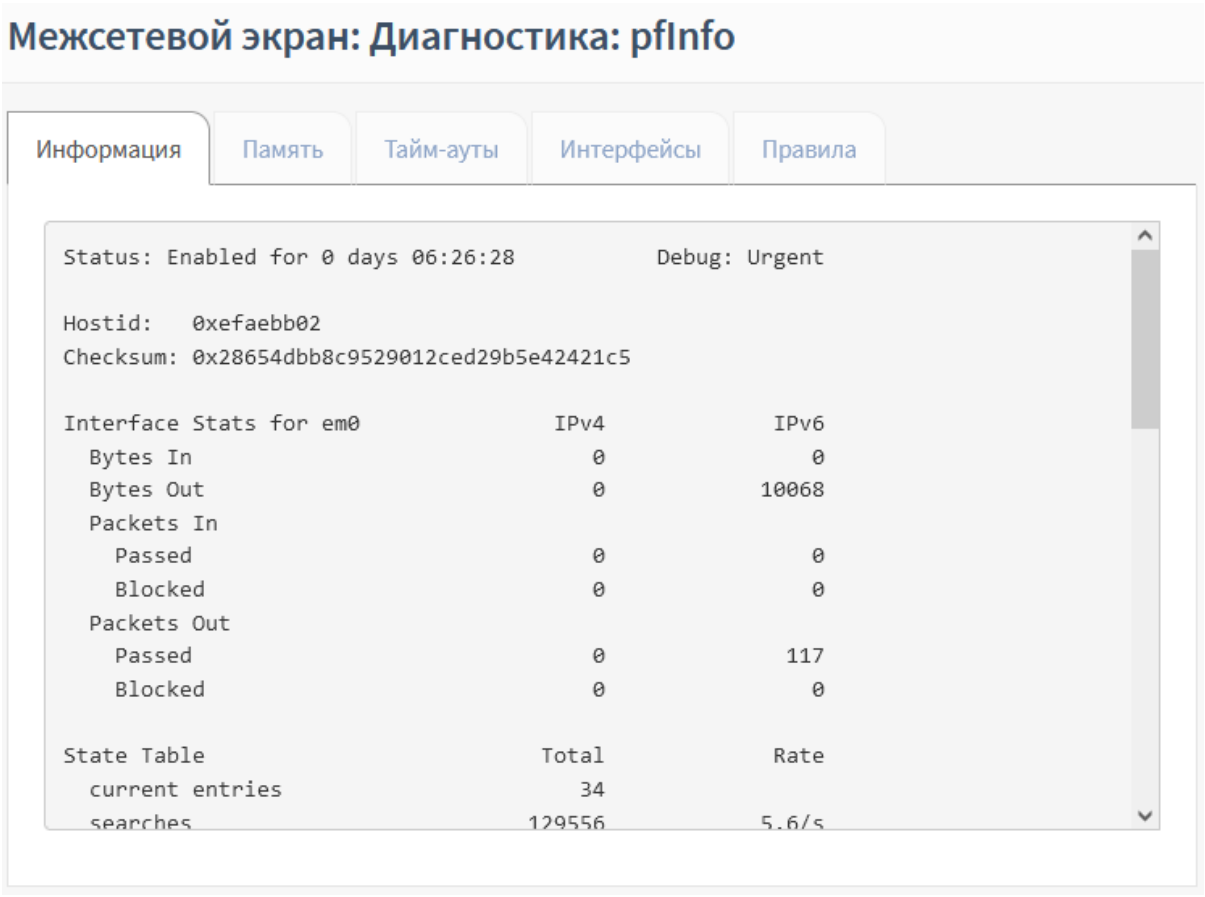


Рисунок – Диагностика pfinfo

Существует возможность переключения по вкладкам:

- **«Информация»** – отображает различную общую информацию о работе МЭ;
- **«Память»** – отображает заданные ограничения памяти;
- **«Тайм-ауты»** – отображает информацию о тайм-аутах;
- **«Интерфейсы»** – отображает информацию об интерфейсах;
- **«Правила»** – отображает информацию о правилах МЭ.

32.3.2 Диагностика pfTop

Для просмотра доступных маршрутов в текущее время необходимо перейти в подраздел диагностики pfTop (**«Межсетевой экран» - «Диагностика» - «pfTop»**) (см. Рисунок – Диагностика pfTop).

Существует возможность изменить вид, настроить сортировку или указать количество строк в соответствующих выпадающих списках.

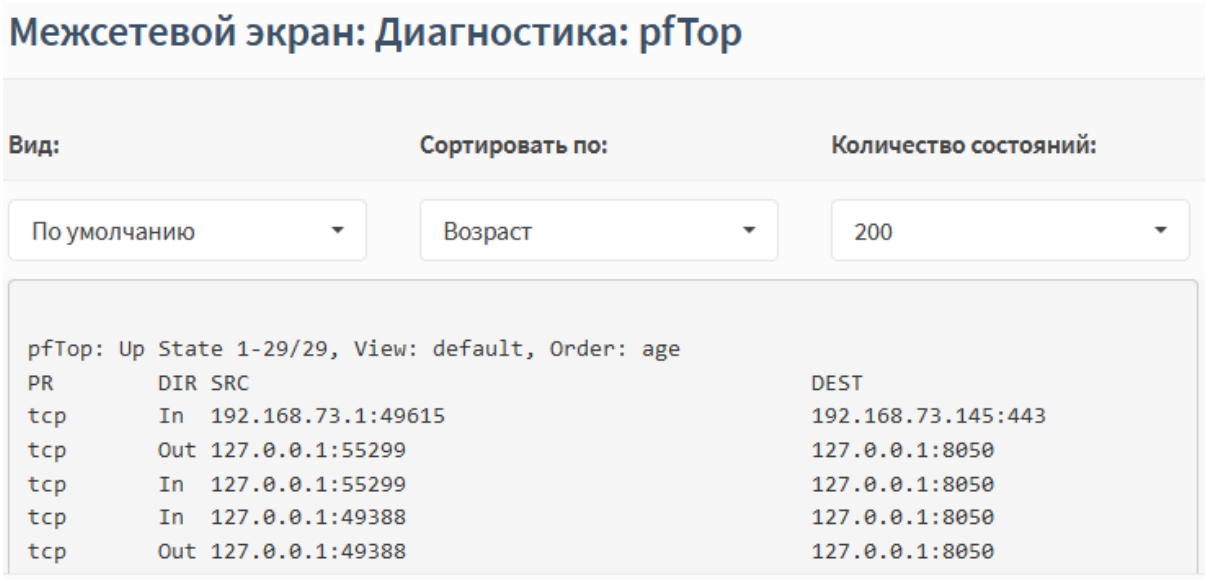


Рисунок – Диагностика pfTop

32.3.3 Диагностика pfTables

Для просмотра IP-адресов, указанных в псевдонимах необходимо перейти в подраздел диагностики pfTables (**«Межсетевой экран» - «Диагностика» - «pfTables»**) (см. Рисунок – Диагностика pfTables).

Выпадающие списки позволяют выбрать псевдоним, очистить и обновить базу псевдонима, нажав соответствующие кнопки.

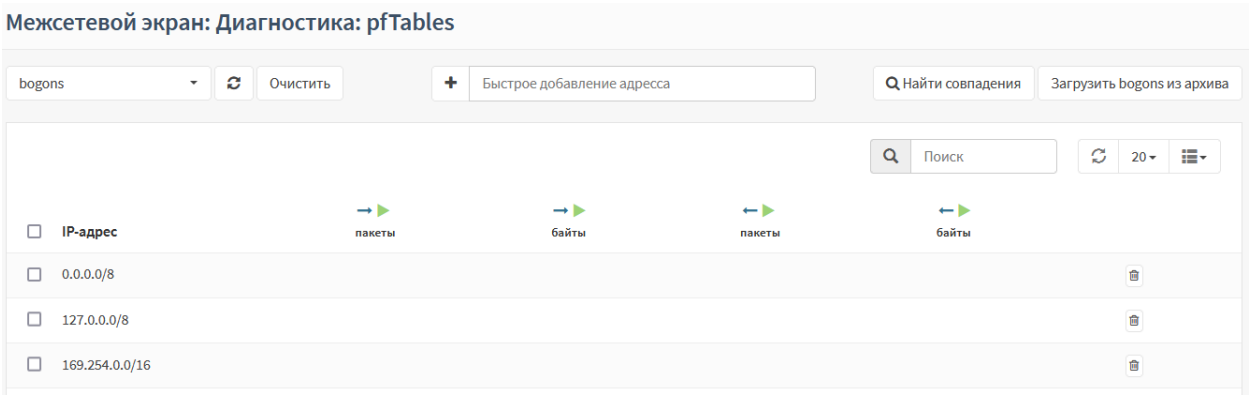


Рисунок – Диагностика pfTables

32.4 Диагностика системы

32.4.1 Действия пользователей

Для просмотра действий пользователей, в том числе системных пользователей, необходимо перейти в подраздел отслеживания активности пользователей (**«Система» - «Диагностика» - «Активность»**) (см. Рисунок – Активность).

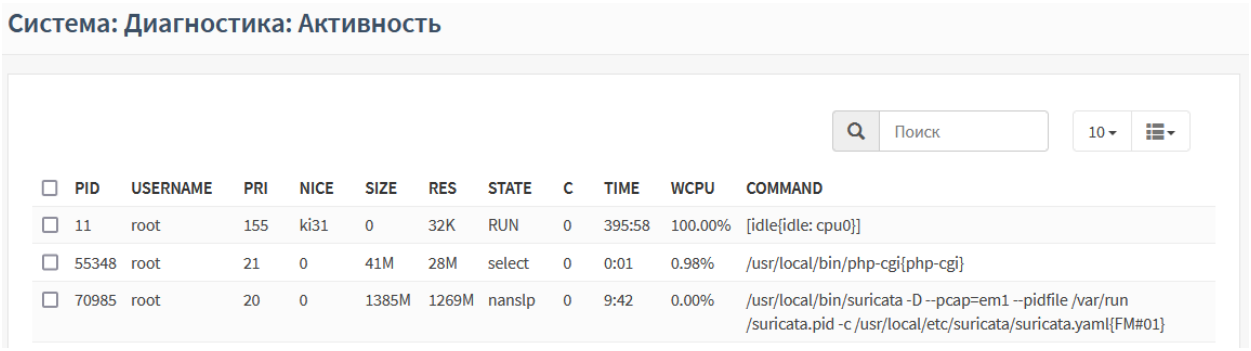


Рисунок – Активность

32.4.2 Службы

Для просмотра и управления настроенными службами необходимо перейти в подраздел управления службами (**«Система» - «Диагностика» - «Службы»**) (см. Рисунок – Службы).

Для служб возможны следующие действия при нажатии соответствующей кнопки:

- **кнопка** « ■ » – остановить службу;
- **кнопка** « ▶ » – запустить службу;
- **кнопка** « ↻ » – перезапустить службу.

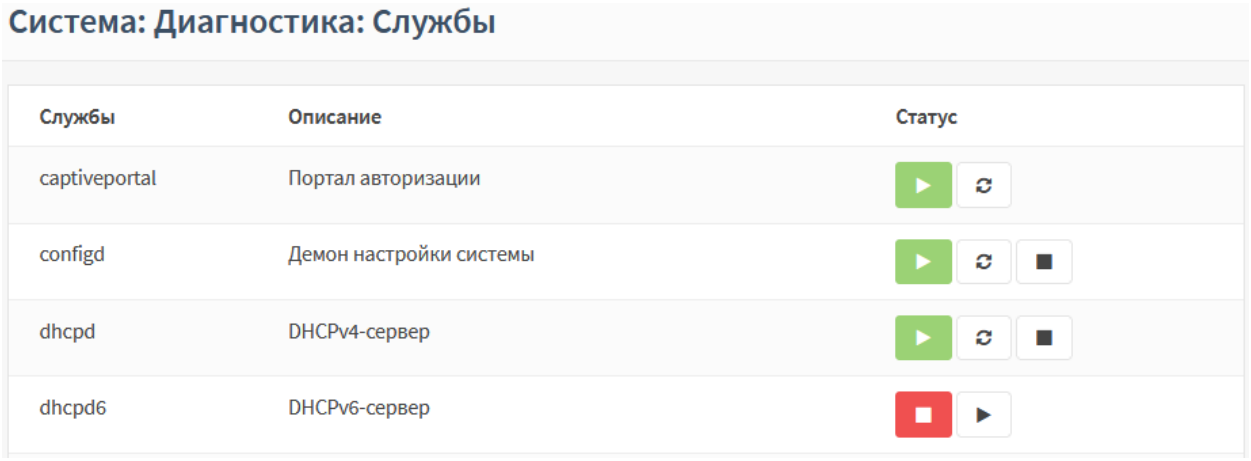


Рисунок – Службы

32.5 Диагностика сетевых интерфейсов

Диагностика сетевых интерфейсов позволяет выполнять следующие действия:

- просматривать таблицу ARP;
- запускать сканирование ARP;
- просматривать таблицу DNS-записей;
- просматривать таблицу NDP-записей;
- экспортировать дамп трафика определённого сетевого интерфейса;

- выполнять и просматривать результаты команды «ping»;
- выполнять проверку порта на наличие подключения;
- выполнять маршрут трассировки.

32.5.1 ARP-таблица

Для просмотра ARP-таблицы необходимо перейти в подраздел просмотра ARP-таблицы (**«Интерфейсы» - «Диагностика» - «ARP-таблица»**) (см. Рисунок – ARP-таблица).

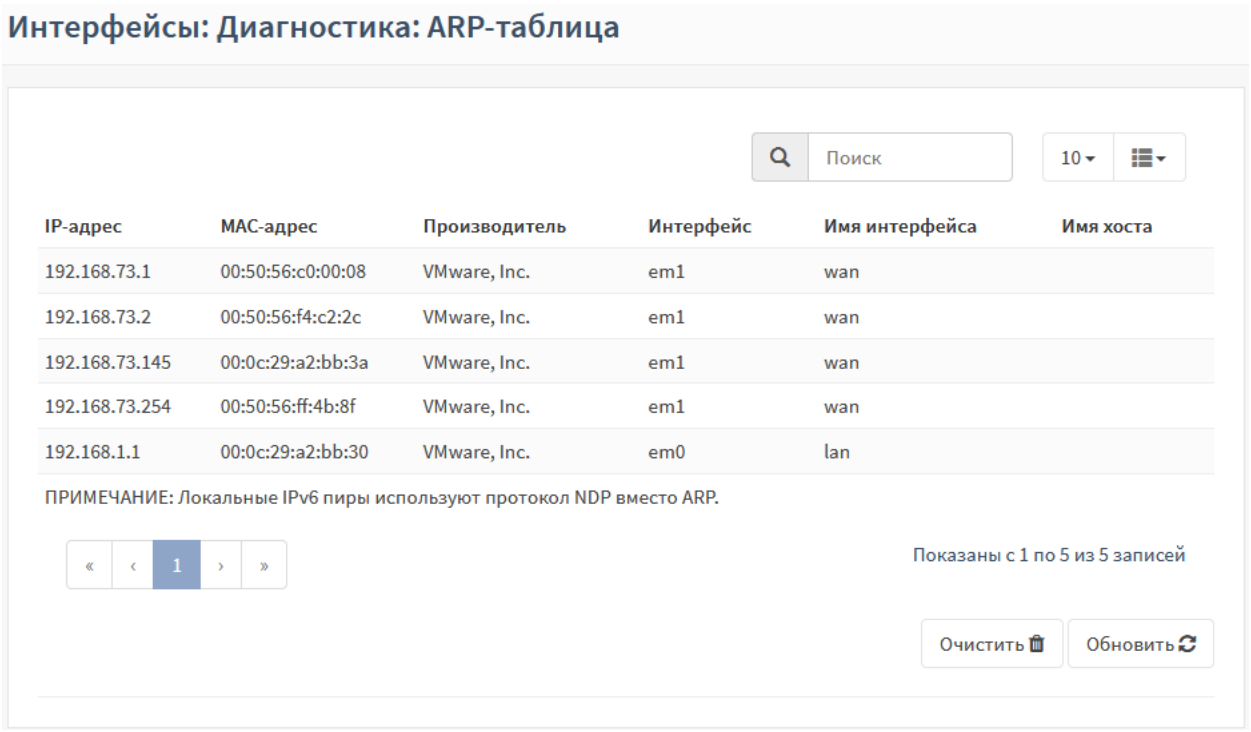


Рисунок – ARP-таблица

32.5.2 Просмотр DNS-записей

Для поиска IP-адресов и записей, принадлежащих заданному имени хоста необходимо перейти в подраздел просмотра DNS-записей (**«Интерфейсы» - «Диагностика» - «Просмотр DNS-записей»**) (см. Рисунок – Просмотр DNS-записей), указать в параметре **«Имя хоста или IP-адрес»** IP-адрес и нажать **кнопку «Просмотр DNS-записей»**.

Рисунок – Просмотр DNS-записей

32.5.3 Индикатор интерфейса

Для включения светового индикатора физического сетевого интерфейса необходимо перейти в подраздел управления индикаторами интерфейсов (**«Интерфейсы» - «Диагностика» - «Индикатор интерфейса»**) (см. Рисунок – Индикатор интерфейса).

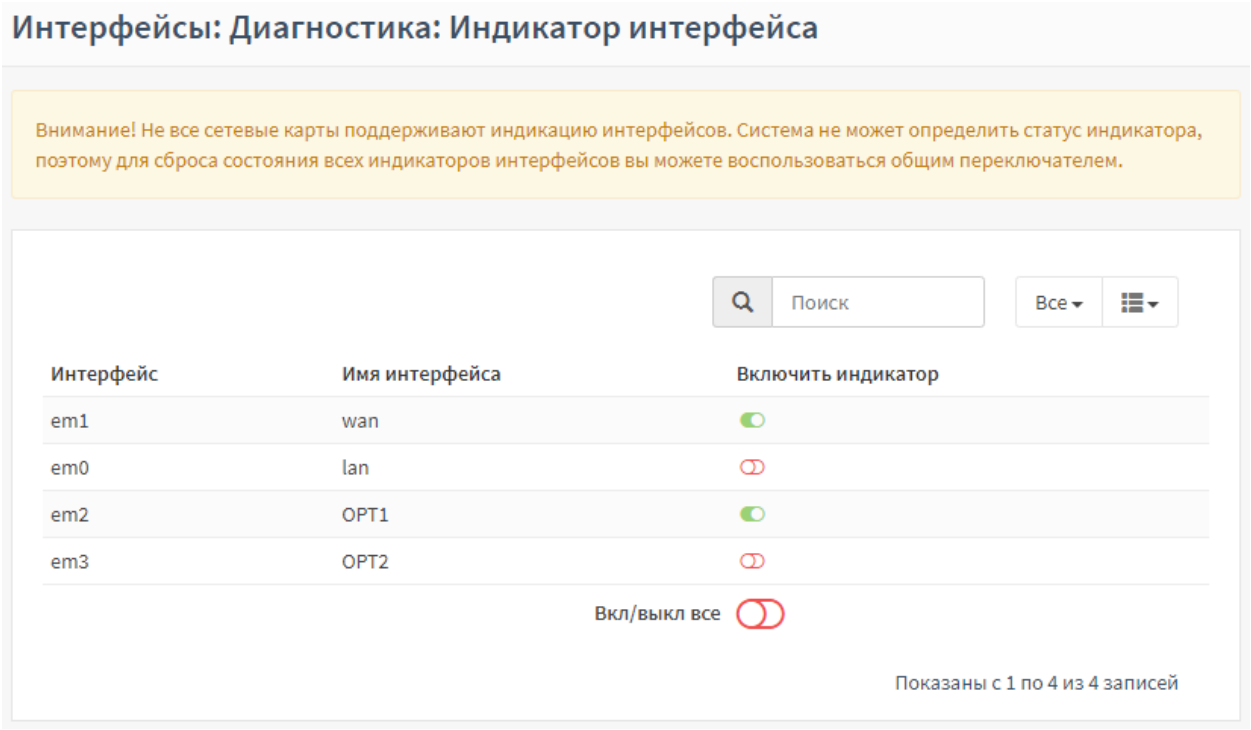


Рисунок – Индикатор интерфейса

Возможность принудительного включения световых индикаторов позволяет визуально определить местоположение физического сетевого интерфейса **ARMA FW**, соответствующего какому-либо сетевому интерфейсу, отображаемому в подразделе настройки интерфейсов.

Примечание:

Не все сетевые карты поддерживают возможность управления состоянием световых индикаторов.

Не все физические сетевые порты могут быть оснащены световыми индикаторами.

Поддерживается одновременное изменение состояния световых индикаторов всех сетевых интерфейсов с помощью **переключателя «Вкл/выкл все»**.

При нажатии на **переключатель «Вкл/выкл все»** следующего вида:

- «  » – будет выполнено включение всех индикаторов;
- «  » – будет выполнено отключение всех индикаторов.

32.5.4 NDP-таблица

Для просмотра NDP-таблицы, в которой перечислены локально подключённые узлы IPv6 необходимо перейти в подраздел просмотра NDP-таблицы (**«Интерфейсы» - «Диагностика» - «NDP-таблица»**) (см. Рисунок – NDP-таблица).

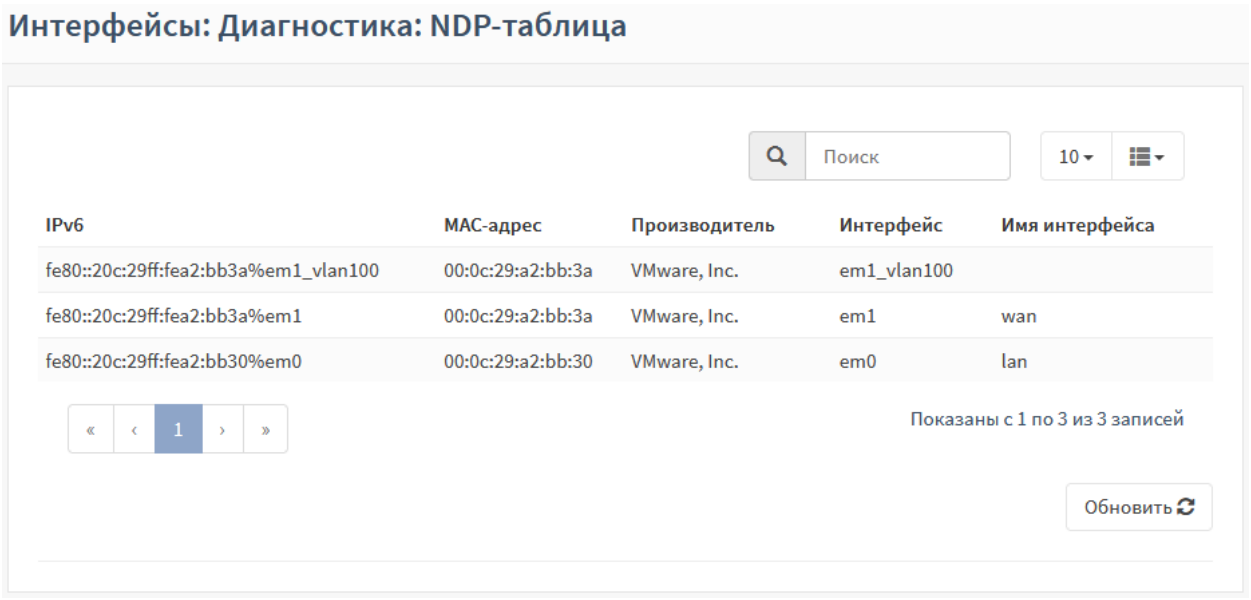


Рисунок – NDP-таблица

32.5.5 Netstat

Для просмотра статистики работы с сетевыми интерфейсами необходимо перейти в подраздел диагностики Netstat (**«Интерфейсы» - «Диагностика» - «Netstat»**) (см. Рисунок – Статистика работы Netstat).

Статистика работы с сетевыми интерфейсами отображается в группированном виде во вкладках:

- **«Bpf»** – bpf-статистика;

- **«Интерфейсы»** – статистика по интерфейсам;
- **«Память»** – mbuf-статистика;
- **«Netisr»** – netisr-статистика;
- **«Протокол»** – статистика по протоколам;
- **«Сокеты»** –статистика по сокетам.

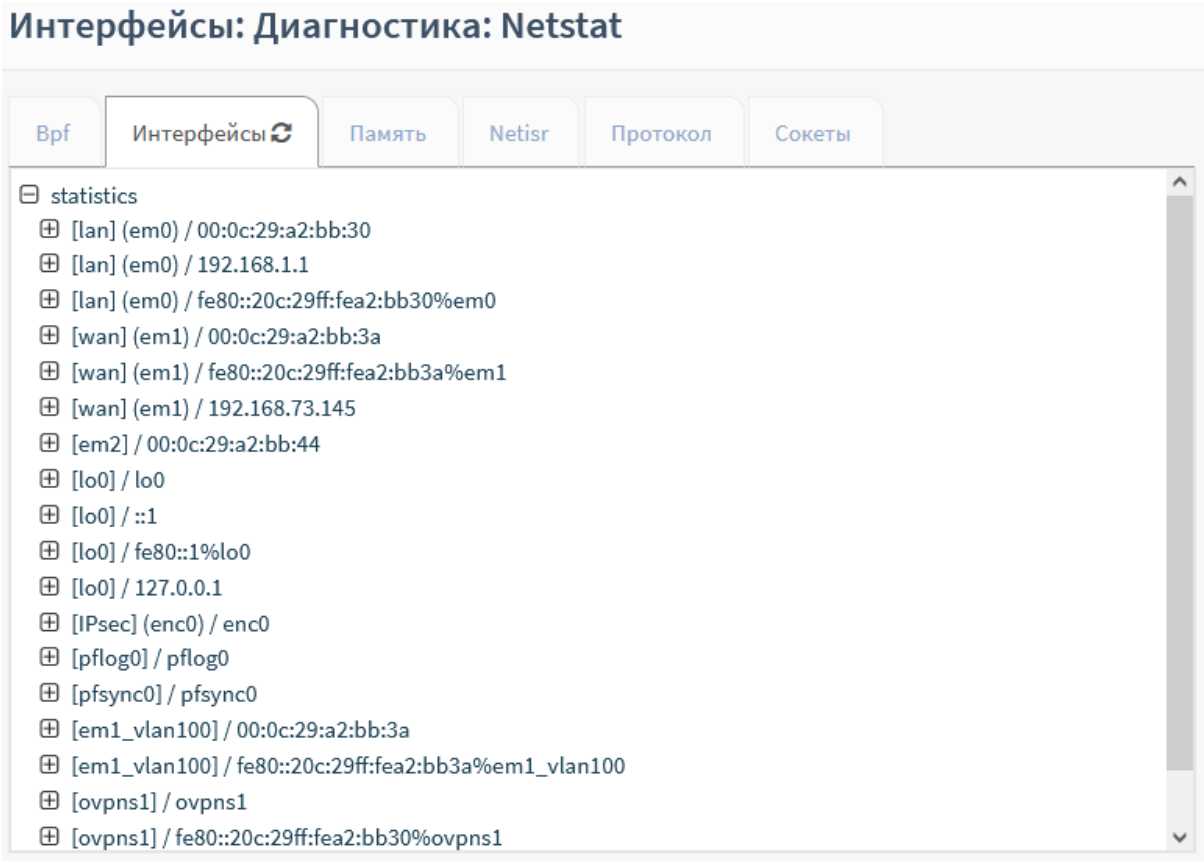


Рисунок – Статистика работы Netstat

32.5.6 Захват пакетов

Функция захвата пакетов предоставляет возможность записи дампов трафика с последующим экспортом в файл с расширением **«cap»**, например, для проведения расследования инцидентов ИБ.

В качестве примера будет рассмотрен захват HTTP-трафика с ПК **«Admin»** до ПК **«Webserver»** по интерфейсу «LAN» (см. Рисунок – Схема стенда для проверки функции захвата пакетов).

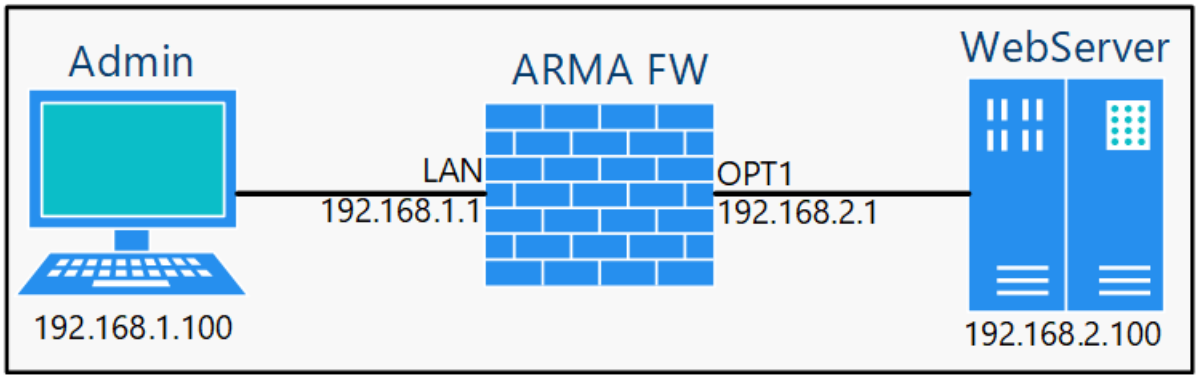


Рисунок – Схема стенда для проверки функции захвата пакетов

Для запуска механизма сбора дампов необходимо выполнить следующие действия:

1. Перейти в подраздел диагностики захватом пакетов (**«Интерфейсы» – «Диагностика» – «Захват пакетов»**) (см. Рисунок – Захват пакетов).

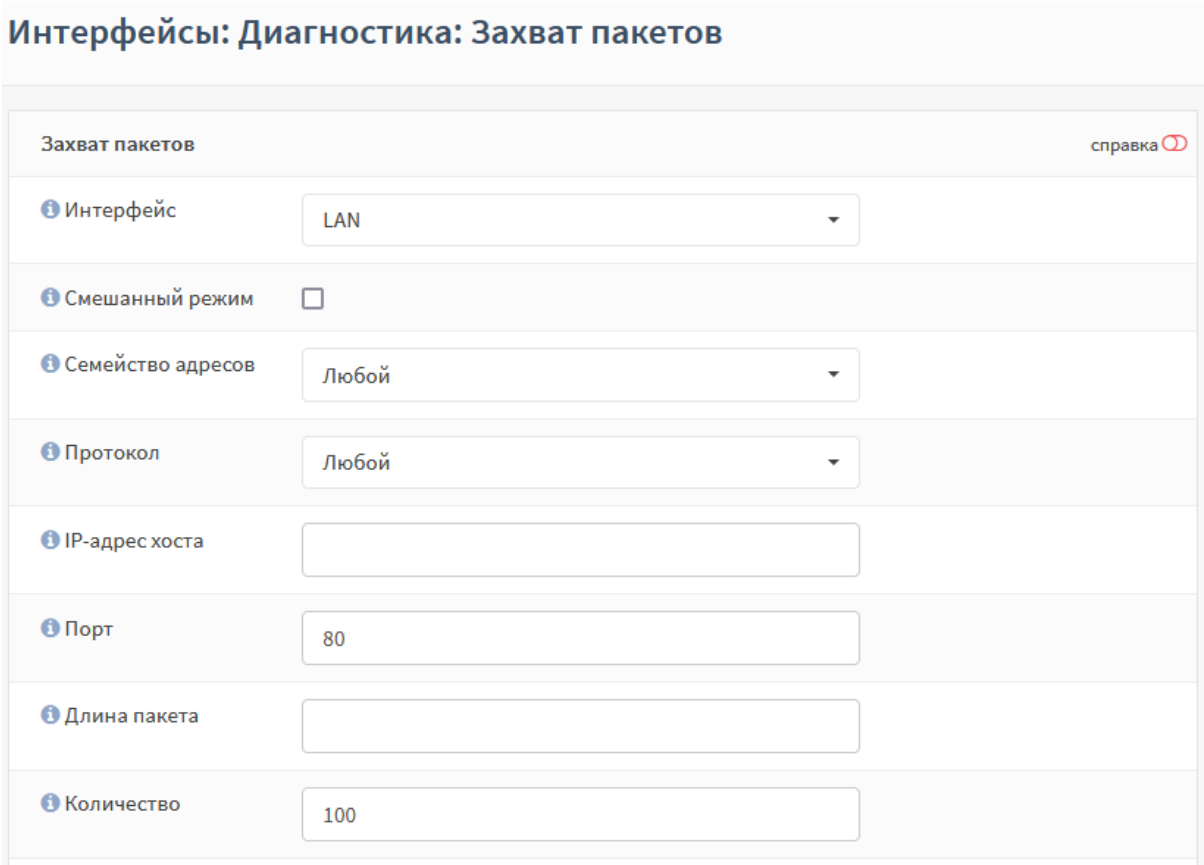


Рисунок – Захват пакетов

2. Указать следующие значения параметров:
   - **«Интерфейс»** – «LAN»;
   - **«Порт»** – «80»;

   остальные параметры отставить без изменений и нажать **кнопку «Запустить»**.
3. На ПК **«Admin»** открыть веб-браузер и перейти по адресу «192.168.2.100».

4. В подразделе **«Захват пакетов»** нажать **кнопку «Остановить»**. Дамп трафика будет отображён в нижней части страницы подраздела (см. Рисунок – Дамп трафика).

Для просмотра захваченных пакетов в веб-интерфейсе **ARMA FW** необходимо нажать **кнопку «Просмотр захваченных пакетов»**. Уровень детализации просматриваемых пакетов выбирается в выпадающем списке **«Уровень детализации»**.

Для сохранения дампа захваченных пакетов на локальный ПК необходимо нажать на гиперссылку **«packetcapture_emX.cap»**, где **«X»** – это номер физического интерфейса, и выполнить сохранение с помощью интерфейса веб-браузера.

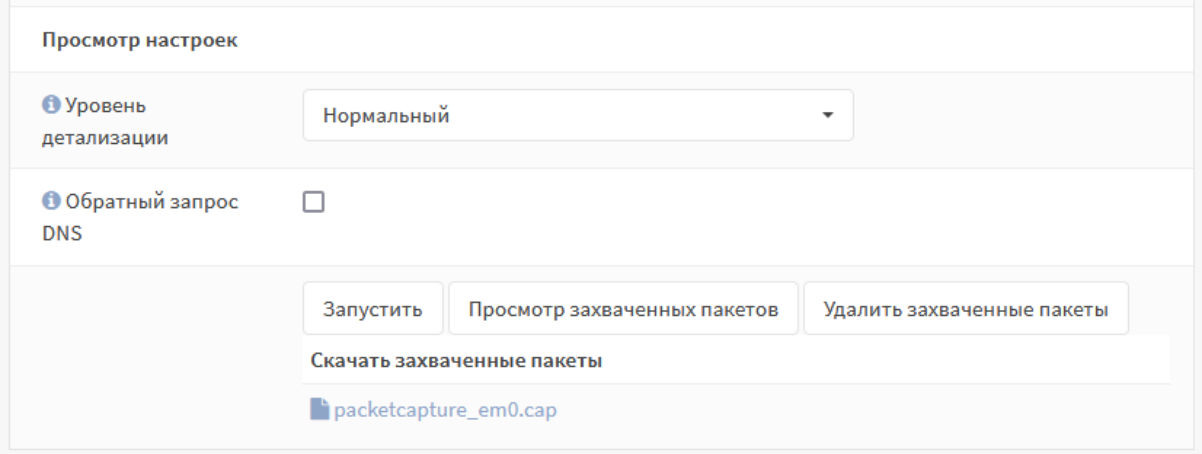


Рисунок – Дамп трафика

Краткое описание параметров при захвате пакетов:

- **«Смешанный режим»** – установка флажка позволяет принимать все пакеты трафика, независимо от адресата;
- **«Семейство адресов»** – позволяет оставлять только трафик IPv4 или IPv6;
- **«IP-адрес хоста»** – указывает IP-адрес/сеть получателя или источника, также существует возможность указания исключения или множество значений, используя логическое выражение с аргументами **«not»** и **«and»**;
- **«Порт»** – указывается порт получателя или источника;
- **«Длина пакета»** – указывается значение количества бит каждого захваченного пакета;
- **«Количество»** – указывается значение количества захватываемых пакетов;
- **«Обратный запрос DNS»** – установка флажка позволяет захватывать пакеты трафика, ассоциируемые со всеми IP-адресами обратного запроса DNS:

для этого в группе настроек **«Захват пакетов»** в поле **«Интерфейсы»** необходимо выбрать интерфейсы для захвата трафика. В поле **«Смешанный режим»** необходимо установить флажок для того, чтобы принимать все пакеты, независимо от того, кому они адресованы. В поле **«Семейство адресов»** необходимо выбрать тип трафика для захвата. В поле **«Протокол»** необходимо выбрать протокол для захвата трафика. В поле **«IP-адрес хоста»** необходимо ввести IP-адрес источника. В поле **«Порт»** необходимо ввести порт. В поле **«Длина пакета»** необходимо ввести длину пакета (в битах). В поле **«Количество»** необходимо ввести количество пакетов, которые будут захватываться.

32.5.7 Ping

Ping – утилита для проверки целостности и качества соединений в сетях TCP/IP.

Функция ping используется, например, для проверки наличия доступа к устройству сети. В качестве примера будет рассмотрена проверка наличия доступа к ПК **«Admin»** (см. Рисунок – Схема стенда для проверки функции захвата пакетов).

Для запуска утилиты ping необходимо выполнить следующие действия:

1. Перейти в подраздел диагностики ping (**«Интерфейсы» – «Диагностика» – «Ping»**) (см. Рисунок – Ping).
2. Указать IP-адрес «192.168.1.100» в параметре **«Хост»** и нажать **кнопку «Ping»**.

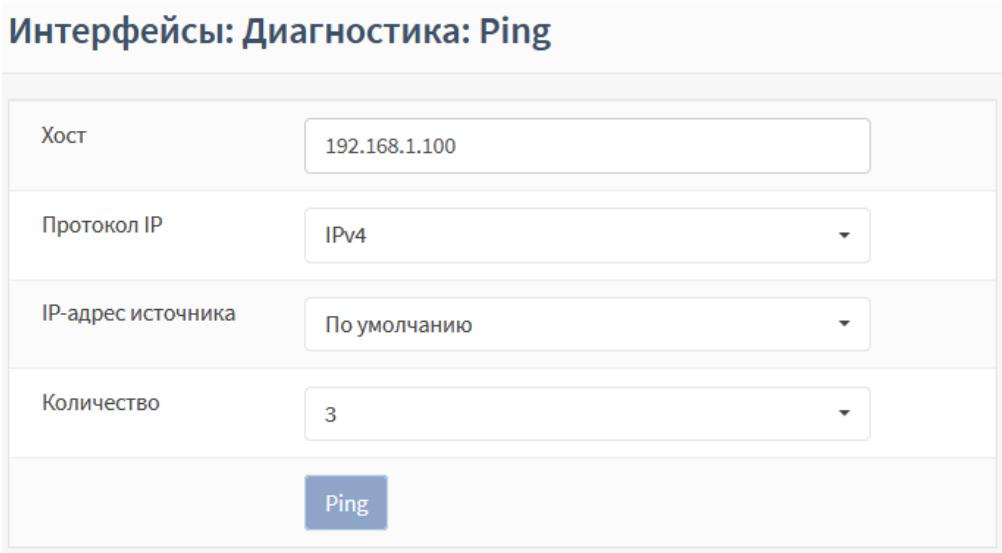


Рисунок – Ping

3. Результат команды отобразится в нижней части страницы (см. Рисунок – Результат выполнения команды Ping).

```
# /sbin/ping -c '3' '192.168.1.100'
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=128 time=0.380 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=0.441 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=128 time=0.383 ms

--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.380/0.401/0.441/0.028 ms
```

Рисунок – Результат выполнения команды Ping

32.5.8 Проверка порта

Функция проверки порта используется для выполнения простого теста TCP-соединения по указанному порту. В качестве примера будет рассмотрена проверка наличия доступа к ПК **«WebServer»** по порту «443» (см. Рисунок – Схема стенда для проверки функции захвата пакетов).

Для проверки соединения необходимо выполнить следующие действия:

1. Перейти в подраздел проверки порта (**«Интерфейсы» – «Диагностика» – «Проверка порта»**) (см. Рисунок – Проверка порта).

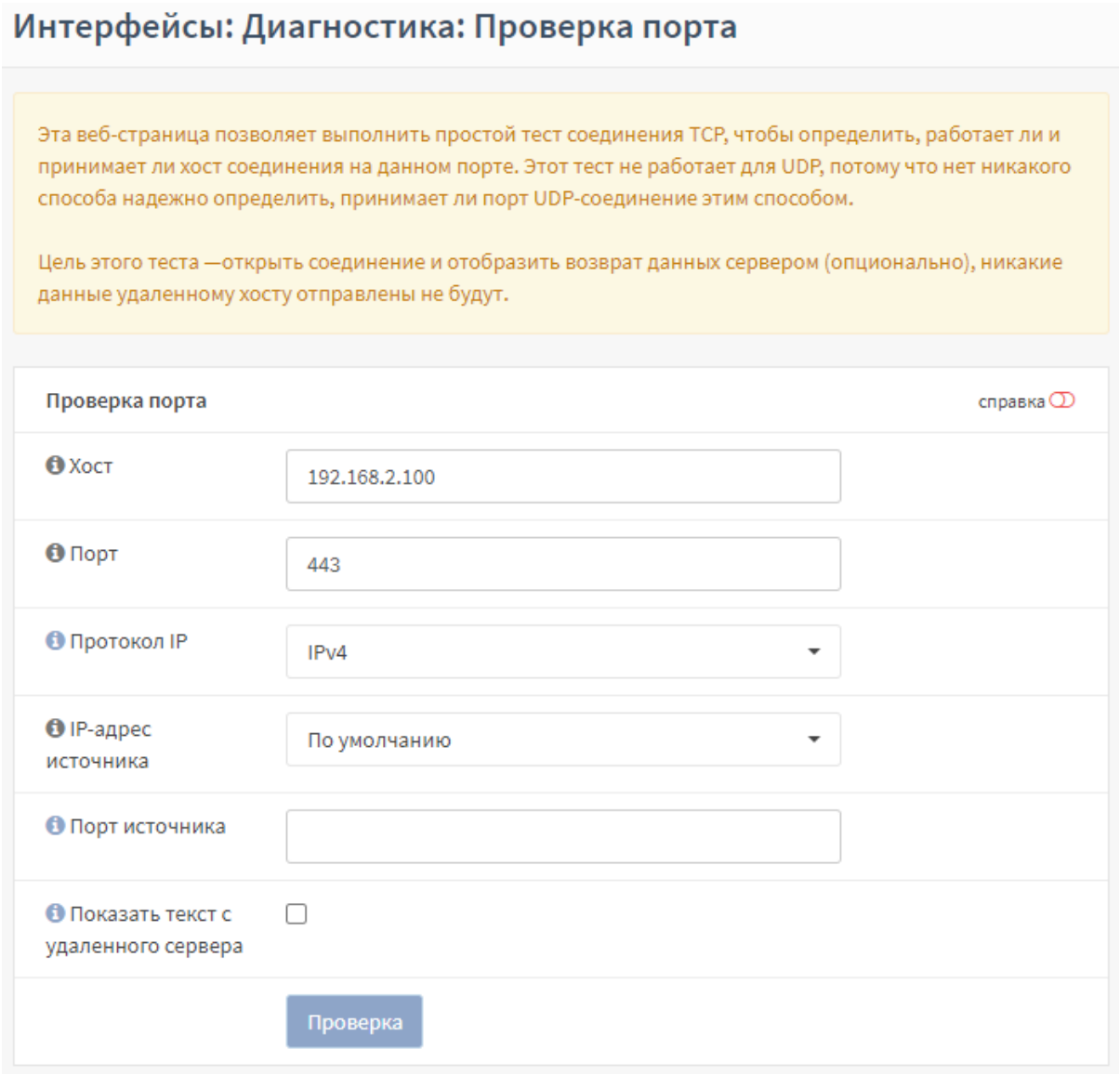


Рисунок – Проверка порта

2. Указать следующие значения параметров:
   - **«Хост»** – «192.168.2.100»;
   - **«Порт»** – «443»;

   остальные параметры отставить без изменений и нажать **кнопку «Проверка»**.
3. Результат команды отобразится в нижней части страницы (см. Рисунок – Результат выполнения команды проверка порта).

```
# /usr/bin/nc -w 10 -z  -4 '192.168.2.100' '443'
Connection to 192.168.2.100 443 port [tcp/https] succeeded!
```

Рисунок – Результат выполнения команды проверка порта

32.5.9 Маршрут трассировки

Трассировка маршрута предназначена для определения маршрутов следования данных в сетях TCP/IP. В качестве примера будет рассмотрено определение маршрута к ПК **«Admin»** (см. Рисунок – Схема стенда для проверки функции захвата пакетов).

Для выполнения трассировки маршрута необходимо выполнить следующие действия:

1. Перейти в подраздел трассировки маршрутов (**«Интерфейсы» – «Диагностика» – «Маршрут трассировки»**) (см. Рисунок – Маршрут трассировки).

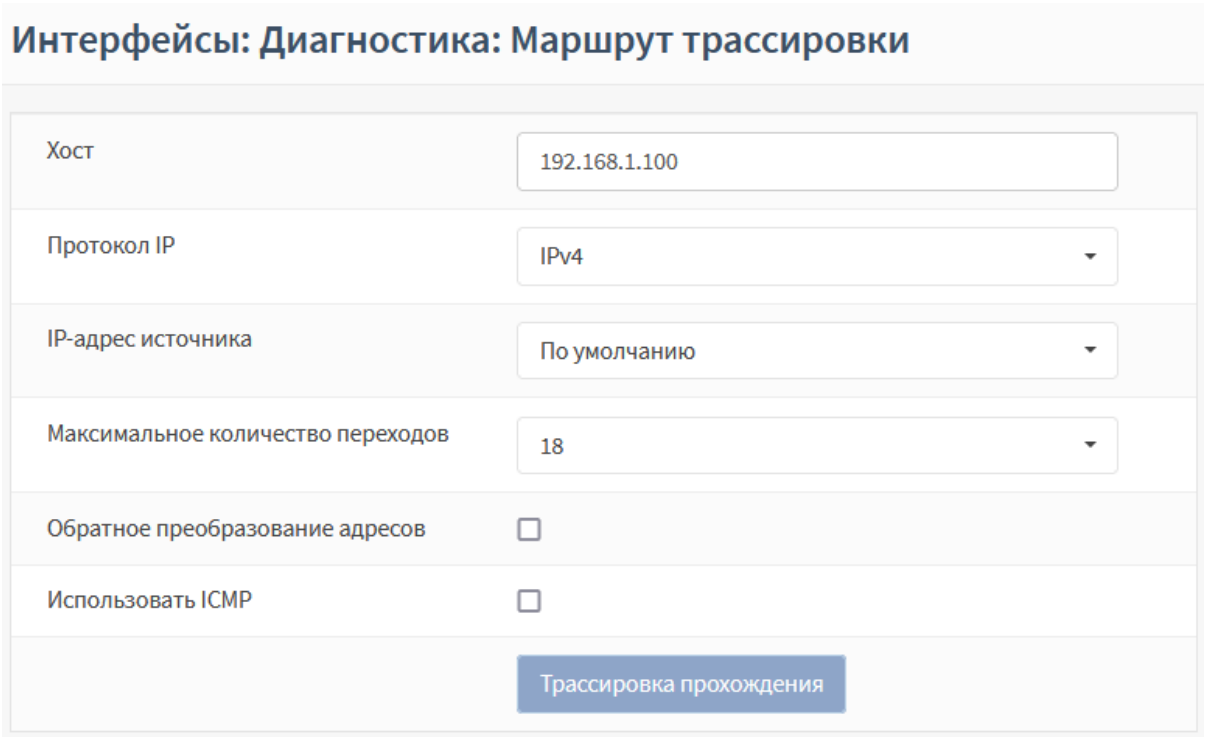


Рисунок – Маршрут трассировки

2. Указать «192.168.1.100» в параметре **«Хост»** и нажать **кнопку «Трассировка прохождения»**.
3. Результат команды отобразится в нижней части страницы (см. Рисунок – Результат выполнения команды трассировки).

```
# /usr/sbin/traceroute -w 2 -n  -m '18'  '192.168.1.100'
traceroute to 192.168.1.100 (192.168.1.100), 18 hops max, 40 byte packets
 1  192.168.1.100  0.719 ms  0.335 ms  0.428 ms
```

Рисунок – Результат выполнения команды трассировки

32.5.10 Обзор

В подразделе обзора журналов (**«Межсетевой экран» - «Журналы» - «Обзор»**) представлены диаграммы трафика, обработанного **ARMA FW**, которые перечислены в списке:

- **«Действия»** – Рисунок – Действия;
- **«Интерфейсы»** – Рисунок – Интерфейсы;
- **«Протоколы»** – Рисунок – Протоколы;
- **«IP-адреса источника»** – Рисунок – IP-адреса источника;
- **«IP-адреса назначения»** – Рисунок – IP-адреса назначения;
- **«Порты источника»** – Рисунок – Порты источника;
- **«Порты назначения»** – Рисунок – Порты назначения.

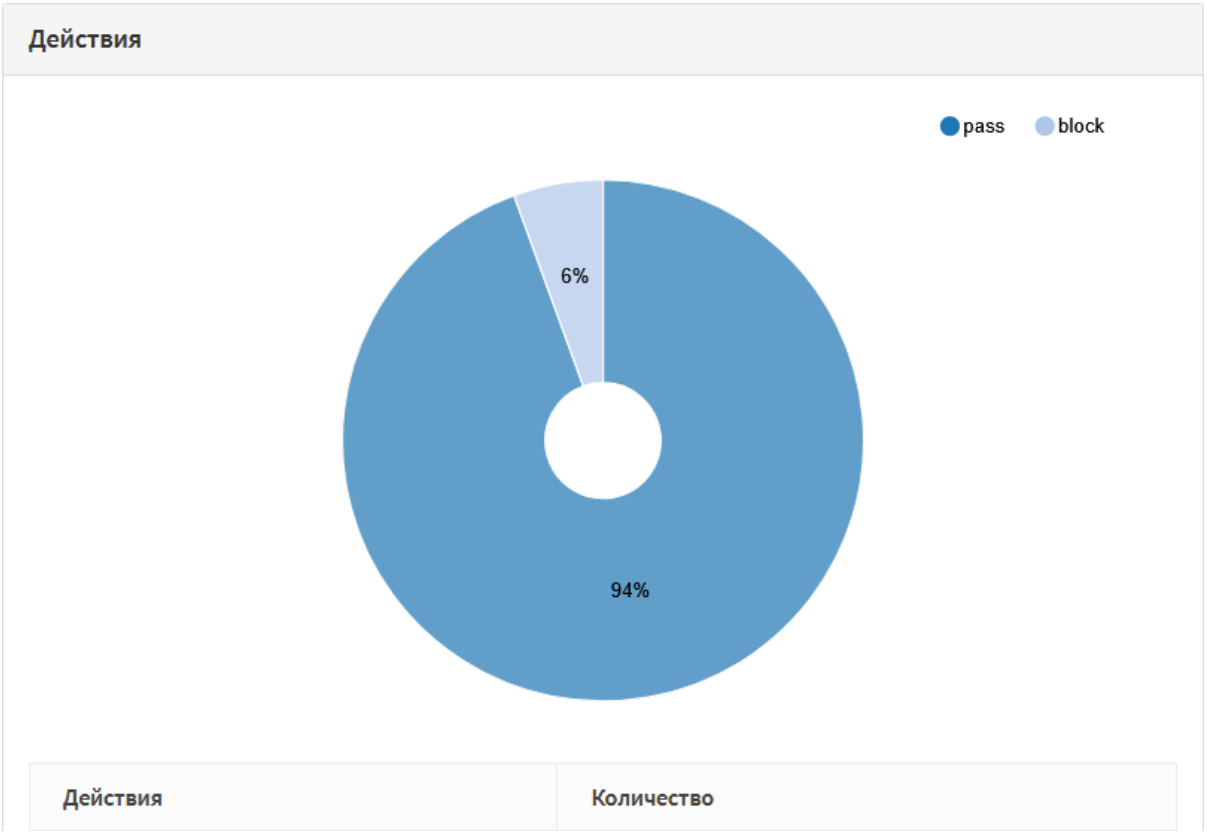


Рисунок – Действия

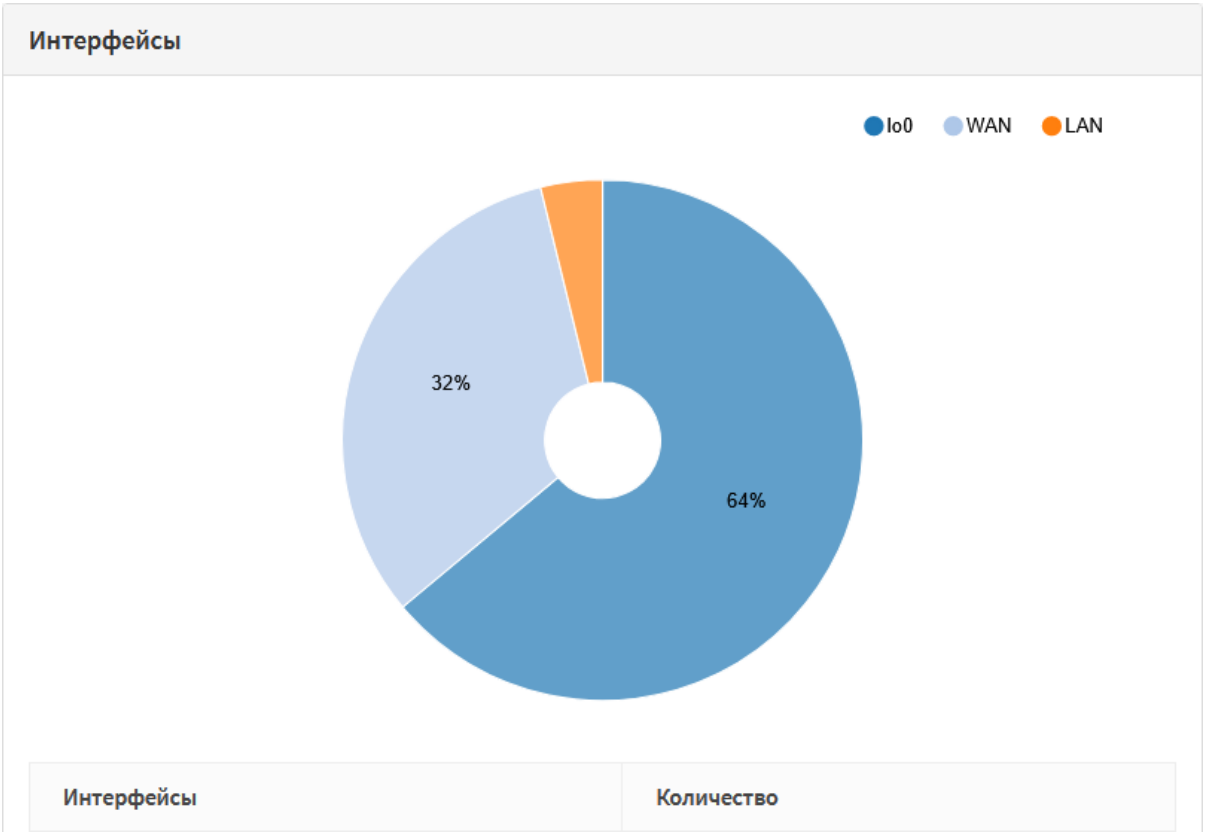


Рисунок – Интерфейсы

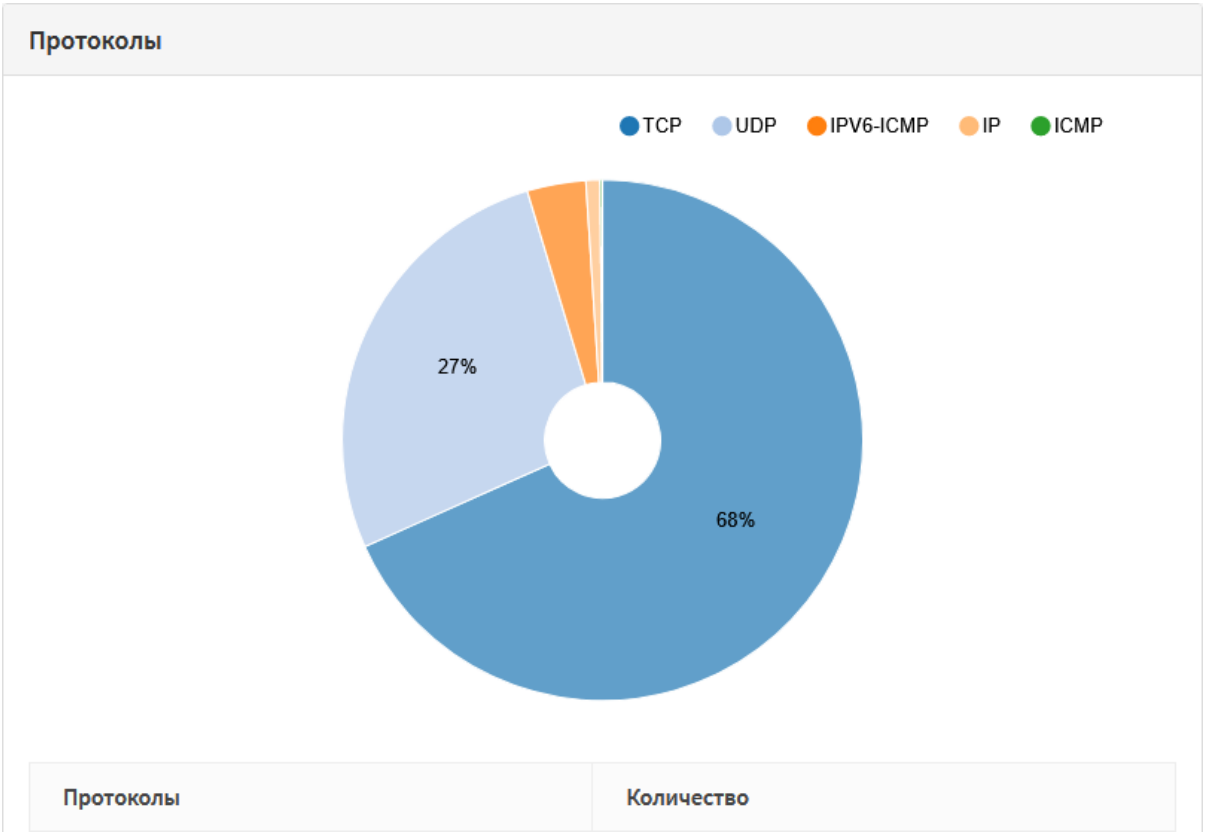


Рисунок – Протоколы

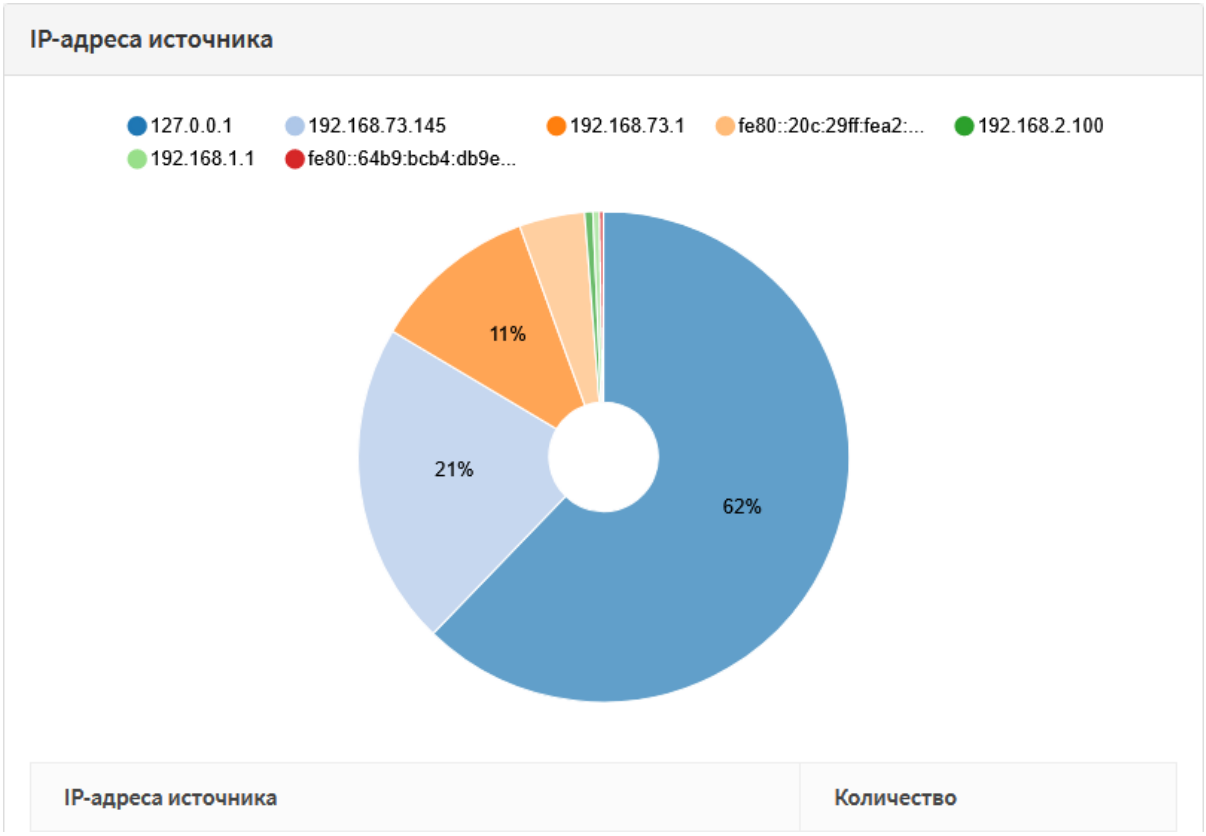


Рисунок – IP-адреса источника

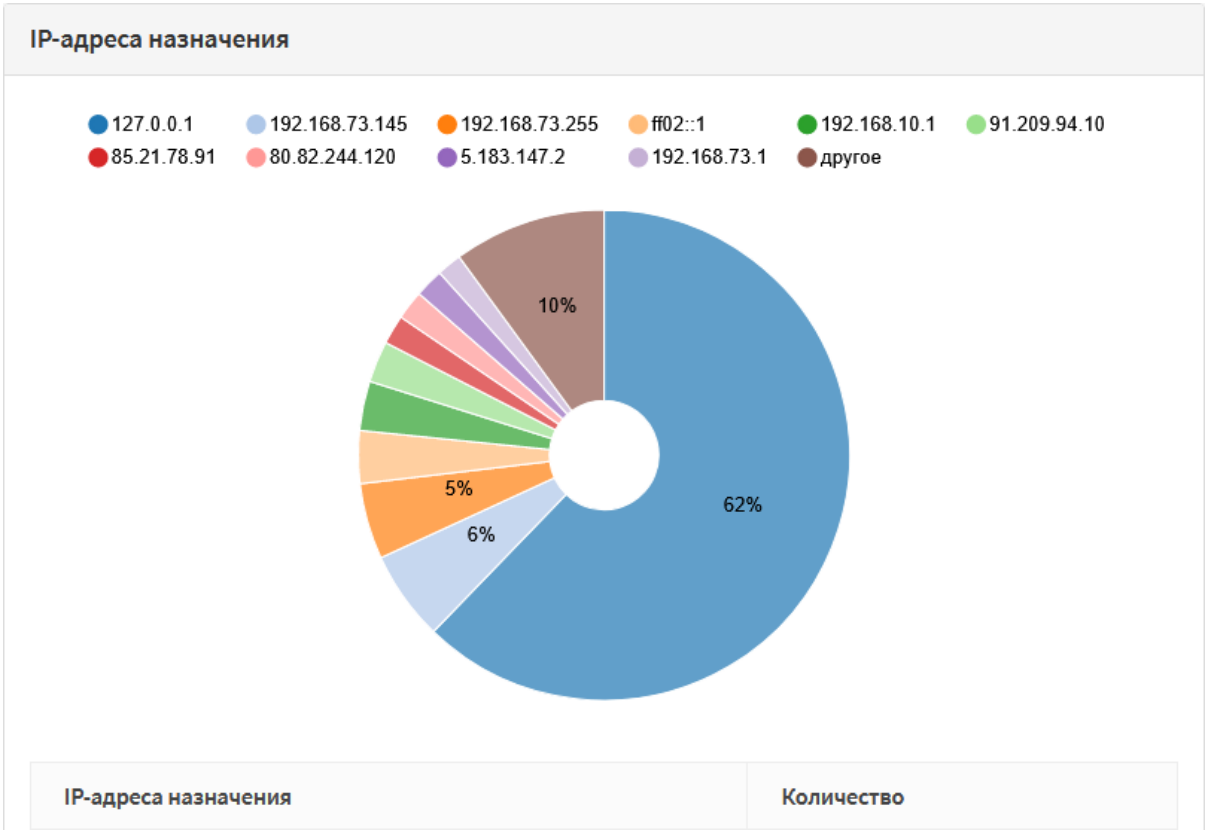


Рисунок – IP-адреса назначения

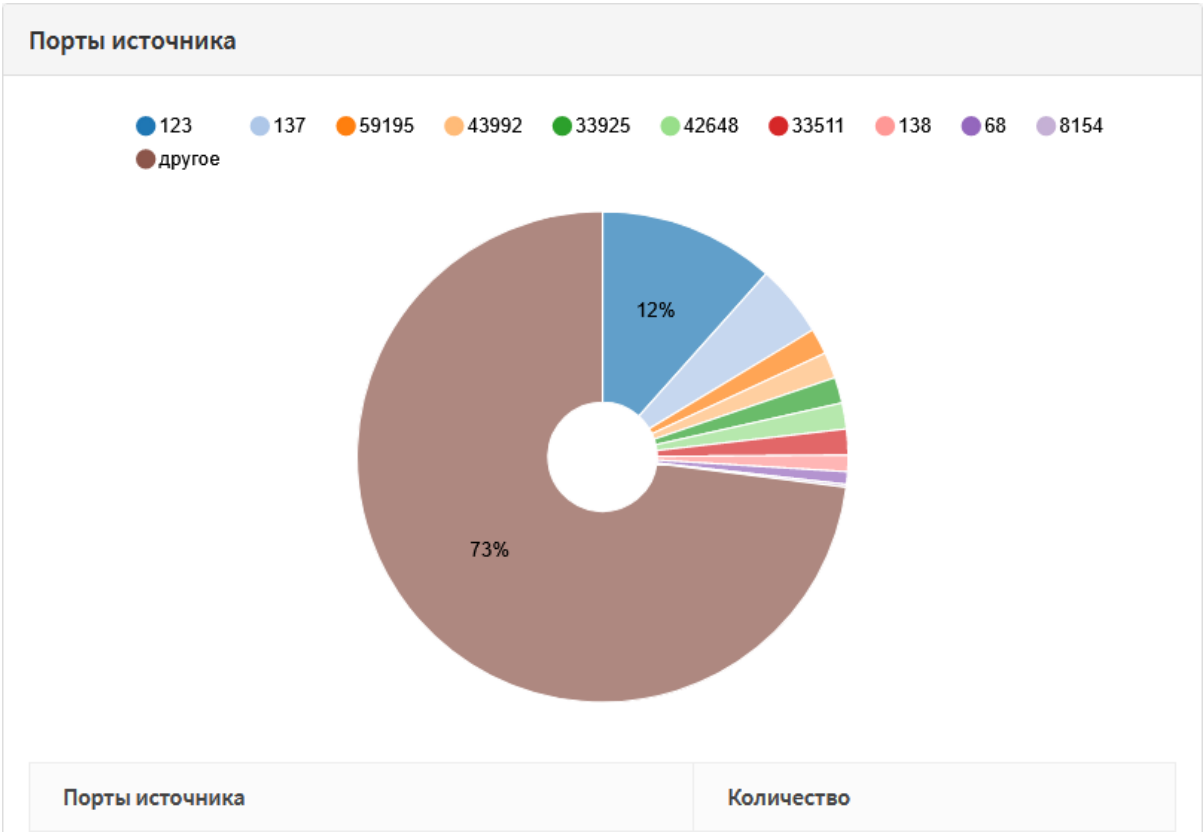


Рисунок – Порты источника

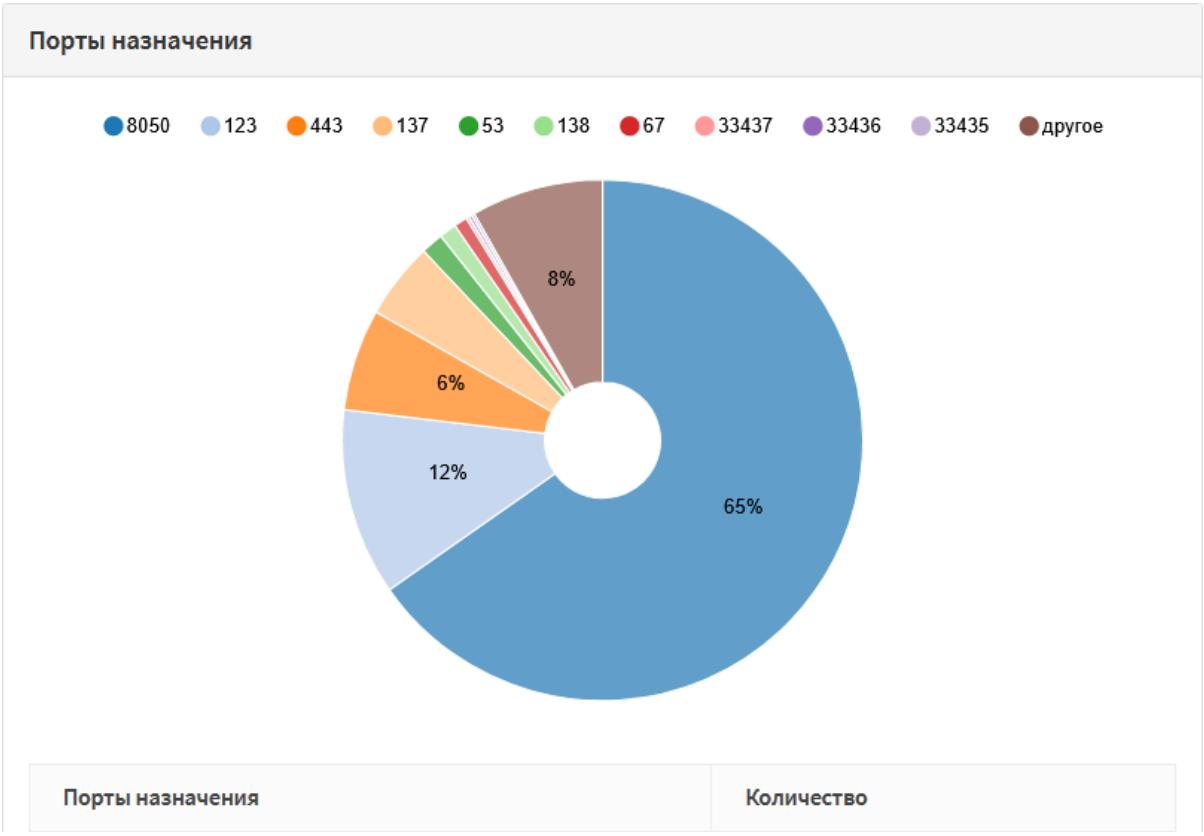


Рисунок – Порты назначения

32.6 Диагностика статической маршрутизации

Для диагностики статической маршрутизации в **ARMA FW** предусмотрены два подраздела:

- статус маршрутизации (**«Система» - «Маршруты» - «Статус»**) – в подразделе приведена таблица маршрутов системы (см. Рисунок – Диагностика статической маршрутизации);

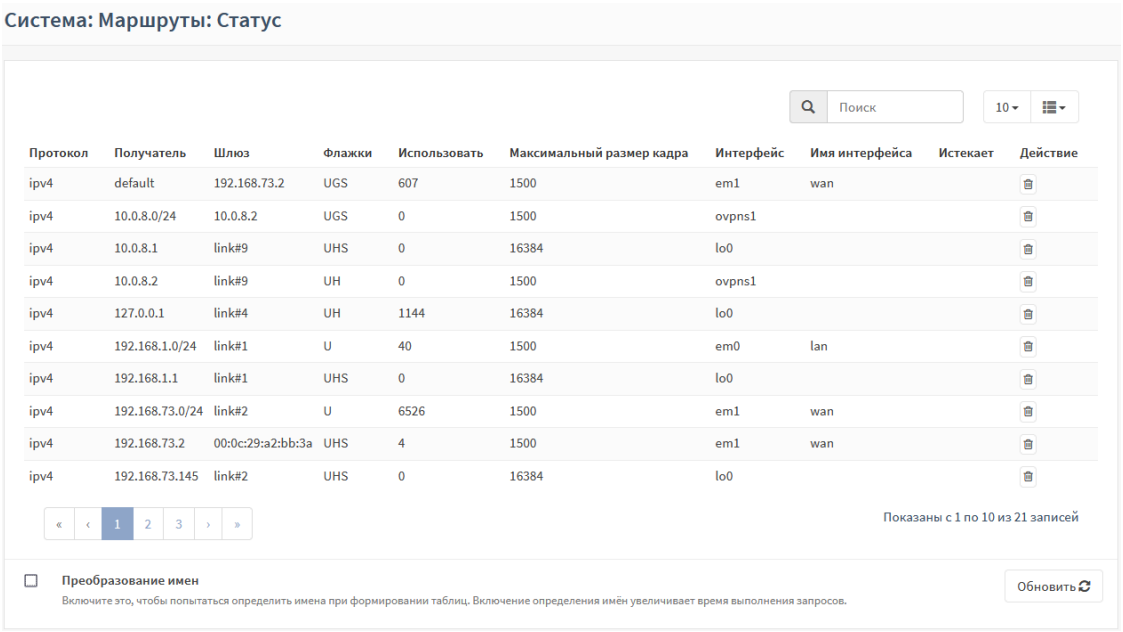


Рисунок – Диагностика статической маршрутизации

- журнал маршрутизации (**«Система» - «Маршруты» - «Журнал»**) – в подразделе отображены события изменения маршрутов (см. Рисунок – Журнал статической маршрутизации).

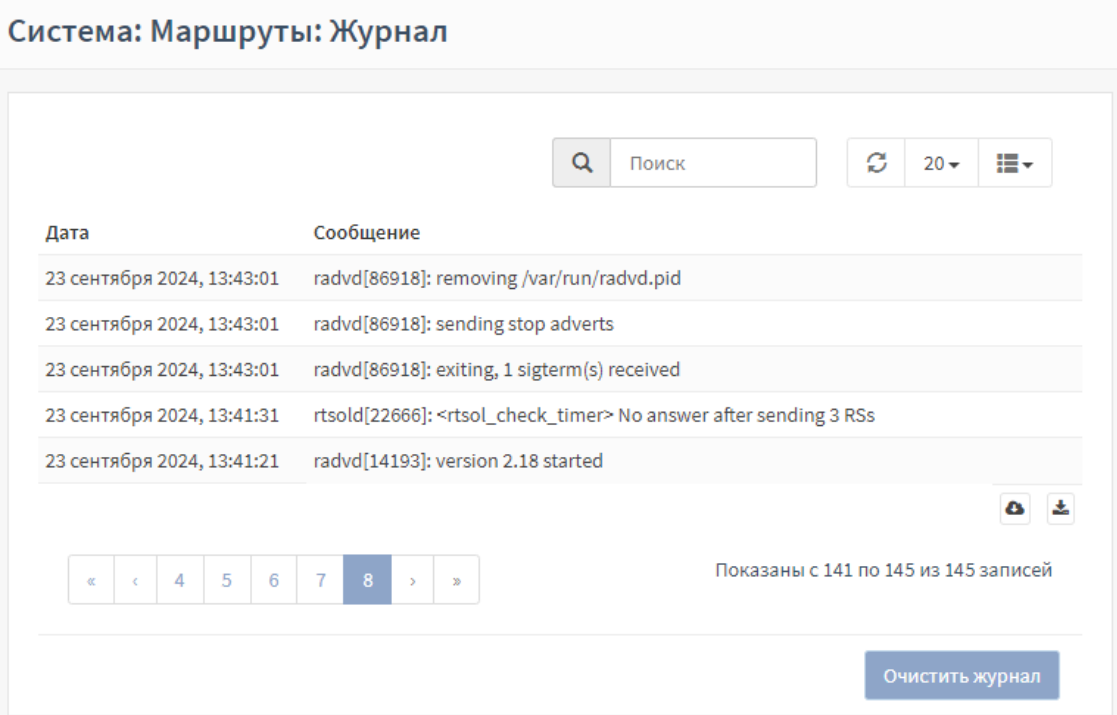


Рисунок – Журнал статической маршрутизации

32.7 Диагностика динамической маршрутизации

Для диагностики динамической маршрутизации в **ARMA FW** предусмотрены следующие вкладки в подразделе общих настроек динамической маршрутизации (**«Маршрутизация» - «Диагностика» - «Общие настройки»**):

- **«Маршруты IPv4»** – отображает данные о маршрутах IPv4 (см. Рисунок – Маршруты IPv4);

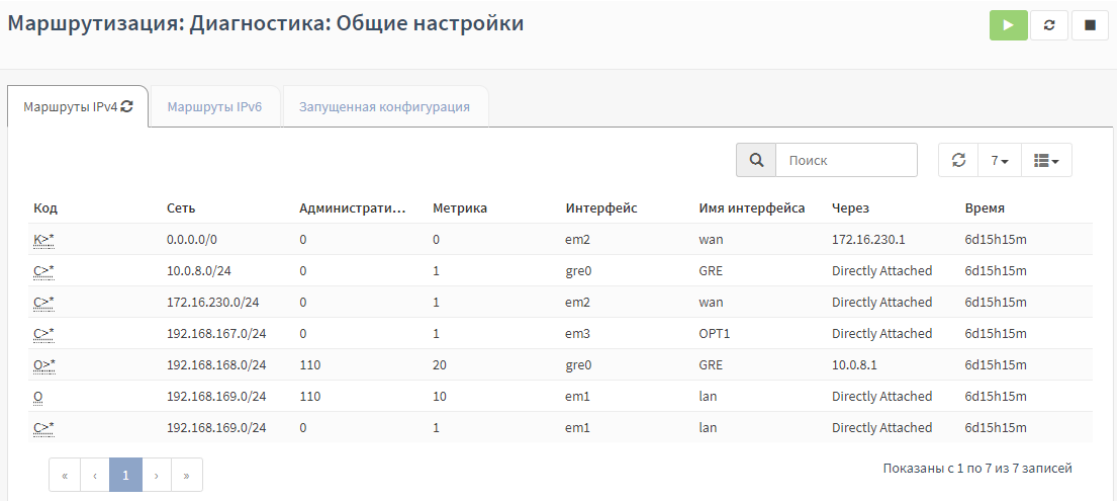


Рисунок – Маршруты IPv4

- **«Маршруты IPv6»** – отображает данные о маршрутах IPv6 (см. Рисунок – Маршруты IPv6);

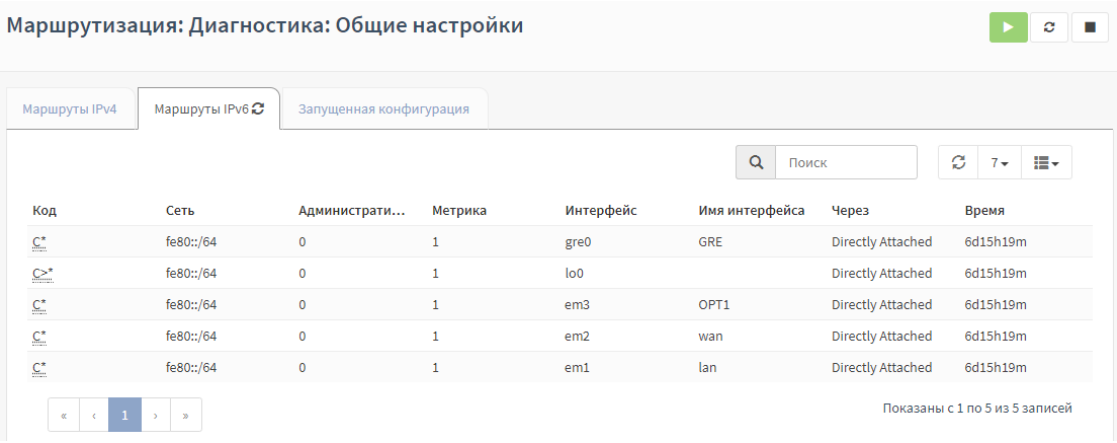


Рисунок – Маршруты IPv6

- **«Запущенная конфигурация»** – отображает общую конфигурацию настроенных динамических маршрутов (см. Рисунок – Запущенная конфигурация).

Рисунок – Запущенная конфигурация

32.7.1 OSPF

Для просмотра данных о настройке динамической маршрутизации по протоколу OSPF в **ARMA FW** предусмотрены следующие вкладки в подразделе OSPF динамической маршрутизации (**«Маршрутизация» - «Диагностика» - «OSPF»**):

- **«Обзор»** – отображает общие данные о настройке динамической маршрутизации по протоколу OSPF (см. Рисунок – Обзор);

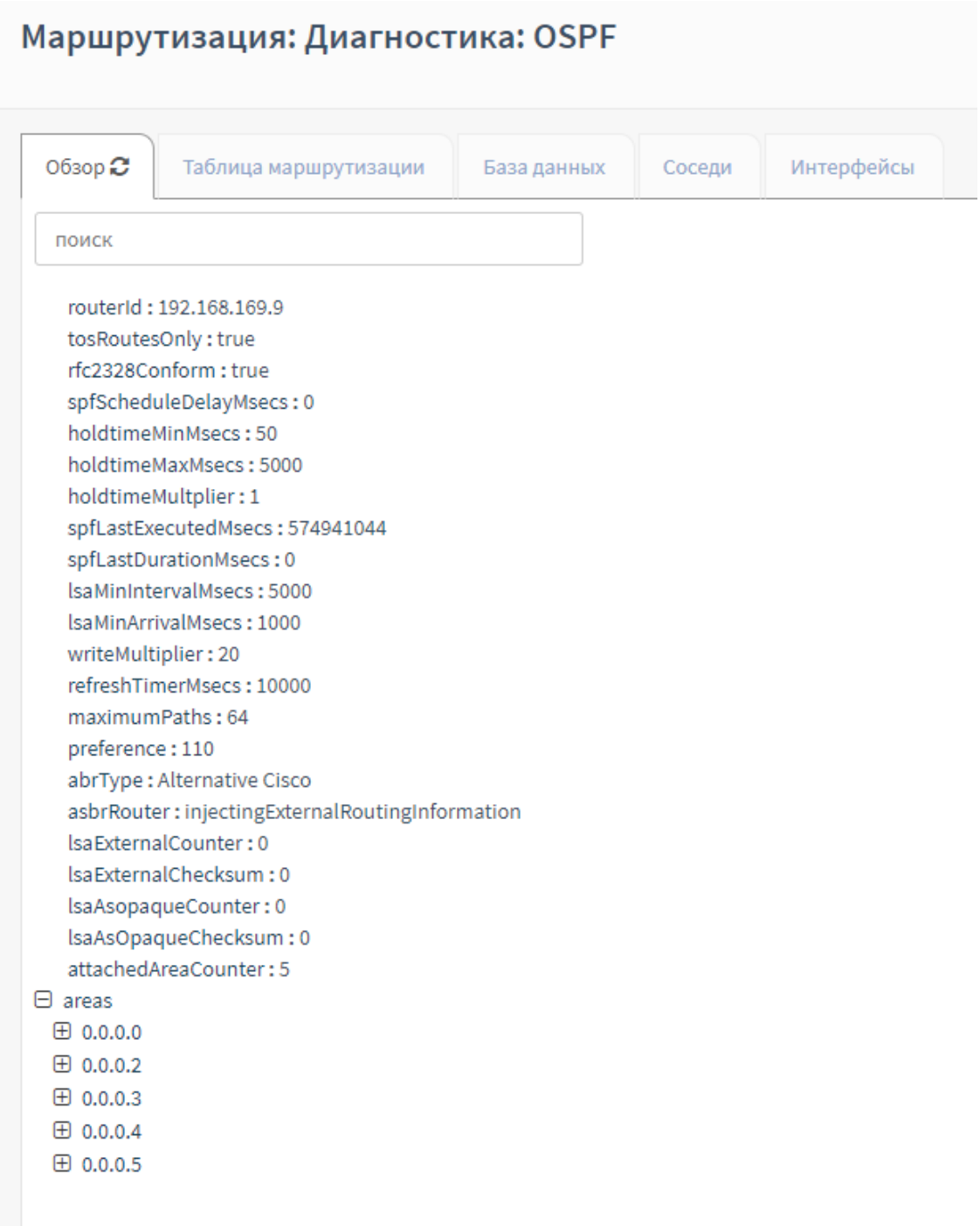


Рисунок – Обзор

- **«Таблица маршрутизации»** – отображает таблицу маршрутизации сети/роутера (см. Рисунок – Таблица маршрутизации);

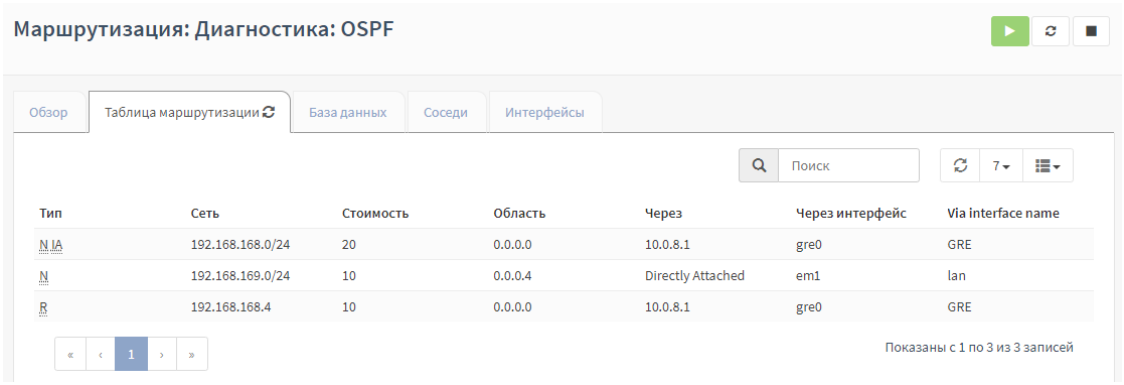


Рисунок – Таблица маршрутизации

- **«База данных»** – отображает информацию о состоянии связи (см. Рисунок – База данных);

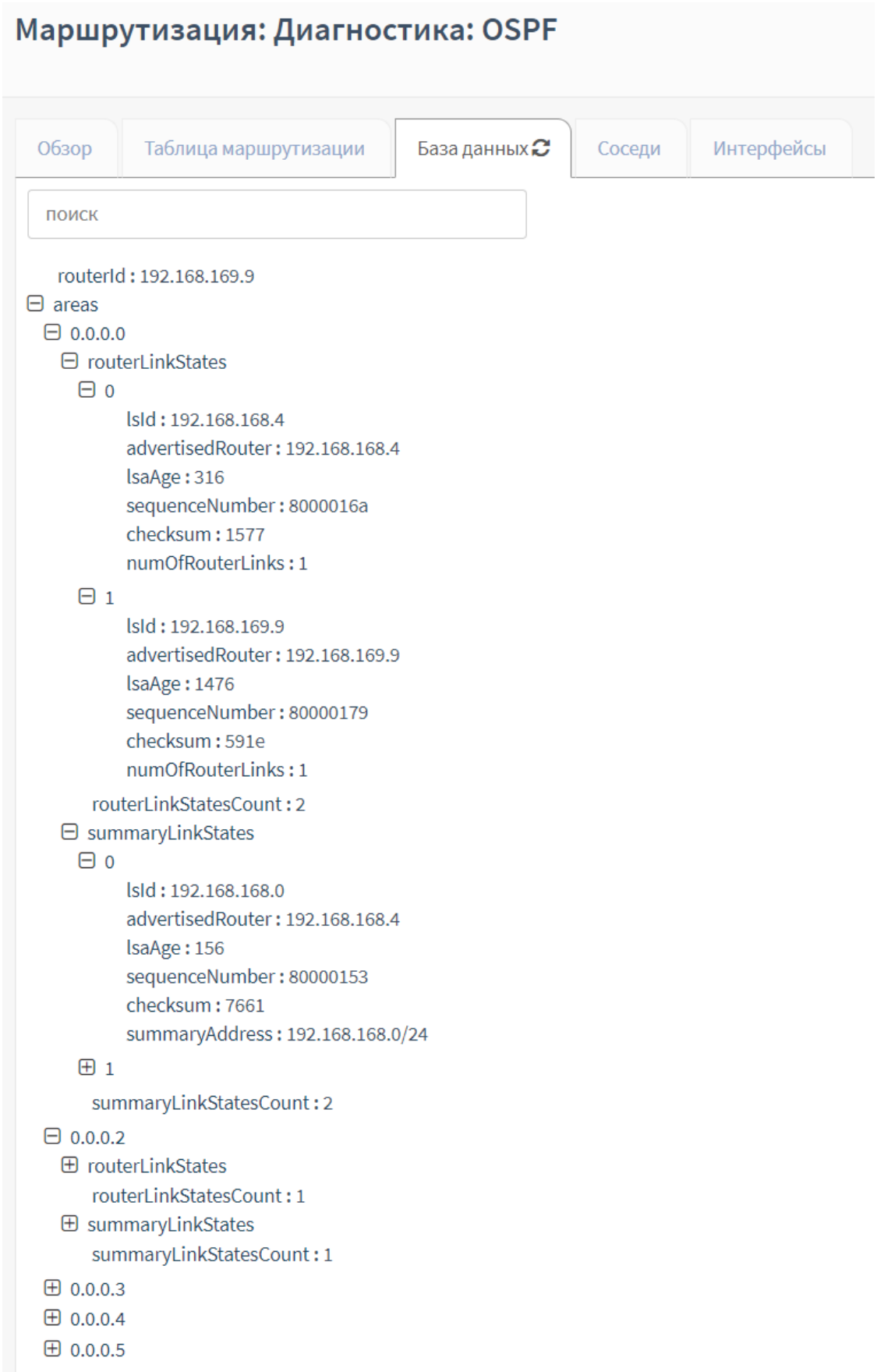


Рисунок – База данных

- **«Соседи»** – отображает таблицу соседей (см. Рисунок – Соседи);

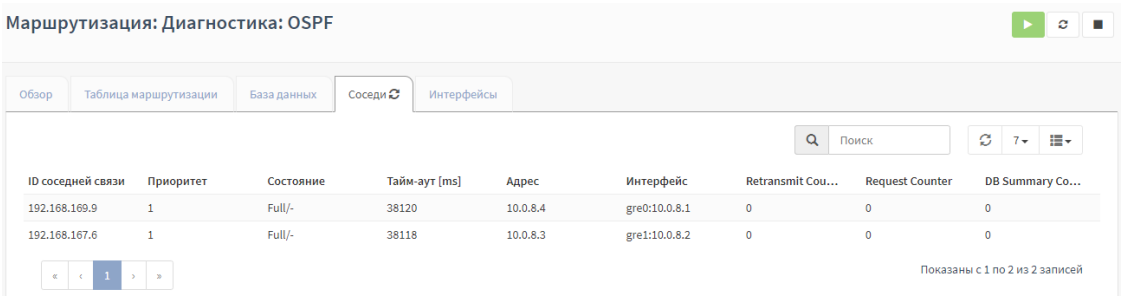


Рисунок – Соседи

- **«Интерфейсы»** – отображает данные о настроенных интерфейсах (см. Рисунок – Интерфейсы).

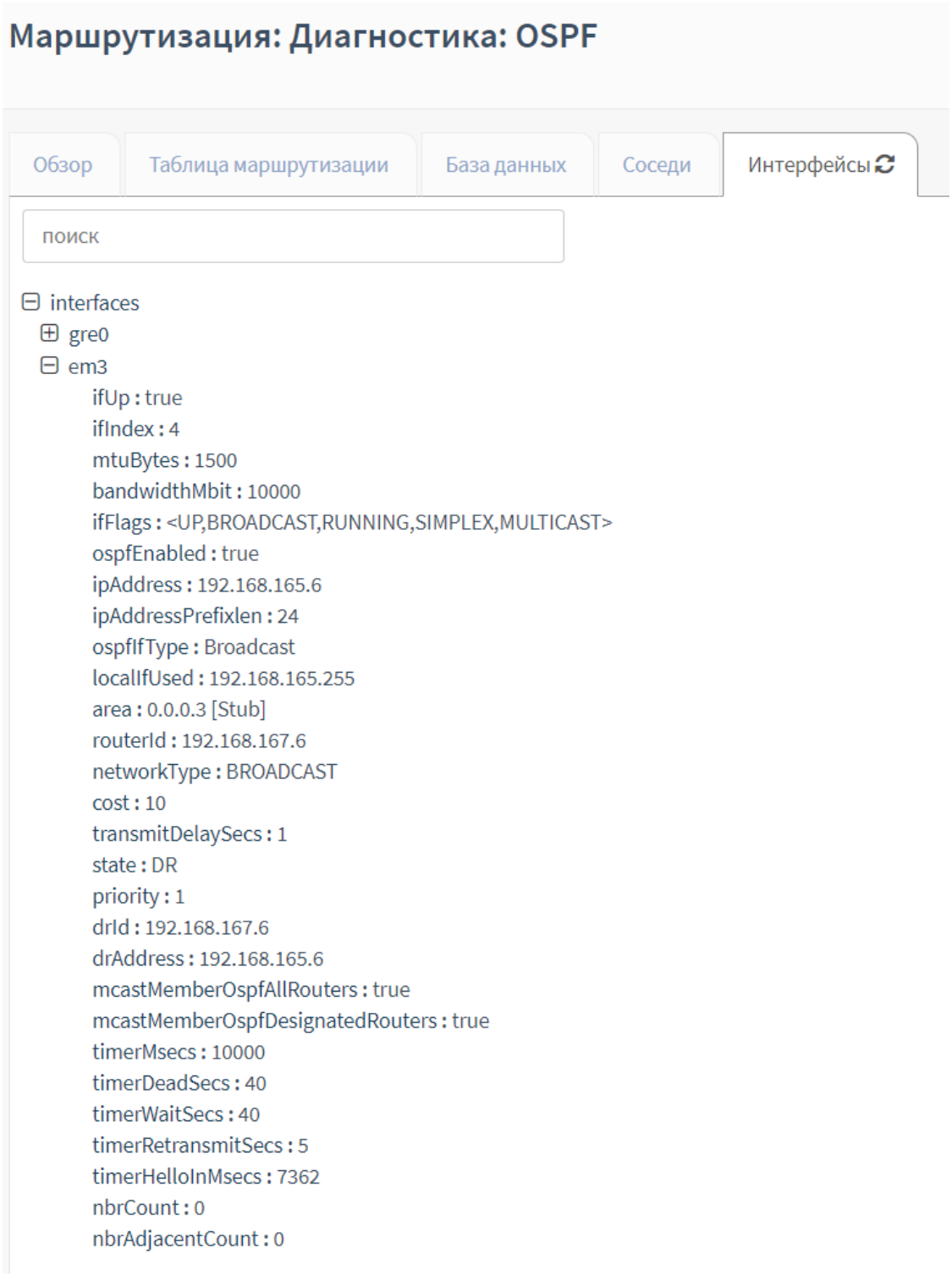


Рисунок – Интерфейсы

32.7.2 BGP

Для просмотра данных о настройке динамической маршрутизации по протоколу BGP в **ARMA FW** предусмотрен соответствующий подраздел (**«Маршрутизация» - «Диагностика» - «BGP»**). Во вкладке **«IPv4 Таблица маршрутизации»** отображаются следующие данные:

- **«Валидный»**;

- **«Лучший»**;
- **«Внутренний префикс»**;
- **«Сеть»**;
- **«Следующий шаг»**;
- **«Метрика»**;
- **«Локальные предпочтения»**;
- **«Весовой коэффициент»**;
- **«Путь»**;
- **«Происхождение»**.

Во вкладках **«Подробности»**, **«Соседи»**, **«Сводка»** отображаются подробные данные о соединении и соседях (см. Рисунок – BGP. Подробности).

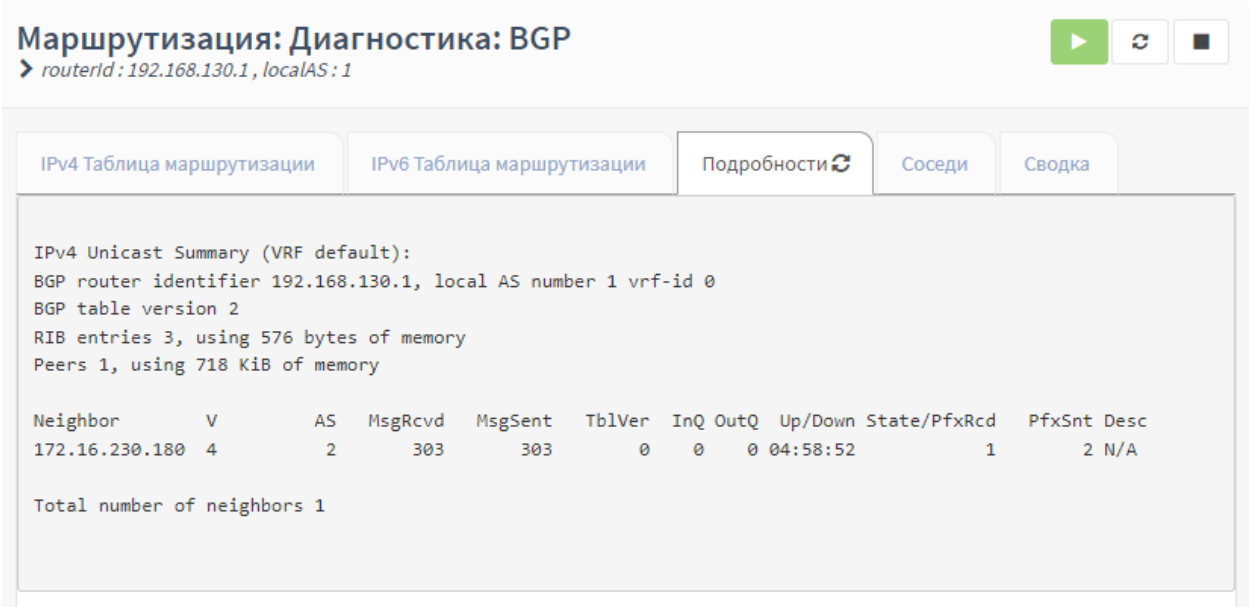


Рисунок – BGP. Подробности

32.8 Диагностика СОВ/СПВ

Для просмотра данных СОВ/СПВ в **ARMA FW**, в подразделе администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**), предусмотрена вкладка **«Журналирование»** (см. Рисунок – Диагностика СОВ/СПВ).

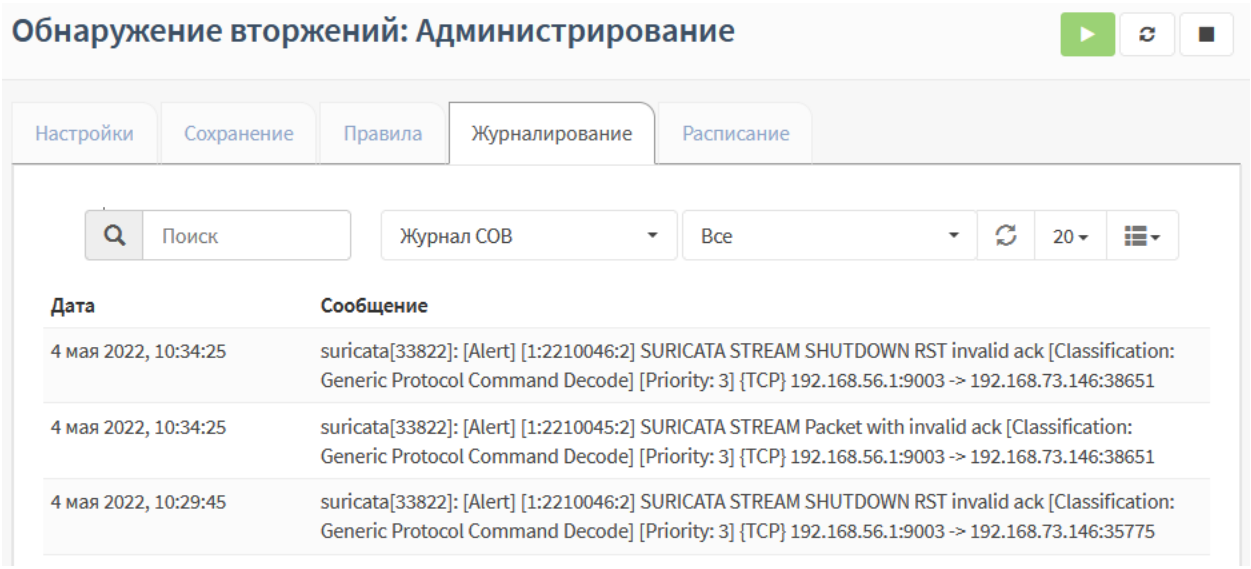


Рисунок – Диагностика СОВ/СПВ

32.9 Диагностика синхронизации времени

Для просмотра данных о синхронизации времени в **ARMA FW** предусмотрен подраздел статуса сетевого времени (**«Службы» - «Сетевое время» - «Статус»**) (см. Рисунок – Диагностика синхронизации времени), показывающий текущий статус сетевого времени.

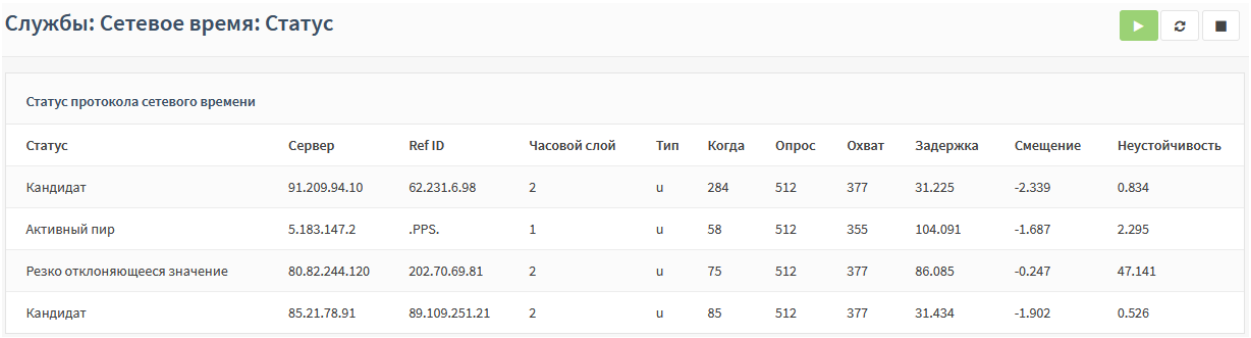


Рисунок – Диагностика синхронизации времени

32.10 Анализ дампа трафика

Для просмотра и анализа дампа трафика, захваченного СОВ, в **ARMA FW** предусмотрен подраздел журналирования (**«Сеть» - «Анализ трафика» - «Журналирование»**) (см. Рисунок – Анализ трафика). Анализ обеспечивается инструментом «Tshark».

Для отображения записей необходимо выбрать из выпадающего списка в верхней левой части формы требуемый файл журнала. Разбиение журналов осуществляется по дате и времени начала записи.

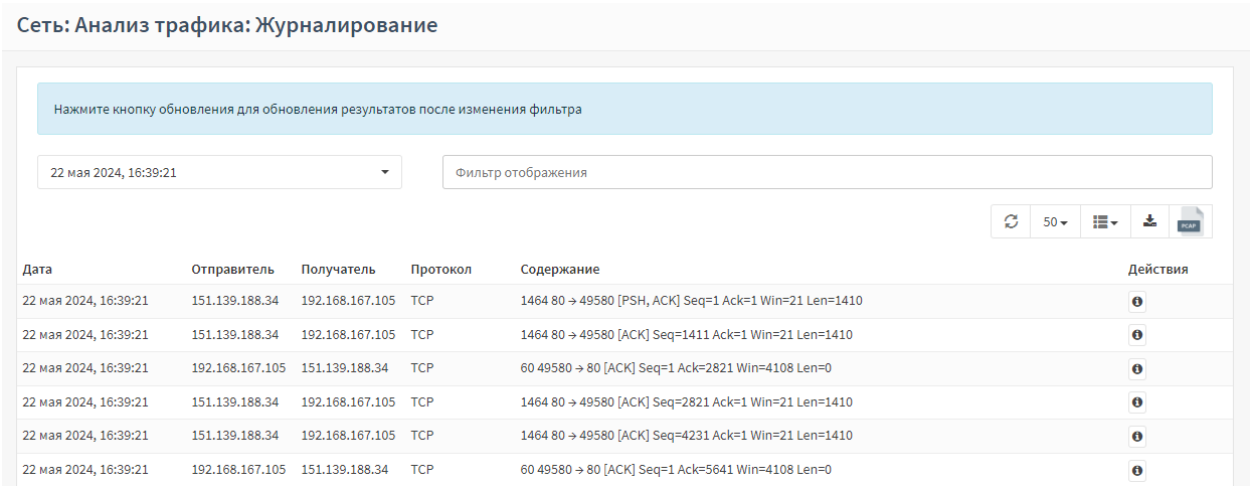


Рисунок – Анализ трафика

ARMA FW позволяет обнаруживать вторжения и осуществлять мониторинг следующих протоколов:

- Modbus TCP;
- Modbus TCP x90 func. code (UMAS);
- S7Comm | S7Comm Plus;
- OPC DA | OPC UA;
- IEC 60870-5-104;
- IEC 61850-8-1 MMS;
- IEC 61850-8-1 GOOSE;
- ENIP / CIP;
- KRUG Круг ПК-контроллер;
- Profinet;
- DNP3.

32.10.1 Настройка анализатора

Для отображения корректной информации в таблице журналирования (**«Сеть» - «Анализ трафика» - «Журналирование»**) о захваченных пакетах может потребоваться дополнительная настройка анализатора.

В случае передачи сетевых пакетов через порт, отличный от стандартного для используемого протокола, информация, отображаемая в таблице журналирования, о переданных пакетах может быть неактуальна.

В качестве примера приведён порядок настройки переопределения порта для протокола при захвате трафика, переданного по протоколу IEC 104 через порт

«2407». В данном случае о переданных пакетах изначально будет отображаться следующая информация (см. Рисунок – Информация о пакетах).

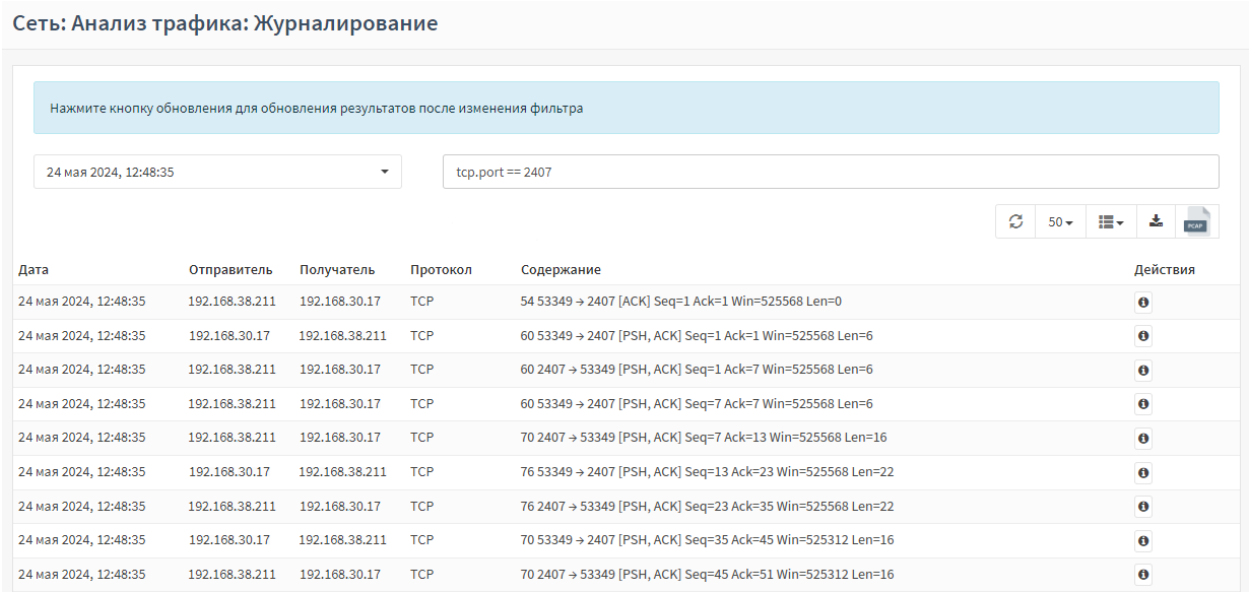


Рисунок – Информация о пакетах

Для настройки переопределения порта для протокола необходимо выполнить следующие действия:

1. Перейти в подраздел настройки анализатора (**«Сеть» - «Анализ трафика» - «Настройки»**) и нажать **кнопку** « + » (см. Рисунок – Настройка анализатора).

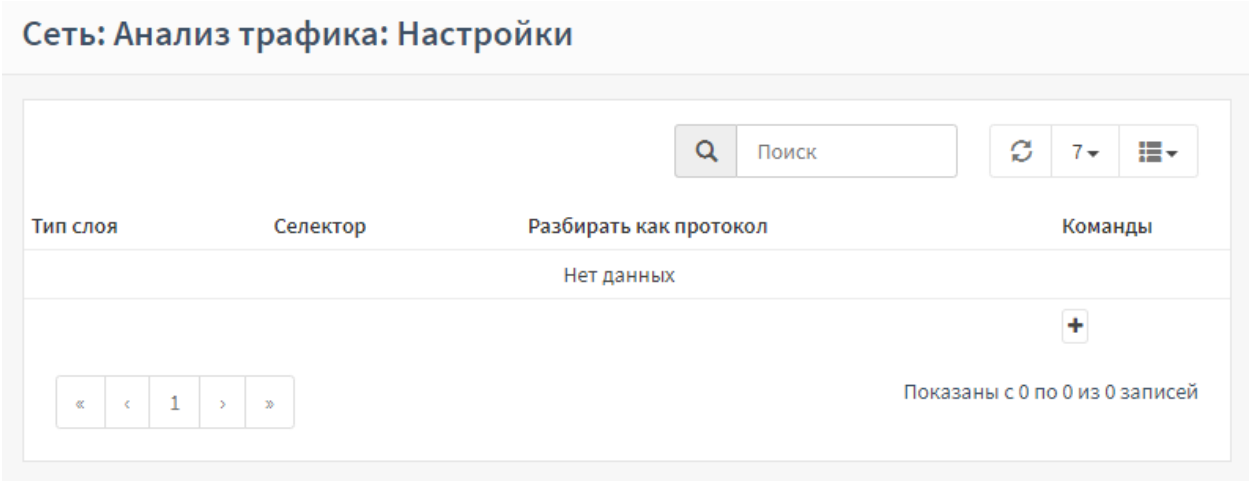


Рисунок – Настройка анализатора

2. В открывшемся окне указать следующие параметры:
   - **«Тип слоя»** – «tcp.port»;
   - **«Селектор»** – «2407»;
   - **«Разбирать как протокол»** – «iec60870_104»;

   и нажать **кнопку «Сохранить»** (см. Рисунок – Переопределение порта).

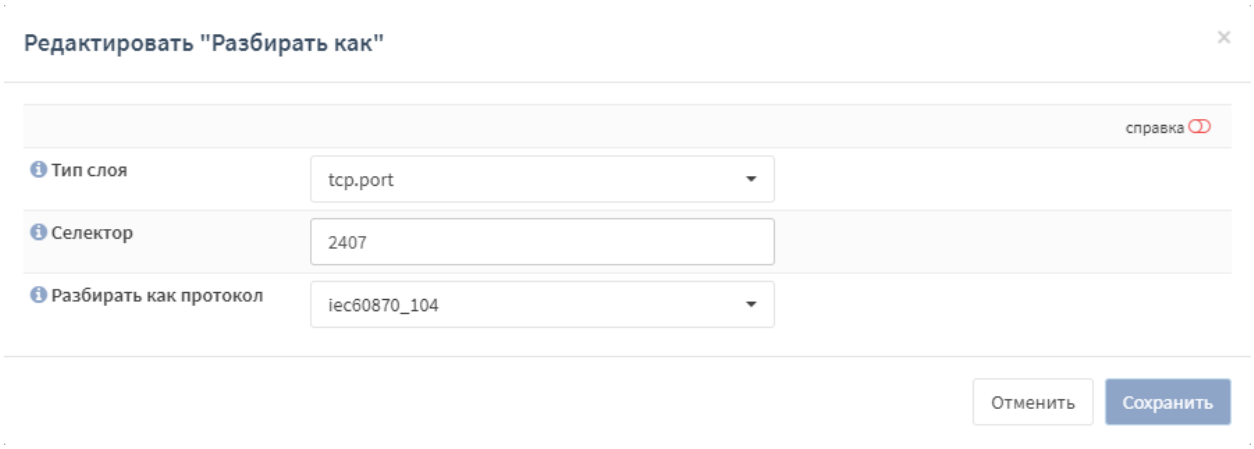


Рисунок – Переопределение порта

3. Перейти в подраздел журналирования (**«Сеть» - «Анализ трафика» - «Журналирование»**), выбрать файл журнала, ввести значение «tcp.port == 2407» в поле **«Фильтр отображения»** и нажать **кнопку** « ».

В журнале для интересующих пакетов будет отображаться актуальная информация (см. Рисунок – Информация о пакетах при настроенном переопределении порта).

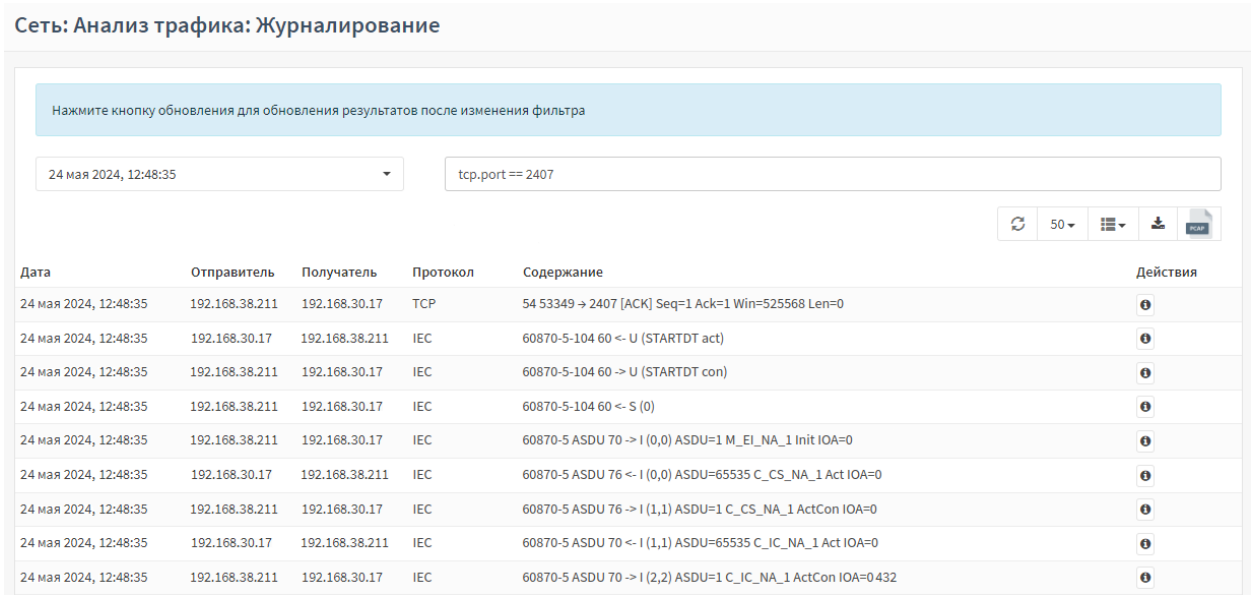


Рисунок – Информация о пакетах при настроенном переопределении порта

32.10.2 Экспорт дампа трафика

В случае необходимости экспорта дампа трафика следует в подразделе журналирования (**«Сеть» - «Анализ трафика» - «Журналирование»**) в зависимости от требуемого формата выгружаемого файла нажать:

- **кнопку** « » – для экспорта файла с расширением **«pcap»**;
- **кнопку** « » – для экспорта файла с расширением **«csv»**.

32.11 Диагностика состояния ARMA FW

32.11.1 Снимок состояний

Для просмотра активных состояний в текущий момент времени в **ARMA FW** предусмотрен подраздел состояний **ARMA FW** (**«Межсетевой экран» - «Диагностика» - «Снимок состояний»**) (см. Рисунок – Снимок состояний МЭ).

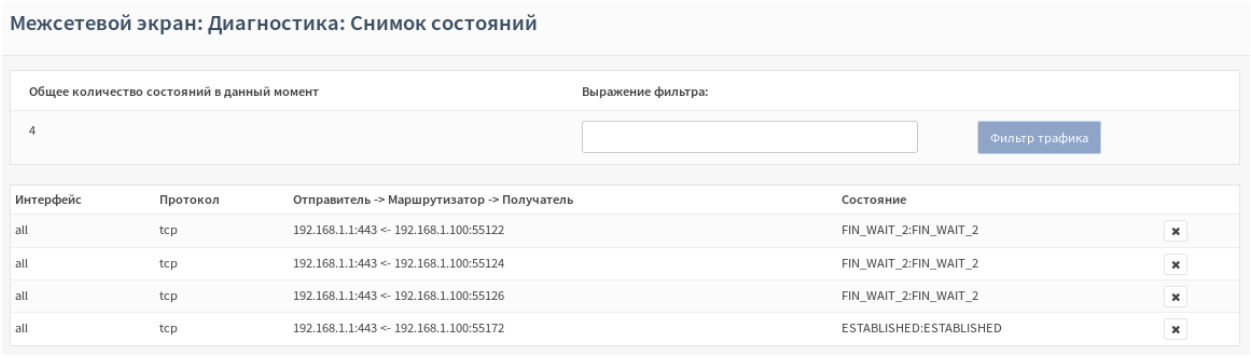


Рисунок – Снимок состояний МЭ

32.11.2 Сброс состояний

Для удаления активных состояний и/или отслеживания источника в **ARMA FW** предусмотрен подраздел сброса состояний (**«Межсетевой экран» - «Диагностика» - «Сброс состояний»**) (см. Рисунок – Сброс состояний МЭ). Для выполнения данных действий необходимо установить соответствующий флажок и нажать **кнопку «Очистить»**.

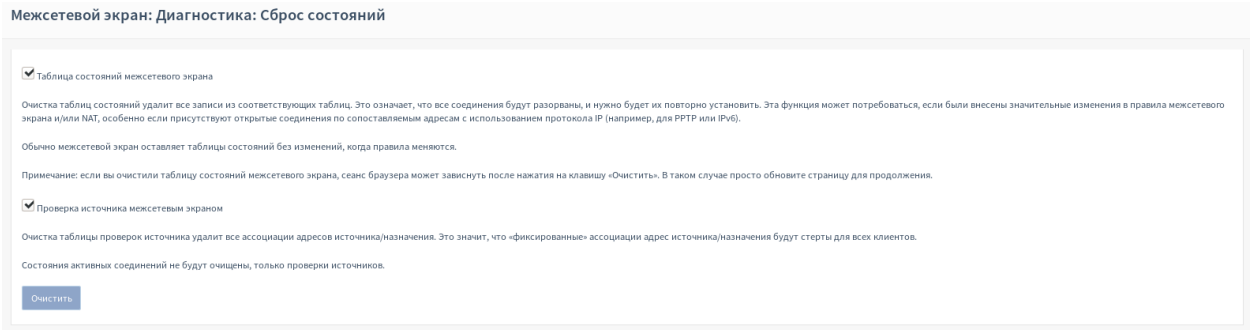
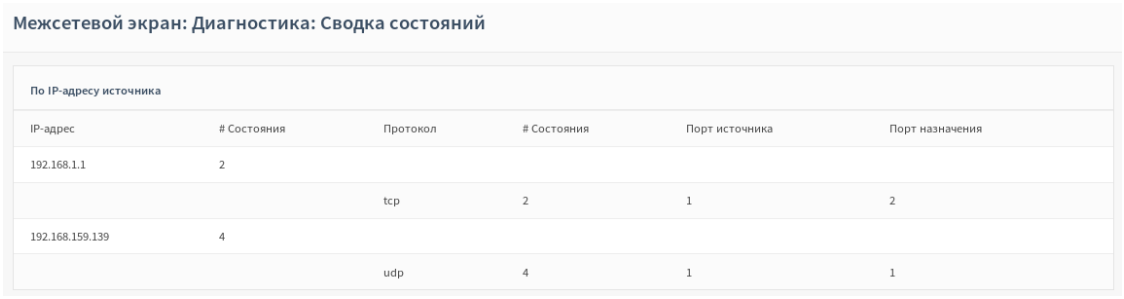


Рисунок – Сброс состояний МЭ

32.11.3 Сводка состояний

Для просмотра состояний МЭ в **ARMA FW** предусмотрен подраздел сводки состояний (**«Межсетевой экран» - «Диагностика» - «Сводка состояний»**). Подраздел позволяет просматривать данные, отсортированные по таблицам:

- **«По IP-адресу источника»** – Рисунок – Сводка состояний МЭ «По IP-адресу источника»;

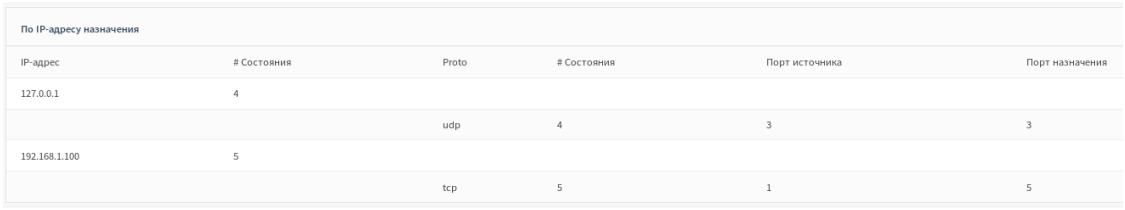

Межсетевой экран: Диагностика: Сводка состояний

По IP-адресу источника

IP-адрес	# Состояния	Протокол	# Состояния	Порт источника	Порт назначения
192.168.1.1	2				
		tcp	2	1	2
192.168.159.139	4				
		udp	4	1	1

Рисунок – Сводка состояний МЭ «По IP-адресу источника»

- **«По IP-адресу назначения»** – Рисунок – Сводка состояний МЭ «По IP-адресу назначения»;


По IP-адресу назначения

IP-адрес	# Состояния	Proto	# Состояния	Порт источника	Порт назначения
127.0.0.1	4				
		udp	4	3	3
192.168.1.100	5				
		tcp	5	1	5

Рисунок – Сводка состояний МЭ «По IP-адресу назначения»

- **«Всего по IP-адресу»** – Рисунок – Сводка состояний МЭ «Всего по IP-адресу»;


Всего по IP-адресу

IP-адрес	# Состояния	Proto	# Состояния	Порт источника	Порт назначения
127.0.0.1	8				
		udp	8	3	3
192.168.1.1	5				
		tcp	5	1	5
192.168.1.100	5				
		tcp	5	1	5

Рисунок – Сводка состояний МЭ «Всего по IP-адресу»

- **«По паре IP-адресов»** – Рисунок – Сводка состояний МЭ «По паре IP-адресов»;


По паре IP-адресов

IP-адрес	# Состояния	Proto	# Состояния	Порт источника	Порт назначения
192.168.1.1 -> 192.168.1.100	5				
		tcp	5	1	5
127.0.0.1 -> 127.0.0.1	4				
		udp	4	3	3

Рисунок – Сводка состояний МЭ «По паре IP-адресов»

32.12 Статистика трафика

Для просмотра текущей загрузки всех сетевых интерфейсов в режиме реального времени в **ARMA FW** предусмотрен подраздел отслеживания трафика (**«Создание отчетов» - «Трафик»**) (см. Рисунок – Трафик).

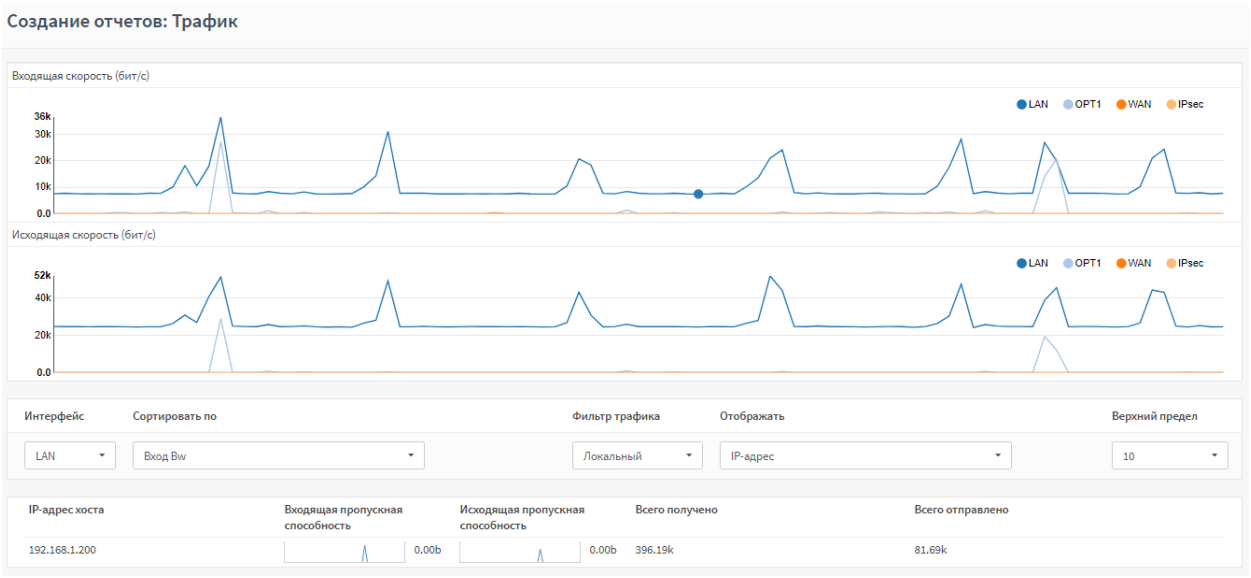


Рисунок – Трафик

32.13 Monit

Сервис Monit является встроенным в систему пакетом. Это утилита мониторинга с возможностью выполнения скриптов в качестве реакции на заданное событие.

Monit используется для следующих действий:

- **отслеживание состояния серверов** – доступность, потребление ресурсов;
- **мониторинг сервисов** – состояние, потребляемые ресурсы, количество дочерних процессов;
- **мониторинг сетевых сервисов** – возможность подключения и корректность ответа;
- **выполнение действий** – встроенных или собственных, созданных с помощью скриптов, запускаемых при свершении определённых событий;
- **отправка уведомлений** – по электронной почте или в централизованный веб-интерфейс Monit.

32.13.1 Включение сервиса Monit

Для включения Monit необходимо выполнить следующие действия:

1. Перейти в подраздел настройки Monit (**«Службы» - «Monit» - «Настройки»**).
2. Установить флажок **«Включить Monit»**.
3. При необходимости указать значения параметров:
   - **«Интервал опроса»** – интервал опроса в секундах;
   - **«Задержка старта»** – задержка запуска проверок Monit после загрузки **ARMA FW** в секундах;

- **«Почтовый сервер»** – IP-адрес или доменное имя почтового сервера. Несколько адресов необходимо разделять знаком «запятая». По умолчанию задано значение «127.0.0.1»;
- **«Порт почтового сервера»** – порт, прослушиваемый почтовым сервером;
- **«Имя пользователя»** – имя пользователя для аутентификации;
- **«Пароль»** – пароль для аутентификации;
- **«Защищённое соединение»** – флажок установить, если почтовый сервер использует шифрование.

Значения параметров **«Почтовый сервер»**, **«Имя пользователя»**, **«Пароль»** указаны справочно.

4. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»** (см. Рисунок – Включение Monit).

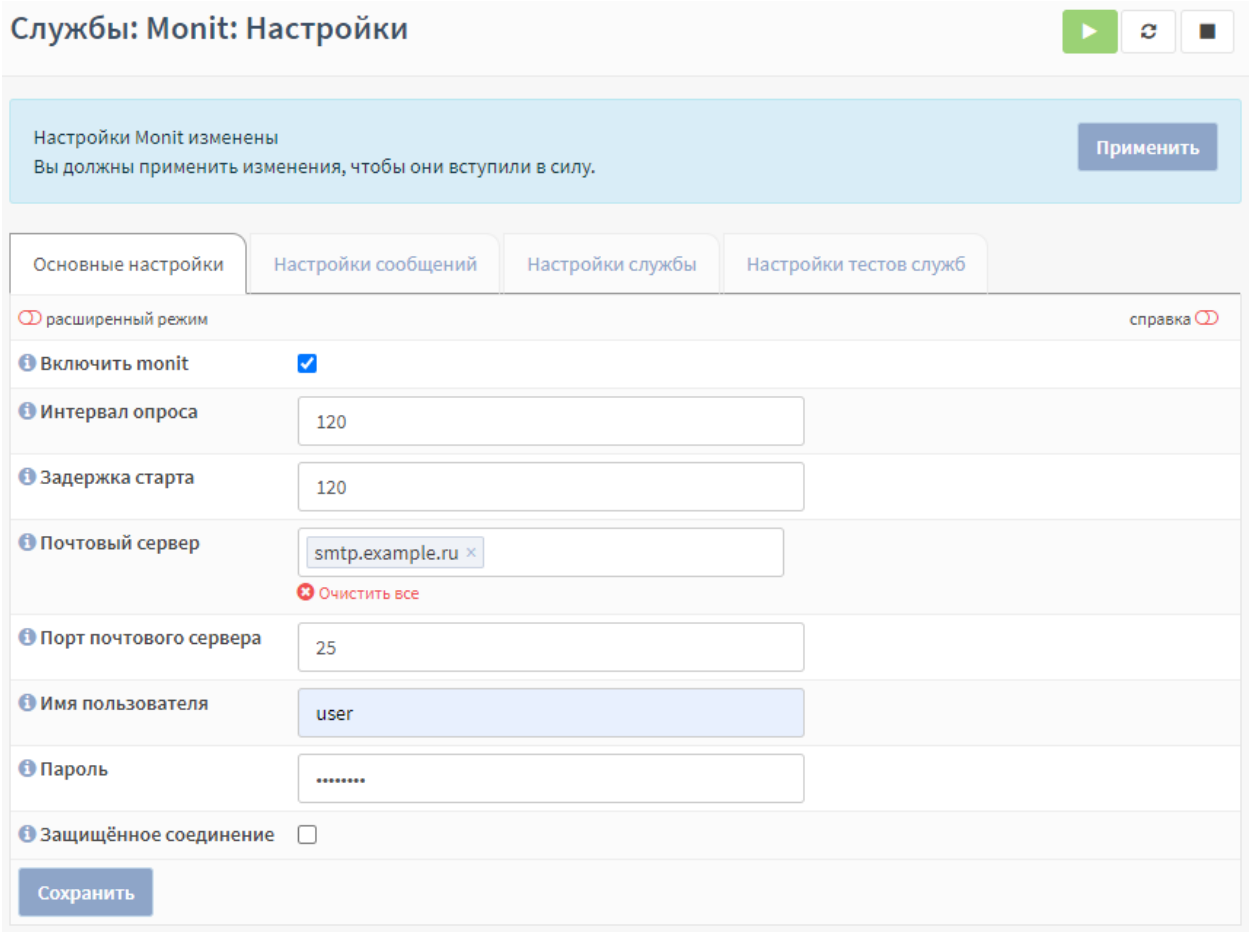


Рисунок – Включение Monit

32.13.2 Настройка рассылки сообщений

Для настройки рассылки сообщений необходимо выполнить следующие действия:

1. Перейти во вкладку **«Настройки сообщений»** подраздела настройки Monit (**«Службы» - «Monit» - «Настройки»**) и нажать **кнопку** « ».
2. В открывшейся форме указать значения параметров:
   - **«Включить сообщения»** – флажок установлен;
   - **«Получатель»** – адрес для рассылки сообщений;
   - **«События»** – список событий, запускающих рассылку. Значение «Не выбрано» означает выбор всех событий.
3. При необходимости указать значения параметров:
   - **«Not on»** – флажок установлен, если требуется отправлять сообщения для событий кроме выбранных;
   - **«Формат почты»** – адрес отправителя, адрес для ответа и тема сообщения, например:

     ```
     From: sender@example.ru
     Reply-To: support@example.ru
     Subject: $SERVICE at $HOST failed
     ```

   - **«Напоминание»** – количество повторных событий для напоминающей рассылки.
4. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

32.13.3 Настройка проверки сервиса

Для настройки проверки сервиса необходимо выполнить следующие действия:

1. Перейти во вкладку **«Настройки службы»** подраздела настройки Monit (**«Службы» - «Monit» - «Настройки»**) и нажать **кнопку** « ».
2. В открывшейся форме указать значения параметров:
   - **«Включить проверки служб»** – флажок установлен;
   - **«Имя»** – имя сервиса;
   - **«Тип»** – тип проверки. Значение «Настроенное пользователем» выбирать при необходимости применения пользовательского скрипта (см. Особенности настройки Monit с использованием пользовательских скриптов).
3. При необходимости указать значения доступных параметров в зависимости от выбранного типа проверки:
   - **«PID файл»** – файл, содержащий уникальный идентификатор процесса;
   - **«Совпадение»** – поиск процесса по шаблону;

- **«Путь»** – путь к файлу или директории;
- **«Адрес»** – целевой IP-адрес;
- **«Интерфейс»** – интерфейс;
- **«Запустить»** – скрипт запуска сервиса;
- **«Остановить»** – скрипт остановки сервиса;
- **«Тесты»** – тесты сервисов. Если в списке отсутствует требуемый тест, необходимо предварительно настроить его во вкладке **«Настройки тестов служб»**;
- **«Зависит от»** – сервисы, от состояния которых будет зависеть настраиваемый сервис.

4. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

32.13.4 Настройка теста

Для настройки тестов, инициируемых сервисом Monit, необходимо выполнить следующие действия:

1. Перейти во вкладку **«Настройки тестов служб»** подраздела настройки Monit (**«Службы» - «Monit» - «Настройки»**) и нажать **кнопку** « + ».
2. В открывшейся форме указать значения параметров:
   - **«Имя»** – имя теста;
   - **«Условие»** – условие выполнения;
   - **«Действие»** – выполняемое действие:
     - **«Предупредить (Alert)»**;
     - **«Перезапуск»**;
     - **«Запустить»**;
     - **«Остановить»**;
     - **«Выполнить»**;
     - **«Перестать мониторить»**.
3. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

32.13.5 Сценарии использования Monit

32.13.5.1 Настройка перезапуска службы «Suricata» на ведущем устройстве отказоустойчивого кластера

Для настройки перезапуска службы «Suricata» на ведущем устройстве отказоустойчивого кластера необходимо выполнить следующие действия:

1. Включить сервис Monit (см. Включение сервиса Monit).
2. Перейти во вкладку **«Настройки тестов служб»**, нажать **кнопку** « + » и в открывшейся форме указать следующие параметры:
   - **«Имя»** – «ChangedStatusRestart»;
   - **«Условие»** – «changed status»;
   - **«Действие»** – «Перезапуск».
3. Нажать **кнопку «Сохранить»**.
4. Перейти во вкладку **«Настройки службы»**, нажать **кнопку** « ✎ » напротив имени **«carp_status_change»** и в открывшейся форме указать следующие параметры:
   - **«Включить проверки служб»** – флажок установлен;
   - **«Запустить»** – «/usr/sbin/service suricata start»;
   - **«Остановить»** – «/usr/sbin/service suricata stop»;
   - **«Тесты»** – «ChangedStatusRestart».
5. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»** (см. Рисунок – Применение изменений).

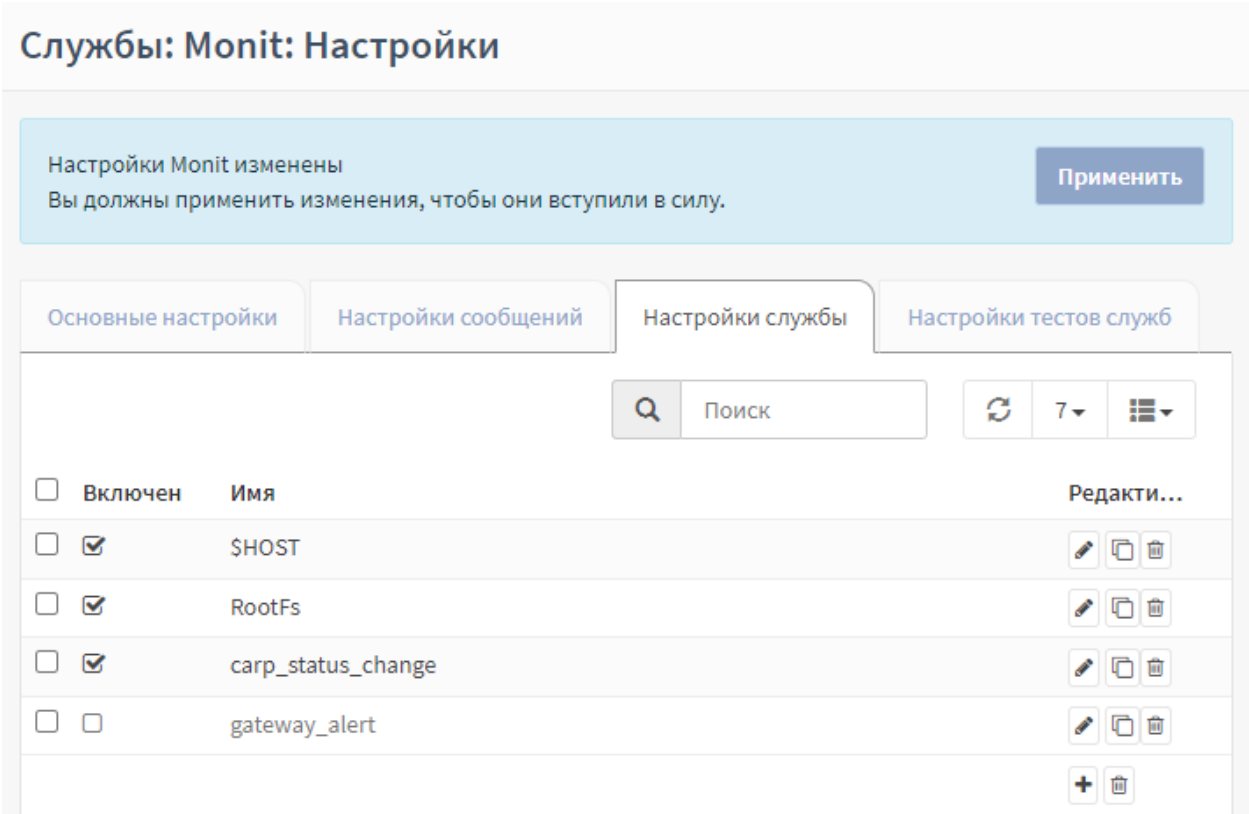


Рисунок – Применение изменений

32.13.5.2 Перезапуск сервиса при его отказе

В качестве примера рассмотрен мониторинг и перезапуск сервиса ARPwatch в случае его отказа.

1. Включить сервис Monit (см. Включение сервиса Monit).
2. Перейти во вкладку **«Настройки тестов служб»**, нажать **кнопку** « + » и в открывшейся форме указать следующие параметры:
   - **«Имя»** – «arpwatch_check»;
   - **«Условие»** – «changed status»;
   - **«Действие»** – «Перезапуск».
3. Нажать **кнопку «Сохранить»**.
4. Перейти во вкладку **«Настройки службы»**, нажать **кнопку** « + » и в открывшейся форме указать следующие параметры:
   - **«Включить проверки служб»** – флажок установлен;
   - **«Имя»** – «arpwatch_restart»;
   - **«Тип»** – «Процесс»;
   - **«PID файл»** – «/var/run/arpwatch-vmx1.pid»;
   - **«Запустить»** – «/usr/sbin/service arpwatch start»;
   - **«Остановить»** – «/usr/sbin/service arpwatch stop».
5. Нажать **кнопку «Сохранить»**, а затем нажать **кнопку «Применить»**.

32.13.5.3 Особенности настройки Monit с использованием пользовательских скриптов

Представлен общий подход к настройкам сервиса Monit, которые необходимо изменять с учётом конкретных ситуаций.

> **Примечание:**
>
> Применение пользовательских скриптов требует уверенности в их безопасности и понимания последствий, к которым могут привести действия, исполняемые системой.

Для настройки ответного действия с использованием пользовательских скриптов необходимо выполнить следующие действия:

1. Добавить скрипт в директорию файловой системы **ARMA FW**, например «/usr/local/scripts/».

2. Создать тест во вкладке **«Настройка тестов служб»** (см. Настройка теста) и указать значения в параметрах:
   - **«Имя»** – имя теста;
   - **«Условие»** – условие срабатывания и путь к добавленному скрипту;
   - **«Действие»** – выполняемое действие.
3. Добавить проверку во вкладке **«Настройки службы»** (см. Настройка проверки сервиса) и указать значения в параметрах:
   - **«Включить проверки служб»** – флажок установлен;
   - **«Имя»** – имя сервиса;
   - **«Тип»** – «Настроенное пользователем»;
   - **«Тесты»** – имя добавленного теста.

32.14 Создание отчетов

В **ARMA FW** реализована возможность формирования отчётов, содержащих информацию о пакетах, состоянии системы или трафике в виде графиков и таблиц.

Для экспорта отчёта необходимо выполнить следующие действия:

1. Перейти в подраздел состояние (**«Создание отчетов» - «Состояние»**).
2. Нажать **кнопку «Вкл.»** (**«Создание отчетов» - «Трафик»**) (см. Рисунок – Отчёты) для добавления отображения таблиц.

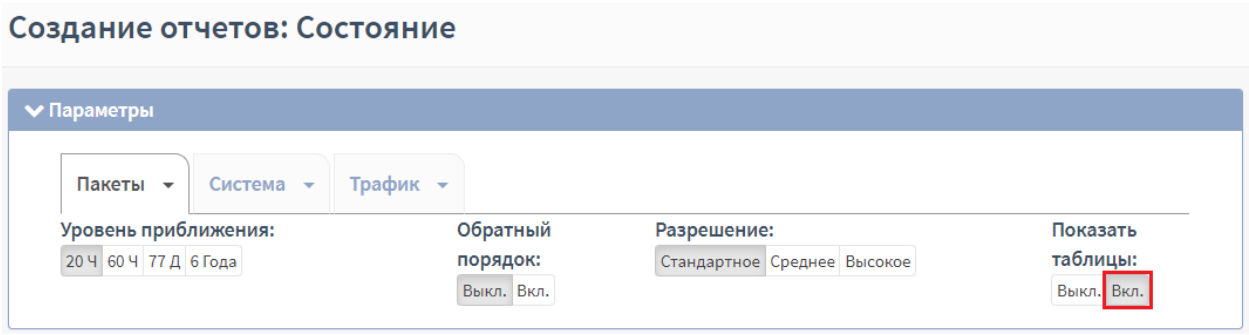


Рисунок – Отчёты

3. Нажать **кнопку «Загрузить как CSV»** в блоке **«Текущий вид – Подробный»** (см. Рисунок – Экспорт отчёта) для загрузки файла отчёта.

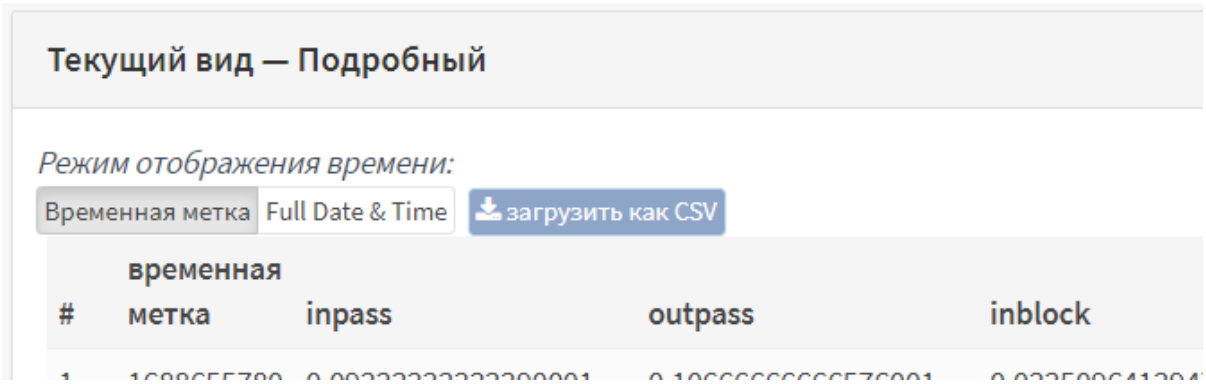


Рисунок – Экспорт отчёта

32.15 Диагностика RSPAN

Для просмотра данных о конфигурации RSPAN в подразделе диагностики RSPAN (**«Службы» - «RSPAN» - «Диагностика»**) предусмотрены следующие вкладки (см. Рисунок – Конфигурация):

- **«Сводка»**;
- **«Информация»**;
- **«Мосты»**;
- **«Порты»**;
- **«Зеркала»**.

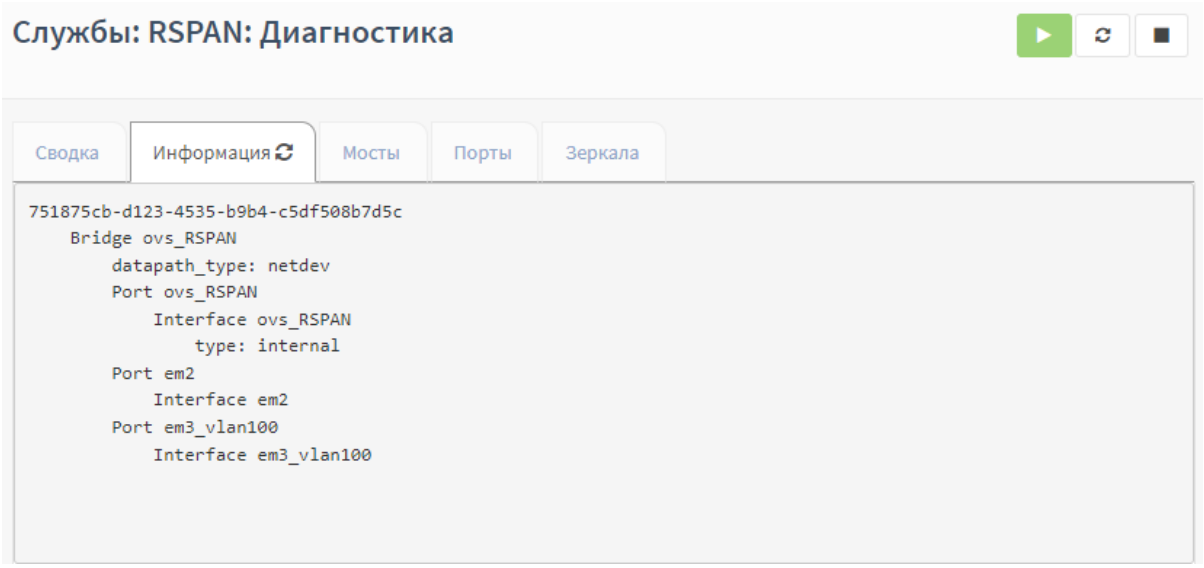


Рисунок – Диагностика RSPAN

32.16 Диагностика VPN

Для просмотра данных о конфигурации сервера или клиента VPN-соединения в **ARMA FW** предусмотрена вкладка в подразделе настройки OpenVPN (**«VPN» - «OpenVPN» - «Конфигурация»**) (см. Рисунок – Конфигурация).

VPN: OpenVPN: Конфигурация

server2.conf

```
dev ovpns2
verb 3
dev-type tun
tun-ipv6
dev-node /dev/tun2
writepid /var/run/openvpn_server2.pid
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
cipher AES-256-CBC
auth SHA256
up /usr/local/etc/inc/plugins.inc.d/openvpn/ovpn-linkup
down /usr/local/etc/inc/plugins.inc.d/openvpn/ovpn-linkdown
log-append /var/log/openvpn/openvpn-server-2.log
local 172.16.230.109
ifconfig 10.10.0.1 10.10.0.2
lport 1194
management /var/etc/openvpn/server2.sock unix
push "route 192.168.109.0 255.255.255.0"
route 192.168.128.0 255.255.255.0
secret /var/etc/openvpn/server2.secret
comp-lzo adaptive
```

Рисунок – Конфигурация

33 УПРАВЛЕНИЕ ПИТАНИЕМ

Раздел **«Питание»** позволяет перезагрузить и выключить систему, а также завершить пользовательскую сессию.

33.1 Перезагрузка

Для перезагрузки системы необходимо перейти в подраздел управления питанием (**«Система» - «Питание» - «Перезагрузка»**) и нажать **кнопку «Да»** (см. Рисунок – Перезагрузка системы). После перезагрузки системы откроется окно входа в систему.

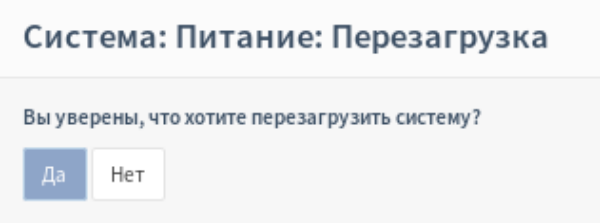


Рисунок – Перезагрузка системы

33.2 Выключение

Для выключения системы необходимо перейти в подраздел управления питанием (**«Система» - «Питание» - «Выключение»**) и нажать **кнопку «Да»** (см. Рисунок – Выключение системы). Система завершит свою работу.

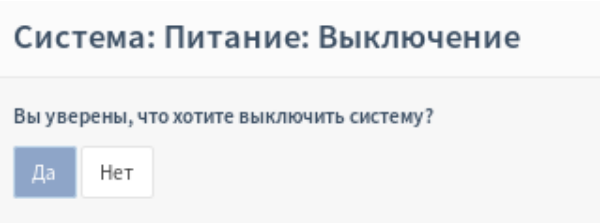


Рисунок – Выключение системы

33.3 Выход

Для завершения пользовательской сессии необходимо нажать на иконку пользователя в верхней правой части веб-интерфейса и выбрать **«Выход»** (см. Рисунок – Завершение пользовательской сессии). Произойдёт моментальный выход из системы и откроется окно входа в систему.

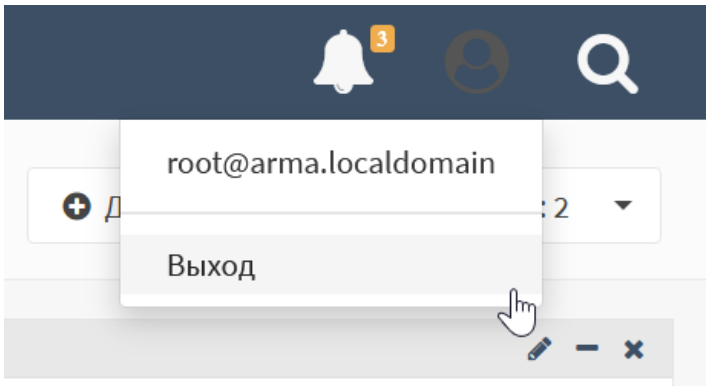


Рисунок – Завершение пользовательской сессии

34 ЖУРНАЛИРОВАНИЕ

34.1 Общие настройки журналирования

В подразделе журналирования (**«Система» - «Настройки» - «Журналирование»**) содержатся настройки, позволяющие управлять журналированием в системе.

Общие параметры журналирования:

- **«Обратный порядок отображения»** – при включении данного параметра последние записи в журнале отображаются сверху списка;
- **«Размер журнала (байт)»** – в поле существует возможность задать размер файлов журнала в диапазоне от 5120 до 100000000 байт, по умолчанию размер 500 Кб;
- **«Журнал веб-сервера»** – при включении данного параметра ошибки веб-сервера, в том числе портала авторизации, будут записаны в главный системный журнал;
- **«Локальные записи»** – при включении данного параметра запись журнала на локальный диск производиться не будет;
- **«Сброс записей»** – при нажатии **кнопки «Очистить файлы журналов»** будет произведена очистка всех локальных журналов.

Для большинства журналов доступны:

- возможность сохранения записей в текстовый файл с помощью кнопок:
  - « » – сохраняет записи журнала, представленные в данный момент в форме;
  - « » – сохраняет все записи журнала;
- удаление записей с помощью **кнопок «Очистить журнал»** или « »;
- поиск в журнале с помощью строки поиска (см. Рисунок – Строка поиска);

Рисунок – Строка поиска

- настройка фильтрации, обновление, выбор количества строк и столбцов записей журнала с помощью блока кнопок управления отображением записей журнала (см. Рисунок – Блок кнопок управления отображением записей журнала).

Рисунок – Блок кнопок управления отображением записей журнала

34.1.1 Настройки журналирования событий МЭ

Выбор регистрируемых событий для журналирования межсетевого экрана производится в подразделе журналирования (**«Система» - «Настройки» - «Журналирование»**) (см. Рисунок – Настройка журналирования).

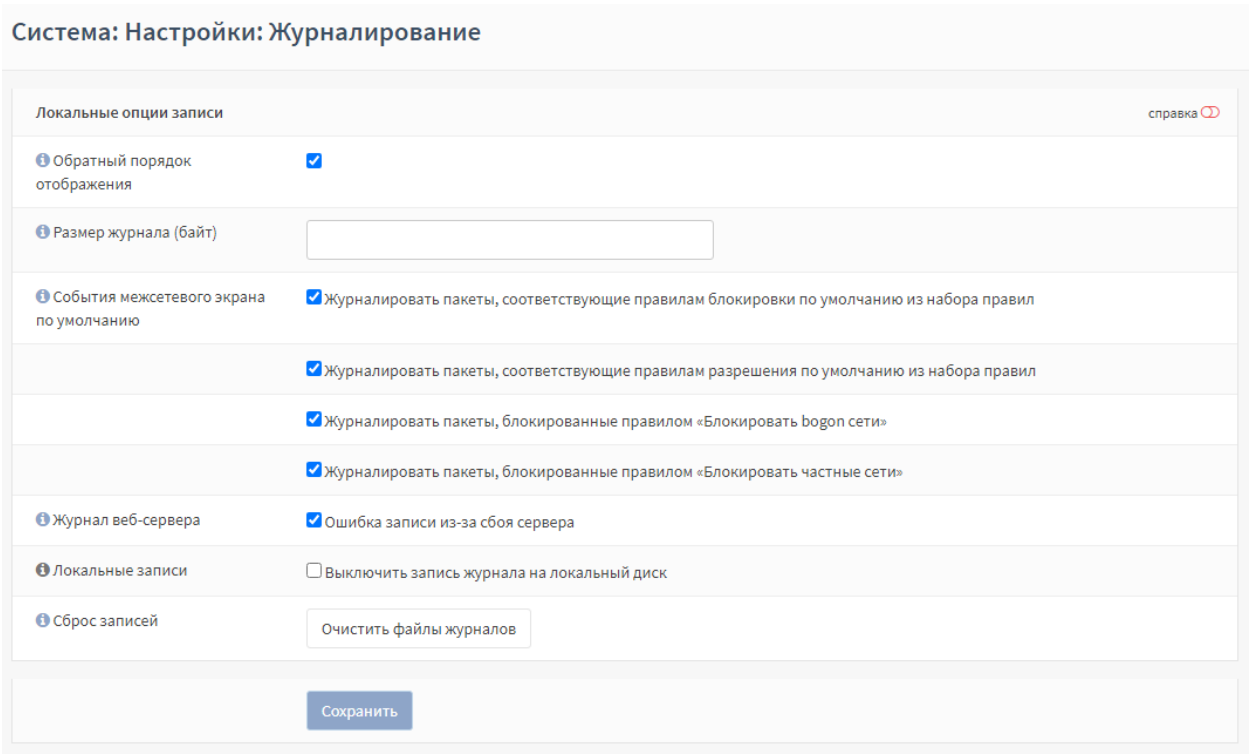


Рисунок – Настройка журналирования

В данном подразделе существует возможность выбрать события, генерируемые **ARMA FW** и подлежащие журналированию.

Выбор событий осуществляется установкой/снятием флажка напротив события, для применения изменения необходимо нажать **кнопку «Сохранить»**. По умолчанию флажки установлены напротив всех событий.

Существует возможность журналировать пакеты, соответствующие правилам МЭ. Для этого необходимо в параметрах создаваемого/созданного правила (см. Создание правил межсетевого экранирования) установить флажок напротив параметра **«Журналирование»** (см. Рисунок – Включение журналирования для правил МЭ).

Примечание:

В случае включения параметра **«Журналирование»** необходимо заполнить поле параметра **«Описание»** для настраиваемого правила МЭ.

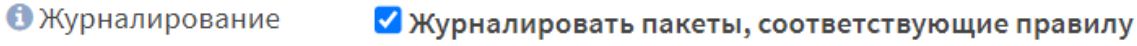


Рисунок – Включение журналирования для правил МЭ

34.1.2 Настройки журналирования действий пользователей

Для включения журналирования действий пользователей необходимо перейти в подраздел администрирования **ARMA FW** (**«Система» - «Настройки» - «Администрирование»**) и поставить флажок в поле **«Журнал доступа»**. Для сохранения изменений необходимо нажать **кнопку «Сохранить»**.

34.2 Журналы МЭ

Журналы МЭ находятся в подразделе журналов МЭ (**«Межсетевой экран» - «Журналы»**).

Журналы МЭ в **ARMA FW** делятся на два вида:

- **«В реальном времени»**;
- **«Открытый вид»**.

Дополнительно присутствует подраздел **«Обзор»**, содержащий в себе различные круговые диаграммы.

34.2.1 Журнал «В реальном времени»

Журнал отображает события МЭ в режиме реального времени в виде списка с динамическим изменением (см. Рисунок – Журнал событий МЭ в реальном времени). Блокированные пакеты выделяются красным цветом, разрешённые – зелёным.

Нажатие **кнопки** «  » напротив записи откроет форму с дополнительной информацией о записи.

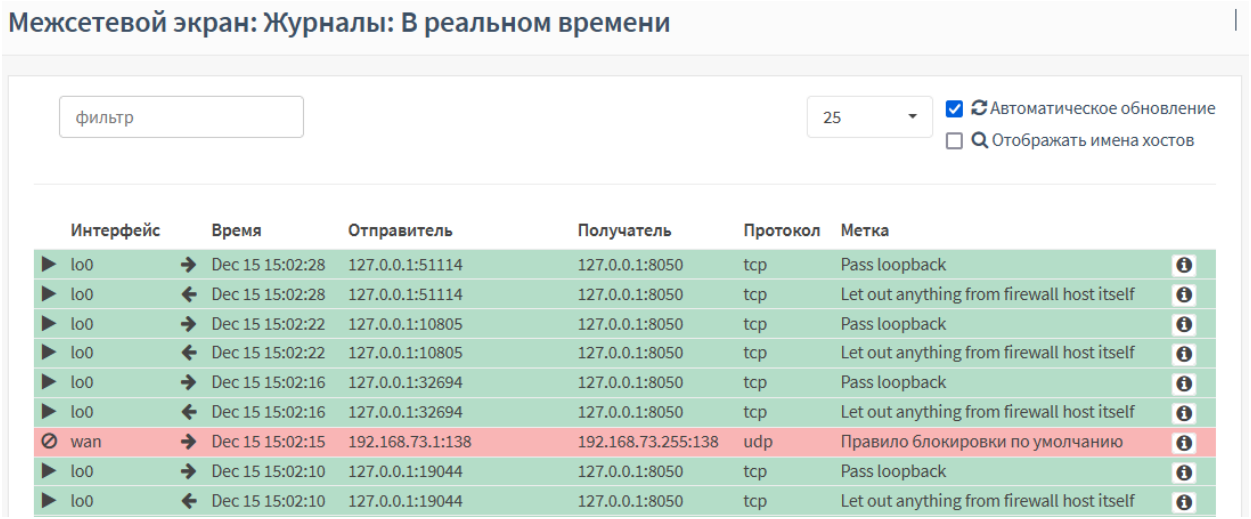


Рисунок – Журнал событий МЭ в реальном времени

34.2.2 Журнал «Открытый вид»

Журнал (см. Рисунок – Журнал событий МЭ, открытый вид) хранит в оригинальном формате, в виде одной текстовой строки, без дополнительной обработки, следующие события МЭ:

- общие правила;
- правила конкретных интерфейсов;
- API правила;
- автоматически генерируемые правила МЭ при включении отдельных опций веб-интерфейса.

При нажатии **кнопки «Очистить журнал»** в нижней части страницы будет предложено удалить весь журнал МЭ.

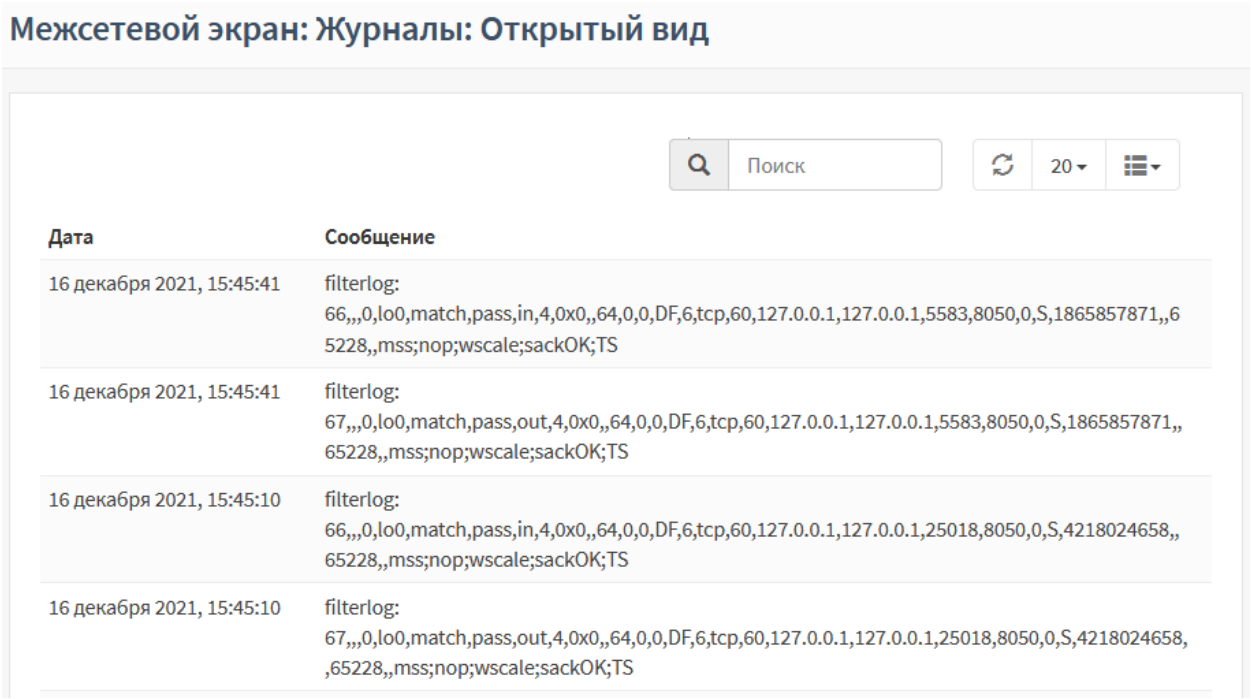


Рисунок – Журнал событий МЭ, открытый вид

34.2.3 Подраздел «Обзор»

Подраздел содержит в себе следующие круговые диаграммы:

- **«Действия»** – отображает процентное соотношение основных действий, которые были применены правилами: «pass» – разрешить / «block» («drop»/«reject») – блокировать;
- **«Интерфейсы»** – отображает процентное соотношение интерфейсов, на которых срабатывали правила. На данной диаграмме возможно проанализировать, на каком интерфейсе правила срабатывают чаще;

- **«Протоколы»** – отображает процентное соотношение протоколов, при работе которых были сработаны правила МЭ: UDP, TCP, ICMP, и т.д.;
- **«IP-адреса источника»** – отображает процентное соотношение IP-адресов, с которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ;
- **«IP-адреса назначения»** – отображает процентное соотношение IP-адресов, для которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ;
- **«Порты источника»** – отображает процентное соотношение портов источников, с которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ;
- **«Порты назначения»** – отображает процентное соотношение портов назначения, для которых отправлялись пакеты, отмеченные в сработавшем правиле МЭ.

34.3 Журналы СОВ

Настройка журналирования СОВ производится в подразделе администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**), вкладка **«Настройки»**.

Имеются 4 параметра для управления журналированием событий СОВ:

- **«Архивировать журнал»** – задаёт периодичность архивирования журналов предупреждений СОВ, по умолчанию – каждое воскресенье в 23:00;
- **«Сохранить журналы»** – указывает количество файлов журналов СОВ, хранящихся в **ARMA FW**;
- **«Содержимое пакета для журнала»** – добавляет в журнал полезную нагрузку пакета трафика;
- **«Журналировать пакет»** – добавляет в журнал весь пакет трафика.

Параметры **«Содержимое пакета для журнала»** и **«Журналировать пакет»** доступны при переключении выключателя **«расширенный режим»**.

Для СОВ предусмотрено два журнала:

- **«Журнал работы СОВ»**;
- **«Журнал ошибок работы сигнатур СОВ»**.

34.3.1 Журнал ошибок работы сигнатур СОВ

Журнал (см. Рисунок – Журнал ошибок работы сигнатур СОВ) расположен на вкладке **«Журналирование»** подраздела администрирования СОВ (**«Обнаружение вторжений» - «Администрирование»**) и разделён на две части:

- **«Журнал СОВ»** – хранит записи, содержащие ошибки и предупреждения ПО «Suricata» о невозможности запустить или включить какие-либо сигнатуры с указанием причины;
- **«Журнал загрузки правил»** – хранит записи, содержащие ошибки и предупреждения загрузки правил СОВ.

Переключение происходит в выпадающем списке в верхней части формы подраздела. Также в верхней части формы подраздела находятся форма поиска и выпадающий список выбора уровня сообщений.

При нажатии **кнопки «Очистить журнал»** в нижней части формы будет предложено удалить весь журнал МЭ.

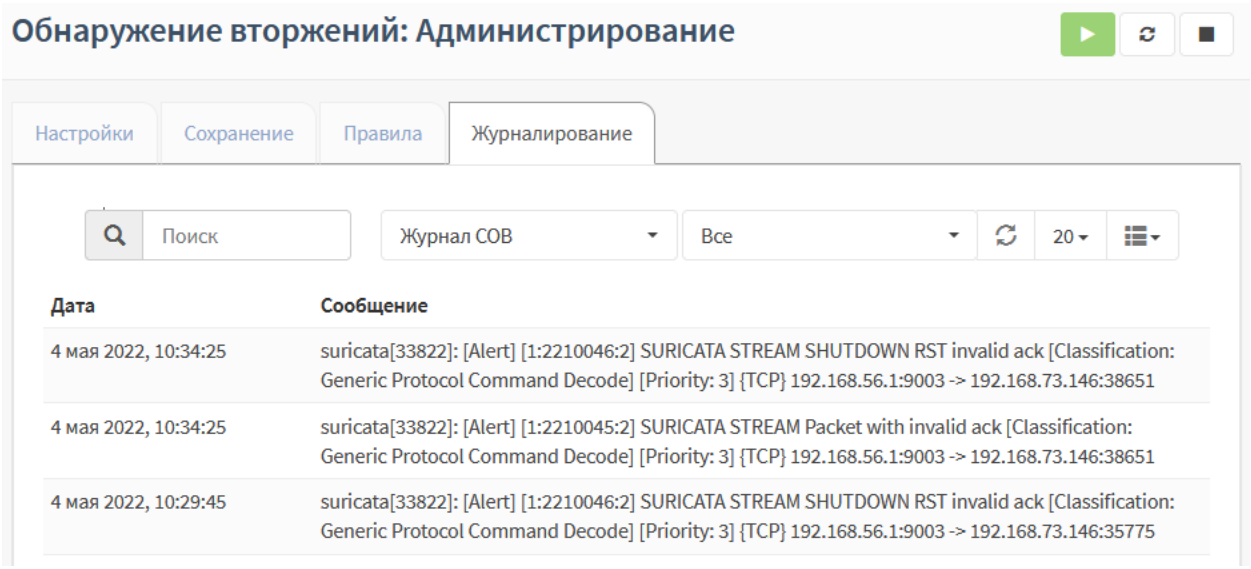
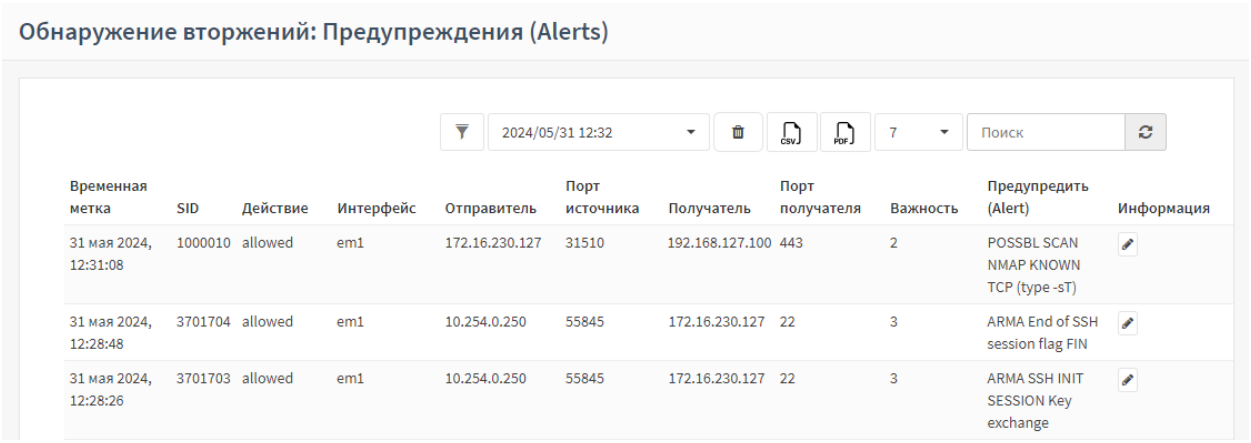


Рисунок – Журнал ошибок работы сигнатур СОВ

34.3.2 Журнал предупреждений СОВ

Журнал (см. Рисунок – Журнал предупреждений СОВ) хранит записи о срабатывании правилах СОВ. Журнал расположен в подразделе предупреждений СОВ (**«Обнаружение вторжений» - «Предупреждения (Alerts)»**).



Временная метка	SID	Действие	Интерфейс	Отправитель	Порт источника	Получатель	Порт получателя	Важность	Предупредить (Alert)	Информация
31 мая 2024, 12:31:08	1000010	allowed	em1	172.16.230.127	31510	192.168.127.100	443	2	POSSBL SCAN NMAP KNOWN TCP (type -sT)	
31 мая 2024, 12:28:48	3701704	allowed	em1	10.254.0.250	55845	172.16.230.127	22	3	ARMA End of SSH session flag FIN	
31 мая 2024, 12:28:26	3701703	allowed	em1	10.254.0.250	55845	172.16.230.127	22	3	ARMA SSH INIT SESSION Key exchange	

Рисунок – Журнал предупреждений СОВ

При нажатии **кнопки** « », напротив сообщения о срабатывании правила СОВ, появится информационное окно (см. Рисунок – Информация о предупреждении).

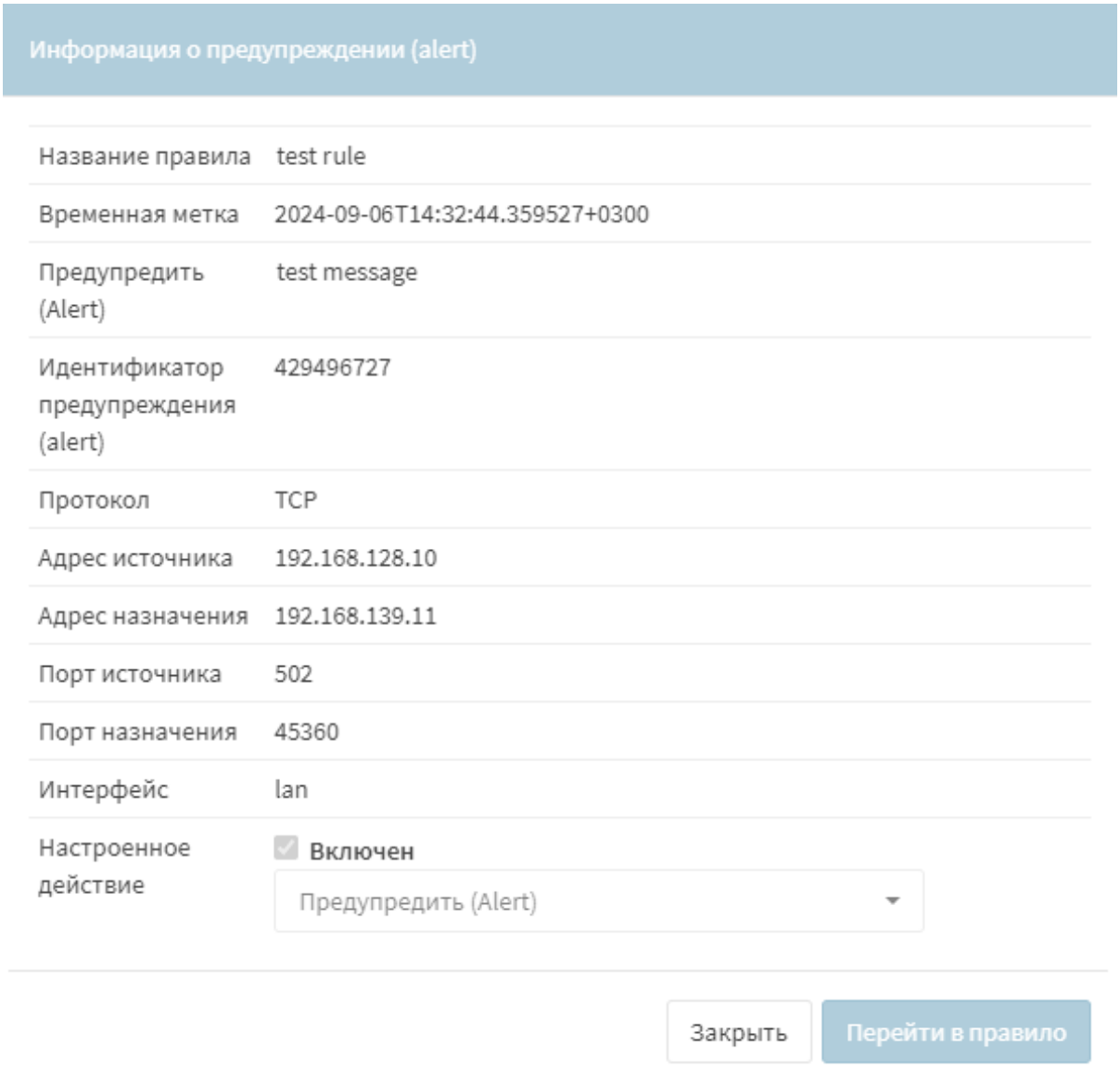


Рисунок – Информация о предупреждении

В информационном окне, сработавшего пользовательского правила СОВ, дополнительно отображается **кнопка «Перейти в правило»**, нажатием на которую возможно выполнить переход к форме редактирования правила.

34.3.2.1 Экспорт журнала предупреждений СОВ

В случае необходимости экспорта журнала предупреждений СОВ следует в зависимости от требуемого формата:

- нажать **кнопку** «  » – для экспорта файла с расширением **«csv»**;
- нажать **кнопку** «  » – для экспорта файла с расширением **«pdf»**, содержащегося в архиве с расширением **«zip»**.

Для корректного отображения журнала с расширением **«csv»** в «MS Office Excel» следует импортировать журнал в качестве внешних данных из текста, указывая формат файла **«65001 : Юникод (UTF-8)»** и разделитель **«точка с запятой»**.

34.4 Системные журналы

Системные журналы располагаются в подразделе журналирования (**«Система» - «Журналы»**). Всего в подразделе содержится 6 журналов:

- **«Журнал Syslog»**;
- **«Backend журнал»**;
- **«Журнал веб-интерфейса»**;
- **«Журнал событий безопасности»**;
- **«Журнал системных событий»**;
- **«Журнал действий пользователя»**.

34.4.1 Журнал syslog

Журнал (см. Рисунок – Журнал Syslog) хранит записи, содержащие события следующих типов:

- успешность входа в систему;
- изменение внутреннего представления времени;
- изменение пароля пользователя;
- изменение настроек системы;
- добавление, изменение, удаление и получение информации об элементах системы – пользователях, правил МЭ, правил и групп правил СОВ;
- уведомления об отказе модулей;
- успешность доступа пользователей к различным страницам системы;

- сообщения от syslog-парсеров;
- сообщения, связанные с активацией или проверкой лицензии.

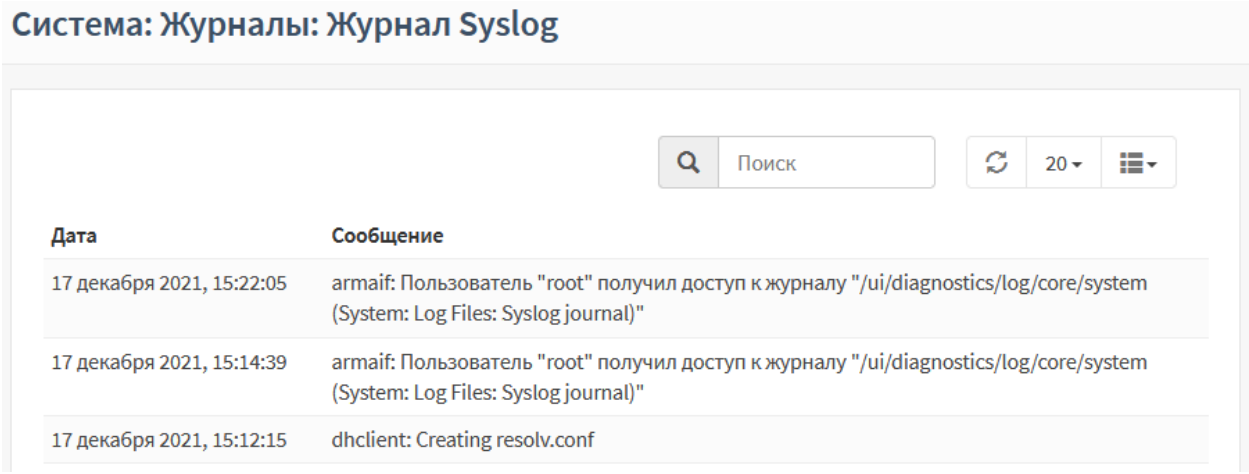


Рисунок – Журнал Syslog

34.4.2 Backend журнал

Журнал (см. Рисунок – Backend журнал) хранит записи, содержащие события следующих типов:

- сгенерированные за счёт использования API сервера – перезагрузка, остановка, запуск сервисов;
- изменение конфигурации – генерирование конфигураций сервисов при сохранении форм.

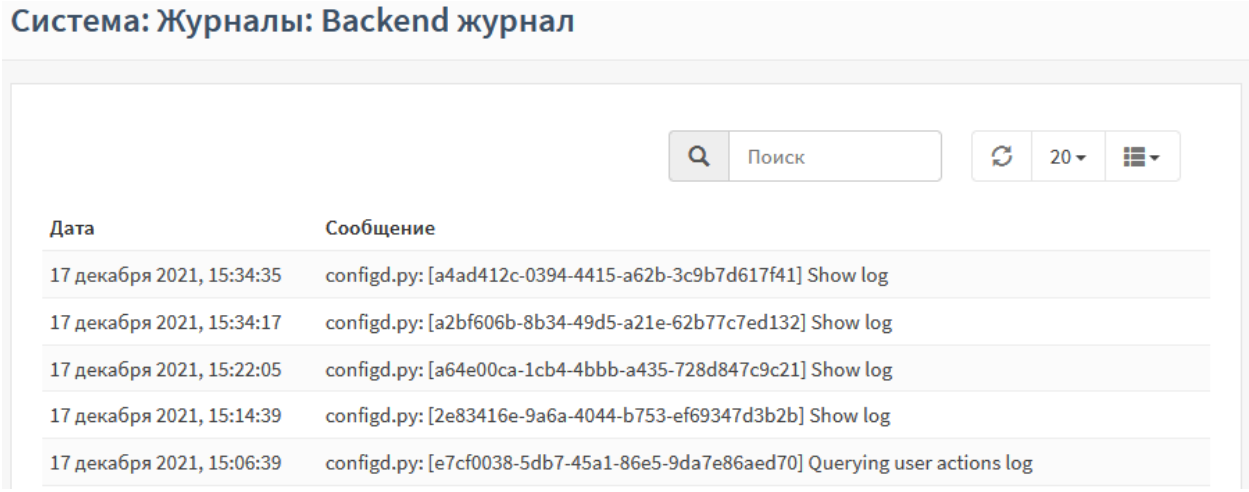


Рисунок – Backend журнал

34.4.3 Журнал веб-интерфейса

Журнал (см. Рисунок – Журнал веб-интерфейса) хранит записи, содержащие события веб-сервера «lighttpd».

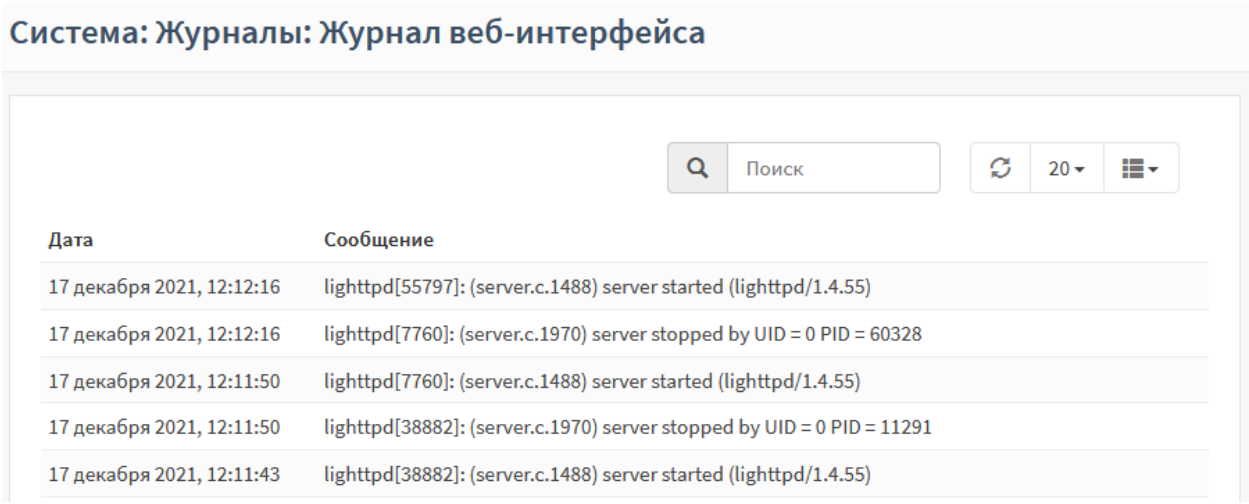


Рисунок – Журнал веб-интерфейса

34.4.4 Журнал событий безопасности

Журнал (см. Рисунок – Журнал событий безопасности) хранит записи, содержащие события следующих типов:

- для СОВ – срабатывание сигнатур;
- для МЭ – срабатывания правил межсетевого экрана;
- для arpwatch:
  - подключение несанкционированного устройства;
  - обнаружение конфликта IP-адресов;
  - обнаружение изменения IP, MAC-адреса;
  - обнаружение подмены IP-адресов;
- для портала авторизации – запуск/остановка/перезагрузка портала авторизации и лог-файлы с записями о событиях в хронологическом порядке.

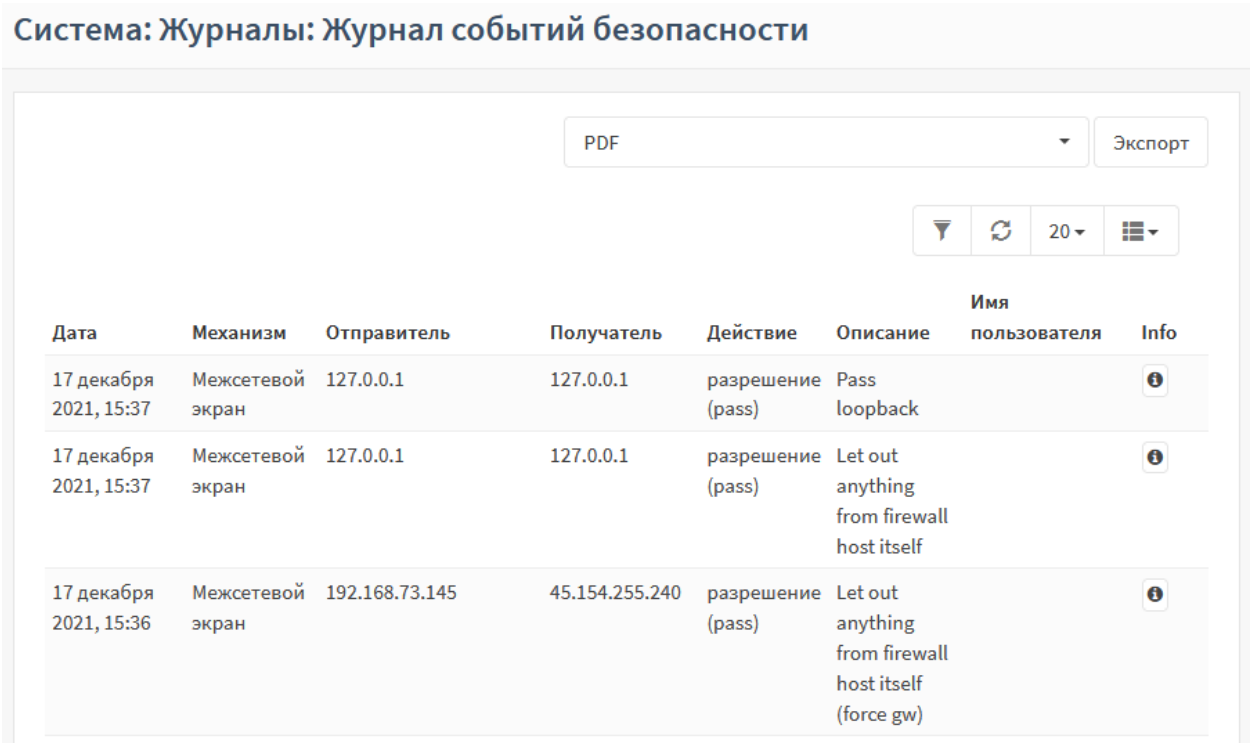


Рисунок – Журнал событий безопасности

Нажатие **кнопки** « » напротив записи откроет форму с дополнительной информацией о записи.

Для экспорта журнала необходимо в верхней части страницы выбрать формат файла и нажать **кнопку «Экспорт»**.

34.4.4.1 Фильтры журнала событий безопасности

В журнале событий безопасности поддерживается возможность фильтрации отображаемых записей.

При нажатии **кнопки** « » дополнительно появятся поля для ввода значений следующих фильтров:

- **«Диапазон дат»**;
- **«Поиск»**;
- **«Механизм»**;
- **«Отправитель»**;
- **«Получатель»**;
- **«Действие»**;
- **«Описание»**;
- **«Имя пользователя»**.

Для настройки фильтра **«Поиск»** необходимо ввести в поле данного фильтра искомое значение и нажать **кнопку «Применить»**.

В журнале будут отображены записи, содержащие информацию, соответствующую искомому значению (см. Рисунок – Фильтр «Поиск»).

Примечание:

Фильтрация выполняется по данным, отображаемым в форме с дополнительной информацией.

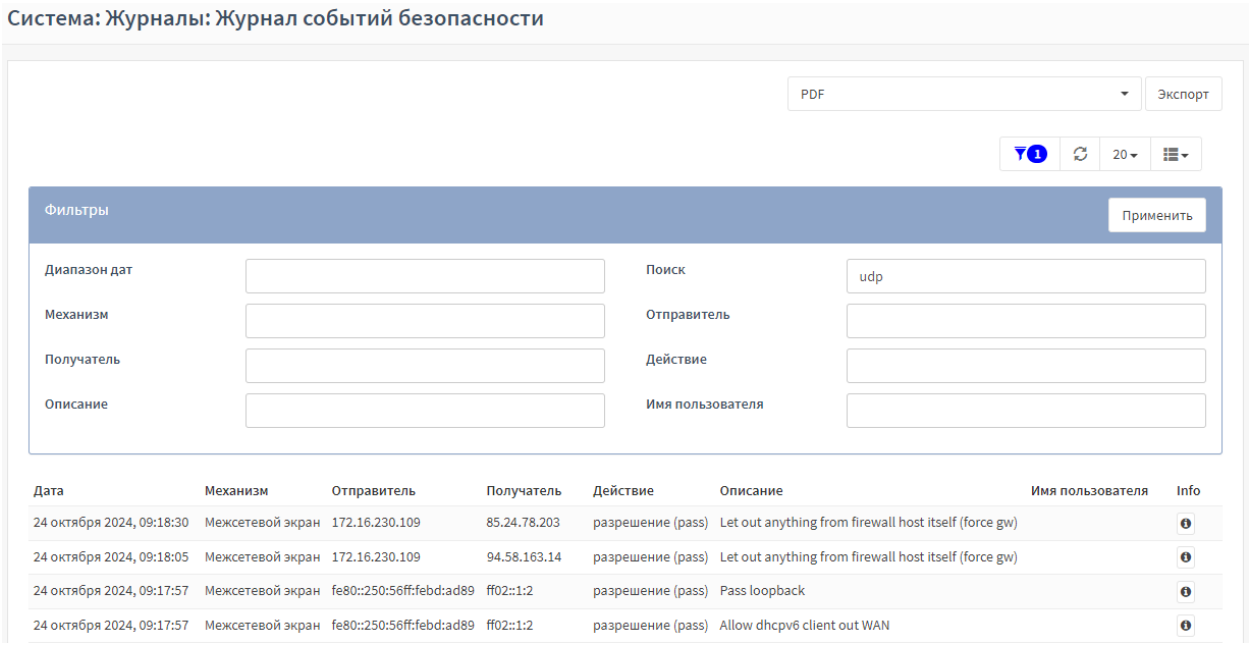


Рисунок – Фильтр «Поиск»

Для очистки фильтра **«Поиск»** необходимо удалить значение из поля данного фильтра и нажать **кнопку «Применить»**.

Фильтры **«Механизм»**, **«Отправитель»**, **«Получатель»**, **«Действие»**, **«Описание»**, **«Имя пользователя»** позволяют отобразить записи событий, информация о которых в соответствующих столбцах, будет содержать искомое значение.

Настройка данных фильтров выполняется аналогично настройке фильтра **«Поиск»** (см. Рисунок – Фильтр «Отправитель»).

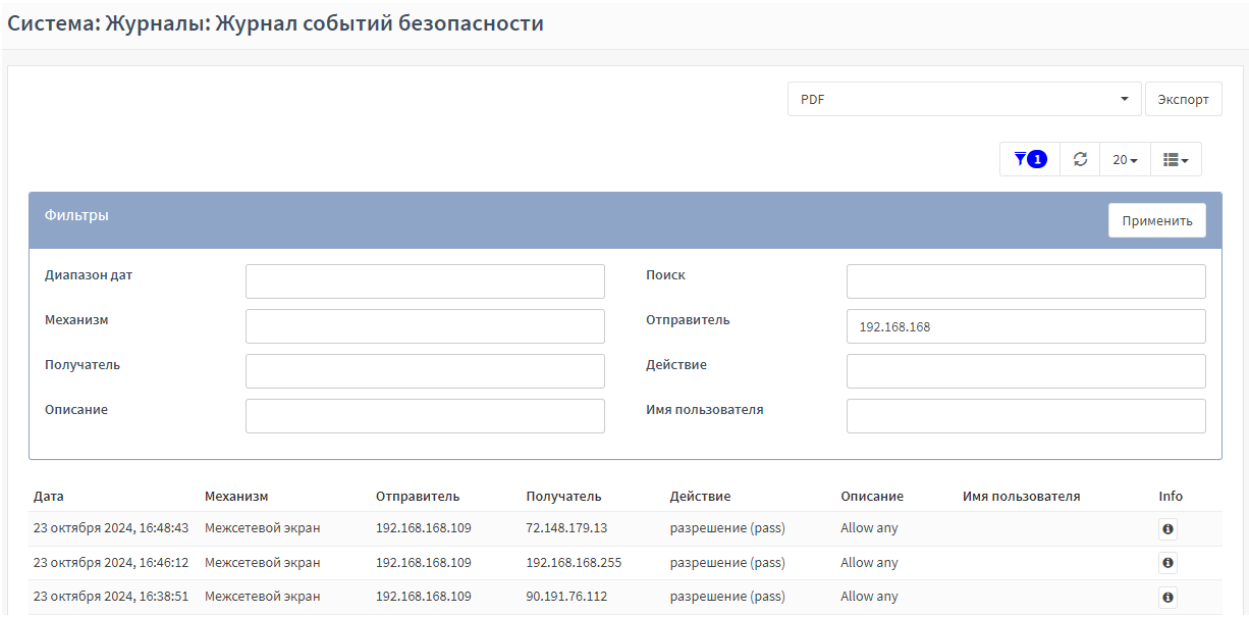


Рисунок – Фильтр «Отправитель»

34.4.4.1.1 Фильтр «Диапазон дат»

Фильтр **«Диапазон дат»** позволяет отобразить записи в журнале событий безопасности за определённый промежуток времени.

Для настройки фильтра **«Диапазон дат»** необходимо выполнить следующие действия:

1. Нажать ЛКМ на поле фильтра **«Диапазон дат»**.
2. В появившейся форме нажать на начальную и конечную даты, указать значения времени и нажать **кнопку «Применить»** (см. Рисунок – Фильтр «Диапазон дат»).

Примечание:

В фильтре поддерживается указание минут значением, кратным «5».

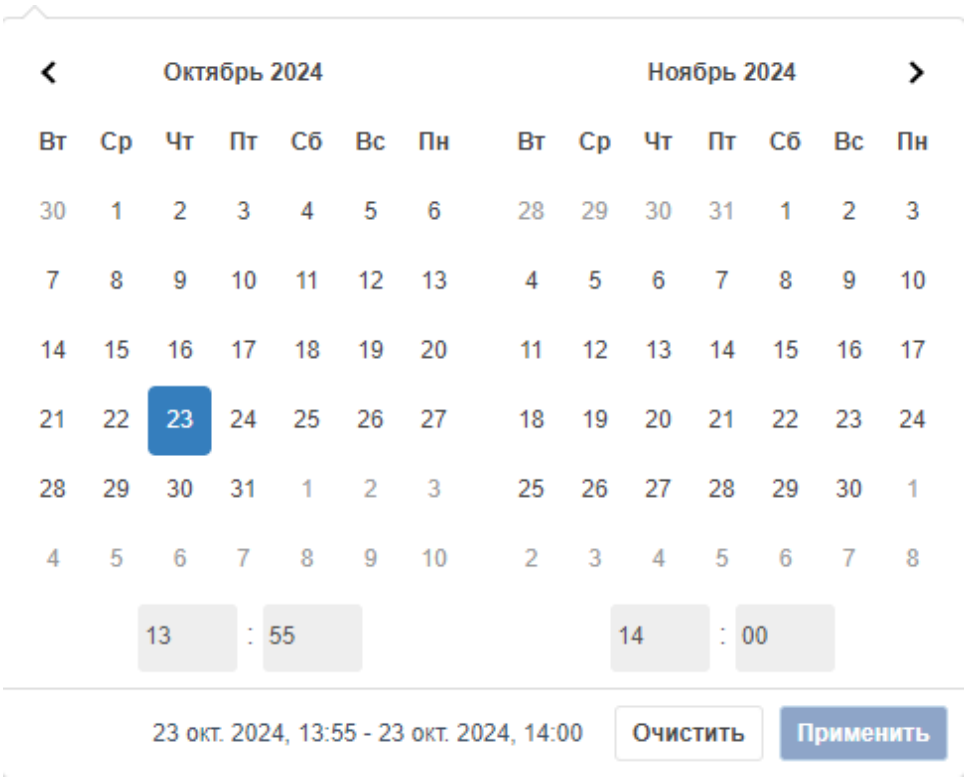


Рисунок – Фильтр «Диапазон дат»

3. Затем нажать **кнопку «Применить»** (см. Рисунок – Фильтры журнала событий безопасности).

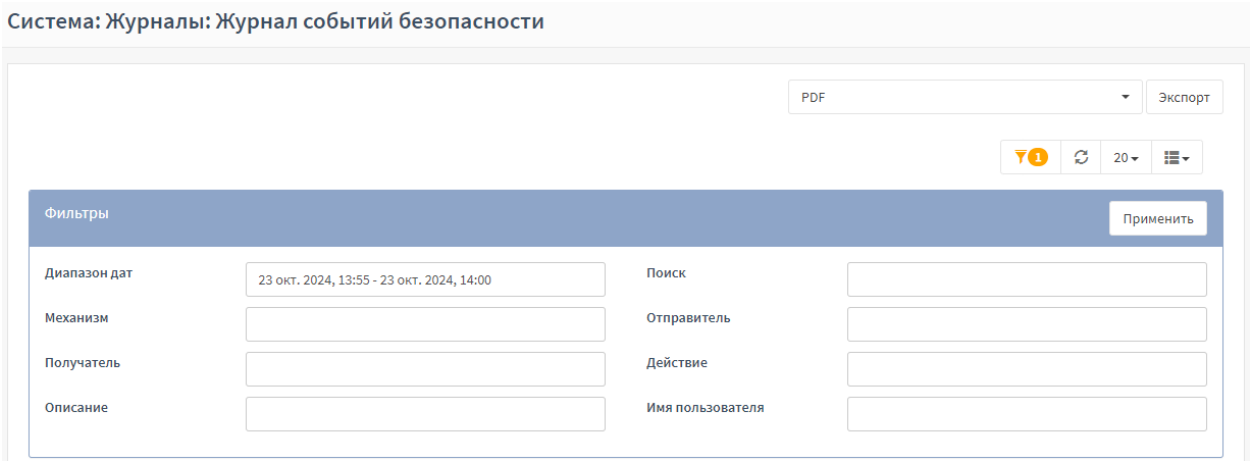


Рисунок – Фильтры журнала событий безопасности

Для очистки поля фильтра **«Диапазон дат»** необходимо нажать ЛКМ на поле фильтра **«Диапазон дат»**, нажать в появившейся форме **кнопку «Очистить»** и нажать **кнопку «Применить»**.

34.4.5 Журнал системных событий

Журнал (см. Рисунок – Журнал системных событий) хранит записи, содержащие события следующих типов:

- NTP-сервер:

- запуск, остановка или перезагрузка сервера;
- успешная синхронизация времени;
- отсутствие подключение к NTP-серверу;

- сбой портала авторизации – неуспешная попытка входа в портал авторизации;
- СОВ:
  - запуск, остановка или перезагрузка СОВ;
  - сбой СОВ;
- события, связанные с состоянием интерфейса CARP;
- события контроля целостности;
- запуск веб-сервера;
- неуспешный доступ к странице веб-интерфейса;
- сообщения при загрузке системы.

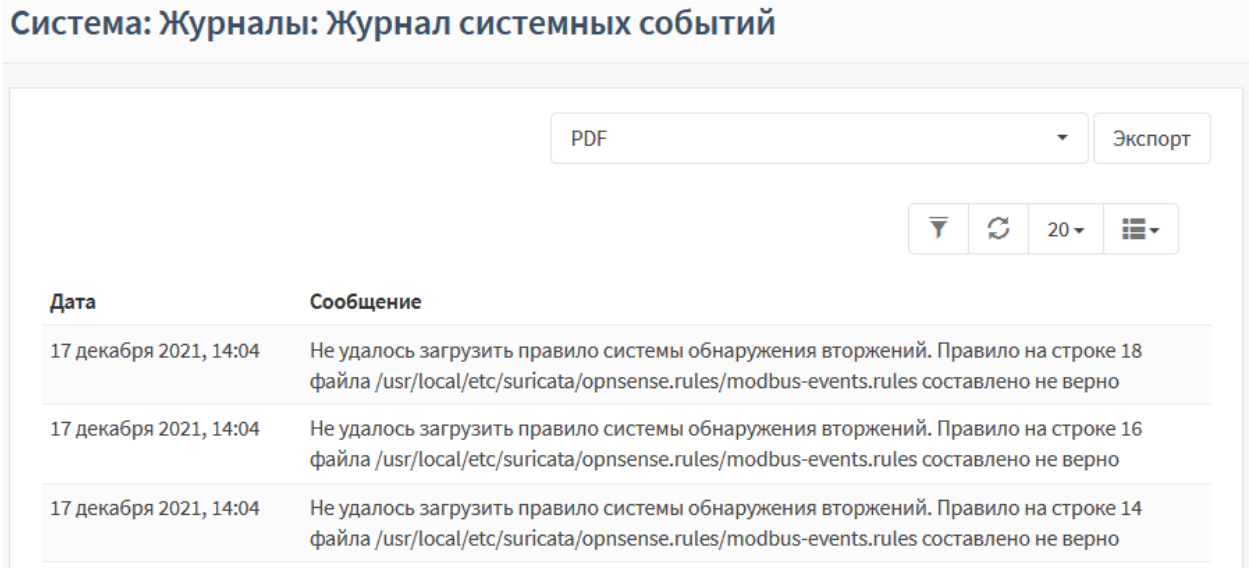


Рисунок – Журнал системных событий

Для экспорта журнала необходимо в верхней части страницы выбрать формат файла и нажать **кнопку «Экспорт»**.

34.4.6 Журнал действий пользователя

Журнал (см. Рисунок – Журнал действий пользователя) хранит записи, содержащие события следующих типов:

- включение/отключение МЭ;
- включение/отключение СОВ;
- добавление/изменение/удаление правил МЭ;

- изменение настроек МЭ;
- изменение правил СОВ;
- изменение настроек СОВ;
- успешная/неуспешная авторизация в граф. интерфейс и интерфейс консоли;
- изменение размера записей в webgui журнале;
- сообщения при работе с пользователями и группами пользователей;
- сообщения, связанные с изменением настроек мониторинга состояния системы на странице анализа трафика, настроек monit;
- перезагрузка системы;
- информация о нештатном завершении работы системы.

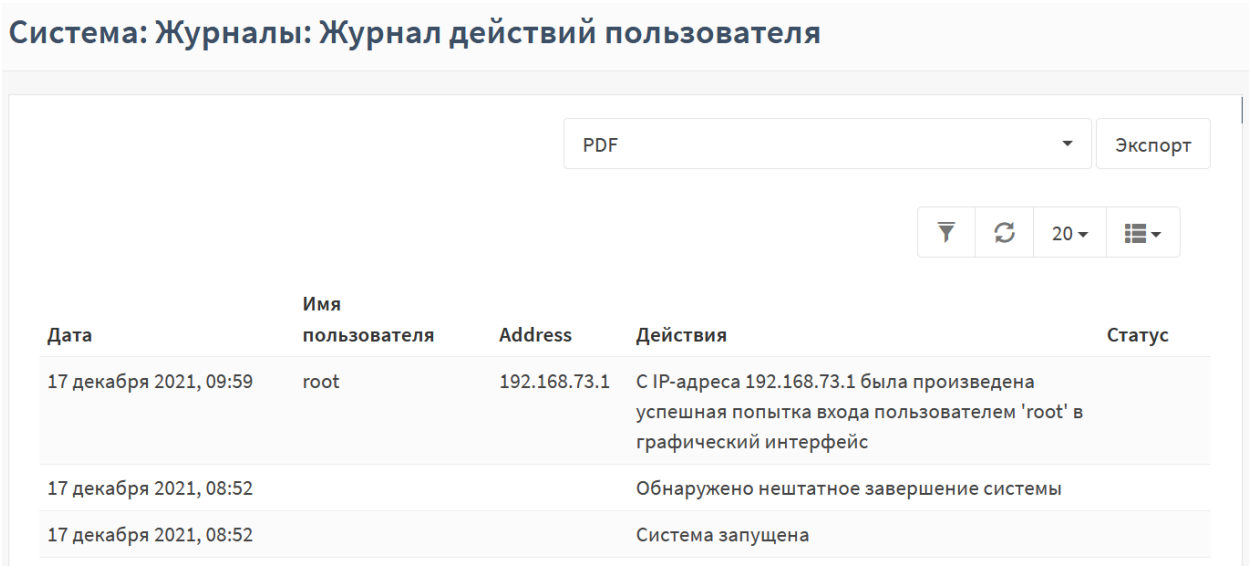


Рисунок – Журнал действий пользователя

Для экспорта журнала необходимо в верхней части страницы выбрать формат файла и нажать **кнопку «Экспорт»**.

34.5 Журналы маршрутизации

Журналы маршрутизации делятся на два типа:

- **«Журнал статической маршрутизации»**;
- **«Журнал динамической маршрутизации»**.

34.5.1 Журнал статической маршрутизации

Журнал (см. Рисунок – Журнал статической маршрутизации) хранит записи, содержащие сообщения от протоколов маршрутизации ZEBRA, OSPF/OSPF6, RIP, a

также от других сервисов, работающих со статическими маршрутами сети, например, radvd и rtsold.

Журнал расположен в подразделе журналирования маршрутизации (**«Система» - «Маршруты» - «Журнал»**).

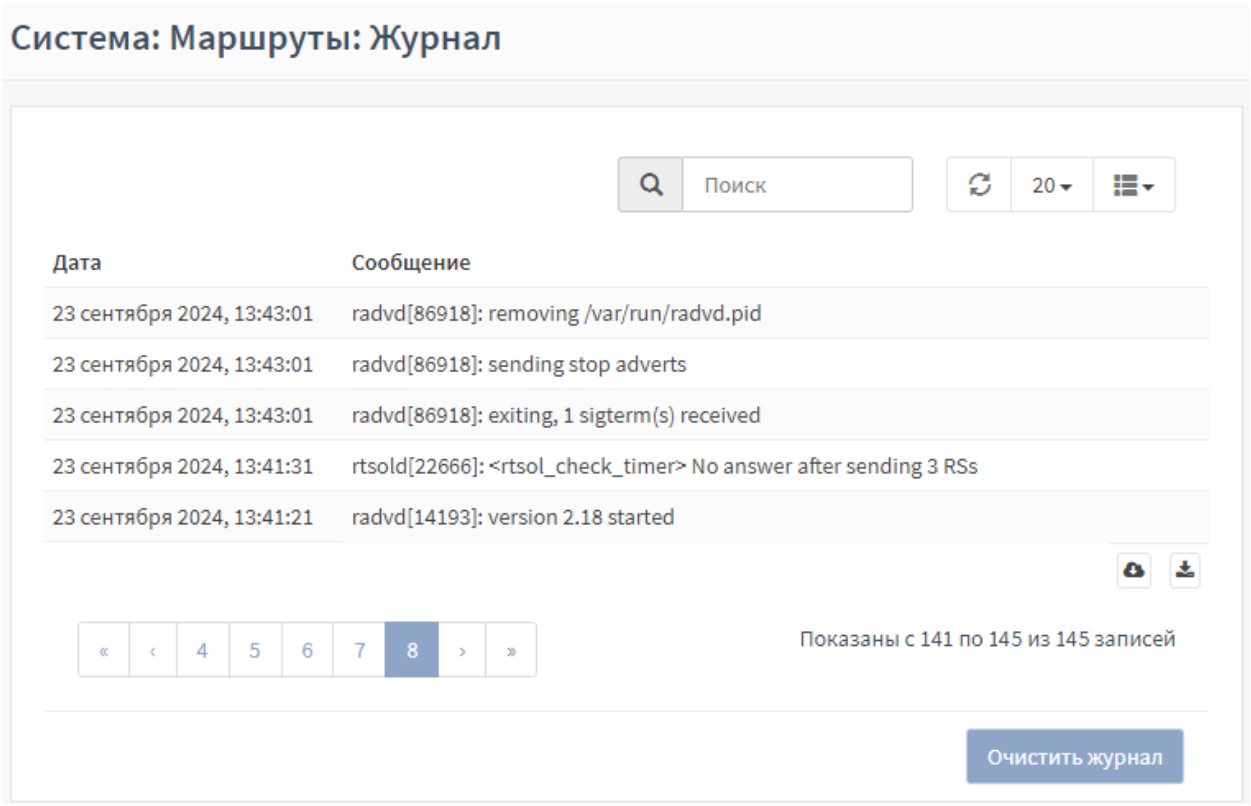


Рисунок – Журнал статической маршрутизации

34.5.2 Журнал динамической маршрутизации

Основой работы данного журнала является ПО Quagga. По умолчанию ведение данного журнала выключено.

Журнал (см. Рисунок – Журнал динамической маршрутизации) хранит записи, содержащие сообщения от протоколов маршрутизации ZEBRA, OSPF/OSPF6, RIP, задействованных в процессе динамической маршрутизации, следующих типов:

- hello-сообщения от ZEBRA и другие сообщения протокола ZEBRA;
- сообщения от OSPF/OSPF6;
- сообщения от протокола RIP;
- ошибки конфигурации протоколов динамической маршрутизации;
- запуск, остановка или перезагрузка сервиса quagga (frr).

Журнал расположен в подразделе журналирования маршрутизации (**«Маршрутизация» - «Диагностика» - «Журналирование»**).

Для включения наполнения журнала необходимо перейти в подраздел общих настроек маршрутизации (**«Маршрутизация» - «Общие настройки»**), установить флажки для параметров **«Включить»** и **«Создание файла журнала»** и нажать **кнопку «Сохранить»**.

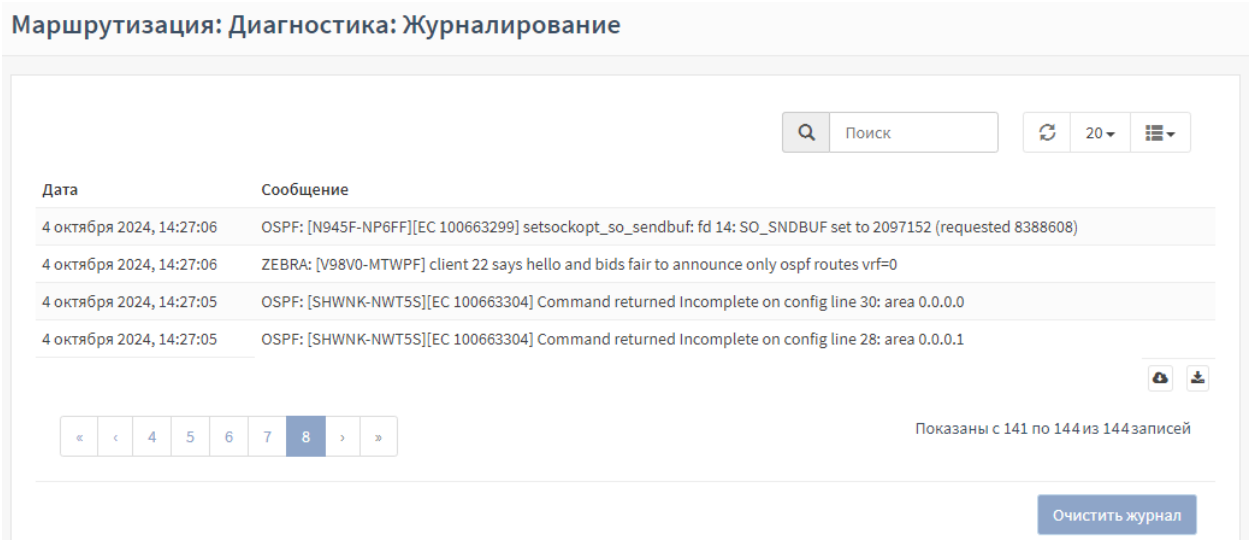


Рисунок – Журнал динамической маршрутизации

34.6 Журнал портала авторизации

Журнал (см. Рисунок – Журнал портала авторизации) хранит записи, содержащие информацию о работе сервиса Captive Portal, отвечающего за работу портала авторизации. В журнале представлены следующие типы событий:

- сообщение об отсутствии у пользователя доступа к определённому URL;
- запуск, остановка или перезагрузка сервиса;
- ошибки сервиса.

Журнал расположен в подразделе журналирования портала авторизации (**«Службы» - «Портал авторизации» - «Журнал»**).

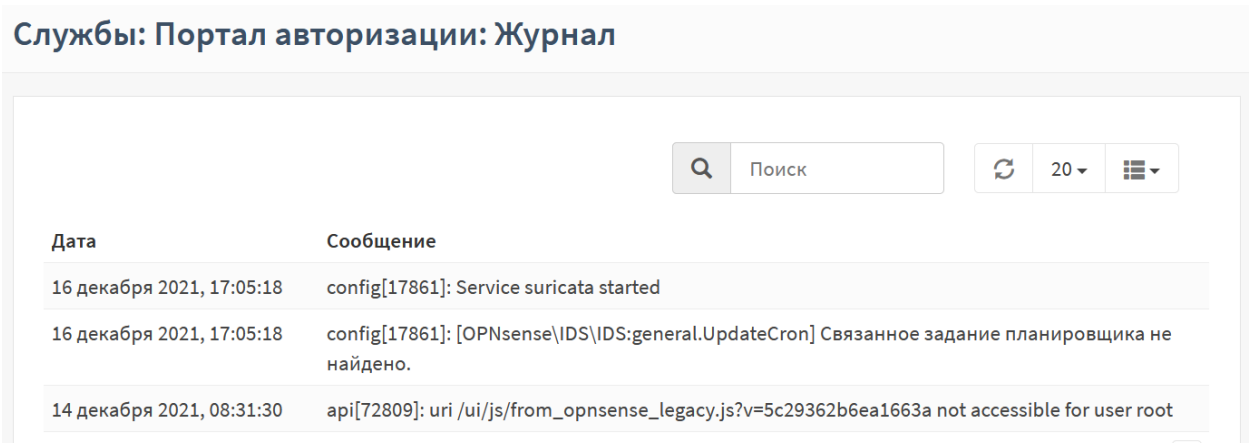


Рисунок – Журнал портала авторизации

34.7 Журнал DHCPv4

Журнал (см. Рисунок – Журнал DHCPv4) хранит записи, содержащие события о работе DHCP-сервера на сетевых интерфейсах следующих типов:

- включение DHCP-сервера на интерфейсе;
- назначение IP-адреса устройству в сети.

Журнал расположен в подразделе журналирования DHCP (**«Службы» - «DHCPv4» - «Журнал»**).

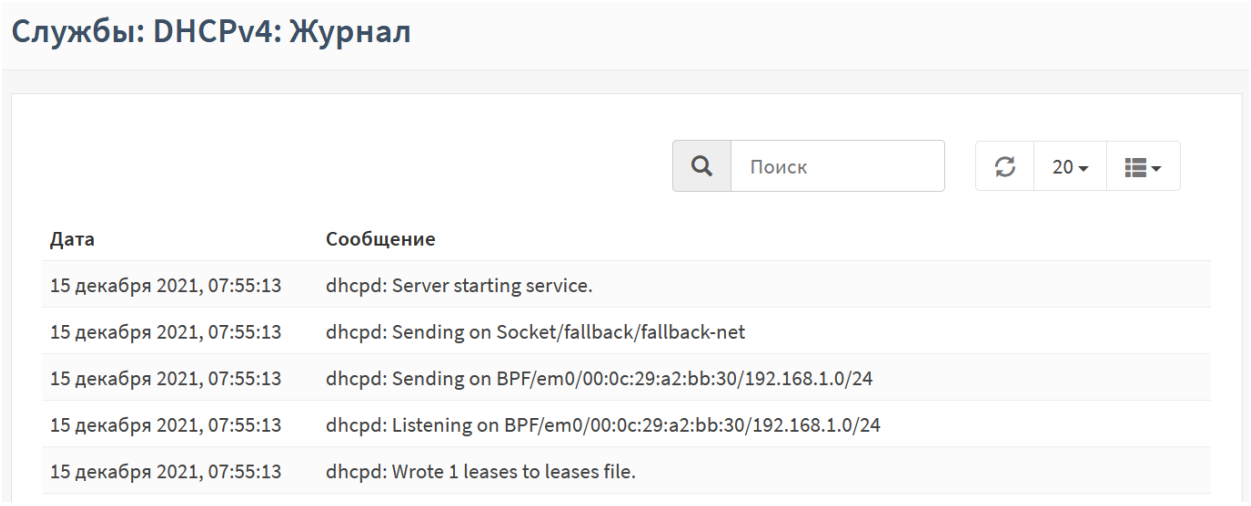


Рисунок – Журнал DHCPv4

34.8 Журнал NTP

Журнал (см. Рисунок – Журнал сетевого времени) хранит записи, содержащие события о работе сервиса NTP следующих типов:

- запуск, остановка или перезагрузка сервиса;
- ошибки сервиса;
- успешность синхронизации времени.

Журнал расположен в подразделе журналирования сетевого времени (**«Службы» - «Сетевое время» - «Журнал»**).

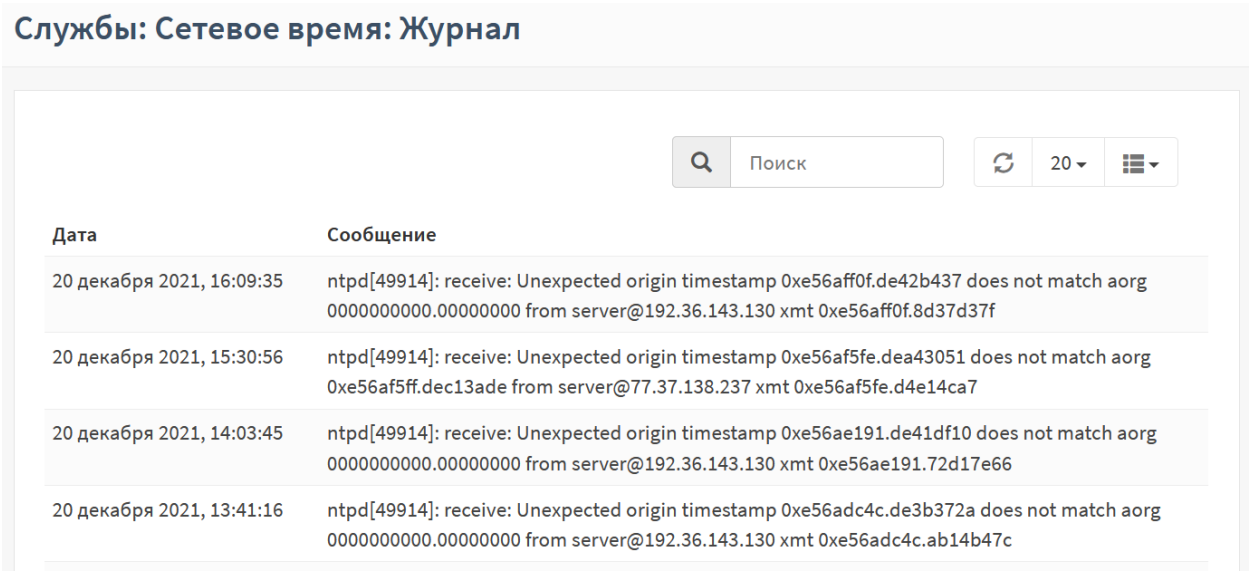


Рисунок – Журнал сетевого времени

34.9 Журнал веб-прокси

Журналы веб-прокси делятся на три типа:

- **«Журнал кэша»**;
- **«Журнал доступа»**;
- **«Журнал хранения»**.

34.9.1 Журнал кэша

Журнал (см. Рисунок – Журнал кэша) хранит записи, содержащие сообщения отладки и ошибок, генерируемые ПО «Squid».

Журнал расположен в подразделе журналирования прокси-сервера (**«Службы» - «Веб-прокси» - «Журнал кэша»**).

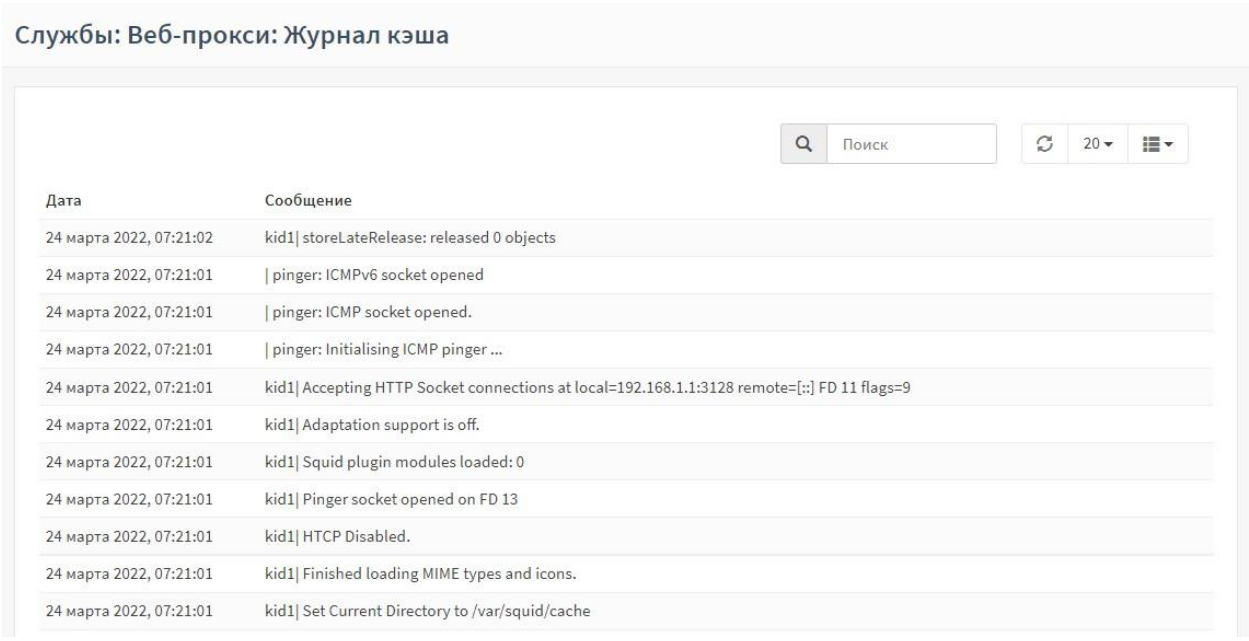


Рисунок – Журнал кэша

34.9.2 Журнал доступа

Журнал (см. Рисунок – Журнал доступа) хранит записи, содержащие сведения о подключениях к веб-прокси.

Журнал расположен в подразделе журналирования прокси-сервера (**«Службы» - «Веб-прокси» - «Журнал доступа»**).

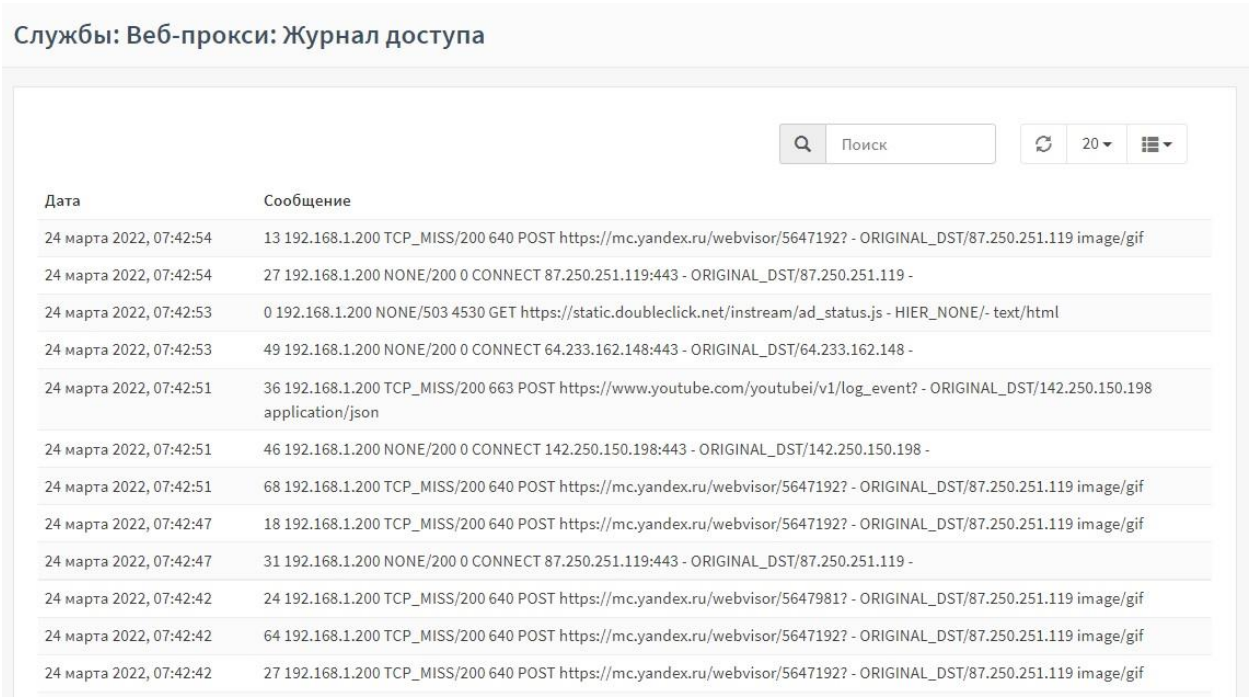


Рисунок – Журнал доступа

34.9.3 Журнал хранения

Журнал (см. Рисунок – Журнал хранения) хранит записи, содержащие информацию об объектах кэша, как хранящихся в данный момент на диске, так и удалённых.

Журнал расположен в подразделе журналирования прокси (**«Службы» - «Веб-прокси» - «Журнал хранения»**).

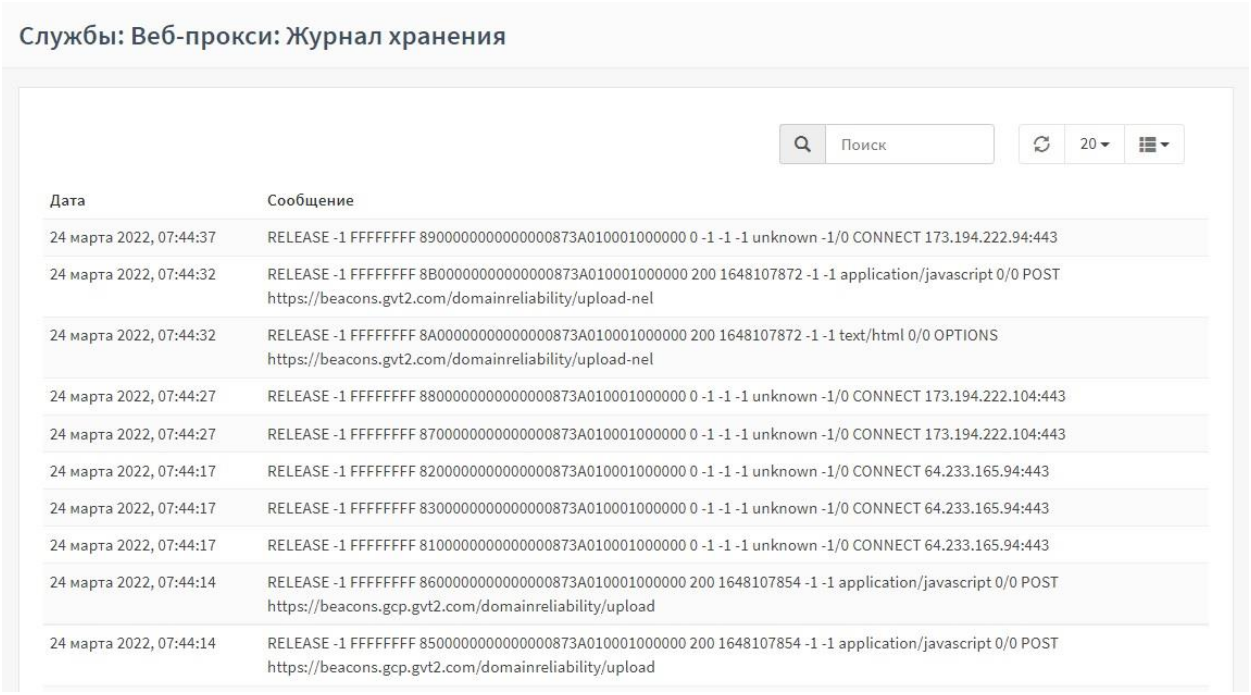


Рисунок – Журнал хранения

34.10 Журнал dnsmasq

Журнал (см. Рисунок – Журнал Dnsmasq DNS) хранит записи, содержащие события работы сервиса dnsmasq следующих типов:

- запуск, остановка и перезагрузка сервиса;
- успешное чтение адресов из каталогов:
  - «/etc/hosts»;
  - «var/etc/dnsmasq-hosts»;
- успешное чтение конфигурации из каталога «/etc/resolv.conf»;
- используемые пространства имен.

Журнал расположен в подразделе журналирования dnsmasq (**«Службы» - «Dnsmasq DNS» - «Журнал»**).

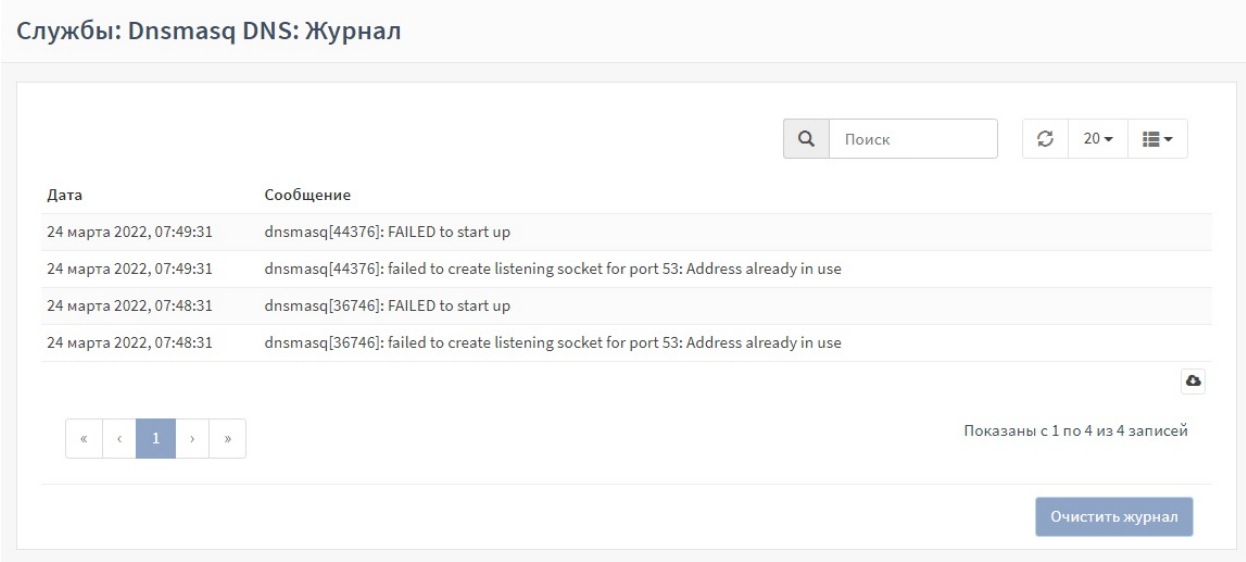


Рисунок – Журнал Dnsmasq DNS

34.11 Журнал ICAPD

Журнал (см. Рисунок – Журнал ICAPD) хранит записи, содержащие события работы сервера по протоколу ICAP.

Типы событий, содержащихся в журнале:

- ошибки сервера;
- запуск, остановка или перезагрузка сервера;
- обнаружение вируса.

Журнал расположен в подразделе журналирования Dr.Web (**«Службы» - «Dr.Web» - «Журнал ICAPD»**).

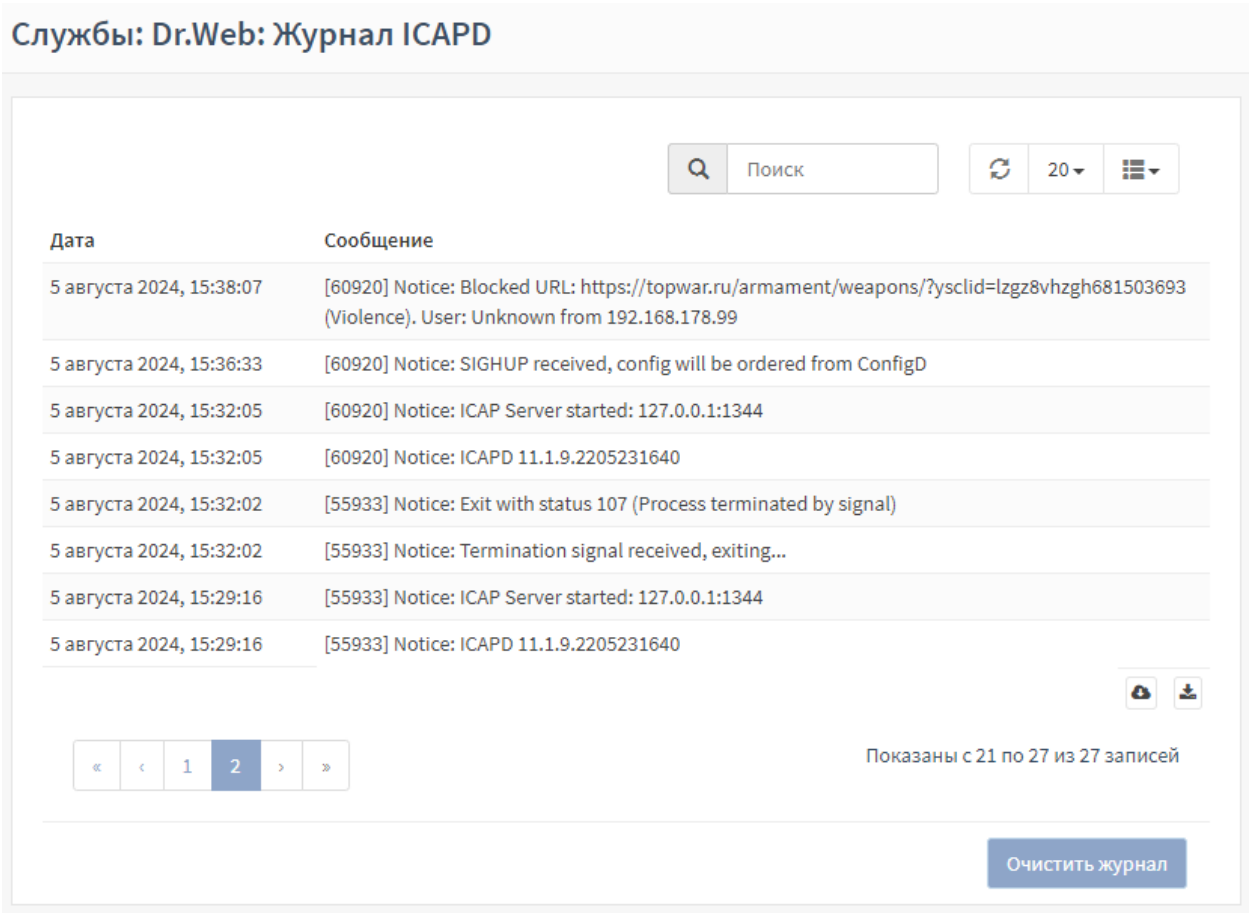


Рисунок – Журнал ICAPD

34.12 Журнал кэширующего DNS

Журнал (см. Рисунок – Журнал кэширующего DNS) хранит записи, содержащие события работы DNS-сервера следующих типов:

- запуск, остановка и перезагрузка сервера;
- общие сведения о кэшировании и рекурсии на сервере.

Журнал расположен в подразделе журналирования DNS (**«Службы» - «Кэширующий DNS-сервер» - «Журнал»**).

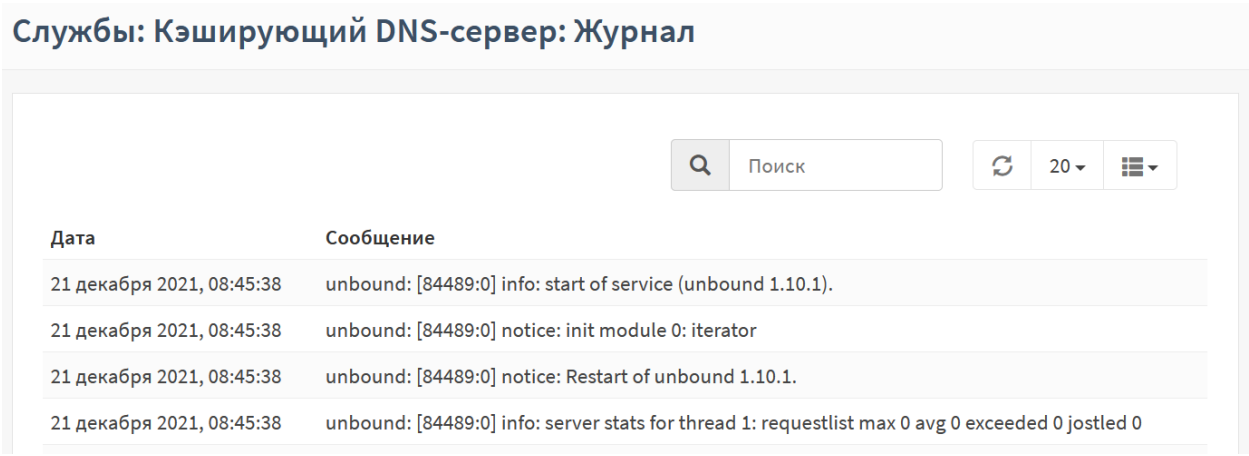


Рисунок – Журнал кэширующего DNS

34.13 Журнал RSPAN

Журнал (см. Рисунок – Журнал RSPAN) хранит записи, содержащие события работы RSPAN.

Журнал расположен в подразделе журналирования RSPAN (**«Службы» - «RSPAN» - «Журналирование»**).

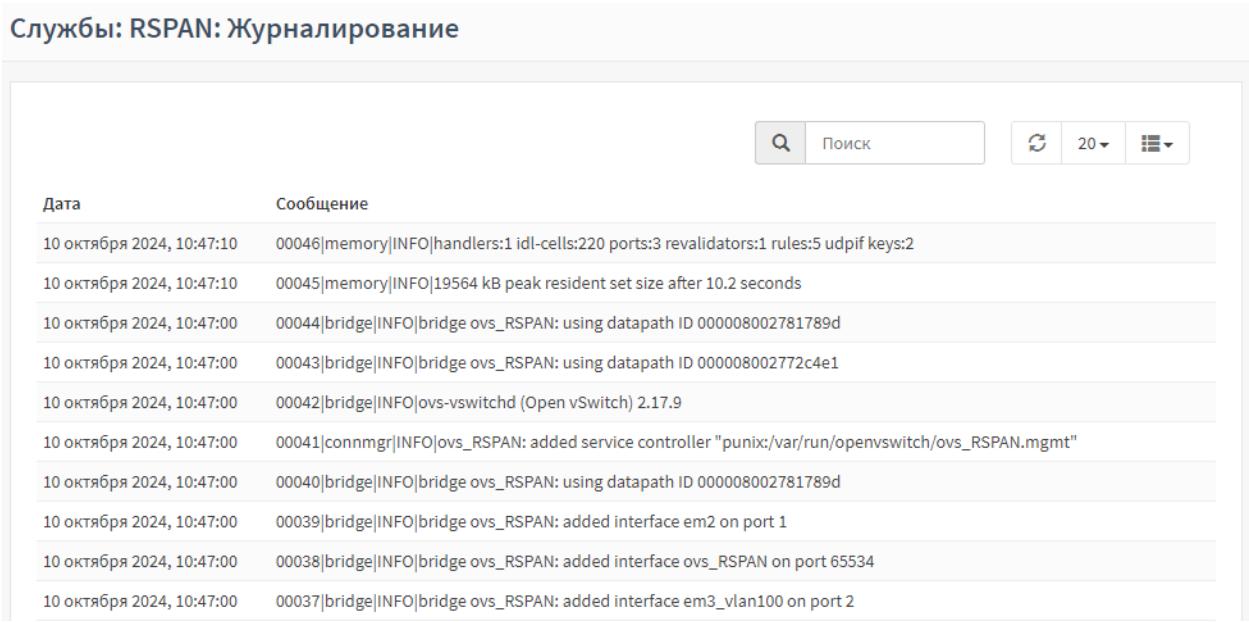


Рисунок – Журнал RSPAN

34.14 Журнал IPsec

Журнал (см. Рисунок – Журнал IPsec) хранит записи, содержащие события работы протокола IPsec VPN следующих типов:

- подключение нового клиента к туннелю:
  - IP-адрес;
  - Логин;

- отключение клиента;
- успешность аутентификации;
- включение, выключение и перезагрузка IPsec-туннеля;
- ошибки и предупреждения IPsec-туннеля.

Журнал расположен в подразделе журналирования IPsec (**«VPN» - «IPсec» - «Журнал»**).

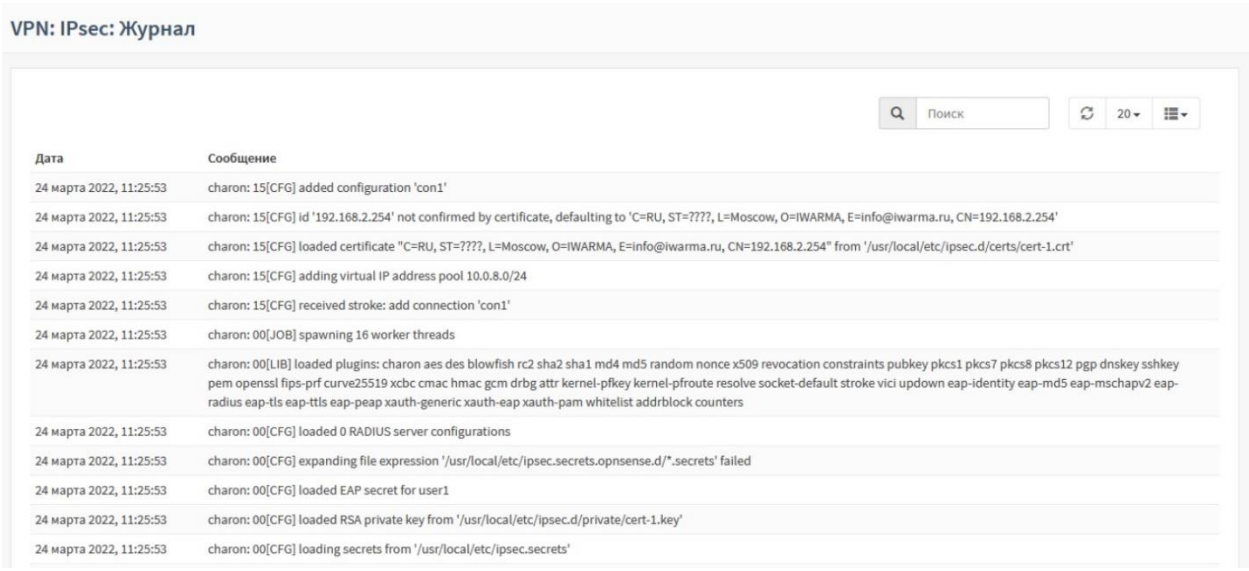


Рисунок – Журнал IPsec

34.15 Журнал OpenVPN

Журнал (см. Рисунок – Журнал OpenVPN) хранит записи, содержащие события работы сервиса OpenVPN следующих типов:

- подключение нового клиента;
- назначение IP-адреса;
- успешность аутентификации;
- тип аутентификации:
  - логин/пароль;
  - общий ключ;
- включение, выключение и перезагрузка сервера;
- ошибки и предупреждения сервера.

Предусмотрено разделение событий по настроенным серверам OpenVPN с помощью выпадающего списка **«Тип фильтра»** в верхней части страницы.

Журнал расположен в подразделе журналирования OpenVPN (**«VPN» - «OpenVPN» - «Журнал»**).

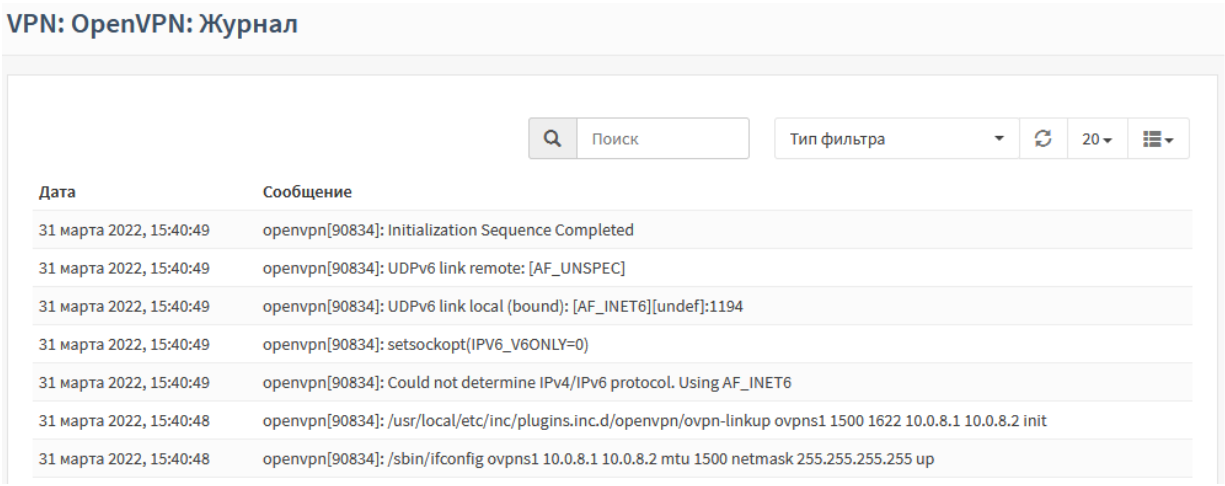


Рисунок – Журнал OpenVPN