INFOWATCH ARMA

Программный комплекс

InfoWatch ARMA Industrial Firewall

Руководство пользователя по эксплуатации

Межсетевой экран с функцией обнаружения вторжений

Листов 445

2020

Содержание

Перечень сокращений

АСУ — автоматизированная система управления

АСУТП — автоматизированная система управления технологическим процессом

МП — материнская плата

МЭ — межсетевой экран

МЭК — международная электротехническая комиссия

ОС — операционная система

ПК — программный комплекс

ПЛК — программируемый логический контроллер

ПО — программное обеспечение

РЗА — релейная защита и автоматика

СЗИ — средство защиты информации

СОВ — система обнаружения вторжений

СПВ — средство предотвращения вторжений

ЦПУ — центральное процессорное устройство

ACK — подтверждение (Acknowledge)

ACL — список управления доступом (Access Control List)

APCI — ACPI усовершенствованный интерфейс управления конфигурацией и питанием (Advanced Configuration and Power Interface)

APDU — протокольный блок данных прикладного уровня (Application Protocol Data Unit)

API — application programming interface, программный интерфейс приложения

ARP — протокол определения адреса (Address Resolution Protocol)

AS — автономная система (Autonomous System)

C2 — командование и управление(Command and Control)

CARP — протокол дупликации общего адреса (Common Address

Redundancy Protocol)

CDN — сеть доставки содержимого (Content Delivery Networks)

CIDR — Бесклассовая адресация (Classless Inter-Domain Routing)

CIP — общий промышленный протокол (Common Industrial Protocol)

CLI — командная строка (Command Line Interface)

COT — причина передачи (Cause Of Transfer)

CPU — центральное процессорное устройство (Central Processing Unit)

CRC — циклический избыточный код (Cyclic Redundancy Check)

CSV — от англ. Comma-Separated Values, значение, разделенные запятыми, формат файла

DCE-RPC — распределённая вычислительная среда / удалённые вызовы процедур (Distributed Computing Environment / Remote Procedure Calls)

DH — протокол Диффи — Хеллмана (Diffie–Hellman)

DHCP — протокол динамической настройки узла (Dynamic Host Configuration Protocol)

DNS — система доменных имён (Domain Name System)

DOS — отказ в обслуживании (Denial of Service)

DSCP — Точка кода дифференцированных услуг (Differentiated Services Code Point)

ECN — явное уведомление о перегруженности (Explicit Congestion Notification)

ENIP — промышленный протокол Ethernet (EtherNet IP)

FQDN — полностью определённое имя домена (Fully Qualified Domain Name)

GOOSE — общее объектно-ориентированное событие на подстанции (Generic Object-Oriented Substation Event)

FTP — протокол передачи файлов по сети (File Transfer Protocol)

HTTP — протокол передачи гипертекста (HyperText Transfer Protocol)

HTTPS — расширенный протокол HTTP (HyperText Transfer Protocol Secure)

IANA — Администрация адресного пространства Интернет (Internet Assigned Numbers Authority)

ICAP — протокол адаптации контента Интернета (Internet Content Adaptation Protocol)

ICMP — протокол межсетевых управляющих сообщений (Internet Control Message Protocol)

ID — идентификатор

IDS — система обнаружения вторжений (Intrusion Detection System)

IEC — Международная электротехническая комиссия (International Electrotechnical Commission)

IOA — адрес объекта информации (Information Object Address)

IP — межсетевой протокол (Internet Protocol)

IPS — система предотвращения вторжений (Intrusion Prevention System)

L2TP — протокол туннелирования второго уровня (Layer 2 Tunneling Protocol)

LAN — локальная вычислительная сеть (Local Area Network)

LDAP — облегчённый протокол доступа к каталогам (Lightweight Directory Access Protocol)

LRO — дефрагментация принимаемых пакетов (Large receive offload)

MAC — управление доступом к среде (Media Access Control)

MMS — протокол передачи данных по технологии «клиент-сервер» (Manufacturing Message Specification)

MSS — максимальный размер полезного блока данных в байтах для TCP-пакета (Maximum Segment Size)

NAT — преобразование сетевых адресов (Network Address Translation)

NPT — протокол сетевого времени (Network Time Protocol)

NTP — протокол трансляции сетевых префиксов (Network Prefix Translation)

OPC — семейство технологий управления объектов автоматизации (Open Platform Communications)

OSI — модель взаимодействия открытых систем (Open Systems Interconnection)

OSPF — протокол динамической маршрутизации (Open Shortest Path First)

PAT — трансляция порт-адрес (Port Address Translation)

pf — межсетевой экран операционной системы FreeBSD (Packet Filter)

PID — идентификатор процесса (Process Identifie)

PPP — двухточечный протокол канального уровня (Point-to-Point Protocol)

PPPoE — сетевой протокол канального уровня передачи кадров PPP через Ethernet (Point-to-Point Protocol Over Ethernet)

PPTP — туннельный протокол типа точка-точка (Point-to-Point Tunneling Protocol)

RAM — оперативная память (Random Access Memory)

RFC — рабочее предложение (Request for Comments)

RIP — протокол маршрутной информации (Routing Information Protocol)

RRD — циклическая база данных (Round-Robin Database)

RTT — время приема-передачи (Round-Trip Time)

SCADA — диспетчерское управление и сбор данных (Supervisory Control And Data Acquisition)

SMB — сетевой протокол прикладного уровня для удалённого

доступа к файлам (Server Message Block)

SNMP — простой протокол сетевого управления (Simple Network Management Protocol)

SPAN — анализатор коммутируемых портов (Switch Port Analyzer)

SSH — безопасная оболочка (Secure Shell)

SSL — уровень защищённых сокетов (Secure Sockets Layer)

SSLBL — черный список SSL (Black List SSL)

TCP — протокол управления передачей (Transmission Control Protocol)

TFTP — простой протокол передачи файлов (Trivial File Transfer Protocol)

TLS — протокол защиты транспортного уровня (Transport Layer Security)

TOTP — алгоритм создания одноразовых паролей (Time Based One Time Password)

TOS — тип обслуживания (Type of Service)

TSO — разгрузка сегментированием на уровне TCP (TCP Segmentation Offload)

TTL — время жизни пакета данных в протоколе IP (Time To Live)

UDP — протокол пользовательских датаграмм (User Datagram Protocol)

UEFI — интерфейс расширяемой прошивки (Unified Extensible Firmware Interface)

URG — указатель важности (Urgent pointer field is significant)

URI — унифицированный идентификатор ресурса (Uniform Resource Identifier)

URL — единый указатель ресурса (Uniform Resource Locator)

USB — универсальная последовательная шина (Universal Serial Bus)

UTC — всемирное координированное время (Coordinated Universal Time)

VHID — виртуальный идентификатор хоста (Virtual Host ID)

VLAN — виртуальная локальная сеть (Virtual Local Area Network)

WAN — глобальная вычислительная сеть (Wide Area Network)

WCCP — протокол перенаправления контента (Web Cache Communication Protocol)

WPAD — протокол автоматической настройки прокси (Web Proxy Auto-Discovery Protocol)

WMI — Инструментарий управления Windows (Windows Management Instrumentation)

XML — расширяемый язык разметки (Extensible Markup Language)

XMLRP — XML-вызов удаленных процедур (Extensible Markup Language Remote Procedure Call)

Аннотация

Руководство пользователя описывает работу с программным комплексом «InfoWatch ARMA Industrial Firewall» версии (далее ПК «InfoWatch ARMA Industrial Firewall»). Руководство предназначено для технических специалистов и пользователей и содержит описание графического и консольного интерфейса пользователя, описание наиболее частых сценариев использования, описание диалога с пользователем и сообщения пользователю. Руководство пользователя предназначено для пользователя, который выполняет конфигурирование и мониторинг работы ПК «InfoWatch ARMA Industrial Firewall». Роль пользователя и администратора может выполнять один сотрудник предприятия.

Пользователю ПК «InfoWatch ARMA Industrial Firewall» необходимо изучить настоящее руководство перед эксплуатацией.

Введение

Название документа	Программный комплекс InfoWatch ARMA Industrial Firewall (ПК «InfoWatch ARMA Industrial Firewall»). Руководство пользователя по эксплуатации.
Версия документа	Версия 60
Дата редакции документа	18.03.2020
Ключевые слова	Межсетевой экран, система обнаружения вторжений

Руководство пользователя описывает доступные пользователям функции, а также подробное описание их настройки и использования.

В Руководстве пользователя представлено описание принципов работы с ПК «InfoWatch ARMA Industrial Firewall».

1. Назначение программы

ПК «InfoWatch ARMA Industrial Firewall» является межсетевым экраном с функцией обнаружения и предотвращения вторжений, который обеспечивает выполнение следующих задач:

– защита устройств и компьютеров сети АСУТП со стороны внешней сети;

– сокрытие архитектуры и конфигурации защищаемой системы и трансляция адресов (NAT и PAT);

– межсетевое экранирование на основе информации с транспортного, сетевого и прикладного уровней;

– обнаружение и предотвращение компьютерных атак на сетевом и прикладном уровне;

– экспорт событий безопасности (syslog);

– статическая и динамическая маршрутизация;

– контроль доступа пользователей локальной сети к сети (Портал авторизации);

– контроль доступа пользователей локальной сети к ресурсам Internet (URL-фильтрация);

– статическая и динамическая маршрутизация;

– зеркалирование трафика с выбранного порта на отдельный порт;

– уведомление о событиях безопасности по электронной почте и syslog;

– сбор и разбор сетевого трафика;

– предотвращения задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом (QoS, Traffic Shaping);

– сбор статистики NetFlow;

– прокси-сервер;

– DHCP-сервер.

1.1. Запуск и авторизация

Для доступа к веб-интерфейсу управления ПК «InfoWatch ARMA Industrial Firewall» необходимо:

– открыть веб-браузер (требования к веб-браузерам приведены в Руководстве администратора в разделе 1.1)

– ввести адрес LAN интерфейса, указанный в консольном интерфейсе, в формате: http(s)://[IP-адрес LAN интерфейса] (по умолчанию используется подключение через протокол https), например, «https://192.168.1.1».

Более подробная информация о настройке системы описана в Руководстве администратора в разделе 2.

Для начала работы с системой необходимо авторизоваться (рисунок 1). Аутентификационные данные по умолчанию:

– имя пользователя — «root»;

– пароль — «root».

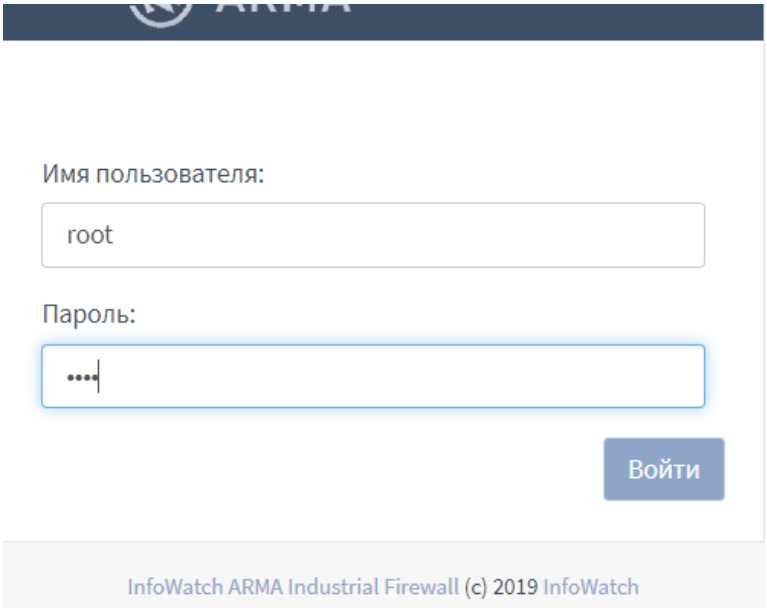


Рисунок 1 — Вход в систему

1.2. Описание графического интерфейса

Внешний вид графического интерфейса в разделе «Инструментальная панель» показан на рисунке (рисунок 2).

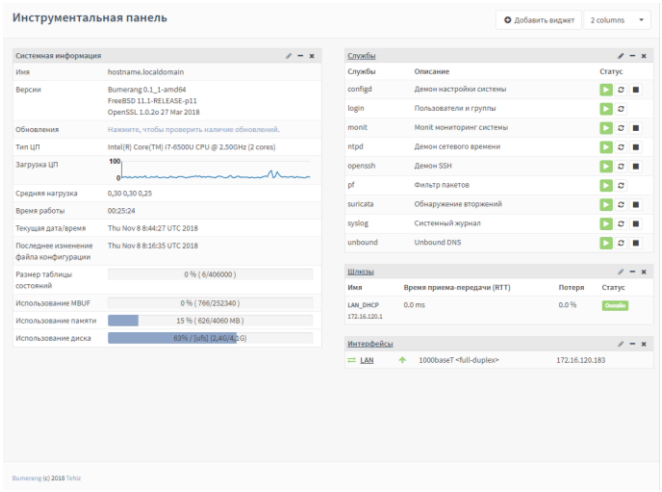


Рисунок 2 — Вид графического интерфейса (раздел «Инструментальная панель»)

1.2.1.Логотип и ссылка на «Инструментальную панель»

Для перехода в раздел меню «Инструментальная панель» необходимо нажать на кнопку логотип ПК «InfoWatch ARMA Industrial Firewall» (из любой страницы веб-интерфейса) в верхнем левом углу экрана или выбрать соответствующий пункт меню.

1.2.2.Область меню

Область меню (рисунок 3) находится в левой части экрана и содержит все разделы и их подразделы. С помощью меню предоставляется доступ к различным функциям ПК «InfoWatch ARMA Industrial Firewall». Переход по пунктам осуществляется нажатием левой кнопки мыши.

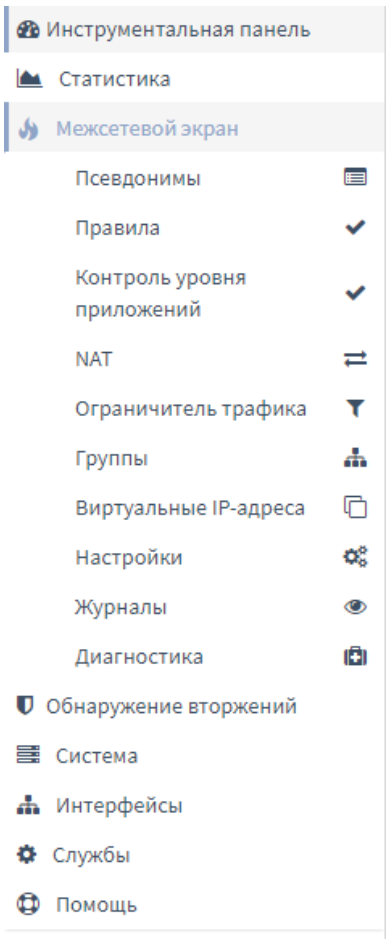


Рисунок 3 — Область меню

Существует три уровня вложенности меню:

– раздел;

– подраздел;

– категория (может не существовать, если подраздел простой).

На рисунке (рисунок 4) раздел — «Система» с подразделом — «Доступ» и категорией — «Пользователи».

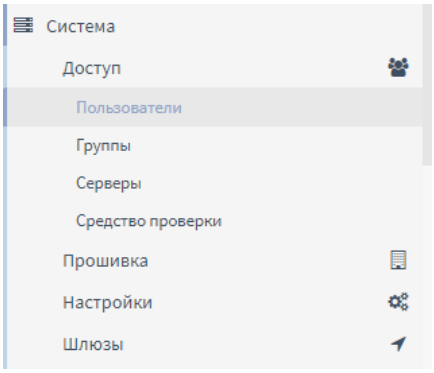


Рисунок 4 — Пример категории системы

1.2.3. Область быстрой навигации

Для быстрой навигации по графическому интерфейсу имеется возможность использовать область поиска в правом верхнем углу экрана. Для выбора области поиска, необходимо нажать на текстовое поле в правом верхнем углу экрана, после чего будет активирован режим ввода текста с клавиатуры в это поле.

Поле для поиска при наборе текста предоставляет предложения поисковых запросов в зависимости от того, какие ключевые слова для поиска набирает пользователь. Пример таких предложений представлен на рисунке (рисунок 5). Для перехода на страницу, необходимо нажать на строку с её именем. Также возможен выбор предложения поискового запроса с помощью клавиш со стрелкой вверх и вниз, а для подтверждения выбора необходимо нажать на клавишу «ENTER».

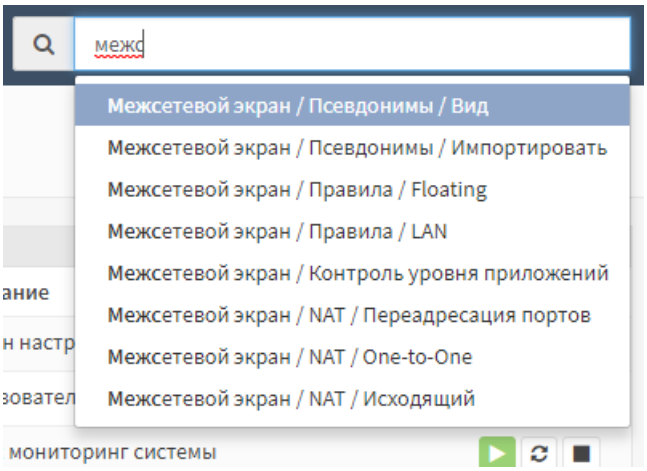


Рисунок 5 — Пример применения поиска

1.2.4. Имя пользователя и доменное имя

В правом углу слева от поля быстрой навигации показано имя пользователя и полное доменное имя, в котором настроен ПК «InfoWatch ARMA Industrial Firewall» (чтобы изменить имя или полное доменное имя необходимо перейти в раздел меню «Система» - «Настройки» - «Общие настройки»).

1.2.5.Справочная информация

Формы веб-интерфейса многих страниц оснащены встроенной справкой (рисунок 6). Для того чтобы включить её, в правом верхнем углу формы необходимо нажать на кнопку-переключатель «Справка» для отображения всех справочных сообщений под соответствующими элементами.

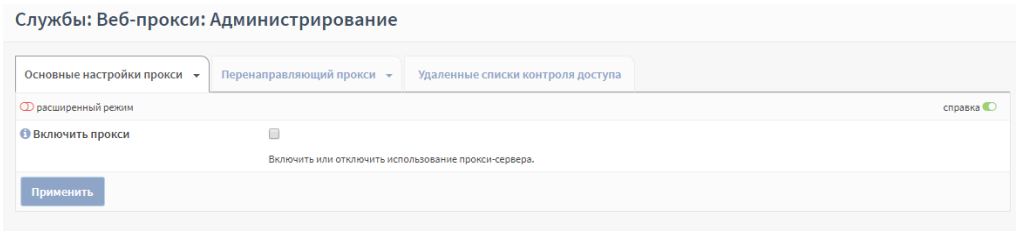


Рисунок 6 — Справочная информация

1.2.6.Расширенный режим

На некоторых страницах имеются расширенные функции (рисунок 7). Для просмотра расширенных функций в левом углу формы необходимо нажать на кнопку-переключатель «Расширенный режим».

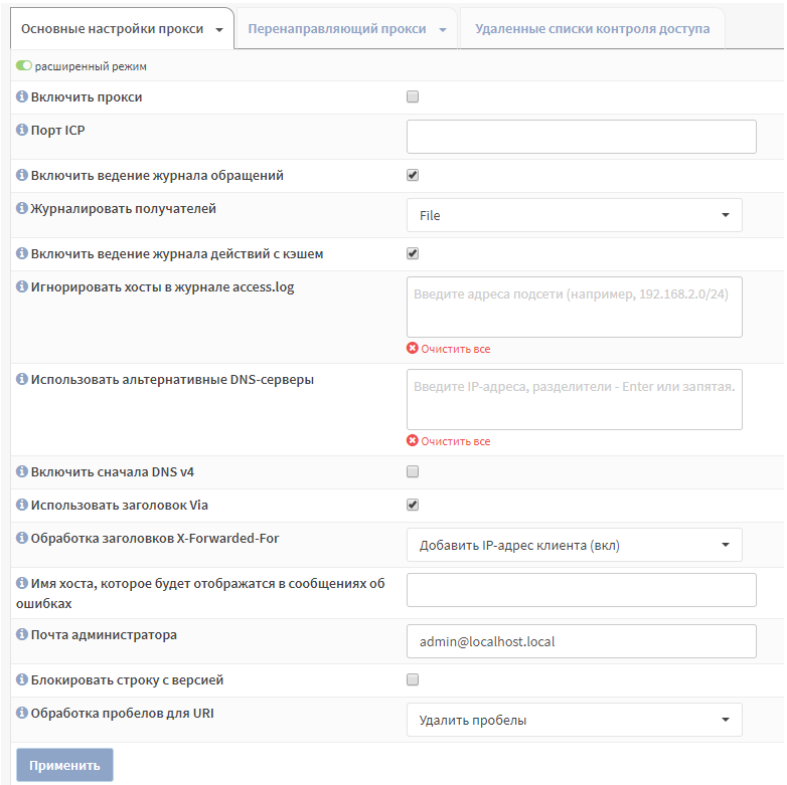


Рисунок 7 — Расширенный режим

1.2.7.Подсказки

Для вывода строки подсказок для элемента формы, необходимо нажать на кнопку , которая расположена слева от него, если она отображается синим цветом (рисунок 8). Если кнопка отображается серым цветом, то элемент формы не включает в себя подсказок.

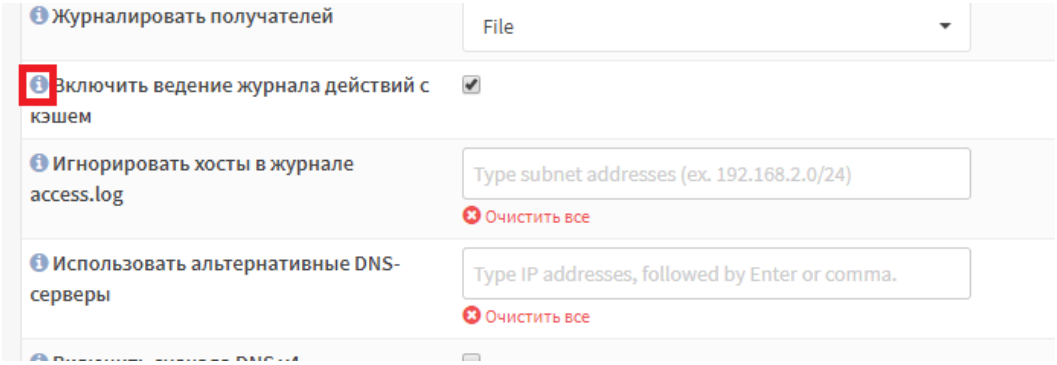


Рисунок 8 — Включение подсказки

1.2.8.Вкладки

Для перехода к вложенной странице (рисунок 9) и открытия соответствующей формы, необходимо нажать на заголовок вкладки.

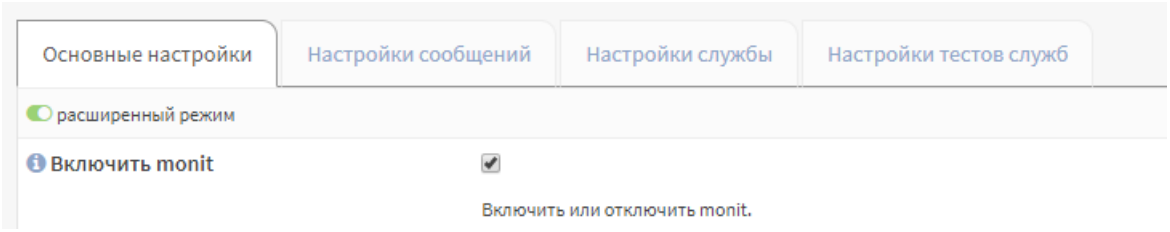


Рисунок 9 — Открытие формы вкладки

1.2.9.Выпадающие списки

Для просмотра всех элементов выпадающего списка, необходимо нажать на стрелку в его правой части, например как показано на рисунке (рисунок 10). В некоторых случаях, при большом количестве элементов выпадающего списка в правой части области доступных элементов списка появится полоса прокрутки. Прокрутка списка возможна с помощью перемещения ползунка полосы прокрутки или с помощью колёсика мыши.

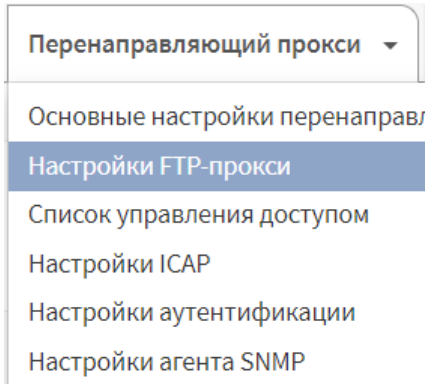


Рисунок 10 — Выпадающий список

1.3. Описание основных разделов графического интерфейса

1.3.1. Инструментальная панель

Раздел «Инструментальная панель» позволяет:

– просматривать информацию, выдаваемую информационными виджетами;

– добавлять, скрывать и/или настраивать виджеты;

– выбирать формат отображения виджетов на инструментальной панели (от 1 до 6 столбцов) и их компоновку (виджеты можно менять местами).

1.3.2. Анализ

Раздел «Анализ» позволяет:

– просматривать общее состояние и производительность системы в течение времени;

– просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику количества пакетов в течение времени на определенном сетевом интерфейсе (в виде графика или таблицы);

– просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику использования памяти, mbuf, состояний, загруженности процессора и (когда доступна) температуры процессора (в виде графика или

таблицы);

– просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику использования сервисов (в виде графика или таблицы);

– просматривать и экспортировать в формате «*.csv» для дальнейшего анализа статистику трафика (полный входящий/исходящий трафик в пакетах и байтах) по всем сетевым интерфейсам (в виде графика или таблицы);

– просматривать и экспортировать в формате «*.csv» для дальнейшего анализа данные Netflow;

– просматривать статистику использования портов и IP-адресов на выбранном сетевом интерфейсе;

– просматривать 25 наиболее используемых пользователей для выбранного сетевого интерфейса.

1.3.3. Межсетевой экран

Раздел меню «Межсетевой экран» позволяет:

– задавать правила фильтрации трафика (блокирование, разрешение, отклонение) для существующих сетевых интерфейсов на промышленном, сетевом, прикладном уровнях;

– настраивать ограничение трафика (настраивать приоритеты, пропускную способность каналов);

– задавать NAT правила;

– создавать виртуальные IP-адреса;

– посматривать журнал событий межсетевого экрана;

– экспортировать события межсетевого экрана за промежуток времени на выбранном интерфейсе.

1.3.4. Обнаружение вторжений

Раздел меню «Обнаружение вторжений» позволяет включить систему обнаружения (предотвращения, если настроено блокирование, то есть «Режим IPS») вторжений и настроить ее работу.

В данном разделе меню графического интерфейса имеется возможность создавать правила системы обнаружения вторжений по шаблону, локально загружать правила в систему обнаружения вторжений, мониторинга событий системы обнаружения вторжений в соответствующем журнале событий, включения системы предотвращения вторжений, настроить импорт баз решающих правил по ftp.

1.3.5.Система

Раздел меню «Система» позволяет:

– добавлять, редактировать, удалять пользователей/группы пользователей;

– назначать привилегии пользователям/группам пользователей;

– задавать сложность паролей;

– создавать, редактировать, удалять серверы аутентификации пользователей;

– просматривать контрольные суммы;

– просматривать отчеты об ошибках работы ПК «InfoWatch ARMA Industrial Firewall»;

– обновлять ПО ПК «InfoWatch ARMA Industrial Firewall»;

– настраивать ПК «InfoWatch ARMA Industrial Firewall:

– выбирать часовой пояс;

– выбирать язык веб-интерфейса;

– настраивать доступ по SSH;

– настраивать консольный интерфейс;

– настраивать веб-интерфейс;

– изменять пароль;

– настраивать системный журнал (сколько записей содержит, какие события отображать и другое);

– настраивать SNMP;

– настраивать планировщик задач (Cron);

– создавать, редактировать, удалять сетевые шлюзы;

– задавать статические маршруты;

– настраивать кластеризацию;

– настраивать отказоустойчивый кластер и просматривать статус ПК «InfoWatch ARMA Industrial Firewall» при работе в режиме отказоустойчивого кластера;

– просматривать, обновлять, останавливать/включать настроенные службы;

– сохранять текущую конфигурацию;

– настраивать экспорт конфигурации на удаленный сервер;

– восстанавливать конфигурацию;

– просматривать и отменять изменения конфигурации ПК «InfoWatch ARMA Industrial Firewall»;

– настраивать экспорт конфигурации и баз решающих правил СОВ по ftp;

– создавать, редактировать и удалять сертификаты;

– осуществлять начальную настройку системы;

– просматривать журнал системных событий;

– просматривать журнал веб-интерфейса;

– просматривать журнал сервера;

– экспортировать события по SYSLOG;

– экспортировать события по SYSLOG по CEF;

– перезагружать или выключать ПК «InfoWatch ARMA Industrial Firewall»;

– выходить из учетной записи пользователя.

1.3.6. Интерфейсы

Раздел меню «Интерфейсы» позволяет:

– создавать, редактировать и удалять сетевые интерфейсы;

– выставлять соответствие между логическими и физическими сетевыми интерфейсами;

– просматривать количество входящих/исходящих (разрешенных/заблокированных) пакетов на выбранном сетевом интерфейсе;

– настраивать VLAN;

– производить захват пакетов на выбранном сетевом интерфейсе (возможен просмотр и выгрузка результата в виде файла);

– осуществлять проверку работы и приема соединения хоста на выбранном порту;

– отправлять ping запрос.

1.3.7.Сеть

Раздел меню «Сеть» позволяет запускать сервис Arpwatch, просматривать таблицу подключаемых устройств к ПК «InfoWatch ARMA Industrial Firewall», запускать анализ дампов трафика, просматривать в виде таблицы все пакеты (удовлетворяющие заданным фильтрам), проходящие через выбранный сетевой интерфейс ПК «InfoWatch ARMA Industrial Firewall».

1.3.8.Маршрутизация

Раздел меню «Маршрутизация» позволяет настраивать динамическую маршрутизацию по протоколам RIPv1, RIPv2, OSPFv2, OSPFv3, BGPv4, а также просматривать журнал событий служб динамической маршрутизации.

1.3.9.Службы

Раздел меню «Службы» позволяет:

– настраивать и просматривать журнал событий Портала авторизации;

– настраивать и просматривать журнал событий DHCP-сервера;

– настраивать «Monit»;

– настраивать синхронизацию времени (по протоколу NTP);

– настраивать и просматривать журнал событий прокси-сервера.

1.4. Журналирование

В ПК «InfoWatch ARMA Industrial Firewall» журналы разделены на категории, отличающиеся в зависимости от сервиса, который использует данный журнал.

В таблице (таблица 1) приведена информация о соответствии различных сервисов определенным журналам с указанием дополнительной информации по типу событий и формату сообщений для этого журнала.

Таблица 1 — Журналирование

Журнал	**Путь в интерфейсе**	**Сохраняемые события**	**Формат сообщений**
Системные события			
Журнал Syslog	«Система» - «Журналы» - «Журнал Syslog»	Системные события	Дата Сервис: Сообщение
Журнал сервера (Backend журнал)	«Система» - «Журналы» - «Backend журнал»	События, сгенерированные за счет использования API сервера и изменения конфигурации	Дата Сервис: Сообщение
Журнал событий веб-интерфейса	«Система» - «Журналы» - «WebGUI журнал»	События сервера (lighthttpd)	Дата Сервис [pid]: Сообщение
Журнал изменения настроек шлюза	«Система» - «Шлюзы» - «Журнал»	Изменения настроек шлюза	Дата Сервис: Сообщение
Журнал маршрутизации	«Система» - «Маршруты» - «Журнал»	Изменения маршрутов	Дата Сервис [pid]: Сообщение
Журнал системных событий	«Система» - «Журналы» - «Журнал системных событий»	Определенные системные события (описано ниже)	Дата Сервис: Сообщение

Журнал	Путь в интерфейсе	Сохраняемые события	Формат сообщений
Журнал событий безопасности	«Система» - «Журналы» - «Журнал событий безопасности»	События системы обнаружения вторжений, события межсетевого экрана, события arpwatch, события Портала авторизации	Дата Событие Механизм Отправитель Получатель Действие Описание Имя пользователя Дополнительная информация
Журнал действий пользователей	«Система» - «Журналы» - «Журнал действий пользователей»	События действий пользователей	Дата Имя пользователя Адрес Действия Успешно
Межсетевой экран			
Журнал событий МЭ в реальном времени	«Межсетевой экран» - «Журналы» - «Реальное время»	События МЭ в реальном времени	Интерфейс Время IP отправителя: Порт отправителя IP получателя: Порт получателя Протокол транспортного уровня Метка и результат обработки
Журнал необработанных событий от pf	«Межсетевой экран» - «Журналы» - «pflog»	Необработанные события из filter.log	Формат зависит от версий протоколов (формат pflog)
Журналы сервисов			
Журнал портала авторизации	«Службы» - «Портал авторизации» - «Журнал»	События Портал авторизации	Дата Сервис: Сообщение
Журнал DHCPv4	«Службы» - «DHCPv4» - «Журнал»	События DHCPv4	Дата Сервис: Сообщение

Журнал	Путь в интерфейсе	Сохраняемые события	Формат сообщений
Системный журнал системы обнаружения вторжений	«Обнаружение вторжений» - «Журнал»	События срабатывания правил системы обнаружения вторжений	Дата Сервис: Сообщение
Журнал инцидентов системы обнаружения вторжений	«Обнаружение вторжений» - «Администрирование» - «Предупреждения (Alert)»	События системы обнаружения вторжений	Дата Сервис: Сообщение
Журнал NTP	«Службы» - «Синхронизация времени» - «Журнал»	События NTP	Дата Сервис: Сообщение
Журнал веб-прокси	«Службы» - «Прокси» - «Журнал»	События прокси-сервера	Дата Сервис: Сообщение

В журнале Syslog содержатся уведомления следующего типа:

– вход в систему (удачный или неудачный);

– изменения внутреннего представления времени;

– изменение пароля пользователя;

– изменения настроек системы;

– события на добавление, изменение, удаление и получение информации о следующих элементах:

– пользователи;

– правила МЭ;

– правила и группы правил СОВ;

– уведомления в случае отказа каких-либо модулей МЭ.

В журнале сервера (Backend журнал) содержатся уведомления следующего типа:

– события, сгенерированные за счет использования API сервера;

– события изменения конфигурации.

В WebGUI журнале содержатся уведомления следующего типа:

– события сервера lighthttpd.

В журнале изменений настроек шлюза содержатся уведомления следующего типа:

– события настроек шлюзов.

В журнале маршрутизации содержатся уведомления следующего типа:

– события изменения маршрутов.

В журнале системных событий содержатся следующие события:

– запуск ntp-сервера;

– нет подключения к ntp-серверу;

– выключение ntp-сервера;

– изменение настроек ntp-сервера;

– сбои Портала авторизации (неуспешная попытка входа в Портал авторизации;

– сбои системы обнаружения вторжений;

– события контроля целостности;

– запуск веб-сервера;

– неуспешный доступ к странице графического интерфейса;

– загрузка системы.

В журнале действий пользователей содержатся следующие события:

– включение и отключение межсетевого экрана;

– включение и отключение системы обнаружения вторжений;

– успешный/неуспешный доступ к страницам интерфейса;

– изменение/добавление/удаление правил межсетевого экрана;

– изменение настроек межсетевого экрана;

– изменение правил системы обнаружения вторжений;

– изменение настроек системы обнаружения вторжений;

– успешная/неуспешная авторизация в графическом и консольном интерфейсах;

– изменение размера записей в WebGUI журнале;

– создание нового пользователя;

– включение «сложного» пароля;

– изменение настроек мониторинга состояния системы на странице анализа трафика, настроек monit;

– перезагрузка системы.

В журнале событий безопасности содержатся следующие события:

– для системы обнаружения вторжений:

  – срабатывание сигнатур;

– для межсетевого экрана:

  – срабатывания правил межсетевого экрана;

– для arpwatch:

  – подключение несанкционированного устройства;

  – обнаружение конфликта IP-адресов;

  – обнаружение изменения IP, MAC адреса;

  – обнаружение подмены MAC адресов;

  – обнаружение подмены IP-адресов.

– для Портала авторизации:

  – удачная/неудачная авторизация пользователя.

– для Портала авторизации:

  – удачная/неудачная авторизация пользователя;

  – запуск портала авторизации.

Журнал событий МЭ в реальном времени динамически отображает все события сети в виде таблицы со следующими полями:

– время инцидента;

– название интерфейса;

– сетевой адрес и порт источника;

– сетевой адрес и порт получателя;

– статус (действие, произведенное с пакетом, инициировавшим

запись);

– действие (предпринимаемое в ответ на возможные нарушения безопасности);

– комментарий (дополнительная информация по данному инциденту).

Журнал необработанных событий от pf отображает все события сети в виде таблицы со следующими полями:

– номер сработавшего правила;

– номер зависимого правила;

– действие (предпринимаемое в ответ на возможные нарушения безопасности);

– имя правила;

– ID правила;

– физический интерфейс;

– причина сохранения (обычно match – совпало с правилом);

– направление (in или out);

– версия IP (4 или 6);

– TOS;

– ECN;

– TTL;

– ID;

– Offset;

– Flags;

– Protocol ID;

– порт источника;

– порт назначения;

– длина данных;

– флаги;

– Seq ID;

– ACK номер;

– размер окна;

– указатель URG;

– опции TCP.

Журнал Портала авторизации содержит уведомления следующего типа:

– события Портала авторизации.

Журнал DHCPv4 содержит уведомления следующего типа:

– события сервиса DHCPv4.

Системный журнал системы обнаружения вторжений отображает информацию обо всех системных событиях системы обнаружения вторжений в виде таблицы со следующими полями:

– время/дата;

– действие (предпринимаемое в ответ на возможные нарушения безопасности);

– сетевой интерфейс;

– сетевой адрес отправителя;

– порт отправителя;

– сетевой адрес получателя;

– порт получателя;

– описание инцидента.

В журнале инцидентов системы обнаружения вторжений содержатся уведомления следующего типа:

– события о срабатывании правил системы обнаружения вторжений.

В журнале NTP содержатся уведомления следующего типа:

– события сервиса NTP.

В журнале прокси-сервера уведомления следующего типа:

– события прокси-сервера.

2. Раздел «Инструментальная панель»

В разделе «Инструментальная панель» отображается информация, выдаваемая следующими информационными виджетами:

- системная информация;
- службы;
- шлюзы;
- интерфейсы;
- загрузка процессора;
- журнал Syslog;
- CARP;
- статистика интерфейса;
- журнал межсетевого экрана;
- Monit;
- синхронизация времени;
- датчики температуры;
- трафик.

2.1. Виджет «Системная информация»

В виджете «Системная информация» отображается основная информация о системе (рисунок 11):

- имя системы;
- версия системы ПК «InfoWatch ARMA Industrial Firewall», операционной системы, OpenSSL;
- доступные обновления;
- тип процессора;
- загрузка процессора (отображается в виде графика);
- средняя нагрузка;
- время работы системы;
- текущее дата/время;

– последние изменения файла конфигурации (отображается последнее дата, время последнего изменения файла конфигурации);

– размер таблицы состояний (максимальный размер равен 98000 записей, также размер таблицы отображается в процентах);

– использование MBUF (максимальный размер равен 61620, также размер использования MBUF отображается в процентах);

– использование памяти (максимальный размер равен 988 Мб, также размер использования памяти отображается в процентах);

– использование диска (максимальный размер равен 5,8 Гб, также размер использования диска отображается в процентах).

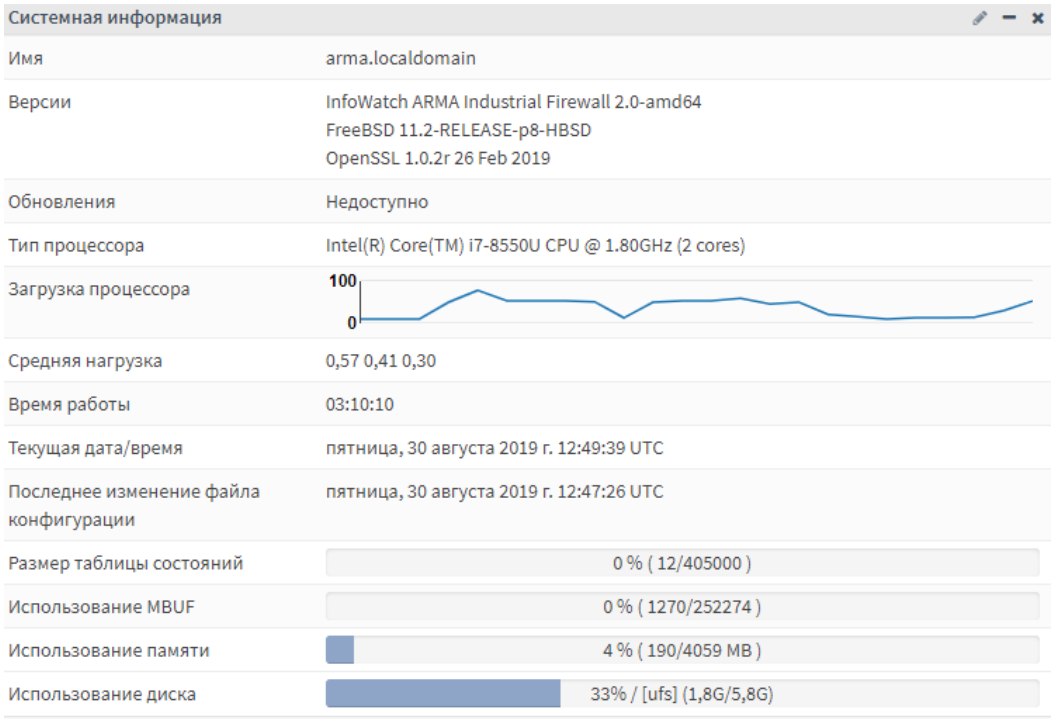


Рисунок 11 — Виджет «Системная информация»

2.2. Виджет «Службы»

В виджете «Службы» отображаются настроенные службы. С службами имеется возможность производить следующие действия:

– «остановить» ■;

– «запустить» ▶;

– «перезагрузить» ⟳.

Взаимодействие (остановка, запуск, перезапуск) со службами происходит путём нажатия соответствующей кнопки. Если кнопка «запустить» зеленого цвета , значит служба работает. Если кнопка «остановить» красная , значит служба выключена. Для удаления из виджета определенных служб необходимо нажать на кнопку и в появившимся поле ввода ввести названия служб (через запятую), которые необходимо скрыть из виджета (рисунок 12). Название необходимо указывать в соответствии с названием службы в колонке «Службы» информационного виджета.

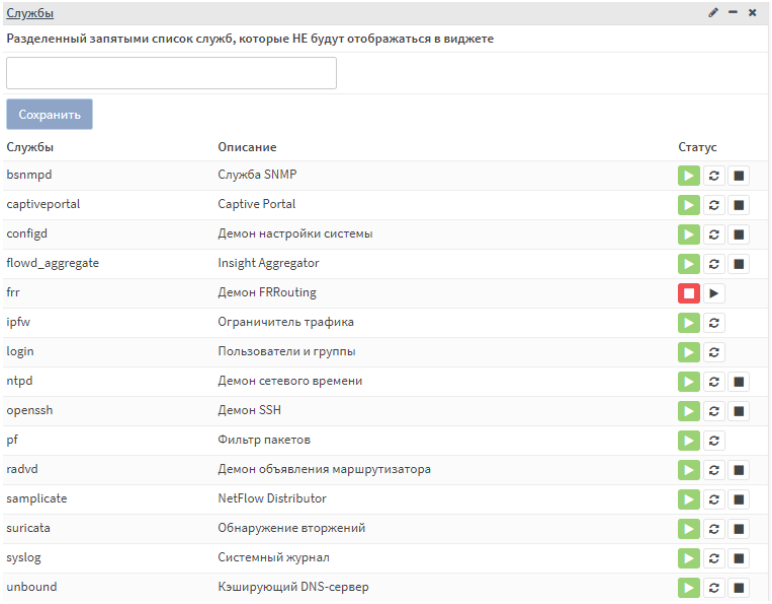


Рисунок 12 — Виджет «Службы»

2.3. Виджет «Шлюзы»

В виджете «Шлюзы» отображаются настроенные шлюзы, их статус, время приема-передачи (RTT), потеря передачи (рисунок 13).

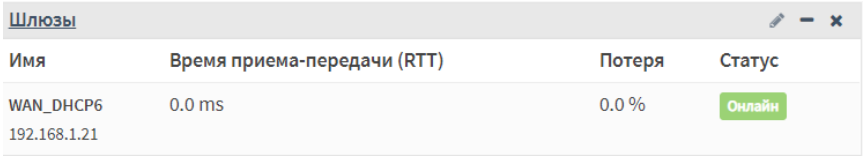


Рисунок 13 — Виджет «Шлюзы»

2.4. Виджет «Интерфейсы»

В виджете «Интерфейсы» отображаются включенные сетевые интерфейсы, их IP-адрес, скорость и режим передачи данных (рисунок 14).

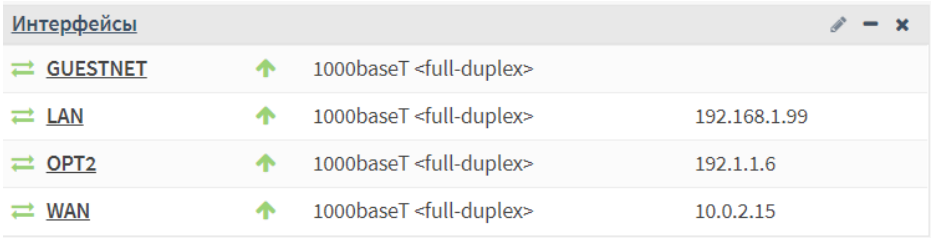


Рисунок 14 — Виджет «Интерфейсы»

2.5. Виджет «Загрузка процессора»

В виджете «Загрузка процессора» отображается загрузка центрального процессора в виде графика (в режиме реального времени) (рисунок 15).

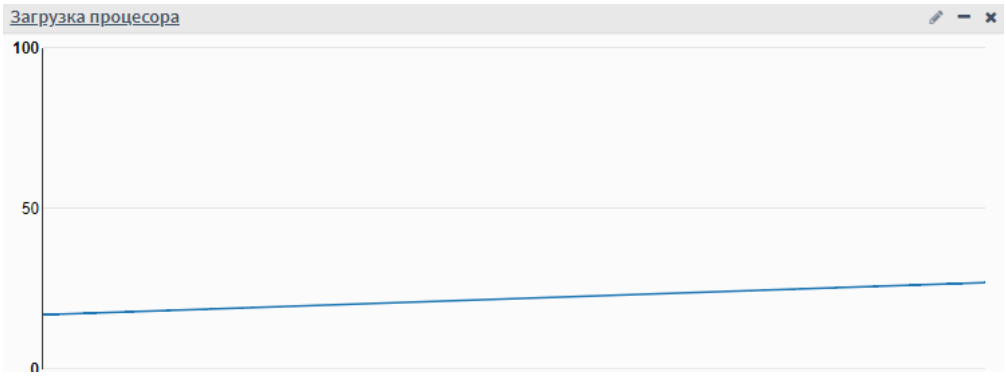


Рисунок 15 — Виджет «Загрузка процессора»

2.6. Виджет «Журнал syslog»

В виджете «Журнал Syslog» (рисунок 16) отображается журнал Syslog в виде таблицы (в режиме реального времени). В таблице присутствует информация о времени, дате события, а также описания этих событий. Для выбора количества отображаемых событий необходимо нажать на кнопку  и ввести необходимое количество событий, которые будут отображены в виджете.

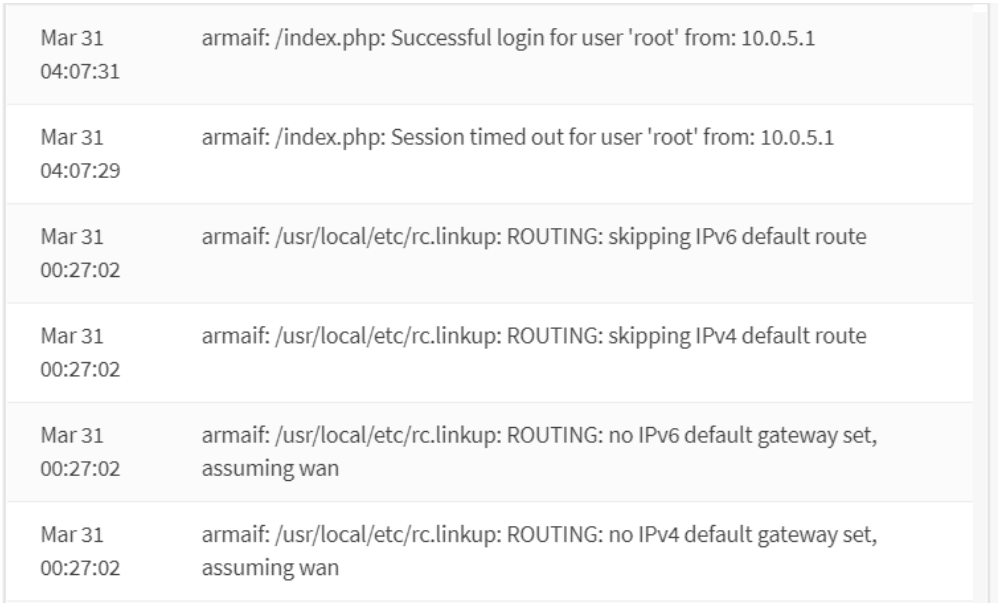


Рисунок 16 — Виджет «Журнал Syslog»

2.7. Виджет «CARP»

В виджете «CARP» отображается статус устройства при работе в режиме отказоустойчивого кластера, общий совместно используемый виртуальный IP-адрес и сетевой интерфейс (рисунок 17).

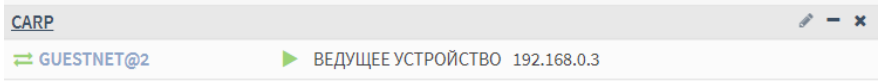


Рисунок 17 — Виджет «CARP»

2.8. Виджет «Статистика интерфейсов»

В виджете «Статистика интерфейсов» отображается сводная таблица по всем настроенным сетевым интерфейсам в режиме реального времени (рисунок 18):

– количество входящих/исходящих пакетов;

– количество входящих/исходящих байтов;

– количество ошибок входящего/исходящего трафика;

– количество коллизий для каждого настроенного сетевого интерфейса.

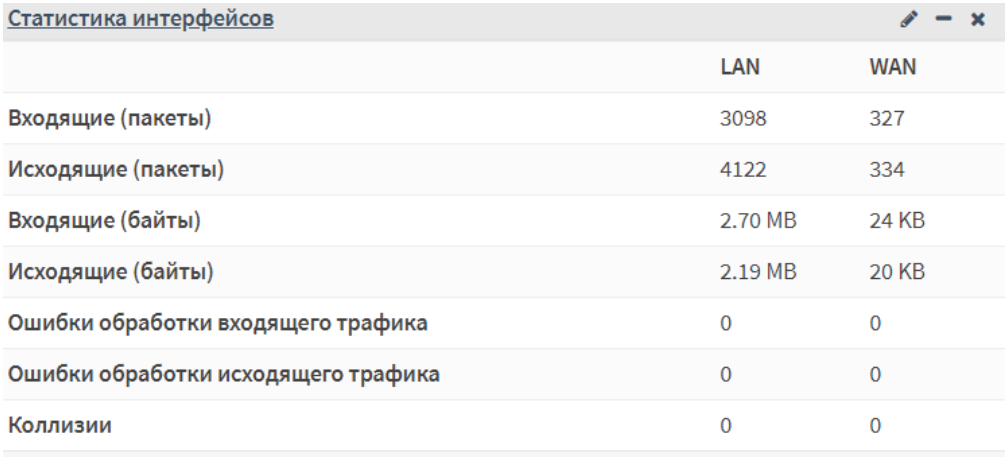


Рисунок 18 — Виджет «Статистика интерфейсов»

2.9. Виджет «Журнал межсетевого экрана»

В виджете «Журнал межсетевого экрана» отображается события межсетевого экрана в виде таблицы (в режиме реального времени) (рисунок 12). В таблице содержится информация о времени/дате события, об интерфейсе, через который прошел трафик, о действии, которое было применено к трафику, об отправителе и получателе. Для настройки дополнительных параметров отображения событий межсетевого экрана необходимо нажать на кнопку . В дополнительных параметрах возможен выбор количества отображаемых событий, интервал обновления таблицы, выбор сетевых интерфейсов, события которых будут отображены в журнале межсетевого экрана, а также возможна фильтрация по действию (разрешить, блокировать, отклонить) (рисунок 19).

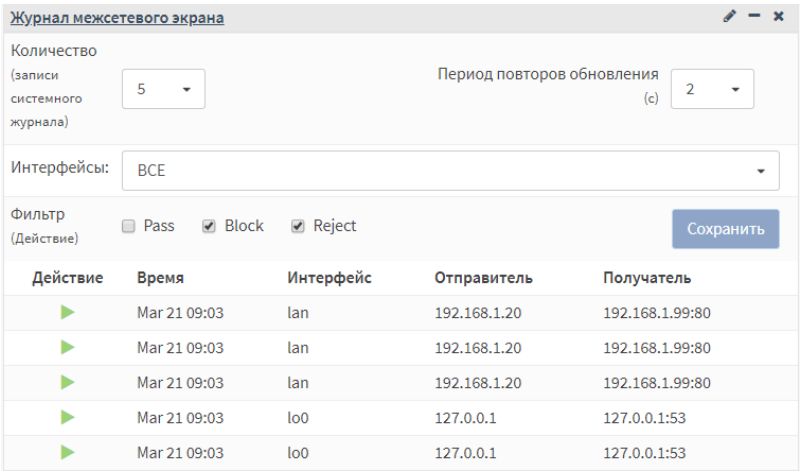


Рисунок 19 — Виджет «Журнал межсетевого экрана»

2.10. Виджет «Monit»

В виджете «Monit» отображаются состояния почтовых серверов (доступность, потребление ресурсов), состояния сервисов (потребляемые ресурсы, количество и другое), состояния сетевых сервисов (в режиме реального времени) (рисунок 20).

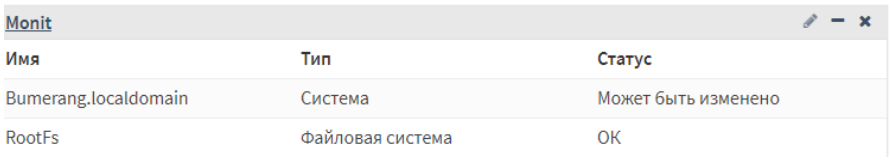


Рисунок 20 — Виджет «Monit»

2.11. Виджет «Синхронизация времени»

В виджете «Синхронизация времени» отображается текущее время системы, а также информация о сервере, с которым синхронизируется время в ПК «InfoWatch ARMA Industrial Firewall» (рисунок 21).

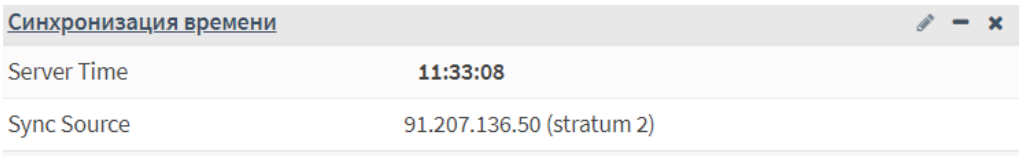


Рисунок 21 — Виджет «Синхронизация времени»

2.12. Виджет «Датчики температуры»

В виджете «Датчики температуры» (рисунок 22) отображается температура центрального процессора, материнской платы (по данным ACPI), если в системе имеется поддерживаемый чип датчика температуры. В настройке отображения индикатора температуры возможен ввод следующих значений:

– пороговое значение температуры предупреждения (то имеется значение температуры материнской платы, достигнув которое индикатор температуры материнской платы будет отображаться оранжевым цветом);

– критическая температура МП (то имеется значение температуры материнской платы, достигнув которое индикатор температуры материнской

платы будет отображаться красным цветом);

– температура предупреждения ЦПУ (то имеется значение температуры процессора, достигнув которое индикатор температуры процессора будет отображаться оранжевым цветом);

– критической температура ЦПУ (то имеется значение температуры процессора, достигнув которое индикатор температуры процессора будет отображаться красным цветом).

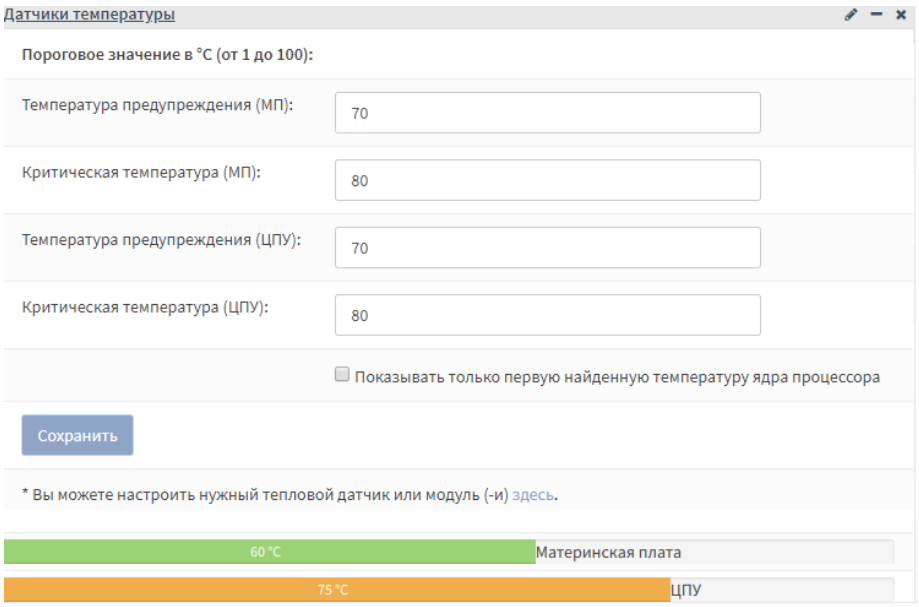


Рисунок 22 — Виджет «Датчики температуры»

2.13. Виджет «Трафик»

В виджете «Трафик» (рисунок 23) отображается входящий/исходящий трафик в виде графика (в режиме реального времени). Отображение в легенде графика сетевого интерфейса LAN означает, что график сетевого интерфейса включен. Для того, чтобы убрать график сетевого интерфейса необходимо нажать на кнопку него в легенде. Отображение в легенде графика сетевого интерфейса LAN означает, что график сетевого интерфейса выключен. Для того, чтобы добавить график сетевого интерфейса необходимо нажать на кнопку него в легенде.

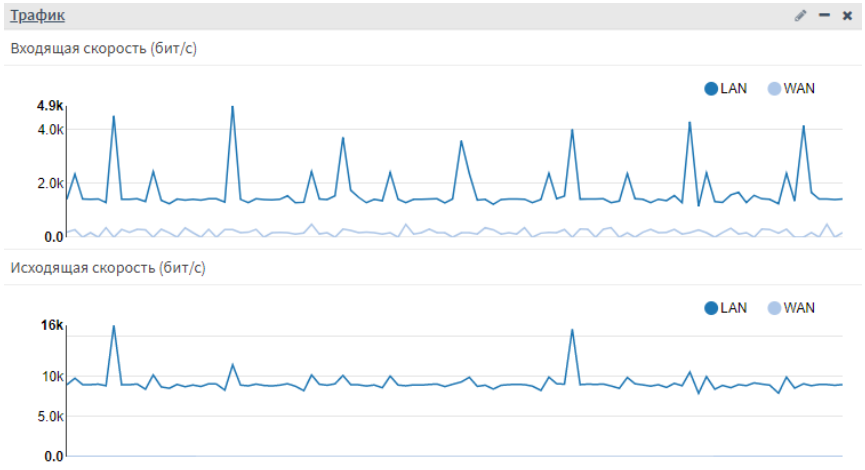


Рисунок 23 — Виджет «Трафик»

3. Раздел «Анализ»

Раздел «Анализ» состоит из следующих подразделов:

– Состояние;

– Анализ Netflow;

– Netflow;

– Настройки;

– Трафик.

3.1. Подраздел «Состояние»

Подраздел «Состояние» — это динамическое представление циклической базы данных (RRD), собранных системой, которое отражает общее состояние и производительность системы с течением времени.

3.1.1. Сокрытие области «Параметры»

Для сокрытия/отображения области «Параметры» необходимо нажать на кнопку  рядом с пунктом «Параметры».

3.1.2. Выбор категорий

Элементы области «Параметры» — выпадающий список, состоящий из следующих пунктов списка:

– пакеты;

– система (в котором отображается отчет об использовании памяти, mbufs, о состояниях, о загрузке процессора, о температуре процессора (когда доступна));

– трафик (в котором отображается зависимость объема сетевого трафика от времени для каждого интерфейса).

Пакеты

При выборе категории «Пакеты» любого интерфейса отобразится график зависимости количества входящих/исходящих пакетов (заблокированных и пропущенных по протоколам IPv4, IPv6) выбранного

интерфейса от времени (рисунок 24). Графики обновляются в режиме реального времени.

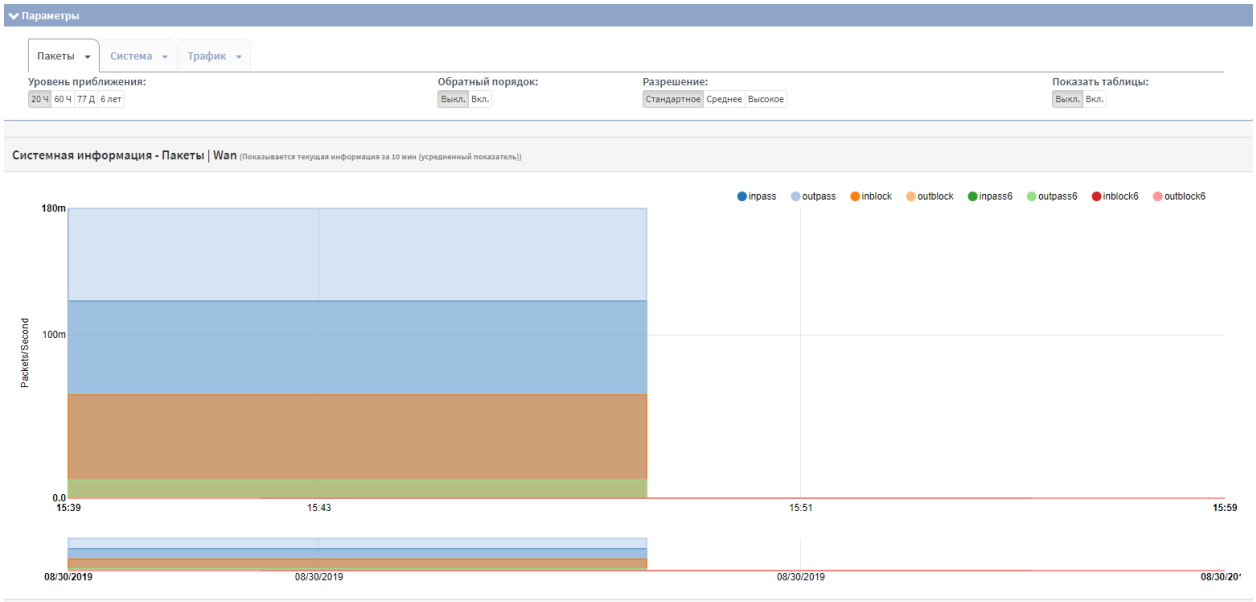


Рисунок 24 — Состояние: Пакеты

Система

При выборе категории «Система» любого системного параметра (память, mbufs, состояния, процессор, температура процессора) будет показан график зависимости использования выбранного параметра системы от времени (рисунок 25). Графики обновляются в режиме реального времени.

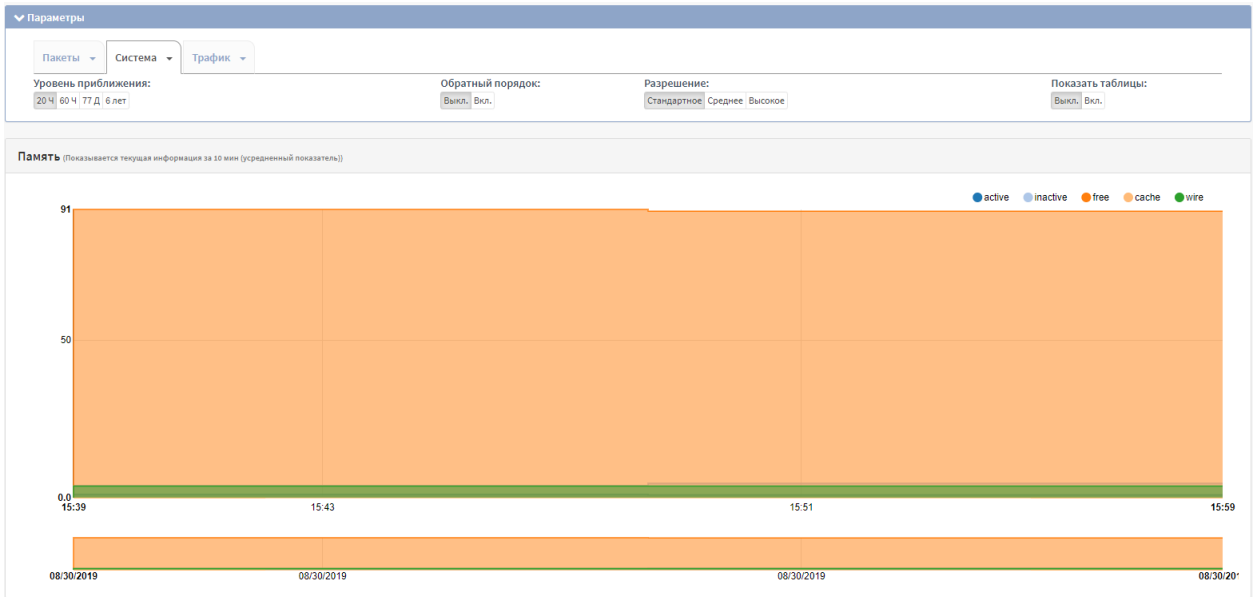


Рисунок 25 — Состояние: Система

Трафик

При выборе категории «Трафик» любого интерфейса будет показан график зависимости количества входящего/исходящего трафика (заблокированных и пропущенных по протоколам IPv4, IPv6) выбранного интерфейса от времени (рисунок 26). Графики обновляются в режиме реального времени.

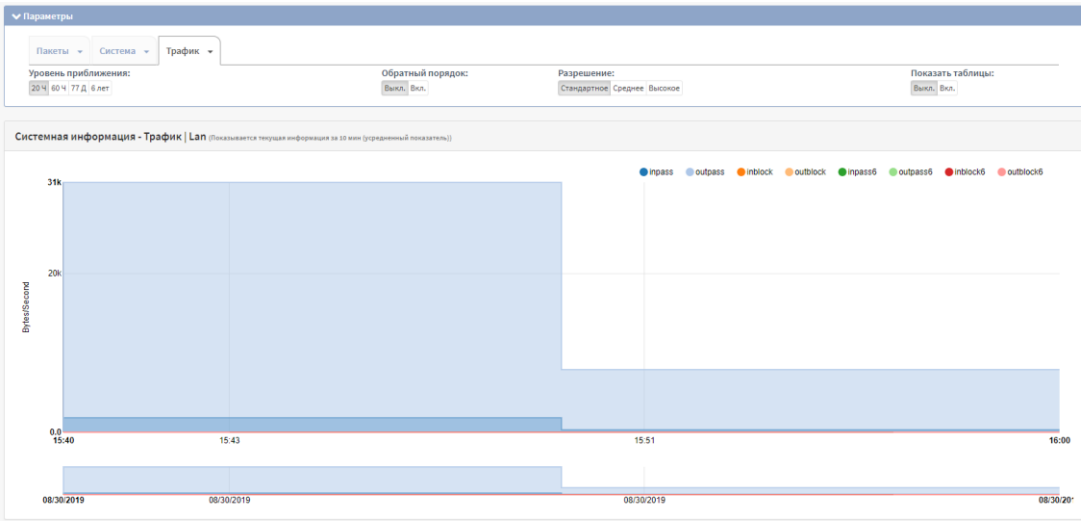


Рисунок 26 — Состояние: Трафик

3.1.3. Выбор уровня приближения

Из набора данных графика для анализа имеется возможность выбрать, за какой промежуток времени отображать данные. Чем больше промежуток времени, тем ниже максимальное разрешение. По умолчанию графики открываются с самым высоким доступным разрешением.

3.1.4. Функция «Обратный порядок»

При выборе «Обратный порядок», каждый нечетный набор данных меняет направление, это необходимо для потоков трафика, где имеется возможность создавать входящие и исходящие потоки в разных направлениях (рисунок 27).

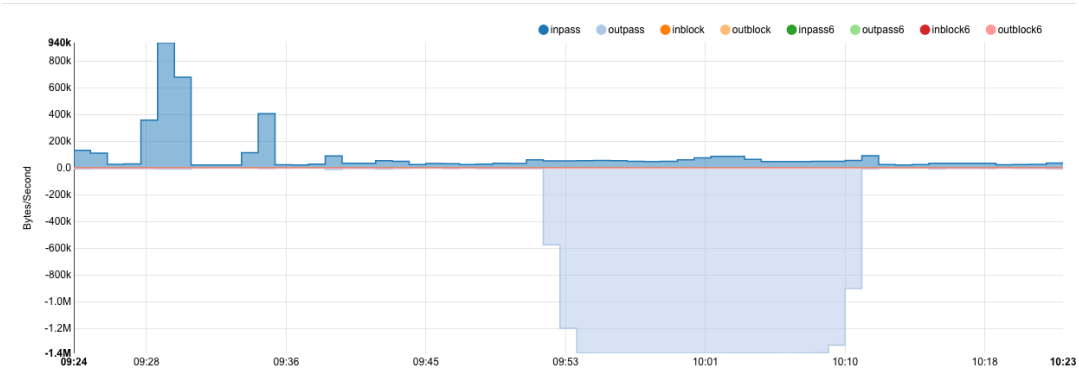


Рисунок 27 — Пример работы функции «Обратный порядок»

3.1.5. Разрешение графика

В параметре «Разрешение графика» возможен выбор максимального количества точек данных, которые будут отображаться на графике.

3.1.6. Функция «Показать таблицы»

По умолчанию таблицы данных скрыты. Чтобы включить их отображение необходимо нажать на кнопку переключатель «Показать таблицы» на параметр «вкл».

3.1.7. Название графика

Отображает название выбранного графика.

3.1.8. Фильтр меток

Фильтр меток используется для фильтрации данных, которые отображаются. Для отключения — необходимо нажать на кнопку один раз, для выбора только этого набора — два раза (рисунок 28). Соответственно inpass — входящий прошедший трафик, outpass — исходящий прошедший трафик, inblock — входящий заблокированный трафик, outblok — исходящий заблокированный трафик, inpass6 — входящий прошедший трафик IPv6, outpass6 — исходящий прошедший трафик IPv6, inblock6 — входящий заблокированный трафик IPv6, outblok6 — исходящий заблокированный трафик IPv6.

Рисунок 28 — Фильтр меток

3.1.9.Область графика

Область графика показывает полный график или только часть, которая выбрана в области масштабирования с более высокой детализацией.

3.1.10. Область масштабирования

Область масштабирования используется для выбора и увеличения масштаба на одной части графика, шкала адаптируются автоматически.

Для использования этой функции необходимо нажать на кнопку график и удерживать, перемещая курсор на другую часть области масштабирования. При этом область графика будет обновляться.

Выбор области масштабирования показан на рисунке (рисунок 29).

Рисунок 29 — Выбор области масштабирования

Результат увеличения масштаба показан на рисунке (рисунок 30).

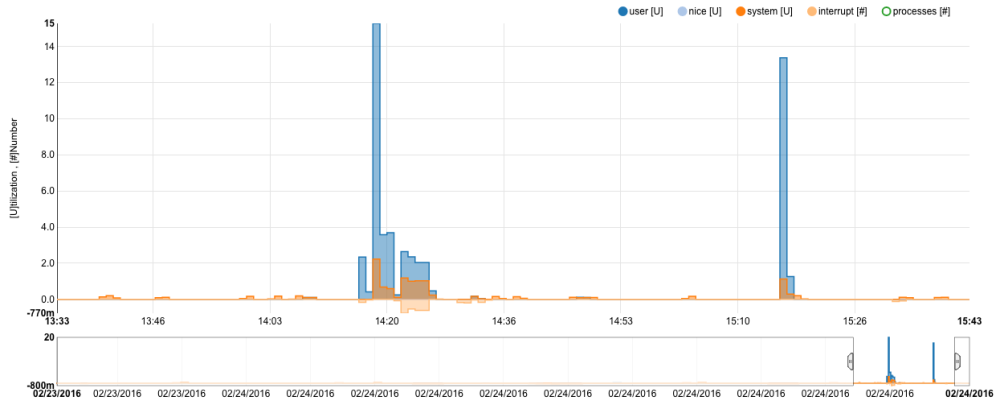


Рисунок 30 — Результат увеличения масштаба

3.1.11. Текущий вид — Общий

Если в пункте «Показать таблицы» выбрано значение «вкл.», то во вкладке «Текущий вид — Общий» будут отображаться:

– минимальное значение каждого набора данных;

– максимальное значение каждого набора данных;

– среднее значение каждого набора данных.

3.1.12. Текущий вид — Подробный

Если в пункте «Показать таблицы» выбрано значение «вкл.», то во вкладке «Текущий вид — Подробный» будет отобраться каждое значение, которое отображается на графике. Имеется возможность переключать режим отображения времени и даты, выбрав режим в поле «Режим отображения времени:». А также экспортировать данные в файл формата «*.csv», нажав кнопку «Загрузить в .CSV».

Экспортированный набор данных может использоваться для построения отчетов (рисунок 31).

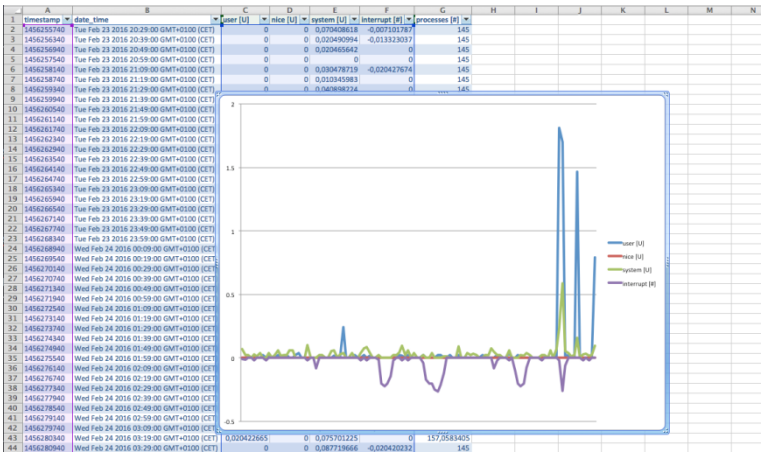


Рисунок 31 — Отчет на основе экспортированных данных

3.2. Подраздел «Анализ Netflow»

Подраздел «Анализ Netflow» разделен на три категории:

– всего;

– подробности;

– экспорт.

Netflow — технология мониторинга, разработанная Cisco для статистического анализа трафика. По Netflow передается информация о сетевых соединениях, включая IP-адрес и номер порта в рамках сетевого соединения.

3.2.1.Категория «Всего»

В категории «Всего» реализованы следующие функции:

– графическое представление соединений;

– визуальное отображение наилучшего использования для каждого интерфейса, как IP-адресов, так и портов;

– визуальное отображение входящего/исходящего трафика в пакетах и байтах.

Дополнительно имеется возможность просмотра данных о потоках, интерфейсах, трафике за следующие промежутки времени:

– последние 2 часа, средний показатель за 30 секунд;

– последние 8 часов, средний показатель за 5 минут;

– на прошлой неделе средний показатель за 1 час;

– в прошлом месяце, средний показатель за 24 часа;

– в прошлом году средний показатель за 24 часа;

Общие данные по интерфейсам

В категории «Всего» показаны графики потоков входящего и исходящего трафика для каждого сконфигурированного интерфейса.

Данный раздел позволяет отображать потоки трафика для всех сетевых интерфейсов в виде «Stacked» (график с накоплениями, по умолчанию) (рисунок 32), в виде «Stream» (потоковый график) или в расширенном виде «Expended» (график зависимости процента трафика выбранного сетевого интерфейса относительно общего трафика всех настроенных сетевых интерфейсов от времени).

Отображение в легенде графика сетевого интерфейса 

означает, что график сетевого интерфейса включен. Для того, чтобы убрать график сетевого интерфейса необходимо нажать на кнопку него в легенде. Отображение в легенде графика сетевого интерфейса 

означает, что график сетевого интерфейса выключен. При двойном нажатии выбирается отображение графика только этого интерфейса.

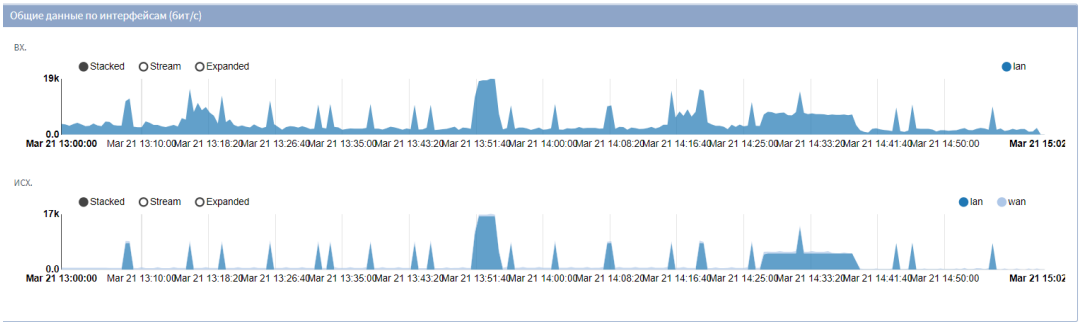


Рисунок 32 — Общие данные по интерфейсам

Самые используемые порты/источники

Круговая диаграмма (показанная справа на рисунке (рисунок 33)) отображает наиболее часто используемые порты назначения/службы в процентном соотношении. Нажатие по сектору круговой диаграммы позволяет открыть страницу с более детализированной информацией.

Круговая диаграмма по IP-адресам (показанная слева на рисунке (рисунок 33)) работает аналогично круговой диаграмме по портам и показывает наиболее часто используемые IP-адреса назначения.

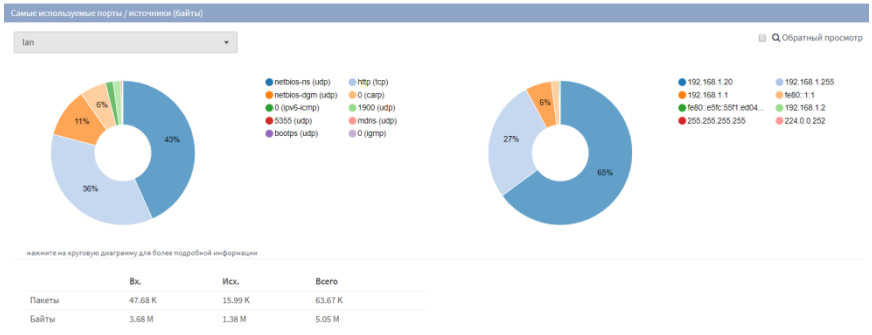


Рисунок 33 — Самые используемые порты/источники

3.2.2.Категория «Подробности»

В категории «Подробности» (рисунок 34) показан отчет по сетевой статистике в виде таблицы.

В рамках данного отчета отображается идентификатор компьютера, адрес и порт обращения данного компьютера, а также количество переданных данных в рамках данного взаимодействия.

Раздел позволяет ограничить вывод данных с помощью фильтров по диапазону дат, порту назначения и IP-адресу источника.

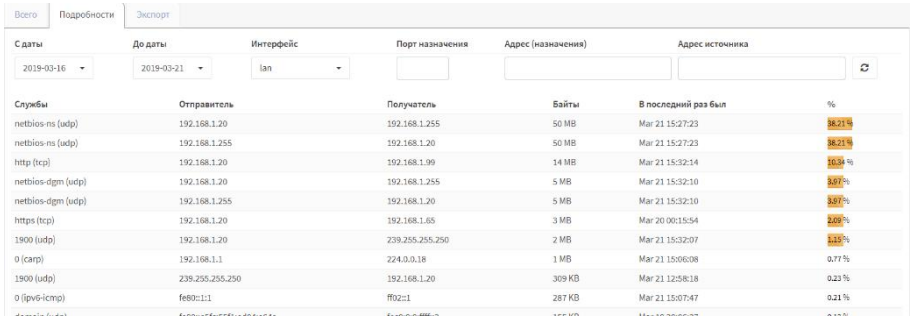


Рисунок 34 — Отчет сетевой статистики

3.2.3. Категория «Экспорт»

Категория «Экспорт» позволяет экспортировать данные в формате «*.csv» для последующего анализа. Для экспорта, необходимо выбрать набор:

– FlowSourceAddrTotals (суммарные данные по IP-адресу источника);

– FlowInterfaceTotals (суммарные данные по интерфейсу);

– FlowDstPortTotals (суммарные данные по порту назначения);

– FlowSourceAddrDetails (полные данные по IP-адресу источника).

Также необходимо выбрать разрешающую точность в секундах (300, 3600, 86400) и диапазон дат. Для экспорта необходимо нажать на кнопку «Экспорт» (рисунок 35).

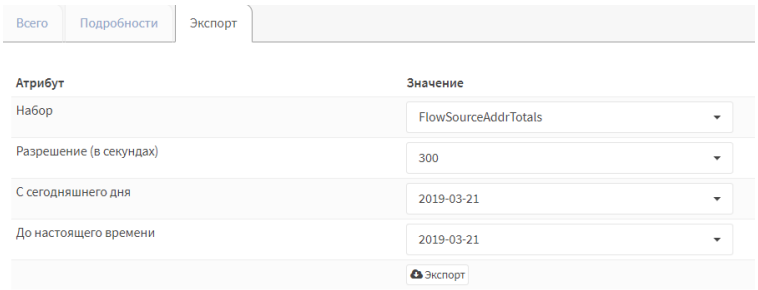


Рисунок 35 — Экспорт данных

3.3. Подраздел «Netflow»

3.3.1. Категория «Захват»

В категории «Захват» (рисунок 36) возможна настройка сервиса Netflow.

В поле «Интерфейсы LAN» необходимо выбрать все интерфейсы, с которых необходимо собирать данные; в большинстве случаев выбираются все доступные интерфейсы.

В поле «Интерфейсы WAN» необходимо выбрать WAN-интерфейсы, чтобы избежать повторного подсчета транслированного трафика.

Для возможности локального анализа с использованием внутреннего трафика, необходимо установить флажок напротив поля «Захватывать внутренний трафик».

Далее необходимо выбрать версию Netflow 5 или 9 в поле «Версия». Версия 5 не поддерживает IPv6.

Для передачи данных Netflow на внешние сервисы необходимо добавить получателей в поле «Получатели» (IP-адрес: порт, затем нажать клавишу «ENTER»). Локальный IP-адрес будет добавлен автоматически, если стоит флажок в поле «Захватывать внутренний трафик».

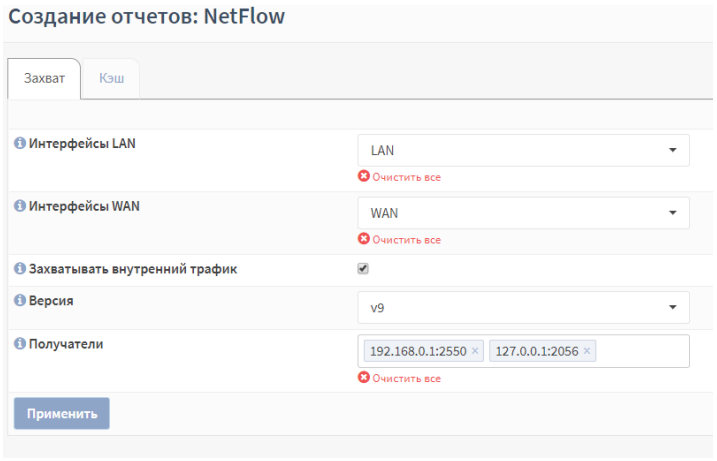


Рисунок 36 — Настройка Netflow

3.3.2.Категория «Кэш»

В категории «Кэш» отображаются потоки данных в виде таблицы, в которой присутствует информация о названии потока данных, интерфейсе, количестве получателей/отправителей и количестве пакетов (рисунок 37).

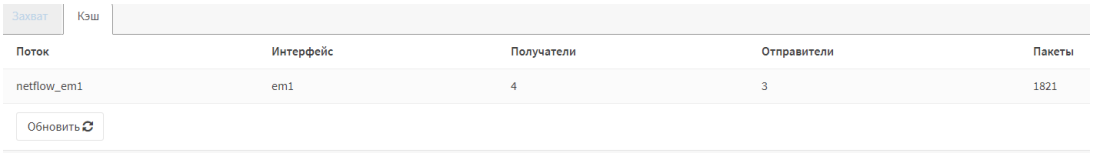


Рисунок 37 — Netflow: кэш

3.4. Подраздел «Настройки»

Циклическая база данных (RRD) — набор динамических данных (т.е. последовательность замеров некоторого изменяющегося во времени параметра). Примером таких данных может служить температура, загрузка процессора, сетевой трафик. Все данные хранятся в циклической базе данных, размер которой остаётся неизменным.

Настройка циклической базы данных осуществляется в подразделе «Настройки». Данный подраздел позволяет включить серверную обработку для построения аналитических графиков. Для этого необходимо нажать на флажок напротив поля «Циклическая база данных». А также данный раздел позволяет очистить данные аналитических графиков, очистить данные Netflow, восстановить данные Netflow, нажав соответствующие кнопки (рисунок 38).

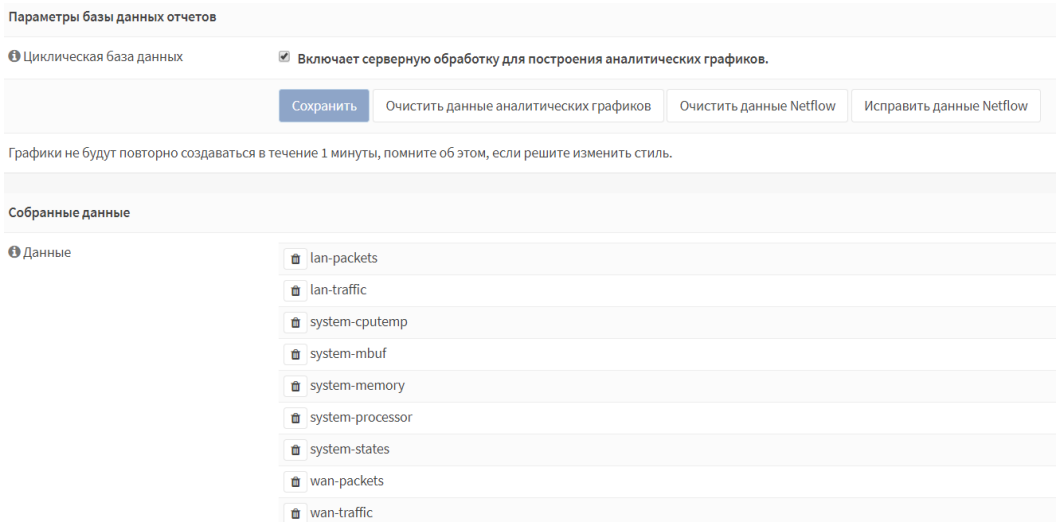


Рисунок 38 — Настройка циклической базы данных

3.5. Подраздел «Трафик»

Подраздел «Трафик» (рисунок 39) позволяет увидеть текущую загрузку всех сетевых интерфейсов в режиме реального времени. Фильтр сетевых интерфейсов используется для фильтрации данных в соответствии с выбранным сетевым интерфейсом. Отображение в легенде графика сетевого

интерфейса LAN означает, что график сетевого интерфейса включен. Для того, чтобы убрать график сетевого интерфейса необходимо нажать на кнопку него в легенде. Отображение в легенде графика сетевого интерфейса LAN означает, что график сетевого интерфейса выключен. При двойном нажатии выбирается отображение графика только этого интерфейса. Также отображается весь трафик в виде таблицы (по выбранным интерфейсам и направлению), в которой отображаются данные о пропускной способности входящего/исходящего трафика, данные об отправителе, полное значение в битах входящего/исходящего трафика.

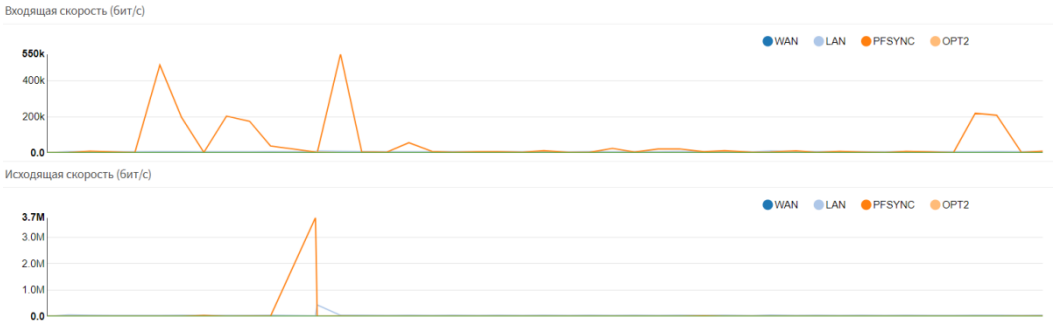


Рисунок 39 — Трафик

4. Раздел «Межсетевой экран»

Раздел «Межсетевой экран» состоит из следующих подразделов:

- подраздел «Псевдонимы»;
- подраздел «Правила»;
- подраздел «NAT»;
- подраздел «Ограничение трафика»;
- подраздел «Группы»;
- подраздел «Виртуальные IP-адреса»;
- подраздел «Настройки»;
- подраздел «Журналы»;
- подраздел «Диагностика».

4.1. Подраздел «Псевдонимы»

Система позволяет создавать псевдонимы – именованные множества сетей, IP-адресов или портов, которые могут использоваться как один объект в различных разделах межсетевого экрана.

4.1.1. Типы псевдонимов

ПК «InfoWatch ARMA Industrial Firewall» предлагает к использованию следующие типы псевдонимов:

- порты;
- таблицы URL-адресов (IP-адресов);
- URL (IP-адреса);
- GeoIP;
- хосты;
- сети;
- внешний (расширенный).

Порты

Порты могут быть указаны в качестве одного числа или диапазона, используя двоеточие. Например, чтобы добавить диапазон от 20 до 25, необходимо ввести 20:25.

Таблицы URL-адресов (IP-адресов)

Таблицы URL-адресов используются для получения списка IP-адресов с удаленного сервера URL страницы.

URL (IP-адреса)

URL-адреса используется для получения IP-адреса с удаленного сервера URL страницы.

GeoIP

С помощью псевдонима GeoIP возможно выбрать одну или несколько стран, или целые континенты, чтобы в последующем их заблокировать или разрешить. Необходимо установить флажок «Название континента (выбрать все)», чтобы выбрать все страны в данном регионе (рисунок 40).

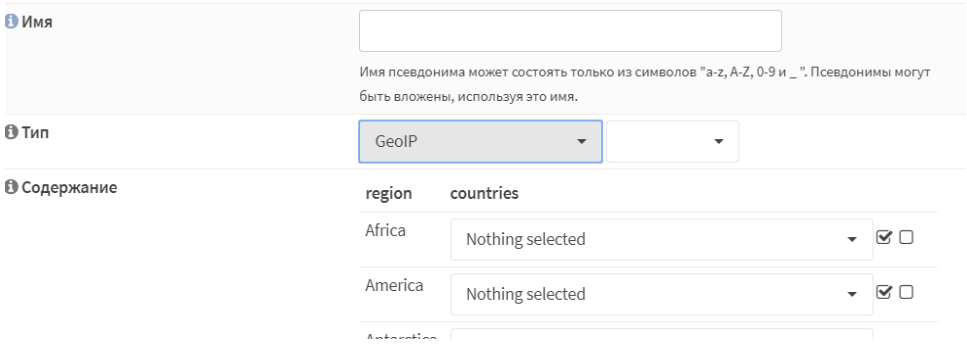


Рисунок 40 — Применение псевдоним GeoIP

Хосты

При создании псевдонимов тип «Хост» возможен ввод любого количества хостов. Однако, необходимо указать для каждого IP-адрес или полностью определенное имя домена (FQDN). FQDN-имена хостов периодически преобразовываются и обновляются. Если DNS-запрос возвращает множественные IP-адреса, они все используются.

Сети

Сети задаются в формате CIDR. Для определения псевдонима необходимо задать сеть и указать её маску CIDR. Маска /32 означает один IPv4-хост, /128 означает один IPv6-хост, /24 означает представление маски в десятичной форме (255.255.255.0), /64 означает нормальную IPv6-сеть и т. д. Также могут быть указаны FQDN-имена хостов с помощью маски /32 для IPv4 или /128 для IPv6.

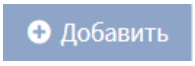
Внешний (расширенный)

Используется для задания версии протокола IP.

4.1.2. Таблица псевдонимов

В таблице псевдонимов отображаются все псевдонимы со следующими параметрами:

- название;
- тип;
- описание;
- значение.

В таблице представлена возможность создавать или редактировать псевдоним. Для редактирования необходимо нажать на кнопку  напротив созданного ранее псевдонима. Для создания нового псевдонима необходимо нажать на кнопку 

.

4.1.3. Редактирование/создание псевдонима

В поле «Включить» необходимо поставить флажок для включения псевдонима. В поле «Имя» необходимо ввести название псевдонима. В поле «Тип» необходимо выбрать тип псевдонима (типы псевдонимов описаны в подразделе 4.1.1). В поле «Содержание» ввести содержание псевдонима. В поле «Описание» необходимо ввести описание псевдонима и нажать кнопку «Сохранить», после чего нажать кнопку «Применить изменения» (рисунок 41).

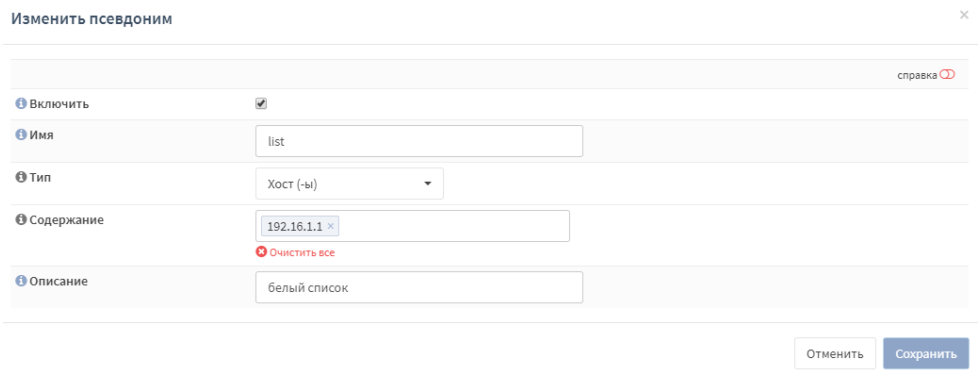


Рисунок 41 — Редактирование псевдонима

4.2. Подраздел «Правила»

Для удобства, в веб-интерфейсе правила межсетевого экрана задаются отдельно для каждого из сетевых интерфейсов, настроенных в ПК «InfoWatch ARMA Industrial Firewall». Правила располагаются в виде списка с приоритетом от верхнего к нижнему. Иными словами, сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз.

Если сетевой пакет удовлетворяет критериям правила, то к пакету применяется действие, заданное в правиле. Если к пакету уже применено правило, то обработка пакета сетевым экраном прекращается. Такой пакет далее не будет сверяться с оставшимися правилами в списке.

Действия «блокировать (block)» и «отклонить (reject)» предполагают блокирование пакета межсетевым экраном (причем в первом случае, удаленная сторона никак не оповещается о свершившейся блокировке). Действие пропустить (pass) разрешает прохождение пакета через межсетевой экран.

Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется (т.е. отбрасывается без индикации удаленной стороне).

4.2.1. Категория «Общие»

В категории «Общие» приведена таблица правил, которые могут применяться как ко всем сетевым интерфейсам, так и к выбранным. Таблица содержит следующие данные (рисунок 42):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку));

– протокол, к которому применяется правило;

– данные отправителя;

– порт;

– шлюз;

– расписание;

– описание правила.

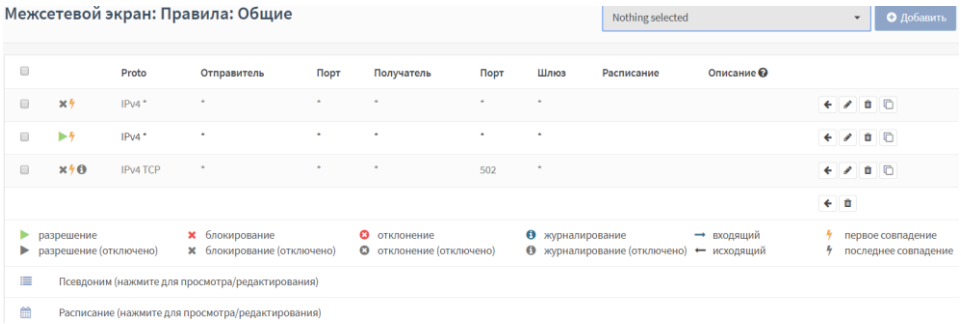


Рисунок 42 — Межсетевой экран: Правила: Общие

Для редактирования существующего правила, необходимо нажать на кнопку напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку Добавить в категории «Общие».

При редактировании правила в поле «Действие» необходимо выбрать действие правила (разрешение, блокирование, отклонение). При необходимости отключить правило - установить флажок напротив поля «Отключить». При необходимости сразу применять действие к пакету, который соответствует этому правилу (вне зависимости от приоритета правила) необходимо установить флажок напротив пункта «Быстрая проверка». В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Версии TCP/IP»

необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 43).

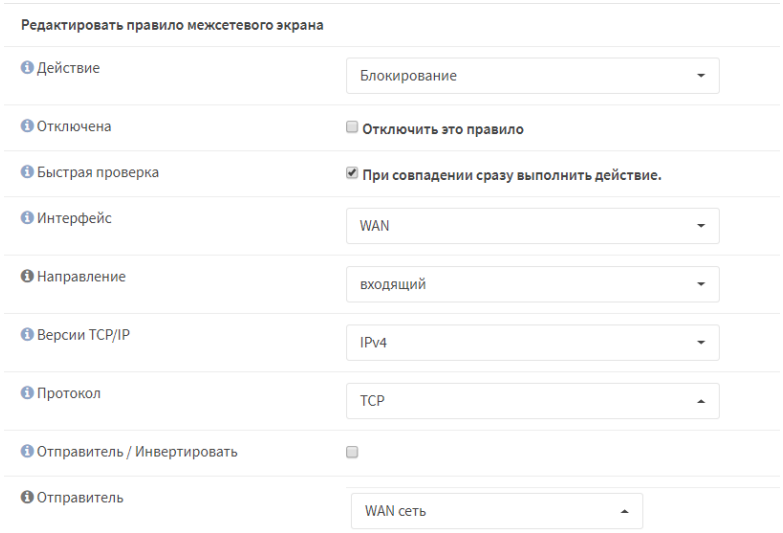


Рисунок 43 — Межсетевой экран: Правила: Общие (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Журналирование» необходимо поставить флажок, если необходимо журналирование пакетов, которые будут соответствовать редактируемому правилу. В поле «Диапазон портов получателя» необходимо указать порт получателя или диапазон портов. Поле «Категория» позволяет указать категорию группы правил (необязательно). В поле «Описание» необходимо ввести описание правила (рисунок 44).

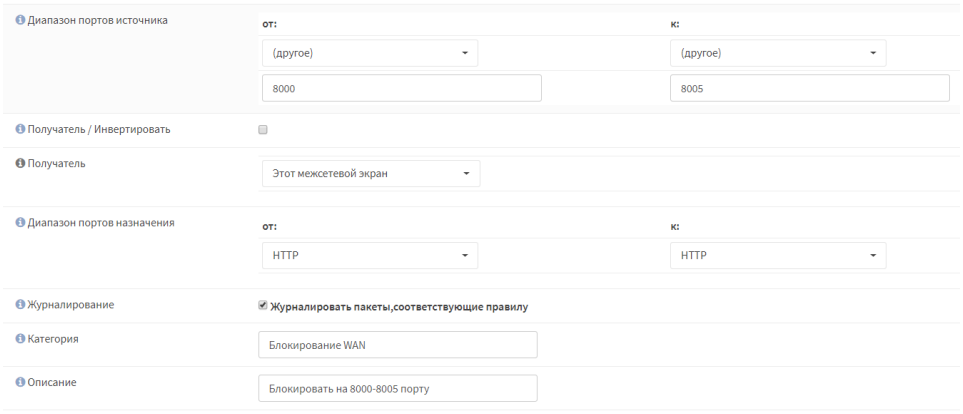


Рисунок 44 — Межсетевой экран: Правила: Общие (редактирование, часть 2)

В разделе «Дополнительные возможности» присутствуют дополнительные параметры настройки правила. В поле «ОС источника» имеется возможность выбрать тип ОС (только при выборе ранее TCP протокола). В поле «Не синхронизовать XMLRPC» необходимо поставить флажок, если необходимо отключить синхронизацию данного правила на ведущем устройстве с другими участниками отказоустойчивого кластера CARP. При необходимости выбора времени работы правила в поле «Расписание» необходимо выбрать настроенное расписание (для настройки расписания необходимо перейти в поле «Межсетевой экран» - «Настройки» - «Расписание»). Для того чтобы правило работало все время, необходимо выбрать «отсутствует». В поле «Шлюз» необходимо выбрать шлюз при использовании маршрутизации (значение «по умолчанию» используется в случае необходимости использования системной таблицы маршрутизации) (рисунок 45).

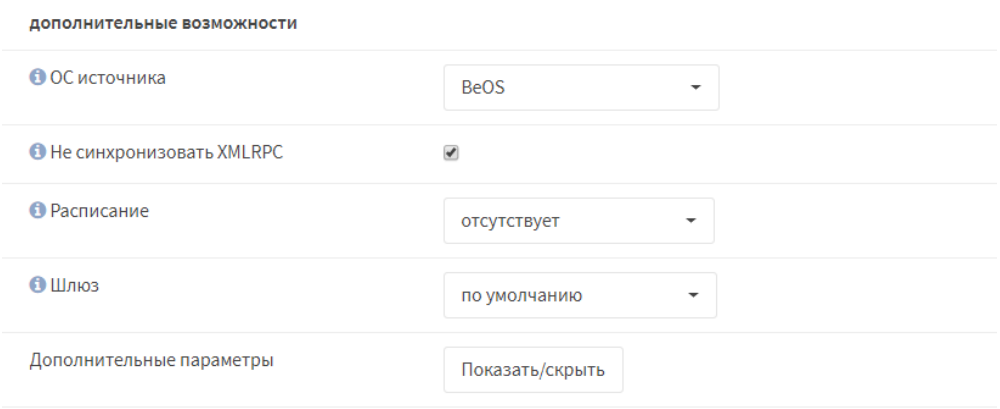


Рисунок 45 — Межсетевой экран: Правила: Общие (редактирование, часть 3)

При нажатии на кнопку «Показать/скрыть» напротив пункта «Дополнительные параметры» появятся дополнительные поля настройки правила (рисунок 46). В поле «Разрешить параметры» необходимо установить флажок для разрешения пакетов с параметрами IP, которые блокируются по умолчанию. В поле «Отключить ответ» необходимо установить флажок в случае необходимости отключения автоматически созданного ответа для этого правила. В поле «Установить приоритет» необходимо установить приоритет пакетов, которые будут попадать под это правило, если это необходимо. В поле «Совпадение приоритета» необходимо выбрать приоритет, который будет совпадать с приоритетом пакета. Поле «Установить локальный тег» позволяет вписать метку (в пакет также необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Макс. состояний» необходимо ввести максимальное число записей состояний, которые может создать это правило. В поле «Макс. узлов-источников» необходимо ввести максимальное количество уникальных хостов-источников. В поле «Макс. установленных соединений» необходимо ввести максимальное количество установленных соединений для хоста. В поле «Макс. состояний-источников» необходимо ввести максимальное количество записей состояний для хоста. В поле «Макс. новых соединений» необходимо ввести максимальное количество новых соединений для хоста за секунду. В поле «Тайм-аут состояния» необходимо ввести состояние тайм-аута в секундах. В поле «TCP-флаги» необходимо выбрать флаги, которые должны быть установлены и которые не должны быть установлены для этого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync в кластере высокой доступности. В поле «Тип состояния» необходимо выбрать тип механизма отслеживания состояний:

– Keep state (используется для отслеживания состояния подключения);

– Sloppy state (работает как keep state, но не проверяет порядковые номера);

– Synproxy state (проксирует входящие соединения TCP для защиты серверов от Spoofed TCP и SYN-flood атак, этот тип включает в себя комбинацию функций keep state и modulate state);

– Отсутствует (невозможно использовать механизмы отслеживания состояний, если используется функция управления очередями).

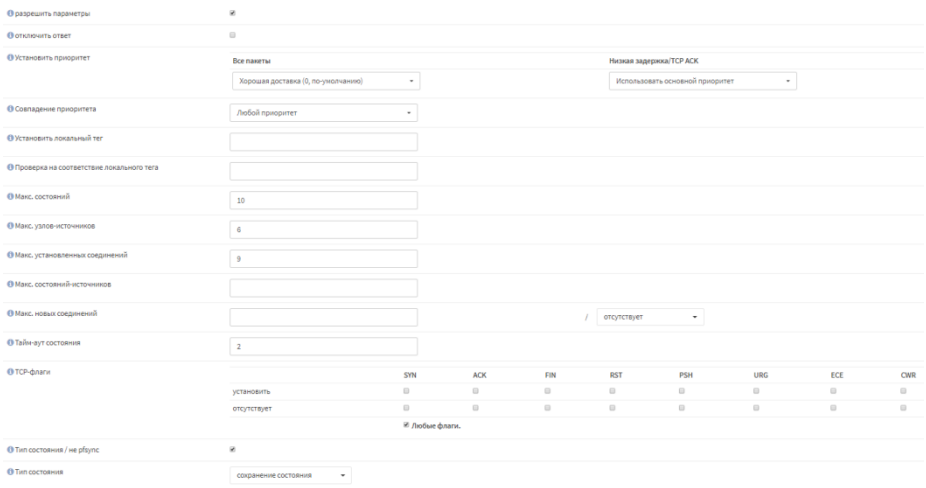


Рисунок 46 — Межсетевой экран: Правила: Общие (редактирование, часть 4)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.2.2.Категория «[Название интерфейса]»

В категории «[Название интерфейса]» приведена таблица правил, которые применяются к сетевому интерфейсу «[Название интерфейса]», где [Название интерфейса] – это имя интерфейса, установленное при ассоциации этого сетевого интерфейса с физическим сетевым интерфейсом. Таблица правил включает в себя следующие данные (рисунок 47):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку));

– протокол, к которому применяется правило;

– данные отправителя;

– порт;

– шлюз;

– расписание;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

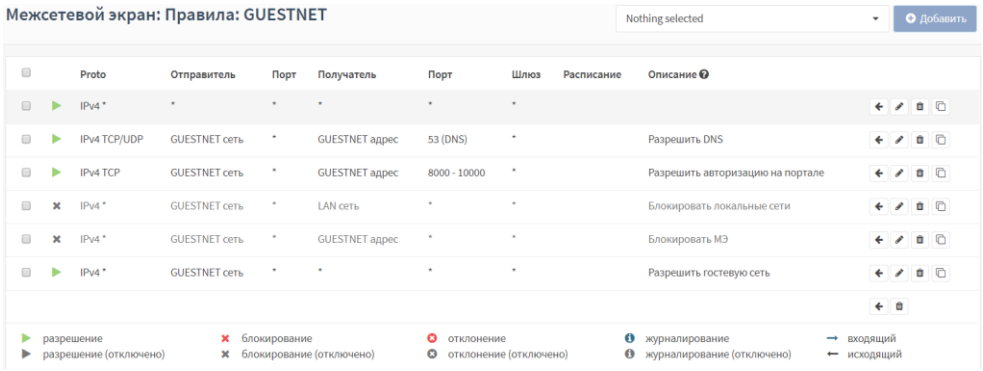


Рисунок 47 — Межсетевой экран: Правила: [Название интерфейса]

Для редактирования существующего правила необходимо нажать на кнопку напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку Добавить в категории «[Название интерфейса]».

При редактировании правила в поле «Действие» необходимо выбрать действие правила (разрешение, блокирование, отклонить), необходимо установить флажок напротив поля «Отключить» для выключения редактируемого правила. В поле «Интерфейс» необходимо выбрать сетевые

интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 48).

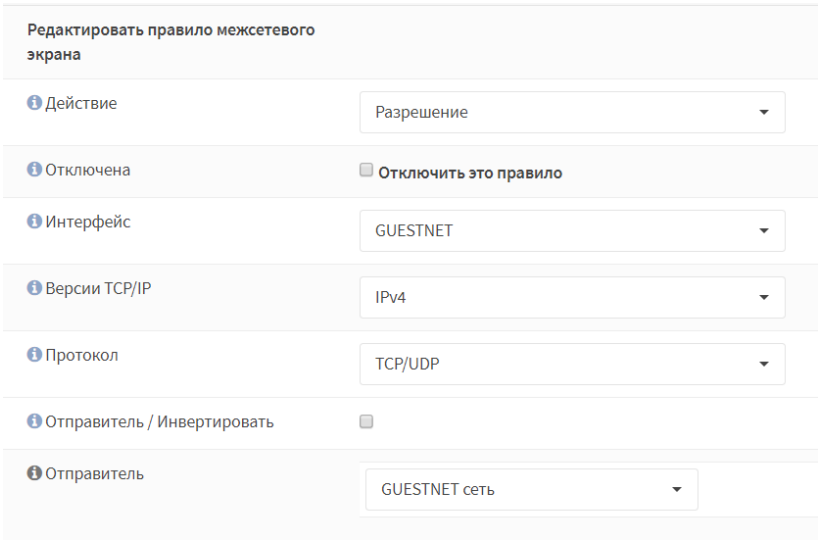


Рисунок 48 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Журналирование» необходимо поставить флажок, если необходимо журналирование пакетов, которые будут соответствовать редактируемому правилу. В поле «Диапазон портов получателя» необходимо указать порт

получателя или диапазон портов. Поле «Категория» позволяет указать категорию группы правил (необязательно). В поле «Описание» необходимо ввести описание правила (рисунок 49).

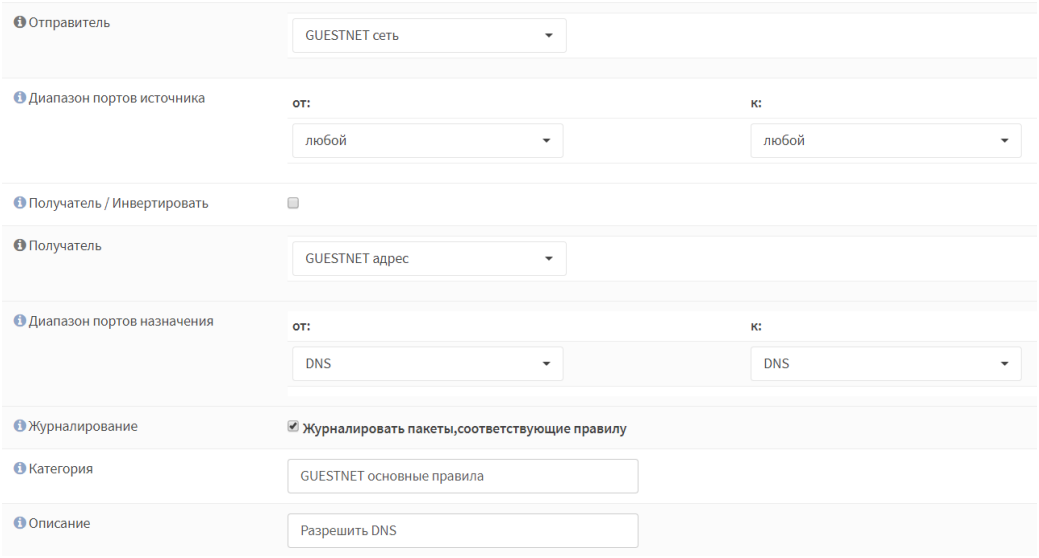


Рисунок 49 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 2)

В разделе «Дополнительные возможности» присутствуют дополнительные параметры настройки правила. В поле «ОС источника» имеется возможность выбрать тип ОС (только при выборе ранее TCP протокола). В поле «Не синхронизовать XMLRPC» необходимо поставить флажок, если необходимо отключить синхронизацию данного правила на ведущем устройстве с другими участниками отказоустойчивого кластера CARP. При необходимости выбора времени работы правила в поле «Расписание» необходимо выбрать настроенное расписание (для настройки расписания необходимо перейти в поле «Межсетевой экран» - «Настройки» - «Расписание»). Для того чтобы правило работало все время, необходимо выбрать «отсутствует». В поле «Шлюз» необходимо выбрать шлюз при использовании маршрутизации (значение «по умолчанию» используется в случае необходимости использования системной таблицы маршрутизации) (рисунок 50).

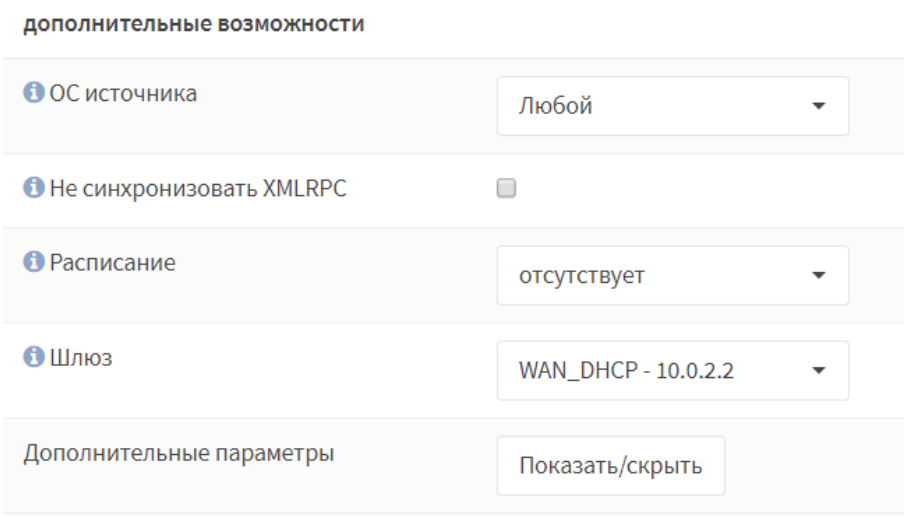


Рисунок 50 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 3)

При нажатии на кнопку «Показать/скрыть» напротив пункта «Дополнительные параметры» появятся дополнительные поля (рисунок 51). В поле «Разрешить параметры» необходимо установить флажок для разрешения пакетов с параметрами IP, которые блокируются по умолчанию. В поле «Отключить ответ» необходимо установить флажок в случае необходимости отключения автоматически созданного ответа для этого правила. В поле «Установить приоритет» необходимо установить приоритет пакетов, которые будут попадать под это правило, если это необходимо. В поле «Совпадение приоритета» необходимо выбрать приоритет, который будет совпадать с приоритетом пакета. Поле «Установить локальный тег» позволяет вписать метку (в пакет также необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Макс. состояний» необходимо ввести максимальное число записей состояний, которые может создать это правило. В поле «Макс. узлов-источников» необходимо ввести максимальное количество уникальных хостов-источников. В поле «Макс. установленных соединений» необходимо ввести максимальное количество установленных

соединений для хоста. В поле «Макс. состояний-источников» необходимо ввести максимальное количество записей состояний для хоста. В поле «Макс. новых соединений» необходимо ввести максимальное количество новых соединений для хоста за секунду. В поле «Тайм-аут состояния» необходимо ввести состояние тайм-аута в секундах. В поле «TCP-флаги» необходимо выбрать флаги, которые должны быть установлены и не должны быть установлены для этого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync в кластере высокой доступности. В поле «Тип состояния» необходимо выбрать тип механизма отслеживания состояний:

– Keep state (используется для отслеживания состояния подключения);

– Sloppy state (работает как keep state, но не проверяет порядковые номера);

– Synproxy state (проксирует входящие соединения TCP для защиты серверов от Spoofed TCP и SYN-flood атак, этот тип включает в себя комбинацию функций keep state и modulate state);

– Отсутствует (невозможно использовать механизмы отслеживания состояний, если используется функция управления очередями).

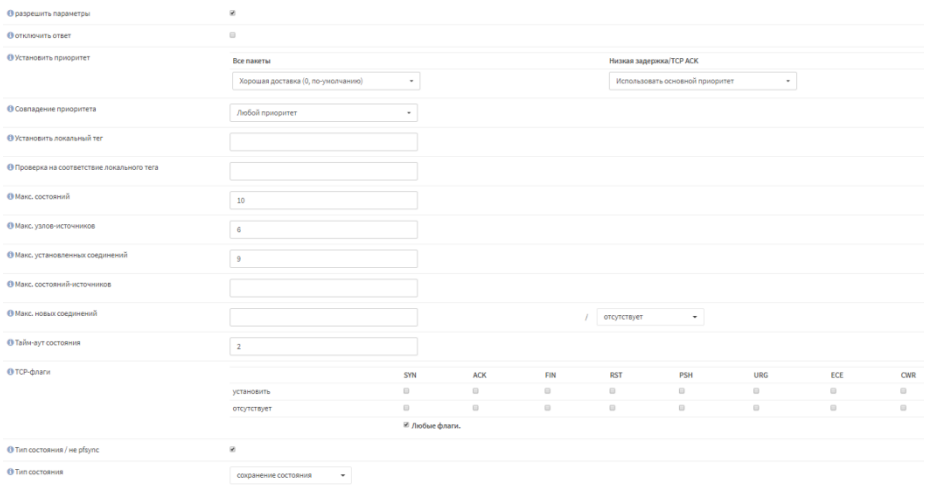


Рисунок 51 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 4)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

4.3. Подраздел «NAT»

4.3.1. Категория «Переадресация портов»

Механизм NAT позволяет множеству компьютеров работать с внешней сетью под одним внешним (иногда называемым «белым») IP-адресом. С другой стороны, возможность обращения к компьютерам внутренней сети из внешней сети при таком использовании и требует дополнительной настройки, которая известна как «переадресация портов».

В категории «Переадресация портов» приведена таблица правил, которые применяются для переадресации портов. Таблица содержит в себе следующие данные (рисунок 52):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку));

– интерфейс;

– протокол, к которому применяется правило;

– данные отправителя (адрес, порты);

– данные получателя (адрес, порты);

– данные NAT (адрес, порты);

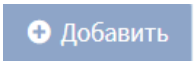
– порты;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как

только совпадение найдено, выполняется действие, присвоенное данному правилу).

Рисунок 52 — Межсетевой экран: NAT: Переадресация портов

Для редактирования существующего правила, необходимо нажать на кнопку  напротив правила. Для того, чтобы создать новое правило, необходимо нажать на кнопку 

в категории «Переадресация портов».

При редактировании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 53).

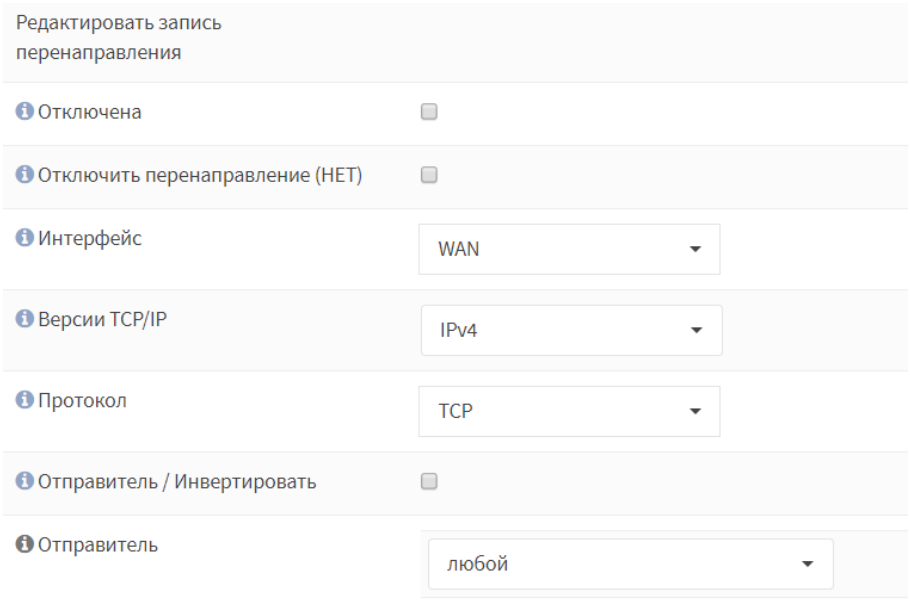


Рисунок 53 — Межсетевой экран: NAT: Переадресация портов (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Диапазон портов назначения» необходимо указать порт получателя или диапазон портов (рисунок 54).

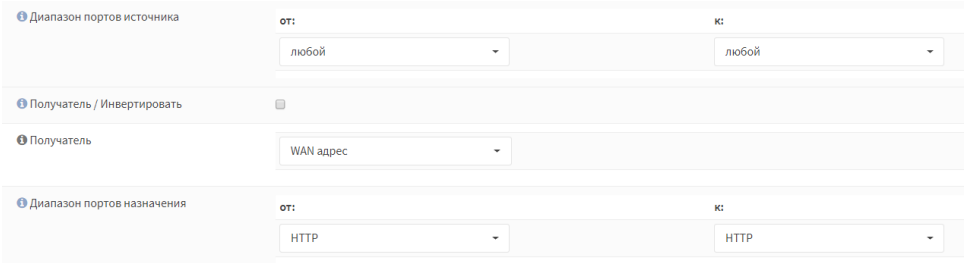


Рисунок 54 — Межсетевой экран: NAT: Переадресация портов (редактирование, часть 2)

В поле «Перенаправление целевого IP-адреса» необходимо ввести внутренний IP-адрес сервера для перенаправления портов. В поле «Целевой порт перенаправления» необходимо ввести порт компьютера с введенным в

поле «Перенаправление целевого IP-адреса» IP-адресом. В поле «Параметры пула:» необходимо выбрать параметры пула:

– Циклический: перебирает транслируемые IP-адреса;

– Случайный: выбирает случайный адрес из пула транслируемых IP-адресов;

– Хеш источника: использует хеш адреса источника для определения транслируемого IP-адреса и проверяет, чтобы IP-адрес перенаправления для указанного источника всегда был один и то же;

– Битовая маска: применяет маску подсети;

– Фиксированные адреса: параметр может использоваться со случайным и циклическим типами, чтобы конкретный IP-адрес источника преобразовывался в одинаковый транслируемый адрес.

В поле «Описание» необходимо ввести описание правила. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенного для другого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync. В поле «Зеркальный NAT» необходимо выбрать состояние (включить, отключить, использовать системное значение по умолчанию). В поле «Связные правила фильтрации» необходимо выбрать связные правила фильтрации (рисунок 55).

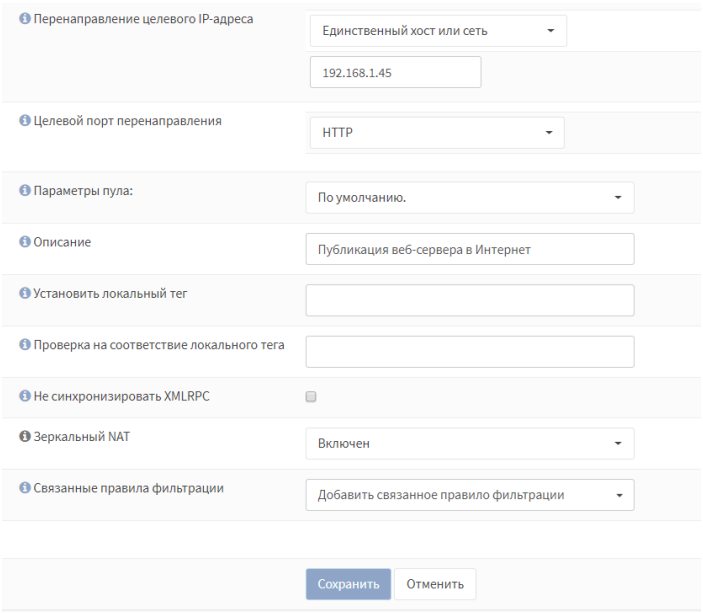


Рисунок 55 — Межсетевой экран: NAT: Переадресация портов (редактирование, часть 3)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений.

4.3.2. Категория «Один к одному»

В категории «Один к одному» приведена таблица правил, которые могут применяться для трансляции сетевых адресов в режиме «один к одному». Таблица содержит следующие данные (рисунок 56):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет (для отключения/включения правила необходимо нажать на кнопку));

– интерфейс;

– внешний IP-адрес;

– внутренний IP-адрес;

– IP-адрес назначения;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как

только совпадение найдено, выполняется действие, присвоенное данному правилу).

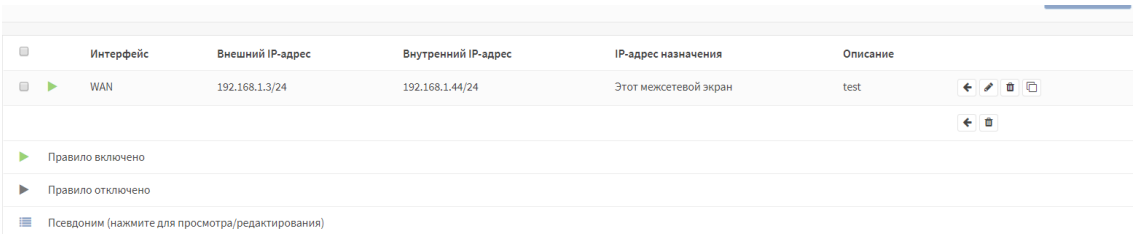
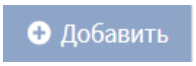


Рисунок 56— Межсетевой экран: NAT: Один к одному

Для редактирования существующего правила необходимо нажать на кнопку  напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку 

в категории «Один к одному».

При редактировании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле тип необходимо выбрать BINAT (по умолчанию) или NAT. Если сети одного размера, обычно используется BINAT. Правило BINAT определяет двунаправленное отображение между внешней и внутренней сетью и может быть использовано в обоих направлениях, NAT применяется только в одном направлении. В поле «Внешняя сеть» необходимо указать начальный адрес внешней подсети для трансляции в режиме «1:1». В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо ввести внутреннюю подсеть для отображения режима «1:1». В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо ввести получателя, с которым будет использоваться режим «1:1». В поле «Описание» необходимо ввести описание данного правила. В поле «Зеркальный NAT» необходимо выбрать

состояние (включен, отключить, использовать системное значение по умолчанию) (рисунок 57).

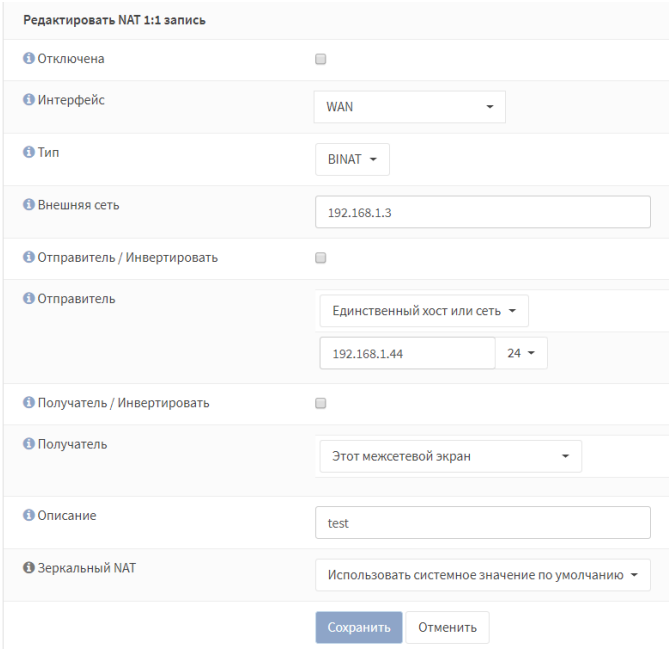


Рисунок 57 — Межсетевой экран: NAT: Один к одному

(редактирование)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений.

4.3.3. Категория «Исходящий»

Категория «Исходящий» позволяет выбрать один из четырех режимов работы исходящего NAT:

– автоматическое создание правил исходящего NAT (нельзя использовать правила, созданные вручную);

– 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 отключен).

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 (рисунок 58).

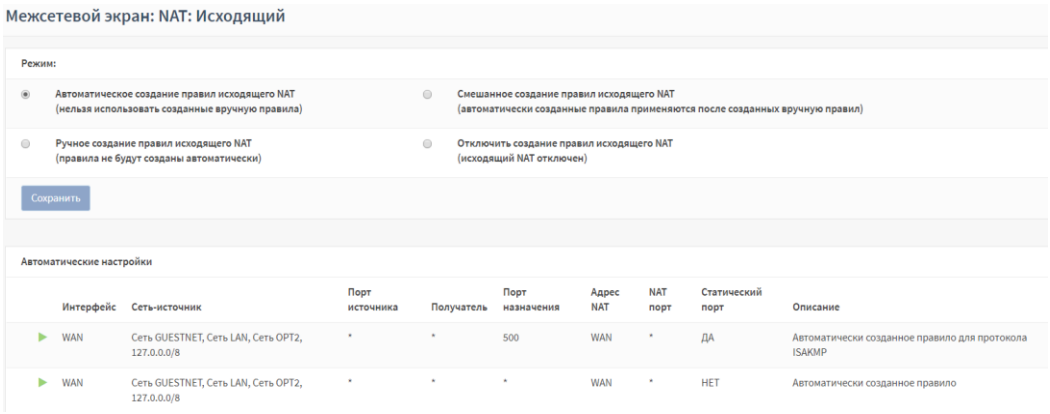
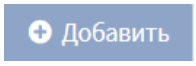


Рисунок 58 — Автоматический режим создания правил исходящего NAT

Ручное создание правил исходящего NAT

Режим ручного создания правил исходящего NAT позволяет вручную создавать правила исходящего NAT. Для этого необходимо нажать на кнопку 

.

При редактировании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Не использовать NAT» необходимо поставить флажок, если необходимо отключить NAT. В поле «Интерфейс» необходимо выбрать сетевые интерфейс, на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Инвертировать источник» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «IP-адрес назначения» необходимо ввести адрес исходной сети для преобразования с

помощью исходящего NAT. В поле «Порт назначения» необходимо выбрать порт получателя (рисунок 59).

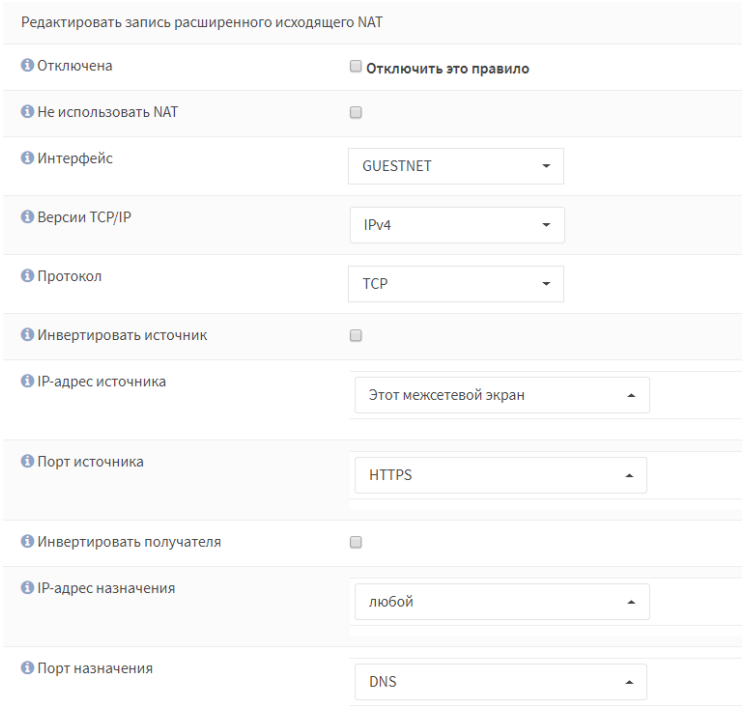


Рисунок 59 — Ручной режим создания правил исходящего NAT (часть 1)

В поле «Транслируемый IP-адрес/целевой IP-адрес» необходимо ввести IP-адрес для использования другого IP-адреса (не выбранного интерфейса). Необходимо установить флажок напротив поля «Журналирование» для включения журналирования событий правила. В поле «Статический порт» необходимо установить флажок для использования статического порта. В поле «Параметры пула:» необходимо выбрать параметры пула:

– Циклический: перебирает транслируемые IP-адреса;

– Случайный: выбирает случайный адрес из пула транслируемых IP-адресов;

– Хеш источника: использует хеш адреса источника для определения транслируемого IP-адреса и проверяет, чтобы IP-адрес перенаправления для указанного источника всегда был один и то же;

– Битовая маска: применяет маску подсети;

– Фиксированные адреса: параметр может использоваться со случайным и циклическим типами, чтобы конкретный IP-адрес источника преобразовывался в одинаковый транслируемый адрес.

Поле «Установить локальный тег» позволяет вписать метку (в пакет необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync. В поле «Описание» необходимо ввести описание правила (рисунок 60).

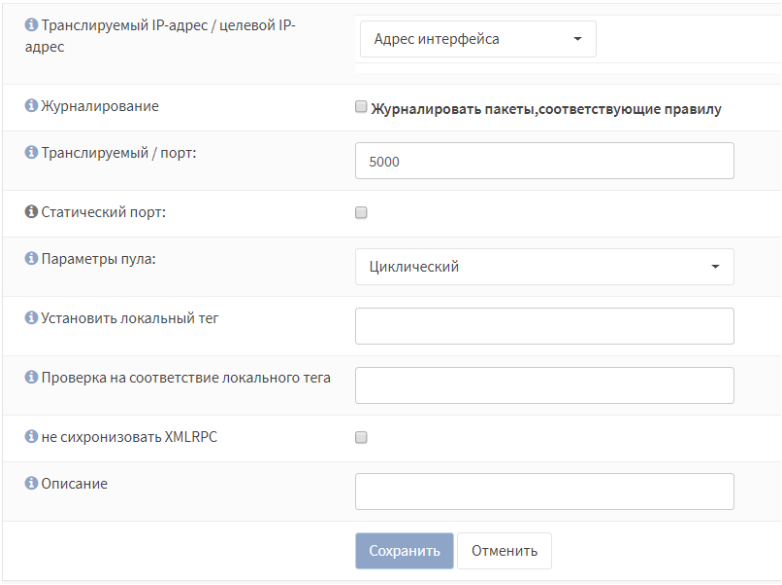


Рисунок 60 — Ручной режим создания правил исходящего NAT (часть 2)

Смешанное создание правил исходящего NAT

Режим смешанного создания правил исходящего NAT позволяет создавать правила исходящего NAT, но также присутствуют автоматические правила исходящего NAT. Автоматически добавленные правила показаны на рисунке (рисунок 58). Добавление правил исходящего NAT описано в подразделе 4.3.3 настоящего руководства.

Отключить создание правил исходящего NAT

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

4.3.4.Категория «NPTv6»

В категории «NPTv6» приведена таблица правил, которые могут применяться для преобразования адресов IPv6.Чаще всего это используется для перевода глобальных («WAN») IP-адресов в локальные. Таблица содержит следующие данные (рисунок 61):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет);

– интерфейс;

– внешний префикс;

– внутренний префикс;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

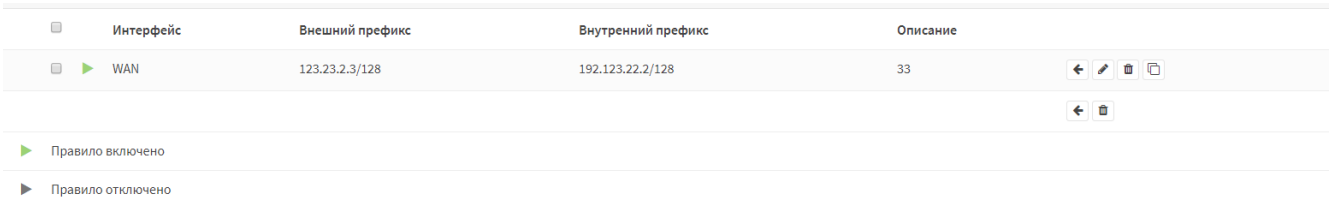


Рисунок 61 — Межсетевой экран: NAT: NPTv6

Для редактирования существующего правила необходимо нажать на кнопку напротив правила. Для того чтобы создать новое правило, необходимо нажать на кнопку Добавить в категории «NPTv6».

При редактировании правила необходимо установить флажок напротив пункта «Отключить» для выключения редактируемого правила. В поле «Интерфейс» необходимо выбрать сетевой интерфейс, на который будут

приходить пакеты для проверки соответствия данному правилу. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель/Адрес» необходимо ввести внутренний (LAN) IPv6-префикс уникального локального адреса для трансляции сетевых префиксов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель/адрес» необходимо ввести глобальный индивидуальный маршрутизируемый IPv6-префикс. В поле «Описание» необходимо ввести описание правила (рисунок 62).

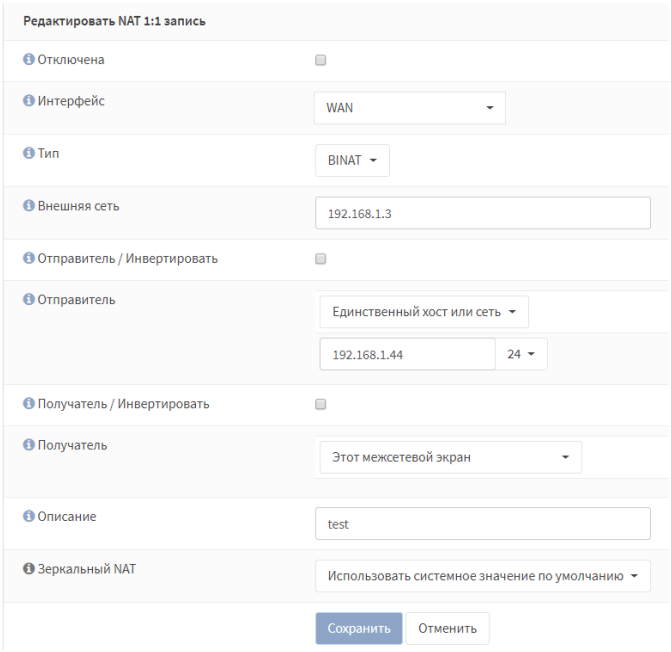


Рисунок 62— Межсетевой экран: NAT: NPTv6 (редактирование правила)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений.

4.4. Подраздел «Ограничение трафика»

Ограничитель трафика позволяет разграничивать пропускную способность каналов связи между пользователями или сегментами сети и назначать приоритет обработки трафика.

4.4.1. Категория «Настройка»

Категория «Настройка» позволяет просматривать и настраивать:

– каналы;

– очереди;

– правила.

Вкладка «Каналы»

В категории «Каналы» приведена таблица каналов, доступных для ограничения трафика. Таблица содержит следующие данные (рисунок 63):

– состояние канала (включен/выключен);

– пропускная способность;

– метрика;

– маска;

– описание канала.

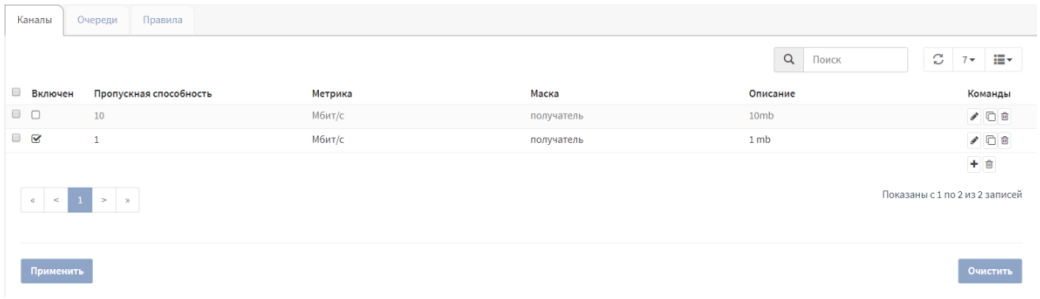
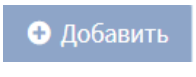


Рисунок 63 — Межсетевой экран: Ограничение трафика: Настройки: Каналы

Для того, чтобы редактировать существующие каналы, необходимо нажать на кнопку  напротив канала. Для того, чтобы создать новый канал, необходимо нажать на кнопку 

.

При редактировании канала необходимо установить флажок напротив поля «Включен». В поле «Пропускная способность» необходимо ввести пропускную способность канала. В поле «Единицы измерения пропускной способности» необходимо выбрать единицы измерения пропускной способности. В поле «Очередь» необходимо ввести количество динамических очередей. В поле маска необходимо выбрать:

– «получатель», чтобы каждому IP-адресу получателя была указана пропускная способность;

– «отправитель», чтобы каждому IP-адресу отправителя была указана пропускная способность;

– «не выбрано», если необходимо создать канал с фиксированной пропускной способностью.

В поле «Buckets» необходимо ввести размер хеш-таблицы, используемой для хранения динамических каналов. В поле «Тип планировщика» необходимо выбрать алгоритм планирования. В поле «Включить CoDel» необходимо установить флажок для включения CoDel (планировщик задержек). В поле «(FQ-)CoDel цель» необходимо ввести минимально допустимую задержку персистентной очереди. В поле «(FQ-)CoDel интервал» необходимо ввести интервал перед отбросом пакетов. В поле «(FQ-)CoDel ECN» необходимо установить флажок для включения уведомления. В поле «(FQ-)CoDel квант» необходимо ввести количество байт, которые может принять очередь перед тем, как она будет передвинута в конец списка очередей. В поле «Включить PIE» необходимо поставить флажок для включения активное управление очередью. В поле «Задержка» необходимо ввести задержку по этому каналу. В поле «Описание» необходимо добавить описание этого канала. Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 64).

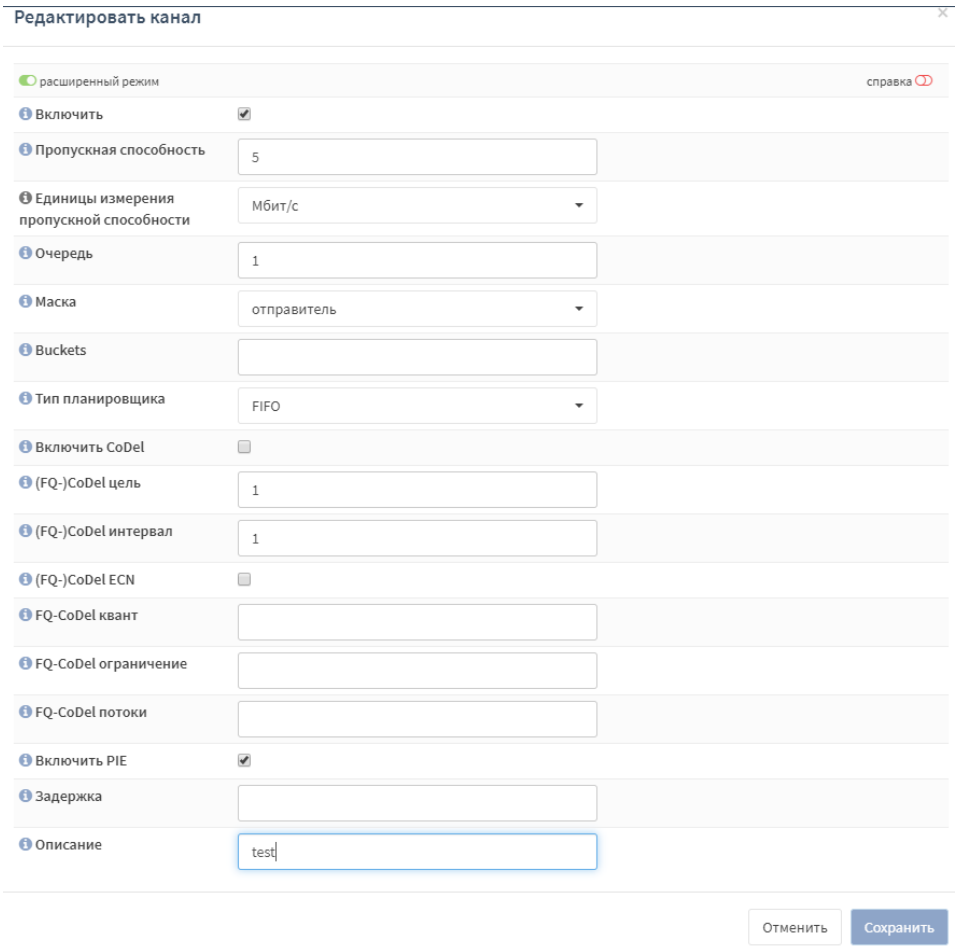


Рисунок 64 — Межсетевой экран: Ограничение трафика: Настройки: Каналы (редактирование)

Вкладка «Очереди»

В категории «Очереди» приведена таблица каналов. Таблица содержит следующие данные (рисунок 65):

– состояние очереди (включена/выключена);
– название очереди;
– весовой коэффициент;
– описание очереди.

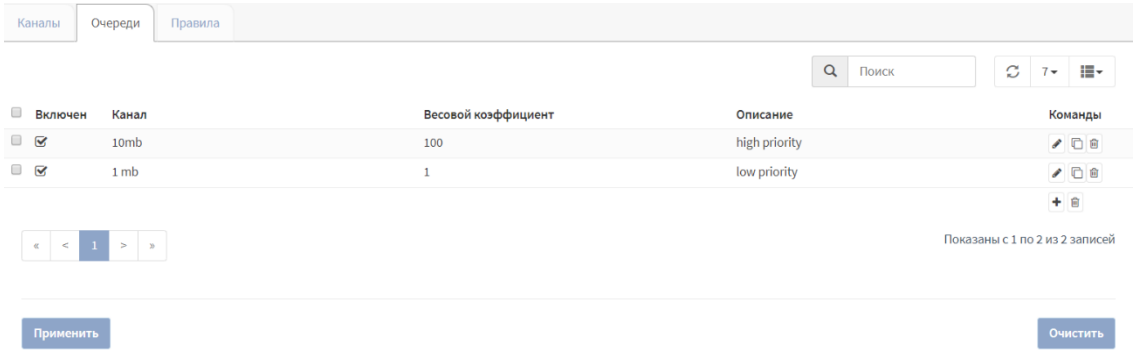
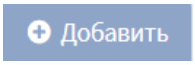


Рисунок 65 — Межсетевой экран: Ограничение трафика: Настройки: Очереди

Для того, чтобы редактировать существующие очереди, необходимо нажать на кнопку  напротив канала. Для того, чтобы создать новую очередь, необходимо нажать на кнопку 

.

При редактировании очереди необходимо установить флажок напротив поля «Включен». В поле «Канал» необходимо выбрать канал, для которого настраивается очередь. В поле «Весовой коэффициент» необходимо ввести приоритет канала от 1 до 100. В поле маска необходимо выбрать:

– «получатель», чтобы каждому IP-адресу получателя была указана пропускная способность;

– «отправитель», чтобы каждому IP-адресу отправителя была указана пропускная способность;

– «не выбрано», если необходимо создать канал с фиксированной пропускной способностью.

В поле «Buckets» необходимо ввести размер хеш-таблицы, используемой для хранения динамических каналов. В поле «Включить CoDel» необходимо установить флажок для включения CoDel. В поле «(FQ-)CoDel цель» необходимо ввести минимально допустимую задержку персистентной очереди. В поле «(FQ-)CoDel интервал» необходимо ввести интервал перед отбросом пакетов. В поле «(FQ-)CoDel ECN» необходимо установить флажок для уведомления. В поле «Включить PIE» необходимо поставить флажок для включения активное управление очередью. В поле

«Описание» необходимо добавить описание этого канала. Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 66).

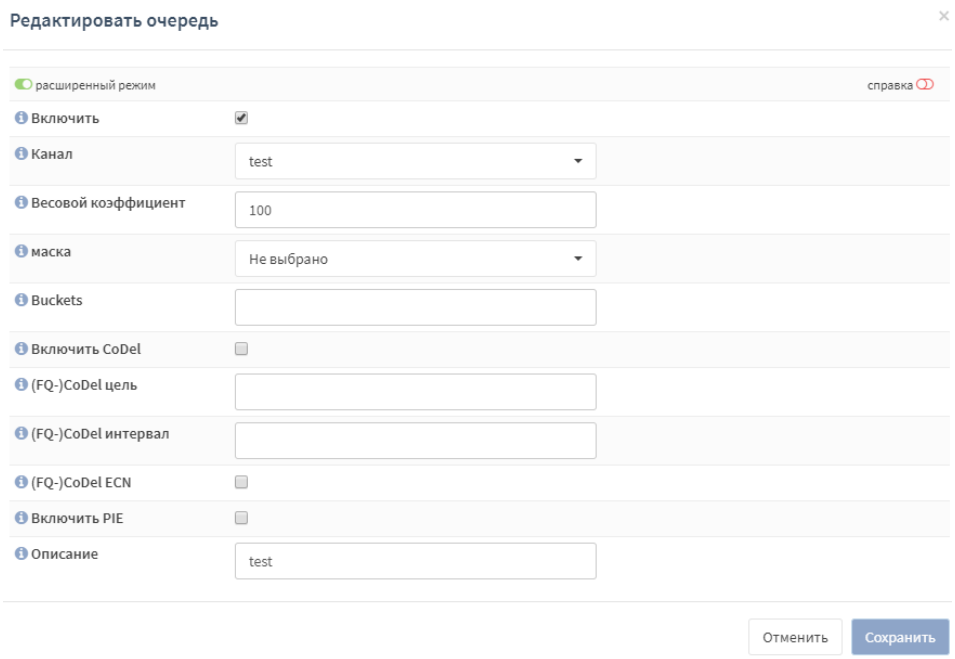


Рисунок 66 — Межсетевой экран: Ограничение трафика: Настройки: Очереди (редактирование)

Вкладка «Правила»

В категории «Правила» приведена таблица правил, которые применяются к настроенным каналам и очередям. Таблица содержит следующие данные (рисунок 67):

- состояние правила (включен/выключен);
- последовательность проверки правил;
- интерфейс;
- протокол;
- отправитель;
- получатель;
- описание правила.

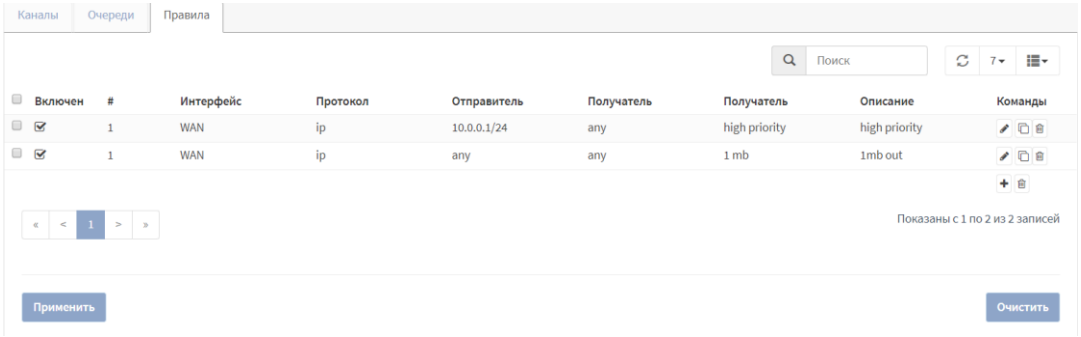


Рисунок 67 — Межсетевой экран: Ограничение трафика: Настройки: Правила

Для того, чтобы редактировать существующие правила, необходимо нажать на кнопку  напротив правила. Для того, чтобы создать новый правило, необходимо нажать на кнопку «+».

При редактировании правила необходимо установить флажок напротив поля «Включить» при необходимости включения редактируемого правила. В поле «Последовательность» необходимо выбрать порядок проверки правил в наборе правил. В поле «Интерфейс» необходимо выбрать сетевой интерфейс, на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Интерфейс 2» необходимо выбрать вспомогательный интерфейс, при этом ПК будет проверять на соответствие правилам пакеты, проходящие от интерфейса 1 к интерфейсу 2 и наоборот. В поле «Протокол» необходимо выбрать протокол, для которого будет выполняться это правило. В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила В поле «Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Получатель» необходимо ввести отправителя. В поле «Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Получатель». В поле «Dst-port» необходимо ввести порт получателя. В поле «Направление» выбрать направление правила. В поле «Цель» необходимо выбрать созданный канал. В поле «Описание» необходимо ввести описание правила (рисунок 68). Необходимо нажать «Сохранить».

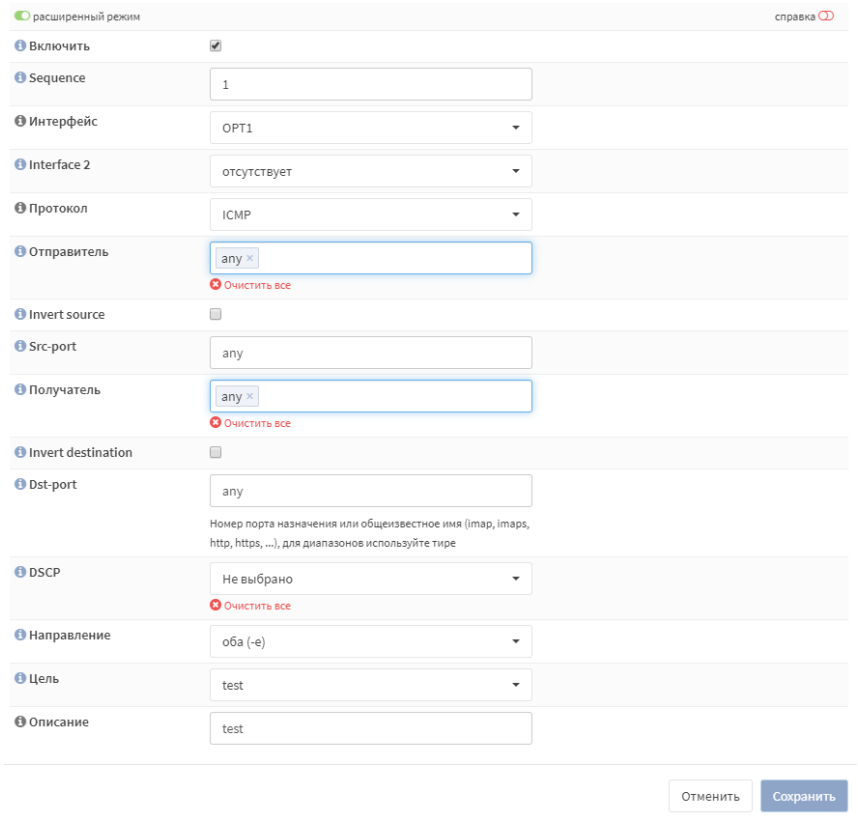


Рисунок 68 — Межсетевой экран: Ограничение трафика: Настройки: Правила (редактирование)

4.4.2. Категория «Статус»

Категория «Статус» позволяет просматривать статус всех настроенных каналов и очередей (рисунок 69).

```
Limiters:
10000:  10.000 Mbit/s    0 ms burst 0
q141072  50 sl. 0 flows (1 buckets) sched 75536 weight 0 lmax 0 pri 0 droptail
 sched 75536 type FIFO flags 0x1 256 buckets 0 active
    mask:  0x00 0x00000000/0x0000 -> 0xffffffff/0x0000
10001:   1.000 Mbit/s    0 ms burst 0
q141073  50 sl. 0 flows (1 buckets) sched 75537 weight 0 lmax 0 pri 0 droptail
 sched 75537 type FIFO flags 0x1 256 buckets 0 active
    mask:  0x00 0x00000000/0x0000 -> 0xffffffff/0x0000


Queues:
q10000  50 sl. 0 flows (256 buckets) sched 10000 weight 100 lmax 0 pri 0 droptail
    mask:  0x00 0x00000000/0x0000 -> 0xffffffff/0x0000
q10001  50 sl. 0 flows (256 buckets) sched 10001 weight 1 lmax 0 pri 0 droptail
    mask:  0x00 0x00000000/0x0000 -> 0xffffffff/0x0000
```

Рисунок 69 — Межсетевой экран: Ограничение трафика: Статус

4.5. Подраздел «Группы интерфейсов»

Подраздел «Группы» позволяет создавать правила, применяемые к нескольким интерфейсам без дублирования правил (рисунок 70).

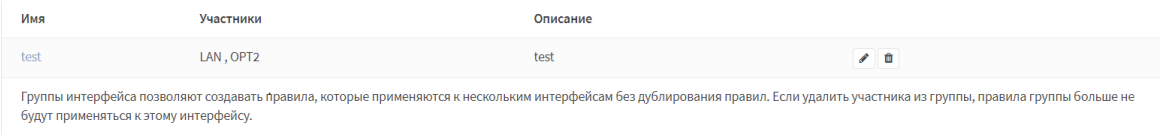


Рисунок 70 — Межсетевой экран: Группы интерфейсов

Для того, чтобы редактировать существующие группы, необходимо нажать на кнопку напротив группы интерфейсов. Для того, чтобы создать новую группу интерфейсов, необходимо нажать на кнопку Добавить.

При редактировании группы в поле «Имя» необходимо ввести название группы интерфейсов. В поле «Описание» необходимо ввести описание группы интерфейсов. В поле «Участники» необходимо выбрать интерфейс, который относятся к этой группе (рисунок 71). Необходимо нажать на кнопку «Сохранить» для сохранения настроек.

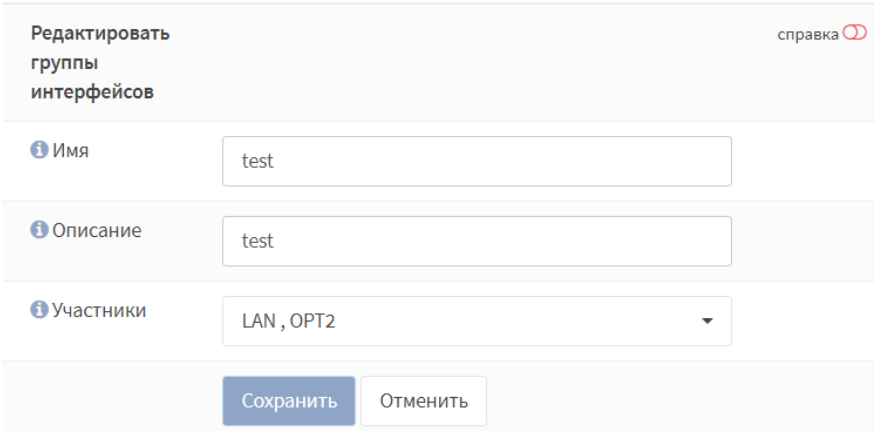


Рисунок 71 — Межсетевой экран: Группы интерфейсов (редактирование)

4.6. Подраздел «Виртуальные IP-адреса»

Виртуальные IP-адреса необходимы для поддержки работы в режиме отказоустойчивого кластера.

4.6.1. Категория «Настройка»

В категории «Настройка» приведена таблица настроенных виртуальных IP-адресов, если таковые имеются. Таблица содержит следующие данные (рисунок 72):

– виртуальный IP-адрес;

– интерфейс;

– тип (режим);

– описание виртуального IP-адреса.

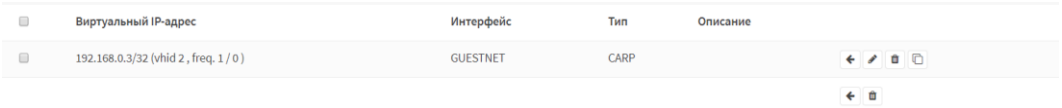
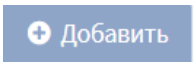


Рисунок 72 — Межсетевой экран: Виртуальные IP-адреса: Настройки

Для того, чтобы редактировать существующие виртуальные IP-адреса, необходимо нажать на кнопку  напротив виртуального IP-адреса. Для того, чтобы создать новый виртуальный IP-адрес, необходимо нажать на кнопку 

.

При редактировании виртуального IP-адреса в поле «Режим» необходимо выбрать режим (тип) виртуального IP-адреса:

– CARP;

– IP-псевдоним;

– Proxy ARP;

– другое.

В поле «Интерфейс» необходимо выбрать сетевой интерфейс для редактируемого виртуального IP-адреса. В поле «Тип» необходимо выбрать тип IP-адреса:

– одиночный IP-адрес;

– сеть.

В поле «Адрес» необходимо ввести IP-адрес и маску подсети. В поле «Шлюз» необходимо ввести адрес шлюза. Для входа через шлюз на

некоторых типах интерфейсов требуется конфигурирование IP-псевдонимов. В других случаях это поле не заполняется. В поле «Пароль виртуального IP-адреса» необходимо ввести пароль группы VHID. Виртуальная группа (VHID) – это группа, в которую объединяются серверы CARP. Виртуальной группе назначается виртуальный IP-адрес, которому протокол CARP выделяет виртуальный MAC-адрес. В поле «Группа VHID» необходимо ввести группу VHID, которая будет распределена межу устройствами. В поле «Частота синхронизации» необходимо выбрать частоту, с которой это устройство будет отправлять сообщения. В поле «Описание» необходимо ввести описание редактируемого виртуального IP-адреса и нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» (рисунок 73).

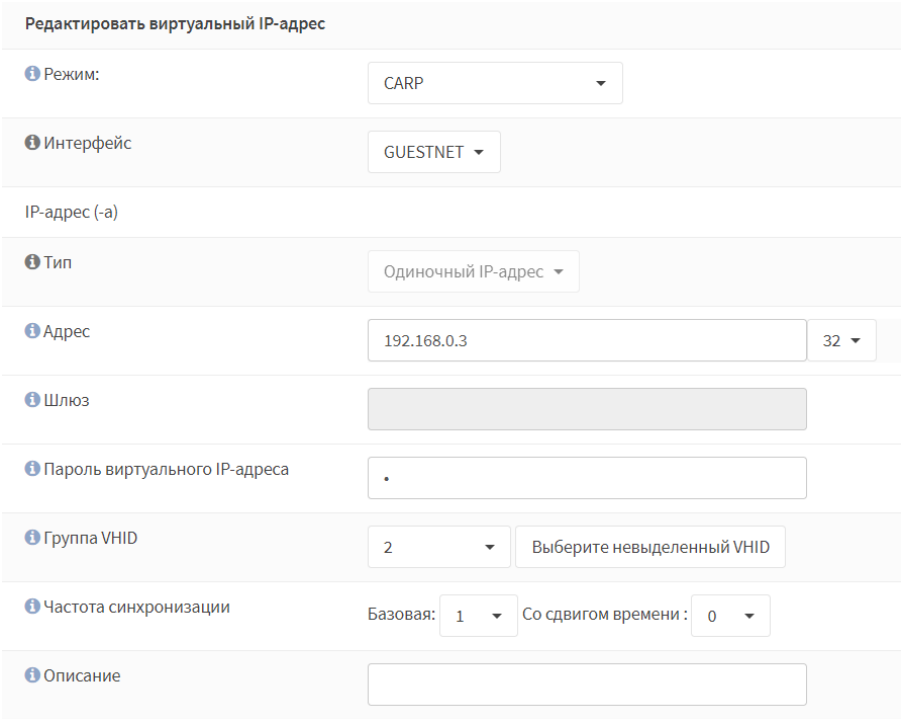


Рисунок 73 — Межсетевой экран: Виртуальные IP-адреса: Настройки (редактирование)

4.6.2. Категория «Статус»

В категории «Статус» отображается информация о статусе работы CARP. Эта категория позволяет просматривать статус CARP всех настроенных IP-адресов, приостановить/включить CARP и

включить/выключить CARP, нажав соответствующие кнопки, а также просматривать pfSync узлы (рисунок 74).

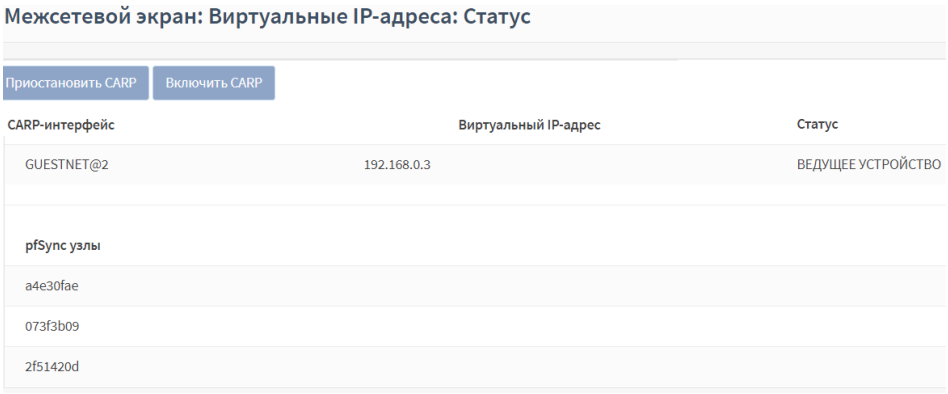


Рисунок 74 — Межсетевой экран: Виртуальные IP-адреса: Статус

4.7. Подраздел «Настройки»

Подраздел «Настройки» позволяет производить настройку дополнительных параметров межсетевого экрана, настройку нормализации (в том числе правил нормализации) и настройку расписания, которое используется в правилах межсетевого экрана.

4.7.1. Категория «Дополнительно»

Категория «Дополнительно» позволяет настраивать дополнительные параметры межсетевого экрана.

В группе настроек «Параметры IPv6» необходимо установить флажок напротив поля «Разрешить IPv6» для разрешения трафика IPv6, если флажок отсутствует, то межсетевой экран будет блокировать весь трафик IPv6 (рисунок 75).

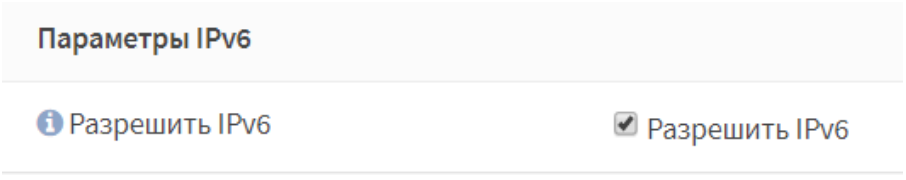


Рисунок 75 — Межсетевой экран: Настройки: Дополнительно (параметры IPv6)

В группе настроек «Преобразование сетевых адресов» необходимо установить флажок напротив поля «Отображение перенаправленных портов» при необходимости автоматического создания правил переадресации NAT, которые нужны для обеспечения доступа к перенаправляющему порту внешнего IP-адреса из внутренних сетей. Необходимо установить флажок напротив поля «Включить отражения для 1:1» при необходимости включения автоматического создания дополнительных правил переадресации NAT, которые нужны для обеспечения доступа к преобразованиям 1:1 внешних IP-адресов из внутренних сетей. В поле «Автоматический исходящий NAT для отображения» необходимо установить флажок для автоматического создания правил исходящего NAT, позволяющие правилам входящего NAT направлять трафик обратно (рисунок 76).

Рисунок 76 — Межсетевой экран: Настройки: Дополнительно (Преобразование сетевых адресов)

В группе настроек «Bogon-сети» в поле «Частота обновлений» необходимо выбрать частоту обновлений зарезервированных или еще не назначенных IANA списков IP-адресов, не относящихся к RFC 1918 (рисунок 77).

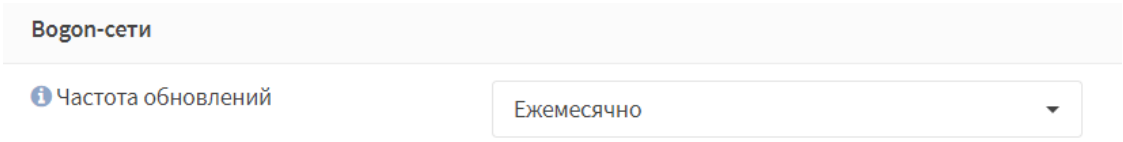


Рисунок 77 — Межсетевой экран: Настройки: Дополнительно (Bogon-сети)

В группе настроек «Мониторинг шлюза» в поле «Сбросить состояния» необходимо установить флажок напротив поля «Отключить сброс состояний при отключении шлюза» при необходимости сохранять состояния для отключенного шлюза. В поле «Игнорировать правила» необходимо установить флажок напротив поля «Игнорировать правила, если шлюз отключен» для отключения правил передачи шлюза по умолчанию при его отключении (рисунок 78).

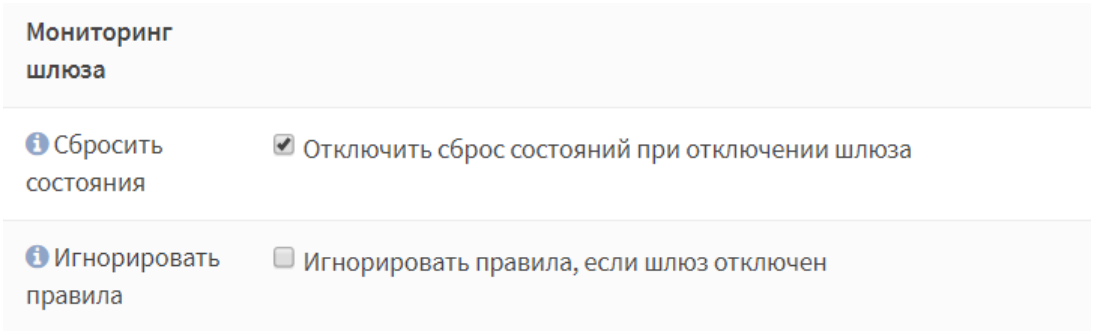


Рисунок 78 — Межсетевой экран: Настройки: Дополнительно (Мониторинг шлюза)

В группе настроек «Мульти-WAN» в поле «Фиксированные соединения» необходимо установить флажок напротив поля «Использовать фиксированные соединения» при необходимости использования «фиксированных соединений». Последовательные соединения будут перенаправлены на серверы в циклическом порядке, а соединения из того же источника будут отправлены на тот же шлюз. Поле «Фиксированное соединение» будет существовать до тех пор, пока существуют состояния, которые относятся к этому соединению. Как только количество состояний становится равным нулю, происходит разрыв фиксированного соединения. Дальнейшие соединения от этого хоста будут перенаправлены на следующий шлюз в циклическом порядке. В поле «Тайм-аут отслеживания источника» необходимо ввести тайм-аут отслеживания источника для «фиксированных соединений» (в секундах). В поле «Общая адресация» необходимо установить флажок напротив поля «Использовать общую переадресацию между фильтром пакетов, ограничением трафика и Порталом авторизации»

при необходимости использования фильтрации пакетов, которые не проходят проверку правилами ограничения трафика и Порталом авторизации. Эта опция позволяет принимать совместное решение о пропуске/фильтрации пакета всех компонентов в особых случаях. В поле «Отключение назначенного шлюза» необходимо установить флажок для отключения использования шлюза по умолчанию (при отключении маршрут будет выбран с помощью таблицы маршрутизации) (рисунок 79).

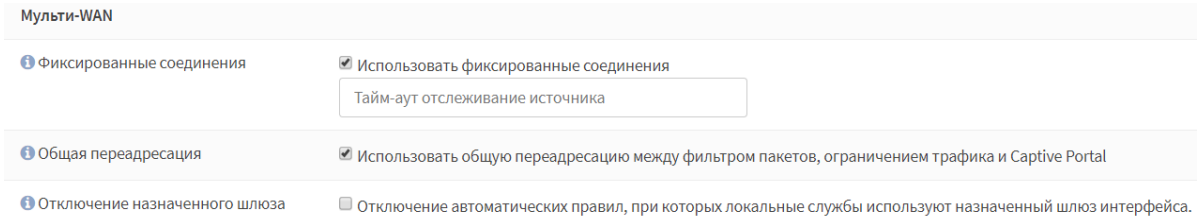


Рисунок 79 — Межсетевой экран: Настройки: Дополнительно (Мульти-WAN)

В группе настроек «Расписания» в поле «Состояние расписания» необходимо установить флажок для сохранения состояний для существующих соединений (рисунок 80).

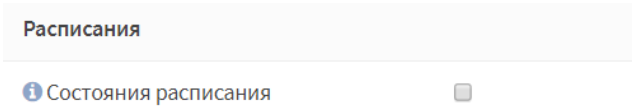


Рисунок 80 — Межсетевой экран: Настройки: Дополнительно (Расписание)

В группе настроек «Прочее» в поле «Оптимизация межсетевого экрана» необходимо выбрать тип оптимизации таблицы состояний:

– нормальный (нормальный алгоритм оптимизации);

– большая задержка (используется для каналов с высокой задержкой, таких как спутниковый канал);

– агрессивный (простаивающие соединения истекают быстрее, более эффективное использование процессора и памяти, но возможен разрыв разрешенных простаивающих соединений);

– консервативный (пытается избегать разрыва любых разрешенных простаивающих соединений за счет дополнительных ресурсов памяти и процессора).

В поле «Оптимизация правил межсетевого экрана» необходимо выбрать тип оптимизации правил:

– базовый (по умолчанию базовая оптимизация правил удаляет дублирующиеся правила, удаляет правила, которые являются подмножеством других правил, комбинирует несколько правил в таблицу если это целесообразно, изменяет порядок правил для увеличения производительности);

– профиль (использовать текущий набор правил как профиль обратной связи для адаптации порядка «Быстрых правил» к актуальному трафику).

В пункте «Привязка состояний к интерфейсу» необходимо установить флажок для привязки состояния к определенному интерфейсу, по умолчанию состояния являются общими, но, когда эта опция установлена, они должны соответствовать интерфейсу. В поле «Отключить межсетевой экран» необходимо установить флажок напротив поля «Отключить фильтрацию пакетов» для выключения фильтрации (будут выполняться функции маршрутизации). В поле «Адаптивные тайм-ауты межсетевого экрана» необходимо ввести тайм-ауты для состояний межсетевого экрана. В поле «начало» необходимо ввести пороговое количество записей состояний, при котором начинает применяться адаптивное масштабирование. В поле «конец» необходимо ввести максимальное количество записей состояний, при достижении которого значения тайм-аутов становятся равными «0». В поле «Максимальное количество состояний межсетевого экрана» необходимо ввести максимальное количество соединений, которые будут храниться в таблице состояний межсетевого экрана. В поле «Максимальное число фрагментов» необходимо ввести максимальное число записей в пул памяти для пересборки фрагмента. В поле «Максимальное количество

записей в таблице» необходимо ввести максимальное количество записей для таких систем, как псевдонимы, sshlockout, bogon и другие. В поле «Фильтрация статических маршрутов» необходимо установить флажок напротив поля «Правила обхода межсетевого экрана для трафика на одном интерфейсе» при необходимости отключения проверки межсетевым экраном входящего/исходящего трафика через один интерфейс. В поле «Отключить reply-to» необходимо установить флажок для отключения reply-to в WAN правилах. В поле «Отключить антиблокировку» необходимо установить флажок для отключения автоматического создания правила антиблокировки. В поле «Интервал разрешения псевдонимов» необходимо ввести интервал, который будет использоваться для разрешения хостов, сконфигурированных на псевдонимах. В поле «Проверить сертификат URL-псевдонимов» необходимо установить флажок для проверки HTTPS-сертификатов при загрузке URL-псевдонимов. В поле «Сброс текущих настроек» необходимо установить флажок для сброса всех настроек в ходе изменения текущего IP-адреса (рисунок 81). Для сохранения настроек необходимо нажать на кнопку «Сохранить».

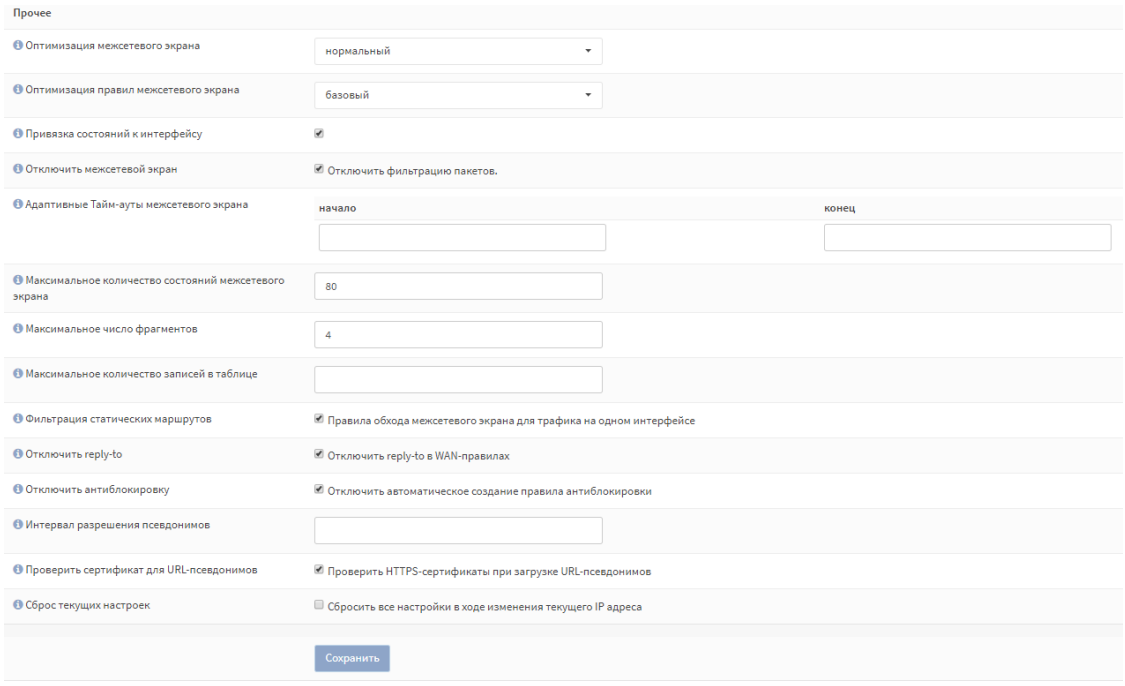


Рисунок 81 — Межсетевой экран: Настройки: Дополнительно (Прочее)

4.7.2.Категория «Нормализация»

Категория «Нормализация» позволяет настраивать нормализацию, просматривать настроенные правила нормализации и добавлять новые правила нормализации (рисунок 82).

В пункте «Общие настройки» в поле «Отключить нормализацию пакетов на интерфейсе» необходимо установить флажок для отключения всех правил нормализации по умолчанию и ограничения размера MSS. В поле «IP Do-Not_Fragment» необходимо установить флажок для того, чтобы осуществлять связь с хостами, которые генерируют фрагментированные пакеты с установленным битом (DF). В поле «Случайный идентификатор IP» необходимо установить флажок для замены значения поля идентификации IP в пакетах случайными значениями, с целью защитить операционные системы, которые используют прогнозируемые значения. Для сохранения настроек необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

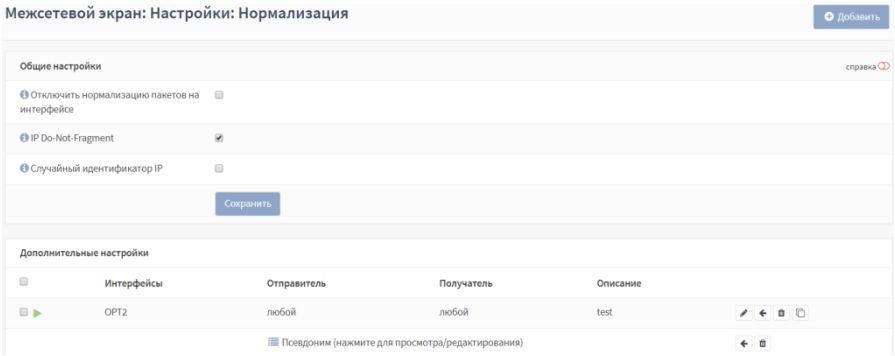
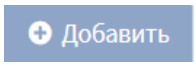


Рисунок 82 — Межсетевой экран: Настройки: Нормализация

Для того, чтобы редактировать существующие правила нормализации, необходимо нажать на кнопку  напротив правила. Для того, чтобы создать новое правило нормализации, необходимо нажать на кнопку  .

При редактировании правила нормализации необходимо установить флажок напротив поля «Отключить» для выключения редактируемого

правила. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Протокол» необходимо выбрать протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 83).

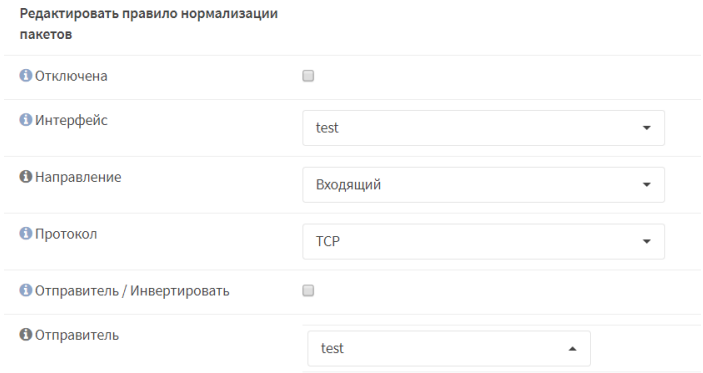


Рисунок 83 — Межсетевой экран: Настройки: Нормализация (редактирование правила нормализации, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Порт отправителя» необходимо указать порт или диапазон портов источника. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Порт получателя» необходимо указать порт или диапазон портов получателя. В поле «Описание» необходимо ввести описание правила (рисунок 84).

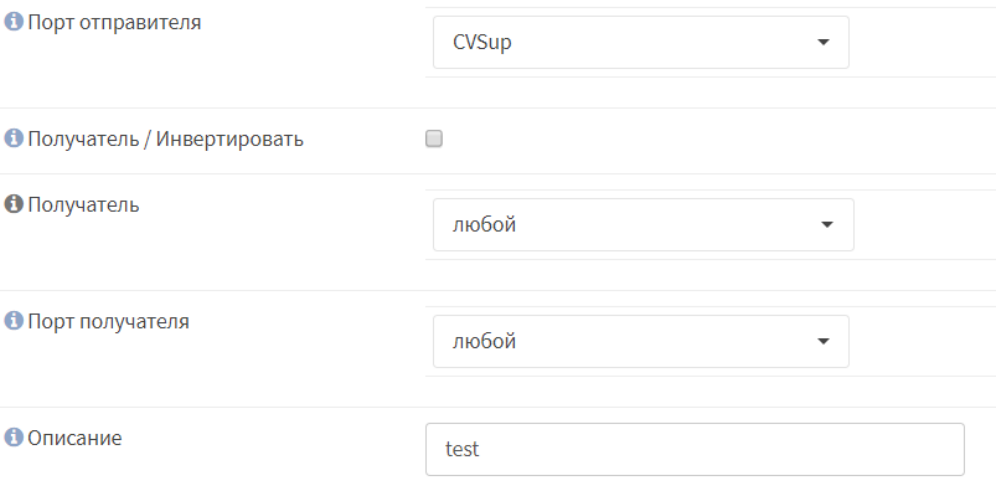


Рисунок 84 — Межсетевой экран: Настройки: Нормализация (редактирование правила нормализации, часть 2)

В пункте «Нормализация» в поле «Макс. MSS» необходимо ввести максимальное значение MSS в TCP-пакетах, соответствующим требованиям. В поле «TOS/DSCP» необходимо выбрать изменение полей TOS/DSCP в проходящих пакетах, в поле «Минимальное TTL» необходимо ввести минимальное значение TTL в IP-пакетах, соответствующим требованиям. В поле «Не фрагментировать» необходимо установить флажок для удаления бит DF (не фрагментированных) в IP-пакетах, соответствующим требованиям. В поле «Случайный ID» необходимо установить флажок для замены идентификационного поля IP-адресом случайными значениями для компенсации прогнозируемых значений, генерируемых большим количеством хостов (рисунок 85).

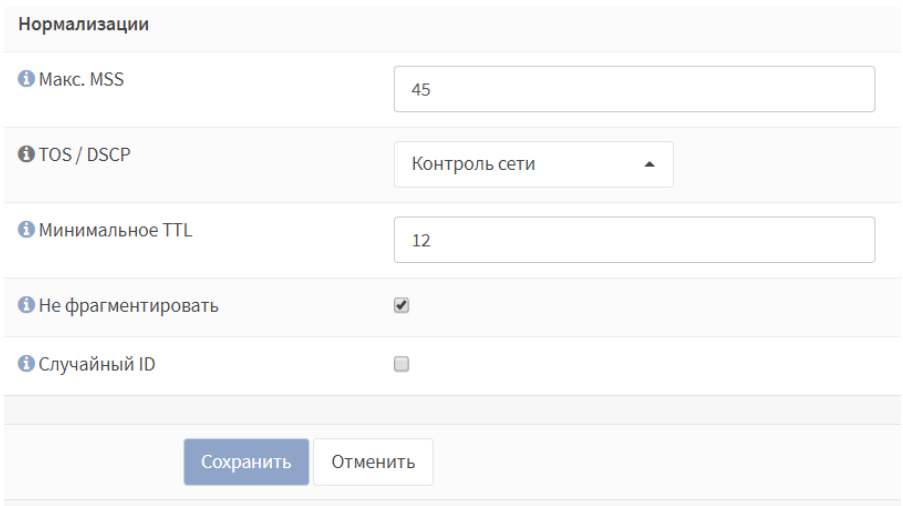


Рисунок 85 — Межсетевой экран: Настройки: Нормализация (редактирование правила нормализации, часть 3)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

4.7.3. Категория «Расписания»

Категория «Расписания» позволяет просмотреть/редактировать настроенные расписания и настроить новое расписание для правил межсетевого экрана (рисунок 86).

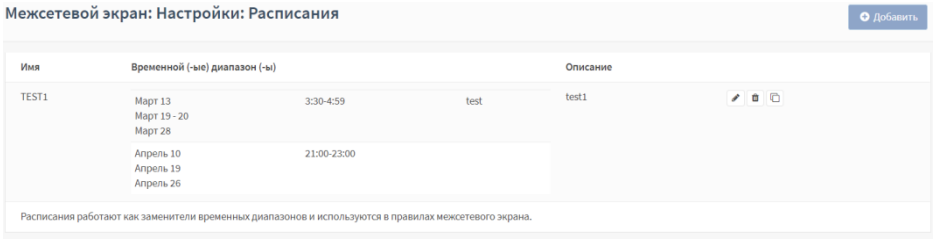
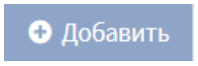


Рисунок 86— Межсетевой экран: Настройки: Расписания

Для того, чтобы отредактировать существующие расписания, необходимо нажать на кнопку  напротив строки расписания. Для того, чтобы создать новое расписание, необходимо нажать на кнопку 

.

При редактировании расписания в поле «Имя» необходимо ввести название расписания, а в поле «Описание» ввести описание расписания. В поле «Месяц» необходимо выбрать месяц для настройки расписания и в появившимся календаре при необходимости выбрать дни месяца. В поле «Время» необходимо выбрать диапазон времени действия расписания. В поле «Описание временного диапазона» необходимо ввести описание диапазона времени, выбранного раннее. Для добавления диапазона в расписание необходимо нажать на кнопку «Добавить время». Для очистки выделенных дат необходимо нажать на кнопку «Очистить выделенное». В поле «Повторение расписания» появится настроенный диапазон времени, имеется возможность добавлять еще диапазоны времени или редактировать

существующие, нажав на  напротив диапазона. Необходимо нажать на кнопку «Сохранить» для сохранения правила (рисунок 87).

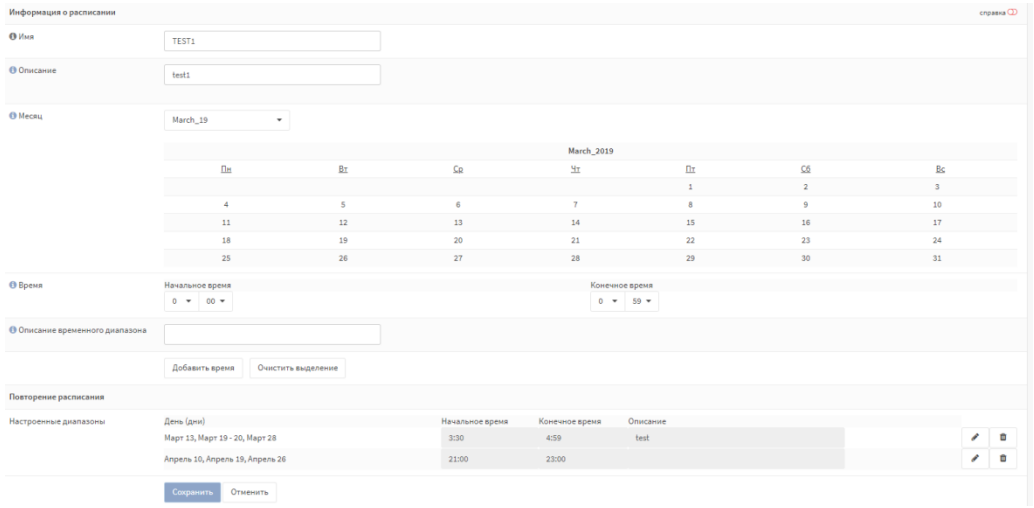


Рисунок 87 — Межсетевой экран: Настройки: Расписания (редактирование)

4.8. Подраздел «Журналы»

Поддерживается ряд форматов отображения журнала межсетевого экрана:

– динамическое представление («В реальном времени»);

– сводное представление («Обзор»);

– открытый вид («Журнал pflog»).

4.8.1. Категория «В реальном времени»

В категории «В реальном времени» отображается каждый пакет, обработанный межсетевым экраном в режиме реального времени. Отображается IP-адрес и порт источника, IP-адрес и порт назначения, входящий интерфейс, время обработки пакета и действие, которое было применено к пакету. Красным отображаются заблокированные записи, зеленым отображаются разрешенные записи (рисунок 88).

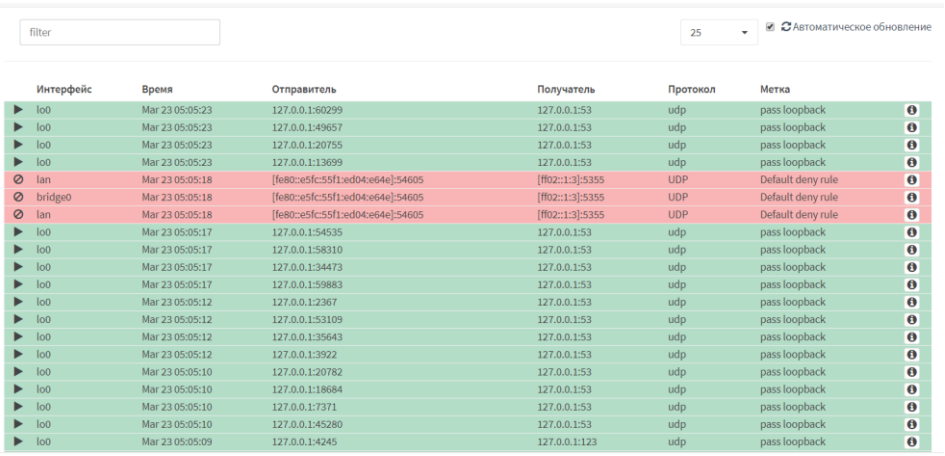


Рисунок 88 — Межсетевой экран: Журналы: В реальном времени

4.8.2. Категория «Обзор»

В категории «Обзор» приведены диаграммы распределения сетевого трафика, обработанного межсетевым экраном с отображением действий (рисунок 89), интерфейсов (рисунок 90), протоколов (рисунок 91), IP-адресов источников (рисунок 92), IP-адресов назначения (рисунок 93), портов источника (рисунок 94), портов назначения (рисунок 95).

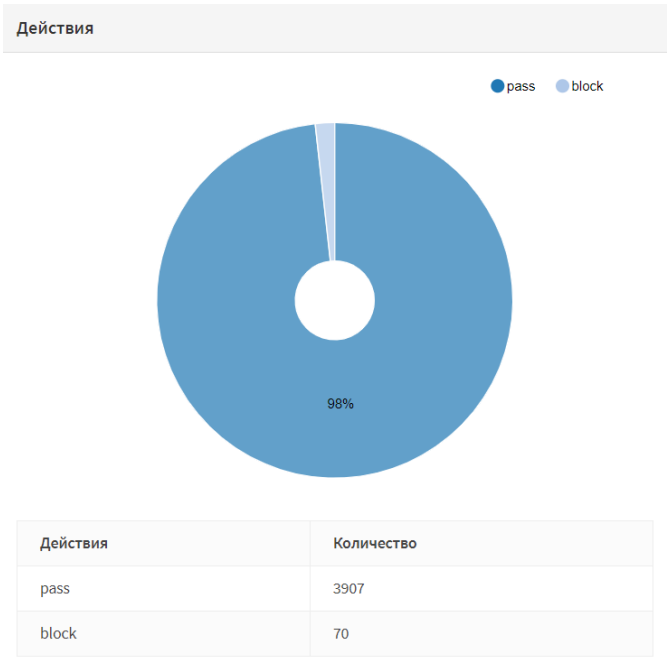
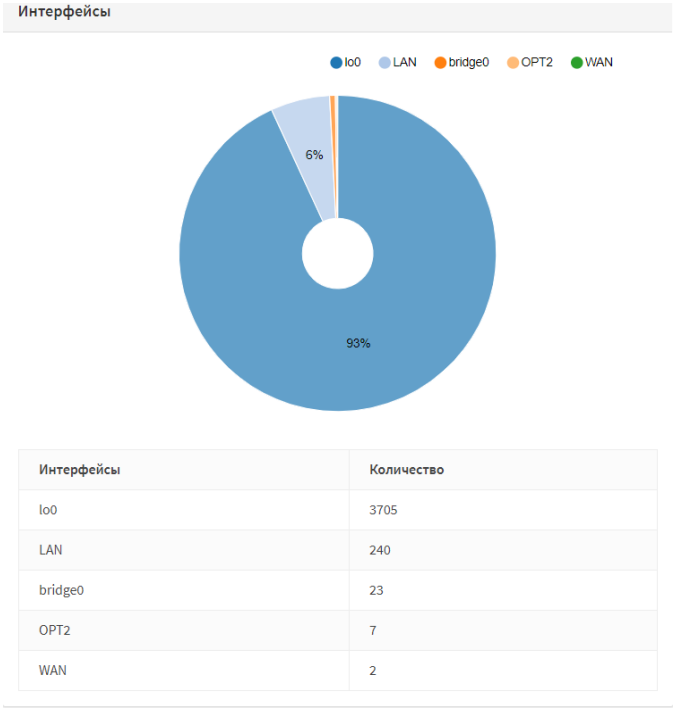
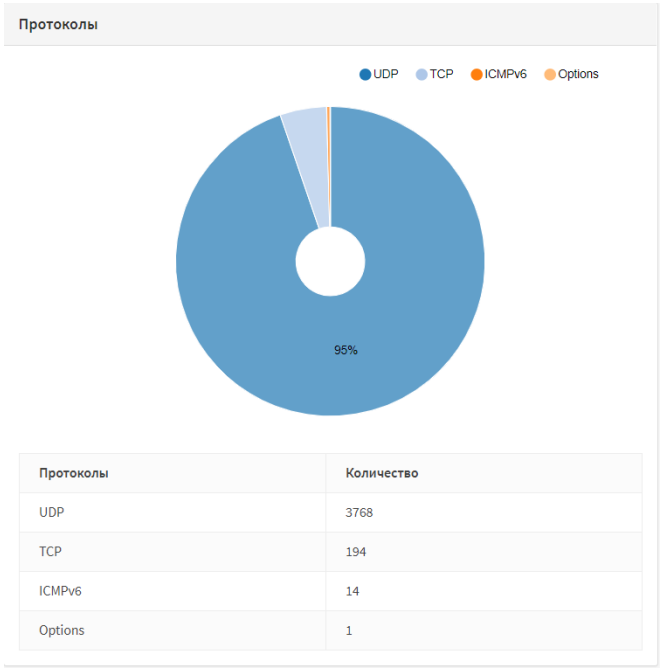


Рисунок 89 — Межсетевой экран: Журналы: Обзор (Действия)



Интерфейсы	Количество
lo0	3705
LAN	240
bridge0	23
OPT2	7
WAN	2

Рисунок 90 — Межсетевой экран: Журналы: Обзор (Интерфейсы)



Протоколы	Количество
UDP	3768
TCP	194
ICMPv6	14
Options	1

Рисунок 91 — Межсетевой экран: Журналы: Обзор (Протоколы)

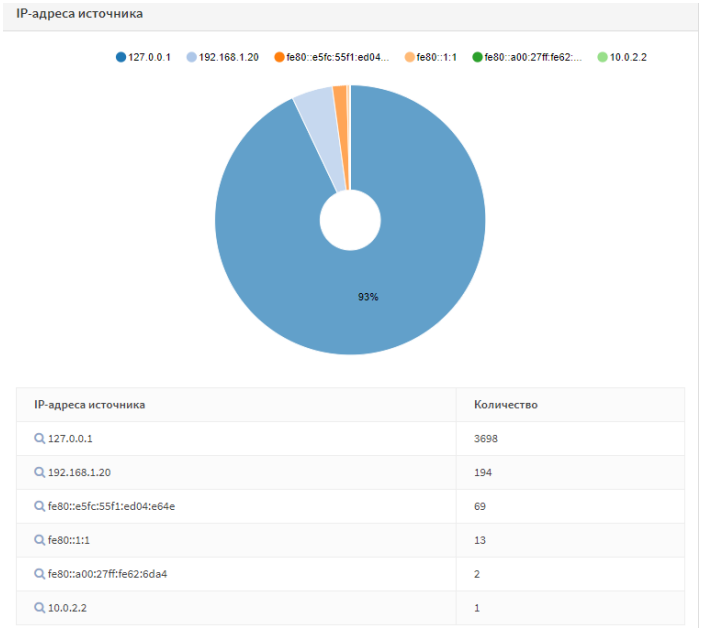


Рисунок 92— Межсетевой экран: Журналы: Обзор (IP-адреса источников)

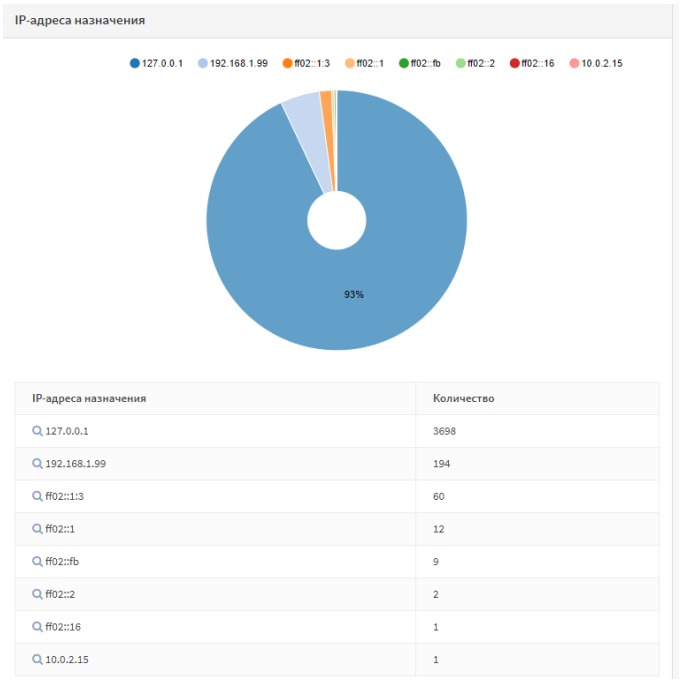
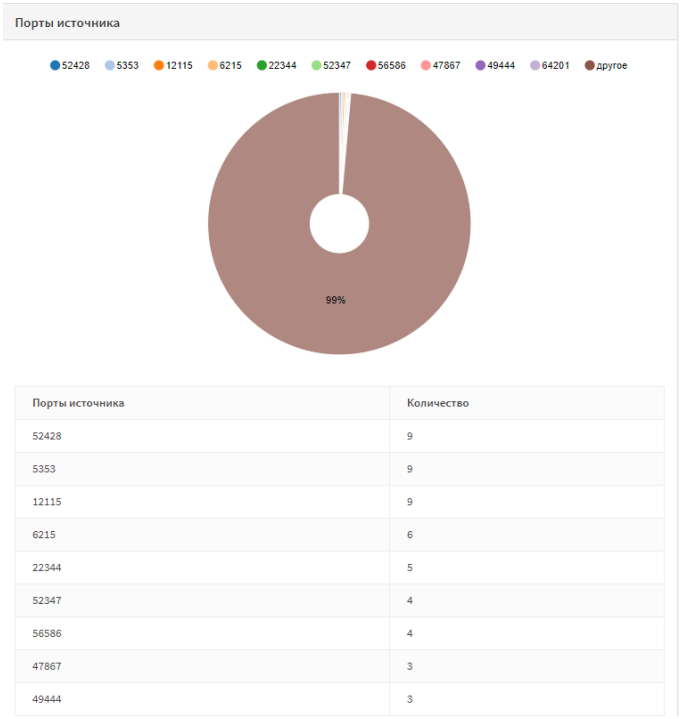
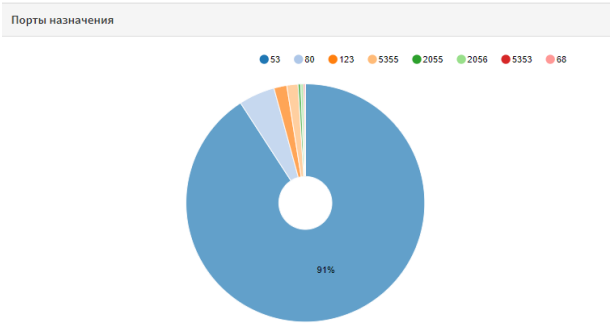


Рисунок 93 — Межсетевой экран: Журналы: Обзор (IP-адреса назначения)



Порты источника	Количество
52428	9
5353	9
12115	9
6215	6
22344	5
52347	4
56586	4
47867	3
49444	3

Рисунок 94 — Межсетевой экран: Журналы: Обзор (Портов источника)



Порты назначения	Количество
53	3600
80	194
123	69
5355	60
2055	15
2056	14
5353	9
68	1

Рисунок 95 — Межсетевой экран: Журналы: Обзор (Портов назначения)

4.8.3. Категория «Журнал pflog»

В категории «Журнал pflog» выводится журнал результатов обработки межсетевого экрана (рисунок 96) в «сыром» виде, на основе которого генерируется таблица журнала «В реальном времени».

Журнал pflog содержит следующую информацию (разделенную «,»):

– номер сработавшего правила фильтрации;

– номер зависимого правила;

– имя правила;

– идентификатор правила;

– имя физического интерфейса, через который проходит пакет;

– причина срабатывания правила (обычно match – совпало с правилом);

– действие (pass, drop);

– направление правила (in, out);

– версия IP протокола;

– обозначения специального байта данных стандартного заголовка IP-пакета (Type of Service);

– уведомление о перегруженности (Explicit Congestion Notification);

– время жизни IP-пакета;

– идентификатор;

– смещение фрагмента;

– флаг;

– порт протокол;

– протокол;

– длина пакета;

– IP-адрес отправителя;

– порт отправителя;

– порт получателя;

– длина данных;

– флаги;

– Seq ID;

– ACK номер;

– размер окна;

– указатель URG;

– опции TCP.

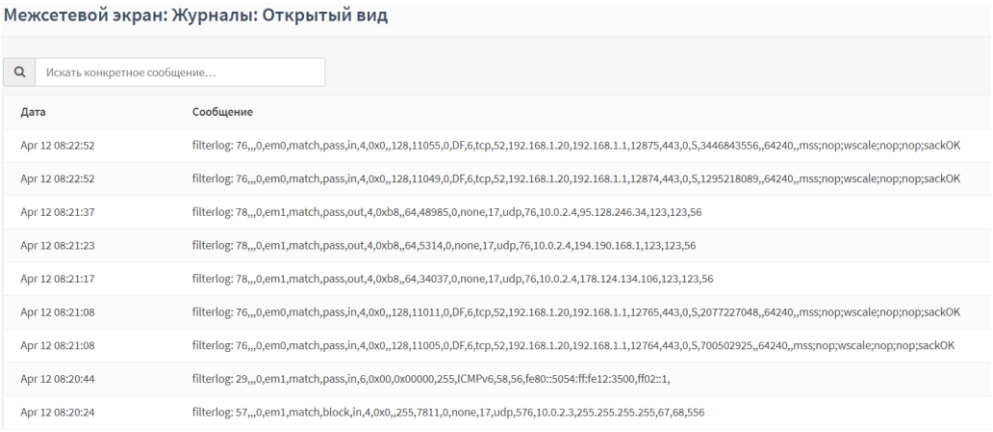


Рисунок 96 — Межсетевой экран: Журналы: Журнал pflog

4.9. Подраздел «Диагностика»

Подраздел «Диагностика» позволяет просматривать общую информацию и статистику pf, 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.

4.9.1. Категория «pfInfo»

Категория «pfinfo» позволяет просматривать общую информацию и статистику (рисунок 97, рисунок 98, рисунок 99, рисунок 100, рисунок 101).

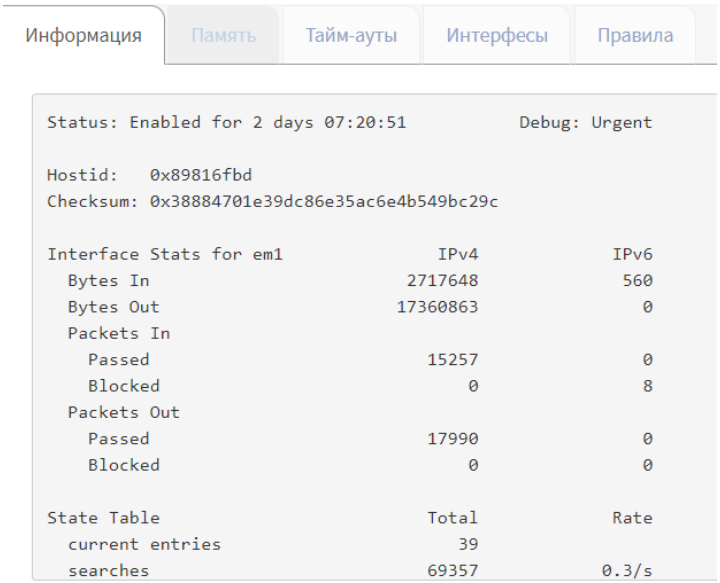


Рисунок 97 — Межсетевой экран: Диагностика: pfinfo (Информация)

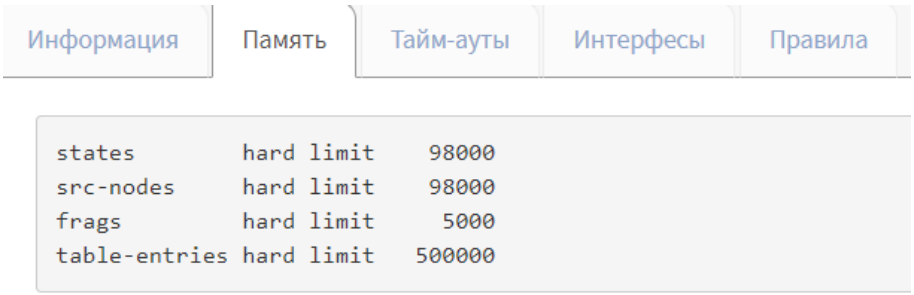


Рисунок 98 — Межсетевой экран: Диагностика: pfinfo (Память)

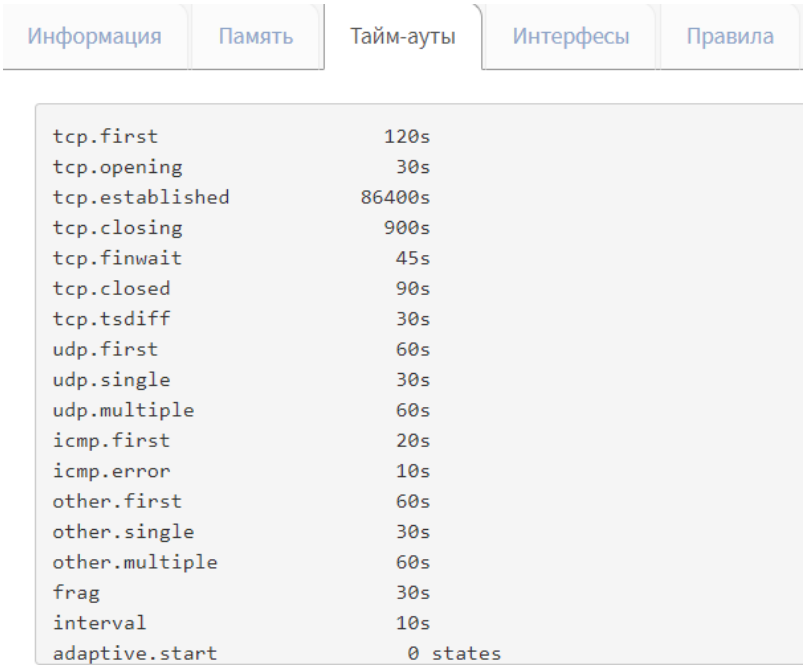


Рисунок 99 — Межсетевой экран: Диагностика: pfinfo (Тайм-Ауты)

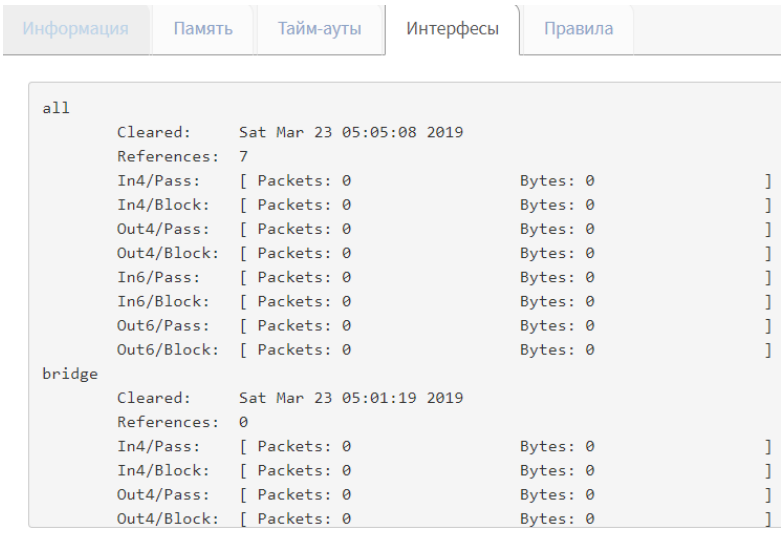


Рисунок 100 — Межсетевой экран: Диагностика: pfinfo (Интерфейсы)

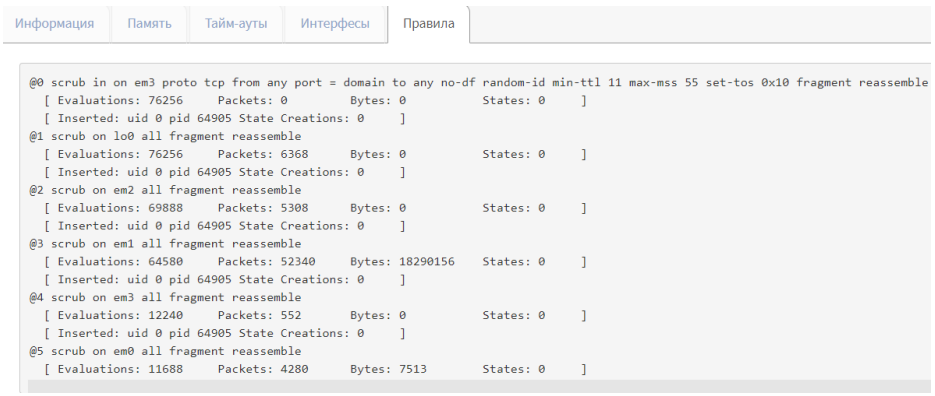


Рисунок 101 — Межсетевой экран: Диагностика: pfinfo (Правила)

4.9.2.Категория «pfTop»

В категории «pfTop» отображаются доступные маршруты в текущее время (рисунок 102). Поле «Вид» позволяет выбрать вид таблицы состояний, «Сортировать по» позволяет выбрать по каким графам таблицы отсортировать, «Количество состояний» позволяет выбрать количество состояний для отображения.

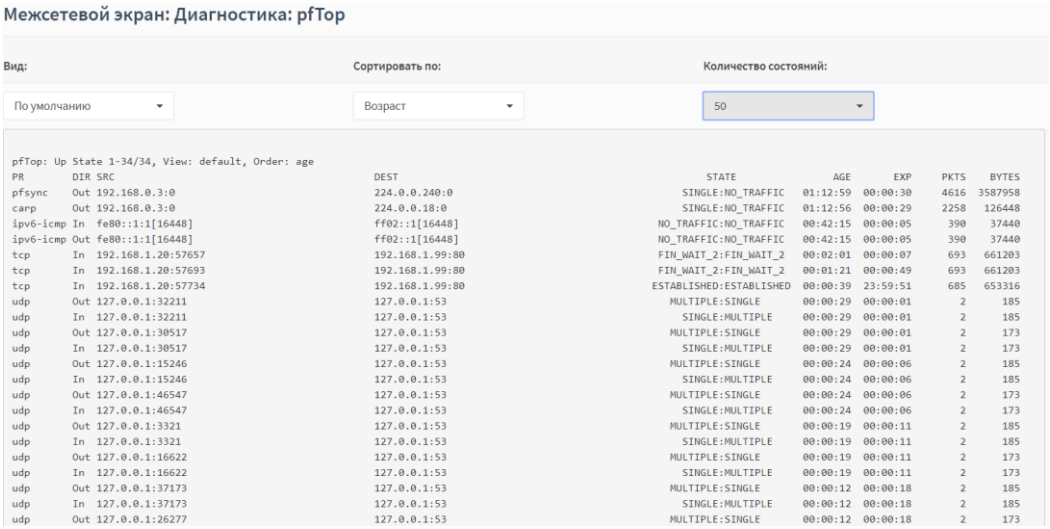


Рисунок 102 — Межсетевой экран: Диагностика: pfTop

4.9.3.Категория «pfTables»

Категория «pfTables» позволяет просматривать IP-адреса, которые указаны в псевдонимах (рисунок 103). Выпадающий список позволяет выбрать псевдоним, очистить и обновить базу псевдонима, нажав соответствующие кнопки.

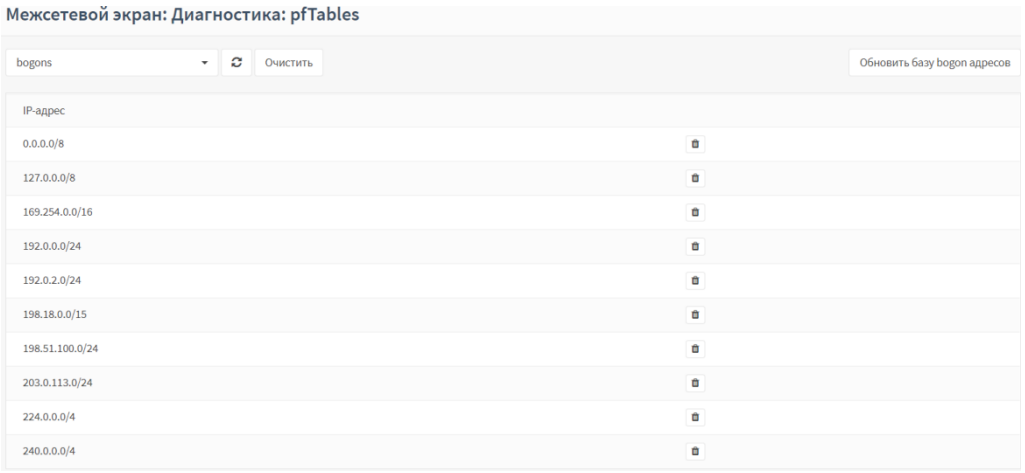


Рисунок 103 — Межсетевой экран: Диагностика: pfTables

4.9.4. Категория «Сокеты»

Категория «Сокеты» позволяет просматривать информацию о прослушивающих сокетах для IPv4 и IPv6 (рисунок 104, рисунок 105). А также просматривать информацию о каждом сокете (рисунок 106).

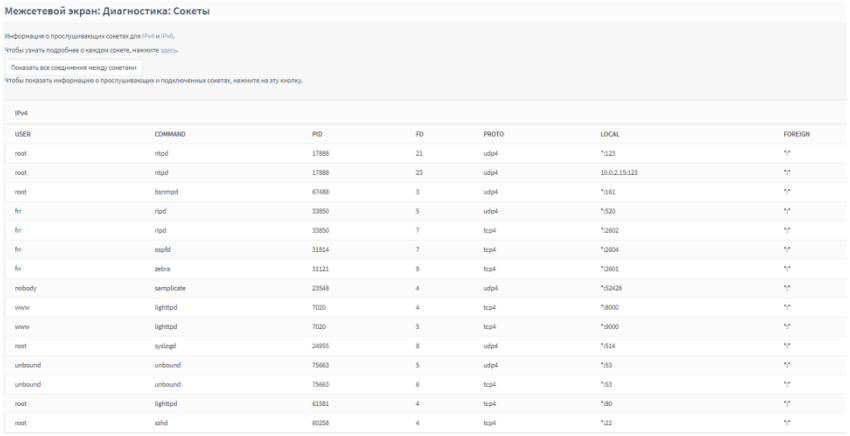


Рисунок 104 — Межсетевой экран: Диагностика: Сокеты (IPv4)

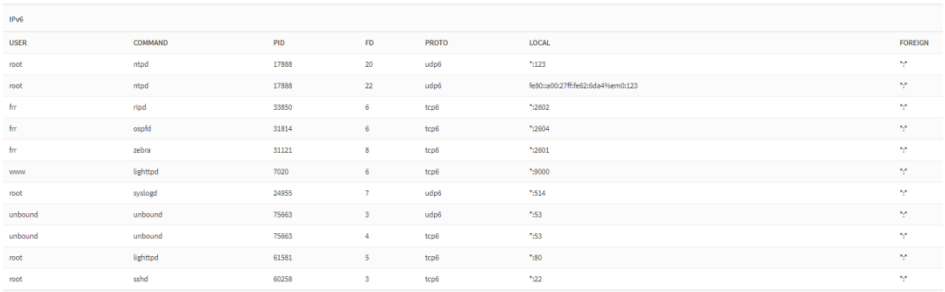
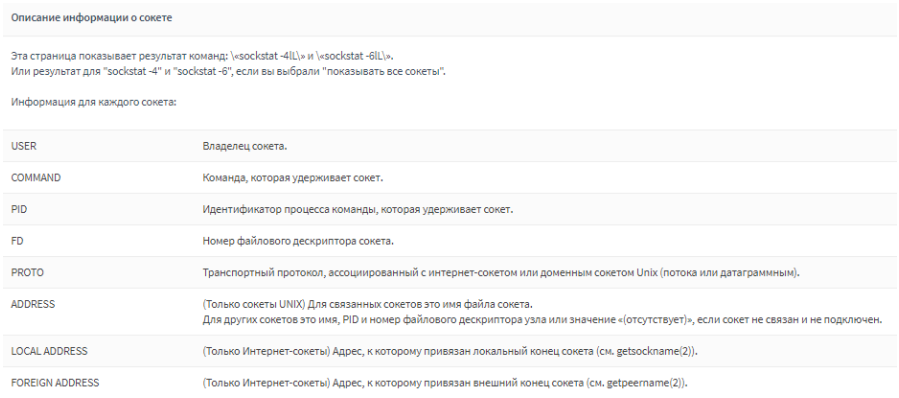


Рисунок 105— Межсетевой экран: Диагностика: Сокеты (IPv6)



Описание информации о сокете

Эта страница показывает результат команд: \«sockstat -4lL\» и \«sockstat -6lL\».
Или результат для "sockstat -4" и "sockstat -6", если вы выбрали "показывать все сокеты".

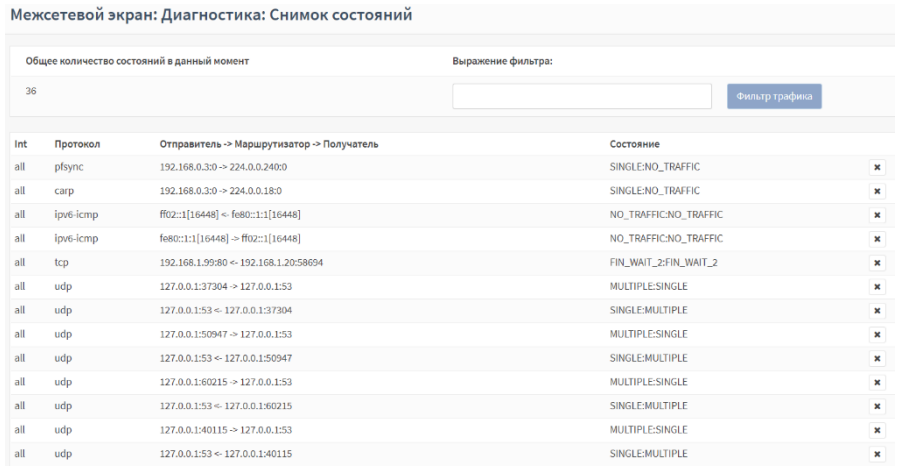
Информация для каждого сокета:

USER	Владелец сокета.
COMMAND	Команда, которая удерживает сокет.
PID	Идентификатор процесса команды, которая удерживает сокет.
FD	Номер файлового дескриптора сокета.
PROTO	Транспортный протокол, ассоциированный с интернет-сокетом или доменным сокетом Unix (потока или датаграммным).
ADDRESS	(Только сокеты UNIX) Для связанных сокетов это имя файла сокета. Для других сокетов это имя, PID и номер файлового дескриптора узла или значение «(отсутствует)», если сокет не связан и не подключен.
LOCAL ADDRESS	(Только Интернет-сокеты) Адрес, к которому привязан локальный конец сокета (см. getsockname(2)).
FOREIGN ADDRESS	(Только Интернет-сокеты) Адрес, к которому привязан внешний конец сокета (см. getpeername(2)).

Рисунок 106 — Межсетевой экран: Диагностика: Сокеты (Общая информация)

4.9.5.Категория «Снимок состояний»

Категория «Снимок состояний» позволяет просматривать активные состояния в текущий момент времени (рисунок 107). В поле «Общее количество состояний в данный момент» отображается количество состояний в текущий момент времени. Поле «Выражение фильтра» позволяет ввести фильтр для фильтрации данных таблицы и нажать на кнопку «Фильтр трафика».



Межсетевой экран: Диагностика: Снимок состояний

Общее количество состояний в данный момент

36

Выражение фильтра:

Фильтр трафика

Int	Протокол	Отправитель -> Маршрутизатор -> Получатель	Состояние
all	pfsync	192.168.0.3:0 -> 224.0.0.240:0	SINGLE:NO_TRAFFIC
all	carp	192.168.0.3:0 -> 224.0.0.18:0	SINGLE:NO_TRAFFIC
all	ipv6-icmp	ff02::1[16448] <- fe80::1:1[16448]	NO_TRAFFIC:NO_TRAFFIC
all	ipv6-icmp	fe80::1:1[16448] -> ff02::1[16448]	NO_TRAFFIC:NO_TRAFFIC
all	tcp	192.168.1.99:80 <- 192.168.1.20:58694	FIN_WAIT_2:FIN_WAIT_2
all	udp	127.0.0.1:37304 -> 127.0.0.1:53	MULTIPLE:SINGLE
all	udp	127.0.0.1:53 <- 127.0.0.1:37304	SINGLE:MULTIPLE
all	udp	127.0.0.1:50947 -> 127.0.0.1:53	MULTIPLE:SINGLE
all	udp	127.0.0.1:53 <- 127.0.0.1:50947	SINGLE:MULTIPLE
all	udp	127.0.0.1:60215 -> 127.0.0.1:53	MULTIPLE:SINGLE
all	udp	127.0.0.1:53 <- 127.0.0.1:60215	SINGLE:MULTIPLE
all	udp	127.0.0.1:40115 -> 127.0.0.1:53	MULTIPLE:SINGLE
all	udp	127.0.0.1:53 <- 127.0.0.1:40115	SINGLE:MULTIPLE

Рисунок 107— Межсетевой экран: Диагностика: Снимок состояний

4.9.6.Категория «Сброс состояний»

Категория «Сброс состояний» позволяет удалить активные состояния и (или) отслеживания источника. Для этого необходимо установить флажок напротив поля «Таблица состояния межсетевого экрана» и (или) «Проверка

источника межсетевым экраном» и нажать на кнопку «Очистить» (рисунок 108).

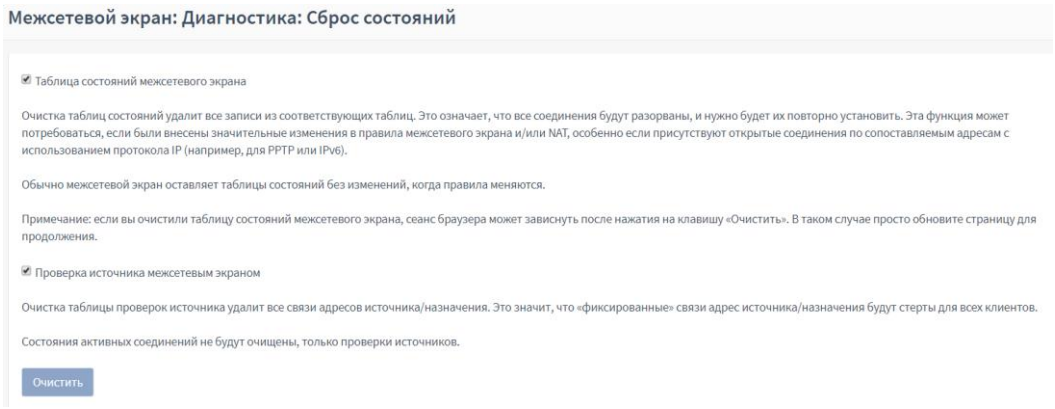
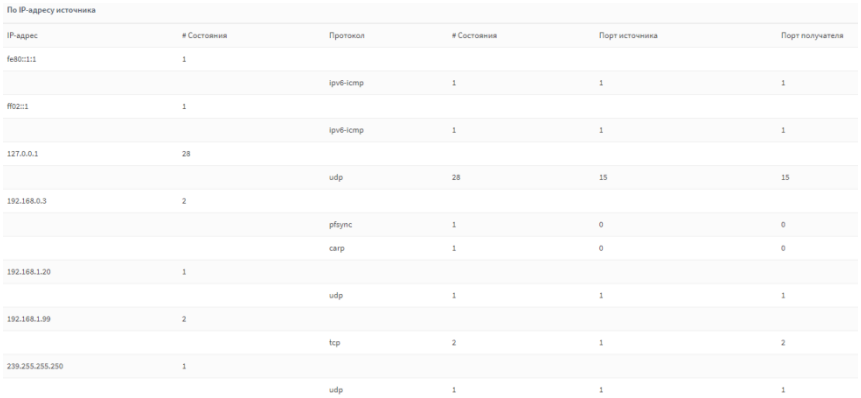


Рисунок 108 — Межсетевой экран: Диагностика: Сброс состояний

4.9.7. Категория «Сводка состояний»

Категория «Сводка состояний» позволяет просматривать состояния, отсортированные по таблицам:

- «По IP-адресу источника» (рисунок 109);
- «По IP-адресу назначения» (рисунок 110);
- «Всего по IP-адресу» (рисунок 111);
- «По паре IP-адресов» (рисунок 112).



По IP-адресу источника

IP-адрес	# Состояния	Протокол	# Состояния	Порт источника	Порт получателя
fe80::1:1	1				
		ipv6-icmp	1	1	1
ff02::1	1				
		ipv6-icmp	1	1	1
127.0.0.1	28				
		udp	28	15	15
192.168.0.3	2				
		pfsync	1	0	0
		carp	1	0	0
192.168.1.20	1				
		udp	1	1	1
192.168.1.99	2				
		tcp	2	1	2
239.255.255.250	1				
		udp	1	1	1

Рисунок 109 — Межсетевой экран: Диагностика: Сводка состояний (по IP-адресу источника)

По IP-адресу назначения

IP-адрес	# Состояния	Протокол	# Состояния	Порт источника	Порт получателя
ff02::1	1				
		ipv6-icmp	1	1	1
fe80::1:1	1				
		ipv6-icmp	1	1	1
127.0.0.1	28				
		udp	28	15	15
192.168.1.20	3				
		tcp	2	1	2
		udp	1	1	1
224.0.0.18	1				
		carp	1	0	0
224.0.0.240	1				
		pfsync	1	0	0
239.255.255.250	1				
		udp	1	1	1

Рисунок 110 — Межсетевой экран: Диагностика: Сводка состояний (по IP-адресу назначения)

Всего по IP-адресу

IP-адрес	# Состояния	Протокол	# Состояния	Порт источника	Порт получателя
ff02::1	2				
		ipv6-icmp	2	1	1
fe80::1:1	2				
		ipv6-icmp	2	1	1
127.0.0.1	56				
		udp	56	15	15
192.168.0.3	2				
		pfsync	1	0	0
		carp	1	0	0
192.168.1.20	4				
		tcp	2	1	2
		udp	2	2	2
192.168.1.99	2				
		tcp	2	1	2
224.0.0.18	1				
		carp	1	0	0
224.0.0.240	1				
		pfsync	1	0	0
239.255.255.250	2				
		udp	2	2	2

Рисунок 111 — Межсетевой экран: Диагностика: Сводка состояний (Всего по IP-адресу)

По паре IP-адресов

IP-адрес	# Состояния	Протокол	# Состояния	Порт источника	Порт получателя
192.168.0.3 -> 224.0.0.240	1				
		pfsync	1	0	0
192.168.0.3 -> 224.0.0.18	1				
		carp	1	0	0
192.168.1.99 -> 192.168.1.20	2				
		tcp	2	1	2
ff02::1 -> fe80::1:1	1				
		ipv6-icmp	1	1	1
fe80::1:1 -> ff02::1	1				
		ipv6-icmp	1	1	1
127.0.0.1 -> 127.0.0.1	28				
		udp	28	15	15
239.255.255.250 -> 192.168.1.20	1				
		udp	1	1	1
192.168.1.20 -> 239.255.255.250	1				
		udp	1	1	1

Рисунок 112 — Межсетевой экран: Диагностика: Сводка состояний (по паре IP-адресов)

5. Раздел «Обнаружение вторжений»

Система обнаружения/предотвращения вторжений основана на ПО Suricata с открытым исходным кодом и использует метод захвата пакетов NETMAP для увеличения производительности и уменьшения нагрузки на центральный процессор.

5.1. Подраздел «Администрирование»

Подраздел «Администрирование» делится на следующие категории меню:

- настройки;
- обновление;
- правила;
- пользовательские;
- предупреждения.

5.1.1. Категория «Настройки»

Категория «Настройки» позволяет настраивать систему обнаружения и предотвращения вторжений.

При использовании системы обнаружения и системы предотвращения вторжений необходимо убедиться, что отключен режим Hardware Offloading. Для выключения режима Hardware Offloading необходимо перейти в «Интерфейсы» - «Настройки» и поставить флажки напротив «CRC аппаратного обеспечения», «TSO аппаратного обеспечения», «LRO аппаратного обеспечения» и нажать кнопку «Сохранить» внизу страницы.

Для включения системы обнаружения вторжений необходимо установить флажок напротив поля «Включен». Для включения системы предотвращения вторжений необходимо установить флажок напротив поля «Режим IPS». Для включения смешанного режима (на некоторых конфигурациях, таких как IPS с VLAN, работа в этом режиме требуется для захвата данных на физическом интерфейсе) необходимо установить флажок

напротив поля «Смешанный режим». В поле «Передавать предупреждения (alerts) в syslog» необходимо установить флажок при необходимости отправления предупреждений (alerts) в syslog в формате fast log. В поле «Сравнение шаблонов» необходимо выбрать используемый алгоритм поиска подстроки при обработке пакетов:

– по умолчанию (используется алгоритм Aho-Corasick);

– Aho-Corasick (алгоритм сопоставления со «словарем», который находит подстроки из «словаря» в пакетах);

– Hyperscan (высокопроизводительная библиотека сопоставления регулярных выражений от Intel).

В поле «Интерфейсы» необходимо выбрать интерфейсы, которые будут использоваться системой обнаружения и предотвращения вторжений. В поле «Домашние сети ($HOME_NET)» необходимо ввести сети, которые будут определяться как домашние. В поле «Размер пакета по умолчанию» необходимо ввести размер пакетов сети по умолчанию. В поле «Архивировать журнал» необходимо выбрать периодичность архивирования журнала предупреждений. В поле «Сохранить журналы» необходимо ввести количество журналов, которые необходимо сохранять. В поле «Содержимое пакета для журнала» необходимо установить флажок для отправки полезной нагрузки (часть пакета данных без служебной информации) в журнал для дальнейшего анализа. Для сохранения настроек необходимо нажать на кнопку «Применить» (рисунок 113).

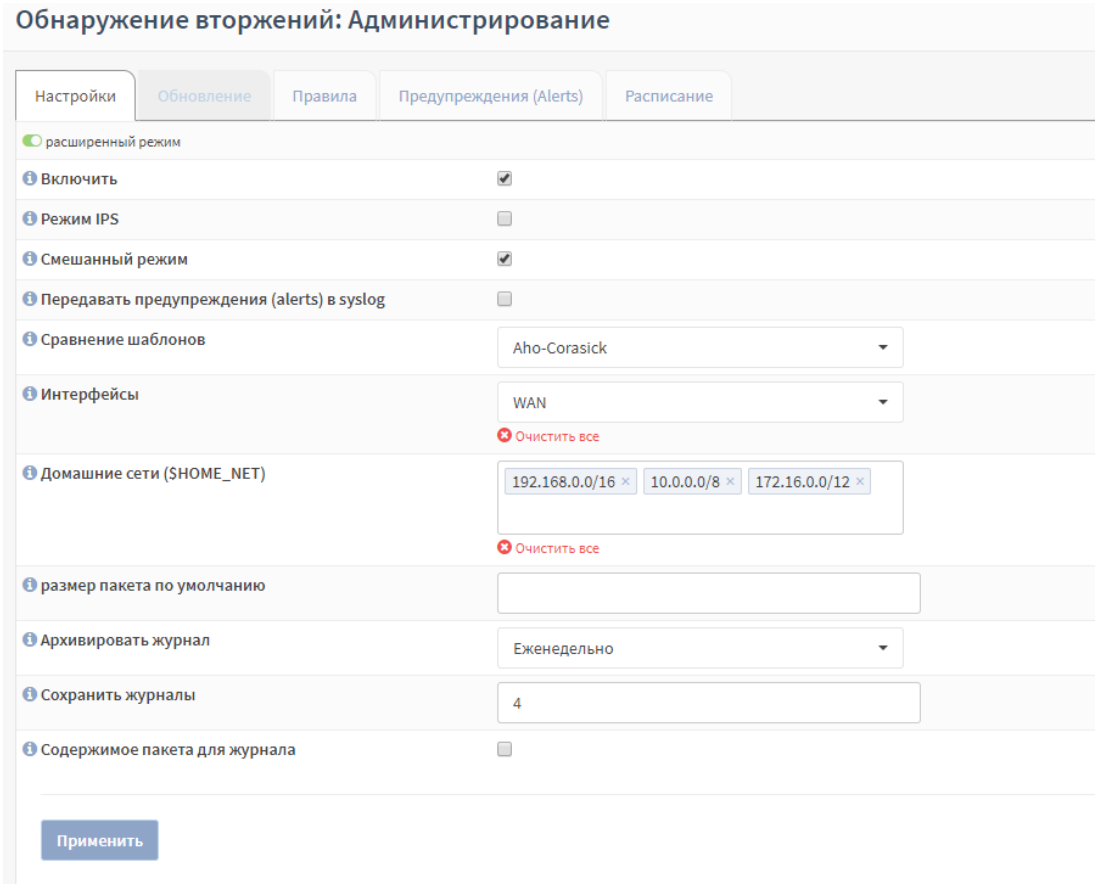


Рисунок 113 — Обнаружение вторжений: Администрирование: Настройки

5.1.2.Категория «Обновление»

Категория «Обновление» позволяет просматривать подгружаемые правила системы обнаружения и предотвращения вторжений, загружать файлы обновления правил.

Для включения имеющихся правил необходимо поставить галочку напротив группы правил и нажать кнопку «Включить выбранные», а затем нажать на кнопку «Скачать и обновить правила» (рисунок 114).

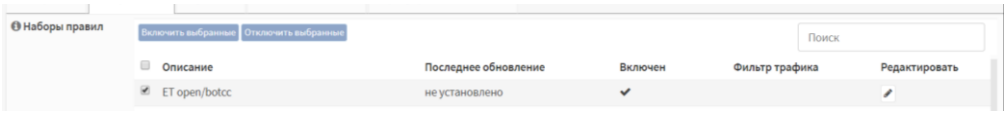


Рисунок 114 — Обнаружение вторжений: Администрирование: Обновление (включение групп правил)

Для загрузки локальных правил необходимо нажать на кнопку «Загрузить новый локальный набор правил». После этого во всплывающем окне необходимо установить флажок напротив поля «Включить», в пункте

«Необходимо выбрать файл» необходимо выбрать файл с правилами. Пункты «Имя файла», «Заголовок» заполнятся автоматически (при необходимости имеется возможность их вписать вручную). Далее необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 115).

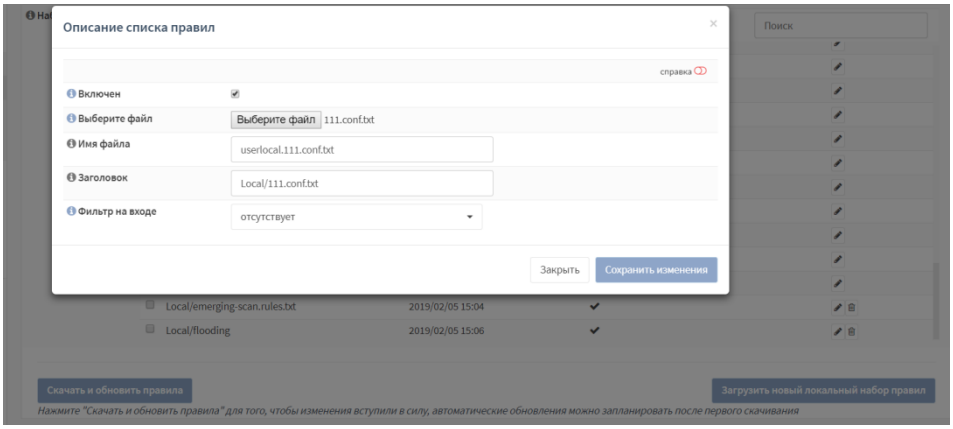


Рисунок 115 — Обнаружение вторжений: Администрирование: Обновление (загрузка локальных правил)

Правила добавятся в список (рисунок 116).

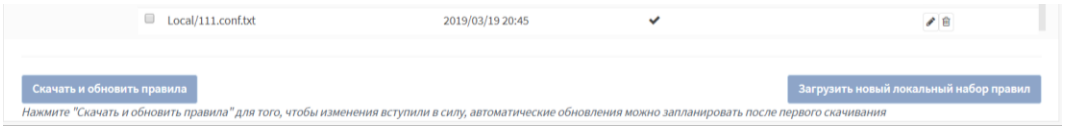


Рисунок 116 — Обнаружение вторжений: Администрирование: Обновление

После этого необходимо нажать на кнопку «Скачать и обновить правила» для того, чтобы активировать выбранные настройки.

Для отключения файлы правил необходимо установить флажок напротив правила, нажать на кнопку «Отключить выбранные» и нажать на кнопку «Скачать и обновить правила».

5.1.3.Категория «Правила»

Категория «Правила» позволяет просматривать все действующие (в том числе из включенных групп правил из категории «Обновление») правила, а также позволяет отсортировать все правила по действию и типу класса, нажав на выпадающий список в соответствующих полях (рисунок 117).

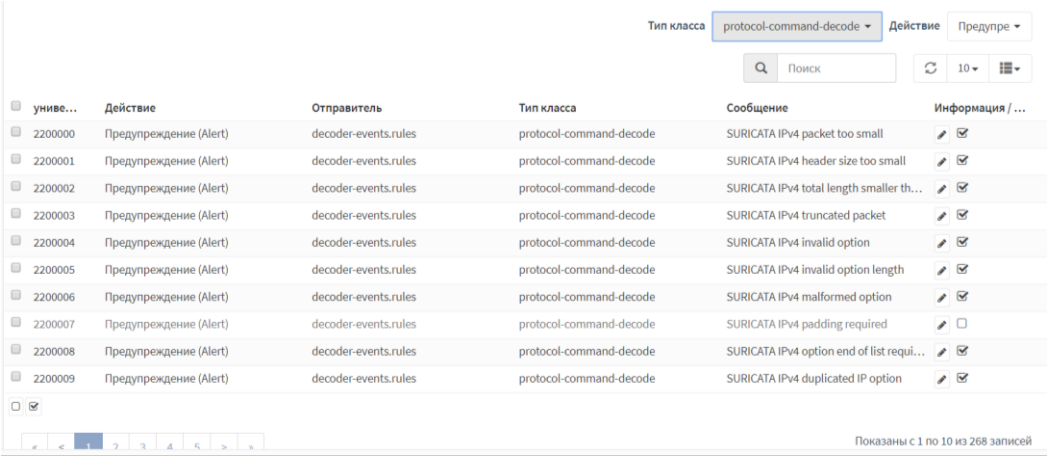


Рисунок 117 — Обнаружение вторжений: Администрирование: Правила

5.1.4. Категория «Предупреждения (Alerts)»

Категория «Предупреждения (Alerts)» позволяет просматривать журнал срабатывания правил системы обнаружения и предотвращения вторжений, а также отсортировать по дате/времени, выполнить поиск, очистить весь журнал оповещений и выбрать сколько последних предупреждений, нажав на соответствующий заголовок (рисунок 118).

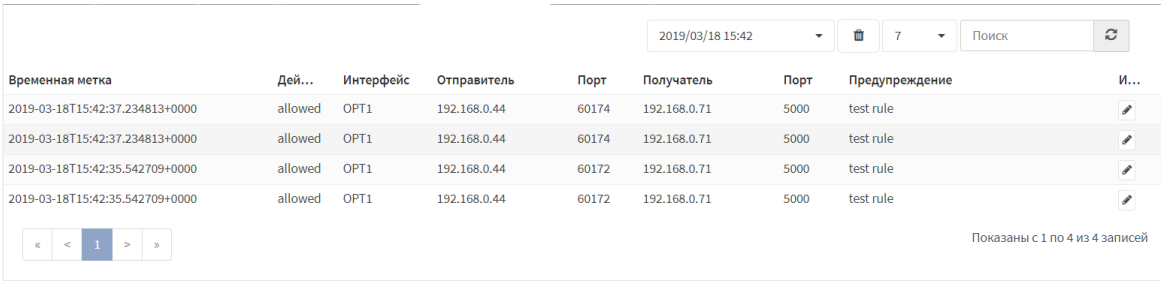


Рисунок 118 — Обнаружение вторжений: Администрирование: Предупреждения (Alert)

5.1.5. Категория «Расписание»

При нажатии на категорию «Расписание» происходит автоматическое перенаправление в редактирование расписания системы предотвращения вторжений, которое находится в разделе «Система» - «Настройки» - «Планировщик задач Cron». При редактировании расписания системы обнаружения вторжений можно выбрать следующие команды в поле «Команда»:

– «Обновить ACL с внешнего прокси и перезагрузить сервис»;

– «Обновить ACL с внешнего прокси»;

– «Выполнять периодическое обновление интерфейса»;

– «Восстановить DH параметры»;

– «Перезагрузить правила обнаружения вторжений»;

– «Выполнить удаленное резервное копирование»;

– «Обновить и перезагрузить псевдонимы межсетевого экрана»;

– «Обновить и перезагрузить правила обнаружения вторжений»;

– «Выполнить перезагрузку»;

– «Пересчитать все чек-суммы».

Остальные параметры расписания расписаны более подробно в настоящем документе в подразделе 6.3.8.

5.2. Подраздел «Контроль уровня приложений»

Подраздел «Контроль уровня приложений» позволяет включать, выключать, просматривать, редактировать, удалять и создавать правила системы обнаружения (предотвращения) вторжений, используя шаблоны протоколов, либо вручную (рисунок 119).

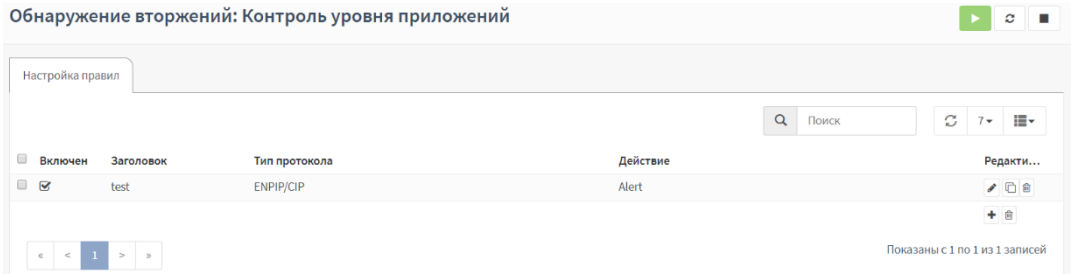


Рисунок 119 — Обнаружение вторжений: Контроль уровня приложений

Далее представлен список поддерживаемых протоколов, для которых представлены шаблоны форм, и степень их разбора (

таблица 2).

Таблица 2 — Поддерживаемые протоколы с указание степени их разбора

Протокол	Стандарт	Степень разбора

Modbus TCP	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; – категория кодов функции (назначенная (коды функций, который определены в Modbus спецификации), не назначенная, общедоступная (стандартные и организационные коды), пользовательская (два диапазона кодов, для которых пользователь может назначить произвольную функцию, зарезервированная (коды функций, которые не являются стандартными), все категории). При классификации по доступу к данным возможно задать следующие дополнительные опции: – тип доступа к данным (записать / считать); – модель данных: ○ «Регистры флагов (Coils)» (битовые данные, доступ чтение / запись); ○ «Регистры хранения (Holding Registers)» (16 битовые данные, доступ

		чтение / запись); o «Дискретные входы (Discrete Inputs)» (битовые данные, доступ чтение); o «Регистры ввода (Input Registers)» (16 битовые данные, доступ чтение).
IEC 60870-5-104	ГОСТ Р МЭК 60870-5-104-2004	Сообщения по протоколу IEC 60870-5-104 могут быть классифицируются по типу пакета (полный APDU, либо 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 разрешенных входящих пакетов (RX); – диапазона разрешенных исходящих пакетов (TX); – типа ASDU; – причины передачи (ASDU cause of transfer)»; – числового значения ASDU адреса; – адреса объекта информации в формате диапазона; – значения IOA.
S7 Communication	Стандарт протокола связи коммуникационных	Сообщения по протоколу S7Communication разделяются по функции: – CPUSERVICE;

	модулей серий Siemens SIMATIC S7-300/400	– 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 поле выбора типа блока, номера блока и целевой файловой системы. При выборе в поле «Функция» функции «DOWNLOADBLOCK» появятся поле выбора типа блока, номера блока и целевой файловой системы. При выборе в поле «Функция» функции «STARTUPLOAD» появятся поле выбора типа блока, номера блока и целевой файловой

		системы. При выборе в поле «Функция» функции «PLCCONTROL» появятся поле выбора функции управления ПЛК: – «INSE (Активация скаченного 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)».
ENIP/CIP	The CIP Networks Library Volume 1 - Common Industrial Protocol (CIP™) (Edition 3.3), The CIP Networks Library Volume 2 - EtherNet/IP Adaptation of CIP (Edition 1.4)	Сообщения по протоколу ENIP/CIP разделяются по протоколу ENIP (номеру команды), по протоколу CIP (сервис, класс и атрибут) и по протоколам ENIP/CIP одновременно.
OPC UA	IEC 62541	Сообщения по протоколу OPC UA разделяются по тип 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» появятся поле выбора политика безопасности. При выборе «MESSAGE» в поле появятся поле выбора типа запроса. При выборе «BROWSE» в поле «Тип запроса» появятся поле ввода диапазон запроса. При выборе «READ» в поле «Тип запроса» появятся поле ввода диапазон запроса. При выборе «WRITE» в поле «Тип запроса» появятся поле ввода диапазон запроса. При выборе «CALL» в поле «Тип запроса» появятся поле ввода идентификатора узла, содержащий вызываемую процедуру и поле ввода идентификатора узла вызываемой процедуры.
OPC DA	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 поле ввода идентификатора вызываемого объекта и поле ввода номера вызываемой функции объекта.
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; – запрос PLC ID; – чтение информации о проекте; – чтение внутренней информации PLC; – чтение информации о внутренней SD карты PLC; – отправка информации обратно PLC; – синхронизация; – назначение PLC владельца; – снятие владельца PLC; – поддержка активного соединения; – чтение блока памяти с PLC; – чтение системных битов, системных слов и переменных; – запись системных битов, системных слов и переменных; – чтение coils и регистров с PLC; – запись катушек и регистров в PLC; – инициализация загрузки (копирование с инженерного ПК на PLC);

		– загрузка блока данных с инженерного ПК на PLC; – завершение загрузки (копирования с инженерного ПК на PLC); – инициализация скачивания (копирование с PLC на инженерный ПК); – скачивание блока данных с PLC на инженерный ПК; – конец скачивания (копирования с PLC на инженерный ПК); – чтение Ethernet Master Data; – включение PLC; – выключение PLC; – мониторинг системных битов, системных слов и переменных; – проверка статуса подключения PLC; – чтение IO объекта; – запись IO объекта; – получение статуса модуля.
MMS	МЭК-61850	Сообщения по протоколу MMS разделяются по типу сообщения. Для типа сообщения «CONFIRMED_REQUEST» возможен выбор типа служб. Для службы «ADDITIONALSERVICE» возможен выбор дополнительного сервиса. Для службы «READ» возможен ввод имени переменной и адреса переменной для функции чтения. Для службы «WRITE» возможен ввод имени переменной для функции записи.
GOOSE	МЭК-61850	Сообщения по протоколу GOOSE разделяются по идентификатору приложения, по значению поля datset, по значению поля

		gocbref, по значению поля goid.

Для того, чтобы редактировать существующие правила, необходимо нажать на кнопку напротив правила. Для того, чтобы создать новое правило, необходимо нажать на кнопку .

При редактировании правила необходимо нажать на флажок напротив поля «Включен» при необходимости включения правила. В поле «Заголовок» необходимо ввести название правила. В поле «Использовать шаблон» необходимо выбрать шаблон протокола, который необходимо использовать (рисунок 120).

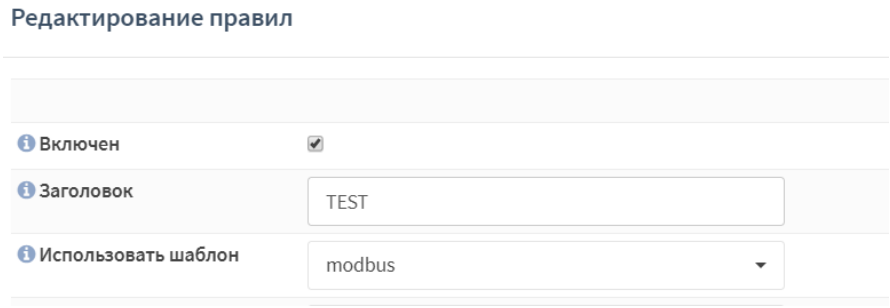


Рисунок 120 — Обнаружение вторжений: Контроль уровня приложений (редактирование)

5.2.1.Modbus

При использовании протокола Modbus появятся следующие настройки. В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя. В поле «Совпадение по» необходимо выбрать признаки совпадения правила:

– свойство функции (код или категория функции);

– доступ к данным (тип доступа и основная таблица);

– диапазон функции (ввод кода функции, адреса и значения переменной вручную).

При выборе «Свойство функции» в поле «Совпадение по» появится поле «Совпадение по» со следующими признаками совпадения:

– код функции (запрашиваемое действие).

– категория функции (категория кодов функции).

При выборе «Код функции» в поле «Совпадение по» появятся следующие поля:

– код функции (необходимо выбрать функцию);

При выборе «08:Diagnostic» в поле «Код функции» появится поле:

– код подфункции (необходимо выбрать код подфункции).

При выборе «Категория функции» в поле «Совпадение по» появятся следующие поля:

– отрицание выбранной категории (необходимо поставить флажок при выборе все категорий кроме указанной в поле «Категория совпадения»);

– категория совпадения (необходимо выбрать категорию кодов функции:

– назначенный (коды функций, который определены в Modbus спецификации);

– не назначено;

– общедоступный (стандартные и организационные коды);

– пользователь (два диапазона кодов (65 – 72, 100 – 110), для которых пользователь может назначить произвольную функцию;

– зарезервировано (коды функций, который не являются стандартными (9, 10, 13, 14, 41, 42, 90, 91, 125, 126, 127);

– все.

При выборе «Доступ к данным» в поле «Совпадение по» появится поле «Совпадение по» со следующими признаками совпадения:

– тип доступа к данным (необходимо выбрать):

– записать (для записи значений в таблицы данных используются функции с кодами 5, 6, 15, 16, 21, 22 и другие);

– считать (для чтения значений из таблиц данных используются функции с кодами 1 – 4, 7, 8, 11, 12, 20, 24 и другие);

– доступ к основной таблице (необходимо выбрать модель данных):

o «Регистры флагов (Coils)» (битовые данные, доступ чтение / запись);

o «Регистры хранения (Holding Registers)» (16 битовые данные, доступ чтение / запись);

o «Дискретные входы (Discrete Inputs)» (битовые данные, доступ чтение);

o «Регистры ввода (Input Registers)» (16 битовые данные, доступ чтение).

При выборе «Диапазон функции» в поле «Совпадение по» появятся следующие поля.

В поле «Код функции» необходимо ввести диапазон функции. Данное поле может принимать значения от 0 до 255.

В поле «Адрес» необходимо ввести диапазон номеров адреса. Данное поле может принимать значения от 0 до 65535.

В поле «Значение» необходимо ввести диапазон значений выбранного адреса. Данное поле может принимать значения от 0 до 65535.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 121).

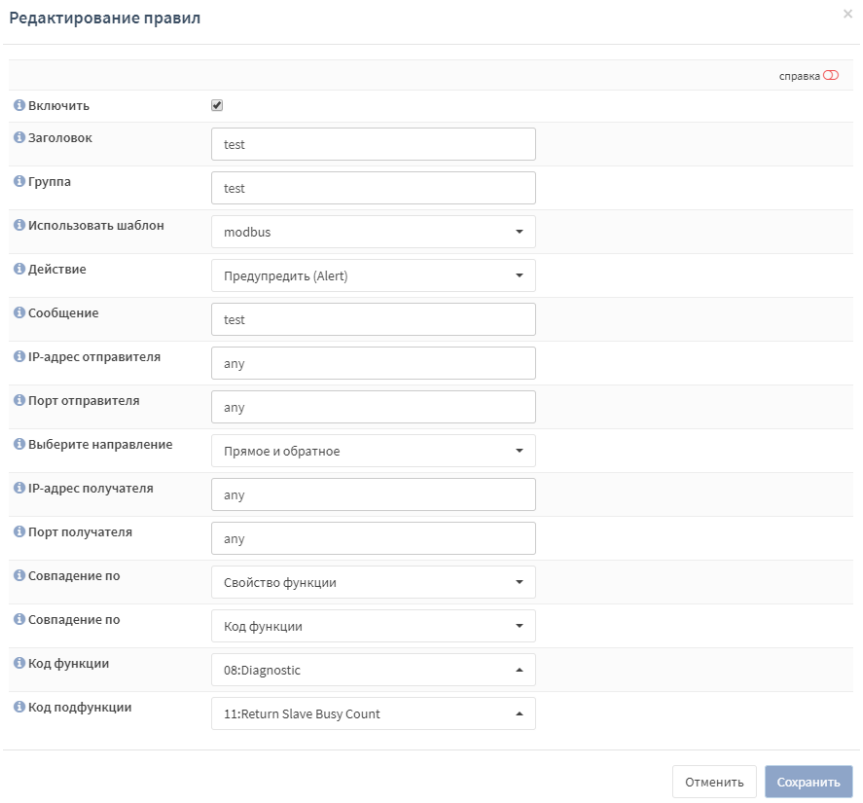


Рисунок 121 — Обнаружение вторжений: Контроль уровня приложений (редактирование: Modbus)

5.2.2.IEC 104

При использовании шаблона протокола IEC 104 появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Application function» необходимо выбрать тип пакета (может быть передан либо полный APDU, либо (для целей управления) только поля APCI):

– «ASDU (блок данных прикладного уровня)»;

– «APCI (управляющая информация прикладного уровня)», используется чтобы определить начало и конец ASDU, каждый заголовок APCI включает следующие маркировочные элементы:

– стартовый символ;

– указание длины ASDU вместе с полем управления.

При выборе «APCI (управляющая информация прикладного уровня)» в поле «Application function» появится поле «Формат». В поле «Формат» необходимо выбрать формат:

– любой;

– «U-format (unnumbered control functions)» — функции управления без нумерации;

– «S-format (numbered supervisory functions)» — функции контроля с нумерацией.

При выборе «ASDU (блок данных прикладного уровня)» в поле «Application function» появится следующие поля. В поле «RX» необходимо ввести диапазон разрешенных входящих пакетов или оставить пустым, в случае отсутствия ограничений (например, [:10] — пропустить первые 10 входящих пакетов). В поле «TX» необходимо ввести диапазон разрешенных исходящих пакетов или оставить пустым, в случае отсутствия ограничений (например, [:10] — пропустить первые 10 исходящих пакетов).

В поле «Тип ASDU» необходимо выбрать тип ASDU. Все возможные тип приведены в таблице (таблица 3).

Таблица 3 — Типы ASDU

Идентификатор типа	**Описание**	**Метка ASDU**
<0>	:= не определяется	
<1>	:= одноэлементная информация	M_SP_NA_1
<3>	:= двухэлементная информация	M_DP_NA_1
<5>	:= информация о положении отпаек	M_ST_NA_1
<7>	:= строка из 32 битов	M_BO_NA_1
<9>	:= значение измеряемой величины, нормализованное значение	M_ME_NA_1
<11>	:= значение измеряемой величины, масштабированное	M_ME_NB_1

	значение	
<13>	:= значение измеряемой величины, короткий формат с плавающей запятой	M_ME_NC_1
<15>	:= интегральные суммы	M_IT_NA_1
<20>	:= упакованная одноэлементная информация с определением изменения состояния	M_PS_NA_1
<21>	:= значение измеряемой величины, нормализованное значение без описателя качества	M_ME_ND_1
<22..29>	:= резерв для дальнейших совместимых определений	
*<30>	:= одноэлементная информация с меткой времени CP56Время2a	M_SP_TB_1
*<31>	:= двухэлементная информация с меткой времени CP56Время2a	M_DP_TB_1
*<32>	:= информация о положении отпаек с меткой времени CP56Время2a	M_ST_TB_1
*<33>	:= строка из 32 битов с меткой времени CP56Время2a	M_BO_TB_1
*<34>	:= значение измеряемой величины, нормализованное значение с меткой времени CP56Время2a	M_ME_TD_1
*<35>	:= значение измеряемой величины, масштабированное значение с меткой времени CP56Время2a	M_ME_TE_1
*<36>	:= значение измеряемой величины, короткий формат с плавающей запятой с меткой времени CP56Время2a	M_ME_TF_1
*<37>	:= интегральная сумма с меткой времени CP56Время2a	M_IT_TB 1
*<38>	:= информация о работе релейной защиты с меткой времени CP56Время2a	M_EP_TD_1
*<39>	:= упакованная информация о срабатывании пусковых органов защиты с меткой времени CP56Время2a	M_EP_TE_1
*<40>	:= упакованная информация о срабатывании выходных цепей защиты с меткой времени CP56Время2a	M_EP_TF_1
<41>..<44>	:= резерв для дальнейших совместимых определений	
<45>	:= одноэлементная команда	C_SC_NA_1
<46>	:= двухэлементная команда	C_DC_NA_1
<47>	:= команда пошагового регулирования	C_RC_NA_1
<48>	:= команда установки, нормализованное значение	C_SE_NA_1
<49>	:= команда установки, масштабированное значение	C_SE_NB_1
<50>	:= команда установки, короткое число с плавающей запятой	C_SE_NC_1
<51>	:= строка из 32 битов	C_BO_NA _1
<52>..<57>	:= резерв для дальнейших совместимых определений	
<58>	:= одноэлементная команда с меткой времени CP56Время2a	C_SC_TA_1
<59>	:= двухэлементная команда с меткой времени CP56Время2a	C_DC_TA_1

<60>	:= команда пошагового регулирования с меткой времени CP56Время2a	C_RC_TA_1
<61>	:= команда уставки, нормализованное значение с меткой времени CP56Время2a	C_SE_TA_1
<62>	:= команда уставки, масштабированное значение с меткой времени CP56Время2a	C_SE_TB_1
<63>	:= команда уставки, короткое число с плавающей запятой с меткой времени CP56Время2a	C_SE_TC_1
<64>	:= строка из 32 битов с меткой времени CP56Время2a	C_BO_TA_1
<65>..<69>	:= резерв для дальнейши	
<70>	:= конец инициализации	M_EI_NA_1
<71>..<99>	:= резерв для дальнейших совместимых определений	M_EI_NA_1
<100>	:= команда опроса	C_IC_NA_1
<101>	:= команда опроса счетчика	C_CI_NA_1
<102>	:= команда считывания	C_RD_NA_1
<103>	:= команда синхронизации времени (опция, см. 7.6)	C_CS_NA 1
<105>	:= команда установки процесса в исходное состояние	C_RP_NA_1
<107>	:= команда тестирования с меткой времени CP56Время2a	C_TS_NA_1
<108>..<109>	:= резерв для дальнейших совместимых определений	C_IC_NA_1
<110>	:= параметр измеряемой величины, нормализованное значение	P_ME_NA_1
<111>	:= параметр измеряемой величины, масштабированное значение	P_ME_NB_1
<112>	:= параметр измеряемой величины, короткий формат с плавающей запятой	P_ME_NC_1
<113>	:= параметр активации	P_AC_NA_1
<114>..<119>	:= резерв для дальнейших совместимых определений	P_AC_NA_1
<120>	:= файл готов	F_FR_NA_1
<121>	:= секция готова	F_SR_NA_1
<122>	:= вызов директории, выбор файла, вызов файла, вызов секции	F_SC_NA_1
<123>	:= последняя секция, последний сегмент	F_LS_NA_1
<124>	:= подтверждение файла, подтверждение секции	F_AF_NA_1
<125>	:= сегмент	F_SG_NA_1
<126>	:= директория	F_DR_TA_1

В поле «ASDU COT (cause of transfer)» необходимо выбрать причину передачи. В поле «AD (ASDU адрес)» необходимо ввести числовое значение ASDU адреса (это адрес станции длиной 1 или 2 байта, который может быть структурирован, чтобы иметь возможность обращаться ко всей станции или к отдельному ее сектору). В поле «IOA (адрес объекта информации)»

необходимо ввести адрес объекта информации в формате диапазона. В поле «IOA значение» необходимо ввести IOA значение или оставить пустым и нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 122).

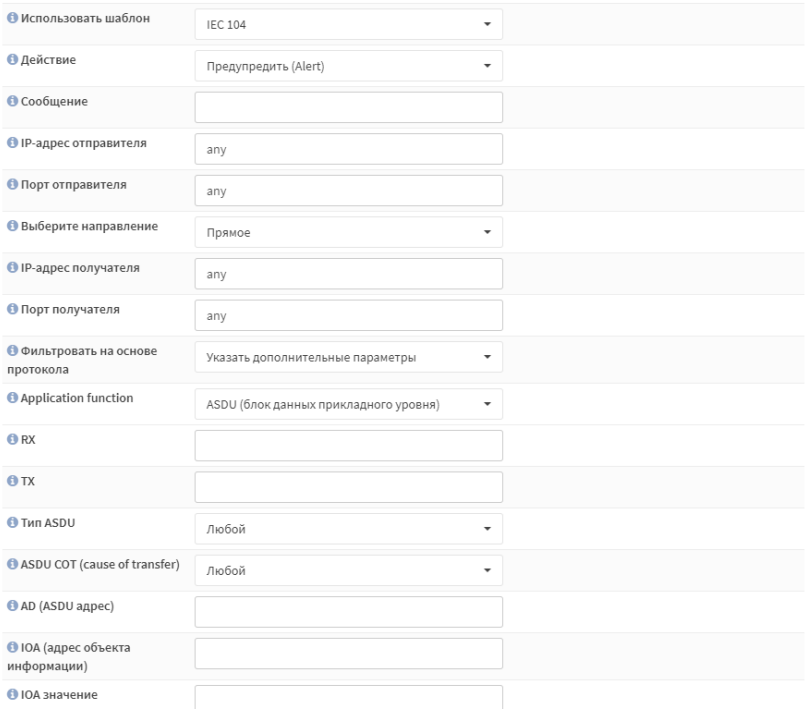


Рисунок 122 — Обнаружение вторжений: Контроль уровня приложений (редактирование IEC104)

5.2.3. S7comm

При использовании шаблона протокола S7comm появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Тип сообщения» необходимо выбрать тип сообщения в соответствие с таблицей (таблица 4).

Таблица 4 — Тип сообщения

№	Тип сообщения	Описание
1	JOBREQUEST	Пакет с запросом на выполнение функции
2	ACK	Пакет с результатом выполнения операции
3	ACKDATA	Пакет с ответом на запрос

4	USERDATA	Пакет с данными пользователя

При выборе «JOBREQUEST» в поле «Тип сообщения» появятся следующие поля.

В поле «Функция» необходимо выбрать функцию в соответствие с таблицей (таблица 5).

Таблица 5 — Функции протокола S7COMM

№	**Функция**	**Описание**
1	CPUSERVICE	Сервисы ЦП
2	SETUPCOMM	Запрос на подключение к ПЛК
3	READVAR	Запрос на чтение
4	WRITEVAR	Запрос на запись
5	REQUESTDOWNLOAD	Запрос на загрузку прошивки
6	DOWNLOADBLOCK	Загрузка прошивки на ПЛК
7	DOWNLOADENDED	Запрос на завершение загрузки прошивки на ПЛК
8	STARTUPLOAD	Запрос на выгрузку прошивки
9	UPLOAD	Выгрузка прошивки с ПЛК
10	ENDUPLOAD	Окончание выгрузки прошивки с ПЛК
11	PLCCONTROL	Управление ПЛК
12	PLCSTOP	Остановка ПЛК

При выборе в поле «Функция» функции «READVAR» появятся следующие поля.

В поле «Тип области» необходимо выбрать тип области чтения (таблица 6).

Таблица 6 — Тип области

№	Тип области	Описание
1	Любой	Любая область чтения
2	SI (System info)	Системная информация
3	SF (System flags)	Системные флаги
4	AI (Analog inputs)	Анлоговый ввод
5	AO (Analog outputs)	Аналоговый вывод
6	C (Counters)	Счетчики
7	T (Timers)	Таймеры
8	IC (IEC Counters)	Счетчики IEC
9	IT (IEC Timers)	Таймеры IEC
10	P (Directp peripheral access)	Прямой доступ к периферии
11	I (Inputs)	Ввод
12	Q (Outputs)	Вывод
13	M (Flags)	Флаги
14	DB (Data blocks)	Блоки данных
15	DI (Instance data blocks)	Блоки данных экземпляра
16	LV (Local data)	Локальные данные

При выборе в поле «Тип области» всех значений кроме значения «Любой» появятся следующие поля:

- «Имя области»;
- «Тип данных»;
- «Количество данных»;

– «Смещение данных».

В поле «Имя области» необходимо ввести номер области (от 0 до 65535).

В поле «Тип данных» необходимо выбрать тип данных.

В поле «Количество данных» необходимо ввести количество записей указанного типа.

В поле «Смещение данных» необходимо указать целочисленное значение в шестнадцатеричной системе счисления в формате 0x000000

При выборе в поле «Функция» функции «WRITEVAR» появятся следующие поля.

В поле «Тип области» необходимо выбрать тип области записи (таблица 6).

При выборе в поле «Тип области» всех значений кроме значения «Любой» появятся следующие поля:

– «Имя области»;

– «Тип данных»;

– «Количество данных»;

– «Смещение данных».

В поле «Имя области» необходимо ввести номер области (от 0 до 65535).

В поле «Тип данных» необходимо выбрать тип данных.

В поле «Количество данных» необходимо ввести количество записей указанного типа.

В поле «Смещение данных» необходимо указать целочисленное значение в шестнадцатеричной системе счисления в формате 0x000000.

В поле «Тип передаваемого значения» необходимо выбрать тип данных из следующих типов значений:

– «NULL» — не выбрано;

– «BIT» — значение в битах;

– «BYTE» — значение в байтах;

– «INT» — целочисленное значение;
– «REAL» — вещественное;
– «STR» — строковое значение.

В поле «Количество передаваемых данных» необходимо ввести число значений указанного типа, которое будет передано в данном сообщении.

В поле «Список значений данных» необходимо ввести число значений указанного типа в 16й системе счисления, которое будет передано в данном сообщении.

При выборе в поле «Функция» функции «REQUESTDOWNLOAD» появятся следующие поля.

В поле «Тип блока» необходимо выбрать тип блока скачивания (таблица 7).

Таблица 7 — Тип блока

№	Тип блока	Описание
1	Любой	-
2	OB (Organisation Block, stores the main programs)	Организационный блок (хранит основные программы)
3	DB (Data Block, stores data required by the PLC program)	Блок данных (хранит данные для ПЛК программы)
4	SDB (System Data Block, stores data required by the PLC program)	Системный блок (хранит данные необходимые для ПЛК программы)
5	FC (Function, functions that are stateless (do not have their own memory), they can be called from other programs)	Функция (функции, которые не имеют состояния и могут быть вызваны другими

		программами)
6	SFC (System Function, functions that are stateless (do not have their own memory), they can be called from other programs)	Система функций (функции, которые не имеют состояния и могут быть вызваны другими программами)
7	FB (Function Block, functions that are stateful, they usually have an associated SDB)	Блок функций (функции, которые имеют состояния)
8	SFB (System Function Block, functions that are stateful, they usually have an associated SDB)	Блок системы функций (функции, которые не имеют состояния и могут быть вызваны другими программами)

При выборе в поле «Тип блока» значения кроме «Любой» появятся следующие поля.

В поле «Номер блока» необходимо ввести пятизначное число в 10ой системе счисления.

В поле «Целевая файловая система» необходимо выбрать:

– «P — пассивная (блок требует активации после скачивания)»;
– «A — активная (блок будет активизирован после скачивания)».

При выборе в поле «Функция» функции «DOWNLOADBLOCK» появятся следующие поля.

В поле «Тип блока» необходимо выбрать тип блока скачивания (таблица 7).

При выборе в поле «Тип блока» значения кроме «Любой» появятся следующие поля.

В поле «Номер блока» необходимо ввести пятизначное число в 10ой системе счисления.

В поле «Целевая файловая система» необходимо выбрать:

– «P — пассивная (блок требует активации после скачивания)»;

– «A — активная (блок будет активизирован после скачивания)».

При выборе в поле «Функция» функции «STARTUPLOAD» появятся следующие поля.

В поле «Тип блока» необходимо выбрать тип блока загрузки (таблица 7).

При выборе в поле «Тип блока» значения кроме «Любой» появятся следующие поля.

В поле «Номер блока» необходимо ввести пятизначное число в 10ой системе счисления.

В поле «Целевая файловая система» необходимо выбрать:

– «P — пассивная (блок требует активации после скачивания)»;

– «A — активная (блок будет активизирован после скачивания)».

При выборе в поле «Функция» функции «PLCCONTROL» появятся следующие поля.

В поле «Функция» необходимо выбрать функцию управления ПЛК:

– «INSE (Активация скаченного 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)».

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 123).

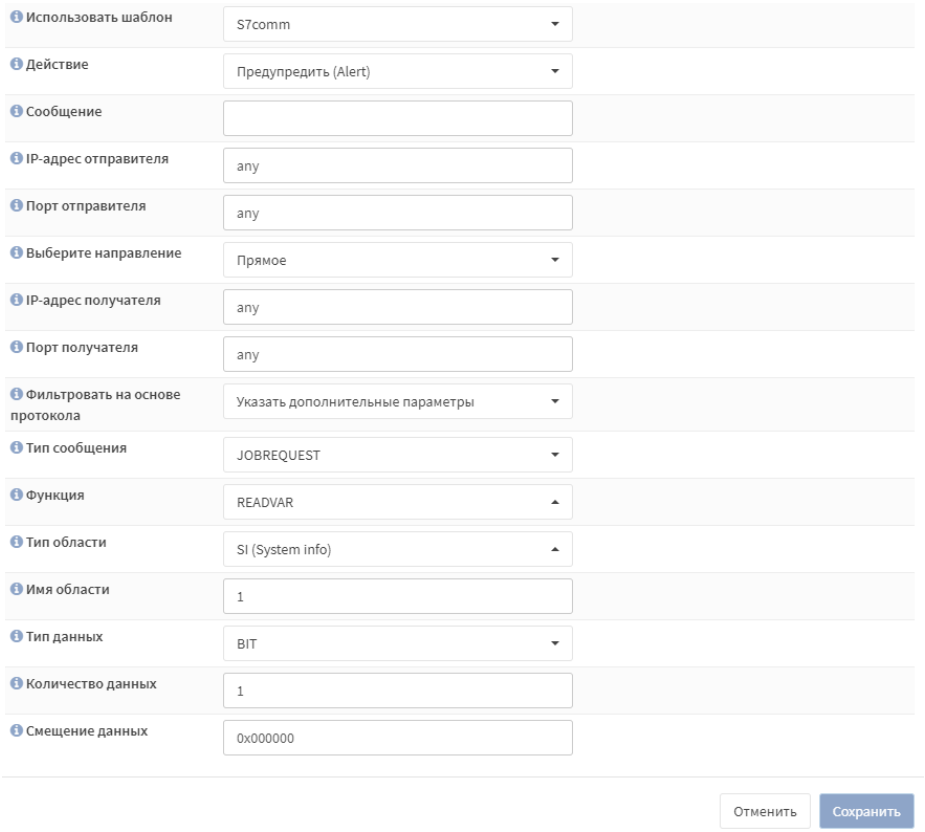


Рисунок 123 — Обнаружение вторжений: Контроль уровня приложений (редактирование: S7comm)

5.2.4.ENIP/CIP

При использовании шаблона протокола ENIP/CIP появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-

адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Совпадение по» необходимо выбрать признаки совпадения:

– ENIP команда (сопоставление по команде ENIP с настройкой «enip_command);

– CIP service (сопоставление в CIP Service с настройкой «cip_service»).

– ENIP команда CIP сервис (сопоставление команды ENIP и службы CIP с «enip_command» и «cip_service» вместе).

Если выбрать «ENIP команда» в поле «Совпадение по», появится поле «Команда». В данное поле необходимо ввести номер команды ENIP (например: 99).

Если выбрать «CIP service» в поле «Совпадение по», появится поле «Службы». В данное поле необходимо ввести сервис.

В «Use class» необходимо поставить флажок при необходимости включения возможности совпадения по классу. При установленном флажке в поле «Use class» появится поле «Class». В поле «Class» необходимо ввести значение класса.

В «Use attribute» необходимо поставить флажок при необходимости включения возможности совпадения по атрибуту. При установленном флажке в поле «Use attribute» появится поле «Атрибут». В поле «Атрибут» необходимо ввести значение атрибута.

Если выбрать «ENIP команда CIP сервис» в поле «Совпадение по», появится поля (описание полей приведено выше):

– «Команда»;

– «Службы»;

– «Use class»;

– «Class»;

– «Use attribute»;

– «Атрибут».

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 124).

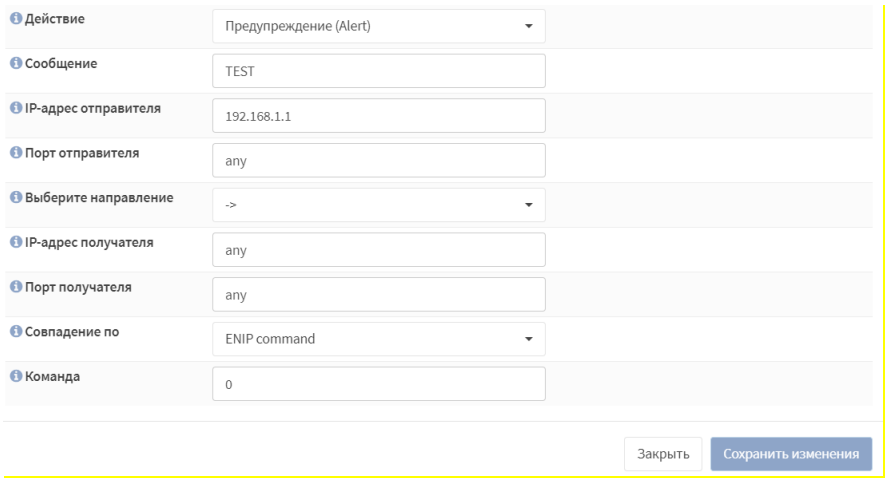


Рисунок 124 — Обнаружение вторжений: Контроль уровня приложений (редактирование: ENIP/CIP)

5.2.5.OPC UA

При использовании шаблона протокола OPC UA появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Тип сообщения» необходимо выбрать тип 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» в поле «Тип сообщения» появятся следующие поля.

В поле «Политика безопасности» необходимо выбрать политику безопасности:

– «Любой» — любая политика безопасности;

– «NONE» — политика безопасности для конфигураций с самыми низкими требованиями безопасности, нет алгоритмов шифрования;

– BASIC128RSA15 — политика безопасности для конфигураций со средними требованиями безопасности такие 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 такие 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 такие 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 такие 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 такие как:

– необходимо шифрование;

– необходима безопасная подпись;

– использование алгоритма шифрования AES 128 CTR;

– PUBSUB_AES256_CTR — политика безопасности для конфигураций со средними требованиями безопасности такие как:

– необходимо шифрование;

– необходима безопасная подпись;

– использование алгоритма шифрования AES 128 CTR.

При выборе «MESSAGE» в поле «Тип сообщения» появятся следующие поля.

В поле «Тип запроса» необходимо выбрать тип запроса в соответствие с таблицей (таблица 8).

Таблица 8 — Типы запросов OPC UA

№	Тип запроса	Описание
1	FINDSERVERS	Запрос известных серверов
2	FINDSERVERSONNETWORK	Запрос известных работающих серверов
3	GETENDPOINTS	Запрос на поддерживаемые сервером конечные точки
4	REGISTERSERVER	Запрос на регистрацию сервера
5	REGISTERSERVER2	Запрос на регистрацию сервера с дополнительной информации для FINDSERVERSONNETWORK
6	CREATESESSION	Запрос на создание сессии
7	ACTIVATESESSION	Запрос на создание сессии (передача идентификационных данных клиента)
8	CLOSESESSION	Запрос на завершение сессии
9	CANCEL	Запрос отмены

		невыполненных запросов на обслуживание
10	ADDNODES	Запрос на добавление узла как дочерний в адресное пространство
11	ADDREFERENCES	Запрос на добавление ссылки на узел
12	DELETENODES	Запрос на удаление узла из адресного пространства
13	DELETEREFERENCES	Запрос на удаление ссылки узла
14	BROWSE	Запрос на просмотр узлов
15	BROWSENEXT	Запрос на продолжение просмотра результата запроса BROWSE, если результат этого запроса превышает максимального значения
16	TRANSLATEBROWSEPATHSTONODEIDS	Запрос на преобразование пути узла в идентификатор узла
17	REGISTERNODES	Запрос на регистрацию узла (например узла, информация о котором пользователю известна)
18	UNREGISTERNODES	Запрос на отмену регистрации узла
19	QUERYFIRST	Запрос просмотр данных из определенного экземпляра
20	QUERYNEXT	Запрос на продолжение

		просмотра результата запроса QUERYFIRST, если результат этого запроса превышает максимального значения
21	READ	Запрос на чтение данных
22	HISTORYREAD	Запрос на просмотр значений или событий узлов
23	WRITE	Запрос на изменение узла
24	HISTORYUPDATE	Запрос на обновление значений или событий узлов
25	CALLMETHOD	Запрос на получение результатов вызова удаленной процедуры
26	CALL	Запрос на вызов удаленной процедуры
27	MONITOREDITEMCREATE	Запрос на начало подписки на событие
28	CREATEMONITOREDITEMS	Запрос на подписку на событие
29	MONITOREDITEMMODIFY	Запрос на изменение параметров подписки на события
30	MODIFYMONITOREDITEMS	Запрос на изменение подписки
31	SETMONITORINGMODE	Запрос на установку режима подписки
32	SETTRIGGERING	Запрос на создание связи между событием и узлом

33	DELETEMONITOREDITEMS	Запрос на завершение подписки
34	CREATESUBSCRIPTION	Запрос на создание подписки на событие
35	MODIFYSUBSCRIPTION	Запрос на изменение подписки на событие
36	SETPUBLISHINGMODE	Запрос на включение отправки уведомлений по подпискам на событие
37	PUBLISH	Запрос на подтверждение получения уведомлений по подпискам на события
38	REPUBLISH	Запрос на повторную отправку уведомлений по подпискам на события
39	TRANSFERSUBSCRIPTIONS	Запрос на передачу подписки на событие из одной сессии в другую
40	DELETESUBSCRIPTIONS	Запрос на удаление подписки на событие

При выборе «BROSE» в поле «Тип запроса» появятся следующие поля.

В поле «Значение» необходимо ввести диапазон запроса, например, «[2:]», «[:2]», «[2:3]».

При выборе «READ» в поле «Тип запроса» появятся следующие поля.

В поле «Значение» необходимо ввести диапазон запроса, например, «[2:]», «[:2]», «[2:3]».

При выборе «WRITE» в поле «Тип запроса» появятся следующие поля.

В поле «Значение» необходимо ввести диапазон запроса, например, «[2:]», «[:2]», «[2:3]».

При выборе «CALL» в поле «Тип запроса» появятся следующие поля.

В поле «Имя вызываемого объекта» необходимо ввести идентификатор узла, содержащий вызываемую процедуру.

В поле «Имя вызываемой процедуры» необходимо ввести идентификатор узла вызываемой процедуры.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 125).

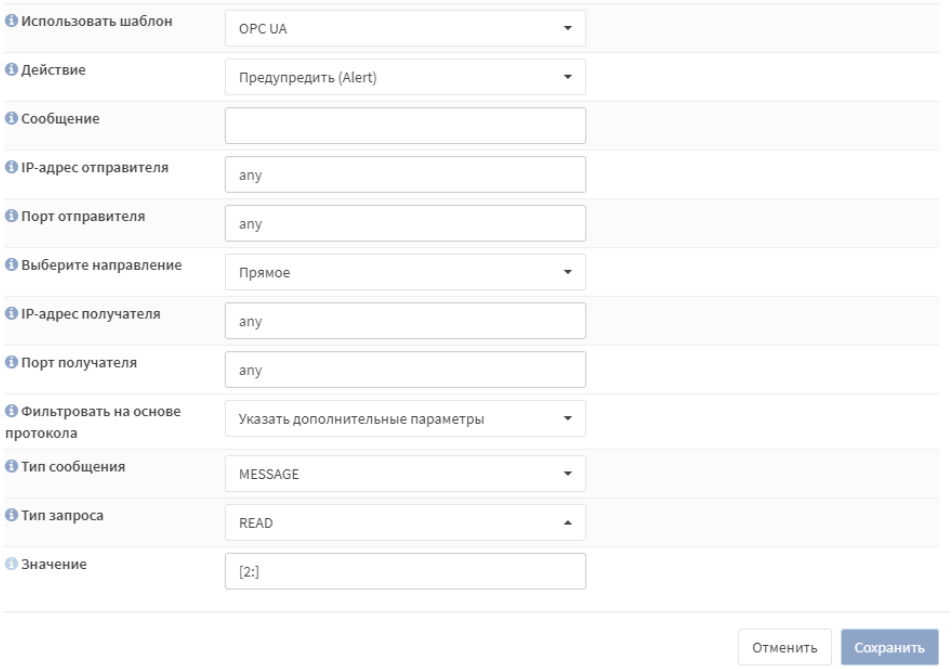


Рисунок 125 — Обнаружение вторжений: Контроль уровня приложений (редактирование: OPC UA)

5.2.6.OPC DA

При использовании шаблона протокола OPC DA появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Тип сообщения» необходимо выбрать тип сообщения в соответствие с таблицей (таблица 9).

Таблица 9 — Типы сообщений OPC DA

№	Тип сообщения	Описание
1	REQUEST	Сообщение запроса на операцию
2	PING	Сообщение запроса обратного вызова
3	RESPONSE	Сообщение ответа

4	FAULT	Сообщение сбоя
5	WORKING	Сообщение подтверждающее, что все исходящие пакеты получены
6	NOCALL	Ответ на команду PING
7	REJECT	Сообщение отклонения пакета
8	ACK	Подтверждение получения ответа
9	CI_CANCEL	Отмена операции
10	FACK	Если состояние вызова не STATE_SEND_FRAGS, отбросить пакет
11	CANCEL_ACK	Подтверждение отмены операции
12	BIND	Установка сессии
13	BIND_ACK	Подтверждение установки сессии
14	BIND_NACK	Отказ в установки сесии с выбранными параметрами
15	ALTER_CONTEXT	Изменение параметров сессии
16	ALTER_CONTEXT_RESP	Подтверждение изменения параметров сессии
17	SHUTDOWN	Сброс соединения
18	AUTH3	Обновление авторизации пользователя
19	CO_CANCEL	Передача команды отмены
20	ORPHANED	Флаг невозможности отмены операции

При выборе «REQUEST» в поле «Тип сообщения» появятся следующие поля.

В поле «Идентификатор вызываемого объекта» необходимо ввести идентификатор объекта, например, «99fcfec4-5260-101b-bbcb-00aa0021347a».

В поле «Номер вызываемой функции объекта» необходимо ввести номер вызываемой функции, например, «3».

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 126).

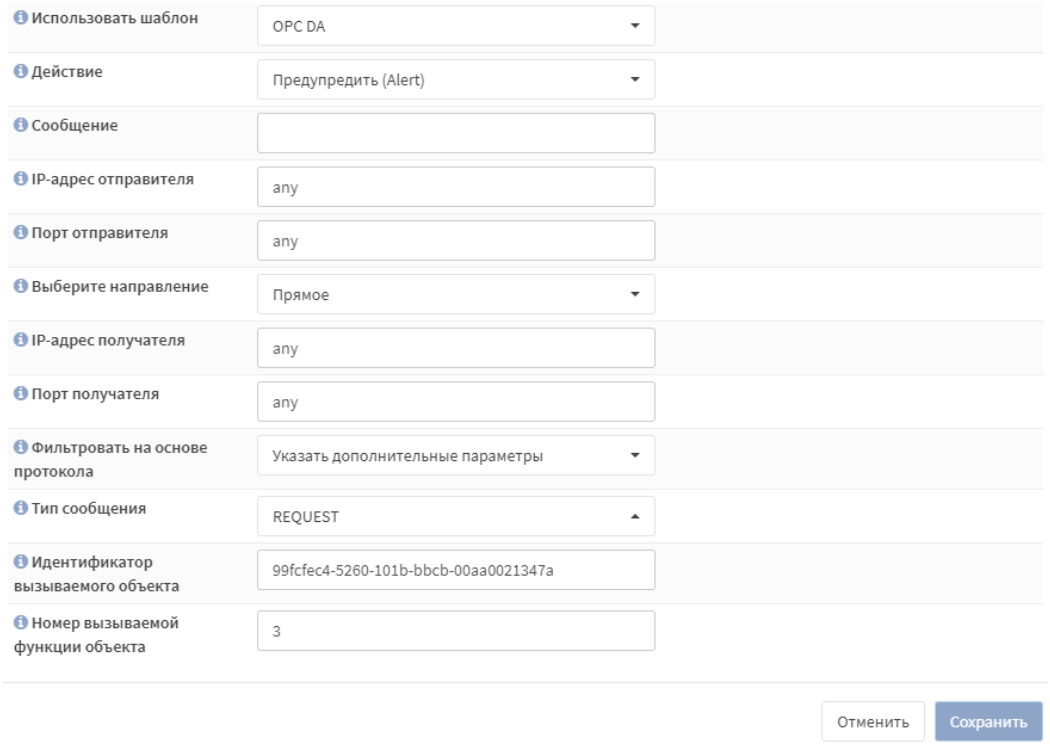


Рисунок 126— Обнаружение вторжений: Контроль уровня приложений (редактирование: OPC DA)

5.2.7. UMAS

При использовании шаблона протокола UMAS появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт

отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Функция» необходимо выбрать одну из функций, перечисленным в таблице (таблица 10).

Таблица 10 — Функции протокола UMAS

Код	**Название**	**Описание**
0x01	INIT_COMM	Инициализация UMAS сессии
0x02	READ_ID	Запрос PLC ID
0x03	READ_PROJECT_INFO	Чтение информации о проекте
0x04	READ_PLC_INFO	Чтение внутренней информации PLC
0x06	READ_CARD_INFO	Чтение информации о внутренней SD карты PLC

Код	Название	Описание
0x0A	REPEAT	Отправить информацию обратно PLC. Используется для синхронизации
0x10	TAKE_PLC_RESERVATION	Назначить PLC владельца
0x11	RELEASE_PLC_RESERVATION	Снять владельца PLC
0x12	KEEP_ALIVE	Поддержка активного соединения
0x20	READ_MEMORY_BLOCK	Чтение блока памяти с PLC
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 PLC
0x25	WRITE_COILS_REGISTERS	Запись катушек и регистров в PLC
0x30	INITIALIZE_UPLOAD	Инициализация загрузки (копирование с инженерного ПК на PLC)
0x31	UPLOAD_BLOCK	Загрузка блока данных с инженерного ПК на PLC
0x32	END_STRATEGY_UPLOAD	Завершение загрузки (копирования с инженерного ПК на PLC)
0x33	INITIALIZE_DOWNLOAD	Инициализация скачивания (копирование с PLC на инженерный ПК)
0x34	DOWNLOAD_BLOCK	Скачивание блока данных с PLC на инженерный ПК
0x35	END_STRATEGY_DOWNLOAD	Конец скачивания (копирования с PLC на инженерный ПК)
0x39	READ_ETH_MASTER_DATA	Чтение Ethernet Master Data

Код	Название	Описание
0x40	START_PLC	Включение PLC
0x41	STOP_PLC	Выключение PLC
0x50	MONITOR_PLC	Мониторинг системных битов, системных слов и переменных
0x58	CHECK_PLC	Проверка статуса подключения PLC
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» в поле «Функция» появятся следующие поля.

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

- «REQ» — запрос;
- «RES» — ответ.

При выборе «READ_MEMORY_BLOCK» в поле «Функция» появятся следующие поля.

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

– «REQ» — запрос;

– «RES» — ответ.

В поле «Номер блока» необходимо ввести номер блока команды в формате диапазона.

В поле «Количество данных» необходимо ввести количество данных команды в формате диапазона.

В поле «Смещение» необходимо ввести смещение команды в формате диапазона.

При выборе «READ_VARIABLES» в поле «Функция» появятся следующие поля.

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

– «REQ» — запрос;

– «RES» — ответ.

В поле «Базовое смещение» необходимо ввести базовое смещение команды.

В поле «Относительное смещение» необходимо ввести относительное смещение команды.

В поле «Номер блока» необходимо ввести номер блока команды.

В поле «Количество значений» необходимо ввести количество значений команды.

В поле «Тип значений» необходимо выбрать тип значения:

– «BIT»;

– «WORD»;

– «DWORD».

При выборе «WRITE_VARIABLES» в поле «Функция» появятся следующие поля.

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

– «REQ» — запрос;

– «RES» — ответ.

В поле «Номер блока» необходимо ввести номер блока команды.

В поле «Смещение» необходимо ввести смещение команды.

В поле «Тип значений» необходимо выбрать тип значения:

– «BIT»;

– «WORD»;

– «DWORD».

В поле «Значение» необходимо ввести значение переменных команды.

При выборе «READ_COILS_REGISTERS» в поле «Функция» появятся следующие поля.

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

– «REQ» — запрос;

– «RES» — ответ.

В поле «Номер регистров флагов (Coils)» необходимо ввести номера регистров флагов (Coils).

В поле «Смещение» необходимо ввести смещение команды.

В поле «Тип значений» необходимо выбрать тип значений:

– «Регистр»;

– «Регистр флага (Coil)»;

– «Отсутствует».

При выборе «WRITE_COILS_REGISTERS» в поле «Функция» появятся следующие поля.

В поле «Информация о проекте» необходимо ввести номер проекта в формате диапазона.

В поле «Тип сообщения» необходимо выбрать тип сообщения:

– «REQ» — запрос;

– «RES» — ответ.

В поле «Номер регистров флагов (Coils)» необходимо ввести номера регистров флагов (Coils).

В поле «Смещение» необходимо ввести смещение команды.

В поле «Тип значений» необходимо выбрать тип значений:

– «Регистр»;

– «Регистр флага (Coil)»;

– «Отсутствует».

В поле «Условие» необходимо выбрать условие:

– «Больше чем»;

– «Меньше чем»;

– «Равно»;

– «Not».

В поле «Значение регистров флагов (Coils)» необходимо ввести значение регистров флагов (Coils).

Затем необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 127).

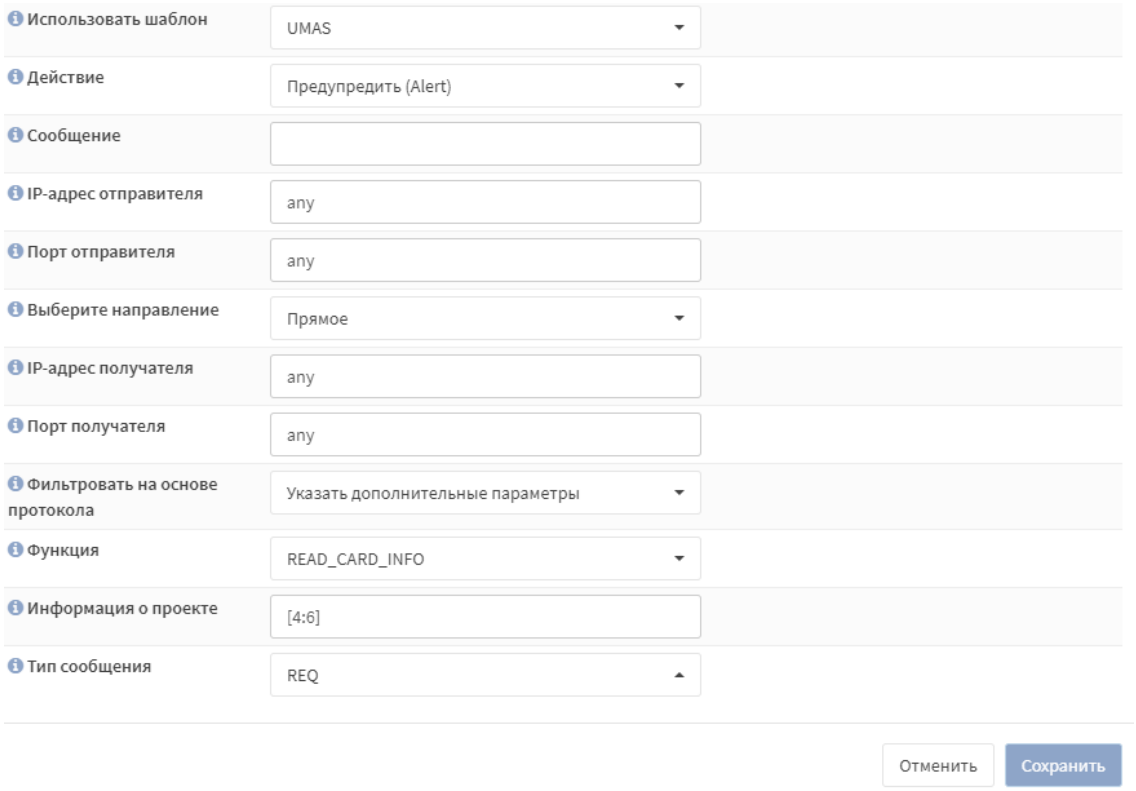


Рисунок 127 — Обнаружение вторжений: Контроль уровня приложений (редактирование: UMAS)

5.2.8.MMS

При использовании шаблона протокола MMS появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-

адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Тип сообщения» необходимо выбрать тип сообщения. Допустимы следующие значения:

- 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 «CONFIRMED_REQUEST» в поле «Тип сообщения» появятся следующие поля.

В поле «Тип службы» необходимо выбрать тип используемой службы. Допустимы следующие значения:

– 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 «ADDITIONALSERVICE» в поле «Тип службы» появятся следующие поля.

В поле «Дополнительный тип сервиса» необходимо выбрать дополнительный тип сервиса. Допустимы следующие значения:

– 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 «READ» в поле «Тип службы» появятся следующие поля.

В поле «ItemID запроса чтения» необходимо ввести значение переменной ItemID для функции чтения.

В поле «DomainID запроса чтения» необходимо ввести значение переменной DomainID для функции чтения.

В поле «Адрес запроса чтения» необходимо ввести адрес переменной для функции чтения в формате строки. Например, "123" или "test".

При выборе «WRITE» в поле «Тип службы» появятся следующие поля.

В поле «ItemID запроса записи» необходимо ввести значение переменной ItemID для функции записи.

В поле «DomainID запроса записи» необходимо ввести значение переменной DomainID для функции записи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 128).

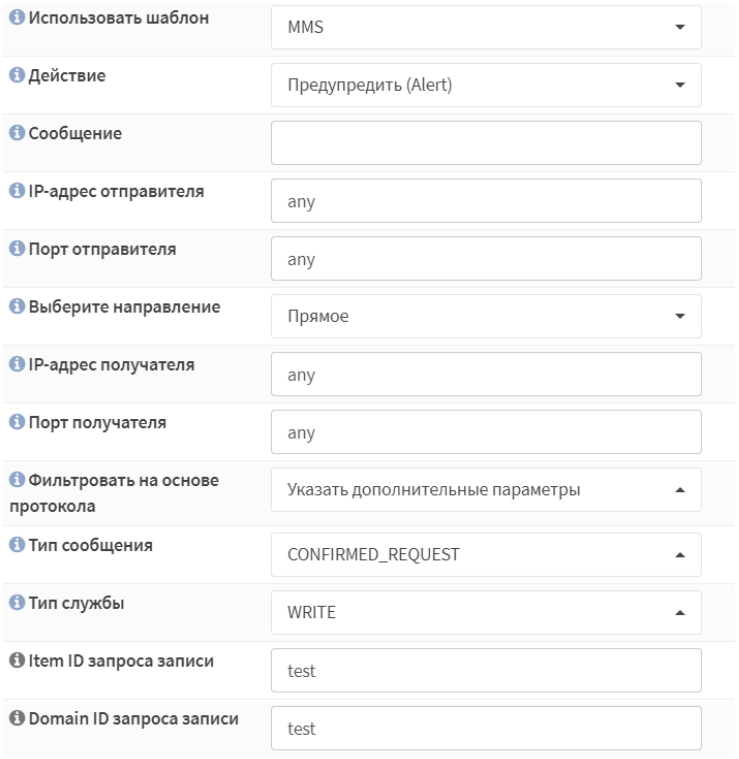


Рисунок 128— Обнаружение вторжений: Контроль уровня приложений (редактирование: MMS)

5.2.9.GOOSE

При использовании шаблона протокола GOOSE появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт

отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

- прямое (от источника к отправителю);
- прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты протокола» для создания правила фильтрации всех пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Любые пакеты кроме протокола» для создания правила фильтрации всех пакетов, кроме пакетов протокола.

В поле «Фильтровать на основе протокола» необходимо выбрать «Указать дополнительные параметры» для создания правила фильтрации с заданными параметрами протокола.

При выборе «Указать дополнительные параметры» в поле «Фильтровать на основе протокола» появятся следующие поля.

В поле «Идентификатор приложения» необходимо ввести диапазон значений идентификаторов приложений.

В поле «DATSET» необходимо ввести значение поля datset (значение не может быть пустым и должно содержать не более 150 символов).

В поле «GOCBREF» необходимо ввести значение поля gocbref (значение не может быть пустым и должно содержать не более 150 символов).

В поле «GOID» необходимо ввести значение поля goid (значение не может быть пустым и должно содержать не более 150 символов).

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 129).

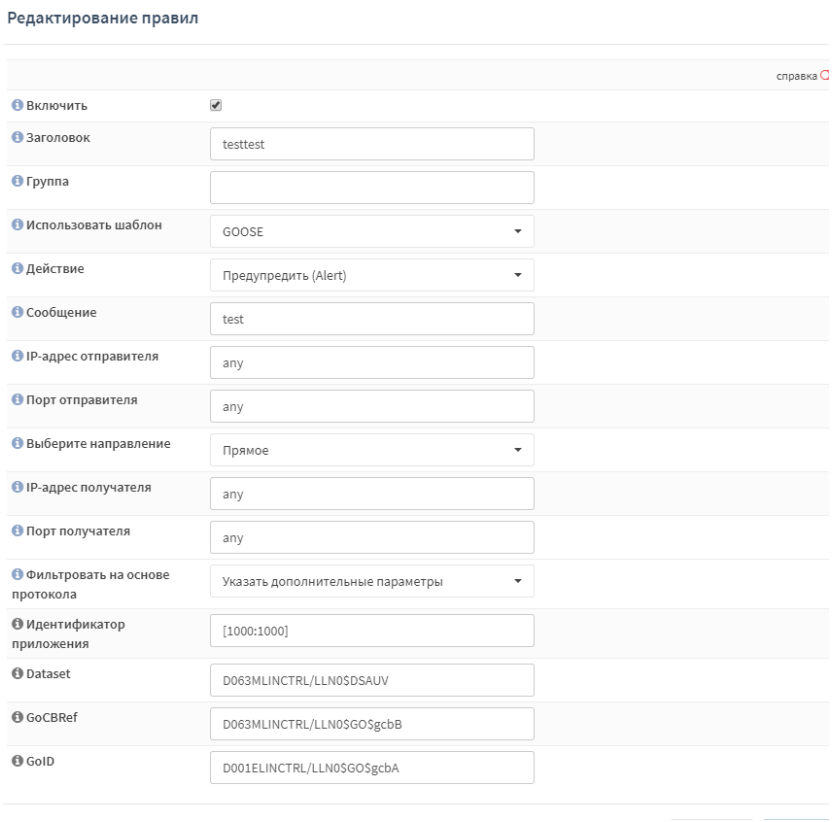


Рисунок 129— Обнаружение вторжений: Контроль уровня приложений (редактирование: GOOSE)

5.2.10. Вручную

При использовании шаблона «Вручную» появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет записываться в журнал предупреждений. В поле «IP-

адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Протокол» необходимо ввести часть протокола в правиле. В поле «Дополнительные параметры» необходимо ввести дополнительные параметры правила в соответствии с подсказками и форматом написания правил Snort/Suricata после чего необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 130).

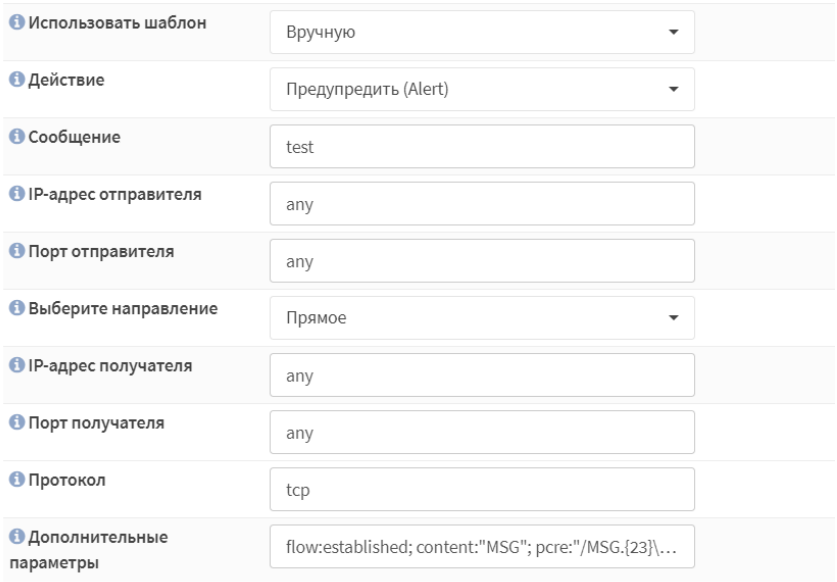


Рисунок 130 — Обнаружение вторжений: Контроль уровня приложений (редактирование: Вручную)

5.3. Подраздел «Журнал»

В подразделе «Журнал» отображается журнал внутренних событий Suricata. Имеется возможность производить поиск по журналу в поле «Искать конкретное сообщение…» и очищать журнал, нажав кнопку «Очистить журнал» (рисунок 131).

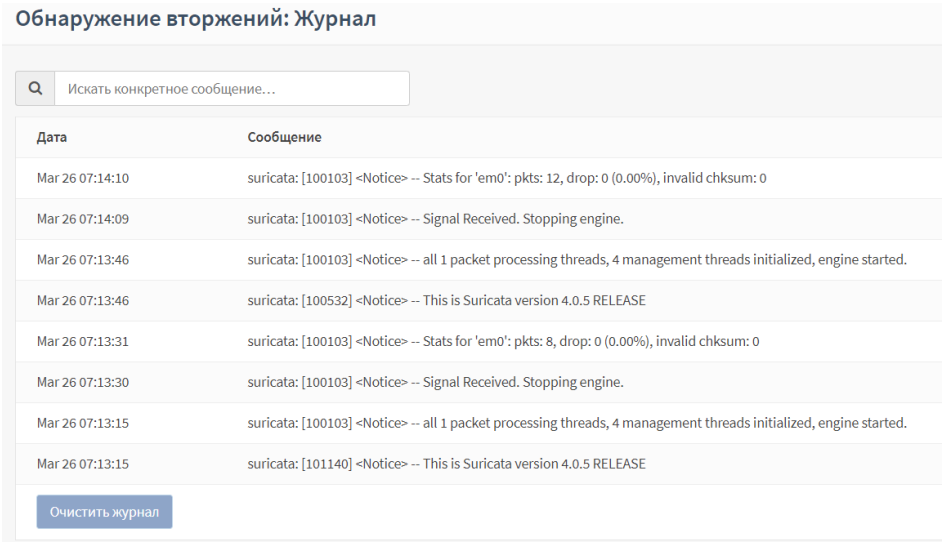


Рисунок 131 — Обнаружение вторжений: Журнал

Если поставлен флажок в поле «Передавать предупреждения (alerts) в syslog» в разделе «Обнаружение вторжений» - «Администрирование» - «Настройки» в журнале отображаются сообщения о срабатывании правил, которые имеют следующую информацию:

- значение gid (ключевое слово для различных групп правил);
- значение sid (идентификатор правила);
- значение rev (версия правила);
- сообщение правила;
- тип классификации правила (ClassType);
- priority типа классификации правила;
- протокол;
- IP-адрес отправителя;
- порт отправителя;
- IP-адрес получателя;
- порт получателя.

5.4. Подраздел «Настройки импорта правил»

Для настройки импорта базы решающих правил по запросу пользователя по протоколу FTP/SMB необходимо настроить подключение к FTP-серверу/samba-серверу.

Для импорта базы решающих правил по запросу пользователя по протоколу FTP во вкладке «Настройки» в поле «Включен» поставить флажок для включения импорта. В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения на FTP сервер. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах).

Нажать кнопку «Выполнить» для сохранения настроек и импорта правил. Нажать кнопку «Применить» только для сохранения настроек (рисунок 132).

Перед импортом баз решающих правил необходимо их заархивировать (при импорте правил используются архив наборов решающих правил формата «tar.gz»). Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz». При импорте правил выбирается файл правил с наиболее новой версией.

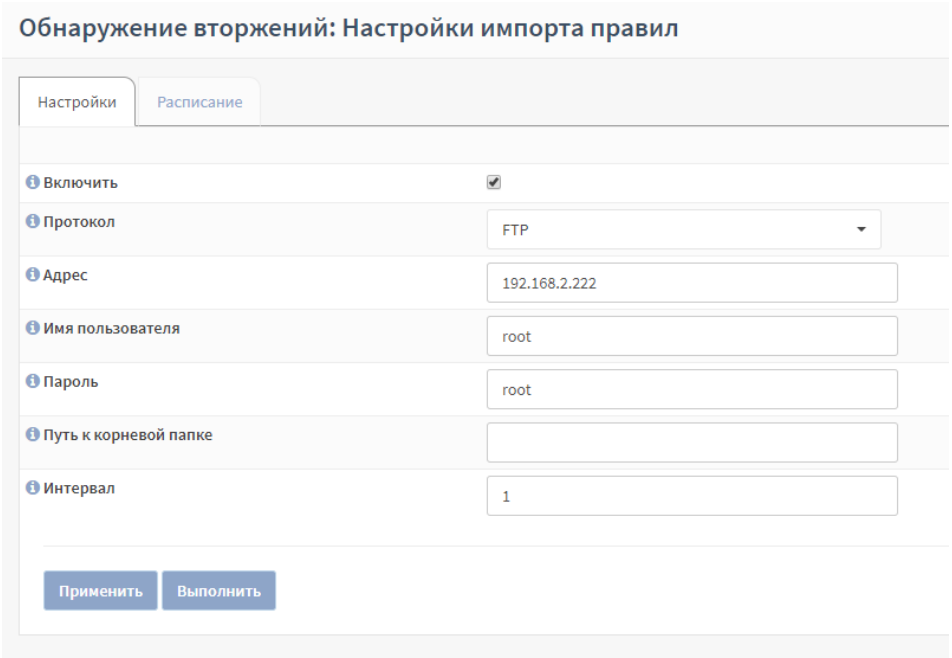


Рисунок 132 — Обнаружение вторжений: Настройки импорта правил (FTP): Настройки

Для импорта базы решающих правил по запросу пользователя по протоколу SMB во вкладке «Настройки» в поле «Включен» поставить флажок для включения импорта. В поле «Протокол» необходимо выбрать «SMB». В поле «Samba сервис» необходимо ввести название samba-сервера. В поле «Адрес» необходимо ввести IP-адрес samba-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения на samba-сервер. Поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах).

Нажать кнопку «Выполнить» для сохранения настроек и импорта правил. Нажать кнопку «Применить» только для сохранения настроек (рисунок 133).

Перед импортом баз решающих правил необходимо их заархивировать (при импорте правил используются архив наборов решающих правил формата «tar.gz»). Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz». При импорте правил выбирается файл правил с наиболее новой версией.

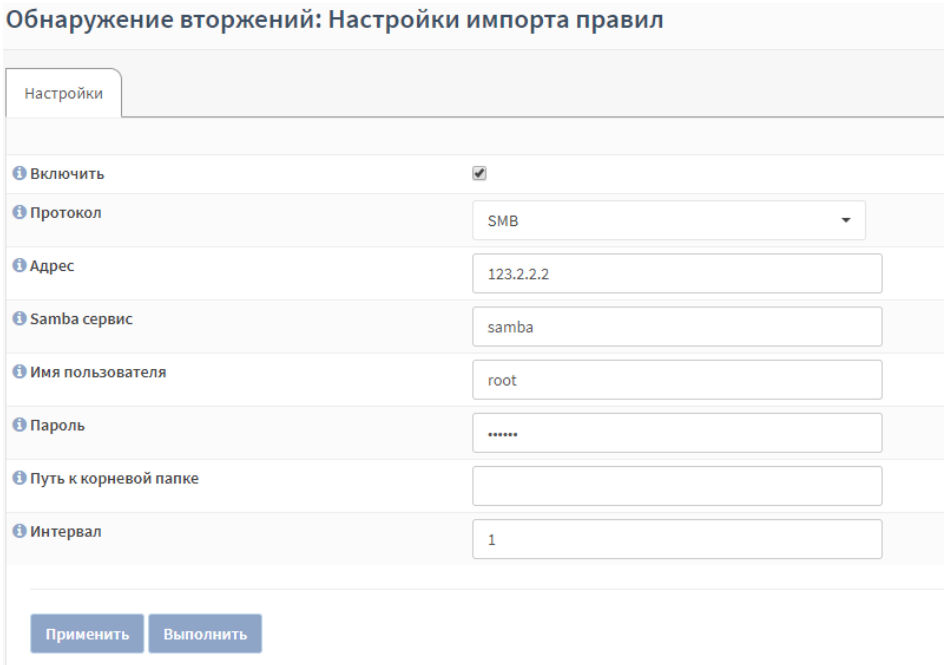


Рисунок 133 — Обнаружение вторжений: Настройки импорта правил (SMB): Настройки

Для настройки расписания импорта правил необходимо задать настройки во вкладке «Настройки», нажать кнопку «Применить» и перейти во вкладку «Расписание».

При нажатии на категорию «Расписание» происходит автоматическое перенаправление в редактирование расписания системы предотвращения вторжений, которое находится в разделе «Система» - «Настройки» - «Планировщик задач Cron». При редактировании расписания в поле «Команда» необходимо выбрать «Импорт правил СОВ» (рисунок 134).

Остальные параметры расписания расписаны более подробно в подразделе 6.3.8 настоящего документа.

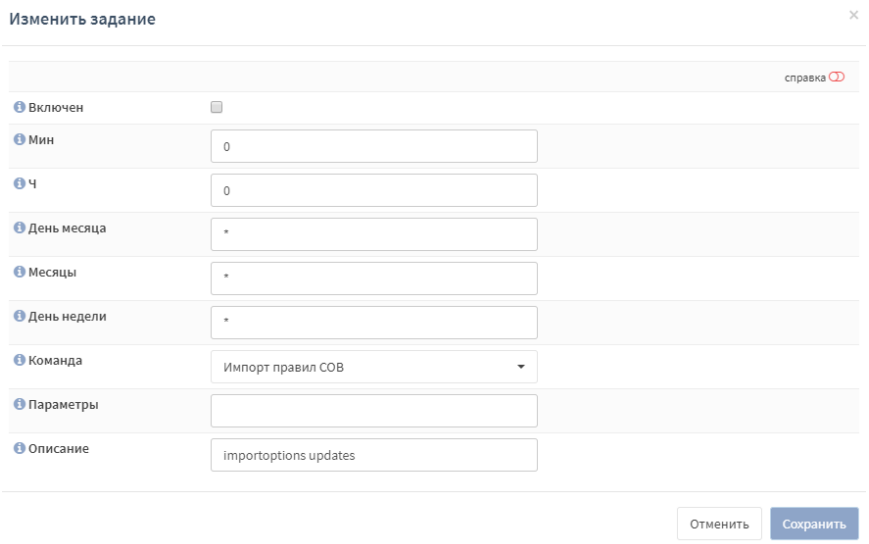


Рисунок 134 — Обнаружение вторжений: Настройки импорта правил: Расписание

6. Раздел «Система»

Раздел «Система» состоит из следующих подразделов:

- Доступ;
- Прошивка;
- Настройки;
- Шлюзы;
- Маршруты;
- Высокая доступность;
- Диагностика;
- Конфигурация;
- Доверенные сертификаты;
- Мастер;
- Журналы;
- Питание.

6.1. Подраздел «Доступ»

Подраздел «Доступ» позволяет настраивать пользователей, группы пользователей, серверы аутентификации, а также произвести проверку работы серверов аутентификации.

6.1.1. Категория «Пользователи»

Категория «Пользователи» описана в документе «Руководство администратора» в разделе 4, подразделе 4.3.

6.1.2. Категория «Группы»

Категория «Группы» описана в документе «Руководство администратора» в разделе 4, подразделе 4.4.

6.1.3. Категория «Серверы»

Категория «Серверы» описана в документе «Руководство администратора» в разделе 4, подразделе 4.1.

6.1.4. Категория «Средство проверки»

Категория «Средство проверки» описана в документе «Руководство администратора» в разделе 4, подразделе 4.1.

6.2. Подраздел «Прошивка»

Подраздел «Прошивка» позволяет загружать обновления ПО, просматривать таблицу контроля целостности и, в случае ошибки, информацию об ошибке системы.

6.2.1. Категория «Обновления»

Категория «Обновления» позволяет загружать обновления ПО ПК «InfoWatch ARMA Industrial Firewall».

Категория «Обновления» описана в документе «Руководство администратора» в разделе 7, подразделе 7.2.

6.2.2. Категория «Контроль целостности»

Категория «Контроль целостности» позволяет просматривать таблицу контроля целостности программных частей ПК:

- scripts — вспомогательные скрипты для различных задач;
- site python — вспомогательные модули Python, подключаемые в северный код;
- contrib — сторонние вспомогательные библиотеки;
- version — версия продукта;
- legacy www, mvc — программный код, связанный с веб сервером;
- service — программный код связанный с северным кодом (не связанный с веб интерфейсом).

В таблице содержится информация о названии ПО, ожидаемое значение контрольной суммы, вычисленное значение контрольной суммы (в случае совпадения с ожидаемым значением, оно будет выделено зеленым цветом, в противном случае — красным и появится уведомление о несовпадении контрольной суммы вверху страницы), время и дату вычисления контрольной суммы, а также позволяет пересчитать контрольную сумму файла, нажав на значок «обновить» напротив файла или пересчитать все контрольные суммы, нажав на кнопку «Все», находящуюся под таблицей. Также в таблице возможен выбор элементов и столбцов таблицы, которые необходимо отобразить (рисунок 135).

Рисунок 135 — Система: Прошивка: Контроль целостности

6.2.3.Категория «Ошибки работы системы»

В категории «Ошибки работы системы» отображается информация об ошибках системы (рисунок 136), в случае их отсутствия, отображается запись об отсутствие ошибок системы (рисунок 137).

Рисунок 136 — Система: Прошивка: Ошибки работы системы (обнаружена ошибка)

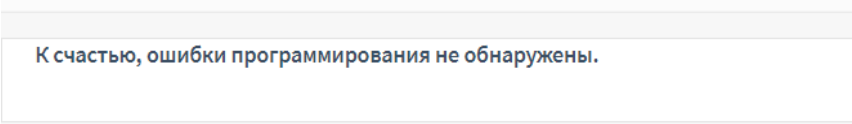


Рисунок 137 — Система: Прошивка: Ошибки работы системы (ошибки отсутствуют)

6.3. Подраздел «Настройки»

Подраздел «Настройки» позволяет ввести общие настройки системы и построения сети, настроить веб-интерфейс, доступ по SSH, консольный интерфейс, серверы аутентификации, изменить пароль входа в систему, настроить журналирование, SNMP, расписания с помощью планировщика Cron, параметры ядра.

6.3.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет настраивать систему и построение сетей.

В группе настроек «Система» в поле «Имя хоста» необходимо ввести имя хоста без доменной части. В поле «Домен» необходимо ввести доменное имя. В поле «Часовой пояс» необходимо выбрать часовой пояс. В поле «Язык» необходимо выбрать язык. В поле «Тема» необходимо выбрать тему визуального оформления интерфейса (рисунок 138).

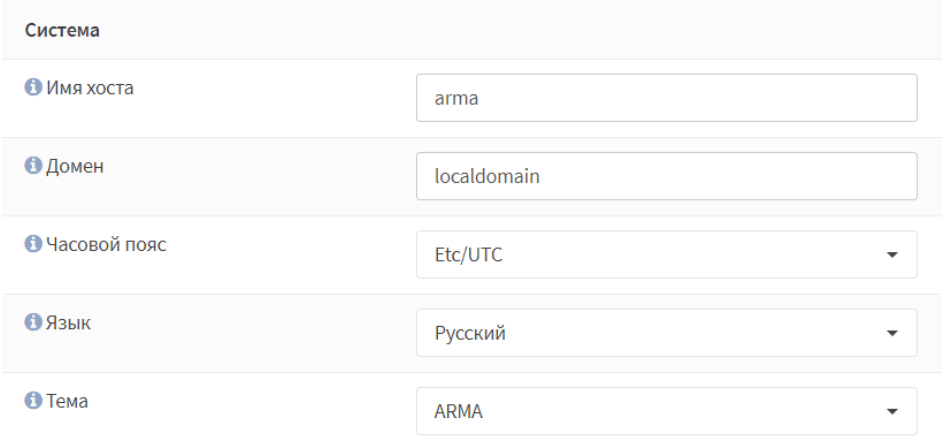


Рисунок 138 — Система: Настройки: Общие настройки (Система)

В группе настроек «Построение сетей» необходимо установить флажок в «Выбрать IPv4 через IPv6» при необходимости принудительного использования IPv4. В поле «DNS-серверы» необходимо выбрать IP-адреса, которые должны использоваться системой для разрешения DNS. В поле «Настройки DNS-сервера» необходимо установить флажок напротив поля «Позволить переопределять список DNS-серверов DHCP/PPP на WAN» для использования DNS-серверов, назначенных DHCP/PPP-сервером на WAN-интерфейсе. При необходимости отключения службы DNS как сервера имен необходимо установить флажок напротив поля «Не использовать службу DNS как сервер имен для данной системы» (рисунок 139).

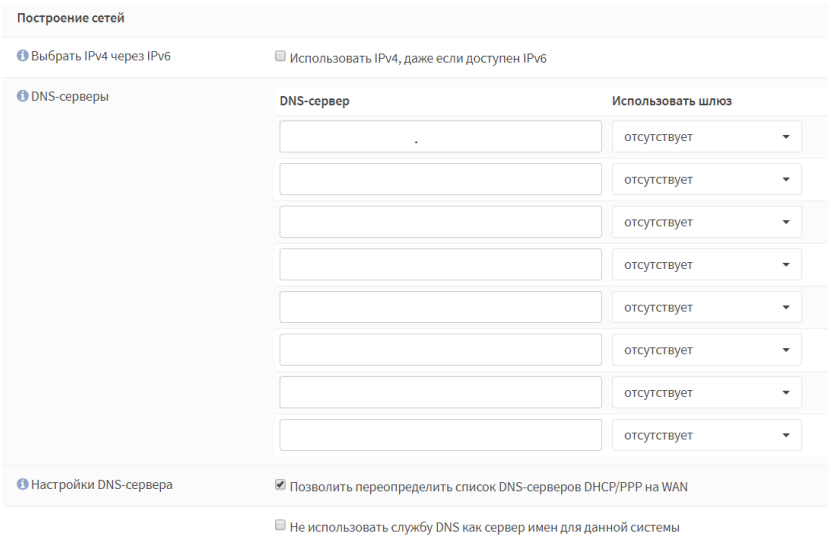


Рисунок 139 — Система: Настройки: Общие настройки (Построение сетей)

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.2. Категория «Администрирование»

Категория «Администрирование» позволяет настраивать веб-интерфейс, доступ через SSH, консольный интерфейс, а также серверы аутентификации.

В группе настроек «Веб-интерфейс» в поле «Протокол» необходимо выбрать протокол для подключения веб-интерфейсу (HTTP/HTTPS). В поле «Протокол Strict Transport Security HTTP» необходимо установить флажок

напротив поля «Включить протокол Strict Transport Security HTTP» при необходимости включения защиты веб-интерфейса от низкоуровневых атак взлома cookie по данному протоколу. В поле «Порт TCP» необходимо ввести номер порта для веб-интерфейса (по умолчанию 80 для HTTP, 443 для HTTPS). В поле «Успешная авторизация» необходимо установить флажок напротив поля «Отключить журналирование успешных входов в веб-интерфейс» при необходимости отключения журналирования успешных входов в веб-интерфейс в журнале событий системы. В поле «Тайм-аут сессии» необходимо ввести время простоя для сеансов. В поле «Проверка DNS Rebinding» необходимо установить флажок напротив поля «Отключить проверку DNS Rebinding» для отключения защиты системы от DNS Rebinding атак. В поле «Альтернативные имена хостов» необходимо ввести альтернативные имена хостов DNS Rebinding и HTTP_REFERER проверки. В поле «Сжатие HTTP» необходимо выбрать сжатие HTTP-страниц и динамического содержимого. В поле «Доступ к журналу» необходимо нажать на флажок напротив поля «Включить доступ к журналу» для включения доступа к журналу веб-интерфейса для отладки и анализа. В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, от которых необходимо принимать соединения для доступа к веб-интерфейсу. В поле «Принудительно использовать HTTP_REFERER» необходимо установить флажок напротив поля «Отключить принудительное использование HTTP_REFERER» для отключения защиты доступа к веб-интерфейсу от попыток перенаправления HTTP_REFERER (рисунок 140).

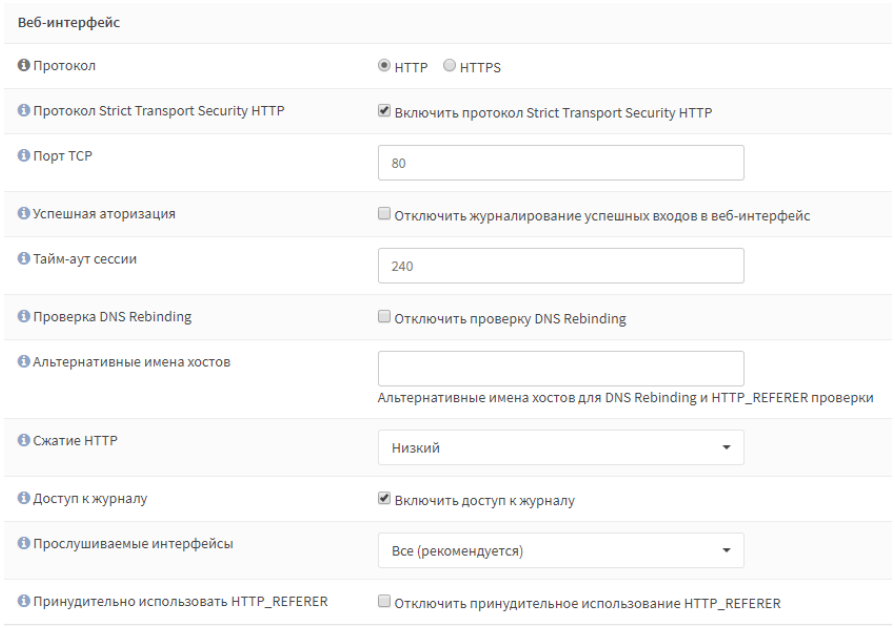


Рисунок 140— Система: Настройки: Администрирование (Веб-интерфейс)

В группе настроек «SSH» в поле «SSH-сервер» необходимо установить флажок напротив поля «Включите SSH» для включения SSH-сервера. В поле «Группа логина» необходимо выбрать разрешенные группы пользователей для удаленной авторизации по SSH. В поле «Вход суперпользователей (root) в учетную запись» необходимо установить флажок напротив «Разрешить парольный вход в учетную запись» для разрешения входа пользователя «root» через SSH. В поле «Метод аутентификации» необходимо установить флажок напротив «Разрешить парольный вход в учетную запись» для разрешения парольного входа в учетную запись по SSH. В поле «Порт SSH» необходимо ввести порт SSH или оставьте по умолчанию (22 порт). В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, через которые будет осуществляться доступ к SSH (рисунок 141).

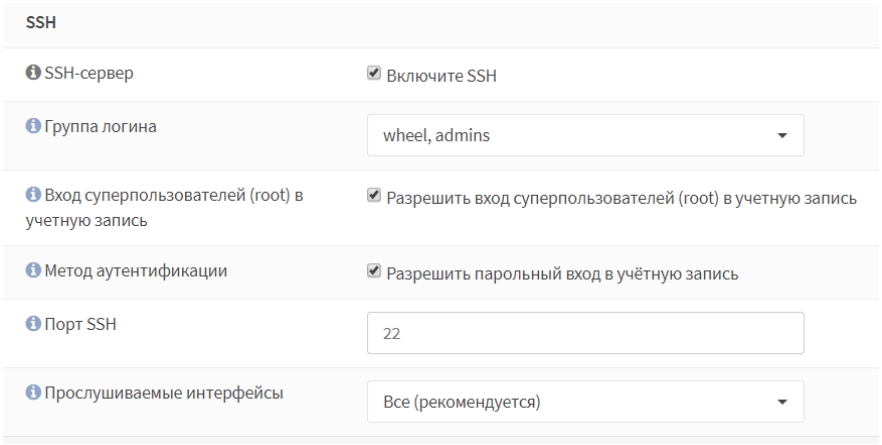


Рисунок 141— Система: Настройки: Администрирование (SSH)

В группе настроек «Консоль» в поле «Драйвер консоли» необходимо установить флажок напротив поля «Использовать драйвер виртуального терминала» для использования драйвера виртуального терминала. В поле «Главная консоль» необходимо выбрать основную консоль, которая будет показывать вывод сценариев загрузки. В поле «Вспомогательная консоль» необходимо выбрать вспомогательные консоли, которые будут отображать сообщения загрузчика ОС, сообщения консоли и меню консоли. В поле «Скорость последовательного порта» необходимо ввести значение скорости последовательного порта консоли. В поле «USB-порт» необходимо установить флажок для использования USB-порта. В поле «Меню консоли» необходимо установить флажок для защиты паролем меню консоли (рисунок 142).

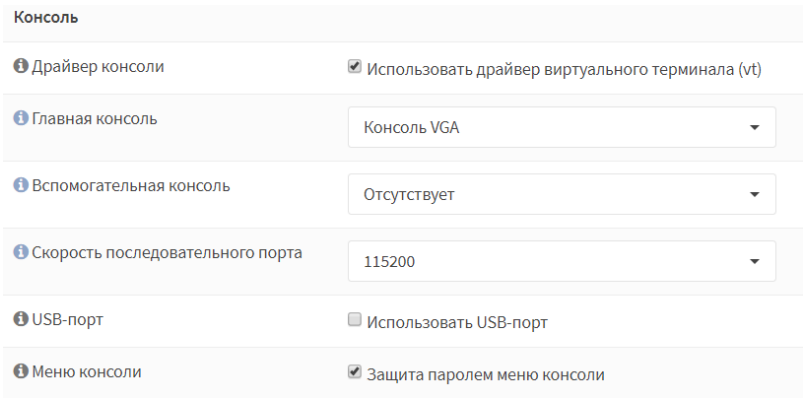


Рисунок 142— Система: Настройки: Администрирование (Консоль)

В группе настроек «Аутентификация» в поле «Серверы» необходимо выбрать серверы аутентификации для проверки учетных данных пользователей. В поле «Sudo (выполнение от имени суперпользователя)» необходимо выбрать разрешать или запрещать использование команды sudo для администраторов с доступом к командной строке. В поле «Система» необходимо установить флажок для отключения встроенной аутентификации (рисунок 143).

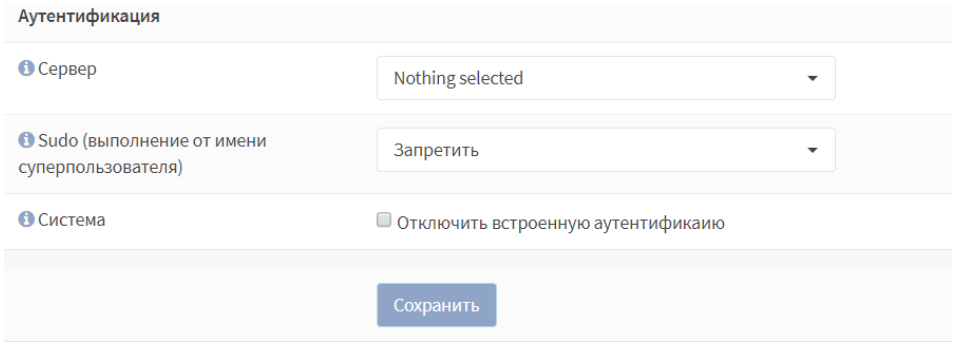


Рисунок 143— Система: Настройки: Администрирование (Аутентификация)

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.3.Категория «Пароль»

Категория «Пароль» позволяет изменить пароль учетной записи. Для этого в поле «Старый пароль» необходимо ввести действующий пароль. В поле «Новый пароль» необходимо ввести новый пароль. В поле «Подтверждение» необходимо ввести новый пароль еще раз. В поле «Язык» необходимо выбрать язык веб-интерфейса, который будет установлен после авторизации пользователя (рисунок 144).

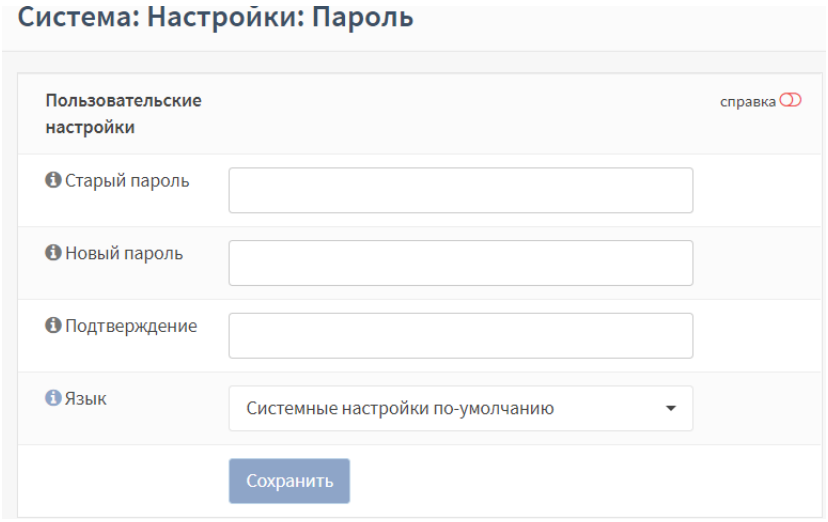


Рисунок 144 — Система: Настройки: Пароль

Для сохранения настроек необходимо нажать на кнопку «Сохранить».

6.3.4. Категория «Журналирование»

Категория «Журналирование» позволяет настраивать опции локальной и удаленной записи.

В группе настроек «Локальные опции записи» в поле «Обратный порядок отображения» необходимо установить флажок для представлять сохраняемые записи в обратном порядке. В поле «Записей в веб-интерфейсе» необходимо ввести количество записей, отображаемых в веб-интерфейсе. В поле «Размер журнала (байт)» необходимо ввести размер журнал веб-интерфейса в байтах. В поле «События межсетевого экрана по умолчанию» необходимо установить флажок напротив поля «Журналировать пакеты, соответствующие правилам блокировки по умолчанию из набора правил» для включения журналирования пакетов, которые заблокированы правилами блокировки по умолчанию, а напротив поля «Журналировать пакеты, соответствующие правилам разрешения (pass) по умолчанию из набора правил» для включения журналирования пакетов, которые разрешены правилами блокировки по умолчанию. Необходимо установить флажок напротив поля «Журналировать пакеты, блокированные правилом «Блокировать bogon сети»» для включения журналирования пакетов, которые заблокированы правилом «Блокировать bogon сети», а напротив

поля «Журналировать пакеты, блокированные правилом «Блокировать частные сети»» для включения журналирования пакетов, которые заблокированы правилом «Блокировать частные сети». В поле «Журнал веб-сервера» необходимо установить флажок напротив поля «Ошибка записи из-за сбоя сервера» для записи ошибок веб-сервера lighttpd в главном системном журнале. В поле «Локальные записи» необходимо установить флажок для выключения записи журнала на локальный диск. В поле «Сброс записей» необходимо нажать на кнопку «Очистить журналы» при необходимости очистить все локальные журналы (рисунок 145).

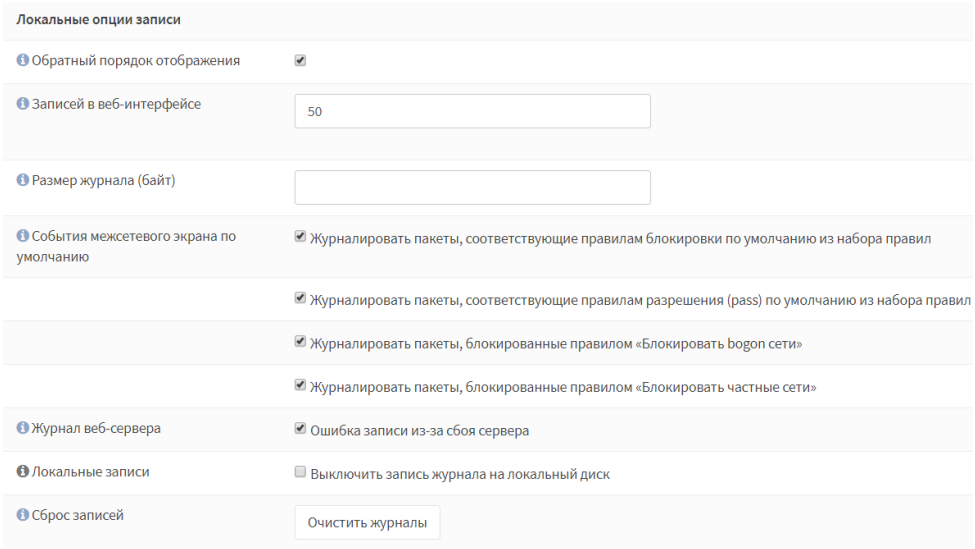


Рисунок 145 — Система: Настройки: Журналирование (Локальные опции записи)

В группе настроек «Опции удаленного журналирования» в поле «IP-адрес источника» необходимо указать IP-адрес источника, с использованием которого будут связываться сервисы выгрузки событий журналов с syslog-серверами в качестве адреса источника. В поле «Протокол IP» необходимо выбрать версию протокола IP. В поле «Включить удаленное журналирование» необходимо установить флажок для отправления сообщения журналов на удаленный syslog-сервер. В поле «Удаленные syslog-серверы» необходимо ввести IP-адреса удаленных syslog-серверов. В поле «Типы отправляемых событий» необходимо выбрать все события, которые необходимо отправлять на удаленные syslog-сервера (рисунок 146).

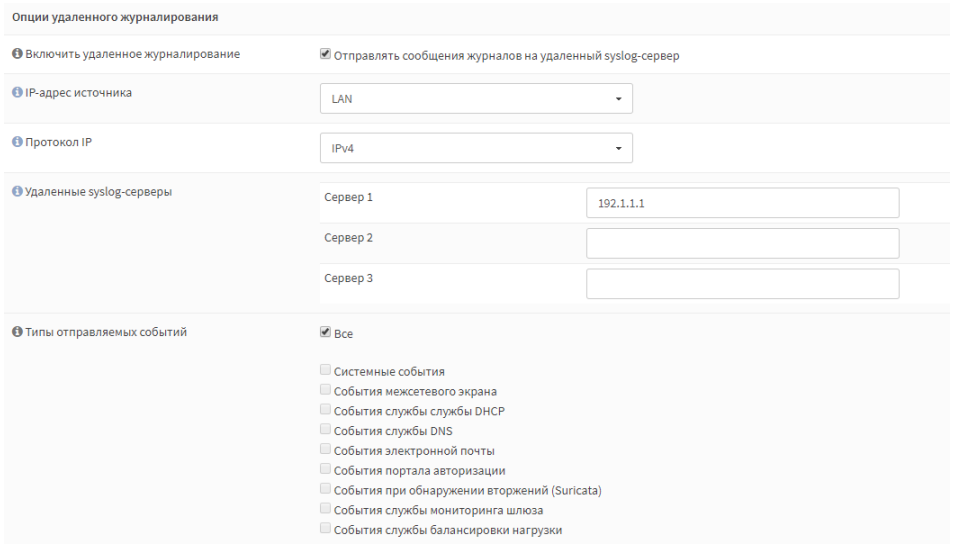


Рисунок 146 — Система: Настройки: Журналирование (Опции удаленного журналирования)

В группе настроек «CEF Опции удаленного журналирования» в поле «IP-адрес источника» необходимо указать IP-адрес источника, с использованием которого будут связываться сервисы выгрузки событий журналов с syslog-серверами в качестве адреса источника. В поле «Протокол IP» необходимо выбрать версию протокола IP. В поле «Включить удаленное журналирование» необходимо установить флажок для отправления сообщения журналов на удаленный syslog-сервер. В поле «Удаленные syslog-серверы» необходимо ввести IP-адреса удаленных syslog-серверов. В поле «Типы отправляемых событий» необходимо выбрать все события, которые необходимо отправлять на удаленные syslog-сервера (рисунок 147).

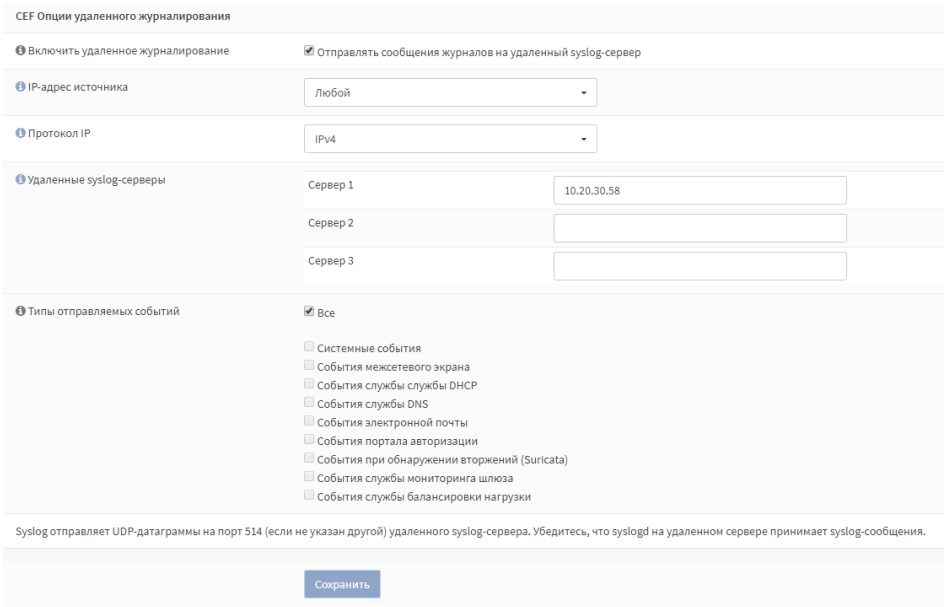


Рисунок 147 — Система: Настройки: Журналирование (Опции удаленного журналирования (CEF))

Для сохранения настроек журналирования необходимо нажать на кнопку «Сохранить».

6.3.5.Категория «SNMP»

Категория «SNMP» позволяет настраивать службу SNMP версии 2 и версии 3.

Во вкладке «Общие настройки» имеется возможность настроить SMNPv2 и SMNPv3. Для этого в поле «Включен» необходимо установить флажок для включения сервиса SNMP. В поле «Community String» необходимо ввести значение «Community String» (по умолчанию значение «public»). В поле «Расположение SNMP» необходимо ввести расположение системы. В поле «Контактная информация» необходимо ввести контактную информацию. В поле «Отображать себя как Layer3 устройство» необходимо поставить флажок для выставления значения iso.3.6.1.2.1.1.7.0 равным 76, что означает, что это оборудование будет видно, как оборудование, работающее на сетевом уровне 3 модели ISO OSI (рисунок 148).

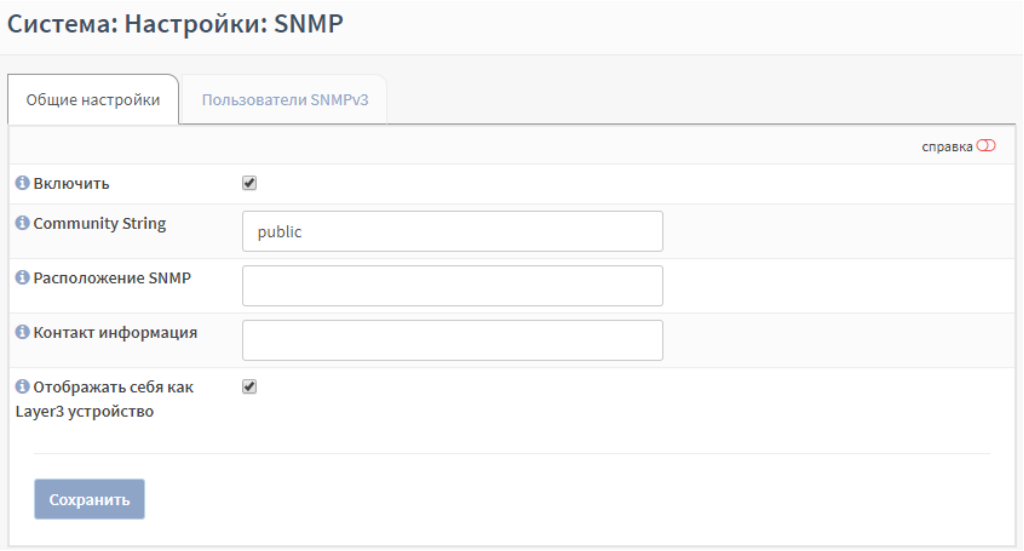


Рисунок 148 — Система: Настройки: SNMP: Общие настройки

Во вкладке «Пользователи SMNPv3» отображается таблица пользователей для возможности доступа по SMNPv3. Вкладка «Пользователи SMNPv3» позволяет включить/выключить /просматривать/редактировать/удалять/создавать пользователей (рисунок 149).

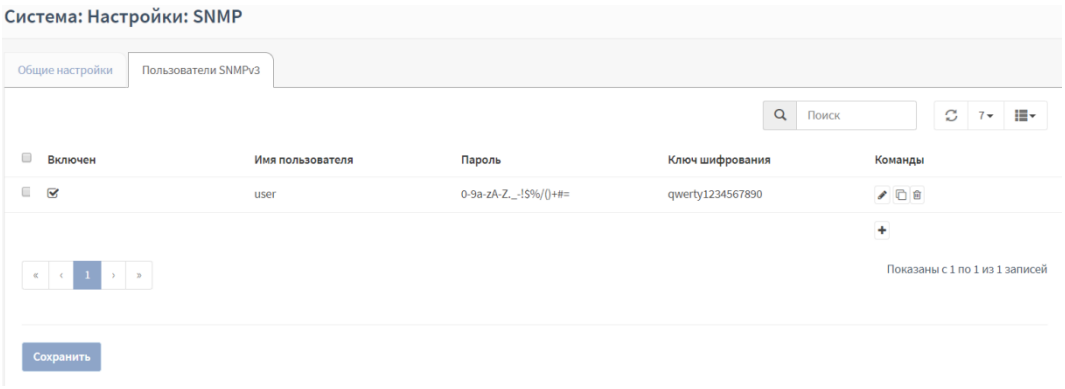


Рисунок 149 — Система: Настройки: SNMP: Пользователи SMNPv3

Для того чтобы редактировать существующего пользователя, необходимо нажать на кнопку напротив пользователя. Для того, чтобы создать нового пользователя, необходимо нажать на кнопку .

При редактировании пользователя в поле «Включен» необходимо установить флажок для возможности использования этого пользователя в SMNPv3. В поле «Имя пользователя» необходимо ввести имя пользователя. В поле «Пароль» необходимо ввести пароль пользователя. В поле «Ключ

шифрования» необходимо ввести ключ шифрования для защиты соединения между клиентом и этим хостом. В поле «Разрешить запись» необходимо установить флажок для включения возможности изменения параметров этому пользователю (рисунок 150).

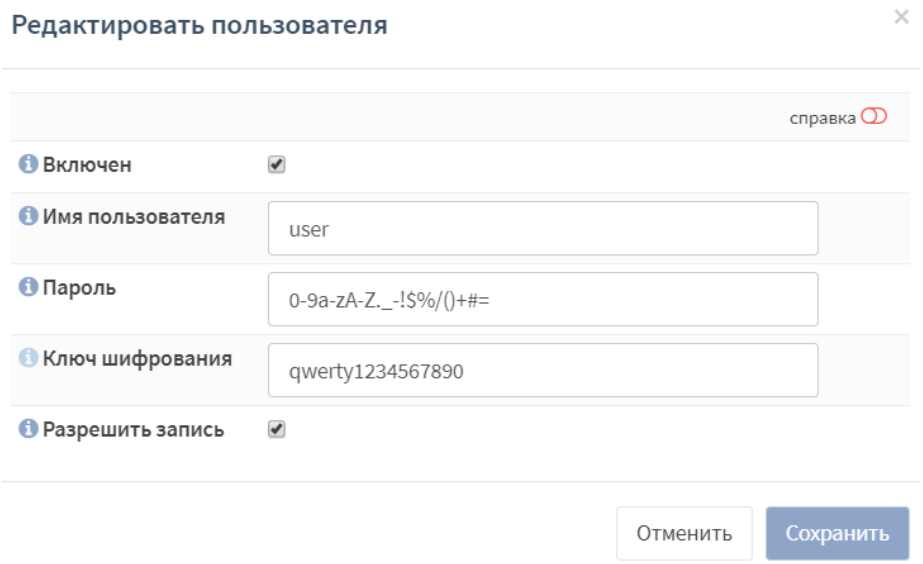


Рисунок 150 — Система: Настройки: SNMP: Пользователи SMNPv3 (редактирование)

Необходимо нажать на кнопку «Сохранить» для сохранения настроек.

6.3.6. Категория «Прочее»

Категория «Прочее» позволяет настраивать датчики температуры, периодичность резервного копирования, средства энергосбережения и настройки диска/памяти.

В группе настроек «Датчики температуры» в поле «Аппаратное обеспечение» необходимо выбрать аппаратное обеспечение (датчик температуры выхода из строя процессоров AMD K8, K10 (amdtemp) и процессоров Intel Core (coretemp), датчик температуры материнской платы ACPI), на которое будет загружен драйвер для считывания его температуры (рисунок 151).

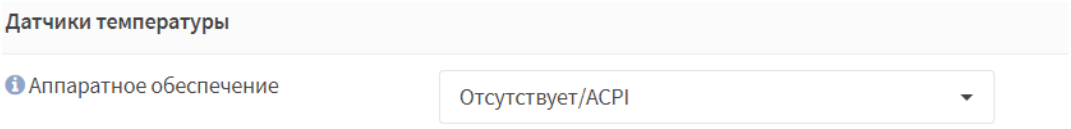


Рисунок 151 — Система: Настройки: Прочее (Датчики температуры)

В группе настроек «Периодические резервные копии» в поле «Периодическая резервная копия данных анализа трафика» необходимо выбрать периодичность резервирования данных графиков анализа. В поле «Периодическая резервная копия DHCP» необходимо выбрать периодичность резервирования данных аренд DHCP. В поле «Периодическая резервная копия Netflow» необходимо выбрать периодичность резервирования данных Netflow. В поле «Периодическая резервная копия данных портала авторизации» необходимо выбрать периодичность резервирования данных сессий Портала авторизации (рисунок 152).

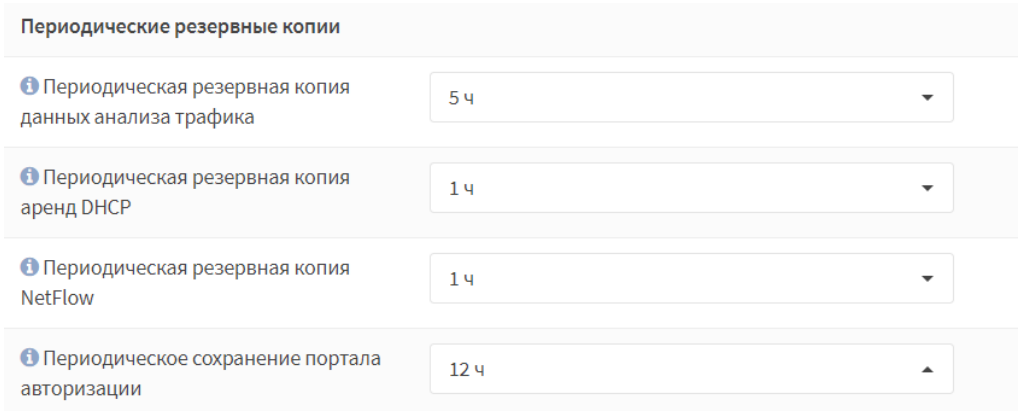


Рисунок 152 — Система: Настройки: Прочее (Периодические резервные копии)

В группе настроек «Средства сбережения» в поле «Использовать Powerd» необходимо установить флажок для использования сервисной программы Powerd. В поле «В режиме питания от сети переменного тока» необходимо выбрать состояние питания в режиме питания от сети переменного тока. В поле «В режиме питания от батареи» необходимо выбрать состояние питания в режиме питания от батареи. В поле «В режиме нормального питания» необходимо выбрать состояние питания в режиме нормального питания (питания от сети) (рисунок 153).

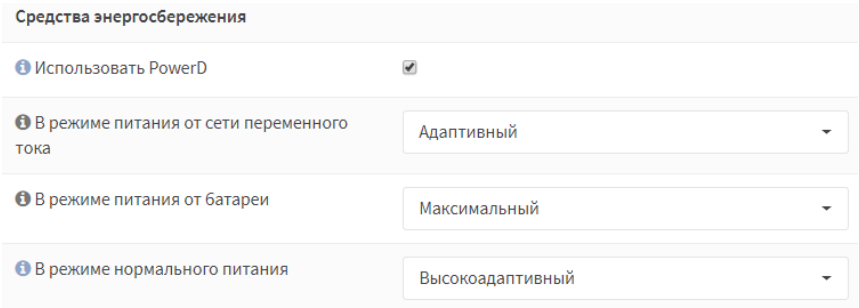


Рисунок 153 — Система: Настройки: Прочее (Средства сбережения)

В группе настроек «Настройки диска/памяти (требуется перезагрузка)» в поле «Файл swap» необходимо установить флажок для добавления 2 ГБ swap-файла в систему, при этом при сохранении изменений после установки данного флажка потребуется перезагрузка ПК. В поле «RAM-диск /var» необходимо установить флажок для использования файловой системы в качестве оперативной памяти в /var. В поле «RAM-диск /tmp» необходимо установить флажок для использования файловой системы в качестве оперативной памяти /tmp (рисунок 154).

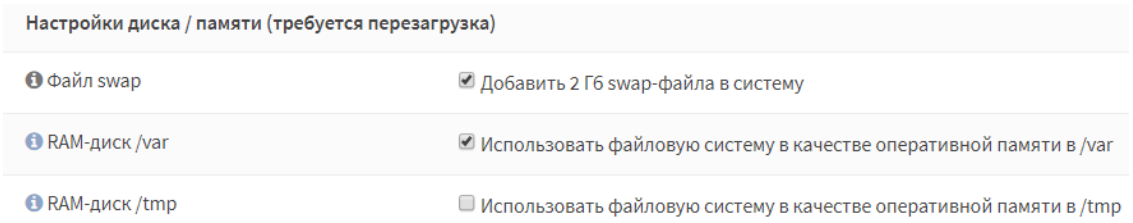


Рисунок 154 — Система: Настройки: Прочее (Настройки диска/памяти (требуется перезагрузка)

В группе настроек «Системные звуки» в поле «Звук включения/выключения» необходимо поставить флажок для отключения звуков включения/выключения устройства (рисунок 155).

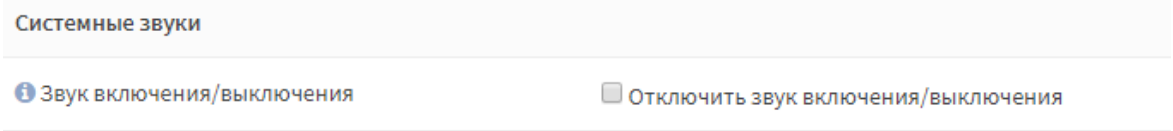


Рисунок 155 — Система: Настройки: Прочее (Системные звуки)

Необходимо нажать на кнопку «Сохранить» для сохранения настроек.

6.3.7. Категория «Параметры»

В категории «Параметры» приведена таблица параметров ядра. Таблица содержит следующие данные (рисунок 156):

– имя параметра;
– описание параметра;
– значение параметра.

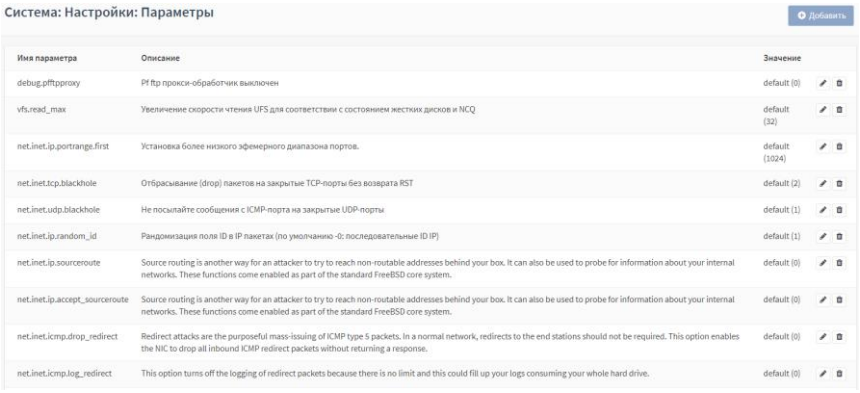
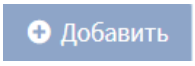


Рисунок 156 — Система: Настройки: Параметры

Для того, чтобы редактировать существующие параметры, необходимо нажать на кнопку  напротив параметра. Для того, чтобы создать новый параметр системы, необходимо нажать на кнопку 

.

При редактировании параметра системы в поле «Параметр» необходимо ввести название параметра. В поле «Описание» необходимо ввести описание параметра. В поле «Значение» необходимо ввести значение параметра (рисунок 157).

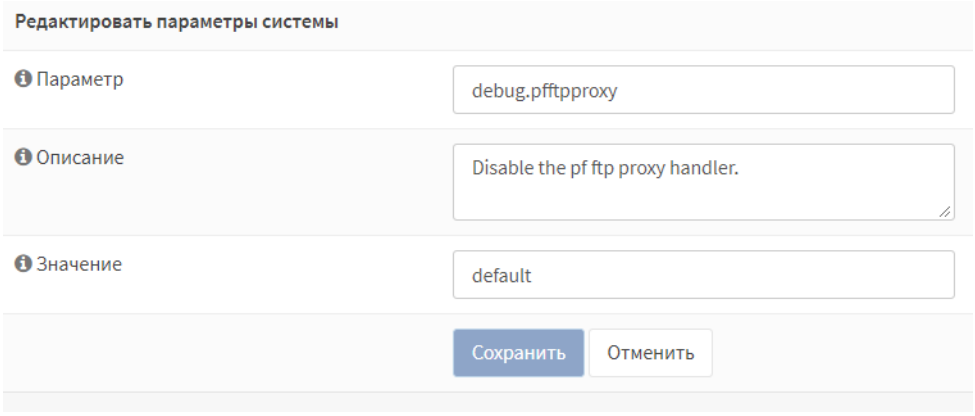


Рисунок 157 — Система: Настройки: Параметры (редактирование)

6.3.8. Категория «Планировщик задач Cron»

В категории «Планировщик задач Cron» приведена таблица планировщика задач системы. Таблица содержит следующие данные (рисунок 158):

- данные о состоянии задачи (включено/выключено);
- данные о задаче:
  - минуты;
  - часы;
  - дни;
  - месяцы;
  - дни недели;
  - описание;
  - команды.

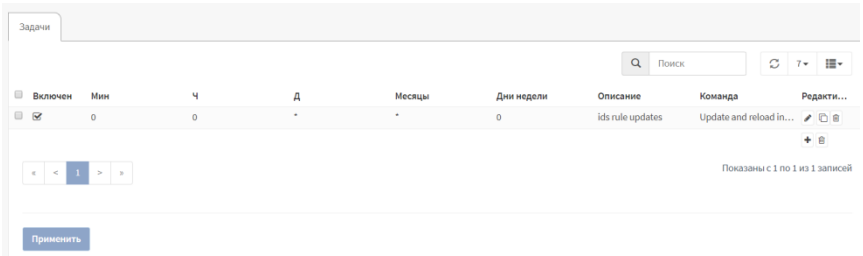
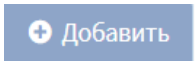


Рисунок 158 — Система: Настройки: Планировщик задач Cron

Для того, чтобы редактировать существующие задачи, необходимо нажать на кнопку  напротив задачи. Для того, чтобы создать новую задачу, необходимо нажать на кнопку 

. Стоит обратить внимание, что в правилах задается не конкретное время запуска задачи, а периодичность запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В

поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду, которая должна выполнена в определенный момент времени. В поле «Параметры» необходимо ввести параметры задачи. В поле «Описание» необходимо ввести описание задачи. Пример готовой строки сценария Cron: «Выполнять перезагрузку в 18 часов 7 минут 13 мая, если это пятница» (рисунок 159).

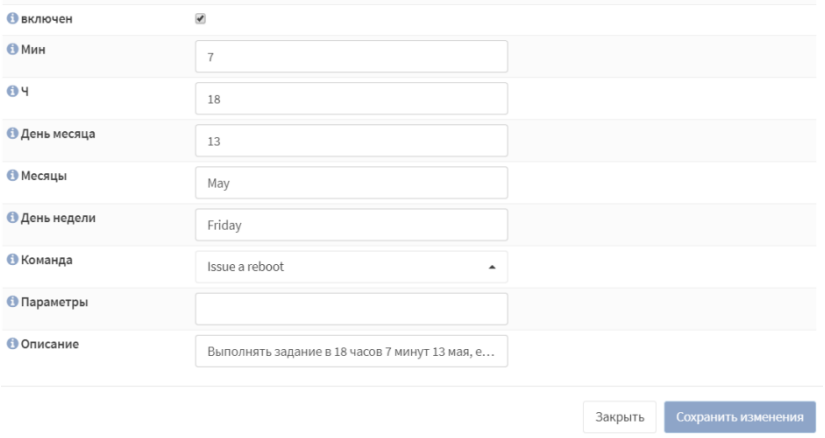


Рисунок 159 — Система: Настройки: Планировщик задач Cron (редактирование)

Необходимо нажать на кнопку «Сохранить изменения», а затем «Применить» для сохранения задачи Cron.

6.4. Подраздел «Шлюзы»

Подраздел «Шлюзы» позволяет просматривать / редактировать / удалять / создавать шлюзы и группы шлюзов, а также просматривать журнал шлюзов / группы шлюзов.

6.4.1. Категория «Единичный»

В категории «Единичный» приведена таблица единичных шлюзов. Таблица содержит следующие данные (рисунок 160):

- имя шлюза;
- время приема-передачи (RTT);

– IP-адрес шлюза;
– монитор IP;
– потеря;
– статус;
– описание.

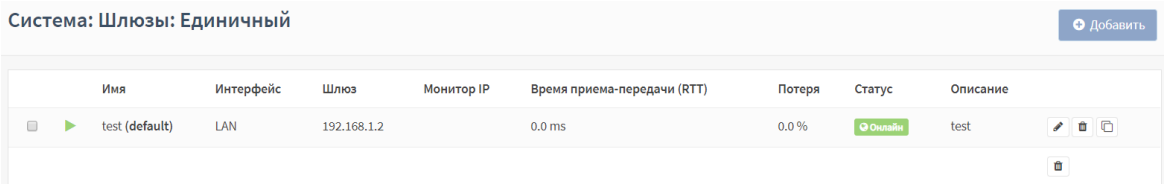
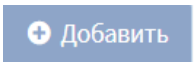


Рисунок 160— Система: Шлюзы: Единичный

Для того, чтобы редактировать существующие шлюзы, необходимо нажать на кнопку  напротив шлюза. Для того, чтобы создать новый шлюз, необходимо нажать на кнопку 

.

При редактировании шлюза в поле «Отключена» необходимо установить флажок для отключения шлюза. В поле «Имя» необходимо ввести название шлюза. В поле «Интерфейс» необходимо выбрать сетевой интерфейс. В поле «Семейство адресов» необходимо выбрать версию IP протокола. В поле «Шлюз» необходимо ввести IP-адрес шлюза. В поле «Шлюз по умолчанию» необходимо установить флажок для использования данного шлюза по умолчанию. В поле «Удаленный шлюз» необходимо установить флажок для создания шлюза вне интерфейса подсети. В поле «Отключите мониторинг шлюзов» необходимо установить флажок для отключения мониторинга шлюза. В поле «Монитор IP» необходимо ввести IP-адрес альтернативного монитора. В поле «Пометить шлюз как недоступный» необходимо установить флажок для того, чтобы принудительного считать каждый шлюз недоступным (рисунок 161).

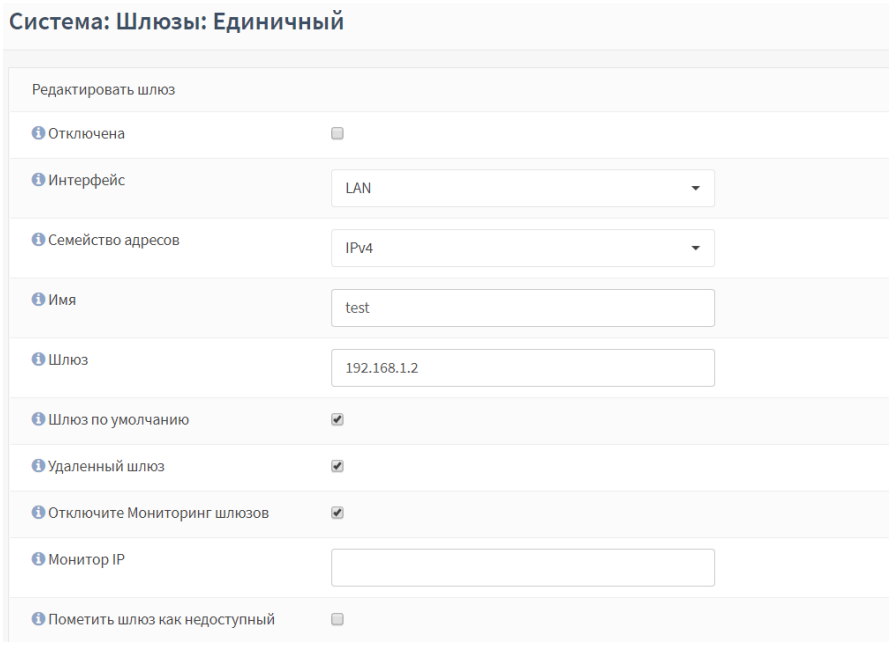


Рисунок 161 — Система: Шлюзы: Единичный (редактирование)

При нажатии на кнопку «Дополнительно» появятся дополнительные настройки. В поле «Весовой коэффициент» необходимо ввести приоритет данного шлюза. В поле «Пороговое значение задержки» необходимо ввести диапазон задержки шлюза. В поле «Интервал опроса» необходимо ввести как часто будет отправляться ICMP запрос. В поле «Интервал уведомлений» необходимо ввести интервал времени между уведомлениями. В поле «Период усреднения» необходимо ввести время, за которое результаты будут усредняться. В поле «Интервал потери» необходимо ввести интервал времени, по истечении которого пакеты будут считаться потерянными (рисунок 162).

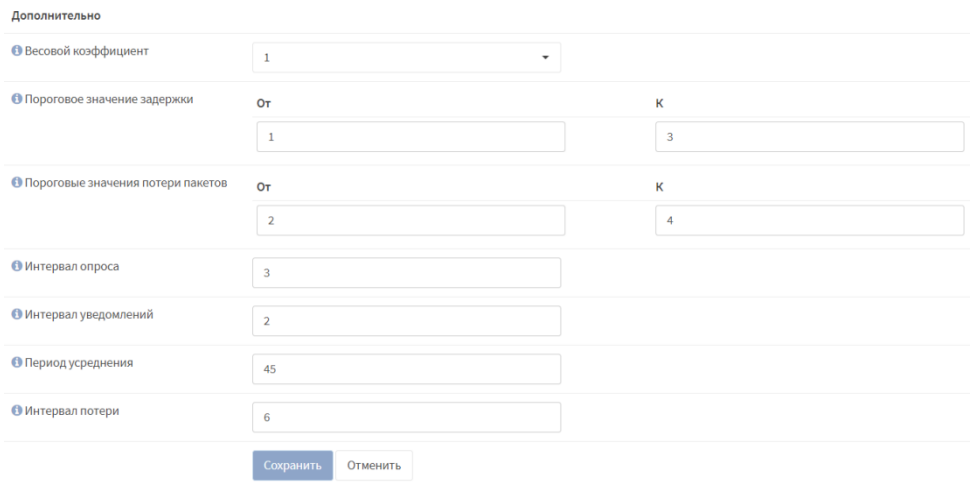


Рисунок 162— Система: Шлюзы: Единичный (редактирование: дополнительное)

Для сохранения шлюза необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

6.4.2.Категория «Группа»

В категории «Группы» приведена таблица группы шлюзов. Таблица содержит следующие данные (рисунок 163):

- имя группы шлюзов;
- шлюзы в группе;
- описание.

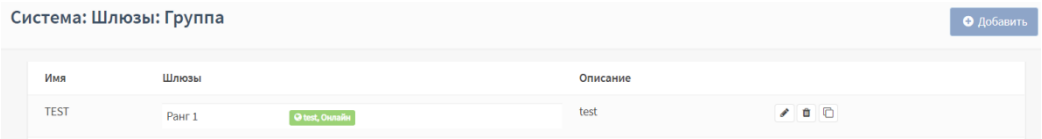
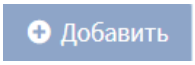


Рисунок 163— Система: Шлюзы: Группы

Для того, чтобы редактировать существующие группы шлюзов, необходимо нажать на кнопку  напротив группы шлюзов. Для того, чтобы создать новую группу шлюзов, необходимо нажать на кнопку 

.

При редактировании группы шлюзов в поле «Имя группы» необходимо ввести название группы шлюзов. В «Приоритет шлюзов» необходимо выбрать в поле «Ранг» приоритет шлюза в группе (то имеется в каком порядке будет происходить аварийное переключение и балансировка), в поле «Виртуальный IP-адрес» необходимо выбрать виртуальный IP-адрес. В поле «Уровень срабатывания» необходимо выбрать уровень срабатывания исключения шлюза. В поле «Описание» необходимо ввести описание группы шлюзов (рисунок 164).

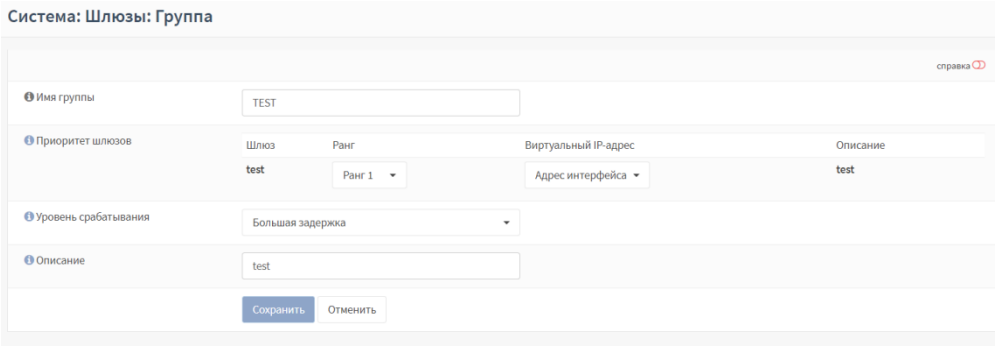


Рисунок 164 — Система: Шлюзы: Группы (редактирование)

Для сохранения группы шлюзов необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

6.4.3. Категория «Журнал»

В категории «Журнал» отображаются сообщения журнала apinger, связанные со шлюзами (рисунок 165).

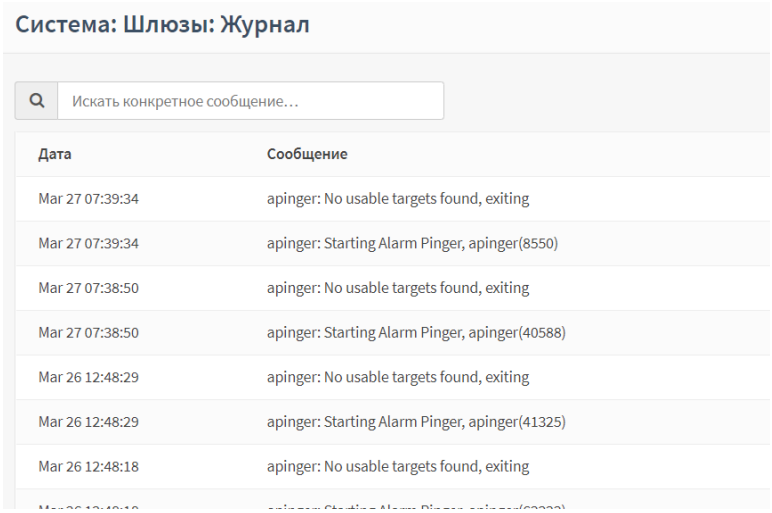


Рисунок 165— Система: Шлюзы: Журнал

6.5. Подраздел «Маршруты»

Подраздел «Маршруты» позволяет просматривать / редактировать / удалять / создавать статические маршруты, а также таблицу всех маршрутов в режиме реального времени и журнал изменения маршрутов.

6.5.1. Категория «Конфигурация»

В категории «Конфигурация» приведена таблица статических маршрутов. Таблица содержит следующие данные (рисунок 166):

– статус (включен/выключен маршрут);
– сеть;
– шлюз;
– описание маршрута;
– команды.

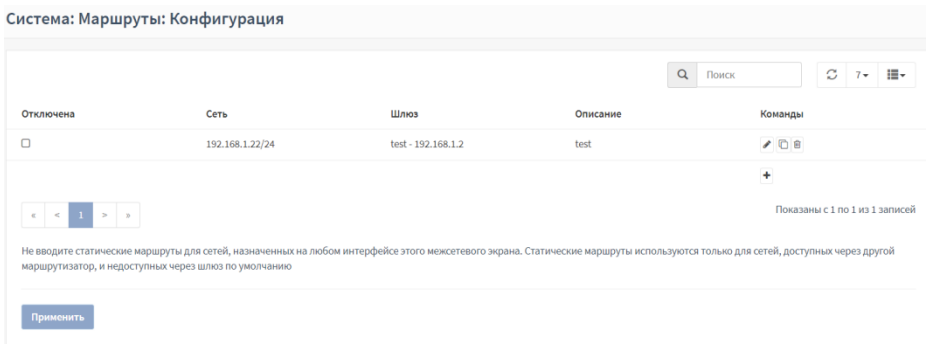
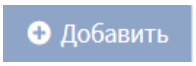


Рисунок 166 — Система: Маршруты: Конфигурация

Для того, чтобы редактировать существующие маршруты, необходимо нажать на кнопку  напротив маршрута. Для того, чтобы создать новый статический маршрут, необходимо нажать на кнопку 

.

При редактировании маршрута в поле «Отключена» необходимо установить флажок для отключения статического маршрута. В поле «Адрес сети» необходимо ввести сеть назначения для статического маршрута. В поле «Шлюз» необходимо выбрать к какому шлюзу применяется этот маршрут. В поле «Описание» необходимо ввести описание маршрута (рисунок 167).

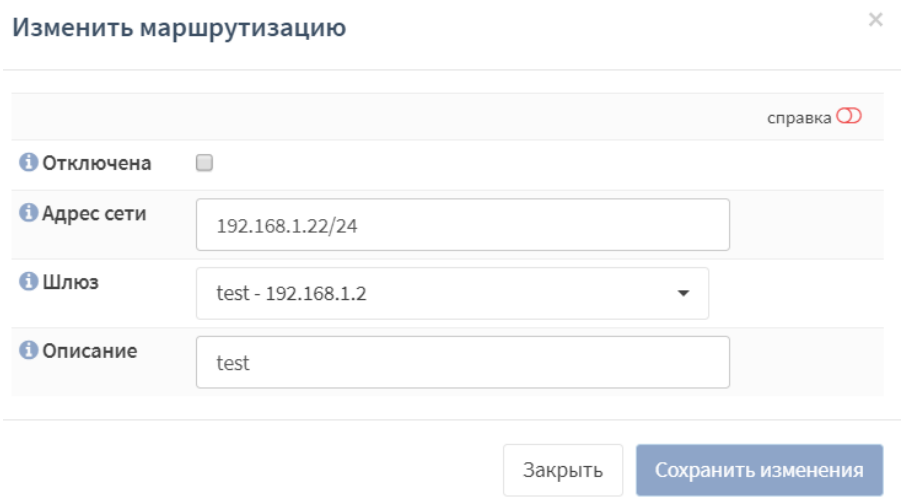


Рисунок 167 — Система: Маршруты: Конфигурация (редактирование)

Для сохранения маршрута необходимо нажать на кнопку «Сохранить изменения», а затем «Применить».

6.5.2.Категория «Статус»

В категории «Статус» приведена таблица маршрутов системы. Таблица содержит следующие данные (рисунок 168):

– протокол;
– получатель;
– шлюз;
– флажки протокола;
– максимальный размер кадра;
– физический интерфейс;
– название сетевого интерфейса.

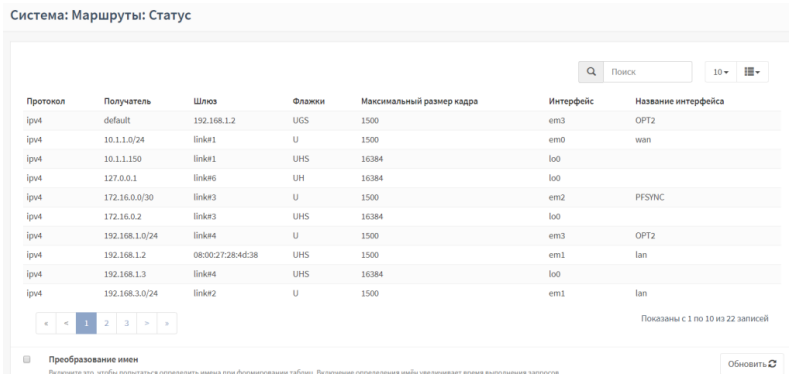


Рисунок 168 — Система: Маршруты: Конфигурация

В таблице возможно выполнить поиск, выбрать сколько маршрутов отображать на странице и добавить/убрать графы таблицы, нажав соответствующие кнопки.

6.5.3. Категория «Журнал»

В категории «Журнал» отображаются события изменения маршрутов (рисунок 169).

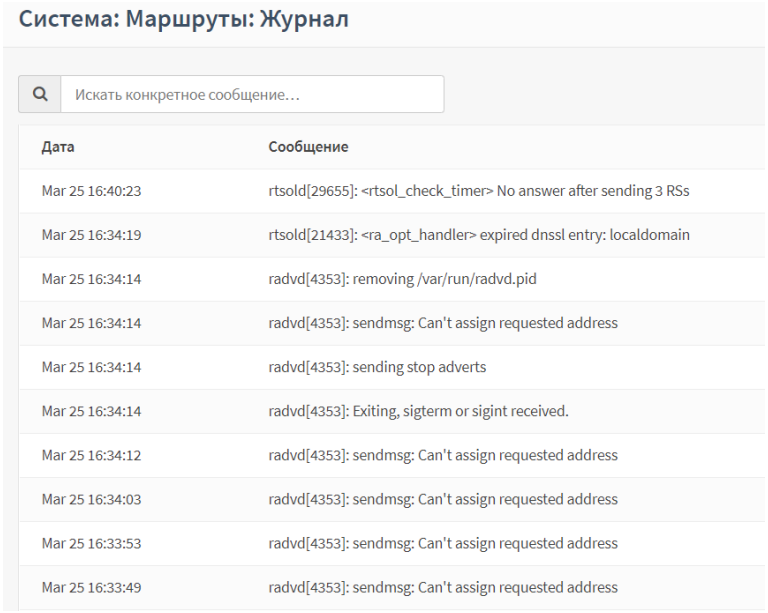


Рисунок 169 — Система: Маршруты: Журналы

6.6. Подраздел «Высокая доступность»

Подраздел «Высокая доступность» при работе системы в режиме отказоустойчивого кластера позволяет настраивать синхронизацию устройств, а также просматривать статус устройства.

6.6.1. Категория «Настройки»

Категория «Настройки» позволяет настраивать синхронизацию состояния и настроить синхронизацию конфигурации (XMLRPC Sync).

В группе настроек «Синхронизация состояния» в поле «Синхронизировать состояния» необходимо установить флажок для включения механизма pfsync. В поле «Отключить упреждение» необходимо установить флажок для того, чтобы оставить устройство в режиме

«Резервный». В поле «Синхронизовать интерфейс» необходимо выбрать сетевой интерфейс, через который будет происходить обмен данными. В поле «Синхронизовать IP-адреса пира» необходимо ввести IP-адрес пира для включения синхронизации таблицы состояний для этого IP-адреса (рисунок 170).

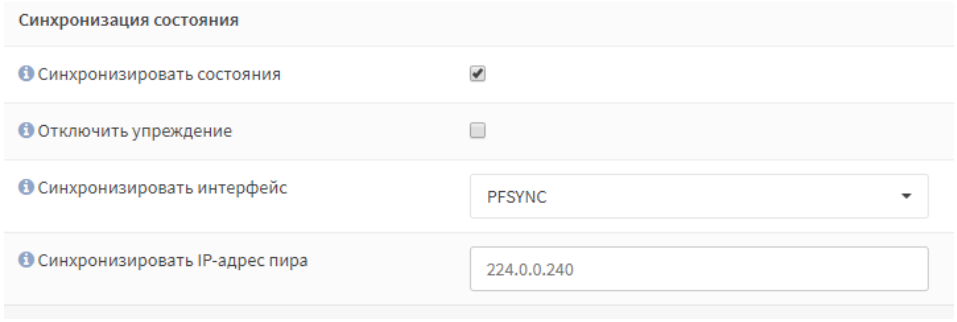


Рисунок 170 — Система: Высокая доступность: Настройки (синхронизация состояния)

В группе настроек «Настройки синхронизации конфигурации (XMLRPC Sync)» в поле «Синхронизовать конфигурацию с IP-адресом» необходимо ввести IP-адрес межсетевого экрана, с которым необходимо синхронизовать выбранные секции конфигурации. В поле «Имя пользователя удаленной системы» необходимо ввести имя пользователя удаленной системы для авторизации в ней. В поле «Пароль удаленной системы» необходимо ввести пароль удаленной системы для авторизации в ней. В поле «Пользователи и группы» необходимо установить флажок для включения автоматической синхронизации пользователей и группы пользователей с другим хостом. В поле «Серверы аутентификации» необходимо установить флажок для включения синхронизации настроек серверов аутентификации с другим хостом. В поле «Сертификаты» необходимо установить флажок для включения автоматической синхронизации сертификатов с другим хостом. В поле «Правила межсетевого экрана» необходимо установить флажок для включения автоматической синхронизации правил межсетевого экрана с другим хостом. В поле «Расписания межсетевого экрана» необходимо установить флажок для включения автоматической синхронизации

расписания межсетевого экрана с другим хостом. В поле «Псевдонимы» необходимо установить флажок для включения автоматической синхронизации псевдонимов с другим хостом. В поле «NAT» необходимо установить флажок для включения автоматической синхронизации настроек NAT с другим хостом. В поле «DHCP» необходимо установить флажок для включения автоматической синхронизации настроек DHCP с другим хостом. В поле «Статические маршруты» необходимо установить флажок для включения автоматической синхронизации настроек статических маршрутов с другим хостом. В поле «Виртуальные IP-адреса» необходимо установить флажок для включения автоматической синхронизации виртуальных IP-адресов с другим хостом. В поле «Ограничение трафика» необходимо установить флажок для включения автоматической синхронизации настроек ограничения трафика с другим хостом. В поле «Портал авторизации» необходимо установить флажок для включения автоматической синхронизации Портала авторизации с другим хостом. В поле «Monit мониторинг системы» необходимо установить флажок для включения автоматической синхронизации настроек Monit с другим хостом. В поле «Прокси» необходимо установить флажок для включения автоматической синхронизации настроек прокси-сервера с другим хостом. В поле «Обнаружение вторжений» необходимо установить флажок для включения автоматической синхронизации настроек системы обнаружения вторжений с другим хостом (рисунок 171).

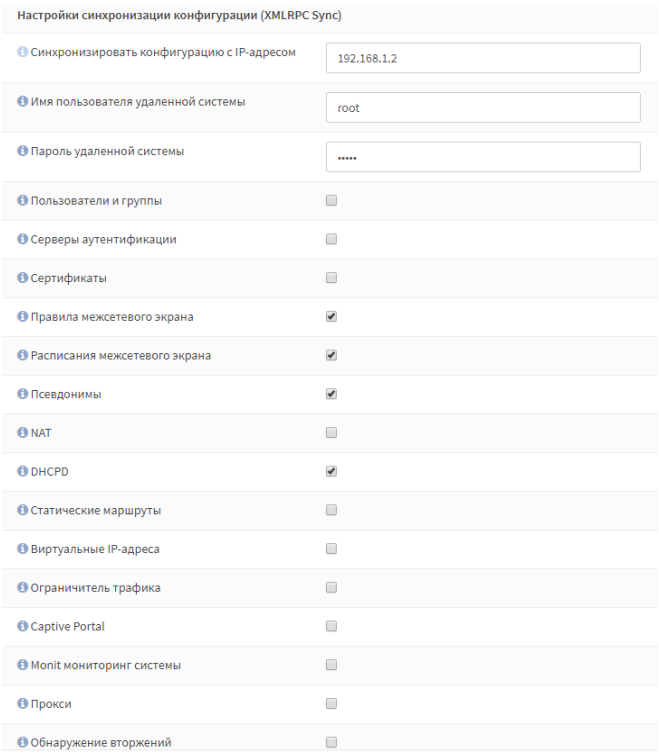


Рисунок 171 — Система: Высокая доступность: Настройки (Настройки синхронизации конфигурации (XMLRPC Sync))

6.6.2.Категория «Статус»

В категории «Статус» отображается статус работы системы в режиме отказоустойчивого кластера.

Если система работает в режиме отказоустойчивого кластера, на ведущем устройстве будет показан статус работы (данные о версии резервного устройства) с возможностью управления настроенными службами резервного устройства (рисунок 172).

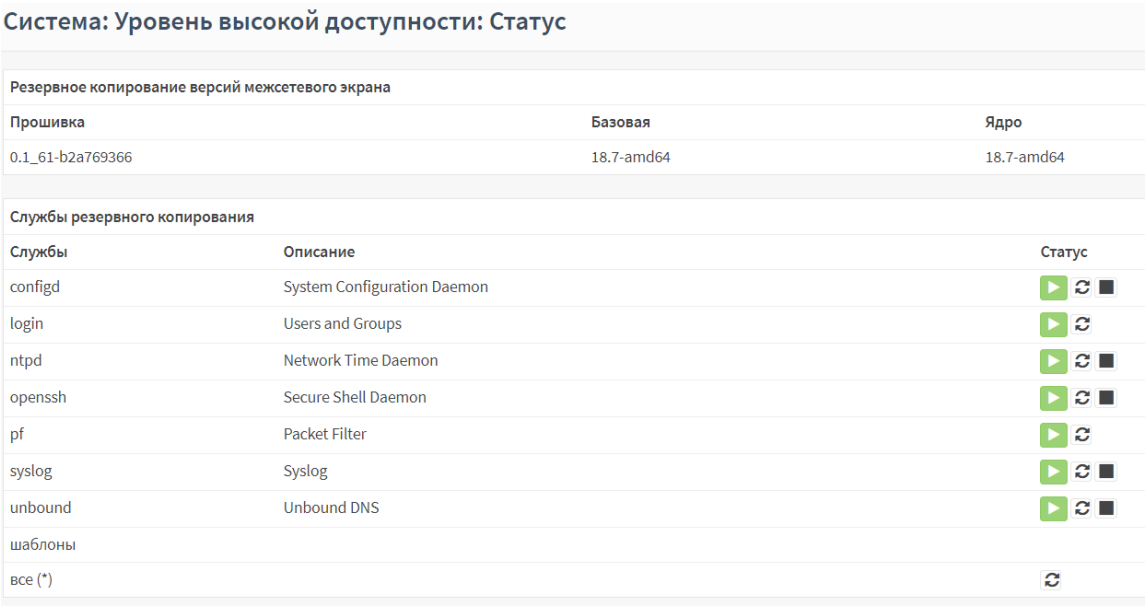


Рисунок 172 — Система: Высокая доступность: Статус (работа в режиме отказоустойчивого кластера)

В противном случае будет отображаться сообщение о том, что резервное копирование недоступно (рисунок 173).

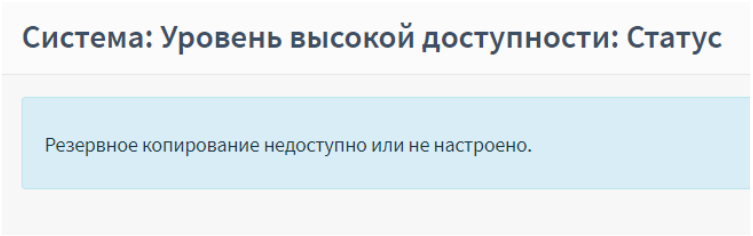


Рисунок 173— Система: Высокая доступность: Статус (резервное копирование недоступно)

6.7. Подраздел «Диагностика»

Подраздел «Диагностика» позволяет просматривать таблицу выполнения действий пользователей (в том числе системных) с различными параметрами и просматривать (управлять) настроенными службами.

6.7.1.Категория «Активность»

В категории «Активность» приведена таблица всех действий пользователей (в том числе системных) в системе. Таблица содержит следующие данные (рисунок 174):

– идентификационный номер;
– имя пользователя;
– информация интерфейса первичного уровня;
– задействованная память;
– размер Res-файлов;
– состояние;
– время;
– загруженность ЦПУ;
– описание выполненной команды.

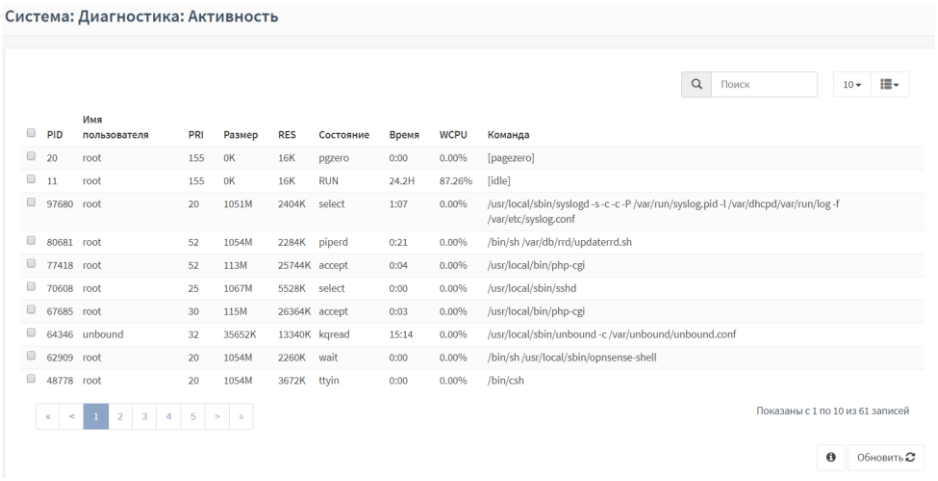


Рисунок 174 — Система: Диагностика: Активность

В таблице возможно выполнить поиск, выбрать сколько записей отображать на странице и добавить/убрать графы таблицы, отсортировать по колонкам таблицы нажав соответствующие кнопки.

6.7.2.Категория «Службы»

Категория «Службы» позволяет просматривать настроенные службы. Эти службы возможно остановить/запустить/перезагрузить, нажав на соответствующие кнопки напротив необходимой службы (рисунок 175).

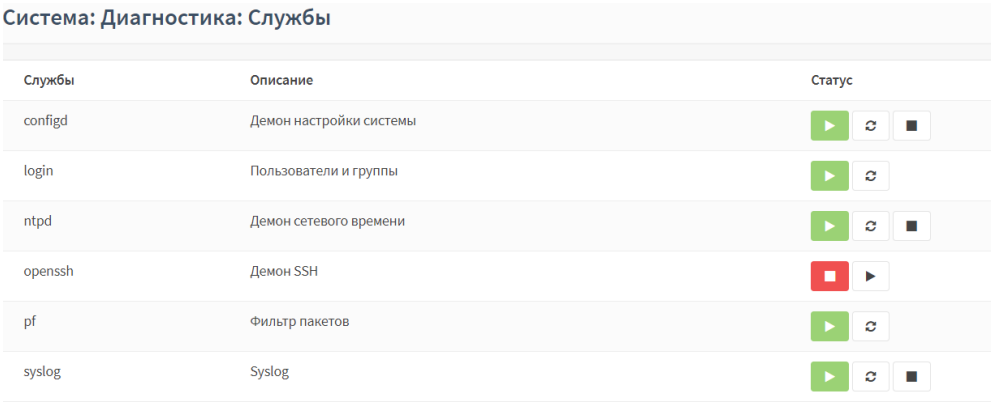


Рисунок 175 — Система: Диагностика: Службы

6.8. Подраздел «Конфигурация»

Подраздел «Конфигурация» позволяет экспортировать текущую конфигурацию на локальный хост и на удаленный FTP-сервер, восстановить конфигурацию, сбросить настройки системы до начальных, просматривать историю изменений (с возможностью отменить действия).

6.8.1. Категория «Резервные копии»

Процедура резервного копирования описана в Руководстве администратора в разделе 7, подразделе 7.3.

Также категория «Резервные копии» позволяет экспортировать наборы правил системы обнаружения вторжений, загруженных пользователями (рисунок 176).

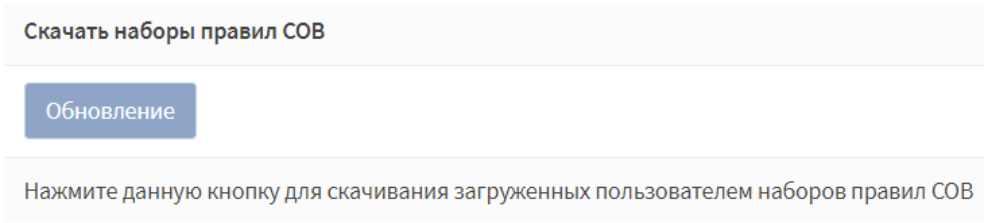


Рисунок 176 — Система: Конфигурация: Резервные копии

6.8.2. Категория «Значение по умолчанию»

Категория «Значение по умолчанию» позволяет сбросить все настройки до начальных:

– настройки установятся по умолчанию;

– IP-адрес локальной сети будет сброшен до 192.168.1.1;

– система будет настроена как DHCP-сервер на LAN-интерфейсе по умолчанию;

– WAN-интерфейс будет автоматически получать адрес от DHCP-сервера;

– имя и пароль администратора будут сброшены (имя — «root», пароль — «root»);

– после внесения изменений система будет выключена.

Для сброса настроек нажми кнопку «Да» (рисунок 177).

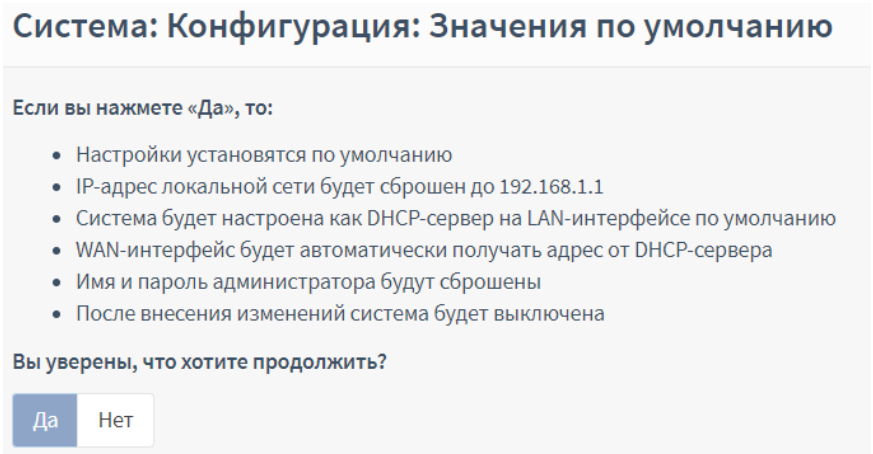


Рисунок 177 — Система: Конфигурация: Значение по умолчанию

6.8.3.Категория «История изменений»

Категория «История изменений» позволяет задать количество резервных копий конфигураций для хранения, сравнивать две конфигурации, а также просматривать конфигурации в виде таблицы. Выбрав одну из резервных копий, имеется возможность вернуться к ней либо просмотреть различия с текущим состоянием.

В группе настроек «Количество резервных копий» необходимо ввести количество конфигураций, которые будут храниться (рисунок 178).

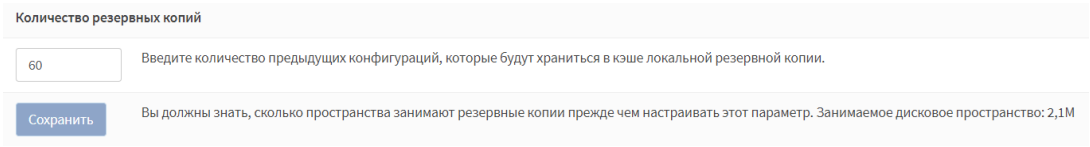


Рисунок 178 — Система: Конфигурация: История изменений (количество резервных копий)

После внесения изменений необходимо нажать на кнопку «Сохранить».

Группа настроек «История изменений» позволяет просматривать отличия конфигураций. Для этого необходимо нажать на флажок (столбец «Отличия») в таблице истории изменений на конфигурации, а затем нажать на кнопку «Просматривать отличия» (рисунок 179).

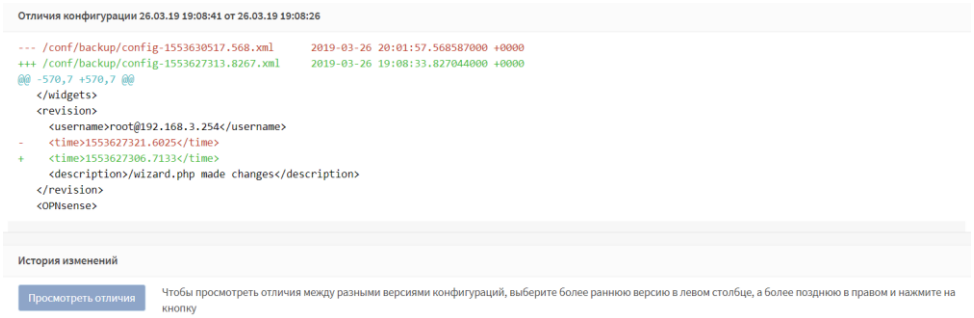


Рисунок 179 — Система: Конфигурация: История изменений (История изменений)

Таблица истории изменений позволяет просматривать:

– дату/время изменения;
– размер изменения в конфигурации;
– идентификатор пользователя и описание совершенного действия.

А также скачать, вернуть и удалить (отменить действие) конфигурацию, нажав на соответствующие кнопки напротив изменения (рисунок 180).

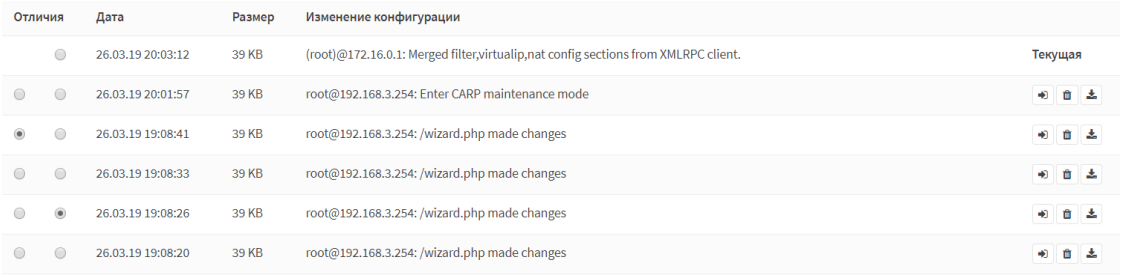


Рисунок 180 — Система: Конфигурация: История изменений (История изменений: таблица)

6.8.4. Категория «Настройки экспорта»

Процедура настройки экспорта конфигурации и набора баз решающих правил по протоколу FTP/SMB описаны в Руководстве администратора в разделе 7, подразделе 7.4.

6.9. Подраздел «Доверенные сертификаты»

Подраздел «Доверенные сертификаты» позволяет настраивать Центр Сертификации, добавлять и импортировать сертификаты, а также отзывать сертификат. Для защищенного подключения графического интерфейса используется TLS протокол версии 1.2.

6.9.1. Категория «Полномочия»

Категория «Полномочия» позволяет настраивать Центр Сертификации. Все настроенные центры сертификации указаны в таблице, которая отображает следующие данные (рисунок 181):

- название сертификата;
- является ли сертификат внутренним;
- эмитент;
- количество сертификатов;
- уникальное имя.

Также имеется возможность удалить, редактировать, экспортировать Центр Сертификации и экспортировать секретный ключ Центра Сертификации.

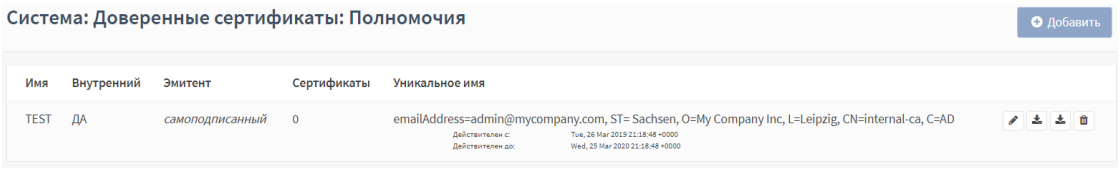
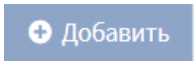


Рисунок 181— Система: Доверенные сертификаты: Полномочия

Для того, чтобы редактировать существующие Центры Сертификации, необходимо нажать на кнопку  напротив центра сертификации. Для того,

чтобы создать новый Центр Сертификации, необходимо нажать на кнопку 

.

При редактировании центра сертификации поле «Название» необходимо ввести название Центра Сертификации. В поле «Метод» необходимо выбрать метод добавления центра сертификации (рисунок 182).

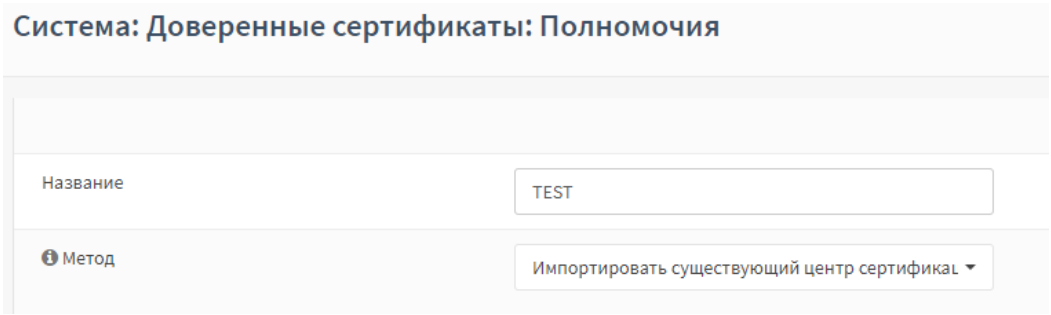


Рисунок 182 — Система: Доверенные сертификаты: Полномочия (редактирование)

Если в поле «Метод» выбрать «Импортировать существующий центр сертификации», то появятся следующие поля. В поле «Данные сертификата» необходимо ввести данные сертификата X.509 в PEM формате. В поле «Секретный ключ сертификата» необходимо ввести секретный ключ для сертификата, указанного в поле «Данные сертификата». В поле «Серийный номер для следующего сертификата» необходимо ввести число, которое будет использоваться как серийный номер для следующего сертификата (рисунок 183).

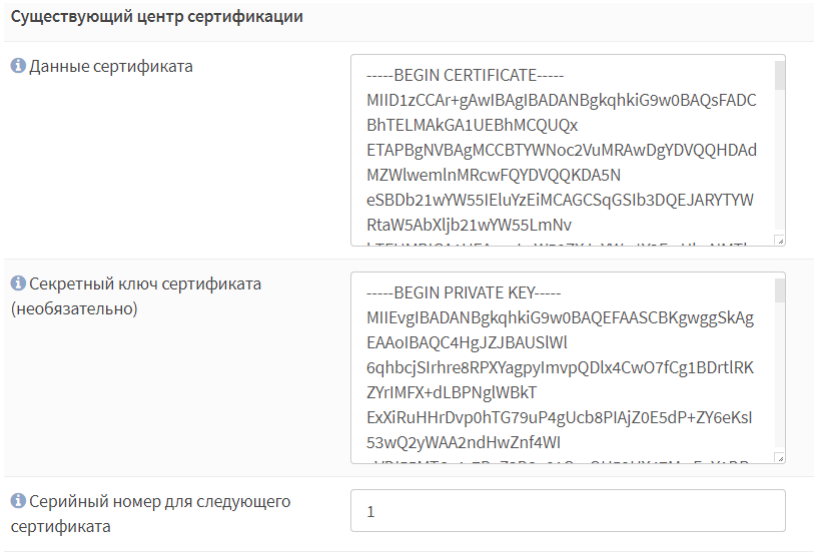


Рисунок 183 — Система: Доверенные сертификаты: Полномочия (редактирование: Импортировать существующий центр сертификации)

Если в поле «Метод» выбрать «Создать внутренний Центр Сертификации», то появятся следующие поля. В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя (рисунок 184).

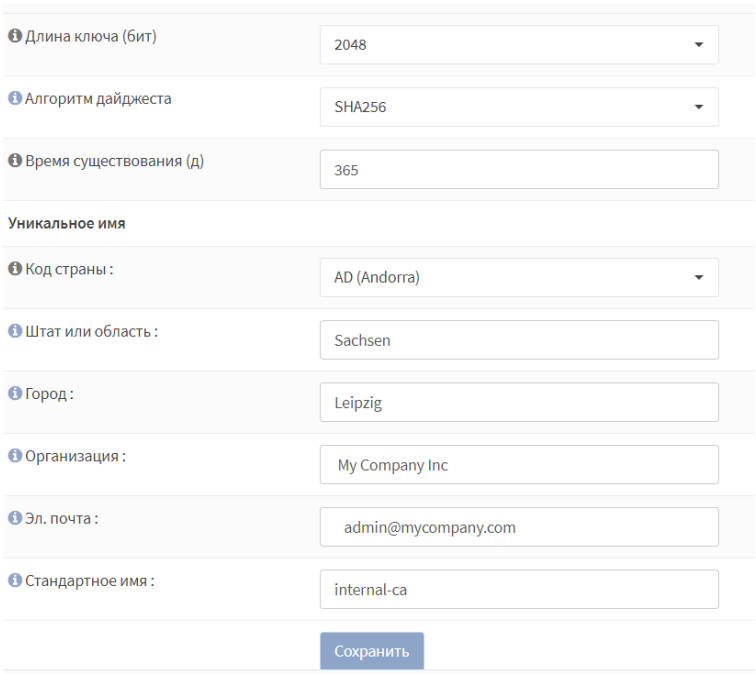


Рисунок 184 — Система: Доверенные сертификаты: Полномочия (редактирование: Создать внутренний Центр Сертификации)

Если в поле «Метод» выбрать «Создать промежуточный Центр Сертификации», то появятся следующие поля. В поле «Подписание Центра Сертификации» необходимо выбрать Центр Сертификации. В поле «Длина ключа (бит)» необходимо выбрать длину ключа в битах. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя (рисунок 185).

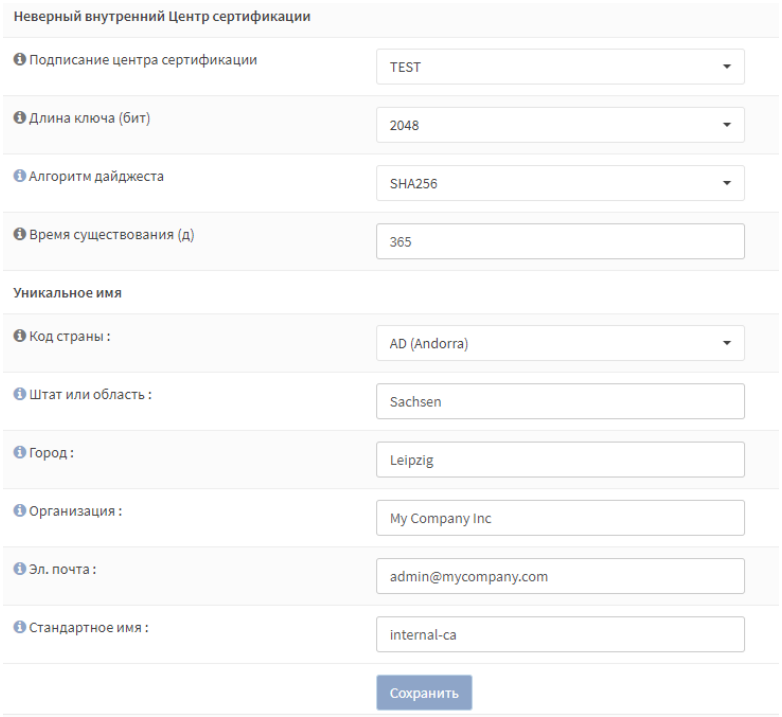


Рисунок 185 — Система: Доверенные сертификаты: Полномочия (редактирование: Создать промежуточный Центр Сертификации)

После внесения изменений необходимо нажать на кнопку «Сохранить».

6.9.2. Категория «Сертификаты»

Субординированный Центр Сертификации позволяет выписывать различные end entity сертификаты, для использования в следующих функциях:

– защищенный доступ к веб-интерфейсу;

– SSL Bump (перехват/дешифровка HTTPS-соединений).

Категория «Сертификаты» позволяет просматривать существующие сертификаты/просматривать информацию о них/удалить/создать сертификаты, а также экспортировать пользовательский ключ и пользовательский сертификат.

Все настроенные сертификаты указаны в таблице, которые отображает следующие данные (рисунок 186):

– название сертификата;

– эмитет;

– уникальное имя (срок действия сертификата).

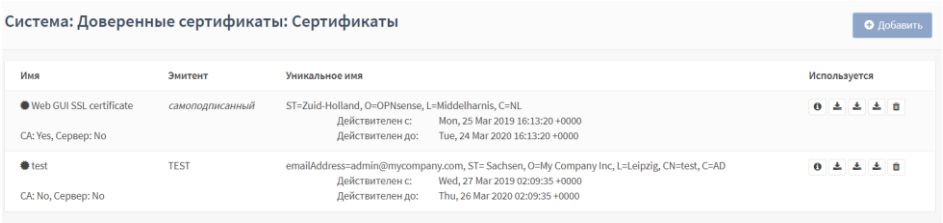
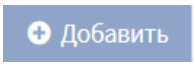


Рисунок 186 — Система: Доверенные сертификаты: Сертификаты

Для того, чтобы создать новый сертификат, необходимо нажать на кнопку 

.

При редактировании сертификата в поле «Метод» необходимо выбрать метод создания сертификата.

Если в поле «Метод» выбрать «Импортировать существующий сертификат», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Данные сертификата» необходимо ввести данные сертификата X.509 в PEM формате. В поле «Данные секретного ключа» необходимо ввести секретный ключ для сертификата, указанного в поле «Данные сертификата» (рисунок 187).

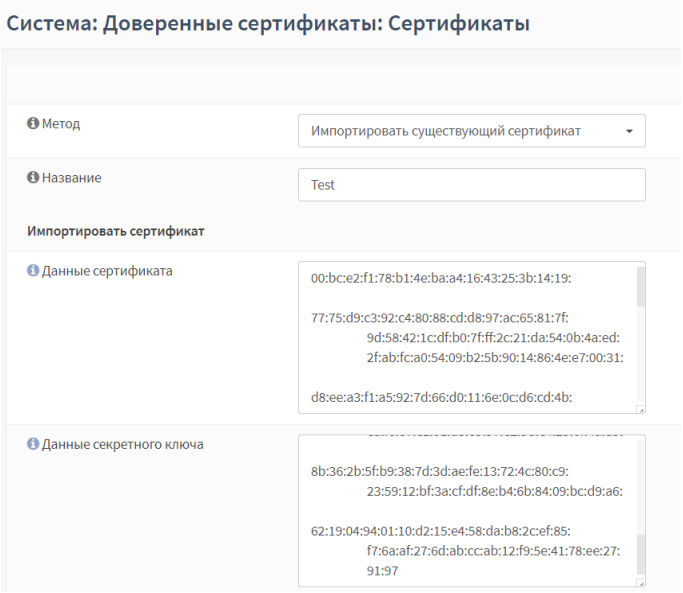


Рисунок 187 — Система: Доверенные сертификаты: Сертификаты (редактирование: Импортировать существующие сертификаты)

Если в поле «Метод» выбрать «Создать внутренний сертификат», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр сертификации» необходимо выбрать Центр Сертификации. В поле «Тип» необходимо выбрать тип сертификата для генерации, определяющий его условия. В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Расположение секретного ключа» необходимо выбрать, где необходимо сохранить секретный ключ. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя. В поле «Альтернативные имена» необходимо выбрать в поле «Тип» тип альтернативного имени и в поле «Значение» необходимо ввести его имя (рисунок 188).

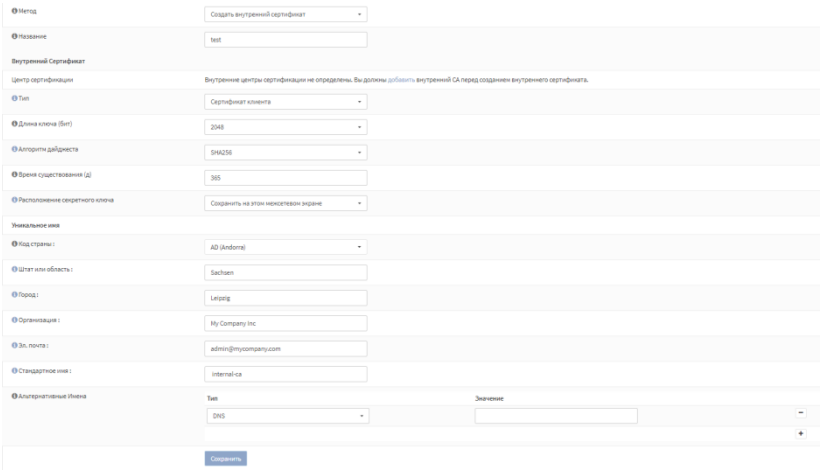


Рисунок 188 — Система: Доверенные сертификаты: Сертификат (редактирование: Создать внутренний сертификат)

Если в поле «Метод» выбрать «Создать запрос на подпись сертификата», то появятся следующие поля. В поле «Название» необходимо

ввести название сертификата. В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Организационное подразделение» необходимо выбрать отдел организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя. В поле «Альтернативные имена» необходимо выбрать в поле «Тип» тип альтернативного имени и в поле «Значение» необходимо ввести его имя (рисунок 189).

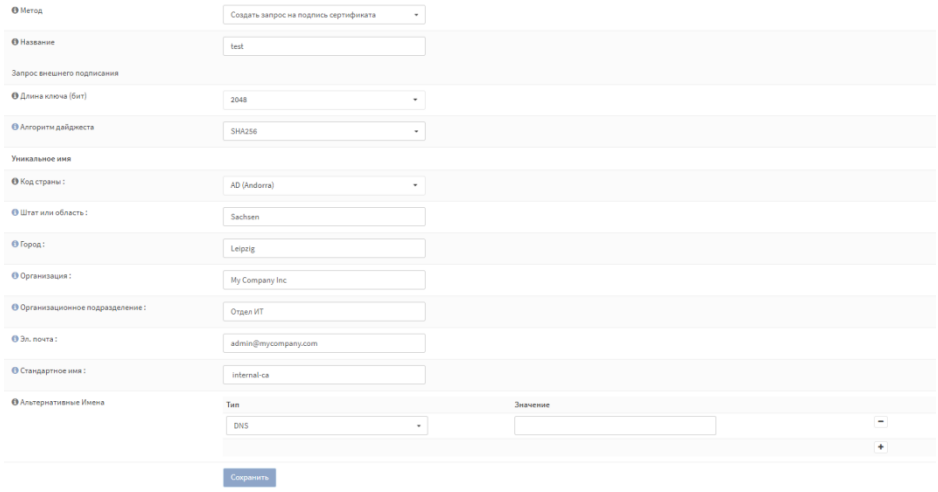


Рисунок 189 — Система: Доверенные сертификаты: Сертификаты (редактирование: Создать запрос на подпись сертификата)

Если в поле «Метод» выбрать «Создать запрос на получение сертификатов», то появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр сертификации» необходимо выбрать Центр сертификации. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «CSR файлы»

необходимо ввести CSR файл. CSR файл — это файл, который содержит в себе небольшой фрагмент зашифрованных данных о Вашем домене и компании, на который выдается сертификат (рисунок 190).

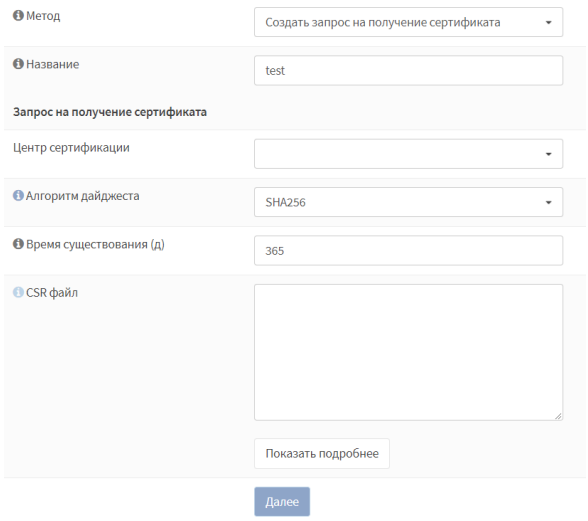


Рисунок 190 — Система: Доверенные сертификаты: Сертификаты (редактирование: Создать запрос на получение сертификата)

Если нажать на кнопку «Показать подробнее» появятся следующие поля (рисунок 191). В поле «Объект» можно просматривать информацию о сертификате. В поле «subjectAltName» необходимо ввести несколько доменных адресов сертификатов. В поле «basicConstraints» необходимо установить флажок напротив поля «Центр Сертификации» для возможности ввода максимального значения сертификатов. В поле «keyUsage» необходимо выбрать параметры для секретного ключа. В поле «extendedKeyUsage» необходимо выбрать параметры расширенного значения ключа.

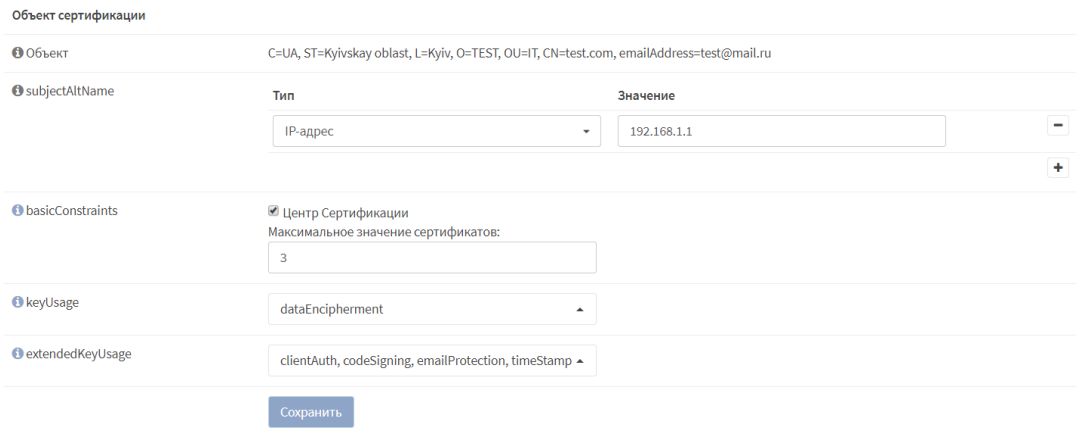


Рисунок 191 — Система: Доверенные сертификаты: Сертификаты (редактирование: Создать запрос на получение сертификата: Показать подробнее)

После внесения изменений необходимо нажать на кнопку «Сохранить».

6.9.3. Категория «Отзыв сертификатов»

Категория «Отзыв сертификатов» позволяет просматривать информацию о существующих списках отзыва сертификатов и добавить списки отзыва сертификатов существующих Центров Сертификации (рисунок 192).

Рисунок 192 — Система: Доверенные сертификаты: Отзыв сертификатов

Для добавления нового сертификата необходимо нажать на кнопку напротив Центра Сертификации.

При добавлении сертификата в поле «Метод» необходимо выбрать способ выбора сертификата.

Если выбрать в поле «Метод» метод «Создать внутренний список сертификатов», появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр Сертификации» необходимо выбрать существующий Центр Сертификации. В поле «Время существования (д)» необходимо ввести срок действия сертификата в днях. В поле «Серийный номер» необходимо ввести серийный номер сертификата. Необходимо нажать на кнопку Сохранить» (рисунок 193).

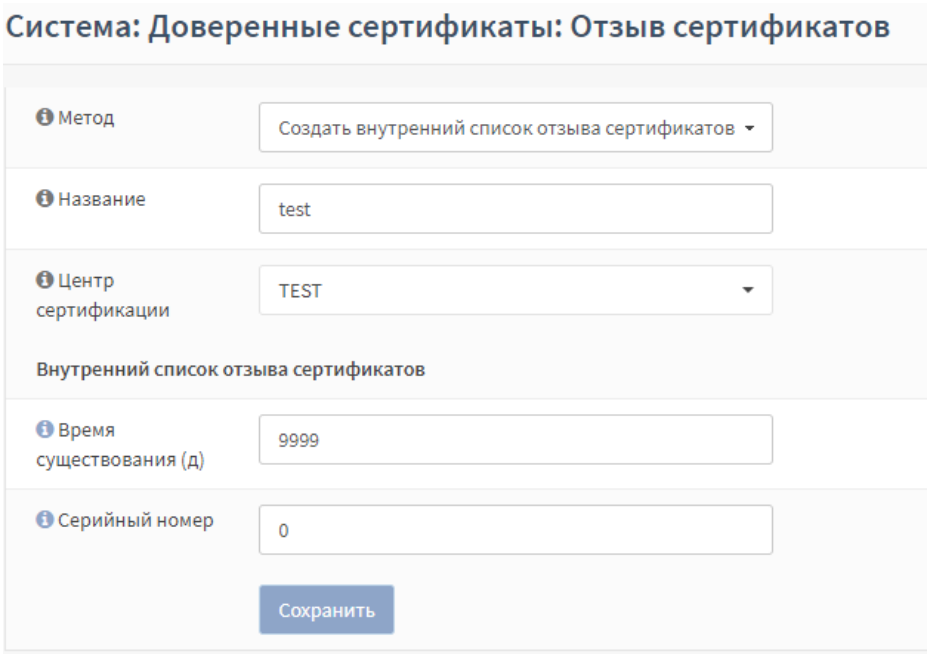


Рисунок 193 — Система: Доверенные сертификаты: Отзыв сертификатов (редактирование: Создать внутренний список сертификатов)

Если выбрать в поле «Метод» метод «Импортировать существующий список сертификатов», появятся следующие поля. В поле «Название» необходимо ввести название сертификата. В поле «Центр Сертификации» необходимо выбрать существующий Центр Сертификации. В поле «Данные CRL» необходимо ввести список отзыва сертификата в формате X.509 CRL. Необходимо нажать на кнопку Сохранить» (рисунок 194).

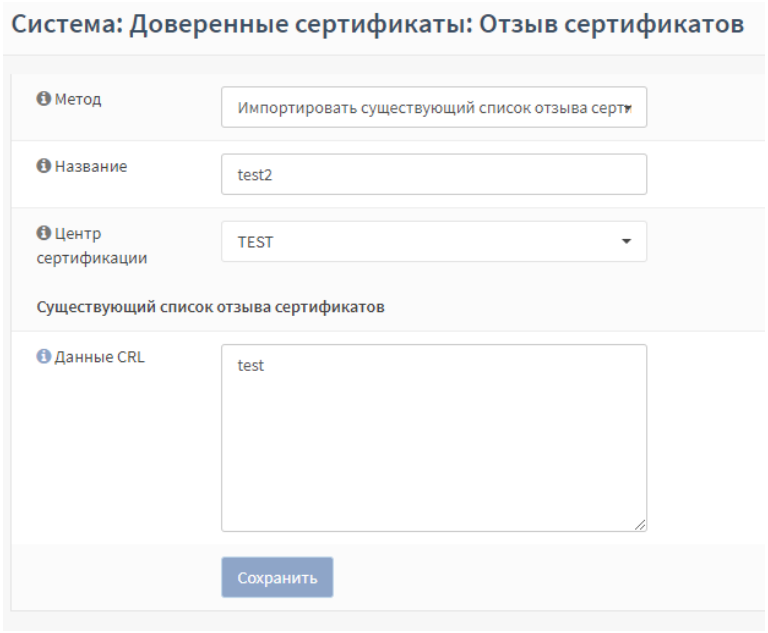


Рисунок 194 — Система: Доверенные сертификаты: Отзыв сертификатов (редактирование: Импортировать существующий список сертификатов)

6.10. Подраздел «Мастер»

Подраздел «Мастер» позволяет пройти начальную настройку системы. Для этого необходимо нажать на кнопку «Далее» (рисунок 195).

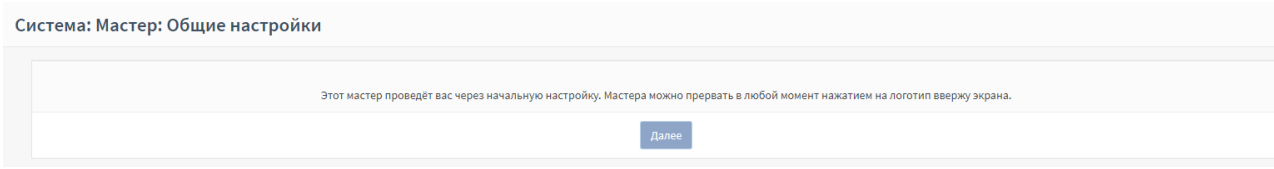


Рисунок 195 — Система: Мастер

6.10.1. Мастер: шаг 1

На первом шаге система предложит настроить общие настройки. Подробнее заполнение всех полей приведено в подразделе 6.3.3 настоящего документа. После настройки необходимо нажать на кнопку «Далее».

6.10.2. Мастер: шаг 2

На втором шаге начальной настройки система предложит настроить время (рисунок 196). В поле «Имя сервера времени:» необходимо ввести полное имя сервера времени, с которым будет производиться синхронизация. В случае, если таки серверов несколько их необходимо вводить через запятую. В поле «Часовой пояс» необходимо выбрать часовой пояс и нажать на кнопку «Далее».

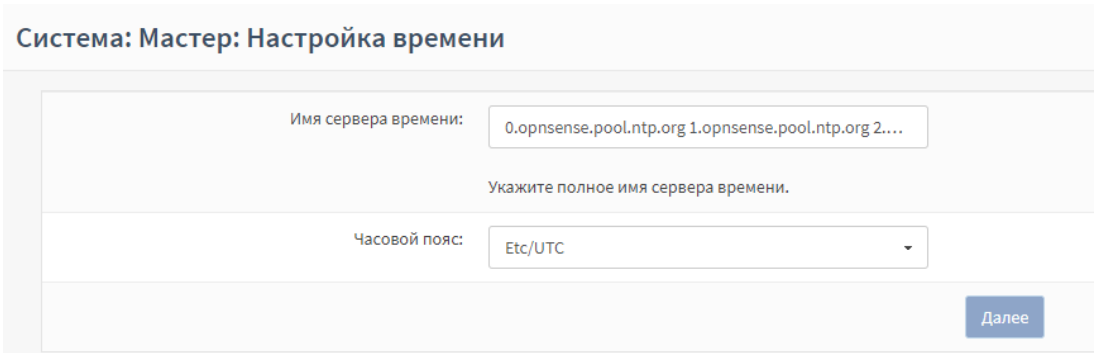


Рисунок 196— Система: Мастер: шаг 2

6.10.3. Мастер: шаг 3

На третьем шаге система предложит настроить WAN интерфейс. Подробнее заполнение всех полей приведено в подразделе 7.1 настоящего документа. После настройки необходимо нажать на кнопку «Далее».

6.10.4. Мастер: шаг 4

На четвертом шаге система предложит настроить LAN интерфейс. Подробнее заполнение всех полей приведено в подразделе 7.1 настоящего документа. После настройки необходимо нажать на кнопку «Далее».

6.10.5. Мастер: шаг 5

На пятом шаге начальной настройки система предложит настроить корневой пароль (рисунок 197). В поле «Пароль пользователя root:» необходимо ввести пароль пользователя root. В поле «Подтверждение пароля пользователя root:» необходимо ввести пароль из поля «Пароль пользователя root:» повторно и нажать на кнопку «Далее».

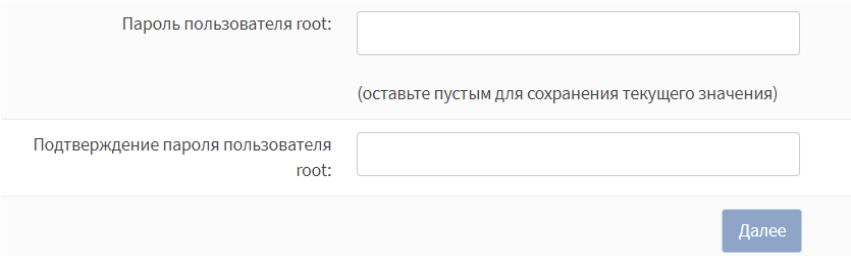


Рисунок 197 — Система: Мастер: шаг 5

6.10.6. Мастер: шаг 6

На шестом шаге начальной настройки система предложит перезагрузиться для применения настроек (рисунок 198). Необходимо нажать на кнопку «Перезагрузить».

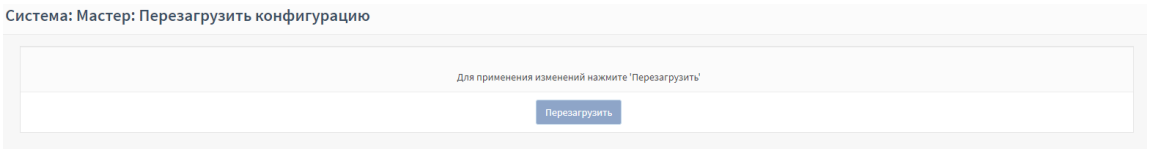


Рисунок 198 — Система: Мастер: шаг 6

6.11. Подраздел «Журналы»

В подразделе «Журналы» отображается журнал Syslog (системный журнал реализован на базе Syslog), журнал событий конфигураций системы (реализован на базе configd), журнал событий веб-интерфейса (реализован на базе lighttpd), журнал системных событий, журнал событий безопасности, журнал действий пользователей.

6.11.1. Категория «Журнал Syslog»

Категория «Журнал Syslog» позволяет просматривать журнал Syslog в формате таблицы, где имеются данные о дате/времени события системы, а также сообщения о выполненном действии системы (рисунок 199). В данном журнале приводятся все основные системные сообщения о работе системы и изменения в ней каких-либо параметров.

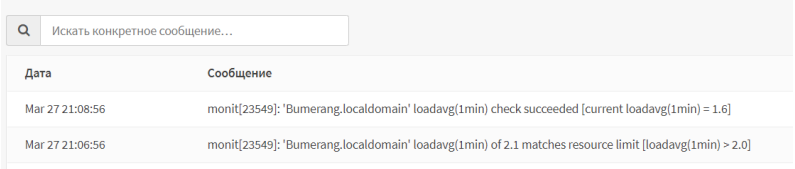


Рисунок 199— Система: Журналы: Журнал Syslog

6.11.2. Категория «Backend журнал»

Категория «Backend журнал» позволяет просматривать журнал Backend, в котором отображается содержимое файла /var/log/configd.log. В журнале Backend отображаются все события, отправленные через веб-интерфейс, а также изменения всех параметров системы (изменения настроек ПК «InfoWatch ARMA Industrial Firewall», добавления правил, маршрутов и т.д.) в виде таблицы. В таблице отображаются данные о дате/времени события, а также сообщение о выполненном действии Backend журнала (рисунок 200). В данном журнале приводятся записи о результатах выполнения различных операций внутреннего конфигуратора сервера.

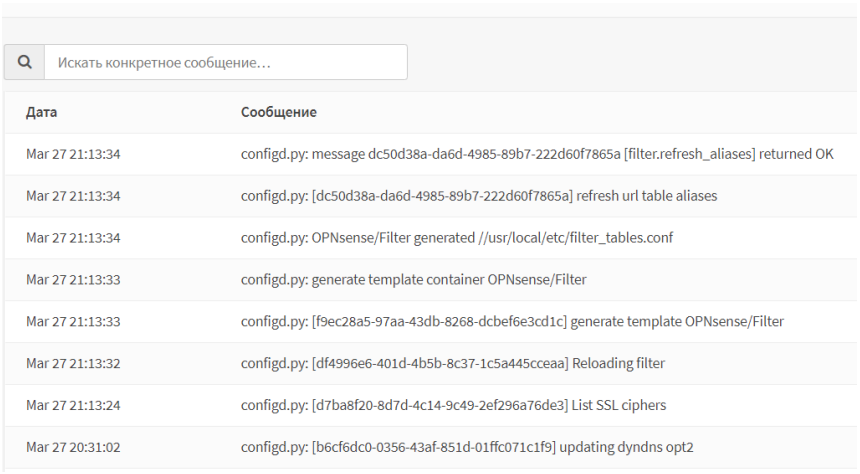


Рисунок 200 — Система: Журналы: Backend журнал

6.11.3. Категория «WebGUI журнал»

Категория «WebGUI журнал» позволяет просматривать журнал веб-интерфейса в формате таблицы, где имеется данные о дате/времени события системы, а также сообщение о выполненном действии в веб-интерфейсе (рисунок 201). В данном журнале представлены записи о событиях, связанных с веб-интерфейсом.

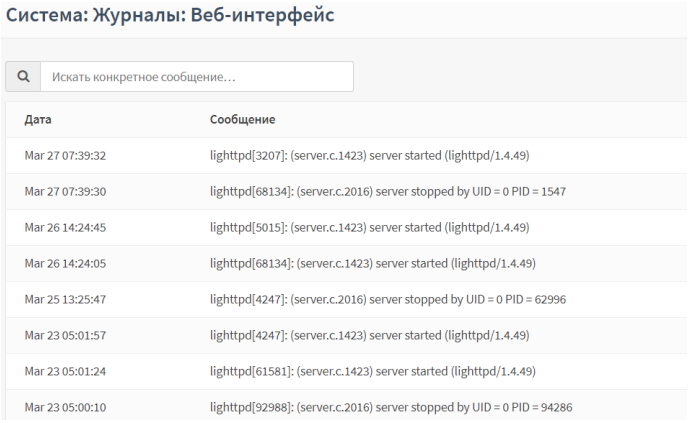


Рисунок 201 — Система: Журналы: WebGUI журнал

6.11.4. Категория «Журнал событий безопасности»

Категория «Журнал событий безопасности» позволяет просматривать журнал событий безопасности в формате таблицы. Таблица содержит следующие данные (рисунок 202):

– дата;

– механизм;

- отправитель;
- получатель;
- действие;
- описание;
- имя пользователя;
- кнопка «Дополнительная информация».

В журнале событий безопасности отображаются следующие события:

- для системы обнаружения вторжений:
  - срабатывание сигнатур;
- для межсетевого экрана:
  - срабатывания правил межсетевого экрана;
- для arpwatch:
  - подключение несанкционированного устройства;
  - обнаружение конфликта IP-адресов;
  - обнаружение изменения IP, MAC адреса;
  - обнаружение подмены MAC адресов;
  - обнаружение подмены IP-адресов.
- для Портала авторизации:
  - удачная/неудачная авторизация пользователя.

В журнале событий безопасности с помощью сквозного поиска по всем полям осуществляется фильтрация. Для поиска по всем полям таблицы событий необходимо ввести строку совпадения в поле «Поиск» вверху таблицы и нажать на кнопку  . Для поиска по определенному столбцу необходимо ввести строку совпадения в поле «Поиск» вверху столбца и нажать на кнопку  .

Для экспорта журнала событий безопасности наверху страницы необходимо выбрать в раскрывающемся меню формат экспортируемого файла:

– CSV (экспортируется файл журнала в формате CSV с примененными фильтрами, со столбцом дополнительной информации);

– PDF расширенный (экспортируется файл журнала в формате PDF с примененными фильтрами, со столбцом дополнительной информации);

– PDF (экспортируется файл журнала в формате PDF с примененными фильтрами, без столбца дополнительной информации).

Нажать кнопку «Экспорт».

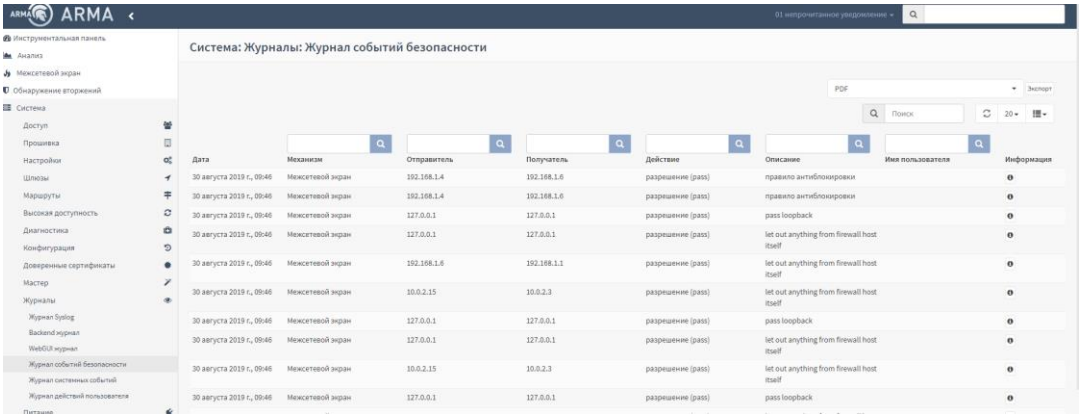


Рисунок 202 — Система: Журналы: Журнал событий безопасности

6.11.5. Категория «Журнал действий пользователей»

Категория «Журнал действий пользователей» позволяет просматривать журнал действий пользователей в формате таблицы. Таблица содержит следующие данные (рисунок 203):

– дата;

– имя пользователя;

– адрес;

– действия;

– успешно.

В журнале действий пользователей отображаются следующие события:

– включение и отключение межсетевого экрана;

– включение и отключение системы обнаружения вторжений;

– успешный/неуспешный доступ к страницам интерфейса;

– изменение/добавление/удаление правил межсетевого экрана;

– изменение настроек межсетевого экрана;

– изменение правил системы обнаружения вторжений;

– изменение настроек системы обнаружения вторжений;

– успешная/неуспешная авторизация в графическом и консольном интерфейсах;

– изменение размера записей в WebGUI журнале;

– создание нового пользователя;

– включение «сложного» пароля;

– изменение настроек мониторинга состояния системы на странице анализа трафика, настроек monit;

– перезагрузка системы.

В журнале действий пользователей с помощью сквозного поиска по всем полям осуществляется фильтрация. Для поиска по всем полям таблицы событий необходимо ввести строку совпадения в поле «Поиск» вверху таблицы и нажать на кнопку  . Для поиска по определенному столбцу необходимо ввести строку совпадения в поле «Поиск» вверху столбца и нажать на кнопку  .

Для экспорта журнала действий пользователей наверху страницы необходимо выбрать в раскрывающемся меню формат экспортируемого файла:

– CSV (экспортируется файл журнала в формате CSV с примененными фильтрами, со столбцом дополнительной информации);

– PDF расширенный (экспортируется файл журнала в формате PDF с примененными фильтрами, со столбцом дополнительной информации);

– PDF (экспортируется файл журнала в формате PDF с примененными фильтрами, без столбца дополнительной информации).

Нажать кнопку «Экспорт».

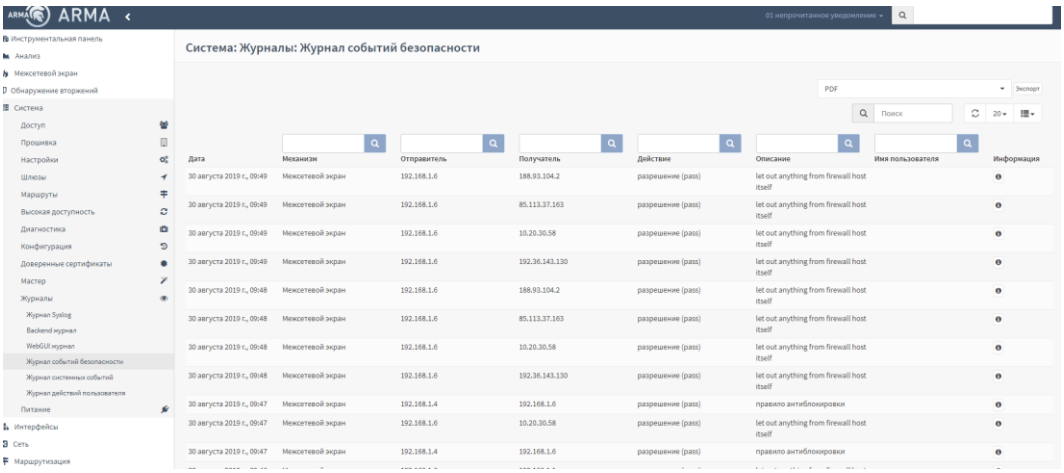


Рисунок 203 — Система: Журналы: Журнал действий пользователей

6.11.6. Категория «Журнал системных событий»

Категория «Журнал системных событий» позволяет просматривать журнал системных событий в формате таблицы, где имеются данные о дате/времени события системы, а также сообщения о выполненном действии системы (рисунок 204).

В журнале системных событий отображаются следующие события:

– запуск ntp-сервера;

– нет подключения к ntp-серверу;

– выключение ntp-сервера;

– изменение настроек ntp-сервера;

– сбои Портала авторизации (неуспешная попытка входа в Портал авторизации;

– сбои системы обнаружения вторжений;

– события контроля целостности;

– запуск веб-сервера;

– неуспешный доступ к странице графического интерфейса;

– загрузка системы.

В журнале системных событий с помощью сквозного поиска по всем полям осуществляется фильтрация. Для поиска по всем полям таблицы событий необходимо ввести строку совпадения в поле «Поиск» вверху

таблицы и нажать на кнопку . Для поиска по определенному столбцу необходимо ввести строку совпадения в поле «Поиск» вверху столбца и нажать на кнопку .

Для экспорта журнала системных событий наверху страницы необходимо выбрать в раскрывающемся меню формат экспортируемого файла:

– CSV (экспортируется файл журнала в формате CSV с примененными фильтрами, со столбцом дополнительной информации);

– PDF расширенный (экспортируется файл журнала в формате PDF с примененными фильтрами, со столбцом дополнительной информации);

– PDF (экспортируется файл журнала в формате PDF с примененными фильтрами, без столбца дополнительной информации).

Нажать кнопку «Экспорт».

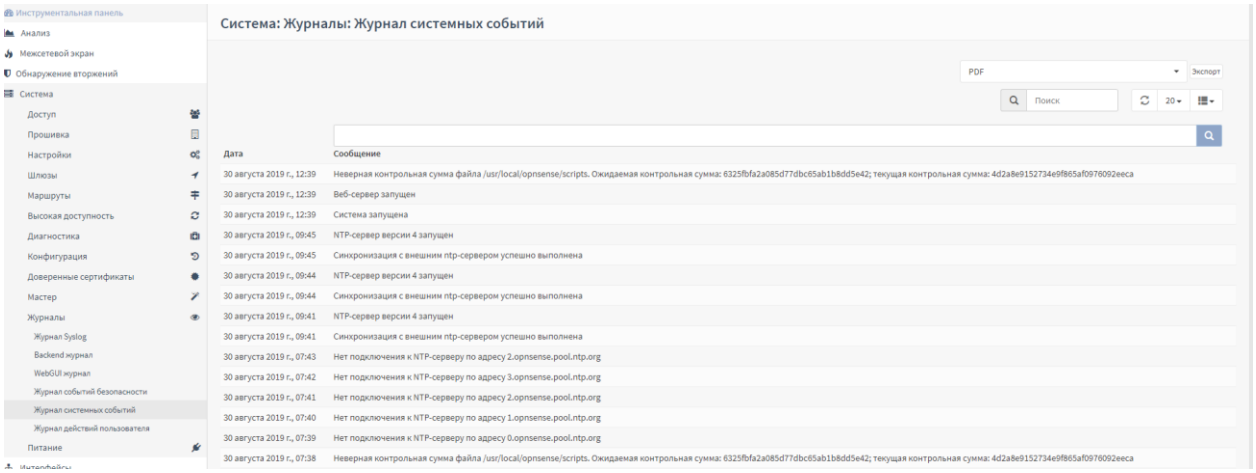


Рисунок 204 — Система: Журналы: Журнал системных событий

6.12. Подраздел «Питание»

Подраздел «Питание» позволяет перезагрузить/выключить систему, а также выйти из учетной записи пользователя.

6.12.1. Категория «Перезагрузка»

Категория «Перезагрузка» позволяет перезагрузить систему. Для этого необходимо нажать на кнопку «Да» после сообщения о перезагрузке (рисунок 205).

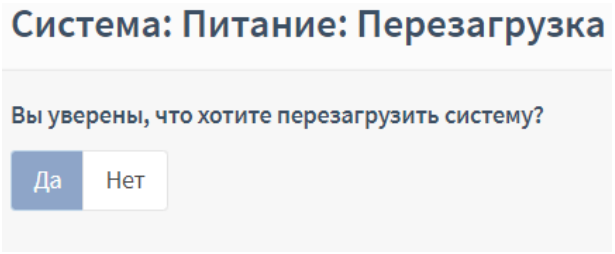


Рисунок 205 — Система: Питание: Перезагрузка

6.12.2. Категория «Выключение»

Категория «Выключение» позволяет выключить систему. Для этого необходимо нажать на кнопку «Да» после сообщения о выключении (рисунок 206).

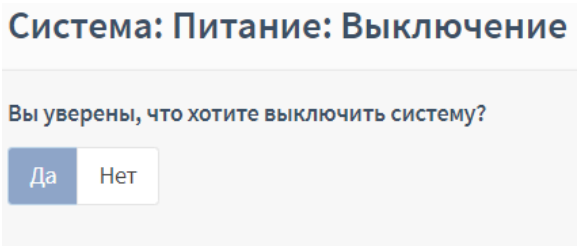


Рисунок 206 — Система: Питание: Выключение

6.12.3. Категория «Выход»

При переходе в категорию «Выход» произойдет моментальный выход из учетной записи пользователя и появится форма авторизации пользователя.

7. Раздел «Интерфейсы»

Раздел «Интерфейсы» позволяет редактировать, добавлять, удалять сетевые интерфейсы, выгружать дампы трафика выбранного интерфейса, осуществлять трассировку маршрута через выбранный сетевой интерфейс, проверять «ping» с выбранного сетевого интерфейса.

7.1. Подраздел «[Название интерфейса]»

Категория «[Название интерфейса]» позволяет настраивать общую конфигурацию интерфейса, конфигурацию статического IP-адреса (при выборе данного типа конфигурации), конфигурацию DHCP (при выборе данного типа конфигурации), конфигурацию PPP (при выборе данного типа конфигурации), конфигурацию PPPoE (при выборе данного типа конфигурации), конфигурацию PPTP (при выборе данного типа конфигурации), конфигурацию L2TP (при выборе данного типа конфигурации).

При редактировании [Название интерфейса] в поле «Включен» необходимо установить флажок для включения данного сетевого интерфейса. В поле «Блокировать» необходимо установить флажок для невозможности удаления данного интерфейса. В поле «Описание» необходимо ввести название интерфейса. В поле «Блокировать частные сети» необходимо установить флажок для блокирования трафика с IP-адресов, которые зарезервированы для частных сетей, в протоколе RFC 1918 (10/8, 172.16/12, 192.168/16), а также "зеркальных" (loopback) адресов (127/8). В настройке «Блокировать bogon сети» необходимо установить флажок для блокирования трафика от IP-адресов, которые зарезервированы или еще не присвоены IANA, не относящиеся к RFC 1918 (bogon — IP-адреса, которые не должны встречаться в таблицах маршрутизации в сети интернет или в качестве адреса отправителя получаемых пакетов). В полях «Тип конфигурации IPv4/IPv6» необходимо выбрать тип конфигурации. В поле «MAC-адрес» необходимо

ввести адрес физического интерфейса, соответствующий редактируемому сетевому интерфейсу. В поле «Максимальный размер кадра» необходимо ввести расчетное значение. В поле «Скорость и двусторонний режим передачи данных» необходимо выбрать скорость и двусторонний режим передачи для редактируемого интерфейса (рисунок 207).

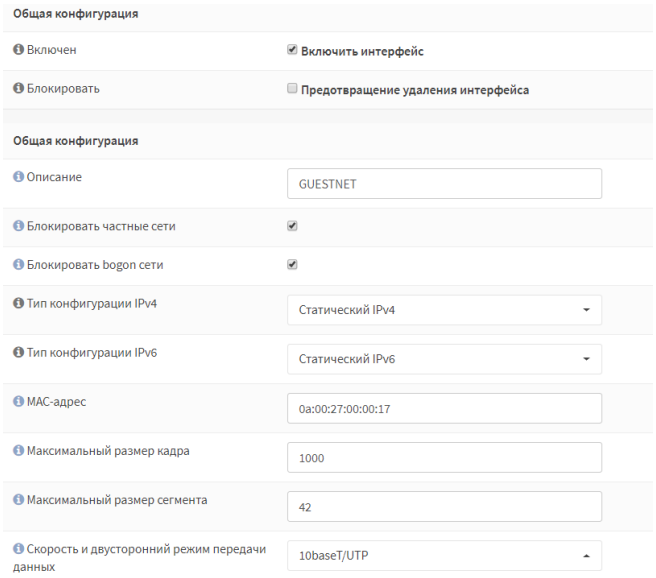


Рисунок 207 — Интерфейсы: [Название интерфейса]: Общая конфигурация

При выборе в поле «Тип конфигурации IPv4/IPv6» тип конфигурации «Статический IPv4/IPv6» появится группа настроек «Конфигурация статического IPv4/IPv6-адреса». В поле «IPv4/IPv6-адрес» необходимо ввести IP-адрес и необходимо выбрать маску подсети. В поле «Публичный IPv4/Ipv6-адрес шлюза» необходимо выбрать имеющийся шлюз из списка или добавить новый, нажав на . В группе настроек «Добавить новый шлюз» в поле «Шлюз по умолчанию» необходимо установить флажок для создания шлюза, который будет использоваться по умолчанию, в поле «Шлюз для Multy-WAN» необходимо установить флажок для включения шлюза для Multy-WAN, в поле «Имя шлюза» необходимо ввести название шлюза, в поле «IPv4/IPv6-адрес шлюза» необходимо ввести IP-адрес шлюза, в поле «Описание» необходимо ввести описание шлюза и необходимо нажать на кнопку «Сохранить». В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения

(данное поле имеется только в поле «Конфигурация статического IPv6») (рисунок 208).

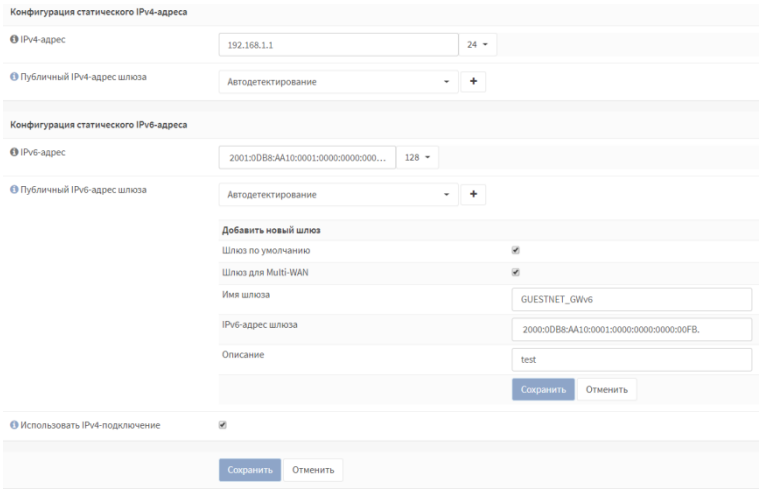


Рисунок 208 — Интерфейсы: [Название интерфейса]: Конфигурация статического IPv4/IPv6

При выборе в поле «Тип конфигурации IPv4» тип конфигурации «DHCP» появится группа настроек «Конфигурация DHCP-клиента». В поле «Режим настройки» необходимо выбрать режим настройки.

Если в поле «Режим настройки» выбран пункт «Базовая», появятся следующие поля настройки. В поле «Псевдоним IPv4-адресов» необходимо ввести значение псевдонима IPv4-адреса. В поле «Отклонить аренду IP-адресов» необходимо ввести IP-адрес публичного DHCP-сервер, который необходимо игнорировать. В поле «Имя хоста» необходимо ввести идентификатор DHCP-клиента (рисунок 209).

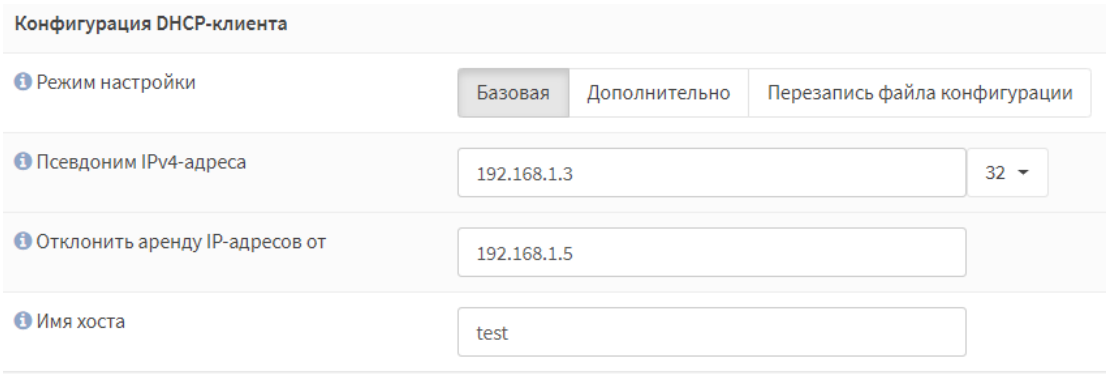


Рисунок 209 — Интерфейсы: [Название интерфейса]: Конфигурация DHCPv4 (Базовая)

Если в поле «Режим настройки» выбран пункт «Дополнительно», появятся следующие поля настройки. В поле «Отклонить аренду IP-адресов» необходимо ввести IP-адрес публичного DHCP-сервера, который необходимо игнорировать. В поле «Имя хоста» необходимо ввести идентификатор DHCP-клиента. В поле «Тайминг протокола» необходимо ввести в соответствующие поля время аренды IP-адресов в DHCP (возможно задать автоматически, нажав на кнопки «FreeBSD по умолчанию», «Очистить», «По умолчанию», «Сохраненный файл конфигурации»). В поле «Требования к аренде адресов» необходимо ввести опции DHCP, которые будут переданы серверу. В поле «Модификаторы параметра» необходимо ввести модификаторы параметров DHCP, которые будут применены для получения аренды DHCP (рисунок 210).

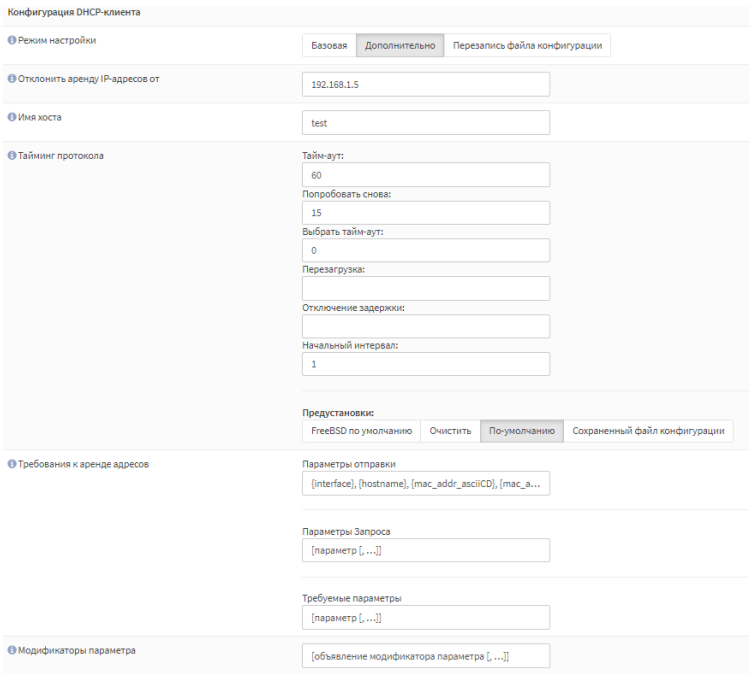


Рисунок 210 — Интерфейсы: [Название интерфейса]: Конфигурация DHCPv4 (Дополнительно)

Если в поле «Режим настройки» выбран пункт «Перезапись файла конфигурации», появятся следующее поле «Перезапись файла конфигурации», в котором надо ввести полный абсолютный путь к файлу конфигурации DHCP (рисунок 211).

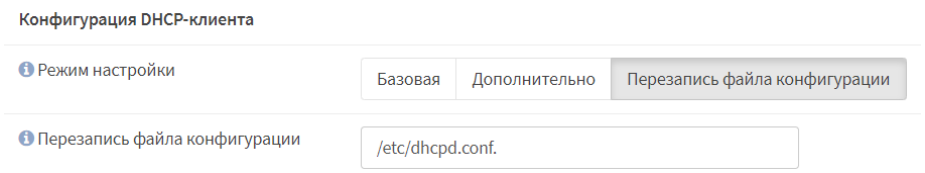


Рисунок 211 — Интерфейсы: [Название интерфейса]: Конфигурация DHCPv4 (Перезапись файла конфигурации)

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «DHCP» появится группа настроек «Конфигурация DHCPv6-клиента». В поле «Режим настройки» необходимо выбрать режим настройки.

Если в поле «Режим настройки» выбран пункт «Базовая», появятся следующие поля настройки. В поле «Запрашивается только префикс IPv6» необходимо установить флажок для того, чтобы запрашивать только префикс IPv6, но не его адрес. В поле «Размер делегирования префикса» необходимо выбрать значения делегируемого префикса. В поле «Отправить prefix-hint IPv6» необходимо установить флажок для отправки prefix-hint IPv6. В поле «Отправлять сообщение SOLOCIT» необходимо установить флажок для предотвращения бесконечного ожидания объявления маршрута. В поле «Предупреждение отправки» необходимо установить флажок для того, чтобы не отправлять сообщение о выходе клиента. В поле «Включить отладку» необходимо установить флажок для включения откладки для DHCPv6. В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения. В поле «Примените приоритет VLAN» необходимо выбрать приоритет VLAN (рисунок 212).

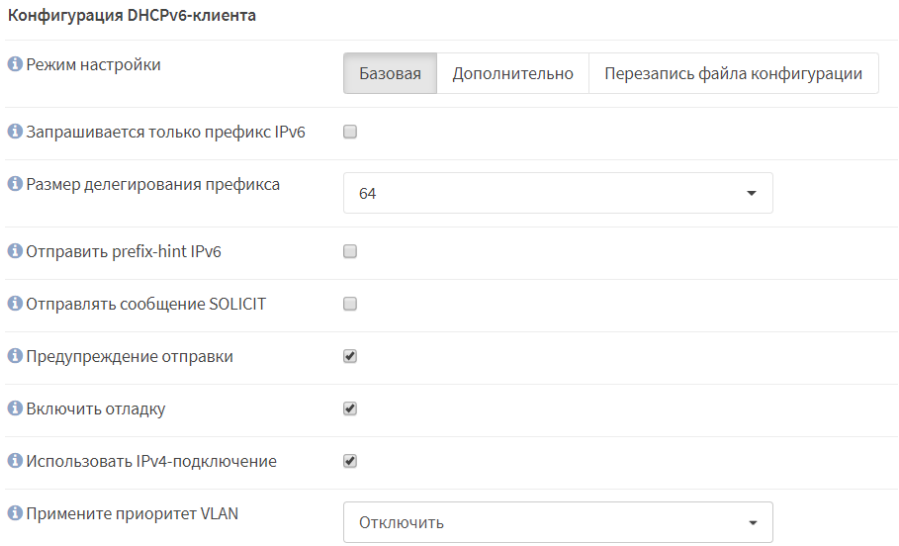


Рисунок 212 — Интерфейсы: [Название интерфейса]: Конфигурация DHCPv6 (Базовая)

Если в поле «Режим настройки» выбран пункт «Дополнительно», появятся следующие поля настройки. В поле «Отправлять сообщение SOLOCIT» необходимо установить флажок для предотвращения бесконечного ожидания объявления маршрута. В поле «Предупреждение отправки» необходимо установить флажок для того, чтобы не отправлять сообщение о выходе клиента. В поле «Включить отладку» необходимо установить флажок для включения откладки для DHCPv6. В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения. В поле «Примените приоритет VLAN» необходимо выбрать приоритет VLAN. В поле «Оператор Интерфейса» необходимо установить флажок напротив поля «Только информация» для того, чтобы заменять параметры информационной конфигурации с серверами, в поле «Параметры отправки» необходимо ввести опции DHCP, передаваемые в ответ на запрос DHCP, в поле «Параметры Запроса» необходимо ввести опции DHCP, которые будут переданы на запрос DHCP, в поле «Сценарий» необходимо ввести абсолютный путь к скрипту. В поле «Объединение идентификации» необходимо установить флажок напротив поля «Постоянное выделение адресов» для постоянного выделения адресов и напротив поля «Делегирование префикса» для делегирования префикса. В

полях в поле «Префикс интерфейса» необходимо ввести префикс и его длину в соответствующих полях. В полях «Аутентификация» необходимо ввести имя, по которому происходит авторизации, протокол, алгоритм, rdm. В полях «Информация о ключе» необходимо ввести в соответствующих полях имя ключа, realm (область авторизации), идентификатор ключа (32 битный идентификатор ключа), secret (значение ключа), окончание функции (время истечения срока действия ключа, если ключ бессрочен необходимо ввести «0») (рисунок 213).

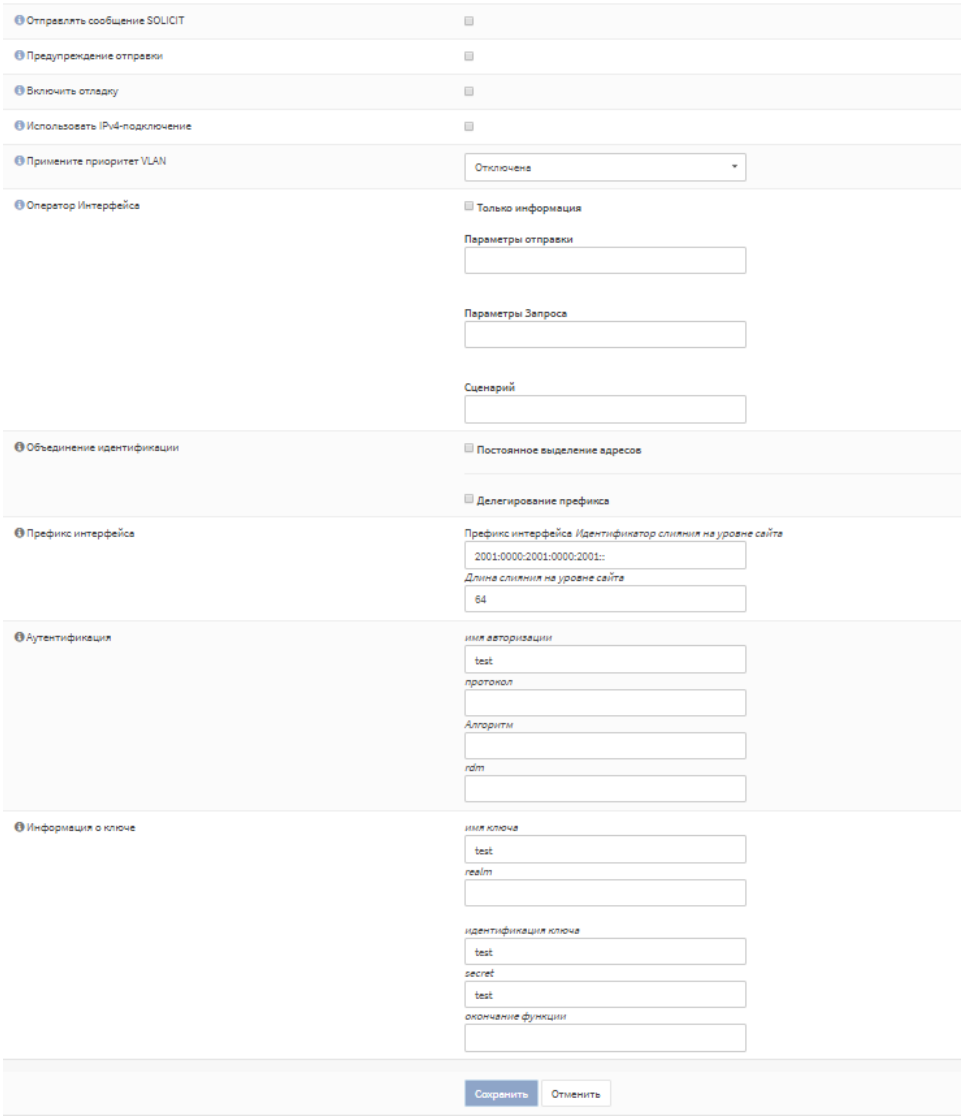


Рисунок 213 — Интерфейсы: [Название интерфейса]: Конфигурация DHCPv6 (Дополнительно)

Если в поле «Режим настройки» выбран пункт «Перезапись файла конфигурации», появятся следующие настройки. В поле «Отправлять

сообщение SOLOCIT» необходимо установить флажок для предотвращения бесконечного ожидания объявления маршрута. В поле «Предупреждение отправки» необходимо установить флажок для того, чтобы не отправлять сообщение о выходе клиента. В поле «Включить отладку» необходимо установить флажок для включения откладки для DHCPv6. В поле «Использовать IPv4-подключение» необходимо установить флажок для использования IPv4-подключения. В поле «Примените приоритет VLAN» необходимо выбрать приоритет VLAN. В поле «Перезапись файла конфигурации» необходимо ввести полный абсолютный путь к файлу конфигурации DHCPv6 (рисунок 214).

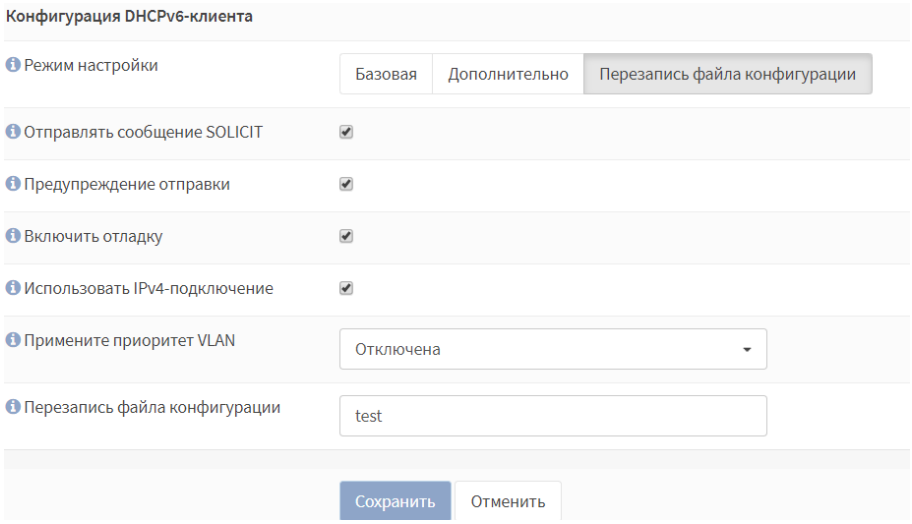


Рисунок 214 — Интерфейсы: [Название интерфейса]: Конфигурация DHCPv6 (Перезапись файла конфигурации)

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «SLAAC» появится группа настроек «Конфигурация SLAAC». В поле «Использовать IPv4-подключение» необходимо установить флажок для включения IPv4-подключения (рисунок 215).

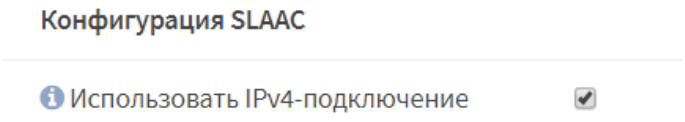


Рисунок 215 — Интерфейсы: [Название интерфейса]: SLAAC

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «Туннель 6RD» появится группа настроек «Конфигурация 6RD». В поле «Префикс 6RD» необходимо ввести IPv6-префикс 6RD-сегмента. В поле «Граничный передатчик 6RD» необходимо ввести IPv6-адрес 6RD-шлюза. В поле «Длина IPv6-префикса 6RD-сегмента» необходимо выбрать значение длины префикса 6RD-сегмента (рисунок 216).

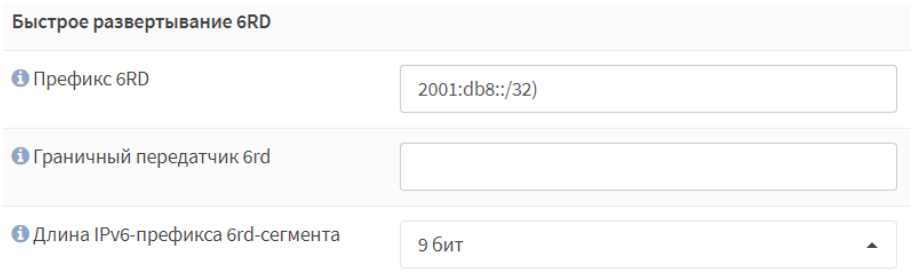


Рисунок 216— Интерфейсы: [Название интерфейса]: 6RD

При выборе в поле «Тип конфигурации IPv6» тип конфигурации «Отслеживать состояние интерфейсов» появится группа настроек «Отслеживать IPv6-интерфейсы». В поле «IPv6-интерфейс» необходимо выбрать динамический IPv6-адрес WAN интерфейса, который будет отслеживаться для конфигурации. В поле «Идентификатор IPv6-префикса» необходимо ввести значение идентификатора IPv6-префикса. В поле «Ручное конфигурирование» необходимо установить флажок для включения ручной настройки DHCPv6 и маршрутизатора (рисунок 217).

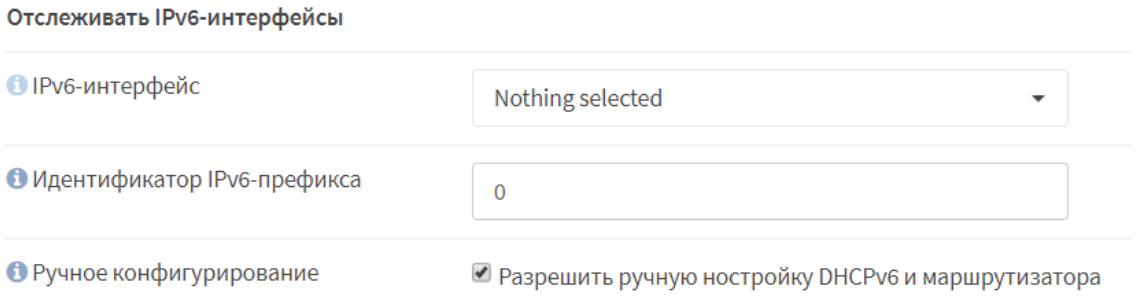


Рисунок 217 — Интерфейсы: [Название интерфейса]: Отслеживать состояние интерфейсов

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.2. Подраздел «Назначение портов»

Подраздел «Назначение портов» позволяет настраивать соответствие между логическими и физическими сетевыми интерфейсами. Для этого необходимо выбрать в выпадающем списке напротив логического сетевого интерфейса соответствующий ему физический сетевой интерфейс. Для удаления сетевого интерфейса необходимо нажать на кнопку соответствующий значок напротив сетевого интерфейса (рисунок 218). Для сохранения настроек необходимо нажать на кнопку «Сохранить».

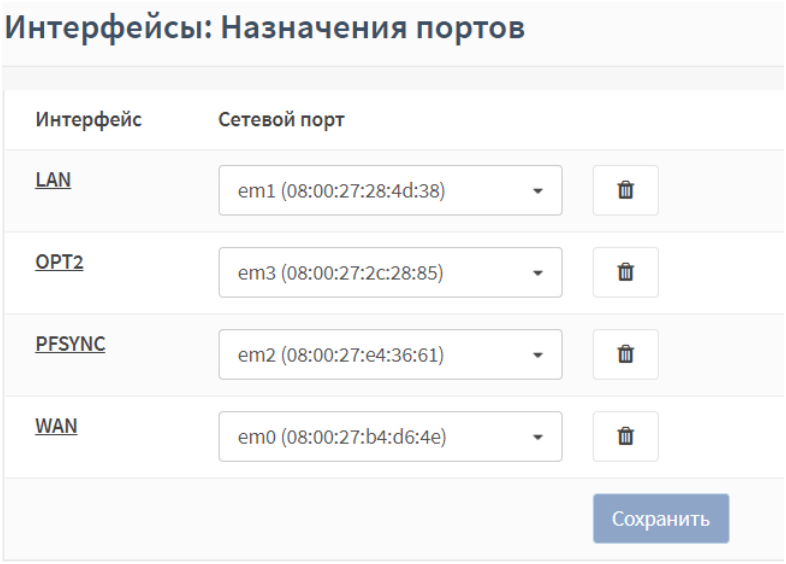


Рисунок 218 — Интерфейсы: Назначение портов

7.3. Подраздел «Обзор»

Подраздел «Обзор» позволяет просматривать следующую информацию о каждом настроенном сетевом интерфейсе (рисунок 219):

- статус интерфейса;
- MAC-адрес интерфейса;
- IPv4-адрес;
- маску подсети IPv4;
- локальный IPv6-адрес канала;
- скорость и двусторонний режим передачи данных;
- количество входящих/исходящих пакетов (их суммарный размер);

– количество разрешенных входящих/исходящих пакетов (их суммарный размер);

– количество заблокированных входящих/исходящих пакетов (их суммарный размер);

– количество коллизий;

– прерывания.

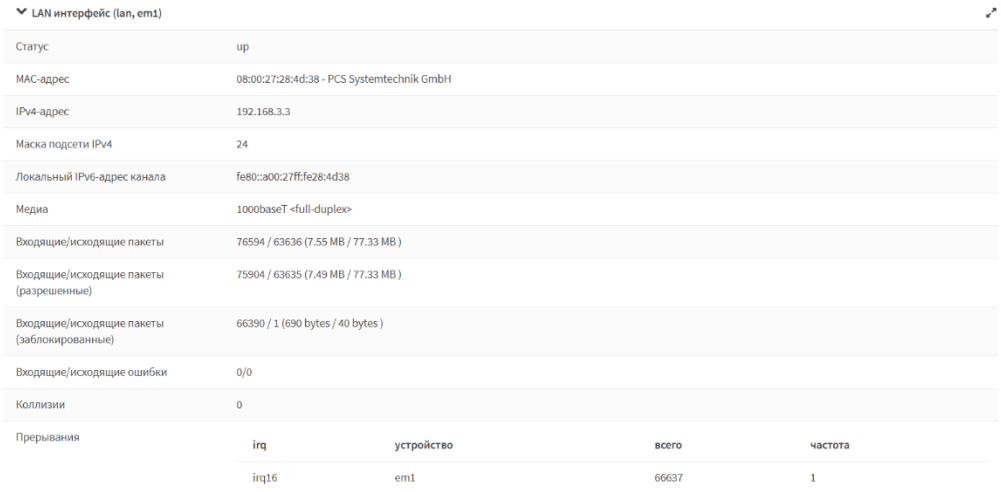


Рисунок 219 — Интерфейсы: Обзор

7.4. Подраздел «Настройки»

В подразделе «Настройки» приведены общие настройки интерфейсов.

В пункте «CRC аппаратного обеспечения» необходимо установить флажок напротив поля «Отключить сброс контрольной суммы аппаратного обеспечения» для отключения расчета контрольной суммы Ethernet-кадра средствами сетевой карты без участия ЦПУ. В поле «TSO аппаратного обеспечения» необходимо установить флажок напротив поля «Отключить сброс сегментации TCP аппаратного обеспечения» для отключения сброса сегментации TCP-пакета без участия ЦПУ с помощью аппаратных возможностей сетевой карты. В поле «LRO аппаратного обеспечения» необходимо установить флажок напротив поля «Отключить LRO аппаратного обеспечения» для отключения буферизации входящих пакетов и их передачи сетевому стеку в агрегированном виде с целью избежания неэффективной передачи каждого пакета в отдельности. В поле «Фильтрация

аппаратного обеспечения VLAN» необходимо выбрать степень использования фильтра VLAN. В поле «Обработка ARP» необходимо установить флажок напротив поля «Блокировать ARP» для того, чтобы заблокировать сообщения в журнале регистрации ARP, если несколько сетевых интерфейсов хранятся на одном широковещательном домене. В поле «Уникальный идентификатор DHCP» необходимо ввести уникальный идентификатор DHCP (рисунок 220). Необходимо нажать на кнопку «Сохранить» для сохранения настроек.

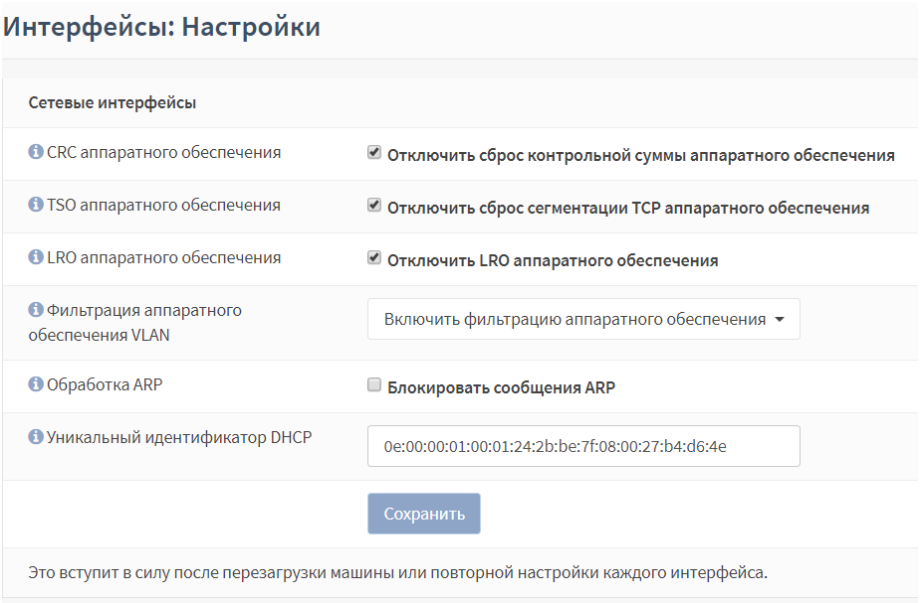


Рисунок 220 — Интерфейсы: Настройки

7.5. Подраздел «Другие типы»

В подразделе «Другие типы» описаны другие типы интерфейсов. К таким типам относятся:

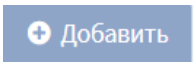
- Сетевой мост;
- GIF;
- GRE;
- LAGG;
- VLAN.

7.5.1. Категория «Сетевой мост»

В категории «Сетевой мост» отображаются настроенные сетевые мосты в виде таблицы с возможностью удаления и редактирования, нажав на соответствующие кнопки напротив необходимого сетевого моста. Таблица содержит следующие данные (рисунок 221):

– название сетевого моста;
– участники (перечень сетевых интерфейсов);
– описание.

Рисунок 221 — Интерфейсы: Другие типы: Сетевой мост

Для того, чтобы редактировать существующие сетевые мосты, необходимо нажать на кнопку  напротив сетевого моста. Для того, чтобы создать новый сетевой мост, необходимо нажать на кнопку 

.

При редактировании сетевого моста в поле «Интерфейсы-участники» необходимо выбрать интерфейсы, соединенные с помощью этого моста. В поле «Описание» необходимо ввести описание сетевого моста (рисунок 222).

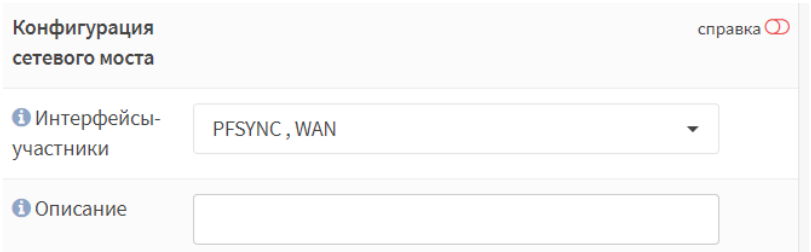


Рисунок 222 — Интерфейсы: Другие типы: Сетевой мост (редактирование)

При нажатии кнопки «Показать дополнительные параметры» появятся следующие группы настроек.

В группе настроек «Протокол связующего дерева (RSTP/STP)» в поле «Включить» необходимо установить флажок для включения протокола связующего дерева (RSTP/STP) для этого моста. В поле «Протокол» необходимо выбрать протокол связующего дерева. В поле «STP-интерфейсы» необходимо выбрать интерфейс для работы протокола связующего дерева. В поле «Действительное время (с)» необходимо ввести время действия конфигурации протокола связующего дерева. В поле «Время приветствия (с)» необходимо ввести интервал времени между широковещательными конфигурационными сообщениями связующего дерева. В поле «Приоритет» необходимо ввести приоритет сетевого моста для связующего дерева. В поле «Счетчик задержки» необходимо ввести значение счетчика задержки для передачи по протоколу связующего дерева. В полях в поле «Приоритет» необходимо установить приоритет для каждого интерфейса. В поле «Cost» необходимо ввести стоимость порта для каждого интерфейса. Каждый порт имеет свою стоимость (cost), обратно пропорциональную пропускной способности (bandwidth) порта и которую можно настраивать вручную (рисунок 223).

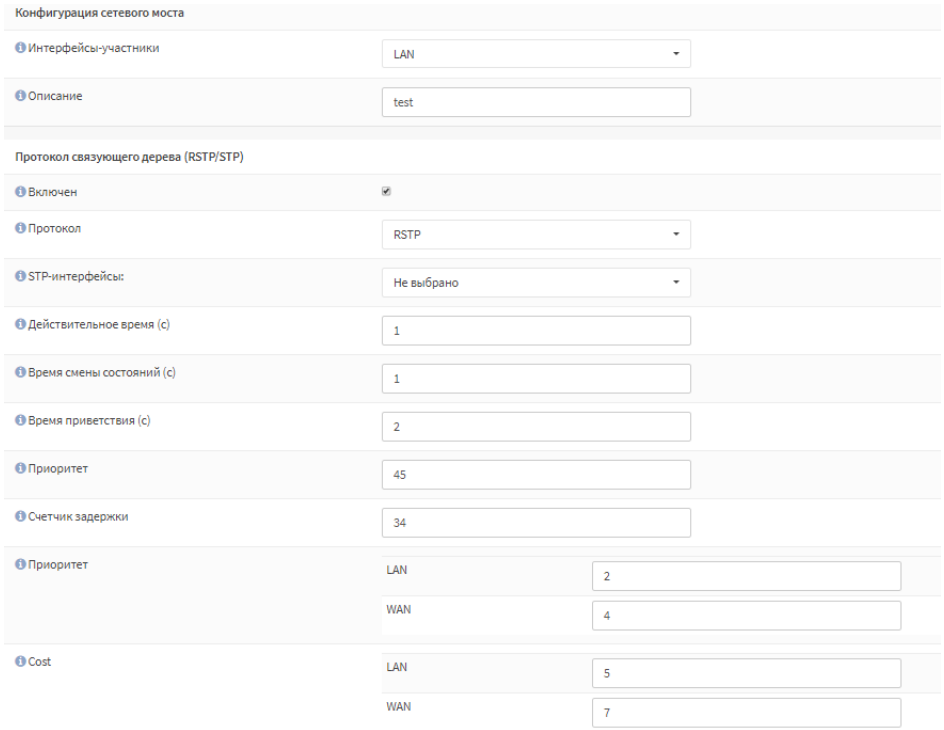


Рисунок 223 — Интерфейсы: Другие типы: Сетевой мост (редактирование: Протокол связующего дерева (RSTP/STP))

В группе настроек «Дополнительные параметры» в поле «Размер кэша (записей)» необходимо ввести значение размера кэша адресов сетевого моста. В поле «Время жизни адреса в кэше (с)» необходимо ввести время нахождения записи адреса в кэше адресов в секундах. В поле «Порт SPAN» необходимо выбрать интерфейс, который будет использоваться в качестве SPAN порта на мосту. В поле «Пограничный порт» необходимо выбрать интерфейс, который будет использоваться в качестве пограничного порта. В поле «Автоопределение граничного порта» необходимо выбрать сетевой интерфейс, для которого будет определяться автоматически граничный порт. В поле «Фиксированные порты» необходимо выбрать интерфейсы, которые будут отмечены как «фиксированные» интерфейсы. В поле «Частные порты» необходимо выбрать интерфейс, который будет отмечен как «частный» (рисунок 224).

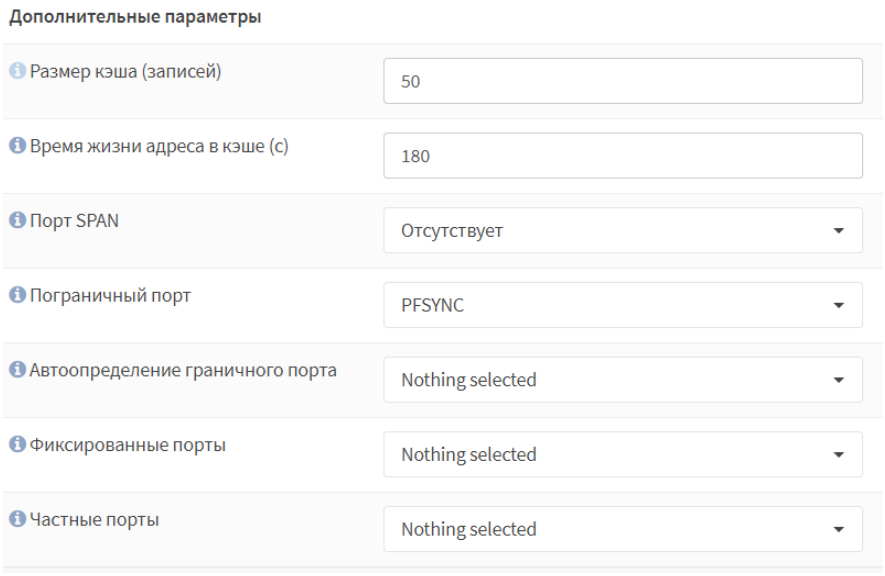


Рисунок 224 — Интерфейсы: Другие типы: Сетевой мост (редактирование: Дополнительные параметры)

Необходимо нажать на кнопку «Сохранить» для сохранения внесенных изменений.

7.5.2.Категория «GIF»

В категории «GIF» отображаются настроенные туннели GIF в виде таблицы с возможностью удаления и редактирования, нажав на соответствующие кнопки напротив GIF-туннеля. Таблица содержит следующие данные (рисунок 225):

– название туннеля GIF;

– удаленный IP-адрес пира GIF-туннеля;

– описание.

Рисунок 225 — Интерфейсы: Другие типы: GIF-туннель

Для того, чтобы редактировать существующие GIF-туннели, необходимо нажать на кнопку  напротив GIF-туннеля. Для того, чтобы создать новый GIF-туннель, необходимо нажать на кнопку  .

При редактировании GIF-туннеля в поле «Родительский интерфейс» необходимо выбрать сетевой интерфейс, который будет служить в качестве локального адреса для GIF-туннеля. В поле «Удаленный IP-адрес пира GIF-туннеля» необходимо ввести IP-адрес пира, по которому будут отправлены инкапсулированные пакеты GIF. В поле «Удаленный IP-адрес GIF-туннеля» необходимо ввести удаленную конечную точку GIF-туннеля. В поле «Кэширование маршрутов» необходимо установить флажок для кэширования маршрутов. В поле «Использовать ECN (Explicit Congestion Notification)» необходимо установить флажок для использования ECN (Explicit Congestion Notification). В поле «Описание» необходимо ввести

описание GIF-туннеля (рисунок 226). Необходимо нажать на кнопку «Сохранить» для сохранения GIF-туннеля.

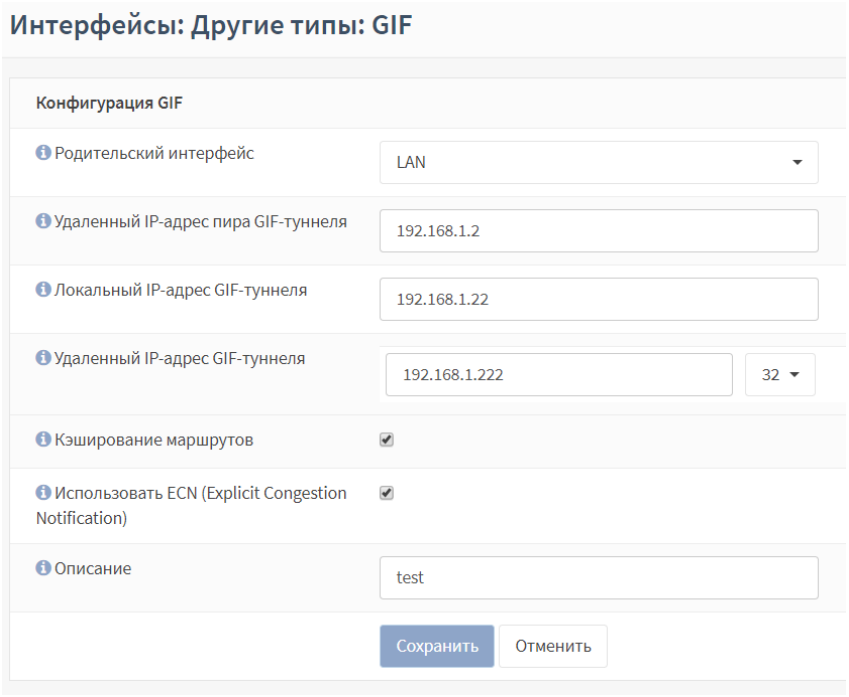


Рисунок 226 — Интерфейсы: Другие типы: GIF-туннель (редактирование)

7.5.3. Категория «GRE»

В категории «GRE» отображаются настроенные туннели GRE в виде таблицы с возможностью удаления и редактирования, нажав на соответствующие кнопки напротив туннеля GRE. Таблица содержит следующие данные (рисунок 227):

– название туннеля GRE;
– удаленный IP-адрес пира GRE-туннеля;
– описание.

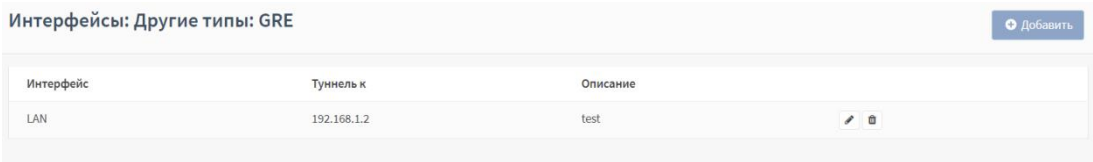
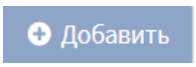


Рисунок 227 — Интерфейсы: Другие типы: GRE-туннель

Для того, чтобы редактировать существующие GRE-туннели, необходимо нажать на кнопку  напротив GRE-туннеля. Для того, чтобы создать новый GIF-туннель, необходимо нажать на кнопку 

.

При редактировании GRE-туннеля в поле «Родительский интерфейс» необходимо выбрать сетевой интерфейс, который будет служить в качестве локального адреса для GRE-туннеля. В поле «Удаленный IP-адрес пира GRE-туннеля» необходимо ввести IP-адрес пира, по которому будут отправлены инкапсулированные пакеты GRE. В поле «Удаленный IP-адрес GRE-туннеля» необходимо ввести удаленную конечную точку GRE-туннеля. В поле «Мобильный туннель» необходимо установить флажок для включения Mobile encapsulation вместо GRE туннеля. В поле «Способ поиска маршрута» необходимо установить флажок для указания неконкретного маршрута для правильной работы устройства GRE (в большинстве случаев это маршрут к хосту декапсуляции, который не проходит через туннель, так как это создаст петлю коммутации). В поле «Версия WCCP» необходимо установить флажок для использования версии 2 протокола WCCP. В поле «Описание» необходимо ввести описание GIF-туннеля (рисунок 228). Необходимо нажать на кнопку «Сохранить» для сохранения GRE-туннеля.

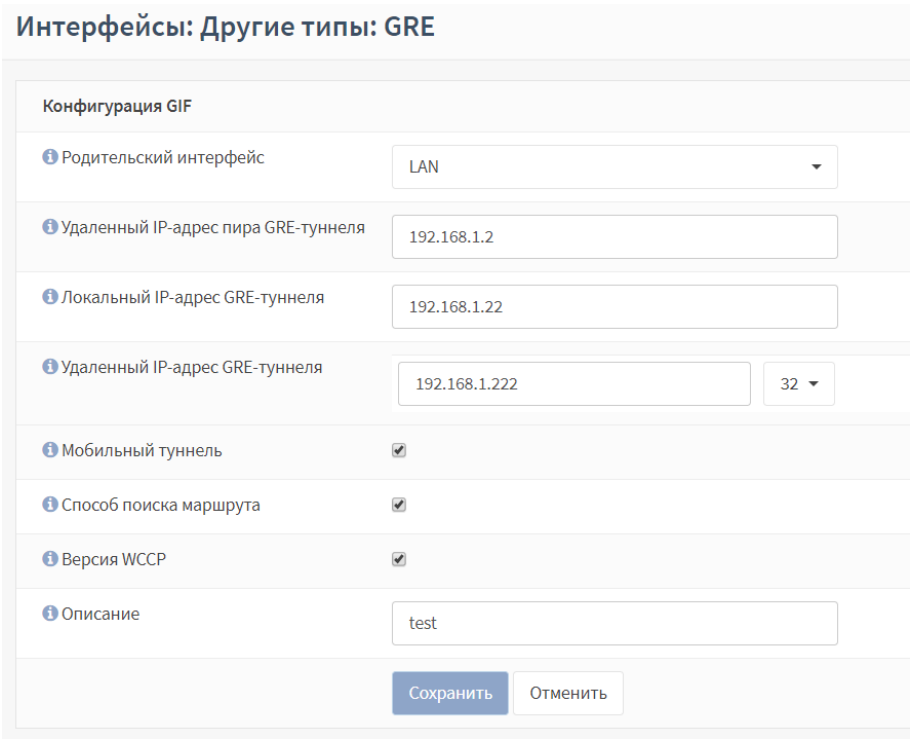


Рисунок 228 — Интерфейсы: Другие типы: GRE -туннель (редактирование)

7.5.4. Категория «LAGG»

Интерфейс LAGG используется для объединения нескольких сетевых интерфейсов в один виртуальный интерфейс для обеспечения аварийного переключения и агрегации каналов.

В категории «LAGG» отображаются настроенные интерфейсы LAGG в виде таблицы с возможностью удаления и редактирования, нажав на соответствующие кнопки напротив интерфейса LAGG. Таблица содержит следующие данные (рисунок 229):

– название интерфейса LAGG;
– удаленный IP-адрес пира интерфейса LAGG;
– описание.

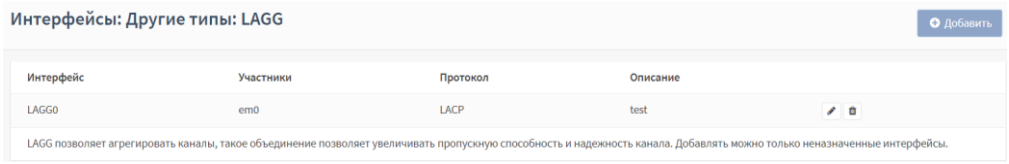


Рисунок 229 — Интерфейсы: Другие типы: LAGG

Для того, чтобы редактировать существующие интерфейсы LAGG, необходимо нажать на кнопку напротив интерфейса LAGG. Для того, чтобы создать новый интерфейс LAGG, необходимо нажать на кнопку Добавить.

При редактировании интерфейса LAGG в поле «Родительский интерфейс» необходимо выбрать не назначенные интерфейсы, которые могут использоваться для агрегации каналов. В поле «Протокол LAG» необходимо выбрать протокол:

– failover (посылает и принимает трафик только через главный порт, если главный порт недоступен, используется следующий активный порт. Первый добавленный интерфейс является ведущим, все добавленные после ведущего интерфейсы используются в качестве аварийных и включаются в

работу при обрыве соединения);

– Fec (поддерживает технологию Cisco EtherChannel);

– Lacp (поддерживает протокол агрегирования каналов (LACP) и протокол маркирования, описанные в IEEE 802.3ad. LACP согласовывает набор агрегированных ссылок с узлом в одну или несколько групп агрегированных каналов (LAG));

– Loadbalance (балансирует трафик между активными портами на основе хешированной информации в заголовке протокола и принимает входящий трафик из любого активного порта);

– roundrobin (исходящий трафик распределяется циклическим планировщиком через все активные порты, а входящий трафик принимается с любого активного порта);

– Отсутствует (этот протокол приостанавливает работу: отключает любой трафик без отключения самого LAGG-интерфейса).

В поле «Описание» необходимо ввести описание интерфейса (рисунок 230).

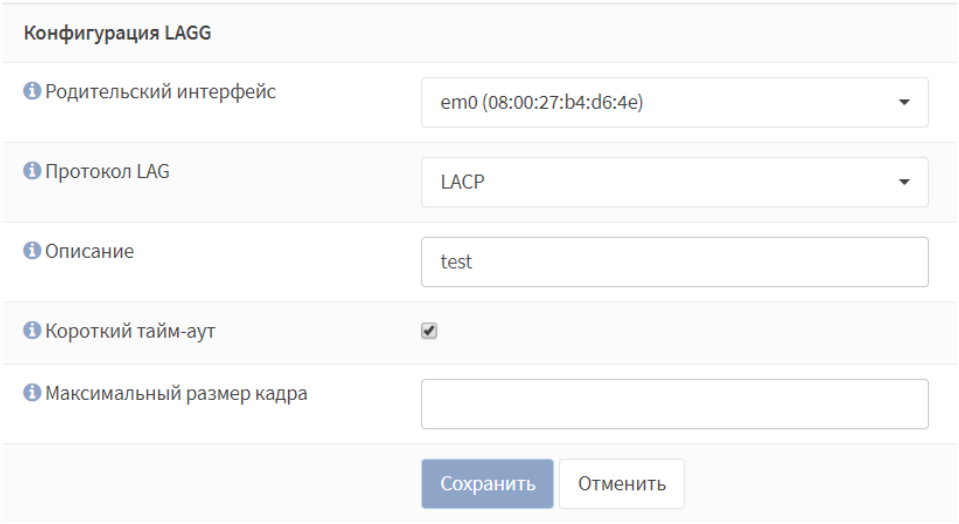


Рисунок 230 — Интерфейсы: Другие типы: LAGG (редактирование)

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.5.5. Категория «VLAN»

В категории «VLAN» отображаются настроенные интерфейсы VLAN в виде таблицы с возможностью удаления и редактирования, нажав на соответствующие кнопки напротив интерфейса VLAN. Таблица содержит следующие данные (рисунок 231):

– название интерфейса VLAN;

– тег;

– приоритет;

– описание.

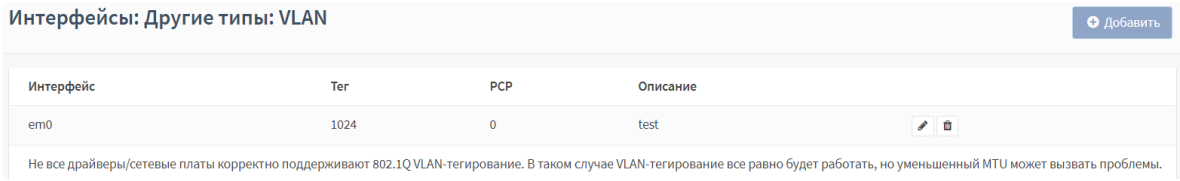
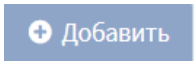


Рисунок 231 — Интерфейсы: Другие типы: VLAN

Для того, чтобы редактировать существующие интерфейсы VLAN, необходимо нажать на кнопку  напротив интерфейса VLAN. Для того, чтобы создать новый интерфейс VLAN, необходимо нажать на кнопку  .

При редактировании интерфейса VLAN в поле «Родительский интерфейс» необходимо выбрать сетевые интерфейсы, которые будут использоваться для агрегации каналов. В поле «Тег VLAN» необходимо ввести тег VLAN. В поле «Приоритет VLAN» необходимо выбрать приоритет VLAN. В поле «Описание» необходимо ввести описание интерфейса (рисунок 232).

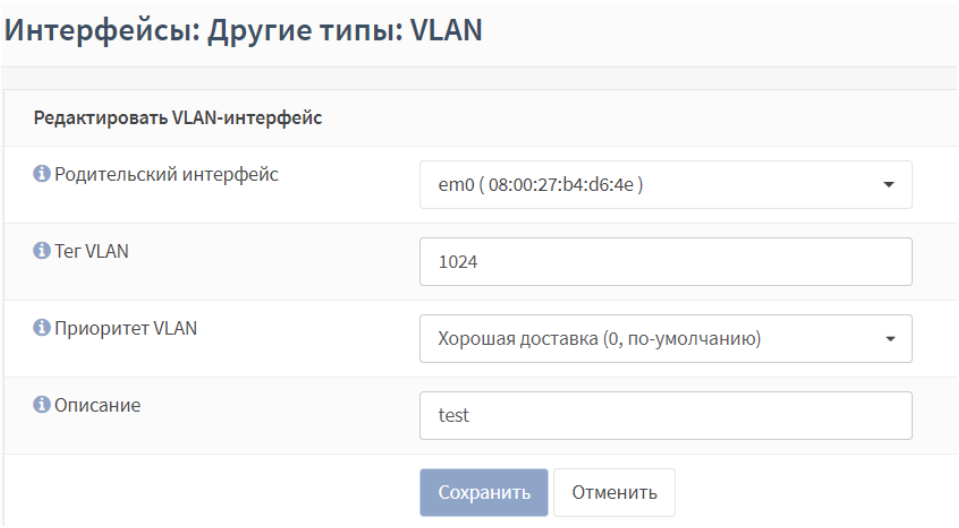


Рисунок 232 — Интерфейсы: Другие типы: VLAN (редактирование)

После внесения изменений необходимо нажать на кнопку «Сохранить».

7.6. Подраздел «Диагностика»

Подраздел «Диагностика» позволяет просматривать таблицу ARP, запускать сканирование ARP, просматривать таблицу DNS-записей, просматривать таблицу NDP-записей, экспортировать дамп трафика определенного сетевого интерфейса, выполнять и просматривать результаты команды «Ping», выполнять проверку порта (имеется ли на нем подключение), выполнять trace route.

7.6.1. Категория «Сканирование ARP»

Категория «Сканирование ARP» позволяет производить сканирование по протоколу ARP. В поле «Прослушиваемый интерфейс» необходимо выбрать сканируемый интерфейс. В поле «Сеть для исследования» необходимо ввести сеть для сканирования и нажать на кнопку «Запустить». По завершении сканирования в таблице появится результат сканирования (рисунок 233).

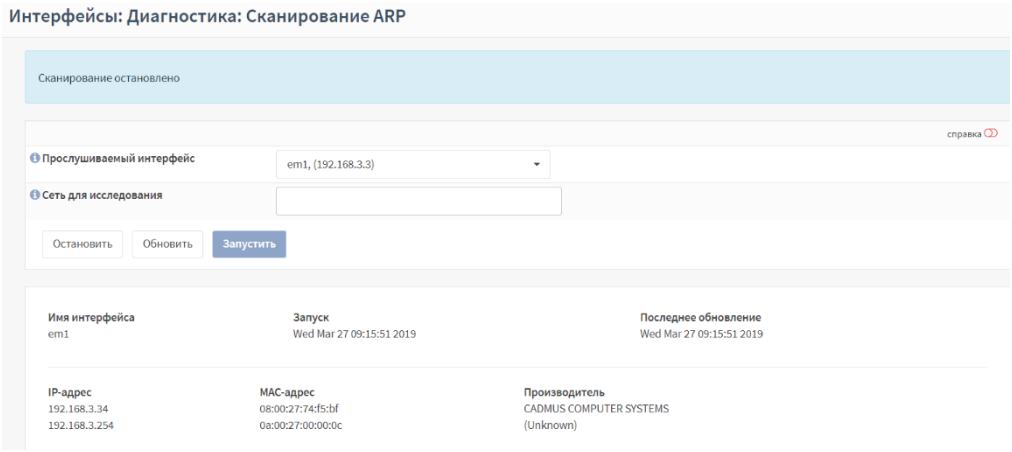


Рисунок 233 — Интерфейсы: Диагностика: Сканирование ARP

7.6.2. Категория «ARP-таблица»

В категории «ARP-таблица» отображается ARP-таблица с возможностью удаления данных и обновления, нажав на соответствующие кнопки. Таблица содержит следующие данные (рисунок 234):

– IP-адрес;
– MAC-адрес;
– производитель;
– название физического интерфейса;
– название сетевого интерфейса;
– имя хоста.

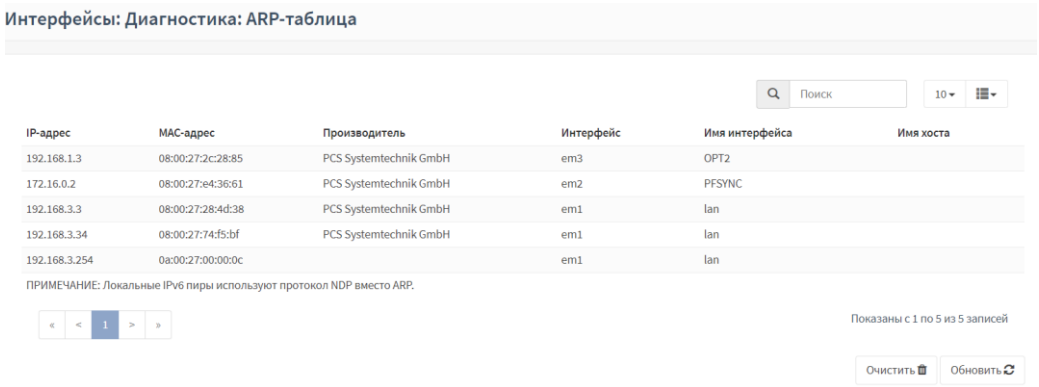


Рисунок 234 — Интерфейсы: Диагностика: ARP-таблица

7.6.3. Категория «Просмотр DNS-записей»

В категории «Просмотр DNS-записей» осуществляется поиск IP-адресов и записей, принадлежащих заданному имени хоста, а также отображается следующая информация (рисунок 235):

– ответ (тип и IP-адрес);

– время разрешения сервером доменных имен и/или IP-адресов (сервер, время запроса);

– дополнительная информация).

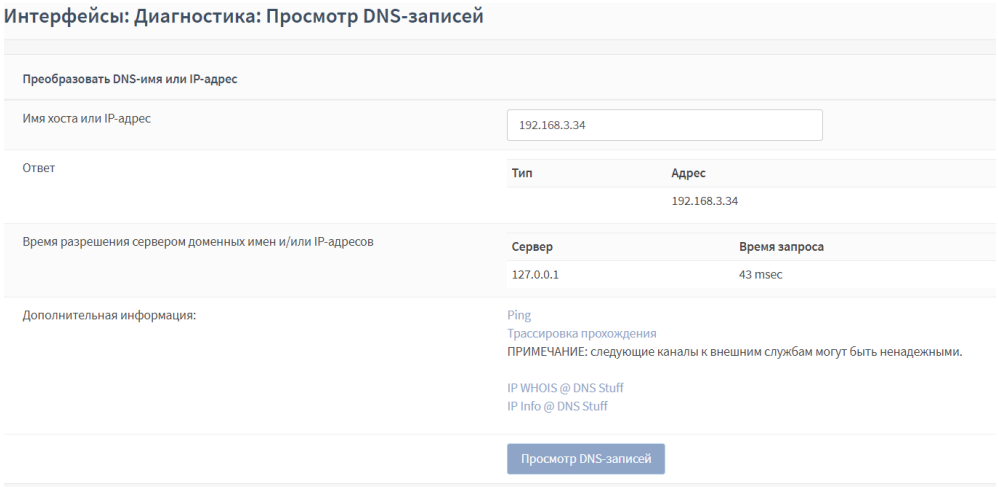


Рисунок 235 — Интерфейсы: Диагностика: Просмотр DNS-записей

7.6.4. Категория «NDP-таблица»

В категории «NDP-таблица» отображается NDP-таблица, в которой перечислены локально подключенные узлы IPv6, с возможностью удаления данных и обновления, нажав на соответствующие кнопки. Таблица содержит следующие данные (рисунок 236):

– IP-адрес;

– MAC-адрес;

– производитель;

– название физического интерфейса;

– название сетевого интерфейса.

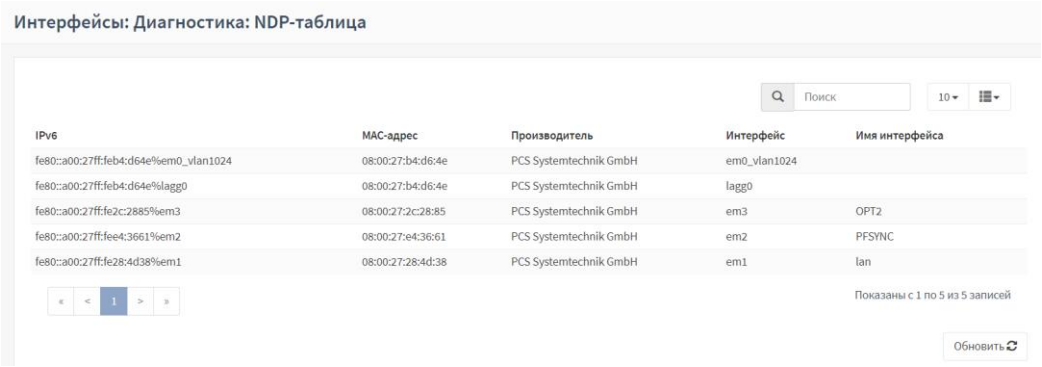


Рисунок 236 — Интерфейсы: Диагностика: NDP-таблица

7.6.5.Категория «Захват пакетов»

Категория «Захват пакетов» позволяет запустить сканирование сети с возможностью дальнейшего экспорта по выбранному интерфейсу.

Для этого 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 (рисунок 237).

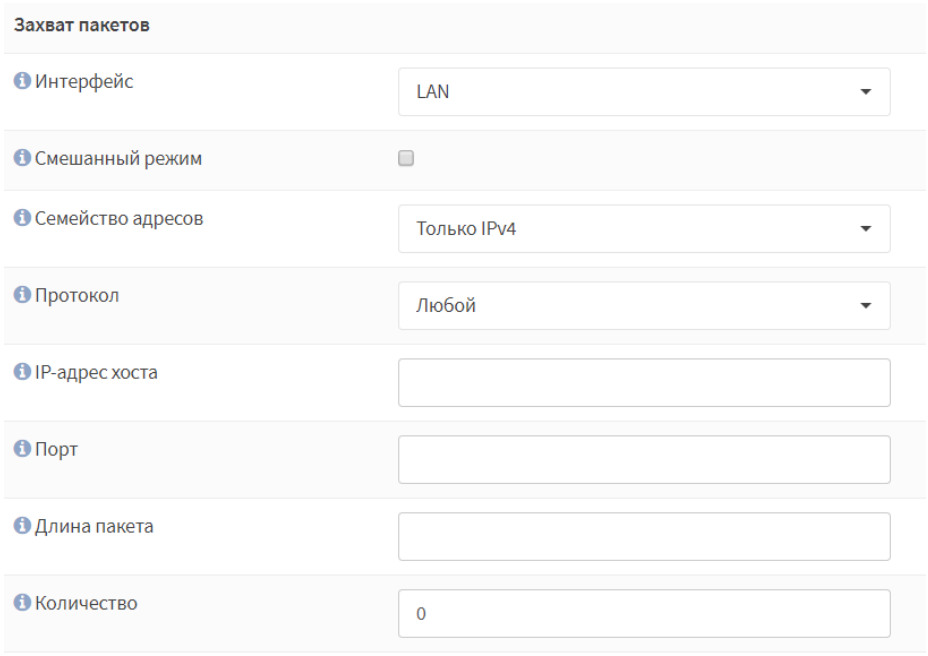


Рисунок 237 — Интерфейсы: Диагностика: Захват пакетов (настройка захвата пакетов)

В группе настроек «Просмотр настроек» в поле «Уровень детализации» необходимо выбрать уровень детализации информации о захваченных пакетах. В поле «Обратный запрос DNS» необходимо установить флажок для захвата пакетов, ассоциируемых со всеми IP-адресами обратного запроса DNS. Для начала захвата необходимо нажать на кнопку «Запустить». Для остановки захвата пакетов необходимо нажать на кнопку «Остановить». Для скачивания захваченных пакетов необходимо нажать на кнопку «Скачать захваченные пакеты». Для удаления захваченных пакетов необходимо нажать на кнопку «Удалить захваченные пакеты». Для просмотра захваченных пакетов необходимо нажать на кнопку «Просмотр захваченных пакетов», появится таблица с результатами захвата пакетов (рисунок 238).

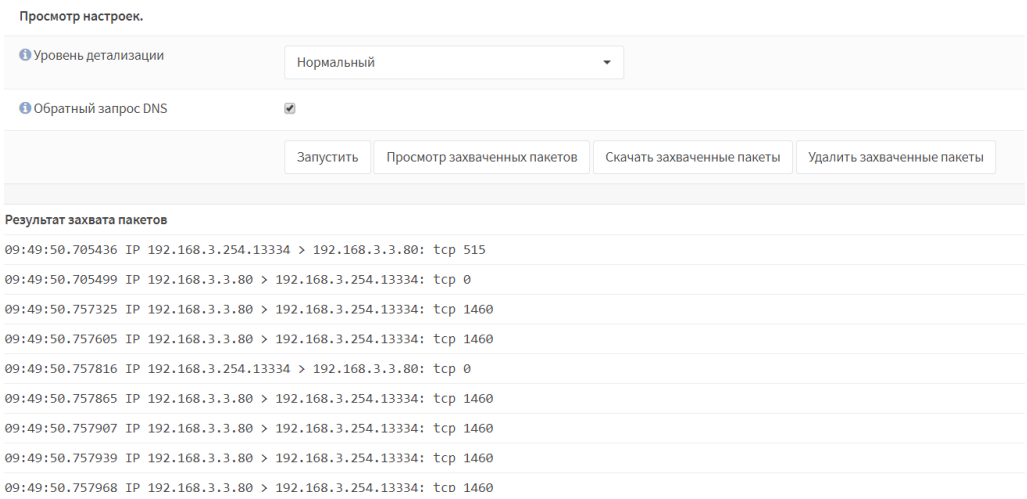


Рисунок 238— Интерфейсы: Диагностика: Захват пакетов (настройка просмотра)

7.6.6.Категория «Ping»

Категория «Ping» позволяет выполнить команду «ping», чтобы проверить наличие доступа к устройству. Для этого в поле «Хост» необходимо ввести IP-адрес устройства, наличие доступа к которому надо проверить. В поле «Протокол IP» необходимо ввести версию протокола IP. В поле «IP-адрес источника» необходимо выбрать IP-адрес источника. В поле «Количество» необходимо выбрать количество отсылаемых пакетов. Необходимо нажать на кнопку «Ping» (рисунок 239).

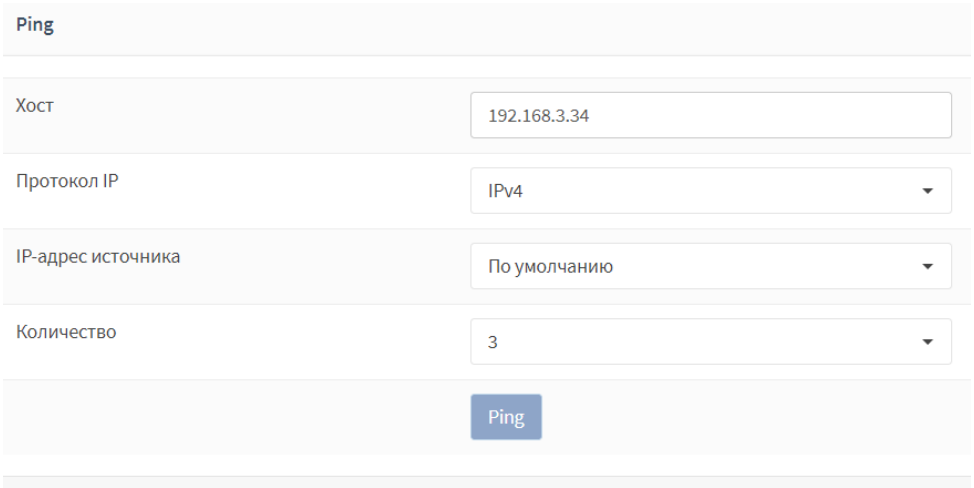


Рисунок 239 — Интерфейсы: Диагностика: Ping

Результат команды ping будет показан внизу страницы (рисунок 240).

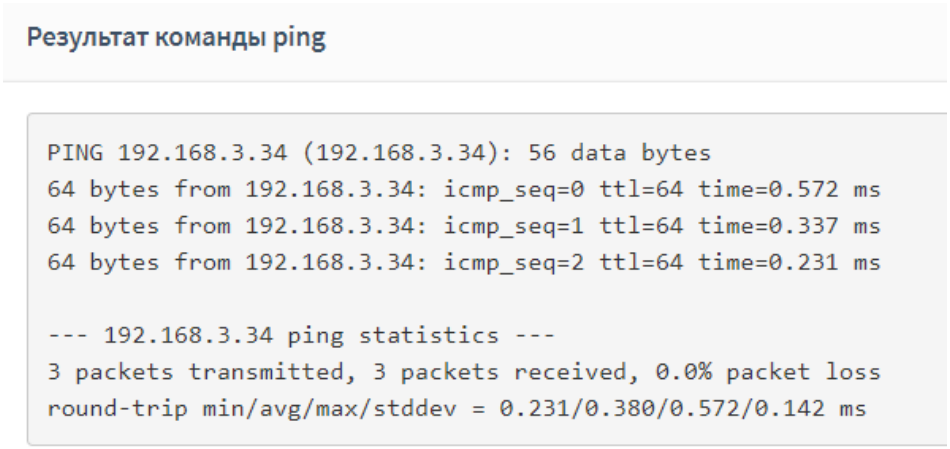


Рисунок 240 — Интерфейсы: Диагностика: Ping (результаты работы команды)

7.6.7. Категория «Проверка порта»

Категория «Проверка порта» позволяет выполнить простой тест соединения TCP, чтобы определить, работает ли и принимает ли хост соединения на данном порте. Этот тест не работает для UDP, потому что нет никакого способа надежно определить, принимает ли порт UDP-соединение этим способом.

Для проверки порта в поле «Протокол IP» необходимо выбрать версию протокола IP. В поле «Хост» необходимо ввести адрес хоста. В поле «Порт» необходимо ввести порт. В поле «Порт отправителя» необходимо ввести порт отправителя. В поле «Показать текст с удаленного сервера» необходимо установить флажок для того, чтобы показать текст, полученный от сервера при попытке подключиться к порту. В поле «IP-адрес источника» необходимо ввести IP-адрес источника и необходимо нажать на кнопку «Проверка» (рисунок 241).

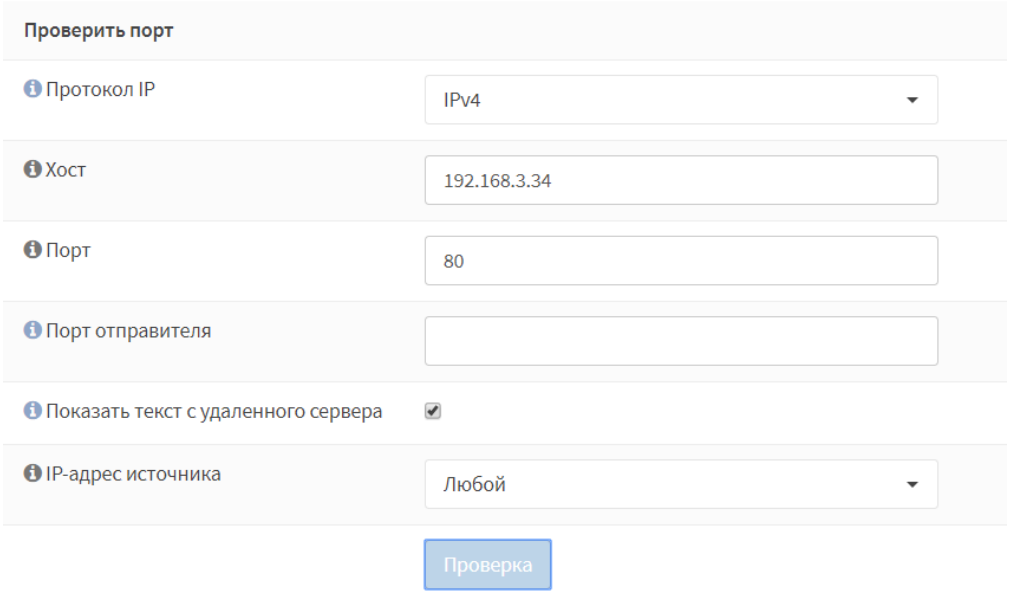


Рисунок 241 — Интерфейсы: Диагностика: Проверка порта

Результат проверки порта будет показан внизу страницы (рисунок 242).

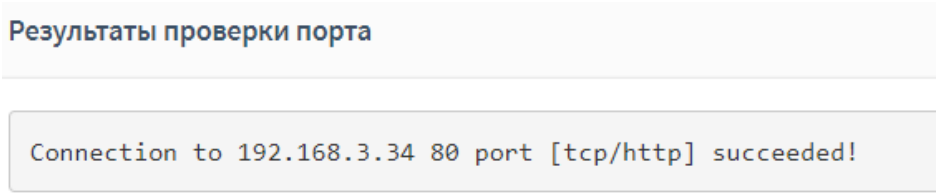


Рисунок 242 — Интерфейсы: Диагностика: Проверка порта (результат)

7.6.8. Категория «Trace Route»

Категория «Trace Route» позволяет выполнить команду trace route. Для этого в поле «Хост» необходимо ввести хост. В поле «Протокол IP» необходимо выбрать версию протокола IP. В поле «IP-адрес источника» необходимо выбрать IP-адрес источника. В поле «Максимальное количество переходов» необходимо выбрать максимальное количество переходов. В поле «Обратное преобразование адресов» необходимо установить флажок для обратного преобразования адресов. В поле «Использовать ICMP» необходимо установить флажок для использования протокола ICMP. Необходимо нажать на кнопку «Трассировка прохождения» (рисунок 243).

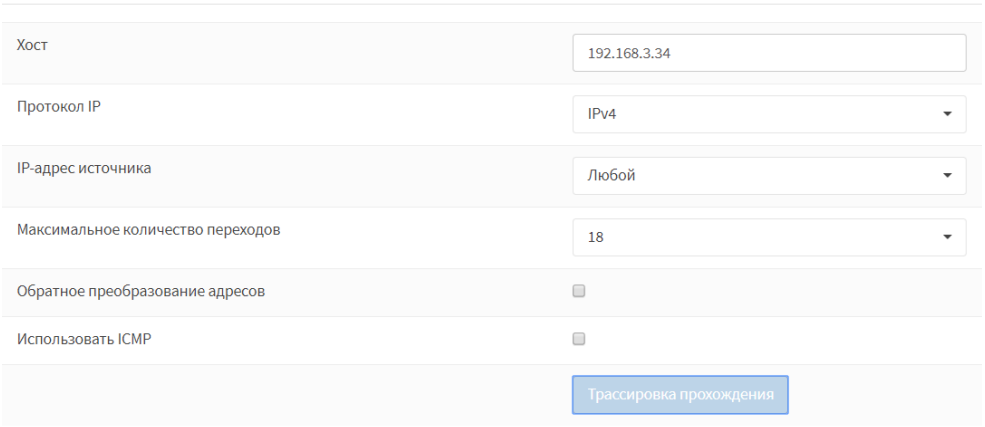


Рисунок 243 — Интерфейсы: Диагностика: Trace Route

Результат выполнения команды Trace Route будет показан внизу страницы (рисунок 244).

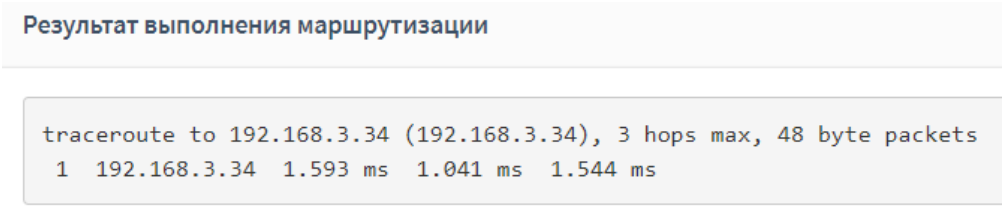


Рисунок 244 — Интерфейсы: Диагностика: Trace Route (результат)

8. Раздел «Сеть»

Раздел «Сеть» позволяет анализировать дампы трафика на выбранных интерфейсах с помощью ПО TShark, просматривать доступные устройства с помощью ARPWatch для выбранных интерфейсов.

8.1. Подраздел «Обнаружение устройств»

Подраздел «Обнаружение устройств» позволяет просматривать таблицу подключенный устройств на выбранном сетевом интерфейсе.

8.1.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет включить ARPwatch сервис и выбрать прослушиваемый сетевой интерфейс. В «Включен» необходимо поставить флажок для включения ARPwatch сервиса. В поле «Прослушиваемые интерфейсы» необходимо выбрать сетевые интерфейсы, которые необходимо прослушивать. Для сохранения настроек необходимо нажать кнопку «Сохранить» (рисунок 245).

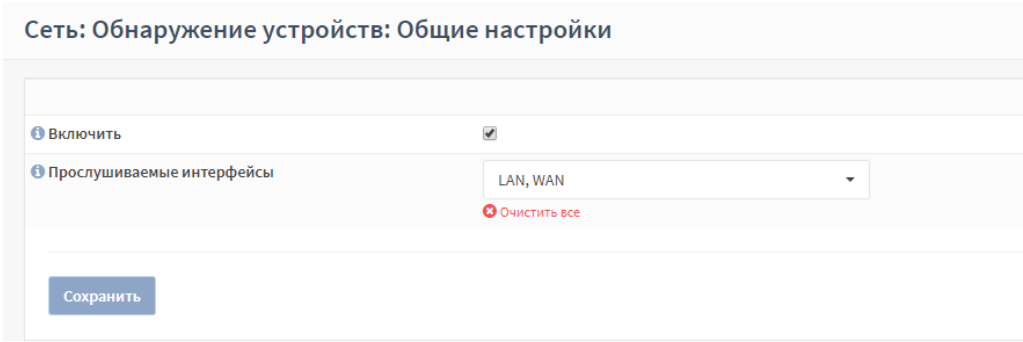


Рисунок 245 — Сеть: Обнаружение устройств: Общие настройки

8.1.2. Категория «Хосты»

В категории «Хосты» отображаются подключаемые устройства в виде таблицы на выбранном сетевом интерфейсе. Таблица содержит следующие данные (рисунок 246):

– название физического интерфейса;

– MAC-адрес устройства;

– IP-адрес устройства;
– дата/время обнаружения устройства;
– состояние устройства (зарегистрировано/не зарегистрировано);
– комментарий;
– хост;
– действия.

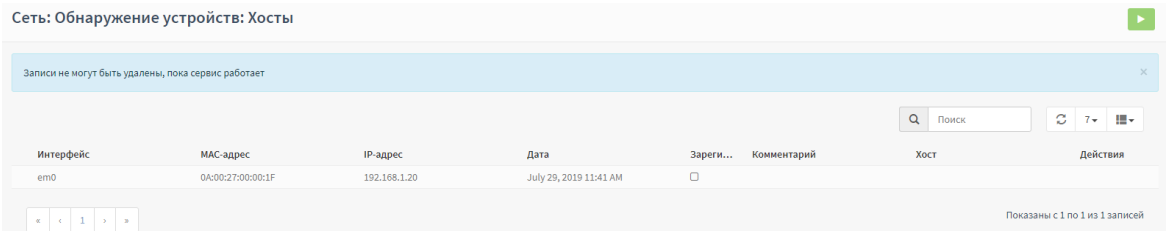


Рисунок 246— Сеть: Обнаружение устройств: Хосты (при включенном ARPwatch сервисе)

Для редактирования/удаления устройства из таблицы необходимо отключить ARPwatch сервис. Для этого необходимо перейти в «Сеть» - «Обнаружение устройств» - «Общие настройки» и в «Включен» убрать флажок. Нажать кнопку «Сохранить» для сохранения внесенных изменений. На странице «Сеть» - «Обнаружение устройств» - «Хосты» появится возможность редактировать/удалять устройства (рисунок 247).

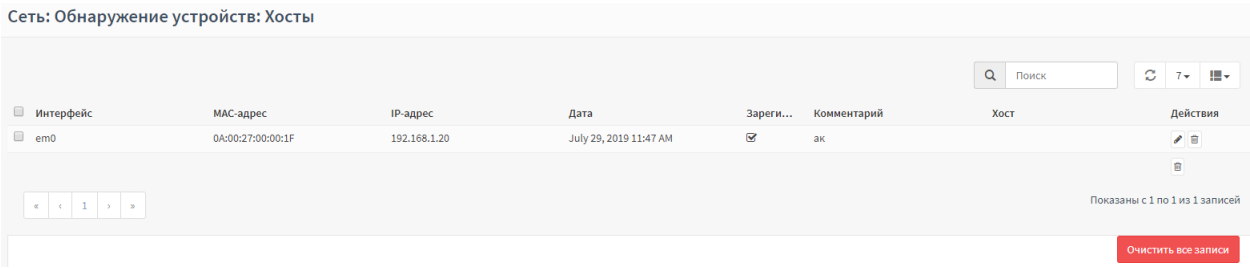


Рисунок 247 — Сеть: Обнаружение устройств: Хосты (при выключенном ARPwatch сервисе)

Для удаления устройства необходимо нажать на кнопку напротив устройства. Для удаления нескольких устройств необходимо поставить флажок напротив устройств в правом столбце таблицы и нажать кнопку

внизу таблицы. Для удаления всех записей таблицы необходимо нажать кнопку 

внизу страницы.

Для редактирования устройства необходимо нажать на кнопку  напротив устройства. В окне редактирования хоста необходимо поставить флажок в «Зарегистрировано» для регистрации устройства. В поле «Комментарий» необходимо ввести описание устройства. Для сохранения необходимо нажать на кнопку «Сохранить».

8.2. Подраздел «Анализ трафика»

Подраздел «Анализ трафика» позволяет просматривать и анализировать входящие / исходящие пакеты по выбранному сетевому интерфейсу.

8.2.1. Категория «Журналирование»

Категория «Журналирование» позволяет просматривать захваченный трафик системой обнаружения вторжений в виде таблицы на выбранном интерфейсе, а именно следующую информацию (рисунок 248):

– дата и время;
– IP-адрес отправителя;
– IP-адрес получателя;
– протокол;
– информация о пакете;
– дополнительная информация о трафике.

В поле «Файл не выбран» необходимо выбрать дамп трафика, захваченный системой обнаружения вторжений. Максимальное количество сохраняемых файлов – 20 файлов по 100 Мбайт каждый.

Для включения сбора дампов трафика необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Настройки». В поле «Включить» поставить флажок. В поле «Интерфейсы» выбрать прослушиваемые сетевые интерфейсы. Нажать кнопку «Сохранить».

Также поле «Фильтр отображения» позволяет осуществлять фильтрацию с помощью встроенных интерактивных фильтров. Для применения фильтра необходимо нажать кнопку  .

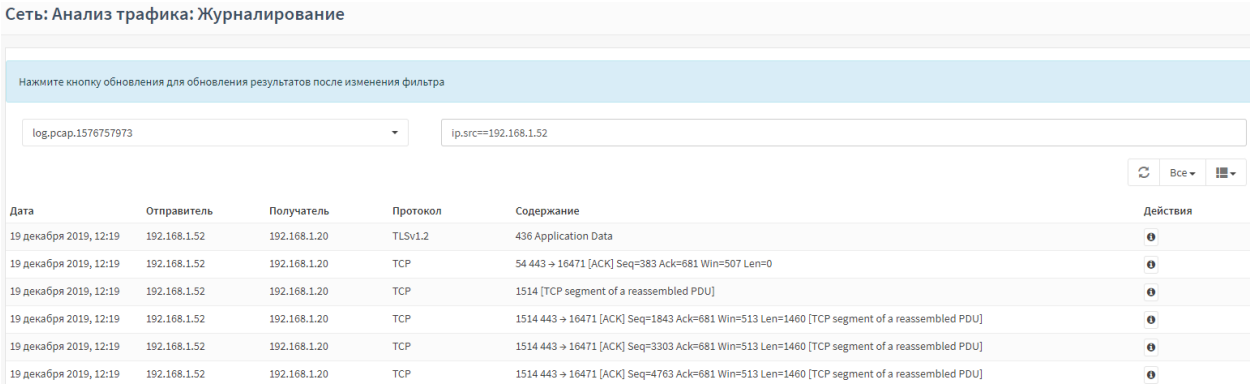


Рисунок 248 — Сеть: Анализ трафика: Журналирование

9. Раздел «Маршрутизация»

Раздел «Маршрутизация» позволяет настраивать динамическую маршрутизацию по следующим протоколам:

– RIP (v1, v2);

– OSPF;

– OSPFv3;

– BGPv4.

А также просматривать информацию о маршрутах по этим протоколам.

9.1. Подраздел «Общие настройки»

Подраздел «Общие настройки» позволяет изменять общие настройки динамической маршрутизации.

В пункте «Включен» необходимо установить флажок для включения динамической маршрутизации. В поле «Создание файла журнала» необходимо установить флажок для записи журнала на диск. В поле «Детализация журнала» необходимо выбрать уровень детализации журнала. В поле «Отправлять сообщения журнала в syslog» необходимо установить флажок для включения отправления событий журнала в syslog. В поле «Детализация журнала для syslog» необходимо выбрать детализацию журнала, который будет направлен в syslog (рисунок 249).

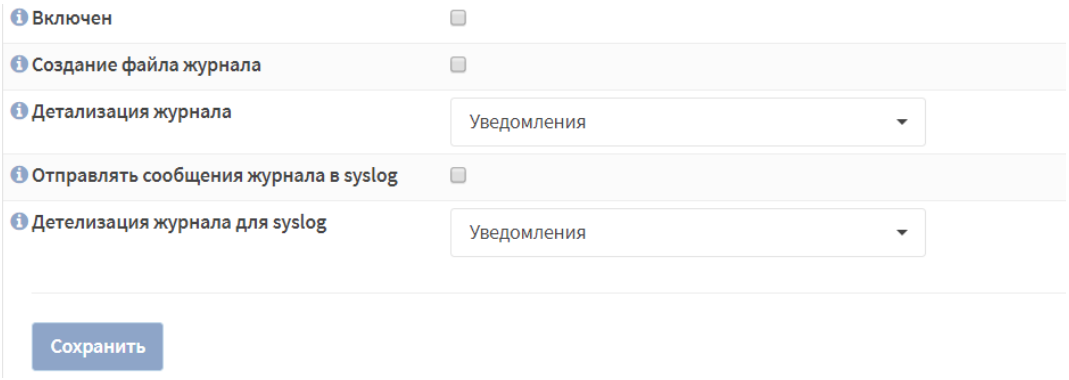


Рисунок 249 — Маршрутизация: Общие настройки

9.2. Подраздел «RIP»

Подраздел «RIP» позволяет настраивать динамическую маршрутизацию по протоколу RIP. В поле «Включен» необходимо установить флажок для включения динамической маршрутизации по протоколу RIP. В поле «Версия» необходимо выбрать версию протокола RIP. В поле «Пассивные интерфейсы» необходимо выбрать интерфейсы, которые не будут использоваться для поиска оптимального маршрута, в поле «Перераспределение маршрута» необходимо выбрать другие источники маршрутизации. В поле «Сети» необходимо ввести сети, которые должны быть известны при построении динамического маршрута. И необходимо нажать на кнопку «Сохранить» (рисунок 250).

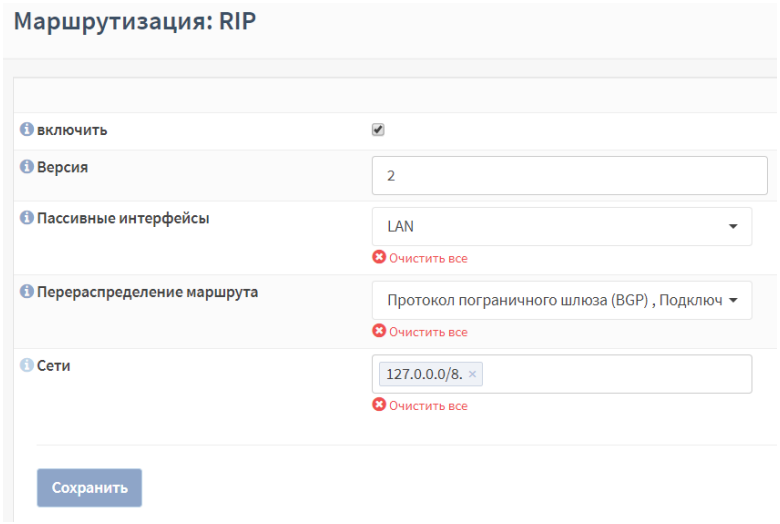


Рисунок 250 — Маршрутизация: RIP

9.3. Подраздел «OSPF»

Подраздел «OSPF» позволяет настраивать динамическую маршрутизацию по протоколу OSPFv2, просматривать в виде таблицы настроенные сети, интерфейсы и список префиксов.

9.3.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет настраивать протокол OSPFv2.

В пункте «Включен» необходимо установить флажок для включения динамической маршрутизации по протоколу OSPFv2. В поле «Идентификатор маршрутизатора» необходимо ввести идентификатор маршрутизатора, если возникают пересечения с настройками CARP. В поле «Пассивные интерфейсы» необходимо выбрать интерфейсы, которые не будут использоваться для поиска оптимального маршрута, в поле «Перераспределение маршрута» необходимо выбрать другие источники маршрутизации. В поле «Объявлять шлюз по умолчанию» необходимо установить флажок для того, чтобы отправить информацию о том, что имеется шлюз по умолчанию. В поле «Всегда объявлять шлюз по умолчанию» необходимо установить флажок для того, чтобы транслировать шлюз по умолчанию. В поле «Объявить метрику шлюза по умолчанию» необходимо ввести метрику шлюза по умолчанию (рисунок 251).

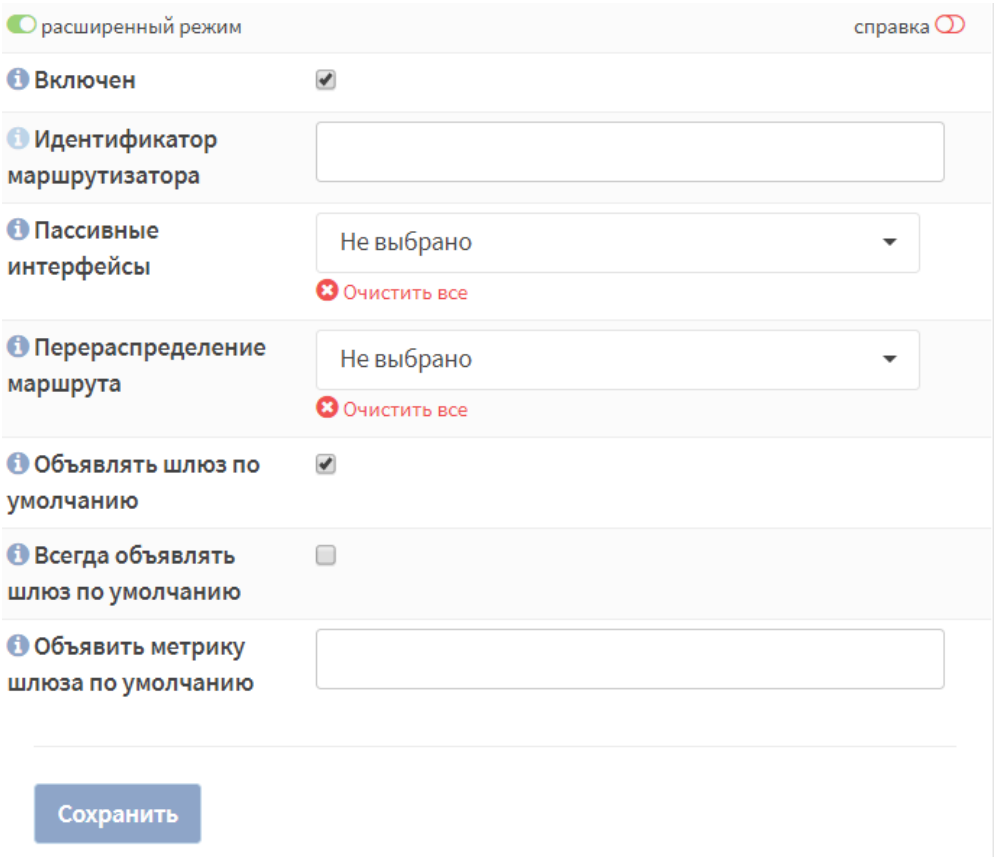


Рисунок 251 — Маршрутизация: OSPFv2: Общие настройки

9.3.2.Категория «Сети»

В категории «Сети» отображается таблица краткого обзора настроенных сетей. Таблица содержит следующие данные (рисунок 252):

– состояние сети (включена/выключена);

– адрес сети;

– маска сети;

– область.

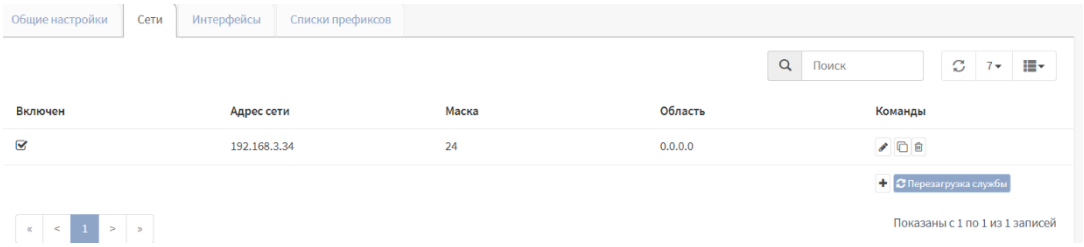


Рисунок 252 — Маршрутизация: OSPFv2: Сети

Для редактирования существующей сети необходимо нажать на кнопку  напротив сети. Для добавления новой сети необходимо нажать на кнопку  .

При редактировании в поле «Включен» необходимо установить флажок для включения сети. В поле «Адрес» необходимо ввести адрес сети. В поле «Маска сети» необходимо ввести маску сети (1-32). В поле «Область» необходимо ввести область сети (то есть какие маршруты принадлежат к той же группе). В поле «Список входящих префиксов» необходимо выбрать список входящих префиксов сети. В поле «Список исходящих префиксов» необходимо выбрать список исходящих префиксов сети (рисунок 253). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

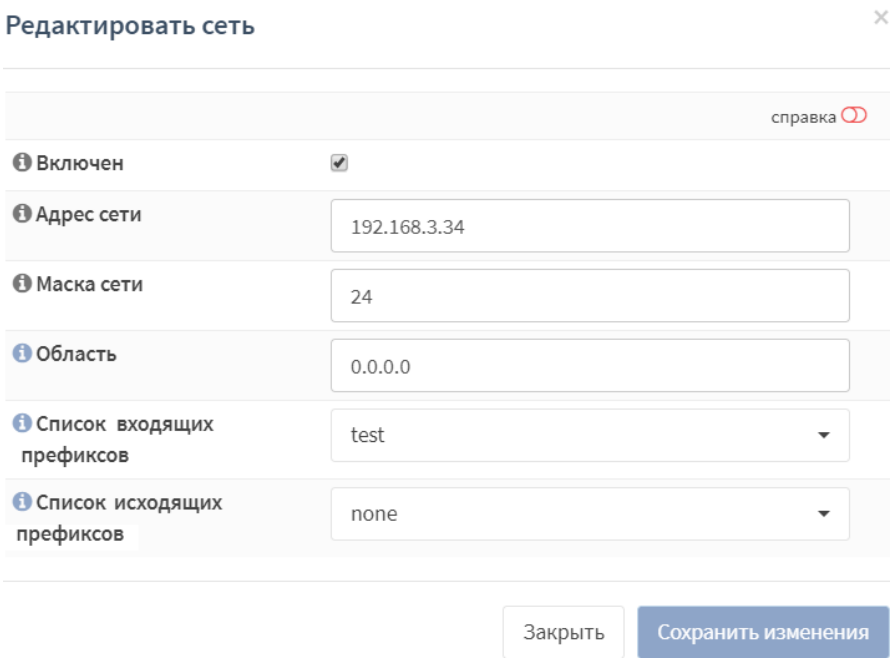


Рисунок 253— Маршрутизация: OSPFv2: Сети (редактирование)

9.3.3.Категория «Интерфейсы»

В категории «Интерфейсы» отображается таблица краткого обзора настроенных интерфейсов. Таблица содержит следующие данные (рисунок 254):

– состояние интерфейса (включена/выключена);
– имя интерфейса;
– тип сети;
– тип аутентификации.

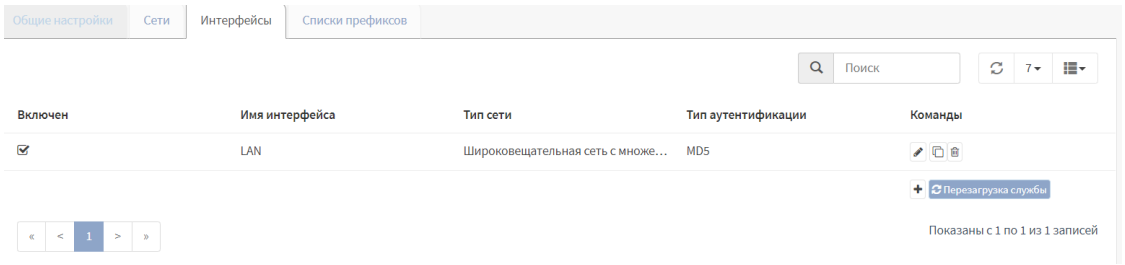


Рисунок 254 — Маршрутизация: OSPFv2: Интерфейсы

Для редактирования существующей интерфейса необходимо нажать на кнопку напротив интерфейса. Для добавления нового интерфейса необходимо нажать на кнопку .

При редактировании в поле «Включен» необходимо установить флажок для включения интерфейса. В поле «Интерфейсы» необходимо выбрать интерфейс, в котором применить эти настройки. В поле «Тип аутентификации» необходимо выбрать тип аутентификации. В поле «Ключ аутентификации» необходимо ввести ключ аутентификации. В поле «Стоимость» необходимо ввести стоимость интерфейса (используется для расчета маршрута). В поле «Интервал приветствия» необходимо ввести интервал, в течение которого отправляются пакеты приветствия. В поле «Мертвое время» необходимо ввести интервал времени, в течение которого интерфейс должен принять эти пакеты. В поле «Интервал повторной передачи» необходимо ввести интервал повторной передачи. В поле «Пауза повторной передачи» необходимо ввести интервал паузы повторной передачи. В поле «Приоритет» необходимо ввести приоритет интерфейса (чем больше приоритет, тем более вероятно, что этот интерфейс будет назначен в динамическом маршруте. В поле «Тип сети» необходимо выбрать тип сети (рисунок 255). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

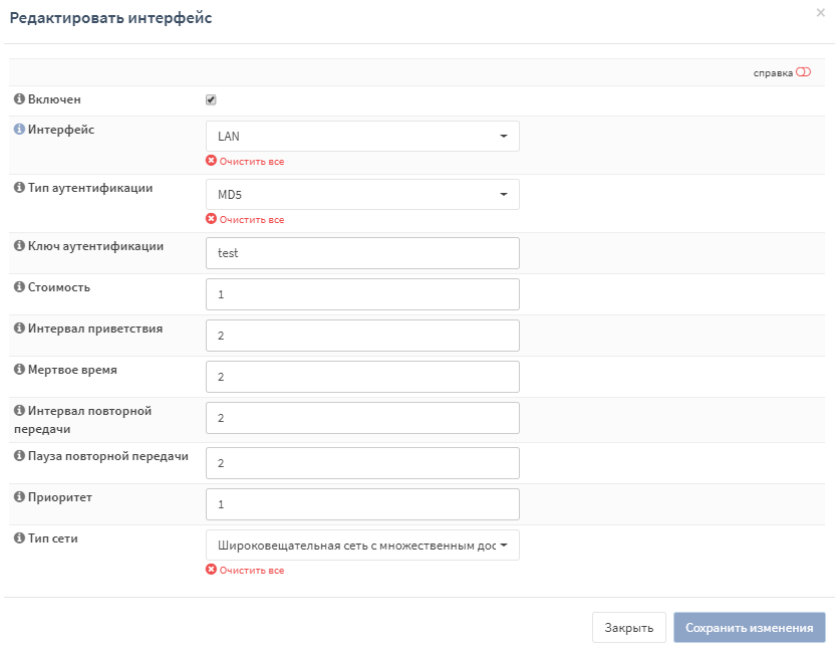


Рисунок 255 — Маршрутизация: OSPFv2: Интерфейсы (редактирование)

9.3.4. Категория «Список префиксов»

В категории «Список префиксов» отображается таблица краткого обзора настроенных списков префиксов. Таблица содержит следующие данные (рисунок 256):

– состояние сети (включена/выключена);
– название списка префиксов;
– порядковый номер;
– действие;
– адрес сети.

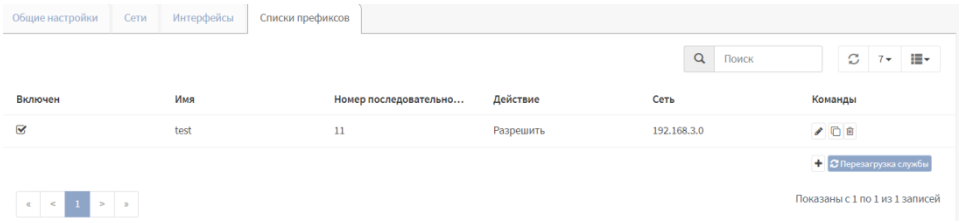


Рисунок 256 — Маршрутизация: OSPFv2: Список префиксов

Для редактирования существующих списков префиксов необходимо нажать на кнопку напротив списка. Для добавления нового списка необходимо нажать на кнопку .

При редактировании в поле «Включен» необходимо установить флажок для включения списка префиксов. В поле «Имя» необходимо ввести название списка. В поле «Номер» необходимо ввести порядковый номер списка (10-99). В поле «Действие» необходимо выбрать действие для разрешения или блокирования правил. В поле «Сеть» необходимо ввести шаблон сети для поиска (рисунок 257). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

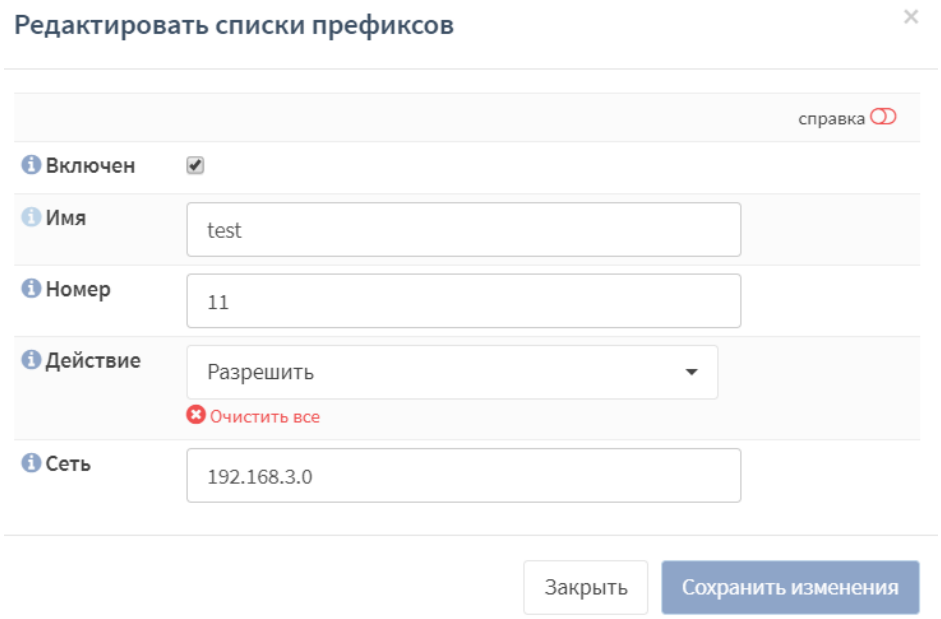


Рисунок 257 — Маршрутизация: OSPFv2: Список префиксов (редактирование)

9.4. Подраздел «OSPFv3»

Подраздел «OSPFv3» позволяет настраивать динамическую маршрутизацию по протоколу OSPFv3, просматривать в виде таблицы настроенные интерфейсы.

9.4.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет настраивать протокол OSPFv3.

В пункте «Включен» необходимо установить флажок для включения динамической маршрутизации по протоколу OSPFv2. В поле «ID роутера» необходимо ввести идентификатор маршрутизатора, если возникают пересечения с настройками CARP. В поле «Перераспределение маршрута» необходимо выбрать другие источники маршрутизации (рисунок 258).

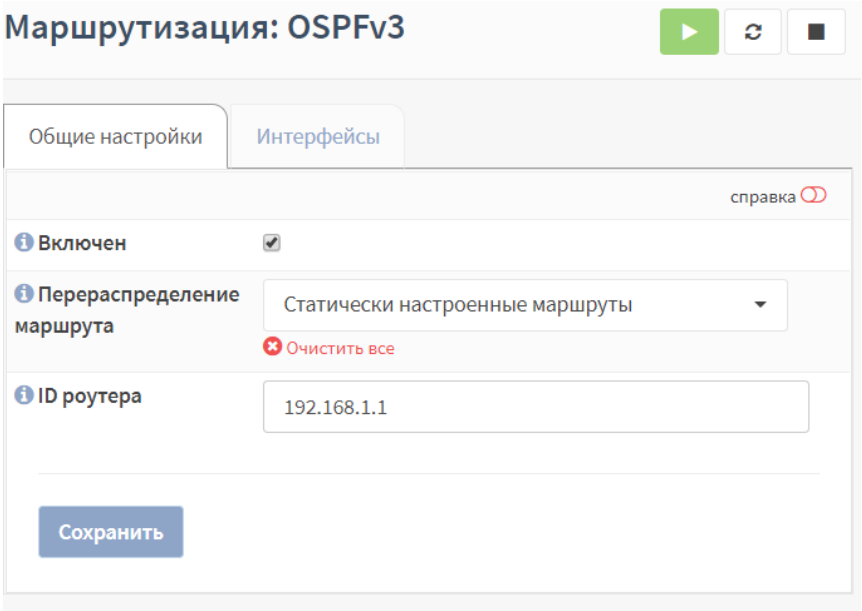


Рисунок 258 — Маршрутизация: OSPFv3: Общие настройки

9.4.2.Категория «Интерфейсы»

В категории «Интерфейсы» отображается таблица краткого обзора настроенных интерфейсов. Таблица содержит следующие данные (рисунок 259):

– состояние интерфейса (включена/выключена);

– имя интерфейса;

– тип сети.

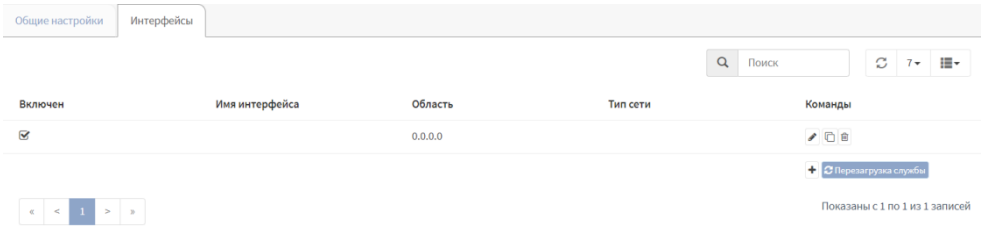


Рисунок 259 — Маршрутизация: OSPFv3: Интерфейсы

Для редактирования существующей интерфейса необходимо нажать на кнопку напротив интерфейса. Для добавления нового интерфейса необходимо нажать на кнопку .

При редактировании в поле «Включен» необходимо установить флажок для включения интерфейса. В поле «Интерфейсы» необходимо выбрать

интерфейс, в котором применить эти настройки. В поле «Область» необходимо ввести область (то есть какие маршруты принадлежат к той же группе). В поле «Стоимость» необходимо ввести стоимость интерфейса (используется для расчета маршрута). В поле «Интервал приветствия» необходимо ввести интервал, в течение которого отправляются пакеты приветствия. В поле «Мертвое время» необходимо ввести интервал времени, в течение которого интерфейс должен принять эти пакеты. В поле «Интервал повторной передачи» необходимо ввести интервал повторной передачи. В поле «Пауза повторной передачи» необходимо ввести интервал паузы повторной передачи. В поле «Приоритет» необходимо ввести приоритет интерфейса (чем больше приоритет, тем более вероятно, что этот интерфейс будет назначен в динамическом маршруте). В поле «Тип сети» необходимо выбрать тип сети (рисунок 260). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

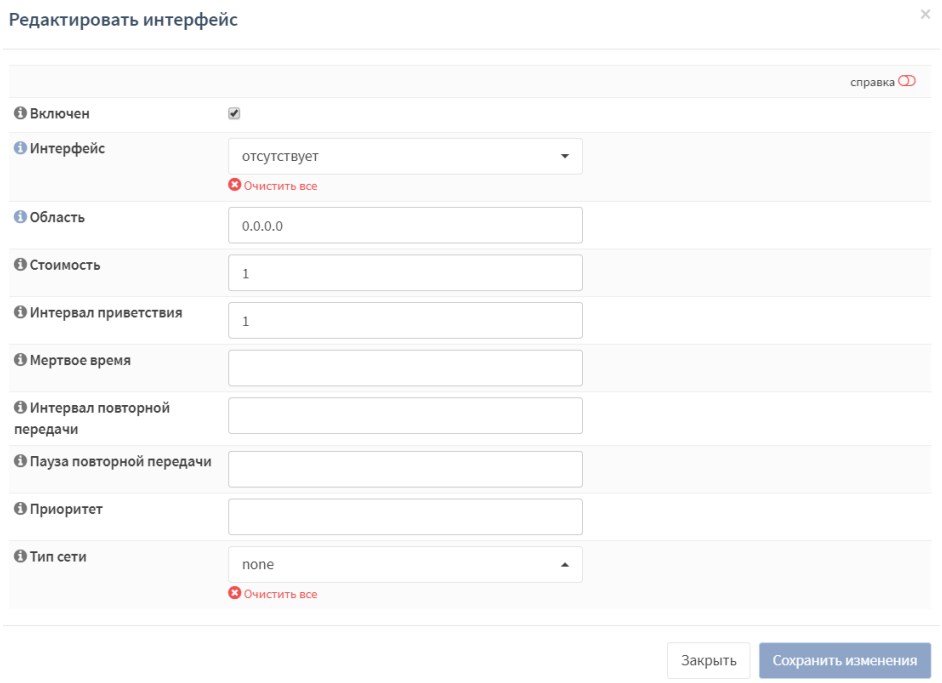


Рисунок 260 — Маршрутизация: OSPFv3: Интерфейсы (редактирование)

9.5. Подраздел «BGPv4»

Подраздел «BGPv4» позволяет настраивать динамическую маршрутизацию по протоколу BGPv4, просматривать в виде таблицы

настроенные соседние AS, списки AS путей и префиксов, и карты маршрутов.

9.5.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет настраивать протокол BGPv4.

В пункте «Включен» необходимо установить флажок для включения динамической маршрутизации по протоколу BGPv4. В поле «Номер BGP AS» необходимо ввести номер AS. В поле «Сеть» необходимо выбрать сеть оповещений. В поле «Переопределение маршрута» необходимо выбрать другие источники маршрутов, которые должны быть известны узлам (рисунок 261). После внесения изменений необходимо нажать на кнопку «Сохранить».

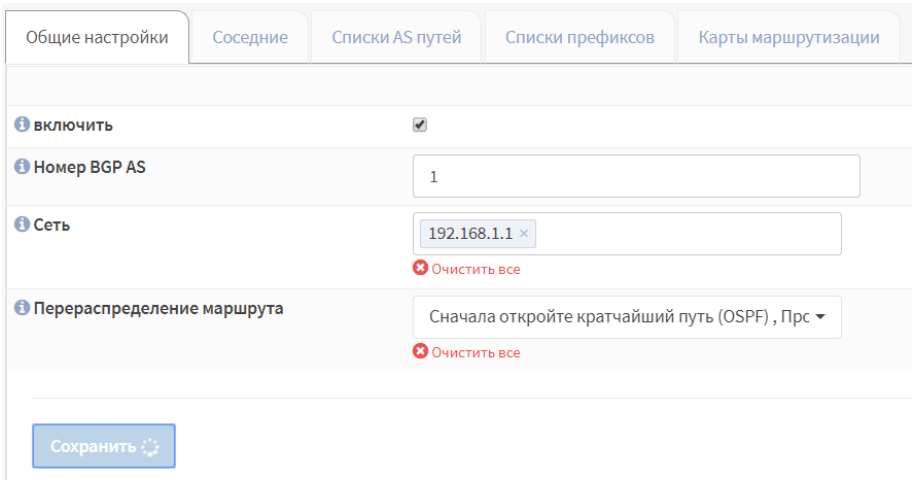


Рисунок 261 — Маршрутизация: BGPv4: Общие настройки

9.5.2. Категория «Соседние»

В категории «Соседние» отображается таблица краткого обзора настроенных соседей автономной системы. Таблица содержит следующие данные (рисунок 262):

- состояние соседей (включена/выключена);
- адрес соседней сети;
- соседний AS;
- интерфейс-источник обновлений;
- IP-адрес следующей AS (учитывать/не учитывать);

– маршрут по умолчанию (посылать/не посылать);
– список входящих/исходящих префиксов;
– карта входящих/исходящих маршрутов.

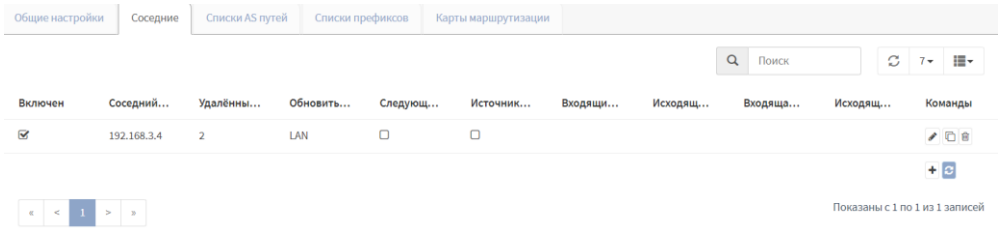


Рисунок 262 — Маршрутизация: BGPv4: Соседние

Для редактирования существующих соседей необходимо нажать на кнопку  напротив соседа. Для добавления нового соседа необходимо нажать на кнопку  .

При редактировании в поле «Включен» необходимо установить флажок для включения соседа. В поле «IP пира» необходимо ввести IP-адрес соседа. В поле «Удаленный AS» необходимо ввести соседний AS. В поле «Интерфейс-источник обновлений» необходимо выбрать физических интерфейс, который обращается к IP-адресу соседа. В поле «Next-Hop-Self» необходимо установить флажок для учитывать IP-адрес следующей AS. В поле «Посылать маршрут по умолчанию» необходимо установить флажок для того, чтобы посылать маршрут по умолчанию. В поле «Список префиксов входящих» необходимо выбрать список входящих префиксов. В поле «Список префиксов входящих» необходимо выбрать список входящих префиксов. В поле «Список префиксов исходящих» необходимо выбрать список исходящих префиксов. В поле «Карта маршрутов входящих» необходимо выбрать карту входящих маршрутов. В поле «Карта маршрутов исходящих» необходимо выбрать карту исходящих маршрутов (рисунок 263). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

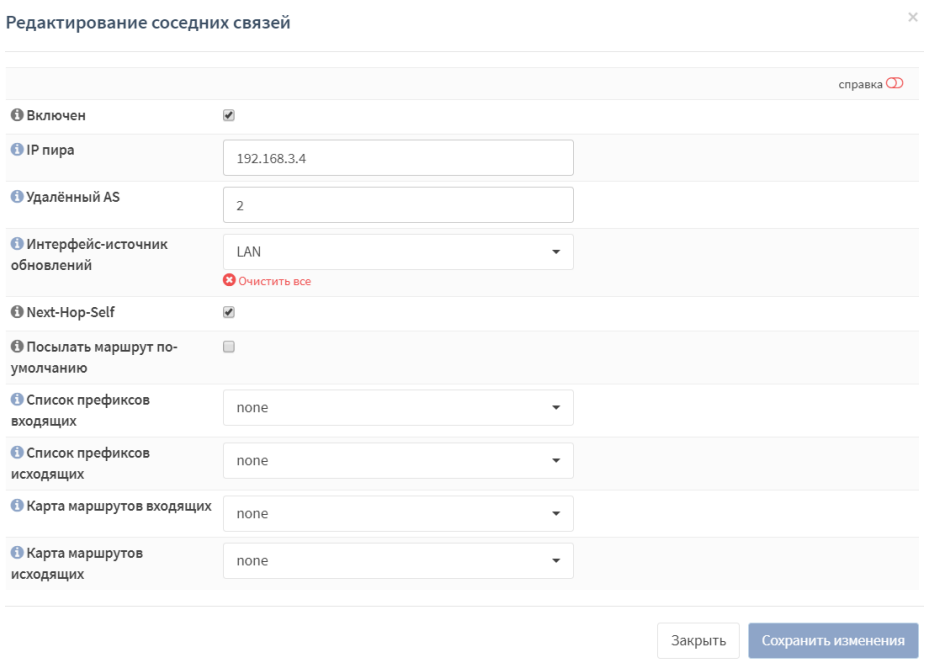


Рисунок 263 — Маршрутизация: BGPv4: Соседние (редактирование)

9.5.3. Категория «Список AS путей»

В категории «Список AS путей» отображается таблица краткого обзора настроенных списков AS путей. Таблица содержит следующие данные (рисунок 264):

– состояние интерфейса (включена/выключена);
– номер правила ACL;
– действие (правила);
– номер AS.

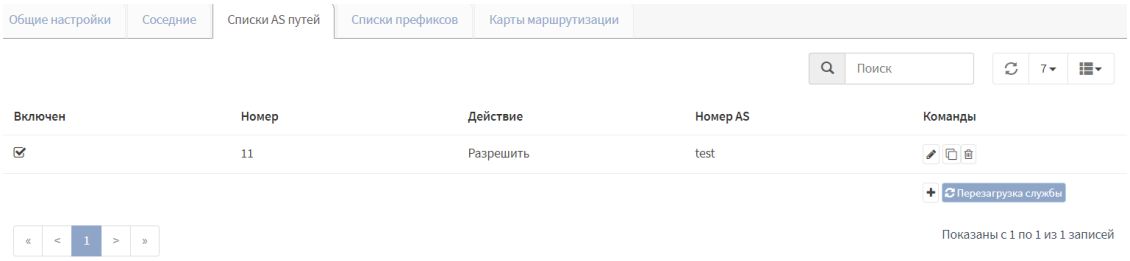


Рисунок 264 — Маршрутизация: BGPv4: Список AS путей

Для редактирования существующих списков AS путей необходимо нажать на кнопку  напротив списка AS путей. Для добавления нового списка AS путей необходимо нажать на кнопку  .

При редактировании в поле «Включен» необходимо установить флажок для включения списка. В поле «Номер» необходимо ввести номер правила ACL. В поле «Действие» необходимо выбрать действие правила (разрешить действие правила или запретить действие правила). В поле AS необходимо ввести шаблон AS для поиска (рисунок 265). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

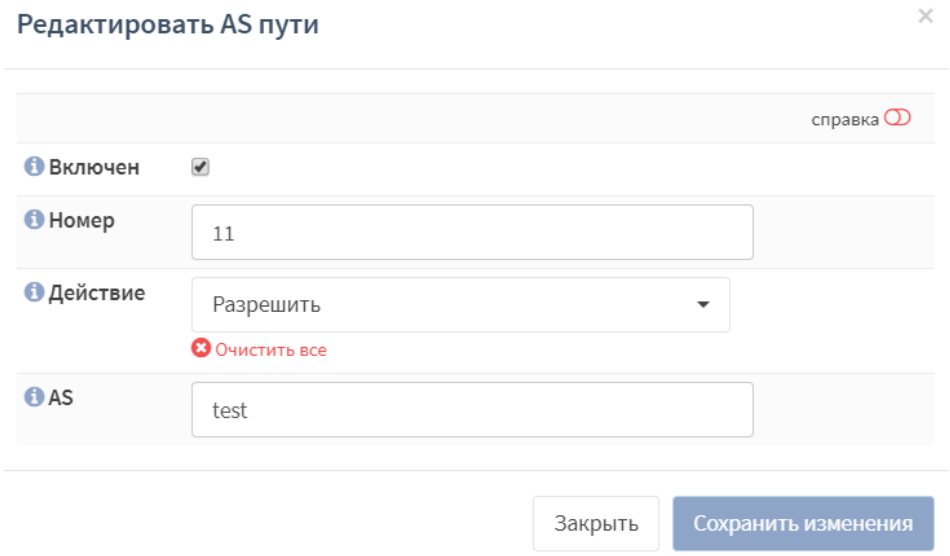


Рисунок 265 — Маршрутизация: BGPv4: Список AS путей (редактирование)

9.5.4. Категория «Списки префиксов»

В категории «Списки префиксов» отображается таблица краткого обзора настроенных списков префиксов. Таблица содержит следующие данные (рисунок 266).

- состояние сети (включена/выключена);
- название списка префиксов;
- порядковый номер;
- действие;
- адрес сети.

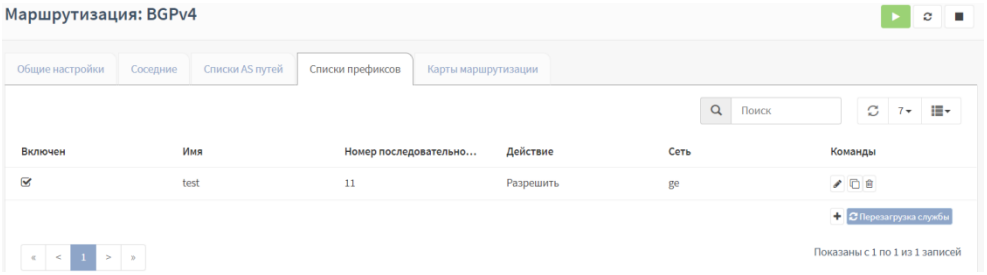


Рисунок 266 — Маршрутизация: BGPv4: Списки префиксов

Для редактирования существующих списков префиксов необходимо нажать на кнопку  напротив списка. Для добавления нового списка необходимо нажать на кнопку  .

При редактировании в поле «Включен» необходимо установить флажок для включения списка. В поле «Имя» необходимо ввести название списка. В поле «Версия IP» необходимо выбрать версию IP протокола. В поле «Номер» необходимо ввести порядковый номер списка (10-99). В поле «Действие» необходимо выбрать действие для разрешения или блокирования правил. В поле «Сеть» необходимо ввести шаблон сети для поиска (рисунок 267). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

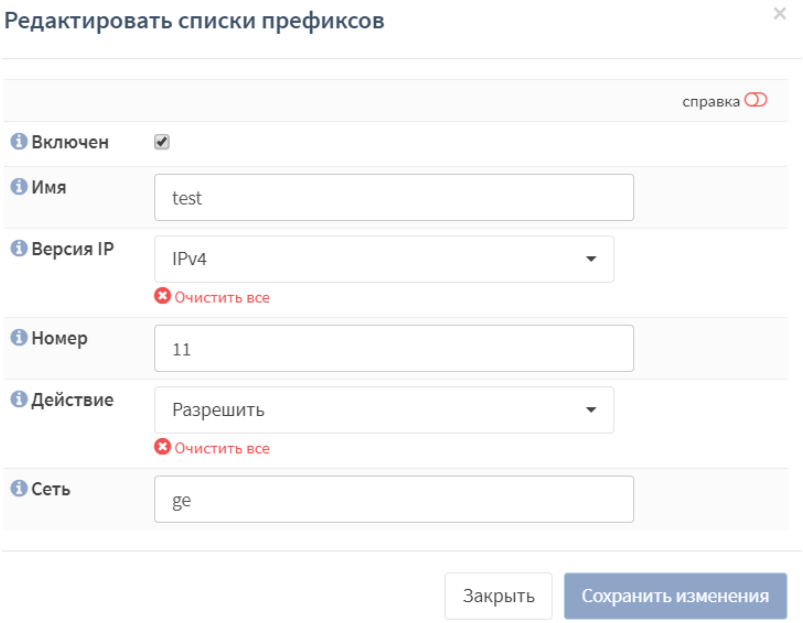


Рисунок 267 — Маршрутизация: BGPv4: Списки префиксов (редактирование)

9.5.5.Категория «Карты маршрутизации»

В категории «Карты маршрутизации» отображается таблица краткого обзора настроенных карт маршрутов. Таблица содержит следующие данные (рисунок 268):

– состояние сети (включена/выключена);

– имя карты маршрутизации;

– действие правила;

– ID карты маршрутов;

– список путей AS;

– установка своего набора.

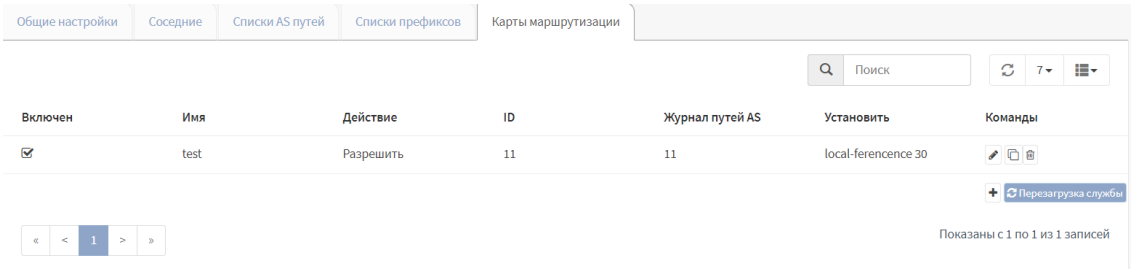


Рисунок 268 — Маршрутизация: BGPv4: Карты маршрутов

Для редактирования существующих карт маршрутов необходимо нажать на кнопку  напротив карты маршрутов. Для добавления новой карты маршрутов необходимо нажать на кнопку  .

При редактировании в поле «Включен» необходимо установить флажок для включения карты маршрутов. В поле «Имя» необходимо ввести название карты маршрутов. В поле «Действие» необходимо выбрать действие для разрешения или блокирования правил. В поле «ID» необходимо ввести ID карты маршрутов. В поле «Список путей AS» необходимо ввести списки AS путей. В поле «Установить» необходимо ввести название набора (рисунок 269). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

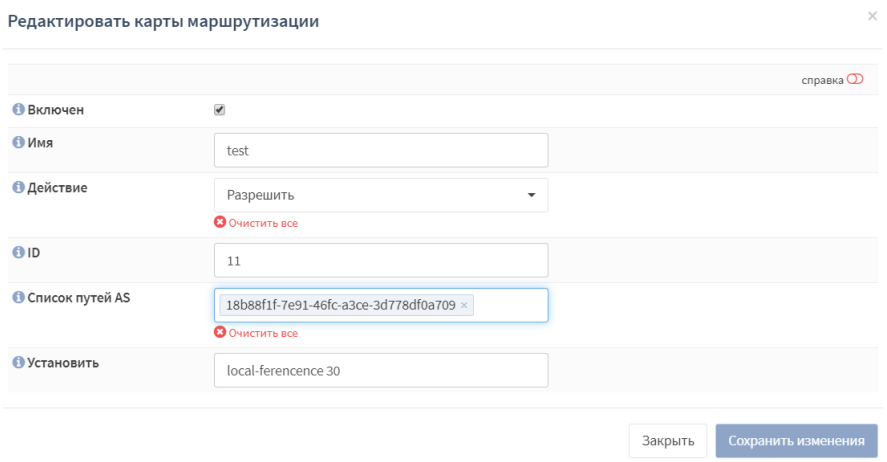


Рисунок 269 — Маршрутизация: BGPv4: Карты маршрутов (редактирование)

9.6. Подраздел «Диагностика»

В подразделе «Диагностика» отображаются данные о настроенных динамических маршрутах по следующим протоколам:

– RIP (v1, v2);

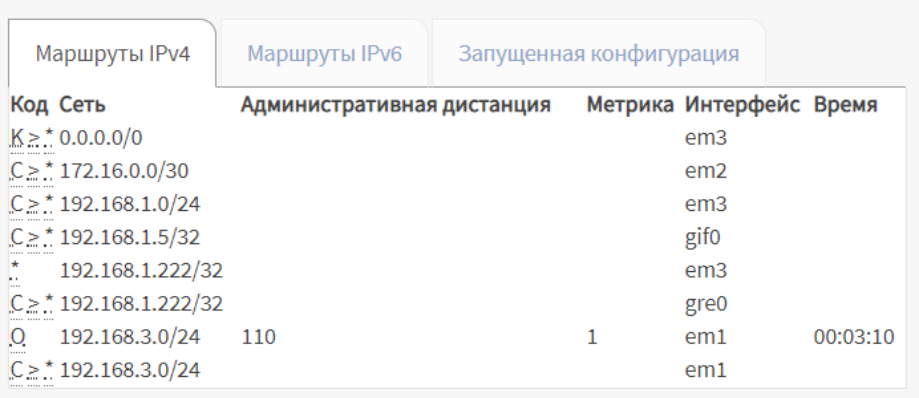
– OSPF;

– OSPFv3;

– BGPv4.

9.6.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет просматривать данные о маршрутах IPv4 (рисунок 270), IPv6 (рисунок 271), а также общую конфигурацию настроенных динамических маршрутов (рисунок 272).



Код	Сеть	Административная дистанция	Метрика	Интерфейс	Время
K>*	0.0.0.0/0			em3	
C>*	172.16.0.0/30			em2	
C>*	192.168.1.0/24			em3	
C>*	192.168.1.5/32			gif0	
*	192.168.1.222/32			em3	
C>*	192.168.1.222/32			gre0	
O	192.168.3.0/24	110	1	em1	00:03:10
C>*	192.168.3.0/24			em1	

Рисунок 270 — Маршрутизация: Диагностика: Общие настройки: Маршруты IPv4

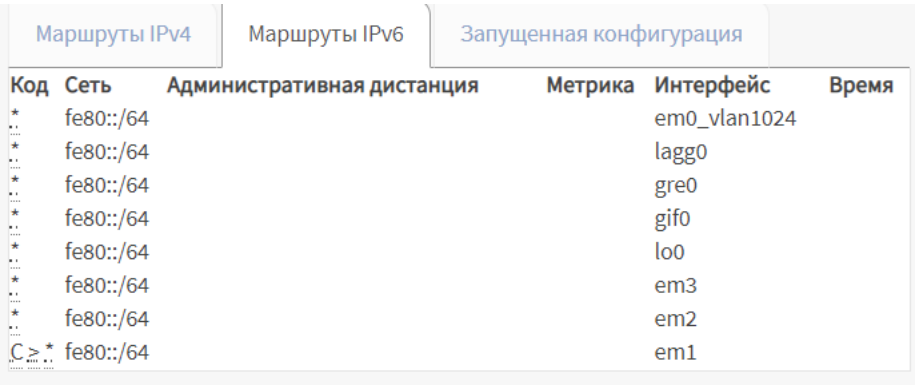


Рисунок 271 — Маршрутизация: Диагностика: Общие настройки: Маршруты IPv6

Рисунок 272 — Маршрутизация: Диагностика: Общие настройки: Запущенная конфигурация

9.6.2.Категория «OSPF»

Категория «OSPF» позволяет просматривать общие данные о настройке динамической маршрутизации по протоколу OSPFv2 (рисунок 273), таблицу

маршрутизации сети/роутера, внешнюю таблицу маршрутизации (рисунок 274), таблицы состояний связи (рисунок 275), таблицу соседей (рисунок 276), данные о настроенных интерфейсах (рисунок 277).

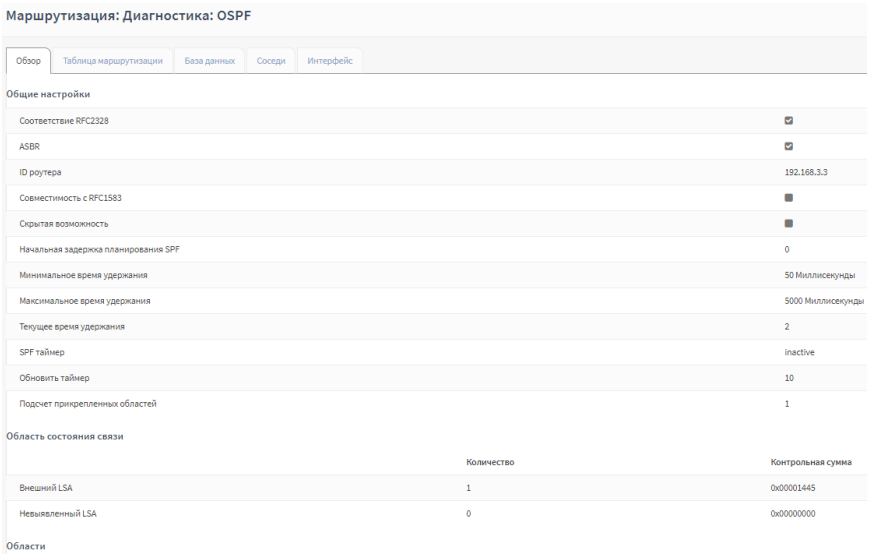


Рисунок 273 — Маршрутизация: Диагностика: OSPF: Обзор

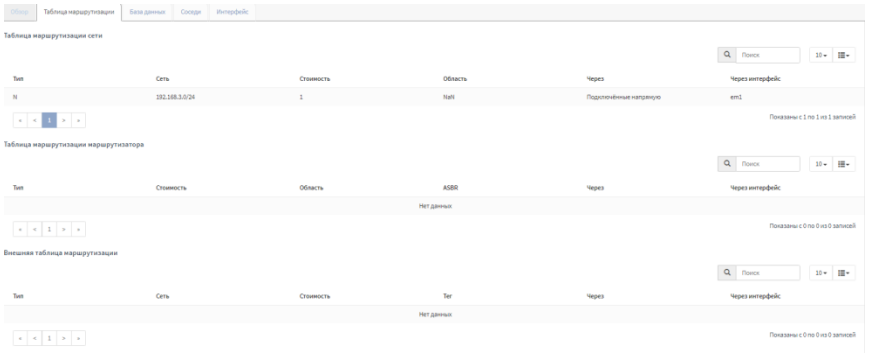


Рисунок 274 — Маршрутизация: Диагностика: OSPF: Таблица маршрутизации

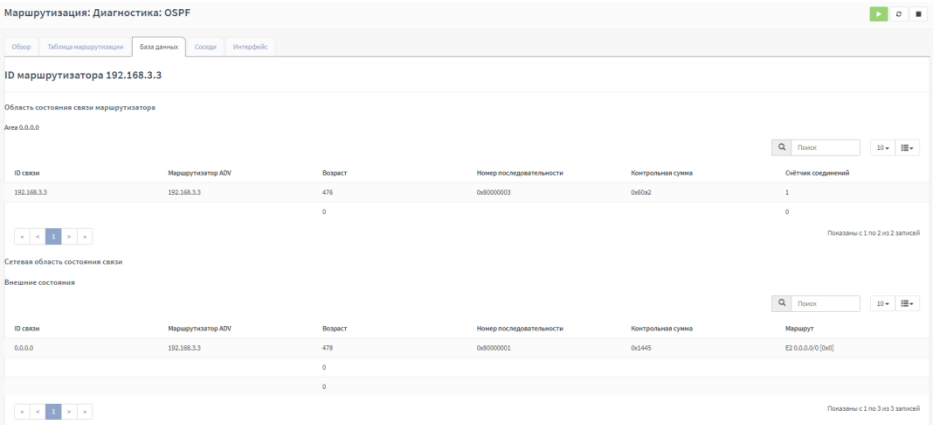


Рисунок 275 — Маршрутизация: Диагностика: OSPF: База данных

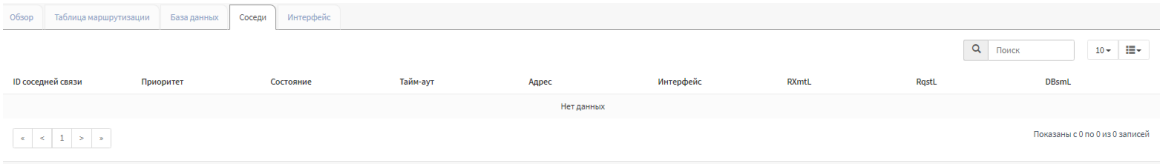


Рисунок 276 — Маршрутизация: Диагностика: OSPF: Соседи

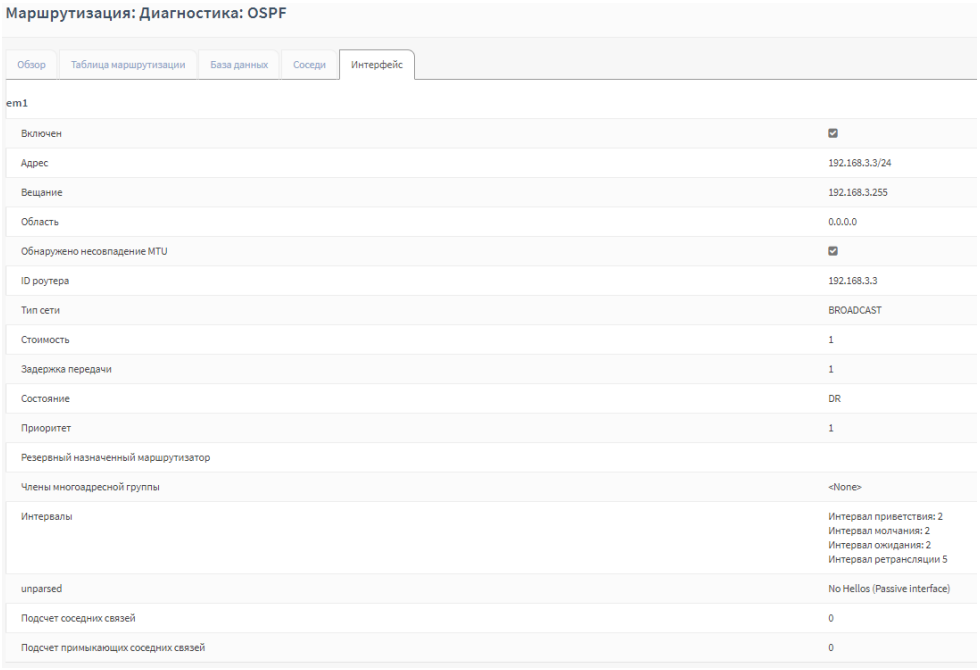


Рисунок 277 — Маршрутизация: Диагностика: OSPF: Интерфейс

9.6.3. Категория «OSPFv3»

Категория «OSPFv3» позволяет просматривать общие данные о настройке динамической маршрутизации по протоколу OSPFv3 (рисунок 278), таблицу маршрутизации сети/роутера, внешнюю таблицу маршрутизации (рисунок 279), таблицы состояний связи (рисунок 280), данные о настроенных интерфейсах (рисунок 281).

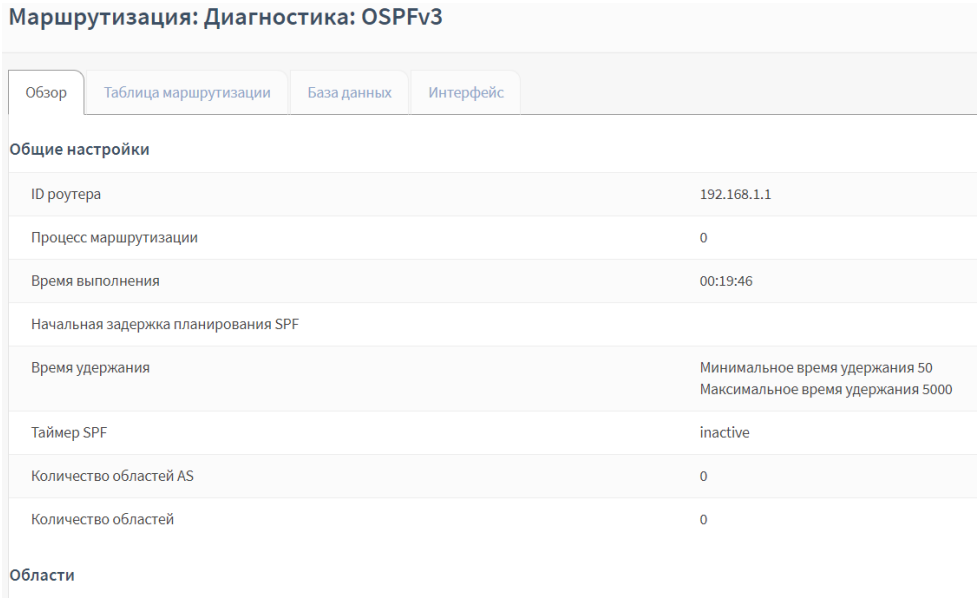


Рисунок 278— Маршрутизация: Диагностика: OSPFv3: Обзор

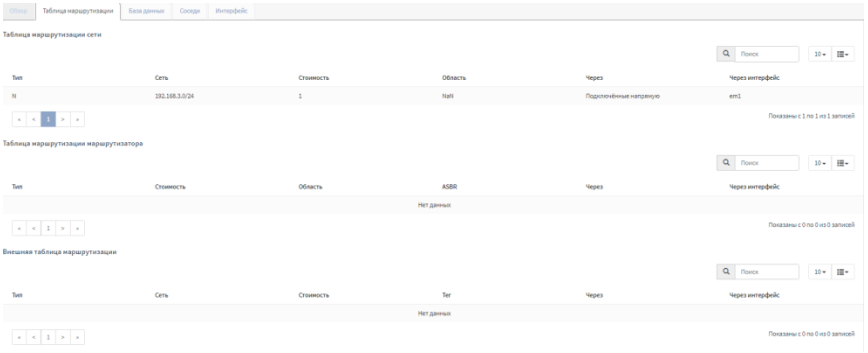


Рисунок 279 — Маршрутизация: Диагностика: OSPFv3: Таблица маршрутизации

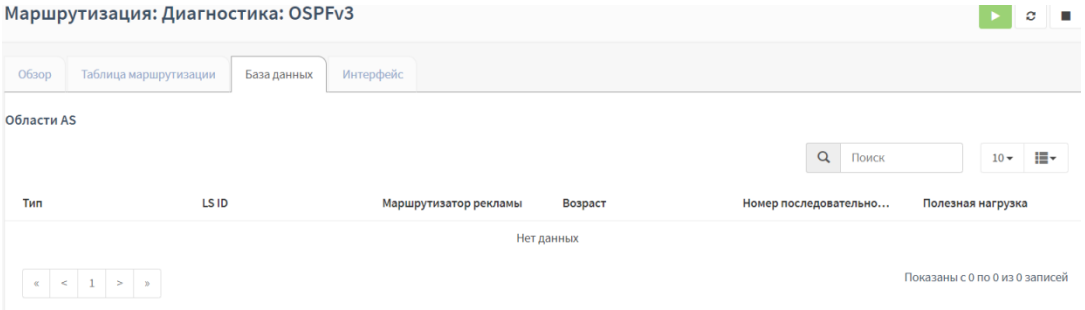


Рисунок 280 — Маршрутизация: Диагностика: OSPFv3: База данных

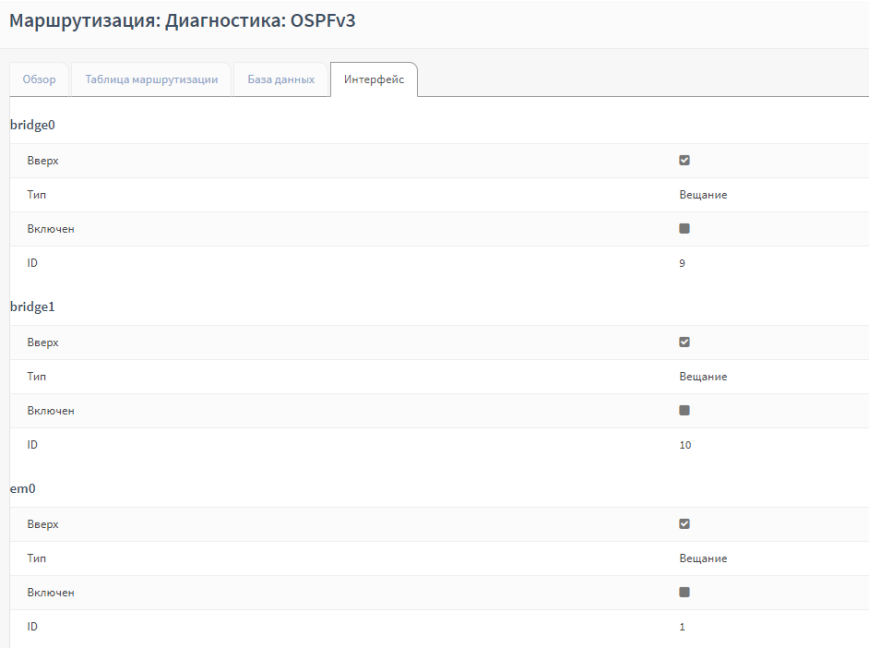


Рисунок 281 — Маршрутизация: Диагностика: OSPFv3: Интерфейс

9.6.4. Категория «BGPv4»

Категория «BGPv4» позволяет просматривать общие данные о настройке динамической маршрутизации по протоколу BGPv4 (рисунок 282).

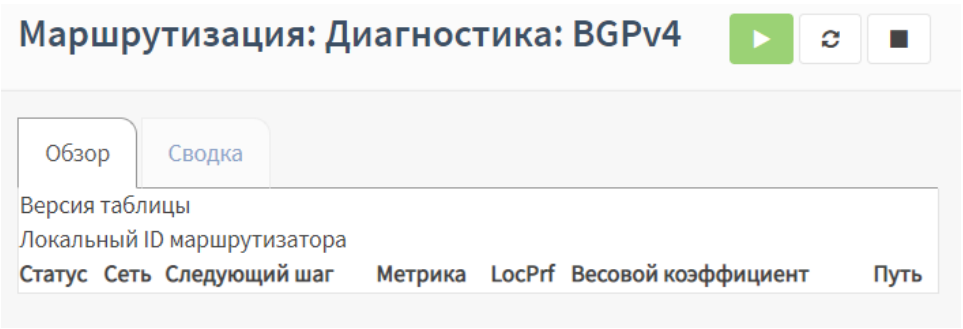


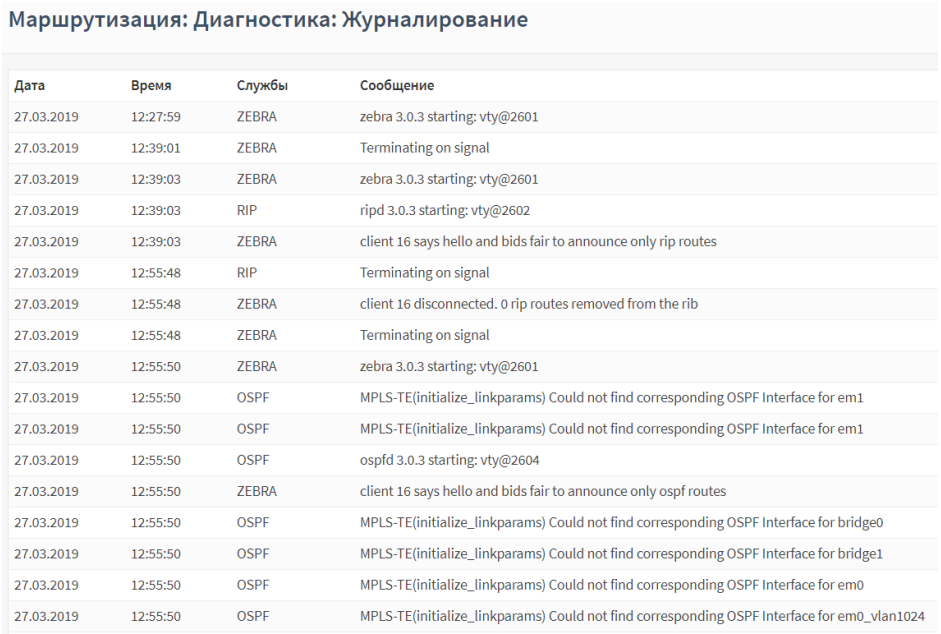
Рисунок 282— Маршрутизация: Диагностика: BGPv4

9.6.5. Категория «Журналирование»

Категория «Журналирование» позволяет просматривать журнал событий динамических маршрутов (рисунок 283), реализованных по следующим протоколам:

– RIP (v1, v2);
– OSPF;
– OSPFv3;

– BGPv4.



Маршрутизация: Диагностика: Журналирование

Дата	Время	Службы	Сообщение
27.03.2019	12:27:59	ZEBRA	zebra 3.0.3 starting: vty@2601
27.03.2019	12:39:01	ZEBRA	Terminating on signal
27.03.2019	12:39:03	ZEBRA	zebra 3.0.3 starting: vty@2601
27.03.2019	12:39:03	RIP	ripd 3.0.3 starting: vty@2602
27.03.2019	12:39:03	ZEBRA	client 16 says hello and bids fair to announce only rip routes
27.03.2019	12:55:48	RIP	Terminating on signal
27.03.2019	12:55:48	ZEBRA	client 16 disconnected. 0 rip routes removed from the rib
27.03.2019	12:55:48	ZEBRA	Terminating on signal
27.03.2019	12:55:50	ZEBRA	zebra 3.0.3 starting: vty@2601
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em1
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em1
27.03.2019	12:55:50	OSPF	ospfd 3.0.3 starting: vty@2604
27.03.2019	12:55:50	ZEBRA	client 16 says hello and bids fair to announce only ospf routes
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for bridge0
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for bridge1
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em0
27.03.2019	12:55:50	OSPF	MPLS-TE(initialize_linkparams) Could not find corresponding OSPF Interface for em0_vlan1024

Рисунок 283 — Маршрутизация: Диагностика: Журналирование

10. Раздел «Службы»

Раздел «Службы» позволяет настраивать следующие службы:

– Портал авторизации;
– DHCPv4;
– DHCPv6;
– Monit;
– синхронизация времени;
– прокси-сервер.

10.1. Подраздел «Портал авторизации»

Подраздел «Портал авторизации» позволяет просматривать, создавать, редактировать зоны, создавать шаблоны начальных страниц, просматривать сессии Портала авторизации по интерфейсам, просматривать / создать / ограничить срок действия ваучеров, просматривать журнал событий Портал авторизации.

10.1.1. Категория «Администрирование»

Категория «Администрирование» вкладка «Зоны» позволяет просматривать существующие зоны Портала авторизации в виде таблицы (рисунок 284). В таблице представлены следующие данные:

– состояние зоны (включена/выключена);
– идентификатор зоны;
– номер зоны;
– описание зоны.

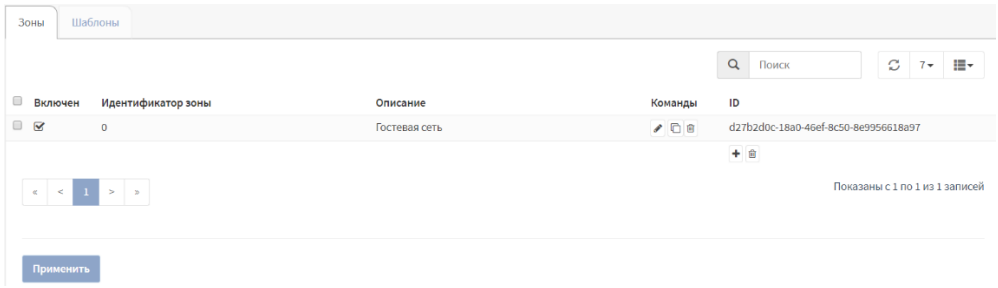


Рисунок 284 — Службы: Портал авторизации: Администрирование: Зоны

Для редактирования существующей зоны необходимо нажать на кнопку  напротив зоны. Для создания новой зоны необходимо нажать на кнопку  .

При редактировании зоны в поле «Включен» необходимо установить флажок для включения этой зоны. В поле «Интерфейсы» необходимо выбрать интерфейсы, для которых будет включен Портал авторизации. В поле «Аутентификация через» необходимо выбрать сервер аутентификации. В поле «Принудительно использовать локальную группу» необходимо выбрать группу, которой будет ограничен доступ. В поле «Значение тайм-аута бездействия (в минутах)» необходимо ввести время, через которое пользователь принудительно выйдет из системы, в случае его бездействия. В поле «Значение тайм-аута сеанса (в минутах)» необходимо ввести значение, через которое пользователь принудительно выйдет из системы. В поле «Множественный вход пользователя в систему» необходимо установить флажок для подключения нескольких устройств, используя один логин. В поле «Сертификат SSL» необходимо выбрать сертификаты. В поле «Имя хоста» необходимо ввести IP-адрес, куда будет перенаправляться пользователь со страницы авторизации. В поле «Разрешенные адреса» необходимо ввести IP-адреса, которым разрешен доступ без авторизации. В поле «Разрешенные MAC-адреса» необходимо ввести MAC-адреса, которым разрешен доступ без авторизации. В поле «Прозрачный прокси (HTTP)» необходимо установить флажок для переадресации HTTP-трафика на прозрачный прокси. В поле «Прозрачный прокси (HTTPS)» необходимо установить флажок для переадресации HTTPS-трафика на прозрачный прокси. В поле «Пользовательский шаблон» необходимо выбрать пользовательский шаблон входа в систему. В поле «Описание» необходимо ввести описание (рисунок 285). Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

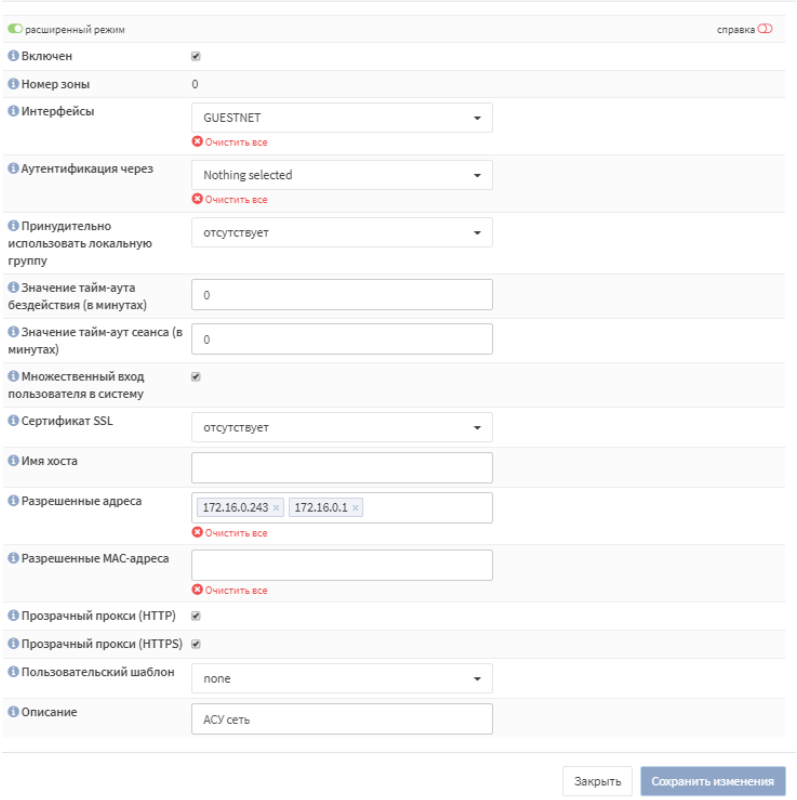


Рисунок 285 — Службы: Портал авторизации: Администрирование: Зоны (редактирование)

Категория «Администрирование» вкладка «Шаблоны» позволяет просматривать существующие шаблоны страницы авторизации Портала авторизации (рисунок 286).

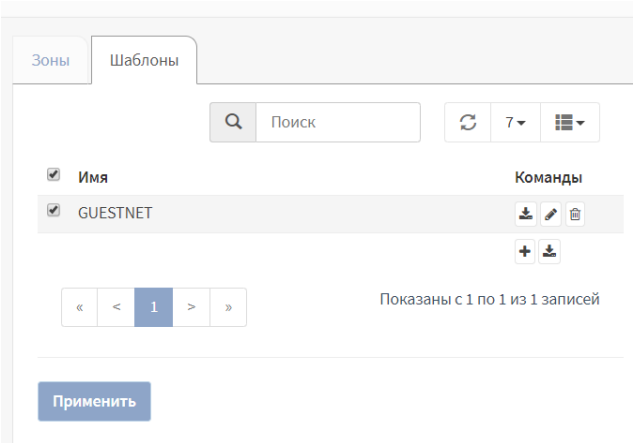


Рисунок 286 — Службы: Портал авторизации: Администрирование: Шаблоны

Также раздел позволяет экспортировать существующий шаблон и импортировать новый шаблон, нажав соответствующие кнопки. При нажатии

на кнопку «Импортировать» появится всплывающее окно со следующими полями. В поле «Имя шаблона» необходимо ввести имя шаблона. Необходимо нажать на кнопку «Необходимо выбрать файл» для локального выбора файла шаблона и необходимо нажать на кнопку «Загрузка» (рисунок 287).

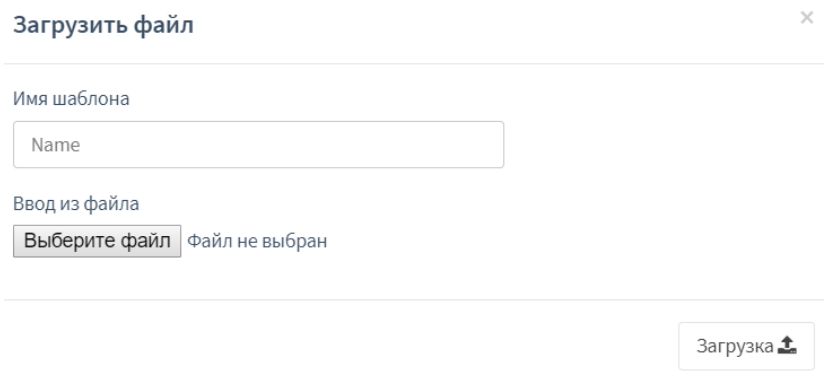


Рисунок 287 — Службы: Портал авторизации: Администрирование: Шаблоны (импорт шаблона)

10.1.2. Категория «Сессии»

В категории «Сессии» отображается информация о запущенных сессиях Портала авторизации в виде таблицы (рисунок 288). Таблица содержит следующие данные:

- идентификатор сессии;
- имя пользователя;
- MAC-адрес пользователя;
- IP-адрес пользователя;
- дата/время сессии.

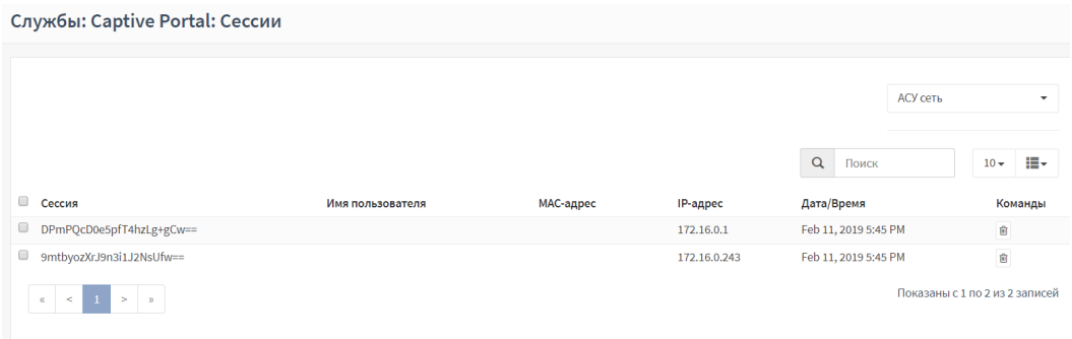


Рисунок 288 — Службы: Портал авторизации: Сессии

10.1.3. Категория «Ваучеры»

В категории «Ваучеры» отображаются все ваучеры выбранного Ваучер-сервера в виде таблицы (рисунок 289).

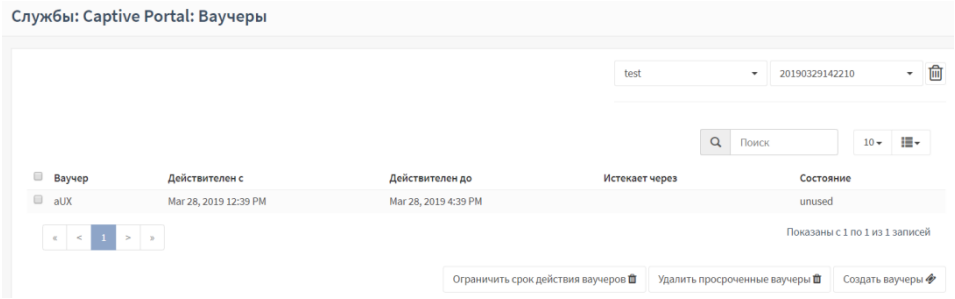


Рисунок 289 — Службы: Портал авторизации: Ваучеры

Раздел позволяет ограничить срок действия ваучеров, для этого необходимо выбрать ваучеры и нажать на кнопку «Ограничить срок действия ваучеров».

Также раздел позволяет удалить просроченные ваучеры, нажав соответствующую кнопку.

Для создания нового ваучера необходимо нажать на кнопку «Создать ваучеры» (рисунок 290). В появившимся всплывающем окне в поле «Срок действия» необходимо выбрать срок действия ваучера (то есть срок действия одного сеанса использования этого ваучера). В поле «Истекает после» необходимо выбрать через сколько ваучер истекает. В поле «Количество ваучеров» необходимо выбрать количество добавляемых ваучеров. В поле «Имя группы» необходимо выбрать имя группы ваучеров и необходимо нажать на кнопку «Сгенерировать». После этого созданый (-ные) ваучер (-ы) будут автоматически экспортированы в локальную систему в формате «*.csv».

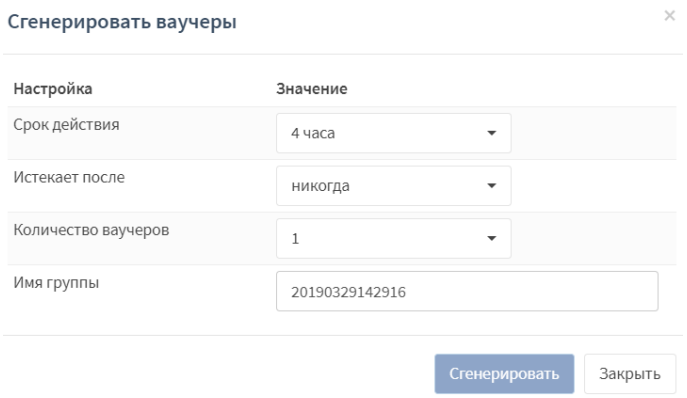


Рисунок 290 — Службы: Портал авторизации: Ваучеры (создание ваучеров)

10.1.4. Категория «Журнал»

В категории «Журнал» отображается журнал событий Портала авторизации (рисунок 291).

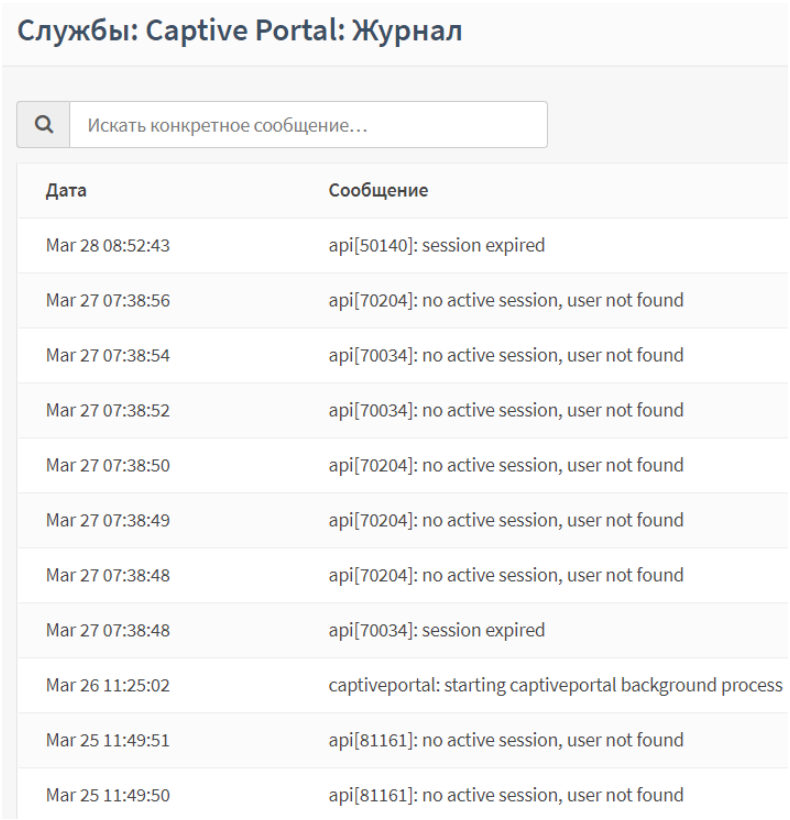


Рисунок 291 — Службы: Портал авторизации: Журнал

10.2. Подраздел «DHCPv4»

Подраздел «DHCPv4» позволяет настраивать DHCPv4-сервер.

10.2.1. Категория «[Название интерфейса]»

Категория [Название интерфейса] позволяет настраивать DHCPv4-сервер для интерфейса.

В пункте «Включен» необходимо установить флажок для включения DHCPv4-сервера. В поле «Блокировать неизвестных клиентов» необходимо установить флажок для разрешения получения IP-адресов только клиентам из выбранного далее диапазона. В поле «Диапазон» необходимо ввести диапазон IP-адресов, входящий в доступный диапазон, указанный в поле «Доступный диапазон». В поле «Дополнительные пулы» необходимо ввести дополнительные пулы адресов внутри подсети, которые не входят в доступный диапазон, указанный в поле «Доступный диапазон». В поле «WINS-серверы» необходимо ввести WINS-сервера. В поле «DNS-серверы» необходимо ввести DNS-серверы. В поле «Имя домена» необходимо ввести доменное имя. В поле «Список поиска доменов» необходимо ввести список поиска домена. В поле «Время аренды по умолчанию (секунд)» необходимо ввести время аренды для клиентов, которые не запрашивают конкретное время аренды. В поле «Максимальное время аренды (с)» необходимо ввести максимальное время аренды для клиентов, которые не запрашивают точное время. В поле «MTU интерфейса» необходимо ввести указание на MTU на этом интерфейсе. В поле «IP-адрес участника для аварийного переключения» необходимо ввести IP-адрес интерфейса на другом устройстве для аварийного переключения. В поле «Статический ARP» необходимо установить флажок для включения статического ARP. В поле «Изменить формат даты» необходимо установить флажок для изменения отображения времени аренды DHCP с UTC на местное время (рисунок 292).

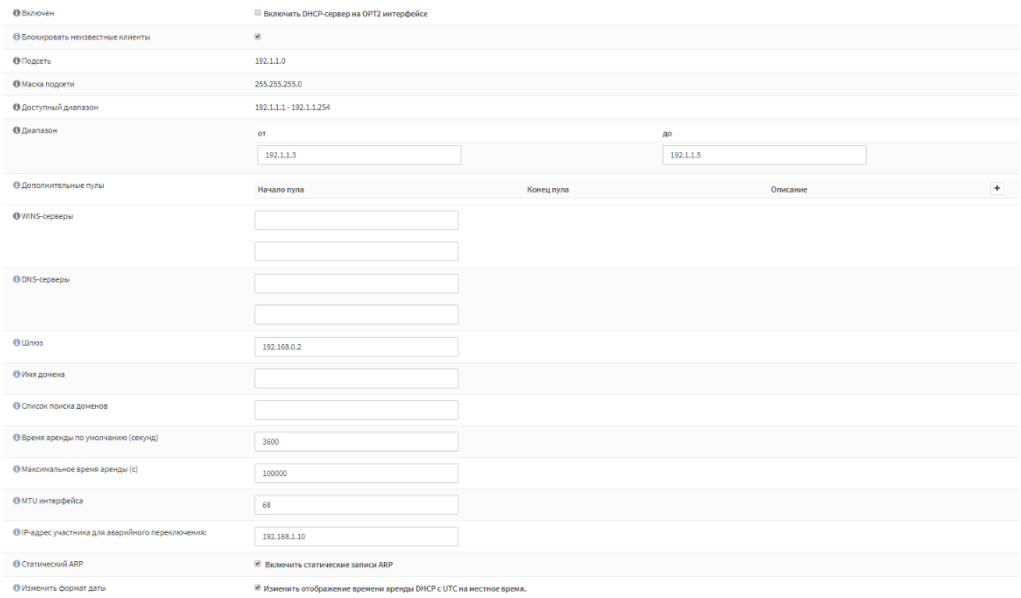


Рисунок 292 — Службы: DHCPv4: [Название интерфейса]

В пункте «Динамический DNS» при нажатии на кнопку «Дополнительно» в поле «Включить регистрацию имен DHCP-клиентов DNS» необходимо установить флажок для включения регистрации имен DHCP-клиентов DNS и в первом поле необходимо ввести IP-адрес основного сервера доменных имен, во втором поле необходимо ввести имя доменного ключа, в третьем поле необходимо ввести секретный ключ домена (рисунок 293)

В пункте «Контроль доступа по MAC-адресам» при нажатии на кнопку «Дополнительно» в первом поле необходимо ввести список разрешенных MAC-адресов, во втором поле необходимо ввести список блокируемых MAC-адресов (рисунок 293).

В пункте «NTP-серверы» при нажатии на кнопку «Дополнительно» в поле необходимо ввести NTP-серверы (рисунок 293).

В пункте «TFTP-сервер» при нажатии на кнопку «Дополнительно» в поле необходимо ввести TFTP-сервер (рисунок 293).

В пункте «LDAP URI» при нажатии на кнопку «Дополнительно» в поле необходимо ввести полный URL для LDAP-сервера (рисунок 293).

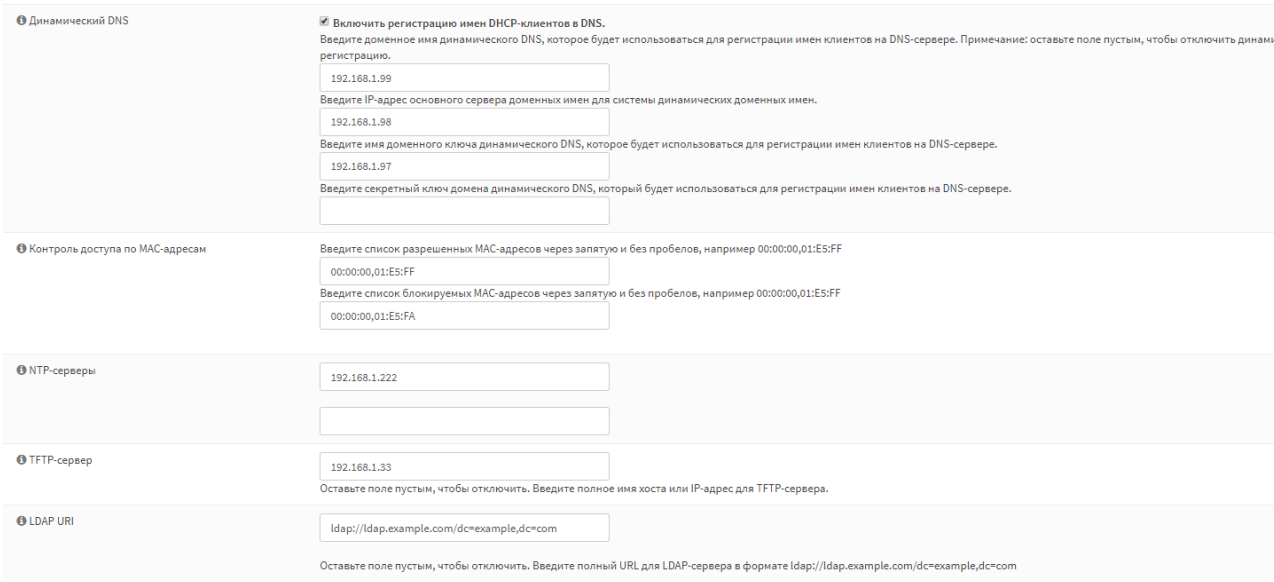


Рисунок 293 — Службы: DHCPv4: [Название интерфейса] (дополнительно, часть 1)

В пункте «Включить загрузку по сети» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить загрузку по сети» для включения загрузки по сети. В первом поле необходимо ввести IP-адрес следующего сервера, во втором поле необходимо ввести имя файла BIOS, в третьем поле необходимо ввести имя файла UEFI 32bit, в четвертом поле необходимо ввести имя файла UEFI 64bit, в пятом поле необходимо ввести корневой путь (рисунок 294).

В пункте «WPAD» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить автоматическую настройку прокси-сервера» для включения автоматической настройки прокси-сервера.

В пункте «Дополнительные параметры» при нажатии на кнопку «Дополнительно» необходимо ввести дополнительные параметры, которые необходимо включить в информацию об аренде DHCP (рисунок 294).

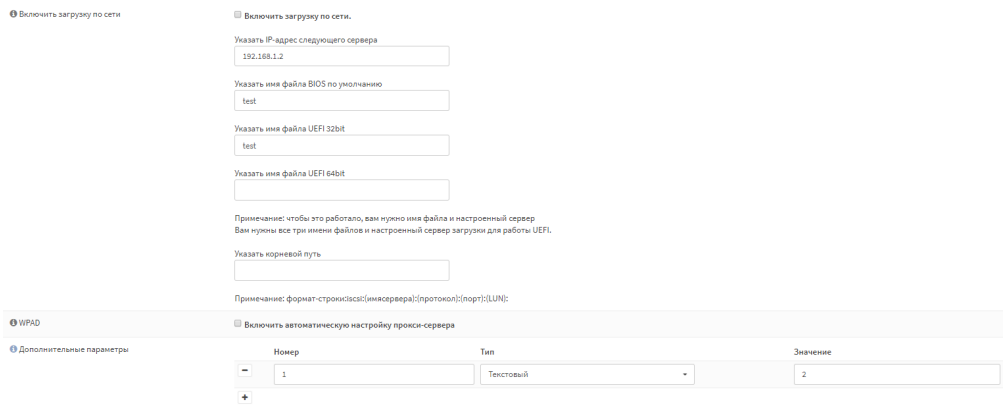


Рисунок 294 — Службы: DHCPv4: [Название интерфейса] (дополнительно, часть 2)

После внесения изменений необходимо нажать на кнопку «Сохранить».

10.2.2. Категория «Ретрансляция»

Категория «Ретрансляция» позволяет настраивать ретрансляцию DHCPv4. При ретрансляции запросы DHCP могут быть «перенаправлены» на другой сервер.

В пункте «Включен» необходимо установить флажок для включения DHCP-ретрансляции. В поле «Интерфейсы» необходимо выбрать интерфейсы, для которых необходимо настроить DHCP-ретранслятор. В поле «Добавлять идентификатор канала» необходимо установить флажок для добавления идентификатора канала и агента в запросы. В поле «Серверы назначения» необходимо ввести IP-адреса серверов, на которые будут перенаправляться DHCP запросы (рисунок 295). После внесения изменений необходимо нажать на кнопку «Сохранить».

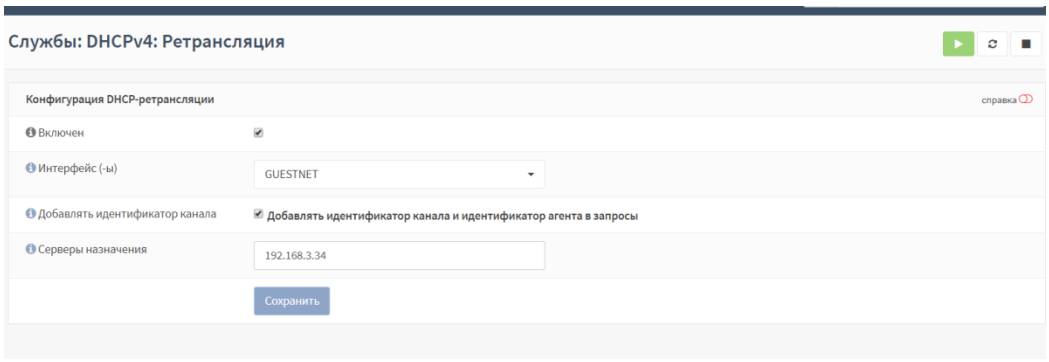


Рисунок 295 — Службы: DHCPv4: Ретрансляция

10.2.3. Категория «Аренда адресов»

Категория «Аренда адресов» позволяет просматривать все IP-адреса, которые раздаются клиентам (рисунок 296). Позволяет просматривать все активные и все настроенные аренды, нажав соответствующие кнопки.

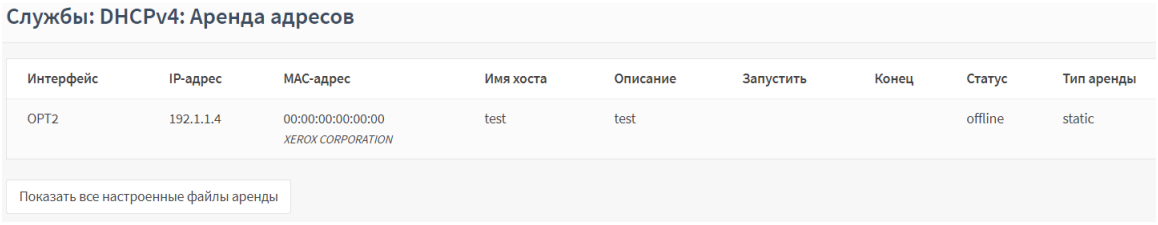


Рисунок 296 — Службы: DHCPv4: Аренда адресов

10.2.4. Категория «Журнал»

Категория «Журнал» позволяет просматривать журнал DHCPv4-сервера (рисунок 297).

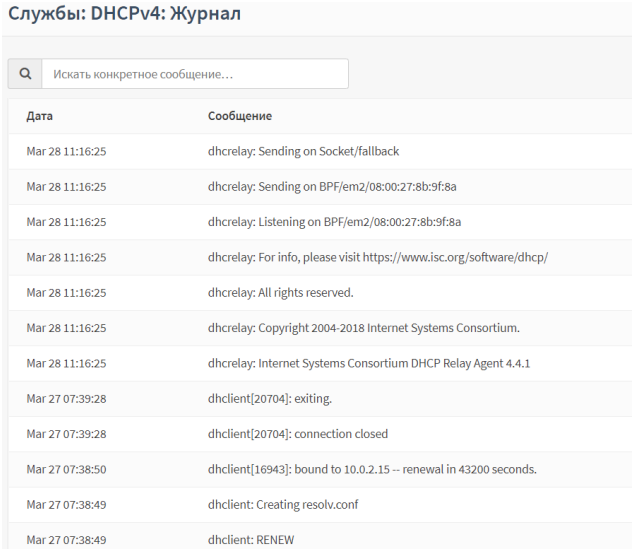


Рисунок 297 — Службы: DHCPv4: Журнал

10.3. Подраздел «DHCPv6»

Подраздел «DHCPv6» позволяет настраивать DHCPv6-сервер.

10.3.1. Категория «[Название интерфейса]»

Категория [Название интерфейса] позволяет настраивать DHCPv6-сервер для интерфейса.

В пункте «Включен» необходимо установить флажок для включения DHCPv4-сервера. В поле «Диапазон» необходимо ввести диапазон IP-адресов, входящий в доступный диапазон, указанный в поле «Доступный диапазон». В поле «Дополнительные делегируемые префиксы» необходимо ввести дополнительные делегируемые префиксы адресов внутри подсети, которые не входят в доступный диапазон, указанный в поле «Доступный диапазон». В поле «DNS-серверы» необходимо ввести DNS-серверы. В поле «Имя домена» необходимо ввести доменное имя. В поле «Список поиска доменов» необходимо ввести список поиска домена. В поле «Время аренды по умолчанию (секунд)» необходимо ввести время аренды для клиентов, которые не запрашивают конкретное время аренды. В поле «Максимальное время аренды (с)» необходимо ввести максимальное время аренды для клиентов, которые не запрашивают точное время. В поле «Изменить формат даты» необходимо установить флажок для изменения отображения времени аренды DHCP с UTC на местное время (рисунок 298).

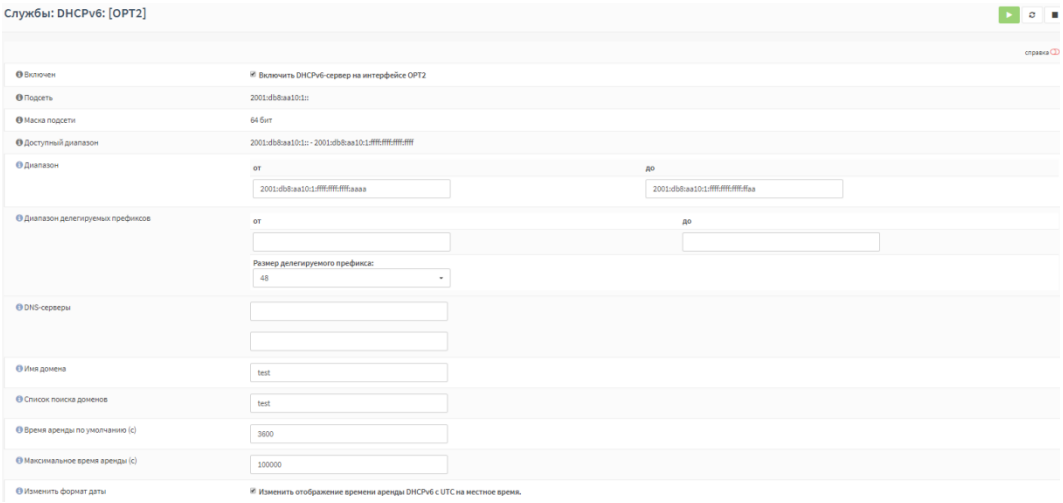


Рисунок 298 — Службы: DHCPv6: [Название интерфейса]

В пункте «Динамический DNS» при нажатии на кнопку «Дополнительно» в поле «Включить регистрацию имен DHCP-клиентов DNS» необходимо установить флажок для включения регистрации имен DHCP-клиентов DNS и в первом поле необходимо ввести IP-адрес основного сервера доменных имен, во втором поле необходимо ввести имя доменного

ключа, в третьем поле необходимо ввести секретный ключ домена (рисунок 299).

В пункте «NTP-серверы» при нажатии на кнопку «Дополнительно» в поле необходимо ввести NTP-серверы (рисунок 299).

В пункте «Включить загрузку по сети» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить загрузку по сети» для включения загрузки по сети. В первом поле необходимо ввести IP-адрес следующего сервера, во втором поле необходимо ввести имя файла BIOS, в третьем поле необходимо ввести имя файла UEFI 32bit, в четвертом поле необходимо ввести имя файла UEFI 64bit, в пятом поле необходимо ввести корневой путь (рисунок 299).

В пункте «Дополнительные параметры BOOTP/DHCP» при нажатии на кнопку «Дополнительно» необходимо ввести дополнительные параметры, которые необходимо включить в информацию об аренде DHCP (рисунок 299).

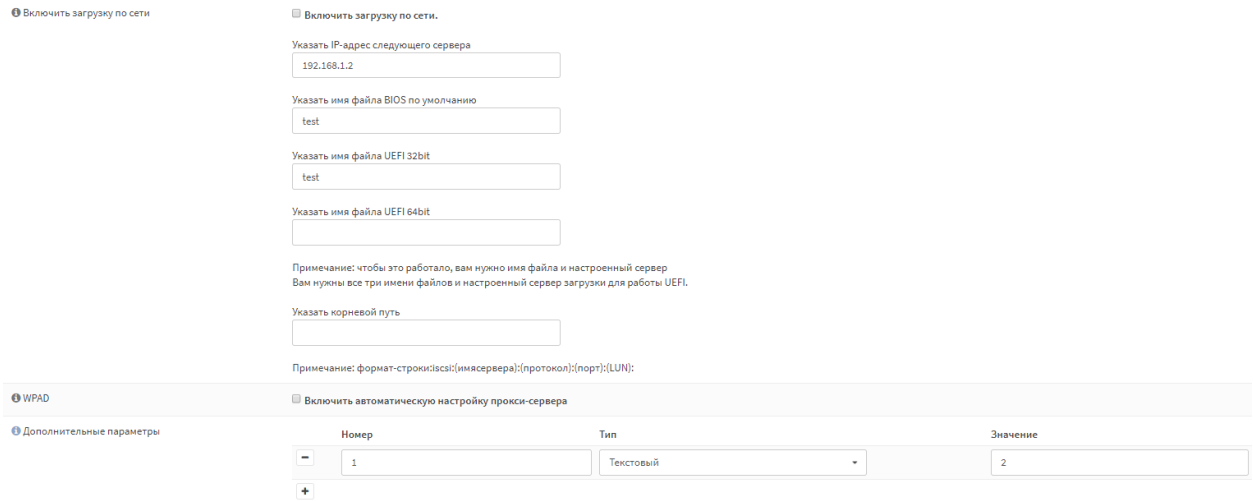


Рисунок 299 — Службы: DHCPv6: [Название интерфейса] (дополнительно)

После внесения изменений необходимо нажать на кнопку «Сохранить».

10.3.2. Категория «Ретрансляция»

Категория «Ретрансляция» позволяет настраивать ретрансляцию DHCPv6. При ретрансляции запросы DHCP могут быть «перенаправлены» на другой сервер.

В пункте «Включен» необходимо установить флажок для включения DHCP-ретрансляции. В поле «Интерфейсы» необходимо выбрать интерфейсы, для которых необходимо настроить DHCP-ретранслятор. В поле «Добавлять идентификатор канала» необходимо установить флажок для добавления идентификатора канала и агента в запросы. В поле «Серверы назначения» необходимо ввести IP-адреса серверов, на которые будут перенаправляться DHCP запросы (рисунок 300). После внесения изменений необходимо нажать на кнопку «Сохранить».

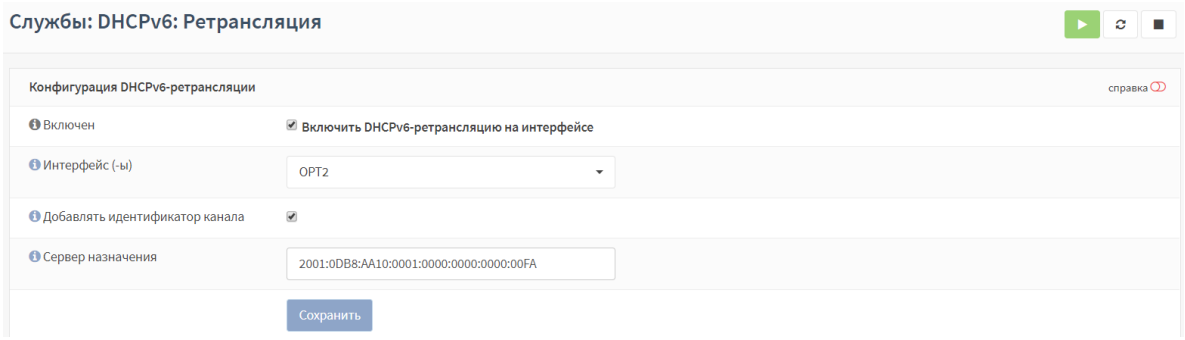


Рисунок 300 — Службы: DHCPv6: Ретрансляция

10.3.3. Категория «Аренда адресов»

Категория «Аренда адресов» позволяет просматривать все IP-адреса, которые раздаются клиентам (рисунок 301). Позволяет просматривать активные и все настроенные аренды, нажав соответствующие кнопки.

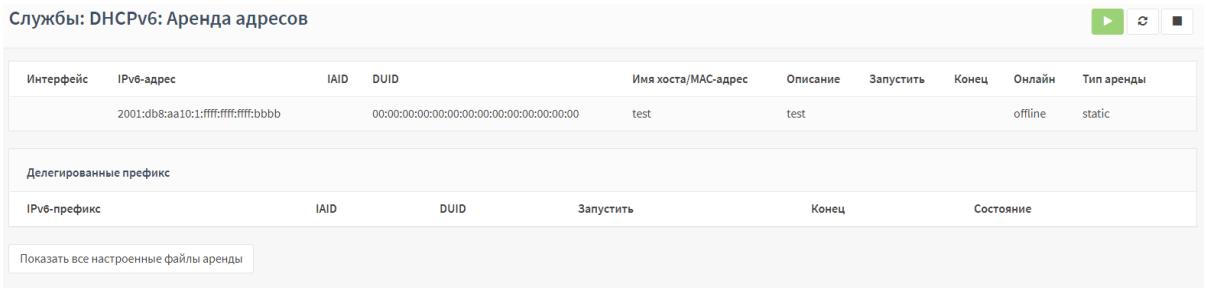


Рисунок 301 — Службы: DHCPv6: Аренда адресов

10.4. Подраздел «Monit»

Сервис «Monit», является встроенным пакетом в систему. Это небольшая утилита с открытым исходным кодом для мониторинга Unix-

систем с возможностью выполнения скриптов в качестве реакции на заданное событие.

Сервис «Monit» выполняется следующее:

– отслеживает состояния серверов (доступность, потребление ресурсов);

– производит мониторинг сервисов (состояние, потребляемые ресурсы, количество child-process и многое другое);

– производит мониторинг сетевых сервисов (возможность подключения и корректность ответа);

– производит выполнение встроенных или собственных (с помощью скриптов) действий при достижении определенных событий;

– производит отправку уведомлений на E-mail или в централизованный web-интерфейс M/Monit (коммерческая надстройка над «Monit»).

10.4.1. Категория «Настройки»

В пункте «Настройки» осуществляется настройка сервиса «Monit».

В категории «Основные настройки» необходимо установить флажок напротив «Включить monit», чтобы включить «Monit». В поле «Интервал опроса» необходимо ввести интервал опроса в секундах. В поле «Задержка старта» необходимо ввести задержку старта системы, чтобы пакет «Monit» запустил контролируемые сервисы. В поле «Почтовый сервер» необходимо ввести список SMNT серверов. В поле «Порт почтового сервера» необходимо ввести порт почтового сервера. В поле «Имя пользователя» необходимо ввести имя пользователя для аутентификации. В поле «Пароль» необходимо ввести пароль для аутентификации пользователя. В поле «Защищенное соединение» необходимо установить флажок для включения шифрования. В поле «Журнал» необходимо ввести журнал процесса «Monit». В поле «Файл состояния» необходимо ввести файл состояния процесса «Monit». В поле «Путь к очереди событий» необходимо ввести путь к каталогу очередей

событий. В поле «Слоты очереди событий» необходимо ввести количество слотов событий. В поле «Включите HTTPD» необходимо установить флажок для запуска «Monit» сервиса httpd (рисунок 302).

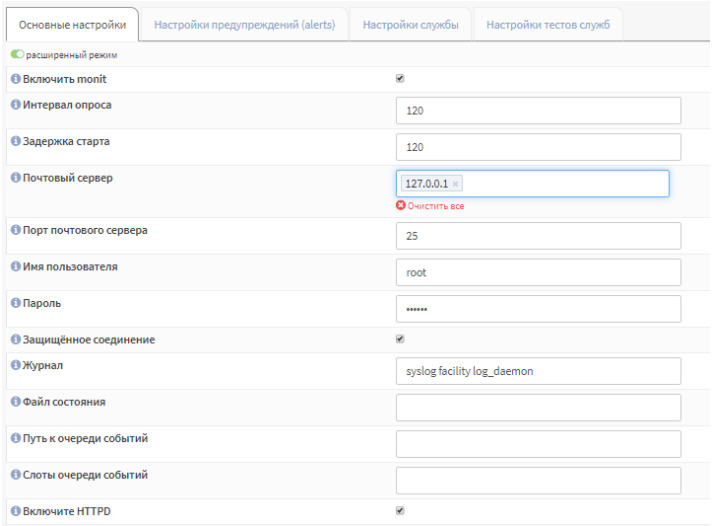


Рисунок 302 — Службы: «Monit»: Настройки: Основные настройки

Категория «Настройки предупреждений (alerts)» позволяет просматривать в виде таблицы настроенные предупреждения (рисунок 303). Таблица содержит следующие данные:

– состояние (включено/выключено);
– получатель;
– событие;
– описание.

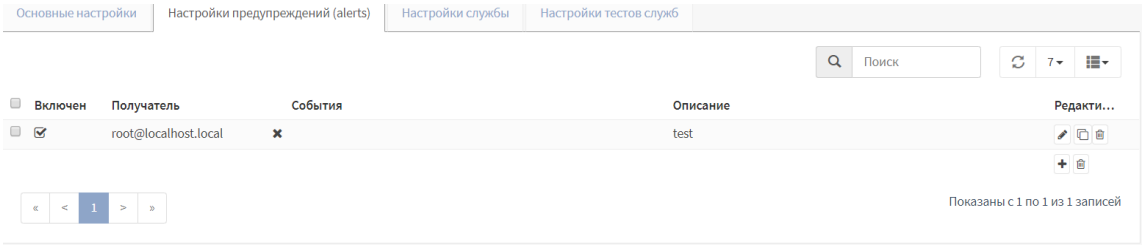


Рисунок 303— Службы: «Monit»: Настройки: Настройки предупреждений (alerts)

Для редактирования существующего предупреждения необходимо нажать на кнопку напротив предупреждения. Для создания нового предупреждения необходимо нажать на кнопку .

При редактировании предупреждения (рисунок 304) в поле «Включить предупреждения (alert)» необходимо установить флажок для включения предупреждения. В поле «Получатель» необходимо ввести e-mail получателя. В поле «Не для следующих» необходимо установить флажок для отключения отправки предупреждения для следующих событий. В пункте «Формат почты» необходимо ввести формат сообщения:

– *$ EVENT* (добавляет описание произошедшего событие);

– *$ SERVICE* (добавляет название сервиса);

– *$ DATE* (добавляет текущее время и дату (стиль даты RFC 822));

– *$ HOST* (добавляет имя хоста, на котором работает «Monit»);

– *$ ACTION* (добавляет название действия, которое было сделано «Monit»);

– *$ ОПИСАНИЕ* (добавляет описание состояния ошибки).

В пункте «Напоминание» необходимо ввести через сколько циклов присылать напоминание. В пункте «Описание» необходимо ввести описание, например, «Оповещение по email» и необходимо нажать на кнопку «Сохранить изменения».

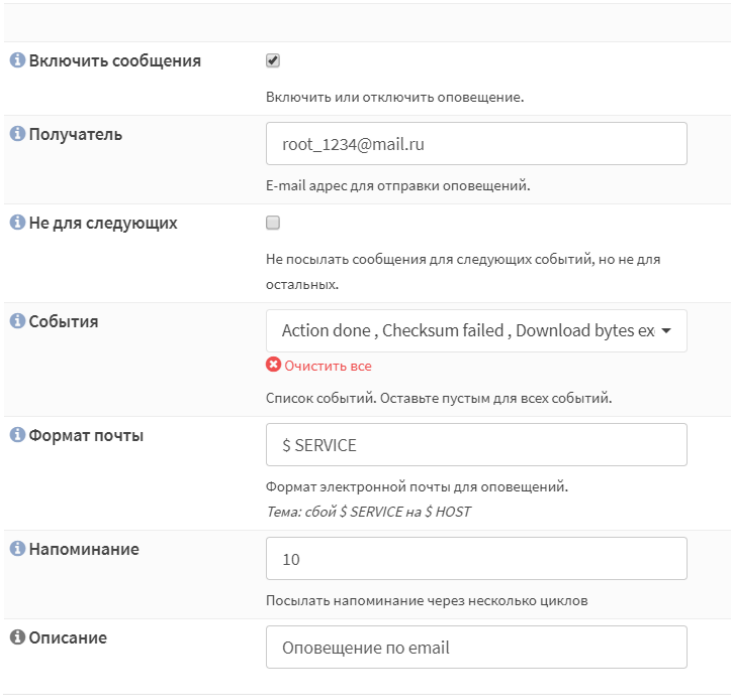


Рисунок 304 — Службы: «Monit»: Настройки: Настройки предупреждений (alerts): редактирование

В категории «Настройки службы» показаны настроенные проверяемые сервисы в виде таблицы (рисунок 305). Таблица содержит следующие данные:

– состояние сервиса (включено/выключено);
– имя сервиса;
– идентификатор сервиса.

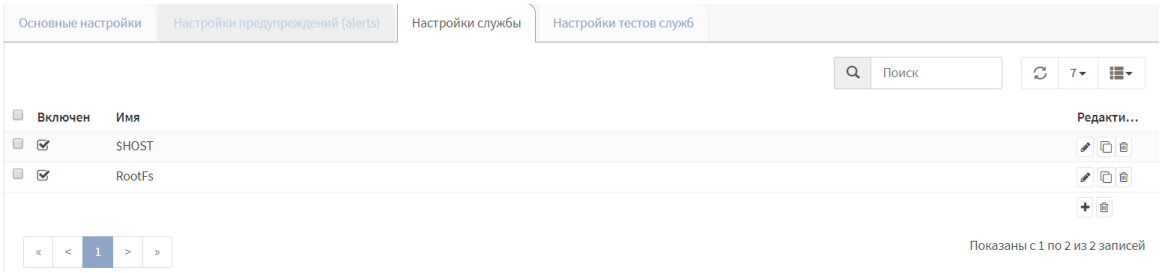


Рисунок 305 — Службы: «Monit»: Настройки: Настройки службы

Для редактирования существующего сервиса необходимо нажать на кнопку  напротив сервиса. Для создания нового сервиса необходимо нажать на кнопку  .

При редактировании сервиса в поле «Включить проверки служб» необходимо установить флажок для включения проверки сервисов. В поле «Имя» необходимо ввести имя сервиса. В поле «Тип» необходимо выбрать тип проверки сервиса. В поле «PID файл» необходимо ввести PID-файл процесса. В поле «Совпадение» необходимо ввести шаблон совпадения. В поле «Запустить» необходимо ввести скрипт запуска сервиса. В поле «Остановить» необходимо ввести скрипт остановки сервиса. В поле «Тесты» необходимо выбрать список тестов сервисов. В поле «Зависит от» необходимо выбрать сервис(ы), от которых зависит данный сервис. В поле «Описание» необходимо ввести описание и необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 306).

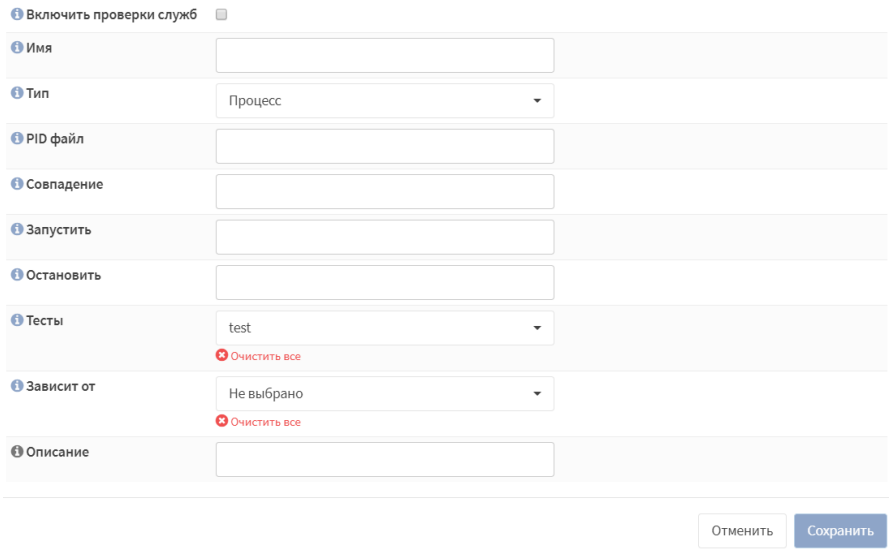


Рисунок 306 — Службы: «Monit»: Настройки: Настройки службы (редактирование)

Категория «Настройка тестов служб» позволяет просматривать таблицу тестов служб (рисунок 307). Таблица содержит следующие данные:

– название теста;
– условие для срабатывания тестов служб;
– действие, которое будет выполнено при срабатывании условия.

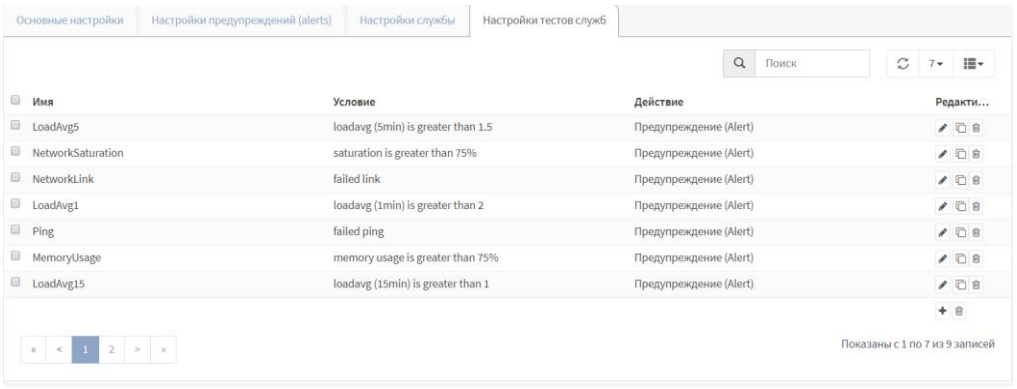


Рисунок 307 — Службы: «Monit»: Настройки: Настройка тестов служб

Для редактирования существующего теста служб необходимо нажать на кнопку  напротив теста. Для создания нового теста необходимо нажать на кнопку  .

При редактировании в поле «Имя» необходимо ввести название теста. В поле «Условие» необходимо ввести условие срабатывания теста. В поле

«Действие» необходимо выбрать действие, которое будет выполнено при срабатывании условия (рисунок 308).

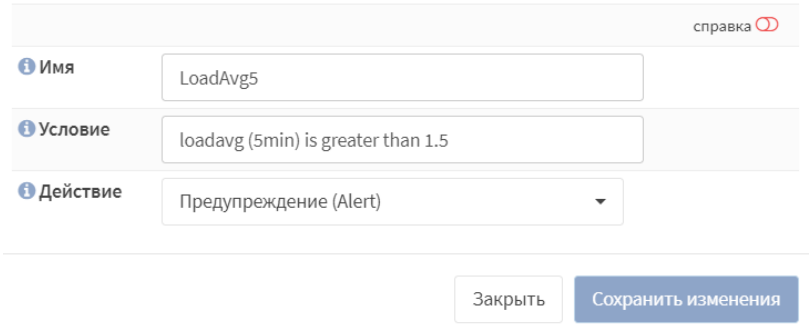


Рисунок 308 — Службы: «Monit»: Настройки: Настройка тестов служб (редактирование)

10.4.2. Категория «Статус»

Категория «Статус» позволяет просматривать информацию о «Monit» (рисунок 309).

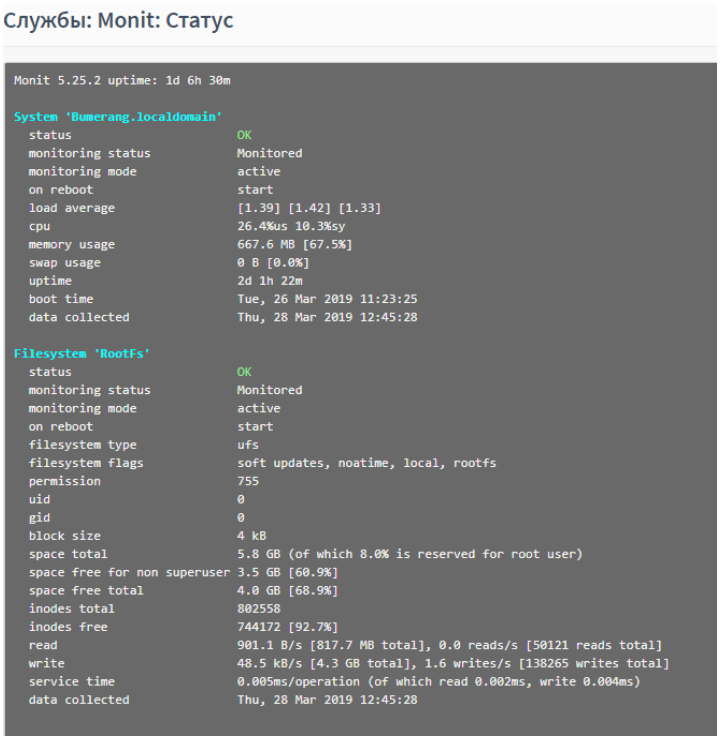


Рисунок 309 — Службы: «Monit»: Статус

10.5. Подраздел «Синхронизация времени»

Подраздел «Синхронизация времени» позволяет производить общие настройки синхронизации времени, настраивать GPS-приемник, PPS, просматривать статус и журнал NTP.

10.5.1. Категория «Общие настройки»

Категория «Общие настройки» позволяет отредактировать конфигурацию NTP-сервера.

В поле «Интерфейсы» необходимо выбрать интерфейсы, которые будут прослушиваться. В поле «Серверы времени» необходимо ввести серверы времени и указать их приоритет. В поле «Автономный режим» необходимо ввести число, указывающее на приоритет автономного режима. Который позволяет использовать системные часы при недоступности остальных. В поле «Графики NTP» необходимо установить флажок для включения RRD-графиков статистики NTP. В поле «Системное журналирование» необходимо установить флажок напротив поля «Включить журналирование сообщений узлов (по умолчанию: отключено)» для включения журналирования сообщений узлов и напротив поля «Включить журналирование системных сообщений (по умолчанию: отключено)» для включения журналирования системных сообщений. В поле «Журналирование статистики» необходимо установить флажок (-и) для включения необходимых параметров. В поле «Ограничения доступа» необходимо установить флажок (-и) при необходимости выполнения выбранных параметров. В поле «Дополнительные секунды» необходимо ввести настройки секунд, добавляемых к всемирному координированному времени для согласования его со средним солнечным временем. Настройки дополнительной секунды вводится в виде текста и загружается с помощью файла нажатием на кнопку «Выбрать файл». В поле «Дополнительно» необходимо ввести дополнительные параметры и нажать на кнопку «Сохранить» для сохранения внесенных изменений (рисунок 310).

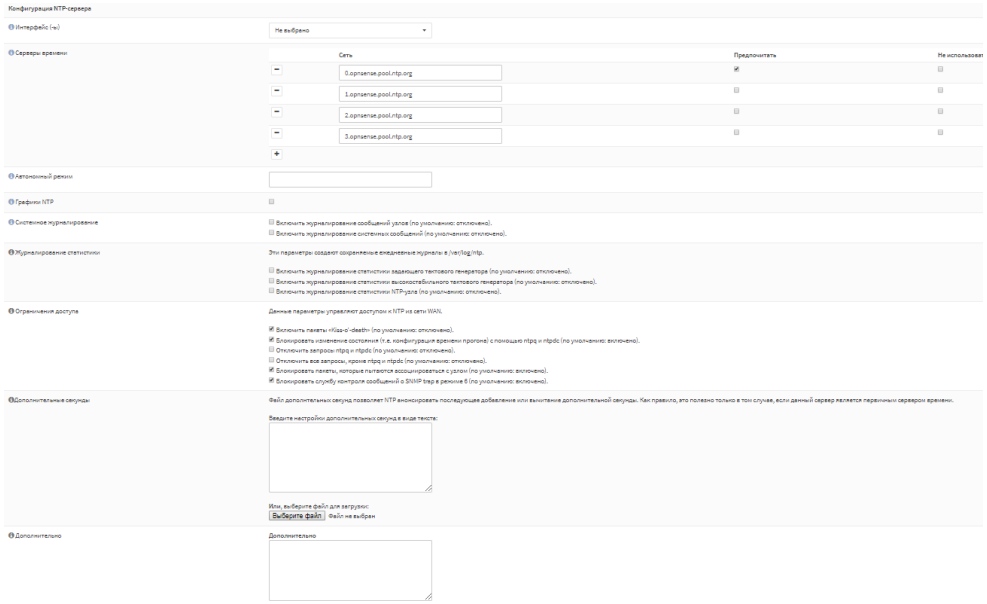


Рисунок 310 — Службы: Синхронизация времени: Общие настройки

10.5.2. Категория «GPS-приемник»

Категория «GPS-приемник» позволяет настраивать GPS-приемник, подключенный к ПК. GPS-приемник, подключенный через порт последовательного ввода-вывода, может использоваться в качестве системных часов для NTP. Кроме того, если GPS-приемник поддерживает PPS, правильно настроен и подключен, то он может также использоваться в качестве системных часов для PPS.

В поле «GPS-приемник» необходимо выбрать предварительно заданную конфигурацию. В поле «Предложения NMEA» необходимо выбрать одно или несколько предложений NMEA. В поле «Fudge time 1 (секунды)» необходимо выбрать смещение сигнала GPS PPS. В поле «Fudge time 2 (секунды)» необходимо выбрать смещение времени GPS. В поле «Часовой слой» необходимо ввести значение для изменения приоритета. В поле «Флажки» необходимо поставить флажки напротив нужных параметров. В поле «Идентификатор часов» необходимо ввести идентификатор GPS. В поле «Инициализация GPS-приемника» в поле необходимо ввести команды GPS-приемнику. В поле «Вычисление контрольной суммы» необходимо ввести текст между "$" и "*" и нажать «Подсчитать». Необходимо нажать на кнопку «Сохранить» (рисунок 311).

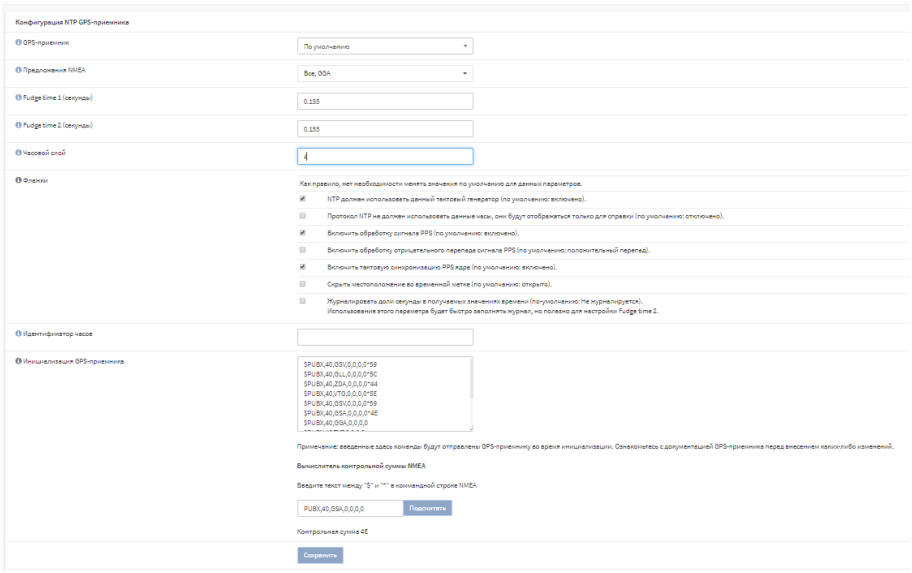


Рисунок 311 — Службы: Синхронизация времени: GPS-приемник

10.5.3. Категория «Статус»

Категория «Статус» позволяет просматривать таблицу состояний синхронизации времени. В таблице отображаются следующие данные (рисунок 312):

– статус сервера сетевого времени;
– IP-адрес сервера;
– идентификатор источника;
– приоритет сервера сетевого времени;
– тип;
– начальное время;
– интервал опроса;
– задержка;
– смещение;
– неусточивость.

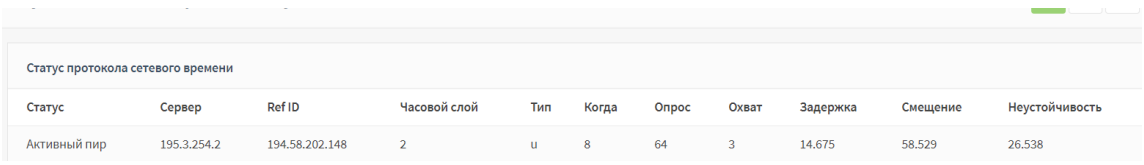


Рисунок 312 — Службы: Синхронизация времени: Статус

10.5.4. Категория «Журнал»

Категория «Журнал» позволяет просматривать журнал NTP (рисунок 313).

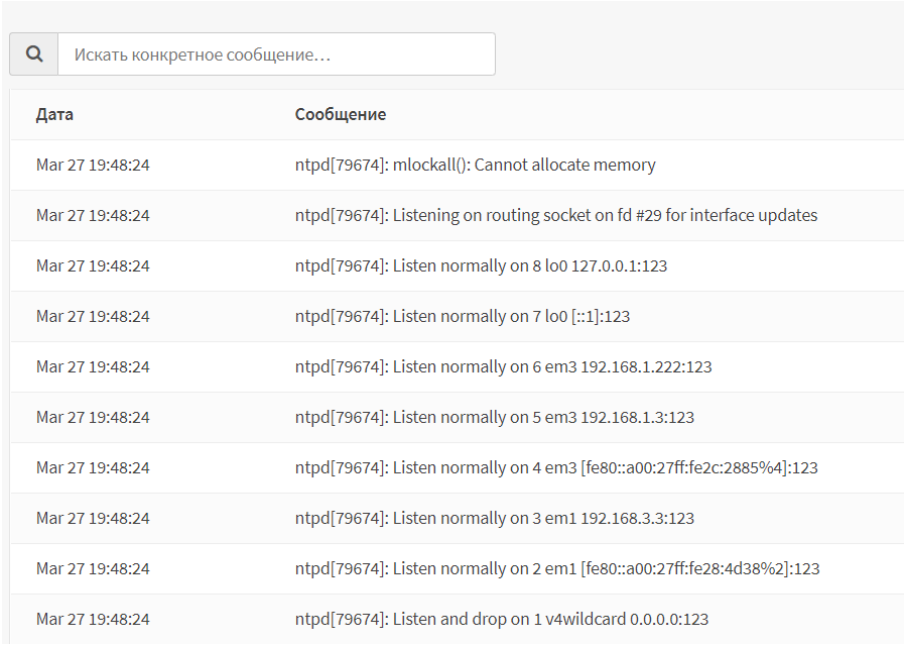


Рисунок 313 — Службы: Синхронизация времени: Журнал

10.6. Подраздел «Прокси»

Подраздел «Прокси» позволяет настраивать прокси-сервер, перенаправляющий прокси-сервер, а также создавать списки контроля доступа.

Веб-прокси Squid (кэширующий прокси) поддерживает широкие возможности фильтрации по различным критериям:

– фильтрация по IP-адресам;

– фильтрация по портам назначения;

– фильтрация по типу браузера;

– фильтрация по типу контента (по MIME-типам);

– фильтрация по общим белым и черным спискам;

– фильтрация по скачиваемым спискам.

Прокси-сервер поддерживает работу в прозрачном режиме (прозрачный HTTP-прокси). Смысл прозрачного проксирования заключается в том, что

пользователи не имеют явных настроек на веб-прокси, тем не менее их трафик все равно будет перехвачен и попадет на веб-прокси.

FTP-прокси обрабатывает только незашифрованный FTP-трафик.

Перенаправляющий прокси-сервер работает за счет использования правил межсетевого экрана («Межсетевой экран» - «NAT» - «Переадресация портов»).

10.6.1. Категория «Администрирование»

Вкладка «Основные настройки»

В элементе «Основные настройки» вкладки «Основные настройки» осуществляются основные настройки прокси-сервера.

В пункте «Включить прокси» необходимо установить флажок для включения прокси-сервера. В поле «Порт ICP» необходимо ввести номер порта, на который сервис Squid будет посылать и принимать ICP-запросы. В поле «Включить ведение журнала обращения» необходимо установить флажок для включения ведения журнала запросов клиентов. В поле «Вести журнал в» необходимо выбрать журнал, данные которого необходимо отправить адресату. В поле «Игнорировать хосты в журнале access.log» необходимо ввести подсети/адреса, которые необходимо игнорировать для записи в журнал access.log. В поле «Использовать альтернативные DNS-серверы» необходимо ввести IP-адреса альтернативных DNS-серверов. В поле «Включить сначала DNSv4» необходимо установить флажок при необходимости, чтобы сервис Squid сначала связывался с веб-сайтами с двумя стеками через IPv4. В поле «Использовать заголовок Via» необходимо установить флажок при необходимости, чтобы сервис Squid добавлял Via заголовок в запросы и ответы. В поле «Обработка заголовков X-Forwarded-For» необходимо выбрать действие с заголовком X-Forwarded-For. В поле «Имя хоста, которое будет отображаться в сообщениях об ошибках» необходимо ввести имя хоста, которое будет отображаться в сообщениях об ошибках прокси-сервера. В поле «Почта администратора» необходимо

ввести почту администратора системы. В поле «Блокировать строку с версией» необходимо установить флажок для блокирования выдачи версии сервиса Squid в HTTP-заголовках и HTML-страницах об ошибках. В поле «Обработка пробелов для URI» необходимо выбрать, что делать с URI, который содержит пробелы. Необходимо нажать на кнопку «Применить» для сохранения настроек (рисунок 314).

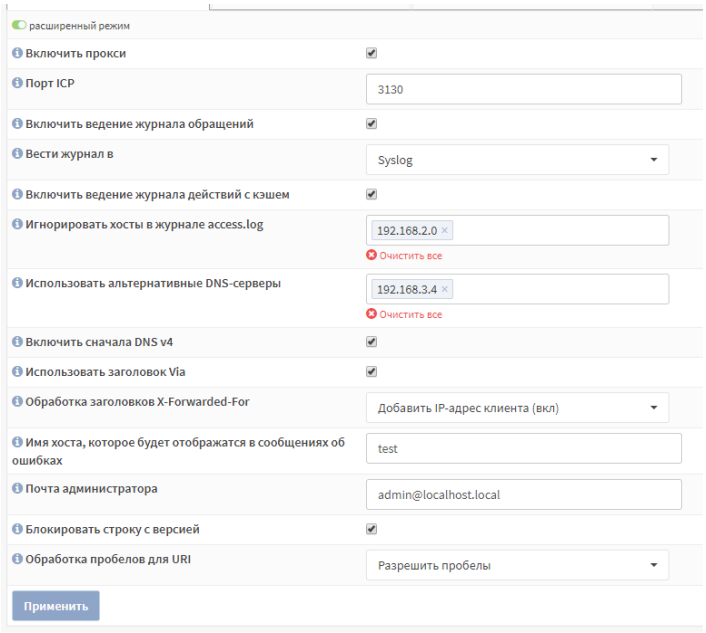


Рисунок 314 — Службы: Прокси: Администрирование (основные настройки прокси)

В элементе «Настройки локального кэша» вкладки «Основные настройки» осуществляются основные настройки локального кэша.

В поле «Размер кэш памяти (в Мб)» необходимо ввести размер памяти кэша. В поле «Включить локальный кэш» необходимо установить флажок для включения локального кэша. В поле «Размер кэша (в Мб)» необходимо ввести количество дискового пространства для хранения локального кэша. В поле «Расположение директории кэша» необходимо ввести расположение директории для локального кэша. В поле «Число подкаталогов первого уровня» необходимо ввести количество подкаталогов первого уровня, которые будут созданы в директории для хранения локального кэша. В поле «Число подкаталогов второго уровня» необходимо ввести количество

подкаталогов второго уровня, которые будут созданы в директории для хранения локального кэша. В поле «Максимальный размер объектов (Кб) необходимо ввести максимальный размер объекта. В поле «Включите кэш-пакет Linux» необходимо установить флажок для включения кэширования пакетов для дистрибутивов Linux. В поле «Включите кэш обновления Windows» необходимо установить флажок для включения кэширования обновлений Windows. Необходимо нажать на кнопку «Применить» (рисунок 315).

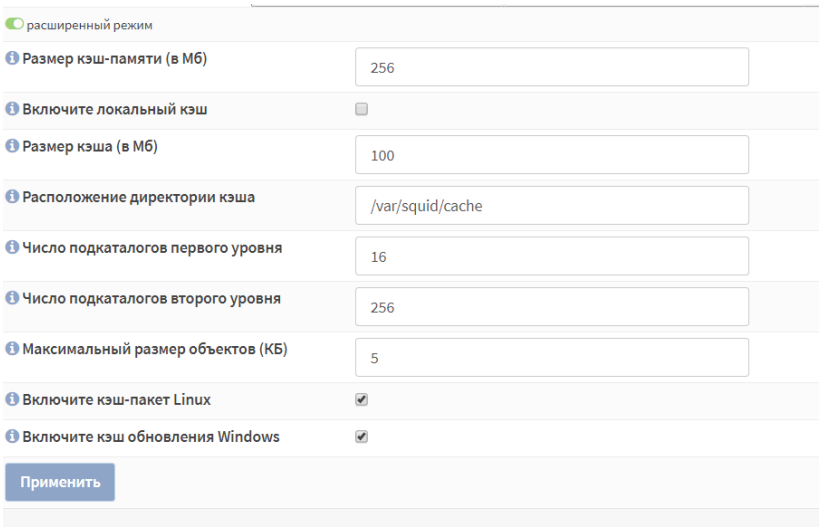


Рисунок 315 — Службы: Прокси: Администрирование (Настройки локального кэша)

В элементе «Настройки управления трафиком» вкладки «Основные настройки» осуществляются основные настройки управления трафиком.

В пункте «Включить управление трафиком» необходимо установить флажок для включения управления трафиком. В поле «Максимальный размер скачиваемых файлов (Кб)» необходимо ввести максимальный размер скачиваемых файлов. В поле «Максимальный размер загружаемых файлов (Кб)» необходимо ввести максимальный размер загружаемых файлов. В поле «Регулирование общей пропускной способности (Кбит/с)» необходимо ввести допустимую общую пропускную способность. В поле «Регулирование общей пропускной способности для хоста (Кбит/с)» необходимо ввести

допустимую пропускную способность для хоста. Необходимо нажать на кнопку «Применить» (рисунок 316).

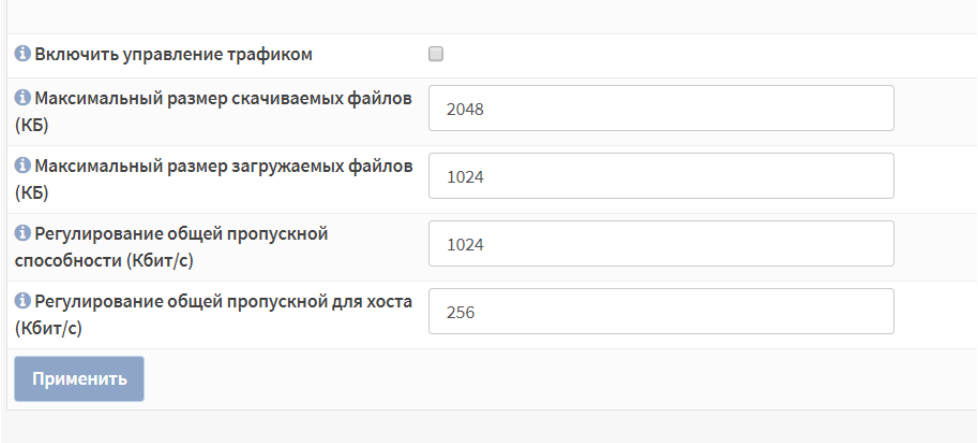


Рисунок 316 — Службы: Прокси: Администрирование: Настройки управления трафиком

Вкладка «Перенаправляющий прокси»

В элементе «Перенаправляющий прокси» вкладки «Перенаправляющий прокси» осуществляются основные настройки перенаправляющего прокси.

В поле «Интерфейсы» необходимо выбрать сетевые интерфейсы, к которым будет привязан перенаправляющий прокси-сервер. В поле «Номер порта прокси-сервера» необходимо ввести порт, который перенаправляющий прокси-сервер будет прослушивать. В поле «Включить прозрачный HTTP-прокси» необходимо установить флажок для включения прозрачного режима прокси-сервера. В поле «Включить проверку SSL необходимо установить флажок для включения режима проверки SSL, который позволяет регистрировать информацию о соединениях HTTPS. В поле «Протоколировать только информацию SNI» необходимо установить флажок для журналирования запрошенных доменов и IP-адресов. В поле «Порт SSL прокси» необходимо ввести порт, который сервис SSL-прокси будет прослушивать. В поле «Использовать Центр Сертификации» необходимо выбрать Центр Сертификации, который необходимо использовать. В поле «SSL no bump sites» необходимо ввести список сайтов, которые не будут проверяться. В поле «Размер кэша SSL» необходимо ввести максимальный

размер для сертификатов SSL. В поле «SSL cert workers» необходимо ввести количество используемых сертификатов SSL. В поле «Разрешить подсети на интерфейсе» необходимо установить флажок для добавления подсетей интерфейсов в список с правами доступа. Необходимо нажать на кнопку «Применить» (рисунок 317).

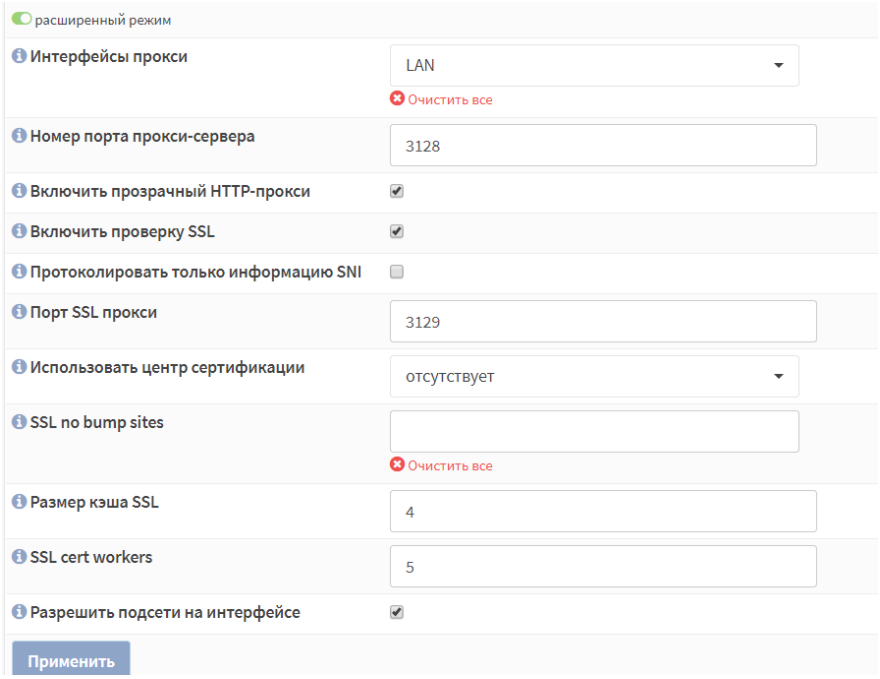


Рисунок 317 — Службы: Прокси: Администрирование: Перенаправляющий прокси

В элементе «Настройки FTP-прокси» вкладки «Перенаправляющий прокси» осуществляются основные настройки FTP-прокси.

В поле «Интерфейсы FTP-прокси» необходимо выбрать интерфейсы, к которым будет привязан прокси-сервер FTP. В поле «Порт FTP-прокси» необходимо ввести порт, который прокси-сервер будет прослушивать. В поле «Включить прозрачный режим» необходимо установить флажок для включения прозрачного режима FTP-прокси. Необходимо нажать на кнопку «Применить» (рисунок 318).

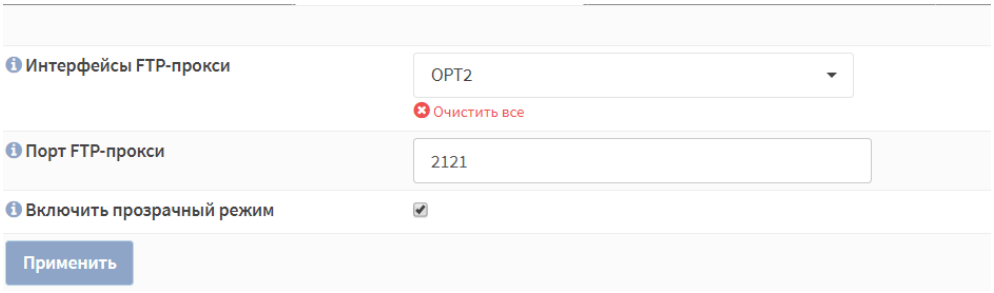


Рисунок 318 — Службы: Прокси: Администрирование: Настройки FTP-прокси

В элементе «Список управления доступом» вкладки «Перенаправляющий прокси» осуществляются основные настройки списка управления доступом.

В поле «Разрешенные подсети» необходимо ввести адреса подсетей, которым будет разрешен доступ к прокси-серверу. В поле «IP-адреса без ограничений» необходимо ввести IP-адреса, которым будет разрешен доступ к прокси-серверу. В поле «Заблокированные IP-адреса хоста» необходимо ввести IP-адреса, которым будет запрещен доступ к прокси-серверу. В поле «Белый список» необходимо ввести доменные адреса, которым будет разрешен доступ к прокси-серверу. В поле «Черный список» необходимо ввести доменные имена, которым будет запрещен доступ. В поле «Блокировать browser/user-agent строки» необходимо ввести user-agent строки, которые будут заблокированы. В поле «Блокировать ответ с конкретным MIME-типом» необходимо ввести ответы MIME-тип, которые будут блокироваться. В поле «Разрешенные TCP-порты» необходимо ввести TCP-порты источника, которым будет разрешен доступ. В поле «Разрешенные SSL-порты» необходимо ввести порты SSL, которым будет разрешен доступ (рисунок 319). Необходимо нажать на кнопку «Применить».

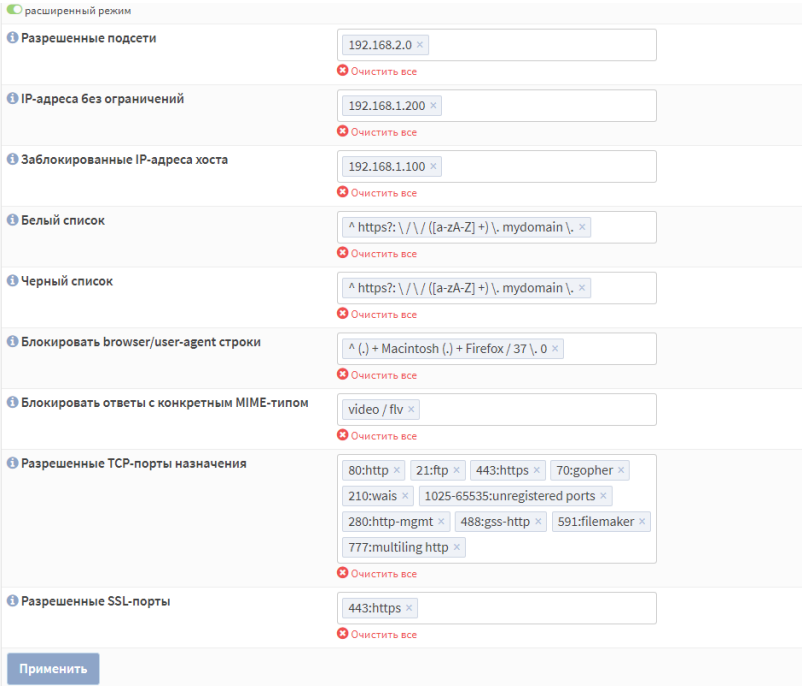


Рисунок 319 — Службы: Прокси: Администрирование: Список управления доступом

В элементе «Настройки ICAP» вкладки «Перенаправляющий прокси» осуществляются основные настройки ICAP.

Протокол ICAP (Internet Content Adaptation Protocol) необходим для осуществления интеграции Squid с сторонними СЗИ.

В пункте «Включить ICAP» необходимо установить флажок для включения ICAP-сервера. В поле «Запрос на изменение URL» необходимо ввести URL, на который должны посылаться REQMOD запросы. В поле «Ответ на изменение URL» необходимо ввести URL, на который должны посылаться REQMOD ответы. В поле «TTL параметры по умолчанию» необходимо ввести TTL параметры. В поле «Отправить IP-адрес по умолчанию» необходимо установить флажок для отправки IP-адреса на ICAP-сервер. В поле «Отправить имя пользователя» необходимо установить флажок для того, чтобы отправить имя пользователя на ICAP-сервер. В поле «Закодировать имя пользователя» необходимо установить флажок для кодировать имена пользователей. В поле «Заголовок имени пользователя» необходимо ввести заголовок, который должен использоваться для отправки имени пользователя. В поле «Включите предпросмотр» необходимо

установить флажок для включения предпросмотра. В поле «Размер в режиме предпросмотра» необходимо ввести размер превью, которое отправится на ICAP сервер. В поле «Список исключений» необходимо ввести целевые домены списка исключений. Необходимо нажать на кнопку «Применить» (рисунок 320).

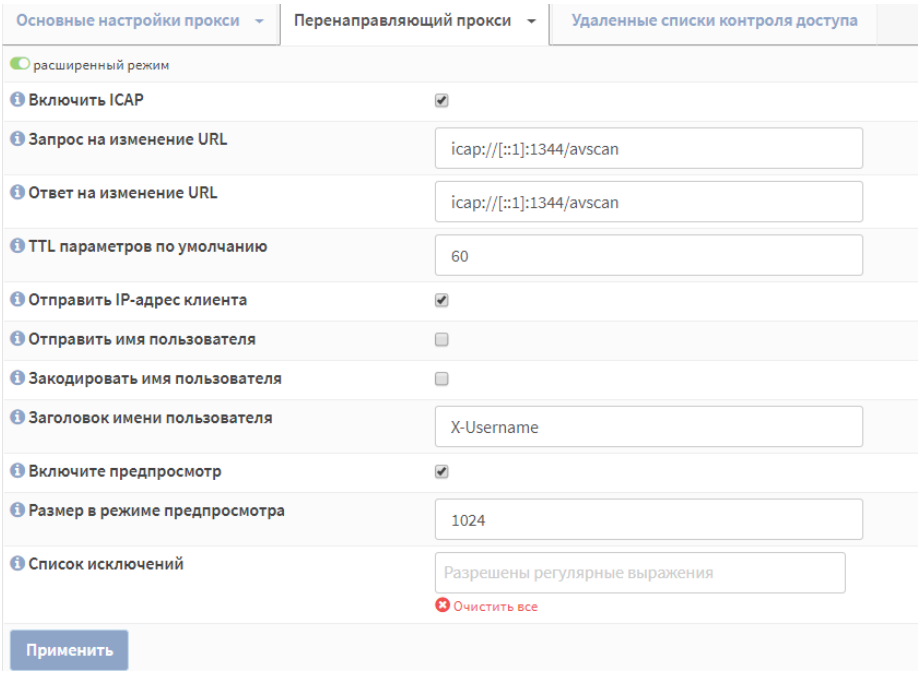


Рисунок 320 — Службы: Прокси: Администрирование: Настройки ICAP

В элементе «Настройки аутентификации» вкладки «Перенаправляющий прокси» осуществляются основные настройки аутентификации.

В поле «Метод аутентификации» необходимо выбрать сервер аутентификации. В поле «Подсказка при аутентификации» необходимо ввести подсказку при аутентификации. В поле «TTL аутентификации (часов)» необходимо ввести срок действия TTL. В поле «Число процессов аутентификации» необходимо ввести число процессов аутентификации, которые могут быть запущены одновременно. Необходимо нажать на кнопку «Применить» (рисунок 321).

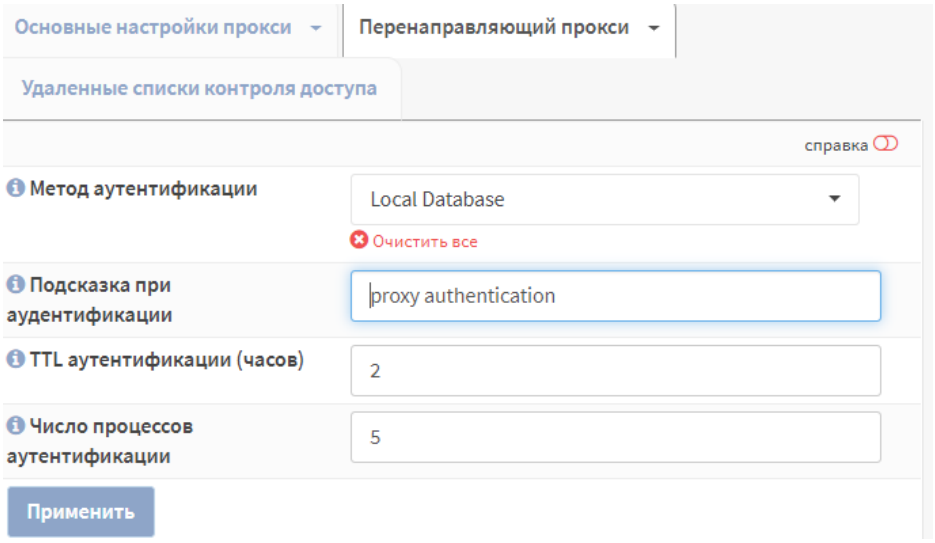


Рисунок 321 — Службы: Прокси: Администрирование: Настройки аутентификации

В элементе «Настройки агента SNMP» вкладки «Перенаправляющий прокси» осуществляются основные настройки агента SNMP.

В пункте «Включение SNMP» необходимо установить флажок для включения агента SNMP. В поле «Порт SNMP» необходимо ввести порт, который Squid будет прослушивать SNMP-запросы. В поле «Пароль SNMP» необходимо ввести пароль доступа к SNMP. Необходимо нажать на кнопку «Применить» (рисунок 322).

Рисунок 322 — Службы: Прокси: Администрирование: Настройки агента SNMP

Вкладка «Автонастройка прокси-сервера»

Категория «Автонастройка прокси-сервера» позволяет настраивать правила прокси-сервера, добавлять несколько прокси-серверов с разными настройками, а также добавлять шаблоны совпадения.

Во вкладке «Правила» отображается таблица правил прокси-сервера со следующей информацией:

– статус правила (включено/выключено);
– описание правила;
– действие правила.

Для редактирования созданного правила необходимо нажать на кнопку напротив правила. Для создания нового правила необходимо нажать на кнопку .

При редактировании правила в поле «Включен» необходимо установить флажок для включения правила. В поле «Описание» необходимо ввести описание правила. В поле «Шаблон совпадения» необходимо выбрать шаблон совпадения. В поле «Тип объединения» необходимо выбрать тип объединения шаблонов совпадения. Поле «Или», если при любом совпадении правило работает, «И», если при всех совпадениях правила работает. В поле «Тип совпадения» необходимо выбрать «Если», если необходимо, чтобы правило работало при соответствии шаблона совпадения, или «Иначе» в противном случае. В поле «Прокси-сервера» необходимо выбрать прокси-сервер, к которому будет применино правило. Для сохранения необходимо нажать на кнопку «Сохранить» (рисунок 323).

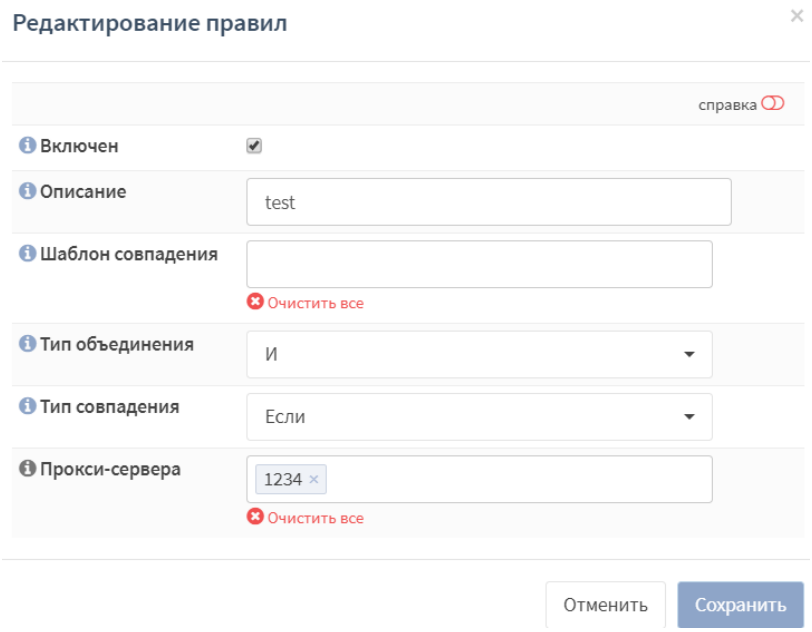


Рисунок 323 — Службы: Прокси: Администрирование: Автонастройка прокси-сервера (Правила)

Во вкладке «Прокси-сервера» отображается таблица прокси-серверов со следующей информацией:

– имя прокси-сервера;

– тип;

– URL;

– описание.

Для редактирования созданного прокси-сервера необходимо нажать на кнопку напротив прокси-сервера. Для создания нового прокси-сервера необходимо нажать на кнопку .

При редактировании прокси-сервера в поле «Имя» необходимо ввести имя прокси-сервера. В поле «Описание» необходимо ввести описание прокси-сервера. В поле «Тип прокси-сервера» необходимо выбрать тип прокси-сервера. В поле «URL» необходимо ввести URL-адрес прокси-сервера. Для сохранения необходимо нажать на кнопку «Сохранить» (рисунок 324).

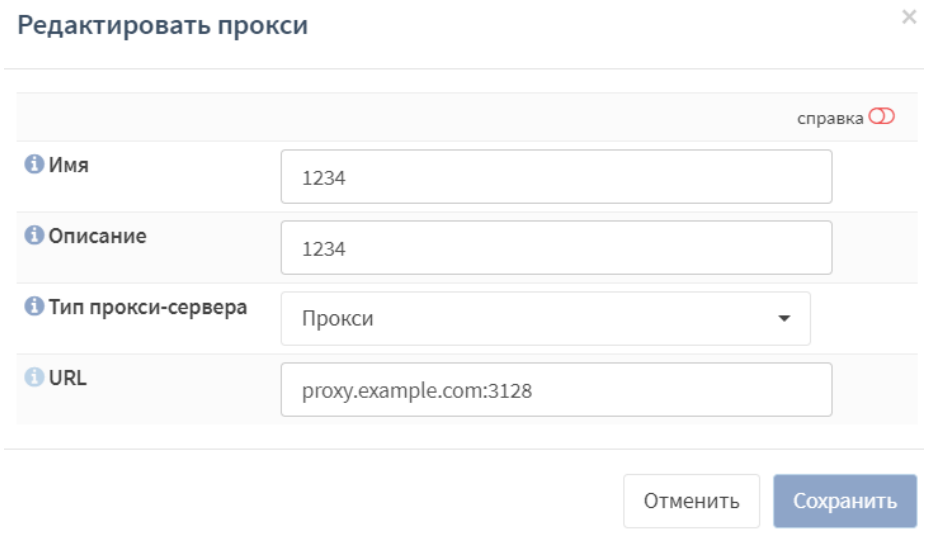


Рисунок 324 — Службы: Прокси: Администрирование: Автонастройка прокси-сервера (Прокси-сервера)

Во вкладке «Шаблон совпадения» отображается таблица шаблонов совпадения со следующей информацией:

– имя шаблона совпадения;
– описание;
– тип совпадения.

Для редактирования созданного шаблона совпадения необходимо нажать на кнопку  напротив шаблона совпадения. Для создания нового шаблона совпадения необходимо нажать на кнопку  .

При редактировании шаблона совпадения в поле «Имя» необходимо ввести имя шаблона совпадения. В поле «Описание» необходимо ввести описание шаблона совпадения. В поле «Отрицание» необходимо установить флажок для отрицания шаблона совпадения. В поле «Тип шаблона совпадения» необходимо выбрать тип шаблона совпадения. В поле «Сеть» необходимо ввести сетевой адрес для шаблона совпадения. В поле «Хост паттерна» необходима ввести хост паттерна. В поле «Шаблон URL» необходимо ввести URL-адрес паттерна. В поле «Уровень домена с» необходимо ввести минимальный уровень домена, для которого действует шаблон совпадения. В поле «Уровень домена до» необходимо ввести максимальный уровень домена, для которого действует шаблон совпадения. В поле «Время начала (час)» необходимо ввести начальное время действия шаблона совпадения. В поле «Время окончания (час)» необходимо ввести время окончания действия шаблона совпадения. В поле «Начало» необходимо ввести месяц начала действия шаблона совпадения. В поле «Окончание» необходимо ввести месяц окончания действия шаблона совпадения. В поле «Начало» необходимо ввести день недели начала действия шаблона совпадения. В поле «Окончание» необходимо ввести день недели окончания действия шаблона совпадения. Для сохранения необходимо нажать на кнопку «Сохранить» (рисунок 325).

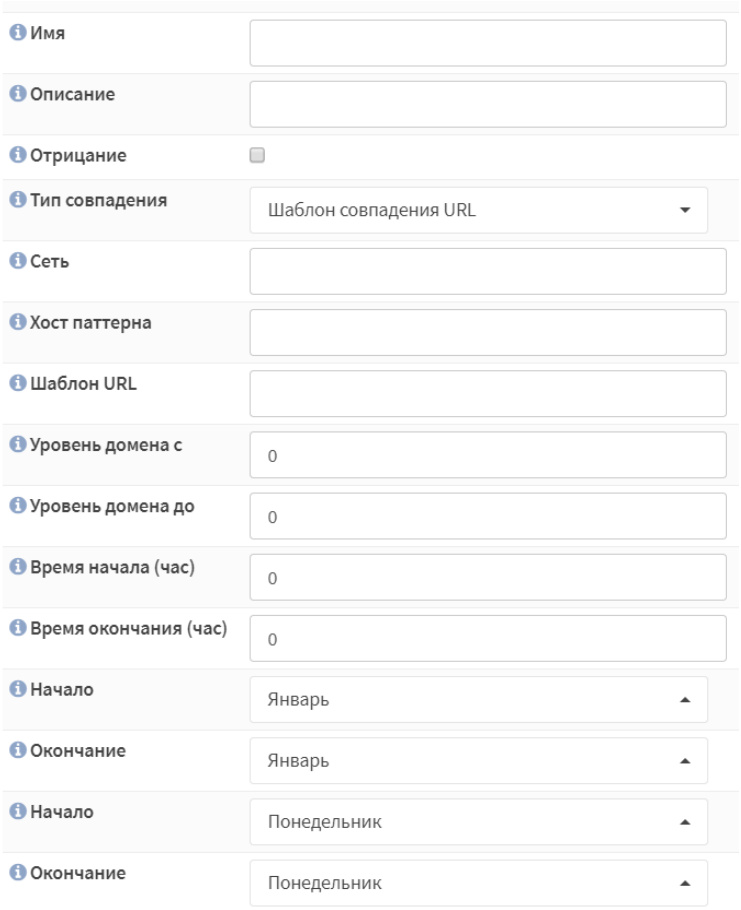


Рисунок 325 — Службы: Прокси: Администрирование: Автонастройка прокси-сервера (Шаблон совпадения)

Вкладка «Удаленные списки контроля доступа»

В категории «Удаленные списки контроля доступа» отображаются списки доступа в виде таблицы. Таблица содержит следующие данные:

- состояние списка (включен/выключен);
- имя списка;
- URL;
- описание.

Также раздел позволяет создать новый список доступа и удалить/редактировать существующие списки. Для редактирование существующего необходимо нажать на кнопку напротив списка. Для создания нового списка необходимо нажать на кнопку .

При редактировании списка в поле «Включен» необходимо установить флажок для включения списка. В поле «Имя файла» необходимо ввести название списка. В поле «URL» необходимо ввести URL для загрузки черного списка. В поле «Имя пользователя (необязательно» необходимо ввести имя пользователя. В поле «Пароль (необязательно)» необходимо ввести пароль пользователя. В поле «Категория (если доступны)» необходимо выбрать категории списков. В поле «ssl ignore cert» необходимо установить флажок для игнорирования проверку SSL-сертификата. В поле «Описание» необходимо ввести описание списка и необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 326).

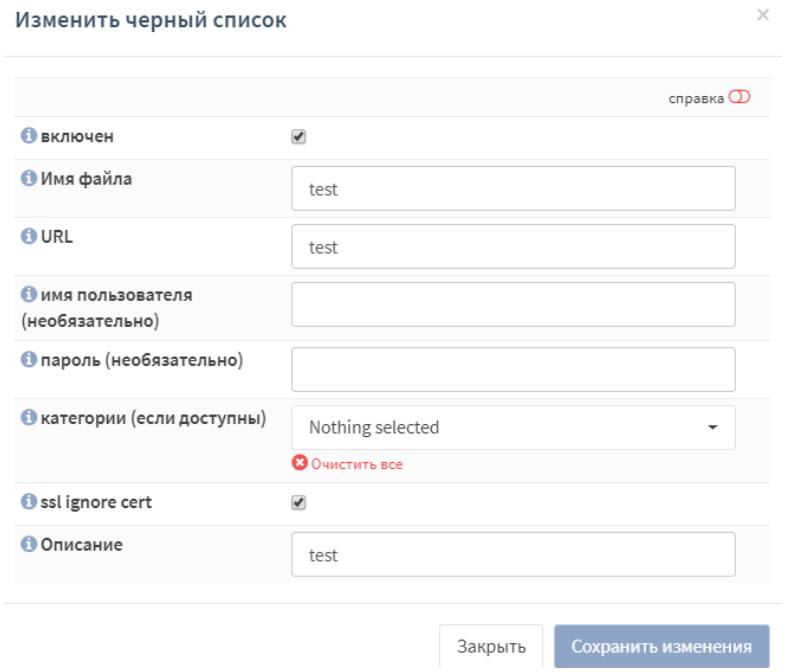


Рисунок 326 — Службы: Прокси: Администрирование: Удаленные списки контроля доступа

Также раздел позволяет скачать списки контроля доступа, скачать и применить списки контроля доступа, запланировать с помощью планировщика Cron работы списков контроля доступа и применить добавленные списки, нажав на соответствующие кнопки.

10.6.2. Категория «Журнал»

Категория «Журнал» позволяет просматривать журнал прокси-сервера (рисунок 327).

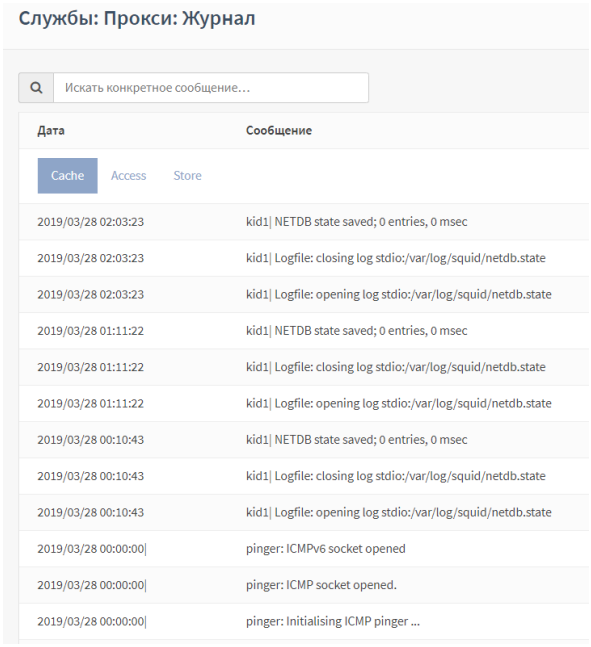


Рисунок 327 — Службы: Прокси: Журнал

11. Пользовательские сценарии

11.1. Настройка Netflow

Для настройки Netflow необходимо перейти в поле «Анализ» - «NetFlow» (рисунок 328).

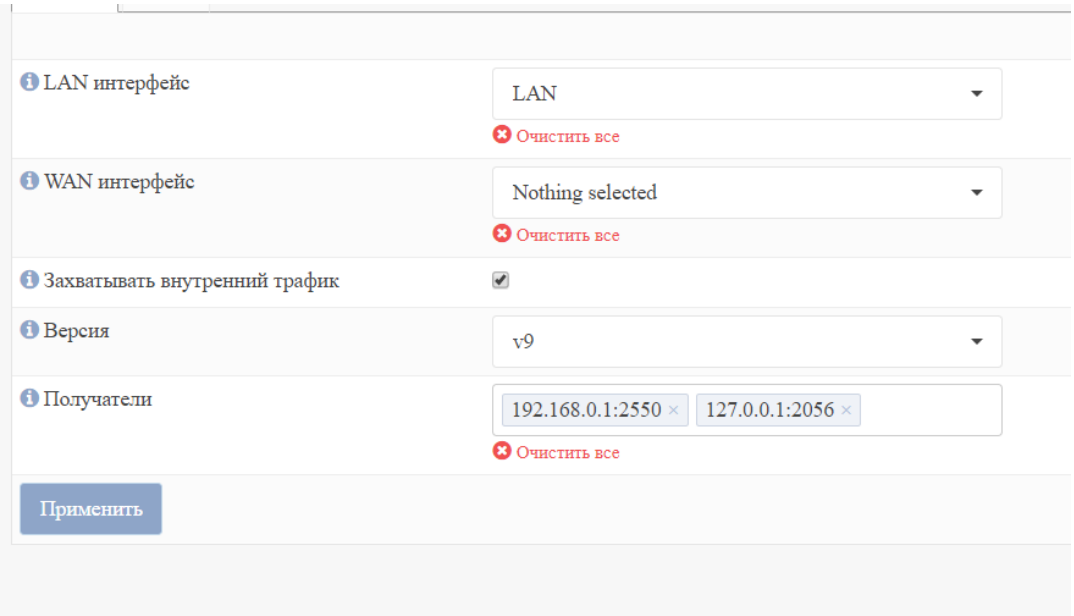


Рисунок 328 — Настройка Netflow

В поле «LAN интерфейс необходимо выбрать все интерфейсы, из которых необходимо собирать данные. В поле «WAN интерфейс» необходимо выбрать все интерфейсы, из которых необходимо экспортировать данные. Для анализа локального трафика необходимо поставить «галочку» напротив поля «Захватывать внутренний трафик». В зависимости от протокола, необходимо выбрать «v5» или «v9» в поле «Версия» («v5» не поддерживает IPv6).

В поле «Получатели» необходимо добавить получателей в формате [IP-адрес: порт]. Внутренний IP-адрес будет добавлен автоматически, если выбрано «Захватывать внутренний трафик». Необходимо нажать на кнопку «Применить».

Необходимо подождать сбор трафика Netflow в зависимости от активности трафика. На удаленном компьютере появится статистика, собранная Netflow (рисунок 329).

```
user@user-VirtualBox:~$ flow-cat /var/log/flow/ft-v05.2019-11-14.161501+0300|flow-print -f5
Start            End              Sif   SrcIPaddress    SrcP  DIf   DstIPaddress    DstP    P Fl Pkts       Octets

1114.16:12:07.516 1114.16:12:07.516 0     192.168.1.1     56531 1     192.168.1.99    2550  17  0  1          1492
1114.16:12:09.516 1114.16:12:09.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  1          100
1114.16:12:43.516 1114.16:12:46.516 1     192.168.1.201   10168 1     192.168.1.52    80    6   2  2          104
1114.16:12:43.516 1114.16:12:46.516 1     192.168.1.201   10169 1     192.168.1.52    80    6   2  2          104
1114.16:12:54.516 1114.16:12:54.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  1          148
1114.16:13:13.516 1114.16:13:13.516 1     192.168.1.99    44922 3     192.168.1.1     2550  17  0  1          100
1114.16:13:14.516 1114.16:13:14.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  1          100
1114.16:13:45.516 1114.16:13:48.516 1     192.168.1.201   60424 3     239.255.255.250 1900  17  0  4          804
1114.16:14:23.516 1114.16:14:23.516 1     192.168.1.99    44922 3     192.168.1.1     2550  17  0  1          148
1114.16:14:19.516 1114.16:14:24.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  2          200
1114.16:14:47.516 1114.16:14:47.516 1     192.168.1.99    44922 3     192.168.1.1     2550  17  0  1          292
1114.16:14:47.516 1114.16:14:47.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  1          292
1114.16:15:00.516 1114.16:15:09.516 1     192.168.1.201   10182 3     192.168.1.1     22    6   2  3          156
1114.16:15:14.516 1114.16:15:14.516 1     192.168.1.201   54241 3     224.0.0.252     5355  17  0  1          50
1114.16:14:29.516 1114.16:15:43.516 0     192.168.1.1     80    1     192.168.1.201   10179 6   3  561        807611
1114.16:15:45.516 1114.16:15:48.516 1     192.168.1.201   56393 1     239.255.255.250 1900  17  0  4          804
1114.16:15:57.516 1114.16:15:57.516 1     192.168.1.99    44922 3     192.168.1.1     2550  17  0  1          148
1114.16:15:57.516 1114.16:15:57.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  1          148
1114.16:16:22.516 1114.16:16:22.516 1     192.168.1.99    44922 3     192.168.1.1     2550  17  0  1          148
1114.16:16:22.516 1114.16:16:22.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  1          148
1114.16:16:28.516 1114.16:16:28.516 0     192.168.1.1     80    1     192.168.1.201   10179 6   0  1          40
1114.16:16:42.516 1114.16:16:57.516 1     192.168.1.99    44922 3     192.168.1.1     2550  17  0  2          200
1114.16:16:42.516 1114.16:16:57.516 1     192.168.1.99    43434 3     192.168.1.1     2550  17  0  2          200
1114.16:14:29.516 1114.16:17:26.516 1     192.168.1.201   10179 3     192.168.1.1     80    6   3  115        12827
1114.16:17:13.516 1114.16:17:26.516 0     192.168.1.1     80    1     192.168.1.201   10179 6   0  2          80
1114.16:17:43.516 1114.16:17:43.516 0     192.168.1.1     0     1     192.168.1.201   0     1   0  1          60
1114.16:17:43.516 1114.16:17:43.516 1     192.168.1.201   0     3     192.168.1.1     0     1   0  1          60
1114.16:17:26.516 1114.16:18:00.516 1     192.168.1.201   10198 3     192.168.1.1     80    6   3  46         7909
1114.16:17:26.516 1114.16:18:00.516 1     192.168.1.201   10196 3     192.168.1.1     80    6   3  110        11678
1114.16:17:26.516 1114.16:18:00.516 0     192.168.1.1     80    1     192.168.1.201   10198 6   3  185        251388
1114.16:17:26.582 1114.16:18:00.582 1     192.168.1.201   10197 3     192.168.1.1     80    6   3  7          1679
1114.16:17:26.582 1114.16:18:00.582 1     192.168.1.201   10195 3     192.168.1.1     80    6   3  7          1678
1114.16:17:26.582 1114.16:18:00.582 0     192.168.1.1     80    1     192.168.1.201   10196 6   3  500        719513
1114.16:17:26.582 1114.16:18:00.582 1     192.168.1.201   10193 3     192.168.1.1     80    6   3  33         3870
1114.16:17:26.582 1114.16:18:00.582 0     192.168.1.1     80    1     192.168.1.201   10197 6   3  7          944
1114.16:17:26.582 1114.16:18:00.582 1     192.168.1.201   10194 3     192.168.1.1     80    6   3  18         4416
1114.16:17:26.582 1114.16:18:00.582 0     192.168.1.1     80    1     192.168.1.201   10195 6   3  7          944
1114.16:17:26.582 1114.16:18:00.582 0     192.168.1.1     80    1     192.168.1.201   10193 6   3  147        206308
```

Рисунок 329 — Экспорт данных Netflow

11.2. Кэширующий прокси (Squid)

11.2.1. Кэширующий прокси: установка

Включение/отключение

Для включения прокси-сервера, необходимо зайти в поле «Службы» - «Прокси» - «Администрирование», установить флажок «Включить прокси» и нажать «Применить». По умолчанию используется прокси-сервер с пользовательской аутентификацией на основе локальной базы данных пользователей и выполняется на порту 3128 интерфейса LAN.

Изменение прокси-интерфейсов

Для изменения интерфейсов (подсетей) необходимо перейти во вкладку «Перенаправляющий прокси» и добавить/удалить интерфейсы в поле «Интерфейсы прокси». После добавления необходимо нажать на кнопку «Применить».

Изменение порта для прослушивания

По умолчанию прокси-сервер будет прослушивать порт 3128, возможно изменить его, перейдя во вкладку «Перенаправляющий прокси». Далее необходимо ввести значение порта в поле «Порт SSL прокси». После внесения изменений необходимо нажать на кнопку «Применить».

Включение кэша

Для включения кэширования, необходимо нажать на кнопку стрелку около вкладки «Основные настройки прокси», чтобы просмотреть выпадающий список и нажать «Настройки локального кэша» (рисунок 330).

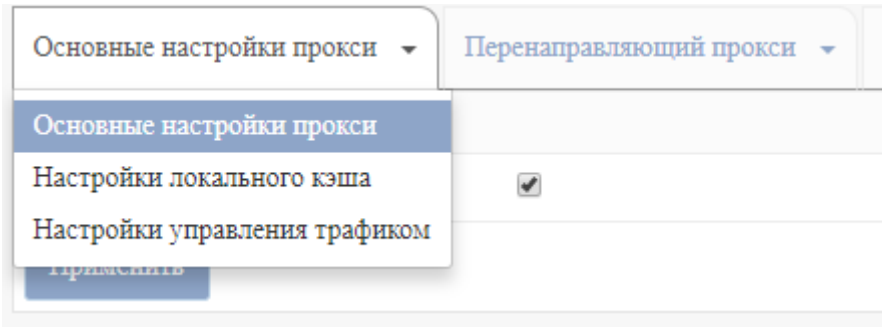


Рисунок 330 — Включение кэша

Необходимо установить флажок напротив поля «Включить локальный кэш» и нажать «Применить».

Поскольку кэш не создается по умолчанию, необходимо остановить и запустить службу в разделе «Система» - «Диагностика» - «Службы», это обеспечит правильное создание кэша и нажать ▶ напротив squid.

Изменение метода проверки подлинности

Необходимо нажать на стрелку рядом со вкладкой «Перенаправляющий прокси», чтобы отобразить выпадающий список и выбрать «Настройки аутентификации». Затем необходимо выбрать требуемый (требуемые) аутентификатор (-ы) в поле «Метод аутентификации» или нажать «Очистить все», если не используется аутентификация.

В зависимости от серверов проверки подлинности, которые настроены в разделе «Система» - «Доступ» - «Серверы», возможно выбрать один или

несколько из следующих параметров:

– нет аутентификации (оставить поле пустым);

– локальная база данных пользователей;

– LDAP;

– Radius.

FTP-прокси

Для включения FTP-прокси, необходимо нажать на стрелку рядом со вкладкой «Перенаправляющий прокси», чтобы отобразить выпадающий список. Далее необходимо выбрать «Настройка FTP-прокси» и один или несколько интерфейсов в поле «Интерфейсы FTP-прокси» и нажать «Применить».

Список контроля доступа

Для настройки списка управления доступом необходимо нажать на стрелку рядом со вкладкой «Перенаправляющий прокси» и выбрать «Список управления доступом». Эта вкладка позволяет:

– настроить список разрешенных подсетей в поле «Разрешенные подсети» (по умолчанию допускаются интерфейсы прокси);

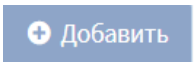
– добавить IP-адреса для ограничения доступа в поле «IP-адреса без ограничений» (отсутствие аутентификации и черного списка для этих IP-адресов);

– добавить IP-адрес заблокированных хостов в поле «Заблокированные IP-адреса хоста» (запрещает клиенту использовать прокси-сервер);

– выбрать белый список в поле «Белый список» (необходимо нажать на кнопку (i), чтобы увидеть примеры, белый список преобладает над черным списком);

– выбрать черный список в поле «Черный список» (если этого нет в белом списке, блокирует трафик, основанный на регулярном выражении).

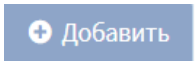
Правило межсетевого экрана: подключение через прокси-сервер

Для подключения через прокси-сервер, необходимо добавить правило межсетевого экрана. Для этого необходимо перейти в раздел «Межсетевой экран» - «Правила» - «LAN» (если пользователи и прокси-сервер находятся в локальной) и нажать кнопку 

. Необходимо добавить правило в соответствии с таблицей (таблица 11) в начало списка правил и нажать кнопку «Сохранить», а далее кнопку «Применить изменения».

Таблица 11 — Правило межсетевого экрана

Настройки	**Значения**
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTP
Категория	Подключение прокси-сервера
Описание	Блокировать HTTP-запрос

Далее необходимо добавить еще одно правило, которое будет блокировать доступ к HTTPS. Для этого необходимо нажать на кнопку 

и заполните поля в соответствии с таблицей (таблица 12). Для сохранения необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

Таблица 12 — Правило блокирования доступа к HTTPS

Настройки	Значения
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTPS
Категория	Подключение прокси-сервера
Описание	Блокировать HTTPS-запрос

Настройка веб-браузера (Firefox)

Для настройки веб-браузера, чтобы использовать его с прокси-сервером, необходимо перейти к настройкам сети и настроить прокси-сервер в веб-браузере, например, Firefox (рисунок 331). В группе настроек «Configure Proxies to Access the Internet» необходимо выбрать «Manual proxy Configration» и ввести в поле «HTTP Proxy» значение IP-адреса ПК «InfoWatch ARMA Industrial Firewall» (например, 192.168.1.1, в поле «Port» необходимо ввести порт ПК «InfoWatch ARMA Industrial Firewall» (например, 3128). В поле «No Proxy for» необходимо ввести подсети, которые будут не проксироваться, например, ввести «Localhost, 127.0.0.1, 192.168.1.0/24».

Для других браузеров необходимо воспользоваться документацией к браузерам для настройки прокси сервера. Значения необходимо подставлять, руководствуясь установленным при настройке прокси на ПК «InfoWatch ARMA Industrial Firewall».

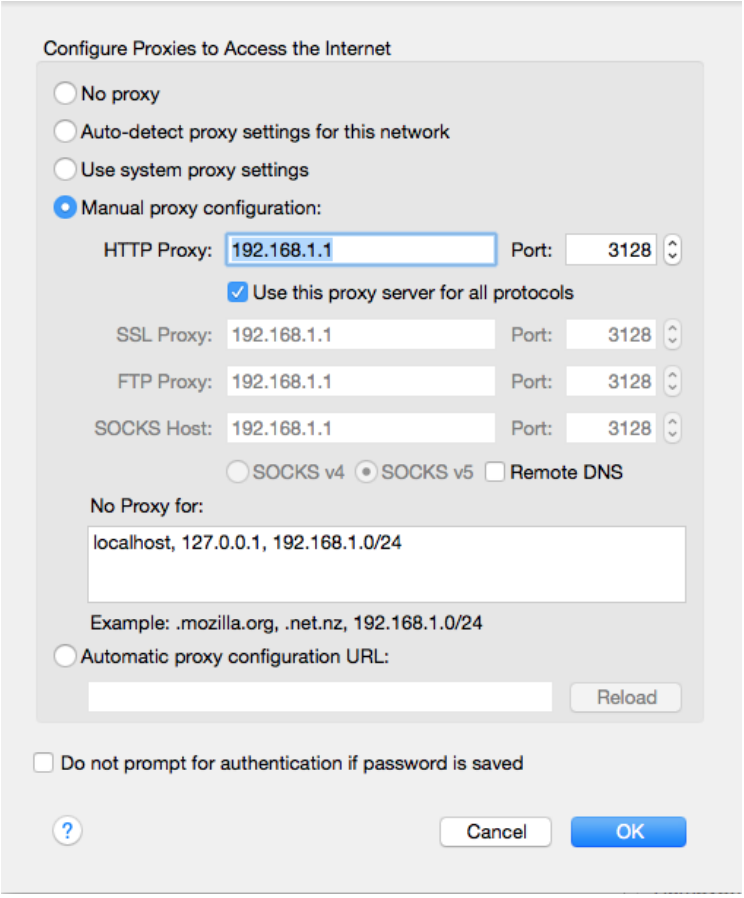


Рисунок 331 — Настройка браузера

11.2.2. Настройка веб-фильтрации

Веб-фильтрация на основе категорий в ПК «InfoWatch ARMA Industrial Firewall» выполняется с использованием встроенного прокси-сервера и одного из свободно доступных черных списков.

Отключение аутентификации

Для отключения аутентификации необходимо перейти в поле «Служба» - «Прокси» - «Администрирование» - «Перенаправляющий прокси» - «Настройки аутентификации». В поле «Метод аутентификации» необходимо нажать на кнопку «Очистить все», чтобы отключить аутентификацию пользователя и нажать «Применить», чтобы сохранить изменения.

Настройка черного списка

Для настройки черного списка необходимо нажать на вкладку «Списки удаленного контроля доступа». Затем нажать на + в нижнем правом углу,

чтобы добавить новый список.

Появится экран, в который необходимо ввести следующие данные в соответствии с таблицей (таблица 13).

Таблица 13 — Настройка черного списка

Настройки	**Значения**	**Комментарий**
Включено	Включено	Включить выключить
Имя файла	UT1	Необходимо выбрать уникальное имя файла
URL	(скопируйте/вставьте URL-адрес)	URL-адрес черного списка
Категории	(Оставить пустым)	Если оставить пустым, будет выбран полный список
Описание	Веб фильтр UT1	Ваше описание

Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

Загрузка категории

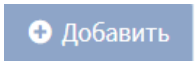
Далее необходимо нажать на кнопку «Скачать списки контроля доступа». Стоит учитывать, что для успешного выполнения данного шага необходимо, чтобы в ПК «InfoWatch ARMA Industrial Firewall» был настроенным порт WAN с доступом в Интернет.

Включение прокси

Для включения прокси-сервера, необходимо перейти в поле «Прокси» - «Администрирование» и установить флажок напротив поля «Включить прокси», далее нажать «Применить». Прокси-сервер будет привязан к локальной сети и порту 3128.

Включение прокси-сервера может занять некоторое время.

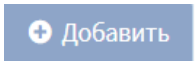
Отключение прокси-сервера

Для подключения через прокси-сервер, необходимо добавить правило межсетевого экрана. Для этого необходимо перейти в раздел «Межсетевой экран» - «Правила» - «LAN», нажать 

и заполнить поля в соответствии с таблицей (таблица 14).

Таблица 14 — Добавление правила

Настройки	**Значения**
Действие	Блокирование
Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTP
Категория	Подключение прокси-сервера
Описание	Блокировать HTTP-запрос

Необходимо добавить еще одно правило, которое будет блокировать доступ к HTTPS. Для этого необходимо нажать на кнопку 

и заполнить поля в соответствии с таблицей (таблица 15). Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

Таблица 15 — Блокирование доступа к HTTPS

Настройки	**Значения**
Действие	Блокирование

Интерфейс	LAN
Протокол	TCP/UDP
Отправитель	LAN сеть
Диапазон портов назначения	HTTPS
Категория	Подключение прокси-сервера
Описание	Блокировать HTTPS-запрос

11.3. Встроенная система предотвращения вторжений

11.3.1. Настройка системы обнаружения вторжений

Чтобы включить IDS, необходимо перейти в поле «Обнаружение вторжений» - «Администрирование» и установить флажок напротив поля «Включен». В примере используется интерфейс WAN, руководствуясь тем, что ПК будет связан с подключением к внешней сети (рисунок 332).

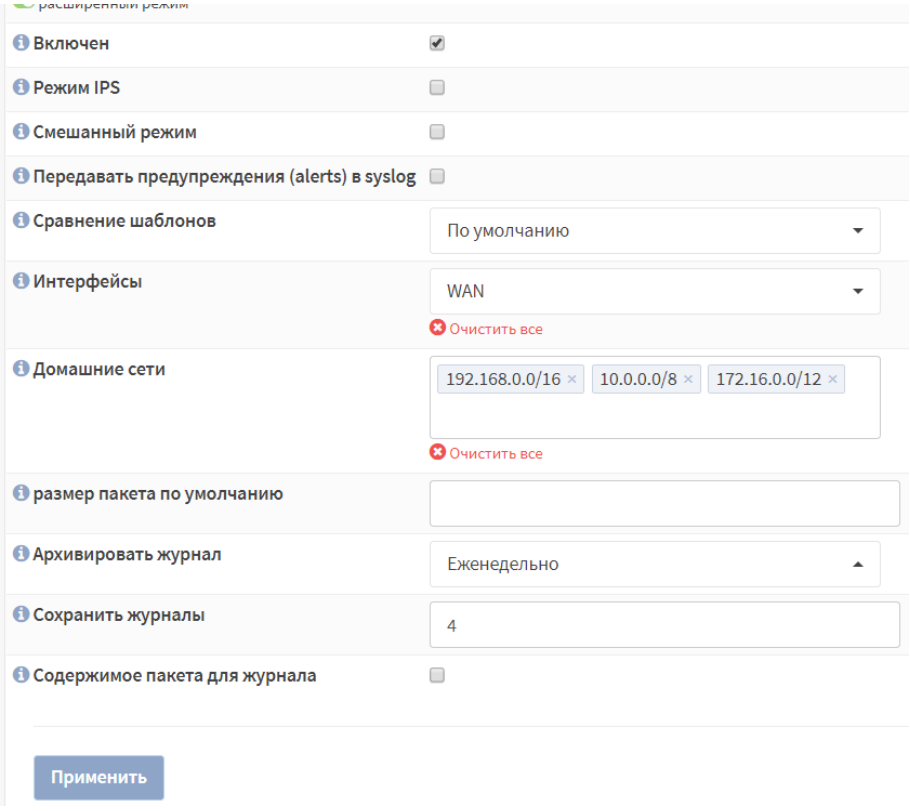


Рисунок 332 — Настройка обнаружения вторжений в режиме IDS

Необходимо нажать на кнопку «Применить» в нижней части формы.

11.3.2. Настройка системы предотвращения вторжений

Чтобы включить IPS, необходимо перейти в поле «Обнаружение вторжений» - «Администрирование» и установить флажок напротив поля «Включен» и «Режим IPS». В примере используется интерфейс WAN, руководствуясь тем, что ПК будет связан с подключением к внешней сети (рисунок 333).

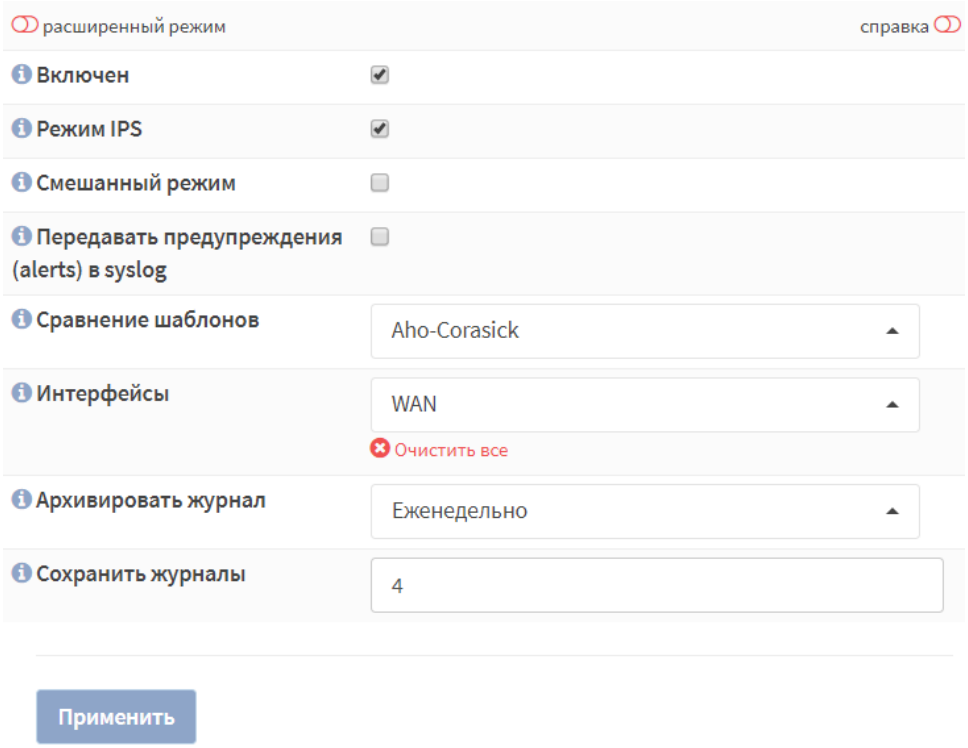


Рисунок 333 — Настройка обнаружения вторжений в режиме IPS

Необходимо нажать на кнопку «Применить» в нижней части формы.

Для выбора правил необходимо перейти в поле «Обнаружение вторжений» - «Администрирование» - «Правила». Для включения правила необходимо нажать на флажок напротив выбранного правила в поле таблицы «Информация/Включен» (рисунок 334).

1	Предупреждение	files.rules	##none##	FILEEXT JPG file claimed		
3	Предупреждение	files.rules	##none##	FILEEXT BMP file claimed		
6	Предупреждение	files.rules	##none##	FILESTORE jpg		
8	Предупреждение	files.rules	##none##	FILESTORE pdf		
9	Предупреждение	files.rules	##none##	FILEMAGIC pdf		
10	Предупреждение	files.rules	##none##	FILEMAGIC jpg(1)		
11	Предупреждение	files.rules	##none##	FILEMAGIC jpg(2)		
12	Предупреждение	files.rules	##none##	FILEMAGIC short		
15	Предупреждение	files.rules	##none##	FILE store all		

Рисунок 334 — Правила

11.4. Задание и синхронизация времени по протоколу NTP

Для задания и синхронизации времени по протоколу NTP необходимо из веб-интерфейса в разделе «Службы» - «Синхронизация времени» - «Общие настройки» задать поле «Серверы времени» (по крайней мере один NTP сервер). После этого, необходимо сохранить конфигурацию путем нажатия на кнопку «Сохранить» внизу текущей страницы (рисунок 335).

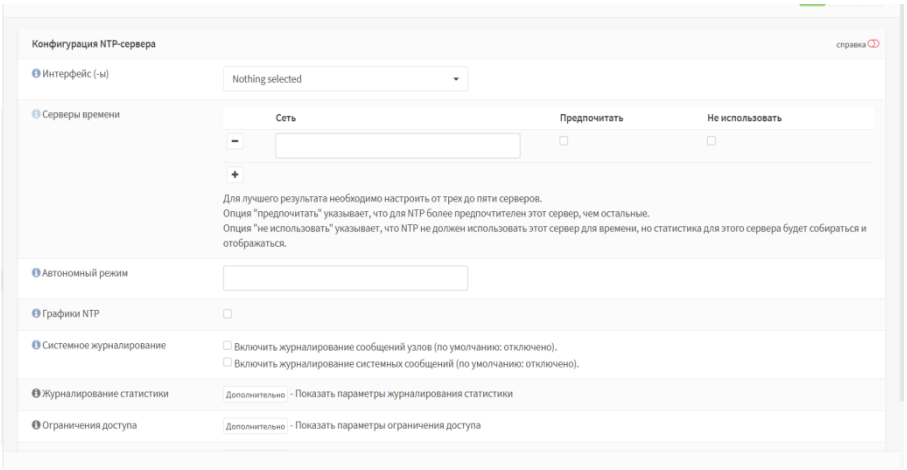


Рисунок 335 — Задание и синхронизация времени по протоколу NTP

В результате, время системы должно синхронизироваться с временем на NTP сервера. Поддерживается только NTP версии 4.

11.5. Настройки экспорта событий по SYSLOG (интеграция с SIEM -системами)

Из графического интерфейса перейти в раздел «Система» - «Настройки» - «Журналирование». В поле «Удаленные syslog-серверы»

необходимо ввести значение IP адреса сервера, агрегирующего syslog. В поле «Типы отправляемых событий», необходимо отметить группы событий для отправки. После этого, необходимо сохранить конфигурацию путем нажатия на кнопку «Сохранить» внизу текущей страницы (рисунок 336).

Далее необходимо проверить наличие разрешающего правила для LAN интерфейса. Для этого необходимо перейти в «Межсетевой экран» - «Правила» - «LAN» и убедиться в наличие разрешающих правил.

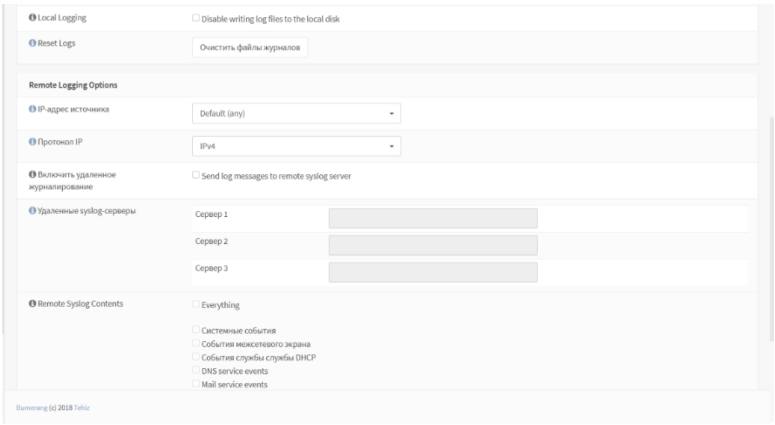


Рисунок 336 — Экспорт событий по SYSLOG

В результате, события должны отправляться на удаленный syslog сервер.

11.6. Изменение возможностей (прав) пользователей

Для редактирования прав группы пользователей необходимо перейти в раздел «Система» - «Доступ» - «Группы». Для редактирования группы нажать на кнопку  «Редактировать группу» и указать необходимые в поле «Присвоенные привилегии» (рисунок 337).

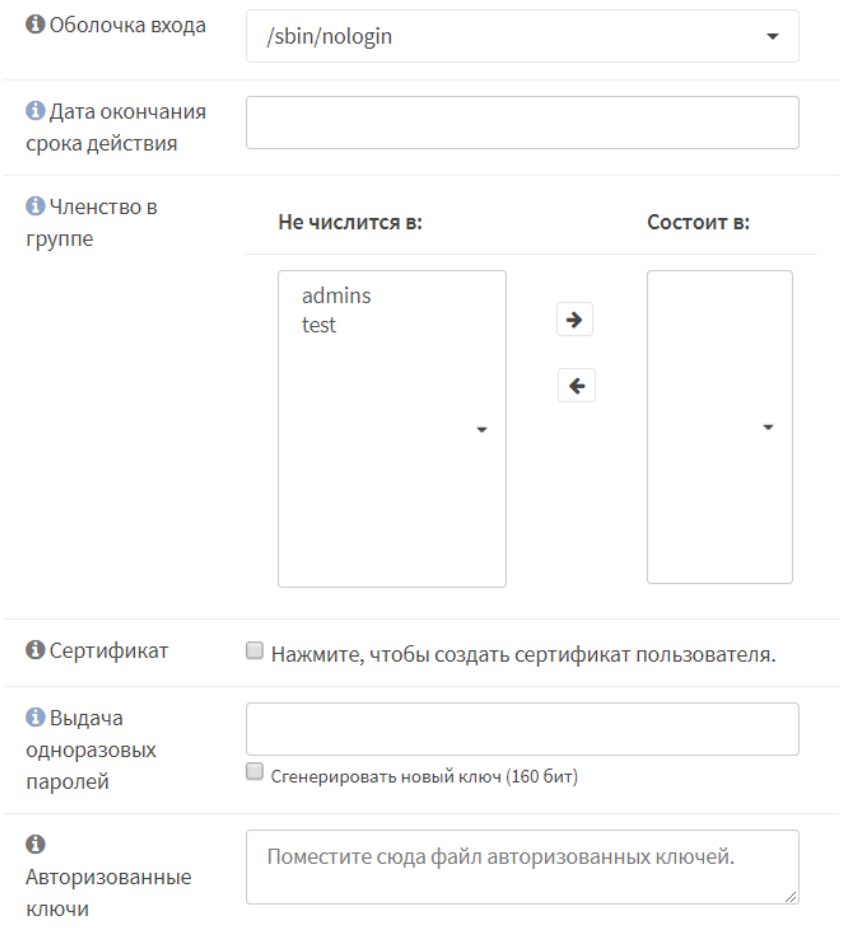


Рисунок 337 — Изменение возможностей (прав) пользователей

11.7. Создание нового пользователя

Для создания нового пользователя необходимо перейти в разделе «Система» - «Пользователи» и нажать кнопку 

. В появившемся меню заполняются данные для нового пользователя. Обязательные поля для заполнения:

– «Имя пользователя» (необходимо ввести имя пользователя);

– «Пароль» (необходимо ввести пароль для входа в учетную запись пользователя в первом поле и повторить этот пароль во втором поле).

После внесения изменений необходимо нажать на кнопку «Сохранить». (рисунок 338).

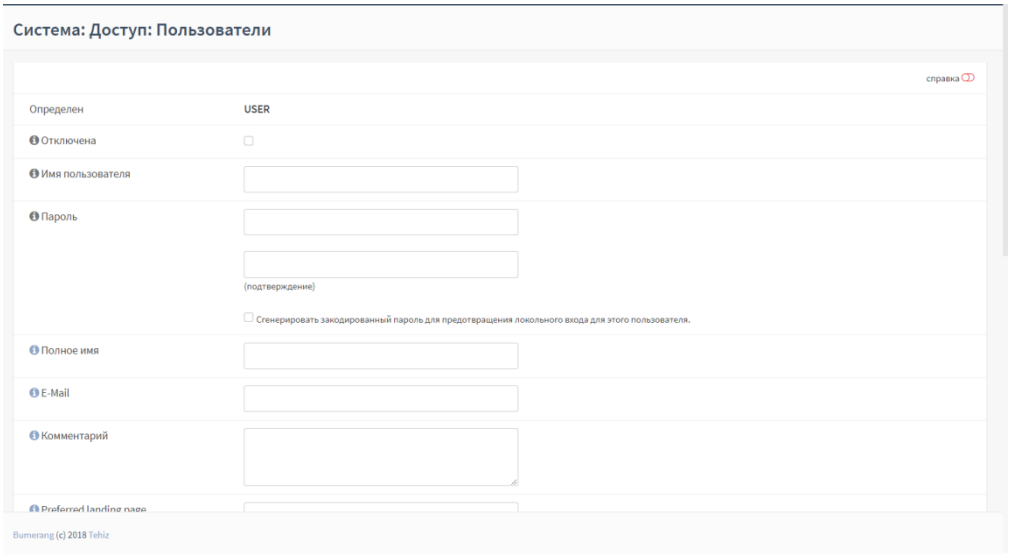


Рисунок 338 — Создание нового пользователя

11.8. Выбор совокупности регистрируемых событий

Для выбора регистрируемых событий для журналирования межсетевого экрана необходимо перейти в раздел «Система» - «Настройки» - «Журналирование» (рисунок 339).

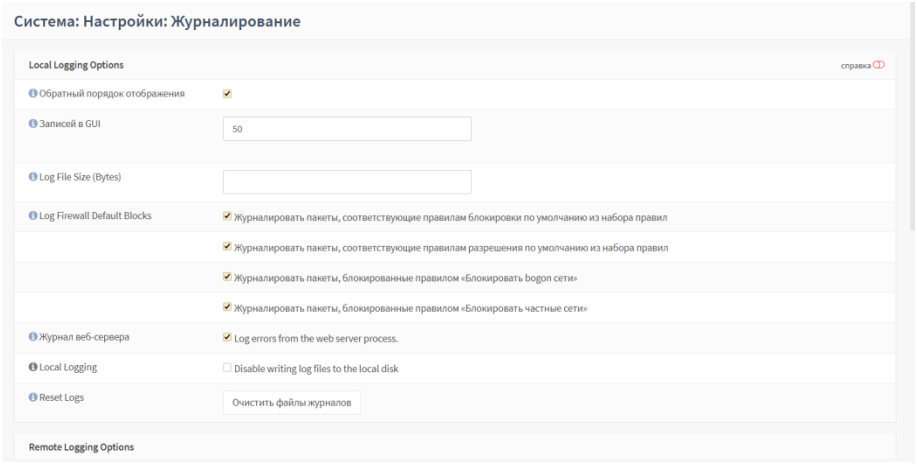


Рисунок 339 — Выбор регистрируемых событий

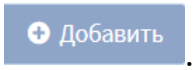
Данная категория позволяет выбрать события, которые необходимо журналировать, генерируемые межсетевым экраном, такие как:

– журналировать пакеты, соответствующие правилам блокировки по умолчанию из набора правил;

– журналировать пакеты, соответствующие правилам разрешения (pass) по умолчанию из набора правил.

Для выбора событий для журналирования необходимо установить флажок напротив и нажать кнопку «Сохранить».

Для настройки журналирования пакетов, соответствующих правилам разрешения (pass) по умолчанию из набора правил, необходимо оставить изначальный (после установки) список правил межсетевого экранирования.

Дополнительно предусмотрена возможность журналировать пакеты, соответствующие правилам межсетевого экранирования. Для этого необходимо создать правило в поле «Межсетевой экран» - «Правила» - «WAN» и добавить правило путем нажатия на кнопку 

. В настройках правила обязательно необходимо задать поля «Отправитель», «Действие», «Протокол» и установить флажок напротив поля «Журналировать пакеты, соответствующие правилу», нажать кнопку «Сохранить», а затем кнопку «Применить изменения» (рисунок 340).

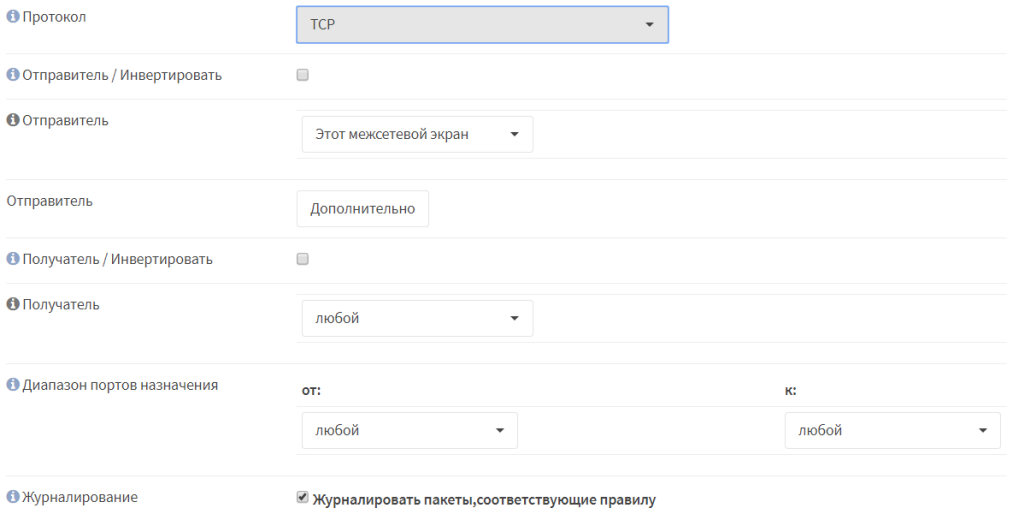


Рисунок 340 — Добавление правила МЭ

Для включения журналирования действий пользователей необходимо перейти в «Система» - «Настройки» - «Администрирование» и поставить флажок в поле «Журналирование доступа», для сохранения необходимо нажать кнопку «Сохранить» внизу страницы.

11.9. Фильтрация промышленных протоколов АСУТП

ПК «InfoWatch ARMA Industrial Firewall» позволяет производить анализ промышленных протоколов АСУТП, осуществлять разбор по функциям и полям этих протоколов, отображать собранную информацию. В текущей версии ПК «InfoWatch ARMA Industrial Firewall» имеется возможность создания правил обнаружения или блокирования пакетов следующих промышленных протоколов:

- Modbus TCP;
- IEC 60870-5-104;
- S7comm;
- ENIP/CIP;
- OPC UA;
- OPC DA;
- UMAS;
- MMS;
- GOOSE.

11.9.1. Настройка протокола Modbus TCP

Описание настройки параметров правила по протоколу Modbus TCP описано в подразделе 5.2.1 настоящего руководства.

11.9.2. Настройка протокола IEC 60870-5-104

Описание настройки параметров правила по протоколу IEC 60870-5-104 описано в подразделе 5.2.2 настоящего руководства.

11.9.3. Настройка протокола S7comm

Описание настройки параметров правила по протоколу S7comm описано в подразделе 5.2.3 настоящего руководства.

11.9.4. Настройка протокола ENIP/CIP

Описание настройки параметров правила по протоколу ENIP/CIP описано в подразделе 5.2.4 настоящего руководства.

11.9.5. Настройка протокола OPC UA

Описание настройки параметров правила по протоколу OPC UA описано в подразделе 5.2.5 настоящего руководства.

11.9.6. Настройка протокола OPC DA

Описание настройки параметров правила по протоколу OPC DA описано в подразделе 5.2.6 настоящего руководства.

11.9.7. Настройка протокола UMAS

Описание настройки параметров правила по протоколу UMAS описано в подразделе 5.2.7 настоящего руководства.

11.9.8. Настройка протокола MMS

Описание настройки параметров правила по протоколу MMS описано в подразделе 5.2.8 настоящего руководства.

11.9.9. Настройка протокола GOOSE

Описание настройки параметров правила по протоколу GOOSE описано в подразделе 5.2.9 настоящего руководства.

11.10. Импорт пользовательских решающих правил в формате Snort

Для импорта пользовательских решающих правил в формате Snort необходимо загрузить правила обнаружения вторжений в текстовом формате (текстовый файл с набором правил в формате Snort с расширением «.rules»). Для этого необходимо перейти в раздел «Обнаружение вторжений» - «Администрирование» - «Обновление». Для обновления

необходимо нажать на кнопку «Загрузить новый локальный набор правил». После этого в всплывающем окне необходимо нажать на флажок напротив поля «Включить», в пункте «Необходимо выбрать файл» выбрать файл с правилами (файл формата «.rules»). Пункты «Имя файла», «Заголовок» заполнятся автоматически (при необходимости можно их изменить). Далее нажать «Сохранить изменения» (рисунок 341).

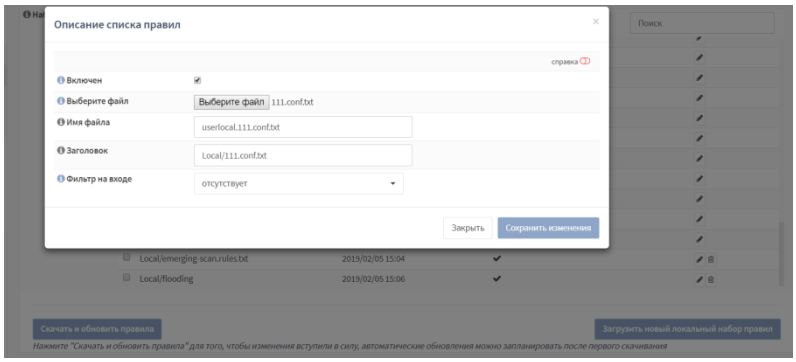


Рисунок 341 — Снимок экрана импорта правил

Затем необходимо убедиться, что правила были добавлены в список (рисунок 342).

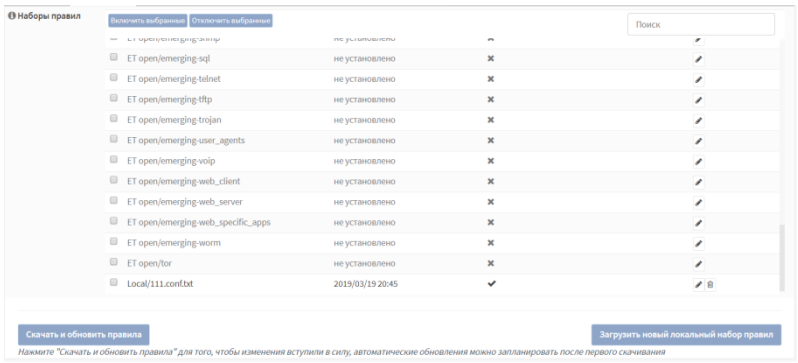


Рисунок 342 — Снимок экрана списков правил

Для активации выбранных настроек необходимо нажать на кнопку «Скачать и обновить правила».

11.11. Экспорт пользовательских решающих правил

Для экспорта пользовательских решающих правил через консольный интерфейс необходимо настроить доступ по SSH. Для этого необходимо перейти в раздел меню «Система» - «Настройки» - «Администрирование» и найдите на этой странице «SSH».

В разделе «SSH-сервер» необходимо установить флажок напротив поля «Включить SSH», в поле «Группа логина» необходимо выбрать все группы, доступ к которым необходимо разрешить через SSH, в поле «Вход суперпользователей (root) в учетную запись» установить флажок напротив поля «Разрешить вход пользователей (root) в учетную запись», в поле «Метод аутентификации» установить флажок напротив поля «Разрешить парольный вход в учетную запись». В поле «Порт SSH» необходимо выбрать порт (по умолчанию 22), в поле «Прослушиваемые интерфейсы» выбрать интерфейс, через который необходимо подключиться по SSH и нажать кнопку «Сохранить» в конце страницы (рисунок 343).

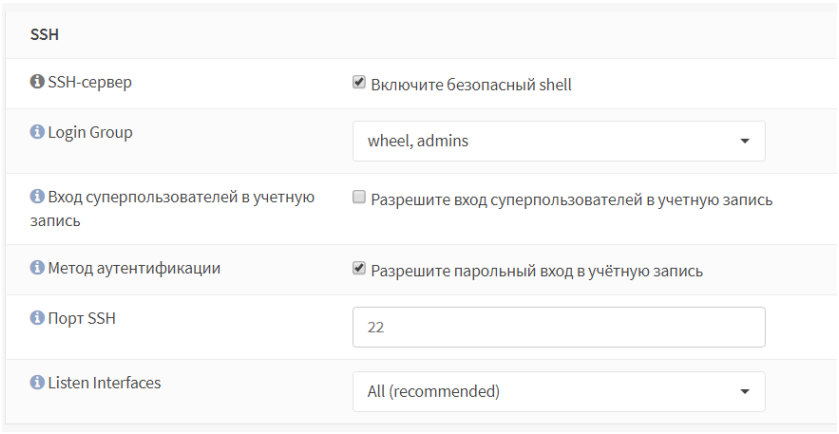


Рисунок 343 — Доступ по SSH

Далее подключится с помощью утилиты «Winscp» к системе и скачать пользовательские правила из директории «/usr/local/etc/suricata/rules».

Для экспорта загруженных пользователем наборов правил системы обнаружения вторжений через веб-интерфейс необходимо перейти в раздел «Система» - «Конфигурация» - «Резервные копии» и в группе настроек «Скачать наборы правил СОВ» нажать кнопку «Сохранение» (рисунок 344).

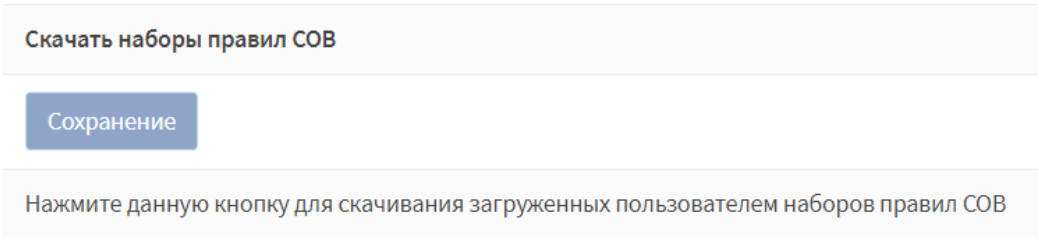


Рисунок 344 — Снимок экрана экспорта правил

11.12. Динамическая маршрутизация

Для примера приведена настройка динамической маршрутизации на трех ПК «InfoWatch ARMA Industrial Firewall». Общая конфигурация представлена на рисунке (рисунок 345).

Необходимо настроить интерфейсы ПК «InfoWatch ARMA Industrial Firewall» в соответствие с рисунком (рисунок 345.

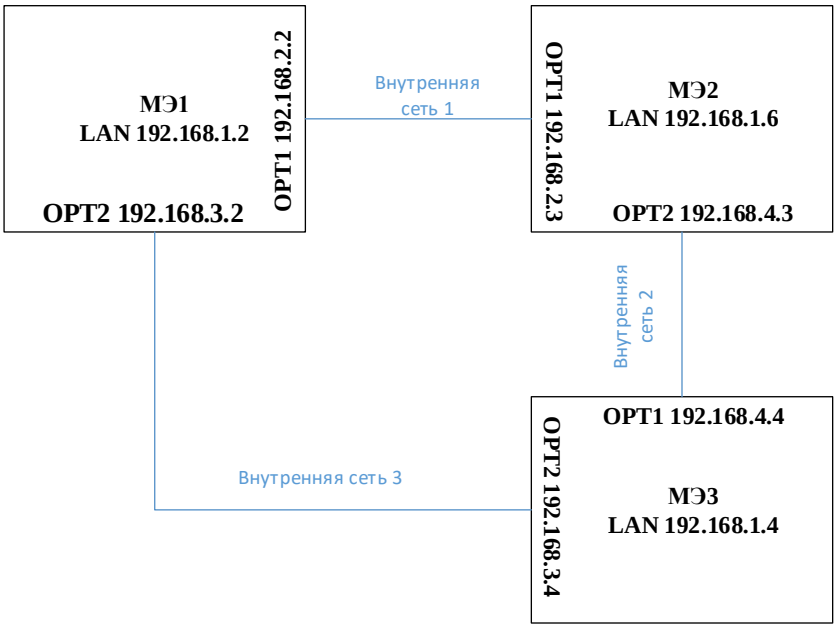
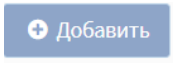


Рисунок 345 — Конфигурация МЭ для примера динамической маршрутизации

Изначально ПК «InfoWatch ARMA Industrial Firewall» пропускает пакеты только на интерфейсах WAN и LAN, а на других блокирует. Поэтому необходимо создать правило, которое будет пропускать пакеты на интерфейсы OPT1 и OPT2. Для этого во всех ПК «InfoWatch ARMA Industrial Firewall» необходимо перейти в поле «Межсетевой экран» - «Правила» - «OPT1» и нажать на кнопку 

. В поле «Действие» необходимо выбрать «Разрешение», в поле «Интерфейс» выбрать «OPT1», в поле «Версия TCP/IP» выбрать «IPv4», в поле «Описание» ввести описание правила, например, «Default allow OPT1 to any rule». Необходимо нажать на кнопку «Сохранить» (рисунок 346, рисунок 347).

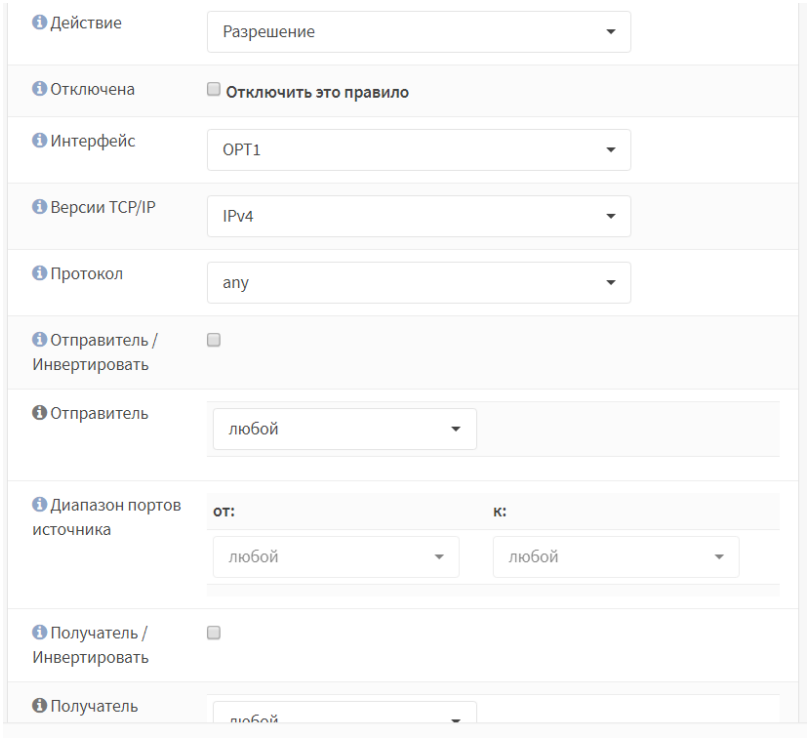


Рисунок 346 — Настройка правила для OPT1 (1)

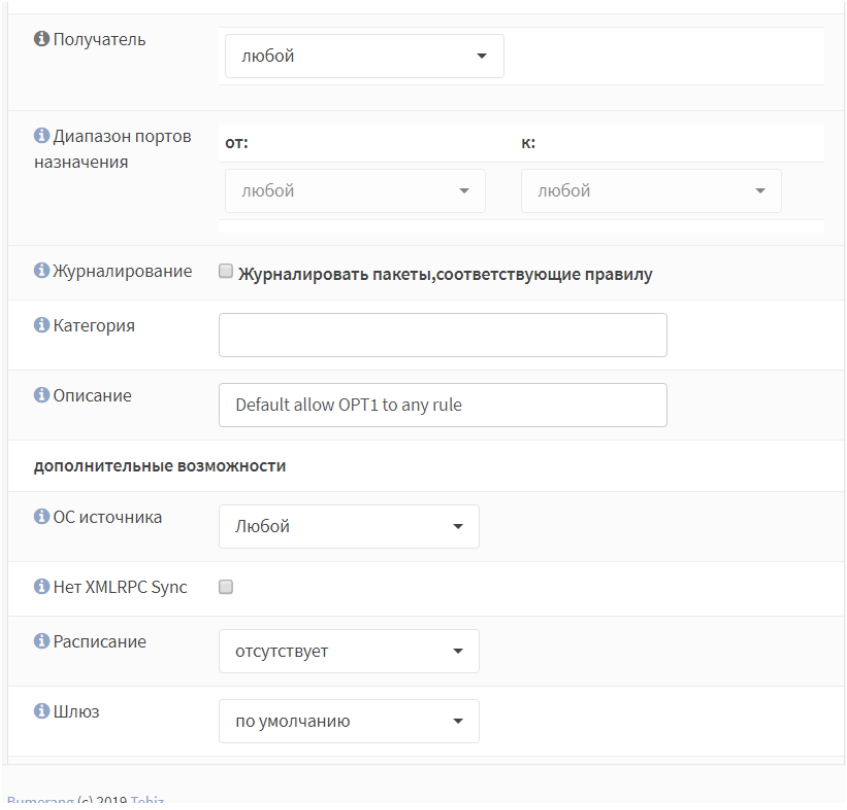
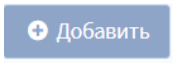


Рисунок 347 — Настройка правила для OPT1 (2)

Для настройки правила OPT2, во всех ПК «InfoWatch ARMA Industrial Firewall» необходимо перейти в поле «Межсетевой экран» - «Правила» -

«OPT2» и нажать на кнопку 

. В поле «Действие» необходимо выбрать «Разрешение», в поле «Интерфейс» выбрать «OPT2», в поле «Версия TCP/IP» выбрать «IPv4», в поле «Описание» ввести описание правила, например, «Default allow OPT2 to any rule». Необходимо нажать на кнопку «Сохранить» (рисунок 348, рисунок 349).

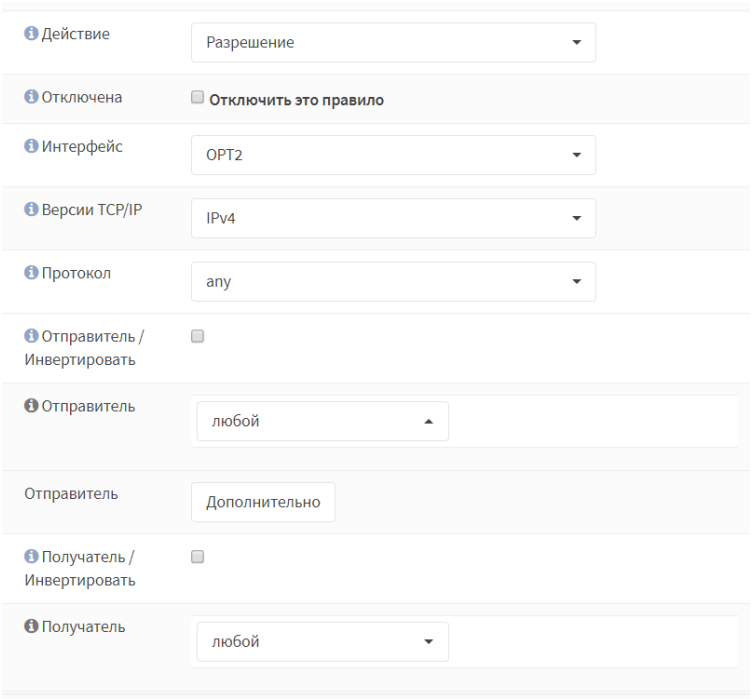


Рисунок 348 — Настройка правила для OPT2 (1)

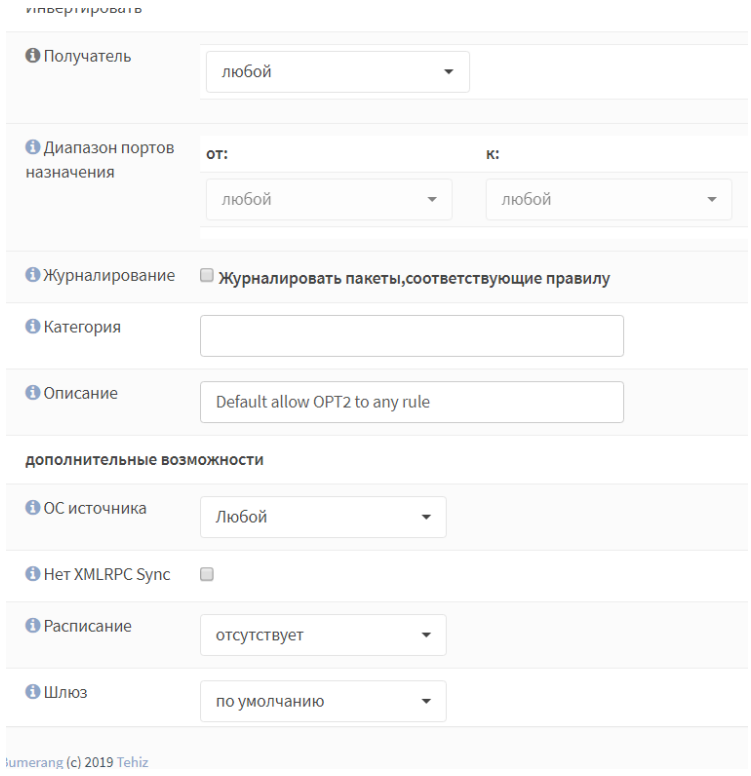


Рисунок 349 — Настройка правила для OPT2 (2)

После проверки корректности настройки правил во всех ПК «InfoWatch ARMA Industrial Firewall» необходимо отправить ping от МЭ 1 к МЭ 3:

– Ping 192.168.3.4.

Наличие ответа на запрос ping означает, что имеется подключение МЭ 1 и МЭ 3.

В МЭ 1 необходимо перейти в раздел «Маршрутизация» - «Общие настройки» и установить флажок напротив поля «Включен». Для настройки динамического маршрута необходимо перейти в поле «Маршрутизация» - «RIP». Необходимо установить флажок напротив поля «Включить», в поле «Версия» выбрать 2, в поле «Пассивные интерфейсы» выбрать «LAN», в поле «Перераспределение маршрута» выбрать «Перераспределение маршрута», в поле «Сети» ввести «192.168.2.0/24» и нажать кнопку «Сохранить», а затем нажать  в верхнем правом углу.

В МЭ 2 необходимо перейти в раздел «Маршрутизация» - «Общие настройки» и установить флажок напротив поля «Включен». Для настройки динамического маршрута необходимо перейти в поле «Маршрутизация» - «RIP». Необходимо установить флажок напротив поля «Включить», в поле «Версия» выбрать 2, в поле «Пассивные интерфейсы» выбрать «LAN», «WAN», в поле «Перераспределение маршрута» выбрать «Перераспределение маршрута», в поле «Сети» ввести «192.168.2.0/24», «192.168.4.0/24» и нажать кнопку «Сохранить», а затем нажать  в верхнем правом углу.

В МЭ 3 необходимо перейти в раздел «Маршрутизация» - «Общие настройки» и установить флажок напротив поля «Включен». Для настройки динамического маршрута необходимо перейти в поле «Маршрутизация» - «RIP». Необходимо установить флажок напротив поля «Включить», в поле «Версия» выбрать 2, в поле «Пассивные интерфейсы» выбрать «LAN», «WAN», в поле «Перераспределение маршрута» выбрать

«Перераспределение маршрута», в поле «Сети» ввести «192.168.4.0/24» и нажать кнопку «Сохранить», а затем нажать в верхнем правом углу.

11.13. Настройки для работы на уровне L2

Для перехода в режим работы на уровне L2 (по умолчанию ПК «InfoWatch ARMA Industrial Firewall» работает на уровне L3) необходимо создать мост между двумя сетевыми интерфейсами.

Переход на уровень L2 может быть использован для создания прозрачного режима, не требующего создания подсетей.

11.13.1. Отключение исходящего NAT

Для отключения исходящего NAT необходимо перейти в раздел «Межсетевой экран» - «NAT» - «Исходящий» и отключить NAT путем установки флажка на значение «Отключить создание правил исходящего NAT (исходящий NAT отключен)» (рисунок 350).

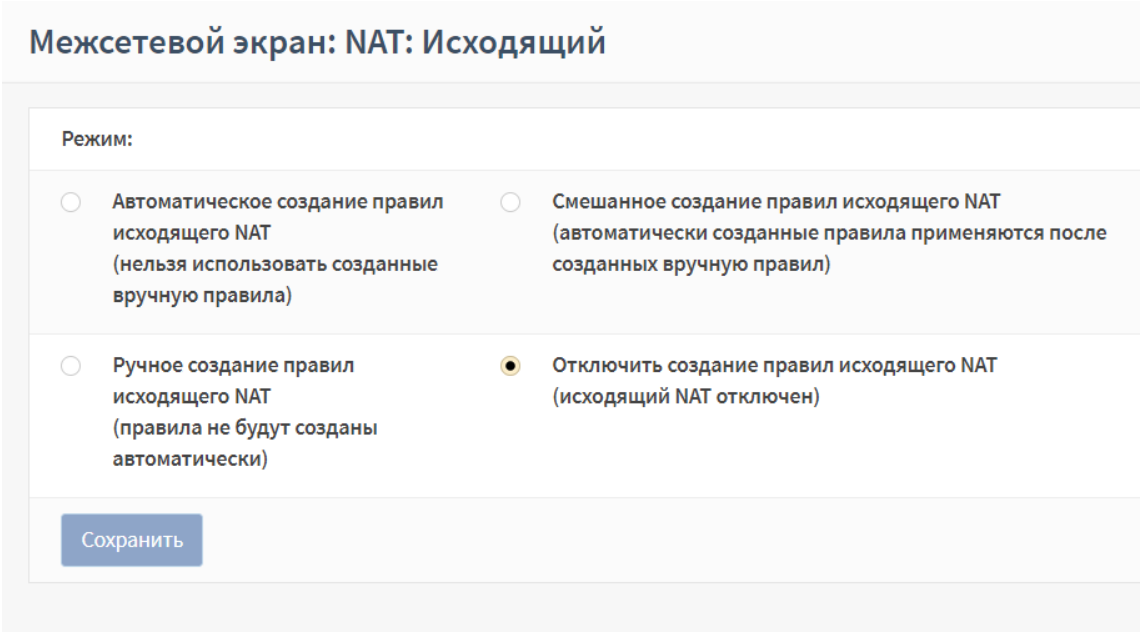


Рисунок 350 — Отключение исходящего NAT

11.13.2. Изменение системных параметров

Необходимо включить мост путем изменения системного параметра (net.link.bridge.pfil_bridge) со значения «default» на «1» в разделе меню

«Система» - «Настройки» - «Параметры» и нажать кнопку «Сохранить» (рисунок 351).

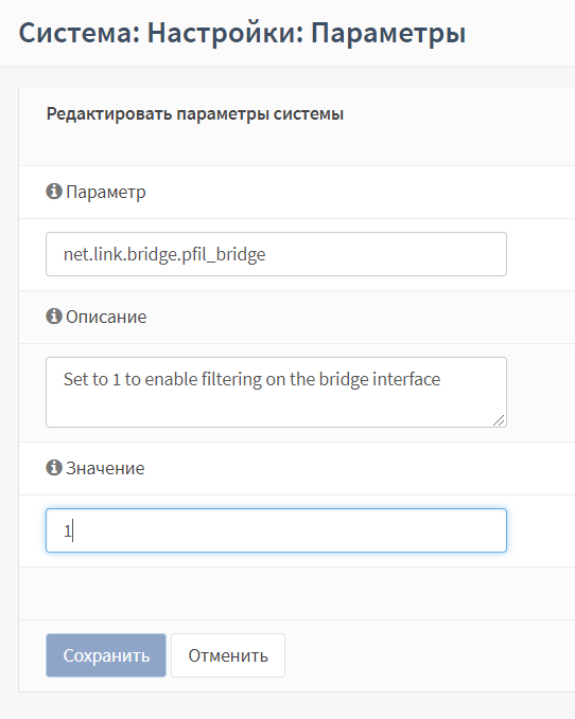
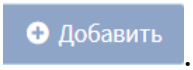


Рисунок 351 — Изменение системных параметров

Аналогичным образом изменить значения параметра net.link.bridge.pfil_member с «default» на «0» и нажать кнопку «Применить изменения».

11.13.3. Создание моста

Для создания моста необходимо перейти в раздел «Интерфейсы» - «Другие типы» - «Сетевой мост» и нажать кнопку 

. В меню необходимо выбрать несколько интерфейсов, которые будут добавлены в сетевой мост и нажать кнопку «Сохранить» (рисунок 352).

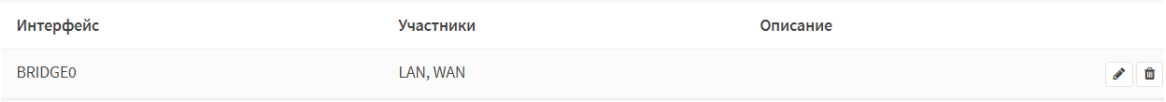


Рисунок 352 — Создание моста

11.13.4. Назначение управляющего интерфейса

Для того, чтобы обеспечить возможность управления ПК, необходимо задать новый управляющий (manage) интерфейс. В разделе «Интерфейсы» - «Назначение портов» и необходимо нажать на кнопку + напротив моста (рисунок 353).

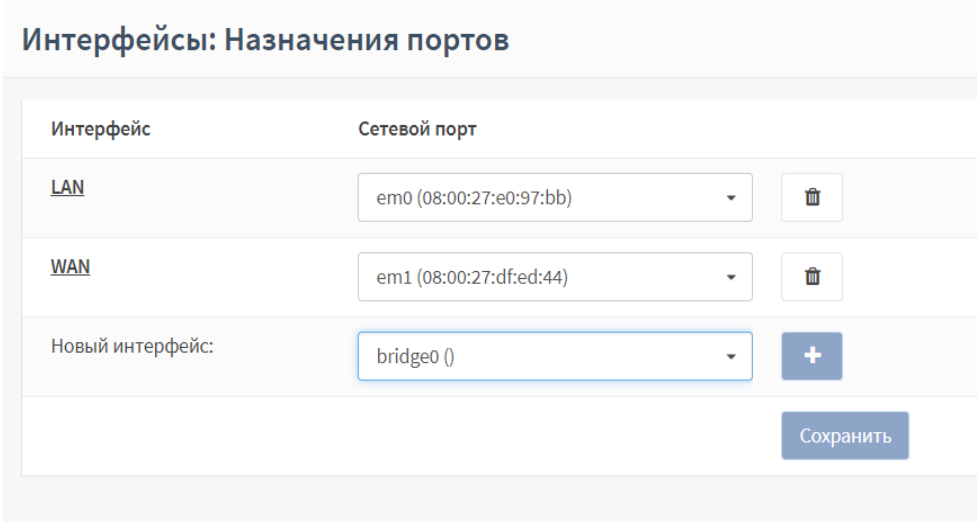


Рисунок 353 — Назначение управляющего интерфейса

После этого необходимо перейти в настройки вновь созданного интерфейса в разделе «Интерфейсы» - «OPT1», включить его, необходимо выбрать «Тип конфигурации»: «Статический IPv4» и установить IP адрес. Нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

11.13.5. Отключение приватных сетей и Bogon

В разделе «Интерфейсы» - «WAN» необходимо отключить поля «Блокировать приватные сети» и «Блокировать Bogon сети» нажать кнопку «Сохранить», затем кнопку «Применить изменения».

11.13.6. Отключение DHCP сервера на LAN

Для отключения DHCP сервера необходимо перейти в раздел «Службы» - «DHCPv4» - «LAN» и отключить функцию «Включить DHCP-сервер на LAN интерфейсе».

11.13.7. Отключение интерфейсов LAN и WAN

После конфигурации моста, необходимо отключить обработку трафика на уровне L3. Для этого необходимо перейти в раздел «Интерфейсы» - «LAN» и в раздел «Интерфейсы» - «WAN», в каждом установить значение «Отсутствует» в поле «Тип конфигурации IPv4» и нажать кнопку «Сохранить».

11.14. Настройки режима отказоустойчивого кластера (высокой доступности)

Для настройки кластера необходимо настроить параметры в разделе «Система» - « Высокая доступность» - «Настройки» (рисунок 354).

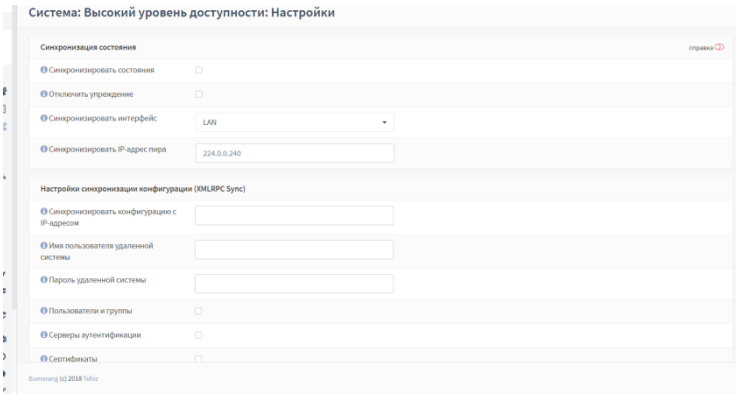


Рисунок 354 — Выбор регистрируемых событий

В примере описывается настройка кластера на основе двух сетей. 192.168.1.0/24 будет использоваться для внутренней сети, а 172.8.0.0/24 будет использоваться для маршрутизации трафика в Интернет.

При использовании CARP все интерфейсы должны иметь выделенный IP-адрес, который будет объединен с одним общим виртуальным IP-адресом для связи с обеими сетями.

11.14.1. Установка интерфейсов и основные правила межсетевого экрана

В примере используются три интерфейса, все имеют базовую настройку.

Необходимо перейти в раздел «Интерфейсы», необходимо убедиться, что имеется все три интерфейса и назначены адреса и подсети в соответствии с таблицей (таблица 16).

Таблица 16 — Интерфейсы

Название интерфейса	**IP-адрес**
LAN	192.168.1.10/24
WAN	172.18.0.101/24
PFSYNC	10.0.0.1

Затем необходимо убедиться, что соответствующие протоколы могут использоваться на разных интерфейсах. Для этого необходимо перейти в «Межсетевой экран» - «Правила» и убедиться, что LAN и WAN принимают CARP-пакеты.

Необходимо задать IP-адреса на резервном устройстве в соответствии с таблицей (таблица 17).

Таблица 17 — Сервер резервного копирования

Название интерфейса	**IP-адрес**
LAN	192.168.1.20/24
WAN	172.18.0.102/24
PFSYNC	10.0.0.2

11.14.2. Настройка виртуальных IP-адресов

Необходимо перейти в поле «Межсетевой экран» - «Виртуальные IP-адреса» - «Настройки» и добавить новый виртуальный IP-адрес в

соответствии с таблицей (таблица 18).

Таблица 18 — Настройка виртуальных IP-адресов

Название	Значение
Тип	CARP
Интерфейс	WAN
IP-адрес	172.18.0.100/24
Виртуальный пароль	root
Группа VHID	1
Частота синхронизации	Base 1/Skew 0
Описание	VIP WAN

11.14.3. Настройка исходящего NAT

Когда трафик выходит из межсетевого экрана, он также должен использовать виртуальный IP-адрес. По умолчанию для ПК «InfoWatch ARMA Industrial Firewall» используется IP-адрес интерфейсов (в примере иначе).

Необходимо перейти в поле «Межсетевой экран» - «NAT» и выбрать «Исходящий». Необходимо выбрать «Ручное создание правил исходящего NAT» на этой странице и измените правила, исходящие из сети 192.168.1.0/24, чтобы использовать виртуальный интерфейс CARP (172.18.0.100).

11.14.4. Настройка синхронизации XMLRPC SYNC

Для настройки синхронизации высокого уровня доступности используя XMLRPC SYNC необходимо включить «pfSync», используя выделенный интерфейс и межсетевой экран. Для этого необходимо перейти в раздел «Система» - «Высокая доступность» - «Настройки», включить «Синхронизовать состояния»» и выбрать сетевой интерфейс в «Синхронизовать интерфейс», используемый для «pfSync». Затем настроить

пир IP-адреса в поле «Синхронизовать пир IP-адреса» ввести адрес: 10.0.0.2.

Затем необходимо настроить параметры, которые будут дублироваться на сервер резервного копирования, используя опцию «Настройка синхронизации конфигурации (XMLRPC SYNC)». Поставить флажок напротив:

– «Правила межсетевого экрана»;
– «NAT»;
– «DHCPD»;
– «Виртуальные IP-адреса».

11.14.5. Настройка тестирования

Чтобы проверить настройку, необходимо подключить пользователя к локальной сети и открыть SSH-соединение с хостом обоих межсетевых экранов. Теперь при подключении необходимо просматривать таблицу состояний на обоих межсетевых экранах («Анализ» - «Состояние»).Таблицы состояний должны быть одинаковы.

11.15. Создание правил МЭ

Для удобства, в веб-интерфейсе правила межсетевого экрана задаются отдельно для каждого из сетевых интерфейсов, настроенных в ПК «InfoWatch ARMA Industrial Firewall». Правила располагаются в виде списка с приоритетом от верхнего к нижнему. Иными словами, сетевой пакет проверяется на совпадение с критериями правил по порядку, сверху вниз.

Если сетевой пакет удовлетворяет критериям правила, то к пакету применяется действие, заданное в правиле. Если к пакету уже применено правило, то обработка пакета сетевым экраном прекращается. Такой пакет далее не будет сверяться с оставшимися правилами в списке.

Действия «блокировать (block)» и «отклонить (reject)» предполагают блокирование пакета межсетевым экраном (причем в первом случае, удаленная сторона никак не оповещается о свершившейся блокировке).

Действие пропустить (pass) разрешает прохождение пакета через межсетевой экран и приводит к созданию состояния.

Если сетевой пакет не удовлетворяет критериям ни одного правила, то пакет блокируется (т.е. отбрасывается без индикации удаленной стороне).

11.15.1. Создание правил МЭ для всех сетевых интерфейсов

Для просмотра правил для всех сетевых интерфейсов необходимо перейти в раздел «Межсетевой экран» - «Правила» - «Общие». В категории «Общие» приведена таблица правил. Таблица содержит следующие данные (рисунок 355):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет);

– протокол, к которому применяется правило;

– данные отправителя;

– порт;

– шлюз;

– расписание;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то имеется правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

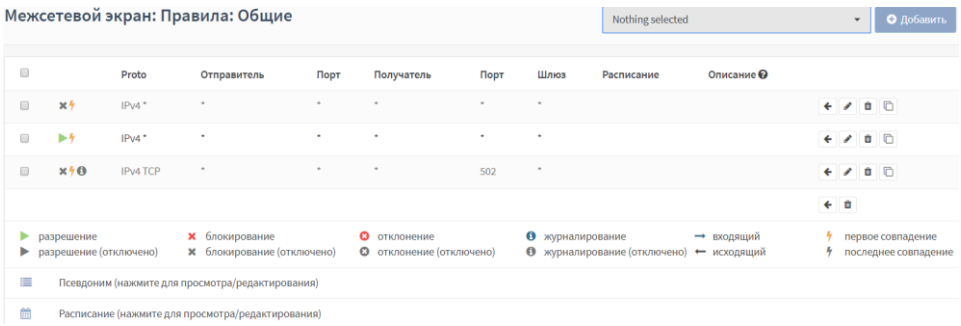


Рисунок 355 — Межсетевой экран: Правила: Общие

Для того чтобы создать новое правило, необходимо нажать на кнопку Добавить в категории «Общие».

При создании правила в поле «Действие» необходимо выбрать действие правила (разрешение, блокирование, отклонение). При необходимости отключить правило - установить флажок напротив поля «Отключить». При необходимости сразу применять действие к пакету, который соответствует этому правилу (вне зависимости от приоритета правила) необходимо установить флажок напротив пункта «Быстрая проверка». В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 356).

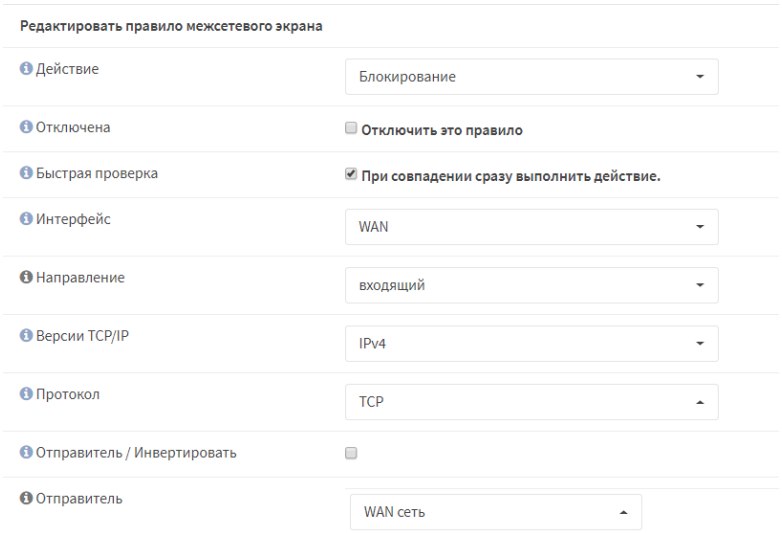


Рисунок 356 — Межсетевой экран: Правила: Общие (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Журналирование» необходимо поставить флажок, если необходимо журналирование пакетов, которые будут соответствовать редактируемому правилу. В поле «Диапазон портов получателя» необходимо указать порт получателя или диапазон портов. Поле «Категория» позволяет указать категорию группы правил (необязательно). В поле «Описание» необходимо ввести описание правила (рисунок 357).

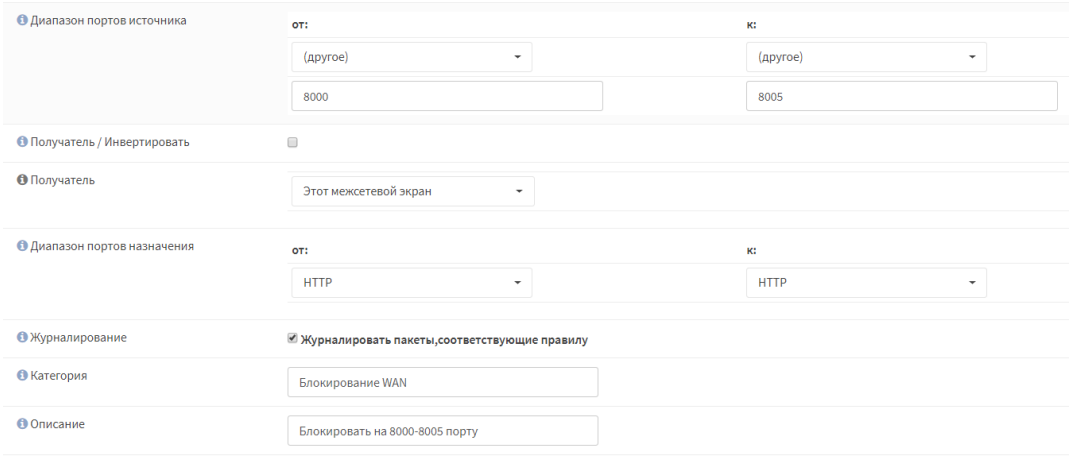


Рисунок 357 — Межсетевой экран: Правила: Общие (редактирование, часть 2)

В разделе «Дополнительные возможности» присутствуют дополнительные параметры настройки правила. В поле «ОС источника» имеется возможность выбрать тип ОС (только при выборе ранее TCP протокола). В поле «Не синхронизовать XMLRPC» необходимо поставить флажок, если необходимо отключить синхронизацию данного правила на ведущем устройстве с другими участниками отказоустойчивого кластера CARP. При необходимости выбора времени работы правила в поле «Расписание» необходимо выбрать настроенное расписание (для настройки

расписания необходимо перейти в поле «Межсетевой экран» - «Настройки» - «Расписание»). Для того чтобы правило работало все время, необходимо выбрать «отсутствует». В поле «Шлюз» необходимо выбрать шлюз при использовании маршрутизации (значение «по умолчанию» используется в случае необходимости использования системной таблицы маршрутизации) (рисунок 358).

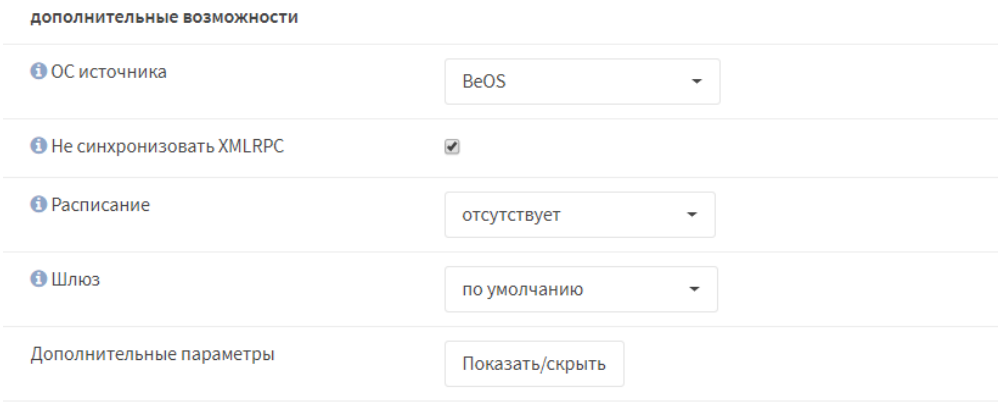


Рисунок 358 — Межсетевой экран: Правила: Общие (редактирование, часть 3)

При нажатии на кнопку «Показать/скрыть» напротив пункта «Дополнительные параметры» появятся дополнительные поля настройки правила (рисунок 359). В поле «Разрешить параметры» необходимо установить флажок для разрешения пакетов с параметрами IP, которые блокируются по умолчанию. В поле «Отключить ответ» необходимо установить флажок в случае необходимости отключения автоматически созданного ответа для этого правила. В поле «Установить приоритет» необходимо установить приоритет пакетов, которые будут попадать под это правило, если это необходимо. В поле «Совпадение приоритета» необходимо выбрать приоритет, который будет совпадать с приоритетом пакета. Поле «Установить локальный тег» позволяет вписать метку (в пакет также необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Макс. состояний»

необходимо ввести максимальное число записей состояний, которые может создать это правило. В поле «Макс. узлов-источников» необходимо ввести максимальное количество уникальных хостов-источников. В поле «Макс. установленных соединений» необходимо ввести максимальное количество установленных соединений для хоста. В поле «Макс. состояний-источников» необходимо ввести максимальное количество записей состояний для хоста. В поле «Макс. новых соединений» необходимо ввести максимальное количество новых соединений для хоста за секунду. В поле «Тайм-аут состояния» необходимо ввести состояние тайм-аута в секундах. В поле «TCP-флаги» необходимо выбрать флаги, которые должны быть установлены и не должны быть установлены для этого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync в кластере высокой доступности. В поле «Тип состояния» необходимо выбрать тип механизма отслеживания состояний:

– Keep state (используется для отслеживания состояния подключения);

– Sloppy state (работает как keep state, но не проверяет порядковые номера);

– Synproxy state (проксирует входящие соединения TCP для защиты серверов от Spoofed TCP и SYN-flood атак, этот тип включает в себя комбинацию функций keep state и modulate state);

– Отсутствует (невозможно использовать механизмы отслеживания состояний, если используется функция управления очередями).

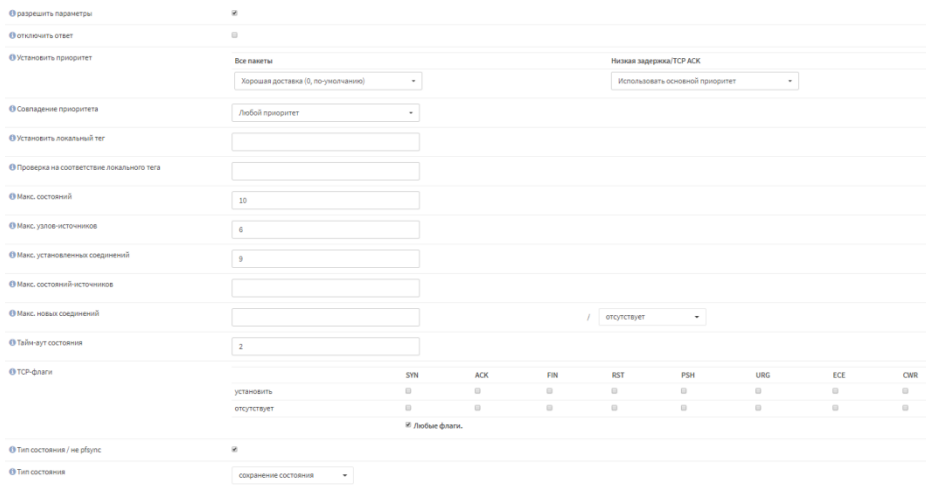


Рисунок 359 — Межсетевой экран: Правила: Общие (редактирование, часть 4)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

11.15.2. Создание правил МЭ для определенного сетевого интерфейса

Для просмотра правил для определенного сетевого интерфейса необходимо перейти в раздел «Межсетевой экран» - «Правила» - «[Название интерфейса]». В категории «[Название интерфейса]» приведена таблица правил, которые применяются к сетевому интерфейсу [Название интерфейса], где [Название интерфейса] – это имя сетевого интерфейса, установленное при ассоциации этого сетевого интерфейса с физическим сетевым интерфейсом. Таблица правил включает в себя следующие данные (рисунок 360):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет);

– протокол, к которому применяется правило;

– данные отправителя;

– порт;

– шлюз;

– расписание;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

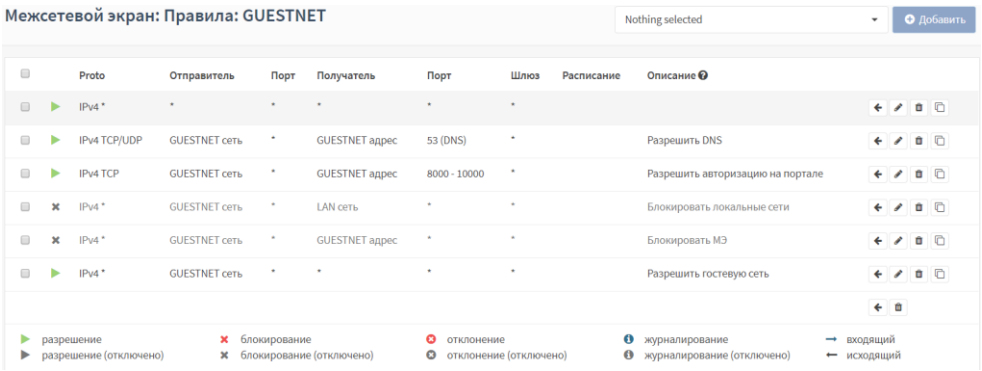


Рисунок 360 — Межсетевой экран: Правила: [Название интерфейса]

Для того чтобы создать новое правило, необходимо нажать на кнопку Добавить в категории «[Название интерфейса]».

При создании правила в поле «Действие» необходимо выбрать действие правила (разрешение, блокирование, отклонение), необходимо установить флажок напротив поля «Отключить» для выключения редактируемого правила. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Направление» необходимо выбрать направление пакетов, на которое будет распространяться правило. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 361).

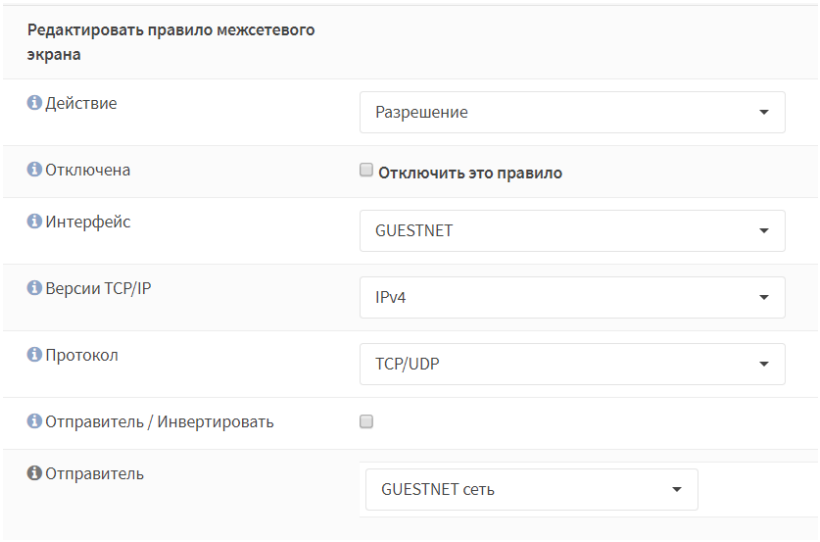


Рисунок 361 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Журналирование» необходимо поставить флажок, если необходимо журналирование пакетов, которые будут соответствовать редактируемому правилу. В поле «Диапазон портов получателя» необходимо указать порт получателя или диапазон портов. Поле «Категория» позволяет указать категорию группы правил (необязательно). В поле «Описание» необходимо ввести описание правила (рисунок 362).

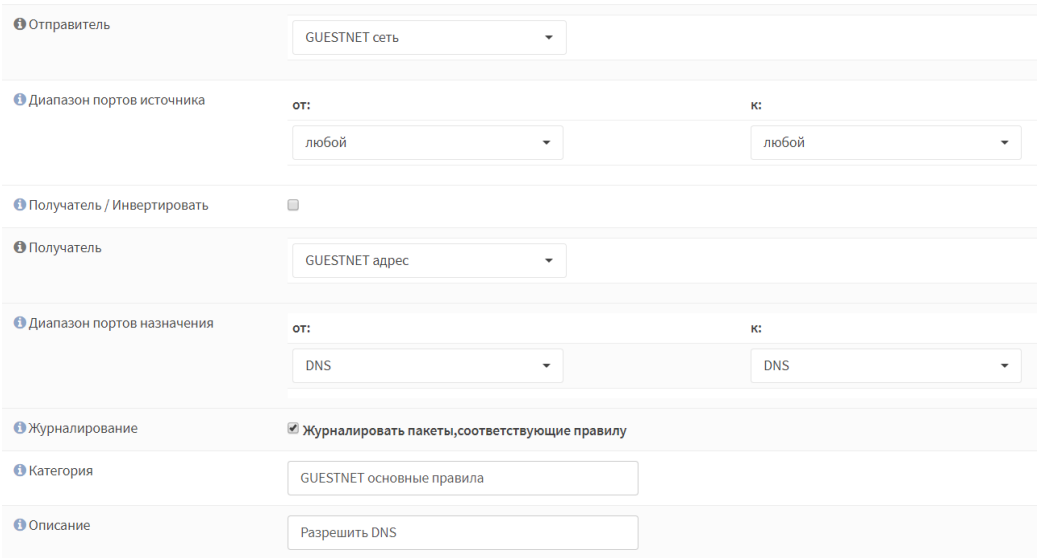


Рисунок 362 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 2)

В разделе «Дополнительные возможности» присутствуют дополнительные параметры настройки правила. В поле «ОС источника» имеется возможность выбрать тип ОС (только при выборе ранее TCP протокола). В поле «Не синхронизовать XMLRPC» необходимо поставить флажок для отключения синхронизации данного правила на ведущем устройстве с другими участниками отказоустойчивого кластера CARP. При необходимости выбора времени работы правила в поле «Расписание» необходимо выбрать настроенное расписание (для настройки расписания необходимо перейти в поле «Межсетевой экран» - «Настройки» - «Расписание»). Для того чтобы правило работало все время, необходимо выбрать «отсутствует». В поле «Шлюз» необходимо выбрать шлюз при использовании маршрутизации (значение «по умолчанию» используется в случае необходимости использования системной таблицы маршрутизации) (рисунок 363).

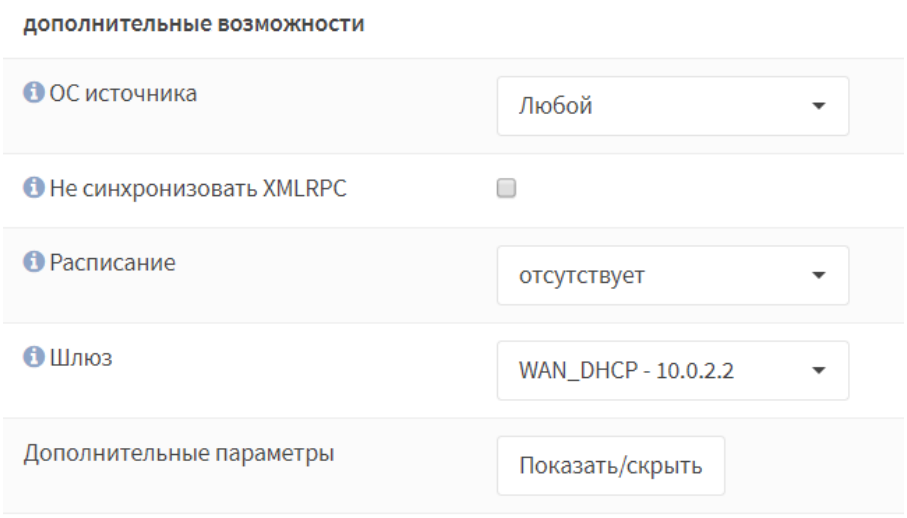


Рисунок 363 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 3)

При нажатии на кнопку «Показать/скрыть» напротив пункта «Дополнительные параметры» появятся следующие поля (рисунок 364). В поле «Разрешить параметры» необходимо установить флажок для разрешения пакетов с параметрами IP, которые блокируются по умолчанию. В поле «Отключить ответ» необходимо установить флажок в случае необходимости отключения автоматически созданного ответа для этого правила. В поле «Установить приоритет» необходимо установить приоритет пакетов, которые будут попадать под это правило, если это необходимо. В поле «Совпадение приоритета» необходимо выбрать приоритет, который будет совпадать с приоритетом пакета. Поле «Установить локальный тег» позволяет вписать метку (в пакет также необходимо вписать эту же метку) для того, чтобы все пакеты, имеющие такую же метку, попадали под правило. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенному для другого правила. В поле «Макс. состояний» необходимо ввести максимальное число записей состояний, которые может создать это правило. В поле «Макс. узлов-источников» необходимо ввести максимальное количество уникальных хостов-источников. В поле «Макс. установленных соединений» необходимо ввести максимальное количество установленных

соединений для хоста. В поле «Макс. состояний-источников» необходимо ввести максимальное количество записей состояний для хоста. В поле «Макс. новых соединений» необходимо ввести максимальное количество новых соединений для хоста за секунду. В поле «Тайм-аут состояния» необходимо ввести состояние тайм-аута в секундах. В поле «TCP-флаги» необходимо выбрать флаги, которые должны быть установлены и не должны быть установлены для этого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync в кластере высокой доступности. В поле «Тип состояния» необходимо выбрать тип механизма отслеживания состояний:

– Keep state (используется для отслеживания состояния подключения);

– Sloppy state (работает как keep state, но не проверяет порядковые номера);

– Synproxy state (проксирует входящие соединения TCP для защиты серверов от Spoofed TCP и SYN-flood атак, этот тип включает в себя комбинацию функций keep state и modulate state);

– Отсутствует (невозможно использовать механизмы отслеживания состояний, если используется функция управления очередями).

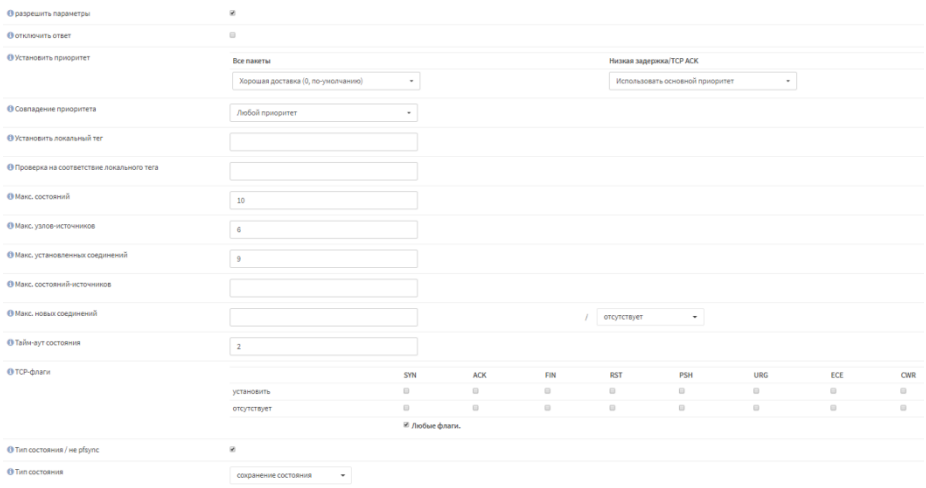


Рисунок 364 — Межсетевой экран: Правила: [Название интерфейса] (редактирование, часть 4)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

11.16. Создание правил NAT

Для обеспечения возможности компьютерам из внутренней сети работать с внешней сетью под одним внешним IP-адресом необходимо создать правило NAT «переадресации портов». Для этого необходимо перейти в «Межсетевой экран» - «NAT» - «Переадресация портов». На странице «Переадресация портов» приведена таблица правил, которые применяются для переадресации портов. Таблица содержит в себе следующие данные (рисунок 365):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет);

– интерфейс;

– протокол, к которому применяется правило;

– данные отправителя (адрес, порты);

– данные получателя (адрес, порты);

– данные NAT (адрес, порты);

– протокол;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то есть правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

Рисунок 365 — Межсетевой экран: NAT: Переадресация портов

Для того чтобы создать новое правило, необходимо нажать на кнопку Добавить в категории «Переадресация портов».

При создании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле «Версии TCP/IP» необходимо выбрать версию протокола, которая будет соответствовать данному правилу. В поле «Протокол» необходимо выбрать IP-протокол, для которого будет выполняться это правило. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила (рисунок 366).

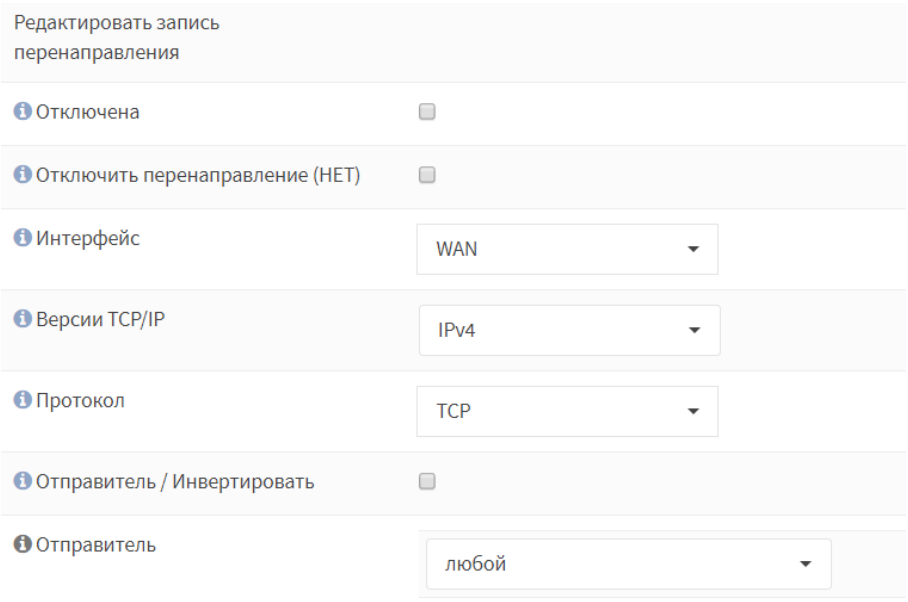


Рисунок 366 — Межсетевой экран: NAT: Переадресация портов (редактирование, часть 1)

При нажатии на кнопку «Дополнительно» появятся поля дополнительной настройки отправителя. В поле «Диапазон портов источника» необходимо указать порт источника или диапазон портов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо выбрать получателя. В поле «Диапазон портов назначения» необходимо указать порт получателя или диапазон портов (рисунок 367).

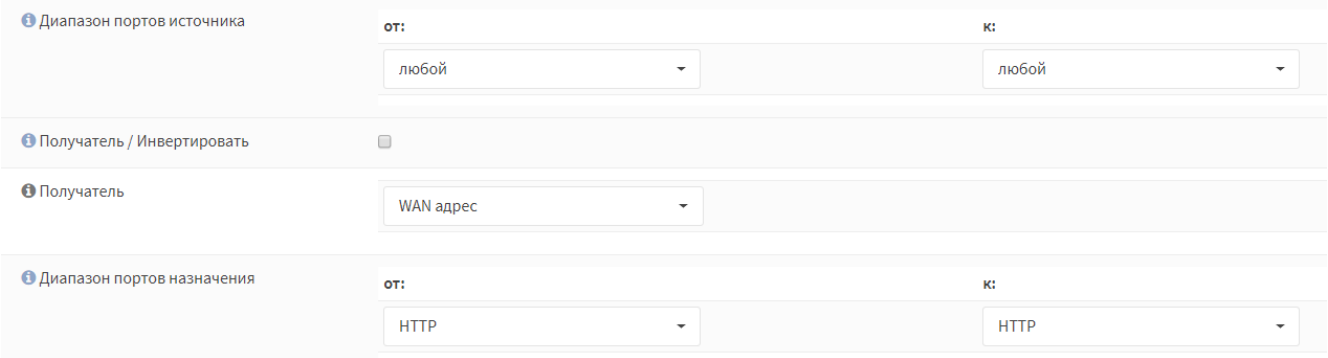


Рисунок 367 — Межсетевой экран: NAT: Переадресация портов (редактирование, часть 2)

В поле «Перенаправление целевого IP-адреса» необходимо ввести внутренний IP-адрес сервера для перенаправления портов. В поле «Целевой порт перенаправления» необходимо ввести порт компьютера с введенным в поле «Перенаправление целевого IP-адреса» IP-адресом. В поле «Параметры пула:» необходимо выбрать параметры пула:

– Циклический: перебирает транслируемые IP-адреса;

– Случайный: выбирает случайный адрес из пула транслируемых IP-адресов;

– Хеш источника: использует хеш адреса источника для определения транслируемого IP-адреса и проверяет, чтобы IP-адрес перенаправления для указанного источника всегда был один и то же;

– Битовая маска: применяет маску подсети и сохраняет последнюю часть идентичной; 10.0.1.50 - x.x.x.50;

– Фиксированные адреса: параметр «липкие адреса» может использоваться со случайным и циклическим типами, чтобы конкретный IP-адрес источника преобразовывался в одинаковый транслируемый адрес.

В поле «Описание» необходимо ввести описание правила. Поле «Проверка на соответствие локального тега» позволяет вписать тег для проверки пакета на соответствие тега, размещенного для другого правила. В поле «Тип состояния/не pfsync» необходимо установить флажок для отключения синхронизации состояний, созданных этим правилом, через pfsync. В поле «Зеркальный NAT» необходимо выбрать состояние (включить, отключить, использовать системное значение по умолчанию). В поле «Связные правила фильтрации» необходимо выбрать связные правила фильтрации (рисунок 368).

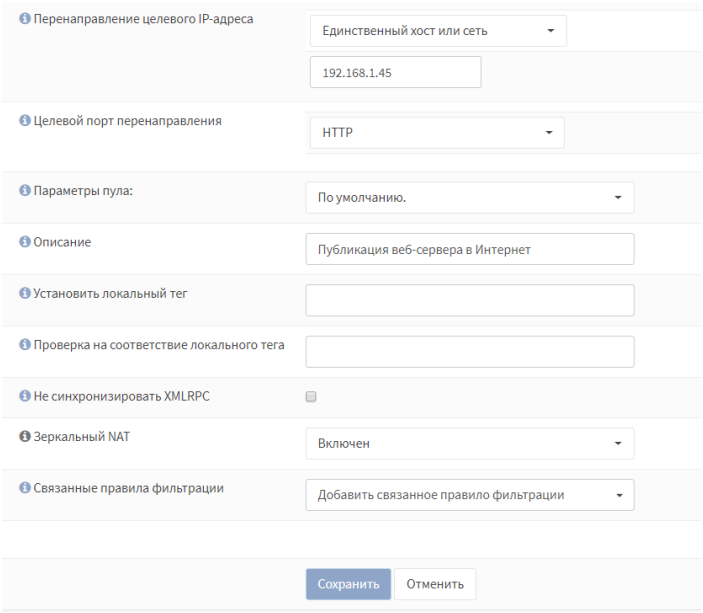


Рисунок 368 — Межсетевой экран: NAT: Переадресация портов (редактирование, часть 3)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

Для создания правил перенаправления «один к одному» необходимо перейти в «Межсетевой экран» - «NAT» - «Один к одному». В категории «Один к одному» приведена таблица правил, которые могут применяться для трансляции сетевых адресов в режиме «один к одному». Таблица содержит следующие данные (рисунок 369):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет);

– интерфейс;

– внешний IP-адрес;

– внутренний IP-адрес;

– IP-адрес назначения;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то имеется правила оцениваются по принципу первого совпадения (как

только совпадение найдено, выполняется действие, присвоенное данному правилу).

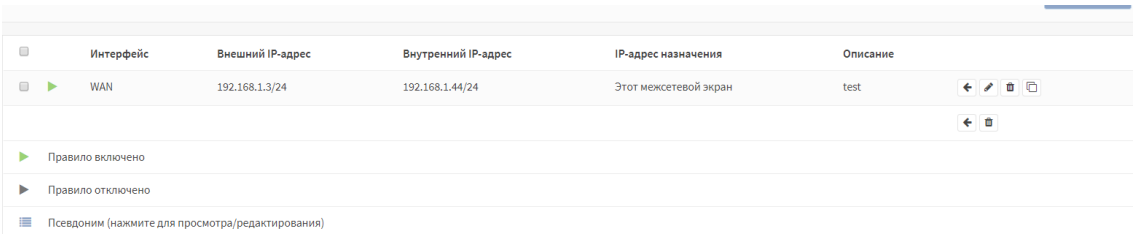
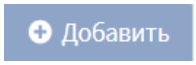


Рисунок 369— Межсетевой экран: NAT: Один к одному

Для того чтобы создать новое правило, необходимо нажать на кнопку 

в категории «Один к одному».

При создании правила необходимо установить флажок напротив поля «Отключить», если необходимо выключить редактируемое правило. В поле «Интерфейс» необходимо выбрать сетевые интерфейсы, на которые будут приходить пакеты для проверки соответствия данному правилу. В поле тип необходимо выбрать BINAT (по умолчанию) или NAT. Если сети одного размера, обычно используется BINAT. Правило BINAT определяет двунаправленное отображение между внешней и внутренней сетью и может быть использовано в обоих направлениях, NAT применяется только в одном направлении. В поле «Внешняя сеть» необходимо указать начальный адрес внешней подсети для трансляции в режиме «1:1». В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель» необходимо ввести внутреннюю подсеть для отображения режима «1:1». В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель» необходимо ввести получателя, с которым будет использоваться режим «1:1». В поле «Описание» необходимо ввести описание данного правила. В поле «Зеркальный NAT» необходимо выбрать

состояние (включен, отключить, использовать системное значение по умолчанию) (рисунок 370).

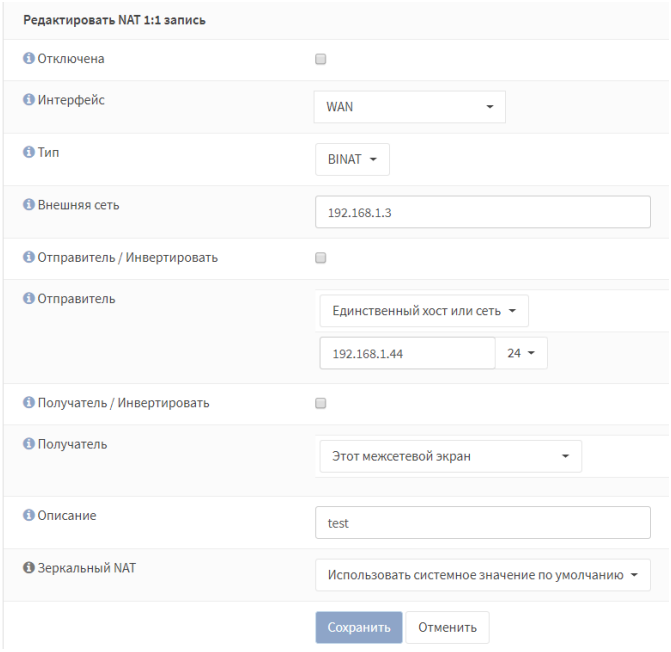


Рисунок 370 — Межсетевой экран: NAT: Один к одному (редактирование)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения», для сохранения и применения внесенных изменений соответственно.

Для создания правил перенаправления адресов IPv6 необходимо перейти в «Межсетевой экран» - «NAT» - «NPTv6». В категории «NPTv6» приведена таблица правил, которые могут применяться для преобразования адресов IPv6. Чаще всего это используется для перевода глобальных («WAN») IP-адресов в локальные. Таблица содержит следующие данные (рисунок 371):

– графическое отображение состояния правила (включено/выключено, какое действие выполняет);

– интерфейс;

– внешний префикс;

– внутренний префикс;

– описание правила.

Таблица правил содержит правила в порядке их приоритета (сверху-вниз), то имеется правила оцениваются по принципу первого совпадения (как только совпадение найдено, выполняется действие, присвоенное данному правилу).

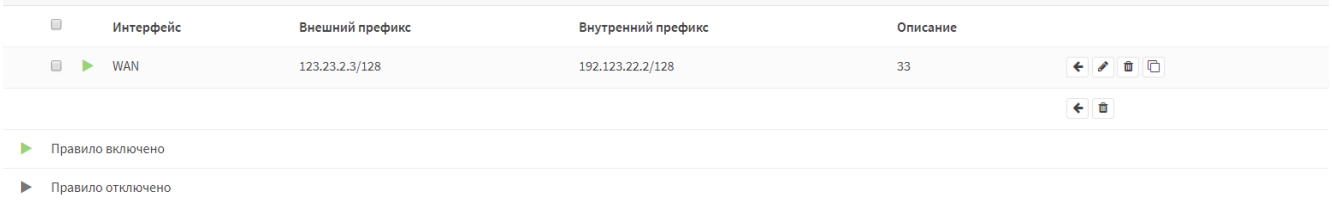
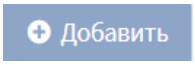


Рисунок 371 — Межсетевой экран: NAT: NPTv6

Для того чтобы создать новое правило, необходимо нажать на кнопку 

в категории «NPTv6».

При редактировании правила необходимо установить флажок напротив пункта «Отключить» для выключения редактируемого правила. В поле «Интерфейс» необходимо выбрать сетевой интерфейс, на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Отправитель/Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Отправитель/Адрес» необходимо ввести внутренний (LAN) IPv6-префикс уникального локального адреса для трансляции сетевых префиксов. В поле «Получатель/Инвертировать» необходимо установить флажок для того, чтобы в качестве получателя выбрать все адреса кроме указанного в поле «Получатель». В поле «Получатель/адрес» необходимо ввести глобальный индивидуальный маршрутизируемый IPv6-префикс. В поле «Описание» необходимо ввести описание правила (рисунок 372).

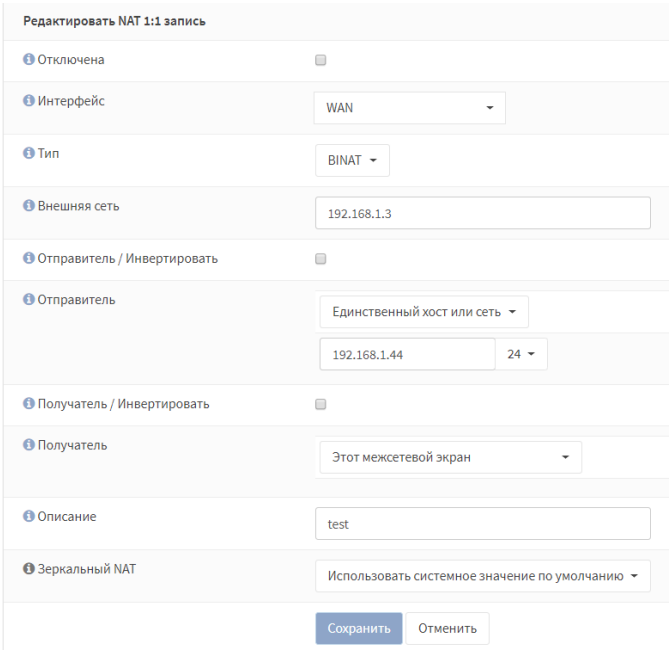


Рисунок 372 — Межсетевой экран: NAT: NPTv6 (редактирование правила)

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений.

11.17. Настройка прокси-сервера для взаимодействия с внешним антивирусом на удаленном хосте по протоколу ICAP

Антивирусная проверка — это проверка на уровне шлюза, которая обеспечивает:

– защиту от опасных веб-сайтов;

– защиту от зараженных файлов.

Для того, чтобы осуществлялась антивирусная проверка, трафик от клиентских машин должен попадать на прокси-сервер устройства ПК «InfoWatch ARMA Industrial Firewall». Далее приведены настройка прокси-сервера, которые обеспечат попадание HTTP и HTTPS трафика на прокси-сервер.

11.17.1. Настройка HTTP-прокси

Для включения HTTP-прокси необходимо перейти в «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси» и поставить флажок напротив «Включен».

Далее необходимо перейти во вкладку «Перенаправляющий прокси» - «Основные настройки перенаправления». В «Включен» необходимо поставить флажок. В поле «Интерфейсы» необходимо выбрать сетевой интерфейсы, к которым будет привязан прокси-сервер. В поле «Номер порта прокси сервера» необходимо ввести номер порта, который прокси-сервер будет прослушивать. В «Включить прозрачный HTTP-прокси» необходимо поставить флажок для включения проксирования. Нажать кнопку «Применить» (рисунок 373).

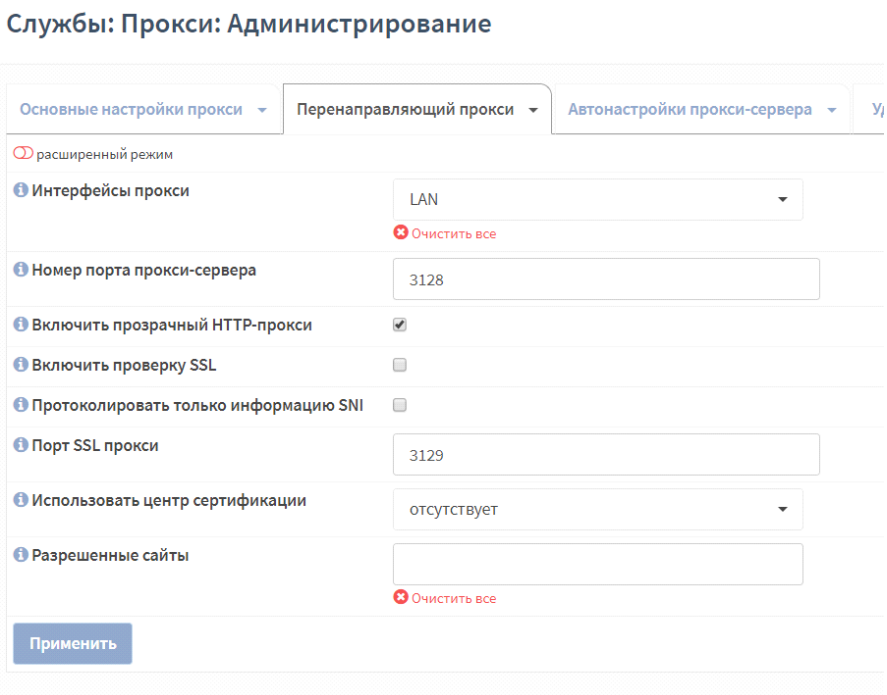


Рисунок 373 — Службы: Прокси: Администрирование (настройка HTTP-прокси)

Следующим шагом необходимо создать правило переадресации NAT. Для этого необходимо нажать на ссылку «Добавление нового правила межсетевого экрана» в описании поля «Включить прозрачный HTTP-прокси» (рисунок 374).

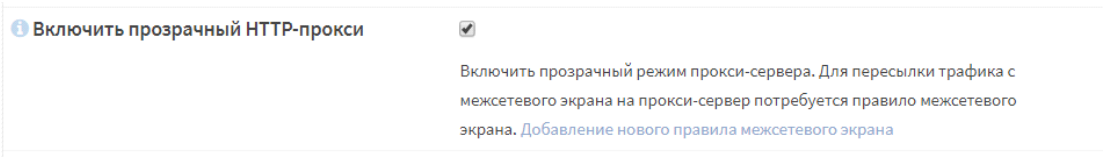


Рисунок 374 — Службы: Прокси: Администрирование (настройка HTTP-прокси: Создание правила NAT)

Затем необходимо заполнить поля правила в соответствие с таблицей и нажать кнопку «Сохранить», а затем «Применить изменения» (таблица 19).

Таблица 19 — Создание NAT правила для настройки HTTP-прокси

Название поля	**Значение**
Интерфейс	LAN [Сетевой интерфейс, выбранный в поле «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси»]
Протокол	TCP
Источник	LAN сеть
Диапазон портов источника	Любой - любой
Назначение	Любой
Диапазон портов назначения	HTTP - HTTP
Адрес перенаправления	127.0.0.1
Порт перенаправления	3128
Описание	Перенаправление трафика на прокси
Зеркальный NAT	Включить
Связные правила фильтрации	Добавить связное правило фильтрации

Необходимо подключиться по внутренней сети устройство. На устройстве в качестве шлюза по умолчанию ввести IP-адрес сетевого интерфейса из поля «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси». Затем необходимо ввести DNS-сервер на устройстве: «8.8.8.8». Это необходимо для возможности перехода на веб-сайт по доменному имени сайта. На удаленном устройстве необходимо открыть в веб-браузере сайт (http, например: http://o-site.spb.ru/). В случае успешного подключения к сети Интернет отобразиться страница сайта.

11.17.2. Настройка HTTPS-прокси

Для включения HTTPS-прокси необходимо перейти в «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси» и поставить флажок напротив «Включен». Далее необходимо перейти во вкладку «Перенаправляющий прокси» - «Основные настройки перенаправления». В «Включен» необходимо поставить флажок. В поле «Интерфейсы» необходимо выбрать сетевой интерфейсы, к которым будет привязан прокси-сервер. В поле «Номер порта прокси сервера» необходимо ввести номер порта, который прокси-сервер (HTTP) будет прослушивать. В «Включить прозрачный HTTP-прокси» необходимо поставить флажок для включения проксирования. В «Включить проверку SSL» необходимо поставить флажок для включения возможности подключения через HTTPS протокол. В поле «Порт SSL прокси» необходимо ввести номер порта, который SSL прокси-сервер будет прослушивать. Нажать кнопку «Применить» (рисунок 375).

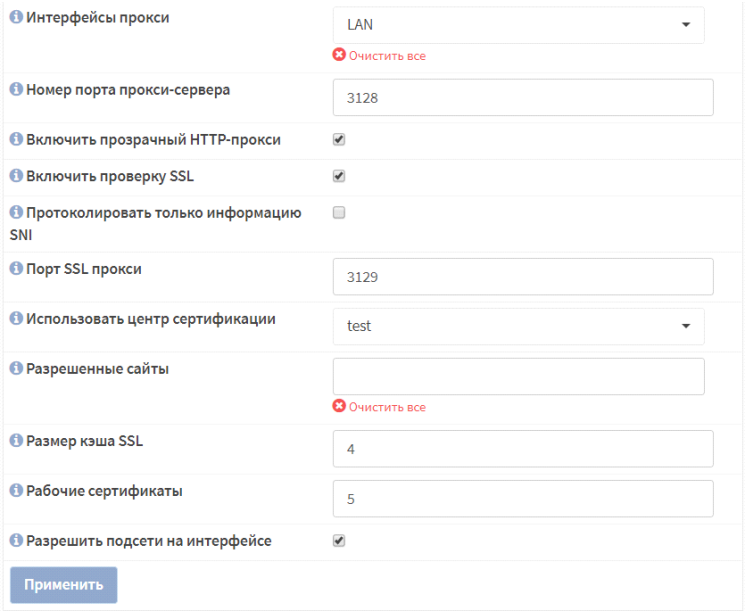


Рисунок 375 — Службы: Прокси: Администрирование (настройка HTTS-прокси)

Следующим шагом необходимо создать правило переадресации NAT. Для этого необходимо нажать на ссылку «Включить проверку SSL» в описании «Добавление нового правила natfirewall rule» рисунок 376).

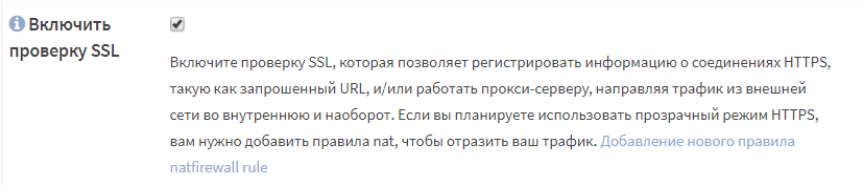


Рисунок 376 — Службы: Прокси: Администрирование (настройка HTTS-прокси: создание NAT правила)

Далее необходимо заполнить поля правила в соответствие с таблицей и нажать кнопку «Сохранить», а затем «Применить изменения» (таблица 20).

Таблица 20 — Создание NAT правила для настройки HTTP-прокси

Название поля	**Значение**
Интерфейс	LAN [Сетевой интерфейс, выбранный в поле «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси»]
Протокол	TCP

Источник	LAN сеть
Диапазон портов источника	Любой - любой
Назначение	Любой
Диапазон портов назначения	HTTPS - HTTPS
Адрес перенаправления	127.0.0.1
Порт перенаправления	3129
Описание	Перенаправление трафика на прокси
Зеркальный NAT	Включить
Связные правила фильтрации	Добавить связное правило фильтрации

Следующим шагом необходимо создать сертификат. Для этого необходимо перейти в «Система» - «Доверенные сертификаты» - «Полномочия» и нажать кнопку 

. Далее необходимо заполнить поля в соответствии с таблицей (таблица 21).

Таблица 21 — Создание сертификата

Поле	**Значение**
Описание	ARMA CA
Метод	Создать внутренний ЦС
Длина ключа (биты)	2048
Digest алгоритм	SHA256
Срок жизни (дней)	356
Код страны	RU (Россия)

Область	МО
Город	Москва
Организация	InfoWatch
Email адрес	admin@infowatch.ru
Простое имя	arma-ca

Для сохранения необходимо нажать кнопку «Сохранить».

Для скачивания сертификата необходимо перейти в «Система» - «Доверенные сертификаты» - «Полномочия» и нажать кнопку «Экспорт сертификата CA» напротив созданного сертификата. Скаченный сертификат необходимо переместить на устройство, которое необходимо подключить к SSL прокси-серверу.

Затем необходимо подключиться по внутренней сети устройство. На устройстве в качестве шлюза по умолчанию ввести IP-адрес сетевого интерфейса из поля «Интерфейсы» на странице «Службы» - «Прокси» - «Администрирование» - «Основные настройки прокси». Затем необходимо ввести DNS-сервер на устройстве: «8.8.8.8». Это необходимо для возможности перехода на веб-сайт по доменному имени сайта.

На устройстве необходимо настроить веб-браузера. Далее описан пример добавления сертификата для веб-браузера FireFox.

Для добавления сертификата необходимо открыть веб-браузер FireFox, перейти в раздел «Приватность» - «Защита» - «Сертификаты» и нажать кнопку «Просмотр сертификатов» (рисунок 377).

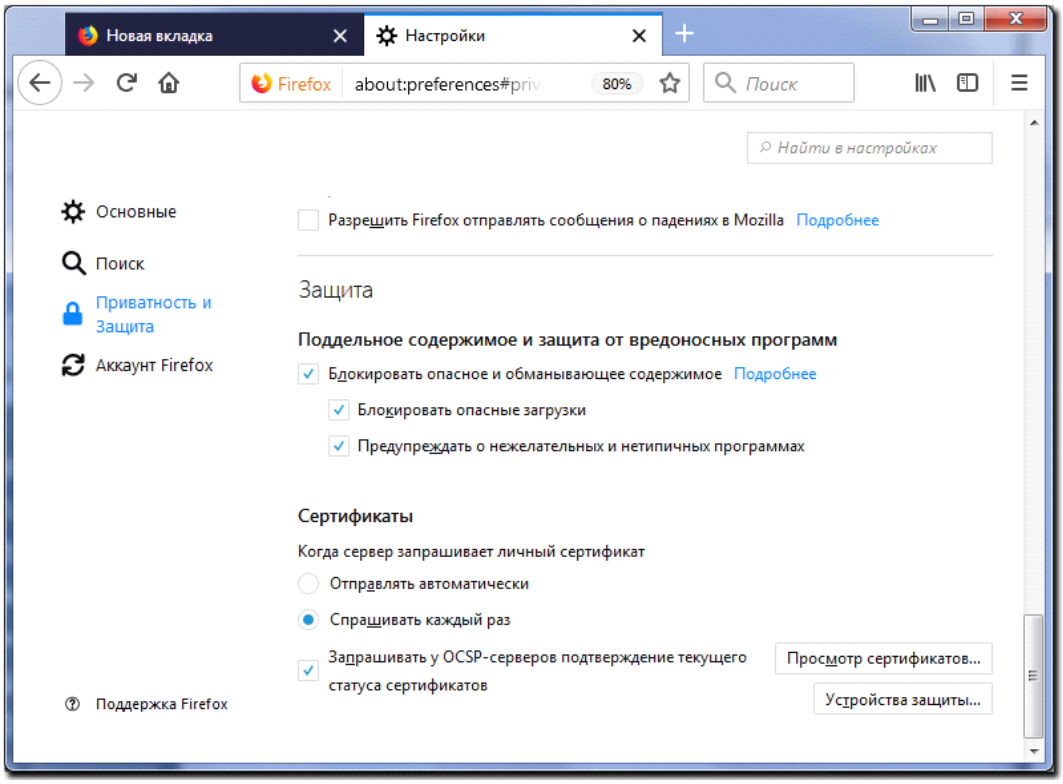


Рисунок 377 — Добавление сертификата (часть 1)

В окне необходимо выбрать вкладку «Центры сертификации» и нажать кнопку «Импортировать...» (рисунок 378).

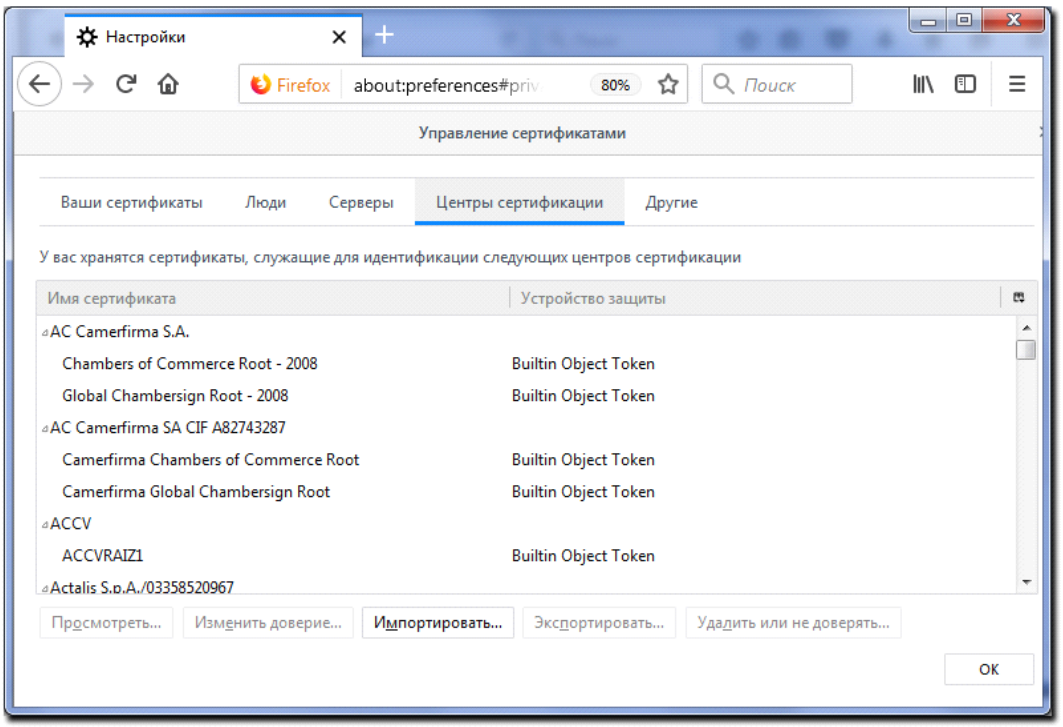


Рисунок 378 — Добавление сертификата (часть 2)

Необходимо найти на жестком диске сохраненный файл сертификата и нажать кнопку «Открыть» (рисунок 379).

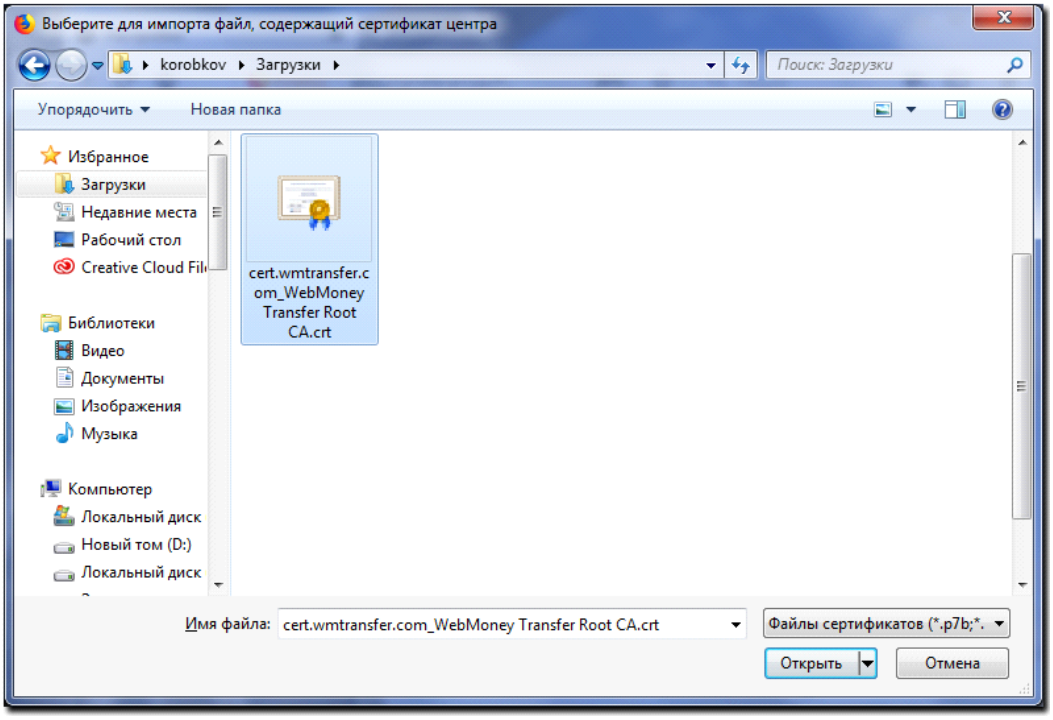


Рисунок 379 — Добавление сертификата (часть 3)

В окне «Загрузка сертификата» необходимо выбрать цели, для которых импортируется сертификат (рисунок 380).

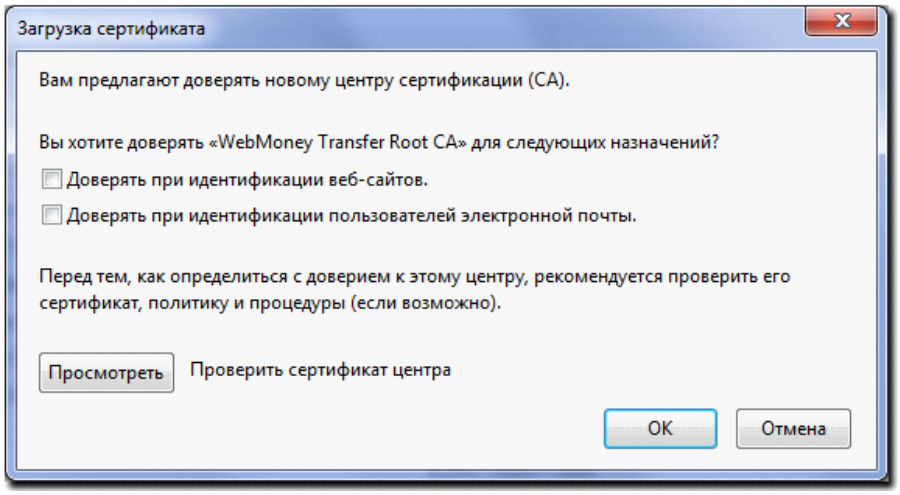


Рисунок 380 — Добавление сертификата (часть 4)

Необходимо выбрать все предложенные варианты, отметив их флажками, после чего жать кнопку «ОК» (рисунок 381).

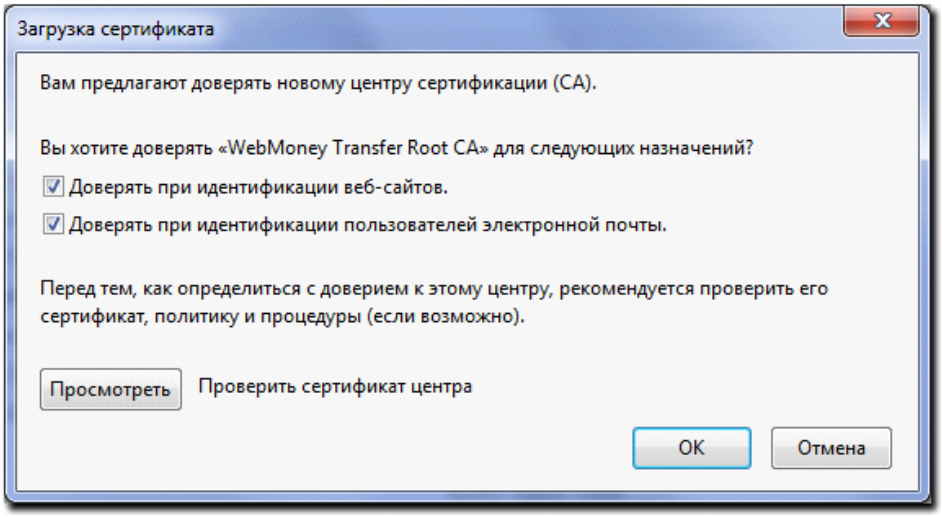


Рисунок 381 — Добавление сертификата (часть 5)

Для контроля правильности проделанных операций необходимо открыть вкладку «Центры сертификации» и в конце списка найти установленный корневой сертификат.

Далее на удаленном устройстве необходимо открыть в веб-браузере сайт (https, например: https://vk.com). В случае успешного подключения к сети Интернет отобразиться страница сайта.

11.17.3. Настройка внешнего антивируса

Настройка антивирусов сторонних производителей выходит за рамки данной инструкции. Необходимо обратиться к документации производителя антивируса для его настройки.

11.17.4. Настройка ПК «InfoWatch ARMA Industrial Firewall» для взаимодействия с внешним антивирусом

Прокси-сервер поддерживает взаимодействие с антивирусом, выполняемом на отдельном внешнем хосте, посредством протокола ICAP.

В данном разделе освещаются настройки на стороне ПК «InfoWatch ARMA Industrial Firewall» для взаимодействия с внешним антивирусом.

Необходимо подключить сервер, на котором выполняется антивирус, к шлюзу ПК «InfoWatch ARMA Industrial Firewall» через свитч или напрямую с помощью отдельного сетевого кабеля. Также, для безопасной передачи

ICAP-трафика, ПК «InfoWatch ARMA Industrial Firewall» и внешний антивирус можно разместить в отдельном VLAN.

Далее необходимо указать в свойствах прокси-сервера как он будет взаимодействовать по ICAP с внешним антивирусом. Для этого необходимо перейти в «Службы» - «Прокси» - «Администрирование» - «Перенаправляющий прокси» - «Настройки ICAP». В «Включить» необходимо поставить флажок. В «Запрос на изменение URL» необходимо ввести URL, идентифицирующие ICAP-сервис (антивирус). Любой ICAP-сервис может поддерживать работу в двух режимах — Request Modification и Response Modification — поэтому задается не один, а два URL-идентификатора. Каждый URL-идентификатор, таким образом, обозначает не столько ICAP-сервис как таковой, а ICAP-сервис + режим работы.

Для проверки функционала антивирусной защиты удобно использовать ресурс: «http://www.eicar.org». EICAR — безвредный тестовый вирус, применяемый для простой проверки - работает ли антивирус.

На странице «http://2016.eicar.org/85-0-Download.html» скачать вирус EICAR по протоколу HTTP, HTTPS, в виде архивного ZIP-файла и т.п.

Проверку необходимо осуществлять с конечного компьютера пользователя.

11.18. Настройка портала авторизации

Для настройки Портала авторизации необходимо добавить новый интерфейс, через который пользователи из внутренней сети получат доступ к Порталу авторизации. Для этого необходимо перейти в раздел «Интерфейсы» - «Назначения портов», нажать  для добавления нового интерфейса и нажать кнопку «Сохранить». Далее необходимо перейти в «Интерфейсы» - «OPT1», поставить флажок в «Включен» и заполнить настройки интерфейса в соответствие с таблицей (таблица 22).

Таблица 22 — Настройка интерфейса

Поле	Значение
Описание	GUESTNET
Блокировать	Не выбрано
Блокировать частные сети	Не выбрано
Блокировать bogon сети	Не выбрано
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
MAC-адрес	(Оставить пустым)
Максимальный размер кадра	(Оставить пустым)
Максимальный размер сегмента	(Оставить пустым)
Скорость и двусторонний режим передачи данных	По умолчанию
Статический адрес IPv4	192.168.200.1/24
Публичный IPv4-адрес шлюз	Автодетектирование

Далее необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

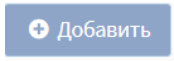
Для настройки DHCP-сервера необходимо перейти в раздел «Службы» - «DHCPv4» - «GUESTNET» и заполнить поля в соответствие с таблицей (таблица 23).

Таблица 23 — Настройки DHCP-сервера

Поле	Значение
Включен	Включен
Диапазон	192.168.200.100 - 192.168.200.200
DNS-серверы	192.168.200.1

Шлюз	192.168.200.1

Необходимо нажать кнопку «Сохранить».

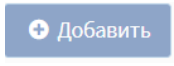
Далее необходимо добавить два разрешающих правила. Для добавления первого разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать 

. И заполнить поля в соответствие с таблицей (таблица 24).

Таблица 24 — Разрешение входа в Портал авторизации

Поле	**Значение**
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	TCP
Отправитель	GUESTNET сеть
Получатель	GUESTNET адрес
Диапазон портов назначения	(Другое) 8000 / (Другое) 10000
Категория	Общие правила GuestNet
Описание	Разрешить вход в Портал авторизации

Необходимо нажать кнопку «Сохранить».

Для добавления второго разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать 

. И заполнить поля в соответствие с таблицей (таблица 25).

Таблица 25 — Разрешение внутренней сети

Поле	**Значение**
Действие	Разрешить

Интерфейс	GUESTNET
Протокол	Any
Отправитель	GUESTNET сеть
Получатель	Любой
Диапазон портов получателя	Любой
Категория	Общие правила GUESTNET
Описание	Разрешить GUESTNET

Необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Далее необходимо загрузить шаблон страницы авторизации для пользователей Портала авторизации. Для этого необходимо перейти в «Службы» - «Портал авторизации» - «Шаблоны» и нажать на внизу таблицы для скачивания шаблона страницы авторизации пользователей. Далее отредактировать скаченный шаблон при необходимости. Затем нажать на , ввести в «Имя шаблона» название шаблона, например, «Test», выбрать скаченный шаблон, нажав на кнопку «Выберите файл» и нажать «Загрузить», а затем кнопку «Применить».

Для создания новой зоны авторизации необходимо перейти в раздел «Службы» - «Портал авторизации» - «Администрирование» и нажать . Необходимо заполнить поля редактирования зоны авторизации в соответствие с таблицей (таблица 26).

Таблица 26 — Настройки зоны авторизации

Поле	**Значение**
Включено	Выбрано
Интерфейсы	GUESTNET
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)
Разрешенные MAC-адреса	(оставить пустым)
Пользовательский шаблон	Test [шаблон созданный в «Службы» - «Портал авторизации» - «Шаблоны»]
Описание	Гостевая

Нажать кнопку «Сохранить», а затем кнопку «Применить».

Далее для авторизации пользователя в портале авторизации необходимо подключиться по локальной сети к ПК «InfoWath ARMA Industrial Firewall». Открыть на внешнем устройстве любой веб-браузер и ввести запрос: «8.8.8.8». При успешной настройке портала авторизации появится форма входа. Необходимо ввести аутентификационные данные и нажать кнопку «Вход». При успешной авторизации в Портале авторизации отобразиться страница «8.8.8.8» в веб-браузере.

При необходимости в выходе из Портала авторизации необходимо перейти на страницу «[IP-адрес графического веб-интерфейса]:8000» и нажать кнопку «Выход».

11.19. Создание Custom правил СОВ

Для создания правил системы обнаружения вторжений «вручную» необходимо перейти в раздел «Обнаружение вторжений» - «Контроль уровня приложений» и нажать на кнопку + для создания нового правила.

При редактировании правила необходимо нажать на флажок напротив поля «Включен» для включения правила. В поле «Заголовок» необходимо ввести название правила. В поле «Использовать шаблон» необходимо выбрать шаблон протокола «Вручную», который необходимо использовать (рисунок 382).

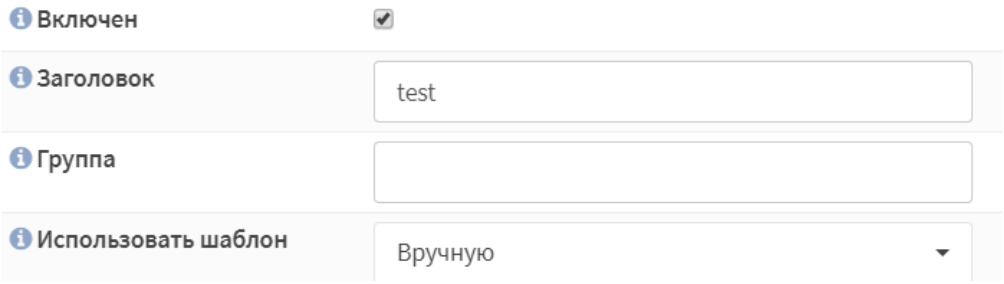


Рисунок 382 — Обнаружение вторжений: Контроль уровня приложений (редактирование)

При использовании шаблона «Вручную» появятся следующие настройки.

В поле «Действие» необходимо выбрать действие этого правила:

– «Предупредить (Alert)» — при необходимости оповещения при срабатывании правила;

– «Отклонить (Reject)» — при необходимости блокировать пакет при срабатывании правила и оповестить о блокировании;

– «Отбросить (Drop)» — при необходимости блокировать пакет при срабатывании правила без уведомления о блокировке;

– «Разрешить (Pass)» — при необходимости разрешить прохождение пакета при срабатывании правила.

В поле «Сообщение» необходимо ввести сообщение с описанием события, которое будет отображаться в журнале предупреждений. В поле «IP-адрес отправителя» необходимо ввести IP-адрес отправителя. В поле «Порт отправителя» необходимо ввести порт или диапазон портов отправителя. В поле «Выберите направление» необходимо выбрать направление правила:

– прямое (от источника к отправителю);

– прямое и обратное (от источника к отправителю и наоборот).

В поле «IP-адрес получателя» необходимо выбрать IP-адрес получателя. В поле «Порт получателя» необходимо ввести порт получателя.

В поле «Протокол» необходимо ввести протокол, пакеты которого будут проверяться в правиле. В поле «Дополнительные параметры» необходимо ввести дополнительные параметры правила в соответствии с подсказками и форматом написания правил Snort/Suricata, например «flow:established; dsize:>40; content:"| 03 00 |"; content:"| 72 03 |"; distance:5; content:"| 31 00 00 04 bb 00 00 |"; distance:34; rev:1;» после чего необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 383).

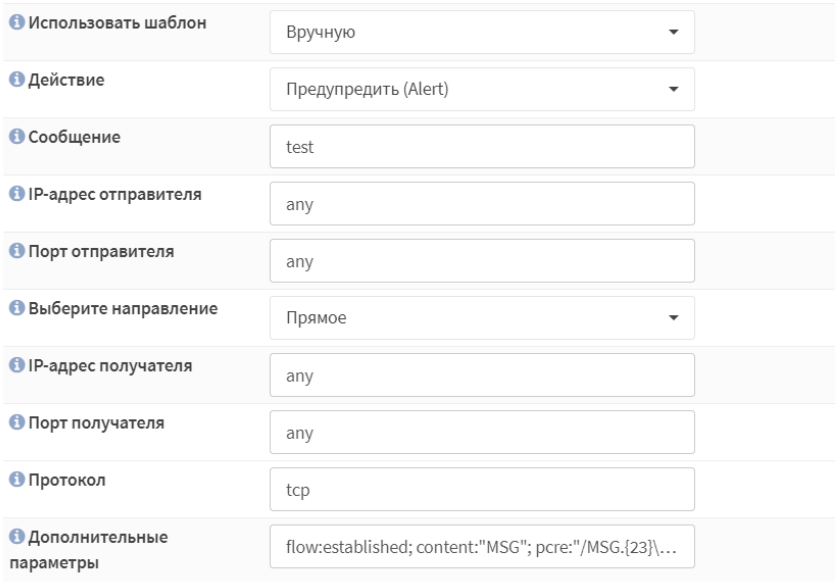


Рисунок 383 — Обнаружение вторжений: Контроль уровня приложений (редактирование: Вручную)

11.20. Настройка записи дампов трафика

Для настройки записи дампов трафика необходимо перейти в «Интерфейсы» - «Диагностика» - «Захват пакетов». Категория «Захват пакетов» позволяет запустить сканирование сети по выбранному сетевому интерфейсу с возможностью дальнейшего экспорта дампа трафика.

Для этого группе настроек «Захват пакетов» в поле «Интерфейсы» необходимо выбрать сетевые 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 источника. В поле «Длина пакета» необходимо ввести длину пакета (в битах). В поле «Количество» необходимо ввести количество пакетов, которые будут захватываться (рисунок 384).

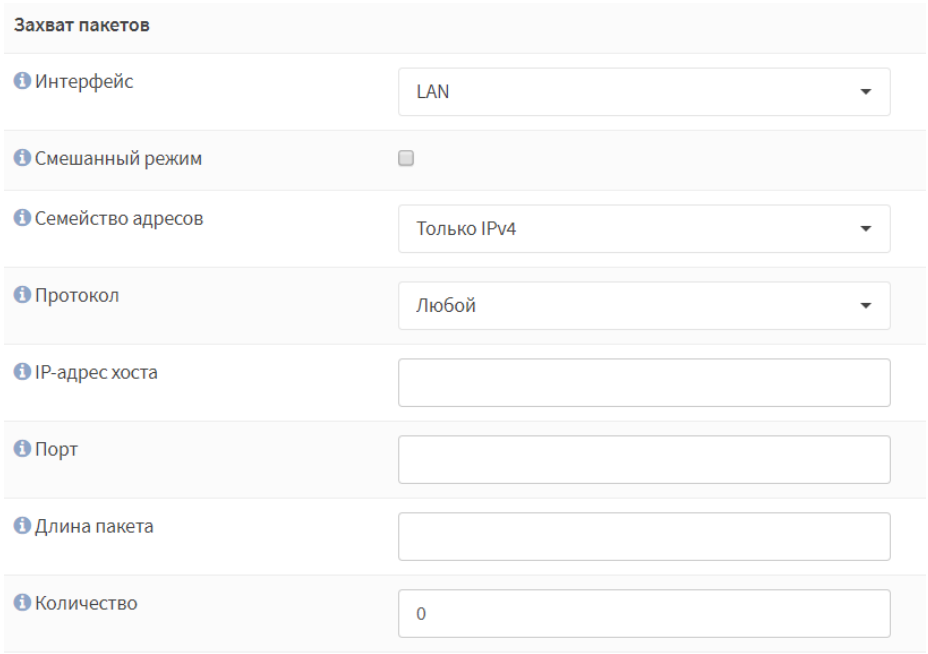


Рисунок 384 — Интерфейсы: Диагностика: Захват пакетов (настройка захвата пакетов)

В группе настроек «Просмотр настроек» в поле «Уровень детализации» необходимо выбрать уровень детализации информации о захваченных пакетах. В поле «Обратный запрос DNS» необходимо установить флажок для захвата пакетов, ассоциируемых со всеми IP-адресами обратного запроса DNS. Для начала захвата необходимо нажать на кнопку «Запустить». Для остановки захвата пакетов необходимо нажать на кнопку «Остановить». Для скачивания захваченных пакетов необходимо нажать на кнопку «Скачать

захваченные пакеты». Для удаления захваченных пакетов необходимо нажать на кнопку «Удалить захваченные пакеты». Для просмотра захваченных пакетов в виде таблицы необходимо нажать на кнопку «Просмотр захваченных пакетов» (рисунок 385).

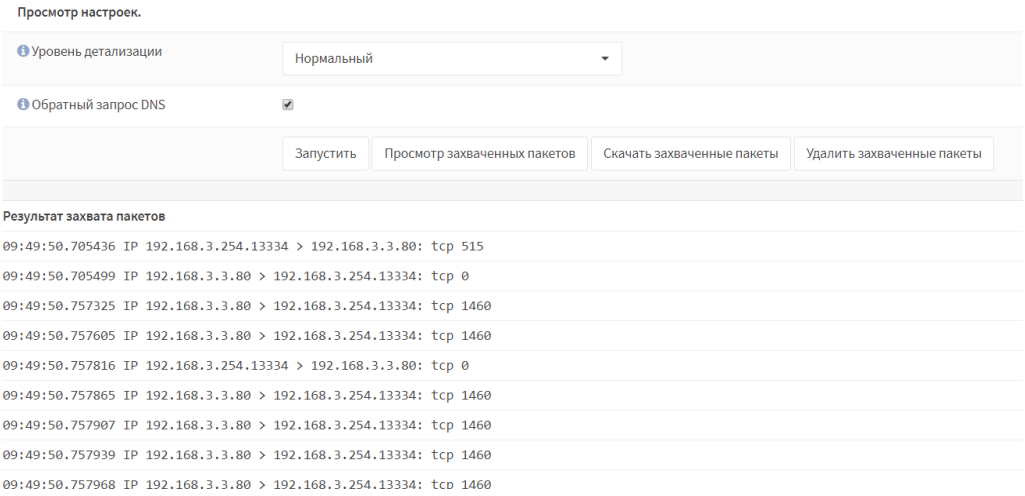


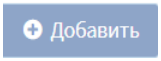
Рисунок 385— Интерфейсы: Диагностика: Захват пакетов (настройка просмотра)

11.21. Настройка Active Directory сервера аутентификации (импорт пользователей)

ПК «InfoWatch ARMA Industrial Firewall» поддерживает использование внешнего LDAP-сервера для аутентификации пользователей.

Для настройки LDAP-сервера ПК «InfoWatch ARMA Industrial Firewall» должен иметь доступ к серверу LDAP по сети. Далее приводятся шаги по настройке и использованию внешнего Active Directory LDAP-сервера.

Шаг 1 — Добавление нового сервера LDAP

Для добавления нового сервера LDAP необходимо перейти в раздел «Система» - «Доступ» - «Серверы» и нажать 

в верхнем правом углу после чего необходимо заполнить поля в соответствии с таблицей (таблица 27).

Таблица 27 — Добавление нового сервера LDAP

Поле	Значение	Комментарий

Название	Test_LDAP	Название сервера
Тип	LDAP	-
Имя хоста или IP-адрес	10.10.2.1	Доменное имя сервера AD LDAP
Значение порта	389	Номер порта, 389 по умолчанию
Транспортный протокол	TCP — стандартный	Стандартный
Центр сертификации пиров	Не выбрано	При использовании SSL-шифрования необходимо выбрать CA
Версия протокола	3	-
Привязать параметры доступа	Уникальное имя пользователя: arma@opc.local Пароль: TVKLcWM6	Параметры взяты с интернет ресурса
Область поиска	Целое поддерево	-
Базовый DN:	dc=opc,dc=local	-
Контейнеры аутентификации	Выбрать (рисунок 386)	Необходимо выбрать контейнеры из списка (в примере выбрано: "CN=Users,DC=opc,DC=local,OU…."

Расширенный запрос	-	Расширить запрос, ограничить результаты для лиц
Начальный шаблон	Microsoft AD	Тип сервера LDAP
Атрибут присвоения имени пользователя	sAMAccountName	Автозаполнение на основе начального шаблона

После внесения изменений необходимо нажать кнопку «Сохранить» для сохранения настроек.

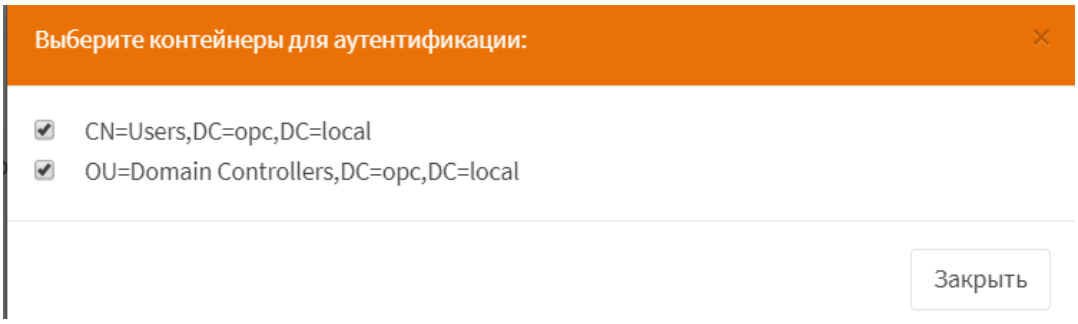


Рисунок 386 — Выбор контейнеров аутентификации

Шаг 2 — Тест

Для проверки правильности настройки сервера необходимо перейти в раздел меню «Система» - «Доступ» - «Средство проверки». В поле «Сервер аутентификации» необходимо выбрать созданный на шаге 1 Active Directory LDAP-сервер и ввести существующие пользовательские учетные данные, например, «arma», в поле «Имя пользователя» и пароль, например, «TVKLcWM6», в поле «Пароль». В случае успешного подключения должно отобразиться сообщение об успешной аутентификации (рисунок 387).

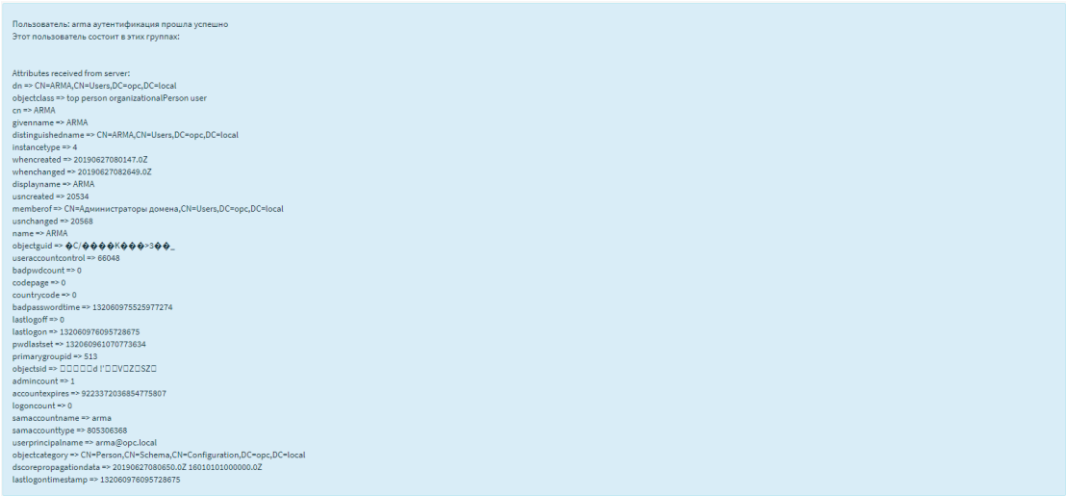


Рисунок 387 — Тестирование сервера

Шаг 3 — Импорт пользовательских учетных записей

Для предоставления доступа к графическому веб-интерфейсу пользовательским учетным записям LDAP-сервера, необходимо их импортировать. В разделе меню настроек пользователей «Система» - «Доступ» - «Пользователи», появится значок импорта  в правом нижнем углу формы (рисунок 388).

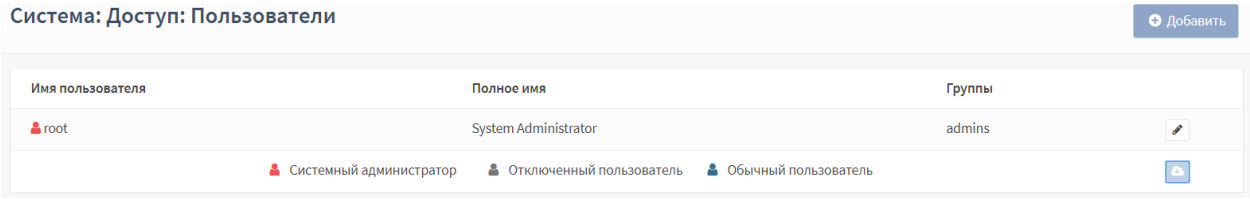


Рисунок 388 — Импорт пользователей

Необходимо нажать на значок импорта, чтобы импортировать пользовательские учетные записи. Импорт произведен успешно, если после нажатия кнопки не появилось сообщений об ошибке (рисунок 389).

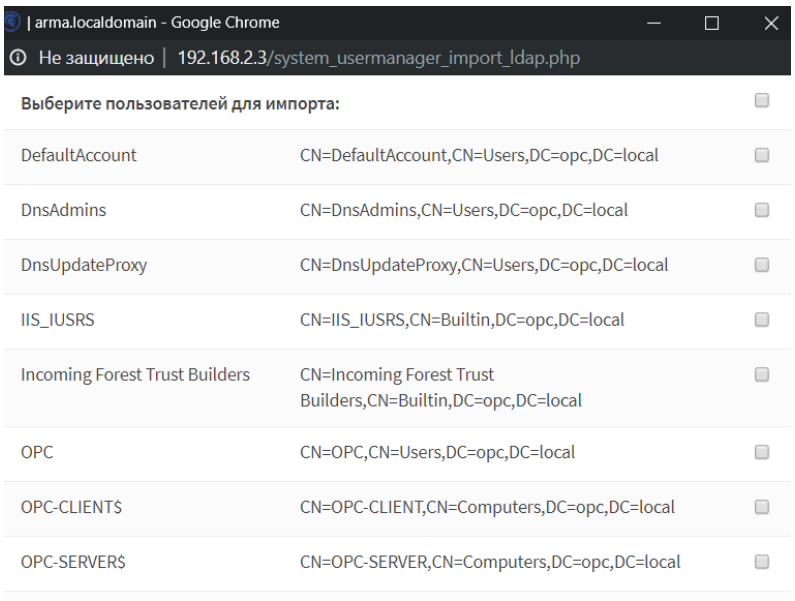


Рисунок 389 — Выбор импортируемых пользователей

Шаг 4 — Обновление пользовательской учетной записи LDAP

Далее необходимо перейти в раздел меню настроек пользователей «Система» - «Доступ» - «Пользователи». Необходимо убедиться, что в данном разделе будут отображены все учетные записи, включая импортированные из LDAP-сервера.

Шаг 5 — Обновление настроек доступа к системе

На данном шаге необходимо изменить настройки по умолчанию, чтобы пользовательские учетные записи LDAP получили доступ к системе.

В разделе «Система» - «Настройки» - «Администрирование» необходимо изменить сервер аутентификации на подключенный сервер LDAP в пункте «Сервер». После внесения изменений для сохранения настроек необходимо нажать кнопку «Сохранить».

11.22. Добавление правил МЭ и СОВ для пользователей сервера аутентификации Active Directory

Для добавления пользователей внешнего сервера аутентификации Active Directory необходимо настроить Active Directory сервер аутентификации в соответствии с разделом 11.21 настоящего руководства.

Далее необходимо настроить Портал авторизации, через который пользователи сервера аутентификации Active Directory получат доступ к ПК «InfoWatch ARMA Industrial Firewall».

Перед началом настройки Портала авторизации в ПК «InfoWatch ARMA Industrial Firewall» должны быть установлены интерфейсы WAN (с доступом в Интернет) и LAN.

Для настройки Портала авторизации необходимо добавить новый интерфейс, через который пользователи из внутренней сети получат доступ к Порталу авторизации. Для этого необходимо перейти в раздел «Интерфейсы» - «Назначения портов», нажать «+» для добавления нового интерфейса и нажать кнопку «Сохранить». Далее необходимо перейти в «Интерфейсы» - «OPT1», поставить флажок в «Включен» и заполнить настройки интерфейса в соответствие с таблицей (таблица 28).

Таблица 28 — Настройка интерфейса

Поле	**Значение**
Описание	GUESTNET
Блокировать	Не выбрано
Блокировать частные сети	Не выбрано
Блокировать bogon сети	Не выбрано
Тип конфигурации IPv4	Статический IPv4
Тип конфигурации IPv6	Отсутствует
MAC-адрес	(Оставить пустым)
Максимальный размер кадра	(Оставить пустым)
Максимальный размер сегмента	(Оставить пустым)
Скорость и двусторонний режим передачи данных	По умолчанию

Статический адрес IPv4	192.168.200.1/24
Публичный IPv4-адрес шлюз	Автодетектирование

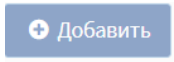
Далее необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Для настройки DHCP-сервера необходимо перейти в раздел «Службы» - «DHCPv4» - «GUESTNET» и заполнить поля в соответствие с таблицей (таблица 29).

Таблица 29 — Настройки DHCP-сервера

Поле	**Значение**
Включить	Включен
Диапазон	192.168.200.100 - 192.168.200.200
DNS-серверы	192.168.200.1
Шлюз	192.168.200.1

Необходимо нажать кнопку «Сохранить».

Далее необходимо добавить два разрешающих правила. Для добавления первого разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать 

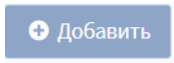
. И заполнить поля в соответствие с таблицей (таблица 30).

Таблица 30 — Разрешить вход в Портал авторизации

Поле	**Значение**
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	TCP
Отправитель	GUESTNET сеть

Получатель	GUESTNET адрес
Диапазон портов назначения	(Другое) 8000 / (Другое) 10000
Категория	Общие правила GuestNet
Описание	Разрешить вход в Портал авторизации

Необходимо нажать кнопку «Сохранить».

Для добавления второго разрешающего правила межсетевого экрана необходимо перейти в раздел «Межсетевой экран» - «Правила» - «GUESTNET» и нажать 

. И заполнить поля в соответствие с таблицей (таблица 31).

Таблица 31 — Разрешить гостевые сети

Поле	**Значение**
Действие	Разрешить
Интерфейс	GUESTNET
Протокол	Any
Отправитель	GUESTNET сеть
Получатель	Любой
Диапазон портов получателя	Любой
Категория	Общие правила GuestNet
Описание	Разрешить гостевую сеть

Необходимо нажать кнопку «Сохранить», а затем кнопку «Применить изменения».

Далее необходимо загрузить шаблон страницы авторизации для пользователей Портала авторизации. Для этого необходимо перейти в «Службы» - «Портал авторизации» - «Шаблоны» и нажать на  внизу

таблицы для скачивания шаблона страницы авторизации пользователей. Далее нажать на «+», ввести в «Имя шаблона» название шаблона «Test», выбрать скаченный шаблон, нажав на кнопку «Выберите файл» и нажать «Загрузить», а затем кнопку «Применить».

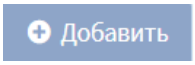
Для создания новой зоны авторизации необходимо перейти в раздел «Службы» - «Портал авторизации» - «Администрирование» и нажать «+». Необходимо заполнить поля редактирования зоны авторизации в соответствие с таблицей (таблица 32).

Таблица 32 — Настройки зоны авторизации

Поле	**Значение**
Включено	Выбрано
Интерфейсы	GUESTNET
Аутентификация через	Active Directory сервер
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)
Разрешенные MAC-адреса	(оставить пустым)
Пользовательский шаблон	Test [шаблон созданный в «Службы» - «Портал авторизации» - «Шаблоны»]
Описание	Гостевая

Нажать кнопку «Сохранить», а затем кнопку «Применить».

Открыть на внешнем устройстве любой браузер и ввести запрос: «8.8.8.8». В окне авторизации необходимо ввести аутентификационные данные пользователя сервера аутентификации Active Directory и нажать кнопку «Войти».

Для добавления правила межсетевого экрана, которое будет распространяться на пользователей сервера аутентификации Active Directory необходимо перейти в раздел «Межсетевой экран» - «Правила» - «OPT1» и нажать кнопку 

.

При создании правила в поле «Отправитель» необходимо выбрать «OPT1 сеть». Заполнение остальных полей описано в подразделе 11.15.2 настоящего руководства.

Необходимо нажать на кнопку «Сохранить», а затем кнопку «Применить изменения» для сохранения и применения внесенных изменений соответственно.

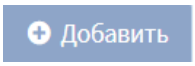
Для добавления правила системы обнаружения вторжений, которое будет распространяться на пользователей сервера аутентификации Active Directory необходимо перейти в раздел «Обнаружение вторжений» - «Контроль уровня приложений» и нажать на кнопку  для создания нового правила.

В поле «IP-адрес отправителя» необходимо ввести подсеть сетевого интерфейса OPT1 (например, 192.168.2.0/24). Заполнение остальных полей описано в подразделах 11.19, 11.9 настоящего руководства. Нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений.

11.23. Ограничение пропускной способности для пользователей сервера аутентификации Active Directory

Для ограничения пропускной способности пользователей сервера аутентификации Active Directory необходимо добавить сервер аутентификации Active Directory. Добавление и настройка сервера аутентификации Active Directory описано в подразделе 11.21 настоящего

руководства. Далее необходимо настроить Портал авторизации. Настройка Портала авторизации подробнее описана в подразделе 11.22 настоящего руководства.

Для добавления ограничения трафика необходимо добавить канал с заданной пропускной способностью. Для этого необходимо перейти в «Межсетевой экран» - «Ограничение трафика» - «Настройки» - «Каналы» и нажать на кнопку 

.

При редактировании канала необходимо установить флажок напротив поля «Включен». В поле «Пропускная способность» необходимо ввести пропускную способность канала. В поле «Единицы измерения пропускной способности» необходимо выбрать единицы измерения пропускной способности. В поле «Очередь» необходимо ввести количество динамических очередей. В поле маска необходимо выбрать:

– «получатель», чтобы каждому IP-адресу получателя была указана пропускная способность;

– «отправитель», чтобы каждому IP-адресу отправителя была указана пропускная способность;

– «не выбрано», если необходимо создать канал с фиксированной пропускной способностью.

В поле «Buckets» необходимо ввести размер хеш-таблицы, используемой для хранения динамических каналов. В поле «Включить CoDel» необходимо установить флажок для включения CoDel (планировщик задержек). В поле «(FQ-)CoDel target» необходимо ввести минимально допустимую задержку персистентной очереди. В поле «(FQ-)CoDel intarval» необходимо ввести интервал перед отбросом пакетов. В поле «(FQ-)CoDel ECN» необходимо установить флажок для включения уведомления. В поле «(FQ-)CoDel quantum» необходимо ввести количество байт, которые может принять очередь перед тем, как она будет передвинута в конец списка очередей. В поле «Задержка» необходимо ввести задержку по этому каналу. В поле «Описание» необходимо добавить описание этого канала.

Необходимо нажать на кнопку «Применить» для сохранения внесенных изменений.

Далее необходимо добавить правило, которое будет применяться к настроенному каналу для пользователей сервера аутентификации Active Directory. Для этого необходимо перейти в «Межсетевой экран» - «Ограничение трафика» - «Настройки» - «Правила» и нажать «+».

При редактировании правила необходимо установить флажок напротив поля «Включить» при необходимости включения редактируемого правила. В поле «Последовательность» необходимо выбрать порядок проверки правил в наборе правил. В поле «Интерфейс» необходимо выбрать сетевой интерфейс «OPT1», на который будут приходить пакеты для проверки соответствия данному правилу. В поле «Интерфейс 2» необходимо выбрать «отсутствует». В поле «Протокол» необходимо выбрать протокол, для которого будет выполняться это правило. В поле «Отправитель» необходимо выбрать отправителя, на пакеты которого будут распространяться правила В поле «Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Отправитель». В поле «Получатель» необходимо ввести отправителя. В поле «Инвертировать» необходимо установить флажок для того, чтобы в качестве отправителя выбрать все адреса кроме указанного в поле «Получатель». В поле «dst-port» необходимо ввести порт получателя. В поле «Направление» выбрать направление правила. В поле «Цель» необходимо выбрать созданный канал. В поле «Описание» необходимо ввести описание правила. Для сохранения необходимо нажать кнопку «Сохранить».

11.24. Импорт правил СОВ по SMB

11.24.1. Импорт правил СОВ по SMB по запросу пользователя

Для импорта базы решающих правил по запросу пользователя по протоколу SMB необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил.

Для просмотра архива баз решаюших правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта» - «Настройки». В поле «Включен» поставить флажок. В поле «Протокол» выбрать «SMB». В поле «Адрес» ввести IP-адрес удаленного компьютера. В поле «Samba сервис» необходимо ввести название samba сервиса. В поле «Логин», «Пароль» необходимо ввести учетные данные для подключения к samba серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Выполнить».

Перейти в разделе «Обнаружение вторжений» - «Администрирование» - «Обновления» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (рисунок 390).

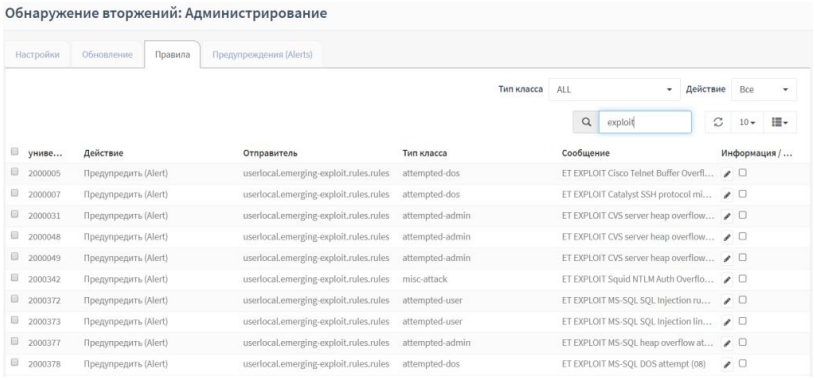


Рисунок 390 — Список правил СОВ (импорт по запросу пользователя)

11.24.2. Импорт правил СОВ по SMB по расписанию

Для настройки импорта базы решающих правил по расписанию пользователя по протоколу SMB необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил, расписание для импорта правил.

Для просмотра архива баз решаюших правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта» - «Настройки». В поле «Включен» поставить флажок. В поле «Протокол» выбрать «SMB». В поле «Адрес» ввести IP-адрес удаленного компьютера. В поле «Samba сервис» необходимо ввести название samba сервиса. В поле «Логин», «Пароль» необходимо ввести учетные данные для подключения к samba серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Применить».

Для импорта наборов правил СОВ по расписанию необходимо создать расписание. Для этого необходимо перейти в раздел Обнаружение вторжений» - «Настройка импорта» - «Расписание». В правилах задается периодичность запуска задачи, а не конкретное время запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле

«Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду «Импорт правил СОВ». В поле «Параметры» ввести параметры. В поле «Описание» необходимо ввести описание задачи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения задачи Cron.

Далее необходимо подождать заданный промежуток времени.

Перейти в раздел «Обнаружение вторжений» - «Администрирование» - «Обновления» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (рисунок 391).

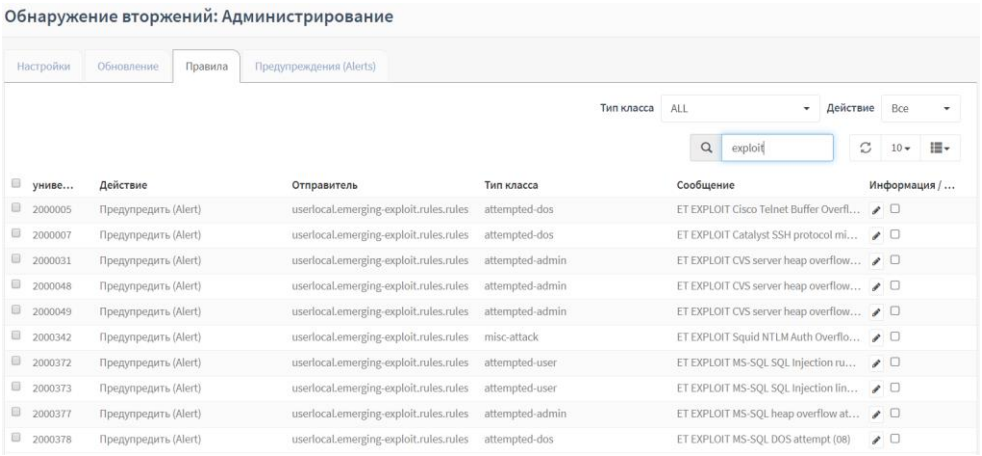


Рисунок 391 — Список правил СОВ (импорт по расписанию)

11.25. Импорт правил СОВ по FTP

11.25.1. Импорт правил СОВ по FTP по запросу пользователя

Для импорта базы решающих правил по запросу пользователя по протоколу FTP необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил.

Для просмотра архива баз решаюших правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта» - «Настройки». В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Выполнить».

Перейти в разделе «Обнаружение вторжений» - «Администрирование» - «Обновления» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (рисунок 390).

11.25.2. Импорт правил СОВ по FTP по расписанию

Для настройки импорта базы решающих правил по расписанию пользователя по протоколу FTP необходимо убедиться в наличии архива с правилами, а затем настроить импорт правил, расписание для импорта правил.

Для просмотра архива баз решаюших правил на удаленном компьютере необходимо перейти в папку формата armaif_[версия ПК «InfoWatch ARMA Industrial Firewall»], например, armaif_3.0. В папке найти архив наборов

решающих правил формата «tar.gz». Название архива имеет формат — «rulesets_[версия ПК «InfoWatch ARMA Industrial Firewall»]_[версия правил].tar.gz», например, rulesets_3.0_1.1.2.tar.gz. При импорте правил выбирается файл правил с наиболее новой версией.

Далее необходимо настроить импорт правил в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall». Для этого необходимо перейти в «Обнаружение вторжений» - «Настройка импорта» - «Настройки». В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к корневой папке» необходимо ввести путь к корневой папке при необходимости. В поле «Интервал» необходимо ввести интервал ожидания до повторной попытки передачи в случае ошибки (в секундах). Нажать кнопку «Применить».

Для импорта наборов правил СОВ по расписанию необходимо создать расписание. Для этого необходимо перейти в раздел «Обнаружение вторжений» - «Настройка импорта» - «Расписание». В правилах задается периодичность запуска задачи, а не конкретное время запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду «Импорт правил СОВ». В поле «Параметры» ввести параметры. В поле «Описание» необходимо ввести описание задачи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения задачи Cron.

Далее необходимо подождать заданный промежуток времени.

Перейти в разделе «Обнаружение вторжений» - «Администрирование» - «Обновления» и нажать кнопку «Скачать и обновить правила».

По завершении настройки импорта необходимо перейти в «Обнаружение вторжений» - «Администрирование» - «Правила» и найти импортируемые правила (рисунок 391).

11.26. Экспорт конфигурации и наборы правил СОВ по SMB

11.26.1. Экспорт конфигурации и наборы правил СОВ по SMB по запросу пользователя

Для настройки экспорта конфигурации ПК «InfoWatch ARMA Industrial Firewall» в формате XML на samba-сервер по запросу пользователя необходимо в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall» перейти раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Настройки». В поле «Протокол» необходимо выбрать «SMB». В поле «Samba сервис» необходимо ввести название samba-сервиса. В поле «Адрес» необходимо ввести IP-адрес удаленного компьютера. В поле «Логин», «Пароль» необходимо ввести учетные данные для подключения на samba-сервер. В поле «Относительный путь» необходимо указать в какую папку необходимо экспортировать конфигурацию и наборы правил СОВ. В поле «Интервал» необходимо выбрать интервал времени в минутах, через который конфигурация и наборы правил СОВ будут экспортироваться повторно в случае неудачной попытки выгрузки. Необходимо нажать кнопку «Выполнить».

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экпортируемой конфигурации и наборов правил СОВ. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» и наборы правил СОВ экспортируются в архиве формата «tar».

11.26.2. Экспорт конфигурации и наборы правил СОВ по SMB по расписанию

Для настройки экспорта конфигурации ПК «InfoWatch ARMA Industrial Firewall» в формате XML на samba-сервер по расписанию необходимо в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall» перейти раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Настройки». В поле «Протокол» необходимо выбрать «SMB». В поле «Samba сервис» необходимо ввести название samba-сервиса. В поле «Адрес» необходимо ввести IP-адрес удаленного компьютера. В поле «Логин», «Пароль» необходимо ввести учетные данные для подключения к samba-серверу. В поле «Относительный путь» необходимо указать в какую папку необходимо экспортировать конфигурацию и наборы правил СОВ. В поле «Интервал» необходимо выбрать интервал времени в минутах, через который конфигурация и наборы правил СОВ будут экспортироваться повторно в случае неудачной попытки выгрузки. Необходимо нажать кнопку «Применить».

Для экспорта конфигурации ПК «InfoWatch ARMA Industrial Firewall» и наборов правил СОВ по расписанию в формате XML на samba-сервер необходимо создать расписание. Для этого необходимо перейти в раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Расписание». В правилах задается периодичность запуска задачи, а не конкретное время запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду «Экспорт

конфигурации». В поле «Параметры» ввести параметры. В поле «Описание» необходимо ввести описание задачи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения задачи Cron.

Необходимо подождать заданный интервал.

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экпортируемой конфигурации и наборов правил СОВ. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» и наборы правил СОВ экспортируются в архиве формата «tar».

11.27. Экспорт конфигурации и наборы правил СОВ по FTP

11.27.1. Экспорт конфигурации и наборы правил СОВ по FTP по запросу пользователя

Для настройки экспорта конфигурации ПК «InfoWatch ARMA Industrial Firewall» в формате XML на FTP-сервер по запросу пользователя необходимо в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall» перейти раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Настройки». В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к файлу» необходимо указать папку для экспорта конфигурации. В поле «Интервал ожидания» необходимо выбрать интервал времени в минутах, через который конфигурация будет экспортироваться повторно в случае неудачной попытки выгрузки.

Необходимо нажать кнопку «Выполнить».

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экпортируемой конфигурации и наборов правил СОВ. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» и наборы правил СОВ экспортируются в архиве формата «tar».

11.27.2. Экспорт конфигурации и наборы правил СОВ по FTP по расписанию

Для настройки экспорта конфигурации ПК «InfoWatch ARMA Industrial Firewall» в формате XML на FTP-сервер по расписанию необходимо в графическом интерфейсе ПК «InfoWatch ARMA Industrial Firewall» перейти раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Настройки». В поле «Протокол» необходимо выбрать «FTP». В поле «Адрес» необходимо ввести IP-адрес FTP-сервера. В поле «Имя пользователя», «Пароль» необходимо ввести учетные данные для подключения к FTP серверу. В поле «Путь к файлу» необходимо указать папку для экспорта конфигурации. В поле «Интервал ожидания» необходимо выбрать интервал времени в минутах, через который конфигурация будет экспортироваться повторно в случае неудачной попытки выгрузки.

Необходимо нажать кнопку «Применить».

Для экспорта конфигурации ПК «InfoWatch ARMA Industrial Firewall» и наборов правил СОВ по расписанию в формате XML на FTP-сервер необходимо создать расписание. Для этого необходимо перейти в раздел «Система» - «Конфигурации» - «Настройки экспорта» - «Расписание». В правилах задается периодичность запуска задачи, а не конкретное время запуска задачи.

При редактировании задачи Cron в поле «Включен» необходимо установить флажок для разрешения выполнения задачи Cron. В поле «Мин» необходимо выбрать время в минутах, когда будет запущена задача. В поле «Ч» необходимо выбрать время в часах, когда будет запущена задача. В поле «День месяца» необходимо выбрать день месяца, когда будет запущена задача. В поле «Месяцы» необходимо выбрать месяцы, когда будет запущена задача. В поле «День недели» необходимо выбрать день недели, когда будет запущена задача. В поле «Команда» необходимо выбрать команду «Экспорт конфигурации». В поле «Параметры» ввести параметры. В поле «Описание» необходимо ввести описание задачи.

Необходимо нажать на кнопку «Сохранить изменения» для сохранения задачи Cron.

Необходимо подождать заданный интервал.

Далее на удаленной машине необходимо перейти в настроенную папку и убедиться в наличие экпортируемой конфигурации и наборов правил СОВ. Конфигурация ПК «InfoWatch ARMA Industrial Firewall» и наборы правил СОВ экспортируются в архиве формата «tar».

11.28. Настройка DHCP сервера

Для настйроки DHCP-сервера на выбранном интерфейсе необходимо перейти в «Службы» - «DHCPv4» - «[Название интерфейса]».

В поле «Включить» необходимо поставить флажок. В поле «Блокировать неизвестных клиентов» необходимо установить флажок для разрешения получения IP-адресов только клиентам из выбранного далее диапазона. В поле «Диапазон» необходимо ввести диапазон IP-адресов, входящий в доступный диапазон, указанный в поле «Доступный диапазон». В поле «Дополнительные пулы» необходимо ввести дополнительные пулы адресов внутри подсети, которые не входят в доступный диапазон, указанный в поле «Доступный диапазон». В поле «WINS-серверы» необходимо ввести WINS-сервера. В поле «DNS-серверы» необходимо ввести DNS-серверы. В поле «Имя домена» необходимо ввести доменное имя. В поле «Список поиска доменов» необходимо ввести список поиска домена. В поле «Время аренды по умолчанию (секунд)» необходимо ввести время аренды для клиентов, которые не запрашивают конкретное время аренды. В поле «Максимальное время аренды (с)» необходимо ввести максимальное время аренды для клиентов, которые не запрашивают точное время. В поле «MTU интерфейса» необходимо ввести указание на MTU на этом интерфейсе. В поле «IP-адрес участника для аварийного переключения» необходимо ввести IP-адрес интерфейса на другом устройстве для аварийного переключения. В поле «Статический ARP» необходимо

установить флажок для включения статического ARP. В поле «Изменить формат даты» необходимо установить флажок для изменения отображения времени аренды DHCP с UTC на местное время.

В пункте «Динамический DNS» при нажатии на кнопку «Дополнительно» в поле «Включить регистрацию имен DHCP-клиентов DNS» необходимо установить флажок для включения регистрации имен DHCP-клиентов DNS и в первом поле необходимо ввести IP-адрес основного сервера доменных имен, во втором поле необходимо ввести имя доменного ключа, в третьем поле необходимо ввести секретный ключ домена (рисунок 293)

В пункте «Контроль доступа по MAC-адресам» при нажатии на кнопку «Дополнительно» в первом поле необходимо ввести список разрешенных MAC-адресов, во втором поле необходимо ввести список блокируемых MAC-адресов.

В пункте «NTP-серверы» при нажатии на кнопку «Дополнительно» в поле необходимо ввести NTP-серверы.

В пункте «TFTP-сервер» при нажатии на кнопку «Дополнительно» в поле необходимо ввести TFTP-сервер.

В пункте «LDAP URI» при нажатии на кнопку «Дополнительно» в поле необходимо ввести полный URL для LDAP-сервера.

В пункте «Включить загрузку по сети» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить загрузку по сети» для включения загрузки по сети. В первом поле необходимо ввести IP-адрес следующего сервера, во втором поле необходимо ввести имя файла BIOS, в третьем поле необходимо ввести имя файла UEFI 32bit, в четвертом поле необходимо ввести имя файла UEFI 64bit, в пятом поле необходимо ввести корневой путь.

В пункте «WPAD» при нажатии на кнопку «Дополнительно» необходимо установить флажок напротив поля «Включить автоматическую

настройку прокси-сервера» для включения автоматической настройки прокси-сервера.

В пункте «Дополнительные параметры» при нажатии на кнопку «Дополнительно» необходимо ввести дополнительные параметры, которые необходимо включить в информацию об аренде DHCP.

Нажать кнопку «Сохранить».

11.29. Настройка DHCP клиент

Для настройки DHCP-клиента необходимо в графическом интерфейсе перейти в «Интерфейсы» - «[Название интерфейса, на котором настраивается DHCP клиент]». В поле «Тип конфигурации IPv4»/ «Тип конфигурации IPv6» необходимо выбрать «DHCP». Остальные поля оставить по умолчанию. Нажать кнопку «Сохранить».

В консольном меню необходимо ввести команду «8», а затем «ping [IP-адрес DHCP-сервера]».

Убедиться, в наличие IP-адреса на выбранном интерфейсе в диапазоне DHCP-сервера.

11.30. Настройка динамической маршрутизации RIP

Для настройки динамической маршрутизации по протоколу RIP необходимо перейти в «Маршрутизация» - «Общие настройки», поставить флажок напротив «Включить», оставить все остальные настройки по умолчанию и нажать кнопку «Сохранить» (рисунок 392).

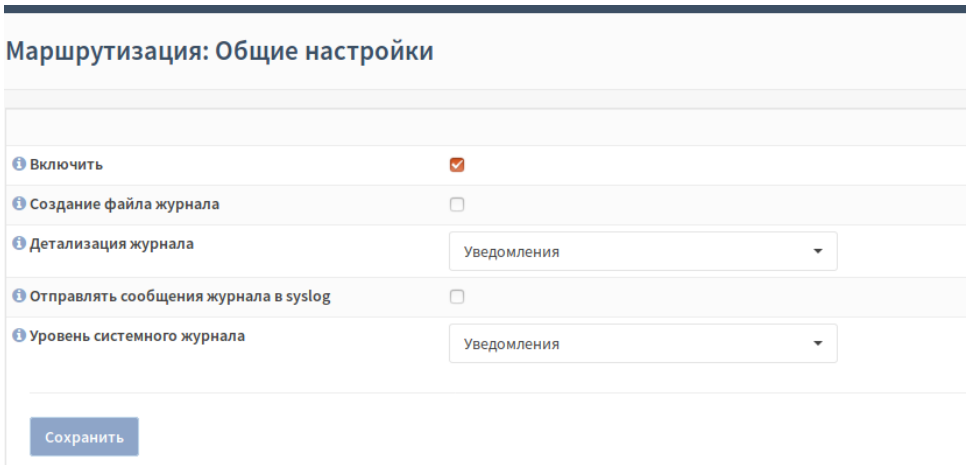


Рисунок 392 — Динамическая маршрутизация: Общие настройки

Для включения динамической маршрутизации по протоколу RIP необходимо перейти в «Маршрутизация» - «RIP», поставить флажок напротив «Включить». В поле «Версия» ввести «1» или «2». В поле «Пассивные интерфейсы» выбрать интерфейс, в который не будут посылаться пакеты. В поле «Перераспределение маршрута» выбрать другие источники маршрутизации, которые должны быть переданы другим узлам. В поле «Сети» ввести сети, по которым будут построены маршруты. Нажать кнопку «Сохранить» (рисунок 393). Настройка завершена.

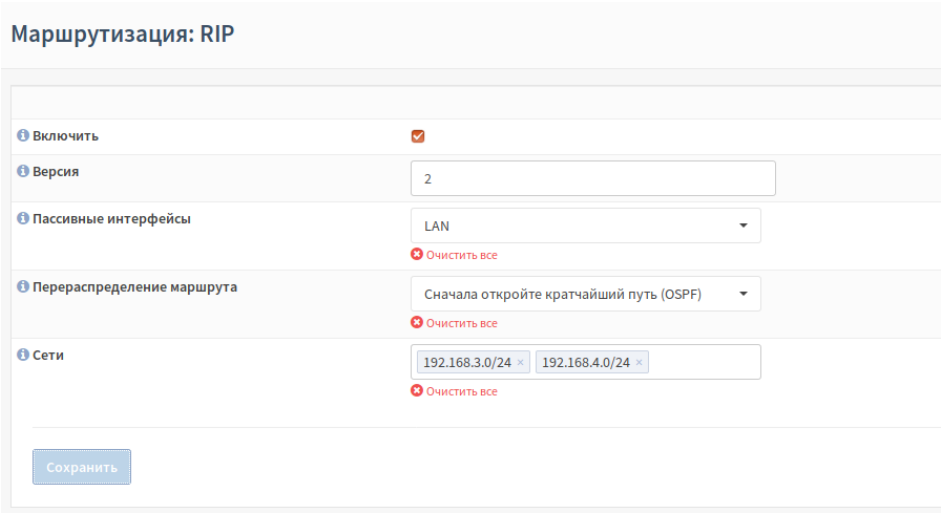


Рисунок 393 — Динамическая маршрутизация: RIP

11.31. Настройка динамической маршрутизации OSPFv2

Для настройки динамической маршрутизации по протоколу OSPFv2 необходимо перейти в «Маршрутизация» - «Общие настройки», поставить флажок напротив «Включить», оставить все остальные настройки по умолчанию и нажать кнопку «Сохранить» (рисунок 392).

Для включения динамической маршрутизации по протоколу OSPFv2 необходимо перейти в «Маршрутизация» - «OSPF» - «Общие настройки», поставить флажок напротив «Включить». В поле «Пассивные интерфейсы» выбрать интерфейс, в который не будут посылаться пакеты. В поле

«Перераспределение маршрута» выбрать другие источники маршрутизации, которые должны быть переданы другим узлам. В поле «Объявлять шлюз по умолчанию» необходимо установить флажок для того, чтобы отправить информацию о том, что имеется шлюз по умолчанию. В поле «Всегда объявлять шлюз по умолчанию» необходимо установить флажок для того, чтобы транслировать шлюз по умолчанию. В поле «Объявить метрику шлюза по умолчанию» необходимо ввести метрику шлюза по умолчанию. Нажать кнопку «Сохранить» (рисунок 394).

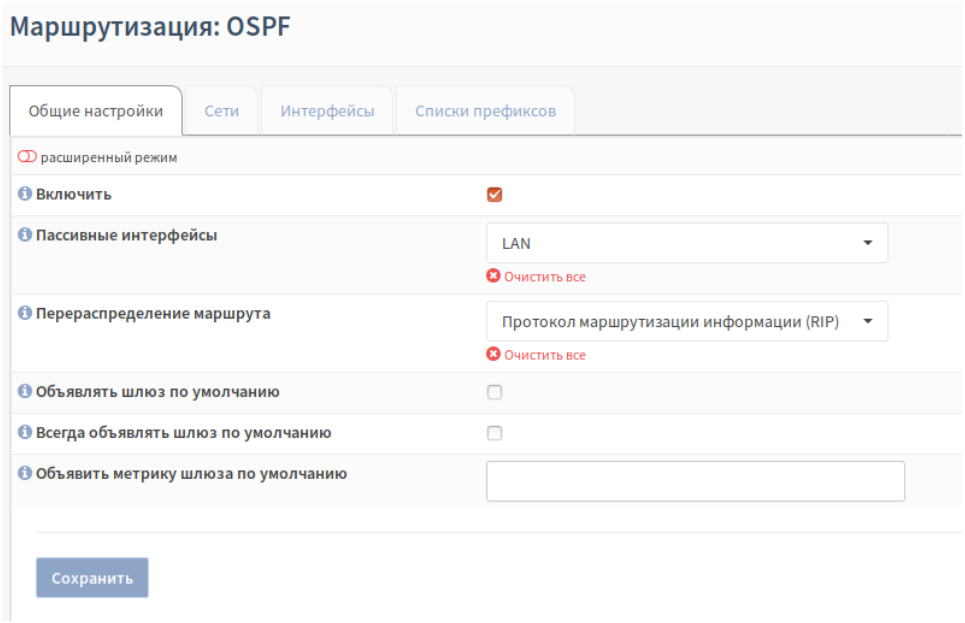


Рисунок 394 — Динамическая маршрутизация: OSPFv2: Общие настройки

Для включения задания сетей необходимо перейти в «Маршрутизация» - «OSPF» - «Сети», нажать кнопку «+». При редактировании в поле «Включен» необходимо установить флажок для включения сети. В поле «Адрес» необходимо ввести адрес сети, по которой будут построены маршруты. В поле «Маска сети» необходимо ввести маску сети (1-32). В поле «Область» необходимо ввести область сети (то есть какие маршруты принадлежат к той же группе). В поле «Список входящих префиксов» необходимо выбрать список входящих префиксов сети. В поле «Список исходящих префиксов» необходимо выбрать список исходящих префиксов сети. Необходимо нажать на кнопку «Сохранить изменения» для сохранения внесенных изменений (рисунок 395). Настройка завершена.

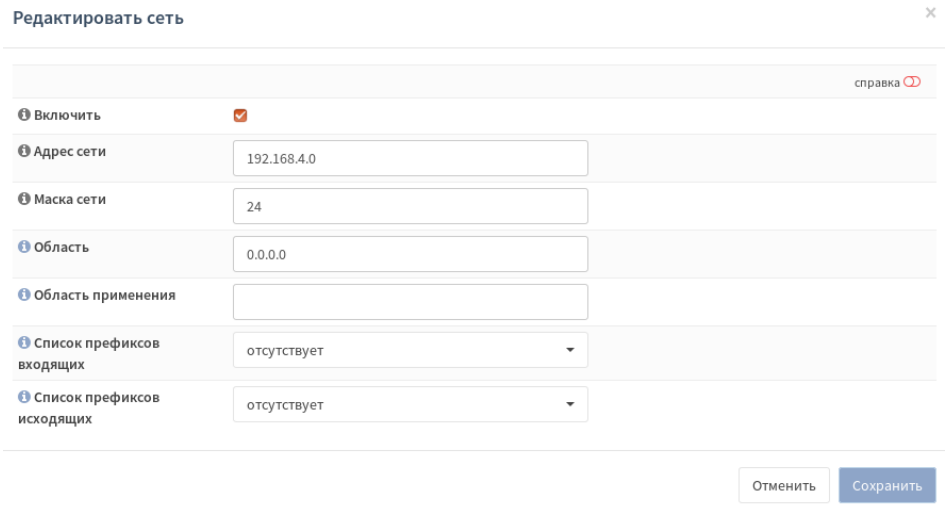


Рисунок 395 — Динамическая маршрутизация: OSPFv2: Сети

11.32. Настройка динамической маршрутизации OSPFv3

Для настройки динамической маршрутизации по протоколу OSPFv3 необходимо перейти в «Маршрутизация» - «Общие настройки», поставить флажок напротив «Включить», оставить все остальные настройки по умолчанию и нажать кнопку «Сохранить» (рисунок 392).

Для включения динамической маршрутизации по протоколу OSPFv3 необходимо перейти в «Маршрутизация» - «OSPFv3» - «Общие настройки», поставить флажок напротив «Включить». В поле «Перераспределение маршрута» выбрать другие источники маршрутизации, которые должны быть переданы другим узлам. В поле «Идентификатор маршрутизатора необходимо ввести идентификатор маршрутизатора в сети. Нажать кнопку «Сохранить».

Затем перейти в «Маршрутизация» - «OSPFv3» - «Интерфейсы» и нажать «+». В поле «Включить» поставить флажок. В поле «Интерфейс» выбрать интерфейс, через который будет проходить маршрут. В поле «Область» ввести область адресов. В поле «Тип сети» тип сети. Нажать кнопку «Сохранить» (рисунок 396). Настройка завершена.

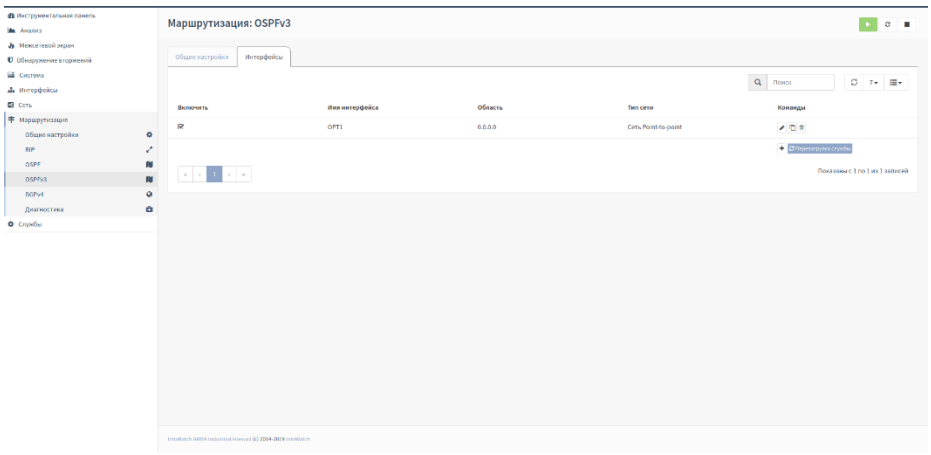


Рисунок 396 — Динамическая маршрутизация: OSPFv3: Сети

11.33. Настройка динамической маршрутизации BGPv4

Для настройки динамической маршрутизации по протоколу RIP необходимо перейти в «Маршрутизация» - «Общие настройки», поставить флажок напротив «Включить», оставить все остальные настройки по умолчанию и нажать кнопку «Сохранить» (рисунок 392).

Для включения динамической маршрутизации по протоколу BGPv4 необходимо перейти в «Маршрутизация» - «BGPv4» - «Общие настройки», поставить флажок напротив «Включить». В поле «Номер BGP AS» необходимо ввести номер AS. В поле «Перераспределение маршрута» выбрать другие источники маршрутизации, которые должны быть переданы другим узлам. Нажать кнопку «Сохранить».

Затем перейти в «Маршрутизация» - «BGPv4» - «Соседние» и нажать «+». В поле «Включить» необходимо поставить флажок. В поле «IP пира» необходимо ввести IP-адрес удаленного маршрутизатора. В поле «Удаленный AS» необходимо ввести AS удаленного маршрутизатора. В поле «Интерфейс-источник обновлений» необходимо выбрать интерфейс, через который будет проходить маршрут. Нажать кнопку «Сохранить» (рисунок 397). Настройка завершена.

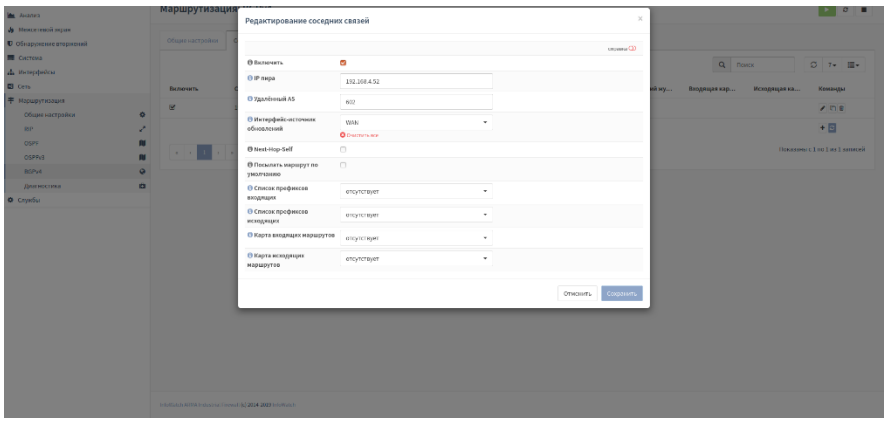


Рисунок 397 — Динамическая маршрутизация: BGPv4: Сети

11.34. Настройка отказоустойчивости каналов (LAGG)

Для настройки отказоустойчивости каналов необходимо настроить LAGG интерфейс. Для этого необходимо перейти в «Интерфейсы» - «Назначение портов» и удалить интерфейсы, на которых необходимо настроить отказоустойчивость. Затем необходимо перейти в «Интерфейсы» - «Другие типы» - «LAGG» и нажать «+». В поле «Родительский интерфейс» выбрать интерфейсы, на которых необходимо настроить отказоустойчивость. В поле «Протокол LAG» необходимо выбрать «FAILOVER». В поле «Описание» ввести описание интерфейса и нажать кнопку «Сохранить».

Далее необходимо перейти в «Интерфейсы» - «Назначение портов» и добавить созданный раннее интерфейс. Перейти в «Интерфейсы» - «[Название нового интерфейса]». В поле «Включить» поставить флажок. В поле «Тип IPv4 конфигурации» выбрать «Статический IPv4». В поле «IPv4 адрес» ввести IP-адрес LAGG интерфейса. Нажать кнопку «Сохранить».

Убедиться в успешном прохождении команды ping через ПК «InfoWatch ARMA Industrial Firewall» при поочердном отключении настроенных интерфейсов.

11.35. Настройка распределения исходящего трафика через все активные порты (LAGG)

Для настройки распределения исходящего трафика через все активные порты необходимо настроить LAGG интерфейс. Для этого необходимо

перейти в «Интерфейсы» - «Назначение портов» и удалить сетевые интерфейсы, на которых необходимо настроить распределение трафика. Затем необходимо перейти в «Интерфейсы» - «Другие типы» - «LAGG» и нажать «+». В поле «Родительский интерфейс» выбрать интерфейсы, на которых необходимо настроить распределение трафика. В поле «Протокол LAG» необходимо выбрать «ROUNDROBIN». В поле «Описание» ввести описание интерфейса и нажать кнопку «Сохранить».

Далее необходимо перейти в «Интерфейсы» - «Назначение портов» и добавить созданный раннее интерфейс. Перейти в «Интерфейсы» - «[Название нового интерфейса]». В поле «Включить» поставить флажок. В поле «Тип IPv4 конфигурации» выбрать «Статический IPv4». В поле «IPv4 адрес» ввести IP-адрес LAGG интерфейса. Нажать кнопку «Сохранить».

Убедиться в успешном прохождении команды ping через ПК «InfoWatch ARMA Industrial Firewall».

11.36. Настройка туннелирования (GRE)

Для настройки туннелирования (GRE) необходимо перейти в «Интерфейсы» - «Другие типы» - «GRE». В поле «Родительский интерфейс» необходимо выбрать интерфейс, через который будет проходить туннель. В поле «Удаленный IP-адрес пира GRE-туннеля» необходимо ввести IP-адрес конечной точки туннеля. В поле «Локальный IP-адрес GRE-туннеля» ввести IP-адрес туннеля. В поле «Удаленный IP-адрес GRE-туннеля» необходимо ввести IP-адрес удаленного туннеля. В поле «Описание» ввести описание интерфейса. Нажать кнопку «Сохранить» (рисунок 398).

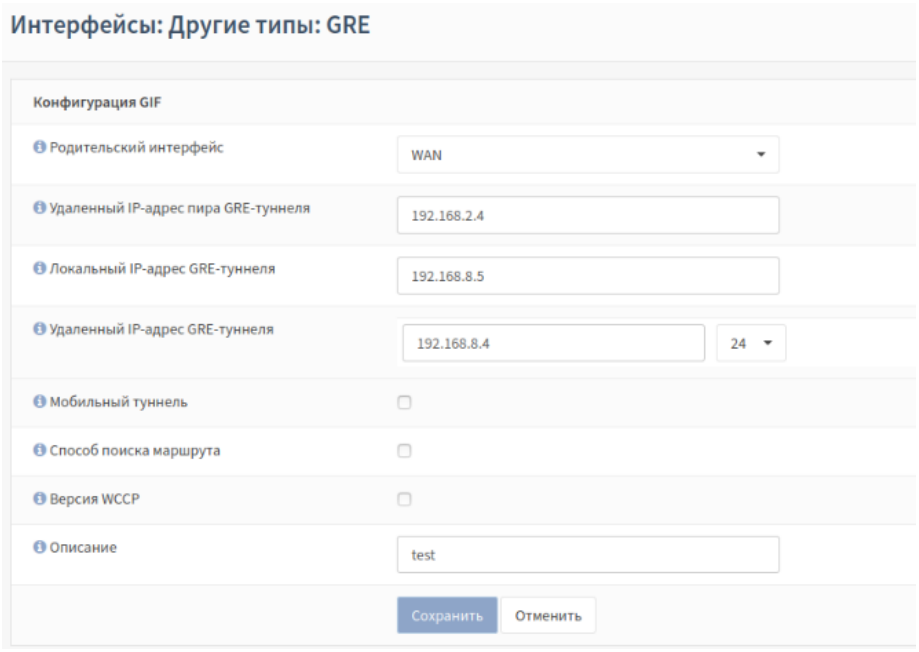


Рисунок 398 — Настройки теннеля GRE

Затем необходимо перейти на страницу «Система» - «Шлюзы» - «Единичный» и убедиться в наличие шлюза для GRE туннеля (рисунок 399, рисунок 400).

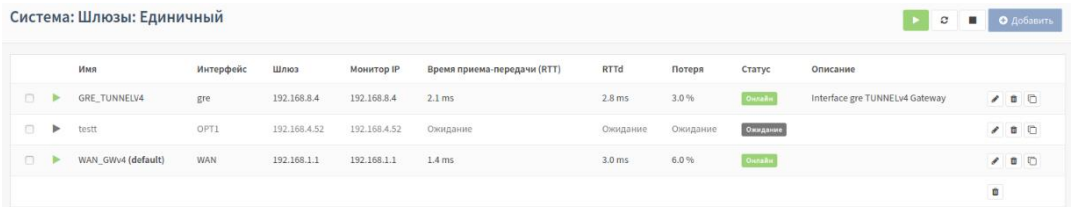


Рисунок 399 — Шлюз GRE-туннеля

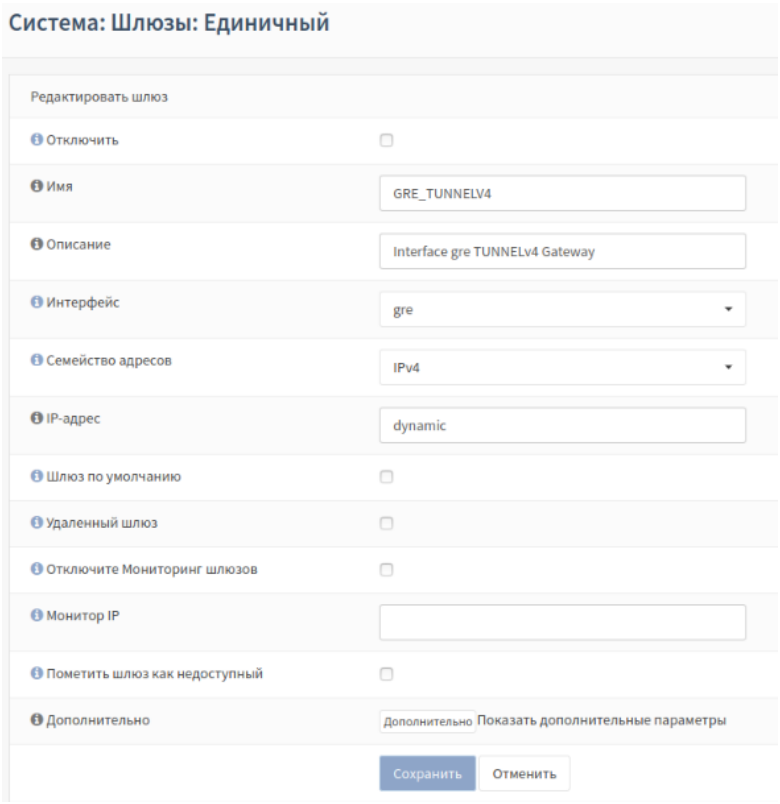


Рисунок 400 — Настройки шлюза GRE-туннеля

Убедиться в наличие связи между настраевываемой и конечной точкой туннеля.

11.37. Настройка туннелирования (GIF)

Для настройки туннелирования (GIF) необходимо перейти в «Интерфейсы» - «Другие типы» - «GIF». ». В поле «Родительский интерфейс» необходимо выбрать интерфейс, через который будет проходить туннель. В поле «Удаленный IP-адрес пира GIF-туннеля» необходимо ввести IP-адрес конечной точки туннеля. В поле «Локальный IP-адрес GIF-туннеля» ввести IP-адрес туннеля. В поле «Удаленный IP-адрес GIF-туннеля» необходимо ввести IP-адрес удаленного туннеля. В поле «Описание» ввести описание интерфейса Нажать кнопку «Сохранить» (рисунок 398).

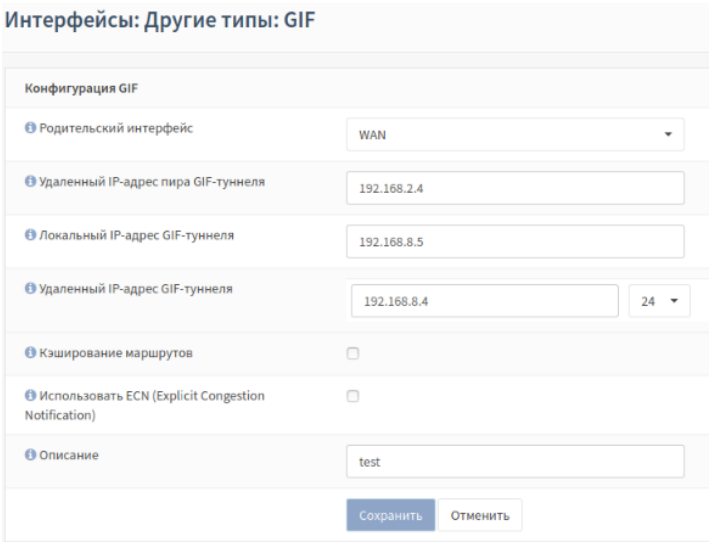


Рисунок 401 — Настройки теннеля GIF

Затем необходимо перейти на страницу «Система» - «Шлюзы» - «Единичный» и убедиться в наличие шлюза для GIF туннеля (рисунок 402, рисунок 403).

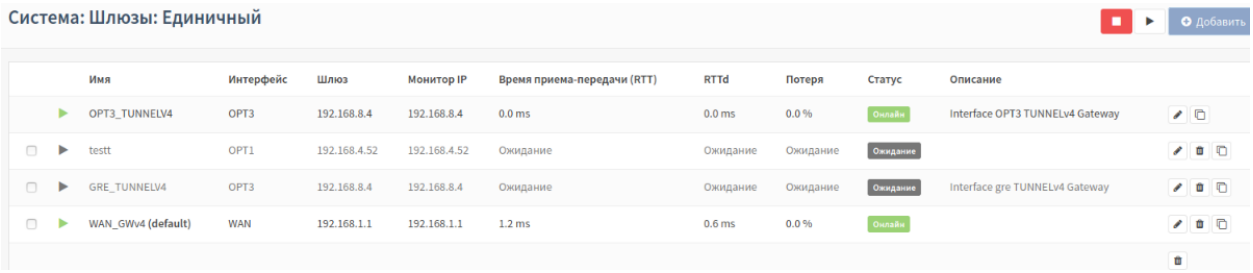


Рисунок 402 — Шлюз GIF-туннеля

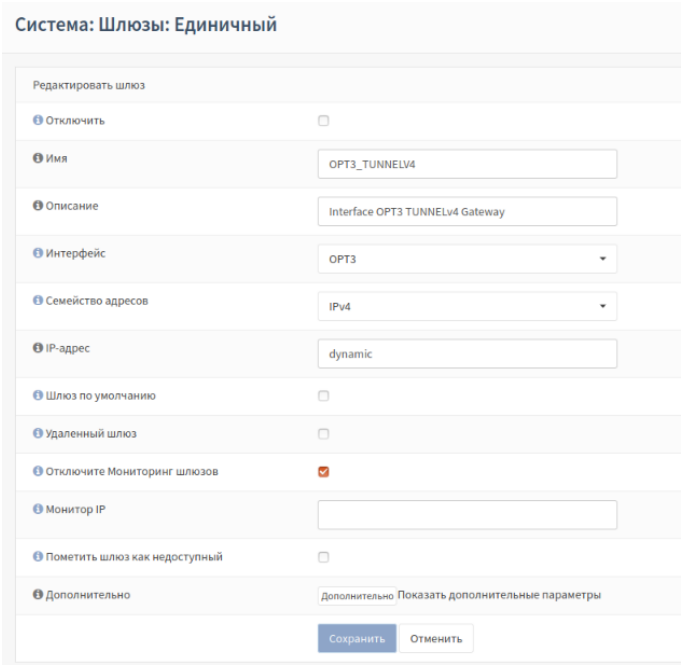


Рисунок 403 — Настройки шлюза GIF-туннеля

Убедиться в наличие связи между настраевываемой и конечной точкой туннеля.

11.38. Настройка блокирования сеанса доступа пользователя при неактивности

Для настройки блокирования сеанса доступа пользователя при неактивности необходимо перейти в «Система» - «Настройки» - «Администрирование» и в поле «Тайм-аут сессии» ввести количество минут, через которое сеанс доступа будет заблокирован при неактивности пользователя. Для сохранения настроек необходимо нажать кнопку «Сохранить».

11.39. Просмотр и фильтрация пакетов, прошедших через ПК «InfoWath ARMA Industrial Firewall»

Для просмотра дампов трафика пакетов, прошедших через ПК «InfoWath ARMA Industrial Firewall» необходимо включить систему обнаружения вторжений.

Перед включением необходимо убедиться, что отключен режим Hardware Offloading. Для выключения режима Hardware Offloading необходимо перейти в «Интерфейсы» - «Настройки» и поставить флажки напротив «CRC аппаратного обеспечения», «TSO аппаратного обеспечения», «LRO аппаратного обеспечения». Нажать кнопку «Сохранить» внизу страницы.

Для включения систмы обнаружения вторжений необходимо установить флажок напротив поля «Включен». В поле «Сравнение шаблонов» необходимо выбрать используемый алгоритм поиска подстроки при обработке пакетов:

– по умолчанию (используется алгоритм Aho-Corasick);

– Aho-Corasick (алгоритм сопоставления со «словарем», который находит подстроки из «словаря» в пакетах);

– Hyperscan (высокопроизводительная библиотека сопоставления регулярных выражений от Intel).

В поле «Интерфейсы» необходимо выбрать интерфейсы, которые будут использоваться системой обнаружения и предотвращения вторжений. Для сохранения настроек необходимо нажать на кнопку «Применить»

Для просмотра собранных дампов трафика необходимо перейти в «Сеть» - «Анализ трафика» - «Журналирование» и выбрать дамп трафика для анализа. Максимальное количество сохраняемых файлов – 20 файлов по 100 Мбайт каждый. В поле «Фильтр отображения» позволяет осуществлять фильтрацию с помощью встроенных интерактивных фильтров. Для применения фильтра необходимо нажать кнопку  .

11.40. Настройка мониторинга по SNMP (v1, v2)

Для настройки мониторинга по протоколу SNMP v1, v2 необходимо перейти в раздел «Система» - «Настройки» - «SNMP» - «Общие настройки» и выполнить следующие действия:

– установить флажок напротив «Включен»;

– установить значение в «Community String» (например, «custom»);

– нажать кнопку «Сохранить».

Настройка завершена. Для подключения к ПК «InfoWath ARMA Industrial Firewall» необходимо использовать IP-адрес, через который будет осущесвляться мониторинг. В качестве Community String необходимо использовать значение, введенное в поле «Community String».

11.41. Настройка мониторинга по SNMPv3

Для настройки мониторинга по протоколу SNMP v3 необходимо перейти в раздел «Система» - «Настройки» - «SNMP» - «Общие настройки» и выполнить следующие действия:

– во вкладке «Общие настройки»:
    - установить флажок напротив «Включен»;
    - оставить поле «Community String» пустым;
    - нажать «Сохранить».
– во вкладке «SMNPv3» создать пользователя:
    - нажать на «+» для создания пользователя;
    - установить флажок напротив «Включен»;
    - ввести имя пользователя в поле «Имя пользователя»;
    - ввести пароль в поле «Пароль»;
    - ввести ключ шифрования в поле «Ключ шифрования»;
    - нажать «Сохранить».

Настройка завершена. Для подключения к ПК «InfoWath ARMA Industrial Firewall» необходимо использовать IP-адрес, через который будет осуществляться мониторинг, и учетные данные созданного пользователя.

11.42. Создание сертификата

Для создания сертификата необходимо создать доверенный центр сертификации, создать сертификат, используя доверенный центр сертификации, а затем добавить сертификат в веб-браузер.

Для создания доверенного цетра сертификации необходимо перейти в «Система» - «Доверенные сертификаты» - «Полномочия» и нажать кнопку «+Добавить». В поле «Название» ввести название центра сертификации. В поле «Метод» выбрать «Создать внутренний центр сертификации». В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм шифрования. В поле «Время существования (д)» необходимо ввести количество дней действия Центра Сертификации. В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл.

Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя. Нажать кнопку «Сохранить».

Для создания сертификата необходимо перейти в «Система» - «Доверенные сертификаты» - «Сертификаты» и нажать кнопку «+Добавить». В поле «Метод» выбрать «Создать внутренний сертификат». В поле «Название» необходимо ввести название сертификата. В поле «Центр сертификации» необходимо выбрать созданный раннее Центр Сертификации. В поле «Тип» необходимо выбрать «Сертификат сервера». В поле «Длина ключа (бит)» необходимо выбрать длину ключа. В поле «Алгоритм Дайджеста» необходимо выбрать алгоритм шифрования. В поле «Время существования (д)» необходимо ввести ввести количество дней действия сертификата. В поле «Расположение секретного ключа» необходимо выбрать «Сохранить на этом межсетевом экране». В поле «Код страны» необходимо выбрать страну. В поле «Штат или область» необходимо выбрать штат или область, где находится доменное имя компании. В поле «Город» необходимо ввести город. В поле «Организация» необходимо ввести название организации. В поле «Эл. Почта» необходимо ввести адрес электронной почты администратора или службы поддержки. В поле «Стандартное имя» необходимо ввести доменное имя. В поле «Альтернативные имена»: необходимо выбрать тип альтернативного имени и ввести его имя. Нажать кнопку «Сохранить».

Необходимо перейти в «Система» - «Доверенные сертификаты» - «Сертификаты» и скачать созданный сертификат.

Затем необходимо добавить сертификат в список доверенных сертификатов в веб-браузере. Далее расписан пример добавления сертификата для веб-браузера Google Chrome.

В веб-браузере Google Chrome необходимо перейти в меню «Настройки» - «Дополнительные настройки» и нажать кнопку «Настроить сертификаты».

Для установки сертификата необходимо перейти во вкладку «Доверенные корневые центры сертификации» и нажать кнопку «Импорт...». В открывшемся окне необходимо нажать кнопку «Далее >».

Для выбора файла сертификата необходимо нажать кнопку «Обзор..» и выбрать файл сертифика. Нажать кнопку «Открыть», а затем кнопку «Далее >».

Предлагаемое по умолчанию хранилище сертификатов должно совпадать с тем, куда следует поместить корневой сертификат. Если импорт был инициирован из другого раздела хранилища сертификатов, то необходимо выбрать по кнопке «Обзор...» хранилище «Доверенные корневые центры сертификации» и нажать кнопку «Далее >».

Затем следует подтвердить завершение работы мастера, нажав кнопку «Готово», затем кнопку «Да» и кнопку «ОК».

Для контроля правильности проделанных операций в «Сертификаты» - «Доверенные корневые центры сертификации» в конце списка необходимо найти установленный раннее корневой сертификат.

Затем необходимо перезагрузить веб-браузер.

11.43. Настройка статической маршрутизации

Для настройки статической маршрутизации необходимо перейти в «Система» - «Шлюзы» - «Единичный» и нажать кнопку «+». В поле «Имя» ввести название шлюза. В поле «Интерфейс» выбрать сетевой интерфейс, через который будет проходить маршрут. В поле «Семейство адресов» выбрать версию протокола IP. В поле «IP-адрес» ввести IP-адрес шлюза. Нажать кнопку «Сохранить».

Затем перейти в «Система» - «Маршруты» - «Конфигурация» и нажать кнопку «+». В поле «Адрес сети» необходимо ввести адрес сети (в формате [адрес сети]/[маска сети]) конечной точки маршрута. В поле «Шлюз»

выбрать созданный шлюз. В поле «Описание» ввести описание маршрута. Нажать кнопку «Сохранить изменения».

12. Сообщения пользователю

При неправильном вводе в системе возникает ошибка «ошибка на стороне сервера (рисунок 404).

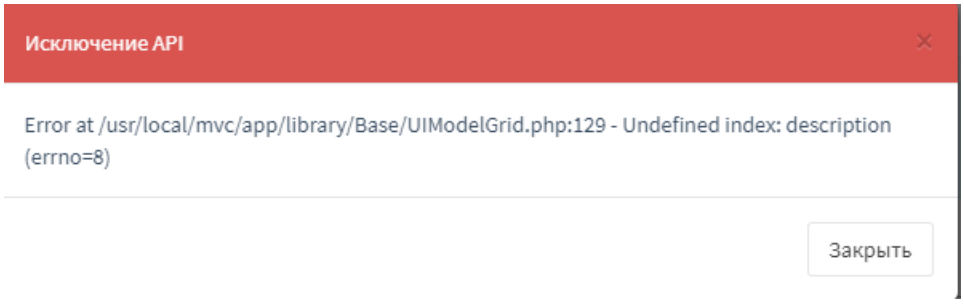


Рисунок 404— Ошибка на стороне сервера

При любом удалении появляется всплывающее предупреждение (рисунок 405).

Рисунок 405 — Удаление

При любом неправильном вводе в поля появляется предупреждение вверху страницы (рисунок 406) или напротив неправильно введенный полей (рисунок 407).

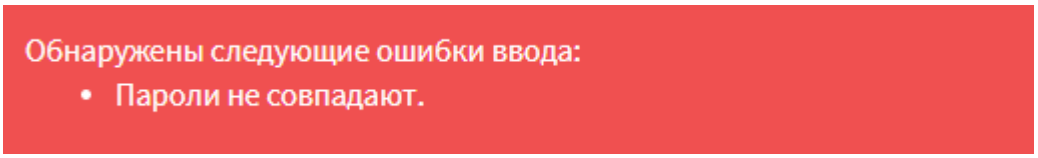


Рисунок 406 — Предупреждение о неправильном вводе в поле (вид 1)

Рисунок 407 — Предупреждение о неправильном вводе в поле (вид 2)

При применении настроек появляется предупреждение вверху страницы (рисунок 408).

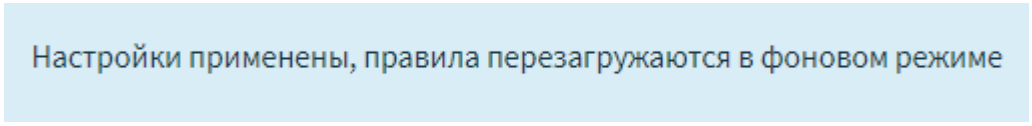


Рисунок 408 — Применено изменение

При импорте файла с некорректными правилами системы обнаружения вторжений в формате Snort в разделе меню «Обнаружение вторжений» - «Администрирование» - «Обновление» правила не будут добавлены. Запись об этом появится в «Обнаружение вторжений» - «Журнал» (рисунок 409).

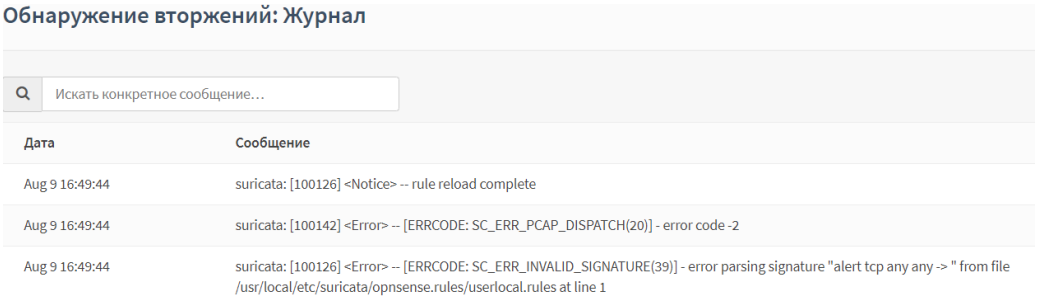


Рисунок 409 — Некорректный файл правил системы обнаружения вторжений