



Программный комплекс INFOWATCH ARMA FIREWALL

Межсетевой экран нового поколения
для промышленных и корпоративных сетей



Руководство по интерфейсу

версия 13 ред. от 22.11.2024

Листов 33

СОДЕРЖАНИЕ

1	Запуск и авторизация.....	8
2	Описание веб-интерфейса	9
2.1	Область быстрой навигации	9
2.1.1	Логотип ARMA FW	10
2.1.2	Индикатор уведомлений	10
2.1.3	Меню пользователя	10
2.1.4	Область поиска	11
2.2	Область меню	11
2.3	Форма раздела меню	13
2.4	Дополнительная функциональность веб-интерфейса.....	13
2.4.1	Справочная информация	13
2.4.2	Расширенный режим	14
2.4.3	Вкладки	15
2.4.4	Выпадающие списки.....	15
2.4.5	Индикатор заполнения.....	16
3	Описание основных разделов	17
3.1	Инструменты	17
3.2	Создание отчетов.....	17
3.3	Межсетевой экран.....	17
3.4	Обнаружение вторжений.....	18
3.5	Система	18
3.6	Интерфейсы	20
3.7	Сеть.....	20
3.8	Маршрутизация	20
3.9	Службы.....	20
3.10	VPN.....	21
4	Описание информационных виджетов	22
4.1	Виджет «Системная информация».....	22
4.2	Виджет «Службы».....	23
4.3	Виджет «Шлюзы».....	24
4.4	Виджет «Интерфейсы».....	24

4.5	Виджет «Использование ЦП»	25
4.6	Виджет «Журнал Syslog»	25
4.7	Виджет «CARP»	26
4.8	Виджет «Статистика интерфейса»	26
4.9	Виджет «Журнал межсетевого экрана»	26
4.10	Виджет «Monit»	27
4.11	Виджет «Сетевое время»	27
4.12	Виджет «Тепловые датчики»	27
4.13	Виджет «Графики трафика»	28
4.14	Виджет «OpenVPN»	29
4.15	Виджет «IPsec»	29
4.16	Виджет «Информация о лицензии»	30
5	Сообщения пользователю	31
5.1	Неправильный ввод в системе	31
5.2	Предупреждение об удалении	31
5.3	Некорректный ввод данных в поле	31
5.4	Предупреждение при применении настроек	32
5.5	Нарушение контроля целостности	32
5.6	Превышение количества попыток авторизации	33

ТЕРМИНЫ И СОКРАЩЕНИЯ

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

Таблица «Термины и сокращения»

Термины и сокращения	Значение
МП	Материнская плата
МЭ	Межсетевой экран
ОС	Операционная система
ПО	Программное обеспечение
СОВ	Система обнаружения вторжений
ЦП	Центральный процессор
ACPI	Advanced Configuration and Power Interface – усовершенствованный интерфейс управления конфигурацией и питанием
ARMA FW	InfoWatch ARMA Firewall
ARP	Address Resolution Protocol – протокол, предназначенный для определения MAC-адреса по известному IP-адресу
CARP	Common Address Redundancy Protocol – протокол дубликации общего адреса
CEF	Common Event Format – открытый формат журнала событий
DHCP	Dynamic Host Configuration Protocol, протокол динамической настройки узла
DNS	Domain Name System, система доменных имён – компьютерная распределённая система для получения информации о доменах
FTP	File Transfer Protocol – протокол передачи файлов по сети
ICAP	Internet Content Adaptation Protocol – протокол адаптации интернет-контента
IP	Internet Protocol, межсетевой протокол – маршрутизируемый протокол сетевого уровня стека TCP/IP

Термины и сокращения	Значение
IPsec	IP Security – набор протоколов для обеспечения защиты данных
LAGG	Link aggregation interface – интерфейс агрегированного канала
LAN	Local Area Network – локальная вычислительная сеть
MAC-адрес	Media Access Control – идентификатор, присваиваемый каждому интерфейсу единицы сетевого оборудования
MBUF	Структура элемента описания в сообщении
NAT	Network Address Translation, преобразование сетевых адресов – механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов
NDP	Neighbor Discovery Protocol, протокол обнаружения соседей – протокол, предназначенный для автонастройки адреса конечных и промежуточных точек сети, обнаружения других узлов на линии, определения адреса других узлов канального уровня, обнаружения конфликта адресов, поиска доступных маршрутизаторов, определения префикса адреса и поддержки доступности информации о путях к другим активным соседним узлам
Netflow	Сетевой протокол, предназначенный для учёта сетевого трафика
NTP	Network Time Protocol, протокол сетевого времени – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью
OpenSSL	Криптографическая библиотека с открытым исходным кодом
OSPF	Open Shortest Path First – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и использующий для нахождения кратчайшего пути алгоритм Дейкстры
RIP	Routing Information Protocol – протокол маршрутной информации
SMB	Server Message Block – сетевой протокол прикладного уровня для удалённого доступа к файлам

Термины и сокращения	Значение
SNMP	Simple Network Management Protocol, простой протокол сетевого управления – стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP
SSH	Secure Shell, безопасная оболочка – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
Syslog	System Log – стандарт отправки и регистрации сообщений о происходящих в системе событиях
VLAN	Virtual Local Area Network – виртуальная локальная компьютерная сеть
VPN	Virtual Private Network, виртуальная частная сеть – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети
VXLAN	Virtual Extensible Local Area Network – технология сетевой виртуализации, созданной для решения проблем масштабируемости

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

Таблица «Смежные документы»

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

АННОТАЦИЯ

Настоящее руководство по интерфейсу предназначено для технических специалистов и пользователей, выполняющих конфигурирование и мониторинг работы **ARMA Firewall v.3.13** и является дополнением к Руководству пользователя **ARMA FW**.

Руководство по интерфейсу описывает порядок работы с веб-интерфейсом **ARMA FW** и функции его основных разделов.

В настоящем руководстве представлено описание веб-интерфейса на русском языке. Параметры первоначальной настройки описаны в разделе **«Установка и первоначальная настройка системы»** Руководства администратора **ARMA FW**.

Для корректного отображения веб-интерфейса к веб-браузерам предъявляются следующие требования:

- для ОС семейства Windows – Яндекс Браузер, Chrome, Firefox;
- для ОС семейства Linux – Яндекс Браузер, Chrome для Linux, Firefox для Linux.

1 ЗАПУСК И АВТОРИЗАЦИЯ

Для доступа к веб-интерфейсу управления **ARMA FW** необходимо открыть веб-браузер, в адресной строке указать IP-адрес интерфейса, используемого для доступа к **ARMA FW**, и нажать **клавишу «Enter»**. В результате будет отображена форма аутентификации (см. [Рисунок – Вход в систему](#)). По умолчанию используются следующие параметры:

- «IP-адрес» – «192.168.1.1»;
- «Протокол подключения» – «HTTPS».

Для начала работы с **ARMA FW** необходимо авторизоваться. Для этого выполнить следующие действия:

1. В поле «Имя пользователя:» ввести «root».
2. В поле «Пароль:» ввести пароль, заданный при установке **ARMA FW**, по умолчанию – «root».
3. Нажать **кнопку «Войти»** для входа в систему.

The image shows a web-based login interface for ARMA Firewall. At the top, there is a dark blue header with the ARMA logo (a stylized helmet) and the word 'FIREWALL' in white. Below the header, the main content area is white. It contains two labels: 'Username:' and 'Password:'. Under 'Username:', there is a text input field with the value 'root'. Under 'Password:', there is a text input field with four dots '....'. Below these fields, there is a blue button labeled 'Login' and a blue link labeled 'Update license'. At the bottom of the page, there is a light gray footer with the text 'InfoWatch ARMA Firewall (c) 2019-2023'.

Рисунок – Вход в систему

2 ОПИСАНИЕ ВЕБ-ИНТЕРФЕЙСА

Общий вид веб-интерфейса **ARMA FW** представлен на рисунке (см. [Рисунок – Веб-интерфейс ARMA FW](#)).

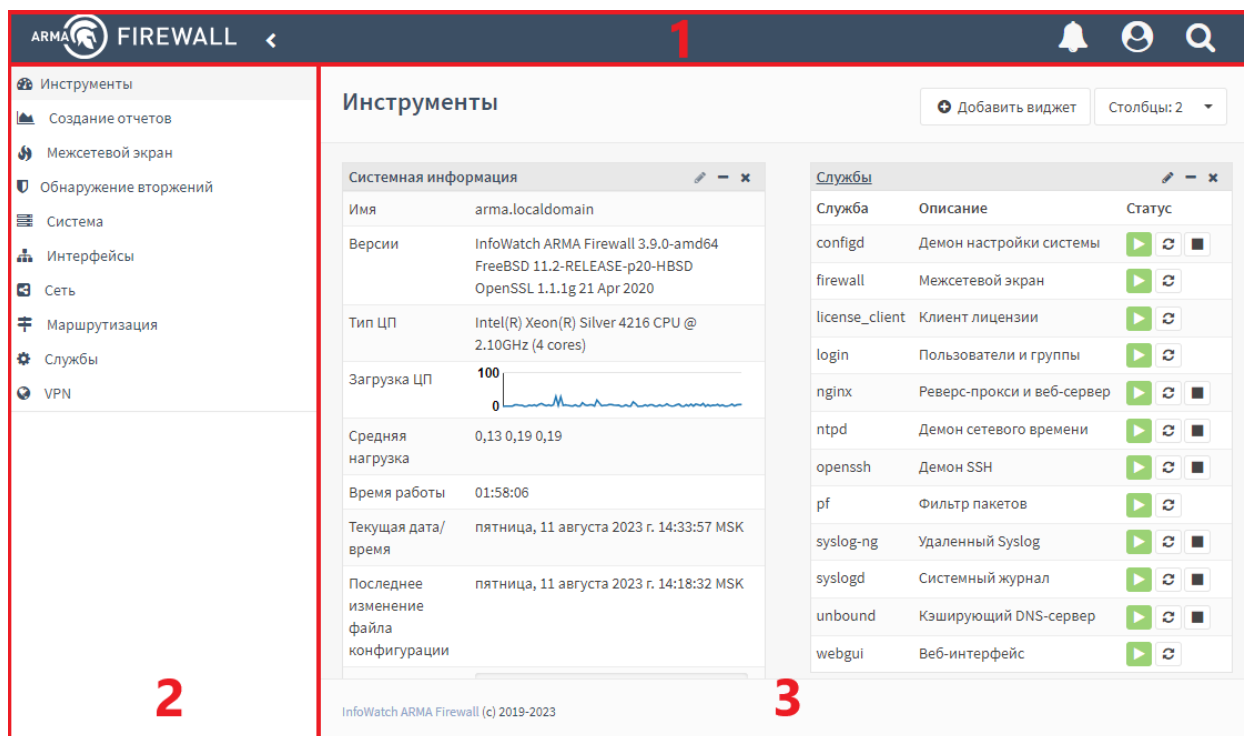


Рисунок – Веб-интерфейс ARMA FW

Основные разделы веб-интерфейса:

- область быстрой навигации (1);
- область меню (2);
- форма раздела меню (3).

2.1 Область быстрой навигации

Область быстрой навигации **ARMA FW** представлена на рисунке (см. [Рисунок – Область быстрой навигации](#)).



Рисунок – Область быстрой навигации

Область быстрой навигации доступна в любом разделе веб-интерфейса и содержит:

- логотип **ARMA FW** (1);
- индикатор уведомлений (2);
- меню пользователя (3);
- область поиска (4).

2.1.1 Логотип ARMA FW

При нажатии на логотип **ARMA FW** в любом разделе веб-интерфейса происходит переход в раздел «**Инструменты**».

2.1.2 Индикатор уведомлений

Индикатор уведомлений выполняет функцию оповещения о новых событиях **ARMA FW**. При появлении нового события на индикаторе отображается количество непрочитанных событий (см. [Рисунок – Оповещение об уведомлении](#)).

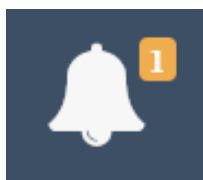


Рисунок – Оповещение об уведомлении

При нажатии **кнопки** «» отображается список всех уведомлений (см. [Рисунок – Список непрочитанных уведомлений](#)).

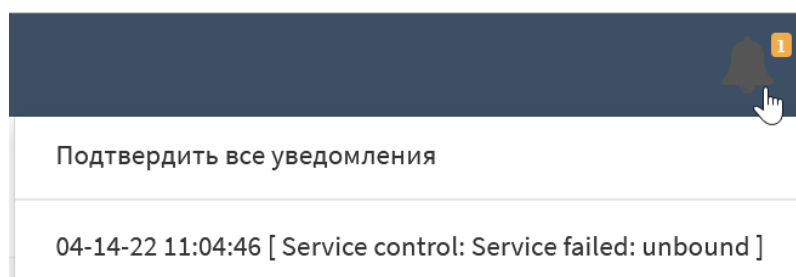


Рисунок – Список непрочитанных уведомлений

2.1.3 Меню пользователя

Меню пользователя выполняет следующие функции:

- отображение профиля текущего пользователя в формате «[Имя_пользователя]@[имя_хоста.название_домена]»;
- выход из веб-интерфейса.

Изменение имени хоста и доменного имени осуществляется в подразделе общих настроек («**Система**» - «**Настройки**» - «**Общие настройки**»).

Для выхода из веб интерфейса необходимо нажать **кнопку** «», а затем нажать **кнопку «Выход»** (см. [Рисунок – Меню пользователя](#)).

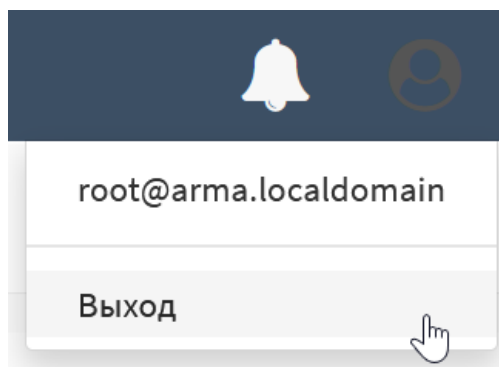


Рисунок – Меню пользователя

2.1.4 Область поиска

Область поиска выполняет функцию быстрой навигации по веб-интерфейсу. Для активации режима поиска по веб-интерфейсу необходимо нажать **кнопку** «».

При наборе текста в поле поиска отображаются предложения поисковых запросов по ключевым словам (см. [Рисунок – Результаты поиска](#)). Для перехода в предложенный раздел необходимо:

- выбрать строку с предложенным разделом **клавишами «Стрелка вверх»** или **«Стрелка вниз»** и нажать **клавишу «ENTER»**;
- выбрать строку с предложенным разделом нажатием **левой кнопки мыши**.

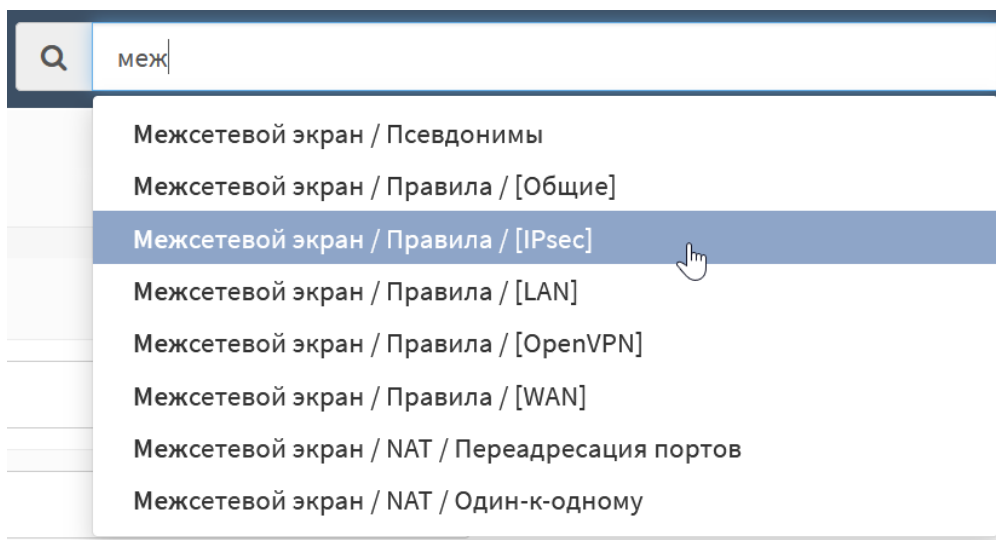


Рисунок – Результаты поиска

2.2 Область меню

Область меню (см. [Рисунок – Область меню](#)) предназначена для осуществления доступа к различным функциям **ARMA FW**, переход к которым осуществляется нажатием **левой кнопки мыши**.

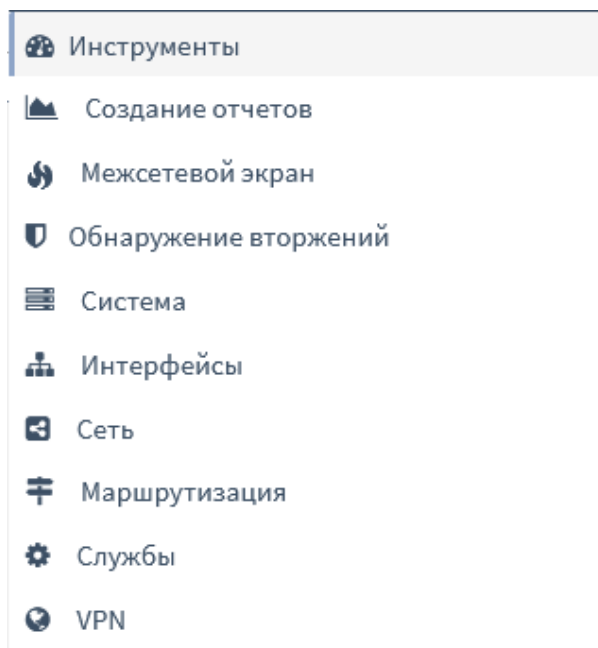


Рисунок – Область меню

В меню существуют следующие уровни вложенности:

- **раздел;**
- **подраздел;**
- **категория** – присутствует не во всех подразделах.

Пример уровней вложенности представлен на рисунке (см. [Рисунок – Пример уровней вложенности](#)):

- **«Система»** – раздел;
- **«Доступ»** – подраздел;
- **«Пользователи»** – категория.

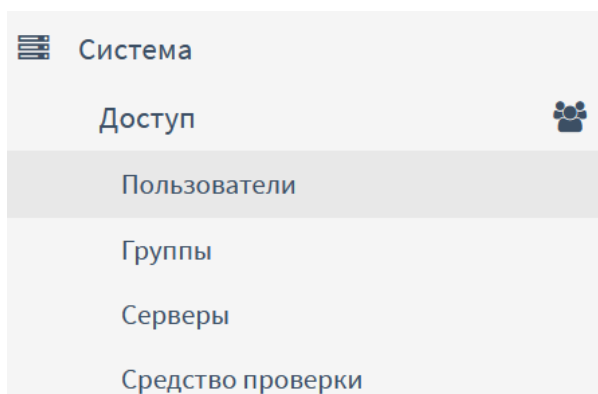


Рисунок – Пример уровней вложенности

2.3 Форма раздела меню

В качестве примера представлена форма раздела «**Инструменты**» (см. [Рисунок – Форма раздела меню](#)).

Инструменты 1

Сохранить настройки | + Добавить виджет | Столбцы: 1 2

Интерфейсы

Имя	Статус	IP-адрес
LAN	↑	192.168.1.1
WAN	↑	192.168.73.145

Шлюзы

Имя	Время приема-передачи (RTT)	RTTd	Потеря	Статус
WAN_DHCP 192.168.73.2	~	~	~	Онлайн 3

Рисунок – Форма раздела меню

Форма раздела меню содержит:

- название раздела/подраздела/категории (1);
- функциональные кнопки (2) – присутствуют не во всех разделах;
- содержание раздела (3).

2.4 Дополнительная функциональность веб-интерфейса

2.4.1 Справочная информация

Формы разделов меню могут иметь встроенную справку (см. [Рисунок – Переключатель справки](#)).

Маршрутизация: Общие настройки

справка 

Включить ☐

Создание файла журнала ☐

Рисунок – Переключатель справки

При нажатии **кнопки-переключателя «Справка»**  в правом верхнем углу формы будут отображены все справочные сообщения под соответствующими элементами (см. [Рисунок – Справочная информация](#)).

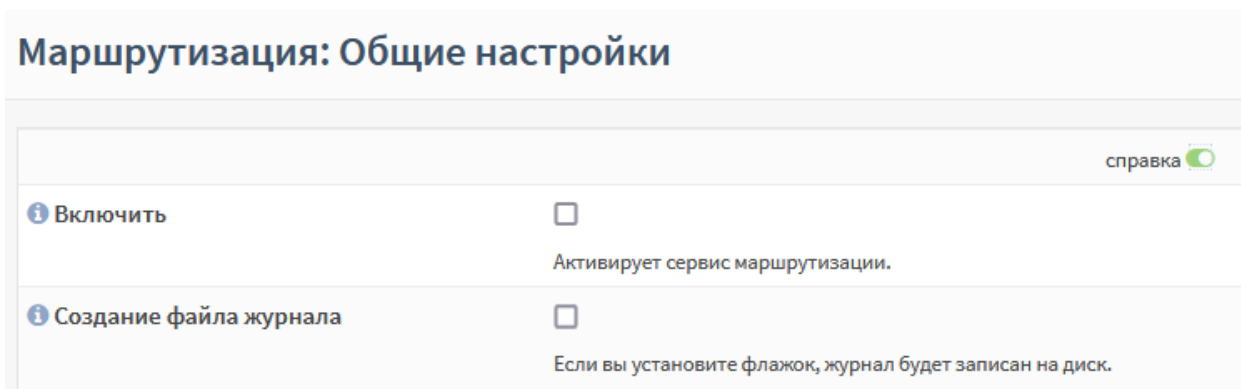


Рисунок – Справочная информация

Для вывода справочного сообщения под единственным элементом (см. [Рисунок – Справочная информация выбранного элемента](#)) необходимо нажать **кнопку** «», расположенную слева от элемента.

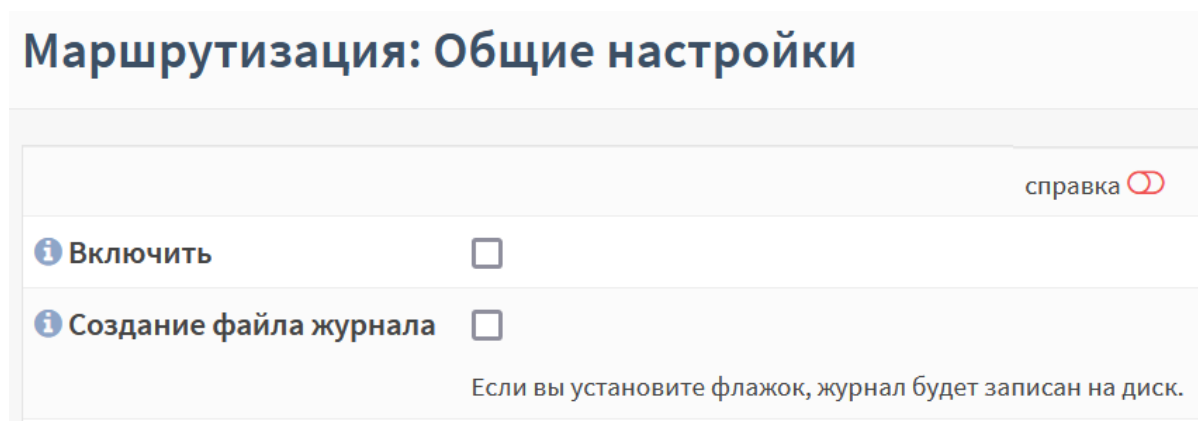


Рисунок – Справочная информация выбранного элемента

Цвет **кнопки** зависит от наличия справочного сообщения для элемента:

- синий «» – элемент содержит справочное сообщение;
- серый «» – элемент не содержит справочное сообщение.

2.4.2 Расширенный режим

Форма раздела меню может иметь расширенный режим работы (см. [Рисунок – Переключатель расширенного режима](#)).

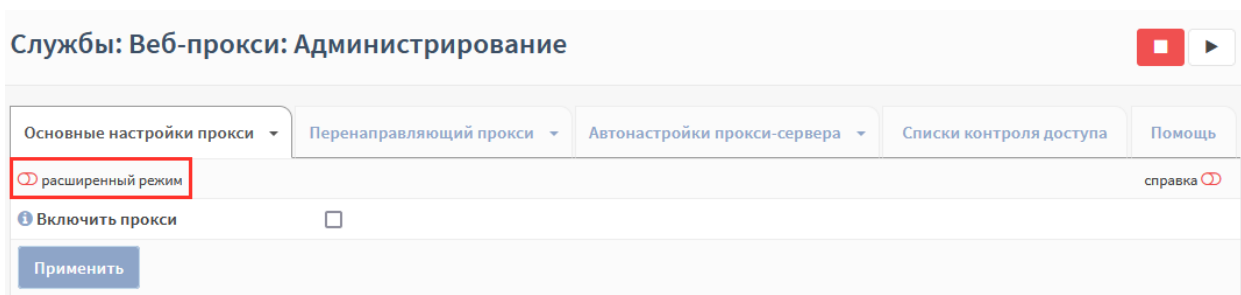


Рисунок – Переключатель расширенного режима

При нажатии **кнопки-переключателя «расширенный режим»**  в левом верхнем углу формы будут отображены дополнительные настройки раздела (см. [Рисунок – Расширенный режим](#)).

Рисунок – Расширенный режим

2.4.3 Вкладки

В разделе могут присутствовать вложенные страницы. Для открытия формы вложенной страницы необходимо нажать на заголовок вкладки (см. [Рисунок – Открытие формы вкладки](#)).

Рисунок – Открытие формы вкладки

2.4.4 Выпадающие списки

В форме раздела меню могут присутствовать выпадающие списки. Для просмотра всех элементов выпадающего списка необходимо нажать **кнопку «▼»** (см. [Рисунок – Выпадающие списки](#)).

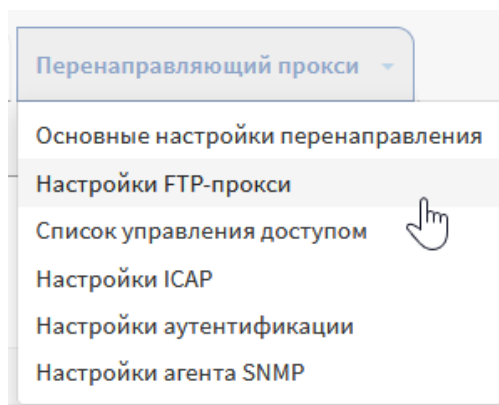


Рисунок – Выпадающие списки

При большом количестве элементов выпадающего списка возможно наличие полосы прокрутки в правой части области доступных элементов списка. Прокрутка списка возможна с помощью перемещения ползунка полосы прокрутки или с помощью колёсика мыши.

2.4.5 Индикатор заполнения

В форме раздела меню может присутствовать индикатор заполнения, отображающий уровень использования выделенной памяти для записей в таблице МЭ (см. [Рисунок – Индикатор заполнения](#)).

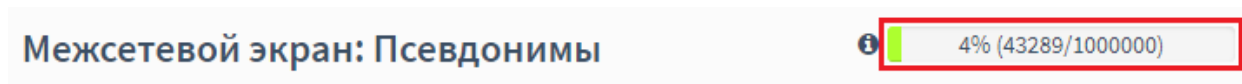


Рисунок – Индикатор заполнения

3 ОПИСАНИЕ ОСНОВНЫХ РАЗДЕЛОВ

3.1 Инструменты

Раздел **«Инструменты»** является стартовым разделом после аутентификации в **ARMA FW** по умолчанию. Раздел позволяет:

- просматривать информацию, выдаваемую информационными виджетами;
- добавлять, скрывать, настраивать виджеты;
- выбирать количество столбцов отображения виджетов на инструментальной панели;
- изменять компоновку виджетов.

3.2 Создание отчетов

Раздел **«Создание отчетов»** позволяет:

- просматривать общее состояние и производительность системы в течение времени;
- просматривать в виде графика или таблицы и экспортировать для дальнейшего анализа статистику количества пакетов в течение времени на определённом сетевом интерфейсе;
- просматривать в виде графика или таблицы и экспортировать для дальнейшего анализа статистику использования памяти, MBUF, состояний, загруженности процессора и в случае доступности температуры процессора;
- просматривать в виде графика или таблицы и экспортировать для дальнейшего анализа статистику использования сервисов;
- просматривать в виде графика или таблицы и экспортировать для дальнейшего анализа статистику полного входящего/исходящего трафика в пакетах и байтах по всем сетевым интерфейсам;
- просматривать и экспортировать для дальнейшего анализа данные Netflow;
- просматривать статистику использования портов и IP-адресов на выбранном сетевом интерфейсе;
- просматривать 25 наиболее активных пользователей для выбранного сетевого интерфейса.

Экспорт данных производится в формате **«csv»**.

3.3 Межсетевой экран

Раздел меню **«Межсетевой экран»** позволяет:

- задавать правила блокировки, разрешения или отклонения трафика для существующих сетевых интерфейсов на промышленном, сетевом и прикладном уровнях;
- настраивать ограничение трафика – приоритеты, пропускную способность каналов;
- задавать правила NAT;
- создавать виртуальные IP-адреса;
- просматривать журнал событий МЭ;
- экспортировать события МЭ за промежуток времени на выбранном интерфейсе.

3.4 Обнаружение вторжений

Раздел меню «**Обнаружение вторжений**» предназначен для включения и настройки COB, в том числе в режиме предотвращения вторжений.

Данный раздел меню позволяет:

- создавать правила COB по шаблонам;
- локально загружать правила COB;
- производить мониторинг событий COB в соответствующем журнале событий;
- включать режим предотвращения вторжений;
- настраивать импорт базы правил COB по FTP/SMB.

3.5 Система

Раздел меню «**Система**» позволяет:

- добавлять, редактировать, удалять пользователей и группы пользователей;
- назначать привилегии пользователям и группам пользователей;
- задавать сложность паролей;
- создавать, редактировать, удалять серверы аутентификации пользователей;
- просматривать контрольные суммы;
- просматривать отчёты об ошибках работы **ARMA FW**;
- обновлять ПО **ARMA FW**;
- настраивать общие параметры **ARMA FW**;
- выбирать часовой пояс;

- выбирать язык веб-интерфейса;
- настраивать доступ по SSH;
- настраивать консольный интерфейс;
- настраивать веб-интерфейс;
- изменять пароль;
- настраивать системный журнал – количество записей, типы отображаемых событий и другое;
- настраивать SNMP;
- настраивать планировщик задач Cron;
- просматривать информацию о лицензии;
- выполнять обновление лицензии;
- создавать, редактировать, удалять сетевые шлюзы;
- задавать статические маршруты;
- настраивать кластеризацию;
- настраивать отказоустойчивый кластер и отслеживать статус **ARMA FW** в составе кластера;
- просматривать, обновлять, останавливать и включать настроенные службы;
- сохранять текущую конфигурацию;
- настраивать экспорт конфигурации на удалённый сервер;
- восстанавливать конфигурацию;
- просматривать и отменять изменения конфигурации **ARMA FW**;
- настраивать экспорт конфигурации по FTP/SMB;
- создавать, редактировать и удалять сертификаты;
- осуществлять начальную настройку системы;
- просматривать журнал системных событий;
- просматривать журнал веб-интерфейса;
- просматривать журнал SYSLOG;
- просматривать журнал backend;
- просматривать журнал событий безопасности;
- просматривать журнал действий пользователя;
- экспортировать события по SYSLOG;

- экспортировать события по CEF;
- перезагружать или выключать **ARMA FW**.

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 и разрешённых, заблокированных пакетов на выбранном сетевом интерфейсе;
- настраивать режим сетевого моста;
- настраивать VLAN, VXLAN, LAGG;
- просматривать DNS-записи, ARP- и NDP-таблицы;
- производить захват пакетов на выбранном сетевом интерфейсе с возможностью экспорта;
- осуществлять проверку работы и приёма соединения хоста на выбранном порте;
- проверять доступность хостов с помощью команды «ping»;
- осуществлять трассировку маршрутов.

3.7 Сеть

Раздел меню «**Сеть**» позволяет:

- запускать сервис обнаружения устройств «Arpwatch»;
- просматривать таблицу обнаруженных устройств;
- запускать анализ дампов трафика;
- просматривать в виде таблицы удовлетворяющие заданным фильтрам пакеты, проходящие через выбранный сетевой интерфейс **ARMA FW**.

3.8 Маршрутизация

Раздел меню «**Маршрутизация**» позволяет настраивать динамическую маршрутизацию по протоколам RIP v1, 2 и OSPF, а также просматривать журнал событий служб динамической маршрутизации.

3.9 Службы

Раздел меню «**Службы**» позволяет:

- включать/выключать и настраивать портал авторизации;
- включать/выключать и настраивать DHCP-сервер;
- включать/выключать и настраивать модуль Dnsmasq DNS;
- включать/выключать и настраивать службу Dr.Web;
- включать/выключать и настраивать службу LLDP;
- включать/выключать и настраивать утилиту мониторинга «Monit»;
- настраивать синхронизацию времени по протоколу NTP;
- включать/выключать и настраивать службу nginx;
- включать/выключать и настраивать службу RSPAN;
- включать/выключать и настраивать кэширующий DNS-сервер;
- включать/выключать и настраивать веб-прокси;
- просматривать журналы событий портала авторизации, прокси-сервера, DHCP-сервера, Dr.Web, ICAPD.

3.10 VPN

Раздел меню «**VPN**» позволяет настраивать виртуальную частную сеть с помощью технологий IPsec и OpenVPN.

Порядок настройки виртуальной частной сети описан в разделе «**VPN**» Руководства пользователя **ARMA FW**.

4 ОПИСАНИЕ ИНФОРМАЦИОННЫХ ВИДЖЕТОВ

ARMA FW позволяет производить мониторинг текущего состояния с помощью различных виджетов, доступных в разделе «**Инструменты**» (см. [Рисунок – Раздел «Инструменты»](#)).

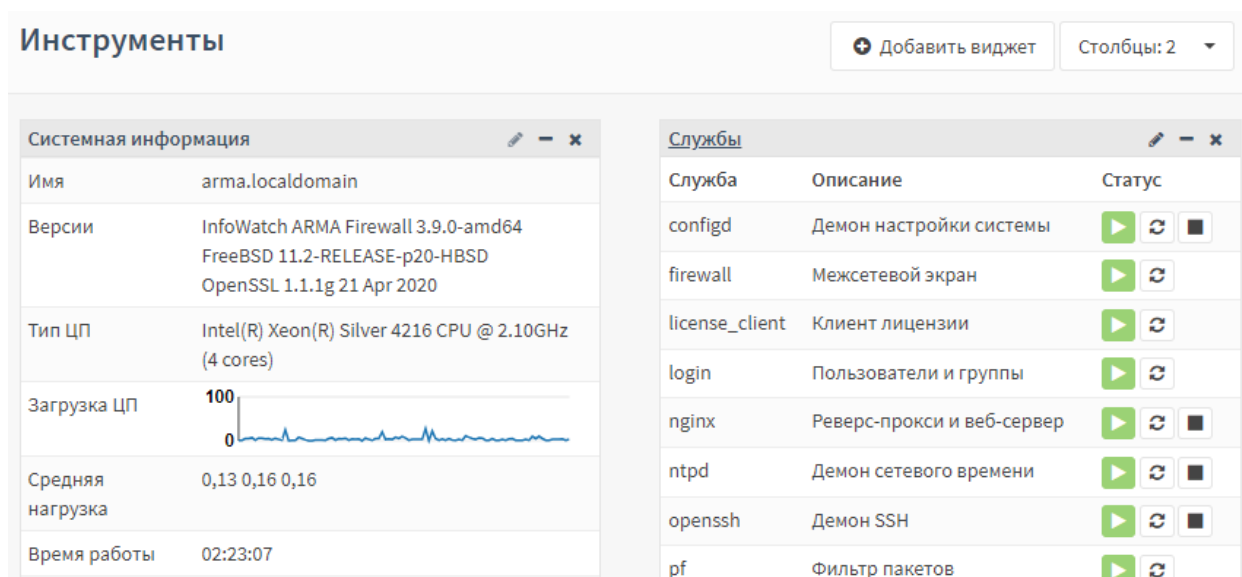


Рисунок – Раздел «Инструменты»

Порядок работы с виджетами описан в разделе «**Мониторинг системы с помощью информационных виджетов**» Руководства пользователя **ARMA FW**.

4.1 Виджет «Системная информация»

Виджет «**Системная информация**» (см. [Рисунок – Виджет «Системная информация»](#)) отображает основную информацию об **ARMA FW**:

- доменное имя **ARMA FW**;
- версию **ARMA FW**, ОС и OpenSSL;
- тип процессора;
- загрузку процессора в виде графика;
- среднюю нагрузку;
- время работы системы;
- текущие дату и время;
- дату последнего изменения файла конфигурации;
- размер таблицы состояний;
- процент использования MBUF;
- процент использования оперативной памяти;

- процент использования дискового накопителя.

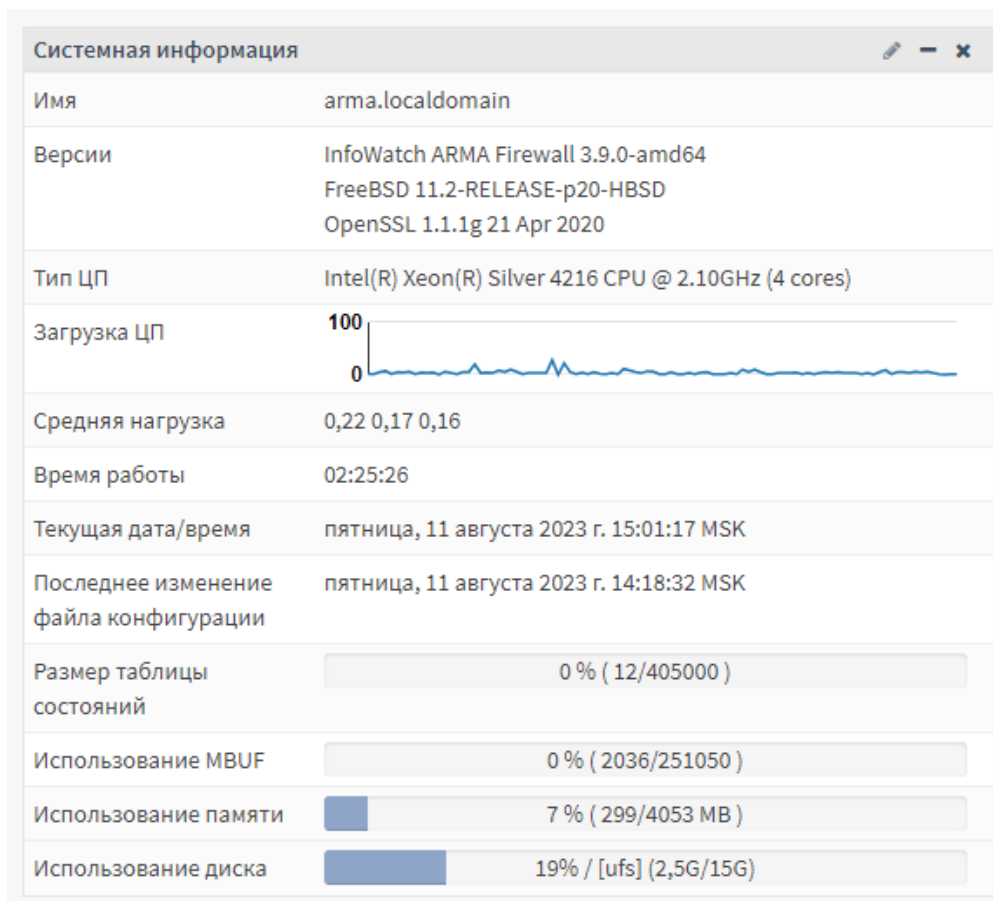


Рисунок – Виджет «Системная информация»

4.2 Виджет «Службы»

Виджет «Службы» (см. [Рисунок – Виджет «Службы»](#)) отображает настроенные службы **ARMA FW**.

Настроенные службы представлены в виде строк, содержащих имя службы с описанием и кнопки управления:

- «» - остановить службу;
- «» - запустить службу;
- «» - перезагрузить службу.

Цвет кнопок обозначает статус службы:

- **кнопка «запустить»** зелёного цвета «» - служба запущена;
- **кнопка «остановить»** красного цвета «» - служба остановлена.

Для удаления из виджета определённых служб необходимо нажать **кнопку** «», в появившемся поле ввести названия служб и нажать **кнопку «Сохранить»**.

Указанные значения должны соответствовать названию из столбца «Службы» виджета. Множественные значения разделяются запятой.

Службы		
Службы	Описание	Статус
captiveportal	Портал авторизации	 
configd	Демон настройки системы	  
dhcpd	DHCPv4-сервер	  
dhcpd6	DHCPv6-сервер	 
firewall	Межсетевой экран	 
license_client	Клиент лицензии	 
login	Пользователи и группы	 
squid	Веб-прокси	 
strongswan	IPsec VPN	  
suricata	Обнаружение вторжений	  

Рисунок – Виджет «Службы»

4.3 Виджет «Шлюзы»

Виджет «Шлюзы» (см. [Рисунок – Виджет «Шлюзы»](#)) отображает настроенные шлюзы, их статус, время приема-передачи и потери передачи.

Шлюзы				
Имя	Время приема-передачи (RTT)	RTTd	Потеря	Статус
WAN_DHCP 192.168.73.2	~	~	~	

Рисунок – Виджет «Шлюзы»

4.4 Виджет «Интерфейсы»

Виджет «Интерфейсы» (см. [Рисунок – Виджет «Интерфейсы»](#)) отображает включённые сетевые интерфейсы и их основные параметры: имя, скорость и режим передачи, IP-адрес.

Для настройки отображаемых интерфейсов необходимо нажать **кнопку** «», выбрать значения из выпадающих списков и нажать **кнопку** «Сохранить».

Интерфейсы			
 LAN		1000baseT <full-duplex>	192.168.1.1
 WAN		1000baseT <full-duplex>	192.168.73.145

Рисунок – Виджет «Интерфейсы»

4.5 Виджет «Использование ЦП»

Виджет «Использование ЦП» (см. [Рисунок – Виджет «Использование ЦП»](#)) отображает график загрузки ЦП в режиме реального времени.

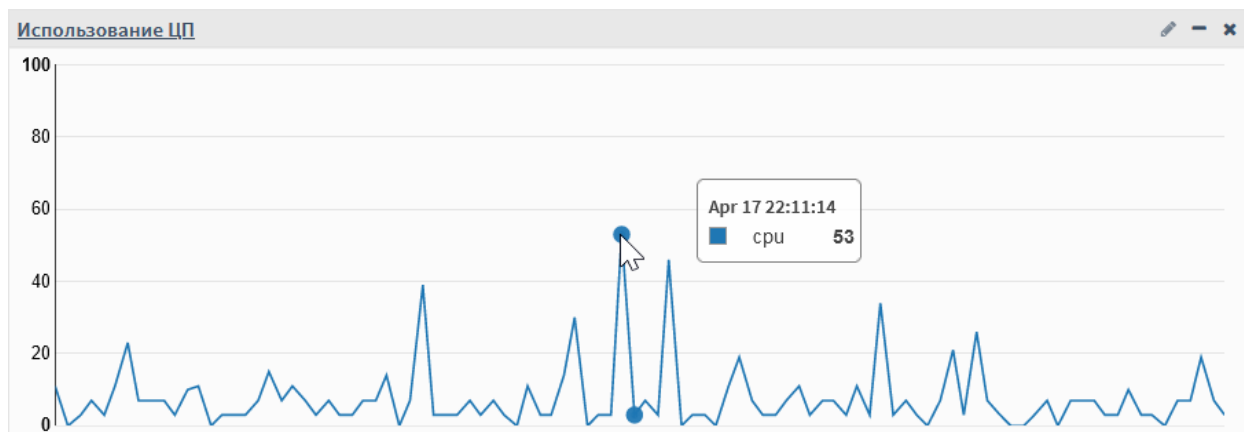


Рисунок – Виджет «Использование ЦП»

4.6 Виджет «Журнал Syslog»

Виджет «Журнал Syslog» (см. [Рисунок – Виджет «Журнал Syslog»](#)) отображает таблицу журнала Syslog в режиме реального времени, содержащую записи с описанием, временем и датой события.

Для редактирования количества отображаемых событий необходимо нажать кнопку «», выбрать значение из выпадающего списка «Количество отображаемых строк журнала:» и нажать кнопку «Сохранить».

Журнал Syslog		 - x
Apr 17 22:18:36	armaif: Пользователь "root" получил доступ к журналу "/ui/diagnostics/firewall/log (Firewall: Log Files: Live View)"	
Apr 17 22:18:36	dhcp6c[6637]: reset a timer on em1, state=SOLICIT, timeo=27, retrans=112500	
Apr 17 22:18:36	dhcp6c[6637]: send solicit to ff02::1:2%em1	
Apr 17 22:18:36	dhcp6c[6637]: set IA_PD	
Apr 17 22:18:36	dhcp6c[6637]: set option request (len 4)	
Apr 17 22:18:36	dhcp6c[6637]: set elapsed time (len 2)	
Apr 17 22:18:36	dhcp6c[6637]: set identity association	
Apr 17 22:18:36	dhcp6c[6637]: set client ID (len 14)	
Apr 17 22:18:36	dhcp6c[6637]: Sending Solicit	
Apr 17 22:18:34	armaif: Пользователь "root" получил доступ к журналу "/ui/diagnostics/firewall/log (Firewall: Log Files: Live View)"	

Рисунок – Виджет «Журнал Syslog»

4.7 Виджет «CARP»

Виджет «**CARP**» (см. [Рисунок – Виджет «CARP»](#)) отображает статус **ARMA FW** при работе в режиме отказоустойчивого кластера, общий совместно используемый виртуальный IP-адрес и сетевой интерфейс.



Рисунок – Виджет «CARP»

4.8 Виджет «Статистика интерфейса»

Виджет «**Статистика интерфейса**» (см. [Рисунок – Виджет «Статистика интерфейса»](#)) отображает сводную таблицу по всем настроенным сетевым интерфейсам в режиме реального времени и содержит следующие данные:

- количество входящих/исходящих пакетов;
- количество входящих/исходящих байтов;
- количество ошибок входящего/исходящего трафика;
- количество коллизий для каждого настроенного сетевого интерфейса.

Для настройки отображаемых интерфейсов необходимо нажать **кнопку** «», выбрать значения из выпадающих списков и нажать **кнопку** «**Сохранить**».

Статистика интерфейса		
	LAN	WAN
Входящие пакеты	2226	40301
Исходящие пакеты	4343	200390
Входящие байты	267 KB	5.83 MB
Исходящие байты	4.84 MB	266.19 MB
Входящие ошибки	0	0
Исходящие ошибки	0	0
Коллизии	0	0

Рисунок – Виджет «Статистика интерфейса»

4.9 Виджет «Журнал межсетевого экрана»

Виджет «**Журнал межсетевого экрана**» (см. [Рисунок – Виджет «Журнал межсетевого экрана»](#)) отображает таблицу событий МЭ в режиме реального времени, содержащую следующую информацию:

- время и дата события;
- интерфейс прохождения трафика;
- действие, применённое к трафику;

- отправители и получатель.

Для настройки виджета необходимо нажать **кнопку** «», выбрать из выпадающих списков значения для:

- количества отображаемых событий;
- интервала обновления таблицы;
- отображаемых сетевых интерфейсов;

установить флажки для фильтрации по действию и нажать **кнопку** «**Сохранить**».

Журнал межсетевого экрана				
Действие	Время	Интерфейс	Отправитель	Получатель
	Apr 17 22:35	wan	192.168.73.1	192.168.73.145
	Apr 17 22:35	wan	192.168.73.145	185.130.104.185
	Apr 17 22:35	lan	fe80::20c:29ff:fea2:bb30	ff02::16
	Apr 17 22:35	lo0	fe80::20c:29ff:fea2:bb30	ff02::1
	Apr 17 22:35	lan	fe80::20c:29ff:fea2:bb30	ff02::1

Рисунок – Виджет «Журнал межсетевого экрана»

4.10 Виджет «Monit»

Виджет «**Monit**» (см. [Рисунок – Виджет «Monit»](#)) отображает состояния почтовых серверов, доступность различных сервисов и ресурсов, состояние сетевых сервисов.

Monit		
Имя	Тип	Статус
Bumerang.localdomain	Система	Может быть изменено
RootFs	Файловая система	ОК

Рисунок – Виджет «Monit»

4.11 Виджет «Сетевое время»

Виджет «**Сетевое время**» (см. [Рисунок – Виджет «Сетевое время»](#)) отображает текущее время системы, а также информацию о сервере синхронизации времени.

Сетевое время	
Время сервера	22:50:05
	46.188.16.150 (stratum 2)

Рисунок – Виджет «Сетевое время»

4.12 Виджет «Тепловые датчики»

Виджет «**Тепловые датчики**» (см. [Рисунок – Виджет «Тепловые датчики»](#)) отображает температуру ЦП, МП по данным ACPI и позволяет задавать различные пороговые значения температуры:

- **«Предупреждение зоны»** – значение температуры МП, достигнув которого, индикатор температуры МП будет отображаться оранжевым цветом;
- **«Критическая зона»** – значение температуры МП, достигнув которого, индикатор температуры МП будет отображаться красным цветом;
- **«Предупреждение ядра»** – значение температуры ЦП, достигнув которого, индикатор температуры ЦП будет отображаться оранжевым цветом;
- **«Критическая ошибка ядра»** – значение температуры ЦП, достигнув которого, индикатор температуры ЦП будет отображаться красным цветом.

Тепловые датчики

Пороговое значение в °C (от 1 до 100):

Предупреждение зоны:

70

Критическая зона:

80

Предупреждение ядра:

70

Критическая ошибка ядра:

80

☐ Показывать только первую найденную температуру ядра процессора

Сохранить

* Вы можете настроить нужный тепловой датчик или модуль (-и) здесь.

60 °C

Материнская плата

75 °C

ЦПУ

Рисунок – Виджет «Тепловые датчики»

4.13 Виджет «Графики трафика»

Виджет **«Графики трафика»** (см. [Рисунок – Виджет «Графики трафика»](#)) отображает график входящего/исходящего трафика в режиме реального времени.

Цвет кнопки рядом с названием интерфейса соответствует цвету линии графика на виджете. Заливка цветом кнопки рядом с названием интерфейса обозначает отображение графика интерфейса на виджете:

- кнопка залита цветом «●» – график интерфейса отображён;
- кнопка не залита цветом «○» – график интерфейса не отображён.

Для переключения режима отображения графика интерфейса необходимо нажать **кнопку** рядом с названием интерфейса.

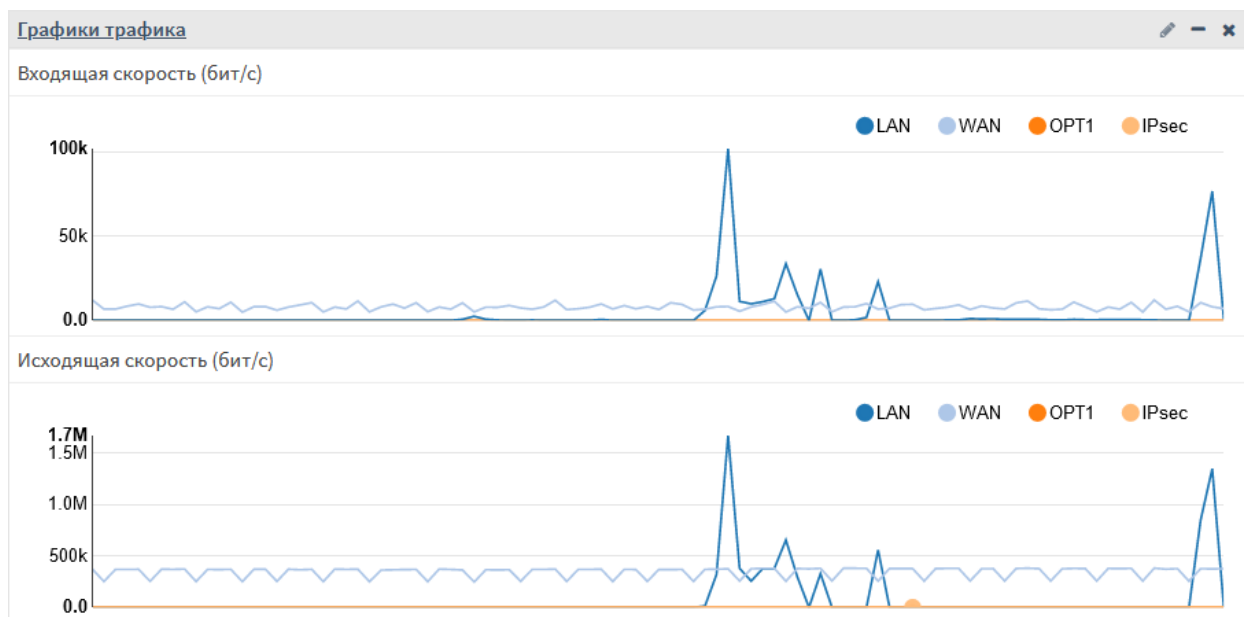


Рисунок – Виджет «Графики трафика»

4.14 Виджет «OpenVPN»

Виджет «OpenVPN» (см. [Рисунок – Виджет «OpenVPN»](#)) отображает настроенные OpenVPN серверы и статистику запросов подключений.

OpenVPN	
GOST#1 TCP:1194 Подключения клиентов	
Имя/время	Реальный/виртуальный IP-адрес
Статистика запросов клиента	
Имя/время	Удаленный/виртуальный IP-адрес
GOST-CLIENT#1 TCP	
2022-04-18 09:29:17	

Рисунок – Виджет «OpenVPN»

4.15 Виджет «IPsec»

Виджет «IPsec» (см. [Рисунок – Виджет «IPsec»](#)) отображает информацию о настроенных туннелях IPsec с возможностью переключения по вкладкам:

- **«Обзор»** – содержит общую информацию о настроенных туннелях;
- **«Туннели»** – содержит информацию о соединении, отправителе, получателе и статусе настроенных туннелей;
- **«Мобильные»** – содержит информацию о пользователе, IP-адресе и статусе мобильных пользователей.

IPsec		
Обзор Туннели Мобильные		
Активные туннели	Неактивные туннели	Мобильные пользователи
0	0	0

Рисунок – Виджет «IPsec»

4.16 Виджет «Информация о лицензии»

Виджет «**Информация о лицензии**» (см. [Рисунок – Виджет «Информация о лицензии»](#)) отображает тип, статус и срок действия лицензии.

Информация о лицензии	
Клиента	Test
Продукт	ARMA Firewall
Тип лицензии	Полная лицензия
Дата активации	10-08-2023 10:47:20
Дата окончания	10-09-2023 10:47:20
Свойства	COB, OPCDA, Промышленные протоколы, Межсетевой экран

Рисунок – Виджет «Информация о лицензии»

5 СООБЩЕНИЯ ПОЛЬЗОВАТЕЛЮ

5.1 Неправильный ввод в системе

При неправильном вводе в системе возникает ошибка «ошибка на стороне сервера» (см. [Рисунок – Ошибка на стороне сервера](#)).

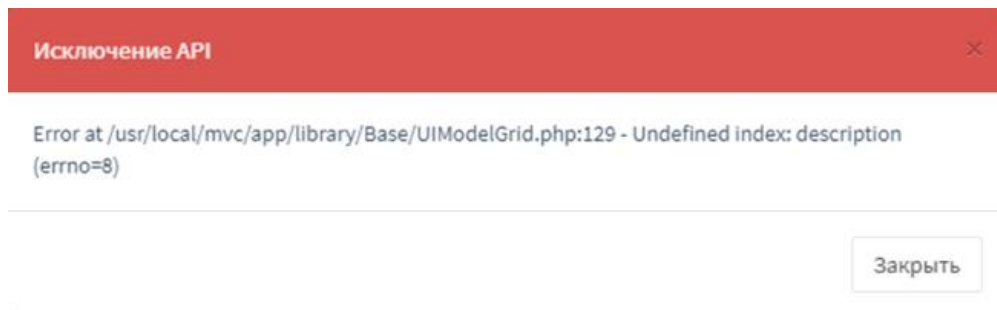


Рисунок – Ошибка на стороне сервера

5.2 Предупреждение об удалении

При любом удалении появляется всплывающее предупреждение (см. [Рисунок – Предупреждение при удалении](#)).

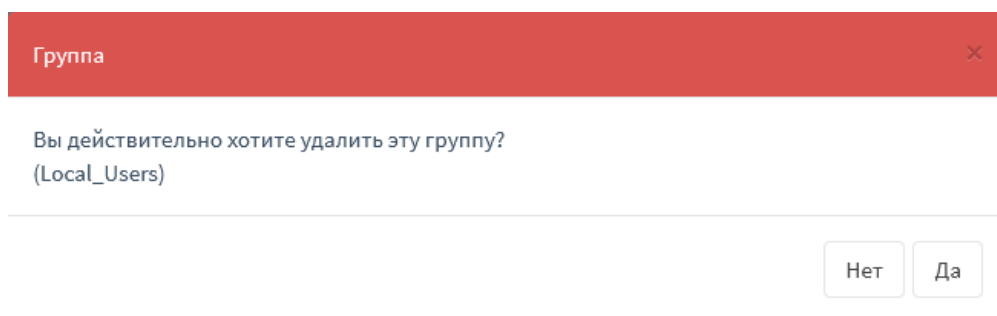


Рисунок – Предупреждение при удалении

5.3 Некорректный ввод данных в поле

При некорректном вводе данных в поле параметра появляется одно из предупреждений:

- вверху страницы (см. [Рисунок – Предупреждение о некорректном вводе вверху страницы](#));

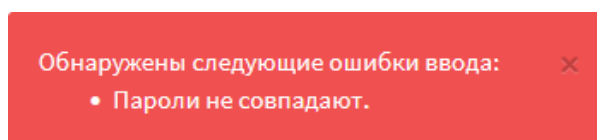


Рисунок – Предупреждение о некорректном вводе вверху страницы

- напротив полей (см. [Рисунок – Предупреждение о некорректном вводе напротив поля](#)).



Сети

192.56 ×

✖ Очистить все

Некорректный список

Рисунок – Предупреждение о некорректном вводе напротив поля

5.4 Предупреждение при применении настроек

При применении настроек появляется уведомление вверху страницы (см. [Рисунок – Применение изменений](#)).

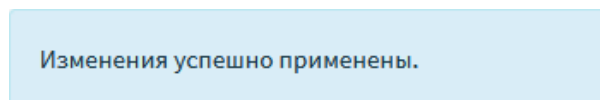


Рисунок – Применение изменений

5.5 Нарушение контроля целостности

В случае, когда проверка контроля целостности не пройдена, будет выведено соответствующее уведомление вверху страницы (см. [Рисунок – Неудачная проверка целостности](#)). Уведомление сохраняется при переходе в любой раздел веб-интерфейса.

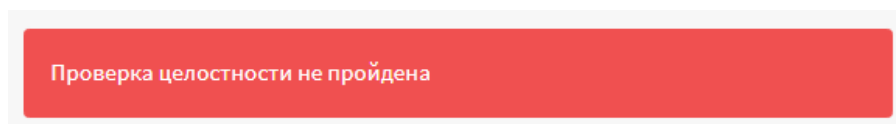


Рисунок – Неудачная проверка целостности

При установке флажка для параметра **«Остановить сервисы»** в подразделе отслеживания контроля целостности (**«Система» - «Прошивка» - «Контроль целостности»**), в случае нарушения целостности любой части **ARMA FW**, блокируется работа всех сервисов **ARMA FW** – дальнейшая эксплуатация невозможна, при этом появится соответствующее уведомление (см. [Рисунок – Автоматическая блокировка межсетевого экрана](#)).

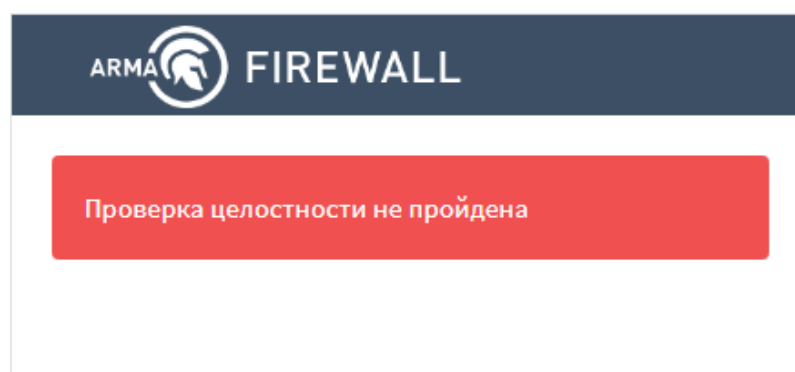


Рисунок – Автоматическая блокировка межсетевого экрана

5.6 Превышение количества попыток авторизации

В случае достижения определённого количества выполняемых подряд попыток авторизации с указанием некорректных учётных данных, **ARMA FW** автоматически выполняет временное блокирование сессии, при этом появится соответствующее уведомление (см. [Рисунок – Превышение количества попыток авторизации](#)).



Рисунок – Превышение количества попыток авторизации